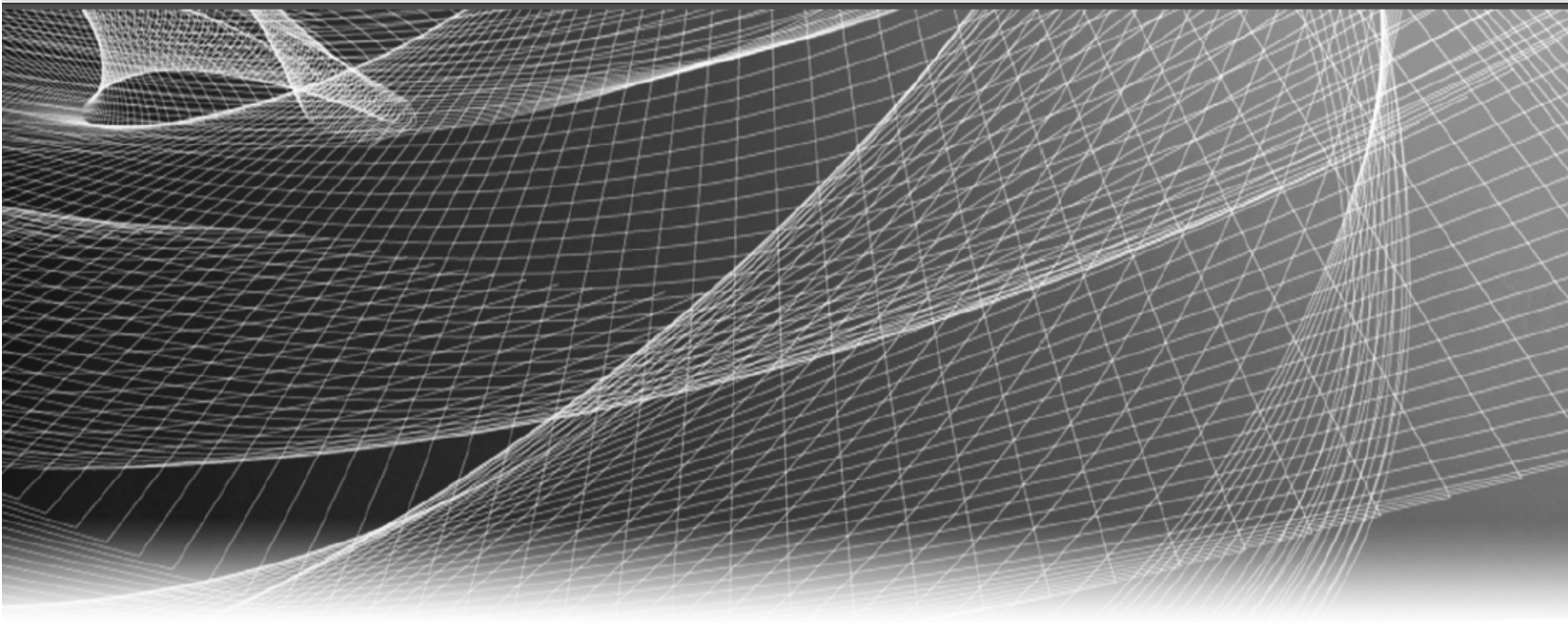


RSA Security Analytics

Alertas mediante ESA

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Introducción de ESA

En este tema se abordan materias relacionadas con el inicio rápido de Event Stream Analysis (ESA) que lo ayudarán a comenzar a usar ESA. Los siguientes temas están diseñados como una ayuda para permitirle trabajar con ESA.

- Este tema lo ayuda a comprender la mejor manera de configurar, implementar y crear reglas. Consulte Mejores prácticas
- Este tema lo ayuda a solucionar problemas relacionados con distintos aspectos de ESA, incluida la escritura y la implementación de reglas:Solucionar problemas de ESA
- Este tema lo ayuda a trabajar con métricas de memoria para comprender el uso de la memoria para los servicios ESA. Consulte Ver métricas de memoria para reglas

Mejores prácticas

Use estas mejores prácticas como guía para escribir y administrar reglas, implementarlas y mantener el estado del sistema para los servicios de ESA.

Comprender tipos de reglas de Event Stream Analysis

El servicio Security Analytics Event Stream Analysis (ESA) proporciona analítica de flujo avanzada como correlación y procesamiento de eventos complejos a altos rendimientos y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de Concentrators. Sin embargo, cuando trabaja con Event Stream Analysis, debe tener en cuenta los factores que afectan el uso de recursos para crear reglas eficaces.

Cada evento que recibe ESA se evalúa para determinar si puede activar una regla. Se pueden implementar tres tipos de reglas para determinar lo que debe hacer el motor de ESA con el evento entrante. Cada uno de estos tipos de reglas tiene distintos impactos en la utilización de recursos del sistema. Los tres tipos de reglas se pueden crear mediante el generador de reglas o reglas de EPL avanzado, o se pueden descargar a través de RSA Live. En la siguiente tabla se indica el tipo de regla y el impacto que puede tener en los recursos del sistema.

Tipo de regla	Descripción
Regla de filtro simple	Esta regla no tiene ninguna correlación con otros eventos. En el momento de la recopilación, esta regla se evalúa con respecto a un conjunto de condiciones y, si esas condiciones se cumplen, se genera una alerta. Si no coincide ninguna condición, el motor deja ir rápidamente el evento para liberar uso de la memoria. Estas reglas no usan memoria puesto que los eventos no se conservan más allá de la evaluación inicial. El uso de recursos de la memoria no aumenta a medida que se implementan más reglas de filtro simple. Sin embargo, si la condición del filtro es demasiado genérica, es posible que esta regla genere demasiadas alertas, las cuales llevarán al límite los recursos del sistema en términos de su almacenamiento y recuperación. Por ejemplo, podría escribir una regla que genere una alerta cuando llegue actividad de red HTTP a través de un puerto HTTP no estándar.
Regla de ventana de eventos	Esta regla evalúa condiciones específicas en un conjunto de eventos durante un periodo. En el momento de la recopilación, la regla se evalúa con respecto a un conjunto de condiciones. Si esas condiciones se cumplen, el evento se conserva en la memoria durante una cantidad de tiempo específica. Cuando transcurre el tiempo especificado, los eventos se eliminan de la ventana de tiempo si la cantidad de eventos recopilados no cumple con el umbral para activar una alerta. El consumo de memoria de estas reglas depende en gran medida de la tasa (tráfico) de eventos entrantes, la cantidad de datos por evento y la cantidad de tiempo especificada en la ventana de eventos. Cada evento coincidente se conserva en la memoria hasta que transcurre la ventana de tiempo. Por lo tanto, mientras más prolongada sea la ventana de tiempo, mayor será el volumen potencial. Por ejemplo, podría escribir una regla que genere una alerta si un usuario no puede iniciar sesión cinco veces en ningún sistema en un intervalo de tiempo de diez minutos.

Tipo de regla	Descripción
Regla Seguido de	Esta regla evalúa una cadena de eventos entrantes para determinar si la secuencia de eventos coincide con una condición específica. En el momento de la recopilación, la regla se evalúa con respecto a un conjunto de condiciones. Si las condiciones se cumplen, se produce una de dos acciones: • Si se trata del primer evento de la secuencia, se inicia un nuevo hilo de ejecución de eventos y el evento se conserva como el principal de la secuencia. • Si el evento pertenece a un hilo de ejecución de eventos existente, se agrega a esa secuencia. En ambos casos, el evento se conserva en la memoria. En este tipo de regla, la cantidad de uso de recursos es especialmente sensible al ambiente del cliente. Si la condición del filtro genera muchos hilos de ejecución de eventos, los recursos se consumen para cada hilo de ejecución nuevo (además del evento). Además, si el final del hilo de ejecución de eventos no se alcanza nunca (es decir, nunca se genera una alerta), el evento completo se guarda en la memoria indefinidamente. Por ejemplo, podría escribir una regla que genere una alerta cuando un usuario no logra iniciar sesión en un servidor, después realiza un inicio de sesión correcto y, a continuación, crea una nueva cuenta.

Además del uso de la memoria analizado anteriormente, la generación de la alerta también consume recursos del sistema. Cada alerta que se genera se debe almacenar para su recuperación e Incident Management también debe procesarla. Este proceso usa espacio en disco para almacenamiento, requiere que se consuma memoria de la base de datos y aumenta la utilización del CPU con la ejecución de consultas.

Cuando escribe e implementa reglas, debe tener en cuenta que cada una de estas acciones le "cuesta" recursos del sistema. Las siguientes secciones están diseñadas para ayudarlo a mantener el uso en un nivel adecuado y a monitorear problemas en caso de sobrecarga de los sistemas.

Mejores prácticas para escribir reglas

Estas son reglas generales para la escritura de reglas.

- **Cree alertas para eventos útiles.** El propósito de una alerta debe ser informar sobre un evento que requiere una acción inmediata y específica. Para aquellos eventos que no

necesitan ninguna acción o que solo requieren reconocimiento, puede crear un informe. Esto ayuda a impedir la sobrecarga de la base de datos que almacena alertas.

- **Configure reglas nuevas como reglas de prueba para que pueda observar cómo reaccionan en su ambiente**. Si implementa reglas nuevas como reglas de prueba, se deshabilitarán si se supera el umbral de memoria configurado. También puede usar la función de instantánea de la memoria para ver cuánta memoria se usó cuando se deshabilitó una regla de prueba. Para obtener más detalles, consulte Trabajar con reglas de prueba.
- **Configure notificaciones de alertas solo después de que se completen las pruebas y el ajuste de las reglas**. Con esto puede asegurarse de que no recibirá una gran cantidad de notificaciones si una regla tiene un comportamiento distinto al previsto.
- **Las reglas deben ser específicas de modo que se limite el uso de recursos**. Utilice las siguientes reglas para limitar el uso:
  - Haga que los filtros de la regla excluyan todos los eventos, salvo los necesarios, de modo que la regla se active con exactitud.
  - Haga que el tamaño de las ventanas (tiempo de la ventana para correlación) sea lo más breve posible.
  - Limite los eventos que incluye en la ventana: por ejemplo, si solo desea ver eventos de IDS, asegúrese de incluir únicamente esos eventos en la ventana de tiempo.
- **Las reglas se deben ajustar a un nivel de alerta que sea administrable**. Si recibe una gran cantidad de alertas, su propósito y su utilidad se pierden. Además, es posible que la base de datos que almacena alertas se desborde, lo cual puede impedir que el sistema procese las alertas o hacer que se retrase. Por ejemplo, es posible que desee saber sobre el tráfico cifrado a otros países. Sin embargo, podría limitar la lista a países que constituyen riesgos conocidos. Esto limita el volumen de alertas a un nivel que puede administrar.

Mejores prácticas para trabajar con reglas de RSA Live

Estas son reglas para las reglas de RSA Live.

- **Implemente reglas de RSA Live en lotes pequeños**. No todas las reglas son aptas para todos los ambientes. La mejor manera de asegurarse de que las reglas de RSA Live funcionen correctamente es implementarlas en lotes pequeños que permitan probarlas en el ambiente. Si implementa lotes pequeños, es mucho más fácil detectar si una regla específica tiene un problema.

- **Lea las descripciones de las reglas que se proporcionan con las reglas de RSA Live**. Las reglas de ESA no se aplican a todas las situaciones. No todas las reglas funcionarán en su ambiente. Las descripciones de las reglas indican los parámetros que tendrá que modificar para implementar correctamente una regla en su ambiente.
- **Configure sus parámetros**. Las reglas de RSA Live tienen parámetros que se deben modificar. Si no modifica los parámetros, es posible que la regla no funcione o puede agotar la memoria.
- **Implemente las reglas nuevas como reglas de prueba de modo que pueda observar cómo reaccionan en el ambiente.** Si implementa reglas nuevas como reglas de prueba, se inhabilitarán si se supera el umbral de la memoria configurado. Para obtener más detalles, consulte Trabajar con reglas de prueba.

Mejores prácticas para implementar reglas

Estas son reglas generales para implementar reglas.

- **Implemente las reglas en lotes pequeños de modo que pueda observar cómo reaccionan en el ambiente.** No todos los ambientes son iguales y será necesario ajustar una regla en cuanto al uso de la memoria, el volumen de alertas y la detección eficaz de eventos.
- **Pruebe las reglas antes de configurar notificaciones de alertas**. Configure notificaciones de alertas solo después de que se completen las pruebas y el ajuste de las reglas. Con esto puede asegurarse de no recibirá una gran cantidad de alertas si una regla tiene un comportamiento distinto al previsto.
- **Monitoree el estado del sistema como parte del proceso de implementación**. Cuando implemente reglas, monitoree el estado del sistema como parte del proceso de implementación. Puede ver la utilización total de la memoria para ESA en la pestaña Estado y condición. Para obtener más información, consulte “Visualización de estadísticas de Estado y condición” en Solucionar problemas de ESA.

Mejores prácticas para el estado del sistema

Estas son reglas generales para el estado del sistema.

- **Configure la base de datos de alertas para mantener un nivel adecuado de alertas**. ESA usa MongoDB para almacenar las alertas. Si MongoDB se desborda con alertas, puede retrasar o detener la base de datos. Para asegurarse de que la base de datos mantenga un nivel adecuado de alertas, configure ajustes con el fin de borrar las alertas regularmente.

Para hacer esto, consulte “Configurar el almacenamiento de ESA” en la **Guía de configuración de Event Stream Analysis (ESA)**.

- **Configure reglas nuevas como reglas de prueba**. Un problema común es que las reglas nuevas pueden causar dificultades relacionadas con la memoria. Para impedir esto, puede configurar las reglas nuevas como reglas de prueba. Si se alcanza el umbral de la memoria configurado, todas las reglas de prueba se inhabilitan para impedir que se agote la memoria del sistema. Para obtener más información acerca de las reglas de prueba, consulte Trabajar con reglas de prueba.
- **Configure umbrales en el módulo Estado y condición que le informen si el uso de la memoria es demasiado alto.** El módulo Estado y condición incluye métricas que rastrean el uso de la memoria. Puede configurar alertas y notificaciones que le informan por correo electrónico si se cruzan esos umbrales. Para obtener más información acerca de las estadísticas de la memoria que puede ver, consulte “Visualización de estadísticas de Estado y condición” en Solucionar problemas de ESA.
- **Monitoree las métricas de memoria para cada regla en el módulo Estado y condición**. Ahora puede ver el uso estimado de la memoria para cada regla activa en el módulo Estado y condición. Puede usar esta información para asegurarse de que las reglas no usen demasiada memoria. Para obtener más información acerca de las estadísticas de memoria que puede ver, consulte “Visualización de estadísticas de Estado y condición” en Solucionar problemas de ESA.

Solucionar problemas de ESA

En esta sección se describen problemas comunes que pueden ocurrir durante el uso de ESA y se sugieren soluciones para abordarlos.

Solucionar problemas de servicios de ESA

Problema	Causas posibles	Soluciones
En el tablero de Security Analytics, el servicio de ESA se muestra en rojo para indicar que está offline. En la página **Alertas** > **Configurar** se muestra el siguiente mensaje: "El servicio está offline o inaccesible".	Varias	Las posibles causas por las cuales un servicio de ESA puede estar offline son muchas. Sin embargo, un problema común es que una regla que se creó usa un exceso de memoria, lo cual hace que el servicio de ESA falle. Para solucionar este problema, consulte "Pasos para solucionar problemas de memoria con un servicio ESA offline". Entre otras causas comunes, el firewall puede estar bloqueando la conexión entre ESA y Security Analytics, o la máquina del servicio de ESA puede estar inactiva.
		Para abrir los servicios de ESA: En **Administration** > **Servicios**, seleccione el ícono de acciones  correspondiente al servicio ESA y elija **iniciar**. Si el servicio de ESA se detiene y se reinicia en un loop, tal vez sea necesario llamar al servicio al cliente para lograr que el servicio se inicie.
Después de una actualización reciente, el servicio de ESA se muestra en rojo en el tablero de Security Analytics para indicar que está offline. En la página **Alertas** > **Configurar** se muestra el siguiente mensaje: "El servicio está offline o inaccesible".	Problemas de configuración	Si el sistema se actualizó recientemente, tal vez se cometió un error de configuración. En **Administration** > **Servicios**, seleccione el servicio ESA y haga clic en **Editar servicio**. En el campo Editar servicio, haga clic en Probar conexión. Si las conexiones fallan, es probable que exista un error de configuración. Intente corregir el error de configuración y vuelva a intentarlo.

Problema	Causas posibles	Soluciones
El servicio de ESA parece funcionar lentamente.	Problemas de configuración	Es posible que pueda mejorar el rendimiento mediante la modificación del búfer (el valor predeterminado es *10,485,760 bytes*) o mediante la configuración del ajuste de TCP en TCPNoDelay para evitar un retraso en la recepción de confirmaciones de TPC. Puede modificar estos ajustes (*readBufferSize* y *tcpNoDelay*) en *Explorer /Workflow/Source/nextgenAggregation*.

Solucionar problemas de la base de datos de ESA

Problema	Causas posibles	Soluciones
Mi tablero de ESA no se carga. • O bien, hay un error al obtener los datos. • O bien, se carga con mucha lentitud.	El tamaño de la base de datos que almacena las alertas aumentó demasiado.	Tal vez sea necesario configurar los ajustes de la base de datos de alertas de modo que la base de datos borre oportunamente las alertas antiguas. Para obtener información sobre cómo configurar estos ajustes, consulte “Configurar el almacenamiento de ESA” en la **Guía de configuración de Event Stream Analysis (ESA)**. Cuando el tamaño de la base de datos aumenta demasiado, debe borrar las alertas. Póngase en contacto con el servicio al cliente para hacerlo.

Solucionar problemas de reglas de RSA Live para ESA

Problema	Causas posibles	Soluciones
Importé un grupo de reglas de RSA Live y ahora se produce una falla general en el servicio de ESA. ¿Por qué?	Es posible que no haya configurado los parámetros de la regla de RSA Live de acuerdo con el ambiente.	En cada regla de RSA Live hay una descripción que incluye los parámetros que debe configurar y los requisitos previos para el ambiente. Revise esta descripción para ver si la regla es apropiada para el ambiente. Para asegurarse de implementar reglas con seguridad en el ambiente, configure reglas nuevas como reglas de prueba de modo que pueda probarlas en el ambiente. Las reglas de prueba son un resguardo para probar las reglas nuevas. Para obtener detalles sobre esto, consulte Implementar reglas como reglas de prueba.

Problema	Causas posibles	Soluciones
Importé un grupo de reglas de RSA Live y, aunque se implementaron sin errores, se deshabilitaron más adelante.	No todas las reglas de RSA Live están diseñadas para cada ambiente. Es posible que no tenga los metadatos correctos en ESA para que se ejecute la regla.	Para verificar si se deshabilitó una regla, vaya a Alertas > Servicios > Estadísticas de reglas implementadas. Si la regla está deshabilitada, el ícono de color verde no se muestra junto a ella. Si una regla se implementó correctamente, pero se deshabilitó, compruebe excepciones relacionadas con la regla en los registros. Específicamente, compruebe si las reglas se deshabilitaron debido a la falta de metadatos. Para ello, vaya a **Administration** > **Servicios**, seleccione el servicio ESA y elija  > **Ver** >**Registros**. A continuación, busque un mensaje similar al siguiente: "Property named '<meta_name>' is not valid in any stream" Por ejemplo, puede ver lo siguiente: `Failed to validate filter expression '(medium=1 and streams=2 or medium=3...(238 chars)': Property named 'tcp_flags_seen' is not valid in any stream` Si se muestra un mensaje similar, debe agregar una clave de metadatos personalizados a Log Decoder o Concentrator. Para ello, siga estas instrucciones: “Crear claves de metadatos personalizados mediante un feed personalizado” en la **Guía de configuración de Decoder y Log Decoder**.

Solucionar problemas de las implementaciones

Problema	Causas posibles	Soluciones
Creé una regla y comprobé la sintaxis. La regla parecía estar bien. Cuando fui a implementar la regla, recibí un error. ¿Por qué?	Es posible que no tenga los metadatos correctos para implementar la regla.	Compruebe las referencias de claves de metadatos. Es posible que no tenga los metadatos correctos para implementar la regla.

Solucionar problemas de reglas

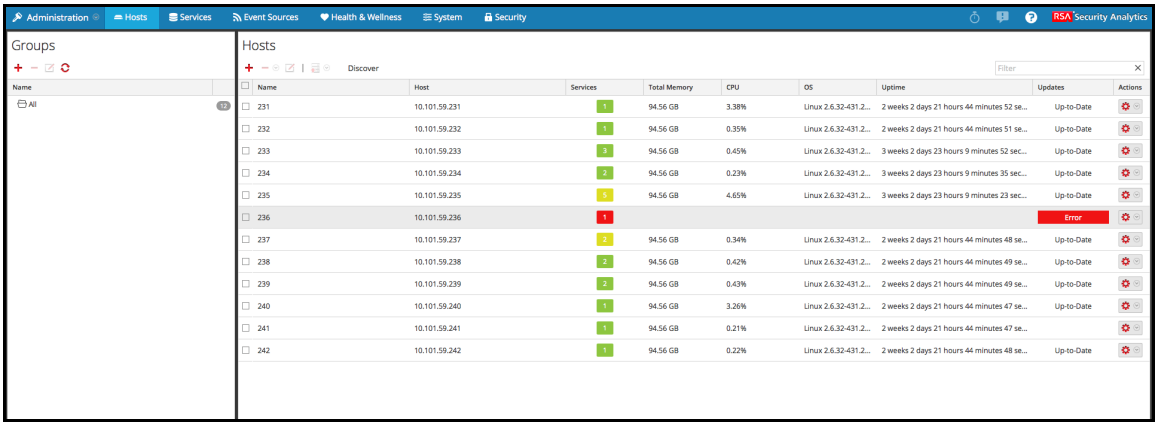
Problema	Causas posibles	Soluciones
Creé una regla personalizada (a través del generador de reglas o de EPL avanzado) y la regla no se activa. ¿Por qué?	Es posible que existan problemas de conectividad.	Compruebe la estadística "Tasa ofrecida" en la pestaña **Alertas** > **Configurar** > **Servicios**. Si la tasa ofrecida es cero, el servicio de ESA no está recibiendo datos de los Concentrators. Valide la conectividad de Concentrator. Vaya a **Administration** > **Servicios**, seleccione su ESA y haga clic en **Ver** > **Configuración**. Asegúrese de que el Concentrator esté habilitado. Seleccione el Concentrator y haga clic en **Probar conexión**. Si la tasa ofrecida no es cero, es probable que el nombre y el tipo de clave de metadatos que se usan en la regla no coincidan con la clave de metadatos presente en los eventos. Compruebe que el nombre y el tipo de clave de metadatos que se usan en la regla sean válidos. Para esto, busque el nombre de la clave de metadatos en la pestaña **Alertas** > **Configurar** > **Configuración** (búsqueda de referencias de claves de metadatos).

Problema	Causas posibles	Soluciones
	Es posible que exista un problema relacionado con la regla.	**Si una regla específica no se activa**, vaya a **Alertas** > **Configurar** > **Servicios** para ver si la regla se deshabilitó. En la sección **Estadísticas de reglas implementadas**, una regla que se inhabilitó muestra un botón de habilitación transparente (en lugar de un botón de habilitación verde). También puede comprobar el campo Eventos con coincidencias. Vaya a **Alertas** > **Configurar** > **Servicios**. Desde ahí, puede ver la cantidad de eventos que coincidieron en la columna **Eventos con coincidencias**. Si no coincidió ningún evento, vea si hay errores en la lógica de la regla. Por ejemplo, vea si hay errores de mayúsculas y minúsculas en la sintaxis y compruebe la ventana de tiempo. Si la regla continúa sin activarse, considere simplificar la lógica de la regla para ver si se activa cuando la complejidad es menor.

Pasos para solucionar problemas de memoria con un servicio de ESA offline

Paso 1: Verifique que el host esté en ejecución

El primer paso para solucionar problemas es asegurarse de que el host esté en ejecución. Para esto, vaya a **Administration** > **Hosts**. Si el host está inactivo, los parámetros del sistema no se muestran (a veces, la actualización de la información del host se puede tardar), los **Servicios** aparecen en rojo y el campo **Actualizaciones** muestra un mensaje de error.



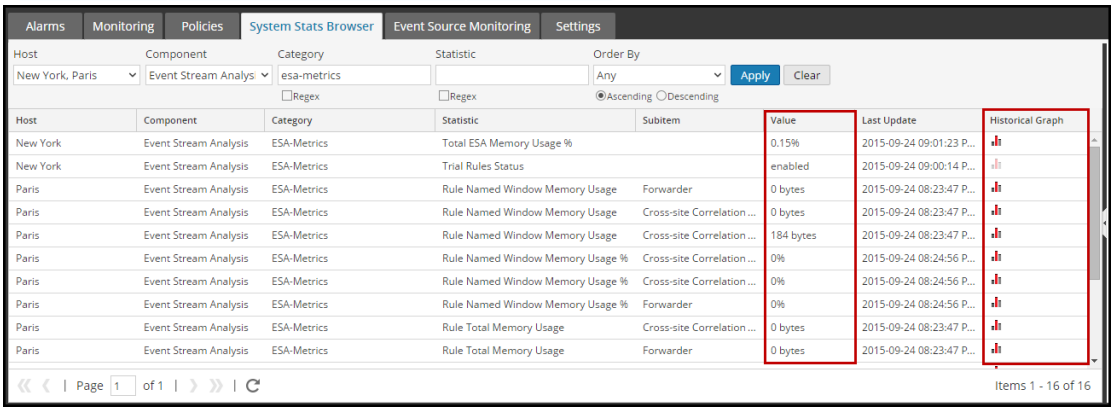
Si el host está inactivo, póngase en contacto con el administrador de SA para que lo reinicie. De lo contrario, vaya al paso 2.

Paso 2: Ver estadísticas detalladas en Estado y condición

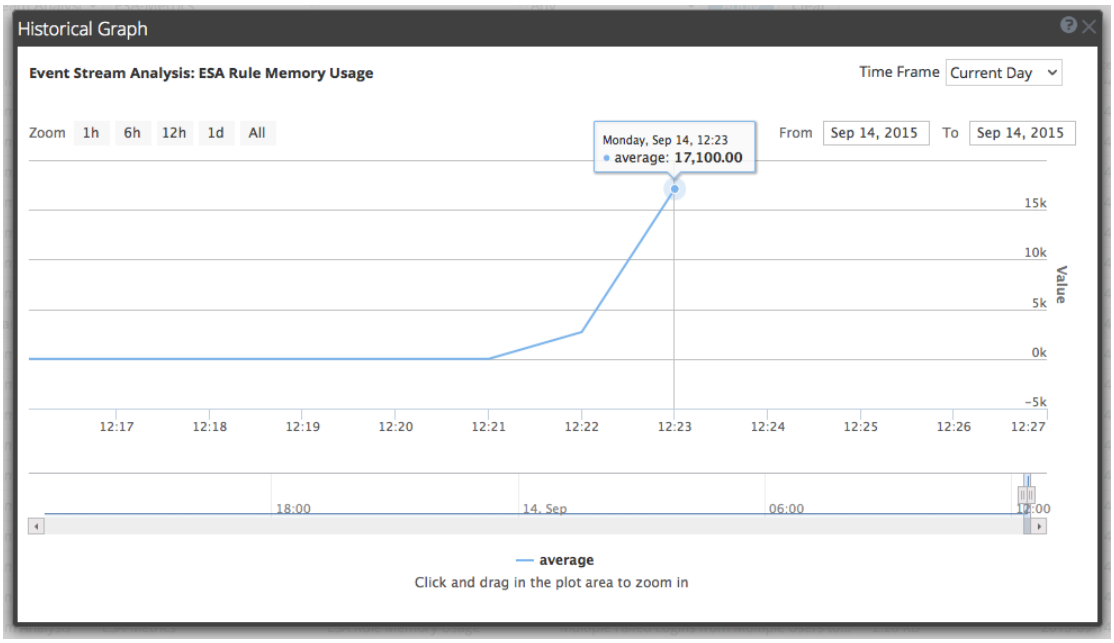
Cuando esté seguro de que el servicio de ESA está inactivo, puede ir a Estado y condición para ver dónde se están produciendo los posibles problemas. El problema más común es que el servicio de ESA está superando los umbrales de la memoria, lo cual causa su detención o falla.

1. Vaya a **Estado y condición**> **Alarmas** para ver si ESA activó alarmas. Busque las siguientes alarmas:
   - Utilización total de memoria de ESA > 85 %
   - Utilización total de memoria de ESA > 95 %
   - Servicio ESA detenido
2. Vaya a **Estado y condición** > **Estadísticas del sistema Navegador** para ver las métricas de memoria del rendimiento de cada regla. Para ver las métricas, escriba lo siguiente:

Host	Componente	Categoría
<your host>	Event Stream Analysis	esa-metrics



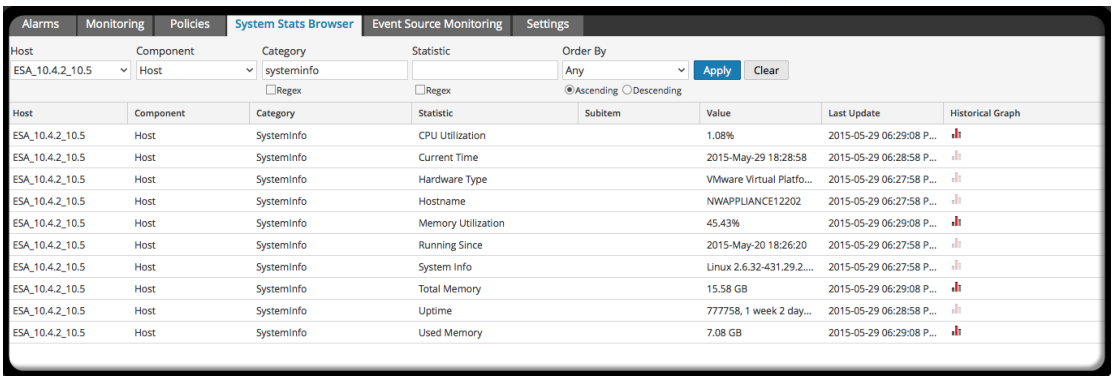
La memoria de cada regla se muestra en la columna **Valor** y el valor se muestra en bytes. Puede ver una vista histórica de uso de memoria en la columna **Gráfico histórico**.



3. Vaya a **Estado y condición** > **Navegador de estadísticas del sistema** para ver detalles del rendimiento de ESA. Seleccione el host y use los filtros que se presentan a continuación para ver las siguientes estadísticas:

Host	Componente	Categoría	Estadísticas	Ejemplo
<your host>	Host	SystemInfo	Utilización de CPU	1.08 %
<your host>	Host	SystemInfo	Memory Utilization	45.43 %
<your host>	Host	SystemInfo	Memoria usada	7.08 GB
<your host>	Host	SystemInfo	Memoria total	15.58 GB
<your host>	Host	SystemInfo	Uptime	77758, 1 semana, 2 días…
<your host>	Event Stream Analysis	ProcessInfo	Memory Utilization	7.07 GB
<your host>	Event Stream Analysis	ProcessInfo	Utilización de CPU	0.2 %

Host	Componente	Categoría	Estadísticas	Ejemplo
<your host>	Event Stream Analysis	JVM.Memory	all	Uso de memoria en montón comprometida 8.0 GB
<your host>	Event Stream Analysis	ESA-Metrics	Porcentaje total de uso de memoria de ESA	4.64 %



Si tiene un problema relacionado con la utilización de la memoria o del CPU, continúe con el paso 3.

Paso 3: Abrir los servicios de ESA

1. En **Administration** > **Servicios**, seleccione el ícono de acciones  correspondiente al servicio ESA y elija **iniciar**.
2. Regrese al servicio de ESA para dar solución a las reglas que crearon problemas de memoria.

Si el servicio de ESA se detiene y se reinicia en un loop, tal vez sea necesario llamar al servicio al cliente para lograr que el servicio se inicie.

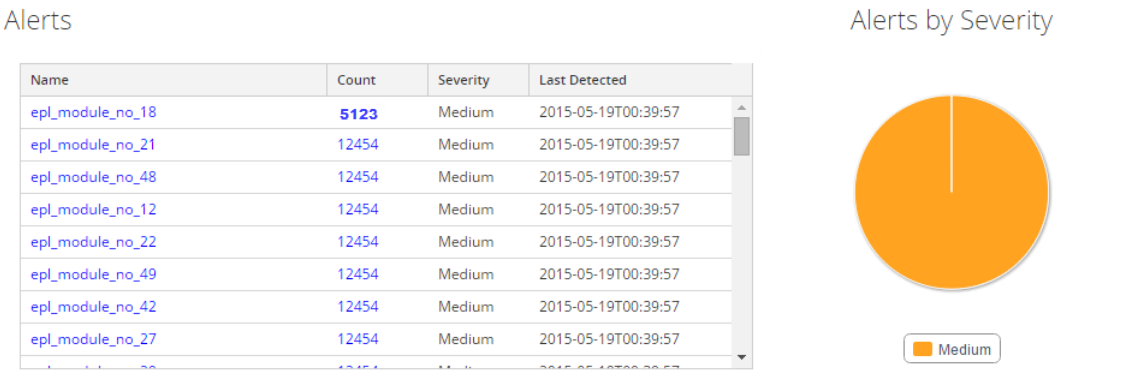
Si puede iniciar el servicio de ESA sin un apagado, continúe con el paso 4.

Paso 4. Comprobar el volumen de alertas y eventos

Cuando pueda reiniciar el servicio ESA sin un apagado inmediato, podrá revisar las estadísticas de las reglas para ver cuáles están consumiendo demasiados recursos. A veces, los servicios ESA fallan porque una regla está generando demasiadas alertas o está coincidiendo con demasiados eventos. Compruebe ambos problemas si determinó que el uso de la memoria es la causa del apagado del servicio de ESA.

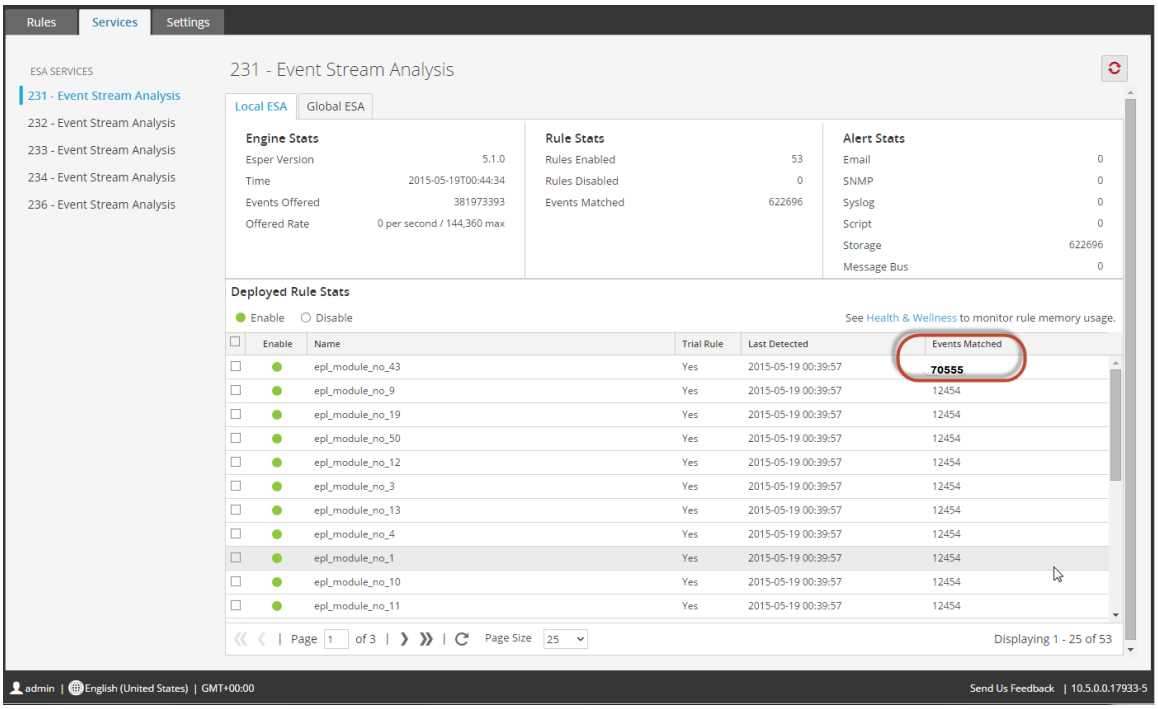
Ver resúmenes de alertas

Las reglas que generan un alto volumen de alertas pueden abrumar el sistema y hacer que falle o que se reinicie. Para ver los resúmenes de las alertas, vaya a **Tablero** > **Alertas** > **Resumen**. En la mitad inferior de la pantalla, puede ver la cantidad de alertas generadas para cada regla en el campo **Conteo**. Si la cantidad es considerablemente alta para una regla específica, debe deshabilitar la regla y reescribirla de modo que sea más eficiente.



Ver eventos con coincidencias

A veces, una regla coincide con demasiados eventos, lo cual puede consumir un exceso de memoria. Esto suele suceder si crea una gran ventana de eventos en la cual se acumula una cantidad considerable de eventos sin que se active una alerta. Estos son un problema porque cada evento se almacena en la memoria mientras la regla espera que se active la alerta. Para comprobar este problema, vaya a **Tablero** > **Alertas** > **Servicios.** Desde ahí, puede ver la cantidad de eventos que coincidieron en la columna **Eventos con coincidencias**. Si una gran cantidad de eventos coincidieron con una determinada regla, puede investigar más a fondo la regla para ver si es posible hacerla más eficiente.



Paso 5: Inhabilitar y reparar la regla que causó problemas

Cuando haya determinado las reglas que se deben reescribir, deshabilítelas y vuelva a escribirlas de modo que no generen un alto volumen de alertas o eventos. Para obtener instrucciones sobre cómo escribir reglas más eficientes, consulte Mejores prácticas.

Inhabilitar reglas

1. Para deshabilitar reglas, vaya a **Alertas** > **Servicios** y seleccione las reglas que desea deshabilitar en el campo **Estadísticas de reglas implementadas**.
2. Seleccione **Desactivar** para inhabilitar las reglas.

Editar reglas

1. Para reparar las reglas, vaya a **Alertas** > **Reglas** > **Biblioteca de reglas**. Seleccione la regla que desea editar y haga clic en el ícono de acciones  .
2. Seleccione **Editar**.
3. Edite la regla para que sea más eficiente. Para obtener instrucciones sobre cómo crear reglas, consulte Agregar reglas a la Biblioteca de reglas
4. Cuando esté conforme con la regla, puede guardarla como una regla de prueba para asegurarse de que los problemas relacionados con la memoria no afecten el rendimiento de los servicios de ESA. Para esto, siga los pasos que se indican en Trabajar con reglas de prueba.

Habilitar reglas

1. Para habilitar reglas, vaya a **Alertas** > **Servicios** y seleccione las reglas que desea habilitar en el campo **Estadísticas de reglas implementadas**.
2. Seleccione **Activar** para habilitar las reglas.

(Opcional) Comprobar los archivos de registro de ESA para obtener más información

Cuando verifique que los servicios están inactivos y algunas causas potenciales de la falla del sistema, compruebe si el servicio se detiene y se reinicia en un loop. Para esto, consulte los registros de ESA. En el módulo **Administration** > **Servicios**, seleccione el servicio ESA, haga clic en el ícono de acciones  y seleccione **Ver** > **Registros**.

Si no puede acceder a los registros de ESA desde la interfaz de Security Analytics, puede acceder al sistema mediante el protocolo SSH y dirigirse a: `opt/rsa/esa/logs/esa.log`.

Ver métricas de memoria para reglas

En este tema se indica a los escritores de reglas de ESA cómo ver métricas de memoria para las reglas. Puede ver el uso estimado de la memoria para cada regla que se ejecuta en un servidor y puede utilizar esta información para modificar las declaraciones y las condiciones de las reglas si usan demasiada memoria.

Las reglas, en ocasiones, pueden consumir más memoria de lo esperado, lo que puede retrasar o detener el ESA. Para ver aproximadamente cuánta memoria está usando una regla, puede configurar métricas de memoria. Las métricas de memoria permiten ver un uso estimado de la memoria para cada regla en el Navegador de estadísticas del sistema de Estado y condición (lo cual hará necesario disponer de permisos para acceder a este módulo). Puede usar esta información para modificar las reglas para que sean más eficientes.

En general, tendrá que realizar los siguientes pasos para usar las métricas de memoria con el fin de solucionar problemas relacionados con el uso de la memoria para las reglas:

1. Asegúrese de que la función de métricas de memoria esté habilitada (mediante Explorador > CEP > Métricas > EnableStats). Esta función está habilitada de manera predeterminada.
2. Asegúrese de disponer de los permisos correctos para ver el módulo Estado y condición. Para obtener información sobre las funciones y los permisos, consulte Permisos de funciones.
3. Vea las estadísticas de memoria en Estado y condición.
4. (Recomendado) Configure políticas de ESA de Estado y condición para enviar un correo electrónico si se superan los umbrales de la memoria. Consulte “Administrar políticas” en la **Guía de mantenimiento del sistema** para obtener instrucciones sobre el envío de notificaciones por correo electrónico.

5. Use los datos de métricas de memoria para modificar las reglas para que sean más eficientes, si es necesario.

Requisitos previos

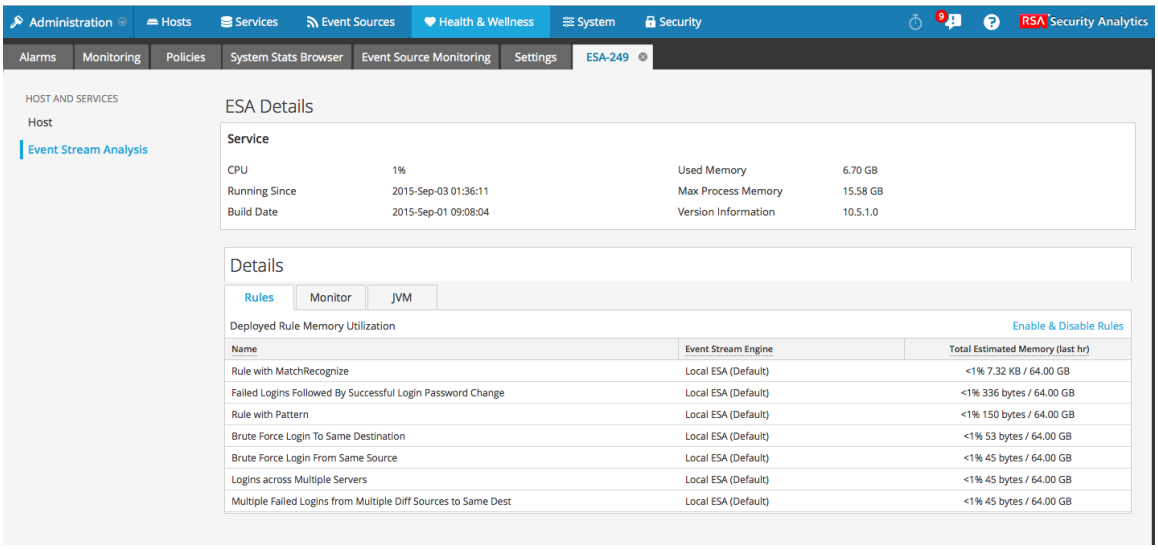
Los siguientes son los requisitos para el uso de métricas de memoria:

- La función Métricas de memoria debe estar habilitada (mediante **Explorador** > **CEP** > **Métricas** > **EnableStats**).
- El usuario debe tener los permisos apropiados para ver estadísticas de Estado y condición.
- (Recomendado) Configure la política de ESA de Estado y condición para enviar un correo electrónico si se superan los umbrales de la memoria.

Procedimientos

Ver las métricas de memoria en el módulo de monitoreo del sistema de Estado y condición

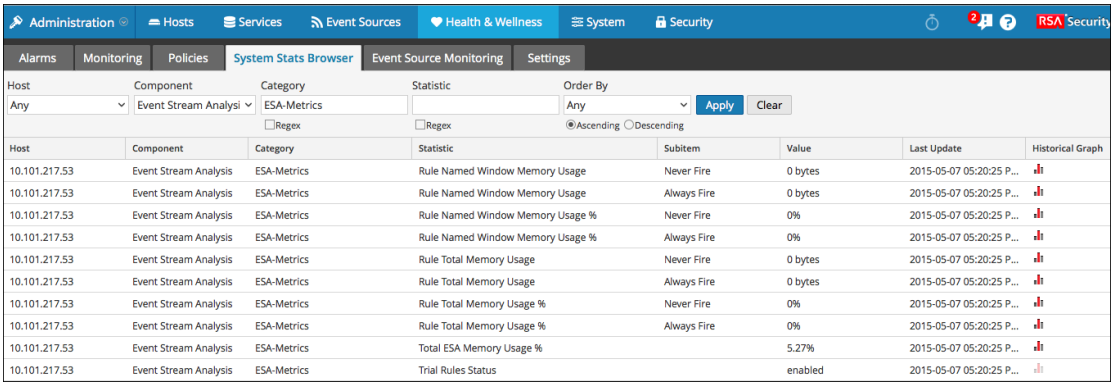
1. En el menú de **Security Analytics**, vaya a **Administration** > **Estado y condición** > **ESA** > **Monitoreo del sistema**.
2. Vea los detalles del servicio de ESA.
3. Seleccione **Reglas**.
4. Puede ver el uso promedio de la memoria de cada regla correspondiente a la hora anterior.



Ver métricas de memoria en el Navegador de estadísticas del sistema de Estado y condición

1. En el menú de **Security Analytics**, vaya a **Administration** > **Estado y condición** > **Navegador de estadísticas del sistema**.

2. Como componente, seleccione **Event Stream Analysis**. Como categoría, ingrese **ESA-Metrics**.



   El nombre de la regla se muestra en el campo **Subelemento** y el uso de la memoria, en la columna **Valor**.

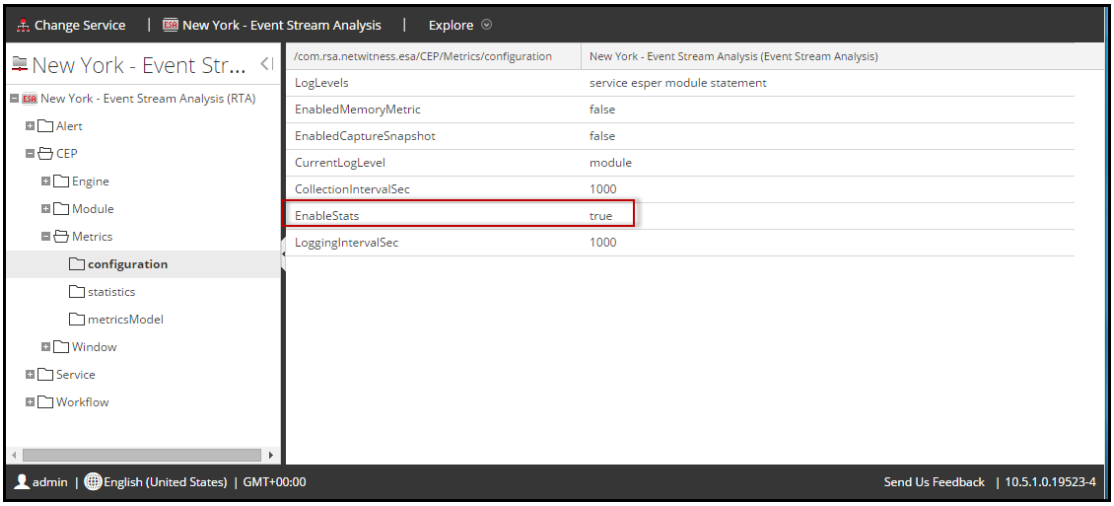
3. Para ver el uso histórico de memoria para la regla, haga clic en el ícono **Gráfico histórico**.

