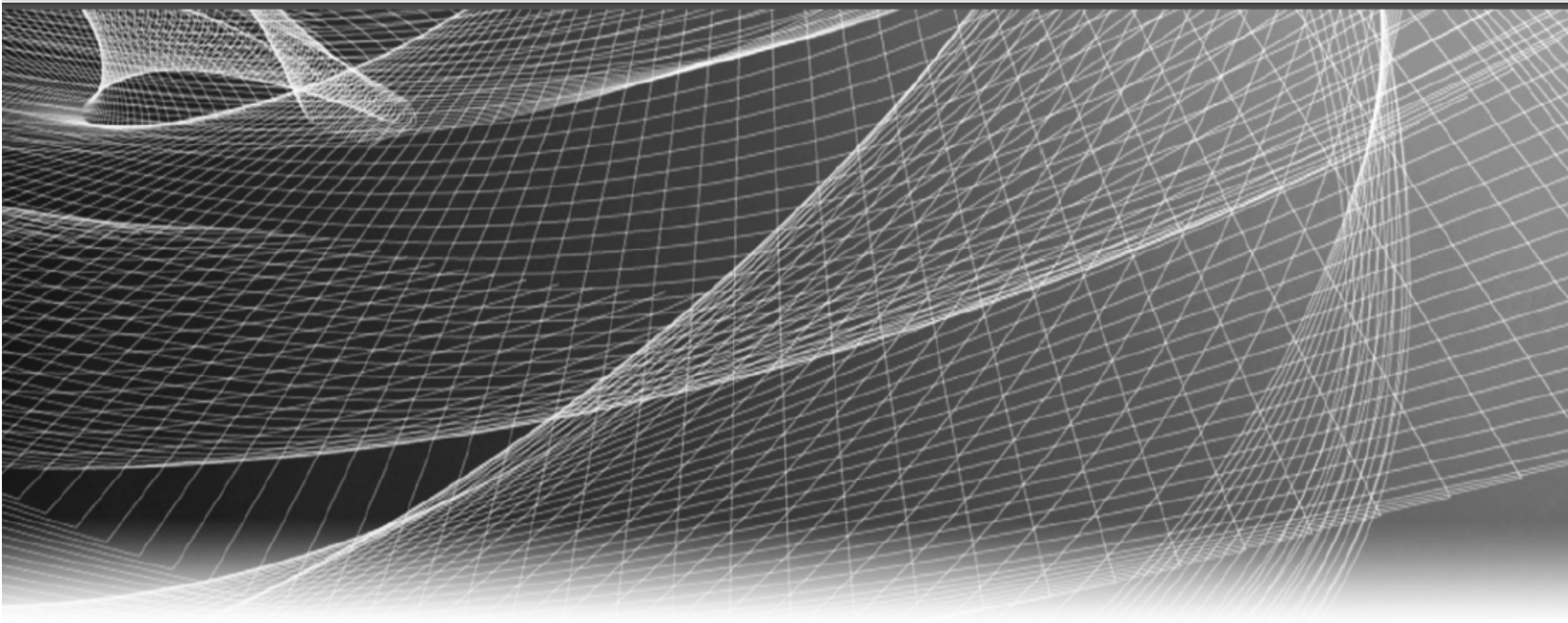


RSA Security Analytics

# Administración de orígenes de eventos

para la versión 10.6

RSA EMC²

## Marcas comerciales



## Acuerdo de licencia



## Licencias de otros fabricantes



## Nota sobre tecnologías de cifrado



## Distribución

# Contenido

# Acerca de la administración de orígenes de eventos

El módulo Origen de evento de Security Analytics proporciona una manera sencilla de administrar orígenes de eventos y configurar políticas de alerta para ellos.

## Requisitos previos

Hay dos permisos que afectan a Administración de orígenes de eventos:

- **Ver orígenes de eventos** permite que los usuarios vean orígenes de eventos, sus atributos y sus umbrales y políticas.
- **Modificar orígenes de eventos** permite que los usuarios agreguen, editen y actualicen de otra manera los orígenes de eventos.

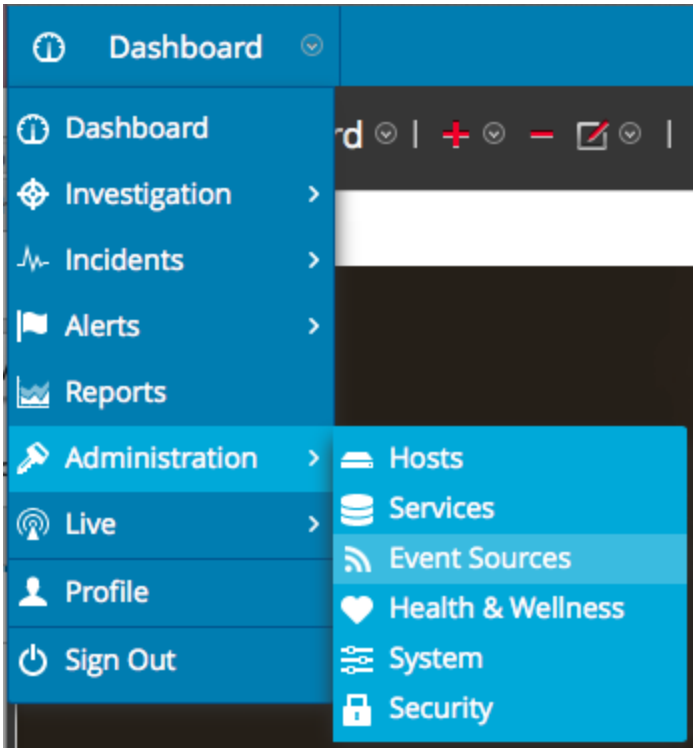
Para obtener más información, consulte los siguientes temas:

- El tema *Pestaña Funciones* disponible en la guía **Administración de usuarios y de la seguridad del sistema** > **Referencias** > **Vista Seguridad de Administration** > **Pestaña Funciones**.
- En el tema *Permisos de funciones* se describen las funciones del sistema incorporadas de Security Analytics, las cuales controlan el acceso a la interfaz del usuario. Disponible en la guía **Administración de usuarios y de la seguridad del sistema** > **Cómo funciona el control de acceso basado en funciones**.
- En el tema *Administrar usuarios con funciones y permisos* se describe cómo administrar usuarios en Security Analytics mediante funciones y permisos. Disponible en la guía **Administración de usuarios y de la seguridad del sistema** > **Administrar usuarios con funciones y permisos**.

## Desplácese hasta Administración de orígenes de eventos

Realice lo siguiente para ver los detalles de los grupos de orígenes de eventos existentes:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.




2. Haga clic en una de las siguientes opciones:
   - La pestaña **Administrar**. En esta pestaña se proporcionan detalles sobre los grupos de orígenes de eventos existentes.
   - La pestaña **Políticas de monitoreo**. Use esta pestaña para ver o editar la configuración de alertas de los orígenes de eventos.
   - La pestaña **Alarmas**. Use esta pestaña para ver los detalles de las alarmas que se han generado. Las alarmas se generan cuando los orígenes de eventos se superan o no alcanzan los umbrales establecidos.
   - La pestaña **Configuración**. Use esta pestaña para ver o cambiar el comportamiento de las alertas automáticas.

**Nota:** Cuando el sistema recibe registros de un origen de eventos que no existe actualmente en la lista de orígenes de eventos, Security Analytics agrega automáticamente el origen de eventos a la lista. Además, si coincide con los criterios de algún grupo existente, pasa a formar parte de ese grupo.

## Alarmas y notificaciones

El módulo Origen de evento en Security Analytics muestra alarmas y envía notificaciones en función de las alarmas que se activan.

Para las alarmas, considere lo siguiente:

Hay dos tipos de alarmas: **automática** (se activa cuando se superan o no se cumplen las bases) y **manual** (se configura con umbrales).

- **Automática**: Si activa las alertas automáticas, el sistema informa las alarmas de **todos** los orígenes de eventos que están por encima o por debajo de su base normal en la cantidad requerida. Puede especificar el porcentaje en exceso/insuficiente en la Pestaña Ajustes de configuración.
- **Manual**: Si apaga las alertas automáticas, recibirá alarmas solo para los grupos de orígenes de eventos para los cuales especificó, y habilitó, políticas (y umbrales).
- Las alarmas aparecen en la interfaz del usuario, en la Pestaña Alarmas.

Para las notificaciones, considere lo siguiente:

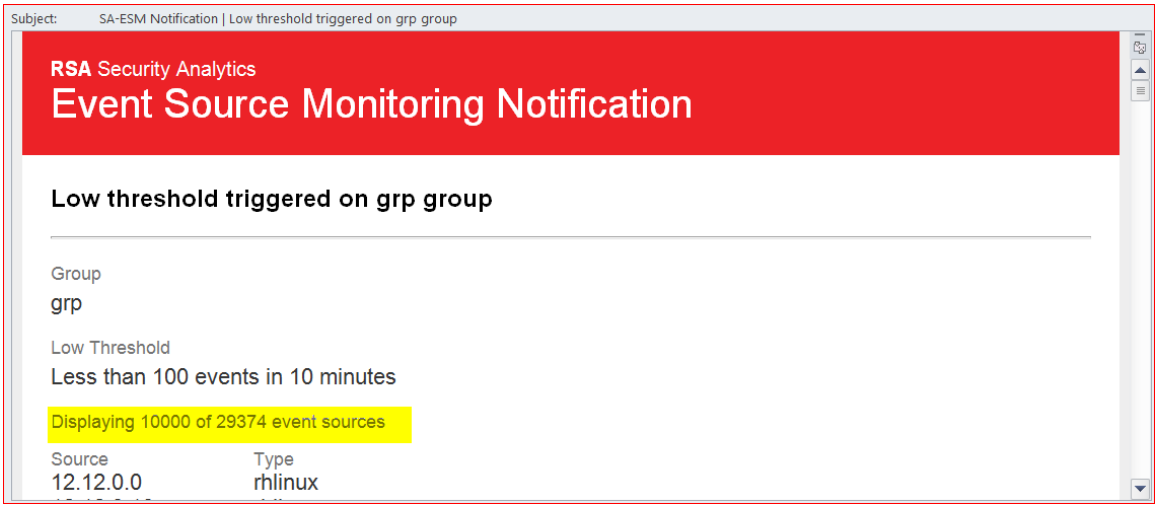
- Para recibir notificaciones manuales (a través de correo electrónico, SNMP o Syslog):
  - Especifique una política para un grupo de orígenes de eventos.
  - Configure un umbral alto o bajo (o ambos).
  - Habilite la política.
- Para recibir notificaciones automáticas (base):
  - Las alertas de base deben estar activadas. Esta opción está habilitada de manera predeterminada.
  - Debe habilitar las notificaciones desde el monitoreo automático. Consulte Configurar alertas automáticas para obtener detalles.
  - El origen de eventos que activa la alarma debe estar en un grupo que tenga habilitada una política.
- Si activó la alerta automática y configuró una política y un umbral para un grupo:
  - Si el origen de evento queda fuera de su base, verá una alerta automática y recibirá una notificación.
  - Si el origen de evento queda fuera de sus umbrales, verá una alerta manual y recibirá una notificación.

- Si se producen ambos escenarios (se supera o no se cumple el umbral y la base), recibirá dos alarmas (visibles en la pestaña Alarmas) y una notificación que indica ambas alarmas. Esa notificación indicará el origen de eventos que emitió dos veces la alarma; una de ellas indicará que se trató de una alarma automática.

## Notificaciones por correo electrónico grandes

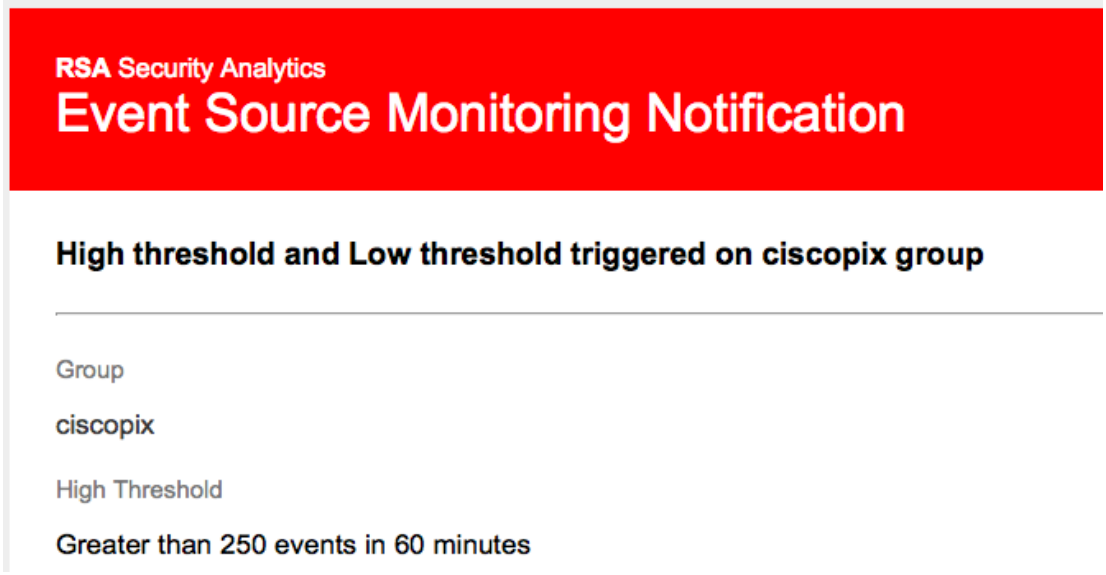
Si configuró notificaciones por correo electrónico, tenga presente que el correo electrónico puede crecer mucho de acuerdo con la cantidad de orígenes de eventos en la notificación.

Si los orígenes de eventos en el estado de alarma superan la cantidad de 10,000, la notificación por correo electrónico incluirá únicamente los detalles de los primeros 10,000 y un conteo total. Esto es para asegurarse de que el correo electrónico se entregue correctamente.




## Umbrales superior e inferior activados

Puede haber ocasiones en que se activen las alarmas superior e inferior para un grupo de orígenes de eventos específico. La manera más fácil de saber cuándo sucede esto es leer el encabezado del correo electrónico, el cual establece claramente si se activan ambos umbrales, como se muestra en esta imagen:




En este ejemplo, el encabezado señala “Se activó el umbral alto y el umbral bajo en el grupo ciscopix”. Para ver los detalles de los orígenes de eventos del umbral inferior, puede ser necesario desplazarse hacia abajo hasta pasar cientos, o incluso miles, de los orígenes de eventos del umbral superior.

## Alertas automáticas

En este tema se describen las alertas automáticas, que se basan en la configuración de base.

**Nota:** Las alertas automáticas y todos los parámetros que determinan su comportamiento, están actualmente en versión beta.

Puede configurar políticas y umbrales para los grupos de orígenes de eventos. Configúrelos de modo que reciba notificaciones cuando no se cumplan los umbrales. Security Analytics también proporciona un modo automático para recibir alarmas en caso de que no desee configurar umbrales para generar alarmas.

Puede usar valores de base para activar alertas automáticas. De esta forma,no es necesario configurar diversas políticas y umbrales de grupo a fin de recibir alertas. Cualquier cantidad anormal de mensajes activará las alertas, sin necesidad de realizar configuración alguna (excepto para la activación de las alertas automáticas).

Tenga en cuenta lo siguiente:

- Una vez que comienza a recopilar los mensajes de un origen de evento, el sistema tarda aproximadamente una semana en almacenar un valor de base para ese origen de evento. Finalizado este período inicial, el sistema le avisa cuando la cantidad de mensajes durante un período se encuentra por encima o por debajo de la base en una cantidad específica. De forma predeterminada, esta cantidad es 2 desviaciones estándares por encima o por debajo de la base.
- Base la configuración de desviación alta y baja en la “regularidad” del comportamiento de sus orígenes de eventos. Es decir, si espera poca o ninguna variación en la cantidad de mensajes que llegan durante una hora determinada (por ejemplo, 8:00 a 9:00 h en un día de semana), puede establecer un valor bajo para la desviación. Por el contrario, si ve a menudo ve horas punta y valle, configure la desviación en un valor superior.
- Si habilita una política, pero no ha configurado umbrales, puede seguir recibiendo notificaciones automáticas (base), siempre y cuando haya activado las alertas automáticas.

## Escenarios comunes para políticas de monitoreo

En general, las organizaciones monitorean sus orígenes de eventos en "depósitos" de acuerdo con la criticidad de estos. Un ejemplo típico es el siguiente:

- Hay un grupo de dispositivos PCI y es fundamental saber si alguno de estos deja de enviar mensajes (o si envía muy pocos) en un intervalo de media hora.
- Hay un grupo de dispositivos Windows y es útil saber si alguno de estos deja de enviar mensajes después de cuatro horas.
- Hay un grupo de dispositivos inactivos que generalmente no envían muchos mensajes, pero se desea saber si no envían nada durante 24 horas.

Muchas organizaciones pueden tener una red que se asemeja a este ejemplo. Es posible que tenga más categorías o categorías diferentes, pero este ejemplo se usa para analizar esta función.

Puede haber decenas o incluso cientos de grupos de orígenes de eventos y, sin embargo, solo necesita configurar umbrales y alertas para algunos grupos de ellos.

**Nota:** Si un origen de eventos es miembro de múltiples grupos en los cuales están configuradas las alertas, solo emitirá una alerta en el primer grupo coincidente en la lista ordenada. (En la pestaña Políticas de monitoreo se presenta una lista ordenada de los grupos).

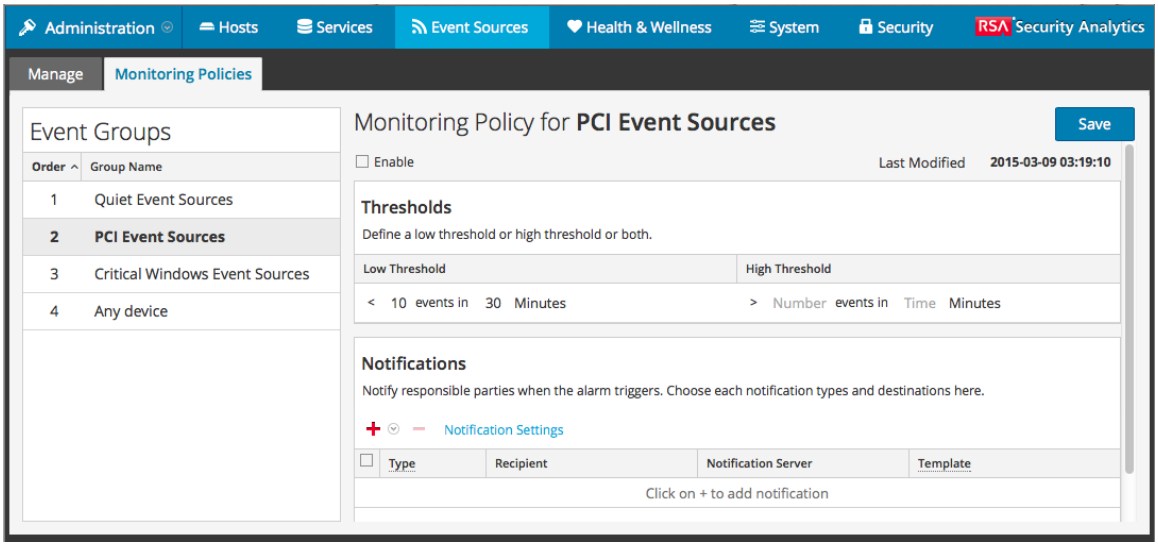
### Orden de los grupos

**Nota:** Para cambiar el orden de los grupos, arrastre y suelte un grupo en su nueva ubicación. Cuanto más alto se enumere un grupo, mayor será la prioridad de los umbrales de ese grupo: RSA Security Analytics comprueba los umbrales en el orden que se proporciona en este panel. De este modo, los grupos con prioridad más alta deben estar en la parte superior de esta lista.

