RSA NETWITNESS® SUITE

Guía de configuración del sistema

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

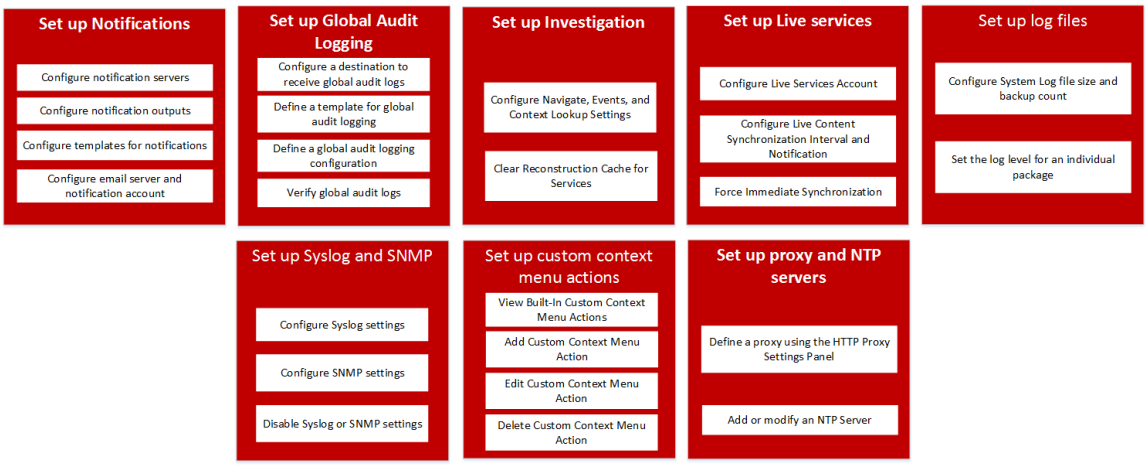
EMC considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

febrero 2018

Contenido

Descripción general de la configuración del sistema

En la vista Sistema de Administration, los administradores pueden configurar ajustes del sistema para obtener un rendimiento óptimo de NetWitness Suite. En este diagrama se muestran las opciones de configuración disponibles.



En esta guía, los procedimientos estándares proporcionan instrucciones para los administradores que desean personalizar los ajustes que se aplican en el sistema en NetWitness Suite. Aunque algunos de estos ajustes tienen valores predeterminados, el administrador tiene que ver y evaluar todos los valores predeterminados.

Los procedimientos adicionales no son esenciales para la configuración de NetWitness Suite, estos incluyen opciones de personalización específicas que van más allá de la configuración habitual; por ejemplo, agregar menús contextuales personalizados o configurar un proxy.

Además, los temas de referencia y los temas de solución de problemas proporcionan información detallada acerca de la interfaz del usuario y sugerencias para solucionar posibles problemas.

En las siguientes secciones se describe la configuración del sistema:

- Procedimientos estándar proporcionan instrucciones para los administradores que desean personalizar los ajustes que se aplican en el sistema en NetWitness Suite.
- Procedimientos adicionales proporcionan instrucciones para configurar las opciones de personalización que estén más allá de la configuración del sistema habitual.

Procedimientos estándar

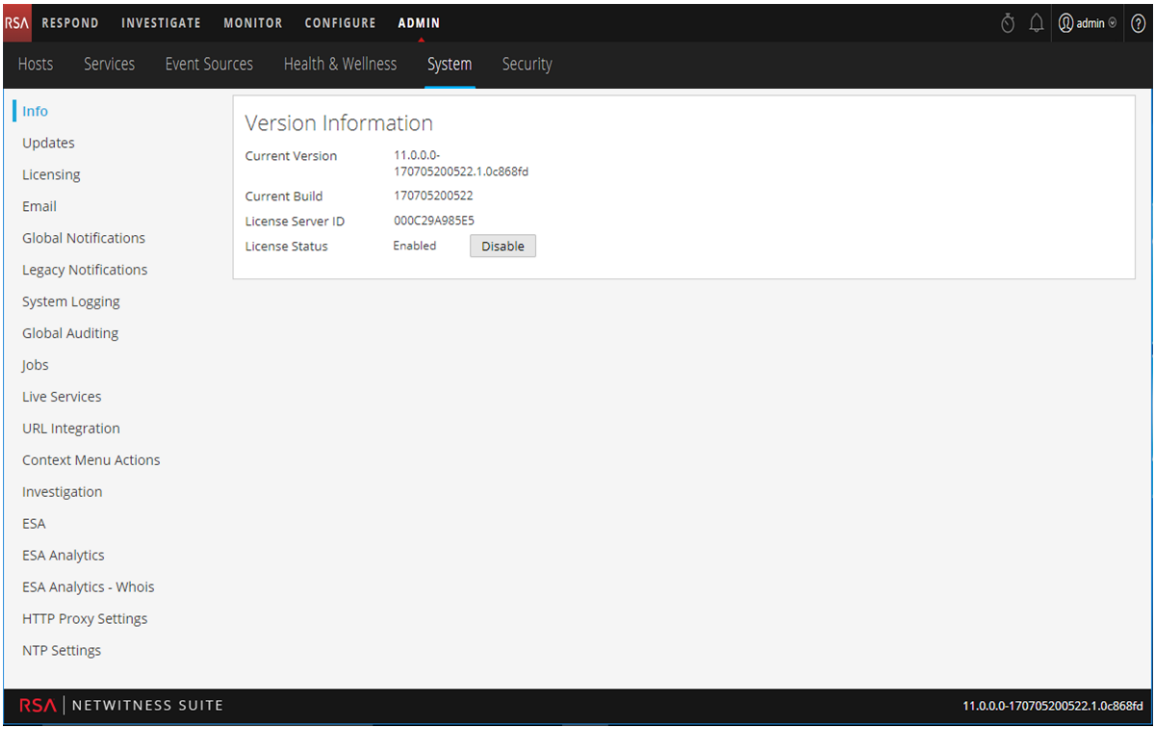
En los temas de esta sección se proporcionan instrucciones para los administradores que desean personalizar los ajustes que se aplican en el sistema en NetWitness Suite. Aunque algunos de estos ajustes tienen valores predeterminados, el administrador tiene que ver y evaluar todos los valores predeterminados. Los procedimientos se pueden ejecutar en cualquier secuencia y se enumeran alfabéticamente.

Acceder a la configuración del sistema

En este tema se presentan las funcionalidades de configuración del sistema de NetWitness Suite en la vista Sistema de Administration. Los administradores pueden configurar notificaciones, notificaciones por correo electrónico, el registro de auditoría global, los ajustes de registro, la conexión a los servicios de Live y la integración de URL en NetWitness Suite.

Para tener acceso a la configuración del sistema:

Vaya a **ADMIN > Sistema**.
Se muestra la vista Sistema de Administration.



En el panel del lado izquierdo de la vista Sistema de Administration hay un panel de opciones que muestra todos los nodos de sistema disponibles para configuración. Cuando selecciona un nodo, el contenido asociado se muestra en el panel de la derecha.

Configurar servidores de notificación

En este tema se proporcionan instrucciones para configurar los servidores de notificación. En ESA, los servidores de notificación se requieren para definir una regla de ESA. Un servidor de notificación también se requiere para configurar el registro de auditoría global.

Las configuraciones de las notificaciones globales definen los ajustes de las notificaciones para Administración de orígenes de eventos (ESM), Estado y condición, el registro de auditoría global, Event Stream Analysis (ESA) y RESPOND. Los servidores de notificación definen los servidores desde los cuales desea recibir notificaciones del sistema. Para el registro de auditoría global, defina Log Decoders como servidores de notificación de syslog.

Puede definir, eliminar, editar, importar y exportar un servidor de notificaciones en NetWitness Suite. Cada tema describe los procedimientos pertinentes. Para obtener más información sobre la configuración de alertas de ESA, consulte “Métodos de notificación” en la **Guía de alertas mediante ESA**. Las salidas de las notificaciones y los servidores de notificación se eliminan, editan, importan y exportan de la misma manera que las plantillas. No puede inhabilitar ni eliminar servidores de notificación asociados a configuraciones del registro de auditoría global.

Descripción general de servidores de notificación

En este tema se proporciona una descripción general de los servidores de notificación. Los servidores de notificación se configuran en la vista Sistema de Administration (Administration > Sistema > Notificaciones > pestaña Servidores).

Varios componentes de NetWitness Suite, como Event Stream Analysis (ESA), RESPOND, Estado y condición, Administración de orígenes de eventos (ESM) y el registro de auditoría global, usan notificaciones globales. Los ajustes de notificaciones se denominan **servidores de notificación**.

Event Stream Analysis envía notificaciones a los usuarios mediante un correo electrónico, SNMP o Syslog, acerca de diversos eventos del sistema. En ESA, estos ajustes de notificaciones de alertas se denominan servidores de notificación. Puede configurar varios servidores de notificación y usarlos mientras define una regla de ESA. Por ejemplo, puede configurar varios servidores de correo o servidores de syslog y utilizar los ajustes durante la definición de una regla de ESA.

Puede configurar los siguientes servidores de notificación:

- Correo electrónico
- SNMP
- Syslog
- Script

Los servidores de notificación por correo electrónico permiten configurar ajustes del servidor de correo electrónico para enviar notificaciones de alerta. Los servidores de notificación de SNMP permiten configurar ajustes de host de SNMP trap como un servidor de notificación para enviar notificaciones de alerta.

Los servidores de notificación de syslog permiten configurar ajustes de syslog como un servidor de notificación para enviar notificaciones. Cuando está activado, syslog proporciona auditoría mediante el uso del protocolo RFC 5424 de syslog. Syslog ha demostrado ser un formato eficaz para consolidar registros, dado que existen muchas herramientas de propiedad o de código abierto para generar informes y análisis. Para el registro de auditoría global, solo puede usar servidores de notificación de syslog.

Los servidores de notificación de script permiten configurar el script como un servidor de notificación.

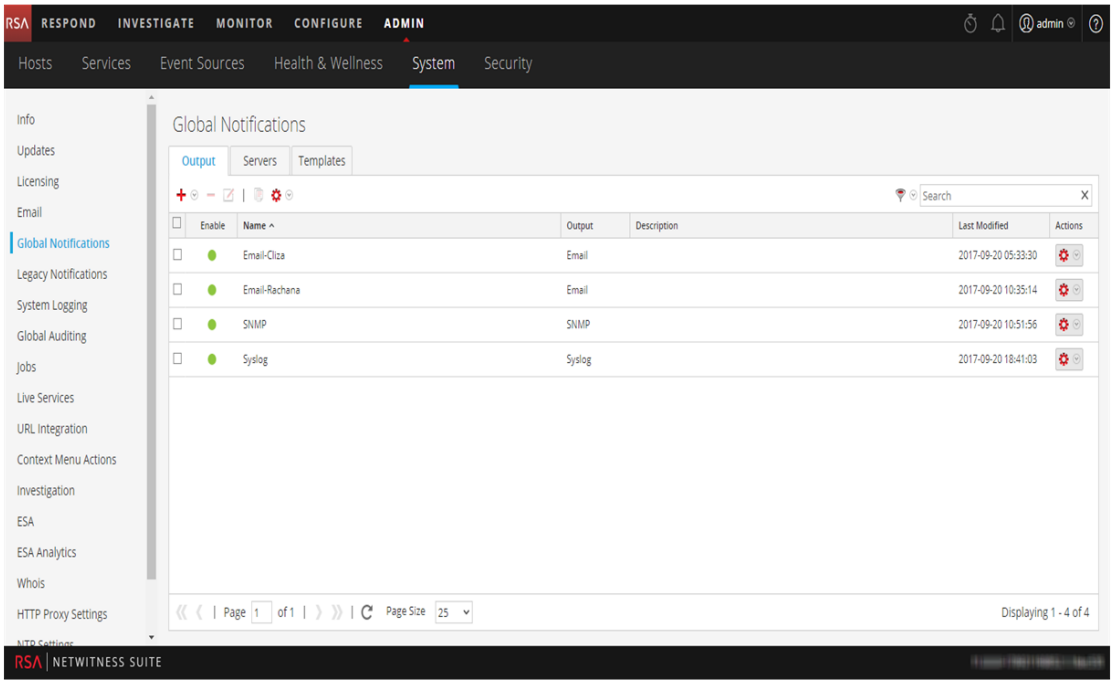
Para obtener información detallada sobre las distintas configuraciones de servidores de notificación, incluidos los parámetros y las descripciones, consulte Cuadros de diálogo de definición de servidores de notificación.

Configurar los ajustes de correo electrónico como un servidor de notificación

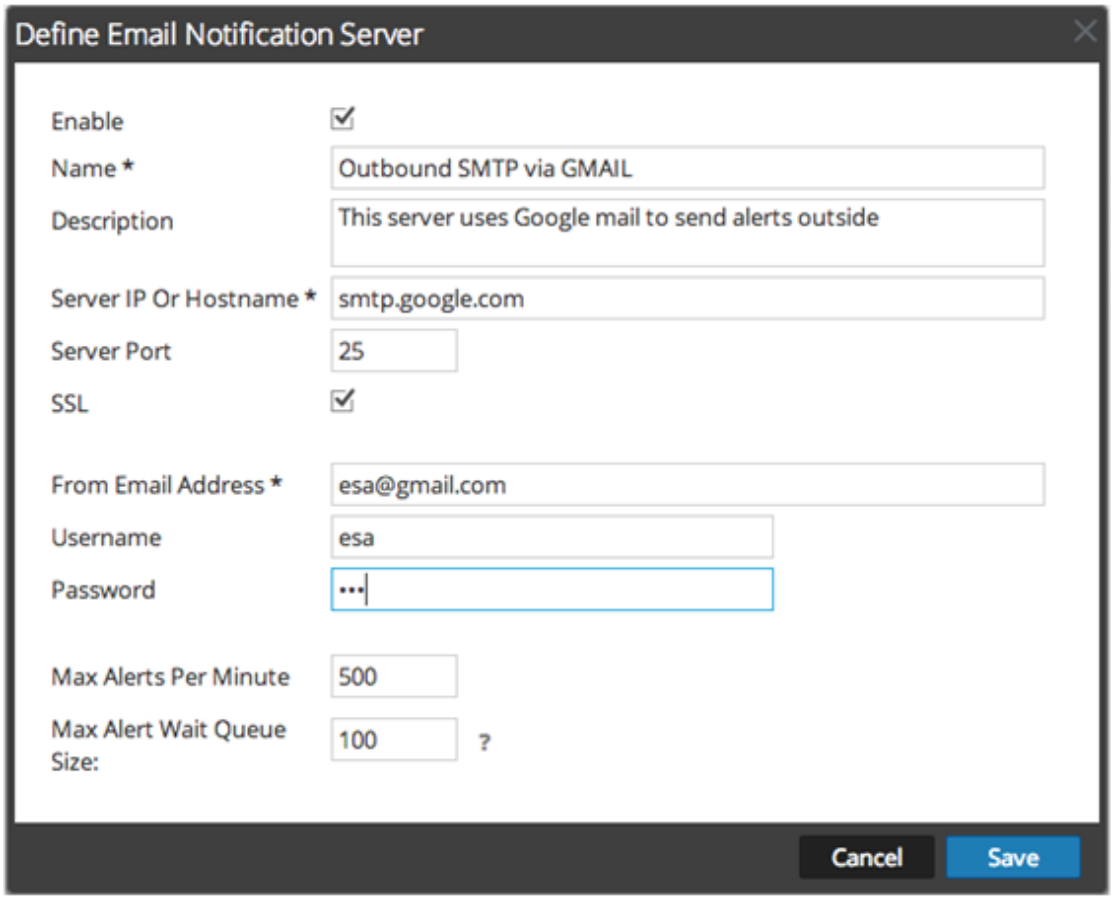
Para configurar los ajustes de servidores de correo electrónico como un servidor de notificación para enviar notificaciones de alertas:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
   El panel de configuración **Notificaciones** se muestra con la pestaña **Salida** abierta.

3. Haga clic en la pestaña **Servidores**.



4. En el menú desplegable + , seleccione **Correo electrónico**.



5. En el cuadro de diálogo **Definir servidor de notificación de correo electrónico**, proporcione la información requerida y haga clic en **Guardar**.

Nota: Para notificaciones de ESM/SMS y ESA, debe especificar solo el nombre de host/nombre de dominio calificado en el campo Dirección IP o nombre de host del servidor.

Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

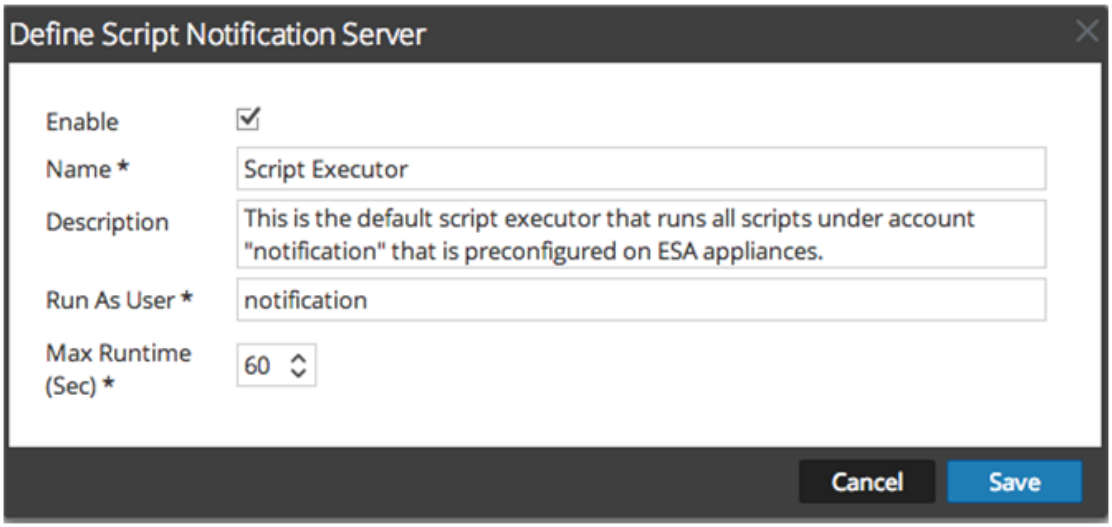
Configurar un script como un servidor de notificación

ESA permite ejecutar scripts en respuesta a alertas de ESA. Primero, debe configurar la identidad del usuario y otros detalles que se requieren para ejecutar los scripts.

Para configurar un script como un servidor de notificación:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Servidores**.

4. En el menú desplegable , seleccione **Script**.



5. En el cuadro de diálogo **Definir servidor de notificación de script**, proporcione la información requerida y haga clic en **Guardar**.

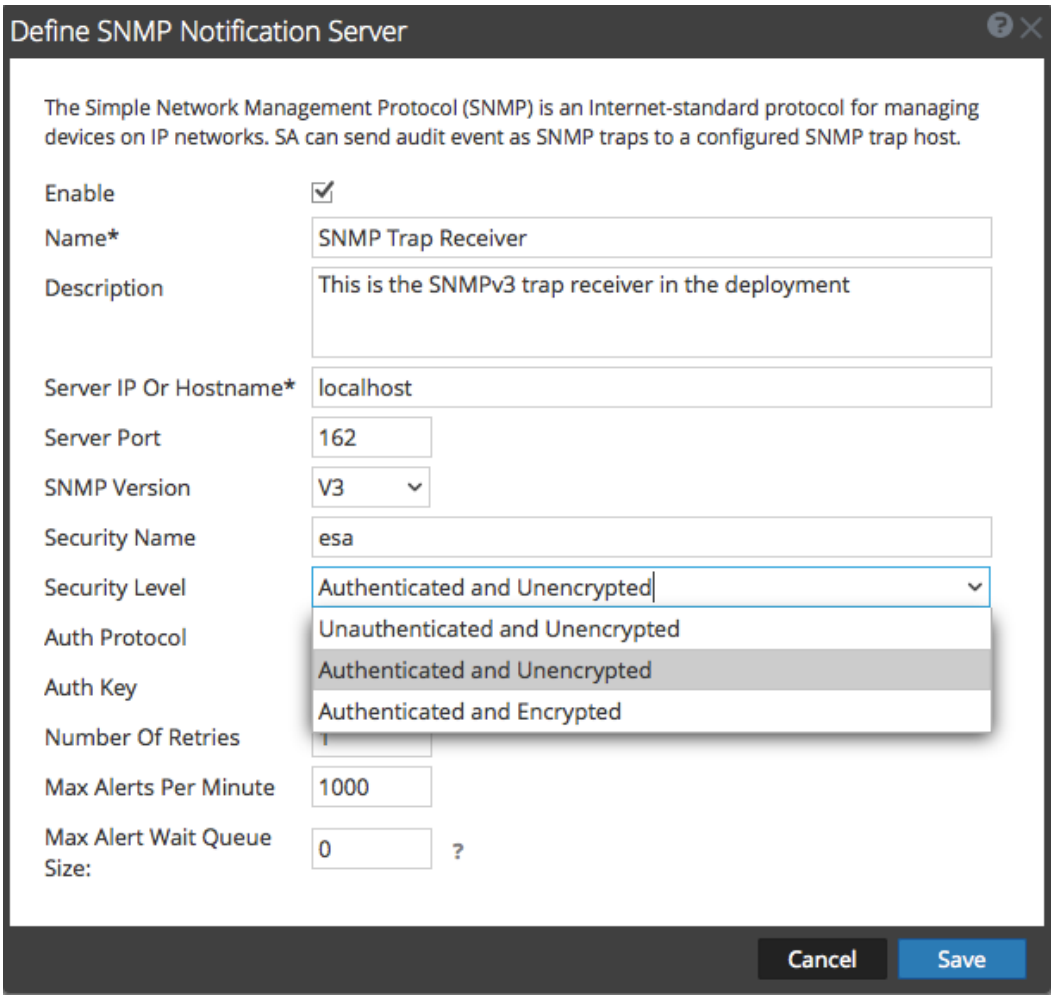
Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

Configurar los ajustes de SNMP como un servidor de notificación

Para configurar los ajustes de host de SNMP trap como un servidor de notificación para enviar notificaciones de alertas:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Servidores**.

4. En el menú desplegable + , seleccione **SNMP**.



5. En el cuadro de diálogo **Definir servidor de notificación de SNMP**, proporcione la información requerida y haga clic en **Guardar**.

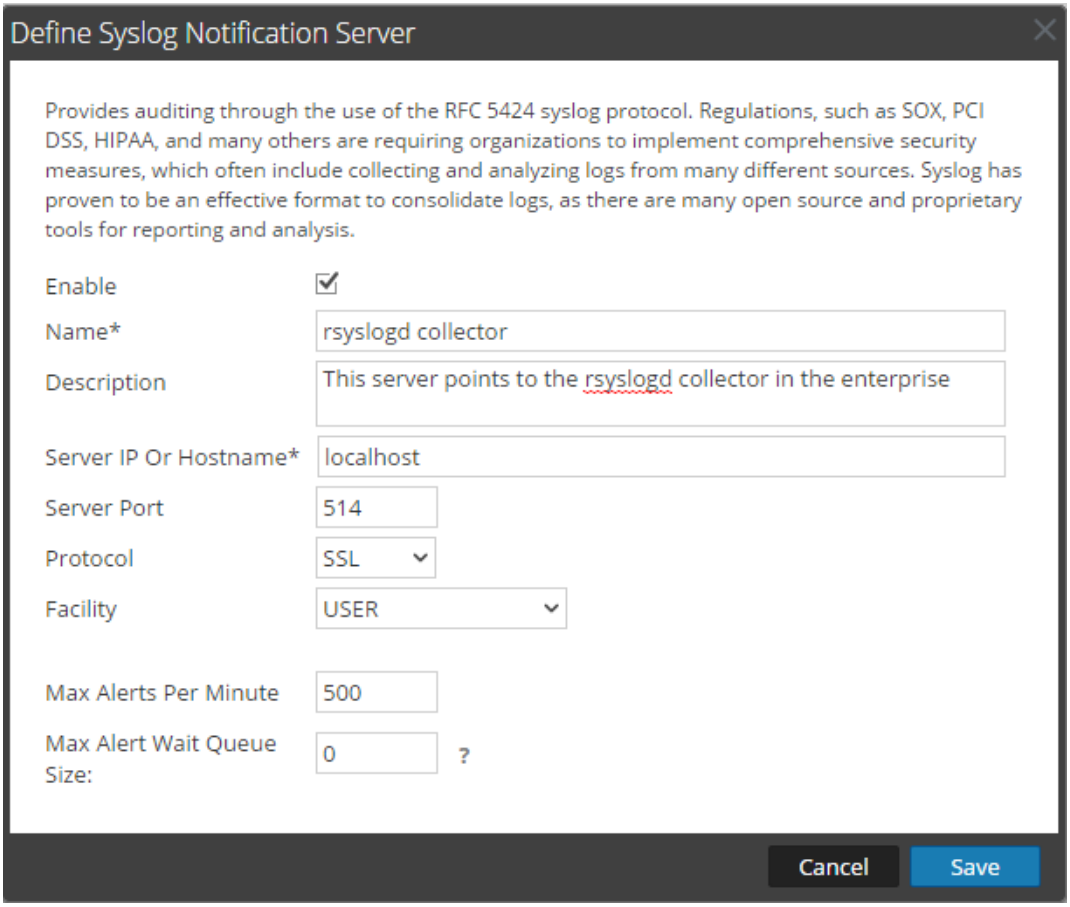
Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

Configurar un servidor de notificación de syslog

En este tema se proporcionan instrucciones para configurar un servidor de notificación de syslog. Cuando está activado, syslog proporciona auditoría mediante el uso del protocolo RFC 5424 de syslog. Syslog ha demostrado ser un formato eficaz para consolidar registros, dado que existen muchas herramientas de propiedad o de código abierto para creación de informes y análisis.

Para configurar syslog como un servidor de notificación:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Servidores**.
4. En el menú desplegable , seleccione **Syslog**.



5. En el cuadro de diálogo **Definir servidor de notificación de syslog**, proporcione la información requerida y haga clic en **Guardar**.

Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

Configurar las salidas de las notificaciones

En este tema se proporcionan instrucciones para configurar las salidas de las notificaciones. Estas salidas de las notificaciones se requieren para definir una regla de ESA.

Las configuraciones de las notificaciones globales definen los ajustes de las notificaciones para Administración de orígenes de eventos (ESM), Estado y condición, el registro de auditoría global, Event Stream Analysis (ESA) y RESPOND.

No es necesario configurar la pestaña Salida para el registro de auditoría global.

Las configuraciones de las salidas de las notificaciones definen direcciones de correo electrónico y líneas de asunto, ajustes de OID de SNMP trap, ajustes de la salida de syslog y el código de scripts.

Puede definir, eliminar, editar, importar y exportar salidas de notificaciones en NetWitness Suite. En cada tema se describen los procedimientos pertinentes. Para obtener más información sobre la configuración de alertas de ESA, consulte “Métodos de notificación”. Las salidas de las notificaciones y los servidores de notificación se eliminan, editan, importan y exportan de la misma manera que las plantillas. Si intenta eliminar una salida de notificación que se usa en alertas, recibirá un mensaje de confirmación de advertencia que señala que las alertas que usan la notificación no funcionarán correctamente. El mensaje muestra la cantidad de alertas en uso.

Descripción general de salidas de notificaciones

En este tema se proporciona una descripción general de las salidas de las notificaciones. Estas salidas de notificaciones se requieren cuando se define una regla de ESA. Las salidas de las notificaciones se configuran en la vista Sistema de Administration (Administration > Sistema > Notificaciones > pestaña Salidas).

Las configuraciones de las notificaciones globales definen los ajustes de las notificaciones para Administración de orígenes de eventos (ESM), Estado y condición, el registro de auditoría global, Event Stream Analysis (ESA) y RESPOND.

Nota: No es necesario configurar salidas de notificaciones (pestaña Salida) para el registro de auditoría global.

Las salidas de notificaciones son los destinos que se usan para el envío de notificaciones. Para ESA, las salidas de las notificaciones permiten definir cómo desea recibir las alertas de ESA. Las siguientes son las distintas salidas de notificaciones compatibles con NetWitness Suite:

- Correo electrónico
- SNMP
- Syslog
- Script

La configuración de notificaciones por correo electrónico define la dirección de correo electrónico de destino a la cual puede enviar las alertas. También permiten agregar una descripción personalizada en el asunto del correo electrónico y definir múltiples direcciones de correo electrónico de destino.

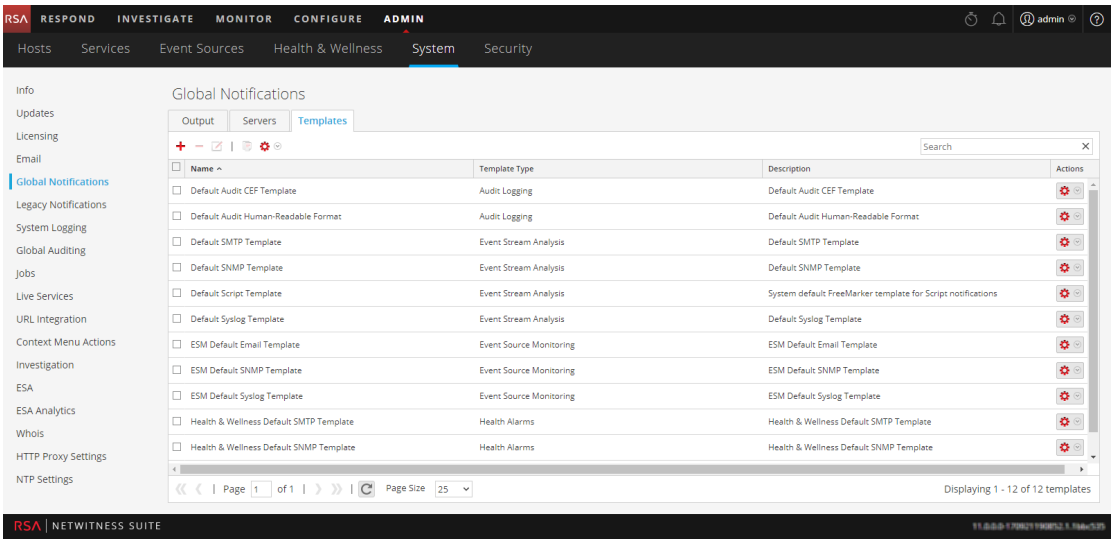
La configuración de notificación de SNMP permite definir la configuración de SNMP para enviar notificaciones de alerta. Las notificaciones de syslog permiten definir los ajustes de syslog que se usan para enviar notificaciones de alerta. Las notificaciones de script permiten definir el script que se ejecuta en respuesta a la alerta.

Para obtener información detallada sobre las configuraciones de notificaciones, incluidos los parámetros y las descripciones, consulte Cuadros de diálogo de definición de servidores de notificación.

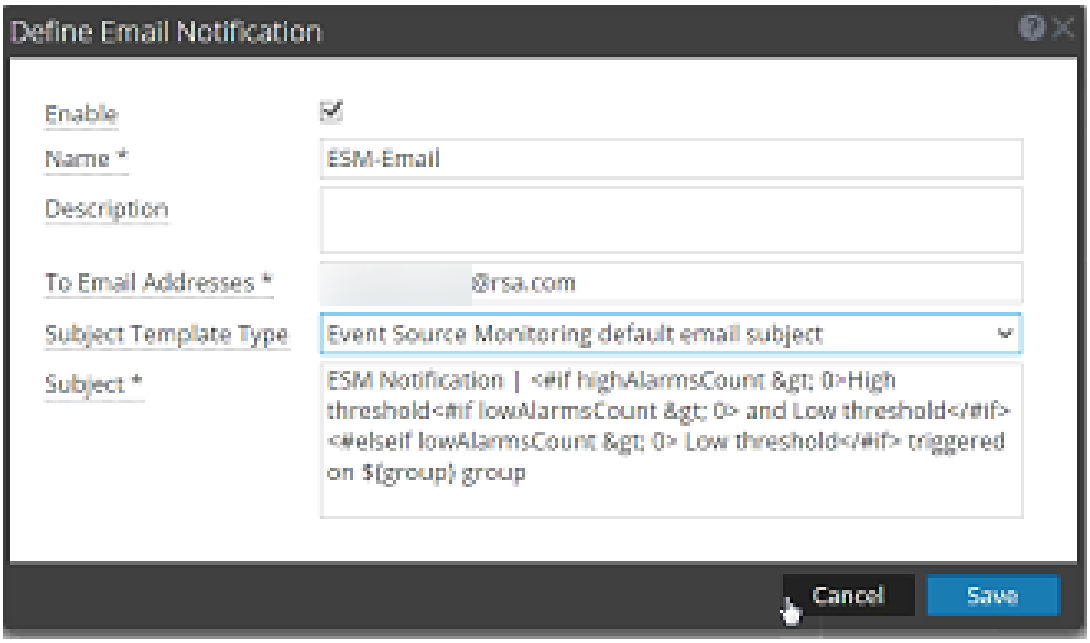
Configurar el correo electrónico como una notificación

Para configurar el correo electrónico como una notificación:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.



3. En la pestaña **Salida**, en el menú desplegable , seleccione **Correo electrónico**.



4. En el cuadro de diálogo **Definir notificación de correo electrónico**, proporcione la información requerida y haga clic en **Guardar**.

Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

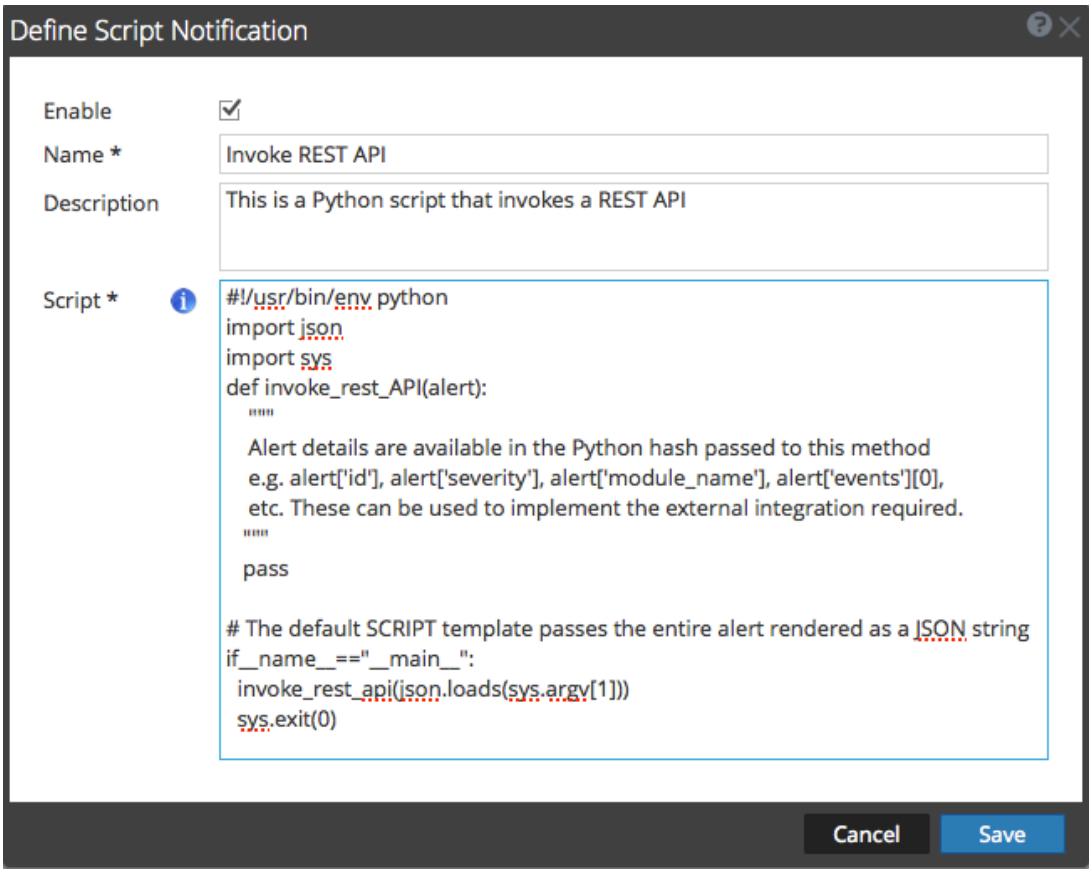
Configurar el script como una notificación

En este tema se proporcionan instrucciones para definir el script y configurarlo como una salida de notificación. ESA permite ejecutar scripts en respuesta a alertas de ESA. Debe definir el script mediante ADMIN > Sistema > Notificaciones > pestaña Salida. Puede usar cualquier script para las notificaciones de ESA.

Para configurar el script como una notificación:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.

3. En la pestaña Salida, en el menú desplegable , seleccione **Script**.



4. En el cuadro de diálogo **Definir notificación de script**, proporcione la información requerida y haga clic en **Guardar**.

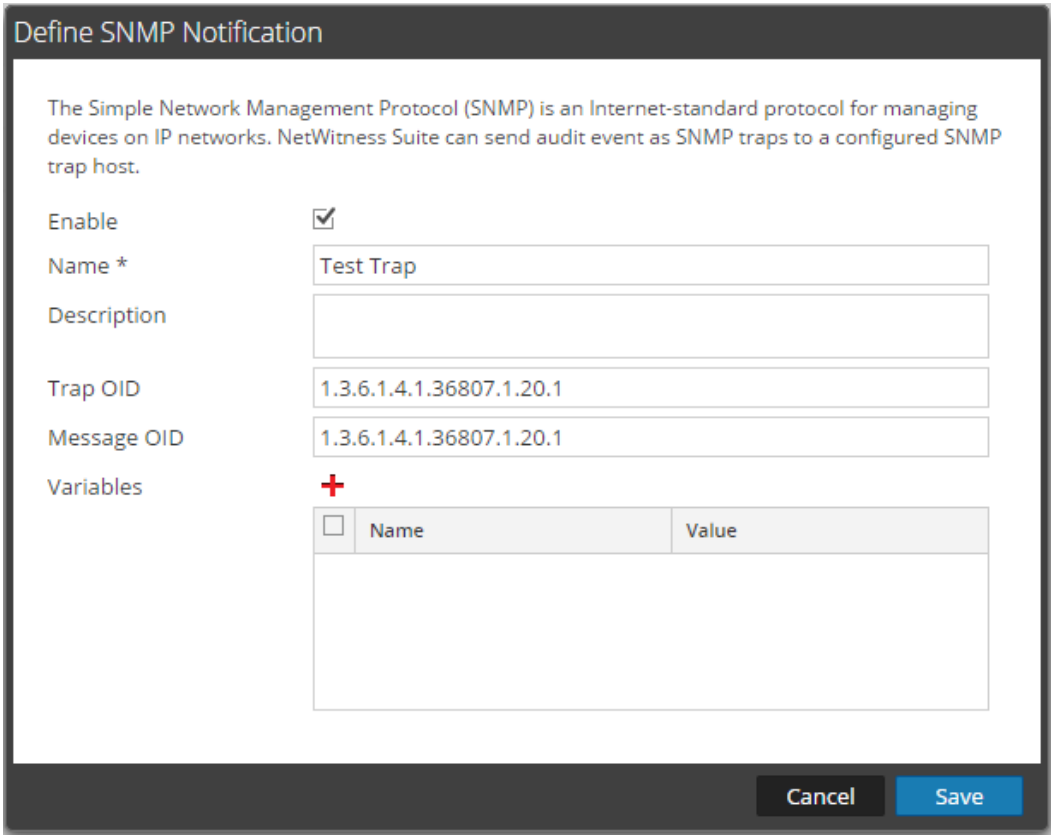
Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

Configurar SNMP como una notificación

Para configurar SNMP como una salida de notificación para enviar notificaciones de alertas:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.

3. En la pestaña Salida, en el menú desplegable + , seleccione **SNMP**.



4. En el cuadro de diálogo Notificación de SNMP, proporcione la información requerida y haga clic en **Guardar**.

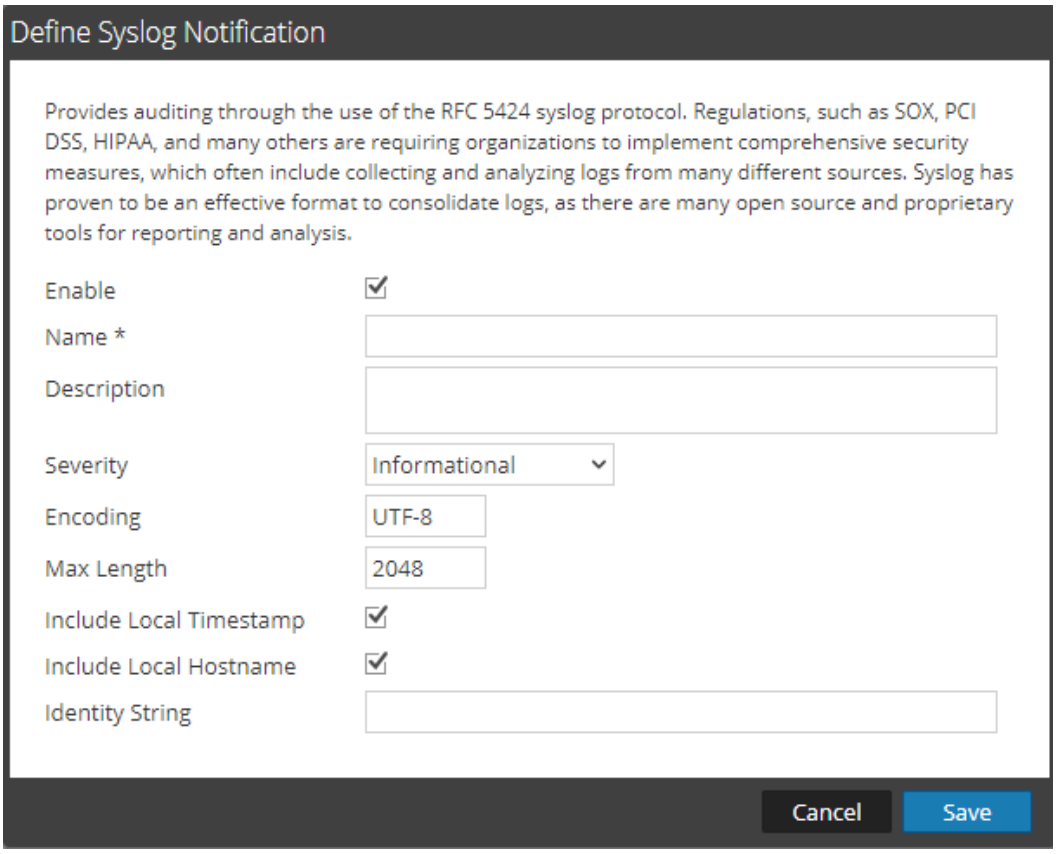
Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

Configurar syslog como una notificación

Para configurar Syslog como una salida de notificación para enviar notificaciones de alertas:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.

3. En la pestaña Salida, en el menú desplegable , seleccione **Syslog**.



4. En el cuadro de diálogo **Definir notificación de syslog**, proporcione la información requerida y haga clic en **Guardar**.

Para obtener detalles y descripciones de los parámetros, consulte Cuadros de diálogo de definición de servidores de notificación.

Configurar plantillas para notificaciones

Las plantillas de notificación se configuran en la vista Sistema de Administration (Administration > Sistema > Notificaciones > pestaña Plantillas). Una plantilla de notificación define el formato y los campos de mensajes de las notificaciones. Puede configurar distintos tipos de plantilla para las notificaciones:

- Registro de auditoría
- Event Stream Analysis
- Monitoreo de orígenes de eventos
- Alarmas de estado

Puede usar las plantillas predeterminadas disponibles o configurar plantillas propias para correo electrónico, SNMP, syslog y script, según el tipo de plantilla.

El registro de auditoría global envía registros de auditoría en el formato que se especifica en la plantilla del registro de auditoría. Puede usar las plantillas predeterminadas del registro de auditoría o puede definir una plantilla del registro de auditoría propia. Para obtener más información sobre cómo definir una plantilla del registro de auditoría, consulte Definir una plantilla para el registro de auditoría global.

Event Stream Analysis (ESA) envía notificaciones en el formato especificado en las plantillas de Event Stream Analysis. Las plantillas predeterminadas de Event Stream Analysis para correo electrónico, SNMP, syslog y script están disponibles en la instalación. Puede personalizar estas plantillas además de crear nuevas plantillas que puede usar para las notificaciones. Para obtener más información sobre cómo definir plantillas de ESA, consulte Definir una plantilla para notificaciones de alertas de ESA.

Para obtener más información sobre la configuración de alertas de ESA, consulte “Métodos de notificación” en la **Guía de alertas mediante ESA**. No puede eliminar plantillas asociadas a configuraciones del registro de auditoría global.

Nota: Cuando se actualiza desde NetWitness Suite 10.4, todas las plantillas de notificación existentes migran al tipo de plantilla de Event Stream Analysis.

Para aprender a definir, eliminar, editar, duplicar, importar y exportar una plantilla de notificación en NetWitness Suite, consulte:

Configurar plantillas de notificaciones globales

Definir una plantilla para notificaciones de alertas de ESA

Importar y exportar una plantilla de notificaciones globales

Configurar plantillas de notificaciones globales

En este tema se proporcionan instrucciones para agregar, editar, duplicar y eliminar plantillas de notificaciones globales.

Puede usar las plantillas predeterminadas disponibles o configurar plantillas propias para correo electrónico, SNMP, syslog y script, según el tipo de plantilla.

El registro de auditoría global envía registros de auditoría en el formato que se especifica en la plantilla del registro de auditoría. Puede usar las plantillas predeterminadas del registro de auditoría o puede definir una plantilla del registro de auditoría propia. Para obtener más información sobre cómo definir una plantilla de registro de auditoría, consulte “Definir una plantilla para el registro de auditoría global”.

Event Stream Analysis (ESA) envía notificaciones en el formato especificado en las plantillas de Event Stream Analysis. Las plantillas predeterminadas de Event Stream Analysis para correo electrónico, SNMP, syslog y script están disponibles en la instalación. Puede personalizar estas plantillas además de crear nuevas plantillas que puede usar para las notificaciones. Para obtener más información sobre cómo definir plantillas de ESA, consulte Definir una plantilla para notificaciones de alertas de ESA.

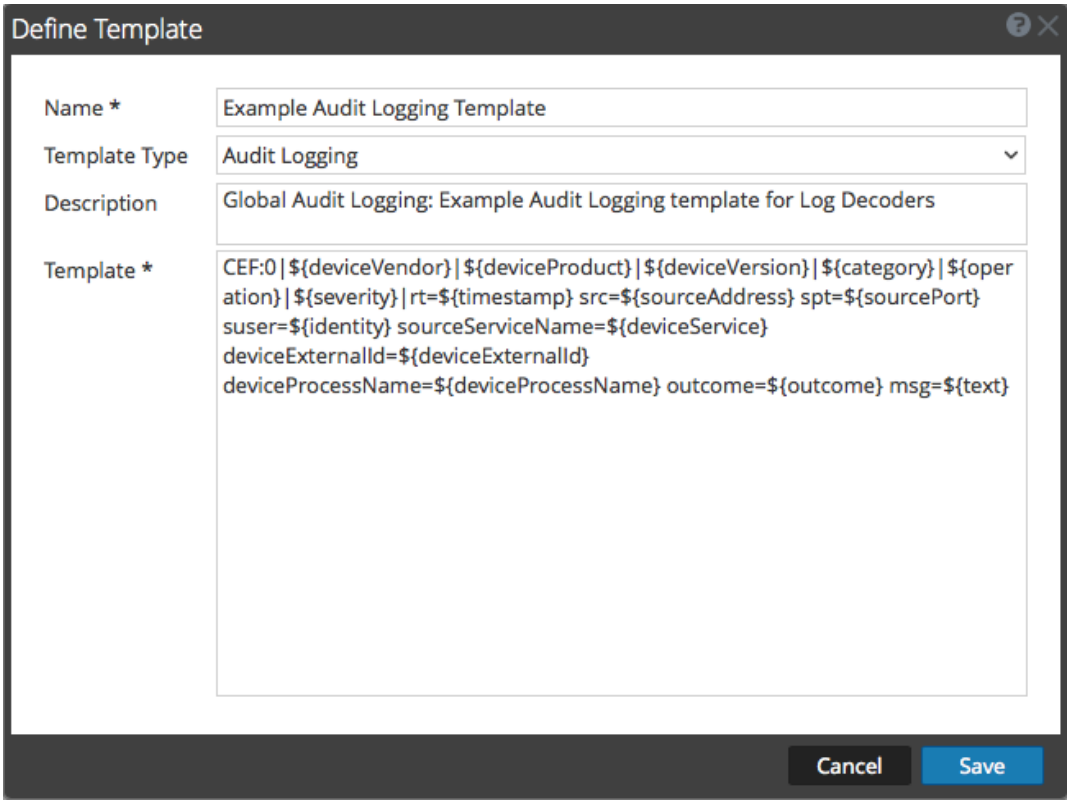
Cuando se actualiza desde NetWitness Suite 10.4, todas las plantillas de notificación existentes migran al tipo de plantilla de Event Stream Analysis.

Agregar una plantilla

Puede usar las plantillas predeterminadas que se proporcionan o puede configurar sus propias plantillas. Para configurar una plantilla propia:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Plantillas**.
4. Haga clic en + para configurar una plantilla.
5. En el cuadro de diálogo **Definir plantilla**, proporcione la siguiente información:
   a. En el campo **Nombre**, escriba el nombre para la plantilla.
   b. En el campo **Tipo de plantilla**, seleccione el tipo de plantilla que desea crear. Por ejemplo, si está creando una plantilla para el registro de auditoría global, seleccione el tipo de plantilla Registro de auditoría.
   c. En el campo **Descripción**, escriba una descripción breve para la plantilla.
   d. En el campo **Plantilla**, especifique el formato de la plantilla.

e. Haga clic en **Guardar** para guardar la plantilla.



Duplicar una plantilla

Puede hacer una copia de una plantilla predeterminada actual o de una plantilla definida por el usuario. Para duplicar una plantilla:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Plantillas**.
4. Seleccione la plantilla que desea duplicar y haga clic en .

   Aparece el cuadro de diálogo Duplicar plantilla de alerta.

5. Escriba el nombre de la plantilla duplicada.
6. Haga clic en **Aceptar**.

Puede modificar una plantilla predeterminada o definida por el usuario. Cuando edita una plantilla, los cambios se reflejan solo cuando se activa la alerta.

Editar una plantilla

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Plantillas**.
4. Seleccione una plantilla y haga clic en .
5. En el cuadro de diálogo **Definir plantilla**, modifique los campos **Nombre**, **Tipo de plantilla**, **Descripción** y **Plantilla** según sea necesario.
6. Haga clic en **Guardar** para guardar la plantilla.

Eliminar una plantilla

Puede eliminar una plantilla definida por el usuario. Cuando se elimina una plantilla que se usa en una regla de ESA, se usa la plantilla predeterminada de Event Stream Analysis para las alertas. No se pueden eliminar plantillas asociadas a configuraciones del registro de auditoría global.

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Plantillas**.
4. Seleccione una o varias plantillas y haga clic en .

   Se muestra un cuadro de diálogo de confirmación.
5. Haga clic en **Sí**.

   La plantilla seleccionada se elimina.

Definir una plantilla para notificaciones de alertas de ESA

En este tema se describe cómo definir una plantilla para las notificaciones de alerta. Event Stream Analysis (ESA) permite definir plantillas útiles para las alertas. Necesita entender bien FreeMarker y el modelo de datos de ESA para definir una plantilla. Para obtener más información sobre FreeMarker, consulte Guía del autor de la plantilla de FreeMarker.

Modelo de datos de ESA

Considere una regla de alerta de ESA como se muestra a continuación:

```
@Name('module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert')
@Description('Brute Force Login To Same Destination')
@RSAAlert(oneInSeconds=0, identifiers={"ip_dst"})
SELECT* FROMEvent (ec_activity = 'Logon',ec_theme = 'Authentication',ec
outcome = 'Failure',ip_dst IS NOT NULL)
.std:groupwin(ip_dst)
.win:time_length_batch(60 seconds, 2)
GROUPBYip_dst HAVING COUNT(*) = 2;
```

Cuando se activa una regla como la de arriba, la alerta generada tendrá dos eventos constitutivos, donde cada uno se asemeja a una sesión de NextGen con múltiples valores de metadatos. El objeto de datos de alerta transmitido al evaluador de la plantilla de FreeMarker será como el siguiente:

```
(root)
  |
  +- id = "4e67012f-9c53-4f0b-ac44-753e2c982b79"                    // Unique identifier for
each alert
  |
  +- severity = 1                                                    // The severity of the
alert
  +- time = 2013-12-31T11:02Z                                        // The alert time (needs a
?datetime for proper rendering)
  |  +- moduleType = "ootb"                                          // The module type
  |
  +- moduleName = "Brute Force Login To Same Destination"            // A description of the
module
  |
  +- statement = "module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert" // The name of the EPL
statement
  |  +- events                                                       // The constituent events -
as a sequence of event maps
       |   +- [0]                                                   // offset 0 (i.e. the first
constituent event)
       |   |       |   |
       |   +- event_cat_name = "User.Activity.Failed Logins"
       |   +- device_class = "Firewall"                             // event meta (accessible
as ${events[0].device_class}$)
       |   |       |   +- event_source_id = "uttam:50002:1703395"   // Investigation URI to the
individual session (used by SA)
       |   |
       |   +- ...                                                   // Other meta
       |   |
       |   +- sessionid = 1703395                                   // NextGen sessionid
       |   |
       |   +- time = 1388487764                                     // event/session time at
NextGen source (as a long Unix timestamp)
       |   |
       |   +- user_dst = "user5"
       |
       +- [1]                                                       // offset 1 (i.e. the
second consituent event)
           |
           +- device_class = "Firewall"
           |
           +- event_cat_name = "User.Activity.Failed Logins"
           |
```

```
+- event_source_id = "uttam:50002:1703405"
|
+- ...
|
+- sessionid = 1703405
|
+- time = 1388487766
|
+- user_dst = "user5"
```

Hay dos tipos de variables de plantillas disponibles en el modelo de datos:

- **Metadatos de alerta:** Contienen detalles a nivel de alerta como nombre de la declaración, nombre del módulo, id de la alerta, hora de la alerta, gravedad y otros. En la terminología FreeMarker, estas son variables de nivel superior asociadas con la instancia de alerta y se pueden consultar simplemente por sus nombres, por ejemplo `${moduleName}`. Los metadatos `time` son especiales porque son del tipo `Date` y deben tener `?datetime` como sufijo para representarse adecuadamente.

- **Metadatos de eventos constitutivos**: incluyen los campos de metadatos de sesión de eventos individuales que constituyen la alerta. Una alerta puede tener múltiples eventos constitutivos por lo que puede haber más de uno de esos mapas en la misma alerta. Estos se muestran como una secuencia de hashes para el evaluador de la plantilla de FreeMarker y s debe hacer referencia a ellos. Por ejemplo, la alerta tiene dos eventos constitutivos, el event_source_id correspondiente al primero está disponible como `${events[0].event_source_id}` y se puede acceder al mismo, correspondiente al segundo como ${`events[1].event_source_id`}. También debe tener en cuenta qué campos de metadatos tienen varios valores, porque es necesario tratarlos como secuencias, por ejemplo, ${`events[0].alias_host`} no funcionará porque es una secuencia.

Nota: Los metadatos disponibles en los eventos constitutivos para una alerta dada los determina la cláusula EPL SELECT. Por ejemplo, las alertas de `SELECT sessionid, time FROM ...` tendrán solo dos valores de metadatos disponibles (sessionid, time). Los eventos constitutivos en `SELECT * FROM Event ...` incluirán todos los campos de metadatos del tipo `Event` con valores **no nulos**.

