RSA NETWITNESS® SUITE

Guía de configuración de ESA

para la versión 11.0

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de EMC, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por EMC.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

EMC considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

febrero 2018

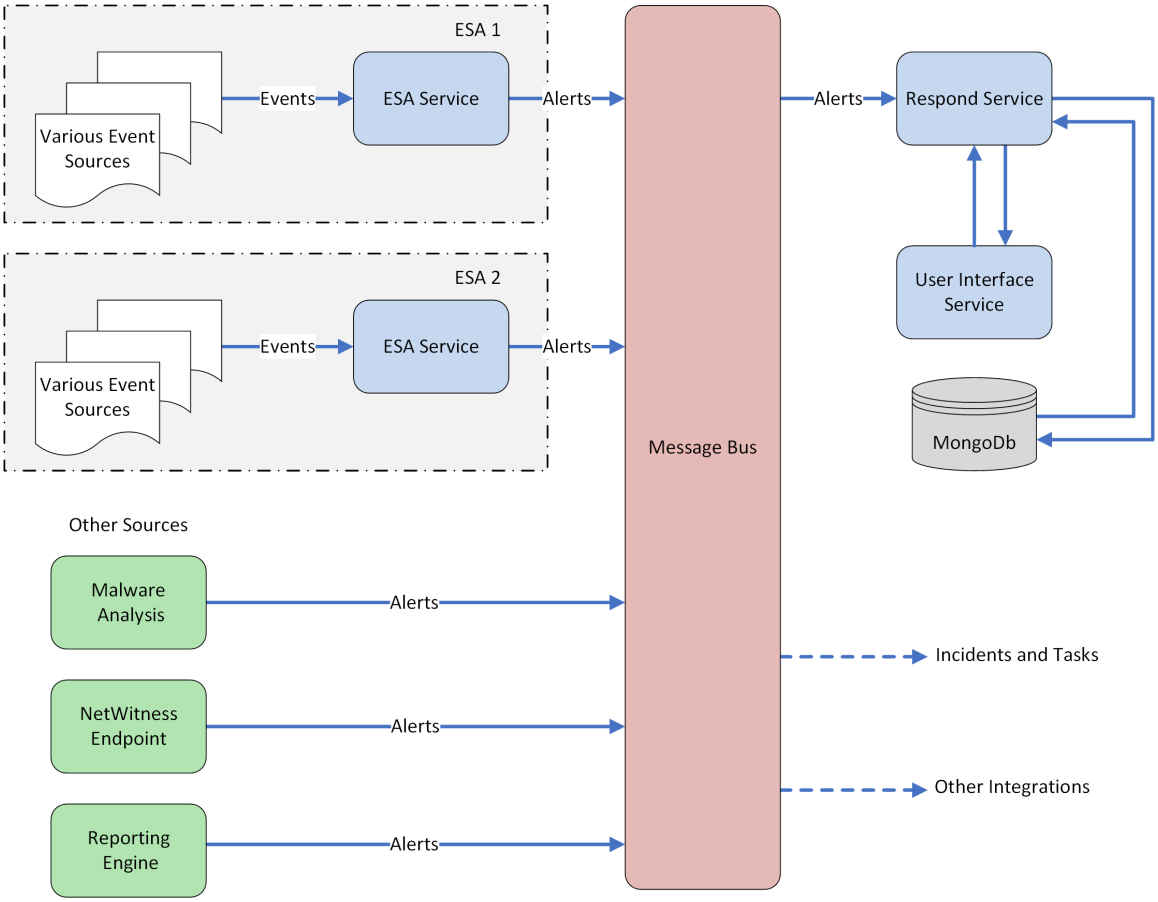
Contenido

Descripción general de Event Stream Analysis

RSA NetWitness® Suite Event Stream Analysis (ESA) proporciona analítica de flujo avanzada, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de Concentrators.

El lenguaje de procesamiento de eventos avanzado de ESA permite expresar filtrado, agregación, combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. Event Stream Analysis ayuda a realizar detección de incidentes y alertas eficaces.

En el siguiente diagrama se muestra el flujo de trabajo de datos general:



Hay dos servicios de ESA que se pueden ejecutar en un host de ESA:

- Event Stream Analysis (ESA Correlation Rules)
- Event Stream Analytics Server (ESA Analytics)

El primer servicio es Event Stream Analysis, un servicio que crea alertas a partir de reglas de ESA, también conocido como ESA Correlation Rules, las cuales se crean manualmente o se descargan desde Live. El segundo servicio es ESA Analytics, un servicio que se utiliza para Detección de amenazas automatizadas. Debido a que el servicio ESA Analytics utiliza módulos preconfigurados de ESA Analytics para Detección de amenazas automatizadas, no es necesario crear ni descargar reglas para usarlo.

Los servicios ESA Analytics utilizan agregación basada en consultas (QBA) para recopilar eventos filtrados para los módulos ESA Analytics desde Concentrators. Solo los datos que requiere un módulo se transfieren entre el Concentrator y el sistema ESA Analytics. Por ejemplo, con el uso de un módulo Suspicious Domains ESA Analytics, como C2 para paquetes (http-packet), un servicio ESA Analytics puede examinar el tráfico HTTP para determinar la probabilidad de que exista actividad maliciosa en el ambiente.

Configurar reglas de correlación de ESA

En este tema se proporcionan tareas generales para configurar reglas de correlación de RSA NetWitness Suite Event Stream Analysis (ESA) mediante el servicio Event Stream Analysis.

Requisitos previos

Asegúrese de que:

- Instaló el servicio Event Stream Analysis en el ambiente de red.
- Instaló y configuró uno o más Concentrators en el ambiente de red.

Procedimiento

Nota: Puede configurar ESA mediante un puerto SSL (50030) solamente. No hay ninguna opción para configurar un puerto que no sea SSL.

Para configurar Event Stream Analysis:

Tareas	Referencia
1. Agregar un Concentrator como un origen de datos al servicio Event Stream Analysis.	Consulte Paso 1. Agregar un origen de datos a un servicio de ESA
2. Configurar notificaciones para el servicio Event Stream Analysis.	Consulte “Métodos de notificación” en la *Guía de alertas mediante ESA*.
3. Descargar contenido de Event Stream Analysis mediante Live.	Consulte “Vista Buscar en Live” en la *Guía de administración de recursos de Live*.
4. (Opcional) Configuración avanzada para el servicio Event Stream Analysis.	Consulte Paso 2. Configurar ajustes avanzados para un servicio de ESA.

Resultado

El servicio Event Stream Analysis se configura y ahora puede agregar reglas de ESA para el procesamiento de eventos y para alertas. Para obtener información sobre cómo agregar reglas de ESA, consulte “Agregar reglas a la Biblioteca de reglas” en la *Guía de alertas mediante ESA*.

Paso 1. Agregar un origen de datos a un servicio de ESA

En este tema se describe cómo agregar un origen de datos nuevo o existente al servicio de Event Stream Analysis.

Un servicio de ESA recopila datos de un Concentrator para detectar incidentes y alertar al usuario. Para que ESA analice datos, debe configurar los orígenes desde los cuales ESA los leerá. Utilice los procedimientos de este tema para agregar orígenes de datos para ESA.

Requisitos previos

Debe tener uno o más Concentrators configurados en NetWitness Suite.

El servicio Event Stream Analysis debe estar instalado y en ejecución en NetWitness Suite.

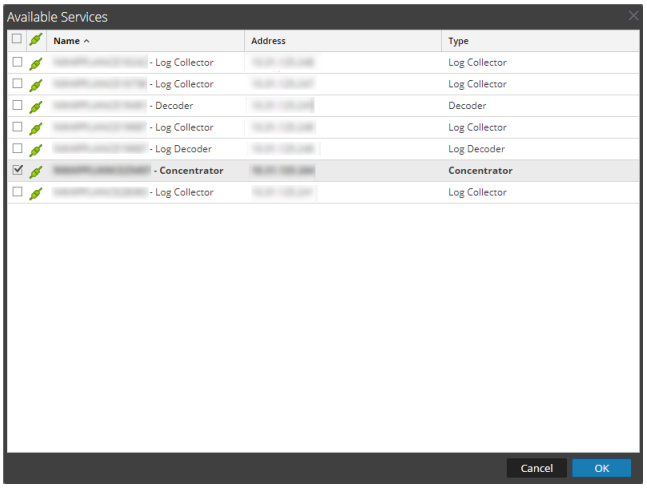
Debe ejecutar los siguientes pasos para agregar un origen de datos:

- Agregar un origen de datos disponible
- Especificar el nombre de usuario y la contraseña del origen de datos

Procedimientos

Agregar servicios existentes como un origen de datos

1. Vaya a **ADMIN> Servicios**.
   Se muestra la vista Servicios.
2. En la vista Servicios, seleccione un servicio ESA y elija > **Ver** > **Configuración**.
3. En la pestaña **Orígenes de datos**, haga clic en .
   Los servicios disponibles aparecen como se muestra en la siguiente figura.



4. Seleccione uno o más Concentrators y haga clic en **Aceptar**.
   El servicio se agrega a la lista de servicios de la pestaña **Orígenes de datos**.

5. (Opcional) Haga clic en **Activar** para habilitar el origen de datos.
6. Haga clic en **Aplicar** para guardar la configuración.

Especificar el nombre de usuario y la contraseña del origen de datos

Nota: Puede agregar un Log Decoder como origen de datos para ESA, pero RSA recomienda agregar un Concentrator para aprovechar la agregación no dividida, puesto que el Decoder puede tener otros procesos que se agregan de este.

Para especificar el nombre de usuario y la contraseña del origen de datos:

1. Vaya a **ADMIN > Servicios**.
   Se muestra la vista Servicios.
2. En la vista **Servicios**, seleccione un servicio Concentrator.
3. Haga clic en  .
4. Especifique el nombre de usuario y la contraseña.
5. Haga clic en **Guardar**.

Paso 2. Configurar ajustes avanzados para un servicio de ESA

En este tema se proporcionan instrucciones para configurar los ajustes avanzados de un servicio de Event Stream Analysis.

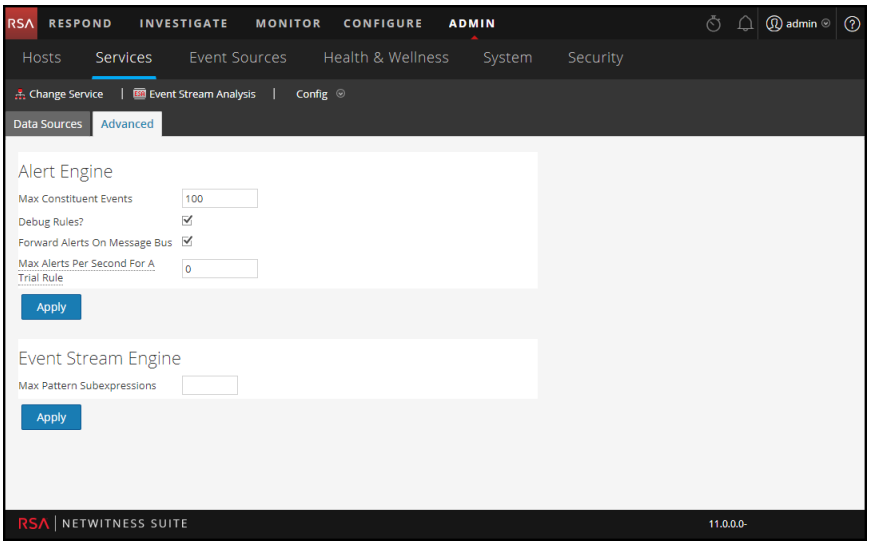
En la vista Opciones avanzadas, puede configurar ajustes avanzados para mejorar el rendimiento, preservar eventos para reglas con múltiples eventos, colocar en el búfer eventos en la memoria y especificar la cantidad de eventos que se almacenarán en ESA.

Procedimientos

Configurar ajustes avanzados

Para acceder a la vista Opciones avanzadas y configurar ajustes avanzados para un servicio de ESA:

1. Vaya a **ADMIN > Servicios**.
   Se muestra la vista Servicios.
2. En la vista Servicios, seleccione un servicio ESA y elija  **> Ver > Configuración**.
3. Seleccione la pestaña **Opciones avanzadas**.
   Se muestra la vista Avanzada.



Configurar ajustes del motor de alertas

La sección Motor de alertas permite especificar valores para conservar eventos para reglas que eligen varios eventos.

Nota: Después de actualizar a 10.5, la opción Depurar reglas se inhabilitará si estaba habilitada anteriormente. Deberá habilitar esta opción después de la actualización.

La figura siguiente muestra la sección Motor de alertas.

Para configurar los ajustes del motor de alertas:

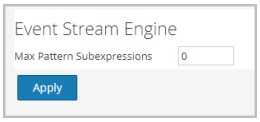
1. En la sección Motor de alertas, especifique un valor para **Máx. de eventos constitutivos**. El valor predeterminado es 100.
2. Seleccione **¿Depurar reglas?** para habilitar la depuración de reglas.
3. Si desea que las alertas se envíen al bus de mensajes y a Respond, seleccione la opción **Reenviar alertas en bus de mensajes**.
4. Para especificar la cantidad máxima de alertas que se reenvían al bus de mensajes para la regla de prueba, seleccione **Cantidad máxima de alertas por segundo para una regla de prueba**. El valor predeterminado es **10**.
5. Haga clic en **Aplicar** para guardar los cambios e implementarlos inmediatamente.

Nota: Para obtener más información acerca de los parámetros de la sección Motor de alertas, consulte Ajustes del motor de alertas en la vista Avanzada de ESA.

Configurar ajustes del motor de flujo de eventos

La sección Motor de flujo de eventos permite especificar detalles para mejorar el rendimiento.

En la siguiente figura se muestra la sección Motor de flujo de eventos.



Para configurar los ajustes del motor de flujo de eventos:

1. En la sección Motor de flujo de eventos, especifique **Máx. de subexpresiones de patrón**.
2. Haga clic en **Aplicar** para guardar los cambios e implementarlos inmediatamente.

Nota: Para obtener más información acerca de los parámetros de la sección Motor de flujo de eventos, consulte Ajustes del motor de flujo de eventos en la vista Avanzada de ESA.

Configurar ESA Analytics

En esta sección se proporcionan tareas generales para configurar los servicios ESA Analytics para Detección de amenazas automatizadas de RSA NetWitness® Suite. La funcionalidad Detección de amenazas automatizadas permite analizar los datos que residen en uno o más Concentrators mediante módulos ESA Analytics preconfigurados, como Suspicious Domains. Por ejemplo, con el uso de un módulo Suspicious Domains, un servicio ESA Analytics puede examinar el tráfico HTTP para determinar la probabilidad de que exista actividad maliciosa en el ambiente.

Hay dos servicios de ESA que se pueden ejecutar en un host de ESA:

- Event Stream Analysis (ESA Correlation Rules)
- Event Stream Analytics Server (ESA Analytics)

El primer servicio es Event Stream Analysis, un servicio que crea alertas a partir de reglas de ESA, también conocido como ESA Correlation Rules, las cuales se crean manualmente o se descargan desde Live. El segundo servicio es ESA Analytics, un servicio que se utiliza para Detección de amenazas automatizadas y se configura en esta sección. Debido a que el servicio ESA Analytics utiliza módulos preconfigurados de ESA Analytics para Detección de amenazas automatizadas, no es necesario crear ni descargar reglas para usarlo.

Actualmente hay dos módulos ESA Analytics disponibles para Suspicious Domains:

- C2 para paquetes (http-packet)
- C2 for Logs (http-log)

Configurar el servicio Búsqueda de Whois

La funcionalidad Detección de amenazas automatizadas de RSA NetWitness Suite le permite analizar automáticamente los orígenes de datos mediante el uso de módulos ESA Analytics preconfigurados. Un módulo ESA Analytics es una canalización que consta de objetos de actividad que enriquecen un evento con información adicional a través de cálculos matemáticos. Los servicios ESA Analytics procesan estos módulos para identificar las amenazas avanzadas.