Lo primero que se debe tener presente es cómo ordenar los grupos en la página Políticas de monitoreo. Suponga que tiene los tres grupos antes mencionados y que debe ordenarlos de la siguiente manera:

1. Orígenes de eventos inactivos. Con este grupo en primer lugar se asegura de no recibir numerosas alertas falsas.
2. Orígenes de eventos de PCI de alta prioridad. Los dispositivos con prioridad más alta se deben ubicar a continuación de los dispositivos inactivos
3. Orígenes de eventos de Windows. El rango de tiempo es mayor (cuatro horas frente a media hora) para estos dispositivos que para los dispositivos PCI. Por lo tanto, deben estar a continuación de los dispositivos de PCI.

4. Todos los orígenes de eventos. De manera opcional, puede configurar umbrales para todos los dispositivos a modo de captura general. Esto garantiza que la red completa funcione según lo previsto. Para el grupo general, no es necesario especificar umbrales; puede usar alertas automáticas para generar alarmas para los orígenes de eventos de este grupo.




En la figura anterior, observe lo siguiente:

- Los grupos se ordenan como se analiza en la sección anterior.
- El umbral para los dispositivos PCI tiene como objetivo advertir si llegan menos de 10 mensajes en 30 minutos a Security Analytics.
- Se define un umbral inferior, pero no uno superior. Esto es típico para muchos casos de uso.

Después de configurar y ordenar los grupos y de comenzar a recibir alertas, puede ser necesario ajustar el orden. Use esta guía como ayuda para ajustar el orden:

- Si recibe más notificaciones de las que necesita, puede colocar el grupo más abajo en el orden. De manera similar, si recibe muy pocas notificaciones, transfiera el grupo hacia la parte superior.
- Si observa que un origen de eventos está creando más alertas de lo que debería, puede transferirlo a otro grupo o crear un nuevo grupo para ese origen de eventos.

# Administrar grupos de orígenes de eventos

## Definiciones

Cuando trabaje con grupos de orígenes de eventos en Security Analytics, tenga en cuenta lo siguiente:

- Un **origen de eventos** es esencialmente la combinación de valores de todos sus atributos.
- Un **grupo de orígenes de eventos** es el conjunto de orígenes de eventos que coinciden con una serie de criterios que se definen para ese grupo.

Por ejemplo, podrían existir los siguientes grupos:

- Un grupo llamado **Dispositivos de Windows**, que consta de todos los tipos de orígenes de eventos asociados a orígenes de eventos de Microsoft Windows (`winevent_nic`, `winevent_er` y `winevent_snare`).
- Un grupo llamado **Servicios de prioridad baja**, que consta de todos los servicios cuyo atributo Prioridad se configuró en un valor menor que 5.
- Un grupo llamado **Servidores de ventas de EE. UU.**, donde se reúnen orígenes de eventos que se encuentran en EE. UU. cuyo atributo Organización corresponde a Ventas, Financiamiento o Marketing.

## Detalles de la pestaña Administrar

En la pestaña Administrar del módulo Origen de evento se proporciona una manera fácil de administrar orígenes de eventos. Esta pestaña permite:

- Configurar grupos de orígenes de eventos de manera coherente.
- Trabajar con atributos de orígenes de eventos de manera coherente y directa.
- Buscar fácilmente en el conjunto de orígenes de eventos completo.
- Editar y actualizar en masa los orígenes de eventos y los grupos de orígenes de eventos.

Realice lo siguiente para ver los detalles de los grupos de orígenes de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Orígenes de evento**.
2. Seleccione el panel **Administrar** para ver los detalles de los grupos de orígenes de eventos existentes.

**Nota:** Cuando el sistema recibe registros de un origen de eventos que no existe actualmente en la lista de orígenes de eventos, Security Analytics agrega automáticamente el origen de eventos a la lista. Además, si coincide con los criterios de algún grupo existente, pasa a formar parte de ese grupo.

## Grupos predeterminados

RSA Security Analytics tiene varios grupos predeterminados. Puede personalizarlos como prefiera y usarlos como plantillas para crear nuevos grupos.

Los valores predeterminados son los siguientes:

- Todos los orígenes de eventos
- Todos los orígenes de eventos de Unix
- Todos los orígenes de eventos de Windows
- Orígenes de eventos de Windows críticos
- Orígenes de eventos de PCI
- Orígenes de eventos inactivos

Puede editar cualquiera de estos grupos para investigar las reglas que los definen.

**Nota:** No puede editar ni eliminar el grupo de orígenes de eventos **Todos**.

## Crear grupos de orígenes de eventos

Los administradores deben recibir notificaciones cuando Security Analytics ya no recopila orígenes de eventos. Deben poder configurar cuánto tiempo pueden estar inactivos los orígenes de eventos (es decir, sin recopilar mensajes de registros) antes de que se envíe una notificación en función de distintos factores.

RSA Security Analytics proporciona grupos de orígenes de eventos de modo que sea posible agrupar dispositivos de similar importancia. Puede crear grupos en función de los atributos que importó desde la CMDB (base de datos de administración de configuración) o de forma manual si selecciona los orígenes de eventos que agregará al grupo.

Por ejemplo, estos son algunos de los tipos de grupos de orígenes de eventos que puede crear:

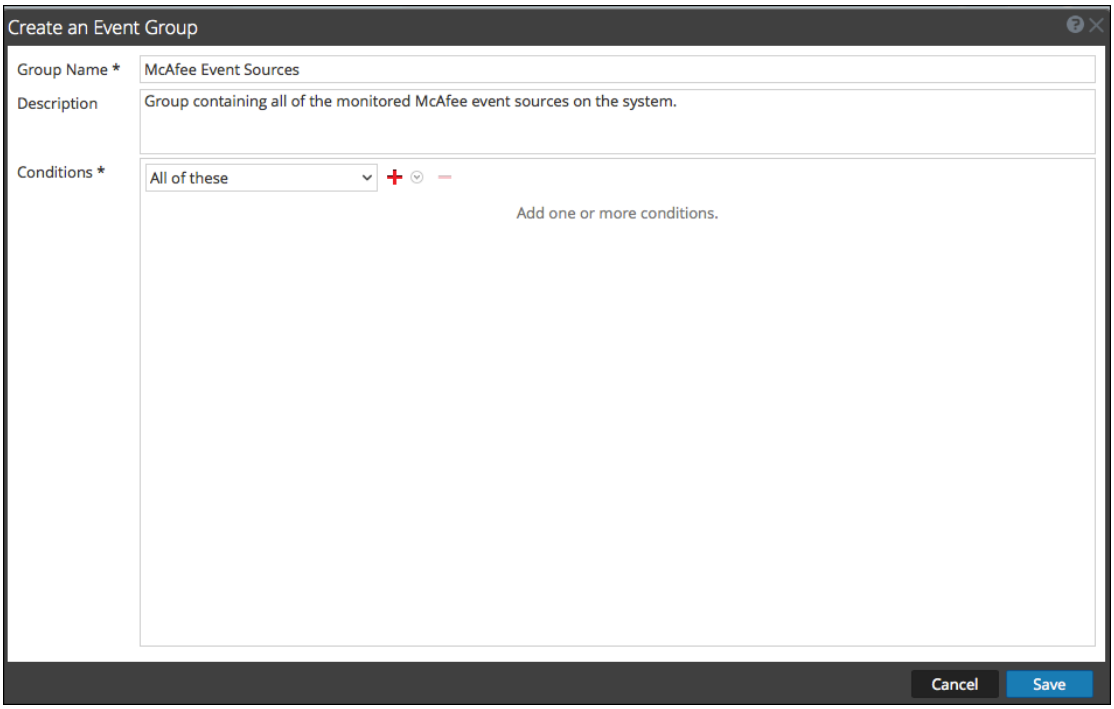
- Orígenes de PCI
- Controladoras de dominio de Windows
- Orígenes inactivos
- Servidores de financiamiento
- Dispositivos de prioridad alta
- Todos los orígenes de Windows

### Procedimiento

Para crear un grupo de orígenes de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. En el panel **Administrar**, haga clic en  .

   Se muestra el cuadro de diálogo Crear un grupo de eventos.




3. Ingrese un nombre del grupo.
4. Escriba una descripción en Description.
5. Haga clic en + para agregar una condición. Continúe agregando condiciones según sea necesario. Para obtener detalles sobre la elaboración de condiciones, consulte Formulario Crear/Editar grupo.
6. Haga clic en **Guardar**.

   El nuevo grupo se muestra en el panel **Administrar**.

## Ejemplos

En esta sección se describe un ejemplo simple y, a continuación, se analiza cómo se configura un conjunto de reglas más complejo.

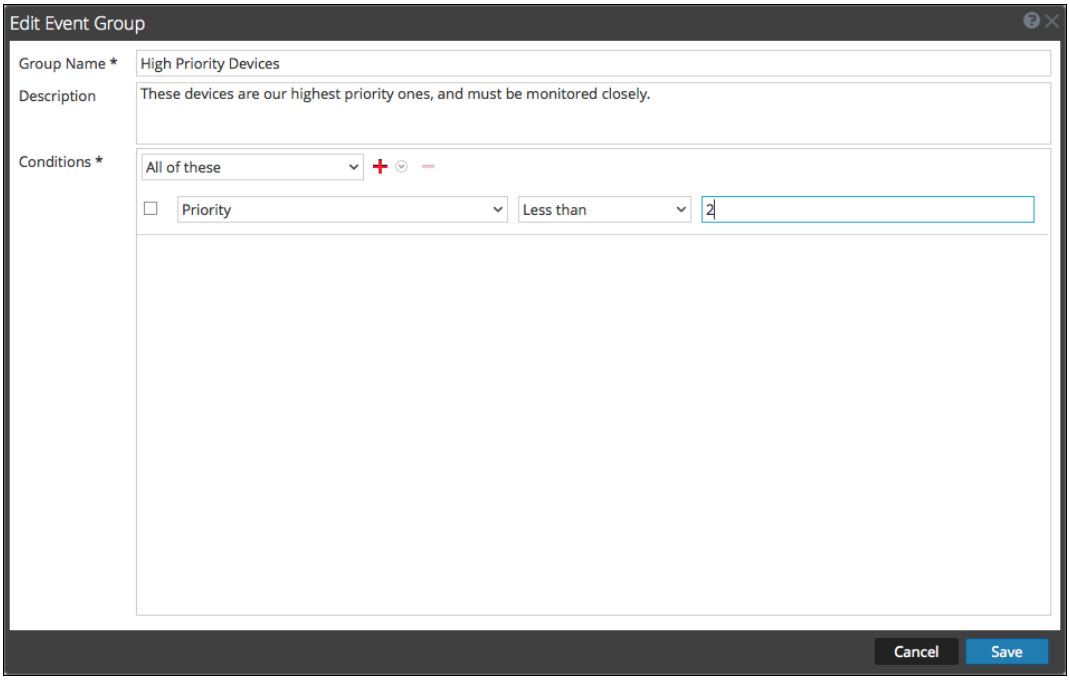
### Ejemplo simple

Si desea crear un grupo de orígenes de eventos que contiene todos los orígenes de eventos de prioridad alta, en este ejemplo se describen los pasos necesarios.

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. En el panel **Administrar > Grupos**, haga clic en +.
3. Ingrese **Dispositivos de prioridad alta** como el nombre del grupo.

4. Ingrese una descripción, como “A estos dispositivos se les dio la prioridad más alta y se deben monitorear cuidadosamente”.
5. Deje seleccionada la opción **Todas estas** y haga clic en + para agregar una condición.
6. Seleccione **Agregar condición** en el menú desplegable.
   a. Seleccione un atributo: **Prioridad**.
   b. Seleccione un operador: **Menor que**.
   c. Ingrese un valor: **2.**

   En la siguiente figura se muestra el cuadro de diálogo Editar grupo de eventos actualizado.




7. Haga clic en **Guardar**.

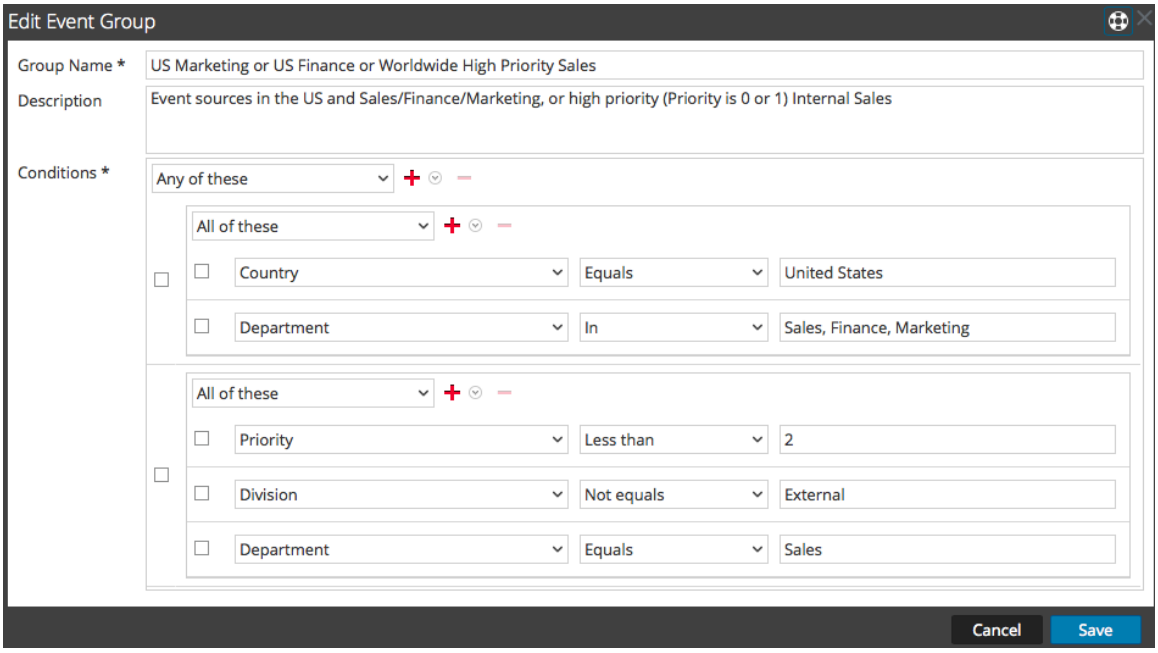
### Ejemplo complejo

En este ejemplo se desea crear una regla bastante compleja: hacer coincidir los orígenes de eventos que están en Estados Unidos y en los departamentos de ventas, financiamiento o marketing. Además, hacer coincidir orígenes de eventos de ventas internos y de prioridad alta en todo el mundo. Se asume que la Alta prioridad es donde la prioridad es 1 o 0. Lógicamente, la definición es la siguiente:

```
(Country=United States AND (Dept.=Sales OR
Dept.=Finance OR Dept.=Marketing))
 O
```

```
(Priority < 2 AND Division != External AND
Dept.=Sales)
```

En la siguiente figura se presenta un ejemplo de los criterios para crear un grupo de orígenes de eventos como este.



# Editar o eliminar grupos de orígenes de eventos

Es posible que ocasionalmente necesite eliminar un grupo de orígenes de eventos. Por ejemplo, si cierra una oficina y existía un grupo que tenía todos los orígenes de eventos de esa oficina, puede quitarlo, ya que ninguno de esos orígenes de eventos enviará información a Security Analytics.

De manera similar, puede ser necesario cambiar algunas de las condiciones que se usaron para completar el grupo.

**Nota:** No puede editar el nombre del grupo de orígenes de eventos. Una vez que crea un grupo, ese nombre existe siempre que exista el grupo.

## Editar un grupo de orígenes de eventos

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. En el panel **Administrar**, seleccione un grupo de orígenes de eventos existente.
3. Haga clic en  .

   Se muestra el cuadro de diálogo Editar grupo de eventos.
4. Modifique cualquiera de los detalles o agregue, edite o elimine condiciones según sea necesario.
5. Haga clic en **Guardar**.

## Eliminar un grupo de orígenes de eventos

Tenga en cuenta lo siguiente:

- Puede eliminar cualquier grupo, excepto el grupo **Todos**, el cual enumera todos los orígenes en el sistema.
- Si elimina un grupo, también se elimina automáticamente la política asociada a él.
- Si hay orígenes de eventos que pertenecen **solo** al grupo eliminado, ya no tendrán una alarma de política asociada a ellos. Recuerde que los orígenes de eventos pueden pertenecer a múltiples grupos.
- La eliminación de un grupo no tiene ningún efecto en las alarmas de base.

Para eliminar un grupo de orígenes de eventos:

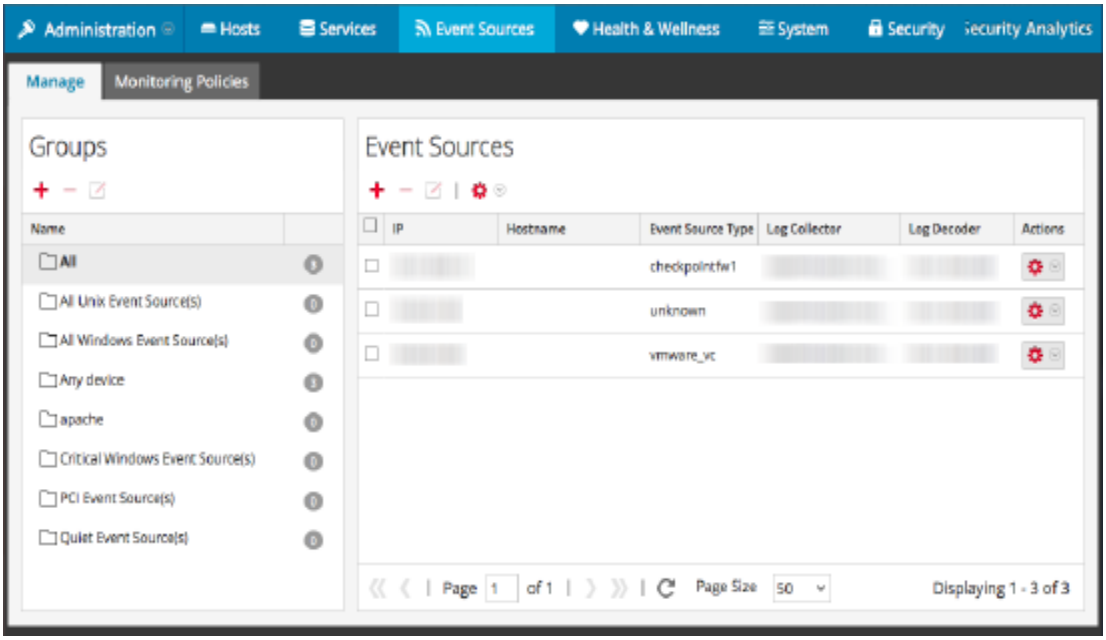
1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. En el panel **Administrar**, seleccione un grupo de orígenes de eventos existente.
3. Haga clic en .

   Se muestra un cuadro de diálogo de confirmación.
4. Haga clic en **Sí** para eliminar el grupo.

## Crear un origen de eventos y editar los atributos

Puede organizar los orígenes de eventos en grupos. Para esto, debe ingresar valores de diversos atributos para cada origen de eventos. Por ejemplo, para todos los orígenes de eventos de prioridad alta, podría configurar la **Prioridad** en 1. Puede ver detalles sobre los atributos disponibles en la Pestaña Administrar origen de eventos.

En la siguiente figura se muestra un ejemplo del panel Orígenes de evento:




Los atributos de orígenes de eventos son una combinación de información que se completa automáticamente y que ingresa el usuario. Cuando un origen de eventos envía información de registro a Security Analytics, se agrega a la lista de orígenes de eventos y cierta información básica se completa automáticamente. En cualquier momento después de eso, los usuarios pueden agregar o editar los detalles de otros atributos de orígenes de eventos.