Si la plantilla usa claves de metadatos que no están presentes en todas las salidas de alertas, debe considerar el uso de las disposiciones de FreeMarker para los valores predeterminados.

Por ejemplo, si una plantilla con texto Id=${id},ec_outcome=${ec_outcome} se evalúa para una alerta que no incluye la clave de metadatos `ec_outcome`, se produce un error en la evaluación de la plantilla. En esos casos, puede usar el marcador de posición del valor omitido`${ec_outcome!”default”}`.

Importar y exportar una plantilla de notificaciones globales

En este tema se proporcionan instrucciones para importar y exportar una plantilla para notificaciones.

- Puede exportar plantillas predeterminadas o definidas por el usuario.
- Puede importar una plantilla que se exportó desde la instancia de NetWitness Suite. Si importa una plantilla con el mismo nombre de una plantilla existente, esta última se sobrescribirá.

Importar una plantilla

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Plantillas**.
4. En la barra de herramientas, seleccione  **> Importar**.
   Se muestra el cuadro de diálogo **Importar**.
5. En el campo **Escribir nombre de archivo**, escriba el nombre de archivo o haga clic en **Navegar** y seleccione el archivo que se va a importar.
6. Haga clic en **Importar**.

Exportar una plantilla

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Plantillas**.
4. Seleccione la plantilla que desea exportar.

   Nota: Puede exportar todas las plantillas mediante la opción  **> Exportar todo**.
5. En la columna **Acciones**, seleccione  **> Exportar**.
   Se mostrará el cuadro de diálogo **Exportar**.
6. En el campo **Escribir nombre de archivo**, escriba el nombre de archivo.
7. Haga clic en **Guardar**.

Configurar los servidores de correo electrónico y las cuentas de notificaciones

En este tema se proporciona instrucciones para configurar el correo electrónico, de modo que los usuarios puedan recibir notificaciones en NetWitness Suite. RSA NetWitness® Suite puede enviar notificaciones a los usuarios mediante correo electrónico sobre diversos eventos del sistema. Para poder configurar estas notificaciones de correo electrónico, primero debe configurar el servidor de correo electrónico SMTP. El panel Configuración de correo electrónico proporciona un método para:

- Configurar el servidor de correo electrónico.
- Configurar una cuenta de correo electrónico para recibir notificaciones.
- Ver las estadísticas sobre las operaciones de correo electrónico.

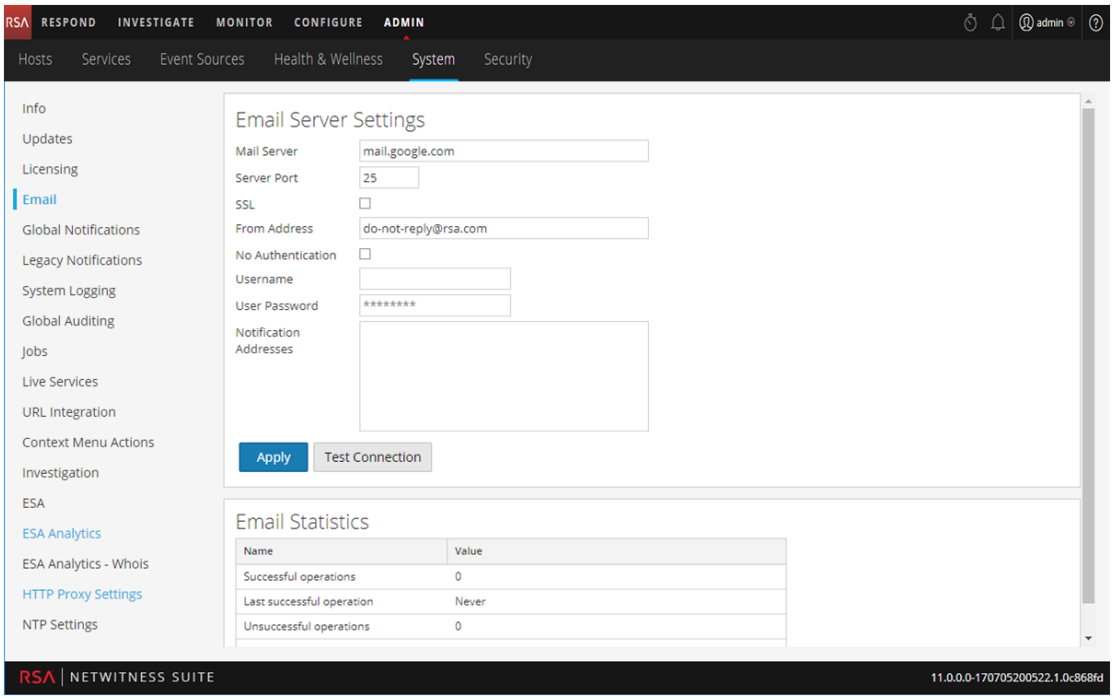
NetWitness Suite requiere acceso a un servidor de correo SMTP para enviar informes a los usuarios. Cada cuenta de usuario puede configurarse para recibir informes por correo electrónico. Estos informes se pueden generar manualmente, a través de la interfaz del usuario, o de forma automática, mediante el sistema de auditoría. Se aplican las siguientes reglas:

- Cualquier host de correo SMTP se puede utilizar para enviar correos electrónicos y cada host necesita una configuración diferente. El proveedor SMTP proporciona los ajustes para la configuración.
- Algunos servidores SMTP necesitan autenticación de usuario para retransmitir los correos electrónicos correctamente. Generalmente, es el inicio de sesión y la contraseña de la cuenta de correo electrónico.
- La mejor práctica es crear una nueva cuenta de correo electrónico dedicada en el servidor de correo electrónico SMTP para informes de NetWitness Suite.

Para configurar notificaciones de correo electrónico de NetWitness Suite:

1. Vaya a **ADMIN > Sistema**.
   Se muestra la vista Sistema de Administration.

2. En el panel de opciones, seleccione **Correo electrónico**.



3. Si desea cambiar el servidor de correo electrónico predeterminado, especifique el nombre del **servidor de correo** y el **puerto del servidor**.
4. Si el servidor de correo electrónico se comunica con NetWitness Suite mediante SSL, seleccione la casilla junto a **Usar SSL.**
5. En el campo **Dirección de remitente**, ingrese el nombre de la cuenta de correo electrónico que envía las notificaciones de correo electrónico de NetWitness Suite.
6. Si el servidor SMTP requiere la autenticación de usuario para enviar correos de forma satisfactoria, ingrese el **Nombre de usuario** y la **Contraseña de usuario** para iniciar sesión en la cuenta de correo electrónico.
7. Para activar las configuraciones, haga clic en **Aplicar**.
   Ahora puede configurar módulos de NetWitness Suite para recibir diversas notificaciones por correo electrónico.

Configurar el registro de auditoría global

El registro de auditoría global proporciona a los auditores de NetWitness Suite la visibilidad consolidada en tiempo real de las actividades de los usuarios dentro de NetWitness Suite desde una ubicación centralizada. Esta visibilidad incluye registros de auditoría recopilados desde el sistema NetWitness Suite y los diversos servicios en toda la infraestructura de NetWitness Suite.

Los registros de auditoría de NetWitness Suite se recopilan en un sistema centralizado que los convierte al formato requerido y los reenvía a un sistema de syslog externo. El sistema de syslog externo puede ser un servidor de syslog de otros fabricantes o un Log Decoder.

El registro de auditoría global se configura en el panel Configuraciones de registro de auditoría global. Una plantilla del registro de auditoría define el formato y los campos de mensajes de las entradas del registro de auditoría. Una configuración de servidor de notificación de syslog define el destino para enviar los registros de auditoría. Si desea reenviar registros de auditoría a un Log Decoder, configure un tipo de servidor de notificación de syslog para el Log Decoder.

Las siguientes son algunas de las acciones de los usuarios que se registran desde NetWitness Suite:

- Sesión iniciada correctamente del usuario
- Error de inicio de sesión del usuario
- Cierres de sesión del usuario
- Máximo de errores al iniciar sesión superado
- Todas las páginas de la interfaz del usuario a las cuales se accedió
- Cambios en la configuración confirmados (incluido cuando un usuario cambia su propia contraseña)
- Consultas que realizó el usuario
- Acceso del usuario denegado
- Operaciones de exportación de datos

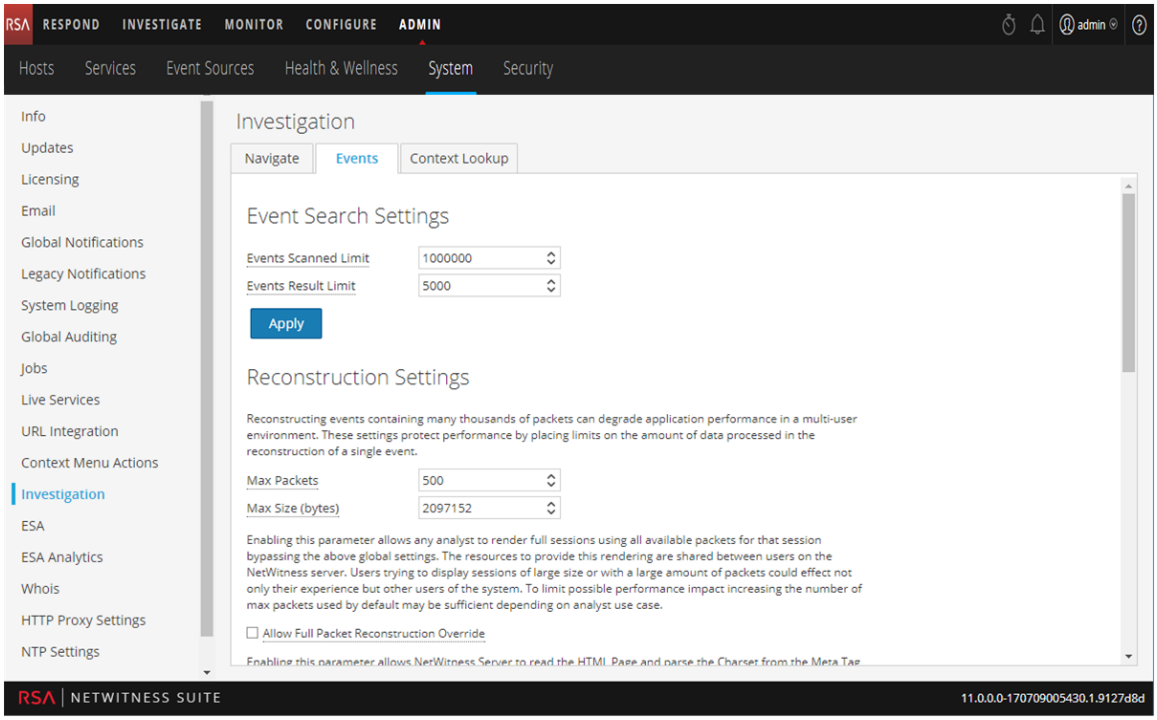
Después de que crea una configuración del registro de auditoría global, los registros de auditoría que contienen estas acciones de usuario se dirigen automáticamente al sistema de syslog externo en el formato especificado en la plantilla del registro de auditoría seleccionada. Puede crear múltiples configuraciones del registro de auditoría global para distintos destinos que usan distintas plantillas. Por ejemplo, puede crear una configuración del registro de auditoría global para un servidor de syslog externo con una plantilla que contiene todas las claves de metadatos disponibles, y otra para un Log Decoder con una plantilla que contiene claves de metadatos seleccionadas.

Para Log Decoders, use Default Audit CEF Template. Puede agregar o eliminar campos de la plantilla del formato de evento común (CEF) si tiene requisitos específicos. En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones y en Claves de metadatos de CEF compatibles se describen las claves de metadatos de CEF disponibles para usar en las plantillas del registro de auditoría.

Para servidores de syslog de otros fabricantes, puede usar una plantilla del registro de auditoría predeterminada o definir un formato propio (CEF o no CEF). En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones y en Variables de claves de metadatos del registro de auditoría global compatibles se describen las variables disponibles.

Los auditores pueden ver los registros de auditoría en el Log Decoder seleccionado o en un servidor de syslog de otros fabricantes. Si usan un Log Decoder, los auditores pueden ver los registros de auditoría mediante NetWitness Suite Investigation o Reports.

En la siguiente figura se muestran registros auditoría global en Investigation (Investigation > Eventos).



Para obtener ejemplos de algunas de las acciones de los usuarios que se registran, consulte Cuadro de diálogo Agregar nueva configuración. Para obtener una lista de los tipos de mensajes que registran los diversos componentes de NetWitness Suite, consulte Referencia de operaciones del registro de auditoría global.

Registro de auditoría global: procedimiento general

El registro de auditoría global se configura en el panel Configuraciones de registro de auditoría global, al cual se accede desde la vista Sistema > Auditoría global de Administration. Antes de que pueda configurar el registro de auditoría global, debe configurar un servidor de notificación de syslog y una plantilla del registro de auditoría. Un servidor de notificación de syslog define el destino al cual se envían los registros de auditoría. Una plantilla del registro de auditoría define el formato y los campos de mensajes de la entrada del registro de auditoría.

El panel Configuraciones de registro de auditoría global proporciona un vínculo **ver configuración** que lo lleva al panel Notificaciones globales (vista Sistema > Notificaciones globales de Administration), donde puede configurar el servidor de notificación de syslog y la plantilla del registro de auditoría.

Realice los siguientes procedimientos en el orden que se muestra para configurar el registro de auditoría global.

Procedimientos	Referencia/instrucciones
1. Configurar un servidor de notificación de syslog.	Configure un servidor de notificación de syslog que se usará para el registro de auditoría global. Puede definir un servidor de syslog de otros fabricantes o un Log Decoder como destino para recibir los registros de auditoría. Configurar un destino para recibir registros de auditoría global. Las configuraciones del registro de auditoría global usan el tipo de servidor de notificación de syslog. Si desea reenviar registros de auditoría a un Log Decoder, cree un servidor de notificación de tipo syslog.

Procedimientos	Referencia/instrucciones
2. Seleccione o configure una plantilla del registro de auditoría que se usará.	Seleccione una plantilla del registro de auditoría para el servidor de notificación de syslog. Puede usar una plantilla del registro de auditoría predeterminada o definir una plantilla propia. Las configuraciones del registro de auditoría global usan el tipo de plantilla del registro de auditoría y un servidor de notificación de syslog. En Configurar plantillas para notificaciones se proporciona información adicional. Para Log Decoders, use **Default Audit CEF Template**. Puede agregar o quitar campos de la plantilla del formato de evento común (CEF) si tiene requisitos específicos. En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones. Para servidores de syslog de otros fabricantes, puede usar una plantilla del registro de auditoría predeterminada o definir un formato propio (CEF o no CEF). En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones y en Variables de clave de metadatos de registro de auditoría global compatibles se describen las variables disponibles.
3. (Opcional: solo si consume con un Log Decoder) Implementar el analizador del formato de evento común en el Log Decoder desde Live.	Asegúrese de haber implementado y habilitado el analizador del formato de evento común más reciente desde Live. En Buscar e implementar recursos de Live y Habilitar e inhabilitar analizadores de registros se proporcionan instrucciones.

Procedimientos	Referencia/instrucciones
4. Definir una configuración del registro de auditoría global, la cual establece cómo se reenvían los registros de auditoría global a sistemas de syslog externos.	En Definir una configuración del registro de auditoría global se proporcionan instrucciones. Después de agregar una configuración del registro de auditoría global, los registros de auditoría se reenvían al servidor de notificación seleccionado en la configuración.
5. Verificar que los registros de auditoría global muestren los eventos de auditoría.	Pruebe los registros de auditoría para asegurarse de que muestren los eventos de auditoría definidos en la plantilla del registro de auditoría. En Verificar registros de auditoría global se proporcionan instrucciones.

Configurar un destino para recibir registros de auditoría global

En el registro de auditoría global, los servidores de notificación de syslog son las configuraciones que definen los destinos para recibir registros de auditoría global. Debe configurar un servidor de notificación de syslog para el uso del registro de auditoría global. Puede definir un servidor de syslog de otros fabricantes o un Log Decoder como el destino para recibir los registros de auditoría.

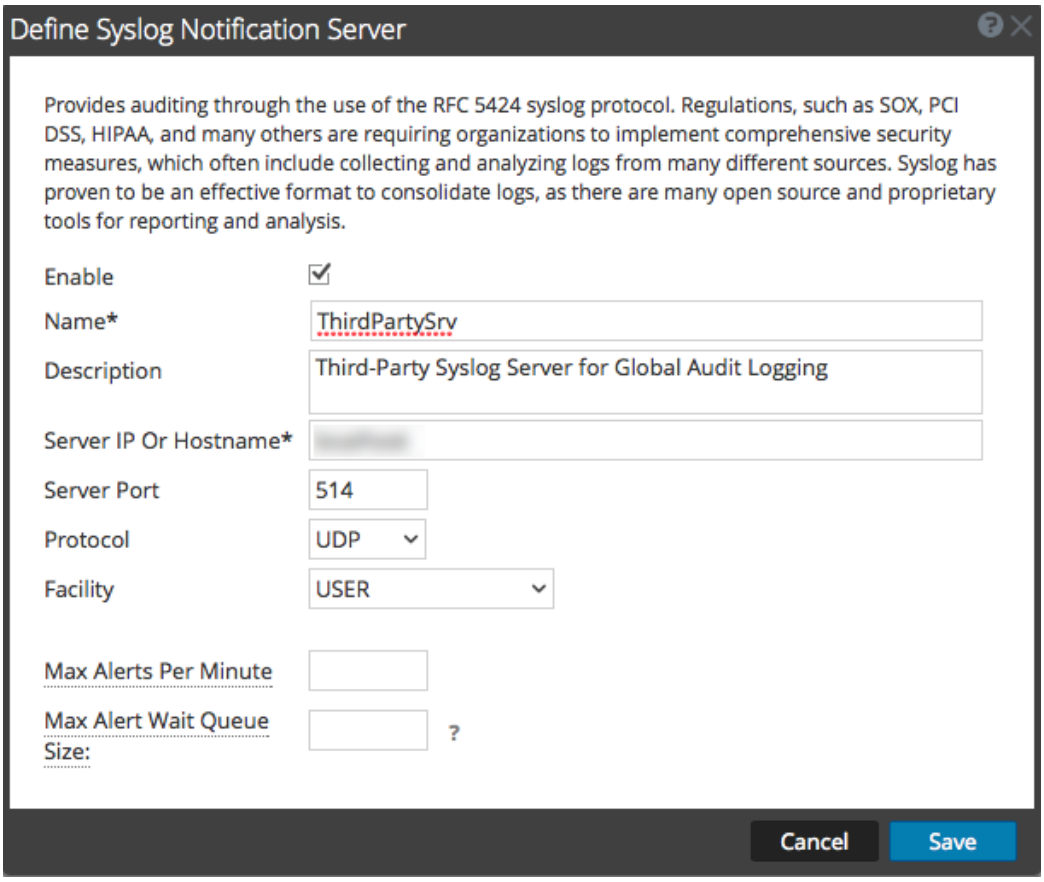
Configurar un servidor de notificación de syslog para un servidor de syslog de otros fabricantes

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Servidores**.

   Nota: No es necesario configurar la pestaña Salida para el registro de auditoría global.

4. En el menú desplegable  , seleccione **Syslog**.

   Se muestra el cuadro de diálogo **Definir servidor de notificación de syslog**.



5. Configure el servidor de notificación de syslog como se describe en la siguiente tabla.

Campo	Descripción
Habilitar	Seleccione esta opción para activar el servidor de notificación.
Nombre	Nombre para identificar o etiquetar el servidor de syslog de otros fabricantes.
Descripción	(Opcional) Descripción breve del servidor de notificación.
Dirección IP o nombre de host del servidor	Nombre de host o dirección IP del servidor de syslog de otros fabricantes.
Puerto del servidor	Número de puerto donde escucha el proceso de syslog de destino.
Protocolo	Protocolo que se usará para transferir registros de auditoría con formato al servidor de syslog de otros fabricantes.

Campo	Descripción
Funcionalidad	Funcionalidad de syslog que se usará para escribir registros de auditoría con formato en el servidor de syslog de otros fabricantes.

Los campos **Máx. de alertas por minuto** y **Tamaño de línea de espera máximo de alertas** no se usan para el registro de auditoría global.

6. Haga clic en **Guardar**.

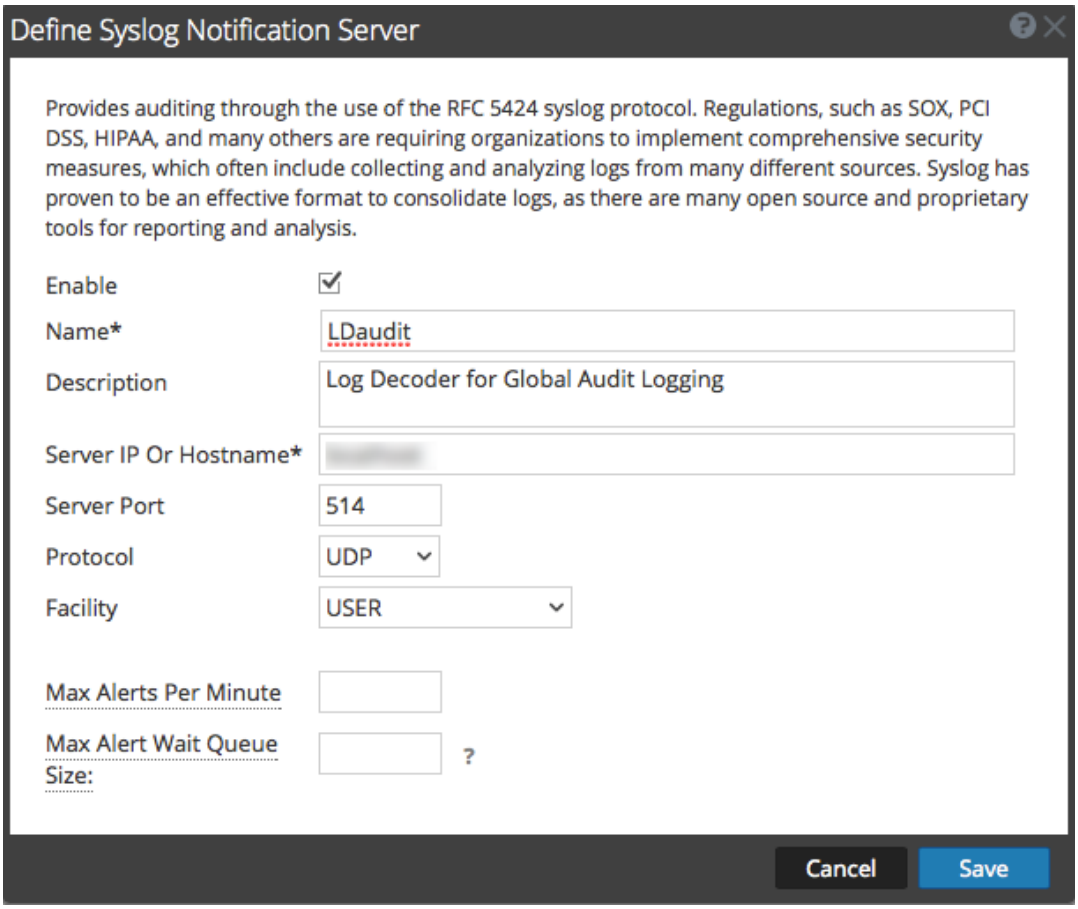
Configurar un servidor de notificación de syslog para un Log Decoder

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Servidores**.

   Nota: No es necesario configurar la pestaña Salida para el registro de auditoría global.

4. En el menú desplegable  , seleccione **Syslog**.

   Se muestra el cuadro de diálogo **Definir servidor de notificación de syslog**.



5. Configure el servidor de notificación de syslog como se describe en la siguiente tabla.

Campo	Descripción
Habilitar	Seleccione esta opción para activar el servidor de notificación.
Nombre	Nombre para identificar o etiquetar el servidor de notificación de syslog de Log Decoder.
Descripción	(Opcional) Descripción breve del servidor de notificación.
Dirección IP o nombre de host del servidor	Nombre de host o dirección IP de Log Decoder.
Puerto del servidor	Número de puerto donde escucha el proceso de syslog de destino.
Protocolo	Protocolo que se usará para transferir registros de auditoría con formato al Log Decoder.

Campo	Descripción
Funcionalidad	Funcionalidad de syslog que se usará para escribir registros de auditoría con formato en el Log Decoder.

Los campos **Máx. de alertas por minuto** y **Tamaño de línea de espera máximo de alertas** no se usan para el registro de auditoría global.

6. Haga clic en **Guardar**.

Próximos pasos

Seleccione una plantilla del registro de auditoría predeterminada que se usará para el registro de auditoría global. Si es necesario, puede definir una plantilla personalizada propia. En Definir una plantilla para el registro de auditoría global se proporciona información adicional.

Definir una plantilla para el registro de auditoría global

En este tema se proporcionan instrucciones para definir una plantilla del registro de auditoría destinada al uso con el registro de auditoría global. Antes de configurar el registro de auditoría global, configure un servidor de notificación de syslog y seleccione una plantilla del registro de auditoría. Puede optar por usar una plantilla del registro de auditoría predeterminada o puede definir una plantilla propia.

NetWitness Suite incluye dos plantillas de registro de auditoría predeterminadas:

- **Default Audit CEF Template**: puede usar esta plantilla para Log Decoders y servidores de syslog de otros fabricantes.
- **Default Audit Human-Readable Format**: puede usar esta plantilla exclusivamente para servidores de syslog de otros fabricantes. No reenvíe mensajes desde esta plantilla a un Log Decoder.

En el primer procedimiento se proporcionan instrucciones para definir una plantilla del registro de auditoría para un Log Decoder. La plantilla del registro de auditoría define el formato y los campos de mensajes de los registros de auditoría que se envían al Log Decoder o al servidor de syslog de otros fabricantes.

Las plantillas del registro de auditoría global que define para un Log Decoder usan el formato de evento común (CEF) y deben cumplir con los siguientes requisitos estándar específicos:

- Incluya los encabezados de CEF en la plantilla.
- Use solo las extensiones (Clave=Valor) que se indican en la tabla Claves de metadatos de CEF compatibles.
- Asegúrese de que las extensiones estén en el formato `key=${string}<space>key=${string}.`

En el segundo procedimiento se proporcionan instrucciones para definir una plantilla personalizada del registro de auditoría global en lenguaje natural para un servidor de syslog de otros fabricantes. Para servidores de syslog de otros fabricantes, puede definir un formato propio (CEF o no CEF).

Definir una plantilla del registro de auditoría global para un Log Decoder

Puede usar **Default Audit CEF Template** para enviar registros de auditoría global a un Log Decoder. Para definir una plantilla propia:

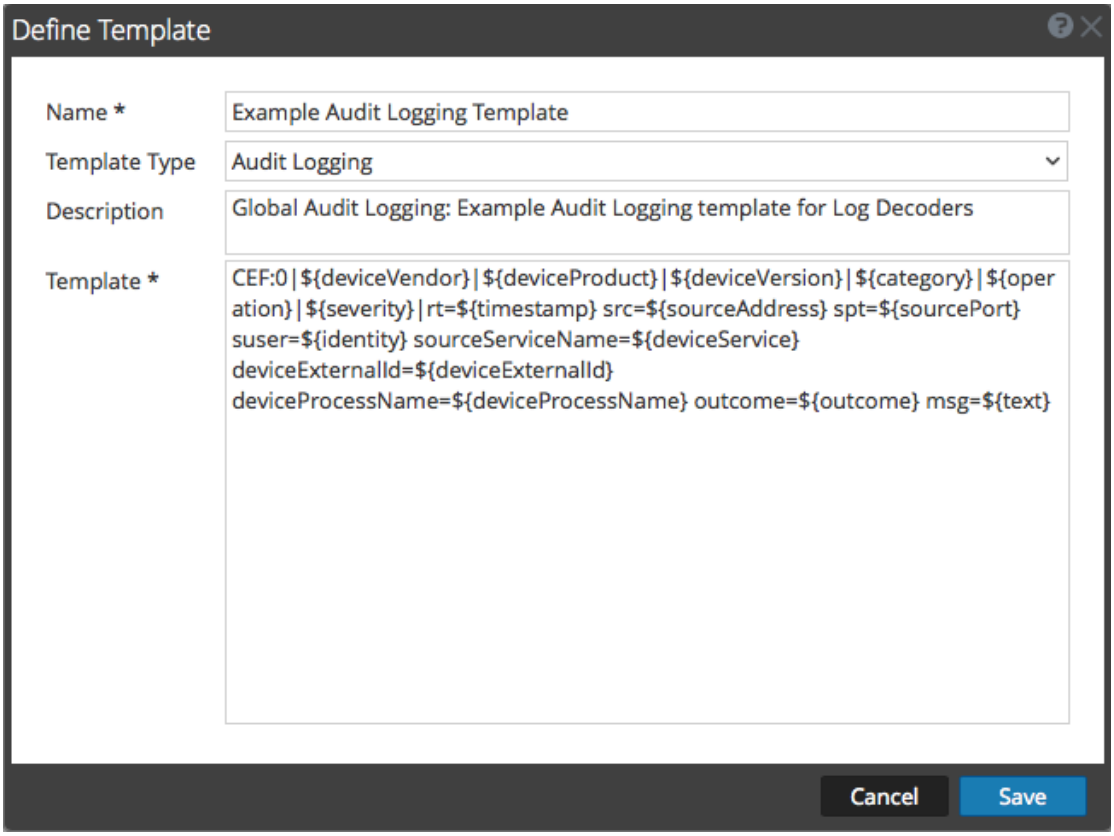
1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. Haga clic en la pestaña **Plantillas**.
4. Haga clic en  para configurar una plantilla.
5. En el cuadro de diálogo **Definir plantilla**, proporcione la siguiente información:
   a. En el campo **Nombre**, escriba el nombre para la plantilla.
   b. En el campo **Tipo de plantilla**, seleccione el tipo de plantilla **Registro de auditoría**.
   c. En el campo **Descripción**, escriba una descripción breve para la plantilla.
   d. En el campo **Plantilla**, ingrese el formato de la plantilla del registro de auditoría.
   El siguiente formato es una plantilla personalizada que se proporciona como ejemplo. Difiere de la plantilla de CEF predeterminada.

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}|${oper
ation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome}
msg=${text}
```

El encabezado de syslog de CEF resaltado se requiere para ajustarse al estándar CEF y es un requisito para el analizador de CEF en el Log Decoder. Las otras claves son opcionales y puede configurarlas. Consulte todas las claves de metadatos compatibles con el analizador de CEF en el Log Decoder en la tabla Claves de metadatos de CEF compatibles.

Nota: Use todas las extensiones en el siguiente formato:
`deviceProcessName=${deviceProcessName} outcome=${outcome}`
Incluya un `<space>` entre cada par key=${string} en la sección de claves de extensión.

6. Haga clic en **Guardar**.



Una vez que defina la plantilla del registro de auditoría de CEF, asegúrese de haber implementado y habilitado el analizador del formato de evento común (CEF) más reciente desde Live. En “Buscar e implementar recursos de Live” y “Habilitar y deshabilitar analizadores de registros” se proporcionan instrucciones.

Nota: Si necesita usar claves de metadatos específicas para Investigation y Reporting, asegúrese de que las claves de metadatos que selecciona estén indexadas en el archivo **table-map.xml** en el Log Decoder. Si no lo están, siga el tema Mantener los archivos de mapa de tablas del procedimiento de la *Guía de configuración de hosts y servicios* para actualizar los mapeos de tablas. Asegúrese de que las claves de metadatos también estén indexadas en **index-concentrator.xml** en el Concentrator. En el tema Editar un archivo de índice de servicios de la *Guía de configuración de hosts y servicios* se proporciona información adicional.

Definir una plantilla personalizada del registro de auditoría global

Para los servidores de syslog de otros fabricantes, puede definir un formato de plantilla propio (CEF o no CEF). Puede usar la plantilla **Default Audit Human-Readable Format** para enviar los registros de auditoría global a un servidor de syslog de otros fabricantes en un formato que es más fácil de leer que el formato CEF. Si desea definir una plantilla propia en lenguaje natural, siga este procedimiento.

Para Log Decoders, debe usar una plantilla de CEF con algunos requisitos específicos. En el procedimiento anterior *Definir una plantilla del registro de auditoría para un Log Decoder* se proporcionan instrucciones para crear una plantilla en el formato CEF.

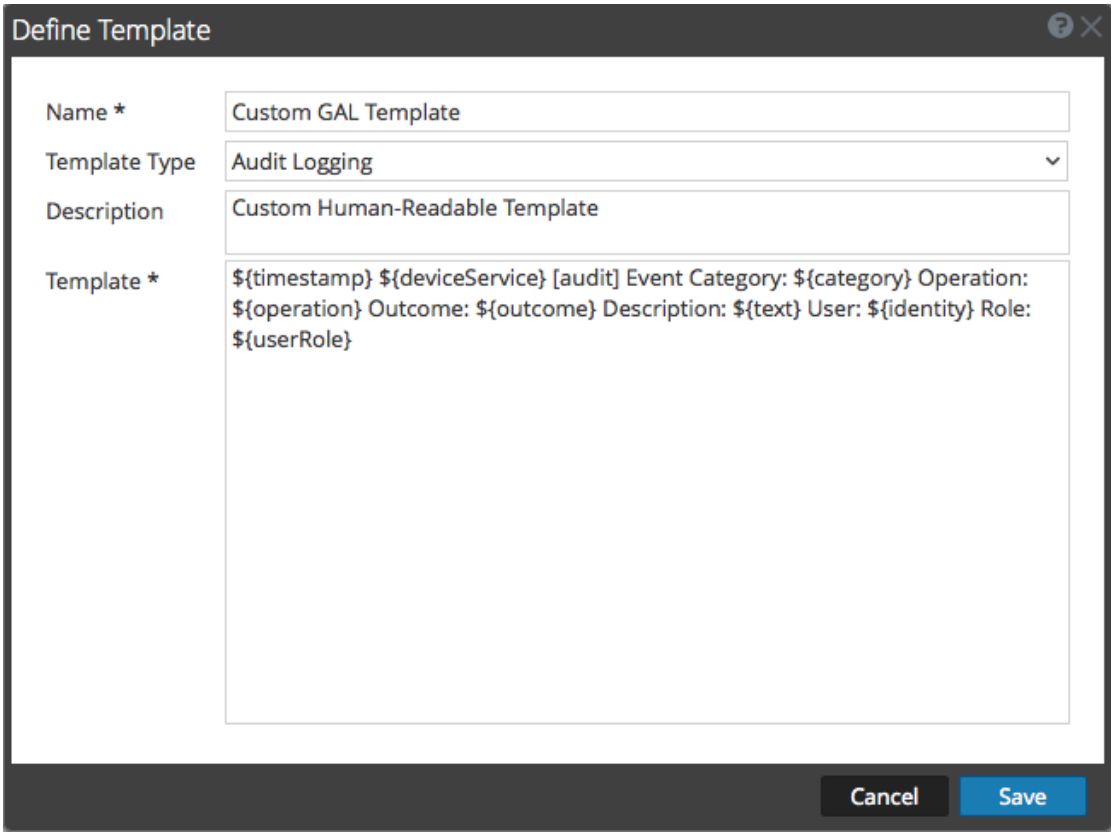
Para definir una plantilla personalizada del registro de auditoría global en el formato en lenguaje natural:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de navegación izquierdo, seleccione **Notificaciones**.
3. Haga clic en la pestaña **Plantillas**.
4. Haga clic en  para configurar una plantilla.
5. En el cuadro de diálogo **Definir plantilla**, proporcione la siguiente información:
   a. En el campo **Nombre**, escriba el nombre para la plantilla.
   b. En el campo **Tipo de plantilla**, seleccione el tipo de plantilla **Registro de auditoría**.
   c. En el campo **Descripción**, escriba una descripción breve para la plantilla.
   d. En el campo **Plantilla**, ingrese el formato de la plantilla del registro de auditoría. En el siguiente ejemplo se muestra el formato en lenguaje natural con variables de claves de metadatos seleccionadas.

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
Operation: ${operation} Outcome: ${outcome} Description: ${text}
User: ${identity} Role: ${userRole}
```

Puede usar cualquiera de las variables de claves de metadatos compatibles con el registro de auditoría global que se muestran en la tabla Variables de claves de metadatos del registro de auditoría global compatibles.

6. Haga clic en **Guardar**.



En el siguiente ejemplo se muestran registros de auditoría global en el formato en lenguaje natural para esta plantilla:

```
06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 NW_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

Paso siguiente

En Definir una configuración del registro de auditoría global se proporcionan instrucciones para definir una configuración del registro de auditoría global para NetWitness Suite.

Definir una configuración del registro de auditoría global

En este tema se indica a los administradores cómo definir una configuración del registro de auditoría global. Este procedimiento solo se requiere si opta por configurar el registro de auditoría centralizado en el ambiente. Estas configuraciones del registro de auditoría global definen cómo se reenvían los registros de auditoría global a sistemas de syslog externos o a Log Decoders. Los registros de auditoría se reenvían a los servidores de notificación seleccionados.

Requisitos previos

Antes de dar inicio a este procedimiento, configure lo siguiente para usar el registro de auditoría global:

- Servidor de notificación de syslog
- Plantilla del registro de auditoría

El servidor y la plantilla de notificación se configuran en el panel Notificaciones globales. Para acceder al panel Notificaciones globales, haga clic en el vínculo **ver configuración** del panel Configuraciones de registro de auditoría global. Solo puede definir un tipo de syslog de Servidor de notificación para el registro de auditoría global. Para Log Decoders, use un tipo de servidor de notificación de syslog y una plantilla del registro de auditoría de formato de evento común (CEF). Es posible usar una plantilla del registro de auditoría predeterminada o definir una plantilla propia. Puede crear varias plantillas del registro de auditoría y servidores de notificación de syslog para su uso en configuraciones del registro de auditoría global.

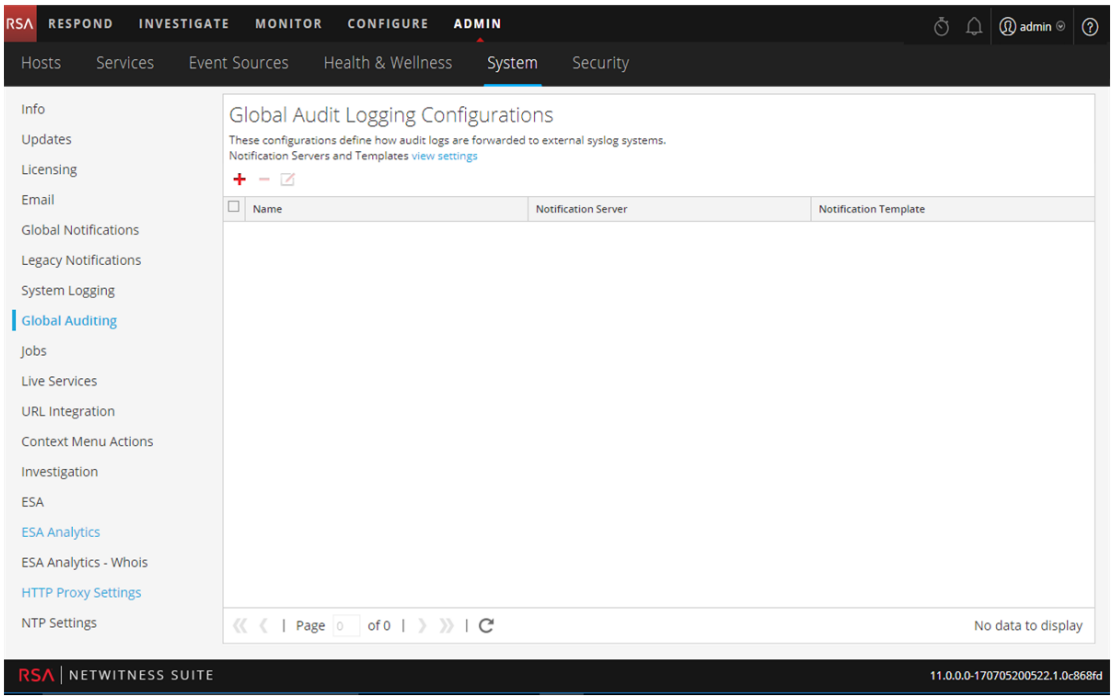
Si desea reenviar registros de auditoría global a un Log Decoder, implemente el analizador del formato de evento común en el Log Decoder desde Live.

Agregar una configuración del registro de auditoría global

1. Vaya a **ADMIN > Sistema**.

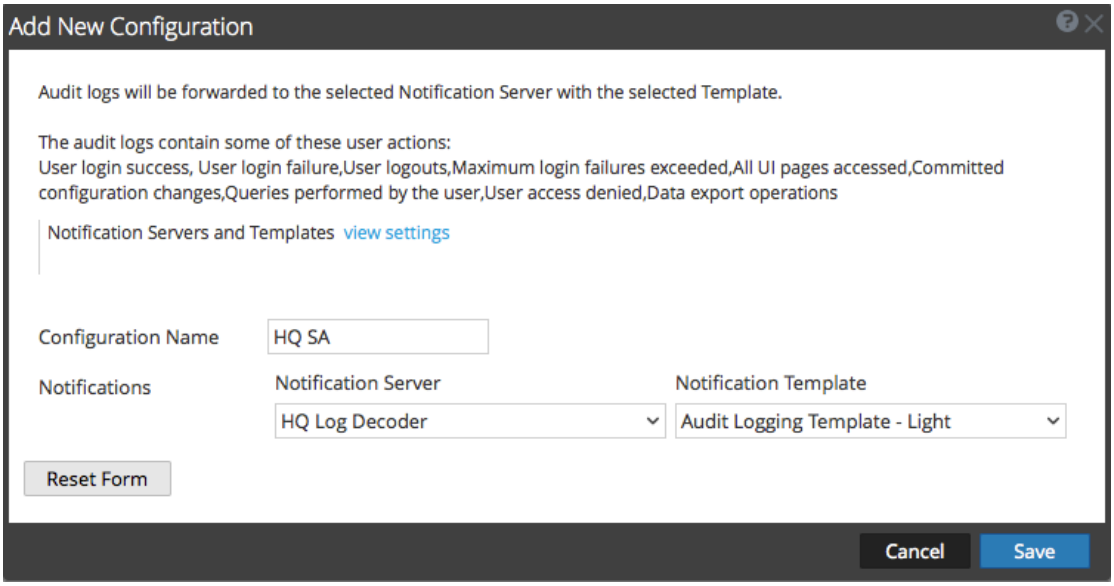
2. En el panel de opciones, seleccione **Auditoría global**.

   Se muestra el panel **Configuraciones de registro de auditoría global**.



3. Haga clic en + para agregar una configuración del registro de auditoría global.

   Se muestra el cuadro de diálogo **Agregar nueva configuración**.



4. En el campo **Nombre de configuración**, escriba un nombre único para la configuración del registro de auditoría global. Por ejemplo, puede crear una configuración para un tipo

específico de configuración del registro de auditoría global, como HQ NW para una configuración de sede central de NetWitness Suite.

5. En la sección **Notificaciones**, seleccione el **Servidor de notificación** de syslog que se usará para esta configuración. El servidor de notificación es el destino al cual se enviarán los registros de auditoría global.
6. Seleccione la **Plantilla de notificación** del registro de auditoría que se usará para esta configuración. La plantilla del registro de auditoría define el formato y los campos de mensajes del registro de auditoría que se enviarán.
7. Haga clic en **Guardar**.

En Cuadro de diálogo Agregar nueva configuración se proporciona información adicional y ejemplos de las acciones de los usuarios que se registran. Para obtener una lista de los tipos de mensajes que registran los diversos componentes de NetWitness Suite, consulte Panel Configuraciones de registro de auditoría global.

Editar una configuración del registro de auditoría global

En este tema se proporcionan instrucciones para editar una configuración del registro de auditoría global. Puede editar una configuración del registro de auditoría global para cambiar el destino de los registros de auditoría global de sus auditorías a los usuarios mediante la selección de otro servidor de notificación. También puede cambiar el formato y los campos de mensaje de las entradas del registro de auditoría global mediante la selección de una plantilla de notificación diferente. Los cambios al servidor de notificación o a la plantilla de notificación se hacen en el panel Notificaciones globales. Para acceder al panel Notificaciones globales, haga clic en el vínculo **ver configuración** del panel Configuraciones de registro de auditoría global.

No puede cambiar las acciones de los usuarios de NetWitness Suite que se registran y se envían en los registros de auditoría global.

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Auditoría global**.
3. En el panel **Configuraciones de registro de auditoría global**, seleccione una configuración que desee editar y haga clic en  .
4. En el cuadro de diálogo **Agregar nueva configuración**, modifique la configuración del registro de auditoría global según sea necesario. Puede modificar el **Nombre de configuración** y seleccionar otro **Servidor de notificación** u otra **Plantilla**.
5. Haga clic en **Guardar.**

Eliminar una configuración del registro de auditoría global

La eliminación de una configuración de auditoría global no elimina el servidor ni la plantilla de notificación asociados. Después que se elimina una configuración del registro de auditoría global, se interrumpe el reenvío de registros de auditoría global especificados en esa configuración.

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Auditoría global**.
3. En el panel **Configuraciones de registro de auditoría global**, seleccione una configuración que desee eliminar y haga clic en .

   Se muestra un cuadro de diálogo de confirmación.
4. Haga clic en **Sí**.

   La configuración seleccionada se elimina.

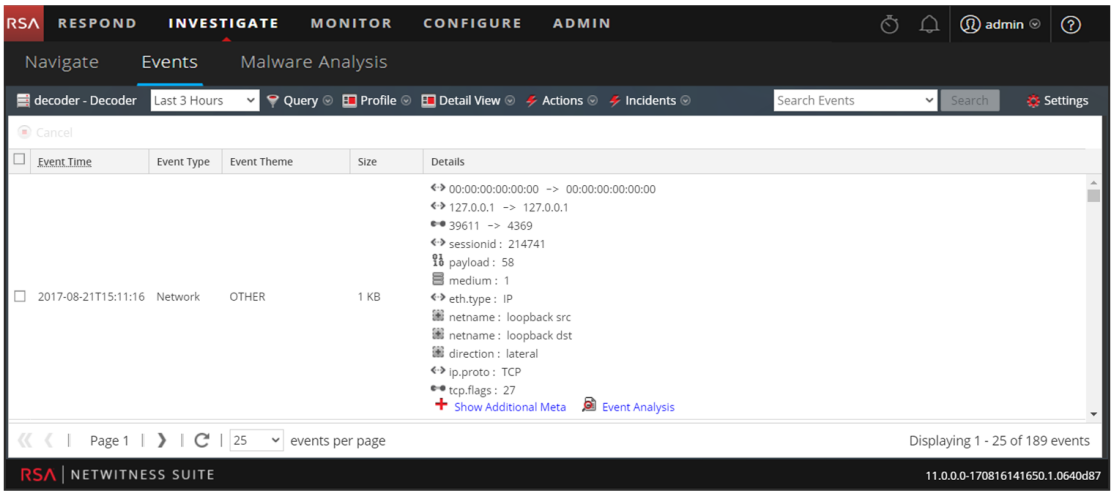
Verificar registros de auditoría global

En este tema se proporcionan instrucciones para verificar registros de auditoría global. Después de configurar el registro de auditoría global, debe probar los registros de auditoría global para asegurarse de que muestren los eventos de auditoría definidos en la plantilla del registro de auditoría global.

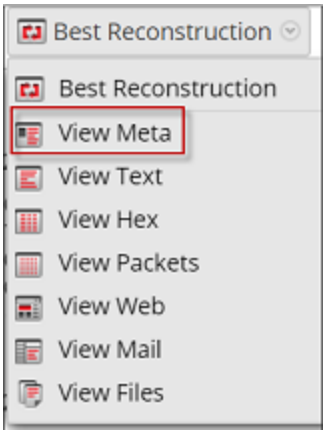
Antes de iniciar esta tarea, complete los pasos que se detallan en Configurar el registro de auditoría global.

Para ver y verificar los registros de auditoría global si está usando un Log Decoder:

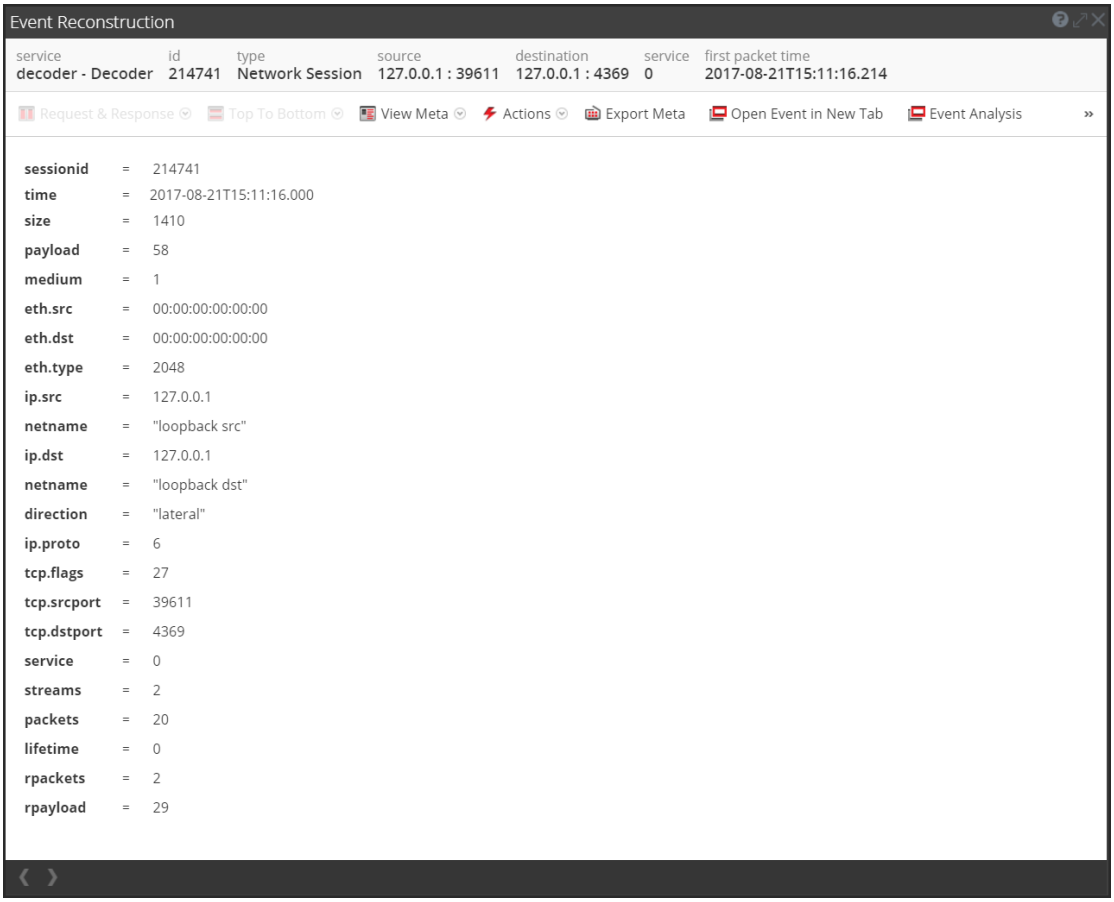
1. Vaya a **Investigar > Eventos**.
2. En la vista Navegar, seleccione el Log Decoder y haga clic en **Navegar**.



3. Compare los campos de los registros de auditoría global con los campos definidos en la plantilla del registro de auditoría global que usó en la configuración del registro de auditoría global.
4. Haga doble clic en un registro y, en el cuadro de diálogo Reconstrucción de evento, seleccione **Ver metadatos**.



5. Verifique que los metadatos que desea auditar estén correctos.



Ejemplo de salida de CEF

En el siguiente ejemplo se muestran registros de auditoría global para una plantilla del formato de evento común (CEF) del registro de auditoría.

Plantilla:

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}|${oper
ation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome} msg=${text}
```

Ejemplo de registros:

```
2017-04-09T18:45:46.313096+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|login|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=51366 suser=admin sourceServiceName=LOG_DECODER
deviceExternalId=96b08193-a9d0-4a79-b362-87b56851f411 outcome=success
2017-04-09T18:45:46.322132+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.204.33 spt=47690 suser=admin sourceServiceName=BROKER
deviceExternalId= 314fb8c8-afe4-4249-9468-a36035008a52 outcome=success
2017-04-09T18:45:46.325792+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=59495 suser=admin sourceServiceName=CONCENTRATOR
deviceExternalId= 96b08193-a9d0-4a79-b362-87b56851f411 outcome=success
```

Donde `<hostname>` es el nombre de host del encabezado de syslog (alias.host).

Para las plantillas de CEF, si un evento de auditoría no tiene un valor para un campo en la plantilla, el campo se eliminará del evento correspondiente que llega al servidor de syslog de otros fabricantes o al Log Decoder.

Ejemplo de salida en formato en lenguaje natural

En el siguiente ejemplo se muestran registros de auditoría global para una plantilla en el formato en lenguaje natural del registro de auditoría en un servidor de syslog de otros fabricantes.

Plantilla:

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
```

Operation: ${operation} Outcome: ${outcome} Description: ${text}

User: ${identity} Role: ${userRole}

Ejemplo de registros:

```
06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2017 14:16:04 SA_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

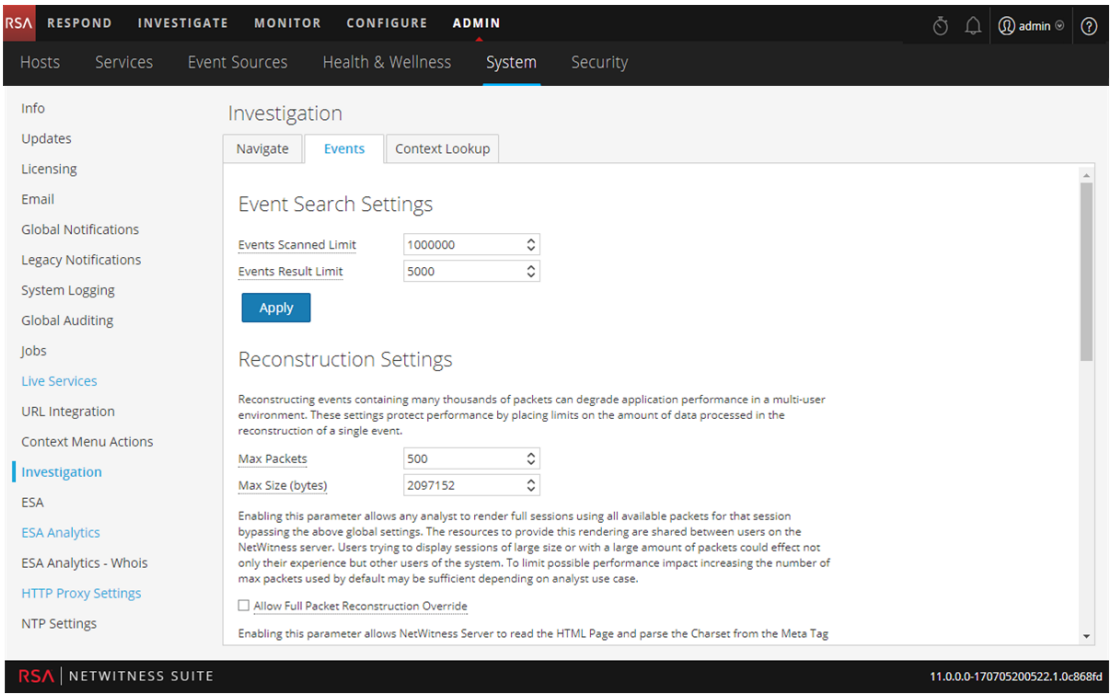
Configurar los ajustes de Investigation

En este tema se proporcionan instrucciones para los administradores que están configurando los ajustes que se aplican a todas las investigaciones en la instancia de NetWitness Suite que se configura. Los ajustes para configurar y ajustar el comportamiento de NetWitness Suite Investigation están disponibles en la vista Sistema > panel Investigation. Estos ajustes se aplican a todas las investigaciones y las reconstrucciones en la instancia actual de NetWitness Suite.