La configuración del servicio de búsqueda de Whois se requiere para los módulos Suspicious Domains.

Nota: (**Importante**) RSA recomienda especialmente configurar el servicio de búsqueda de Whois para lograr exactitud en el puntaje de Detección de amenazas automatizadas.

Requisitos previos

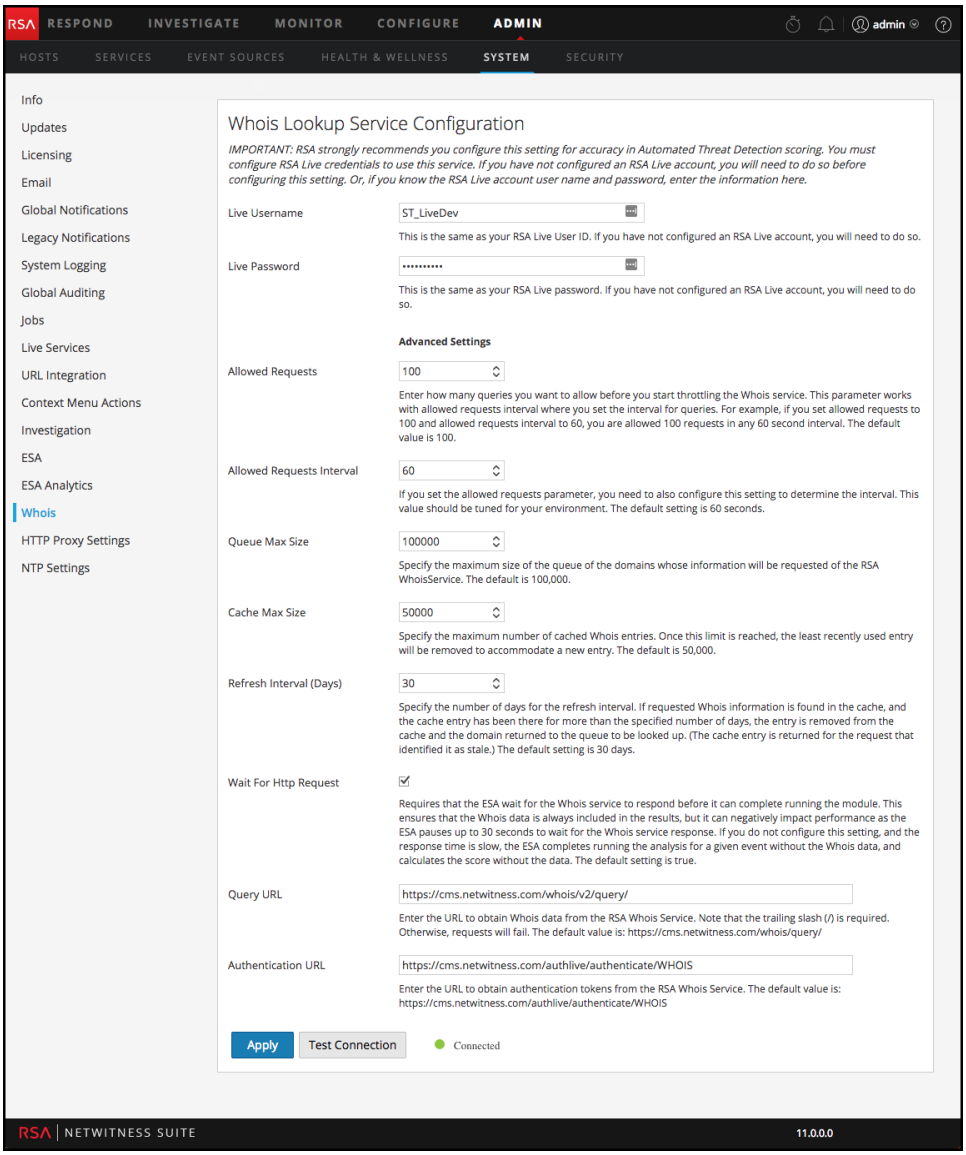
- Debe tener una cuenta de RSA Live para usar el servicio de búsqueda de Whois.
- El servicio Servidor de ESA Analytics debe estar disponible (se muestra un círculo verde) en ADMIN > vista Servicios.

Si configuró una cuenta de Live en el panel Servicios de Live (ADMIN > Sistemas > Servicios de Live), el servicio Búsqueda de Whois se configura automáticamente. Solo debe comprobar la conexión del servicio de búsqueda de Whois.

Nota: Si no tiene una cuenta de RSA Live, puede crear una en el Portal de registro de RSA Live:
https://cms.netwitness.com/registration/
En la *Guía de administración de servicios de Live* se proporciona información adicional.

Configurar el servicio Búsqueda de Whois

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Whois**.
3. En el panel **Configuración del servicio de búsqueda de Whois**, compruebe si el servicio de búsqueda de Whois está conectado. En la parte inferior del panel, un servicio conectado se muestra con un círculo verde junto a **Conectado**:



Si está conectado, terminó de realizar el proceso de configuración y puede omitir los pasos restantes. Para ajustar la configuración avanzada, vaya al paso 5.
Si el servicio no está conectado, continúe con el paso 4.

4. En los campos **Nombre de usuario de Live** y **Contraseña de Live**, ingrese credenciales de la cuenta de RSA Live para acceder al servidor de Whois de RSA.
5. Si es necesario, puede ajustar la configuración avanzada. Sin embargo, RSA recomienda usar los valores predeterminados. Configuración del servicio de búsqueda de Whois proporciona detalles adicionales.
6. Para probar la conexión, haga clic en **Probar conexión**.
   Una conexión correcta se muestra con un círculo verde junto a **Conectado**: ● Connected

7. Haga clic en **Aplicar** para guardar los cambios.

Mapeo de orígenes de datos de ESA a módulos Analytics

En este tema se indica a los administradores cómo mapear módulos ESA Analytics específicos a múltiples orígenes de datos y servicios de ESA Analytics, lo que puede hacer que el procesamiento sea más eficiente.

Puede analizar los datos que residen en uno o más Concentrators con la funcionalidad Detección de amenazas automatizadas de RSA NetWitness Suite mediante la selección de un módulo ESA Analytics preconfigurado. Los datos que analizan estos módulos se usan para identificar las amenazas avanzadas. Para usar mejor sus recursos de red y reducir el flujo de datos innecesario, puede mapear múltiples orígenes de datos, como Concentrators, a múltiples servicios ESA Analytics con el fin de procesar los datos de manera más eficiente y aprovechar la capacidad adicional.

Un *módulo ESA Analytics* es una canalización que consta de objetos de actividad que enriquecen un evento con información adicional a través de cálculos matemáticos. Los módulos ESA Analytics residen dentro de los servicios ESA Analytics.

Cuando implementa el mapeo, los servicios ESA Analytics seleccionados usan agregación basada en consultas para recopilar los eventos filtrados adecuados para el módulo seleccionado desde los Concentrators. La agregación basada en consultas es una consulta predefinida que solo transfiere datos para el módulo ESA Analytics seleccionado. Solo los datos que requiere el módulo se transfieren entre el Concentrator y el sistema ESA Analytics.

Actualmente hay dos módulos ESA Analytics disponibles para Suspicious Domains: C2 for Packets (http-packet) y C2 for Logs (http-log).

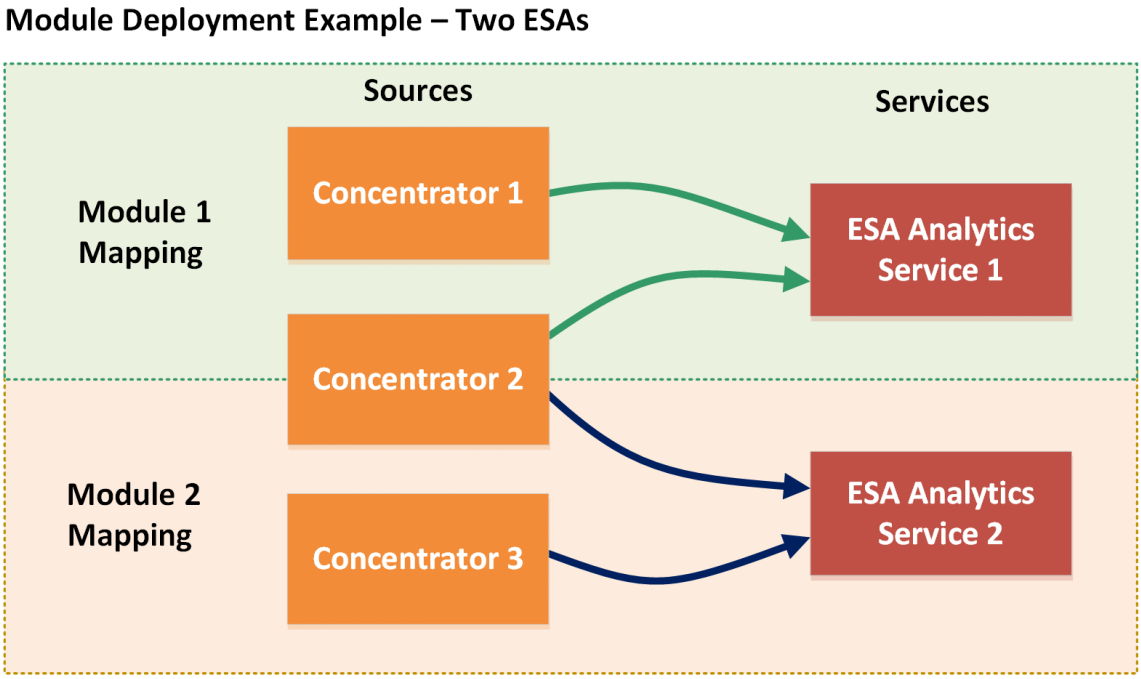
Ejemplo de implementación de módulo: dos ESA

Para aprovechar la capacidad adicional de un Concentrator, puede mapear un módulo ESA Analytics a un servicio ESA Analytics e implementarlo para analizar los datos de múltiples orígenes de datos al mismo tiempo.

Por ejemplo, si tiene tres Concentrators y dos servicios ESA Analytics, puede crear e implementar los siguientes mapeos:

- Mapear el Módulo 1 a los orígenes de los Concentrators 1 y 2 y al servicio ESA Analytics 1. El servicio ESA Analytics 1 analiza los eventos filtrados del Módulo 1 desde los Concentrators 1 y 2.
- Mapear el Módulo 2 a los orígenes de los Concentrators 2 y 3 y al servicio ESA Analytics 2. El servicio ESA Analytics 2 procesa los eventos filtrados del Módulo 2 desde los Concentrators 2 y 3.

En este ejemplo, el Módulo 1 representa un módulo ESA Analytics, como C2 for Packets (http-packet), y el Módulo 2 representa otro módulo ESA Analytics, como C2 for Logs (http-logs) en otra ubicación.



Este ejemplo muestra cómo ambos servicios pueden procesar datos desde el mismo Concentrator. Observe que los servicios ESA Analytics 1 y 2 pueden procesar datos desde el Concentrator 2. El servicio ESA Analytics 1 consulta datos para los eventos del Módulo 1 y el servicio ESA Analytics 2 consulta diferentes datos para los eventos del Módulo 2.

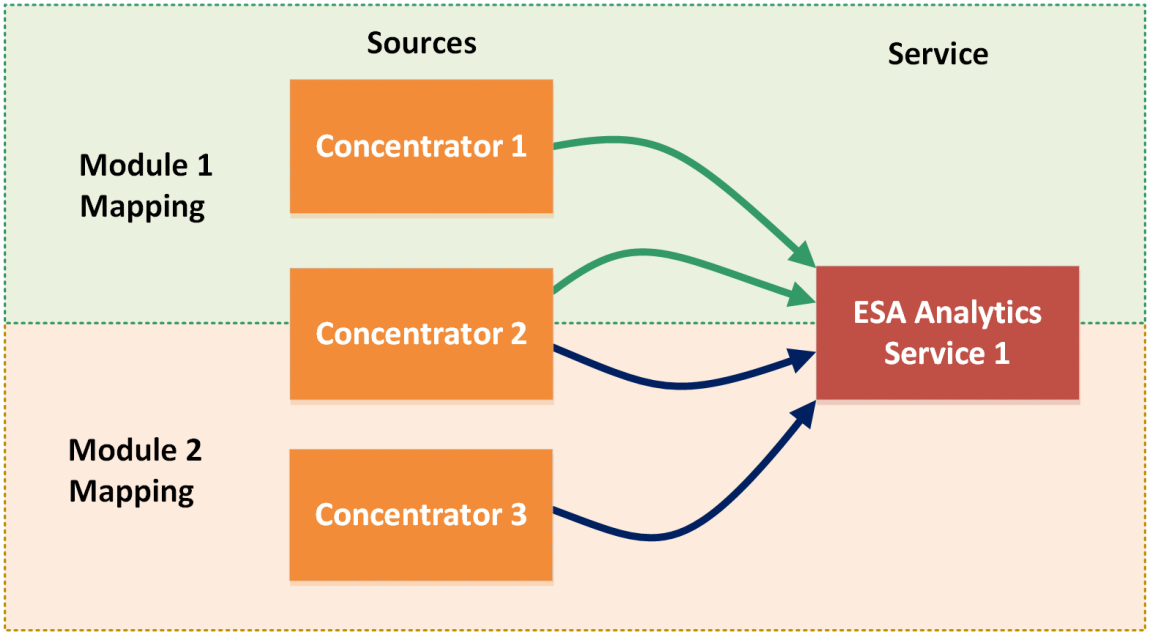
Ejemplo de implementación de módulo: un ESA

Además de crear mapeos de módulo que procesan distintos servicios ESA Analytics, puede mapear más de un módulo al mismo servicio ESA Analytics.

Por ejemplo, si tiene tres Concentrators y un servicio ESA Analytics, puede crear e implementar los siguientes mapeos:

- Mapear el Módulo 1 a los orígenes de los Concentrators 1 y 2 y al servicio ESA Analytics 1. El servicio ESA Analytics 1 analiza los eventos filtrados del Módulo 1 desde los Concentrators 1 y 2.
- Mapear el Módulo 2 a los orígenes de los Concentrators 2 y 3 y al servicio ESA Analytics 1. El servicio ESA Analytics 1 también procesa los eventos filtrados del Módulo 2 desde los Concentrators 2 y 3.

Module Deployment Example – One ESA



En este ejemplo se muestra cómo un servicio puede procesar los datos de más de un módulo. Observe que el servicio ESA Analytics 1 puede procesar datos desde los Concentrators 1 y 2 para el Módulo 1. También procesa datos de los Concentrators 2 y 3 para el Módulo 2. El servicio ESA Analytics 1 consulta datos para los eventos del Módulo 1 y consulta diferentes datos para los eventos del Módulo 2.

Precaución: Asegúrese de que todos los servicios de host de NetWitness Suite estén sincronizados con un origen de tiempo coherente.

Requisitos previos

- Todos los servicios de host de NetWitness Suite deben estar sincronizados con un origen de tiempo coherente.
- Los servicios y los hosts de Concentrator se deben descubrir y deben estar disponibles en la interfaz del usuario de NetWitness Suite.
- Se deben cumplir todos los requisitos específicos de cada módulo.
  - Para Suspicious Domains:
    - Configurar los ajustes de registro (Suspicious Domains para registros solamente)
    - Crear una lista blanca mediante el servicio Context Hub.
    - Configurar el servicio Búsqueda de Whois.