### Atributos obligatorios

Los siguientes atributos de identificación se manejan de manera especial: **IP**, **IPv6**, **Nombre del host**, **Tipo de origen de evento**, **Log Collector** y **Log Decoder**. Si crea un origen de eventos manualmente, puede ingresar estos valores. Una vez que guarda el origen de eventos, estos valores no se pueden cambiar.

Los orígenes de eventos también se pueden descubrir automáticamente; cualquier origen de eventos que envíe mensajes a Log Decoder se agregará a la lista de orígenes de eventos. Si edita los atributos de un origen de eventos descubierto automáticamente, no puede editar ninguno de estos campos.

Tenga en cuenta que no todos estos campos son obligatorios. Para identificar de manera única un origen de eventos se requiere la siguiente información:

- IP o IPv6, Nombre de host y
- Tipo de origen de evento

Además, RSA Security Analytics usa una jerarquía para IP, IPv6 y nombre del host. El orden es el siguiente:

1. IP
2. IPv6
3. Hostname

Si ingresa orígenes de eventos manualmente, debe tener presente este orden o, de lo contrario, se pueden crear duplicados cuando se reciben mensajes de los orígenes de eventos que agregó de forma manual.

Los demás atributos (como Prioridad, País, Empresa, Proveedor, etc.) son opcionales.

## Crear un origen de eventos

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Administrar**.
3. En el panel **Orígenes de evento**, haga clic en  para abrir la pantalla de detalles que contiene todos los atributos de los orígenes de eventos.

   Se muestra la Pestaña Administrar origen de eventos .
4. Ingrese o cambie los valores de cualquier atributo.
5. Haga clic en **Guardar**.

## Actualizar atributos de un origen de eventos

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Administrar**.
3. En el panel **Orígenes de evento**, seleccione un origen de eventos de la lista.
4. En el panel **Orígenes de evento**, haga clic en  para abrir la pantalla de detalles que contiene todos los atributos de los orígenes de eventos.

   Se muestra la Pestaña Administrar origen de eventos .
5. Ingrese o cambie los valores de cualquier atributo, salvo de ciertos atributos que no se

pueden modificar una vez que se ingresan.

6. Haga clic en **Guardar**

## Atributos de edición masiva de origen de evento

Puede seleccionar varios orígenes de eventos, un grupo completo o incluso todos ellos para editarlos en masa. Por ejemplo, tal vez desee cambiar la prioridad o el administrador de una gran cantidad de orígenes de eventos.

**Nota:** no puede seleccionar orígenes de eventos individuales a través de las páginas mostradas. Por ejemplo, si tiene un grupo con 225 orígenes de eventos y el Tamaño de página es 50, solo puede seleccionar orígenes de eventos de los 50 elementos mostrados actualmente.

Si desea editar elementos que abarcan múltiples páginas, puede realizar lo siguiente:

- En el navegador, aumente el tamaño de página (el máximo es 500 entradas en una única página). Si el tamaño de página es pequeño, tal vez pueda ver todos los elementos en una única página.
- Cree un nuevo grupo de orígenes de eventos que contenga solo los elementos que desea editar en masa. A continuación, puede seleccionar todos los elementos de ese grupo en lugar de seleccionar elementos individuales.
- Edite en masa de manera incremental. En la primera página, seleccione los elementos que desea editar. Realice las ediciones y, a continuación, vaya a la página siguiente y repita el proceso hasta que haya hecho todos los cambios.

### Edición en masa de atributos

**Nota:** los campos obligatorios no se pueden editar; IP, IPv6, Nombre del host, Tipo de origen de evento, Log Collector y Log Decoder.

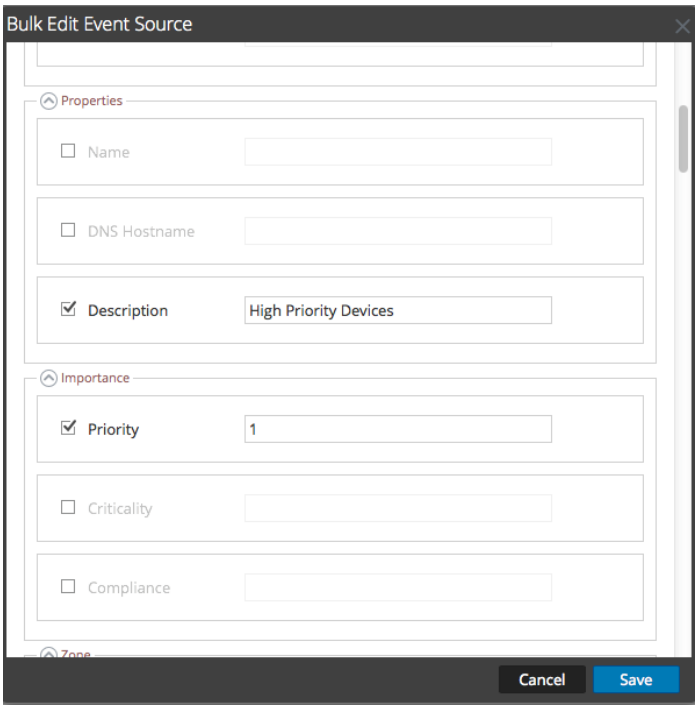
Para editar atributos de orígenes de eventos en masa:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Administrar**.
3. De manera opcional, seleccione un grupo de orígenes de eventos.
4. En el panel **Orígenes de evento**, seleccione uno o más orígenes de eventos para editar.

   **Nota:** para seleccionar todos los orígenes de eventos, seleccione la casilla junto a la columna **Acciones** en la última columna (extremo derecho) de la tabla de lista.

5. Seleccione el ícono **Editar** en la barra de menú.

   Se muestra el cuadro de diálogo Edición masiva de origen de evento.




6. Ingrese valores para cualquiera de los atributos disponibles. En la captura de pantalla anterior se actualizaron los atributos Nombre y Prioridad.
7. Cuando haya actualizado todos los atributos necesarios, haga clic en **Guardar**.

## Importar orígenes de eventos

Puede importar atributos de orígenes de eventos desde un archivo con formato CSV. Para importar información desde una base de datos de administración de configuración (CMDB), una hoja de cálculo u otro tipo de archivo, primero convierta o guarde la información en un archivo CSV.

**Nota:** Los siguientes atributos de identificación se manejan de manera especial: **IP**, **IPv6**, **Nombre del host**, **Tipo de origen de evento**, **Log Collector** y **Log Decoder**. Si importa un origen de evento que incluye un valor distinto para cualquiera de estos campos (en comparación con el valor de Security Analytics), el valor original de Security Analytics **no** se sobrescribirá.

Los atributos importados se asocian con el origen de eventos con el cual hubo coincidencia y están disponibles para su uso en reglas de creación de grupos de orígenes de eventos.

RSA Security Analytics considera el archivo de importación como el registro completo correcto. Esta suposición conlleva los siguientes comportamientos relacionados con la importación de atributos de orígenes de eventos:

- De manera predeterminada, cuando importa atributos, el sistema actualiza únicamente los atributos de los orígenes de eventos existentes.
- Si el origen de eventos existe en el archivo de importación, pero no en Security Analytics, los atributos de ese origen de evento se omiten. Es decir, Security Analytics **no** crea un nuevo origen de eventos para estos atributos.
- Si el origen de eventos existe en el archivo de importación y en Security Analytics, los valores de ese origen de eventos se sobrescriben.
- Si un atributo está en blanco en el archivo de importación, este borra el atributo correspondiente en Security Analytics.
- Si un atributo no se especifica en el archivo de importación, el atributo correspondiente se omite en Security Analytics (es decir, **no** se borra).

**Nota:** hay una diferencia entre un atributo en blanco y uno que no se especifica. Si un atributo se especifica, pero en blanco, la suposición es que está en blanco a propósito y Security Analytics lo borra para el origen de eventos correspondiente. Sin embargo, si un atributo no se especifica, se da por hecho que no se espera ningún cambio.

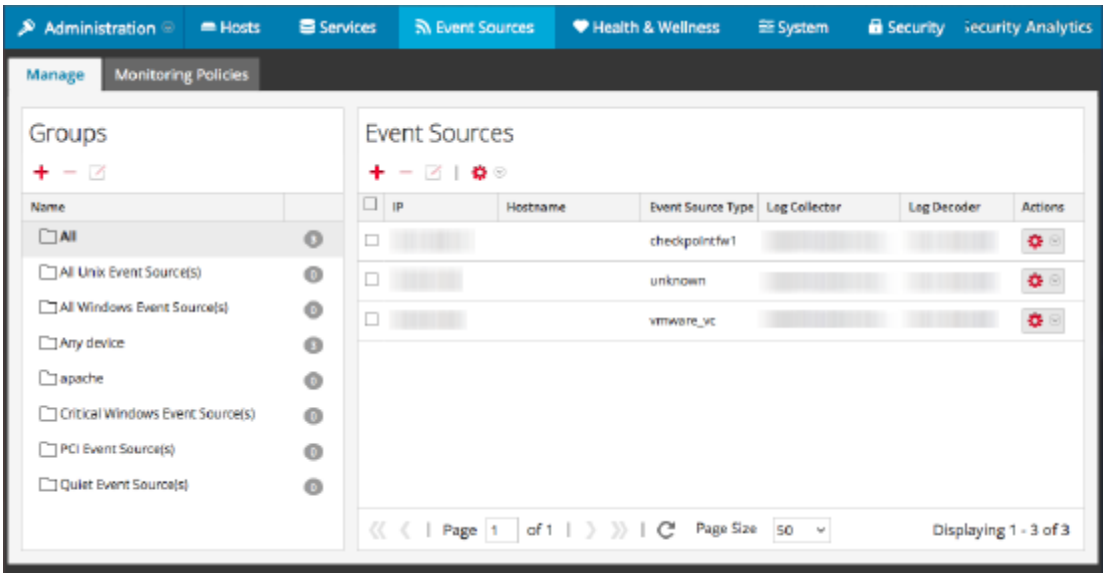
Los comportamientos anteriores son los predeterminados. Es posible cambiarlos como se especifica en el siguiente procedimiento.

## Importar atributos de orígenes de eventos

Para importar atributos de orígenes de eventos desde un archivo:

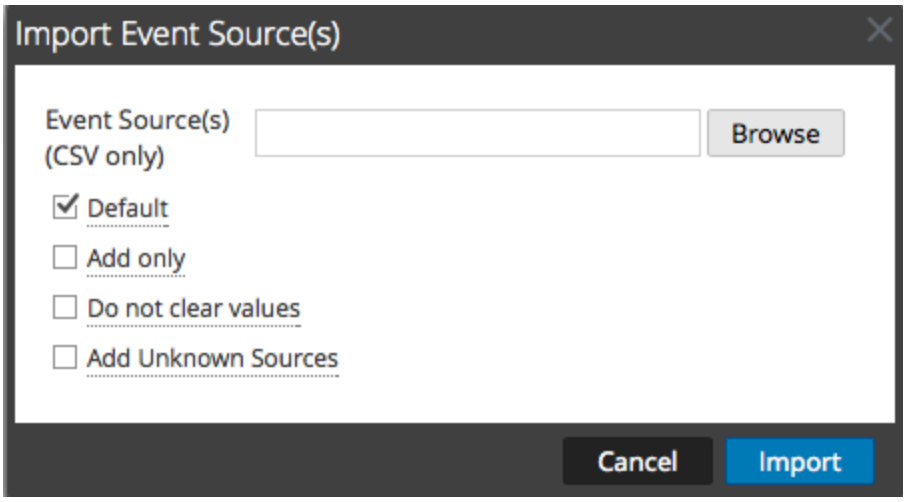
1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Administrar**.

   Se muestra la pestaña Administrar de orígenes de eventos.




3. En el menú Importar/Exportar de la barra de herramientas ( ), seleccione **Importar** ( Import ).

   Se muestra el cuadro de diálogo Importar orígenes de eventos.




4. Navegue al archivo de importación y seleccione las casillas correspondientes:

- **Valor predeterminado**: el comportamiento predeterminado, como se describió anteriormente.
- **Solo agregar**: Importa un atributo solo si el campo correspondiente en Security Analytics está en blanco. Por lo tanto, los valores existentes no se sobrescriben.
- **No borrar valores**: No borra valores de atributos en Security Analytics para los elementos del archivo de importación que están en blanco.
- **Agregar orígenes desconocidos**: agrega nuevos orígenes de eventos en función de los elementos del archivo de importación.

  **Nota:** puede seleccionar varias opciones.

5. Haga clic en **Importar**.
6. Haga clic en **Sí** en el cuadro de diálogo de confirmación para realizar la importación.

## Solución de problemas del archivo de importación

Si el archivo de importación no tiene el formato correcto o si le falta información requerida, se muestra un error y el archivo no se importa.

Revise lo siguiente:

- Si está agregando orígenes desconocidos, cada línea del archivo debe contener una combinación de los atributos requeridos:
  - IP o IPv6, Nombre de host y
  - Tipo de origen de evento
- La primera línea del archivo debe contener nombres de encabezado y estos deben coincidir con los nombres en Security Analytics. Para obtener una lista de nombres de columna correctos, puede exportar un único origen de eventos. Examine el archivo CSV exportado: la primera fila del archivo contiene el conjunto correcto de atributo/nombres de columna.

# Exportar orígenes de eventos

Puede exportar todos o algunos de los orígenes de eventos, junto con sus atributos correspondientes, a un archivo CSV.

Tenga en cuenta lo siguiente:

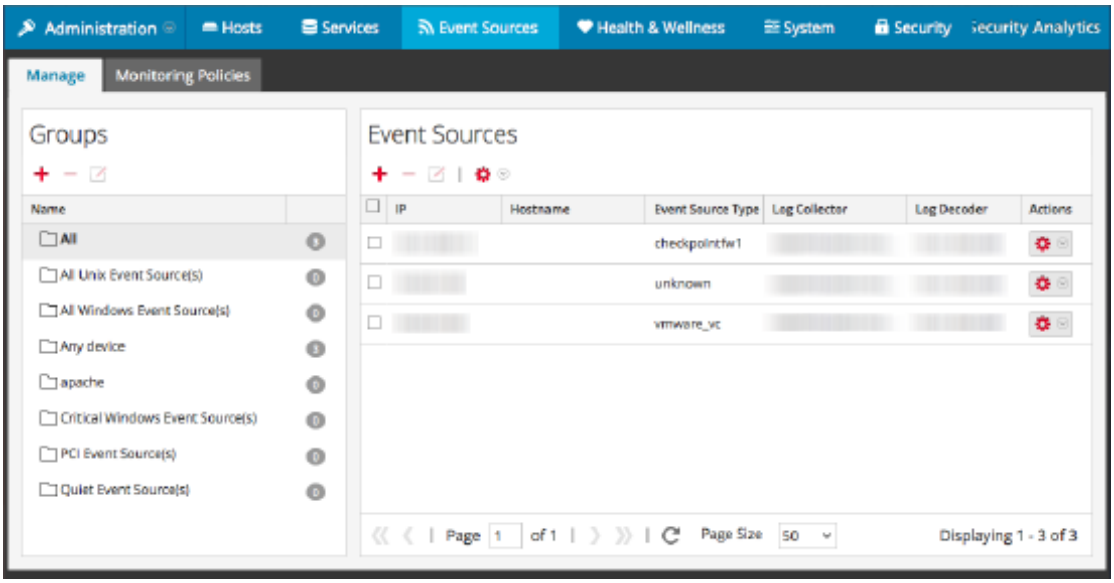
- El archivo CSV exportado incluye todas las columnas de atributos.
- El archivo CSV exportado incluye una línea de encabezado en la parte superior, la cual enumera cada nombre de columna.
- Puede exportar todas las entradas de un grupo.
- Puede exportar todas las entradas (seleccione el grupo **Todos**).
- Puede seleccionar algunas entradas y exportar solo estas.

## Exportar orígenes de eventos

Para exportar los orígenes de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Administrar**.

   Se muestra la pestaña Administrar de orígenes de eventos.

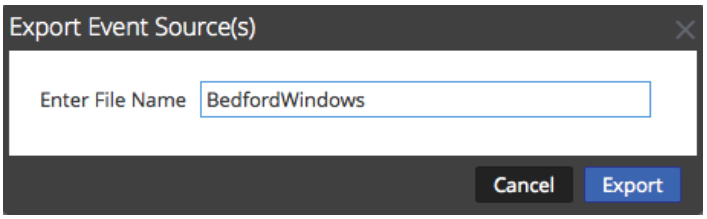



3. Seleccione el grupo que contiene los orígenes de eventos que desea exportar.

4. Seleccione todos los orígenes de eventos que necesite. Como alternativa, puede exportar el grupo completo: para exportar el grupo completo, no necesita seleccionar orígenes de eventos individuales.

5. En el menú Importar/Exportar de la barra de herramientas ( ), seleccione **Exportar (.csv)** o **Exportar grupo (.csv)**.

   Se muestra el cuadro de diálogo Exportar orígenes de eventos.




6. Ingrese un nombre de archivo y haga clic en Exportar.

Los atributos de los orígenes de eventos se guardan en formato CSV con el nombre de archivo que especificó.

## Ordenar orígenes de eventos

En el panel de orígenes de eventos se muestran atributos para el grupo de orígenes de eventos actualmente seleccionado. Puede configurar la lista de atributos que se muestran, así como ordenarla por cualquiera de los atributos mostrados.

### Comportamiento

Tenga en cuenta los siguientes comportamientos cuando ordene los orígenes de eventos:

- Se ordena la lista completa, no solo los elementos que se muestran en la página actual. (La barra de navegación de la parte inferior de la página muestra cuántas páginas existen para esta lista de orígenes de eventos).
- En el orden de clasificación se distingue mayúsculas de minúsculas. En cualquier columna de cadena, si los valores contienen una combinación de minúscula y mayúscula, la mayúscula aparece en la lista antes que la minúscula.

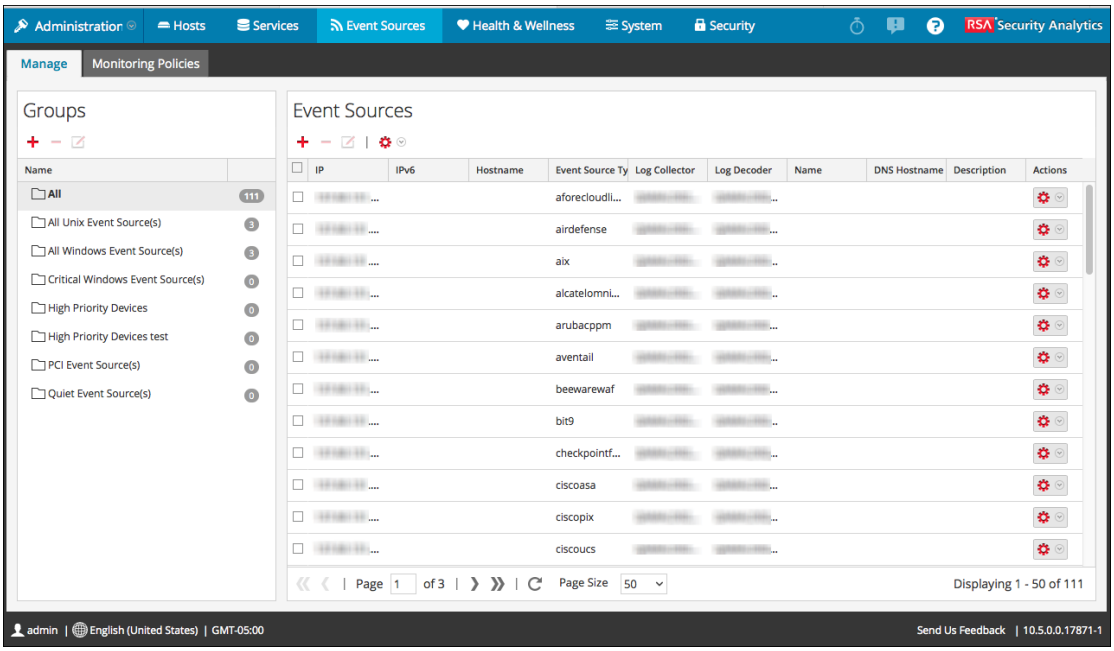
  Por ejemplo, suponga que la columna Tipo de origen de evento contiene las siguientes entradas: Netflow, APACHE, netwitnesspectrum y ciscoasa. El orden de clasificación sería el siguiente:

  - APACHE
  - Flujo de red
  - ciscoasa
  - netwitnesspectrum

Para ordenar los orígenes de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Administrar**.