Configurar los ajustes de las pestañas Navegar, Eventos y Búsqueda de contexto

1. Vaya a **ADMIN > Sistema.**
2. En el panel de opciones, seleccione **Investigation.**

   Se muestra el panel Configuración de Investigation.



3. En el campo **Configuración de hilos de ejecución de representación** de la pestaña **Navegar**, seleccione la cantidad máxima de valores de claves de metadatos simultáneos que carga un único usuario en la vista Navegar. Haga clic en **Aplicar**.
4. En la sección **Configuración de coordenadas paralelas** de la pestaña **Navegar**, configure los límites máximos para los valores de metadatos escaneados y los resultados de valores de metadatos que se pueden incluir en una visualización de coordenadas paralelas. Para mejorar el rendimiento, esta es la configuración recomendada: Límite de escaneo de valores de metadatos: 100,000 y Límite de resultados de valores de metadatos: entre 1,000 y 10,000 Haga clic en **Aplicar**.
5. En la sección **Configuración de búsqueda de eventos** de la pestaña **Eventos**, configure la cantidad máxima de eventos escaneados y de resultados de eventos que se muestran cuando un analista realiza una búsqueda de eventos en la vista Eventos. Haga clic en **Aplicar**.
6. En la sección **Configuración de la reconstrucción** de la pestaña **Eventos**, configure los límites para la cantidad de datos que se procesan en la reconstrucción de un único evento. Los valores predeterminados son un máximo de 100 paquetes y 2,097,152 de bytes. Si los analistas perciben un bajo rendimiento cuando reconstruyen sesiones en Investigation, la configuración de la reconstrucción puede requerir ajustes. Haga clic en **Aplicar**.

Precaución: La configuración de un valor más alto afecta el rendimiento del Servidor de NetWitness, ya que aumenta el tiempo y la memoria necesarios para crear la reconstrucción de un evento. La configuración del valor en cero deshabilita los límites y puede hacer que un Servidor de NetWitness falle.

7. (Opcional) En la pestaña **Eventos** de la sección **Configuración de reconstrucción de vista web**, habilite el uso de archivos de soporte en una reconstrucción de vistas web y configure ajustes adicionales para calibrar estas reconstrucciones. Estos incluyen el rango de tiempo (en segundos) para escanear en busca de eventos relacionados, la cantidad máxima de eventos relacionados que se escanearán y reemplazos a la configuración de la reconstrucción que se usarán con reconstrucciones de vistas web. Haga clic en **Aplicar**.
8. En la pestaña **Búsqueda de contexto**, administre el mapeo de tipos de metadatos de Context Hub con claves de metadatos en Investigation. Puede agregar o quitar claves de metadatos en la lista de tipos de metadatos compatibles en Investigation mediante Context Hub. Los procedimientos asociados con esta pestaña se proporcionan en "Administrar mapeo de tipos de metadatos y claves de metadatos" en la *Guía de Investigation y Malware Analysis*.

Limpiar la caché de reconstrucción para los servicios

La opción Configuración de caché de reconstrucción permite a los administradores limpiar la caché de uno o más servicios. Por ejemplo, el administrador puede limpiar la caché de un único Broker, un Broker y un Decoder o de todos los servicios conectados. Estos son algunos ejemplos de causas del uso de una caché obsoleta en una reconstrucción.

- Las sesiones de los servicios downstream pueden haber perdido su validez o pueden haberse restablecido sus datos. Como ejemplo, si Investigation navega en un Broker y se produce un restablecimiento de datos en un Concentrator o un Decoder descendentes, los metadatos y los datos de sesión del servicio que realiza la investigación (Broker) no coinciden con el contenido si el servicio descendente se restableció y se volvió a completar. La reconstrucción en Investigation muestra contenido de la caché, el cual no coincide con el contenido real. Incluso si el Decoder está offline, el contenido continúa mostrándose en la reconstrucción del Broker. La limpieza de la caché en el Broker hace que NetWitness Suite acceda al Decoder y que se muestre un error debido a que el Decoder está offline.
- Otro caso en el cual la caché puede estar obsoleta es cuando cambia un ID de servicio para un servicio descendente. Esto puede suceder cuando se exportan, se importan, se eliminan y se agregan servicios a NetWitness Suite, debido a que NetWitness Suite puede reutilizar los ID de servicio. En este caso, la limpieza de la caché en el Broker hace que NetWitness Suite solicite datos de los servicios.

Para borrar la caché de reconstrucción, realice una de las siguientes acciones:

1. Para borrar la caché de uno o más servicios, seleccione los servicios y haga clic en **Borrar caché de los servicios seleccionados**.
2. Para borrar la caché de todos los servicios enumerados, haga clic en **Borrar caché de todos los servicios**
   . Se borra la caché de reconstrucción para los servicios seleccionados. NetWitness Suite envía una solicitud de datos a los servicios.

Configurar los ajustes de servicios de Live

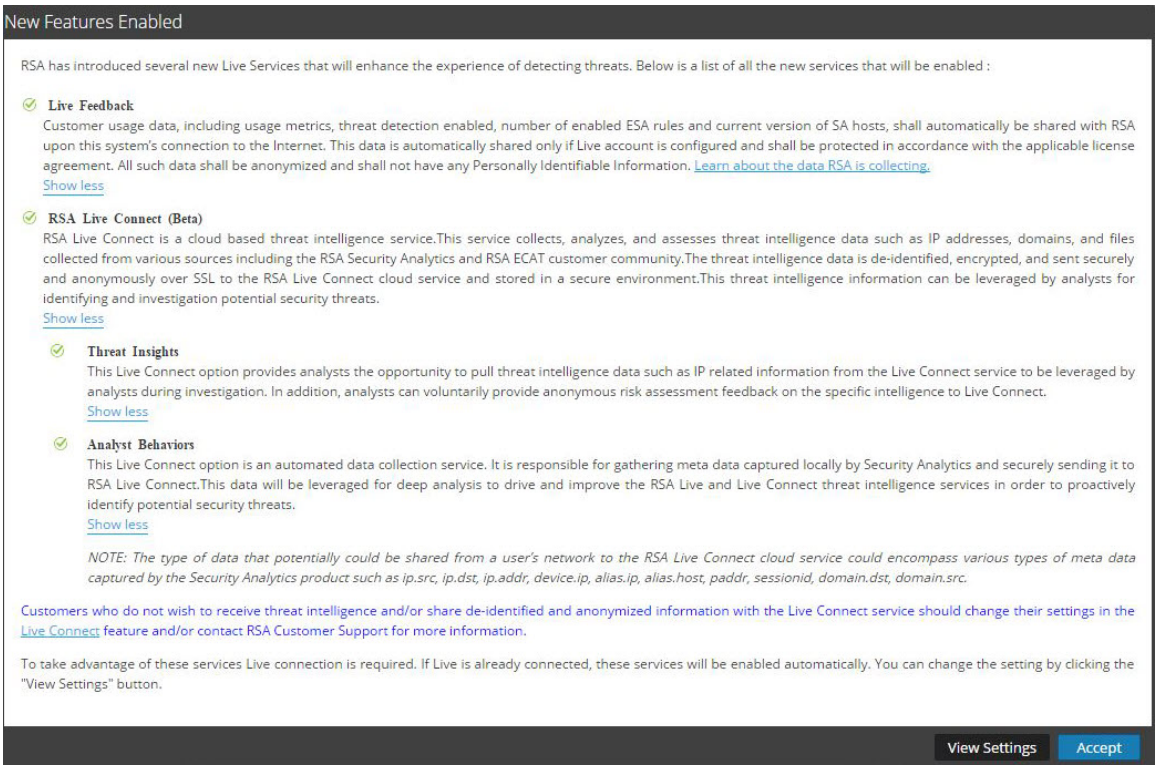
Las opciones para configurar los servicios de Live están en la vista Sistema > panel Configuración de servicios de Live. El panel Configuración de Live permite que configure:

- La cuenta de Live.
- El calendario y las preferencias de actualización del contenido de Live para la notificación de actualizaciones.
- Participación en Servicios de Live Feedback.
- Uso compartido del contenido de Live
- RSA Live Connect (beta)

Requisito previo

Para activar su cuenta de Live para NetWitness Suite, comuníquese con Atención al cliente de RSA. Cuando se confirma la configuración de su cuenta de Live, puede configurar y probar la conexión del servidor de CMS.

Cuando inicia sesión en NetWitness Suite por primera vez, aparece el cuadro de diálogo **Nuevas funciones habilitadas**.



Cuando hace clic en **Aceptar**, acepta automáticamente lo siguiente:

- Participar en Live Feedback.
- Usar las funciones de Live Connect para recibir datos de inteligencia de amenazas.
- Permitir que NetWitness Suite envíe datos anónimos, técnicos sobre su ambiente a RSA.

Si hace clic en **Ver configuración**, se le redirige a la interfaz del usuario de los servicios de Live para ver la configuración de Live Feedback y Live Connect Threat Data Sharing. Si no configuró la cuenta de Live, se muestra una pantalla enmascarada.

Para obtener información sobre comportamientos de analistas y uso compartido de datos, consulte **Comentarios y uso compartido de datos de NetWitness Suite** en la *Guía de administración de servicios de Live*.

Acerca de la participación en Live Feedback

Cuando participa en Live Feedback, se recopila información pertinente que permite mejoras. Para obtener información sobre Live Feedback, consulte Descripción general de Live Feedback.

Cuando instale NetWitness Suite, se le preguntará si desea participar en Live Feedback. Para obtener información, consulte Configurar los ajustes de servicios de Live

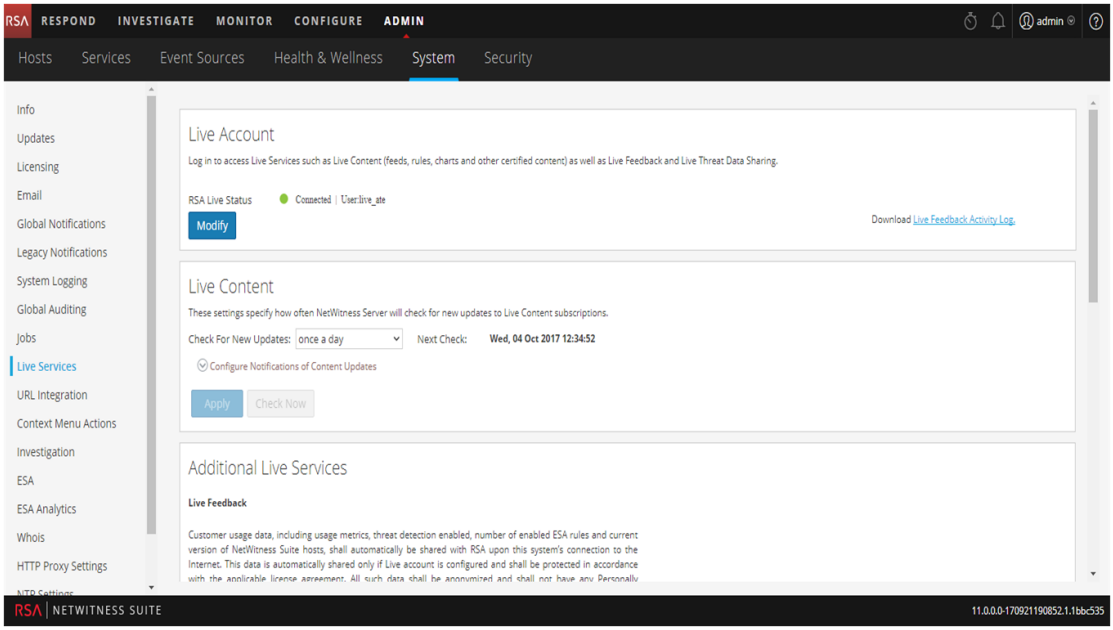
Si es necesario, puede descargar manualmente los datos de uso histórico y compartirlos con RSA. Para obtener información sobre cómo descargar los datos de uso histórico y compartirlos con RSA, consulte Cargar datos en RSA para Live Feedback.

Este tema contiene los siguientes procedimientos:

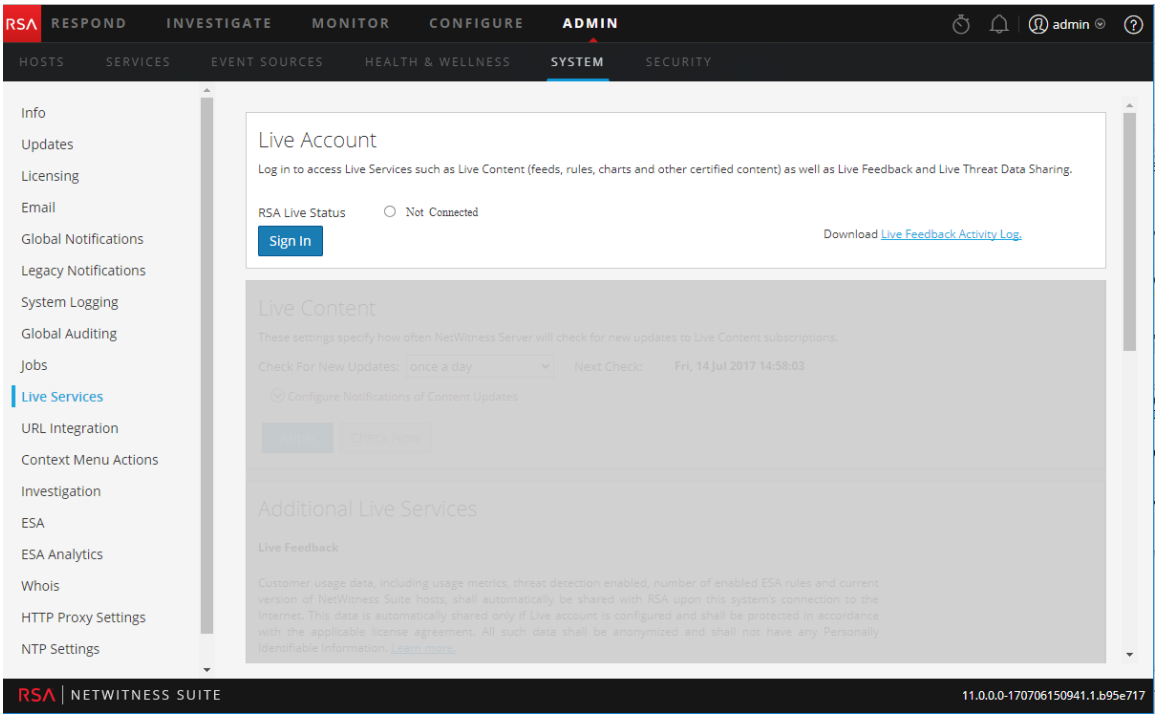
- Acceder al panel Configuración de servicios de Live
- Configurar cuenta de Live
- Configurar el intervalo y la notificación de sincronización de contenido de Live
- Forzar sincronización inmediata
- Uso de RSA Live Connect (beta)

Acceder al panel Configuración de servicios de Live

1. Vaya a **ADMIN > SISTEMA**.
2. En el panel de navegación izquierdo, seleccione **Servicios de Live**.



Nota: Si no inició sesión con sus credenciales de cuenta de Live, se muestra una pantalla enmascarada.



Configurar cuenta de Live

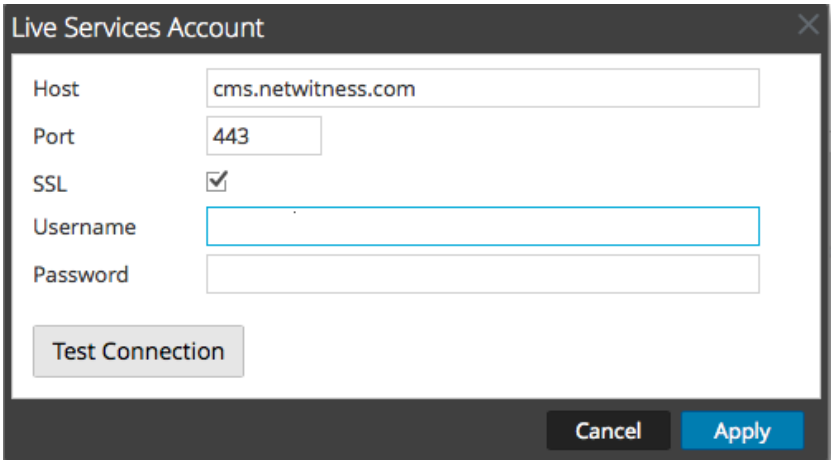
En la sección **Cuenta de Live**, debe establecer la cuenta de Live del usuario. La información que se necesita para configurar la cuenta de Live del usuario consta del nombre de usuario, la contraseña y la URL de Live para el sistema de administración de contenido. Esta información la proporciona Atención al cliente.

Para configurar una cuenta de Live:

1. En la sección **Cuenta de Live**, haga clic en **Iniciar sesión**.

   Nota: El botón **Modificar** muestra que la cuenta de live está configurada. Haga clic en **Modificar** para cambiar el usuario que tiene acceso a los servicios de Live.

2. En el cuadro de diálogo Cuenta de servicios de Live, ingrese el host (por lo general **cms.netwitness.com**) y escriba su nombre de usuario y contraseña.

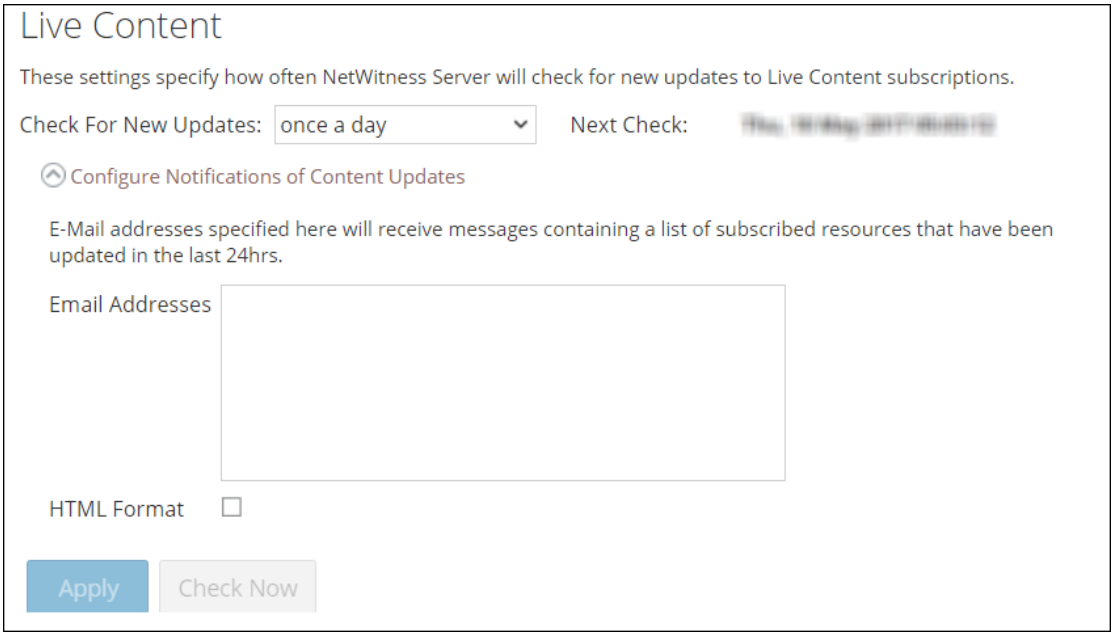


3. (Opcional) Si está utilizando un CMS diferente, ingrese la URL de host del sistema de administración de contenido. El valor predeterminado apunta al CMS en **cms.netwitness.com**.
4. (Opcional) Si está utilizando un CMS diferente, ingrese el puerto de comunicaciones para que Live envíe solicitudes al sistema de administración de contenido. El valor determinado para este campo es **443**, el cual es el puerto de comunicaciones del sistema de administración de contenido.
5. (Opcional) Si no desea utilizar SSL, deseleccione la opción **SSL**. (SSL se encuentra activado de forma predeterminada.)
6. Haga clic en **Probar conexión** para probar la conexión a CMS.
7. Para guardar y aplicar la configuración, haga clic en **Aplicar**.

Configurar el intervalo y la notificación de sincronización de contenido de Live

Puede cambiar el intervalo en el que NetWitness Suite busca nuevas actualizaciones para el contenido de Live:

1. Utilice el campo **Comprobar si hay nuevas actualizaciones** para cambiar el intervalo. Seleccione un intervalo de la lista desplegable. El valor predeterminado para este ajuste es **una vez por día**.



2. Para configurar Servicios de Live de modo que envíe informes de actualización a una o más personas, en el campo **Direcciones de correo electrónico**, ingrese las direcciones de correo electrónico como una lista separada por comas; por ejemplo, **john@company.com,ted@company.com,brian@company.com**
3. (Opcional) Para recibir mensajes en formato HTML en lugar de texto plano, seleccione **Formato HTML**.
4. Para guardar y aplicar, haga clic en **Aplicar**.

   Se muestra la hora y la fecha de la próxima sincronización de Live calendarizada en función del intervalo configurado para la comprobación.

Forzar sincronización inmediata

En lugar de esperar el próximo ciclo de recursos programados, esta opción obliga a Live a comenzar la sincronización inmediata de los recursos suscritos en esta instancia de NetWitness Suite. Un uso para esto es ver el impacto inmediato de un cambio de configuración. Por ejemplo, se agregó un nuevo servicio, o se han alternado nuevos recursos para una implementación automática. La sincronización programada podría realizarse horas más tarde si Servicios de Live está configurado para sincronizarse varias veces al día.

Precaución: la sincronización puede hacer que se vuelva a cargar un analizador si se implementa un FlexParser en el ciclo de actualización. Esto es aceptable una o dos veces al día, pero una cantidad de recargas de analizadores consecutivas puede provocar la pérdida de paquetes en el Decoder. Si esta es la configuración inicial y no ha configurado las suscripciones a recursos de Live, no realice la sincronización. Espere hasta que haya configurado las suscripciones.

Para forzar la sincronización inmediata, haga clic en **Comprobar ahora**. NetWitness Suite busca actualizaciones en los recursos suscritos.

Uso de RSA Live Connect (beta)

RSA Live Connect es un servicio de inteligencia de amenazas basado en la nube. Este servicio recopila, analiza y evalúa datos de inteligencia de amenazas, como direcciones IP, dominios y archivos recopilados desde diversos orígenes, incluida la comunidad de clientes de RSA NetWitness® Suite y RSA NetWitness® Endpoint. RSA Live Connect consta de las siguientes funciones:

- Información valiosa de amenazas
- Comportamientos de analistas

Información valiosa de amenazas

Proporciona a los analistas la oportunidad de extraer datos de inteligencia de amenazas, como información relacionada con direcciones IP, desde el servicio Live Connect para que los analistas los aprovechen durante una investigación.

De manera predeterminada, **Información valiosa de amenazas** está habilitada en la sección **Servicios adicionales de Live**. Si se configura el servicio Context Hub, Live Connect se agrega automáticamente como un origen de datos para Context Hub. Para obtener más información, consulte el tema **Configurar un origen de datos de Live Connect para Context Hub** en la *Guía de configuración de Context Hub*.

Con Live Connect como un origen de datos de Context Hub, puede usar la opción Búsqueda de contexto en Investigation > vista Navegar o en Investigation > vista Eventos para obtener información contextual. Para obtener instrucciones, consulte el tema **Ver el contexto adicional de un punto de datos** de la *Guía de Investigation y Malware Analysis*.

Comportamientos de analistas

Comportamientos de analistas es una función en la cual los analistas participan en el uso compartido de datos con la comunidad de RSA. Este es un servicio de recopilación de datos automatizada. Su objetivo es compartir datos de inteligencia de amenazas potenciales en el servicio de nube de RSA Live Connect con fines de análisis. El tipo de datos que se podría compartir desde la red con RSA Live Connect incluye diversos tipos de metadatos que captura NetWitness Suite, como ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst y domain.src. Para obtener información sobre comportamientos de analistas y uso compartido de datos, consulte **Comentarios y uso compartido de datos de NetWitness Suite** en la *Guía de administración de servicios de Live*.

Descripción general de Live Feedback

En este tema se proporciona una introducción a Live Feedback. Live Feedback recopila información pertinente, como los datos de uso de licencias de Packet Decoder, Log Decoder y Malware Analysis, el estado Habilitado o Deshabilitado de la detección de amenazas, la cantidad de reglas de ESA habilitadas y detalles del número de versión de todos los servicios de NetWitness Suite. Para obtener más información acerca de los datos de uso de licencias de Packet Decoder, Log Decoder y Malware Analysis, consulte el tema **Pestaña Licencias medidas** de la *Guía de licencia*. La información se recopila para mejorar las versiones futuras de NetWitness Suite. Quedará inscrito automáticamente en Live Feedback y no podrá deshabilitar esta opción.

Además de esto, también se puede compartir con RSA información sobre el uso de Live Content. Puede compartir con RSA las métricas de uso de Live Content correspondientes a los tipos de recursos de **CONFIGURAR > LIVE CONTENT > Criterios de búsqueda**, como el conteo total de reglas de aplicación de RSA, la regla de correlación de RSA, etc. La información recopilada sirve para mejorar el uso de Live Content. Para obtener más información acerca del uso compartido de la configuración de Live Content, consulte Panel Configuración de servicios de Live.

Acerca de la participación en Live Feedback

Cuando participa en Live Feedback, se recopila información pertinente que permite mejoras. Para obtener información sobre Live Feedback, consulte Descripción general de Live Feedback.

Cuando instale NetWitness Suite, se le preguntará si desea participar en Live Feedback. Para obtener información, consulte Configurar los ajustes de servicios de Live

Si es necesario, puede descargar manualmente los datos de uso histórico y compartirlos con RSA. Para obtener información sobre cómo descargar los datos de uso histórico y compartirlos con RSA, consulte Cargar datos en RSA para Live Feedback.

Nota: Live Feedback se activa solo si configuró su cuenta de Live.

Los datos de Live Feedback están en formato JSON como se indica a continuación. Cuando se inscribe con sus credenciales de cuenta de Live, se carga automáticamente un solo archivo JSON cifrado en los servidores de RSA todos los días.

Archivo JSON

El archivo JSON consta de información de datos de uso para un componente o un conjunto de componentes. En el caso de un conjunto de componentes con el mismo ID de licencia, los datos de uso de todos los componentes se agregan y se representan como un componente denominado Entitlement. Sin embargo, incluso si hay un único componente, como un Log Decoder o un Decoder, se generará un componente Entitlement y se mostrarán los datos de uso de un único componente. Esta agregación es para componentes específicos, como Log Decoders, Decoders o Malware Analysis.

Nota: La versión de Entitlement es siempre nula, ya que es el agregado de datos de una licencia.

Por ejemplo, si hay tres Decoders con el mismo ID de licencia “xxx” y los siguientes datos de uso:
Decoder1 = 150 MB
Decoder2 = 250 MB
Decoder3 = 100 MB
Se muestran los datos de uso agregados de 500 MB.

Este archivo JSON se describe en las siguientes secciones:

- Componentes
- Métricas
- Otros detalles del producto
- Ejemplo

Componentes

Detalles de cada servicio en la implementación de NetWitness Suite. Esto se representa como Componente. Para cada componente, se muestran los siguientes detalles.

Componente	Descripción
Versión	Número de versión del componente en la implementación de NetWitness Suite. Por ejemplo, 11.0.0.0.x.x.x.x.
ID	Este es el ID de componente único que representa el host y se utiliza para establecer un vínculo a las métricas que se generan.
Propiedades	• **Name**: Este es el nombre de la propiedad para ese componente. Por ejemplo, malware analysis, ESA, log decoder, etc. • **Value**: Este es el valor único para identificar el componente.

Métricas

Métricas de los componentes (hosts), como log decoder, decoder y malware analysis. Se comparten datos de uso de licencia para cada host. Para las métricas de uso de Live Content, se comparten los tipos de recursos de **Live > Buscar**, como el conteo total de reglas de aplicación de RSA, la regla de correlación de RSA, etc.

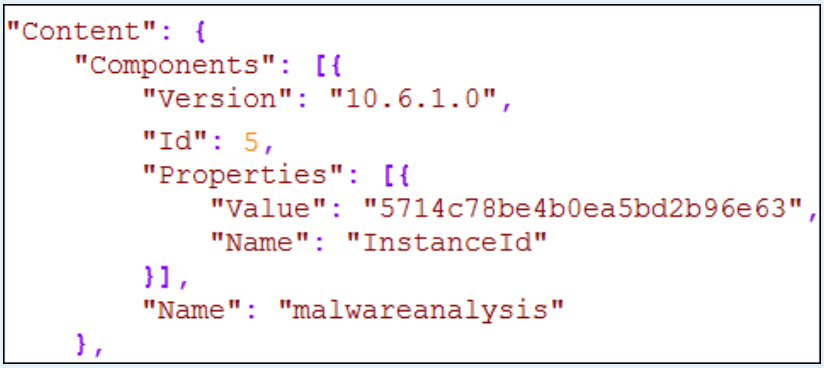
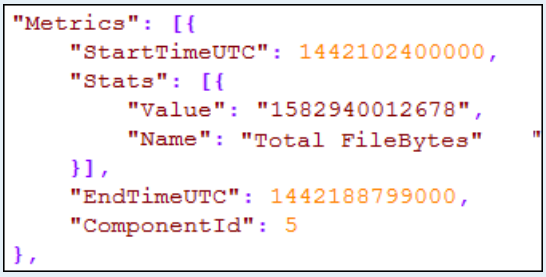
Componente	Descripción
StartTimeUTC	Esta es la hora desde la cual se recopilan métricas (en formato EPOCH).
Estadísticas	• **Value**: Este es el valor generado para el ID de componente específico de cada componente. • **Name**: Este es el nombre de las estadísticas para las cuales se recopilan las métricas. Por ejemplo, Capture Total Bytes.
EndTimeUTC	Esta es la hora en que se completa la recopilación de métricas (en formato EPOCH).
Component ID	Este es el ID del componente para el cual se registra el valor.

Otros detalles del producto

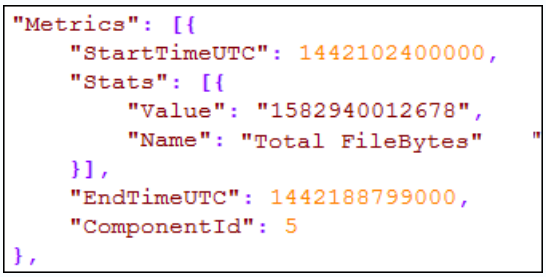
- **Product Type**: Este es el nombre del producto. En este ejemplo, el tipo de producto es NetWitness Suite.
- **Version**: Esta es la versión del archivo JSON que rastrea los cambios realizados en el formato del archivo.
- **Product Instance**: Este es el ID del servidor de licencia.
- **Checksum**: Esta es la información que se utiliza para las comprobaciones de integridad.

En la siguiente tabla se describen detalles del archivo JSON con ejemplos.

Métricas	Descripción
Contenido	Muestra contenido que incluye todos los componentes, las métricas, el tipo de producto y los datos de instancia del producto, salvo la suma de comprobación.

Métricas	Descripción
Componentes	Los detalles de todos los servicios en NetWitness Suite se representan como un componente. Los detalles del componente, como el número de versión, el nombre y el valor, se muestran de la siguiente manera:  **Versión**: Muestra la versión del servicio NetWitness Suite. Por ejemplo, 11.0.0.0. **ID**: Muestra un ID único que se genera para el servicio de NetWitness Suite y que se utiliza para establecer un vínculo a las métricas de ese componente específico. En este ejemplo, el ID de Malware Analysis es 5 y las métricas se muestran para ComponentId 5 en bytes, como puede ver a continuación:  **Propiedades**: Muestra las propiedades del componente, como el nombre y el valor, que se aprecian en la figura anterior. **Valor**: Muestra el valor de la propiedad que es un UUID interno para un componente, como se aprecia en la figura anterior. Esto lo genera NetWitness Suite. Por ejemplo, para Malware Analysis, el valor se muestra como `"55f7a0b30e502231c42d063f"`. **Nombre: "InstanceId"**: Muestra el nombre de la propiedad, como se aprecia en la figura anterior.

Métricas	Descripción
	Name: “malwareanalysis”: Muestra el nombre del componente que es un nombre de servicio, como LogDecoder, Decoder o MalwareAnalysis.

Métricas	Muestra la lista de las métricas con los datos de uso de componentes, como log decoder, decoder y malware analysis.
	En este ejemplo, las métricas se muestran para ComponentId 5 en bytes, como se aprecia a continuación.
	 
	"Metrics": [{
	"StartTimeUTC": 1442102400000,
	"Stats": [{
	"Value": "1582940012678",
	"Name": "Total FileBytes"
	}],
	"EndTimeUTC": 1442188799000,
	"ComponentId": 5
	},

	StartTimeUTC: Muestra la hora en que se recopilan métricas, en formato EPOCH.
	Stats: Muestra las estadísticas de valor de uso y tipo de uso del componente.
	Valor: Muestra el valor de las estadísticas. Por ejemplo, “Value”: “1582940012678”, como se muestra en la figura anterior.
	Nombre: Muestra el nombre de la estadística. Por ejemplo, Capture Total Bytes o Total File bytes.
	EndTimeUTC: Muestra la hora en que se completa la recopilación de métricas, en formato EPOCH.
	ComponentId: Muestra el ID de componente para el cual se recopilan valores de métricas. Es el mismo que el “ID” de la sección Components.
Contenido	Muestra contenido que incluye todos los componentes, las métricas, el tipo de producto y los datos de instancia del producto, salvo la suma de comprobación.

Métricas	Descripción
Componentes	Los detalles de todos los servicios en NetWitness Suite se representan como un componente. Los detalles del componente, como el número de versión, el nombre y el valor, se muestran de la siguiente manera:


```
"Content": {
    "Components": [{
        "Version": "10.6.2.0",
        "Id": 6,
        "Properties": [{
            "Value": "57444ddde4b0dd618093064d",
            "Name": "InstanceId"
        }],
        "Name": "reportingengine"
    },
```


Versión: Muestra la versión del servicio NetWitness Suite. Por ejemplo, 11.0.0.0

ID: Muestra un ID único que se genera para el servicio de NetWitness Suite y que se utiliza para establecer un vínculo a las métricas de ese componente específico. En este ejemplo, el ID de Reporting Engine es 6 y las métricas se muestran para ComponentId 6 en Conteo total, como se aprecia a continuación:


```
"Metrics": [{
    "StartTimeUTC": 1473292800000,
    "Stats": [{
        "Value": "10",
        "Name": "Number of RE Report"
    },
    {
        "Value": "2",
        "Name": "Number of RE Alert"
    },
    {
        "Value": "1",
        "Name": "Number of RE Chart"
    },
    {
        "Value": "14",
        "Name": "Number of RE Rule"
    },
    {
        "Value": "2",
        "Name": "Number of Enabled RE Alert"
    },
    {
        "Value": "1",
        "Name": "Number of Enabled RE Chart"
    }],
    "EndTimeUTC": 1473379199000,
    "ComponentId": 6
},
```

Métricas	Descripción
	Propiedades: Muestra las propiedades del componente, como el nombre y el valor, que se aprecian en la figura anterior.
	Valor: Muestra el valor de la propiedad que es un UUID interno para un componente, como se aprecia en la figura anterior. Esto lo genera NetWitness Suite. Por ejemplo, para Reporting Engine, el valor aparece como "`57444ddde4b0dd618093064d`".
	Nombre: "**InstanceId**": Muestra el nombre de la propiedad, como se aprecia en la figura anterior.
	Nombre: "**reportingengine**": Muestra el nombre del componente que es un nombre de servicio, como LogDecoder, Decoder o ReportingEngine.

	Nombre: Muestra la lista de las métricas con los datos de uso de componentes, como log decoder, decoder y reportingengine.
	En este ejemplo, las métricas se muestran para ComponentId 6 en bytes, como se aprecia a continuación.
	"Metrics": [{
	"StartTimeUTC": 1473292800000,
	"Stats": [{
	"Value": "10",
	"Name": "Number of RE Report"
	},
	{
	"Value": "2",
	"Name": "Number of RE Alert"
	},
	{
	"Value": "1",
	"Name": "Number of RE Chart"
	},
	{
	"Value": "14",
	"Name": "Number of RE Rule"
	},
	{
	"Value": "2",
	"Name": "Number of Enabled RE Alert"
	},
	{
	"Value": "1",
	"Name": "Number of Enabled RE Chart"
	}],
	"EndTimeUTC": 1473379199000,
	"ComponentId": 6
	},

	StartTimeUTC: Muestra la hora en que se recopilan métricas, en formato EPOCH.

Métricas	Descripción
	Stats: Muestra las estadísticas de valor de uso y tipo de uso del componente.
	Valor: Muestra el valor de las estadísticas. Por ejemplo, Número de informe de RE es 10, Número de alerta de RE es 2, Número de gráfico de RE es 1, etc., como se muestra en la figura anterior.
	Nombre: Muestra el nombre de la estadística. Por ejemplo, Número de informe de RE, Número de alerta de RE, Número de gráfico de RE, Número de regla de RE, Número de alerta de RE habilitada y Número de gráfico de RE habilitado.
	EndTimeUTC: Muestra la hora en que se completa la recopilación de métricas, en formato EPOCH.
	ComponentId: Muestra el ID de componente para el cual se recopilan valores de métricas. Es el mismo que el "ID" de la sección Components.
ProductType	Muestra el tipo de producto que genera el archivo. Por ejemplo, `"ProductType": "NetWitness Suite"`
ProductInstance	Muestra el ID del servidor de licencia, el cual es único por NetWitness Suite. Por ejemplo, `"ProductInstance": "00-0C-29-6C-66-E3"`
Suma de comprobación	Muestra la suma de comprobación de la sección "Content" del archivo. La usa RSA para la comprobación de integridad. Por ejemplo, `"Checksum": "883DACF97E4BCD9F590A1461A4DD0A312B5883A6CF82E0518E77AAB6A6DDB654"`

Ejemplo

Este es un archivo JSON de ejemplo.


```
{
    "Content": {
        "Components": [{
            "Version": "10.6.1.0",
            "Id": 7,
            "Properties": [{
                "Value": "57470c96e4b0cf62c7bfbd53",
                "Name": "InstanceId"
            }],
            "Name": "esa"
        },
        {
            "Version": "10.6.1.0",
            "Id": 4,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e69",
                "Name": "InstanceId"
            }],
            "Name": "incidentmanagement"
        },
        {
            "Version": "10.6.1.0",
            "Id": 2,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e65",
                "Name": "InstanceId"
            }],
            "Name": "sa"
        },
        {
            "Version": "10.6.1.0",
            "Id": 1,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e63",
                "Name": "InstanceId"
            }],
            "Name": "malwareanalysis"
        },
        {
            "Version": "10.6.1.0",
            "Id": 3,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e67",
                "Name": "InstanceId"
            }],
            "Name": "reportingengine"
        }],
        "Metrics": [{
            "StartTimeUTC": 1464480000000,
            "Stats": [{
                "Value": "Disabled",
                "Name": "Threat Detection"
            },
            {
                "Value": "3.0",
                "Name": "Number Of Enabled ESA Rules"
            }],
            "EndTimeUTC": 1464566399000,
            "ComponentId": 7
        }],
        "EndTime": 1464566399000,
        "Version": "1.0",
        "StartTime": 1464479999000,
        "ProductType": "Security Analytics",
        "ProductInstance": "00-0C-29-A2-57-B4"
    },
    "Checksum": "6445C704D3F9E67D24DBA8F11EB6C003CBCC0E199576342E6E6D2545524F583F"
}
```

Cargar datos en RSA para Live Feedback

En este tema se proporciona instrucciones para que un administrador de NetWitness Suite exporte las métricas en NetWitness Suite para Live Feedback.

Si no está configurada la cuenta de Live, puede cargar manualmente los datos de uso en RSA. Para obtener más información, consulte Panel Configuración de servicios de Live.

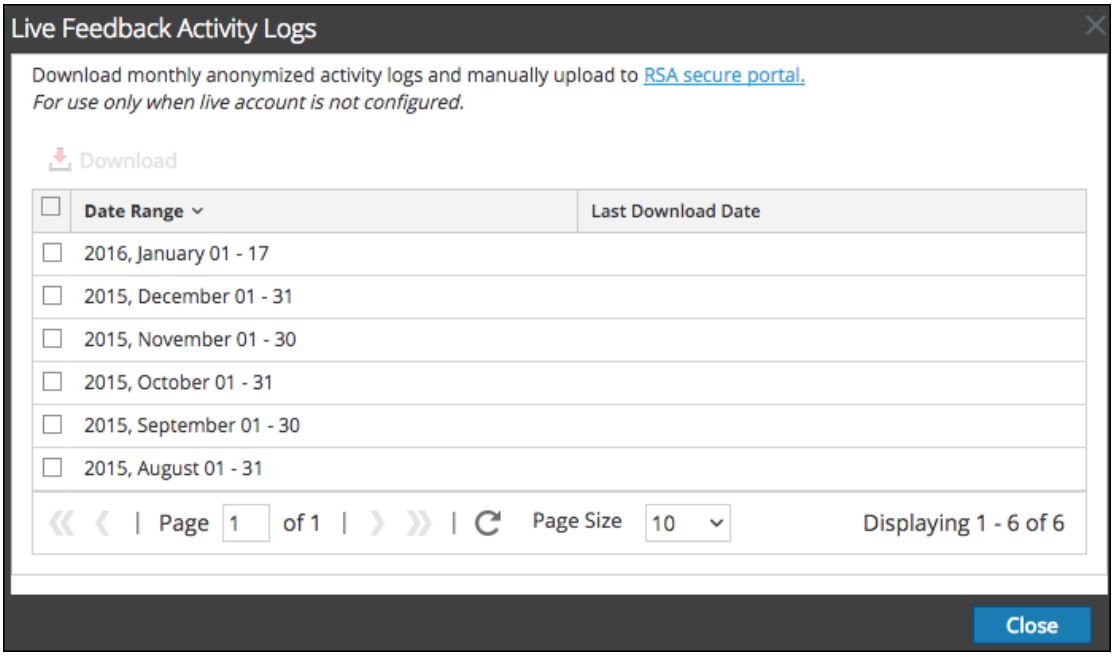
La sección Cuenta de Live tiene un registro de actividad de Live Feedback, el cual permite descargar los datos de uso requeridos para Live Feedback. Esto está activo, independientemente de la configuración de la cuenta de Live.

Puede descargar los datos históricos de Live Feedback y luego cargarlos para compartirlos con RSA.

Descargar datos históricos de Live Feedback

Para descargar los datos históricos de Live Feedback:

1. Vaya a **ADMIN** > **Sistema**.
2. En el panel de opciones, seleccione **Servicios de Live**.
   Se muestra la pantalla **Cuenta de Live**, la cual consta de **Estado de RSA Live** y **Descargar registro de actividad de Live Feedback**.
3. Haga clic en **Descargar registro de actividades de Live Feedback**.
   Se abre la ventana **Descargar registro de actividades de Live Feedback**, la cual permite que el usuario de NetWitness Suite descargue los datos históricos requeridos de Live Feedback.



4. Elija una o varias entradas mediante la selección de las casillas de verificación y haga clic

en **Descargar**.

Nota: Si selecciona varias entradas en la tabla de historial, el archivo zip descargado consta de un archivo JSON individual para cada mes.

Los datos descargados de Live Feedback están en formato JSON y se encuentran empaquetados como un archivo .zip. Para obtener más información, consulte Descripción general de Live Feedback.

Compartir datos con RSA

Después de descargar los datos de Live Feedback, puede cargarlos mediante el siguiente procedimiento.

Para compartir los datos en RSA:

1. Haga clic en el **Portal seguro de RSA** disponible en la ventana **Registros de actividad de Live Feedback**.
   Aparece la pantalla de inicio de sesión de RSA NetWitness® Suite Live Feedback.
2. Inicie sesión en el portal Cargar registros de actividad de Live Feedback mediante sus credenciales de ID de Live.
3. Haga clic en **Elegir archivo** y seleccione el archivo descargado.
4. Haga clic en **Cargar.**

Configurar los ajustes del archivo de registro

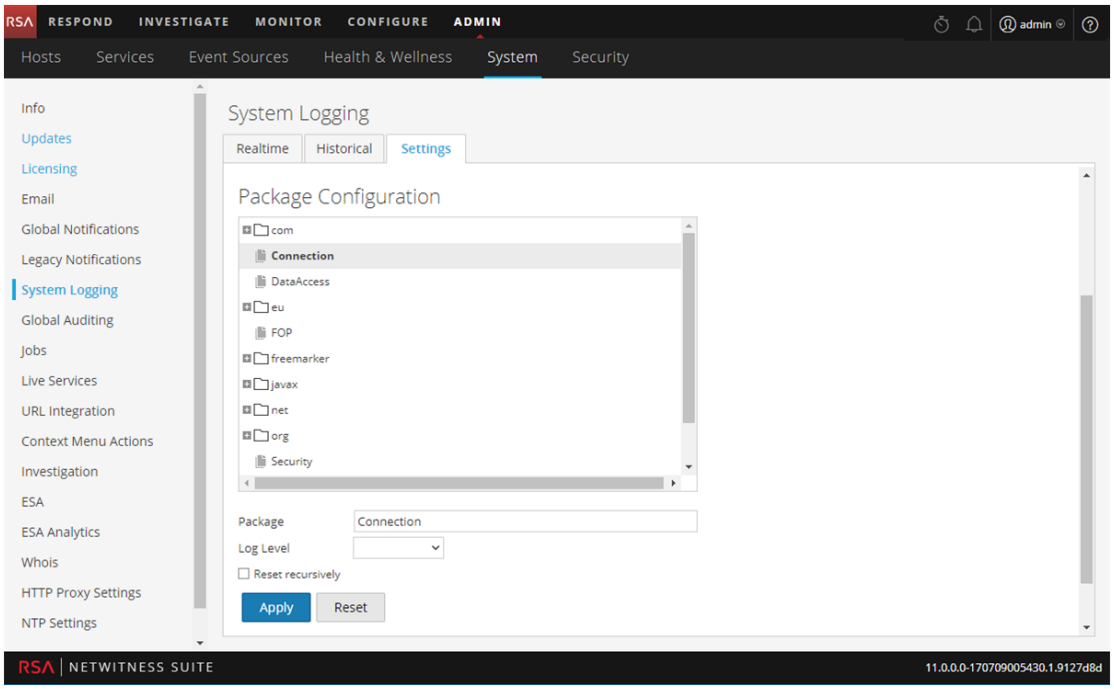
En RSA NetWitness® Suite, puede configurar el tamaño de los archivos de registro, el número de archivos de registro de respaldo que se mantienen, así como los niveles de registro predeterminados para los paquetes en NetWitness Suite.

Configurar el tamaño del archivo de registro del sistema y el conteo de respaldo

El tamaño del archivo de registro y el conteo de respaldo se configuran con valores predeterminados. Si desea cambiar los valores predeterminados para el tamaño del archivo de registro y el número de respaldos:

1. Vaya a **ADMIN > Sistema.**
2. En el panel de opciones, seleccione **Registro de sistema**.
   El panel Configuración del registro de sistema se abre de manera predeterminada en la pestaña Tiempo real.

3. Haga clic en la pestaña **Ajustes de configuración**.

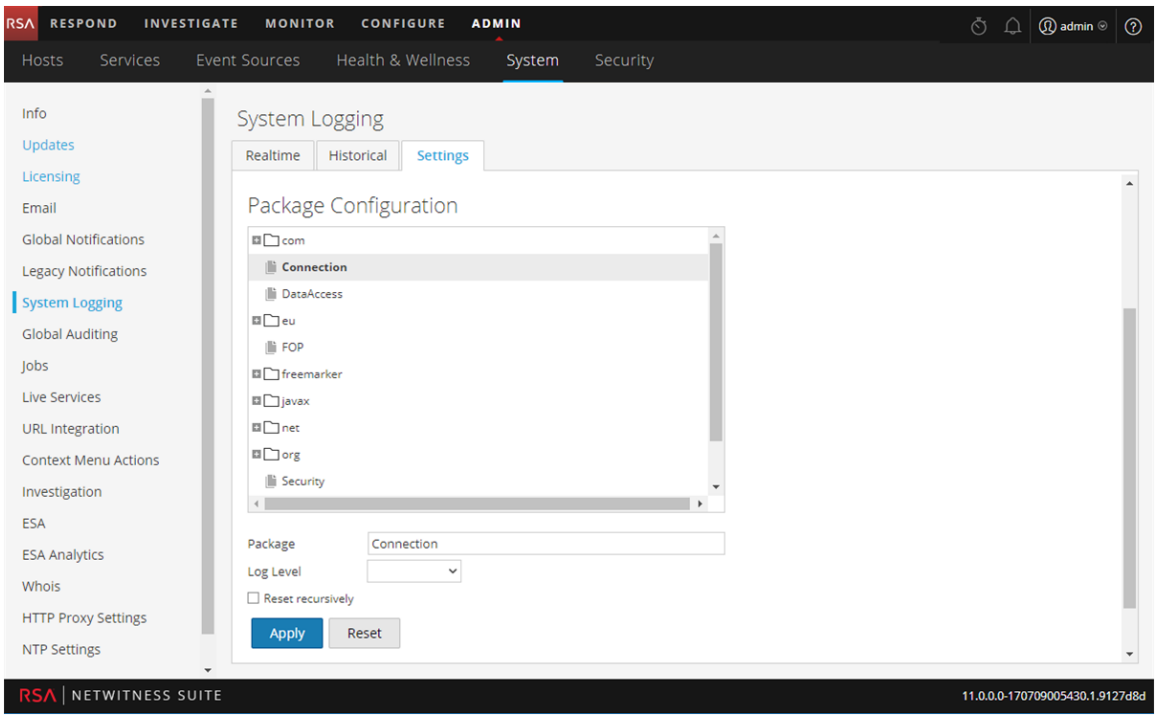


4. En el campo **Tamaño máximo de registro**, ingrese el tamaño máximo en bytes. El valor mínimo de este ajuste es **4096**.
5. En el campo **Número máximo de archivos de respaldo**, ingrese el número máximo de registros de respaldo para mantener. El valor mínimo de este ajuste es **0**. Cuando se alcanza la cantidad máxima de archivos de registro y se crea un nuevo archivo de respaldo, se elimina el respaldo más antiguo.
6. Haga clic en **Aplicar**.
   Los cambios se aplican de inmediato.

Configurar el nivel de registro para un paquete individual

La sección Configuración de paquete muestra los paquetes de Paquetes de NetWitness en una estructura de árbol. El árbol contiene todos los paquetes utilizados dentro de NetWitness Suite. Puede desglosar el árbol para ver los niveles de registro de cada paquete. El nivel de registro para todos los paquetes que no están explícitamente configurados es igual que el nivel de registro **raíz**. Para configurar el nivel de registro para un paquete:

1. Seleccione el paquete en el árbol **Paquete**.
   El nombre del paquete se muestra en el campo **Paquete**. Si ya hay un nivel de registro configurado para el paquete, se muestra ese nivel.



2. Seleccione el **Nivel de registro** en la lista desplegable.
3. Haga clic en **Aplicar**.
   El nuevo nivel de registro se aplica de inmediato.
4. (Opcional) Si desea revertirlo en el nivel de registro predeterminado especificado para la **raíz**, haga clic en **Restablecer**.

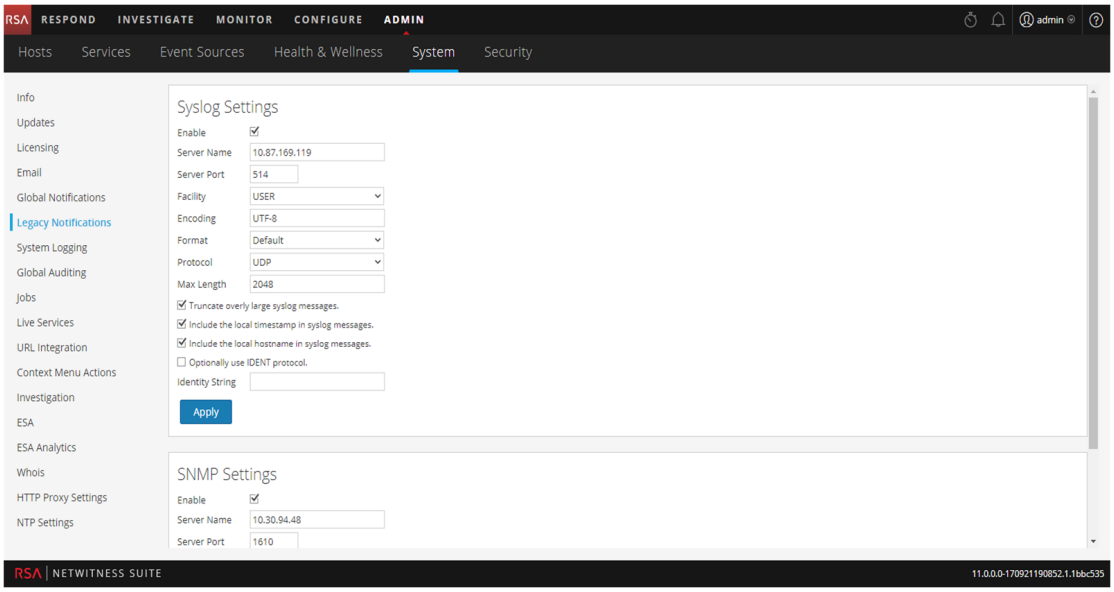
Configurar ajustes de syslog y SNMP

En el panel Notificaciones antiguas, puede configurar ajustes de notificaciones de syslog y SNMP. Estas configuraciones se usan para Autorización, Administración de orígenes de eventos (ESM) heredada, monitoreo de Warehouse Connector y monitoreo de Archiver.

Configurar y habilitar ajustes de syslog

1. Vaya a **ADMIN > Sistema**.

2. En el panel de opciones, seleccione **Notificaciones antiguas**.
   Se muestra el panel Configuración de notificaciones antiguas.

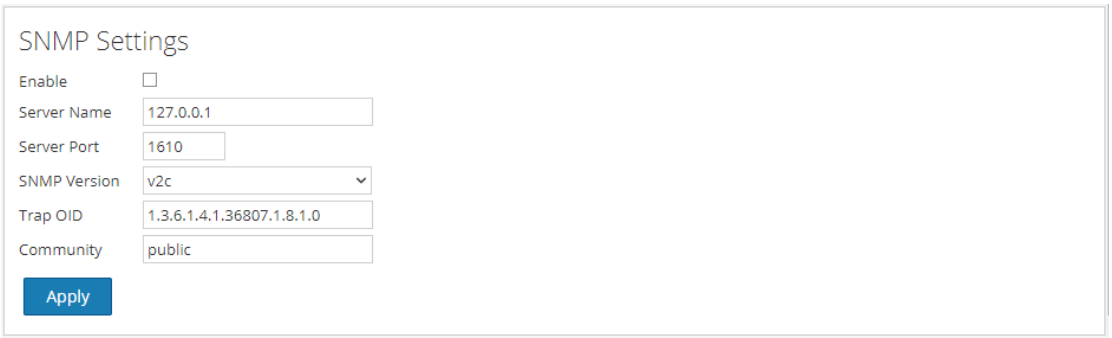


3. En los campos **Nombre del servidor** y **Puerto del servidor** de **Configuración de syslog**, ingrese el nombre de host donde se está ejecutando el proceso de syslog objetivo y el puerto donde está escuchando.
4. En los campos **Instalación**, **Codificación**, **Formato** y **Longitud máxima**, especifique la instalación de syslog, la codificación de texto del mensaje, el formato del mensaje y la longitud máxima del mensaje.
5. En el campo **Protocolo**, seleccione UDP o TCP.
6. (Opcional) Seleccione las opciones que se incluirán en los mensajes: **Truncar los mensajes de syslog demasiado grandes**, **Incluir el registro de fecha y hora local en los mensajes de syslog** e **Incluya el nombre de host local en los mensajes de syslog**.
7. (Opcional) Configure el syslog para adjuntar una cadena de identidad antes de cada alerta de syslog.
8. Haga clic en la casilla de verificación **Habilitar**.
9. Haga clic en **Aplicar**.
   Las notificaciones de syslog se habilitan de inmediato.

