RSA NETWITNESS® SUITE

# Guía de administración de servicios de Live

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

# Administración de servicios de Live

RSA NetWitness Suite Live es el gateway a un ambiente enriquecido que ofrece acceso a feeds, herramientas y otros recursos.

## NetWitness Suite Live

Live es el componente de NetWitness Suite que administra la comunicación y la sincronización entre los servicios de NetWitness Suite y una biblioteca de contenido de Live disponible para los clientes de RSANetWitness Suite. Live proporciona una interfaz sencilla para navegar, seleccionar e implementar contenido desde el Sistema de administración de contenido de NetWitness Suite Live en los servicios y el software de NetWitness Suite. Además, para administrar feeds desde la librería de CMS, Live permite a los usuarios implementar feeds y paquetes personalizados.

## Librería de CMS

La biblioteca del sistema de administración de contenidos (CMS) (conocida como *Live*) es una valiosa fuente de los últimos recursos de seguridad en Internet para los clientes de NetWitness Suite. Proporciona una vista de la inteligencia colectiva y las habilidades analíticas de la comunidad de seguridad de todo el mundo para garantizar que los usuarios cuenten con la visibilidad más reciente de los vectores de ataque.

Live recopila la mejor inteligencia de amenazas avanzadas y el contenido de la comunidad de seguridad global (las ideas, las investigaciones, el rastreo continuo y los análisis), y los lleva directamente al centro de operaciones de seguridad del usuario para clasificar de manera definitiva las computadoras asociadas a botnets, malware y otras vulnerabilidades de seguridad maliciosas. Live agrega, consolida y destaca solo la información más pertinente para una organización en tiempo real.

## Comentarios y uso compartido de datos de NetWitness Suite

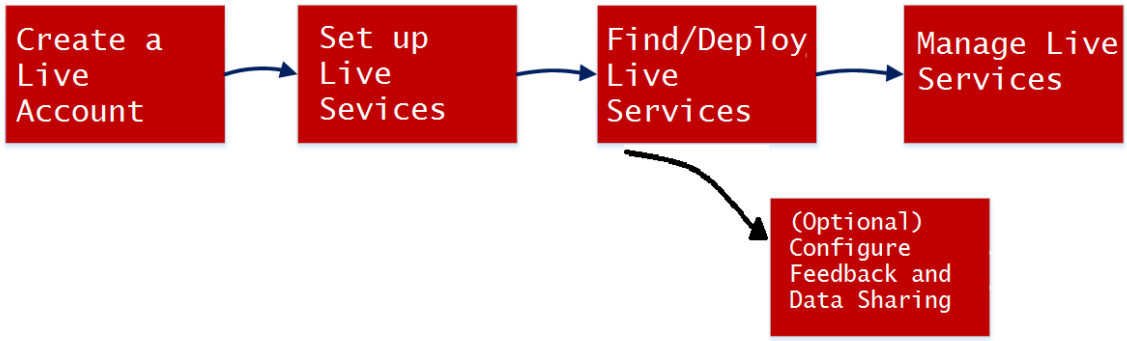
**Live Feedback** está diseñado para ayudar a mejorar RSA NetWitness Suite. Una vez que se configura una cuenta de Live, los datos de uso se comparten con RSA.

**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 de diversos orígenes. Proporciona **información valiosa de amenazas**, que ofrece a los analistas la capacidad para extraer datos de inteligencia de amenazas desde el servicio de Live Connect. También ofrece **Comportamientos de analistas**, un servicio de recopilación de datos automatizado con el objetivo de compartir inteligencia de amenazas potenciales para el análisis.

Para obtener más detalles, consulte Comentarios y uso compartido de datos de NetWitness Suite.

# Procedimientos requeridos de los servicios de Live

El siguiente flujo de trabajo detalla la configuración básica en cuatro pasos, que se pueden realizar de forma individual. La manera más fácil de configurar el Decoder es seguir el procedimiento de punto a punto en esta sección, Procedimientos requeridos de los servicios de Live), que incluye todos los pasos.

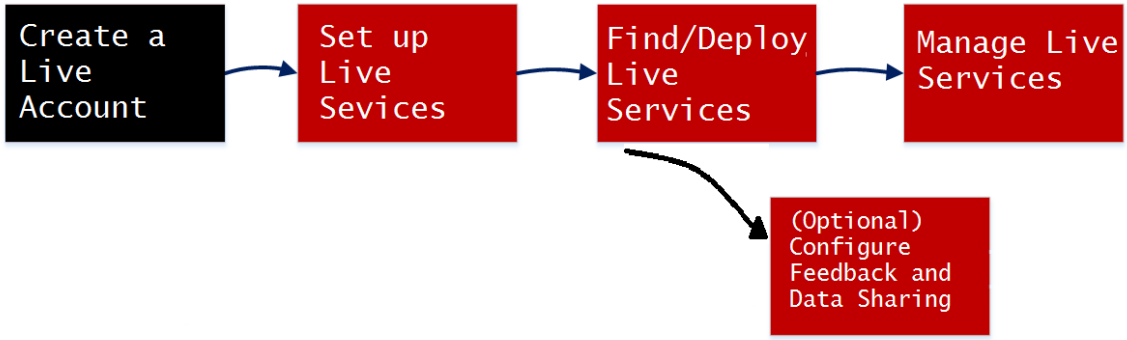



| Paso de configuración | Descripción |
|---|---|
| Crear una cuenta de Live | Crear una cuenta de Live en el portal de registro de RSA Live, URL: https://cms.netwitness.com/registration/. Si tiene una cuenta, puede administrarla mediante este portal. |
| Configurar los servicios de Live en NetWitness Suite | Configurar los servicios de Live en NetWitness Suite mediante la configuración de una conexión con el servidor de CMS. |
| Buscar e implementar recursos de Live | Buscar recursos en la vista Búsqueda en Live y, a continuación, implementar los recursos seleccionados. |
| Administrar de recursos de Live | Procedimientos para que los administradores puedan buscar, suscribirse e implementar recursos de Live. |

| Paso de configuración | Descripción |
| --- | --- |
| Comentarios y uso compartido de datos de NetWitness Suite | Describe los comentarios y las funciones de uso compartido de datos que se proporcionan en RSA NetWitness® Suite, desde los servicios de Live. La participación es opcional, pero puede ayudar a proporcionar inteligencia de amenazas útil para la comunidad. |

## Crear una cuenta de Live

Debe crear una cuenta de Live mediante el Portal de registro de RSA Live en el servidor de CMS. La biblioteca de CMS proporciona acceso a todo el contenido de RSA en un lugar donde puede ver, buscar, implementar y suscribirse a este contenido. Debe registrarse en el Portal de registro de RSA Live y seleccionar un nivel de suscripción.



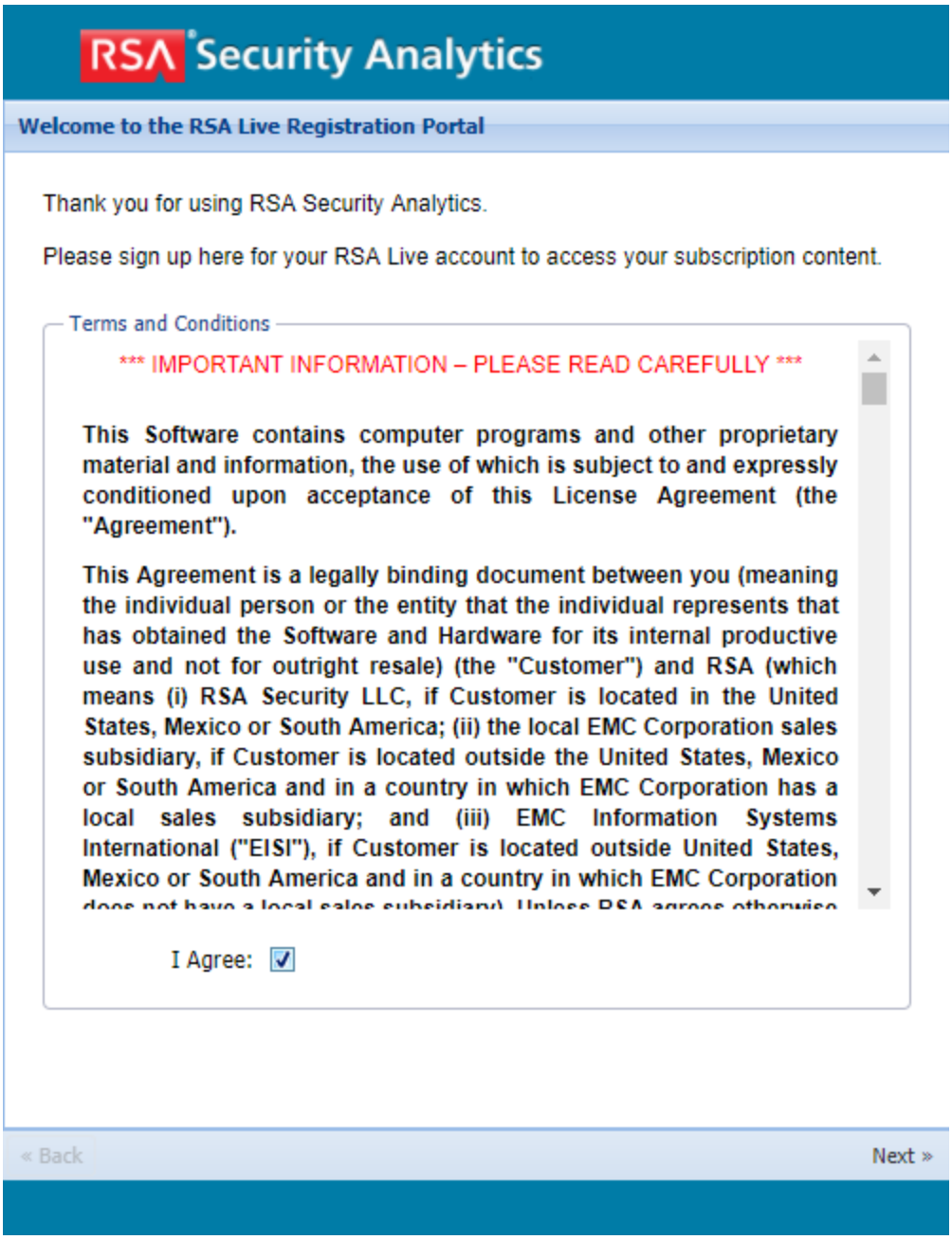

Asegúrese de que esté disponible lo siguiente para configurar una cuenta de RSA Live:

- Una conexión a Internet activa para acceder al portal.
- Un servidor de licencia de NetWitness Suite válido y registrado en el servidor de Flexera antes de que pueda registrarse para una cuenta de Live. Puede ver el ID de licencia en el panel **ADMIN > Sistema > Información**.

**Nota:** Si el servidor de licencia no está configurado, póngase en contacto con el servicio al cliente de RSA.

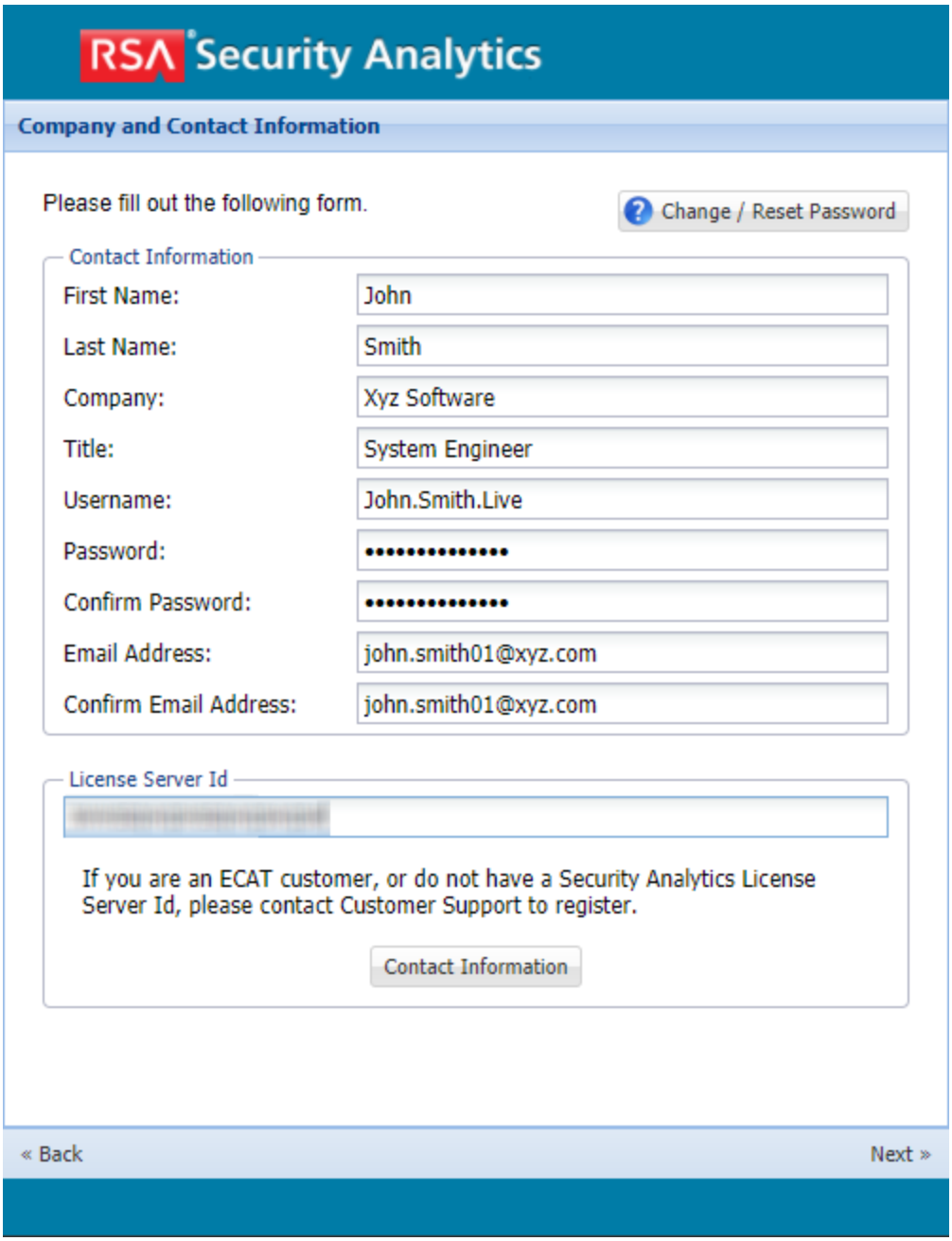
### Para crear una cuenta de Live:

1. Acceda al portal Registro de RSA Live mediante la URL: https://cms.netwitness.com/registration/.
   Se muestra la página Bienvenida.
2. Lea detenidamente los Términos y condiciones y seleccione la casilla de verificación **Acepto**, como se muestra a continuación:




3. Haga clic en **Siguiente**.
4. En la sección **Información de contacto**, ingrese valores en todos los campos, como se muestra a continuación:
   - El **nombre de usuario** debe contener un mínimo de nueve caracteres y un máximo de 60.
   - La **contraseña** debe contener un mínimo de nueve caracteres y un máximo de 60, con al menos uno en mayúscula, uno en minúscula, un número y un carácter especial.

- La **dirección de correo electrónico** que ingresa se usa para enviar notificaciones relacionadas con la cuenta de Live.




5. En la sección **Nivel de suscripción**, seleccione uno de los siguientes niveles de suscripción:
   - **Basic**: Brinda acceso al contenido de Live etiquetado para grupos como Basic, Panorama for Log Decoder y Spectrum for Malware Analysis.
   - **Enhanced**: Brinda acceso al contenido de Live etiquetado para grupos como Enhanced, Basic, Panorama for Log Decoder y Spectrum for Malware Analysis.

- **Premium**: Brinda acceso al contenido de Live etiquetado para grupos como Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder y Spectrum for Malware Analysis.

6. En la sección **Confirmar nivel de suscripción**, seleccione nuevamente el nivel de suscripción para confirmarlo.
7. Ingrese el **Identificador de servidor de licencia**. Puede ver el ID de licencia en la página **ADMIN > Sistema > Información**.

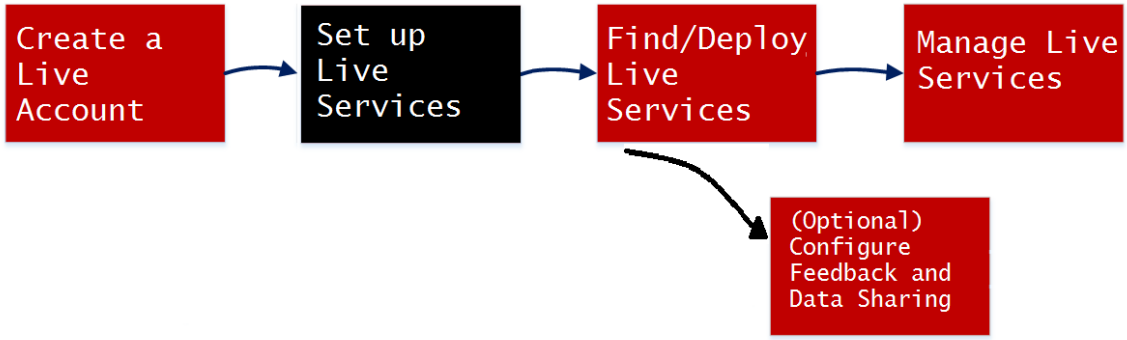
   **Precaución:** Asegúrese de que el ID del servidor de licencia en NetWitness Suite sea válido y que esté registrado en el servidor de Flexera. Si no es así, póngase en contacto con el servicio al cliente de RSA.

8. Haga clic en **Siguiente**.

Si el registro se realiza correctamente, recibirá un correo electrónico de confirmación de la cuenta de RSA Live con su nombre de usuario. Ahora tiene acceso al contenido suscrito.

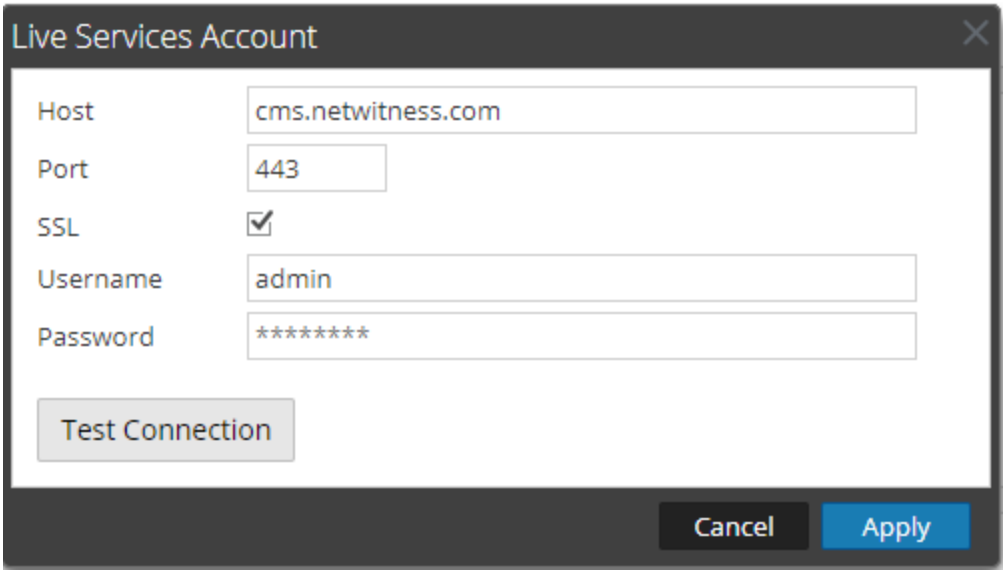
## Configurar los servicios de Live en NetWitness Suite

Para configurar Live en NetWitness Suite, configure la conexión y la sincronización entre el servidor de CMS y NetWitness Suite. La interfaz del usuario para esta configuración es ADMIN > Sistema > panel Configuración de servicios de Live.




### Para configurar la conexión al servidor de CMS:

1. Configure la conexión al servidor CMS y la cuenta de Live.

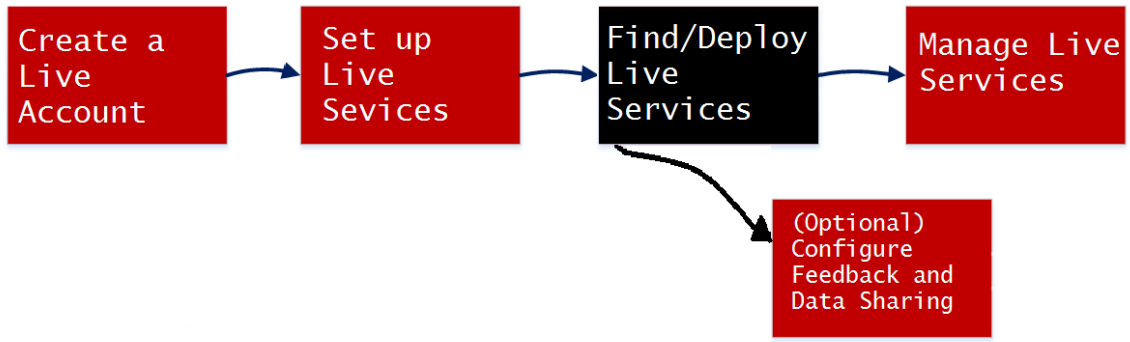



2. Configure el tiempo de la sincronización de NetWitness Suite con actualizaciones de Live.

Para obtener más detalles, consulte el tema “Configurar los ajustes de servicios de Live” de la *Guía de configuración del sistema*.

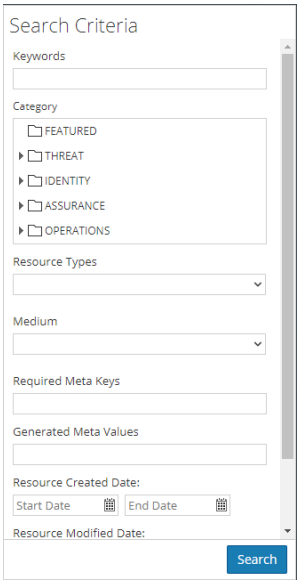
## Buscar e implementar recursos de Live

Los administradores pueden buscar recursos en la vista Buscar en Live, que es lo mismo que navegar por Live CMS para ver recursos con el panel Criterios de búsqueda de la Vista Buscar en Live.



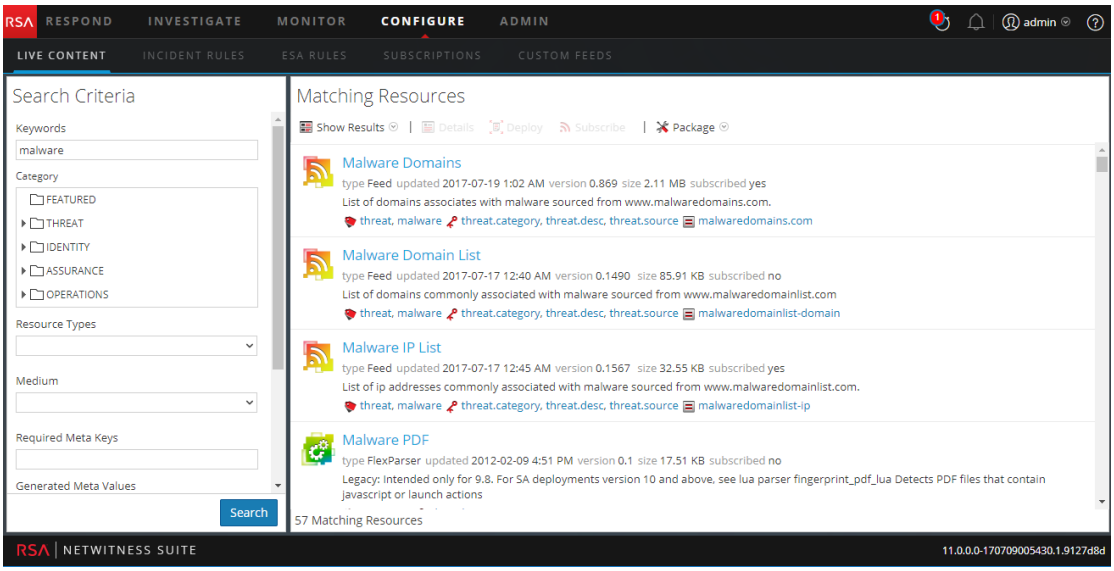

### Buscar recursos

1. En el panel **Criterios de búsqueda**, especifique los criterios de búsqueda. Ingrese una o todas las siguientes opciones: teclado, categoría, tipo de recurso, medio, claves de metadatos, valores de metadatos, fecha de creación de los recursos y fecha de modificación de los recursos.




2. Haga clic en **Buscar**.

   Los resultados en detalle se muestran en el panel Coincidencias de recursos.




3. (Opcional) Para restringir más los resultados en el panel Coincidencias de recursos, haga clic en una etiqueta, una clave de metadatos, un valor de metadatos de medio o recurso de un resultado.

## Implementar recursos en Live

En RSA NetWitness Suite, puede implementar manualmente los recursos seleccionados mediante el Asistente de implementación, o puede suscribirse a un grupo de recursos.

- Cuando tenga resultados de la navegación de recursos en NetWitness Suite Live, podrá implementar los recursos manualmente en un servicio o un grupo de servicios sin suscribirse a los recursos.
- La implementación manual de recursos se realiza en los servicios sin aprovechar las eficaces funcionalidades de administración de recursos de NetWitness Suite. Si desea recibir notificaciones y actualizaciones de los recursos actualizados y poder quitar fácilmente los recursos de un servicio, debe suscribirse a los recursos en la vista Buscar en Live e implementarlos en la Vista Configuración de Live.

Este es el procedimiento básico para la implementación manual:

1. Seleccione un recurso o un grupo de recursos, o un paquete de recursos creado previamente.
2. Haga clic en Implementar, lo cual inicia el Asistente de implementación.
3. Revise la lista de recursos seleccionados.
4. Seleccione los servicios o los grupos de servicios en los cuales desea implementar los recursos seleccionados

5. Revise las selecciones anteriores
6. Implementación

El siguiente procedimiento describe cómo implementar un grupo de recursos o un paquete de recursos:

- Puede seleccionar uno o más recursos en la Vista Recurso de Live e implementarlos en los servicios.
- O bien, si anteriormente creó y guardó un paquete de recursos, puede implementar el paquete en los servicios. Consulte Asistente Implementación de paquete de recursos para obtener instrucciones para crear un paquete.

### Para implementar recursos manualmente:

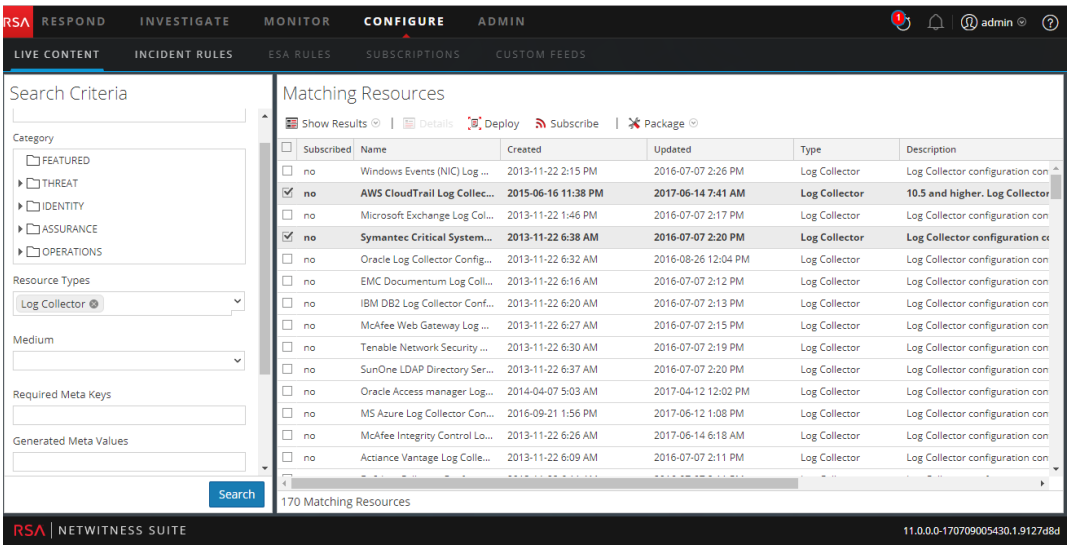
1. Vaya a **CONFIGURAR > Contenido de Live**.
2. Seleccione un grupo de recursos o un paquete de recursos creado previamente.

   Para seleccionar un recurso o un grupo de recursos:

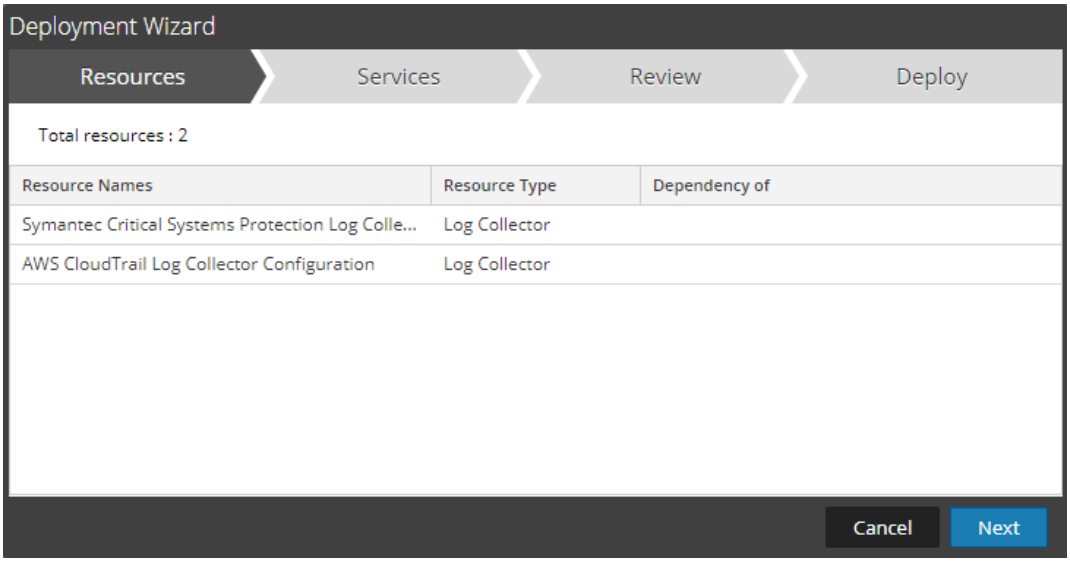
   a. En la **vista Buscar en Live,** navegue por el recurso de Live (por ejemplo, busque el tipo de recurso **Log Collector**).

   b. En el panel **Coincidencias de recursos**, seleccione **Mostrar resultados > Cuadrícula**.

   c. Seleccione la casilla de verificación de la izquierda o los recursos que desee implementar.



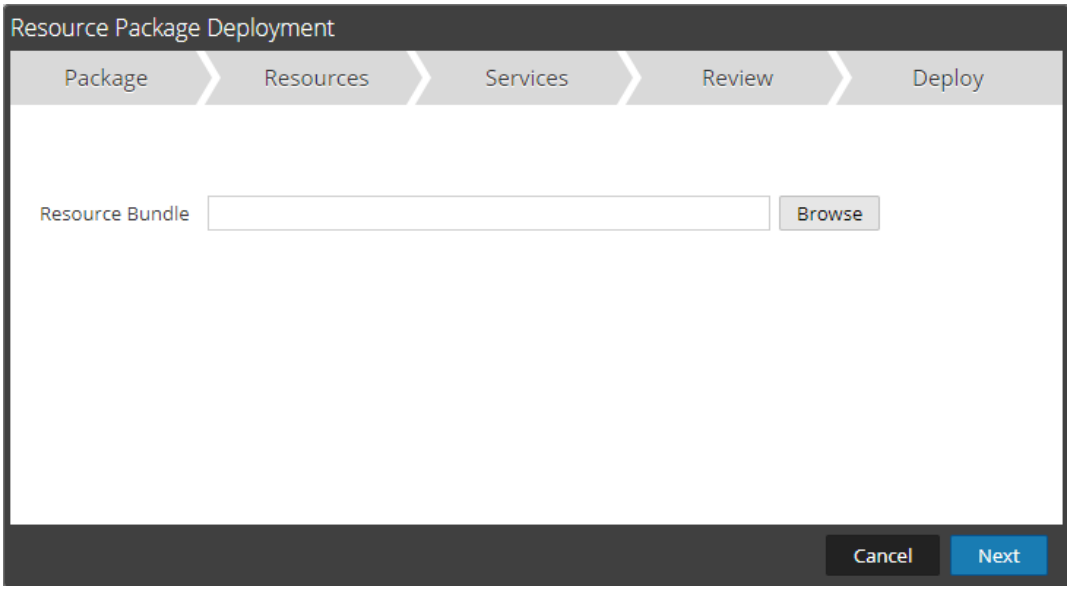
d. En la barra de herramientas Coincidencias de recursos, haga clic en Deploy.




3. Para seleccionar un paquete de recursos para implementar:

a. En la vista **Buscar en Live**, barra de herramientas **Coincidencias de recursos**, seleccione **Paquete** > **Implementar**:

Se muestra la página Paquete del asistente Implementación de paquete de recursos.




b. Haga clic en Navegar y seleccione un paquete de la red (por ejemplo **resourceBundle-FeedsParsersContent.zip**).

c. Haga clic en **Abrir**.

En este punto, si está implementando un paquete o un grupo de recursos, se abre el **Asistente de implementación** y se muestra la página **Recursos**.

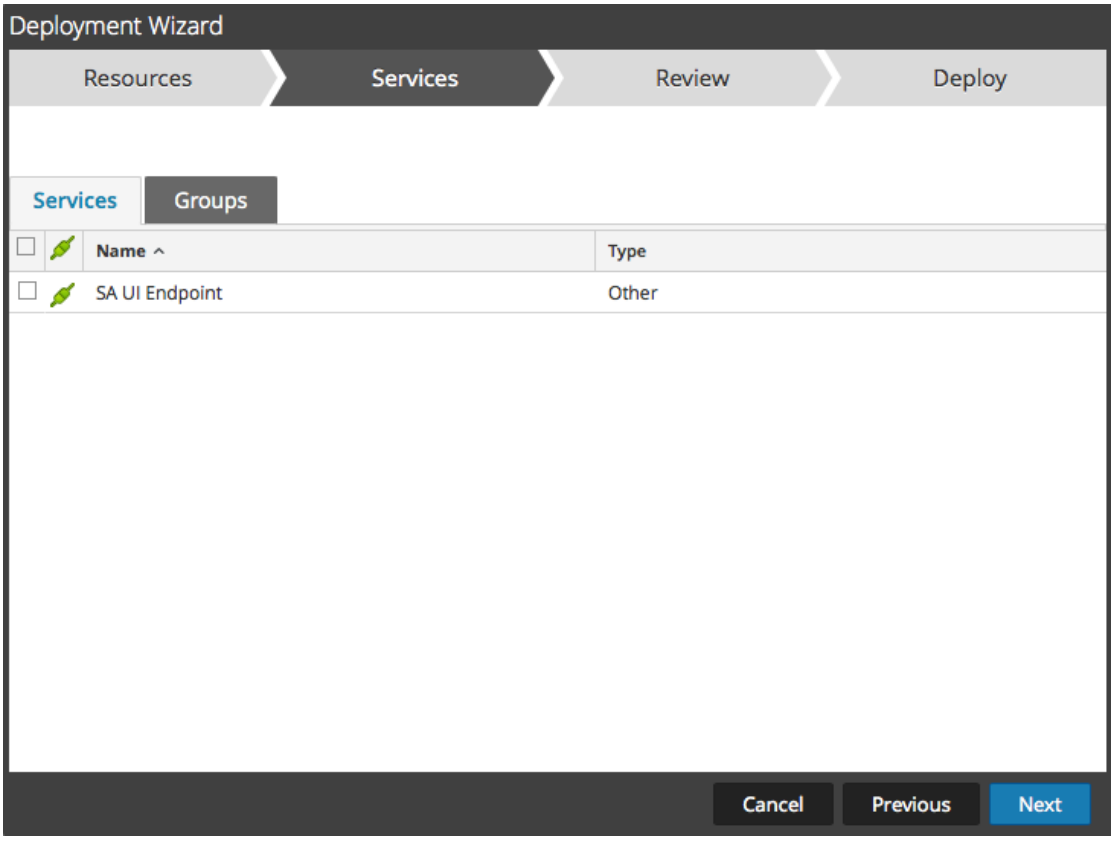
4. Haga clic en **Siguiente**.

   Se muestra la página **Servicios**, la cual tiene dos pestañas, **Servicios** y **Grupos**. Estas proporcionan una lista de servicios y grupos de servicios que se configuran en Administration > vista Servicios. Las columnas son un subconjunto de las columnas disponibles en la vista Servicios.

   **Nota:** El servidor de Live es "inteligente" acerca de cómo implementar recursos en servicios. Por ejemplo, no implementa recursos que tienen un medio de paquetes en ningún Log Decoder. Esto significa que solo los recursos de contenido aplicable se implementan en cada servicio.

