



RSA | Security Analytics

Administración de servicios de Live
para la versión 10.6

Índice de contenidos

Administración de servicios de Live	6
Security Analytics Live	6
Librería de CMS	6
Procedimientos requeridos de los servicios de Live	7
Lista de verificación de administración de recursos de Live	7
Paso 1. Crear una cuenta de Live	8
Introducción	8
Requisitos previos	8
Crear una cuenta de Live	8
Paso 2. Configurar Live Services en Security Analytics	12
Paso 3. Buscar e implementar recursos de Live	13
Requisitos previos	13
Buscar recursos	13
Paso 4. Administración de recursos de Live	15
Requisitos previos	15
Procedimientos	15
Procedimientos adicionales de los servicios de Live	18
Implementar recursos en Live	20
Implementar recursos manualmente	20
Implementar recursos desde un paquete de recursos	25
Implementar recurso en servicios	30
Implementar recursos de Live mediante el Asistente de implementación	34
Exportar datos a RSA	36
Acerca de Live Feedback	36
Descargar datos históricos de Live Feedback	36
Compartir datos en RSA	37
Administrar feeds personalizados	40
Creación de feeds personalizados	40
Archivo de definición de feed de muestra	40
Equivalentes de definición de feed para los parámetros del asistente Feed personalizado	41
Crear un feed personalizado	45

Crear y administrar un feed de identidad	56
Editar un feed	62
Eliminar un feed	65
Procedimientos varios de los servicios de Live	68
Agregar recursos suscritos para implementación en los servicios	68
Crear un paquete de recursos	69
Eliminar una suscripción	71
Mostrar detalles de un recurso en la vista Recurso de Live	71
Descargar un recurso	72
Localizar y eliminar un recurso implementado desde servicios	73
Eliminar recursos suscritos de la cuadrícula Suscripciones de implementaciones	74
Mostrar los resultados como una cuadrícula o en detalle	75
Suscribirse y cancelar la suscripción a un recurso	76
Ver detalles del recurso	78
Ver los recursos suscritos seleccionados para implementación en los servicios	78
Referencias de los servicios de Live	80
Vista Configuración de Live	80
Pestaña Implementaciones	80
Pestaña Suscripciones	83
Vista Feeds de Live	84
Barra de herramientas	85
Cuadrícula Feeds	86
Vista Recurso de Live	87
Detalles de recursos	88
Barra de herramientas de la vista Recurso	91
Vista Buscar en Live	92
Panel Criterios de búsqueda	92
Panel Coincidencias de recursos	96
Asistente Implementación de paquete de recursos	99
Características	100
Pestaña Paquete	100
Pestaña Recursos	101
Pestaña Servicios	102
Pestaña Revisión	104
Pestaña Implementar	105
Portal de registro de RSA Live	107

Comentarios y uso compartido de datos de Security Analytics	112
Servicios adicionales de Live	112
Live Feedback	112
Live Connect Threat Data Sharing (beta)	113
Participación	114

Copyright © 2016 EMC Corporation. Todos los derechos reservados.

Marcas comerciales

RSA, el logotipo de RSA y EMC son marcas registradas o marcas comerciales de EMC Corporation en los Estados Unidos y en otros países. Todas las demás marcas comerciales utilizadas en este documento pertenecen a sus respectivos propietarios. Para obtener una lista de las marcas comerciales de EMC, visite mexico.emc.com/legal/emc-corporation-trademarks.htm (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 del acuerdo de licencia que se aplica al software de otros fabricantes en este producto puede encontrarse en el archivo [thirdpartylicenses.pdf](#).

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

El uso, la copia y la distribución de cualquier software de EMC descrito en esta publicación requieren una licencia de software correspondiente. 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.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA "TAL CUAL". EMC CORPORATION NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIALIZABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Administración de servicios de Live

En esta guía se proporciona una descripción general del acceso de Security Analytics a Security Analytics Live. RSA Security Analytics Live es el gateway a un ambiente enriquecido que ofrece acceso a feeds, herramientas y otros recursos.

Security Analytics Live

Live es el componente de Security Analytics que administra la comunicación y la sincronización entre los servicios de Security Analytics y una biblioteca de contenido de Live disponible para los clientes de RSA Security Analytics. Live proporciona una interfaz simple para navegar, seleccionar e implementar contenido desde el sistema de administración de contenido de Security Analytics Live en los servicios y el software de Security Analytics. 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 contenido (CMS) (conocida como *Live*) es una valiosa fuente de los recursos de seguridad en Internet más recientes para los clientes de Security Analytics. 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.

Próximos pasos

- [Procedimientos requeridos de los servicios de Live](#)
- [Procedimientos adicionales de los servicios de Live](#)
- [Referencias de los servicios de Live](#)

Procedimientos requeridos de los servicios de Live

En este tema se explica cómo configurar Live en Security Analytics.

Lista de verificación de administración de recursos de Live

Después de analizar este tema, el administrador habrá aprendido a configurar Live en Security Analytics, buscar recursos en Live y administrar los recursos de Live.

Paso	Descripción
1	Paso 1. Crear una cuenta de Live en el portal de registro de RSA Live, URL: http://cms.netwitness.com/registration/ . Si tiene una cuenta, puede administrarla mediante este portal.
2	Paso 2. Configurar Live Services en Security Analytics mediante la configuración de una conexión con el servidor de CMS
3	Utilice la vista Buscar en Live para Paso 3. Buscar e implementar recursos de Live
4	Paso 4. Administración de recursos de Live

Paso 1. Crear una cuenta de Live

En este tema se describe cómo crear una cuenta de Live mediante el Portal de registro de RSA Live en el servidor de CMS.

Introducción

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.

Requisitos previos

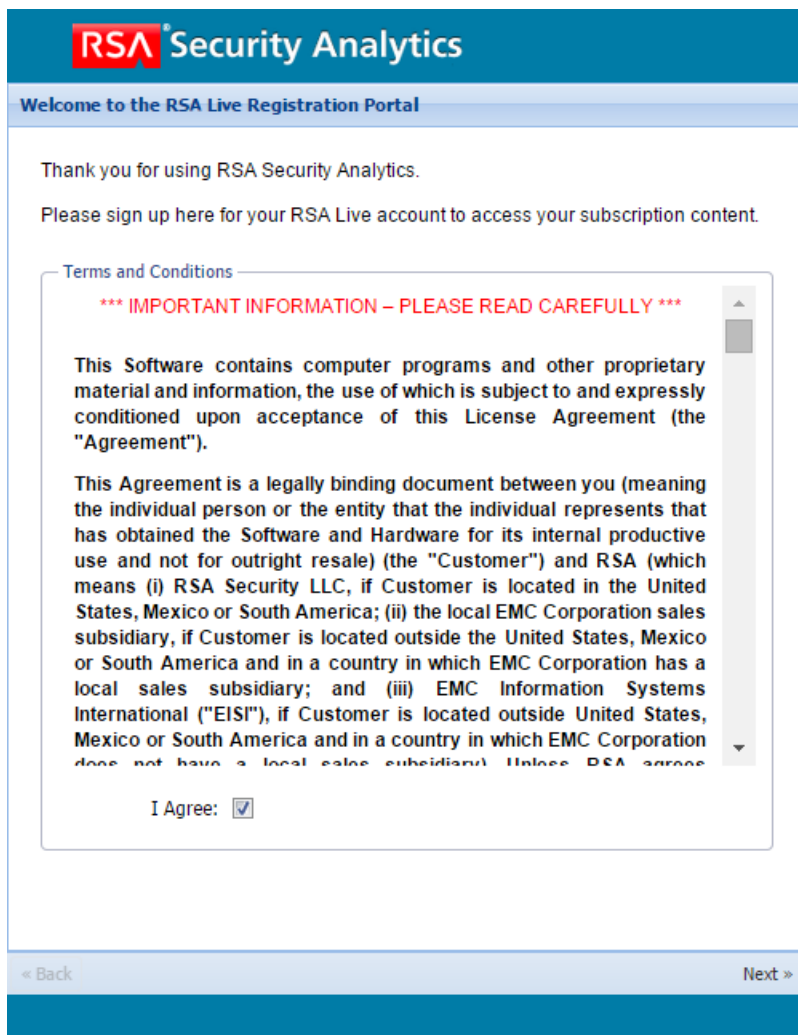
Asegúrese de que esté disponible lo siguiente para configurar una cuenta de RSA Live:

- Una conexión a Internet activa para acceder al portal.
- Un servidor de licencia de Security Analytics 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 **Administration > Sistema > Información**.

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

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:

RSA Security Analytics

Company and Contact Information

Please fill out the following form. [? Change / Reset Password](#)

Contact Information

First Name: John

Last Name: Smith

Company: Xyz Software

Title: System Engineer

Username: John.Smith.live

Password:

Confirm Password:

Email Address: user@example.com

Confirm Email Address: user@example.com

Subscription Level

Basic

Enhanced

Premium

Confirm Subscription Level

Basic

Enhanced

Premium

License Server Id

.....

< Back Next >

Notas acerca de las credenciales de su cuenta de Live:

- 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 **Administration > Sistema > Información**.

Precaución: Asegúrese de que el ID del servidor de licencia en Security Analytics 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**.

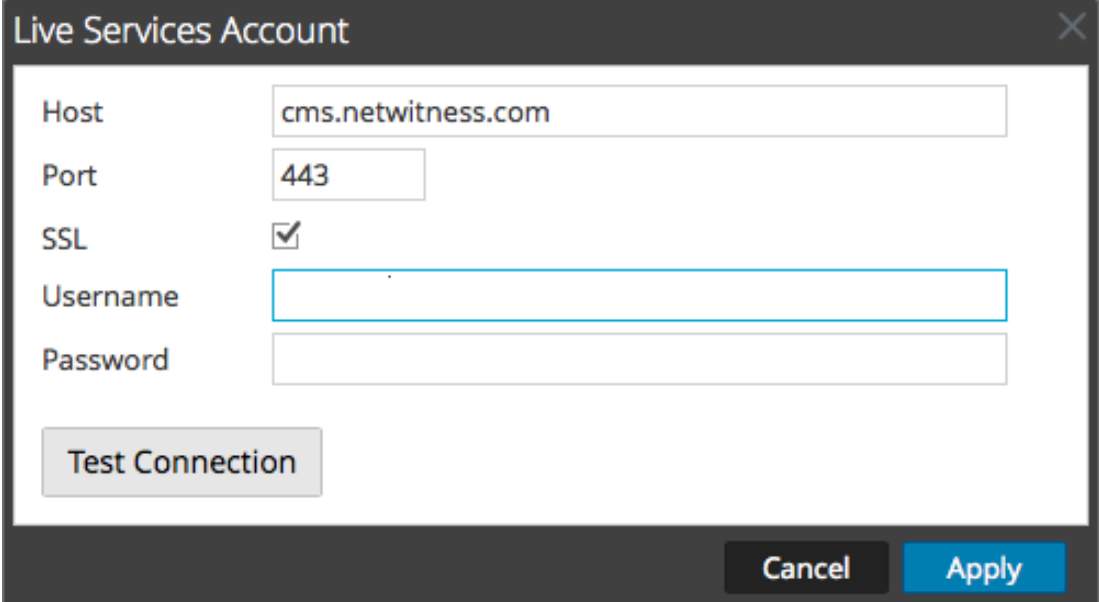
Si el registro se realiza correctamente, recibirá un correo electrónico de confirmación de la cuenta de RSA Live con su nombre de usuario. Ahora tiene acceso al contenido suscrito.

Paso 2. Configurar Live Services en Security Analytics

En este tema se indica a los administradores cómo configurar Live en Security Analytics mediante la configuración de la conexión y la sincronización entre el servidor de CMS y Security Analytics.

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

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



The screenshot shows a dialog box titled "Live Services Account" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Host:** A text input field containing "cms.netwitness.com".
- Port:** A text input field containing "443".
- SSL:** A checkbox that is checked.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Test Connection:** A button located below the Username and Password fields.
- Cancel:** A button located at the bottom right of the dialog.
- Apply:** A blue button located at the bottom right of the dialog, next to the Cancel button.

2. Configure el tiempo de la sincronización de Security Analytics 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*.

Paso 3. Buscar e implementar recursos de Live

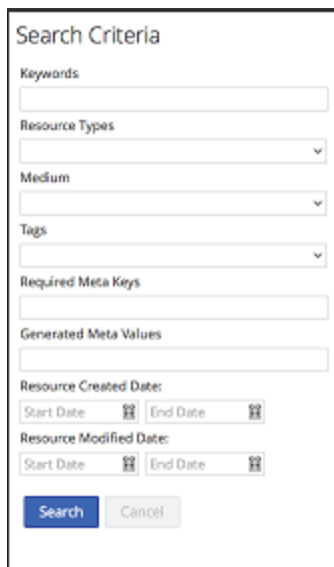
En este tema se indica a los administradores cómo buscar recursos en la vista Buscar en Live, que también es lo mismo que navegar por Live CMS para ver recursos con el panel Criterios de búsqueda de la [Vista Buscar en Live](#).

Requisitos previos

Un requisito previo para la búsqueda de recursos de Live es la configuración de la conexión y la sincronización entre el servidor de CMS y Security Analytics.

Buscar recursos

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



The screenshot shows a 'Search Criteria' panel with the following fields and controls:

- Keywords:** A text input field.
- Resource Types:** A dropdown menu.
- Medium:** A dropdown menu.
- Tags:** A dropdown menu.
- Required Meta Keys:** A text input field.
- Generated Meta Values:** A text input field.
- Resource Created Date:** Two date pickers labeled 'Start Date' and 'End Date'.
- Resource Modified Date:** Two date pickers labeled 'Start Date' and 'End Date'.
- Buttons:** A blue 'Search' button and a grey 'Cancel' button.

2. Haga clic en **Buscar**.

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

The screenshot displays the RSA Security Analytics interface. On the left, the 'Search Criteria' panel includes fields for Keywords, Resource Types (with selected options: RSA CEP Module, RSA Feed, RSA FlexParser, RSA Investigator Custom Action), Tags, Required Meta Keys, Generated Meta Values, Resource Created Date (with Start and End Date pickers), and Resource Modified Date (with Start and End Date pickers). A 'Search' button is at the bottom of this panel. The main area, 'Matching Resources', shows a table of results with columns: Subscribed, Name, Created, Updated, Type, and Description. Below the table, it indicates '213 Matching Resources'. The bottom status bar shows 'admin | English (United States) | GMT-05:00' and a 'Send Us Feedback' link.

Subscribed	Name	Created	Updated	Type	Description
<input type="checkbox"/>	SRI Attackers	2012-02-09 11:49 AM	2014-02-21 3:01 PM	RSA Feed	List of malicious
<input type="checkbox"/>	RSA FirstWatch Criminal Socks ...	2012-02-09 11:48 AM	2014-05-14 8:03 AM	RSA Feed	This feed contai
<input type="checkbox"/>	SpyEye Tracker	2012-02-09 11:49 AM	2014-10-13 8:00 PM	RSA Feed	SpyEye tracker i
<input type="checkbox"/>	SpyEye Domain Tracker	2012-02-09 11:49 AM	2014-10-13 8:00 PM	RSA Feed	SpyEye domain
<input type="checkbox"/>	RSA FirstWatch APT Threat Do...	2012-05-15 8:07 PM	2015-05-05 2:03 AM	RSA Feed	This feed contai
<input type="checkbox"/>	RSA FirstWatch Criminal VPN E...	2012-02-09 11:48 AM	2015-05-07 2:02 AM	RSA Feed	This feed contai
<input type="checkbox"/>	RSA FirstWatch Criminal VPN E...	2012-02-09 11:48 AM	2015-05-07 8:02 AM	RSA Feed	This feed contai
<input type="checkbox"/>	RSA FirstWatch Criminal VPN E...	2012-02-09 11:48 AM	2015-05-07 8:02 AM	RSA Feed	This feed contai
<input type="checkbox"/>	RSA FirstWatch Criminal VPN E...	2012-02-09 11:48 AM	2015-05-07 8:02 AM	RSA Feed	This feed contai
<input type="checkbox"/>	Malware Domains	2012-02-09 11:48 AM	2015-05-08 8:00 PM	RSA Feed	List of domains
<input type="checkbox"/>	RSA FirstWatch APT Threat IPs	2012-05-15 8:07 PM	2015-05-08 8:03 PM	RSA Feed	This feed contai
<input type="checkbox"/>	RSA FirstWatch Exploit IPs	2012-12-22 7:35 PM	2015-05-09 8:16 AM	RSA Feed	This feed contai
<input type="checkbox"/>	RSA FirstWatch Exploit Domains	2012-12-22 7:35 PM	2015-05-09 8:16 AM	RSA Feed	This feed contai
<input type="checkbox"/>	RSA FirstWatch Criminal SOCKS...	2012-02-09 11:48 AM	2015-05-10 2:05 PM	RSA Feed	This feed contai
<input type="checkbox"/>	Palevo Tracker Domains	2012-05-15 8:03 PM	2015-05-10 2:06 PM	RSA Feed	Palevo Tracker c
<input type="checkbox"/>	Spamhaus EDROP List IP Ranges	2012-07-24 12:24 AM	2015-05-10 2:06 PM	RSA Feed	DROP (Don't Ro
<input type="checkbox"/>	IDefense Threat Indicators Do...	2012-02-09 11:48 AM	2015-05-11 2:02 AM	RSA Feed	Verisign idefens
<input type="checkbox"/>	Zeus Tracker	2012-02-09 11:49 AM	2015-05-11 8:00 AM	RSA Feed	Zeus tracker is z
<input type="checkbox"/>	Zeus Domain Tracker	2012-02-09 11:49 AM	2015-05-11 8:00 AM	RSA Feed	Zeus domain tre

- (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.

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*.

Paso 4. Administración de recursos de Live

En este tema se indica a los administradores cómo administrar recursos en 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.

Requisitos previos

Los requisitos previos para realizar estas tareas son los siguientes:

- Acceso a Internet
- Una cuenta de RSA Live
- Sincronización del servidor de CMS con Security Analytics

Procedimientos

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

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

Implementar recursos manualmente

El flujo de trabajo más simple para implementar recursos en los servicios es el método manual, el cual implementa instantáneamente los recursos en los servicios. Debido a que este método no implica una suscripción a los recursos, Security Analytics no se sincroniza con Live cuando los recursos implementados se actualizan en Live.

- En la [Vista Buscar en Live](#), puede buscar recursos de Live, seleccionar recursos en el panel Resultados coincidentes e implementarlos manualmente.

- En la [Vista Recurso de Live](#), puede implementar el recurso actual manualmente mediante el [Asistente Implementación de paquete de recursos](#).

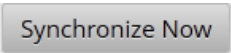
Suscripción e implementación

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 **Administration** > panel **Configuración de Live**.

Con la adición de recursos suscritos a la lista de implementaciones, se configura Security Analytics para migrar automáticamente esos recursos a los servicios seleccionados en los intervalos de sincronización establecidos. Este método requiere planificación de los servicios y grupos de servicios donde se implementan los recursos. Además:

- Puede quitar un recurso de la lista de implementaciones en la [Pestaña Implementaciones](#).
- Puede cancelar la suscripción a un recurso en la [Pestaña Suscripciones](#) y en la [Vista Recurso de Live](#).

Para administrar suscripciones e implementaciones:

1. En **Administration** > **Sistema**> panel **Live**, especifique un intervalo en el cual Security Analytics comprobará 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 actualizaron.
2. En la vista **Live** > **Buscar**, busque recursos de Live y suscríbase a ellos.
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 **Administration** > **Sistema** > **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 quítelos 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 servicios 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

En la vista Recurso de Live [Asistente Implementación de paquete de recursos](#), puede implementar un paquete de contenido creado en Live en uno o más servicios. Security Analytics acepta paquetes en archivos **.nwp** o archivos **.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 de los servicios de Live

En los siguientes temas se describen los procedimientos asociados con la administración de servicios de Live

- [Implementar recursos en Live](#)
 - [Implementar recursos manualmente](#)
 - [Implementar recursos desde un paquete de recursos](#)
 - [Implementar recurso en servicios](#)
 - [Implementar recursos de Live mediante el Asistente de implementación](#)
- [Exportar datos a RSA](#)
- [Administrar feeds personalizados](#)
 - [Crear un feed personalizado](#)
 - [Crear y administrar un feed de identidad](#)
 - [Editar un feed](#)
 - [Eliminar un feed](#)
- [Procedimientos varios de los servicios de Live](#)

Implementar recursos en Live

Hay varios métodos para implementar recursos de RSA en Security Analytics Live.

- [Implementar recursos manualmente](#)
- [Implementar recursos desde un paquete de recursos](#)
- [Implementar recurso en servicios](#)
- [Implementar recursos de Live mediante el Asistente de implementación](#)

Implementar recursos manualmente

En este tema se describe el procedimiento para implementar recursos que están seleccionados actualmente en la cuadrícula Coincidencias de recursos de la [Vista Buscar en Live](#) mediante el [Asistente Implementación de paquete de recursos](#).

Cuando tenga resultados de la navegación de recursos en Security Analytics Live, podrá implementar los recursos manualmente en un servicio o un grupo de servicios sin suscribirse a ellos.

La implementación manual de recursos se realiza en los servicios sin aprovechar las funcionalidades eficaces de administración de recursos de Security Analytics. Si desea recibir notificaciones y actualizaciones de los recursos actualizados y poder quitar fácilmente los recursos de un servicio, debe suscribirse a ellos en la vista [Buscar en Live](#) e implementarlos en la [Vista Configuración de Live](#).

Después de realizar este procedimiento, habrá:

- Implementado recursos seleccionados actualmente en la cuadrícula Coincidencias de recursos de la vista [Buscar en Live](#).
- Implementado recursos de un paquete de recursos creado previamente en la red.

Para implementar recursos manualmente:

1. En la **vista [Buscar en Live](#)**, navegue por el recurso de Live (por ejemplo, busque el tipo de recurso **Contenido de RSA**).
2. En el panel **Coincidencias de recursos**, seleccione **Mostrar resultados > Cuadrícula**.


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

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

The screenshot shows the RSA Security Analytics interface. On the left, the 'Search Criteria' panel includes fields for Keywords, Resource Types (set to 'RSA Event Stream Analysis Rule'), Tags, Required Meta Keys, and Generated Meta Values. It also has date pickers for 'Resource Created Date' and 'Resource Modified Date', and 'Search' and 'Cancel' buttons. The main area, 'Matching Resources', displays a table of 130 resources. The table has columns for 'Subscribed', 'Name', 'Created', 'Updated', 'Type', and 'Description'. The first few rows are:

Subscribed	Name	Created	Updated	Type	Description
<input checked="" type="checkbox"/>	User Account Created Logge...	2013-12-24 6:23 AM	2015-04-21 9:48 AM	RSA Event Strea...	Detects when i
<input checked="" type="checkbox"/>	Basic Rule Template	2013-12-24 6:23 AM	2014-11-05 10:18 PM	RSA Event Strea...	This template i
<input checked="" type="checkbox"/>	RDP traffic from non RFC 191...	2014-02-27 6:24 AM	2015-02-14 3:22 AM	RSA Event Strea...	Identify RDP tr
<input checked="" type="checkbox"/>	Internal Data Posting to 3rd ...	2014-08-16 4:02 AM	2015-02-14 3:24 AM	RSA Event Strea...	10.4 or higher.
<input checked="" type="checkbox"/>	Multi Service Connection Att...	2013-12-24 6:20 AM	2015-02-14 3:21 AM	RSA Event Strea...	Multiple Conne
<input checked="" type="checkbox"/>	File Transfer followed by ECA...	2014-09-17 3:31 PM	2015-02-14 3:25 AM	RSA Event Strea...	Detects a sessi
<input checked="" type="checkbox"/>	Detection of Encrypted Traffl...	2014-03-20 10:56 AM	2015-02-14 3:23 AM	RSA Event Strea...	Detects when t

At the bottom of the interface, there is a status bar showing 'admin | English (United States) | GMT-05:00' and a 'Send Us Feedback' link.

