IBM Security QRadar

Guía del usuario de orígenes de datos

Abril de 2016

Nota

Antes de utilizar esta información y el producto al que sirve de complemento, lea la información contenida en la sección "Avisos" en la página 61.

Información sobre el producto

Este documento es aplicable a IBM QRadar Security Intelligence Platform V7.2.5 y a los releases subsiguientes a menos que sean reemplazados por una versión actualizada de este documento.

Contenido

Acerca de esta guía

Los orígenes de registro son dispositivos de terceros que envían sucesos a IBM® Security QRadar para su recopilación, almacenamiento, análisis y proceso.

Público al que va dirigido este manual

Los administradores deben tener acceso a QRadar y conocer las tecnologías de redes corporativas.

Documentación técnica

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

Para conocer cómo acceder a más documentación técnica de la biblioteca de productos de QRadar, consulte la página web Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Contactar con el servicio de soporte al cliente

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

Declaración de buenas prácticas de seguridad

La seguridad de los sistemas de tecnologías de la información supone proteger los sistemas y la información mediante la prevención, detección y respuesta al acceso no autorizado desde dentro y fuera de la empresa. El acceso no autorizado puede dar como resultado la alteración, destrucción, apropiación indebida o mal uso de la información, y también daños en los sistemas o mal uso de ellos, incluida su utilización para atacar a otros sistemas. Ningún producto o sistema de tecnologías de la información se debe considerar completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo para impedir la utilización o acceso no autorizado. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un sistema de seguridad completo y legítimo, que necesariamente incluye procedimientos operativos adicionales y puede necesitar otros sistemas, productos o servicios para lograr la máxima efectividad. IBM NO GARANTIZA QUE UN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE, O HAGA QUE SU EMPRESA SEA INMUNE, FRENTE A LA CONDUCTA MALICIOSA O ILEGAL DE UN TERCERO CUALQUIERA.

Tenga en cuenta lo siguiente:

El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM Security QRadar solamente se puede utilizar con fines legales y de forma legal. El cliente se compromete a utilizar este programa 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. Visión general de la gestión de orígenes de registro

Puede configurar IBM Security QRadar para aceptar registros de sucesos procedentes de orígenes de registro que se encuentran en la red. Un *origen de registro* es un origen de datos que crea un registro de sucesos.

Por ejemplo, un cortafuegos o sistema de prevención de intrusiones (IPS) registra sucesos de seguridad y conmuta o direcciona sucesos de red.

Para recibir sucesos en bruto procedentes de orígenes de registro, QRadar da soporte a varios protocolos. Los *protocolos pasivos* están a la escucha de sucesos en puertos determinados. Los *protocolos activos* utilizan interfaces de programación de aplicaciones (API) u otros métodos de comunicación para conectar con sistemas externos que sondean y recuperan sucesos.

Dependiendo de los límites de la licencia del producto, QRadar puede leer e interpretar sucesos procedentes de más de 300 orígenes de registro.

Para configurar un origen de registro para QRadar, realice las tareas siguientes:

1. Descargue e instale un módulo de soporte de dispositivo (DSM) que sea compatible con el origen de registro. Un *DSM* es aplicación de software que contiene los patrones de sucesos que son necesarios para identificar y analizar sucesos desde el formato original del registro de sucesos al formato que QRadar puede utilizar. Para obtener más información, sobre los DSM y los orígenes de registro soportados, consulte la *Guía de configuración de DSM*.
2. Si el descubrimiento automático está soportado para el DSM, espere a que QRadar añada automáticamente el origen de registro a la lista de orígenes de registro configurados.
3. Si el descubrimiento automático no está soportado para el DSM, cree manualmente la configuración del origen de registro.

Añadir un origen de registro

Si un origen de registro no se descubre automáticamente, puede añadirlo manualmente para recibir sucesos procedentes de dispositivos de la red.

Acerca de esta tarea

La tabla siguiente describe los parámetros de todos los tipos de orígenes de registro:

Tabla 1. Parámetros de origen de registro

Parámetro	Descripción
Identificador de origen de registro	Dirección IPv4 o nombre de host que identifica el origen de registro. Si la red contiene varios dispositivos que están conectados a una sola consola de gestión, especifique la dirección IP del dispositivo que ha creado el suceso. El especificar un identificador exclusivo, tal como una dirección IP, impide que las búsquedas de sucesos identifiquen la consola de gestión como origen de todos los sucesos.
Habilitado	Cuando esta opción no está habilitada, el origen de registro no recopila sucesos y no se contabiliza para el límite de licencias.
Credibilidad	La credibilidad es una representación de la integridad o validez de los sucesos creados por un origen de registro. El valor de credibilidad que se asigna a un origen de registro puede aumentar o disminuir de acuerdo con los sucesos entrantes o se puede ajustar en respuesta a reglas de suceso creadas por el usuario. La credibilidad de los sucesos de orígenes de registro contribuye al cálculo de la magnitud del delito y puede aumentar o disminuir el valor de magnitud de un delito.
Recopilador de sucesos de destino	Especifica el recopilador de sucesos de QRadar que sondea el origen de registro remoto. Utilice este parámetro en un despliegue distribuido para mejorar el rendimiento del sistema mediante la asignación de la tarea de sondeo a un recopilador de sucesos.
Fusionar sucesos	Aumenta el recuento de sucesos cuando el mismo suceso ocurre varias veces en un intervalo de tiempo corto. Los sucesos fusionados proporcionan una manera de ver y determinar la frecuencia con la que un mismo tipo de suceso aparece en el panel **Actividad de registro**. Cuando esta casilla no está seleccionada, los sucesos se visualizan por separado y no se agrupan. Los orígenes de registro nuevos y descubiertos automáticamente heredan el valor de esta opción tal como está definida en la configuración de **Valores del sistema** en el panel **Administración**. Puede utilizar esta casilla para alterar temporalmente el comportamiento predeterminado de los valores del sistema para un origen de registro individual.

Procedimiento

1. Pulse la pestaña **Admin**.
2. Pulse el icono **Orígenes de registro**.
3. Pulse **Añadir**.
4. Configure los parámetros comunes del origen de registro.
5. Configure los parámetros específicos del protocolo correspondientes al origen de registro.
6. Pulse **Guardar**.
7. En el panel **Admin**, pulse **Desplegar cambios**.

Opciones de configuración del protocolo de API REST Blue Coat Web Security Service

Para recibir sucesos de Blue Coat Web Security Service, configure un origen de registro para utilizar el protocolo de API REST Blue Coat Web Security Service.

El protocolo de API REST Blue Coat Web Security Service consulta la API de sincronización de Blue Coat Web Security Service y recupera de la nube datos de registro forzados recientemente.

La tabla siguiente describe los parámetros específicos del protocolo de API REST Blue Coat Web Security Service:

Tabla 2. Parámetros del protocolo de API REST Blue Coat Web Security Service

Parámetro	Descripción
Nombre de usuario de API	El nombre de usuario de API utilizado para autenticarse en Blue Coat Web Security Service. El nombre de usuario de API se configura a través de Blue Coat Threat Pulse Portal.
Contraseña	La contraseña utilizada para autenticarse en Blue Coat Web Security Service.
Confirmar contraseña	Confirmación del campo **Contraseña**.
Utilizar proxy	Si se configura un proxy, todo el tráfico del origen de registro viaja a través del proxy para que QRadar acceda a Blue Coat Web Security Service. Configure los campos **IP o nombre de host de proxy**, **Puerto de proxy**, **Nombre de usuario de proxy** y **Contraseña de proxy**. Si el proxy no requiere autenticación, puede dejar en blanco los campos **Nombre de usuario de proxy** y **Contraseña deproxy**.
Adquirir automáticamente certificado(s) de servidor	Si selecciona Sí en la lista, QRadar descarga el certificado y empieza a confiar en el servidor de destino.
Recurrencia	Puede especificar cuándo recopila datos el registro. El formato es M/H/D para Meses/Horas/Días. El valor predeterminado es 5 M.
Regulador de EPS	El límite superior para el número máximo de sucesos por segundo (EPS). El valor predeterminado es 5000.

Opciones de configuración del protocolo Cisco NSEL

Para supervisar los flujos de paquetes de NetFlow desde un dispositivo ASA (Adaptive Security Appliance) de Cisco, configure el origen de protocolo NSEL (Network Security Event Logging) de Cisco.

Para integrar Cisco NSEL con QRadar, debe crear manualmente un origen de registro para recibir sucesos de NetFlow. QRadar no descubre ni crea automáticamente orígenes de registro para sucesos de syslog procedentes de Cisco NSEL. Para obtener más información, consulte la *Guía de configuración de DSM*.

La tabla siguiente describe los parámetros específicos del protocolo Cisco NSEL:

Tabla 3. Parámetros del protocolo Cisco NSEL

Parámetro	Descripción
Configuración de protocolo	**Cisco NSEL**
Identificador de origen de registro	Si la red contiene dispositivos que están conectados a una consola de gestión, puede especificar la dirección IP del dispositivo que creó el suceso. El especificar un identificador exclusivo, tal como una dirección IP, impide que las búsquedas de sucesos identifiquen la consola de gestión como origen de todos los sucesos.
Puerto recopilador	Número de puerto UDP que Cisco ASA utiliza para reenviar sucesos de NSEL. QRadar utiliza el puerto 2055 para datos de flujo en recopiladores de QRadar QFlow. Debe asignar un puerto UDP diferente en Cisco Adaptive Security Appliance para NetFlow.

Opciones de configuración del protocolo EMC VMware

Para recibir datos de suceso desde el servicio web VMWare para entornos virtuales, configure un origen de registro para utilizar el protocolo EMC VMWare.

La tabla siguiente describe los parámetros específicos del protocolo EMC VMware:

Tabla 4. Parámetros del protocolo EMC VMware

Parámetro	Descripción
Configuración de protocolo	**EMC VMware**
Identificador de origen de registro	El valor de este parámetro debe coincidir con el parámetro **IP de VMware**.
IP de VMware	Dirección IP del servidor VMWare ESXi, por ejemplo, `1.1.1.1`. El protocolo VMware añade la dirección IP del servidor VMware ESXi junto con HTTPS antes de que el protocolo solicite datos de suceso.

Opciones de configuración del protocolo Forwarded

Para recibir sucesos de otra consola del despliegue, configure un origen de registro para que utilice el protocolo Forwarded.

El protocolo Forwarded se suele utilizar para reenviar sucesos a otra consola de QRadar. Por ejemplo, la Consola A tiene configurada la Consola B como destino externo. Los datos de los orígenes de registro descubiertos automáticamente se reenvían a la Consola B. Los orígenes de registro creados manualmente de la Consola A también se deben añadir como origen de recurso a la Consola B mediante el protocolo Forwarded.

Opciones de configuración del protocolo IBM Tivoli Endpoint Manager SOAP

Para recibir sucesos formateados por Log Extended Event Format (LEEF) desde dispositivos de IBM Tivoli Endpoint Manager, configure un origen de registro que utilice el protocolo IBM Tivoli Endpoint Manager SOAP.

Este protocolo necesita IBM Tivoli Endpoint Manager versión V8.2.x o posterior, y la aplicación Web Reports para Tivoli Endpoint Manager.

El protocolo Tivoli Endpoint Manager SOAP recupera sucesos a intervalos de 30 segundos a través de HTTP o HTTPS. A medida que se recuperan sucesos, IBM Tivoli Endpoint Manager DSM analiza y clasifica los sucesos.

La tabla siguiente describe los parámetros específicos del protocolo IBM Tivoli Endpoint Manager SOAP:

Tabla 5. Parámetros del protocolo IBM Tivoli Endpoint Manager SOAP

Parámetro	Descripción
Configuración de protocolo	**IBM Tivoli Endpoint Manager SOAP**
Utilizar HTTPS	Si es necesario un certificado para conectar con HTTPS, copie los certificados necesarios en el directorio siguiente: `/opt/qradar/conf/trusted_certificates`. Se pueden utilizar certificados que tengan las extensiones de archivo siguientes: `.crt`, `.cert` o `.der`. Copie los certificados en el directorio de certificados de confianza antes de guardar y desplegar el origen de registro.
Puerto SOAP	El número de puerto predeterminado para comunicar con IBM Tivoli Endpoint Manager es 80. Las mayoría de las configuraciones utilizan el puerto 443 para las comunicaciones HTTPS.

Opciones de configuración del protocolo JDBC

QRadar utiliza el protocolo JDBC para recoger información procedente de tablas o vistas que contienen datos de sucesos pertenecientes a varios tipos de bases de datos.

La tabla siguiente describe los parámetros específicos del protocolo JDBC:

Tabla 6. Parámetros del protocolo JDBC

Parámetro	Descripción
Tipo de base de datos	En el cuadro de lista, seleccione el tipo de base de datos que contiene los sucesos.
Nombre de base de datos	El nombre de base de datos debe coincidir con el nombre de base de datos que está especificado en el campo **Identificador de origen de registro**.
Puerto	El puerto de JDBC debe coincidir con el puerto de escucha que está configurado en la base de datos remota. La base de datos debe permitir conexiones TCP entrantes. Si se utiliza una **Instancia de base de datos** con el tipo de base de datos MSDE, los administradores deben en blanco el parámetro **Puerto** en la configuración del origen de registro.
Nombre de usuario	Cuenta de usuario para QRadar en la base de datos.

Tabla 6. Parámetros del protocolo JDBC (continuación)

Parámetro	Descripción
Contraseña	La contraseña necesaria para conectarse a la base de datos.
Confirmar contraseña	La contraseña necesaria para conectarse a la base de datos.
Dominio de autenticación	Se debe configurar un dominio para las bases de datos MSDE que están dentro de un dominio Windows. Si la red no utiliza un dominio, deje en blanco este campo.
Instancia de base de datos	La instancia de base de datos, si es necesaria. Las bases de datos MSDE pueden incluir varias instancias de servidor SQL en un solo servidor. Cuando se utiliza un puerto no estándar para la base de datos o el acceso al puerto 1434 está bloqueado para la resolución de bases de datos SQL, el parámetro **Instancia de base de datos** debe estar en blanco en la configuración del origen de registro.
Consulta predefinida	Opcional.
Nombre de tabla	Nombre de la tabla o vista que incluye los registros de sucesos. El nombre de tabla puede incluir los caracteres especiales siguientes: signo de dólar ($), signo de número (#), subrayado (_), guión corto (-) y punto (.).
Lista de selección	Lista de campos que se deben incluir cuando la tabla busca sucesos. Puede utilizar una lista separada por comas o escribir * para seleccionar todos los campos de la tabla o vista. Si se define una lista separada por comas, la lista debe contener el campo que está definido en el **Campo de comparación**.
Campo de comparación	Campo numérico o de fecha y hora procedente de la tabla o vista que identifica los sucesos de tabla nuevos que se añaden a la tabla entre una consulta y otra. Permite que el protocolo identifique los sucesos que el protocolo sondeó previamente para asegurarse de que no se creen sucesos duplicados.
Utilizar sentencias preparadas	Las sentencias preparadas permiten que el origen de protocolo JDBC configure la sentencia SQL y luego ejecute la sentencia SQL muchas veces con parámetros diferentes. Por motivos de seguridad y rendimiento, la mayoría de las configuraciones de protocolo JDBC pueden utilizar sentencias preparadas.
Fecha y hora de inicio	Si no se define una hora de inicio, el protocolo intenta buscar sucesos después de que se guarde y despliegue la configuración del origen de registro.
Intervalo de sondeo	El intervalo de sondeo predeterminado es 10 segundos.
Regulador de EPS	Número máximo permitido de sucesos por segundo (EPS).
Entorno local de base de datos	Para instalaciones en varios idiomas, utilice el campo **Entorno local de base de datos** para especificar el idioma a utilizar.
Conjunto de códigos de base de datos	Para instalaciones en varios idiomas, utilice el campo **Conjunto de códigos** para especificar el juego de caracteres a utilizar.

Tabla 6. Parámetros del protocolo JDBC (continuación)

Parámetro	Descripción
Utilizar comunicación por conducto	Las conexiones por conducto para bases de datos MSDE requieren que los campos de nombre de usuario y contraseña utilicen un nombre de usuario y contraseña de autenticación de Windows en lugar del nombre de usuario y contraseña de la base de datos. La configuración del origen de registro debe utilizar la conexión por conducto predeterminada en la base de datos MSDE.
Utilizar NTLMv2	Seleccionar la casilla **Utilizar NTLMv2** no interrumpe las comunicaciones para las conexiones MSDE que no necesitan autenticación NTLMv2.
Utilizar cifrado Oracle	La configuración de cifrado e integridad de datos de Oracle también se conoce como Oracle Advanced Security. Si se selecciona, los conexiones JDBC de Oracle requerirán que el servidor dé soporte a valores de cifrado de datos de Oracle similares a los del cliente.
SSL	Marque el recuadro de selección SSL si la conexión da soporte a SSL. Esta opción sólo se muestra para MSDE.