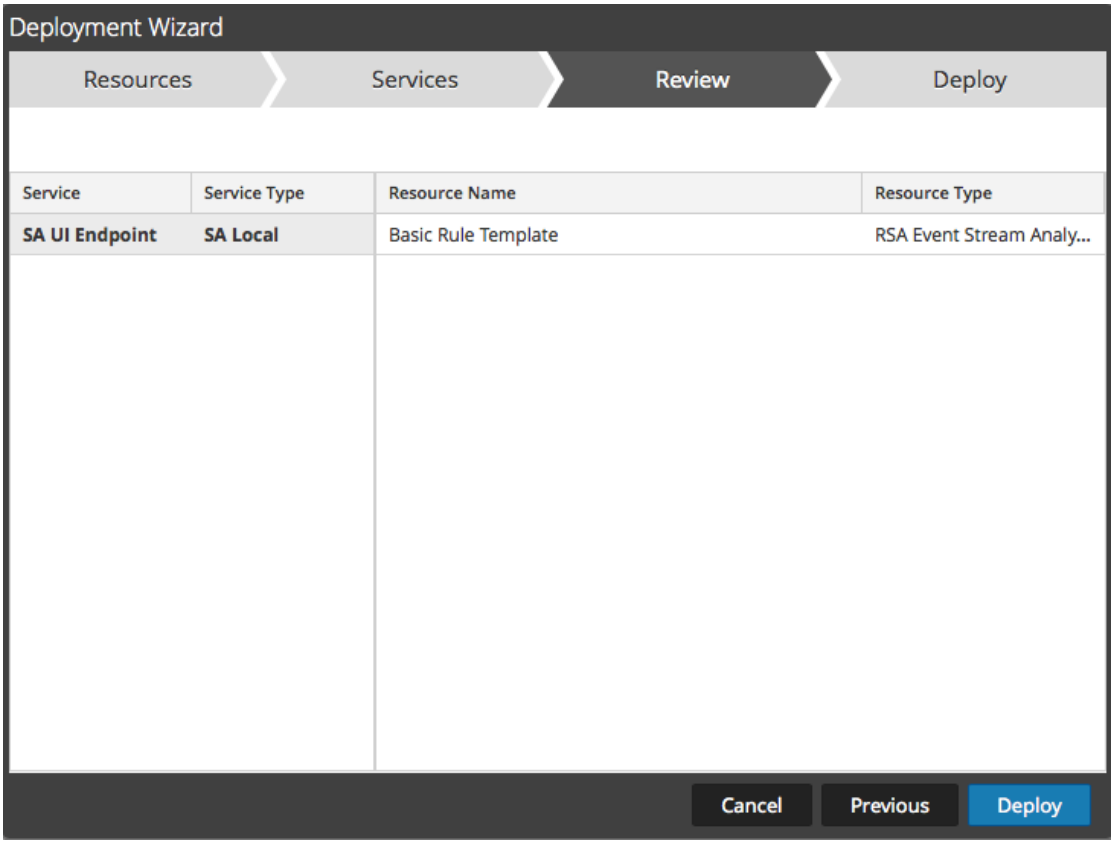
5. Seleccione los servicios en los cuales desea implementar el contenido. Puede seleccionar cualquier combinación de servicios y grupos de servicios.

   - Use la pestaña **Servicios** para seleccionar servicios individuales, la lista de servicios y grupos de servicios que se configuran en la vista Servicios de ADMIN.
   - Use la pestaña **Grupos** para seleccionar grupos de servicios




6. Haga clic en **Siguiente**.

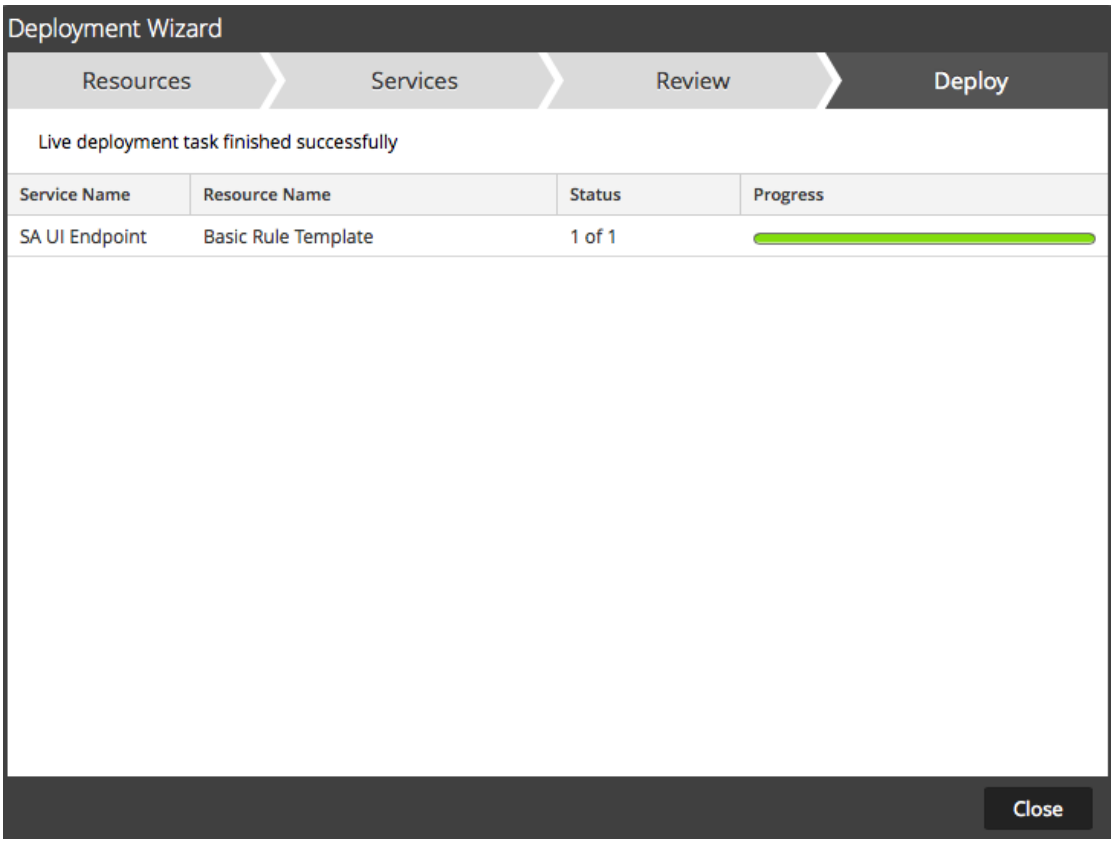
Se muestra la página **Revisión**.



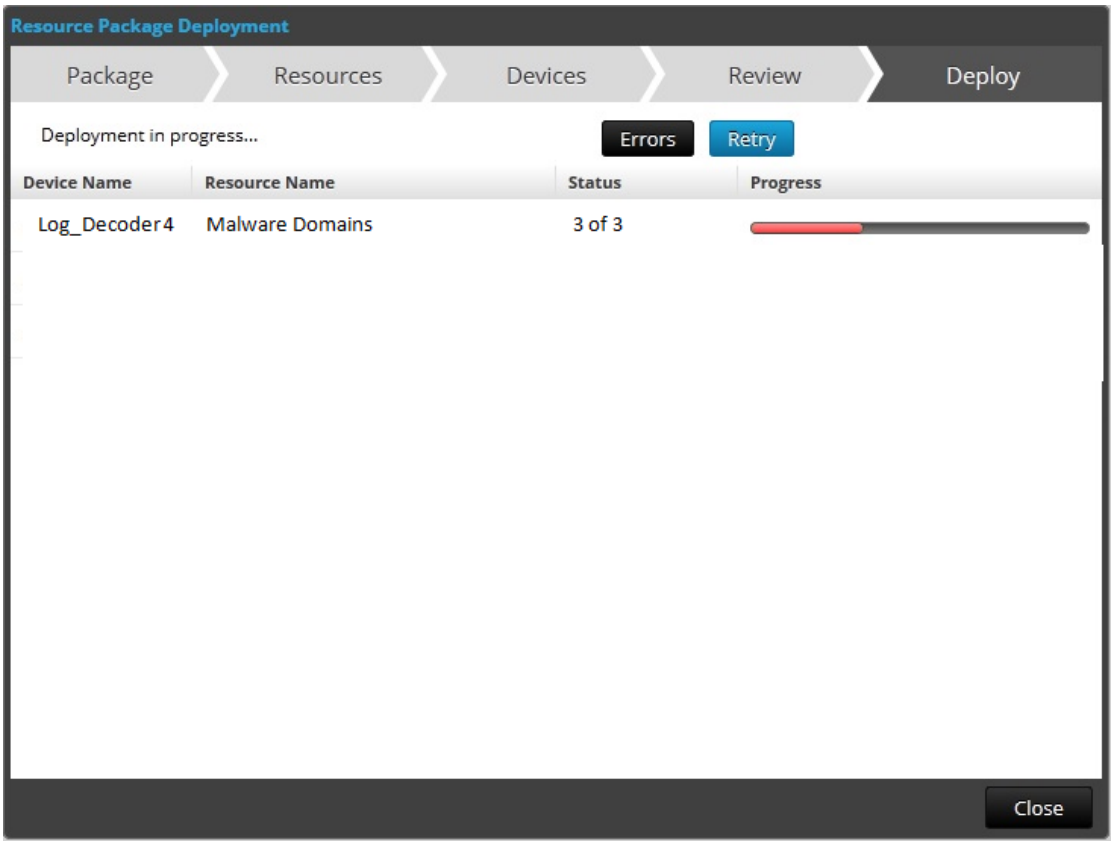

Asegúrese de haber seleccionado los recursos correctos y los servicios en los cuales desea implementarlos.

7. Haga clic en **Implementar**.

   Se muestra la página **Implementar**. La barra de progreso se vuelve verde cuando los recursos se implementan correctamente en los servicios seleccionados.




Si intenta implementar recursos y servicios que no son compatibles, NetWitness Suite muestra los botones Errores y Reintentar en los cuales puede hacer clic para revisar los errores y volver a intentar la implementación.



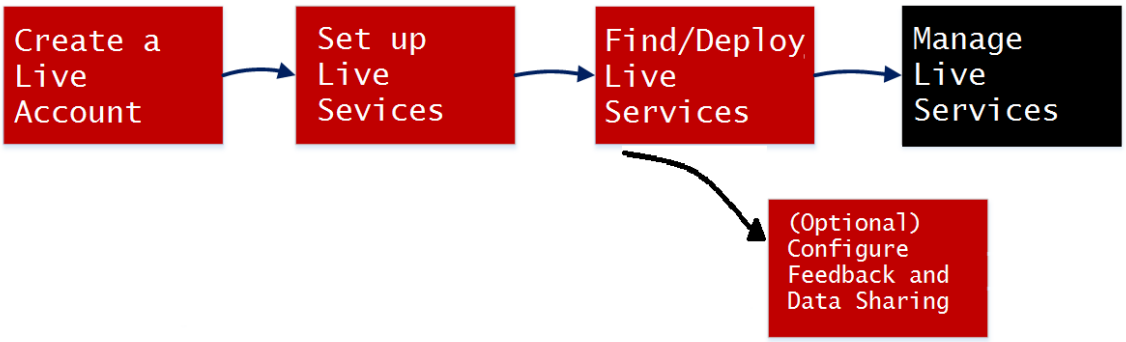

8. Haga clic en **Cerrar**.

## Próximos pasos

Después de la implementación de analizadores en Decoders y Log Decoders, debe habilitar analizadores en cada servicio como se describe en la *Guía de configuración de Decoder y Log Decoder*.

# Administrar de recursos de Live

Estos procedimientos son necesarios cuando los administradores desean buscar, suscribirse y/o implementar recursos de Live. Con una conexión al servidor de CMS, puede buscar, suscribirse e implementar recursos de Live de acuerdo con su nivel de suscripción. Cuando encuentra los recursos, los implementa en servicios y grupos de servicios configurados en la vista Servicios de Administration.




## Procedimientos

Hay varios flujos de trabajo posibles para implementar recursos en servicios y administrar esas implementaciones. Entre ellas, se incluyen las siguientes:

- Suscribirse e implementar recursos.
- Implementar un paquete de recursos.
- Eliminar implementaciones de recursos.
- Descargar recursos.
- Configurar feeds de datos.

### Administrar la suscripción y la implementación

El flujo de trabajo de suscripción e implementación aprovecha las herramientas de administración de recursos disponibles en Live. Cuando se suscribe a recursos, acepta recibir recursos actualizados según la sincronización configurada en **ADMIN > panel Configuración de Live**.

Al agregar recursos suscritos a la lista de implementaciones, configure NetWitness Suite para migrar automáticamente esos recursos a los servicios seleccionados en los intervalos de sincronización configurados. Este método requiere planificación de los servicios y grupos de servicios donde se implementan los recursos. Además:

- Puede eliminar un recurso de la lista de implementaciones en la pestaña Pestaña Implementaciones.
- Puede cancelar la suscripción a un recurso en la pestaña Pestaña Suscripciones y la vista Vista Recurso de Live.

### Para administrar suscripciones e implementaciones:

1. En **ADMIN > SISTEMA > panel Live** , especifique un intervalo en el cual NetWitness Suite compruebe las actualizaciones de los recursos suscritos en Live y especifique las direcciones de correo electrónico de las personas que recibirán un correo electrónico con la lista de los recursos suscritos que se han actualizado.
2. En la vista **Live** > **Buscar**, busque y suscríbase a los recursos de Live.
3. En la vista **Live** > **Configurar** > pestaña **Implementaciones** , seleccione los recursos suscritos y agréguelos a la lista de implementaciones de los grupos de servicios.
4. (Opcional) En el panel **ADMIN**> **SISTEMA**> **panel Live** , haga clic en 

para implementar inmediatamente los recursos que aparecen en la pestaña Implementaciones.
5. En la vista **Live** > **Configurar** > pestaña **Implementaciones** , seleccione los recursos implementados y elimínelos de los grupos de servicios.
6. En la vista **Live** > **Configurar** > pestaña **Suscripciones** , cancele las suscripciones a los recursos.

#### Quitar un recurso implementado

Una vez que se han implementado en un servicio, los recursos de Live permanecen en el servicio hasta que se eliminan. Es una buena práctica eliminar los recursos sin uso de los servicio en los cuales se implementaron.

Para quitar recursos, vaya a la Vista Recurso de Live, cancele la suscripción a un recurso y quítelo de los servicios donde se implementó.

#### Implementar un paquete de recursos

Para implementar un paquete de contenido, use el Asistente Implementación de paquete de recursos. Puede implementar un paquete de contenido creado en Live en uno o más servicios. NetWitness Suite acepta paquetes en archivos **.nwp** o **.zip**.

#### Descargar recursos

En la vista Recurso de Live, puede descargar recursos de Live a su sistema de archivos local con el botón **Descargar**.

### Configurar feeds de datos

En la vista **Live** > **Feeds** , puede configurar y mantener feeds personalizados y de identificación.

# Procedimientos adicionales

En este tema se explican los procedimientos adicionales que debería seguir un administrador y que no son esenciales para la configuración o el uso de los servicios de Live.

- Exportar datos a RSA
- Administrar feeds personalizados
  - Crear un feed personalizado
  - Crear un feed personalizado de STIX
  - Crear y administrar un feed de identidad
  - Editar un feed
  - Quitar un feed
- Procedimientos varios de los servicios de Live

# Exportar datos a RSA

Un administrador de NetWitness Suite puede exportar las métricas en NetWitness Suite para Live Feedback.

## Acerca de Live Feedback

Si no está configurada la cuenta de Live, puede cargar manualmente los datos de uso en RSA. Para obtener más información, consulte el tema "Panel Configuración de servicios de Live" de la *Guía de configuración del sistema*.

En el panel Configuración de servicios de Live hay 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

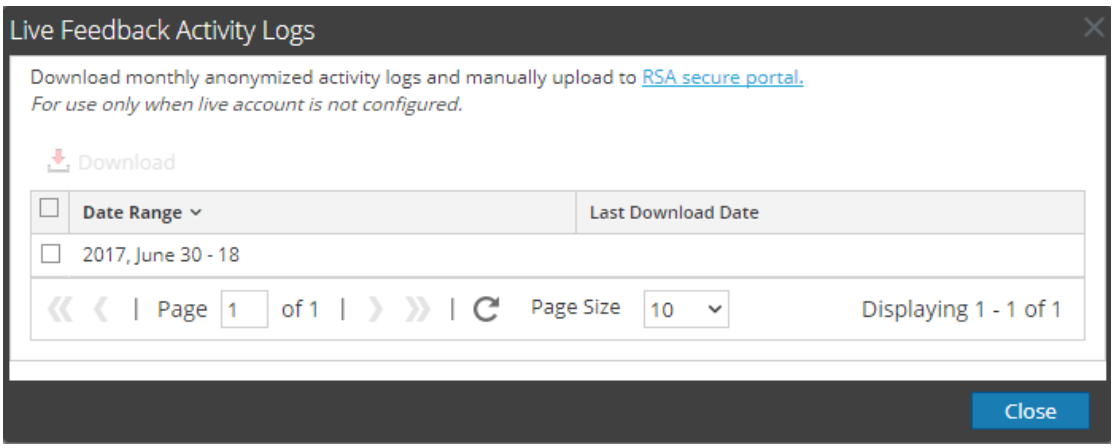
## Descargar datos históricos de Live Feedback

### 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 descargar 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" de la *Guía de configuración del sistema*.

## Compartir datos en RSA

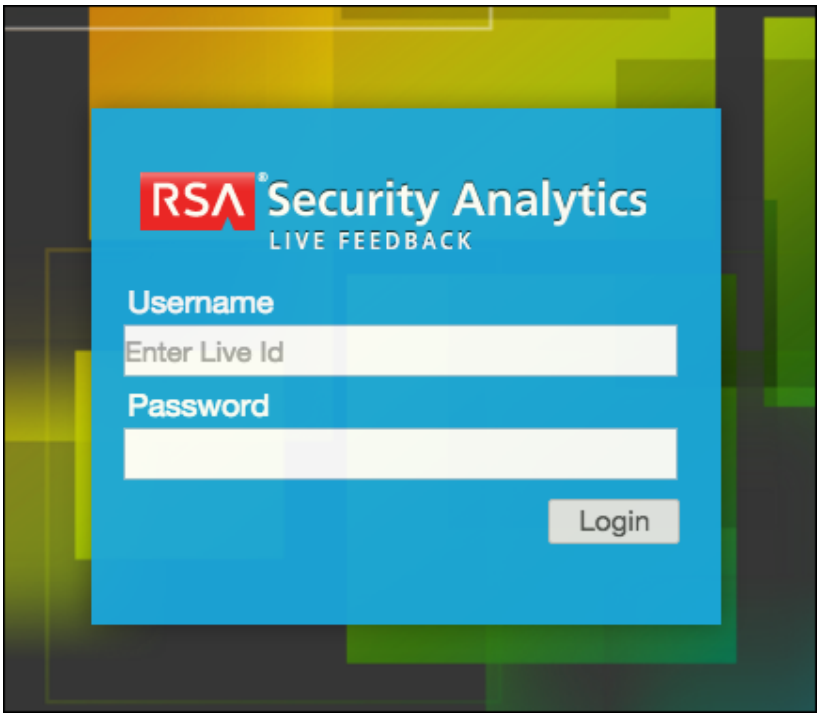
Después de descargar los datos de Live Feedback, puede cargarlos mediante el siguiente procedimiento.

### Para compartir los datos en RSA:

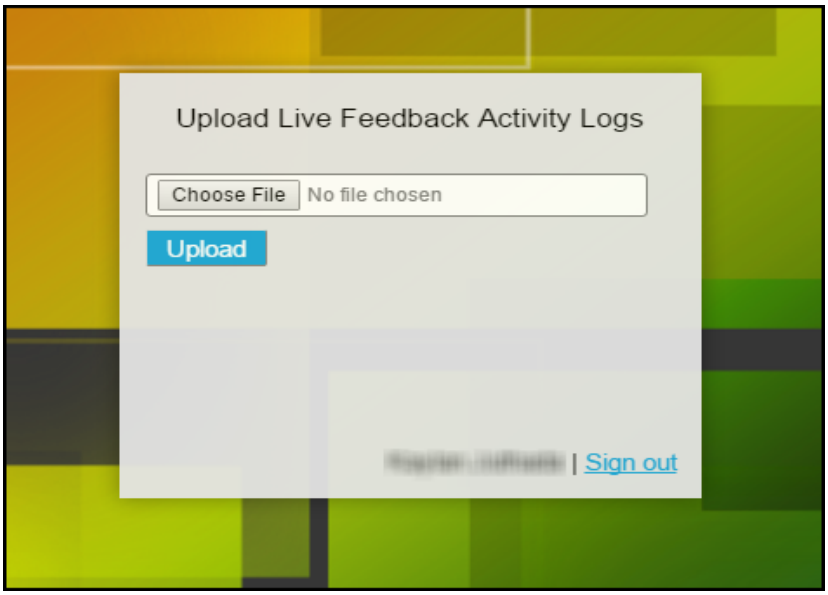
1. Haga clic en el **Portal seguro de RSA** disponible en la ventana **Registros de actividad de Live Feedback**.

   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 Live ID.




3. Haga clic en **Descargar registro de actividades de Live Feedback**.




4. Haga clic en **Cargar**.

# Administrar feeds personalizados

En este tema se presenta la funcionalidad de feeds personalizados, la cual se implementa mediante el Asistente de feed personalizado en RSA NetWitness Suite con el fin de completar rápidamente los Decoders con feeds personalizados y de identidad.

## Creación de feeds personalizados

Se usa **Live** > **Feeds** > **Configurar feed** > **Asistente para configurar un feed personalizado** para crear e implementar rápidamente feeds de Decoder basados en lógica determinista que ofrece las claves de metadatos específicas para los Decoders y los Log Decoders seleccionados. A pesar de que el asistente lo guiará por el proceso para crear feeds según demanda y recurrentes, debe comprender la forma y el contenido de un archivo de feed cuando crea un feed.

Los nombres de archivo de feed en RSA NetWitness Suite tienen el formato `<filename>.feed`. Para crear un feed, NetWitness Suite requiere un archivo de **datos** de feed en el formato `.csv` o `.xml` (para STIX) y un archivo de **definición** de feed en el formato `.xml`, el cual describe la estructura de un archivo de feed de datos. El asistente Configurar un feed personalizado puede crear un archivo de definición de feed basado en un archivo de datos de feed o en un archivo de datos de feed y en el archivo de definición de feed correspondiente.

Los archivos que se utilizan para crear un feed según demanda deben estar almacenados en el sistema de archivos local. Los archivos que se utilizan para crear un feed recurrente deben estar almacenados en una URL accesible, en la cual NetWitness Suite pueda buscar la versión actual del archivo para cada recurrencia. Después de la creación de un feed de NetWitness Suite, puede descargar el feed al sistema de archivos local, editar los archivos de feed y, a continuación, editar el feed de NetWitness Suite para usar los archivos de feed actualizados.

## Archivo de definición de feed de muestra

Este es un ejemplo de un archivo de definición de feed denominado `dynamic_dns.xml`, que NetWitness Suite crea en función de las entradas de los asistentes de feed. Define la estructura del archivo de datos del feed denominado `dynamic_dns.csv`.

**Nota:** La ruta de archivo de feed debe ser `.csv` independientemente del tipo de feed (valor predeterminado o STIX).

```
<?xml version="1.0" encoding="utf-8"?>
 <FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">

   <FlatFileFeed name="Dynamic DNS Domain Feed"
   path="dynamic_dns.csv"
   separator=","
   comment="#"
   version="1">

   <MetaCallback
   name="alias.host"
   valuetype="Text"
   apptype="0"
   truncdomain="true"/>

   <LanguageKeys>
            <LanguageKey name="threat.source" valuetype="Text" />
            <LanguageKey name="threat.category" valuetype="Text" />
            <LanguageKey name="threat.desc" valuetype="Text" />
   </LanguageKeys>

   <Fields>
   <Field index="1" type="index" key="alias.host" />
   <Field index="4" type="value" key="threat.desc" />
   <Field index="2" type="value" key="threat.source" />
   <Field index="3" type="value" key="threat.category" />
   </Fields>
   </FlatFileFeed>

 </FDF>
```

## Equivalentes de definición de feed para los parámetros del asistente Feed personalizado

El asistente de feeds de NetWitness Suite proporciona opciones para definir la estructura del archivo de feed de datos. Esto se corresponde directamente con los atributos en el archivo (.xml) de definición del feed.

| Parámetro de NetWitness Suite | Equivalente en el archivo de definición del feed |
|---|---|
| Pestaña **Definir feed** | |

| Parámetro de NetWitness Suite | Equivalente en el archivo de definición del feed |
|---|---|
| **Tipo de feed** | Seleccione: **Valor predeterminado**: para definir un feed basado en un archivo de datos de feed con formato `.csv` . **STIX**: para definir un feed basado en un `.xml` con formato STIX. |
| **Tipo de tarea de feed** | Seleccione: **Ad hoc**: para crear un feed según demanda. **Recurrente**: para crear un feed que se repite automáticamente. |
| **Nombre** | El nombre del feed personalizado en el archivo de datos del feed. Corresponde al atributo **`flatfeedfile name`** en el archivo de definición del feed; por ejemplo, Feed de prueba de DNS dinámico. |
| **Archivo/ Navegar** | Este es el nombre del archivo de datos del feed. Corresponde al atributo **`flatfeedfile path`** en el archivo de definición del feed; por ejemplo, dynamic_dns.csv. |
| (STIX, recurrente) **Confiar en todos los certificados** | Si no desea validar el certificado del servidor REST, seleccione **Confiar en todos los certificados**. Esta opción está habilitada de manera predeterminada (seleccionada). |
| (STIX, recurrente) **Certificado/navegar** | Para la autenticación de cliente con la URL de REST, en el campo **Certificado**, haga clic en **Navegar** y seleccione el certificado autofirmado. Los formatos de certificados compatibles son .cer, .crt con archivos con codificación Base64 y DER. |
| | Pestaña **Definir feed**: Opciones avanzadas |
| **Archivo de feed XML** | El nombre del archivo de definición del feed, por ejemplo, `dynamic_dns.xml`. |
| **Separador** | El carácter separador que se utiliza para separar atributos en el archivo de datos del feed. Corresponde al atributo **`flatfeedfile separator`** en el archivo de definición del feed; por ejemplo, una coma. |

| Parámetro de NetWitness Suite | Equivalente en el archivo de definición del feed |
|---|---|
| **Comentario** | El carácter que se utiliza para identificar un comentario en el archivo de datos del feed. Corresponde al atributo `flatfeedfile comment` en el archivo de definición del feed; por ejemplo, #. |
| **Quitar datos de STIX más antiguos que** | La cantidad de días durante los cuales se deben almacenar los paquetes STIX que se descargan del servidor TAXII. Los paquetes STIX más antiguos que la cantidad especificada de días se eliminan automáticamente. El valor predeterminado es 180 días, que es el valor máximo. |
| **Pestaña Seleccionar servicios** | Seleccione los servicios a los cuales desea enviar el feed de datos. |
| (Pestaña Definir columnas, Definir índice) **Tipo** | El tipo de valor de búsqueda en la posición del índice del archivo de datos de feed.<br>**IP** significa que cada fila del archivo de datos del feed contiene una dirección IP en la posición del valor de búsqueda. El valor de la dirección IP está en formato de punto decimal (por ejemplo, 10.5.187.42).<br>**Rango de IP** significa que cada columna del archivo de datos de feed contiene un rango de direcciones IP en la posición del valor de búsqueda. El rango de direcciones IP está en formato CIDR (for example, 192.168.2.0/24). **No IP** significa que cada fila del archivo de datos de feed contiene un valor de metadatos distinto a una dirección IP en la posición del valor de búsqueda. Los campos Tipo de servicio, Truncar dominio y Claves de callback se activan en los índices No IP. |
| (Pestaña Definir columnas, Definir índice) **CIDR** | Especifica que el valor de la dirección IP en la posición de búsqueda está en formato CIDR. El atributo **CIDR** define el formato de dirección IP del campo en notación Classless Inter-Domain Routing (CIDR). |

| Parámetro de NetWitness Suite | Equivalente en el archivo de definición del feed |
|---|---|
| (Pestaña Definir columnas, Definir índice)<br>**Tipo de servicio** | Para un índice No IP, el tipo de servicio entero para filtrar las búsquedas de metadatos. Corresponde al atributo **MetaCallback apptype** en el archivo de definición del feed. Un valor de **0** indica que no hay filtrado por tipo de servicio. |
| (Pestaña Definir columnas, Definir índice)<br>**Truncar dominio** | Para un índice No IP, en los valores de metadatos que contienen nombres de dominio (por ejemplo, nombres de host), el sistema puede quitar el elemento específico de host en los datos. Truncar dominio se corresponde con el atributo **MetaCallback truncdomain**. Si el valor es www.example.com, se trunca a example.com. Con un valor **Falso** se selecciona sin truncamiento y con un valor **Verdadero**, truncamiento. |
| (Pestaña Definir columnas, Definir índice)<br>**Claves de devolución de llamadas** | En un índice No IP, se pueden seleccionar en la lista desplegable las claves de metadatos disponibles para coincidencia en lugar de ip.src/ip.dst (los valores predeterminados para un tipo de índice IP). La clave de callback corresponde al atributo **MetaCallback name** y la columna de índice del archivo csv debe contener datos que puedan coincidir con la clave de metadatos seleccionada. Por ejemplo, si elige la clave de metadatos de nombre de usuario, la columna de índice del archivo csv debe completarse con los usuarios que se deban hacer coincidir. |

| Parámetro de NetWitness Suite | Equivalente en el archivo de definición del feed |
|---|---|
| (Pestaña Definir columnas, Definir índice) **Columna de índice** | Identifica la columna en el archivo de datos de feed que proporciona el valor de búsqueda para la fila. Cada posición en cada fila del archivo de datos de feed se identifica con un atributo **Field index** en el archivo de definición de feed. Un campo con un índice de **1** es la primera entrada en una fila, el segundo campo tiene un índice de **2**, el tercer campo tiene un índice de **3** y así sucesivamente. Puede seleccionar varias columnas de índice, si el **tipo de Feed** es **STIX** y el **tipo de índice** es **no IP**. Cuando selecciona varias columnas de índice se combinan los valores de todas las columnas seleccionadas en la primera columna de índice que seleccionó. |
| (DEFINIR VALORES) **Clave** | El nombre de **LanguageKey**, según se define en el archivo de definición del feed, para el cual se crean los metadatos a partir de esta fila del archivo de datos del feed. Se corresponde con el atributo **Field key** en el archivo de definición del feed. Una clave se aplica solamente a un campo cuyo tipo está definido en **valor**. En el archivo de definición del feed, hay una lista de LanguageKeys desde **index.xml** o un nombre del resumen si se utiliza el nombre de origen y el nombre de destino. Por ejemplo, **reputation** es un nombre de resumen para **reputation.src** y **reputation.dst**). El atributo Field key hace referencia a este valor. |

### Próximos pasos

- Crear un feed personalizado
- Crear y administrar un feed de identidad
- Editar un feed
- Quitar un feed

## Crear un feed personalizado

En este tema se proporcionan instrucciones para crear un feed personalizado mediante un archivo .csv o un archivo de datos de feed con formato STIX en RSA NetWitness Suite.

**Nota:** A partir de 10.6.1 o superior, NetWitness Suite es compatible con Structured Threat Information Expression (STIX). Para obtener más información acerca de STIX y la creación de un feed personalizado de STIX, consulte Crear un feed personalizado de STIX.

Puede crear fácilmente un feed personalizado mediante el asistente de feed personalizado. Para realizar este procedimiento, necesita un archivo de datos de feed en formato `.csv` o `.xml`. Si también tiene un archivo de definición de feed relacionado en formato `.xml`, que describe la estructura del archivo de datos del feed, puede usarlo para crear un feed. Con el asistente Feed personalizado, se pueden crear feeds basados en un archivo de datos de feed o basados en un archivo de datos de feed y el archivo de definición de feed correspondiente.

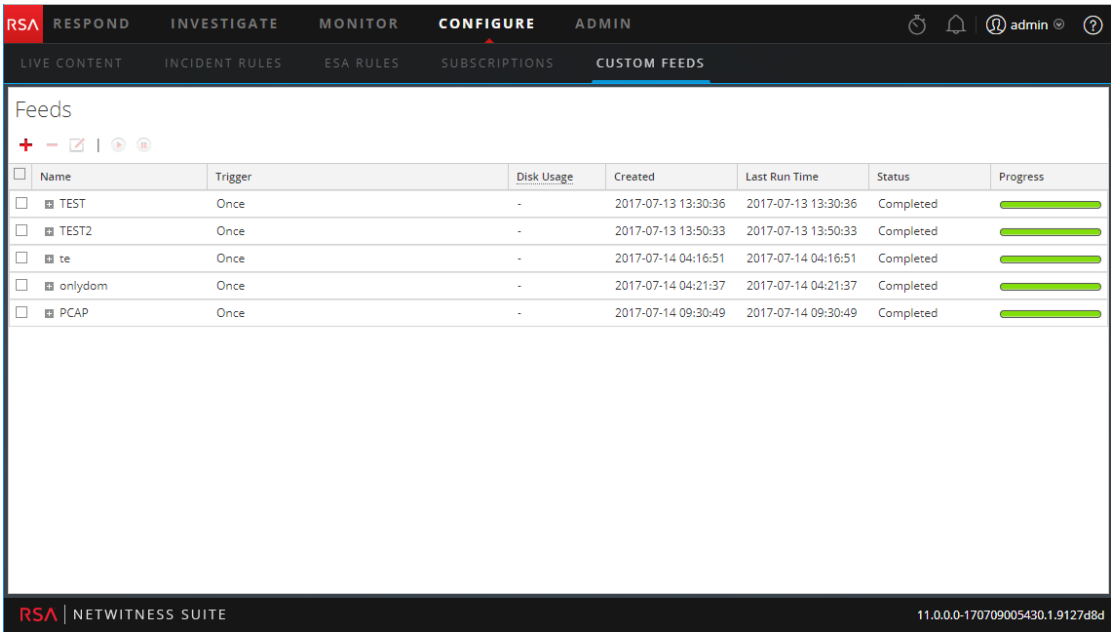
Después de realizar este procedimiento, habrá creado un feed personalizado.

El archivo de datos de feed (`.csv` o STIX (`.xml`)) y, de manera opcional, el archivo de definición de feed (`.xml`) deben estar disponibles en el sistema de archivos local para un feed personalizado según demanda. Para crear un feed personalizado recurrente, los archivos deben estar disponibles en una URL a la que se pueda acceder desde el servidor de NetWitness Suite.

### Para crear un feed personalizado:

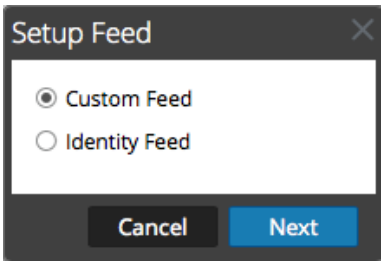
1. Vaya a **CONFIGURAR > FEEDS PERSONALIZADOS**.

   Se muestra la vista Feeds personalizados.



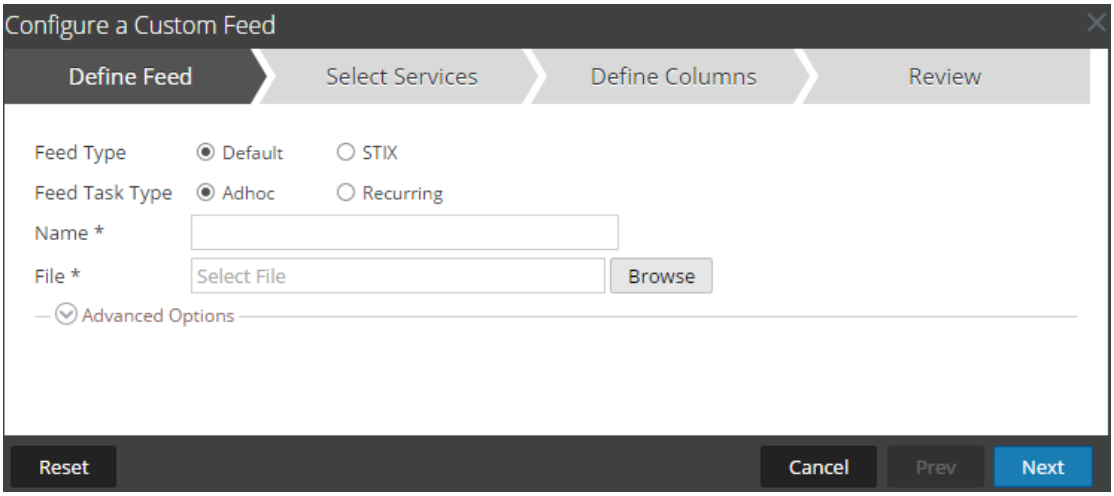

2. En la barra de herramientas, haga clic en +.

   Se muestra el cuadro de diálogo Configurar feed.




3. Para seleccionar el tipo de feed, haga clic en **Feed personalizado** y luego en **Siguiente**.

   El asistente Configurar un feed personalizado se muestra con el formulario Definir feed abierto.

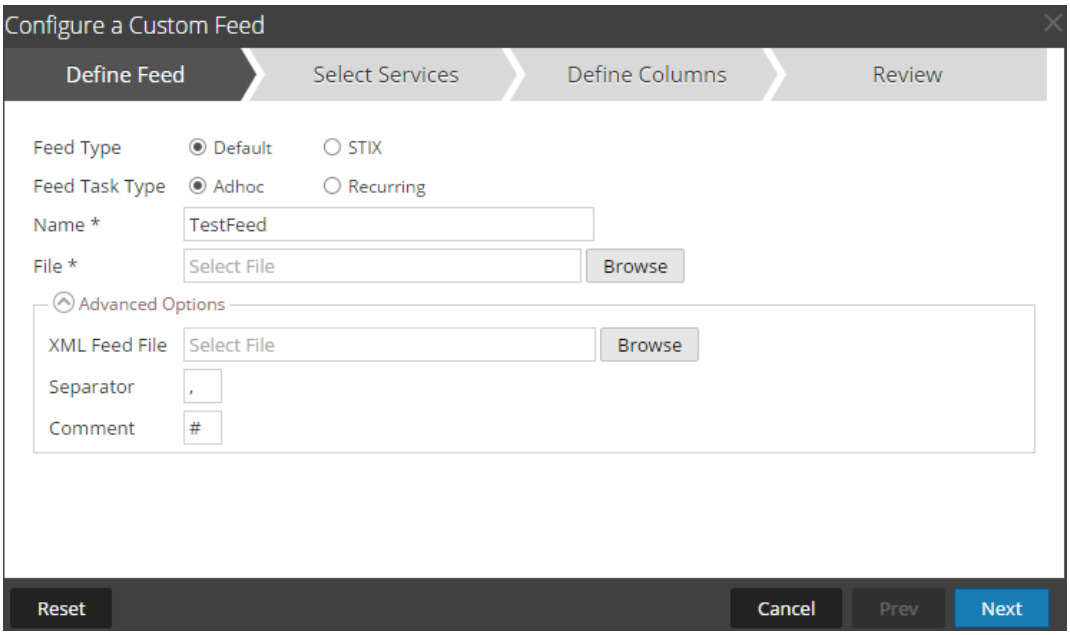



4. Para definir un feed basado en un archivo de datos de feed con formato `.csv`, seleccione **Valor predeterminado** en el campo **Tipo de feed**.
5. Para definir una tarea de feed según demanda que se ejecute una sola vez, seleccione **Ad hoc** en el campo **Tipo de tarea de feed** y realice una de las siguientes acciones:

   a. (Condicional) Para definir un feed basado en un archivo de datos de feed con formato .csv, escriba el **Nombre** del feed, seleccione un **archivo** de contenido .csv en el sistema de archivos local y haga clic en **Siguiente**.