- En la barra de herramientas Coincidencias de recursos, haga clic en  Deploy .
Se abre el **Asistente de implementación** y se muestra la página **Recursos**.

The screenshot shows the 'Deployment Wizard' with four steps: Resources, Services, Review, and Deploy. The 'Resources' step is active. It shows 'Total resources : 1'. Below this is a table with columns 'Resource Names', 'Resource Type', and 'Dependency Of'.

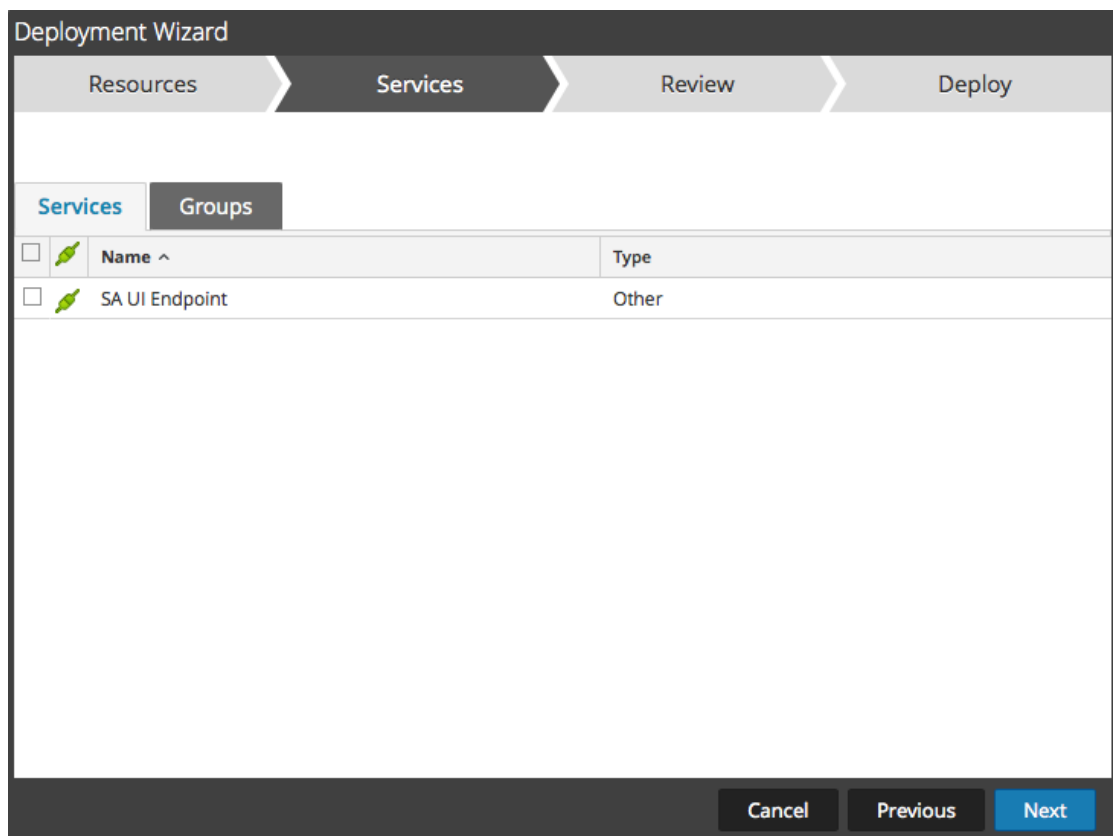
Resource Names	Resource Type	Dependency Of
Basic Rule Template	RSA Event Stream An...	

At the bottom right, there are 'Cancel' and 'Next' buttons.

5. Haga clic en **Siguiente**.

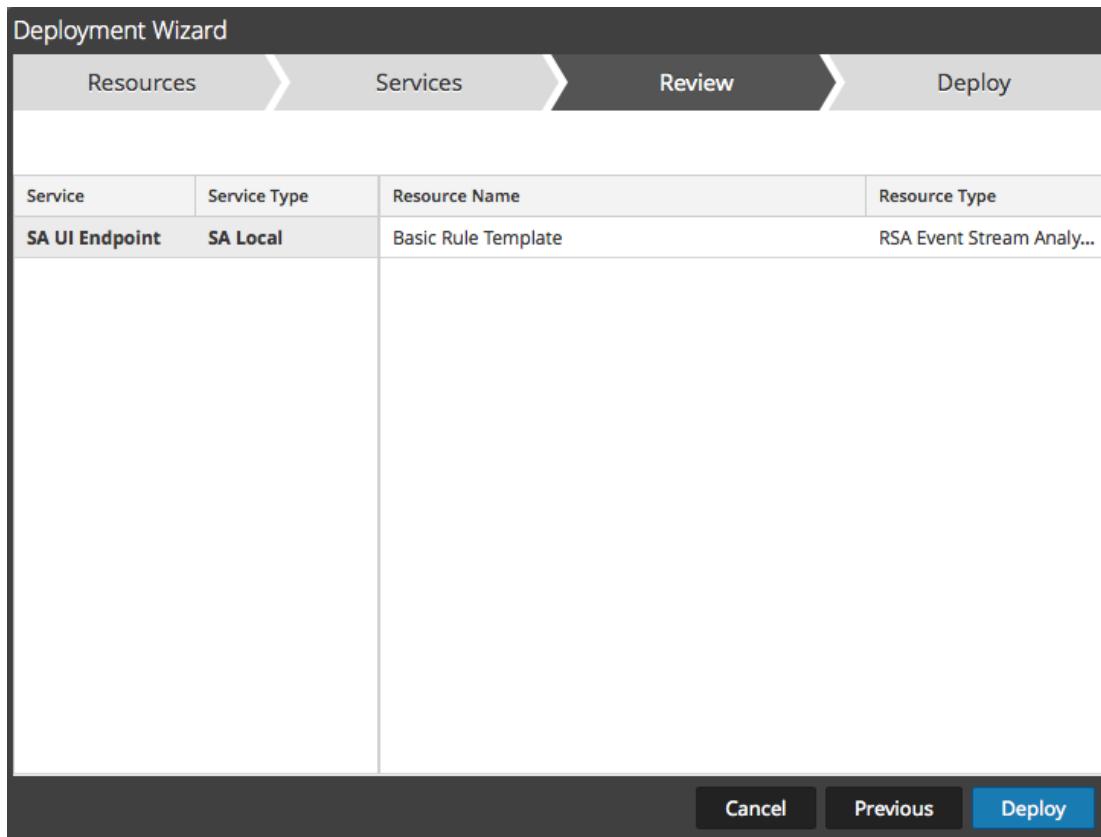
Se muestra la página **Servicios**, la cual tiene dos pestañas, **Servicios** y **Grupos**. Estas proporcionan una lista de servicios y grupos de servicios que se configuran en Administration > vista Servicios. Las columnas son un subconjunto de las columnas disponibles en la vista Servicios.

6. 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 Administration.
 - Use la pestaña **Grupos** para seleccionar grupos de servicios



7. Haga clic en **Siguiente**.

Se muestra la página **Análisis**.



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

- Haga clic en **Implementar**.

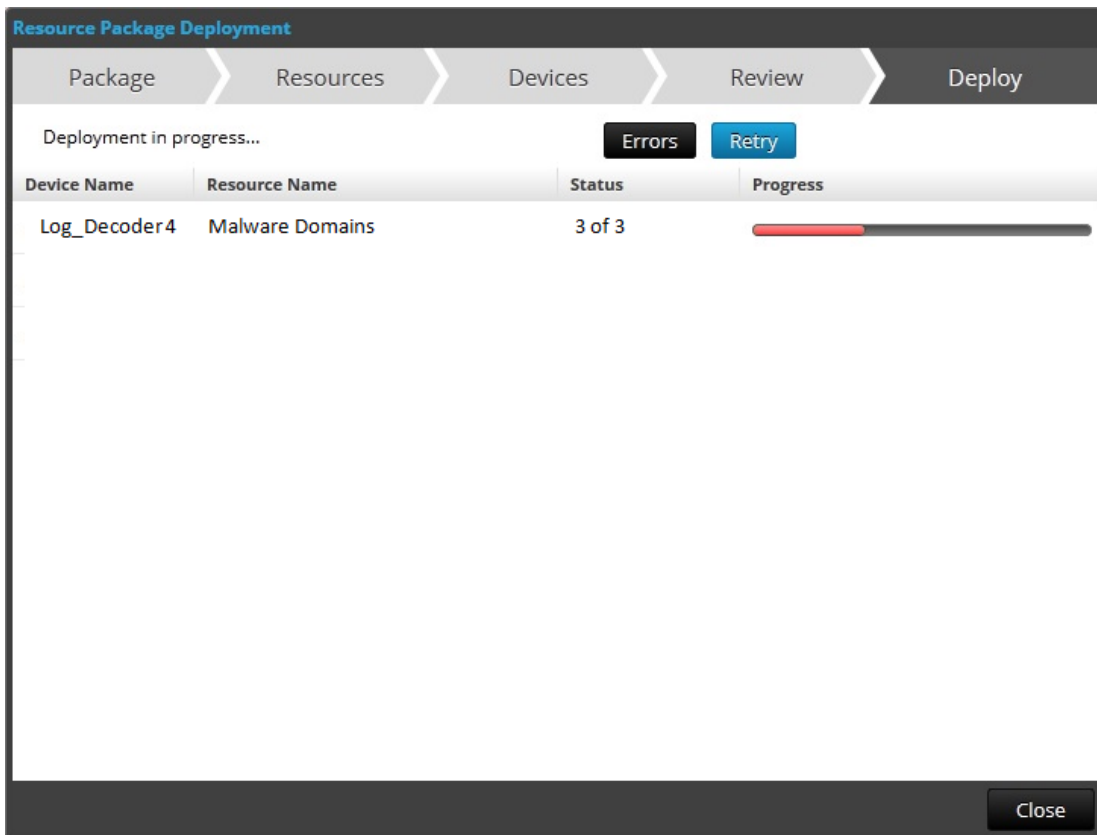
Se muestra la página **Implementar**. La barra de progreso se vuelve verde cuando los recursos se implementan correctamente en los servicios seleccionados.

The screenshot shows the 'Deployment Wizard' interface with four steps: Resources, Services, Review, and Deploy. The 'Deploy' step is active. A message states 'Live deployment task finished successfully'. Below this is a table with the following data:

Service Name	Resource Name	Status	Progress
SA UI Endpoint	Basic Rule Template	1 of 1	

A 'Close' button is located at the bottom right of the wizard.

Si intenta implementar recursos y servicios que no son compatibles, Security Analytics muestra los botones **Errors** y **Retry** en los cuales puede hacer clic para revisar los errores y volver a intentar la implementación.



9. Haga clic en Close.

Implementar recursos desde un paquete de recursos

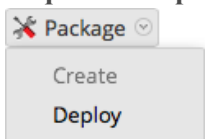
En este tema se indica cómo implementar recursos desde un paquete de recursos con el [Asistente Implementación de paquete de recursos](#).

Después de completar este procedimiento, habrá implementado recursos desde un paquete de recursos creado previamente y guardado en la red. Consulte [Crear un paquete de recursos](#) para obtener instrucciones sobre cómo crear un paquete.

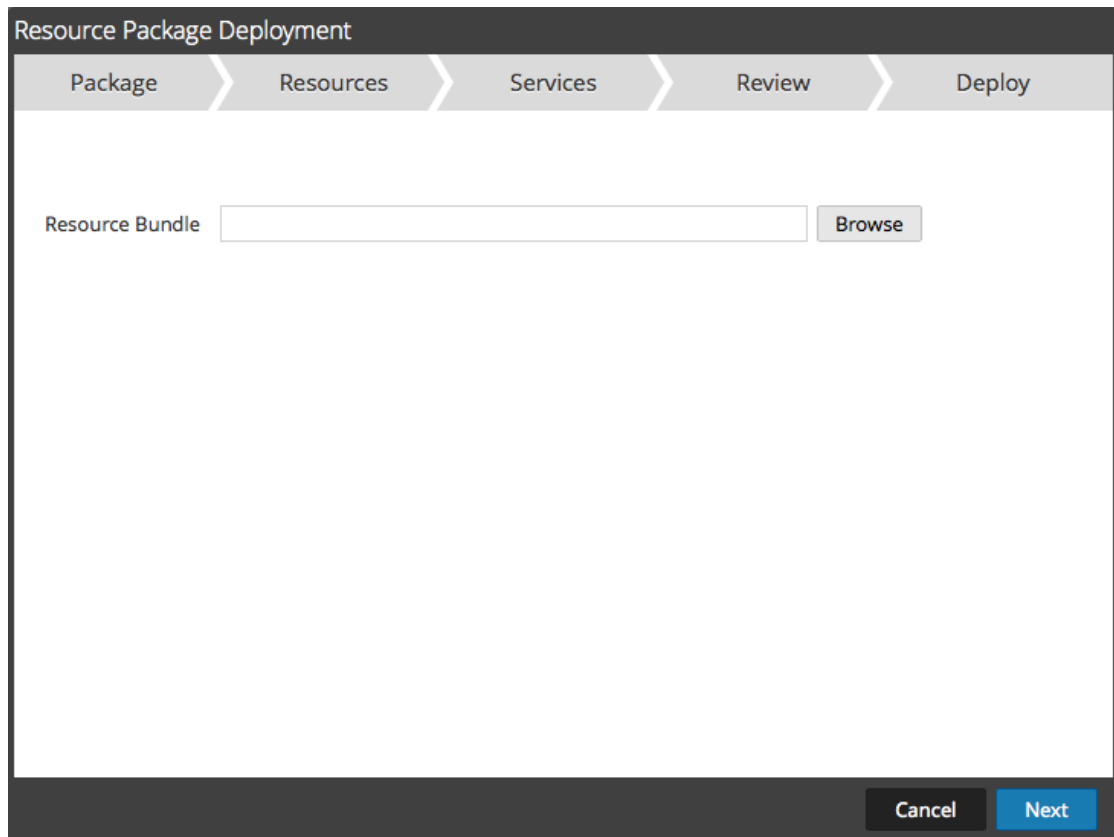
Nota: El permiso necesario para obtener acceso a esta vista es **Implementación de recursos de Live**.

Para implementar recursos desde un paquete de recursos:

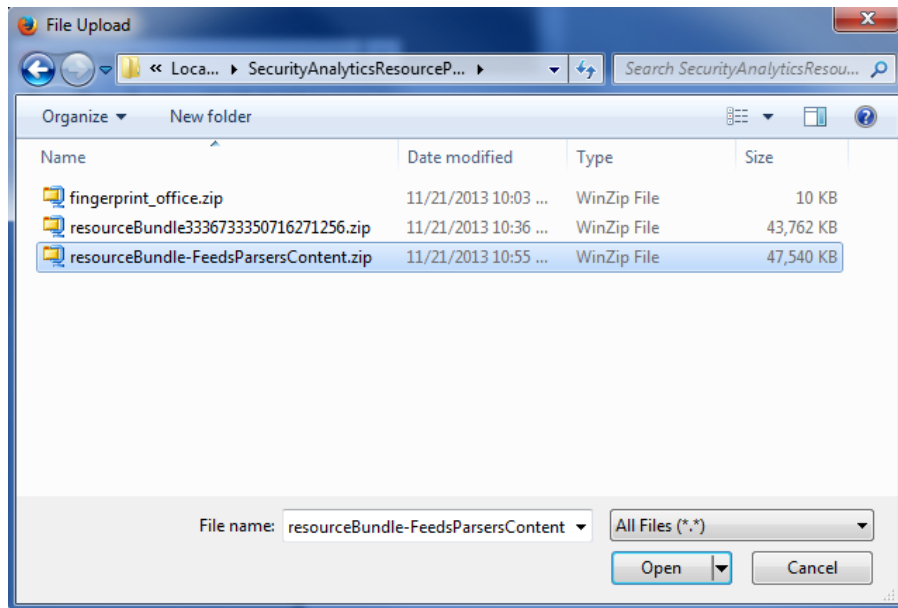
1. En la vista **Buscar en Live**, barra de herramientas **Coincidencias de recursos**, seleccione **Paquete > Implementar**:



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

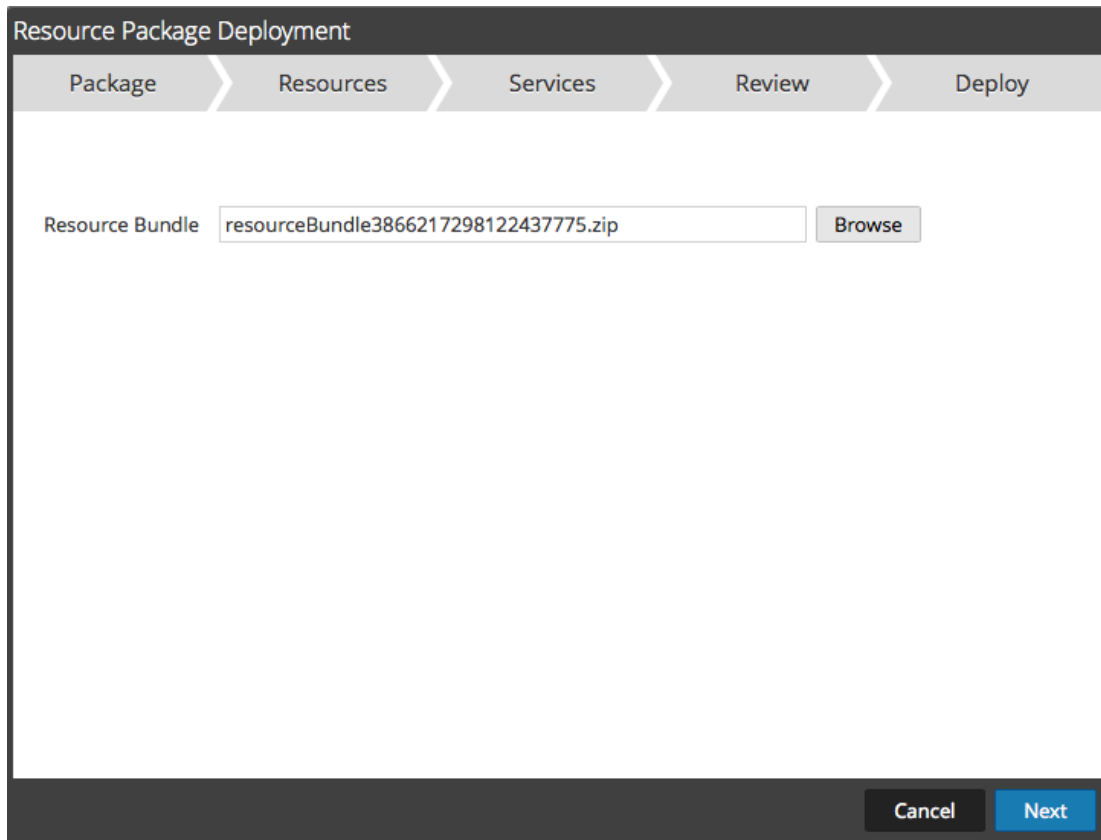


2. Haga clic en **Browse** y seleccione un paquete de la red (por ejemplo **resourceBundle-FeedsParsersContent.zip**).



3. Haga clic en **Abrir**.

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



4. Haga clic en **Siguiente**.

Se muestra la página **Recursos**.

The screenshot shows a wizard titled "Resource Package Deployment" with five steps: Package, Resources, Services, Review, and Deploy. The "Resources" step is currently active. Below the step indicators, it states "Total resources : 2". A table lists the resources:

Resource Names	Resource Type	Dependency Of
suspicious php put long query	RSA Application Rule	
APT Domain Intelligence	RSA Application Rule	

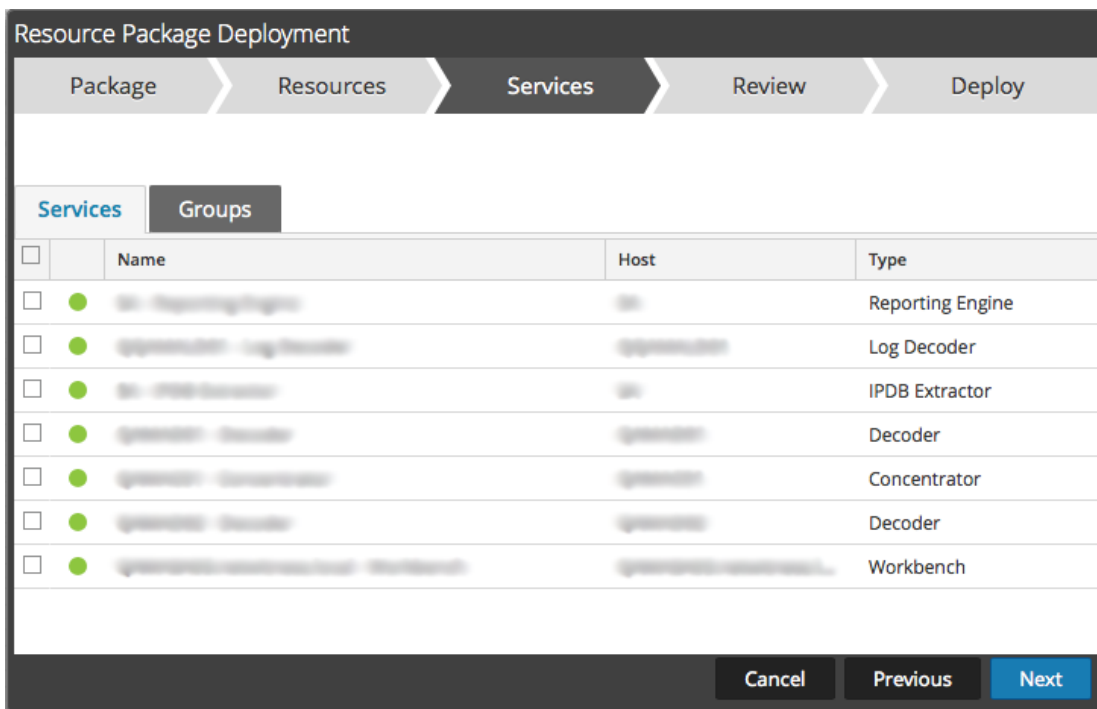
At the bottom right of the wizard, there are two buttons: "Cancel" and "Next".

5. Haga clic en **Siguiente**.

Se muestra la página **Servicios**.