En el Panel Configuración de notificaciones antiguas se proporciona información detallada sobre estos ajustes.

Configurar y habilitar ajustes de SNMP

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones antiguas**.
   Se muestra el panel Configuración de notificaciones antiguas, con una configuración de SNMP en la parte inferior del panel.



3. En los campos **Nombre del servidor** y **Puerto del servidor** de **Configuración de SNMP**, ingrese el nombre de host y el puerto de escucha del host de SNMP trap.
4. Seleccione la **versión de SNMP** en el menú desplegable, **v1** o **v2c**.
5. En el campo **OID de traps**, especifique el ID de objeto para el SNMP trap en el host de traps que recibe el evento de auditoría. El valor predeterminado es **0.0.0.0.0.1**.
6. En el campo **Comunidad**, especifique la cadena de comunidad utilizada para autenticarse en el host de SNMP trap; el valor predeterminado es **público**.
7. Haga clic en la casilla de verificación **Habilitar**.
8. Haga clic en **Aplicar**.
   Las notificaciones de SNMP se habilitan de inmediato.

En el Panel Configuración de notificaciones antiguas se proporciona información detallada sobre estos ajustes.

Deshabilitar la configuración de syslog o SNMP

Para deshabilitar la configuración de syslog o SNMP en esta instancia de NetWitness Suite:

1. Deseleccione la casilla de verificación **Activar** correspondiente.
2. Haga clic en **Aplicar**.
   La configuración seleccionada se inhabilita de inmediato.

Procedimientos adicionales

Los procedimientos adicionales no son esenciales para la configuración de NetWitness Suite, estos incluyen opciones de personalización específicas que van más allá de la configuración habitual; por ejemplo, agregar menús contextuales personalizados o configurar un proxy.

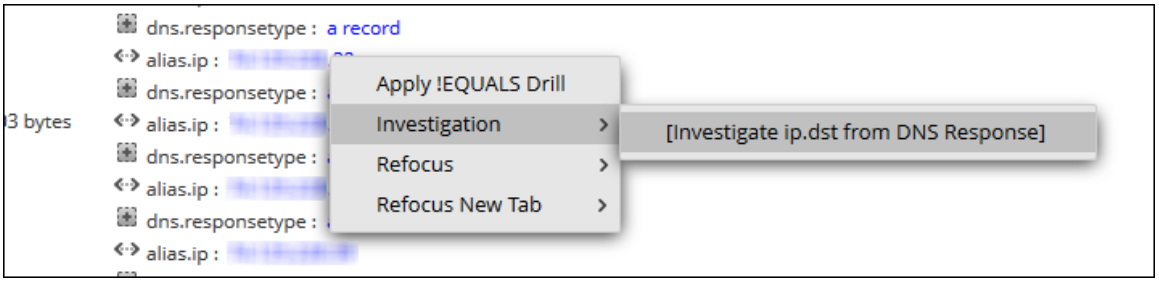
Agregar acciones de menú contextual personalizadas

En el panel Acciones del menú contextual, pueden ver, agregar y editar las acciones del menú contextual para la instancia actual de NetWitness Suite. Cada acción del menú contextual se aplica a un contexto específico en la interfaz del usuario de NetWitness Suite y aparece como una opción cuando se hace clic con el botón secundario en una ubicación específica de la interfaz del usuario.

Algunas acciones del menú contextual están incorporadas en NetWitness Suite; no puede editar ni eliminar ninguna de las acciones del menú contextual de forma predeterminada. Puede crear y editar las acciones del menú contextual personalizadas. Si desea crear una variación personalizada de una acción del menú contextual integrada, puede copiar la configuración en una acción de menú contextual nueva y modificar la acción de menú contextual personalizada. Una acción de menú contextual se define por el código de la hoja de estilo en cascada (CSS) que define:

- El título de la opción en el menú contextual.
- El módulo NetWitness Suite en el que está disponible el menú contextual.
- El contenido al cual se aplica la acción.

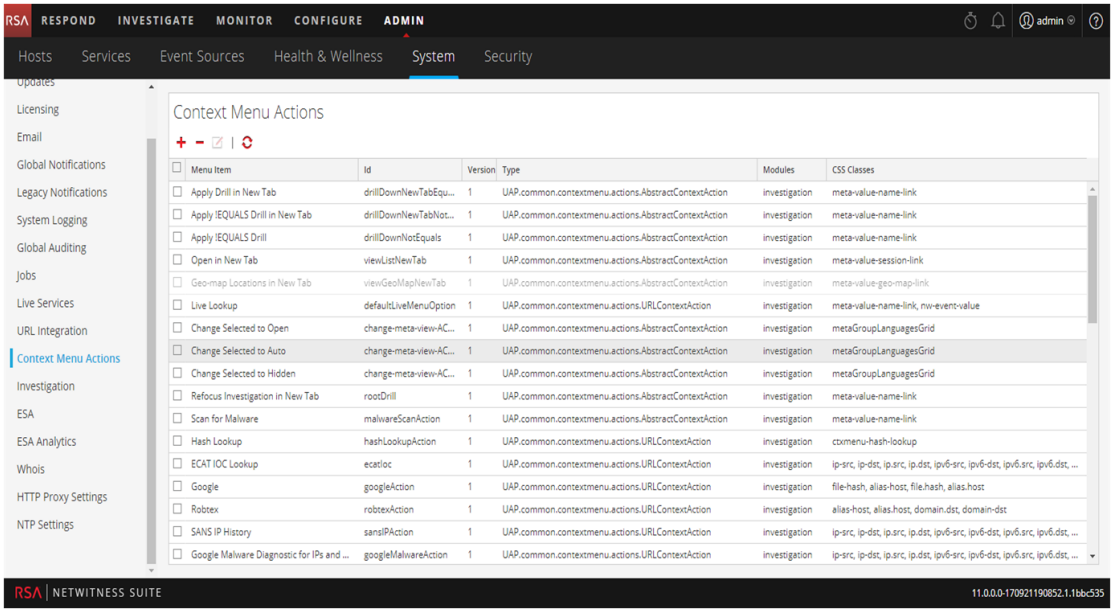
Este es un ejemplo de una acción del menú contextual personalizada; los pasos y el código CSS para crear este ejemplo se proporcionan como un procedimiento de ejemplo a continuación.



Ver Acciones del menú contextual en NetWitness Suite

Para ver las acciones contextuales existentes en NetWitness Suite predeterminadas y personalizadas:

1. Vaya a **ADMIN > Sistema.**
2. En el panel de opciones, seleccione **Acciones del menú contextual**.



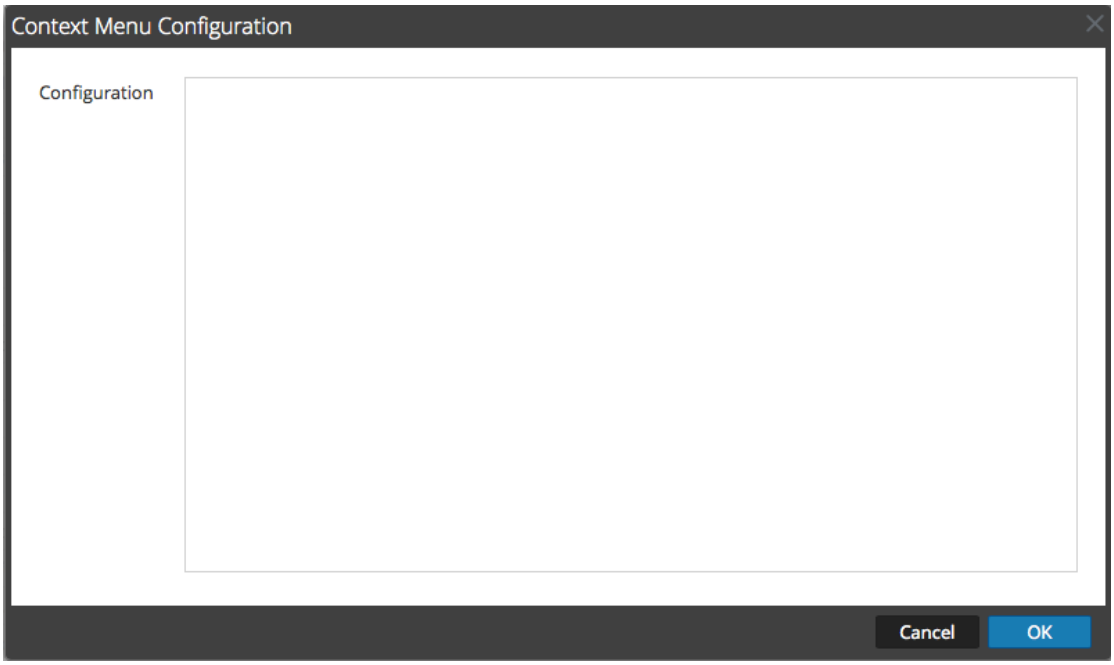
Se proporcionan detalles de la información en el panel Acción del menú contextual en el Panel Acciones del menú contextual

Agregar una acción del menú contextual

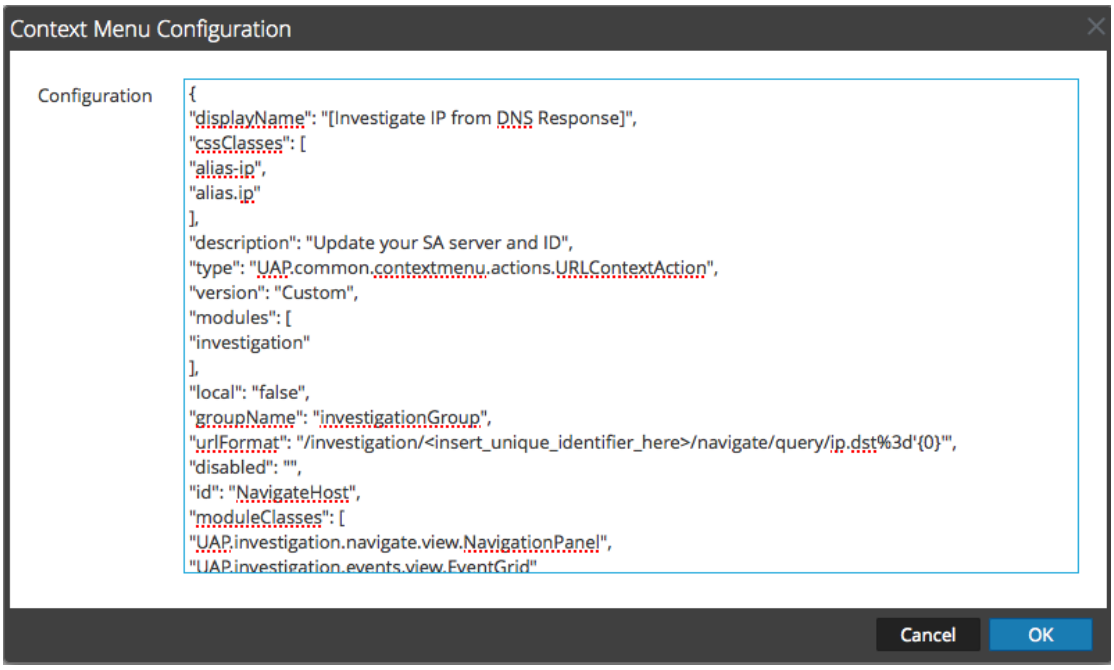
Para agregar una acción del menú contextual en NetWitness Suite:

1. En la barra de herramientas, haga clic en +.

   Se muestra el cuadro de diálogo Configuración de menú contextual.



2. Ingrese el código CSS para definir la acción el menú contextual. El procedimiento de ejemplo al final de este tema proporciona instrucciones paso a paso que puede usar para crear una acción del menú contextual útil.



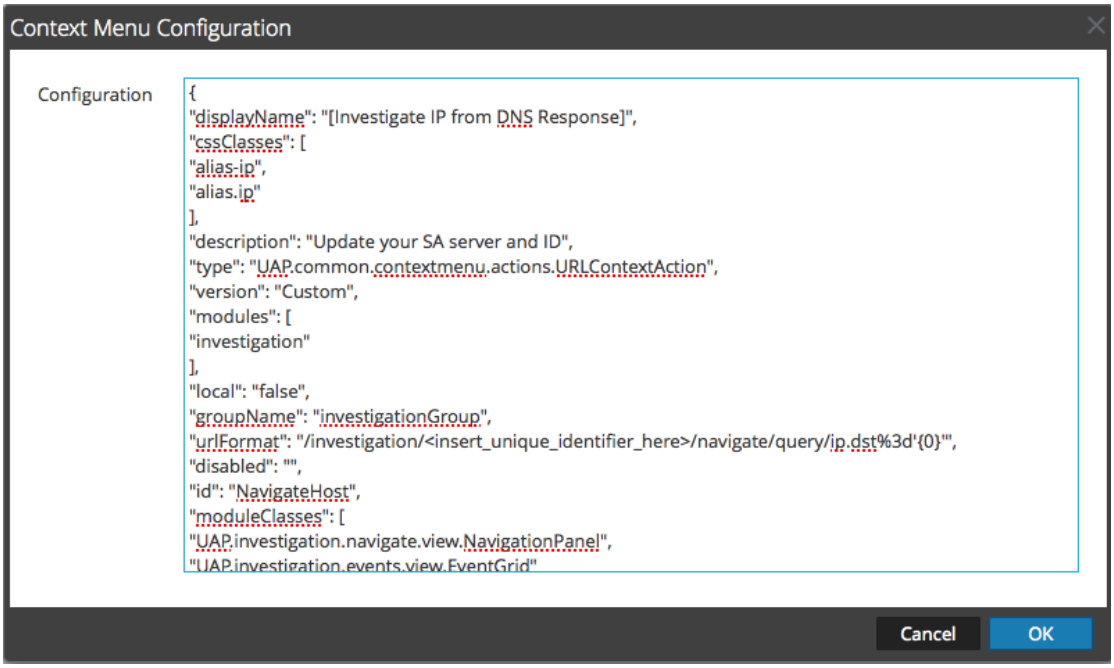
3. Haga clic en **Aceptar.**
   Se crea la nueva acción del menú contextual y se agrega al final de la lista de acciones del menú contextual.

4. Para activar la nueva acción del menú contextual, reinicie el navegador.
   La acción del menú contextual estará disponible en la ubicación configurada.

Editar una acción contextual

Para editar una acción contextual:

1. Seleccione la fila de la cuadrícula y **haga doble clic** en la fila o haga clic en .
   Se muestra el **cuadro de diálogo Configuración de menú contextual**.



2. Edite la **Configuración**.
3. Para guardar los cambios, haga clic en **Aceptar**.
4. Para utilizar la acción actualizada, reinicie el navegador.

Eliminar una acción contextual

Para quitar completamente una acción del menú contextual de NetWitness Suite:

1. Seleccione la acción.
2. Haga clic en .
   Un cuadro de diálogo solicita confirmar la intención de eliminar la acción de menú contextual.
3. Haga clic en **Sí**.
   La opción se elimina del panel Acciones del menú contextual.

4. Reinicie el navegador para eliminar la acción de los menús contextuales en los cuales aparecía.

Procedimiento de ejemplo: Acción del menú contextual para investigar ip.dst desde alias.ip

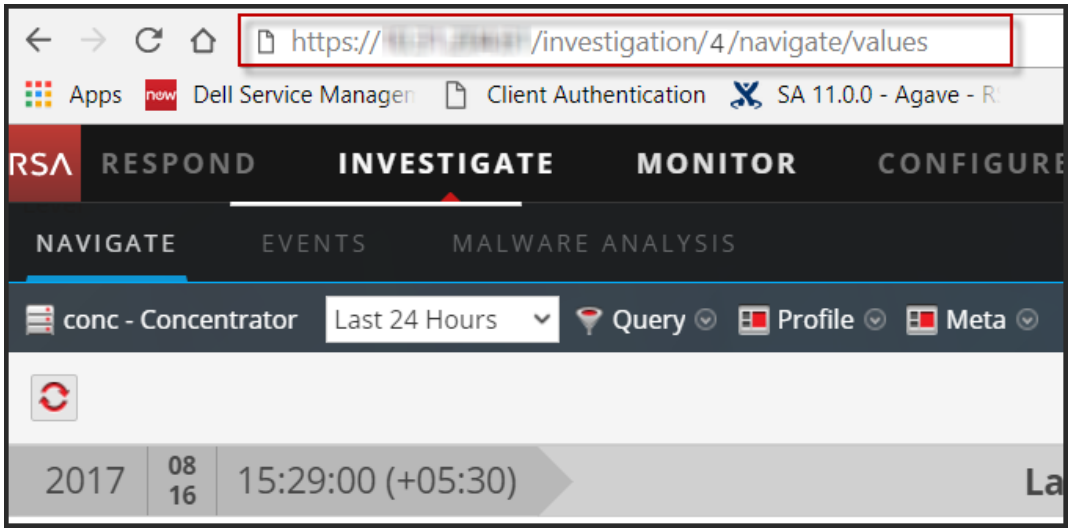
En este ejemplo se agrega una acción del menú contextual que permite a los analistas pasar de los valores de `alias.ip` (las direcciones IP que devuelve una solicitud DNS) a la clave de metadatos `ip.dst`. Ayuda a los analistas para ubicar cualquier tráfico detectado en la dirección IP, devuelto por una consulta DNS.

Para implementar la acción del menú contextual:

1. Determine el identificador único para su Servidor de NetWitness como se muestra a continuación:

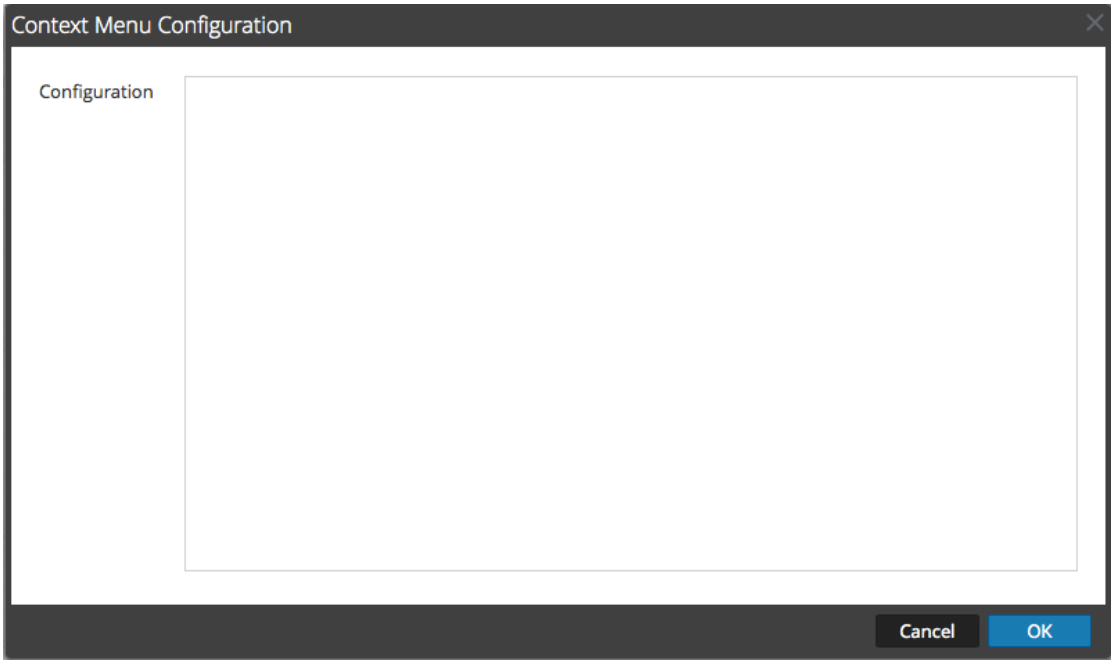
   a. Inicie sesión en NetWitness Suite, en el menú principal, seleccione **Investigation** > **Navegar**, elija un servicio (por ejemplo, Concentrator) para investigar y esperar la carga de los valores.

   b. Busque la dirección URL y el número después de `investigation`. En este ejemplo, el identificador único de la acción es 4. Se necesita este identificador único para agregar a la acción del menú contextual.



2. En la barra de herramientas, haga clic en +.

   Se muestra el cuadro de diálogo Configuración de menú contextual.



3. Copie el bloque de código de ejemplo completo que aparece a continuación y péguelo en la ventana.

```
{
    "displayName": "[Investigate IP from DNS Response]",
    "cssClasses": [
        "alias-ip",
        "alias.ip"
    ],
    "description": "Update your NW server and ID",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "Custom",
    "modules": [
        "investigation"
    ],
    "local": "false",
    "groupName": "investigationGroup",
    "urlFormat": "/investigation/<insert_unique_identifier_
here>/navigate/query/ip.dst%3d'{0}'",
    "disabled": "",
    "id": "NavigateHost",
```

```
    "moduleClasses": [
        "UAP.investigation.navigate.view.NavigationPanel",
        "UAP.investigation.events.view.EventGrid"
    ],
    "openInNewTab": "true"
}
```

4. En la línea **urlFormat**, reemplace **<insert-unique_identifier_here>** por su identificador único.

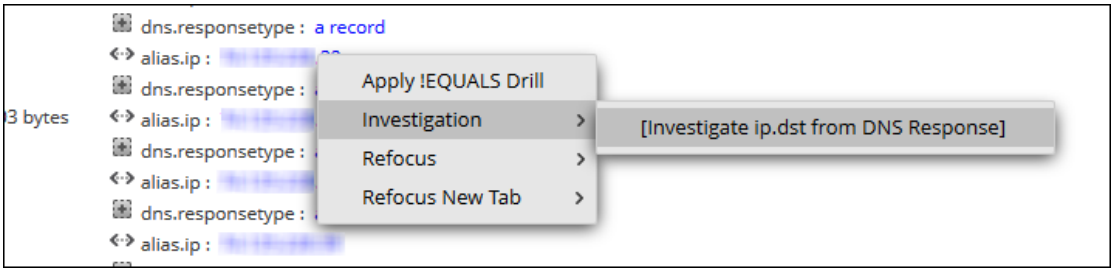
   La URL debe verse así:

   `"/investigation/4/navigate/query/ip.dst%3d'{0}'"`

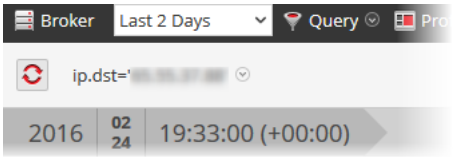
5. Haga clic en **Aceptar** y reinicie el navegador.

6. Para probar la acción, abra una investigación en la vista Navegar y haga clic con el botón secundario en la clave de metadatos `alias.ip`.

   El menú contextual con la opción de investigación debe parecerse a la siguiente figura.



7. Debe generar una actividad como esta.



8. Si utiliza este ejemplo para la investigación de tráfico DNS, puede ser útil crear un grupo de metadatos específico del tráfico DNS, como se describe en "Administrar grupos de metadatos definidos por el usuario" en la *Guía de Investigation y Malware Analysis*.

Configurar servidores NTP

En este tema se proporcionan instrucciones para configurar los servidores de Network Time Protocol (NTP). NTP es un protocolo diseñado para sincronizar los relojes de la máquina host en una red. Para obtener más información sobre NTP, vaya a su página de inicio (http://www.ntp.org/).

Nota: Los hosts principales de NW deben ser capaces de comunicarse con el host de NW con el puerto 123 de UDP para la sincronización horaria de NTP.

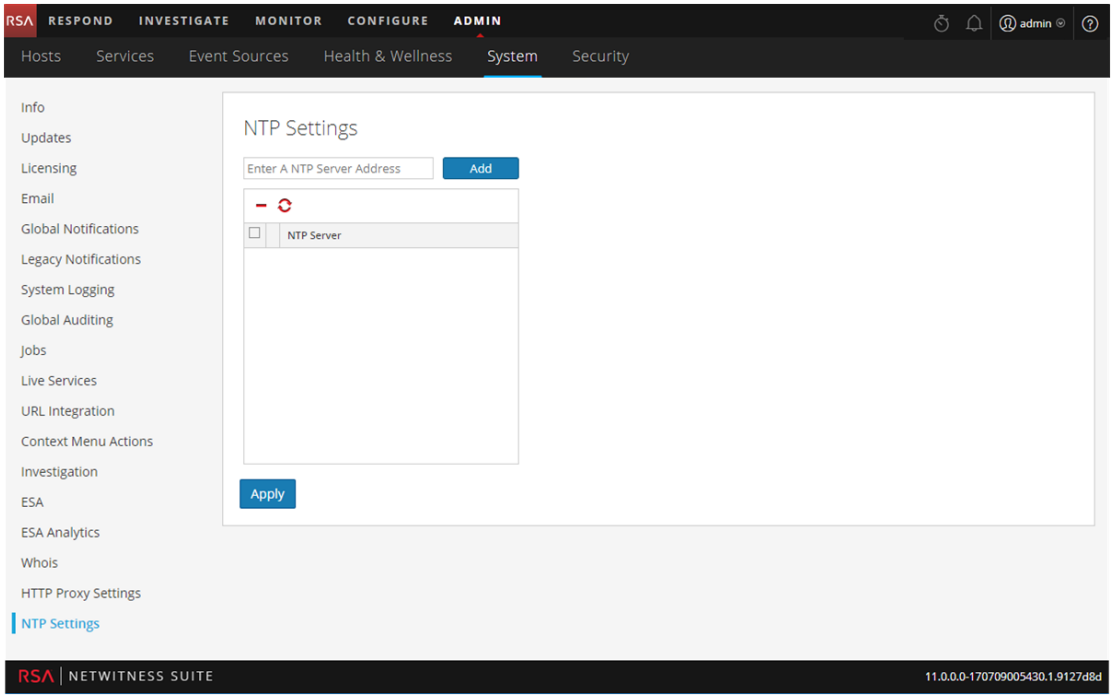
Use la vista **ADMIN** > **Sistema** > **Configuración de NTP** para configurar uno o más servidores NTP. Después de configurar un servidor NTP, NetWitness Suite usa NTP para sincronizar los relojes de la máquina host. Configure varios servidores NTP con fines de conmutación por error. Este tema contiene los siguientes procedimientos:

- Agregar un servidor NTP
- Modificar un servidor NTP

Agregar un servidor NTP

Para agregar un servidor NTP:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Configuración de NTP**.
   Se muestra el panel Configuración de NTP, donde se le solicita que ingrese el nombre de host (es decir, la dirección IP o el nombre de dominio calificado) de un servidor NTP.



3. Ingrese la dirección IP o el nombre de dominio calificado de un servidor NTP.
   Si la sintaxis del nombre de host no es válida, NetWitness Suite deshabilita los botones **Agregar** y **Aplicar** y muestra **Se ingresó un nombre de host no válido**.
4. Haga clic en **Agregar**.

- Si la sintaxis del nombre de host es válida y NetWitness Suite puede conectarse con el servidor, se muestra **Validando**.
- Si la sintaxis del nombre de host es válida y NetWitness Suite no puede conectarse a un servidor, se muestra lo siguiente, donde ***hostname*** es el nombre de host que intentó agregar: **El *nombre de host* del servidor NTP está inaccesible. Verifique la dirección o compruebe la configuración del firewall.**

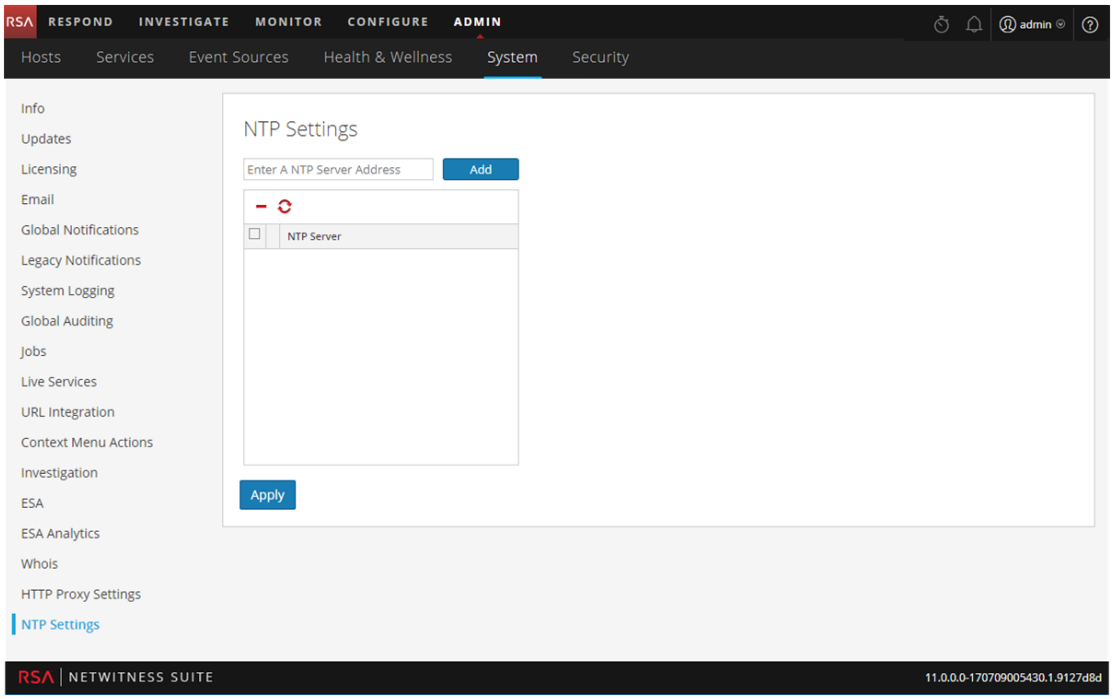
5. Haga clic en **Aplicar**.
   Un cuadro de diálogo muestra una notificación que señala que la configuración se guardó y que solicita confirmar la intención de aplicarla ahora.
6. Haga clic en **Sí**.
   El servidor NTP especificado se asegura ahora de que los relojes de la máquina host estén sincronizados. Si decide configurar varios servidores NTP y un servidor no está disponible, NetWitness Suite realizará una conmutación por error al siguiente servidor configurado.

Para obtener detalles y descripciones de los parámetros, consulte Panel Configuración de NTP.

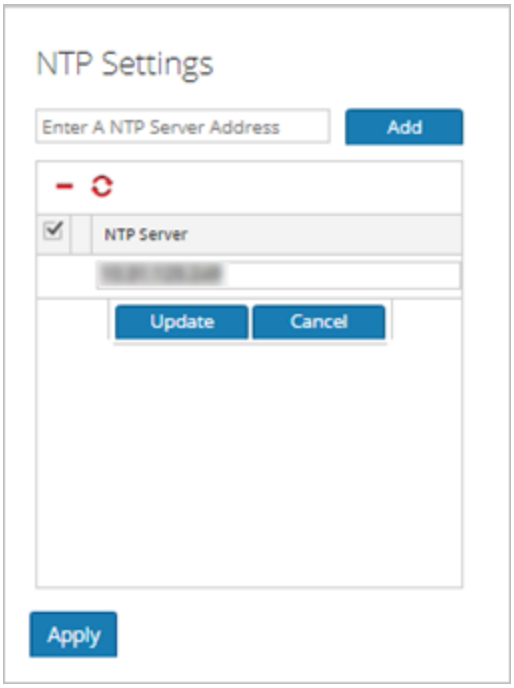
Modificar un servidor NTP

Para modificar un servidor NTP existente:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Configuración de NTP**.
   Se muestra el panel Configuración de NTP.



3. Haga doble clic en el nombre de host del **Servidor NTP** que desea modificar.
   El cuadro de texto Servidor NTP pasa a ser editable y se muestran los botones Actualizar y Cancelar.



4. Edite el nombre de host, haga clic en **Actualizar** y en **Aplicar**(haga clic en **Cancelar** antes de hacer clic en **Aplicar** para cancelar la edición).
   NetWitness Suite cambia el nombre de host de acuerdo con sus ediciones.

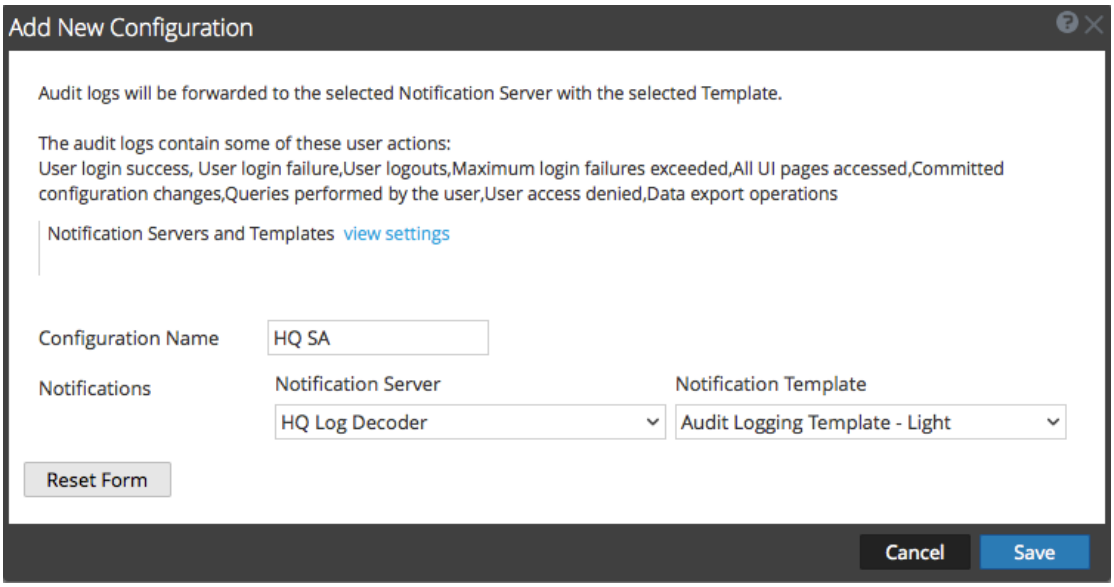
Cuadro de diálogo Agregar nueva configuración

El panel Configuraciones de log de auditoría global de la vista Sistema de Administration en RSA NetWitness® Suite permite crear múltiples configuraciones del registro de auditoría global. Estas configuraciones se usan para reenviar registros de auditoría global a una ubicación central con el fin de realizar auditorías a los usuarios.

Los procedimientos relacionados con el registro de auditoría global se describen en Configurar el registro de auditoría global.

Para acceder al cuadro de diálogo **Agregar nueva configuración**:

1. En el menú principal, seleccione **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Auditoría global**.
3. En el panel **Configuraciones de log de auditoría global**, haga clic en +.
   Se muestra el cuadro de diálogo **Agregar nueva configuración**.



La sección Notificaciones permite seleccionar un servidor de notificación de syslog para la configuración del registro de auditoría global y una plantilla que se usa para los registros de auditoría global. La plantilla define los detalles de las entradas del registro de auditoría global.

Funciones

En la siguiente tabla se describen las funciones de los cuadros de diálogo Agregar nueva configuración y Editar configuración.

Función	Descripción
Vínculo **ver configuración** de servidores y plantillas de notificación	Lo lleva al panel Notificaciones globales, donde puede ver o configurar los ajustes de servidores y plantillas de notificación. Se requiere un servidor de notificación de syslog y una plantilla del registro de auditoría antes de poder crear una configuración de auditoría global.
Nombre de configuración	Especifica el nombre único que se usa para identificar la configuración del registro de auditoría global.
Servidor de notificación	Especifica el servidor de notificación de syslog al cual se enviará la información del registro de auditoría seleccionado. En Configurar un destino para recibir registros de auditoría global se proporcionan instrucciones para crear un servidor de notificación de syslog para el registro de auditoría global.
Plantilla de notificación	Especifica la plantilla que se usará para la configuración del registro de auditoría global. La plantilla debe ser una plantilla del registro de auditoría. Para Log Decoders, use **Default Audit CEF Template**. Puede agregar o quitar campos de la plantilla del formato de evento común (CEF) si tiene requisitos específicos. En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones. Para servidores de syslog de otros fabricantes, puede usar una plantilla del registro de auditoría predeterminada o definir un formato propio (CEF o no CEF). En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones y en Variables de claves de metadatos del registro de auditoría global compatibles se describen las variables disponibles.
Botón **Restablecer formulario**	Borra los ajustes de configuración del cuadro de diálogo.

Acciones de los usuarios que se registran

En la siguiente tabla se proporcionan ejemplos de algunas de las acciones de los usuarios que se registran desde NetWitness Suite. Estas acciones son las acciones mínimas de los usuarios que se registran cuando corresponde.

Acción del usuario	Ejemplo
Sesión iniciada correctamente del usuario	Un usuario inicia sesión con credenciales válidas.
Error de inicio de sesión del usuario	Un usuario intenta iniciar sesión con credenciales no válidas.
Cierres de sesión del usuario	Un usuario cierra la sesión de NetWitness Suite (Administration > Cerrar sesión) o la sesión se cierra debido a un tiempo de espera agotado.
Máximo de errores al iniciar sesión superado	Un usuario intenta iniciar sesión cinco veces con credenciales no válidas. Cinco (5) es el Número máximo de errores al iniciar sesión definido en la vista Seguridad > pestaña Ajustes de configuración de Administration (Administration > Seguridad > pestaña Ajustes de configuración).
Todas las páginas de la interfaz del usuario a las cuales se accedió	Cuando un usuario accede al módulo Reporting (Administration > Informes), se registra como `[REP] Reports`. Cuando un usuario accede a la vista Sistema de Administration (Administration > Sistema), se registra como `[ADM] System`.
Cambios en la configuración confirmados	Un usuario cambia su contraseña y/o cualquier configuración de seguridad (Administration > Seguridad > pestaña Ajustes de configuración).

Acción del usuario	Ejemplo
Consultas que realizó el usuario	Un usuario realiza una consulta de investigación.
Acceso del usuario denegado	Un usuario intenta acceder a un módulo y no tiene permisos para hacerlo.
Operaciones de exportación de datos	Un usuario exporta datos desde la vista Eventos (Investigation > Eventos > Acciones > Exportar).

Para obtener listas de los tipos de mensajes que registran los diversos componentes de NetWitness Suite, consulte Referencia de operaciones del registro de auditoría global.

Claves de metadatos de CEF compatibles

En este tema se describen las claves de metadatos del formato de evento común (CEF) compatibles con el registro de auditoría global de NetWitness Suite.

Las plantillas del registro de auditoría global que define para un Log Decoder usan el formato de evento común (CEF) y deben cumplir con los siguientes requisitos estándar específicos:

- Incluya los encabezados de CEF en la plantilla.
- Use solo las extensiones y las extensiones personalizadas en el formato (Clave=Valor) que se presenta más abajo en la tabla de claves de metadatos.
- Asegúrese de que las extensiones y las extensiones personalizadas estén en el formato `key=${string}<space>key=${string}`.

Para servidores de syslog de otros fabricantes, puede definir un formato propio (CEF o no CEF).

Los procedimientos relacionados con esta tabla se describen en Definir una plantilla para el registro de auditoría global y Configurar el registro de auditoría global.

Claves de metadatos del formato de evento común (CEF) compatibles

En la siguiente tabla se describen las claves de metadatos de syslog de CEF compatibles con el registro de auditoría global de NetWitness Suite. Los campos Fecha y hora y Nombre del host en Prefijo de syslog no son configurables y no se incluyen en la plantilla, pero se anteponen de manera predeterminada a cada mensaje del registro. El encabezado de CEF es requisito para cumplir con el estándar CEF y para cualquier analizador de CEF. Las extensiones y las extensiones personalizadas son opcionales. Default Audit CEF Template contiene muchos de los campos de esta tabla. Puede agregar cualquiera de las extensiones y las extensiones personalizadas que se enumeran en la plantilla del registro de auditoría global que usted define.

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
Prefijo de syslog				

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
Fecha y hora	No configurable	Fecha y hora del encabezado de syslog	event.time.str	Transitorio
Hostname	No configurable	Nombre de host del encabezado de syslog	alias.host	Ninguno
Encabezado de CEF		El campo Encabezado de CEF es requisito para cumplir con el estándar CEF y para cualquier analizador de CEF.		
CEF:Version	CEF:0	Encabezado de CEF	--STATIC--	N/D
DeviceVendor	${deviceVendor}	El proveedor del producto, RSA	-	N/D
DeviceProduct	${deviceProduct}	La familia de productos. Es siempre Auditoría de NetWitness Suite.	product	Transitorio

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
DeviceVersion	${deviceVersion}	Versión del host/servicio	version	Transitorio
ID de la firma	${category}	Identificador del evento de auditoría. Especifica la categoría del evento de auditoría.	event.type	Ninguno
Nombre	${operation}	Descripción del evento	event.desc	Ninguno
Gravedad	${severity}	Severidad del evento de auditoría	severity	Transitorio
Extensiones				
deviceExternalId	${deviceExternalId}	ID único del host o servicio que genera el evento de auditoría	hardware.id	Transitorio
deviceFacility	${deviceFacility}	Funcionalidad de syslog que se usa cuando el evento se escribe en el demonio de syslog. Por ejemplo, authpriv.	cs.devfacility	Personalizado

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
deviceProcessName	${deviceProcessName}	Nombre del archivo ejecutable que corresponde a dvcpid	process	Ninguno
dpt	${destinationPort}	Puerto de destino	ip.dstport	Ninguno
dst	${destinationAddress}	Dirección IP de destino	ip.dst	Ninguno
dvcpid	${deviceProcessId}	ID del proceso que genera el evento, que es el ID de proceso del servicio de NetWitness Suite	process.id	Transitorio
msg	${text}	Texto libre, información adicional o descripción real del evento	msg	Transitorio
outcome	${outcome}	Resultado de la operación realizada correspondiente al evento de auditoría	result	Transitorio

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
proto	${transportProtocol}	Protocolo de red utilizado	protocol	Transitorio
requestClientApplication	${userAgent}	Detalle del navegador del usuario que accede a la página	user.agent	Transitorio
rt	${timestamp}	Hora en que se informa el evento	event.time	Ninguno
sourceServiceName	${sourceService}	Servicio que es responsable de generar este evento	service.name	Transitorio
spt	${sourcePort}	Puerto de origen	ip.srcport	Transitorio

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
spriv	${userRole}	Asignación de permisos de función del usuario. Por ejemplo: admin.owner, appliance.manage, connections.manage, everyone, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage y users.manage	privilege	Transitorio
src	${sourceAddress}	Dirección IP de origen	ip.src	Ninguno
suser	${identity}	Identidad del usuario que inició sesión y que es responsable de generar el evento de auditoría	-user|-u	Ninguno
Extensiones personalizadas				

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
deviceService	${deviceService}	Servicio responsable de generar el evento	cs.devservice	Personalizado
parameters	${parameters}	Parámetros de la API y de operación que capturan parámetros específicos sobre una consulta	index	Transitorio
paramKey	${key}	Clave de elemento de configuración. Es el parámetro de configuración para el cual se captura el evento de auditoría. Por ejemplo: /sys/config/stat.interval	cs.key	Personalizado
paramValue	${value}	Valor de configuración. Es el valor capturado durante la actualización.	cs.value	Personalizado

Campo de CEF	Cadena	Descripción	Claves de metadatos de NW	Índice en Log Decoder
userGroup	${userGroup}	Asignación de funciones. Por ejemplo: Administradores, Analistas, MalwareAnalysts, Malware_ Analysts, Operators, PRIVILEGED_ CONNECTION_ AUTHORITY y SOC_Managers	grupo	Ninguno
referrerURL	${referrerUrl}	URL principal que hace referencia a la URL actual	url	Transitorio
sessionId	${sessionId}	Identificador de la sesión o la conexión	log.session.id	Transitorio

Nota: Use todas las extensiones en el siguiente formato:
`deviceProcessName=${deviceProcessName} outcome=${outcome}`
Incluya un `<space>` entre un valor y un nombre de etiqueta.

De manera predeterminada, ninguna clave de metadatos se indexa. En la tabla anterior, la columna **Índice en Log Decoder** muestra el estado de la palabra clave `flags` (Transitorio, Ninguno y Personalizado). Si una clave se configura en `Transient`, se analiza pero no se almacena en la base de datos. Si se configura en `None`, se indexa y se almacena en la base de datos. Una clave enumerada como “Personalizada” no existe en el archivo table-map.xml y, por lo tanto, no se almacena ni se analiza.

En “Mantener los archivos de mapa de tablas” se proporcionan instrucciones para verificar y actualizar los mapeos de tablas. En “Editar un archivo de índice de servicios” se proporciona información sobre la actualización del archivo de índice personalizado en el Concentrator.

Variables de claves de metadatos del registro de auditoría global compatibles

En este tema se describen las variables de claves de metadatos compatibles con el registro de auditoría global de NetWitness Suite.

NetWitness Suiteproporciona plantillas predefinidas del registro de auditoría global que se pueden usar para las configuraciones del registro de auditoría global. Para servidores de syslog de otros fabricantes, puede definir un formato de plantilla (CEF o no CEF) propio mediante el uso de variables de claves de metadatos compatibles.

Los procedimientos relacionados con esta tabla se describen en Definir una plantilla para el registro de auditoría global y Configurar el registro de auditoría global.

Variables de claves de metadatos del registro de auditoría global compatibles

En la siguiente tabla se describen las variables de claves de metadatos compatibles con el registro de auditoría global de NetWitness Suite. Use estos valores para crear una plantilla personalizada del registro de auditoría para un servidor de syslog de otros fabricantes.

Variable	Descripción
${category}	Identificador del evento de auditoría. Especifica la categoría del evento de auditoría.
${destinationAddress}	Dirección IP de destino
${destinationPort}	Puerto de destino
${deviceExternalId}	ID único del servicio que genera el evento de auditoría
${deviceFacility}	Funcionalidad de syslog que se usa cuando el evento se escribe en el demonio de syslog. Por ejemplo, authpriv.
${deviceProcessId}	ID del proceso que genera el evento, que es el ID de proceso del servicio de NetWitness Suite
${deviceProcessName}	Nombre del archivo ejecutable que corresponde a dvcpid
${deviceProduct}	La familia de productos. Es siempre Auditoría de NetWitness Suite.

Variable	Descripción
${deviceService}	Servicio responsable de generar el evento
${deviceVendor}	El proveedor del producto, RSA
${deviceVersion}	Versión del host/servicio
${identity}	Identidad del usuario que inició sesión y que es responsable de generar el evento de auditoría
${key}	Clave de elemento de configuración. Es el parámetro de configuración para el cual se captura el evento de auditoría.
${operation}	Descripción del evento
${outcome}	Resultado de la operación realizada correspondiente al evento de auditoría
${parameters}	Parámetros de la API y de operación que capturan parámetros específicos sobre una consulta
${referrerUrl}	URL principal que hace referencia a la URL actual
${sessionId}	Identificador de la sesión o la conexión
${severity}	Severidad del evento de auditoría
${sourceAddress}	Dirección IP de origen
${sourcePort}	Puerto de origen
${sourceService}	Servicio que es responsable de generar este evento
${text}	Texto libre, información adicional o descripción real del evento
${timestamp}	Hora en que se informa el evento
${transportProtocol}	Protocolo de red utilizado
${userAgent}	Detalle del navegador del usuario que accede a la página

Variable	Descripción
${userGroup}	Asignación de funciones
${userRole}	Asignación de permisos de función del usuario
${value}	Valor de configuración. Es el valor capturado durante la actualización

Referencia de operaciones del registro de auditoría global

En este tema se enumeran los tipos de mensajes que registran los diversos componentes de NetWitness Suite. La mayoría de los mensajes establecen claramente la operación que se registran; cuando sea necesario, se explica el significado del mensaje.

Después de que crea una configuración del registro de auditoría global, los registros de auditoría se dirigen automáticamente al sistema de syslog externo en el formato especificado en la plantilla del registro de auditoría seleccionada. Los tipos de mensajes que registran los diversos componentes de NetWitness Suite se muestran en las siguientes tablas.

CARLOS

En la siguiente tabla se indican las operaciones que registra CARLOS.

Número de serie	Nombre de la operación	Significado
1	SetProviderConfiguration	Se agregó o se actualizó un nuevo servidor de notificación (por ejemplo, servidor de SMTP)
2	SetInstanceConfiguration	Se agregó o se actualizó un nuevo tipo de notificación (por ejemplo, destino de correo electrónico)
3	SetTemplateDefinition	Se agregó o se actualizó una nueva plantilla
4	RemoveProviderConfiguration	Se eliminó un servidor de notificación
5	RemoveInstanceConfiguration	Se eliminó un tipo de notificación
6	RemoveTemplateDefinition	Se eliminó una definición de plantilla

Número de serie	Nombre de la operación	Significado
7	Confirmar	Se confirmó un cambio en un bean de configuración
8	Establecer	Se estableció un valor de propiedad JMX a través de la vista Explorar de NetWitness Suite

ESA

En la siguiente tabla se indican las operaciones que registra Event Stream Analysis (ESA).

Número de serie	Nombre de la operación	Significado
9	SetSourceRequest	Se agregó o se actualizó un Concentrator a ESA como origen
10	RemoveSourceRequest	Se eliminó un Concentrator de ESA como origen
11	SetEplModule	Se implementó o se actualizó un módulo de EPL en ESA
12	RemoveEplModule	Se eliminó un módulo de EPL de ESA
13	SetEnrichmentSourceRequest	Se agregó/actualizó un origen de enriquecimiento de ESA
14	RemoveEnrichmentSourceRequest	Se eliminó un origen de enriquecimiento de ESA

Número de serie	Nombre de la operación	Significado
15	SetDatabaseReference	Se hizo una referencia a la base de datos de enriquecimiento a ESA
16	UpdateEnrichmentData	Se agregaron filas de datos a un origen de enriquecimiento de ESA
17	SetEnrichmentConnection	Se hizo una conexión entre un módulo de EPL y un origen de enriquecimiento
18	RemoveEnrichmentConnection	Se eliminó una conexión entre un módulo de EPL y un origen de enriquecimiento
19	DisableTrialModule	Se inhabilitaron reglas de prueba de ESA

Investigation

En la siguiente tabla se indican las operaciones que registra Investigations.

Número de serie	Nombre de la operación	Significado
1	VisualizePreferences	Operaciones relacionadas con una solicitud de visualización de Informer.
2	ParallelCoordinates	Operaciones relacionadas con la carga de la navegación en la vista Coordinar.

Número de serie	Nombre de la operación	Significado
3	TimeLine	Operaciones relacionadas con la carga de la navegación en la vista Cronograma.
4	ExteralQuery	Operación cuando se activa una consulta directa a través de la dirección URL.
5	PrintView	Operaciones para abrir Investigation en la vista Imprimir.
6	submitExtractFiles	Operación para enviar una solicitud de extracción de archivos desde sesiones.
7	submitExtractLogs	Operación para enviar una solicitud de extracción de registros desde sesiones.
8	submitExtractPcap	Operación para enviar una solicitud de extracción de sesiones desde sesiones.
9	DataScienceDrill	Operación para investigar desde el informe de Data Science.
10	breadCrumbs	Operación para acceder a las rutas de navegación de consulta.
11	Crear	Operación cuando se guarda una nueva consulta de Investigation como un predicado que se usará para la integración de URL.

Número de serie	Nombre de la operación	Significado
12	userPredicates	Operación para acceder a las consultas recientes de un usuario.
13	chartDefaultMetas	Operación para acceder a los últimos metadatos usados para generar el gráfico de coordenadas.
14	defaultDevice	Operación para acceder al dispositivo de Investigation predeterminado.
15	deleteDefaultDevice	Operación para eliminar el dispositivo de Investigation predeterminado.
16	chartPreferences	Operación para editar los parámetros del gráfico de navegación de Investigation, como la Altura.
17	devicePreferences	Operación para guardar las preferencias del dispositivo de Investigation, como Rango de tiempo, Perfil, Grupos de metadatos, etc.
18	topValues	Operación para obtener los valores principales para los metadatos. Normalmente se llama desde el dashlet Valores principales.
19	MetaLanguages	Operación para leer los idiomas de metadatos desde un dispositivo.

Número de serie	Nombre de la operación	Significado
20	MetaGroups	Operaciones relacionadas con grupos de metadatos de Investigation.
21	DefaultMetaKeys	Operaciones relacionadas con claves de metadatos predeterminadas de Investigation.
22	UpdateDefaultMetaKeys	Operaciones para actualizar claves de metadatos predeterminadas de Investigation.
23	UpdateMetaGroup	Operaciones para actualizar grupos de metadatos de Investigation.
24	ApplyMetaGroup	Operaciones para usar grupos de metadatos de Investigation.
25	DeactivateMetaGroup	Operaciones para restablecer grupos de metadatos de Investigation en la interfaz del usuario.
26	DeleteMetaGroup	Operaciones para quitar el grupo de metadatos de Investigation.
27	DeleteMetaGroups	Operaciones para quitar varios grupos de metadatos de Investigation.
28	ImportMetaGroups	Operaciones para importar grupos de metadatos de Investigation.

Número de serie	Nombre de la operación	Significado
29	ExportMetaGroup	Operaciones para exportar varios grupos de metadatos de Investigation.
30	GeoMap	Operación para acceder a la vista Geomap de Investigation.
31	deleteEndpointCache	Operación para borrar la caché de reconstrucción de un dispositivo.
32	eliminación	Operación para eliminar plantillas de alerta.
33	CustomColumnGroup	Operación para aplicar o leer un grupo de columnas personalizado.
34	Importar	Operaciones relacionadas con la importación de un grupo de columnas o perfiles.
35	Exportar	Operaciones relacionadas con la exportación de un grupo de columnas o perfiles.
36	SaveProfile	Operación para guardar un perfil de Investigation.
37	ApplyProfile	Operación para aplicar un perfil de Investigation.
38	DeactivateProfile	Operación para desactivar un perfil de Investigation.
39	DeleteProfile	Operación para eliminar un perfil de Investigation.

Número de serie	Nombre de la operación	Significado
40	DeleteProfiles	Operación para eliminar varios perfiles de Investigation.

Reporting Engine

En la siguiente tabla se indican las operaciones que registra Reporting Engine.

Número de serie	Nombre de la operación	Significado
1	TEMPLATE	Para todas las operaciones relacionadas con plantillas
2	CHART	Para todas las operaciones relacionadas con gráficos
3	REPORT	Para todas las operaciones relacionadas con informes
4	RULE	Para todas las operaciones relacionadas con reglas
5	IMAGEN	Para todas las operaciones relacionadas con imágenes de logotipo que se usan en los informes.
6	LISTA	Para todas las operaciones relacionadas con listas
7	ALERTA	Para todas las operaciones relacionadas con alertas
8	CONFIG	Para todas las operaciones relacionadas con cambios en la configuración

Número de serie	Nombre de la operación	Significado
9	SCHEDULE	Para todas las operaciones relacionadas con calendarios
10	FUNCIÓN	Para todas las operaciones relacionadas con funciones/autorizaciones
11	BATCH_JOB	Para todas las operaciones relacionadas con trabajos por lotes
12	SCHEDULER	Para todas las operaciones relacionadas con el programador
13	QUERYPROCESSOR	Para todas las operaciones relacionadas con procesadores de consultas
14	FORMATTER	Para todas las operaciones relacionadas con formateadores
15	OUTPUTACTION	Para todas las operaciones relacionadas con acciones de salida
16	STATUSMANAGER	Para todas las operaciones relacionadas con administrador de estado
17	BATCH_RUNDEF	Para todas las operaciones relacionadas con valores predeterminados de ejecución de lote
18	CHARTGROUP	Para todas las operaciones relacionadas con grupos de gráficos

Número de serie	Nombre de la operación	Significado
19	REPORTGROUP	Para todas las operaciones relacionadas con grupos de informes
20	RULEGROUP	Para todas las operaciones relacionadas con grupos de reglas
21	LISTGROUP	Para todas las operaciones relacionadas con grupos de listas
22	DISKSPACE	Para todas las operaciones relacionadas con espacio de disco

Warehouse Connector

En la siguiente tabla se indican las operaciones que registra Warehouse Connector.