Nota: El campo **Última actualización** refleja el momento en que Estado y condición sondea a ESA. Sin embargo, las métricas de memoria no están sincronizadas con el sondeo de Estado y condición. Por ejemplo, si el umbral de la memoria se supera el 10/10/2015 a las 12:00 h, pero Estado y condición realiza un sondeo el 10/10/2015 a las 12:10 h, el campo **Última actualización** mostrará un registro de fecha y hora 10/10/2015 12:10 h.

Habilitar o deshabilitar la función de métricas de memoria

1. En el menú de **Security Analytics**, vaya a **Administration** > **Servicios** y seleccione su ESA.

2. Cuando haya seleccionado su ESA, haga clic en **Acciones** > **Ver** > **Explorar** y navegue a **Métricas de CEP** > **Configuración**, como se muestra a continuación.



3. Cambie el campo EnabledStats a **true** o **false** de acuerdo con su decisión de habilitar o deshabilitar la función de métricas de memoria.

Cómo ESA genera alertas

En este tema se proporciona una descripción breve de cómo un servicio Event Stream Analysis (ESA) ejecuta reglas para generar alertas. El servicio Security Analytics Event Stream Analysis (ESA) ejecuta reglas que especifican criterios para el comportamiento de problemas o los eventos amenazantes en la red. Cuando ESA detecta un incidente que coincide con los criterios de la regla, genera una alerta.

Para generar alertas, ESA ejecuta las siguientes funciones:

1. Recopila datos
2. Ejecuta reglas de ESA contra los datos
3. Captura eventos que cumplen los criterios de la regla
4. Genera alertas para esos eventos capturados

Puede usar el módulo Alerts para obtener visibilidad de la red y para detectar problemas que se producen en ella.

Datos confidenciales

En este tema se explica la forma en que ESA maneja los datos confidenciales, como nombres de usuario o dirección IP, que recibe de Security Analytics Core. La función Encargado de la privacidad de datos (DPO) puede identificar claves de metadatos que contienen datos confidenciales y que deben mostrar datos ocultos. ESA no mostrará ni almacenará metadatos confidenciales. Por lo tanto, ESA no transmitirá datos confidenciales a Incident Management.

De manera opcional, ESA puede agregar una versión oculta de los datos confidenciales a un evento. Por ejemplo, el DPO identifica user_dst como confidencial. ESA puede agregar una versión oculta, como user_dst_hash, a un evento. Los metadatos ocultos no son confidenciales, razón por la cual ESA los mostrará y los almacenará de la misma manera que otros metadatos no confidenciales.

Para obtener más información sobre la estrategia y los beneficios del ocultamiento de datos, consulte la **Guía de administración de la privacidad de datos de Security Analytics**.

En este tema se explica lo siguiente:

- Cómo ESA maneja los datos confidenciales que recibe de Security Analytics Core
- Cómo impedir filtraciones de datos confidenciales en una regla de EPL avanzado

Cómo ESA maneja datos confidenciales de Security Analytics Core

Cuando ESA recibe datos confidenciales de Security Analytics Core, solo transmite la versión oculta de los datos. ESA no almacena ni muestra datos confidenciales.

Las siguientes funciones se ven afectadas:

- Salidas: ESA no reenvía datos confidenciales a salidas, las cuales incluyen alertas, notificaciones y almacenamiento en MongoDB.
- Reglas de EPL avanzado: si una declaración de EPL crea un alias para una clave de metadatos confidenciales, los datos confidenciales se filtrarán. En este tema se ilustra cómo sucede esto de modo que pueda evitarlo.
- Enriquecimientos: si se usa una clave de metadatos confidenciales en la condición de combinación, los datos confidenciales se filtrarán. En este tema se ilustra cómo sucede esto de modo que pueda evitarlo.

Regla de EPL avanzado

Si una declaración de consulta de EPL cambia el nombre de una clave de metadatos confidenciales, los datos no se protegerán.

ESA identifica una clave de metadatos confidenciales por el nombre:

ip_src es la clave de metadatos confidenciales.
ip_src_hash es la versión oculta no confidencial.

Para ofrecer compatibilidad con la privacidad de datos, no se debe cambiar el nombre de la clave de metadatos confidenciales en una consulta EPL. Si se cambia el nombre de una clave de metadatos confidenciales, los datos ya no estarán protegidos.

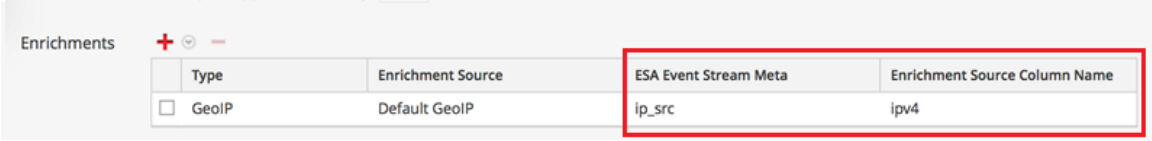
Por ejemplo, en una regla como select ip_src as ip_alias…, ip_alias contiene los datos confidenciales, pero no está protegido porque ESA solo tiene conocimiento de ip_src, no de ip_alias. En este caso, las direcciones IP no se ocultarían. Se mostrarían los valores reales.

Origen de enriquecimiento

Cuando se usa una clave de metadatos confidenciales en una condición de combinación, los datos confidenciales se pueden mostrar.

La base de datos de enriquecimiento, que es la otra parte de la condición de combinación, tiene una columna que coincide con la clave de metadatos confidenciales. Esta referencia cruzada es a valores reales y no a valores ocultos. Por lo tanto, se muestran valores reales.

En el siguiente ejemplo se resaltan ambas partes de la condición de combinación.



- ip_src contiene datos confidenciales.
- ipv4 se agregará a la alerta y se expondrá como datos no confidenciales

Debido a que el valor de ipv4 es igual que el valor de ip_src, ipv4 contiene y muestra datos confidenciales.

Tipos de reglas de ESA

En este tema se describe cada tipo de regla de ESA, cuándo se deben usar y los permisos que tiene cada función con ellos. En la siguiente tabla se enumera, se describe y se explica cuándo se debe usar cada tipo.

Tipo de regla	Descripción	Cuándo se debe usar
Generador de reglas	El generador de reglas permite definir los criterios de reglas en un interfaz fácil de usar.	Use el generador de reglas para crear sus primeras reglas. Muchas de las condiciones de las reglas se seleccionan en listas.
EPL avanzado	El lenguaje de procesamiento de eventos (EPL) permite definir criterios de reglas mediante la escritura de una consulta.	Use reglas de EPL avanzado para las cuales definirá criterios en la sintaxis de EPL.
ESA de RSA Live	RSA Live dispone de un catálogo de reglas de ESA que puede descargar y modificar para ejecutarlas en su red.	Descargue reglas de ESA de RSA Live para aprovechar reglas ya creadas. Modifique los parámetros configurables para personalizarlos de acuerdo con sus requisitos.

Reglas del paquete de inicio

Algunos ejemplos de reglas del generador de reglas vienen con Security Analytics y aparecen en la Biblioteca de reglas. Utilice reglas del paquete de inicio para acostumbrarse a trabajar con reglas antes de crear las propias. Puede editar e implementar con seguridad estos ejemplos de reglas.

Modo de reglas de prueba

Para cualquier tipo de regla, puede seleccionar la configuración Regla de prueba como resguardo adicional. Las reglas de prueba se inhabilitan si superan un umbral de la memoria que configura el administrador. Ejecute una regla en modo de prueba para monitorear el uso de la memoria e inhabilitarla automáticamente si usa más memoria de la que permite el umbral.

Permisos de funciones

Este tema se enumeran todos los permisos de ESA y se muestran los permisos que se asignan a cada función de Security Analytics preconfigurada. El acceso de los usuarios está restringido según las funciones y los permisos que se asignan a ellas.

- Administradores
- Operadores
- Analista
- Administradores del centro de operaciones de seguridad (SOC)
- Analistas de malware (MA)
- Encargado de la privacidad de datos

Hay cuatro permisos para ESA:

1. Acceder al módulo Alerting: se requiere para cualquier permiso
2. Ver reglas: otorga el permiso de solo visualización para las reglas en la Biblioteca de reglas
3. Ver alertas: otorga el permiso de solo visualización para las alertas que genera ESA
4. Administrar reglas: permite ver, crear, editar y eliminar reglas

En la siguiente tabla se enumeran los permisos para ESA y las funciones a las cuales están asignados. Use esta tabla para ver cómo cada función puede trabajar con reglas y alertas.

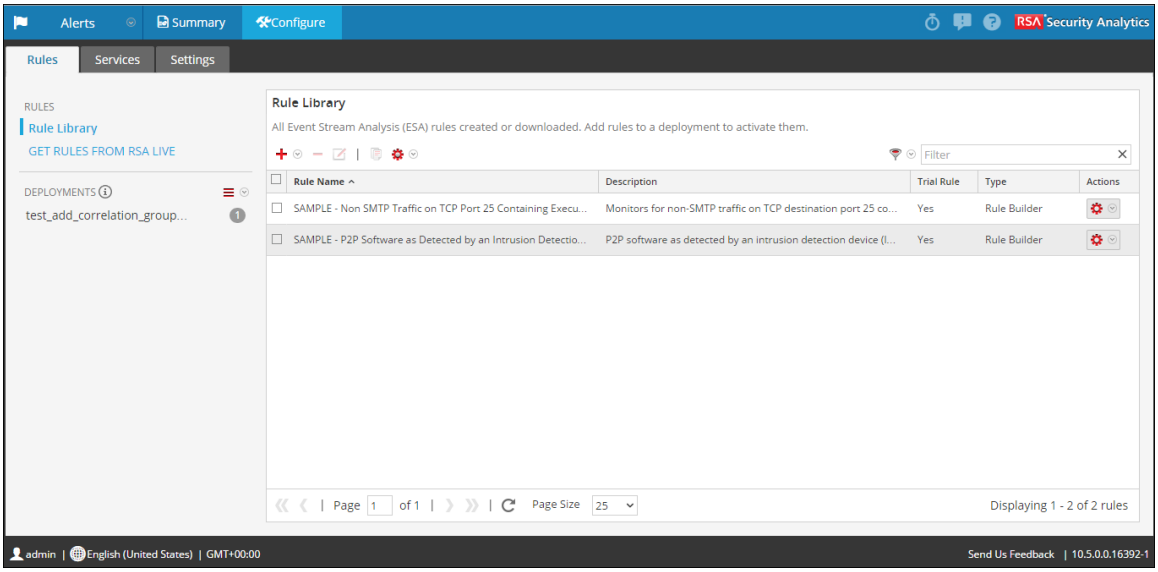
Permiso	Administradores	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceder al módulo Alerting	Sí	Sí	Sí	Sí		Sí
Ver reglas	Sí	Sí		Sí		Sí
Ver alertas	Sí		Sí	Sí		Sí
Administrar reglas	Sí	Sí		Sí		Sí

Para obtener más información sobre las funciones y los permisos, consulte la **Guía de administración de usuarios y seguridad del sistema**.

Práctica con reglas del paquete de inicio

Security Analytics incluye dos reglas del paquete de inicio que permiten a los analistas familiarizarse con la apariencia de las reglas antes de crear propias. Use las reglas del paquete de inicio para familiarizarse con el generador de reglas y practicar la edición y la implementación de una regla.

Las reglas del paquete de inicio están instaladas en la Biblioteca de reglas, la cual alojará todas las reglas que descargue o cree. En la siguiente figura se muestra la Biblioteca de reglas después de la instalación.



Estas son las reglas del paquete de inicio disponibles:

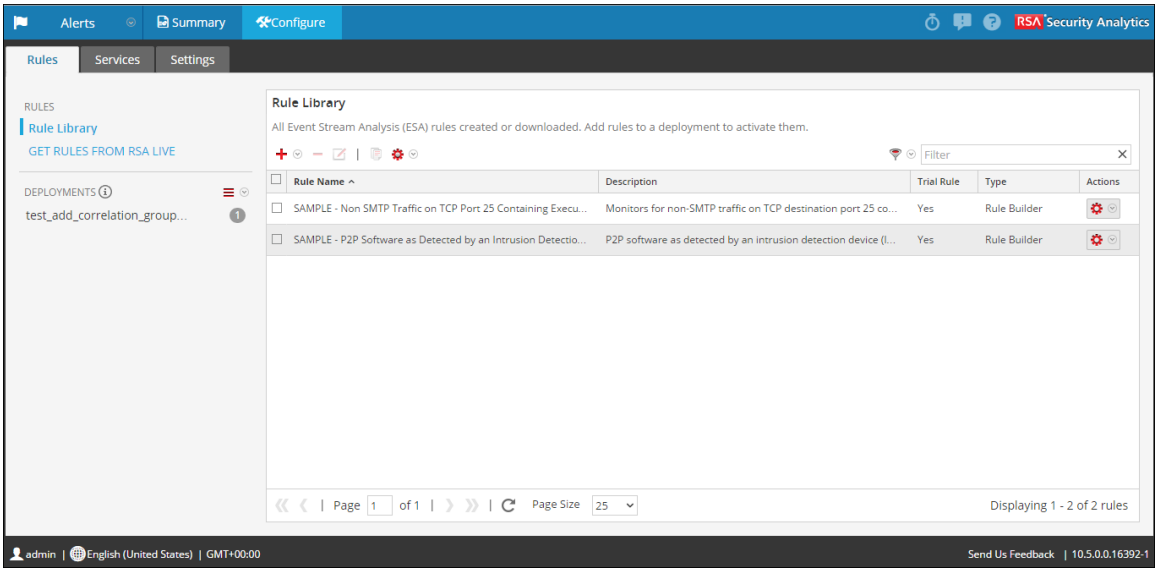
- SAMPLE: P2P Software as Detected by an Intrusion Detection Device
- SAMPLE: Non SMTP Traffic on TCP Port 25 Containing Executable
- SAMPLE: Whitelist - From outside of Germany, P2P Software as Detected by an Intrusion Detection Device.
- SAMPLE: Blacklist - From inside countries that are not the US, Non-SMTP Traffic on TCP Port 25 Containing Executable
- SAMPLE: User Added to Admin Group Same User su Sudo

Cada nombre comienza con SAMPLE para diferenciar las reglas que se instalan con Security Analytics de aquellas que se descargan y se crean.

Biblioteca de reglas

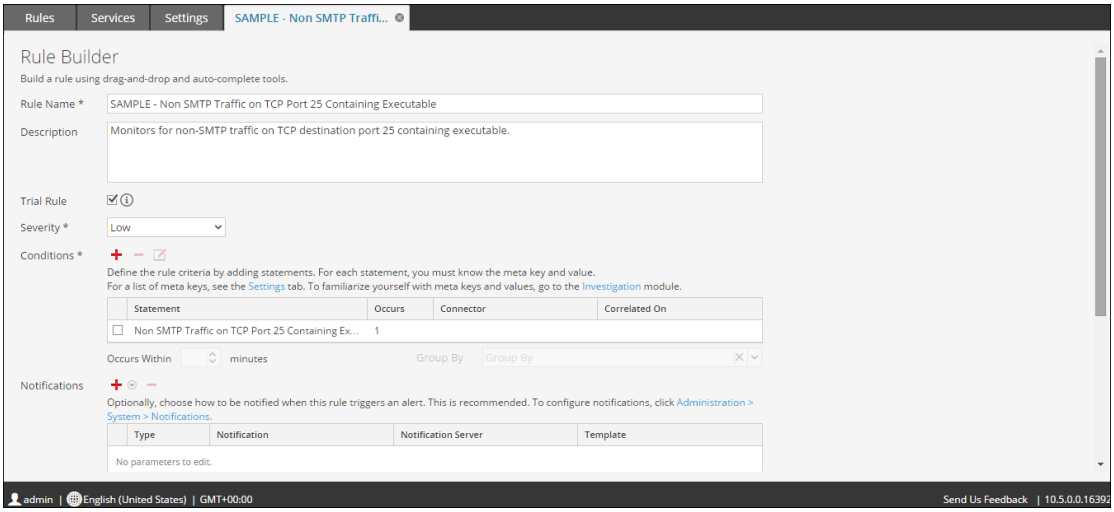
En la Biblioteca de reglas se muestra la siguiente información para una regla:

- **Nombre** resume los datos o los eventos que recopila la regla.
- **Descripción** explica la regla de manera más detallada, aunque solo se muestra el principio en la Biblioteca de reglas.
- **Regla de prueba** indica si el modo de prueba está habilitado o inhabilitado para la regla.
- **Tipo** muestra el origen de la regla, creada en el generador de reglas o EPL avanzado, o descargada desde RSA Live.



Procedimiento

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   La vista Configurar se muestra con la pestaña Reglas abierta.
2. En la **Biblioteca de reglas**, seleccione un ejemplo de regla y haga clic en  o haga doble clic en una regla.
   La regla se abre en el generador de reglas.



3. Para practicar con una regla del paquete de inicio, consulte los siguientes temas con el fin de obtener descripciones y procedimientos detallados:

   - Para familiarizarse con la interfaz del usuario del generador de reglas, consulte Pestaña Generador de reglas para obtener una descripción de cada campo.
   - Para aprender a editar una regla, consulte Agregar una regla del generador de reglas con el fin de obtener un procedimiento paso a paso.
   - Para implementar una regla del paquete de inicio, consulte Implementar reglas para ejecutar en ESA con el fin de aprender a asociar la regla a un servicio ESA.

Después de practicar con reglas del paquete de inicio, podrá descargar, crear e implementar reglas propias.

Trabajar con reglas de prueba

Cuando las reglas usan demasiada memoria, el servicio ESA puede ser lento o dejar de responder. Para asegurarse de que las reglas no usen una cantidad excesiva de memoria, puede habilitar reglas de prueba para cualquier tipo de regla. Cuando se crea una regla de prueba, se configura un umbral global del porcentaje de memoria que pueden usar las reglas. Si se supera ese umbral de la memoria configurado, todas las reglas de prueba se inhabilitan.

El servicio Security Analytics Event Stream Analysis (ESA) puede procesar grandes volúmenes de datos de eventos dispares desde Concentrators. Sin embargo, cuando trabaja con Event Stream Analysis, es posible crear reglas que usan una cantidad excesiva de memoria. Esto puede retrasar el servicio de ESA o incluso hacer que se apague de forma inesperada. Para asegurarse de que esto no suceda, puede configurar una regla como regla de prueba. Cuando se configura una regla de prueba, también se configura un umbral global del porcentaje de memoria que pueden usar las reglas. Si se supera ese umbral de la memoria configurado, todas las reglas de prueba se inhabilitan automáticamente.

Para obtener sugerencias sobre la creación de reglas más eficientes, consulte “Mejores prácticas para escribir reglas” en Mejores prácticas

Como mejor práctica, cuando agrega una nueva regla o edita una existente, seleccione la opción Regla de prueba que le permite:

- Implementar la regla con un resguardo adicional.
- Opcionalmente, ver un snapshot de la utilización de la memoria para comprender si la regla crea problemas relacionados con la memoria.
- Saber si debe modificar los criterios de la regla para mejorar el rendimiento.

Nota: ejecute una regla como regla de prueba bastante tiempo, de modo que pueda determinar el rendimiento durante el tráfico de red normal y máximo.

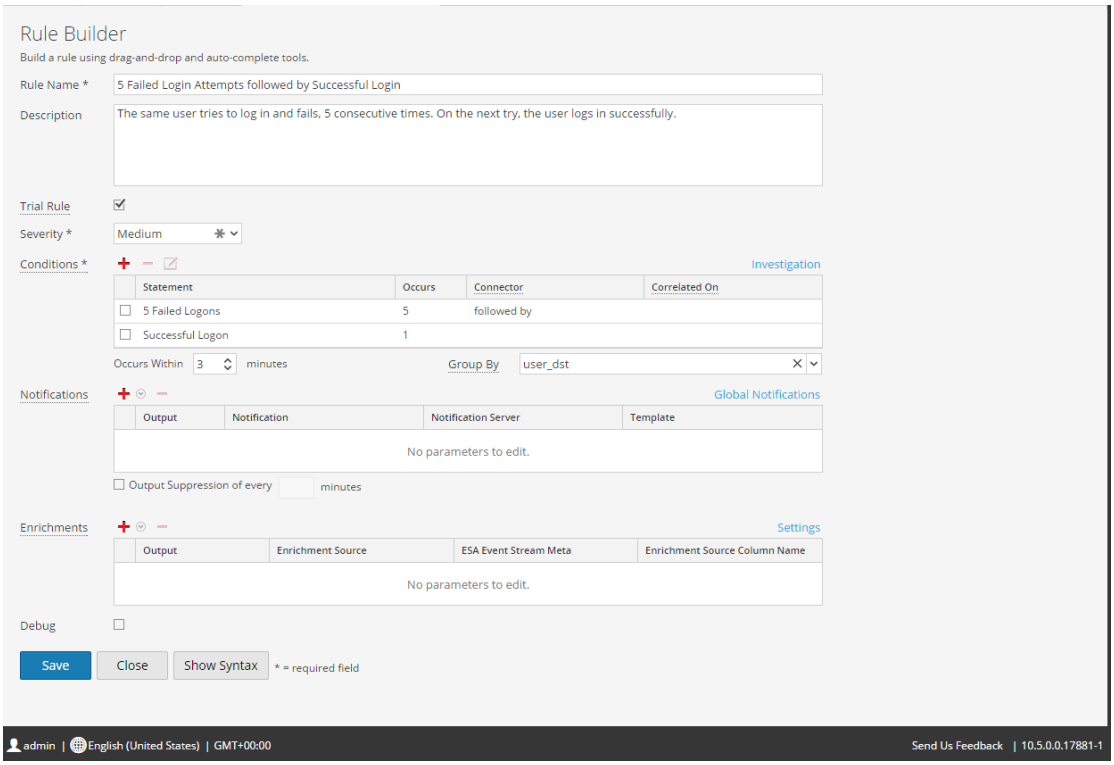
Implementar reglas como reglas de prueba

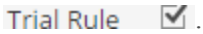
En este tema se explica a los administradores cómo habilitar reglas de prueba cuando se crean nuevas reglas o se editan reglas. Las reglas de prueba se inhabilitan automáticamente si se supera un umbral especificado de utilización total de la memoria de JVM.

Procedimiento

Para implementar reglas como reglas de prueba:

1. En el menú de **Security Analytics**, vaya a **Alertas** > **Configurar**.
   La vista Configurar se muestra con la pestaña Reglas abierta.
2. En la Biblioteca de reglas, elija la opción para agregar o editar una regla. El generador de reglas se muestra en una nueva pestaña de Security Analytics.



3. Para convertir una regla nueva o existente en una regla de prueba, seleccione 

.

4. Agregue las condiciones de la regla o modifique la regla según sea necesario. Para obtener instrucciones sobre cómo editar reglas, consulte Agregar reglas a la Biblioteca de reglas.
5. Haga clic en **Guardar**.
6. Compruebe que las reglas de prueba estén habilitadas para ESA y asegúrese de estar confirme con los umbrales configurados para las reglas de prueba.
   El umbral de memoria se establece en el archivo de configuración. Para configurarlo, consulte “Cambiar el umbral de memoria de las reglas de prueba” en la **Guía de configuración de ESA**.
   El umbral se configura por ESA y es un porcentaje de la memoria virtual de Java.

El valor predeterminado del parámetro de configuración MemoryThresholdforTrialRules es 85.

7. De manera opcional, puede configurar políticas en Estado y condición de modo que se envíe una notificación por correo electrónico si se supera el umbral de utilización total de la memoria de JVM.

La próxima vez que implementa la regla, se ejecuta en modo de regla de prueba.

Nota: Si una regla de prueba está deshabilitada, debe ir a la pestaña **Alertas** > **Configurar** > **Servicios** para volver a habilitarla. Para obtener más instrucciones sobre cómo volver a habilitar reglas de prueba en un servicio, consulte Ver estadísticas y alertas de ESA.

Ver métricas de memoria para reglas mediante el modo de prueba

En este tema se explica a los escritores de reglas de ESA cómo ver las métricas de memoria cuando se supera el umbral de la memoria configurado para las reglas de prueba. Si se supera el umbral de la memoria, puede configurar la toma de una instantánea del uso de la memoria para las reglas de ESA en el momento en que las reglas de prueba están deshabilitadas, lo cual permite investigar el uso de la memoria y editar las reglas para que sean más eficientes.

Cuando configura reglas de prueba y habilita la función Snapshot de la memoria, si se supera el umbral de la memoria, se inhabilitan todas las reglas de prueba y se toma un snapshot del uso de la memoria para todas las reglas de ESA en el momento en que las reglas están inhabilitadas. Esto permite ver cuánta memoria se usó y también permite modificar las reglas de ESA de modo que sean más eficientes. El snapshot de la memoria se puede ver en el Navegador de estadísticas del sistema de Estado y condición, lo cual hará necesario disponer de permisos para acceder este módulo. Una vez que consulta los detalles en el Navegador de estadísticas del sistema, puede modificar la sintaxis de las reglas de prueba y volver a habilitarlas.

En general, tendrá que realizar los siguientes pasos para usar el snapshot de la memoria con el fin de solucionar problemas relacionados con el uso de la memoria para las reglas:

1. Habilite reglas de prueba para cualquier regla nueva que implemente. Consulte Implementar reglas como reglas de prueba.
2. Asegúrese de haber configurado políticas de ESA de Estado y condición para enviar un correo electrónico si se superan los umbrales de la memoria.
3. Asegúrese de disponer de los permisos correctos para ver el módulo Estado y condición. Para obtener información sobre las funciones y los permisos, consulte Permisos de funciones.

4. Asegúrese de que la función Snapshot de la memoria esté habilitada (mediante el parámetro EnabledCaptureSnapshot en el Explorador de SA). La función Instantánea de la memoria está deshabilitada de forma predeterminada. Consulte “Habilitación y deshabilitación de la función Instantánea de la memoria” a continuación. RSA recomienda inhabilitar la función cuando se haya terminado de probar las reglas nuevas.
5. Si el umbral de la memoria se activa para las reglas de prueba, vea las estadísticas del umbral en Estado y condición.
6. Modifique la o las reglas que activaron la alarma. Para revisar mejores prácticas relacionadas con la escritura de reglas, consulte Mejores prácticas.
7. Vuelva a habilitar las reglas de prueba que se deshabilitaron cuando se activó el umbral de la memoria. Para obtener instrucciones sobre la rehabilitación de las reglas de prueba en un servicio, consulte Ver estadísticas y alertas de ESA.
8. Continúe probando las reglas de prueba.

Nota: Como sucede con cualquier herramienta de depuración, puede haber una sobrecarga excepcional asociada al uso de la función Snapshot de la memoria. Cuando se toma activamente un snapshot, la función Snapshot de la memoria puede implicar demoras en los servicios de ESA. El servicio ESA deja de generar alertas mientras se toma una instantánea. RSA recomienda deshabilitar la función una vez que haya terminado de probar las reglas nuevas. Si deshabilita la función Snapshot de la memoria, las reglas de prueba continuarán deshabilitadas cuando el uso de la memoria supere los umbrales configurados, pero el snapshot de la memoria no se tomará y las estadísticas no aparecerán en el Navegador de estadísticas del sistema de Estado y condición.

Requisitos previos

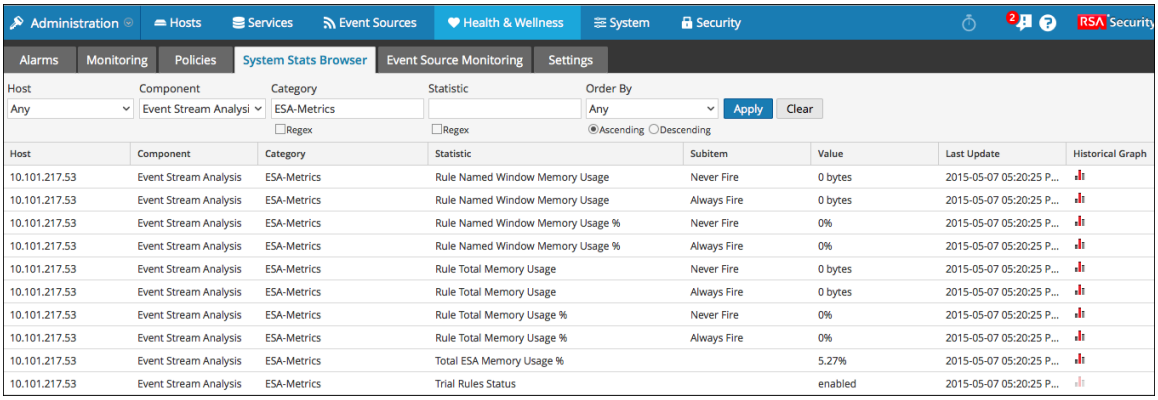
Estos son los requisitos para la visualización de métricas de memoria:

- Se debe configurar una o más reglas de ESA como una regla de prueba.
- La función Snapshot de la memoria debe estar habilitada (mediante el parámetro EnabledCaptureSnapshot en el Explorador de SA).
- El usuario debe tener los permisos apropiados para ver estadísticas de Estado y condición.
- El usuario debe haber configurado la política de ESA de Estado y condición para enviar un correo electrónico si se superan los umbrales de la memoria.

Procedimientos

Ver métricas de memoria

1. En el menú de **Security Analytics**, vaya a **Administration** > **Estado y condición** > **Navegador de estadísticas del sistema**.
2. Como componente, seleccione **Event Stream Analysis**. Como categoría, ingrese **ESA-Metrics**.

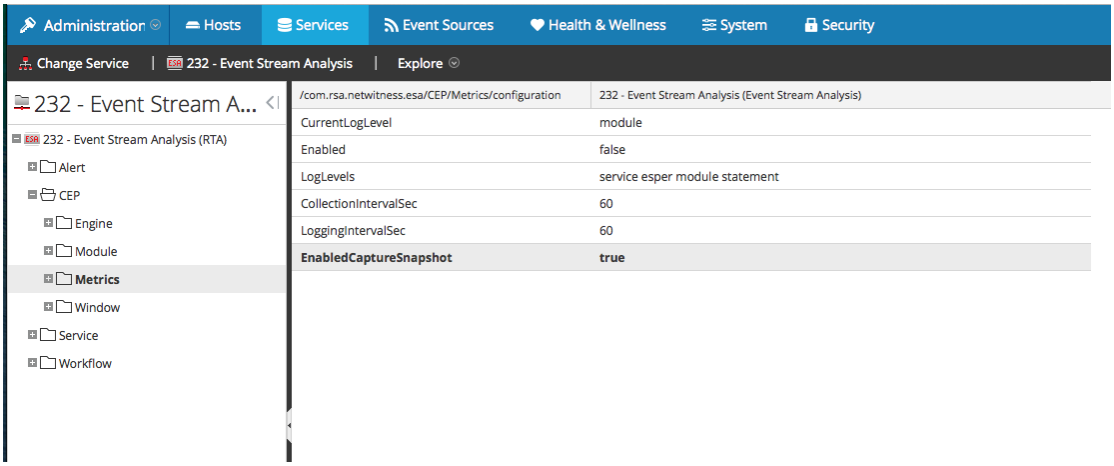


El nombre de la regla se muestra en el campo **Subelemento** y el uso de la memoria, en la columna **Valor**.

Nota: El campo **Última actualización** refleja el momento en que Estado y condición sondea a ESA. Sin embargo, el snapshot de la memoria solo ocurre cuando se superan los umbrales de la memoria, razón por la cual este campo no refleja cuándo se tomó o se actualizó el snapshot. El snapshot permanece estático hasta que se vuelve a superar el umbral de la memoria. Por ejemplo, si el umbral de la memoria se supera el 10/10/2015 a las 12:00 h, pero Estado y condición realiza un sondeo el 10/10/2015 a las 15:00 h, el campo **Última actualización** mostrará la fecha 10/10/2015 15:00 h.

Habilitar o inhabilitar la función Snapshot de la memoria

1. En el menú de **Security Analytics**, vaya a **Administration** > **Servicios** y seleccione su ESA.
2. Cuando haya seleccionado un ESA, haga clic en **Acciones** > **Ver** > **Explorar** y navegue a Métricas de CEP, como se muestra a continuación.



3. Cambie el campo EnabledCaptureSnapshot a **true** o **false** de acuerdo con su decisión de habilitar o inhabilitar la función Snapshot de la memoria.

Agregar reglas a la Biblioteca de reglas

En este tema se explica cómo agregar cada tipo de regla a la Biblioteca de reglas. Debe agregar una regla a la Biblioteca de reglas antes de que pueda implementarla. El permiso para administrar reglas se requiere para todas las tareas de esta sección. Para agregar reglas, puede descargarlas desde ESA Live, crear una regla mediante el generador de reglas o escribir reglas de EPL avanzado.

Para obtener más detalles sobre cada uno de estos procedimientos, consulte:

- Descargar reglas de ESA de RSA Live configurables
- Agregar una regla del generador de reglas
- Agregar una regla de EPL avanzado

Además de la implementación de una regla, la Biblioteca de reglas permite editar, duplicar, importar, exportar y eliminar una regla. Para obtener detalles sobre estos procedimientos, consulte Trabajo con reglasTrabajo con reglas

Descargar reglas de ESA de RSA Live configurables

En este tema se explica cómo descargar reglas configurables desde el sistema de administración de contenido de Security Analytics Live de modo que pueda personalizarlas para satisfacer sus necesidades.

RSA Live contiene un catálogo de reglas. Cada regla tiene parámetros configurables que permiten personalizarla para un ambiente. Si RSA Live tiene una regla para detectar eventos que desea monitorear en la red, descárguela para ahorrar tiempo. Puede editar los parámetros configurables y guardar la regla en la Biblioteca de reglas.

Este es un ejemplo de cómo se describe cada regla de ESA de RSA Live en RSA Live:

Nombre de la regla	Descripción
Inicios de sesión en varios servidores	Detecta inicios de sesión del mismo usuario en tres o más servidores por separado en un periodo de cinco minutos. La ventana de tiempo y la cantidad de destinos únicos son configurables.

Como indica el nombre, la regla busca inicios de sesión en varios servidores. La descripción explica los criterios de la regla de forma más detallada y especifica los parámetros que se modifican.

Nota: Cuando una descripción de regla incluye un parámetro configurable, se usa la configuración predeterminada para el parámetro. En el ejemplo de la regla, la descripción establece cinco minutos. Sin embargo, la ventana de tiempo es configurable, de modo que cinco es la cantidad predeterminada de minutos.

Requisitos previos

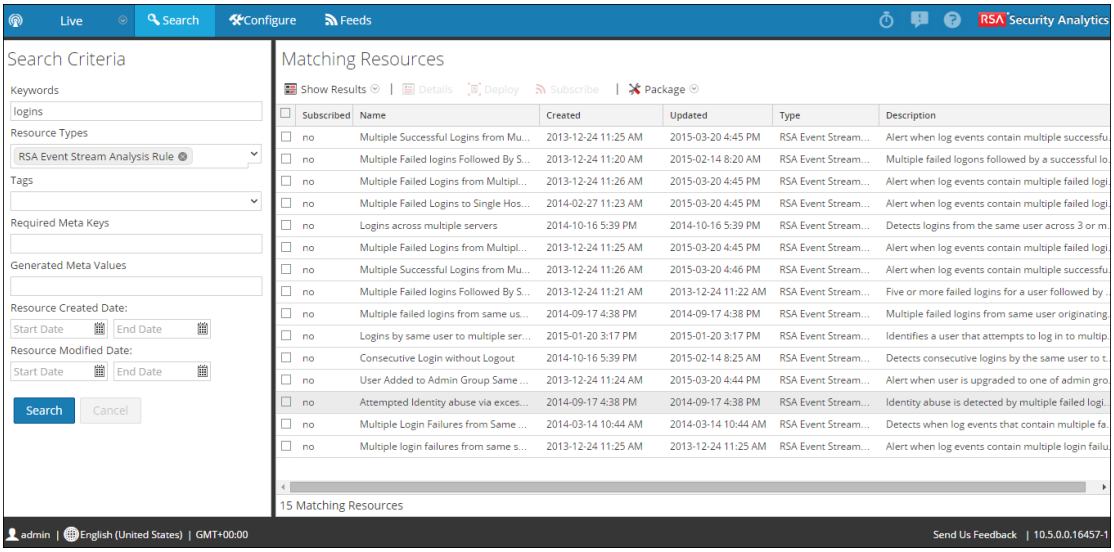
Estos son los requisitos previos para la descarga de las reglas de ESA de RSA Live configurables:

- Tener permiso para administrar reglas
- Crear una cuenta de Live. Consulte la **Guía de administración de servicios de Live** para obtener detalles.
- Configurar Live en Security Analytics. Consulte la **Guía de administración de servicios de Live** para obtener detalles.

Procedimiento

Para descargar reglas de ESA de RSA Live configurables:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   Se muestra la pestaña Reglas.
2. En el panel de opciones, haga clic en **Obtener reglas de RSA Live**.
   Se muestra la pestaña Buscar.



3. En **Criterios de búsqueda**, para **Tipo de recurso**, seleccione **Regla de RSA Event Stream Analysis**.
4. Especifique cualquiera de los siguientes criterios para buscar una regla y configurarla para el ambiente.

   Para obtener una descripción detallada de los criterios de búsqueda, consulte "Vista Buscar en Live" en la **Guía de administración de servicios de Live**.

   a. Palabras clave
   b. Etiquetas
   c. Claves de metadatos requeridas
   d. Valores de metadatos generados
   e. Fecha de creación de recurso
   f. Fecha de modificación de recurso
5. Haga clic en **Buscar**. Las reglas que coinciden con los criterios de búsqueda se muestran en Coincidencias de recursos.
6. Seleccione cada regla que desee descargar y haga clic en **Implementar**.

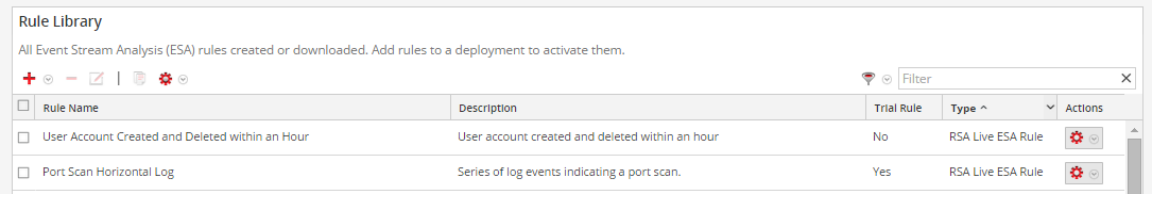
   Se muestra el Asistente de implementación
7. Siga los pasos del asistente. Si necesita obtener más información, consulte "Implementar recursos en Live" en la **Guía de administración de servicios de Live**.

Cuando completa los pasos del asistente, las reglas seleccionadas se muestran en la Biblioteca de reglas.

Personalizar una regla de ESA de RSA Live

En este tema se explica cómo configurar parámetros en una regla de ESA de RSA Live. Cuando descarga una regla de ESA de RSA Live, esta aparece en la Biblioteca de reglas, la cual incluye las siguientes columnas:

- Nombre
- Descripción
- Regla de prueba
- Tipo



El tipo es Regla de ESA de RSA Live.

Requisitos previos

- Se requieren los permisos de función administrador, operador, administrador del SOC o DPO.
- Las reglas se deben descargar a la Biblioteca de reglas.

Procedimiento

Para personalizar una regla de ESA de RSA Live:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Regla**.
2. En la **Biblioteca de reglas**, seleccione una regla de ESA de RSA Live y haga clic en .
   Se muestra la pestaña Regla de ESA de RSA Live.
3. (Opcional) Cambie los siguientes campos:

- Nombre de la regla
- Descripción
- Regla de prueba
- Gravedad

4. Para configurar la regla para el ambiente, reemplace el valor predeterminado de la columna **Valor** en la sección **Parámetros**.

5. Haga clic en **Guardar**

Agregar una regla del generador de reglas

En este tema se presenta un conjunto de procedimientos de punto a punto para agregar una regla del tipo generador de reglas.

Cada regla de ESA está diseñada para detectar algo en la red y para generar una alerta sobre lo que se detectó:

- Actividad de los usuarios no permitida, como el intento de descargar software que no está autorizado
- Comportamiento sospechoso, como el borrado masivo de auditorías
- Amenazas maliciosas conocidas, como la propagación de gusanos o una herramienta de modificación ilegal de contraseñas

Hay dos métodos para diseñar una regla en ESA:

- El generador de reglas es una interfaz fácil de usar. Se proporciona una clave de metadatos y un valor y después se seleccionan opciones de listas para completar los criterios.
- El EPL avanzado permite escribir consultas en el lenguaje de procesamiento de eventos. Debe conocer la sintaxis del EPL.

Si conoce el EPL, puede usar cualquiera de los métodos. Si no conoce el EPL, debe usar el generador de reglas. En estos temas se explica el generador de reglas.

Paso 1. Asignar un nombre a la regla y describirla

En este tema se proporcionan instrucciones para identificar una regla, indicar si es una regla de prueba y asignar un nivel de gravedad. Cuando agrega una nueva regla, la primera información que se debe proporcionar es un nombre único y una descripción de lo que detecta la regla. Una vez que se guarda la regla, esta información se muestra en la Biblioteca de reglas.

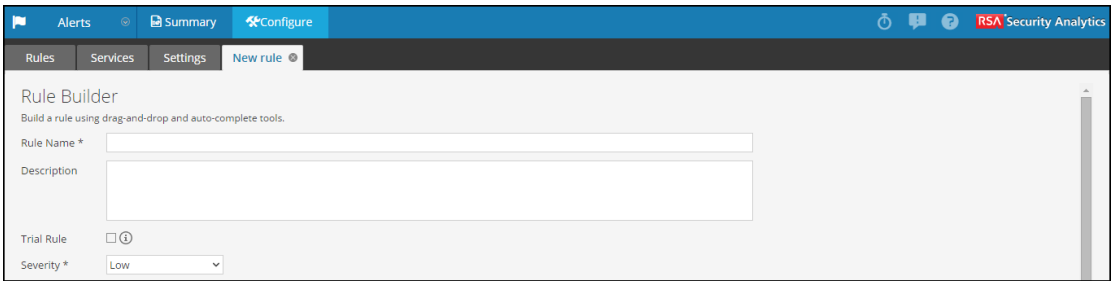
Requisitos previos

Debe tener permiso para administrar reglas. Consulte Permisos de funciones.

Procedimiento

Para ingresar un nombre y una descripción de una regla:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Regla**.
2. En la **Biblioteca de reglas**, seleccione  **> Generador de reglas**.
   Se muestra la pestaña Nueva regla.



3. Escriba un nombre descriptivo único en el campo **Nombre de la regla**.
   Este nombre aparecerá en la Biblioteca de reglas, por lo cual debe ser muy específico para diferenciar esta regla de las demás.
4. En el campo **Descripción**, explique los eventos que detecta la regla.
   El principio de esta descripción aparecerá en la Biblioteca de reglas
5. Seleccione **Regla de prueba** para deshabilitar automáticamente la regla si todas las reglas de prueba superan en conjunto el umbral de la memoria.
   Use el modo de regla de prueba como resguardo para ver si una regla se ejecuta eficientemente e impedir que se produzca tiempo fuera debido a la falta de memoria. Para obtener más información, consulte Trabajar con reglas de prueba.
6. En **Severidad**, clasifique la regla como Baja, Media, Alta o Crítico.

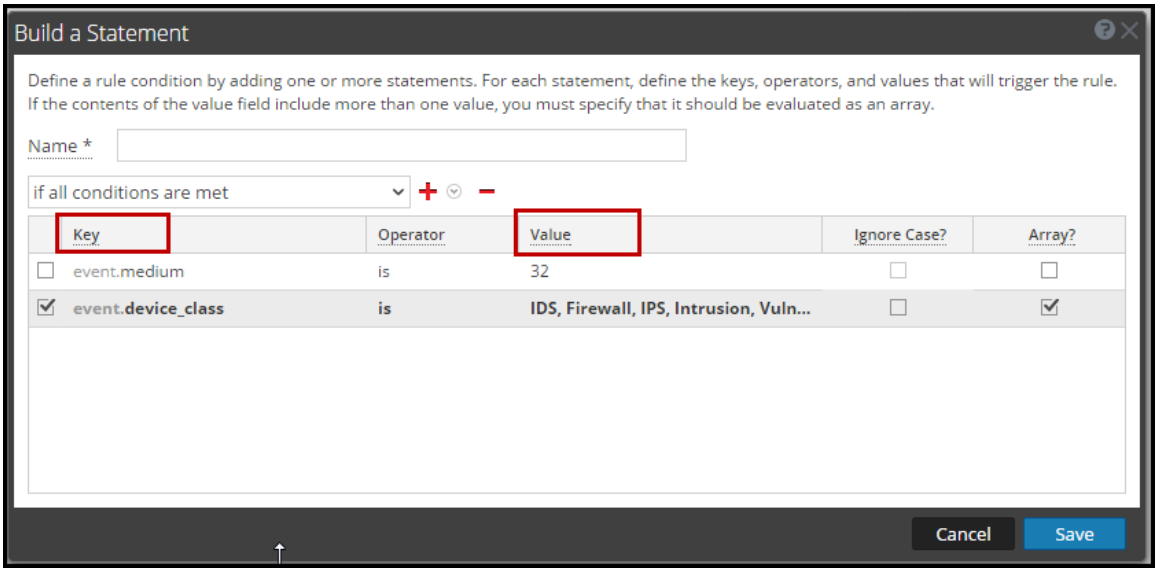
Paso 2. Crear una declaración de regla

En este tema se proporcionan instrucciones para definir criterios de regla en el generador de reglas mediante la adición de declaraciones. Una declaración es una agrupación lógica de criterios de regla en el generador de reglas. Las declaraciones se agregan para definir lo que detecta una regla.

Ejemplo

En el siguiente gráfico se muestra un ejemplo de una declaración del generador de reglas.

Cada declaración contiene una clave y un valor. A continuación se crea la lógica en torno al par mediante la selección de una opción en cada uno de los campos.



Requisitos previos

Para crear una declaración de regla, debe conocer la clave de metadatos y el valor de metadatos.
Para obtener una lista completa de claves de metadatos, vaya a **Alertas > Configurar > Ajustes de configuración > Referencias de claves de metadatos**.

Procedimiento

Para crear una declaración de regla:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.

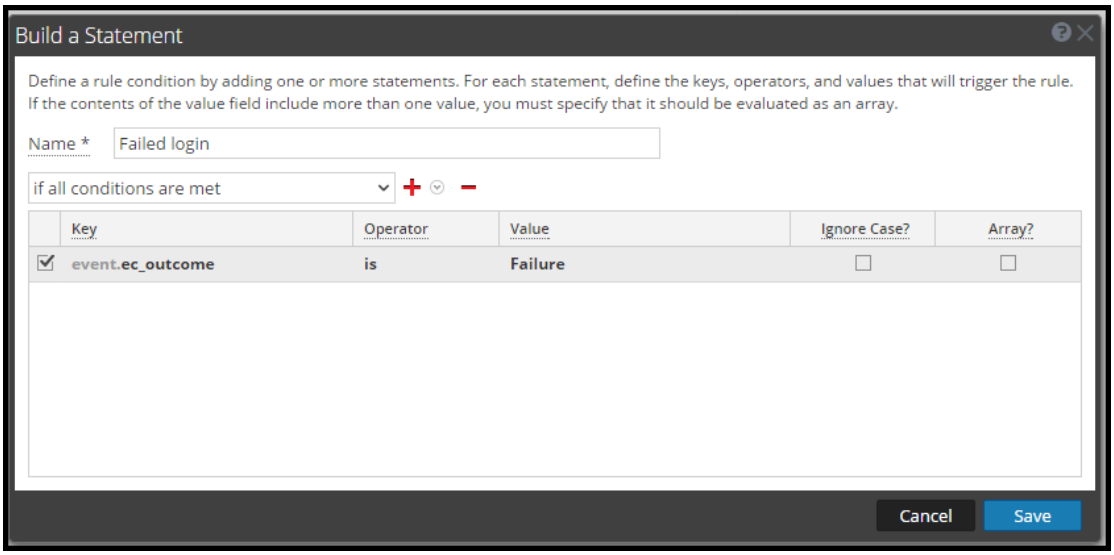
   La pestaña Reglas se muestra de manera predeterminada.