Opciones de configuración de JDBC SiteProtector

Puede configurar orígenes de registro para utilizar el protocolo Java™ Database Connectivity (JDBC) SiteProtector a fin de sondear de forma remota bases de datos IBM Proventia® Management SiteProtector® en busca de sucesos.

El protocolo JDBC - SiteProtector combina información de las tablas SensorData1 y SensorDataAVP1 en la creación de la carga útil de origen de registro. Las tablas SensorData1 y SensorDataAVP1 residen en la base de datos IBM Proventia® Management SiteProtector®. El número máximo de filas que el protocolo JDBC - SiteProtector puede sondear en una sola consulta es 30.000 filas.

La tabla siguiente describe los parámetros específicos del protocolo JDBC - SiteProtector:

Tabla 7. Parámetros del protocolo JDBC - SiteProtector

Parámetro	Descripción
Configuración de protocolo	**JDBC - SiteProtector**
Tipo de base de datos	En la lista, seleccione **MSDE** como tipo de base de datos que se debe utilizar para el origen de registro.
Nombre de base de datos	Escriba `RealSecureDB` para el nombre de la base de datos a la que se puede conectar el protocolo.
IP o nombre de host	Dirección IP o nombre de host del servidor de bases de datos.
Puerto	Número de puerto que es utilizado por el servidor de bases de datos. El puerto de la configuración de JDBC SiteProtector debe coincidir con el puerto de escucha. La base de datos debe permitir conexiones TCP entrantes. Si define una **Instancia de base de datos** y utiliza MSDE como tipo de base de datos, debe dejar en blanco el parámetro **Puerto** en la configuración del origen de registro.

Tabla 7. Parámetros del protocolo JDBC - SiteProtector (continuación)

Parámetro	Descripción
Nombre de usuario	Si desea hacer un seguimiento del acceso a una base de datos mediante el protocolo JDBC, puede crear un usuario específico para el sistema QRadar.
Dominio de autenticación	Si selecciona MSDE y la base de datos está configurada para Windows, debe definir un dominio Windows. Si la red no utiliza un dominio, deje en blanco este campo.
Instancia de base de datos	Si selecciona MSDE y tiene varias instancias de servidor SQL en un mismo servidor, defina la instancia con la que desee conectar. Si utiliza un puerto no estándar en la configuración de base de datos, o el acceso al puerto 1434 está bloqueado para la resolución de bases de datos SQL, debe dejar en blanco el parámetro **Instancia de base de datos** en la configuración.
Consulta predefinida	Consulta de base de datos predefinida para el origen de registro. Las consultas de base de datos predefinidas solamente se pueden utilizar para conexiones de origen de registro especiales.
Nombre de tabla	`SensorData1`
Nombre de vista AVP	`SensorDataAVP`
Nombre de vista de respuesta	`SensorDataResponse`
Lista de selección	Escriba `*` para incluir todos los campos de la tabla o vista.
Campo de comparación	`SensorDataRowID`
Utilizar sentencias preparadas	Las sentencias preparadas permiten que el origen de protocolo JDBC configure la sentencia SQL y luego ejecute la sentencia SQL muchas veces con parámetros diferentes. Por motivos de seguridad y rendimiento, utilice sentencias preparadas. Puede deseleccionar esta casilla para utilizar un método alternativo de consulta que no utiliza sentencias precompiladas.
Incluir sucesos de auditoría	Especifica que se deben recopilar sucesos de auditoría de IBM SiteProtector®.
Fecha y hora de inicio	Opcional. Fecha y hora en que el protocolo puede comenzar a sondear la base de datos.
Intervalo de sondeo	Periodo de tiempo entre consultas a la tabla de sucesos. Puede definir un intervalo de sondeo mayor añadiendo una H (de horas) o una M (de minutos) al valor numérico. Los valores numéricos sin el indicador H ni M denotan un intervalo de sondeo en segundos.
Regulador de EPS	Número máximo de sucesos por segundo (EPS) que el protocolo no debe sobrepasar.
Entorno local de base de datos	Para instalaciones en varios idiomas, utilice el campo **Entorno local de base de datos** para especificar el idioma a utilizar.
Conjunto de códigos de base de datos	Para instalaciones en varios idiomas, utilice el campo **Conjunto de códigos** para especificar el juego de caracteres a utilizar.

Tabla 7. Parámetros del protocolo JDBC - SiteProtector (continuación)

Parámetro	Descripción
Utilizar comunicación por conducto	Si selecciona MSDE como tipo de base de datos, seleccione la casilla para utilizar un método alternativo para una conexión de puerto TCP/IP. Cuando utiliza una conexión por conducto, el nombre de usuario y la contraseña deben ser un nombre de usuario y contraseña adecuados de autenticación de Windows en lugar del nombre de usuario y contraseña de la base de datos. La configuración del origen de registro debe utilizar la conexión por conducto predeterminada.
Nombre de clúster de base de datos	Nombre de clúster para asegurarse de que las comunicaciones por conducto funcionan correctamente.
Utilizar NTLMv2	Obliga a que las conexiones MSDE utilicen el protocolo NTLMv2 con los servidores SQL que necesitan autenticación NTLMv2. Seleccionar la casilla **Utilizar NTLMv2** no interrumpe las comunicaciones para las conexiones MSDE que no necesitan autenticación NTLMv2.
Utilizar SSL	Permite el cifrado SSL para el protocolo JDBC.
Idioma del origen de registro	Seleccione el idioma de los sucesos que son generados por el origen de registro. El idioma del origen de registro ayuda al sistema a analizar sucesos de dispositivos externos o sistemas operativos que puede crear sucesos en varios idiomas.

Opciones de configuración del protocolo Juniper Networks NSM

Para recibir registros de sucesos de Juniper Networks NSM y Juniper Networks Secure Service Gateway (SSG), configure un origen de registro para utilizar el protocolo Juniper Networks NSM.

La tabla siguiente describe los parámetros específicos del protocolo Juniper Networks NSM:

Tabla 8. Parámetros del protocolo Juniper Networks NSM

Parámetro	Descripción
Tipo de origen de registro	**Juniper Networks Network y Security Manager**
Configuración de protocolo	**Juniper NSM**

Opciones de configuración del protocolo Juniper Security Binary Log Collector

Puede configurar un origen de registro para utilizar el protocolo Security Binary Log Collector. Cuando se utiliza este protocolo, los dispositivos Juniper pueden enviar sucesos de auditoría, sucesos del sistema, sucesos de cortafuegos y sucesos del sistema de prevención de intrusiones (IPS) en formato binario a QRadar.

El formato de registro binario de los dispositivos Juniper SRX o J Series se canaliza mediante el protocolo UDP. Debe especificar un puerto exclusivo para canalizar sucesos con formato binario. El puerto syslog estándar 514 no se puede utilizar para sucesos con formato binario. El puerto predeterminado que está asignado para recibir sucesos binarios de dispositivos Juniper es el puerto 40798.

La tabla siguiente describe los parámetros específicos del protocolo Juniper Security Binary Log Collector:

Tabla 9. Parámetros del protocolo Juniper Security Binary Log Collector

Parámetro	Descripción
Configuración de protocolo	**Security Binary Log Collector**
Ubicación del archivo de plantilla XML	Vía de acceso del archivo XML que se utiliza para decodificar la secuencia de datos binarios procedente del dispositivo Juniper SRX o Juniper J Series. De forma predeterminada, el módulo de soporte de dispositivo (DSM) incluye un archivo XML para decodificar la secuencia de datos binarios. El archivo XML reside en el directorio siguiente: `/opt/qradar/conf/security_log.xml`.

Opciones de configuración del protocolo de archivo de registro

Para recibir sucesos de hosts remotos, configure un origen de registro para utilizar el protocolo de archivo de registro.

El protocolo de archivo de registro está pensado para sistemas que escriben registros de sucesos diariamente. No es apropiado utilizar el protocolo de archivo de registro para dispositivos que añaden información a sus archivos de sucesos.

Los archivos de registro se recuperan de uno en uno. El protocolo de archivo de registro puede manejar texto sin formato, archivos comprimidos o archivadores. Los archivadores deben contener archivos de texto sin formato que se pueden procesar una línea cada vez. Cuando el protocolo de archivo de registro descarga un archivo de suceso, la información recibida en el archivo actualiza el panel **Actividad de registro**. Si se escribe más información en el archivo después de terminar la descarga, la información añadida no se procesa.

La tabla siguiente describe los parámetros específicos del protocolo de archivos de registro:

Tabla 10. Parámetros de protocolo de archivo de registro

Parámetro	Descripción
Configuración de protocolo	**Archivo de registro**
Puerto remoto	Si el host remoto utiliza un número de puerto no estándar, debe ajustar el valor de puerto para recuperar sucesos.
Archivos de claves SSH	Vía de acceso del archivo de claves SSH, si el sistema está configurado para utilizar la autenticación de clave. Cuando se utiliza un archivo de claves SSH, el campo **Contraseña remota** no se tiene en cuenta.
Directorio remoto	Para FTP, si los archivos de registro residen en el directorio de inicio del usuario remoto, puede dejar en blanco el campo de directorio remoto. Un campo de directorio remoto en blanco da soporte a sistemas en los que el mandato Cambiar directorio de trabajo (CWD) está restringido.

Tabla 10. Parámetros de protocolo de archivo de registro (continuación)

Parámetro	Descripción
Recursivo	Habilite este recuadro de selección para permitir que las conexiones FTP o SFTP realicen búsquedas de datos de sucesos recursivamente en las subcarpetas del directorio remoto. Los datos recopilados de las subcarpetas dependen de las coincidencias con la expresión regular en el Patrón de archivo FTP. La opción **Recursivo** no está disponible para conexiones SCP.
Patrón de archivo FTP	Expresión regular (regex) necesaria para identificar los archivos que se deben descargar desde el host remoto.
Modalidad de transferencia FTP	Para las transferencias ASCII mediante FTP, debe seleccionar `NONE` en el campo **Procesador** y `LINEBYLINE` en el campo **Generador de sucesos**.
Recurrencia	Intervalo de tiempo que determina la frecuencia con que se explora el directorio remoto en busca de nuevos archivos de registro de sucesos. El intervalo de tiempo puede incluir valores en horas (H), minutos (M) o días (D). Por ejemplo, una recurrencia de 2H explora el directorio remoto cada 2 horas.
Ejecutar al guardar	Inicia la importación del archivo de registro inmediatamente después de guardar la configuración del origen de registro. Cuando se selecciona esta casilla, se borra la lista de archivos descargados y procesados anteriormente. Después de la importación del primer archivo, el protocolo de archivo de registro sigue la planificación de hora de inicio y recurrencia que ha definido el administrador.
Regulador de EPS	Número de sucesos por segundo (EPS) que el protocolo no puede sobrepasar.
¿Cambiar directorio local?	Cambia el directorio local en el **Recopilador de sucesos de destino** para almacenar registros de sucesos antes de que se procesen.
Directorio local	Directorio local en el **Recopilador de sucesos de destino**. El directorio debe existir para que el protocolo de archivo de registro pueda intentar recuperar sucesos.
Codificación de archivo	Codificación de caracteres que es utilizada por en los sucesos contenidos en el archivo de registro.
Separador de carpetas	Carácter que se utiliza para separar carpetas del sistema operativo. La mayoría de las configuraciones pueden utilizar el valor predeterminado del campo **Separador de carpetas**. Este campo está pensado para los sistemas operativos que utilizan un carácter diferente para separar carpetas. Por ejemplo, los puntos que separan carpetas en sistemas principales.

Opciones de configuración del protocolo Microsoft DHCP

Para recibir sucesos de servidores Microsoft DHCP, configure un origen de registro para que utilice el protocolo Microsoft DHCP.

Para leer los archivos de registro, las vías de acceso a carpeta que contienen un recurso compartido administrativo (C$) necesitan privilegios NetBIOS para el

recurso compartido administrativo (C$). Los administradores locales o de dominio tiene privilegios suficientes para acceder a los archivos de registro en recursos compartidos administrativos.

Los campos del protocolo Microsoft DHCP que son compatibles con vías de acceso de archivo permiten que los administradores definan una letra de unidad junto con la vía de acceso. Por ejemplo, el campo puede contener el directorio `c$/LogFiles/` para un recurso compartido administrativo, o el directorio `LogFiles/` para una vía de acceso de carpeta de recurso compartido público, pero no puede contener el directorio `c:/LogFiles`.

Restricción: El protocolo de autenticación Microsoft NTLMv2 no es compatible con el protocolo Microsoft DHCP.

La tabla siguiente describe los parámetros específicos del protocolo Microsoft DHCP:

Tabla 11. Parámetros del protocolo Microsoft DHCP

Parámetro	Descripción
Configuración de protocolo	**Microsoft DHCP**
Dominio	Opcional.
Vía de acceso a carpeta	Vía de acceso de los archivos de registro de DHCP.
Patrón de archivo	Expresión regular (regex) que identifica registros de sucesos. Los archivos de registro deben contener una abreviatura correspondiente a un día de la semana y formada por tres caracteres. Utilice uno de los patrones de archivo siguientes: • Patrón de archivo para IPv4: `DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`. • Patrón de archivo para IPv6: `DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`. • Patrón de archivo mixto para IPv4 e IPv6: `Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) \.log`.

Opciones de configuración del protocolo Microsoft Exchange

Para recibir sucesos de servidores de SMTP, OWA y Microsoft Exchange 2007 y 2010, configure un origen de registro para que utilice el protocolo Microsoft Windows Exchange.

Para leer los archivos de registro, las vías de acceso a carpeta que contienen un recurso compartido administrativo (C$) necesitan privilegios NetBIOS para el recurso compartido administrativo (C$). Los administradores locales o de dominio tiene privilegios suficientes para acceder a los archivos de registro en recursos compartidos administrativos.

Los campos del protocolo Microsoft Exchange que son compatibles con vías de acceso de archivo permiten que los administradores definan una letra de unidad junto con la vía de acceso. Por ejemplo, el campo puede contener el directorio `c$/LogFiles/` para un recurso compartido administrativo, o el directorio `LogFiles/` para una vía de acceso de carpeta de recurso compartido público, pero no puede contener el directorio `c:/LogFiles`.

Importante: El protocolo Microsoft Exchange no es compatible con Microsoft Exchange 2003 ni con el protocolo de autenticación Microsoft NTLMv2.

La tabla siguiente describe los parámetros específicos del protocolo Microsoft Exchange:

Tabla 12. Parámetros del protocolo Microsoft Exchange

Parámetro	Descripción
Configuración de protocolo	**Microsoft Exchange**
Dominio	Opcional.
vía de acceso de carpeta del archivo de registro de SMTP	Cuando la vía de acceso de carpeta está vacía, la recopilación de sucesos SMTP está inhabilitada.
Vía de acceso de carpeta del archivo de registro de OWA	Cuando la vía de acceso de carpeta está vacía, la recopilación de sucesos OWA está inhabilitada.
Vía de acceso de carpeta del archivo de registro de MSGTRK	Se puede utilizar el seguimiento de mensajes en los servidores de Microsoft Exchange 2007 o 2010 que tienen asignado el rol de servidor de Hub Transport, Mailbox o Edge Transport.
Patrón de archivo	Expresión regular (regex) que identifica los registros de sucesos. El valor predeterminado es `.*\.(?:log|LOG)`.
Forzar lectura de archivo	Si se deselecciona la casilla, el archivo de registro solamente se lee cuando QRadar detecta un cambio en la hora o tamaño de archivo.
Regulador (sucesos/segundo)	Número máximo de sucesos que el protocolo Exchange puede reenviar por segundo.

Opciones de configuración del protocolo Microsoft IIS

Puede configurar un origen de registro para que utilice el protocolo Microsoft IIS. Este protocolo permite utilizar un punto de recogida individual para archivos de registro con formato W3C que residen en un servidor web de Microsoft IIS.

Para leer los archivos de registro, las vías de acceso a carpeta que contienen un recurso compartido administrativo (C$) necesitan privilegios NetBIOS para el recurso compartido administrativo (C$). Los administradores locales o de dominio tiene privilegios suficientes para acceder a los archivos de registro en recursos compartidos administrativos.

Los campos del protocolo Microsoft IIS que son compatibles con vías de acceso de archivo permiten que los administradores definan una letra de unidad junto con la vía de acceso. Por ejemplo, el campo puede contener el directorio `c$/LogFiles/` para un recurso compartido administrativo, o el directorio `LogFiles/` para una vía de acceso de carpeta de recurso compartido público, pero no puede contener el directorio `c:/LogFiles`.

Restricción: El protocolo de autenticación Microsoft NTLMv2 no es compatible con el protocolo Microsoft IIS.