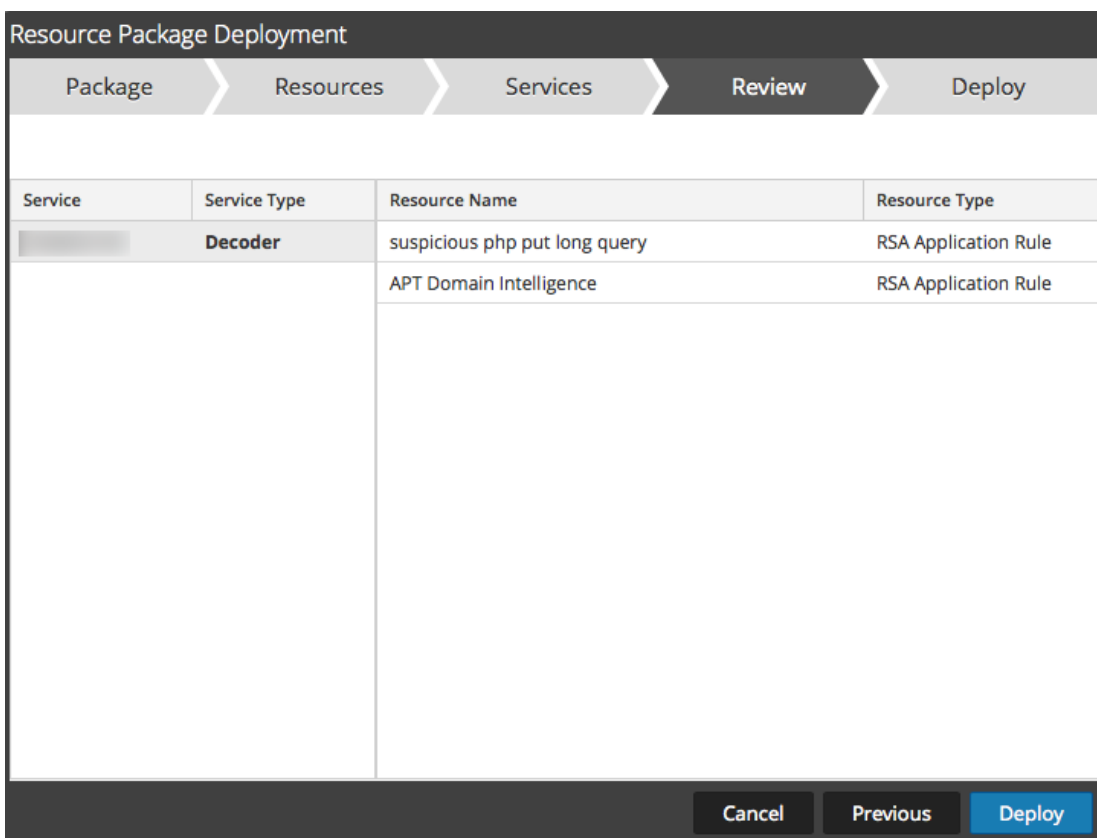
La página **Servicios** tiene dos pestañas, **Servicios** y **Grupos**, las cuales proporcionan una lista de servicios y grupos de servicios que se configuran en la vista **Administration > Servicios**.

6. 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 Administration.
 - Use la pestaña **Grupos** para seleccionar grupos de servicios.



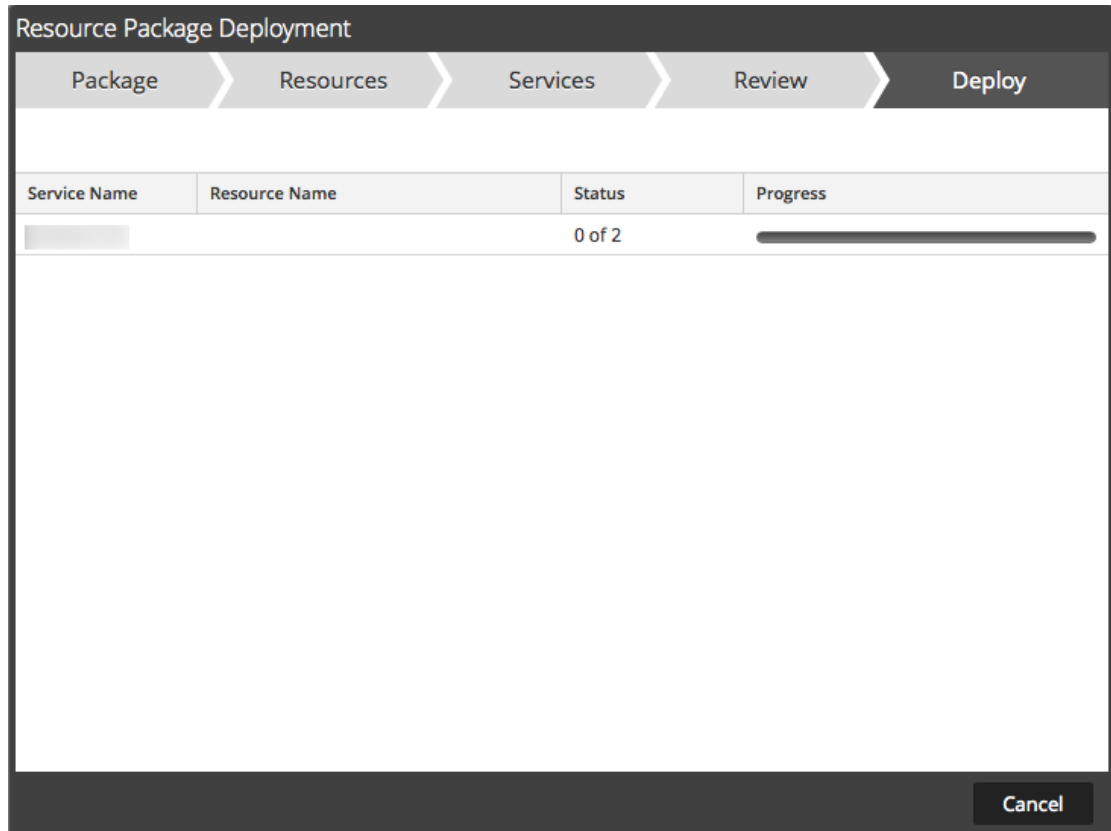
7. Haga clic en **Siguiente**.

Se muestra la página **Análisis**.



8. Asegúrese de haber seleccionado los recursos correctos y los servicios en los cuales desea implementarlos.
9. 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, Security Analytics muestra los botones **Errors** y **Retry** en los cuales puede hacer clic para revisar los errores y volver a intentar la implementación.

10. Haga clic en **Close**.


Implementar recurso en servicios

En este tema se indica cómo implementar un recurso seleccionado en la [Vista Recurso de Live](#) en servicios mediante el [Asistente Implementación de paquete de recursos](#).

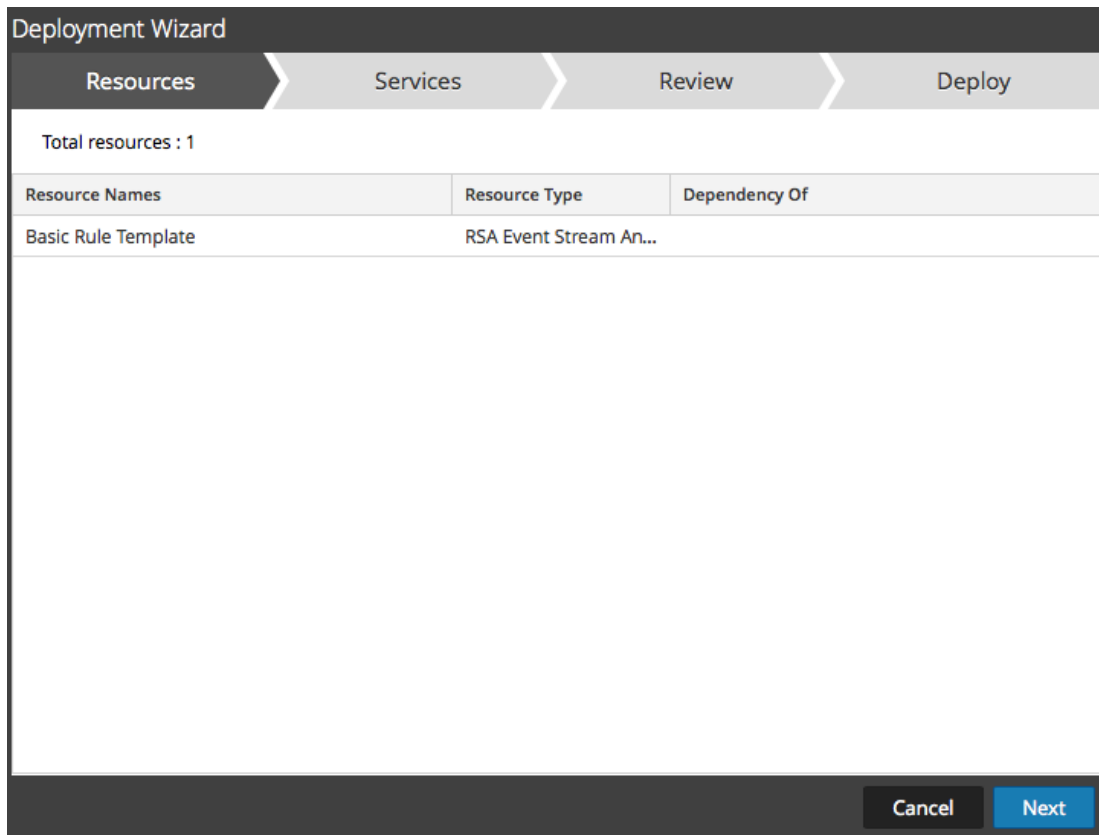
Después de completar este procedimiento, habrá implementado un recurso seleccionado en la vista Recursos de Live para servicios que utilizan el asistente de implementación.

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

Para implementar recursos mediante el asistente:

1. En el menú de **Security Analytics**, seleccione **Live > Buscar > Tipos de recursos**.
2. Ingrese los criterios de búsqueda y haga clic en **Buscar**.
3. En el panel **Coincidencias de recursos**, seleccione un recurso.
4. En la barra de herramientas Coincidencias de recursos, haga clic en  **Deploy**.

El **Asistente de implementación** abre la página **Recursos**.



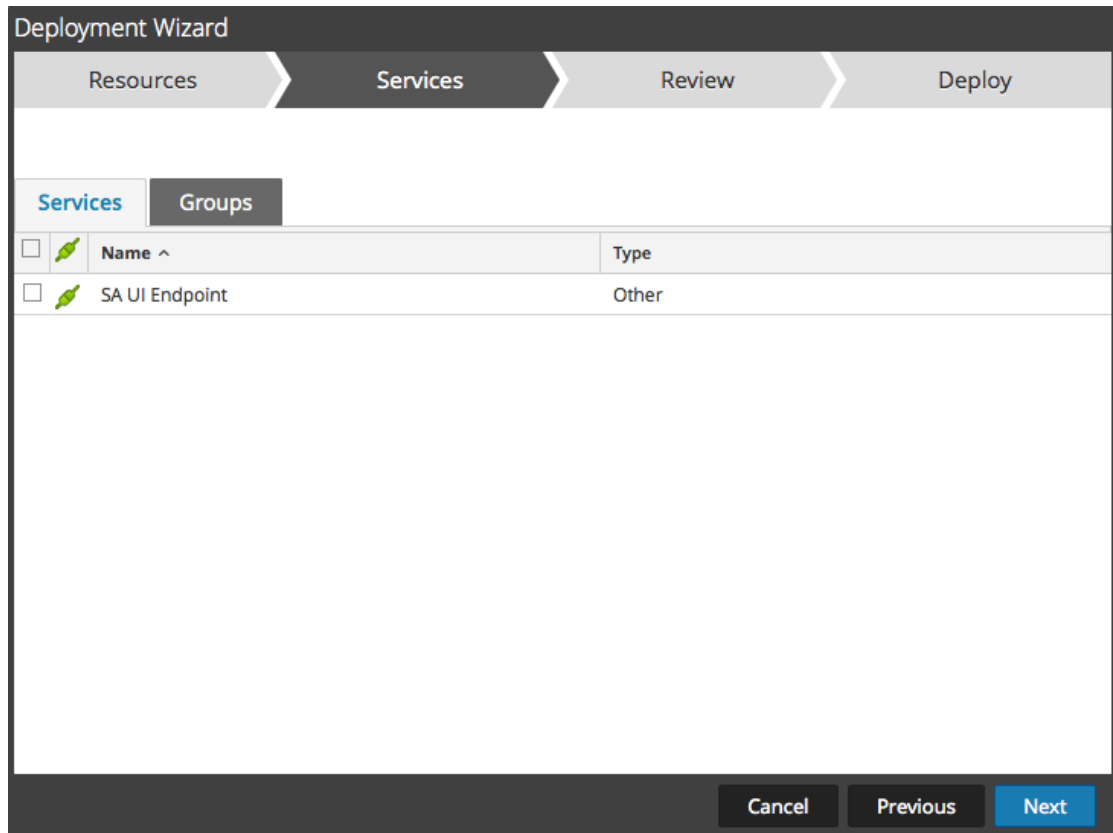
5. Haga clic en **Siguiente**.

Se muestra la página **Servicios**.

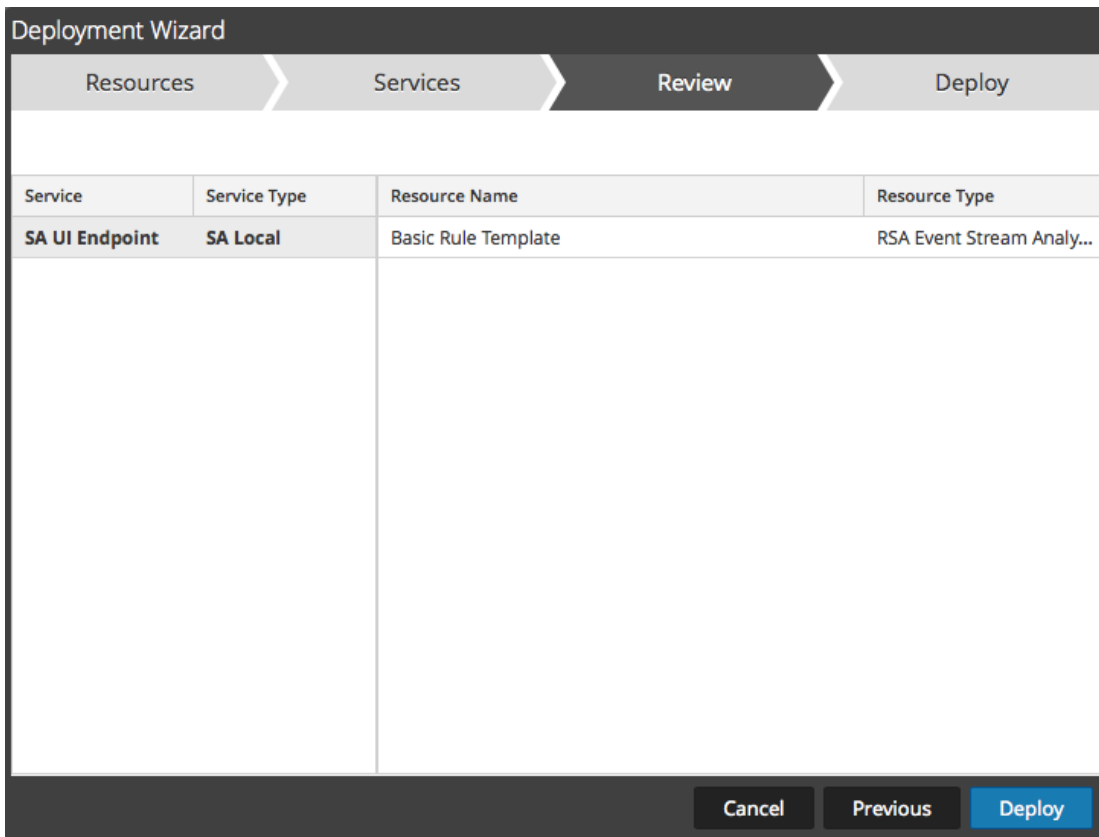
La página **Servicios** tiene dos pestañas, **Servicios** y **Grupos**, las cuales proporcionan una lista de servicios y grupos de servicios que se configuran en la vista **Administration > Servicios**. Las columnas son un subconjunto de las columnas disponibles en la vista **Servicios**.

6. 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 Administration.
- Use la pestaña **Grupos** para seleccionar grupos de servicios



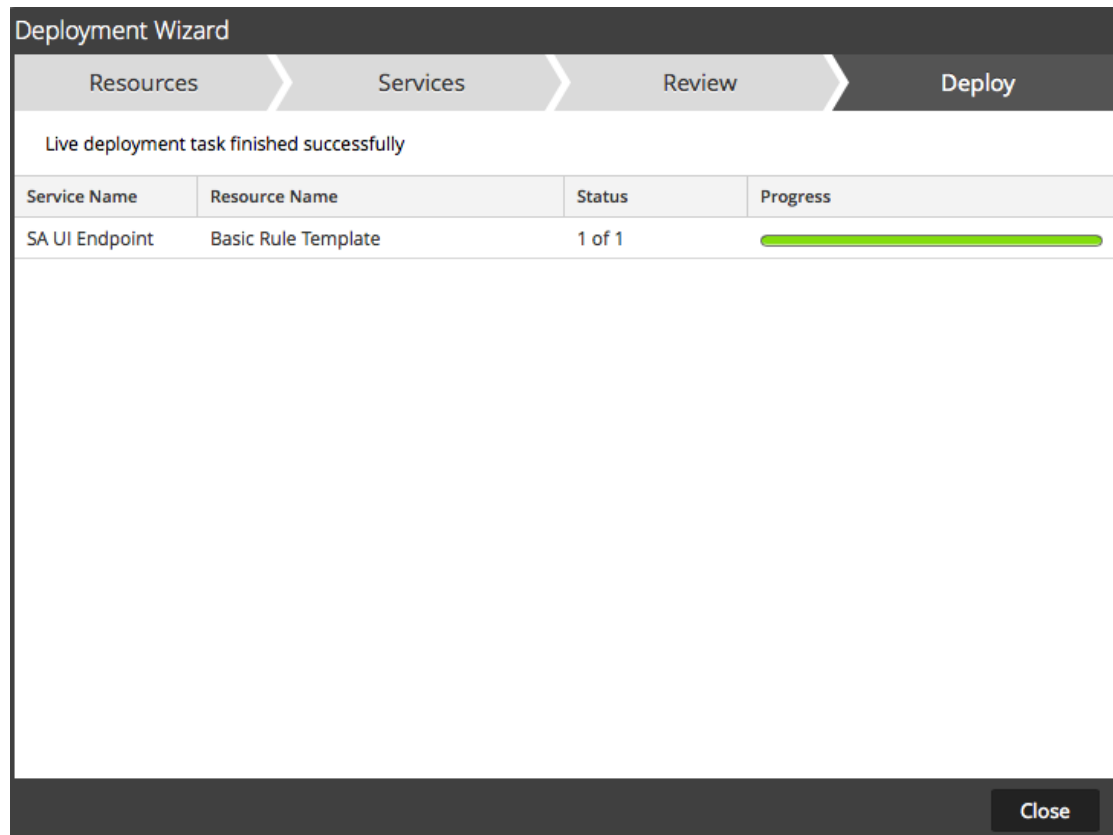
7. Haga clic en **Siguiente**.
Se muestra la página **Análisis**.



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

8. Haga clic en **Implementar**.

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



9. Haga clic en **Close**.

Implementar recursos de Live mediante el Asistente de implementación

Un requisito previo para esta tarea es la configuración y sincronización entre el servidor de CMS y Security Analytics, y la capacidad de buscar recursos de Live.

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

Para acceder al asistente de implementación:

1. En la vista **Buscar en Live**, navegue por los recursos de Live.
2. En el panel **Coincidencias de recursos**, seleccione **Mostrar resultados > Cuadrícula**.

The screenshot displays the RSA Security Analytics interface. On the left, the 'Search Criteria' panel includes fields for Keywords, Resource Types (with selected options: RSA CEP Module, RSA Feed, RSA FlexParser, RSA Investigator Custom Action), Tags, Required Meta Keys, Generated Meta Values, Resource Created Date (with Start and End Date pickers), and Resource Modified Date (with Start and End Date pickers). A 'Search' button is at the bottom of this panel. The main area, 'Matching Resources', shows a table of results with columns: Subscribed, Name, Created, Updated, Type, and Description. The table lists various resources such as 'SRI Attackers', 'RSA FirstWatch Criminal Socks...', 'SpyEye Tracker', 'SpyEye Domain Tracker', 'RSA FirstWatch APT Threat Do...', 'RSA FirstWatch Criminal VPN E...', 'Malware Domains', 'RSA FirstWatch APT Threat IPs', 'RSA FirstWatch Exploit IPs', 'RSA FirstWatch Exploit Domains', 'RSA FirstWatch Criminal SOCKS...', 'Palevo Tracker Domains', 'Spamhaus EDROP List IP Ranges', 'IDefense Threat Indicators Do...', 'Zeus Tracker', and 'Zeus Domain Tracker'. Each row has a checkbox in the 'Subscribed' column. Below the table, it indicates '213 Matching Resources'. The top navigation bar includes 'Live', 'Search', 'Configure', 'Feeds', and 'RSA Security Analytics'. The bottom status bar shows 'admin | English (United States) | GMT-05:00' and 'Send Us Feedback'.

3. Seleccione el recurso que desee implementar.

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

Exportar datos a RSA

En este tema se proporcionan instrucciones para que un administrador de Security Analytics exporte las métricas en Security Analytics 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*.

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

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

Descargar datos históricos de Live Feedback

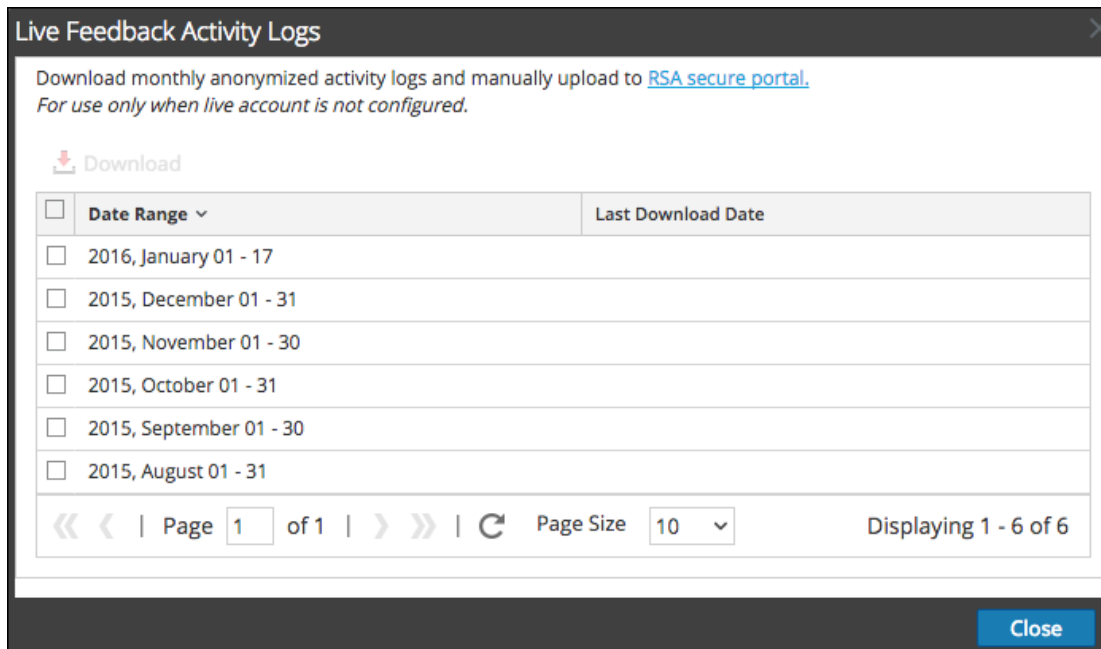
Para descargar los datos históricos de Live Feedback:

1. En el menú de **Security Analytics**, seleccione **Administration > 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 actividad de Live Feedback**, la cual permite que el usuario de Security Analytics descargue los datos históricos requeridos de Live Feedback.



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

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

Los datos descargados de Live Feedback están en formato JSON y se encuentran empaquetados como un archivo .zip. Para obtener más información, consulte el tema **Descripción general de Live Feedback** de la *Guía de configuración del sistema*.

