IBM Security QRadar Log Manager
Versión 7.2.4

Guía del usuario

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado "Avisos" en la página 155.

Información sobre el producto

Este documento se aplica a IBM QRadar Security Intelligence Platform V7.2.4 y a los releases subsiguientes a menos que se reemplace por una versión actualizada de este documento.

Contenido

Acerca de la Guía del usuario de QRadar Log Manager

La guía del usuario de IBM® Security QRadar Log Manager proporciona información sobre la gestión de IBM Security QRadar SIEM, incluyendo las pestañas Panel de control, Actividad de registro e Informes.

A quién va dirigida esta guía

Esta guía está pensada para todos los usuarios de QRadar SIEM responsables de investigar y gestionar la seguridad de red. En esta guía se da por supuesto que tiene acceso a QRadar SIEM y que conoce las tecnologías de su empresa.

Documentación técnica

Para obtener información sobre cómo acceder a documentación más técnica, notas técnicas y notas del release, consulte Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0 &uid=swg21612861).

Cómo ponerse en contacto con el servicio de soporte al cliente

Para obtener información sobre cómo ponerse en contacto con el servicio de soporte al cliente, consulte la Support and Download Technical Note (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 los sistemas y la 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 a la información o puede ocasionar daños o un uso erróneo de los sistemas, incluidos los ataques a terceros. Ningún sistema o producto de TI debe ser considerado completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo para impedir el acceso o uso inadecuado. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un procedimiento global de seguridad de acuerdo con la legalidad vigente, lo que implica necesariamente procedimientos operativos adicionales y puede requerir otros sistemas, productos o servicios para ser más eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, NI QUE HAGAN QUE SU EMPRESA SEA INMUNE, A LAS CONDUCTAS MALINTENCIONADAS 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 solo se puede utilizar con fines legales y de forma legal. El cliente se compromete a utilizar este programa en conformidad con las leyes, regulaciones y políticas aplicables y asume toda la responsabilidad de su cumplimiento. El licenciatario declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM Security QRadar.

Capítulo 1. Novedades para los usuarios de QRadar Log Manager V7.2.4

IBM Security QRadar Log Manager V7.2.4 presenta una integración de IBM Security X-Force Threat Intelligence mejorada.

Utilice el canal de información de IBM Security X-Force Threat Intelligence para proporcionar en tiempo real una lista de direcciones IP potencialmente maliciosas

Al contenido del canal de información de X-Force se le da una puntuación de amenaza relativa. Los usuarios de QRadar pueden utilizar esta puntuación de amenaza para priorizar los incidentes y delitos que se generan mediante este contenido. Los datos de estos orígenes de inteligencia se incorporan automáticamente en las funciones de correlación y análisis de QRadar y enriquecen las capacidades de detección de amenazas con datos de amenaza de Internet de última hora. Cualesquiera sucesos de seguridad o datos de actividad de red en los que se vean implicadas estas direcciones se marcan automáticamente y por lo tanto se añade contenido valioso a los análisis y las investigaciones de incidentes de seguridad. Más información.

Más opciones de búsqueda

Los usuarios pueden expandir el cuadro de Búsqueda avanzada para tener más espacio para varias líneas de texto.

Los usuarios pueden buscar sucesos que hayan desencadenado una regla específica mediante la función RuleName.

Más información.

Ariel Query Language (AQL)

Los usuarios disponen de funciones nuevas para sentencias AQL. Más información.

Capítulo 2. QRadar Log Manager

IBM Security QRadar Log Manager es una plataforma de gestión de seguridad de red que proporciona conciencia situacional y apoyo de conformidad a través de correlación de sucesos de seguridad, análisis y generación de informes.

Navegar por la aplicación basada en web

Cuando utilice QRadar Log Manager, utilice las opciones de navegación disponibles en la interfaz de usuario en lugar del botón **Atrás** del navegador web.

Navegadores web soportados

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

Al acceder al sistema de QRadar, se le solicitará un nombre de usuario y una contraseña. El administrador debe configurar de antemano el nombre de usuario y la contraseña.

La tabla siguiente lista las versiones soportadas de navegadores web.

Tabla 1. Navegadores web soportados para productos de QRadar

Navegador web	Versiones soportadas
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, con el modo de documento y el modo de explorador habilitados	9.0 10.0
Google Chrome	Versión actual a partir de la fecha de publicación de los productos de IBM Security QRadar V7.2.4

Habilitación del modo de documento y modo de explorador en Internet Explorer

Si utiliza Microsoft Internet Explorer para acceder a productos de IBM Security QRadar, debe habilitar el modo de explorador y el modo de documento.

Procedimiento

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

Inicio de sesión de IBM Security QRadar

IBM Security QRadar es una aplicación basada en web. QRadar utiliza la información de inicio de sesión predeterminada para el URL, el nombre de usuario y la contraseña.

Utilice la información de la tabla siguiente cuando inicie la sesión en la consola de IBM Security QRadar.

Tabla 2. Información de inicio de sesión predeterminada para QRadar

Información de inicio de sesión	**Valor predeterminado**
URL	https://<Dirección IP>, donde <Dirección IP> es la dirección IP de la consola de QRadar. Para iniciar la sesión en QRadar en un entorno de IPv6 o mixto, escriba la dirección IP entre corchetes: `https://[<Dirección IP>]`
Nombre de usuario	admin
Contraseña	La contraseña que se asigna a QRadar durante el proceso de instalación.
Clave de licencia	Una clave de licencia predeterminada le proporciona acceso al sistema durante 5 semanas.

API RESTful

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

Acceso y permisos de rol de usuario

Debe tener permisos de rol de usuario administrativo en QRadar para acceder y utilizar las API RESTful. Para obtener más información sobre cómo gestionar los permisos de rol de usuario, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

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

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

Tabla 3. Interfaces de 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 las búsquedas guardadas así como actualizar un activo.
`/api/auth`	Cerrar la sesión e invalidar la sesión actual.

Tabla 3. Interfaces de API REST (continuación)

API REST	Descripción
`/api/help`	Devuelve una lista de prestaciones de API.
`/api/siem`	Devuelve una lista de todos los delitos.
`/api/qvm`	Revisar y gestionar datos de QRadar Vulnerability Manager.
`/api/reference_data`	Ver y gestionar recopilaciones de datos de referencia.
`/api/qvm`	Recupera activos, vulnerabilidades, redes, servicios abiertos y filtros. También puede crear o actualizar tíquets de remediación.
`/api/scanner`	Ver, crear o iniciar una exploración remota que esté 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 necesario que se necesita para implementar funciones de QRadar en otros productos.

1. Entre el URL siguiente en el navegador web para acceder a la interfaz de documentación técnica: `https://`*`direcciónIPConsola`*`/api_doc/`.
2. Pulse la cabecera de 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 *experimental* o *estable*.

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

   Estable
   Indica que el punto final de la API se ha probado y se soporta por completo.
5. Pulse **Try it out** para recibir respuestas HTTPS formateadas correctamente.
6. Revise y recopile la información que necesita implementar en la solución de terceros.

Ejemplos de código y de foro de la API de QRadar

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

Pestañas de interfaz de usuario

La funcionalidad se divide en pestañas. La pestaña **Panel de control** se visualiza cuando se inicia la sesión.

Puede desplazarse fácilmente por las pestañas para localizar los datos o la funcionalidad que necesita.

Pestaña Panel de control

La pestaña **Panel de control** es la pestaña predeterminada que se visualiza cuando se inicia la sesión.

La pestaña **Panel de control** es la pestaña predeterminada que se despliega al iniciar la sesión en IBM Security QRadar Log Manager. Proporciona un entorno de espacio de trabajo que ofrece información detallada y de resumen sobre los sucesos que se producen en la red.

Pestaña Actividad de registro

La pestaña **Actividad de registro** le permitirá investigar los registros de sucesos que se envían a QRadar en tiempo real, realizar búsquedas potentes y ver la actividad de registro utilizando gráficos de series temporales configurables.

La pestaña **Actividad de registro** le permitirá realizar investigaciones en profundidad sobre datos de suceso.

Para obtener más información, consulte Investigación de actividad de registro.

Pestaña Activos

QRadar descubre automáticamente los activos, servidores y hosts que operan en la red.

Los perfiles de activo proporcionan información sobre cada activo conocido de la red, incluyendo información de identidad, si está disponible, y sobre qué servicios se ejecutan en cada activo. Estos datos de perfil se utilizan para la correlación con el fin de ayudar a reducir falsos positivos.

Por ejemplo, un ataque intenta utilizar un servicio específico que se está ejecutando en un activo específico. En esta situación, QRadar puede determinar si el activo es vulnerable a este ataque correlacionando el ataque con el perfil de activo. Mediante la pestaña **Activos**, puede ver los activos aprendidos o buscar activos específicos para ver los perfiles.

Para obtener más información, consulte Gestión de activos.

Pestaña Informes

La pestaña **Informes** le permite crear, distribuir y gestionar informes para los datos en QRadar.

La característica Informes le permitirá crear informes personalizados para uso operativo y ejecutivo. Para crear un informe, puede combinar la información (por ejemplo seguridad o red) en un único informe. También puede utilizar plantillas de informe preinstaladas que se incluyen con QRadar.

La pestaña **Informes** también le permitirá marcar los informes con logotipos personalizados. Esta personalización es beneficiosa para distribuir informes a diferentes públicos.

Para obtener más información sobre informes, consulte Gestión de informes.

Pestaña IBM Security QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager es un componente de QRadar que puede adquirir por separado. Puede utilizar una clave de licencia para habilitar QRadar Vulnerability Manager.

QRadar Vulnerability Manager es una plataforma de exploración de red que proporcionan conciencia de las vulnerabilidades existentes en las aplicaciones, los sistemas o dispositivos de su red. Después de que las exploraciones identifiquen las vulnerabilidades, puede buscar y revisar datos de vulnerabilidad, remediar vulnerabilidades y volver a ejecutar exploraciones para evaluar el nuevo nivel de riesgo.

Cuando IBM Security QRadar Vulnerability Manager está habilitado, puede realizar tareas de evaluación de vulnerabilidades en la pestaña Vulnerabilidades. En la pestaña Activos, puede ejecutar exploraciones de IBM Security QRadar Vulnerability Manager sobre activos seleccionados.

Para obtener más información, consulte la Guía del usuario de *IBM Security IBM Security QRadar Vulnerability Manager*.

Pestaña Admin

Los administradores utilizan la pestaña Admin para configurar y gestionar los usuarios, sistemas, redes, plug-ins y componentes. Los usuarios con privilegios de administración pueden acceder a la pestaña **Admin**.

Las herramientas de administración a las que los administradores pueden acceder en la pestaña **Admin** se describe en la Tabla 1.

Tabla 4. Herramientas de gestión de administración disponibles en QRadar

Herramienta de administración	Descripción
Configuración del sistema	Configurar opciones de gestión de sistema y usuarios.
Orígenes de datos	Configurar orígenes de registro.
Configuración de redes remotas y servicios	Configurar redes remotas y grupos de servicios.
Plug-ins	Acceder a componentes de plug-in, por ejemplo el plug-in de IBM Security QRadar Risk Manager. Esta opción sólo se visualiza si hay plug-ins que están instalados en la consola.
Editor de despliegue	Gestionar los componentes individuales del despliegue de QRadar.

Todas las actualizaciones de configuración que realiza en la pestaña **Admin** se guardan en un área de transferencia. Cuando se hayan completado todos los cambios, puede desplegar las actualizaciones de configuración realizadas en el host gestionado en el despliegue.

Procedimientos comunes de QRadar

Varios controles de la interfaz de usuario de QRadar son comunes en la mayoría de las pestañas de interfaz de usuario.

En las secciones siguientes se describe la información sobre estos procedimientos comunes.

Visualización de mensajes

El menú **Mensajes**, que se encuentra en la esquina superior derecha de la interfaz de usuario, proporciona acceso a una ventana en la que puede leer y gestionar las notificaciones del sistema.

Antes de empezar

Para que las notificaciones del sistema se muestren en la ventana **Mensajes**, el administrador debe crear una regla que se base en cada tipo de mensaje de notificación y seleccionar el recuadro de selección **Notificar** en el **Asistente de reglas personalizadas**.

Acerca de esta tarea

El menú **Mensajes** indica cuántas notificaciones de sistema no leídas tiene en el sistema. Este indicador incrementa el número hasta que se cierran las notificaciones de sistema. Para cada notificación de sistema, la ventana **Mensajes** proporciona un resumen y la indicación de fecha y hora en que se ha creado la notificación de sistema. Puede pasar el puntero del ratón sobre una notificación para ver más detalles. Utilizando las funciones de la ventana **Mensajes**, puede gestionar las notificaciones del sistema.

Las notificaciones del sistema también están disponibles en la pestaña **Panel de control** y en una ventana emergente opcional que se puede visualizar en la esquina inferior izquierda de la interfaz de usuario. Las acciones que se realizan en la ventana **Mensajes** se propagan a la pestaña **Panel de control** y la ventana emergente. Por ejemplo, si cierra una notificación de sistema de la ventana **Mensajes**, la notificación de sistema se elimina de todas las pantallas de notificación de sistema.

Para obtener más información sobre las notificaciones de sistema del panel de control, consulte Elemento de notificaciones de sistema.

La ventana **Mensajes** proporciona las funciones siguientes:

Tabla 5. Funciones disponibles en la ventana Mensajes

Función	Descripción
Todos	Pulse **Todos** para ver todas las notificaciones del sistema. Esta opción es el valor predeterminado, por lo tanto, pulse **Todos** sólo si ha seleccionado otra opción y desea visualizar de nuevo todas las notificaciones del sistema.
Salud	Pulse **Salud** para ver solo las notificaciones de sistema que tienen un nivel de gravedad de Salud.
Errores	Pulse **Errores** para ver solo las notificaciones de sistema sólo que tienen un nivel de gravedad de Error.
Avisos	Pulse **Avisos** para ver sólo las notificaciones de sistema que tienen un nivel de gravedad de Aviso.

Tabla 5. Funciones disponibles en la ventana Mensajes (continuación)

Función	Descripción
Información	Pulse **Información** para ver sólo las notificaciones de sistema que tienen un nivel de gravedad de información.
Descartar todo	Pulse **Descartar todo** para cerrar en el sistema todas las notificaciones de sistema. Si ha filtrado la lista de notificaciones de sistema utilizando los iconos de **Salud**, **Errores**, **Avisos** o **Información**, el texto en el icono **Ver todos** cambia a una de las opciones siguientes: • **Descartar todos los errores** • **Descartar toda la salud** • **Descartar todos los avisos** • **Descartar todos los avisos** • **Descartar toda la información**
Ver todos	Pulse **Ver todos** para ver los sucesos de notificación de sistema en la pestaña **Actividad de registro**. Si ha filtrado la lista de notificaciones de sistema utilizando los iconos de **Salud**, **Errores**, **Avisos** o **Información**, el texto en el icono **Ver todos** cambia a una de las opciones siguientes: • **Ver todos los errores** • **Ver toda la salud** • **Ver todos los avisos** • **Ver toda la información**
Descartar	Pulse el icono **Descartar** junto a una notificación de sistema para cerrar en el sistema la notificación de sistema.

Procedimiento

1. Inicie la sesión en QRadar.
2. En la esquina superior derecha de la interfaz de usuario, pulse **Mensajes**.
3. En la ventana **Mensajes**, vea los detalles de la notificación de sistema.
4. Opcional. Para refinar la lista de notificaciones de sistema, pulse una de las opciones siguientes:
   - **Errores**
   - **Avisos**
   - **Información**
5. Opcional. Para cerrar las notificaciones de sistema, elija entre las opciones siguientes:

Opción	Descripción
Descartar todo	Pulse aquí para cerrar todas las notificaciones de sistema.
Descartar	Pulse el icono **Descartar** junto a la notificación de sistema que desea cerrar.

6. Opcional. Para ver los detalles de notificación de sistema, pase el puntero de ratón sobre la notificación de sistema.

Ordenación de resultados

Puede ordenar los resultados en tablas pulsando una cabecera de columna. Una flecha en la parte superior de la columna indica la dirección de la ordenación.

Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la cabecera de columna una vez para ordenar la tabla en orden descendente; pulse dos veces para ordenar la tabla en orden ascendente.

Renovación y pausa de la interfaz de usuario

Puede renovar, poner en pausa y reproducir manualmente los datos que se visualizan en las pestañas.

Acerca de esta tarea

La pestaña **Actividad de registro** se renueva automáticamente cada 60 segundos si está viendo la pestaña en modalidad de Último intervalo (renovación automática).

El temporizador, que se encuentra en la esquina superior derecha de la interfaz, indica la cantidad de tiempo hasta que la pestaña se renueve automáticamente.

Cuando vea la pestaña **Actividad de registro** en modalidad de Tiempo real (modalidad continua) o de Último minuto (renovación automática), puede utilizar el icono **Pausa** para poner en pausa la visualización actual.

También puede poner en pausa la visualización actual en la pestaña **Panel de control**. Al pulsar en cualquier lugar dentro de un elemento de panel de control, la pestaña se pone en pausa automáticamente. El temporizador parpadea en rojo para indicar que la visualización actual se ha puesto en pausa.

Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la pestaña que desea ver.
3. Elija una de las siguientes opciones:

Opción	Descripción
Renovar	Pulse **Renovar**, en la esquina derecha de la pestaña, para renovar la pestaña.
Pausa	Pulse aquí para poner en pausa la visualización de la pestaña.
Reproducir	Pulse aquí para reiniciar el temporizador después de que éste se haya puesto en pausa.

Investigación de direcciones IP

Puede utilizar varios métodos para investigar la información sobre direcciones IP en las pestañas Panel de control, Actividad de registro y Actividad de red.

Acerca de esta tarea

Puede encontrar más información acerca de una dirección IP mediante cualquiera de los métodos que se enumeran en la tabla siguiente.

Tabla 6. Información de direcciones IP

Opción	Descripción
Información > **Búsqueda de DNS**	Busca entradas DNS que están basados en la dirección IP.
Información > **Búsqueda de WHOIS**	Busca el propietario registrado de una dirección IP remota. El servidor WHOIS predeterminado es whois.arin.net.
Información > **Exploración de puertos**	Realiza una exploración de Network Mapper (NMAP) de la dirección IP seleccionada. Esta opción solo está disponible si NMAP está instalado en el sistema. Para obtener más información sobre la instalación de NMAP, consulte la documentación de proveedor.
Información > **Perfil de activo**	Visualiza información de perfil de activo. Esta opción se visualiza si se ha adquirido IBM Security QRadar Vulnerability Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*. Esta opción de menú está disponible si QRadar ha adquirido datos de perfil activamente mediante una exploración.
Información > **Sucesos de búsqueda**	Busca los sucesos que están asociados con esta dirección IP.
Información > **Buscar en conexiones**	Busca las conexiones que están asociadas con esta dirección IP. Esta opción solo se visualiza si ha adquirido IBM Security QRadar Risk Manager y ha conectado QRadar y el dispositivo de IBM Security QRadar Risk Manager. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
Información > **Switch Port Lookup**	
Información > **Ver topología**	Visualiza la pestaña , que representa la topología de capa 3 de la red. Esta opción está disponible si ha adquirido IBM Security QRadar Risk Manager y ha conectado QRadar y el dispositivo de IBM Security QRadar Risk Manager.

Tabla 6. Información de direcciones IP (continuación)

Opción	Descripción
Información > **Ejecutar exploración de QVM**	Seleccione la opción Ejecutar Exploración de QVM para realizar una exploración de IBM Security QRadar Vulnerability Manager en esta dirección IP. Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Para obtener información sobre la pestaña Riesgos o IBM Security QRadar Risk Manager, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.

Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la pestaña que desea ver.
3. Mueva el puntero de ratón sobre una dirección IP para ver la ubicación de la dirección IP.
4. Pulse el botón derecho del ratón en la dirección IP o el nombre de activo y seleccione una de las opciones siguientes:

Investigar nombres de usuario

Puede pulsar el botón derecho del ratón en un nombre de usuario para acceder a más opciones de menú. Use estas opciones para ver más información sobre el nombre de usuario o la dirección IP.

Puede investigar los nombres de usuario al comprar IBM Security QRadar Vulnerability Manager y obtener la licencia del mismo. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Al pulsar el botón derecho del ratón en un nombre de usuario, puede elegir las siguientes opciones de menú.

Tabla 7. Opciones de menú para investigación de nombre de usuario

Opción	Descripción
Ver activos	Visualiza los activos actuales que están asociados con el nombre de usuario seleccionado. Para obtener más información sobre cómo ver activos, consulte Gestión de activos.
Ver historial de usuario	Visualiza todos los activos que están asociados con el nombre de usuario seleccionado durante las 24 horas anteriores.
Ver sucesos	Visualiza los sucesos que están asociados con el nombre de usuario seleccionado. Para obtener más información sobre la ventana Lista de sucesos, consulte Supervisión de actividad de registro.

Para obtener más información sobre cómo personalizar el menú que aparece al pulsar el botón derecho del ratón, consulte la publicación *Guía de administración* correspondiente al producto.

Hora del sistema

En la esquina derecha de la interfaz de usuario de QRadar se visualiza la hora del sistema, que es la hora de la consola.

La hora de consola sincroniza los sistemas QRadar en el despliegue de QRadar. La hora de consola se utiliza para determinar qué sucesos de hora se han recibido de otros dispositivos para la correlación de sincronización de hora correcta.

En un despliegue distribuido, la consola puede estar en un huso horario diferente del correspondiente al del sistema.

Cuando se aplican filtros y búsquedas basados en la hora en la pestaña **Actividad de registro**, debe utilizar la hora de sistema de la consola para especificar un intervalo de tiempo.

Actualización de preferencias de usuario

Puede establecer las preferencias de usuario, por ejemplo entorno local, en la interfaz de usuario de QRadar principal.

Procedimiento

1. Para acceder a la información de usuario, pulse **Preferencias**.
2. Actualice las preferencias.

Opción	Descripción
Nombre de usuario	Visualiza el nombre de usuario. No puede editar este campo.
Contraseña	La contraseña debe cumplir los siguientes criterios: • Un mínimo de 6 caracteres • Un máximo de 255 caracteres • Contener al menos un carácter especial • Contener un carácter en mayúsculas
Contraseña (Confirmar)	Confirmación de contraseña,
Dirección de correo electrónico	La dirección de correo electrónico debe cumplir los requisitos siguientes: • Un mínimo de 10 caracteres • Un máximo de 255 caracteres
Entorno local	QRadar está disponible en los idiomas siguientes: inglés, chino simplificado, chino tradicional, japonés, coreano, francés, alemán, italiano, español, ruso y portugués (Brasil). Si un entorno local no aparece en la lista, la interfaz de usuario no está traducida al idioma asociado. Sin embargo, se soportan otros convenios culturales asociados, como tipo de carácter, clasificación, formato de fecha y hora, unidad de moneda.

Opción	Descripción
Habilitar notificaciones emergentes	Marque este recuadro de selección si desea permitir que se visualicen notificaciones de sistema emergentes en la interfaz de usuario.

Redimensionar columnas

Puede redimensionar las columnas en varias pestañas en QRadar.

Coloque el puntero del ratón por encima de la línea que separa las columnas y arrastre el borde de la columna a la nueva ubicación. También puede redimensionar las columnas efectuando una doble pulsación en la línea que separa las columnas para redimensionar automáticamente la columna a la anchura del campo más grande.

Nota: El redimensionamiento de columna no funciona en los navegadores web Microsoft Internet Explorer, Versión 7.0 cuando las pestañas visualizan registros en modalidad continua.

Tamaño de página

Los usuarios con privilegios administrativos pueden configurar el número máximo de resultados que se visualizan en las tablas de varios separadores de QRadar.

Capítulo 3. Gestión de panel de control

La pestaña **Panel de control** es la vista predeterminada cuando se inicia la sesión.

Proporciona un entorno de espacio de trabajo en el que puede visualizar las vistas de los datos que se recopilan.

Utilice la pestaña Panel de control para supervisar el comportamiento de sucesos de seguridad.

Puede personalizar el panel de control. El contenido que se visualiza en la pestaña **Panel de control** es específico del usuario. Los cambios que se realizan dentro de una sesión sólo afectan el sistema.

Para personalizar la pestaña **Panel de control**, puede realizar las tareas siguientes:

- Añadir y eliminar elementos de panel de control de los paneles de control.
- Mover y colocar elementos para satisfacer los requisitos. Cuando coloca elementos, cada elemento se redimensiona automáticamente en proporción al panel de control.
- Añada elementos de panel de control personalizados que se basen en datos cualesquiera.

  Por ejemplo, puede añadir un elemento del panel de control que proporcione un gráfico de serie temporal o un gráfico de barras que represente la actividad de las 10 principales redes.

  Para crear elementos personalizados, puede crear búsquedas guardadas en la pestaña **Actividad de registro** y elegir cómo desea los resultados que están representados en el panel de control. Cada gráfico de panel de control visualiza datos actualizados al minuto en tiempo real. Los gráficos de serie temporal del panel de control se renuevan cada 5 minutos.

Actividad de registro

Los elementos de panel de control**Actividad de registro** le permitirán supervisar e investigar sucesos en tiempo real.

Nota: Los sucesos ocultos o cerrados no están incluidos en los valores que se visualizan en la pestaña **Panel de control** .

Tabla 8. Elementos de actividad de registro

Elemento de panel de control	Descripción
Búsquedas de suceso	Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña Actividad de registro. Los elementos de búsqueda de sucesos se listan en el menú **Añadir elemento** > **Actividad de registro** > **Búsquedas de suceso**. El nombre del elemento de búsqueda de sucesos coincide con el nombre de los criterios de búsqueda guardados en los que se basa el elemento. QRadar incluye criterios de búsqueda guardados predeterminados que están preconfigurados para visualizar elementos de búsqueda de sucesos en el menú de pestaña **Panel de control**. Puede añadir más elemento de panel de control de búsqueda de sucesos en el menú de pestaña **Panel de control**. Para obtener más información, consulte Adición de elementos de panel de control basados en búsqueda a la lista de adición de elementos Añadir. En un elemento de panel de control **Actividad de registro**, los resultados de búsqueda visualizan datos de última hora en tiempo real en un gráfico. Los tipos de gráfico soportados son series de tiempo, tabla, circular y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar. Los gráficos de series temporales son interactivos. Puede ampliar y explorar en una línea temporal para investigar la actividad de registro.
Sucesos por gravedad	El elemento de panel de control **Sucesos por gravedad** visualiza el número de sucesos activos que están agrupados por gravedad. Este elemento le permitirá ver el número de sucesos que se reciben por el nivel de gravedad asignada. La gravedad indica la cantidad de amenaza que representa un origen de delito en relación al grado de preparación del destino ante el ataque. El rango de gravedad es de 0 (baja) a 10 (alta). Los tipos de gráfico soportados son tabla, circular y de barras.

Tabla 8. Elementos de actividad de registro (continuación)

Elemento de panel de control	Descripción
Orígenes de registro principales	El elemento de panel de control **Orígenes de registro principales** visualiza los 5 orígenes de registro principales que han enviado sucesos a QRadar Log Manager en los últimos 5 minutos. El número de sucesos que se envían desde el origen de registro especificado se indica en el gráfico circular. Este elemento le permitirá ver los cambios potenciales en el comportamiento, por ejemplo si un origen de registro de cortafuegos que normalmente no está en la lista de 10 principales ahora contribuye en un gran porcentaje del recuento de mensajes global, debe investigar esta aparición. Los tipos de gráfico soportados son tabla, circular y de barras.

Informes más recientes

El elemento de panel de control **Informes más recientes** visualiza los informes generados más recientemente.

La pantalla proporciona el título de informe, la hora y fecha en que se ha generado el informe y el formato del informe.

Resumen del sistema

El elemento de panel de control **Resumen del sistema** proporciona un resumen de alto nivel de la actividad dentro las últimas 24 horas.

Dentro del elemento de resumen, puede ver la información siguiente:

- **Sucesos actuales por segundo**: Visualiza la tasa de sucesos por segundo.
- **Sucesos nuevos (pasadas 24 horas)**: Visualiza el número total de sucesos nuevos que se reciben dentro de las últimas 24 horas.

Elementos de Gestión de vulnerabilidades

Los elementos de panel de control Gestión de vulnerabilidades solo se visualizan cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se ha obtenido la licencia.

Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña **Vulnerabilidades**. Los elementos de búsqueda se listan en el menú **Añadir elemento** > **Gestión de vulnerabilidades** > **Búsqueda de vulnerabilidades**. El nombre del elemento de búsqueda coincide con el nombre de los criterios de búsqueda guardada en los que se basa el elemento.

QRadar incluye criterios de búsqueda guardada predeterminados que se han preconfigurado para visualizar elementos de búsqueda en el menú de la **pestaña Panel de control**. Puede añadir más elementos de panel de control de búsqueda en el menú de la **pestaña Panel de control**.

Los tipos de gráfico soportados son tabla, circular y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar.

Notificación del sistema

El elemento de panel de control Notificación del sistema muestra notificaciones de sucesos recibidas por el sistema.

Para que las notificaciones se muestren en el panel de control **Notificación del sistema**, el administrador debe crear una regla que se base en cada tipo de mensaje de notificación y seleccione el recuadro de selección **Notificar** en el Asistente de reglas personalizadas.

Para obtener más información sobre cómo configurar notificaciones de sucesos y crear reglas de suceso, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.

En el elemento de panel de control **Notificaciones del sistema**, puede ver la información siguiente:

- **Distintivo**: Visualiza un símbolo para indicar el nivel de gravedad de la notificación. Apunte al símbolo para ver más detalle sobre el nivel de gravedad.
  - Icono **Salud**
  - Icono **Información** (?)
  - Icono **Error** (X)
  - Icono **Aviso** (!)
- **Creado**: Visualiza la cantidad de tiempo transcurrido desde que se ha creado la notificación.
- **Descripción**: Visualiza información acerca de la notificación.
- **Icono Descartar (x)**: Le permitirá cerrar una notificación del sistema.

Puede apuntar el ratón sobre una notificación para ver más detalles:

- **IP de host**: Visualiza la dirección IP del host que ha originado la notificación.
- **Gravedad**: Visualiza el nivel de gravedad de la incidencia que ha creado esta notificación.
- **Categoría de nivel bajo**: Visualiza la categoría de bajo nivel que está asociada con el incidente que ha generado esta notificación. Por ejemplo: Interrupción de servicio.
- **Carga útil**: Visualiza el contenido de carga útil que está asociado con el incidente que ha generado esta notificación.
- **Creado**: Visualiza la cantidad de tiempo transcurrido desde que se ha creado la notificación.

Cuando se añade el elemento de panel de control **Notificaciones del sistema**, las notificaciones del sistema también se pueden visualizar como notificaciones emergentes en la interfaz de usuario de QRadar. Estas notificaciones emergentes se visualizan en la esquina inferior derecha de la interfaz de usuario, independientemente de la pestaña seleccionada.

Las notificaciones emergentes sólo están disponibles para los usuarios con permisos administrativos y están habilitadas de forma predeterminada. Para inhabilitar las notificaciones emergentes, seleccione **Preferencias de usuario** y borre el recuadro de selección **Habilitar notificaciones emergentes**.

En la ventana emergente Notificaciones del sistema, se resalta el número de notificaciones de la cola. Por ejemplo, si se visualiza (1 – 12) en la cabecera, la notificación actual es de 1 de 12 de notificaciones a visualizar.

La ventana emergente Notificación del sistema proporciona las opciones siguientes:

- **Icono Siguiente (>)**: Visualiza el siguiente mensaje de notificación. Por ejemplo, si el mensaje de notificación actual es 3 de 6, pulse el icono para ver 4 de 6.
- **Icono Cerrar (X)** : Cierra esta ventana emergente de notificación.
- **(detalles)**: Visualiza más información acerca de esta notificación del sistema.

Adición de elementos de panel de control

Puede añadir varios elementos de panel de control a la pestaña Panel de control.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En la barra de herramientas, pulse **Añadir elemento**.
3. Seleccione el elemento que desee agregar. Consulte los elementos del panel de control Disponible.

Utilización del panel de control para investigar la actividad de registro

Los elementos de panel de control basados en búsqueda proporcionan un enlace a la pestaña **Actividad de registro** lo que permite seguir investigando la actividad de registro.

Acerca de esta tarea

Para investigar flujos de un elemento de panel de instrumentos **Actividad de registro**:

1. Pulse el enlace **Ver en actividad de registro**. Se visualiza la pestaña **Actividad de registro** que muestra los resultados y dos gráficos que emparejan los parámetros en el elemento de panel de control.

Los tipos de gráfico que se visualizan en la pestaña **Actividad de registro** dependen de qué gráfico está configurado en el elemento de panel de control:

Tipo de gráfico	Descripción
Barra, Circular y Tabla	La pestaña **Actividad de registro** visualiza un gráfico de barras, un gráfico circular y una tabla de detalles.

Tipo de gráfico	Descripción
Serie temporal	La pestaña **Actividad de registro** visualiza gráficos según los criterios siguientes: 1. Si el rango temporal es menor o igual que 1 hora, se visualizan un gráfico de serie temporal, un gráfico de barras y una tabla de detalles de suceso. 2. Si el rango temporal es mayor que 1 hora, se muestra un gráfico de serie temporal y se le solicita que pulse Actualizar detalles. Esta acción inicia la búsqueda que llena los detalles de suceso y genera el gráfico de barras. Una vez finalizada la búsqueda, se visualizan el gráfico de barras y la tabla de detalles de suceso.

Configuración de gráficos

Puede configurar los elementos de panel de control **Actividad de registro**, **Actividad de red** y **Conexiones** (si procede) para especificar el tipo de gráfico y cuántos objetos de datos desea ver.

Acerca de esta tarea

Tabla 9. Configuración de gráficos. Opciones de parámetro.