La tabla siguiente describe los parámetros específicos del protocolo Microsoft IIS:

Tabla 13. Parámetros del protocolo Microsoft IIS

Parámetro	Descripción
Configuración de protocolo	**Microsoft IIS**

Tabla 13. Parámetros del protocolo Microsoft IIS (continuación)

Parámetro	Descripción
Patrón de archivo	Expresión regular (regex) que identifica los registros de sucesos.
Regulador (sucesos/segundo)	Número máximo de sucesos que el protocolo IIS puede reenviar por segundo.

Opciones de configuración del protocolo Microsoft Security Event Log

Puede configurar un origen de registro para utilizar el protocolo Microsoft Security Event Log. Puede utilizar Microsoft Windows Management Instrumentation (WMI) para recopilar registros de sucesos personalizados o registros de sucesos de Windows sin agente.

La API de WMI necesita que las configuraciones de cortafuegos acepten comunicaciones externas entrantes en el puerto 135 y en cualquier puerto dinámico que sea necesario para DCOM. La lista siguiente describe las limitaciones referentes a los orígenes de registro cuando utiliza el protocolo Microsoft Security Event Log:

- Los sistemas con más de 50 sucesos por segundo pueden sobrepasar las capacidades de este protocolo. Utilice WinCollect para los sistemas con más de 50 sucesos por segundo.
- Una instalación completa de QRadar puede soportar hasta 250 orígenes de registro mediante el protocolo Microsoft Security Event Log.
- Los recopiladores de sucesos dedicados pueden soportar hasta 500 orígenes de registro mediante el protocolo Microsoft Security Event Log.

El protocolo Microsoft Security Event Log no está recomendado para servidores remotos a los que se accede mediante enlaces de red, por ejemplo, sistemas que tienen tiempos de respuesta altos, tales como redes WAN lentas. Para verificar los tiempos de respuesta, examine el tiempo de solicitud y de respuesta que hay entre pings de servidor. Los retardos de red producidos por conexiones lentas reducen el número de sucesos por segundo (EPS) que pueden llegar a esos servidores remotos. Además, la recopilación de sucesos procedentes de servidores o controladores de dominio ocupados depende de tiempos de respuesta bajos para seguir el ritmo de los sucesos entrantes. Si no puede reducir el tiempo de respuesta de la red, puede utilizar WinCollect para procesar sucesos de Windows.

El protocolo Microsoft Security Event Log soporta las versiones de software siguientes con la API de Microsoft Windows Management Instrumentation (WMI):

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R3
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7

La tabla siguiente describe los parámetros específicos del protocolo Microsoft Security Event Log:

Tabla 14. Parámetros del protocolo Microsoft Security Event Log

Parámetro	Descripción
Configuración de protocolo	**Windows Security Event Log**

Opciones de configuración del protocolo MQ

Para recibir mensajes de un servicio de cola de mensajes (MQ), configure un origen de registro para utilizar el protocolo MQ. El nombre del protocolo aparece en IBM Security QRadar como **MQ JMS**.

IBM MQ está soportado.

El protocolo MQ puede supervisar varias colas de mensajes, hasta un máximo de 50 por origen de registro.

La tabla siguiente describe los parámetros específicos del protocolo MQ:

Tabla 15. Parámetros del protocolo MQ

Parámetro	Descripción
Nombre del protocolo	**MQ JMS**
IP o nombre de host	La dirección IP o el nombre de host del gestor de colas primario.
Puerto	El puerto predeterminado utilizado para comunicar con el gestor de colas primario es 1414.
IP o nombre de host en espera	La dirección IP o el nombre de host del gestor de colas en espera.
Puerto de espera	El puerto que se utiliza para comunicar con el gestor de colas en espera.
Gestor de colas	El nombre del gestor de colas.
Canal	El canal a través del cuál el gestor de colas envía mensajes. El canal predeterminado es `SYSTEM.DEF.SVRCONN`.
Cola	La cola o la lista de colas a supervisar. Una lista de colas se especifica con una lista separada por comas.
Nombre de usuario	El nombre de usuario utilizado para autenticar con el servicio MQ.
Contraseña	**Opcional:** La contraseña utilizada para autenticar con el servicio MQ.
Regulador de EPS	El límite superior para el número máximo de sucesos por segundo (EPS).
Codificación de mensaje entrante	Codificación de caracteres utilizada por los mensajes entrantes.

Opciones de configuración del protocolo de API REST Okta

Para recibir sucesos de Okta, configure un origen de registro para utilizar el protocolo de API REST Okta.

El protocolo de API REST Okta consulta los puntos finales de la API de sucesos y usuarios de Okta para recuperar información acerca de las acciones realizadas por los usuarios de una organización.

La tabla siguiente describe los parámetros específicos del protocolo Okta de API REST:

Tabla 16. Parámetros del protocolo de API REST Okta

Parámetro	Descripción
IP o nombre de host	oktaprise.okta.com
Señal de autenticación	Una única señal de autenticación generada por la consola de Okta y que debe utilizarse para todas las transacciones de API.
Utilizar proxy	Si se configura un proxy, todo el tráfico del origen de registro viaja a través del proxy para que QRadar acceda a Okta. Configure los campos **IP o nombre de host de proxy**, **Puerto de proxy**, **Nombre de usuario de proxy** y **Contraseña de proxy**. Si el proxy no requiere autenticación, puede dejar en blanco los campos **Nombre de usuario de proxy** y **Contraseña de proxy**.
Adquirir automáticamente certificado(s) de servidor	Si selecciona **Sí** en la lista, QRadar descarga el certificado y empieza a confiar en el servidor de destino.
Recurrencia	Puede especificar cuándo recopila datos el origen de registro. El formato es M/H/D para Meses/Horas/Días. El valor predeterminado es 1 M.
Regulador de EPS	El límite máximo para el número de sucesos por segundo (EPS).

Opciones de configuración del protocolo OPSEC/LEA

Para recibir sucesos en el puerto 18184, configure un origen de registro para utilizar el protocolo OPSEC/LEA.

La tabla siguiente describe los parámetros específicos del protocolo OPSEC/LEA:

Tabla 17. Parámetros del protocolo OPSEC/LEA

Parámetro	Descripción
Configuración de protocolo	**OPSEC/LEA**
Puerto de servidor	Debe verificar que QRadar se puede comunicar en el puerto 18184 mediante el protocolo OPSEC/LEA.
Intervalo de informe estadístico	Intervalo, en segundos, durante el cual se registran sucesos de syslog en el archivo `qradar.log`.
Atributo SIC del objeto de aplicación OPSEC (Nombre de SIC)	El nombre de SIC (Secure Internal Communications) es el nombre distinguido de la aplicación, por ejemplo: `CN=LEA, o=fwconsole..7psasx`.
Atributo SIC de origen de registro (Nombre de SIC de entidad)	Nombre de SIC del servidor, por ejemplo: `cn=cp_mgmt,o=fwconsole..7psasx`.
Aplicación OPSEC	Nombre de la aplicación que realiza la solicitud de certificado.

Importante: Después de una actualización, si recibe el mensaje de error **No se puede extraer el certificado SSL**, siga estos pasos:

1. Quite la marca del recuadro de selección **Especificar certificado**.

2. Vuelva a especificar la contraseña para **Recuperar contraseña de certificado**.

Opciones de configuración del protocolo Oracle Database Listener

Para recopilar de forma remota archivos de registro producidos por un servidor de bases de datos Oracle, configure un origen de registro para utilizar el protocolo Oracle Database Listener.

Antes de configurar el protocolo Oracle Database Listener para supervisar archivos de registro para su proceso, debe obtener la vía de acceso de los archivos de registro de la base de datos Oracle.

La tabla siguiente describe los parámetros específicos del protocolo Oracle Database Listener:

Tabla 18. Parámetros del protocolo Oracle Database Listener

Parámetro	Descripción
Configuración de protocolo	**Oracle Database Listener**
Patrón de archivo	Expresión regular (regex) que identifica los registros de sucesos.

Opciones de configuración del protocolo PCAP Syslog Combination

Para recopilar sucesos procedentes de dispositivos de Juniper Networks SRX Series que reenvían datos de captura de paquetes, configure un origen de registro para utilizar el protocolo PCAP Syslog Combination.

Antes de configurar un origen de registro que utiliza el protocolo PCAP Syslog Combination, determine el puerto de PCAP saliente que está configurado en el dispositivo de Juniper Networks SRX. Los datos de PCAP no se pueden reenviar al puerto 514.

La tabla siguiente describe los parámetros específicos del protocolo PCAP Syslog Combination:

Tabla 19. Parámetros del protocolo PCAP Syslog Combination

Parámetro	Descripción
Configuración de protocolo	**PCAP Syslog Combination**
Puerto de PCAP entrante	Si el puerto de PCAP saliente se edita en el dispositivo de Juniper Networks SRX Series, debe editar el origen de registro para actualizar el puerto de PCAP entrante. Después de editar el campo **Puerto de PCAP entrante**, debe desplegar los cambios.

Opciones de configuración del protocolo SDEE

Puede configurar un origen de registro para utilizar el protocolo Security Device Event Exchange (SDEE). QRadar utiliza este protocolo para recopilar sucesos procedentes de dispositivos que utilizan servidores SDEE.

La tabla siguiente describe los parámetros específicos del protocolo SDEE:

Tabla 20. Parámetros del protocolo SDEE

Parámetro	Descripción
Configuración de protocolo	**SDEE**
URL	URL de HTTP o HTTPS que es necesario para acceder al origen de registro, por ejemplo, https://www.mysdeeserver.com/cgi-bin/sdee-server. Para SDEE/CIDEE (Cisco IDS v5.x y posterior), el URL debe finalizar con `/cgi-bin/sdee-server`. Para administradores con RDEP (Cisco IDS v4.x), el URL debe finalizar con `/cgi-bin/event-server`.
Forzar suscripción	Cuando se selecciona esta casilla, el protocolo obliga al servidor a cerrar la conexión menos activa y aceptar una nueva conexión de suscripción SDEE para el origen de registro.
Espera máxima para bloquear sucesos	Cuando se realiza una solicitud de recopilación y no hay nuevos sucesos disponibles, el protocolo permite un bloqueo de sucesos. El bloqueo impide que se realice otra solicitud de sucesos a un dispositivo remoto que no tiene sucesos nuevos. Este tiempo de espera está pensado para ahorrar recursos del sistema.

Opciones de configuración del protocolo SMB Tail

Puede configurar un origen de registro para utilizar el protocolo SMB Tail. Utilice este protocolo para observar sucesos en un recurso compartido Samba remoto y recibir sucesos del recurso compartido Samba cuando se añadan nuevas líneas al registro de sucesos.

La tabla siguiente describe los parámetros específicos del protocolo SMB Tail:

Tabla 21. Parámetros del protocolo SMB Tail

Parámetro	Descripción
Configuración de protocolo	**SMB Tail**
Vía de acceso de carpeta de archivos de registro	Vía de acceso de los archivos de registro. Por ejemplo, los administradores pueden utilizar el directorio `c$/LogFiles/` para un recurso compartido administrativo, o el directorio `LogFiles/` para una vía de acceso de recurso compartido público. Pero el directorio `c:/LogFiles` no se puede utilizar como vía de acceso de archivos de registro. Si una vía de acceso de archivos de registro contiene un recurso compartido administrativo (C$), los usuarios con acceso NetBIOS para el recurso compartido administrativo (C$) tienen los privilegios necesarios para leer los archivos de registro. También son suficientes los privilegios de administrador del sistema local o de administrador de dominio para acceder a los archivos de registro que residen en un recurso compartido administrativo.
Patrón de archivo	Expresión regular (regex) que identifica los registros de sucesos.
Forzar lectura de archivo	Si se deselecciona la casilla, el archivo de registro solamente se lee cuando QRadar detecta un cambio en la hora o tamaño de archivo.

Tabla 21. Parámetros del protocolo SMB Tail (continuación)

Parámetro	Descripción
Regulador (sucesos/segundo)	Número máximo de sucesos que el protocolo SMB Tail reenvía por segundo.

Opciones de configuración del protocolo SNMPv2

Puede configurar un origen de registro para utilizar el protocolo SNMPv2 para recibir sucesos de SNMPv2.

La tabla siguiente describe los parámetros específicos del protocolo SNMPv2:

Tabla 22. Parámetros del protocolo SNMPv2

Parámetro	Descripción
Configuración de protocolo	**SNMPv3**
Comunidad	Nombre de comunidad de SNMP que es necesario para acceder al sistema que contiene sucesos de SNMP.
Incluir los OID en la carga útil de suceso	Especifica que la carga útil de suceso SNMP se construye mediante pares nombre-valor en lugar del formato de carga útil de suceso. Cuando selecciona orígenes de registro específicos en la lista **Tipos de orígenes de registro**, son necesarios los OID de la carga de útil de suceso para procesar sucesos de SNMPv2 o SNMPv3.

Opciones de configuración del protocolo SNMPv3

Puede configurar un origen de registro para utilizar el protocolo SNMPv3 para recibir sucesos de SNMPv3.

La tabla siguiente describe los parámetros específicos del protocolo SNMPv3:

Tabla 23. Parámetros del protocolo SNMPv3

Parámetro	Descripción
Configuración de protocolo	**SNMPv3**
Protocolo de autenticación	Algoritmos que se deben utilizar para autenticar condiciones de excepción SNMP:
Incluir los OID en la carga útil de suceso	Especifica que la carga útil de suceso SNMP se construye mediante pares nombre-valor en lugar del formato estándar de carga útil de suceso. Cuando selecciona orígenes de registro específicos en la lista **Tipos de orígenes de registro**, son necesarios los OID de la carga de útil de suceso para procesar sucesos de SNMPv2 o SNMPv3.

Opciones de configuración del protocolo de API REST Seculert Protection

Para recibir sucesos de Seculert, configure un origen de registro para utilizar el protocolo de API REST Seculert Protection.

Seculert Protection proporciona alertas sobre incidentes confirmados de programas maliciosos que están comunicando o exfiltrando información de forma activa.

Para poder configurar un origen de registro para Seculert, debe obtener la clave de API del portal web de Seculert.

1. Inicie la sesión en el portal web de Seculert.
2. En el panel de control, pulse la pestaña **API**.
3. Copie el valor de **Your API Key**.

La tabla siguiente describe los parámetros específicos del protocolo de API REST Seculert Protection:

Tabla 24. Parámetros del protocolo de API REST Seculert Protection

Parámetro	Descripción
Clave de API	La clave de API utilizada para autenticarse en la API REST de Seculert Protection. El valor de clave de API se obtiene del portal web de Seculert.
Utilizar proxy	Si se configura un proxy, todo el tráfico del origen de registro viaja a través del proxy para que QRadar acceda a la API REST de Seculert Protection. Configure los campos **IP o nombre de host de proxy**, **Puerto de proxy**, **Nombre de usuario de proxy** y **Contraseña de proxy**. Si el proxy no requiere autenticación, puede dejar en blanco los campos **Nombre de usuario de proxy** y **Contraseña de proxy**.
Adquirir automáticamente certificado(s) de servidor	Si selecciona **Sí** en la lista, QRadar descarga el certificado y empieza a confiar en el servidor de destino.
Recurrencia	Especifique cuándo recopila datos el registro. El formato es M/H/D para Meses/Horas/Días. El valor predeterminado es 1 M.
Regulador de EPS	El límite superior para el número máximo de sucesos por segundo (eps) para los sucesos recibidos de la API.

Opciones de configuración del protocolo Sophos Enterprise Console JDBC

Para recibir sucesos de Sophos Enterprise Console JDBC, configure un origen de registro para utilizar el protocolo Sophos Enterprise Console JDBC.

El protocolo Sophos Enterprise Console JDBC combina la información de carga útil de los registros de control de aplicación, los registros de control de dispositivo, los registros de control de datos, los registros de protección contra la manipulación indebida y los registros de cortafuegos contenidos en la tabla vEventsCommonData. Si Sophos Enterprise Console no tiene la interfaz de informes de Sophos, puede utilizar el protocolo JDBC estándar para recopilar sucesos de antivirus.