   Se muestra la pestaña Administrar de orígenes de eventos.




3. Para ordenar una columna, haga clic en  en su encabezado.

   Se muestra el menú desplegable Opciones de clasificación.

4. Seleccione el orden de clasificación que desee.

# Políticas de monitoreo

Use la vista Políticas de monitoreo para administrar la configuración de alertas para los grupos de orígenes de eventos.

Puede crear políticas que alertan sobre grupos de orígenes de eventos mediante la configuración de umbrales y notificaciones:

- Los umbrales definen los rangos para la frecuencia de los mensajes de registro. Puede especificar un umbral inferior, un umbral superior o ambos.
- Las notificaciones describen cómo y dónde se envían las alertas cuando no se alcanzan los umbrales.
- Los umbrales y las notificaciones se combinan para crear alertas de acuerdo con la frecuencia que especifica.
- Si está habilitada la función de alertas automáticas (lo está de forma predeterminada), puede crear y habilitar una política ***sin*** configurar umbrales. Si, a continuación, activa las notificaciones automáticas, estas se enviarán cada vez que un origen de eventos en el grupo esté por encima o por debajo de su base en la cantidad especificada.

Por ejemplo, suponga que creó un grupo de orígenes de eventos que consta de todos los orígenes de eventos de Windows que se encuentran en el Reino Unido. Podría especificar una política que emita alertas cada vez que lleguen menos de 1,000 eventos cada 30 minutos.

**Nota:** Además de configurar políticas de monitoreo para los grupos de orígenes de eventos o en lugar de configurarlas, puede Configurar alertas automáticas para ver las alarmas cuando la cantidad de mensajes para un origen de eventos está fuera de los límites normales.

## Configurar alertas de grupo de orígenes de eventos

Cada grupo de orígenes de eventos puede tener su propia política de alerta. Esto incluye configurar los umbrales que determinan cuándo se activa la alerta y el tipo de notificación de la activación de una alerta. En este tema se describen los pasos relacionados con la creación de una política de alerta para un grupo de orígenes de eventos.

### Procedimientos

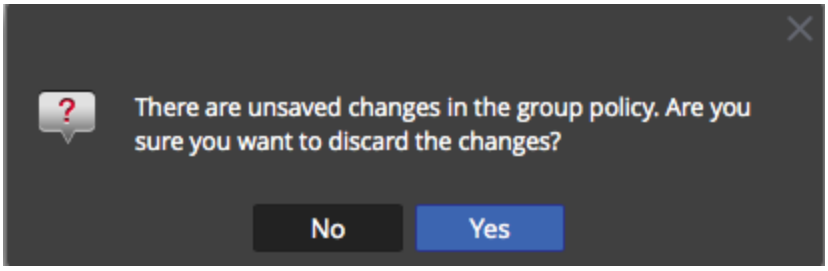
#### Crear una política de alerta para un grupo de orígenes de eventos

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Políticas de monitoreo**.
3. En el panel **Grupos de eventos**, seleccione un grupo.
4. Ingrese valores en los campos Umbral inferior y Umbral superior.

   Este es un ejemplo de umbrales de alerta.


5. Seleccione **Activar** y haga clic en **Guardar** para habilitar la política de alerta que configuró.

**Nota:** Si hace cambios en una política e intenta salir de la página antes de guardarlos, se muestra el mensaje de advertencia Cambios no guardados:



### Configurar y ver los umbrales de una política de alerta

Cada grupo de orígenes de eventos también es una política de alerta. Los umbrales son parte de una política de alerta. Puede configurar umbrales para cada política de alerta. Para cada política, puede configurar un umbral inferior, un umbral superior o ambos. Además, puede habilitar una política sin configurar umbrales; esto le permite recibir notificaciones basadas en alertas automáticas. Cuando la base de un origen de evento está fuera de los límites normales, se generan alertas automáticas.

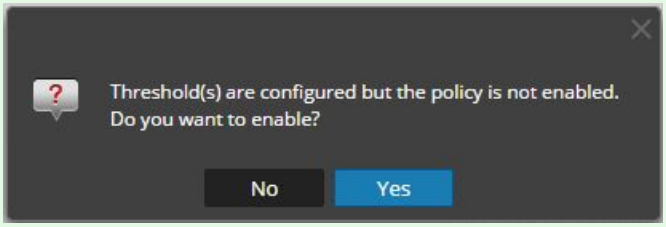
1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Políticas de monitoreo**.
3. En el panel **Grupos de eventos**, seleccione un grupo.
   Los umbrales configurados para el grupo seleccionado se muestran en el panel **Umbrales**.


4. Edite los valores de Umbral inferior o Umbral superior de la siguiente manera:
   a. Ingrese la cantidad de eventos para el umbral.
   b. Ingrese la cantidad de minutos u horas para el umbral. El valor mínimo es 5 minutos

**Nota:** para cada umbral, puede configurar valores inferiores, superiores o ambos.

5. Seleccione **Habilitar** para habilitar alarmas cuando no se alcancen los umbrales.

**Nota:** Si configura un umbral e intenta guardar la página sin habilitarlo, recibirá un mensaje de confirmación, donde se le preguntará si desea habilitar la política:



Por ejemplo, suponga que ingresa 10 y 30 para los valores del umbral inferior: **10** events in **30** minutes y 20 y 30 para los valores del umbral superior: **20** events in **30** minutes. Esto significa que espera que se registren entre 10 y 20 eventos en 30 minutos (para el grupo de orígenes de eventos seleccionado). Es decir, cualquier valor entre los umbrales inferior y superior se considera normal y no activa una alerta.

**Nota:** una vez que agrega un umbral para una política, no puede eliminarlo. Puede inhabilitar la política o configurar el umbral inferior o superior en 0 eventos en 5 minutos. Cinco minutos es la duración mínima para un umbral.

# Configurar notificaciones

En este tema se describe cómo configurar notificaciones para grupos de orígenes de eventos. Las notificaciones se envían cuando no se alcanzan los umbrales.

Las notificaciones van a la par con los umbrales. Antes de configurar notificaciones, debe configurar los umbrales para un grupo de orígenes de eventos.

**Nota:** Después de configurar los umbrales para un grupo de orígenes de eventos, si no configura notificaciones, incluso si se activa una alerta, los usuarios no reciben notificaciones. Sin embargo, todas las alarmas son visibles en la Pestaña Alarmas.

## Requisitos previos

Antes de configurar notificaciones para un grupo de orígenes de eventos, debe revisar los elementos de notificación disponibles:

- **Servidores de notificación:** son los servidores desde los cuales desea recibir notificaciones del sistema. Para obtener más detalles, consulte el tema **Configurar servidores de notificación** de la *Guía de configuración del sistema*.
- **Plantillas de notificación:** son las plantillas disponibles para cada tipo de notificación. Para Administración de orígenes de eventos, se proporcionan plantillas predeterminadas para correo electrónico (SMTP), SNMP y syslog. Puede usar estas plantillas como se proporcionan o personalizarlas si es necesario. Para obtener más detalles, consulte el tema **Descripción general de plantillas** de la *Guía de configuración del sistema*.
- **Salida de notificación:** las salidas contienen los parámetros para el tipo de notificación. Por ejemplo, un tipo de notificación por correo electrónico contiene las direcciones de correo electrónico y el asunto de la notificación. Para obtener más detalles, consulte el tema **Descripción general de las salidas de las notificaciones** de la *Guía de configuración del sistema*.

## Agregar notificaciones para un grupo de orígenes de eventos

Para agregar notificaciones para un grupo de orígenes de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Políticas de monitoreo**.
3. En el panel **Grupos de eventos**, seleccione un grupo.

**Nota:** ya debe haber configurado un umbral para el grupo. Si no es así, consulte Configurar y ver los umbrales de una política de alerta para configurar un umbral y, a continuación, regrese a este procedimiento. Como alternativa, si tiene activada la función de alertas automáticas, no necesita configurar umbrales para una política. Las alarmas automáticas generan notificaciones sin la necesidad de establecer umbrales.

4. En el panel Notificaciones, haga clic en + y, en el menú desplegable, seleccione el tipo de notificación que desea agregar:
   - Correo electrónico
   - SNMP
   - Syslog

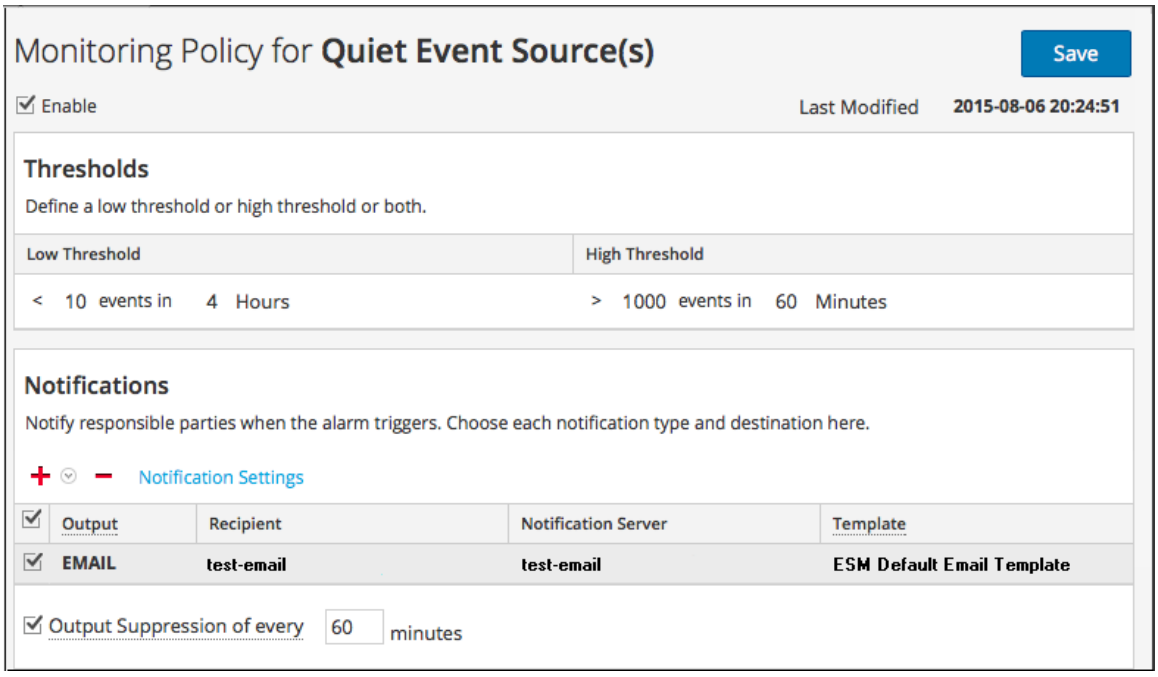
**Nota:** Se proporcionan plantillas predeterminadas de ESM (monitoreo de orígenes de eventos) para cada tipo de notificación.

5. Ingrese valores en los campos Notificación, Servidor de notificación y Plantilla.
   a. En Notificación, seleccione un valor de la lista o agregue un tipo de notificación apropiado en **Notificaciones** y selecciónelo aquí.
   b. En Servidor, seleccione un valor de la lista o agregue un servidor apropiado en **Notificaciones** y selecciónelo aquí.
   c. En Plantilla, seleccione una plantilla disponible o cree una plantilla apropiada en **Notificaciones** y selecciónela aquí.

**Nota:** Si necesita agregar o editar uno de estos elementos, haga clic en **Configuración de notificaciones**. Se abre una nueva ventana del navegador en la página **Administration > Sistema > Notificaciones globales**. Úsela para ver o actualizar los elementos de notificación disponibles.

6. De manera opcional, puede limitar el índice de notificaciones para una política.
   a. Seleccione **Supresión de salida** para habilitar la configuración de un límite.
   b. Ingrese un valor, en minutos, para el índice de supresión. Por ejemplo, si ingresa **30**, las notificaciones para esta política se limitan a una cada 30 minutos.
   c. Haga clic en **Guardar**.

El siguiente es un ejemplo de una política de monitoreo que contiene un umbral y una notificación para un grupo de orígenes de eventos.


Monitoring Policy for Quiet Event Source(s)
Save
Enable
Last Modified 2015-08-06 20:24:51
Thresholds
Define a low threshold or high threshold or both.
Low Threshold
High Threshold
< 10 events in 4 Hours
> 1000 events in 60 Minutes
Notifications
Notify responsible parties when the alarm triggers. Choose each notification type and destination here.
Notification Settings
Output
Recipient
Notification Server
Template
EMAIL
test-email
test-email
ESM Default Email Template
Output Suppression of every 60 minutes

## Inhabilitar notificaciones

Cuando no se alcanzan los umbrales se envían notificaciones. Además, se envían notificaciones automáticas cuando no se cumplen las bases. Sin embargo, puede determinar que ya no requiere notificaciones para los orígenes de eventos de un grupo específico. En este caso, puede inhabilitar las notificaciones para el grupo de orígenes de eventos.

**Nota:** Incluso si deshabilita todas las notificaciones, los detalles de las alarmas continúan visibles en la Pestaña Alarmas.

### Requisitos previos

Debe haber configurado umbrales y notificaciones para un grupo de orígenes de eventos y haberlos habilitado En el caso de las notificaciones automáticas, debe haber seleccionado **Habilitar notificaciones desde el monitoreo automático** en la Pestaña Ajustes de configuración.

### Inhabilitar notificaciones

Para deshabilitar las notificaciones (manuales y automáticas) para un grupo de orígenes de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Políticas de monitoreo**.
3. En el panel **Grupos de eventos**, seleccione un grupo.
4. Haga clic en **Habilitar** para eliminar la marca de verificación. La deselección de esta opción significa que no se envían notificaciones para este grupo de orígenes de eventos, incluso si los umbrales no se alcanzan o se superan.
5. Además, puede eliminar todas las notificaciones. Sin embargo, esto no se requiere para detenerlas.

# Ver alarmas de origen de evento

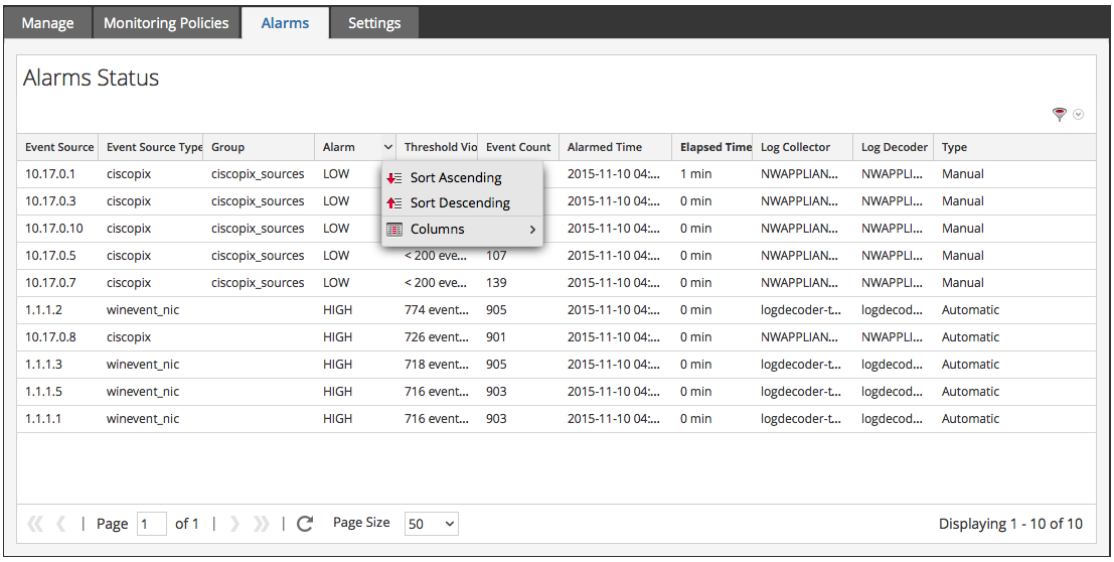
En este tema se describe cómo ver las alarmas de los grupos de orígenes de eventos. Una vez que ha configurado y establecido alertas, puede ver todas las alarmas generadas en la pestaña **Alarmas** de la vista **Orígenes de evento**.

## Ordenar la información de alarmas

Cuando se accede por primera vez a esta vista, los datos se ordenan según la alarma más reciente (la columna Hora de activación de la alarma). Puede ordenar por cualquier columna.

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Active con el mouse la columna que desea ordenar.
3. Haga clic en la pestaña **Alarmas** para seleccionarla.
4. Active con el mouse la columna que desea ordenar y haga clic en el ícono .

   Este es un ejemplo de la activación con el mouse de la columna Alarma.



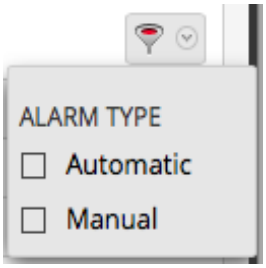

5. Seleccione **Orden ascendente** u **Orden descendente** para ordenar la columna según su preferencia.

   Los datos se ordenan en todas las páginas.

**Nota:** También puede ordenar por dos columnas. Para hacerlo, ordene primero por la columna secundaria y después por la columna principal. Por ejemplo, si desea ver todas las alarmas ALTAS por su orden de grupo, en primer lugar ordene por **Grupo** y, a continuación, por **Alarma**.

## Filtrar alarmas por tipo

También puede filtrar las alarmas por su tipo: puede mostrar solo las alarmas manuales o automáticas (base). Para filtrar por tipo de alarma, seleccione el ícono de filtro en el lado derecho de la pantalla, en el área de encabezado:




Seleccione el modo Automático o Manual:

- Si selecciona Automático, solo se muestran las alertas que se basan en las bases.
- Si selecciona Manual, solo se muestran las alarmas para las cuales configuró umbrales.