2. En la **Biblioteca de reglas**, haga clic en + **> Generador de reglas** o edite una regla del generador de reglas existente.

   Se muestra la vista Generador de reglas.

3. En la sección **Condiciones**, haga clic en +.

   Se muestra el cuadro de diálogo Crear declaración.



4. Dé un **Nombre** a la declaración. Sea claro y específico. El nombre de la declaración aparecerá en el generador de reglas.
5. En la lista desplegable, seleccione las circunstancias que requiere la regla:
   - si se cumplen **todas las condiciones**
   - si se cumple **una de estas condiciones**
6. Especifique los criterios para la declaración:
   a. En **Clave**, escriba el nombre de la **Clave de metadatos**.
   b. En **Operador**, especifique la relación entre la clave de metadatos y el valor que proporcionará para ella.
   Las opciones son: es, no es, no es nulo, es mayor que (>), es mayor o igual que (>=), es menor que (<), es menor o igual que (<=), contiene, no contiene, comienza con y termina con
   c. Escriba el **Valor** para la clave de metadatos.
   No escriba el valor entre comillas. Separe varios valores con una coma.
   d. El campo **¿Omitir mayúsculas y minúsculas?** está diseñado para su uso con valores de cadenas y matrices de cadenas. Cuando se selecciona el campo **Omitir mayúsculas y minúsculas**, la consulta trata todo el texto de la cadena como un valor en minúscula. Esto garantiza la activación de una regla que busca el nombre de usuario Johnson si el evento contiene “johnson”, “JOHNSON” o “JoHnSoN”.
   e. El campo **¿Arreglo?** indica si el contenido del campo Valor representa un valor o más.

Seleccione la casilla de verificación Arreglo si ingresó varios valores separados por comas en el campo **Valor**. Por ejemplo, "ec_activity is Logon, Logoff" requiere que se seleccione la casilla de verificación Arreglo.

7. Para usar otra clave de metadatos en la declaración, haga clic en +, seleccione **Agregar condición de metadatos** y repita el paso 6.
8. Para agregar una lista blanca, haga clic en + y seleccione **Agregar condición de lista blanca**.
9. Para agregar una lista negra, haga clic en + y seleccione **Agregar condición de lista negra**.
10. Para guardar la declaración, haga clic en **Guardar**.

Para agregar una lista blanca

Utilice una lista blanca para asegurarse de que los eventos especificados se excluyan de la activación de la regla. Las listas blancas se pueden basar en la ubicación geográfica o en orígenes de CSV de enriquecimiento definidos por el cliente. Por ejemplo, si desea crear una regla que solo se active para direcciones IP fuera de los Estados Unidos, puede crear una lista blanca de direcciones IP de los Estados Unidos.

1. Después de agregar una condición de metadatos, haga clic en + y seleccione **Agregar condición de lista blanca**.
2. En el campo **Ingresar nombre de lista blanca**, seleccione un origen de enriquecimiento. Cualquier origen de enriquecimiento cargado a partir de un CSV o de una ventana con nombre en Esper puede utilizarse como origen para una lista blanca.
3. Si usó un origen de GeoIP para la lista blanca, ipv4 se ingresa automáticamente para la subcondición. Ingrese el valor de metadatos para el campo de valor correspondiente. Por ejemplo, ingrese *ipv4 is ip_src* para asegurarse de que los registros de GeoIP se seleccionen en función del ip_src que se encuentra en la base de datos de búsqueda de GeoIP. Además, si utilizó un origen de GeoIP para la lista blanca, es posible que desee agregar una subcondición para especificar la región geográfica que desea excluir de los resultados de la regla. Por ejemplo, para especificar que el código de país debe ser USA, escriba "*CountryCode is US*".

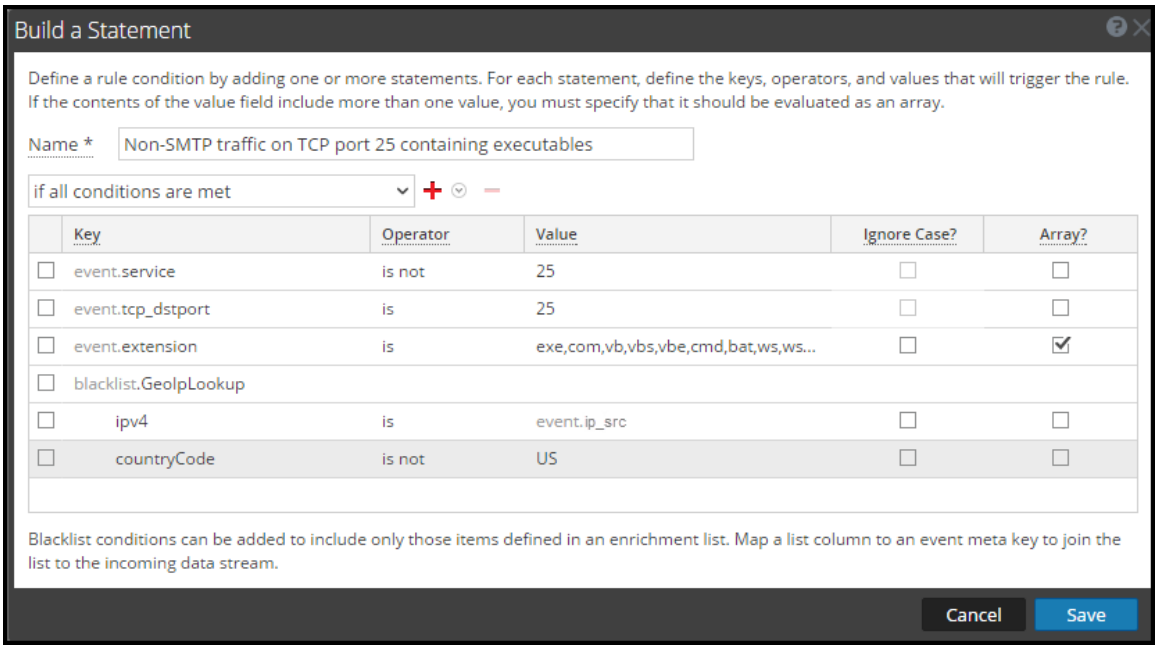
Para agregar una lista negra

Utilice una lista negra para asegurarse de que los eventos especificados activen la regla. Las listas negras se pueden basar en la ubicación geográfica o en orígenes CSV de enriquecimiento definidos por el cliente. Por ejemplo, puede especificar que la regla solo incluya los resultados de Alemania.

1. Después de agregar una condición de metadatos, haga clic en + y seleccione **Agregar condición de lista negra**.
2. En el campo **Ingresar nombre de lista negra**, seleccione un origen de enriquecimiento. Cualquier origen de enriquecimiento cargado a partir de un CSV o de una ventana con nombre en Esper puede utilizarse como origen para una lista negra.
3. Si usó un origen de GeoIP para la lista negra, ipv4 se ingresa automáticamente para la subcondición. Ingrese el valor de metadatos para el campo de valor correspondiente. Por ejemplo, ingrese ipv4 is ip_src para asegurarse de que los registros de GeoIP se seleccionen en función del ip_src que se encuentra en la base de datos de búsqueda de GeoIP. Además, si utilizó un origen de GeoIP para la lista negra, es posible que desee agregar una subcondición para especificar la región geográfica que desea incluir en los resultados de la regla. Por ejemplo, para especificar que la regla solo incluya los resultados para Alemania, ingrese "*CountryCode is DE*".

Ejemplo: Lista negra

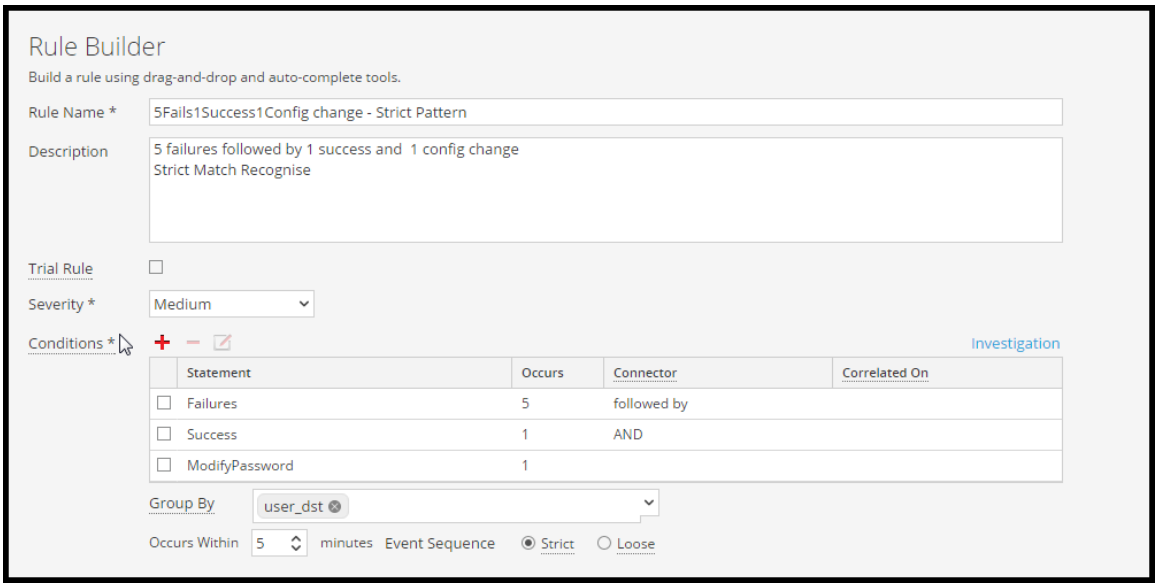
A continuación se muestra una declaración de lista negra para una regla que monitorea tráfico no SMTP en el puerto de destino TCP 25 que contiene un archivo ejecutable de países que se encuentran fuera de los Estados Unidos.



Declaración	Descripción
el servicio no es 25	El tráfico no es SMTP.
tcp_dstport es 25	El tráfico se ejecuta en el puerto TCP 25.
la extensión es exe, com, vb, vbs, vbe, cmd, bat, ws, wsf, src, sh	La extensión del archivo es un archivo ejecutable.
GeoIpLookup	La lista negra se basa en un origen GeoIPLookup.
ipv4 is ip_src	Los registros de GeoIP se seleccionan en función del ip_src que se encuentra en la base de datos de búsqueda de GeoIP.
el código de país no es US	Cuando se busca la dirección IP Event.ip_src en la base de datos de GeoIP, el registro que se devuelve no contiene “US” en el campo countryCode.

Ejemplo: Omisión de mayúsculas y minúsculas, coincidencia estricta de patrones y uso del operador *No es nulo*

En el siguiente ejemplo se utiliza la capacidad de omitir mayúsculas y minúsculas, excluir valores nulos y crear una coincidencia estricta de patrones para asegurarse de que se devuelvan los resultados esperados de la regla. La regla se compone de las siguientes condiciones:

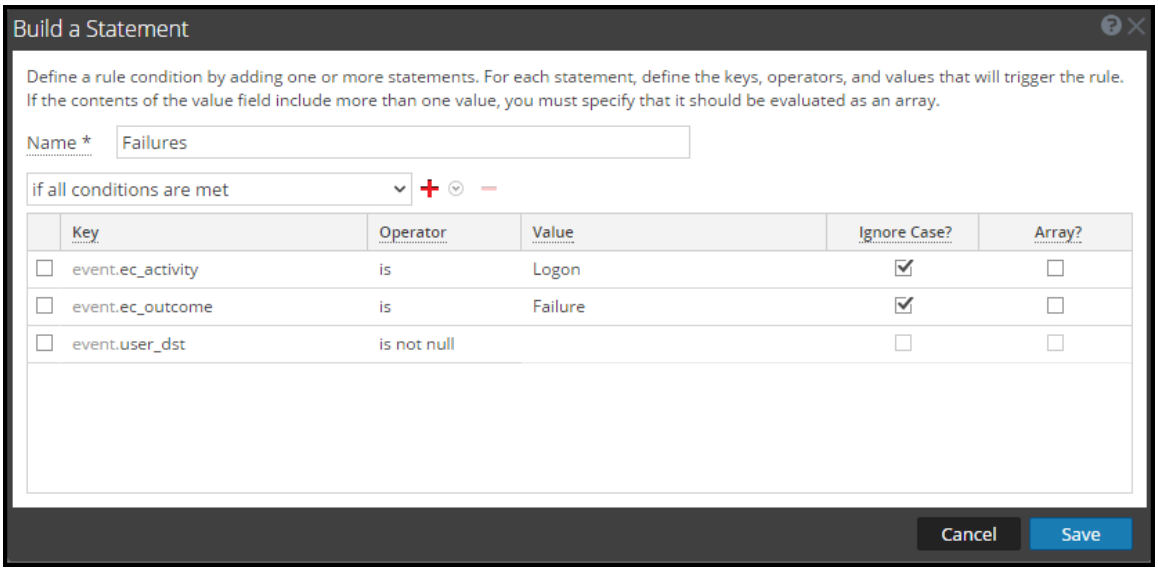


Condición de la regla	Descripción
Fallas	Esta condición busca cinco inicios de sesión fallidos con un conector “seguido de”, lo que significa que a la condición (Fallas) le debe seguir la siguiente condición (Satisfactorio).
Satisfactorio	Esta condición busca un inicio de sesión satisfactorio.
Modificar contraseña	Esta condición busca una instancia donde se modifica la contraseña.

Condición de la regla	Descripción
Agrupar por: user_dst	El campo Agrupar por garantiza que todas las condiciones anteriores se agrupen por los metadatos user_dst (la cuenta de destino del usuario). Esto es importante para la construcción de la regla porque la regla intenta encontrar un caso donde un usuario intentó iniciar sesión en la misma cuenta de destino varias veces, finalmente inició sesión correctamente y, a continuación, cambió la contraseña. La regla puede dar resultados inesperados si no se agrupa por la cuenta de usuario de destino.
Ocurre dentro de 5 minutos	La ventana de tiempo para que se produzcan los eventos es cinco minutos. Si se producen los eventos fuera de esta ventana de tiempo, la regla no se activa.
Secuencia de eventos: Strict	La secuencia de eventos está configurada para una coincidencia estricta de patrones. Esto significa que el patrón debe coincidir exactamente como se especifica, sin eventos intermedios. La coincidencia estricta de patrones le permite asegurarse de que el motor de Esper solo genera alertas para las reglas que coincidan exactamente con el patrón que desea buscar. Por ejemplo, es posible que una regla común busque cinco inicios de sesión fallidos seguidos de un inicio de sesión correcto. Si selecciona a una coincidencia flexible de patrones, esta regla se activará si hay una cantidad cualquiera de inicios de sesión correctos entre los inicios de sesión fallidos. Dado que el punto de la regla es encontrar intentos de inicio de sesión frecuentes *y* secuenciales, se requiere una coincidencia estricta para asegurarse de obtener los resultados que se esperan.

Nota: Cada una de estas condiciones se explica más detalladamente en las secciones siguientes.

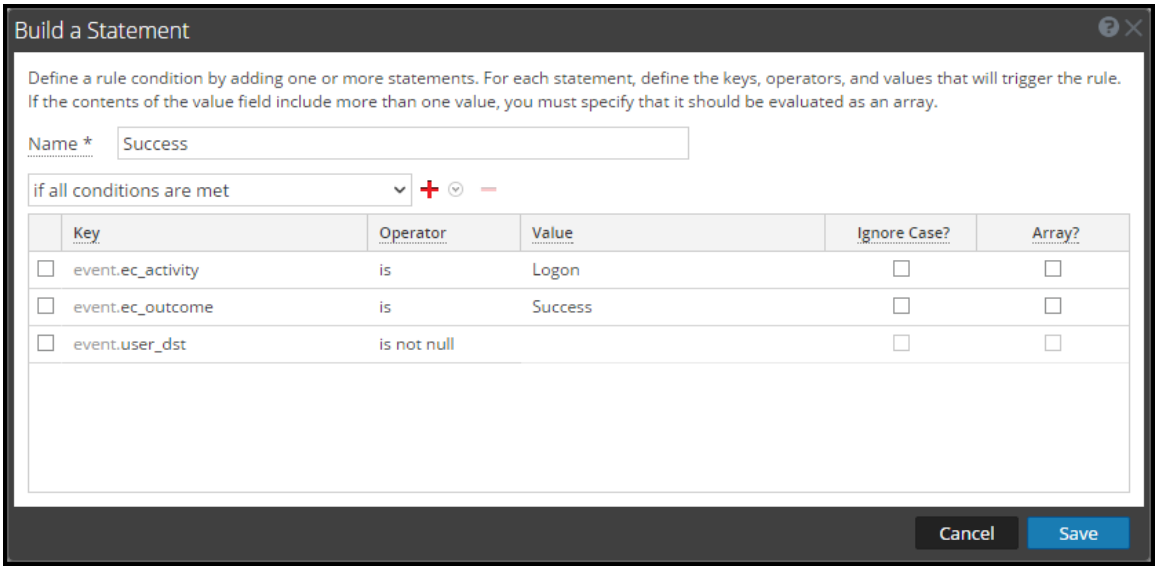
Para cada condición, se crea una declaración en el generador de reglas. La siguiente declaración compone la condición de fallas:



Declaración de regla	Descripción
ec-activity es inicio de sesión (omitir mayúsculas y minúsculas)	Identifica una actividad que intenta iniciar sesión en un sistema. El campo **Omitir mayúsculas y minúsculas** está diseñado para su uso con valores de cadenas y matrices de cadenas. Cuando se selecciona el campo **Omitir mayúsculas y minúsculas**, la consulta trata todo el texto de la cadena como un valor en minúscula. Puede utilizar este campo si no está seguro de usar mayúsculas o minúsculas para registrar un evento específico. Debido a que se omite el uso de mayúsculas o minúsculas, la regla puede activarse si la actividad se registra como Inicio de sesión, inicio de sesión o InicioSesión.
ec_outcome es falla (omitir mayúsculas y minúsculas)	Identifica el resultado de una actividad registrado como “falla”. Debido a que se omite el uso de mayúsculas o minúsculas, la regla se puede activar si la actividad se registra como “falla”, “Falla” o “FaLla”.

Declaración de regla	Descripción
user_dst no es nulo	Garantiza que la condición solo es verdadera si se completa user_dst. El operador **no es nulo** permite asegurarse de que un campo devuelva un valor. Puede utilizar este campo cuando una regla depende de que un campo específico devuelva un valor. Por ejemplo, desea crear una regla que identifique al mismo usuario que intenta iniciar sesión varias veces en la misma cuenta de destino (potencialmente un ataque de pruebas para adivinar contraseñas). Si el campo que representa la cuenta de destino del usuario está vacío, no desea que se active la regla. Para asegurarse de que el campo contenga un valor, se utiliza el operador **no es nulo**.

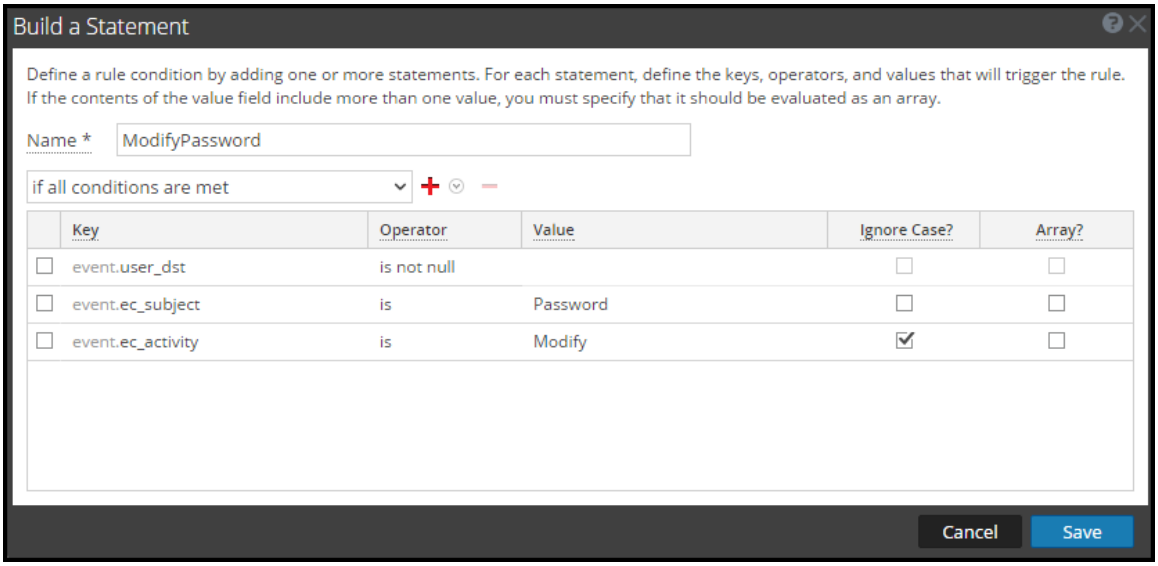
La siguiente declaración compone la condición de éxito:



Declaración de regla	Descripción
ec_activity es inicio de sesión	Identifica la actividad de inicio de sesión.
ec_outcome es éxito	Identifica un inicio de sesión correcto.

Declaración de regla	Descripción
user_dst no es nulo	Garantiza que el campo de la cuenta de destino del usuario deba completarse para que la condición sea verdadera.

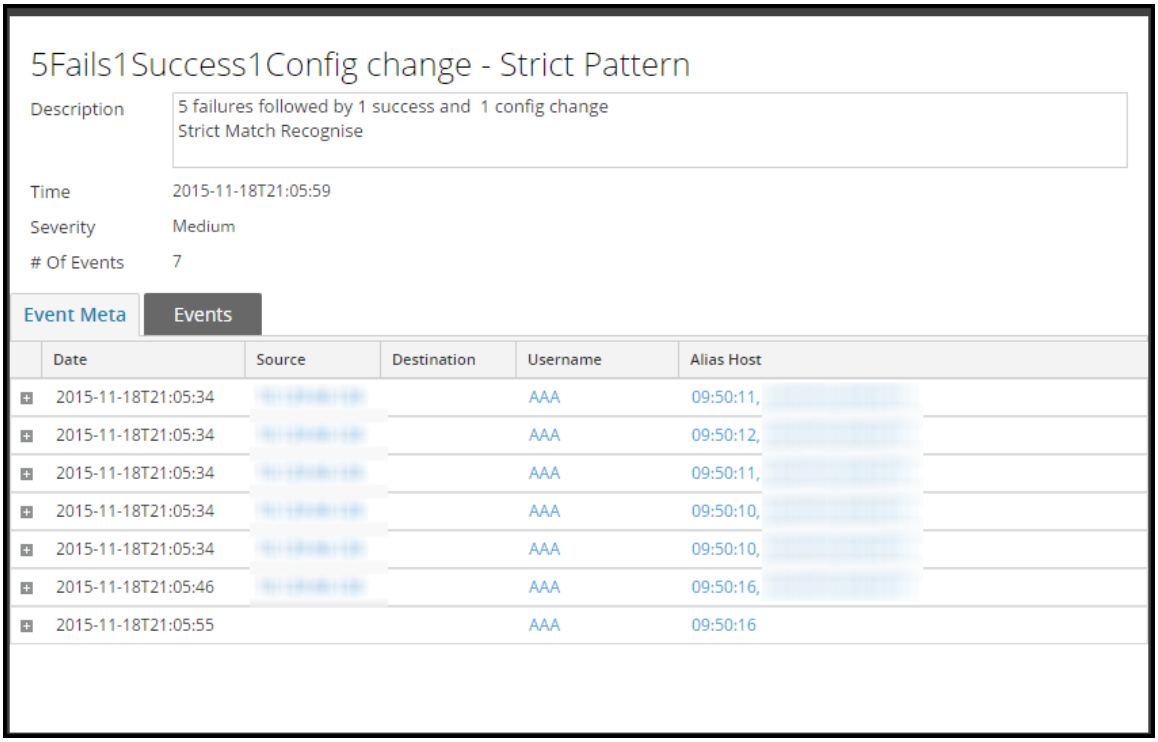
La siguiente declaración forma la condición Modificar contraseña:



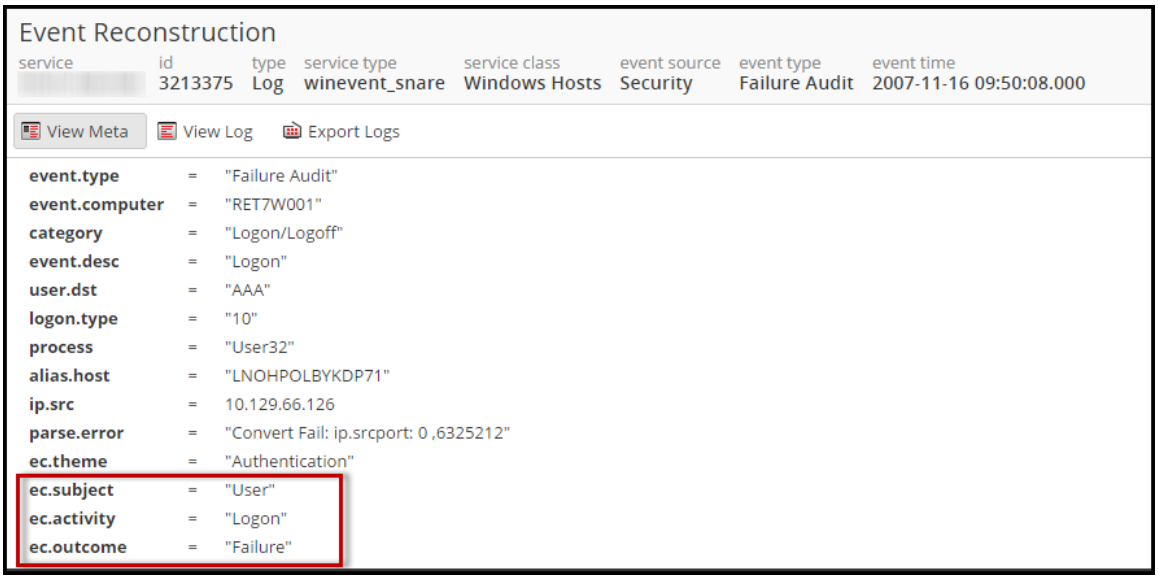
Declaración de regla	Descripción
user_dst no es nulo	Garantiza que el campo de la cuenta de destino del usuario deba completarse para que la condición sea verdadera.
ec_subject es contraseña	Identifica al sujeto de una contraseña.
ec_activity es modificar	Identifica actividad en la cual se modificó la contraseña.

Ejemplo de resultados

Cuando se activa la alerta para la regla de ejemplo, puede ver que la regla se activa para siete eventos y que cada evento contiene un usuario. También puede ver que los eventos siguen un patrón estricto: cinco eventos de inicio de sesión fallidos, seguidos de un evento de inicio de sesión correcto, seguido de una modificación en la cuenta.



Cuando desglosa el módulo Investigation haciendo clic en el origen de uno de los eventos, puede ver el uso de minúscula o mayúscula de cada uno de los valores de cadena. Debido a que utilizó **Omitir mayúsculas y minúsculas**, la regla se activaría si los valores de cadena estuvieran en mayúsculas o minúsculas.

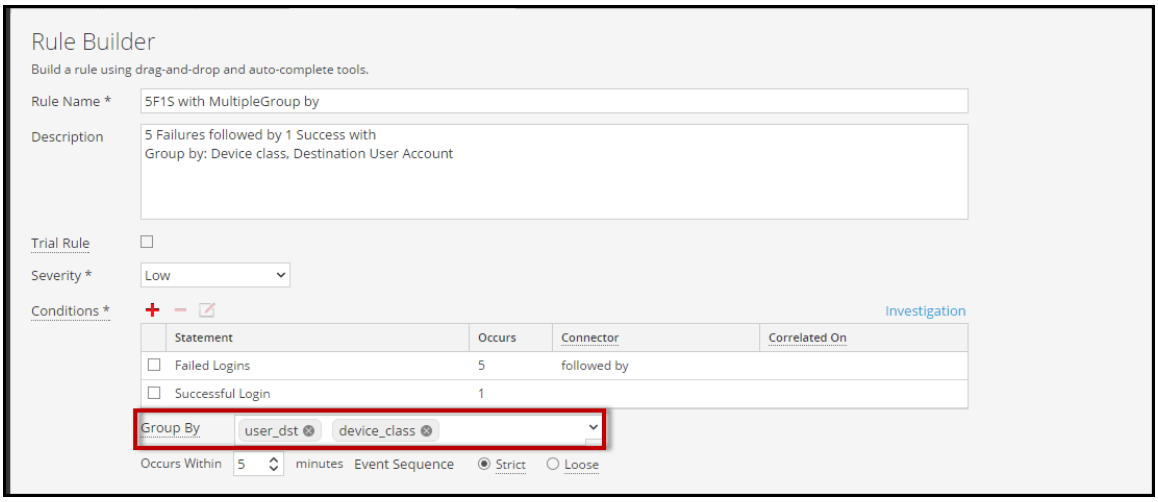


Ejemplo: Agrupación de los resultados de regla

El campo **Agrupar por** permite agrupar y filtrar los resultados de la regla. Por ejemplo, suponga que hay tres cuentas de usuario; Joe, Jane y John y se utilizan los metadatos **Agrupar por**, user_dst. El resultado mostrará eventos agrupados bajo las cuentas de Joe, Jane y John.

También puede agrupar por varias claves, que pueden filtrar aún más los resultados de la regla. Por ejemplo, es posible que desee agrupar por la cuenta de destino y la máquina del usuario para ver si un usuario que inició sesión en la misma cuenta de destino desde la misma máquina intenta iniciar sesión varias veces en una cuenta. Para hacerlo, puede agrupar por device_class y user_dst.

En el siguiente ejemplo se muestra una regla agrupada por device_class y user_dst.

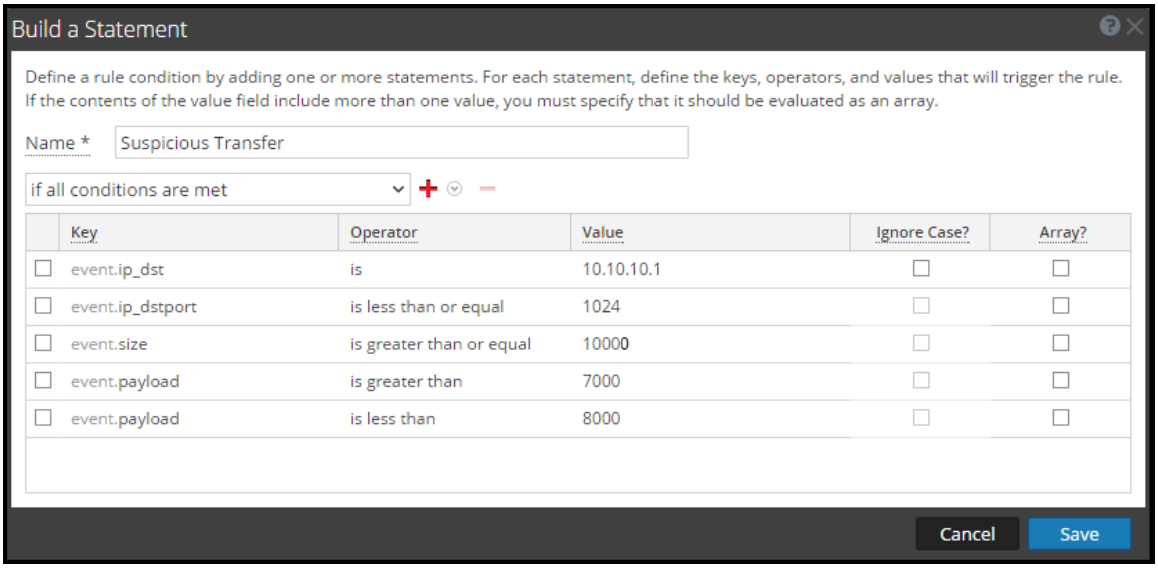


Condición de la regla	Descripción
Inicios de sesión fallidos	Identifica cinco intentos de inicio de sesión fallidos (les debe seguir la condición siguiente; es decir, después de los cinco inicios de sesión fallidos debe haber un inicio de sesión correcto).
Inicio de sesión correcto	Identifica un inicio de sesión correcto.
Agrupar por: user_dst y device_class	Agrupa los resultados de la regla por user_dst (cuenta de destino del usuario) y device_class (tipo de máquina en que el usuario inicia sesión). Esto permite que la regla busque un usuario que inició sesión en la misma máquina y en la misma cuenta de destino, lo que genera un resultado de la regla mucho más específico.
Se produce dentro de 5 minutos con una coincidencia estricta de patrones	Los eventos deben ocurrir dentro de cinco minutos y la coincidencia de patrones es estricta, lo que significa que debe seguir el patrón exactamente para que se active la regla.

Ejemplo: Trabajar con los operadores numéricos

Los operadores numéricos le permiten escribir reglas con valores numéricos como, por ejemplo, especificar que un valor sea mayor que, menor que o igual a un valor específico. Esto es especialmente útil en los casos donde desea especificar un umbral numérico, es decir, *la carga útil es mayor que 7,000*.

En el siguiente ejemplo se intenta identificar una transferencia de datos a un determinado destino a través de puertos comunes donde el tamaño de la transferencia es alto y la carga útil está en un rango sospechoso.



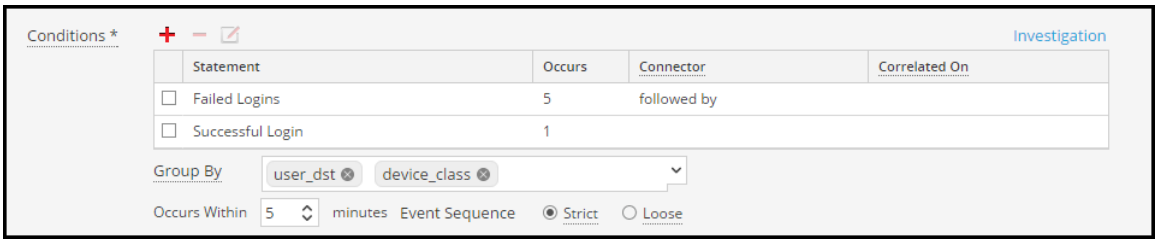
Declaración de regla	Descripción
ip_dst es 10.10.10.1	El puerto de destino es 10.10.10.1.
ip_dstport es mayor o igual que 1,024	El puerto de destino está en un rango de puertos de uso común, 1,024 o superior.
el tamaño es mayor o igual que 10,000	El tamaño de la transferencia es 10,000 o superior, lo cual es una transferencia sospechosamente grande.
la carga útil es mayor que 7,000	La carga útil está entre 7,000 y 8,000, lo cual es una carga útil sospechosamente grande.
la carga útil es menor que 8,000	La carga útil está entre 7,000 y 8,000, lo cual es una carga útil sospechosamente grande.

Paso 3. Agregar condiciones a una declaración de regla

En este tema se proporcionan instrucciones para agregar condiciones, como la especificación de cierto intervalo de tiempo, a una declaración de regla. Cuando se crea una declaración, se especifica qué detecta una regla. Se pueden agregar condiciones para hacer otras estipulaciones, como cuántas veces o cuándo se deben producir los criterios.

Ejemplo

En el siguiente gráfico se muestra un ejemplo de las condiciones para dos declaraciones del generador de reglas. En combinación, las declaraciones y las condiciones comprenden los criterios de la regla.



Esta regla detecta cinco intentos fallidos de inicio de sesión seguidos de un inicio de sesión correcto, lo cual podría ser señal de que alguien hackeó la cuenta de usuario. Estos son los criterios de la regla:

A. Se requieren cinco inicios de sesión fallidos.

B. Después de las fallas, debe haber un inicio de sesión correcto

C. Todos los eventos deben ocurrir en el lapso de 5 minutos.

D. Agrupar las alertas por usuario (user_dst), debido a que se deben realizar los pasos A y B en la misma cuenta de destino del usuario. Además, agrupar por máquina (device_class) para asegurarse de que el usuario que inició sesión en la misma máquina intenta iniciar sesión varias veces en una cuenta.

E. La coincidencia es un patrón estricto, lo que significa que el patrón debe coincidir exactamente sin eventos intermedios.

Procedimiento

Para agregar condiciones a una declaración de regla:

1. En la sección **Condiciones**, seleccione una declaración y haga clic en .
2. En **Ocurre**, ingrese un valor para especificar cuántas apariciones se requieren para satisfacer los criterios de la regla.
3. Si tiene múltiples declaraciones, seleccione un operador lógico para unirlas en el campo

Conector:

- seguido de
- no seguido de
- y
- O

4. **Correlacionado en** se aplica solo a **no seguido de**.

   Si seleccionó **no seguido de** en el paso anterior, escriba la clave de metadatos que no debe venir a continuación.

5. Si los eventos deben suceder en un intervalo de tiempo específico, ingrese una cantidad de minutos en el campo **Ocurre dentro de**.

6. Elija si el patrón debe seguir una coincidencia **Estricta** o una **Flexible**. Si especifica una coincidencia estricta, esto significa que el patrón se debe producir en la secuencia exacta que se especificó, sin eventos adicionales entremedio. Por ejemplo, si la secuencia especifica cinco inicios de sesión fallidos (F) seguidos de un inicio de sesión correcto (S), este patrón solo coincidirá si el usuario ejecuta la siguiente secuencia: F, F, F, F, F, S. Si especifica una coincidencia flexible, significa que se pueden producir otros eventos dentro de la secuencia, pero que la regla se activará si también se producen todos los eventos especificados. Por ejemplo, cinco intentos de inicio de sesión fallidos (F), seguidos de un número indeterminado de intentos de inicio de sesión correctos intermedios (S), seguidos de un intento de inicio de sesión correcto pueden crear el siguiente patrón: F, S, F, S, F, S, F, S, F, S, lo cual activará la regla a pesar de los inicios de sesión intermedios correctos.

7. En la lista desplegable, elija los campos para agrupar por. El campo **Agrupar por** le permite agrupar y evaluar los eventos entrantes. Por ejemplo, en la regla que detecta 5 intentos de inicio de sesión fallidos seguidos de 1 intento correcto, el usuario debe ser el mismo, razón por la cual user_dst es la clave de metadatos **Agrupar por**. También puede agrupar por varias claves. Con el ejemplo anterior, es posible que desee agrupar por usuario y por máquina para asegurarse de que el mismo usuario que inició sesión en la misma máquina intente iniciar sesión varias veces en una cuenta. Para hacerlo, puede agrupar por device_ class y user_dst.

Agregar una regla de EPL avanzado

En este tema se proporcionan instrucciones para definir criterios de regla mediante la redacción de una consulta de EPL. EPL es un lenguaje declarativo para manejar datos de eventos de alta frecuencia basados en tiempo. Se utiliza para expresar filtrado, agregación y uniones en ventanas posiblemente deslizantes de varios flujos de eventos. EPL también incluye una semántica de patrones para expresar causalidad temporal compleja entre eventos.

Escriba una regla de EPL avanzado cuando los criterios de regla sean más complejos que los que se pueden especificar en el generador de reglas.

La explicación de la sintaxis de EPL está fuera del alcance de esta guía.

- Para revisar la documentación de EPL, consulte http://www.espertech.com/esper/documentation.php.
- Para usar la herramienta en línea de EPL, consulte http://esper-epl-tryout.appspot.com/epltryout/mainform.htm

Requisitos previos

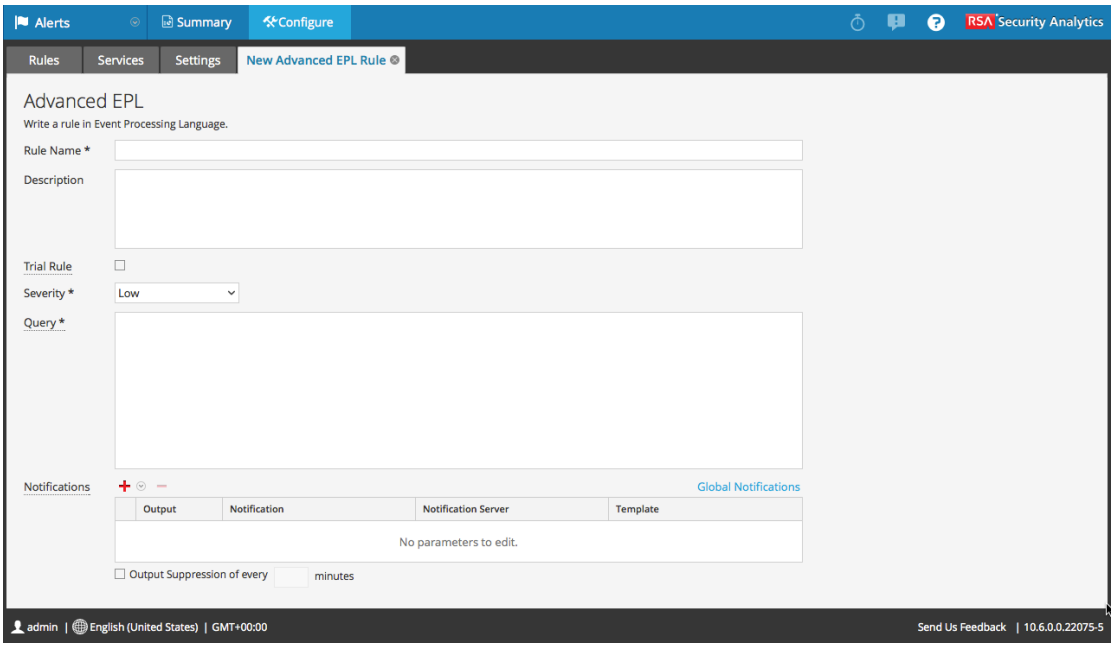
Los siguientes son requisitos previos para agregar una regla avanzada:

- Debe conocer el lenguaje de procesamiento de eventos (EPL).
- Debe comprender las anotaciones de ESA para marcar las declaraciones de EPL vinculadas a la generación de alertas.

Procedimiento

Para agregar una regla de EPL avanzado:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
2. En la **Biblioteca de reglas**, seleccione  **> EPL avanzado**.



3. Escriba un nombre descriptivo único en el campo **Nombre de la regla**.

   Este nombre aparecerá en la Biblioteca de reglas, por lo cual debe ser muy específico para diferenciar esta regla de las demás.

4. En el campo **Descripción**, explique los eventos que detecta la regla.

   El principio de esta descripción aparecerá en la Biblioteca de reglas

5. Seleccione **Regla de prueba** para deshabilitar automáticamente la regla si todas las reglas de prueba superan en conjunto el umbral de la memoria.

   Use el modo de regla de prueba como resguardo para ver si una regla se ejecuta eficientemente e impedir que se produzca tiempo fuera debido a la falta de memoria. Para obtener más información, consulte Trabajar con reglas de prueba.

6. En **Severidad**, clasifique la regla como Baja, Media, Alta o Crítico.

7. Para definir criterios de regla, escriba una **Consulta** en EPL.

   Nota: En todos los nombres de clave de metadatos, use un guion bajo y no un punto. Por ejemplo,`ec_outcome` es correcto, pero `ec.outcome` no lo es.

8. Si una regla debe generar una alerta, incluya esta anotación de ESA en la sintaxis:

   ```
   @RSAAlert
   ```

   ESA proporciona dos anotaciones. Para obtener información detallada, consulte Anotaciones de ESA.

Lenguaje de procesamiento de eventos (EPL)

En este tema se describe Event Processing Language (EPL), un lenguaje declarativo para tratar con datos de eventos basados en tiempo de alta frecuencia. ESA utiliza Event Processing Language (EPL), un lenguaje declarativo para tratar con datos de eventos basados en tiempo de alta frecuencia. Se utiliza para filtrado expreso, agregación y se une a ventanas posiblemente deslizantes de varios flujos de eventos. EPL también incluye una semántica de patrones para expresar la causalidad temporal compleja entre eventos. Puede ejecutar las siguientes funciones, entre otras:

- Filtrar evento
- Alerta sobre supresiones
- Calcular porcentajes o raciones
- Promediar, contar, minimizar y maximizar durante un periodo de tiempo determinado
- Correlacionar eventos que llegan en varios flujos
- Correlacionar eventos que llegan dañados
- Activar o desactivar ventanas
- Soporte para Seguido por y No seguido por
- Soporte de filtro Regex

Las bases de datos requieren una solicitud explícita para devolver datos importantes y que no son aptas para migrar datos dado que cambian. El desarrollador debe implementar la lógica temporal y de agregación por sí mismo. En cambio, el motor EPL proporciona una mayor abstracción e inteligencia y puede considerarse como una base de datos puesta al revés: En lugar de almacenar los datos y ejecutar consultas contra los datos almacenados, EPL permite a las aplicaciones almacenar consultas y ejecutar continuamente los datos a través de ellas. La respuesta del motor EPL es en tiempo real cuando ocurren condiciones que coinciden con las consultas definidas por el usuario.

Para los propósitos de la ayuda en línea, se utilizan declaraciones básicas con el fin de mostrar cómo se configura ESA; sin embargo, para obtener más información acerca de cómo escribir declaraciones EPL, en el sitio http://www.espertech.com se ofrecen cursos y ejemplos.

Nota: ESA es compatible con Esper versión 5.1.0.

Anotaciones de ESA

En este tema se describen dos anotaciones que Security Analytics proporciona para su uso en reglas de EPL avanzado.

Anotación @RSAAlert

La anotación @RSAAlert se utiliza para marcar qué declaraciones EPL están vinculadas para generar alertas. La anotación @RSAAlert es opcional en reglas avanzadas y es útil solo con declaraciones que deben generar alertas de ESA.

Nota: Esta anotación no es necesaria en todas las declaraciones EPL, como las que crean ventanas con nombre, etc.

Anotación @RSAPersist

La anotación @RSAPersist se utiliza para marcar una ventana con nombre como ventana administrada de ESA para obtener persistencia. Al marcar la ventana con nombre como ventana administrada de ESA, ESA escribe periódicamente el contenido de la ventana en el disco y lo restaura si la ventana ya no está implementada y se vuelve a implementar. Los sistemas crean una instantánea justo antes de que se anule la implementación del módulo y se quite la ventana. Por el contrario, restaura el contenido de la ventana desde el snapshot justo después de que el módulo se vuelva a implementar. Esto garantiza que el contenido de la ventana no se pierda si el estado del módulo se altera o si el servicio de ESA queda inactivo.

Por ejemplo, considere una ventana con nombre, `DHCPTracker` que cuenta con un mapeo desde direcciones IP a cada nombre de host asignado. Puede anotar la declaración con la anotación @RSAPersist como:

```
@RSAPersist
 create window DHCPTracker.std:unique(ip_src) as (ip_src string, alias_
host string);
 insert into DHCPTracker select IP as ip_src, HostName as alias_
host from DHCPAssignment(ID=32);
```

Nota: Ninguna de las definiciones de ventanas es adecuada para persistencia. La anotación `@RSAPersist` se debe utilizar con cuidado. Si la ventana tiene registros con tiempo o si depende de restricciones basadas en tiempo, es muy probable que los snapshots revertidos no la restauren en el estado correcto. Además, cualquier cambio en la definición de la ventana invalidará los snapshots y restablecerá la ventana a un estado en blanco. El sistema no realiza ningún análisis semántico para determinar si los cambios a la definición de la ventana tendrán conflictos o no. Tenga en cuenta que otras partes de un módulo (por ejemplo, aparte de la llamada CREAR VENTANA específica que define la ventana) pueden cambiar, sin invalidar los snapshots.

