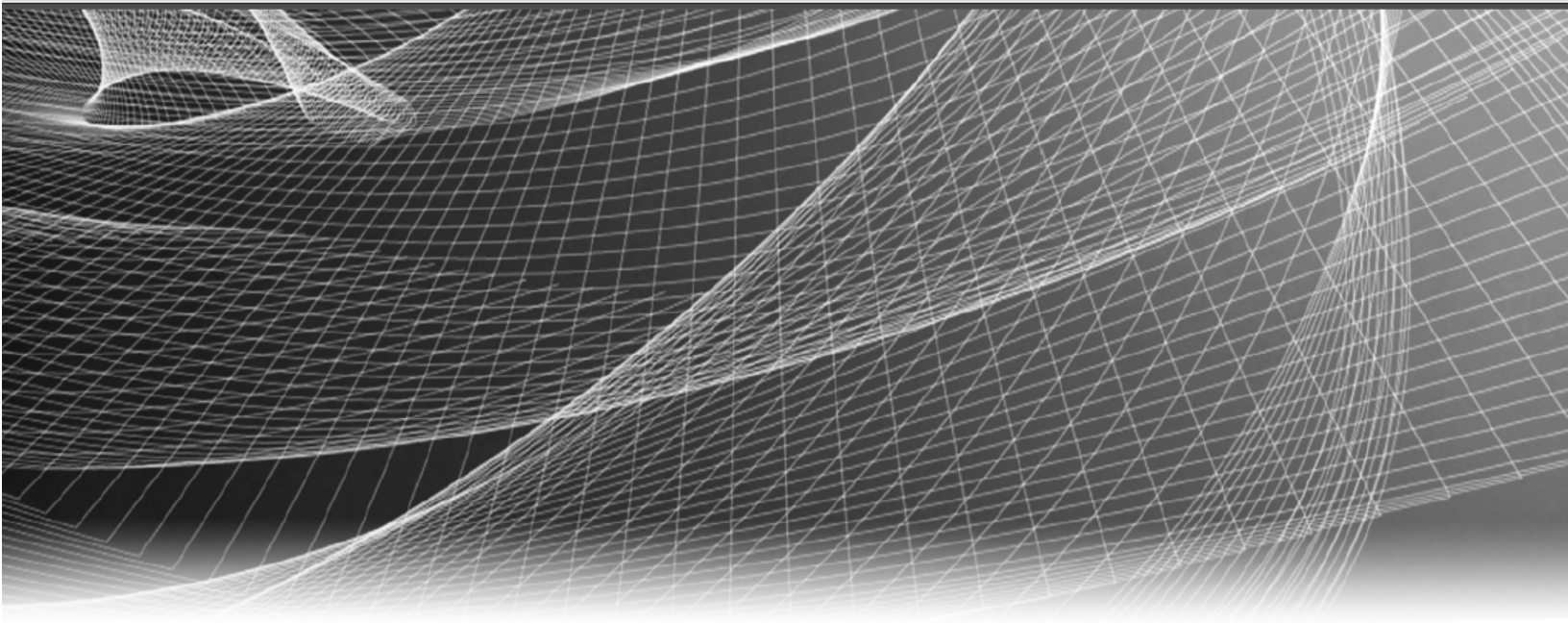


RSA Security Analytics

Recopilación de registros

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Guía de introducción a la recopilación de registros

Esta guía contiene las tareas básicas que debe completar para comenzar a recopilar eventos mediante la recopilación de registros.

Esta guía le indica:

- La función de la recopilación de registros y una descripción general de su funcionamiento con diagramas de implementación generales.
- Cómo comenzar a recopilar eventos.
- Dónde encontrar instrucciones para configurar implementaciones más complejas.
- Cómo iniciar cualquier protocolo de recopilación.
- Cuál es la estructura de la interfaz del usuario de configuración de la recopilación de registros.
- Qué herramientas se deben usar para solucionar problemas de la recopilación de registros, con una lista de instrucciones globales de solución de problemas.
- Cómo ajustar y personalizar la recopilación de registros en un ambiente.

Esta guía no le indica cómo:

- Implementar la recopilación de registros en múltiples ubicaciones con alta disponibilidad y balanceo de carga. Esta información se encuentra en la Guía de implementación de la recopilación de registros.
- Configurar la recopilación de registros por completo después de la implementación. Esta información se encuentra en la Guía de configuración de la recopilación de registros.
- Configure protocolos de recopilación individuales. Las instrucciones se encuentran en las guías de recopilación de registros individuales:

- Guía de configuración de la recopilación de AWS (CloudTrail)
- Guía de configuración de la recopilación de punto de comprobación
- Guía de configuración del protocolo de recopilación de archivos
- Guía de configuración de la recopilación de Netflow
- Guía de configuración de la recopilación de ODBC
- Guía de configuración de la recopilación de SDEE
- Guía de configuración de la recopilación de SNMP
- Guía de configuración de la recopilación de VMware
- Guía de configuración de la recopilación de Windows
- Guía de configuración de la recopilación de Windows existente y NetApp
- Las guías de configuración de cada origen de eventos compatible están disponibles en la página Orígenes de eventos compatibles.

Aspectos básicos de la recopilación de registros

En este tema se indica cómo funciona y cómo se implementa la recopilación de registros, se señalan los protocolos de recopilación compatibles, se describe la implementación básica y se ilustra la configuración y la implementación de la recopilación de registros.

Cómo funciona la recopilación de registros

El servicio Log Collector recopila registros de orígenes de eventos en todo el ambiente de TI de una organización y los reenvía a otros componentes de Security Analytics. Los registros y el contenido descriptivo se almacenan como metadatos para utilizarlos en investigaciones e informes.

Los orígenes de eventos son los recursos en la red, como servidores, switches, enrutadores, arreglos de almacenamiento, sistemas operativos y firewalls. En la mayoría de los casos, el equipo de tecnología de la información (TI) configura orígenes de eventos para enviar sus registros al servicio Log Collector y el administrador de Security Analytics configura este servicio para sondear orígenes de eventos y recuperar sus registros. En consecuencia, Log Collector recibe todos los registros en su forma original.

Qué protocolos de recopilación son compatibles

El servicio Log Collector es compatible con los siguientes protocolos de recopilación:

Protocolo de recopilación	Descripción
AWS	Recopila eventos desde Amazon Web Services (AWS) CloudTrail. Específicamente, CloudTrail registra llamadas API de AWS para una cuenta. Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de AWS (CloudTrail)*. Para obtener información sobre la configuración y la implementación de un Remote Log Collector en un ambiente AWS, consulte Paso 1: Iniciar sesión en AWS y crear una instancia en la *guía Configurar e implementar un Remote Log Collector en AWS*. Para obtener información sobre la implementación de un Remote Log Collector en un ambiente Azure, consulte Paso 1: Iniciar sesión en Azure y crear una máquina virtual en la *guía Implementar Remote Log Collector en Azure*.
Punto de comprobación	Recopila eventos desde orígenes de eventos de punto de control mediante OPSEC LEA. OPSEC LEA es la API de exportación de registros de seguridad de operaciones de punto de comprobación que facilita la extracción de registros. Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de punto de control*.
Archivo	Recopila eventos desde archivos de registro. Los orígenes de eventos generan archivos de registro que se transfieren al servicio Log Collector a través de un método de transferencia segura de archivos. Para obtener más información, consulte Conceptos básicos en la *Guía de configuración del protocolo de recopilación de archivos*.
Flujo de red	Acepta eventos de Netflow v5 y Netflow v9. Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de Netflow*.
ODBC	Recopila eventos de orígenes de eventos que almacenan datos de auditoría en una base de datos con el uso de la interfaz de software Open Database Connectivity (ODBC). Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de ODBC*.

Protocolo de recopilación	Descripción
SDEE	Recopila mensajes de un sistema de detección de intrusiones (IDS) y de un servicio de prevención de intrusiones (IPS). Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de SDEE*.
SNMP Trap	Acepta SNMP traps. Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de SNMP*.
Syslog	Acepta mensajes de orígenes de eventos que emiten mensajes de syslog.
VMware	Recopila eventos de una infraestructura virtual de VMware. Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de VMware*.
Windows	Recopila eventos de máquinas Windows compatibles con el modelo de Microsoft Windows. Windows 6.0 es una plataforma de rastreo y registro de eventos que se incluye en el sistema operativo a partir de Microsoft Windows Vista y Windows Server 2008. Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de Windows*.

Protocolo de recopilación	Descripción
Windows existente	Recopila eventos de: • Versiones de Windows más antiguas, como Windows 2000 y Windows 2003, y recopila de orígenes de eventos de Windows ya configurados para la recopilación enVision sin necesidad de reconfigurarlos. • Origen de eventos del dispositivo ONTAP de NetApp, de modo que ahora puede recopilar y analizar archivos evt de NetApp. • Para obtener más información, consulte Conceptos básicos en la *Guía de configuración de la recopilación de Windows heredado y NetApp*. **Nota:** El recopilador de Windows heredado de Security Analytics se instala en un servidor Windows 2008 R2 SP1 de 64 bits físico o virtual mediante el archivo **SALegacyWindowsCollector-*version-number*.exe**. Consulte la *Guía de configuración de la recopilación de Windows* para obtener instrucciones detalladas sobre cómo implementar el recopilador de Windows heredado.

Este tema describe las tareas básicas que debe realizar para comenzar a recopilar eventos mediante el servicio Security Analytics Log Collector. Consulte la *Guía de implementación de la recopilación de registros* para obtener instrucciones sobre cómo configurar implementaciones más complejas.

Implementación básica

Para implementar la recopilación de registros, debe:

1. Configurar un Log Collector localmente en un Log Decoder (es decir un Local Collector). También puede configurar recopiladores de registros en tantas ubicaciones remotas (es decir Remote Collectors) como requiera una empresa.
2. Configurar:
   - La recopilación de registros de Security Analytics para recopilar eventos desde orígenes de eventos
   - Orígenes de eventos para enviar eventos al servicio de recopilación de registros de Security Analytics.

Funciones de los Local y Remote Collectors

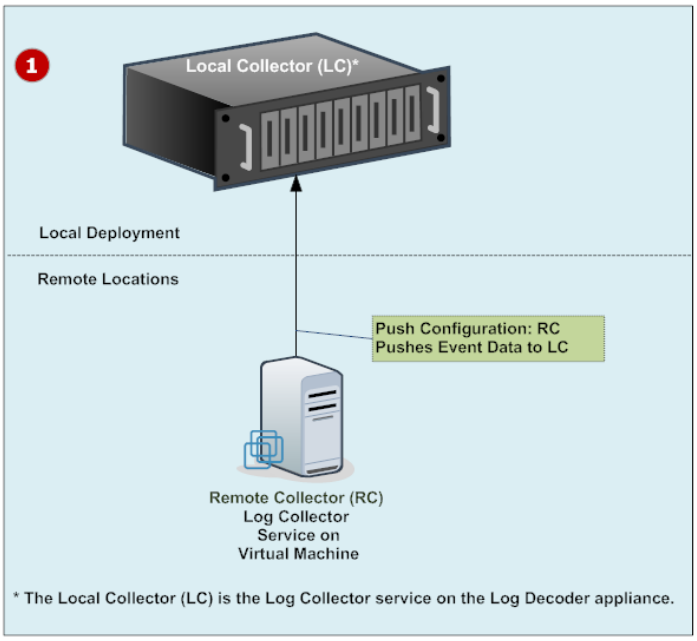
Un Local Collector (LC) es un servicio Log Collector que se ejecuta en un host de Log Decoder. En un escenario de implementación local, el servicio Log Collector se implementa en un host de Log Decoder con el servicio Log Decoder. La recopilación de registros de varios protocolos, como Windows, ODBC, etc., se ejecuta a través del servicio Log Collector y los eventos se reenvían al servicio Log Decoder. El Local Collector envía todos los datos de eventos recopilados al servicio Log Decoder.

Debe tener al menos un Local Collector para recopilar eventos no relacionados con syslog.

Un Remote Collector (RC), al cual también se denomina Virtual Log Collector (VLC), es un servicio Log Collector que se ejecuta en una máquina virtual independiente. Los Remote Collectors son opcionales y deben enviar los eventos que recopilan a un Local Collector. La implementación de Remote Collector es ideal cuando se deben recopilar registros desde ubicaciones remotas. Los Remote Collectors comprimen y cifran los registros antes de enviarlos a un Local Collector.

Implementación y configuración de la recopilación de registros

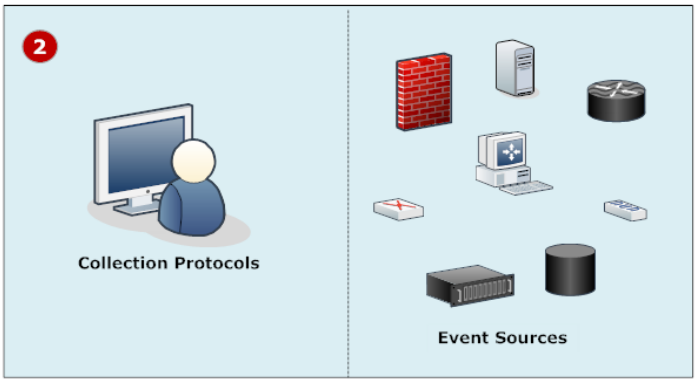
En la siguiente figura se ilustran las tareas básicas que debe realizar para implementar y configurar la recopilación de registros. Para implementar la recopilación de registros, debe configurar un Local Collector. También puede implementar uno o más Remote Collectors. Después de implementar la recopilación de registros, debe configurar los orígenes de eventos en Security Analytics y en los propios orígenes de eventos. El siguiente diagrama muestra el Local Collector que recibe eventos migrados desde un Remote Collector.



1 Configure Local Collectors y Remote Collectors.

El Local Collector es el servicio Log Collector que se ejecuta en el host de Log Decoder.

Un Remote Collector es el servicio Log Collector que se ejecuta en una máquina virtual o en un servidor Windows en una ubicación remota.

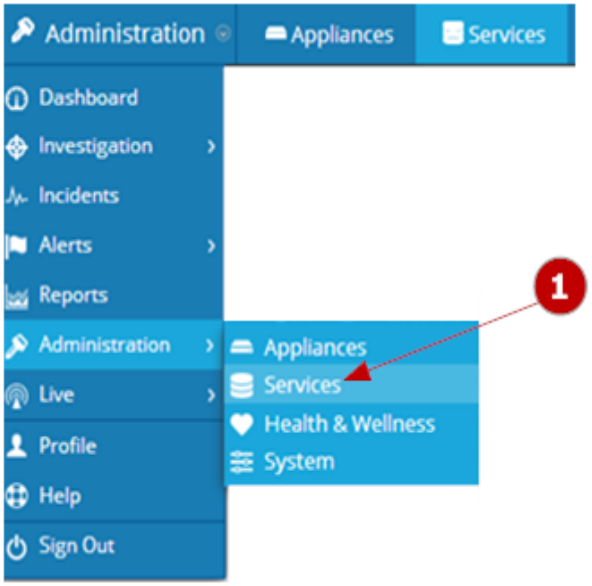


2 Configure orígenes de eventos:

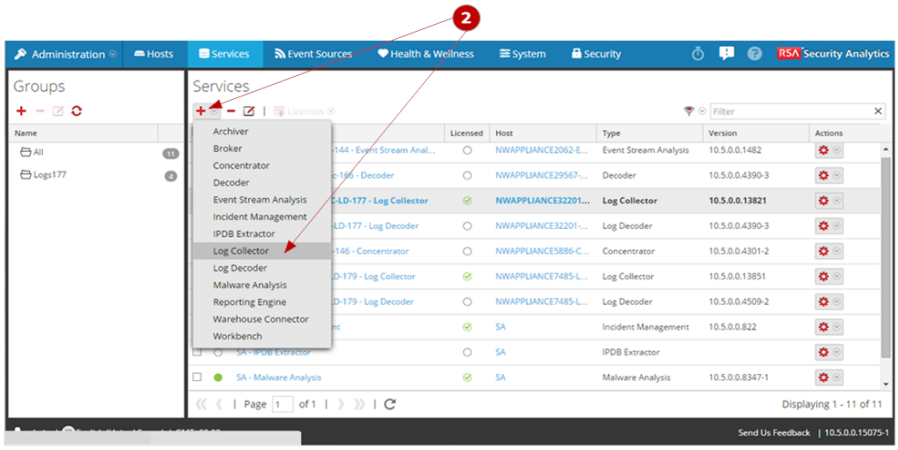
- Configure protocolos de recopilación en Security Analytics.
- Configure cada origen de eventos para que se comunique con Security Analytics Log Collector.

Adición de Local Collector y Remote Collector a Security Analytics

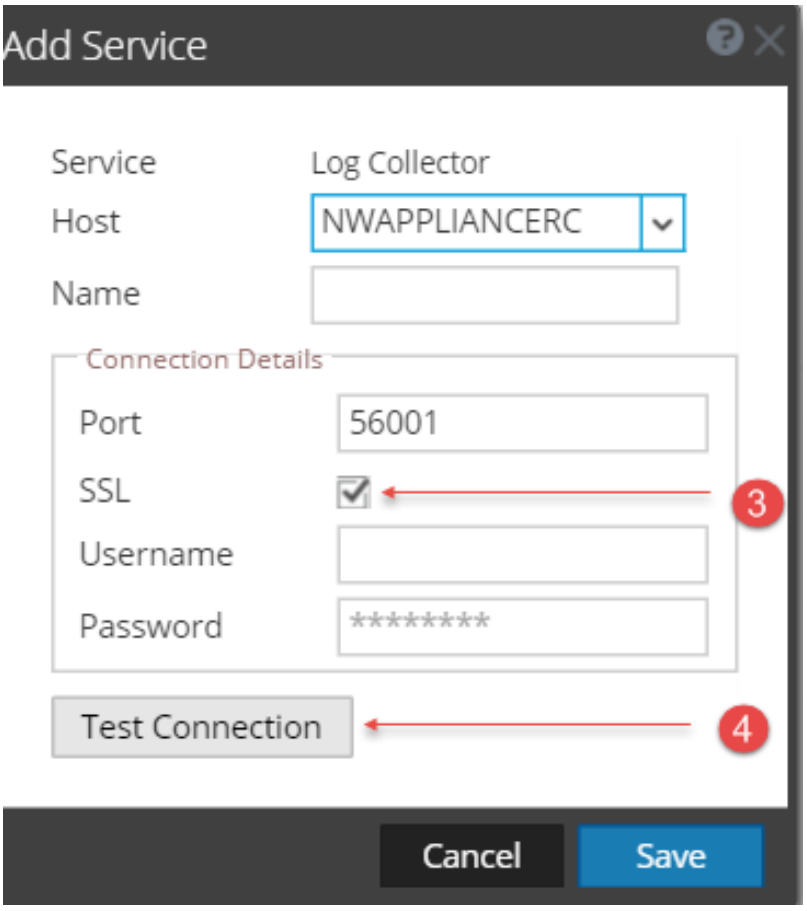
En la siguiente figura se muestra cómo agregar un Local Collector y un Remote Collector a Security Analytics.