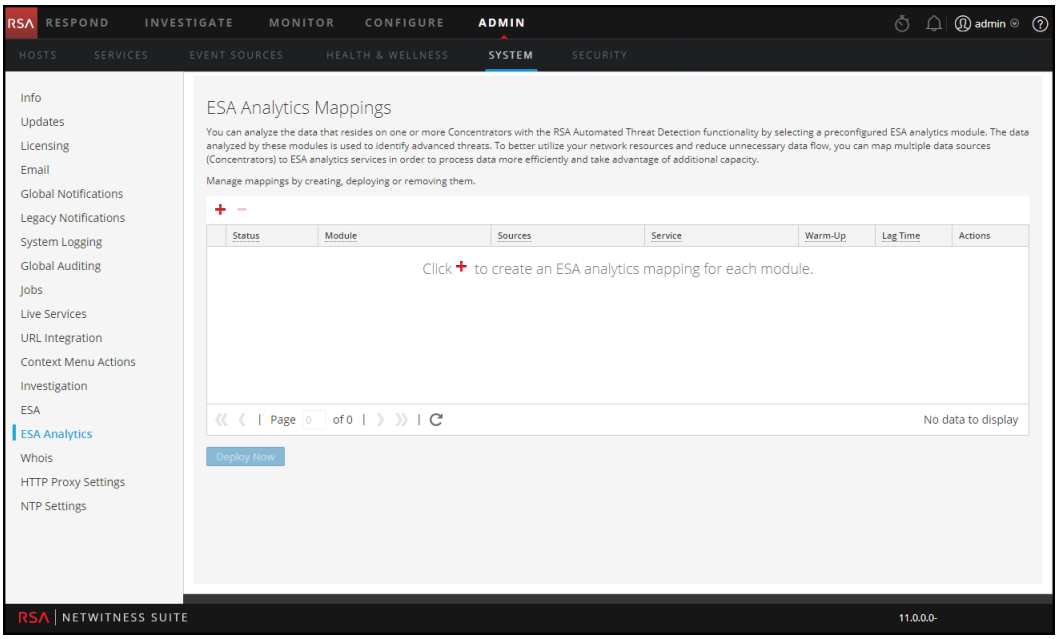
- Verificar que la regla de incidentes C2 esté habilitada y monitorear la actividad.
- Verificar que los incidentes se agrupen por Sospecha de C&C.

Para conocer los procedimientos paso a paso, consulte la *Guía de Detección de amenazas automatizadas* de *NetWitness Suite*.

Crear mapeos de ESA Analytics

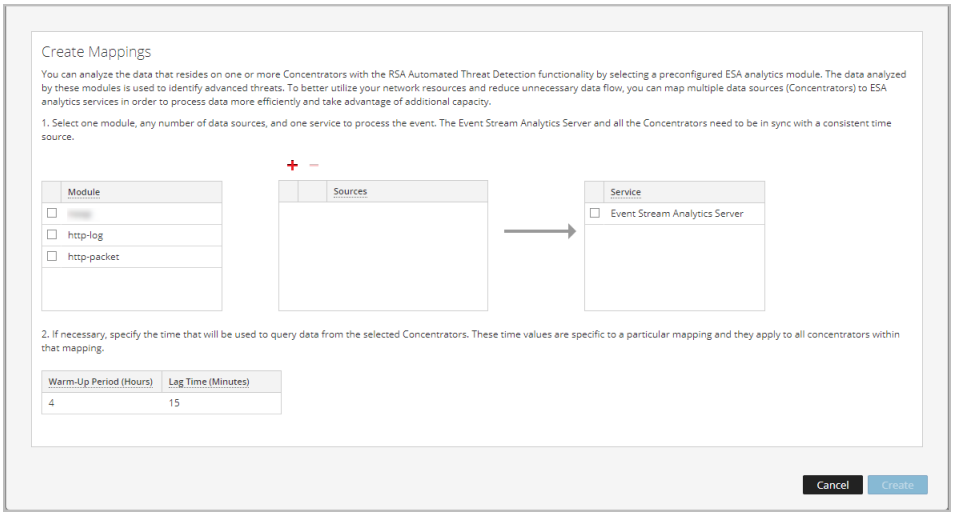
En el siguiente procedimiento se indica cómo mapear módulos ESA Analytics a orígenes y servicios. Después de crear y revisar los mapeos, impleméntelos de manera que puedan iniciar la agregación de datos.

1. Vaya a **ADMIN** > **Sistema** y, en el panel de opciones, seleccione **ESA Analytics**.
   Se muestra el panel **Mapeos de ESA Analytics**.

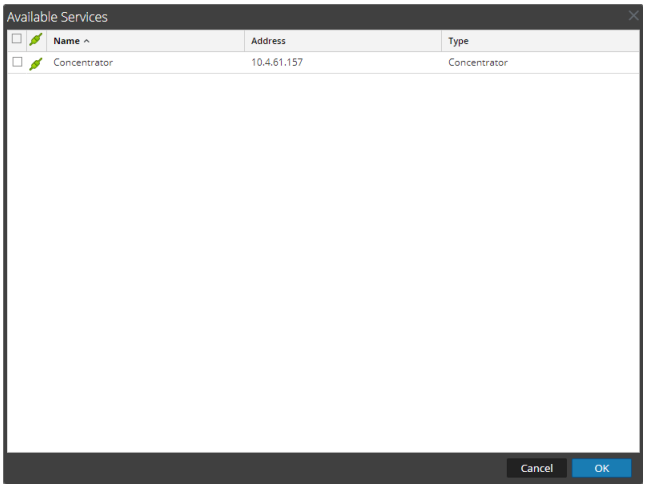


2. Haga clic en + para crear un mapeo de ESA Analytics. Cree un mapeo por separado para cada módulo.

Se muestra el cuadro de diálogo **Crear mapeos**.

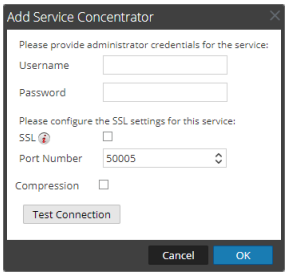


3. En la lista **Módulo**, seleccione un módulo.
4. Configure uno o más orígenes de datos (Concentrators) para los mapeos. Para cada Concentrator, realice lo siguiente:
   a. Haga clic en + .
      En el cuadro de diálogo Orígenes disponibles se muestran los orígenes de datos que están disponibles en la vista Admin > Servicios.



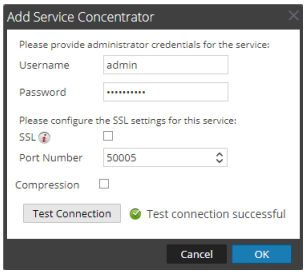
   b. En el cuadro de diálogo **Orígenes disponibles**, seleccione un Concentrator y haga clic en **Aceptar**.

Se muestra el cuadro de diálogo Agregar origen.



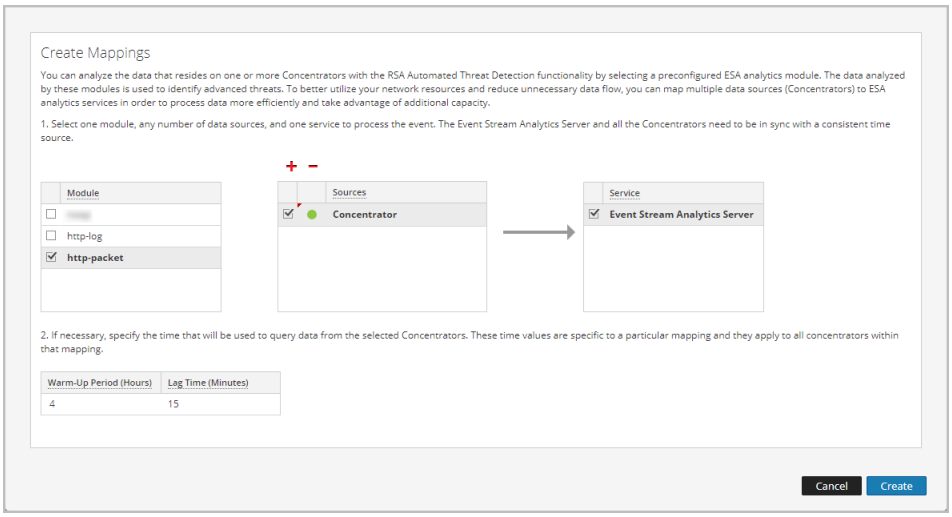
c. En el cuadro de diálogo **Agregar origen**, escriba el nombre de usuario y la contraseña de administrador para el Concentrator.

d. Haga clic en **Probar conexión** para asegurarse de que pueda comunicarse con el servicio ESA Analytics.



e. Haga clic en **Aceptar**.
Después de configurar los orígenes de datos y que estos aparezcan en la lista Orígenes, puede volver a usarlos para mapeos adicionales.

5. En la lista **Orígenes**, seleccione uno o más orígenes de datos para agregar los datos para el módulo.



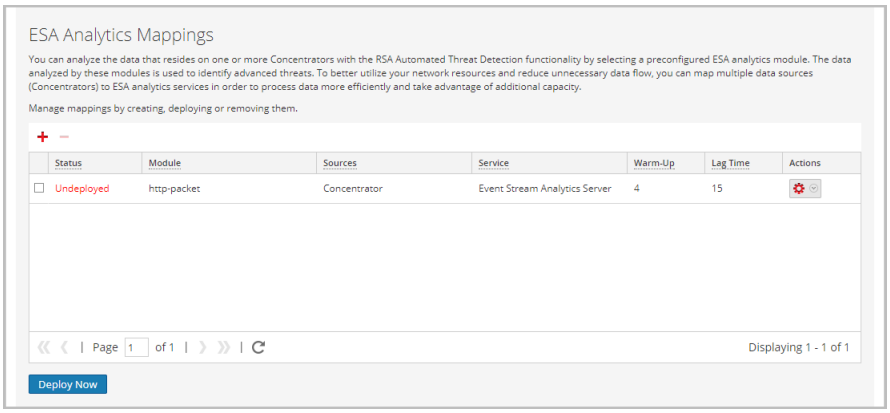
Un círculo de color verde indica un servicio en ejecución y un círculo de color blanco indica un servicio detenido.

6. En la lista **Servicio**, seleccione un servicio ESA Analytics para procesar los datos para el módulo.
7. Si es necesario, especifique el tiempo que se usará para consultar los datos desde los Concentrators seleccionados:

Campo	Descripción
Período de preparación (horas)	Especifica una duración de preparación (en horas). Se requiere un período de preparación para permitir que Detección de amenazas automatizadas "conozca" su tráfico. El período de preparación se debe ejecutar cuando se esté ejecutando el tráfico típico. Durante este tiempo, se suprimen las alertas para el mapeo de módulo. El período de preparación prepara el módulo con datos históricos y garantiza que se complete la cantidad especificada de horas de recopilación de datos antes de que se envíen alertas. RSA proporciona módulos ESA Analytics preconfigurados. Cada tipo de módulo tiene un período de preparación predeterminado, que puede ajustar a su ambiente, si es necesario. Después de este período de preparación, se pueden ver las alertas. Para obtener más información sobre el período de preparación y el tiempo de retardo, consulte Configuración del módulo.

Campo	Descripción
Tiempo de retardo (minutos)	Especifica el retraso de tiempo constante en minutos, el cual se suma para evitar la pérdida de eventos que los orígenes de datos procesan durante períodos de gran actividad. Por ejemplo, el rendimiento del Concentrator varía en función de factores como carga entrante, consultas continuas e indexación. Debido a estos factores, es posible que un Concentrator no pueda agregar eventos en tiempo real, lo que genera el retraso. El parámetro Retardo da al Concentrator la oportunidad de terminar de agregar todos los datos. Después de que finaliza el período de preparación, la agregación de datos continúa en **Hora (del sistema) actual - Tiempo de retardo**. Esto es útil cuando la agregación de datos en un Concentrator se realiza con lentitud. El tiempo de retardo garantiza que el módulo no procese los datos que llegan al Concentrator dentro de la ventana de tiempo de retardo, de modo que haya un retraso adecuado para asegurar que el módulo pueda procesar todos los eventos que se generan en la empresa. Por ejemplo, si el tiempo de retardo es 30 minutos y actualmente son las 14:00 h, el Concentrator comienza a extraer registros a las 13:30 h. La ventana de tiempo de retardo, 30 minutos en este ejemplo, permanece constante a medida que avanza la hora. Cuando la hora actual avanza hasta las 14:01 h, el Concentrator extrae los datos al minuto siguiente, a las 13:31 h, etc. **Importante**: El tiempo de retardo define el búfer entre la hora actual y la hora en que el módulo recopila los datos. **Precaución:** RSA recomienda que los administradores ajusten el parámetro Retardo de forma dinámica en función del rendimiento de cada uno de los Concentrators individuales para evitar la pérdida de eventos durante la agregación. Para obtener más información sobre el período de preparación y el tiempo de retardo, consulte Configuración del módulo.

8. Haga clic en **Crear**.
   Los mapeos que crea aparecen en la lista de mapeos existentes con un estado de **Implementación anulada**.



Importante: Para iniciar un módulo de manera que inicie la agregación de datos, debe implementarlo.

Implementar mapeos de ESA Analytics

Después de crear los mapeos, debe implementarlos para iniciar la agregación de datos para los módulos.

1. En la lista de mapeos, verifique que el estado de los mapeos que desea implementar se muestre como **Implementación anulada**.
2. Seleccione uno o más mapeos con un estado de Implementación anulada y seleccione **Implementar ahora**.
   Todos los mapeos seleccionados en el estado Implementación anulada inician la agregación de datos como está configurado en el mapeo. El estado del mapeo cambia a **Implementado**.
   No puede implementar un mapeo que ya está implementado.

Actualizar un mapeo

Solo puede tener un mapeo por módulo. Si desea realizar cambios en un mapeo implementado, como agregar o quitar Concentrators o cambiar el servicio, debe anular la implementación y eliminar el mapeo existente y, a continuación, crear e implementar un nuevo mapeo para ese módulo.

Puede realizar las siguientes actualizaciones a un mapeo implementado sin eliminarlo:

- Anular la implementación del mapeo
- Cambiar el período de preparación y el tiempo de retardo

También puede cambiar el período de preparación y el tiempo de retardo para un mapeo de módulo con implementación anulada.

Anular la implementación de un mapeo

Si desea detener la agregación de datos para un mapeo de módulo, pero no desea eliminar el mapeo, puede anular la implementación de este. Esto le ofrece la opción de implementarlo posteriormente. Cuando anula la implementación de un mapeo, el servicio ESA Analytics especificado deja de extraer datos del origen de datos para ese módulo.

Precaución: Anular la implementación de un mapeo con un estado de Implementado afectará la agregación de datos para ese módulo.

Para anular la implementación de un mapeo:

1. En el panel Mapeos de ESA Analytics, seleccione el mapeo implementado para el cual desea anular la implementación.
2. En la columna **Acciones**, seleccione  > **Anular implementación**.

   El estado cambia de Implementado a Implementación anulada y se detiene la agregación de datos.

Eliminar un mapeo

Puede eliminar un mapeo con un estado de Implementación anulada en cualquier momento. Puesto que un mapeo en el estado Implementación anulada no se está ejecutando, no afecta la agregación de datos.

Debe anular la implementación de un mapeo con un estado de Implementado antes de eliminarlo. Anular la implementación de un mapeo y eliminarlo borran la configuración en el servidor de ESA, revierte la implementación para ese mapeo y detiene la extracción de datos del origen de datos para ese módulo.

Precaución: Anular la implementación de un mapeo y eliminarlo afectarán la agregación de datos para ese módulo.