Ejemplo de reglas de EPL avanzado

Los siguientes son ejemplos de reglas avanzadas de ESA. Cada ejemplo tiene varias formas de implementar el mismo caso de uso.

Ejemplo n.º 1:

Cree una cuenta de usuario y elimine la misma cuenta de usuario en 300 s. La información del usuario se almacena en los metadatos user_src.

EPL n.º 1:

Nombre de la regla	CreateuseraccountFollowedbyDeletionof Useraccount1
Descripción de la regla	Creación de una cuenta de usuario seguida de una acción para eliminar la misma cuenta de usuario en 300 segundos.

Código de la regla	`SELECT * FROM Event(ec_subject='User'`
	`  AND ec_outcome='Success'`
	`  AND user_src is NOT NULL`
	`  AND ec_activity IN ('Create', 'Delete')`
	`  ).win:time(300 seconds)`
	`match_recognize (partition by user_src`
	`   measures C as c, D as d`
	`   pattern (C D)`
	`  define`
	`   C as C.ec_activity='Create' ,`
	`   D as D.ec_activity='Delete');`

Nota	• Filtre eventos necesarios para el patrón en el intervalo de tiempo dado. Las condiciones de filtrado solo deben requerir que se transmitan eventos a la función de reconocimiento de coincidencias. En este caso son crear y eliminar la cuenta de usuario Eventos. Es decir, Event(ec_subject='User' AND ec_outcome='Success' AND user_src is NOT NULL AND ec_ activity IN ('Create', 'Delete') • Partición mediante la creación de agrupaciones. En este caso, Esper crea depósitos por valor de user_src. Por lo tanto, el valor de user_src es común entre ambos eventos. • Defina el patrón que desea. Actualmente está configurado para Crear y luego eliminar. Puede ejecutar varias veces Crear y luego eliminar (C + D). El patrón es muy similar a una expresión regular. • Caso de uso más eficiente.

EPL n.º 2:

Nombre de la regla	CreateuseraccountFollowedbyDeletionof Useraccount2
Descripción de la regla	Creación de una cuenta de usuario seguida de una acción para eliminar la misma cuenta de usuario en 300 segundos.

Código de la regla	`SELECT * from pattern[every (a= Event(ec_subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create'))`
	`->`
	`( Event(ec_subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create') AND user_src = a.user_src)`
	`) )where timer:within(300 Sec) ];`

Nota	• Digamos que se crea el mismo usuario dos veces y se elimina una vez en ese orden. En ese caso, el patrón anterior activará dos alertas. • Se crea un hilo de ejecución para cada creación de usuario. • No hay forma de controlar los hilos de ejecución. Es importante tener bonos de tiempo y preferentemente intervalos cortos.

Ejemplo n.º 2:

Detecte el patrón donde se crea el usuario, el mismo usuario inicia sesión y, finalmente, el usuario se elimina. En caso de que Windows registre información del usuario, esta se almacena en user_dst o user_src según el evento.

user_src(create) = user_dst(Login) = user_src(Delete)

EPL n.º 3:

Nombre de la regla	CreateUserLoginandDeleteUser
Descripción de la regla	Detección de un patrón en el cual un usuario crea una cuenta de usuario, seguida del inicio de sesión del mismo usuario y la posterior eliminación de la cuenta de usuario.

Código de la regla	`SELECT * FROM Event(ec_subject='User'`
	`and ec_activity in ('Create','Logon','Delete')`
	`and ec_theme in ('UserGroup', 'Authentication')`
	`and ec_outcome='Success'`
	`).win:time(300 seconds)`
	`match_recognize (measures C as c, L as l, D as d`
	`pattern (C L D)`
	`define`
	`C as C.ec_activity = 'Create',`
	`L as L.ec_activity = 'Logon' AND L.user_dst = C.user_src,`
	`D as D.ec_activity = 'Delete' AND D.user_src = C.user_src`
	`);`

Nota	• Debido a que user_src/user_dst es no es común en todos los eventos, no podemos usar la partición. Será una sola agrupación que ejecuta un patrón por vez. Por ejemplo, para el usuario 1 y 2 si el flujo de eventos es C1C2L1D1, C1L1C2D1, no habrá alerta debido a que el hilo de ejecución C2 restableció C1. La alerta se activará solo si C1L1D1 está en orden y no hay otro evento entremedio, ya sea del mismo usuario o de otro. • Otra solución sería usar la ventana con nombre y combinar user_dst con user_src en una única columna y, a continuación, ejecutar el reconocimiento de coincidencias. (EPL n.º 3). • También se puede usar el patrón. Es posible que obtenga más alertas de lo esperado. (EPL n.º4).

EPL n.º 4: Uso de NamedWindows y reconocimiento de coincidencias

Nombre de la regla	CreateUserLoginandDeleteUser
Descripción de la regla	Detección de un patrón en el cual un usuario crea una cuenta de usuario, seguida del inicio de sesión del mismo usuario y la posterior eliminación de la cuenta de usuario.
Código de la regla	`@Name('NormalizedWindow')create window FilteredEvents.win:time(300 sec) (user String, ecactivity string, sessionid Long);` `@Name('UsersrcEvents') Insert into FilteredEvents select`

```
user_src as user, ec_activity as ecactivity, sessionid
from Event(ec_subject='User' and ec_activity in
('Create','Delete') and ec_theme in ('UserGroup',
'Authentication') and ec_outcome='Success' and user_src is
not null );

@Name('UsrdstEvents') Insert into FilteredEvents select
user_dst as user, ec_activity

as ecactivity, sessionid from Event(ec_subject='User' and
ec_activity in (Logon') and ec_theme in ('UserGroup',
'Authentication') and ec_outcome='Success' and user_dst is
not null );

@Name('Pattern')

@RSAAlert(oneInSeconds=0, identifiers={"user"})

select * from FilteredEvents
    match_recognize (
  partition by user
  measures C as c, L as l, D as d
  pattern (C L+D)
   define C as C.ecactivity= 'Create',
  L as L.ecactivity= 'Logon',
   D as D.ecactivity='Delete'
  );
```

EPL n.º 5: Uso cada @RSAAlert(oneInSeconds=0, identifiers={"user_src"})

SELECT a.time as time,a.ip_src as ip_src,a.user_dst as user_dst,a.ip_dst as ip_dst,a.alias_host as alias_host from pattern[every (a=Event (`ec_subject`='User' and `ec_activity`='Create' and `ec_theme`='UserGroup' and `ec_outcome`='Success') -> (Event(`ec_subject`='User' and `ec_activity`='Logon' and `ec_theme`='Authentication' and `user_src`=a.user_dst) -> b=Event (`ec_subject`='User' and `ec_activity`='Delete' and `ec_theme`='UserGroup' and `user_dst`=a.user_dst))) where timer:within(300 sec)];

Nombre de la regla	CreateUserLoginandDeleteUser
Descripción de la regla	Detección de un patrón en el cual un usuario crea una cuenta de usuario, seguida del inicio de sesión del mismo usuario y la posterior eliminación de la cuenta de usuario.

Ejemplo n.º 3:

Exceso de errores al iniciar sesión desde el mismo IP de origen

EPL n.º 6: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Nombre de la regla	ExcessLoginFailure
Descripción de la regla	El mismo usuario intentó iniciar sesión desde la misma dirección IP de origen y recibió errores al iniciar sesión
Código de la regla	`SELECT * FROM Event( ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time_length_batch(300 sec, 10) GROUP BY ip_src HAVING COUNT(*) = 10;`
Nota	• Crea una ventana por ip_src • Usa time_length_batch: Puede ver eventos en lotes (ventana extensible). Cada evento será parte de solo una ventana. La ventana libera eventos cuando transcurre el tiempo o cuando se alcanza el conteo. • Uno de los problemas con las ventanas extensibles es que es posible que los eventos que ocurren cerca del final del lote no activen una alerta. En la secuencia de eventos a continuación en t=301, incluso cuando se produjeron diez fallas de inicio de sesión para el mismo inicio de sesión en los últimos 300 segundos, no hubo una alerta porque el lote de eventos se descartó en t=300

Hora t	Fallas de inicio de sesión para usuarios específicos	Alerta	Lote de tiempo
0	0	0	1
295	6	0	1
299	3	0	1
301	1	0	2
420	6	0	2
550	3	0	2
600	0	0	3
720	6	0	3

	850 3 0 3 900 1 1 3 finaliza y comienza 4 • El problema anterior se puede solucionar con ventanas win:time (EPL#7) en lugar de ventanas win:time_length_batch. • Agrupar exteriormente por es para controlar eventos cuando transcurre el tiempo. Por ejemplo, tiene nueve eventos con un fin de 60 segundos, el motor Esper enviará esos nueve eventos al oyente. Agrupar por y conteo lo restringirán debido a que el conteo no es igual a 10. • La hora y el conteo se pueden modificar según sea necesario.

EPL n.º 7: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Nombre de la regla	ExcessLoginFailure
Descripción de la regla	El mismo usuario intentó iniciar sesión desde la misma dirección IP de origen y recibió errores al iniciar sesión
Código de la regla	`SELECT * FROM Event( ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time (300 sec) GROUP BY ip_src HAVING COUNT(*) = 10`
Nota	• Esta es una ventana deslizante y, por lo tanto, una vez que se activa la alarma para un conjunto de eventos, se pueden utilizar para otra alerta además de hasta que haya pasado el tiempo. • Si hubiera diez eventos implicados en la activación de la alerta, solo aparecerá el último evento • Si usa < o >, puede ver más de una alerta. Debe usar la supresión de alertas según corresponda.

Ejemplo n.º 4:

Múltiples inicios de sesión fallidos a partir de múltiples usuarios distintos desde el mismo origen al mismo destino, un solo usuario desde múltiples orígenes distintos al mismo destino.

EPL n.º 8: Uso de groupwin , time_length_batch y unique

Nombre de la regla	MultiplefailedLogins
Descripción de la regla	Existen múltiples inicios de sesión fallidos para los mismos casos: - Desde varios usuarios desde el mismo origen al mismo destino. - Usuarios solos desde varios orígenes al mismo destino.
Código de la regla	`SELECT * FROM Event( ec_activity='Logon' AND ec_outcome='Failure' AND ip_src IS NOT NULL AND ip_dst IS NOT NULL AND user_dst IS NOT NULL ).std:groupwin(ip_src,ip_dst).win:time_length_batch(300 seconds, 5}).std:unique(user_dst) group by ip_src,ip_dst having count(*) = 5;`
Nota	• ip.dst and ip.src es común en todos los eventos. • user_dst es único para todos los eventos. • Se activa la alerta cuando hay por lo menos cinco usuarios distintos que intentan iniciar sesión desde la misma combinación de ip.src e ip.dst.

Ejemplo n.º 5:

NoLog traffic desde un dispositivo en un marco de tiempo determinado.

EPL n.º 9: Uso de groupwin, time_length_batch y unique

Nombre de la regla	NoLogTraffic
Descripción de la regla	No se observa un tráfico de registros desde un dispositivo en un marco de tiempo determinado.
Código de la regla	`SELECT * FROM pattern [every a = Event(device_ip IN ('10.0.0.0','10.0.0.1') AND medium = 32) -> (timer:interval (3600 seconds) AND NOT Event(device_ip = a.device_ip AND device_type = a.device_type AND medium = 32))];`
Nota	• La regla solo detecta una pérdida repentina de tráfico. No alertará si no hay tráfico en primer lugar. Necesita al menos 1 evento para que la regla emita una alerta.

	• Lista de direcciones IP de dispositivo o nombres de host de dispositivo como entrada. Solo se rastrearán estos sistemas. • Se requiere una entrada de tiempo. Se activa la alerta cuando el intervalo de tiempo entre eventos excede el tiempo de entrada.

Ejemplo n.º 6:

Múltiples inicios de sesión a los que NO les sigue un evento de bloqueo realizados por el mismo usuario.

EPL n.º 10: uso de groupwin, time_length_batch y unique

Nombre de la regla	FailedloginswoLockout
Descripción de la regla	Existen múltiples inicios de sesión fallidos a los que no les sigue un evento de bloqueo realizados por el mismo usuario.

Código de la regla	`SELECT * FROM pattern [every-distinct(a.user_dst, a.device_ip, 1 msec) (a= Event(ec_activity='Logon' and ec_outcome='Failure' and user_dst IS NOT NULL)-> [2]( Event( device_ip =a.device_ip and ec_activity='Logon' and ec_outcome='Failure' and user_dst=a.user_dst)`
	`AND NOT Event( ( ec_activity='Logon' and ec_outcome='Success' and device_ip = a.device_ip and user_dst=a.user_dst) or (ec_activity='Lockout' and device_ip = a.device_ip and user_dst=a.user_dst))))`
	`where timer:within(60 seconds) -> (timer:interval(30 seconds) and not Event(device_ip=a.device_ip and user_dst=a.user_dst and ec_activity='Lockout'))];`

Nota	• La consulta detecta la ausencia de un evento de bloqueo después de que se produzcan dos inicios de sesión fallidos por parte del mismo usuario. • La aparición de múltiples inicios de sesión fallidos se cronometra y se asume que sucede dentro de cierto período. Además, en la práctica, se asume que el evento de bloqueo se produce dentro de un período corto después de la aparición del último evento de inicio de sesión fallido debido a que el valor del umbral de inicios de sesión fallidos por usuario está establecido en cierto dominio.

	• En la consulta actual, cada valor distinto suprimirá el nuevo hilo de ejecución para la combinación de usuario y dispositivo para 1 milisegundo. • El tiempo permitido para tres inicios de sesión fallidos es de 60 segundos desde el primer intento fallido. El período de espera para que se produzca el evento de bloqueo es de 30 segundos

Nota:
1. “.” en las claves de metadatos se debe reemplazar por (“_”).
2. Todos los patrones deben tener bonos de tiempo.
3. Use las etiquetas adecuadas frente a las declaraciones
 a) @RSAPersist:
 b) @RSAAlert:

Para obtener detalles adicionales, puede consultar:

- Documentación de EPL: http://www.espertech.com/esper/documentation.php
- Herramienta en línea de EPL: http://esper-epl-tryout.appspot.com/epltryout/mainform.html

Trabajo con reglas

En este tema se analizan procedimientos adicionales que puede realizar en las reglas. Tal vez desee realizar cualquiera de los siguientes procedimientos:

- Editar, duplicar o eliminar una regla
- Filtrar o buscar reglas
- Importar o exportar reglas

Editar, duplicar o eliminar una regla

En este tema se proporcionan instrucciones para editar, duplicar o eliminar una regla de Event Stream Analysis (ESA). Cuando edita una regla, ESA aplica los criterios actualizados de ahí en adelante. En las alertas generadas con anterioridad no se hacen cambios.

Procedimientos

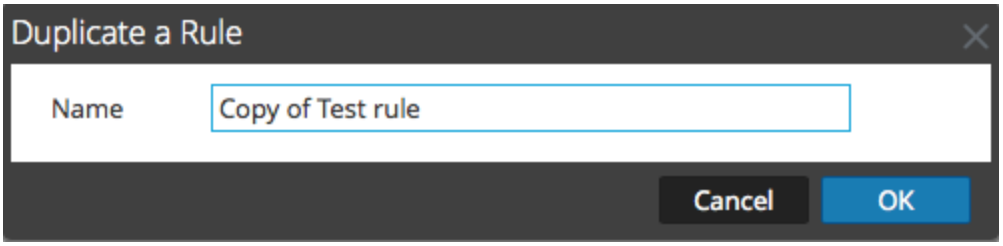
Editar una regla

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Reglas**.
   Se muestra la pestaña Reglas.

2. En la **Biblioteca de reglas**, seleccione la regla que desea editar y haga clic en .
   Según el tipo de regla, se muestra la pestaña de regla respectiva.
3. Modifique los parámetros requeridos.
4. Haga clic en **Guardar**.

Duplicar una regla

1. En la **Biblioteca de reglas**, seleccione la regla que desea duplicar y haga clic en .
2. Se muestra el cuadro de diálogo Duplicar una regla. El sistema agrega **Copia de** frente al nombre de la regla.

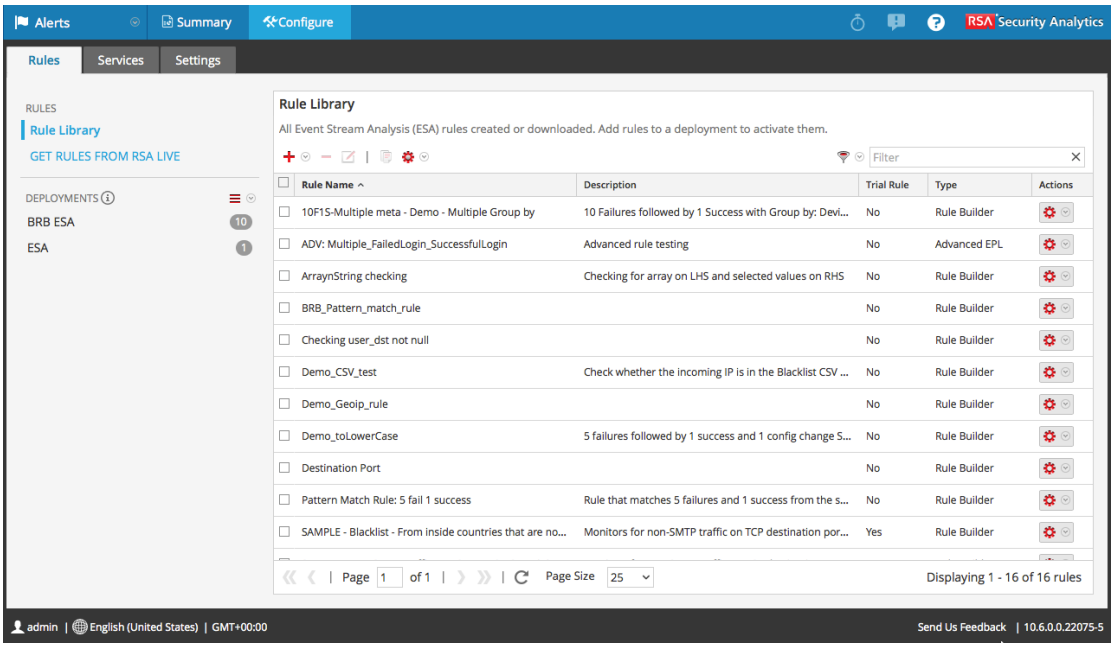


3. En el campo **Nombre**, ingrese un nombre único para la regla duplicada y haga clic en **Aceptar**.

Una regla duplicada con el nuevo nombre se agrega a la Biblioteca de reglas.

Eliminar una regla

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Reglas**.
   Se muestra la pestaña Reglas.



2. En la Biblioteca de reglas, seleccione una o más reglas y haga clic en .

   Se muestra un cuadro de diálogo de advertencia.

3. Haga clic en **Sí**.
   Se muestra un mensaje de confirmación que indica que la regla se eliminó correctamente y la regla seleccionada se elimina de la Biblioteca de reglas.

Filtrar o buscar reglas

En este tema se muestra a los analistas cómo especificar el tipo de reglas que se presentan en la Biblioteca de reglas.

Requisitos previos

Asegúrese de comprender los componentes de la vista Biblioteca de reglas. Para obtener más información, consulte Panel Biblioteca de reglas.

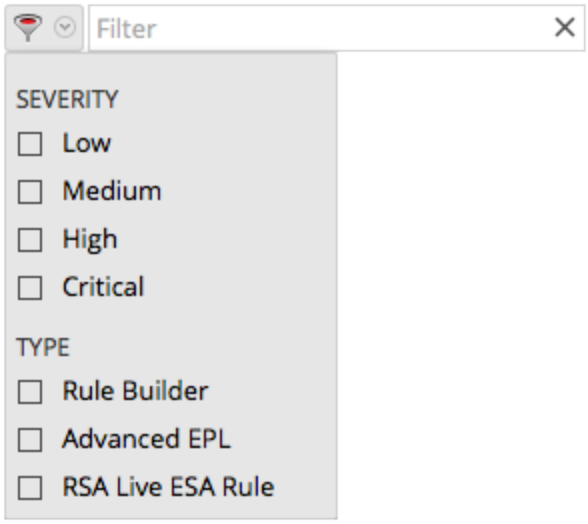
Procedimientos

Filtro

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   La pestaña Reglas se muestra de manera predeterminada.

2. En la barra de herramientas del panel **Biblioteca de reglas**, haga clic en y seleccione la gravedad y el tipo de reglas que desea que aparezcan en la lista de la Biblioteca de reglas.

En la siguiente figura se muestra la lista desplegable Filtrar.



Los tipos de reglas seleccionados aparecen en la lista.

Buscar

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   La pestaña Reglas se muestra de manera predeterminada.
2. En la barra de herramientas del panel **Biblioteca de reglas**, escriba el nombre de una regla en el campo Filtrar.
   En el panel Biblioteca de reglas se enumeran las reglas que coinciden con los nombres ingresados en el campo Filtrar.

Importar o exportar reglas

En el tema se proporcionan instrucciones para importar reglas de ESA desde una instancia de Security Analytics y para exportarlas a un disco duro de modo que pueda mantener una copia local.

Si exportó una regla en una versión anterior de Security Analytics, se aplican las siguientes condiciones cuando importa la regla en la versión 10.5 o superior:

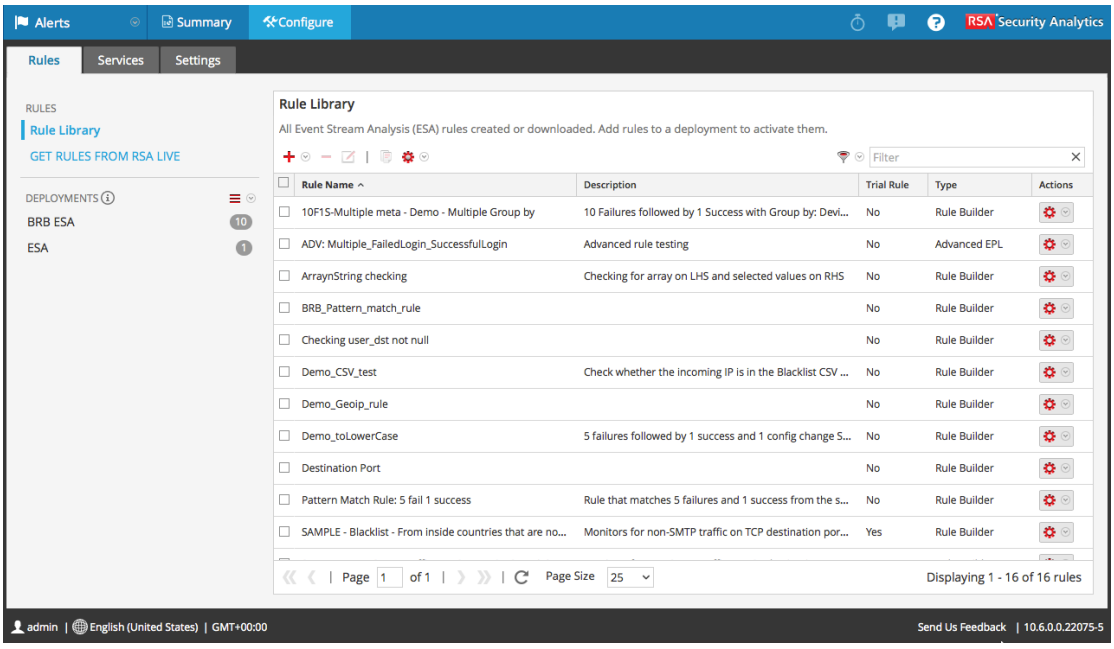
- Se exportó en la versión 10.3: no puede importar reglas a la versión 10.5.
- Se exportó en la versión 10.4: el comportamiento de la regla depende de si la correlación entre sitios está inhabilitada, que es el valor predeterminado, o habilitada:
  - Inhabilitada: puede importar reglas a la versión 10.5.
  - Habilitada: Debe reiniciar Security Analytics o hacer un cambio secundario en la regla, guardarla, quitar el cambio secundario y volver a guardarla. Ambos procedimientos

generan la regla de reenvío que requiere la función de correlación entre sitios de la versión 10.5.

Procedimientos

Importar reglas de ESA

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Reglas**.
   Se muestra la pestaña Reglas.



2. En la barra de herramientas de la **Biblioteca de reglas**, haga clic en  **> Importar**.
   Se muestra el cuadro de diálogo Importar reglas de ESA.

3. Haga clic en **Navegar** para navegar y seleccionar el archivo que contiene las reglas de ESA.
4. Haga clic en Importar.

Exportación

1. Seleccione una o varias reglas de ESA y haga clic en  > **Exportar** en la barra herramientas de la Biblioteca de reglas.
   Se muestra un cuadro de diálogo de advertencia.
2. Haga clic en **Sí**.
   Se muestra el cuadro de diálogo Exportar reglas.
3. En el campo **Escribir nombre de archivo**, escriba un nombre para el archivo que contiene las reglas de ESA y haga clic en **Exportar**.
   El archivo se exporta como un archivo binario a la máquina.

Nota: El archivo binario no se puede editar.

Seleccionar cómo se desea recibir una notificación sobre alertas

En este tema se explican los distintos métodos de notificación y cómo agregar un método de notificación a una regla. Se requieren los permisos de función administrador, administrador del SOC o DPO para todas las tareas de esta sección.

Cuando una regla activa una alerta, ESA puede enviar una notificación de las siguientes maneras:

- Correo electrónico
- SNMP
- Syslog
- Script

Para configurar una notificación, se definen los siguientes componentes:

- Servidor de notificación: después de configurar un servidor de notificación, puede agregarlo a una regla. Cuando la regla activa una alerta, usará ese servidor para enviar notificaciones de alertas.
- Notificaciones: son las salidas, entre las cuales se incluye correo electrónico, script, SNMP y syslog. Cuando diseña una regla, puede especificar la notificación para una alerta.
- Plantillas: el formato de una notificación de alerta se define en una plantilla.

La supresión de alertas y la normativa de tasa de alertas son dos funciones que proporciona Event Stream Analysis. La supresión de alertas asegura que no se envíen varios correos electrónicos para la misma alerta. Por ejemplo, considere una regla para detectar nombres de inicio de sesión del usuario fallidos. Si establece la supresión de alertas en tres minutos, solo verá las alertas generadas en ese intervalo de tiempo. Esto es menor que la cantidad de alertas que vería sin la supresión de alertas. Algunas alertas pueden estar duplicadas. Con la supresión de alertas, no se envían correos electrónicos para las alertas duplicadas. Esto garantiza que la bandeja de entrada no se inunde de notificaciones de alertas redundantes.

La normativa de tasas de alertas es una medida preventiva que asegura que las alertas que provienen de reglas malinterpretadas no inunden el sistema. De esta manera se impide que ESA envíe más del límite de correos electrónicos configurado en un minuto.

Los servidores de notificación, las notificaciones y las plantillas se configuran en la vista Sistema de Administration. Para obtener más información, consulte “Configurar servidores de notificación”, “Configurar las salidas de las notificaciones” y “Configurar plantillas para notificaciones” en la **Guía de configuración del sistema**.

Métodos de notificación

Cuando una regla activa una alerta, ESA puede enviar una notificación de las siguientes maneras:

- Correo electrónico
- SNMP
- Syslog
- Script

Notificaciones por correo electrónico

Event Stream Analysis puede enviar notificaciones a los usuarios mediante un correo electrónico acerca de diversos eventos del sistema.

Para configurar estas notificaciones por correo electrónico, debe:

- Configurar el servidor de correo electrónico de SMTP como un proveedor de salida. Para obtener instrucciones, consulte “Configurar los ajustes de correo electrónico como un servidor de notificación” en la **Guía de configuración del sistema**.
- Configurar una cuenta de correo electrónico para recibir notificaciones. Para obtener instrucciones, consulte “Configurar el correo electrónico como una notificación” en la **Guía de configuración del sistema**.
- Configurar una plantilla para notificación por correo electrónico. Para obtener instrucciones, consulte “Configurar una plantilla” en la **Guía de configuración del sistema**.

SNMP

Event Stream Analysis puede enviar eventos como un SNMP trap a un host de SNMP trap configurado.

Para configurar estas notificaciones de SNMP, debe:

- Configurar el host de SNMP trap como un proveedor de salida. Para obtener instrucciones, consulte “Configurar los ajustes de SNMP como un servidor de notificación” en la **Guía de configuración del sistema**.

- Configurar los ajustes de SNMP trap como una acción de salida. Para obtener instrucciones, consulte “Configurar SNMP como una notificación” en la **Guía de configuración del sistema**.
- Configurar una plantilla para SNMP. Para obtener instrucciones, consulte “Configurar una plantilla” en la **Guía de configuración del sistema**.

Syslog

Event Stream Analysis puede enviar eventos y consolidar registros en formato syslog a un servidor de syslog.

Para configurar estas notificaciones de syslog, debe:

- Configurar los ajustes del servidor syslog como un proveedor de salida. Para obtener instrucciones, consulte “Configurar los ajustes de syslog como un servidor de notificación” en la **Guía de configuración del sistema**.
- Configurar un formato de mensaje de syslog como una acción de salida. Para obtener instrucciones, consulte “Configurar syslog como una notificación” en la **Guía de configuración del sistema**.
- Configurar una plantilla para syslog. Para obtener instrucciones, consulte “Configurar una plantilla” en la **Guía de configuración del sistema**.

Script Alerter

Además de las notificaciones de alerta, ESA permite a los usuarios ejecutar scripts en respuesta a las alertas de ESA.

Los scripts le permiten hacer una integración personalizada con aplicaciones que existen en su ambiente. Por ejemplo, si desea abrir un vale de incidente de una aplicación cuando se activa una alerta específica, Script Alerter le permite escribir un script que llama a la API de la aplicación y hacer que ESA lo invoque cuando se activa la regla de ESA específica. Puede configurar una plantilla de FreeMarker para definir los detalles que desea extraer de la salida de la regla de ESA y transmitirlos como argumentos de la línea de comandos al script.

Para usar Script Alert, debe:

- Configurar la identidad del usuario y otros detalles que se requieren para ejecutar el script. Para obtener instrucciones, consulte “Configurar un script como un servidor de notificación” en la **Guía de configuración del sistema**.
- Definir el script. Para obtener instrucciones, consulte “Configurar el script como una notificación” en la **Guía de configuración del sistema**.

- Configurar una plantilla para el script. Para obtener instrucciones, consulte “Configurar una plantilla” en la **Guía de configuración del sistema**.

Agregar un método de notificación a una regla

En este tema se indica a los administradores cómo agregar una notificación, como el correo electrónico, a una regla. ESA usa el método de notificación cuando genera una alerta para un evento que cumple con los criterios de una regla.

Una notificación se agrega a una regla para que ESA pueda informar cuando una regla activa una alerta. Aunque los campos de notificación no son obligatorios, constituye una mejor práctica agregar una notificación a una regla.

Cuando agrega un método de notificación a una regla, selecciona la siguiente información:

- Salida
- Notificación
- Servidor de notificación
- Plantilla

Requisitos previos

- La función debe tener permiso para administrar reglas.
- La regla debe existir.
- El método de notificación debe estar configurado con un servidor y una plantilla compatibles:
  - Haga clic en **Administration > Sistema > Notificaciones globales**.
  - Para conocer los procedimientos detallados, consulte la **Guía de configuración del sistema**.

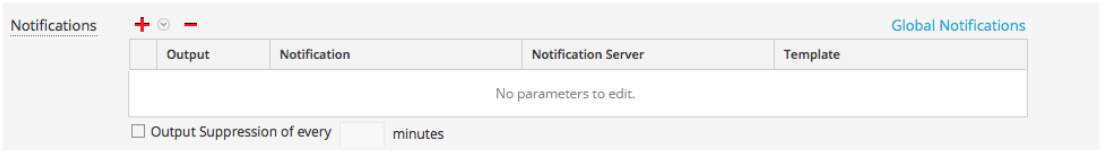
Procedimiento

Para agregar un método de notificación a una regla:

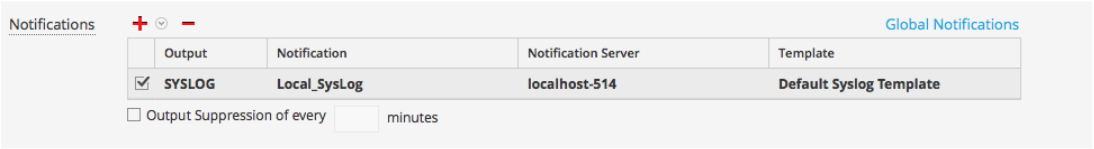
1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Reglas**.
2. En la **Biblioteca de reglas**, haga clic en  para agregar una nueva regla o seleccionar una regla existente, y haga clic en  .

   Según el tipo de regla, se muestra la pestaña Generador de reglas o EPL avanzado.

   La sección Notificaciones es igual para ambas pestañas.



3. Haga clic en y seleccione la **Salida** para la alerta:
   - Correo electrónico
   - SNMP
   - Syslog
   - Script
4. Haga doble clic en el campo **Notificación** y seleccione el nombre de una salida configurada con anterioridad.
   Por ejemplo, Analista de nivel 1 podría ser el nombre de una notificación por correo electrónico que se dirige al grupo de distribución de correo electrónico Analistas L1.
5. Haga doble clic en el campo **Servidor de notificación** y seleccione el servidor que envía la notificación.
6. Haga doble clic en el campo **Plantilla** y seleccione un formato para la alerta.
   En la siguiente figura se muestra la configuración de una notificación de syslog.

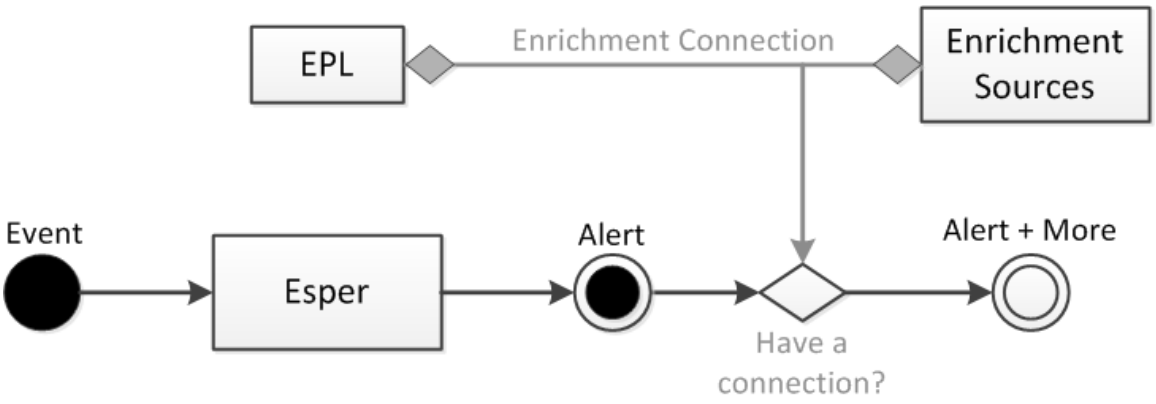


7. Si desea especificar la frecuencia, seleccione **Supresión de salida** e ingrese la cantidad de **minutos**.
8. Si desea agregar otra notificación, repita los pasos del 3 al 7.
9. Haga clic en **Guardar**.
   Cuando ESA genere una alerta para un evento que coincida con los criterios de la regla, recibirá una notificación sobre la alerta a través de cada método de notificación agregado a la regla.

Agregar un origen de enriquecimiento de datos

En este tema se indica cómo agregar un origen de enriquecimiento configurado con anterioridad a una regla. Cuando ESA crea una alerta, la información del origen se incluye en ella.

Los enriquecimientos brindan la capacidad de incluir información contextual en la lógica de correlación y la salida de alertas. Sin los enriquecimientos, toda la información que se incluye en una alerta de ESA proviene de un servicio Security Analytics Core. Con los enriquecimientos, puede solicitar búsquedas en diversos orígenes e incluir los resultados en las alertas salientes. En la siguiente figura se ilustra la función de los enriquecimientos.



La configuración de los enriquecimientos está compuesta por dos unidades lógicas:

- Orígenes de enriquecimiento: son áreas de almacenamiento de datos de información contextual.
- Conexiones de enriquecimiento: actúan como conectores entre metadatos de alertas y columnas de origen.

ESA permite establecer conexiones entre declaraciones del lenguaje de procesamiento de eventos (EPL) y orígenes de enriquecimiento. Una vez que se establecen las conexiones, el sistema combina los campos seleccionados de la salida de las alertas con la información de los orígenes y usa los datos coincidentes para enriquecer la alerta que se envía. ESA puede establecer conexión con los siguientes orígenes:

- Ventanas con nombre de Esper
- Tablas de bases de datos relacionales
- Base de datos de MaxMindGeoIP
- Listas de seguimiento de RSA Warehouse Analytics

Nota: el origen de enriquecimiento geoIP no se puede crear ni eliminar. Se proporciona al usuario para uso inmediato.

Ejemplo de regla con enriquecimiento

En el siguiente ejemplo de regla se ilustra la función de enriquecimiento que proporciona ESA:

```
@RSAAlert @Name("simple") SELECT * FROM CoreEvent(ec_theme='Login Failure')
```

La regla genera una alerta para cada error al iniciar sesión y, de este modo, si se recibe el siguiente flujo de eventos (simplificado) en ESA:

sessionid	ec_theme	username	ip_src	ip_dst	host_dst
1	Login Success	dshrute	23.xx.23x.16		
2	Login Failure	jhalpert	23.xx.23x.16	31.1X.X9.1x8	www.facebook.com

Se podría generar una alerta con los siguientes `events` constitutivos en respuesta a la segunda sesión:

```
{
     "events": [
         {
             "username": "jhalpert",
             "host_dst": "www.facebook.com",
             "ip_dst": "31.1x.x9.1x8",
             "sessionid": 2,
             "ec_theme": "Login Failure",
             "esa_time": 1406148964130,
             "ip_src": "23.xx.23x.16"
         }
     ]
 }
```

La salida JSON muestra toda la información disponible que se incluirá en una notificación de ESA mediante el uso de una plantilla apropiada de FreeMarker
. Por ejemplo, la expresión de la plantilla `${events[0].username}` sería equivalente a `jhalpert`.

Con enriquecimientos, el mismo módulo con el mismo flujo de eventos puede generar la alerta que se muestra a continuación. El sistema
puede establecer múltiples conexiones de enriquecimiento y extraer datos contextuales de modo que la alerta sea más significativa.

Por ejemplo:
`${events[0]["RSADataScienceLookup"][0].score}` entrega el puntaje de **"riesgo"** del dominio de destino que calcula el módulo RSA Warehouse Analytics, mientras que `${events[0]["orgchart"][0].supervisor}` entrega el nombre del supervisor del empleado relacionado con la alerta (extraído de una base de datos de RR. HH.) y `${events[0]["LoginRegister"][0].username}` entrega el nombre del usuario con el último inicio de sesión correcto para el mismo `ip_src` (mediante el uso de una ventana con nombre basada en flujo).


```
{"events": [
     {
         "username": "jhalpert",
         "host_dst": "www.facebook.com",
         "GeoIpLookup": [
         {
             "city": "Cambridge",
             "longitude": -71,
             "countryCode": "US",
             "areaCode": 617,
             "metroCode": 506,
             "region": "MA",
             "dmaCode": 506,
             "ipv4Obj": "/23.62.236.16",
             "countryName": "United States",
             "postalCode": "02142",
             "ipv4": "23.62.236.16",
             "latitude": 42,
             "organization": "Verizon Business"
         }
     ],
     "RSADataScienceLookup": [
         {
             "model_id": "suspiciousDomains_1",
             "_id": "EXEC_BATCH_1_20140630153740_facebook.com",
             "score": 10,
             "key": "www.facebook.com"
         }
     ],
     "orgchart": [
         {
             "supervisor": "mscott",
             "name": "James Halpert",
             "extension": 3692,
             "location": "Scranton",
```

```
            "department": "Sales",
            "id": "jhalpert"
        }
    ],
    "ip_dst": "31.13.69.128",
    "sessionid": 2,
    "LoginRegister": [
        {
            "username": "dshrute",
            "ip_src": "23.62.236.16"
        }
    ],
    "ec_theme": "Login Failure",
    "esa_time": 1406155218912,
    "ip_src": "23.62.236.16"
    }
]}
```


Configurar una conexión de base de datos

En este tema se proporciona información para configurar una conexión a una base de datos externa que puede proporcionar información adicional en alertas. Una conexión de base de datos se configura para que posteriormente sea posible configurar la base de datos como un origen de enriquecimiento con el fin de agregar detalles adicionales a las alertas. Este proceso tiene tres pasos:

1. Configurar una conexión a una base de datos.
2. Configurar la base de datos externa como un origen de enriquecimiento.
3. Agregar el origen de enriquecimiento a una regla

En este tema se explica el paso 1.

Ejemplo

En este ejemplo se ilustra cómo la adición de una base de datos como un origen de enriquecimiento añade valor a las alertas.

Una regla detecta a usuarios que intentan inscribirse en un servicio de correo electrónico fantasma. 25 usuarios coinciden con los criterios de la regla. Sin el enriquecimiento, la alerta contiene 25 ID de usuario. Con el enriquecimiento, la alerta también incluye la siguiente información para cada ID de usuario:

- Nombre
- Título

- Departamento
- Ubicación de la oficina

Dependencias

Cuando configura una base de datos, se aplican las siguientes condiciones:

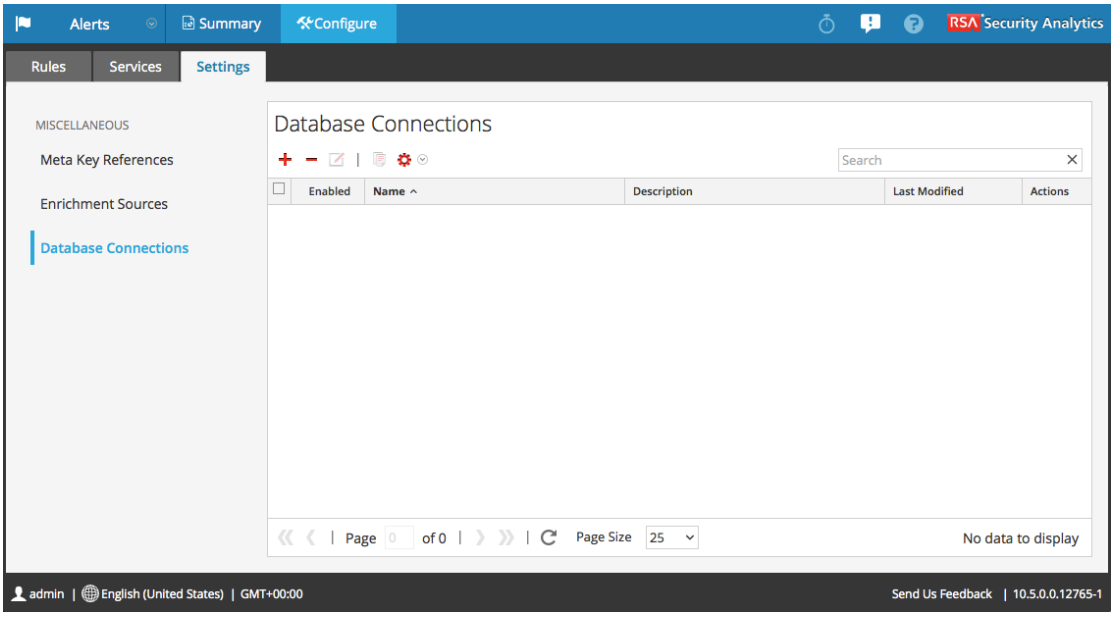
- Se implementa una referencia a la base de datos en cada ESA, incluso si ESA no implementa reglas que usan la base de datos como un origen de enriquecimiento.
- Si el servidor que aloja la base de datos queda inactivo, esto afecta a una implementación.
  - Una implementación activa continuará recopilando datos y ejecutando reglas, pero los enriquecimientos no aparecerán en las alertas.
  - Una implementación nueva fallará hasta que se reinicie el host.

Procedimiento

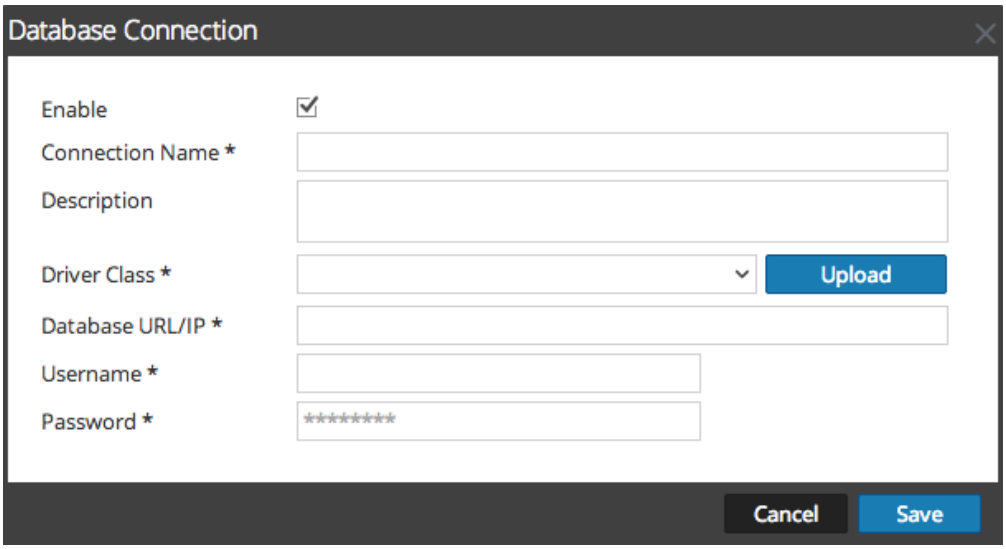
Para configurar una conexión de base de datos:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
2. Haga clic en la pestaña **Configuración**.
3. En el panel de opciones, seleccione **Conexiones de la base de datos**.

   Se muestra el panel Conexiones de la base de datos.



4. Haga clic en + para agregar una conexión de base de datos.



5. En el cuadro de diálogo **Conexión de base de datos**, proporcione la siguiente información.

Campo	Descripción
Habilitar	Seleccione Activar para enriquecer una alerta con datos adicionales. El campo Habilitar está seleccionado de forma predeterminada. Deseleccione Habilitar para excluir los datos adicionales de la alerta.
Nombre de conexión	Escriba un nombre para identificar la conexión. Cuando agrega una base de datos como un origen de enriquecimiento, este nombre aparece en la lista de Conexiones de la base de datos.
Descripción	(Opcional) Escriba una descripción breve de la conexión de base de datos.
Clase de controlador	Seleccione una clase de controlador apropiada para la base de datos. Security Analytics incluye dos drivers, MongoDB y Postgres. Para importar un nuevo controlador, haga clic en **Cargar**.  En el cuadro de diálogo **Importar clase de controlador**, haga clic en **Navegar**, seleccione un nuevo controlador y haga clic en **Importar**.

Campo	Descripción
Dirección URL de base de datos o Dirección IP	Escriba la dirección o la dirección IP de la base de datos que se configurará.
Nombre de usuario	Escriba el nombre de usuario para acceder a la base de datos.
Contraseña	Escriba la contraseña para acceder a la base de datos.

6. Haga clic en **Guardar**.

Para obtener información relacionada, consulte Pestaña Ajustes de configuración

Orígenes de enriquecimiento

En este tema se explican las opciones para agregar un origen de datos externo con el fin de proporcionar información adicional en las alertas. Los orígenes de enriquecimiento proporcionan información adicional en las alertas. Por ejemplo, una base de datos puede proporcionar un nombre, un departamento y la ubicación de una oficina si un usuario coincide con los criterios de la regla. Existen tres tipos de orígenes de enriquecimiento:

- Referencia de base de datos externa
- Tabla en la memoria
- Warehouse Analytics

Configurar una base de datos como origen de enriquecimiento

Una base de datos se configura como un origen de enriquecimiento de modo que se pueda agregar a una regla. Posteriormente, el motor de Esper que analiza los eventos puede acceder a la información de la base de datos para proporcionar información adicional en la alerta.