La tabla siguiente describe los parámetros del protocolo Sophos Enterprise Console JDBC:

Tabla 25. Parámetros del protocolo Sophos Enterprise Console JDBC

Parámetro	Descripción
Configuración de protocolo	**Sophos Enterprise Console JDBC**
Tipo de base de datos	**MSDE**

Tabla 25. Parámetros del protocolo Sophos Enterprise Console JDBC (continuación)

Parámetro	Descripción
Nombre de base de datos	El nombre de base de datos debe coincidir con el nombre de base de datos que está especificado en el campo **Identificador de origen de registro**.
Puerto	El puerto predeterminado para MSDE en Sophos Enterprise Console es 1168. El puerto de la configuración JDBC debe coincidir con el puerto de escucha de la base de datos Sophos para comunicar con QRadar. La base de datos Sophos debe permitir conexiones TCP entrantes. Si se utiliza una **Instancia de base de datos** con el tipo de base de datos MSDE, debe dejar en blanco el parámetro **Puerto**.
Dominio de autenticación	Si la red no utiliza un dominio, deje en blanco este campo.
Instancia de base de datos	La instancia de base de datos, si es necesaria. Las bases de datos MSDE pueden incluir varias instancias de servidor SQL en un solo servidor. Cuando se utiliza un puerto no estándar para la base de datos o los administradores bloquean el acceso al puerto 1434 para la resolución de bases de datos SQL, el parámetro **Instancia de base de datos** debe estar en blanco.
Nombre de tabla	`vEventsCommonData`
Lista de selección	*
Campo de comparación	`InsertedAt`
Utilizar sentencias preparadas	Las sentencias preparadas permiten que el origen de protocolo configure la sentencia SQL y luego ejecute la sentencia SQL muchas veces con parámetros diferentes. Por motivos de seguridad y rendimiento, la mayoría de las configuraciones pueden utilizar sentencias preparadas. Puede deseleccionar esta casilla para utilizar un método alternativo de consulta que no utiliza sentencias precompiladas.
Fecha y hora de inicio	Opcional. Fecha y hora en que el protocolo puede comenzar a sondear la base de datos. Si no se define una hora de inicio, el protocolo intenta buscar sucesos después de que se guarde y despliegue la configuración del origen de registro.
Intervalo de sondeo	Periodo de tiempo entre consultas a la base de datos. Puede definir un intervalo de sondeo mayor añadiendo una H (de horas) o una M (de minutos) al valor numérico. El intervalo de sondeo máximo es de 1 semana en cualquier formato de hora. Los valores numéricos sin el indicador H ni M denotan un intervalo de sondeo en segundos.
Regulador de EPS	Número máximo de sucesos por segundo (EPS) que el protocolo no debe sobrepasar.

Tabla 25. Parámetros del protocolo Sophos Enterprise Console JDBC (continuación)

Parámetro	Descripción
Utilizar comunicación por conducto	Si se configura MSDE como tipo de base de datos, los administradores pueden seleccionar esta casilla para utilizar un método alternativo para una conexión de puerto TCP/IP. Las conexiones por conducto para bases de datos MSDE requieren que los campos de nombre de usuario y contraseña utilicen un nombre de usuario y contraseña de autenticación de Windows en lugar del nombre de usuario y contraseña de la base de datos. La configuración del origen de registro debe utilizar la conexión por conducto predeterminada en la base de datos MSDE.
Nombre de clúster de base de datos	Si utiliza el servidor SQL en un entorno de clúster, defina el nombre de clúster para asegurarse de que las comunicaciones por conducto funcionen correctamente.
Utilizar NTLMv2	Obliga a que las conexiones MSDE utilicen el protocolo NTLMv2 con los servidores SQL que necesitan autenticación NTLMv2. De forma predeterminada, esta casilla está seleccionada. Seleccionar la casilla **Utilizar NTLMv2** no interrumpe las comunicaciones para las conexiones MSDE que no necesitan autenticación NTLMv2.

Opciones de configuración del protocolo Sourcefire Defense Center Estreamer

Para recibir sucesos de un servicio de Sourcefire Defense Center Estreamer (Event Streamer), configure un origen de registro para que utilice el protocolo Sourcefire Defense Center Estreamer.

Se envían archivos de suceso a QRadar para su proceso una vez configurado Sourcefire Defense Center DSM.

La tabla siguiente describe los parámetros específicos del protocolo Sourcefire Defense Center Estreamer:

Tabla 26. Parámetros del protocolo Sourcefire Defense Center Estreamer

Parámetro	Descripción
Configuración de protocolo	**Sourcefire Defense Center Estreamer**
Puerto de servidor	El puerto predeterminado que QRadar utiliza para Sourcefire Defense Center Estreamer es 8302.
Nombre de archivo del almacén de claves	Vía de acceso del directorio y el nombre de archivo de la clave privada del almacén de claves y certificado asociado. De forma predeterminada, el script de importación crea el archivo de almacén de claves en el directorio siguiente: `/opt/qradar/conf/estreamer.keystore`.
Nombre de archivo de almacén de claves de confianza	El archivo de almacén de claves de confianza contiene los certificados fiables del cliente. De forma predeterminada, el script de importación crea el archivo de almacén de claves de confianza en el directorio siguiente: `/opt/qradar/conf/estreamer.truststore`.

Tabla 26. Parámetros del protocolo Sourcefire Defense Center Estreamer (continuación)

Parámetro	Descripción
Solicitar datos adicionales	Seleccione esta opción para solicitar datos adicionales de Sourcefire Defense Center Estreamer, por ejemplo, los datos adicionales incluyen la dirección IP original de un suceso.
Utilizar solicitudes ampliadas	Seleccione esta opción para utilizar un método alternativo para recuperar sucesos de un origen eStreamer. Las solicitudes ampliadas están soportadas en Sourcefire DefenseCenter Estreamer versión 5.0 o posterior.

Visión general del protocolo Syslog Redirect

El protocolo Syslog Redirect se utiliza como alternativa al protocolo Syslog. Utilice este protocolo cuando desee que QRadar identifique el nombre de dispositivo específico que ha enviado los sucesos. QRadar puede estar a la escucha de sucesos de Syslog en el puerto 517 de UDP.

La tabla siguiente describe los parámetros específicos del protocolo Syslog Redirect:

Tabla 27. Parámetros del protocolo Syslog Redirect

Parámetro	Descripción
Configuración de protocolo	**Syslog Redirect**
Expresión regular del identificador del origen de registro	`devname=([\w-]+)`
Puerto de escucha	517
Protocolo	**UDP**

Opciones de configuración del protocolo TCP Multiline Syslog

Puede configurar un origen de registro para utilizar el protocolo TCP Multiline Syslog. Para crear un suceso de una sola línea, este protocolo utiliza expresiones regulares para identificar el patrón de inicio y finalización de sucesos multilínea.

El ejemplo siguiente es un suceso multilínea:

```
06/13/2012 08:15:15 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: 1.1.1.1
Source Port: 80
Destination Address: 1.1.1.12
Destination Port:444
```

La tabla siguiente describe los parámetros específicos del protocolo TCP Multiline Syslog:

Tabla 28. Parámetros del protocolo TCP Multiline Syslog

Parámetro	Descripción
Configuración de protocolo	**TCP Multiline Syslog**
Puerto de escucha	El puerto de escucha predeterminado es 12468.
Formateador de sucesos	Utilice la opción **Windows Multiline** para sucesos multilínea que están formateados específicamente para Windows.
Patrón de inicio de suceso	Expresión regular (regex) que es necesaria para identificar el inicio de una carga útil de TCP Multiline a suceso. Las cabeceras de Syslog suelen comenzar con una fecha o indicación de fecha y hora. El protocolo puede crear un suceso de una sola línea que se basa exclusivamente en un patrón de inicio de sucesos, tal como una indicación de fecha y hora. Cuando sólo existe un patrón de inicio, el protocolo captura toda la información entre cada valor de inicio para crear un suceso válido.
Patrón de final de suceso	Expresión regular (regex) que es necesaria para identificar el último campo de una carga útil de TCP a suceso multilínea. Si el suceso de syslog termina con el mismo valor, puede utilizar una expresión regular para determinar el final de un suceso. El protocolo puede capturar sucesos que están basados únicamente en un patrón de final de sucesos. Cuando sólo existe un patrón de final, el protocolo captura toda la información entre cada valor de finalización para crear un suceso válido.

Opciones de configuración del protocolo TLS Syslog

Para recibir sucesos de syslog cifrados procedentes de hasta 50 dispositivos de red que son compatibles con el reenvío de sucesos de TLS Syslog, configure un origen de registro para utilizar el protocolo TLS Syslog.

El origen de registro crea un puerto de escucha para los sucesos entrantes de TLS Syslog y genera un archivo de certificado para los dispositivos de red. Hasta 50 dispositivos de red pueden reenviar sucesos al puerto de escucha que se crea para el origen de registro. Si necesita más de 50 dispositivos de red, cree puertos de escucha adicionales.

La tabla siguiente describe los parámetros específicos del protocolo TLS Syslog:

Tabla 29. Parámetros del protocolo TLS Syslog

Parámetro	Descripción
Configuración de protocolo	**TLS Syslog**
Puerto de escucha TLS	El puerto de escucha predeterminado de TLS es 6514.
Modalidad de autenticación	Modalidad utilizada para autenticar la conexión TLS. Si selecciona la opción **TLS y autenticación de cliente**, debe configurar los parámetros de certificado.
Vía de acceso de certificado de cliente	Vía de acceso absoluta del certificado de cliente en el disco. El certificado se debe almacenar en la consola o en el Recopilador de sucesos para este origen de registro.

Tabla 29. Parámetros del protocolo TLS Syslog (continuación)

Parámetro	Descripción
Tipo de certificado	Tipo de certificado que se debe utilizar para la autenticación. Si selecciona la opción **Proporcionar certificado**, debe definir las vías de acceso del certificado de servidor y la clave privada.
Vía de acceso de certificado de servidor proporcionada	Vía de acceso absoluta del certificado de servidor.
Vía de acceso de clave privada proporcionada	Vía de acceso absoluta de la clave privada. **Nota:** La clave privada correspondiente debe ser una clave PKCS8 con codificación DER. La configuración falla si se utiliza cualquier otro formato de clave.
Máximo de conexiones	El parámetro **Máximo de conexiones** controla cuántas conexiones simultáneas puede aceptar el protocolo TLS Syslog para cada Recopilador de sucesos. Existe un límite de 1000 conexiones en todas las configuraciones de origen de registro TLS syslog para cada Recopilador de sucesos. El valor predeterminado para cada conexión de dispositivo es de 50. **Nota:** los orígenes de registro descubiertos automáticamente que comparten un escucha con otro origen de registro se contabilizan una sola vez con respecto al límite. Por ejemplo, el mismo puerto en el mismo recopilador de sucesos.

Casos de uso de TLS Syslog

Los casos de uso siguientes representan configuraciones posibles que puede crear:

Autenticación de cliente
Puede proporcionar un certificado de cliente que permite que el protocolo intervenga en la autenticación de cliente. Si selecciona esta opción y proporciona el certificado, las conexiones entrantes se validan por comparación con el certificado de cliente.

Certificados de servidor proporcionados por el usuario
Puede definir un certificado de servidor propio y la clave privada correspondiente. El proveedor configurado de TLS Syslog utiliza el certificado y la clave. Las conexiones entrantes se presentan con el certificado proporcionado por el usuario, en lugar del certificado de TLS Syslog que se crea automáticamente.

Autenticación predeterminada
Para utilizar el método de autenticación predeterminado, utilice los valores predeterminados para los parámetros **Modalidad de autenticación** y **Tipo de certificado**. Después de guardar el origen de registro, se crea un certificado `syslog-tls` para el dispositivo de origen de registro. El certificado se debe copiar en cualquier dispositivo de la red que esté configurado para reenviar datos cifrados de syslog.

Opciones de configuración del protocolo UDP Multiline Syslog

Para crear un suceso de Syslog de una sola línea a partir de un suceso multilínea, configure un origen de registro para utilizar el protocolo UDP Multiline. El

protocolo UDP Multiline Syslog utiliza una expresión regular para identificar mensajes multilínea de syslog y recomponerlos en una sola carga útil de suceso.

El suceso original debe contener un valor que repite una expresión regular la cual puede identificar y recomponer el suceso multilínea. Por ejemplo, este suceso contiene un valor repetido:

```
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH base="dc=iso-n,dc=com"
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=1 SRCH base="dc=iso-n,dc=com"
```

La tabla siguiente describe los parámetros específicos del protocolo UDP Multiline Syslog:

Tabla 30. Parámetros del protocolo UDP Multiline Syslog

Parámetro	Descripción
Configuración de protocolo	**UDP Multiline Syslog**
Patrón de ID de mensaje	Expresión regular (regex) necesaria para filtrar los mensajes de carga útil de suceso. Los mensajes de suceso multilínea UDP deben contener un valor identificador común que se repite en cada línea del mensaje de suceso.

Una vez guardado el origen de registro, se crea un certificado syslog-tls para el origen de registro. El certificado se debe copiar en cualquier dispositivo de la red que esté configurado para reenviar syslog cifrado. Otros dispositivos de red que tienen un archivo de certificado syslog-tls y el número de puerto de escucha TLS se pueden descubrir automáticamente como origen de registro syslog de TLS.

Opciones de configuración del protocolo VMware vCloud Director

Para recopilar sucesos de los entornos virtuales de VMware vCloud Director, puede crear un origen de registro que utiliza el protocolo VMware vCloud Director.

La tabla siguiente describe los parámetros específicos del protocolo VMware vCloud Director:

Tabla 31. Parámetros del protocolo VMware vCloud Director

Parámetro	Descripción
Configuración de protocolo	**VMware vCloud Director**
URL de vCloud	URL que se configura en el dispositivo de Mware vCloud para acceder a la API REST. El URL debe coincidir con la dirección que está configurada como URL base de la API REST pública de VCD en el servidor vCloud, por ejemplo, `https://1.1.1.1.`.
Nombre de usuario	Nombre de usuario que es necesario para acceder de forma remota al servidor vCloud, por ejemplo, `console/user@organization`. Para configurar una cuenta de sólo lectura a fin de utilizarla con el protocolo vCloud Director, un usuario debe tener permiso de Acceso de consola solamente.

Añadir orígenes de registro masivos

Puede añadir cada vez hasta 500 orígenes de registro de Microsoft Windows o Universal DSM. Cuando añade varios orígenes de registro a la vez, añade un origen de registro masivo en QRadar. Los orígenes de registro masivos deben compartir una configuración común.

Procedimiento

1. Pulse la pestaña **Admin**.
2. Pulse el icono **Orígenes de registro**.
3. En la lista **Acciones masivas**, seleccione **Adición masiva**.
4. Configure los parámetros para el origen de registro masivo.
   - Carga de archivo – cargar un archivo de texto que tenga un nombre de host o dirección IP por línea
   - Manual - Especifique el nombre de host o dirección IP del host que desea añadir
5. Pulse **Guardar**.
6. Pulse **Continuar** para añadir los orígenes de registro.
7. En el panel **Admin**, pulse **Desplegar cambios**.

Añadir un orden de análisis de los orígenes de registro

Puede asignar un orden de prioridad con el que el recopilador de sucesos de destino analiza los sucesos.

Acerca de esta tarea

Puede ordenar la importancia de los orígenes de registro definiendo el orden de análisis de los orígenes de registro que comparten una dirección IP o nombre de host comunes. Esto asegura que determinados orígenes de registro se analicen en un orden específico, sin importar los cambios hechos en la configuración del origen de registro. El orden de análisis asegura que el rendimiento del sistema no se vea afectado por cambios en la configuración del origen de registro al impedir análisis innecesarios. De esta manera los orígenes de registro de bajo nivel no se analizan antes que un origen de registro más importante.

Procedimiento

1. Pulse la pestaña **Admin**.
2. Pulse el icono **Orden de análisis de orígenes de registro**.
3. Seleccione un origen de registro.
4. Opcional: En la lista **Recopilador de sucesos seleccionado**, seleccione el recopilador de sucesos para definir el orden de análisis de orígenes de registro.
5. Opcional: En la lista **Host de origen de registro**, seleccione un origen de registro.
6. Defina un orden de prioridad para el análisis de orígenes de registro.
7. Pulse **Guardar**.

Capítulo 2. Extensiones de origen de registro

Un documento de extensión puede ampliar o modificar cómo se analizan los elementos de un origen de registro determinado. Puede utilizar el documento de extensión para corregir un problema de análisis o alterar temporalmente el análisis predeterminado para un suceso de un DSM existente.

Un documento de extensión también puede proporcionar soporte de sucesos cuando no existe un DSM para analizar sucesos para un dispositivo o dispositivo de seguridad de la red.

Un documento de extensión es un documento con formato XML (Extensible Markup Language) que puede crear o editar utilizando cualquier editor de texto, código o marcación habitual. Puede crear varios documentos de extensión, pero sólo uno puede aplicarse a un origen de registro.