Número de serie	Nombre de la operación	Significado
1	Creación de contraseña de Lockbox	Operación para crear la contraseña de Lockbox.
2	Actualización de contraseña de Lockbox	Operación para actualizar la contraseña de Lockbox.
3	Actualización de contraseña de Lockbox	Operación para actualizar la contraseña de Lockbox.
4	Adición de flujo	Operación para agregar un flujo.
5	Adición de origen	Operación para agregar un origen.
6	Adición de destino	Operación para agregar un destino.
7	Eliminación	Operación para quitar un origen, un flujo o un destino.

Número de serie	Nombre de la operación	Significado
8	Cambio de contraseña	Operación para cambiar la contraseña.
9	Actualización de origen	Operación para actualizar un origen.
10	Adición de origen a flujo	Operación para agregar un origen a un flujo.
11	Eliminación de origen de flujo	Operación para eliminar un origen de un flujo.
12	Configuración de destino en flujo	Operación para configurar un destino en un flujo.
13	Finalización de flujo	Operación para finalizar un flujo e iniciar la agregación.
14	Detención de flujo	Operación para detener un flujo.
15	Inicio de flujo	Operación para iniciar un flujo.
16	Recarga de flujo	Operación para volver a cargar un flujo.

Estado y condición

En la siguiente tabla se indican las operaciones que registra Estado y condición.

Número de serie	Nombre de la operación	Significado
1	SavePolicyRequest	Operación mientras se agrega o se modifica una política.
2	RemovePolicyRequest	Operación mientras se quita una política.

NetWitness Suite Servicios principales

En la siguiente tabla se indican las operaciones que registran los servicios de NetWitness Suite Core.

Número de serie	Nombre de la operación	Significado
1	FILE-Command	Operación para enumerar, recuperar y eliminar archivos de directorios aprobados en este dispositivo.
2	SERVICE-Start	Servicio iniciado
3	SERVICE-Stop	Servicio detenido
4	REDIRECT-Syslog	Operación para reenvío de syslog.
5	ADD-Monitor	Emisión de una operación de monitoreo del sistema de archivos
6	DELETE-Monitor	Emisión de una operación de eliminación del sistema de archivos
7	SHUTDOWN-Service/shutdown.service	Apagado del servicio del dispositivo
8	REBOOT-Service	Reinicio del servicio del dispositivo
9	CONFIGURE-Network	Emisión de un cambio en la configuración de la red
10	SET-NTP	Emisión de una operación de configuración de NTP
11	STOP-NTP	Emisión de una operación de detención de NTP

Número de serie	Nombre de la operación	Significado
12	NTP-Timesync	Emisión de una operación de sincronización de hora de NTP
13	SET-SNMP	Emisión de una configuración de SNMP
14	UPGRADE/upgrade	Emisión de una operación de actualización
15	create.collection	Operación para crear una recopilación vacía.
16	restauración	Emisión de una restauración
17	session.aggregation	Emisión de un inicio/detención de agregación
18	add.device	Adición de un dispositivo para agregación
19	edit.device	Edición de un dispositivo que se usa para agregación
20	delete.device	Eliminación de un dispositivo que se usa para agregación
21	capture.start	Inicio de la operación de captura
22	capture.stop	Detención de la operación de captura
23	select.interface	Selección de una interfaz de captura
24	export	Operación para exportar paquetes o sesiones.
25	reload	Emisión de una recarga de analizador

Número de serie	Nombre de la operación	Significado
26	schema	Emisión de una solicitud de esquema para los analizadores cargados
27	upload/file.upload	Emisión de una carga de archivo
28	notify	Emisión de una notificación de feed
29	eliminación	Emisión de una eliminación de archivo
30	edit.config	Operación de cambio en la configuración
31	parsers.transforms	Realización de una transformación de clave de idioma
32	data.reset	Operación de restablecimiento de datos
33	timeout	Tiempo de espera agotado de solicitud REST
34	cancelar	Cancelación de una consulta en ejecución
35	timeroll	Operación para eliminar los archivos de base de datos que superan un determinado límite.
36	volcado	Operación para volcar información fuera de la base de datos en archivos con formato nwd.
37	session.wipe	Emisión de una operación de borrado de sesión

Número de serie	Nombre de la operación	Significado
38	REPLACE-Rule	Emisión de una operación de reemplazo de regla
39	MERGE-Rule	Emisión de una operación de combinación de regla
40	ERASE-Rule	Emisión de la eliminación de un conjunto de todas las reglas
41	ADD-Rule	Emisión de una operación de adición de regla
42	DELETE-Rule	Emisión de la eliminación de un conjunto de reglas
43	sdk.info	Emisión de información de resumen de SDK
44	sdk.session	Emisión de información de sesión de SDK
45	sdk.language	Emisión del lenguaje de SDK
46	sdk.aliases	Emisión de una solicitud de alias de SDK
47	sdk.transform	Emisión de una solicitud de transformación de SDK
48	sdk.search	Emisión de una solicitud de búsqueda de contenido de sesión
49	sdk.cache	Operación relacionada con la caché de contenido de sesión

Número de serie	Nombre de la operación	Significado
50	sdk.content	Emisión de una solicitud de contenido de sesión
51	check.authorization	Operación para comprobar las funciones de usuario relacionadas con permisos de ejecución de una operación.
52	close.connection	Emisión de una operación de cierre de conexión
53	handshake	Emisión de handshake de SSL
54	logon/login	Operación para iniciar sesión desde NW a los demás servicios, principalmente para los usuarios con privilegios.
55	STOREDPROCOP	Emisión de una cancelación/inicio de carga de archivo
56	ADD-Task	Adición de una tarea calendarizada
57	DELETE-Task	Eliminación de una tarea calendarizada
58	logoff	Emisión de una operación de cierre de sesión
59	list.cacerts	Emisión de una operación de enumeración de certificados de CA de confianza

Número de serie	Nombre de la operación	Significado
60	delete.cacerts	Emisión de una operación de eliminación de certificados de CA de confianza
61	add.cacerts	Emisión de una operación de adición de certificados de CA de confianza
62	restart.command	Emisión de la opción de reinicio de la línea de comandos
63	delete.file/file.delete	Operación para eliminar los archivos de configuración del sistema.
64	update.file/file.update	Operación para actualizar el archivo de configuración del sistema.
65	create.file	Emisión de una operación de creación de archivo
66	query	Emisión de una consulta de base de datos
67	desbloquear	Emisión de una operación de desbloqueo de cuenta de usuario
68	user.add	Operación para crear cuentas de usuario en dispositivos individuales.
69	user.delete	Operación para eliminar un usuario en dispositivos individuales.
70	group.create	Operación para agregar un nuevo grupo al sistema.

Número de serie	Nombre de la operación	Significado
71	user.remove	Eliminar una cuenta de usuario de un grupo
72	group.delete	Eliminar un grupo del árbol de usuarios/grupos
73	add.user	Emisión de un comando de adición de usuario a recopilación
74	delete.user	Emisión de un comando de eliminación de usuario de recopilación
75	remove.user	Eliminación de un usuario de una recopilación
76	collection.open	Emisión de un comando de apertura para una recopilación
77	collection.close	Emisión de un comando de cierre para una recopilación
78	collection.delete	Emisión de un comando de eliminación de una recopilación
79	reingest.start	Operación para iniciar nuevamente la recopilación de datos de paquetes en la recopilación.
80	feed.notify	Emisión de un comando de notificación de feed
81	collect	Emisión de un comando de recopilación

Número de serie	Nombre de la operación	Significado
82	collect.start	Emisión de un inicio de recopilación de datos
83	collection.global	Emisión de un comando de importación de analizador
84	parser.reload	Emisión de un comando de recarga de analizador
85	reingest	Operación para volver a recopilar datos de paquetes en la recopilación.
86	collection.create	Emisión de un comando de creación de recopilación
87	collection.restore	Emisión de un comando de restauración de recopilación
88	collection.clone	Emisión de un comando de clonación de recopilación
89	parser.reload	Emisión de un comando de recarga de analizador
90	sdk.query	Ejecuta una consulta contra la base de datos de metadatos
91	sdk.msearch	Busca coincidencias de patrones en muchas sesiones o paquetes
92	sdk.values	Ejecuta una consulta de conteo de valores y devuelve los valores coincidentes para un informe

Número de serie	Nombre de la operación	Significado
93	sdk.timeline	Devuelve el conteo de sesiones/tamaño/paquetes en intervalos de tiempo discretos

Malware Analysis

En la siguiente tabla se indican las operaciones que registra el componente Malware Analysis (MA).

Número de serie	Nombre de la operación	Significado
1	GetDashBoardSummaryRequest	Obtener estadísticas de análisis de tableros
2	GetFileScoreSummaryRequest	Obtener puntajes de archivos agregados por tipo de puntaje y nivel de riesgo
3	CountEventsAndFilesRequest	Obtener el conteo de eventos y archivos en un intervalo de tiempo
4	GetAvVendorDetectionRequest	Obtener resultados de análisis del proveedor de antivirus
5	GetAVVendorsRequest	Obtener la lista de proveedores de antivirus compatibles
6	SetInstalledAVVendors	Solicitar la actualización de la lista de proveedores de antivirus instalados en la configuración

Número de serie	Nombre de la operación	Significado
7	CountEventByCriteriaRequest	Contar eventos por criterios
8	FindEventByIdRequest	Obtener evento por ID
9	FindEventByCriteriaRequest	Obtener evento por criterios
10	DeleteEventRequest	Eliminar evento
11	CommentOnEventRequest	Agregar un comentario a un evento
12	ReSubmitEventRequest	Reenviar un evento para análisis
13	FindEventScoreByIdRequest	Obtener el puntaje del evento por ID de evento
14	FindEventScoreByCriteriaRequest	Obtener el puntaje del evento por criterios
15	FindMetaByIdRequest	Obtener metadatos por ID
16	FindMetaByCriteriaRequest	Obtener metadatos por criterios
17	FindMetaValueByCriteriaRequest	Obtener el valor de metadatos por criterios
18	CountByDistinctMetaValueRequest	Contar valores de metadatos distintos
19	CountByMetaNameAndValueWithDate RangeIntervalRequest	Contar metadatos y valores con intervalo para la creación de gráficos
20	CountByValueAndAverageOverallScore Request	Contar metadatos y mapear a puntajes generales para eventos

Número de serie	Nombre de la operación	Significado
21	CountByValueAndAverageGroupScore Request	Contar metadatos y mapear a puntajes de grupo para eventos
22	CountFileEntryByCriteriaRequest	Contar archivos por criterios
23	FindFileEntryByIdRequest	Obtener archivo por ID
24	FindFileEntryByCriteriaRequest	Obtener archivo por criterios
25	ReSubmitFileEntryRequest	Reenviar un archivo para análisis
26	FileDownloadRequest	Descargar archivo del repositorio
27	FileUploadRequest	Cargar un archivo para análisis
28	FindFileScoreByIdRequest	Obtener puntaje de archivo por ID
29	FindFileScoreByCriteriaRequest	Obtener puntaje de archivo por criterios
30	FindHashValueByIdRequest	Obtener valor de hash de lista blanca/lista negra por ID
31	FindHashValueByCriteriaRequest	Obtener valor de hash de lista blanca/lista negra por criterios
32	AddHashValueRequest	Agregar valor de hash de lista blanca/lista negra
33	UpdateHashValueRequest	Actualizar valor de hash de lista blanca/lista negra
34	DeleteHashValueRequest	Eliminar valor de hash de lista blanca/lista negra
35	FindHashValueByMd5Request	Buscar valor de hash de lista blanca/lista negra por md5

Número de serie	Nombre de la operación	Significado
36	AddHashValueInFileRequest	Agregar el archivo al repositorio y también el valor de hash
37	GetDefaultRulesRequest	Obtener la configuración predeterminada de reglas de IOC
38	ResetToDefaultRulesRequest	Restablecer la configuración de reglas de IOC al valor predeterminado
39	GetAllOverrideRulesRequest	Obtener la configuración de reemplazo creada por el usuario de reglas de IOC
40	FindOverrideRuleByIdRequest	Buscar regla de reemplazo de IOC por ID
41	AddOverrideRuleRequest	Agregar regla de reemplazo de IOC
42	UpdateOverrideRuleRequest	Actualizar regla de reemplazo de IOC
43	DeleteOverrideRuleRequest	Eliminar regla de reemplazo de IOC
44	SubmitOnDemandNextGenRequest	Enviar nuevo escaneo de NextGen según demanda
45	FindOnDemandJobEntryByIdRequest	Obtener entidad de trabajo según demanda por ID
46	FindOnDemandJobEntryByCriteria Request	Obtener entidad de trabajo según demanda por criterios

Número de serie	Nombre de la operación	Significado
47	GetOnDemandJobInfoRequest	Obtener entidad de referencia de trabajo según demanda por ID
48	GetOnDemandDefaultConfiguration	Solicitud para obtener configuración predeterminada según demanda
49	CancelOnDemandJobRequest	Cancelar trabajo según demanda en curso
50	DeleteOnDemandJobRequest	Eliminar un trabajo según demanda
51	ReSubmitOnDemandJobRequest	Reenviar un trabajo según demanda
52	SubscriptionRequest	Suscribirse a la comunicación con la nube de MA
53	UnSubscribeRequest	Cancelar la suscripción a la comunicación con la nube de MA
54	GetTopEventInfluencesRequest	Obtener las N influencias de evento principales
55	GetServerInfoRequest	Obtener información del servidor, como la hora del servidor
56	DataResetRequest	Restablecer la base de datos
57	OnDemandJobStatusNotification	Informar el progreso del trabajo según demanda a los suscriptores
58	LicenseStatusNotification	Informar el estado de la licencia, cantidad de muestras analizadas

Número de serie	Nombre de la operación	Significado
59	DataResetNotification	Informar que se restablecieron los datos
60	GetIocSummaryRequest	Obtener reglas de IOC agregadas por puntajes de evento/archivo
61	FindAlertTemplatesByCriteriaRequest	Obtener plantillas de alerta de rabbitmq por criterios
62	SaveAlertTemplateRequest	Actualizar una plantilla de alerta
63	DeleteAlertTemplateRequest	Eliminar una plantilla de alerta
64	GetJobStatusRequest	Obtener el estado del hilo de ejecución de análisis del trabajo en curso
65	GetEventTypeCountSummaryRequest	Obtener conteos de análisis de evento por gráfico de fecha
66	Inicio de sesión	Iniciar sesión en el servicio de MA
67	Modificada	Modificación de cambios en la configuración
68	GetNextGenSummaryRequest	Obtener estadísticas de resumen del tablero de NextGen

Interfaz del usuario de NetWitness Suite

En la siguiente tabla se indican las operaciones que registra el componente Interfaz del usuario de NetWitness Suite.

Número de serie	Nombre de la operación	Significado
1	uploadTrialLicense	Cargar licencia de prueba
2	LicenseEntitle	Autorizar licencia
3	LicenseDeactivation	Inhabilitar licencia
4	ExpiredLicense	Venció la licencia
5	LicenseOutOfComplianceAcknowledgement	Confirmación de EULA
6	resetLicense	Restablecer licencia
7	usageDateExport	Uso de datos de licencia: csv/pdf
8	refreshLicense	Actualizar licencia de LLS
9	LicenseOutOfCompliance	Incumplimiento de normas
10	OOTBEntitlementOutOfCompliance	Incumplimiento de normas de licencia de prueba OOTB
11	OOTBEntitlementFirstLoginTimeModified	Se modificó la hora de OOTB
12	OOTBEntitlementFileDeleted	Se eliminó el archivo de OOTB
13	OOTBEntitlementDataTampering	Manipulación de datos de OOTB
14	uploadOfflineResponse	Cargar respuesta offline
15	offlineDownloadCapRequest	Descargar solicitud offline

Número de serie	Nombre de la operación	Significado
16	movePerpetualToMetered	Cambiar licencia basada en servicios a medida
17	moveMeteredToPerpetual	Cambiar licencia medida a basada en servicios
18	mapServiceLicense	Mapear servicio a licencia real
19	eliminación	Operación para eliminar plantillas de alerta.
20	HttpRequest	Operación para el registro de auditoría de la dirección URL a la cual se accedió.
21	Página a la cual se accedió	Operación para el registro de auditoría de la página a la cual se accedió.
22	Navegar	Operación para navegar a la página a la cual se accedió.
23	Eventos	Operación para ver la página de evento a la cual se accedió.
24	Recon	Operación para la reconstrucción de evento solicitada.
25	Servicios	Operación al leer la lista de dispositivos disponibles para la investigación.

Número de serie	Nombre de la operación	Significado
26	Servicio	Operación para una lista de dispositivos cuya investigación se solicitó.
27	Recopilaciones	Operación para ver la lista de recopilaciones que se solicitó.
28	Perfiles.	Operación para aplicar un perfil.
29	ColumnGroups	Operación para aplicar o leer un grupo de columnas.
30	ParallelCoordinates	Operaciones relacionadas con la carga de la navegación en la vista Coordinar.
31	Cronograma	Operaciones relacionadas con la carga de la navegación en la vista Cronograma.
32	PrintView	Operaciones para abrir Investigation en la vista Imprimir.
33	Preferencias	Operaciones relacionadas con una solicitud de Informer.

Número de serie	Nombre de la operación	Significado
34	import	Operaciones relacionadas con la importación de un grupo de columnas o perfiles.
35	export	Operaciones relacionadas con la exportación de un grupo de columnas o perfiles.
36	Predicado	Operaciones relacionadas con consultas (predicados) que se usan para Investigation.
37	Idiomas	Operación para el idioma que se solicitó desde un dispositivo.
38	CancelLanguageLoad	Operación para la carga de idioma que se canceló desde la página Navegar.
39	resumen	Operación para un resumen que se solicitó desde un dispositivo.
40	languages	Operación para un idioma que se solicitó desde un dispositivo.

Número de serie	Nombre de la operación	Significado
41	aliases	Operación para alias de metadatos que se solicitaron desde un dispositivo.
42	query	Operación para consulta de SDK que se solicitó desde un dispositivo.
43	msearch	Operación para una búsqueda de metadatos que se solicitó desde un dispositivo.
44	nodeListing	Enumeración de nodos correspondiente a un nodo que se solicitó desde un dispositivo.
45	contenido	Llamada SDK Content que se solicitó desde un dispositivo para la descarga de una PCAP o un registro.
46	Export Files	Enumeración de archivos que se solicitó para una sesión en la vista Archivo o en trabajos de extracción.
47	packets	Paquetes que se solicitaron para sesiones en la vista Paquete o en trabajos de extracción.

Número de serie	Nombre de la operación	Significado
48	deleteEndpointCache	Operación para borrar la caché de reconstrucción de un dispositivo.
49	Inicio de sesión	Operación para que el usuario inicie sesión en la interfaz del usuario de NetWitness Suite.
50	Logoff	Operación para que el usuario cierre sesión en la interfaz del usuario de NetWitness Suite.
51	defaultDevice	Operación para acceder al dispositivo Interfaz del usuario de SA predeterminado.
52	deleteDefaultDevice	Operación para eliminar el dispositivo de Investigation predeterminado.
53	submitExtractFiles	Operación para enviar una solicitud de extracción de archivos desde sesiones.
54	submitExtractLogs	Operación para enviar una solicitud de extracción de registros desde sesiones.

Número de serie	Nombre de la operación	Significado
55	submitExtractPcap	Operación para enviar una solicitud de extracción de sesiones desde sesiones.
56	MetaGroup	Operaciones relacionadas con grupos de metadatos de la interfaz del usuario de SA.
57	ExternalQuery	Operación cuando se activa una consulta directa a través de la dirección URL.
58	GeoMap	Operación para acceder a la vista Geomap de Investigation.
59	SaveProfile	Operación para guardar un perfil de Investigation.
60	ApplyProfile	Operación para aplicar un perfil de Investigation.
61	DeleteProfile	Operación para aplicar un perfil de Investigation.
62	DeactivateProfile	Operación para aplicar un perfil de Investigation.
63	VisualizePreferences	Operaciones relacionadas con una solicitud de visualización de Informer.

Número de serie	Nombre de la operación	Significado
64	ExportMetaGroup	Operaciones para exportar varios grupos de metadatos de la interfaz del usuario de SA.
65	userPredicates	Operaciones para exportar varios grupos de metadatos de la interfaz del usuario de SA.
66	FileView	Operación para la solicitud de reconstrucción para la vista Archivo.
67	resource.update	Operación cuando cambia el estado de suscripción de Live.

Respond

En la siguiente tabla se indican las operaciones que registra el componente RESPOND.

Número de serie	Nombre de la operación	Significado
1	actualizar	Actualizar la configuración de la notificación
2	actualizar	Actualizar la configuración de los ajustes de integración
3	eliminación	Eliminar alertas
4	create	Crear incidente nuevo

Número de serie	Nombre de la operación	Significado
5	actualizar	Actualizar los detalles de incidentes
6	read	Leer los detalles de incidentes
7	eliminación	Eliminar incidentes
8	read	Leer las tareas de corrección
9	eliminación	Eliminar las tareas de corrección
10	actualizar	Actualizar las tareas de corrección
11	create	Crear nueva regla
12	actualizar	Actualizar regla de alerta existente
13	reordenar	Cambiar el orden de prioridad de las reglas de alertas

Ubicaciones de los registros de auditoría locales

NetWitness Suite incluye funcionalidades de registro de auditoría global. Cuando configura el registro de auditoría global, los registros de auditoría de todos los componentes de NetWitness Suite se recopilan en un sistema centralizado, el cual los convierte al formato requerido y los reenvía a un servidor de syslog de terceros o a un Log Decoder.

Para ver los registros de auditoría de cada servicio, puede observar las ubicaciones de los registros de auditoría locales. En la siguiente tabla se muestran las rutas de directorio local de los registros de auditoría correspondientes a la interfaz del usuario de NetWitness Suite y a los diversos servicios de NetWitness Suite.

Servicio/módulo	Ubicación del registro de auditoría
NetWitness Suite Interfaz del usuario de (NetWitness Suite Web Server)	La interfaz del usuario de NetWitness Suite envía registros de auditoría a las siguientes ubicaciones: • **/var/lib/netwitness/uax/logs/audit/audit.log** (formato en lenguaje natural) • Syslog que se ejecuta en el host local (formato JSON) La interfaz del usuario de NetWitness Suite utiliza la funcionalidad AUTH de syslog para escribir registros de auditoría en syslog. Solo puede ver registros de auditoría en la primera ubicación (/var/lib/netwitness/uax/logs/audit/audit.log).
Servicios principales (Decoder, Log Decoder, Concentrator, Broker y Archiver), Log Collector, Warehouse Connector, Workbench e IPDB Extractor	Los servicios principales y los servicios similares envían registros de auditoría a syslog que se ejecuta en el host local. Ruta: **/var/log/secure** (formato JSON) Los servicios principales usan la funcionalidad AUTHPRIV de syslog para escribir registros de auditoría en syslog.

Servicio/módulo	Ubicación del registro de auditoría
Reporting Engine, Malware Analysis, RESPOND y Event Stream Analysis (ESA)	Estos servicios envían registros de auditoría a las siguientes ubicaciones: • **<application home directory>/logs/audit/audit.log** (formato en lenguaje natural) • Syslog que se ejecuta en el host local (formato JSON) Las siguientes son las ubicaciones de los registros de auditoría de estos servicios: Reporting Engine: **/home/rsasoc/rsa/soc/reporting-engine/logs/audit/audit.log** Servidor de Respond /var/log/netwitness/respond-server/respond-server-audit.log Malware Analysis: **/var/lib/netwitness/rsamalware/spectrum/logs/audit/audit.log** Event Stream Analysis: **/opt/rsa/esa/logs/audit/audit.log** Estos servicios usan la funcionalidad AUTH de syslog para escribir registros de auditoría en syslog. Solo puede ver registros de auditoría en la primera ubicación (<application home directory>/logs/audit/audit.log).

Servicio/módulo	Ubicación del registro de auditoría
Estado y condición, Administración de orígenes de eventos (ESM) y Agrupación de dispositivos y servicios (ASG)	Estos servicios envían registros de auditoría a las siguientes ubicaciones: • **/opt/rsa/sms/logs/audit/audit.log** (formato en lenguaje natural) • Syslog que se ejecuta en el host local (formato JSON) Estos servicios usan la funcionalidad AUTH de syslog para escribir registros de auditoría en syslog. Solo puede ver registros de auditoría en la primera ubicación (/opt/rsa/sms/logs/audit/audit.log).

Solución de problemas de configuración del sistema

Los temas de esta sección proporcionan información de solución de problemas para los administradores que están configurando los ajustes que se aplican en todo el sistema en NetWitness Suite.

Solucionar problemas del registro de auditoría global

Solución de problemas de configuración del servidor NTP

Solucionar problemas del registro de auditoría global

En este tema se proporciona información sobre posibles problemas que pueden encontrar los usuarios de NetWitness Suite cuando implementan el registro de auditoría global en NetWitness Suite. Busque explicaciones y soluciones en este tema.

Después de configurar el registro de auditoría global, se deben probar los registros de auditoría para asegurarse de que muestren los eventos de auditoría según se define en la plantilla del registro de auditoría. Si no puede ver los registros de auditoría en el servidor de syslog de otros fabricantes o en un Log Decoder, o si los registros de auditoría no aparecen según lo previsto, busque en las sugerencias básicas de solución de problemas que aparecen a continuación. Si los problemas persisten, puede consultar las sugerencias avanzadas de solución de problemas.

Solución de problemas básica

Si no puede ver registros de auditoría en un servidor de syslog de otros fabricantes o en Log Decoder:

- Verifique que RabbitMQ esté en funcionamiento.
- Verifique la configuración del servidor de notificación de syslog y asegúrese de que esté habilitado.
  (Esta configuración se encuentra en ADMIN > Sistema > Notificaciones globales. No seleccione Notificaciones antiguas).
- Compruebe la configuración del registro de auditoría global.

En Configurar el registro de auditoría global y Verificar registros de auditoría global se proporcionan instrucciones. Si está enviando registros de auditoría a un Log Decoder:

- Asegúrese de que Log Decoder realice la agregación en el Concentrator en el mismo host (ADMIN > Servicios > (seleccione Concentrator) >  > Ver > Configuración).

- Verifique que el analizador de CEF más reciente esté implementado y habilitado.
- Compruebe la plantilla de notificación del registro de auditoría. Debe usar una plantilla de CEF, al igual que todos los registros que alimentan el Log Decoder.

Si está enviando registros de auditoría a un servidor de syslog de otros fabricantes:

- Asegúrese de que un firewall no bloquee el puerto de destino configurado para el servidor de syslog de otros fabricantes.

Solución de problemas avanzada

Para usar el registro de auditoría global en la red, RabbitMQ debe estar en funcionamiento.

Para el registro de auditoría centralizado, cada uno de los servicios de NetWitness Suite escribe registros de auditoría en rsyslog, el cual escucha en el puerto 50514 mediante UDP en el host local. El plug-in de rsyslog que se proporciona en el paquete del registro de auditoría agrega información adicional y carga estos registros en RabbitMQ. Logstash que se ejecuta en el host del Servidor de NetWitness agrega registros de auditoría de todos los servicios de NetWitness Suite, los convierte al formato requerido y los envía a un servidor de syslog de otros fabricantes o a un Log Decoder con fines de investigación. El formato de los registros de auditoría global y el destino que usa Logstash se configuran a través de la interfaz del usuario de NetWitness Suite.

En Definir una configuración del registro de auditoría global se proporcionan instrucciones.

Verificar los paquetes y los servicios en los hosts

NetWitness SuiteHost

Los siguientes paquetes o servicios deben estar presentes en el host del Servidor de NetWitness:

- rsyslog-8.4.1
- rsa-audit-rt
- logstash-1.5.4-1
- rsa-audit-plugins
- rabbitmq server

Servicios en un host además del host de NetWitness Suite

Los siguientes paquetes o servicios deben estar presentes en cada uno de los hosts de NetWitness Suite además del host del Servidor de NetWitness:

- rsyslog-8.4.1
- rsa-audit-rt

- rabbitmq server

Log Decoder

Si reenvía registros de auditoría global a un Log Decoder, el siguiente analizador debe estar presente y habilitado:

- CEF

Posibles problemas

¿Qué sucede si ejecuto una acción en un servicio, pero los registros de auditoría no llegan al servidor de syslog de otros fabricantes o a Log Decoder configurados?

Las causas posibles podrían ser una o todas las siguientes:

- Un servicio no está realizando el registro en el servidor de syslog local.
- Los registros de auditoría no se están cargando en RabbitMQ desde el syslog local.
- Los registros de auditoría no se están agregando en el host del Servidor de NetWitness.
- Los registros agregados en el host del Servidor de NetWitness no se están reenviando al servidor de syslog de otros fabricantes o a Log Decoder configurados.
- El Log Decoder no está configurado para recibir registros de auditoría global en formato CEF:
  - La captura de Log Decoder no está activada
  - El analizador de CEF no está presente
  - El analizador de CEF no está habilitado

Posibles soluciones

En la siguiente tabla se proporcionan posibles soluciones para los problemas.

Problema	Posibles soluciones

Un servicio no está realizando el registro en el servidor de syslog local.	• Asegúrese de que rsyslog esté en funcionamiento.
	Puede usar el siguiente comando:
	`service rsyslog status`
	• Asegúrese de que rsyslog esté escuchando en el puerto 50514 mediante UDP.
	Puede usar el siguiente comando:
	`netstat -tulnp|grep rsyslog`
	• Asegúrese de que la aplicación o el componente estén enviando registros de auditoría al puerto 50514. Ejecute la utilidad tcpdump en la interfaz local para el puerto 50514.
	Puede usar el siguiente comando:
	`sudo tcpdump -i lo -A udp and port 50514`
	
	Consulte *"Ejemplos de soluciones"*, a continuación, para ver las salidas del comando.

Los registros de auditoría no se están cargando en RabbitMQ desde el syslog local.	• Asegúrese de que el plug-in de rsyslog esté en funcionamiento.
	Puede usar el siguiente comando:
	`ps -ef|grep rsa_audit_onramp`
	• Asegúrese de que el servidor de RabbitMQ esté en funcionamiento.
	Puede usar el siguiente comando:
	`service rabbitmq-server status`
	
	Consulte "Ejemplos de soluciones" para ver las salidas del comando.

Problema	Posibles soluciones

Los registros de auditoría no se están agregando en el host del Servidor de NetWitness.	• Asegúrese de que Logstash esté en funcionamiento.
	Puede usar los siguientes comandos:
	`ps -ef|grep logstash`
	`service logstash status`
	• Asegúrese de que el servidor de RabbitMQ esté en funcionamiento.
	Puede usar el siguiente comando:
	`service rabbitmq-server status`
	• Asegúrese de que el servidor de RabbitMQ esté escuchando en el puerto 5672.
	Puede usar el siguiente comando:
	`netstat -tulnp|grep 5672`
	• Compruebe si se generaron errores en el nivel de Logstash.
	Puede usar el siguiente comando para obtener la ubicación de los archivos de registro:
	`ls -l /var/log/logstash/logstash.*`
	Consulte “Ejemplos de soluciones” para ver las salidas del comando.

Problema	Posibles soluciones

Los registros agregados en el host del Servidor de NetWitness no se están reenviando al servidor de syslog de otros fabricantes o a Log Decoder configurados.	• Asegúrese de que Logstash esté en funcionamiento.
	Puede usar los siguientes comandos:
	`ps -ef|grep logstash`
	`service logstash status`
	• Compruebe si se generaron errores en el nivel de Logstash.
	Puede ingresar el siguiente comando para obtener la ubicación de los archivos de registro:
	`ls -l /var/log/logstash/logstash.`
	Consulte “Ejemplos de soluciones”, a continuación, para ver las salidas del comando.
	• Asegúrese de que el servicio de destino esté en funcionamiento.
	• Asegúrese de que el servicio de destino esté escuchando en el puerto correcto y que use el protocolo correcto.
	• Asegúrese de que el puerto configurado en el host de destino no esté bloqueado.

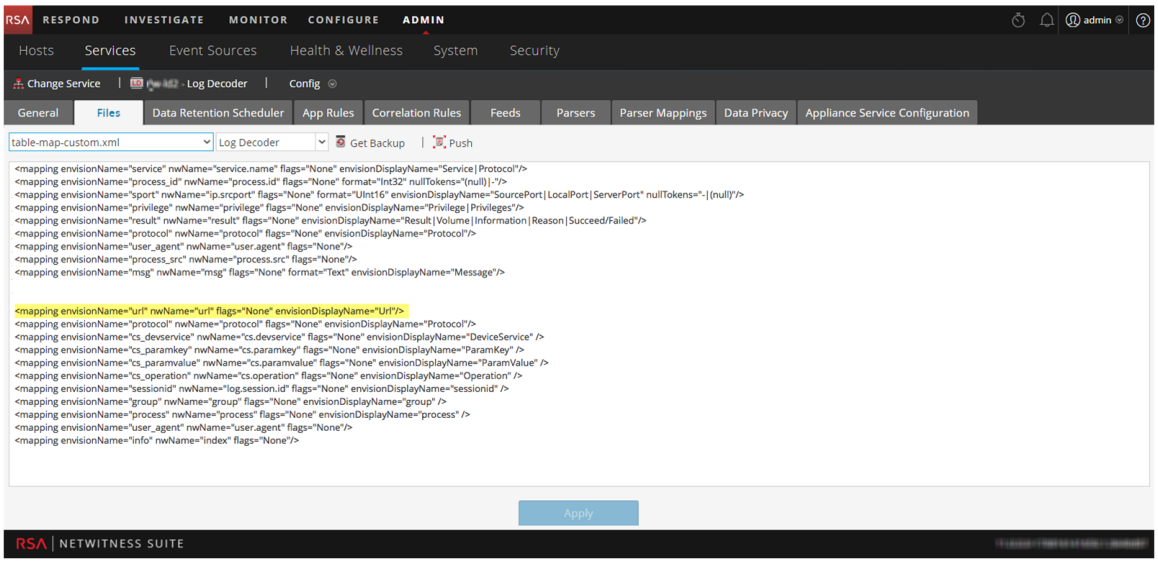
Problema	Posibles soluciones
Los registros de auditoría reenviados desde Logstash causan una falla de análisis en el Log Decoder.	• Asegúrese de estar usando una plantilla de notificación apropiada. Los registros de auditoría que analiza un Log Decoder deben estar en formato CEF. El destino desde el cual los registros de auditoría llegan directa o indirectamente al Log Decoder también debe usar una plantilla de CEF. • La plantilla de notificación debe seguir el estándar CEF. Siga los pasos de esta guía para usar la plantilla de CEF predeterminada o cree una plantilla de CEF personalizada de acuerdo con estrictas reglas. En Definir una plantilla para el registro de auditoría global se proporciona información adicional. • Verifique la configuración de Logstash.

¿Por qué no se pueden ver los metadatos personalizados en Investigation?

Generalmente, si una clave de metadatos no se ve en Investigation, se debe a que no está indexada. Si necesita usar claves de metadatos personalizadas para Investigation y Reporting, asegúrese de que las claves de metadatos que selecciona estén indexadas en el archivo **table-map-custom.xml** en el Log Decoder. Siga el procedimiento “Mantener los archivos de mapa de tablas” para modificar el archivo **table-map-custom.xml** en el Log Decoder.

Asegúrese de que las claves de metadatos personalizadas también estén indexadas en el archivo **index-concentrator-custom.xml** en el Concentrator. En “Editar un archivo de índice de servicios” se proporciona información adicional.

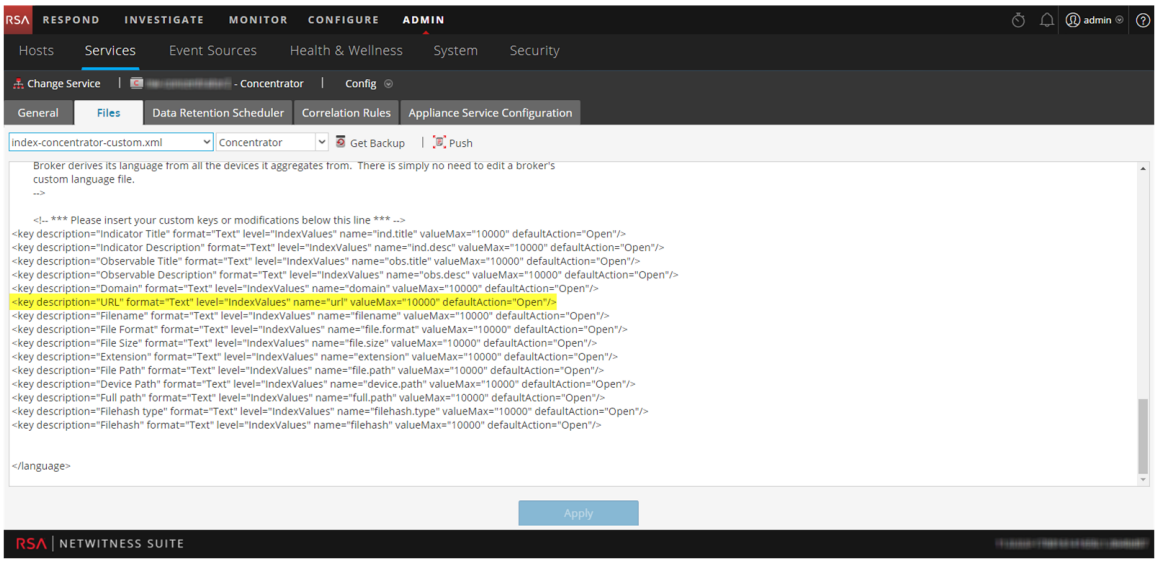
En la siguiente figura se muestra un ejemplo del archivo **table-map-custom.xml** en Servidor de NetWitness (ADMIN > Servicios > (seleccione el Log Decoder) >  >Ver > Configuración) y se resalta un ejemplo de los metadatos personalizados `url`.



El ejemplo de los metadatos personalizados `url` se resalta en el siguiente ejemplo de código del archivo **table-map-custom.xml** anterior:

```
<mapping envisionName="url" nwName="url" flags="None"
envisionDisplayName="Url"/>
<mapping envisionName="protocol" nwName="protocol" flags="None"
envisionDisplayName="Protocol"/><mapping envisionName="cs_devservice"
nwName="cs.devservice" flags="None" envisionDisplayName="DeviceService"
/><mapping envisionName="cs_paramkey" nwName="cs.paramkey" flags="None"
envisionDisplayName="ParamKey" /><mapping envisionName="cs_paramvalue"
nwName="cs.paramvalue" flags="None" envisionDisplayName="ParamValue"
/><mapping envisionName="cs_operation" nwName="cs.operation"
flags="None" envisionDisplayName="Operation" /><mapping
envisionName="sessionid" nwName="log.session.id" flags="None"
envisionDisplayName="sessionid" /><mapping envisionName="group"
nwName="group" flags="None" envisionDisplayName="group" /><mapping
envisionName="process" nwName="process" flags="None"
envisionDisplayName="process" /><mapping envisionName="user_agent"
nwName="user.agent" flags="None"/><mapping envisionName="info"
nwName="index" flags="None"/>
```

En la siguiente figura se muestra un ejemplo del archivo **index-concentrator-custom.xml** en Servidor de NetWitness (ADMIN > Servicios > (seleccione el Concentrator) >  > Ver > Configuración) y se resalta un ejemplo de los metadatos personalizados `url`.



El ejemplo de los metadatos personalizados `url` se resalta en el siguiente ejemplo de código del archivo **index-concentrator-custom.xml** anterior:

```
<key description="Severity" level="IndexValues" name="severity"
valueMax="10000" format="Text"/><key description="Result"
level="IndexValues" name="result" format="Text"/><key
level="IndexValues"  name="ip.srcport" format="UInt16"
description="SourcePort"/><key description="Process" level="IndexValues"
name="process" format="Text"/><key description="Process ID"
level="IndexValues" name="process_id" format="Text"/><key
description="Protocol" level="IndexValues" name="protocol"
format="Text"/><key description="UserAgent" level="IndexValues"
name="user_agent" format="Text"/><key description="DestinationAddress"
level="IndexValues" name="ip.dst" format="IPv4"/><key
description="SourceProcessName" level="IndexValues" name="process.src"
format="Text"/><key description="Username" level="IndexValues"
name="username"  format="Text"/><key description="Info"
level="IndexValues" name="index"  format="Text"/><key
description="customdevservice" level="IndexValues" name="cs.devservice"
format="Text"/>
<key description="url" level="IndexValues" name="url"  format="Text"/>
<key description="Custom Key" level="IndexValues" name="cs.paramkey"
format="Text"/><key description="Custom Value" level="IndexValues"
```

```
name="cs.paramvalue"  format="Text"/><key description="Operation"
level="IndexValues" name="cs.operation"  format="Text"/><key
description="CS Device Service" level="IndexValues" name="cs.device"
format="Text" valueMax="10000" defaultAction="Closed"/>
```

Ejemplos de soluciones

Los siguientes ejemplos de posibles soluciones muestran las salidas de los ejemplos de comandos. Consulte la tabla anterior para obtener la lista completa de posibles soluciones.

Asegúrese de que rsyslog esté en funcionamiento

Puede usar el siguiente comando:

```
service rsyslog status
```

```
[root@NWAPPLIANCE22574 ~]# service rsyslog status
rsyslogd (pid  1293) is running...
[root@NWAPPLIANCE22574 ~]#
```

Asegúrese de que rsyslog esté escuchando en el puerto 50514 mediante UDP

Puede usar el siguiente comando:

```
netstat -tulnp|grep rsyslog
```

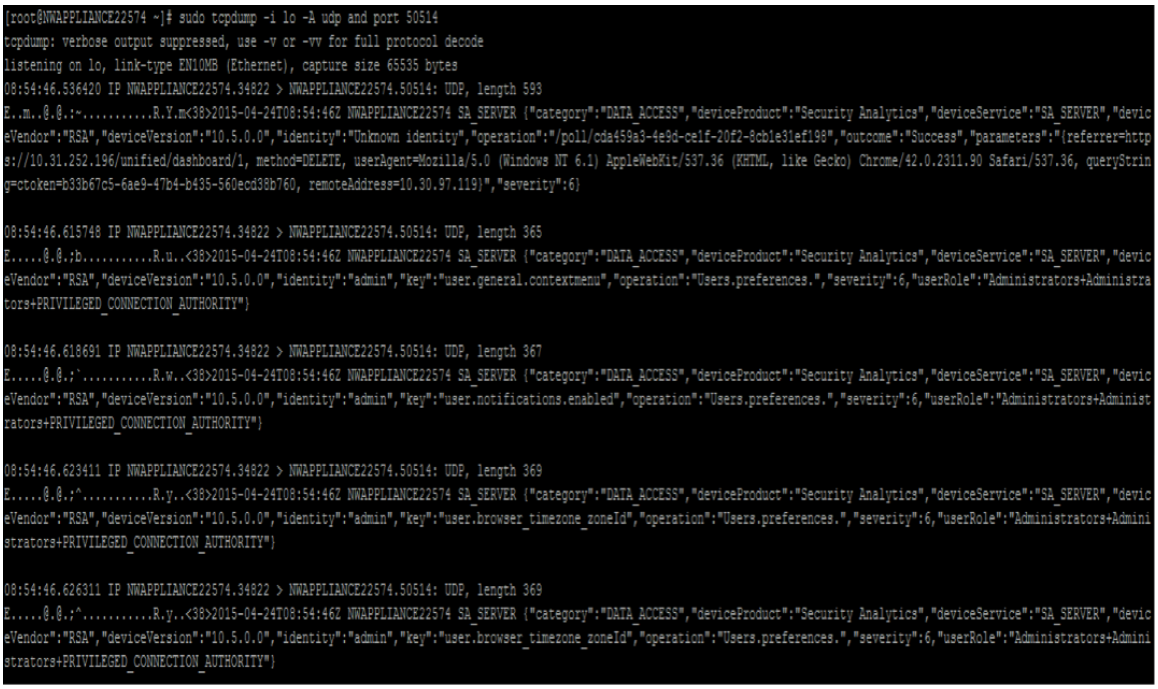
```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep rsyslog
udp        0      0 127.0.0.1:50514           0.0.0.0:*                               1293/rsyslogd
[root@NWAPPLIANCE22574 ~]#
```

Asegúrese de que la aplicación o el componente estén enviando registros de auditoría al puerto 50514

En la siguiente figura se muestra la salida de la ejecución de la utilidad tcpdump en la interfaz local para el puerto 50514.

Puede usar el siguiente comando:

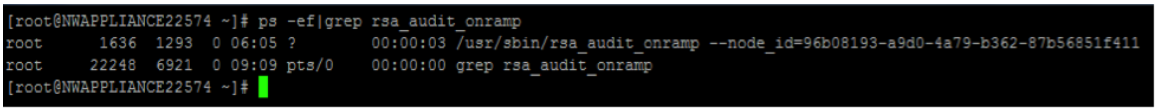
```
sudo tcpdump -i lo -A udp and port 50514
```



Asegúrese de que el plug-in de rsyslog esté en funcionamiento

Puede usar el siguiente comando:

```
ps -ef|grep rsa_audit_onramp
```



Asegúrese de que el servidor de RabbitMQ esté en funcionamiento

Puede usar el siguiente comando:

```
service rabbitmq-server status
```

```
[root@NWAPPLIANCE22574 ~]# service rabbitmq-server status
Status of node sa@localhost ...
[{pid,1862},
 {running_applications,
     [{rabbitmq_federation_management,"RabbitMQ Federation Management",
         "3.4.2"},
      {rabbitmq_management,"RabbitMQ Management Console","3.4.2"},
      {rabbitmq_web_dispatch,"RabbitMQ Web Dispatcher","3.4.2"},
      {webmachine,"webmachine","1.10.3-rmq3.4.2-gite9359c7"},
      {mochiweb,"MochiMedia Web Server","2.7.0-rmq3.4.2-git680dba8"},
      {rabbitmq_federation,"RabbitMQ Federation","3.4.2"},
      {rabbitmq_stomp,"Embedded Rabbit Stomp Adapter","3.4.2"},
      {rabbitmq_management_agent,"RabbitMQ Management Agent","3.4.2"},
      {rabbit,"RabbitMQ","3.4.2"},
      {ssl,"Erlang/OTP SSL application","5.3.2"},
      {public_key,"Public key infrastructure","0.21"},
      {crypto,"CRYPTO version 2","3.2"},
      {asn1,"The Erlang ASN1 compiler version 2.0.4","2.0.4"},
      {os_mon,"CPO  CXC 138 46","2.2.14"},
      {inets,"INETS  CXC 138 49","5.9.7"},
      {mnesia,"MNESIA  CXC 138 12","4.11"},
      {amqp_client,"RabbitMQ AMQP Client","3.4.2"},
      {rabbitmq_auth_mechanism_ssl,
          "RabbitMQ SSL authentication (SASL EXTERNAL)","3.4.2"},
      {xmerl,"XML parser","1.3.5"},
      {sasl,"SASL  CXC 138 11","2.3.4"},
      {stdlib,"ERTS  CXC 138 10","1.19.4"},
      {kernel,"ERTS  CXC 138 10","2.16.4"}]},
 {os,{unix,linux}},
 {erlang_version,
     "Erlang R16B03 (erts-5.10.4) [source] [64-bit] [smp:2:2] [async-threads:30] [kernel-poll:true]\n"},
 {memory,
```

Asegúrese de que Logstash esté en funcionamiento

Puede usar los siguientes comandos:

```
ps -ef|grep logstash
service logstash status
```

```
[root@NWAPPLIANCE22574 ~]# ps -ef|grep logstash
logstash  1583     1  0 06:05 ?       00:01:09 /usr/bin/java -Djava.io.tmpdir=/var/lib/logstash -Xmx500m -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -Djava.awt.headless=true -XX:C
MSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -jar /opt/logstash/vendor/jar/jruby-complete-1.7.11.jar -I/opt/logstash/lib /opt/logstash/lib/logstash/runner
.rb agent --pluginpath /opt/logstash -f /etc/logstash/conf.d -l /var/log/logstash/logstash.log
root      8509  6921  0 09:31 pts/0    00:00:00 grep logstash
[root@NWAPPLIANCE22574 ~]# service logstash status
logstash is running
[root@NWAPPLIANCE22574 ~]#
```

Asegúrese de que el servidor de RabbitMQ esté escuchando en el puerto 5672

Por ejemplo, escriba el siguiente comando:

```
netstat -tulnp|grep 5672
```

```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep 5672
tcp        0      0 127.0.0.1:5672              0.0.0.0:*                   LISTEN      1862/beam.smp
tcp        0      0 0.0.0.0:25672               0.0.0.0:*                   LISTEN      1862/beam.smp
[root@NWAPPLIANCE22574 ~]#
```

Compruebe si se generaron errores en el nivel de Logstash

Puede ingresar el siguiente comando para obtener la ubicación de los archivos de registro:

```
ls -l /var/log/logstash/logstash.*
```

```
[root@NWAPPLIANCE22574 ~]# ls -l /var/log/logstash/logstash.*
-rw-r--r--. 1 root     root        0 Apr 24 06:05 /var/log/logstash/logstash.err
-rw-r--r--. 1 logstash logstash 1043 Apr 24 06:04 /var/log/logstash/logstash.log
-rw-r--r--. 1 root     root       57 Apr 24 06:12 /var/log/logstash/logstash.stdout
[root@NWAPPLIANCE22574 ~]#
```

Consulte la tabla anterior Posibles soluciones para obtener la lista completa de problemas y posibles soluciones.

Solución de problemas de configuración del servidor NTP

En este tema se describen los problemas de configuración del servidor NTP que puede encontrar y se sugieren soluciones para abordarlos.

Problemas identificados en mensajes del panel Configuración de NTP o de los archivos de registro

En esta sección se proporciona información de solución de problemas para los problemas identificados en los mensajes que NetWitness Suite muestra en el panel Configuración de NTP y en los archivos de registro.

Mensaje	Interfaz del usuario: **Se produjo un error inesperado. En primer lugar compruebe los registros y, a continuación, póngase en contacto con atención al cliente para resolver el error.** **System Log:** **Timestamp Level Message** *yyyy-dd-mm*Thh:mm:ss:ms ERROR com.rsa.smc.sa.adm.exception.MCOAgent Exception: No request sent, we did not discover any nodes
Causa posible	La configuración de NetWitness Suite de nivel bajo está incorrecta o el servicio de soporte no se está ejecutando.
Solución	Póngase en contacto con el servicio al cliente.
Mensaje	Interfaz del usuario: **Se especificó una sintaxis de nombre de host no válida**.
Causa posible	Intentó ingresar un nombre de host del servidor NTP que no cumple con la sintaxis de nombre de dominio calificado o dirección IP.
Solución	Vuelva a ingresar el nombre de host con la sintaxis correcta.
Mensaje	Interfaz del usuario: **Servidor NTP especificado ya existe.**
Causa posible	Intentó ingresar un nombre de host de servidor NTP que ya está definido en NetWitness Suite.

Solución	Ingrese el nombre de host de un servidor NTP que no está configurado en NetWitness Suite.
Mensaje	Interfaz del usuario: **No puede conectarse con el *nombre de host* del servidor NTP**. Verifique la dirección del servidor y compruebe la configuración del firewall.
Causa posible	Los ajustes de la dirección del servidor o firewall pueden estar incorrectos.
Solución	Verifique la dirección del servidor y la configuración del firewall, y corríjalos si es necesario.

Referencias

En este tema se proporcionan materiales de referencia que describen la interfaz del usuario para configurar ajustes del sistema en NetWitness Suite y definir parámetros. Los administradores usan las opciones de la vista Sistema de Administration para configurar ajustes del sistema. Cada panel se describe en un tema aparte.

- Panel Configuraciones de registro de auditoría global
- Panel Notificaciones globales
  - Cuadros de diálogo de definición de servidores de notificación
  - Cuadros de diálogo de definición de salida de notificación
  - Cuadro de diálogo Definir plantilla de notificación
  - Pestaña Salida
  - Pestaña Servidores
  - Pestaña Plantillas
- Panel Configuración de proxy HTTP
- Panel Configuración de correo electrónico
- Panel Configuración de ESA
- Panel Configuración de Investigation
- Panel Configuración de servicios de Live
- Panel Configuración de NTP
- Panel Acciones del menú contextual
- Panel Configuración de notificaciones antiguas

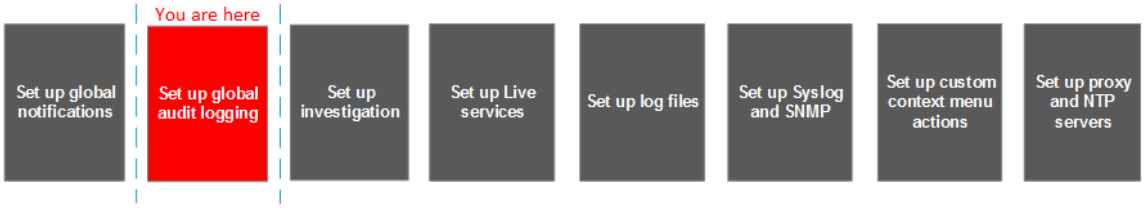
Panel Configuraciones de registro de auditoría global

El panel **Configuraciones de log de auditoría global** (Admin > Sistema > Auditoría global) permite configurar el registro de auditoría global mediante la adición de configuraciones que definen la forma en que los registros de auditoría global se reenvían a sistemas de syslog externos. Los registros de auditoría global se reenvían al servidor de notificación seleccionado en la configuración del registro de auditoría global mediante el uso de la plantilla de notificación seleccionada.

El registro de auditoría global proporciona a los auditores la visibilidad consolidada en tiempo real de las actividades de los usuarios dentro de NetWitness Suite desde una ubicación centralizada.

Flujo de trabajo

En este flujo de trabajo se muestran los procedimientos necesarios para configurar y verificar el registro de auditoría global.



Antes de poder definir una configuración del registro de auditoría global, debe crear un servidor de notificación de syslog en Notificaciones globales > pestaña Servidor. El servidor de notificación de syslog es el destino que recibe los registros de auditoría global. A continuación, debe seleccionar o definir una plantilla del registro de auditoría en Notificaciones globales > pestaña Plantillas. La plantilla del registro de auditoría define el formato y los campos de mensajes de los registros de auditoría que se envían al Log Decoder o al servidor de syslog de otros fabricantes. Si consume con un Log Decoder, implemente el analizador del formato de evento común en el Log Decoder desde Live.

Nota: No es necesario configurar ajustes en Notificaciones globales > pestaña Salida para el registro de auditoría global.

Después de agregar una configuración del registro de auditoría global aquí, los registros de auditoría se reenvían al servidor de notificación seleccionado en la configuración. Verifique los registros de auditoría para asegurarse de que muestren los eventos de auditoría definidos en la plantilla del registro de auditoría.

¿Qué desea hacer?