Para eliminar un mapeo:

1. En el panel Mapeos de ESA Analytics, seleccione el mapeo que desea eliminar. Solo puede eliminar un mapeo a la vez.
2. Haga clic en .

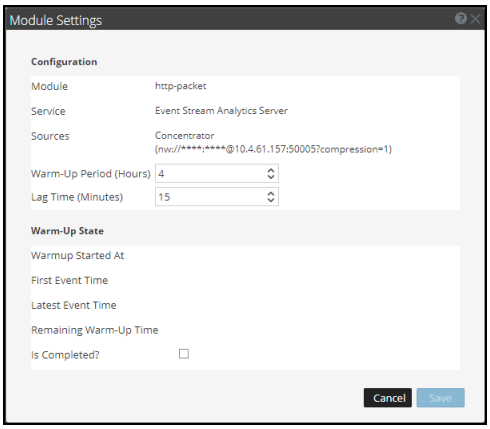
Cambiar el período de preparación y el tiempo de retardo

Puede ajustar el período de preparación para un mapeo de módulo específico. Por ejemplo, una vez que se completa el período de preparación, puede aumentar la configuración del período de preparación para permitir un tiempo de preparación adicional. Incluso puede aumentar el período de preparación cuando el mapeo de módulo se está preparando activamente.

Si es necesario, puede cambiar el tiempo de retardo para el módulo. El tiempo de retardo define el búfer entre la hora (del sistema) actual y la hora en que el módulo recopila los datos.

1. En el panel Mapeos de ESA Analytics, seleccione el mapeo que desea cambiar y en la columna **Acciones**, seleccione > **Editar módulo**.

   En el cuadro de diálogo Configuración del módulo se muestra el módulo seleccionado, el servicio ESA Analytics y los orígenes de datos para el mapeo. Los orígenes de datos muestran las direcciones URL que se usan para comunicarse con ESA.



2. Revise la sección **Estado de preparación** para determinar el estado de preparación actual:
   - **La preparación se inició a las**: La hora en que el módulo ESA Analytics procesó el primer evento desde el origen de datos.
   - **Hora del primer evento**: La hora en que se produjo el primer evento. El tiempo de preparación se basa en esta hora.
   - **Hora del último evento**: La hora en que se produjo el último evento..
   - **Tiempo de preparación restante**: La cantidad de horas restantes en el período de preparación.
   - **¿Se completó?** : Indica si el período de preparación se completó. Si es verdadero, el período de preparación se completó. Si es falso, el módulo aún se está preparando y la cantidad de horas restantes se puede ver en el campo Tiempo de preparación restante.

3. En la sección **Configuración**, puede actualizar **Período de preparación (horas)**, en función de si se completó o no el período de preparación.
   - **Durante el período de preparación**: Puede agregar horas al período de preparación o restar cualquier tiempo de preparación restante.
   - **El período de preparación se completó**: Puede agregar horas al período de preparación mediante la suma de la diferencia entre la hora actual y la Hora del primer evento a las horas que desea agregar.
     Por ejemplo, un período de preparación de 10 horas se completó y en la opción Hora del primer evento se muestra 12:00:00. La hora actual son las 16:00:00 (4 horas después) y desea agregar 5 horas más al tiempo de preparación. Para hacerlo, debe agregar 9 horas (4+5=9) al período de preparación de 10 horas; por lo tanto, debe configurar el nuevo período de preparación en 19 horas.
     No puede disminuir el período de preparación si se completó, a menos que elimine el mapeo y cree uno nuevo.
4. Si es necesario, puede ajustar el **Tiempo de retardo (minutos)** para dar a los Concentrators en el mapeo el tiempo adicional para completar la agregación de todos los datos.
5. Haga clic en **Guardar**.
   Los cambios NO se aplican de inmediato. Para que la configuración tenga efecto, debe anular la implementación del mapeo y volverlo a implementar.
6. Para anular la implementación del mapeo, en el panel Mapeos de ESA Analytics, seleccione el mapeo cuya implementación desea anular y elija  **> Anular implementación**.
   La agregación de datos se detiene para el mapeo seleccionado.
7. Para volver a implementar el mapeo, seleccione el mapeo que desea implementar y elija  **> Implementar**.
   El mapeo seleccionado se implementa e inicia la agregación de datos como está configurado en el mapeo.

Procedimientos adicionales de reglas de correlación de ESA

Este tema es un conjunto de procedimientos individuales que un administrador puede ejecutar en cualquier momento, los cuales no son necesarios para llevar a cabo la configuración inicial de las reglas de correlación de ESA.

Use esta sección cuando busque instrucciones para ejecutar una tarea específica después de la configuración inicial de ESA.

- Cambiar el umbral de la memoria para las reglas de prueba
- Configurar ESA para que use un pool de memoria
- Configurar ESA para que use el orden por hora de captura
- Iniciar, detener o reiniciar el servicio ESA
- Registros de auditoría y verificar las versiones y el estado de los componentes de ESA

Cambiar el umbral de la memoria para las reglas de prueba

Este procedimiento es opcional y solo se aplica a las reglas de correlación de ESA.

Los administradores pueden aumentar o disminuir el umbral de la memoria para las reglas de prueba. El umbral se refiere al uso de la memoria de ESA, lo cual incluye la memoria base de ESA, las reglas de prueba y las reglas que no son de prueba. Cuando se supera el umbral, todas las reglas de prueba implementadas en un servicio ESA se deshabilitan.

Las reglas de prueba se usan para ver si una regla se ejecuta de manera eficiente y no consume un exceso de memoria, lo cual puede afectar el rendimiento o forzar el apagado del servicio.

De manera predeterminada, el umbral de la memoria es 85, lo cual equivale al porcentaje de la memoria virtual de Java (JVM).

- El umbral de la memoria se establece por ESA, no por regla.
- Cuando se supera, todas las reglas de prueba que se ejecutan en ESA se inhabilitan automáticamente.
- La configuración de ESA tiene dos parámetros para las reglas de prueba:
  - MemoryThresholdforTrialRules
  - MemoryCheckPeriod, que tiene un valor predeterminado de 300 segundos

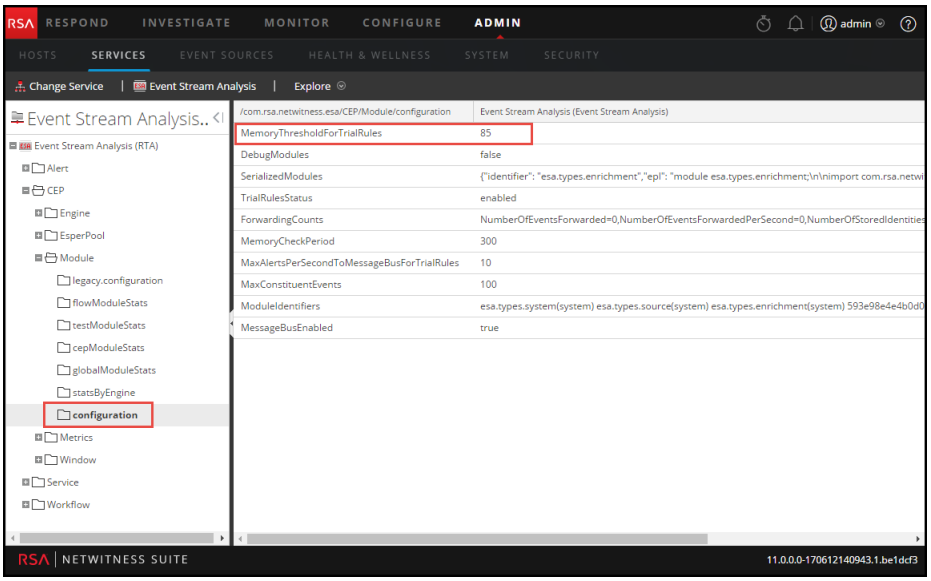
Para obtener más información, consulte “Trabajo con reglas de prueba” en la “Guía de alertas mediante ESA”.

Requisitos previos

Se le debe asignar una función con privilegios administrativos.

Procedimiento

1. Inicie sesión en NetWitness Suite como administrador.
2. Vaya a **ADMIN** > **Servicios**.
3. Seleccione un servicio ESA y seleccione  > **Ver** > **Explorar**.
4. En el lado izquierdo, seleccione **CEP > Módulo** > **configuración**.



5. En el panel de la derecha, en **MemoryThresholdForTrialRules**, escriba un porcentaje de JVM que no pueden superar las reglas de prueba en ESA.
   El nuevo umbral de la memoria se aplica de inmediato.

Configurar ESA para que use un pool de memoria

Este procedimiento solo se aplica a las reglas de correlación de ESA.

Los administradores pueden configurar ESA para que use un pool de memoria. Un pool de memoria es una implementación personalizada de memoria virtual para eventos que mantienen las reglas en ESA. Esto ayuda a escalar la funcionalidad de las reglas en un orden de magnitud. Cuando desee crear reglas que abarquen un amplio intervalo de tiempo o que sean muy complejas, se recomienda usar un pool de memoria para manejar la memoria de manera más eficiente. Cuando utiliza un pool de memoria, en lugar de que todos los eventos estén en la memoria, se pueden escribir en el disco. Esto resulta útil porque cuando existe una regla que es compleja o que abarca un intervalo de tiempo prolongado, se debe mantener una gran cantidad de eventos en la memoria.

Puede configurar el pool de memoria para que se ejecute en un modo por lotes o no por lotes:

- **Modo no por lotes**. En el modo no por lotes, los eventos se escriben en disco a medida que ingresan al pool de memoria. Para configurar el modo no por lotes, establezca el atributo **MapPoolBatchWriteSize** en 1. El modo no por lotes ofrece una solución más estable debido a que cada evento se descarga y se recupera por separado sin crear incrementos repentinos de memoria.

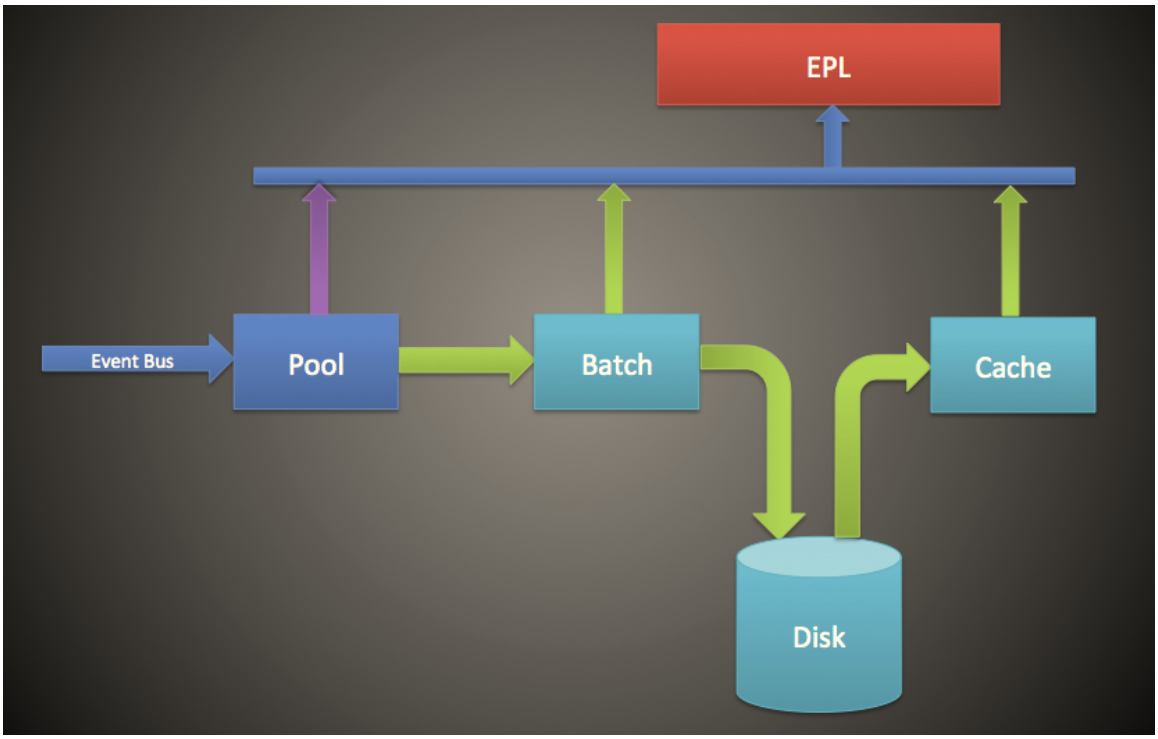
- **Modo por lotes**. En el modo por lotes, los eventos se agrupan en lotes y, a continuación, se escriben en el disco. Para configurar el modo por lotes, establezca el atributo de tamaño de lote **MapPoolBatchWriteSize** en un valor mayor que 1. El modo por lotes ofrece un mejor rendimiento, ya que se optimiza la actividad del disco para descargar eventos en él.

Nota: Todos los cambios en estos ajustes requerirán el reinicio de ESA. Tras el reinicio de ESA, si el pool de memoria está manteniendo eventos, estos se descartarán.

Precaución: Si bien esta función puede ser muy útil en la administración de la memoria, puede afectar la velocidad de procesamiento de eventos de ESA. Puede haber un impacto en el rendimiento de entre el 10 y el 30 % según las reglas y los ajustes de configuración.

Flujo de trabajo

En el siguiente diagrama se muestra el flujo de datos que usa el pool de memoria para el modo por lotes.



1. Los eventos se agregan en el pool de memoria, donde también se almacenan las referencias a los eventos.
2. A continuación, los eventos se agrupan en lotes para su envío al disco (en el modo no por lotes, este paso se omite).
3. Una vez que el lote alcanza el umbral, los eventos se escriben en el disco (en el modo no por lotes, no se requiere ningún umbral).
4. Cuando el EPL requiere un evento que se escribió en el disco, este se envía a la caché y se usa en la regla de EPL.

Procedimiento

Realice los siguientes pasos para configurar un pool de memoria de ESA.

1. Vaya a **ADMIN** > **Servicios**, seleccione el servicio ESA y elija > **Ver** > **Explorar**.
2. Seleccione **CEP** > **EsperPool** > **Configuración**.
3. Ingrese valores en los siguientes campos:

Atributo	Descripción	Configuración

MapPoolPersistenceURI	Ubicación para almacenar el archivo de pool de memoria.	El valor predeterminado es **/opt/rsa/esa/pool/esperPool**. RSA recomienda no modificar el valor predeterminado. Si modifica esta configuración para utilizar una partición diferente, asegúrese de que la partición tenga al menos 10 veces más espacio que la memoria asignada para ESA. **Precaución:** Si el pool de memoria está en uso mientras se cambia esta ruta, se requiere un reinicio de ESA. Cuando esto ocurre, ESA no descarta los eventos almacenados y usted debe depurarlos manualmente.
MapPoolEnable	Habilite o deshabilite el pool de memoria.	El valor predeterminado es **false**. Establezca el valor en **true** para habilitar el pool de memoria. Cuando habilita o deshabilita el pool de memoria, se requiere un reinicio.
MapPoolFlushIntervalSecs	Intervalo de tiempo para vaciar los eventos en el disco. Por ejemplo, cualquier evento que se mantiene en Esper durante más de 15 minutos se vacía al disco.	El valor predeterminado es **15 minutos**. Un valor inferior garantiza la estabilidad de ESA cuando hay EPL que mantienen una gran cantidad de eventos en la memoria. Un valor mayor (superior a 30 minutos) garantiza que solo los eventos pertinentes que se requieren durante un período más prolongado se vacían en el disco. **Nota:** Debido al diseño de la administración de memoria de Java, en ocasiones, eventos que EPL no mantiene se pueden enviar al disco. Para impedir que esto ocurra, es posible establecer un valor mayor para MapPoolFlushIntervalSecs.