Opción	Descripción
Valor para gráfico	En el cuadro de lista, seleccione el tipo de objeto que desee representar en el gráfico. Las opciones incluyen todos los parámetros de suceso y de flujo normalizados y personalizados que se incluyen en los parámetros de búsqueda.
Tipo de gráfico	En el cuadro de lista, seleccione el tipo de gráfico que desee ver. Las opciones incluyen: 1. **Gráfico de barras**: muestra los datos en un gráfico de barras. Esta opción solo está disponible para sucesos agrupados. 2. **Gráfico circular**: muestra los datos en un gráfico circular. Esta opción solo está disponible para sucesos agrupados. 3. **Tabla**: Visualiza los datos en una tabla. Esta opción solo está disponible para sucesos agrupados. 4. **Serie temporal**: muestra un gráfico de líneas interactivo que representa los registros correspondientes a un intervalo de tiempo especificado.
Mostrar parte superior	En el cuadro de lista, seleccione el número de objetos que desea ver el gráfico. Las opciones son **5** y **10**. El valor predeterminado es **10**.

Tabla 9. Configuración de gráficos (continuación). Opciones de parámetro.

Opción	Descripción
Capturar datos de serie temporal	Seleccione esta casilla para habilitar la captura de series temporales. Cuando selecciona esta casilla, la función de representación gráfica comienza a acumular datos para gráficos de serie temporal. De forma predeterminada, esta opción está inhabilitada.
Rango de tiempo	En el cuadro de lista, seleccione el rango de tiempo que desee ver.

Las configuraciones para gráficos personalizados se conservan, por lo que se muestran como configurados cada vez que accede al panel **Panel de control**.

QRadar Log Manager recopila datos por lo que cuando realiza una búsqueda guardada de serie temporal, existe una memoria caché de datos de suceso o de flujo para mostrar los datos correspondientes al periodo de tiempo anterior. Los parámetros acumulados se indican mediante un asterisco (*) en el cuadro de lista **Valor para gráfico**. Si selecciona un valor para representar gráficamente que no está acumulado (sin asterisco), no habrá datos de serie temporal disponibles.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el cuadro de lista **Mostrar panel de control**, seleccione el panel de control donde reside el elemento que desee personalizar.
3. En la cabecera del elemento de panel de control que desee configurar, pulse el icono **Valores**.
4. Configure los parámetros de gráfico descritos en la Tabla 1.

Eliminación de elementos de panel de control

Puede eliminar elementos de un panel de control y añadir el elemento de nuevo en cualquier momento.

Acerca de esta tarea

Cuando se elimina un elemento del panel de control, el elemento no se elimina por completo.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control del que desea eliminar un elemento.
3. En la cabecera de elemento de panel de control, pulse el icono rojo [x] para eliminar el elemento del panel de control.

Desconexión de un elemento del panel de control

Puede desconectar un elemento del panel de control y visualizar el elemento en una ventana nueva en el sistema.

Acerca de esta tarea

Al desconectar un elemento de panel de control, el elemento de panel de control original permanece en la pestaña **Panel de control**, mientras que una ventana desconectada con un elemento del panel de control duplicado permanece abierta y se renueva durante intervalos planificados. Si cierra la aplicación de QRadar, la ventana desconectada permanecerá abierta para supervisión y continúa renovándose hasta que se cierra manualmente la ventana o se cierra el sistema.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control del que desea desconectar un elemento.
3. En la cabecera de elemento de panel de control, pulse el icono verde para desconectar el elemento de panel de control y abrirlo en una ventana independiente.

Renombrar un panel de control

Puede renombrar un panel de control y actualizar la descripción.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control que desea editar.
3. En la barra de herramientas, pulse el icono **Renombrar panel de control** .
4. En el campo **Nombre**, escriba un nuevo nombre para el panel de control. La longitud máxima es de 65 caracteres.
5. En el campo **Descripción**, escriba una nueva descripción del panel de control. La longitud máxima es de 255 caracteres
6. Pulse **Aceptar**.

Supresión de un panel de control

Puede suprimir un panel de control.

Acerca de esta tarea

Después de suprimir un panel de control, la pestaña **Panel de control** se renueva y se visualiza el primer panel de control que se lista en el recuadro de lista **Mostrar panel de control**. El panel de control que ha suprimido ya no se visualiza en el recuadro de lista **Mostrar panel de control**.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control que desea suprimir.
3. En la barra de herramientas, pulse **Suprimir panel de control**.
4. Pulse **Sí**.

Gestión de notificaciones del sistema

Puede especificar el número de notificaciones que desea visualizar en el elemento de panel de control **Notificación del sistema** y cerrar las notificaciones del sistema después de leerlas.

Antes de empezar

Asegúrese de que el elemento de panel de control **Notificación del sistema** se añade al panel de control.

Procedimiento

1. En la cabecera de elemento de panel de control Notificación del sistema, pulse el icono **Valores**.
2. En el recuadro de lista **Visualizar**, seleccione el número de notificaciones de sistema que desea ver.
   - Las opciones son **5**, **10** (valor predeterminado), **20**, **50** y **Todos**.
   - Para ver todas las notificaciones del sistema que se han registrado en las últimas 24 horas, pulse **Todos**.
3. Para cerrar una notificación del sistema, pulse el icono **Suprimir**.

Adición de elementos de panel de control basados en búsqueda a la lista de adición de elementos

Puede añadir elementos de panel de control basados en búsqueda al menú **Añadir elementos**.

Antes de empezar

Para añadir un elemento de panel de control de sucesos al menú **Añadir elemento** en la pestaña **Panel de control**, debe acceder a la pestaña **Actividad de registro** para crear criterios de búsqueda que especifiquen que los resultados de búsqueda se pueden visualizar en la pestaña **Panel de control**. Los criterios de búsqueda también deben especificar que los resultados se agrupen en un parámetro.

Procedimiento

1. Elija:
   - Para añadir un elemento de panel de control de búsqueda de sucesos, pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, elija una de las opciones siguientes:
   - Para crear una búsqueda, seleccione **Nueva búsqueda**.
   - Para editar una búsqueda guardada, seleccione **Editar búsqueda**.
3. Configure o edite los parámetros de búsqueda, según sea necesario.
   - En el panel Editar búsqueda, seleccione la opción **Incluir en Panel de control**.
   - En el panel Definición de columna, seleccione una columna y pulse el icono **Añadir columna** para mover la columna a la lista **Agrupar por**.
4. Pulse **Filtro**. Se visualizan los resultados de búsqueda.
5. Pulse **Guardar criterios**. Consulte Guardar criterios de búsqueda en la pestaña Delito.
6. Pulse **Aceptar**.

7. Verifique que los criterios de búsqueda guardados han añadido satisfactoriamente el elemento de panel de control de búsqueda de sucesos o flujos a la lista de **Añadir elementos**
8. Pulse la pestaña **Panel de control**.
9. Para verificar un elemento de búsqueda de sucesos, seleccione **Añadir elemento** > **Actividad de registro** > **Búsquedas de suceso** > **Añadir elemento**

Capítulo 4. Investigación de la actividad de registro

Puede supervisar e investigar sucesos en tiempo real o realizar búsquedas avanzadas.

Utilizando la pestaña **Actividad de registro**, puede supervisar e investigar la actividad de registro (sucesos) en tiempo real o realizar búsquedas avanzadas.

Visión general de la pestaña Actividad de registro

Un suceso es un registro de un origen de registro, como un cortafuegos o dispositivo de direccionador, que describe una acción en una red o un host.

Debe tener permiso para ver la pestaña **Actividad de registro**.

Barra de herramientas de pestaña Actividad de registro

Puede acceder a varias opciones desde la barra de herramientas Actividad de registro

Mediante la barra de herramientas, puede acceder a las siguientes opciones:

Tabla 10. Opciones de barra de herramientas Actividad de registro

Opción	Descripción
Buscar	Pulse **Buscar** para realizar búsquedas avanzadas en sucesos. Las opciones incluyen: • **Nueva búsqueda**: Seleccione esta opción para crear una nueva búsqueda de sucesos. • **Editar búsqueda**: Seleccione esta opción para seleccionar y editar una búsqueda de sucesos. • **Gestionar resultados de búsqueda**: Seleccione esta opción para ver y gestionar los resultados de búsqueda.
Búsquedas rápidas	En este cuadro de lista, puede guardar búsquedas guardadas anteriormente. Las opciones se muestran en el recuadro de lista**Búsquedas rápidas** sólo cuando ha guardado los criterios de búsqueda que especifican la opción **Incluir en Búsquedas rápidas**.
Añadir filtro	Pulse **Añadir filtro** para añadir un filtro a los resultados de búsqueda actuales.
Guardar criterios	Pulse **Guardar criterios** para guardar los criterios de búsqueda actuales.
Guardar resultados	Pulse **Guardar criterios** para guardar los resultados de búsqueda actuales. Esta opción sólo se visualiza después de que se haya completado una búsqueda. Esta opción está inhabilitada en modalidad continua.

Tabla 10. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Cancelar	Pulse **Cancelar** para cancelar una búsqueda en curso. Esta opción está inhabilitada en modalidad continua.
Reglas	La opción Reglas sólo es visible si tiene permiso para ver reglas. Pulse **Reglas** para configurar reglas de suceso personalizadas. Las opciones incluyen: • **Reglas**: Seleccione esta opción para ver o crear una regla. Si solo tiene permiso para ver reglas, se visualiza la página de resumen del asistente de reglas. Si tiene permiso para mantener reglas personalizadas, se visualiza el asistente de reglas y puede editar la regla. Para habilitar las opciones de regla de detección de anomalías (Añadir regla de umbral, Añadir regla conductual y Añadir regla de anomalía), debe guardar los criterios de búsqueda agregados porque los criterios de búsqueda guardados especifican los parámetros necesarios. **Nota:** Las opciones de regla de detección de anomalías sólo están visibles si tiene el permiso **Actividad de registro** > **Mantener reglas personalizadas** . • **Añadir regla de umbral**: Seleccione esta opción para crear una regla de umbral. Una regla de umbral prueba en el tráfico de sucesos la actividad que supera un umbral configurado. Los umbrales pueden basarse en los datos que QRadar recopila. Por ejemplo, si crea una regla de umbral que indica que no pueden iniciar la sesión en el servidor más de 220 clientes entre las 08:00 y las 17:00, las reglas generan una alerta cuando el cliente número 221 intenta iniciar la sesión. Cuando se selecciona la opción **Añadir regla de umbral**, el asistente de reglas se visualiza, lleno con las opciones adecuadas para crear una regla de umbral.

Tabla 10. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Reglas (continuación)	• **Añadir regla conductual**: Seleccione esta opción para crear una regla conductual. Una regla conductual prueba en el tráfico de sucesos la actividad anormal como, por ejemplo, la existencia de tráfico nuevo o desconocido, que es tráfico que cesa de repente o un cambio de porcentaje en la cantidad de tiempo que un objeto está activo. Por ejemplo, puede crear una regla conductual para comparar el promedio de volumen de tráfico durante los últimos 5 minutos con el promedio de volumen de tráfico durante la última hora. Si el cambio es superior al 40%, la regla genera una respuesta. Cuando se selecciona la opción **Añadir regla conductual**, el asistente de reglas se visualiza, llenado previamente con las opciones adecuadas para crear una regla conductual. • **Añadir regla de anomalía**: Seleccione esta opción para crear una regla de anomalía. Una regla de anomalía prueba en el tráfico de sucesos la actividad anormal como, por ejemplo, la existencia de tráfico nuevo o desconocido, que es tráfico que cesa de repente o un cambio de porcentaje en la cantidad de tiempo que un objeto está activo. Por ejemplo, si un área de la red que nunca se comunica con Asia empieza a comunicarse con hosts de ese país, una regla de anomalía genera una alerta. Cuando se selecciona la opción **Añadir regla de anomalía**, el asistente de reglas se visualiza, llenado previamente con las opciones adecuadas para crear una regla de anomalía.

Tabla 10. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Acciones	Pulse **Acciones** para realizar las acciones siguientes: • **Mostrar todo**: Seleccione esta opción para eliminar todos los filtros en los criterios de búsqueda y visualizar todos los sucesos no filtrados. • **Imprimir**: Seleccione esta opción para imprimir los sucesos que se visualizan en la página. • **Exportar a XML** > **Columnas visibles**: Seleccione esta opción para exportar sólo las columnas que son visibles en la pestaña Actividad de registro. Esta es la opción recomendada. Vea Exportación de sucesos. • **Exportar a XML** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse. Vea Exportación de sucesos. • **Exportar a CSV** >**Columnas visibles**: Seleccione esta opción para exportar solo las columnas que están visibles en la pestaña Actividad de registro. Esta es la opción recomendada. Vea Exportación de sucesos. • **Exportar a CSV** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse. Vea Exportación de sucesos. • **Suprimir**: Seleccione esta opción para suprimir un resultado de búsqueda. Consulte Gestión de resultados de búsqueda de sucesos y flujos. • **Notificar**: Seleccione esta opción para especificar que desea que se le envíe una notificación por correo electrónico cuando terminen las búsquedas seleccionadas. Esta opción solo está habilitada para las búsquedas en curso. **Nota:** Las opciones **Imprimir**, **Exportar a XML** y **Exportar a CSV** están inhabilitadas en modalidad continua y cuando se ven resultados de búsqueda parciales.

Tabla 10. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Barra de herramientas Buscar	**Búsqueda avanzada** Seleccione **Búsqueda avanzada** en el recuadro de lista para entrar una serie de búsqueda AQL (Ariel Query Language) para especificar los campos que desea que se devuelvan. **Filtro rápido** Seleccione Filtro rápido en el recuadro de lista para buscar cargas útiles utilizando palabras o frases simples.

Opciones del menú que aparece al pulsar el botón derecho del ratón

En la pestaña **Actividad de registro**, puede pulsar el botón derecho del ratón en un suceso para acceder a más información de filtro de sucesos.

Las opciones del menú que aparece al pulsar el botón derecho del ratón son las siguientes:

Tabla 11. Opciones del menú que aparece al pulsar el botón derecho del ratón

Opción	Descripción
Filtro en	Seleccione esta opción para filtrar en el suceso seleccionado, en función del parámetro seleccionado del suceso.
Más opciones:	Seleccione esta opción para investigar una dirección IP o un nombre de usuario. Para obtener más información sobre la investigación una dirección IP, consulte Investigación de direcciones IP. Para obtener más información sobre la investigación de un nombre de usuario, consulte Investigación de nombres de usuario. **Nota:** Esta opción no se visualiza en modalidad continua.

Barra de estado

Al transmitir sucesos, la barra de estado visualiza el número promedio de resultados que se reciben por segundo.

Este es el número de resultados que la consola ha recibido satisfactoriamente de los procesadores de sucesos. Si este número supera los 40 resultados por segundo, sólo se visualizarán 40 resultados. El resto se acumula en el almacenamiento intermedio de resultados. Para ver más información de estado, mueva el puntero del ratón sobre la barra de estado.

Cuando no se transmiten sucesos, la barra de estado muestra el número de resultados de búsqueda que se visualizan actualmente en la pestaña y la cantidad de tiempo que se necesita para procesar los resultados de búsqueda.

Supervisión de actividad de registro

De forma predeterminada, la pestaña **Actividad de registro** visualiza sucesos en modalidad continua, lo que le permite ver los sucesos en tiempo real.

Para obtener más información sobre la modalidad continua, consulte Visualización de sucesos de modalidad continua. Puede especificar un rango de tiempo distinto para filtrar sucesos mediante el recuadro de lista **Ver**.

Si anteriormente ha configurado criterios de búsqueda guardados como el valor predeterminado, los resultados de dicha búsqueda se visualizan automáticamente cuando se accede a la pestaña **Actividad de registro**. Para obtener más información acerca de cómo guardar criterios de búsqueda, consulte Guardar criterios de búsqueda de sucesos y flujos.

Visualización de sucesos en modalidad continua

La modalidad continua le permitirá ver los datos de sucesos que entran en el sistema. Esta modalidad le proporciona una vista en tiempo real de la actividad actual de sucesos visualizando los últimos 50 sucesos.

Acerca de esta tarea

Si se aplican filtros en la pestaña **Actividad de registro** o en los criterios de búsqueda antes de habilitar la modalidad continua, los filtros se mantienen en modalidad continua. Sin embargo, la modalidad continua no soporta búsquedas que incluyan sucesos agrupados. Si habilita la modalidad continua en sucesos agrupados o criterios de búsqueda agrupados, la pestaña **Actividad de registro** visualiza los sucesos normalizados. Consulte Visualización de sucesos normalizados.

Cuando desea seleccionar un suceso para ver detalles o realizar una acción, debe poner en pausa la modalidad continua antes de efectuar una doble pulsación en un suceso. Cuando la modalidad continua está en pausa, se visualizan los últimos 1.000 sucesos.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Ver**, seleccione **Tiempo real (modalidad continua)**. Para obtener información sobre las opciones de la barra de herramientas, consulte la Tabla 4-1. Para obtener más información sobre los parámetros que se visualizan en modalidad continua, consulte la Tabla 4-7.
3. Opcional. Poner en pausa o reproducir los sucesos en modalidad continua. Elija una de las siguientes opciones:
   - Para seleccionar un registro de sucesos, pulse el icono de **Pausa** para poner en pausa la modalidad continua.
   - Para reiniciar la modalidad continua, pulse el icono de **Reproducir**.

Visualización de sucesos normalizados

Los sucesos se recopilan en formato en bruto y, a continuación, se normalizan para visualizarse en la pestaña **Actividad de registro**.

Acerca de esta tarea

La normalización implica analizar los datos de sucesos en bruto y preparar los datos para visualizar información legible sobre la pestaña. Cuando los sucesos se normalizan, el sistema también normaliza los nombres. Por lo tanto, el nombre que se muestra en la pestaña **Actividad de registro** puede no coincidir con el nombre que se visualiza en el suceso.

Nota: Si ha seleccionado que se visualice un intervalo de tiempo, se visualiza un gráfico de serie temporal. Para obtener más información sobre la utilización de gráficos de serie temporal, consulte Visión general de gráfico de serie temporal.

La pestaña **Actividad de registro** muestra los parámetros siguientes cuando se visualizan sucesos normalizados:

Tabla 12. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado)

Parámetro	Descripción
Filtros actuales	En la parte superior de la tabla se muestran los detalles de los filtros que se aplican a los resultados de búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**. **Nota:** Este parámetro sólo se visualiza después de aplicar un filtro.
Ver	En este recuadro de lista, puede seleccionar el rango de tiempo por el que desea filtrar.

Tabla 12. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado) (continuación)

Parámetro	Descripción
Estadísticas actuales	Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto a **Estadísticas actuales** para visualizar u ocultar las estadísticas • **Resultados totales**: Especifica el número total de resultados que coincidían con los criterios de búsqueda. • **Archivos de datos buscados**: Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado. • **Duración**: Especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para solucionar los problemas de sucesos, es posible que se le solicite que proporcione información estadística actual.
Gráficos	Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse **Ocultar gráficos** si desea eliminar los gráficos de la pantalla. Los gráficos sólo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar. Para obtener más información sobre cómo configurar gráficos, consulte Gestión de gráficos. **Nota:** Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.

Tabla 12. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado) (continuación)

Parámetro	Descripción
Icono de delitos	Pulse este icono para ver detalles del delito que está asociado con este suceso. Para obtener más información, consulte Gestión de gráficos. **Nota:** Dependiendo del producto, es posible que este icono no esté disponible. Debe tener IBM Security QRadar SIEM.
Hora de inicio	Especifica la hora del primer suceso, tal como lo ha indicado el origen de registro a QRadar.
Nombre de suceso	Especifica el nombre normalizado del suceso.
Origen de registro	Especifica el origen de registro que ha originado el suceso. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Recuento de sucesos	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se detectan muchos sucesos del mismo tipo para la misma dirección IP de origen y dirección en un breve periodo de tiempo.
Hora	Especifica la fecha y hora en que QRadar ha recibido el suceso.
Categoría de nivel bajo	Especifica la categoría de bajo nivel que está asociada con este suceso. Para obtener más información sobre categorías de suceso, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.
IP de origen	Especifica la dirección IP de origen del suceso.
Puerto de origen	Especifica el puerto de origen del suceso.
IP de destino	Especifica la dirección IP de destino del suceso.
Puerto de destino	Especifica el puerto de destino del suceso.
Nombre de usuario	Especifica el nombre de usuario que está asociado con este suceso. Normalmente los nombres de usuario están disponibles en sucesos relacionados con la autenticación. Para todos los demás tipos de sucesos donde el nombre de usuario no está disponible, este campo especifica N/A.

Tabla 12. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado) (continuación)

Parámetro	Descripción
Magnitud	Especifica la magnitud de este suceso. Las variables incluyen credibilidad, pertinencia y gravedad. Apunte el ratón sobre la barra de magnitud para visualizar los valores y la magnitud calculada.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Visualizar**, seleccione **Valor predeterminado (normalizado)**.
3. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
4. Pulse el icono **Pausa** para poner en pausa la modalidad continua.
5. Efectúe una doble pulsación en el suceso que desea con más detalle. Para obtener más información, consulte Detalles de suceso.

Visualización de sucesos en bruto

Puede ver los datos de sucesos en bruto, que son los datos de sucesos sin analizar desde el origen de registro.

Acerca de esta tarea

Al ver datos de sucesos en bruto, la pestaña **Actividad de registro** proporciona los parámetros siguientes para cada suceso.

Tabla 13. Parámetros de sucesos en bruto

Parámetro	Descripción
Filtros actuales	En la parte superior de la tabla se muestran los detalles de los filtros que se aplican a los resultados de búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**. **Nota:** Este parámetro sólo se visualiza después de aplicar un filtro.
Ver	En este recuadro de lista, puede seleccionar el rango de tiempo por el que desea filtrar.

Tabla 13. Parámetros de sucesos en bruto (continuación)

Parámetro	Descripción
Estadísticas actuales	Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto a **Estadísticas actuales** para visualizar u ocultar las estadísticas • **Resultados totales**: Especifica el número total de resultados que coincidían con los criterios de búsqueda. • **Archivos de datos buscados**: Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado. • **Duración**: Especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para solucionar los problemas de sucesos, es posible que se le solicite que proporcione información estadística actual.
Gráficos	Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse **Ocultar gráficos** si desea eliminar los gráficos de la pantalla. Los gráficos sólo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar. **Nota:** Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.
Hora de inicio	Especifica la hora del primer suceso, tal como lo ha indicado el origen de registro a QRadar.

Tabla 13. Parámetros de sucesos en bruto (continuación)

Parámetro	Descripción
Origen de registro	Especifica el origen de registro que ha originado el suceso. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Carga útil	Especifica la información de carga útil de suceso original en formato UTF-8.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Visualizar**, seleccione **Sucesos en bruto**.
3. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
4. Efectúe una doble pulsación en el suceso que desea con más detalle. Consulte Detalles del suceso.

Visualización de sucesos agrupados

Utilizando la pestaña **Actividad de registro**, puede ver sucesos que están agrupados por diversas opciones. En el recuadro de lista **Visualizar**, puede seleccionar el parámetro por el que desea agrupar los sucesos.

Acerca de esta tarea

El recuadro de lista Visualizar no aparece en modalidad continua porque la modalidad continua no soporta los sucesos agrupados. Si ha entrado en modalidad continua utilizando criterios de búsqueda no agrupados, se visualiza esta opción.

El recuadro de lista Visualizar proporciona las opciones siguientes:

Tabla 14. Opciones de sucesos agrupados

Opción de grupo	Descripción
Categoría de nivel bajo	Muestra una lista resumida de sucesos que están agrupados por la categoría de bajo nivel del suceso.
Nombre de suceso	Muestra una lista resumida de sucesos que están agrupados por el nombre normalizado del suceso.
IP de destino	Muestra una lista resumida de sucesos que están agrupados por la dirección IP de destino del suceso.
Puerto de destino	Muestra una lista resumida de sucesos que están agrupados por la dirección de puerto de destino del suceso.
IP de origen	Muestra una lista resumida de sucesos que están agrupados por la dirección IP de origen del suceso.
Regla personalizada	Muestra una lista resumida de sucesos que están agrupados por la regla personalizada asociada.

Tabla 14. Opciones de sucesos agrupados (continuación)

Opción de grupo	Descripción
Nombre de usuario	Muestra una lista resumida de sucesos que están agrupados por el nombre de usuario que está asociado con los sucesos.
Origen de registro	Muestra una lista resumida de sucesos que están agrupados por los orígenes de registro que han enviado el suceso a QRadar.
Categoría de nivel alto	Muestra una lista resumida de sucesos que están agrupados por la categoría de nivel alto del suceso.
Red	Muestra una lista resumida de sucesos que están agrupados por la red que está asociada con el suceso.
Puerto de origen	Muestra una lista resumida de sucesos que están agrupados por la dirección de puerto de origen del suceso.

Después de seleccionar una opción en el cuadro de lista **Visualizar**, la disposición de las columnas de datos depende de la opción de agrupación elegida. Cada fila de la tabla de sucesos representa un grupo de sucesos. La pestaña **Actividad de registro** proporciona la siguiente información para cada grupo de sucesos

Tabla 15. Parámetros de sucesos agrupados

Parámetro	Descripción
Agrupando por	Especifica el parámetro para el que se agrupa la búsqueda.
Filtros actuales	En la parte superior de la tabla se muestran los detalles del filtro que se aplica a los resultados de búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**.
Ver	En el cuadro de lista, seleccione el rango de tiempo para el que desee aplicar el filtro.

Tabla 15. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Estadísticas actuales	Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto a **Estadísticas actuales** para mostrar u ocultar las estadísticas. • **Resultados totales**: Especifica el número total de resultados que coincidían con los criterios de búsqueda. • **Archivos de datos buscados**: Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado. • **Duración**: Especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para resolver problemas de los sucesos, es posible que se le solicite que proporcione información estadística actual.

Tabla 15. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Gráficos	Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse **Ocultar gráficos** si desea eliminar el gráfico de la pantalla. Cada gráfico proporciona una leyenda, que es una referencia visual para ayudarle a asociar los objetos de gráfico con los parámetros que representan. Mediante la característica de leyenda, puede realizar las acciones siguientes: • Mueva el puntero del ratón sobre un elemento de leyenda para ver más información sobre los parámetros que representa. • Pulse el botón derecho del ratón en el elemento de leyenda para investigar el elemento adicionalmente. • Pulse en un elemento de leyenda para ocultar el elemento en el gráfico. Pulse el elemento de leyenda de nuevo para mostrar el elemento oculto. También puede pulsar el elemento de gráfico correspondiente para ocultar y mostrar el elemento. • Pulse **Leyenda** si desea eliminar la leyenda de la pantalla gráfica. **Nota:** Los gráficos sólo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar. **Nota:** Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.
IP de origen (Recuento exclusivo)	Especifica la dirección IP de origen que está asociada con este suceso. Si hay varias direcciones IP que están asociados con este suceso, este campo especifica el término Múltiple y el número de direcciones IP.
IP de destino (Recuento exclusivo)	Especifica la dirección IP de destino que está asociada con este suceso. Si hay varias direcciones IP que están asociados con este suceso, este campo especifica el término Múltiple y el número de direcciones IP.

Tabla 15. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Puerto de destino (Recuento exclusivo)	Especifica los puertos de destino que están asociados con este suceso. Si hay varios puertos que están asociados con este suceso, este campo especifica el término Múltiple y el número de puertos.
Nombre de suceso	Especifica el nombre normalizado del suceso.
Origen de registro (Recuento exclusivo)	Especifica los orígenes de registro que han enviado el suceso a QRadar. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Categoría de nivel alto (Recuento exclusivo)	Especifica la categoría de alto nivel de este suceso. Si hay varias categorías que están asociadas con este suceso, este campo especifica el término Múltiple y el número de categorías. Para obtener más información sobre las categorías, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.
Categoría de nivel bajo (Recuento exclusivo)	Especifica la categoría de bajo nivel de este suceso. Si hay varias categorías que están asociadas con este suceso, este campo especifica el término Múltiple y el número de categorías.
Protocolo (Recuento exclusivo)	Especifica el ID de protocolo asociado con este suceso. Si hay varios protocolos que están asociados con este suceso, este campo especifica el término Múltiple y el número de ID de protocolo.
Nombre de usuario (Recuento exclusivo)	Especifica el nombre de usuario que está asociado con este suceso, si está disponible. Si hay varios nombres de usuario que están asociados con este suceso, este campo especifica el término Múltiple y el número de nombres de usuario.
Magnitud (máxima)	Especifica la magnitud máxima calculada para sucesos agrupados. Las variables que se utilizan para calcular la magnitud incluyen la credibilidad, la pertinencia y la gravedad. Para obtener más información sobre la credibilidad, el pertinencia y la gravedad, consulte el Glosario.
Recuento de sucesos (Suma)	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se ven muchos sucesos del mismo tipo para la misma dirección IP de origen y destino en un corto periodo de tiempo.
Recuento	Especifica el número total de sucesos normalizados en este grupo de sucesos.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
3. En el recuadro de lista Visualizar, elija el parámetro por el que desea agrupar los sucesos. Consulte la Tabla 2.Se listan los grupos de sucesos. Para obtener más información sobre los detalles de grupo de sucesos, consulte la Tabla 1.
4. Para ver la página Lista de sucesos para un grupo, efectúe una doble pulsación en el grupo de sucesos que desea investigar. La página Lista de sucesos no conserva las configuraciones de gráfico que pueda haber definido en la pestaña **Actividad de registro**. Para obtener más información sobre los parámetros de página Lista de sucesos, consulte la Tabla 1.
5. Para ver los detalles de un suceso, efectúe una doble pulsación en el suceso que desea investigar. Para obtener más información sobre los detalles de suceso, consulte la Tabla 2.

Detalles de suceso

Puede ver una lista de sucesos en varias modalidades, incluida la modalidad continua o en grupos de sucesos. Sea cual sea la modalidad que elija para ver sucesos, puede localizar y ver los detalles de un único suceso.

La página de detalles de suceso proporciona la siguiente información:

Tabla 16. Detalles de suceso

Parámetro	Descripción
Nombre de suceso	Especifica el nombre normalizado del suceso.
Categoría de nivel bajo	Especifica la categoría de bajo nivel de este suceso.
Descripción del suceso	Especifica una descripción del suceso, si está disponible.
Magnitud	Especifica la magnitud de este suceso. Para obtener más información sobre la magnitud, consulte el Glosario
Pertinencia	Especifica la pertinencia de este suceso. Para obtener más información sobre la pertinencia, consulte el Glosario.
Gravedad	Especifica la gravedad de este suceso. Para obtener más información sobre la gravedad, consulte el Glosario.
Credibilidad	Especifica la credibilidad de este suceso. Para obtener más información sobre credibilidad, consulte el Glosario.
Nombre de usuario	Especifica el nombre de usuario que está asociado con este suceso, si está disponible.
Hora de inicio	Especifica la hora en que se ha recibido el suceso del origen de registro.
Hora de almacenamiento	Especifica el tiempo que el suceso ha estado almacenado en la base de datos de QRadar.
Hora de origen de registro	Especifica la hora de sistema indicada por el origen de registro en la carga útil de suceso.

Tabla 16. Detalles de suceso (continuación)

Parámetro	Descripción
Información de origen y destino	
IP de origen	Especifica la dirección IP de origen del suceso.
IP de destino	Especifica la dirección IP de destino del suceso.
Nombre de activo de origen	Especifica el nombre de activo definido por el usuario del origen de suceso. Para obtener más información sobre activos, consulte Gestión de activos.
Nombre de activo de destino	Especifica el nombre de activo definido por el usuario del destino de suceso. Para obtener más información sobre activos, consulte Gestión de activos
Puerto de origen	Especifica el puerto de origen de este suceso.
Puerto de destino	Especifica el puerto de destino de este suceso.
IP de origen NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT (Network Address Translation - Conversión de direcciones de red), este parámetro especifica la dirección IP de origen antes de que se aplicaran los valores de NAT. NAT convierte una dirección IP de una red en una dirección IP diferente de otra red.
IP de destino NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de destino antes de que se aplicaran los valores de NAT.
Puerto de origen NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen antes de que se aplicaran los valores de NAT.
Puerto de destino NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino antes de que se aplicaran los valores de NAT.
IP de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de origen después de que se aplicaran los valores de NAT.
IP de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de destino después de que se aplicaran los valores de NAT.

Tabla 16. Detalles de suceso (continuación)

Parámetro	Descripción
Puerto de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen después de que se aplicaran los valores de NAT.
Puerto de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino después de que se aplicaran los valores de NAT.
Puerto de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen después de que se aplicaran los valores de NAT.
Puerto de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino después de que se aplicaran los valores de NAT.
Origen IPv6	Especifica la dirección IPv6 de origen del suceso.
Destino IPv6	Especifica la dirección IPv6 de destino del suceso.
MAC de origen	Especifica la dirección MAC de origen del suceso.
MAC de destino	Especifica la dirección MAC de destino del suceso.
Información de carga útil	
Carga útil	Especifica el contenido de carga útil del suceso. Este campo ofrece 3 pestañas para ver la carga útil: • Universal Transformation Format (UTF): Pulse UTF. • Hexadecimal: Pulse HEX. • Base64: Pulse Base64.
Información adicional	
Protocolo	Especifica el protocolo que está asociado con este suceso.
QID	Especifica el QID para este suceso. Cada suceso tiene un QID exclusivo. Para obtener más información sobre la correlación de un QID, consulte Modificación de correlación de sucesos.
Origen de registro	Especifica el origen de registro que ha enviado el suceso a QRadar. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.