Compartir datos en RSA

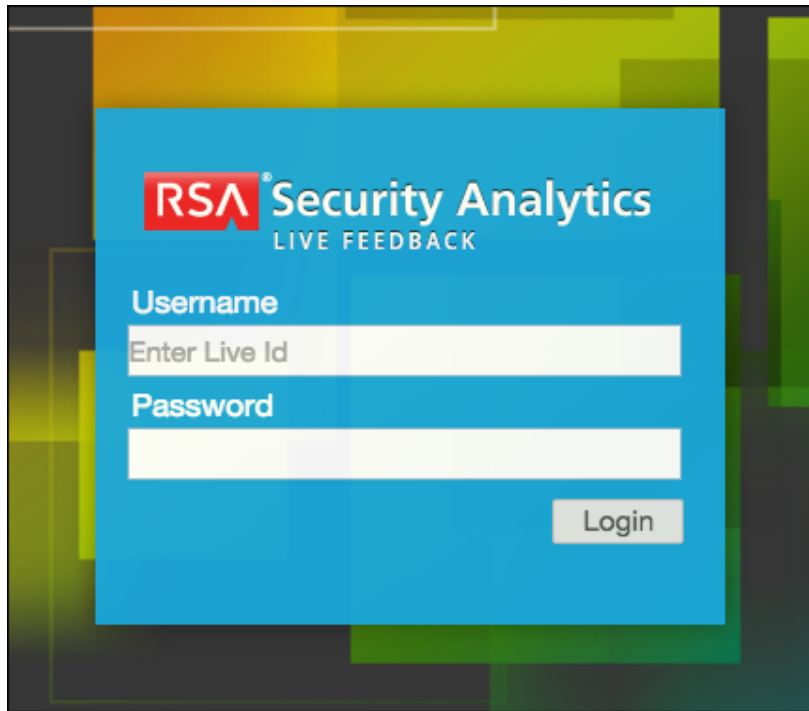
Después de descargar los datos de Live Feedback, puede cargarlos mediante el siguiente procedimiento.

Para compartir los datos en RSA:

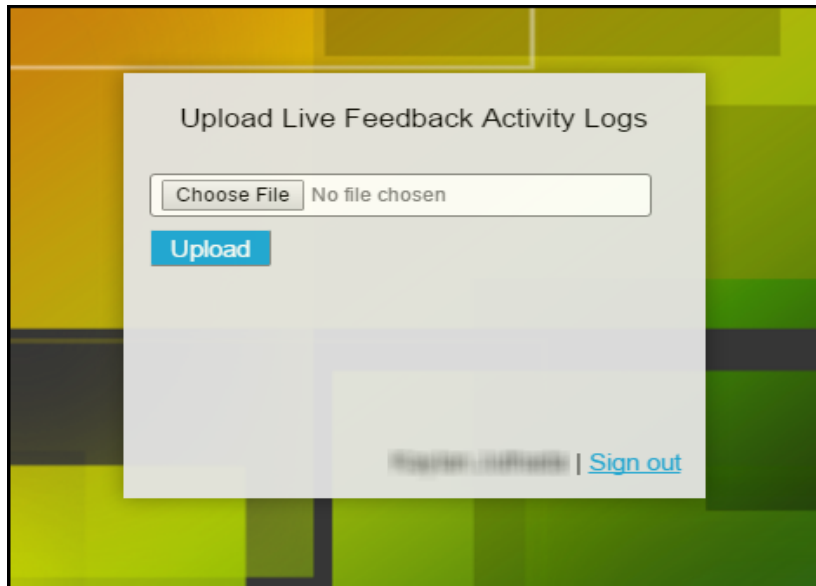
1. Haga clic en el **Portal seguro de RSA** disponible en la ventana **Registros de actividad de Live Feedback**.

Aparece la pantalla de inicio de sesión de RSA Security Analytics 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 Feed personalizado en RSA Security Analytics con el fin de completar rápidamente los Decoders con feeds personalizados y de identidad.

Creación de feeds personalizados

Se utiliza **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 feeds en RSA Security Analytics tienen el formato `<filename>.feed`. Para crear un feed, Security Analytics requiere un archivo de **datos** de feed en el formato `.csv` y un archivo de **definición** de feed en el formato `.xml`, el cual describe la estructura de un archivo de datos de feed. 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 a petición 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 Security Analytics pueda buscar la versión más reciente del archivo para cada recurrencia. Después de la creación de un feed de Security Analytics, puede descargarlo al sistema de archivos local, editar sus archivos y, a continuación, editar el feed de Security Analytics 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 Security Analytics crea en función de las entradas de los asistentes de feed. Define la estructura del archivo de datos del feed llamado **dynamic_dns.csv**.

```
<?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>

<Campos>
<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 Feeds de Security Analytics 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 Security Analytics	Equivalente en el archivo de definición del feed
---------------------------------	--

Pestaña Definir feed

Tipo de tarea de feed	Seleccione: Ad hoc : para crear un feed según demanda. Recurrente : para crear un feed que se repite automáticamente.
-----------------------	---

Parámetro de Security Analytics	Equivalente en el archivo de definición del feed
Nombre	El nombre del feed personalizado en el archivo de datos del feed. Corresponde al atributo <code>flatfeedfile name</code> 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 <code>flatfeedfile path</code> en el archivo de definición del feed; por ejemplo, <code>dynamic_dns.csv</code> .
Pestaña Definir feed: Opciones avanzadas	
Archivo de feed XML	El nombre del archivo de definición del feed, por ejemplo, <code>dynamic_dns.xml</code> .
Separador	El carácter separador que se utiliza para separar atributos en el archivo de datos del feed. Corresponde al atributo <code>flatfeedfile separator</code> en el archivo de definición del feed; por ejemplo, una coma.
Comentario	El carácter que se utiliza para identificar un comentario en el archivo de datos del feed. Corresponde al atributo <code>flatfeedfile comment</code> en el archivo de definición del feed; por ejemplo, <code>#</code> .
Pestaña Seleccionar servicios	Seleccione los servicios a los cuales desea enviar el feed de datos.

Parámetro de Security Analytics	Equivalente en el archivo de definición del feed
(Pestaña Definir columnas, Definir índice) Tipo	<p>El tipo de valor de búsqueda en la posición del índice del archivo de datos de feed.</p> <p>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).</p> <p>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.</p>
(Pestaña Definir columnas, Definir índice) CIDR	<p>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).</p>
(Pestaña Definir columnas, Definir índice) Tipo de servicio	<p>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.</p>

Parámetro de Security Analytics	Equivalente en el archivo de definición del feed
(Pestaña Definir columnas, Definir índice) 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 <code>www.example.com</code> , se trunca a <code>example.com</code> . Con un valor Falso se selecciona sin truncamiento y con un valor Verdadero , truncamiento.
(Pestaña Definir columnas, Definir índice) Claves de callback	En un índice No IP, se pueden seleccionar en la lista desplegable las claves de metadatos disponibles para coincidencia en lugar de <code>ip.src/ip.dst</code> (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.
(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.

Parámetro de Security Analytics	Equivalente en el archivo de definición del feed
(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](#)
- [Eliminar un feed](#)

Crear un feed personalizado

Puede crear fácilmente un feed personalizado mediante el asistente Feed personalizado. Para realizar este procedimiento, necesita un archivo de datos de feed en formato `.csv`. 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.

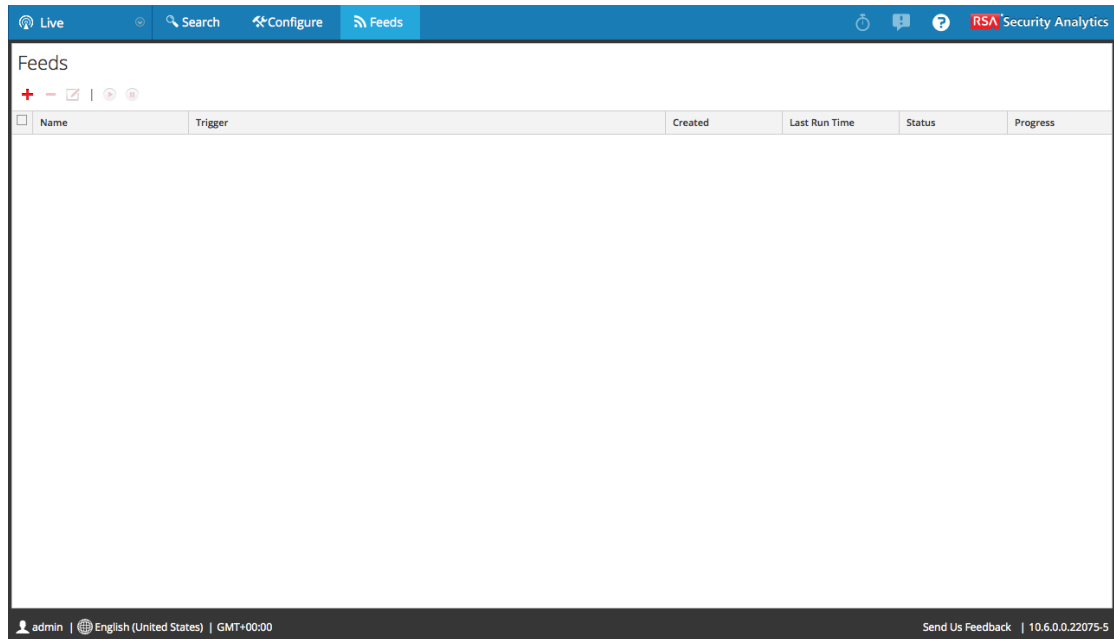
Después de realizar este procedimiento, habrá creado un feed personalizado.

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

Para crear un feed personalizado:

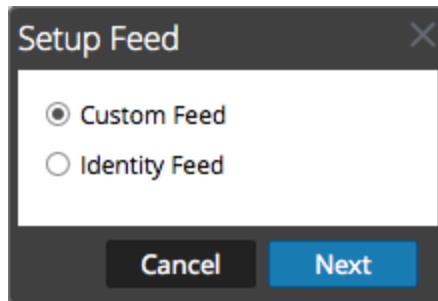
1. En el menú de **Security Analytics**, seleccione **Live > Feeds**.

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.

Configure a Custom Feed

Define Feed | Select Services | Define Columns | Review

Feed Task Type Adhoc Recurring

Name *

File *

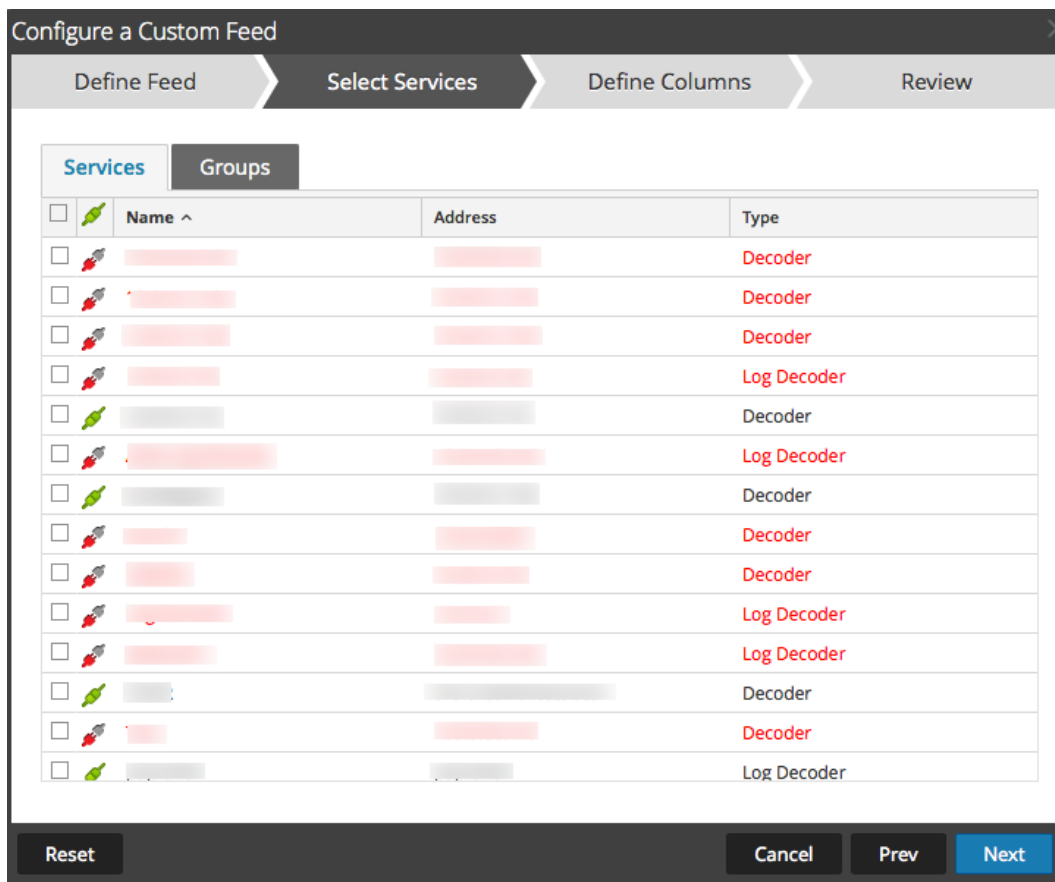
— Advanced Options —

4. 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:

The screenshot shows a dialog box titled "Configure a Custom Feed" with a close button (X) in the top right corner. The dialog has four tabs: "Define Feed" (active), "Select Services", "Define Columns", and "Review". Under "Define Feed", there are two radio buttons for "Feed Task Type": "Adhoc" (selected) and "Recurring". Below this are two text input fields: "Name *" containing "Test" and "File *" containing "testprange.csv". To the right of the "File *" field is a "Browse" button. Below the input fields is a section titled "Advanced Options" with a downward arrow icon. At the bottom of the dialog are four buttons: "Reset", "Cancel", "Prev", and "Next".

- 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.



5. 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**.

Security Analytics verifica la ubicación en la cual está almacenado el archivo con el fin de 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**.

Security Analytics proporciona su nombre de usuario y contraseña con fines de autenticación en la dirección URL.

- d. Si desea que el servidor de Security Analytics 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 **Configure el proxy de Security Analytics** 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 días para la ejecución recurrente del feed, especifique la hora y la **Fecha inicial** y la hora y la **Fecha de finalización**.

The screenshot shows a dialog box titled "Configure a Custom Feed" with a close button (X) in the top right corner. The dialog has four tabs: "Define Feed" (active), "Select Services", "Define Columns", and "Review".

Under "Define Feed", the "Feed Task Type" is set to "Recurring" (radio button selected). The "Name" field contains "TestFeed". The "URL" field contains "https://qasa2.netwitness.local/live/feeds" and has a "Verify" button to its right. There are checkboxes for "Authenticated" and "Use proxy", both of which are unchecked. The "Recur Every" field is set to "3" and the unit is "Day (s)".

Below these fields is a "Date Range" section with a dropdown arrow. An "Advanced Options" section is expanded, showing an "XML Feed File" field with a "Select File" button and a "Browse" button. The "Separator" field contains a comma (,) and the "Comment" field contains a hash symbol (#).

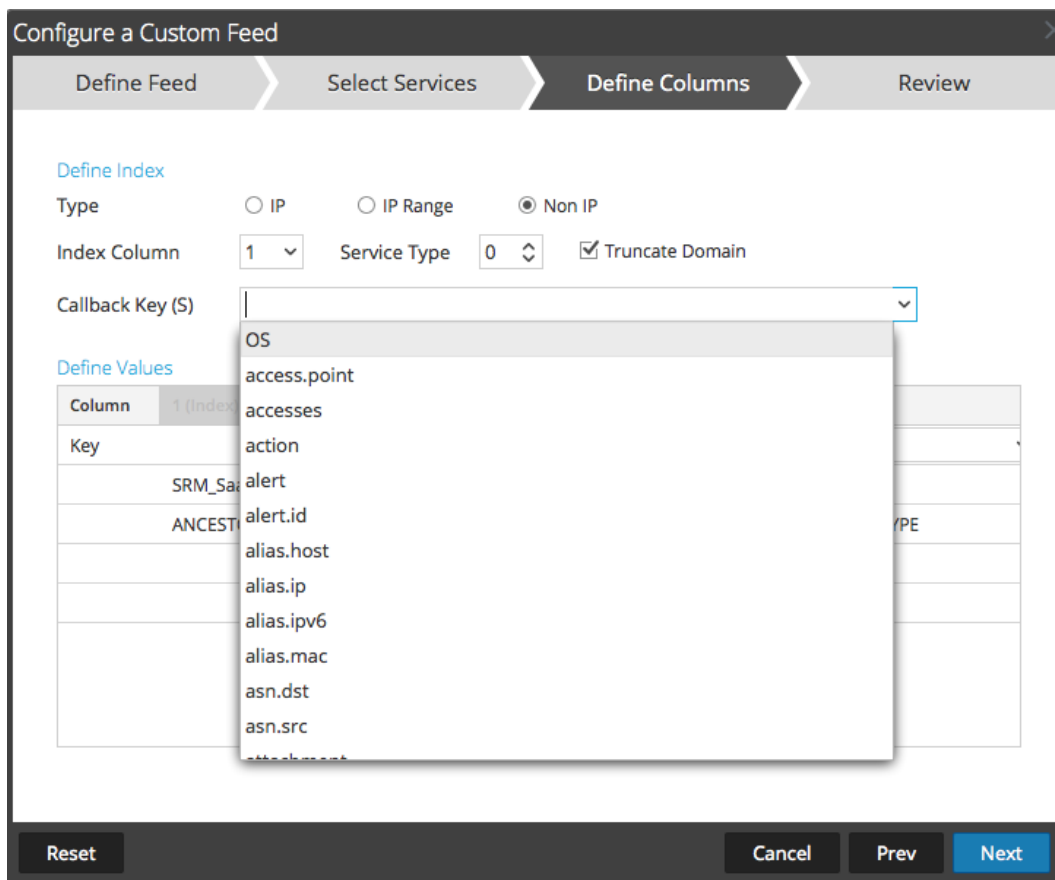
At the bottom of the dialog are four buttons: "Reset", "Cancel", "Prev", and "Next".

6. (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.

<input type="checkbox"/>		Name ^	Address	Type
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Log Decoder
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Log Decoder
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Log Decoder
<input type="checkbox"/>				Log Decoder
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Decoder
<input type="checkbox"/>				Log Decoder

7. 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.
8. 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.

Configure a Custom Feed
✕

Define Feed
Select Services
Define Columns
Review

Define Index

Type IP IP Range Non IP

Index Column Service Type Truncate Domain

Callback Key (S)

Define Values

Column	1 (Index)	2	3	4
Key		threat.source	threat.category	threat.desc
	SRM_SaaS_ES	MXASSETInterface	AddChange	EN
	ANCESTOR	ASSETNUM	ASSETTAG	ASSETTYPE
		cent45	9164	
		cent45	9164	

Reset
Cancel
Prev
Next

- e. Haga clic en **Siguiente**.
Se muestra el formulario Revisión.

Configure a Custom Feed

Define Feed | Select Services | Define Columns | **Review**

Feed Details

Name: Testing
 CSV File: AssetsImportCompleteSample.csv

Service Details

Services: Log Decoder, Decoder

Column Mapping Details

Index Type: Other
 Callback Key(s): action
 Truncate Domain: true
 Service Type: 0

Value Columns

1 Index	2 threat.source	3 threat.category	4 threat.desc
------------	--------------------	----------------------	------------------

Reset | Cancel | Prev | **Finish**

9. 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).
10. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.
11. 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.

Name	Trigger	Created	Last Run Time	Status	Progress
Testing	Once	2014-08-21 18:30:46	2014-08-21 18:30:46	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>

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.

Requisitos previos

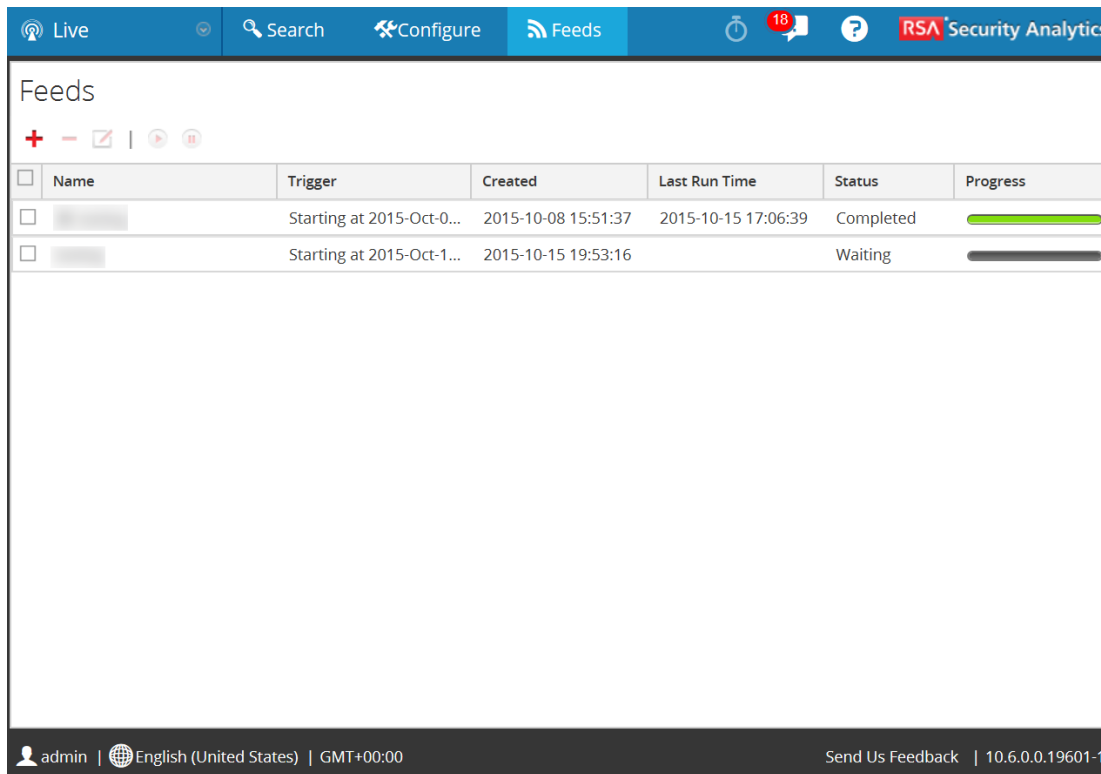
Para crear un feed de identidad, debe tener:

- Un servicio Log Collector con un procesador de eventos de feed de identidad
- Un servicio Log Collector con la recopilación de Windows configurada y habilitada.

Crear un feed de identidad

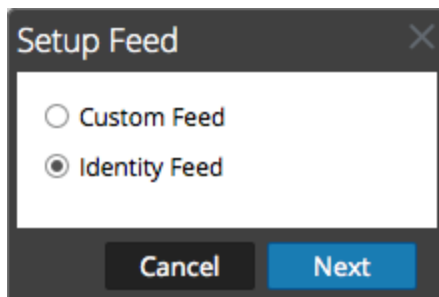
1. En el menú de **Security Analytics**, seleccione **Live > Feeds**.

Se muestra la cuadrícula Feeds.



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

El cuadro de diálogo Configurar feed se muestra con la opción Feed de identidad seleccionada de manera predeterminada.



3. Seleccione **Feed de identidad** y haga clic en **Siguiente**.

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

4. (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.

The screenshot shows a 'Configure Identity Feed' dialog box with three tabs: 'Define Feed', 'Select Services', and 'Review'. The 'Define Feed' tab is active. It contains the following fields and controls:

- Feed Task Type:** Radio buttons for 'Adhoc' and 'Recurring' (selected).
- Name *:** A text input field.
- URL *:** A text input field containing the example URL: `>r name]?msg=getFile&force-content-type=application/octet-stream&expiry=600`. A 'Verify' button is to the right.
- Authentication:** A checked checkbox for 'Authenticated'. To its right are 'User Name' (input field with 'admin') and 'Password' (input field with masked characters).
- Use proxy:** An unchecked checkbox.
- Recur Every:** A spinner set to '5' and a dropdown menu set to 'Minute (s)'.
- Date Range:** A section with a 'Date Range' header, 'Start Date' (calendar icon, value: 2015-12-14 19:10:25), and 'End Date' (calendar icon, value: 2015-12-14 13:11:27).

At the bottom of the dialog are four buttons: 'Reset', 'Cancel', 'Prev', and 'Next'.

Nota: Security Analytics verifica la ubicación en la cual está almacenado el archivo con el fin de comprobar automáticamente el archivo más reciente antes de cada recurrencia.

En el campo **URL**, escriba la dirección URL en la cual está ubicado el archivo de datos del feed. Por ejemplo:

```
http://<LogCollector>:50101/event-
processors/<ID Event processor name>?msg=getFile&force-
content-type=application/octet-stream&expiry=600
```

- (Opcional) Si la URL tiene acceso restringido y se solicita autenticación con nombre de usuario y contraseña, seleccione **Autenticado**. Security Analytics proporciona a la dirección URL su nombre de usuario y contraseña con fines de autenticación.
- 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**.
7. Haga clic en **Verificar** para verificar su configuración de feed de identidad antes de continuar con el formulario Seleccionar servicios.
 8. Haga clic en **Siguiente**.

Se muestra el formulario Seleccionar servicios.

The screenshot shows a dialog box titled "Configure Identity Feed" with a close button (X) in the top right corner. The dialog has three tabs: "Define Feed", "Select Services", and "Review". The "Select Services" tab is active. Below the tabs, there are two sub-tabs: "Services" (selected) and "Groups". Under "Services", there is a table with the following columns: "Name ^", "Address", and "Type". The table contains two rows of data:

<input type="checkbox"/>		Name ^	Address	Type
<input type="checkbox"/>		192.168.1.1 Decoder	192.168.1.1	Decoder
<input type="checkbox"/>		192.168.1.1 Log Decoder	192.168.1.1	Log Decoder

At the bottom of the dialog, there are four buttons: "Reset", "Cancel", "Prev", and "Next". The "Next" button is highlighted in blue.

9. Para identificar los servicios en los cuales se implementará el feed, seleccione uno o más Decoders y Log Decoders, y haga clic en **Siguiente**.
10. Haga clic en la pestaña **Grupos**, seleccione un grupo y haga clic en **Siguiente**.
Se muestra el formulario Revisión.

Configure Identity Feed

Define Feed | Select Services | **Review**

Feed Details

Name	Testing
Feed File	zip sample.zip

Service Details

Services	Decoder
----------	---------

Reset | Cancel | Prev | **Finish**

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.

11. 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).
12. 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.

<input type="checkbox"/>	Name	Trigger	Created	Last Run Time	Status	Progress
<input type="checkbox"/>	[Redacted]	Starting at 2015-Oct-0...	2015-10-08 15:51:37	2015-10-15 17:06:39	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>
<input type="checkbox"/>	[Redacted]	Starting at 2015-Oct-1...	2015-10-15 19:53:16		Waiting	<div style="width: 0%; height: 10px; background-color: gray;"></div>

admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.6.0.0.19601-1

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.

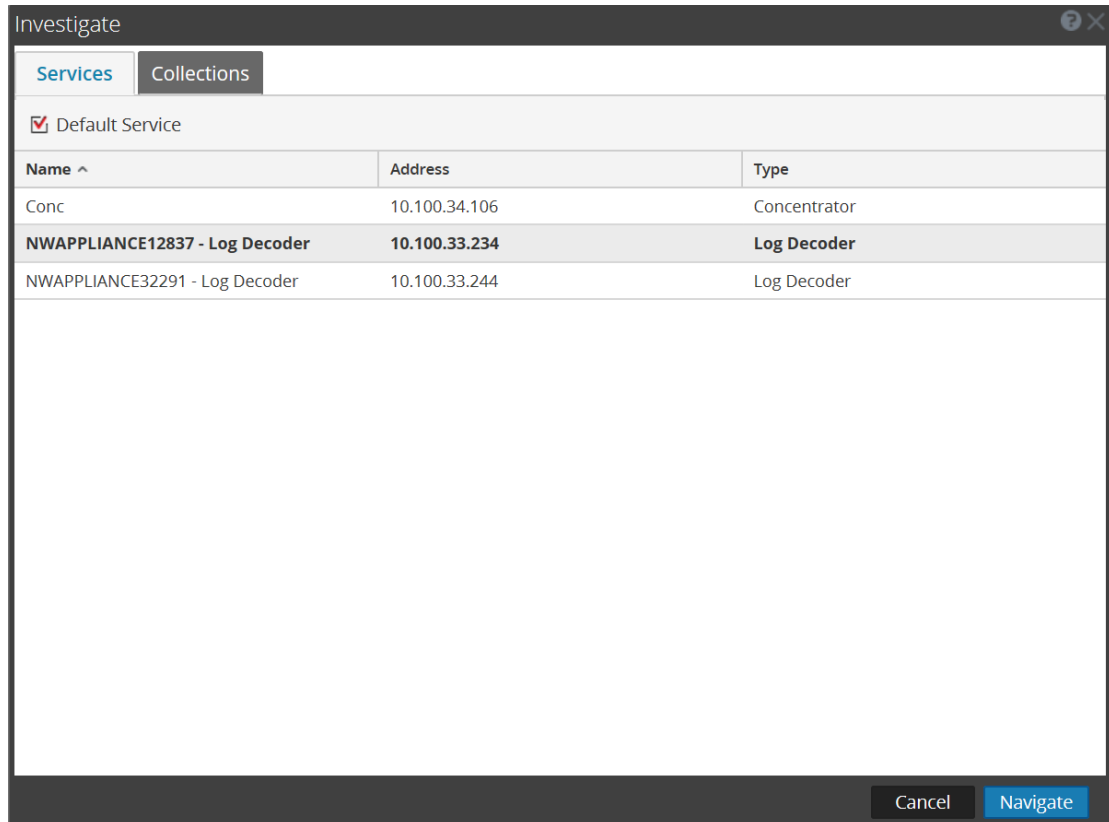
Para que un feed de identidad procese eventos y los etiquete, los eventos deben recopilarse mediante un módulo de recopilación de registros de Windows, en el cual se configura una controladora de dominio/controladora no de dominio activa. Tenga en cuenta que los feeds de identidad solo pueden procesarse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

Para investigar una feed de identidad configurado:

1. Vaya al menú de Security Analytics.
2. Seleccione **Investigar > Navegar**.
Se muestra la pantalla Investigation.



3. Seleccione **Conc** (Concentrator) y, a continuación, **Navegar**.
4. Seleccione **Cargar valores** para recuperar las claves de metadatos.

En el panel inferior, 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 investigar.

Editar un feed

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

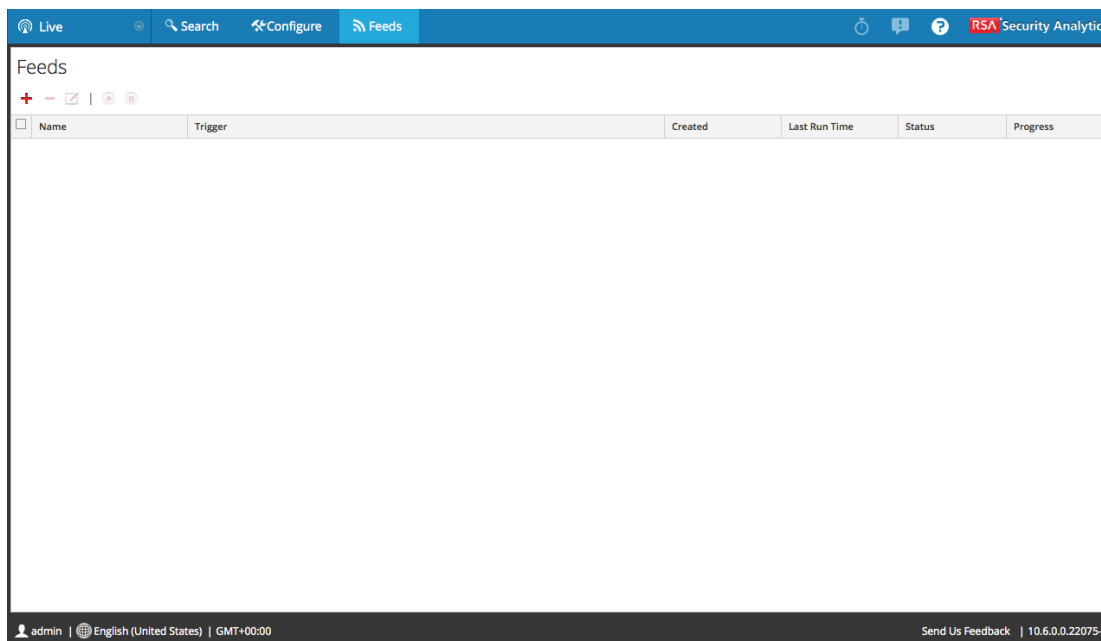
Si se realiza este procedimiento, se logrará:

- 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. En el menú de **Security Analytics**, seleccione **Live > Feeds**.

Se muestra la vista Feeds.



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.

Configure Identity Feed

Define Feed | Select Services | Review

Feed Task Type Adhoc Recurring

Name *

File *

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 cuadrícula Feed. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles se ejecutaron correctamente.

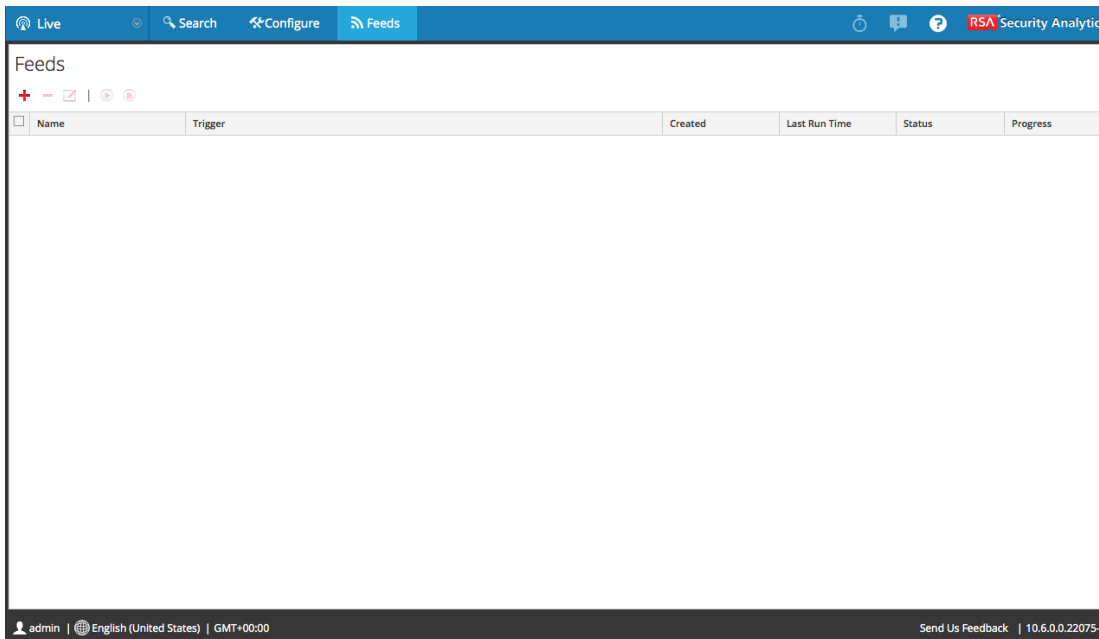
Eliminar un feed


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

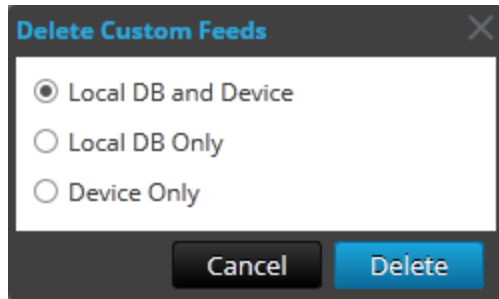
Para eliminar un feed:

1. En el menú de **Security Analytics**, seleccione **Live > Feeds**.

Se muestra la vista Feeds.



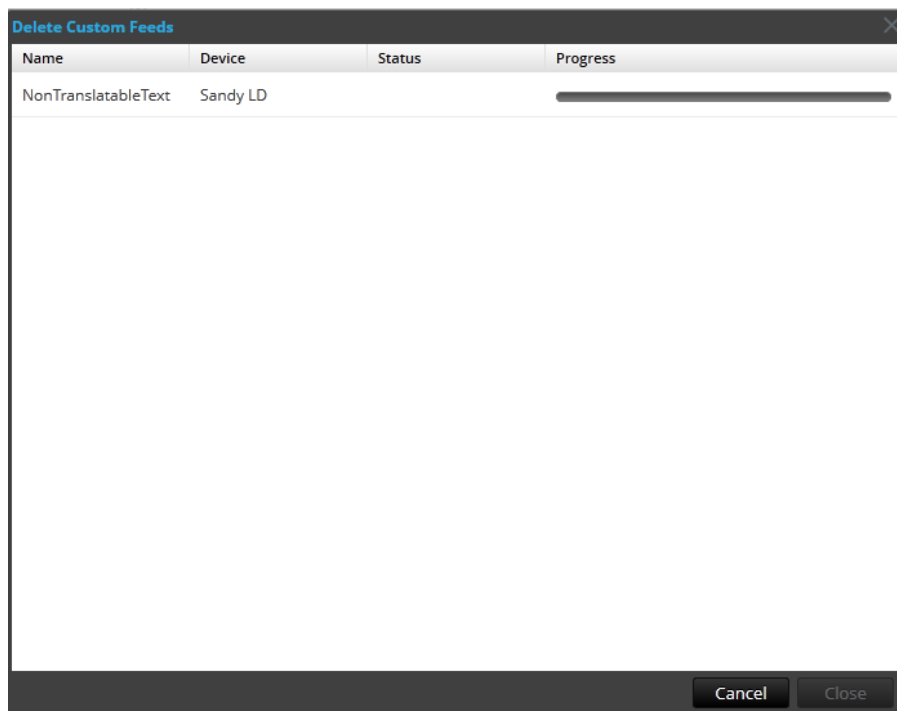
2. En la barra de herramientas, seleccione un feed y haga clic en  .
Se muestra el cuadro de diálogo Eliminar feeds personalizados.



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

- Si decide eliminar el feed desde **Base de datos local y servicio**, el feed se elimina tanto del servicio como de la computadora local de Security Analytics. El feed eliminado ya no se verá en la interfaz del usuario de Security Analytics.
 - Si decide eliminar el feed desde **Solo base de datos local**, el feed se elimina de la computadora local de Security Analytics. El feed eliminado no se verá en la interfaz del usuario de Security Analytics; 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 Security Analytics 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


Esta sección contiene los siguientes procedimientos:

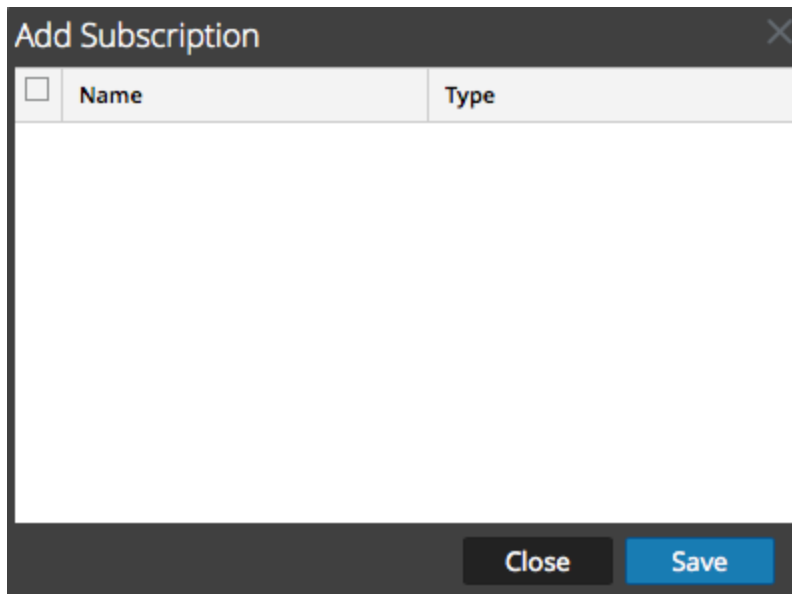
- [Agregar recursos suscritos para implementación en los servicios](#)
- [Crear un paquete de recursos](#)
- [Eliminar una suscripción](#)
- [Mostrar detalles de un recurso en la vista Recurso de Live](#)
- [Descargar un recurso](#)
- [Localizar y eliminar un recurso implementado desde servicios](#)
- [Eliminar recursos suscritos de la cuadrícula Suscripciones de implementaciones](#)
- [Mostrar los resultados como una cuadrícula 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

Después de completar este procedimiento, habrá agregado recursos suscritos para su implementación en servicios.

Para agregar recursos suscritos para su implementación en servicios:

1. Navegue a la vista Configurar > pestaña Implementaciones en Live.
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. Consulte [Implementar recursos desde un paquete de recursos](#) para obtener instrucciones sobre cómo implementar recursos desde un paquete.

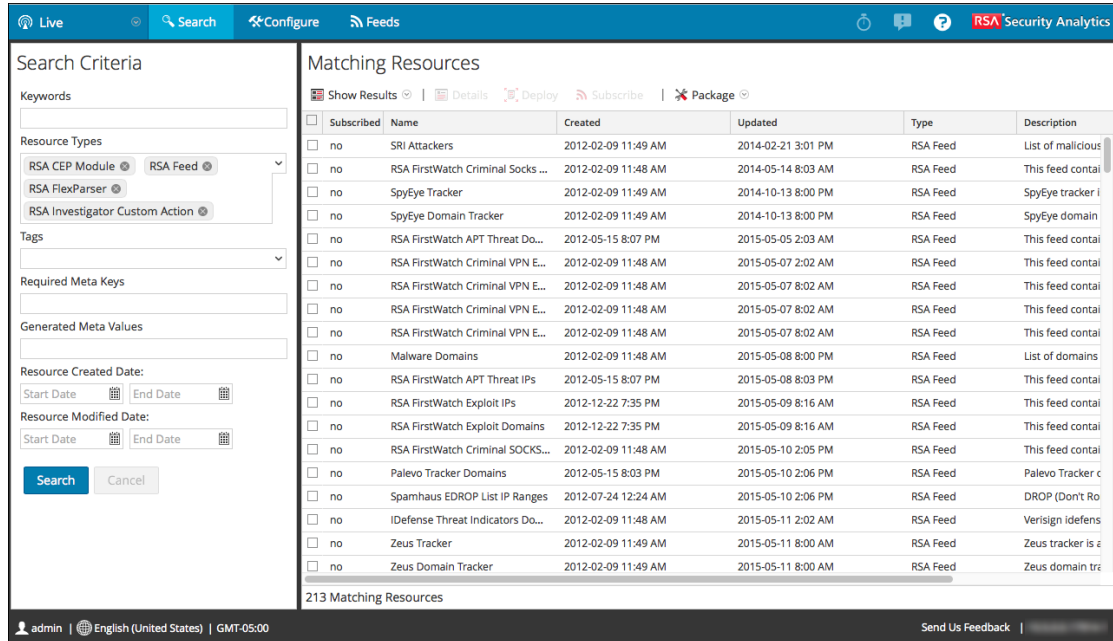
Después de realizar este procedimiento, habrá creado un paquete de recursos y lo habrá guardado en una unidad de red.

Requisitos previos

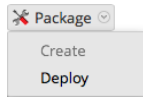
Un requisito previo para la creación de paquetes de recursos es la configuración de la conexión y la sincronización entre el servidor de CMS y Security Analytics y la capacidad de buscar recursos en la interfaz del usuario.

Para crear un paquete de recursos:

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

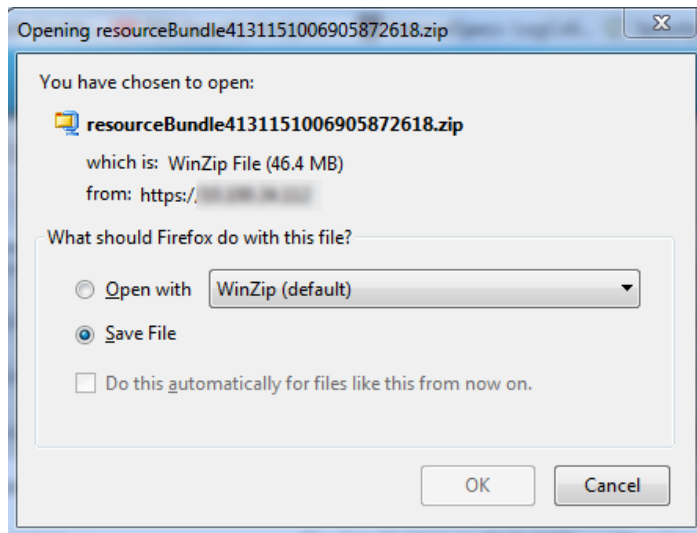


2. Seleccione **Paquete > Crear:**



Security Analytics 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.


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



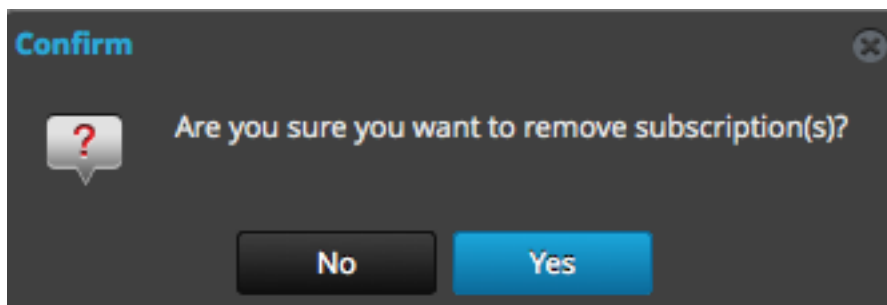
Eliminar una suscripción

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 Security Analytics 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**.

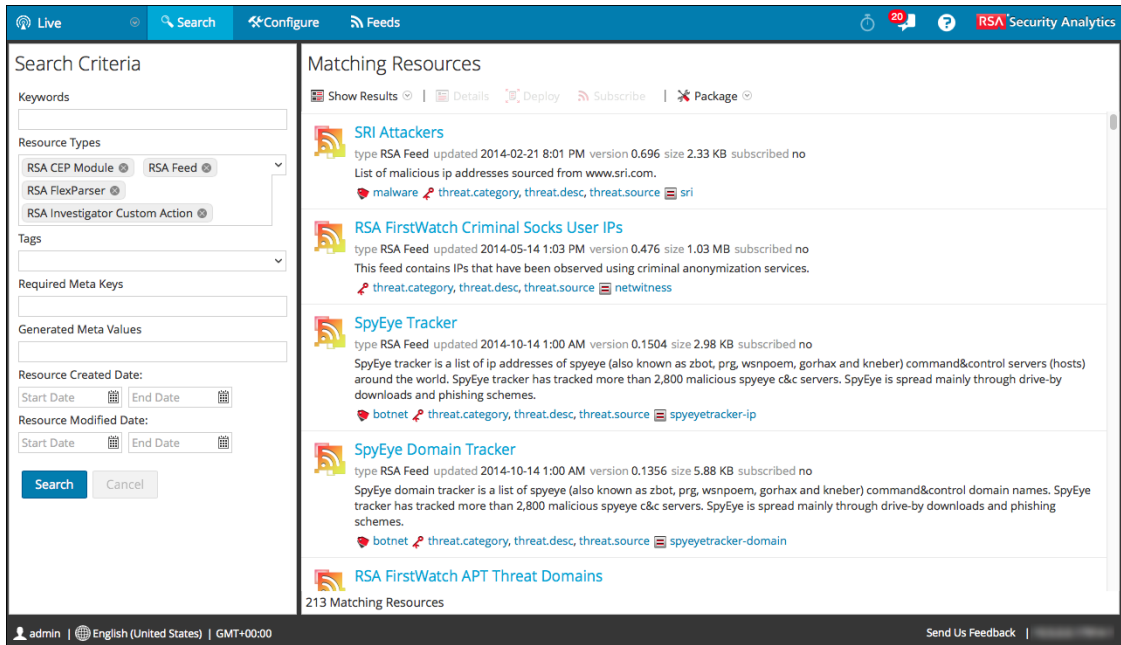
La suscripción se elimina de la lista de suscripciones, pero todas las instancias implementadas del recurso suscrito permanecen en los servicios.

Mostrar detalles de un recurso en la vista Recurso de Live

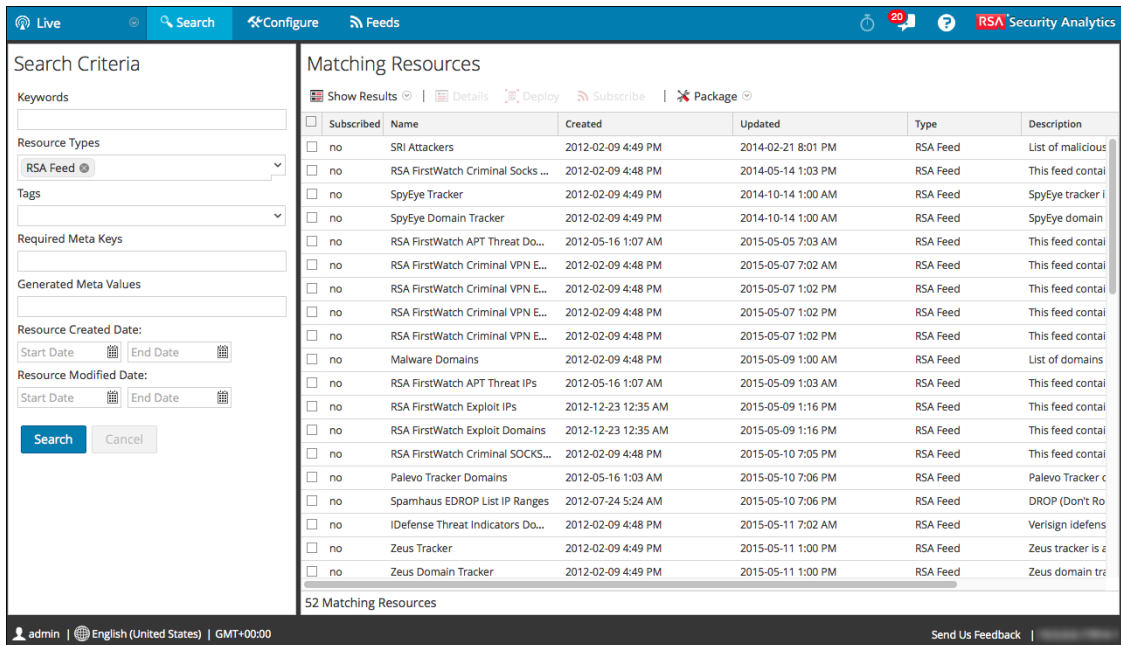
Después de seleccionar un recurso (en la [Vista Recurso de Live](#)), puede mostrar su información detallada.

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 en cuadrícula**, haga doble clic en un recurso o seleccione un recurso y haga clic en **Detalles**.



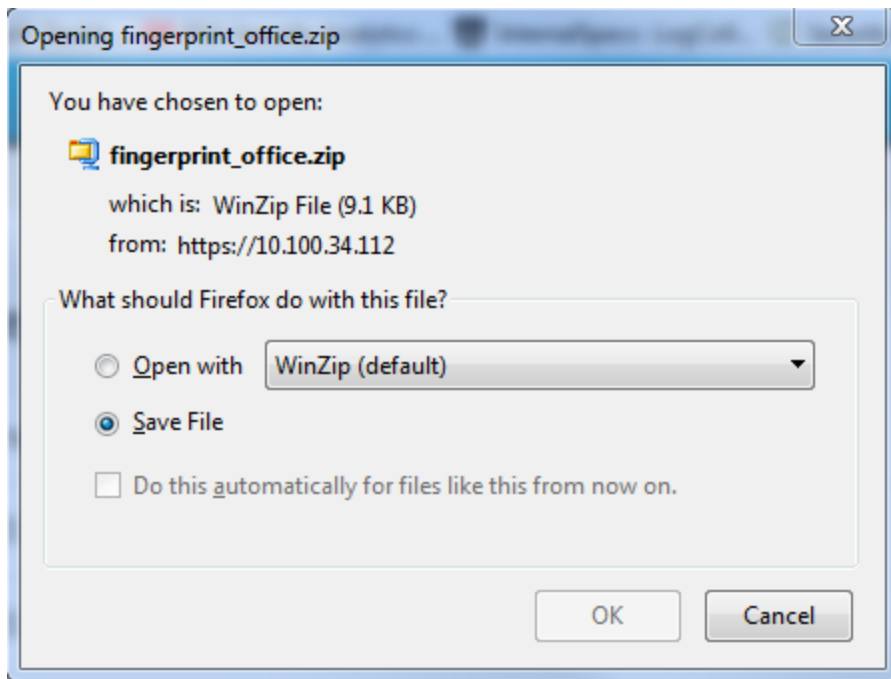
Descargar un recurso

Use la [Vista Recurso de Live](#) para descargar un recurso.

Para descargar un recurso:

1. Seleccione un recurso en la **Vista de recursos**.
2. Haga clic en  **Download**.

Un cuadro de diálogo ofrece la opción de abrir el archivo o guardarlo.



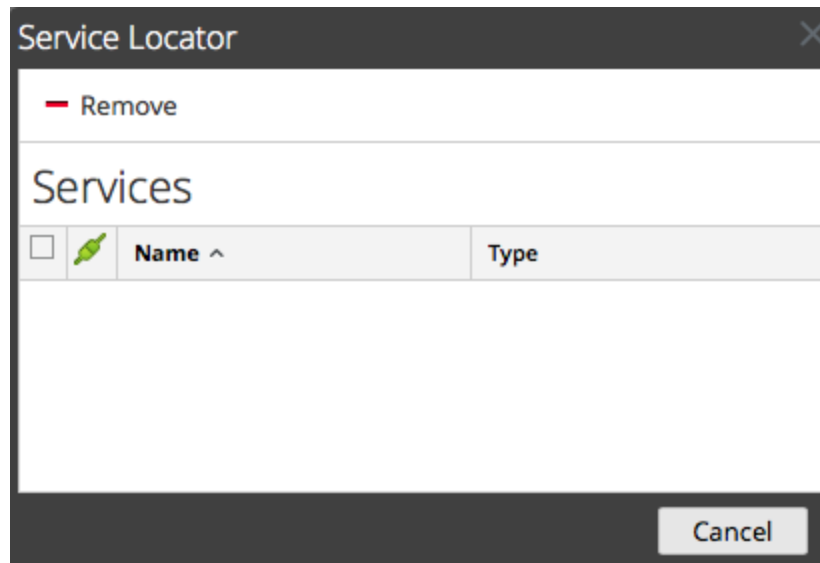
Localizar y eliminar un recurso implementado desde servicios

Puede localizar y quitar un recurso implementado en servicios desde 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 cuadrícula **Servicios**.
3. Haga clic en **Remove**.

El recurso se elimina de los servicios seleccionados.

Eliminar recursos suscritos de la cuadrícula Suscripciones de implementaciones

Puede quitar recursos de la vista Configurar > pestaña Implementaciones > panel Suscripciones de Live.

Este procedimiento elimina recursos del panel Suscripciones de la pestaña Implementaciones.

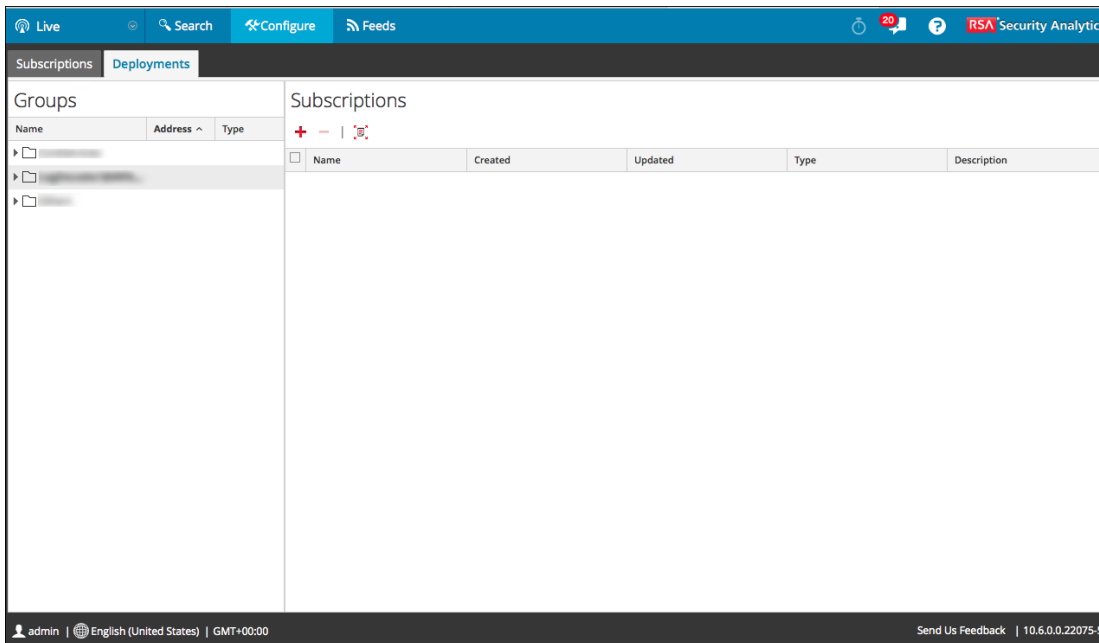
Las suscripciones que se seleccionan para implementación en un grupo de servicios se implementan durante la sincronización. Puede eliminar suscripciones del panel Suscripciones de implementaciones, pero cualquiera que se haya implementado realmente en los servicios permanecerá implementada hasta que alguien la elimine.

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 **Remove**.

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.

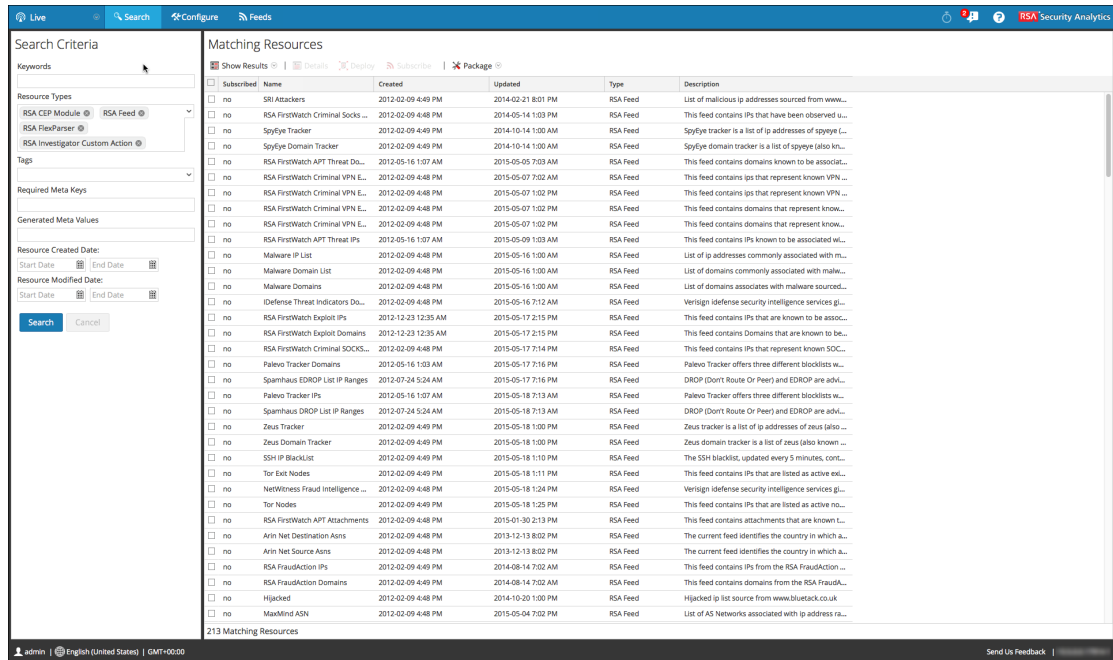


Mostrar los resultados como una cuadrícula o en detalle

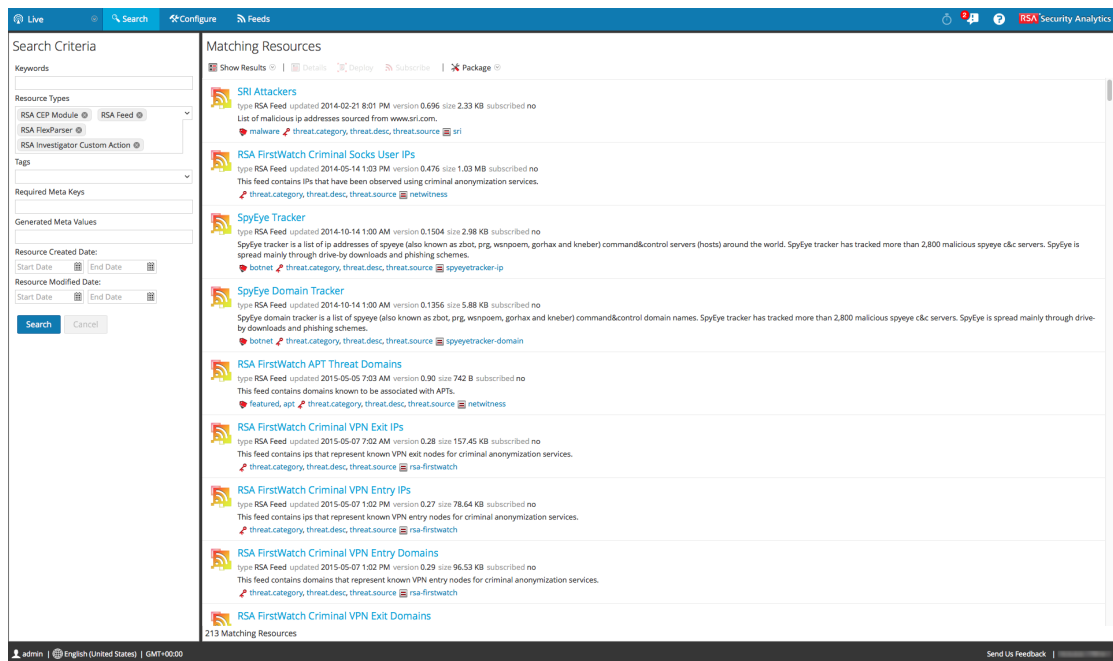
En este procedimiento se describe cómo alternar entre la visualización Detalle y Cuadrícula en el panel Coincidencias de recursos de la vista Buscar en Live.

Para cambiar entre una vista de página a una vista en cuadrícula:

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



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