MapPoolBatchWriteSize	Especifique el tamaño de lote (y si se desea usar el modo por lotes). Los eventos se agrupan en lotes y se vacían en el disco. Para usar el modo no por lotes, configure este valor en 1. Para usar el modo por lotes, configure un valor mayor que 1.	El tamaño del lote predeterminado es **100,000** eventos. Al final del intervalo de vaciado, si no se alcanza la capacidad del lote, el lote vence en 30 segundos y todo su contenido se escribe en el disco como archivos del pool de memoria. Un valor menor para el tamaño del lote (por ejemplo, 10,000 eventos) garantiza que, cuando se obtienen eventos desde el disco, no se genera un riesgo de crecimiento excesivo de la memoria, lo cual crea mayor estabilidad. Sin embargo, con un tamaño mayor del lote (100,000 eventos), se minimiza la actividad de entrada/salida cuando se escriben eventos en el disco, lo cual puede crear un mejor rendimiento.
MapPoolMinSize	Tamaño mínimo del pool de memoria. Este valor se utiliza para la inicialización y generalmente no requiere edición.	El valor predeterminado es **10,000** eventos. Un valor mayor puede aumentar el rendimiento. Un valor menor garantiza la estabilidad del sistema.
MapPoolPersistType	Este es un parámetro de solo vista que muestra el tipo de optimización utilizado.	El valor predeterminado es **RMSerialize**.

Nota: La eficacia de esta característica depende de su ambiente. Si escribe reglas que requieren acceso frecuente de eventos durante un período, esta característica puede degradar el rendimiento con una mejora nula o mínima de la escalabilidad.

Los archivos del pool de memoria se eliminan cuando un EPL deja de hacer referencia a todos los eventos que se mantienen en el archivo del pool.

Resultado

Para una regla de EPL simple, ESA suele optimizar la memoria aproximadamente entre ocho y nueve veces.

Configurar ESA para que use el orden por hora de captura

Este procedimiento solo se aplica a las reglas de correlación de ESA.

Los administradores cómo configurar ESA para que use el orden por hora de captura cuando se utilizan dos o más Concentrators como origen.

De forma predeterminada, ESA utiliza la hora de registro de ESA (la hora en la cual ESA recibe los eventos) para correlacionar los eventos. Sin embargo, ESA también es compatible con el orden de las sesiones en función de la hora de captura (la hora a la cual el evento de registro o el paquete llegaron a los Decoders). Esta característica es útil si está correlacionando eventos desde dos o más Concentrators. Cuando tiene dos o más Concentrators como orígenes, el orden por hora garantiza que sus sesiones se correlacionen según la hora de captura. Esto asegura la correlación de las sesiones capturadas a la misma hora y garantiza que las alertas sean coherentes con las expectativas del usuario, incluso cuando se producen demoras en la transmisión. Si cualquiera de los orígenes queda offline o tarda en enviar las sesiones, ESA hace una pausa para asegurarse de que las sesiones con la misma hora de registro de captura se correlacionen.

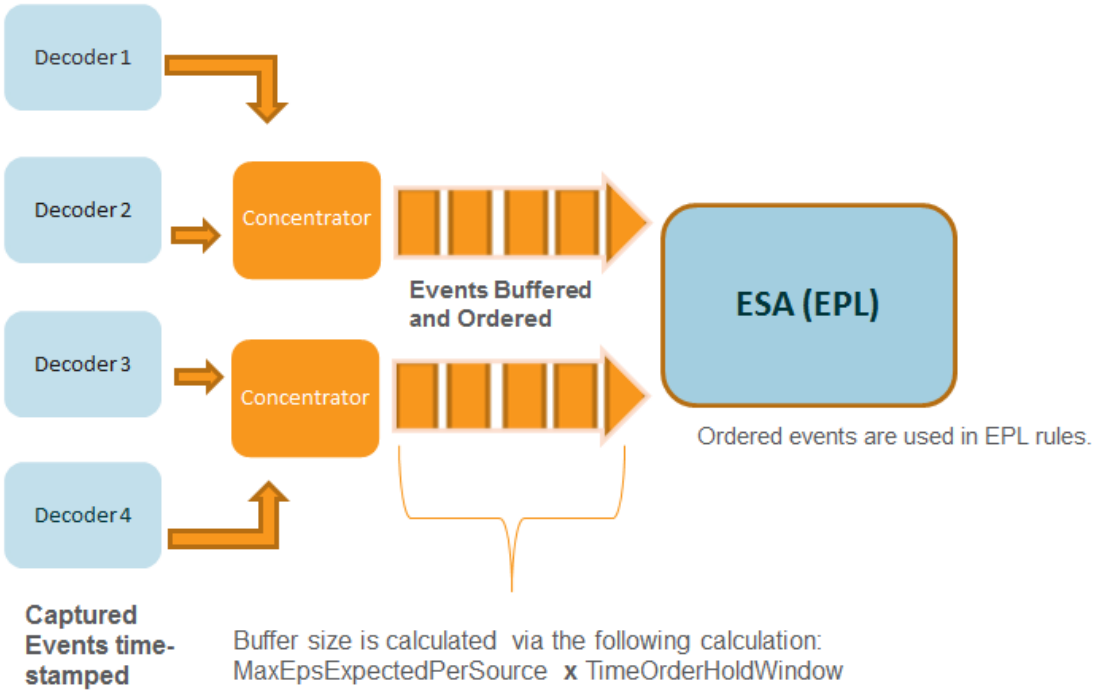
Por ejemplo, tiene dos orígenes con eventos que ocurren a las 10:00 h. Si se usa el orden por hora de captura, estos eventos se mantienen en el búfer hasta que ESA detecta la adición en el búfer de todos los eventos que ocurren a las 10:00 h. Una vez que llegan todos los eventos, estos se procesan mediante reglas de EPL. Esto garantiza que en una regla estén todos los eventos de diferentes orígenes con la misma hora de registro, con lo cual se obtienen resultados correctos. Si, por ejemplo, un Concentrator queda atrás respecto de otro, ESA hace una pausa antes de aplicar a los eventos las reglas de EPL hasta que recibe todos los eventos con la hora de registro 10:00 h de ambos orígenes.

Precaución: Aunque aumenta la precisión, esta función afecta el rendimiento. La configuración predeterminada de ESA garantiza la transmisión constante de los datos, pero debido a que el orden por hora de captura utiliza un búfer, el procesamiento de eventos tarda más. Esto se cumple especialmente si ESA debe hacer una pausa durante el tiempo que sea para esperar que el búfer se llene. Puede configurar varios parámetros (consulte a continuación) para manejar esta situación; sin embargo, el rendimiento se puede ver afectado de todos modos.

De manera predeterminada, esta función está deshabilitada.

Flujo de trabajo del orden por hora de captura

En el siguiente diagrama se muestra el flujo de trabajo del orden por hora de captura cuando está habilitado.



1. Los eventos se marcan con la hora de registro a medida que el Decoder los captura.
2. Después del procesamiento de Concentrator, los eventos se colocan en el búfer y se ordenan. El tamaño del búfer se calcula mediante dos parámetros MaxEPSExpectedPerSource (el volumen máximo de tráfico (EPS) que se espera que reciba ESA **por origen**) por TimeOrderHoldWindow (la cantidad de tiempo que se permite la llegada de los eventos de todos los orígenes).
3. A continuación, los eventos ordenados se correlacionan correctamente en reglas de EPL.

Requisitos previos

Debe haber dos o más Concentrators configurados como un origen de datos en ESA.

Cuando el parámetro **StreamEnabled** se establece en true, es importante que todas las máquinas que ejecutan servicios Core estén sincronizadas con NTP.

Procedimientos

En los siguientes procedimientos se indica cómo habilitar y configurar el orden por hora de captura.

Habilitar la colocación en el búfer y el orden por hora de captura

Nota: Después de una actualización o en un ambiente con una gran cantidad de EPS, debe volver a agregar los orígenes de datos para comenzar a apreciar los beneficios. O bien, debe esperar hasta que las sesiones se pongan al día antes de habilitar el orden por hora de captura.

1. Vaya a **ADMIN** > **Servicios**, seleccione el servicio ESA y elija  > **Ver** > **Explorar**.
2. Vaya a **Flujo de trabajo** > **Origen** > **nextgenAggregationSource**.
3. Configure el atributo **StreamEnabled** en **true**. StreamEnabled permite que ESA coloque en el búfer los eventos que recibe desde los Concentrators.
4. Configure el atributo **TimeOrdered** en **true**. Esto permite que los eventos en el búfer ser ordenen según la hora de registro desde el Concentrator.

Configurar el orden por hora de captura

Cuando se trabaja con el orden por hora de captura, es necesario configurar varios otros parámetros para garantizar el rendimiento. En la siguiente tabla se enumeran los parámetros y su función. Para la configuración de estos parámetros se requiere conocimiento de la tasa y el volumen de tráfico.

Nota: Si no conoce el volumen de tráfico o la latencia, consulte al representante de servicios profesionales antes de configurar esta función.

MaxEPSExpectedPerSource	Especifique el volumen de tráfico máximo (EPS o eventos por segundo) que se espera que reciba el servicio ESA del origen más activo (por ejemplo, si un origen recibe 20,000 EPS y otro recibe 25,000 EPS, configure el valor en 25,000 EPS). El establecimiento de esta tasa en un valor demasiado bajo afecta el rendimiento a corto plazo. Sin embargo, ESA aumenta automáticamente el valor de `MaxEPSExpectedPerSource` según sea necesario para avanzar en el modo de orden por tiempo. El valor predeterminado es 20,000.
TimeOrderHoldWindow	Especifique en segundos (enteros) la cantidad de tiempo que se permite la llegada de los eventos de todos los orígenes. Configure este valor en función de la latencia entre los orígenes. El valor predeterminado es 2 segundos. La disminución de este valor puede aumentar la probabilidad de pérdida de eventos. El aumento de este valor puede disminuir el rendimiento debido a que se consume más memoria.
IdleSourceAdvanceAfterSeconds	Especifique el intervalo (en segundos) tras el cual ESA quita de la ecuación a un origen inactivo (no provienen eventos del origen, pero este no está offline) para permitir el avance de un flujo ordenado por hora de captura. El valor predeterminado es 0, lo cual significa que ESA espera indefinidamente la llegada de eventos.
OfflineSourceAdvanceAfterSeconds	Especifique el intervalo (en segundos) tras el cual ESA quita de la ecuación un origen offline para permitir el avance de un flujo ordenado por hora de captura. El valor predeterminado es 0, lo cual significa que ESA espera indefinidamente. Este parámetro no afecta los reintentos de reconexión; aquellos que se realizan en todos los casos.

Consejos para la solución de problemas

Cuando se usa esta función, es posible que se produzca una situación de acumulación de eventos. Para solucionar este problema, puede realizar una de las siguientes opciones.

Deshabilitar el orden por hora de captura

1. Vaya a **ADMIN** > **Servicios**, seleccione el servicio ESA y elija  **> Ver > Explorar**.
2. Vaya a **Flujo de trabajo** > **Origen** > **nextgenAggregationSource**.
3. Configure el atributo StreamEnabled en false.
4. Configure el atributo TimeOrdered en false.

Si deshabilita el orden por hora de captura, perderá los datos acumulados y los eventos dejarán de ordenarse por hora de captura.

Deshabilitar el rastreo de posición

El rastreo de posición permite que ESA rastree la posición en la cual dejó de procesar eventos en caso de que se detenga o se apague. El rastreo de posición está habilitado de forma predeterminada con el orden por hora de captura. Si lo deshabilita, ESA omite los eventos acumulados. Por ejemplo, si ESA queda inactivo a las 7:00 h y se reinicia a las 11:00 h con el rastreo de posición deshabilitado, ESA comienza a procesar eventos que ocurrieron a las 10:55 h. Con el rastreo de posición habilitado, ESA comenzará a procesar eventos en el punto en que se detuvo.

1. Vaya a **ADMIN** > **Servicios**, seleccione el servicio ESA y elija  > **Ver** > **Explorar**.
2. Vaya a **Flujo de trabajo** > **Origen** > **nextgenAggregationSource**.
3. Configure el atributo **PositionTrackingEnabled** en false.

Si deshabilita el rastreo de posición, perderá los datos acumulados, pero en adelante, los eventos se ordenarán por hora de captura.

Iniciar, detener o reiniciar el servicio ESA

En este tema se proporcionan instrucciones para iniciar, detener o reiniciar el servicio Event Stream Analysis. Este procedimiento se aplica a las reglas de correlación de ESA.

Iniciar el servicio ESA

Antes de comenzar:

- Asegúrese de que MongoDB esté en ejecución.
- Si el servicio MongoDB no está en ejecución, use el siguiente comando para iniciar el servicio MongoDB:
  ```
  systemctl start mongod
  ```

Para iniciar el servicio ESA:

1. Use el protocolo SSH para conectarse al servicio de ESA e iniciar sesión como el usuario raíz.
2. Escriba el siguiente comando y presione INTRO:
   ```
   systemctl start rsa-nw-esa-server
   ```

Detener el servicio ESA

Para detener el servicio ESA:

1. Use el protocolo SSH para conectarse al servicio de ESA e iniciar sesión como el usuario raíz.
2. Escriba el siguiente comando y presione INTRO:
   ```
   systemctl stop rsa-nw-esa-server
   ```

Reiniciar el servicio ESA

Para reiniciar el servicio ESA:

1. Use el protocolo SSH para conectarse al servicio de ESA e iniciar sesión como el usuario raíz.
2. Escriba el siguiente comando y presione INTRO:
   ```
   systemctl restart rsa-nw-esa-server
   ```

Registros de auditoría y verificar las versiones y el estado de los componentes de ESA

En este tema se proporcionan detalles sobre el registro de auditoría e instrucciones para verificar las versiones de los componentes de Event Stream Analysis instalados. Estos procedimientos se aplican a las reglas de correlación de ESA.

Reglas de registro de auditoría

El registro de auditoría permite ver los detalles acerca de las reglas que se crean y se editan en NetWitness Suite.

Para obtener detalles sobre cómo acceder a los registros de auditoría, consulte "Ubicaciones de los registros de auditoría locales" en la *Guía de configuración del sistema*.

El siguiente ejemplo muestra un registro de creación, actualización y eliminación para una regla determinada.

- **Ejemplo de registro de creación:** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: "CREATE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true, Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR"`
- **Ejemplo de registro de actualización:** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: "UPDATE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR`
- **Ejemplo de registro de eliminación:** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS"category: SYSTEM operation: "DELETE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR "`

Cada registro contiene los siguientes parámetros:

- Time stamp: La hora en que se modificó la regla. Ejemplo: 2016-03-10 14:19:37,951
- DeviceVersion: Versión del dispositivo ESA. Ejemplo: "10.6.1.0-SNAPSHOT"
- DeviceService: Ejemplo: EVENT_STREAM_ANALYSIS
- Category: Ejemplo: SYSTEM
- Operation: Ejemplo: DELETE/CREATE/UPDATE RULE
- Parámetros: Marcador de posición para las siguientes claves:
- Epl Module Identifier: Identificador único de la regla. Ejemplo: 56e1f2adbee8290008241296
- Esper Instance: Instancia de Esper en la cual se implementa la regla. Ejemplo: default
- Rule Enabled: Muestra si la regla está o no habilitada. Ejemplo: Rule Enabled: true
- Trial Rule: Muestra si la regla está o no configurada como una regla de prueba. Ejemplo: Trial Rule: false
- Epl Rule: Muestra la sintaxis de la regla. Ejemplo:

  ```
  @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_
  ESA_ADMINISTRATOR+ROLE_ESA_ADMINISTRATOR+ROLE_ESA_ADMIN"
  ```

- Identity: Ejemplo: “admin"
- userRole: Ejemplo: "ROLE_ESA_ADMINISTRATOR"

Nota: Cuando una regla está deshabilitada, se generan dos registros para la misma regla. Primero se crea un registro de auditoría “Delete Rule” [atributo Rule enabled = true] y después, un registro de auditoría “Create Rule” [atributo Rule enabled =false].