# Configurar alertas automáticas

**Nota:** Actualmente, las alertas automáticas y su configuración están en versión beta.

## Requisitos previos

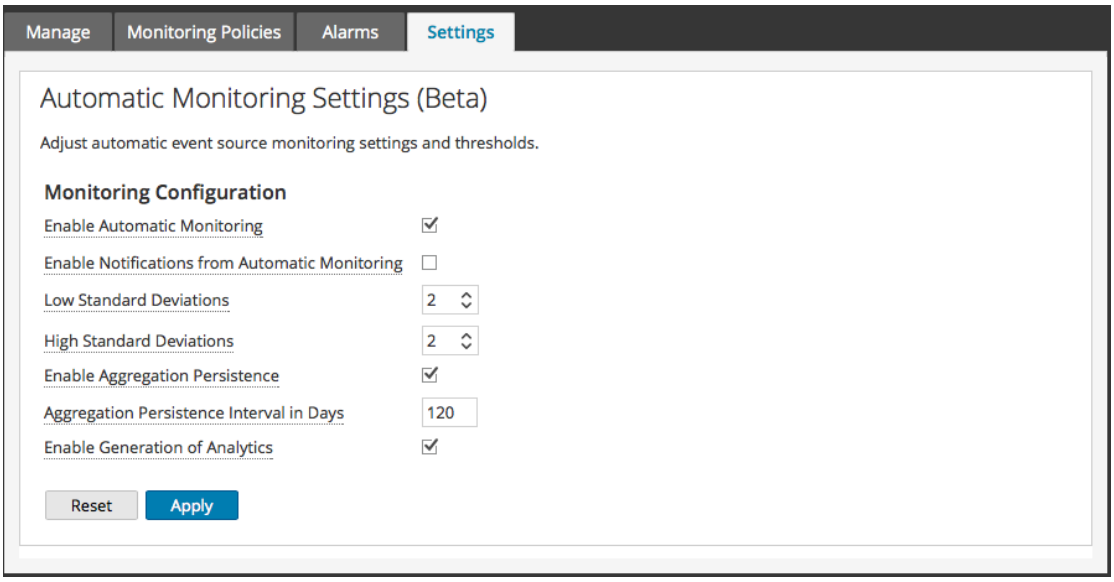
Antes de configurar notificaciones para un grupo de orígenes de eventos, debe revisar los elementos de notificación disponibles:

- **Servidores de notificación:** son los servidores desde los cuales desea recibir notificaciones del sistema. Para obtener más detalles, consulte el tema **Configurar servidores de notificación** de la *Guía de configuración del sistema*.
- **Plantillas de notificación:** son las plantillas disponibles para cada tipo de notificación. Para Administración de orígenes de eventos, se proporcionan plantillas predeterminadas para correo electrónico (SMTP), SNMP y syslog. Puede usar estas plantillas como se proporcionan o personalizarlas si es necesario. Para obtener más detalles, consulte el tema **Descripción general de plantillas** de la *Guía de configuración del sistema*.
- **Salida de notificación:** las salidas contienen los parámetros para el tipo de notificación. Por ejemplo, un tipo de notificación por correo electrónico contiene las direcciones de correo electrónico y el asunto de la notificación. Para obtener más detalles, consulte el tema **Descripción general de las salidas de las notificaciones** de la *Guía de configuración del sistema*.

## Configurar alertas automáticas

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Configuración**.

   Se muestra la pestaña Configuración.




3. De forma predeterminada, el monitoreo automático está activado. Para apagar las alertas automáticas, desactive la opción **Habilitar el monitoreo automático**.
4. De forma predeterminada, las notificaciones de alertas automáticas está desactivada. Para activar las notificaciones automáticas, seleccione la opción **Habilitar notificaciones desde el monitoreo automático**.
5. Configure los parámetros en función de los patrones de uso:
   - **Desviaciones estándares bajas**: Desviaciones estándares por debajo de las cuales se reciben alertas. El valor predeterminado es **2.0** (confianza del 95 %).
   - **Desviaciones estándares altas**: Desviaciones estándares por sobre las cuales se reciben alertas. El valor predeterminado es **2.0** (confianza del 95 %).

   **Nota:** Puede ajustar la configuración de la desviación estándar en incrementos de 0.1 (una décima parte) de una desviación estándar.
6. Haga clic en **Guardar** para cerrar el cuadro de diálogo y guardar la configuración.

# Referencia de Administración de orígenes de eventos

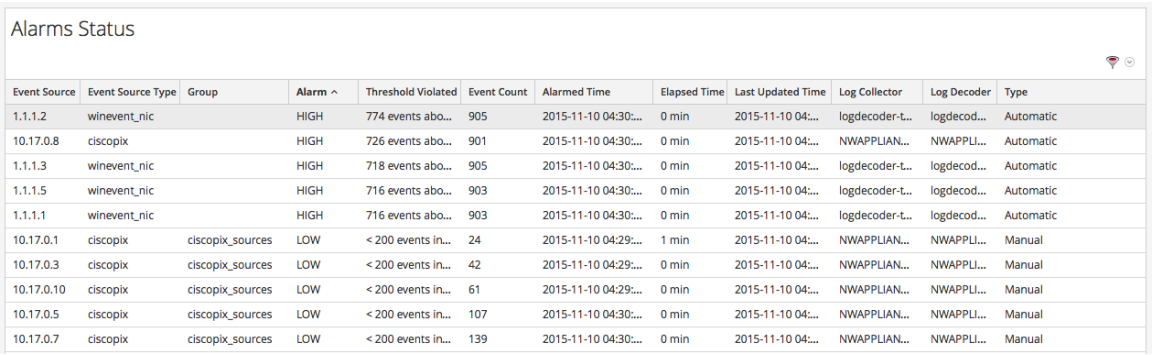
Temas de referencia de ESM:

- Ver orígenes de eventos
- Pestaña Administrar
- Pestaña Políticas de monitoreo
- Pestaña Alarmas
- Pestaña Ajustes de configuración
- Formulario Crear/Editar grupo
- Pestaña Administrar origen de eventos

## Pestaña Alarmas

La pestaña Alarmas presenta los detalles de los orígenes de eventos que actualmente infringen una política y un umbral. En la lista solo aparecen los orígenes de eventos que infringen una política. Una vez que el origen de evento vuelve a un estado normal, la alarma correspondiente desaparece de la lista.

Para acceder a esta pestaña, en el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento > Alarmas**.


Alarms Status

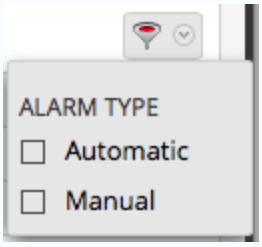
| Event Source | Event Source Type | Group | Alarm | Threshold Violated | Event Count | Alarmed Time | Elapsed Time | Last Updated Time | Log Collector | Log Decoder | Type |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1.1.1.2 | winevent_nic | | HIGH | 774 events abo... | 905 | 2015-11-10 04:30:... | 0 min | 2015-11-10 04:... | logdecoder-t... | logdecod... | Automatic |
| 10.17.0.8 | ciscopix | | HIGH | 726 events abo... | 901 | 2015-11-10 04:30:... | 0 min | 2015-11-10 04:... | NWAPPLIAN... | NWAPPLI... | Automatic |
| 1.1.1.3 | winevent_nic | | HIGH | 718 events abo... | 905 | 2015-11-10 04:30:... | 0 min | 2015-11-10 04:... | logdecoder-t... | logdecod... | Automatic |
| 1.1.1.5 | winevent_nic | | HIGH | 716 events abo... | 903 | 2015-11-10 04:30:... | 0 min | 2015-11-10 04:... | logdecoder-t... | logdecod... | Automatic |
| 1.1.1.1 | winevent_nic | | HIGH | 716 events abo... | 903 | 2015-11-10 04:30:... | 0 min | 2015-11-10 04:... | logdecoder-t... | logdecod... | Automatic |
| 10.17.0.1 | ciscopix | ciscopix_sources | LOW | < 200 events in... | 24 | 2015-11-10 04:29:... | 1 min | 2015-11-10 04:... | NWAPPLIAN... | NWAPPLI... | Manual |
| 10.17.0.3 | ciscopix | ciscopix_sources | LOW | < 200 events in... | 42 | 2015-11-10 04:29:... | 0 min | 2015-11-10 04:... | NWAPPLIAN... | NWAPPLI... | Manual |
| 10.17.0.10 | ciscopix | ciscopix_sources | LOW | < 200 events in... | 61 | 2015-11-10 04:29:... | 0 min | 2015-11-10 04:... | NWAPPLIAN... | NWAPPLI... | Manual |
| 10.17.0.5 | ciscopix | ciscopix_sources | LOW | < 200 events in... | 107 | 2015-11-10 04:30:... | 0 min | 2015-11-10 04:... | NWAPPLIAN... | NWAPPLI... | Manual |
| 10.17.0.7 | ciscopix | ciscopix_sources | LOW | < 200 events in... | 139 | 2015-11-10 04:30:... | 0 min | 2015-11-10 04:... | NWAPPLIAN... | NWAPPLI... | Manual |

Para conocer los procedimientos relacionados con esta pestaña, consulte Ver alarmas de origen de evento.

### Características

La pestaña Alarmas contiene las siguientes funciones.

| Característica | Descripción |
|---|---|
| **Origen de eventos** | La dirección IP, IPv6 o el nombre de host del origen de eventos en el cual se emitió la alarma |
| **Tipo de origen de evento** | El tipo de origen de evento con alarma. Por ejemplo, **winevent_nic** (para Microsoft Windows) o **rhlinux** (para Linux). |
| **Grupo** | Este es el grupo de orígenes de eventos que contiene el origen de evento para el cual se activó la alarma. |
| **Alarma** | El tipo de umbral que se activó: **Alta** o **Baja** |
| **Infracción de umbral** | Las condiciones del umbral que se activó. Por ejemplo:<br>`5,000,000 eventos en 5 minutos` |

| Característica | Descripción |
|---|---|
| **Conteo de eventos** | La cantidad de eventos en el periodo del umbral que causan la alarma. |
| **Hora de activación de la alarma** | La hora inicial en que el origen de eventos entró en un estado de alarma<br>**Nota:** Cuando se accede por primera vez a esta vista, los datos se ordenan según esta columna (en primer lugar la alarma más reciente). |
| **Tiempo transcurrido** | Tiempo transcurrido desde que el origen de eventos ingresó en un estado de alarma. |
| **Hora de última actualización** | La última vez que se confirmó que el origen de eventos estuvo en un estado de alarma.<br>**Nota:** Esta columna aparece oculta de manera predeterminada. |
| **Log Collector** | El Log Collector que recopiló por última vez desde este origen de eventos. |
| **Log Decoder** | El Log Decoder que recibió por última vez desde este origen de eventos. |
| **Tipo** | El tipo de alarma es **Manual** o **Automática**:<br>• **Manual**: Son alarmas que infringen la política de umbral configurada.<br>• **Automática**: Son alarmas que se desvían de la base para el origen de evento en el cual se emitió la alarma. |
| **Filtro** | Seleccione el ícono de filtro para mostrar el menú Filtro:<br>  <br>Seleccione el modo Automático o Manual:<br>• Si selecciona Automático, solo se muestran las alertas que se ajustan a bases.<br>• Si selecciona Manual, solo se muestran las alarmas para las cuales configuró umbrales. |

**Nota:** Puede ocultar o mostrar columnas, para lo cual debe hacer clic con el botón secundario en el encabezado de la tabla y elegir **Columnas** en el menú desplegable. Seleccione una columna para mostrarla o bórrela para ocultarla.

## Ver orígenes de eventos

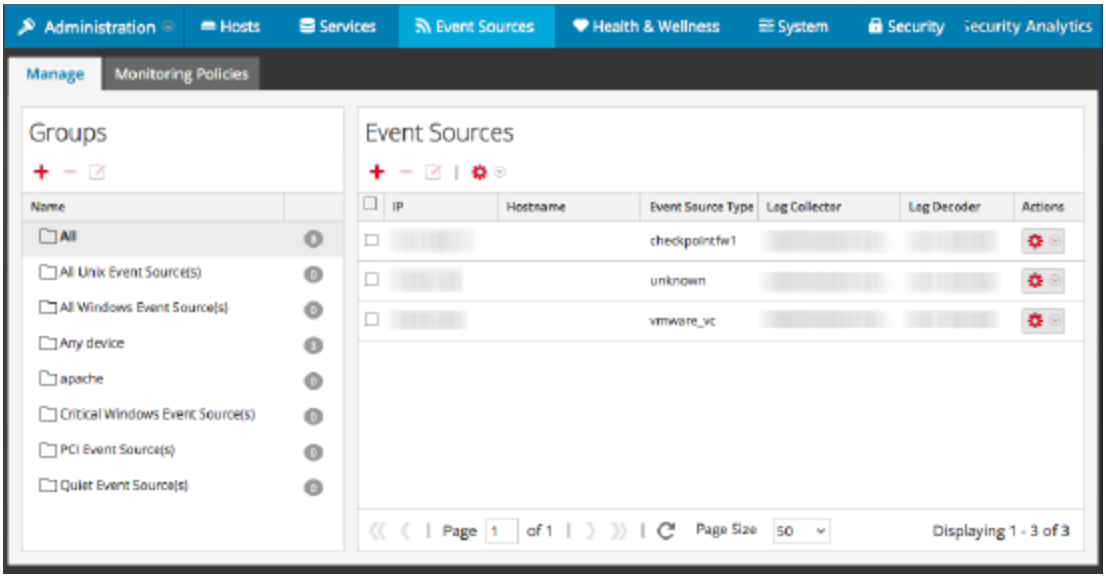
El panel Atributos de orígenes de eventos tiene las siguientes pestañas.

| Característica | Descripción |
|---|---|
| Pestaña Administrar | Use esta pestaña para crear, editar y eliminar grupos de orígenes de eventos. Presenta a una vista personalizable con capacidad de búsqueda de todos los orígenes de eventos y los grupos. |
| Pestaña Políticas de monitoreo | Use esta pestaña para administrar la configuración de alertas para orígenes de eventos. |
| Pestaña Alarmas | Use esta pestaña para ver los detalles de las alarmas que se han generado. |
| Pestaña Ajustes de configuración | Use esta pestaña para ver o cambiar el comportamiento de las alertas automáticas (base). |

# Pestaña Administrar

La pestaña Administrar organiza orígenes de eventos en grupos y muestra atributos para cada origen de eventos.

Para acceder a esta pestaña, en el menú de **Security Analytics**, seleccione **Administration** > **Orígenes de evento**. La pestaña **Administrar** se muestra de manera predeterminada.



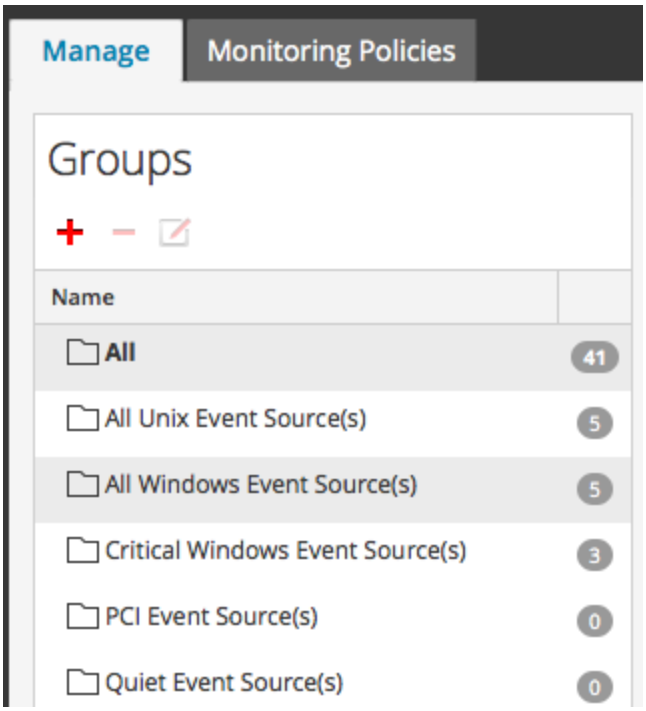

Los procedimientos relacionados con esta pestaña se describen en Administrar grupos de orígenes de eventos.

## Características

La pestaña Administrar consta de dos paneles, Grupos y Orígenes de evento.

### Panel Grupos

El panel Grupos enumera los grupos de orígenes de eventos, así como un conteo de los miembros de cada grupo. Para ver todos los orígenes de eventos, seleccione **Todos** en la lista de grupos. Este es un ejemplo del panel Grupos.

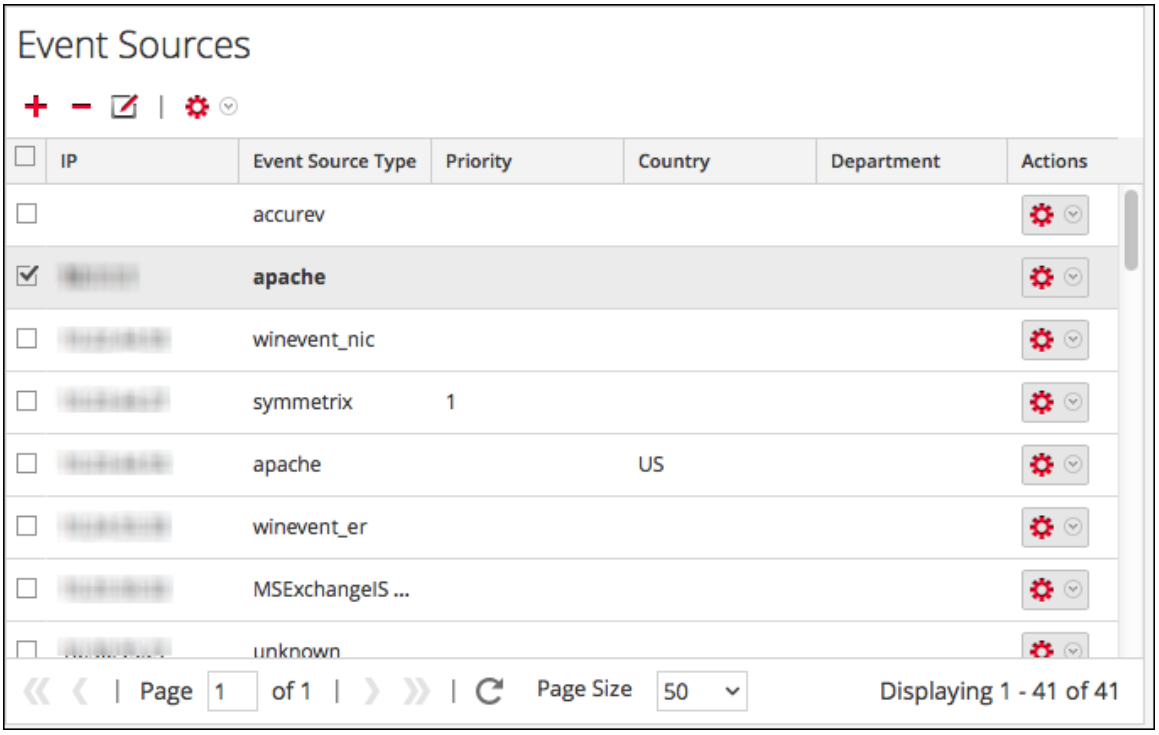



El panel Grupos contiene las siguientes funciones.

| Característica | Descripción |
|---|---|
| **Herramientas** | Estos son los íconos estándar de Security Analytics para agregar, quitar o editar grupos. |
| **Count** | El conteo para un grupo de orígenes de eventos indica la cantidad de orígenes de eventos en ese grupo. Es decir, la cantidad de orígenes de eventos que coinciden con los criterios que se usan para definir el grupo.<br>**Nota:** El conteo no se actualiza dinámicamente cuando se agregan nuevos orígenes de eventos. Por lo tanto, puede ser necesario realizar una actualización para ver un conteo de grupos actualizado. |
| **Nombre** | La columna Nombre enumera el identificador para cada grupo. Puede usar nombres de grupo para identificar rápidamente algunos de los criterios que se usan para formar el grupo.<br>Por ejemplo, si crea un grupo que consta de orígenes de eventos de Windows para la organización Ventas, puede llamar **Orígenes de ventas de Windows** al grupo.<br>**Nota:** No se puede editar el nombre del grupo de orígenes de eventos. Una vez que crea un grupo, ese nombre existe siempre que exista el grupo. |

### Panel Orígenes de evento

El panel Orígenes de evento muestra los atributos de los orígenes de eventos del grupo seleccionado. O bien, si se selecciona Todos en el panel Grupos, este panel enumera todos los orígenes de eventos.



| Característica | Descripción |
|---|---|
| **Herramientas** | La barra de herramientas incluye las siguientes herramientas:<br>• **Agregar**: agregue manualmente un origen de eventos<br>• **Eliminar**: elimine un origen de eventos<br>• **Editar**: actualice los atributos de un origen de eventos existente<br>• Menú **Importar/Exportar**  : muestra un menú con las siguientes opciones:<br>  • **Importar**: Importe orígenes de eventos desde una base de datos de administración de contenido (CMDB), una hoja de cálculo u otra herramienta.<br>  • **Exportar**: exporte los orígenes de eventos seleccionados y sus atributos en formato CSV.<br>  • **Exportar grupo**: exporte el grupo completo seleccionado actualmente. |
| **Atributos** | Presentación de los atributos en columnas. Puede elegir los atributos que se mostrarán. |
| **Acciones** | Menú de acceso directo para comandos de uso frecuente: Editar, Eliminar y Exportar. |
| **Casillas de verificación** | Seleccione las filas que se usarán cuando se realicen tareas en varios orígenes de eventos, como la edición en masa. |

| Característica | Descripción |
| --- | --- |
| **Herramientas de navegación** | En la parte inferior de la pantalla, hay elementos que ayudan a navegar en el grupo:<br>• **Página *x* de *y***: indica la página que se está mostrando actualmente y cuántas páginas existen en total para este grupo.<br>• <<, <, > y >>: haga clic en estos íconos para ir de una página a otra, ya sea una por vez (< y >), a la primera (<<) o a la última (>>).<br>• **Tamaño de página**: use este selector para elegir el tamaño de la página.<br>• **Mostrando *x* - *y* de *z***: comprobación rápida de los orígenes de eventos que se muestran actualmente de la cantidad total para el grupo. |

### Orden

En el panel Orígenes de evento, la lista de elementos se presenta de manera ordenada. Puede elegir la columna según la cual se aplicará el orden. Sin embargo, tenga en cuenta que el orden de clasificación depende de las mayúsculas y minúsculas.