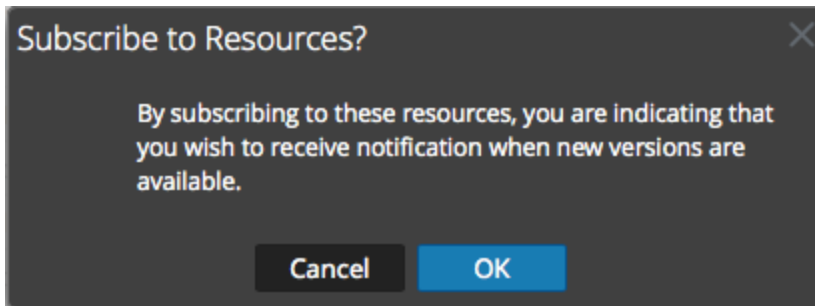
Suscribirse y cancelar la suscripción a un recurso

Puede suscribirse a un recurso y cancelar la suscripción de este en la vista Live > Buscar.

Suscribirse

Para suscribirse a un recurso:

1. En el panel **Criterios de búsqueda**, especifique los criterios de búsqueda y haga clic en **Buscar**.
2. Seleccione uno o más recursos y haga clic en  **Subscribe**.
Se muestra un cuadro de diálogo de confirmación.




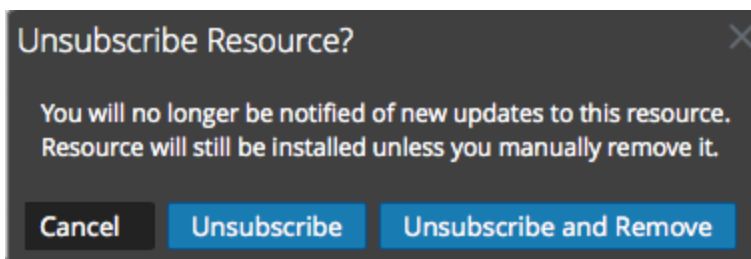
3. Para confirmar que desea suscribirse al recurso, haga clic en **Aceptar**.
El recurso se agrega a las suscripciones administradas en la pestaña Suscripciones y está disponible para implementarse en la pestaña Implementaciones.

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 mostrado en la **vista Recurso**, 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.

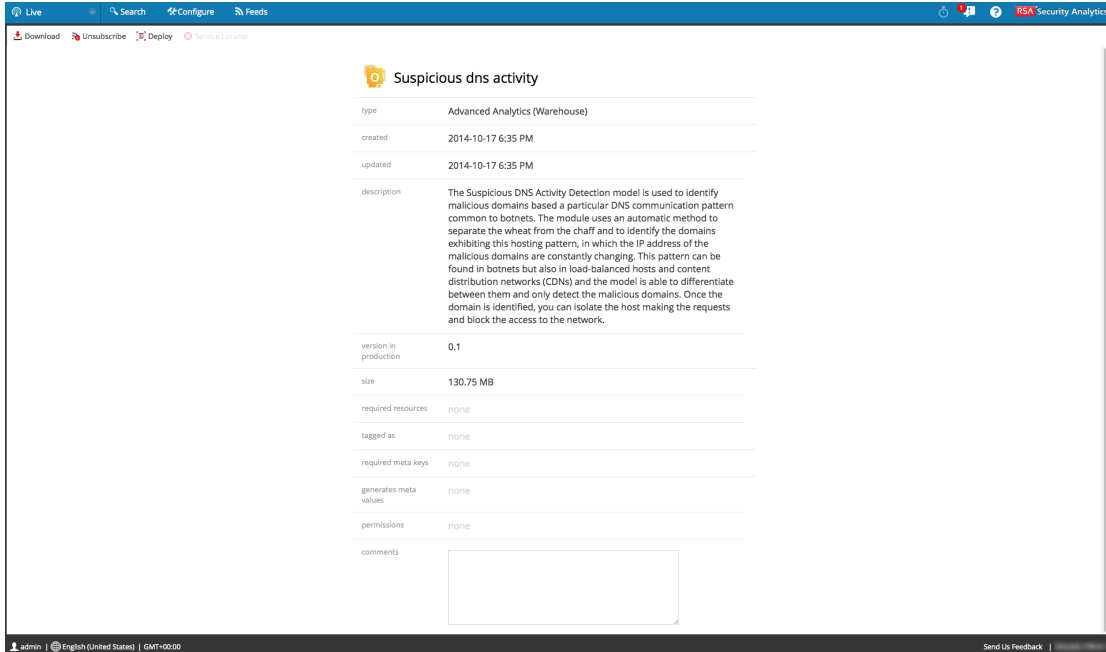
Ver detalles del recurso

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.



Suspicious dns activity	
type	Advanced Analytics (Warehouse)
created	2014-10-17 6:35 PM
updated	2014-10-17 6:35 PM
description	The Suspicious DNS Activity Detection model is used to identify malicious domains based a particular DNS communication pattern common to botnets. The module uses an automatic method to separate the wheat from the chaff and to identify the domains exhibiting this hosting pattern, in which the IP address of the malicious domains are constantly changing. This pattern can be found in botnets but also in load-balanced hosts and content distribution networks (CDNs) and the model is able to differentiate between them and only detect the malicious domains. Once the domain is identified, you can isolate the host making the requests and block the access to the network.
version in production	0.1
size	130.75 MB
required resources	none
tagged as	none
required meta keys	none
generates meta values	none
permissions	none
comments	<input type="text"/>

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.

Referencias de los servicios de Live

Los siguientes temas de referencia están disponibles para los servicios de Live:

- [Vista Configuración de Live](#)
 - [Pestaña Implementaciones](#)
 - [Pestaña Suscripciones](#)
- [Vista Feeds de Live](#)
- [Vista Recurso de Live](#)
- [Vista Buscar en Live](#)
- [Portal de registro de RSA Live](#)
- [Asistente Implementación de paquete de recursos](#)
- [Comentarios y uso compartido de datos de Security Analytics](#)

Vista Configuración de Live

En la vista Configuración de Live, Security Analytics proporciona herramientas integradas para administrar los recursos de Live. Puede administrar las suscripciones a recursos y las implementaciones en servicios. 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 Security Analytics Live, lea [Administración de servicios de Live](#).

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

- En el menú de **Security Analytics**, seleccione **Live > Configurar**.
- Desde cualquier vista del módulo Live, seleccione **Configurar** en la barra de herramientas de Security Analytics.

Las funciones de la vista Configurar se dividen en dos pestañas:

- [Pestaña Implementaciones](#)
- [Pestaña Suscripciones](#)

Pestaña Implementaciones

En este tema se presentan las funciones de la vista Configurar > pestaña Implementaciones en Live.

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.

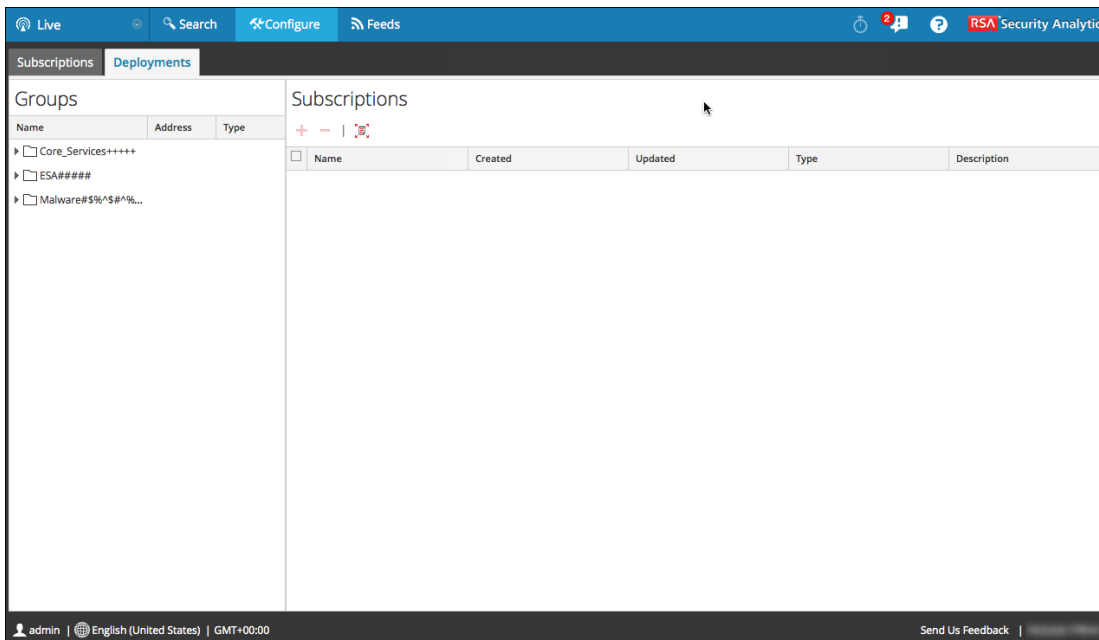
Los recursos que se muestran aquí no se implementan de inmediato después de la adición a un grupo de servicios. En vez de eso, los recursos suscritos se migran a los servicios cuando Security Analytics se sincroniza con RSA Security Analytics Live. El calendario de sincronización se configura en el panel Configuración de Live. Si no desea esperar hasta la sincronización programada, también puede indicar a Security Analytics que se sincronice ahora 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. En el menú de **Security Analytics**, seleccione **Live > Configurar**.
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.

Característica	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.

Característica	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.
Created	Esta es la fecha y la hora en que se creó el recurso.
Fragmento C	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 Security Analytics Live a los cuales se suscribió en la vista Buscar en Live o en la vista Recurso de Live. Cuando se suscribió a un recurso, aceptó recibir actualizaciones de RSA Security Analytics 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 al cual Security Analytics está suscrito se muestra en esta pestaña.

En la pestaña Suscripciones, puede:

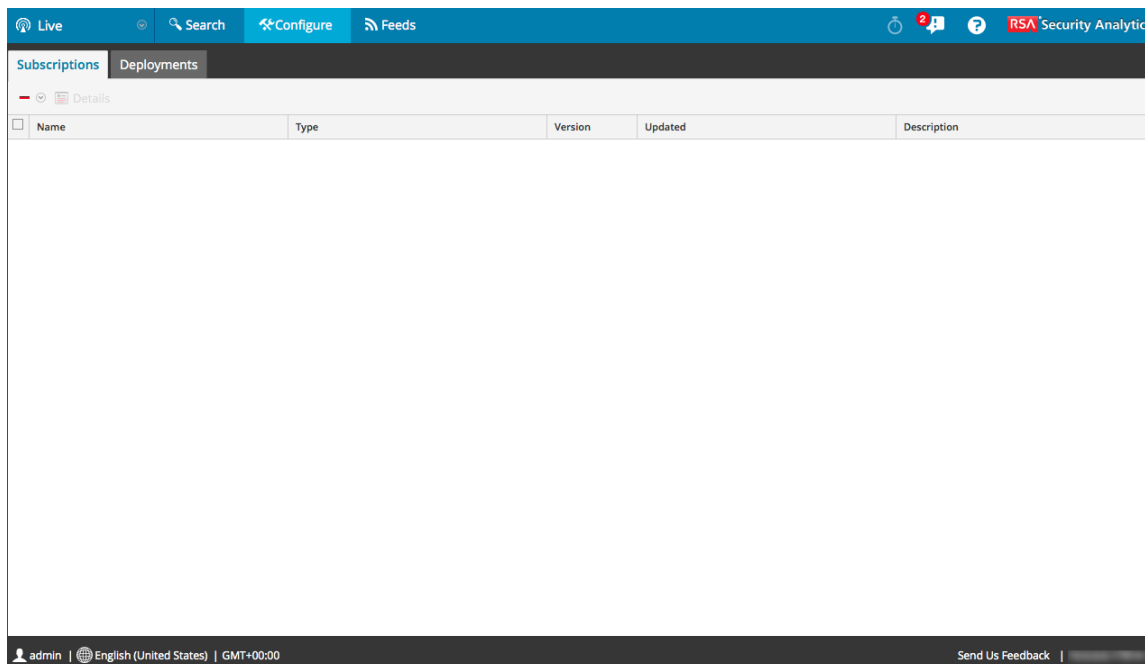
- Ver todos los recursos a los cuales está suscrita esta instancia de Security Analytics.
- Abrir una vista detallada de una suscripción en la vista Recurso de Live.
- Eliminar una suscripción.

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 **Security Analytics**, seleccione **Live > Configuración**.



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.

Característica	Descripción
	Elimina las suscripciones seleccionadas.
 Details	Muestra los detalles de un único recurso suscrito en la vista Recurso.

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.
Fragmento C	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.

Vista Feeds de Live

Use la vista Feeds de Live para:

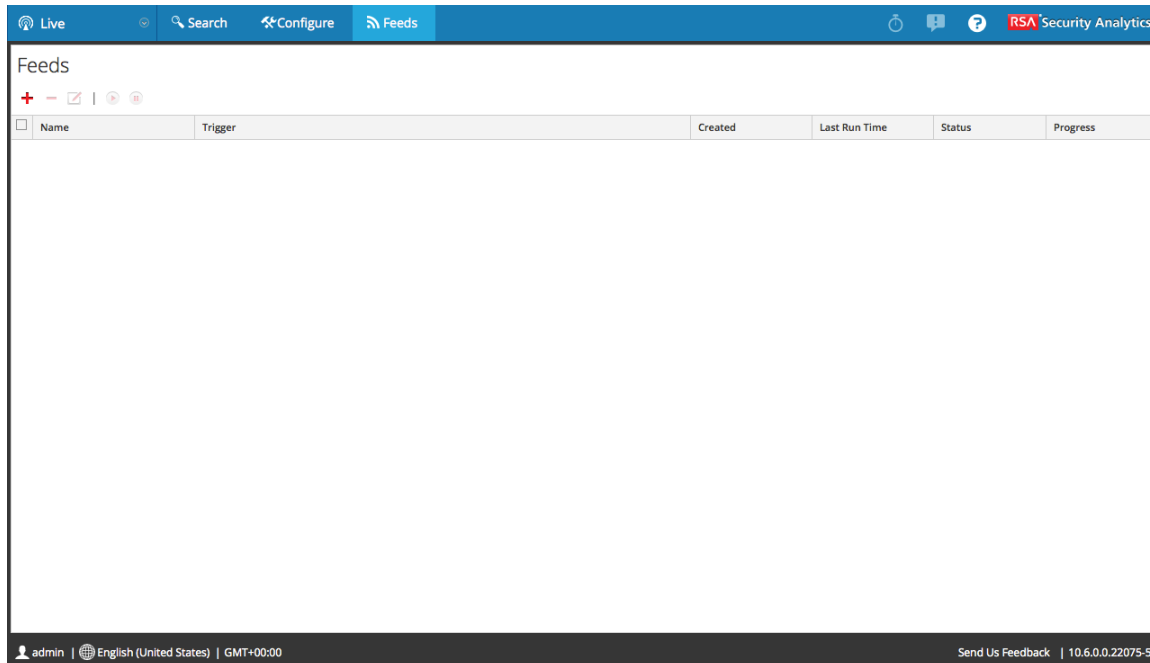
- Crear feeds personalizados.
- Crear feeds de identidad.
- Editar feeds.

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 el menú de **Security Analytics**, seleccione **Live > Feeds**.
- Desde cualquier vista del módulo Live, seleccione **Feeds** en el menú de **Security Analytics**.


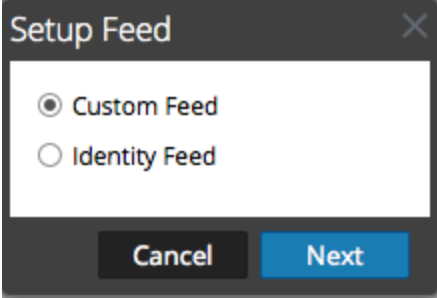




Este es un ejemplo de la vista Feeds.



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


Barra de herramientas

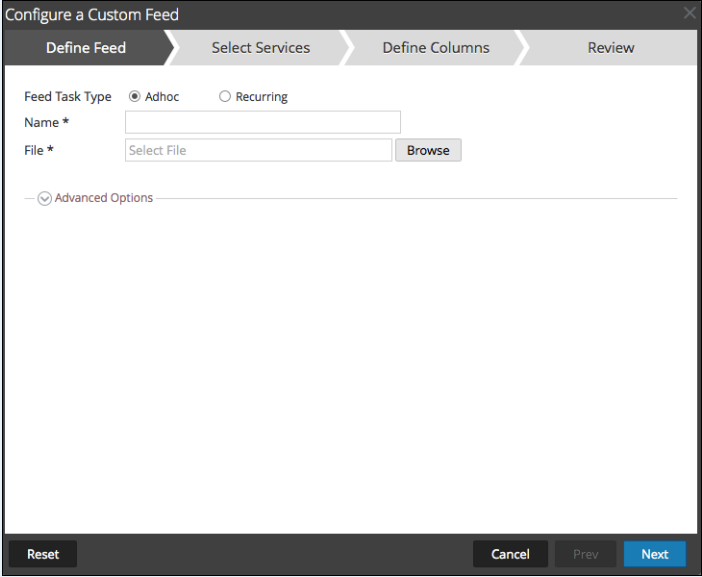
En esta tabla se describen las opciones de la barra de herramientas.

Característica	Descripción
	<p>Inicia la creación de un feed personalizado o de identificación mediante el despliegue del cuadro de diálogo Configurar feed.</p>  <ul style="list-style-type: none"> • El feed personalizado abre el asistente Configurar un feed personalizado (consulte Crear un feed personalizado). • El feed de identidad abre el asistente Configurar feed de identidad (consulte Crear y administrar un feed de identidad).
	Elimina el feed que seleccionó.
	Abre el asistente Configurar feed personalizado o Configurar feed de identidad para el feed que seleccionó (consulte Editar un feed).
	Iniciar/reanudar feed de datos.
	Detener/pausar feed de datos.

Cuadrícula Feeds

Esta tabla describe las columnas en la cuadrícula.

Columna	Descripción
	Selecciona un feed.

Columna	Descripción
Nombre	<p>Nombre del feed.</p> <p>Nota: Ahora puede utilizar caracteres especiales para definir el nombre del feed personalizado.</p> 
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.
Created	Esta es la fecha y la hora en que se creó el feed.
Hora de última ejecución	Esta es la fecha y la hora en que el feed se ejecutó por última vez.
Status	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 de **Security Analytics**, seleccione **Live > Buscar > Tipos de recursos**.
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.

The screenshot displays the 'SpyEye Tracker' resource details in the RSA Security Analytics interface. The interface includes a top navigation bar with 'Live', 'Search', 'Configure', and 'Feeds' options, and a user profile 'admin' in the bottom left. The resource details are as follows:

Download	Subscribe	Deploy	Service Locator
	SpyEye Tracker		
type	RSA Feed		
created	2012-02-09 4:49 PM		
updated	2014-10-14 1:00 AM		
description	SpyEye tracker is a list of ip addresses of spyeye (also known as zbot, prg, wsnpoem, gorhax and kneber) command&control servers (hosts) around the world. SpyEye tracker has tracked more than 2,800 malicious spyeye c&c servers. SpyEye is spread mainly through drive-by downloads and phishing schemes.		
version in production	0.1504		
size	2.977 KB		
required resources	none		
tagged as	botnet		
required meta keys	threat.category , threat.desc , threat.source		
generates meta values	spyeyetracker-ip		
permissions	none		

admin | English (United States) | GMT+00:00 | Send Us Feedback

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.

IPv4 Vertical TCP Port Scan 5

type	RSA Correlation Rule
created	2014-05-20 11:27 AM
updated	2014-05-20 11:27 AM
description	Detects when a unique combination of IPv4 source and destination addresses communicate over five or more unique TCP ports within one minute across network sessions.
version in production	0.1
size	153 bytes
required resources	None
tagged as	none
required meta keys	none
generates meta values	none
permissions	none
your comments	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div> <p><small>comments should be no longer than 2000 characters</small></p> <input type="button" value="Submit"/>

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





Característica	Descripción
Ícono Tipo de recurso	Una representación gráfica del tipo de recurso, por ejemplo  .
Nombre	El nombre del recurso, por ejemplo, fingerpint_office_lua .

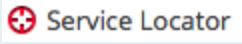
Característica	Descripción
Tipo	El tipo de recurso, por ejemplo, RSA Lua Parser .
Created	La fecha en que se creó el recurso; por ejemplo, 2013-09-15 02:16 PM .