El formato XML requiere que todos los patrones de expresión regular (regex) se encuentren en secciones de datos de caracteres (CDATA) para evitar que los caracteres especiales que son necesarios para las expresiones regulares interfieran en el formato de códigos. Por ejemplo, el código siguiente muestra la expresión regular para buscar protocolos:

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns="">
<![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
```

`(TCP|UDP|ICMP|GRE)` es el patrón de expresión regular.

La configuración de la extensión de origen de registro consta de las siguientes secciones:

Patrón Patrones de expresiones regulares que se asocian con un nombre de campo determinado. Se hace referencia a los patrones varias veces en el archivo de extensión de origen de registro.

Grupos de coincidencias
Una entidad dentro de un grupo de coincidencia que se analiza, por ejemplo, EventName, y se empareja con el patrón y grupo adecuados para el análisis. Puede aparecer cualquier número de grupos de coincidencia en el documento de extensión.

Ejemplos de extensiones de origen de registro en el foro de QRadar

Puede crear extensiones de origen de registro (LSX) para orígenes de registro que no tienen un DSM soportado. Como ayuda para crear sus propias extensiones de origen de registro (también denominadas extensiones de DSM), puede modificar extensiones existentes.

Puede acceder a ejemplos de extensión de origen de registro (https://www.ibm.com/developerworks/community/forums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25) en el foro Discussion about DSM Extensions, Custom Properties and other REGEX related topics (https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000003046&ps=25).

Los foros de IBM Security QRadar son un sitio de debate en línea donde usuarios y expertos colaboran y comparten información.

Conceptos relacionados:

"Crear un documento de extensiones de origen de registro" en la página 40
Cree extensiones de origen de registro (LSX) para los orígenes de registro que no tienen un DSM soportado, para reparar un suceso que tiene información incorrecta o faltante o para analizar un suceso cuando el DSM asociado no puede producir un resultado.

Patrones de documentos de extensión de origen de registro

En lugar de asociar una expresión regular directamente con un nombre de campo determinado, los patrones (`patterns`) se declaran por separado al principio del documento de extensión. Puede hacerse referencia a estos patrones de expresión regular varias veces en el archivo de extensión de origen de registro.

Todos los caracteres situados entre código de inicio <pattern> y el código de finalización </pattern> se consideran parte del patrón. No utilice espacios adicionales ni caracteres de retorno dentro o alrededor del patrón o expresión <CDATA>. Los caracteres o espacios adicionales pueden impedir que la extensión de DSM coincida con el patrón especificado.

Tabla 32. Descripción de parámetros de patrón

Patrón	Tipo	Descripción
`id` (Obligatorio)	Serie	Una serie regular que es exclusiva dentro del documento de extensión.
`case-insensitive` (Opcional)	Booleano	Si es true, las mayúsculas y minúsculas de los caracteres se ignoran. Por ejemplo, `abc` es lo mismo que `ABC`. Si no se especifica, este parámetro toma de forma predeterminada el valor false.
`trim-whitespace` (Opcional)	Booleano	Si es true, los espacios en blanco y retornos de carro se ignoran. Si las secciones CDATA se dividen en varias líneas, los espacios adicionales y retornos de carro no se interpretan como parte del patrón. Si no se especifica, este parámetro toma de forma predeterminada el valor false.

Grupos de coincidencia

Un *grupo de coincidencia* (`match-group`) es un conjunto de patrones que se utilizan para analizar o modificar uno o varios tipos de sucesos.

Un *buscador de coincidencias* es una entidad dentro de un grupo de coincidencia que se analiza, por ejemplo, EventName, y se empareja con el patrón y el grupo adecuados para el análisis. Puede aparecer cualquier número de grupos de coincidencia en el documento de extensión.

Tabla 33. Descripción de parámetros de grupo de coincidencia

Parámetro	Descripción
`order` (Obligatorio)	Un entero mayor que cero que define el orden de ejecución de los grupos de coincidencia. Debe ser exclusivo dentro del documento de extensión.
`description` (Opcional)	Descripción del grupo de coincidencia, que puede ser cualquier serie. Esta información puede aparecer en los registros. Si no se especifica, este parámetro toma el valor predeterminado vacío.
`device-type-id-override` (Opcional)	Define un ID de dispositivo diferente para alterar temporalmente el QID. Permite al grupo de coincidencia en concreto buscar el tipo de suceso en el dispositivo especificado. Debe ser un ID de tipo de origen de registro válido, representado como un entero. En la sección Tabla 40 en la página 51 figura una lista de los ID de tipo de origen de registro. Si no se especifica, este parámetro toma de forma predeterminada el tipo de origen de registro del origen de registro al que está conectada la extensión.

Los grupos de coincidencia pueden tener estas entidades:

- "Buscador de coincidencias (matcher)"
- "Modificador de suceso único (`event-match-single`)" en la página 36
- "Modificador multisuceso (`event-match-multiple`)" en la página 36

Buscador de coincidencias (matcher)

Una entidad de buscador de coincidencias es un campo que se analiza, por ejemplo, EventName, y se empareja con el patrón y grupo adecuados para el análisis.

Los buscadores de coincidencias tienen un orden asociado. Si se especifican varios buscadores de coincidencias para el mismo nombre de campo, los buscadores de coincidencias se ejecutan en el orden especificado hasta que se encuentra un análisis satisfactorio o se produce una anomalía.

Tabla 34. Descripción de parámetros de buscador de coincidencias

Parámetro	Descripción
`field` (Obligatorio)	El campo al que debe aplicarse el patrón, por ejemplo, EventName o SourceIp. Puede utilizar cualquiera de los nombres de campo que figuran en la tabla Lista de nombres de campo de buscador de coincidencias válidos .
`pattern-id` (Obligatorio)	El patrón que desea utilizar cuando el campo se analice desde la carga útil. Este valor debe coincidir (incluyendo mayúsculas y minúsculas) con el parámetro de ID del patrón que se ha definido anteriormente en un parámetro de ID de patrón (Tabla 32 en la página 30).
`order` (Obligatorio)	El orden en el que desea que se intente este patrón entre los buscadores de coincidencias que están asignados al mismo campo. Si dos buscadores de coincidencias están asignados al campo EventName, el que tiene el orden más bajo se intenta en primer lugar.
`capture-group` (Opcional)	Referenciado en la expresión regular entre paréntesis ( ). Estas capturas se indexan a partir de uno y se procesan de izquierda a derecha en el patrón. El campo `capture-group` debe ser un entero positivo inferior o igual al número de grupos de captura contenidos en el patrón. El valor predeterminado es cero, que es la coincidencia completa. Por ejemplo, puede definir un único patrón para una dirección IP y puerto de origen, donde el buscador de coincidencias SourceIp puede utilizar un grupo de captura de 1, y el buscador de coincidencias SourcePort puede utilizar un grupo de captura de 2, pero sólo es necesario definir un patrón. Este campo tiene un doble objetivo cuando se combina con el parámetro `enable-substitutions`. Para ver un ejemplo, consulte el Ejemplo de documento de extensión.

Tabla 34. Descripción de parámetros de buscador de coincidencias (continuación)

Parámetro	Descripción

`enable-substitutions` (Opcional)	Booleano
	
	Si se establece en `true`, un campo no puede representarse adecuadamente con un grupo de captura directo. Puede combinar varios grupos con texto adicional para formar un valor.
	
	Este parámetro cambia el significado del parámetro `capture-group`. El parámetro `capture-group` crea el nuevo valor, y las sustituciones de grupo se especifican mediante `\x`, donde `x` es un número de grupo, 1 - 9. Puede utilizar los grupos varias veces, y también puede insertar cualquier texto de formato libre en el valor. Por ejemplo, para formar un valor a partir del grupo de 1, seguido de un signo de subrayado, seguido del grupo 2, @ y luego de nuevo el grupo 1, se muestra la sintaxis adecuada de capture-group en el código siguiente:
	
	`capture-group="\1_\2@\1"`
	
	En otro ejemplo, una dirección MAC está separada por signos de dos puntos, pero en QRadar, las direcciones MAC suelen estar separadas por guiones. La sintaxis para analizar y capturar las partes individuales se muestra en el ejemplo siguiente:
	
	`capture-group="\1:\2:\3:\4:\5:\6"`
	
	Si no se especifican grupos en el grupo de captura cuando se habilitan las sustituciones, se produce una sustitución de texto directa.
	
	El valor predeterminado es false.

`ext-data` (Opcional)	Un parámetro de datos adicionales que define cualquier información o formato de campo adicional que un campo de buscador de coincidencias puede proporcionar en la extensión. El único campo que utiliza este parámetro es DeviceTime. Por ejemplo, puede tener un dispositivo que envía sucesos mediante una indicación de fecha y hora exclusiva, pero desea reformatear el suceso con una hora de dispositivo estándar. Utilice el parámetro ext-data incluido en el campo DeviceTime para reformatear la indicación de fecha y hora del suceso. Para obtener más información, consulte la Lista de nombres de campo de buscador de coincidencias válidos.

La tabla siguiente lista los nombres de campo de buscador de coincidencias válidos.

Tabla 35. Lista de nombres de campo de buscador de coincidencias válidos

Nombre de campo	Descripción
EventName (Obligatorio)	El nombre del suceso que debe recuperarse del QID para identificar el suceso. **Nota:** este parámetro no aparece como campo en el panel **Actividad de registro**.
EventCategory	Una categoría de suceso para cualquier suceso con una categoría no manejada por una entidad event-match-single o una entidad event-match-multiple. Combinado con EventName, EventCategory se utiliza para buscar el suceso en el QID. Los campos que se utilizan para búsquedas de QIDmap requieren establecer un distintivo de alteración temporal cuando QRadar ya conoce los dispositivos, por ejemplo, `<event-match-single event-name= "Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity= "OverrideAndNeverSend" />` `force-qidmap-lookup-on-fixup="true"` es el distintivo de alteración temporal. **Nota:** este parámetro no aparece como campo en el panel **Actividad de registro**.
SourceIp	La dirección IP de origen del mensaje.
SourcePort	El puerto de origen del mensaje.
SourceIpPreNAT	La dirección IP de origen del mensaje antes de que se produzca la conversión de direcciones de red (NAT).
SourceIpPostNAT	La dirección IP de origen del mensaje después de que se produzca la NAT.
SourceMAC	La dirección MAC de origen del mensaje.
SourcePortPreNAT	El puerto de origen del mensaje antes de que se produzca la NAT.
SourcePortPostNAT	El puerto de origen del mensaje después de que se produzca la NAT.
DestinationIp	La dirección IP de destino del mensaje.
DestinationPort	El puerto de destino del mensaje.
DestinationIpPreNAT	La dirección IP de destino del mensaje antes de que se produzca la NAT.
DestinationIpPostNAT	La dirección IP de destino del mensaje después de que se produzca la NAT.
DestinationPortPreNAT	El puerto de destino del mensaje antes de que se produzca la NAT.
DestinationPortPostNAT	El puerto de destino del mensaje después de que se produzca la NAT.

Tabla 35. Lista de nombres de campo de buscador de coincidencias válidos (continuación)

Nombre de campo	Descripción
DestinationMAC	La dirección MAC de destino del mensaje.
DeviceTime	El formato de fecha y hora que se utiliza en el dispositivo. Esta indicación de fecha y hora representa la hora a la que se ha enviado el suceso, según el dispositivo. Este parámetro no representan la hora a la que ha llegado el suceso. El campo `DeviceTime` da soporte a la capacidad de utilizar una indicación de fecha y hora personalizada para el suceso utilizando el atributo ext-data del buscador de coincidencias. La lista siguiente contiene ejemplos de formatos de indicación de fecha y hora que se pueden utilizar en el campo `DeviceTime`: • ext-data="dd/MMM/AAAA:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd AAAA / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/AAAA" 05:26:00:11/Mar/2015 Para obtener más información sobre los valores posibles del formato de indicación de fecha y hora, consulte la página web de Joda-Time (http://www.joda.org/joda-time/key_format.html). DeviceTime es el único campo de suceso que utiliza el parámetro opcional ext-data.
Protocol	El protocolo que está asociado con el suceso; por ejemplo, TCP, UDP o ICMP.
UserName	El nombre de usuario que está asociado con el suceso.
HostName	El nombre de host que está asociado con el suceso. Normalmente, este campo está asociado a sucesos de identidad.
GroupName	El nombre de grupo que está asociado con el suceso. Normalmente, este campo está asociado a sucesos de identidad.
NetBIOSName	El nombre de NetBIOS que está asociado con el suceso. Normalmente, este campo está asociado a sucesos de identidad.
ExtraIdentityData	Los datos específicos de usuario que están asociados con el suceso. Normalmente, este campo está asociado a sucesos de identidad.
SourceIpv6	La dirección IP de origen IPv6 del mensaje.
DestinationIpv6	La dirección IP de destino IPv6 del mensaje.

Modificador multisuceso (event-match-multiple)

El modificador multisuceso (event-match-multiple) compara un rango de tipos de sucesos y a continuación los modifica según lo especificado en los parámetros pattern-id y capture-group-index.

Esta comparación no se realiza en la carga útil, sino que se realiza en los resultados del buscador de coincidencias EventName analizado anteriormente en la carga útil.

Esta entidad permite la mutación de sucesos satisfactorios cambiando la categoría de sucesos de dispositivo, la gravedad o el método que el suceso utiliza para enviar sucesos de identidad. capture-group-index debe ser un valor entero (las sustituciones no están soportadas) y pattern-ID debe hacer referencia a una entidad de patrón existente. Todas las demás propiedades son idénticas a sus equivalentes del modificador de suceso único.

Modificador de suceso único (event-match-single)

El modificador de suceso único (event-match-single) empareja y luego modifica exactamente un tipo de suceso, según lo especificado por el parámetro obligatorio case-sensitive de EventName.

Esta entidad permite la mutación de sucesos satisfactorios cambiando la categoría de sucesos de dispositivo, la gravedad o el método de envío de sucesos de identidad.

Cuando se analizan los sucesos que coinciden con este nombre de suceso, las propiedades de categoría de dispositivo, gravedad e identidad se imponen al suceso resultante.

Debe establecer un atributo event-name y este valor de atributo coincidirá con el valor del campo **EventName**. Además, una entidad event-match-single consta de estas propiedades opcionales:

Tabla 36. Descripción de parámetros de suceso único

Parámetro	Descripción
device-event-category	Una categoría nueva para buscar un QID para el suceso. Este es un parámetro de optimización debido a que algunos dispositivos tienen la misma categoría para todos los sucesos.
severity	La gravedad del suceso. Este parámetro debe ser un valor entero 1 - 10. Si se especifica una gravedad menor que 1 o mayor que 10, el sistema adopta el valor predeterminado 5. Si no se especifica, el valor predeterminado es el se encuentre en el QID.

Tabla 36. Descripción de parámetros de suceso único (continuación)

Parámetro	Descripción
`send-identity`	Especifica el envío de información de cambio de identidad del suceso. Seleccione una de las opciones siguientes: • `UseDSMResults` Si el DSM devuelve un suceso de identidad, el suceso se pasa. Si el DSM no devuelve un suceso de identidad, la extensión no crea o modifica la información de identidad. Esta opción es el valor predeterminado si no se especifica ningún valor. • `SendIfAbsent` Si el DSM crea información de identidad, el suceso de identidad se pasa sin afectación. Si El DSM no genera ningún suceso de identidad, pero hay información suficiente en el suceso para crear un suceso de identidad, se genera un suceso con todos los campos relevantes establecidos. • `OverrideAndAlwaysSend` Ignora cualquier suceso de identidad devuelto por el DSM y crea un nuevo suceso de identidad, si hay suficiente información. • `OverrideAndNeverSend` Suprime cualquier información de identidad devuelta por el DSM. Es la opción sugerida, a menos que se estén procesando sucesos que deban entrar en actualizaciones de activos.

Plantilla de documento de extensión

El ejemplo de documento de extensión proporciona información sobre cómo analizar un tipo determinado de Cisco FWSM para que los sucesos no se envíen con un nombre de suceso incorrecto.

Por ejemplo, si desea resolver la palabra `session`, que está intercalada en medio del nombre de suceso:

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015:
Built UDP connection for faddr 38.116.157.195/80
gaddr 129.15.127.254/31696 laddr 10.194.2.196/2157
duration 0:00:00 bytes 57498 (TCP FINs)
```

Esta condición hace que el DSM no reconozca ningún suceso, y todos los sucesos quedan sin analizar y se asocian con el registrador genérico.

Aunque sólo una parte de la serie de texto (`302015`) se utiliza para la búsqueda de QID, la serie de texto completa (`%FWSM-session-0-302015`) identifica el suceso como procedente de un FWSM de Cisco. Dado que la serie de texto completa no es válido, el DSM asume que el suceso no es válido.

Ejemplo de documento de extensión para analizar un tipo de suceso

Un dispositivo FWSM tiene muchos tipos de sucesos y muchos con formatos exclusivos. El siguiente ejemplo de documento de extensión indica cómo analizar un tipo de suceso.

Nota: los ID de patrón no tienen que coincidir con los nombres de campo que están analizando. Aunque el ejemplo siguiente duplica el patrón, el campo `SourceIp` y el campo `SourceIpPreNAT` pueden utilizar el mismo patrón exacto en este caso. Esta situación podría no ser cierta en todos los sucesos FWSM.