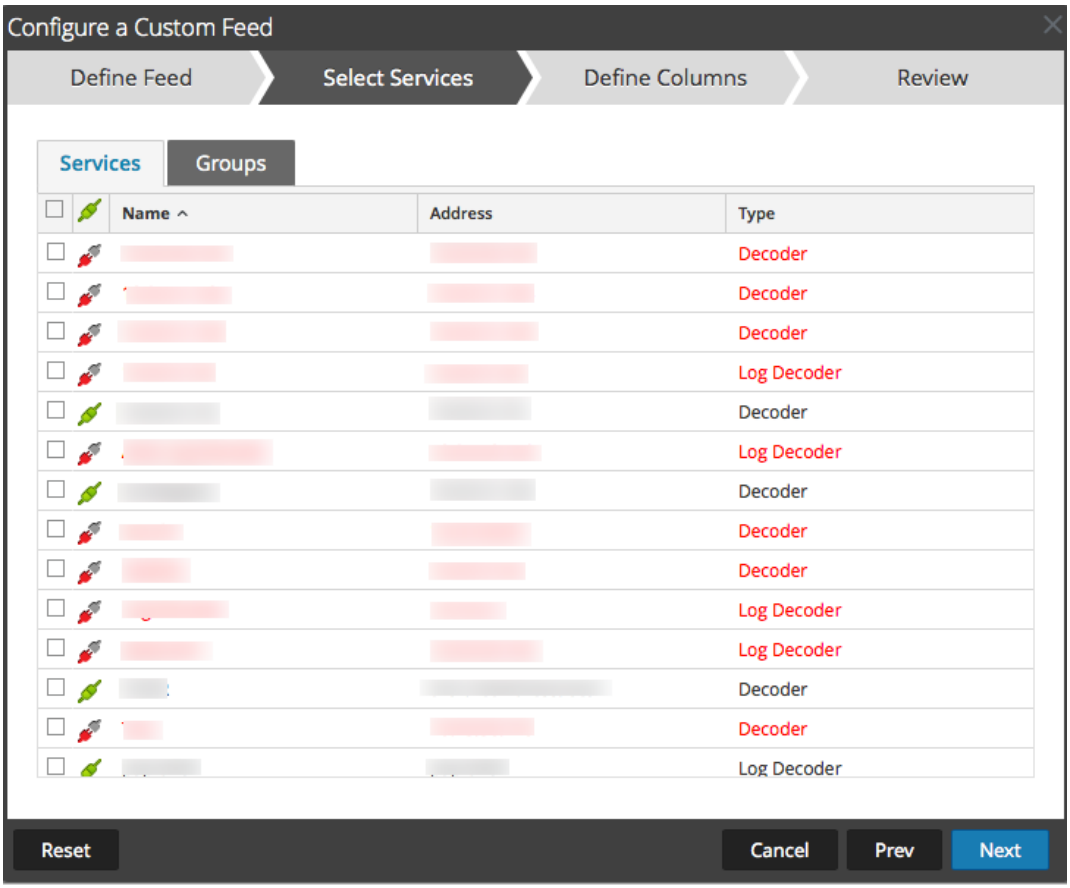
   b. (Condicional) Para definir un feed basado en un archivo de feed XML, seleccione **Opciones avanzadas**.

      Se muestran las opciones avanzadas:




c. Seleccione un archivo de feed XML en el sistema de archivos local, elija el **Separador** (el valor predeterminado es coma), especifique los caracteres de **Comentario** que se utilizarán en el archivo de datos del feed (el valor predeterminado es #) y haga clic en **Siguiente**.

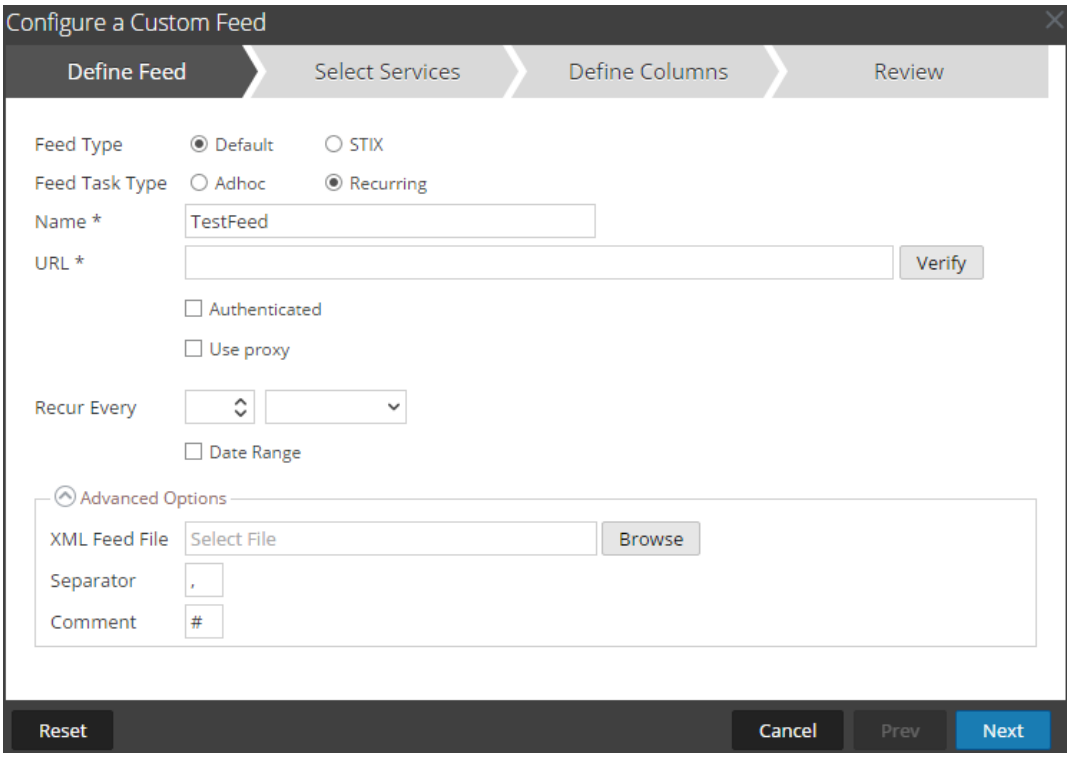
d. Se muestra el formulario Seleccionar servicios. Este es un ejemplo del formulario de un feed basado en un archivo de datos de feed sin archivo de definición de feed. Si define un feed basado en un archivo de definición de feed, la pestaña Definir columnas no es necesaria.




6. Para definir una tarea de feed recurrente que se ejecute de manera repetida a intervalos especificados durante un rango de fechas especificado:

   a. Seleccione **Recurrente** en el campo **Tipo de tarea de feed**.

      En el formulario Definir feed se incluyen los campos de un feed recurrente.




b. En el campo **URL**, escriba la dirección URL en la cual está ubicado el archivo de datos del feed, por ejemplo, `http://<hostname>/<feeddatafile>.csv`, y haga clic en **Verificar**.

   NetWitness Suite verifica la ubicación en la cual está almacenado el archivo con el fin de que NetWitness Suite pueda comprobar el archivo más reciente automáticamente antes de cada recurrencia.

c. (Opcional) Si la URL tiene acceso restringido y se solicita autenticación con nombre de usuario y contraseña, seleccione **Autenticada**.

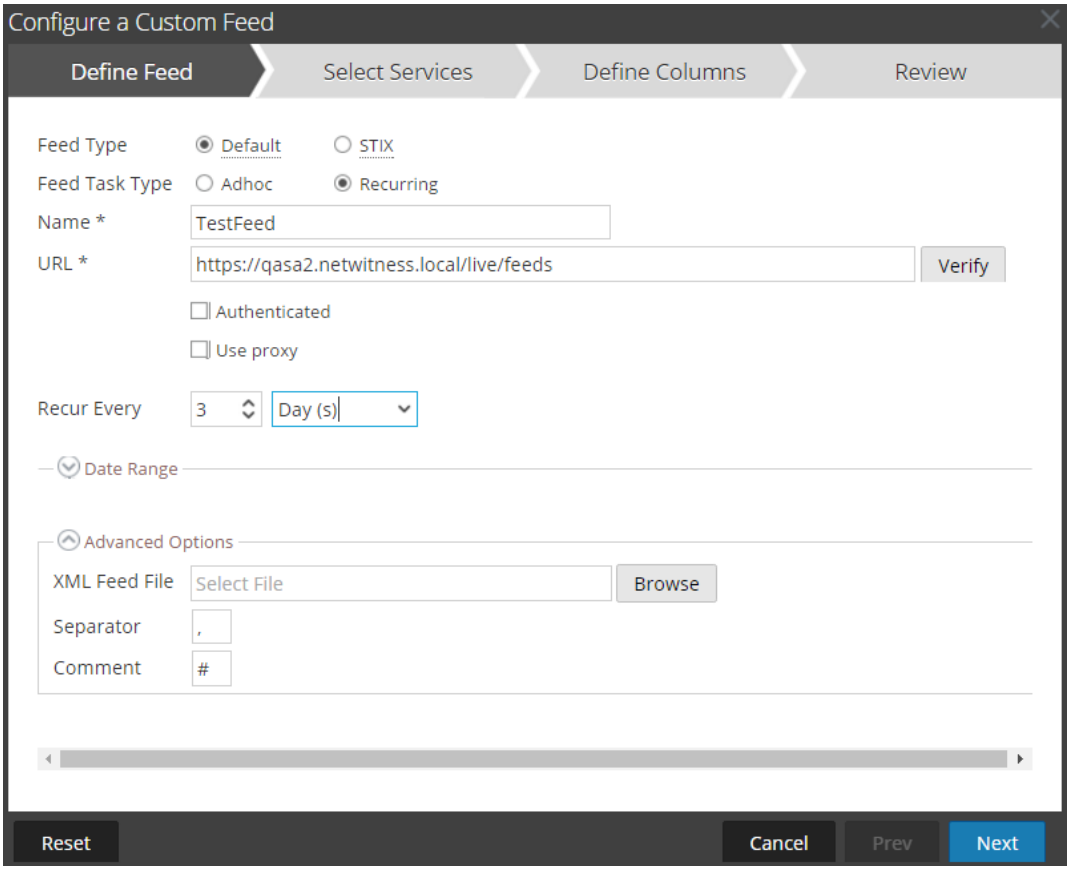
   NetWitness Suite proporciona su nombre de usuario y contraseña para autenticación en la dirección URL.

d. Si desea que el servidor de NetWitness Suite acceda a la dirección URL del feed a través de un proxy, seleccione **Usar proxy**. Para obtener más información sobre la configuración de un proxy, consulte el tema **Configurar el proxy de NetWitness Suite** en la *Guía de configuración del sistema*. De forma predeterminada, la casilla de verificación **Usar proxy** no está seleccionada.

e. Para definir el intervalo de recurrencia, puede realizar alguna de las siguientes acciones:

   - Especifique la cantidad de minutos, horas o días entre cada recurrencia del feed.
   - Especifique la recurrencia cada semana y seleccione los días de la semana.

f. Para definir el rango de fechas para la ejecución recurrente del feed, especifique la hora y la **Fecha de inicio** y la hora y la**Fecha de finalización**.



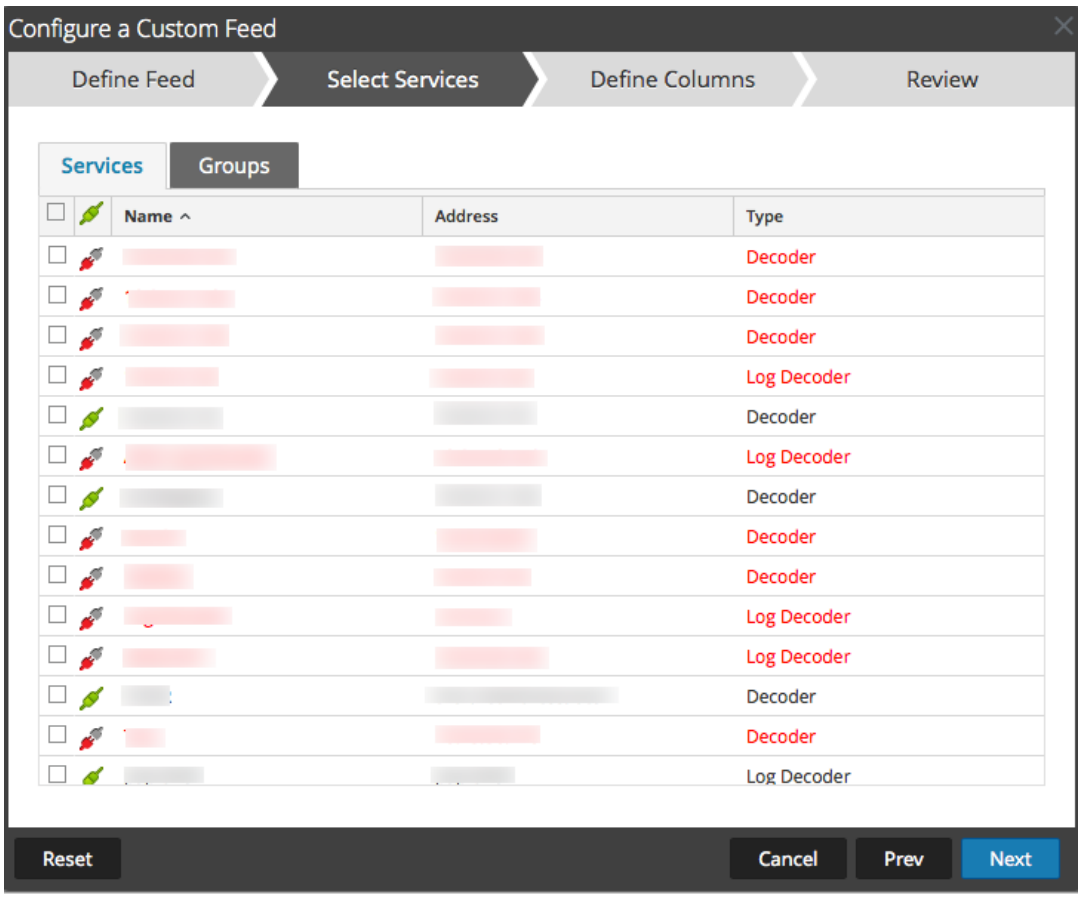

7. (Condicional) Si desea definir un feed basado en un archivo de feed XML:

   - Escriba el **Nombre** del feed y seleccione **Opciones avanzadas**.

     Se muestran los campos Opciones avanzadas.

   - Seleccione un archivo de feed XML del sistema de archivos local, elija el **Separador** (la opción predeterminada es coma), especifique los caracteres de **Comentario** que se utilizarán en el archivo de datos del feed (la opción predeterminada es #) y haga clic en **Siguiente**.

Se muestra el formulario Seleccionar servicios.




8. Para identificar los servicios en los cuales se implementará el feed, realice una de las siguientes acciones:

   a. Seleccione uno o más Decoders y Log Decoders y haga clic en **Siguiente**.

   b. Haga clic en la pestaña **Grupos** y seleccione un grupo. Haga clic en **Siguiente**.

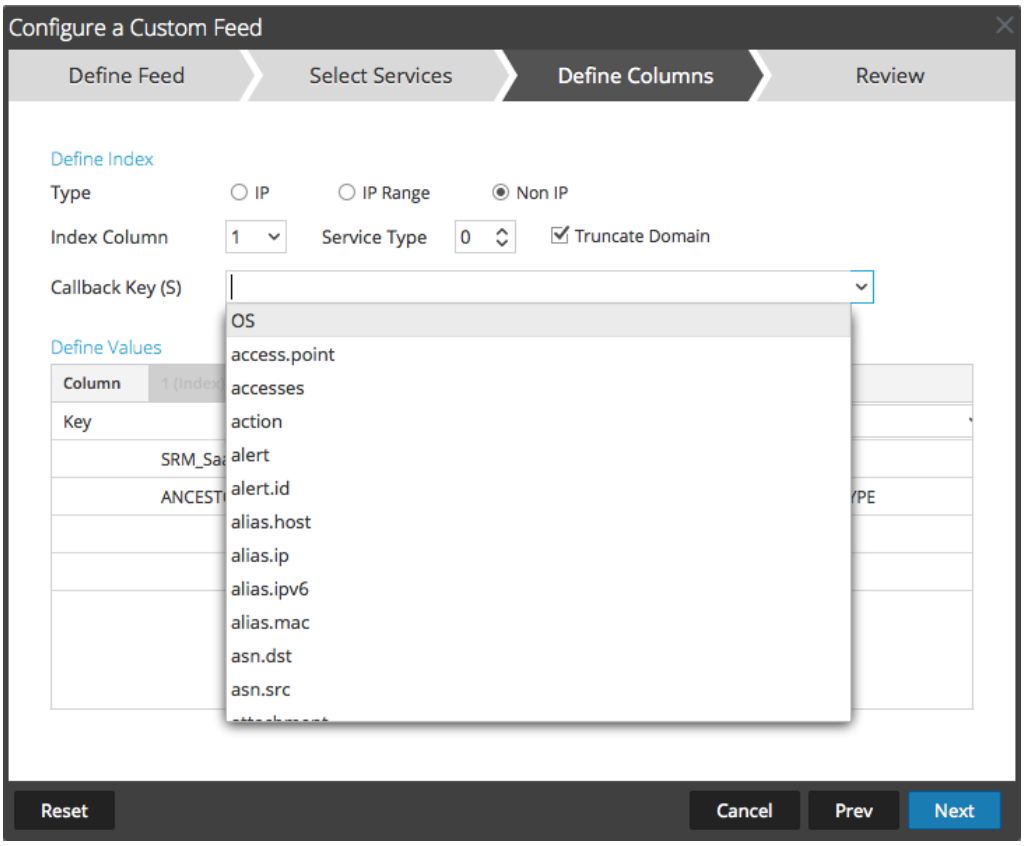
      Se muestra el formulario Definir columnas.

9. Para asignar columnas en el formulario Definir columnas, haga lo siguiente:

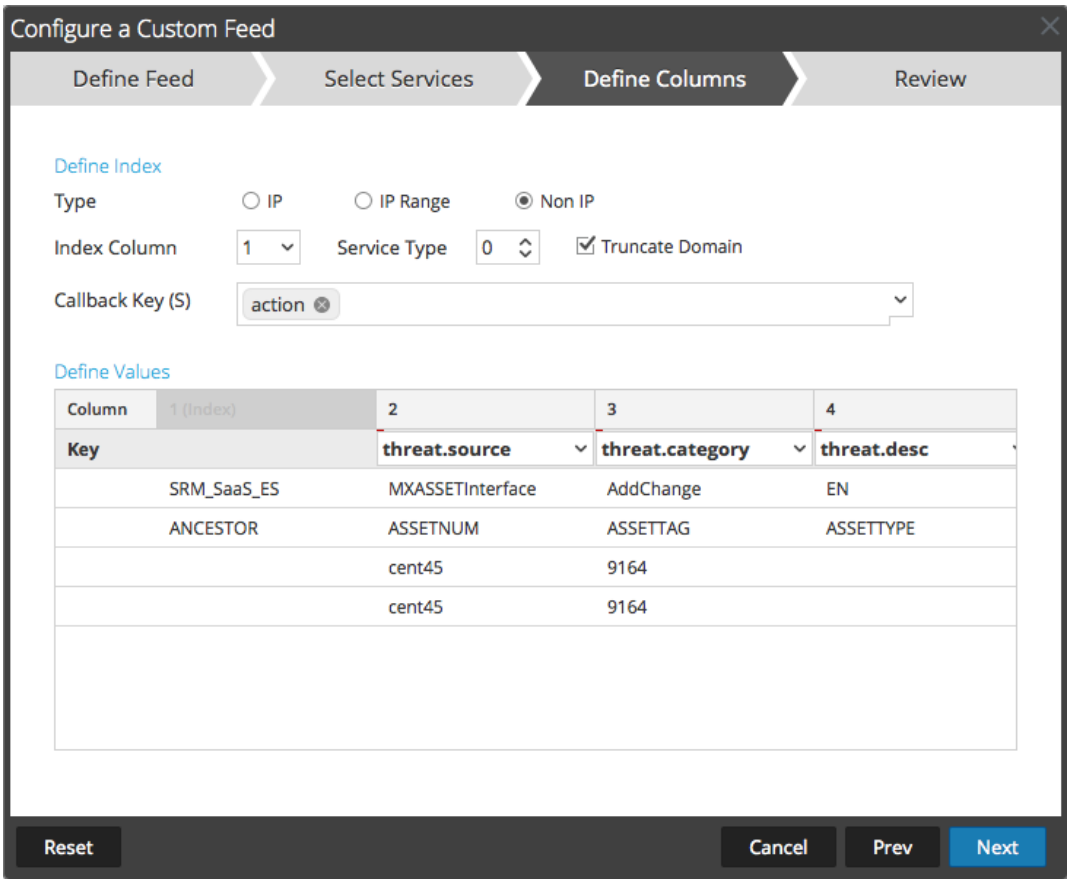
   a. Defina el tipo de Índice: **IP**, **Rango de IP** o **No IP** y seleccione la columna de índice.

   b. (Condicional) Si el tipo de índice es **IP** o **Rango de IP** y la dirección IP está en notación CIDR, seleccione **CIDR.**

   c. (Condicional) Si el tipo de índice es **No IP**, se muestran ajustes adicionales. Seleccione el tipo de servicio, las **Claves de devolución de llamadas** y, de manera opcional, la opción **Truncar dominio**.

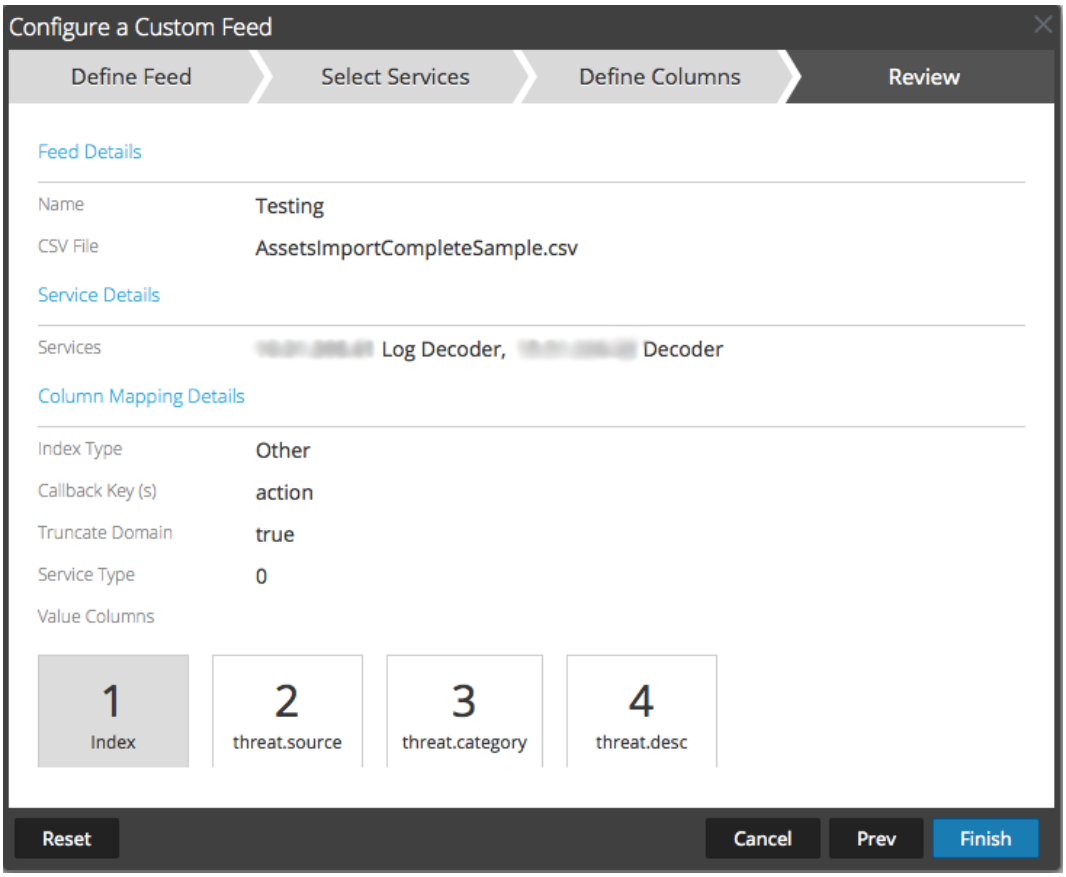



d. En la lista desplegable, seleccione la clave de idioma que se aplicará a los datos en cada columna. Los metadatos que se muestran en la lista desplegable se basan en los metadatos disponibles para los valores definidos del servicio. También puede agregar otros metadatos de acuerdo con su pericia avanzada.




e. Haga clic en **Siguiente**.

   Se muestra el formulario Revisión.




10. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:
    - Hacer clic en **Cancelar** para cerrar el asistente sin guardar la definición del feed.
    - Hacer clic en **Restablecer** para borrar los datos del asistente.
    - Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).
    - Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario).

11. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.
12. Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, el feed y el archivo de token correspondiente aparecen en la Feed grid y la barra de progreso muestra que se completó la tarea. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles tuvieron éxito.

### Feeds Metacallback con rango de índice CIDR para IPv4 e IPv6

En esta sección se describe cómo usar rangos de índice CIDR para IPv4 e IPv6 en feeds MetaCallback personalizados. Al igual que con otros feeds personalizados, debe crear el archivo de datos de feed en formato .csv y un archivo de definición de feed en formato .xml.

**Nota:** El uso de feeds MetaCallback con rangos de índice CIDR solo se admite mediante el asistente Configuración avanzada o la interfaz de REST.

En el siguiente ejemplo se muestra el contenido de un archivo .csv y un archivo .xml para un feed MetaCallback con rangos de índice CIDR para IPv4 o IPv6.

**.csv file:**

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

**.xml file:**

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator=","
comment="#">
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0"
truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

**Nota:** Para configurar un rango de índice CIDR para los feeds con uno o varios MetaCallbacks de tipo de valor IPv4 o IPv6, el campo de índice de tipo DEBE contener un atributo de rango con range="cidr". Además, no se admite la configuración de rangos de índice “cidr” para los feeds con MetaCallbacks de varios tipos de valor diferente.

## Crear un feed personalizado de STIX

Puede crear un feed personalizado con un archivo de datos de feed con formato STIX o .csv en RSA NetWitness Suite.

**Nota:** NetWitness Suite solo admite las versiones 1.0, 1.1 y 1.2 de Structured Threat Information Expression (STIX).

**Nota:** A partir de 10.6.1 o superior, Security Analytics admite Structured Threat Information Expression (STIX).

Structured Threat Information Expression (STIX™) es un lenguaje estructurado para describir información de amenazas cibernéticas, de modo que se pueda compartir, almacenar y analizar de manera coherente. Para obtener más información acerca de STIX, consulte https://stixproject.github.io/.

**Precaución:** Si se configura un feed recurrente STIX y se actualiza Security Analytics de 10.6x a NetWitness Suite 11.0, debe volver a configurar el feed recurrente STIX.

En NetWitness Suite, se admite el feed STIX (`.xml`) de tipo Indicador u Observable, que contiene propiedades como direcciones IP, hashes de archivo, nombres de dominio, URI y direcciones de correo electrónico. Solo se admite los valores de propiedades en el operador Es igual a. Y, los atributos, como Tipo y Título también se leen desde STIX (`.xml`). Solo se admite el STIX (`.xml` ) con un solo STIX_Package.

TAXII (Trusted Automated eXchange of Indicator Information) es el mecanismo de transporte principal para obtener información de amenazas cibernéticas que se representa en STIX. Mediante los servicios TAXII, las organizaciones pueden compartir la información sobre amenazas cibernéticas de manera segura y automatizada.

Las comunidades de STIX y TAXII trabajan en estrecha colaboración para asegurarse de proporcionar de forma constante una plataforma completa para el uso compartido de inteligencia de amenazas.

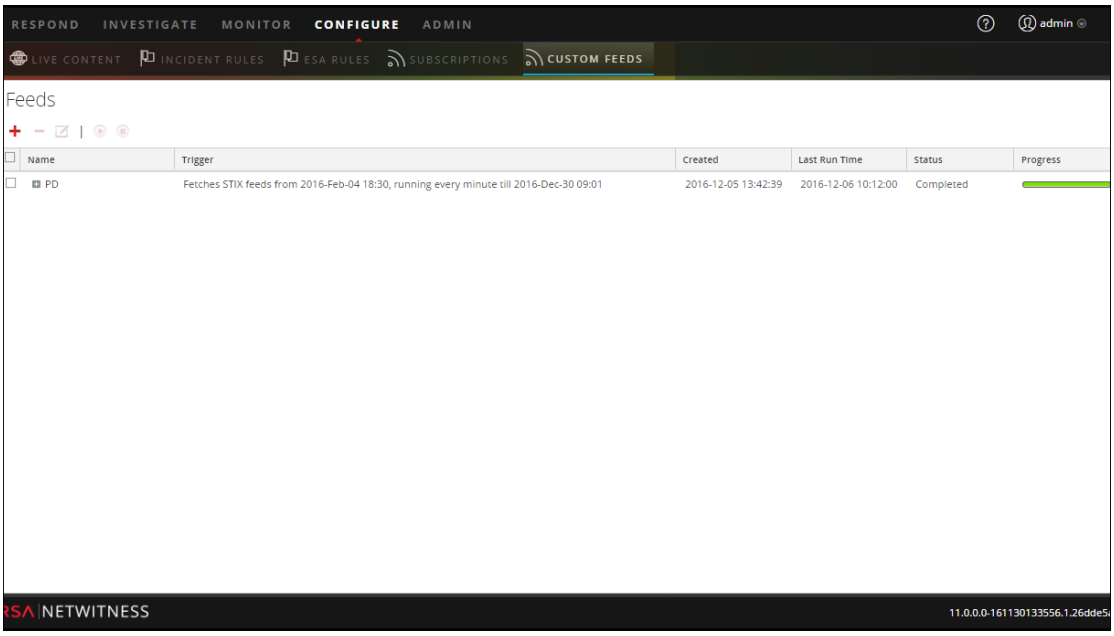
Aparte del servidor de TAXII, los datos de STIX también pueden residir en el servidor de REST y puede buscar el archivo STIX desde el servidor de REST mediante la dirección URL del servidor de REST. Por ejemplo, http://stixrestserver.internal.com.

El archivo de datos de feed (`.csv` o STIX (`.xml`)) y, de manera opcional, el archivo de definición de feed (`.xml`) deben estar disponibles en el sistema de archivos local para un feed personalizado según demanda. Para crear un feed personalizado recurrente, los archivos deben estar disponibles en una URL a la que se pueda acceder desde el servidor de NetWitness Suite.

### Para crear un feed personalizado de STIX:

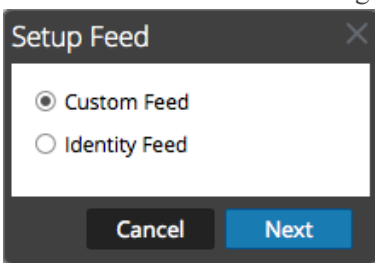
1. Vaya a **Configurar > Feeds personalizados**.

   Se muestra la vista Feeds.



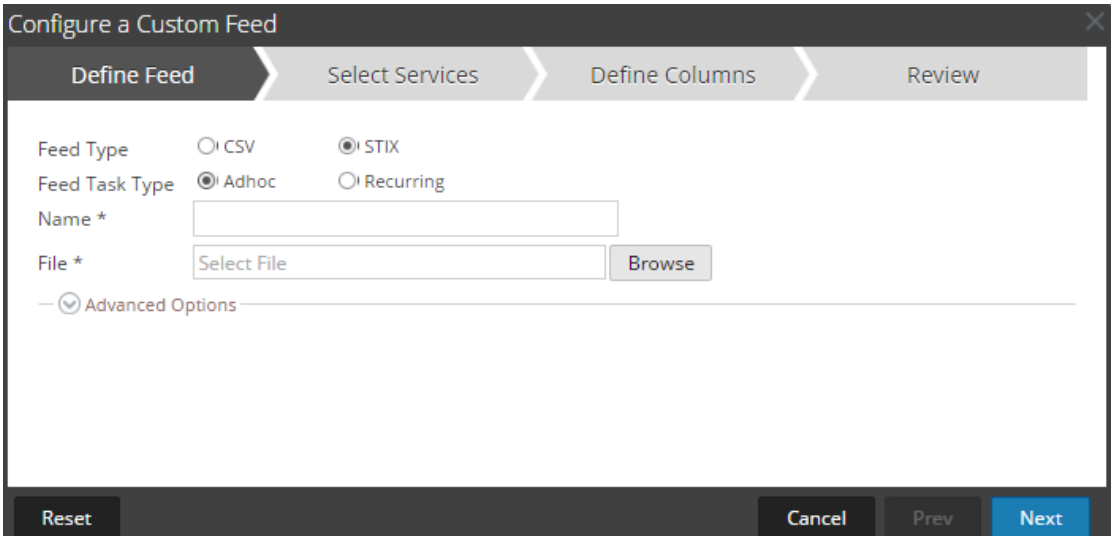

2. En la barra de herramientas, haga clic en +.

   Se muestra el cuadro de diálogo Configurar feed.



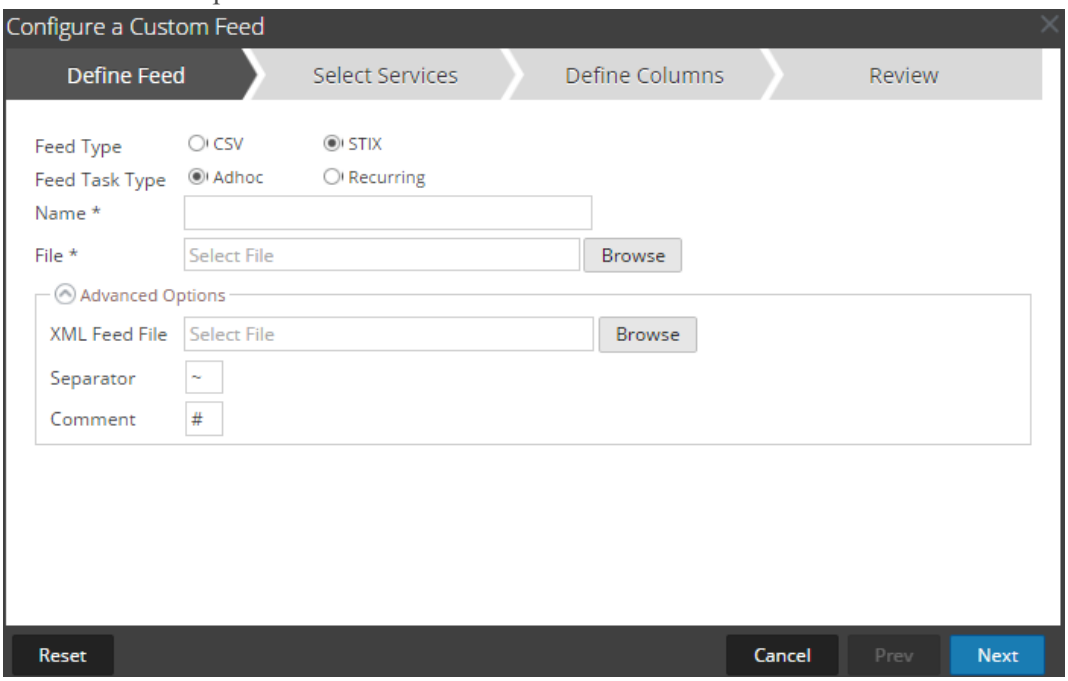

3. Para seleccionar el tipo de feed, haga clic en **Feed personalizado** y luego en **Siguiente**.

El asistente Configurar un feed personalizado se muestra con el formulario Definir feed abierto.



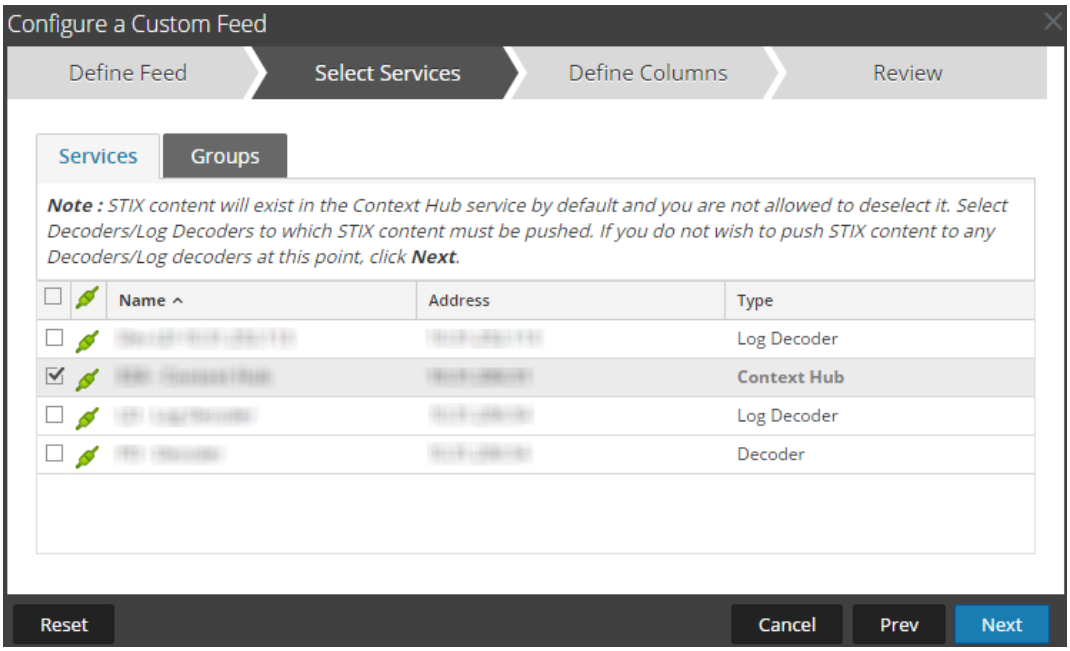

4. Para definir un feed basado en un archivo `.xml` con formato STIX, seleccione **STIX** en el campo **Tipo de feed**.
5. Para definir una tarea de feed según demanda que se ejecute una sola vez, seleccione **Ad hoc** en el campo **Tipo de tarea de feed** y realice una de las siguientes acciones:
   a. (Condicional) Para definir un feed basado en un archivo `.xml` con formato STIX, escriba el **Nombre** del feed, seleccione `.xml`un **archivo** de contenido con formato STIX en el sistema de archivos local y haga clic en **Siguiente**.
   b. (Condicional) Para definir un feed basado en un archivo de feed XML, seleccione **Opciones avanzadas**.