Fragmento C	La fecha en que el recurso se actualizó por última vez; por ejemplo, 2013-09-15 02:16 PM .
Descripción	La descripción del recurso, 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 reemplazan 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.
Genera valores de metadatos	Los valores de metadatos  que el recurso genera. 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.

Característica	Descripción
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.

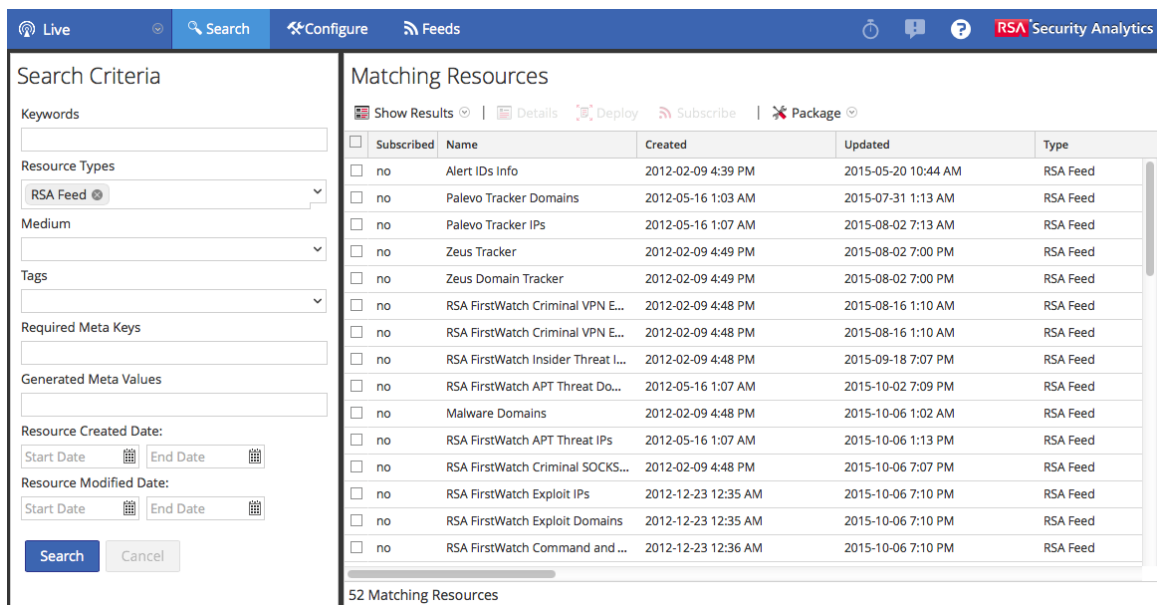
Característica	Ícono	Descripción
Descarga	 Download	Esta opción descarga el recurso que se muestra actualmente en la vista Recurso.
Suscribirse o cancelar suscripción	 Subscribe  Unsubscribe	<p>Esta opción suscribe o cancela la suscripción al recurso que se muestra actualmente en la vista Recurso.</p> <ul style="list-style-type: none"> 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. 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.
Implementación	 Deploy	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.

Característica	Ícono	Descripción
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.



The screenshot shows the 'Buscar en Live' interface with the following components:

- Search Criteria Panel:**
 - Keywords: [Empty text box]
 - Resource Types: RSA Feed (selected)
 - Medium: [Empty dropdown]
 - Tags: [Empty dropdown]
 - Required Meta Keys: [Empty text box]
 - Generated Meta Values: [Empty text box]
 - Resource Created Date: Start Date [Calendar] End Date [Calendar]
 - Resource Modified Date: Start Date [Calendar] End Date [Calendar]
 - Buttons: Search, Cancel
- Matching Resources Panel:**
 - Actions: Show Results, Details, Deploy, Subscribe, Package
 - Table with columns: Subscribed, Name, Created, Updated, Type
 - 52 Matching Resources (indicated at the bottom)

Subscribed	Name	Created	Updated	Type
<input type="checkbox"/>	Alert IDs Info	2012-02-09 4:39 PM	2015-05-20 10:44 AM	RSA Feed
<input type="checkbox"/>	Palevo Tracker Domains	2012-05-16 1:03 AM	2015-07-31 1:13 AM	RSA Feed
<input type="checkbox"/>	Palevo Tracker IPs	2012-05-16 1:07 AM	2015-08-02 7:13 AM	RSA Feed
<input type="checkbox"/>	Zeus Tracker	2012-02-09 4:49 PM	2015-08-02 7:00 PM	RSA Feed
<input type="checkbox"/>	Zeus Domain Tracker	2012-02-09 4:49 PM	2015-08-02 7:00 PM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch Criminal VPN E...	2012-02-09 4:48 PM	2015-08-16 1:10 AM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch Criminal VPN E...	2012-02-09 4:48 PM	2015-08-16 1:10 AM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch Insider Threat L...	2012-02-09 4:48 PM	2015-09-18 7:07 PM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch APT Threat Do...	2012-05-16 1:07 AM	2015-10-02 7:09 PM	RSA Feed
<input type="checkbox"/>	Malware Domains	2012-02-09 4:48 PM	2015-10-06 1:02 AM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch APT Threat IPs	2012-05-16 1:07 AM	2015-10-06 1:13 PM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch Criminal SOCKS...	2012-02-09 4:48 PM	2015-10-06 7:07 PM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch Exploit IPs	2012-12-23 12:35 AM	2015-10-06 7:10 PM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch Exploit Domains	2012-12-23 12:35 AM	2015-10-06 7:10 PM	RSA Feed
<input type="checkbox"/>	RSA FirstWatch Command and ...	2012-12-23 12:36 AM	2015-10-06 7:10 PM	RSA Feed

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.

Search Criteria

Keywords

Resource Types

Medium

Tags

Required Meta Keys

Generated Meta Values


Resource Created Date:
 Start Date End Date


Resource Modified Date:
 Start Date End Date

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

Característica	Descripción
Palabras clave	Ingrese una o más palabras clave para buscar recursos que incluyan estas palabras en su nombre o descripción. Cuando ingresa una palabra clave, puede utilizar comodines.

Característica	Descripción
Tipos de recursos	<p>Seleccione los tipos de recursos en la lista desplegable para filtrar los recursos por tipo. Los valores posibles son:</p> <ul style="list-style-type: none">• Analítica avanzada (Warehouse)• Regla de aplicación de RSA• Módulo RSA CEP• Contenido de RSA• Regla de correlación de RSA• Regla de RSA Event Stream Analysis• Feed de RSA• RSA FlexParser• Acción personalizada de investigador de RSA• Log Collector de RSA• RSA Log Device• Analizador Lua de RSA• Reglas de malware de RSA• Clave de metadatos de RSA• Lista de RSA Security Analytics• Informe de RSA Security Analytics• Regla de RSA Security Analytics• Documento de orígenes de RSA

Característica	Descripción
(10.5.1 o posterior) Mediano	<p>Seleccione uno o más medios en la lista desplegable para buscar contenido en función del origen de metadatos.</p> <p>Los valores disponibles para medio son los siguientes:</p> <ul style="list-style-type: none"> • registro: se aplica al contenido que utiliza metadatos derivados de datos de registros • paquete: se aplica al contenido que utiliza metadatos derivados de paquetes de red • paquetes y registros: se aplica al contenido que correlaciona metadatos derivados a través de datos de paquetes y registros
Etiquetas	<p>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.</p>
Claves de metadatos requeridas	<p>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.</p>
Valores de metadatos generados	<p>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.</p>
Fecha de creación de investigación	<p>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.</p>

Característica	Descripción
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.


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.

Característica	Descripción
Ícono Tipo de recurso	Una representación gráfica del tipo de recurso. Por ejemplo 
Nombre	El nombre del recurso, por ejemplo, Administración de grupos .
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 .






Característica	Descripción
Tamaño	El tamaño del recurso, por ejemplo, 153 B .
Subscribed	Estado de suscripción: <ul style="list-style-type: none"> • sí: Esta instancia de Security Analytics está suscrita a este recurso de contenido. • no: Esta instancia de Security Analytics no se ha suscrito a este recurso de contenido.
Descripción	La descripción del recurso, por ejemplo, Administración de grupos-reglas de cumplimiento de normas .
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,  featured , apt  .
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,  threat.category , threat.desc , threat.source .
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,  netwitness .

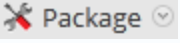
Resultados en cuadrícula

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.

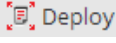
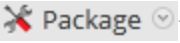
En la siguiente tabla se describen los elementos de los resultados de la cuadrícula.

Característica	Descripción
Cuadrícula	

Característica	Descripción
Subscribed	Estado de suscripción: <ul style="list-style-type: none"> • sí: Esta instancia de Security Analytics está suscrita a este recurso de contenido. • no: Esta instancia de Security Analytics no se ha suscrito a este recurso de contenido.
Nombre	El nombre del recurso, por ejemplo, Administración de grupos .
Created	La fecha en que se creó el recurso, por ejemplo, 2015-08-12 3:11 PM .
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 .
Descripción	La descripción del recurso, por ejemplo, Administración de grupos-reglas de cumplimiento de normas .
Barra de herramientas	
 Show Results 	Este menú ofrece dos formas para ver los resultados de búsqueda: en detalle y en cuadrícula .
 Details	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.
 Deploy	Esta opción se aplica a uno o más recursos seleccionados.
 Subscribe	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.

Característica	Descripción
	<p>Este menú ofrece dos funciones de creación de paquetes para los recursos seleccionados:</p> <ul style="list-style-type: none"> • Crear: crea un archivo resourceBundle.zip que contiene los recursos seleccionados y abre un cuadro de diálogo en el que puede: <ul style="list-style-type: none"> • abrir el archivo, o • guardar el archivo para su posterior implementación. • 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 [Implementar recursos manualmente](#).
- Para obtener más detalles sobre la implementación de un paquete () **Package**), consulte [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. Security Analytics acepta paquetes en archivos **.nwp** o **.zip**.

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

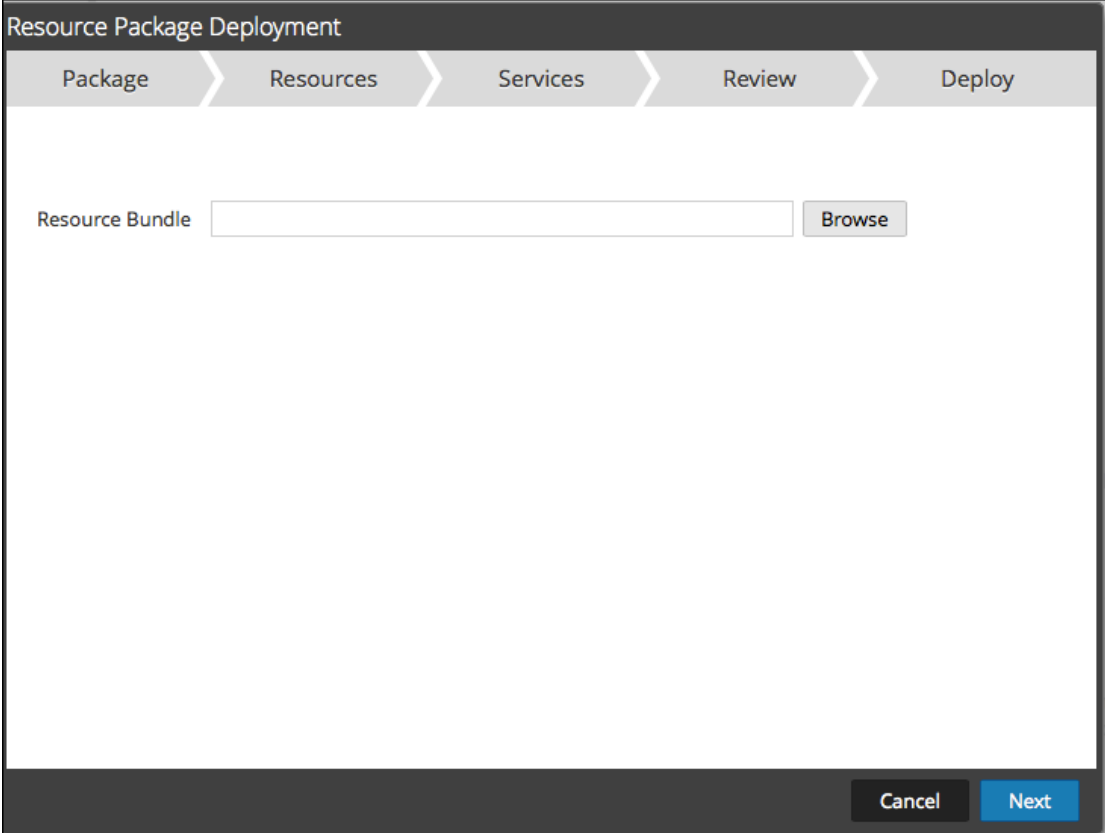
Si desea recibir notificaciones y actualizaciones de los recursos actualizados y poder eliminar fácilmente los recursos de un servicio, debe suscribirse a los recursos en la vista **Buscar en Live** e implementarlos en la vista **Configurar de Live**.

Nota: Use Security Analytics Live para crear paquetes de recursos; esta es una aplicación distinta que no es parte de Security Analytics. 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 Security Analytics.

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

1. En el menú de **Security Analytics**, seleccione **Live > Buscar**.
2. En **Buscar en Live - barra de herramientas Coincidencias de recursos**, seleccione **Paquete > Implementar**.

Se muestra el asistente Implementación de paquete de recursos.



Resource Package Deployment

Package Resources Services Review Deploy

Resource Bundle Browse

Cancel Next

Características

El Asistente de implementación tiene cinco pestañas: **Paquete**, **Recursos**, **Servicios**, **Análisis e Implementar**.