Verificar la versión del servidor de ESA

Para verificar la versión del servidor de ESA:

1. Use el protocolo SSH para conectarse al servicio de ESA e iniciar sesión como el usuario raíz.
2. Escriba el siguiente comando y presione INTRO:

   ```
   rpm -qa | grep rsa-nw-esa-server
   ```

   Se muestra la versión del servidor de ESA.

Verificar la versión de MongoDB

Para verificar la versión de MongoDB:

1. Use el protocolo SSH para conectarse al servicio de ESA e iniciar sesión como el usuario raíz.
2. Escriba el siguiente comando y presione INTRO:
   ```
   mongo --version
   ```
   Se muestra la versión de MongoDB.

Verificar el estado de MongoDB

Para verificar el estado de MongoDB:

1. Use el protocolo SSH para conectarse al servicio de ESA e iniciar sesión como el usuario raíz.
2. Escriba el siguiente comando y presione INTRO:
   ```
   systemctl status mongod
   ```
3. Ejecute el siguiente comando si MongoDB no se ejecuta.
   ```
   systemctl start mongod
   ```

Referencias

Esta sección es un conjunto de referencias que describen la interfaz del usuario para la configuración de ESA en NetWitness Suite.

Consulte los siguientes temas para obtener más información:

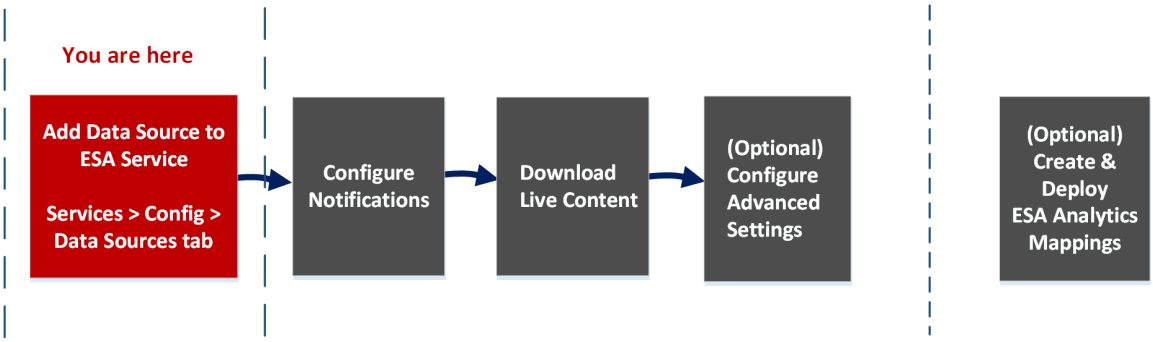
- Pestaña Opciones avanzadas de la vista Configuración de servicios
- Pestaña Orígenes de datos de la vista Configuración de servicios
- Mapeos de ESA Analytics
- Configuración del módulo
- Configuración del servicio de búsqueda de Whois

Pestaña Orígenes de datos de la vista Configuración de servicios

La **vista Configuración de servicios > pestaña Orígenes de datos** de un servicio de ESA permite configurar los orígenes que utiliza ESA para analizar los datos. Un servicio de ESA recopila datos de Concentrators para detectar incidentes y alertar a los analistas sobre posibles amenazas.

Flujo de trabajo

En este flujo de trabajo se muestra el proceso general de configuración de ESA. También se muestra dónde se encuentra la configuración de orígenes de datos en el proceso.



ESA tiene dos servicios, el servicio Event Stream Analysis (ESA Correlation Rules) y el servicio Event Stream Analytics Server (ESA Analytics). Los primeros cuatro procedimientos que se muestran corresponden a la configuración del servicio Event Stream Analysis:

- Agregar un origen de datos a un servicio de ESA
- Configurar notificaciones
- Descargar Live Content
- (Opcional) Configurar ajustes avanzados

El último procedimiento es independiente del resto y corresponde a la creación de mapeos para los servicios de ESA Analytics de modo que comiencen automáticamente a detectar amenazas avanzadas:

- (Opcional) Crear e implementar mapeos de ESA Analytics

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Agregar un Concentrator como un origen de datos al servicio Event Stream Analysis*	Consulte Configurar reglas de correlación de ESA y Paso 1. Agregar un origen de datos a un servicio de ESA
Administrador	Configurar notificaciones	Consulte "Métodos de notificación" en la *Guía de alertas mediante ESA*.
Administrador	Descargar Live Content	Consulte "Vista Buscar en Live" en la *Guía de administración de recursos de Live*.
Administrador	Configurar ajustes avanzados	Paso 2. Configurar ajustes avanzados para un servicio de ESA

*Puede realizar estas tareas aquí (es decir, en la pestaña Orígenes de datos de la vista Configuración de servicios).

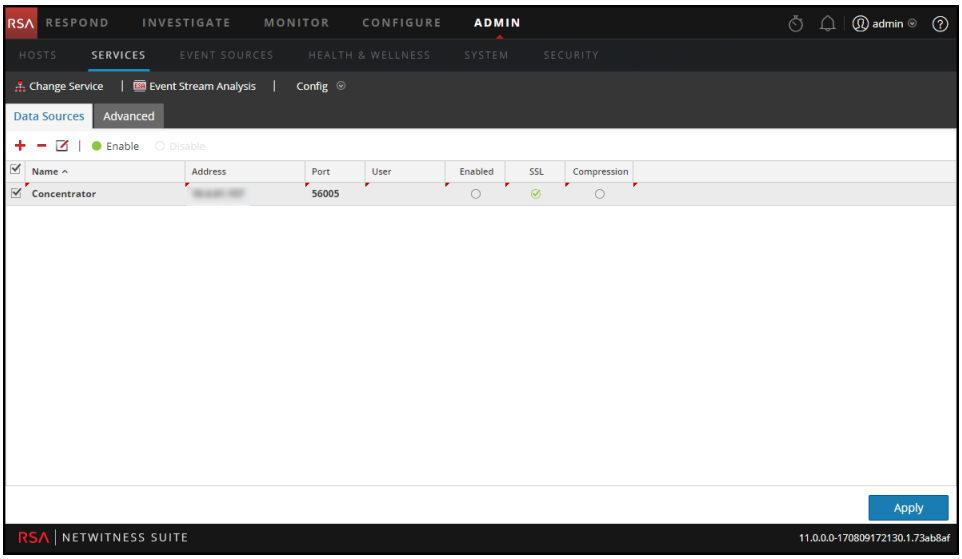
Temas relacionados

- Consulte "Agregar o actualizar un host" en la *Guía de introducción de hosts y servicios*.

Vista rápida

Para acceder a la pestaña Orígenes de datos, vaya a **ADMIN > Servicios >** (seleccione un servicio de ESA) >  **> Ver > Configuración**.

En la siguiente figura se muestra la pestaña Orígenes de datos de la vista Configuración de servicios correspondiente a un servicio de ESA.



Barra de herramientas

En la siguiente tabla se describen las opciones de la barra de herramientas.

Opción	Descripción
+	Agrega un origen de datos nuevo al servicio de ESA.
−	Elimina un origen de datos del servicio de ESA.
✎	Edita un origen de datos. Si desea hacer cambios, debe disponer de credenciales de nombre de usuario y contraseña para el servicio.
Enable	Habilita el origen de datos seleccionado.
Disable	Inhabilita el origen de datos seleccionado.

Orígenes de datos

La lista Orígenes de datos muestra todos los orígenes de datos agregados al servicio de ESA. En la siguiente tabla se describen las columnas de la lista Orígenes de datos.

Columna	Descripción
Nombre	El nombre del servicio del origen de datos.

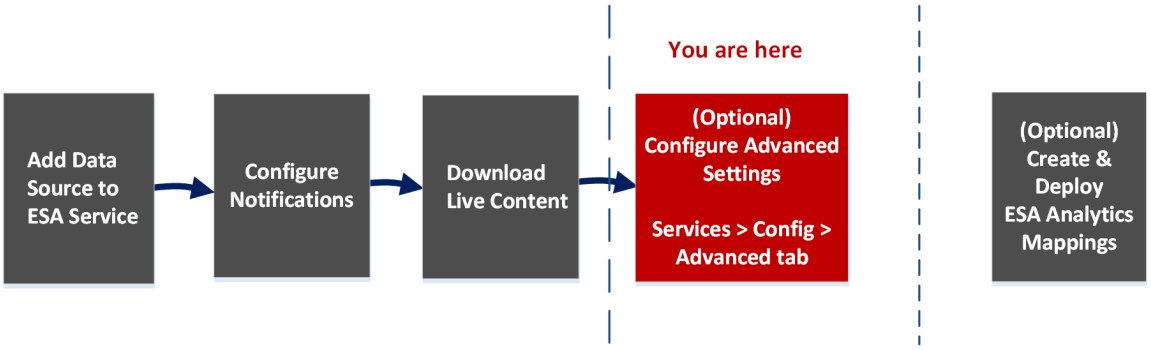
Columna	Descripción
Dirección	La dirección del servicio del origen de datos.
Puerto	El puerto que usa el origen de datos.
Usuario	El usuario conectado con el origen de datos.
Habilitado	Indica si el origen de datos está habilitado.
SSL	Indica si la comunicación SSL está habilitada.
Compresión	Indica si la compresión está habilitada.

Pestaña Opciones avanzadas de la vista Configuración de servicios

La **vista Configuración de servicios > pestaña Opciones avanzadas** de un servicio de ESA permite configurar ajustes avanzados. En la vista Opciones avanzadas, puede configurar ajustes avanzados para mejorar el rendimiento, preservar eventos para reglas con múltiples eventos, colocar en el búfer eventos en la memoria y establecer la cantidad de eventos que se almacenarán en ESA.

Flujo de trabajo

En este flujo de trabajo se muestra el proceso general de configuración de ESA. También se muestra dónde se encuentra la configuración de ajustes avanzados en el proceso.



ESA tiene dos servicios, el servicio Event Stream Analysis (ESA Correlation Rules) y el servicio Event Stream Analytics Server (ESA Analytics). Los primeros cuatro procedimientos que se muestran corresponden a la configuración del servicio Event Stream Analysis:

- Agregar un origen de datos a un servicio de ESA
- Configurar notificaciones
- Descargar Live Content
- (Opcional) Configurar ajustes avanzados

El último procedimiento es independiente del resto y corresponde a la creación de mapeos para los servicios de ESA Analytics de modo que comiencen automáticamente a detectar amenazas avanzadas:

- (Opcional) Crear e implementar mapeos de ESA Analytics

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Agregar un Concentrator como un origen de datos al servicio Event Stream Analysis	Consulte Configurar reglas de correlación de ESA y Paso 1. Agregar un origen de datos a un servicio de ESA
Administrador	Configurar notificaciones	Consulte "Métodos de notificación" en la *Guía de alertas mediante ESA*.
Administrador	Descargar Live Content	Consulte "Vista Buscar en Live" en la *Guía de administración de recursos de Live*.
Administrador	Configurar ajustes avanzados*	Paso 2. Configurar ajustes avanzados para un servicio de ESA

*Puede realizar estas tareas aquí (es decir, en la pestaña Opciones avanzadas de la vista Configuración de servicios).

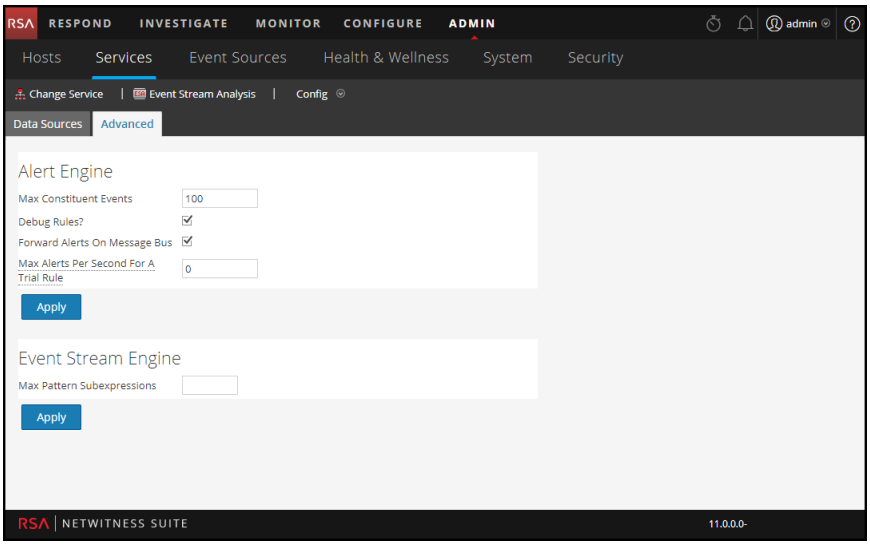
Temas relacionados

- Consulte "Agregar o actualizar un host" en la *Guía de introducción de hosts y servicios*.

Vista rápida

Para acceder a la pestaña Opciones avanzadas, vaya a **ADMIN > Servicios >** (seleccione un servicio de ESA) >  **> Ver > Configuración**.

En la siguiente figura se muestra la pestaña Opciones avanzadas de la vista Configuración de servicios correspondiente a un servicio de ESA.



Configuración del motor de alertas

La sección Motor de alertas permite especificar valores para conservar eventos para reglas que eligen varios eventos. La figura siguiente muestra la sección Motor de alertas.

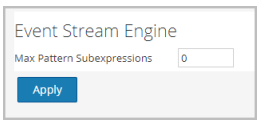
En la siguiente tabla se indican los parámetros de la sección Motor de alertas y sus descripciones.

Parámetro	Descripción
Máx. de eventos constitutivos	Para reglas que escogen múltiples eventos, este valor de configuración decide cuántos eventos asociados se preservan. Por ejemplo, si una regla activa una alerta con 200 eventos asociados y este parámetro está configurado en 100, ESA solo conserva los primeros 100 y el resto se descarta. El valor predeterminado es **100**.
¿Depurar reglas?	La selección habilita la depuración de reglas.
Reenviar alertas en bus de mensajes	Para reenviar alertas de ESA a NetWitness Respond, debe seleccionar esta opción. Las alertas de ESA generadas se enviarán al bus de mensajes y, posteriormente, a Respond. Esta es la opción predeterminada. Es posible que desee asegurarse de que el servicio Servidor de Respond esté en ejecución.

Parámetro	Descripción
Cantidad máxima de alertas por segundo para una regla de prueba	Puede especificar la cantidad máxima de alertas que se reenvían al bus de mensajes para la regla de prueba. Por ejemplo, si el valor está configurado en **50**, solo se reenviarán 50 alertas al bus de mensajes para la regla de prueba. Si el valor se configura en **0**, las alertas que genera la regla de prueba no se reenvían al bus de mensajes. El valor predeterminado es **10**.

Configuración del motor de flujo de eventos

La sección Motor de flujo de eventos permite especificar detalles para mejorar el rendimiento. En la siguiente figura se muestra la sección Motor de flujo de eventos.



En la siguiente tabla se indica el parámetro de la sección Motor de flujo de eventos y su descripción.

Parámetro	Descripción
Máx. de subexpresiones de patrón	Ciertas reglas requieren que ESPER mantenga las subexpresiones en la memoria antes de decidir activarlas o no. Estas subexpresiones consumen memoria y si se dejan deseleccionadas podrían hacer que el servicio se interrumpo por agotamiento de la memoria. Este parámetro es una medida de seguridad que mantiene dichas reglas de monopolización de la memoria en supervisión. Si una regla excede la cantidad específica de subexpresiones, se retrasa su procesamiento. El valor predeterminado es **0**, lo cual significa que esta configuración está inhabilitada. Debe configurar un valor si el servicio presenta problemas de estabilidad.