Se muestran las opciones avanzadas:




c. Seleccione un archivo de feed XML en el sistema de archivos local, elija el **Separador** (el valor predeterminado es coma), especifique los caracteres de **Comentario** que se utilizarán en el archivo de datos del feed (el valor predeterminado es #) y haga clic en **Siguiente**.

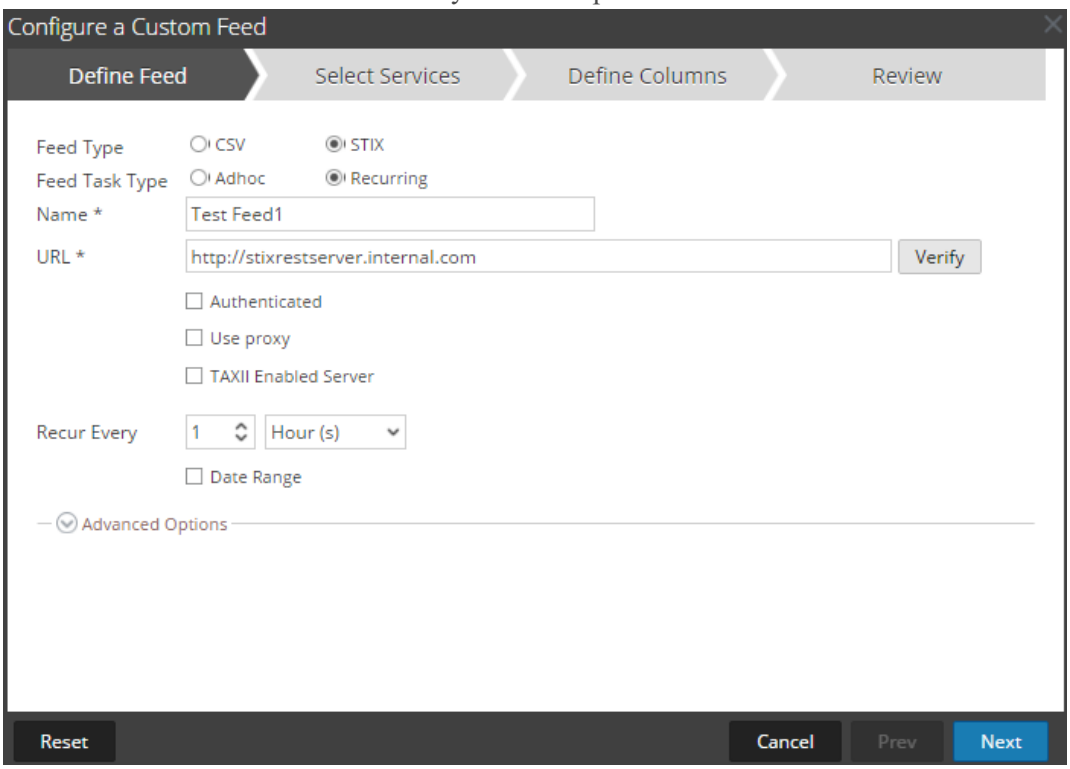
d. Se muestra el formulario Seleccionar servicios. Este es un ejemplo del formulario de un feed basado en un archivo de datos de feed sin archivo de definición de feed. Si define un feed basado en un archivo de definición de feed, la pestaña Definir columnas no es necesaria.




6. Para definir una tarea de feed recurrente que se ejecute de manera repetida a intervalos especificados durante un rango de fechas especificado:

   a. Seleccione **Recurrente** en el campo **Tipo de tarea de feed**.

   En el formulario Definir feed se incluyen los campos de un feed recurrente.

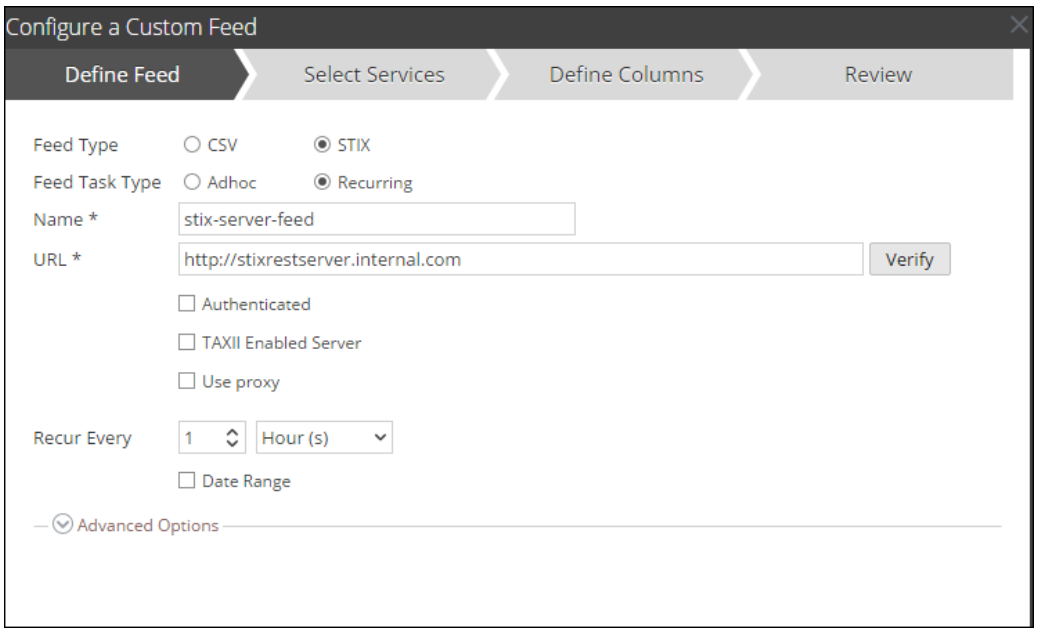


b. En el campo **URL**, realice una de las siguientes acciones:

- Para definir un feed recurrente basado en STIX que extrae paquetes de STIX desde un servidor de TAXII, ingrese la URL del servicio de descubrimiento del servidor de TAXII, por ejemplo, http://hailataxii.com/taxii-discovery-service.

  **Nota:** El servicio de Context Hub instalado en el host de Event Stream Analysis debe ser accesible para el servidor de TAXII especificado.

- Para definir un feed recurrente basado en un archivo .xml con formato STIX mediante el servidor de REST, ingrese la dirección URL del servidor de REST donde se encuentra el archivo de datos STIX, por ejemplo, http://stixrestserver.internal.com.




NetWitness Suite verifica la conexión con el servidor, para que NetWitness Suite pueda comprobar automáticamente el archivo más reciente antes de cada recurrencia.

c. Si no desea que NetWitness Suite verifique el certificado SSL del servidor de REST, seleccione **Confiar en todos los certificados**. Esta opción está habilitada de manera predeterminada (seleccionada)

d. Para la autenticación de cliente con la URL de REST, en el campo **Certificado**, haga clic en **Navegar** y seleccione el certificado autofirmado. Los formatos de certificados compatibles son .cer, .crt con archivos con codificación Base64 y DER.

e. (Opcional) Si la URL tiene acceso restringido y se solicita autenticación con nombre de usuario y contraseña, seleccione **Autenticada**.

NetWitness Suite proporciona su nombre de usuario y contraseña para autenticación en la dirección URL.

f. Seleccione **Servidor habilitado para TAXII** si desea seleccionar una recopilación de TAXII de la lista.
Para una URL válida, en función de sus credenciales se muestra una o más recopilaciones TAXII que contienen el archivo de datos STIX. Seleccione la recopilación TAXII requerida en la lista. Solo se puede agregar una recopilación desde un servidor de TAXII para un feed.

**Nota:** Aunque se admiten varios feeds de múltiples servidores de TAXII, solo se admite una cuenta (nombre de usuario y contraseña) con cada servidor de TAXII.

g. Si desea que el servidor de NetWitness Suite acceda a la dirección URL del feed a través de un proxy, seleccione **Usar proxy**. Para obtener más información sobre la configuración de un proxy, consulte el tema **Configurar el proxy de NetWitness Suite** en la *Guía de configuración del sistema*. De forma predeterminada, la casilla de verificación **Usar proxy** no está seleccionada.

h. (Opcional) Haga clic en **Verificar** para probar la configuración.

**Nota:** Asegúrese de que todos los parámetros de conexión requeridos, como Autenticación, Proxy, Confianza de certificados, Servidor habilitado para TAXII, etc. estén configurados antes de hacer clic en **Verificar**.

i. Para definir el intervalo de recurrencia para migrar a Decoder o Log Decoder, realice alguna de las siguientes acciones:

- Especifique la cantidad de minutos, horas o días entre cada recurrencia del feed.
- Especifique la recurrencia cada semana y seleccione los días de la semana.

j. Para definir el rango de fechas para la ejecución recurrente del feed, especifique la hora y la **Fecha de inicio** y la hora y la **Fecha de finalización**. La Fecha de inicio debe definirse desde cuando desea buscar los datos. Asegúrese de que la **fecha de inicio** no sea anterior a 180 días a partir de hoy.

7. (Condicional) Si desea definir un feed basado en un archivo de feed XML:

- Escriba el **Nombre** del feed y seleccione **Opciones avanzadas**.

  Se muestran los campos Opciones avanzadas.

- Seleccione un archivo de feed XML del sistema de archivos local, elija el **Separador** (el valor predeterminado es coma), especifique los caracteres de **Comentario** que se utilizarán en el archivo de datos del feed (el valor predeterminado es #).

- En el campo **Quitar datos de STIX más antiguos que**, especifique la cantidad de días durante los cuales se almacenarán los paquetes de STIX que se extraen del servidor de

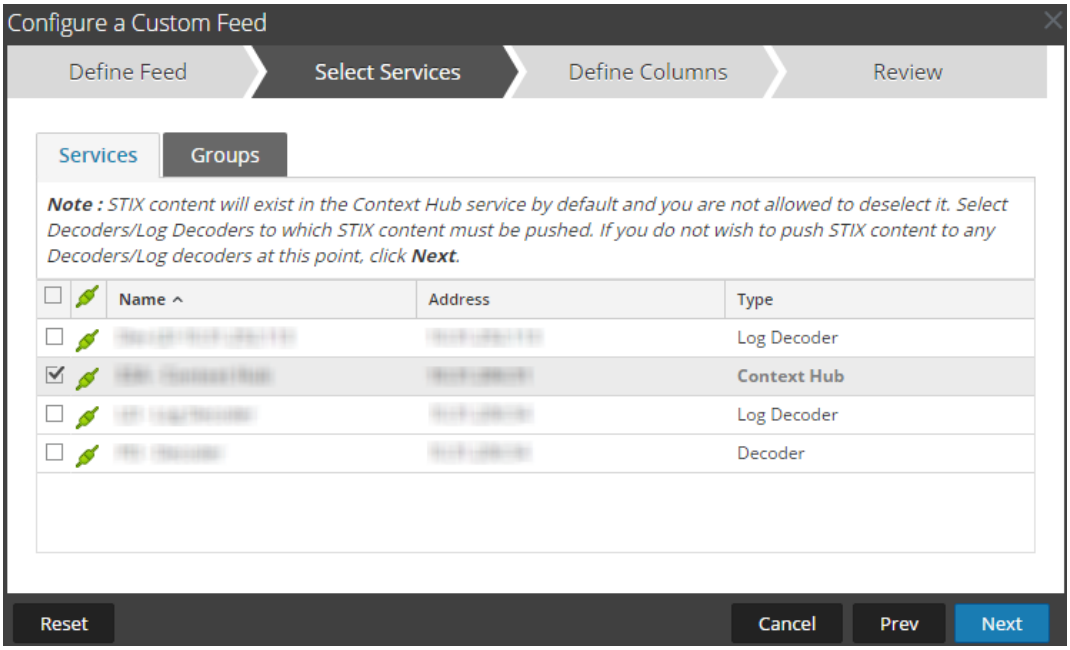
TAXII. Los paquetes de STIX más antiguos que la cantidad especificada de días se eliminan automáticamente.

- Haga clic en **Siguiente**.
  Se muestra el formulario Seleccionar servicios.

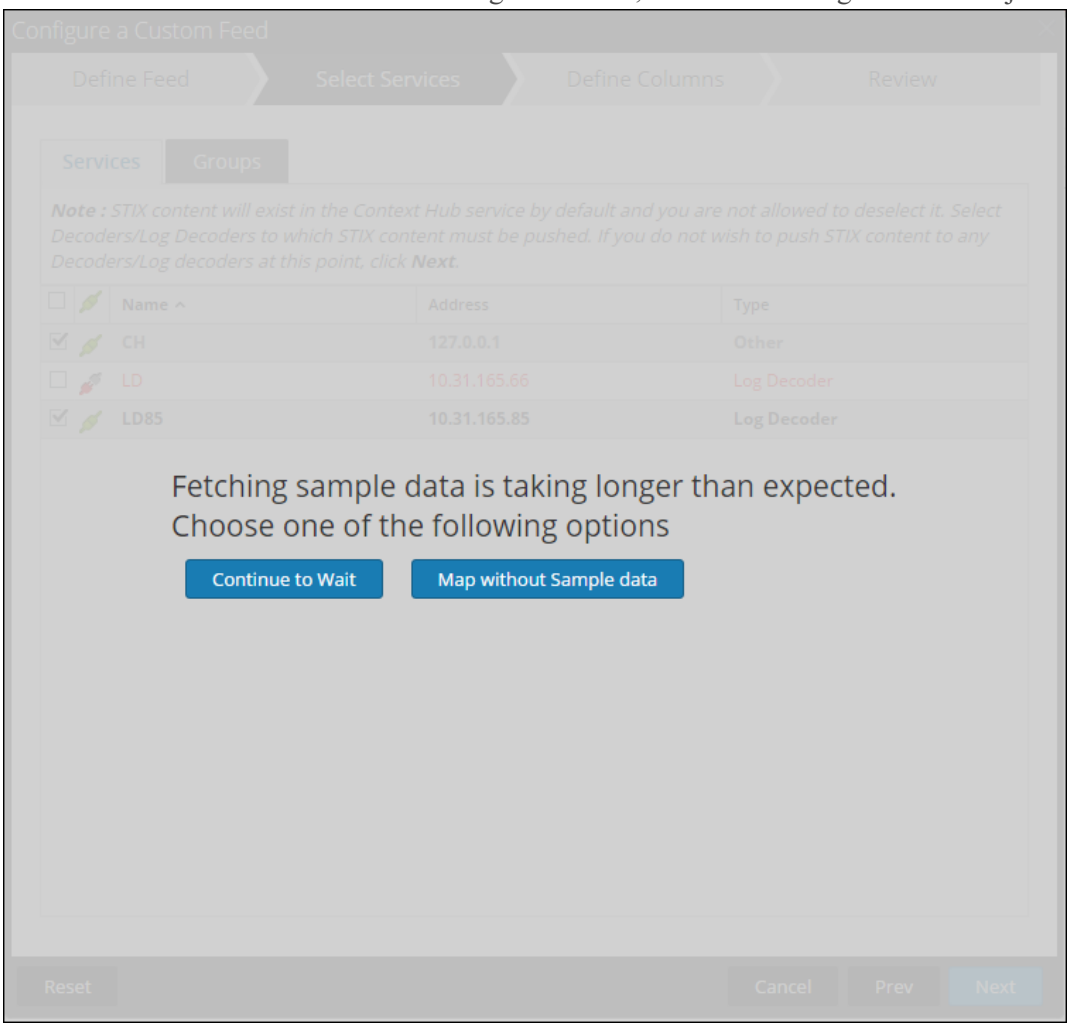
8. Para identificar los servicios en los cuales se implementará el feed, realice una de las siguientes acciones:

   a. Seleccione uno o más Decoders y Log Decoders y haga clic en **Siguiente**.

   b. En el caso del feed STIX, Context Hub se selecciona de manera predeterminada y no se permite deseleccionar la opción. Además, puede seleccionar uno o más Decoders y Log Decoders y hacer clic en **Siguiente** o en la pestaña **Grupos** y seleccionar un grupo. Haga clic en **Siguiente**.



Si los datos del servidor de STIX son de gran tamaño, se muestra el siguiente mensaje:

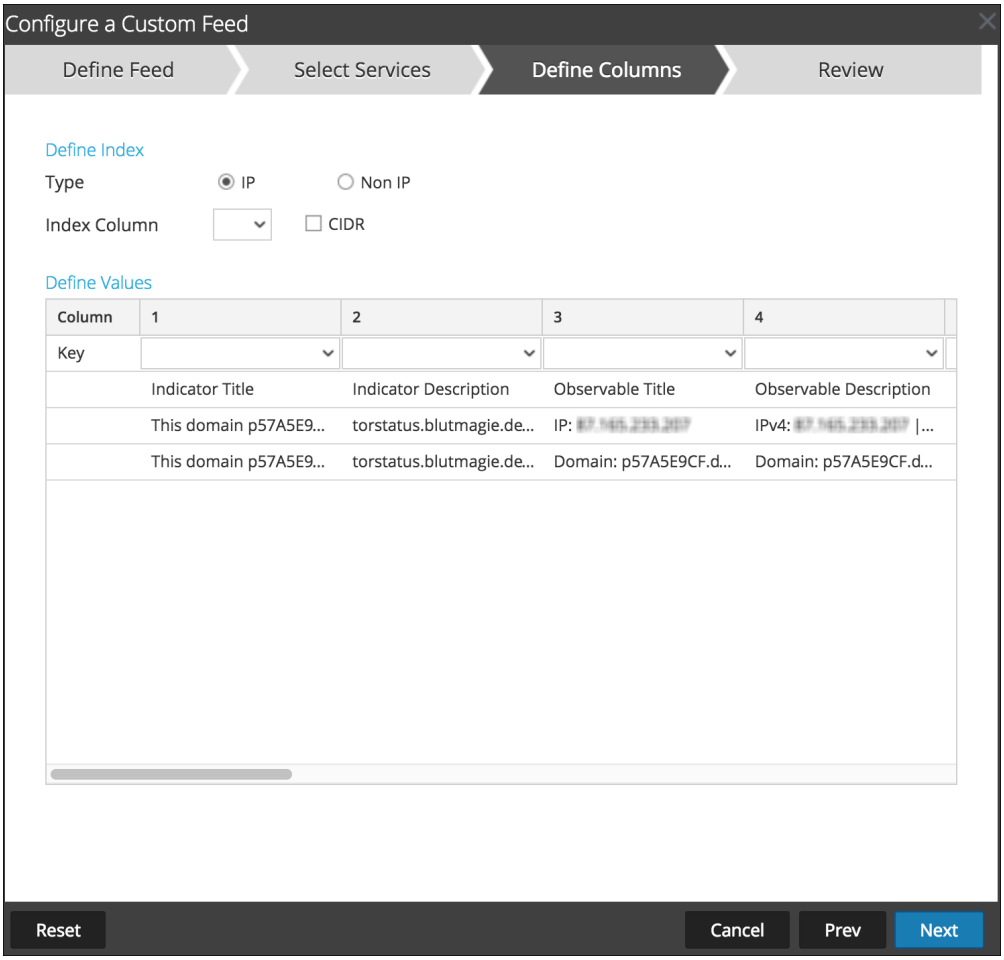



- Si hace clic en **Continuar esperando**, continúa esperando hasta que se buscan los datos de ejemplo o se agota el tiempo de espera (10 minutos), lo que primero ocurra. En el caso de tiempo de espera agotado, no se recupera ningún dato de ejemplo incluso después de 10 minutos.
- Si hace clic en **Mapear sin datos de ejemplo**, se muestra la columna de mapeo sin los datos de ejemplo.

Se muestra el formulario Definir columnas.

9. Para asignar columnas en el formulario Definir columnas, haga lo siguiente:
   a. Defina el tipo de Índice: **IP**, Rango de IP **o** No IP
      y seleccione la columna de índice.
   b. (Condicional) Si el tipo de índice es **IP** o **Rango de IP** y la dirección IP está en notación CIDR, seleccione **CIDR.**

c. (Condicional) Si el tipo de índice es **No IP**, se muestran ajustes adicionales. Seleccione el tipo de servicio, las **Claves de devolución de llamadas** y, de manera opcional, la opción **Truncar dominio**.



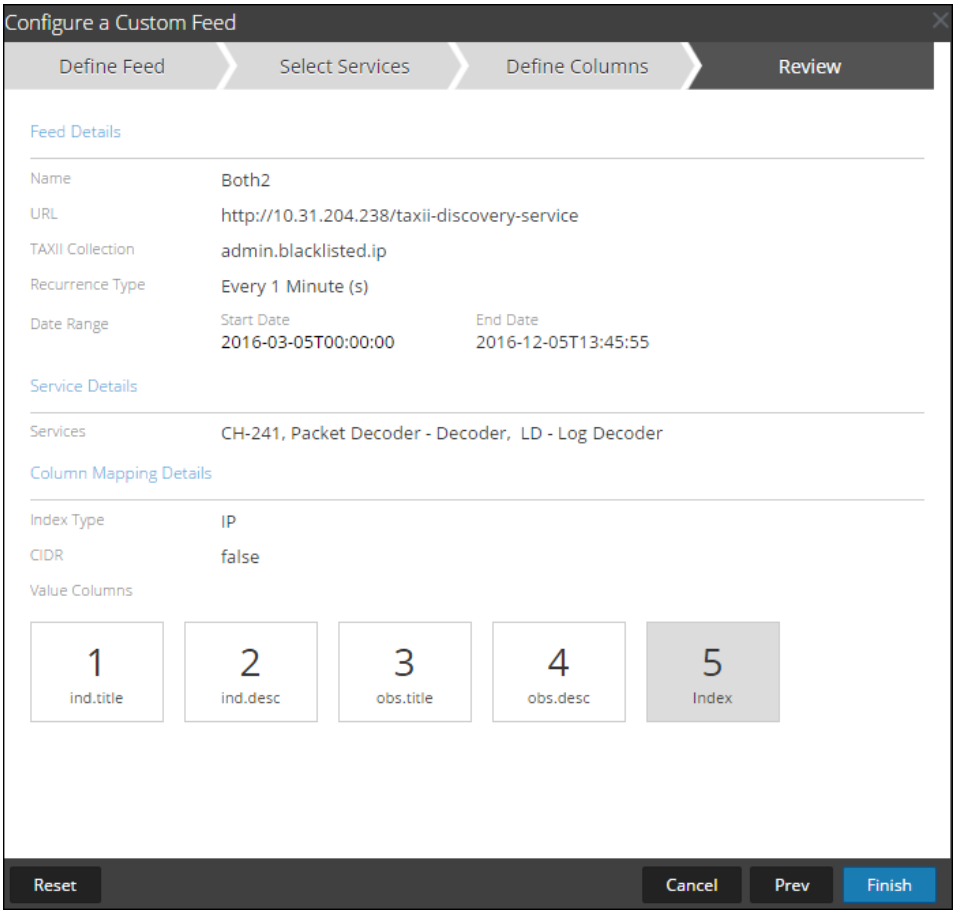

**Nota:**
-Si el **tipo de índice** es no IP, puede seleccionar varias columnas de índice en las **columnas de índice**. Los valores de todas las columnas seleccionadas se combinan en la primera columna de índice que seleccionó y los valores combinados se envían a Log Decoder para análisis. Por ejemplo, en las **columnas de índice** si selecciona 2,4,7 como columnas de índice, los valores de las columnas 2, 4 y 7 se combinan en la columna 2 y los valores se envían a Log Decoder para análisis.
- La indexación no se puede hacer para las columnas como Título del indicador, Descripción del indicador, Título observable, Descripción observable, ya que la búsqueda no se puede realizar para esas columnas.

d. En la lista desplegable, seleccione la clave de idioma que se aplicará a los datos en cada columna. Los metadatos que se muestran en la lista desplegable se basan en los metadatos disponibles para los valores definidos del servicio. También puede agregar

otros metadatos de acuerdo con su pericia avanzada.

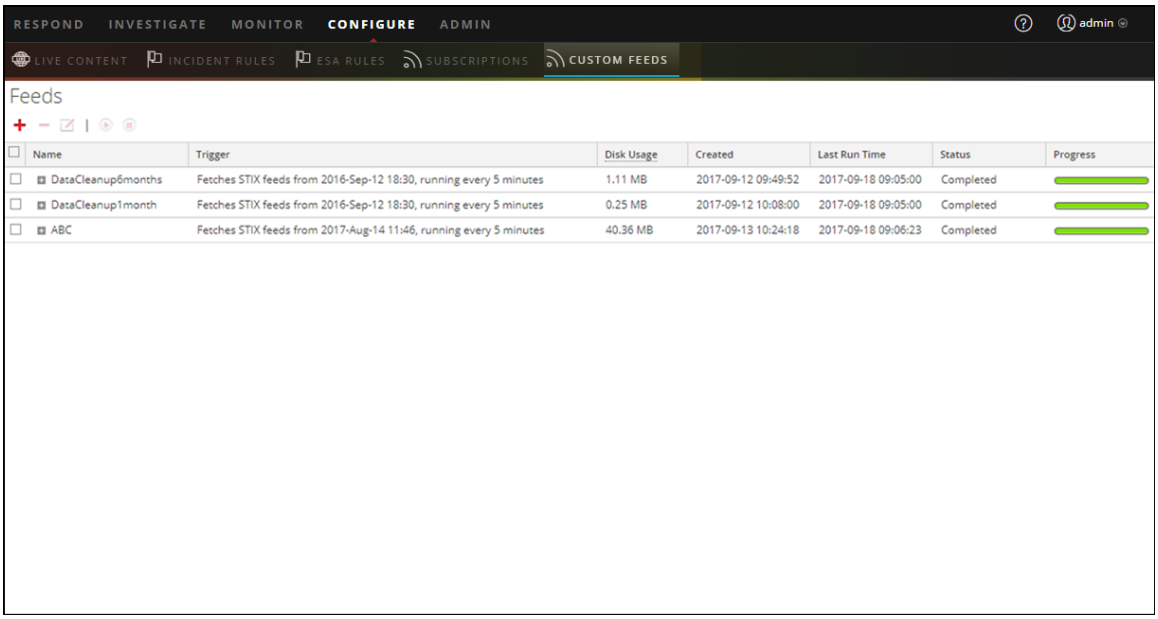
e. Haga clic en **Siguiente**.

Se muestra el formulario Revisión.




10. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:
    - Hacer clic en **Cancelar** para cerrar el asistente sin guardar la definición del feed.
    - Hacer clic en **Restablecer** para borrar los datos del asistente.
    - Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).
    - Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario).
11. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.
12. Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, el feed y el archivo de token correspondiente aparecen en la Feed grid y la barra de

progreso muestra que se completó la tarea. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles tuvieron éxito.




**Nota:** Estado y condición genera alertas cuando la memoria en montón disponible del servidor de Context Hub está en un nivel críticamente bajo. Si el servidor de Context Hub está en mal estado debido a la falta de memoria. Para obtener más información sobre cómo solucionar problemas de `OutOfMemoryError` en el servidor de `Contexthub`, consulte "Solución de problemas" en la *Guía de administración de servicios de Live*.

### Feeds Metacallback con rango de índice CIDR para IPv4 e IPv6

En esta sección se describe cómo usar rangos de índice CIDR para IPv4 e IPv6 en feeds MetaCallback personalizados. Al igual que con otros feeds personalizados, debe crear el archivo de datos de feed en formato .csv y un archivo de definición de feed en formato .xml.

**Nota:** El uso de feeds MetaCallback con rangos de índice CIDR solo se admite mediante el asistente Configuración avanzada o la interfaz de REST.

En el siguiente ejemplo se muestra el contenido de un archivo .csv y un archivo .xml para un feed MetaCallback con rangos de índice CIDR para IPv4 o IPv6.

**`.csv file:`**

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

**`.xml file:`**

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
```

```
<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," comment="#">
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0" truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

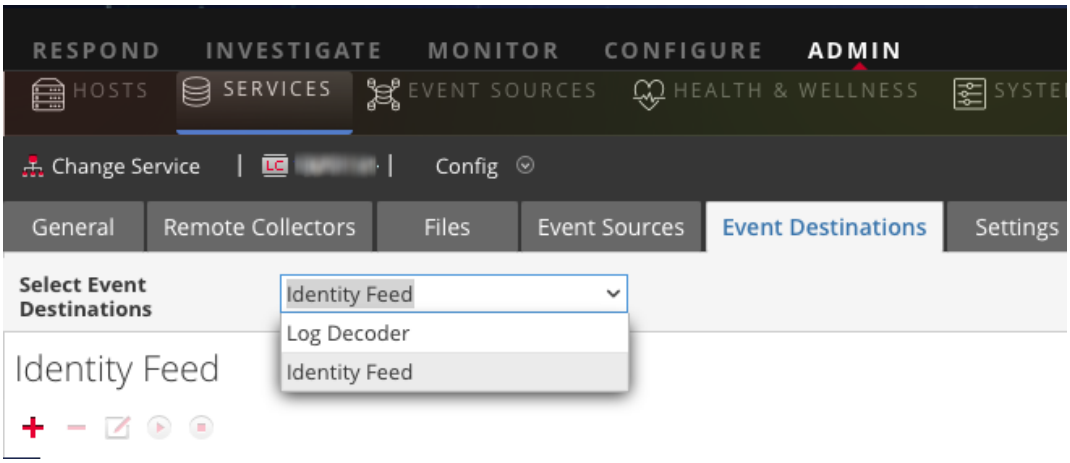
**Nota:** Para configurar un rango de índice CIDR para los feeds con uno o varios MetaCallbacks de tipo de valor IPv4 o IPv6, el campo de índice de tipo DEBE contener un atributo de rango con range="cidr". Además, no se admite la configuración de rangos de índice “cidr” para los feeds con MetaCallbacks de varios tipos de valor diferente.

## Crear y administrar un feed de identidad

Puede crear fácilmente un feed de identidad y completarlo para los Decoders y los Log Decoders seleccionados. Después de realizar este procedimiento, habrá creado un feed de identidad.

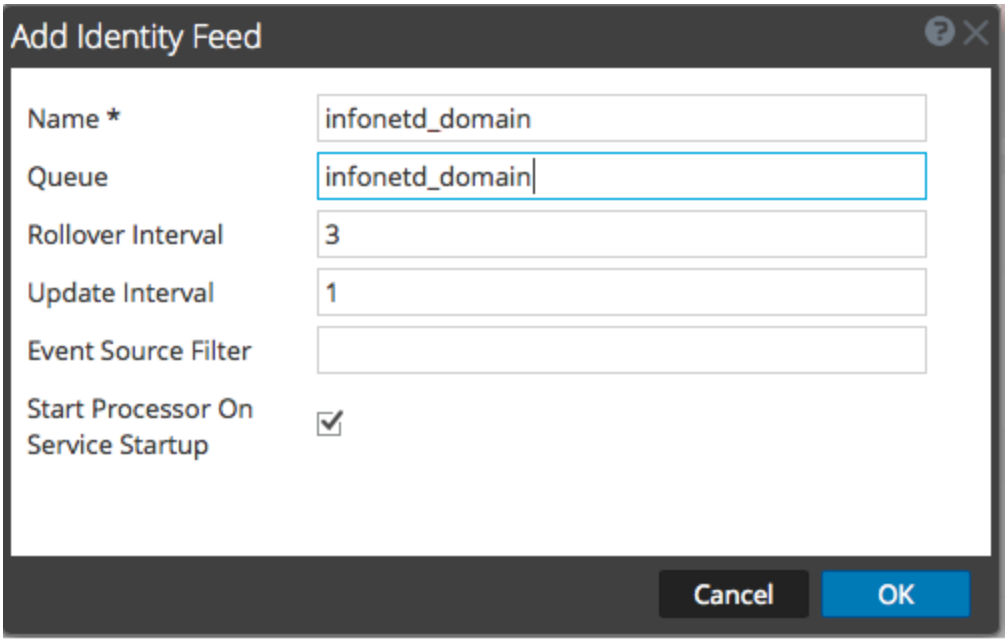
### Para crear un feed de identidad:

1. Agregue un destino para el feed.
   a. Vaya a **ADMIN > Servicios**, en la lista **Servicios** seleccione un servicio **Log Collector** y luego **Ver > Configuración**.
   b. Seleccione la pestaña **Destinos de evento**.
   c. En el campo **Seleccionar destinos de evento**, seleccione **Feed de identidad**.




d. Haga clic en + e ingrese un nombre único para el feed.

El nombre Línea de espera identifica el feed en el Log Collector. Use el nombre del feed para la Línea de espera.



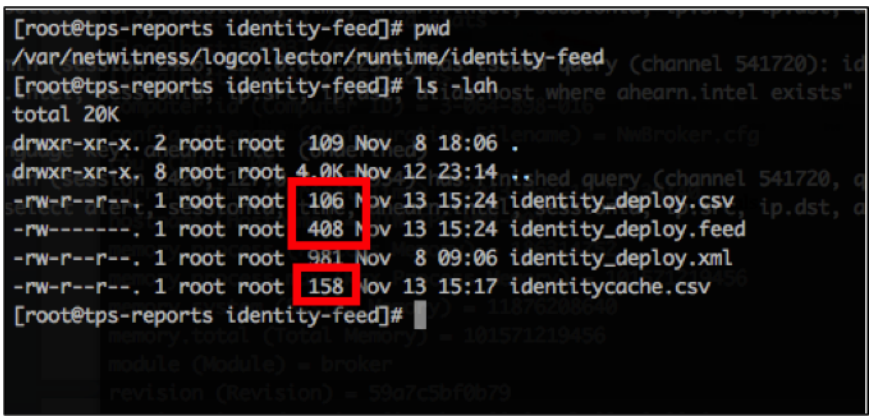

e. Haga clic en **Aceptar**.

2. Pruebe la generación de mensajes.

a. Compruebe que los usuarios hayan iniciado sesión en los cuadros de Windows en el dominio para generar los mensajes de registro correspondientes en los controladores de dominio para las pruebas.

b. Verifique que los datos estén escritos en los archivos de feed. Acceda mediante el protocolo SSH a Log Decoder/Collector o a Virtual Log Collector que se están

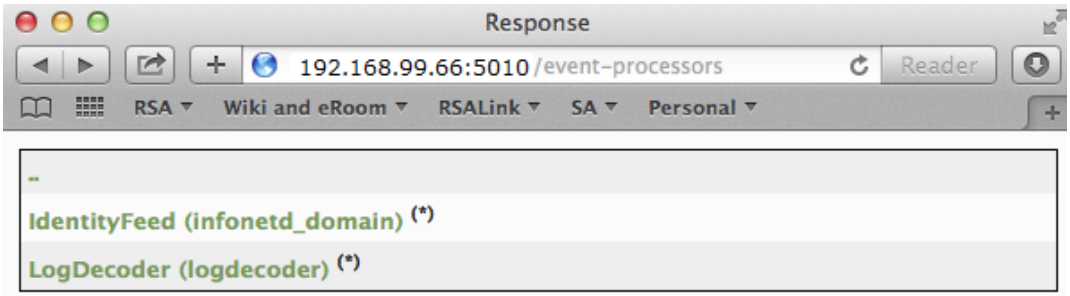
configurando. Navegue a `/var/netwitness/logcollector/runtime/identity-feed` y verifique que los archivos `Identity_deploy` se completen con los datos.




c. Abra un navegador web (se recomienda usar un navegador distinto de Internet Explorer) e inicie sesión en la interfaz de REST de Log Collector. Use las credenciales administrativas cuando inicie sesión. Por ejemplo, si la dirección IP de su Log Collector es 192.168.99.66, entonces la dirección URL sería:

- SSL no habilitado: **http://192.168.99.66:50101/event-processors**
- SSL habilitado: **https://192.168.99.66:50101/event-processors**

La pantalla del navegador debe verse así:

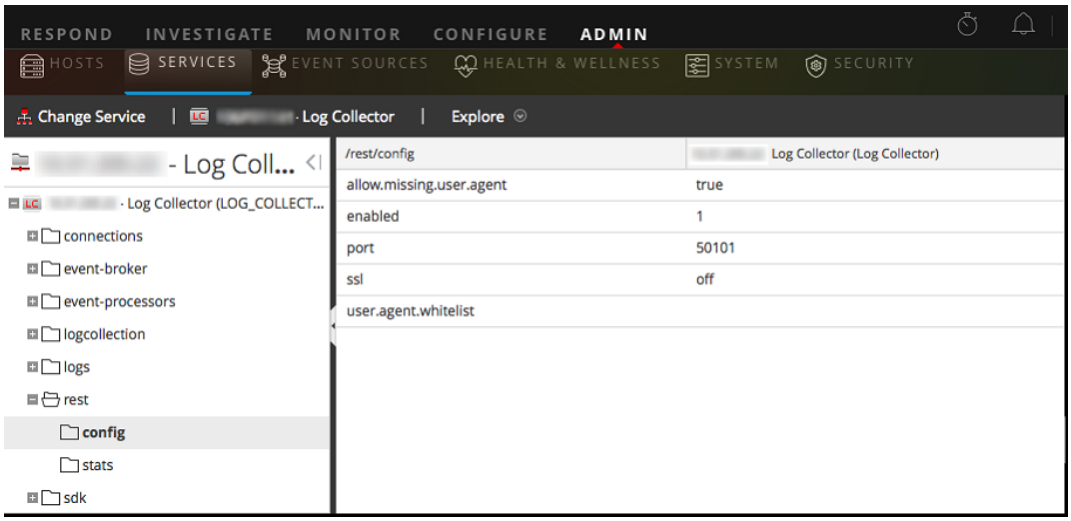



Observe que la pantalla contiene el nombre del feed de identidad del feed que creó anteriormente (`infonetd_domain`, en este ejemplo).