Tabla 16. Detalles de suceso (continuación)

Parámetro	Descripción
Recuento de sucesos	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se ven muchos sucesos del mismo tipo para la misma dirección IP de origen y destino en un corto periodo de tiempo.
Reglas personalizadas	Especifica las reglas personalizadas que coinciden con este suceso. .
Reglas personalizadas coinciden parcialmente	Especifica reglas personalizadas que coinciden parcialmente con este suceso.
Anotaciones	Especifica el anotación para este suceso. Las anotaciones son descripciones de texto que las reglas pueden añadir automáticamente a los sucesos como parte de la respuesta de regla.
Información de identidad: QRadar recopila información de identidad, si está disponible, de los mensajes de origen de registro. La información de identidad proporciona detalles adicionales acerca de los activos en la red. Los orígenes de registro sólo generan información de identidad si el mensaje de registro enviado a QRadar contiene una dirección IP y al menos uno de los elementos siguientes: Nombre de usuario o Dirección MAC. No todos los orígenes de registro generan información de identidad. Para obtener más información sobre la identidad y los activos, consulte Gestión de activos.	
Nombre de usuario de identidad	Especifica el nombre de usuario del activo que está asociado con este suceso.
IP de identidad	Especifica la dirección IP del activo que está asociado con este suceso.
Nombre de NetBios de identidad	Especifica el nombre del Sistema básico de entrada/salida de red (NetBios) del activo que está asociado con este suceso.
Campo ampliado de identidad	Especifica más información sobre el activo que está asociado con este suceso. El contenido de este campo es texto definido por el usuario y depende de los dispositivos de la red que están disponibles para proporcionar información de identidad. Los ejemplos incluyen: ubicación física de dispositivos, políticas pertinentes, conmutador de red y nombres de puerto.
Tiene identidad (distintivo)	Especifica Verdadero si QRadar ha recopilado información de identificación para el activo que está asociado con este suceso. Para obtener más información sobre qué dispositivos envían información de identidad, consulte la publicación *IBM Security QRadar DSM Configuration Guide*.
Nombre de host de identidad	Especifica el nombre de host del activo que está asociado con este suceso.
MAC de identidad	Especifica la dirección MAC del activo que está asociado con este suceso.

Tabla 16. Detalles de suceso (continuación)

Parámetro	Descripción
Nombre de grupo de identidad	Especifica el nombre de grupo del activo que está asociado con este suceso.

Barra de herramientas de detalles de suceso

La barra de herramientas de detalles de sucesos proporciona varias funciones para ver detalles de sucesos.

La barra de herramientas de **detalles de suceso** proporciona las siguientes funciones:

Tabla 17. Barra de herramientas de detalles de suceso

Volver a lista de sucesos	Pulse **Volver** a **Lista de sucesos** para volver a la lista de sucesos.
Correlación de sucesos	Pulse **Correlación de suceso** para editar la correlación de sucesos. Para obtener más información, consulte Modificación de correlación de sucesos.
Falso positivo	Pulse **Falso positivo** para ajustar QRadar a fin de evitar que los sucesos positivos falsos generen delitos.
Extraer propiedad	Pulse **Extraer propiedad** para crear una propiedad de suceso personalizada a partir del suceso seleccionado.
Anterior	Pulse **Anterior** para ver el suceso anterior en la lista de sucesos.
Siguiente	Pulse **Siguiente** para ver el siguiente suceso en la lista de sucesos.
Datos de PCAP	**Nota:** Esta opción sólo se visualiza si la consola de QRadar se ha configurado para integrarse con el DSM de Juniper JunOS Platform. Para obtener más información sobre cómo gestionar datos de PCAP, consulte Gestión de datos de PCAP. • **Ver información de PCAP**: Seleccione esta opción para ver la información de PCAP. Para obtener más información, consulte Visualización de información de PCAP. • **Descargar archivo de PCAP**: Seleccione esta opción para descargar el archivo de PCAP en el sistema de escritorio. Para obtener más información, consulte Descarga del archivo de PCAP en el sistema.
Imprimir	Pulse **Imprimir** para imprimir los detalles de suceso.

Visualización de delitos asociados

En la pestaña Actividad de registro, puede ver el delito que está asociado con el suceso.

Acerca de esta tarea

Si un suceso coincide con una regla, se puede generar un delito en la pestaña **Delitos**.

Cuando vea un delito en la pestaña **Actividad de registro**, es posible que el delito no se visualice si el magistrado aún no se ha guardado en disco el delito que está asociado con el suceso seleccionado o si el delito se ha depurado de la base de datos. Si esto ocurre, el sistema se lo notificará.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Pulse el icono **Delito** junto al suceso que desea investigar.
4. Vea el delito asociado.

Modificación de la correlación de sucesos

Puede correlacionar manualmente un suceso normalizado o en bruto con una categoría de alto nivel y de bajo nivel (o QID).

Antes de empezar

Esta acción manual se utiliza para correlacionar sucesos de origen de registro desconocidos con sucesos de QRadar conocidos para que se puedan categorizar y procesar adecuadamente.

Acerca de esta tarea

A efectos de normalización, QRadar correlaciona automáticamente sucesos de orígenes de registro con categorías de alto y bajo nivel.

Para obtener más información sobre categorías de suceso, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.

Si los sucesos se reciben de orígenes de registro que el sistema no puede categorizar, los sucesos se categorizan como desconocidos. Dichos sucesos se producen por distintos motivos, incluyendo:

- **Sucesos definidos por el usuario**: Algunos orígenes de registro, como Snort, le permiten crear sucesos definidos por el usuario.
- **Sucesos nuevos o antiguos**: Los orígenes de registro de proveedor pueden actualizar el software con releases de mantenimiento para soportar sucesos nuevos que es posible que QRadar no soporte.

Nota: El icono **Correlacionar suceso** está inhabilitado para los sucesos cuando la categoría de alto nivel es Auditoría SIM o el tipo de origen de registro es Protocolo de acceso a objetos simple (SOAP).

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Efectúe una doble pulsación en el suceso que desea correlacionar.
4. Pulse **Correlación de suceso**.
5. Si conoce el QID que desea correlacionar con este suceso, escriba el QID en el campo **Especifique los QID**.
6. Si no conoce el QID que desea correlacionar con este suceso, puede buscar un QID específico:
   a. Elija una de las opciones siguientes: `Para buscar un QID por categoría, seleccione la categoría de alto nivel en el recuadro de lista Categoría de alto nivel. Para buscar un QID por categoría, seleccione la categoría de bajo nivel en el recuadro de lista Categoría de bajo nivel. Para buscar un QID por tipo de origen de registro, seleccione un tipo de origen de registro en el recuadro de lista Tipo de origen de registro. Para buscar un QID por nombre, escriba un nombre en el campo QID/Nombre.`
   b. Pulse **Buscar**.
   c. Seleccione **QID** con el que desea asociar este suceso.
7. Pulse **Aceptar**.

Datos de PCAP

Si la consola de QRadar se ha configurado para integrarse con el DSM Juniper JunOS Platform, Packet Capture (PCAP) se puede recibir, procesar y los datos se pueden almacenar de un origen de registro Juniper SRX-Series Services Gateway.

Para obtener más información sobre el DSM Juniper JunOS Platform, consulte la publicación *IBM Security QRadar DSM Configuration Guide*.

Visualización de la columna de datos de PCAP

La columna **Datos de PCAP** no se visualiza en la pestaña **Actividad de registro** de forma predeterminada. Al crear criterios de búsqueda, debe seleccionar la columna **Datos de PCAP** en el panel Definición de columna.

Antes de empezar

Para poder visualizar los datos de PCAP en la pestaña **Actividad de registro**, se debe configurar el origen de registro de Juniper SRX-Series Services Gateway con el protocolo de combinación PCAP Syslog. Para obtener más información sobre cómo configurar protocolos de origen de registro, consulte la publicación *Managing Log Sources Guide*.

Acerca de esta tarea

Cuando se realiza una búsqueda que incluye la columna **Datos de PCAP**, se visualiza un icono en la columna **Datos de PCAP** de los resultados de búsqueda si hay datos de PCAP disponibles para un suceso. Utilizando el icono de **PCAP**, puede ver los datos de PCAP o descargar el archivo **PCAP** en el sistema.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, seleccione **Nueva búsqueda**.
3. Opcional. Para buscar sucesos que tienen datos de PCAP, configure los criterios de búsqueda siguientes:
   a. En el primer recuadro de lista, seleccione **Datos de PCAP**.
   b. En el segundo recuadro de lista, seleccione **Igual que**.
   c. En el tercer recuadro de lista, seleccione **Verdadero**.
   d. Pulse **Añadir filtro**.
4. Configure las definiciones de columna para incluir la columna **Datos de PCAP**:
   a. En la lista **Columnas disponibles** del panel Definición de columna, pulse **Datos de PCAP**.
   b. Pulse el icono **Añadir columna** en el conjunto inferior de iconos para mover la columna **Datos de PCAP** a la lista **Columnas**.
   c. Opcional. Pulse el icono **Añadir columna** en el conjunto superior de iconos para mover la columna **Datos de PCAP** a la lista **Agrupar por**.
5. Pulse **Filtro**.
6. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
7. Efectúe una doble pulsación en el suceso que desee investigar.

Qué hacer a continuación

Para obtener más información sobre cómo ver y descargar datos de PCAP, consulte las secciones siguientes:

- Visualización de la información de PCAP
- Descarga del archivo de PCAP en el sistema

Visualización de la información de PCAP

En el menú de barra de herramientas **Datos de PCAP**, puede ver una versión legible de los datos en el archivo de PCAP o descargar el archivo de PCAP en el sistema.

Antes de empezar

Para poder ver información de PCAP, debe realizar o seleccionar una búsqueda que visualice la columna **Datos de PCAP**.

Acerca de esta tarea

Antes de poder visualizar los datos de PCAP, se debe recuperar el archivo de PCAP para visualizarlo en la interfaz de usuario. Si el proceso de descarga tarda un período de tiempo prolongado, se visualiza la ventana Downloading PCAP Packet information. En la mayoría de los casos, el proceso de descarga es rápido y esta ventana no se visualiza.

Una vez recuperado el archivo, una ventana emergente proporciona una versión legible del archivo de PCAP. Puede leer la información que se visualiza en la ventana o descargar la información en el sistema

Procedimiento

1. Para el suceso que desea investigar, elija una de las opciones siguientes:
   - Seleccione el suceso y pulse el icono **PCAP**.
   - Pulse el botón derecho del ratón en el icono **PCAP** para el suceso y seleccione **Más opciones** > **Ver información de PCAP**.
   - Efectúe una doble pulsación en el suceso que desea investigar y, a continuación, seleccione **Datos de PCAP** > **Ver información de PCAP** en la barra de herramientas de detalles de suceso.
2. Si desea descargar la información en el sistema, seleccione una de las opciones siguientes:
   - Pulse **Descargar archivo de PCAP** para descargar el archivo de PCAP original que se debe utilizar en una aplicación externa.
   - Pulse **Descargar texto de PCAP** para descargar la información de PCAP en formato .TXT
3. Elija una de las siguientes opciones:
   - Si desea abrir el archivo para su visualización inmediata, seleccione la opción **Open with** y seleccione una aplicación en el recuadro de lista.
   - Si desea guardar la lista, seleccione la opción **Save File** .
4. Pulse **Aceptar**.

Descarga del archivo de PCAP en el sistema

Puede descargar el archivo PCAP en el sistema para almacenarlo o para utilizar en otras aplicaciones.

Antes de empezar

Antes de poder ver la información de PCAP, debe realizar o seleccionar una búsqueda que muestre la columna Datos de PCAP. consulte **Visualización de la columna de datos de PCAP**.

Procedimiento

1. Para el suceso que desea investigar, elija una de las opciones siguientes:
   - Seleccione el suceso y pulse el icono **PCAP**.
   - Pulse el botón derecho del ratón en el icono de PCAP para el evento y seleccione **Más opciones** > **Descargar archivo de PCAP**.
   - Efectúe una doble pulsación en el suceso que desea investigar, y, a continuación, seleccione **Datos de PCAP** > **Descargar archivo de PCAP** en la barra de herramientas de detalles de suceso.
2. Elija una de las siguientes opciones:
   - Si desea abrir el archivo para su visualización inmediata, seleccione la opción **Open with** y seleccione una aplicación en el recuadro de lista.
   - Si desea guardar la lista, seleccione la opción **Save File** .
3. Pulse **Aceptar**.

Exportación de sucesos

Puede exportar sucesos en formato XML (Extensible Markup Language - Lenguaje de marcas extensible) o CSV (Valores separados por comas).

Antes de empezar

El periodo de tiempo necesario para exportar los datos depende del número de parámetros especificados.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:
   - **Exportar a XML** > **Columnas visibles**: seleccione esta opción para exportar solo las columnas que están visibles en la pestaña Actividad de registro. Esta es la opción recomendada.
   - **Exportar a XML** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
   - **Exportar a CSV** > **Columnas visibles**: Seleccione esta opción para exportar sólo las columnas que están visibles en la pestaña **Actividad de registro**. Esta es la opción recomendada.
   - **Exportar a CSV** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
4. Si desea reanudar las actividades mientras la exportación está en curso, pulse **Notificar cuando termine**.

Resultados

Cuando la exportación se haya completado, recibirá una notificación de que la exportación se ha completado. Si no ha seleccionado el icono **Notificar cuando termine**, se visualiza la ventana de estado.

Capítulo 5. Gestión de gráficos

Puede utilizar varias opciones de configuración de gráficos para ver los datos.

Si selecciona un intervalo de tiempo o una opción de agrupación para ver los datos, los gráficos se visualizan sobre la lista de sucesos.

Los gráficos no se visualizan mientras se está en modalidad continua.

Puede configurar un gráfico para seleccionar los datos que desea trazar. Puede configurar gráficos independientemente el uno del otro para visualizar los resultados de búsqueda desde diferentes perspectivas.

Los tipos de gráfico incluyen:

- Gráfico de barras: Visualiza los datos en un gráfico de barras. Esta opción solo está disponible para sucesos agrupados.
- Gráfico circular: Visualiza datos en un gráfico circular. Esta opción solo está disponible para sucesos agrupados.
- Tabla: Visualiza datos en una tabla. Esta opción solo está disponible para sucesos agrupados.
- Serie temporal: Visualiza un gráfico de líneas interactivo que representa los registros que se comparan por un intervalo de tiempo especificado. Para obtener información sobre cómo configurar criterios de búsqueda de serie temporal, consulte Visión general de gráfico de serie temporal.

Después de configurar un gráfico, las configuraciones de gráfico se conservan al:

- Cambiar la vista utilizando el recuadro de lista **Visualizar**.
- Aplicar un filtro.
- Guardar criterios de búsqueda.

Las configuraciones de gráfico no se conservan al:

- Iniciar una búsqueda nueva.
- Acceder a una búsqueda rápida.
- Ver los resultados agrupados en una ventana de rama.
- Guarde los resultados de búsqueda.

Nota: Si utiliza el navegador web Mozilla Firefox y se instala una extensión de navegador de bloqueador de anuncios, no se visualizan gráficos. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.

Visión general de gráfico de serie temporal

Los gráficos de serie temporal son representaciones gráficas de la actividad a lo largo del tiempo.

Los picos y valles que se visualizan en los gráficos describen la actividad de volumen alto y bajo. Los gráficos de serie temporal son útiles para las tendencias de corto plazo y largo plazo de los datos.

Mediante el uso de gráficos de serie temporal, puede acceder, navegar e investigar la actividad de registro o de red desde diversas vistas y perspectivas.

Nota: Debe tener los permisos de rol adecuados para gestionar y ver gráficos de serie temporal.

Para visualizar gráficos de serie temporal, debe crear y guardar una búsqueda que incluya opciones de agrupación y serie temporal. Puede guardar hasta 100 búsquedas de serie temporal.

Las búsquedas guardadas de serie temporal predeterminadas son accesibles desde la lista de búsquedas disponibles en la página de búsqueda de sucesos.

Puede identificar fácilmente las búsquedas de serie temporal guardadas en el menú **Búsquedas rápidas**, porque el nombre de búsqueda se añade con el rango de tiempo especificado en los criterios de búsqueda.

Si los parámetros de búsqueda coinciden con una búsqueda guardada anteriormente para las opciones de agrupación y definición de columna, es posible que se visualice automáticamente un gráfico de serie temporal para los resultados de búsqueda. Si no se visualiza automáticamente un gráfico de series temporal para los criterios de búsqueda no guardados, no existen criterios de búsqueda guardados anteriormente que coincidan con los parámetros de búsqueda. Si esto ocurre, debe habilitar la captura de datos de serie temporal y guardar los criterios de búsqueda.

Puede ampliar y explorar una línea temporal en un gráfico de series temporal para investigar la actividad. La tabla siguiente proporciona funciones que puede utilizar para ver gráficos de serie temporal.

Tabla 18. Funciones de gráficos de serie temporal

Función	Descripción
Ver datos con mayor detalle	Utilizando la característica de zoom, puede investigar segmentos de tiempo más pequeños del tráfico de sucesos. • Mueva el puntero del ratón sobre el gráfico y, a continuación, utilice la rueda del ratón para ampliar el gráfico (girar la rueda del ratón hacia arriba). • Resalte el área del gráfico que desea ampliar. Cuando suelte el botón del ratón, el gráfico muestra un segmento de tiempo más pequeño. Ahora puede pulsar y arrastrar el gráfico para explorar el gráfico. Al ampliar un gráfico de series temporal, el gráfico se renueva para mostrar un segmento de tiempo más pequeños.

Tabla 18. Funciones de gráficos de serie temporal (continuación)

Función	Descripción
Ver un intervalo de tiempo mayor de datos	Utilizando la característica de zoom, puede investigar segmentos de tiempo más grandes o volver al rango de tiempo máximo. Puede expandir un rango de tiempo utilizando una de las opciones siguientes: • Pulsar en el restablecimiento de zoom en la esquina superior izquierda del gráfico. • Mover el puntero de ratón sobre el gráfico y, a continuación, utilizar la rueda del ratón para expandir la vista (girar la rueda del ratón hacia abajo).
Explorar el gráfico	Cuando haya aumentado un gráfico de series temporal, puede pulsar y arrastrar el gráfico a la izquierda o a la derecha para explorar la línea temporal.

Leyendas de gráficos

Cada gráfico proporciona una leyenda, que es una referencia visual para ayudarle a asociar los objetos de gráfico con los parámetros que representan.

Mediante la característica de leyenda, puede realizar las acciones siguientes:

- Mueva el puntero del ratón sobre un elemento de leyenda o el bloque de color de leyenda para ver más información sobre los parámetros que representa.
- Pulse el botón derecho del ratón en el elemento de leyenda para investigar el elemento adicionalmente.
- Pulse un elemento de leyenda de gráfico circular o de barras para ocultar el elemento en el gráfico. Pulse el elemento de leyenda de nuevo para mostrar el elemento oculto. También puede pulsar el elemento de gráfico correspondiente para ocultar y mostrar el elemento.
- Pulse **Leyenda**, o la flecha que se encuentra junto a ella, si desea eliminar la leyenda de la pantalla de gráfico.

Configuración de gráficos

Puede utilizar opciones de configuración para cambiar el tipo de gráfico, el tipo de objeto del que desea crear el gráfico y el número de objetos que se representan en el gráfico. Para gráficos de serie temporal, también puede seleccionar un intervalo de tiempo y habilitar la captura de datos de serie temporal.

Antes de empezar

Los gráficos no se visualizan cuando se ven sucesos en modalidad de tiempo real (modalidad continua). Para visualizar gráficos, debe acceder a la pestaña **Actividad de registro** y elija una de las opciones siguientes:

- Seleccione opciones en los recuadros de lista **Ver** y **Visualizar** y, a continuación, pulse **Guardar criterios** en la barra de herramientas. Consulte Guardar criterios de búsqueda de sucesos y flujos.
- En la barra de herramientas, seleccione una búsqueda guardada en la lista **Búsqueda rápida**.

- Realice una búsqueda agrupada y, a continuación, pulse **Guardar criterios** en la barra de herramientas.

Si piensa configurar un gráfico de serie temporal, asegúrese de que los criterios de búsqueda guardada se agrupen y especifiquen un rango de tiempo.

Acerca de esta tarea

Los datos se pueden acumular para que cuando se realice una búsqueda de serie temporal, esté disponible una memoria caché de datos para visualizar datos para el periodo de tiempo anterior. Después de habilitar la captura de datos de serie temporal para un parámetro seleccionado, se visualiza un asterisco (*) junto al parámetro en el recuadro de lista Valor para gráfico.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el panel Gráficos, pulse el icono **Configurar**.
3. Configure valores para los parámetros siguientes:

Opción	Descripción
Parámetro	Descripción
Valor para gráfico	En el recuadro de lista, seleccione el tipo de objeto que desea trazar en el eje Y del gráfico. Las opciones incluyen todos los parámetros de sucesos normalizados y personalizadas incluidos en los parámetros de búsqueda.
Mostrar parte superior	En el cuadro de lista, seleccione el número de objetos que desee ver en el gráfico. El valor predeterminado es 10. Si se crean gráficos de más de 10 elementos es posible que los datos de gráfico no sean legibles.
Tipo de gráfico	En el cuadro de lista, seleccione el tipo de gráfico que desee ver. Si el gráfico de barras, circular o de tabla se basa en criterios de búsqueda guardados con un rango de tiempo de más de 1 hora, debe pulsar **Actualizar detalles** para actualizar el gráfico y llenar los detalles de suceso
Capturar datos de serie temporal	Seleccione este recuadro de selección si desea habilitar la captura de datos de serie temporal. Cuando se selecciona este recuadro de selección, la característica de gráfico empieza a acumular datos para gráficos de serie temporal. De forma predeterminada, esta opción está inhabilitada. Esta opción solo está disponible en gráficos de serie temporal.

Opción	Descripción
Rango de tiempo	En el cuadro de lista, seleccione el rango de tiempo que desee ver. Esta opción solo está disponible en gráficos de serie temporal.

4. Si ha seleccionado la opción de gráfico **Serie temporal** y ha habilitado la opción **Capturar datos de serie temporal**, pulse **Guardar criterios** en la barra de herramientas.
5. Para ver la lista de sucesos si el rango de tiempo es mayor que 1 hora, pulse **Actualizar detalles**.

Capítulo 6. Búsquedas de datos

En la pestaña **Actividad de registro**, puede buscar sucesos mediante criterios específicos.

Puede crear una búsqueda o cargar un conjunto de criterios de búsqueda guardados anteriormente. Puede seleccionar, organizar y agrupar las columnas de datos a visualizar en los resultados de la búsqueda.

Después de seleccionar una búsqueda, puede guardar los criterios de búsqueda y los resultados de la búsqueda.

Búsqueda de elementos que coinciden con los criterios

Puede buscar datos que coincidan con los criterios de búsqueda.

Acerca de esta tarea

Puesto que se busca en la base de datos entera, es posible que las búsquedas tarden un tiempo prolongado, dependiendo del tamaño de la base de datos.

Puede utilizar el parámetro de búsqueda **Filtro rápido** para buscar elementos que coinciden con la serie de búsqueda en la carga útil de suceso.

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de suceso y de flujo:

Tabla 19. Opciones de búsqueda

Opciones	Descripción
Grupo	Seleccione un grupo de búsqueda de sucesos para verlo en la lista **Búsquedas guardadas disponibles**.
Escriba la búsqueda guardada o seleccione en la lista	Escriba el nombre de una búsqueda guardada o una palabra clave para filtrar la lista **Búsquedas guardadas disponibles**.
Búsquedas guardadas disponibles	Esta lista muestra todas las búsquedas disponibles, a menos que utilice las opciones **Agrupe o Escriba la búsqueda guardada** o **Seleccione en la lista** para aplicar un filtro a la lista. Puede seleccionar una búsqueda guardada en esta lista para visualizarla o editarla.
Buscar	El icono **Buscar** está disponible en varios paneles de la página de búsqueda. Puede pulsar Buscar cuando haya terminado de configurar la búsqueda y desee ver los resultados.
Incluir en Búsquedas rápidas	Marque este recuadro de selección para incluir esta búsqueda en el menú **Búsqueda rápida**.

Tabla 19. Opciones de búsqueda (continuación)

Opciones	Descripción
Incluir en Panel de control	Marque este recuadro de selección para incluir los datos de la búsqueda guardada en la pestaña **Panel de control**. Para obtener más información sobre la pestaña **Panel de control**, consulte Gestión de panel de control. **Nota:** Este parámetro sólo se visualiza si se agrupa la búsqueda.
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada.
Compartir con todos	Marque este recuadro de selección para compartir esta búsqueda con todos los demás usuarios.
Tiempo real (modalidad continua)	Visualiza resultados en modalidad continua. Para obtener más información sobre la modalidad continua, consulte Visualización de sucesos de modalidad continua. **Nota:** Cuando se habilita Tiempo real (modalidad continua), no puede agrupar los resultados de búsqueda. Si selecciona cualquier opción de agrupación en el panel Definición de columna, se abre un mensaje de error.
Último intervalo (renovación automática)	Visualiza los resultados de búsqueda en modalidad de renovación automática. En la modalidad de renovación automática, la pestaña **Actividad de registro** se renueva a intervalos de un minuto para visualizar la información más reciente.
Reciente	Seleccione un rango de tiempo predefinido para la búsqueda. Después de seleccionar esta opción, debe seleccionar una opción de rango de tiempo en el cuadro de lista.
Intervalo específico	Seleccione un rango de tiempo personalizado para la búsqueda. Después de seleccionar esta opción, debe seleccionar el rango de fecha y hora en los calendarios **Hora de inicio** y **Hora de finalización**.

Tabla 19. Opciones de búsqueda (continuación)

Opciones	Descripción
Acumulación de datos	Este panel sólo se visualiza cuando se carga una búsqueda guardada. La habilitación de recuentos exclusivos en datos acumulados que se comparten con muchos otros informes y búsquedas guardadas puede disminuir el rendimiento del sistema. Al cargar una búsqueda guardada, este panel muestra las opciones siguientes: • Si no se acumulan datos para esta búsqueda guardada, se visualiza el siguiente búsqueda: `No se están acumulando datos para esta búsqueda`. • Si se acumulan datos se acumulan para esta búsqueda guardada, se visualizan las opciones siguientes: – **columnas**: Al pulsar este enlace o pasar el puntero del ratón sobre él, se abre una lista de las columnas que están acumulando datos. – **Habilitar recuentos exclusivos/Inhabilitar recuentos exclusivos**: Este enlace le permite habilitar o inhabilitar los resultados de búsqueda para visualizar los recuentos de sucesos exclusivos en lugar de promedios de recuentos a lo largo del tiempo. Después de pulsar el enlace **Habilitar recuentos exclusivos**, se abre un recuadro de diálogo que indica qué informes y búsquedas guardadas comparten los datos acumulados.
Filtros actuales	Esta lista muestra los filtros que se aplican a esta búsqueda. Las opciones para añadir un filtro se encuentran sobre la lista **Filtros actuales**.
Guardar resultados cuando finalice la búsqueda	Marque este recuadro de selección para guardar y dar nombre a los resultados de la búsqueda.
Visualizar	Seleccione esta lista para especificar una columna predefinida que se ha establecido para visualizarse en los resultados de búsqueda.
Escriba la columna o seleccione en la lista	Puede utilizar el campo para filtrar las columnas que figuran en la lista Columnas disponibles. Escriba el nombre de la columna que desea localizar o escriba una palabra clave para visualizar una lista de nombres de columna. Por ejemplo, escriba `Device` para visualizar una lista de columnas que incluyan Device en el nombre de columna.

Tabla 19. Opciones de búsqueda (continuación)

Opciones	Descripción
Columnas disponibles	Esta lista muestra las columnas disponibles. Las columnas que se están utilizando actualmente para esta búsqueda guardada se resaltan y se visualizan en la lista de **Columnas**.
Añadir y eliminar iconos de columna (conjunto superior)	Utilice el conjunto superior de iconos para personalizar la lista **Agrupar por**. • **Añadir columna**: Seleccione una o más columnas de la lista **Columnas disponibles** y pulse el icono **Añadir columna**. • **Eliminar columna**: Seleccione una o más columnas de la lista **Agrupar por** y pulse el icono **Eliminar columna**.
Añadir y eliminar iconos de columna (conjunto inferior)	Utilice el conjunto inferior de iconos para personalizar la lista **Columnas**. • **Añadir columna**: Seleccione una o más columnas de la lista Columnas disponibles y pulse el icono **Añadir columna**. • **Eliminar columna**: Seleccione una o más columnas de la lista Columnas y pulse el icono **Eliminar columna**.
Agrupar por	Esta lista especifica las columnas en las que la búsqueda guardada agrupa los resultados. Utilice las opciones siguientes para personalizar adicionalmente la lista Agrupar por: • Subir: Seleccione una columna y muévala hacia arriba en la lista de prioridad utilizando el icono **Subir**. • Bajar: Seleccione una columna y muévala hacia abajo en la lista de prioridad utilizando el icono **Bajar**. La lista de prioridad especifica en qué orden se agrupan los resultados. Los resultados de búsqueda se agrupan por la primera columna de la lista **Agrupar por** y, a continuación, se agrupan por la columna siguiente de la lista.

Tabla 19. Opciones de búsqueda (continuación)

Opciones	Descripción
Columnas	Especifica las columnas que se han elegido para la búsqueda. Puede seleccionar más columnas de la lista **Columnas disponibles**. Puede personalizar adicionalmente la lista **Columnas** utilizando las opciones siguientes: • **Subir**: Mueve la columna seleccionada hacia arriba en la lista de prioridades. • **Bajar**: Mueve la columna seleccionada hacia abajo en la lista de prioridades. Si el tipo de columna es numérico o está basado en el tiempo y hay una entrada en la lista **Agrupar por**, la columna incluye un recuadro de lista. Utilice el recuadro de lista para elegir cómo desea agrupar la columna. Si el tipo de columna es grupo, la columna incluye un recuadro de lista para elegir cuántos niveles desea incluir para el grupo.
Ordenar por	En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda. A continuación, en el segundo recuadro de lista, seleccione el orden que desea para visualizar para los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.
Límite de resultados	Puede especificar el número de filas que una búsqueda devuelve en la ventana Editar búsqueda . El campo **Límite de resultados** también aparece en la ventana Resultados . • Para una búsqueda guardada, el límite se almacena en la búsqueda guardada y se vuelve a aplicar al cargar la búsqueda. • Cuando se realiza una ordenación en una columna del resultado de búsqueda que tiene un límite de filas, la ordenación se realiza dentro de las filas limitadas que se muestran en la cuadrícula de datos. • En el caso de una búsqueda agrupada por con el gráfico de serie temporal activado, el límite de filas sólo se aplica a la cuadrícula de datos. El desplegable **N principales** del gráfico de serie temporal sigue controlando cuántas series temporales se dibujan en el gráfico.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
3. Para seleccionar una búsqueda guardada anteriormente:
   a. Elija una de las opciones siguientes: `En la lista Búsquedas guardadas disponibles, seleccione la búsqueda guardada que desea guardar. En el`

campo Escriba la búsqueda guardada o seleccione en la lista´, escriba el nombre de la búsqueda que desea cargar.

b. Pulse **Cargar**.

c. En el panel Editar búsqueda, seleccione las opciones que desea para esta búsqueda. Consulte la Tabla 1.

4. Para crear una búsqueda, en el panel Rango de tiempo, seleccione las opciones para el rango de tiempo que desea capturar para esta búsqueda.
5. Opcional. En el panel Acumulación de datos, habilite recuentos exclusivos:
   a. Pulse **Habilitar recuentos exclusivos**.
   b. En la ventana Aviso, lea el mensaje de aviso y pulse **Continuar**. Para obtener más información sobre cómo habilitar recuentos exclusivos, consulte la Tabla 1.
6. En el panel Parámetros de búsqueda, defina los criterios de búsqueda:
   a. En el primer recuadro de lista, seleccione un parámetro que desee buscar. Por ejemplo, Dispositivo, Puerto de origen o Nombre de suceso.
   b. En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda.
   c. En el campo de entrada, escriba información específica que está relacionada con el parámetro de búsqueda.
   d. Pulse **Añadir filtro**.
   e. Repita los pasos a hasta d para cada filtro que desea añadir a los criterios de búsqueda.
7. Opcional. Para guardar automáticamente los resultados de búsqueda cuando la búsqueda se ha completado, marque el recuadro de selección **Guarde los resultados cuando finalice la búsqueda** y, a continuación, escriba un nombre para la búsqueda guardada.
8. En el panel Definición de columna, defina las columnas y el diseño de columna que desea utilizar para ver los resultados:
   a. En el recuadro de lista **Visualizar**, seleccione la columna preconfigurada establecida para asociarse con esta búsqueda.
   b. Pulse la flecha situada junto a **Definición de vista avanzada** para visualizar parámetros de búsqueda avanzada.
   c. Personalice las columnas que se visualizarán en los resultados de búsqueda. Consulte la Tabla 1.
   d. Opcional. En el campo **Límite de resultados**, escriba el número de filas que desea que devuelva la búsqueda.
9. Pulse **Filtro**.

Resultados

Se visualiza el estado **En curso (<porcentaje>%completado)** en la esquina superior derecha.

.

Al ver resultados de búsqueda parciales, el motor de búsqueda funciona en segundo plano para completar la búsqueda y renueva los resultados parciales para actualizar la vista.

Cuando la búsqueda se ha completado, se visualiza el estado **Completado** en la esquina superior derecha.

Conceptos relacionados:

"Opciones de búsqueda avanzada" en la página 65
Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para ejecutar una consulta.

"Ejemplos de serie de búsqueda de AQL" en la página 67
Utilice Ariel Query Language (AQL) para recuperar campos específicos de los sucesos, flujos y las tablas simarc en la base de datos de Ariel.

Guardar criterios de búsqueda

Puede guardar los criterios de búsqueda configurados para poder reutilizar los criterios y utilizar los criterios de búsqueda guardados en otros componentes como, por ejemplo, informes. Los criterios de búsqueda guardados no caducan.

Acerca de esta tarea

Si se especifica un rango temporal para la búsqueda, el nombre de búsqueda se añade con el rango de tiempo especificado. Por ejemplo, una búsqueda guardada denominada Explotaciones por origen con un rango de tiempo de Últimos 5 minutos se convierte en Explotaciones por origen - Últimos 5 minutos.

Si cambia una columna establecida en una búsqueda guardada anteriormente y luego guarda los criterios de búsqueda utilizando el mismo nombre, se perderán las acumulaciones anteriores de gráficos de series temporales.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Realice una búsqueda.
3. Pulse **Guardar criterios**.
4. Entre valores para los parámetros:

Opción	**Descripción**
Parámetro	Descripción
Nombre de búsqueda	Escriba el nombre exclusivo que desee asignar a este criterio de búsqueda.
Asignar búsqueda a grupo(s)	Marque el recuadro de selección para el grupo al que desea asignar esta búsqueda guardada. Si no selecciona un grupo, esta búsqueda guardada se asigna al grupo Otros de forma predeterminada. Para obtener más información, consulte Gestión de grupos de búsqueda.
Gestionar grupos	Pulse **Gestionar grupos** para gestionar grupos de búsqueda. Para obtener más información, consulte Gestión de grupos de búsqueda.