Configuración del servicio de búsqueda de Whois

El panel Configuración de Búsqueda de Whois (ADMIN > Sistema > Whois) permite configurar una conexión al servicio Búsqueda de Whois para los módulos ESA Analytics preconfigurados que se usan en Detección de amenazas automatizadas de RSA. 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.

Debe tener una cuenta de RSA Live para usar este servicio.

Si configuró una cuenta de Live en el panel Servicios de Live (ADMIN > Sistemas > Servicios de Live), el servicio Búsqueda de Whois se configura automáticamente. Solo debe comprobar la conexión del servicio Búsqueda de Whois.

Nota: Si no tiene una cuenta de RSA Live, puede crear una en el Portal de registro de RSA Live:
https://cms.netwitness.com/registration/
En la *Guía de administración de servicios de Live* se proporciona información adicional.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar el servicio de búsqueda de Whois.	Configurar el servicio Búsqueda de Whois
Administrador	Comprobar la conexión del servicio Búsqueda de Whois.	Configurar el servicio Búsqueda de Whois

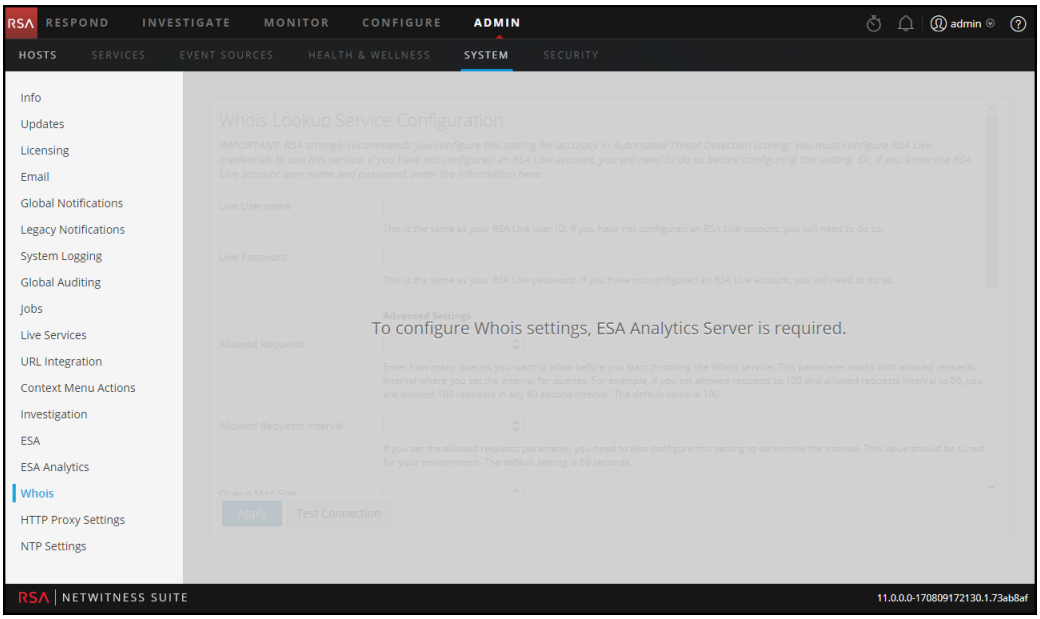
Temas relacionados

- Mapeos de ESA Analytics

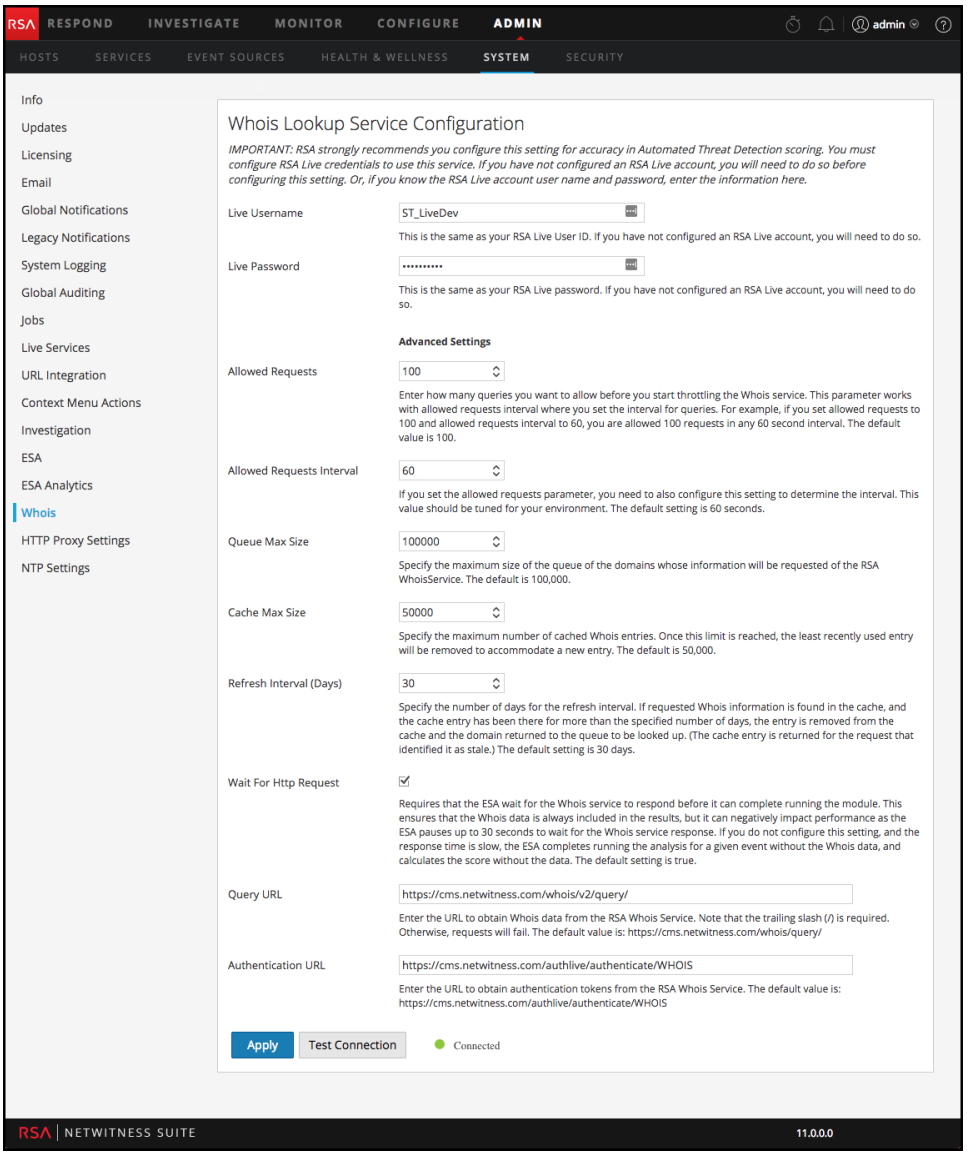
Configuración del servicio de búsqueda de Whois

Para acceder a la Configuración del servicio de búsqueda de Whois, vaya a ADMIN > Sistema y, en el panel de opciones, seleccione Whois.

El servicio Servidor de ESA Analytics debe estar disponible (se muestra un círculo verde) en ADMIN > vista Servicios. Si no está disponible un servicio Servidor de ESA Analytics, verá el panel siguiente.



Si está disponible un servicio Servidor de ESA Analytics, verá el panel siguiente.



En la siguiente tabla se describen los ajustes de configuración del servicio de búsqueda de Whois.

Parámetro	Descripción
Nombre de usuario de Live	**Solo se requiere si aún no configura el servicio de búsqueda de Whois.** 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”.

Parámetro	Descripción
Contraseña de Live	**Solo se requiere si ya configuró el servicio de búsqueda de Whois.** 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.
Solicitudes permitidas	(Opcional) Especifique cuántas consultas desea permitir antes de comenzar a regular el servicio Whois. Este parámetro funciona con **Intervalo de solicitudes permitidas** (en segundos), donde se define el intervalo de consultas. Por ejemplo, si configura **Solicitudes permitidas** en 100 e **Intervalo de solicitudes permitidas** en 60, se permiten 100 solicitudes en un intervalo de 60 segundos. El valor predeterminado es 100.
Intervalo de solicitudes permitidas	(Opcional) Si configura el parámetro **Solicitudes permitidas**, también debe configurar este ajuste para determinar el intervalo. Este valor debe ajustarse para su ambiente. La configuración predeterminada es 60 segundos.
Tamaño máximo de la línea de espera	(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.
Tamaño máximo de la caché	(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.
Intervalo de actualización (días)	(Opcional) Especifique la cantidad de días 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 días 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 30 días.

Parámetro	Descripción
Esperar solicitud HTTP	(Opcional) Requiere que ESA espere hasta que el servicio Whois responda antes de que pueda completar la ejecución del módulo. 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**.
URL de consulta	(Opcional) Ingrese la URL para obtener datos de Whois desde el servicio Whois de RSA. La barra diagonal final (“/”) es obligatoria. De lo contrario, se producirá un error en las solicitudes. El valor predeterminado es: **https://cms.netwitness.com/whois/v2/query/**
URL de autenticación	(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**

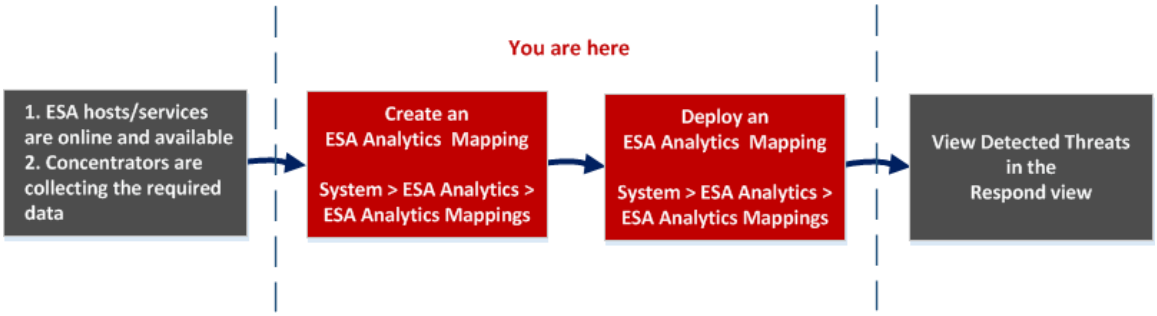
Mapeos de ESA Analytics

El panel Mapeos de ESA Analytics (ADMIN > Sistema > ESA Analytics) permite definir la manera en que la funcionalidad Detección de amenazas automatizadas de RSA debe detectar automáticamente las amenazas avanzadas. Puede analizar los datos que residen en uno o más Concentrators mediante la selección de un módulo ESA Analytics preconfigurado.

Para usar mejor sus recursos de red y reducir el flujo de datos innecesario, puede mapear múltiples orígenes de datos, como Concentrators, a servicios ESA Analytics disponibles con el fin de procesar los datos de manera más eficiente y aprovechar la capacidad adicional.

Flujo de trabajo

En este flujo de trabajo se muestra el proceso de creación y habilitación de un mapeo de ESA Analytics de modo que comience a detectar automáticamente las amenazas avanzadas.



Antes de crear un mapeo de ESA Analytics, asegúrese de que los hosts y los servicios de ESA que desea usar para los mapeos estén en línea y disponibles. Todos los servicios deben estar sincronizados con un origen de tiempo coherente. Asegúrese también de que los Concentrators estén recopilando los datos requeridos. Cuando crea un mapeo de ESA Analytics, usted selecciona un módulo ESA Analytics para realizar el mapeo, como Suspicious Domains. A continuación, selecciona los orígenes de datos, como Concentrators, que se usarán para ese módulo junto con un servicio de ESA Analytics para procesar los datos. Cuando está listo para comenzar a agregar los datos, usted implementa el mapeo. Los analistas pueden ver las amenazas detectadas para ese módulo en la vista Respond.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Verificar que los hosts y los servicios de ESA estén en línea y disponibles.	ADMIN > HOSTS y ADMIN > SERVICIOS Consulte *Guía de introducción de hosts y servicios*.
Administrador	Asegurarse de que los Concentrators estén recopilando los datos requeridos.	Consulte *Guía de configuración de Broker y Concentrator*.
Administrador	Crear mapeos de ESA Analytics*	Mapeo de orígenes de datos de ESA a módulos Analytics
Administrador	Implementar mapeos de ESA Analytics*	Mapeo de orígenes de datos de ESA a módulos Analytics
Administrador, analista	Ver las amenazas detectadas	Consulte la *Guía del usuario de NetWitness Respond*.

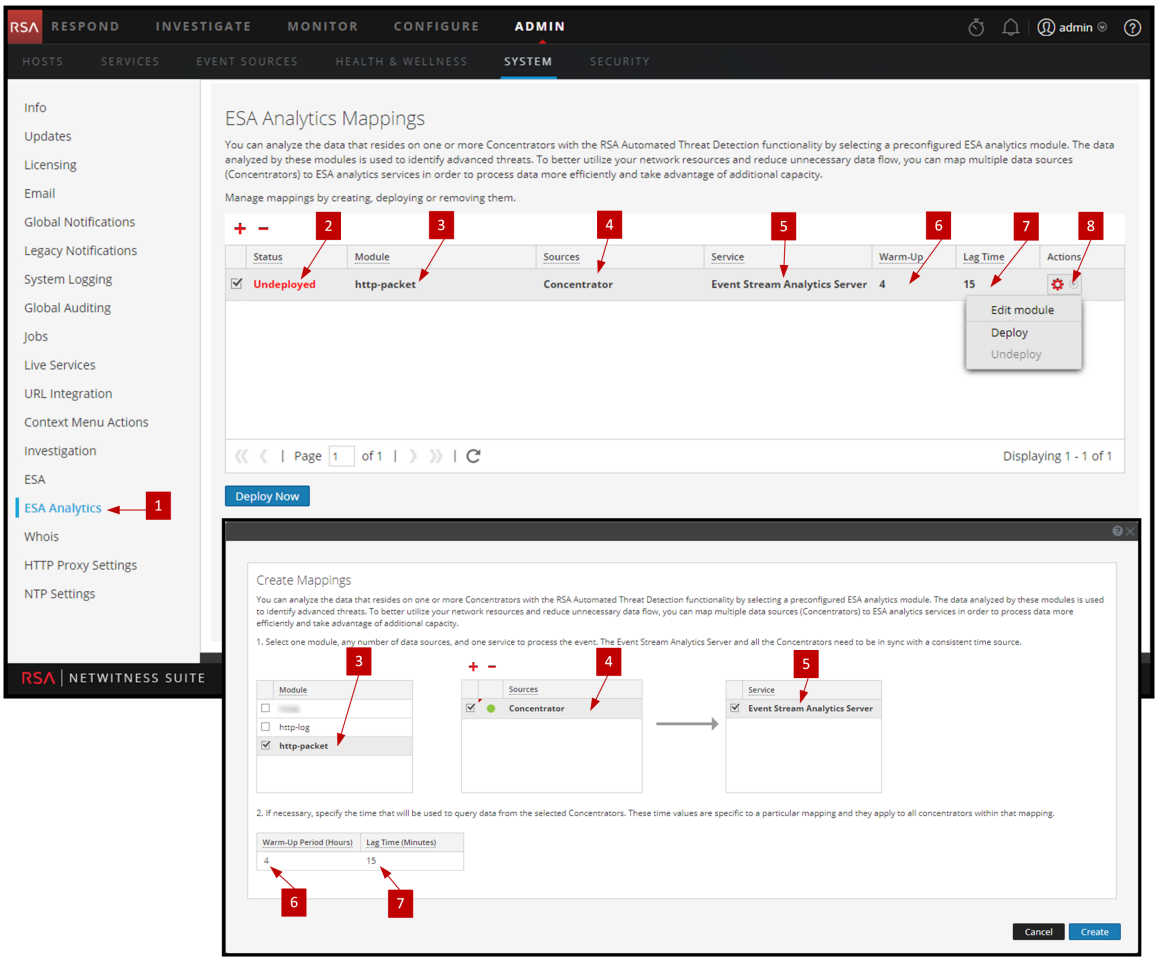
*Puede realizar estas tareas aquí (es decir, en el panel Mapeos de ESA Analytics).