Para que el feed de identidad funcione correctamente, el puerto 50101 debe estar activo en el Log Collector y debe determinar si el cifrado SSL está activo.

d. Vaya a **ADMIN > Servicios > *<Log Collector que se debe configurar>***  **> Ver > Explorar**.

e. En el panel izquierdo, expanda **rest > configuración**.



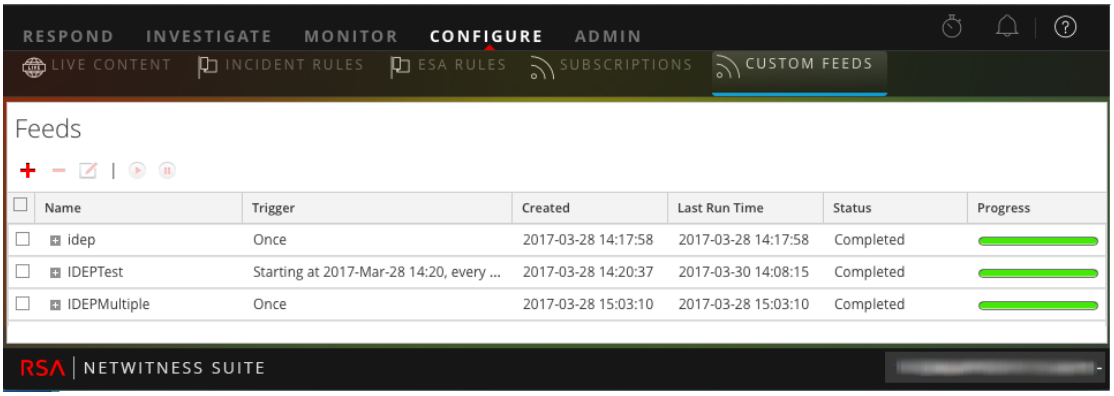

Para que REST esté activo, **habilitado** se debe configurar en **1**.

f. Observe el valor para **ssl**. Si SSL debe estar habilitado para su ambiente, se debe configurar en **activado**.

> **Nota:** Si cambió la configuración para la opción **habilitado** o la opción **ssl**, debe reiniciar el servicio Log Collector antes de continuar.

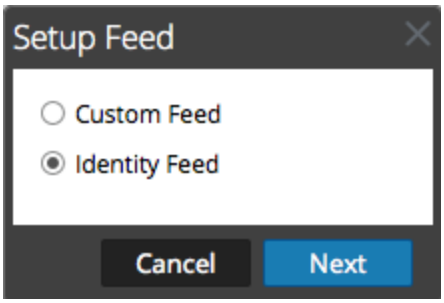
3. Vaya a **CONFIGURAR > Live Content > Feeds personalizados**.

   Se muestra la cuadrícula Feeds.




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

   Se muestra el cuadro de diálogo Configurar feed.



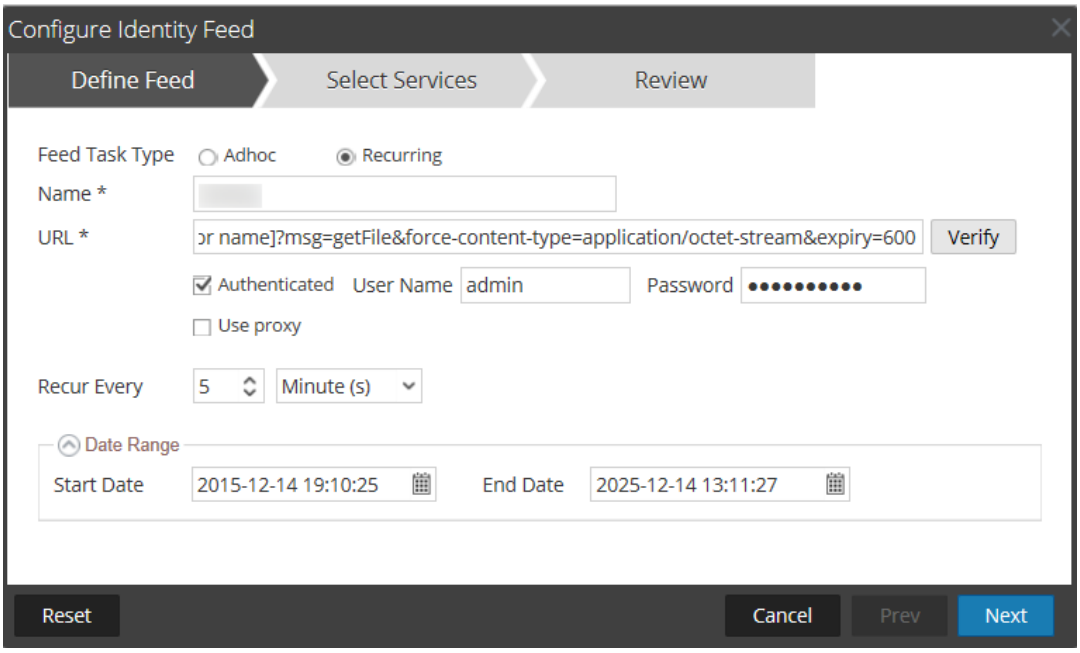

5. Asegúrese de que la opción **Feed de identidad** esté seleccionada y haga clic en **Siguiente**.

   El panel Configurar feed de identidad se abre con la pestaña **Definir feed** abierta.

6. (Condicional) Puede crear un feed según demanda o recurrente.

   - Para definir una tarea de feed de identidad según demanda que se ejecute una vez, seleccione **Ad hoc** en el campo **Tipo de tarea de feed**, escriba el **Nombre** del feed y, a continuación, busque y abra el feed.
   - Para definir una tarea recurrente de feed de identidad que se ejecuta de manera recurrente, seleccione **Recurrente** en el campo **Tipo de tarea de feed**.

     En el formulario **Definir feed** se incluyen los campos de un feed recurrente.




**Nota:** RSA NetWitness Suite verifica la ubicación en la cual está almacenado el archivo para que Security Analytics pueda comprobar automáticamente el archivo más reciente antes de cada recurrencia.

7. Rellene y verifique el campo URL.

a. En el campo **URL**, escriba la dirección URL en la cual está ubicado el archivo de datos del feed. Esta es la interfaz de API REST que se configuró anteriormente. Debe contar con la siguiente información para construir la dirección URL:

   - La dirección IP del Log Collector que se usa para construir el archivo de feed de identidad.
   - El nombre de la línea de espera de identidad, como se configuró en el paso 2c.
   - Si SSL está habilitado o no en el puerto REST de Log Collector, como se configuró en el paso 2f.

   Construya este valor de la siguiente manera:

   - SSL habilitado: `https://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`
   - SSL no habilitado: `http://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

   Por lo tanto, si se usa nuestro ejemplo anterior, el valor completo que debe ingresar en este campo es el siguiente:

   ```
   http://192.168.99.66:50101/event-processors/infonetd_domain?msg=getFile&force-content-type=application/octet-stream&expiry=600?msg=getFile&force-content-type=application/octet-stream&expiry=600
   ```

b. Para que la verificación de la dirección URL funcione correctamente, es importante que el servidor de interfaz del usuario de Security Analytics pueda acceder al puerto de API REST del Log Collector (50101). Esto se puede probar al acceder mediante el protocolo SSH al servidor de interfaz del usuario de Security Analytics. Una vez que esté ahí, ejecute el siguiente comando:

   - SSL habilitado: `curl -vk https://<ip of log collector>:50101`
   - SSL no habilitado: `curl -v http://<ip of log collector>:50101`

   Si el comando `curl` no se conecta, entonces puede haber un problema de firewall de la red o de enrutamiento entre el servidor de interfaz del usuario de Security Analytics y el Log Collector.

   Ejemplo de mala conexión:

   ```
   * About to connect() to 192.168.99.66 port 50105 (#0)
   * Trying 192.168.99.66... No route to host
   ```

```
* couldn't connect to host

* Closing connection #0

curl: (7) couldn't connect to host

Example of Good connection:

* About to connect() to 192.168.99.66 port 50105 (#0)

* Trying 192.168.99.66... connected

* Connected to 192.168.99.66 (192.168.99.66) port 50105
(#0)

> GET / HTTP/1.1

> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu)
libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18
libssh2/1.4.2

> Host: 192.168.99.66:50105

> Accept: */*

>

< HTTP/1.1 401 Unauthorized

< Content-Length: 71

< Connection: Keep-Alive

< Pragma: no-cache

< Expires: -1

< Cache-Control: no-cache, no-store, must-revalidate

< WWW-Authenticate: Basic realm="NetWitness"

< Content-Type: text/xml; charset=utf-8

<

<?xml version="1.0" encoding="utf-8"?>

<error>401 Unauthorized</error>

* Connection #0 to host 192.168.99.66 left intact

* Closing connection #0
```

8. La API REST requiere un nombre de usuario y una contraseña al intentar extraer el archivo `identity_deploy.csv` del Log Collector. Puede ser cualquier nombre de usuario y contraseña que estén disponibles en el propio servicio. Para obtener detalles, consulte el tema “Vista Seguridad de servicios” en la *Guía de hosts y servicios*.

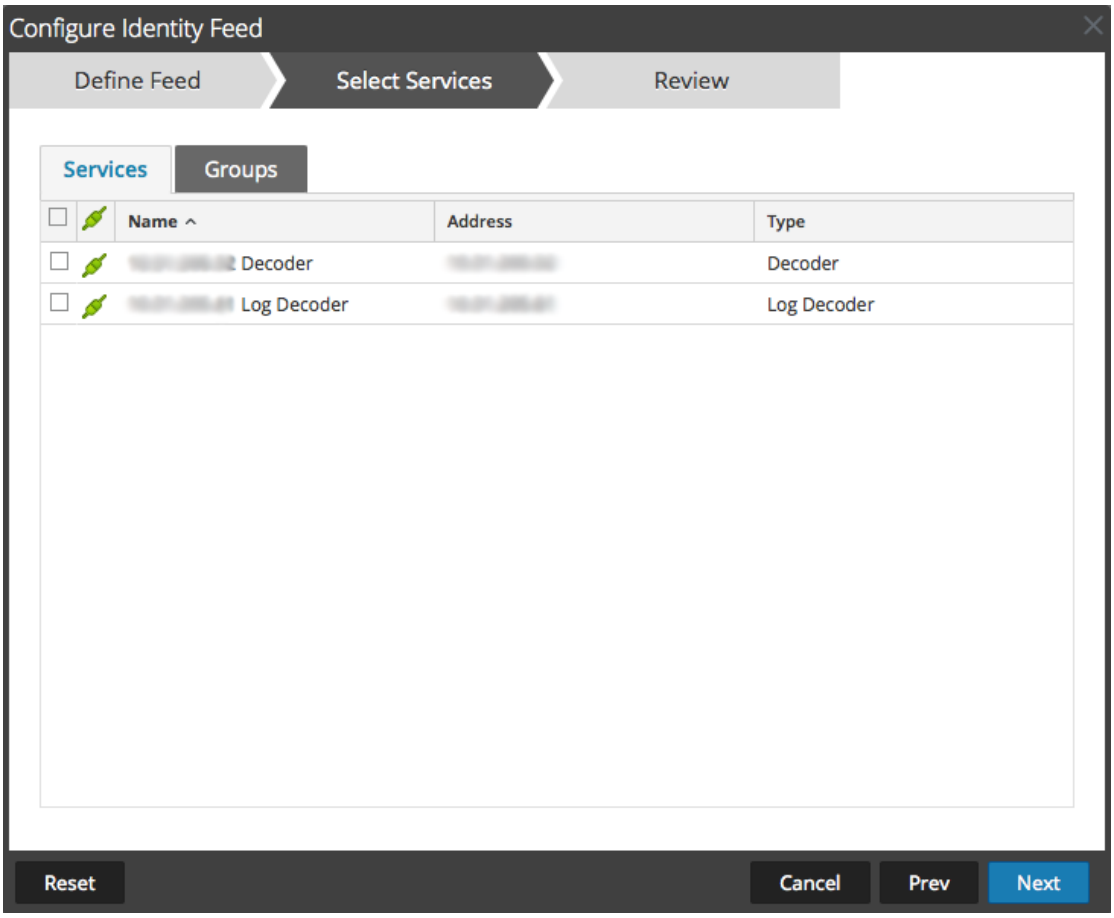
Para ver las cuentas que están disponibles, vaya a **ADMIN > Servicios > <Log Collector que se debe configurar> > Acciones > Ver > Seguridad**.

En la tabla Usuarios, verá todos los usuarios que se pueden usar en este paso. Se sugiere crear una cuenta de usuario separada específicamente para esta configuración, que no se usa en ninguna otra parte en el ambiente para brindar mayor seguridad. Para obtener detalles, consulte "Agregar un usuario y asignar una función" en la *Guía de administración de usuarios y seguridad del sistema*. (Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.)

9. Para definir el intervalo de recurrencia, puede realizar alguna de las siguientes acciones:
   - Especifique la cantidad de minutos, horas o días entre cada recurrencia del feed.
   - Para definir el rango de días para la ejecución recurrente del feed, especifique la hora y la **Fecha inicial** y la hora y la **Fecha de finalización**.
10. Si usa el cifrado SSL, debe instalar el certificado SSL de API REST para el Log Collector en el servidor de interfaz del usuario de Security Analytics. Para obtener detalles, consulte Importar el certificado SSL.

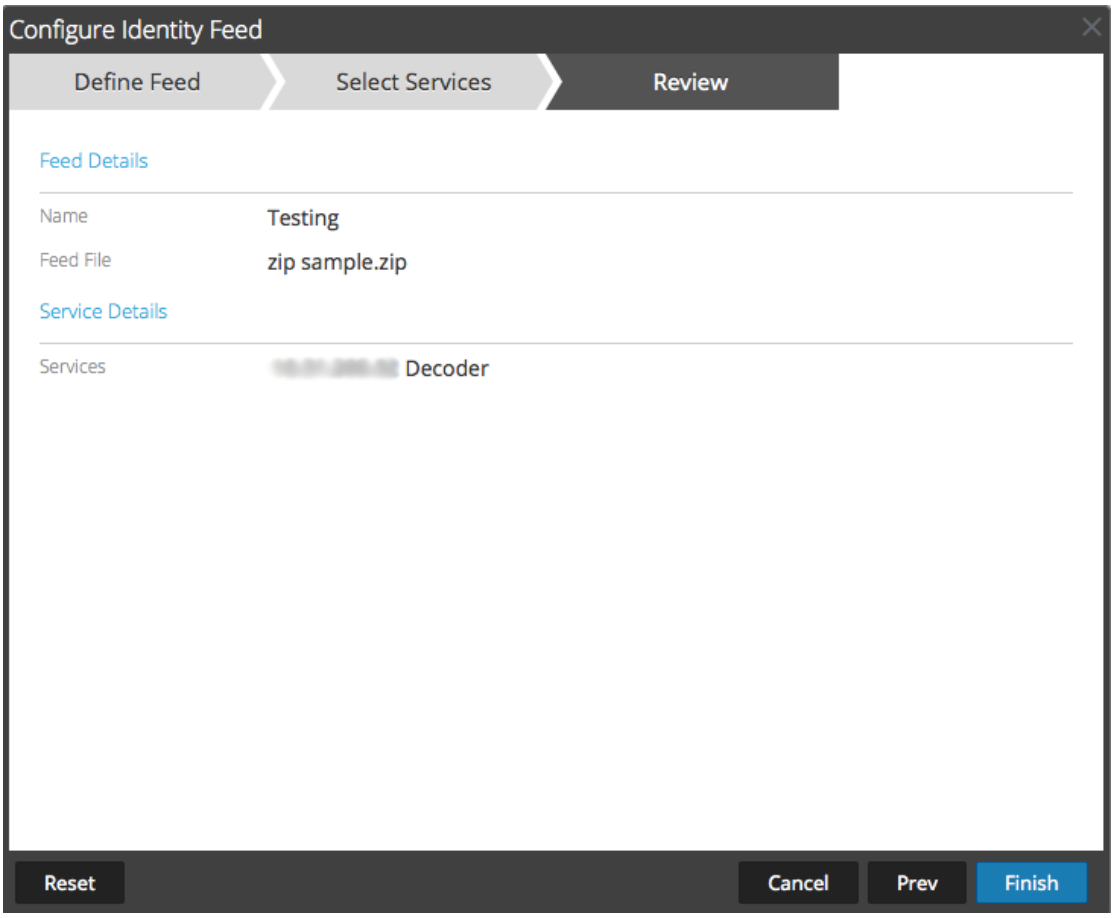
    Si, después de importar el certificado SSL, aún falla la verificación de la dirección URL, consulte No se puede verificar la dirección URL del feed de identidad.
11. Haga clic en **Verificar** para verificar su configuración de feed de identidad antes de continuar con el formulario Seleccionar servicios.
12. Haga clic en **Siguiente**.

    Se muestra el formulario Seleccionar servicios.




13. Para identificar los servicios en los cuales se implementará el feed, seleccione uno o más Decoders y Log Decoders, y haga clic en **Siguiente**.
14. Haga clic en la pestaña **Grupos**, seleccione un grupo y haga clic en **Siguiente**.

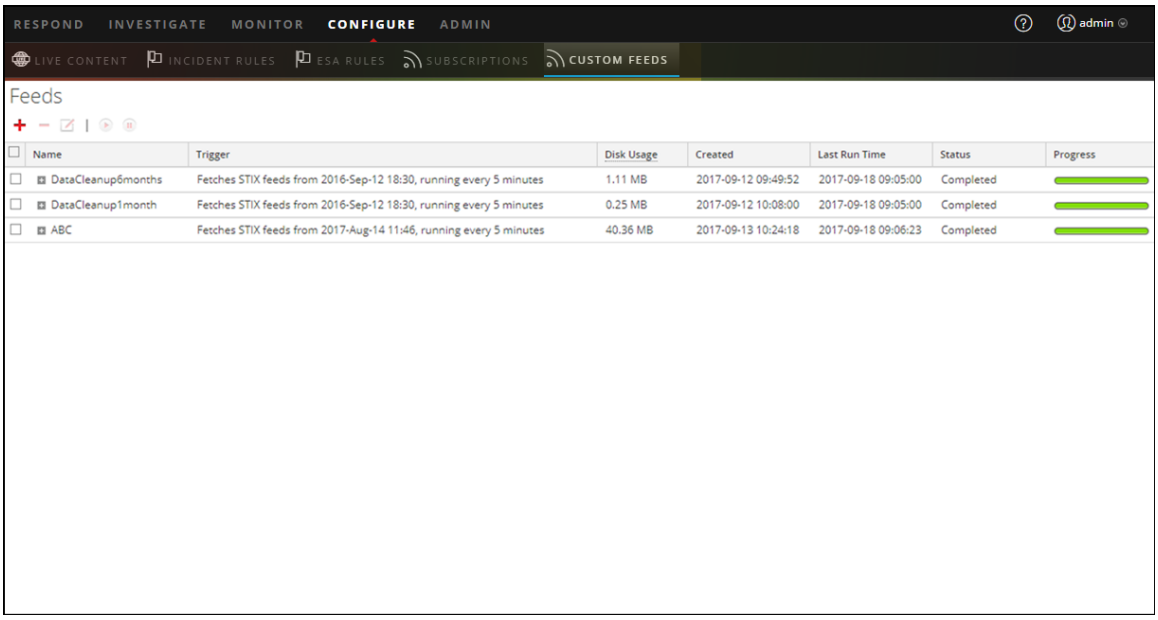
    Se muestra el formulario Revisión.




**Nota:** Si un grupo de dispositivos con Decoders y Log Decoders se usa para crear feeds personalizados o recurrentes y se puede eliminar este grupo, puede editar el feed y agregarle un grupo nuevo.

15. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:
    - Hacer clic en **Cancelar** para cerrar el asistente sin guardar la definición del feed.
    - Hacer clic en **Restablecer** para borrar los datos del asistente.
    - Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).
    - Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario).
16. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.

Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, el feed y el archivo de token correspondiente aparecen en la Feed grid y la barra de progreso muestra que se completó la tarea. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles tuvieron éxito.




### Importar el certificado SSL

Si SSL está configurado en el Log Collector del feed de identidad, siga estos pasos para importar el certificado SSL del Log Collector al almacenamiento de claves del servidor de interfaz del usuario de Security Analytics. Si este certificado no se importa, el servidor de interfaz del usuario de Security Analytics no podrá extraer el archivo de feed de identidad del Log Collector.

1. Para extraer el certificado SSL del Log Collector, acceda mediante el protocolo SSH al servidor de interfaz del usuario de Security Analytics y ejecute el siguiente comando:

   ```
   echo -n | openssl s_client -connect <HOST>:<PORT> | sed -ne
   '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/<SERVERNAME>.cert
   ```

   Este comando guarda el certificado SSL en `/tmp/<SERVERNAME>.cert`.

   Por ejemplo:

   ```
   echo -n | openssl s_client -connect 192.168.99.66:50101 | sed
   -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/logcollector.cert
   ```

2. Para importar el certificado SSL al servidor de interfaz del usuario de Security Analytics, acceda mediante el protocolo SSH al servidor de interfaz del usuario y ejecute el siguiente comando:

   ```
   keytool -importcert -alias <name an alias for the cert> -file
   <the cert file pathname> -keystore /etc/pki/java/cacerts
   ```

   Por ejemplo:

```
keytool -importcert -alias logcollector01 -file
/tmp/logcollector.cert -keystore /etc/pki/java/cacerts
```

3. El sistema solicita una contraseña. Ingrese la contraseña para el almacenamiento de claves en el servidor de interfaz del usuario de Security Analytics, no para el almacenamiento de claves de jetty. La contraseña predeterminada es **changeit**.
4. Reinicie **jettysrv** para permitir que jetty lea el nuevo certificado en el almacenamiento.

### No se puede verificar la dirección URL del feed de identidad

Si no puede verificar la dirección URL del feed de identidad y está usando SSL, asegúrese de haber seguido los pasos descritos en Importar el certificado SSL.

Si aún hay problemas, es posible que el nombre interno del certificado no coincida con el nombre de host del Log Collector. El siguiente procedimiento comprueba esto.

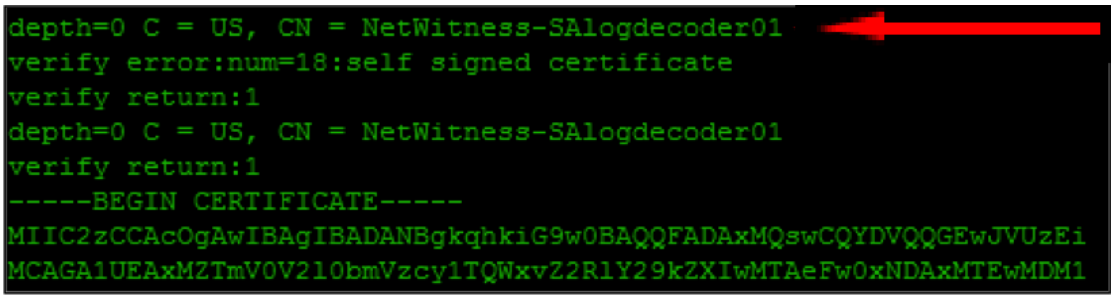
1. Acceda mediante el protocolo SSH al servidor de interfaz del usuario de Security Analytics.
2. Ejecute el siguiente comando para generar el nombre de CN del certificado SSL:

   ```
   echo -n | openssl s_client -connect <log decoder>:50101 | sed
   -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

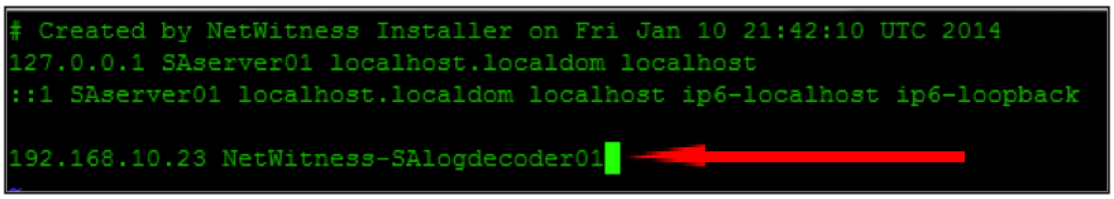
   Ejemplo:

   ```
   echo -n | openssl s_client -connect salogdecoder01:50101 |
   sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

3. Recupere el nombre de CN del certificado SSL.




4. Edite el archivo `/etc/hosts` y agregue la dirección IP y el nombre de CN al archivo.




5. Reinicie el servicio de red en el dispositivo.

6. Confirme que el nombre colocado en el archivo **/etc/hosts** se use en lugar del nombre de dominio calificado o de la dirección IP en la dirección URL del feed de identidad.
7. Vuelva a verificar la dirección URL del feed de identidad.

### Investigar un feed de identidad

Un feed de identidad rastrea eventos interactivos de inicio de sesión del sistema operativo Windows. Los feeds de identidad no rastrean eventos interactivos de cierre de sesión.

Para que un feed de identidad procese eventos y los etiquete, los eventos deben recopilarse mediante un módulo de recopilación de registros de Windows, en el cual se configura una controladora de dominio/controladora no de dominio activa. Tenga en cuenta que los feeds de identidad solo pueden procesarse mediante un procesador de eventos de feed de identidad.

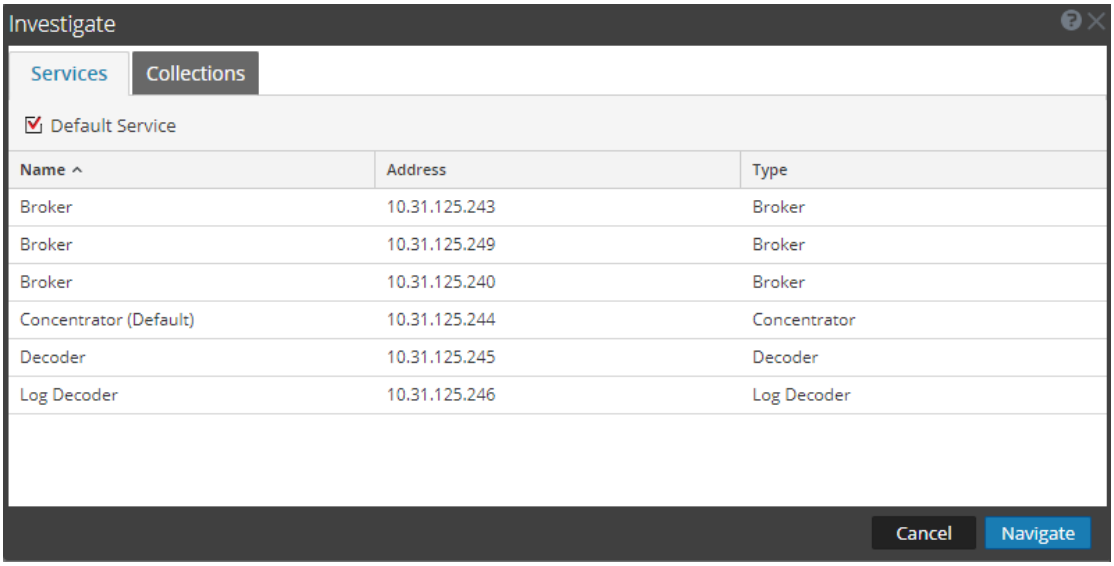
**Nota:** Un feed de identidad solo rastrea un registro a la vez. Si dos usuarios inician sesión en un sistema al mismo tiempo, el segundo usuario sobrescribe los datos del primer usuario en el feed de identidad.

Una vez que haya creado un feed de identidad, puede ver los resultados mediante una investigación del feed.

#### Para investigar una feed de identidad configurado:

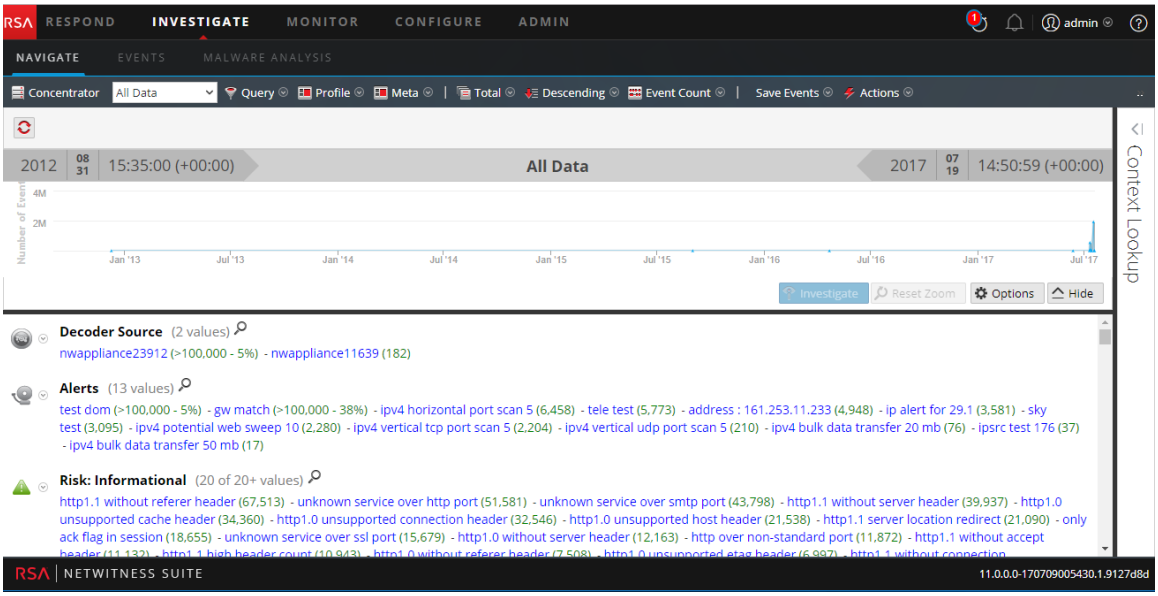
1. Vaya a **INVESTIGATE > Navegar**.

   Si no se selecciona ningún servicio predeterminado, se muestra el cuadro de diálogo Investigate.




2. Seleccione un servicio, generalmente Concentrator, y haga clic en **Navegar**.
3. Seleccione **Cargar valores** para recuperar los metadatos.

En el panel Valores, desplácese hacia abajo para buscar las claves de metadatos que se muestran en la siguiente ilustración.




El feed de identidad proporciona información de los Decoders y los Log Decoders seleccionados. Asocia los datos de IP del host desde el sistema operativo Windows con el usuario que inicia sesión en ese host para etiquetar todos los registros asociados con esa dirección IP e Investigate.

## Editar un feed

En este tema se proporcionan instrucciones para editar un feed personalizado mediante el asistente Feed personalizado.

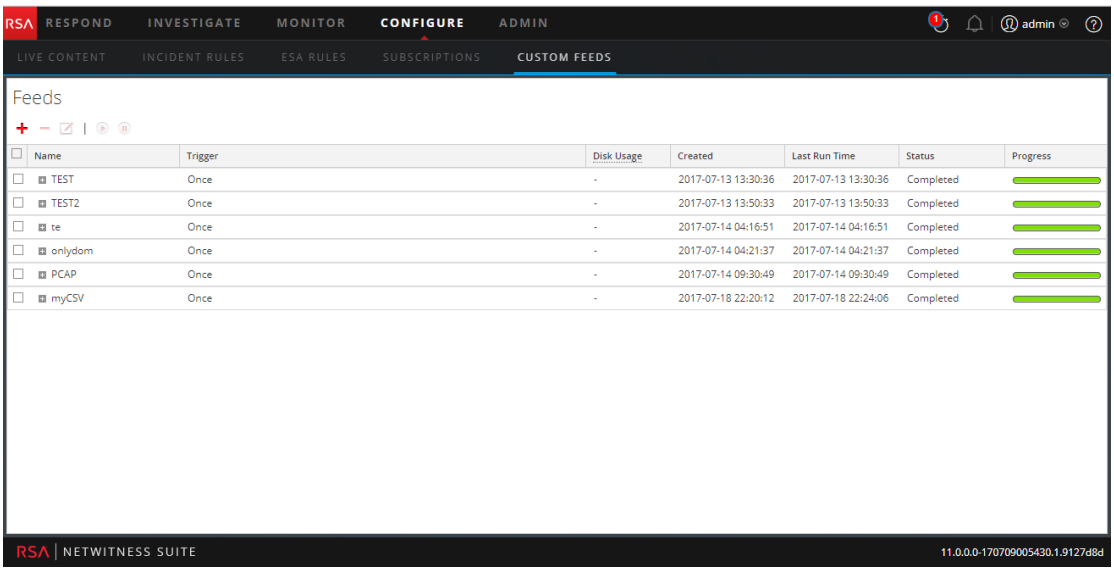
Si se realiza este procedimiento, se logrará:

- La apertura de un feed personalizado existente.
- La descarga o la edición del feed (formato **.zip**) o del archivo que se usó para crear el feed (**.csv** o **.xml**).
- La nueva creación del feed con el archivo actualizado y las nuevas especificaciones del feed.

### Para editar un feed existente:

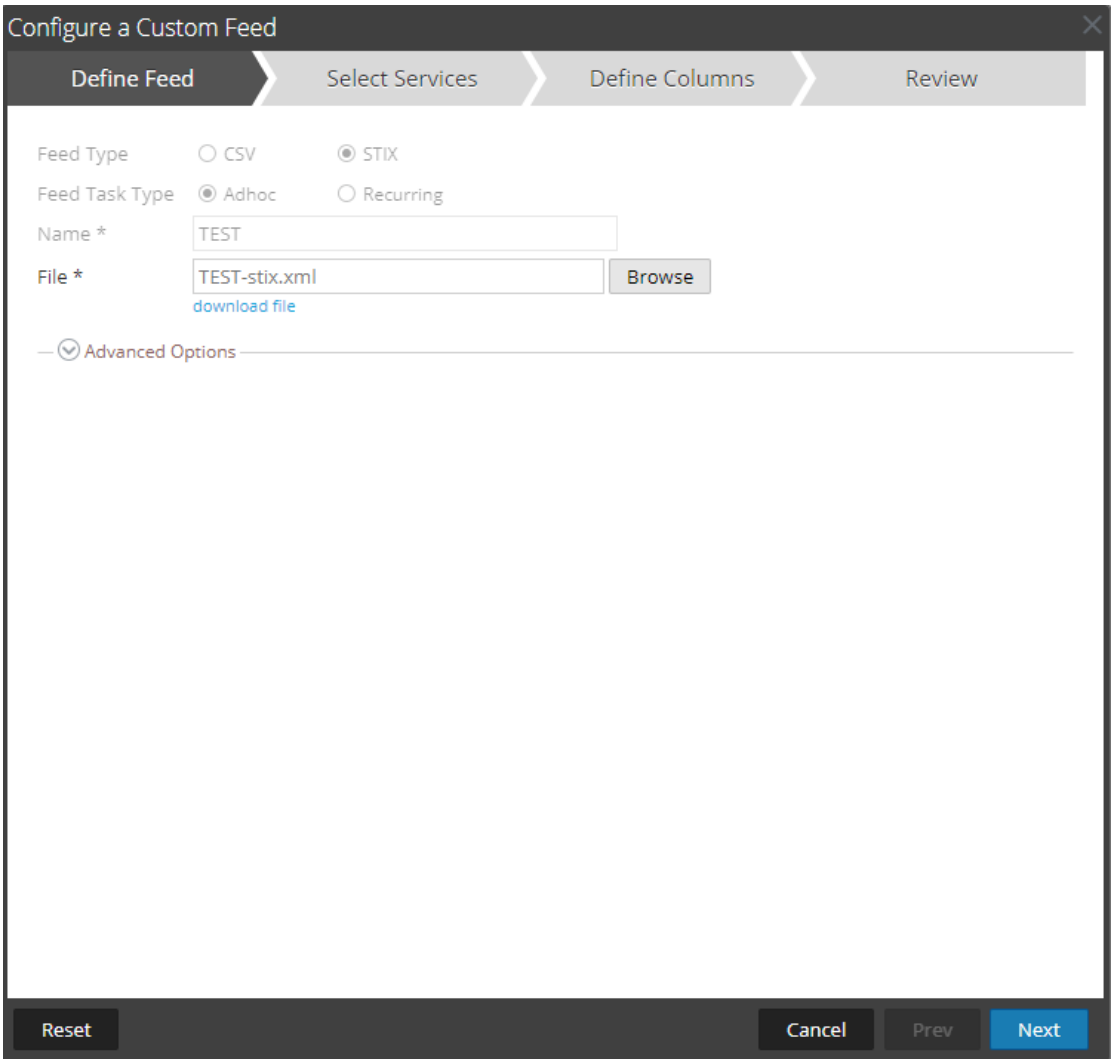
1. Vaya a **CONFIGURAR > FEEDS PERSONALIZADOS**.

   Se muestra la vista Feeds personalizados.




2. En la barra de herramientas, seleccione un feed y haga clic en .

   Se abre el panel Configurar feed personalizado o Configurar feed de identidad en el asistente Feed personalizado.




3. Si desea editar el archivo de feed:
   a. Haga clic en **Descargar archivo**.

      En el caso de un feed de identidad, se descarga el archivo .zip. En el caso de los feeds personalizados, se descarga el archivo .csv o .xml en el sistema de archivos local.

   b. Edite y guarde el archivo.

   c. En la pestaña **Definir feed**, busque y abra el archivo editado.
4. Edite cualquier otro parámetro en las pestañas **Definir feed**, **Seleccionar servicios** y **Definir columnas** que se aplique al tipo de feed.
5. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:
   - Hacer clic en **Cancelar** para cerrar el asistente sin guardar los cambios.
   - Hacer clic en **Restablecer** para borrar los datos del asistente.

- Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).
- Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario).

6. En la pestaña **Revisión**, revise la información del feed y, si los datos son correctos, haga clic en **Finalizar**.

El feed se agrega a la lista de feeds y la barra de progreso muestra la finalización de la tarea. Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, y el feed y el archivo de token correspondiente aparecen en la lista Feeds. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles se ejecutaron correctamente.