1 Acceda a la vista **Servicios**.



2 Abra el cuadro de diálogo **Agregar servicio**.

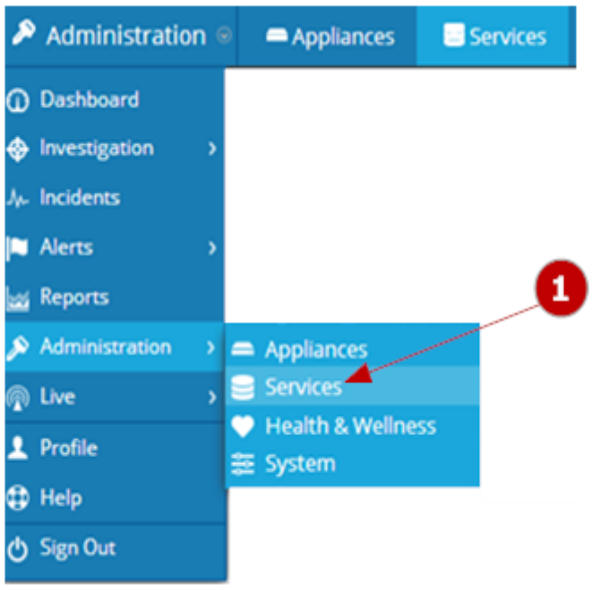


3 Defina los detalles del servicio de **recopilación de registros**.

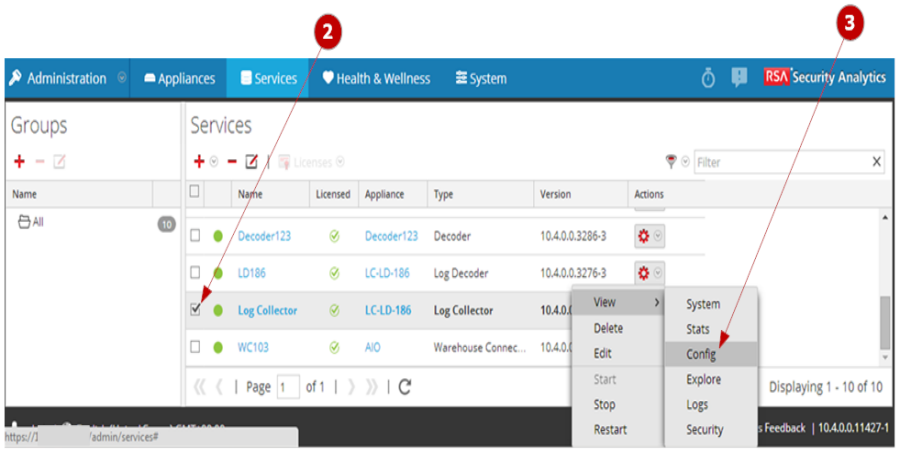
4 Seleccione **Probar conexión** para verificar la adición del Local Collector o del Remote Collector.

Configuración de la recopilación de registros

Debe elegir el Log Collector, es decir un Local Collector (LC) o un Remote Collector (RC), para el cual desea definir parámetros en la vista Servicios. En la siguiente figura se muestra cómo navegar a la vista Servicios, seleccionar un servicio Log Collector y mostrar la interfaz de parámetros de configuración de ese servicio.

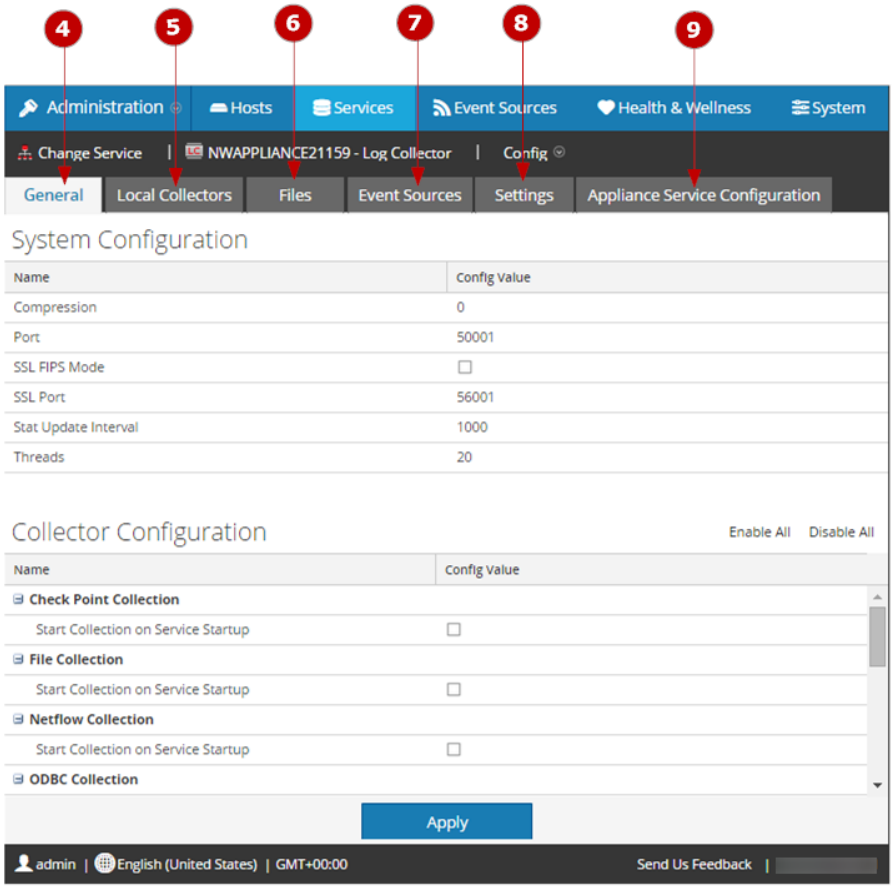


1 Acceda a la vista **Servicios**.



2 Seleccione un servicio de **recopilación de registros**.

3 Haga clic en ⌄ bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



4 Defina los parámetros globales de recopilación de registros en la pestaña **General**.

5 Para un:

- Local Collector, Security Analytics muestra la pestaña **Remote Collectors**. En esta pestaña, seleccione los Remote Collectors desde los cuales el Local Collector extrae eventos.
- Remote Collector, Security Analytics muestra **Local Collectors**. En esta pestaña, seleccione los Local Collectors a los cuales el Remote Collector migra eventos.

6 Edite los archivos de configuración como archivos de texto en la pestaña **Archivos**.

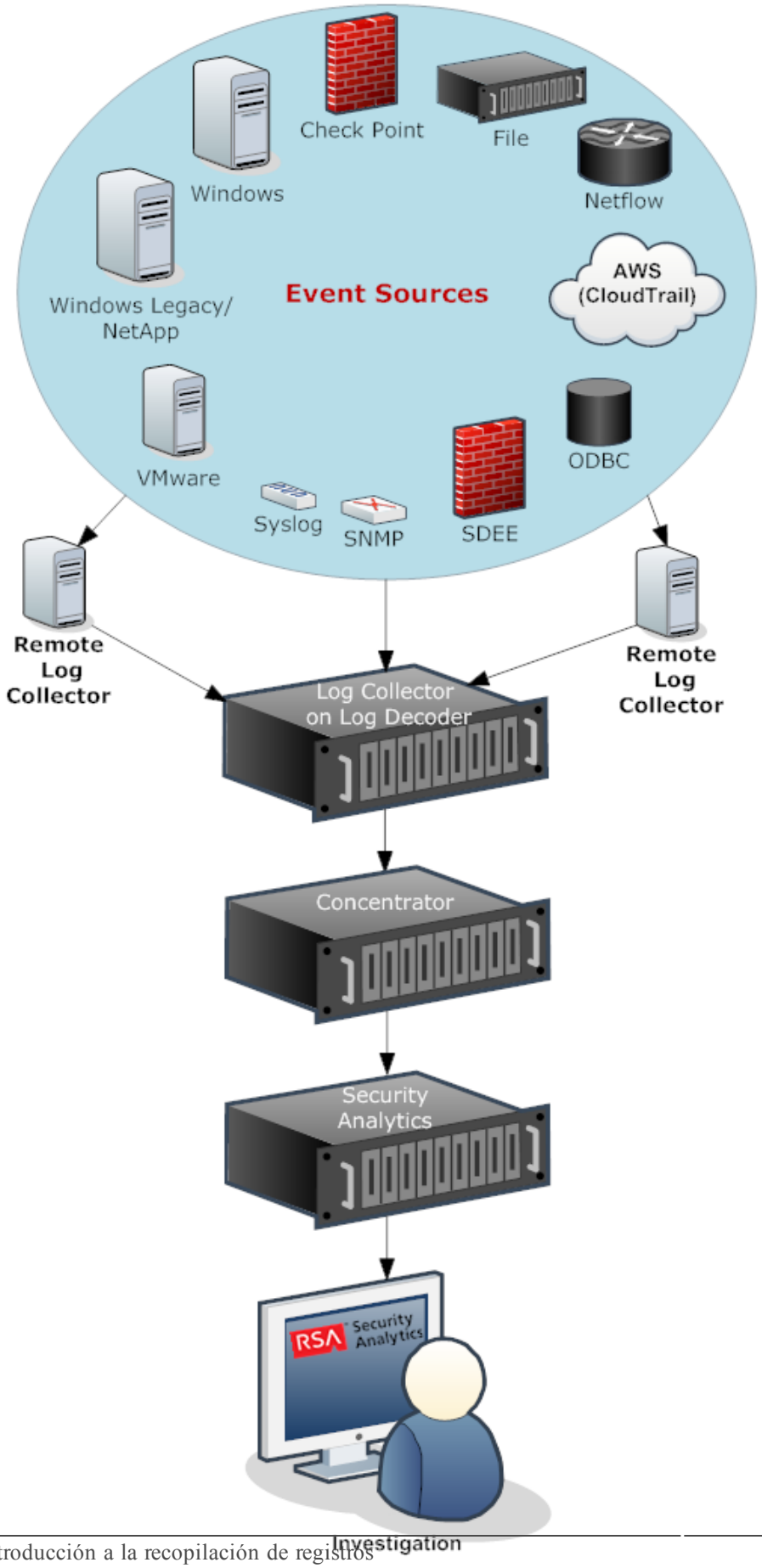
7 Defina parámetros del protocolo de recopilación en la pestaña **Orígenes de evento**.

8 Defina el Lockbox, claves de cifrado y certificados en la pestaña Configuración.

9 Defina parámetros del servicio Appliance en la pestaña **Configuración del servicio Appliance**.

Diagrama del flujo de datos

Puede usar los datos de log recopilados por el servicio de Log Collector para supervisar el estado de su empresa y realizar investigaciones. En la siguiente figura se muestra cómo es el flujo de datos desde la recopilación de registros de Security Analytics hasta Investigation.


Check Point
File
Windows
Netflow
Windows Legacy/
NetApp
Event Sources
AWS
(CloudTrail)
VMware
ODBC
Syslog
SNMP
SDEE
Remote
Log
Collector
Remote
Log
Collector
Log Collector
on Log Decoder
Concentrator
Security
Analytics
RSA Security Analytics
Investigation

Procedimientos

En este tema se proporciona una descripción general de los pasos secuenciales de punto a punto que debe realizar para comenzar a recopilar eventos.

Lista de verificación general

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción
1	Agregar Local y Remote Collectors a Security Analytics.
2	Descargar el contenido más reciente de LIVE.
3	Configurar el Lockbox.
4	Configurar protocolos de recopilación y orígenes de eventos.
5	Iniciar el servicio de recopilación para los protocolos de recopilación configurados.
6	Verifique que la recopilación de registros funcione.

Paso 1. Agregar Local y Remote Collectors

En este tema se indica cómo realizar la instalación inicial de Local Collectors y Remote Collectors para que pueda configurarlos.

Después de realizar este procedimiento, habrá...

- Agregado un servicio Local Collector.
- Agregado un servicio de Remote Collector

Verificar que Log Decoder está configurado

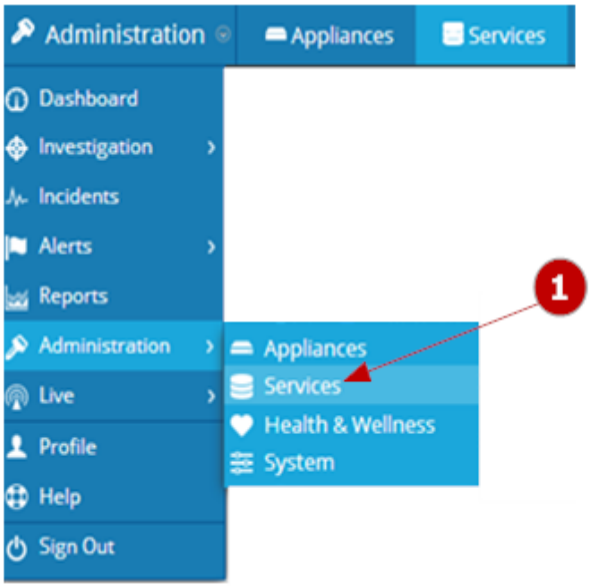
Verifique que Log Decoder:

- Esté capturando datos.
- Tenga el contenido actual cargado.
- Tenga la licencia correcta.

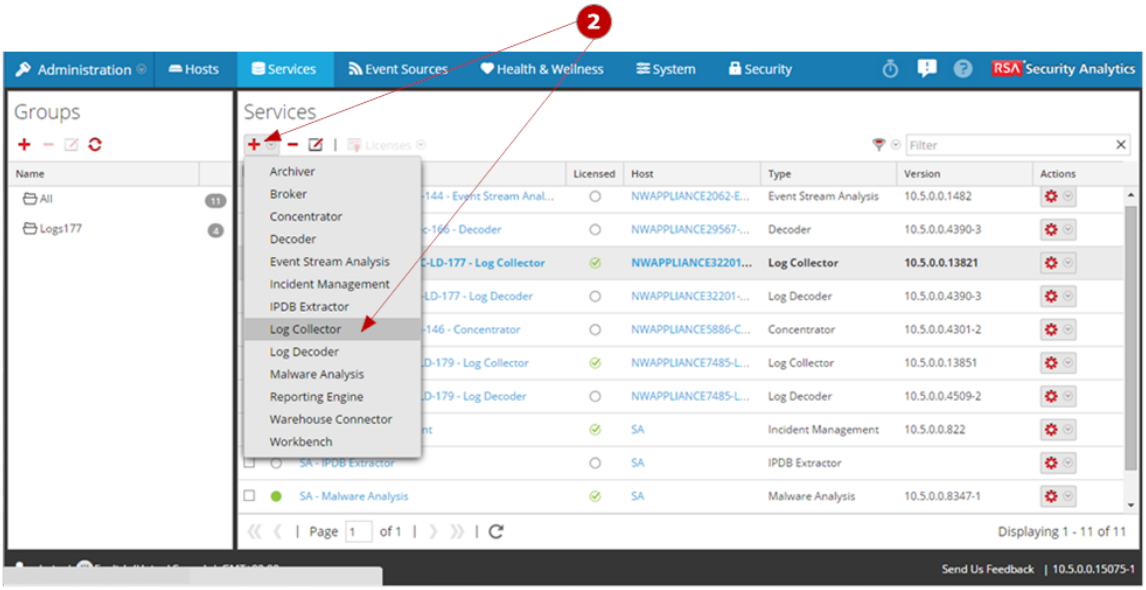
Consulte la *Guía de configuración de Log Decoder* para obtener instrucciones para configurar Log Decoder.

Agregar un Local Collector

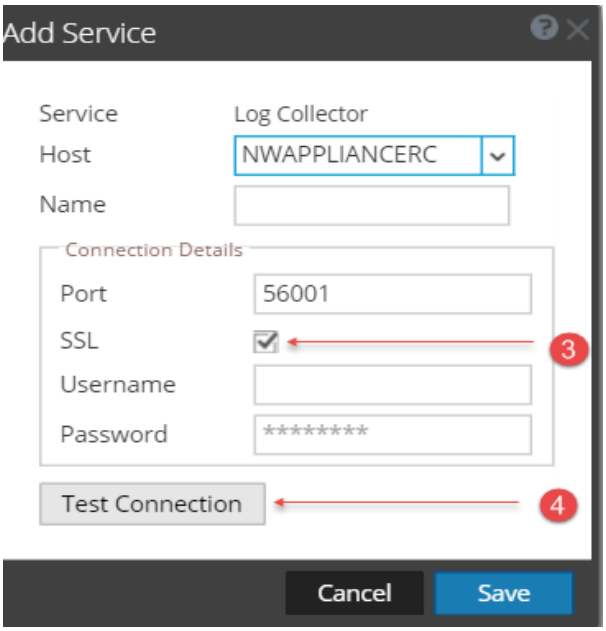
Puede agregar un Local Collector si agrega el servicio Log Collector a un host de Log Decoder en Security Analytics, como se muestra en la siguiente figura.



1 Acceda a la vista **Servicios**.



2 Abra el cuadro de diálogo **Agregar servicio**.



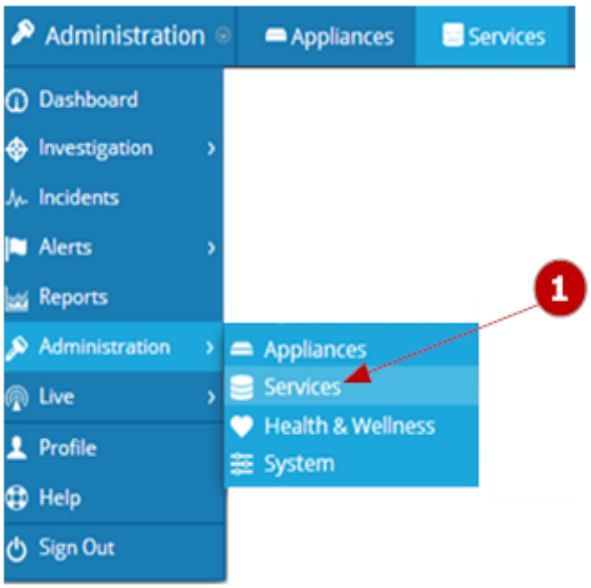
3 Defina los detalles de conexión del servicio de recopilación de registros en un Local Collector.

4 Haga clic en **Probar conexión**. Si la conexión es válida, verá La conexión se prueba se estableció correctamente. Si la conexión falla, verá Falla. Si falla, asegúrese de que el host de Log Decoder esté en ejecución y que se haya ingresado la información correcta en el cuadro de diálogo **Agregar servicio**, y haga clic en **Guardar**.

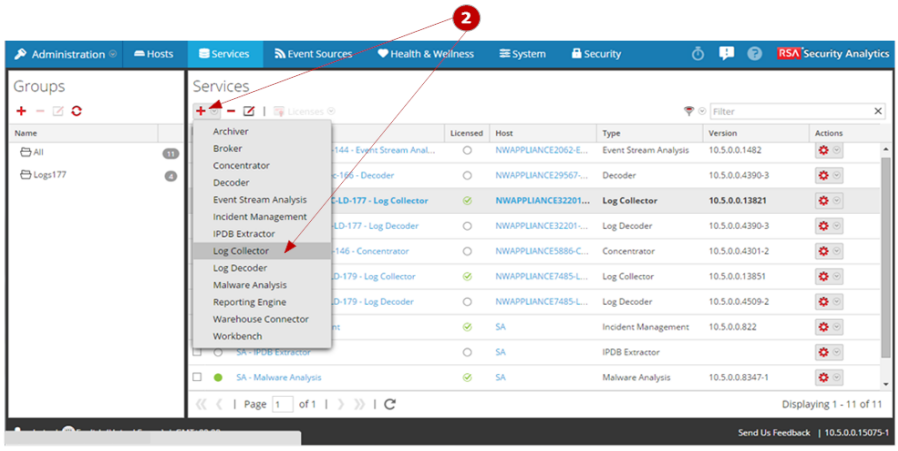
Agregar un Remote Collector (opcional)

Puede agregar un Remote Collector si agrega el servicio Log Collector a un host remoto, como se muestra en la siguiente figura.