Para cualquier columna de cadena, si los valores contienen una combinación de minúscula y mayúscula, la mayúscula aparece en la lista antes que los valores en minúscula.

Por ejemplo, suponga que la columna Tipo de origen de evento contiene las siguientes entradas: Netflow, APACHE, netwitnesspectrum y ciscoasa. El orden de clasificación sería el siguiente:

- APACHE
- Flujo de red
- ciscoasa
- netwitnessspectrum

## Pestaña Políticas de monitoreo

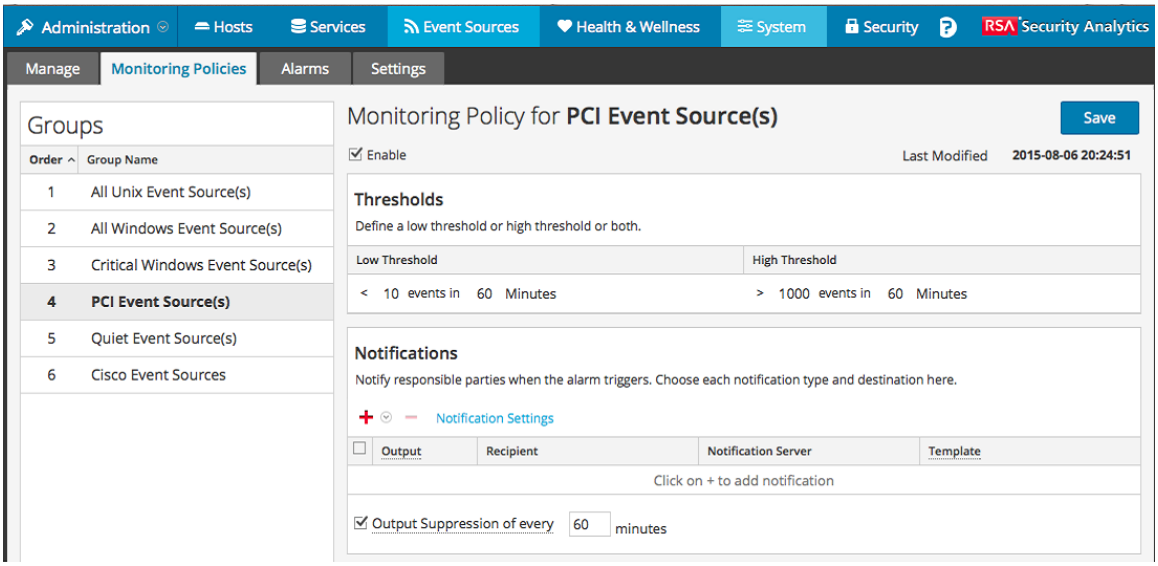
La pestaña Políticas de monitoreo organiza umbrales por grupo de orígenes de eventos.

Para acceder a esta pestaña:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.

   Se muestra la pestaña **Administrar**.

2. Seleccione la pestaña **Políticas de monitoreo**.

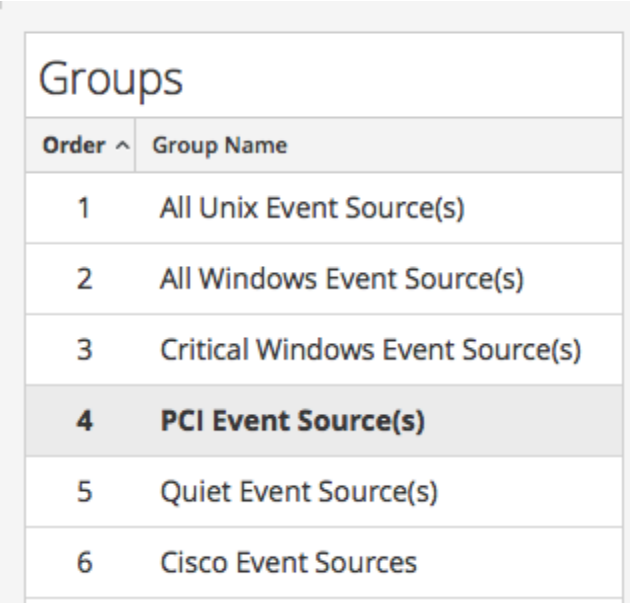



Los procedimientos relacionados con esta pestaña se describen en Políticas de monitoreo.

### Características

La pestaña **Políticas de monitoreo** consta de tres paneles.

### Panel Grupos de eventos




El grupo que se selecciona en este panel determina los umbrales que aparecen en el panel Umbrales. Puede definir un conjunto de umbrales para cada grupo de orígenes de eventos. Tenga en cuenta que los grupos se enumeran en un orden específico:

- Arrastre y suelte grupos para cambiar el orden especificado.
- Cuanto más alto se enumere un grupo, mayor será la prioridad de los umbrales de ese grupo: RSA Security Analytics comprueba los umbrales en el orden que se proporciona en este panel. De este modo, los grupos con prioridad más alta deben estar en la parte superior de esta lista

### Panel Umbrales

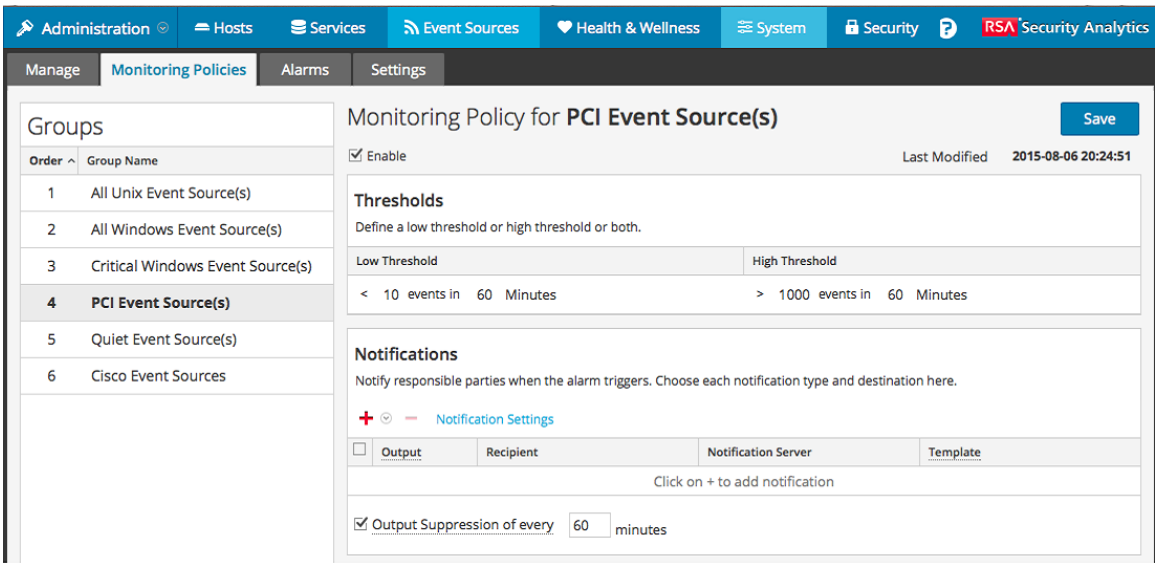
Este es un ejemplo del panel Umbrales para un grupo de orígenes de eventos.


El panel Umbrales incluye las siguientes funciones.

| Característica | Descripción |
|---|---|
| **Habilitar** | La casilla de verificación Activar determina si los umbrales que define para un grupo están o no habilitados. Si lo están, se envían notificaciones cada vez que los umbrales para ese grupo están fuera del rango definido. Si no, ese grupo de orígenes de eventos no se monitorea.<br>**Nota:** Si configura un umbral e intenta guardar la página sin habilitarlo, recibirá un mensaje de confirmación, donde se le preguntará si desea habilitar la política.<br>Si habilita una política, pero no ha configurado umbrales, puede seguir recibiendo notificaciones automáticas (base), siempre y cuando las haya activado.<br>Consulte a continuación para obtener más detalles sobre la apariencia de las notificaciones. |
| **Baja cantidad de eventos**<br>**Baja cantidad de minutos u horas** | Este es el límite inferior del umbral. Ingrese la menor cantidad de eventos y el rango de tiempo. Si el grupo de orígenes de eventos recibe menos mensajes de los que se especifican aquí, el umbral no se alcanza y se envían notificaciones. |
| **Alta cantidad de eventos**<br>**Alta cantidad de minutos u horas** | Funciona de manera similar a los valores menores: si se reciben más mensajes de los que se especifican aquí, el umbral no se alcanza y se envían notificaciones. |
| **Fecha y hora de la última modificación** | Este campo indica la última fecha y hora en que se cambiaron los umbrales. |
| **Guardar** | Guarda los cambios que se hicieron en los umbrales. |

### Panel Notificaciones

Este es un ejemplo del panel Notificaciones para un grupo de orígenes de eventos.



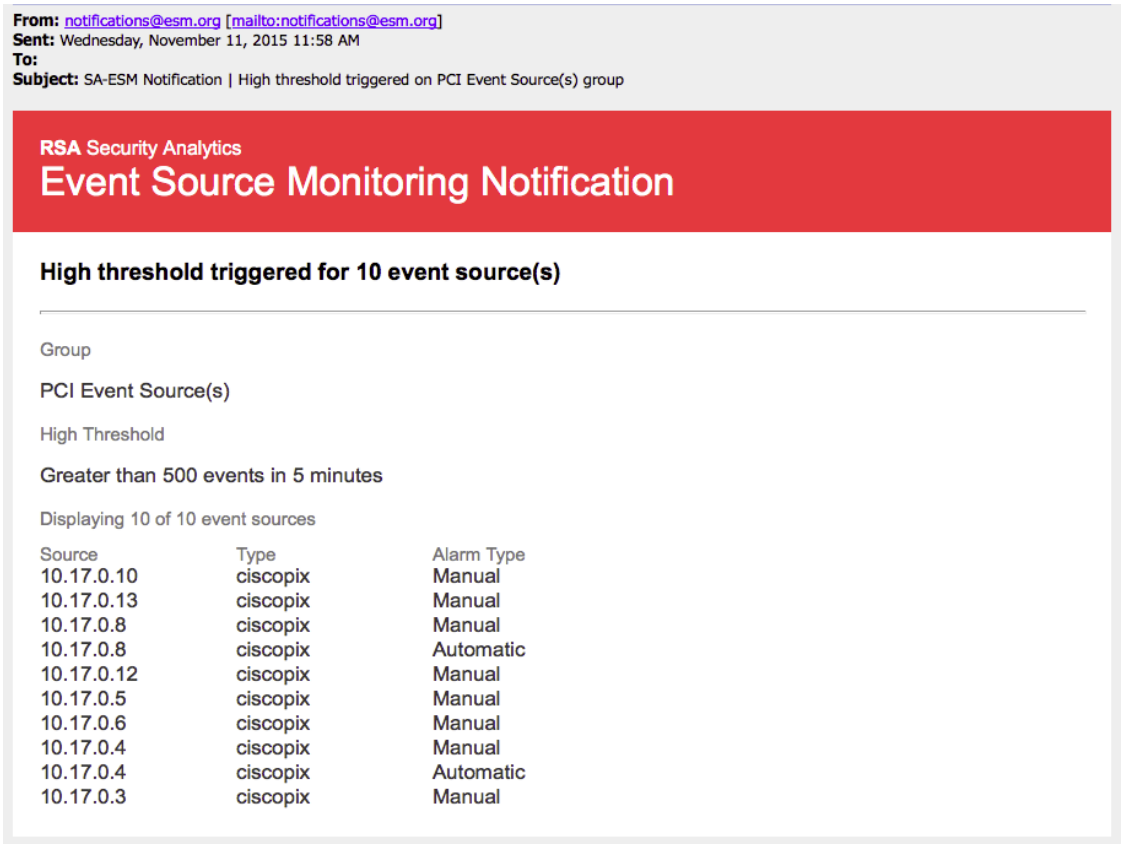

En la siguiente tabla se describen los campos del panel Notificaciones

| Campo | Descripción |
|---|---|
| **Herramientas**<br>+ - | En la barra de herramientas están disponibles los siguientes elementos:<br>• **Agregar (+)**: si se hace clic en **Agregar**, se presenta un menú que permite elegir el tipo de notificación.<br>• **Eliminar (-)**: elimina la fila seleccionada de la lista. |
| Configuración de notificaciones | Si se hace clic en este vínculo, se abre una nueva pestaña del navegador y se lo dirige a la página **Administrador** > **Sistema** > **Notificaciones** en Security Analytics. |
| **Tipo** | Muestra el tipo de notificación que eligió. Las opciones disponibles son las siguientes:<br>• Correo electrónico<br>• SNMP<br>• Syslog |
| **Notificación** | Consulte el tema **Configurar las salidas de las notificaciones** de la *Guía de configuración del sistema* para obtener más detalles. |
| **Servidor de notificación** | Consulte el tema **Configurar servidores de notificación** de la *Guía de configuración del sistema* para obtener más detalles. |

| Campo | Descripción |
| --- | --- |
| **Plantilla** | Para Administración de orígenes de eventos, RSA proporciona tres plantillas de uso inmediato para las notificaciones. Puede usar las siguientes plantillas como se entregan o puede personalizarlas en función de las necesidades de la organización:<br>• **Plantilla de correo electrónico**: envía notificaciones a las direcciones de correo electrónico especificadas.<br>• **Plantilla SNMP**: envía notificaciones al servidor SNMP especificado.<br>• **Plantilla de syslog**: envía notificaciones al servidor de syslog especificado.<br>Consulte el tema **Configurar plantillas para notificaciones** de la *Guía de configuración del sistema* para obtener más detalles. |
| **Supresión de salida** | Use este elemento para limitar la frecuencia con que se reciben notificaciones para esta política, en caso de que se activen muchas alertas en un periodo breve. |

Los siguientes son ejemplos de notificaciones que se basan en las plantillas proporcionadas.

- Correo electrónico:



**From:** notifications@esm.org [mailto:notifications@esm.org]
**Sent:** Wednesday, November 11, 2015 11:58 AM
**To:**
**Subject:** SA-ESM Notification | High threshold triggered on PCI Event Source(s) group

RSA Security Analytics

## Event Source Monitoring Notification

**High threshold triggered for 10 event source(s)**

Group

PCI Event Source(s)

High Threshold

Greater than 500 events in 5 minutes

Displaying 10 of 10 event sources

| Source | Type | Alarm Type |
|---|---|---|
| 10.17.0.10 | ciscopix | Manual |
| 10.17.0.13 | ciscopix | Manual |
| 10.17.0.8 | ciscopix | Manual |
| 10.17.0.8 | ciscopix | Automatic |
| 10.17.0.12 | ciscopix | Manual |
| 10.17.0.5 | ciscopix | Manual |
| 10.17.0.6 | ciscopix | Manual |
| 10.17.0.4 | ciscopix | Manual |
| 10.17.0.4 | ciscopix | Automatic |
| 10.17.0.3 | ciscopix | Manual |

**Nota:** En el caso de las notificaciones por correo electrónico, la tercera columna, **Tipo de alarma**, especifica si la alarma activada se basó en un umbral de usuario o si los datos de base están fuera de los límites normales. Si desactivó el monitoreo automático o las notificaciones, no recibirá notificaciones **automáticas**. Lo mismo es válido para Syslog y SNMP, excepto porque las notificaciones tienen un formato diferente.

- SNMP trap:

```
11-11-2015 11:57:33 Local7.Debug 127.0.0.1 community=public,
enterprise=1.3.6.1.4.1.36807.1.20.1, uptime=104313, agent_
ip=10.251.37.92, version=Ver2,
1.3.6.1.4.1.36807.1.20.1="Security Analytics Event Source
Monitoring Notification:
Group: PCI Event Source(s)
High Threshold:
Greater than 500 events in 5 minutes
10.17.0.10,ciscopix,Manual
10.17.0.13,ciscopix,Manual
```

```
10.17.0.8,ciscopix,Manual
10.17.0.8,ciscopix,Automatic
10.17.0.12,ciscopix,Manual
10.17.0.5,ciscopix,Manual
10.17.0.6,ciscopix,Manual
10.17.0.4,ciscopix,Manual
10.17.0.4,ciscopix,Automatic
10.17.0.3,ciscopix,Manual"
```

- Ejemplo de syslog:

```
11-11-2015 11:57:33 User.Info 127.0.0.1 Nov 11 11:57:33
localhost CEF:0|RSA|Security Analytics Event Source
Monitoring|10.6.0.0.0|
HighThresholdAlert|ThresholdExceeded|1|cat=PCI Event Source(s)
|Devices|
src=10.17.0.10,ciscopix,Manual|src=10.17.0.13,ciscopix,Manual|sr
c=10.17.0.8,ciscopix,Manual|src=10.17.0.8,ciscopix,Automatic|src
=10.17.0.12,ciscopix,Manual|src=10.17.0.5,ciscopix,Manual|src=10
.17.0.6,ciscopix,Manual|src=10.17.0.4,ciscopix,Manual|src=10.17.
0.4,ciscopix,Automatic|src=10.17.0.3,ciscopix,Manual|
```

## Formulario Crear/Editar grupo

El formulario Crear grupo de orígenes de eventos se muestra cuando se crea o se edita un grupo de orígenes de eventos.

Los procedimientos relacionados con este formulario se describen en Crear grupos de orígenes de eventos y Editar o eliminar grupos de orígenes de eventos.