Opción	Descripción
Opciones de intervalo de tiempo:	Elija una de las siguientes opciones: • **Tiempo real (modalidad continua)**: Seleccione esta opción para filtrar los resultados de búsqueda mientras se está en modalidad continua. • **Último intervalo (renovación automática)**: Seleccione esta opción para filtrar los resultados de búsqueda mientras se está en modalidad de renovación automática. Las pestañas **Actividad de registro** y **Actividad de red** se renuevan a intervalos de un minuto para visualizar la información más reciente. • **Reciente**: Seleccione esta opción y, desde este recuadro de lista, seleccione el rango de tiempo por el que desea filtrar. • **Intervalo específico**: Seleccione esta opción y, en el calendario, seleccione el rango de fecha y hora por el que desea filtrar.
Incluir en Búsquedas rápidas	Marque este recuadro de selección para incluir esta búsqueda en el recuadro de lista **Búsqueda rápida** en la barra de herramientas.
Incluir en Panel de control	Marque este recuadro de selección para incluir los datos de la búsqueda guardada en la pestaña **Panel de control**. Para obtener más información sobre la pestaña **Panel de control**, consulte Gestión de panel de control. **Nota:** Este parámetro sólo se visualiza si se agrupa la búsqueda.
Establecer como valor predeterminado	
Compartir con todos	Marque este recuadro de selección para compartir estos requisitos de búsqueda con todos los usuarios.

5. Pulse **Aceptar**.

Búsqueda planificada

Utilice la opción de búsqueda planificada para planificar una búsqueda y ver los resultados.

Puede planificar que una búsqueda se ejecute a una hora específica del día o de la noche.

Ejemplo:
Si planifica que una búsqueda se ejecute por la noche, puede investigar por la mañana. A diferencia de los informes, tiene la opción de agrupar los resultados de búsqueda e investigar adicionalmente. Puede buscar el número de inicios de sesión anómalos en el grupo de red. Si el resultado es generalmente 10 y el resultado de la búsqueda es 100, puede agrupar los resultados de búsqueda para facilitar la

investigación. Para ver qué usuario tiene la mayoría de inicios de sesión anómalos, puede agruparlos por nombre de usuario. Puede continuar investigando adicionalmente.

Puede planificar una búsqueda en sucesos o flujos desde la pestaña **Informes**. Debe seleccionar un conjunto de criterios de búsqueda previamente guardado para la planificación.

1. Cree un informe

   Especifique la siguiente información en la ventana **Asistente de informes**:

   - El tipo de gráfico es Sucesos/archivos de registro o Flujos.
   - El informe se basa en una búsqueda guardada.
   - Genere un delito.

     Puede elegir la opción **Crear un delito individual** o la opción **Añadir resultado a un delito existente**.

     También puede generar una búsqueda manual.
2. Vea los resultados de búsqueda

Puede ver los resultados de la búsqueda planificada desde la pestaña **Delitos**.

- Los delitos de búsqueda planificada se identifican por la columna **Tipo de delito**.

  Si crea un delito individual, se genera un delito cada vez que se ejecuta el informe. Si añade el resultado de búsqueda guardada en un delito existente, se crea un delito la primera vez que se ejecuta el informe. Las ejecuciones de informe subsiguientes se añaden a este delito. Si no se devuelven resultados, el sistema no añade o crea un delito.
- Para ver el resultado de búsqueda más reciente en la ventana Resumen de delitos, efectúe una doble pulsación en un delito de búsqueda planificada de la lista de delitos. Para ver la lista de todas las ejecuciones de búsqueda planificada, pulse **Resultados de búsqueda** en el panel **Últimos 5 resultados de búsqueda**.

Puede asignar un delito de búsqueda planificada a un usuario.

Conceptos relacionados:

"Opciones de búsqueda avanzada"
Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para ejecutar una consulta.

"Ejemplos de serie de búsqueda de AQL" en la página 67
Utilice Ariel Query Language (AQL) para recuperar campos específicos de los sucesos, flujos y las tablas simarc en la base de datos de Ariel.

Opciones de búsqueda avanzada

Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para ejecutar una consulta.

El campo **Búsqueda avanzada** tiene finalización automática y resaltado de sintaxis.

Utilice la finalización automática y el resaltado de sintaxis para ayudar a crear consultas. Para obtener información sobre los navegadores web soportados, consulte "Navegadores web soportados" en la página 3

Acceso a búsqueda avanzada

Acceda a la opción **Búsqueda avanzada** desde la barra de herramientas **Buscar** que está en el separador **Actividad de registro** para escribir una consulta de AQL.

Seleccione **Búsqueda avanzada** desde el recuadro de lista de la barra de herramientas **Buscar**.

Expanda el campo **Búsqueda avanzada** siguiendo estos pasos:

1. Arrastre el icono de expansión que se encuentra a la derecha del campo.
2. Pulse Mayús + Intro para ir a la línea siguiente.
3. Pulse Intro.

Puede pulsar el botón derecho del ratón en cualquier valor del resultado de búsqueda y filtrar por ese valor.

Efectúe una doble pulsación en cualquier fila del resultado de búsqueda para ver más detalles.

Todas las búsquedas, incluidas las búsquedas de AOL, se incluyen en el registro de auditoría.

Ejemplos de serie de búsqueda de AQL

La tabla siguiente proporciona ejemplos de las series de búsqueda de AOL.

Tabla 20. Ejemplos de series de búsqueda de AOL

Descripción	Ejemplo
Seleccionar columnas predeterminadas en sucesos.	`SELECT * FROM events`
Seleccionar columnas específicas.	`SELECT sourceip, destinationip FROM events`
Seleccionar columnas específicas y ordenar los resultados.	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
Ejecutar una consulta de búsqueda agregada.	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
Ejecutar una llamada de función en una cláusula SELECT.	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
Filtrar los resultados de búsqueda utilizando una cláusula WHERE.	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`
Buscar sucesos que han desencadenado una regla específica, que se basa en el nombre de regla o el texto parcial en el nombre de regla.	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
Hacer referencia a nombres de campo que contienen caracteres especiales, por ejemplo caracteres aritméticos o espacios, poniendo el nombre de campo entre comillas.	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

Para obtener más información acerca de las funciones, los campos simarc y los operadores, consulte la publicación *Ariel Query Language guide*.

Conceptos relacionados:

"Búsqueda planificada" en la página 64
Utilice la opción de búsqueda planificada para planificar una búsqueda y ver los resultados.

"Búsqueda de filtros" en la página 70
Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

Tareas relacionadas:

"Búsqueda de elementos que coinciden con los criterios" en la página 57
Puede buscar datos que coincidan con los criterios de búsqueda.

Ejemplos de serie de búsqueda de AQL

Utilice Ariel Query Language (AQL) para recuperar campos específicos de los sucesos, flujos y las tablas simarc en la base de datos de Ariel.

Informes de uso de cuenta

Comunidades de usuarios diferentes pueden tener indicadores de amenazas y de uso diferentes.

Utilice datos de referencia para informar sobre diversas propiedades de usuario, tales como departamento, ubicación o gestor.

Puede utilizar datos de referencia externos.

La consulta siguiente devuelve información de metadatos sobre el usuario a partir de sucesos de inicio de sesión.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Identificadores de cuenta múltiples

En este ejemplo, los usuarios tienen varias cuentas en la red. La empresa necesita tener una vista individual de la actividad de un usuario.

Utilice datos de referencia para correlacionar un ID de usuario local con un ID global.

La consulta siguiente devuelve las cuentas de usuario que son utilizadas por un ID global en sucesos que están marcados como sospechosos.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

La consulta siguiente muestra las actividades que se han realizado mediante un ID global.

```
SELECT
QIDNAME(qid) as 'Event name,
starttime as Time,
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event  Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Identificar una emisión larga de señales de baliza sospechosa

Muchas amenazas utilizan mandato y control para transmitir periódicamente durante días, semanas y meses.

Las búsquedas avanzadas pueden identificar patrones de conexión a lo largo del tiempo. Por ejemplo, puede investigar conexiones breves, constantes y de pequeño volumen que se realizan cada día/semana/mes entre direcciones IP o entre una dirección IP y una ubicación geográfica.

Utilice la API REST de IBM Security QRadar para generar un delito o para llenar un conjunto de referencia o tabla de referencia.

La consulta siguiente detecta la emisión diaria de señales de baliza hacia un dominio utilizando sucesos de registro de proxy. Las horas de emisión de señales de baliza no son las mismas cada día. El intervalo de tiempo entre emisiones es corto.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

La propiedad **url_domain** es una propiedad personalizada de los archivos de registro de proxy.

Datos de inteligencia sobre amenazas externas

Los datos de uso y de seguridad que están correlacionados con datos de inteligencia sobre amenazas externas pueden proporcionar indicadores importantes sobre amenazas.

Las búsquedas avanzadas pueden asociar indicadores de amenazas externas con otros sucesos de seguridad y datos de uso.

Esta consulta muestra cómo puede analizar datos de amenazas externas durante muchos días, semanas o meses para identificar y priorizar el nivel de riesgo de activos y cuentas.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
```

```
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

Inteligencia y configuración de activos

Los indicadores de amenazas y de uso varían según el tipo de activo, sistema operativo, vulnerabilidad, tipo de servidor, clasificación y otros parámetros.

La consulta siguiente utiliza búsquedas avanzadas y el modelo de activos para obtener conocimientos operativos respecto a una ubicación.

La función **Assetproperty** obtiene valores de propiedad de activos, lo cual permite incluir datos de activos en los resultados.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

La función **AssetUser** obtiene el nombre de usuario a partir de la base de datos de activos.

Función de búsqueda de red

Puede utilizar la función de **búsqueda de red** para obtener el nombre de red que está asociado a una dirección IP.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Función de búsqueda de regla

Puede utilizar la función de **búsqueda de regla** para obtener el nombre de una regla por su identificador.