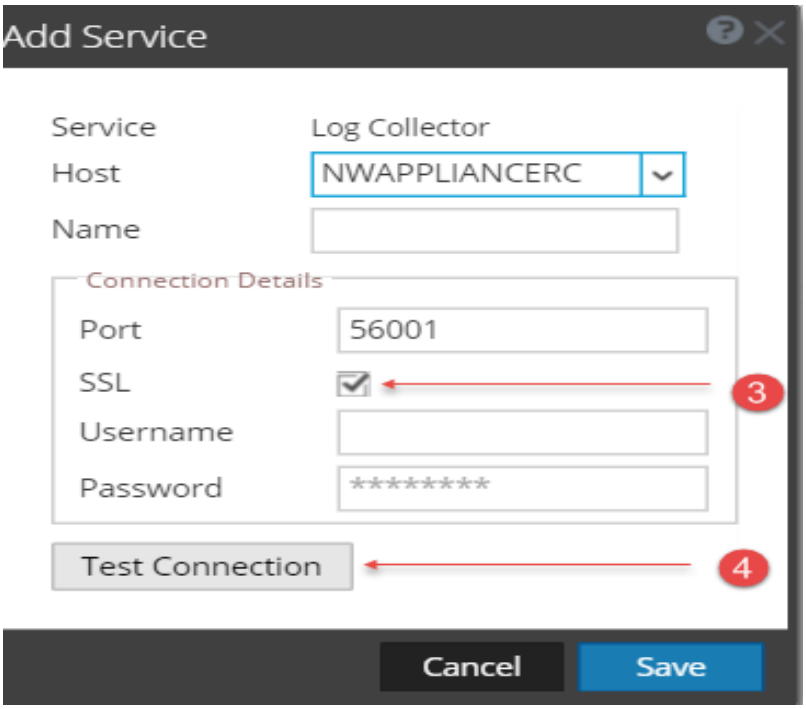
Nota: Antes de agregar un Remote Collector de Windows heredado, debe instalar el recopilador de Windows heredado de Security Analytics en un servidor Windows 2008 SP1 de 64 bits físico o virtual mediante **SALegacyWindowsCollector-*version-number.exe***. El archivo **SALegacyWindowsCollector-*version-number.exe*** se descarga desde SCOL (consulte las instrucciones de la *Guía de configuración de eventos de Windows heredado de Microsoft Windows*).



1 Acceda a la vista **Servicios**.



2 Abra el cuadro de diálogo **Agregar servicio**.



3 Defina los detalles de conexión del servicio de recopilación de registros en un Remote Collector y haga clic en **Guardar**.

4 Haga clic en **Probar conexión**. Si la conexión es válida, verá La conexión se prueba se estableció correctamente. Si la conexión falla, verá Falla. Si falla, asegúrese de que el host de Log Decoder esté en ejecución y que se haya ingresado la información correcta en el cuadro de diálogo **Agregar servicio**, y vuelva a hacer clic en **Guardar**.

Paso 2. Descargar el contenido más reciente de LIVE

En este tema se le dirige a la documentación de Contenido y recursos de RSA, donde encontrará instrucciones para recuperar contenido de la recopilación de registros.

Volver a Procedimientos

LIVE es el sistema de administración de contenido de Security Analytics que permite descargar el contenido más reciente. Los dos tipos de recursos que se usan para descargar contenido de recopilación de registros son:

- **RSA Log Collector**: Contenido que permite recopilar tipos de orígenes de eventos.
- **RSA Log Device**: los últimos analizadores de orígenes de eventos compatibles. **Consulte Adición o actualización de analizadores de registros de orígenes de eventos compatibles**

en la *Guía de contenido y recursos de RSA* para obtener instrucciones sobre cómo descargar analizadores de registros desde LIVE.

Paso 3. Configurar un Lockbox

En este tema, se explica cómo cambiar la configuración de seguridad de lockbox.

Qué es un Lockbox

Un Lockbox es un archivo cifrado que se usa para almacenar información confidencial sobre una aplicación. Security Analytics Lockbox almacena una clave de cifrado para el Log Collector.

La clave de cifrado se usa para cifrar todas las contraseñas de origen de eventos y la contraseña del intermediador de eventos.

Cuando crea el Lockbox, debe definir una contraseña para el Lockbox.

Durante la recopilación de datos, Log Collector usa el Lockbox en un modo que no requiere que se especifique la contraseña (Log Collector usa en su lugar la huella digital del sistema host).

Los siguientes son los ajustes de seguridad de lockbox.

Característica	Descripción
Contraseña anterior de lockbox	Cuando configure un lockbox por primera vez, este campo estará en blanco. Security Analytics completa este campo una vez que se ingresa una Nueva contraseña de Lockbox y se hace clic en Aplicar.
Nueva contraseña de lockbox	Contraseña inicial o nueva del lockbox. Para maximizar la seguridad del Lockbox, especifique una contraseña que tenga ocho o más caracteres de longitud con al menos un carácter numérico, un carácter en mayúsculas y un carácter que no sea alfanumérico, como # o !
Aplicar	Haga clic en **Aplicar** para guardar los cambios realizados en la contraseña del lockbox.

Configurar un Lockbox

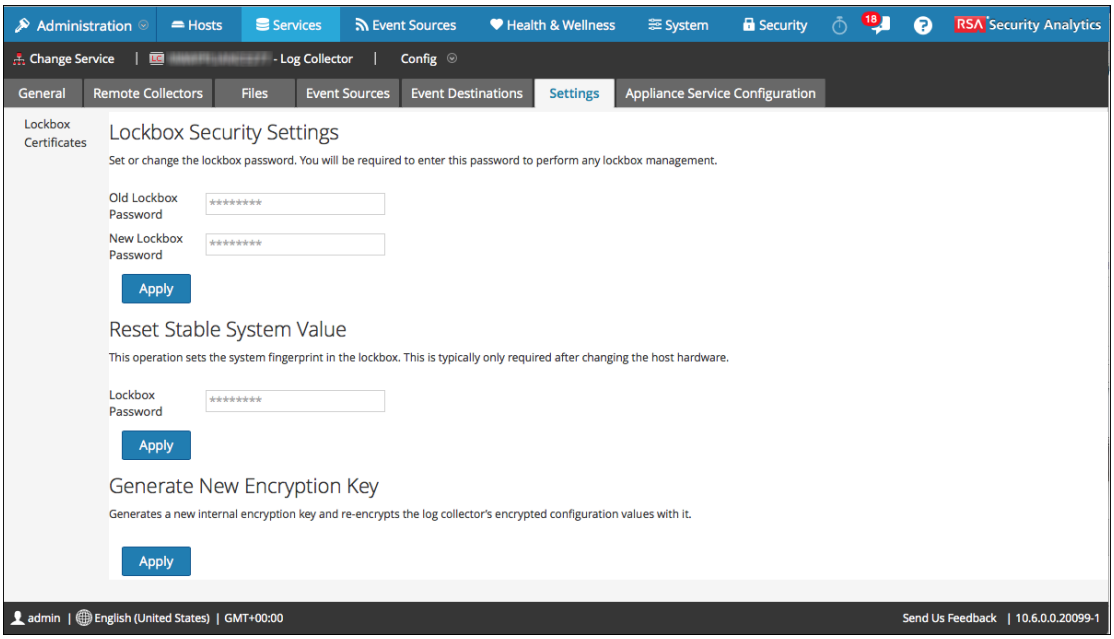
Para configurar un Lockbox debe establecer una contraseña de la siguiente manera:

1. En el menú de Security Analytics, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un servicio **Log Collector**.

3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.

   La vista Configuración del servicio se muestra con la pestaña **General de Log Collector** abierta.

4. Haga clic en la pestaña **Configuración**.



5. En el panel de opciones, seleccione **Lockbox** para establecer la configuración de Lockbox.
6. En **Configuración de seguridad de lockbox**, ingrese una contraseña en el campo **Nueva contraseña de Lockbox** y haga clic en **Aplicar**.

Paso 4. Configurar protocolos y orígenes de eventos de recopilación

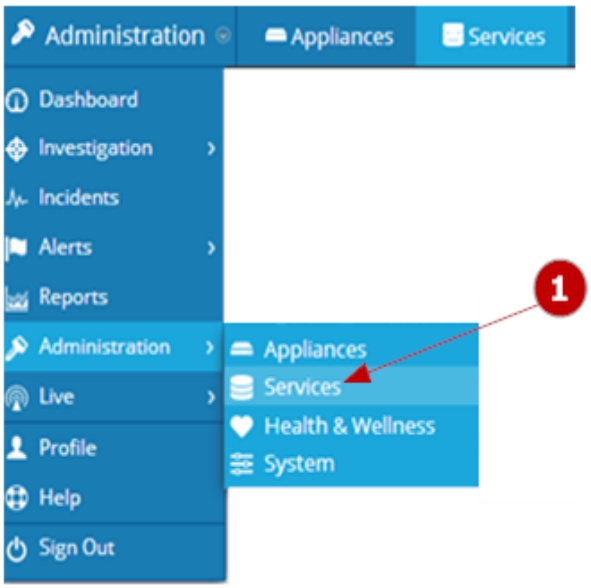
En este tema se describe cómo configurar los protocolos de recopilación y los orígenes de eventos mediante esos protocolos.

Debe configurar Log Collector para recopilar datos de eventos de orígenes de eventos en la pestaña Orígenes de evento de la vista de parámetros de recopilación de registros.

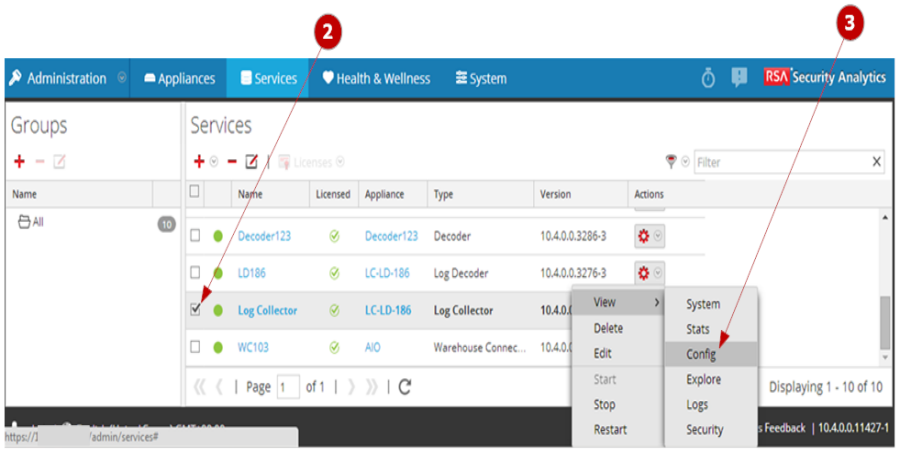
Procedimientos

Configurar un protocolo de recopilación

En la siguiente figura se muestra el flujo de trabajo básico para configurar un origen de eventos en Security Analytics. Cada origen de eventos tiene parámetros diferentes por lo que debe consultar las guías correspondientes al origen de eventos que se configura para obtener todas las instrucciones.

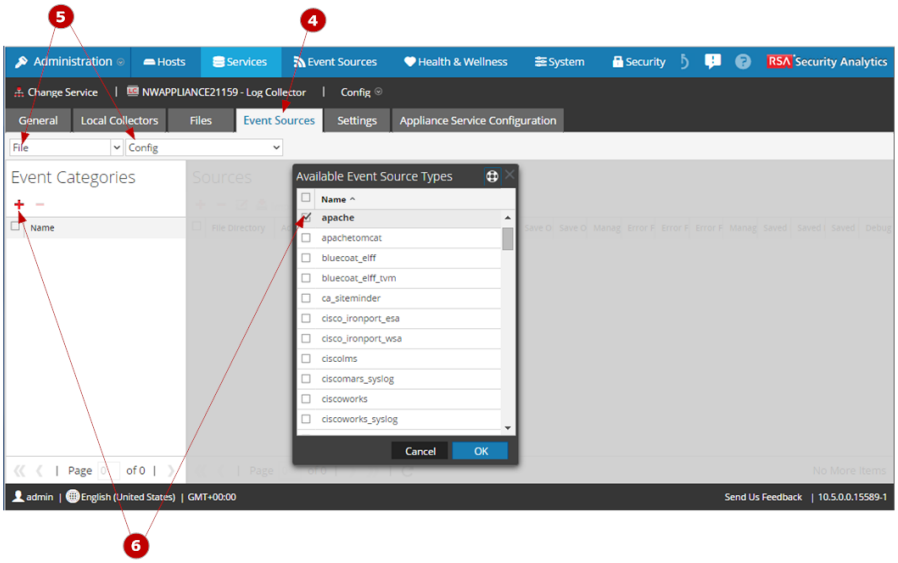


1 Acceda a la vista Servicios.



2 Seleccione un servicio de recopilación de registros.

3 Haga clic en ⌄ bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.

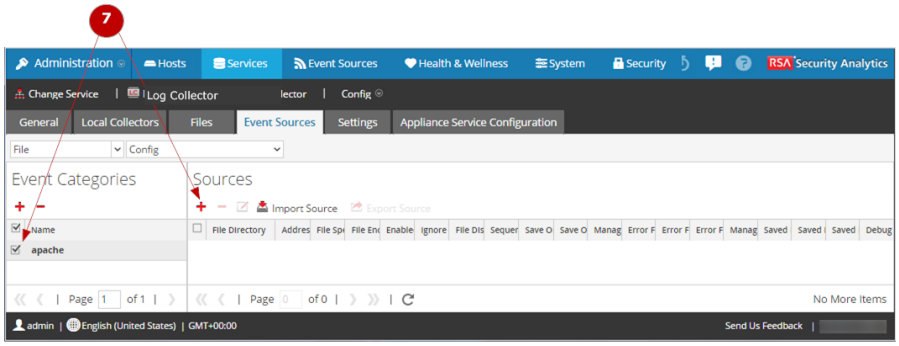


4 Haga clic en la pestaña **Orígenes de evento**.

5 Seleccione un protocolo de recopilación (por ejemplo, **Archivo**) y seleccione **Configurar**.

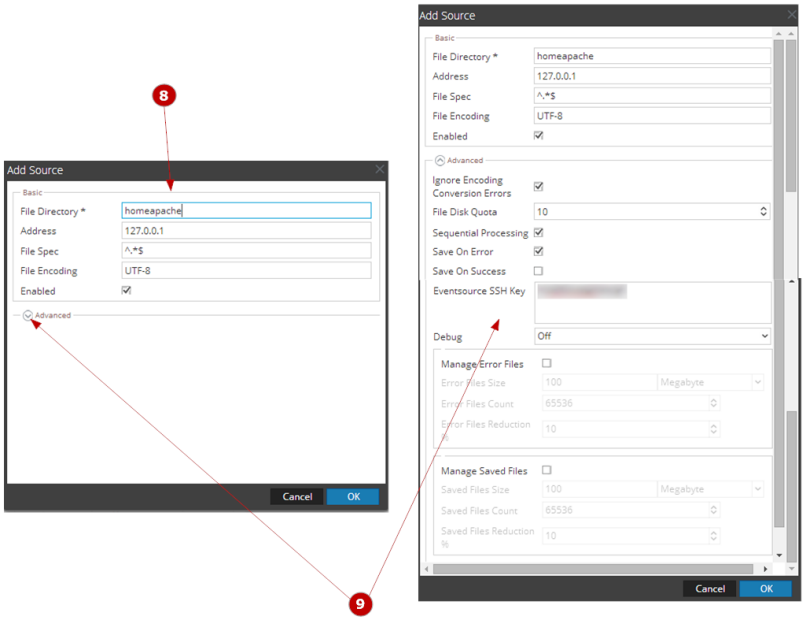
6 Haga clic en + y seleccione una categoría de origen de eventos (por ejemplo, **apache**).

La categoría de origen de eventos es parte del contenido que descargó de LIVE.



7 Seleccione la categoría recién agregada (por ejemplo, **apache**).

Haga clic en +.



8 Especifique los parámetros básicos requeridos para el origen de eventos.

9 Haga clic en y especifique parámetros adicionales que mejoran la manera en que el protocolo maneja la recopilación de eventos para el origen de eventos.

Guías de los protocolos de recopilación individuales

En las siguientes guías se proporcionan instrucciones detalladas para configurar los protocolos de recopilación y sus orígenes de eventos asociados en Security Analytics. En cada guía se incluye un índice para las instrucciones de configuración de los orígenes de eventos compatibles para ese protocolo de recopilación.

Configure protocolos de recopilación individuales. Las instrucciones se encuentran en las guías de recopilación de registros individuales:

- Guía de configuración de la recopilación de AWS (CloudTrail)
- Guía de configuración de la recopilación de punto de comprobación
- Guía de configuración del protocolo de recopilación de archivos
- Guía de configuración de la recopilación de Netflow
- Guía de configuración de la recopilación de ODBC
- Guía de configuración de la recopilación de SDEE
- Guía de configuración de la recopilación de SNMP
- Guía de configuración de la recopilación de VMware
- Guía de configuración de la recopilación de Windows
- Guía de configuración de la recopilación de Windows existente y NetApp
- Las guías de configuración de cada origen de eventos compatible están disponibles en la página Orígenes de eventos compatibles.

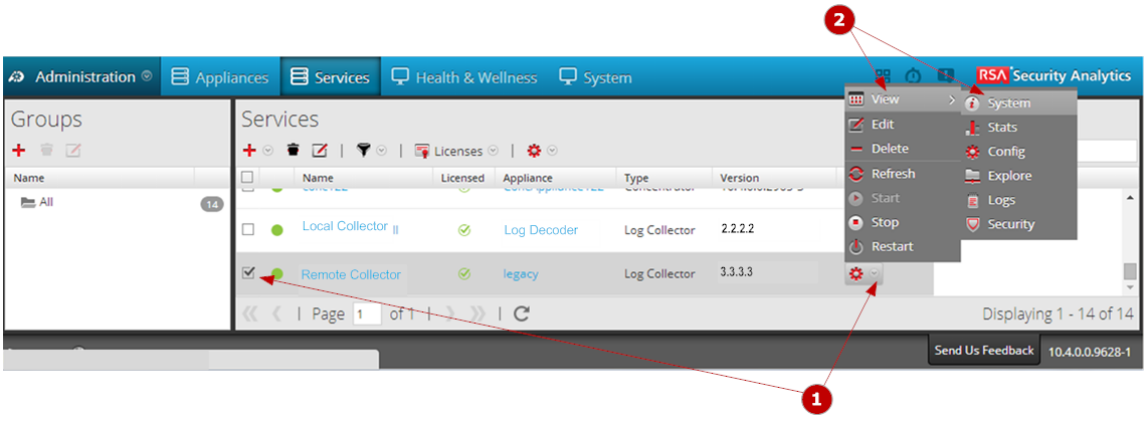
Paso 5. Iniciar servicios de recopilación y habilitar el inicio automático

Si un servicio de recopilación se detiene, tal vez deba iniciarlo nuevamente. También puede habilitar el inicio automático de servicios de recopilación.