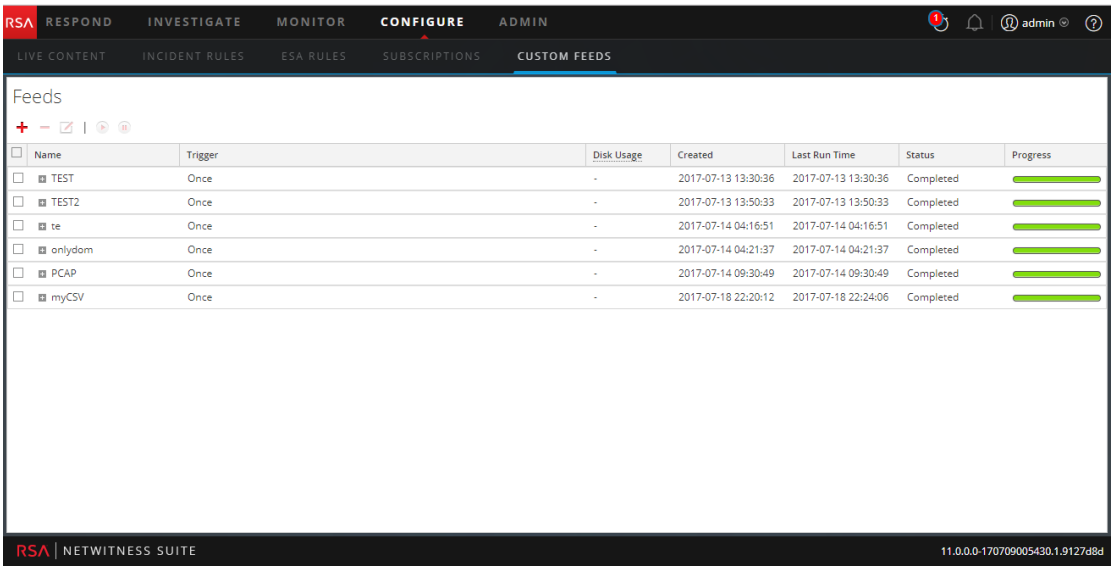
## Quitar un feed

En este tema se proporcionan instrucciones para quitar un feed.

### Para eliminar un feed:

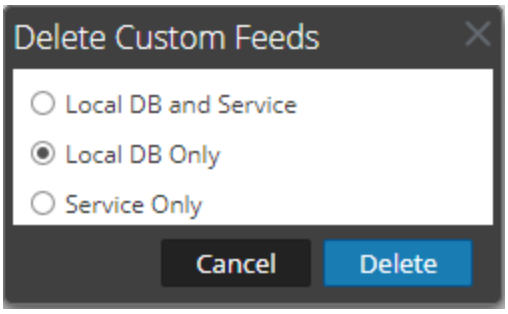
1. Vaya a **CONFIGURAR > FEEDS PERSONALIZADOS**.

   Se muestra la vista Feeds personalizados.




2. En la barra de herramientas, seleccione un feed y haga clic en .

   Se muestra el cuadro de diálogo Eliminar feeds personalizados.




Puede seleccionar una de las siguientes opciones para eliminar el feed:

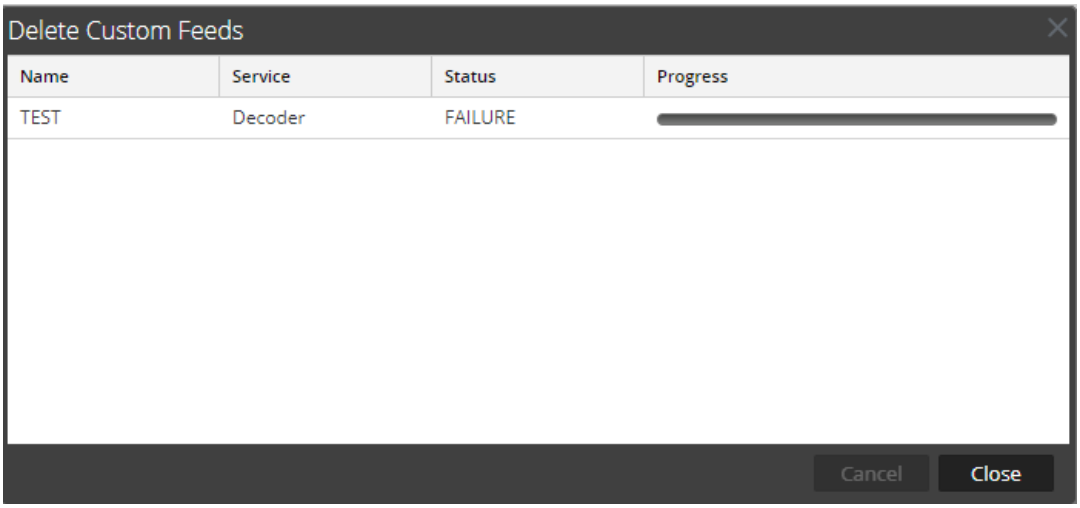
- Si opta por eliminar el feed desde **Base de datos local y servicio**, este se elimina del servicio y de la computadora local de NetWitness Suite. El feed eliminado ya no se verá en la interfaz del usuario de NetWitness Suite.
- Si opta por eliminar el feed desde **Solo base de datos local**, este se elimina de la computadora local de NetWitness Suite. El feed eliminado no se verá en la interfaz del usuario de NetWitness Suite; sin embargo, la última versión implementada de los feeds estará presente en el servicio. Los feeds no implementados se eliminarán permanentemente.
- Si opta por eliminar el feed desde **Solo servicio**, el feed se elimina del servicio. El feed eliminado aparecerá en la interfaz del usuario de NetWitness Suite y se puede implementar nuevamente

3. Seleccione dónde desea eliminar el feed y haga clic en **Eliminar**.

   Se muestra un cuadro de diálogo de advertencia.

4. Haga clic en **sí** para confirmar que desea eliminar el feed desde las áreas seleccionadas.
   - Si escoge eliminar el feed desde **Solo base de datos local**, el feed se elimina.
   - Si decide eliminar el feed desde **Base de datos local y servicio** o **Solo servicio**, se muestra la vista Eliminar feeds personalizados, donde aparece el progreso de la

eliminación del servicio.



# Procedimientos varios de los servicios de Live

Este sección contiene los siguientes procedimientos:

- Agregar recursos suscritos para implementación en los servicios
- Crear un paquete de recursos
- Eliminar una suscripción
- Mostrar detalles de un recurso en la vista Recurso de Live
- Descargar un recurso
- Localizar y quitar un recurso implementado desde servicios
- Quitar recursos suscritos de la cuadrícula Suscripciones de implementaciones
- Mostrar los resultados como una lista o en detalle
- Suscribirse y cancelar la suscripción a un recurso
- Ver detalles del recurso
- Ver los recursos suscritos seleccionados para implementación en los servicios

## Agregar recursos suscritos para implementación en los servicios

1. Navegue a **CONFIGURAR > SUSCRIPCIONES > PESTAÑA IMPLEMENTACIONES**.
2. En el panel **Grupos**, seleccione un grupo.

   Los recursos suscritos, si los hay, se muestran en la pestaña Implementaciones del panel Suscripciones.
3. En el panel **Suscripciones**, haga clic en  .

   Se muestra el cuadro de diálogo Agregar suscripción, el cual muestra las suscripciones disponibles para su implementación.
4. Seleccione los recursos suscritos que desea implementar en el grupo de servicios.
5. Haga clic en **Guardar**.

   El cuadro de diálogo se cierra y las suscripciones se agregan a la lista del panel Suscripciones de la pestaña Implementaciones. Esto coloca al recurso para implementación en la sincronización siguiente.

## Crear un paquete de recursos

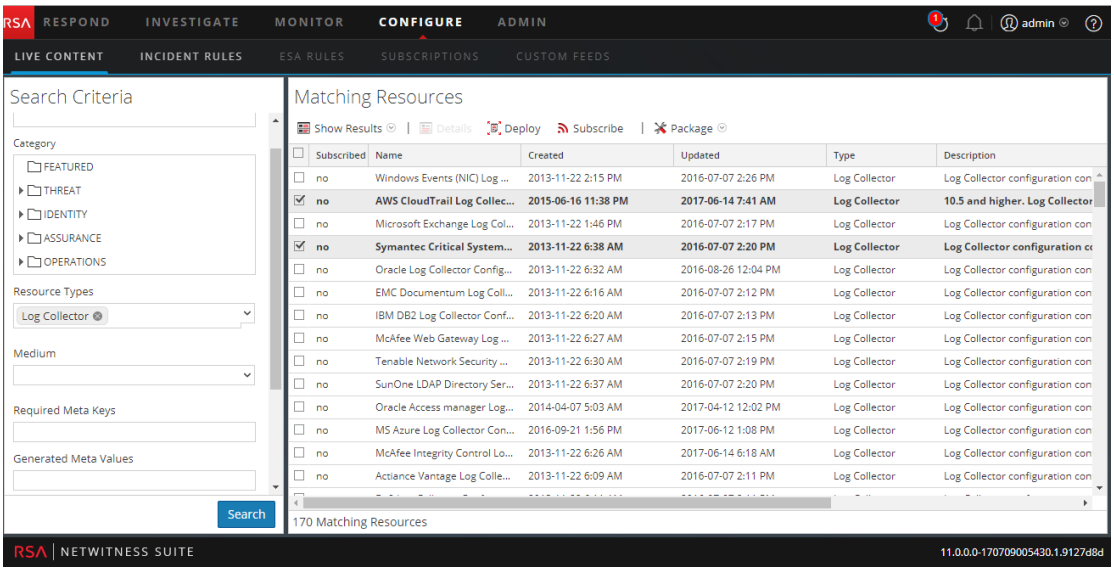
Puede crear un paquete de recursos que puede guardar en un archivo .zip y compartir con otros.

### Requisitos previos

Un requisito previo para la creación de paquetes de recursos es la configuración de la conexión y la sincronización entre el servidor de CMS y NetWitness Suite y la capacidad de buscar recursos en la interfaz del usuario.

### Para crear un paquete de recursos:

1. Seleccione los recursos que desea empaquetar en la cuadrícula Coincidencias de recursos.




2. Seleccione **Paquete** > **Crear** :

   NetWitness Suite crea un archivo **.zip** que contiene los recursos seleccionados y muestra el siguiente cuadro de diálogo, desde el cual puede abrir el archivo .zip o guardarlo en una unidad de red de modo que pueda compartir los recursos del paquete o implementarlos con posterioridad.

   NetWitness Suite da un nombre genérico al paquete. Cámbiele el nombre cuando lo guarde para que identifique los recursos que contiene.

## Eliminar una suscripción

Cuando elimina una suscripción a un recurso, no se eliminan las instancias del recurso implementadas. El recurso implementado permanece en los servicios hasta que se quita explícitamente, pero ya no se sincroniza con el recurso en NetWitness Suite Live.

### Para eliminar una suscripción:

1. Haga clic en la **pestaña Suscripciones**, seleccione las suscripciones que desea eliminar.
2. Haga clic en .

   Un cuadro de diálogo solicita confirmar la intención de eliminar la suscripción.
3. Para confirmar la eliminación, haga clic en **Sí**.

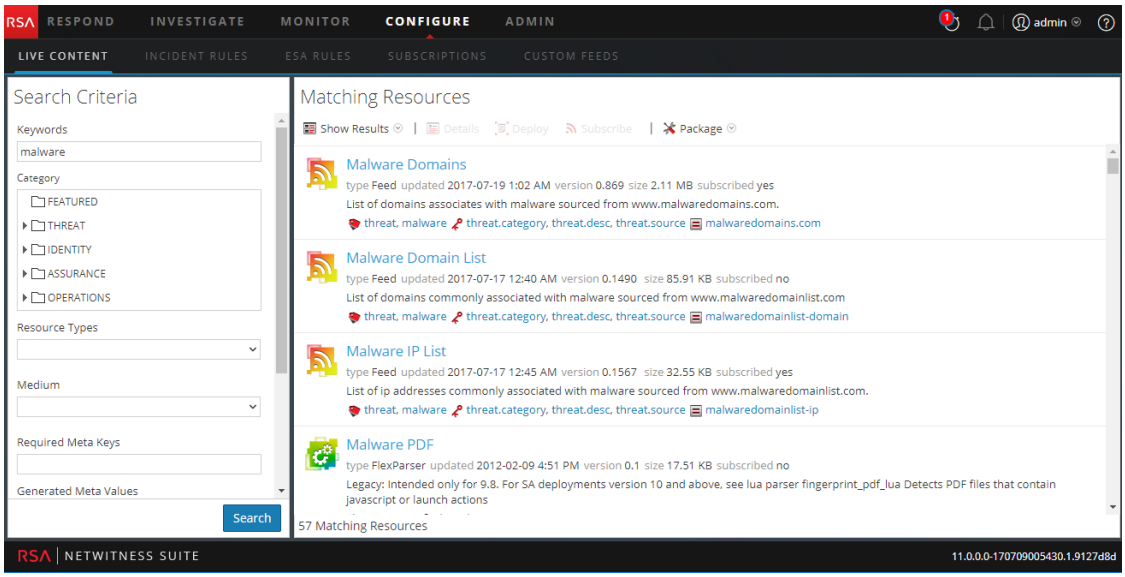
   La suscripción se elimina de la lista de suscripciones, pero todas las instancias implementadas del recurso suscrito permanecen en los servicios.

## Mostrar detalles de un recurso en la vista Recurso de Live

Después de seleccionar un recurso (en la vista Recurso de Live), puede mostrar su información detallada.

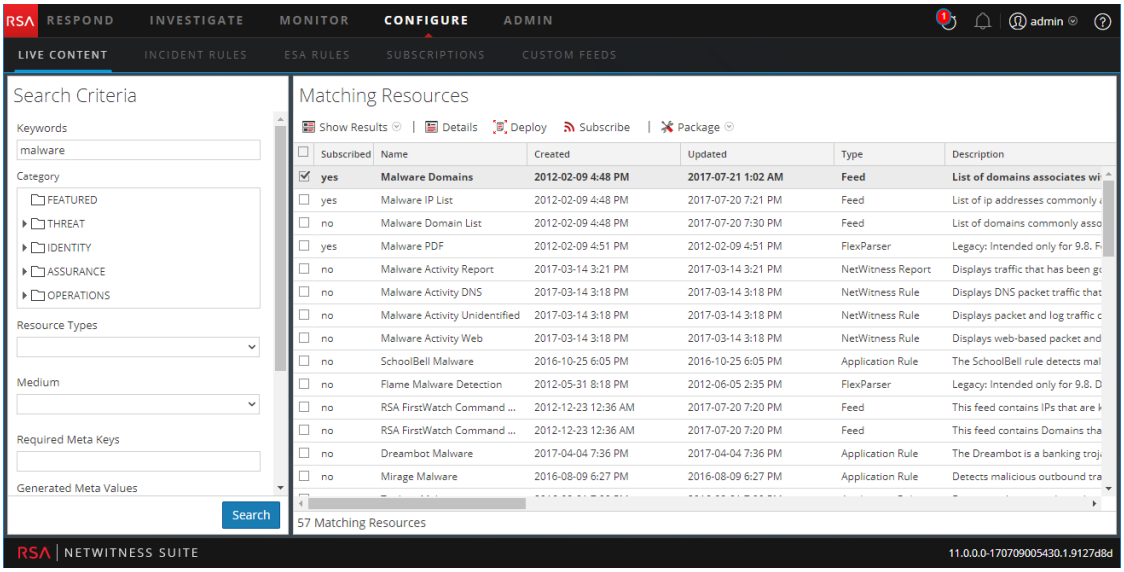
Para abrir una pestaña independiente en la vista Recurso de Live con los detalles del recurso seleccionado, realice una de las siguientes opciones:

- Si ve los **Resultados en detalle**, haga clic en el ícono del tipo de recurso o en el nombre del recurso.




- Si ve los resultados de la lista, haga doble clic en un recurso o seleccione un recurso y haga

clic en **Detalles**.




## Descargar un recurso

Puede descargar un único recurso desde la Vista Recurso de Live.

### Para descargar un recurso:

1. Vaya a **CONFIGURAR > Contenido de Live**.
2. En el panel **Criterios de búsqueda**, ingrese los criterios necesarios para devolver el recurso que desea descargar.
3. Seleccione un único recurso, a continuación, haga clic en Details.
4. Haga clic en Download.

El recurso se guarda como un archivo ZIP en la carpeta local de descargas.

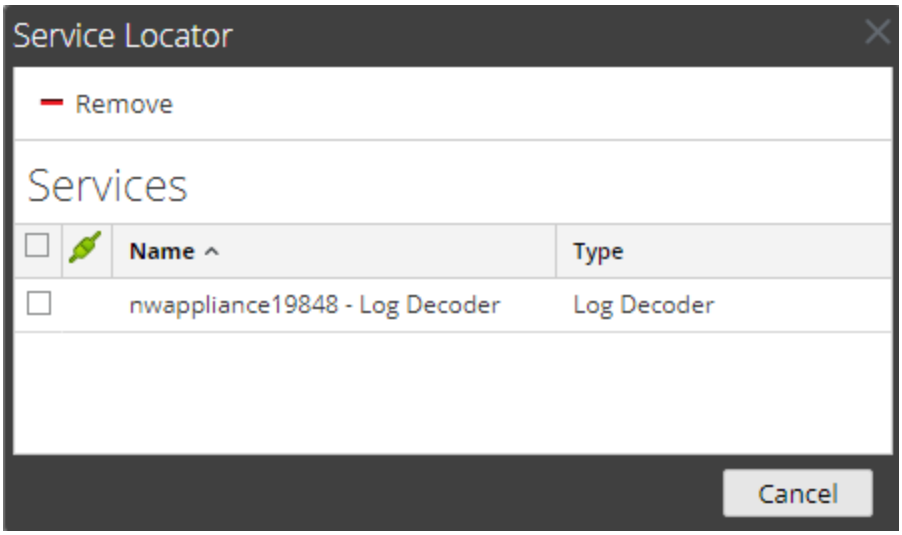
## Localizar y quitar un recurso implementado desde servicios

Puede localizar y quitar un recurso implementado desde servicios en la Vista Recurso de Live.

### Para ver una lista de los servicios en los cuales se implementó un recurso:

1. Con un recurso mostrado en la **vista Recurso**, haga clic en Service Locator .

   Se muestra el cuadro de diálogo Localizador de servicios.




2. Seleccione uno o más servicios en la lista **Servicios**.
3. Haga clic en .

   El recurso se elimina de los servicios seleccionados.

## Quitar recursos suscritos de la cuadrícula Suscripciones de implementaciones

Las suscripciones que se seleccionan para implementación en un grupo de servicios se implementan durante la sincronización. Puede quitar suscripciones de la vista Configuración de Live > pestaña Implementaciones > panel Suscripciones, pero cualquiera que se haya implementado realmente en los servicios permanecerá implementada hasta que alguien la quite.

### Para eliminar recursos del panel Suscripciones de la pestaña Implementaciones:

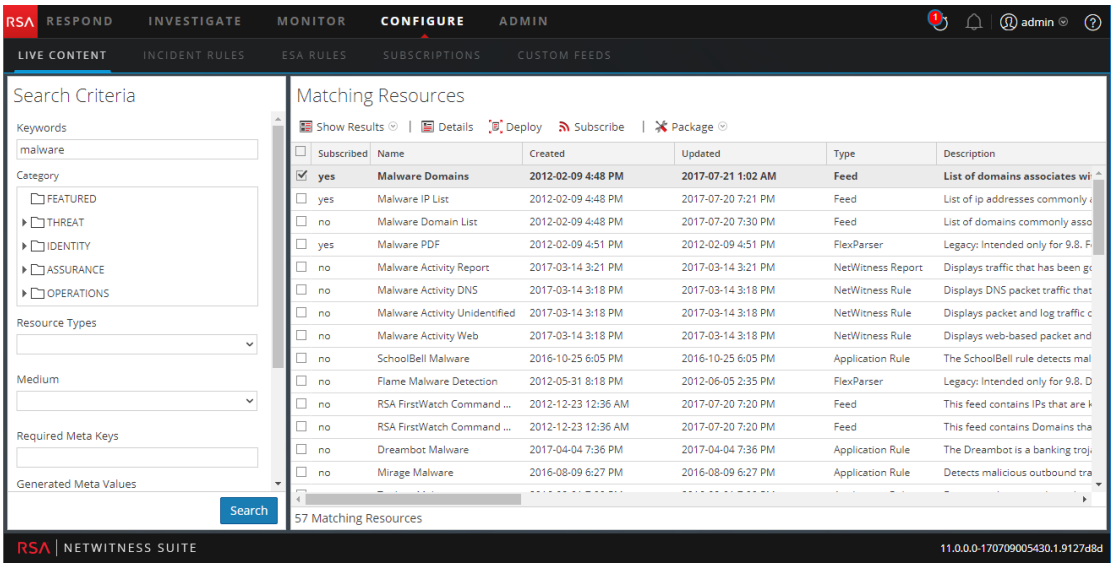
1. En el panel **Grupos**, seleccione un grupo.

   Los recursos suscritos, si los hay, se muestran en el panel Suscripciones.
2. En el panel Suscripciones, haga clic en .

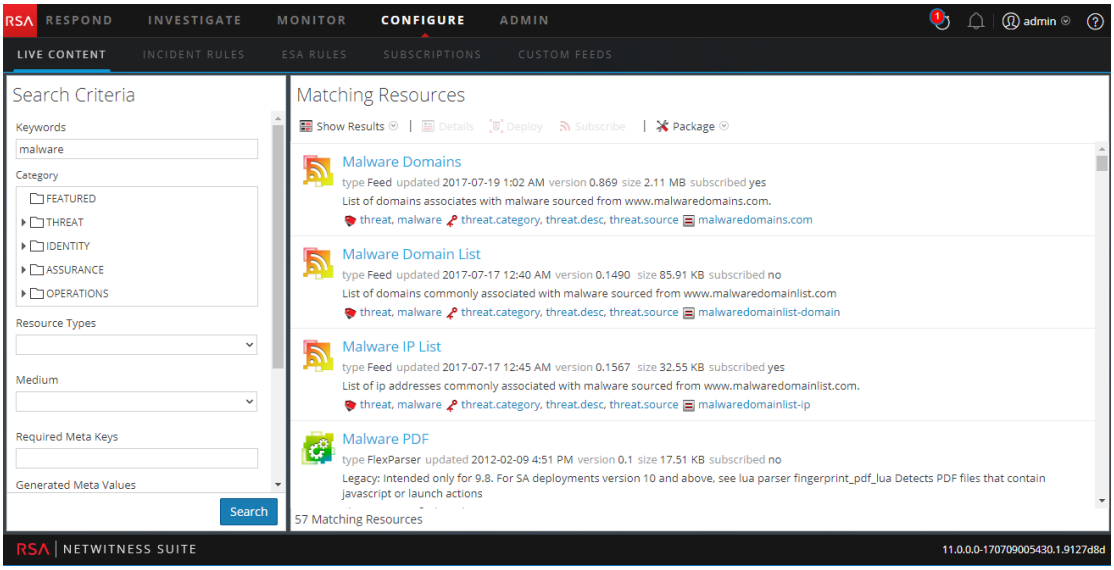
   Un cuadro de diálogo solicita confirmar la intención de eliminar el recurso del grupo de servicios. El recurso se elimina del panel Suscripciones de la pestaña Implementaciones, pero no se elimina de los servicios en los cuales se ha implementado.

## Mostrar los resultados como una lista o en detalle

1. Para cambiar a resultados en cuadrícula cuando se visualizan los resultados en detalle, seleccione **Mostrar resultados > Cuadrícula**.




2. Para cambiar a resultados en detalle cuando se visualizan los resultados en cuadrícula, seleccione **Mostrar resultados > Detalles**.




## Suscribirse y cancelar la suscripción a un recurso

### Suscribirse

Cuando se suscribe a recursos, recibirá una notificación cuando estén disponibles nuevas versiones de los recursos.

### Para suscribirse a un recurso:

1. Navegue a Live > vista Buscar.
2. En el panel **Criterios de búsqueda**, especifique los criterios de búsqueda y haga clic en **Buscar**.
3. Seleccione uno o más recursos y haga clic en Subscribe.

   Se muestra un cuadro de diálogo de confirmación: **Al suscribirse a estos recursos, indica que desea recibir una notificación cuando haya versiones nuevas disponibles.**
4. Para confirmar que desea suscribirse al recurso, haga clic en **Aceptar**.

   El recurso se agrega a las suscripciones administradas en la pestaña Suscripciones y está disponible para implementarse en la pestaña Implementaciones.

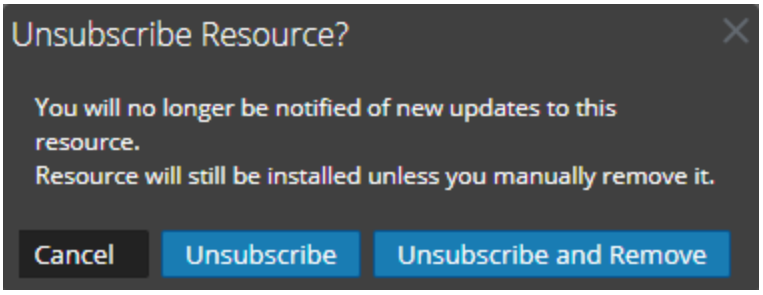
## Cancelar la suscripción

Cuando cancela la suscripción a un recurso, tiene la opción de dejar el recurso en los servicios en los cuales se implementó o eliminarlo de estos servicios.

### Para cancelar la suscripción a un recurso:

1. Con un recurso que se muestre en **SUSCRIPCIONES**, haga clic en Unsubscribe.

   Se muestra un cuadro de diálogo de confirmación.




2. Realice una de las siguientes acciones:
   - Para confirmar que desea cancelar la suscripción al recurso y dejarlo en los servicios donde se ha implementado, haga clic en **Cancelar suscripción**.
   - Para confirmar que desea cancelar la suscripción al recurso y eliminarlo de los servicios en los que se ha implementado, haga clic en **Cancelar la suscripción y eliminar de los servicios**.
   - Para cerrar el cuadro de diálogo sin cancelar la suscripción, haga clic en **Cancelar**.

   Se aplica la acción seleccionada.

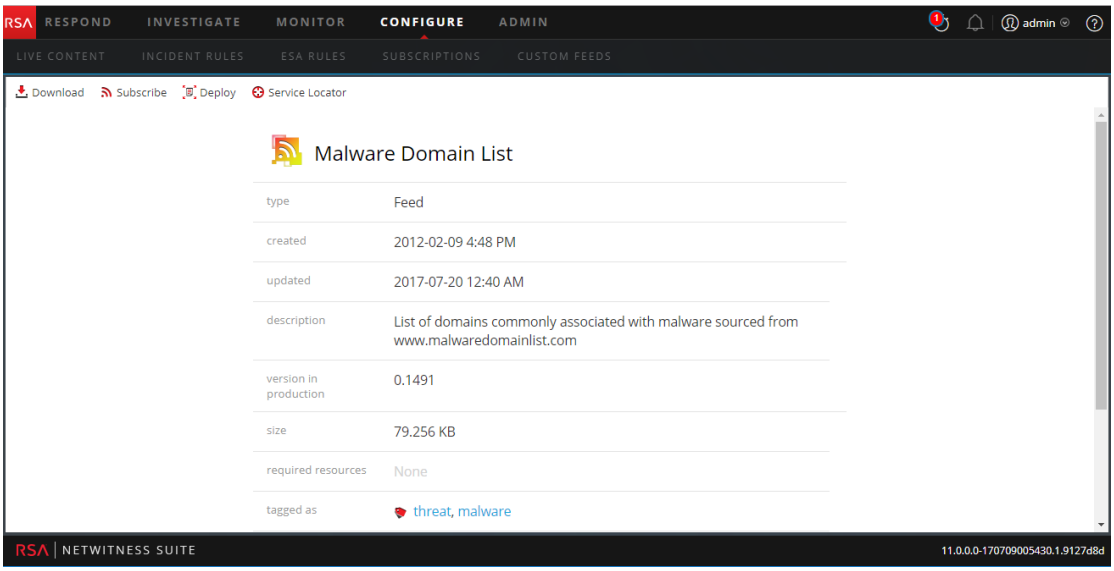
## Ver detalles del recurso

Puede mostrar la información en detalle acerca de un recurso suscrito en la vista Recurso.

### Para ver los detalles:

1. En la pestaña **Suscripciones** , seleccione una suscripción.
2. Haga clic en Details .

   Los detalles del recurso se muestran en la vista Recurso.




## Ver los recursos suscritos seleccionados para implementación en los servicios

En la vista Configurar > pestaña Implementaciones de Live puede ver recursos suscritos que se han seleccionado para su implementación en servicios.

### Para ver los recursos suscritos que se han seleccionado para implementarse en servicios:

En el panel **Grupos**, seleccione un grupo y expándalo para ver los servicios del grupo.

Las suscripciones a recursos seleccionadas para implementación se muestran en la pestaña Implementaciones del panel Suscripciones.

# Solución de problemas

En esta sección se proporcionan instrucciones de solución de problemas que se experimentan cuando se usa el módulo Servicios de Live enNetWitness Suite.

## Solución de problemas OutOfMemoryError en el servidor de Context Hub

En esta sección se proporcionan instrucciones para solucionar problemas cuando encuentra OutOfMemoryError en el servidor de Context Hub y el servicio deja de responder.

Si hay feeds TAXII configurados, Estado y condición genera alertas cuando la memoria en montón disponible del servidor de Context Hub está en un nivel críticamente bajo. Si el servidor de Context Hub está en mal estado debido a la falta de memoria, realice lo siguiente:

1. Asegúrese de que los feeds **Fecha de inicio** estén dentro de 180 días.
2. Compruebe si algún feed TAXII consume demasiado espacio en disco. Un feed TAXII puede consumir un máximo de 300 MB. Si consume más espacio en disco, debe reducir el valor en el campo **Quitar datos de STIX más antiguos que** en **Opciones avanzadas** en el **Asistente de creación de feed personalizado** cuando edita un feed TAXII.

**Nota:** Si el problema persiste, se debe ejecutar el paso 3.

3. Para disminuir la cantidad de subprocesos paralelos disponibles para el procesamiento de STIX, realice lo siguiente:
    a. Vaya a **ADMIN** > **Servicios** > **servicio de Context Hub** > **Ver** > **Explorar**.
    b. En el panel de árbol, navegue a **enrichment/stix/config**.
    c. En el panel derecho, configure en 2 el valor del campo **stix-query-scheduler-pool-size**. El valor predeterminado es 5. Esta configuración controla la cantidad de subprocesos que pueden procesar consultas de datos STIX al mismo tiempo.
    d. Configure en 2 el valor del campo **taxii-poll-scheduler-pool-size**. El valor predeterminado es 5. Esta configuración controla la cantidad de subprocesos que pueden sondear servidores de TAXII al mismo tiempo.
    e. Reinicie el servidor de Context Hub.

# Referencias

Este tema es un conjunto de referencias que describen la interfaz del usuario e información más detallada sobre cómo funciona Live en NetWitness Suite. Estos temas se presentan en orden alfabético.

- Pestaña Implementaciones
- Pestaña Recursos suspendidos
- Vista Configuración de Live
- Vista Feeds de Live
- Vista Recurso de Live
- Vista Buscar en Live
- Comentarios y uso compartido de datos de NetWitness Suite
- Asistente Implementación de paquete de recursos
- Portal de registro de RSA Live
- Pestaña Suscripciones

## Vista Configuración de Live

En la vista Configurar de Live, NetWitness Suite proporciona herramientas integradas para administrar recursos de Live. Puede administrar las suscripciones a recursos, las implementaciones en servicios y los recursos suspendidos. La función necesaria para acceder a esta vista es **Configurar recursos de Live**. Para obtener una descripción general de cómo utilizar las distintas vistas en NetWitness Suite Live, lea Administración de servicios de Live.

Para acceder a esta vista, vaya a **CONFIGURAR > Suscripciones**. Esta vista incluye las siguientes pestañas:

- Pestaña Implementaciones
- Pestaña Suscripciones
- Pestaña Recursos suspendidos

### Pestaña Implementaciones

La pestaña Implementaciones proporciona una interfaz del usuario en la vista Configurar de Live para:

- Ver los recursos suscritos que están seleccionados para implementarse en los servicios de un grupo de servicios.
- Seleccionar los recursos suscritos para su implementación en los servicios de un grupo de servicios.
- Eliminar los recursos que están seleccionados para implementarse en los servicios de un grupo de servicios.

Los recursos que se muestran aquí no se implementan de inmediato después de la adición a un grupo de servicios. En vez de eso, los recursos suscritos se migran a los servicios cuando NetWitness Suite se sincroniza con RSANetWitness Suite Live. El calendario de sincronización se configura en el panel Configuración de Live. Si no desea esperar hasta la sincronización programada, también puede indicar a NetWitness Suite que se sincronice en el momento, en el panel Configuración de Live.

De igual manera, los recursos eliminados en el panel Implementaciones no se eliminan del servicio en el cual se implementaron. Para eliminar recursos de los servicios, elimínelos en la vista Recurso de Live.

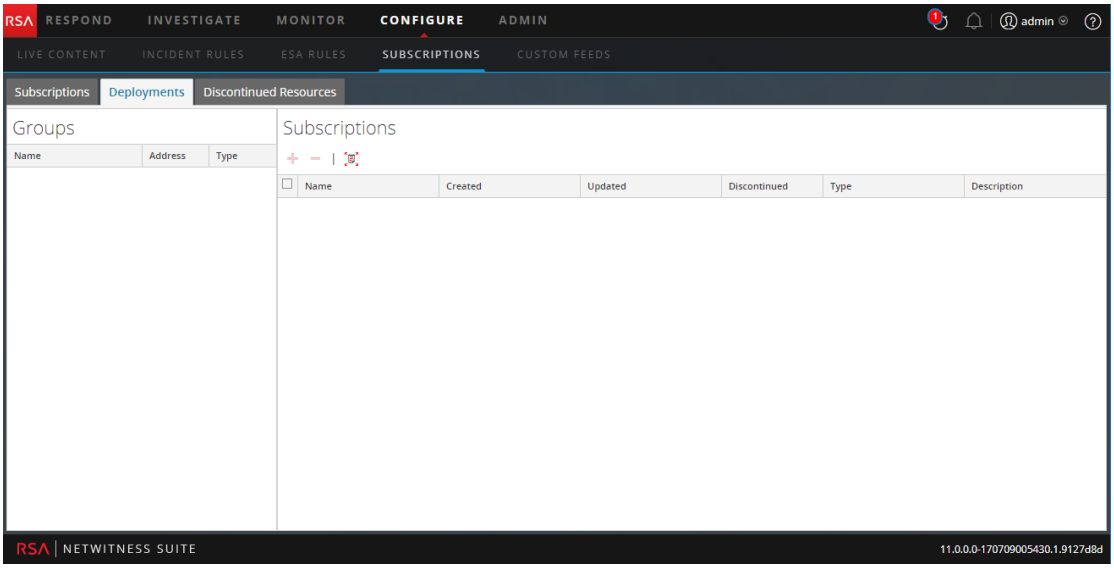
El permiso necesario para acceder a esta vista es **Administración de recursos de Live**.

### Para acceder a esta vista:

1. Vaya a **CONFIGURAR > Suscripciones**.

   La pestaña **Suscripciones** está abierta de manera predeterminada.

2. Haga clic en la pestaña **Implementaciones**.




La pestaña Implementaciones tiene dos paneles: **Grupos** y **Suscripciones**.

### Panel Grupos

El panel Grupos es una pantalla estática de los grupos de servicios configurados que se crearon en la vista Servicios de Administration. Cuando se selecciona un grupo en el panel Grupos, se completa el panel Suscripciones con una lista de las suscripciones seleccionadas para implementación en los servicios del grupo de servicios.

| Función | Descripción |
|---|---|
| **Nombre** | Este es el nombre del grupo de servicios. Cuando se hace clic en el signo más se muestra una lista anidada de los servicio del grupo. |
| **Dirección** | Esta es la dirección IP de cada servicio del grupo. |
| **Tipo** | Este es el tipo de servicio. |

### Panel Suscripciones

En la siguiente tabla se describen las funciones del panel Suscripciones.

| Función | Descripción |
|---|---|
|  | Haga clic en  para abrir un cuadro de diálogo que muestra las suscripciones que se agregaron en las vistas Buscar o Recurso de Live y que están disponibles para implementación. |
|  | Haga clic en  para eliminar las suscripciones seleccionadas en la lista de implementaciones del grupo de servicios. |
|  | Haga clic en  para sincronizar los recursos con las últimas versiones disponibles en Live. |
| **Nombre** | Este es el nombre del recurso. |
| **Creado** | Esta es la fecha y la hora en que se creó el recurso. |
| **Actualizado** | Esta es la fecha y la hora en que el recurso se actualizó por última vez. |
| **Tipo** | Este es el tipo de recurso. |
| **Descripción** | Esta es una descripción del recurso. |

## Pestaña Suscripciones

Las suscripciones son los recursos de NetWitness Suite Live a los cuales se inscribió en la vista Buscar en Live o la vista Recurso de Live. Cuando se suscribió a un recurso, aceptó recibir actualizaciones de RSA NetWitness Suite Live de manera habitual. Las opciones seleccionadas en el panel Configuración de Live determinan la frecuencia con la que ocurre la sincronización y si recibe notificaciones por correo electrónico de las actualizaciones. Además, si no desea esperar hasta la próxima actualización, puede forzar una sincronización inmediata.

La pestaña Suscripciones proporciona una forma de administrar suscripciones. Cada recurso en los cuales NetWitness Suite está suscrito se muestra en esta pestaña.