```
SELECT RULENAME(123) FROM events
```

La consulta siguiente devuelve los sucesos que activaron un nombre de regla determinado.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

Conceptos relacionados:

"Búsqueda planificada" en la página 64
Utilice la opción de búsqueda planificada para planificar una búsqueda y ver los resultados.

"Búsqueda de filtros" en la página 70
Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

Tareas relacionadas:

"Búsqueda de elementos que coinciden con los criterios" en la página 57
Puede buscar datos que coincidan con los criterios de búsqueda.

Búsqueda de filtros

Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

Puede filtrar las búsquedas desde estas ubicaciones:

Barra de herramientas Actividad de registro y barras de herramientas
Seleccione **Filtro rápido** en el recuadro de lista de la barra de herramientas **Buscar** para escribir una serie de búsqueda de texto. Pulse el icono **Filtro rápido** para aplicar el a la lista de sucesos o flujos.

Recuadro de diálogo Añadir filtro
Pulse el icono **Añadir filtro** en la pestaña **Actividad de registro** o .

Seleccione **Filtro rápido** como parámetro de filtro y escriba una serie de búsqueda de texto.

Páginas de búsqueda de flujos
Añada un filtro rápido a la lista de filtros.

Cuando vea en tiempo real (modalidad continua) o modalidad del último intervalo, puede escribir sólo palabras o frases simples en el campo **Filtro rápido**. Cuando vea **sucesos** o con un rango de tiempo, siga las directrices de sintaxis de la tabla siguiente:

Tabla 21. Directrices de sintaxis de filtro rápido

Descripción	Ejemplo
Incluir cualquier texto sin formato que se espera encontrar en la carga útil.	`Firewall`
Buscar frases exactas incluyendo varios términos entre comillas.	`"Denegación de cortafuegos"`
Incluir caracteres comodín individuales y múltiples. El término de búsqueda no puede empezar con un comodín.	`F?rewall` o `F??ew*`
Agrupar términos con expresiones lógicas, por ejemplo AND, OR y NOT. Para que se reconozca como expresiones lógicas y no como términos de búsqueda, la sintaxis y los operadores deben estar en mayúsculas.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
Al crear criterios de búsqueda que incluyen la expresión lógica NOT, debe incluir al menos otro tipo de expresión lógica, de lo contrario, no se devuelven resultados.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
Preceder los siguientes caracteres por una barra inclinada invertida para indicar que el carácter es parte del término de búsqueda: `+ - && || ! () {} [] ^ " ~ * ? : \.`	`"%PIX\-5\-304001"`

Los términos de búsqueda se comparan en secuencia desde el primer carácter de la palabra o frase de carga útil. El término de búsqueda user coincide con `user_1` y `user_2`, pero no coincide con las frases siguientes: `ruser`, `myuser` o `anyuser`.

Conceptos relacionados:

"Opciones de búsqueda avanzada" en la página 65
Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para

ejecutar una consulta.

"Ejemplos de serie de búsqueda de AQL" en la página 67
Utilice Ariel Query Language (AQL) para recuperar campos específicos de los sucesos, flujos y las tablas simarc en la base de datos de Ariel.

Utilización de una sub-búsqueda para refinar los resultados de búsqueda

Puede utilizar una sub-búsqueda para buscar en un conjunto de resultados de búsqueda completada. La sub-búsqueda se utiliza para refinar los resultados de búsqueda, sin buscar de nuevo en la base de datos.

Antes de empezar

Al definir una búsqueda que desea utilizar como base para realizar una sub-búsqueda, asegúrese de que la opción Tiempo real (modalidad continua) está inhabilitada y la búsqueda no se ha agrupado.

Acerca de esta tarea

Esta característica no está disponible para búsquedas agrupados, búsquedas en curso o en modalidad continua.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Realice una búsqueda.
3. Cuando la búsqueda se haya completado, añada otro filtro:
   a. Pulse **Añadir filtro**.
   b. En el primer recuadro de lista, seleccione un parámetro que desee buscar.
   c. En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda. La lista de modificadores que están disponibles depende del atributo que se ha seleccionado en la primera lista.
   d. En el campo de entrada, escriba información específica que esté relacionada con la búsqueda.
   e. Pulse **Añadir filtro**.

Resultados

El panel Filtros originales especifica los filtros originales que se aplican a la búsqueda de base. El panel Filtros actuales especifica los filtros que se aplican a la sub-búsqueda. Puede borrar filtros de sub-búsqueda sin reiniciar la búsqueda de base. Pulse el enlace **Borrar filtro** junto al filtro que desea borrar. Si borra un filtro en el panel Filtros originales, se reinicia la búsqueda de base.

Si suprime los criterios de búsqueda de base para los criterios de sub-búsqueda guardados, seguirá teniendo acceso a los criterios de sub-búsqueda guardados. Si añade un filtro, la sub-búsqueda busca en la base de datos entera porque la función de búsqueda ya no basa la búsqueda en un conjunto de datos buscado previamente.

Qué hacer a continuación

Guardar criterios de búsqueda

Gestión de resultados de búsqueda

Puede iniciar varias búsquedas y, a continuación, ir a otras pestañas para realizar otras tareas mientras las búsquedas se completan en segundo plano.

Puede configurar una búsqueda para que, al finalizarse, envíe una notificación por correo electrónico.

En cualquier momento mientras una búsqueda está en curso, puede volver a la pestaña **Actividad de registro** para ver los resultados de búsqueda parciales o completos.

Supresión de criterios de búsqueda

Puede suprimir criterios de búsqueda.

Acerca de esta tarea

Al suprimir una búsqueda guardada, es posible que los objetos que están asociados con la búsqueda guardada no funcionen. Los informes y las reglas de detección de anomalías son objetos de QRadar que utilizan criterios de búsqueda guardada. Después de suprimir una búsqueda guardada, edite los objetos asociados para asegurarse de que siguen funcionando.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, seleccione **Nueva búsqueda** o **Editar búsqueda**.
3. En el panel Búsquedas guardadas, seleccione una búsqueda guardada en el recuadro de lista **Búsquedas guardadas disponibles**.
4. Pulse **Suprimir**.
   - Si los criterios de búsqueda guardada no están asociado con otros objetos de QRadar, se visualiza una ventana de confirmación.
   - Si los criterios de búsqueda guardada están asociado con otros objetos, se visualiza la ventana Suprimir búsqueda guardada. La ventana lista objetos que están asociados con la búsqueda guardada que desea suprimir. Tome nota de los objetos asociados.
5. Pulse **Aceptar**.
6. Elija una de las siguientes opciones:
   - Pulse **Aceptar** para continuar.
   - Pulse **Cancelar** para cerrar la ventana Suprimir búsqueda guardada.

Qué hacer a continuación

Si los criterios de búsqueda guardada estaban asociados con otros objetos de QRadar, acceda a los objetos asociados que ha anotado y edite los objetos para eliminar o sustituir la asociación con la búsqueda guardada suprimida.

Guardado de resultados de la búsqueda

Puede guardar los resultados de la búsqueda.

Acerca de esta tarea

Si realiza una búsqueda y no guarda explícitamente los resultados de la búsqueda, estos están disponibles en Gestionar ventanas de búsqueda durante 24 horas y a continuación se suprimen automáticamente.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Realice una búsqueda.
3. Pulse **Guardar resultados**.
4. En la ventana Guardar resultado de búsqueda, teclee un nombre exclusivo para los resultados de la búsqueda.
5. Pulse **Aceptar**.

Visualización de resultados de la búsqueda gestionados

Mediante la página Gestionar resultados de búsqueda, puede ver resultados de la búsqueda parciales o completos.

Acerca de esta tarea

Los resultados de la búsqueda guardados retienen configuraciones de gráfico de los criterios de búsqueda asociados, sin embargo, si el resultado de la búsqueda está basado en los criterios de búsqueda suprimidos, se visualizan los gráficos predeterminados (barras y circular).

La página Gestionar resultados de búsqueda proporciona los parámetros siguientes

Tabla 22. Parámetros de la página Gestionar resultados de búsqueda

Parámetro	Descripción
Distintivos	Indica que una notificación de correo electrónico está pendiente cuando la búsqueda esta completa.
Usuario	Especifica el nombre del usuario que inició la búsqueda.
Nombre	Especifica el nombre de la búsqueda, si la búsqueda se ha guardado. Para obtener más información acerca de cómo guardar una búsqueda, consulte Guardar resultados de búsqueda.
Se inició el	Especifica la fecha y la hora en que la búsqueda se ha iniciado.
Finalizó el	Especifica la fecha y la hora en que la búsqueda ha finalizado.
Duración	Especifique el tiempo que ha tardado la búsqueda en llevarse a cabo. Si la búsqueda está en curso, el parámetro **Duración** especifica el tiempo que la búsqueda ha estado procesándose hasta la fecha. Si la búsqueda se ha cancelado, el parámetro **Duración** especifica el periodo de tiempo que la búsqueda ha estado procesándose antes de cancelarse.

Tabla 22. Parámetros de la página Gestionar resultados de búsqueda (continuación)

Parámetro	Descripción
Caduca el	Especifica la fecha y la hora en que caducará un resultado de la búsqueda no guardado. La figura de retención de búsqueda guardada se configura en los valores del sistema. Para obtener más información sobre la configuración de valores del sistema, consulte la guía *IBM Security QRadar Log Manager Administration Guide*.
Estado	Especifica el estado de la búsqueda. Los estados son: • **En cola**: especifica que la búsqueda está en cola para empezar. • **<porcentaje>%Completado**: especifica el progreso de la búsqueda en términos de porcentaje completado. Puede pulsar el enlace para ver resultados parciales. • **Ordenando**: especifica que la búsqueda ha terminado de recopilar resultados y está actualmente preparando los resultados para su visualización. • **Cancelado**: especifica que la búsqueda se ha cancelado. Puede pulsar el enlace para ver los resultados recopilados antes de la cancelación. • **Completado**: especifica que la búsqueda se ha completado. Puede pulsar el enlace para ver los resultados. Consulte Supervisión de actividad de registro
Tamaño	Especifica el tamaño de archivo del conjunto de resultados de la búsqueda.

La barra de herramientas de la ventana Gestionar resultados de búsqueda proporciona las funciones siguientes

Tabla 23. Barra de herramientas de Gestionar resultados de búsqueda

Función	Descripción
Nueva búsqueda	Pulse **Nueva búsqueda** para crear una búsqueda nueva. Cuando pulsa este icono, se visualiza la página de búsqueda.
Guardar resultados	Pulse **Guardar resultados** para guardar los resultados de la búsqueda seleccionados. Consulte Guardar resultados de búsqueda.
Cancelar	Pulse **Cancelar** para cancelar el resultado de la búsqueda seleccionada que está en curso o en cola para iniciarse. Consulte Cancelación de una búsqueda.
Suprimir	Pulse **Suprimir** para suprimir el resultado de la búsqueda seleccionado. Consulte Suprimir un resultado de la búsqueda.

Tabla 23. Barra de herramientas de Gestionar resultados de búsqueda (continuación)

Función	Descripción
Notificar	Pulse **Notificar** para habilitar la notificación por correo electrónico una vez completada la búsqueda seleccionada.
Ver	En este cuadro de lista puede seleccionar qué resultados de la búsqueda desea lista en la página Resultados de búsqueda. Las opciones son: • Resultados de búsqueda guardada • Todos los resultados de búsqueda • Búsquedas canceladas/erróneas • Búsquedas en curso

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el menú **Buscar**, seleccione **Gestionar resultados de búsqueda**.
3. Ver la lista de los resultados de la búsqueda.

Cancelación de una búsqueda

Mientras una búsqueda está en cola o en curso, puede cancelar la búsqueda en la página Gestionar resultados de búsqueda.

Acerca de esta tarea

Si la búsqueda está en curso cuando se cancela, se mantienen los resultados que se han acumulado hasta que la cancelación.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el menú **Buscar**, seleccione **Gestionar resultados de búsqueda**.
3. Seleccione el resultado de búsqueda en cola o en curso que desea cancelar.
4. Pulse **Cancelar**.
5. Pulse **Sí**.

Supresión de una búsqueda

Si un resultado de búsqueda ya no es necesario, puede suprimir el resultado de búsqueda de la página Gestionar resultados de búsqueda.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el menú **Buscar**, seleccione **Gestionar resultados de búsqueda**.
3. Seleccione el resultado de búsqueda que desea suprimir.
4. Pulse **Suprimir**.
5. Pulse **Sí**.

Gestión de grupos de búsqueda

Utilizando la ventana Grupos de búsqueda, puede crear y gestionar grupos de búsqueda de sucesos, flujos y delitos.

Estos grupos le permiten localizar fácilmente criterios de búsqueda guardados en la pestaña **Actividad de registro** y en el asistente de informes.

Visualización de grupos de búsqueda

Está disponible un conjunto predeterminado de grupos y subgrupos.

Acerca de esta tarea

Puede ver grupos de búsqueda en la ventana Grupos de búsqueda de sucesos.

Todas las búsquedas guardadas que no se asignan a un grupo están en el grupo **Otros**.

La ventana Grupo de búsqueda de sucesos muestra los parámetros siguientes para cada grupo.

Tabla 24. Parámetros de ventanas de grupos de búsqueda

Parámetro	Descripción
Nombre	Especifica el nombre del grupo de búsqueda.
Usuario	Especifica el nombre del usuario que ha creado el grupo de búsqueda.
Descripción	Especifica la descripción del grupo de búsqueda.
Fecha de modificación	Especifica la fecha en que se ha modificado el grupo de búsqueda.

La barra de herramientas de la ventana Grupos de búsqueda de sucesos proporciona las siguientes funciones:

Tabla 25. Funciones de barra de herramientas de ventanas de grupos de búsqueda

Función	Descripción
Grupo nuevo	Para crear un nuevo grupo de búsqueda, puede pulsar **Grupo nuevo**. Consulte Creación de un grupo de búsqueda nuevo.
Editar	Para editar un grupo de búsqueda existente, puede pulsar en **Editar**. Consulte Edición de un grupo de búsqueda.
Copiar	Para copiar una búsqueda guardada en otro grupo de búsqueda, puede pulsar en **Copiar**. Consulte Copia de una búsqueda guardada en otro grupo.
Eliminar	Para eliminar un grupo de búsqueda o una búsqueda guardada de un grupo de búsqueda, seleccione el elemento que desea eliminar y luego pulse **Eliminar**. Consulte Eliminación de un grupo o una búsqueda guardada de un grupo.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. **Seleccionar búsqueda** >**Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Vea los grupos de búsqueda.

Creación de un grupo de búsqueda nuevo

Puede crear un grupo de búsqueda nuevo.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. **Seleccionar búsqueda Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Seleccione la carpeta para el grupo donde desea crear el nuevo grupo.
5. Pulse **Grupo nuevo**.
6. En el campo **Nombre**, escriba un nombre exclusivo para el nuevo grupo.
7. Opcional. En el campo **Descripción**, escriba una descripción.
8. Pulse **Aceptar**.

Edición de un grupo de búsqueda

Puede editar los campos **Nombre** y **Descripción** de un grupo de búsqueda.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Seleccione **Buscar** > **Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Seleccione el grupo que desea editar.
5. Pulse **Editar**.
6. Edite los parámetros:
   - Escriba un nombre nuevo en el campo **Nombre**.
   - Escriba una nueva descripción en el campo **Descripción**.
7. Pulse **Aceptar**.

Copia de una búsqueda guardada en otro grupo

Puede copiar una búsqueda guardada en uno o varios grupos.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Seleccione **Buscar** > **Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Seleccione la búsqueda guardada que desea copiar.
5. Pulse **Copiar**.
6. En la ventana Grupos de elementos, marque el recuadro de selección para el grupo en el que desea copiar la búsqueda guardada.
7. Pulse **Asignar grupos**.

Eliminación de un grupo o una búsqueda guardada de un grupo

Puede utilizar el icono **Eliminar** para eliminar una búsqueda de un grupo o eliminar un grupo de búsqueda.

Acerca de esta tarea

Cuando se elimina una búsqueda guardada de un grupo, la búsqueda guardada no se suprime del sistema. La búsqueda guardada se elimina del grupo y se mueve automáticamente al grupo **Otros**.

No puede eliminar Grupos de búsqueda de sucesos del sistema.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Seleccione **Buscar** > **Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Elija una de las siguientes opciones:
   - Seleccione la búsqueda guardada que desea eliminar del grupo.
   - Seleccione el grupo que desea eliminar.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Capítulo 7. Propiedades de suceso personalizadas

Las propiedades de suceso y flujo personalizadas permiten buscar, ver y crear informes de información dentro de registros que QRadar SIEM no normaliza ni visualiza normalmente.

Puede crear propiedades de suceso personalizadas de varias ubicaciones en la pestaña **Actividad de registro**:

- Detalles de suceso: puede seleccionar un suceso en la pestaña **Actividad de registro** para crear una propiedad de suceso personalizada que se deriva de su carga útil.
- Página de búsqueda: puede crear y editar un suceso o propiedad personalizados en la página Buscar. Cuando se crea una propiedad personalizada nueva en la página Buscar, la propiedad no se deriva de ningún suceso en concreto; por lo tanto, la ventana Definición de propiedad personalizada no se llena automáticamente. Puede copiar y pegar la información de carga útil de otro origen.

Permisos necesarios

Crear propiedades personalizadas si tiene el permiso correcto.

Debe tener el permiso Propiedades de suceso definidas por el usuario.

Si tiene permisos administrativos, también puede crear y modificar las propiedades personalizadas de la pestaña Admin.

Pulse **Admin** > **Orígenes de datos** > **Propiedades de sucesos personalizadas**.

Consulte con el administrador para asegurarse de que tiene los permisos correctos.

Para obtener más información, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.

Tipos de propiedad personalizada

Puede crear un tipo de propiedad personalizada.

Cuando se crea una propiedad personalizada, puede optar por crear una expresión regular o un tipo de propiedad calculado.

Utilizando las sentencias de expresión regular (Regex), puede extraer datos no normalizados de cargas útiles de suceso.

Por ejemplo, un informe se crea para informar a todos los usuarios que realizan cambios de permiso de usuario en un servidor Oracle. Se informa de una lista de usuarios y del número de veces que realizan un cambio en el permiso de otra cuenta. Sin embargo, normalmente el permiso o la cuenta de usuario real que se ha cambiado no se puede visualizar. Puede crear una propiedad personalizada para extraer esta información de los registros y, a continuación, utilizar la propiedad en las búsquedas y los informes. El uso de esta característica requiere conocimientos avanzados de expresiones regulares (regex).

La expresión regular define el campo que desea que se convierta en la propiedad personalizada. Después de entrar una sentencia de expresión regular, puede validarla para la carga útil. Cuando defina patrones de expresión regular personalizados, respete las reglas de expresión regular definidas por el lenguaje de programación Java™.

Para obtener más información, puede consultar las guías de aprendizaje de expresión regular disponibles en la web. Una propiedad personalizada puede asociarse con varias expresiones regulares.

Cuando se analiza un suceso, se prueba cada patrón de expresión regular en el suceso hasta que un patrón de expresión regular coincide con la carga útil. El primer patrón de expresión regular que coincide con la carga útil de suceso determina los datos que se deben extraer.

Utilizando propiedades personalizadas basadas en cálculo, puede realizar cálculos en propiedades de suceso numérico o flujo existentes para producir una propiedad calculada

Por ejemplo, puede crear una propiedad que visualice un porcentaje dividiendo una propiedad numérica por otra propiedad numérica.

Creación de una propiedad personalizada basada en expresión regular

Puede crear una propiedad personalizada basada en expresión regular para comparar cargas útiles de sucesos o flujos con una expresión regular.

Acerca de esta tarea

Cuando configure una propiedad personalizada basada en expresión regular, la ventana Propiedades de sucesos personalizadas proporciona parámetros. La tabla siguiente describe algunos de estos parámetros.

Tabla 26. Parámetros de ventana Propiedades de sucesos personalizadas (expresión regular)

Parámetro	Descripción
Campo de prueba	Especifica la carga útil que se ha extraído del suceso o flujo no normalizado. Especifica la carga útil que se ha extraído del suceso no normalizado.
Propiedad nueva	El nombre de propiedad nueva no puede ser el nombre de una propiedad normalizada, por ejemplo `nombre de usuario`, `IP de origen` o `IP de destino`.
Optimizar el análisis de reglas, informes y búsquedas	Analiza y almacena la propiedad la primera vez que se recibe el suceso o flujo. Al marcar el recuadro de selección, la propiedad no necesita más análisis para el informe, la búsqueda y la prueba de regla. Si se elimina la marca de este recuadro de selección, la propiedad se analiza cada vez que se aplica un informe, una búsqueda o una prueba de regla.

Tabla 26. Parámetros de ventana Propiedades de sucesos personalizadas (expresión regular) (continuación)

Parámetro	Descripción
Origen de registro	Si se asocian varios orígenes de registro con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
RegEx	La expresión regular que desea utilizar para extraer los datos de la carga útil. Las expresiones regulares son sensibles a las mayúsculas y minúsculas. A continuación, se muestran expresiones regulares de ejemplo: • Correo electrónico: `(.+@[^\.].*\.[a-z]{2,}$)` • URL: `(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)` • Nombre de dominio: `(http[s]?://(.+?)["/?:])` • Número de coma flotante: `([-+]?\d*\.?\d*$)` • Entero: `([-+]?\d*$)` • Dirección IP: `(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)` Los grupos de capturas deben estar entre paréntesis.
Grupo de capturas	Los grupos de capturas tratan varios caracteres como una sola unidad. En un grupo de capturas, los caracteres se agrupan en un conjunto de paréntesis.
Habilitado	Si quita la marca del recuadro de selección, esta propiedad personalizada no se visualiza en los filtros de búsqueda o las listas de columna y la propiedad no se analiza desde las cargas útiles.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Efectúe una doble pulsación en el suceso en el que desea basar la propiedad personalizada
4. Pulse **Extraer propiedad**.
5. En el panel **Selección de tipo de propiedad**, seleccione la opción **Basado en expresión regular**.
6. Configure los parámetros de propiedad personalizada.
7. Pulse **Probar** para probar la expresión regular en la carga útil.
8. Pulse **Guardar**.

Resultados

La propiedad personalizada se visualiza como una opción en la lista de columnas disponibles de la página de búsqueda. Para incluir una propiedad personalizada en una lista de sucesos o flujos, debe seleccionar la propiedad personalizada en la lista de columnas disponibles cuando cree una búsqueda.

Creación de una propiedad personalizada basada en el cálculo

Puede crear una propiedad de cliente basada en cálculo para comparar las cargas útiles con una expresión regular.

Acerca de esta tarea

Cuando configure una propiedad personalizada basada en cálculo, las ventanas Propiedad de suceso personalizada o Propiedad de flujo personalizada proporcionan los parámetros siguientes:

Tabla 27. Parámetros de ventana de definición de propiedad personalizada (cálculo)

Parámetro	Descripción
Definición de propiedad	
Nombre de propiedad	Escriba un nombre exclusivo para esta propiedad personalizada. El nuevo nombre de propiedad no puede ser el nombre de una propiedad normalizada, por ejemplo Nombre de usuario, IP de origen o IP de destino.
Descripción	Escriba una descripción de esta propiedad personalizada.
Definición de cálculo de propiedad	
Propiedad 1	En el recuadro de lista, seleccione la primera propiedad que desee utilizar en el cálculo. Las opciones incluyen todas las propiedades personalizadas numéricas y normalizadas numéricas. También puede especificar un valor numérico específico. En el recuadro de lista **Propiedad 1**, seleccione la opción **Definido por el usuario**. Se visualiza el parámetro **Propiedad numérica**. Escriba un valor numérico específico.
Operador	En el recuadro de lista, seleccione el operador que desea aplicar a las propiedades seleccionadas en el cálculo. Las opciones incluyen: • Sumar • Restar • Multiplicar • Dividir

Tabla 27. Parámetros de ventana de definición de propiedad personalizada (cálculo) (continuación)

Parámetro	Descripción
Propiedad 2	En el recuadro de lista, seleccione la segunda propiedad que desee utilizar en el cálculo. Las opciones incluyen todas las propiedades personalizadas numéricas y normalizadas numéricas. También puede especificar un valor numérico específico. En el recuadro de lista **Propiedad 1**, seleccione la opción **Definido por el usuario**. Se visualiza el parámetro **Propiedad numérica**. Escriba un valor numérico específico.
Habilitado	Seleccione este recuadro de selección para habilitar esta propiedad personalizada. Si quita la marca del recuadro de selección, esta propiedad personalizada no se visualiza en los filtros de búsqueda de sucesos o las listas de columna y la propiedad de suceso o flujo no se analiza en las cargas útiles.

Procedimiento

1. Elija una de las opciones siguientes: Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos o flujos en modalidad continua, pulse el icono **Pausa** para poner en pausa la modalidad continua.
3. Efectúe una doble pulsación en el suceso en el que desea basar la propiedad personalizada.
4. Pulse **Extraer propiedad**.
5. En el panel Selección de tipo de propiedad, seleccione la opción **Basado en cálculo**.
6. Configure los parámetros de propiedad personalizada.
7. Pulse **Probar** para probar la expresión regular en la carga útil.
8. Pulse **Guardar**.

Resultados

Ahora la propiedad personalizada se visualiza como una opción en la lista de columnas disponibles en la página de búsqueda. Para incluir una propiedad personalizada en una lista de sucesos o flujos, debe seleccionar la propiedad personalizada en la lista de columnas disponibles al crear una búsqueda.

Modificación de una propiedad personalizada

Puede modificar una propiedad personalizada.

Acerca de esta tarea

Puede utilizar la ventana Propiedades de sucesos personalizadas para modificar una propiedad personalizada.

Las propiedades personalizadas se describen en la tabla siguiente.

Tabla 28. Columnas de ventana de propiedades personalizadas

Columna	Descripción
Nombre de propiedad	Especifica un nombre exclusivo para esta propiedad personalizada.
Tipo	Especifica el tipo para esta propiedad personalizada.
Descripción de propiedad	Especifica una descripción para esta propiedad personalizada.
Tipo de origen de registro	Especifica el nombre del tipo de origen de registro al que se aplica esta propiedad personalizada. Esta columna sólo se visualiza en la ventana Propiedades de sucesos personalizadas.
Origen de registro	Especifica el origen de registro al que se aplica esta propiedad personalizada. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro. Esta columna sólo se visualiza en la ventana Propiedades de sucesos personalizadas.
Expresión	Especifica la expresión para esta propiedad personalizada. La expresión depende del tipo de propiedad personalizada: Para una propiedad personalizada basada en expresión regular, este parámetro especifica la expresión regular que desea utilizar para extraer los datos de la carga útil. Para una propiedad personalizada basada en cálculo, este parámetro especifica el cálculo que desea utilizar para crear el valor de propiedad personalizada.
Nombre de usuario	Especifica el nombre del usuario que ha creado esta propiedad personalizada.
Habilitado	Especifica si esta propiedad personalizada está habilitada. Este campo especifica Verdadero o Falso.
Fecha de creación	Especifica la fecha en que se ha creado esta propiedad personalizada.
Fecha de modificación	Especifica la hora en que se ha modificado por última vez esta propiedad personalizada.

La barra de herramientas Propiedades de sucesos personalizadas proporciona las funciones siguientes:

Tabla 29. Opciones de barra de herramientas de propiedades personalizadas

Opción	Descripción
Añadir	Pulse **Añadir** para añadir una nueva propiedad personalizada.
Editar	Pulse **Editar** para editar la propiedad personalizada seleccionada.
Copiar	Pulse **Copiar** para copiar propiedades personalizadas seleccionadas.
Suprimir	Pulse **Suprimir** para suprimir propiedades personalizadas seleccionadas.
Habilitar/Inhabilitar	Pulse **Habilitar/Inhabilitar** para habilitar o inhabilitar las propiedades personalizadas seleccionadas para el análisis y la visualización en los filtros de búsqueda o las listas de columna.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, seleccione **Editar búsqueda**.
3. Pulse **Gestionar propiedades personalizadas**.
4. Seleccione la propiedad personalizada que desea editar y pulse **Editar**.
5. Edite los parámetros necesarios.
6. Opcional. Si ha editado la expresión regular, pulse **Probar** para probar la expresión regular en la carga útil.
7. Pulse **Guardar**.

Copia de una propiedad personalizada

Para crear una nueva propiedad personalizada que esté basada en una propiedad personalizada existente, puede copiar la propiedad personalizada existente y, a continuación, modificar los parámetros.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, seleccione **Editar búsqueda**.
3. Pulse **Gestionar propiedades personalizadas**.
4. Seleccione la propiedad personalizada que desea copiar y pulse **Copiar**.
5. Edite los parámetros necesarios.
6. Opcional. Si ha editado la expresión regular, pulse **Probar** para probar la expresión regular en la carga útil.
7. Pulse **Guardar**.

Supresión de una propiedad personalizada

Puede suprimir cualquier propiedad personalizada, a condición que la propiedad personalizada no esté asociada con otra propiedad personalizada.

Procedimiento

1. En el recuadro de lista **Buscar**, seleccione **Editar búsqueda**.
2. Pulse **Gestionar propiedades personalizadas**.
3. Seleccione la propiedad personalizada que desea suprimir y pulse **Suprimir**.
4. Pulse **Sí**.

Capítulo 8. Gestión de reglas

En la pestaña **Actividad de registro** puede ver y mantener reglas.

Este tema se aplica a los usuarios que tienen permisos de rol de usuario **Ver reglas personalizadas** o **Mantener reglas personalizadas**.

Consideraciones sobre el permiso de regla

Puede ver y gestionar reglas para las áreas de la red a la que puede acceder si tiene los permisos de rol de usuario Ver reglas personalizadas y Mantener reglas personalizadas.

Para crear reglas de detección de anomalía, debe tener el permiso **Mantener reglas personalizadas** adecuado para la pestaña en la que desea crear la regla. Por ejemplo, para poder crear una regla de detección de anomalía en la pestaña Actividad de registro, debe tener el permiso **Actividad de registro** > **Mantener reglas personalizadas**.

Para obtener más información sobre los permisos de rol de usuario, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.

Visión general de las reglas

Las reglas realizan pruebas sobre sucesos y si se cumplen todas las condiciones de una prueba, la regla genera una respuesta.

Las pruebas de una regla pueden también hacer referencia a otros componentes y reglas. No es necesario crear las reglas en un orden determinado, pues el sistema comprueba si existen dependencias cada vez que se añade, edita o suprime una regla. Si se intenta suprimir o inhabilitar una regla a la que hace referencia otra regla, se muestra un aviso y no se emprende ninguna acción.

Para obtener una lista completa de reglas, consulte la *Guía de administración de IBM Security QRadar SIEM*.

Regla de suceso

Una regla de suceso realiza pruebas en los sucesos a medida que el Procesador de sucesos los procesan en tiempo real.

Puede crear una regla de suceso para detectar un solo suceso dentro de ciertas secuencias de sucesos o propiedades. Por ejemplo si desea supervisar la red en busca de intentos de inicio de sesión no satisfactorios, acceso a varios hosts o un suceso de reconocimiento seguido de una explotación, puede crear una regla de suceso. Es habitual que las reglas de suceso creen delitos como respuesta.

Condiciones de regla

Cada regla puede contener funciones, componentes básicos o pruebas.

Con las funciones, puede utilizar bloques componentes básicos y otras reglas para crear una función de varios sucesos. Puede conectar reglas utilizando funciones

que soportan operadores booleanos, por ejemplo OR y AND. Por ejemplo, si desea conectar reglas de suceso, puede utilizar la función cuando un suceso coincide con alguna | todas las reglas siguientes.

Un componente básico es una regla sin una respuesta y se utiliza como una variable común en varias reglas o crear reglas complejas o lógica que desea utilizar en otras reglas. Puede guardar un grupo de pruebas como componentes básicos para utilizarlas con otras funciones. Los componentes básicos le permitirán reutilizar pruebas de regla específicas en otras reglas. Por ejemplo, puede guardar un componente básico que incluye las direcciones IP de todos los servidores de correo en la red y, a continuación, utilizar ese componente básico para excluir esos servidores de correo de otra regla. Los componentes básicos predeterminados se proporcionan como directrices, que deben revisarse y editarse en función de las necesidades de la red.

Nota: De forma predeterminada, los componentes básicos no se cargan. Defina una regla para crear componentes básicos.

Puede ejecutar pruebas en la propiedad de un suceso como dirección IP de origen o gravedad de suceso.

Reglas específicas de dominio

Si una regla tiene una prueba de dominio, puede restringir esa regla para que se aplique solo a los sucesos que están ocurriendo dentro de un dominio especificado. Un suceso que tiene una etiqueta de dominio diferente del dominio establecido en la regla no desencadena una respuesta de suceso.

Para crear una regla que prueba condiciones sobre cosas que están pasando en todo el sistema, establezca la condición de dominio en **Cualquier dominio**.

Respuestas de regla

Cuando se cumplen las condiciones de regla, una regla puede generar una o más respuestas.

Las reglas pueden generar una o varias de las respuestas siguientes:

- Crear un delito.
- Enviar un correo electrónico.
- Generar notificaciones de sistema en la característica de panel de control.
- Añadir datos a conjuntos de referencia.
- Añadir datos a colecciones de datos de referencia.
- Generar una respuesta a un sistema externo.
- Añadir datos a recopilaciones de datos de referencia que se pueden utilizar en pruebas de regla.

Tipos de recopilación de datos de referencia

Antes de poder configurar una respuesta de regla para enviar datos a una recopilación de datos de referencia, debe crear la recopilación de datos de referencia utilizando la interfaz de línea de mandatos (CLI). QRadar soporta los siguientes tipos de recopilación de datos:

Conjunto de referencia
Un conjunto de elementos, por ejemplo una lista de direcciones IP o nombres de usuario, que se derivan de los sucesos y flujos que se producen en la red.

Correlación de referencia
Los datos se almacenan en registros que correlacionan una clave con un valor. Por ejemplo, para correlacionar la actividad de usuario en la red, puede crear una correlación de referencia que utiliza el parámetro **Nombre de usuario** como clave y el **ID global** del usuario como valor.

Correlación de referencia de conjuntos
Los datos se almacenan en registros que correlacionan una clave con varios valores. Por ejemplo, para probar el acceso autorizado a una patente, utilice una propiedad de suceso personalizada para **ID de patente** como clave y el parámetro **Nombre de usuario** como valor. Utilice una correlación de conjuntos para llenar una lista de usuarios autorizados.

Correlación de referencia de correlaciones
Los datos se almacenan en registros que correlacionan una clave a otra clave, que a continuación se correlaciona con un valor único. Por ejemplo, para probar las violaciones de ancho de banda de red, puede crear una correlación de correlaciones. Utilice el parámetro **IP de origen** como la primera clave, el parámetro **Aplicación** como segunda clave y el parámetro **Bytes totales** como valor.

Tabla de referencia
En una tabla de referencia, los datos se almacenan en una tabla que correlaciona una clave con otra clave, que a continuación se correlaciona con un valor único. La segunda clave tiene un tipo asignado. Esta correlación es similar a una tabla de base de datos donde cada columna de la tabla está asociada con un tipo. Por ejemplo, puede crear una tabla de referencia que almacena el parámetro **Nombre de usuario** como primera clave y tiene varias claves secundarias que tienen un tipo asignado definido por el usuario como **Tipo de IP** con el parámetro **IP de origen** o **Puerto de origen** como valor. Puede configurar una respuesta de regla para añadir una o más claves definidas en la tabla. También puede añadir valores personalizados a la respuesta de regla. El valor personalizado debe ser válido para el tipo de la clave secundaria.

Nota: Para obtener información sobre los conjuntos de referencia y las recopilaciones de datos de referencia, consulte la *Guía de administración* correspondiente al producto.

Visualización de reglas

Puede ver los detalles de una regla, incluyendo las pruebas, los componentes básicos y las respuestas.

Antes de empezar

En función de los permisos de rol de usuario, puede acceder a la página de reglas de la pestaña **Actividad de registro**. Para obtener más información sobre los permisos de rol de usuario, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.

Acerca de esta tarea

La página Reglas muestra una lista de reglas con los parámetros asociados. Para localizar la regla que desea abrir y cuyos detalles desea ver, puede utilizar el recuadro de lista Grupo o el campo **Buscar en reglas** en la barra de herramientas.

Procedimiento

1. Pulse la pestaña **Actividad de registro** y, a continuación, seleccione **Reglas** en el recuadro de lista **Reglas** de la barra de herramientas.
2. En el recuadro de lista **Visualizar**, seleccione **Reglas**.
3. Efectúe una doble pulsación en la regla que desea ver.
4. Revise los detalles de regla.

Resultados

Si tiene el permiso **Ver reglas personalizadas**, pero no tiene el permiso **Mantener reglas personalizadas**, se visualiza la página **Resumen de regla** y la regla no se puede editar. Si tiene el permiso **Mantener reglas personalizadas**, se visualiza la página **Editor de pila de prueba de regla**. Puede revisar y editar los detalles de regla.

Creación de una regla personalizada

Puede crear reglas nuevas para satisfacer las necesidades del despliegue.

Acerca de esta tarea

Para crear una regla nueva, debe tener el permiso **Delitos** > **Mantener reglas personalizadas**.

Pruebe probar las reglas de forma local o global. Una prueba local significa que la regla se prueba en el procesador de sucesos local y no se comparte con el sistema. Una prueba global significa que cualquier procesador de sucesos del sistema comparte y prueba la regla. Las reglas globales envían sucesos y flujos al procesador de sucesos central, lo que puede disminuir el rendimiento en el procesador de sucesos central.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. En el recuadro de lista **Acciones**, seleccione **Nueva regla de sucesos**.
4. Lea el texto de introducción del asistente de reglas. Pulse **Siguiente**.
5. Pulse **Siguiente** para ver la página Editor de pila de prueba de regla.
6. En el campo **especifique aquí el nombre de la regla** en el panel Regla, escriba un nombre exclusivo que desee asignar a esta regla.
7. En el recuadro de lista, seleccione **Local** o **Global**.
8. Añada uno o más pruebas a una regla:
   a. Opcional. Para filtrar las opciones en el recuadro de lista **Grupo de pruebas**, escriba el texto por el que desea filtrar en el campo Tipo por filtrar.
   b. En el recuadro de lista **Grupo de pruebas**, seleccione el tipo de prueba que desea añadir a esta regla.

c. Para cada prueba que desee añadir a la regla, seleccione el signo más (+) junto a la prueba.
d. Opcional. Para identificar una prueba como prueba excluida, pulse **and** al principio de la prueba en el panel Regla. **and** se visualiza como **and not**.
e. Pulse los parámetros configurables subrayados para personalizar las variables de la prueba.
f. En el recuadro de diálogo, seleccione valores para la variable y, a continuación, pulse **Enviar**.

9. Para exportar la regla configurada como un componente básico para utilizarlo con otras reglas:
   a. Pulse **Exportar como componente básico**.
   b. Escriba un nombre exclusivo para este componente básico.
   c. Pulse **Guardar**.
10. En el panel Grupos, seleccione los recuadros de selección de los grupos a los que desea asignar esta regla.
11. En el campo **Notas**, escriba una nota que desea incluir para esta regla. Pulse **Siguiente**.
12. En la página Respuestas de regla, configure las respuestas que desea que genere esta regla.
13. Pulse **Siguiente**.
14. Revise la página Resumen de regla para asegurarse de que los valores son correctos. Realice los cambios si es necesario y, a continuación, pulse **Finalizar**.

Creación de una regla de detección de anomalías

Utilice el asistente de Regla de detección de anomalías para crear reglas que apliquen criterios de rango de tiempo utilizando pruebas de datos y hora.

Antes de empezar

Para crear una regla de detección de anomalías nueva, debe cumplir con los siguientes requisitos:

- Tener el permiso para Mantener reglas personalizadas.
- Realizar una búsqueda agrupada.

Las opciones de detección de anomalías se visualizan después de realizar una búsqueda agrupada y guardar los criterios de búsqueda.

Acerca de esta tarea

Debe tener el permiso de rol apropiado para poder crear una regla de detección de anomalías.

Para crear reglas de detección de anomalías en la pestaña **Actividad de registro**, debe tener el permiso de rol de **Actividad de registro Mantener reglas personalizadas**.

Para crear reglas de detección de anomalías en la pestaña **Actividad de red**, debe tener el permiso de rol de **Red Mantener reglas personalizadas**.

Las reglas de detección de anomalías utilizan todos los criterios de agrupación y filtro de los criterios de búsqueda guardados en los que se basa la regla, pero no utilizan rangos de tiempo de los criterios de búsqueda.

Cuando se crea una regla de detección de anomalías, la regla se rellena con una pila de prueba predeterminada. Puede editar las pruebas predeterminadas o añadir pruebas a la pila de prueba. Al menos se debe incluir una prueba de Propiedad acumulada en la pila de prueba.

De forma predeterminada, la opción **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado** está seleccionada en la página Editor de pila de prueba de regla.

Esto hace que una regla de detección de anomalías pruebe la propiedad acumulada seleccionada para cada grupo de sucesos por separado. Por ejemplo, si el valor acumulado seleccionado es **UniqueCount(sourceIP)**, la regla prueba cada dirección IP de origen exclusiva para cada grupo de sucesos.

Esta opción **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado** es dinámica. El valor **[Propiedad acumulada seleccionada]** depende de la opción que seleccione para el campo **esta prueba de propiedad acumulada** de la pila de prueba predeterminada. El valor **[grupo]** depende de las opciones de agrupación que se han especificado en los criterios de búsqueda guardados. Si se incluyen varias opciones de agrupación, es posible que el texto se trunque. Mueva el puntero del ratón sobre el texto para ver todos los grupos.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Realice una búsqueda.
3. En el menú **Reglas**, seleccione el tipo de regla que desea crear. Las opciones incluyen:
   - Añadir regla de anomalía
   - Añadir regla de umbral
   - Añadir regla conductual
4. Lea el texto de introducción del asistente de reglas. Pulse **Siguiente**. Se selecciona la regla que ha elegido anteriormente.
5. Pulse **Siguiente** para ver la página Editor de pila de prueba de regla.
6. En el campo **especifique aquí el nombre de la regla**, escriba un nombre exclusivo que desee asignar a esta regla.
7. Para añadir una prueba a una regla:
   a. Opcional. Para filtrar las opciones en el recuadro de lista Grupo de pruebas, escriba el texto por el que desea filtrar en el campo Tipo por filtrar.
   b. En el recuadro de lista Grupo de pruebas, seleccione el tipo de prueba que desea añadir a esta regla.
   c. Para cada prueba que desee añadir a la regla, seleccione el signo + junto a la prueba.
   d. Opcional. Para identificar una prueba como prueba excluida, pulse "and" al principio de la prueba en el panel Regla. "and" se visualiza como "and not".
   e. Pulse los parámetros configurables subrayados para personalizar las variables de la prueba.

f. En el recuadro de diálogo, seleccione valores para la variable y, a continuación, pulse **Enviar**.

8. Opcional. Para probar las propiedades acumuladas seleccionadas totales para cada grupo de sucesos o flujos, borre la marca del recuadro de selección **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado**.
9. En el panel Grupos, seleccione los recuadros de selección de los grupos a los que desea asignar esta regla. Para obtener más información, consulte Gestión de grupos de reglas.
10. En el campo **Notas**, escriba las notas que desea incluir para esta regla. Pulse **Siguiente**.
11. En la página Respuestas de regla, configure las respuestas que desea que genere esta regla. "Parámetros de página Rule Response" en la página 100
12. Pulse **Siguiente**.
13. Revise la regla configurada. Pulse **Finalizar**.

Tareas de gestión de reglas

Puede gestionar reglas personalizadas y de anomalía.

Puede habilitar e inhabilitar reglas, según sea necesario. También puede editar, copiar o suprimir una regla.

Solo puede crear reglas de detección de anomalías en la pestaña **Actividad de registro**.

Habilitación e inhabilitación de reglas

Al ajustar el sistema, puede habilitar o inhabilitar las reglas adecuadas para asegurarse de que el sistema genera delitos significativos para el entorno.

Acerca de esta tarea

Debe tener el permiso de rol **Actividad de registro** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. En el recuadro de lista **Visualizar** de la página **Reglas**, seleccione **Reglas**.
4. Seleccione la regla que desea habilitar o inhabilitar.
5. En el recuadro de lista **Acciones**, seleccione **Habilitar/Inhabilitar**.

Edición de una regla

Puede editar una regla para cambiar el nombre de regla, el tipo de regla, las pruebas o las respuestas.

Acerca de esta tarea

Debe tener el permiso de rol **Actividad de registro** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. En el recuadro de lista **Visualizar** de la página **Reglas**, seleccione **Reglas**.
4. Efectúe una doble pulsación en la regla que desea editar.
5. En el recuadro de lista **Acciones**, seleccione **Abrir**.
6. Opcional. Si desea cambiar el tipo de regla, pulse **Anterior** y seleccione un nuevo tipo de regla.
7. En la página Editor de pila de prueba de regla, edite los parámetros.
8. Pulse **Siguiente**.
9. En la página Respuesta de regla, edite los parámetros.
10. Pulse **Siguiente**.
11. Revise la regla editada. Pulse **Finalizar**.

Copia de una regla

Puede copiar una regla existente, entrar un nombre nuevo para la regla y, a continuación, personalizar los parámetros en la nueva regla según sea necesario.

Acerca de esta tarea

Debe tener el permiso de rol **Actividad de registro** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. En el recuadro de lista **Visualizar**, seleccione **Reglas**.
4. Seleccione la regla que desea duplicar.