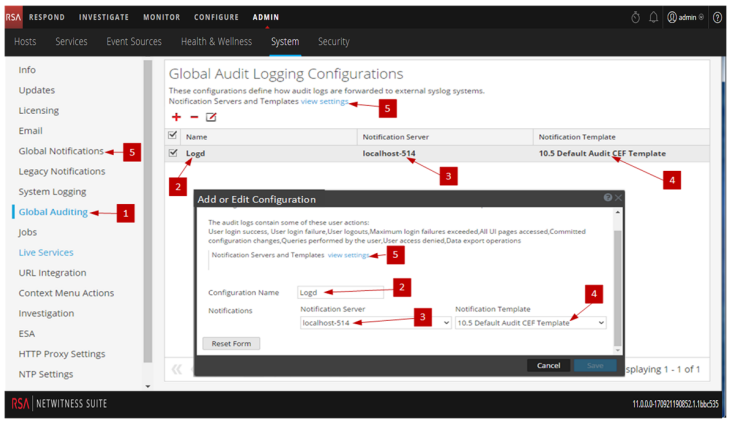
Función	Deseo…	Mostrarme cómo
Administrador	Crear un servidor de notificación de syslog.	Configurar un destino para recibir registros de auditoría global
Administrador	Elegir una plantilla del registro de auditoría.	Definir una plantilla para el registro de auditoría global
Administrador	Configurar el registro de auditoría global	Definir una configuración del registro de auditoría global Para conocer el procedimiento completo, consulte "Registro de auditoría global: procedimiento general" en Configurar el registro de auditoría global.
Administrador	Verificar registros de auditoría global	Verificar registros de auditoría global

Temas relacionados

- Solucionar problemas del registro de auditoría global
- Cuadro de diálogo Agregar nueva configuración
- Claves de metadatos de CEF compatibles
- Variables de claves de metadatos del registro de auditoría global compatibles
- Referencia de operaciones del registro de auditoría global
- Ubicaciones de los registros de auditoría locales

Vista rápida

En el siguiente ejemplo se ilustra una configuración del registro de auditoría global. La configuración define la forma en que NetWitness Suite reenvía los registros de auditoría global a sistemas de syslog externos.



1 Se muestra el panel Configuraciones de log de auditoría global.

2 Nombre que identifica la configuración del registro de auditoría global.

3 Servidor de notificación asignado a la configuración del registro de auditoría global.

4 Plantilla de notificación asignada a la configuración del registro de auditoría global.

5 Muestra el panel Notificaciones globales, en el cual se configuran las plantillas y los servidores necesarios para establecer una configuración del registro de auditoría global.

Barra de herramientas

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

Ícono	Descripción
+	Agrega una configuración del registro de auditoría global.
−	Elimina una configuración del registro de auditoría global. La eliminación de una configuración de auditoría global no elimina el servidor ni la plantilla de notificación asociados. Después de que se elimina una configuración del registro de auditoría global, se interrumpe el reenvío de registros de auditoría global especificados en esa configuración.

Ícono	Descripción
	Edita una configuración del registro de auditoría global. Puede cambiar el destino de los registros de auditoría global para las auditorías de los usuarios mediante la selección de otro servidor de notificación. También puede cambiar el formato y los campos de mensajes de las entradas del registro de auditoría global, para lo cual debe elegir otra plantilla de notificación. No puede cambiar las acciones de los usuarios de NetWitness Suite que se registran y se envían en los registros de auditoría global.

Configuraciones

En la siguiente tabla se describen las configuraciones enumeradas.

Título	Descripción
	Para seleccionar una configuración individual, seleccione la casilla de verificación junto a la configuración. Para seleccionar todas las configuraciones, seleccione la casilla de verificación de la barra de título de la tabla.
Nombre	Muestra el nombre de la configuración de la auditoría global. Por ejemplo, puede asignar nombres a las configuraciones en función del destino de los registros de auditoría global, como HQ SA y Mi servidor de syslog.
Servidor de notificación	Muestra el servidor de notificación de syslog seleccionado como el destino para los registros de auditoría global. Si desea reenviar registros de auditoría global a Log Decoder, cree el tipo de syslog Servidor de notificación. En Configurar un destino para recibir registros de auditoría global se proporcionan instrucciones para crear un servidor de notificación de syslog para el registro de auditoría global.

Título	Descripción
Plantilla de notificación	Muestra la plantilla de notificación del registro de auditoría seleccionada para la configuración. Define el formato y los campos de mensajes de las entradas del registro de auditoría. Para Log Decoders, use **Default Audit CEF Template**. Puede agregar o quitar campos de la plantilla del formato de evento común (CEF) si tiene requisitos específicos. En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones y en Claves de metadatos de CEF compatibles se describen las claves de metadatos de CEF disponibles. Para servidores de syslog de otros fabricantes, puede usar una plantilla del registro de auditoría predeterminada o definir un formato propio (CEF o no CEF). En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones y en Variables de claves de metadatos del registro de auditoría global compatibles se describen las variables de claves de metadatos disponibles.

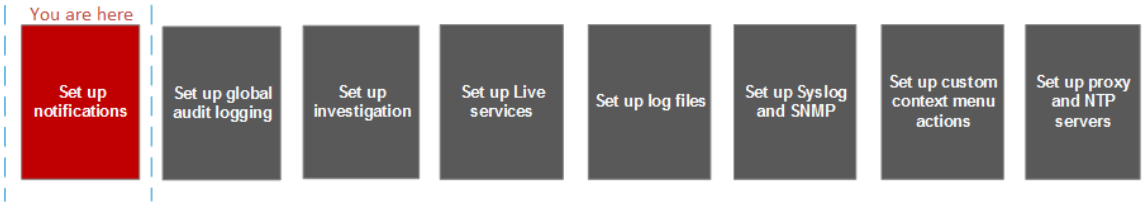
Panel Notificaciones globales

En el panel Notificaciones globales se presentan las funciones para la configuración de ajustes de notificación. Las configuraciones de las notificaciones globales definen los ajustes de las notificaciones para Administración de orígenes de eventos (ESM), Estado y condición, el registro de auditoría global, Event Stream Analysis (ESA) y RESPOND.

El panel Notificaciones globales permite configurar los siguientes ajustes globales de notificación:

- Salidas de notificación
- Servidores de notificación
- Plantillas

Flujo de trabajo



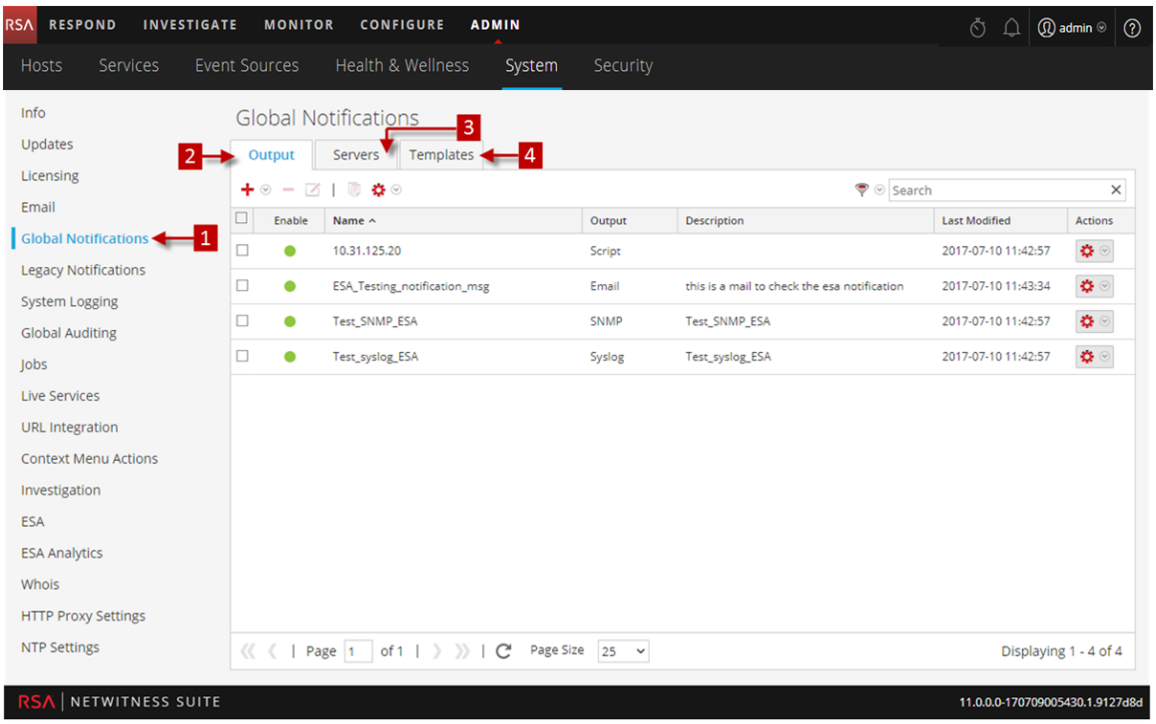
¿Qué desea hacer?

Función	Deseo...	Mostrarme cómo
Administrador	Configurar servidores de notificación	Pestaña Servidores
Administrador	Configurar las salidas de las notificaciones	Pestaña Salida
Administrador	Configurar plantillas de notificación	Pestaña Plantillas

Temas relacionados

- Configurar un servidor de notificación de syslog
- Configurar un script como un servidor de notificación

Vista rápida



1 Muestra el panel Notificaciones globales.

2 Muestra la pestaña Salida.

3 Muestra la pestaña Servidores.

4 Muestra la pestaña Plantillas.

Barra de herramientas y funciones

El panel Notificaciones globales tiene tres pestañas: Salida, Servidores y Plantillas.

Función	Descripción
Pestaña Salida	Esta pestaña permite configurar salidas de notificaciones. Consulte Pestaña Salida para obtener más información.
Pestaña Servidores	Esta pestaña permite configurar servidores de notificación. Consulte Pestaña Servidores para obtener más información.
Pestaña Plantillas	Esta pestaña permite configurar plantillas de notificación. Consulte Pestaña Plantillas para obtener más información.

En esta tabla se describen las columnas de la cuadrícula para las salidas y los servidores de notificación.

Columna	Descripción
	Seleccione una fila de una acción de la barra de herramientas. Al hacer clic en la casilla de verificación del título de la columna, se seleccionan o deseleccionan todas las filas de la cuadrícula.
Habilitar	Indica si la configuración está habilitada. Un círculo de color verde indica que la configuración está habilitada. Un círculo de color blanco indica que una configuración no está habilitada.
Nombre	Nombre que identifica o etiqueta la configuración.
Salida	La salida de la configuración. Las salidas son Correo electrónico, SNMP, Syslog y Script.
Descripción	Descripción breve sobre la configuración.
Última modificación	Muestra la fecha y la hora del último cambio en la configuración.
Acciones	Proporciona un menú Acciones  para la configuración seleccionada, con acciones que se pueden aplicar a la configuración. El menú Acciones permite eliminar, editar, duplicar y exportar la configuración.

En esta tabla se describen las columnas de la cuadrícula para las plantillas de notificación.

Columna	Descripción
	Seleccione una fila de una acción de la barra de herramientas. Al hacer clic en la casilla de verificación del título de la columna, se seleccionan o deseleccionan todas las filas de la cuadrícula.
Nombre	Nombre que identifica o etiqueta la plantilla.
Tipo de plantilla	El tipo de plantilla. Los tipos son Registro de auditoría, Event Stream Analysis, Monitoreo de orígenes de eventos y Alarmas de estado.
Descripción	Descripción breve sobre la plantilla.

Columna	Descripción
Acciones	Proporciona un menú Acciones para la configuración seleccionada, con acciones que se pueden aplicar a la plantilla. El menú Acciones permite eliminar, editar, duplicar y exportar la plantilla.

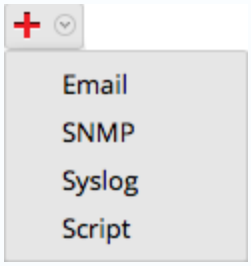
Barra de herramientas del panel Notificaciones globales

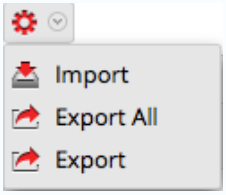
La barra de herramientas del panel Notificaciones globales está en la parte superior de las pestañas Salida, Servidores y Plantillas.

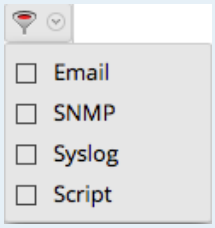
En la siguiente figura se muestra la barra de herramientas de las pestañas Salida y Servidores.

En la siguiente figura se muestra la barra de herramientas de la pestaña Plantillas.

En la siguiente tabla se describen las funciones de la barra de herramientas del panel Notificaciones globales.

Función	Descripción
	Agrega un servidor de notificación en la pestaña Servidores, una salida de notificación (notificación) en la pestaña Salida y una plantilla de notificación en la pestaña Plantillas. En las pestañas Servidores y Salida, puede optar por configurar los ajustes de notificación Correo electrónico, SNMP, Syslog y Script.
	

Función	Descripción
	Quita una configuración de notificación seleccionada. No puede eliminar servidores de notificación y tipos de notificaciones asociados con configuraciones del registro de auditoría global. Si intenta eliminar una salida de notificación (notificación) que se usa en alertas, recibirá un mensaje de confirmación de advertencia que señala que las alertas que usan la notificación no funcionarán correctamente. El mensaje muestra la cantidad de alertas en uso. También puede eliminar una configuración si la selecciona y, a continuación, en la columna Acciones, elige  > Eliminar.
	Edita una configuración de notificación seleccionada. También puede editar una configuración si la selecciona y, a continuación, en la columna Acciones, elige > Editar.
	Duplica una configuración de notificación seleccionada. También puede duplicar una configuración si la selecciona y, a continuación, en la columna Acciones, elige  > Duplicar.
	Muestra las siguientes opciones: • **Importar**: importa un servidor, un tipo o una plantilla de notificación. Por ejemplo, en la pestaña Servidores, puede importar una configuración de servidor de notificación. • **Exportar todo**: exporta todas las configuraciones. Por ejemplo, si está en la pestaña Servidores, puede exportar todas las configuraciones de servidores de notificación. • **Exportar**: Exporta una configuración seleccionada. También puede exportar una configuración si la selecciona y, a continuación, en la columna Acciones, elige  > Exportar.

Función	Descripción
	Filtra por correo electrónico, SNMP, syslog o script.
	Busca configuraciones en la cuadrícula.

Cuadros de diálogo de definición de servidores de notificación

En este tema se describen los cuadros de diálogo de definición de servidores de notificación que se usan para configurar los ajustes de los diversos tipos de servidores de notificación. Los servidores de notificación se configuran en Administration > Sistema > Notificaciones > pestaña Servidores.

Las notificaciones se usan en diversos componentes de NetWitness Suite, como Event Stream Analysis (ESA), RESPOND y el registro de auditoría global. Los ajustes de notificaciones se denominan servidores de notificación. La pestaña Servidores del panel Notificaciones de la vista Sistema de Administration permite crear varias configuraciones de servidores de notificación.

Puede configurar los siguientes tipos de ajustes de servidores de notificación en NetWitness Suite:

- Correo electrónico
- SNMP
- Syslog
- Script

Para el registro de auditoría global, solo puede usar servidores de notificación de syslog.

Los procedimientos relacionados con servidores de notificación se describen en Configurar servidores de notificación.

Para acceder a los cuadros de diálogo de definición de servidores de notificación:

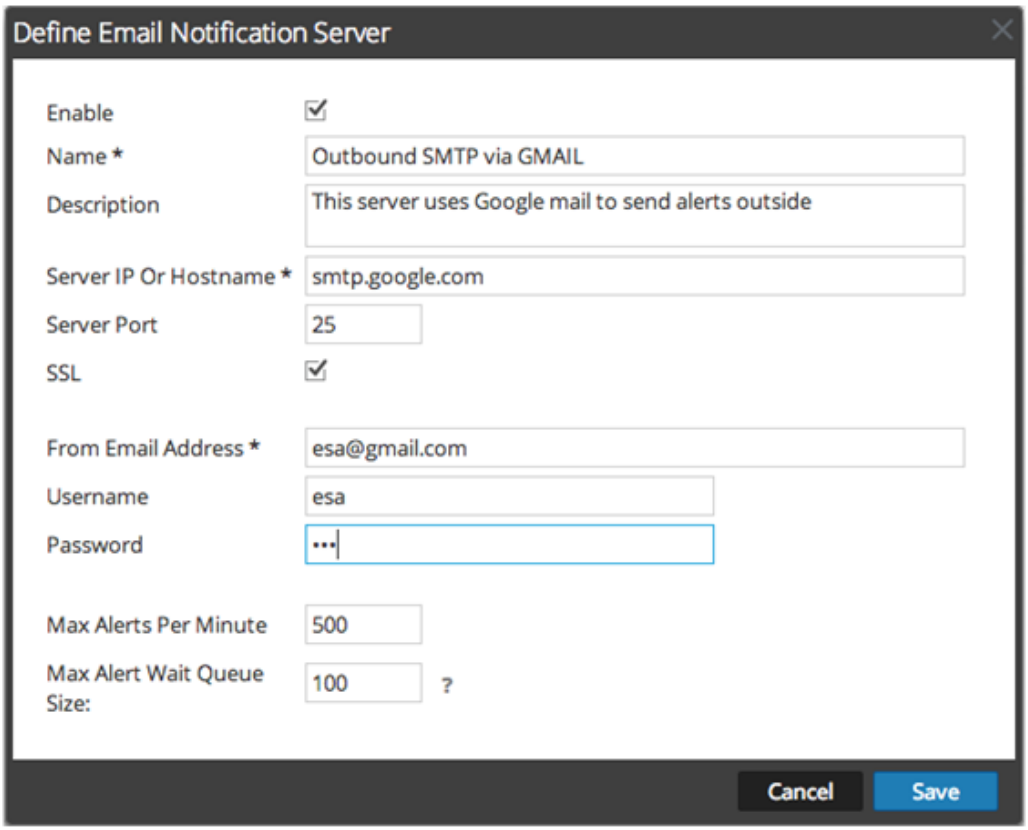
1. Vaya a **ADMIN > Sistema**.
2. En el panel de navegación izquierdo, seleccione **Notificaciones globales**.
3. En el panel **Servidores de notificación**, haga clic en + y, a continuación, seleccione el tipo de servidor de notificación (Correo electrónico, SNMP, Syslog o Script)
   El cuadro de diálogo Definir servidor de notificación se muestra para su selección.

Hay cuatro cuadros de diálogo de servidores de notificación, los cuales permiten configurar los servidores de notificación.

Correo electrónico

Los servidores de notificación por correo electrónico permiten configurar ajustes de servidores de correo electrónico para enviar notificaciones de alertas.

En la siguiente figura se muestra el cuadro de diálogo Definir servidor de notificación de correo electrónico.



En la siguiente tabla se indican los diversos parámetros que se deben definir para los servidores de notificación de correo electrónico.

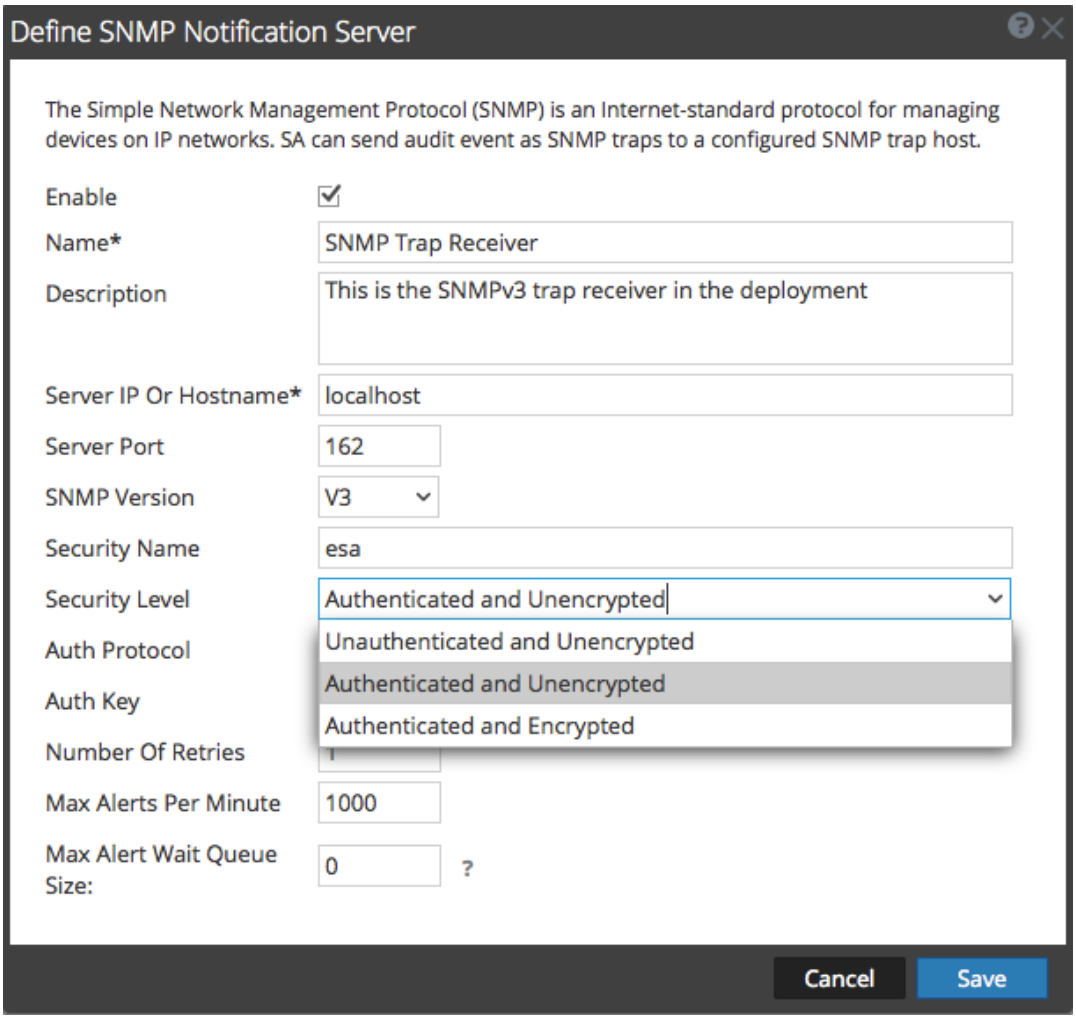
Parámetros	Descripción
Habilitar	Seleccione esta opción para activar el servidor de notificación.
Nombre	Nombre para identificar o etiquetar el servidor de notificación.
Descripción	Descripción breve del servidor de notificación.
Dirección IP o nombre de host del servidor	Nombre de host del servidor de correo electrónico. Para notificaciones de ESM/SMS y ESA, debe especificar solo el nombre de host/nombre de dominio calificado.
Puerto del servidor	El puerto del servidor.

Parámetros	Descripción
SSL	Seleccione esta opción para comunicarse a través del protocolo SSL.
Dirección de correo electrónico de remitente	Cuenta de correo electrónico desde la cual desea enviar notificaciones por correo electrónico.
Nombre de usuario	Nombre de usuario para iniciar sesión en la cuenta de correo electrónico si el servidor SMTP requiere autenticación de usuario para retransmitir correctamente los correos electrónicos.
Contraseña	Contraseña del usuario para iniciar sesión en la cuenta de correo electrónico si el servidor SMTP requiere autenticación de usuario para retransmitir correctamente los correos electrónicos.
Máximo de alertas por minuto	Describe la cantidad máxima de alertas por minuto.
Tamaño de línea de espera máximo de alertas	Describe la cantidad máxima de alertas que se pondrán en línea de espera antes de que se descarten.

SNMP

Los servidores de notificación de SNMP permiten configurar ajustes de host de SNMP trap como un servidor de notificación para enviar notificaciones de alertas.

En la siguiente figura se muestra el cuadro de diálogo Definir servidor de notificación de SNMP.



En la siguiente tabla se indican los diversos parámetros que debe definir para los servidores de notificación de SNMP.

Parámetros	Descripción
Habilitar	Seleccione esta opción para activar el servidor de notificación.
Nombre	Nombre para identificar o etiquetar el servidor de notificación.
Descripción	Descripción breve del servidor de notificación.

Parámetros	Descripción
Dirección IP o nombre de host del servidor	Dirección IP o nombre de host de SNMP trap.
Puerto del servidor	Número de puerto de escucha del host SNMP trap.

<table>
<tr><th>Parámetros</th><th>Descripción</th></tr>
<tr><td>Versión de SNMP</td><td>Versión de SNMP. Estas son las opciones:
V1
V2C
V3
Si selecciona la versión 3 (v3) de SNMP, se muestran los siguientes parámetros:

<table><tr><th>Parámetros</th><th>Descripción</th></tr><tr><td>Tipo de notificación</td><td>En función del tipo de notificación, se envían mensajes SNMP cada vez que se genera una alerta.
Se admiten los siguientes tipos de notificación:
Inform: Inform es una trap confirmada. El remitente obtiene una confirmación del receptor.
Trap: Trap es notificación no confirmada.</td></tr><tr><td>ID de motor autorizado (este opción está disponible solo para el tipo de notificación TRAP)</td><td>Un identificador que se utiliza para identificar a los agentes. El ID de motor autorizado junto con el nombre de usuario se utilizan para identificar al agente de manera exclusiva.</td></tr><tr><td>Nivel de seguridad</td><td>Defina el nivel de seguridad. Estas son las opciones:
No autenticado y no cifrado
Autenticado y no cifrado
Autenticado y cifrado</td></tr></table></td></tr>
</table>

Parámetros	Descripción	
	Protocolo de autenticación (esta opción está disponible solo para los niveles de seguridad Autenticado y no cifrado, y Autenticado y cifrado)	Protocolo de autenticación que se usa para validar a un usuario antes de proporcionar un acceso al servidor. Las opciones son: • SHA • MD5
	Clave de autenticación (esta opción está disponible solo para los niveles de seguridad Autenticado y no cifrado, y Autenticado y cifrado)	Una contraseña que desea utilizar para la autenticación.
	Protocolo de privacidad (esta opción está disponible solo para el nivel de seguridad Autenticado y cifrado)	El protocolo de privacidad es una técnica de cifrado para la comunicación de datos.
	Clave privada (esta opción está disponible solo para el nivel de seguridad Autenticado y cifrado)	Una contraseña que desea usar para el cifrado.
Comunidad	Cadena de Community que se usa para autenticación en el host de SNMP trap. El valor predeterminado es **público**.	
Número de reintentos	Número de reintentos del trap.	

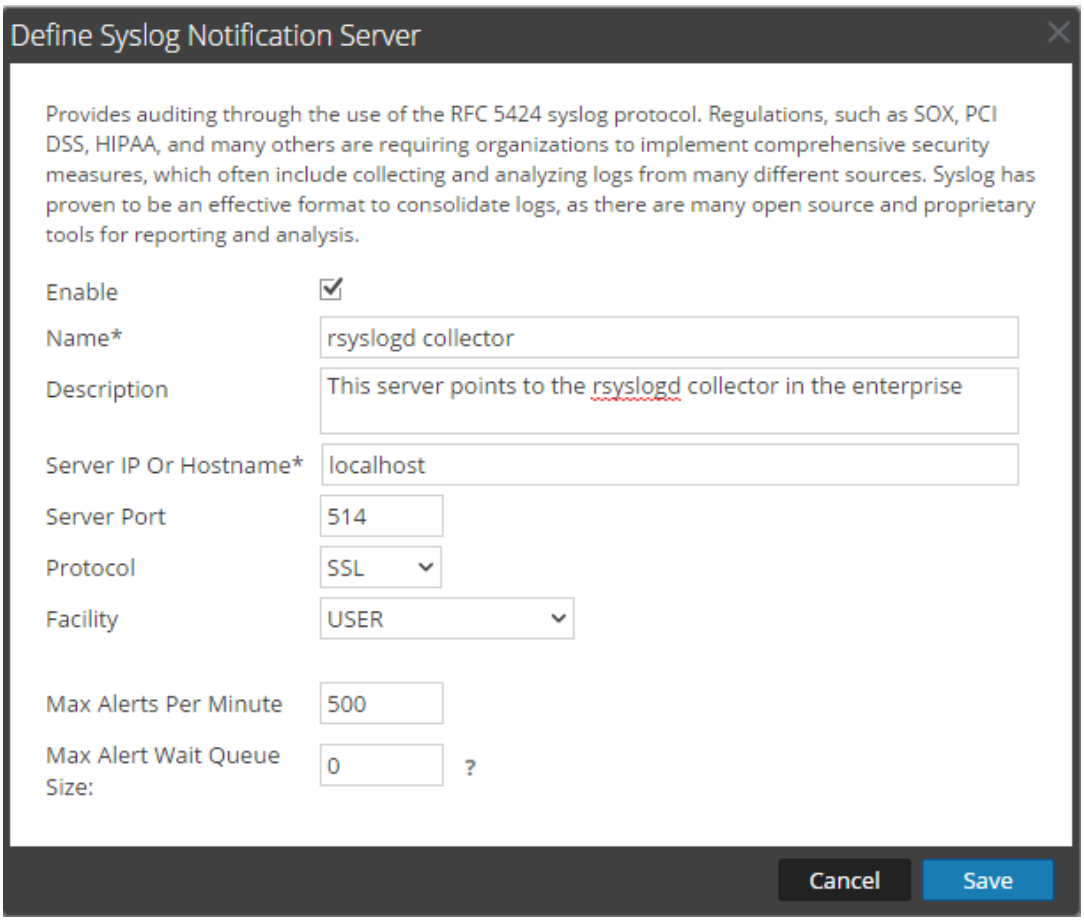
Parámetros	Descripción
Máximo de alertas por minuto	Cantidad máxima de alertas por minuto.
Tamaño de línea de espera máximo de alertas	Cantidad máxima de alertas que se pondrán en línea de espera antes de que se descarten.

Syslog

Los servidores de notificación de syslog permiten configurar ajustes de syslog como un servidor de notificación para enviar notificaciones. Cuando está activado, syslog proporciona auditoría mediante el uso del protocolo RFC 5424 de syslog. Syslog ha demostrado ser un formato eficaz para consolidar registros, dado que existen muchas herramientas patentadas o de código abierto para generar informes y análisis.

No puede inhabilitar servidores de notificación asociados a configuraciones del registro de auditoría global.

En la siguiente figura se muestra el cuadro de diálogo Definir servidor de notificación de syslog.



En la siguiente tabla se indican los diversos parámetros que se deben definir los servidores de notificación de syslog.

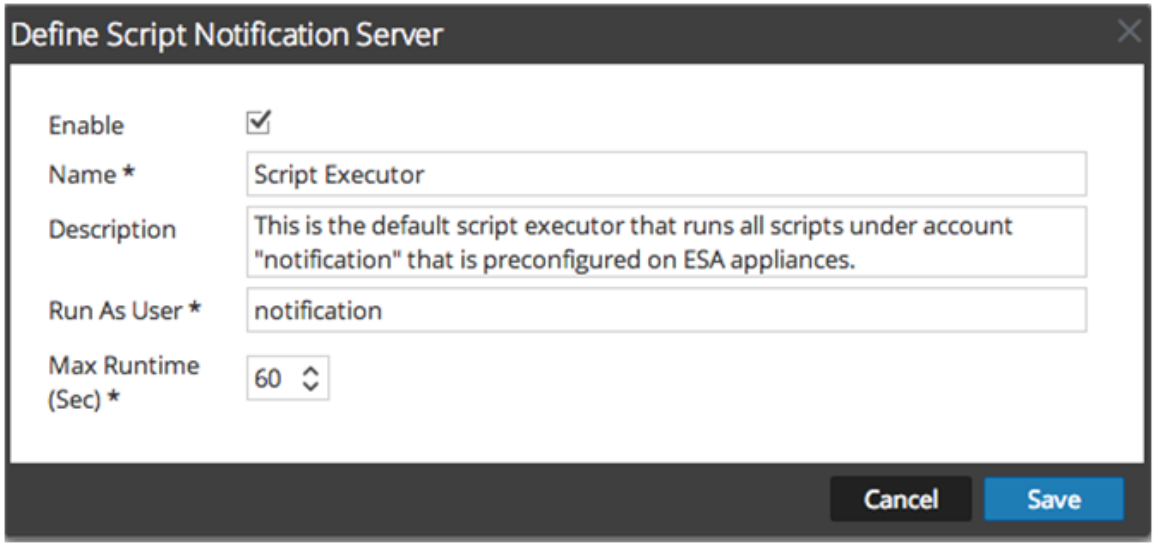
Parámetros	Descripción
Habilitar	Seleccione esta opción para activar el servidor de notificación.
Nombre	Nombre para identificar o etiquetar el servidor de notificación.
Descripción	Descripción breve del servidor de notificación.
Dirección IP o nombre de host del servidor	Nombre de host del host donde se ejecuta el proceso de Syslog de destino.

Parámetros	Descripción
Puerto del servidor	Número de puerto donde se ejecuta el proceso de Syslog de destino.
Protocolo	Protocolo que se usa para transferir los archivos Syslog.
Funcionalidad	La funcionalidad de syslog designada que se usará en todos los mensajes salientes. Se usa para indicar el tipo de programa que registra el mensaje. Algunos valores posibles son KERN, USER, MAIL y DAEMON. Esto permite que el archivo de configuración especifique que los mensajes de diferentes instalaciones se manejarán de manera diferente.
Máximo de alertas por minuto	Cantidad máxima de alertas por minuto. Este campo no se usa para el registro de auditoría global.
Tamaño de línea de espera máximo de alertas	Cantidad máxima de alertas que se pondrán en línea de espera antes de que se descarten. Este campo no se usa para el registro de auditoría global.

Script

Los servidores de notificación de script permiten configurar el script como un servidor de notificación.

En la siguiente figura se muestra el cuadro de diálogo Definir servidor de notificación de script.



En la siguiente tabla se indican los diversos parámetros que debe definir para los servidores de notificación de script.

Parámetros	Descripción
Habilitar	Seleccione esta opción para activar el servidor de notificación.
Nombre	Nombre para identificar o etiquetar el servidor de notificación.
Descripción	Descripción breve del servidor de notificación.
Ejecutar como usuario	Nombre de la identidad del usuario con el cual se ejecuta el script. La identidad predeterminada del usuario es **notificación**. Para ESA, no puede configurarla en otro valor, a menos que haya creado la cuenta en el host de ESA.
Tiempo de ejecución máx. (s)	El tiempo máximo (en segundos) que se permite la ejecución del script.

Cuadros de diálogo de definición de salida de notificación

En este tema se proporcionan descripciones de los diversos cuadros de diálogo de salida de notificación. Las salidas de las notificaciones se configuran en ADMIN > Sistema > Notificaciones > pestaña Salida. Las notificaciones son básicamente los destinos que se usan para el envío de notificaciones. Para ESA, las notificaciones permiten definir cómo se desea recibir las alertas de ESA. Las siguientes son las distintas notificaciones compatibles con NetWitness Suite:

- Correo electrónico
- SNMP
- Syslog
- Script

Los procedimientos relacionados con las notificaciones se describen en Configurar las salidas de las notificaciones.

Para acceder a los cuadros de diálogo de definición notificaciones:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de opciones, seleccione **Notificaciones globales**.
3. En la pestaña **Salida**, haga clic en + y seleccione una salida de notificación (correo electrónico, SNMP, syslog o script)
   El cuadro de diálogo Definir notificación se muestra para su selección.

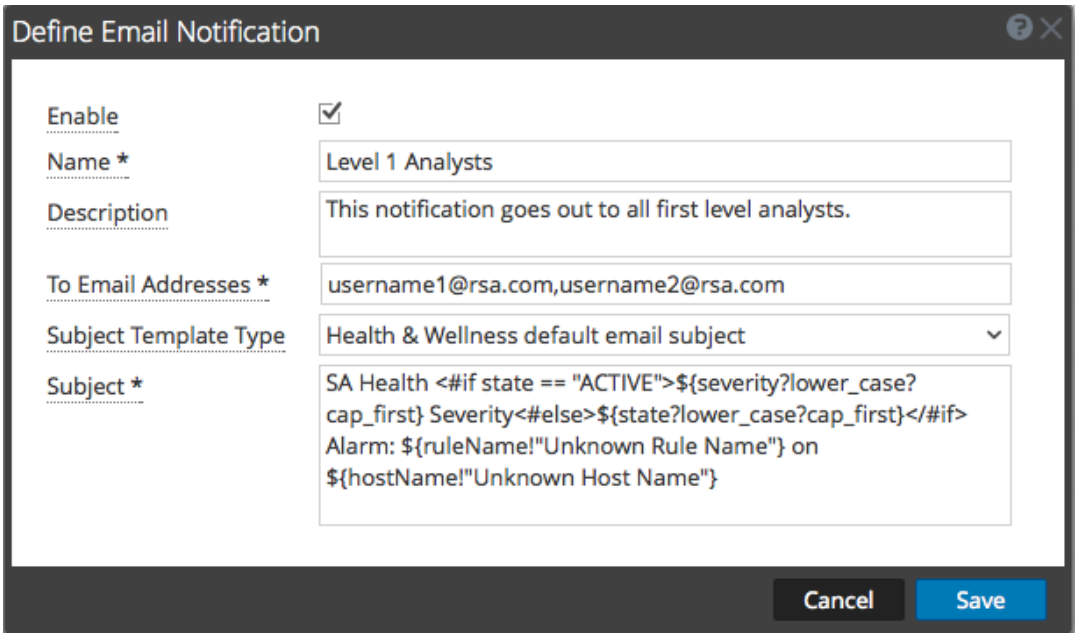
Funciones

Hay cuatro cuadros de diálogo de notificación, los cuales permiten configurar las salidas de notificación.

Correo electrónico

Las notificaciones por correo electrónico permiten definir la dirección de correo electrónico de destino a la cual puede enviar las alertas. También permiten agregar una descripción personalizada en el asunto del correo electrónico y, además, definir múltiples direcciones de correo electrónico de destino.

En la siguiente figura se muestra el cuadro de diálogo Definir notificación de correo electrónico.



En la siguiente tabla se indican los diversos parámetros que se deben definir para las notificaciones por correo electrónico.

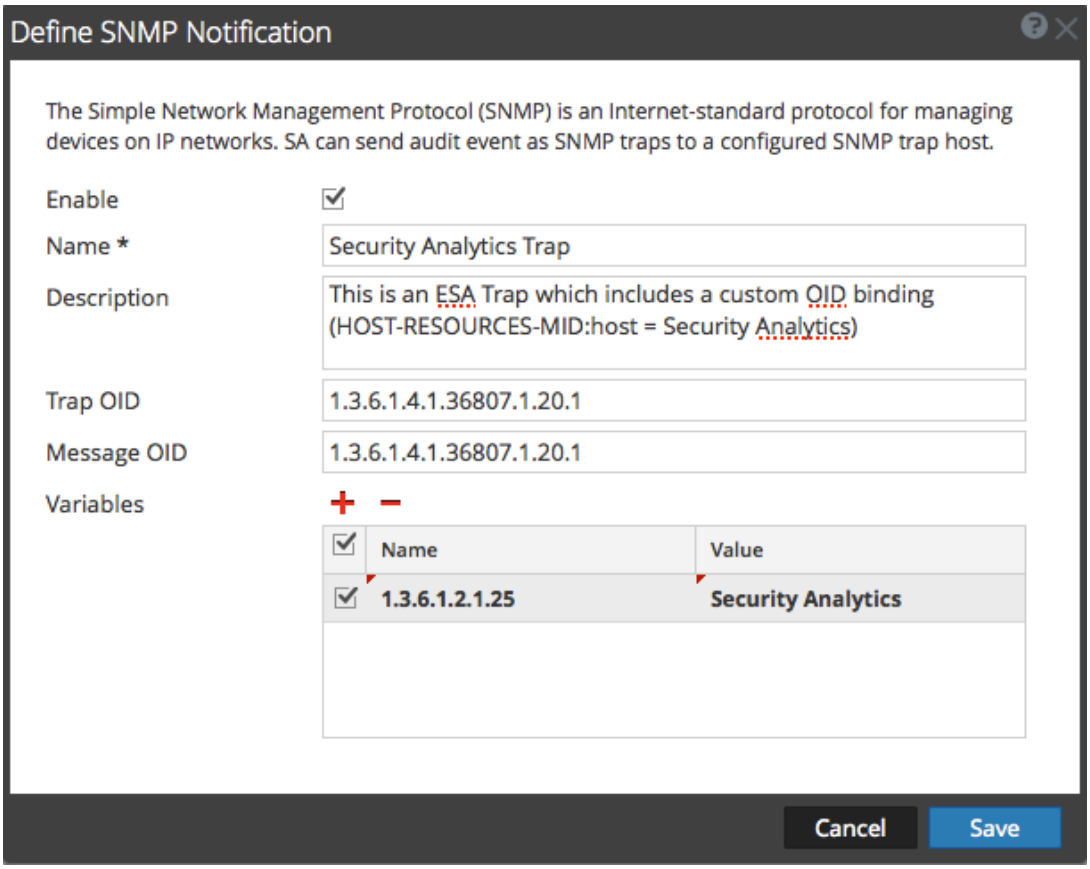
Parámetro	Descripción
Habilitar	Seleccione esta opción para activar la notificación.
Nombre	Nombre para identificar o etiquetar la notificación.
Descripción	Descripción breve sobre la notificación.
Direcciones de correo electrónico de destino	Describe la dirección de correo electrónico de destino a la cual se debe enviar la alerta. **Nota:** Puede definir múltiples direcciones de correo electrónico.
Tipo de plantilla de asunto	Enumera las plantillas disponibles para crear un asunto. Cuando elige una plantilla, el campo Asunto se completa automáticamente con el código de la plantilla que eligió.

Parámetro	Descripción
Asunto	Descripción personalizada acerca de la alerta activada. Esta información se completa automáticamente si elige una de las plantillas predefinidas en el menú desplegable Tipo de plantilla de asunto. **Nota:** Para proporcionar un asunto personalizado, Incluir la línea de asunto de correo electrónico predeterminada en la *Guía de mantenimiento del sistema*.

SNMP

Las notificaciones de SNMP permiten definir la configuración de SNMP para enviar notificaciones de alertas.

En la siguiente figura se muestra el cuadro de diálogo Definir notificación de SNMP.



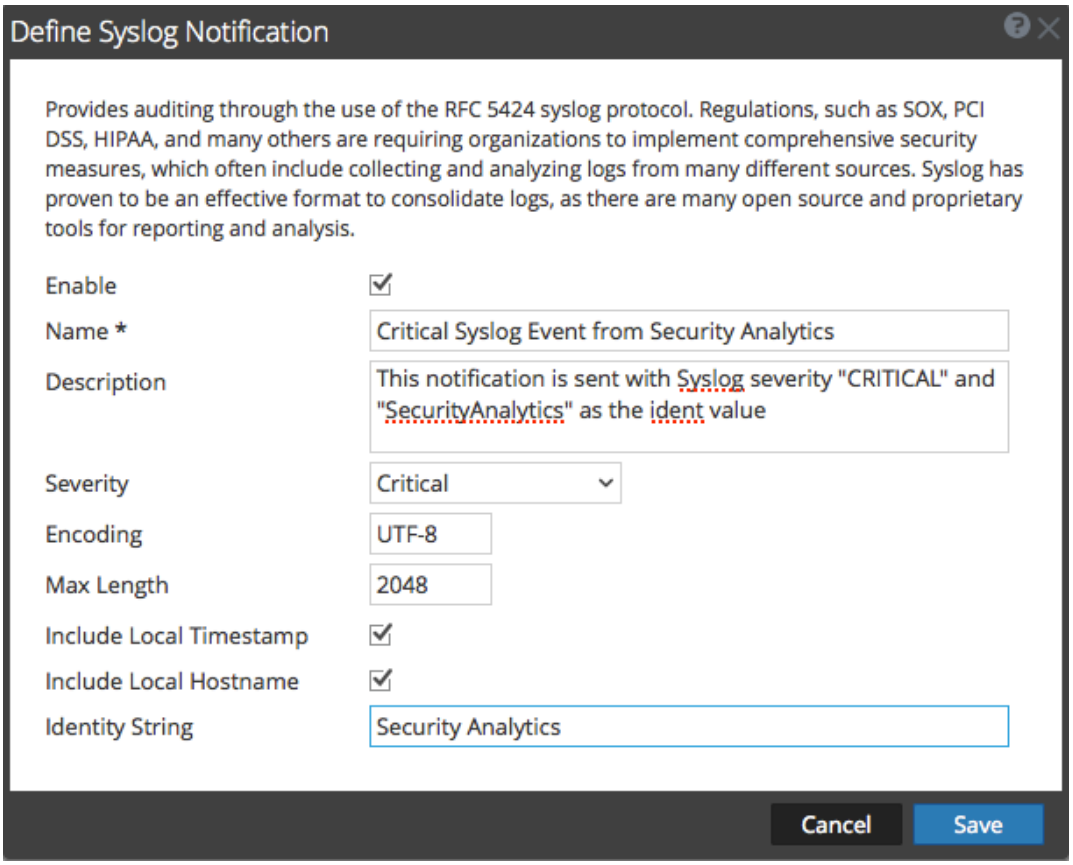
En la siguiente tabla se indican los diversos parámetros que se deben definir para las notificaciones de SNMP.

Parámetro	Descripción
Habilitar	Seleccione esta opción para activar la notificación.
Nombre	Nombre para identificar o etiquetar la notificación.
Descripción	Descripción breve sobre la notificación.
OID de traps	El ID de objeto del SNMP trap en el host de trap que recibe el evento. El valor predeterminado es **1.3.6.1.4.1.36807.1.20.1**. Este valor es un nombre jerárquico que representa el sistema que genera el trap. 1.3.6.1.4.1 es el prefijo común para todas las empresas y 36807.1.20.1 identifica a NetWitness Suite.
OID del mensaje	El identificador de objeto de mensaje para el SNMP trap.
Variables	Información adicional que debe incluir en el trap. Es una variable que es un par de nombre/valor.

Syslog

Las notificaciones de syslog permiten definir la configuración de syslog para enviar notificaciones de alertas.

En la siguiente figura se muestra el cuadro de diálogo Definir notificación de syslog.



En la siguiente tabla se indican los diversos parámetros que se deben definir para las notificaciones de syslog.

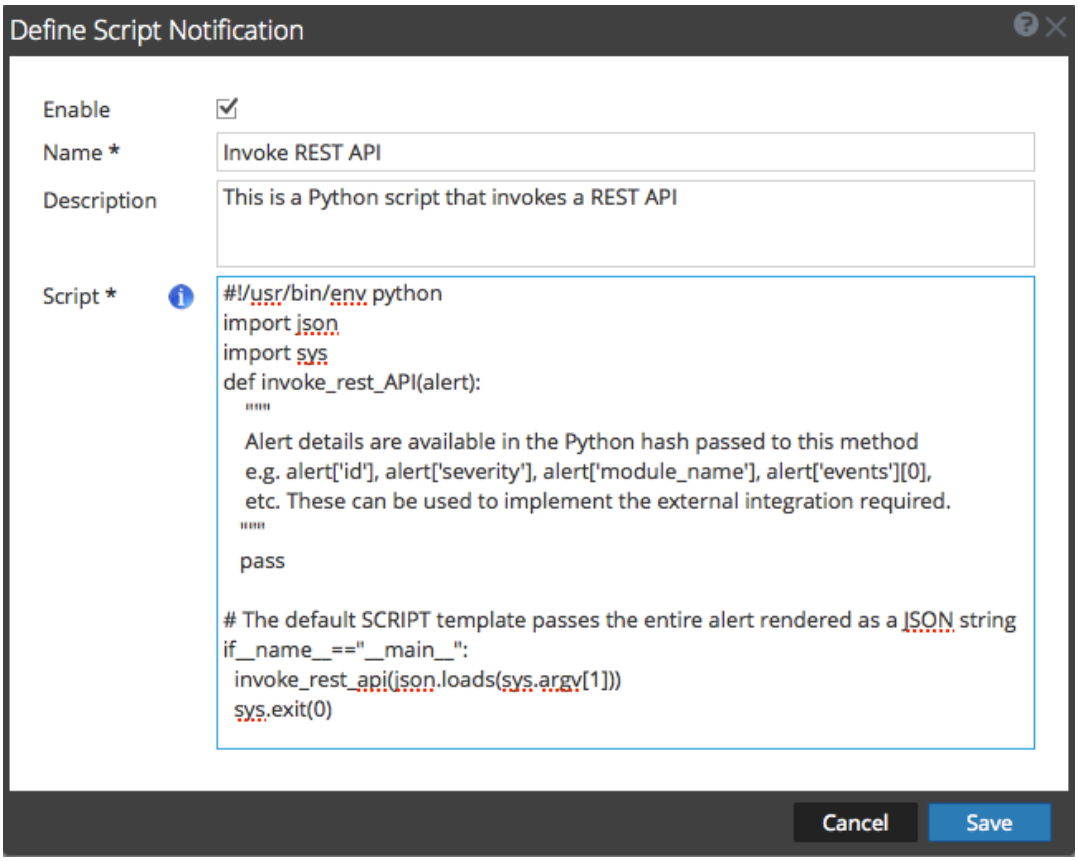
Parámetro	Descripción
Habilitar	Seleccione esta opción para activar la notificación.
Nombre	Nombre para identificar o etiquetar la notificación.
Descripción	Descripción breve sobre la notificación.
Gravedad	Define la severidad de la alerta.
Codificación	Define el formato de codificación. En algunos ambientes donde no se utilizan conjuntos de caracteres normales (por ejemplo, caracteres japoneses), este campo ayudará a seleccionar la codificación correcta de los caracteres.

Parámetro	Descripción
Longitud máxima	La longitud máxima de un mensaje de syslog en bytes. El valor predeterminado es **2,048**. Los mensajes que superan la longitud máxima se truncan cuando se selecciona la casilla de verificación **Truncar los mensajes de syslog demasiado grandes** que se encuentra en Administration > Sistema > Notificaciones antiguas. En Panel Configuración de notificaciones antiguas se proporciona información adicional.
Incluir registro de fecha y hora local	Seleccione para incluir el registro de fecha y hora local en los mensajes.
Incluir nombre de host local	Seleccione para incluir el nombre de host local en los mensajes de syslog.
Cadena de identidad	Una cadena de identidad que se adjuntará al inicio de cada alerta de syslog. Si la cadena está en blanco, no hay cadena de identidad adjuntada al principio de las alertas de salida de syslog. Puede usar esto para identificar las alertas desde ESA.

Script

Las notificaciones de script permiten definir el script que se ejecuta en respuesta a la alerta. Puede usar cualquier script para las notificaciones de ESA.

En la siguiente figura se muestra el cuadro de diálogo Definir notificación de script.



En la siguiente tabla se indican los diversos parámetros que se deben definir para las notificaciones de script.

Parámetro	Descripción
Habilitar	Seleccione esta opción para activar la notificación.
Nombre	Nombre para identificar o etiquetar la notificación.
Descripción	Descripción breve sobre la notificación.
Script	Define el script.

Cuadro de diálogo Definir plantilla de notificación

El panel Notificaciones globales permite configurar ajustes globales de notificación para servidores de notificación, salidas de las notificaciones y plantillas de notificación. Las plantillas para las diversas notificaciones se configuran en la pestaña Plantillas. La plantilla de notificación define el formato y los campos de mensajes de las notificaciones. Puede seleccionar una plantilla predeterminada o puede usar el cuadro de diálogo Definir plantilla para configurar y editar plantillas.

Puede definir los siguientes tipos de plantillas:

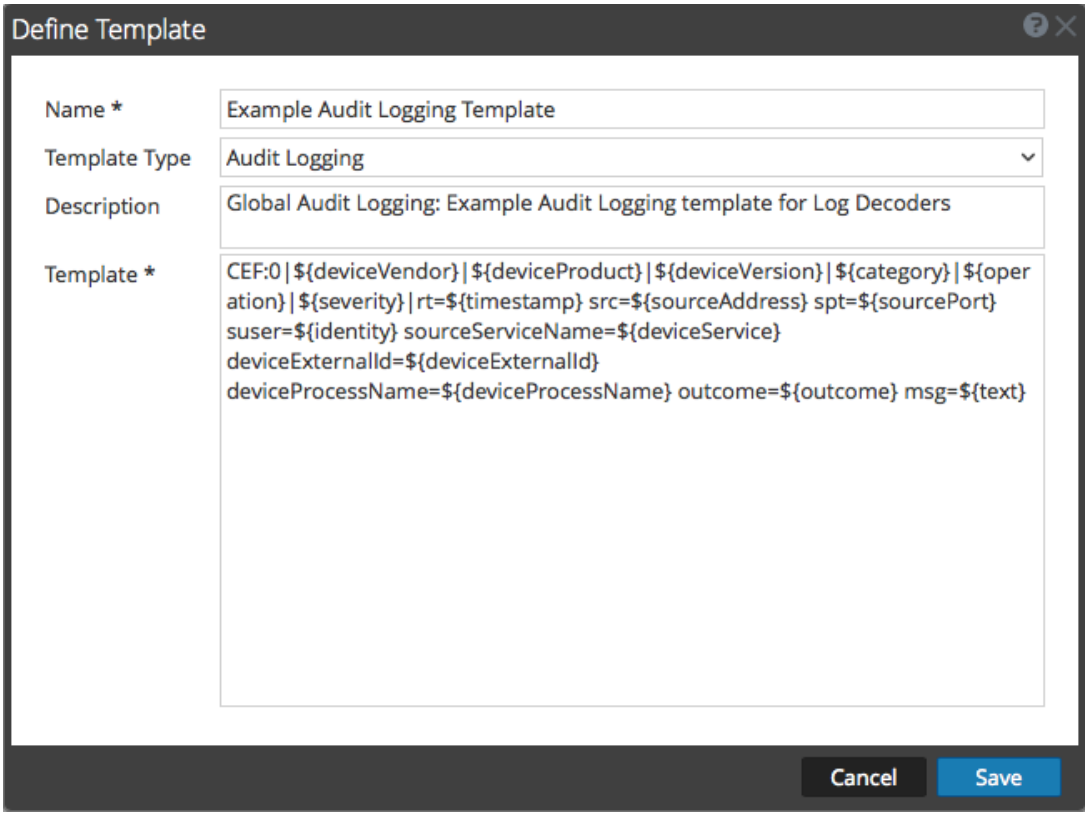
- Registro de auditoría
- Event Stream Analysis
- Monitoreo de orígenes de eventos
- Alarmas de estado

Los procedimientos relacionados con plantillas de notificación se describen en Configurar plantillas para notificaciones.

Para acceder al cuadro de diálogo Definir plantilla:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de navegación izquierdo, seleccione **Notificaciones globales > pestaña Plantilla**.
3. En el panel **Configuración de notificación**, haga clic en  o seleccione una configuración y haga clic en  .

Se muestra el cuadro de diálogo **Definir plantilla**.



Funciones

En la siguiente tabla se describen las funciones del cuadro de diálogo Definir plantilla.

Campo	Descripción
Nombre	Escriba un nombre único para la plantilla de notificación.
Tipo de plantilla	Seleccione el tipo de plantilla que desea crear: • **Registro de auditoría**: use esta plantilla para el registro de auditoría global. • **Event Stream Analysis**: use este tipo de plantilla para notificaciones de alertas de ESA. • **Monitoreo de orígenes de eventos**: use este tipo de plantilla para notificaciones de ESM. • **Alarmas de estado**: use este tipo de plantilla para notificaciones de Estado y condición.

Campo	Descripción
Descripción	Agregue una descripción de la plantilla. Por ejemplo, si crea una plantilla de notificación para Log Decoders que se usará para el registro de auditoría global, podría mencionar esa información en la descripción.
Plantilla	Especifique el formato de la plantilla. En Definir una plantilla para el registro de auditoría global se proporcionan instrucciones para definir una plantilla del registro de auditoría que se usará para el registro de auditoría global. Para definir una plantilla para Event Stream Analysis (ESA), consulte Definir una plantilla para notificaciones de alertas de ESA.