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
      <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1"/>
      <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />
      <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2"/>
      <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />
      <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />
      <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />
      <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />
      <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
      <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="2" />
      <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />
      <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true/>
      <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
   </match-group>
</device-extension>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<!-- No elimine el valor "allEventNames" -->
<pattern id="EventName-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceIp-Fakeware_Pattern" xmlns=""><![CDATA[]]</pattern>
<pattern id="SourcePort-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationPort" order="1" pattern-id="SDestinationPort-Fakeware_Pattern" capture-group="1" />
   <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
   <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
</match-group>
</device-extension>
```

Aspectos básicos del análisis

El ejemplo de documento de extensión anterior muestra algunos de los aspectos básicos del análisis:

- Direcciones IP
- Puertos
- Protocolo
- Varios campos que utilizan el mismo patrón con grupos diferentes

Este ejemplo analiza todos los sucesos FWSM que siguen el patrón especificado. Los campos que se analizan podrían no estar presente en esos sucesos cuando los sucesos incluyen contenido diferente.

La información necesaria para crear esta configuración que no estaba disponible en el suceso:

- El nombre del suceso son sólo los últimos 6 dígitos (`302015`) de la parte `%FWSM-session-0-302015` del suceso.

- El FWSM tiene una categoría de suceso de dispositivo codificada de `Cisco Firewall`.
- El DSM FWSM utiliza la QIDmap Cisco Pix y, por tanto, incluye el parámetro `device-type-id-override="6"` en el grupo de coincidencia. El ID del tipo de origen de registro de cortafuegos Pix es 6. Para obtener más información, consulte el apartado "IDs de tipo de origen de registro" en la página 51).

Nota: si la información de QID no se especifica o no está disponible, puede modificar la correlación de sucesos. Para obtener más información, consulte la sección dedicada a la modificación de correlaciones de sucesos en la publicación *IBM Security QRadar SIEM Users Guide*.

Nombre de suceso y categoría de sucesos de dispositivo

Son necesarios un nombre de suceso y una categoría de sucesos de dispositivo cuando se busca la QIDmap. Esta categoría de sucesos de dispositivo es un parámetro de agrupación dentro de la base de datos que ayuda a definir sucesos parecidos dentro de un dispositivo. El valor `event-match-multiple` al final del grupo de coincidencia incluye la codificación de la categoría. `event-match-multiple` utiliza el patrón EventNameId en el nombre de suceso analizado para comparar un máximo de 6 dígitos. Este patrón no se ejecuta en la carga completa, sólo en la parte analizada como el campo EventName.

El patrón EventName hace referencia a la parte `%FWSM` de los sucesos; todos los sucesos de Cisco FWSM contienen la parte `%FWSM`. El patrón del ejemplo compara `%FWSM` seguido de cualquier número (cero o más) de letras y guiones. Esta coincidencia de patrón resuelve que la palabra `session` que está intercalada en medio del nombre de suceso debe eliminarse. La gravedad del suceso (según Cisco), seguida por un guión y, a continuación, el nombre de suceso verdadero según lo esperado por QRadar. La serie `(\d{6})` es la única serie dentro del patrón EventNameFWSM que tiene un grupo de captura.

Todas las direcciones IP y puertos del suceso siguen el mismo patrón básico: una dirección IP seguida de un signo de dos puntos seguido del número de puerto. Este patrón analiza dos fragmentos de datos (la dirección IP y el puerto) y especifica grupos de captura diferentes en la sección de buscador de coincidencias (matcher).

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\] </pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
       capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username" capture-group="1"/>
</match-group>
</device-extension>
```

Patrones de dirección IP y puerto

Los patrones de dirección IP y puerto están formados por cuatro conjuntos de uno a tres dígitos, separados por puntos seguidos de un signo de dos puntos y el número de puerto. La sección de dirección IP está en un grupo, como el número de puerto, pero no los dos puntos. Las secciones de buscador de coincidencias

(matcher) para estos campos hacen referencia al mismo nombre de patrón, pero a un grupo de captura diferente (la dirección IP es del grupo 1 y el puerto es del grupo 2).

El protocolo es un patrón común que busca en la carga útil la primera instancia de TCP, UDP, ICMP o GRE. El patrón se marca con el parámetro case-insensitive, de modo que cualquier aparición coincida.

Aunque no aparece un segundo patrón de protocolo en el suceso de que se utiliza en el ejemplo, hay un segundo patrón de protocolo que se define con una orden de dos. Si el patrón de protocolo lowest-ordered no coincide, se intenta el siguiente, y así sucesivamente. El segundo patrón de protocolo también muestra la sustitución directa; no hay grupos de coincidencia en el patrón, pero con el parámetro enable-substitutions habilitado, puede utilizarse el texto TCP en lugar de protocol=6.

Crear un documento de extensiones de origen de registro

Cree extensiones de origen de registro (LSX) para los orígenes de registro que no tienen un DSM soportado, para reparar un suceso que tiene información incorrecta o faltante o para analizar un suceso cuando el DSM asociado no puede producir un resultado.

Para los orígenes de registro que no tienen un DSM oficial, utilice un DSN Universal, o UDSM, para integrar orígenes de registro. A continuación, se aplicará una extensión de origen de registro (también denominada extensión de dispositivo) al UDSM para proporcionar la lógica para analizar los registros. La LSX se basa en expresiones regulares Java y puede utilizarse en cualquier protocolo de registro, tales como syslog, JDBC y LFPS. Pueden extraerse valores de los registros y correlacionarse con todos los campos comunes dentro de QRadar.

Al utilizar extensiones de origen de registro para reparar contenido incorrecto o faltante, los nuevos sucesos generados por las extensiones de origen de registro se asocian con el origen de registro que no ha podido analizar la carga útil original. La creación de una extensión evita que sucesos desconocidos o no categorizados se almacenen como desconocidos en IBM Security QRadar.

Siga estos pasos para crear una extensión de origen de registro:

1. Asegúrese de que se crea un origen de registro en QRadar.

   Utilice Universal DSM como el tipo de origen de registro para manejar los elementos que no estén en la lista. También puede crear manualmente un origen de registro para impedir que los registros se clasifiquen automáticamente.
2. Para determinar qué campos están disponibles, utilice el panel **Actividad de registro** para exportar los registros para su evaluación.
3. Utilice la plantilla de ejemplo de documentos de extensión para determinar los campos que puede utilizar. (“Plantilla de documento de extensión” en la página 37).

   No es necesario utilizar todos los campos de la plantilla. Determine los valores del origen de registro que se pueden correlacionar con los campos de la plantilla de documento de extensión. Para obtener más información, consulte “Plantilla de documento de extensión” en la página 37.
4. Elimine los campos no utilizados y sus ID de patrón correspondientes del documento de extensión de origen de registro.

5. Cargue el documento de extensión y aplique la extensión al origen de registro.
6. Correlacione los sucesos con sus equivalentes de QIDmap.

   Esta acción manual en el panel **Actividad de registro** se utiliza para correlacionar sucesos de origen de registro desconocidos con sucesos de QRadar conocidos para que puedan clasificarse y procesarse.

Conceptos relacionados:

"Ejemplos de extensiones de origen de registro en el foro de QRadar" en la página 29

Puede crear extensiones de origen de registro (LSX) para orígenes de registro que no tienen un DSM soportado. Como ayuda para crear sus propias extensiones de origen de registro (también denominadas extensiones de DSM), puede modificar extensiones existentes.

Crear un DSM Universal

El primer paso para crear un DSM Universal es crear el origen de registro en IBM Security QRadar. Al crear el origen de registro, se impide que los registros se clasifiquen automáticamente y puede exportarlos para su revisión.

Procedimiento

1. En la pestaña **Admin**, cree un origen pulsando el icono **Orígenes de registro**.
2. Pulse **Añadir**.
3. Especifica el nombre en el campo **Nombre de origen de registro**.
4. En la lista **Tipo de origen de registro**, seleccione **Universal DSM**.

   Es posible que no visualice **Extensión de origen de registro** a menos que ya haya aplicado una extensión de origen de registro a QRadar Console.
5. En la lista **Configuración de protocolo**, especifique el protocolo que desee utilizar.

   QRadar utiliza este método para obtener los registros del origen de registro no soportado.
6. En **Identificador de origen de registro**, especifique la dirección IP o el nombre de host del origen de registro no soportado.
7. Haga clic en **Guardar** para guardar el nuevo origen de registro y cerrar la ventana.
8. En la pestaña **Admin**, pulse **Desplegar cambios**.

Qué hacer a continuación

"Exportar los registros"

Exportar los registros

Exporte los registros creados después de crear un Universal DSM

Acerca de esta tarea

Normalmente, deseará revisar un número significativo de registros. Según la velocidad de EPS del origen de registro no soportado, puede tardar varias horas en obtener una muestra registro exhaustiva.

Cuando QRadar no puede detectar el tipo de origen de registro, los sucesos se recopilan, pero no se analizan. Puede filtrar estos sucesos no analizados y, a continuación, revisar la última notificación del sistema que haya recibido. Después

de haber revisado la notificación del sistema, puede crear una búsqueda basada en ese intervalo de tiempo.

Procedimiento

1. Para ver sólo los sucesos que no se han analizado, filtre los registros.
   a. Pulse la pestaña **Actividad de registro**.
   b. Pulse **Añadir filtro**.
   c. Seleccione **El suceso está sin analizar**.

      Consejo: Escriba dentro del cuadro de texto **Parámetro** para ver el elemento **El suceso está sin analizar**.
   d. Seleccione un marco de tiempo.
   e. Si ve sucesos de **Información** de notificaciones del sistema, pulse el botón derecho para filtrarlos.
   f. Revise la columna **IP de origen** para determinar qué dispositivo está enviando los sucesos.

      Puede visualizar las cargas útiles de suceso en bruto. Normalmente, los fabricantes colocan nombres de producto identificables en las cabeceras, por lo que puede establecer la búsqueda en **Visualizar: Sucesos en bruto** para mostrar las cargas útiles sin tener que abrir cada suceso manualmente. Clasificar por red también puede ayudarle a encontrar un dispositivo específico en el que se originó el suceso.
2. Cree una búsqueda para exportar los registros.
   a. En la pestaña **Actividad de registro**, seleccione **Buscar** > **Editar búsqueda**.
   b. En **Rango de tiempo**, especifique un tiempo suficiente, por ejemplo 6 horas, desde el momento de la creación del origen de registro.
   c. En **Parámetros de búsqueda**, en la lista **Parámetro**, seleccione **Origen de registro (Indexado)**, en la lista **Operador** seleccione **Igual que**, y en la lista **Grupo de origen de registro** seleccione **Otros**, y especifique el origen de registro que se ha creado al crear el DSM Universal.

      Nota: En función de los valores, es posible que observe **Origen de registro** en la lista **Parámetro** en lugar de **Origen de registro (Indexado)**.
   d. Pulse **Buscar** para ver los resultados.
3. Revise los resultados en la consola para comprobar la carga útil.
4. De forma opcional, puede exportar los resultados pulsando **Acciones** > **Exportar a XML** > **Exportación completa (Todas las columnas)**.

   No seleccione **Exportar a CSV**, ya que la carga útil podría dividirse en varias columnas, haciendo que sea difícil encontrar la carga útil. XML es el formato preferido para revisiones de sucesos.
   a. Se le solicitará que descargue un archivo comprimido. Abra el archivo comprimido y, a continuación, abra el archivo resultante.
   b. Revise los registros.

      Las cargas útiles de sucesos se encuentran entre los códigos siguientes:

```
<payloadAsUTF>
...
</payloadAsUTF>
```

El código siguiente muestra una carga útil de ejemplo:

```
<payloadAsUTF>ecs-ep (pid 4162 4163 4164) is running... </payloadAsUTF>
```

Un paso crítico en la creación de un DSM Universal es revisar la usabilidad de los registros de utilización. Como mínimo, los registros deben tener un valor que pueda correlacionarse con un nombre de suceso. El nombre del suceso debe tener un valor exclusivo que pueda distinguir los diversos tipos de registros.

El código siguiente muestra un ejemplo de registros utilizables:

```
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root'
from 192.168.50.80:3364
May 20 17:16:26 dropbear[22331]: password auth succeeded for
'root' from 192.168.50.80:3364
May 20 16:42:19 kernel: DROP IN=vlan2 OUT=
MAC=00:01:5c:31:39:c2:08:00 SRC=172.29.255.121
DST=255.255.255.255 PROTO=UDP SPT=67 DPT=68
```

Los códigos de ejemplo siguientes muestran registros ligeramente menos utilizables:

```
Oct 26 08:12:08 loopback 1256559128 autotrace[215824]: W: trace:
no map for prod 49420003, idf 010029a2, lal 00af0008
Oct 26 16:35:00 sxpgbd0081 last message repeated 7 times
Nov 24 01:30:00 sxpgbd0081 /usr/local/monitor-rrd/sxpgbd0081/.rrd
(rc=-1, opening '/usr/local/monitor-rrd/sxpgbd0081/.rrd':
No such file or directory)
```

Expresiones regulares comunes

Utilice expresiones regulares para hacer coincidir patrones de texto en el archivo de origen de registro. Puede explorar los mensajes con respecto a patrones de letras, números o una combinación de ambos. Por ejemplo, puede crear expresiones regulares que coincidan con direcciones IP, puertos y direcciones MAC de origen y destino, etc.

Los códigos siguientes muestran varias expresiones regulares comunes:

```
\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3} \d{1,5}
(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2} (TCP|UDP|ICMP|GRE)
\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
\s \t .*?
```

El carácter de escape, o "\", se utiliza para indicar un carácter literal. Por ejemplo, el carácter "." significa "cualquier carácter individual" y coincide con A, B, 1, X, etc. Para comparar los caracteres ".", una coincidencia literal, debe utilizar "\."

Tabla 37. Expresiones regulares comunes

Tipo	Expresión
Tipo	\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
Dirección IP	\d{1,5}
Número de puerto	(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}
Protocolo	(TCP|UDP|ICMP|GRE)
Hora del dispositivo	\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
Espacio en blanco	\s
Tabulador	\t
Cualquier coincidencia	.*?

Consejo: Para asegurarse de no comparar accidentalmente otros caracteres, especifique un escape para cualquier carácter que no sea un dígito o alfanumérico.

Crear patrones de expresión regular

Para crear un DSM Universal, puede utilizar expresiones regulares (regex) para comparar series de texto del origen de registro no soportado.

Acerca de esta tarea

El ejemplo siguiente muestra una entrada de registro a la que se hace referencia en los pasos.

```
May 20 17:24:59 kernel: DROP MAC=5c:31:39:c2:08:00
SRC=172.29.255.121 DST=10.43.2.10 LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
May 20 17:24:59 kernel: PASS MAC=5c:14:ab:c4:12:59
SRC=192.168.50.10 DST=192.168.10.25 LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
May 20 17:24:59 kernel: REJECT
MAC=5c:ad:3c:54:11:07 SRC=10.10.10.5 DST=192.168.100.25 LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

Procedimiento

1. Analice visualmente el origen de registro no soportado para identificar patrones exclusivos.

   Estos patrones se convierten posteriormente en expresiones regulares.
2. Busque las series de texto que deben coincidir.

   Consejo: Para proporcionar comprobación básica de errores, incluya caracteres antes y después de los valores para impedir que coincidan accidentalmente valores similares. Posteriormente puede aislar el valor real de los caracteres adicionales.
3. Desarrolle pseudocódigo para la coincidencia de patrones e incluya el carácter de espacio para indicar el principio y el final de un patrón.

   Puede ignorar las comillas. En la entrada de registro de ejemplo, los nombres de suceso son DROP, CORRECTOS y REJECT. La lista siguiente muestra los campos de sucesos utilizables.
   - EventName: " kernel: VALUE "
   - SourceMAC: " MAC=VALUE "
   - SourceIp: " SRC=VALUE "
   - DestinationIp: " DST=VALUE "
   - Protocol: " PROTO=VALUE "
   - SourcePort: " SPT=VALUE "
   - DestinationPort: " DPT=VALUE "
4. Sustituya un espacio con la expresión regular `\s`.

   Debe utilizar un carácter de escape para los caracteres que no sean dígitos o alfanuméricos. Por ejemplo, = se convierte en \= y : se convierte en \:.
5. Convierta el pseudocódigo en una expresión regular.

Tabla 38. Conversión de pseudocódigo a expresiones regulares

Campo	Pseudocódigo	Expresión regular
EventName	" kernel: VALUE "	\skernel\:\s.*?\s
SourceMAC	" MAC=VALUE "	\sMAC\=(?:[0-9a-fA-F]{2}\ :){5}[0-9a-fA-F]{2}\s
SourceIP	" SRC=VALUE "	\sSRC\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s
DestinationIp	" DST=VALUE "	\sDST\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s
Protocol	" PROTO=VALUE "	\sPROTO\ =(TCP|UDP|ICMP|GRE)\s
SourcePort	" SPT=VALUE "	\sSPT\=\d{1,5}\s
DestinationPort	" DPT=VALUE "	\sDPT\=\d{1,5}\s

6. Especifique grupos de captura.

   Un grupo de captura aísla un valor determinado en la expresión regular.

   Por ejemplo, en el patrón SourcePort del ejemplo anterior, no puede pasar el valor completo, ya que éste incluye espacios y `SRC=<code>`. En lugar de ello, especifique sólo el número de puerto utilizando un grupo de captura. El valor del grupo de captura es lo que se pasa al campo relevante de IBM Security QRadar.

   Inserte paréntesis alrededor de los valores que desee capturar:

Tabla 39. Correlación de expresiones regulares con grupos de captura para campos de suceso

Campo	Expresión regular	Grupo de captura
EventName	\skernel\:\s.*?\s	\skernel\:\s(.*?)\s
SourceMAC	\sMAC\=(?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2}\s	\sMAC\=((?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2})\s
SourceIP	\sSRC\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s	\sSRC\=(\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3})\s
Destination IP	\sDST\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s	\sDST\=(\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3})\s
Protocol	\sPROTO\ =(TCP|UDP|ICMP|GRE)\s	\sPROTO\ =((TCP|UDP|ICMP|GRE))\s
SourcePort	\sSPT\=\d{1,5}\s	\sSPT\=(\d{1,5})\s
DestinationPort	\sDPT\=\d{1,5}\s	\sDPT\=(\d{1,5})\s

7. Migre los patrones y grupos de captura al documento de extensiones de origen de registro.

   El fragmento de código siguiente muestra parte del documento que se utiliza.