En la pestaña Suscripciones, puede:

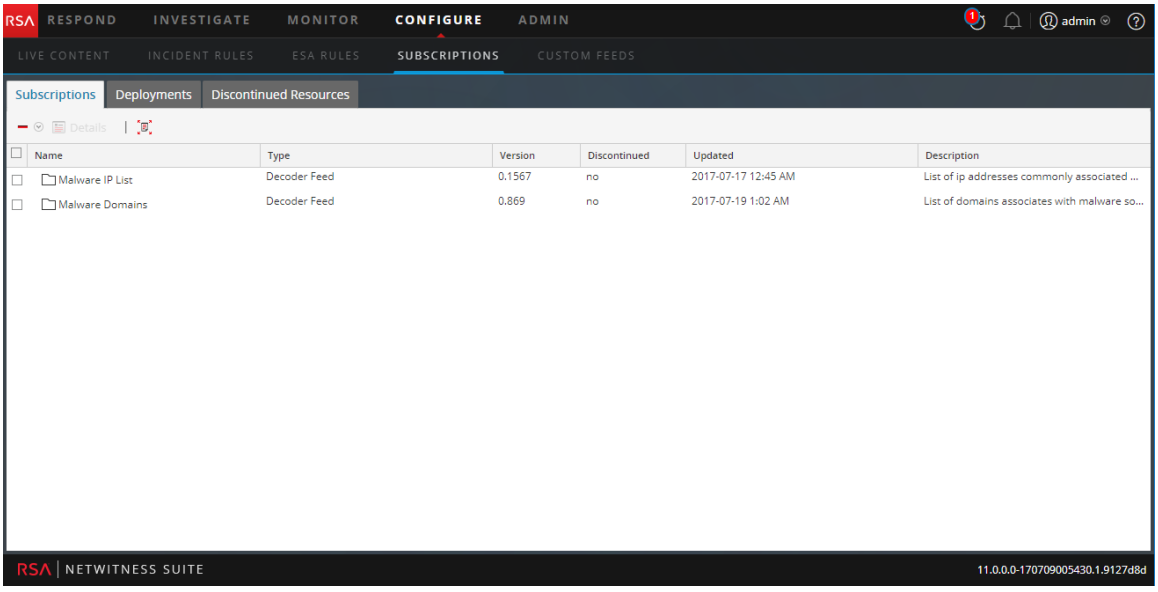
- Ver todos los recursos a los cuales está suscrita esta instancia de NetWitness Suite.
- Abrir una vista detallada de una suscripción en la vista Recurso de Live.
- Eliminar una suscripción.

**Nota:** La suscripción a un recurso no implementa el recurso en ningún servicio. Para implementar uno o más recursos suscritos, vaya a la pestaña Implementaciones. Para implementar un único recurso manualmente, use la opción Implementar en la vista Recurso.

El permiso necesario para acceder a esta vista es **Administración de recursos de Live**.

Para acceder a esta vista, en el menú de menú principal, seleccione **CONFIGURAR > Suscripciones**.

La pestaña Suscripciones está abierta de manera predeterminada.




La pestaña **Suscripciones** tiene una barra de herramientas y una cuadrícula.

### Barra de herramientas

En esta tabla se describen las opciones disponibles en la barra de herramientas.

| Función | Descripción |
|---|---|
|  | Elimina las suscripciones seleccionadas. |
|  | Muestra los detalles de un único recurso suscrito en la vista Recurso. |
|  | Buscar los recursos suspendidos más recientes en el servidor de Live. |

### Cuadrícula

| Columna | Descripción |
|---|---|
|  | Selecciona los recursos suscritos para verlos en detalle o eliminarlos. Puede ver los detalles de un único recurso. Puede eliminar uno o más recursos de los recursos suscritos y cancelar la suscripción a ellos. |
| **Nombre** | Este es el nombre del recurso suscrito. |
| **Tipo** | Este es el tipo de recurso suscrito. |
| **Versión** | Esta es la versión del recurso suscrito. |
| **Suspendido** | Indica el estado de los recursos suspendidos para el recurso suscrito.<br>**Sí**: El recurso está suspendido.<br>**No**: El recurso no está suspendido.<br>**--**: El servidor de Live no está seleccionado para los recursos suspendidos. |
| **Actualizado** | Esta es la fecha y la hora en que el recurso suscrito se actualizó por última vez. |
| **Descripción** | Esta es una descripción del recurso suscrito. |

## Pestaña Recursos suspendidos

En este tema se presentan las funciones de la **vista Configurar de Live > pestaña Recursos suspendidos**.

La pestaña Recursos suspendidos proporciona una interfaz del usuario en la vista Configurar de Live para:

- Escanear los servicios en busca de recursos suspendidos.
- Quitar los recursos suspendidos de cualquier servicio o grupo de servicios.

El permiso necesario para acceder a esta vista es **Administración de recursos de Live**.

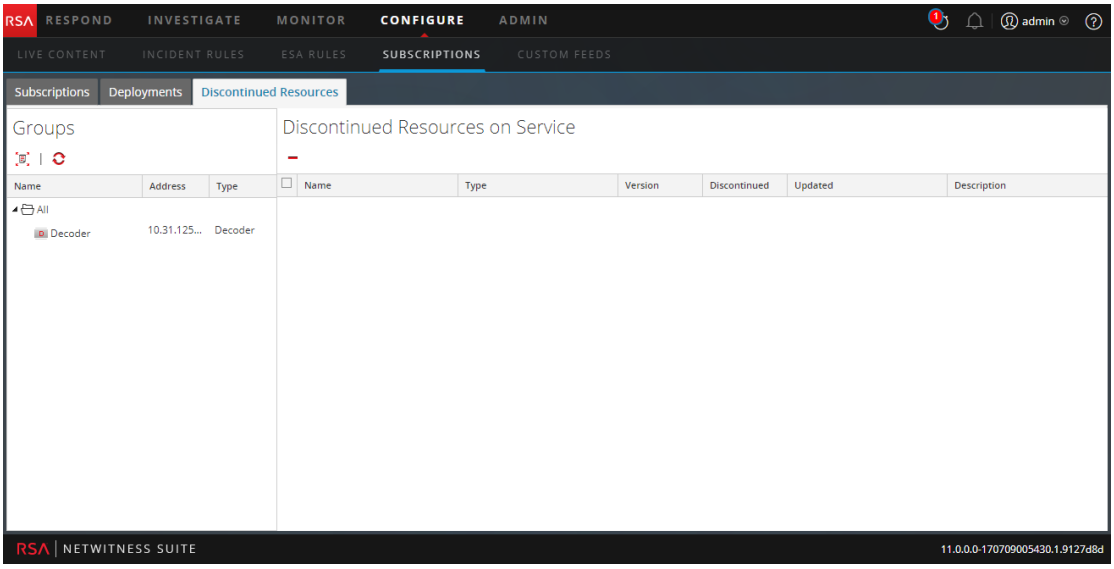
### Para acceder a esta vista:

1. Vaya a **CONFIGURAR > Suscripciones**.

   La pestaña **Suscripciones** está abierta de manera predeterminada.

2. Haga clic en la pestaña **Recursos suspendidos**.

   Este es un ejemplo de la pestaña Recursos suspendidos.




La pestaña Suspendido tiene dos paneles: Grupos y Recursos suspendidos en el servicio.

#### Panel Grupos

El panel Grupos es una pantalla estática de los grupos de servicios configurados que se crearon en la vista Servicios de Admin. Si se selecciona un grupo en el panel Grupos, el panel Recursos suspendidos se completa con una lista de recursos suspendidos, los cuales están implementados en el servicio o el grupo de servicios seleccionados.

| Función | Descripción |
|---|---|
|  | Haga clic en  para escanear los servicios en busca de un recurso suspendido. |

| Función | Descripción |
|---|---|
|  | Muestra el estado actual de los recursos suspendidos en un servicio.<br>**Nota:** El estado de un servicio puede cambiar mientras se escanean los servicios. |
| **Nombre** | Este es el nombre del grupo de servicios. Cuando se hace clic en el signo más se muestra una lista anidada de los servicio del grupo. |
| **Dirección** | Esta es la dirección IP de cada servicio del grupo. |
| **Tipo** | Este es el tipo de servicio. |

#### Recursos suspendidos en el panel Servicio

En la siguiente tabla se describen las funciones relacionadas con los Recursos suspendidos en el panel Servicio.

| Función | Descripción |
|---|---|
|  | Haga clic en  para eliminar los recursos seleccionados del servicio o el grupo de servicios. |
| **Nombre** | Este es el nombre del recurso. |
| **Tipo** | Este es el tipo de recurso. |
| **Versión** | Versión del recurso suspendido. |
| **Suspendido** | Indica el estado de los recursos suspendidos para el recurso suscrito.<br>**Sí**: El recurso está suspendido.<br>**No**: El recurso no está suspendido.<br>**--**: El servidor de Live no está seleccionado para los recursos suspendidos. |
| **Actualizado** | Esta es la fecha y la hora en que el recurso se actualizó por última vez. |
| **Descripción** | Esta es una descripción del recurso. |

## Vista Feeds de Live

Use la vista Feeds de Live para:

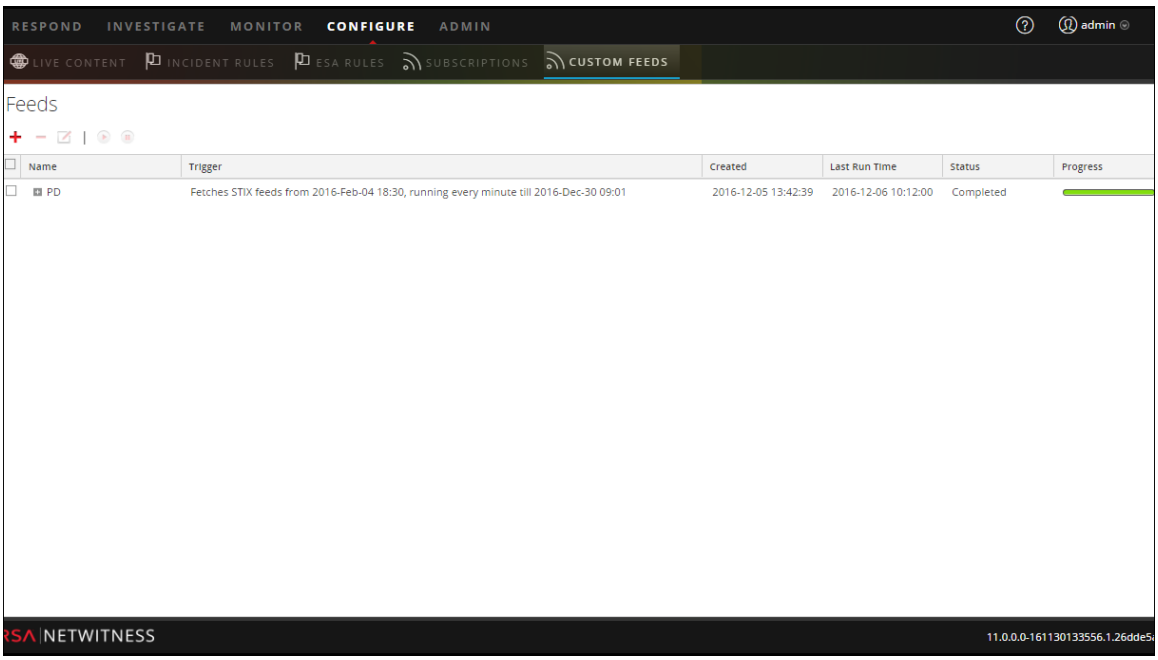
- Crear feeds personalizados.
- Crear feeds de identidad.
- Editar feeds.

La función necesaria para obtener acceso a esta vista es **Administrar dispositivos**.

Para tener acceso a esta vista, realice una de las opciones siguientes:

- En menú principal, seleccione **Live > Feeds.**
- Desde cualquier vista del módulo Live, seleccione **Feeds** en el menú principal.

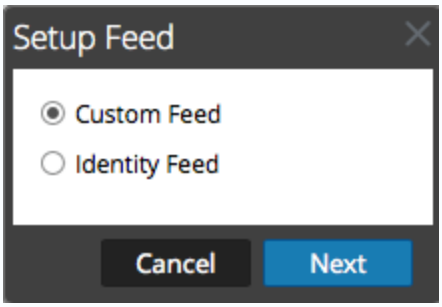
Este es un ejemplo de la vista Feeds.




La pestaña **Feeds** tiene una barra de herramientas y una cuadrícula.

## Barra de herramientas

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

| Función | Descripción |
|---|---|
|  | Inicia la creación de un feed personalizado o de identificación mediante el despliegue del cuadro de diálogo **Configurar feed**.<br>  <br>• El feed personalizado abre el asistente **Configurar un feed personalizado**.<br>• El feed de identidad abre el asistente **Configurar feed de identidad**. |
|  | Elimina el feed que seleccionó. |
|  | Abre el asistente Configurar feed personalizado o Configurar feed de identidad que seleccionó (consulte Editar un feed). |
|  | Iniciar o reanudar un feed de datos. |
|  | Detener o pausar un feed de datos. |

## Cuadrícula Feeds

Esta tabla describe las columnas en la cuadrícula.

| Columna | Descripción |
|---|---|
|  | Selecciona un feed. |
| **Nombre** | Nombre del feed.<br>**Nota:** Ahora puede utilizar caracteres especiales para definir el nombre del feed personalizado. |
| **Desencadenante** | Muestra la frecuencia de ejecución del feed, la cual está determinada por lo que definió en **Tipo de tarea de feed** cuando se creó el feed. |
| **Creado** | Esta es la fecha y la hora en que se creó el feed. |

| Columna | Descripción |
|---|---|
| **Uso de disco** | Muestra el tamaño del almacenamiento de MongoDB que utiliza el feed TAXII. |
| **Hora de última ejecución** | Esta es la fecha y la hora en que el feed se ejecutó por última vez. |
| **Estado** | El estado del feed. |
| **Progreso** | Barra de progreso. |

## Vista Recurso de Live

La vista Recurso de Live muestra una vista detallada de un recurso seleccionado y cuenta con opciones para:

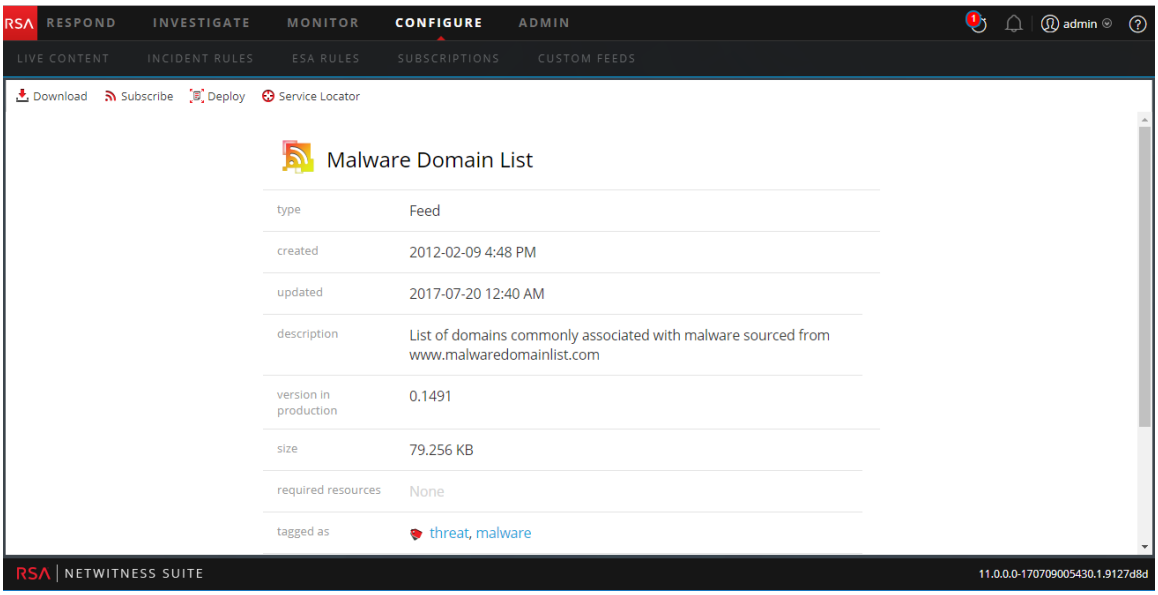
- Descargar el recurso.
- Suscribirse o cancelar la suscripción a un recurso.
- Implementar el recurso en los servicios.
- Encontrar servicios en los cuales se ha implementado el recurso y eliminar el recurso de los servicios.

El permiso necesario para tener acceso a esta vista es Ver detalles de recursos de Live.

Para tener acceso a esta vista, realice una de las opciones siguientes:

1. En el menú principal, seleccione **CONFIGURAR > LIVE CONTENT > Criterios de búsqueda**.
2. En la vista Buscar en Live, **Resultados en detalle**, haga clic en el ícono tipo de recurso o en el nombre del recurso.
3. En la vista Buscar en Live **Recursos en cuadrícula**, haga doble clic en un recurso o seleccione un recurso y haga clic en **Detalles**.

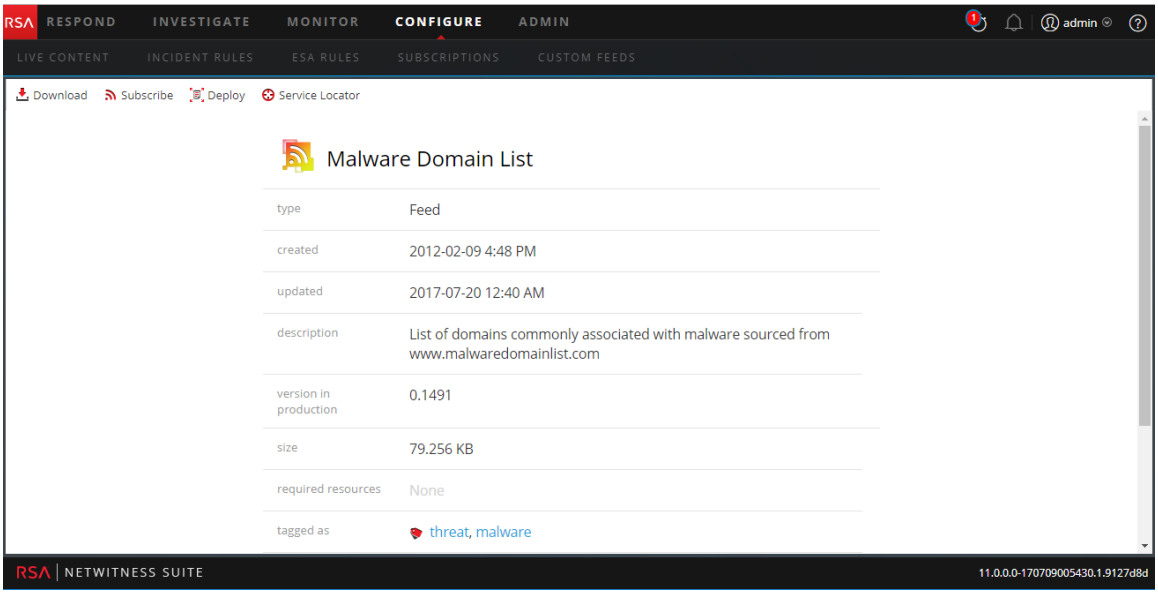
Este es un ejemplo de la vista Recurso.




La vista Recurso de Live tiene una vista detallada de un único recurso y una barra de herramientas.

## Detalles de recursos

Este es un ejemplo de los detalles de recursos que se muestran en la vista Recurso.




En la siguiente tabla se describen los elementos de la sección Detalles de recursos.

| Función | Descripción |
|---|---|
| **Ícono Tipo de recurso** | Una representación gráfica del tipo de recurso, por ejemplo  . |
| **Nombre** | El nombre del recurso, por ejemplo,**fingerprint_office_lua**. |
| **Tipo** | El tipo de recurso, por ejemplo, **RSA Lua Parser**. |
| **Creado** | La fecha en que se creó el recurso; por ejemplo, **2013-09-15 02:16 PM**. |
| **Actualizado** | La fecha en que el recurso se actualizó por última vez; por ejemplo, **2013-09-15 02:16 PM**. |
| **Descripción** | La descripción del recurso, por ejemplo, **Identifica documentos Word, Excel y PowerPoint de Microsoft Office 95, 2007**. |
| **Versión en producción** | La versión del recurso, por ejemplo, **0.1**. |
| **Tamaño** | El tamaño del recurso, por ejemplo, **9,079 KB**. |
| **Recursos requeridos** | Una lista de recursos de los cuales depende este recurso, por ejemplo, **NetWitness Lua Library**. Cuando se hace clic en un recurso, los detalles que se muestran actualmente se remplazan por los detalles del recurso en el que se hizo clic. |
| **Etiquetado como** | Las etiquetas  que se aplican al recurso. En el ejemplo, la etiqueta es **featured, informational**. Cuando se hace clic en una etiqueta, se abre la vista Buscar en Live con la búsqueda restringida para encontrar los recursos que contienen esa etiqueta. |
| **Claves de metadatos requeridas** | Las claves de metadatos  que se aplican al recurso. En el ejemplo, no se requieren claves de metadatos. Cuando se hace clic en una clave de metadatos, se abre la vista Buscar en Live con la búsqueda restringida para encontrar recursos que contienen esa clave de metadatos. |

| Función | Descripción |
|---|---|
| **Genera valores de metadatos** | Los valores de metadatos  que genera el recurso. En el ejemplo, no se generan valores de metadatos. Cuando se hace clic en un valor de metadatos, se abre la vista Buscar en Live con la búsqueda restringida para encontrar recursos que contienen ese valor de metadatos. |
| **Permisos** | Los permisos necesarios para el recurso. |

## Barra de herramientas de la vista Recurso

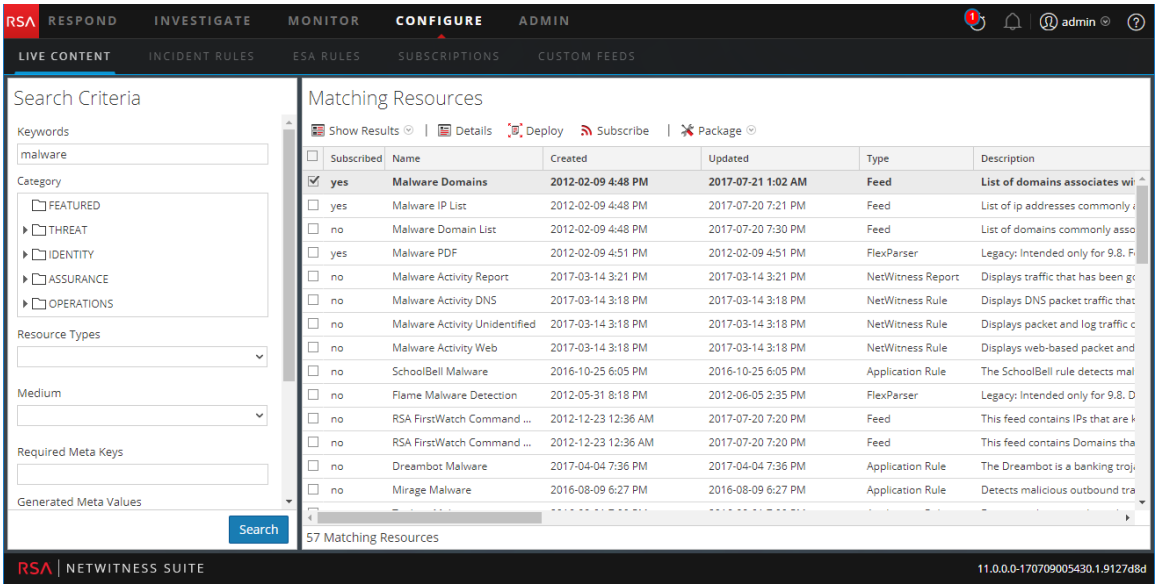
En esta tabla se describen las opciones de la barra de herramientas de la vista Recurso de Live.

| Función | Ícono | Descripción |
|---|---|---|
| Descarga |  | Esta opción descarga el recurso que se muestra actualmente en la vista Recurso. |
| Suscribirse o cancelar suscripción |  | Esta opción suscribe o cancela la suscripción al recurso que se muestra actualmente en la vista Recurso.<br>• Al hacer clic en **Suscribir** se abre un cuadro de diálogo que debe aceptar para recibir una notificación cuando se actualicen los recursos seleccionados. Puede cancelar o hacer clic en **Aceptar**.<br>• Al hacer clic en **Cancelar suscripción** se pide la confirmación de que desea dejar de recibir la notificación de actualización de los recursos seleccionados. A continuación, puede elegir cancelar o puede hacer clic en **Cancelar suscripción** o en **Cancelar la suscripción y eliminar**, lo cual elimina el recurso de los servicios en los cuales se ha implementado. |
| Implementar |  | Esta opción proporciona una manera de implementar el recurso que se muestra actualmente en la vista Recurso. Al hacer clic en **Implementar** se abre el cuadro de diálogo Implementación manual de recursos. |
| Localizador de servicios |  | Esta opción muestra una lista de los servicios en los cuales se ha implementado el recurso que se muestra actualmente. Puede eliminar el recurso de todos los servicios o solo de los servicios seleccionados. |

## Vista Buscar en Live

La vista Buscar en Live proporciona la capacidad para navegar por los recursos del CMS Live configurado. Una vez que se encuentran las coincidencias de recursos, puede ver los detalles, suscribirse a los recursos e implementar los recursos en servicios y grupos de servicios.

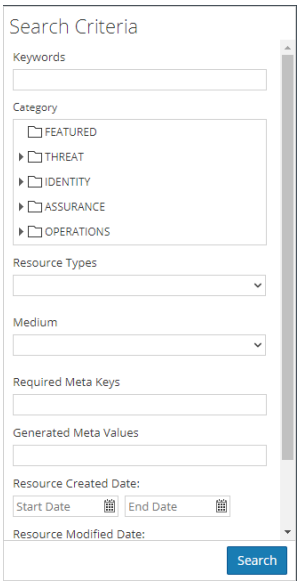
Este es un ejemplo de la vista Buscar.




La vista Buscar en Live tiene un panel para especificar los criterios de búsqueda y un panel que muestra las coincidencias de recursos. El panel Criterios de búsqueda se expande para proporcionar mayor ancho de visualización del panel Coincidencias de recursos.

### Panel Criterios de búsqueda

Este es un ejemplo del panel Criterios de búsqueda.




En la siguiente tabla se proporcionan descripciones de las funciones del panel Criterios de búsqueda.

| Función | Descripción |
|---|---|
| Palabras clave | Ingrese una o más palabras clave para buscar recursos que incluyen estas palabras en su nombre o descripción. Cuando ingresa una palabra clave, puede utilizar comodines. |
| Categoría | Las categorías reflejan el modelo jerárquico de investigación que usa RSA para organizar los recursos. El propósito del modelo de investigación es ofrecer una ruta precisa a la respuesta ante incidentes de seguridad de información. Para obtener más detalles, consulte el tema Modelo de investigación. |

| Función | Descripción |
| --- | --- |
| Tipos de recursos | Seleccione los tipos de recursos en la lista desplegable para filtrar los recursos por tipo. Los valores posibles son:<br>• Analítica avanzada (Warehouse)<br>• Regla de aplicación<br>• Paquete<br>• Regla de correlación<br>• Regla de Event Stream Analysis<br>• Feed<br>• FlexParser<br>• Log Collector<br>• Dispositivo de registro<br>• Analizador Lua<br>• Reglas de malware<br>• Lista de NetWitness<br>• Informe de NetWitness<br>• Regla de NetWitness |
| Medio | Seleccione uno o más medios en la lista desplegable para buscar contenido en función del origen de metadatos.<br>Los valores disponibles para medio son los siguientes:<br>• **registro**: se aplica al contenido que utiliza metadatos derivados de datos de registros<br>• **paquete**: se aplica al contenido que utiliza metadatos derivados de paquetes de red<br>• **paquetes y registros**: se aplica al contenido que correlaciona metadatos derivados a través de datos de paquetes y registros |

| Función | Descripción |
|---|---|
| Etiquetas | Seleccione las etiquetas de metadatos en la lista desplegable para navegar en función del etiquetado de los metadatos. Por ejemplo, para buscar recursos en un Log Decoder, seleccione la etiqueta **netwitness para registros**. Como alternativa, puede hacer clic en una etiqueta en el panel Coincidencias de recursos para insertarla en este campo. |
| Claves de metadatos requeridas | Ingrese una clave de metadatos específica; por ejemplo, **threat.source**. Como alternativa, puede hacer clic en una clave de metadatos en el panel Coincidencias de recursos para insertar esa etiqueta en este campo. |
| Valores de metadatos generados | Ingrese un valor de metadatos generado; por ejemplo, **netwitness**. Como alternativa, puede hacer clic en una clave de metadatos generada en el panel Coincidencias de recursos para insertar esa etiqueta en este campo. |
| Fecha de creación de investigación | Especifique un rango de fechas durante el cual se crearon los recursos. Por ejemplo, para navegar por los recursos que se crearon entre el 1 y el 4 de enero, seleccione 1 de enero como la fecha inicial y 4 de enero como la fecha de finalización. Debe ingresar fechas en formato mm/dd/aaaa o hacer clic en  y elegir fechas de un calendario. |
| Fecha de modificación de investigación | Especifique un rango de fechas durante el cual se modificaron los recursos. Por ejemplo, para navegar por los recursos que se modificaron entre el 1 y el 4 de enero, seleccione 1 de enero como la fecha inicial y 4 de enero como la fecha de finalización. Debe ingresar fechas en formato mm/dd/aaaa o hacer clic en  y elegir fechas de un calendario. |
| Buscar | Haga clic en **Buscar** para enviar la solicitud de búsqueda al servidor de Live. Los criterios de búsqueda más específicos revuelven coincidencias de recursos más rápidamente. |
| Cancelar | Haga clic en **Cancelar** para cancelar la búsqueda en curso. |
| Incluir recursos suspendidos | Seleccione **Incluir recursos suspendidos** para incluir los recursos suspendidos en el resultado de búsqueda. Para obtener una lista actualizada de recursos que se suspendieron, consulte el tema Contenido suspendido. |

## Panel Coincidencias de recursos

El panel Coincidencias de recursos presenta cada recurso según las selecciones realizadas en el panel Criterios de búsqueda. Los resultados se muestran inicialmente en una cuadrícula, pero puede cambiar entre dos opciones para mostrar resultados: en detalle o en cuadrícula.

### Resultados en detalle

En los resultados en detalle, puede hacer clic en una etiqueta, clave de metadatos o valor de metadatos de un recurso para completar automáticamente el panel Criterios de búsqueda y agilizar los resultados de la búsqueda.

En la siguiente tabla se describen los elementos de los resultados detallados.

| Función | Descripción |
|---|---|
| **Ícono Tipo de recurso** | Una representación gráfica del tupo de recurso. Por ejemplo,  . |
| **Nombre** | El nombre del recurso, por ejemplo, **Administración de grupos**.<br>**Nota:** (Suspendido) se muestra junto al nombre del recurso, si se suspende un recurso. |
| **Tipo** | El tipo de recurso, por ejemplo, **Regla**. |
| **Fragmento C** | La fecha en que el recurso se actualizó por última vez, por ejemplo, **2015-09-15 4:27 PM**. |
| **Versión** | La versión del recurso, por ejemplo, **0.1**. |
| **Tamaño** | El tamaño del recurso, por ejemplo, **153 B**. |
| **Subscribed** | Estado de suscripción:<br>• **sí**: Esta instancia de NetWitness Suite está suscrita a este recurso de contenido.<br>• **no**: Esta instancia de NetWitness Suite no se ha suscrito a este recurso de contenido. |
| **Descripción** | La descripción del recurso, por ejemplo, **Administración de grupos-reglas de cumplimiento de normas**. |

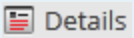
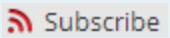
| Función | Descripción |
|---|---|
| **Etiquetas** | Las etiquetas que se aplican al recurso. Cuando se hace clic en una etiqueta, la búsqueda se restringe a los recursos que contienen esa etiqueta. Por ejemplo,  . |
| **Claves de metadatos** | Las claves de metadatos que se aplican al recurso. Cuando se hace clic en una clave de metadatos, la búsqueda se restringe a los recursos que contienen esa clave de metadatos. Por ejemplo,  . |
| **Valores de metadatos de recursos** | Los valores de metadatos que generó el recurso. Cuando se hace clic en un valor de metadatos, la búsqueda se restringe a los recursos que generaron el valor de metadatos. Por ejemplo,  . |

### Resultados en cuadrícula

En la vista de cuadrícula, puede seleccionar uno o más recursos y utilizar las opciones adicionales en la barra de herramientas para ver los detalles de un único recurso, suscribirse a los recursos e implementar recursos.

En la siguiente tabla se describen los elementos de los resultados de la cuadrícula.

| Función | Descripción |
|---|---|
| **Subscribed** | Estado de suscripción:<br>• **sí**: Esta instancia de NetWitness Suite está suscrita a este recurso de contenido.<br>• **no**: Esta instancia de NetWitness Suite no se ha suscrito a este recurso de contenido. |
| **Nombre** | El nombre del recurso, por ejemplo, **Administración de grupos**.<br>**Nota:** El nombre del recurso se muestra de color rojo si está suspendido. |
| **Creado** | La fecha en que se creó el recurso, por ejemplo, **2015-08-12 3:11 PM**. |

| Función | Descripción |
|---|---|
| **Fragmento C** | La fecha en que el recurso se actualizó por última vez, por ejemplo, **2015-09-15 4:27 PM**. |
| **Tipo** | El tipo de recurso, por ejemplo, **Regla**. |
| **Suspendido** | El estado de los recursos suspendidos:<br>**sí**: El recurso que coincide con los criterios de búsqueda está suspendido.<br>**no**: El recurso no está suspendido.<br>**--**: El servidor de Live no está seleccionado para los recursos suspendidos. |
| **Descripción** | La descripción del recurso, por ejemplo, **Administración de grupos-reglas de cumplimiento de normas**. |
| | **Barra de herramientas** |
|  | Este menú ofrece dos formas para ver los resultados de búsqueda: **Detallado** y **Cuadrícula**. |
|  | Esta opción se aplica a un único recurso seleccionado. Al hacer clic en **Detalles** se abre el recurso seleccionado en la vista Recurso de Live. |
|  | Esta opción se aplica a uno o más recursos seleccionados. |
|  | Esta opción se aplica a uno o más recursos seleccionados. Al hacer clic en **Suscribir** se abre un cuadro de diálogo que pide confirmar que desea recibir una notificación cuando se actualicen los recursos seleccionados. |

| Función | Descripción |
|---|---|
| Package | Este menú ofrece dos funciones de creación de paquetes para los recursos seleccionados:<br>• **Crear**: Crea un archivo **resourceBundle.zip** que contiene los recursos seleccionados y abre un cuadro de diálogo en el que puede:<br>  • abrir el archivo, o<br>  • guardar el archivo para su posterior implementación.<br>• **Implementar**: Abre el asistente de implementación, en el cual puede escoger un archivo **resourceBundle.zip** e implementarlo. |

**Consulte también**

- Para obtener más detalles sobre la implementación (Deploy), consulte Buscar e implementar recursos de Live.
- Para obtener más detalles sobre la implementación de un paquete (Package), consulte el Asistente Implementación de paquete de recursos.

## Asistente Implementación de paquete de recursos

Si creó un paquete de recursos y lo guardó en una unidad de red, puede usar el asistente Implementación de paquete de recursos para implementar los recursos manualmente en un servicio o un grupo de servicios sin suscribirse a ellos. NetWitness Suite acepta paquetes en archivos **.nwp** o **.zip**.

La implementación manual de recursos se realiza directamente en los servicios sin aprovechar las eficaces funcionalidades de administración de recursos de NetWitness Suite.

Si desea recibir notificaciones y actualizaciones de los recursos actualizados y poder eliminar fácilmente los recursos de un servicio, debe suscribirse a los recursos en la vista Buscar en Live e implementarlos en la vista **Configurar de Live**.

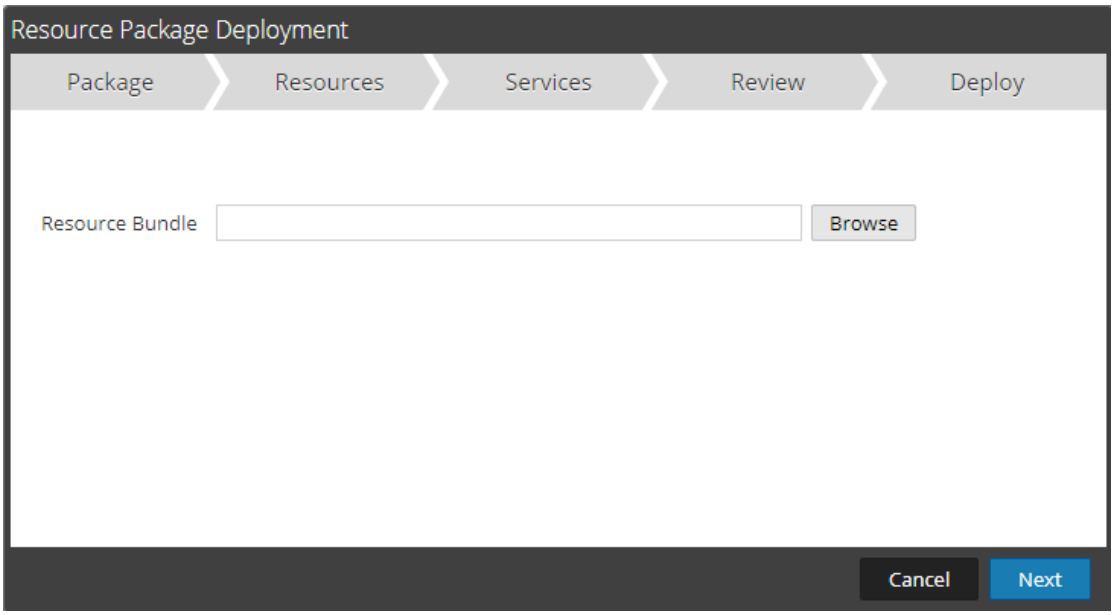
**Nota:** Use NetWitness Suite Live para crear paquetes de recursos; esta es una aplicación distinta que no es parte de NetWitness Suite. Si selecciona **Paquete** > **Crear** en la barra de herramientas **Buscar en Live: Coincidencias de recursos**, se muestra la ventana Herramienta de paquete de contenido. Puede elegir los recursos que desea incluir en un paquete y guardar el paquete como un archivo de paquete de NetWitness Suite.

El permiso necesario para obtener acceso a esta vista es **Implementación de recursos de Live**.

Para acceder a esta vista:

1. En el menú principal, seleccione **CONFIGURAR > LIVE CONTENT**.
2. En la barra de herramientas **Buscar en Live: Coincidencias de recursos**, seleccione **Paquete** > **Implementar**.

   Se muestra el asistente Implementación de paquete de recursos.