Pestaña Salida

En el panel **Notificaciones globales**, pestaña **Salida** (Admin > Sistema > Notificaciones > Salida), se configuran las salidas de las notificaciones. Las configuraciones de las notificaciones globales definen los ajustes de las notificaciones para Administración de orígenes de eventos (ESM), Estado y condición, el registro de auditoría global, Event Stream Analysis (ESA) y RESPOND.

Las configuraciones de las **salidas de las notificaciones** definen direcciones de correo electrónico y líneas de asunto, ajustes de OID de SNMP trap, ajustes de la salida de syslog y el código de scripts.

Las notificaciones son los destinos configurados para las notificaciones de alertas que envía el servicio ESA. La pestaña Salida permite configurar los siguientes elementos como destinos:

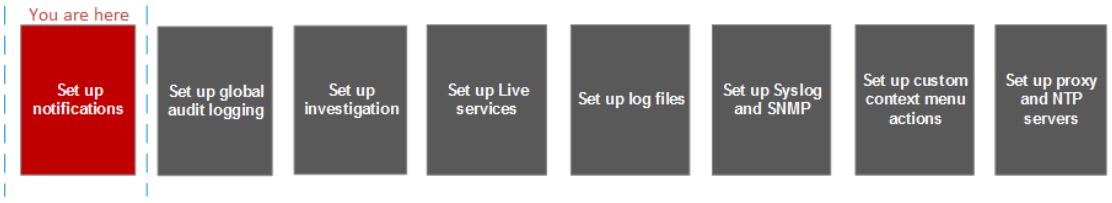
- Correo electrónico
- SNMP
- Syslog
- Script

Nota: No es necesario configurar la pestaña Salida para el registro de auditoría global. Para conocer los pasos detallados, consulte Configurar el registro de auditoría global.

Flujo de trabajo

En este flujo de trabajo se muestran los procedimientos necesarios para configurar y verificar la salida de las notificaciones globales. Es posible realizar las siguientes tareas:

- Configurar los ajustes de correo electrónico como notificación.
- Configurar los ajustes de SNMP como notificación.
- Configurar los ajustes de Syslog como notificación.
- Configurar un script como notificación.



¿Qué desea hacer?

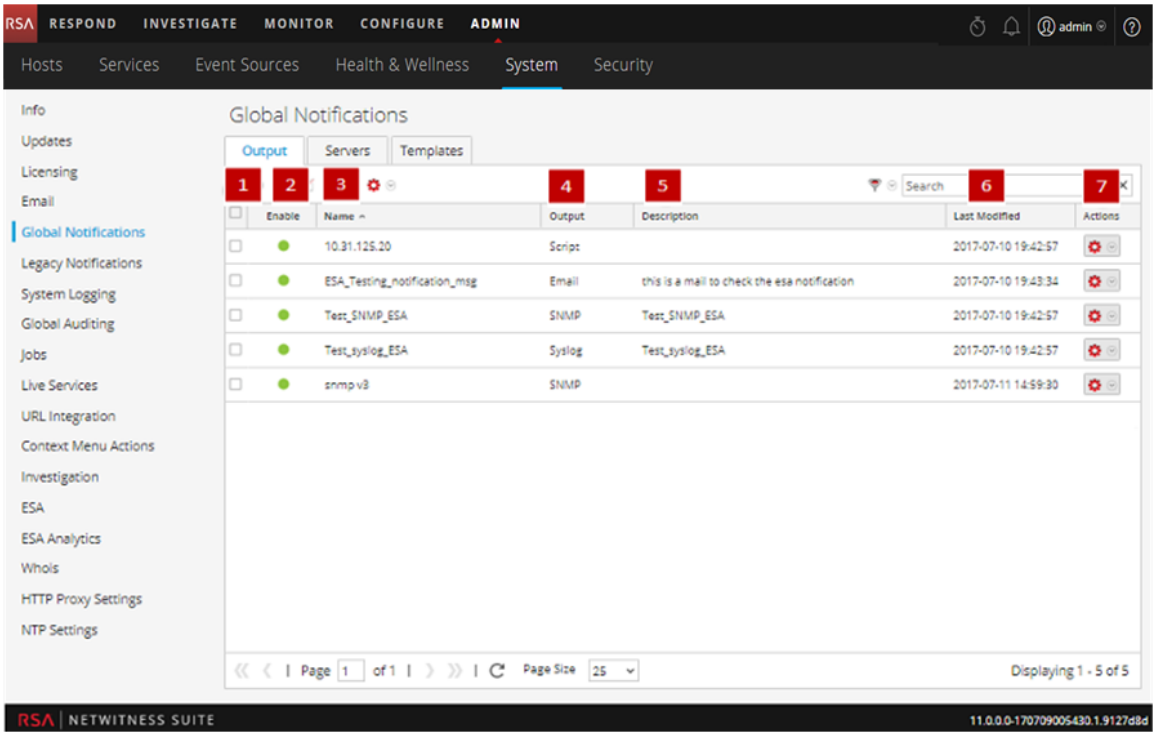
Función	Deseo…	Mostrarme cómo
Administrador	Definir las salidas de las notificaciones.	Configurar las salidas de las notificaciones

Temas relacionados

- Descripción general de salidas de notificaciones
- Configurar el correo electrónico como una notificación
- Configurar el script como una notificación
- Configurar SNMP como una notificación
- Configurar syslog como una notificación

Vista rápida

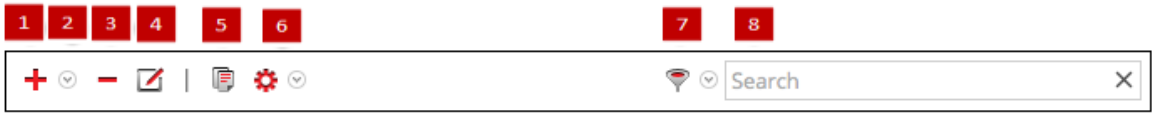
En el siguiente ejemplo se ilustra la configuración de las salidas de las notificaciones globales.



1 Seleccione una fila de una acción de la barra de herramientas. Si selecciona la casilla de verificación del título de la columna, se seleccionan o deseleccionan todas las filas de la cuadrícula.

2	Indica si la configuración está habilitada. Un círculo de color verde indica que la configuración está habilitada. Un círculo de color blanco indica que una configuración no está habilitada.
3	Identifica o etiqueta la configuración.
4	Identifica la salida de la configuración. Las salidas son Correo electrónico, SNMP, Syslog y Script.
5	Describe la configuración.
6	Muestra la fecha y la hora del último cambio en la configuración.
7	Proporciona un menú Acciones para la configuración seleccionada, con acciones que se pueden aplicar a la configuración. El menú Acciones permite eliminar, editar, duplicar y exportar la configuración.

La barra de herramientas del panel Notificaciones globales está en la parte superior de la pestaña Salida y proporciona las siguientes opciones:



1	Agrega una salida de notificación
2	Configura los ajustes de notificaciones por correo electrónico, SNMP, syslog y script.
3	Quita una configuración de notificación seleccionada. No puede eliminar servidores de notificación y tipos de notificaciones asociados con configuraciones del registro de auditoría global. Si intenta eliminar una salida de notificación (notificación) que se usa en alertas, recibirá un mensaje de confirmación de advertencia que señala que las alertas que usan la notificación no funcionarán correctamente. El mensaje muestra la cantidad de alertas en uso. También puede eliminar una configuración si la selecciona y, a continuación, en la columna Acciones, elige > Eliminar.
4	Edita una configuración de notificación seleccionada. También puede editar una configuración si la selecciona y, a continuación, en la columna Acciones, elige > Editar.
5	Duplica una configuración de notificación seleccionada. También puede duplicar una configuración si la selecciona y, a continuación, en la columna Acciones, elige > Duplicar.

6 Muestra las siguientes opciones:

- **Importar**: importa un servidor, un tipo o una plantilla de notificación. Por ejemplo, en la pestaña Servidores, puede importar una configuración de servidor de notificación.
- **Exportar todo**: exporta todas las configuraciones. Por ejemplo, si está en la pestaña Servidores, puede exportar todas las configuraciones de servidores de notificación.
- **Exportar**: Exporta una configuración seleccionada. También puede exportar una configuración si la selecciona y, a continuación, en la columna Acciones, elige  > Exportar.

7 Filtra por correo electrónico, SNMP, syslog o script.

8 Busca configuraciones en la cuadrícula.

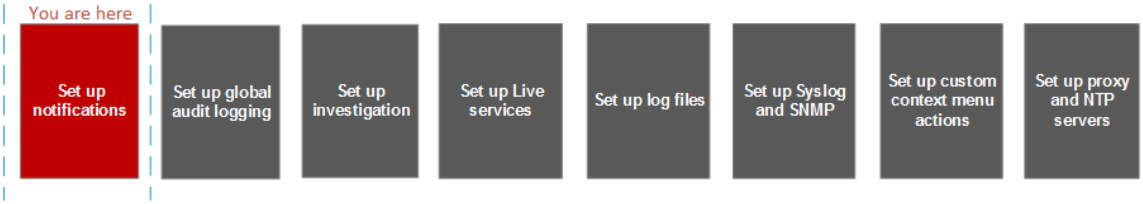
Pestaña Servidores

En la pestaña Servidores se describen los componentes de Notificaciones globales > pestaña Servidores. Esta pestaña permite configurar servidores de notificación. Las configuraciones de las notificaciones globales definen los ajustes de las notificaciones para Administración de orígenes de eventos (ESM), Estado y condición, el registro de auditoría global, Event Stream Analysis (ESA) y RESPOND.

Configure los **Servidores de notificación** en la pestaña Servidores. En la pestaña Servidores, puede agregar los servidores desde los cuales desea recibir notificaciones del sistema. Para el registro de auditoría global, defina Log Decoders como servidores de notificación de syslog.

Event Stream Analysis puede enviar notificaciones a los usuarios mediante correo electrónico, SNMP o Syslog cuando se activa una alerta en el servicio ESA. Estos emisores de notificación de alerta se conocen como servidores de notificación. Puede configurar varios ajustes de notificación y usarlos mientras define una regla de ESA. Por ejemplo, puede configurar varios servidores de correo o servidores de syslog y utilizar los ajustes durante la definición de una regla de ESA.

Flujo de trabajo



En el flujo de trabajo se muestran los procedimientos necesarios para configurar y verificar los servidores para las notificaciones globales. Es posible realizar las siguientes tareas:

- Configurar los ajustes de correo electrónico como un servidor de notificación.
- Configurar los ajustes de SNMP como un servidor de notificación.
- Configurar los ajustes de syslog como un servidor de notificación.
- Configurar un script como un servidor de notificación.

¿Qué desea hacer?

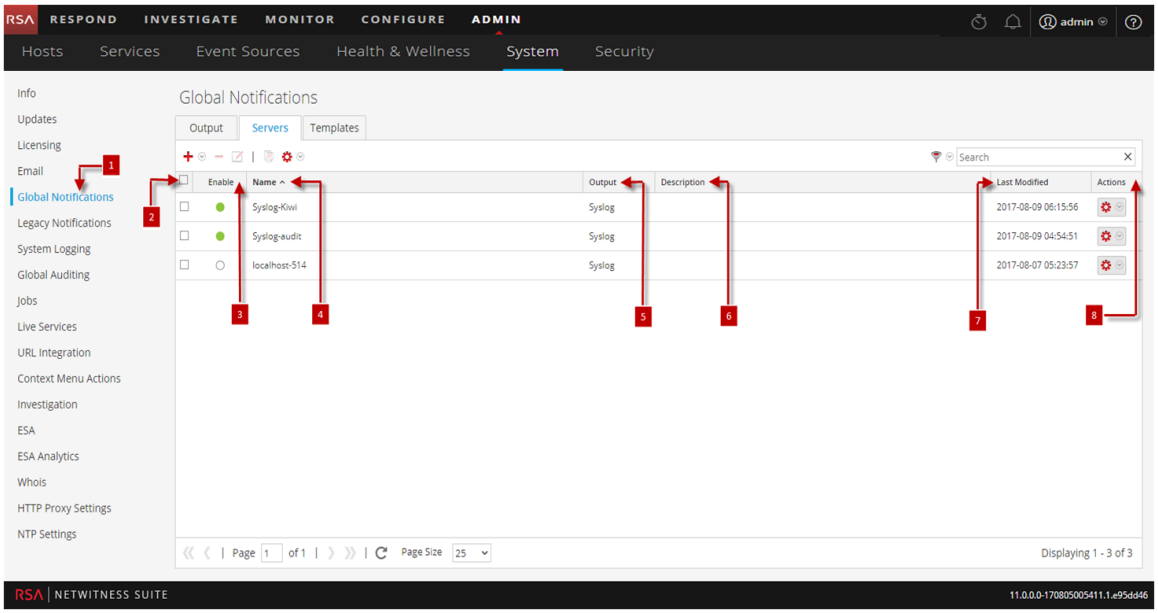
Función	Deseo…	Mostrarme cómo
Administrador	Definir servidores de notificación	Configurar servidores de notificación

Temas relacionados

- Descripción general de servidores de notificación
- Configurar los ajustes de correo electrónico como un servidor de notificación
- Configurar un script como un servidor de notificación
- Configurar los ajustes de SNMP como un servidor de notificación
- Configurar un servidor de notificación de syslog

Vista rápida

En el siguiente ejemplo se ilustra la configuración de los servidores de notificaciones globales.



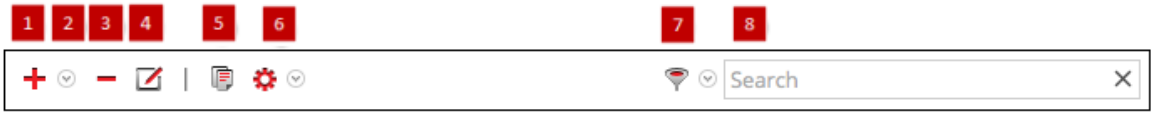
1	Muestra el panel de la pestaña Servidores.
2	Seleccione una fila de una acción de la barra de herramientas. Si selecciona la casilla de verificación del título de la columna, se seleccionan o deseleccionan todas las filas de la cuadrícula.
3	Indica si la configuración está habilitada. Un círculo de color verde indica que la configuración está habilitada. Un círculo de color blanco indica que una configuración no está habilitada.
4	Identifica o etiqueta la configuración.
5	Identifica la salida de la configuración. Las salidas son Correo electrónico, SNMP, Syslog y Script.

6 Describe la configuración.

7 Muestra la fecha y la hora del último cambio en la configuración.

8 Proporciona un menú Acciones para la configuración seleccionada, con acciones que se pueden aplicar a la configuración. El menú Acciones permite eliminar, editar, duplicar y exportar la configuración.

La barra de herramientas del panel Notificaciones globales está en la parte superior de la pestaña Salida y proporciona las siguientes opciones:



1 Agrega una salida de notificación

2 Configura los ajustes de notificaciones por correo electrónico, SNMP, syslog y script.

3 Quita una configuración de notificación seleccionada. No puede eliminar servidores de notificación y tipos de notificaciones asociados con configuraciones del registro de auditoría global. Si intenta eliminar una salida de notificación (notificación) que se usa en alertas, recibirá un mensaje de confirmación de advertencia que señala que las alertas que usan la notificación no funcionarán correctamente. El mensaje muestra la cantidad de alertas en uso. También puede eliminar una configuración si la selecciona y, a continuación, en la columna Acciones, elige > Eliminar.

4 Edita una configuración de notificación seleccionada. También puede editar una configuración si la selecciona y, a continuación, en la columna Acciones, elige > Editar.

5 Duplica una configuración de notificación seleccionada. También puede duplicar una configuración si la selecciona y, a continuación, en la columna Acciones, elige > Duplicar.

6 Muestra las siguientes opciones:

- **Importar**: importa un servidor, un tipo o una plantilla de notificación. Por ejemplo, en la pestaña Servidores, puede importar una configuración de servidor de notificación.

- **Exportar todo**: exporta todas las configuraciones. Por ejemplo, si está en la pestaña Servidores, puede exportar todas las configuraciones de servidores de notificación.
- **Exportar**: Exporta una configuración seleccionada. También puede exportar una configuración si la selecciona y, a continuación, en la columna Acciones, elige  > Exportar.

7 Filtra por correo electrónico, SNMP, syslog o script.

8 Busca configuraciones en la cuadrícula.

Pestaña Plantillas

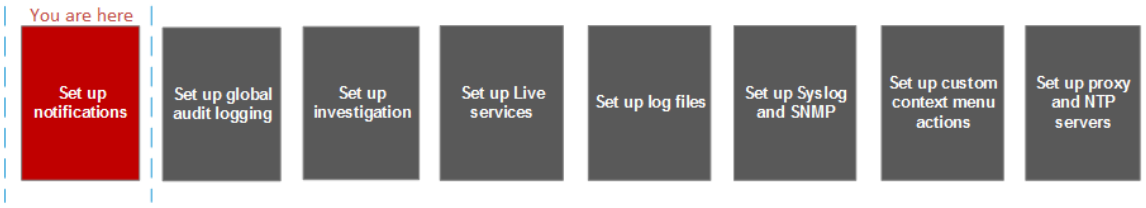
La pestaña Plantillas de notificación permite configurar plantillas de notificación. Las configuraciones de las notificaciones globales definen los ajustes de las notificaciones para Administración de orígenes de eventos (ESM), Estado y condición, el registro de auditoría global, Event Stream Analysis (ESA) y RESPOND. Las plantillas de notificación definen el formato y los campos de mensajes de las notificaciones.

Seleccione una plantilla predeterminada o configure plantillas para correo electrónico, SNMP, syslog y script, según el tipo de plantilla. Para plantillas de Event Stream Analysis (ESA), configure correo electrónico, SNMP, syslog y script. Para plantillas del registro de auditoría, configure syslog.

Las plantillas de Event Stream Analysis no son específicas de ningún tipo de notificaciones de alertas; es decir, la misma plantilla se puede utilizar para todos los tipos de notificaciones.

Cuando se actualiza desde NetWitness Suite 10.4, todas las plantillas de notificación existentes migran al tipo de plantilla de Event Stream Analysis.

Flujo de trabajo



¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Definir plantillas de notificación	Configurar plantillas para notificaciones

Temas relacionados

Configurar plantillas de notificaciones globales

Configurar una plantilla

Definir una plantilla para notificaciones de alertas de ESA

Eliminar una plantilla

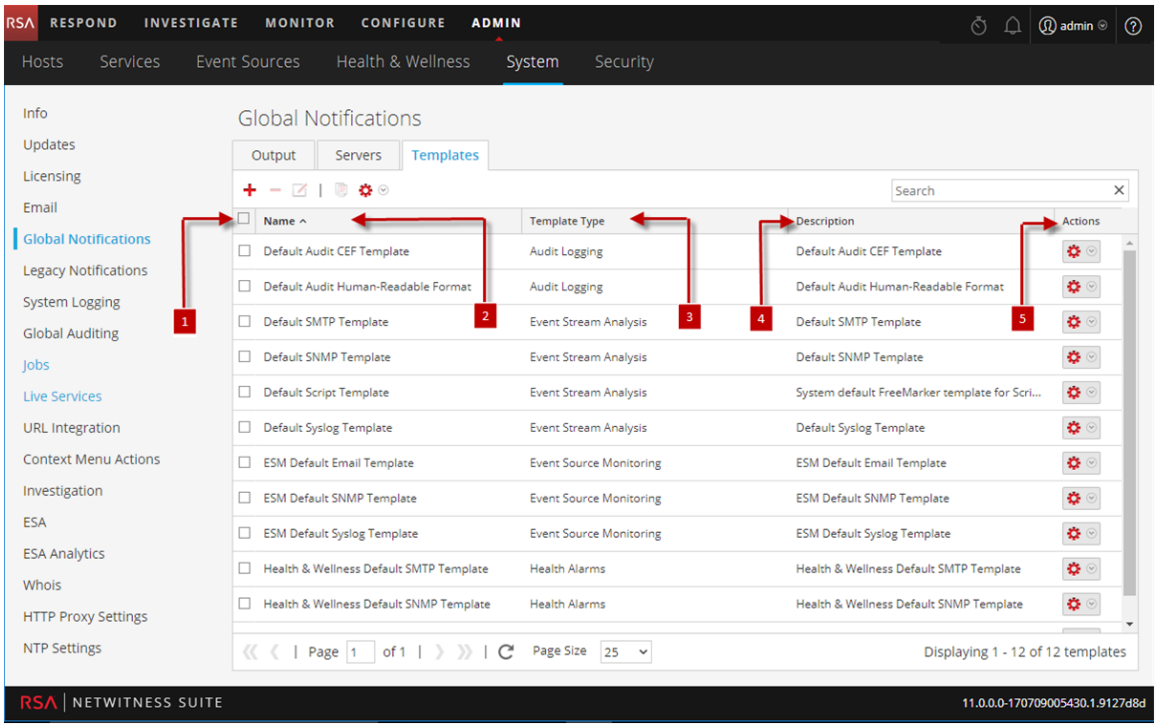
Duplicar una plantilla

Editar una plantilla

Importar y exportar una plantilla de notificaciones globales

Vista rápida

En el siguiente ejemplo se ilustra la pestaña Plantillas de notificaciones globales.



1. Seleccione una fila de una acción de la barra de herramientas. Si selecciona la casilla de verificación del título de la columna, se seleccionan o deseleccionan todas las filas de la cuadrícula.
2. Identifica o etiqueta las plantillas
3. Elegir un tipo de plantilla
4. Describe las plantillas
5. Proporciona un menú Acciones para las plantillas seleccionadas, con acciones que se pueden aplicar a las plantillas. El menú Acciones permite eliminar, editar, duplicar y exportar la configuración.

Panel Configuración de proxy HTTP

En Panel Configuración de proxy HTTP se presentan las funciones de compatibilidad con proxy de la vista Sistema > panel Configuración de proxy HTTP de Administration.

Nota: La compatibilidad con proxies es solo para los proxies HTTP y HTTPS y no para SOCKS5.

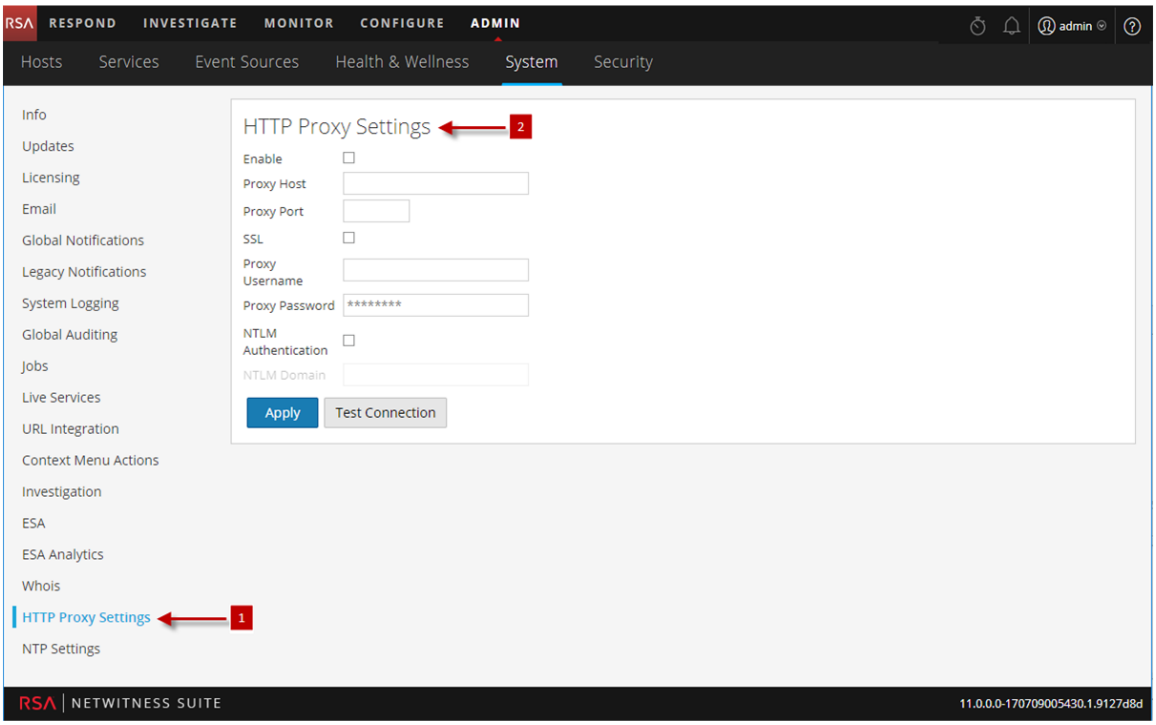
El panel Configuración de proxy HTTP proporciona una interfaz del usuario para configurar un proxy con el fin de utilizarlo en los módulos y los servicios de NetWitness Suite. La configuración de proxy establece un proxy que se usa cada vez que se requiere en NetWitness Suite. Los ajustes en este panel reemplazan cualquier configuración de proxy establecida para un servicio individual, como Malware Analysis o Live.

Temas relacionados

Configurar el proxy de NetWitness Suite

Vista rápida

En el siguiente ejemplo se ilustra un panel Configuración de proxy HTTP.



1 Muestra el panel Configuración de proxy HTTP.

2 Permite al usuario establecer la Configuración de proxy HTTP.

Barra de herramientas y funciones

Esta tabla describe las funcionalidades de la sección Configuración de proxy.

Función	Descripción
Habilitar	Activa la configuración del proxy del sistema para usarlo en NetWitness Suite.
Host proxy	El nombre de host del host de proxy.
Puerto de proxy	El puerto que se utiliza para la comunicación en el host de proxy.
Nombre de usuario de proxy	(Opcional) El nombre de usuario que se utiliza para iniciar sesión en el host de proxy si el proxy requiere autenticación.
Contraseña de proxy	(Opcional) La contraseña que se utiliza para iniciar sesión en el host de proxy si el proxy requiere autenticación.
Usar autenticación NTLM	Usar la autenticación de NT LAN Manager y los protocolos de seguridad de sesión.
Dominio de NTLM	El nombre del dominio de NTLM.
Use SSL	(Opcional) Activa la comunicación utilizando SSL.
Aplicar	Aplica todos los cambios realizados y se implementan inmediatamente.

Panel Configuración de correo electrónico

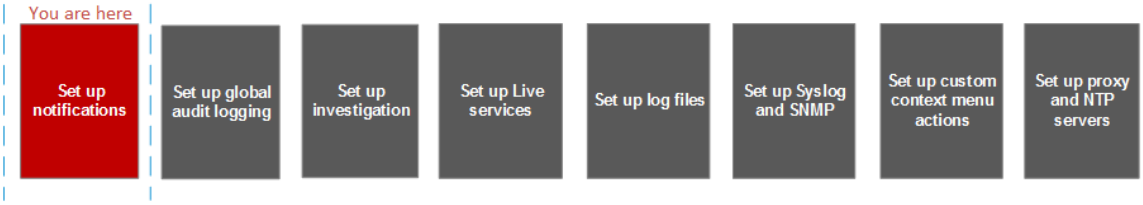
En el panel Configuración de correo electrónico se proporciona información sobre los ajustes de configuración del correo electrónico en la vista Sistema > panel Configuración de correo electrónico. RSA NetWitness® Suiteenvía notificaciones a los usuarios mediante un correo electrónico acerca de varios eventos del sistema. Para poder configurar estas notificaciones por correo electrónico, primero configure el servidor de correo electrónico de SMTP (consulte Configurar los servidores de correo electrónico y las cuentas de notificaciones).

El panel Configuración de correo electrónico proporciona un método para:

- Configurar el servidor de correo electrónico.
- Configurar una cuenta de correo electrónico para recibir notificaciones.
- Ver las estadísticas sobre las operaciones de correo electrónico.

Flujo de trabajo

En este flujo de trabajo se muestran los procedimientos necesarios para configurar y verificar el panel Correo electrónico.



¿Qué desea hacer?

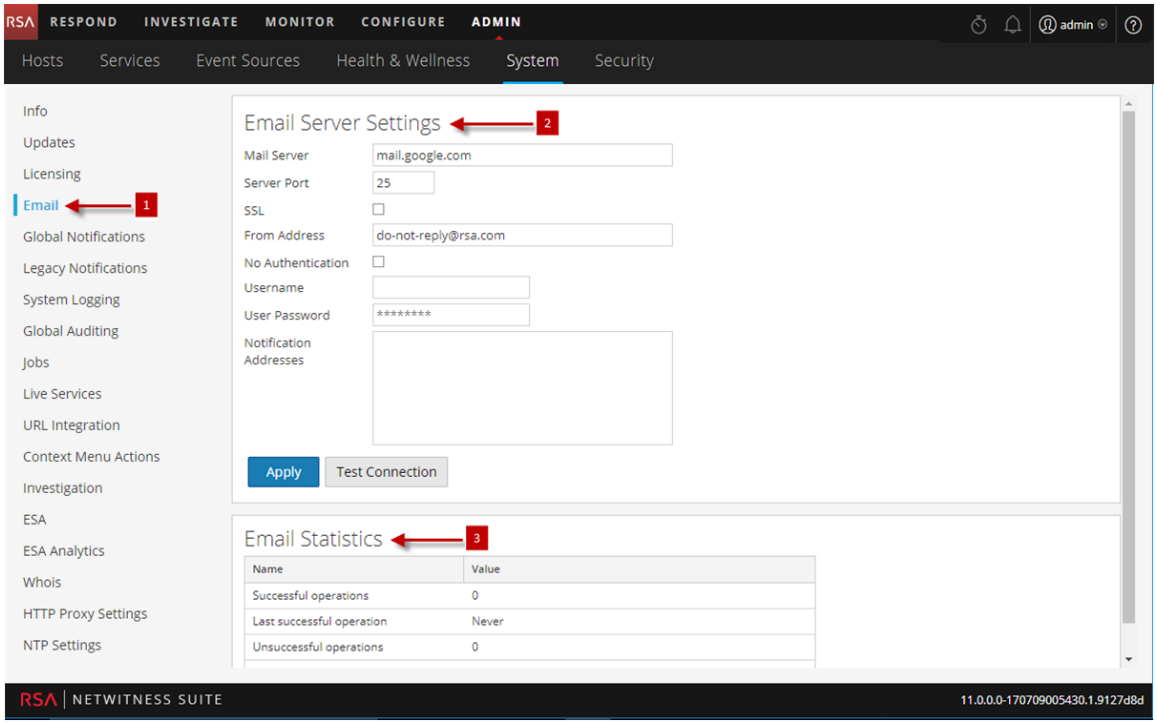
Función	Deseo…	Mostrarme cómo
Administrador	Configurar el servidor de correo SMTP	Configurar los servidores de correo electrónico y las cuentas de notificaciones
Administrador	Configuración de correo electrónico como un servidor de notificación	Configurar los ajustes de correo electrónico como un servidor de notificación
Administrador	Configurar, verificar y activar la cuenta de correo electrónico	Recibir una notificación por correo electrónico

Temas relacionados

- Configurar los ajustes de correo electrónico como un servidor de notificación
- Configurar el correo electrónico como una notificación
- Configurar los servidores de correo electrónico y las cuentas de notificaciones

Vista rápida

En el siguiente ejemplo se ilustra la configuración de correo electrónico. La configuración define la manera en que los eventos se notifican por correo electrónico.



1	Muestra el panel Configuración de correo electrónico.
2	Permite al usuario configurar los ajustes del servidor de correo electrónico.
3	Proporciona comentarios sobre las operaciones de correo electrónico.

Barra de herramientas y funciones

El panel **Configuración de correo electrónico** tiene dos secciones: **Configuración de servidor de correo electrónico** y **Estadísticas de correo electrónico**.

Configuración de servidor de correo electrónico

En la sección **Configuración de servidor de correo electrónico**, puede configurar los siguientes parámetros.

Función	Descripción
Servidor de correo	El nombre del servidor de correo electrónico. El valor predeterminado es **mail.google.com**.
Puerto del servidor	El puerto del servidor que se utiliza para enviar y recibir correos electrónicos. El valor predeterminado es **25**.
Usar SSL	La preferencia para usar SSL en las comunicaciones entre el servidor de correo electrónico y NetWitness Suite. El valor predeterminado es no utilizar SSL (deseleccionado).
Dirección de remitente	La dirección que aparece en todos los correos electrónicos de NetWitness Suite. La dirección de remitente predeterminada para los correos electrónicos es **do-not-reply@rsa.com**.
Nombre de usuario	El nombre de usuario para obtener acceso al servidor de correo electrónico. El valor predeterminado está **en blanco**.
Contraseña de usuario	La contraseña de usuario para obtener acceso al servidor de correo electrónico. El valor predeterminado está **en blanco**.
Probar conexión	Prueba la conexión con el servidor de correo electrónico.
Aplicar	Aplica la configuración de correo electrónico en esta instancia de NetWitness Suite.

Estadísticas de correo electrónico

La sección Estadísticas de correo electrónico proporciona retroalimentación de una serie de operaciones de correo electrónico correctas y fallidas, así como la hora de la última operación de correo electrónico correcta y fallida. En cada estadística se muestra el nombre de la estadística y el valor.

Panel Configuración de ESA

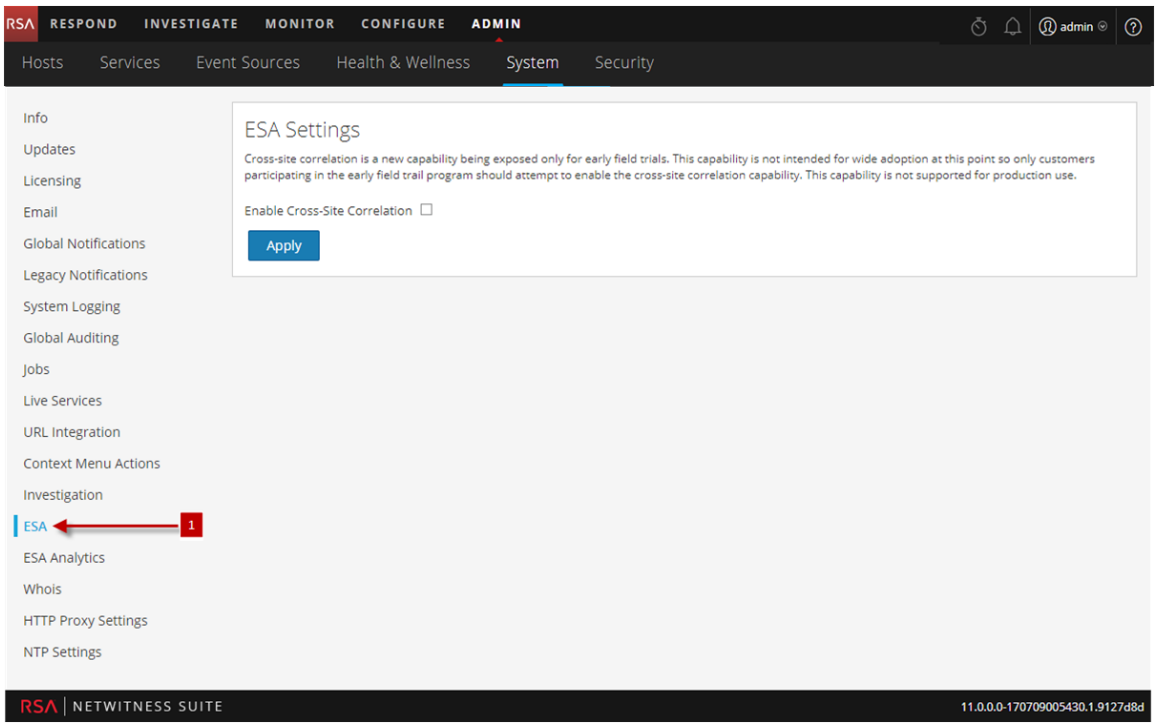
El panel Configuración de ESA permite habilitar y deshabilitar la correlación entre sitios. La correlación entre sitios es una nueva funcionalidad que se presenta solo para las pruebas de campo preliminares. Esta funcionalidad no está destinada a adopción generalizada.

Precaución: Solo los clientes que participan en el programa de prueba de campo preliminar deben intentar habilitar la funcionalidad de correlación entre sitios. Esta funcionalidad no es compatible para su uso en producción.

Temas relacionados

- Definir una plantilla para notificaciones de alertas de ESA
- Guía de Investigation y Malware Analysis
- Guía de configuración de Context Hub

Vista rápida



1 Muestra el panel Configuración de ESA.

Barra de herramientas y funciones

Las funciones del panel Configuración de ESA son las siguientes:

- Casilla de verificación Activar correlación entre sitios: Cuando se selecciona, habilita la correlación entre sitios en ESA. Cuando agrega una implementación en ADMIN > Alertas > Configurar, puede implementar el mismo conjunto de reglas en varios servicios de ESA para el procesamiento centralizado de reglas.
- Botón Aplicar: habilita la selección.

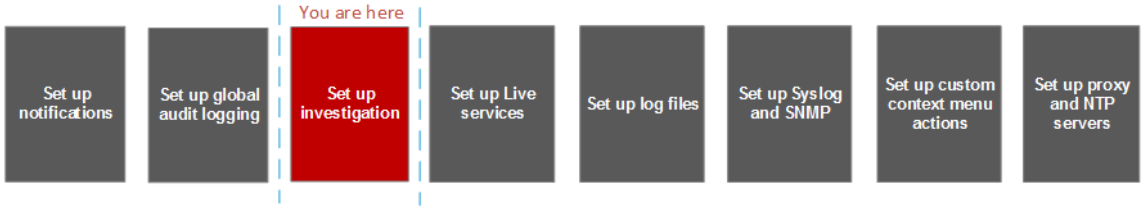
Panel Configuración de Investigation

En la vista Sistema > panel Configuración de Investigation se proporciona la interfaz del usuario para que los administradores configuren ajustes en todo el sistema que NetWitness Suite Investigation usa cuando analiza datos y reconstruye un evento.

Los ajustes de Configuración de Investigation permiten que un administrador administre el rendimiento de las aplicaciones para Investigation. A medida que los analistas reconstruyen y analizan las sesiones que están investigando, el rendimiento se puede ver afectado por operaciones que implican la carga, la búsqueda, la visualización y la reconstrucción de grandes cantidades de datos.

Nota: los analistas también pueden configurar preferencias individuales para Investigation en la vista Perfiles y en la vista Navegación.

Flujo de trabajo



¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar los ajustes de Navegar, Eventos y Búsqueda de contexto	Configurar los ajustes de Investigation
Administrador	Limpiar la caché de reconstrucción para los servicios	Configurar los ajustes de Investigation

Temas relacionados

- Procedimientos estándar

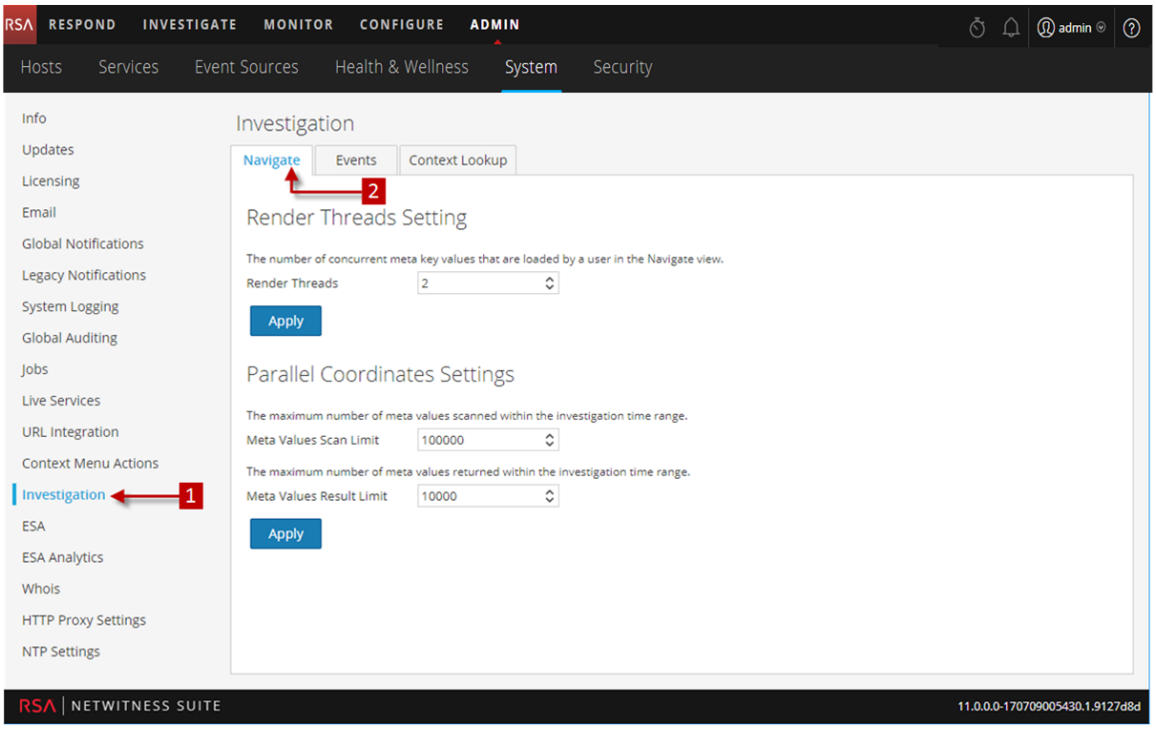
Vista rápida

El panel Configuración de Investigation tiene tres pestañas: Navegar, Eventos y Búsqueda de contexto.

Aunque la mayoría de los campos de las pestañas tiene una lista de selección con incrementos específicos a través del rango de valores posibles, puede ingresar manualmente un valor dentro del rango permitido. Una entrada no válida se señala mediante el campo resaltado en rojo. Cuando se seleccionan valores válidos, si se hace clic en Aplicar en una determinada sección, los cambios se aplican de inmediato.

Pestaña Navegar

En la siguiente figura se muestra la pestaña Navegar.



1 Muestra el panel Configuración de Investigation.

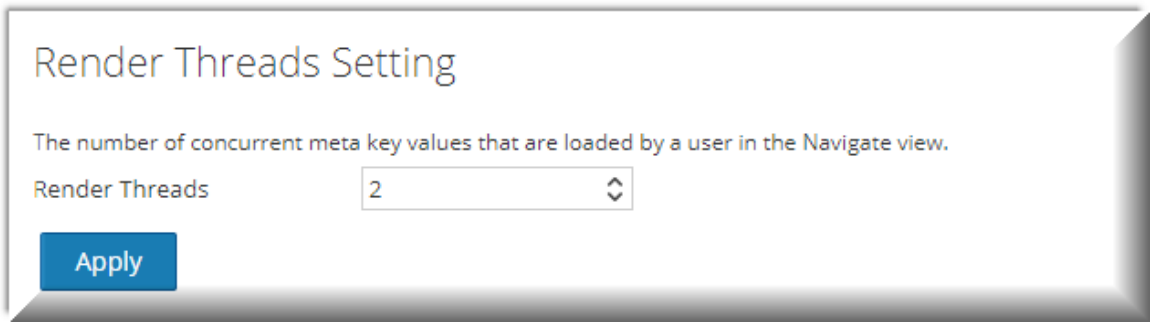
2 Muestra la pestaña Navegar.

Barra de herramientas y funciones

La pestaña Navegar tiene dos secciones: Configuración de hilos de ejecución de representación y Configuración de coordenadas paralelas.

Configuración de hilos de ejecución de representación

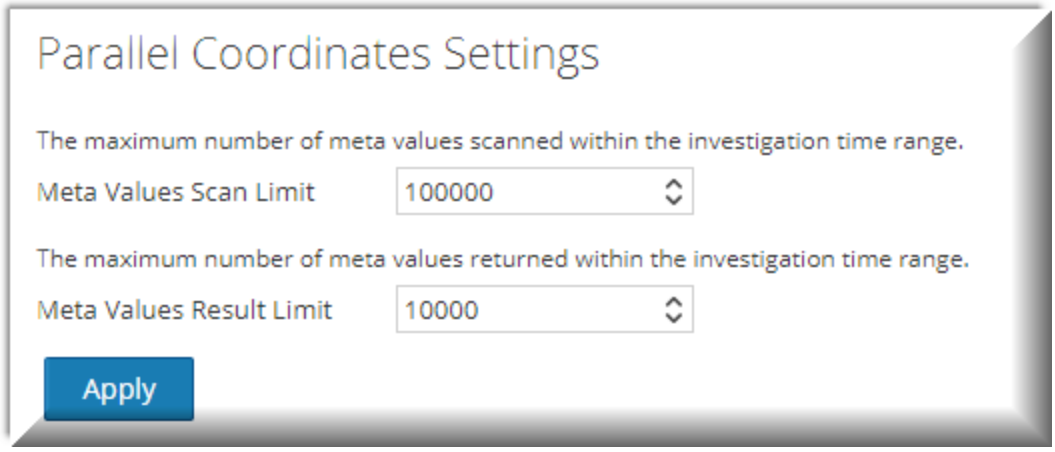
Este es un valor seleccionable entre 1 y 20 que define la cantidad de cargas (valores) simultáneas en la vista Navegar. El valor predeterminado es 1.



Configuración de coordenadas paralelas

La configuración de coordenadas paralelas se aplica a la visualización de coordenadas paralelas en la vista Navegar. Hay un límite fijo en la cantidad de datos que se pueden representar como un gráfico de coordenadas paralelas. En NetWitness Suite, el administrador puede configurar aquí los límites de las coordenadas paralelas.

Nota: Para mejorar el rendimiento, la configuración recomendada es **Límite de escaneo de valores de metadatos: 100000** y **Límite de resultados de valores de metadatos: entre 1,000 y 10,000**.



En la siguiente tabla se describe la configuración de coordenadas paralelas.

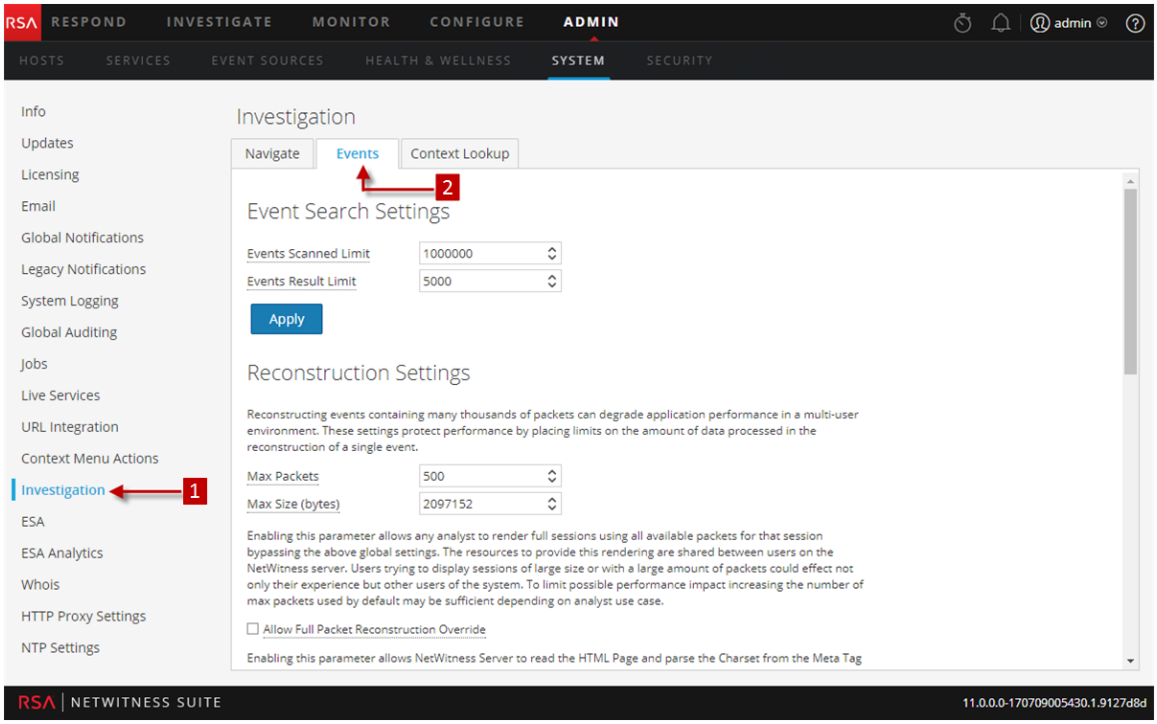
Parámetro	Descripción
Límite de escaneo de valores de metadatos	La cantidad máxima de valores de metadatos que se escanean en el rango de tiempo de Investigation que seleccionó el analista en la vista Navegar. Los valores posibles están en el rango de 1,000 a 10,000,000. El valor predeterminado es 100,000.

Parámetro	Descripción
Límite de resultados de valores de metadatos	La cantidad máxima de valores de metadatos que se devuelven en el rango de tiempo de Investigation que seleccionó el analista en la vista Navegar. Los valores posibles están en el rango de 100 a 1,000,000,000. El valor predeterminado es 10,000.

Vista rápida

Pestaña Eventos

En la siguiente figura se muestra la pestaña Eventos.



Los procedimientos asociados a este panel se proporcionan en Procedimientos estándar.

1 Muestra el panel Configuración de Investigation.

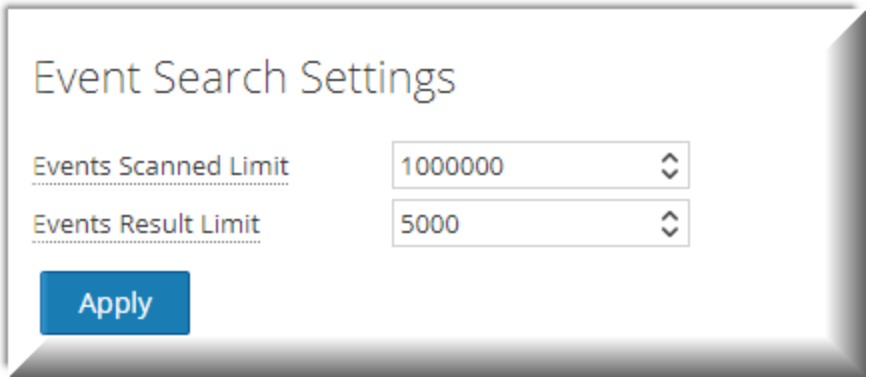
2 Muestra la pestaña Evento.

Barra de herramientas y funciones

En la pestaña Eventos se proporcionan ajustes configurables que afectan a la investigación de eventos. Esta pestaña tiene cuatro secciones: Configuración de búsqueda de eventos, Configuración de la reconstrucción, Configuración de reconstrucción de vista web y Configuración de caché de reconstrucción.

Configuración de búsqueda de eventos

La configuración de búsqueda de eventos ayuda a limitar la cantidad de eventos que se escanean cuando se realizan búsquedas en la vista Eventos.



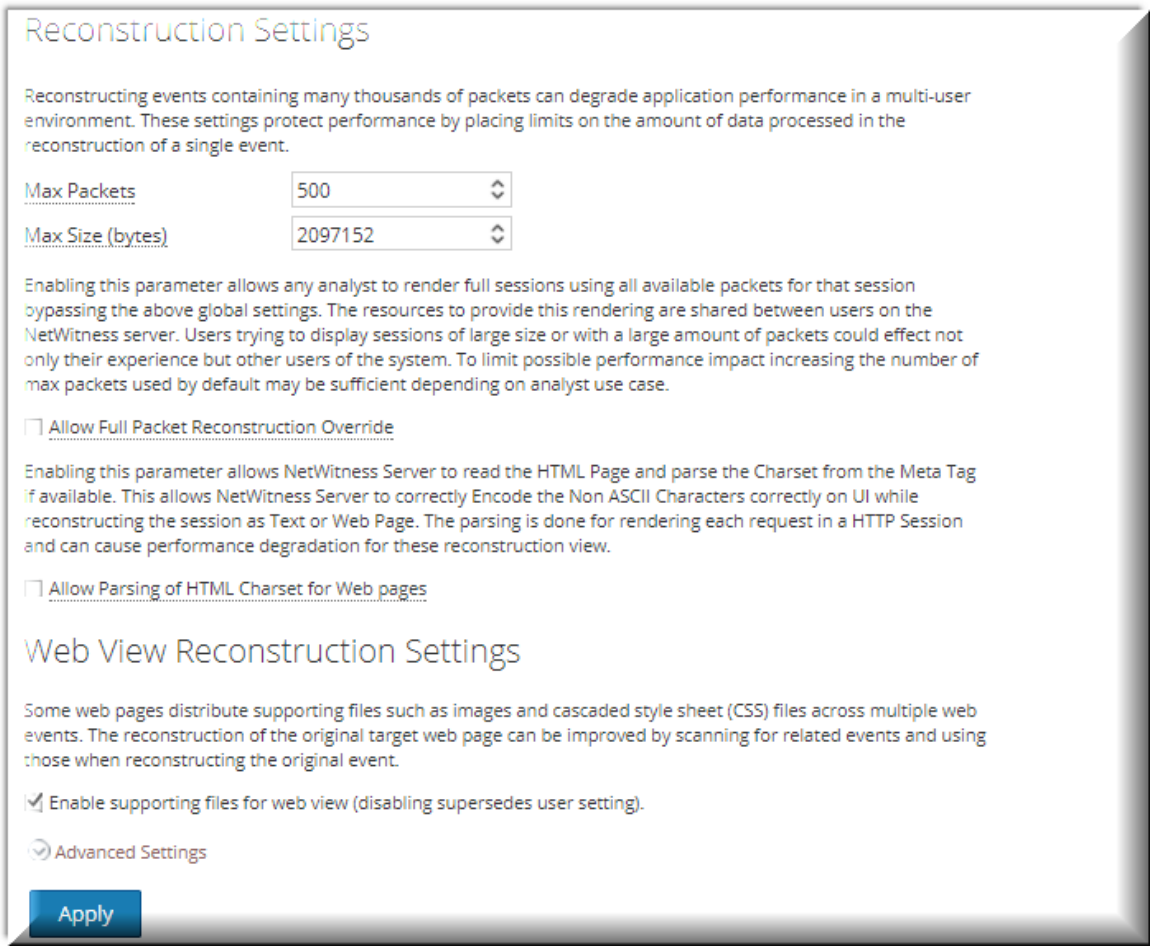
En la siguiente tabla se describe la configuración de búsqueda de eventos.

Parámetro	Descripción
Límite de eventos escaneados	Cantidad máxima de eventos que se escanean cuando se realizan búsquedas en la vista Eventos.
Límite de resultados de eventos	Cantidad máxima de resultados que se devuelven cuando se realizan búsquedas en la vista Eventos.

Configuración de la reconstrucción

A medida que los analistas reconstruyen sesiones que están investigando, algunos eventos pueden ser muy grandes y pueden contener muchos miles de paquetes de origen. La reconstrucción de estas sesiones, especialmente en un ambiente multiusuario, puede degradar el rendimiento de las aplicaciones. La configuración de la reconstrucción permite que un administrador limite la cantidad de paquetes y el tamaño de un único evento durante la reconstrucción.

Nota: se puede configurar un reemplazo para la sección Configuración de la reconstrucción para las vistas web (en Configuración de reconstrucción de vista web).



En la siguiente tabla se describen las funciones de Configuración de la reconstrucción.

Parámetro	Descripción
Cantidad máxima de paquetes para un único evento	Esta configuración protege el rendimiento mediante la definición de un límite en la cantidad de paquetes que se procesan para la reconstrucción de un único evento. Los valores posibles están en el rango de 100 a 10,000 paquetes y se ingresan manualmente o en incrementos de 100 de la lista de selección. El valor predeterminado es 100 paquetes.