```
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
```

Cargar documentos de extensión en QRadar

Puede crear varios documentos de extensión y, a continuación, cargarlos y asociarlos a diversos tipos de origen de registro. La lógica de la extensión de origen de registro (LSX) se utiliza a continuación para analizar los registros del origen de registro no soportado.

Los documentos de extensión pueden almacenarse en cualquier lugar antes de cargarlos en IBM Security QRadar.

Procedimiento

1. En la pestaña **Admin**, pulse **Orígenes de datos** > **Extensiones de origen de registro**.
2. En la ventana Añadir extensiones de origen de registro, pulse **Añadir**.
3. Asigne un nombre.
4. Si está utilizando el Universal DSM, no seleccione el documento de extensión como valor predeterminado para un **Tipo de origen de registro**.

   La selección del Universal DSM como valor predeterminado afecta a todos los orígenes de registro asociados. Un Universal DSM puede utilizarse para definir la lógica de análisis para varios orígenes de sucesos personalizados y no soportados.
5. Opcional: Si desea aplicar esta extensión de origen de registro a más de una instancia de un tipo de origen de registro, seleccione el tipo de origen de registro en la lista de **Tipos de origen de registro** disponibles y pulse la flecha de adición para establecerlos como predeterminado.

   El establecimiento del tipo de origen de registro predeterminado aplica la extensión de origen de registro a todos los sucesos de un tipo de origen de registro, incluidos los orígenes de registro que se descubren automáticamente.

   Asegúrese de probar primero la extensión para el tipo de origen de registro para asegurarse de que los sucesos se analizan correctamente.
6. Pulse **Examinar** para localizar la LSX que ha guardado y, a continuación, pulse **Cargar**.

   QRadar valida el documento con respecto al XSD interno y verifica la validez del documento antes de que el documento de extensión se cargue en el sistema.
7. Haga clic en **Guardar** y cierre la ventana.
8. Asocie la extensión de origen de registro a un origen de registro.
   a. En la pestaña **Admin**, pulse **Orígenes de datos** > **Orígenes de registro**.
   b. Efectúe una doble pulsación en el tipo de origen de registro para el que ha creado el documento de extensión.
   c. En la lista **Extensión de origen de registro**, seleccione el documento que ha creado.
   d. Haga clic en **Guardar** y cierre la ventana.

Correlacionar sucesos desconocidos

Inicialmente, todos los sucesos del Universal DSM aparecen como desconocidos en la pestaña **Actividad de registro** de QRadar. Debe correlacionar manualmente todos los sucesos desconocidos con sus equivalentes de la correlación de QID.

Aunque los nombres de suceso, tales como DROP, DENY y ACCEPT, pueden ser valores comprensibles al visualizarlos en los archivos de registro, QRadar no entiende lo que estos valores representan. Para QRadar, estos valores son series de texto que no están correlacionadas con ningún valor conocido. Los valores aparecen según lo esperado y se tratan como sucesos normalizados hasta que se correlacionan manualmente.

En algunos casos, como por ejemplo en un sistema de detección de intrusiones (IDS) o en un sistema de detección y prevención de intrusiones (IDP), existen miles de sucesos que requieren correlación. En estas situaciones, puede correlacionar una

categoría como el nombre de suceso en lugar del suceso propiamente dicho. Por ejemplo, en el ejemplo siguiente, para reducir el número de correlaciones, en lugar de utilizar el campo de nombre para el nombre de suceso, se utiliza el campo de categoría. Puede utilizar una propiedad personalizada para visualizar el nombre de suceso (Code Red v412):

```
date: "Feb 25 2010 00:43:26"; name: "SQL Slammer v312"; category: "Worm
Activity"; source ip: "100.100.200.200";⌂date:
"Feb 25 2015 00:43:26"; name: "Code Red v412"; category: "Worm Activity";
source ip: "100.100.200.200"; date: "Feb 25 2015 00:43:26"; name:
"Annoying Toolbar"; category: "Malware"; source ip: "100.100.200.200";
```

En lugar de utilizar el campo de nombre para el nombre de suceso, utilice el campo de categoría. El nombre real del suceso, por ejemplo Code Red v412, puede visualizarse utilizando una propiedad personalizada.

Antes de empezar

Asegúrese de haber cargado el documento de extensión de origen de registro y de haberlo aplicado al DSM Universal. Para obtener más información, consulte "Cargar documentos de extensión en QRadar" en la página 45.

Procedimiento

1. En la pestaña **Actividad de registro**, pulse **Buscar** > **Editar búsqueda**.
2. En las opciones de **Rango de tiempo**, seleccione un tiempo suficiente, por ejemplo 15 minutos, a partir del momento en que la extensión de origen de registro se ha aplicado al DSM Universal.
3. En **Parámetros de búsqueda**, seleccione **Origen de registro [Índice]** en la lista **Parámetro**, **Igual que** en la lista **Operador** y, a continuación, seleccione el origen de registro que ha creado en las listas **Grupo de origen de registro** y **Origen de registro**.
4. Pulse **Buscar** para ver los resultados.

   Todos los sucesos aparecen como desconocidos.
5. Efectúe una doble pulsación sobre una entrada desconocida para ver los detalles del suceso.
6. Pulse **Correlacionar suceso** en la barra de herramientas.

   El valor **ID de suceso de origen de registro** muestra un **valor de EventName**, por ejemplo, DROP, DENY o ACCEPT, de la extensión de origen de registro. El valor no puede estar en blanco. Un valor en blanco indica que hay un error en el documento de extensión de origen de registro.
7. Correlacione el valor que se visualiza como **ID de suceso de origen de registro** con el QID adecuado.

   Utilice **Examinar por categoría**, **Búsqueda de QID** o ambos para encontrar el valor que mejor coincida con el valor de **ID de suceso de origen de registro**. Por ejemplo, el valor DROP puede correlacionarse con **QID Firewall Deny - Event CRE**.

   Utilice el QID con Event CRE en el nombre. La mayoría de los sucesos son específicos de un tipo de origen de registro determinado. Por ejemplo, cuando se correlaciona con un cortafuegos aleatorio, **Deny QID** es similar a correlacionar el DSM Universal con sucesos de otro tipo de origen de registro. Las entradas de QID que contienen el nombre Event CRE son genéricos y no están asociados a un tipo de origen de registro determinado.
8. Repita estos pasos hasta que todos los sucesos desconocidos se hayan correlacionado satisfactoriamente.

A partir de este punto, los sucesos adicionales del DSM Universal que contengan ese ID de suceso de origen de registro en particular aparecerán como el QID especificado. Los sucesos que hayan llegado antes de la correlación del QID seguirán siendo desconocidos. No hay ningún método soportado para la correlación de sucesos anteriores con un QID actual. Este proceso debe repetirse hasta que todos los tipos de sucesos desconocidos se hayan correlacionado satisfactoriamente con un QID.

Problemas y ejemplos de análisis

Cuando se crea una extensión de origen de registro, es posible que encuentre algunos problemas de análisis. Utilice estos ejemplos de XML para resolver problemas específicos de análisis.

Convertir un protocolo

El ejemplo siguiente muestra una conversión de protocolo habitual que busca TCP, UDP, ICMP o GRE en cualquier lugar de la carga útil. El patrón de búsqueda está delimitado por cualquier límite de palabra, por ejemplo, tabulador, espacio o fin de línea. Además, las mayúsculas y minúsculas de los caracteres se ignoran:

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[\b(TCP|UDP|ICMP|GRE)\b]]>
</pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol" capture-group="1" />
```

Efectuar una única sustitución

El ejemplo siguiente muestra una sustitución que analiza la dirección IP de origen y, a continuación, altera temporalmente el resultado y establece la dirección IP en 100.100.100.100, ignorando la dirección IP de la carga útil.

En este ejemplo se presupone que la dirección IP de origen coincide con algo parecido a `SrcAddress=10.3.111.33` seguido por una coma:

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}),]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK"
capture-group="100.100.100.100" enable-substitutions="true"/>
```

Generar una dirección MAC separada por dos puntos

QRadar detecta direcciones MAC en un formato de separación por dos puntos. Puesto que es que posible que no todos los dispositivos utilicen este formato, el ejemplo siguiente muestra cómo corregir dicha situación:

```
<pattern id="SourceMACWithDashes" xmlns="">
    <![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-
    ([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})]]>
</pattern>
 <matcher field="SourceMAC" order="1" pattern-id="
    SourceMACWithDashes" capture-group="\1:\2:\3:\4:\5:\6" />
```

En el ejemplo anterior, `SourceMAC=12-34-56-78-90-AB` se convierte a una dirección MAC `12:34:56:78:90:AB`.

Si se eliminan los guiones del patrón, éste convierte una dirección MAC y no tiene separadores. Si se insertan espacios, el patrón convierte una dirección MAC separadas por espacios.

Combinar dirección IP y puerto

Normalmente, una dirección IP y un puerto se combinan en un campo, que está separado por dos puntos.

En el ejemplo siguiente se utilizan varios grupos de captura con un patrón:

```
pattern id="SourceIPColonPort" xmlns="">
<! [CDATA[Source=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([\d]{1,5})]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1" pattern-id="SourceIPColonPort" capture-group="2" />
```

Modificar una categoría de suceso

Puede codificarse una categoría de suceso de dispositivo o ajustarse la gravedad.

El ejemplo siguiente ajusta la gravedad de un tipo de suceso único:

```
<event-match-single event-name="TheEvent" device-event-category="Actual
Category" severity="6" send-identity="UseDSMResults" />
```

Suprimir sucesos de cambio de identidad

Un DSM puede enviar innecesariamente sucesos de cambio de identidad.

Los ejemplos siguientes muestran cómo suprimir sucesos de cambio de identidad para que no se envíen desde un tipo de suceso único y un grupo de sucesos.

```
// No enviar nunca la identidad del suceso con un EventName de Authen OK
<event-match-single event-name="Authen OK" device-event-category="ACS"
severity="6" send-identity="OverrideAndNeverSend" />

// No enviar nunca ninguna identidad para un suceso con un nombre de suceso que
empiece por 7, seguido de uno a cinco dígitos:
<pattern id="EventNameId" xmlns=""><![CDATA[(7\d{1,5})]]>
</pattern>

<event-match-multiple pattern-id="EventNameId" capture-group-index="1"
device-event-category="Cisco Firewall" severity="7"
send-identity="OverrideAndNeverSend"/>
```

Codificar registros

Están soportados los siguientes formatos de codificación:

- US-ASCII
- UTF-8

Puede reenviar registros al sistema en una codificación que no coincida con los formatos US-ASCII o UTF-8. Puede configurar un distintivo avanzado para asegurarse de que la entrada pueda recodificarse en UTF-8 a efectos de análisis y almacenamiento.

Por ejemplo, si desea asegurarse de que los registros de origen lleguen en la codificación SHIFT-JIS (ANSI/OEM japonés), escriba el código siguiente:

```
<device-extension source-encoding=SHIFT-JIS xmlns=event_parsing/device_extension>
```

Los registros se especifican en formato UTF-8.

Formato de indicaciones de fecha y hora de suceso

Una extensión de origen de registro puede detectar varios formatos de indicación de fecha y hora en los sucesos.

Dado que los fabricantes de dispositivos no se ajustan a un formato de indicación de fecha y hora estándar, se incluye el parámetro opcional ext-data en la extensión de origen de registro para permitir el formateo de DeviceTime. El ejemplo siguiente muestra cómo puede reformatearse un suceso para corregir el formato de indicación de fecha y hora:

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\]</pattern>
<pattern id="Username">(TLSv1)</pattern>

<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1_Pattern" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1_Pattern"
   capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username_Pattern" capture-group="1"/>
</match-group>
</device-extension>
```

Varios formatos de registro en un único origen de registro

Ocasionalmente, se incluyen varios formatos de registro en un único origen de registro.

```
May 20 17:15:50 kernel: DROP IN=vlan2 OUT= MAC= SRC=67.149.62.133
DST=239.255.255.250 PROTO=UDP SPT=1900 DPT=1900
May 20 17:16:26 dropbear[22331]: password auth succeeded for 'root' from 192.168.50.80:3364
May 20 17:16:28 dropbear[22331]: exit after auth (root): Exited normally </br>
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root' from 192.168.50.80:3364
```

Por ejemplo, hay 2 formatos de registro: uno para los sucesos de cortafuegos y uno para los sucesos de autenticación. Debe escribir varios patrones para analizar los sucesos. Puede especificar el orden de análisis. Normalmente, los sucesos más frecuentes se analizan en primer lugar, seguidos de los sucesos menos frecuentes. Puede tener tantos patrones como sean necesarios para analizar todos los sucesos. La variable de orden determina el orden de comparación de los patrones.

El ejemplo siguiente muestra varios formatos para los campos siguientes EventName y UserName

se escriben patrones independientes para analizar cada tipo de registro exclusivo. Se hace referencia a ambos patrones al asignar el valor a los campos normalizados.

```
<pattern id="EventName-DDWRT-FW_Pattern" xmlns=""><![CDATA[kernel\:\s(.*?)\s]]></pattern>
<pattern id="EventName-DDWRT-Auth_Pattern" xmlns=""><![CDATA[sdrophear\[\d{1,5}\]|:\s(.*?\s.*?)\s]]>
</pattern>

<pattern id="UserName_DDWRT-Auth1__Pattern" xmlns=""><![CDATA[\sfor\s\'(.*?)\'s]]></pattern>
<pattern id="UserName_DDWRT-Auth2__Pattern" xmlns=""><![CDATA[\safter\sauth\s\((.*?)\)\:]]></pattern>

<match-group order="1" description="DD-WRT Device Extensions xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-DDWRT-FW_Pattern" capture-group="1"/>
   <matcher field="EventName" order="2" pattern-id="EventName-DDWRT-Auth_Pattern" capture-group="1"/>

   <matcher field="UserName" order="1" pattern-id="UserName-DDWRT-Auth1_Pattern" capture-group="1"/>
   <matcher field="UserName" order="2" pattern-id="UserName-DDWRT-Auth2_Pattern" capture-group="1"/>
```

Analizar un formato de registro CSV

Un archivo de registro con formato CSV puede utilizar un solo analizador que tenga varios grupos de captura. No siempre es necesario crear varios ID de patrón cuando se analiza este tipo de registro.

Acerca de esta tarea

Se utiliza el ejemplo de registro siguiente:

```
Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,bjones,192.168.50.100,1024,10.100.24.25,22
Successful Login,nlabadie,192.168.64.76,1743,10.100.24.25,110
Privilege Escalation,bjones,192.168.50.100,1028,10.100.1.100,23
```

Procedimiento

1. Cree un analizador que compare todos los valores relevantes utilizando los patrones anteriores.

   ```
   .*?\,.*?\,\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
   \,\d{1,5}\,\d{1,3}\.\d{1,3} \.\d{1,3}\.\d{1,3}\,\d{1,5}
   ```

2. Coloque los grupos de captura alrededor de cada valor:

   ```
   (.*?)\,(.*?)\,(\d{1,3}\.\d{1,3}\.\d{1,3}\.
   \d{1,3})\,(\d{1,5})\,(\d{1,3} \.\d{1,3}\.\d{1,3}\.\d{1,3})\,(\d{1,5})
   ```

3. Correlacione el campo con el que está correlacionado cada grupo de captura, incrementando el valor al realizar el movimiento.

   ```
   1 = Event, 2 = User, 3 = Source IP,
   4 = Source Port, 5 = Destination IP, 6 = Destination Port
   ```

4. Incluya los valores de la extensión de origen de registro correlacionando el grupo de captura con el suceso relevante.