5. En el recuadro de lista **Acciones**, seleccione **Duplicar**.
6. En el campo Escriba un nombre para la regla copiada:, escriba un nombre para la regla nueva. Pulse **Aceptar**.

Supresión de una regla

Puede suprimir una regla del sistema.

Acerca de esta tarea

Debe tener el permiso de rol **Actividad de registro** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. En el recuadro de lista **Visualizar**, seleccione **Reglas**.
4. Seleccione la regla que desea suprimir.
5. En el recuadro de lista **Acciones**, seleccione **Suprimir**.

Gestión de grupo de reglas

Si el usuario es administrador, puede crear, editar y suprimir grupos de reglas. La categorización de reglas y componentes básicos en grupos le permite ver las reglas y realizar su seguimiento de forma eficiente.

Por ejemplo, puede ver todas las reglas que están relacionados con la conformidad.

Al crear nuevas reglas, puede asignar la regla a un grupo existente. Para obtener información sobre la asignación de un grupo utilizando el asistente de reglas, consulte Creación de una regla personalizada o Creación de una regla de detección de anomalías.

Visualización de un grupo de reglas

En la página Reglas, puede filtrar las reglas o componentes básicos para ver sólo las reglas o componentes básicos que pertenecen a un grupo específico.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. En el recuadro de lista **Visualizar**, seleccione si desea ver reglas o componentes básicos.
4. En el recuadro de lista **Filtro**, seleccione la categoría de grupo que desea ver.

Creación de un grupo

Aunque la página Reglas proporciona grupos de reglas predeterminados, puede crear un grupo nuevo.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. Pulse **Grupos**.
4. En el árbol de navegación, seleccione el grupo bajo el que desea crear un grupo nuevo.
5. Pulse **Grupo nuevo**.
6. Escriba valores para los parámetros siguientes:
   - **Nombre**: Escriba un nombre exclusivo para asignarlo al nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Escriba una descripción que desee asignar a este grupo. La descripción puede tener un máximo 255 caracteres de longitud.
7. Pulse **Aceptar**.
8. Opcional. Para cambiar la ubicación del grupo nuevo, pulse el nuevo grupo y arrastre la carpeta a la nueva ubicación en el árbol de navegación.

Asignación de un elemento a un grupo

Puede asignar una regla o un componente básico seleccionados a un grupo.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.

3. Seleccione la regla o el componente básico que desea asignar a un grupo.
4. En el recuadro de lista **Acciones**, seleccione **Asignar grupos**.
5. Seleccione el grupo al que desea asignar la regla o el componente básico.
6. Pulse **Asignar grupos**.
7. Cierre la ventana **Elegir grupo**.

Edición de un grupo

Puede editar un grupo para cambiar el nombre o la descripción.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. Pulse **Grupos**.
4. En el árbol de navegación, seleccione el grupo que desea editar.
5. Pulse **Editar**.
6. Actualice los valores para los parámetros siguientes:
   - **Nombre**: Escriba un nombre exclusivo para asignarlo al nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Escriba una descripción que desee asignar a este grupo. La descripción puede tener un máximo 255 caracteres de longitud.
7. Pulse **Aceptar**.
8. Opcional. Para cambiar la ubicación del grupo, pulse el nuevo grupo y arrastre la carpeta a la nueva ubicación en el árbol de navegación.

Copia de un elemento en otro grupo

Puede copiar una regla o un componente básico de un grupo a otros grupos.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. Pulse **Grupos**.
4. En el árbol de navegación, seleccione la regla o el componente básico que desea copiar en otro grupo.
5. Pulse **Copiar**.
6. Marque el recuadro de selección para el grupo en el que desea copiar la regla o el componente básico.
7. Pulse **Copiar**.

Supresión de un elemento de un grupo

Puede suprimir un elemento de un grupo. Cuando suprime un elemento de un grupo, la regla o el componente básico sólo se suprime del grupo; sigue estando disponible en la página Reglas.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. Pulse **Grupos**.

4. Utilizando el árbol de navegación, vaya al elemento que desea suprimir y selecciónelo.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Supresión de un grupo

Puede suprimir un grupo. Cuando se suprime un grupo, las reglas o los componentes básicos de ese grupo permanecen disponibles en la página Reglas.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. Pulse **Grupos**.
4. Utilizando el árbol de navegación, vaya al grupo que desea suprimir y selecciónelo.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Edición de componentes básicos

Puede editar cualquiera de los componentes básicos predeterminados para que coincidan con las necesidades del despliegue.

Acerca de esta tarea

Un componente básico es una pila de prueba de regla reutilizable que puede incluir como componente en otras reglas.

Por ejemplo, puede editar el componente básico BB:HostDefinition: Servidores de correo para identificar todos los servidores de correo del despliegue. A continuación, puede configurar cualquier regla para excluir los servidores de correo de las pruebas de regla.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas**.
3. En el recuadro de lista **Visualiza**, seleccione **Componentes básicos**.
4. Efectúe una doble pulsación en el componente básico que desea editar.
5. Actualice el componente básico, como sea necesario.
6. Pulse **Siguiente**.
7. Continúe con el asistente. Para obtener más información, consulte Creación de una regla personalizada.
8. Pulse **Finalizar**.

Parámetros de página Reglas

Descripción de los parámetros de la página Reglas.

La lista de reglas desplegadas proporciona la siguiente información para cada regla:

Tabla 30. Parámetros de página Reglas

Parámetro	Descripción
Nombre de regla	Visualiza el nombre de la regla.
Grupo	Visualiza el grupo al que está asignada esta regla. Para obtener más información sobre grupos, consulte Gestión de grupo de reglas.
Categoría de reglas	Visualiza la categoría de la regla. Las opciones incluyen Regla personalizada y Regla de detección de anomalías.
Tipo de regla	Visualiza el tipo de regla.
Habilitado	Indica si la regla está habilitada o inhabilitada. Para obtener más información sobre cómo habilitar e inhabilitar reglas, consulte Habilitación e inhabilitación de reglas.
Respuesta	Visualiza la respuesta de regla, si existe. Las respuestas de regla incluyen: • Asignar suceso nuevo • Correo electrónico • Notificación de registro • SNMP • Conjunto de referencia • Datos de referencia • Respuesta de IF-MAP Para obtener más información sobre las respuestas de regla, consulte Respuestas de regla.
Recuento de sucesos	Visualiza el número de sucesos que están asociados a esta regla cuando la regla contribuye a un delito.
Origen	Visualiza si esta regla es una regla predeterminada (Sistema) o una regla personalizada (Usuario).
Fecha de creación	Especifica la fecha y hora en que se ha creado esta regla.
Fecha de modificación	Especifica la fecha y hora en que se ha modificado esta regla.

Barra de herramientas de página Reglas

Utilice barra de herramientas de la página Reglas para visualizar reglas, componentes básicos o grupos. Puede gestionar grupos de reglas y trabajar con reglas.

La barra de herramientas de página Reglas proporciona las funciones siguientes:

Tabla 31. Función de barra de herramientas de página Reglas

Función	Descripción
Visualizar	En el recuadro de lista, seleccione si desea visualizar reglas o componentes básicos en la lista de reglas.
Grupo	En el recuadro de lista, seleccione qué grupo de reglas desea que se visualice en la lista de reglas.
Grupos	Pulse **Grupos** para gestionar grupos de reglas.
Acciones	Pulse **Acciones** y seleccione una de las opciones siguientes: • **Nueva regla de sucesos**: Seleccione esta opción para crear una regla de suceso nueva. • **Habilitar/Inhabilitar**: Seleccione esta opción para habilitar o inhabilitar reglas seleccionadas. • **Duplicar**: Seleccione esta opción para copiar una regla seleccionada. • **Editar**: Seleccione esta opción para editar una regla seleccionada. • **Suprimir**: Seleccione esta opción para suprimir una regla seleccionada. • **Asignar grupos**: Seleccione esta opción para asignar reglas seleccionadas a grupos de reglas.
Revertir regla	Pulse **Revertir regla** para revertir una regla de sistema modificada al valor predeterminado. Al pulsar **Revertir regla**, se visualiza una ventana de confirmación. Al revertir una regla, las modificaciones anteriores se eliminan de forma permanente. Para revertir la regla y mantener una versión modificada, duplique la regla y utilice la opción **Revertir regla** en la regla modificada.

Tabla 31. Función de barra de herramientas de página Reglas (continuación)

Función	Descripción
Buscar en reglas	Escriba los criterios de búsqueda en el campo **Buscar en reglas** y pulse el icono **Buscar en reglas** o pulse Intro en el teclado. Todas las reglas que coinciden con los criterios de búsqueda se muestran en la lista de reglas. En los parámetros siguientes se busca una coincidencia con los criterios de búsqueda: • Nombre de regla • Regla (descripción) • Notas • Respuesta La característica Buscar en reglas intenta localizar una coincidencia de serie de texto directa. Si no se encuentra ninguna coincidencia, la característica Buscar en reglas intenta una coincidencia de expresión regular (regex).

Parámetros de página Rule Response

Existen parámetros para la página Rule Response.

La tabla siguiente proporciona los parámetros de la página Rule Response.

Tabla 32. Parámetros de página Respuesta de regla de suceso, flujo, común

Parámetro	Descripción
Gravedad	Marque este recuadro de selección si desea que esta regla establezca o ajuste la gravedad. Cuando se ha seleccionado, puede utilizar los recuadros de lista para configurar el nivel de gravedad apropiado.
Credibilidad	Marque este recuadro de selección si desea que esta regla establezca o ajuste lar credibilidad. Cuando se ha seleccionado, puede utilizar los recuadros de lista para configurar el nivel de credibilidad apropiado.
Pertinencia	Marque este recuadro de selección si desea que esta regla establezca o ajuste la pertinencia. Cuando se ha seleccionado, puede utilizar los recuadros de lista para configurar el nivel de pertinencia apropiado.
Anotar suceso	Marque este recuadro de selección si desea añadir una anotación a este suceso y escriba la anotación que desea añadir al suceso.
Descartar el suceso detectado	Marque este recuadro de selección para forzar que un suceso, que normalmente se envía al componente Magistrado, se envíe a la base de datos de Ariel para la creación de informes o la realización de búsquedas.

Tabla 32. Parámetros de página Respuesta de regla de suceso, flujo, común (continuación)

Parámetro	Descripción
Asignar suceso nuevo	Marque este recuadro de selección para asignar un suceso nuevo además del suceso original, que se procesa igual que todos los demás sucesos del sistema. Los parámetros **Asignar suceso nuevo** se visualizan cuando se marca este recuadro de selección. De forma predeterminada, el recuadro de selección no está marcado.
Nombre de suceso	Escriba un nombre exclusivo para el suceso que desea que se visualice en la pestaña **Actividad de registro**.
Descripción del suceso	Escriba una descripción para el suceso. La descripción se visualiza en el panel Anotaciones de los detalles de suceso.
Gravedad	En el recuadro de lista, seleccione la gravedad para el suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 0. La gravedad se visualiza en el panel Anotación de los detalles de suceso.
Credibilidad	En el recuadro de lista, seleccione la credibilidad del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 10. La credibilidad se visualiza en el panel Anotación de los detalles de suceso.
Pertinencia	En el recuadro de lista, seleccione la pertinencia del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 10. La pertinencia se visualiza en el panel Anotación de los detalles de suceso.
Categoría de alto nivel	En el recuadro de lista, seleccione la categoría de sucesos de alto nivel que desea que esta regla utilice al procesar sucesos.
Categoría de bajo nivel	En el recuadro de lista, seleccione la categoría de sucesos de bajo nivel que desea que esta regla utilice al procesar sucesos.
Correo electrónico	Seleccione este recuadro de selección para visualizar las opciones de correo electrónico. **Nota:** Para cambiar el valor **Entorno local del correo electrónico**, seleccione **Valores del sistema** en la pestaña **Admin**.
Especifique las direcciones de correo electrónico que se deben notificar:	Escriba la dirección de correo electrónico a la que hay que enviar una notificación si se genera esta regla. Utilice una coma para separar varias direcciones de correo electrónico.
Condición de excepción de SNMP	Este parámetro sólo se visualiza cuando los parámetros Valores de SNMP se han configurado en los valores del sistema. Marque este recuadro de selección para permitir que esta regla envíe una notificación de SNMP (condición de excepción). La salida de condición de excepción SNMP incluye la hora del sistema, el OID de condición de excepción y los datos de notificación, como los define el MIB.

Tabla 32. Parámetros de página Respuesta de regla de suceso, flujo, común (continuación)

Parámetro	Descripción
Enviar a SysLog Local	Marque este recuadro de selección si desea registrar el suceso localmente. De forma predeterminada, este recuadro de selección no está marcado. **Nota:** Sólo los sucesos normalizados se pueden registrar localmente en un dispositivo. Si desea enviar datos de sucesos en bruto, debe utilizar la opción Enviar a destinos de reenvío para enviar los datos a un host de syslog remoto.
Enviar a destinos de reenvío	Este recuadro de selección sólo se visualiza para las reglas de suceso. Marque este recuadro de selección si desea registrar el suceso o flujo en un destino de reenvío. Un destino de reenvío es un sistema de proveedor, por ejemplo SIEM, tíquets o sistemas de alerta. Al marcar este recuadro de selección, se visualiza una lista de destinos de reenvío. Marque este recuadro de selección para el destino de reenvío al que desea enviar este suceso o flujo. Para añadir, editar o suprimir un destino de reenvío, pulse el enlace **Gestionar destinos**.
Notificar	Marque este recuadro de selección si desea que, los sucesos que se generan como resultado de esta regla se visualicen en el elemento Notificaciones del sistema en la pestaña Panel de control. Si habilita las notificaciones, configure el parámetro **Limitador de respuestas**.
Añadir a un conjunto de referencia	Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta regla añadan datos a un conjunto de referencia. Para añadir datos a un conjunto de referencia: 1. En el primer recuadro de lista, seleccione los datos que desea añadir. Las opciones incluyen todos los datos normalizados o personalizados. 2. En el segundo recuadro de lista, seleccione la referencia que está establecida en la que desea añadir los datos especificados. La respuesta de la regla **Añadir a un conjunto de referencia** proporciona las funciones siguientes: **Renovar** Pulse **Renovar** para renovar el primer recuadro de lista para asegurarse de que la lista es actual. **Configurar conjuntos de referencia** Pulse **Configurar conjuntos de referencia** para configurar el conjunto de referencia. Esta opción sólo está disponible si tiene permisos administrativos.

Tabla 32. Parámetros de página Respuesta de regla de suceso, flujo, común (continuación)

Parámetro	Descripción
Añadir a datos de referencia	Antes de poder utilizar esta respuesta de regla, debe crear la recopilación de datos de referencia utilizando la interfaz de línea de mandatos (CLI). Para obtener más información sobre cómo crear y utilizar recopilaciones de datos de referencia, consulte la *Guía de administración* correspondiente al producto. Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta regla se añadan a una recopilación de datos de referencia. Después de marcar el recuadro de selección, seleccione una de las opciones siguientes: **Añadir a una correlación de referencia** Seleccione esta opción para enviar datos a una recopilación de pares de clave única/múltiples valores. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccione la correlación de referencia a la que desea añadir el registro de datos. **Añadir a una correlación de referencia de conjuntos** Seleccione esta opción para enviar datos a una recopilación de pares de clave/valor único. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccionar la correlación de referencia de conjuntos a los que desea añadir el registro de datos. **Añadir a una correlación de referencia de correlaciones** Seleccione esta opción para enviar datos a una recopilación de pares de varias claves/valor único. Debe seleccionar una clave para la primera correlación, una clave para la segunda correlación y, a continuación, el valor para el registro de datos. También debe seleccionar la correlación de referencia de correlaciones a la que desea añadir el registro de datos. **Añadir a una tabla de referencia** Seleccione esta opción para enviar datos a una recopilación de pares de múltiples claves/valor único, donde se ha asignado un tipo a las claves secundarios. Seleccione la tabla de referencia a la que desea añadir datos y, a continuación, seleccione una clave primaria. Seleccione las claves internas (claves secundarias) y sus valores para los registros de datos.
Publicar en el servidor IF-MAP	Si los parámetros IF-MAP están configurados y desplegados en los valores del sistema, seleccione esta opción para publicar la información de suceso sobre el servidor IF-MAP.
Limitador de respuestas	Marque este recuadro de selección y utilice los recuadros de lista para configurar la frecuencia con la que desea que responda esta regla.
Habilitar regla	Marque este recuadro de selección para habilitar esta regla.

Una notificación SNMP puede tener el aspecto siguiente:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

Una salida de syslog puede tener este aspecto:

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

Capítulo 9. Integración de canal de información de IBM Security X-Force Threat Intelligence

El canal de información de IBM Security X-Force Threat Intelligence proporciona una lista en tiempo real de direcciones IP potencialmente maliciosas. Utilice estas direcciones IP con IBM QRadar Security Intelligence Platform para identificar actividad sospechosa en el entorno.

Debe tener una suscripción al canal de información de X-Force Threat Intelligence para utilizarla con QRadar.

Al contenido del canal de información de X-Force se le da una puntuación de amenaza relativa. Los usuarios de QRadar pueden utilizar esta puntuación de amenaza para priorizar los incidentes y delitos que se generan mediante este contenido. Los datos de estos orígenes de inteligencia se incorporan automáticamente en las funciones de correlación y análisis de QRadar y enriquecen las capacidades de detección de amenazas con datos de amenaza de Internet de última hora. Los datos de actividad de red o de suceso de seguridad que impliquen estas direcciones se señalan automáticamente y, por consiguiente, añaden contexto valiosos a las investigaciones y los análisis de incidentes de seguridad

Para priorizar la amenaza e identificar los incidentes de seguridad que requieren más análisis, puede elegir qué canales de información de X-Force se deben incorporar en las reglas, los delitos y los sucesos de QRadar. Por ejemplo, puede utilizar los canales de información para identificar estos tipos de incidentes:

- Una serie de inicios de sesión intentados para un rango dinámico de direcciones IP
- Una conexión proxy anónima a un portal de business partner
- Una conexión entre un punto final interno y un mandato y control de botnet conocido
- Comunicación entre un punto final y un sitio distribución de programas maliciosos conocido

El canal de información de X-Force Threat Intelligence categoriza las direcciones IP y, a continuación, crea una clasificación de confianza que se utiliza para evaluar la amenaza. Las direcciones IP se agrupan en las categorías siguientes:

- Hosts de programas maliciosos
- Orígenes de SPAM
- Direcciones IP dinámicas
- Proxies anónimos
- Mandato y control de Botnet

El canal de información de X-Force Threat Intelligence también categoriza direcciones URL. Por ejemplo, las direcciones URL pueden categorizarse como sitios de citas, apuestas o pornografía. Para ver la lista completa de categorías para la clasificación de URL, consulte el sitio web de X-Force (www.xforce-security.com).

Antes de poder utilizar reglas basadas en URL, debe crear una propiedad de suceso personalizada para extraer el URL de la carga útil. La propiedad

personalizada de URL ya está definida para sucesos de diversos orígenes como orígenes de registro de Blue Coat SG y Juniper Networks Secure Access.

Reglas de X-Force mejoradas

Después de añadir el canal de información de X-Force Threat Intelligence a IBM QRadar Security Intelligence Platform, puede recibir inmediatamente datos de amenaza avanzados.

Las reglas siguientes forman parte del grupo de **Reglas de X-Force mejoradas**. Se pueden utilizar tal cual o se pueden personalizar.

Estas reglas están basadas en IP:

X-Force Premium: Conexión interna a posible host de programa malicioso
Esta comunicación indica una fuerte posibilidad de que se haya realizado un intento de infectar el sistema cliente o de que se haya descargado un programa malicioso.

X-Force Premium: Hosts internos comunicándose con proxies anónimos
Los *proxies anónimos* son direcciones que son conocidas por enmascarar la identidad. Las utilizan con frecuencia los programas maliciosos o se utilizan durante las amenazas persistentes avanzadas de ocultar el origen de las comunicaciones con los orígenes externos. Estas direcciones pueden estar relacionadas con actividades tales como la comunicación de programas maliciosos o la exfiltración de datos.

X-Force Premium: Servidor de correo interno que envía correo a posible host de correo no deseado
Normalmente, los servidores de correo que se comunican con hosts de correo no deseado se están utilizando incorrectamente.

X-Force Premium: Servidores no de correo que se comunican con hosts de envío de correo no deseado conocidos
Este comportamiento es un fuerte indicador de que el servidor se ha comprometido y está siendo utilizado como una retransmisión de correo no deseado.

X-Force Premium: No servidores que se comunican con IP dinámica externa
Las direcciones IP asignadas dinámicamente no están normalmente asociadas con servidores legítimos en Internet. Las estaciones de trabajo internas que se están comunicando con direcciones dinámicas pueden indicar actividad interna sospechosa o actividad de botnet o programas maliciosos.

X-Force Premium: El servidor ha iniciado la conexión con hosts dinámicos
Generalmente, los servidores se comunican con hosts que tienen una identidad fija y no direcciones IP dinámicas.

Dado que el URL es un indicador más específico de los datos que se transfieren, las reglas basadas en URL pueden ser más precisas que las reglas basadas en IP.

Estas reglas están basadas en URL:

X-Force Premium: Host interno que se comunica con URL de mandato y control de Botnet
A veces los servidores legítimos pueden utilizarse para proporcionar conectividad de botnet en direcciones de URL específicas.

X-Force Premium: Comunicación de host interno con URL de programa malicioso

A veces los servidores legítimos pueden utilizarse para proporcionar programas maliciosos en direcciones de URL específicas.

Ejemplo: Creación de una regla utilizando la categorización de URL para supervisar el acceso a determinados tipos de sitios web

Puede crear una regla que envíe una notificación de correo electrónico si los usuarios de la red interna acceden a direcciones de URL que están categorizadas como sitios web de apuestas.

Antes de empezar

Para utilizar reglas de categorización de URL, debe tener una suscripción al canal de información de X-Force Threat Intelligence.

Para crear una regla nueva, debe tener el permiso **Delitos** > **Mantener reglas personalizadas**.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Acciones**, seleccione **Nueva regla de sucesos**.
4. Lea el texto introductorio en el asistente de reglas y pulse **Siguiente**.
5. Pulse **Sucesos** y pulse **Siguiente**.
6. En el recuadro de lista **Grupo de pruebas**, seleccione **X-Force Tests**.
7. Pulse el signo más (+) signo junto a la prueba **when this URL property is categorized by X-Force as one of the following categories**.
8. En el campo **especifique aquí el nombre de la regla** en el panel Regla, escriba un nombre exclusivo que desee asignar a esta regla.
9. En el recuadro de lista, seleccione **Local** o **Global**.
10. Pulse los parámetros configurables subrayados para personalizar las variables de la prueba.
    a. Pulse **URL (personalizado)**.
    b. Seleccione la propiedad de URL que contiene el URL que se ha extraído de la carga útil y pulse **Enviar**.
    c. Pulse **una de las siguientes categorías**.
    d. Seleccione **Gambling / Lottery** en las categorías de URL de X-Force, pulse **Añadir +** y pulse **Enviar**.
11. Para exportar la regla configurada como un componente básico para utilizarlo con otras reglas:
    a. Pulse **Exportar como componente básico**.
    b. Escriba un nombre exclusivo para este componente básico.
    c. Pulse **Guardar**.
12. En el panel Grupos, seleccione los recuadros de selección de los grupos a los que desea asignar esta regla.
13. En el campo **Notas**, escriba una nota que desee incluir para esta regla y pulse **Siguiente**.

14. En la página Respuestas de regla, pulse **Correo electrónico** y escriba las direcciones de correo electrónico que recibirán la notificación. Para obtener información sobre otros parámetros de respuesta para una regla de suceso, consulte Parámetros de página de respuesta de regla común, flujo y suceso.
15. Pulse **Siguiente**.
16. Si la regla es precisa, pulse **Finalizar**.

Capítulo 10. Perfiles de activo

Los perfiles de activo proporcionan información sobre cada activo conocido en la red, incluyendo qué servicios se ejecutan en cada activo.

La información del perfil de activo se utiliza a efectos de correlación para ayudar a reducir los falsos positivos. Por ejemplo, si un origen intenta atacar un servicio específico que se ejecuta en un activo, QRadar determina si el activo es vulnerable a este ataque correlacionando el ataque con el perfil de activo.

Los perfiles de activo se descubren automáticamente si tiene exploraciones de evaluación de vulnerabilidad (VA) configuradas.

Vulnerabilidades

Puede utilizar exploradores de QRadar Vulnerability Manager y de terceros para identificar vulnerabilidades.

Los exploradores de terceros identifican e informan de las vulnerabilidades descubiertas utilizando referencias externas, como Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVDB) y Critical Watch. Los exploradores de terceros incluyen, por ejemplo, QualysGuard y nCircle ip360. OSVDB asigna un identificador de referencia exclusiva (OSVDB ID) a cada vulnerabilidad. Las referencias externas asignan un identificador de referencia exclusiva a cada vulnerabilidad. Los ID de referencia de datos externos incluyen, por ejemplo, el ID de Common Vulnerability and Exposures (CVE) o el ID de Bugtraq. Para obtener más información sobre exploradores y evaluación de vulnerabilidad, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

QRadar Vulnerability Manager es un componente que puede comprar por separado y habilitar utilizando una clave de licencia. QRadar Vulnerability Manager es una plataforma de exploración de red que proporciona conocimiento de las vulnerabilidades que existen en las aplicaciones, sistemas o dispositivos de la red. Después de que las exploraciones identifiquen las vulnerabilidades, puede buscar y revisar datos de vulnerabilidad, remediar vulnerabilidades y volver a ejecutar exploraciones para evaluar el nuevo nivel de riesgo.

Cuando se habilita QRadar Vulnerability Manager, puede realizar tareas de evaluación de vulnerabilidades en la pestaña **Vulnerabilidades**. En la pestaña **Activos**, puede ejecutar exploraciones en los activos seleccionados.

Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*

Visión general de la pestaña Activos

La pestaña **Activos** le proporciona un espacio de trabajo desde el que puede gestionar los activos de red e investigar las vulnerabilidades de un activo, los puertos, las aplicaciones, el historial y otras asociaciones.

Mediante el uso de la pestaña **Activos**, puede:

- Ver todos los activos descubiertos.
- Añadir manualmente perfiles de activo.
- Buscar activos específicos.
- Ver información sobre activos descubiertos.
- Editar perfiles de activo para activos añadidos o descubiertos manualmente.
- Ajustar vulnerabilidades positivas falsas.
- Importar activos.
- Imprimir o exportar perfiles de activo.
- Descubrir activos.
- Configurar y gestionar exploración de volumen de terceros.
- Iniciar exploraciones de QRadar Vulnerability Manager.

Para obtener más información sobre la opción de Exploración de VA en el panel de navegación, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.

Lista de pestaña Activo

La página Perfiles de activo proporciona información sobre el ID, la dirección IP, el nombre de activo, la puntuación de CVSS agregada, las vulnerabilidades y los servicios.

La página Perfiles de activo proporciona la siguiente información sobre cada activo:

Tabla 33. Parámetros de página Perfil de activo

Parámetro	Descripción
ID	Visualiza el número de ID del activo. El número de ID de activo se genera automáticamente cuando se añade un perfil de activo manualmente o cuando se descubren activos mediante exploraciones de vulnerabilidad o suceso.
Dirección IP	Visualiza la última dirección IP conocida del activo.
Nombre de activo	Visualiza el nombre, el nombre NetBios, el nombre de DSN o la dirección MAC del activo. Si se desconoce, este campo visualiza la última dirección IP conocida. **Nota:** Estos valores se visualizan en orden de prioridad. Por ejemplo, si el activo no tiene un nombre, se visualiza el nombre de NetBios de agregado. Si el activo se descubre automáticamente, este campo se llena automáticamente, sin embargo, puede editar el nombre de activo si es necesario.

Tabla 33. Parámetros de página Perfil de activo (continuación)

Parámetro	Descripción
Puntuación de riesgo	Visualiza una de las siguientes puntuaciones de CVSS (Common Vulnerability Scoring System): • Puntuación de CVSS de entorno agregada fusionada • Puntuación de CVSS temporal agregada • Puntuación base de CVSS agregada • Estas puntuaciones se visualizan en orden de prioridad. Por ejemplo, si la puntuación de CVSS de entorno agregada fusionada no está disponible, se visualiza la puntuación de CVSS temporal agregada. Una puntuación de CVSS es una medida de evaluación de la gravedad de una vulnerabilidad. Puede utilizar puntuaciones de CVSS para medir el grado de preocupación garantizada por una vulnerabilidad en comparación con otras vulnerabilidades. La puntuación de CVSS se calcula a partir de los siguientes parámetros definidos por el usuario: • Potencial de daños colaterales • Requisito de confidencialidad • Requisito de disponibilidad • Requisito de integridad Para obtener más información sobre cómo configurar estos parámetros, consulte "Adición o edición de un perfil de activo" en la página 116. Para obtener más información sobre CVSS, consulte http://www.first.org/cvss/ .
Vulnerabilidades	Visualiza el número de vulnerabilidades exclusivas que se han descubierto en este activo. Este valor también incluye el número de vulnerabilidades activas y pasivas.
Servicios	Visualiza el número de aplicaciones de capa 7 exclusivas que se ejecutan en este activo.
Último usuario	Visualiza el último usuario asociado con el activo.
Usuario visto por última vez	Visualiza la hora en que se ha visto por última vez el último usuario asociado con el activo.

Barra de herramientas de la pestaña Activos

La barra de herramientas de la página Perfiles de activo permite buscar, guardar, añadir, borrar, editar y realizar otras acciones sobre activos.

La barra de herramientas de página Perfiles de activo proporciona las funciones siguientes:

Tabla 34. Funciones de la barra de herramientas de la página Perfiles de activo

Función	Descripción
Buscar	Pulse **Buscar** para realizar búsquedas avanzadas sobre activos. Las opciones incluyen: • **Nueva búsqueda**: seleccione esta opción para crear una búsqueda de activo nueva. • **Editar búsqueda**: seleccione esta opción para editar una búsqueda de activo. Para obtener más información sobre la característica búsqueda, consulte Búsqueda de perfiles de activos .
Búsquedas rápidas	En este cuadro de lista, puede guardar búsquedas guardadas anteriormente. Solo se muestran las opciones en el cuadro de lista **Búsquedas rápidas** cuando tiene criterios de búsqueda guardados que especifican la opción **Incluir en Búsquedas rápidas**.
Guardar criterios	Pulse **Guardar criterios** para guardar los criterios de búsqueda actuales.
Añadir filtro	Pulse **Añadir filtro** para añadir un filtro a los resultados de la búsqueda actuales.
Añadir activo	Pulse **Añadir activo** para añadir un perfil de activo. Consulte Añadir o editar un perfil de activo.
Editar activo	Pulse **Editar activo** para editar un perfil. Esta opción está habilitada solo si ha seleccionado un perfil de activo en la lista de resultados. Consulte “Adición o edición de un perfil de activo” en la página 116.

Tabla 34. Funciones de la barra de herramientas de la página Perfiles de activo (continuación)

Función	Descripción
Acciones	Pulse **Acciones** para realizar las acciones siguientes: • **Suprimir activo**: seleccione esta opción para suprimir los perfiles de activo seleccionados. Consulte Supresión de activos. • **Suprimir listados**: seleccione esta opción para suprimir todos los perfiles de activo que aparecen en la lista de resultados. Consulte Supresión de activos. • **Importar activos**: seleccione esta opción para importar activos. Consulte Importación de perfiles de activos. • **Exportar a XML**: seleccione esta opción para exportar perfiles de activo en formato XML. Consulte Exportación de activos. • **Exportar a CSV**: marque esta opción para exportar perfiles de activo en formato CSV. Consulte Exportación de activos. • **Imprimir**: seleccione esta opción para imprimir los perfiles de activo visualizados en la página. • El menú **Acciones** solo está disponible si tiene privilegios administrativos.
Borrar filtro	Después de aplicar un filtro mediante la opción **Añadir filtro** puede pulsar **Borrar filtro** para eliminar el filtro.

Opciones del menú que aparece al pulsar el botón derecho del ratón

Al pulsar el botón derecho del ratón en un activo de la pestaña Activo se visualizan menús para obtener más información de filtro de sucesos.

En la pestaña **Activos**, puede pulsar el botón derecho del ratón en un activo para acceder a más información de filtro de sucesos.

Tabla 35. Opciones del menú que aparece al pulsar el botón derecho del ratón

Opción	Descripción
Información	El menú **Información** proporciona las opciones siguientes: • **Búsqueda de DNS**: Busca entradas DNS que se basan en la dirección IP. • **Búsqueda de WHOIS**: Busca el propietario registrado de una dirección IP remota. El servidor WHOIS predeterminado es whois.arin.net. • **Exploración de puertos**: Realiza una exploración de MAP (Network Mapper - Correlacionador de red) de la dirección IP seleccionada. Esta opción solo está disponible si NMAP está instalado en el sistema. Para obtener más información sobre la instalación de NMAP, consulte la documentación de proveedor. • **Perfil de activo**: Visualiza información de perfil de activo. Esta opción de menú sólo está disponible cuando los datos de un perfil los adquiere activamente una exploración. • **Sucesos de búsqueda**: Seleccione la opción **Sucesos de búsqueda** para buscar sucesos que están asociados con esta dirección IP.
Ejecutar Exploración de QVM	Seleccione esta opción para ejecutar una exploración de gestor de vulnerabilidad en el activo seleccionado. Esta opción solo se visualiza después de instalar QRadar Vulnerability Manager.

Visualización de un perfil de activo

En la lista de activos de la pestaña **Activos**, puede seleccionar y ver un perfil de activo. Un perfil de activo proporciona información sobre cada perfil.

Acerca de esta tarea

La información de perfil de activo se descubre automáticamente a través del servidor de descubrimiento o se configura manualmente. Puede editar la información de perfil de activo generada automáticamente.

La página Perfil de activo proporciona la información sobre el activo que se organiza en varios paneles. Para ver un panel, puede pulsar la flecha **(>)** en el panel para ver más detalles o seleccionar el panel en el recuadro de lista **Visualizar** en la barra de herramientas.

La barra de herramientas de página Perfil de activo proporciona las funciones siguientes:

Tabla 36. Funciones de barra de herramientas de página Perfil de activo

Opciones	Descripción
Volver a lista de activos	Pulse esta opción para volver a la lista de activos.
Visualizar	En el recuadro de lista, puede seleccionar el panel que desea ver en el panel Perfil de activo. Los paneles Resumen de activo y Resumen de interfaz de red se visualizan siempre. Para obtener más información sobre los parámetros que se muestran en cada panel, consulte Parámetros de página de perfil de activos.
Editar activo	Pulse esta opción para editar el Perfil de activo. Consulte "Adición o edición de un perfil de activo" en la página 116.
Ver resumen de destino	Si este activo es el destino de un delito, esta opción le permitirá ver información de resumen de destino.
Historial	Pulse **Historial** para ver información de historial de sucesos para este activo. Al pulsar el icono **Historial**, se visualiza la ventana Búsqueda de sucesos, previamente rellenada con los criterios de búsqueda de sucesos: Si es necesario, puede personalizar los parámetros de búsqueda. Pulse **Buscar** para ver información de historial de sucesos.
Aplicaciones	Pulse **Aplicaciones** para ver información de aplicación para este activo. Al pulsar el icono **Aplicaciones**, se visualiza la ventana Búsqueda de flujos, previamente rellenada con criterios de búsqueda de sucesos. Si es necesario, puede personalizar los parámetros de búsqueda. Pulse **Buscar** para ver la información de aplicación.
Buscar en conexiones	Pulse **Buscar en conexiones** para buscar conexiones. Se visualiza la ventana Búsqueda de conexión. Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
Ver topología	Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.

Tabla 36. Funciones de barra de herramientas de página Perfil de activo (continuación)

Opciones	Descripción
Acciones	En la lista **Acciones**, seleccione **Historial de vulnerabilidades.** Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**
3. Efectúe una doble pulsación en el activo que desea ver.
4. Utilice las opciones de la barra de herramientas para visualizar los diversos paneles de información de perfil de activo. Consulte Edición de un perfil de activo.
5. Para investigar las vulnerabilidades asociadas, pulse cada vulnerabilidad en el panel Vulnerabilidades. Consulte la Tabla 10-10
6. Si es necesario, edite el perfil de activo. Consulte Edición de un perfil de activo.
7. Pulse **Volver a lista de activos** para seleccionar y ver otro activo, si es necesario.

Adición o edición de un perfil de activo

Los perfiles de activo se descubren y añaden automáticamente; sin embargo, puede ser necesario añadir manualmente un perfil

Acerca de esta tarea

Cuando se descubren activos mediante la utilización de la opción Descubrimiento de servidores, algunos detalles de perfil de activo se rellenan automáticamente. Se puede añadir manualmente información al perfil de activo y se pueden editar determinados parámetros.

Sólo se pueden editar los parámetros que se han entrado manualmente. Los parámetros generados por el sistema aparecen en cursiva y no son editables. Los parámetros generados por el sistema pueden suprimirse, si es necesario.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Elija una de las siguientes opciones:
   - Para añadir un activo, pulse **Añadir activo** y escriba la dirección IP o el rango de CIDR del activo en el campo **Nueva dirección IP**.
   - Para editar un activo, efectúe una doble pulsación en el activo que desea ver y pulse **Editar activo**.
4. Configure los parámetros del panel MAC y dirección MAC. Configure una o varias de las opciones siguientes:

- Pulse el icono **Nueva dirección MAC** y escriba una dirección MAC en el recuadro de diálogo.
- Pulse el icono **Nueva dirección IP** y escriba una dirección IP en el recuadro de diálogo.
- Si se lista **NIC desconocido**, puede seleccionar este elemento, pulsar el icono **Editar** y escribir una nueva dirección MAC en el recuadro de diálogo.
- Seleccione una dirección MAC o IP en la lista, pulse el icono **Editar** y escriba una dirección MAC nueva en el recuadro de diálogo.
- Seleccione una dirección MAC o IP en la lista y pulse el icono **Eliminar**.

5. Configure los parámetros del panel Nombres y descripción. Configure una o varias de las opciones siguientes:

Parámetro	Descripción
DNS	Elija una de las siguientes opciones: • Escriba un nombre DNS y pulse **Añadir**. • Seleccione un nombre de DNS en la lista y pulse **Editar**. • Seleccione un nombre de DNS en la lista y pulse **Eliminar**.
NetBIOS	Elija una de las siguientes opciones: • Escriba un nombre NetBIOS y pulse **Añadir**. • Seleccione un nombre de NetBIOS en la lista y pulse **Editar**. • Seleccione un nombre de NetBIOS en la lista y pulse **Eliminar**.
Nombre	Escriba un nombre para este perfil de activo.
Ubicación	Escriba una ubicación para este perfil de activo.
Descripción	Escriba una descripción para este perfil de activo.
AP inalámbrico	Escriba el punto de acceso (AP) inalámbrico para este perfil de activo.
SSID inalámbrico	Escriba el identificador de conjunto de servicios (SSID) inalámbrico para este perfil de activo.
ID de conmutador	Escriba el ID de conmutador para este perfil de activo.
ID de puerto de conmutador	Escriba el ID de puerto de conmutador para este perfil de activo.

6. Configure los parámetros del panel Sistema operativo:
   a. En el recuadro de lista **Proveedor**, seleccione un proveedor de sistema operativo.
   b. En el recuadro de lista **Producto**, seleccione el sistema operativo para el perfil de activo.
   c. En el recuadro de lista **Versión**, seleccione la versión del sistema operativo seleccionado.
   d. Pulse el icono **Añadir**.

e. En el recuadro de lista **Alterar temporalmente**, seleccione una de las opciones siguientes:
   - **Hasta próxima exploración**: Seleccione esta opción para especificar que el explorador proporciona información de sistema operativo y la información se puede editar temporalmente. Si edita los parámetros de sistema operativo, el explorador restaura la información en su próxima exploración.
   - **Siempre**: Seleccione esta opción para especificar que desea entrar manualmente la información del sistema operativo e impedir que el explorador actualice información.

f. Seleccione un sistema operativo de la lista.

g. Seleccione un sistema operativo y pulse en el icono **Conmutar alteración temporal**.

7. Configure los parámetros del panel CVSS y peso. Configure una o varias de las opciones siguientes:

Parámetro	Descripción
Potencial de daños colaterales	Configure este parámetro para indicar la posibilidad de pérdida de vidas humanas o activos físicos a través de daños o robo de este activo. También puede utilizar este parámetro para indicar el potencial de pérdida económica de productividad o ingresos. El mayor potencial de daños colaterales aumenta el valor calculado en el parámetro de puntuación de CVSS. En el recuadro de lista **Potencial de daños colaterales**, seleccione una de las opciones siguientes: • Ninguno • Bajo • Medio bajo • Medio alto • Alto • No definido Al configurar el parámetro **Potencial de daños colaterales**, el parámetro **Peso** se actualizar automáticamente.

Parámetro	Descripción
Requisito de confidencialidad	Configure este parámetro para indicar el impacto en la confidencialidad de una vulnerabilidad atacada con éxito en este activo. Un mayor impacto de confidencialidad aumenta el valor calculado en el parámetro Puntuación de CVSS. En el recuadro de lista **Requisito de confidencialidad**, seleccione una de las opciones siguientes: • Bajo • Medio • Alto • No definido
Requisito de disponibilidad	Configure este parámetro para indicar el impacto en la disponibilidad del activo cuando una vulnerabilidad se ataca con éxito. Los ataques que consumen ancho de banda de red, ciclos de procesador o espacio de disco impactan la disponibilidad de un activo. Un mayor impacto de disponibilidad aumenta el valor calculado en el parámetro Puntuación de CVSS. En el recuadro de lista **Requisito de disponibilidad**, seleccione una de las opciones siguientes: • Bajo • Medio • Alto • No definido
Requisito de integridad	Configure este parámetro para indicar que el impacto en la integridad del activo cuando una vulnerabilidad se ataca con éxito. La integridad hace referencia a la fiabilidad y la veracidad garantizada de la información. Un mayor impacto de integridad aumenta el valor calculado en el parámetro Puntuación de CVSS. En el recuadro de lista **Requisito de integridad**, seleccione una de las opciones siguientes: • Bajo • Medio • Alto • No definido

Parámetro	Descripción
Peso	En el recuadro de lista **Peso** , seleccione un peso para este perfil de activo. El rango de valores es de 0 a 10. Cuando configure el parámetro **Peso**, el parámetro **Potencial de daños colaterales** se actualiza automáticamente.

8. Configure los parámetros del panel Propietario. Elija una o varias de las opciones siguientes:

Parámetro	Descripción
Propietario del negocio	Escriba el nombre del propietario del negocio del activo. Un propietario de negocio es, por ejemplo, un director de departamento. La longitud máxima es de 255 caracteres.
Contacto del propietario del negocio	Escriba la información de contacto para el propietario de negocio. La longitud máxima es de 255 caracteres.
Propietario técnico	Escriba el propietario técnico del activo. Un propietario técnico es, por ejemplo, el director o gestor de TI. La longitud máxima es de 255 caracteres.
Contacto de propietario técnico	Escriba la información de contacto para el propietario técnico. La longitud máxima es de 255 caracteres.
Usuario técnico	En el recuadro de lista, seleccione el nombre de usuario que desea asociar con este perfil de activo. También puede utilizar este parámetro para habilitar la remediación de vulnerabilidad automática para IBM Security QRadar Vulnerability Manager. Para obtener más información sobre la remediación automática, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

9. Pulse **Guardar**.

Búsqueda de perfiles de activo

Puede configurar parámetros de búsqueda para mostrar sólo los perfiles de activo que desea investigar en la página Activo en la pestaña **Activos**.

Acerca de esta tarea

Al acceder a la pestaña **Activos**, se visualiza la página Activo llena con todos los activos descubiertos en la red. Para refinar esta lista, puede configurar parámetros de búsqueda para visualizar solo los perfiles de activo que desea investigar.

En la página Búsqueda de activo, puede gestionar Grupos de búsqueda de activos. Para obtener más información sobre Grupos de búsqueda de activos, consulte Grupos de búsqueda de activos.

La característica de búsqueda le permitirá buscar perfiles de host, activos e información de identidad. La información de identidad proporciona más detalles sobre los orígenes de registro en la red, incluyendo información de DNS, inicios de sesión de usuario y direcciones MAC.

Mediante la característica de búsqueda de activos, puede buscar activos por referencias de datos externas para determinar si existen vulnerabilidades conocidas en el despliegue.

Por ejemplo:

Recibe una notificación de que el ID de CVE: CVE-2010-000 está siendo utilizado activamente en el campo. Para verificar si los hosts del despliegue son vulnerables a este ataque, puede seleccionar **Referencia externa de vulnerabilidad** en la lista de parámetros de búsqueda, seleccionar **CVE** y, a continuación, escribir