Por ejemplo, una regla detecta a usuarios que intentan inscribirse en un servicio de correo electrónico fantasma. 25 usuarios coinciden con los criterios de la regla. La alerta contiene 25 ID de usuario. Una base de datos externa mejoraría la alerta con la entrega de la siguiente información adicional para cada ID de usuario:

- Nombre
- Título
- Departamento
- Ubicación de la oficina
- Rinde cuentas a

Puede editar, duplicar, importar o exportar una conexión de base de datos.

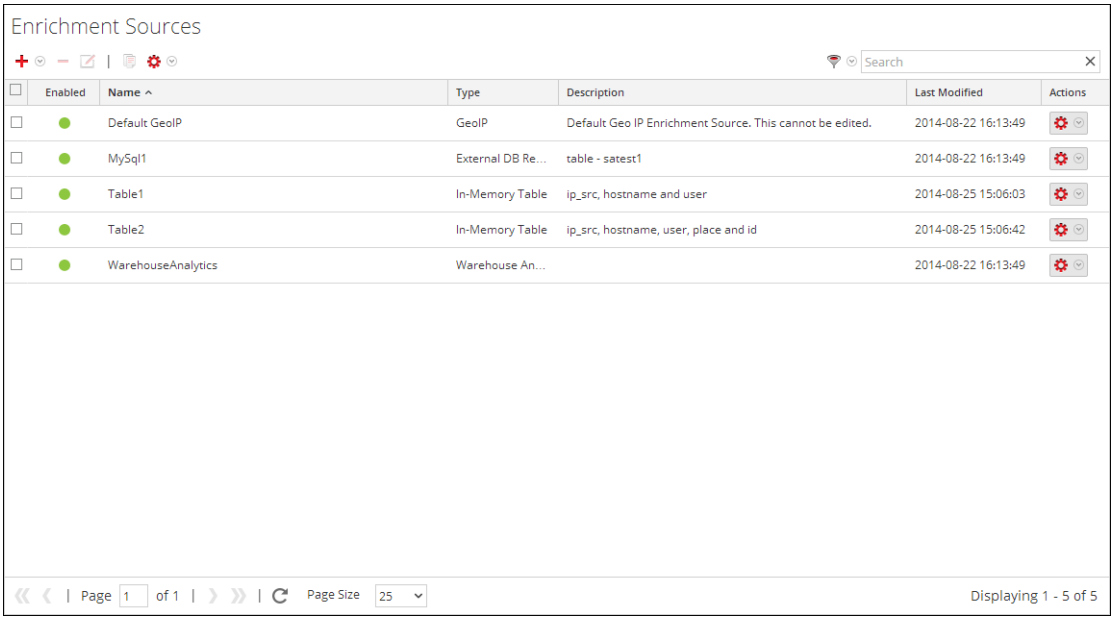
Requisitos previos

Debe configurar una conexión de base de datos. Para obtener más información, consulte Configurar una conexión de base de datos.

Procedimiento

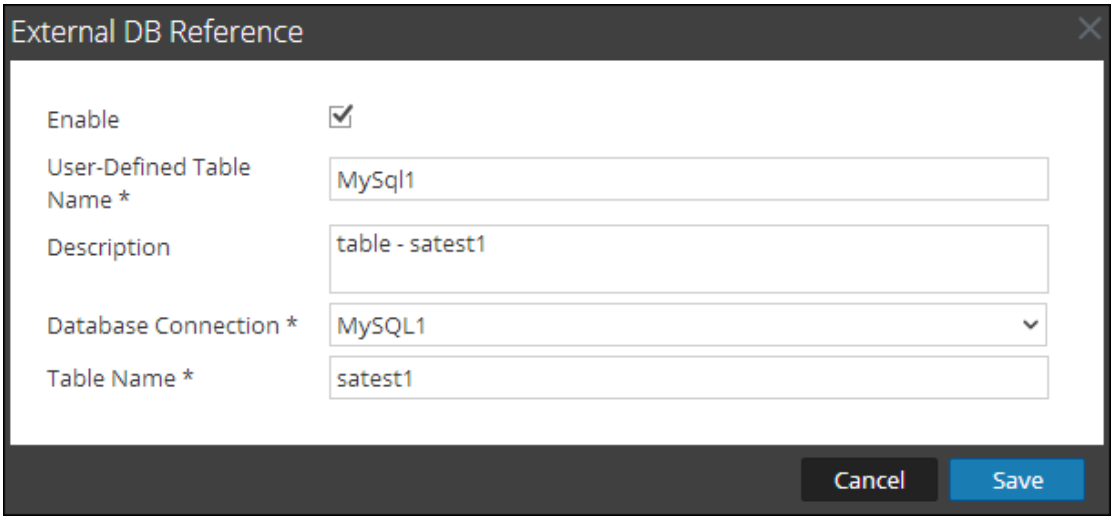
Para configurar una base de datos como un origen de enriquecimiento:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
2. Haga clic en la pestaña **Configuración**.
   Se muestra la pestaña Configuración.
3. En el panel de opciones, seleccione **Orígenes de enriquecimiento**.
   Se muestra el panel Orígenes de enriquecimiento.



4. En el menú desplegable  , seleccione **Referencia de base de datos externa**. Debe agregar una referencia de base de datos para que la base de datos se enumere.

Se muestra el cuadro de diálogo Referencia de base de datos externa.



5. Seleccione **Habilitar** para enriquecer una alerta con datos adicionales. Esta opción está seleccionada de forma predeterminada. Si se deshabilita, la alerta no se enriquece con datos adicionales.
6. En el campo **Nombre de tabla definido por el usuario**, escriba un nombre para identificar o etiquetar la configuración de la base de datos.
7. En el campo **Descripción**, escriba una descripción breve de la configuración de la base de datos.
8. En el menú desplegable **Conexión de base de datos**, seleccione las conexiones de la base de datos definidas.
9. En el campo **Nombre de tabla**, ingrese el nombre de tabla de la base de datos
10. Haga clic en **Guardar**.

Para obtener detalles de los parámetros y sus descripciones, consulte Pestaña Ajustes de configuración.

Configurar una tabla en la memoria como origen de enriquecimiento

En este tema se proporcionan instrucciones para configurar una tabla en la memoria. Cuando se configura una tabla en la memoria, se carga un archivo .CSV como entrada para la tabla. Puede asociar esta tabla con una regla como un origen de enriquecimiento. Cuando la regla asociada genere una alerta, ESA enriquecerá la alerta con información pertinente de la tabla en la memoria.

Por ejemplo, se podría configurar una regla para detectar cuando un usuario intenta descargar freeware e identificar a la persona por ID de usuario en la alerta. La alerta se podría enriquecer con información adicional de una tabla en la memoria que contiene detalles como nombre completo, cargo, ubicación de la oficina y número de empleado.

Una tabla en la memoria es ideal para manejar datos ligeros. Es fácil de configurar y requiere menos mantenimiento que una base de datos. Por ejemplo, AllTech Company es una organización pequeña y, por lo tanto, el administrador del sistema puede mantener la información de los empleados en un archivo .CSV. Si AllTech crece y se transforma en una empresa muy grande, el administrador tendría que configurar una referencia de base de datos externa como un enriquecimiento y asociar la base de datos a una regla.

Requisitos previos

El nombre de columna en el archivo .CSV no puede tener espacios en blanco.

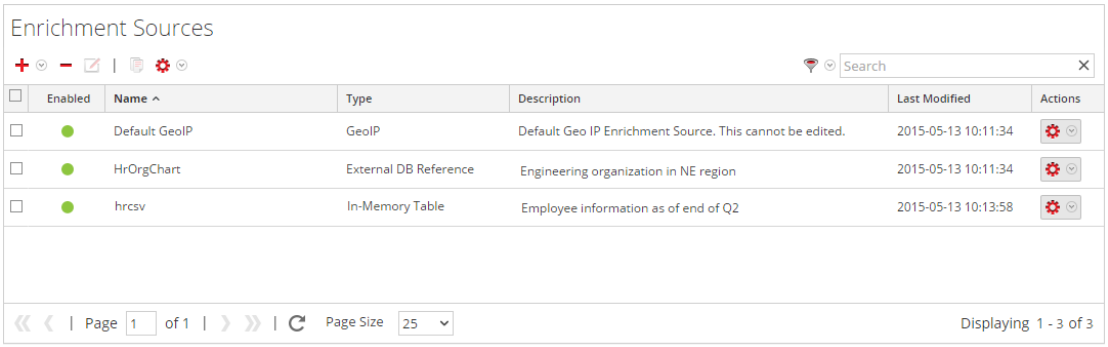
La primera línea del archivo .CSV debe tener el siguiente formato para cada columna:
name_of_column_1 type_of_column_1

Por ejemplo, estas tres columnas tienen el formato correcto:
Last_Name string
First_Name string
Phone integer

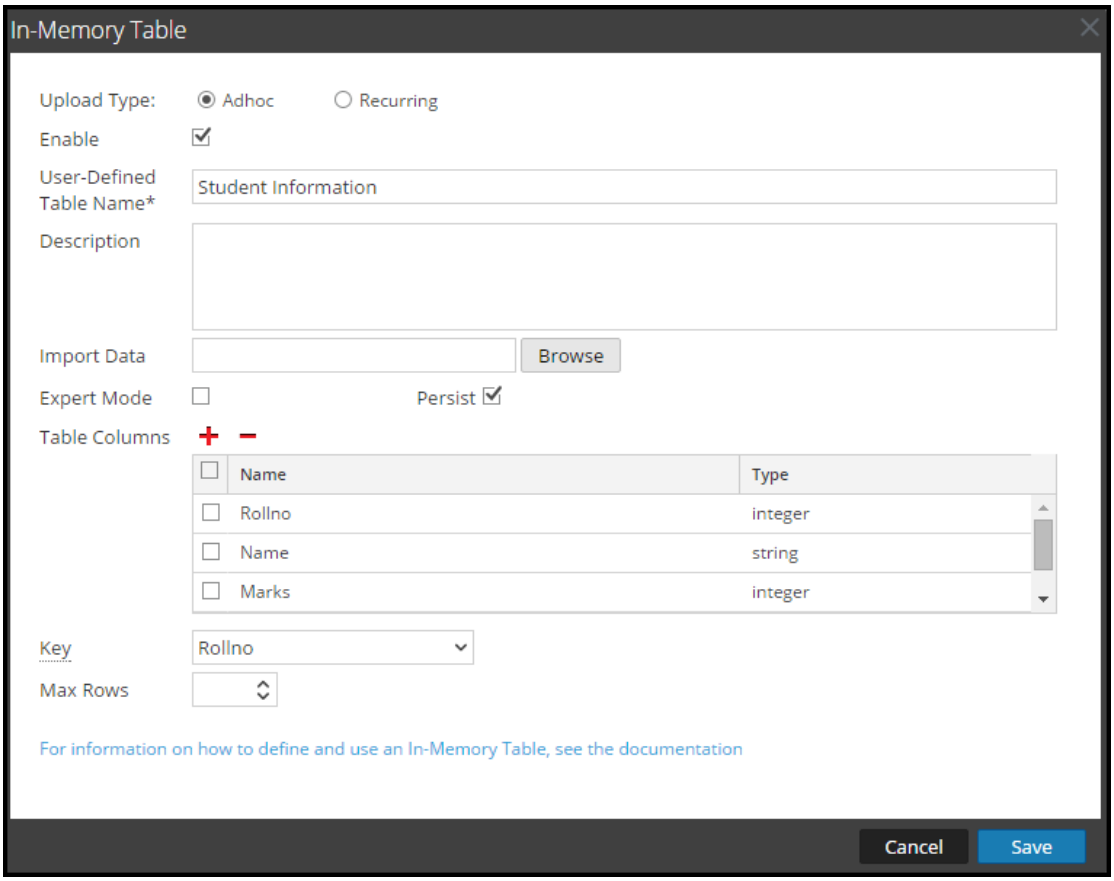
Procedimientos

Configurar una tabla en la memoria ad hoc

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   La vista Configurar se muestra con la pestaña Reglas abierta.
2. Haga clic en la pestaña **Configuración**.
3. En el panel de opciones, seleccione **Orígenes de enriquecimiento**.



4. En la sección **Orígenes de enriquecimiento**, haga clic en + > **Tabla en la memoria**.



5. Describa la tabla en la memoria:

   a. Seleccione **Ad hoc**.

   b. De manera predeterminada, la opción **Activar** está seleccionada. Cuando se agrega la tabla en la memoria a una regla, las alertas se enriquecen con datos de ella.
   Si agrega una tabla en la memoria a una regla, pero no desea que las alertas se enriquezcan, deseleccione la casilla de verificación.

   c. En el campo **Nombre de tabla definido por el usuario**, escriba un nombre para la configuración de la tabla en la memoria, como Información de estudiante.

   d. Si desea explicar lo que agrega el enriquecimiento a una alerta, escriba una **Descripción** como la siguiente:
   Cuando una alerta se agrupa por Rollno, este enriquecimiento agrega información de estudiantes, como el nombre y marcas.

6. En el campo **Importar datos**, seleccione el archivo .CSV que alimentará datos a la tabla en la memoria.

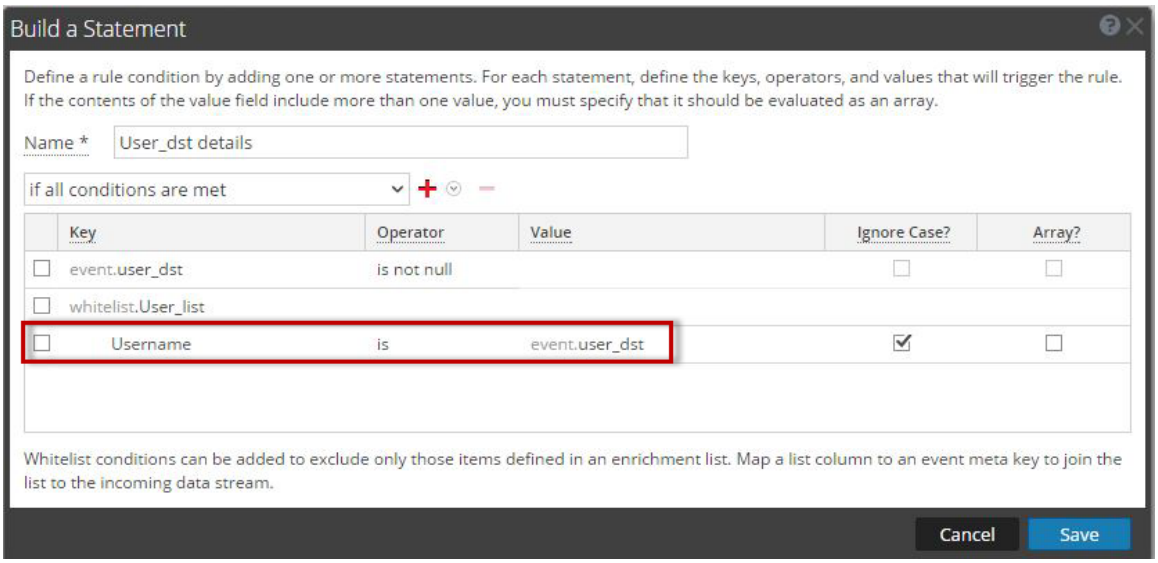
7. Si desea escribir una consulta de EPL para definir una configuración avanzada de la tabla en la memoria, seleccione Modo experto.
   Columnas de la tabla se reemplaza por un campo **Consulta**.
8. Seleccione Persistir para conservar la tabla en la memoria en disco cuando el servicio de ESA se detenga y para volver a completar la tabla cuandose reinicie.
9. En la sección **Columnas de la tabla**, haga clic en + para agregar columnas a la tabla en la memoria.
10. Si se selecciona un archivo válido en el campo Importar datos, las columnas se completan automáticamente.

Nota: si seleccionó Modo experto, se muestra un campo Consulta en lugar de Columnas de la tabla.

11. En el menú desplegable **Clave**, seleccione el campo que se usará como la clave predeterminada para unir eventos entrantes con la tabla en la memoria cuando se usa una tabla en la memoria basada en CSV como un enriquecimiento. De forma predeterminada, se selecciona la primera columna. También puede modificar posteriormente la clave cuando abra la tabla en la memoria en los orígenes de enriquecimiento.
12. En el menú desplegable **Máx. de filas**, seleccione la cantidad máxima de filas que pueden residir en la tabla en la memoria en una instancia específica.
13. Haga clic en **Guardar**.
    La tabla en la memoria ad hoc se configura. Puede agregarlo a la regla como un enriquecimiento o como parte de la condición de regla. Consulte Agregar un enriquecimiento a una regla.

Cuando agrega una tabla en la memoria, puede agregarla a una regla como un enriquecimiento o como parte de la condición de regla. Por ejemplo, la regla siguiente utiliza una tabla en la memoria como parte de la condición de regla para crear una lista blanca y también utiliza una tabla en la memoria de detalles en el archivo user_dst para enriquecer la alerta que se muestra.

La regla muestra la tabla en la memoria como una condición de regla de lista blanca:



A continuación, la alerta se enriquece con la tabla en la memoria User_list:

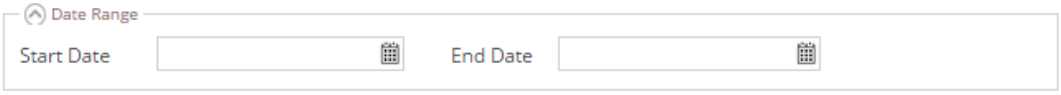
Por lo tanto, la tabla en la memoria user_dst se usa para crear una lista blanca y también para enriquecer los datos en la alerta si esta se activa.

Agregar una tabla en la memoria recurrente

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar.**
   La vista Configurar se muestra con la pestaña Reglas abierta.
2. Haga clic en la pestaña **Configuración**.
3. En el panel de opciones, seleccione **Orígenes de enriquecimiento**.
4. Haga clic en > **Tabla en la memoria**.
5. Describa la tabla en la memoria:
   a. Haga clic en **Periódica**.
   b. De manera predeterminada, la opción **Activar** está seleccionada. Cuando se agrega la tabla en la memoria a una regla, las alertas se enriquecen con datos de ella.
   Si agrega una tabla en la memoria a una regla, pero no desea que las alertas se enriquezcan, deseleccione la casilla de verificación.
   c. En el campo **Nombre de tabla definido por el usuario**, escriba un nombre para la configuración de la tabla en la memoria, como Información de estudiante.

d. Si desea explicar lo que agrega el enriquecimiento a una alerta, escriba una **Descripción** como la siguiente:
Cuando una alerta se agrupa por Rollno, este enriquecimiento agrega información del estudiante, como el nombre y las calificaciones.

6. Escriba la URL del archivo .CSV que alimentará datos en la tabla en la memoria. Haga clic en Verificar para validar el vínculo y completar las columnas del archivo .CSV. Puede agregar o eliminar columnas con el signo más o menos.
7. Si el servidor está configurado detrás de otro servidor, seleccione **Usar proxy**.
8. Si el servidor requiere credenciales de inicio de sesión, seleccione **Autenticado**
9. En **Repetir cada**, indique la frecuencia con que ESA debe comprobar el archivo .CSV más reciente:
   a. Seleccione Minuto(s), Hora(s), Día(s) o Semana.
   b. Si selecciona Semana, seleccione un día de la semana.
   c. Haga clic en **Rango de fechas** para seleccionar una **Fecha inicial** y una **Fecha de finalización** para el calendario recurrente.



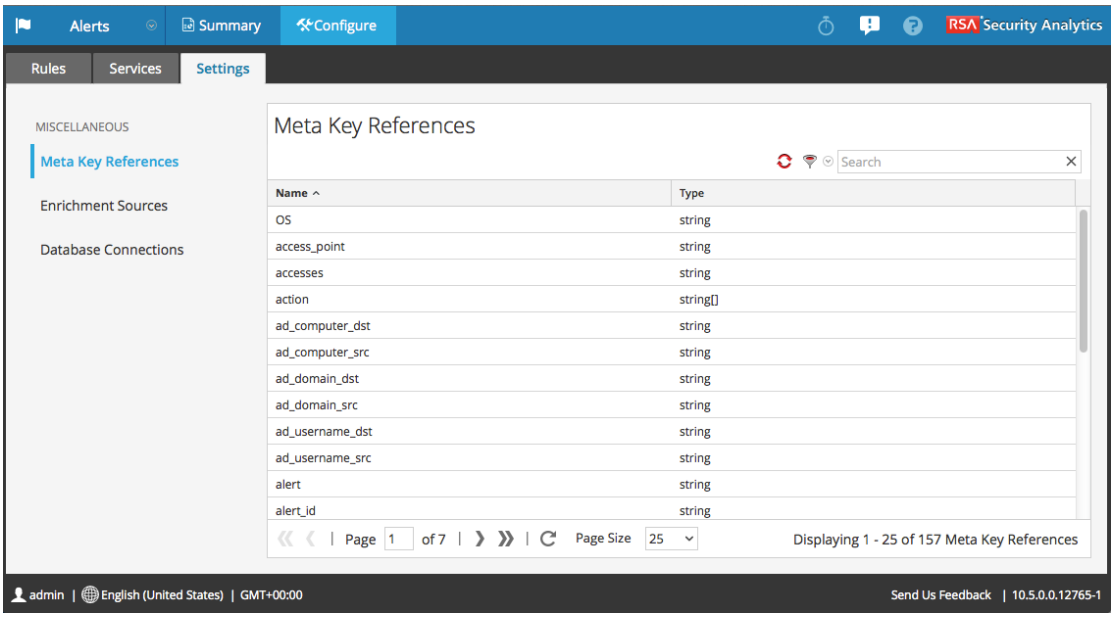
10. Seleccione **Persistir** para conservar la tabla en la memoria en disco cuando el servicio de ESA se detenga y para volver a completar la tabla cuando se reinicie.
11. En el menú desplegable **Clave**, seleccione el campo que se usará como la clave predeterminada para unir eventos entrantes con la tabla en la memoria cuando se usa una tabla en la memoria basada en CSV como un enriquecimiento. De forma predeterminada, se selecciona la primera columna. También puede modificar posteriormente la clave cuando abra la tabla en la memoria en los orígenes de enriquecimiento.
12. En el menú desplegable **Máx. de filas**, seleccione la cantidad de filas que pueden residir en la tabla en la memoria en una instancia específica.
13. Haga clic en **Guardar**.
La tabla en la memoria recurrente se configura. Puede agregarlo a la regla como un enriquecimiento o como parte de la condición de regla. Consulte Agregar un enriquecimiento a una regla.

Configurar Warehouse Analytics como origen de enriquecimiento

En este tema se proporcionan instrucciones para configurar RSA Warehouse Analytics como un origen de enriquecimiento para ESA. Los analistas de datos pueden aprovechar los datos de RSA Analytics Warehouse para analizar datos de sesiones y registros.

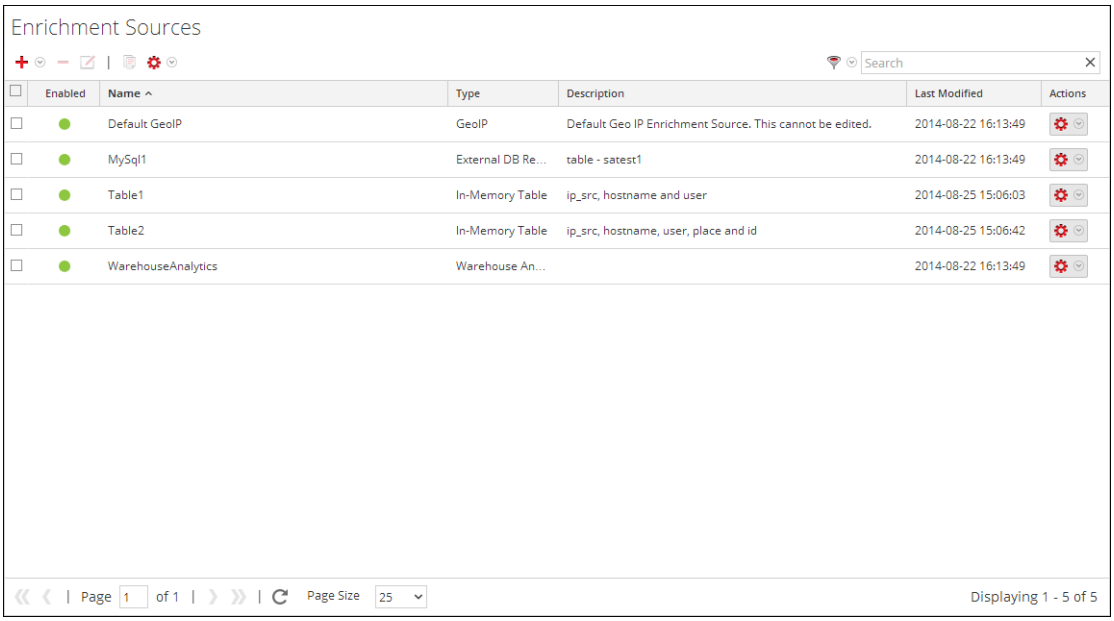
Para configurar Warehouse Analytics como un origen de enriquecimiento:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
2. Haga clic en la pestaña **Configuración**.

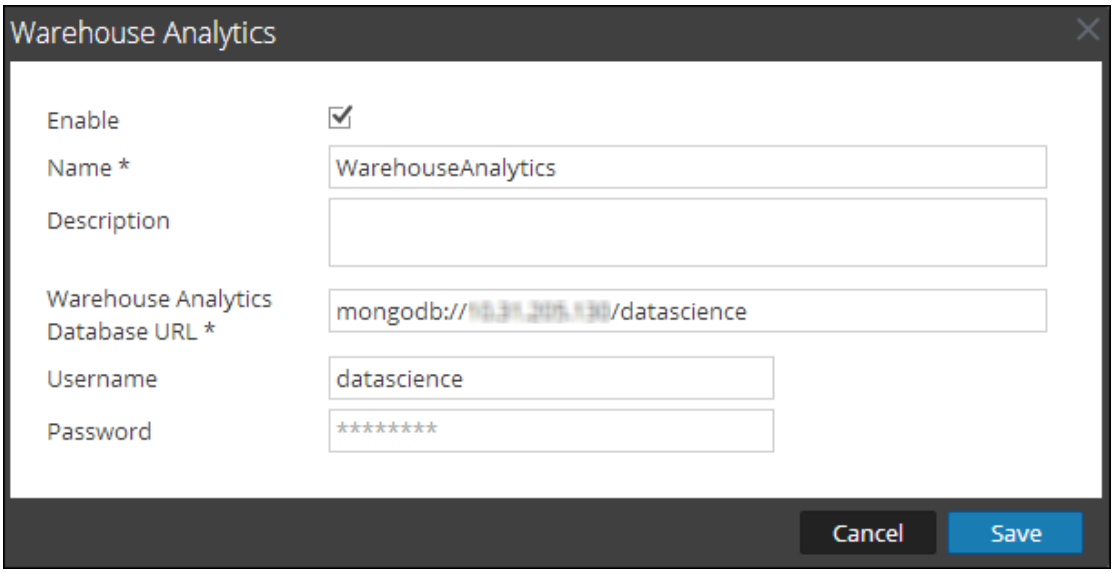


3. En el panel de opciones, seleccione **Orígenes de enriquecimiento**.

   Se muestra el panel Orígenes de enriquecimiento.



4. En el menú desplegable , seleccione **Warehouse Analytics**.



5. Seleccione **Habilitar** para enriquecer las alertas con datos adicionales. Esta opción está seleccionada de forma predeterminada. Si se deshabilita, las alertas no se enriquecen con datos adicionales.
6. En el campo **Nombre**, escriba un nombre que identifique o etiquete la configuración de Warehouse Analytics.
7. En el campo **Descripción**, escriba una descripción breve de la configuración de Warehouse Analytics.

8. En el campo **URL de base de datos de Warehouse Analytics**, escriba la URL de MongoDb a la base de datos de Warehouse Analytics.
9. En el campo **Nombre de usuario**, escriba el nombre de usuario para acceder a MongoDB.
10. En el campo **Contraseña**, escriba la contraseña para acceder a MongoDB.
11. Haga clic en **Guardar**.

Para obtener más información, consulte Pestaña Ajustes de configuración.

Agregar un enriquecimiento a una regla

En este tema se indica cómo agregar un origen de enriquecimiento configurado con anterioridad a una regla. Cuando ESA crea una alerta, la información del origen se incluye en ella.

La adición de un enriquecimiento a una regla permite solicitar búsquedas en diversos orígenes e incluir los resultados en las alertas salientes, con lo cual se obtiene una alerta más detallada. Este procedimiento requiere permisos de función para administrador, DPO y administrador del SOC.

Procedimiento

Para agregar un enriquecimiento a una regla:

1. En el menú desplegable de **Security Analytics**, seleccione **Alertas > Configurar**.
2. En la vista **Biblioteca de reglas**, realice una de las siguientes acciones:
   - Haga doble clic en una regla.
   - Seleccione una regla y haga clic en  en la barra de herramientas de la **Biblioteca de reglas**.

   El panel Generador de reglas se muestra en una nueva pestaña de Security Analytics.
3. En la sección **Enriquecimientos**, haga clic en  y seleccione cualquiera de los siguientes tipos de enriquecimientos:
   - Tabla en la memoria
   - Referencia de base de datos externa
   - Warehouse Analytics
   - GeoIP

- **Nota:** Si se usa un origen de GeoIP, ipv4 se completa automáticamente y no es editable.

Los tipos de enriquecimientos que seleccionó se muestran en la tabla.

4. Para el tipo de enriquecimiento agregado, realice lo siguiente:
   - En la columna **Salida**, seleccione el tipo que configuró.
   - En la lista desplegable **Origen de enriquecimiento**, seleccione el origen de enriquecimiento que definió.
   - En el campo **Metadatos de flujos de eventos de ESA**, escriba la clave de metadatos del flujo de eventos cuyo valor se usará como un operando de la condición de combinación.

   - En el campo **Nombre de columna de origen de enriquecimiento**, escriba el nombre de la columna del origen de enriquecimiento cuyo valor se usará como otro operando de la condición de combinación.
5. Seleccione **Depurar**. Esto agregará una anotación @Audit('stream') a la regla. Esto es útil al depurar las reglas de Esper.
6. Haga clic en **Mostrar sintaxis** para probar si la regla de ESA definida es válida.
7. Haga clic en **Guardar**.

Para obtener detalles de los parámetros y sus descripciones, consulte Pestaña Generador de reglas.

Implementar reglas para ejecutar en ESA

En este tema se explica cómo seleccionar un servicio de ESA y las reglas que se ejecutan en él. Se requieren los permisos de función administrador, administrador del SOC o DPO para todas las tareas de esta sección.

Para crear una implementación, debe realizar los pasos que se describen en Pasos de implementación

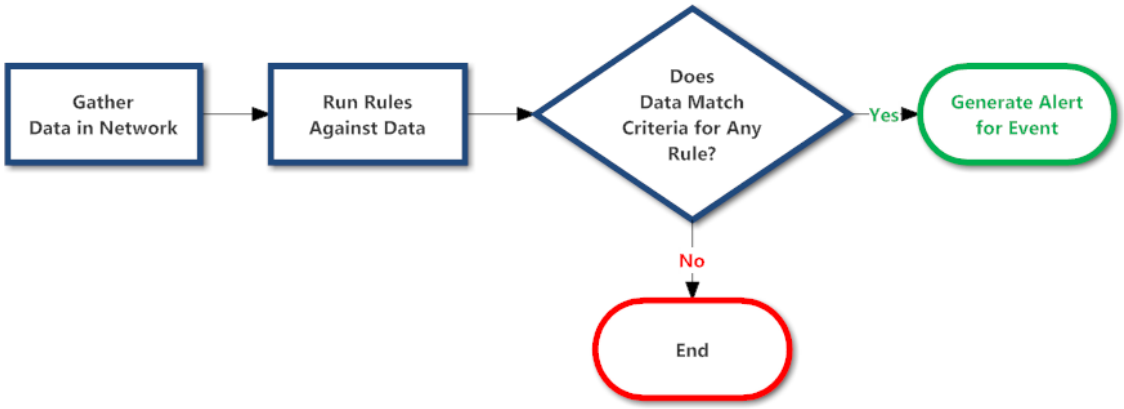
Cómo funciona la implementación

Una implementación consta de un servicio de ESA y un conjunto de reglas de ESA. Cuando implementa reglas, el servicio de ESA las ejecuta para detectar actividad sospechosa o indeseable en la red. Cada regla de ESA detecta un evento distinto, como cuando se crea una cuenta de usuario y se elimina en el plazo de una hora.

El servicio de ESA ejecuta las siguientes funciones:

1. Recopila **datos** en la red
2. Ejecuta **reglas** de ESA contra los datos
3. Aplica **criterios** de regla a los datos
4. Genera una **alerta** para el evento capturado

En el siguiente gráfico se muestra este flujo de trabajo:



Además, tal vez desee realizar otros pasos en la implementación, como eliminar un servicio ESA, editar o eliminar una regla, editar o eliminar una implementación o mostrar las actualizaciones en una implementación. Para obtener descripciones de estos procedimientos, consulte Procedimientos de implementación adicionales

Pasos de implementación

En este tema se explica cómo agregar una implementación que incluye un servicio de ESA y un conjunto de reglas de ESA. Puede agregar una implementación para organizar y administrar servicios y reglas de ESA. La implementación se puede considerar como un contenedor para ambos componentes:

1. Un servicio de ESA
2. Un conjunto de reglas de ESA

Por ejemplo, si agrega una implementación Actividad de spam, esta podría incluir ESA Londres y un conjunto de reglas de ESA para detectar actividad de correo electrónico sospechosa.

Para agregar una implementación, debe completar los siguientes procedimientos:

- Paso 1. Agregar una implementación
- Paso 2. Agregar un servicio de ESA
- Paso 3. Agregar e implementar reglas

Paso 1. Agregar una implementación

Requisitos previos

Para agregar una implementación, se requieren las siguientes acciones:

- El servicio de ESA se debe configurar en el host. Consulte “Configurar ESA” en la **Guía de configuración de Event Stream Analysis (ESA)**.
- Las reglas deben estar en la Biblioteca de reglas. Consulte Agregar reglas a la Biblioteca de reglas.

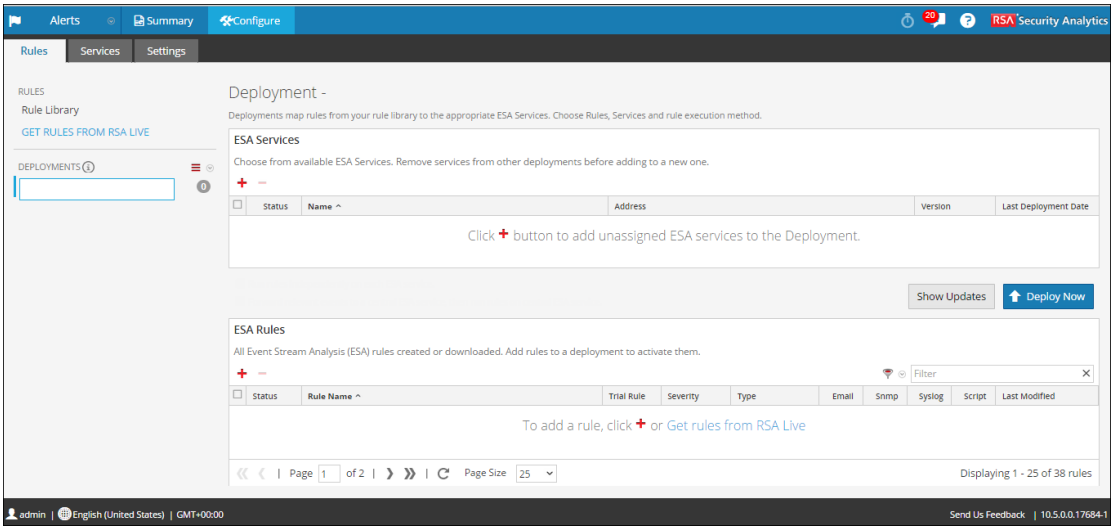
Procedimiento

Para agregar una implementación:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   Se muestra la pestaña Reglas.

2. En el panel de opciones, junto a Implementaciones, seleccione  > **Agregar**.

   La vista Implementación se muestra a la derecha.

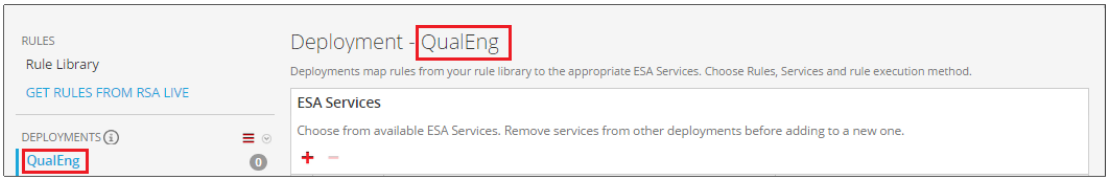


3. Escriba un **nombre** para la implementación. Usted decide la convención de asignación de nombres.

   Por ejemplo, podría indicar el propósito o identificar un propietario.

4. Presione **Enter**.

   La implementación se agrega.



Paso 2. Agregar un servicio de ESA

El servicio de ESA en una implementación recopila datos de la red y les aplica reglas de ESA. El objetivo es capturar eventos que coinciden con criterios de regla y, a continuación, generar una alerta para el evento capturado.

Puede agregar el mismo servicio ESA a múltiples implementaciones. Por ejemplo, ESA Londres podría estar simultáneamente en estas implementaciones:

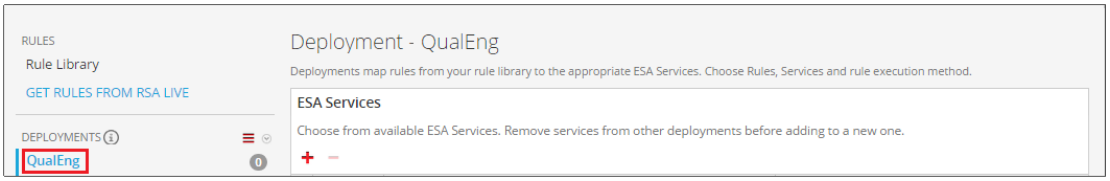
- Implementación EUR, que incluye un conjunto de reglas de ESA
- Implementación CORP, que incluye otro conjunto de reglas de ESA

Cuando elimina un servicio de ESA de una implementación, las reglas también se eliminan del servicio de ESA. Por ejemplo, la implementación EUR podría incluir a ESA Londres y un conjunto de 25 reglas. Si elimina ESA Londres de la implementación EUR, las 25 reglas también se eliminan de ESA Londres. Por lo tanto, si un servicio de ESA no forma parte de ninguna implementación, el servicio no tiene ninguna regla.

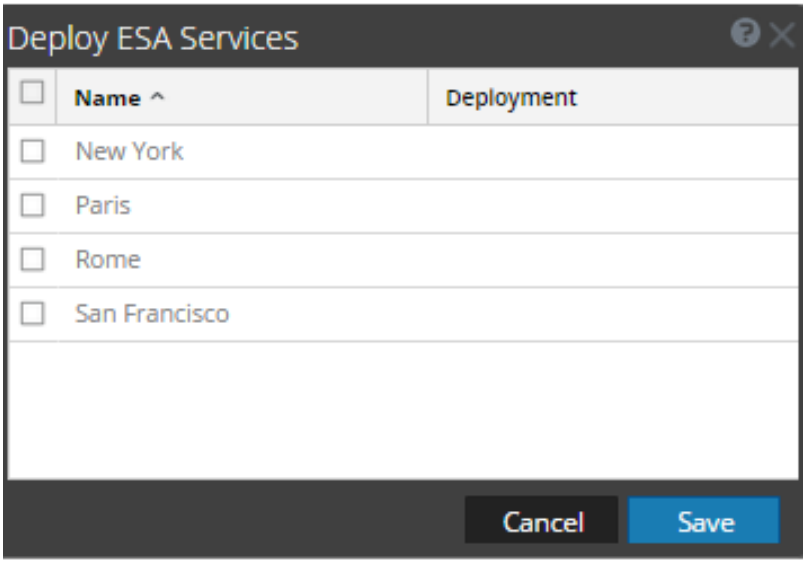
Procedimiento

Para agregar un servicio de ESA:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   Se muestra la pestaña Reglas.
2. En el panel de opciones, seleccione una **implementación**:



3. En la vista **Implementación**, haga clic en + en **Servicios de ESA**.
   El cuadro de diálogo Implementar servicios de ESA muestra cada servicio de ESA configurado.



4. Seleccione un servicio de ESA y haga clic en **Guardar**.
   Se muestra la vista Implementación. El servicio de ESA se muestra en la sección **Servicios de ESA** y su estado es Agregada.

Paso 3. Agregar e implementar reglas

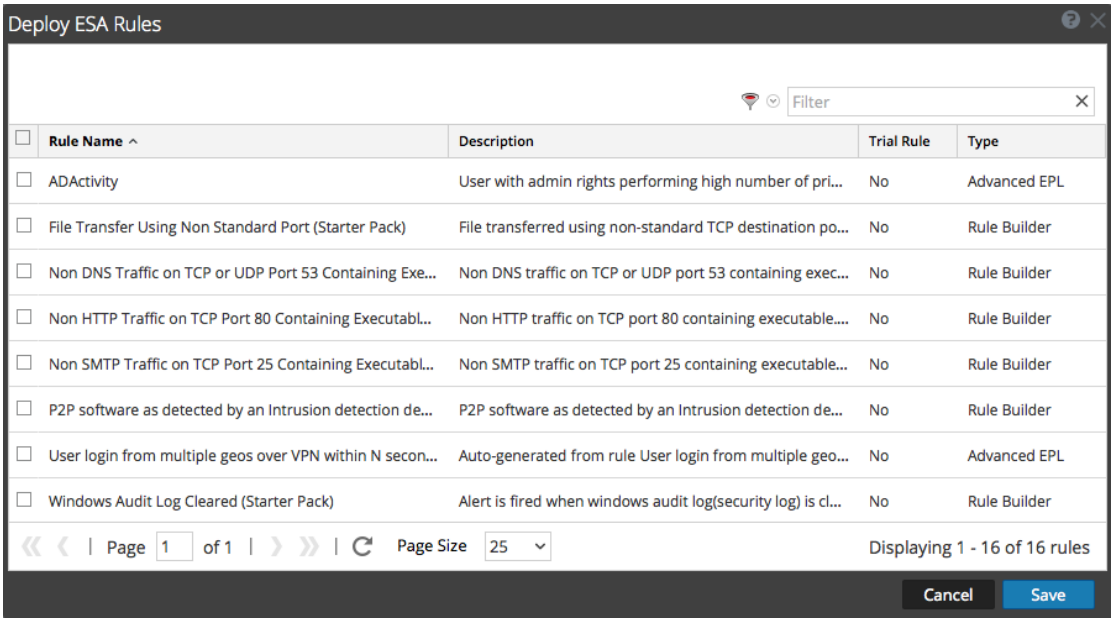
En este tema se explica cómo agregar reglas de ESA a una implementación y, a continuación, implementar las reglas en ESA. Cada regla de ESA tiene criterios únicos. Las reglas de ESA en una implementación determinan los eventos que captura ESA, lo cual, a la vez, determina las alertas que se reciben.

Por ejemplo, la implementación A incluye ESA París y, entre otros, una regla para detectar la transferencia de archivos a través de un puerto no estándar. Cuando ESA París detecta una transferencia de archivos que coincide con los criterios de regla, captura el evento y genera una alerta para él. Si elimina esta regla de la implementación A, ESA dejará de generar una alerta para dicha aparición.

Procedimiento

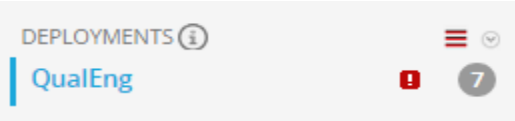
Para agregar e implementar reglas:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   Se muestra la pestaña Reglas.
2. En el panel de opciones, seleccione una implementación.
3. En la vista **Implementación**, haga clic en + en **Reglas de ESA**.
   Aparece el cuadro de diálogo Implementar reglas de ESA, el cual muestra cada regla en la Biblioteca de reglas:



4. Seleccione las reglas y haga clic en **Guardar**.
   Se muestra la vista Implementación.
5. Las reglas se enumeran en la sección Reglas de ESA.

- En la columna Estado, **Agregada** aparece junto a cada regla nueva.
- En la sección Implementaciones, indica que hay actualizaciones para la implementación.
- La cantidad total de reglas de la implementación aparece a la derecha.



6. Haga clic en **Implementar ahora**.
   El servicio de ESA ejecuta el conjunto de reglas.

Procedimientos de implementación adicionales

Además de implementar un servicio y reglas de ESA, tal vez desee realizar otros pasos en la implementación, como eliminar un servicio ESA, editar o eliminar una regla, editar o eliminar una implementación o mostrar las actualizaciones en una implementación.

Para realizar estos procedimientos, consulte:

- Eliminar un servicio de ESA en una implementación
- Editar o eliminar una regla en una implementación
- Editar o eliminar una implementación
- Mostrar actualizaciones a una implementación

Eliminar un servicio de ESA en una implementación

En este tema se proporcionan instrucciones para eliminar un servicio de ESA en una implementación. En una implementación con un servicio, puede editar las reglas que se aplican al servicio y eliminar el servicio de la implementación.

Cada uno de los siguientes procedimientos comienza en la pestaña Reglas.

Procedimiento

Para eliminar un servicio de ESA:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Reglas**.
   Se muestra la pestaña Reglas.
2. En el panel de opciones, bajo **Implementaciones**, seleccione una implementación.
3. En el panel **Servicios de ESA**, seleccione un servicio y haga clic en en la barra de herramientas.
   Se muestra un cuadro de diálogo de confirmación.
4. Haga clic en **Sí**.
   El servicio se elimina.

Editar o eliminar una regla en una implementación

En una implementación con reglas, puede editar y eliminar reglas para personalizar la implementación. Cada uno de los siguientes procedimientos comienza en la pestaña Reglas.

Procedimientos

Editar una regla

1. En el menú de Security Analytics, seleccione Alertas > Configurar > Reglas.
   Se muestra la pestaña Reglas.
2. En el panel de opciones, bajo Implementaciones, seleccione una implementación.
3. En el panel **Reglas de ESA**, haga doble clic en una regla para abrirla en una nueva pestaña de Security Analytics.
4. Modifique la regla y haga clic en **Aplicar**.
   La regla se guarda.

Eliminar una regla

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Reglas**.
   Se muestra la pestaña Reglas.
2. En el panel de opciones, bajo **Implementaciones**, seleccione una implementación.
3. En el panel **Reglas de ESA**, seleccione una regla y haga clic en en la barra de herramientas.
   Se muestra un cuadro de diálogo de confirmación.
4. Haga clic en **Sí**.
   La regla se elimina.

Editar o eliminar una implementación

En este tema se explica la forma en que Security Analytics reenvía una regla de correlación a cada servicio ESA en un grupo de correlación. En un grupo de correlación, cada servicio de ESA debe ejecutar el mismo conjunto de reglas. Cuando agrega una regla a un grupo de correlación, Security Analytics la reenvía a cada ESA del grupo.