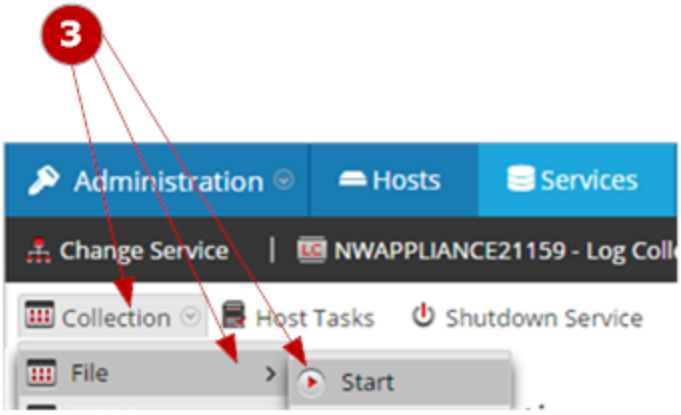
Iniciar un servicio de recopilación

Volver a Procedimientos

En la siguiente figura se muestra cómo iniciar un servicio de recopilación.



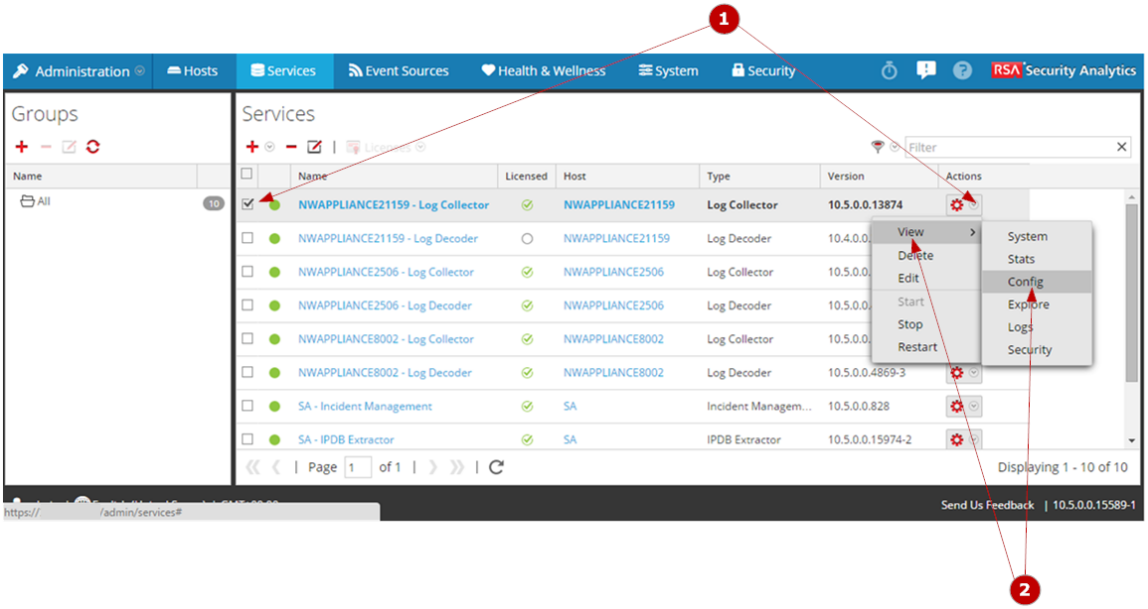
1. Seleccione un servicio Log Collector y haga clic en bajo Acciones.
2. Haga clic en Ver > Sistema.



3. Haga clic en Recopilación > servicio (por ejemplo, Archivo) y, a continuación, en Iniciar.

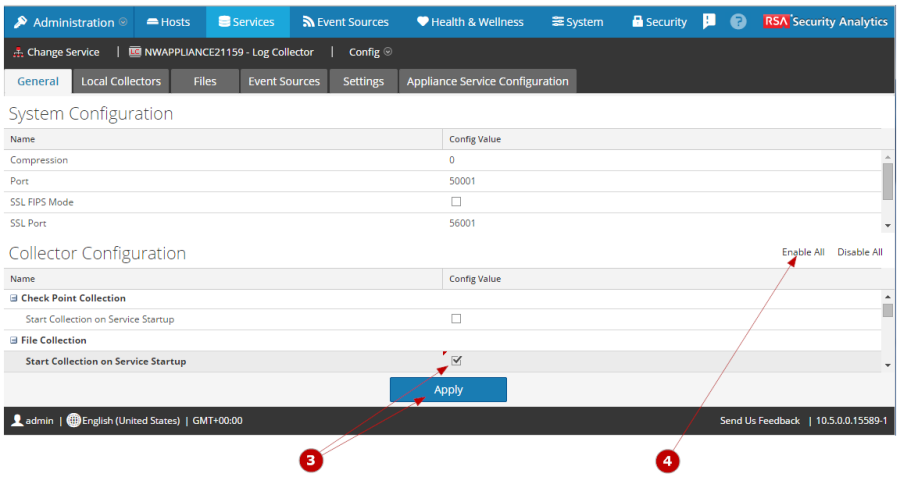
Habilitar el inicio automático de servicios de recopilación

En la siguiente figura se muestra cómo habilitar el inicio automático de un servicio de recopilación.



1 Seleccione un servicio Log Collector y haga clic en ⌄ bajo Acciones.

2 Haga clic en **Ver > Configuración**.



3 Seleccione la casilla de verificación **Iniciar la recopilación en el arranque del servicio** para un servicio de recopilación (por ejemplo, **Archivo**) y haga clic en **Aplicar**.

4 (Opcional) Puede hacer clic en Enable All y, a continuación, en Aplicar para establecer el inicio de cada servicio de recopilación en el arranque del servicio Log Collector.

Paso 6. Verificar que la recopilación de registros esté funcionando

En este tema se indica cómo verificar la correcta configuración de la recopilación de registros.

Debe verificar que la recopilación de registros se haya configurado correctamente; de lo contrario, podría no funcionar.

Los siguientes métodos permiten verificar que la recopilación de registros esté funcionando.

- Verifique que haya actividad de evento en la pestaña Monitoreo de orígenes de eventos de **Administration > vista Estado y condición**.
- Verifique que haya analizadores en el campo **device.type** de la columna **Detalles** de **Investigation > vista Eventos** para el protocolo de recopilación que configuró.

Consulte los pasos para verificar que el protocolo esté configurado correctamente en la *Guía de configuración de la recopilación de registros* de cada protocolo de recopilación.

Referencia: Interfaz de parámetros de configuración

Temas de referencia para el parámetro de configuración de la recopilación de registros y la interfaz del usuario de comandos del sistema:

- Interfaz de parámetros de configuración de Log Collector: En la vista Configuración del servicio Log Collector se mantienen todos los parámetros de configuración de Log Collector.
- Interfaz de la vista Sistema del servicio de recopilación de registros: En la vista Sistemas de Log Collector se ejecutan todos los comandos del sistema Log Collector y se revisa el estado del servicio.

Interfaz de parámetros de configuración de Log Collector

En este tema se señala la documentación de referencia para la interfaz del usuario del parámetro Log Collection.

La vista Configuración del servicio Log Collector es la vista en la cual se mantienen todos los parámetros de Log Collector. En los siguientes diagramas se muestra dónde buscar la documentación de cada pestaña en la vista Parámetros.

Pestaña	Descripción	Se describe en esta guía
Aspectos generales	Parámetros de alto nivel que controlan la operación del servicio Log Collector y cada protocolo de recopilación.	Guía de configuración de la recopilación de registros

Pestaña	Descripción	Se describe en esta guía
Remote/Local Collectors	Para Local Collector, la pestaña **Remote Collectors** define desde qué Remote Collectors (RC) envía eventos Local Collector. Para Remote Collector, la pestaña **Local Collectors** define a qué Local Collectors (LC) envía eventos Remote Collector.	Guía de implementación de la recopilación de registros
Orígenes de eventos	Protocolos de recopilación compatibles.	Guía de configuración de la recopilación de AWS (CloudTrail) Guía de configuración de la recopilación de punto de comprobación Guía de configuración del protocolo de recopilación de archivos Guía de configuración de la recopilación de Netflow Guía de configuración de la recopilación de ODBC Guía de configuración de la recopilación de SDEE Guía de configuración de la recopilación de SNMP Guía de configuración de la recopilación de VMware Guía de configuración de la recopilación de Windows Guía de configuración de la recopilación de Windows existente y NetApp
Configuración	Lockbox, clave de cifrado y certificados	Guía de configuración de la recopilación de registros

Interfaz de la vista Sistema del servicio de recopilación de registros

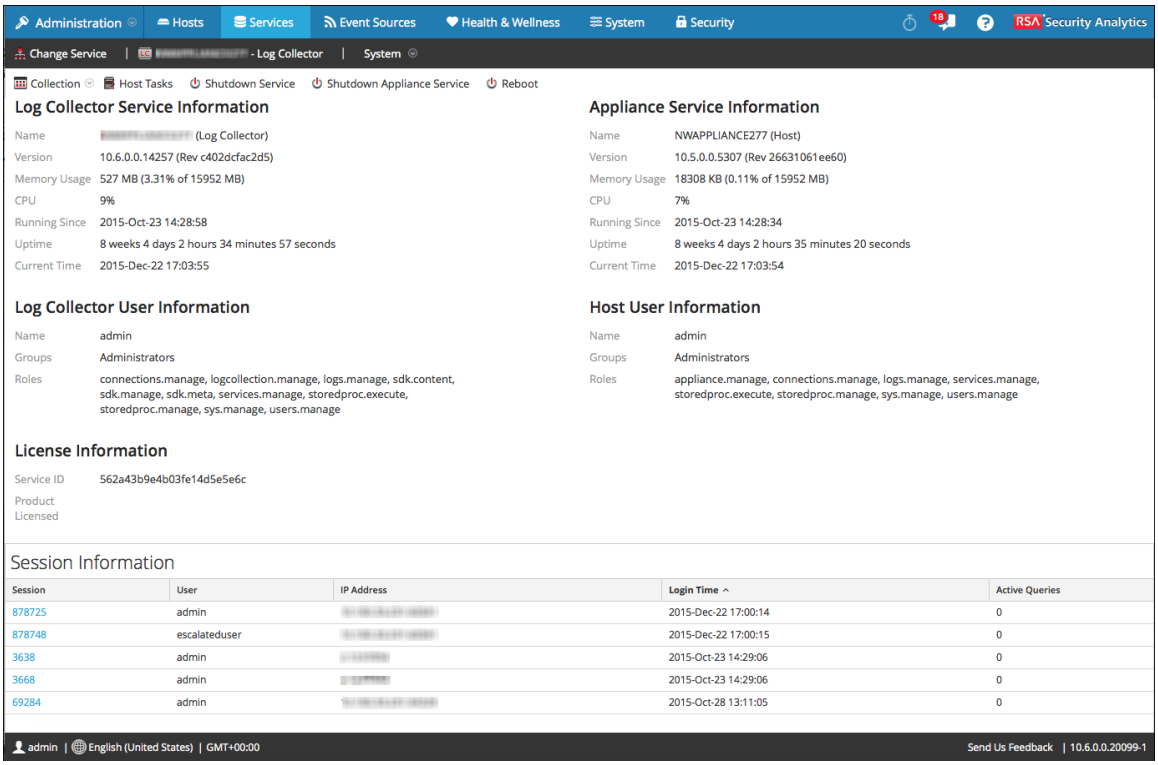
En este tema se presentan las funcionalidades de la vista Sistema relacionadas específicamente con la recopilación de registros.

Log Collector es un servicio que se ejecuta en un host de Log Decoder (conocido como un Local Collector) o que envía eventos desde un Remote Collector a un Local Collector, y se configura y administra de manera similar a un Log Decoder. Por lo tanto, la mayor parte de la información en esta sección se refiere a los Decoders en general. Se especifican las diferencias para los Log Collectors. Para mostrar esta vista:

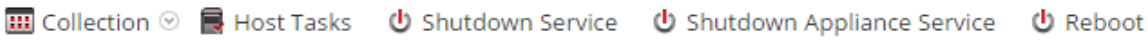
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.

   Se muestra la vista Servicios de Administration.

2. Haga clic en la casilla de verificación junto a un Log Collector y seleccione **Ver > Sistema**.



Barra de herramientas de Información del servicio



La barra de herramientas Información del servicio comparte muchas opciones con la barra de herramientas de la vista Sistema de servicio. En la siguiente tabla se describen las opciones que son únicas de la barra de herramientas Información del servicio.

Acción	Descripción
Collection	Muestra una lista de los protocolos de recopilación y ofrece las opciones: • **Iniciar**: iniciar la recopilación de datos de eventos desde un protocolo detenido. • **Detener**: detener la recopilación de datos de eventos desde un protocolo iniciado. • **Pausar**: pausar la recopilación de datos de eventos desde un protocolo iniciado. Consulte la Paso 5. Iniciar servicios de recopilación y habilitar el inicio automático

Solución de problemas de la recopilación de registros

En este tema se describe el formato y el contenido de la solución de problemas de la recopilación de registros. Security Analytics le informa sobre problemas o posibles problemas de Log Collector de las dos maneras siguientes.

- Archivos de registro.
- Vistas de monitoreo del estado y la condición.

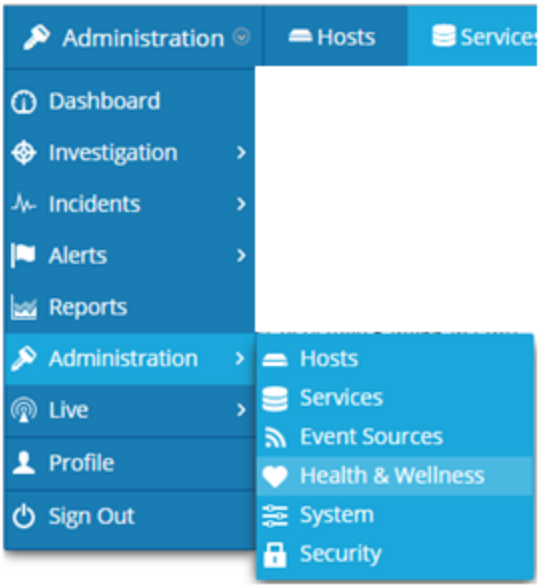
Archivos de registro

Si un protocolo de recopilación de orígenes de eventos específico presenta problemas, puede revisar los registros de depuración para investigarlos. Cada origen de eventos posee un parámetro de Depuración que puede activar (configurar en Activado o Detallado) para capturar estos registros.

Precaución: Active la depuración solamente si este origen de eventos presenta problemas y necesita investigarlos. Si activa la depuración en todo momento, esta afectará negativamente al rendimiento de Log Collector.

Monitoreo del estado y la condición

El monitoreo del estado y la condición le permite informarse oportunamente de posibles problemas de hardware y software de modo que pueda evitar interrupciones. RSA recomienda monitorear los campos estadísticos de Log Collector para asegurarse de que el servicio funcione de manera eficiente y que no se encuentre en los valores máximos configurados ni cerca de estos. Puede monitorear las siguientes estadísticas que se describen en la vista **Administration > Estado y condición**.



Ejemplo de formato de solución de problemas

Security Analytics devuelve los siguientes tipos de mensajes de error en los archivos de registro.

Mensajes de registro	`timestamp failure (LogCollection) Message-Broker Statistics: …`
	
	`timestamp failure (AMQPClientBaseLogCollection): …`
	`timestamp failure (MessageBrokerLogReceiver): …`

Causa posible	El Log Collector no puede comunicarse con el Message Broker porque el Message Broker: • dejó de funcionar. • posee una configuración de conexión errónea.

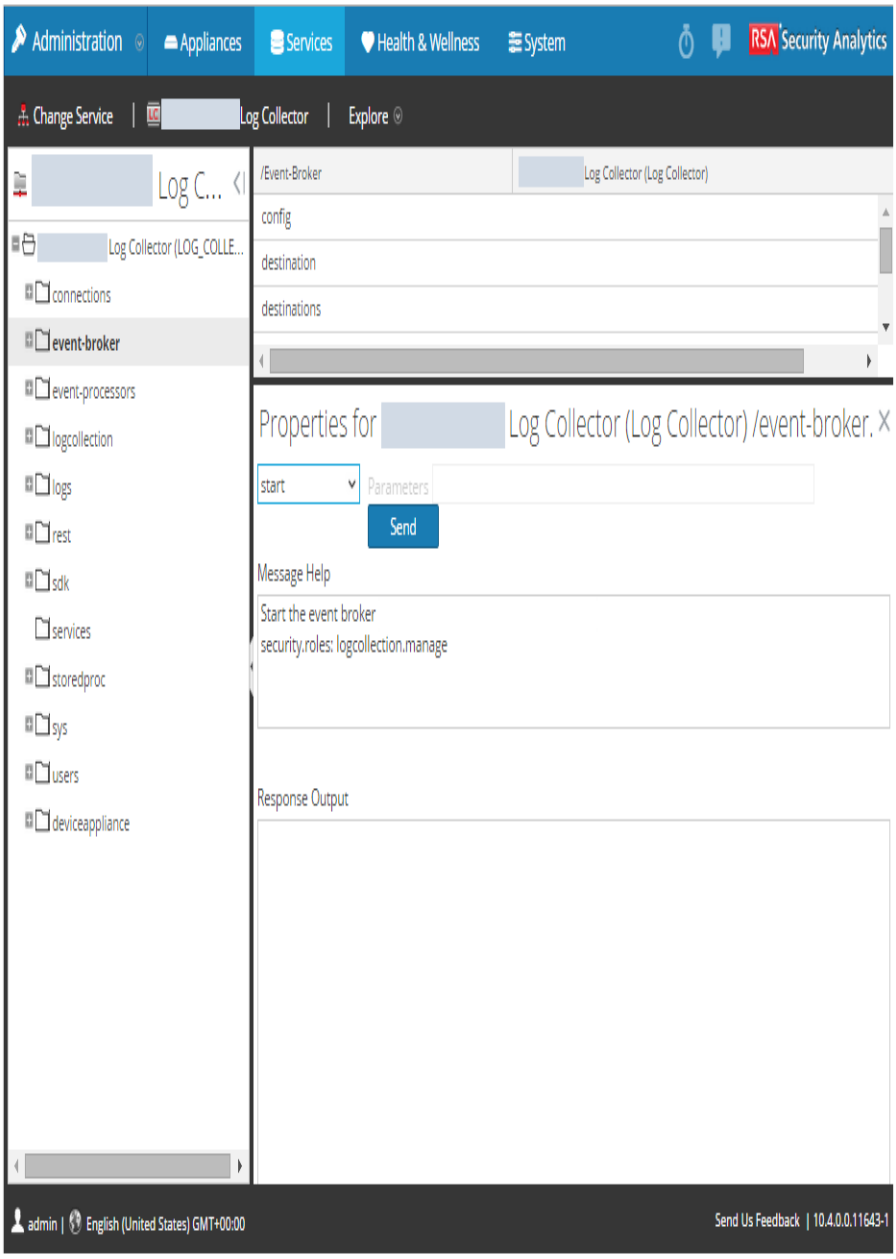
Soluciones

1. <use the="the" initctl="initctl" command="command" on="on" console="console" to="to" check="check" status="status" of="of" message="message" broker="broker" shell="shell" console.="console.">returns the following if the message broker is not running:</use>

```
prompt$ status rabbitmq

rabbitmq start/running, process 10916
```

2. Inicie el RabbitMQ Message Broker en el nodo event-broker en la vista Explorar:


Administration
Appliances
Services
Health & Wellness
System
RSA Security Analytics
Change Service
Log Collector
Explore
Log C...
Log Collector (LOG_COLLE...
connections
event-broker
event-processors
logcollection
logs
rest
sdk
services
storedproc
sys
users
deviceappliance
/Event-Broker
Log Collector (Log Collector)
config
destination
destinations
Properties for
Log Collector (Log Collector) /event-broker.
start
Parameters
Send
Message Help
Start the event broker
security.roles: logcollection.manage
Response Output
admin |
English (United States) GMT+00:00
Send Us Feedback | 10.4.0.0.11643-1

Guía de implementación de la recopilación de registros

En esta guía se indica cómo implementar la recopilación de registros en el dominio de Security Analytics. Se proporcionan instrucciones de implementación detalladas (es decir, cómo configurar Local y Remote Collectors). No contiene información global sobre la recopilación de registros ni los protocolos de recopilación individuales.