```
2010-000
```

para ver una lista de todos los hosts que son vulnerables a ese ID de CVE específico.

Nota: Para obtener más información acerca de OSVDB, consulte *http://osvdb.org/*. Para obtener más información acerca de NVDB, consulte *http://nvd.nist.gov/*.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En la barra de herramientas, pulse **Buscar** > **Nueva búsqueda**.
4. Elija una de las siguientes opciones:
   - Para cargar una búsqueda guardada anteriormente, vaya al Paso 5.
   - Para crear una nueva búsqueda, vaya al Paso 6.
5. Seleccione una búsqueda guardada anteriormente:
   a. Elija una de las siguientes opciones:
      - Opcional. En el recuadro de lista **Grupo**, seleccione el grupo de búsqueda de activos que desea visualizar en la lista **Búsquedas guardadas disponibles**.
      - En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desea cargar.
      - En el campo **Escriba la búsqueda guardada o seleccione en la lista**, escriba el nombre de la búsqueda que desea cargar.
   b. Pulse **Cargar**.
6. En el panel Parámetros de búsqueda, defina los criterios de búsqueda:
   a. En el primer recuadro de lista, seleccione el parámetro de activo que desea buscar. Por ejemplo, **Nombre de host**, **Clasificación de riesgo de vulnerabilidad** o **Propietario técnico**.
   b. En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda.
   c. En el campo de entrada, escriba información específica que está relacionada con el parámetro de búsqueda.

d. Pulse **Añadir filtro**.
e. Repita estos pasos para cada filtro que desee añadir a los criterios de búsqueda.

7. Pulse **Buscar**.

Resultados

Puede guardar los criterios de búsqueda de activos. Consulte Guardar criterios de búsqueda de activos.

Guardar criterios de búsqueda de activos

En la pestaña **Activo**, puede guardar criterios de búsqueda configurados para poder reutilizar los criterios. Los criterios de búsqueda guardados no caducan.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Realice una búsqueda. Consulte Búsqueda de perfiles de activo.
4. Pulse **Guardar criterios**.
5. Entre valores para los parámetros:

Parámetro	Descripción
Especifique el nombre de esta búsqueda	Escriba el nombre exclusivo que desee asignar a este criterio de búsqueda.
Gestionar grupos	Pulse **Gestionar grupos** para gestionar grupos de búsqueda. Para obtener más información, consulte Grupos de búsqueda de activos. Esta opción sólo se visualiza si tiene permisos administrativos.
Asignar búsqueda a grupo(s)	Marque el recuadro de selección para el grupo al que desea asignar esta búsqueda guardada. Si no selecciona un grupo, esta búsqueda guardada se asigna al grupo **Otros** de forma predeterminada. Para obtener más información, consulte Grupos de búsqueda de activos.
Incluir en Búsquedas rápidas	Marque este recuadro de selección para incluir esta búsqueda en el recuadro de lista **Búsqueda rápida**, que se encuentra en la barra de herramientas de la pestaña **Activos**.
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada cuando accede a la pestaña **Activos**.
Compartir con todos	Marque este recuadro de selección para compartir estos requisitos de búsqueda con todos los usuarios.

Grupos de búsqueda de activos

Utilizando la ventana Grupos de búsqueda de activos, puede crear y gestionar grupos de búsqueda de activos.

Estos grupos le permiten localizar fácilmente criterios de búsqueda guardados en la pestaña **Activos**.

Visualización de grupos de búsqueda

Utilice la ventana Grupos de búsqueda de activos para ver una lista de grupos y subgrupos.

Acerca de esta tarea

En la ventana Grupos de búsqueda de activos, puede ver detalles acerca de cada grupo, incluyendo una descripción y la fecha en que se ha modificado por última vez el grupo.

Todas las búsquedas guardadas que no se asignan a un grupo están en el grupo **Otros**.

La ventana Grupos de búsqueda de activos muestra los parámetros siguientes para cada grupo:

Tabla 37. Funciones de barra de herramientas de ventanas Grupos de búsqueda de activos

Función	Descripción
Grupo nuevo	Para crear un nuevo grupo de búsqueda, puede pulsar **Grupo nuevo**. Consulte Creación de un grupo de búsqueda nuevo.
Editar	Para editar un grupo de búsqueda existente, puede pulsar en **Editar**. Consulte Edición de un grupo de búsqueda.
Copiar	Para copiar una búsqueda guardada en otro grupo de búsqueda, puede pulsar en **Copiar**. Consulte Copia de una búsqueda guardada en otro grupo.
Eliminar	Para eliminar un grupo de búsqueda o una búsqueda guardada de un grupo de búsqueda, seleccione el elemento que desea eliminar y luego pulse **Eliminar**. Consulte Eliminación de un grupo o una búsqueda guardada de un grupo.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Vea los grupos de búsqueda.

Creación de un grupo de búsqueda nuevo

En la ventana Grupos de búsqueda de activos, puede crear un nuevo grupo de búsqueda.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.

3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la carpeta para el grupo donde desea crear el nuevo grupo.
6. Pulse **Grupo nuevo**.
7. En el campo **Nombre**, escriba un nombre exclusivo para el nuevo grupo.
8. Opcional. En el campo **Descripción**, escriba una descripción.
9. Pulse **Aceptar**.

Edición de un grupo de búsqueda

Puede editar los campos **Nombre** y **Descripción** de un grupo de búsqueda.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione el grupo que desea editar.
6. Pulse **Editar**.
7. Escriba un nombre nuevo en el campo **Nombre**.
8. Escriba una nueva descripción en el campo **Descripción**.
9. Pulse **Aceptar**.

Copia de una búsqueda guardada en otro grupo

Puede copiar una búsqueda guardada en otro grupo. También puede copiar la búsqueda guardada en más de un grupo.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la búsqueda guardada que desea copiar.
6. Pulse **Copiar**.
7. En la ventana Grupos de elementos, marque el recuadro de selección para el grupo en el que desea copiar la búsqueda guardada.
8. Pulse **Asignar grupos**.

Eliminación de un grupo o una búsqueda guardada de un grupo

Puede utilizar el icono **Eliminar** para eliminar una búsqueda de un grupo o eliminar un grupo de búsqueda.

Acerca de esta tarea

Cuando se elimina una búsqueda guardada de un grupo, la búsqueda guardada no se suprime del sistema. La búsqueda guardada se elimina del grupo y se mueve automáticamente al grupo **Otros**.

No puede eliminar los grupos siguientes del sistema:

- Grupos de búsqueda de activos
- Otros

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la búsqueda guardada que desea eliminar del grupo:
   - Seleccione la búsqueda guardada que desea eliminar del grupo.
   - Seleccione el grupo que desea eliminar.

Tareas de gestión de perfiles de activo

Puede suprimir, importar y exportar perfiles de activos utilizando la pestaña Activos.

Acerca de esta tarea

Utilizando la pestaña **Activos**, puede suprimir, importar y exportar perfiles de activos.

Supresión de activos

Puede suprimir activos específicos o todos los perfiles de activo listados.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione el activo que desea suprimir y, a continuación, seleccione **Suprimir activo** en el recuadro de lista **Acciones**.
4. Pulse **Aceptar**.

Importación de perfiles de activo

Puede importar información de perfil de activo.

Antes de empezar

El archivo importado debe ser un archivo CSV con el formato siguiente:

```
ip,nombre,peso,descripción
```

Donde:

- **IP**: Especifica cualquier dirección IP válida en formato decimal con puntos. Por ejemplo: 192.168.5.34.
- **Nombre**: Especifica el nombre de este activo con una longitud de hasta 255 caracteres. Las comas no son válidas en este campo e invalidan el proceso de importación. Por ejemplo: WebServer01 es correcto.
- **Peso**: Especifica un número de 0 a 10, que indica la importancia de este activo en la red. Un valor de 0 indica una importancia baja y 10 es muy alta.

- **Descripción**: Especifica una descripción textual para este activo con una longitud de hasta 255 caracteres. Este valor es opcional.

Por ejemplo, las siguientes entradas se pueden incluir en un archivo CSV:

- ```
  192.168.5.34,WebServer01,5,Main Production Web Server
  ```
- ```
  192.168.5.35,MailServ01,0,
  ```

El proceso de importación fusiona los perfiles de activo importados con la información de perfil de activo que está actualmente almacenada en el sistema.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En el recuadro de lista **Acciones**, seleccione **Importar activos**.
4. Pulse **Examinar** para localizar y seleccionar el archivo CSV que desea importar.
5. Pulse **Importar activos** para empezar el proceso de importación.

Exportación de activos

Puede exportar perfiles de activo listados a un archivo XML (Extended Markup Language - Lenguaje de marcado extensible) o CSV (Comma-Separated Value - Valor separado por comas).

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:
   - Exportar a XML
   - Exportar a CSV
4. Vea la ventana de estado para el estado del proceso de exportación.
5. Opcional: Si desea utilizar otras pestañas y páginas mientras la exportación está en curso, pulse el enlace **Notificar cuando termine**.

   Cuando la exportación se haya completado, se visualizará la ventana Descarga de archivo.
6. En la ventana Descarga de archivo, elija una de las opciones siguientes:
   - **Abrir**: Seleccione esta opción para abrir los resultados de exportación en el navegador que haya elegido.
   - **Guardar**: Seleccione esta opción para guardar los resultados en el escritorio.
7. Pulse **Aceptar**.

Investigar vulnerabilidades de activo

El panel Vulnerabilidades en la página Perfil de activo visualiza una lista de vulnerabilidades descubiertas para el activo.

Acerca de esta tarea

Puede efectuar una doble pulsación en la vulnerabilidad a mostrar más detalles de vulnerabilidad.

La ventana Investigar detalles de vulnerabilidad proporciona los detalles siguientes:

Parámetro	Descripción
ID de vulnerabilidad	Especifica el ID de la vulnerabilidad. El ID de vulnerabilidad es un identificador exclusivo generado por VIS (Vulnerability Information System - Sistema de información de vulnerabilidad).
Fecha de publicación	Especifica la fecha en la que los detalles de vulnerabilidad se han publicado en la OSVDB.
Nombre	Especifica el nombre de la vulnerabilidad.
Activos	Especifica el número de activos de la red que tienen esta vulnerabilidad. Pulse el enlace para ver la lista de activos.
Activos, incluyendo excepciones	Especifica el número de activos de la red que tienen excepciones de vulnerabilidad. Pulse el enlace para ver la lista de activos.
CVE	Especifica el identificador de CVE para la vulnerabilidad. Los identificadores de CVE los proporciona la NVDB. Pulse el enlace para obtener más información. Al pulsar en el enlace, el sitio web NVDB se visualiza en una ventana de navegador nueva.
xforce	Especifica el identificador de X-Force para la vulnerabilidad. Pulse el enlace para obtener más información. Al pulsar el enlace, el sitio web de IBM Internet Security Systems se visualiza en una ventana de navegador nueva.
OSVDB	Especifica el identificador de OSVDB para la vulnerabilidad. Pulse el enlace para obtener más información. Al pulsar el enlace, el sitio web OSVDB se visualiza en una ventana de navegador nueva.
Detalles de plug-in	Especifica el ID de QRadar Vulnerability Manager. Pulse el enlace para ver definiciones de Oval, entradas de Windows Knowledge Base o avisos de UNIX para la vulnerabilidad. Esta característica proporciona información sobre cómo QRadar Vulnerability Manager comprueba los detalles de vulnerabilidad durante una exploración de parches. Puede utilizarla para identificar por qué se ha generado una vulnerabilidad en un activo o por qué no se ha generado.

Parámetro	Descripción
Puntuación base CVSS	Visualiza la puntuación de CVSS (Common Vulnerability Scoring System) de agregado de las vulnerabilidades en este activo. Una puntuación de CVSS es una medida de evaluación de la gravedad de una vulnerabilidad. Puede utilizar puntuaciones de CVSS para medir el grado de preocupación garantizada por una vulnerabilidad en comparación con otras vulnerabilidades. La puntuación de CVSS se calcula utilizando los siguientes parámetros definidos por el usuario: • Potencial de daños colaterales • Requisito de confidencialidad • Requisito de disponibilidad • Requisito de integridad Para obtener más información sobre cómo configurar estos parámetros, consulte "Adición o edición de un perfil de activo" en la página 116. Para obtener más información acerca de CVSS, consulte *http://www.first.org/cvss/*.
Impacto	Visualiza el tipo de daño o perjuicio que se puede esperar si se aprovecha esta vulnerabilidad.
Medidas base de CVSS	Muestra las medidas que se utilizan para calcular la puntuación base de CVSS, incluyendo: • Vector de acceso • Complejidad de acceso • Autenticación • Impacto de confidencialidad • Impacto de integridad • Impacto de disponibilidad
Descripción	Especifica una descripción de la vulnerabilidad detectada. Este valor sólo está disponible cuando el sistema integra herramientas de VA.
Problema	Especifica los efectos que la vulnerabilidad puede tener en la red.
Solución	Siga las instrucciones que se proporcionan para resolver la vulnerabilidad.

Parámetro	Descripción
Parcheo virtual	Visualiza la información de parche virtual asociada con esta vulnerabilidad, si está disponible. Un parche virtual es una solución de mitigación a corto plazo para una vulnerabilidad descubierta recientemente. Esta información se deriva de los sucesos de IPS (Intrusion Protection System - Sistema de prevención de intrusiones). Si desea instalar el parche virtual, consulte la información de proveedor de IPS.
Referencia	Visualiza una lista de referencias externas, incluyendo: • **Tipo de referencia**: Especifica el tipo de referencia que se lista, por ejemplo una lista de envío de correo o URL de advertencia. • **URL**: Especifica el URL que puede pulsar para ver la referencia. Pulse el enlace para obtener más información. Al pulsar el enlace, el recurso externo se visualiza en una ventana de navegador nueva.
Productos	Visualiza una lista de productos que están asociados con esta vulnerabilidad. • **Proveedor**: Especifica el proveedor del producto. • **Producto**: Especifica el nombre de producto. • **Versión**: Especifica el número de versión del producto.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione un perfil de activo.
4. En el panel de vulnerabilidades, pulse el valor de parámetro **ID** o **Vulnerabilidad** para la vulnerabilidad que desea investigar.

Parámetros de página de perfil de activos

Puede encontrar descripciones de parámetro de página de perfil de activo para el panel Resumen de activo, panel Interfaz de red, panel Vulnerabilidad, panel Servicios, panel Paquetes, panel Parches de Windows, panel Propiedades, panel Políticas de riesgo y panel Productos.

Esta referencia incluye tablas que describen los parámetros que se visualizan en cada panel del separador**Perfil de activo**.

Panel Resumen de activo

Puede encontrar descripciones de parámetros para el panel Resumen de activo al que se accede desde la página Perfil de activo.

El panel Resumen de activo de la página Perfil de activo proporciona la información siguiente:

Tabla 10-8 Parámetros de panel Resumen de activo

Parámetro	Descripción
ID de activo	Visualiza el número de ID que se ha asignado al perfil de activo.
Dirección IP	Visualiza la última dirección IP del activo indicada.
Dirección MAC	Visualiza la última dirección MAC conocida del activo.
Red	Visualiza la última red indicada que está asociada con el activo.
Nombre de NetBIOS	Visualiza el nombre de NetBIOS del activo, si se conoce. Si el activo tiene más de un nombre de NetBIOS, este campo indica el número de nombres de NetBIOS. Mueva el puntero de ratón sobre el valor para ver una lista de nombres de NetBIOS asociados.
Nombre DNS	Visualiza la dirección IP o el nombre DNS del activo, si se conoce. Si el activo tiene más de un nombre DNS, este campo indica el número de nombres DNS. Mueva el puntero de ratón sobre el valor para ver una lista de nombres DNS asociados.
Nombre	Visualiza el nombre del activo. De forma predeterminada, este campo está vacío. Para proporcionar un nombre dado para el activo, edite el perfil de activo.
Nombre de grupo	Visualiza el último grupo de usuarios conocido del activo, si se conoce.
Último usuario	Visualiza el último usuario conocido del activo. La información de usuario se deriva de los sucesos de identidad. Si hay más de un usuario asociado con este activo, puede pulsar el enlace para mostrar todos los usuarios.
Sistema operativo	Visualiza el sistema operativo que se ejecuta en el activo. Si el activo tiene más de un sistema operativo, este campo indica el número de sistemas operativos. Mueva el puntero de ratón sobre el valor para ver una lista de sistemas operativos asociados. Puede editar este parámetro directamente si el parámetro **Alterar temporalmente** se especifica como **hasta próxima exploración** o **Siempre**.

Parámetro	Descripción
Peso	Visualiza el nivel de importancia que está asociada con este activo. El rango es de 0 (No importante) a 10 (Muy importante). De forma predeterminada, este campo está vacío. Para proporcionar un peso para el activo, edite el perfil de activo.
Puntuación de CVSS agregada	Visualiza la puntuación de CVSS (Common Vulnerability Scoring System) de agregado de las vulnerabilidades en este activo. Una puntuación de CVSS es una medida de evaluación de la gravedad de una vulnerabilidad. Puede utilizar puntuaciones de CVSS para medir el grado de preocupación garantizada por una vulnerabilidad en comparación con otras vulnerabilidades. La puntuación de CVSS se calcula utilizando los siguientes parámetros definidos por el usuario: • Potencial de daños colaterales • Requisito de confidencialidad • Requisito de disponibilidad • Requisito de integridad Para obtener más información sobre cómo configurar estos parámetros, consulte "Adición o edición de un perfil de activo" en la página 116. Para obtener más información acerca de CVSS, consulte *http://www.first.org/cvss/*.
Propietario del negocio	Visualiza el nombre del propietario del negocio del activo. Un propietario de negocio es, por ejemplo, un director de departamento.
Información de contacto del propietario del negocio	Visualiza la información de contacto para el propietario del negocio.
Potencial de daños colaterales de CVSS	Visualiza el potencial que este activo tiene para los daños colaterales. Este valor se incluye en la fórmula para calcular el parámetro **Puntuación de CVSS**. De forma predeterminada, este campo no está definido. Para proporcionar una ubicación para el activo, edite el perfil de activo.
Propietario técnico	Visualiza el propietario técnico del activo. Un propietario técnico es, por ejemplo, un gestor de TI o director.
Información de contacto de propietario técnico	Visualiza la información de contacto del propietario técnico.

Parámetro	Descripción
Disponibilidad de CVSS	Visualiza el impacto en la disponibilidad del activo cuando se ataca con éxito una vulnerabilidad.
AP inalámbrico	Visualiza el punto de acceso (AP) sin cables para este perfil de activo.
SSID inalámbrico	Visualiza el identificador de conjunto de servicios inalámbricos (SSID) para este perfil de activo.
Requisitos de confidencialidad de CVSS	Visualiza el impacto sobre la confidencialidad de una vulnerabilidad atacada con éxito en este activo.
ID de conmutador	Visualiza el ID de conmutador para este perfil de activo.
ID de puerto de conmutador	Visualiza el ID de puerto de conmutador para este perfil de activo.
Requisitos de integridad de CVSS	Visualiza el impacto en la integridad del activo cuando se ataca con éxito una vulnerabilidad.
Usuario técnico	Especifica el nombre de usuario que está asociado con este perfil de activo.
Servicios abiertos	Visualiza el número de aplicaciones de capa 7 exclusivas que se ejecutan en este perfil de activo.
Vulnerabilidades	Visualiza el número de vulnerabilidades que se han descubierto en este perfil de activo.
Ubicación	Especifica la ubicación física del activo. De forma predeterminada, este campo está vacío. Para proporcionar una ubicación para el activo, edite el perfil de activo.
Descripción del activo	Especifica una descripción para este activo. De forma predeterminada, este campo está vacío. Para proporcionar una descripción para el activo, edite el perfil de activo.
Datos adicionales	Especifica cualquier información ampliada que se base en un suceso.

Panel Resumen de interfaz de red

Puede encontrar descripciones de parámetros para el panel Resumen de interfaz de red al que se accede desde la página Perfil de activo.

El panel Resumen de interfaz de red de la página Perfil de activo proporciona la información siguiente:

Tabla 1 Parámetros de panel Resumen de interfaz de red

Parámetro	Descripción
Dirección MAC	Visualiza la dirección MAC de este activo, si se conoce.

Parámetro	Descripción
Dirección IP	Visualiza la dirección IP que se detecta para esta dirección MAC.
Red	Visualiza la red con la que está asociada la dirección IP, si se conoce.
Última visualización	Visualiza la fecha y hora en la que se ha detectado por última vez la dirección IP en esta dirección MAC.

Panel Vulnerabilidad

Puede encontrar descripciones de parámetros para el panel Vulnerabilidad al que se accede desde la página Perfil de activo.

El panel Vulnerabilidad en la página Perfil de activo proporciona la información siguiente:

Tabla 38. Parámetros de panel Vulnerabilidad

Parámetro	Descripción
ID	Visualiza el ID de la vulnerabilidad. El ID es un identificador exclusivo generado por VIS (Vulnerability Information System - Sistema de información de vulnerabilidad).
Gravedad	Muestra la gravedad de PCI (Payment Security Industry) que está asociada a la vulnerabilidad.
Riesgo	Nivel de riesgo que está asociado a la vulnerabilidad. La ordenación en esta columna debe ser por el código de nivel de riesgo subyacente
Servicio	Servicio que está asociado con la vulnerabilidad (como lo ha descubierto la exploración). Si sólo se ha asociado 1 servicio, visualice el servicio. De lo contrario, visualice Múltiple (N), donde N indica el número total de los servicios asociados a esta vulnerabilidad.
Puerto	Visualiza el número de puerto en el que se ha descubierto esta vulnerabilidad. Si la vulnerabilidad se ha descubierto en más de un puerto, este campo indica el número de puertos. Mueva el puntero del ratón sobre el valor para ver una lista de números de puerto.
Vulnerabilidad	Nombre o título de esta vulnerabilidad.
Detalles	Texto detallado específicos que está asociado a esta vulnerabilidad como lo determina la exploración. Si sólo se ha asociado 1 Detalle, visualice el texto de este detalle. De lo contrario, visualice Múltiple (N), donde N indica que el número total de detalles que están asociados a esta vulnerabilidad.

Tabla 38. Parámetros de panel Vulnerabilidad (continuación)

Parámetro	Descripción
Puntuación de CVSS	Visualiza la puntuación de CVSS (Common Vulnerability Scoring System) de agregado de las vulnerabilidades en este activo. Una puntuación de CVSS es una medida de evaluación de la gravedad de una vulnerabilidad. Puede utilizar puntuaciones de CVSS para medir el grado de preocupación garantizada por una vulnerabilidad en comparación con otras vulnerabilidades. La puntuación de CVSS se calcula utilizando los siguientes parámetros definidos por el usuario: • Potencial de daños colaterales • Requisito de confidencialidad • Requisito de disponibilidad • Requisito de integridad Para obtener más información sobre cómo configurar estos parámetros, consulte "Adición o edición de un perfil de activo" en la página 116. Para obtener más información acerca de CVSS, consulte *http://www.first.org/cvss/*.
Encontrad	Visualiza la fecha en que esta vulnerabilidad se ha encontrado originalmente en una exploración.
Última visualización	Visualiza la fecha en la que se ha visto por última vez esta vulnerabilidad en una exploración.

Panel Servicios

Puede buscar descripciones de parámetro para el panel Servicios al que se accede desde la página Perfil de activo.

El panel Servicios en la página Perfil de activo proporciona la información siguiente:

Tabla 39. Parámetros del panel Servicios

Parámetro	Descripción
Servicio	Visualiza el nombre del servicio abierto.
Producto	Visualiza el producto que se ejecuta en este servicio, si se conoce.
Puerto	Visualiza el puerto en el que se ha descubierto la aplicación de la Capa 7. Si este servicio tiene más de un puerto, este campo indica el número de puertos. Mueva el puntero del ratón sobre el valor para ver una lista de números de puerto.

Tabla 39. Parámetros del panel Servicios (continuación)

Parámetro	Descripción
Protocolo	Visualiza una lista separada por comas de protocolos que se han descubierto en el puerto que ejecuta el servicio abierto.
Visto como pasivo por última vez	Visualiza la fecha y hora en la que se ha visto pasivamente por última vez el servicio abierto.
Visto como activo por última vez	Visualiza la fecha y hora en la que se ha visto activamente por última vez el servicio abierto.
Puertos predeterminados de servicio	Visualiza una lista separada por comas de puertos conocidos en los que se sabe que se ejecuta la aplicación de la Capa 7.
Vulnerabilidades	Visualiza el número de vulnerabilidades que están asociadas con este servicio abierto.

Panel Servicios de Windows

Puede buscar descripciones de parámetro para el panel Servicios de Windows al que accede desde la página Perfil de activo. El panel Servicios de Windows solo se visualiza cuando QRadar Vulnerability Manager está instalado en el sistema.

El panel Servicios de Windows de la pagina Perfil de activo proporciona la información siguiente:

Tabla 40. Parámetros de panel Servicios de Windows

Parámetro	Descripción
Nombre	Visualiza el nombre del servicio de Windows que se ha visto activamente en el activo.
Estado	Visualiza el estado del servicio de Windows. Las opciones incluyen: • Habilitado • Manual • Inhabilitado

Panel Paquetes

Puede encontrar descripciones de parámetros para el panel Paquetes al que se accede desde la página Perfil de activo.

El panel Paquetes se visualiza sólo cuando QRadar Vulnerability Manager está instalado en el sistema. El panel Paquetes en la página Perfil de activo proporciona la información siguiente:

Tabla 41. Parámetros del panel Paquetes

Parámetro	Descripción
Paquetes	Visualiza el nombre del paquete que se aplica al activo.
Versión	Visualiza la versión del paquete que se aplica al activo.

Tabla 41. Parámetros del panel Paquetes (continuación)

Parámetro	Descripción
Revisión	Visualiza la revisión del paquete que se aplica al activo.

Panel Parches de Windows

Puede buscar descripciones de parámetro para el panel Parches de Windows al que accede desde la página Perfil de activo.

El panel Parches de Windows se visualiza solo cuando QRadar Vulnerability Manager está instalado en el sistema. El panel Parches de Windows en la página Perfil de activo proporciona la información siguiente:

Tabla 42. Parámetros de panel Parches de Windows

Parámetro	Descripción
Número de KB de Microsoft	Visualiza el número de Microsoft Knowledge Base (KB) del parche de Windows que se ejecuta en el activo.
Descripción	Visualiza la descripción del parche de Windows.
ID de boletín	Visualiza el número de ID de boletín del parche de Windows.
ID de vulnerabilidad	Visualiza el ID de vulnerabilidad del parche de Windows.
CVE-ID	Visualiza el ID de CVE asociado con el parche de Windows. Si hay más de un ID de CVE asociado con el parche de Windows, pase el ratón por encima del enlace Múltiple para visualizar la lista de ID de CVE. Puede pulsar un enlace ID de CVE para acceder a más información.
Sistema	Visualiza el sistema Windows para el parche.
Service Pack	Visualiza el Service Pack para el parche.

Panel Propiedades

Puede encontrar descripciones de parámetros para el panel Propiedades al que se accede desde la página Perfil de activo. El panel Propiedades se visualiza sólo cuando QRadar Vulnerability Manager está instalado en el sistema.

El panel Propiedades en la página Perfil de activo proporciona la información siguiente:

Tabla 43. Parámetros del panel Propiedades

Parámetro	Descripción
Nombre	Visualiza el nombre de la propiedad de configuración que se ha visto activamente en el activo.
Valor	Visualiza el valor para la propiedad de configuración.

Panel Políticas de riesgo

Puede encontrar descripciones de parámetro para el panel Políticas de riesgo al que se accede desde la página Perfil de activo. El panel Políticas de riesgo solo se visualiza cuando QRadar Vulnerability Manager se ha instalado en el sistema.

El panel Políticas de riesgo de la página Perfil de activo proporciona la información siguiente:

Tabla 44. Parámetros de panel Políticas de riesgo

Parámetro	Descripción
Política	Visualiza el nombre de la política que está asociada con este activo.
Aprobado/Suspendido	Indica si la política tiene un estado de **Aprobado** o **Suspendido**.
Evaluado por última vez	Visualiza la fecha en que se ha evaluado esta política por última vez.

Panel Productos

Puede encontrar descripciones de parámetros para el panel Productos al que se accede desde la página Perfil de activo.

El panel Productos en la página Perfil de activo proporciona la información siguiente:

Tabla 45. Parámetro del panel Productos

Parámetro	Descripción
Producto	Visualiza el nombre del producto que se ejecuta en el activo.
Puerto	Visualiza el puerto que el producto utiliza.
Vulnerabilidad	Visualiza el número de vulnerabilidades que están asociados con este producto.
ID de vulnerabilidad	Visualiza el ID de vulnerabilidad.

Capítulo 11. Gestión de informes

Puede utilizar la pestaña **Informes** para crear, editar, distribuir y gestionar informes.

Unas opciones de creación de informes detalladas y flexibles satisfacen diversos estándares normativos como, por ejemplo, la conformidad con PCI.

Puede crear sus propios informes personalizados o utilizar informes predeterminados. Puede personalizar y cambiar el nombre de informes predeterminados y distribuirlos a otros usuarios.

La pestaña **Informes** puede necesitar un largo periodo de tiempo para renovarse si el sistema incluye muchos informes.

Nota: Si ejecuta Microsoft Exchange Server 5.5, es posible que aparezcan caracteres de tipos no disponibles en la línea del asunto de los informes enviados por correo electrónico. Para resolver este problema, descargue e instale el Service Pack 4 de Microsoft Exchange Server 5.5. Para obtener más información, póngase en contacto con el soporte de Microsoft.

Consideraciones sobre el huso horario

Para asegurarse de que la característica de creación de informes utiliza la fecha y hora correctas para crear informes de datos, la sesión debe estar sincronizada con el huso horario.

Durante la instalación y configuración de los productos de QRadar, se configura el huso horario. Consulte con el administrador para asegurarse de que la sesión de QRadar está sincronizada con el huso horario.

Permisos de la pestaña de informes

Los usuarios administrativos pueden ver todos los informes creados por otros usuarios.

Los usuarios no administrativos solo pueden ver los informes que ellos han creado o los informes compartidos por otros usuarios.

Parámetros de la pestaña de informes

La pestaña **Informes** muestra una lista de informes personalizados y predeterminados.

En la pestaña **Informes**, puede ver información estadística acerca de la plantilla de informes, realizar acciones en las plantillas de informes, ver los informes generados y suprimir el contenido generado.

Si un informe no especifica una planificación de intervalo, debe generar manualmente el informe.

Puede pasar el puntero del ratón sobre cualquier informe para previsualizar un resumen de informe en una ayuda contextual. El resumen especifica la

configuración del informe y el tipo de contenido que genera el informe.

Visión general de la pestaña Informes

Puede crear sus propios informes personalizados o utilizar informes predeterminados. Puede personalizar y cambiar el nombre de informes predeterminados y distribuirlos a otros usuarios.

La pestaña **Informes** puede necesitar un largo periodo de tiempo para renovarse si el sistema incluye muchos informes.

Nota: Si ejecuta Microsoft Exchange Server 5.5, es posible que aparezcan caracteres de tipos no disponibles en la línea del asunto de los informes enviados por correo electrónico. Para resolver este problema, descargue e instale el Service Pack 4 de Microsoft Exchange Server 5.5. Para obtener más información, póngase en contacto con el soporte de Microsoft.

Consideraciones sobre el huso horario

Para asegurarse de que la característica de creación de informes utiliza la fecha y hora correctas para crear informes de datos, la sesión debe estar sincronizada con el huso horario.

Durante la instalación y configuración de los productos de QRadar, se configura el huso horario. Consulte con el administrador para asegurarse de que la sesión de QRadar está sincronizada con el huso horario.

Permisos de la pestaña de informes

Los usuarios administrativos pueden ver todos los informes creados por otros usuarios.

Los usuarios no administrativos solo pueden ver los informes que ellos han creado o los informes compartidos por otros usuarios.

Parámetros de la pestaña de informes

La pestaña **Informes** muestra una lista de informes personalizados y predeterminados.

En la pestaña **Informes**, puede ver información estadística acerca de la plantilla de informes, realizar acciones en las plantillas de informes, ver los informes generados y suprimir el contenido generado.

La pestaña **Informes** proporciona la información siguiente:

Tabla 46. Parámetros de la pestaña de informes

Parámetro	Descripción
Columna Distintivo	Si se ha producido un error, provocando el fallo de la generación, el icono **Error** se visualiza en esta columna.
Nombre de informe	Especifica el nombre del informe.
Grupo	Especifica el grupo al que pertenece este informe.

Tabla 46. Parámetros de la pestaña de informes (continuación)

Parámetro	Descripción
Planificar	Especifica la frecuencia con la que se generó el informe. Los informes que especifican una planificación de intervalo, cuando está habilitada, se generan automáticamente según el intervalo especificado. Si un informe no especifica una planificación de intervalo, debe generar manualmente el informe.
Próxima hora de ejecución	Especifica el tiempo, en horas y minutos hasta que se genera el informe siguiente.
Última modificación	Especifica la última fecha en la que se modificó este informe.
Propietario	Especifica el usuario que posee el informe.
Autor	Especifica el usuario que ha creado el informe.
Informes generados	En el recuadro de lista, selecciona la indicación de la fecha del informe generado que desea ver. Cuando selecciona la indicación de fecha, el parámetro **Formato** visualiza los formatos disponibles para los informes generados. Si no se han generado informes, se visualiza **Ninguno**.
Formatos	Especifica los formatos de informe del informe seleccionado actualmente en la columna Informes generados. Pulse el icono correspondiente al formato que desea ver.

Puede pasar el puntero del ratón sobre cualquier informe para previsualizar un resumen de informe en una ayuda contextual. El resumen especifica la configuración de informe y el tipo de contenido que genera el informe.

Orden de clasificación de la pestaña de informes

De forma predeterminada, los informes están clasificados por la columna **Última modificación**. En el menú **Navegación de informes** los informes están ordenados por la planificación del intervalo.

Para filtrar el informe para que solo muestre informes de una frecuencia específica, pulse la flecha junto al elemento de menú **Informe** del menú de navegación y seleccione la carpeta de grupo (frecuencia).

Barra de herramientas de la pestaña de informes

Puede utilizar la barra de herramientas para realizar una serie de acciones en los informes.

La tabla siguiente identifica y describe las opciones de la barra de herramientas de Informes.

Tabla 47. Opciones de barra de herramientas de Informes

Opción	Descripción
Grupo	

Tabla 47. Opciones de barra de herramientas de Informes (continuación)

Opción	Descripción
Gestionar grupos	Pulse **Gestionar grupos** para gestionar grupos de informes. Mediante el uso de la característica Gestionar grupos, puede organizar los informes en grupos funcionales.
Acciones	Pulse **Acciones** para realizar las acciones siguientes: • **Crear**: Seleccione esta opción para crear un informe nuevo. • **Editar**: Seleccione esta opción para editar el informe seleccionado. También puede efectuar una doble pulsación en un informe para editar el contenido. • **Duplicar**: Seleccione esta opción para duplicar o renombrar el informe seleccionado. • **Asignar grupos**: Seleccione esta opción para asignar el informe seleccionado a un grupo de informes. • **Compartir**: Seleccione esta opción para compartir el informe seleccionado con otros usuarios. Debe tener privilegios administrativos para compartir informes. • **Conmutar planificación**: Seleccione esta opción para conmutar el informe seleccionado al estado Activo o Inactivo. • **Ejecutar informe**: Seleccione esta opción para generar el informe seleccionado. Para generar varios informes, mantenga pulsada la tecla Control y pulse los informes que desea generar. • **Ejecutar informe para datos en bruto**: Seleccione esta opción para generar el informe seleccionado utilizando datos en bruto. Esta opción es útil si desea generar un informe antes de que estén disponibles los datos acumulados necesarios. Por ejemplo, si desea ejecutar un informe semanal antes de que haya transcurrido una semana completa desde que creó el informe, puede generar el informe utilizando esta opción. • **Suprimir informe**: Seleccione esta opción para suprimir el informe seleccionado. Para suprimir varios informes, mantenga pulsada la tecla Control y pulse los informes que desea suprimir. • **Suprimir contenido generado**: Seleccione esta opción para suprimir todo el contenido generado para las filas seleccionadas. Para suprimir varios informes generados, mantenga pulsada la tecla Control y pulse los informes generados que desea suprimir.

Tabla 47. Opciones de barra de herramientas de Informes (continuación)

Opción	Descripción
Ocultar informes inactivos	Seleccione este recuadro de selección para ocultar las plantillas de informes inactivos. La pestaña **Informes** se renueva automáticamente y muestra sólo los informes de activos. Quite la marca del recuadro de selección para mostrar los informes inactivos ocultos.
Buscar en informes	Escriba los criterios de búsqueda en el campo **Buscar en informes** y pulse el icono **Buscar en informes**. Se ejecuta una búsqueda en los parámetros siguientes para determinar cuáles coinciden con los criterios especificados: • Título de informe • Descripción de informe • Grupo de informes • Grupos de informes • Nombre de usuario de autor de informes

Diseño de informe

Un informe puede constar de varios elementos de datos y puede representar datos de red y de seguridad en diversos estilos, tales como tablas, gráficos de línea, gráficos circulares y gráficos de barras.

Al seleccionar el diseño de un informe, tenga en cuenta el tipo de informe que desea crear. Por ejemplo, no elija un contenedor de gráfico pequeño para un contenido de gráfico que muestra muchos objetos. Cada gráfico incluye una leyenda y una lista de redes de las que se deriva el contenido; elija un contenedor suficientemente grande para contener los datos. Para ver previamente cómo visualiza cada gráfico los datos, consulte Tipos de gráfico.

Tipos de gráfico

Cuando se crea un informe, debe elegir un tipo de gráfico para cada gráfico que desea incluir en el informe.

El tipo de gráfico determina cómo presenta el informe generado los datos y objetos de red. Puede crear un gráfico de datos con varias características y crear los gráficos en un único informe generado.

Puede utilizar cualquiera de los tipos de gráficos siguientes:

- **Ninguno**: Utilice esta opción para visualizar un contenedor vacío en el informe. Esta opción puede ser útil para crear espacio en blanco en el informe. Si selecciona la opción **Ninguno** para cualquier contenedor, no es necesario realizar ninguna configuración adicional para dicho contenedor.
- **Vulnerabilidades de activos**: Utilice este gráfico para ver los datos de vulnerabilidad para cada activo definido en el despliegue. Puede generar gráficos de vulnerabilidad de activos cuando una exploración de VA ha detectado vulnerabilidades. Este gráfico está disponible después de instalar IBM Security QRadar Vulnerability Manager.

- **Vulnerabilidades**: La opción Vulnerabilidades sólo se visualiza cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se dispone de licencia para el mismo. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Tipos de gráfico

Cada tipo de diagrama soporta varios tipos de gráfico que puede utilizar para visualizar datos.

Están disponibles los siguientes tipos de gráfico para informes de QRadar Log Manager:

- Gráfico de líneas
- Gráfico de líneas apiladas
- Gráfico de barras
- Gráfico de barras apiladas
- Gráfico circular
- Gráfico de tabla

Para visualizar el contenido en una tabla, debe diseñar un informe con un contenedor de ancho de página completa.

Creación de informes personalizados

Puede utilizar el Asistente de informes para crear un nuevo informe.

Antes de empezar

Debe tener los permisos de red apropiados para compartir un informe generado con otros usuarios.

Para obtener más información sobre los permisos, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.

Acerca de esta tarea

El Asistente de informes proporciona una guía paso a paso sobre cómo diseñar, planificar y generar informes.

El asistente utiliza los siguientes elementos clave para ayudarle a crear un informe:

- **Diseño**: Posición y tamaño de cada contenedor
- **Contenedor**: Marcador para el contenido presentado
- **Contenido**: Definición del gráfico que se coloca en el contenedor

Después de crear un informe que se genera semanal o mensualmente, la hora planificada debe haber transcurrido antes de que el informe generado devuelva resultados. Para un informe planificado, debe esperar el periodo de tiempo planificado para que se creen los resultados. Por ejemplo, una búsqueda semanal necesita siete días para crear los datos. Esta búsqueda no devuelve resultados antes de que hayan transcurrido siete días.

Cuando especifique el formato de salida para el informe, tenga en cuenta que el tamaño de archivo de los informes generados puede tener de uno a dos megabytes, dependiendo del formato de salida seleccionado. El formato PDF es

menor de tamaño y no consume una gran cantidad de espacio de almacenamiento de disco.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el cuadro de lista **Acciones**, seleccione **Crear**.
3. En Bienvenido al Asistente de informes, pulse **Siguiente** para pasar a la página siguiente del Asistente de informes.
4. Seleccione una de las opciones siguientes:

Opción	Descripción
Manualmente	Genera un informe una vez. Este es el valor predeterminado; sin embargo, puede generar este informe tan a menudo como sea necesario.
Cada hora	Planifica que el informe se genere al final de cada hora utilizando los datos de la hora anterior. Si elige la opción Cada hora, se necesita configuración adicional. En los recuadros de lista, seleccione un intervalo de tiempo para empezar y finalizar el ciclo del informe. Se genera un informe para cada hora dentro de este intervalo de tiempo. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m. para los campos **Desde** y **Hasta**.
Semanalmente	Planifica que el informe se genere semanalmente utilizando los datos de la semana anterior. Si elige la opción **Semanalmente**, se necesita configuración adicional. Seleccione el día que desea generar el informe. El valor predeterminado es Lunes. En el recuadro de lista, seleccione una hora para empezar el ciclo del informe. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.
Mensualmente	Planifica el informe para generar mensualmente utilizando los datos del mes anterior. Si elige la opción **Mensualmente**, se necesita configuración adicional. En el recuadro de lista, seleccione la fecha en la que desea generar el informe. El valor predeterminado es el primer día del mes. Asimismo, utilice el recuadro de lista para seleccionar una hora para empezar el ciclo de creación de informes. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.

5. En el panel **Permitir que este informe se genere manualmente**, seleccione **Sí** o **No**.

6. Configure el diseño del informe:
   a. En el recuadro de lista **Orientación**, seleccione la orientación de página: Vertical u Horizontal.
   b. Seleccione una de las seis opciones de diseño que se muestran en el asistente de informes.
   c. Pulse **Siguiente** para pasar a la página siguiente del asistente de informes.
7. Especifique valores para los parámetros siguientes:
   - **Título de informe**: Escriba un título de informe. El título puede tener una longitud máxima de 100 caracteres. No utilice caracteres especiales.
   - **Logotipo**: En el recuadro de lista, seleccione un logotipo.
   -
8. Configure cada contenedor en el informe:
   a. En el recuadro de lista **Tipo de gráfico**, seleccione un tipo de gráfico.
   b. En la ventana Detalles de contenedor - <tipo_gráfico>, configure los parámetros de gráfico.
   c. Pulse **Guardar detalles de contenedor**.
   d. Si es necesario, repita los pasos a a c para todos los contenedores.
   e. Pulse **Siguiente** para pasar a la página siguiente del asistente de informes.
9. Vea previamente la página Vista previa del diseño y, a continuación, pulse **Siguiente** para ir al paso siguiente del asistente de informes.
10. Marque los recuadros de selección para los formatos de informe que desea generar y pulse **Siguiente**.

    Nota: Extensible Markup Language sólo está disponible para tablas.
11. Seleccione los canales de distribución para el informe y, a continuación, pulse **Siguiente**. Las opciones incluyen los siguientes canales de distribución:

Opción	Descripción
Consola de informes	Marque este recuadro de selección para enviar el informe generado a la pestaña **Informes**. Este es el canal de distribución predeterminado.
Seleccione los usuarios que deben poder ver el informe generado.	Esta opción se muestra después de seleccionar el recuadro de selección **Consola de informes**. En la lista de usuarios, seleccione los usuarios a los que desea otorgar permiso para ver los informes generados.
Seleccionar todos los usuarios	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Consola de informes**. Marque este recuadro de selección si desea otorgar permiso a todos los usuarios para ver los informes generados. Debe tener permisos de red apropiados para compartir el informe generado con otros usuarios.
Correo electrónico	Marque este recuadro de selección si desea distribuir el informe generado utilizando el correo electrónico.

Opción	Descripción
Escriba la dirección o direcciones de correo electrónico de destino del informe:	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Correo electrónico**. Escriba la dirección de correo electrónico para cada destinatario de informe generado; separe una lista de direcciones de correo electrónico con comas. El máximo de caracteres para este parámetro es de 255. Los destinatarios de correo electrónico reciben este correo electrónico desde no_reply_reports@qradar.
Incluir informe como archivo adjunto (sólo no HTML)	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Correo electrónico**. Marque este recuadro de selección para enviar el informe generado como un archivo adjunto.
Incluir enlace a consola de informes	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Correo electrónico**. Marque este recuadro de selección para incluir un enlace a la Consola de informes en el correo electrónico.

12. En la página Se está terminando, entre valores para los parámetros siguientes:

Opción	Descripción
Descripción de informe	Escriba una descripción para este informe. La descripción se visualiza en la página Resumen de informe y en el correo electrónico de distribución de informes generados.
Grupos	Seleccione los grupos a los que desea asignar este informe. Para obtener más información sobre grupos, consulte Grupos de informes.
¿Desea ejecutar el informe ahora?	Marque este recuadro de selección si desea generar el informe cuando se complete el asistente. De manera predeterminada, el recuadro de selección aparece seleccionado.

13. Pulse **Siguiente** para ver el resumen de informe.
14. En la página Resumen de informe, seleccione las pestañas disponibles en el informe de resumen para previsualizar la configuración de informe.

Resultados

El informe se genera inmediatamente. Si ha borrado el recuadro de selección **¿Desea ejecutar el informe ahora?** en la página final del asistente, el informe se guarda y se genera a la hora planificada. El título de informe es el título predeterminado para el informe generado. Si reconfigura un informe para entrar título de informe nuevo, el informe se guarda como un informe nuevo con el nombre nuevo; sin embargo, el informe original sigue siendo el mismo.

Tareas de gestión de informes

Puede utilizar la pestaña Informes y el asistente Informes para gestionar informes.

Puede editar, duplicar, compartir y marcar informes. También puede suprimir informes generados.

Edición de un informe

Utilizando el asistente de informes, puede editar cualquier informe personalizado o predeterminado para cambiarlo.

Acerca de esta tarea

Puede utilizar o personalizar un número significativo de informes predeterminados. La pestaña **Informes** predeterminada visualiza la lista de informes. Cada informe captura y visualiza los datos existentes.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Efectúe una doble pulsación en el informe que desea personalizar.
3. En el asistente de informes, cambie los parámetros para personalizar el informe para generar el contenido que necesita.

Resultados

Si vuelve a configurar un informe para entrar un título de informe nuevo, el informe se guarda como un informe nuevo con el nombre nuevo; sin embargo, el informe original sigue siendo el mismo.

Visualización de informes generados

En la pestaña **Informes**, se visualiza un icono en la columna **Formatos** si un informe ha generado contenido. Puede pulsar el icono para ver el informe.

Acerca de esta tarea

Cuando un informe ha generado contenido, la columna **Informes generados** visualiza un recuadro de lista. El recuadro de lista muestra todo el contenido generado, que se organiza por la indicación de fecha y hora del informe. Los informes más recientes se muestran en la parte superior de la lista. Si un informe no tiene ningún contenido generado, se visualiza el valor **Ninguno** en la columna **Informes generados**.

Los iconos que representan el formato del informe generado se visualizan en la columna **Formatos**.

Los informes pueden generarse en los formatos PDF, HTML, RTF, XML y XLS.

Nota: Los formatos XML y XLS sólo están disponibles para los informes que utilizan un formato de tabla de un solo gráfico (vertical u horizontal).

Puede ver sólo los informes a los que se le ha dado acceso desde el administrador. Los usuarios administrativos pueden acceder a todos los informes.

Si utiliza el navegador web Mozilla Firefox y selecciona el formato de informe RTF, el navegador web Mozilla Firefox inicia una nueva ventana de navegador. Este nuevo inicio de ventana es el resultado de la configuración de navegador web Mozilla Firefox y no afecta a QRadar. Puede cerrar la ventana y continuar con la sesión de QRadar.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el recuadro de lista de la columna **Informes generados**, seleccione la indicación de fecha y hora del informe desea ver.
3. Pulse el icono correspondiente al formato que desea ver.

Supresión de contenido generado

Cuando suprime el contenido generado, todos los informes que se han generado a partir de la plantilla de informe se suprimen, pero la plantilla de informe se conserva.

Procedimiento

1. Pulse la pestaña **Informe**.
2. Seleccione los informes para los que desea suprimir el contenido generado.
3. En el recuadro de lista **Acciones**, pulse **Suprimir contenido generado**.

Generación manual de un informe

Un informe puede configurarse para que se genere automáticamente, sin embargo, el usuario puede generar manualmente un informe en cualquier momento.

Acerca de esta tarea

Mientras se genera un informe, la columna Próxima hora de ejecución visualiza uno de los tres mensajes siguientes:

- **Generando**: El informe se está generando.
- **En cola (posición en la cola)**: El informe se pone en cola para generarse. El mensaje indica la posición en la que está el informe en la cola. Por ejemplo, 1 de 3.
- **(x hora(s) x min(s) y seg(s))**: Está planificado que el informe se ejecute. El mensaje es un temporizador de cuenta atrás que especifica cuándo se ejecutará el informe la próxima vez.

Puede seleccionar el icono **Renovar** para renovar la vista, incluida la información de la columna **Próxima hora de ejecución**.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea generar.
3. Pulse **Ejecutar informe**.

Qué hacer a continuación

Una vez que se ha generado el informe, puede ver el informe generado desde la columna Informes generados.

Duplicación de un informe

Para crear un informe que se parezca detenidamente a un informe existente, puede duplicar el informe que desea modelar y, a continuación, personalizarlo.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea duplicar.
3. En el recuadro de lista **Acciones**, pulse **Duplicar**.
4. Escriba un nuevo nombre, sin espacios, para el informe.

Qué hacer a continuación

Puede personalizar el informe duplicado.

Compartición de un informe

Puede compartir informes con otros usuarios. Cuando se comparte un informe, se proporciona una copia del informe seleccionado a otro usuario para editarlo o planificarlo.

Acerca de esta tarea

Las actualizaciones que el usuario realiza en un informe compartido no afectan a la versión original del informe.

Debe tener privilegios administrativos para compartir informes. Además, para que un usuario nuevo vea y acceda a los informes, un usuario administrativo debe compartir todos los informes necesarios con el nuevo usuario.

Sólo puede compartir el informe con los usuarios que tienen el acceso adecuado.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione los informes que desea compartir.
3. En el recuadro de lista **Acciones**, pulse **Compartir**.
4. En la lista de usuarios, seleccione los usuarios con los que desea compartir este informe.

Creación de marca de informes

Para marcar de informes, puede importar logotipos e imágenes específicas. Para marcar informes con logotipos personalizados, debe cargar y configurar los logotipos antes de empezar a utilizar el asistente de informes.

Antes de empezar

Asegúrese de que el gráfico que desea utilizar tiene 144 x 50 píxeles con un fondo en blanco.

Para asegurarse de que el navegador visualice el nuevo logotipo, borre la caché de navegador.

Acerca de esta tarea

La creación de marcas de informe es beneficiosa para la empresa cuando se soporta más de un logotipo. Cuando se carga una imagen, esta imagen se guarda de forma automática en formato PNG (Portable Network Graphic).

Cuando se carga una nueva imagen y se establece la imagen como valor predeterminado, la nueva imagen predeterminada no se aplica a los informes que se han generado anteriormente. Para actualizar el logotipo en informes generados previamente es necesario generar manualmente contenido nuevo desde el informe.

Si carga una imagen que tiene una longitud mayor que la que puede soportar la cabecera del informe, la imagen se redimensiona automáticamente para ajustarse a la cabecera; esto tiene aproximadamente una altura de 50 píxeles.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el menú de navegación, pulse **Creación de una identidad visual**.
3. Pulse **Examinar** para examinar los archivos que están ubicados en el sistema.
4. Seleccione el archivo que contiene el logotipo que desea cargar. Pulse **Abrir**.
5. Pulse **Cargar imagen**.
6. Seleccione el logotipo que desea utilizar como valor predeterminado y pulse **Establecer imagen predeterminada**.

Grupos de informes

Los informes pueden ordenarse en grupos funcionales. Si se categorizan los informes por grupos, puede organizar y buscar informes de forma eficiente.

Por ejemplo, puede ver todos los informes relacionados con la conformidad con el estándar PCIDSS (Payment Card Industry Data Security Standard).

De forma predeterminada, la pestaña **Informes** muestra la lista de todos los informes, sin embargo, puede categorizar los informes en grupos tales como:

- Conformidad
- Ejecutivo
- Orígenes de registro
- Gestión de red
- Seguridad
- VoIP
- Otros

Cuando se crea un informe nuevo, se puede asignar el informe a un grupo existente o crear un grupo nuevo. Debe tener acceso administrativo para crear, editar o suprimir grupos.

Para obtener más información sobre los roles de usuario, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.

Creación de un grupo de informes

Puede crear grupos nuevos.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. Utilizando el árbol de navegación, seleccione el grupo en el que desea crear un nuevo grupo.
4. Pulse **Grupo nuevo**.
5. Escriba valores para los parámetros siguientes:
   - **Nombre**: Escriba el nombre del nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Opcional. Escriba una descripción para este grupo. La descripción puede tener un máximo 255 caracteres de longitud.
6. Pulse **Aceptar**.
7. Para cambiar la ubicación del nuevo grupo, pulse el nuevo grupo y arrastre la carpeta a la nueva ubicación en el árbol de navegación.
8. Cierre la ventana Grupos de informes.

Edición de un grupo

Puede editar un grupo de informes para cambiar el nombre o la descripción.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, seleccione el grupo que desea editar.
4. Pulse **Editar**.
5. Actualice los valores de los parámetros, según sea necesario:
   - **Nombre**: Escriba el nombre del nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Opcional. Escriba una descripción para este grupo. La descripción puede tener un máximo 255 caracteres de longitud. Este campo es opcional.
6. Pulse **Aceptar**.
7. Cierre la ventana Grupos de informes.

Asignar un informe a un grupo

Puede utilizar la opción **Asignar grupos** para asignar un informe a otro grupo.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea asignar a un grupo.
3. En el recuadro de lista **Acciones**, seleccione **Asignar grupos**.
4. En la lista **Grupos de elementos**, seleccione el recuadro de selección del grupo que desee asignar a este informe.
5. Pulse **Asignar grupos**.

Copia de un informe en otro grupo

Utilice el icono **Copiar** para copiar un informe en uno o más grupos de informes.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, seleccione el informe que desea copiar.
4. Pulse **Copiar**.
5. Seleccione el grupo o los grupos en los que desea copiar el informe.
6. Pulse **Asignar grupos**.
7. Cierre la ventana Grupos de informes.

Eliminación de un informe

Utilice el icono **Eliminar** para eliminar un informe de un grupo.

Acerca de esta tarea

Cuando se elimina un informe de un grupo, el informe sigue existiendo en la pestaña **Informes**. El informe no se elimina del sistema.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, vaya a la carpeta que contiene el informe que desea eliminar.
4. En la lista de grupos, seleccione el informe que desea eliminar.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.
7. Cierre la ventana Grupos de informes.

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. Las referencias hechas a productos, programas o servicios IBM IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios IBM. En su lugar se puede utilizar 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 pendientes relacionadas con los temas que se describen 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.

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 suministre de cualquier modo que considere adecuado sin incurrir por ello en ninguna obligación con el remitente.

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido, en algunos casos, el pago de una 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 Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM o cualquier otro acuerdo equivalente entre IBM y el cliente.

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 relativa a productos no IBM se ha obtenido de los distribuidores de dichos productos, de anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad ni otras declaraciones referentes a 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 cambios 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 de International Business Machines Corporation en Estados Unidos o en otros países. Si estas y otras marcas registradas de IBM se marcan en su primera aparición en esta información con un símbolo de marca registrada (® o ™), estos símbolos indican que se tratan de marcas registradas en Estados Unidos o en el Derecho anglosajón (Common Law) por parte de IBM en la fecha de publicación de esta información. Estas marcas registradas también pueden ser marcas registradas o marcas registradas según el derecho consuetudinario en otros países. Puede encontrar una lista actual de marcas registradas de IBM en la Web en: Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java y todas las marcas registradas y los logotipos basados en Java son marcas comerciales o marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y/o en otros países.

Linux es una marca comercial de Linus Torvalds en los Estados Unidos o en otros países.

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

Otros nombres de empresas, productos 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 ofrecido como soluciones de servicio (“Ofertas de software”), pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, ayudar a mejorar la experiencia del usuario final, adaptar 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, incluidos los cookies, para estos fines, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, la sección titulada "Cookies, Web Beacons and Other Technologies" y la declaración "IBM Software Products and Software-as-a-Service Privacy Statement" en http://www.ibm.com/software/info/product-privacy.

Glosario

Este glosario proporciona términos y definiciones para el software de [nombre de producto] y los productos.

En este glosario se utilizan las siguientes referencias cruzadas:

- *Véase* le remite de un término no preferido al término preferido o de un acrónimo o abreviatura a la forma completa.
- *Véase también* le remite a un término relacionado u opuesto.

Para otros términos y definiciones, consulte el sitio web de terminología de IBM (se abre en una ventana nueva).

A

activo Objeto gestionable que se despliega o se tiene previsto desplegar en un entorno operativo.

acumulador
Registro en el que un operando de una operación se puede almacenar y posteriormente sustituir por el resultado de esa operación.

agregación de enlaces
Agrupación de tarjetas de interfaz de red física, como cables o puertos, en una única 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 vuelve a configurar cuando se producen anomalías de nodo o daemon para que las cargas de trabajo se puedan redistribuir en los nodos restantes del clúster.

anomalía
Desviación del comportamiento esperado de la red.

archivo de almacén de confianza
Archivo de base de datos de claves que contiene las claves públicas para 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 vía de acceso entre sistemas abiertos con una calidad de servicio predecible.

captura de contenido
Proceso que captura una cantidad configurable de carga útil y, a continuación, almacena los datos en un registro de flujo.

CIDR Véase Classless Inter-Domain Routing.

cifrado
En seguridad de sistemas, proceso de transformación de datos a un formato ininteligible de manera que los datos originales no se puedan obtener o sólo se puedan obtener utilizando un proceso de decodificación.

Classless Inter-Domain Routing (CIDR)
Método para añadir direcciones de Protocolo Internet (IP) de clase C. Las direcciones se proporcionan a los proveedores de servicios de Internet (ISP) para que las utilicen sus clientes. Las direcciones CIDR reducen el tamaño de las tablas de direccionamiento y hacen que haya más direcciones IP disponibles en las organizaciones.

cliente
Programa de software o sistema que solicita servicios de un servidor.

clúster de alta disponibilidad
Configuración de alta disponibilidad que consta de un servidor primario y un servidor secundario.

código de autenticación de mensaje basado en hash (HMAC)
Código criptográfico que utiliza una función hash críptica y una clave secreta.

Common Vulnerability Scoring System (CVSS)
Sistema de puntuación mediante el cual se mide la gravedad de una vulnerabilidad.

compartimiento administrativo
Recurso de red que se oculta a los usuarios sin privilegios administrativos. Los compartimientos administrativos proporcionan a los administradores acceso a todos los recursos en un sistema de red.

comportamiento
Efectos observables de una operación o suceso, incluidos los 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 en la que un operador puede controlar y observar el funcionamiento del sistema.

contexto de host
Servicio que supervisa los componentes para asegurarse de que cada componente está funcionando como se esperaba.

conversión de direcciones de red (NAT)
En un cortafuegos, conversión de las direcciones seguras del protocolo de 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 bajo nivel y alto nivel 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 de los bytes totales de una aplicación con una IP de origen.

credencial
Conjunto de información que otorga a un usuario o proceso determinados derechos de acceso.

credibilidad
Calificación numérica entre 0 y 10 que se utiliza para determinar la integridad de un suceso o un delito. La credibilidad aumenta a medida que varios orígenes informan el mismo suceso o delito.

CVSS Véase Common Vulnerability Scoring System.

D

datos de carga útil
Datos de aplicación contenidos en un flujo de IP, excluyendo la cabecera y la información administrativa.

delito Mensaje enviado o suceso generado en respuesta a una condición supervisada. Por ejemplo, un delito proporcionará información sobre si una política se ha incumplido o la red está bajo ataque.

destino de reenvío
Uno o varios sistemas de proveedores que reciben datos en bruto y normalizados de orígenes de registro y orígenes de flujo.

destino externo
Dispositivo que está fuera del sitio primario que recibe el flujo de sucesos o datos de un recopilador de sucesos.

DHCP Véase Protocolo de configuración dinámica de hosts.

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 está conectada a la red para recopilar información de vulnerabilidad sobre los activos de la red.

DNS Véase Sistema de nombres de dominio.

DSM Véase Módulo de soporte de dispositivos.

E

exploración en directo
Exploración de vulnerabilidad que genera datos de informe a partir de los resultados de exploración basándose en el nombre de sesión.

explorador
Programa de seguridad automático que busca vulnerabilidades de software dentro de las aplicaciones web.

extensión de origen de registro
Archivo XML que incluye todos los patrones de expresión regular necesarios para identificar y categorizar sucesos de la carga útil de sucesos.

F

falso positivo
Resultado de prueba clasificado como positivo (indicando que el sitio es vulnerable a ataques), que el usuario decide que en realidad es negativo (no una vulnerabilidad).

firma de aplicación
Conjunto exclusivo de características que se derivan mediante el examen de la carga útil de paquete y, a continuación, se utilizan para identificar una aplicación específica.

flujo Transmisión única de datos que pasan a través de un enlace durante una conversación.

flujo duplicado
Varias instancias de la misma transmisión de datos recibida de 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 plantea en un destino.

H

HA Véase alta disponibilidad.

HMAC
Véase Código de autenticación de mensaje basado en hash.

hoja En un árbol, entrada o nodo que no tiene hijos.

host primario de alta disponibilidad
Sistema principal que está conectado al clúster de alta disponibilidad.

host secundario de alta disponibilidad
Sistema en espera que está conectado al clúster de alta disponibilidad. El host secundario de alta disponibilidad asume la responsabilidad del host primario de alta disponibilidad si el host primario de alta disponibilidad falla.

I

ICMP Véase protocolo de mensajes de control de Internet.

identidad
Colección de atributos de un origen de datos que representan una persona, una organización, un lugar o un elemento.

IDS Véase sistema de detección de intrusiones.

informe
En gestión de consultas, datos formateados que se obtienen al ejecutar una consulta y aplicarle un formato.

interconexión de sistemas abiertos (OSI)
Interconexión de sistemas abiertos de acuerdo con los estándares de la ISO (International Organization for Standardization) para el intercambio de información.

interfaz enlazada
Véase agregación de enlaces.

intervalo de fusión
Intervalo en el que se empaquetan los sucesos. El empaquetado de sucesos se produce a intervalos de 10 segundos y empieza con el primer suceso que no coincide con ningún suceso de fusión simultánea. En el intervalo de fusión, los tres primeros sucesos coincidentes se empaquetan y 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 proporcionar acceso a directorios que soportan un modelo X.500, y que no está sujeto a los requisitos de recursos del protocolo de acceso a directorios (DAP) X.500 más complejo. Por ejemplo, se puede utilizar LDAP para localizar personas, organizaciones y otros recursos en un directorio de Internet o de intranet.

Local a local (L2L)
Relativo al tráfico interno de una red local a otra red local.

Local a remoto (L2R)
Relativo al tráfico interno de una red local a otra red remota.

L2R Véase Local a remoto.

L2L Véase Local a local.

M

magistrado
Componente interno que analiza el tráfico de red y los sucesos de seguridad respecto a las reglas personalizadas definidas.

magnitud
Medida de la importancia relativa de un determinado delito. Magnitud es un valor ponderado calculado a partir de pertinencia, gravedad y credibilidad.

máscara de subred
Para la gestión de subredes de internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred de la parte de host de una dirección IP.

Módulo de soporte de dispositivo (DSM)
Archivo de configuración que analiza los sucesos recibidos de varios orígenes de registro y los convierte a un formato de taxonomía estándar que puede visualizarse como salida.

multidifusión IP
Transmisión de un datagrama de Protocolo Internet (IP) para establecer un conjunto de sistemas que forman un grupo de multidifusión único.

N

NAT Véase conversión de direcciones de red.

NetFlow
Protocolo de red Cisco que supervisa datos de flujo de tráfico de red. Los datos de NetFlow incluyen la información de cliente y servidor, los puertos que se utilizan y el número de bytes y paquetes que fluyen a través de los conmutadores y direccionadores conectados a una red. Los datos se envían a recopiladores de NetFlow donde se realiza el análisis de datos.

nombre de dominio completo (FQDN)
En 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 un nombre de red completo es CompanyA.Department.Marketing.

número de sistema autónomo (ASN)
En TCP/IP, número asignado a un sistema autónomo por la misma autoridad central que asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automáticos distingan los sistemas autónomos.

O

objeto de hoja de base de datos
Nodo u objeto de terminal en una jerarquía de base de datos.

objeto de red
Componente de una jerarquía de red.

Open Source Vulnerability Database (OSVDB)
Creado por la comunidad de seguridad de red para la comunidad de seguridad de red, base de datos de código abierto que proporciona información técnica sobre las vulnerabilidades de seguridad de la red.

orden de análisis
Una definición de origen de registro en la que el usuario puede definir el orden de importancia para los orígenes de registro que comparten una dirección IP o un nombre de host comunes.

origen de registro
Equipo de seguridad o equipo de red desde el que se origina une registro de sucesos.

orígenes de flujo
Origen del que se captura el flujo. Un origen de flujo se clasifica como interno cuando el flujo procede del hardware instalado en un host gestionado o se clasifica como externo cuando el flujo se envía a un recopilador de flujo.

origen externo
Dispositivo que está fuera del sitio primario que reenvía datos normalizados a un recopilador de sucesos.

OSI Véase interconexión de sistemas abiertos.

OSVDB
Véase Open Source Vulnerability Database.

P

pasarela
Dispositivo o programa utilizado para conectar redes o sistemas con diferentes arquitecturas de red.

pertinencia
Medida de impacto relativo de un suceso, una categoría o un delito en la red.

peso de red
Valor numérico aplicado a cada red que significa la importancia de la red. El peso de la red lo define el usuario.

protocolo
Conjunto de reglas que controlan la comunicación y la transferencia de datos entre dos o varios dispositivos o sistemas en una red de comunicaciones.

Protocolo de configuración dinámica de hosts (DHCP)
Protocolo de comunicación que se utiliza para gestionar de forma central información de configuración. Por ejemplo, DHCP asigna automáticamente direcciones IP a sistemas de una red.

Protocolo de control de transmisiones (TCP)
Protocolo de comunicación utilizado en Internet y en cualquier red que cumple los estándares de IETF (Internet Engineering Task Force) para el protocolo entre redes. TCP proporciona un protocolo fiable de host a host en las redes de comunicaciones de conmutación de paquetes y en los sistemas interconectados de dichas redes. Véase también Protocolo Internet.

Protocolo de Internet (IP)
Protocolo que direcciona los datos a través de una red o de redes interconectadas. Este protocolo actúa como intermediario entre las capas de protocolo más altas y la red física. Véase también Protocolo de control de transmisiones.

Protocolo de mensajes de control de Internet (ICMP)
Protocolo de Internet utilizado por una pasarela para comunicarse con un host de origen, por ejemplo, para informar 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 simple de gestión de red (SNMP)
Conjunto de protocolos para supervisar sistemas y dispositivos en redes complejas. La información sobre dispositivos gestionados se define y almacena en una MIB (Management Information Base - Base de información de gestión).

proveedor de servicios de Internet (ISP)
Organización que proporciona acceso a Internet.

punto de datos
Valor calculado de una medida en un punto en el tiempo.

punto final
Dirección de una API o un 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 mediante el cual se recopila información que pertenece a la identidad de los recursos de red. Se utilizan técnicas de exploración de red y otras para compilar una lista de sucesos de recursos de red a los que entonces se les asigna un nivel de gravedad.

red de área local (LAN)
Red que conecta varios dispositivos en un área limitada (como un único edificio o campus) y que se puede conectar a una red más grande.

Redirección de ARP
Método 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 a los sistemas identificar relaciones y ejecutar respuestas automáticas como corresponda.

regla de direccionamiento
Condición en la que, cuando los datos de sucesos satisfacen sus criterios, se ejecutan un conjunto de condiciones y el direccionamiento consecuente.

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 un recurso de Internet registrado, por ejemplo nombres de dominio y asignaciones de dirección IP.

sistema activo
En un clúster de alta disponibilidad (HA), sistema que tiene todos los servicios en ejecución.

sistema de detección de intrusiones (IDS)
Software que detecta los intentos o los ataques satisfactorios en los recursos supervisados que forman parte de una red o un 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 denegar la actividad potencialmente maliciosa. Los mecanismos de denegación pueden implicar el filtrado, seguimiento o establecimiento de límites de velocidad.

sistema en espera
Sistema que se activa automáticamente cuando el sistema activo falla. Si se ha habilitado la replicación de disco, replica los 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. Se puede utilizar SOAP para consultar y devolver información e invocar servicios en Internet.

sub-búsqueda
Función que permite realizar una consulta de búsqueda en un conjunto de resultados de búsqueda completada.

subred
Red que se divide en subgrupos independientes más pequeños, que siguen estando interconectados.

subred
Véase subred.

superflujo
Flujo único que consta de varios flujos con propiedades similares con el fin de aumentar la capacidad de proceso reduciendo las restricciones de almacenamiento.

T

tabla de referencia
Tabla donde el registro de datos correlaciona claves que tienen un tipo asignado con otras claves, que a continuación se correlacionan con un único valor.

TCP Véase Protocolo de control de transmisiones.

temporizador de renovación
Dispositivo interno que se desencadena manual o automáticamente a intervalos temporizados que actualiza los datos de actividad de red actuales.

V

violación
Acto que ignora o contraviene la política corporativa.

vista de sistema
Representación visual de hosts primarios y gestionados que componen un sistema.

vulnerabilidad
Exposición de seguridad en un sistema operativo, software de sistema o componente de software de aplicación.

Índice

H

I

L

M

N

O

P

Q

R

S

T

U

V