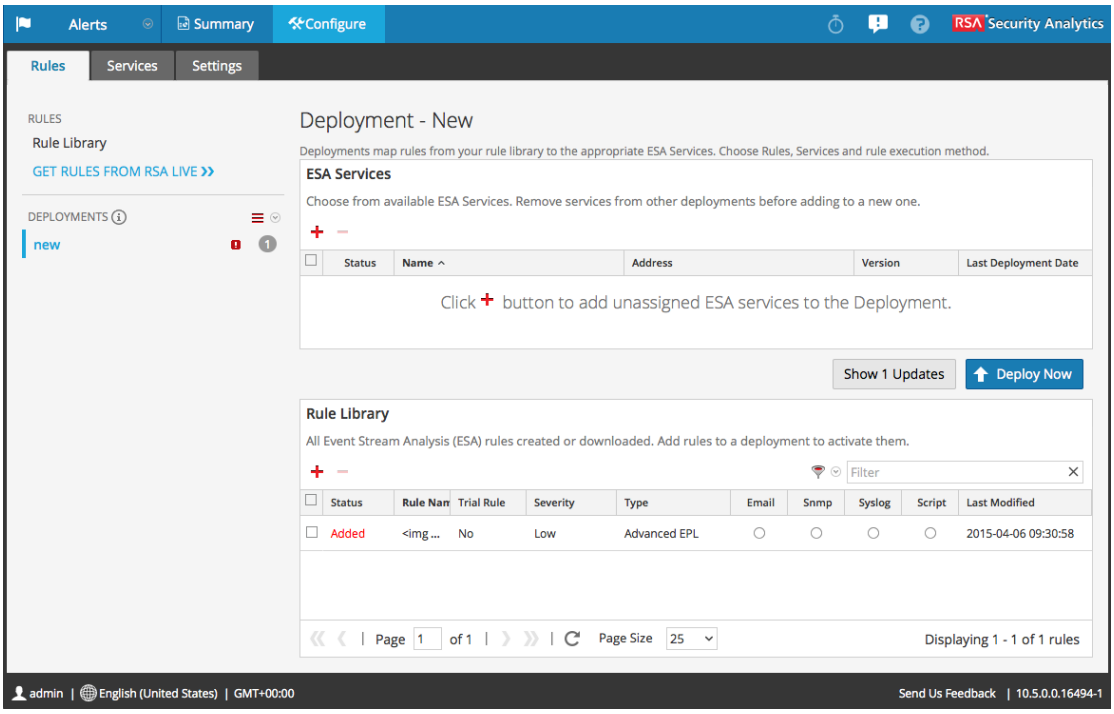
Para acceder a las implementaciones:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.

   La vista Configurar se muestra con la pestaña Reglas abierta.

2. En el panel de opciones, bajo **Implementaciones**, seleccione una implementación.

   Se muestra la vista Implementación.



Editar una implementación

1. En el panel de opciones, bajo **Implementaciones**, seleccione una implementación.

   Se muestra la vista Implementación.

2. Seleccione  **> Editar**.

   El nombre de la implementación queda disponible para su edición.

Eliminar una implementación

1. En el panel de opciones, bajo **Implementaciones**, seleccione una implementación.

   Se muestra la vista Implementación.

2. Seleccione  > **Eliminar**.

   Se muestra un cuadro de diálogo de confirmación.

3. Haga clic en **Sí**.

   La implementación se elimina.

Mostrar actualizaciones a una implementación

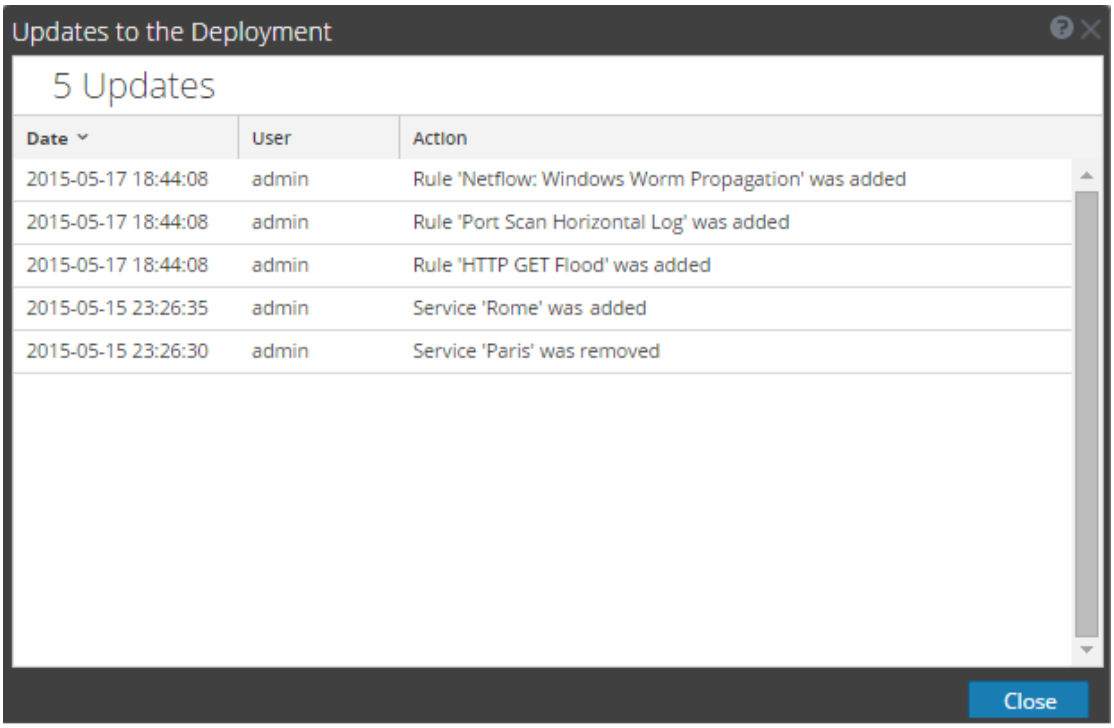
En este tema se explica cómo mostrar actualizaciones, como la adición o la eliminación de reglas, en una implementación. Cuando hace un cambio en una implementación, el ícono de actualización () aparece junto al nombre de la implementación.

Procedimiento

Para mostrar las actualizaciones a una implementación:

1. En el menú de Security Analytics, seleccione Alertas > Configurar.
   Se muestra la pestaña Reglas.

2. En el panel de opciones, bajo **Implementaciones**, haga clic en **Mostrar actualizaciones** en el extremo derecho.



3. Haga clic en **Close**.

Ver estadísticas y alertas de ESA

Cuando ESA genera alertas, puede ver detalles acerca del desempeño de las reglas, como estadísticas sobre el motor, la regla y la alerta, así como información sobre las reglas que están habilitadas o deshabilitadas. Para obtener instrucciones sobre la visualización de estadísticas de ESA, consulte Ver estadísticas del servicio de ESA

Cuando ESA genera alertas, puede ver los resultados en la página Resumen de alertas. Esto le permite ver tendencias y comprender el volumen y la frecuencia de las alertas. Para obtener instrucciones sobre la visualización de alertas, consulte Ver un resumen de alertas

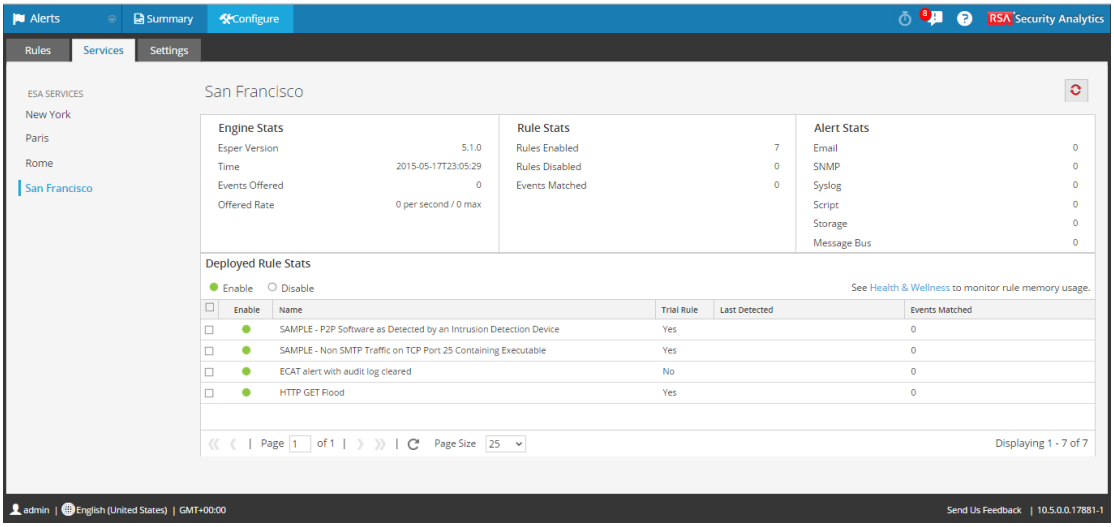
Ver estadísticas del servicio de ESA

En este tema se describe cómo ver las estadísticas de implementación para un servicio de ESA. Este procedimiento es útil cuando se intenta determinar la eficacia de una regla o solucionar problemas de una implementación.

Procedimientos

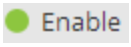
Ver estadísticas de ESA

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar > Servicios**.
2. En la lista **Servicios de ESA** de la izquierda, seleccione un servicio.
   Se muestran las estadísticas de implementación del servicio seleccionado.



3. Revise las siguientes secciones de las estadísticas de ESA.
   Para obtener una descripción completa de cada estadística en cada sección, consulte Pestaña Servicios.
   - **Estadísticas de motor**
   - **Estadísticas de reglas**
   - **Estadísticas de alerta**
4. En las Estadísticas de reglas implementadas, revise los detalles de las reglas implementadas en ESA.
   Para obtener una descripción completa de cada columna en cada sección, consulte Pestaña Servicios.
   - Si la regla está habilitada o inhabilitada
   - El nombre de la regla
   - Si la regla se está ejecutando en modo de regla de prueba
   - La última detección
   - Eventos con coincidencias
5. Para obtener un snapshot de la memoria de la regla, haga clic en **Estado y condición**.

Habilitar e inhabilitar reglas

1. En el panel **Estadísticas de reglas implementadas**, seleccione una regla en la cuadrícula.
2. Haga clic en 

para habilitar la regla o en 

para inhabilitarla.

   La pestaña Servicios se actualiza para mostrar los cambios, los cuales se aplican de inmediato.

Actualizar las estadísticas

La pestaña Servicios no actualiza las estadísticas automáticamente, a menos que se habilite o se inhabilite una regla. Para comprobar que ve las estadísticas actuales:

1. Haga clic en  en la esquina superior derecha para actualizar la información.
2. Vea la información actualizada.

Ver un resumen de alertas

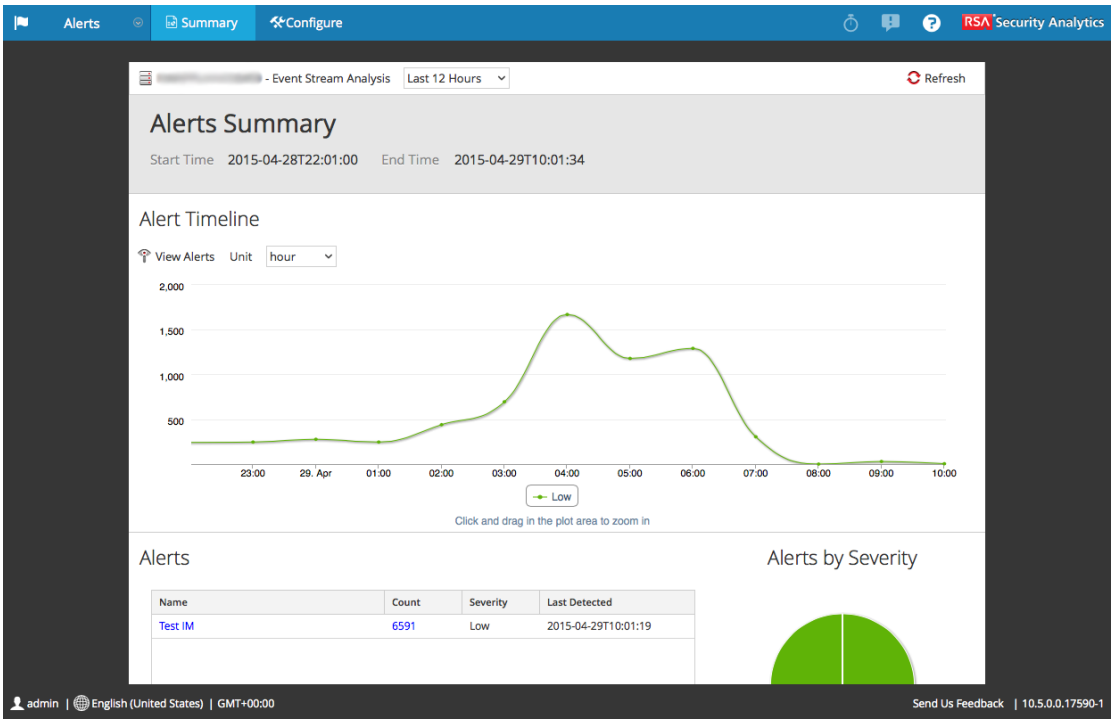
En este tema se describe cómo ver un resumen de alertas. Puede obtener una vista consolidada de alertas generadas en un rango de tiempo específico.

Procedimiento

Para ver un resumen de alertas:

1. En el menú de **Security Analytics**, seleccione **Alertas > Resumen**.

   Si hay un servicio de ESA predeterminado, la vista Resumen se muestra con la información de ese servicio.



   Si no se seleccionó ningún servicio predeterminado, se muestra el cuadro de diálogo Seleccionar un servicio de ESA.

2. En el cuadro de diálogo **Seleccionar un servicio de ESA**, elija un servicio y haga clic en **Seleccionar**.

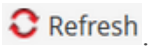
   Se muestra la vista Resumen.

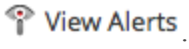
3. Para elegir un nuevo servicio para ver:

   a. Haga clic en  .

      Se muestra el cuadro de diálogo Seleccionar un servicio de ESA.

b. Elija un servicio de la lista y haga clic en **Seleccionar**.
   La vista Resumen se muestra con la información del servicio seleccionado.

4. Para elegir el intervalo de tiempo del resumen, abra el menú desplegable **Rango de tiempo** y seleccione un rango de tiempo.
   Los campos Hora de inicio y Hora de finalización reflejan el nuevo rango.
5. Para elegir el cronograma, abra el menú desplegable **Unidad** y seleccione una unidad de tiempo.
6. Para actualizar la información de la vista Resumen, haga clic en 

.
7. Para ver las alertas en una lista, haga clic en 

.

Para obtener más información, consulte Vista Resumen de alertas.

Detección de amenazas automatizadas

En este tema se explica cómo configurar y utilizar la detección de amenazas automatizadas. La detección de amenazas automatizadas es un servicio que se implementa en la instalación de ESA y que examina el tráfico HTTP para determinar la probabilidad de que exista actividad maliciosa en su ambiente.

Para obtener detalles sobre cómo trabajar con la detección de amenazas automatizadas, consulte los siguientes temas:

- Configurar la detección de amenazas automatizadas
- Trabajar con resultados de detección de amenazas automatizadas
- Solucionar problemas de detección de amenazas automatizadas

Nociones básicas sobre la detección de amenazas automatizadas

En este tema se proporciona una descripción general de la detección de amenazas automatizadas. La detección de amenazas automatizadas es un servicio que se implementa en ESA. Analítica del comportamiento: El módulo Dominios sospechosos examina el tráfico HTTP para detectar dominios que posiblemente se traten de servidores de control y comando de malware que se conectan a su ambiente. Una vez que la detección de amenazas automatizadas examina el tráfico HTTP, genera puntajes según diversos aspectos del comportamiento del tráfico (como la frecuencia y la regularidad con las cuales se establece contacto con un dominio determinado). Si estos puntajes alcanzan un umbral establecido, se genera una alerta de ESA. Esta alerta de ESA también activa una alerta en el administrador de incidentes. La alerta en el administrador de incidentes se enriquece con datos que ayudan a interpretar los puntajes para determinar los pasos de moderación que se deben seguir.

Esta versión de detección de amenazas automatizadas proporciona puntuación para detectar las comunicaciones de comando y control. Las comunicaciones de comando y control se producen cuando el malware ha puesto en riesgo un sistema y envía datos a un origen. A menudo, el malware de comando y control se puede detectar a través de un comportamiento de Beacon. La señalización ocurre cuando el malware envía comunicaciones al servidor de comando y control para informarle que se ha puesto en riesgo una máquina y que espera más instrucciones. La capacidad de detectar el malware en esta etapa de riesgo puede evitar que se produzcan daños a la máquina en riesgo y se considera una etapa crítica en la “cadena de ataques”.

Esta función resuelve varios problemas comunes que se producen cuando se busca malware:

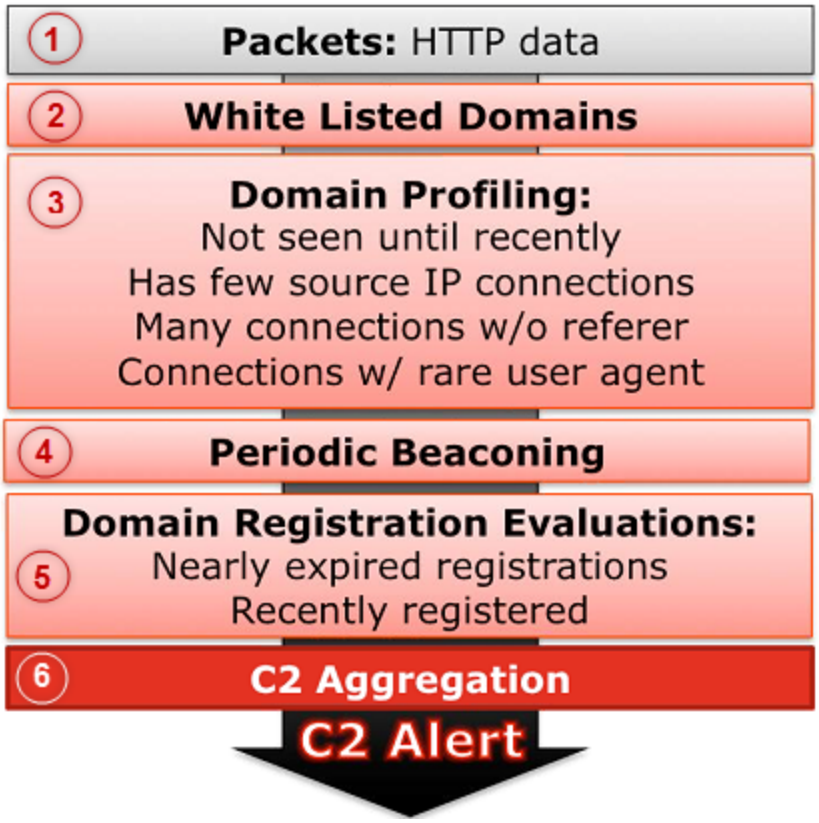
- **Capacidad de usar algoritmos en lugar de firmas**. Debido a que muchos creadores de malware han comenzado a usar segmentos de código polimórfico o cifrado para los cuales es muy difícil crear una firma, es posible que en ocasiones este enfoque no detecte el malware.

Debido a que la detección de amenazas automatizadas usa un algoritmo basado en comportamiento, puede detectar malware de forma más rápida y eficaz.

- **Capacidad de automatizar la búsqueda.** La búsqueda manual en los datos es un método eficaz de encontrar malware, pero también es extremadamente lento. La automatización de este proceso permite que un analista use su tiempo con mayor eficacia.
- **Capacidad de buscar un ataque rápidamente**. En lugar de la creación de lotes y el posterior análisis de los datos, Detección de amenazas automatizadas los analiza a medida que Security Analytics los recopila, lo cual permite la detección de los ataques casi en tiempo real.

Flujo de trabajo

La detección de amenazas automatizadas funciona de manera muy similar a un sistema de filtrado. Comprueba si se produce un comportamiento determinado (o si existen ciertas condiciones) y, si se produce ese comportamiento o condición, continúa con el paso siguiente del proceso. Esto ayuda a hacer que el sistema sea eficiente y libera recursos, de modo que los eventos que no se consideran amenazas no se mantengan en la memoria. En el siguiente diagrama se proporciona una versión simplificada del flujo de trabajo.



1.) **Los paquetes HTTP se enrutan a ESA**. Los paquetes HTTP se analizan en el Decoder y se envían al dispositivo de ESA.

2.) **Se comprueba la lista blanca**. Si creó una lista blanca mediante Context Hub, ESA comprueba esta lista para descartar dominios. Si un dominio del evento está en la lista blanca, se ignora el evento.

3.) **Se comprueba el perfil de dominio**. La detección de amenazas automatizadas comprueba si el dominio se vio recientemente (aproximadamente tres días), si tiene pocas conexiones de IP de origen, muchas conexiones sin un remitente o conexiones con un agente de usuario poco frecuente. Si una o varias de estas condiciones son verdaderas, se comprueba el Beacon periódico en el dominio. Para obtener una descripción detallada de estos puntajes de perfil de dominio, consulte "Trabajar con puntajes de detección de amenazas automatizadas".

4.) **Se comprueba el Beacon periódico del dominio**. El proceso de Beacon ocurre cuando el malware envía comunicaciones periódicas al servidor de comando y control para informarle que se ha puesto en riesgo una máquina y que espera más instrucciones. Si el sitio muestra un comportamiento de Beacon, se comprueba la información de registro del dominio.

5.) **Se comprueba la información de registro del dominio**. Se usa el servicio Whois para ver si el dominio se registró recientemente o si está por vencer. Los dominios que poseen una vida útil muy breve a menudo son aspectos distintivos del malware.

6.) **Puntajes de agregado de comando y control (C2)** . Cada uno de los factores anteriores genera un puntaje independiente, el cual se pondera para denotar diversos niveles de importancia. Los puntajes ponderados determinan si se debe generar una alerta. Si se genera una alerta, las alertas agregadas aparecen en el administrador de incidentes y se pueden investigar adicionalmente desde ahí. Una vez que las alertas comienzan a aparecer en el administrador de incidentes, continúan agregándose bajo el incidente asociado. Esto facilita ordenar los volúmenes de alertas que pueden generarse para un incidente de comando y control.

Si es un analista, puede ver las alertas generadas en el módulo Resumen de alertas o en el módulo del administrador de incidentes. Si utiliza SecOps, puede ver las alertas en SecOps, versiones 1.2 y 1.3.

Configurar la detección de amenazas automatizadas

En este tema se indica a los administradores y analistas cómo configurar y trabajar con detección de amenazas automatizadas.

Este procedimiento proporciona los pasos necesarios para configurar la detección de amenazas automatizadas en ESA. Sin embargo, antes de habilitar la detección de amenazas automatizadas, es importante destacar que hay muchas configuraciones de instalación posibles que se pueden instalar en ESA, incluidas las siguientes: Detección de amenazas automatizadas, reglas de ESA y Context Hub. Cada uno de estos puede ocupar recursos, por lo que es importante considerar el dimensionamiento antes de habilitar esta función en ESA.

Requisitos previos

Debe haber configurado un Decoder para datos de paquete HTTP.

Debe haber configurado un analizador Lua o Flex HTTP.

Para obtener mejor rendimiento, habilite el servicio Context Hub. Esto permite crear una lista blanca.

Procedimiento: Configuración de detección de amenazas automatizadas

Este procedimiento proporciona los pasos necesarios para configurar la detección de amenazas automatizadas.

Los pasos básicos necesarios son:

1. **Configurar los ajustes de WhoIs**. El servicio Whois permite obtener datos exactos acerca de los dominios a los cuales se conecta. A fin de garantizar un puntaje eficaz, es importante configurar los ajustes del servicio Whois.
2. **Crear una lista blanca (opcional) mediante el servicio Context Hub**. La creación de una lista blanca permite garantizar que los sitios web de acceso frecuente se excluyan del puntaje de la detección de amenazas automatizadas.
3. **Habilitar la detección de amenazas automatizadas para el ESA especificado**. Debe habilitar la detección de amenazas automatizadas para cada ESA donde desea ejecutar el servicio.
4. **Permitir una preparación de 24 horas y habilitar la regla del administrador de incidentes de C2**. Cuando se usa la detección de amenazas automatizadas, la preparación del algoritmo de puntaje demora aproximadamente 24 horas. Después de 24 horas, se habilita la regla C2 en el administrador de incidentes.

Paso 1: Configurar los ajustes del servicio WhoIs para ESA

Los ajustes se configuran para permitir que ESA se conecte al servicio Whois. Esto permite que el servicio de ESA obtenga información detallada sobre el dominio que activa el puntaje de detección de amenazas automatizadas.

1. En Administration > Servicios, seleccione el servicio ESA y elija  > Ver > Explorar.
2. En el explorador, haga clic en **Servicio** > **Whois** > **whoisClient.**
3. Configure los siguientes ajustes (tenga en cuenta que solo es necesario modificar los primeros dos parámetros. RSA recomienda usar los ajustes predeterminados para otros parámetros):

Parámetro	Descripción
whoisUserId	**Se requiere lo siguiente:** Ingrese la credencial de autenticación para el servidor Whois de RSA. Es igual que el ID de usuario de RSA Live. Si no ha configurado una cuenta de RSA Live, deberá hacerlo. El valor predeterminado es "whois".
whoisPassword	**Se requiere lo siguiente:** Ingrese la credencial de autenticación para el servidor Whois de RSA. Es igual que la contraseña de RSA Live. Si no ha configurado una cuenta de RSA Live, deberá hacerlo. El valor predeterminado es nulo.
whoisUrl	**Opcional:** Ingrese la URL para obtener datos de Whois desde el servicio Whois de RSA. Tenga en cuenta que se requiere la barra diagonal final (“/”). De lo contrario, se producirá un error en las solicitudes. El valor predeterminado es: **“**https://cms.netwitness.com/whois/query/**”**
whoisAuthUrl	**Opcional:** Ingrese la URL para obtener los tokens de autenticación del servicio Whois de RSA. El valor predeterminado es: **“** https://cms.netwitness.com/authlive/authenticate/WHOIS**”**
whoisAuthTokenLifespanSeconds	**Opcional:** Ingrese la hora, en segundos, después de la cual se debe renovar un token de autenticación. El valor predeterminado es 3300.
whoisHttpsProxy	**Opcional:** Si las solicitudes de HTTP requieren un proxy, configúrelo en el mismo valor que se utiliza para el servicio RSA Live. Solo debe usar este parámetro cuando **insecureConnection** está configurado en **verdadero**. El valor predeterminado es falso. (Requiere el reinicio de ESA).

Parámetro	Descripción
insecureConnection	**Opcional:** Configure este parámetro en **verdadero** para permitir que la solicitud HTTP para el servicio Whois de RSA omita los certificados de SSL. **Nota:** Si se accede al servicio Whois de RSA mediante un proxy, este parámetro se debe configurar en **verdadero**. El valor predeterminado es falso. (Requiere el reinicio de ESA).
allowedRequests	**Opcional:** Especifique cuántas consultas desea permitir antes de comenzar a regular el servicio Whois. Este parámetro funciona con allowedRequestsIntervalSeconds, donde se define el intervalo de consultas. Por ejemplo, si configura **allowedRequests** en 100 y **allowedRequestsIntervalSeconds** en 60, se permiten 100 solicitudes en un intervalo de 60 segundos. El valor predeterminado es 100. (Requiere el reinicio de ESA).
allowedRequestsIntervalSeconds	**Opcional:** Si configura el parámetro **allowedRequests**, también debe configurar este ajuste para determinar el intervalo. Este valor debe ajustarse para su ambiente. La configuración predeterminada es 60 segundos. (Requiere el reinicio de ESA).
queueMaxSize	**Opcional:** Especifique el tamaño máximo de la línea de espera de los dominios cuya información se solicitará al servicio Whois de RSA. El valor predeterminado es 100,000.
cacheMaxSize	**Opcional:** Especifique la cantidad máxima de entradas de Whois almacenadas en caché. Una vez que se alcance este límite, se quitará la entrada menos usada recientemente para dar espacio a una nueva entrada. El valor predeterminado es 50,000. (Requiere el reinicio de ESA).

Parámetro	Descripción
refreshIntervalSeconds	**Opcional**: Especifique la cantidad de segundos del intervalo de actualización. Si la información de Whois solicitada se encuentra en la caché y la entrada de la caché superó la cantidad de segundos de permanencia especificada, la entrada se quita de la caché y el dominio vuelve a la línea de espera para su consulta. (La entrada de la caché vuelve a la solicitud que la identifica como obsoleta). La configuración predeterminada es 2,592,000 segundos (30 días).
waitForHTTPRequest	**Opcional:** Requiere que ESA espere hasta que el servicio Whois responda antes de que complete la ejecución del EPL. Esto garantiza que los datos de Whois siempre se incluyan en los resultados, pero puede afectar negativamente el rendimiento debido a que el ESA queda en pausa hasta 30 segundos a la espera de la respuesta del servicio Whois. Si no configura este ajuste y el tiempo de respuesta es lento, ESA completa la ejecución del análisis de un evento determinado sin los datos de Whois y calcula el puntaje sin ellos. La configuración predeterminada es **verdadero**.

Paso 2: Crear una lista blanca de dominios (opcional)

Nota: Este paso es opcional: Si utiliza el administrador de incidentes para administrar estos incidentes, también puede crear una lista blanca mediante el cierre de un incidente como falso positivo.

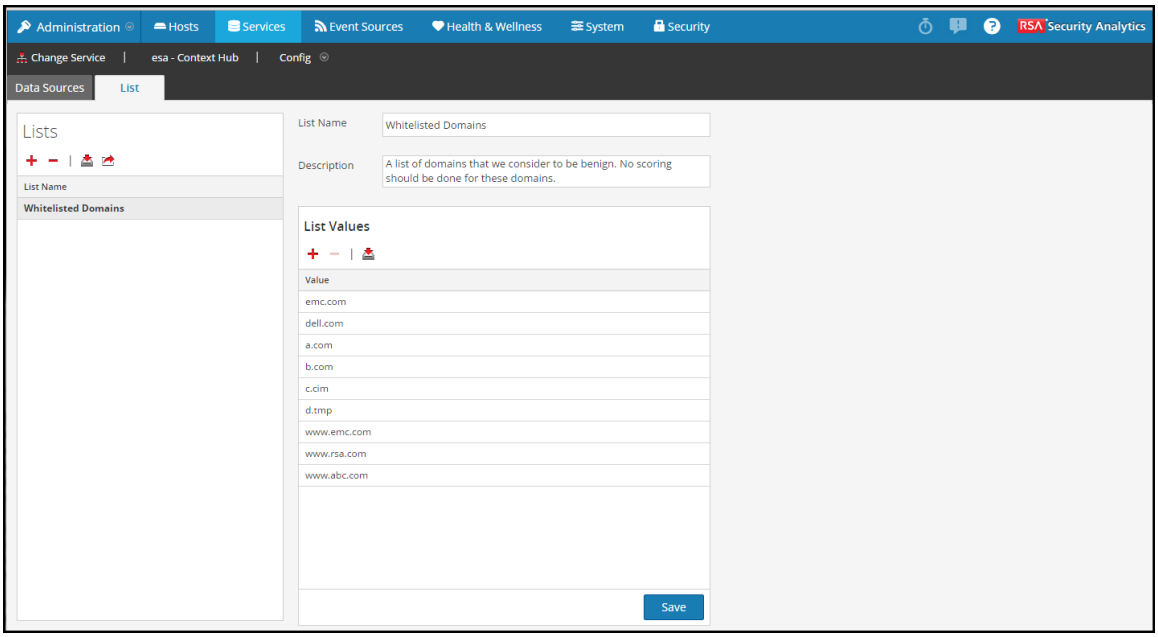
Este procedimiento se utiliza cuando se trabaja con detección de amenazas automatizadas a fin de garantizar que determinados dominios no activen un puntaje de amenazas. En ocasiones, un dominio al que se accede habitualmente puede activar un puntaje de detección de amenazas automatizadas. Por ejemplo, un servicio de clima podría tener un comportamiento de Beacon similar a una comunicación de comando y control, razón por la cual se activaría un puntaje negativo no justificado. Cuando sucede, esto se denomina un falso positivo. Para impedir la activación de un falso positivo con un dominio específico puede agregar el dominio a una lista blanca. La mayoría de los dominios no necesita estar en una lista blanca, porque la solución solo alerta sobre comportamientos muy sospechosos. Los dominios que tal vez desee incluir en la lista blanca son servicios automatizados válidos a los cuales se conectan unos pocos hosts.

Nota: Solo puede tener una instancia del servicio Context Hub habilitada en su implementación de Security Analytics. Si su servicio Context Hub se ejecuta en otro ESA, debe configurarlo para que se conecte al ESA que ejecuta el servicio Context Hub. Para obtener instrucciones, consulte "Configurar un ESA para que se conecte a Context Hub en otro ESA" en la **Guía de configuración de Event Stream Analysis**.

1. Desde el servicio Context Hub, puede crear una lista y agregar dominios manualmente o puede cargar un archivo. CSV que contenga una lista de dominios.
   a. En Administration > Servicios, seleccione el Context Hub.
   b. Seleccione el Context Hub y luego  Ver > **Configurar**.
   c. Seleccione la pestaña **Lista** para abrir las listas para su edición.
   d. En el panel izquierdo, haga clic en  para agregar una lista. Ingrese un nombre para la lista y, a continuación, agregue dominios manualmente, para lo cual debe hacer clic en  en el panel derecho.

Precaución: La lista blanca debe denominarse *Dominios en lista blanca.* De lo contrario, Context Hub no podrá procesarla como una lista blanca.

   e. O bien, para importar un archivo .CSV, haga clic en  y, en el cuadro de diálogo Importar archivo, vaya al archivo .CSV. Tenga en cuenta que el archivo debe denominarse *Dominios en lista blanca*. Elija entre los siguientes delimitadores: Coma, LF (salto de línea) y CR (retorno de carro), según cómo separa los valores en el archivo. A continuación, haga clic en **Cargar**.
   f. Desde el servicio Context Hub, también puede modificar una lista blanca existente para agregar o quitar un dominio.
   g. En el panel derecho, la opción **Lista** muestra la lista blanca de dominios existente.
   h. Haga clic en **Dominios en lista blanca**. Los valores de la lista blanca se muestran en el panel derecho.



i. Para agregar un dominio, haga clic en + e ingrese el nombre del dominio.

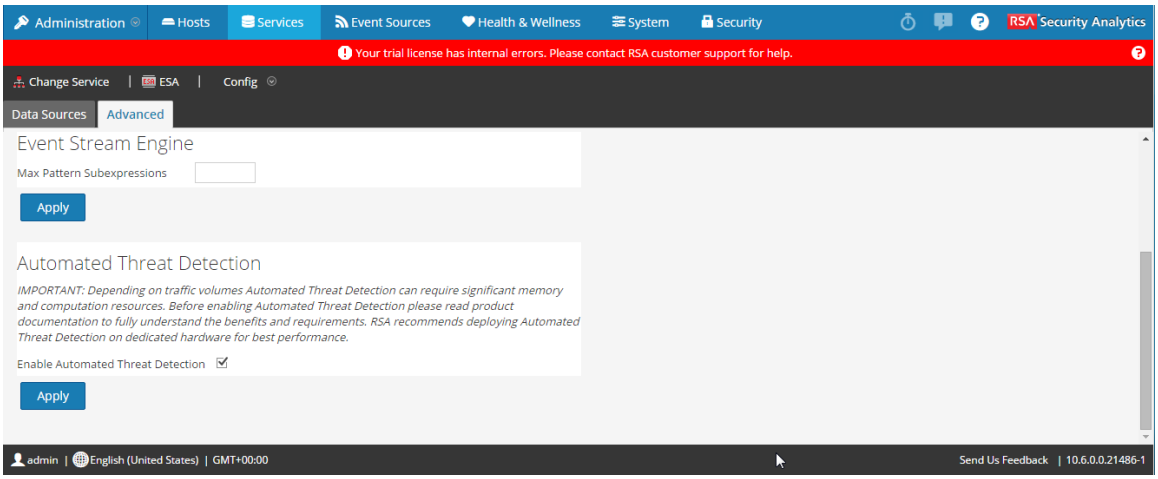
j. Para eliminar un dominio, selecciónelo y haga clic en −.

k. Para importar un archivo .CSV, haga clic en y, en el cuadro de diálogo Importar archivo, vaya al archivo .CSV. Seleccione uno de los siguientes delimitadores: Coma, LF (salto de línea) y CR (retorno de carro), según cómo separa los valores en el archivo. A continuación, haga clic en **Cargar**.

Nota: Es importante configurar una lista blanca antes de habilitar la detección de amenazas automatizadas para asegurarse de que los dominios estén en la lista blanca antes de que comience el puntaje de amenazas.

Paso 3: Habilitar la detección de amenazas automatizadas

1. En Administration > Servicios, seleccione el servicio ESA y elija > Ver > Configuración.
2. Haga clic en la pestaña Opciones avanzadas y seleccione **Habilitar la detección de amenazas automatizadas**, después haga clic en **Aplicar.**

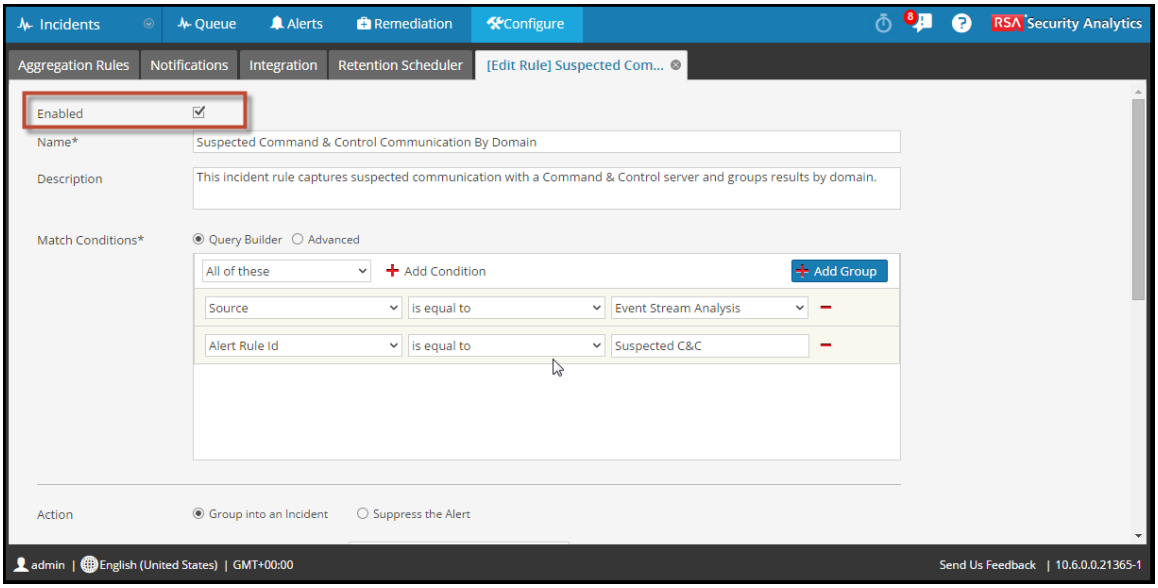


La detección de amenazas automatizadas ahora está habilitada en el ESA seleccionado.

Paso 4. Activar la regla de detección C2 en el administrador de incidentes

Habilite la regla de detección C2 en el **administrador de incidentes**.

1. En **Incidentes** > **Configurar**, seleccione **Reglas de agregación**.
2. Seleccione la regla **Comunicación de comando y control sospechosa por dominio** y haga doble clic en ella para abrirla.



3. Haga clic en **Activado** y, a continuación, en **Guardar**.

La regla muestra un botón Habilitado en verde una vez que se habilita.

Resultado

Una vez que se habilita la detección de amenazas automatizadas, ESA comienza a ejecutar la analítica en el tráfico HTTP. Puede ver información detallada de cada incidente en la línea de espera de Incident Management.

Los próximos pasos

Una vez que ha habilitado la regla, monitoree el administrador de incidentes para ver si se activa la regla. Si se activa la regla, siga los pasos de la sección siguiente para investigar el dominio asociado con la regla activada.

Trabajar con resultados de detección de amenazas automatizadas

Trabajar con resultados de detección de amenazas automatizadas

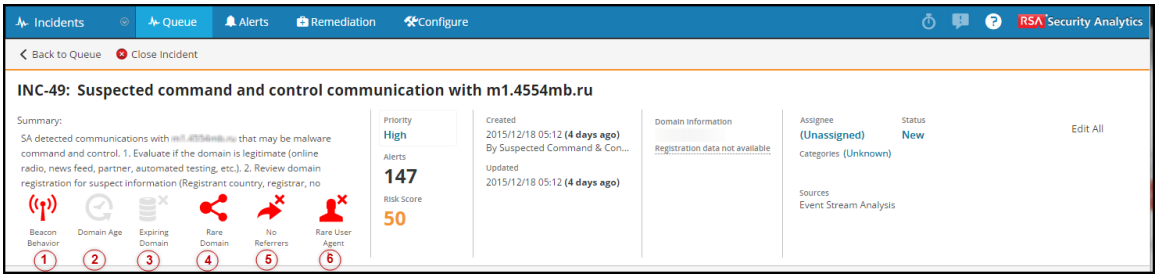
En este tema se explica cómo interpretar y trabajar con los resultados de detección de amenazas automatizadas.

Cuando se visualizan los resultados de detección de amenazas automatizadas en el administrador de incidentes, hay una serie de factores diferentes que se utilizan para determinar el puntaje general. Esta sección está diseñada para ayudarlo a comprender cómo se generan estos puntajes y su significado.

Comprender los resultados de detección de amenazas

Cuando se trabaja con detección de amenazas automatizadas, varios puntajes se agregan juntos para constituir el puntaje de detección de comando y control. Para comprender mejor cómo se activa este puntaje, es buena idea comprender los elementos que componen el puntaje final.

Cuando reciba una alerta de detección de comando & control, podrá ver el siguiente resumen de alerta detallado en el módulo Incident Management:

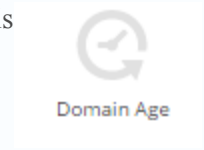
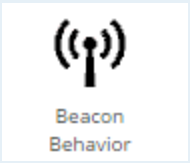
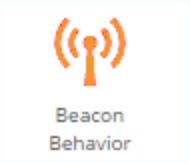
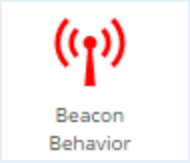


Cada ícono representa un puntaje diferente que compone el riesgo total calculado. Tenga en cuenta que los puntajes se ponderan, por lo tanto, cada puntaje representa una proporción diferente del puntaje final. Por ejemplo, el puntaje de comportamiento de Beacon podría ser un 20 % del puntaje final, mientras que la antigüedad del dominio podría ser un 5 %:

1. **Comportamiento de Beacon** La detección de comando y control intenta encontrar conexiones periódicas altamente regulares con un dominio sospechoso, por lo que el comportamiento de Beacon tiene relación con la regularidad con la cual la dirección IP de origen se conecta al servidor de dominio. Un puntaje alto significa que las conexiones entre esta dirección IP de origen y el dominio son altamente regulares.
2. **Antigüedad del dominio**. Con frecuencia, un servidor de comando y control utiliza un dominio nuevo para crear conexiones; por lo tanto, si un dominio es nuevo en la red, significa que es más probable que sea un dominio de comando y control. Un puntaje alto indica que este dominio es relativamente nuevo en esta red. Este puntaje se deriva del servicio Whois. Si su servicio Whois no funciona o si ESA no puede conectarse con él, el ícono aparece en gris. Si hay un problema de conectividad o el servicio Whois devuelve un valor nulo o un valor en un formato inesperado, se utiliza un valor predeterminado para calcular el puntaje. Esto garantiza que el puntaje general sea más preciso.
3. **Dominio por vencer**. Con frecuencia, un servidor de comando y control utiliza un dominio por vencer para crear conexiones; por lo tanto, si un dominio vencerá pronto, es muy probable que sea un dominio de comando y control. Este puntaje se deriva del servicio Whois. Si su servicio Whois no funciona o si ESA no puede conectarse con él, el ícono aparece en gris. Si hay un problema de conectividad o el servicio Whois devuelve un valor nulo o un valor en un formato inesperado, se utiliza un valor predeterminado para calcular este puntaje. Esto garantiza que el puntaje general sea más preciso.
4. **Dominio poco común**. Un dominio poco común es aquel al cual se han conectado relativamente pocas direcciones IP de origen en una red determinada en la semana más reciente. Si un dominio se utiliza con poca frecuencia, la posibilidad de que se trate de un dominio de comando y control es mayor que si es un dominio legítimo de uso común, como *Google.com*.
5. **Sin remitentes**. Un remitente es un campo HTTP que identifica la dirección de la página web vinculada al recurso que se solicita. Por ejemplo, si accedo al sitio web de mi banco desde el sitio web de mi trabajo, el sitio web del trabajo aparecerá como el remitente. Debido a que con frecuencia las personas se vinculan a un sitio a través de un remitente, un puntaje alto (lo que significa que un bajo porcentaje de direcciones IP que se conectan a este dominio han utilizado remitentes) indica que es más probable que se trate de una comunicación de comando y control.
6. **Agente de usuario poco común**. Los agentes de usuario identifican el software de cliente que se originan en la solicitud. Un puntaje alto indica que el agente de usuario asociado con la dirección IP no se utiliza comúnmente. Al igual que el puntaje de dominio poco común, un

agente de usuario poco común tiene una mayor probabilidad de estar asociado con un dominio de comando y control.

Los íconos se muestran en diferentes colores y los colores ayudan a indicar visualmente el nivel de riesgo. Consulte la tabla a continuación para obtener más información.

Ícono	Significado
Gris 	No se generó puntaje debido a que no hay datos disponibles. Esto puede ocurrir si el servicio Whois está deshabilitado o no hay datos disponibles para generar un puntaje determinado.
Negro 	El indicador de puntaje es débil.
naranja 	El indicador de puntaje es moderado.
Rojo 	El indicador de puntaje es alto.

Qué hacer a continuación

Hay tres rutas posibles que puede seguir una vez que ha visto los puntajes de amenazas:

- **Desglosar para obtener más detalles**. Hay varios factores que conforman un puntaje. Puede ver estos detalles en la página **Detalles de eventos**.

- **Investigar el dominio en el módulo Investigation**. Puede ir a la pantalla Investigaciones para obtener más detalles sobre el dominio y los incidentes relacionados.
- **Agregar dominios a una lista blanca**. Si observamos los detalles y determinamos que el dominio en cuestión no es una amenaza, es buena idea agregarlo a una lista blanca. Esto garantizará que el dominio ya no active un puntaje de detección de amenazas y ayudará a optimizar la precisión del puntaje.