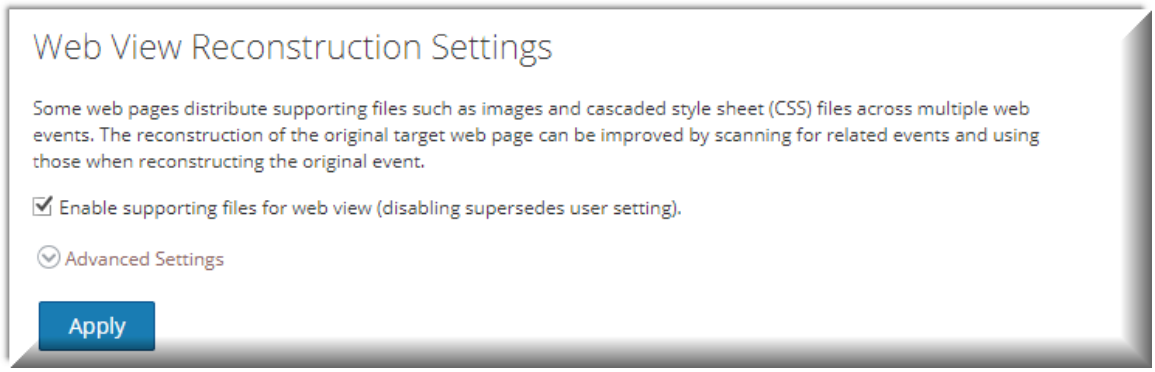
Parámetro	Descripción
Tamaño máximo, en bytes, de un único evento	Esta configuración protege el rendimiento mediante la definición de un límite en el tamaño máximo, en bytes, de la reconstrucción de un único evento. Los valores posibles están en el rango de 102,400 a 104,857,600 bytes y se ingresan manualmente o en incrementos de 10,240 de la lista de selección. El valor predeterminado es 2,097,152 bytes.
Permitir el reemplazo de Reconstrucción completa con paquetes	Cuando se selecciona esta casilla de verificación, se proporciona a los analistas un botón Usar más paquetes en el panel Reconstrucción. Esto permite que el servidor de NW vuelva a generar eventos con el uso de todos los paquetes disponibles en el evento.
Permitir el análisis del conjunto de caracteres HTML para las páginas web	Esta opción permite que el Servidor de NetWitness identifique la codificación de las páginas web definida en la etiqueta de metadatos HTML en lugar del encabezado HTTP. La configuración predeterminada es deshabilitado.

Configuración de reconstrucción de vista web

La configuración de reconstrucción de vista web permite que un administrador configure ajustes que mejoran la reconstrucción de una vista web mediante el escaneo y la reconstrucción de eventos relacionados que contienen los mismos archivos de soporte. Cuando NetWitness Suite reconstruye una vista web que abarca múltiples eventos, es posible mejorar la reconstrucción del evento objetivo con el escaneo y la reconstrucción de eventos relacionados que contienen los mismos archivos de soporte, como imágenes y archivos de hoja de estilo en cascada (CSS).

- Los únicos eventos relacionados que se escanean son eventos de tipo de servicio HTTP con la misma dirección de origen que el evento objetivo y un registro de fecha y hora dentro de un rango de tiempo especificado antes y después del evento objetivo.
- La cantidad máxima de eventos relacionados que se escanean es configurable.

Si se hace clic en la opción Configuración avanzada, se muestran todos los ajustes configurables de esta sección.



En la siguiente tabla se describe la configuración de reconstrucción de vista web.

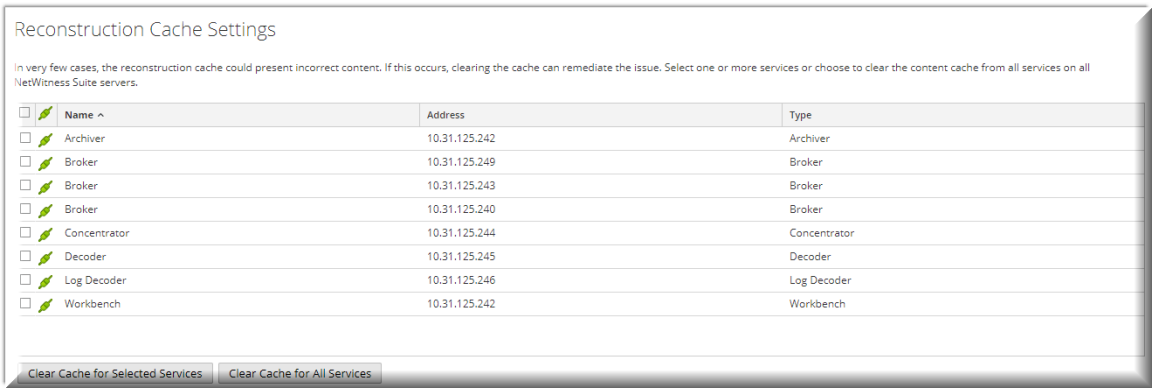
Parámetro	Descripción
Habilite los archivos de soporte para la vista web	Esta opción determina cómo se reconstruyen las vistas web que tienen datos relacionados en otras sesiones. De manera predeterminada, la opción está habilitada. Cuando está habilitada, los archivos de soporte de eventos relacionados se pueden usar en la reconstrucción de vistas web. En esta sección se habilitan ajustes adicionales para calibrar el rendimiento y los analistas tienen la opción de habilitar el uso de CSS en las reconstrucciones. Cuando está deshabilitada, los archivos de soporte de eventos relacionados no se usan y el ajuste para que los analistas habiliten el uso de CSS en reconstrucciones está deshabilitado.
Rango de tiempo para escanear eventos relacionados	Está disponible cuando se selecciona **Habilite los archivos de soporte para la vista web**. Configura el rango de tiempo dentro del cual NetWitness Suite escanea eventos relacionados que son del tipo de servicio HTTP y que tienen la misma dirección de origen que el evento objetivo. Este es un valor entre 0 y 60. • Segundos antes del evento objetivo • Segundos después del evento objetivo

Parámetro	Descripción
Limite la cantidad de eventos relacionados que se procesan	Permite la configuración de la cantidad máxima de eventos relacionados que NetWitness Suite escanea en el rango de tiempo especificado para descubrir archivos de soporte para el evento objetivo. De manera predeterminada, el parámetro está deshabilitado. Cuando se habilita, también lo hace el campo Máximo de eventos relacionados.
Máximo de eventos relacionados	Cuando se habilita el parámetro **Limite la cantidad de eventos que se procesan**, este campo especifica la cantidad máxima de eventos relacionados que NetWitness Suite escanea en el rango de tiempo especificado con el fin de descubrir archivos de soporte para el evento de destino. Este es un valor seleccionable entre 10 y 1,000 y se ingresa en incrementos de 100. El valor predeterminado es 100.
Limite la cantidad de paquetes y el tamaño de cada evento relacionado	Reemplaza la configuración general para la cantidad máxima de paquetes y el tamaño máximo (en bytes) de eventos relacionados individuales.
Cantidad máxima de paquetes para un único evento relacionado	Los valores posibles están en el rango de 100 a 10,000 paquetes y se ingresan en incrementos de 100 de la lista de selección. El valor predeterminado es 100 paquetes.

Parámetro	Descripción
Tamaño máximo, en bytes, de un único evento relacionado	Los valores posibles están en el rango de 102,400 a 104,857,600 bytes y se ingresan en incrementos de 10,240 de la lista de selección. El valor predeterminado es 524,288 bytes.

Configuración de caché de reconstrucción

En algunos casos, la caché de reconstrucción puede presentar contenido incorrecto; por esta razón, NetWitness Suite quita de la caché las reconstrucciones que tienen más de un día. La caché se borra a diario a la medianoche. Entre las limpiezas diarias de la caché, ciertas acciones pueden dejar obsoleta la caché que se usa en una reconstrucción y, si es necesario, los administradores pueden borrar manualmente la caché para uno o más servicios que están conectados al Servidor de NetWitness actual.



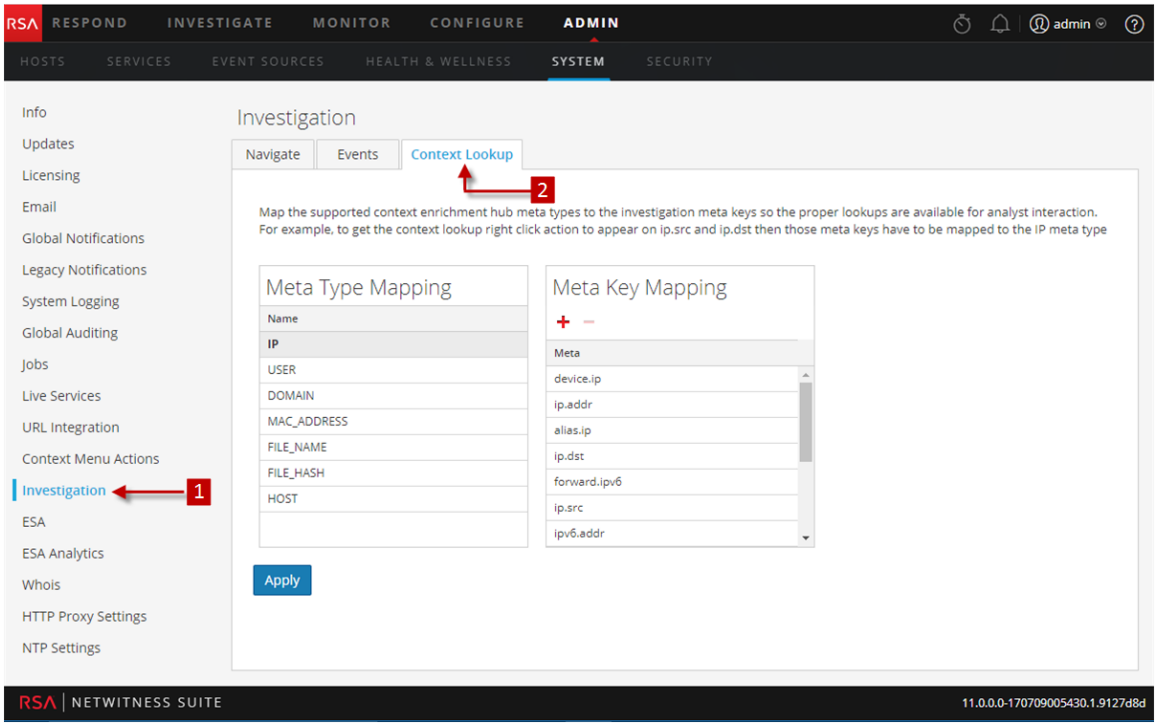
En la siguiente tabla se describen las funciones de Configuración de caché de reconstrucción.

Función	Descripción
Cuadro de selección	El cuadro de selección en filas individuales y en la barra de título permite la selección de uno o más servicios, o de todos ellos, cuya caché se debe borrar manualmente.
Borrar caché de los servicios seleccionados	Borra la caché de reconstrucción de cada servicio seleccionado.
Borrar caché de todos los servicios	Borra la caché de reconstrucción de todos los servicios.

Vista rápida

Pestaña Búsqueda de contexto

En la siguiente figura se muestra la pestaña Búsqueda de contexto.



Los procedimientos asociados con este panel se proporcionan en "Administrar mapeo de tipos de metadatos y claves de metadatos" en la *Guía de configuración de Context Hub*.

1 Muestra el panel Configuración de Investigation.

2 Muestra la pestaña Búsqueda de contexto.

Barra de herramientas y funciones

La pestaña Búsqueda de contexto permite al administrador configurar el mapeo de claves de metadatos y tipos de metadatos de Investigation. El administrador puede agregar claves de metadatos que se encuentran en Investigation a la lista de tipos de metadatos compatibles con el servicio Context Hub o quitarlas de ella.

En la siguiente tabla se describen las funciones de la pestaña Búsqueda de contexto.

Función	Descripción
+	Agrega una clave de metadatos al tipo de metadatos seleccionado compatible con Context Hub.

Función	Descripción
	Elimina la clave de metadatos del tipo de metadatos seleccionado.
Aplicar	Guarda los cambios realizados en la pestaña Búsqueda de contexto.

Panel Configuración de servicios de Live

En el panel Configuración de Servicios de Live se presentan las funciones necesarias para configurar la cuenta de Live y la conexión al servidor CMS.

Cuenta de Live consta de dos secciones: Estado de RSA Live y Descargue el registro de actividad de Live Feedback. **Inicie sesión** mediante el ingreso de sus credenciales de cuenta de Live para acceder a los servicios de Live. Para activar su cuenta de Live para NetWitness Suite, comuníquese con Atención al cliente de RSA. Cuando recibe confirmación de la configuración de su cuenta de Live, puede configurar la conexión al servidor CMS según se describe en Configurar los ajustes de servicios de Live.

El panel Servicios de Live proporciona la interfaz del usuario para:

- La cuenta de Live
- El calendario y las preferencias de actualización del contenido de Live para la notificación de actualizaciones.
- Participación en Live Feedback
- Compartir detalles de uso de Live Content
- RSA Live Connect (beta)

Cuadro de diálogo Nuevas funciones habilitadas

Cuando inicia sesión en NetWitness Suite por primera vez, aparece el cuadro de diálogo **Nuevas funciones habilitadas**.

Función	Descripción
Aceptar	Si hace clic en Aceptar, indica que está de acuerdo con lo siguiente: • Participar en Live Feedback • Permitir que NetWitness Suite envíe a RSA las métricas de uso y la versión de hosts de NW relacionadas con su ambiente, siempre que esté configurada una cuenta de Live. • Recibir datos de inteligencia de amenazas de Live Connect.
Ver configuración	Cuando hace clic en **Ver configuración**, se le redirige a la interfaz del usuario de servicios de Live para ver la configuración. Si no configuró la cuenta de Live, se muestra una pantalla enmascarada.

Para obtener información sobre Live Feedback, consulte Descripción general de Live Feedback

Para obtener información sobre comportamientos de analistas y uso compartido de datos, consulte el tema **"Comentarios y uso compartido de datos de NetWitness Suite"** en la *Guía de administración de servicios de Live*.

Para obtener información sobre Información valiosa de amenazas de Live Connect, consulte Configurar los ajustes de servicios de Live.

Flujo de trabajo

¿Qué desea hacer?

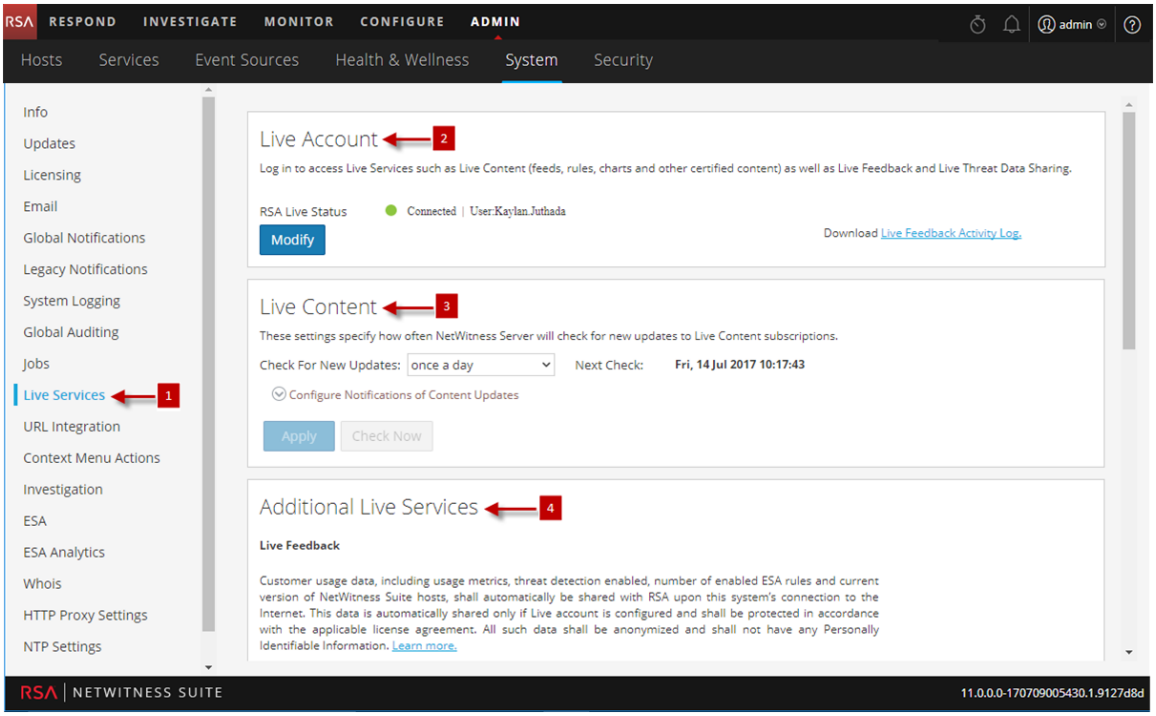
Función	Deseo…	Mostrarme cómo
Administrador	Configurar una cuenta de Live y la conexión al servidor CMS	Configurar los ajustes de correo electrónico como un servidor de notificación
Administrador	Cargar datos en RSA para Live Feedback	Cargar datos en RSA para Live Feedback
Administrador	Configurar y verificar el panel Configuración de servicios de Live	Panel Configuración de servicios de Live
Administrador	Descripción general de Live Feedback	Descripción general de Live Feedback

Temas relacionados

- Descripción general de Live Feedback
- Configurar los ajustes de servicios de Live
- Cargar datos en RSA para Live Feedback
- Guía de administración de servicios de Live

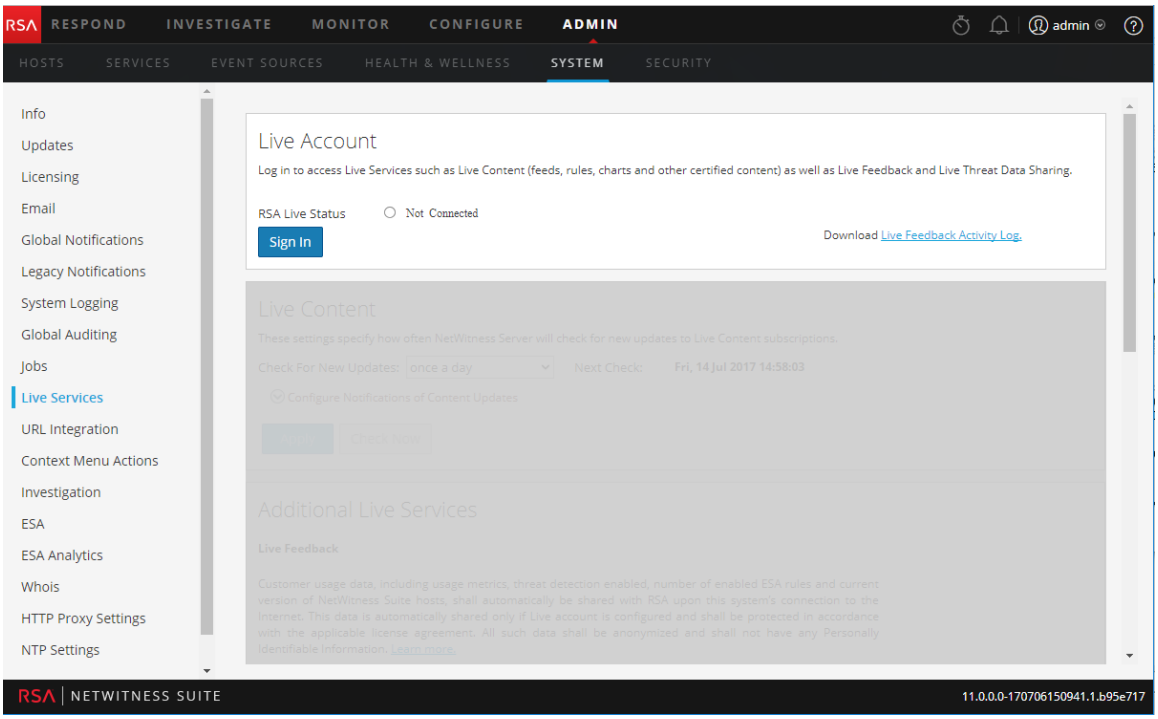
Vista rápida de los servicios de Live

Acceda a esta vista en **ADMIN > SISTEMA > Servicios de Live**.



Nota: Si no inició sesión con sus credenciales de cuenta de Live, se muestra una pantalla enmascarada.

1. Muestra el panel Configuración de Servicios de Live.
2. Ingrese las credenciales de la cuenta de Live con la ayuda de atención al cliente.
3. Ofrece una actualización para Live Content.
4. Servicios adicionales de Live proporciona Live Feedback



Barra de herramientas y funciones

El panel Configuración de Live tiene tres secciones: Cuenta de Live, contenido de Live y servicios adicionales de Live.

Sección Cuenta de Live

En la sección **Cuenta de Live**, debe ingresar las credenciales de Live. La información necesaria para configurar la cuenta de Live de un usuario consta del nombre de usuario, la contraseña y la URL de Live del sistema de administración de contenido de RSA. Esta información la proporciona Atención al cliente.

En la siguiente tabla se describen las funciones de la sección Cuenta de Live.

Función	Descripción
Host	La URL de Live del sistema de administración de contenido. Los puntos de valor predeterminado en el CMS de RSA en **cms.netwitness.com**.
Puerto	El puerto de comunicación de Live para enviar solicitudes al sistema de administración de contenido. El valor determinado para este campo es **443**, el cual es el puerto de comunicaciones del sistema de administración de contenido.
SSL	Permite que el usuario se comunique mediante SSL.
Nombre de usuario	El nombre de usuario de la cuenta de Live proporcionado por la Atención al cliente de RSA.

Función	Descripción
Contraseña	La contraseña de la cuenta de Live proporcionada por la Atención al cliente de RSA.
Probar conexión	Comprueba si la conexión se realiza correctamente o no.
Aplicar	Guarda y aplica la configuración.

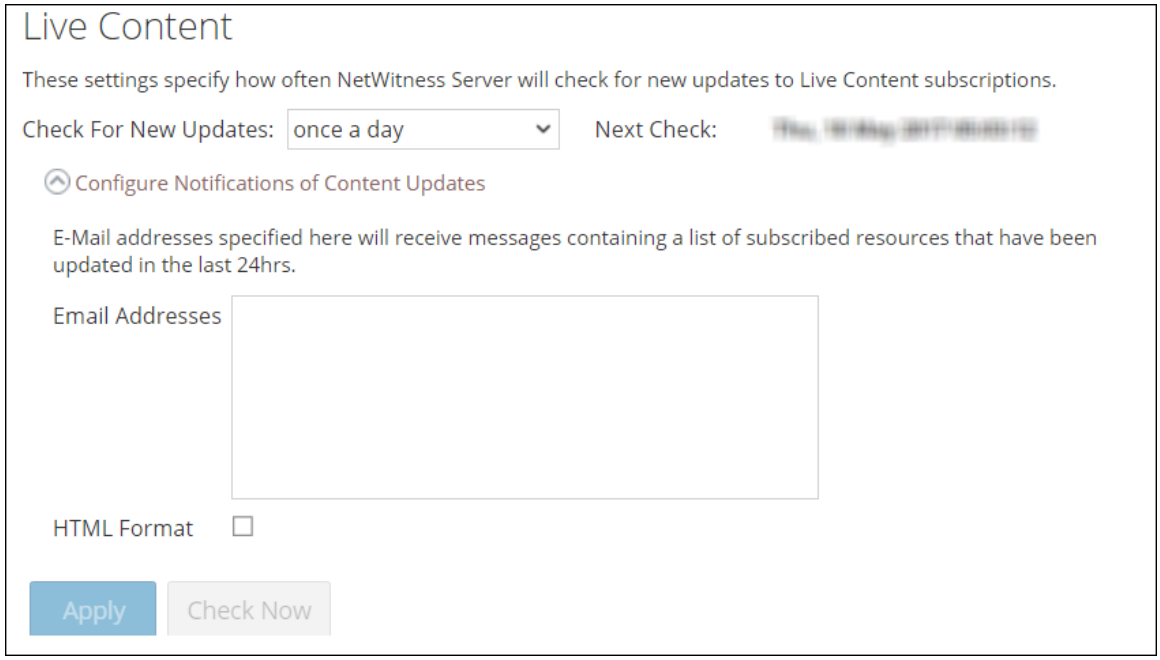
En la sección Cuenta de Live se proporciona una opción para descargar y compartir los datos históricos de Live Feedback, para lo cual se debe hacer clic en Registro de actividad de Live Feedback.

Para obtener más información sobre cómo descargar datos históricos, consulte Cargar datos en RSA para Live Feedback.

Sección Contenido de Live

Puede configurar el intervalo de sincronización y la notificación de Live Content para que NetWitness Suite compruebe si hay nuevas actualizaciones para Live Content:

Utilice el campo **Comprobar si hay nuevas actualizaciones** para cambiar el intervalo. Seleccione un intervalo en la lista desplegable. El valor predeterminado para este ajuste es **una vez al día**.



En la siguiente tabla se describen las funciones de Contenido de Live.

Función	Descripción
Comprobar si hay nuevas actualizaciones	Este ajuste indica la frecuencia con la que NetWitness Suite comprueba si hay actualizaciones nuevas para las suscripciones de Live y sincroniza los recursos y etiquetas suscritos: • una vez al día • dos veces al día • cuatro veces al día • cada hora • cada dos horas • cada media hora El valor predeterminado para este ajuste es una vez al día.
Next Check	Muestra la hora y fecha de la próxima sincronización de Live calendarizada según el intervalo configurado para la comprobación.
Direcciones de correo electrónico	Las direcciones de correo electrónico que se especifican aquí reciben mensajes con una lista de los recursos suscritos actualizados en las últimas 24 horas.
Formato HTML	Especifica el formato del mensaje de correo electrónico. • Seleccionada = HTML • No seleccionada = texto
Comprobar ahora	En lugar de esperar el próximo ciclo de recursos programados, esta opción obliga a Live a comenzar la sincronización inmediata de los recursos suscritos en esta instancia de NetWitness Suite. **Precaución:** Use esta función con precaución, porque la sincronización puede hacer se vuelva a cargar un analizador si se implementa un analizador Lua o un analizador Flex en el ciclo de actualización. Esto es aceptable una o dos veces al día, pero una cantidad de recargas de analizadores consecutivas puede provocar la pérdida de paquetes en el Decoder. Si esta es la configuración inicial y no ha configurado las suscripciones a recursos de Live, no realice la sincronización. Espere hasta que haya configurado las suscripciones.

Función	Descripción
Aplicar	Aplica la configuración modificada al comportamiento de sincronización de la suscripción. Los cambios se implementan inmediatamente. Si se modifica la fecha, se actualiza el campo **La próxima sincronización de Live está calendarizada para**.

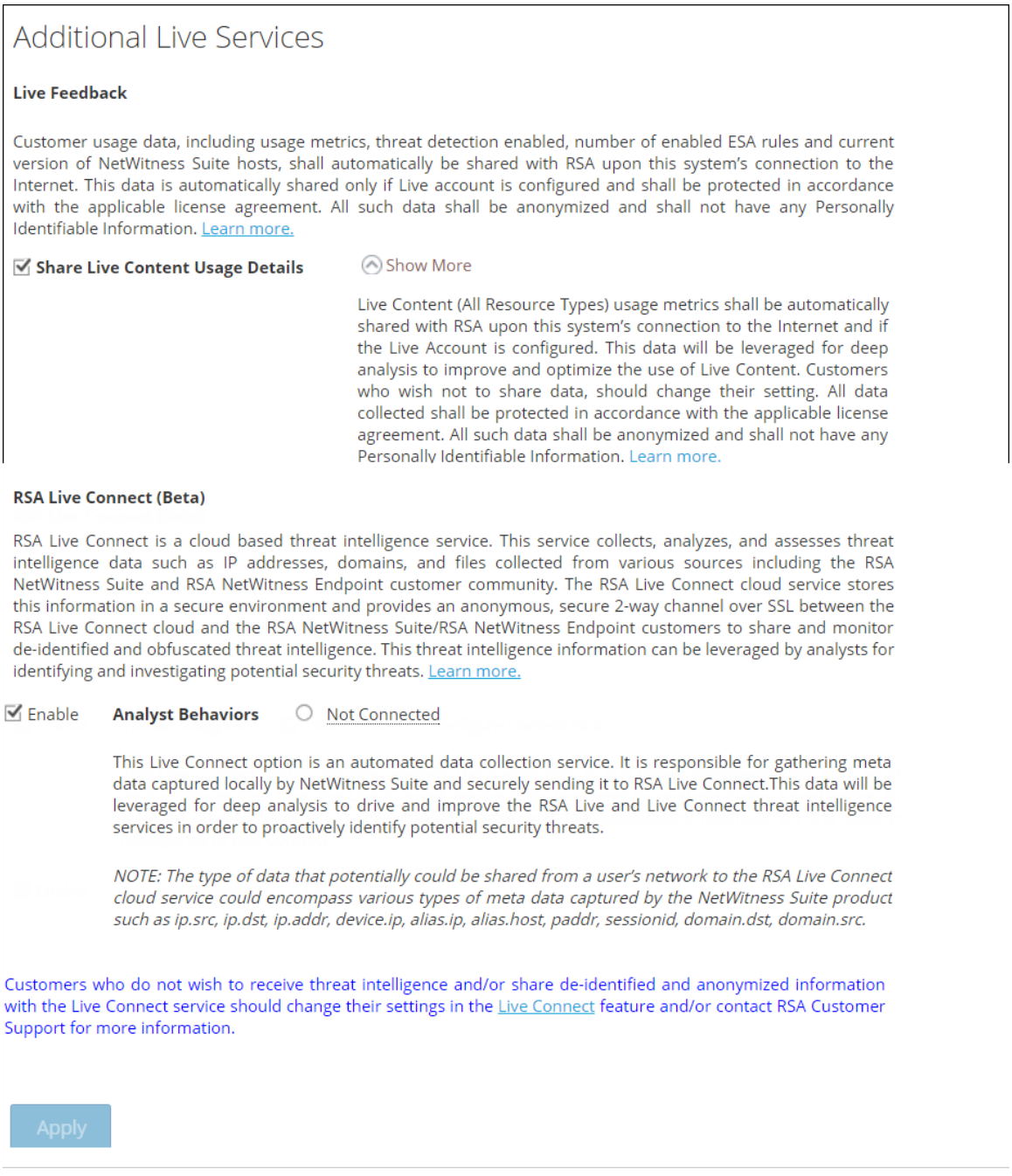
Forzar sincronización inmediata

Para forzar la sincronización inmediata, haga clic en **Comprobar ahora**. NetWitness Suite busca actualizaciones en los recursos suscritos.

En lugar de esperar el próximo ciclo de recursos programados, esta opción obliga a Live a comenzar la sincronización inmediata de los recursos suscritos en esta instancia de NetWitness Suite. Un uso para esto es ver el impacto inmediato de un cambio de configuración. Por ejemplo, se agregó un nuevo servicio, o se han alternado nuevos recursos para una implementación automática. La sincronización programada podría realizarse horas más tarde si Servicios de Live está configurado para sincronizarse varias veces al día.

Precaución: La sincronización puede hacer que se vuelva a cargar un analizador si se implementa un analizador Flex en el ciclo de actualización. Esto es aceptable una o dos veces al día, pero una cantidad de recargas de analizadores consecutivas puede provocar la pérdida de paquetes en el Decoder. Si esta es la configuración inicial y no ha configurado las suscripciones a recursos de Live, no realice la sincronización. Espere hasta que haya configurado las suscripciones.

Servicios adicionales de Live



Nota: Haga clic en Más información para conocer más sobre los datos que recopila RSA. Para obtener más información, consulte Descripción general de Live Feedback.

En las siguientes tablas se describen las funciones de Servicios adicionales de Live.

Función	Descripción

Live Feedback	Muestra los tipos de datos que recopila RSA:
	• Nombre del producto
	• Versión del producto
	• Instancia del producto
	• Clave de activación
	• Detalles de cada componente, como:
	  • ID
	  • Nombre
	  • Versión
	  • ID de la instancia
	• Métricas de cada componente

Compartir detalles de uso de Live Content	Permite que NetWitness Suite envíe a RSA datos técnicos anónimos sobre las métricas de uso del contenido. Esta opción está habilitada de manera predeterminada.
RSA Live Connect	Proporciona más información sobre el servicio Live Connect y la configuración de los servicios de Live.
Habilitar (Información valiosa de amenazas)	Habilita la función Información valiosa de amenazas, en la cual Live Connect se agrega como un origen de datos para el servicio Context Hub y el analista puede extraer datos de inteligencia de amenazas durante una investigación. Antes de habilitar esta función, asegúrese de que Context Hub esté configurado. Esta opción está habilitada de manera predeterminada (seleccionada)
Habilitar (Comportamientos de analistas)	Permite que NetWitness Suite envíe a RSA datos técnicos anónimos sobre su ambiente. Esta opción está habilitada de manera predeterminada (seleccionada)

Función	Descripción
Aplicar	Aplica los cambios configurados. Los cambios se implementan inmediatamente. **Nota:** Esta opción se aplica solo a Información valiosa de amenazas y Comportamientos de analistas.

Acerca de la participación en Live Feedback

Cuando participa en Live Feedback, se recopila información pertinente que permite mejoras. Para obtener información sobre Live Feedback, consulte Descripción general de Live Feedback.

Cuando instale NetWitness Suite, se le preguntará si desea participar en Live Feedback. Para obtener información, consulte Configurar los ajustes de servicios de Live

Si es necesario, puede descargar manualmente los datos de uso histórico y compartirlos con RSA. Para obtener información sobre cómo descargar los datos de uso histórico y compartirlos con RSA, consulte Cargar datos en RSA para Live Feedback.

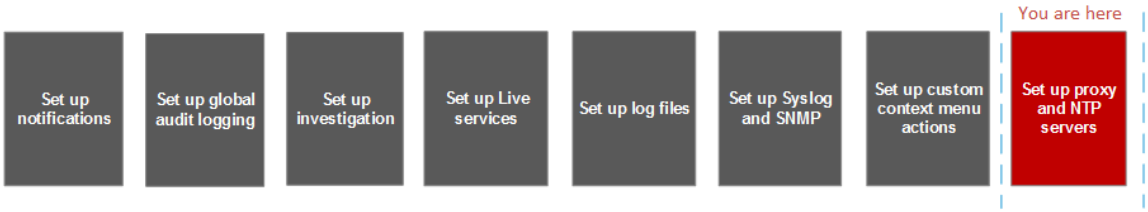
Panel Configuración de NTP

El panel Configuración de NTP es un protocolo diseñado para sincronizar los relojes de la máquina host en una red. Para obtener más información sobre NTP, consulte su página de inicio (http://www.ntp.org/).

Nota: Los hosts de NetWitness Suite Core deben poder comunicarse con el host de NW con el puerto 123 de UDP para la sincronización horaria de NTP.

Use la vista **ADMIN** > **Sistema** > **Configuración de NTP** para configurar uno o más servidores NTP. Después de configurar un servidor NTP, NetWitness Suite usa NTP para sincronizar los relojes de la máquina host. Configure varios servidores NTP con fines de conmutación por error.

Flujo de trabajo



¿Qué debe hacer?

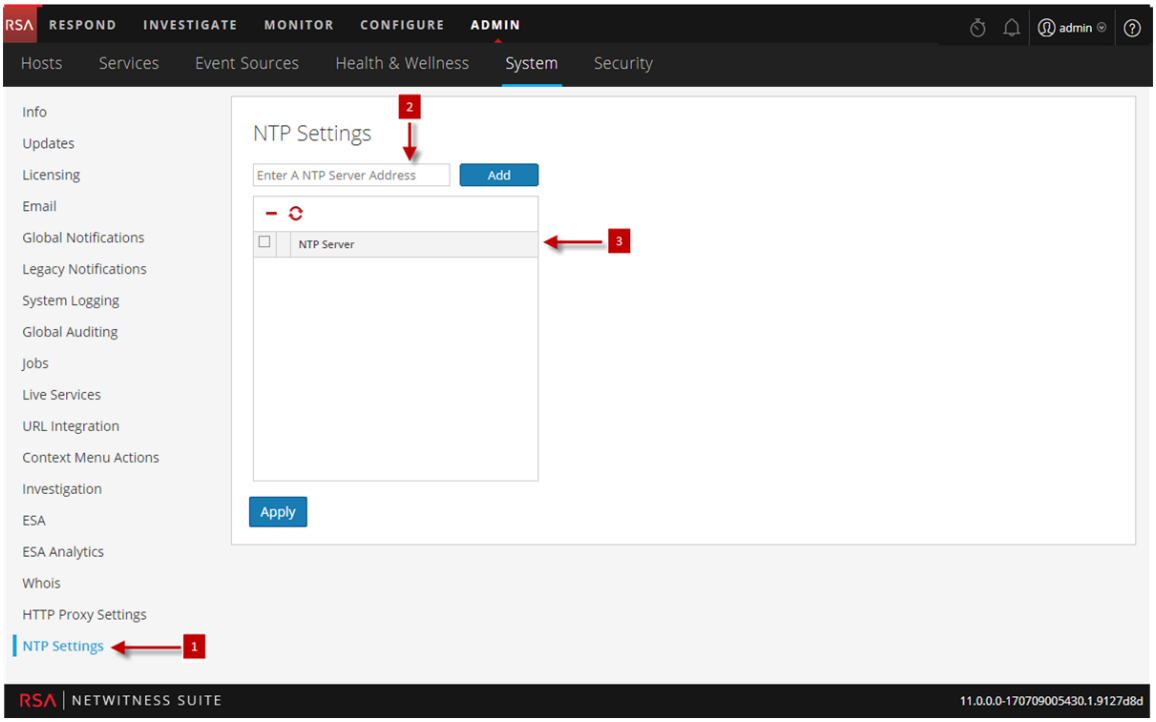
Función	Deseo…	Mostrarme cómo
Administrador	Agregar o modificar un servidor NTP	Configurar servidores NTP

Temas relacionados

- Configurar servidores NTP
- Solución de problemas de configuración del servidor NTP

Vista rápida

En el siguiente ejemplo se ilustra un panel Configuración de NTP. En el panel se define cómo agregar un servidor NTP al panel Configuración de NTP.



1 Muestra el panel Configuración de NTP.

2 Ingrese el nombre de host o la dirección IP del servidor NTP.

3 haga clic en un nombre de host existente

Barra de herramientas y funciones

En la siguiente tabla se describen los ajustes del panel Configuración de NTP.

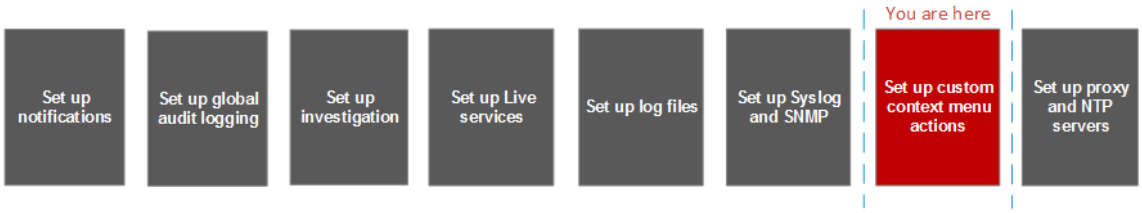
Configuración	Descripción
	Ingrese el nombre de host o la dirección IP del servidor NTP.
Agregar	Agrega el servidor NTP a NetWitness Suite.
	Elimina el servidor NTP seleccionado.
	Sincroniza el servidor NTP seleccionado.
	Selecciona el servidor NTP que desea eliminar o sincronizar.

Configuración	Descripción
Servidor NTP	Nombre de host o dirección IP del servidor NTP. Si hace clic en un nombre de host existente, NetWitness Suite hace que el nombre de host sea editable y muestra los siguientes botones de comando: • **Actualizar**: aplica las ediciones. • **Cancelar**: cancela las ediciones.
Aplicar	Aplica la configuración del servidor NTP y sincroniza los relojes de la máquina host con NTP.

Panel Acciones del menú contextual

En el panel Acciones del menú contextual, los administradores pueden ver acciones de menú contextual integradas, y agregar, editar o eliminar acciones de menú contextual personalizadas que aparecen como opciones en un menú contextual.

Flujo de trabajo



¿Qué desea hacer?

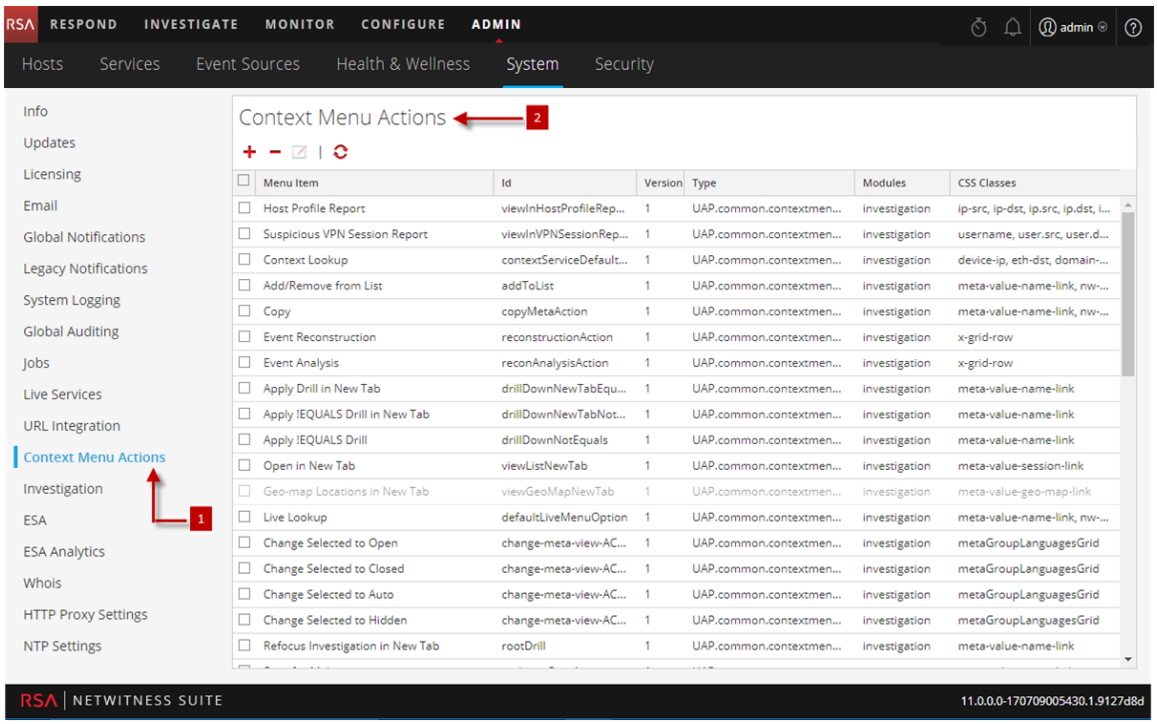
Función	Deseo…	Mostrarme cómo
Administrador	Panel Acciones del menú contextual personalizadas	Agregar acciones de menú contextual personalizadas.

Temas relacionados

- Agregar acciones de menú contextual personalizadas

Vista rápida

La siguiente figura es un ejemplo del panel Acciones del menú contextual.



1	Muestra el panel Acciones del menú contextual.
2	La barra de herramientas permite que el usuario agregue, edite y elimine acciones del menú contextual.

Barra de herramientas y funciones

El panel Acciones del menú contextual tiene una cuadrícula y una barra de herramientas. En la siguiente tabla se describen las opciones de la barra de herramientas y las funciones de la cuadrícula.

Funciones	Descripción
+	Muestra el cuadro de diálogo Configuración de menú contextual, en el cual puede crear una acción contextual nueva.
↻	Actualiza la lista.
−	Elimina las acciones contextuales nuevas. NetWitness Suite no solicita la confirmación de que desea eliminar la acción. Las acciones seleccionadas se eliminan inmediatamente sin oportunidad de cancelación.

Funciones	Descripción
	Muestra el cuadro de diálogo Editar acción contextual, en el cual puede editar una acción contextual existente.
Elemento de menú	El elemento de menú como aparece en el menú contextual. Cuando se crea una acción de menú contextual, el parámetro es `displayName`. La siguiente es una línea de código de ejemplo: `"displayName": "User Agent String Lookup”`
ID	El ID único para la acción en contexto. Cuando se crea una acción de menú contextual, el parámetro es `id`. La siguiente es una línea de código de ejemplo: `"id": "UserAgentStringAction"`
Versión	El número de la versión de la acción contextual. Cuando se crea una acción de menú contextual, el parámetro es `version`. La siguiente es una línea de código de ejemplo: `"version": "1"`
Tipo	El tipo de acción de contexto. Cuando se crea una acción de menú contextual, el parámetro es `type`. Todos los tipos de acción contextual de NetWitness Suite comienzan con esta cadena: `UAP.common.contextmenu.actions`. La última parte de la cadena identifica el menú dentro de NetWitness Suite, por ejemplo, `URLContextAction` o `LivePostContextAction`. La siguiente es una línea de código de ejemplo: `"type": "UAP.common.contextmenu.actions.URLContextAction"`

Funciones	Descripción

Módulos	Los nombres de los módulos en los cuales la acción de contexto está disponible. Actualmente, todas las acciones de menú contextual incorporadas corresponden al módulo Investigation.
	Cuando se crea una acción de menú contextual, el parámetro es `modules`.
	La siguiente es una línea de código de ejemplo:
	`"modules": [`
	`"investigation"`
	`],`

Clases de módulo	Las clases CSS que identifican los nombres de los módulos en los cuales la acción contextual está disponible. Actualmente, todas las acciones de menú contextual incorporadas corresponden al módulo Investigation y a continuación se describen detalladamente las clases de módulo de claves no de metadatos.
	Estas son algunas líneas de código de ejemplo:
	`"moduleClasses": [`
	`"UAP.investigation.navigate.view.NavigationPanel", <-- Enabled in Navigate pane-->`
	`"UAP.investigation.events.view.EventGrid"`
	`],`

Clases de CSS	Las clases CSS a las cuales se aplica la acción de menú contextual. Las clases CSS definen el lugar donde se muestra el menú contextual dentro de Investigation cuando hace clic con el botón secundario. Cuando se crea una acción de menú contextual, el parámetro es `cssClasses`.
	La siguiente es una línea de código de ejemplo:
	`"cssClasses": [`
	`"client"`
	`]`
	La mayoría de las clases CSS que puede agregar son claves de metadatos. También puede agregar determinadas clases CSS de claves que no son de metadatos A continuación consulte detalles adicionales y ejemplos.

Clases CSS y ejemplos

Las clases CSS pueden ser claves de metadatos y no de metadatos.

Clases CSS de clave de metadatos

Un tipo de clase CSS que puede agregar corresponde a claves de metadatos. En el caso de las claves de metadatos que tienen un punto, cámbielo por un guión cuando defina una clase CSS. Por ejemplo, la clave de metadatos `alias.host` se convierte en la clase CSS `alias-host`. La clave de metadatos `ip.src` se convierte en la clase CSS `ip-src`.

Clases CSS de clave no de metadatos

Las clases CSS de clave no de metadatos integrados también están disponibles. Las clases de la siguiente tabla definen acciones y la parte de la interfaz del usuario donde la acción está disponible.

Clase CSS	Tipo	Descripción
`meta-value-session-link`	Acción	Abrir en número de conteo de sesiones de metadatos
`meta-value-name-link`	Acción	Abrir en nombre de valor de metadatos
`nw-event-value`	Acción	Usar para acciones contextuales de reconstrucción en valor de metadatos
`UAP.investigation.navigate.view.NavigationPanel`	Interfaz del usuario	Se aplica a la vista Navegar
`UAP.investigation.events.view.EventGrid`	Interfaz del usuario	Se aplica a la vista Eventos
`UAP.investigation.reconstruction.view.content.ReconstructedEventDataGrid`	Interfaz del usuario	Se aplica a la vista Reconstrucción de evento

Ejemplo

Este es un ejemplo comentado de una acción de menú contextual para validar al agente de usuario de la clave de metadatos Aplicación de cliente (cliente). Los comentarios se eliminan automáticamente una vez aplicados en la vista sistema de Administration. El nuevo elemento de menú se muestra después del reinicio del navegador.

```
{
     "displayName": "User Agent String Lookup”, <!-- What name shows up
in NW UI -->
     "cssClasses": [
         “client”  <!-- What meta key to launch from -->
     ],
     "description": "",
     "type": "UAP.common.contextmenu.actions.URLContextAction",
     "version": "1",
     "modules": [
         "investigation"
     ],
     "local": "false",
     "groupName": "externalLookupGroup”, <!-- What group to show link
in. Remove line to show in main list -->
     "urlFormat": "http://www.useragentstring.com/?uas={0}&getText=all”, <!-- The
{0} gets replaced with whatever was right clicked on -->
     "disabled": "",
     "id": "UserAgentStringAction",
    "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel”, <-- Enabled
in Navigate pane-->
        “UAP.investigation.events.view.EventGrid” <-- Enabled in Event
View pane -->
     ],
     "openInNewTab": "true",
     "order": "15"
 }
```

Panel Configuración de notificaciones antiguas

El panel Configuración de notificaciones antiguas proporciona la capacidad de configurar ajustes de notificación de syslog y SNMP. Estas configuraciones se usan para la autorización, la administración de orígenes de eventos (ESM) existente, el monitoreo de Warehouse Connector y el monitoreo de Archiver.

Los procedimientos relacionados con estos ajustes se describen en Configurar ajustes de syslog y SNMP.

Flujo de trabajo

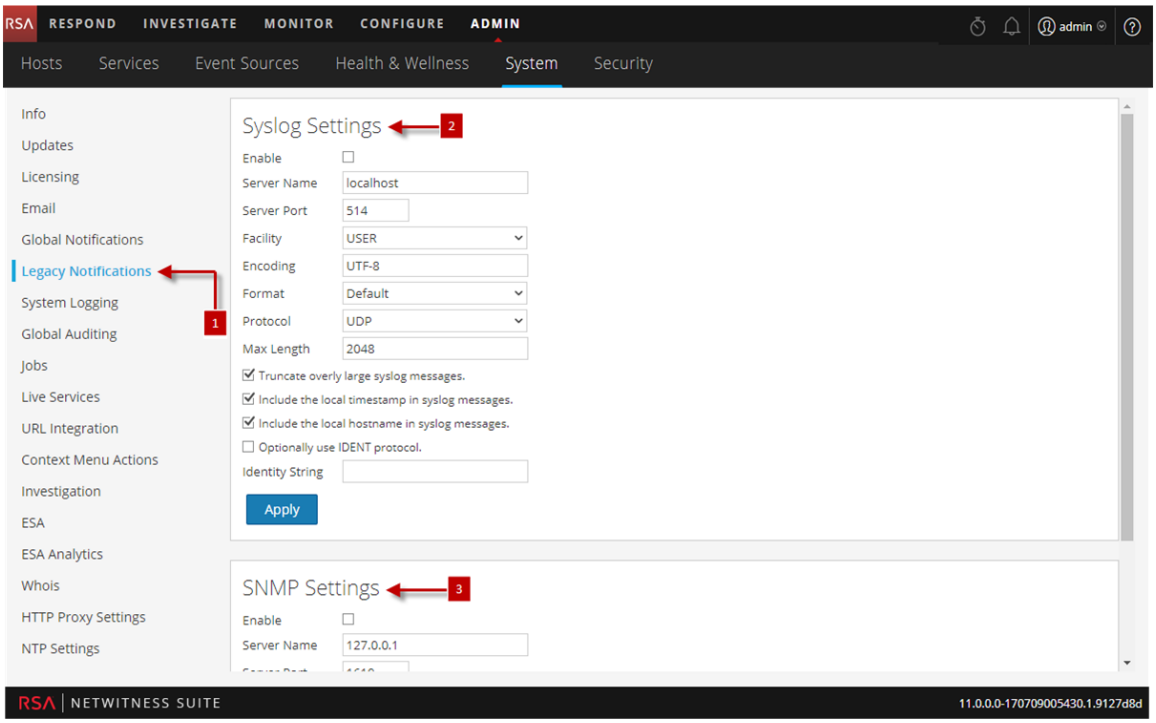
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar ajustes de syslog	Configurar ajustes de syslog y SNMP
Administrador	Configurar ajustes de SNMP	Configurar ajustes de syslog y SNMP

Temas relacionados

- Configurar ajustes de syslog y SNMP

Vista rápida



1	Muestra el panel Configuración de notificaciones antiguas.
2	Permite que el usuario configure notificaciones de syslog para la autorización, la administración de orígenes de eventos (ESM) existente, el monitoreo de Warehouse Connector y el monitoreo de Archiver.
3	Permite que el usuario configure notificaciones de SNMP para la autorización, la administración de orígenes de eventos (ESM) existente, el monitoreo de Warehouse Connector y el monitoreo de Archiver.

Barra de herramientas y funciones

El panel Configuración de notificaciones antiguas consta de dos secciones: Configuración de syslog y Configuración de SNMP.

Configuración de syslog

En la siguiente tabla se describen las opciones disponibles para configurar notificaciones de syslog para la autorización, la administración de orígenes de eventos (ESM) existente, el monitoreo de Warehouse Connector y el monitoreo de Archiver.

Función	Descripción
Habilitar	Habilita los ajustes de syslog configurados aquí.
Nombre del servidor	Especifica el host donde se ejecuta el proceso de syslog objetivo.
Puerto del servidor	Especifica el puerto donde se ejecuta el proceso de syslog objetivo.
Funcionalidad	Especifica la instalación de syslog designada que se usará en todos los mensajes salientes. Los valores posibles son KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP y LOCAL1 a LOCAL7.
Codificación	Especifica la codificación que se utilizará para el texto de los mensajes de syslog, por ejemplo, UTF-8.
Formato	Especifica el formato del mensaje. Los valores posibles son: Predeterminado, PCI DSS o SEC.
Protocolo	Especifica el protocolo de comunicaciones que se usa cuando se envían syslogs: UDP o TCP. El protocolo UDP se selecciona de forma predeterminada.
Longitud máxima	Especifica la longitud máxima de cualquier mensaje de syslog en bytes. El valor predeterminado es **2048**. Los mensajes que superan la longitud máxima se truncan cuando se selecciona la casilla de verificación **Truncar los mensajes de syslog demasiado grandes**.
Truncar los mensajes de syslog demasiado grandes.	Cuando se selecciona, se truncan todos los mensajes que excedan la longitud máxima.
Incluye el registro de fecha y hora local en los mensajes de syslog	Cuando se selecciona, NetWitness Suite incluye el registro de fecha y hora local en los mensajes.

Función	Descripción
Incluya el nombre de host local en los mensajes de syslog	Cuando se selecciona, NetWitness Suite incluye el nombre de host local en los mensajes de syslog.
De manera opcional, use el protocolo IDENT	Cuando se selecciona, NetWitness Suite adjunta la cadena de identidad a las alertas de syslog salientes.
Cadena de identidad	Esta es una cadena de identidad que se adjuntará al inicio de cada alerta de syslog. Si la cadena está en blanco, no hay cadena de identidad adjuntada al principio de las alertas de salida de syslog. Puede usar esto para identificar el origen de la alerta. Los usuarios la establecen de manera convencional en el nombre del programa que envía el mensaje de syslog.
Aplicar	Aplica los ajustes de configuración de syslog.

Configuración de SNMP

En la siguiente tabla se describen las opciones disponibles para configurar notificaciones de SNMP para la autorización, la administración de orígenes de eventos (ESM) existente, el monitoreo de Warehouse Connector y el monitoreo de Archiver.

Función	Descripción
Habilitar	Habilita los ajustes de SNMP configurados aquí.
Nombre del servidor	Especifica el host de SNMP trap.
Puerto del servidor	Especifica el puerto de escucha del host SNMP trap
Versión de SNMP	Especifica la versión de SNMP, **v1** o **v2c**.
OID de traps	Especifica el ID de objeto del SNMP trap en el host de trap que recibe el evento de auditoría. El valor predeterminado es **0.0.0.0.0.1**.

Función	Descripción
Comunidad	Especifica la cadena de Community que se usa para la autenticación en el host de SNMP trap. El valor predeterminado es **public**.
Habilitar	Habilita las notificaciones de SNMP como se configuraron aquí.
Aplicar	Aplica los ajustes de configuración de SNMP.