En esta guía se indica cómo configurar las implementaciones de recopilación de registros actualmente disponibles en Security Analytics.

Esta guía no le indica cómo:

- Dar los primeros pasos con la creación de la implementación y la configuración mínimas y básicas. Esta información se encuentra en la Guía de introducción a la recopilación de registros.
- Configurar la recopilación de registros por completo después de la implementación. Esta información se encuentra en la Guía de configuración de la recopilación de registros.
- Configure protocolos de recopilación individuales. Las instrucciones se encuentran en las guías de recopilación de registros individuales:
  - Guía de configuración de la recopilación de AWS (CloudTrail)
  - Guía de configuración de la recopilación de punto de comprobación
  - Guía de configuración del protocolo de recopilación de archivos
  - Guía de configuración de la recopilación de Netflow
  - Guía de configuración de la recopilación de ODBC
  - Guía de configuración de la recopilación de SDEE
  - Guía de configuración de la recopilación de SNMP
  - Guía de configuración de la recopilación de VMware
  - Guía de configuración de la recopilación de Windows
  - Guía de configuración de la recopilación de Windows existente y NetApp
  - Las guías de configuración de cada origen de eventos compatible están disponibles en la página Orígenes de eventos compatibles.

Conceptos básicos

En este tema se describen los procedimientos básicos que debe completar para implementar Log

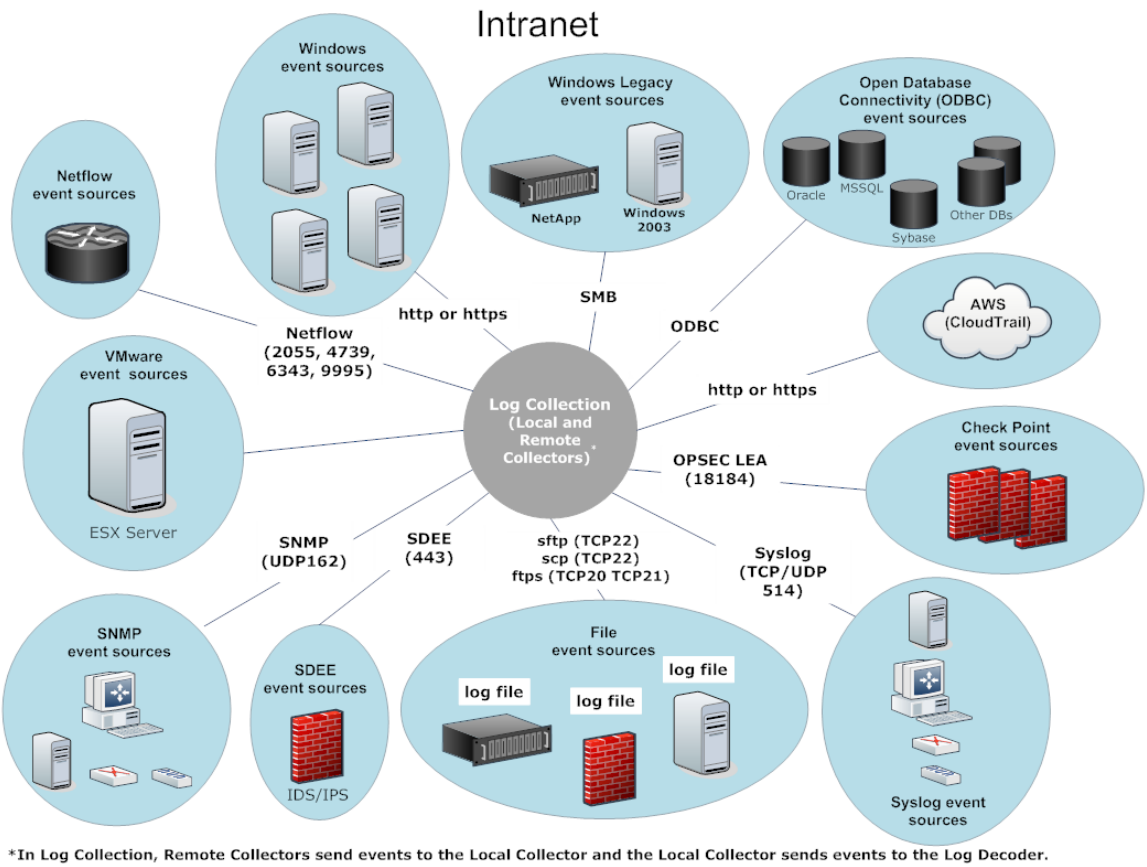
Collection con el fin de satisfacer las necesidades de su empresa

Cómo implementar Log Collection

Puede implementar Log Collection según las necesidades y preferencias de su empresa. Esto incluye implementar Log Collection a lo largo de múltiples ubicaciones y recopilar datos de varios conjuntos de orígenes de eventos. Puede hacer esto si configura un Local Collector con uno o varios Remote Collectors.

Componentes de Log Collection

En la siguiente figura se muestran todos los componentes que participan en la recopilación de eventos mediante Security Analytics Log Collector.



Para obtener más información sobre el contenido del origen de eventos de Log Collector, consulte el tema **Configurar orígenes de eventos para enviar eventos a Security Analytics** de la *Guía de configuración de la recopilación de registros*.

Local y Remote Collectors

En la siguiente figura se ilustra cómo interactúan Local y Remote Collectors para recopilar eventos desde todas sus ubicaciones.

En este escenario, la recopilación de registros desde varios protocolos, como Windows, ODBC, etc., se ejecuta mediante los servicios Remote Collector y Log Collector. Si la recopilación de registros se realiza mediante el Local Collector, se reenvía al servicio Log Decoder, al igual que en el escenario de implementación local. Si se realiza mediante un Remote Collector, existen dos métodos a través de los cuales se transfiere al Local Collector:

- **Extraer configuración**: En un Local Collector, seleccione los Remote Collectors desde los cuales desea extraer eventos.

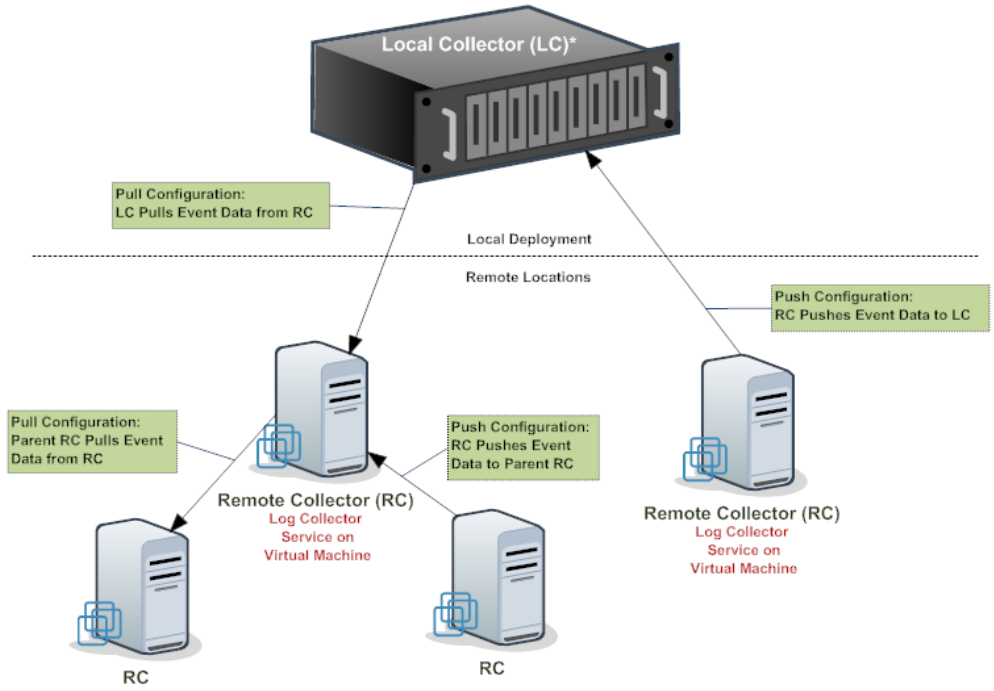
- **Migrar configuración:** En un Remote Collector, seleccione el Local Collector al cual desea migrar eventos.

Puede configurar uno o más Remote Collectors para migrar datos de eventos a un Local Collector, o puede configurar un Local Collector para extraer datos de eventos de uno o más Remote Collectors.

Para un Remote Collector 10.4 y versiones superiores, puede establecer una cadena de Remote Collectors para la cual puede configurar:

- Uno o más Remote Collectors para migrar datos de eventos a un Remote Collector.
- Un Remote Collector para extraer datos de eventos de uno o más Remote Collectors.

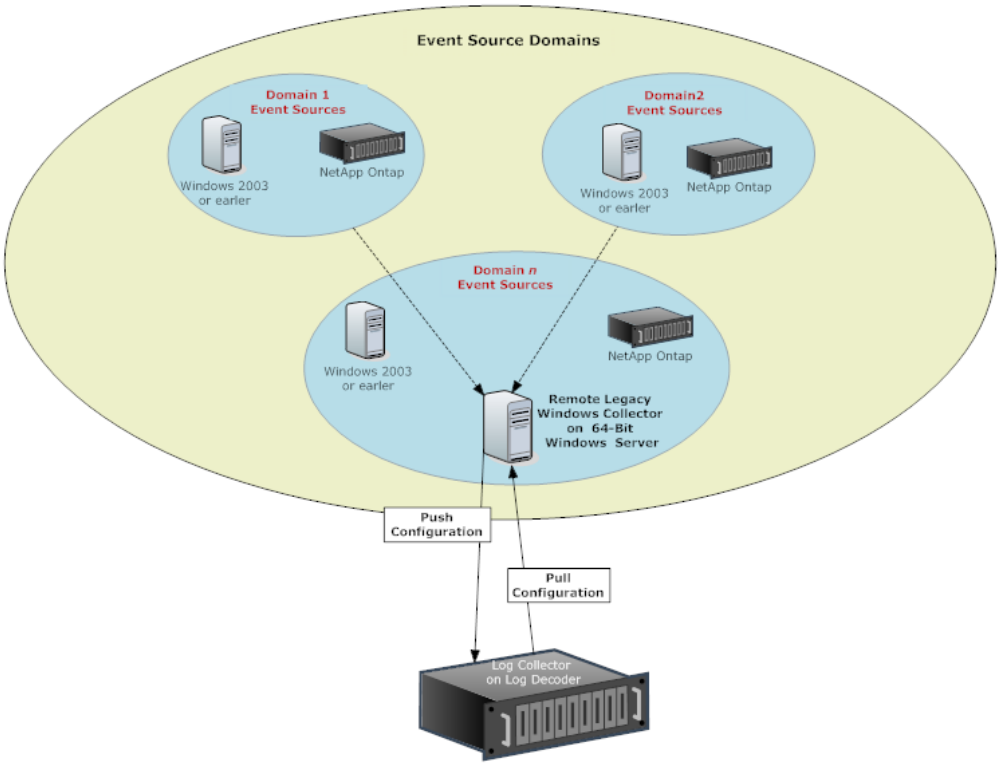
Nota: Para el encadenamiento de Remote Collector, solo puede:
Migrar datos desde un Remote Collector 10.4 o superior a otros Remote Collectors 10.4 o superiores o Local Collectors 10.4 o superiores.
Usar un Remote Collector 10.4 o superior para extraer datos desde uno o más Remote Collectors 10.4 o superiores.



* The Local Collector (LC) is the Log Collector service on the Log Decoder appliance.

Remote Collector de Windows existente

En la siguiente figura se ilustra la implementación requerida para recopilar eventos desde orígenes de eventos de Windows existentes (Windows 2003/2000 y NetApp).



Procedimientos

En este tema se presentan los pasos de alto nivel que necesita completar para implementar y configurar la recopilación de registros

Lista de verificación de implementación

Antes de implementar la recopilación de registros, asegúrese de que el Log Decoder:

- Esté capturando datos. Consulte la *Guía de configuración de Decoder y Log Decoder* para obtener más información que explica la manera en que se capturan los datos.
- Tenga su contenido cargado.
- Tenga la licencia correcta. Consulte la *Guía de licencia* para obtener más información sobre el proceso de licencia.

Descripción de pasos	√
Acceder a Local y Remote Collectors	

Descripción de pasos	√
Configurar Local y Remote Collectors. • Extraer eventos de Remote Collectors. • Migrar eventos a Local Collectors.	
Configurar una cadena de Remote Collectors.	
Regular un Remote Collector al ancho de banda del Local Collector.	

Acceder a Local y Remote Collectors

En este tema se indica cómo acceder a Local Collectors y Remote Collectors para que pueda configurarlos. Puede acceder a un Local Collector o a un Remote Collector mediante la selección del servicio que desea en la vista **Administration > Servicios**. Si no ve un Local Collector o un Remote Collector en la vista Servicios, debe agregarlo.

Después de realizar este procedimiento, habrá:

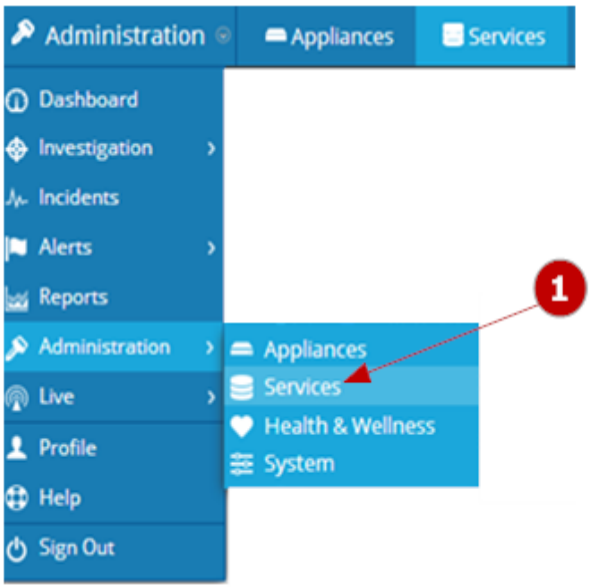
- Agregado un servicio Local Collector/Remote Collector.
- Agregado un servicio remoto de Windows heredado.

Procedimientos

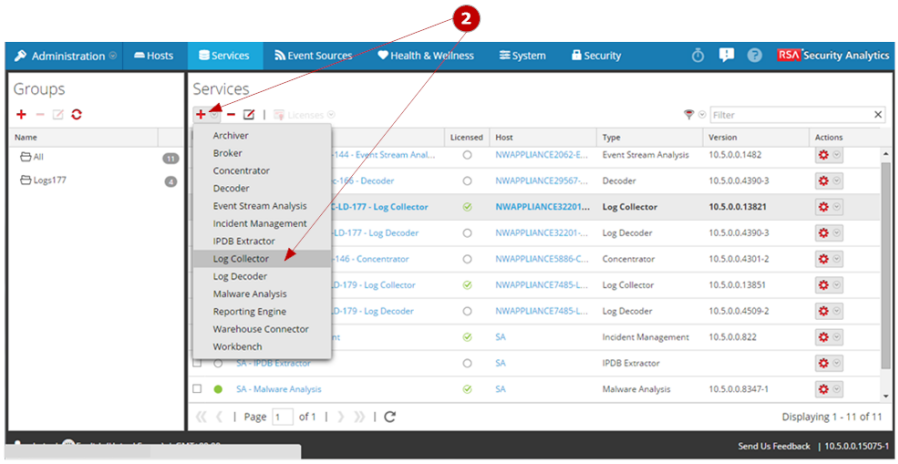
Agregar un Local Collector/Remote Collector

Puede agregar un Local Collector si agrega el servicio Log Collector a un host de Log Decoder en Security Analytics.
Para agregar un Remote Collector, debe agregar el servicio Log Collector a un host en Security Analytics.

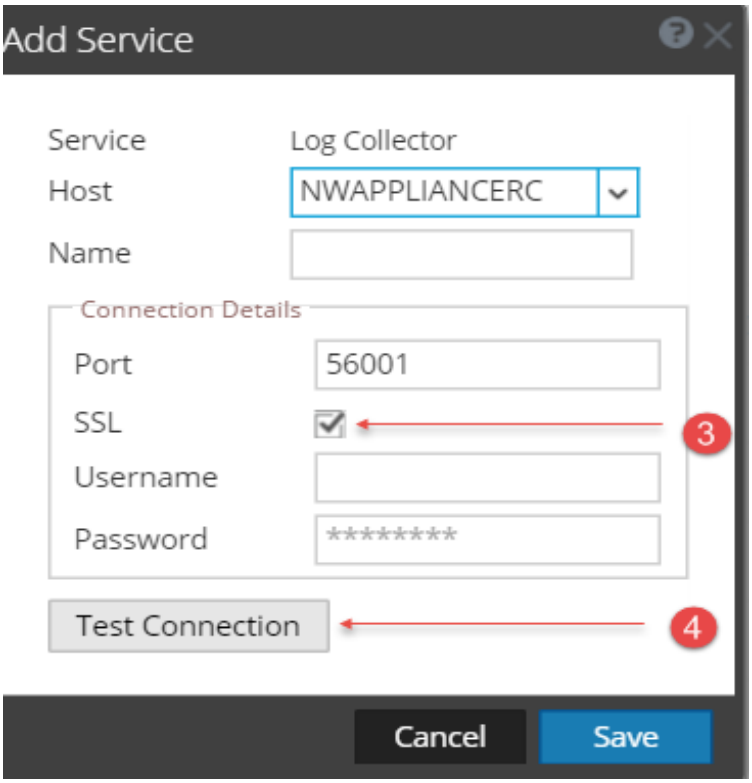
Nota: Los cuadros de diálogo son idénticos para los Local Collectors, los Remote Collectors y los recopiladores de Windows heredado.