Desglosar los puntajes para obtener más detalles

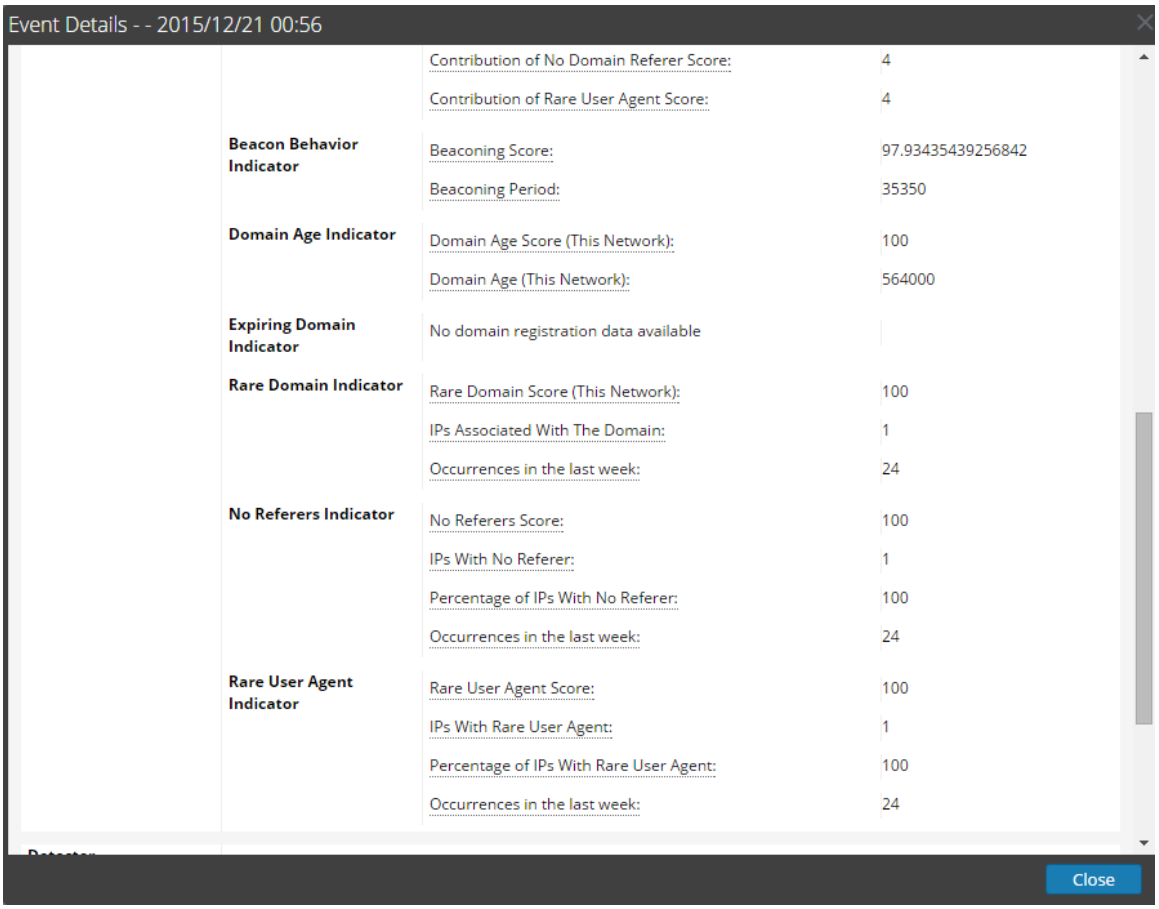
El puntaje de cada evento se enriquece con datos para ayudarlo a determinar si la comunicación con el dominio es malware y la severidad del ataque en caso de que lo sea. Para cada uno de los puntajes mencionados anteriormente, hay más detalles que se incluyen en los detalles de cada evento.

Para acceder a estos detalles:

1. En la línea de espera **Incidentes**, haga doble clic en un incidente para ver los **Detalles del incidente**.
2. En la sección **Detalles de la alerta**, haga doble clic en una alerta.
3. Se abre la página **Detalles de eventos**.

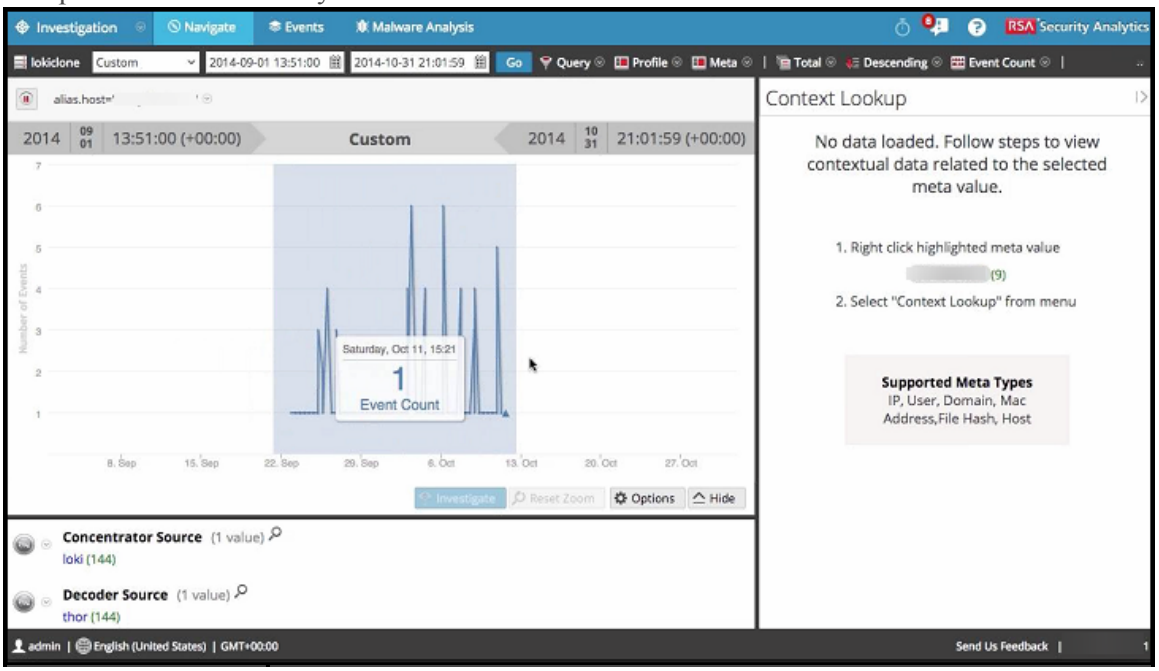
Desde allí, puede ver los detalles del evento y, en cada detalle, hay texto de desplazamiento para ayudarlo a interpretar los datos. Puede ver detalles como el rango de puntaje, la cantidad de apariciones para cada hora del puntaje, el período de Beacon, la información disponible en los datos de registro de Whois, etc.

Por ejemplo, puede ver en los siguientes detalles del evento que el puntaje de dominio poco común fue 100 (el puntaje más alto), pero que solo hubo una dirección IP asociada a este dominio y que hubo 24 apariciones en la semana anterior.



Investigar el dominio en el módulo Investigation

En Detalles de la alerta, también puede abrir el módulo investigaciones para desglosar los detalles del dominio. Para ello, en **Detalles de la alerta**, haga clic en > **Investigar el dominio de destino**. Desde allí, puede buscar los días en que se produjo el evento para ver qué más puede haber ocurrido y ver otros detalles sobre el evento.



Reducir los falsos positivos

En ocasiones, un dominio al que se accede habitualmente puede activar un puntaje de detección de amenazas automatizadas. Por ejemplo, un servicio de clima podría tener el mismo comportamiento de Beacon que una comunicación de comando y control, razón por la cual se activaría un puntaje negativo no justificado. Cuando sucede, esto se denomina un falso positivo. Si, después de investigar el evento, descubre que es un falso positivo, puede marcarlo como tal, lo cual agregará el dominio a una lista blanca. Una vez que el dominio se agrega a la lista blanca, ya no activará un puntaje de detección de amenazas automatizadas.

Nota: Si utiliza SecOps u otra solución de generación de vales, puede agregar manualmente dominios a la lista blanca mediante el servicio Context Hub. Consulte "Paso 2: Configurar una lista blanca" en Configurar la detección de amenazas automatizadas.

Procedimiento

1. En la página **Detalles de incidentes**, puede marcar un incidente específico como un falso positivo, lo cual lo agregará automáticamente a la lista blanca.
    1. En el **Administrador de incidentes**, seleccione el incidente que activó un puntaje de falso positivo. Haga clic en  > **Editar incidente**.

       Se muestra el cuadro de diálogo **Editar incidente**.
    2. En el cuadro de diálogo **Editar incidente**, haga clic en el campo **Estado** y seleccione *Cerrado: falso positivo*. Esto agrega el dominio a la lista blanca y cierra el incidente. Una vez que el dominio se agrega a la lista blanca, se omite cuando se produce el puntaje de detección de amenazas automatizadas.

Solucionar problemas de detección de amenazas automatizadas

La detección de amenazas automatizadas es un motor de analítica que examina los datos de HTTP. También facilita el uso de otros componentes, como un servicio WhoIs y Context Hub, los cuales pueden agregar complejidad a la instalación. En este tema se proporcionan sugerencias para ayudarlo a buscar problemas si su implementación de detección de amenazas automatizadas no proporciona los resultados esperados.

Cuando se solucionan problemas de detección de amenazas automatizadas, es importante considerar el modo utilizado. Si se utiliza el modo mixto (la detección de amenazas automatizadas está habilitada en la misma máquina que las reglas de ESA o Context Hub), deberá tener en cuenta el uso de la memoria y las I/O de estas aplicaciones durante la solución de problemas. Por lo general, cuando se configura la instalación de modo mixto, la detección de amenazas automatizadas está habilitada para utilizar aproximadamente un cincuenta por ciento de la memoria disponible, mientras que el uso de la memoria de reglas de ESA es ilimitado. Por lo tanto, es probable que desee comprobar las reglas de ESA como primer paso para solucionar el problema en modo mixto.

Si está utilizando el modo mixto, también debe considerar si el servicio ESA está configurado para pool de memoria u orden por hora de eventos. El pool de memoria puede afectar el rendimiento, mientras que el orden por hora de eventos puede afectar el uso de memoria y el rendimiento.

Posibles problemas

Problema	Causas posibles	Soluciones
Veo demasiadas alertas (falsos positivos).	Varias	Una causa posible es que la búsqueda de Whois falla o no está configurada. La búsqueda de Whois es útil para determinar si una URL es válida y, si la conexión falla o no está configurada correctamente, puede generar falsos positivos. Hay una serie de contadores para el servicio de búsqueda de Whois que puede ver. 1. En Administration > Servicios, seleccione el servicio ESA y elija > Ver > Explorar. 2. En el explorador, haga clic en **Servicio** > **Whois** > **whoisClient**. Los siguientes son algunos contadores útiles para comprobar: • **FailedLookupCount**: Cada vez que falla una solicitud de datos de Whois del servicio Whois de RSA, se incrementa este conteo. • **LookupEnqueueFailureCount**: Cuenta los intentos fallidos por agregar una entrada en la caché. Estas fallas se deben a errores internos de la caché. • **Response401Count**: Cuenta las solicitudes al servidor Whois de RSA que fallaron con un código de estado 401. Las solicitudes con tokens de autenticación vencidos se incluyen en este conteo. Este conteo se incluye en **FailedLookupCount**.
		Puede ser necesario ingresar direcciones URL en la lista blanca. En ocasiones, el comportamiento legítimo de una URL activa una alerta. Una manera de evitarlo es agregar la URL a la lista blanca. Para obtener instrucciones sobre cómo hacer esto, consulte “Reducir los falsos positivos” en Trabajar con resultados de detección de amenazas automatizadas.

Problema	Causas posibles	Soluciones
No se ven las alertas.	ESA requiere un período de "preparación" de 24 horas cuando se habilita la detección de amenazas automatizadas.	Cuando habilita la detección de amenazas automatizadas, hay un período de "preparación" durante el cual no se ven alertas. El período predeterminado es 24 horas. Después de este período de aprendizaje de 24 horas, se pueden ver las alertas. Si se reinicia el servicio de ESA, este período de aprendizaje vuelve a comenzar, por lo cual se restablece el período de espera de 24 horas.
Veo problemas de rendimiento (más uso de recursos o una caída de rendimiento).	Varias	Si tiene problemas de rendimiento en un servicio de ESA que también ejecuta reglas de ESA, siga los pasos de solución de problemas para las reglas. Las reglas de ESA son ilimitadas siempre que la detección de amenazas automatizadas esté configurada para usar una cantidad específica de recursos (por lo general, aproximadamente un 50 %). Para conocer estos pasos de solución de problemas, consulte Solucionar problemas de ESA.

Referencias

El módulo Alerts permite configurar e implementar reglas de ESA para recibir alertas sobre posibles amenazas de red.

En estos temas se explica la interfaz del usuario del módulo Alerts.

Pestaña Nueva regla de EPL avanzado

En este tema se describe la pestaña Regla de EPL avanzado que se usa para definir criterios de regla con una consulta del lenguaje de procesamiento de eventos (EPL).

Para acceder a la pestaña Regla de EPL avanzado:

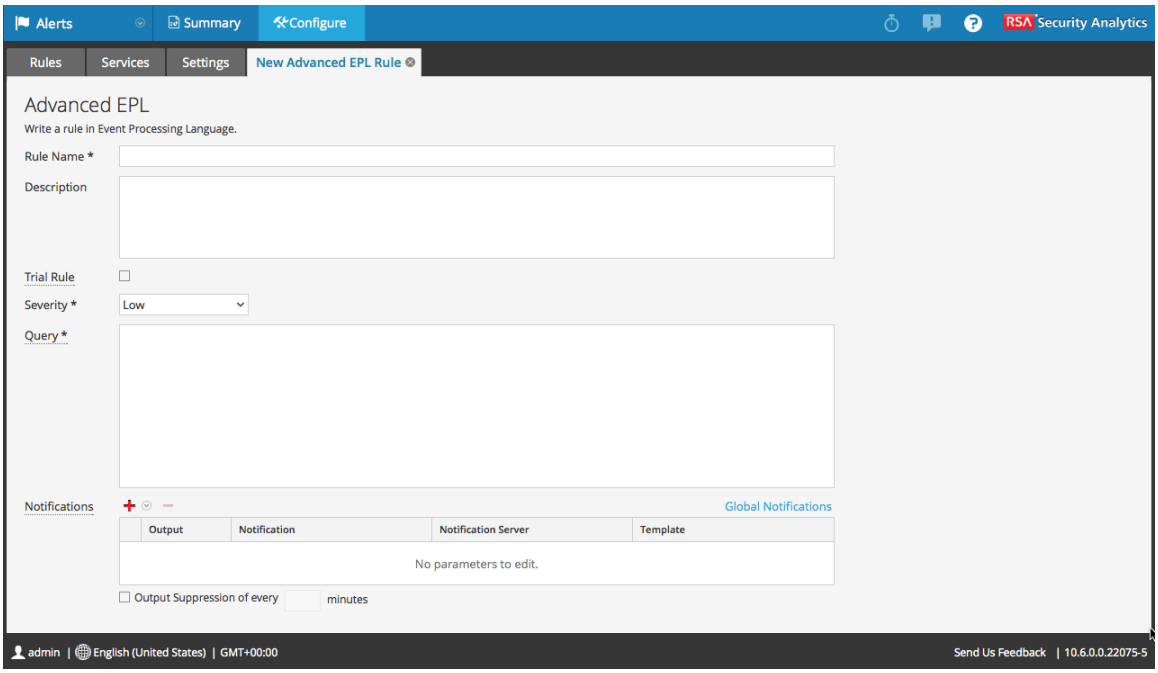
1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.

   La vista Configurar se muestra con la pestaña Reglas abierta de forma predeterminada.

2. En la barra de herramientas de la **Biblioteca de reglas**, seleccione  **> EPL avanzado**.

   Se muestra la pestaña Regla de EPL avanzado.

La siguiente es una captura de pantalla de la pestaña Regla de EPL avanzado.



Características

En la siguiente tabla se enumeran los parámetros de la pestaña Regla de EPL avanzado.

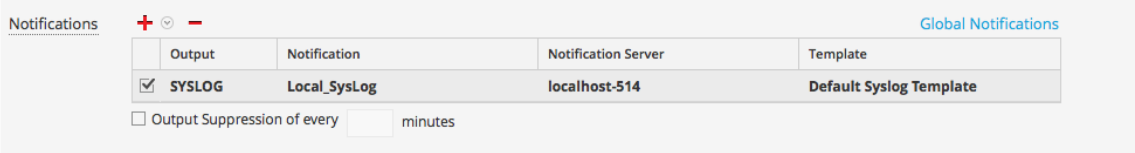
Parámetros	Descripción
Nombre de la regla	Objetivo de la regla de ESA.
Descripción	Resumen de lo que detecta la regla de ESA.
Regla de prueba	Modo de implementación para ver si la regla se ejecuta eficientemente.
Gravedad	Nivel de amenaza de la alerta que activó la regla.
Consulta	Consulta de EPL que define criterios de regla.

Notificaciones

En la sección Notificaciones, puede elegir cómo desea que se le informe cuando ESA genere una alerta para la regla.

Para obtener más información sobre las notificaciones de alertas, consulte Agregar un método de notificación a una regla.

En la siguiente figura se muestra la sección Notificaciones.



Parámetro	Descripción
+	Para agregar un tipo de notificación de alerta.
−	Para eliminar el tipo de notificación de alerta seleccionado.
Salida	Tipo de notificación de alerta. Las opciones son: • Correo electrónico • SNMP • Syslog • Script
Notificación	Nombre de la salida configurada con anterioridad, como una lista de distribución de correo electrónico.
Servidor de notificación	Nombre del servidor que envía la salida.
Plantilla	Nombre de la plantilla para la notificación de la alerta.
Supresión de salida de cada	Opción para especificar la frecuencia de la alerta.
Minutos	Frecuencia de la alerta en minutos.

Enriquecimientos

En la sección Enriquecimientos, puede agregar un origen de enriquecimiento de datos a una regla.

Para obtener más información sobre los enriquecimientos, consulte Agregar un enriquecimiento a una regla.

En la siguiente figura se muestra la sección Enriquecimientos.

Parámetro	Descripción
+	Para agregar un enriquecimiento.
−	Para eliminar el enriquecimiento seleccionado.
Salida	Tipo de origen de enriquecimiento. Las opciones son: • Tabla en la memoria • Referencia de base de datos externa • Warehouse Analytics • GeoIP
Origen de enriquecimiento	Nombre del origen de enriquecimiento configurado con anterioridad, como un nombre de archivo .CSV para una tabla en la memoria.
Metadatos de flujos de eventos de ESA	Clave de metadatos de ESA cuyo valor se usará como un operando de la condición de combinación.
Nombre de columna de origen de enriquecimiento	Nombre de la columna de origen de enriquecimiento cuyo valor se usará como otro operando de la condición de combinación.

Vista Resumen de alertas

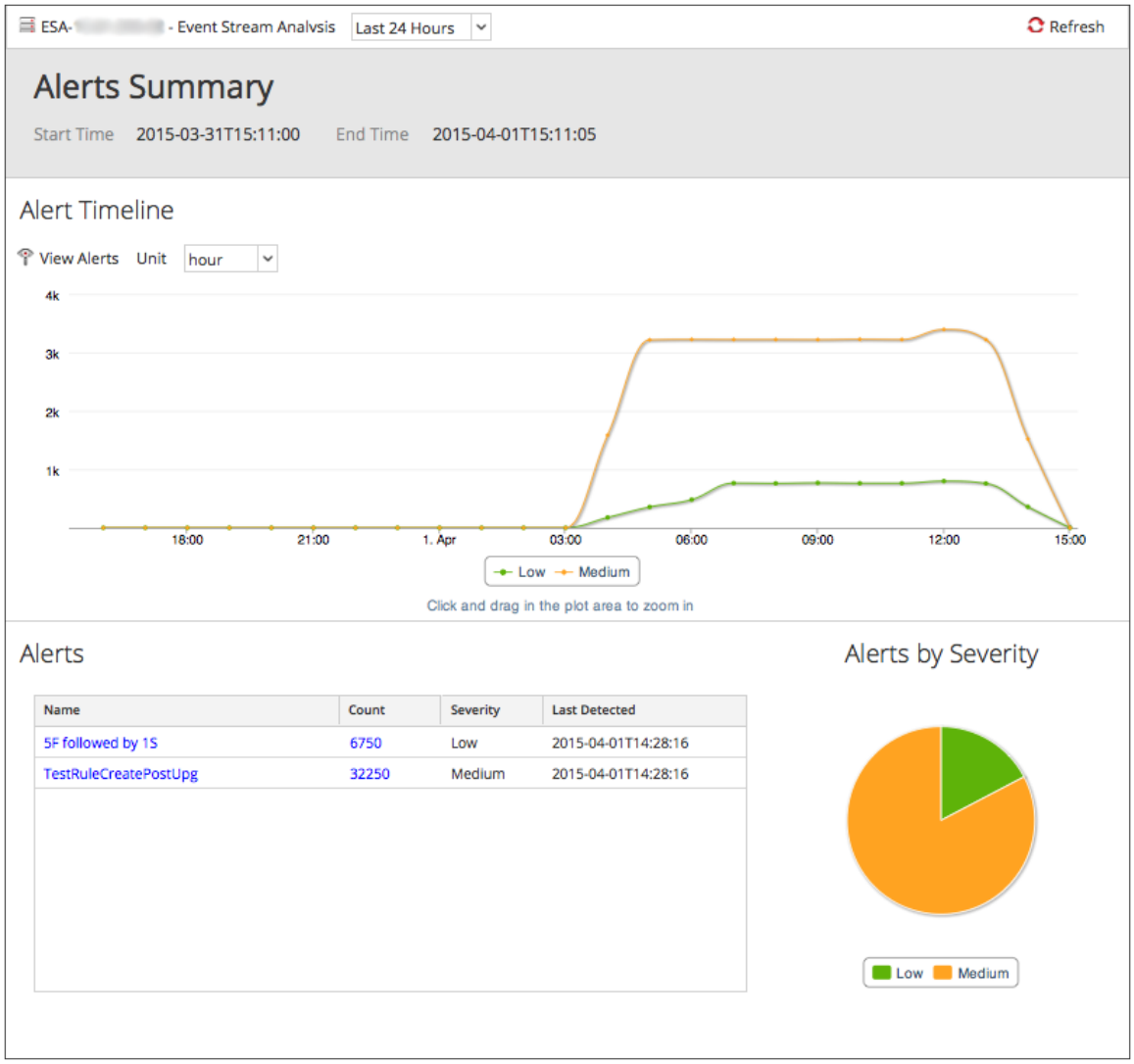
La vista Resumen de alertas proporciona una vista consolidada de todas las alertas generadas en un rango de tiempo específico. Puede especificar un rango de tiempo y representar las alertas como gráficos, diagramas y en formato tabular. Por ejemplo, si desea ver cuántas alertas de gravedad baja, media y alta se generan en un rango de tiempo determinado, puede utilizar un gráfico para mayor claridad. También puede ver la cantidad de alertas generadas en un minuto, hora o día específicos.

En un desglose más detallado, la vista también proporciona metadatos de eventos y detalles de eventos para cada alerta generada.

Nota: En la interfaz del usuario, la fecha o la hora mostradas dependen del perfil de zona horaria que seleccionó el usuario.

En Security Analytics, la vista Resumen de alertas se muestra cuando se navega a **Alertas** > **Resumen** y se selecciona un servicio ESA.

En la siguiente figura se muestran los diversos componentes de la vista Resumen de alertas.



Características

La vista Resumen de alertas se compone de las siguientes secciones:

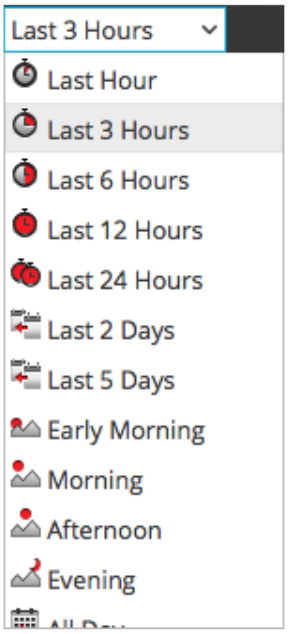
- Resumen de alertas
- Cronograma de alertas

- Alertas
- Alertas por severidad

Resumen de alertas

En la sección Resumen de alertas se muestra el período en el cual se generan alertas. En la figura siguiente se muestra la sección Resumen de alertas.

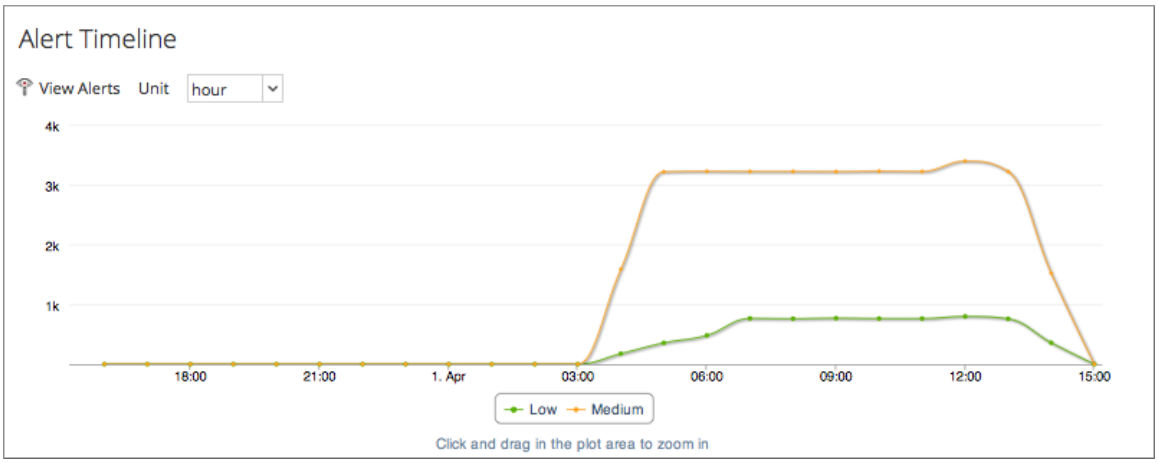
En la parte superior izquierda de la sección, se muestra el servicio de ESA seleccionado. Puede seleccionar un período de tiempo en función del cual desea que se muestren las alertas. En la siguiente figura se muestran algunas de las opciones disponibles.



Basándose en el período de tiempo que selecciona, en la sección se muestra la hora de inicio y la hora de finalización.

Cronograma de alertas

En la sección Cronograma de alertas se muestra una representación gráfica de las alertas generadas durante un período de tiempo específico. En la figura siguiente se muestra la sección Cronograma de alertas.



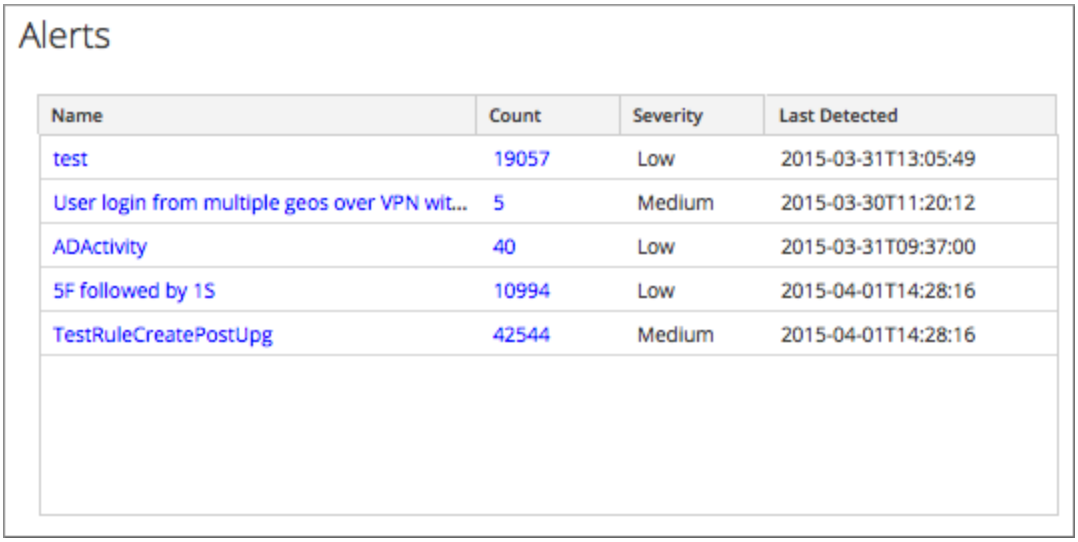
Puede ejecutar lo siguiente en la sección Cronograma de alertas:

- Ver las alertas generadas durante un minuto, una hora o un día determinados mediante la selección de la opción en la lista desplegable de **Unidad**.
- Ver detalles de cada alerta generada, para lo cual debe hacer clic en **Ver alertas**.
- Ver la cantidad de alertas generadas, el nivel de gravedad de las alertas y la hora en que se generan, con solo activar con el mouse un punto específico en el gráfico.

Nota: También puede hacer clic en las leyendas que se proporcionan en el Cronograma de alertas en función de la **Gravedad**. También puede hacer clic y arrastrar en el área de trazado para realizar un acercamiento y ver los datos.

Alertas

En la sección Alertas se muestran las alertas generadas durante un período de tiempo específico en formato tabular. En la figura siguiente se muestra la sección Alertas.



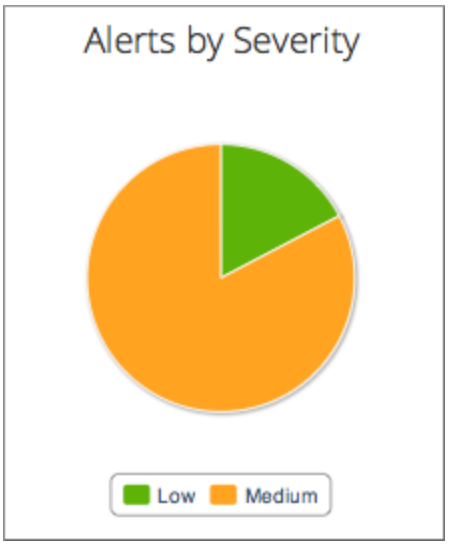
En la siguiente tabla se indican las diversas columnas de la sección Alertas y su descripción.

Columna	Descripción
Nombre	Nombre que identifica la alerta.
Count	Cantidad de veces que se activa la alerta.
Gravedad	Nivel de gravedad de la alerta.
Última detección	Última hora en que se detectó la alerta.

Puede ver los detalles de cada alerta generada, para lo cual debe hacer clic en una alerta y exportar los registros relacionados con cada evento en la alerta.

Alertas por severidad

En la sección Alertas por severidad se muestra una representación gráfica de las alertas según el nivel de gravedad. En la siguiente figura se muestra la sección Alertas por severidad.



Puede ver los detalles de las alertas generadas si hace clic en el gráfico.

Cuadro de diálogo Crear una declaración

El cuadro de diálogo Crear una declaración permite construir una declaración de condición cuando se crea una nueva regla del generador de reglas.

Para acceder al cuadro de diálogo Crear una declaración:

1. En el menú de Security Analytics, seleccione **Alertas > Configurar**.

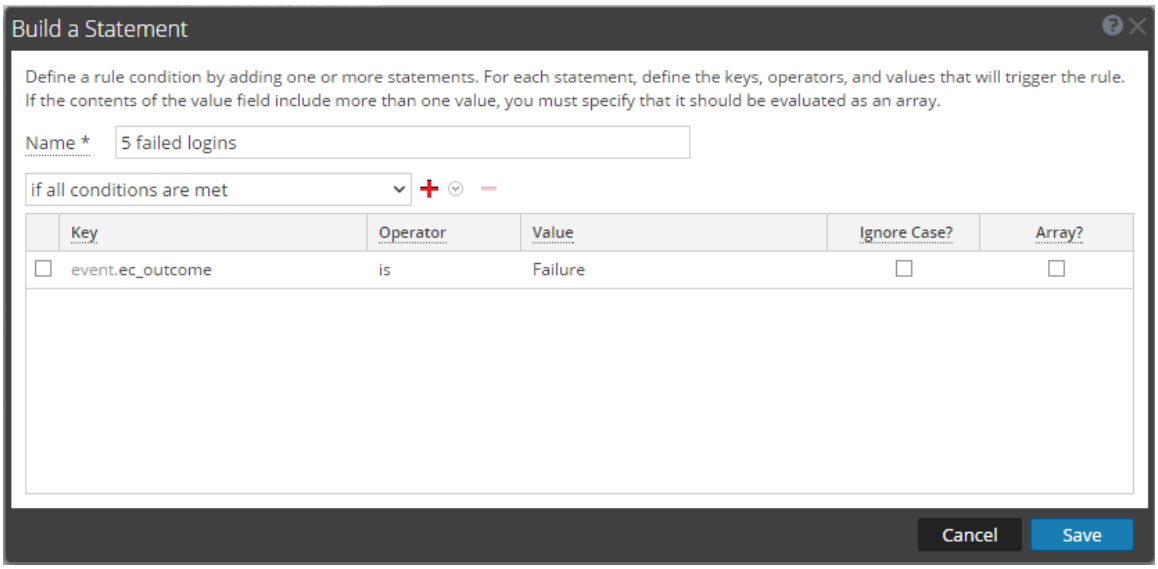
   La vista Configurar se muestra con la pestaña Reglas abierta.

2. En la barra de herramientas **Biblioteca de reglas**, seleccione  **> Generador de reglas**.

   Se muestra la pestaña Nueva regla en Security Analytics.

3. En la sección **Condiciones**, haga clic en  .

   Se muestra el cuadro de diálogo Crear una declaración.



Características

En la siguiente tabla se describen los parámetros del cuadro de diálogo Crear una declaración.

Parámetro	Descripción
Nombre	Propósito de la declaración.
Seleccionar	Condiciones que requiere la regla. Existen dos opciones: • Si se cumplen todas las condiciones • Si se cumple una de estas condiciones
Clave	Clave que ESA debe comprobar en la declaración de la regla.

Parámetro	Descripción
Tipo de evaluación	Relación entre la clave de metadatos y el valor de la clave: • es • no es • no es nulo • es mayor que (>) • es mayor o igual que (>=) • es menor que (<) • es menor o igual que (<=) • contiene • no contiene • comienza con • termina con
Valor	Valor que ESA debe buscar en la clave.
¿Omitir mayúsculas y minúsculas?	Este campo está diseñado para su uso con cadenas y matrices de valores de cadena. Cuando se selecciona el campo **Omitir mayúsculas y minúsculas**, la consulta trata todo el texto de la cadena como un valor en minúscula. Esto garantiza la activación de una regla que busca el nombre de usuario Johnson si el evento contiene “johnson”, “JOHNSON” o “JoHnSoN”.
¿Arreglo?	Opción para indicar si el contenido del campo Valor representa uno o varios valores: • Seleccione la casilla paraindicar valores múltiples. • Deseleccione la casilla para indicar un valor.
+	Agregue una declaración. Puede agregar una condición de metadatos, de lista blanca o de lista negra.
−	Elimine la declaración seleccionada.
Guardar	Agregue la declaración a la sección Condiciones de la pestaña Generador de reglas.

En la siguiente tabla se muestran los operadores que puede usar en el generador de reglas:

Operador	Valor obligatorio	Uso	Ejemplo	Significado
es	Valor de cadena único	La clave de metadatos es igual al campo *valor*.	***user_dst*** es John Doe.	***user_dst*** es igual a la cadena *"John Doe"*.
es	Valor de cadena del arreglo	La clave de metadatos es igual a uno de los elementos del campo *valor*.	*user_dst* es John, Doe, Smith.	*user_dst* es igual a la cadena *"John"*, a la cadena *"Doe"* o a la cadena *"Smith"* (Tenga en cuenta que se eliminan los espacios).
no es	Valor de cadena único	La clave de metadatos no es igual al campo *valor*.	***tamaño*** no es 200.	***tamaño*** no es igual al número 200 (el tamaño es un valor numérico).
no es	Valor de cadena del arreglo	La clave de metadatos no es igual a ninguno de los elementos del campo *valor*.	***tamaño*** no es 200, 300, 400.	***tamaño*** no es igual a *200*, *300* ni *400*.
no es nulo	N/D (busca cualquier valor)	El valor de clave de metadatos no es nulo.	***user_dst*** no es nulo.	***user_dst*** es un metadato que contiene un valor.
es mayor que (>)	Número	El valor numérico de la clave de metadatos es mayor que el número en el campo *valor*.	***la carga útil*** es mayor que 7,000.	***la carga útil*** es un valor numérico que es mayor que 7,000.
es mayor o igual que (>=)	Número	El valor numérico de la clave de metadatos es mayor o igual al número en el campo *valor*.	***la carga útil*** es mayor o igual que 7,000.	***la carga útil*** es un valor numérico que es mayor o igual que 7,000.
es menor que (<)	Número	El valor numérico de la clave de metadatos es menor que el número en el campo *valor*.	***ip_dstport*** es menor que 1,024.	***ip_dstport*** es un valor numérico menor que el valor numérico 1,024.
es menor o igual que (<=)	Número	El valor numérico de la clave de metadatos es menor o igual que el número en el campo *valor*.	***ip_dstport*** es menor o igual que 1,024.	***ip_dstport*** es un valor numérico menor o igual que el valor numérico 1,024.
contiene	Cadena	El campo *valor* es una subcadena de la clave de metadatos (este operador solo está disponible para una clave de metadatos con valor de cadena).	***ec_outcome*** contiene la falla.	***ec_outcome*** es una cadena que contiene la subcadena *"falla"*.

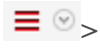
Operador	Valor obligatorio	Uso	Ejemplo	Significado
no contiene	Cadena	El campo *valor* no es una subcadena de la clave de metadatos (este operador solo está disponible para una clave de metadatos con valor de cadena).	***ec_outcome*** no contiene la falla.	***ec_outcome*** es una cadena que no contiene la subcadena *"falla"*.
comienza con	Cadena	El campo *valor* es el comienzo de la clave de metadatos (este operador solo está disponible para una clave de metadatos con valor de cadena).	***ip_dst*** comienza con 127.0.	***ip_dst*** es una cadena que comienza con *"127.0"*.
termina con	Cadena	El campo *valor* es el final de la clave de metadatos (este operador solo está disponible para una clave de metadatos con valor de cadena).	***user_dst*** termina en hijo.	***user_dst*** es una cadena que termina en *"hijo"*.

Nota: Los términos en ***negrita cursiva*** son metadatos que probablemente no existen en todos los ambientes de cliente.

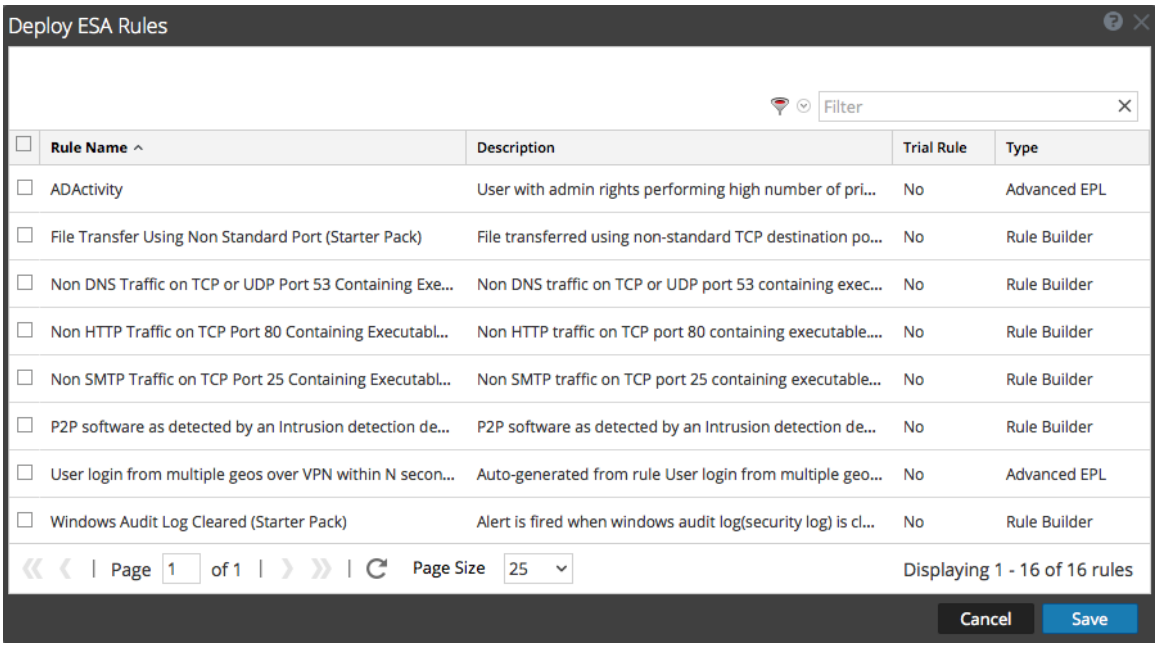
Cuadro de diálogo Implementar reglas de ESA

El cuadro de diálogo Implementar reglas de ESA permite filtrar y seleccionar reglas para implementar en un servicio de ESA.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   La pestaña Reglas se muestra de manera predeterminada.
2. En la sección **Implementación** del panel de opciones, seleccione una implementación o haga clic en  > **Agregar** para agregar una nueva.
3. En el panel **Reglas de ESA**, haga clic en  .
   Se muestra el cuadro de diálogo Implementar reglas de ESA.

En la siguiente figura se muestra un ejemplo de este cuadro de diálogo.



Características

En la siguiente tabla se describen los parámetros del cuadro de diálogo Implementar reglas de ESA.

Parámetros	Descripción
	Filtra la lista de reglas de acuerdo con la gravedad y el tipo. El cuadro de texto junto a este ícono filtra en función del nombre de la regla.
Nombre de la regla	Muestra el nombre de la regla.
Descripción	Describe la regla.
Regla de prueba	Indica si la regla es o no una regla de prueba.
Tipo	Indica el tipo de regla: RSA Live ESA, EPL avanzado o Generador de reglas.

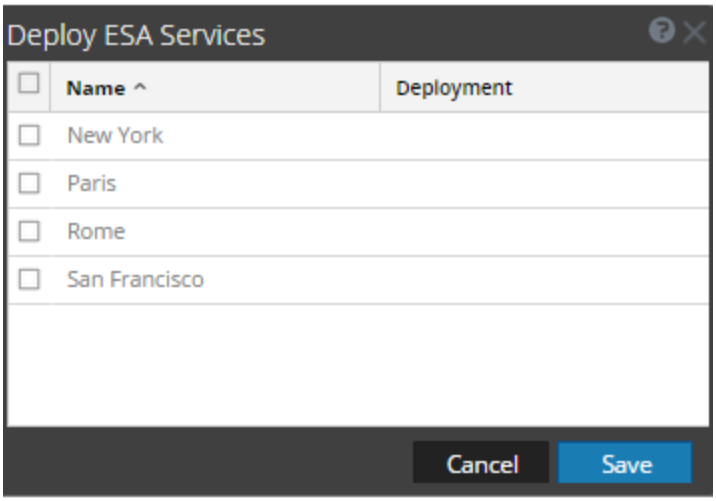
Cuadro de diálogo Implementar servicios de ESA

El cuadro de diálogo Implementar servicios de ESA muestra todos los servicios de ESA disponibles para agregar en una implementación.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   La pestaña Reglas se muestra de manera predeterminada.
2. En la sección **Implementación** del panel de opciones, seleccione o agregue una implementación.
3. En el panel **Servicios de ESA**, haga clic en +.
   Se muestra el cuadro de diálogo Implementar servicios de ESA.

En la siguiente figura se muestra un ejemplo de este cuadro de diálogo.



Características

En la siguiente tabla se describen los parámetros del cuadro de diálogo Implementar servicios de ESA.

Parámetros	Descripción
Nombre	Muestra el nombre de los servicios de ESA configurados.
Implementación	Muestra las implementaciones a las cuales ya se agregó el servicio.

Pestaña Generador de reglas

La pestaña Generador de reglas permite definir una regla del generador de reglas.

Para acceder a la pestaña Generador de reglas:

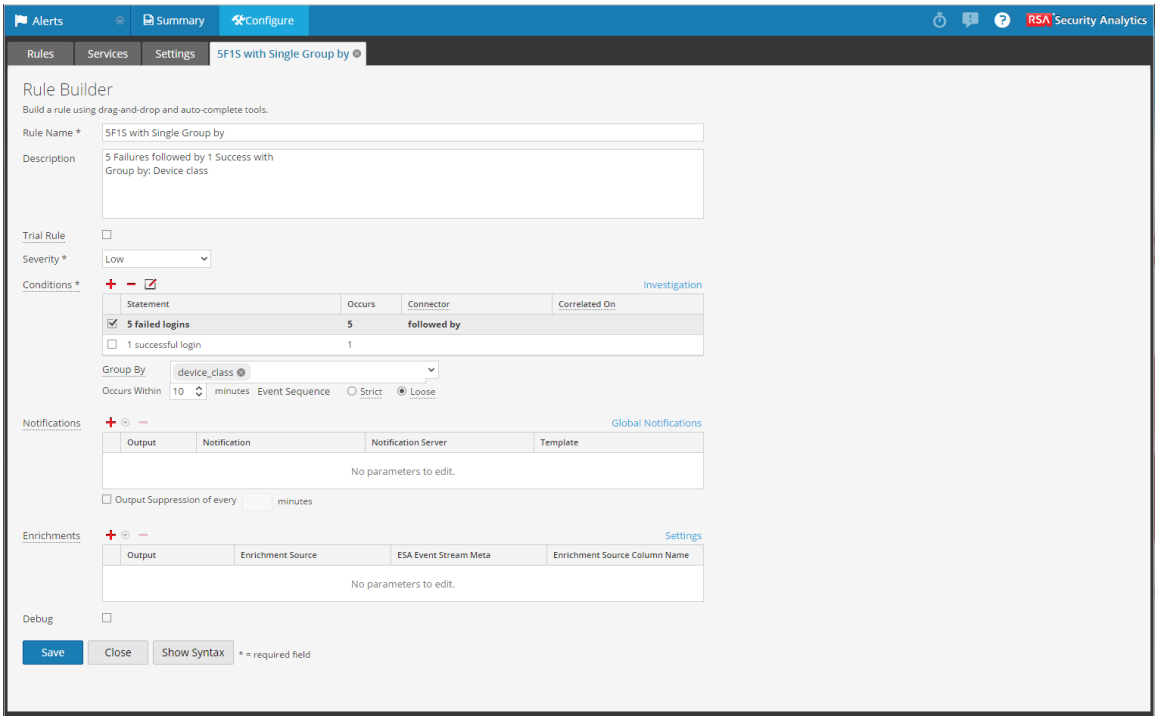
1. En el menú de Security Analytics, seleccione **Alertas** > **Configurar**.

   La vista Configurar se muestra con la pestaña Reglas abierta de forma predeterminada.

2. En la barra de herramientas **Biblioteca de reglas**, seleccione  > **Generador de reglas**.

   Se muestra la pestaña Generador de reglas.

En la siguiente figura se muestra la pestaña Generador de reglas.



Características

En la siguiente tabla se indican los parámetros de la pestaña Generador de reglas.

Parámetros	Descripción
Nombre de la regla	Objetivo de la regla de ESA.
Descripción	Resumen de lo que detecta la regla de ESA.

Parámetros	Descripción
Regla de prueba	Modo de implementación para ver si la regla se ejecuta eficientemente.
Gravedad	Nivel de amenaza de la alerta que activó la regla.

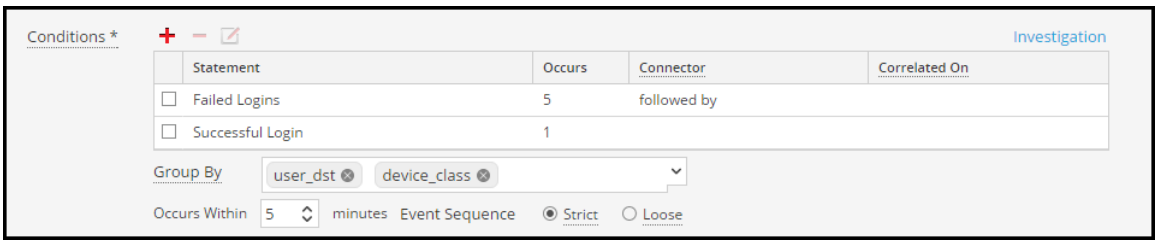
En la pestaña Generador de reglas se incluyen los siguientes componentes:

- Sección Condiciones
- Sección Notificaciones
- Sección Enriquecimientos

Sección Condiciones

La sección Condiciones de la pestaña Generador de reglas permite definir lo que detecta la regla.

En la siguiente figura se muestra la sección Condiciones.



En la siguiente tabla se enumeran los parámetros de la sección Condiciones.