Temas relacionados

- Configurar ESA Analytics
- Actualizar un mapeo
- Anular la implementación de un mapeo
- Eliminar un mapeo
- Cambiar el período de preparación y el tiempo de retardo
- Configuración del módulo

Vista rápida

En el siguiente ejemplo se ilustra un mapeo de ESA Analytics. La configuración define los orígenes de datos para el módulo seleccionado y el servicio ESA Analytics que procesará los eventos de esos orígenes de datos.



1	Muestra el panel Mapeos de ESA Analytics.
2	Muestra el estado del mapeo de ESA Analytics.
3	El nombre del módulo que se mapea.
4	Orígenes de datos, como Concentrators, asignados al mapeo.
5	El servicio ESA Analytics que procesa los datos del mapeo.
6	Configuración del período de preparación (en horas) en los orígenes de datos para el mapeo.
7	El intervalo de retardo (en minutos) en los orígenes de datos del mapeo.
8	Acciones para cambiar la configuración del módulo, implementar mapeos del módulo y anular la implementación de mapeos del módulo.

Barra de herramientas

En la siguiente tabla se describen las acciones de la barra de herramientas.

Icono/botón	Descripción
	Abre el cuadro de diálogo Crear mapeos, el cual permite crear un mapeo de ESA Analytics. Cree un mapeo por separado para cada módulo. Implemente los mapeos después de crearlos y revisarlos.
	Elimina un mapeo de ESA Analytics. • Puede eliminar un mapeo con un estado de Implementación anulada en cualquier momento. Puesto que un mapeo en el estado Implementación anulada no está implementado y no se está ejecutando, no afecta la agregación de datos. • La eliminación de un mapeo implementado borra la configuración en el servidor de ESA, revierte la implementación para ese mapeo y detiene la extracción de datos del origen de datos para ese módulo. Debe anular la implementación de un mapeo con un estado de Implementado antes de eliminarlo.
Implementar ahora	Después de crear los mapeos, debe implementarlos para iniciar la agregación de datos para los módulos. Puede seleccionar uno o más mapeos con un estado de Implementación anulada para implementarlos.

Nota: Si desea realizar cambios en un mapeo implementado, como agregar o quitar Concentrators o cambiar el servicio, debe anular la implementación y eliminar el mapeo existente y, a continuación, crear e implementar un nuevo mapeo para ese módulo.

Mapeos de ESA Analytics

En la siguiente tabla se describen los mapeos de ESA Analytics enumerados.

Título	Descripción
	Para seleccionar un mapeo individual, seleccione la casilla de verificación junto al mapeo.

Título	Descripción
Estado	Muestra el estado del mapeo. Hay dos estados: **No implementado**: Un mapeo no implementado mapea un módulo ESA Analytics a orígenes y a un servicio ESA Analytics. No inicia la agregación de datos para el módulo hasta que el mapeo se implementa. **Implementado**: Un mapeo implementado está implementado y en ejecución. En un mapeo implementado, el servicio ESA Analytics seleccionado usa agregación basada en consultas para recopilar los eventos filtrados adecuados para el módulo seleccionado desde los Concentrators.
Módulo	Indica el módulo ESA Analytics seleccionado. Un módulo ESA Analytics es una canalización que consta de objetos de actividad que enriquecen un evento con información adicional a través de cálculos matemáticos. El módulo reside dentro del servicio ESA Analytics.
Orígenes	Los orígenes son los orígenes de datos, como Concentrators, desde los cuales ESA agregará los datos del módulo especificado.
Servicio	Indica el servicio ESA Analytics que procesará los datos del módulo especificado. El servicio seleccionado debe estar sincronizado con un origen de tiempo coherente.
Período de preparación (horas)	Especifica una duración de preparación (en horas). Se requiere un período de preparación para permitir que Detección de amenazas automatizadas “conozca” su tráfico. El período de preparación se debe ejecutar cuando se esté ejecutando el tráfico típico. Durante este tiempo, se suprimen las alertas para el mapeo de módulo. El período de preparación prepara el módulo con datos históricos y garantiza que se complete la cantidad especificada de horas de recopilación de datos antes de que se envíen alertas. RSA proporciona módulos ESA Analytics preconfigurados. Cada tipo de módulo tiene un período de preparación predeterminado, que puede ajustar a su ambiente, si es necesario. Después de este período de preparación, se pueden ver las alertas. Para obtener más información sobre el período de preparación y el tiempo de retardo, consulte Configuración del módulo.

Título	Descripción
Tiempo de retardo (minutos)	Especifica el retraso de tiempo constante en minutos, el cual se suma para evitar la pérdida de eventos que los orígenes de datos procesan durante períodos de gran actividad. Por ejemplo, el rendimiento del Concentrator varía en función de factores como carga entrante, consultas continuas e indexación. Debido a estos factores, es posible que un Concentrator no pueda agregar eventos en tiempo real, lo que genera el retraso. El parámetro Retardo da al Concentrator la oportunidad de terminar de agregar todos los datos. Después de que finaliza el período de preparación, la agregación de datos continúa en **Hora (del sistema) actual - Tiempo de retardo**. Esto es útil cuando la agregación de datos en un Concentrator se realiza con lentitud. El tiempo de retardo garantiza que el módulo no procese los datos que llegan al Concentrator dentro de la ventana de tiempo de retardo, de modo que haya un retraso adecuado para asegurar que el módulo pueda procesar todos los eventos que se generan en la empresa. Por ejemplo, si el tiempo de retardo es 30 minutos y actualmente son las 14:00 h, el Concentrator comienza a extraer registros a las 13:30 h. La ventana de tiempo de retardo, 30 minutos en este ejemplo, permanece constante a medida que avanza la hora. Cuando la hora actual avanza hasta las 14:01 h, el Concentrator extrae los datos al minuto siguiente, a las 13:31 h, etc. **Importante**: El tiempo de retardo define el búfer entre la hora actual y la hora en que el módulo recopila los datos. **Precaución:** RSA recomienda que los administradores ajusten el parámetro Retardo de forma dinámica en función del rendimiento de cada uno de los Concentrators individuales para evitar la pérdida de eventos durante la agregación. Para obtener más información sobre el período de preparación y el tiempo de retardo, consulte Configuración del módulo.

Título	Descripción
	Permite seleccionar acciones adicionales para el mapeo del módulo seleccionado: • **Editar módulo**: Permite configurar el período de preparación y el tiempo de retardo para el mapeo del módulo seleccionado. • **Implementar**: Implementa el mapeo del módulo seleccionado. El servicio ESA Analytics especificado comienza a extraer datos de los orígenes de datos para ese módulo. • **Anular implementación**: Anula la implementación del mapeo del módulo seleccionado. El servicio ESA Analytics especificado deja de extraer datos de los orígenes de datos para ese módulo. **Precaución:** Anular la implementación de un mapeo con un estado de Implementado afectará la agregación de datos para ese módulo.

Configuración del módulo

Después de crear o implementar el mapeo de un módulo en el panel Mapeos de ESA Analytics (ADMIN > Sistema > ESA Analytics), tiene la opción de cambiar algunas configuraciones del módulo para ese mapeo.

¿Qué desea hacer?

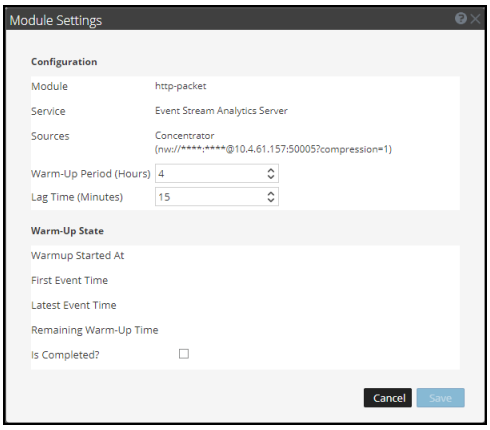
Función	Deseo…	Mostrarme cómo
Administrador	Cambiar el período de preparación de un mapeo de módulo no implementado.	Cambiar el período de preparación y el tiempo de retardo
Administrador	Cambiar el período de preparación de un mapeo de módulo durante el período de preparación.	Cambiar el período de preparación y el tiempo de retardo
Administrador	Cambiar el período de preparación de un mapeo de módulo una vez completo el período de preparación.	Cambiar el período de preparación y el tiempo de retardo

Temas relacionados

- Mapeo de orígenes de datos de ESA a módulos Analytics
- Mapeos de ESA Analytics

Configuración del módulo

Para acceder a la configuración del módulo, en el panel Mapeos de ESA Analytics, seleccione el mapeo que desea cambiar y, en la columna **Acciones**,  **> Editar módulo**. El cuadro de diálogo Configuración del módulo tiene una sección Configuraciones y una sección Estado de preparación.



Configuraciones

La sección Configuraciones permite modificar los ajustes de Período de preparación y Tiempo de retardo.

En la siguiente tabla se describe la configuración disponible para el mapeo de un módulo ESA Analytics.

Campo	Descripción
Módulo	Muestra el nombre del módulo mapeado.
Servicio	Muestra el servicio ESA Analytics que procesa los datos del mapeo.
Orígenes	Muestra los orígenes de datos mapeados y las direcciones URL que se usan para comunicarse con ESA.

Campo	Descripción
Período de preparación (horas)	Especifica una duración de la preparación en horas. Se requiere un período de preparación para permitir que Detección de amenazas automatizadas “conozca” su tráfico. El período de preparación se debe ejecutar cuando se esté ejecutando el tráfico típico. Durante este tiempo, se suprimen las alertas para el mapeo de módulo. El período de preparación prepara el módulo con datos históricos y garantiza que se complete la cantidad especificada de horas de recopilación de datos antes de que se envíen alertas. RSA proporciona módulos ESA Analytics preconfigurados. Cada tipo de módulo tiene un período de preparación predeterminado, que puede ajustar a su ambiente, si es necesario. Después de este período de preparación, se pueden ver las alertas. Puede actualizar el Período de preparación del mapeo de un módulo implementado en función de si este se completó o no: • **Durante el período de preparación**: Puede agregar horas al período de preparación o restar cualquier tiempo de preparación restante. • **El período de preparación se completó**: Puede agregar horas al período de preparación mediante la suma de la diferencia entre la hora actual y la Hora del primer evento a las horas que desea agregar. Por ejemplo, un período de preparación de 10 horas se completó y en la opción Hora del primer evento se muestra 12:00:00. La hora actual (sistema) son las 16:00:00 (4 horas después) y desea agregar 5 horas más al tiempo de preparación. Para hacerlo, debe agregar 9 horas (4+5=9) al período de preparación de 10 horas; por lo tanto, debe configurar el nuevo período de preparación en 19 horas. No puede disminuir el período de preparación si se completó, a menos que elimine el mapeo y cree uno nuevo. El valor de Período de preparación es específico de un mapeo determinado y se aplica a todos los Concentrators dentro de ese mapeo después de su implementación. Si dos módulos con distintos tiempos de preparación comparten un Concentrator, este utiliza valores de Período de preparación por separado para el mapeo de cada módulo.

Campo	Descripción
Tiempo de retardo (minutos)	Especifica el retraso de tiempo constante en minutos, el cual se suma para evitar la pérdida de eventos que los orígenes de datos procesan durante períodos de gran actividad. Por ejemplo, el rendimiento del Concentrator varía en función de factores como carga entrante, consultas continuas e indexación. Debido a estos factores, es posible que un Concentrator no pueda agregar eventos en tiempo real, lo que genera el retraso. El parámetro Retardo da al Concentrator la oportunidad de terminar de agregar todos los datos. Cuando se especifica un tiempo de retardo, la primera vez que se implementa el módulo, la agregación de datos comienza en **Hora (del sistema) actual - Tiempo de retardo - Tiempo de preparación**. Por ejemplo, si actualmente son las 14:00 h, el tiempo de retardo es 30 minutos y el tiempo de preparación es 4 horas, cuando el módulo se implementa por primera vez, la recopilación de datos se inicia a las 9:30 h (14:00 h - 0.5 horas - 4 horas). Después de que finaliza el período de preparación, la agregación de datos continúa en **Hora (del sistema) actual - Tiempo de retardo**. Esto es útil cuando la agregación de datos en un Concentrator se realiza con lentitud. El tiempo de retardo garantiza que el módulo no procese los datos que llegan al Concentrator dentro de la ventana de tiempo de retardo, de modo que haya un retraso adecuado para asegurar que el módulo pueda procesar todos los eventos que se generan en la empresa. Por ejemplo, si el tiempo de retardo es 30 minutos y actualmente son las 14:00 h, el Concentrator comienza a extraer registros a las 13:30 h. La ventana de tiempo de retardo, 30 minutos en este ejemplo, permanece constante a medida que avanza la hora. Cuando la hora actual avanza hasta las 14:01 h, el Concentrator extrae los datos al minuto siguiente, a las 13:31 h, etc. **Importante**: El tiempo de retardo define el búfer entre la hora actual y la hora en que el módulo recopila los datos. El valor de Tiempo de retardo es específico de un mapeo determinado y se aplica a todos los Concentrators dentro de ese mapeo después de su implementación. Si dos módulos con distintos tiempos de retardo comparten un Concentrator, este utiliza valores de retardo por separado para el mapeo de cada módulo. **Precaución:** RSA recomienda que los administradores ajusten el parámetro Retardo de forma dinámica en función del rendimiento de cada uno de los Concentrators individuales para evitar la pérdida de eventos durante la agregación. Para determinar el tiempo de retardo correcto, sume lo siguiente con el fin de obtener el tiempo de retardo de un ambiente:

Campo	Descripción
	1. **Latencia de registros o paquetes**: Este es el tiempo que tarda el Log Decoder en recibir los registros o el (Packet) Decoder en recibir los paquetes. Por ejemplo, el Log Decoder puede recibir registros cada 20 minutos. En este caso, tal vez desee configurar Tiempo de retardo en 20 minutos como mínimo, de preferencia 25 minutos, de modo que no se pierdan eventos. 2. **Latencia de agregación**: Este es el tiempo que tarda la transmisión de datos desde el Log Decoder al Concentrator. 3. **Otro búfer**: Sume cualquier retraso de tiempo adicional específico del ambiente.

Estado de preparación

En la sección Estado de preparación se proporciona información acerca del estado de preparación, la que puede usar para determinar los ajustes adecuados al período de preparación.

Campo	Descripción
La preparación se inició a las	La hora en que el módulo ESA Analytics procesó el primer evento desde el origen de datos.
Hora del primer evento	La hora a la que ocurrió el primer evento. El tiempo de preparación se basa en esta hora.
Hora del último evento	La hora a la que ocurrió el último evento.
Tiempo de preparación restante	La cantidad de horas restantes en el período de preparación.
¿Se completó?	Indica si el período de preparación se completó. Si es verdadero, el período de preparación se completó. Si es falso, el módulo aún se está preparando y la cantidad de horas restantes se puede ver en el campo Tiempo de preparación restante.