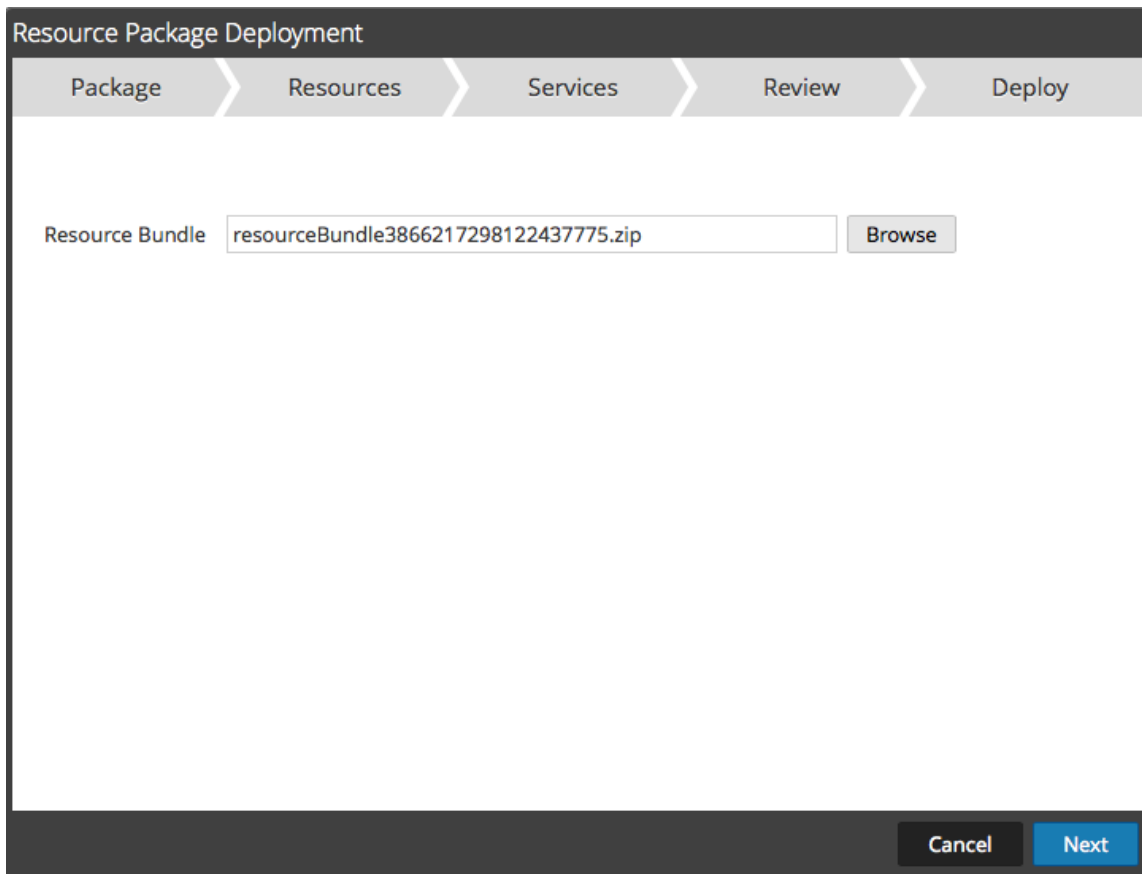
Use **Cerrar** para salir antes de completar al asistente.

Cuando completa el asistente, Security Analytics regresa a la vista Recursos de Live.

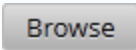
Pestaña Paquete

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  .
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.

Resource Names	Resource Type	Dependency Of
suspicious php put long query	RSA Application Rule	
APT Domain Intelligence	RSA Application Rule	

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

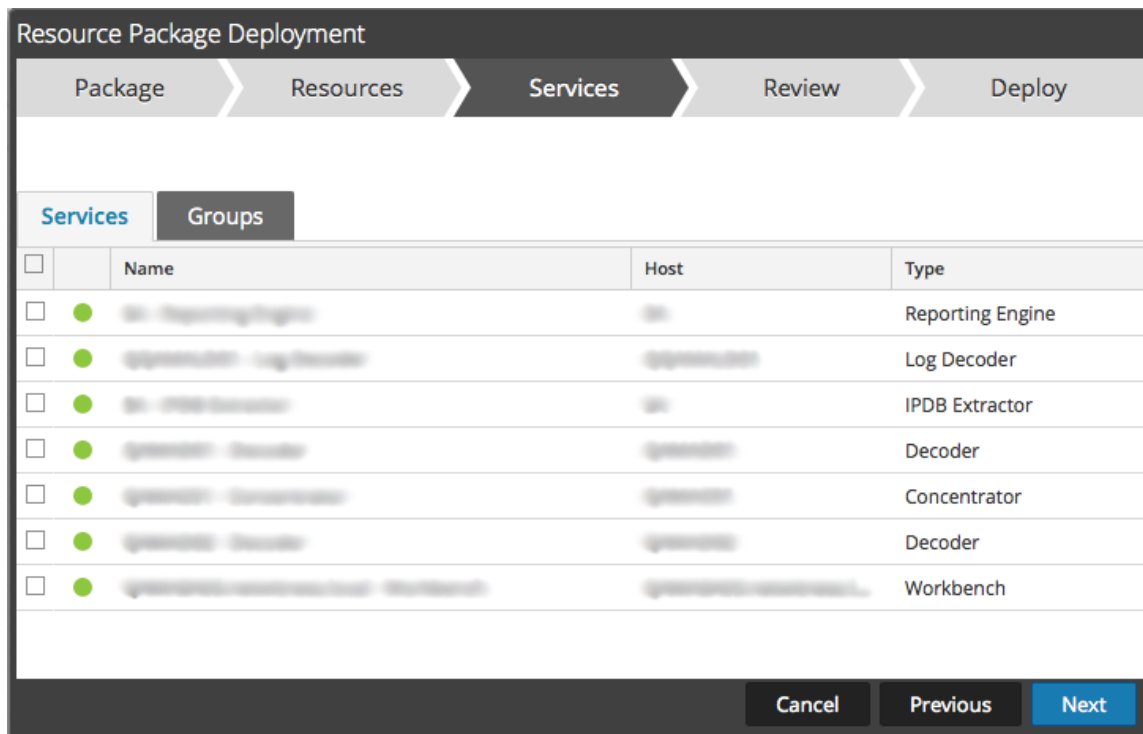
Columna	Descripción
Nombre del recurso	Muestra el nombre de los recursos del paquete (por ejemplo, NetWitness Lua Library).
Tipo de recurso	Muestra los tipos de recursos del paquete (por ejemplo, RSA Lua Parser).
Dependencia de	Muestra los recursos de los cuales depende el recurso seleccionado (por ejemplo, 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 Administration > 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	
<input type="checkbox"/>	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.
Tipo	Muestra el tipo de servicio de Security Analytics.
Grupos	

Columna	Descripción
	Selecciona grupos de servicios (si hay grupos de servicios definidos en el ambiente).
Nombre	Muestra los nombres de los grupos de servicios.

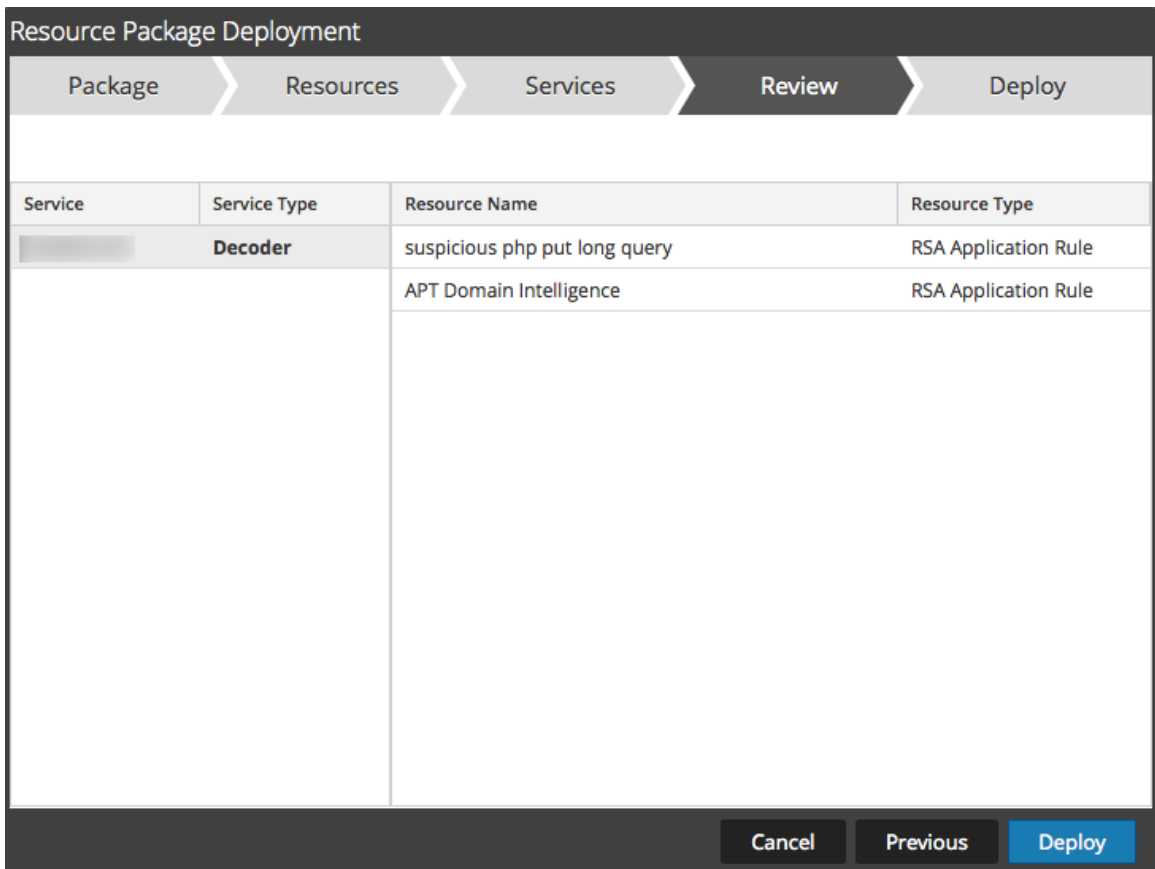
Pestaña Revisión

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.



Service	Service Type	Resource Name	Resource Type
	Decoder	suspicious php put long query	RSA Application Rule
		APT Domain Intelligence	RSA Application Rule

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

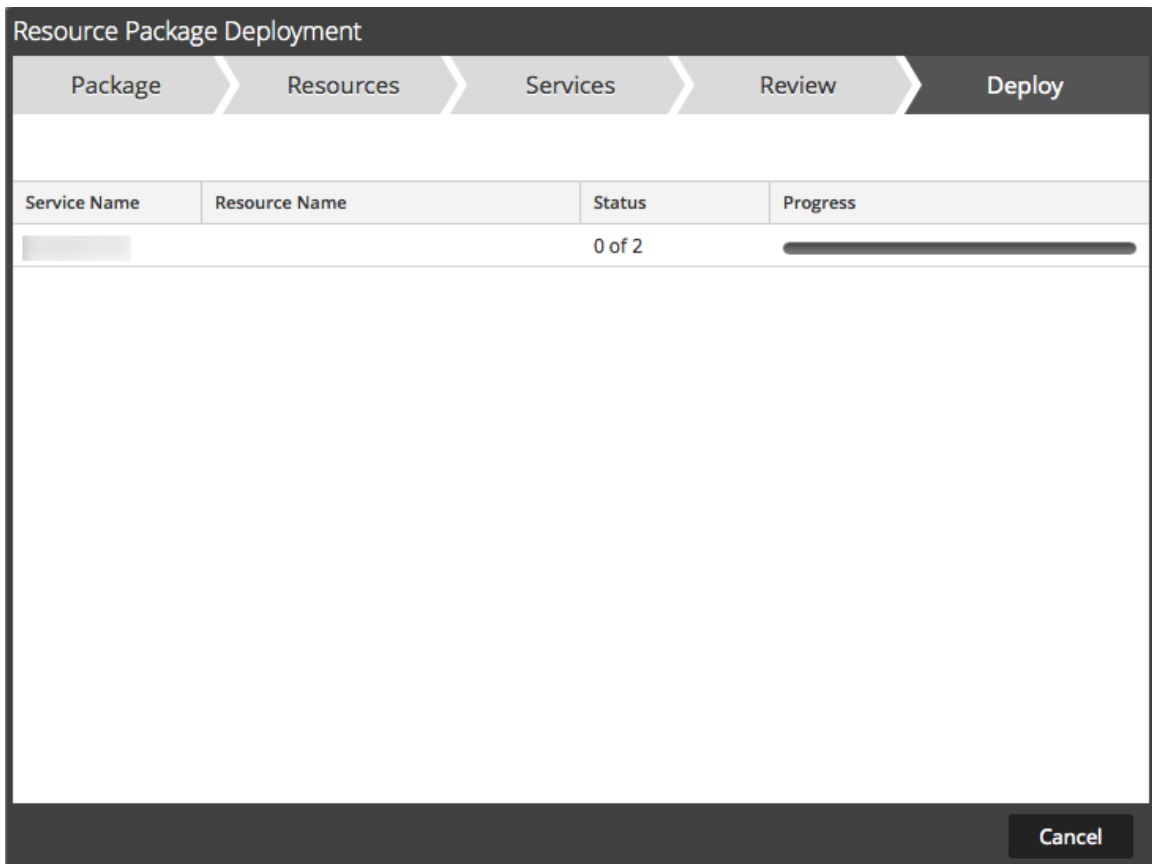
Columna	Descripción
Información de servicio	
Servicio	Muestra los servicios del ambiente en los cuales puede implementar el contenido.
Tipo de servicio	Muestra el tipo de cada servicio de Security Analytics (tipo de host/servicio).
Información de recursos	
Nombre del recurso	Muestra el nombre de los 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.

Característica	Descripción
Nombre del servicio	Nombre de los servicios para los cuales se implementan los recursos.
Nombre del recurso	Nombre de los recursos.
Status	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	
Cerrar	Cierra el asistente.

Característica	Descripción
Errores	Solo se muestra si Security Analytics encontró errores. Haga clic para mostrar los errores.
Reintentar	Solo se muestra si Security Analytics 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/>.



Welcome to the RSA Live Registration Portal

Thank you for using RSA Security Analytics.

Please sign up here for your RSA Live account to access your subscription content.

Terms and Conditions

***** IMPORTANT INFORMATION – PLEASE READ CAREFULLY *****

This Software contains computer programs and other proprietary material and information, the use of which is subject to and expressly conditioned upon acceptance of this License Agreement (the "Agreement").

This Agreement is a legally binding document between you (meaning the individual person or the entity that the individual represents that has obtained the Software and Hardware for its internal productive use and not for outright resale) (the "Customer") and RSA (which means (i) RSA Security LLC, if Customer is located in the United States, Mexico or South America; (ii) the local EMC Corporation sales subsidiary, if Customer is located outside the United States, Mexico or South America and in a country in which EMC Corporation has a local sales subsidiary; and (iii) EMC Information Systems International ("EISI"), if Customer is located outside United States, Mexico or South America and in a country in which EMC Corporation does not have a local sales subsidiary). Unless RSA agrees

I Agree:

[« Back](#) [Next »](#)

RSA Security Analytics

Company and Contact Information

Please fill out the following form. [? Change / Reset Password](#)

Contact Information

First Name: John

Last Name: Smith

Company: Xyz Software

Title: System Engineer

Username: John.Smith.live

Password:

Confirm Password:

Email Address: user@example.com

Confirm Email Address: user@example.com

Subscription Level

Basic

Enhanced

Premium

Confirm Subscription Level

Basic

Enhanced

Premium

License Server Id

.....

« Back Next »

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.

Parámetro	Descripción
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.
Nivel de suscripción/Confirmar nivel de suscripción	<ul style="list-style-type: none"> • 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.

Parámetro	Descripción
Identificador de servidor de licencia	<p>Este es el ID de licencia que se muestra en la página Administration > Sistema > Información.</p> <p>Precaución: El ID de servidor de licencia en Security Analytics 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.</p>

Comentarios y uso compartido de datos de Security Analytics

En este tema se presentan las funciones de comentarios y uso compartido de datos de Security Analytics.

La configuración de estas funciones está disponible en Administration > 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 Administration > Sistema > vista Servicios de Live.

Additional Live Services

Enable

Live Feedback ● Connected

Customer usage data, including usage metrics and current version of SA hosts, shall automatically be shared with RSA upon this system's connection to the Internet. This data is automatically shared only if Live account is configured and shall be protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable Information.

[Learn about the data RSA is collecting.](#)

Enable

Live Connect Threat Data Sharing (Beta) ○ Not Connected

RSA Live Connect Threat Data Sharing is an automated data collection service. It is responsible for gathering meta data captured locally by Security Analytics which is then de-identified and obfuscated with a one-way hash algorithm and sent securely and anonymously over SSL to the RSA Live Connect cloud service. The RSA Live Connect cloud service stores this information in a secure environment along with other data collected across the entire RSA Security Analytics community. This data will be leveraged for deep analysis to drive and improve the RSA Live and Live Connect threat intelligence services in order to proactively identify potential security threats. Customers who wish not to share de-identified and anonymized information regarding threat intelligence should change their settings in the Live-Connect feature and/or contact Customer Care.

NOTE: The type of data that potentially could be shared from a user's network to the RSA Live Connect cloud service could encompass any type of meta data that is captured by the Security Analytics product and will vary depending on Security Analytics deployment and configuration options and the user interaction with the Security Analytics product.

[Learn about the data RSA is collecting.](#)

Live Feedback

Live Feedback está diseñado para ayudar a mejorar RSA Security Analytics.

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 Security Analytics, 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.

Live Connect Threat Data Sharing (beta)

RSA Live Threat Data Sharing es un servicio de recopilación automatizada de datos. Su objetivo es compartir datos de inteligencia de amenazas potenciales en el servicio de nube de RSA Live Connect con fines de análisis. Se puede recopilar cualquier tipo de metadatos según la implementación, la configuración, la actividad de red y la interacción de los analistas con Security Analytics.

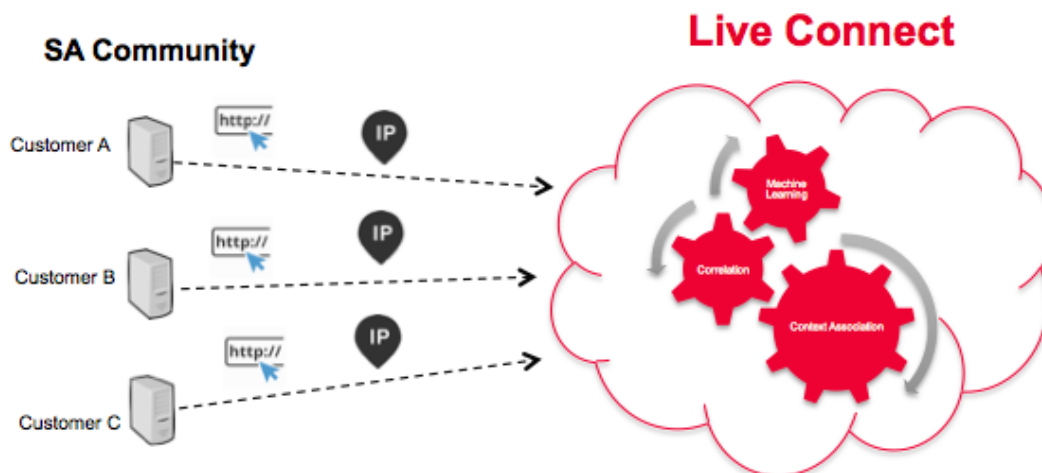
De manera predeterminada, este servicio está activado. Para cambiar la configuración, vaya a Administration > Sistema > vista Servicios de Live (o póngase en contacto con atención al cliente para que no participe).

Security Analytics captura localmente los metadatos, los cuales se envían de manera segura y anónima al servicio de nube de RSA Live. El servicio de nube de RSA Live almacena esta información junto con otros datos recopilados en la comunidad RSA Security Analytics a fin de mejorar los servicios de inteligencia de amenazas de RSA Live.

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 Security Analytics 10.6, 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 Security Analytics. 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 Security Analytics, seleccione **Administración > 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 de metadatos y valores de metadatos de vistas de las páginas de un analista de Security Analytics desde registros de consulta de Security Analytics Core.
- Proceso de recopilación de registros de consulta:
 - Periodicidad: Modo de lotes cada 24 horas (04:00 a 06:00 h UTC).
 - Recopilación de registros: El servidor de Security Analytics recopila entradas de registro de dispositivos de SA 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, Security Analytics 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)
- ID del servidor de licencia de Security Analytics (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: "03b81ffdf109a05a3dac88dbec10c59",
        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. En el menú de Security Analytics, seleccione **Administration > Sistema > Registro de sistema**.
2. Seleccione la pestaña **Configuración**.
3. En la sección Configuración de paquetes, seleccione **com > netwitness > platform > server > liveconnect > service (DEBUG)**.