1 Acceda a la vista **Servicios**.



2 Haga clic en + para abrir el cuadro de diálogo **Agregar servicio** y seleccione **Log Collector**.



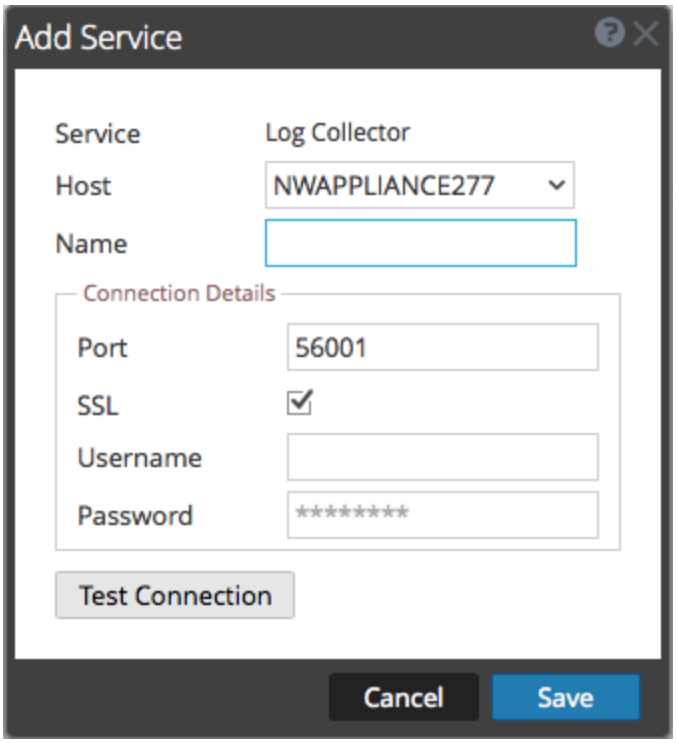
3 Defina los detalles de conexión del servicio Log Collector en un Local Collector.

4 Haga clic en **Probar conexión**. Si la conexión es válida, verá **La conexión se prueba se estableció correctamente**. Si la conexión falla, verá **Falla**. Si falla, asegúrese de que el host de Log Decoder esté en ejecución y que se haya ingresado la información correcta en el cuadro de diálogo **Agregar servicio**, y vuelva a hacer clic en **Guardar**.

Para agregar un Local Collector o un Remote Collector:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione + en la barra de herramientas.

   Se muestra el cuadro de diálogo **Agregar servicio**.



3. En el cuadro de diálogo **Agregar servicio** , proporcione la siguiente información.

Campo	Descripción
Servicio	Seleccione Log Collector como el tipo de servicio.
Nombre	Escriba el nombre que desee asignar al servicio.
Host	Seleccione el host de Log Collector que agregó a la vista Hosts donde reside el servicio Log Collector correspondiente.
Puerto	El puerto predeterminado es 50001 para el texto no cifrado y 56001 para el cifrado con SSL.
SSL	Seleccione SSL si desea que Security Analytics se comunique con el host mediante SSL. La seguridad de la transmisión de datos se administra mediante el cifrado de la información y el suministro de autenticación con certificados SSL.
(Opcional) Nombre de usuario	Escriba el nombre de usuario del Local Collector.

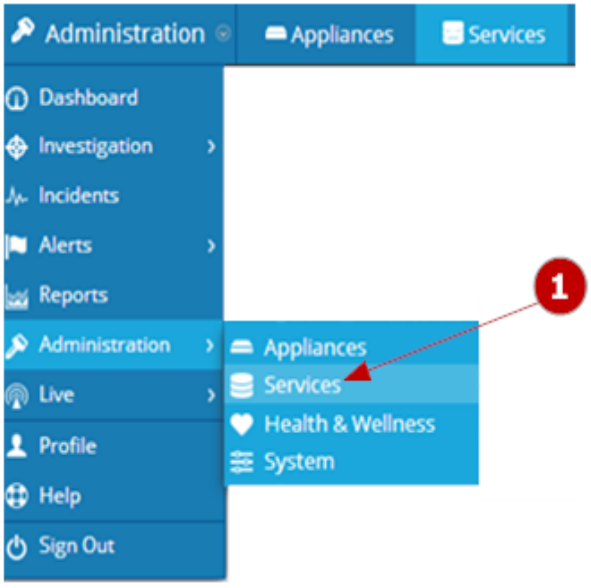
Campo	Descripción
(Opcional) Contraseña	Escriba la contraseña del Local Collector.

4. Haga clic en **Probar conexión** para determinar si Security Analytics se conecta al servicio.
5. Cuando el resultado sea satisfactorio, haga clic en **Guardar**.
   si el resultado de la prueba no es satisfactorio, edite la información del servicio y vuelva a intentarlo.

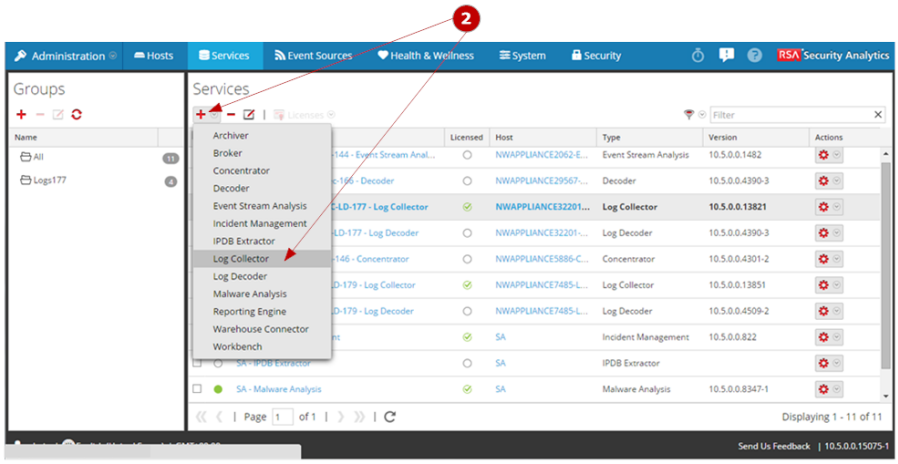
Agregar un Remote Collector de Windows heredado

Para agregar un Remote Collector, debe agregar el servicio Log Collector a un host remoto.

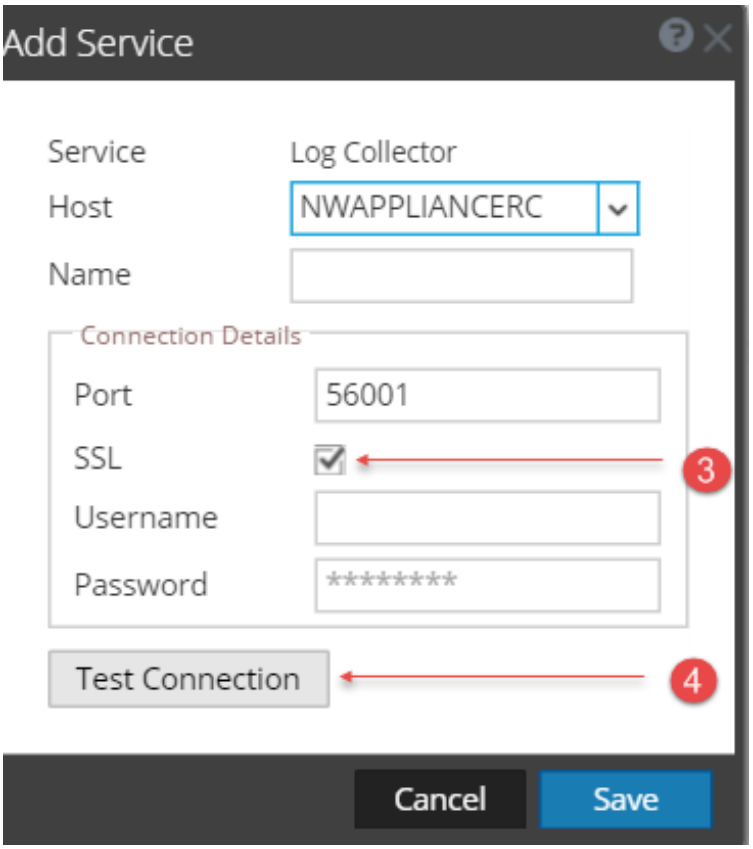
Nota: Antes de agregar un Remote Collector de Windows heredado, debe instalar el recopilador de Windows heredado de Security Analytics en un servidor Windows 2008 SP1 de 64 bits físico o virtual mediante **SALegacyWindowsCollector-*version-number.exe***. El archivo **SALegacyWindowsCollector-*version-number.exe*** se descarga desde Download Central (consulte las Instrucciones de actualización e instalación de Windows heredado para SA-v10.6).



1 Acceda a la vista **Servicios**.



2 Haga clic en + para abrir el cuadro de diálogo **Agregar servicio** y seleccione **Log Collector**.



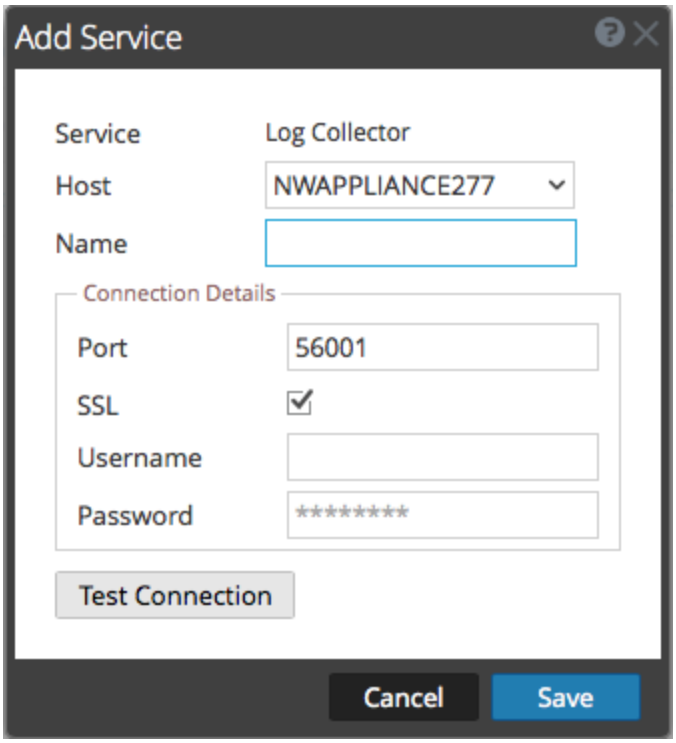
3 Defina los detalles del servicio de recopilación de registros en un Remote Collector.

4 Haga clic en **Probar conexión**. Si la conexión es válida, verá **La conexión se prueba se estableció correctamente**. Si la conexión falla, verá **Falla**. En este caso, asegúrese de que el host de Log Decoder esté en ejecución y que se haya ingresado la información correcta en el cuadro de diálogo **Agregar servicio** y vuelva a hacer clic en **Guardar**.

Para agregar un Remote Collector:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione + en la barra de herramientas.

   Se muestra el cuadro de diálogo **Agregar servicio**.



3. En el cuadro de diálogo **Agregar servicio** , proporcione la siguiente información.

Campo	Descripción
Servicio	Seleccione Log Collector como el tipo de servicio.
Nombre	Escriba el nombre del servicio.
Host	Seleccione un host remoto.

Campo	Descripción
Puerto	El puerto predeterminado es 50001 para el texto no cifrado y 56001 para el cifrado con SSL.
SSL	Seleccione **SSL** si desea que Security Analytics se comunique con el host mediante SSL. La seguridad de la transmisión de datos se administra mediante el cifrado de la información y el suministro de autenticación con certificados SSL.
(Opcional) Nombre de usuario	Escriba el nombre de usuario del Remote Collector.
(Opcional) Contraseña	Escriba la contraseña del Remote Collector.

4. Haga clic en **Probar conexión** para determinar si Security Analytics se conecta al servicio.
5. Cuando el resultado sea satisfactorio, haga clic en **Guardar**.
   si el resultado de la prueba no es satisfactorio, edite la información del servicio y vuelva a intentarlo.

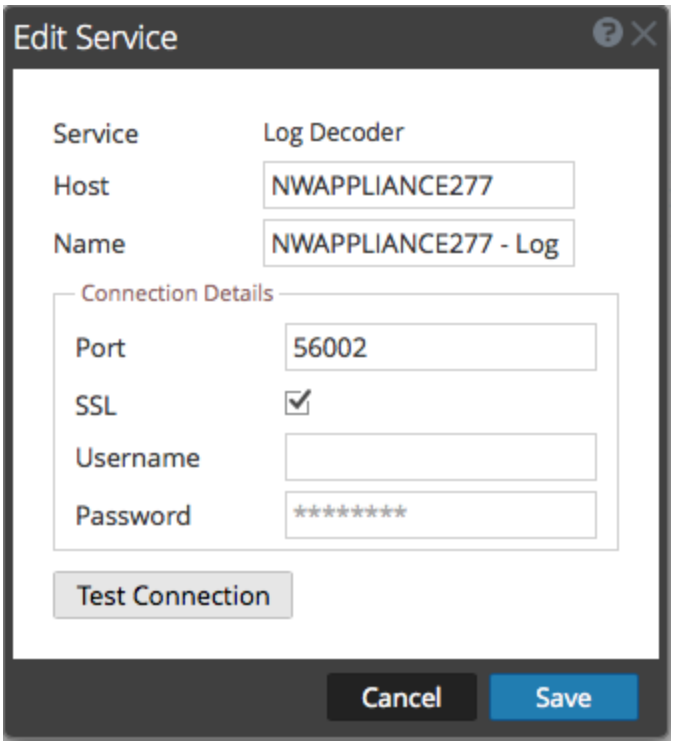
Aprovisionamiento de Local y Remote Collectors

El servidor de Security Analytics verifica si un dispositivo tiene un servicio Log Decoder. Si hay un servicio Log Decoder, se convierte en un Local Collector. Si falta un servicio Log Decoder, se convierte en un Remote Collector. Un Log Collector local tiene un destino de evento y, de manera predeterminada, se dirige al servicio Log Decoder local. Un Remote Collector no tiene un destino de evento. El servidor de Security Analytics identifica un recopilador de Windows heredado como un Remote Collector.

Nota: La casilla de verificación Remote Collector se quitó del cuadro de diálogo Editar servicio. Security Analytics determina dinámicamente si se trata de un Local o un Remote Collector.

Para editar un Local o un Remote Collector:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione en la barra de herramientas.
   Se muestra el cuadro de diálogo **Editar servicio**.



3. En el cuadro de diálogo **Editar servicio** , proporcione la siguiente información.

Campo	Descripción
Servicio	Seleccione Log Collector como el tipo de servicio.
Host	Seleccione un host de Log Decoder.
Nombre	Escriba el nombre que desee asignar al servicio.
Puerto	El puerto predeterminado es 50001 para el texto no cifrado y 56001 para el cifrado con SSL.
SSL	Seleccione **SSL** si desea que Security Analytics se comunique con el host mediante SSL. La seguridad de la transmisión de datos se administra mediante el cifrado de la información y el suministro de autenticación con certificados SSL.
(Opcional) Nombre de usuario	Escriba el nombre de usuario del Local Collector.

Campo	Descripción
(Opcional) Contraseña	Escriba la contraseña del Local Collector.

4. Haga clic en **Probar conexión** para determinar si Security Analytics se conecta al servicio.
5. Cuando el resultado sea satisfactorio, haga clic en **Guardar**.
   si el resultado de la prueba no es satisfactorio, edite la información del servicio y vuelva a intentarlo.

Configurar Local y Remote Collectors

En este tema se indica cómo configurar Local y Remote Collectors.

Cuando implementa Log Collection, debe configurar los Log Collectors para recopilar los eventos de registro de diversos orígenes de eventos y entregarlos de manera fiable y segura al host de Log Decoder, donde se analizan y se almacenan para su posterior análisis.

Puede configurar uno o más Remote Collectors para migrar datos de eventos a un Local Collector, o puede configurar un Local Collector para extraer datos de eventos de uno o más Remote Collectors.

Volver a Procedimientos

Este tema le indica cómo:

- Configurar Local Collector para extraer eventos de Remote Collector
  Si desea que un Local Collector extraiga eventos de un Remote Collector, realice esta configuración en la pestaña Remote Collectors de la vista Configuración del Local Collector.
- Configurar un Remote Collector para migrar eventos a Local Collectors
  Si desea que un Remote Collector migre eventos a un Local Collector, realice esta configuración en la pestaña Local Collector de la vista Configuración del Remote Collector.
  En Migrar configuración, también puede:
  - Configurar un Local Collector de conmutación por error para un Remote Collector
    Puede configurar un destino compuesto por Local Collectors. Cuando el Local Collector primario está inaccesible, el Remote Collector intenta conectarse a cada Local Collector en este destino hasta que establece una conexión correcta.
  - Configurar la replicación
    Debe configurar varios grupos de destino para que Security Analytics replique los datos de

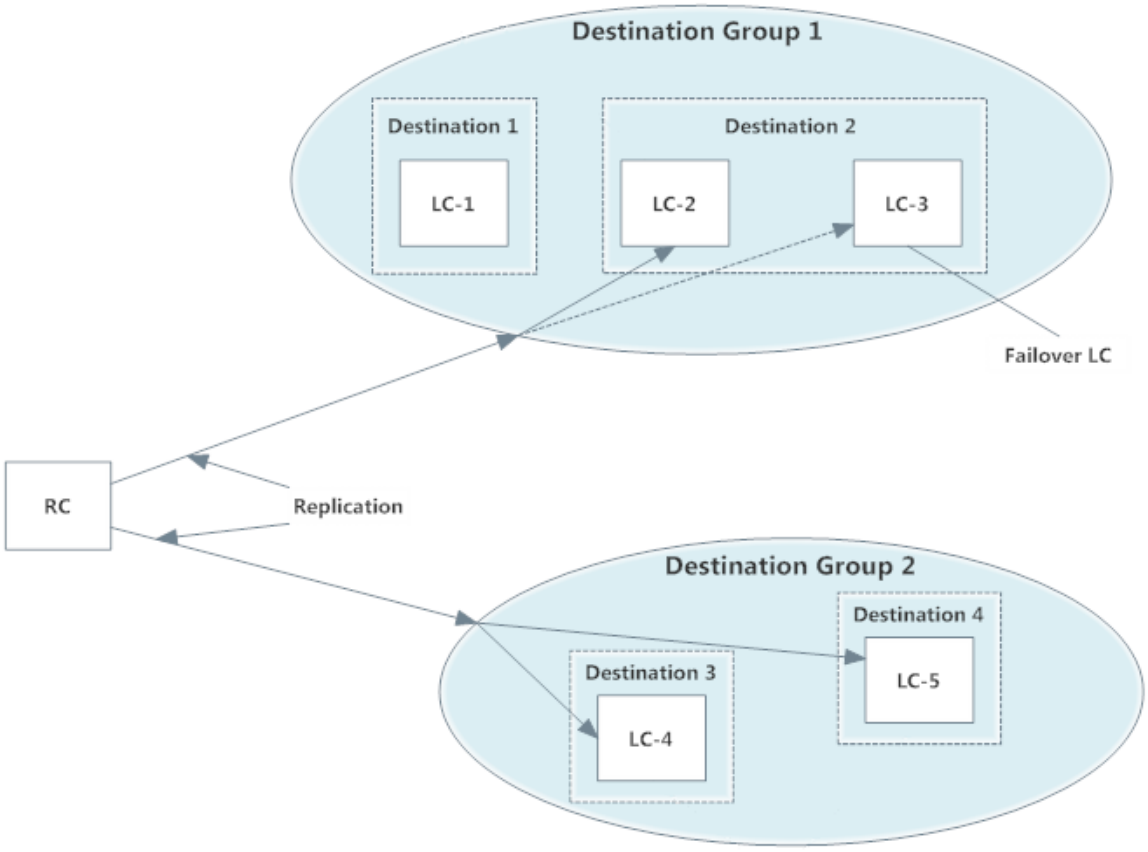
eventos en cada grupo. Si falla la conexión con uno de los grupos de destino, puede recuperar los datos requeridos, ya que se replica en el otro grupo de destino.