### Parámetros

En la siguiente tabla se describen los campos del formulario Crear/Editar un grupo de eventos.

| Campo | Descripción |
|---|---|
| **Group Name** | Este campo es obligatorio y aparece en toda la interfaz del usuario de Security Analytics como el identificador del grupo. |
| **Descripción** | Descripción opcional que ayuda a describir el propósito o los detalles del grupo. |
| **Herramientas**  | En la barra de herramientas están disponibles los siguientes elementos:<br>• **Agregar (+)**: si se hace clic en **Agregar**, se muestra un menú que permite optar por agregar una condición o un grupo.<br>• **Eliminar (−)**: elimina la regla o el grupo de reglas seleccionados de la lista.<br>Cuando se agrega un nuevo grupo, esto tiene el efecto de crear niveles de condiciones anidados. |
| **Condiciones** | Se describen a continuación, en la tabla **Criterios de las reglas**. |
| **Cancelar/Guardar** | Las opciones **Cancelar** y **Guardar** están disponibles en el formulario. |

### Criterios de las reglas

Las reglas que especifica determinan los orígenes de eventos que formarán parte de este grupo de orígenes de eventos. Una regla consta de lo siguiente:

- Agrupación: cómo interactúa la regla con otras reglas
- Atributo: con qué atributo se hace coincidir la regla
- Operador: cómo coincide la regla con el atributo
- Valor: el valor del atributo que se usa para la regla

En la siguiente tabla se proporcionan detalles acerca de estos constructores de reglas.

| Constructor de reglas | Detalles |
|---|---|
| **Agrupamiento** | Puede agrupar condiciones para crear reglas complejas para un grupo de orígenes de eventos. Cuando se agrupan las reglas, están disponibles las siguientes opciones:<br>• **Todas estas**: lógicamente equivalente a AND<br>• **Cualquiera de estas**: lógicamente equivalente a OR<br>• **Ninguna de estas**: lógicamente equivalente a NOT<br><br>Si está creando un grupo simple y especificando una única condición, puede dejar seleccionado el valor predeterminado (**Todas estas**). |
| **Atributo** | Contiene una lista desplegable que consta de todos los atributos de orígenes de eventos. Los atributos se muestran por la sección a la cual pertenecen. Por ejemplo, todos los atributos de **Identificación** se muestran primero, seguidos de las **Propiedades**, la **Importancia**, etc. |

| Constructor de reglas | Detalles |
|---|---|
| **Operador** | Elija entre las siguientes opciones:<br>• **Es igual a**: coincide con el valor especificado<br>• **No es igual a**: devuelve orígenes de eventos cuyo atributo especificado no es igual al valor proporcionado<br>• **En**: proporcione una lista de valores en formato separado por comas y se incluirán orígenes de eventos que coinciden con cualquiera de los valores especificados. Por ejemplo:<br>`Where IP in 10.25.50.146, 10.25.50.248`<br>Esta condición devuelve orígenes de eventos que tienen el atributo de IP `10.25.50.146 o 10.25.50.248`.<br>• **No en**: similar a **En**, salvo que coincide con elementos cuyo atributo no es igual a ninguno de los valores enumerados.<br>• **Como**: coincide con elementos que comienzan con la cadena especificada. Por ejemplo:<br>`Where Event Source Type Like Apache`<br>Esta condición devuelve orígenes de eventos cuyo tipo de origen de eventos comienza con `Apache`.<br>• **No como**: similar a **Como**, salvo que coincide con elementos cuyo atributo no comienza con la cadena especificada.<br>• **Mayor que**: coincide con elementos cuyo atributo es mayor que el valor especificado. Por ejemplo, si especifica Prioridad Mayor que 5, la condición coincidiría con cualquier elemento que tuviera una prioridad de 6 o más.<br>• **Menor que**: similar a **Mayor que**. Coincide con elementos cuyo atributo es menor que el valor especificado. |
| **Valor** | Ingrese un valor o un grupo de valores. El tipo de valor depende del atributo para la condición. Por ejemplo, para IPv6 debe especificar un valor en formato IPv6. |

# Pestaña Ajustes de configuración

En este tema se describen las funciones de la pestaña Ajustes de configuración. En la pestaña Ajustes de configuración se presentan opciones para el monitoreo automático (alertas de base).

**Nota:** Actualmente, las alertas automáticas y su configuración están en versión beta.

## Acerca de las alertas automáticas

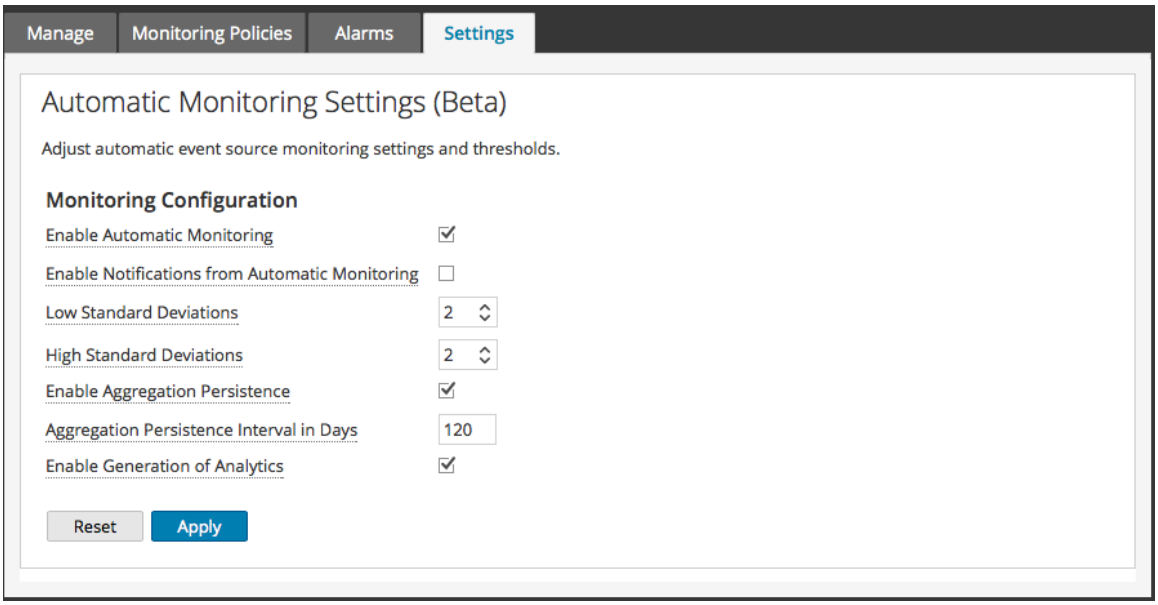
Puede configurar políticas y umbrales para los grupos de orígenes de eventos. Configúrelos de modo que reciba notificaciones cuando no se cumplan los umbrales. Security Analytics también proporciona un modo automático para recibir alarmas en caso de que no desee configurar umbrales para generar alarmas.

Puede usar valores de base para activar alertas automáticas. De esta forma,no es necesario configurar diversas políticas y umbrales de grupo a fin de recibir alertas. Cualquier cantidad anormal de mensajes activará las alertas, sin necesidad de realizar configuración alguna (excepto para la activación de las alertas automáticas).

Tenga en cuenta lo siguiente:

- Una vez que comienza a recopilar los mensajes de un origen de evento, el sistema tarda aproximadamente una semana en almacenar un valor de base para ese origen de evento. Finalizado este período inicial, el sistema le avisa cuando la cantidad de mensajes durante un período se encuentra por encima o por debajo de la base en una cantidad específica. De forma predeterminada, esta cantidad es 2 desviaciones estándares por encima o por debajo de la base.
- Base la configuración de desviación alta y baja en la “regularidad” del comportamiento de sus orígenes de eventos. Es decir, si espera poca o ninguna variación en la cantidad de mensajes que llegan durante una hora determinada (por ejemplo, 8:00 a 9:00 h en un día de semana), puede establecer un valor bajo para la desviación. Por el contrario, si ve a menudo ve horas punta y valle, configure la desviación en un valor superior.
- Si habilita una política, pero no ha configurado umbrales, puede seguir recibiendo notificaciones automáticas (base), siempre y cuando haya activado las alertas automáticas.

Para acceder a esta pestaña, en el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento > Ajustes de configuración**.




Para conocer los procedimientos relacionados con esta pestaña, consulte Configurar alertas automáticas.

## Características

La pestaña Ajustes de configuración contiene las siguientes funciones.

| Característica | Descripción |
|---|---|
| **Habilitar el monitoreo automático** | Determina si la alerta automática está activada o desactivada. De forma predeterminada, esta opción está seleccionada (la alerta automática está activada) |
| **Habilitar notificaciones desde el monitoreo automático** | Determina si las notificaciones de alertas automáticas están activadas o desactivadas. De forma predeterminada, esta opción está desactivada (no se envían notificaciones automáticas cuando las alertas automáticas están activadas) |
| **Desviaciones estándares bajas** | Las desviaciones estándares por debajo de las cuales se reciben alertas. El valor predeterminado es **2.0** (confianza del 95 %) |
| **Desviaciones estándares altas** | Las desviaciones estándares por sobre las cuales se reciben alertas. El valor predeterminado es **2.0** (confianza del 95 %) |

| Característica | Descripción |
|---|---|
| **Habilitar la persistencia de la agregación** | Cuando se selecciona esta opción, almacena los conteos de orígenes de eventos por intervalo de una hora. Los datos que se recopilan se usan para formar la base de cada origen de eventos.<br>• Habilitado (valor predeterminado): en la base de datos subyacente se almacena un conteo por hora por cada origen de evento. Estos conteos (o agregaciones) de una hora forman la base histórica para el procesamiento del rango normal de cada origen de evento.<br>• Desactivado: cuando se reinicie el servidor de SMS, el monitoreo de orígenes de eventos no tendrá ningún dato histórico con el cual procesar el rango normal y el usuario tendrá que esperar hasta que se recopilen datos suficientes (aproximadamente durante una semana) para formar una nueva base para cada origen de eventos |
| **Intervalo de persistencia de agregación en días** | Controla cuántos datos históricos (consulte **Habilitar la persistencia de la agregación**) se deben mantener para cada origen de eventos. El valor predeterminado de 120 días significa que se mantiene un historial de aproximadamente 4 meses, el cual se usa para reconstruir la base de cada origen de eventos |
| **Habilitar la generación de analítica** | Cuando se habilita, los datos sobre el comportamiento de las alertas automáticas se almacenan en el disco. El valor predeterminado es **Habilitado**.<br>Los datos que se conservan, incluyen el valor de base en el tiempo y el historial de alertas para cada origen de evento. Tenga en cuenta, sin embargo, que la dirección y el tipo del origen de evento son anónimos, por lo tanto, solo se muestra la información de la tasa de eventos.<br>Dado que la alerta automática es una función en versión beta, estos datos son importantes para medir la eficacia de la función, la cual se puede deshabilitar sin afectar su funcionalidad |
| **Restablecer** | Esta opción descarta los cambios no guardados para todas las configuraciones en la página |
| Aplicar | Haga clic en **Aplicar** para guardar los cambios en los valores de esta pestaña. |

## Pestaña Administrar origen de eventos

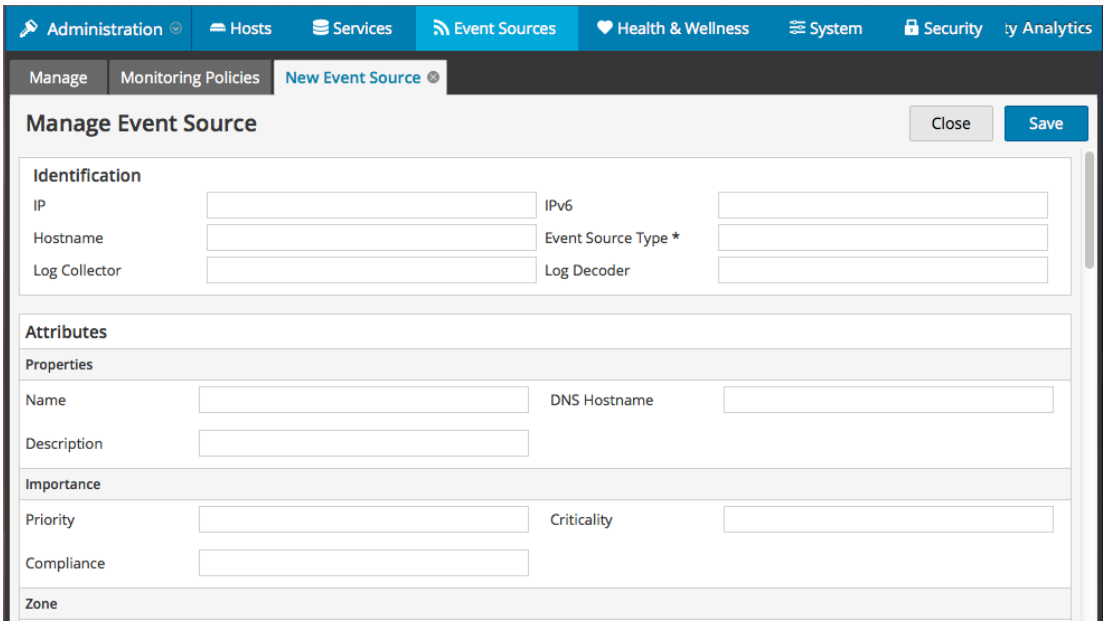
La pantalla Administrar origen de eventos se utiliza para realizar las siguientes tareas:

- Mostrar detalles de orígenes de eventos
- Agregar valores de atributo a un origen de eventos
- Eliminar valores de atributo de un origen de eventos

Para ver la pantalla Administrar origen de eventos para un origen de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Orígenes de evento**.
2. Seleccione la pestaña **Administrar**.
3. En el panel Orígenes de evento, seleccione un origen de eventos de la lista y haga clic en + o en .

   Este es un ejemplo de la pestaña Nuevo origen de eventos:

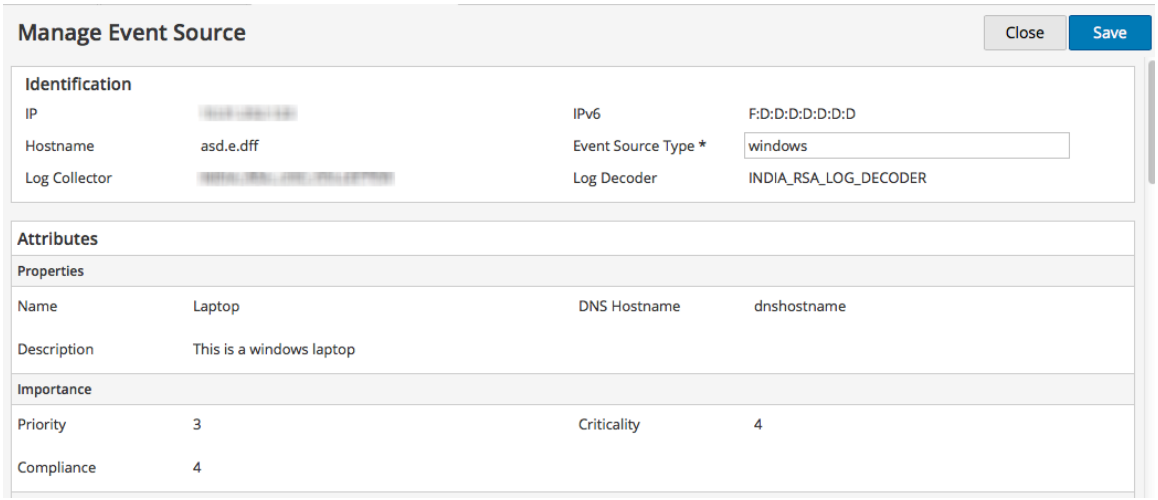



Los procedimientos relacionados con esta pestaña se describen en Crear un origen de eventos y editar los atributos.

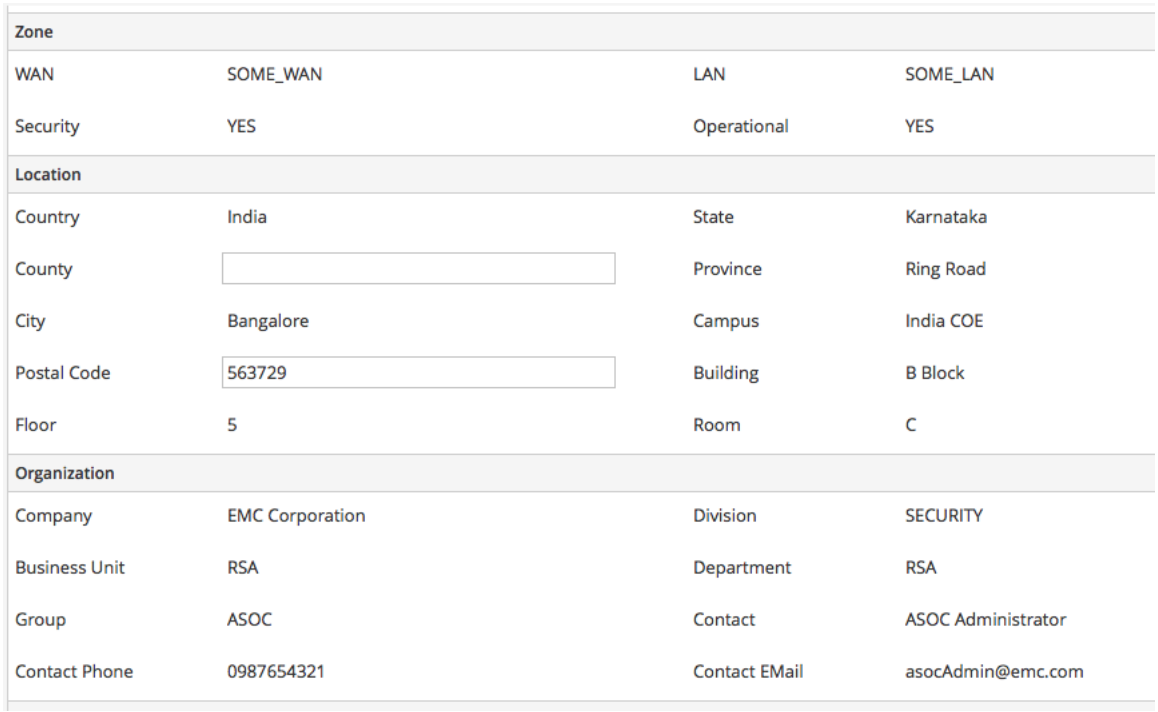
## Características

Los ajustes de la pestaña Administrar origen de eventos son una combinación de información autocompletada e ingresada por el usuario. Cuando un origen de eventos envía información de registro a Security Analytics, se agrega a la lista de orígenes de eventos y cierta información básica se completa automáticamente. En cualquier momento después de eso, los usuarios pueden agregar o editar los detalles de otros atributos de orígenes de eventos.

En esta figura se muestra un ejemplo de las secciones **Identificación**, **Propiedades** e **Importancia**.




En esta figura se muestra un ejemplo de las secciones **Zona**, **Ubicación** y **Organización**.