Parámetro	Descripción
+	Agregue una declaración.
−	Elimine la declaración seleccionada.
	Edite la declaración seleccionada.
Declaración	Grupo lógico de condiciones para una operación.
Ocurre	Frecuencia de la alerta si se cumple la condición. Esto especifica que debe haber al menos esa cantidad de eventos que satisfagan los criterios para activar una alerta. La ventana de tiempo en minutos vincula el conteo de Ocurre.

Parámetro	Descripción
Connector	Opciones para especificar la relación entre las declaraciones: • seguido de • no seguido de • y • O El conector une dos declaraciones con Y, O, seguido de o no seguido de. Cuando se usa seguido de, especifica que hay una secuencia de esos eventos. Y y O crean un criterio grande. Seguido de crea criterios distintos que ocurren en secuencia.
Correlacionado en	Opción para el conector “No seguido de”. Especifique la clave de metadatos del campo que desea asegurarse de que no siga en la secuencia.
ocurre dentro de minutos	Ventana de tiempo dentro de la cual deben producirse las condiciones.
Secuencia de eventos	Elija si el patrón debe seguir una coincidencia *Estricta* o una *Flexible*. Si especifica una coincidencia estricta, esto significa que el patrón se debe producir en la secuencia *exacta* que se especificó, sin eventos adicionales entremedio. Por ejemplo, si la secuencia especifica cinco inicios de sesión fallidos (F) seguidos de un inicio de sesión correcto (S), este patrón solo coincidirá si el usuario ejecuta la siguiente secuencia: F, F, F, F, F, S. Si especifica una coincidencia flexible, significa que se pueden producir otros eventos dentro de la secuencia, pero que la regla se activará si también se producen todos los eventos especificados. Por ejemplo, cinco intentos de inicio de sesión fallidos (F), seguidos de un número indeterminado de intentos de inicio de sesión correctos intermedios (S), seguidos de un intento de inicio de sesión correcto pueden crear el siguiente patrón: F, S, F, S, F, S, F, S, F, S, lo cual activará la regla a pesar de los inicios de sesión intermedios correctos.

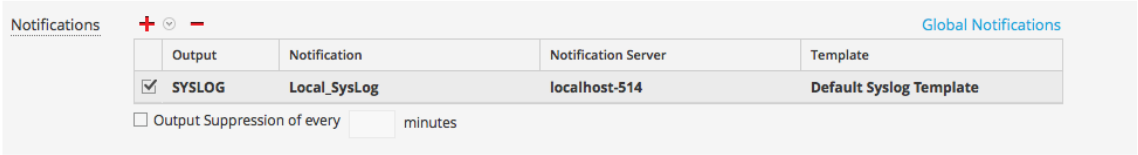
Parámetro	Descripción
Agrupar por	Seleccione la clave de metadatos por la cual se agrupan los resultados en la lista desplegable. Por ejemplo, suponga que hay tres usuarios, Joe, Jane y John, y utiliza los metadatos Agrupar por, **user_dst** (user_dst es el campo de metadatos para la cuenta de destino de usuario). El resultado mostrará eventos agrupados bajo las cuentas de destino de usuario, Joe, Jane y John. También puede agrupar por varias claves. Por ejemplo, es posible que desee agrupar por usuario y por máquina para ver si un usuario que inició sesión en la misma máquina intenta iniciar sesión varias veces en una cuenta. Para hacerlo, puede agrupar por device_class y user_dst.

Notificaciones

En la sección Notificaciones, puede elegir cómo desea que se le informe cuando ESA genere una alerta para la regla.

Para obtener más información sobre las notificaciones de alertas, consulte Agregar un método de notificación a una regla.

En la siguiente figura se muestra la sección Notificaciones.



Parámetro	Descripción
+	Para agregar un tipo de notificación de alerta.
−	Para eliminar la notificación de alerta seleccionada.
Salida	Tipo de notificación de alerta. Las opciones son: • Correo electrónico • SNMP • Syslog • Script
Notificación	Nombre de la salida configurada con anterioridad, como una lista de distribución de correo electrónico.

Parámetro	Descripción
Servidor de notificación	Nombre del servidor que envía la salida.
Plantilla	Nombre de la plantilla para la notificación de la alerta.
Supresión de salida de cada	Opción para especificar la frecuencia de la alerta.
Minutos	Frecuencia de la alerta en minutos.

Enriquecimientos

En la sección Enriquecimientos, puede agregar un origen de enriquecimiento de datos a una regla.

Para obtener más información sobre los enriquecimientos, consulte Agregar un enriquecimiento a una regla.

En la siguiente figura se muestra la sección Enriquecimientos.

Parámetro	Descripción
+	Para agregar un enriquecimiento.
−	Para eliminar el enriquecimiento seleccionado.
Salida	Tipo de origen de enriquecimiento. Las opciones son: • Tabla en la memoria • Referencia de base de datos externa • Warehouse Analytics • GeoIP

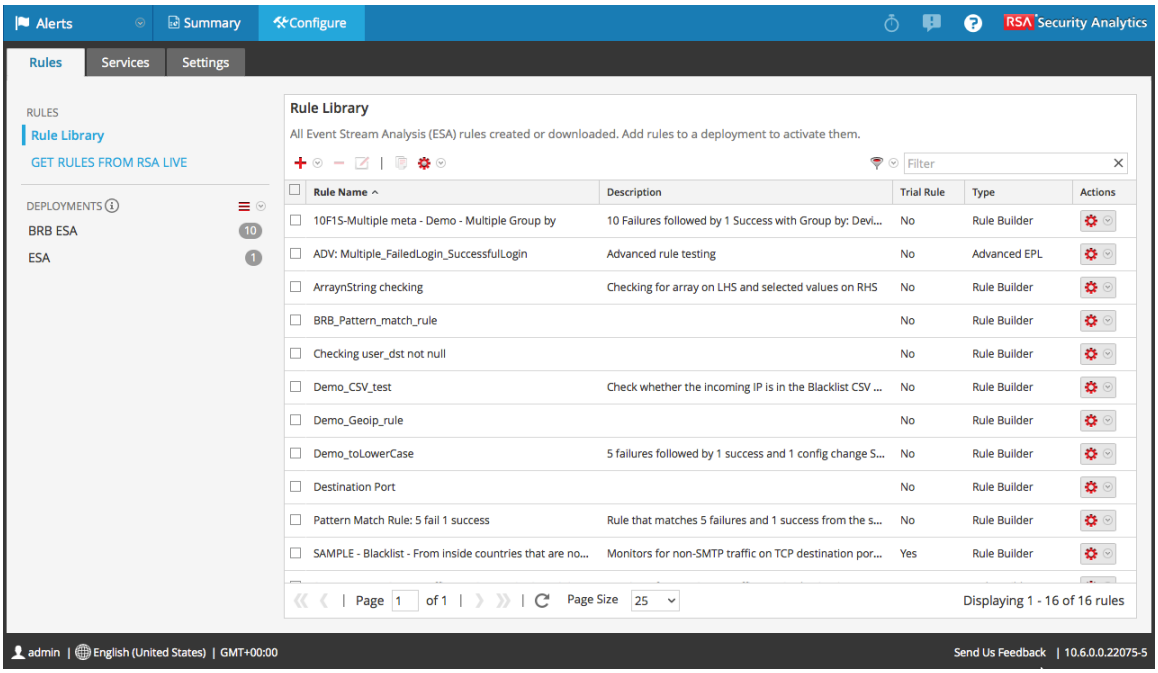
Parámetro	Descripción
Origen de enriquecimiento	Nombre del origen de enriquecimiento configurado con anterioridad, como un nombre de archivo .CSV para una tabla en la memoria.
Metadatos de flujos de eventos de ESA	Clave de metadatos de ESA cuyo valor se usará como un operando de la condición de combinación.
Nombre de columna de origen de enriquecimiento	Nombre de la columna de origen de enriquecimiento cuyo valor se usará como otro operando de la condición de combinación. Para una tabla en la memoria, si configuró una clave cuando creó un enriquecimiento basado en .CSV, esta columna se completa automáticamente con la clave seleccionada. Sin embargo, la puede cambiar si lo desea. Para un origen de enriquecimiento GeoIP, ipv4 se selecciona automáticamente.

Pestaña Reglas

En este tema se describe la pestaña Reglas, la cual se usa para administrar reglas e implementaciones de ESA.

La pestaña Reglas se muestra cuando selecciona **Alertas > Configurar** en el menú de Security Analytics.

En la siguiente figura se muestra la pestaña Reglas.



Características

La pestaña Reglas se divide en tres secciones:

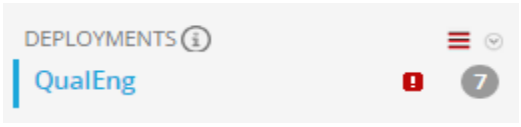
- Panel de opciones
- Panel Biblioteca de reglas
- Panel de implementación

Panel de opciones

En el panel de opciones de la pestaña **Reglas**, puede realizar lo siguiente:

- Ver las reglas de ESA en la Biblioteca de reglas
- Crear implementaciones

En la siguiente figura se muestra el panel de opciones de la pestaña **Reglas**.



Características

El panel de opciones tiene dos secciones: Reglas e Implementaciones.

Sección Reglas

La sección Reglas incluye dos opciones. **Biblioteca de reglas** se selecciona de forma predeterminada y, cuando se selecciona, la vista Biblioteca de reglas se muestra en la pestaña. **Obtener reglas de RSA Live** se desplaza a la vista Buscar en Live, donde puede buscar reglas.

Sección Implementaciones

La sección Implementaciones muestra las implementaciones e indica si hay actualizaciones para ellas. Desde esta sección, las implementaciones se pueden agregar, eliminar, editar y actualizar. La selección de una implementación en la lista muestra el panel Implementación dentro de la pestaña. En la siguiente tabla se describen las funciones de esta sección.

Característica	Descripción
	Muestra un menú desplegable desde el cual puede optar por agregar, editar o eliminar una implementación. También puede actualizar la lista de implementaciones para ver si incluye nuevas actualizaciones.
	Indica si hay actualizaciones para la implementación.
	Indica la cantidad de reglas en la implementación.

Panel Biblioteca de reglas

En este tema se describen los componentes del panel Biblioteca de reglas. El panel Biblioteca de reglas permite realizar las siguientes tareas:

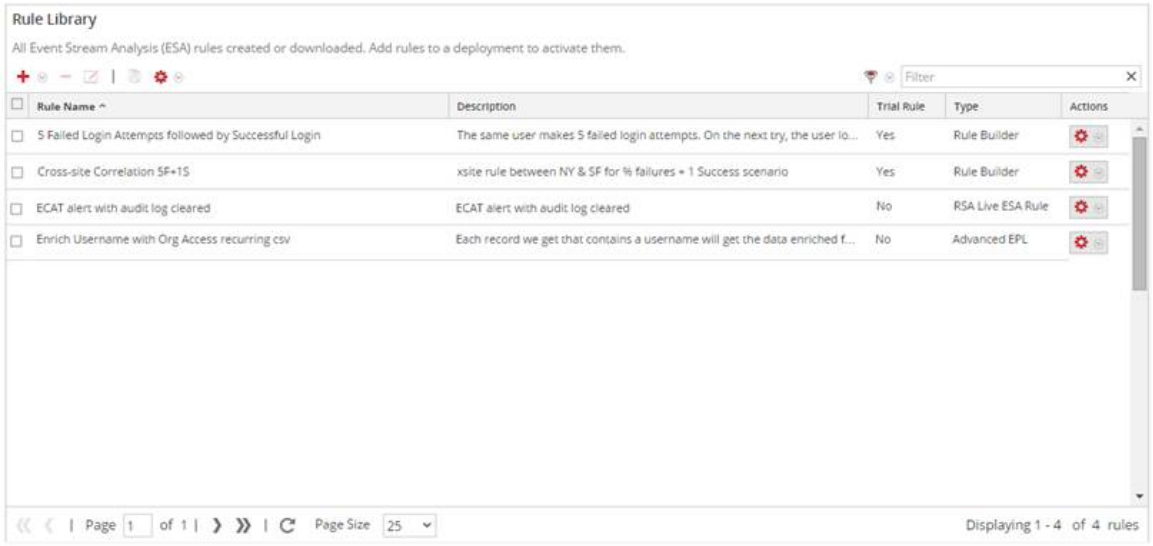
- Agregar una regla de ESA
- Eliminar una regla de ESA
- Editar una regla de ESA
- Duplicar una regla de ESA

- Importar reglas de ESA
- Exportar una regla de ESA
- Filtrar la lista de reglas de ESA

Para acceder a esta vista, en el menú de Security Analytics, seleccione **Alertas > Configurar**. La pestaña Reglas se muestra con el panel Biblioteca de reglas a la derecha.

Características

En la siguiente figura se muestra el panel Biblioteca de reglas.



El panel Biblioteca de reglas incluye los siguientes componentes:

- Barra de herramientas de la Biblioteca de reglas

- Lista de la Biblioteca de reglas

Barra de herramientas de la Biblioteca de reglas

La barra de herramientas de la Biblioteca de reglas permite agregar, eliminar, editar, duplicar, filtrar, exportar e importar reglas de ESA. En la siguiente figura se muestran los íconos para estas acciones.

Lista de la Biblioteca de reglas

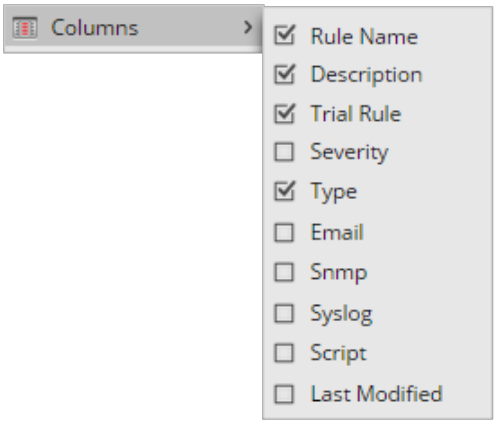
En la siguiente figura se muestra la lista de la Biblioteca de reglas.

La lista de la Biblioteca de reglas muestra todas las reglas de ESA que se descargaron desde RSA Live o que se crearon en las pestañas EPL avanzado y Generador de reglas. En la siguiente tabla se indican las columnas de la lista de la Biblioteca de reglas y su descripción.

Columna	Descripción
Nombre de la regla	Objetivo de la regla de ESA.
Descripción	Resumen de lo que detecta la regla de ESA.
Regla de prueba	Modo de implementación para ver si la regla se ejecuta eficientemente.
Tipo	El tipo de regla.

Columna	Descripción
Acciones ( )	Menú para eliminar, editar, duplicar o exportar la regla seleccionada.
Gravedad	Nivel de amenaza de la alerta que activó la regla.
Correo electrónico	Indica si se envía una notificación de alerta para la regla por correo electrónico. De manera predeterminada, esta columna no está visible.
Snmp	Indica si se envía una notificación de alerta para la regla mediante SNMP. De manera predeterminada, esta columna no está visible.
Syslog	Indica si se envía una notificación de alerta para la regla mediante syslog. De manera predeterminada, esta columna no está visible.
Script	Indica si una notificación de alerta para la regla ejecuta un script. De manera predeterminada, esta columna no está visible.
Última modificación	La fecha y la hora en que se modificó la regla ESA por última vez. De manera predeterminada, esta columna no está visible.

Para mostrar columnas que no están visibles de manera predeterminada, mantenga el mouse sobre el título de una columna y haga clic en la **v** de la derecha. Esto abre un menú desplegable en el cual puede ordenar el contenido de la columna o elegir las columnas que desea ver en la lista de la Biblioteca de reglas.

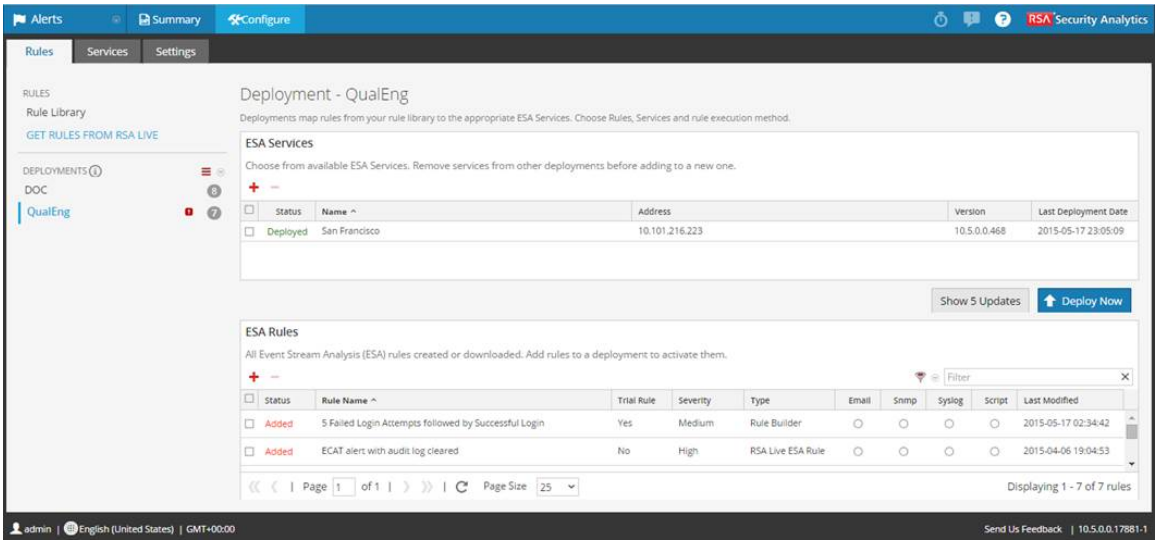


Panel de implementación

En este tema se proporciona una descripción general del panel de implementación. El panel de implementación permite crear y configurar las implementaciones. El panel Implementación incluye las siguientes secciones:

- Servicios de ESA
- Reglas de ESA

En la siguiente figura se muestra el panel Implementación.



Características

Servicios de ESA

Con la sección Servicios de ESA, puede administrar cada servicio de ESA en la implementación.

La sección Servicios de ESA permite realizar lo siguiente.

Tarea	Descripción
+	Agregar un servicio ESA a la implementación.
−	Eliminar el servicio de ESA seleccionado de la implementación.
Mostrar actualizaciones	Abre el cuadro de diálogo Actualizaciones a la implementación.
Implementar ahora	Implementa el conjunto de reglas actual.

En la siguiente tabla se indican los parámetros de la sección Servicios de ESA.

Parámetro	Descripción
Status	Indica si el estado de la implementación es **Agregada**, **Implementado**, **Actualizado** o **Falla**.
Nombre	Nombre del servicio ESA.
Dirección	La dirección IP del host donde se instala el servicio ESA.
Versión	Versión del servicio ESA.
Fecha de última implementación	La fecha y la hora en que se implementó por última vez el servicio de ESA.

Reglas de ESA

La sección Reglas de ESA permite administrar las reglas de la implementación. Esta sección enumera todas las reglas presentes actualmente en la implementación.

La sección **Reglas de ESA** permite realizar lo siguiente.

Tarea	Descripción
	Abrir el cuadro de diálogo Implementar reglas de ESA, en el cual puede seleccionar una regla.
	Elimine las reglas de ESA seleccionadas de la implementación.
	Filtrar la lista de reglas.
	Buscar una regla.

En la siguiente tabla se enumeran los parámetros de la sección Reglas de ESA.

Parámetro	Descripción
Status	Indica el estado de la regla: • Implementado: la regla está implementada. • Actualizado: la regla se actualizó desde la última implementación. • Agregada: la regla se agregó desde la última implementación. • Falla: la implementación falló.
Nombre de la regla	Objetivo de la regla de ESA.
Regla de prueba	Modo de implementación para ver si la regla se ejecuta eficientemente.
Gravedad	Nivel de amenaza de la alerta que activó la regla.
Salida	El tipo de regla de ESA.
Correo electrónico, SNMP, Syslog y Script	Indica los tipos de notificación que se usan para las alertas que generan las reglas.
Última modificación	La fecha y la hora en que se modificó la regla ESA por última vez.

Cuadro de diálogo Sintaxis de regla

En este tema se describen las funciones del cuadro de diálogo Sintaxis de regla. En el cuadro de diálogo Sintaxis de regla se muestra la sintaxis de EPL de condiciones, declaraciones y parámetros de depuración, y se proporciona una advertencia cuando la sintaxis no es válida.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
2. En la vista **Biblioteca de reglas**, realice una de las siguientes acciones:
   a. Haga clic en y seleccione **EPL avanzado** o **Generador de reglas**.
   b. Haga doble clic en una regla existente.
   c. Seleccione una regla existente y haga clic en  en la barra de herramientas de la

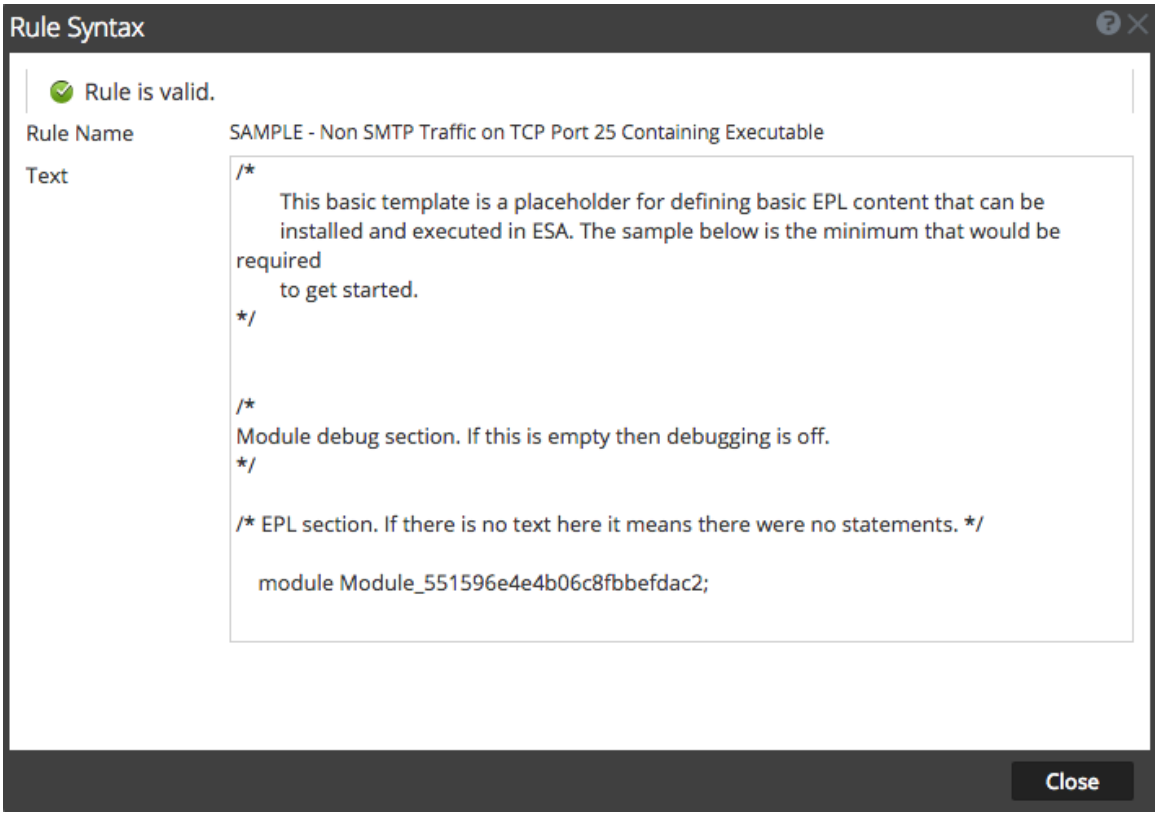
Biblioteca de reglas.

d. En la fila de una regla existente, seleccione > **Editar**.

La regla nueva o existente se muestra en una nueva pestaña y se puede editar.

3. Haga clic en **Mostrar sintaxis** en la parte inferior de la pestaña.

La siguiente figura es un ejemplo del cuadro de diálogo Sintaxis de regla.



Características

En la siguiente tabla se describen los parámetros del cuadro de diálogo Sintaxis de regla.

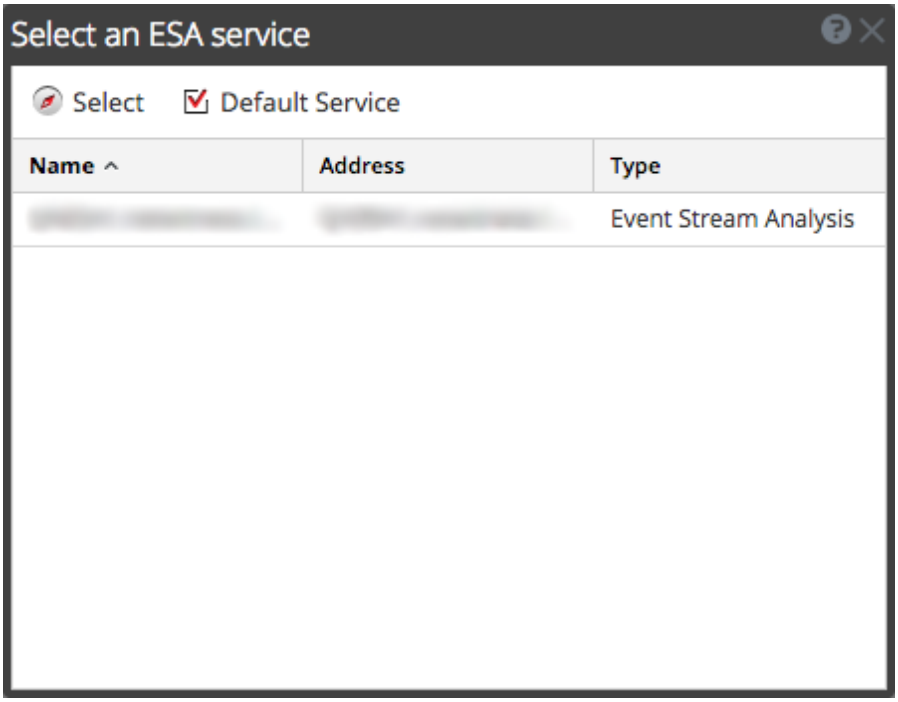
Parámetros	Descripción
La regla es válida o **Error de validación en la regla**	Indica si la sintaxis de la regla es válida o si se debe modificar.
Nombre de la regla	Muestra el nombre de la regla.
Texto	Muestra la sintaxis de EPL de condiciones, declaraciones y parámetros de depuración si la regla es válida.

Cuadro de diálogo Seleccionar un servicio de ESA

En este tema se describen las funciones del cuadro de diálogo Seleccionar un servicio de ESA. El cuadro de diálogo Seleccionar un servicio de ESA muestra todos los servicios de ESA disponibles. La selección de un servicio permite ver un resumen del servicio en la vista Resumen.

Para acceder a este cuadro de diálogo, en el menú de Security Analytics, seleccione **Alertas** > **Resumen**. Si el cuadro de diálogo Seleccionar un servicio de ESA no se muestra automáticamente, haga clic en  .

En la siguiente figura se muestra un ejemplo de este cuadro de diálogo.



Características

En la siguiente tabla se describen las funciones del cuadro de diálogo Seleccionar un servicio de ESA.

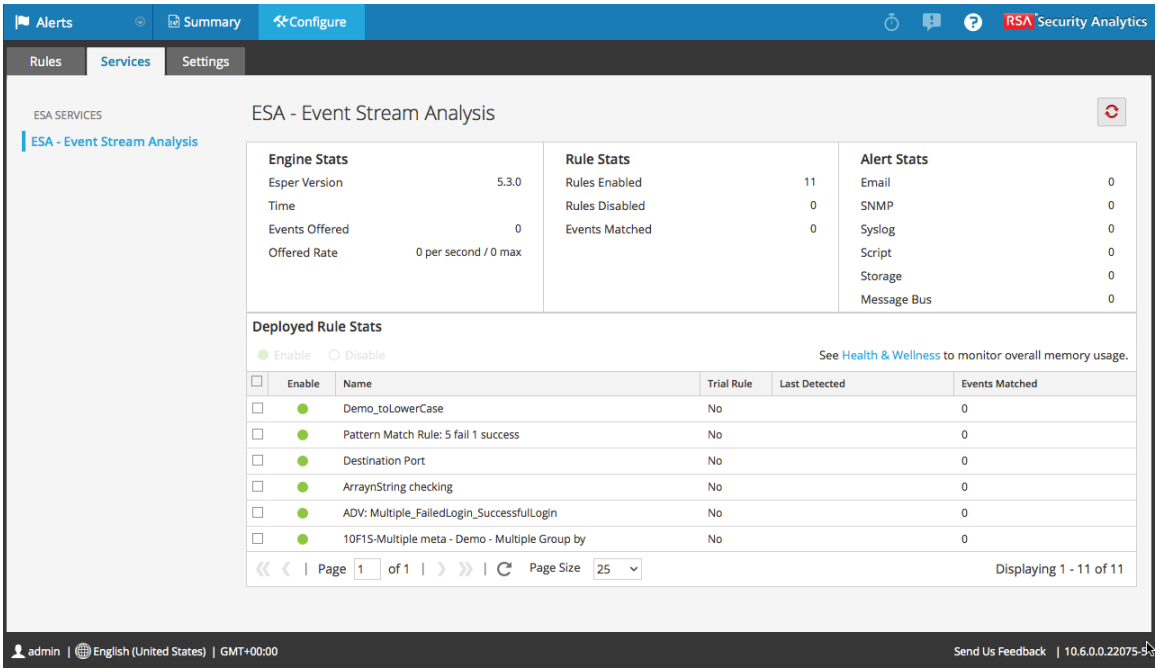
Parámetros	Descripción
Seleccionar	Se muestra la vista Resumen del servicio seleccionado.
Servicio predeterminado	Designa un servicio predeterminado. La vista Resumen se mostrará automáticamente para el servicio predeterminado.

Parámetros	Descripción
Nombre	Muestra el nombre del servicio de ESA.
Dirección	Muestra la dirección del servicio de ESA.
Tipo	Muestra el tipo de servicio.

Pestaña Servicios

En este tema se proporciona una descripción general de la pestaña **Alertas > Configurar > Servicios**. En la pestaña Servicios se proporcionan detalles de los servicios de ESA agregados a Security Analytics.

En la siguiente figura se muestra la pestaña Servicios:



La pestaña Servicios incluye las siguientes secciones:

- Panel Servicios de ESA
- Panel Estadísticas generales
- Panel Estadísticas de reglas implementadas

Características

Panel Servicios de ESA

En el panel Servicios de ESA se muestra el nombre de cada servicio de ESA agregado a Security Analytics.

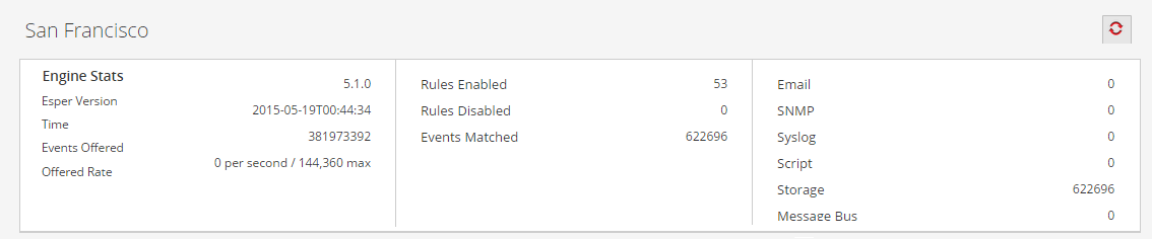
Panel Estadísticas generales

En el panel Estadísticas generales se proporciona información sobre el motor, las reglas y las alertas de Esper.

El panel Estadísticas generales incluye las siguientes secciones:

- Estadísticas de motor
- Estadísticas de reglas
- Estadísticas de alerta

En la siguiente figura se muestra el panel Estadísticas generales.



En la tabla se enumeran y se describen los parámetros de cada sección.

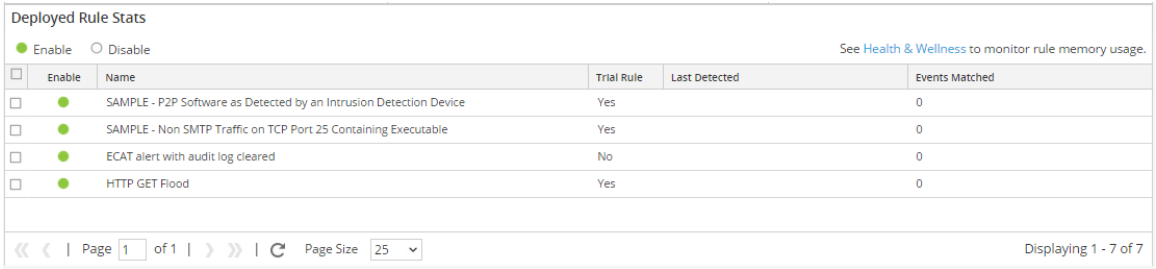
Secciones	Parámetro	Descripción
Estadísticas de motor	Versión de Esper	La versión de Esper que se ejecuta en el servicio de ESA
	Hora	La hora en que se envió el último evento al motor de Esper
	Eventos ofre-cidos	La cantidad de eventos que analizó el servicio de ESA desde el último inicio del servicio
	Tasa ofrecida	La tasa ofrecida de eventos actual en el servicio de ESA

Secciones	Parámetro	Descripción
Estadísticas de reglas	Reglas activadas	La cantidad de reglas habilitadas
	Reglas des-activadas	La cantidad de reglas inhabilitadas
	Eventos con coin-cidencias	Cantidad total de eventos que coinciden con todas las reglas del servicio de ESA
Estadísticas de alerta	Correo elec-trónico	Cantidad de notificaciones por correo electrónico que envió el servicio de ESA
	SNMP	Cantidad de notificaciones SNMP que envió el servicio de ESA
	Syslog	Cantidad de notificaciones de syslog que envió el servicio de ESA
	Script	Cantidad de notificaciones de script que envió el servicio de ESA
	Storage	Cantidad total de alertas almacenadas en la base de datos
	Bus de mensajes	Cantidad de alertas enviadas al bus de mensajes

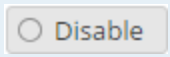
Panel Estadísticas de reglas implementadas

En el panel Estadísticas de reglas implementadas se proporcionan detalles sobre las reglas que se implementan en el servicio de ESA.

En la siguiente figura se muestra el panel Estadísticas de reglas implementadas.



En la tabla se indican los diversos parámetros de la vista y su descripción.

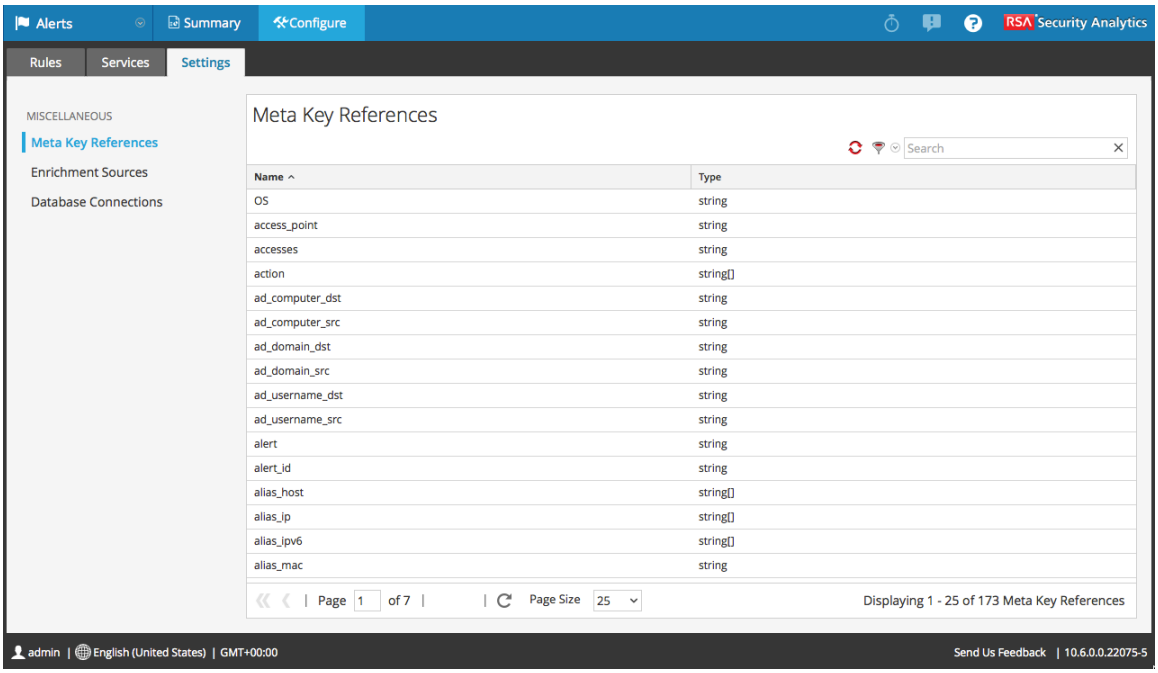
Parámetros	Descripción
	Indica que la regla está habilitada. Habilita una regla que se deshabilitó.
	Indica que la regla está deshabilitada. Deshabilita una regla que se habilitó.
Estado y condición	Muestra un snapshot del uso de la memoria cuando se inhabilitan las reglas de prueba.
Habilitar	Indica si la regla está activada o desactivada. El ícono verde indica que la regla está habilitada. El ícono blanco indica que la regla está inhabilitada.
Nombre	Nombre de la regla de ESA.
Regla de prueba	Indica si la regla se está ejecutando en modo de regla de prueba.
Última detección	La última vez que se activó la alerta para la regla.
Eventos con coincidencias	La cantidad total de eventos que coincidieron con la regla.

Pestaña Ajustes de configuración

En este tema se describen los componentes de la pestaña Configuración. La pestaña Ajustes de configuración permite realizar las siguientes tareas:

- Ver una lista de claves de metadatos
- Configurar un origen de enriquecimiento de datos
- Agregar una conexión a una base de datos externa

En la siguiente figura se muestra la sección Referencias de claves de metadatos de la pestaña Configuración.



Características

Referencias de claves de metadatos

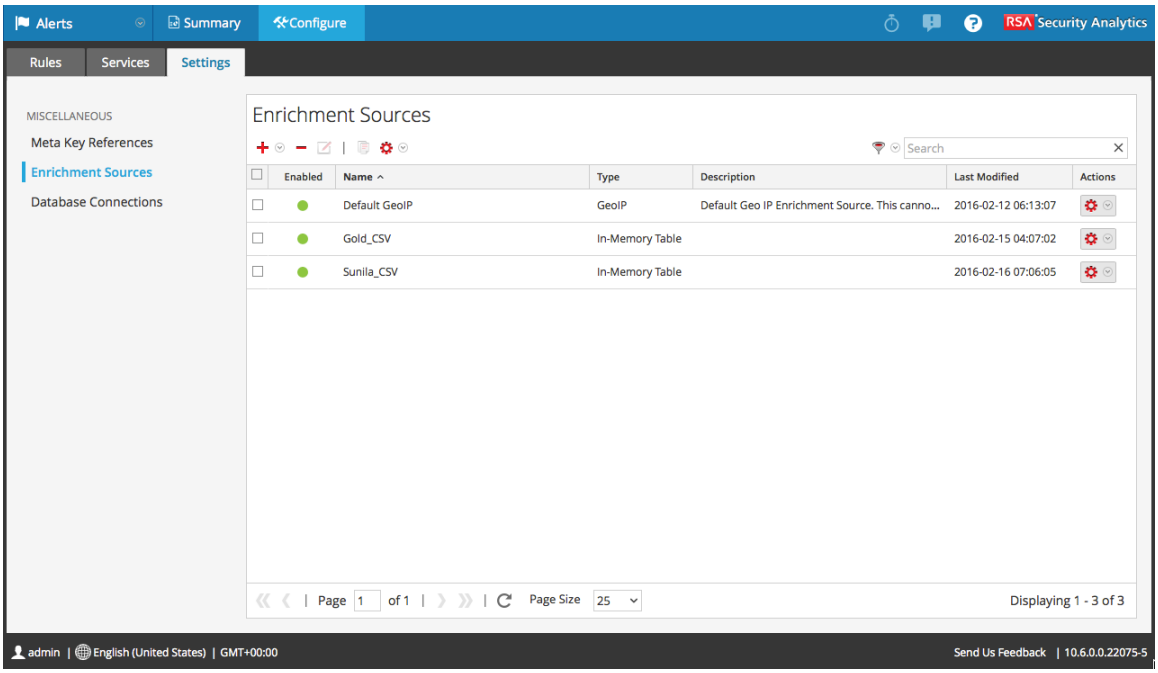
En la sección Referencias de claves de metadatos se enumera cada clave de metadatos y el tipo de valor que requiere la clave.

Orígenes de enriquecimiento

La sección Orígenes de enriquecimiento permite configurar los siguientes orígenes de datos externos:

- GeoIP
- Referencia de base de datos externa
- Tabla en la memoria
- Warehouse Analytics

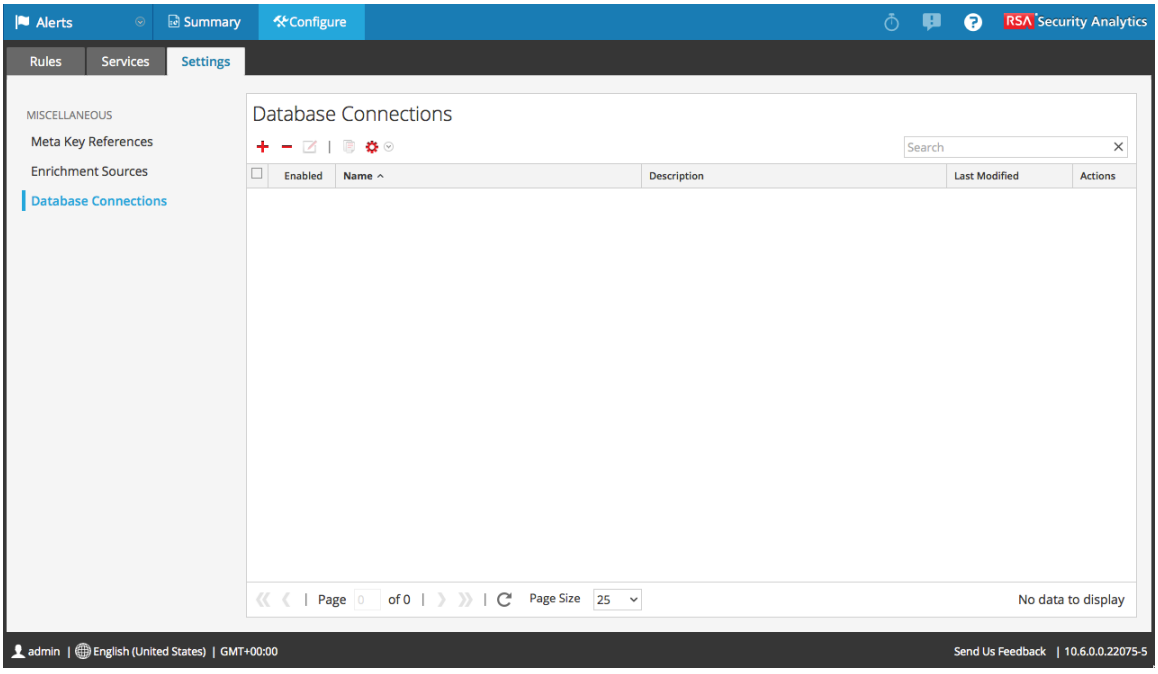
En la siguiente figura se muestra la sección Orígenes de enriquecimiento de la pestaña Configuración.



Conexiones de la base de datos

La sección Conexiones de la base de datos permite configurar una conexión a una base de datos externa de modo que ESA pueda acceder a esos datos.

En la siguiente figura se muestra la sección Conexiones de la base de datos de la pestaña Configuración.



En la sección Conexiones de la base de datos, puede ejecutar lo siguiente:

- Agregar una conexión de base de datos
- Eliminar una conexión de base de datos
- Editar una conexión de base de datos
- Duplicar una conexión de base de datos
- Importar una conexión de base de datos
- Exportar una conexión de base de datos

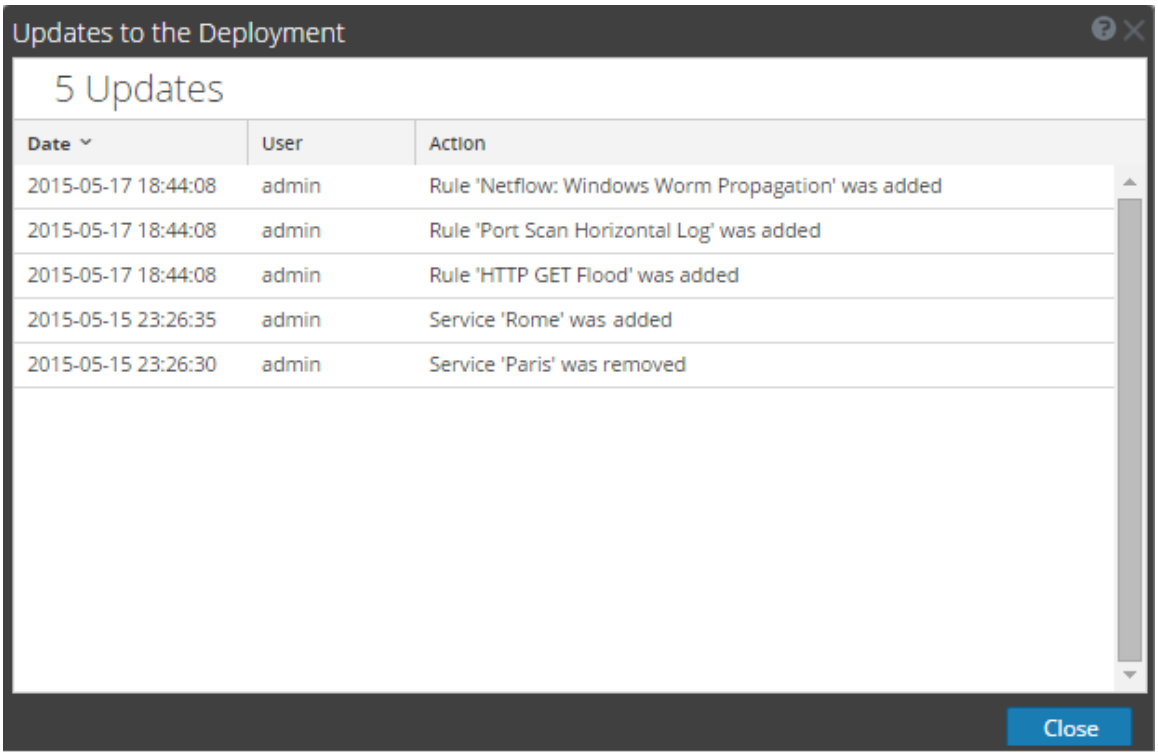
Cuadro de diálogo Actualizaciones a la implementación

En el cuadro de diálogo Actualizaciones a la implementación se muestran los cambios en la implementación, como la adición de una regla o un servicio. Las actualizaciones a la implementación se indican con el ícono de actualización ( ) junto al nombre de la implementación en el panel de opciones de la pestaña Reglas.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Alertas > Configurar**.
   La pestaña Reglas se muestra de manera predeterminada.
2. En la sección **Implementaciones** del panel de opciones, seleccione o agregue una implementación.
3. En el panel **Implementación**, haga clic en **Mostrar actualizaciones**.
   Se muestra el cuadro de diálogo Actualizaciones a la implementación.

En la siguiente figura se muestra un ejemplo de este cuadro de diálogo.



Características

En la parte superior del cuadro de diálogo Actualizaciones a la implementación se muestra la cantidad de actualizaciones. En la siguiente tabla se describen los parámetros de este cuadro de diálogo.

Parámetros	Descripción
Fecha	Muestra el día y la hora de la actualización.
Usuario	Muestra el usuario que realizó la actualización.
Acción	Describe la actualización.