   El código siguiente muestra un ejemplo parcial de la correlación del grupo de captura con el suceso relevante.

   ```
   <pattern id="CSV-Parser_Pattern" xmlns=""><![CDATA 9.*?)\,(.*?)\,(\d{1,3}\.\{1,3}\.{1,3}]]></pattern>
   <match-group order="1" description="Log Source Extension xmlns="">
      <matcher field="EventName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="1"/>
      <matcher field="SourceIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="3"/>
      <matcher field="SourcePort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="4"/>
      <matcher field="DestinationIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="5"/>
      <matcher field="DestinationPort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="6"/>
      <matcher field="UserName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="2"/>
   ```

5. Cargue la extensión de origen de registro.
6. Correlacione los sucesos.

Tareas relacionadas:

"Correlacionar sucesos desconocidos" en la página 46
Inicialmente, todos los sucesos del Universal DSM aparecen como desconocidos en la pestaña **Actividad de registro** de QRadar. Debe correlacionar manualmente todos los sucesos desconocidos con sus equivalentes de la correlación de QID.

IDs de tipo de origen de registro

IBM Security QRadar admite diversos orígenes de registro, y cada origen de registro tiene un identificador. Utilice los ID de tipo de origen de registro en una sentencia `match-group`:

En la tabla siguiente se enumeran los tipos de origen de registro soportados y sus ID.

Tabla 40. ID de tipo de origen de registro

ID	Tipo de origen de registro
2	Snort Open Source IDS
3	Check Point Firewall-1
4	Filtro de cortafuegos configurable
5	Juniper Networks Firewall and VPN

Tabla 40. ID de tipo de origen de registro (continuación)

ID	Tipo de origen de registro
6	Cortafuegos PIX de Cisco
7	Filtro de mensajes de autenticación configurable
9	Enterasys Dragon Network IPS
10	Apache HTTP Server
11	SO Linux
12	Registro de sucesos de seguridad de Microsoft Windows
13	Windows IIS
14	Cortafuegos iptables de Linux
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Juniper Networks Intrusion Detection and Prevention (IDP)
19	TippingPoint Intrusion Prevention System (IPS)
20	Cisco IOS
21	Nortel Contivity VPN Switch
22	Nortel Multiprotocol Router
23	Cisco VPN 3000 Series Cntrator
24	Solaris Operating System Authentication Messages
25	McAfee IntruShield Network IPS Appliance
26	Cisco CSA
28	Enterasys Matrix E1 Switch
29	Solaris Operating System Sendmail Logs
30	Cisco Intrusion Prevention System (IDS)
31	Cisco Firewall Services Module (FWSM)
33	IBM Proventia Management SiteProtector
35	Cyberguard FW/VPN KS Family
36	Juniper Networks Secure Access (SA) SSL VPN
37	Nortel Contivity VPN Switch
38	Top Layer Intrusion Prevention System (IPS)
39	Universal DSM
40	Tripwire Enterprise
41	Cisco Adaptive Security Appliance (ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager (NSM)
46	Squid Web Proxy
47	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)

Tabla 40. ID de tipo de origen de registro (continuación)

ID	Tipo de origen de registro
48	Oracle RDBMS Audit Records
49	F5 Networks BIG-IP LTM
50	Solaris Operating System DHCP Logs
55	Array Networks SSL VPN Access Gateway
56	Cisco CatOS for Catalyst Switches
57	ProFTPD Server
58	Linux DHCP Server
59	Juniper Networks Infranet Controller
64	Juniper JunOS Platform
68	Enterasys Matrix K/N/S Series Switch
70	Extreme Networks ExtremeWare Operating System (OS)
71	Sidewinder G2 Security Appliance
73	Fortinet FortiGate Security Gateway
78	Dispositivo SonicWall UTM/Firewall/VPN
79	Vericept Content 360
82	Dispositivo Symantec Gateway Security (SGS)
83	Juniper Steel Belted Radius
85	IBM AIX Server
86	Metainfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	Dispositivo CiscoNAC
96	TippingPoint X Series Appliances
97	Microsoft DHCP Server
98	Microsoft IAS Server
99	Microsoft Exchange Server
100	Trend Interscan VirusWall
101	Microsoft SQL Server
102	MAC OS X
103	Dispositivo Bluecoat SG
104	Nortel Switched Firewall 6000
106	3Com 8800 Series Switch
107	Nortel VPN Gateway
108	Nortel Threat Protection System (TPS) Intrusion Sensor
110	Nortel Application Switch

Tabla 40. ID de tipo de origen de registro (continuación)

ID	Tipo de origen de registro
111	Juniper DX Application Acceleration Platform
112	SNARE Reflector Server
113	Cisco 12000 Series Routers
114	Cisco 6500 Series Switches
115	Cisco 7600 Series Routers
116	Cisco Carrier Routing System
117	Cisco Integrated Services Router
118	Juniper M-Series Multiservice Edge Routing
120	Nortel Switched Firewall 5100
122	Juniper MX-Series Ethernet Services Router
123	Juniper T-Series Core Platform
134	Nortel Ethernet Routing Switch 8300/8600
135	Nortel Ethernet Routing Switch 2500/4500/5500
136	Nortel Secure Router
138	OpenBSD OS
139	Juniper Ex-Series Ethernet Switch
140	Sysmark Power Broker
141	Oracle Database Listener
142	Samhain HIDS
143	Bridgewater Systems AAA Service Controller
144	Par nombre-valor
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)
148	IBM AS/400 iSeries
149	Foundry Fastiron
150	Juniper SRX Series Services Gateway
153	CRYPTOCard CRYPTOShield
154	Imperva Securesphere
155	Aruba Mobility Controller
156	Enterasys NetsightASM
157	Enterasys HiGuard
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan

Tabla 40. ID de tipo de origen de registro (continuación)

ID	Tipo de origen de registro
166	Direccionadores de seguridad XSR de Enterasys
167	Conmutadores apilables y autónomos de Enterasys
168	Juniper Networks AVT
169	OS Services Qidmap
170	Enterasys A-Series
171	Enterasys B2-Series
172	Enterasys B3-Series
173	Enterasys C2-Series
174	Enterasys C3-Series
175	Enterasys D-Series
176	Enterasys G-Series
177	Enterasys I-Series
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro
194	Cisco ACE Firewall
195	IBM DB2
196	Oracle Audit Vault
197	Sourcefire Defense Center
198	Websense V Series
199	Oracle RDBMS OS Audit Record
206	Palo Alto PA Series
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
213	F5 Networks BIG-IP ASM
214	FireEye

Tabla 40. ID de tipo de origen de registro (continuación)

ID	Tipo de origen de registro
215	Fair Warning
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	McAfee Web Gateway
221	CA Access Control Facility (ACF2)
222	McAfee Application / Change Control
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron Smart Meter
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Sophos Web Security Appliance
241	Sophos Astaro Security Gateway
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory
249	IBM Guardium
251	Stonesoft Management Center
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
263	Conmutador Digital China Networks DCS y DCRS Series
264	Juniper Security Binary Log Collector
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business

Tabla 40. ID de tipo de origen de registro (continuación)

ID	Tipo de origen de registro
268	Verdasys Digital Guardian
269	Hauwei S Series Switch
271	HBGary Active Defense
272	APC UPS
272	Cisco Wireless LAN Controller
276	IBM Customer Information Control System (CICS)
278	Cortafuegos de correo no deseado & virus Barracuda
279	Open LDAP
280	Application Security DbProtect
281	Barracuda Web Application Firewall
283	Huawei AR Series Router
286	IBM AIX Audit
289	IBM Tivoli Endpoint Manager
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Enterasys 800-Series Switch
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP AFM
297	IBM Security Network IPS (GX)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS
303	ThreatGRID Malware Threat Intelligence Platform
304	IBM Security Access Manager for Enterprise Single Sign-On
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT
311	Pirean Access: One
312	Venustech Venusense Security Platform
313	PostFix MailTransferAgent
314	Oracle Fine Grained Auditing
315	VMware vCenter

Tabla 40. ID de tipo de origen de registro (continuación)

ID	Tipo de origen de registro
316	Cisco Identity Services Engine
318	Honeycomb Lexicon File Integrity Monitor
319	Oracle Acme Packet SBC
320	Juniper WirelessLAN
330	Arbor Networks Peakflow SP
331	Zscaler Nss
332	Proofpoint Enterprise Protection/Enterprise Privacy
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Vormetric Data Security
341	SafeNet DataSecure/KeySecure
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	Trusteer Apex
348	IBM Security Directory Server
349	Enterasys A4-Series
350	Enterasys B5-Series
351	Enterasys C5-Series
354	Avaya VPN Gateway
356	DG Technology MEAS
358	CloudPassage Halo
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS
361	IBM Fiberlink MaaS360
362	Trend Micro Deep Discovery Analyzer
363	AccessData InSight
364	BM Privileged Session Recorder
367	Universal CEF
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
372	SSH CryptoAuditor
373	IBM WebSphere DataPower
374	Symantec Critical System Protection
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
378	Lastline Enterprise
379	genua genugate
383	Oracle Enterprise Manager

Capítulo 3. Gestión de extensiones de orígenes de registro

Puede crear extensiones de orígenes de registro para ampliar o modificar las rutinas de análisis de dispositivos determinados.

Una *extensión de origen de registro* es un archivo XML que incluye todos los patrones de expresión regular que son necesarios para identificar y categorizar sucesos de la carga útil de sucesos. Se pueden utilizar archivos de extensión para analizar sucesos cuando el usuario debe corregir un problema de análisis o debe alterar temporalmente el análisis predeterminado para un suceso de un DSM (Device Support Module). Cuando no existe un DSM para analizar sucesos para un dispositivo o dispositivo de seguridad de la red, una extensión puede proporcionar soporte de sucesos. El panel **Actividad de registro** distingue estos tipos básicos de sucesos de origen de registro:

- Orígenes de registro que analizan debidamente el suceso. Los sucesos analizados debidamente se asignan al tipo y categoría correctos de origen de registro. En este caso, no es necesaria ninguna intervención ni extensión.
- Orígenes de registro que analizan sucesos, pero cuyo parámetro **Origen de registro** tiene el valor **Desconocido**. Los sucesos desconocidos son sucesos de origen de registro en los que se conoce el tipo de origen de registro, pero el DSM no puede comprender la información de carga útil. El sistema no puede determinar un identificador de suceso a partir de la información disponible para clasificar correctamente el suceso. En este caso, no se puede asignar el suceso a una categoría ni escribir una extensión de origen de registro para reparar el análisis de sucesos para sucesos desconocidos.
- Orígenes de registro que no pueden identificar el tipo de origen de registro y cuyo parámetro **Origen de registro** tiene el valor **Almacenado**. Los sucesos almacenados necesitan que el usuario actualice los archivos de DSM o escriba una extensión de origen de registro para analizar debidamente el suceso. Una vez analizado el suceso, puede correlacionarlo.

Para añadir una extensión de origen de registro, debe crear el documento de la extensión. El documento de extensión es un documento XML que puede crear con cualquier aplicación habitual de proceso o edición de texto. Se pueden crear y cargar varios documentos de extensión y asociarlos a diversos tipos de origen de registro. El formato del documento de extensión se debe ajustar al formato XSD (XML Schema Document). Para crear un documento de extensión, es necesario tener conocimientos y experiencia sobre la codificación XML.

Añadir una extensión de origen de registro

Puede añadir una extensión de origen de registro para ampliar o modificar las rutinas de análisis de dispositivos determinados.

Procedimiento

1. Pulse la pestaña **Admin**.
2. Pulse el icono **Extensiones de origen de registro**.
3. Pulse **Añadir**.
4. En la lista **Tipos de origen de registro**, seleccione una de las opciones siguientes:

Opción	Descripción
Disponible	Seleccione esta opción cuando el módulo de soporte de dispositivo (DSM) analiza correctamente la mayoría de los campos del origen de registro. Los valores de campo analizados incorrectamente se mejoran con los nuevos valores XML.
Establecido en el valor predeterminado para	Seleccione los orígenes de registro que se deben añadir o eliminar del análisis de extensión. Puede añadir o eliminar extensiones de un origen de registro. Cuando una extensión de origen de registro se ha **Establecido en el valor predeterminado para** un origen de registro, los orígenes de registro nuevos del mismo **Tipo de origen de registro** utilizan la extensión de origen de registro asignada.

5. Pulse **Examinar** para localizar el documento XML de la extensión de origen de registro.
6. Pulse **Cargar**. Se mostrará el contenido de la extensión de origen de registro para asegurarse de que se carga el archivo de extensión adecuado. Cuando se carga el archivo de extensión, el archivo se compara con el XSD para comprobar si contiene errores.
7. Pulse **Guardar**.

Resultados

Si el archivo de extensión no contiene ningún error, se crea y habilita la nueva extensión de origen de registro. Se puede cargar una extensión de origen de registro sin aplicar la extensión a un origen de registro. Los cambios en el estado de una extensión se aplican inmediatamente y los hosts gestionados o consolas aplican los nuevos parámetros de análisis de sucesos en la extensión de origen de registro.

Qué hacer a continuación

En el panel **Actividad de registro**, verifique que los patrones de análisis para sucesos se han aplicado correctamente. Si el origen de registro clasifica los sucesos como **Almacenado**, es necesario ajustar el patrón de análisis en la extensión de origen de registro. Puede comparar el archivo de extensión con sucesos de origen de registro para localizar problemas de análisis de sucesos.

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 y características descritos en este documento. Consulte al representante local de IBM para obtener información sobre los productos y servicios que están disponibles actualmente en su localidad. Cualquier referencia a un programa, producto o servicio de IBM no pretende establecer ni implicar que sólo se pueda utilizar ese producto, programa o servicio de 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. Pero corresponde al usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen la materia descrita en este documento. El suministro de este documento no le otorga ninguna licencia sobre estas 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), consulte al departamento de Propiedad intelectual de IBM de su país o envíe 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 al Reino Unido ni a 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 ADECUACIÓN PARA UN FIN DETERMINADO. Algunas legislaciones no permiten la renuncia de garantías expresas ni implícitas en determinadas transacciones, por lo que es posible que esta declaración no sea aplicable en su caso.

Esta información puede contener inexactitudes 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.

Cualquier referencia en esta información a sitios web que no sean de IBM se proporciona sólo a efectos prácticos y no constituye un aval de esos sitios web. La información de esos sitios web no forman parte de la información del presente producto de IBM y el uso de esos sitios web se realiza bajo la 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 licenciatarios de este programa que deseen tener información sobre él para permitir: (i) el intercambio de información entre programas creados por separado y otros programas (incluido el presente) y (ii) el uso mutuo de la información intercambiada, se deben poner en contacto con:

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

Esta información puede estar disponible, sujeta a los términos y condiciones apropiados, 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 él según los términos del Acuerdo del cliente de IBM, el Acuerdo internacional de programas bajo licencia de IBM o cualquier acuerdo equivalente entre ambas partes.

Los datos de rendimiento contenidos en este documento se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Algunas mediciones se han realizado en sistemas a nivel de desarrollo y no es seguro que estas mediciones serán las mismas en los sistemas de uso general. Además, algunas mediciones se han calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios del presente documento deben verificar los datos aplicables correspondientes al entorno específico utilizado.

La información referente a productos que no son de IBM se ha obtenido a partir de los proveedores de esos productos, sus anuncios publicados u otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad ni ninguna otra declaración referente a productos que no son de IBM. Las preguntas referentes a prestaciones de productos que no son de IBM se debe dirigir a los proveedores de esos 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 recomendados por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden variar.

La presente información contiene ejemplos de datos e informes que se utilizan en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos

estos nombres son ficticios. Cualquier similitud con los nombres y direcciones utilizados por una empresa real es completamente accidental.

Si está viendo la presente información en forma de copia software, las fotografías y figuras en color pueden no ser visibles.

Marcas registradas

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

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

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

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

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

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 éstas y otras marcas registradas de IBM aparecen marcadas en su primera aparición en esta información con un símbolo de marca registrada (® o ™), estos símbolos denotan marcas registradas en Estados Unidos o marcas registradas de derecho común que son propiedad de IBM en el momento de publicar esta información. Estas marcas registradas también pueden ser marcas registradas o marcas registradas de derecho común en otros países. Encontrará una lista actual de marcas registradas de IBM en el sitio web: Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Los siguientes términos son marcas registradas de otras empresas:

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

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

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

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

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

Consideraciones sobre la política de privacidad

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

Dependiendo de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que obtienen el ID de sesión de cada usuario para gestionar y autenticar la sesión. Estos cookies se pueden inhabilitar, pero si se inhabilitan, también se elimina la funcionalidad que los cookies hacen posible.

Si las configuraciones desplegadas para esta Oferta de software le proporcionan como cliente la capacidad 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, lo cual 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.

Índice

Impreso en España