## Categorías

En esta tabla se describen las categorías de atributos de orígenes de eventos.

| Sección de atributo | Descripción |
|---|---|
| Identificación | Estos son los atributos principales que identifican colectivamente a un origen de eventos.<br>Los siguientes atributos se completan automáticamente y no se pueden cambiar mientras se está en esta pantalla:<br>• Dirección IP<br>• Valor IPv6<br>• Hostname<br>• Tipo de origen de evento<br>Estos atributos se pueden modificar:<br>• Log Collector<br>• Log Decoder |
| Properties | Estos atributos proporcionan el nombre y la descripción.<br>• Nombre<br>• Nombre de host de DNS<br>• Descripción |
| Importancia | Estos atributos se pueden usar para agrupar por prioridad.<br>• Prioridad<br>• Importancia<br>• Cumplimiento de normas |
| Zona | Estos atributos se pueden usar para agrupar por zona.<br>• WAN (Red de área extensa)<br>• LAN (Red de área local)<br>• Seguridad<br>• Operacional |

| Sección de atributo | Descripción |
|---|---|
| Ubicación | Estos atributos se pueden usar para agrupar por la ubicación física o geográfica.<br>• País<br>• State<br>• Condado<br>• Provincia<br>• Ciudad<br>• Campus<br>• Código postal<br>• ecológico<br>• Piso<br>• Sala |
| Organización | Estos atributos se pueden usar para agrupar por organización y también para proporcionar información de contacto.<br>• Empresa<br>• División<br>• Business Unit<br>• Departamento<br>• Grupo<br>• Contacto<br>• Teléfono de contacto<br>• Correo electrónico de contacto |
| Propietario | Estos atributos especifican a los responsables del origen de eventos.<br>• Manager<br>• Administrador primario<br>• Administrador de respaldo |

| Sección de atributo | Descripción |
|---|---|
| Física | Estos atributos especifican las propiedades físicas del origen de eventos.<br>• Proveedor<br>• Número de serie<br>• Etiqueta de recurso<br>• Voltage<br>• Protegido por UPS<br>• Altura del rack<br>• Profundidad<br>• Salida de BTU<br>• Color |
| Función | Estos atributos se pueden usar para agrupar por función.<br>• Función primaria<br>• Subfunción 1<br>• Subfunción 2 |
| Información del sistema | Estos atributos especifican información del sistema.<br>• Nombre del dominio<br>• Nombre del sistema<br>• Identifier<br>• Descripción del sistema |
| Personalizado | Esta sección proporciona ocho atributos personalizados para cualquier otro atributo que se pueda requerir en la organización. |

# Solucionar problemas de la administración de orígenes de eventos

Temas de solución de problemas:

- Problemas de notificaciones y alarmas
- Mensajes de registro duplicados
- Solucionar problemas de feeds
- Problemas de importación de archivos
- Numeración de política negativa

# Problemas de notificaciones y alarmas

En este tema se describe cómo solucionar los problemas que puede encontrar con las alarmas o las notificaciones.

## Alarmas

Si no ve las alarmas que espera ver, asegúrese de que ha configurado todos los elementos necesarios, tal como se describe a continuación.

### Alarmas automáticas

Para ver las alarmas automáticas que aparecen en la pantalla Alarmas, la opción **Habilitar el monitoreo automático** debe estar seleccionada.

Esta opción se encuentra en la pestaña **Configuración** (**Administration** > **Orígenes de evento** > **Ajustes de configuración**) y se selecciona de manera predeterminada. Sin embargo, en algún momento alguien puede haber desactivado esta opción.

### Alarmas manuales

Para ver las alarmas manuales que aparecen en la pantalla Alarmas, se deben cumplir todas las condiciones siguientes:

- El origen de evento debe ser parte de un grupo.
- El grupo debe tener definido un umbral bajo o alto (o ambos) para la política.
- La política de grupo debe estar habilitada.

## Notificaciones

Si se ven alarmas, pero no se reciben las notificaciones esperadas, asegúrese de haber configurado todos los elementos necesarios, como se describe a continuación.

Además, asegúrese de que ha configurado correctamente los servidores de notificación y las salidas de las notificaciones. Gran parte de la configuración preliminar de las notificaciones se realiza en **Administration > Sistema > Notificaciones globales**. Para obtener detalles, consulte el tema **Panel Notificaciones globales** de la *Guía de configuración del sistema*.

### Notificaciones automáticas

Para permitir que el sistema envíe notificaciones automáticas, se deben cumplir todas las condiciones siguientes:

- La opción **Habilitar el monitoreo automático** debe estar seleccionada (esta opción está seleccionada de forma predeterminada).

- La opción **Habilitar notificaciones desde el monitoreo automático** debe estar seleccionada. Esta opción está desactivada de forma predeterminada, por lo que usted o alguien en su organización debe seleccionarla. Vaya a **Administration** > **Orígenes de evento** > **Ajustes de configuración** para ver esta opción.
- El origen de eventos que activó la alarma debe estar en un grupo que tenga habilitada una política: tenga en cuenta que no es necesario configurar umbrales para las notificaciones automáticas.
- La política debe tener configurada al menos una notificación (ya sea por correo electrónico, SNMP o syslog).

#### Notificaciones manuales

Para que el sistema envíe notificaciones manuales (es decir, una notificación que afirme que se activó una alarma manual):

- El origen de eventos que activó la alarma debe estar en un grupo que tenga habilitada una política de grupo.
- Debe haber un umbral configurado para la política.
- Debe haber al menos una notificación configurada para la política.

## Mensajes de registro duplicados

Es posible que esté recopilando mensajes del mismo origen de eventos en dos o más Log Collectors. En este tema se describe el problema y las maneras de solucionarlo.

### Detalles

Si el agregador de ESM detecta los mismos eventos para el mismo origen de eventos en varios Log Collectors, se recibe una advertencia similar a la siguiente:

```
2015-03-17 15:25:29,221 [pool-1-thread-6] WARN
com.rsa.smc.esm.groups.events.listeners.EsmStatEventListener -
 192.0.2.21-apache had a previous event only 0 seconds ago;
likely because it exists on multiple log collectors
```

Este mensaje de advertencia significa que varios hosts están recopilando el origen de eventos `192.0.2.22-apache`. Puede ver la lista de hosts en la columna Log Collector en la pestaña **Administrar** de la vista Administration > Orígenes de evento.

### Borrar los mensajes duplicados

1. Detenga collectd en Security Analytics y en los Log Decoders:

   ```
   Service collectd stop
   ```

2. Quite el archivo del agregador de ESM que persistió en Security Analytics:

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Restablezca el Log Decoder.

   a. Navegue a REST de Log Decoder en `http://<LD_IP_Address>:50102`.

   b. Haga clic en **decoder(*)** para ver las propiedades del Decoder.

   c. En el menú desplegable Propiedades, seleccione **Restablecer** y haga clic en **Enviar**.

4. En el panel Orígenes de evento de la pestaña Administrar de orígenes de eventos, seleccione todos los orígenes de eventos y haga clic en − para eliminarlos.

# Solucionar problemas de feeds

El propósito del generador de feeds es generar un mapeo de un origen de eventos a la lista de grupos a la cual pertenece.

Si tiene un origen de eventos desde el cual recopila mensajes, pero no se muestra en los grupos de orígenes de eventos correctos, en este tema se proporcionan antecedentes e información que lo ayudarán a rastrear el problema.

## Detalles

El feed de ESM mapea múltiples claves a un único valor. Mapea los atributos DeviceAddress, Forwarder y DeviceType a groupName.

El propósito del feed de ESM es enriquecer los metadatos de orígenes de eventos con el groupName recopilado en el Log Decoder.

## Cómo funciona

El generador de feeds está programado para actualizarse cada minuto. Sin embargo, solo se activa si hay cambios (crear, actualizar o eliminar) en los orígenes de eventos o los grupos.

Genera un único archivo de feed con mapeo de origen de eventos a grupo y migra el mismo feed a todos los Log Decoders conectados a Security Analytics.

Una vez que el archivo de feed se carga en los Log Decoders, para los eventos nuevos, enriquece los metadatos de los eventos con groupName y agrega este groupName a logstats.

Cuando groupName está en logstats, el agregador de ESM agrupa la información y la envía a ESM. En este punto, debe ver la columna **Nombre del grupo** bajo la pestaña **Monitoreo de orígenes de eventos**.

El proceso completo puede tardar algún tiempo. Por lo tanto, tal vez deba esperar varios segundos después de agregar un nuevo grupo u origen de eventos antes de que se muestre el nombre del grupo.

**Nota:** Si el atributo de tipo de origen de eventos cambia cuando se actualiza el feed, Security Analytics agrega una nueva entrada en logstats en lugar de actualizar la existente. De este modo, habrá dos entradas de logstats distintas en logdecoder. Los mensajes existentes se enumeran bajo el tipo anterior y todos los mensajes nuevos se registran para el nuevo tipo de origen de eventos.

## Archivo de feed

El formato del archivo de feed es el siguiente:

```
DeviceAddress, Forwarder, DeviceType, GroupName
```

`DeviceAddress` es `ipv4, ipv6` o `hostname`, de acuerdo con lo que se definió para el origen de eventos.

El siguiente es un ejemplo del archivo de feed:

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apac
hegrp"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"
"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","
Apachegrp"
```

## Solución de problemas de feeds

Puede consultar los siguientes elementos para delimitar la causa del problema.

#### Log Decoders 10.5

¿Está usando la versión 10.5 o superior de Security Analytics Log Decoders? Si no es así, debe actualizarlos. Para Security Analytics versión 10.6, solo se envían feeds a Log Decoders versión 10.5 y superior.

#### Existencia del archivo de feed

Compruebe exista que el archivo Zip de los feeds en la siguiente ubicación:

`/opt/rsa/sms/esmfeed.zip`

No modifique este archivo.

#### Metadatos de grupo completados en LD

Verifique que los metadatos de grupo estén completados en el Log Decoder. Navegue a REST de Log Decoder y compruebe logstats:

`http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain`

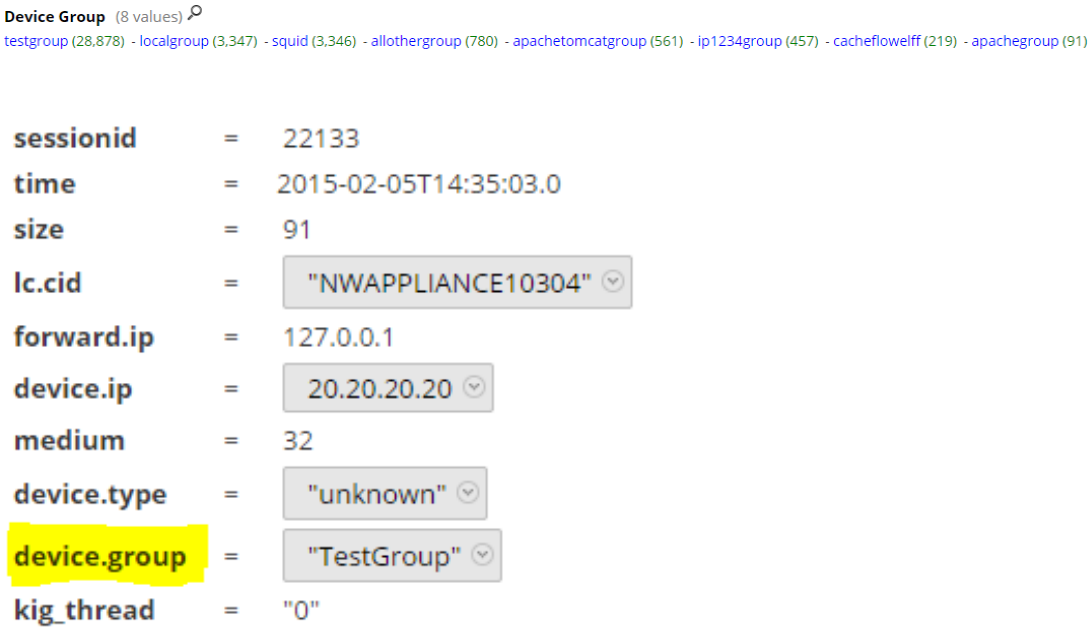
Este es un ejemplo de un archivo logstats con información de grupo:

```
device=apache forwarder=NWAPPLIANCE10304 source=1.2.3.4
count=338 lastSeenTime=2015-Feb-04 22:30:19
lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group,apacheGroup
device=apachetomcat forwarder=NWAPPLIANCE10304
source=5.6.7.8 count=1301 lastSeenTime=2015-Feb-04
22:30:19 lastUpdatedTime=2015-Feb-04 22:30:19
groups=AllOtherGroup,ApacheTomcatGroup
```

En el texto anterior, la información de grupo aparece en negrita.

### Metadatos de grupo de dispositivos en Concentrator

Compruebe que los metadatos de **grupo de dispositivos** existan en el Concentrator y que los eventos tengan valores para el campo `device.group`.




### Archivo de registro de SMS

Compruebe el archivo de registro de SMS en la siguiente ubicación para ver mensajes informativos y de error: `/opt/rsa/sms/logs/sms.log`

Los siguientes son ejemplos de mensajes *informativos*:

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

Los siguientes son ejemplos de mensajes de *error*:

```
 Error creating CSV File : <reason>Unable to push the
ESM Feed: Unable to create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> :
Error: <error>
Unable to push the ESM Feed: CSV file is empty, make
sure you have al-least on group with al-least one
eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file
on LogDecoder-<logdecoderIP>Unable to push the ESM
Feed: admin@<logdecoderIP>:50002/decoder/parsers
received error: The zip archive
"/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could
not be opened
Unable to push the ESM Feed: <reason>
```

#### Verificar que ESMReader y ESMAggregator lean y publiquen los datos de Logstats

Estos son los pasos para verificar que **collectd** recopile logstats y los publique en Administración de orígenes de eventos.

**ESMReader**

1. En Log Decoders, agregue la marca **debug "true"** en **/etc/collectd.d/NwLogDecoder_ESM.conf**:

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>
        </stats>
    </Module>
```

```
    <Module "NgEsmReader" "update">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "60"
        query     "update"
        <stats>
        </stats>
    </Module>
</Plugin>
```

2. Ejecute el siguiente comando:

   ```
   service collectd restart
   ```

3. Ejecute el siguiente comando:

   ```
   tail –f /var/log/messages | grep collectd
   ```

   Verifique que ESMReader esté leyendo logstats y que no existan errores. Si hay problemas de lectura, verá errores similares al siguiente:

   ```
   Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
   all: error getting ESM data for field "groups" from logstat
   device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
   <reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
   NgEsmReader_update: error getting ESM data for field "forwarder" from
   logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
   ```

**ESMAggregator**

1. En Security Analytics, quite la condición de comentario de la marca verbose en **/etc/collectd.d/ESMAggregator.conf**:

   ```
   # ESMAggregator module collectd.conf configuration file
   #
   # Copyright (c) 2014 RSA The Security Divsion of EMC
   #
   <Plugin generic_cpp>
   PluginModulePath "/usr/lib64/collectd"
   <Module "ESMAggregator">
           verbose 1
           interval "60"
   ```

```
            cache_save_interval "600"
            persistence_dir "/var/lib/netwitness/collectd"
        </Module>
        </Plugin>
```

2. Ejecute lo siguiente:

   ```
   service collectd restart
   ```

3. Ejecute el siguiente comando:

   ```
   run "tail -f /var/log/messages | grep ESMA
   ```

   Busque los datos de ESMAggregator y asegúrese de que la entrada de logstat esté disponible en los registros.

Ejemplo de salida:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: Dis-
patching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_coun-
ter-3.3.3.3 with a value of 1752 for NWAPPLIANCE15788/cacheflowelff/esm_
counter-3.3.3.3 aggregated from 1 log decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
```

```
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: Dis-
patching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_counter-
3.3.3.3 with a value of 1752 for NWAPPLIANCE15788/cacheflowelff/esm_coun-
ter-3.3.3.3 aggregated from 1 log
```

#### Configurar el intervalo de trabajo del generador de feeds JMX

Aunque el trabajo de generación de feeds está calendarizado para ejecutarse cada minuto de manera predeterminada, puede cambiar esto con el uso de **jconsole**, si es necesario.

**Para cambiar el intervalo de trabajo del generador de feeds:**

1. Abra **jconsole** para el servicio SMS.
2. En la pestaña MBeans, navegue a **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attributes**.
3. Modifique el valor de la propiedad **FeedGeneratorJobIntervalInMinutes**.
4. Vaya a **Operations** en el mismo árbol de navegación y haga clic en **commit()**. Esto hace persistir el nuevo valor en el archivo json correspondiente bajo **/opt/rsa/sms/conf** y usa el valor si SMS se reinicia.

La configuración de un nuevo valor vuelve a programar el trabajo del generador de feeds en el nuevo intervalo.

## Problemas de importación de archivos

Si el archivo de importación no tiene el formato correcto o si le falta información requerida, se muestra un error y el archivo no se importa.

Revise lo siguiente:

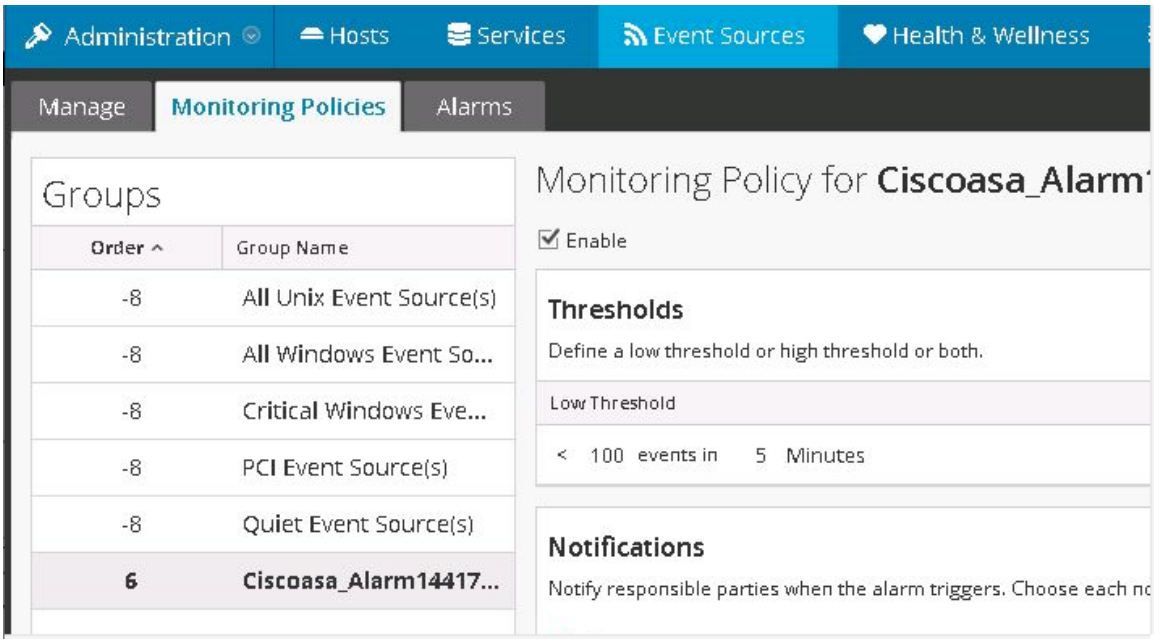
- Si está agregando orígenes desconocidos, cada línea del archivo debe contener una combinación de los atributos requeridos:
  - IP o IPv6, Nombre de host y
  - Tipo de origen de evento
- La primera línea del archivo debe contener nombres de encabezado y estos deben coincidir con los nombres en Security Analytics. Para obtener una lista de nombres de columna correctos, puede exportar un único origen de eventos. Examine el archivo CSV exportado: la primera fila del archivo contiene el conjunto correcto de atributo/nombres de columna.

## Numeración de política negativa

Es posible que vea números negativos en el campo Orden en la sección Grupos de la pestaña Políticas de monitoreo. En este tema se describe una solución alternativa para restaurar el esquema de numeración correcto para sus políticas.

### Detalles

En la siguiente pantalla se muestra un ejemplo de la situación donde los números de las políticas de grupo se convierten en negativos.




Si se produce esta situación, arrastre y suelte el grupo superior (**Todos los orígenes de eventos de Unix** en la imagen anterior) después del último grupo (**Ciscoasa_Alarm14417**). Esto restaura la numeración normal, ordinal. Puede seguir arrastrando y soltando grupos hasta tenerlos en el orden adecuado para su organización.

### Borrar los mensajes duplicados

1. Detenga collectd en Security Analytics y en los Log Decoders:

   ```
   Service collectd stop
   ```

2. Quite el archivo del agregador de ESM que persistió en Security Analytics:

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Restablezca el Log Decoder.

a. Navegue a REST de Log Decoder en `http://<LD_IP_Address>:50102`
b. Haga clic en **decoder(*)** para ver las propiedades del Decoder.
c. En el menú desplegable Propiedades, seleccione **Restablecer** y haga clic en **Enviar**.

4. En el panel Orígenes de evento de la pestaña Administrar de orígenes de eventos, seleccione todos los orígenes de eventos y haga clic en − para eliminarlos.