## Funciones

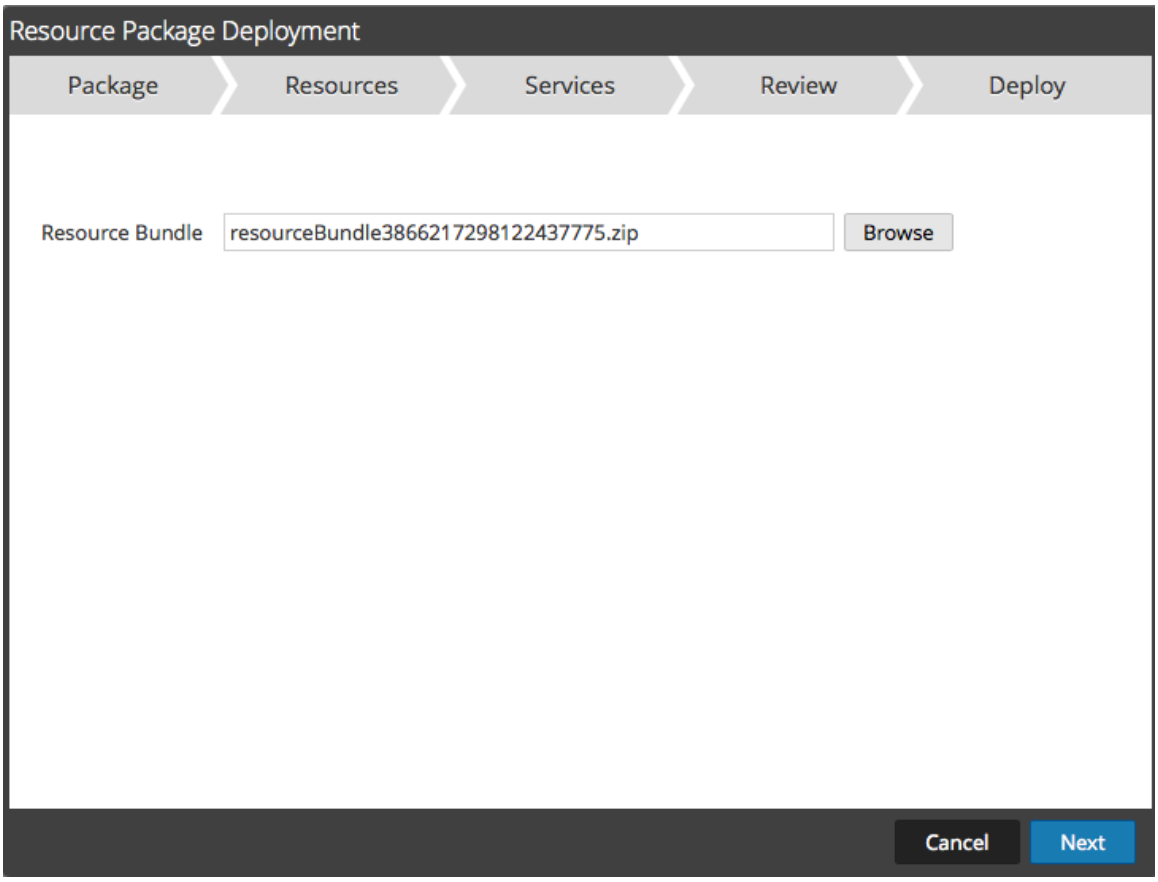
El Asistente de implementación tiene cinco pestañas: **Paquete, Recursos**, **Servicios**, **Revisión** e **Implementar**.
Use **Cerrar** para salir antes de completar al asistente.

Cuando completa el asistente, NetWitness Suite regresa a la vista Recursos de Live.

## Pestaña Paquete

Esta pestaña se usa para seleccionar un paquete de recursos de la red en esta página.

Este es un ejemplo de la pestaña Paquete, con un paquete de recursos ya seleccionado.



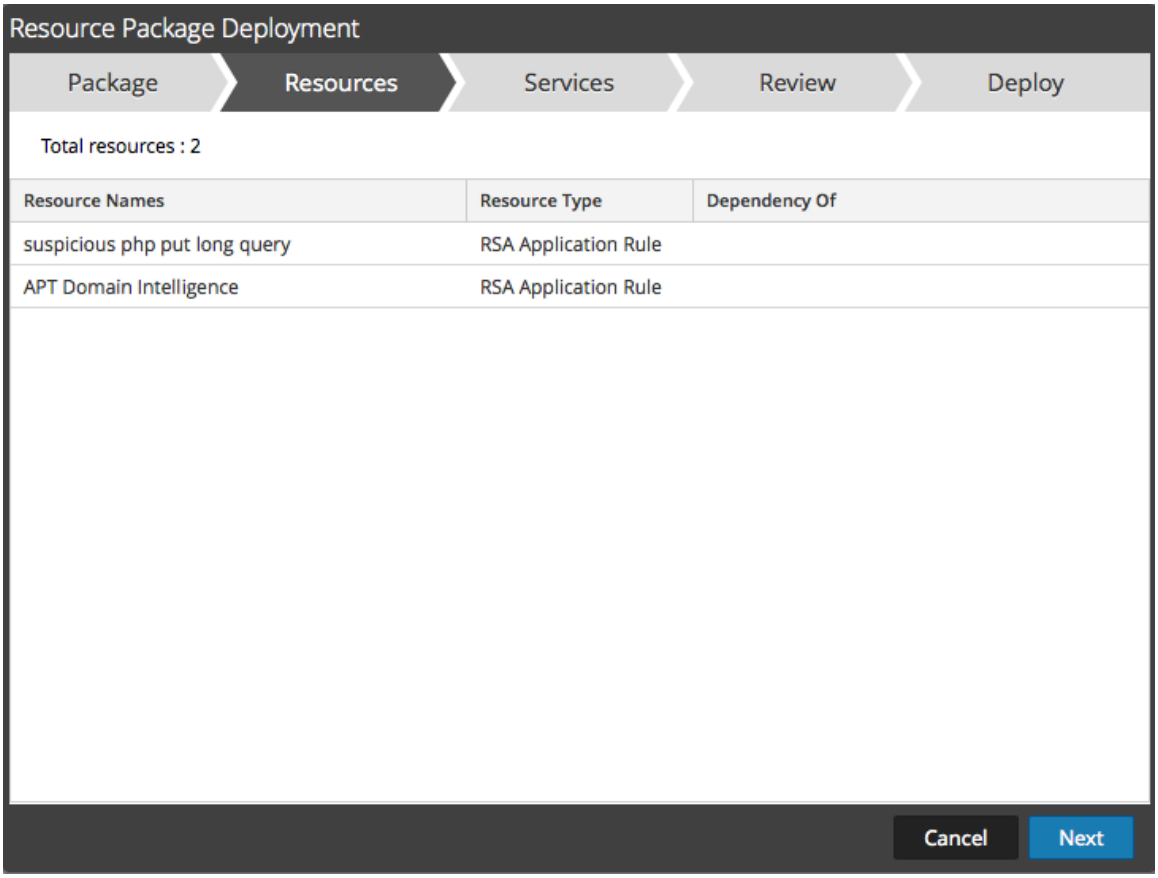

En la siguiente tabla se describen los elementos de la pestaña Paquete.

| Columna | Descripción |
|---|---|
| Paquete de recursos | El campo de entrada para especificar un paquete de recursos. Puede escribir una ruta en este campo o realizar una búsqueda mediante el botón Browse. |
| Botones de comandos | |
| Examinar | Este botón abre el cuadro de diálogo Carga de archivo, en el cual, puede buscar el sistema de archivos locales y seleccionar un paquete. |
| Cancelar | Cancela la implementación y cierra el asistente. |
| Siguiente | Muestra la pestaña siguiente del asistente. |

## Pestaña Recursos

Esta pestaña muestra los recursos que se incluyen en el paquete.

En la siguiente figura se muestra un ejemplo de la pestaña Recursos.




En la siguiente tabla se describen los elementos de la pestaña Recursos.

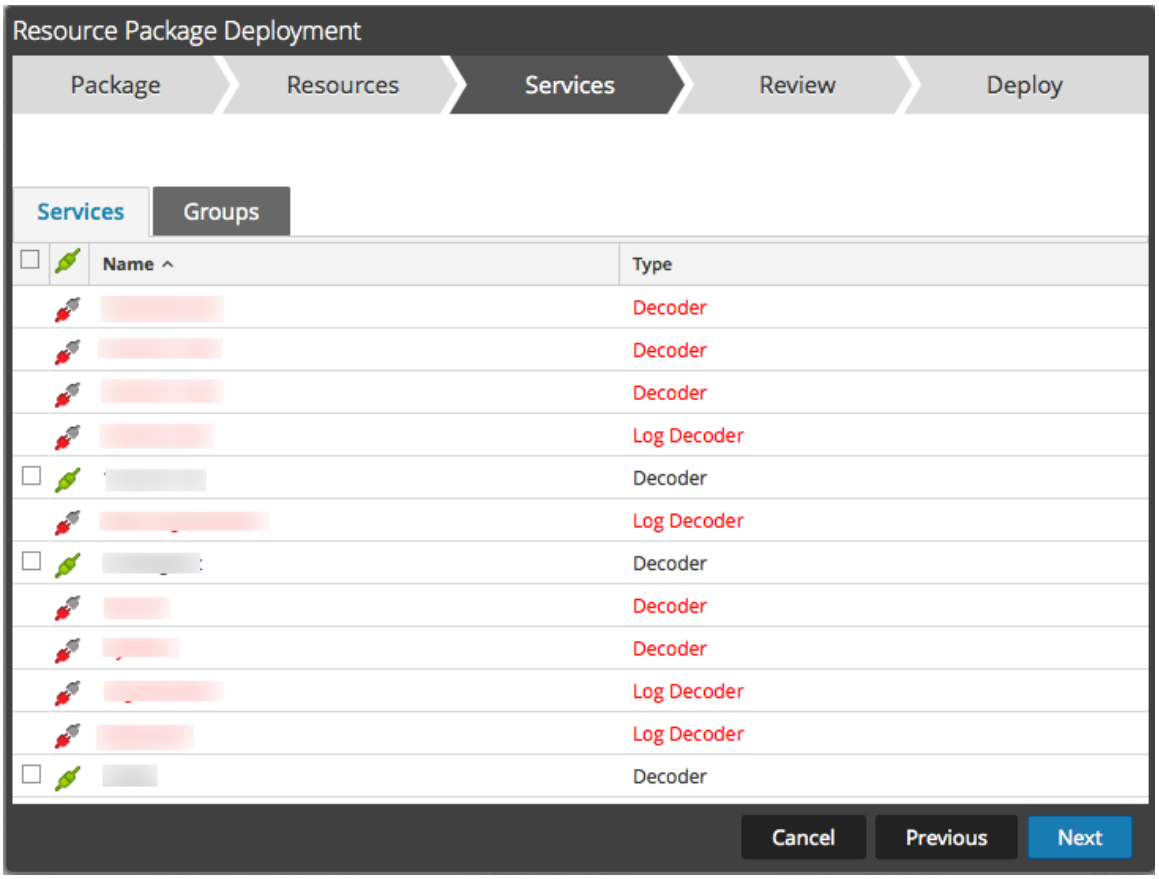
| Columna | Descripción |
|---|---|
| Nombre del recurso | Muestra el nombre de los recursos del paquete (por ejemplo, **NetWitness Lua Library**). |
| Tipo de recurso | Muestra los tipos de recursos del paquete (por ejemplo, **RSA Lua Parser**). |
| Dependencia de | Muestra los recursos de los cuales depende el recurso seleccionado (por ejemplo, **AIM lua**) |

## Pestaña Servicios

Seleccione los servicios en los cuales desea implementar los recursos del paquete.

La pestaña Servicios tiene dos pestañas, **Servicios** y **Grupos**. Estas proporcionan una lista de servicios y grupos de servicios que se configuran en la vista ADMIN > Servicios. Las columnas son un subconjunto de las columnas disponibles en la vista Servicios. Puede seleccionar los servicios o los grupos de servicios en los cuales desea implementar los recursos del paquete.

Este es un ejemplo de la pestaña Servicios.




En la siguiente tabla se describen los elementos de la pestaña Servicios.

| Columna | Descripción |
|---|---|
| **Servicios** | |
| | Selecciona los servicios en los cuales desea implementar el contenido. Puede seleccionar cualquier combinación de servicios y grupos de servicios. |
| Nombre | Muestra los servicios del ambiente en los cuales puede implementar el contenido. |
| Host | Muestra el nombre del host del recurso. |

| Columna | Descripción |
|---|---|
| Tipo | Muestra el tipo de servicio de NetWitness Suite. |
| **Grupos** | |
| | Selecciona grupos de servicios (si hay grupos de servicios definidos en el ambiente). |
| Nombre | Muestra los nombres de los grupos de servicios. |

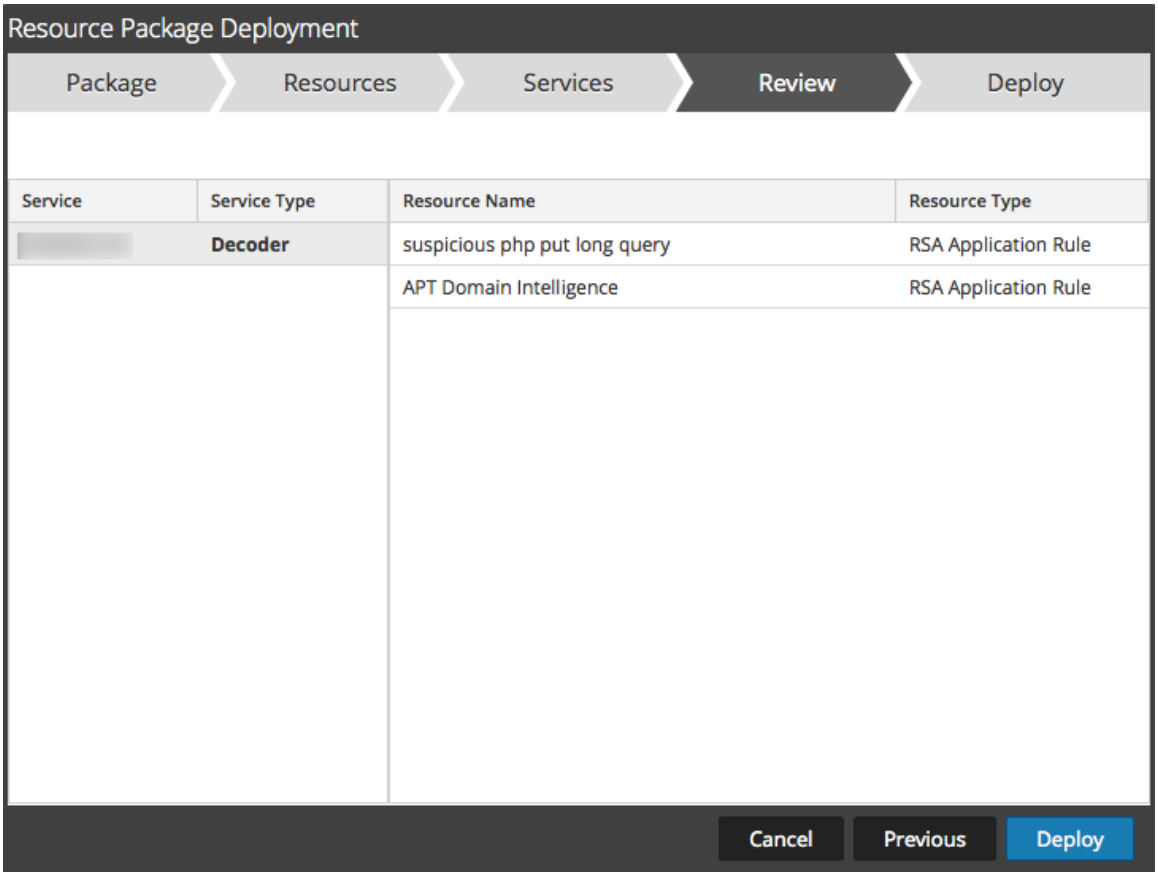
## Pestaña Revisión

Muestra los recursos y servicios en los cuales se implementarán los recursos.

Esta pestaña permite realizar lo siguiente:

- Revisar el contenido y los servicios antes de implementarlos.
- Iniciar la implementación de los recursos.

En la siguiente figura se muestra un ejemplo de la pestaña Análisis.



En la siguiente tabla se describen los elementos de la pestaña Análisis.

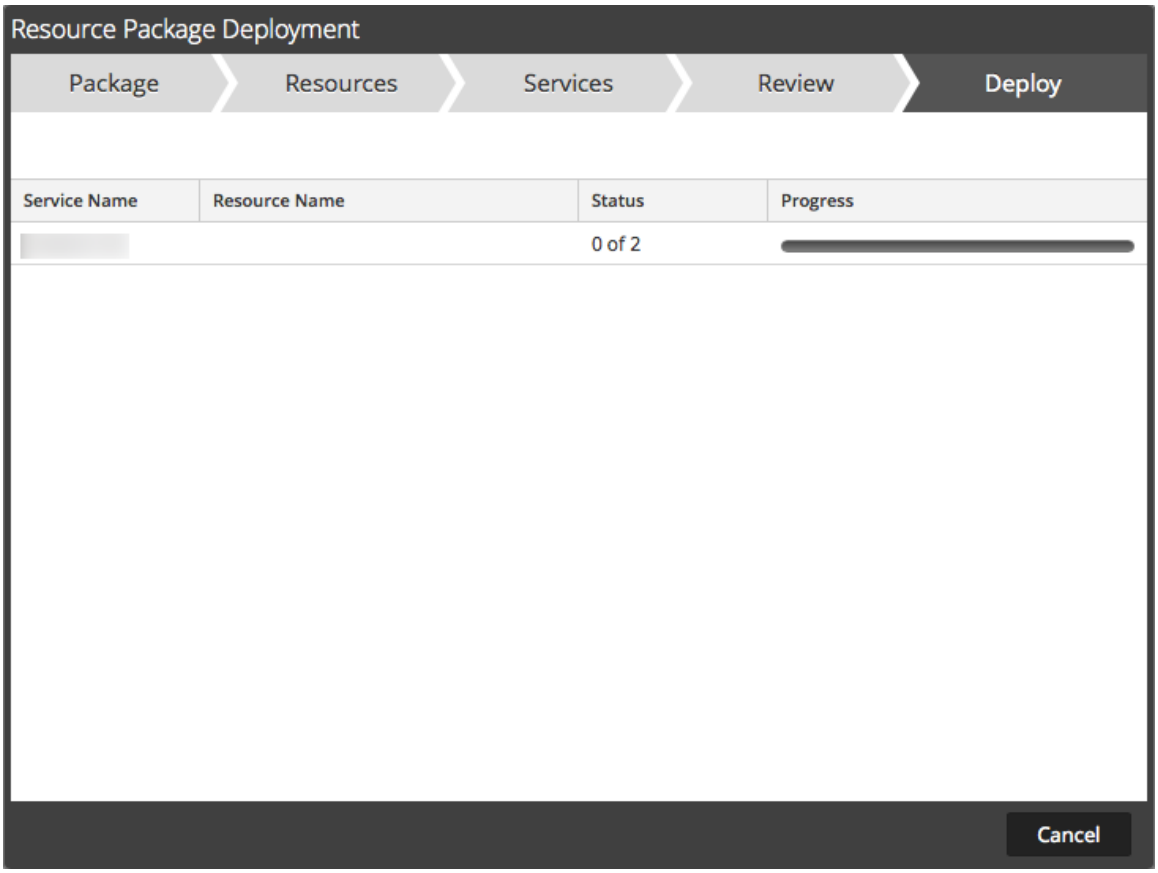
| Columna | Descripción |
|---|---|
| **Información de servicio** | |
| Servicio | Muestra los servicios del ambiente en los cuales puede implementar el contenido. |
| Tipo de servicio | Muestra el tipo de cada servicio de NetWitness Suite (tipo de host/servicio). |
| **Información de recursos** | |
| Nombre del recurso | Muestra el nombre de los recursos que seleccionó (por ejemplo, **NetWitness Lua Library**). |
| Tipo de recurso | Muestra los tipos de recursos que seleccionó (por ejemplo, **RSA Lua Parser**). |
| Implementación | Inicia la implementación de los recursos y muestra la página **Implementar** (página final del asistente). |

### Pestaña Implementar

Esta pestaña permite realizar lo siguiente:

- Ver el progreso del trabajo
- Cancelar el trabajo

Este es un ejemplo de la pestaña Implementar.



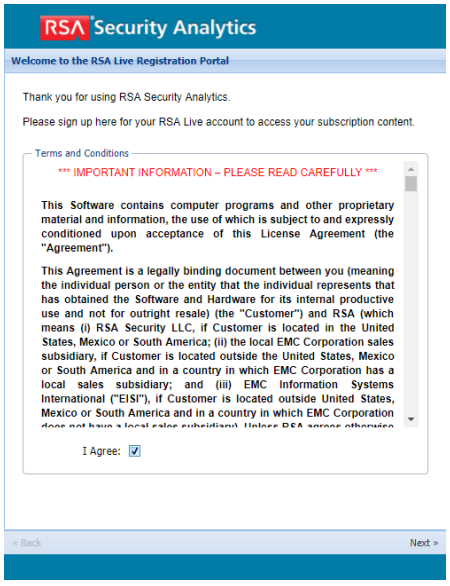

En la siguiente tabla se describen los elementos de la pestaña Implementar.

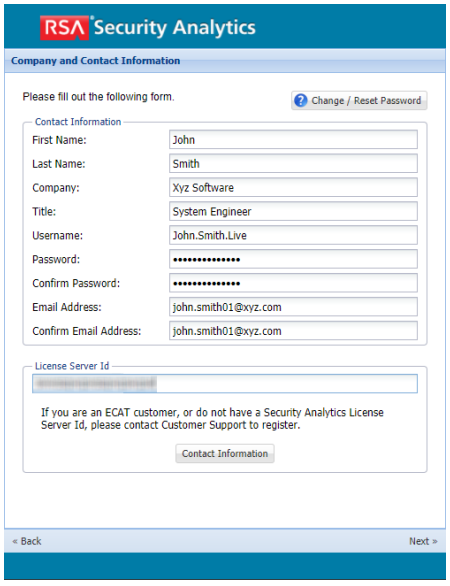
| Función | Descripción |
|---|---|
| Nombre del servicio | Nombre de los servicios para los cuales se implementan los recursos. |
| Nombre del recurso | Nombre de los recursos. |
| Estado | Estado de la implementación manual. |
| Progreso | Progreso de la implementación manual en una barra de progreso. Una vez que haya finalizado, la barra será de color verde. |
| **Botones de comandos** | |

| Función | Descripción |
|---|---|
| Cerrar | Cierra el asistente. |
| Errores | Solo se muestra si NetWitness Suite encontró errores. Haga clic para mostrar los errores. |
| Reintentar | Solo se muestra si NetWitness Suite encontró errores. Haga clic en este botón para volver a intentar la implementación de los recursos mediante el asistente. |

## Portal de registro de RSA Live

El Portal de registro de RSA Live es un asistente de autoservicio en el cual los clientes pueden configurar una cuenta de Live y cambiar o restablecer la contraseña. Se requiere una cuenta de Live para obtener acceso a los feeds, los analizadores, las reglas y otro contenido de la biblioteca de RSA Live. Para acceder al portal, vaya a la siguiente URL: https://cms.netwitness.com/registration/.




Después de aceptar los Términos y condiciones y de hacer clic en **Siguiente**, se muestran los campos necesarios para configurar una cuenta. Entre estos se incluyen Información de contacto, Nivel de suscripción e Identificador de servidor de licencia.

En la siguiente tabla se indican los campos de la sección Información de contacto y sus descripciones:

| Parámetro | Descripción |
|---|---|
| **Cambiar/restablecer contraseña** | Permite a los usuarios cambiar o restablecer su contraseña de RSA Live. |
| **Nombre** | Su nombre. |
| **Apellido** | Su apellido. |
| **Empresa** | El nombre de la empresa. |
| **Título** | Su cargo o función en la empresa. |
| **Nombre de usuario** | El nombre de usuario que se usa para iniciar sesión en la cuenta de RSA Live. El nombre de usuario debe contener un mínimo de nueve caracteres y un máximo de 60. |
| **Contraseña** | La contraseña de la cuenta de RSA Live. La contraseña debe contener un mínimo de nueve caracteres y un máximo de 60, con al menos uno en mayúscula, uno en minúscula, un número y un carácter especial. |
| **Confirmar contraseña** | Confirmación de la contraseña. |
| **Dirección de correo electrónico** | La dirección de correo electrónico donde desea recibir notificaciones relacionadas con la cuenta de Live. |
| **Confirmar dirección de correo electrónico** | Confirmación de la dirección de correo electrónico. |

| Parámetro | Descripción |
| --- | --- |
| **Nivel de suscripción/Confirmar nivel de suscripción** | • **Basic**: Brinda acceso al contenido de Live etiquetado para grupos como Basic, Panorama for Log Decoder y Spectrum for Malware Analysis.<br>• **Enhanced**: Brinda acceso al contenido de Live etiquetado para grupos como Enhanced, Basic, Panorama for Log Decoder y Spectrum for Malware Analysis.<br>• **Premium**: Brinda acceso al contenido de Live etiquetado para grupos como Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder y Spectrum for Malware Analysis. |
| **Identificador de servidor de licencia** | Este es el ID de licencia que se muestra en la página **ADMIN > SISTEMA > Información**.<br>**Precaución:** El ID de servidor de licencia en NetWitness Suite debe ser válido y debe estar registrado en el servidor de Flexera. Si no es así, póngase en contacto con el servicio al cliente de RSA. |

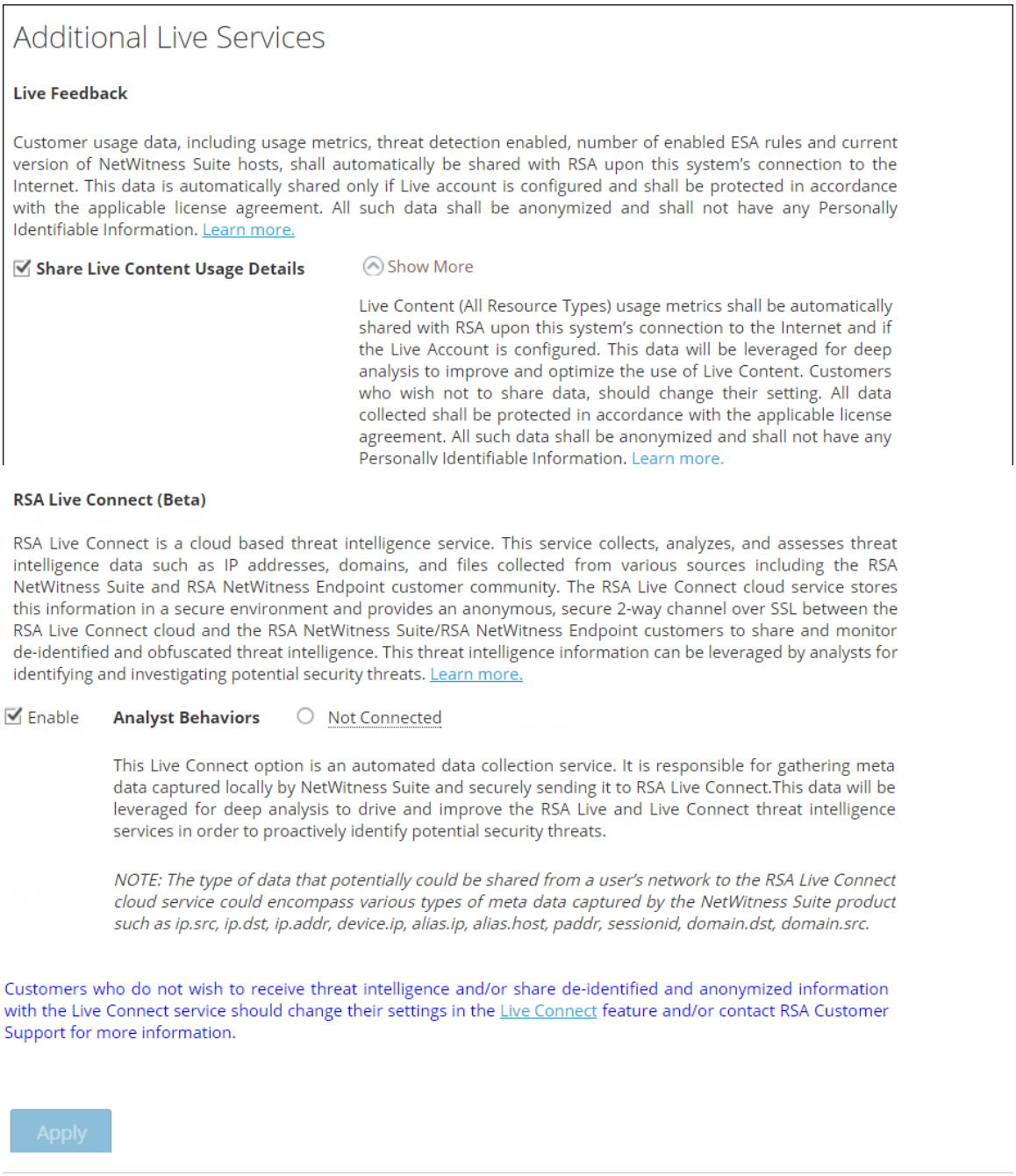
# Comentarios y uso compartido de datos de NetWitness Suite

En este tema se presentan las funciones comentarios y uso compartido de datos de NetWitness Suite.

La configuración de estas funciones está disponible en **ADMIN** > **SISTEMA** > vista **Servicios de Live** en la sección Servicios adicionales de Live.

## Servicios adicionales de Live

La participación en los servicios adicionales de Live se configura en **ADMIN > SISTEMA > vista Servicios de Live**.




## Live Feedback

Live Feedback está diseñado para ayudar a mejorar RSA NetWitness Suite.

Una vez que se configura una cuenta de Live, los datos de uso se comparten con RSA. Los datos se encuentran protegidos conforme al acuerdo de licencia correspondiente. Los datos de uso del cliente, como métricas de uso y la versión actual de los hosts de NetWitness Suite, se comparten automáticamente con RSA cuando el sistema se conecta a Internet.

Antes de que los datos se envíen a RSA, se elimina toda la información de identificación personal. Por lo tanto, solo los datos de uso anónimo se transfieren a RSA.

Para obtener más información, consulte el tema **Descripción general de Live Feedback** de la *Guía de configuración del sistema*.

## RSA Live Connect

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 ECAT. 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 Ver el contexto adicional de un punto de datos.

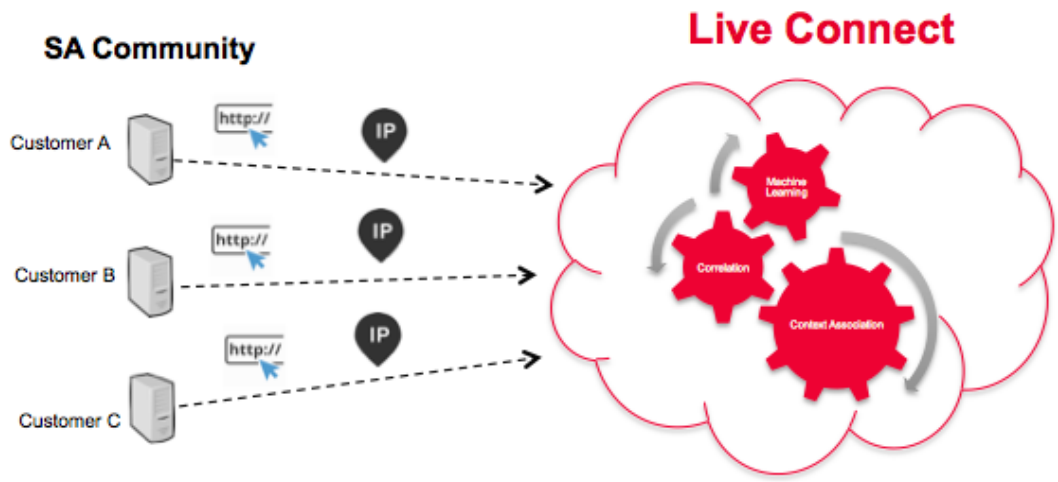
### Comportamientos de analistas

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.

**Nota:** Todos los datos recopilados localmente quedan inidentificables y protegidos, y se envían de manera segura y anónima al servicio de nube de RSA Live Connect, donde se almacenan en un ambiente seguro.

### Descripción

Live Connect Threat Data Sharing se desarrolló como una plataforma de uso compartido de inteligencia de amenazas basada en la comunidad.




Tiene las siguientes características y objetivos:

- Colaboración abierta: la comunidad de RSA contribuye a la recopilación de inteligencia completa
- Recopilar y analizar de forma centralizada los datos de la comunidad de RSA
- Reducir el tiempo del ciclo de inteligencia de días a minutos

Algunos detalles que se deben considerar son los siguientes:

- Se aprovecha la actividad de investigación de los analistas
- Se recopilan metadatos, como direcciones IP y nombres de dominio
- Se realiza un análisis exhaustivo de los datos: Tendencias, correlación y detección de anomalías
- Se debe recordar que esta función se encuentra en versión beta

## Participación

La participación del cliente es opcional. Tras la instalación inicial o una actualización a NetWitness Suite 11.0, se muestra una pantalla de confirmación. De forma predeterminada, se le incorpora al programa, pero puede salir de él en cualquier momento.

### Autenticación en la nube

La autenticación para el programa se realiza en la interfaz del usuario de NetWitness Suite. Aquí debe configurar la cuenta de Live en la sección Servicios de Live.

### Configuración

Para ver o cambiar la configuración de Live Connect Threat Data Sharing, en el menú de menú principal, seleccione **ADMIN > SISTEMA > Servicios de Live**. Seleccione o deseleccione la casilla **Habilitar** para participar o dejar de participar en el programa.

### Recopilación de datos

Los datos se recopilan de la siguiente manera:

- Atribución de los datos: Anónimo
- Origen de datos: Subconjunto de claves y valores de metadatos de vistas de las páginas de un analista de NetWitness Suite desde registros de consulta de NetWitness Suite Core.
- Proceso de recopilación de registros de consulta:
  - Periodicidad: Modo de lotes cada 24 horas (04:00 a 06:00 h UTC).
  - Log Collection: El servidor de NetWitness Suite recopila entradas de registro del dispositivo de NetWitness Suite Core de las últimas 24 horas
  - Entradas de registro: Solo se recopilan llamadas de API de valor de SDK y consulta de SDK que contienen una cláusula where.
  - Análisis de atributos de registro: En cada entrada debe estar presente uno de los siguientes indicadores de claves de metadatos: **ip.src**, **ip.dst**, **ip.addr**, **device.ip**, **alias.ip**, **alias.host**, **paddr**, **sessionid**, **domain.dst** o **domain.src**. Si es así, se recopilarán las claves y los valores de metadatos de la entrada.

  **Nota:** Una vez que se cumplen los criterios anteriores, NetWitness Suite envía todas las claves y los valores de metadatos de la consulta a la nube, no solo a los indicadores de claves de metadatos.

El informe de registro se envía en formato JSON a través de SSL. Incluye:

- Registros de fecha y hora
- Nombre de usuario de Live CMS (sha256)
- NetWitness SuiteIdentificador de servidor de licencia (sha256)
- Lista de ID de terminal de SA (sha256)
- Valores de metadatos recopilados (MD5 y SHA256 con hash)

### Ejemplo

En esta sección se muestran las entradas de un registro y, a continuación, la sección correspondiente de datos extrapolados.

Sección de un archivo de registro:

```
User admin (session 204298, 10.4.50.60:57454) has issued values (channel 205237)
(thread 2332): fieldName=filter id1=1 id2=23138902 threshold=100000 size=20
flags=sessions,sort-total,order-descending,ignore-cache where="(alias.host =
'mail.google.com') && (ip.src = 161.253.31.130) && time=\"2015-12-07 18:08:00\"-
\"2015-12-07 21:07:59\""
```

Extrapolación de datos con aplicación de hash:


```
{
    timestamp: 1452282588000,
    session: 204298,
    id1: 1,
    id2: 23138902,
    userName: "8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918",
    loggerName: "SDK-Values",
    timeRange: "\"2015-12-07 18:08:00\"-\"2015-12-07 21:07:59\"",
  - metaList: [
      - {
            metaKey: "alias.host",
          - properties: {
                domain_hint: "mai*********.com",
                domain_tld: "com",
                md5_value: "be5cab0695415d9363d18ad1345c73eb",
                sha256_value: "3f2728499a4b29460f3e3150df508e06b19edf0f58efd051fac777844d28e452"
            }
        },
      - {
            metaKey: "ip.src",
          - properties: {
                md5_value: "03b81ffdff109a05a3dac88dbec10c59",
                sha256_value: "1d88c6893797c896070bd5470d0026e11b515d5dee97c6173771a43719fa7e78"
            }
        }
    ]
},
```


### Solución de problemas

En esta sección se realiza un análisis breve de la solución de problemas de Live Connect Threat Data Sharing.

**Ejemplo de recuperación de registros de consulta**

Para recuperar una muestra de datos de inteligencia de amenazas enviados a Live Connect, debe formar una dirección URL mediante la configuración de los siguientes parámetros:

- **sendReport**: El valor es **true** o **false**: true para enviar este informe al servidor de Live Connect. Con false, el informe solo se crea para su visualización. El valor se configura de manera predeterminada en false.
- **hashValues**: El valor es **true** o **false**: true para aplicar hash a los valores, como md5/sha256. Con false, los valores se muestran en texto no cifrado; solo se debe usar para su visualización manual. Se configura de manera predeterminada en false.

- **startDate/endDate**: Fechas que corresponden a los límites de tiempo de las entradas del registro. Formato: AAAA-MM-DD HH:mm:ss

El siguiente es un ejemplo de la dirección URL que se usará para recuperar registros de consulta:

`https://<server>/admin/liveconnect/force_aggregation?startDate=2016-01-18%2000:00:00&endDate=2016-01-19%2010:10:00&sendReport=false&hashValues=true`

**Registro de sistema: Depurar**

Puede acceder a cierta información de depuración de la siguiente manera.

1. Seleccione **ADMIN > SISTEMA > Registro de sistema**.
2. Seleccione la pestaña **Configuración**.
3. En la sección Configuración de paquetes, seleccione **com > netwitness > platform > server > liveconnect > service (DEBUG)**.