- Configurar el enrutamiento de registros para protocolos específicos
  Puede configurar varios destinos de un grupo de destino para dirigir datos de eventos a ubicaciones específicas según el tipo de protocolo.

- Configurar una cadena de Remote Collectors
  Puede configurar una cadena de Remote Collectors para migrar datos de eventos a un Local Collector o puede configurar un Local Collector para extraer datos de eventos desde una cadena de Remote Collectors.
  - Uno o más Remote Collectors para migrar datos de eventos a un Remote Collector.
  - Un Remote Collector para extraer datos de eventos de uno o más Remote Collectors.

Conmutación por error y replicación

En la siguiente figura se ilustra un Remote Collector configurado para conmutación por error y replicación.



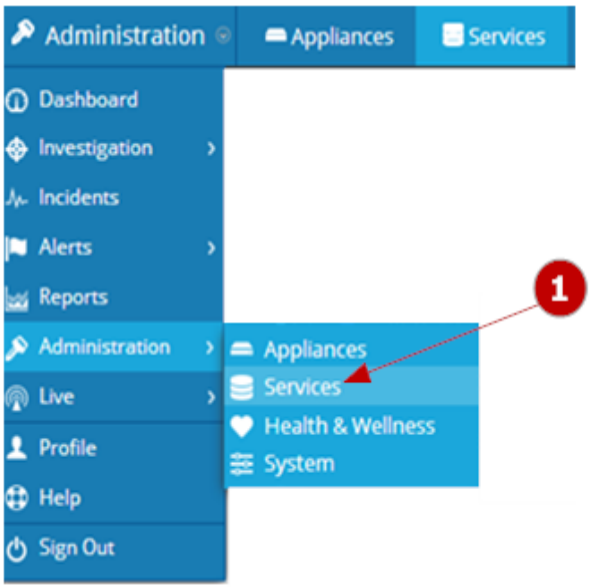
En el grupo de destino 1, LC-2 y LC-3 son los Local Collectors de failover configurados para LC-1. Si por algún motivo el Remote Collector no puede conectarse a LC1, este intenta conectarse a LC-2 o LC-3 hasta que establece una conexión correcta.

El grupo de destino 1 y el grupo de destino 2 están configurados para replicación. Si falla el Local Collector en el grupo de destino 1, puede usar los datos replicados en el Local Collector del grupo de destino 2.

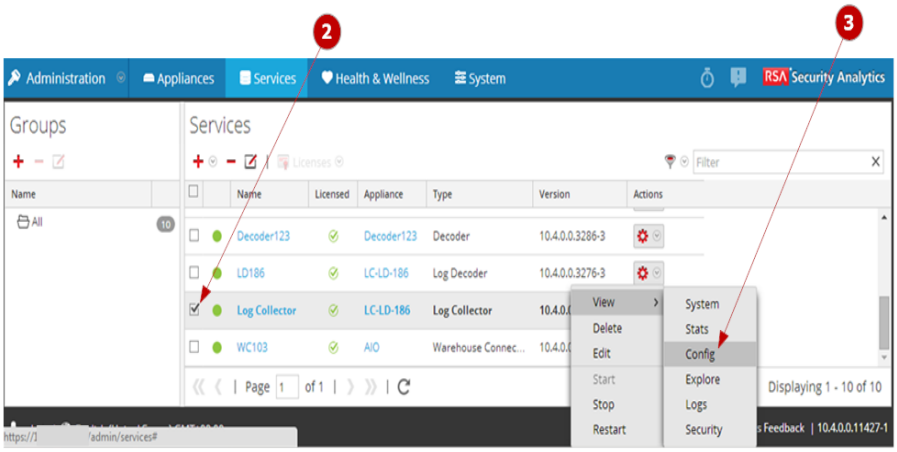
Nota: También puede configurar el enrutamiento de registros para que los datos de eventos de protocolos específicos se envíen a destinos específicos.

Procedimiento

Debe elegir el Log Collector, es decir un Local Collector (LC) o un Remote Collector (RC), para el cual desea definir parámetros de implementación en la vista Servicios. En el siguiente procedimiento se muestra cómo navegar a la vista Servicios, seleccionar un Local Collector o un Remote Collector y mostrar la interfaz de parámetros de implementación de ese servicio.

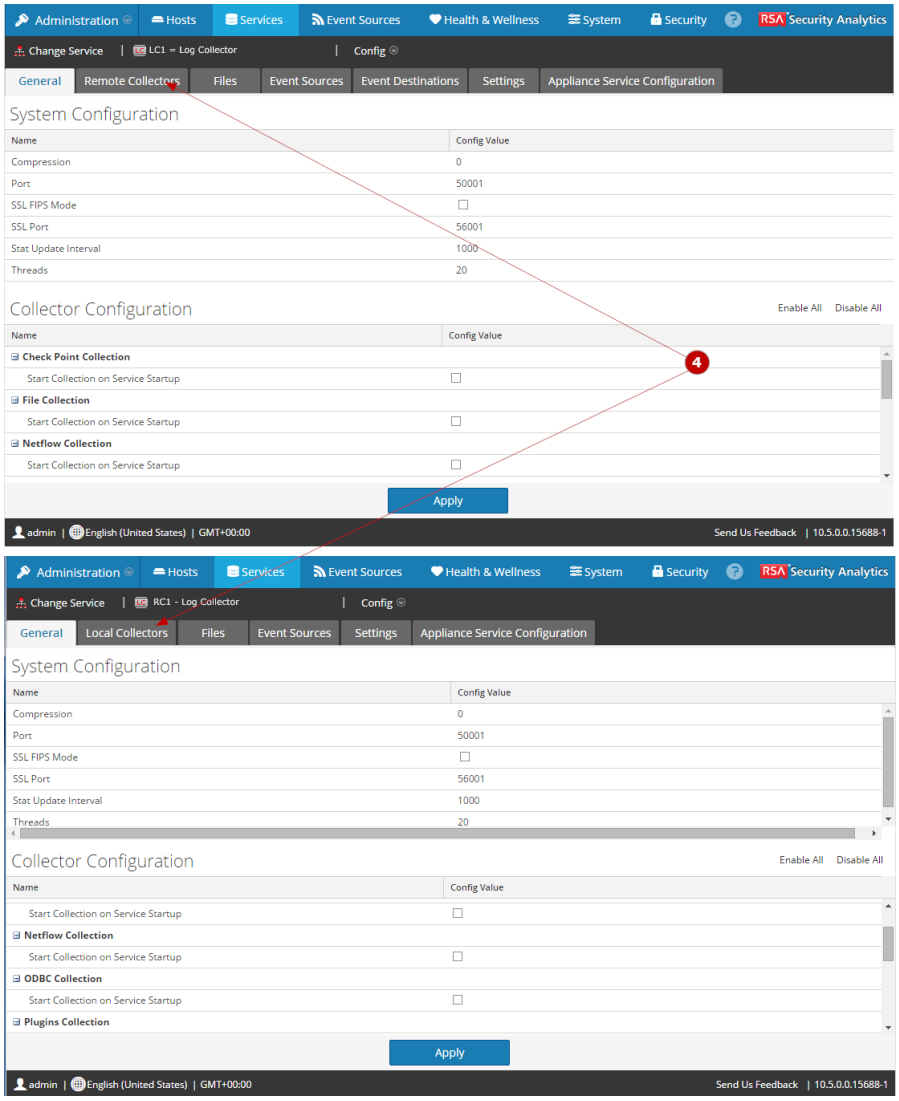


1 Acceda a la vista **Servicios**.



2 Seleccione un servicio Log Collector.

3 Haga clic en ⌄ bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



4 En el paso 2, si seleccionó un servicio Log Collector para un:

- Local Collector, se muestra la pestaña **Remote Collectors**. En esta pestaña, seleccione los Remote Collectors desde los cuales el Local Collector extrae eventos.
- Remote Collector, se muestra la pestaña **Local Collectors**. En esta pestaña, seleccione los Local Collectors a los cuales el Remote Collector migra eventos.

Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Extraer eventos de un Remote Collector

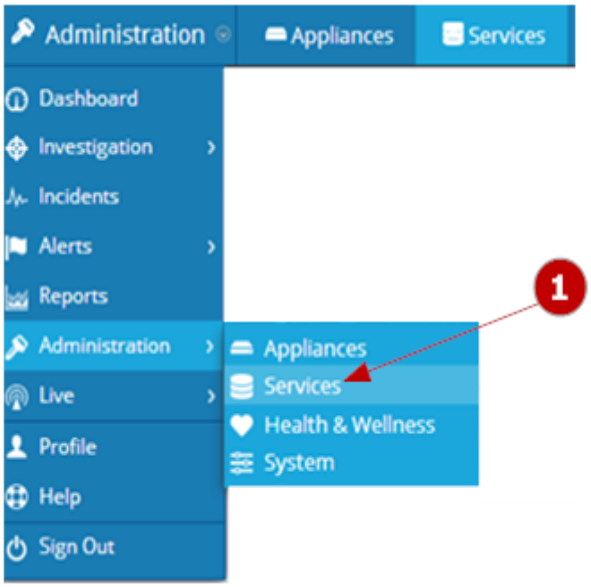
En este tema se indica cómo configurar un Local Collector para extraer eventos de un Remote Collector.

Después de realizar este procedimiento, habrá configurado un Local Collector para extraer eventos de un Remote Collector.

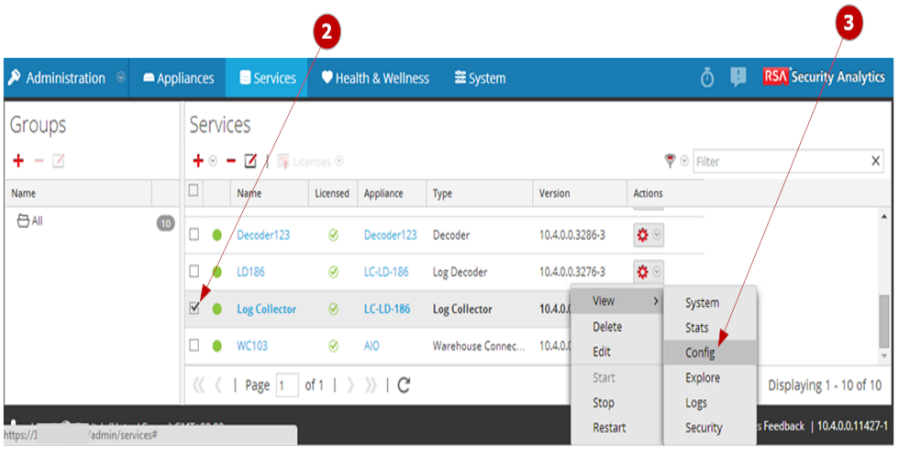
Configurar Local Collector para extraer eventos de Remote Collector

Puede configurar un Local Collector para extraer datos de eventos de uno o más Remote Collectors.

En la siguiente figura se muestra cómo configurar un Local Collector para extraer eventos de un Remote Collector.

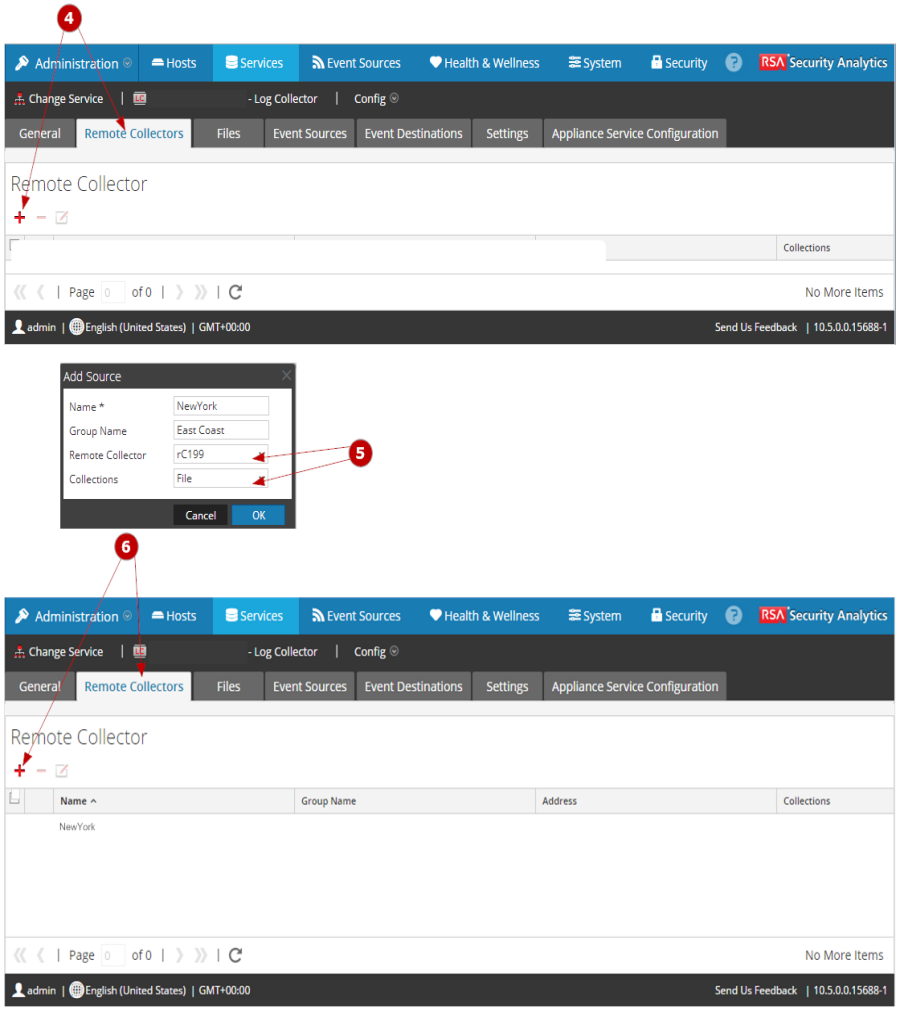


1 Acceda a la vista **Servicios**.



2 Seleccione un servicio Log Collector.

3 Haga clic en ⚙ bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



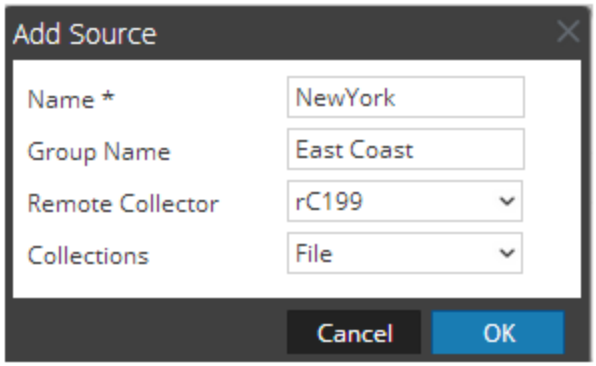
4 Seleccione la pestaña **Remote Collectors** y haga clic en + para mostrar el cuadro de diálogo **Agregar origen**.

5 Especifique un Remote Collector desde donde el Local Collector extrae eventos. Especifique los protocolos de recopilación que se usarán en la migración.

6 El Remote Collector que acaba de agregar se muestra en la pestaña **Remote Collector**.

Configurar el Local Collector seleccionado para extraer eventos de un Remote Collector especificado

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un **Log Collector**.
3. Haga clic en bajo Acciones y seleccione Ver > Configuración.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Haga clic en la pestaña **Configuración**.
5. Seleccione la pestaña **Remote Collectors**.
6. Haga clic en .
   Se muestra el cuadro de diálogo **Agregar origen**.
7. En el cuadro de diálogo **Agregar origen**:
   a. Seleccione un Remote Collector en la lista desplegable.
   b. Seleccione uno o más protocolos de recopilación.

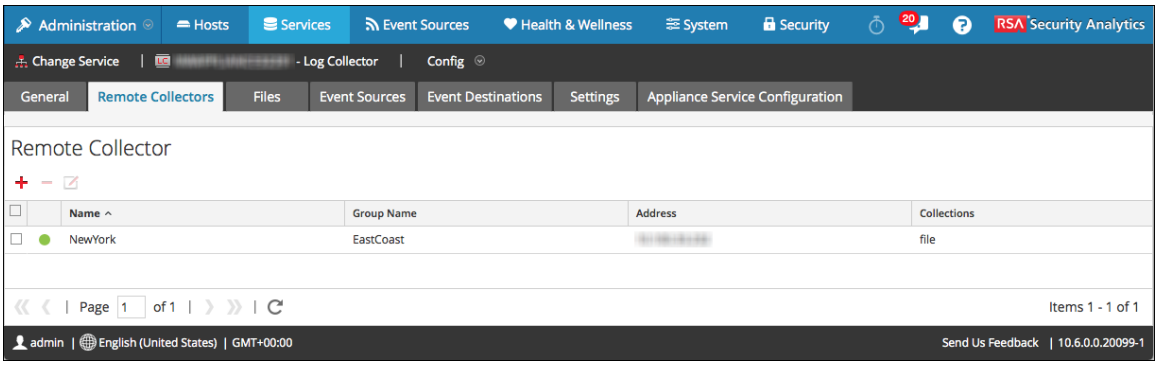


> **Nota:** Si no selecciona un protocolo de recopilación, el Local Collector extrae todos los protocolos de recopilación desde el Remote Collector.

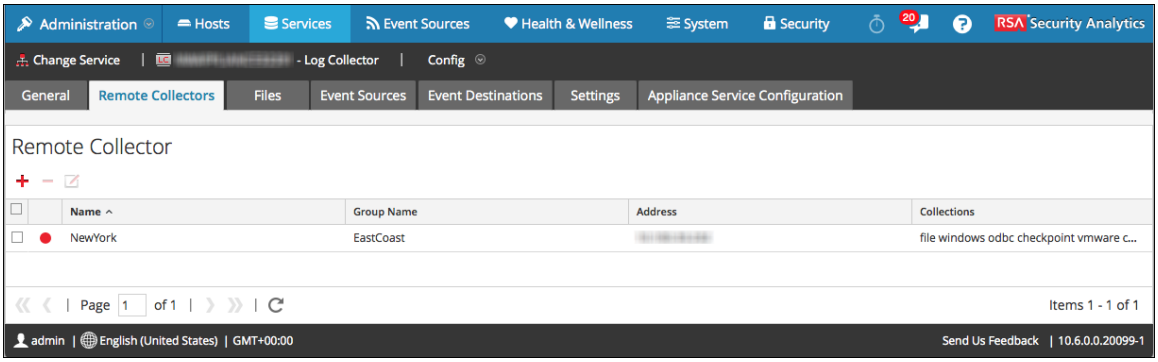
   c. Haga clic en **Aceptar**.

El Remote Collector se agrega a la sección Remote Collector. Cuando el Log Collector comienza a recopilar datos, extrae datos de eventos de este Remote Collector.

La siguiente pestaña muestra **Archivo** como el único protocolo seleccionado.



La siguiente pestaña muestra todos los protocolos seleccionados. Security Analytics selecciona todos los protocolos si deja el campo Recopilaciones en blanco.



Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Migrar eventos a Local Collectors

En este tema se indica cómo configurar un Remote Collector para migrar eventos a un Local Collector.

Después de realizar este procedimiento, habrá configurado un Remote Collector para migrar eventos a Local Collectors.

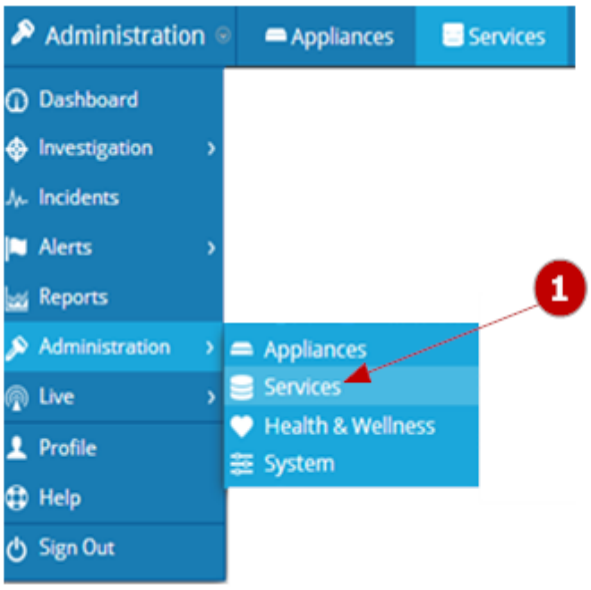
Volver a Procedimientos

Procedimientos

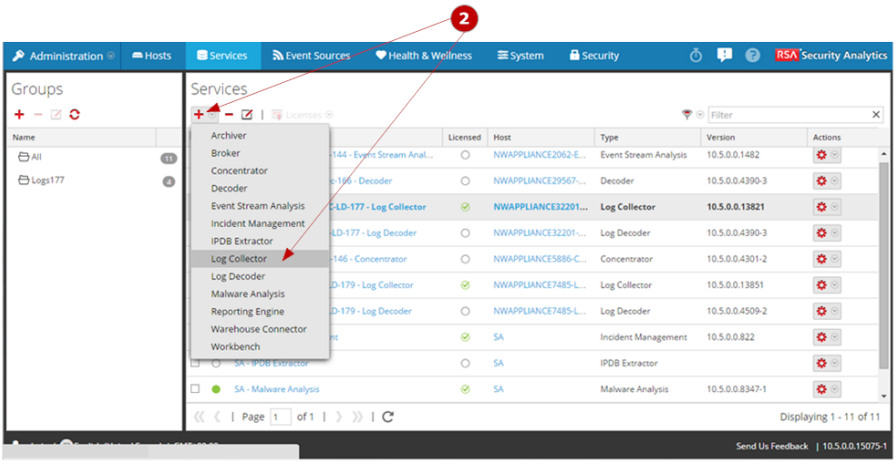
Configurar Remote Collector para migrar eventos a Log Collectors

Puede configurar un Remote Collector para migrar datos de eventos a uno o más Local Collectors.

En la siguiente figura se muestra cómo configurar un Remote Collector para migrar eventos a un Local Collector.

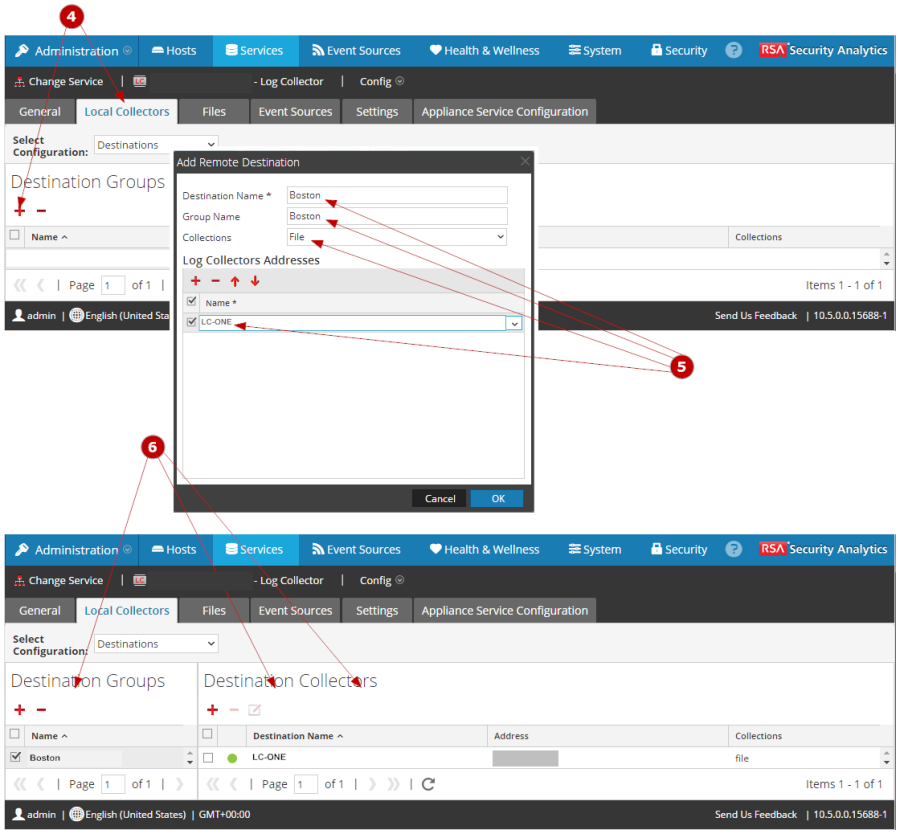


1 Acceda a la vista **Servicios**.



2 Seleccione un Remote Collector.

3 Haga clic en bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



4 Seleccione la pestaña **Local Collectors**, seleccione **Destinos** en el menú desplegable **Seleccionar configuración** y haga clic en + en **Grupos de destino** para mostrar el cuadro de diálogo **Agregar destinos remotos**.

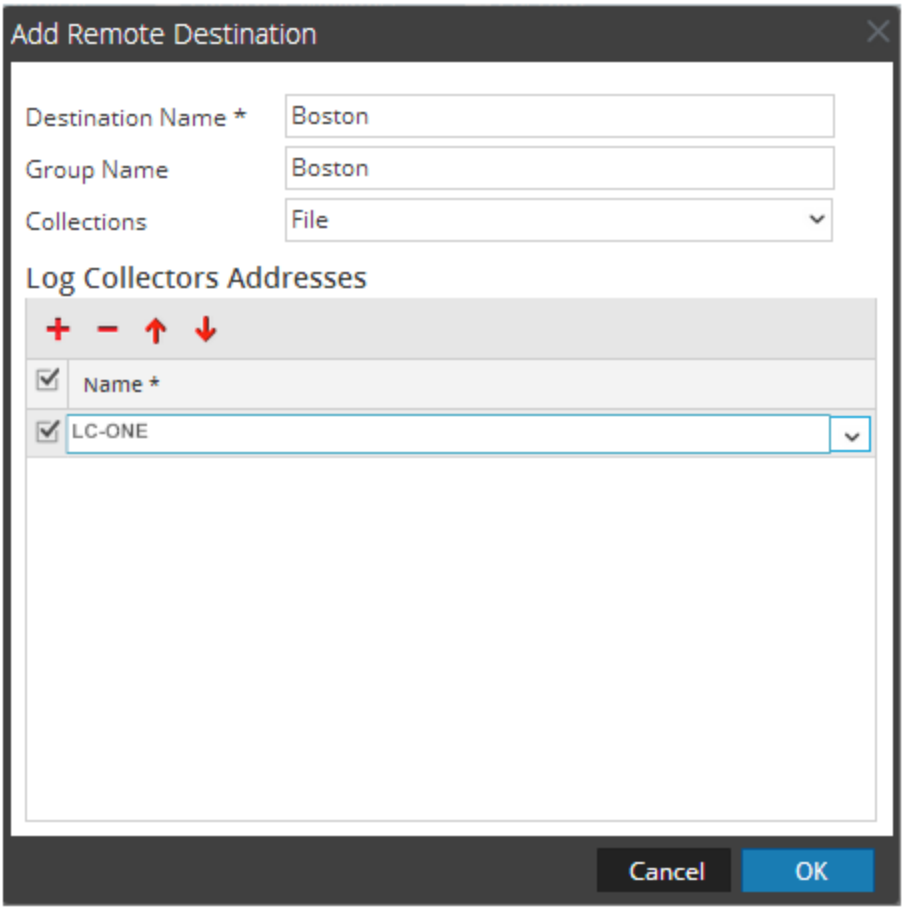
5 Especifique un Local Collector al cual el Remote Collector migra eventos. Especifique los protocolos de recopilación que se usarán en la migración.

6 El Local Collector que acaba de agregar se muestra en la pestaña **Local Collector**.

Configurar el Remote Collector seleccionado para migrar eventos a Log Collectors especificados

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un **Remote Collector**.
3. Haga clic en ⚙ bajo Acciones y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.

5. En la sección del panel Grupos de destino, haga clic en +.
   Se muestra el cuadro de diálogo **Agregar destino remoto**.
6. Configure un grupo de destino:
   a. Ingrese un **Nombre de destino**.
   b. (Opcional) Ingrese un Nombre del grupo. Si deja Nombre del grupo en blanco, Security Analytics lo establece en el valor que especificó en Nombre del destino.
   c. Seleccione uno o más protocolos de recopilación en la lista desplegable **Recopilaciones**.
   d. En **Direcciones de Log Collector**, haga clic en + para seleccionar un Local Collector.



Nota: Si no selecciona un protocolo de recopilación, el Remote Collector migra todos los protocolos de recopilación a los Local Collectors.

Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Configurar el Local Collector de failover

En este tema se indica cómo configurar un Local Collector de failover para un Remote Collector.

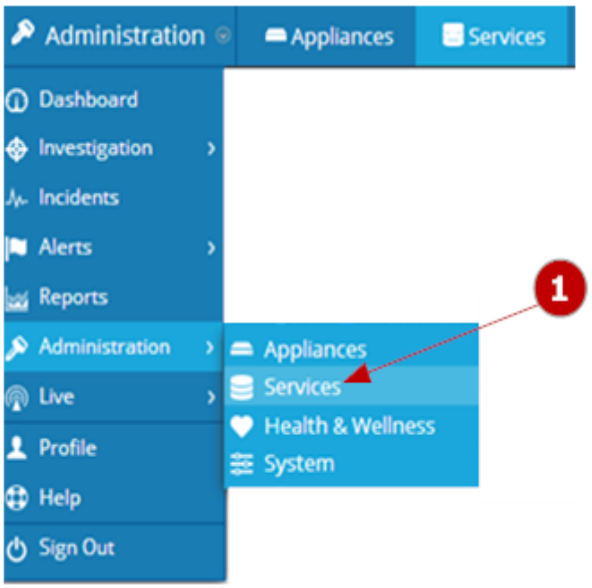
Después de completar este procedimiento, habrá configurado un destino compuesto por Local Collectors de tal manera que cuando el Local Collector primario esté inaccesible, el Remote Collector intente conectarse a cada Local Collector en este destino hasta que establezca una conexión correcta.

Volver a Procedimientos

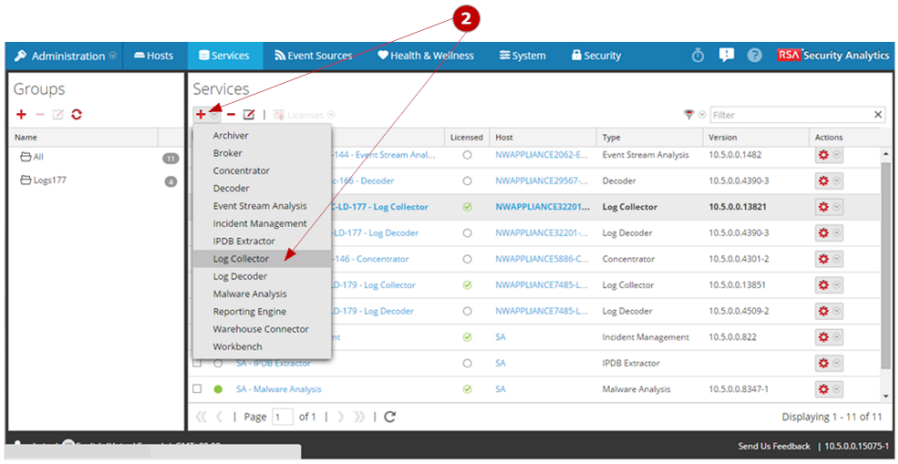
Configurar un Local Collector de conmutación por error

Puede configurar un Local Collector de conmutación por error al cual Security Analytics conmutará por error si el Local Collector primario deja de funcionar por algún motivo.

En la siguiente figura se muestra cómo configurar un Local Collector de conmutación por error.

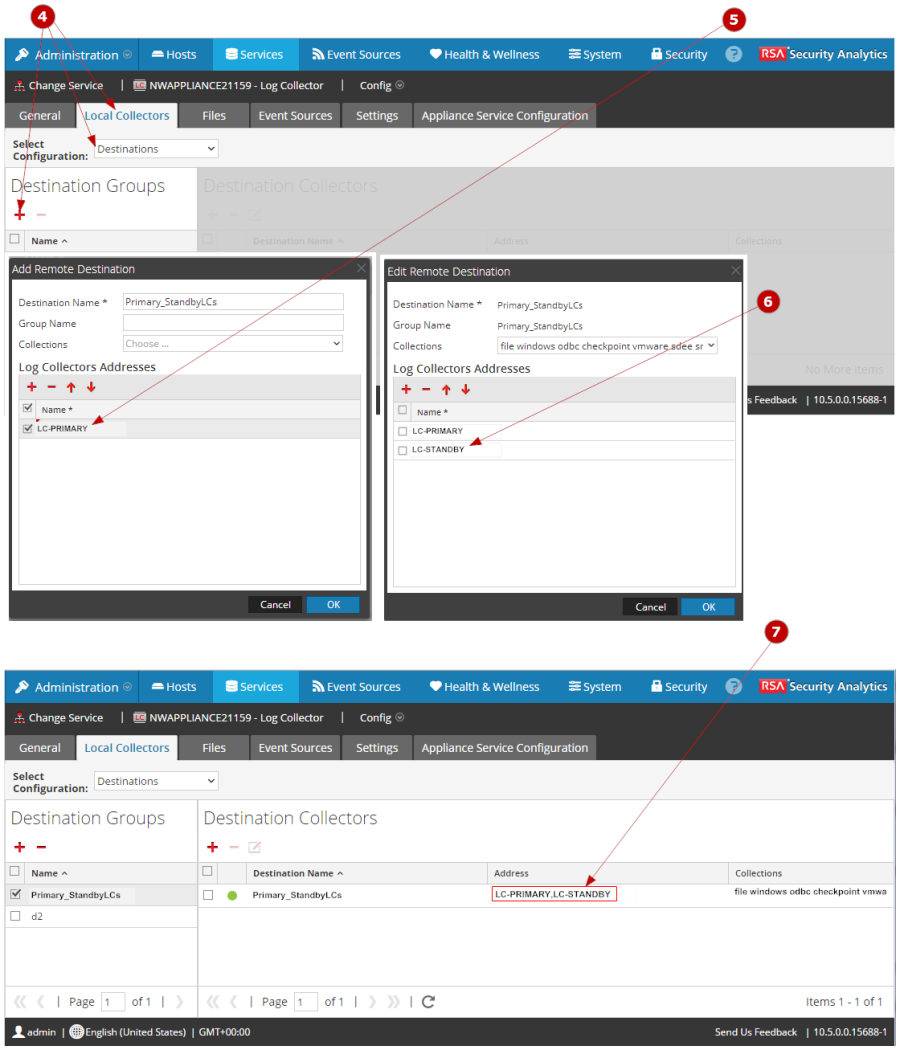


1 Acceda a la vista **Servicios**.



2 Seleccione un Remote Collector.

3 Haga clic en bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



4 Seleccione la pestaña **Local Collectors**, seleccione **Destinos** en el menú desplegable **Seleccionar configuración** y haga clic en + en **Grupos de destino** para mostrar el cuadro de diálogo **Agregar destinos remotos**.

5 Agregue un Local Collector primario.

6 Edite el destino remoto y agregue un Local Collector en espera.

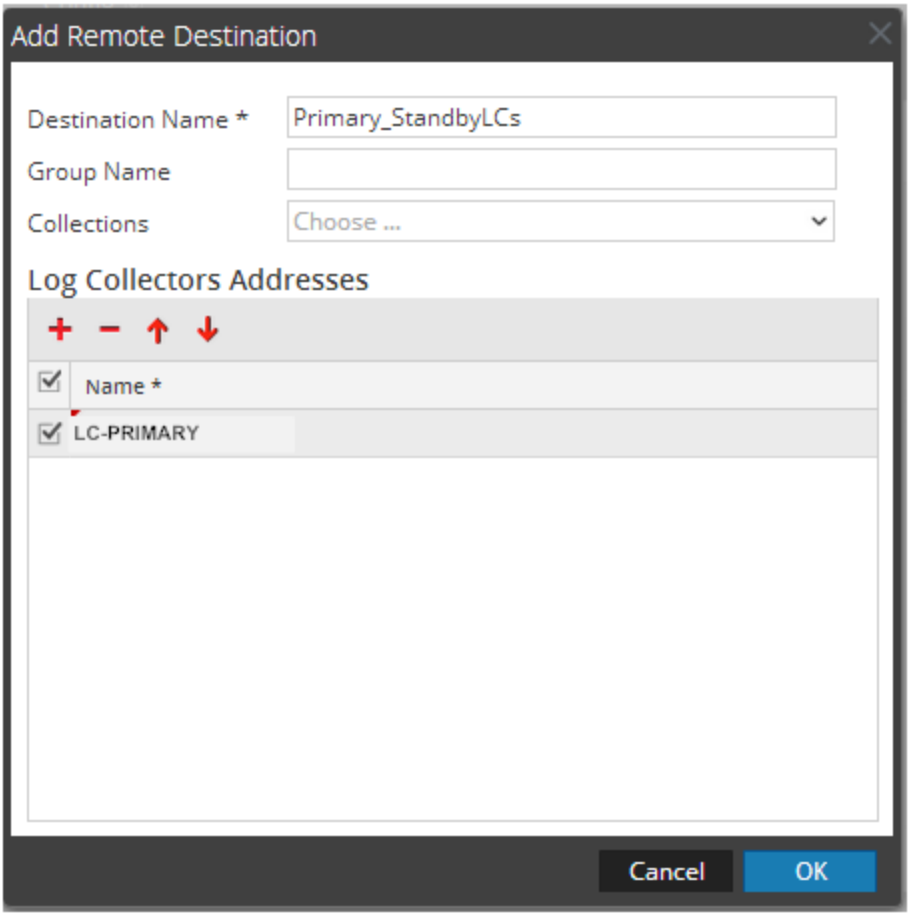
7 Los Local Collectors primario y en espera que acaba de agregar se muestran en la pestaña **Local Collector**.

Configurar un Local Collector de conmutación por error

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un Remote Collector.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.

   La vista Configuración del servicio se muestra con la pestaña General de Log Collector abierta.
4. Seleccione la pestaña **Local Collectors**.
5. En la sección del **panel Grupos de destino**, seleccione  .

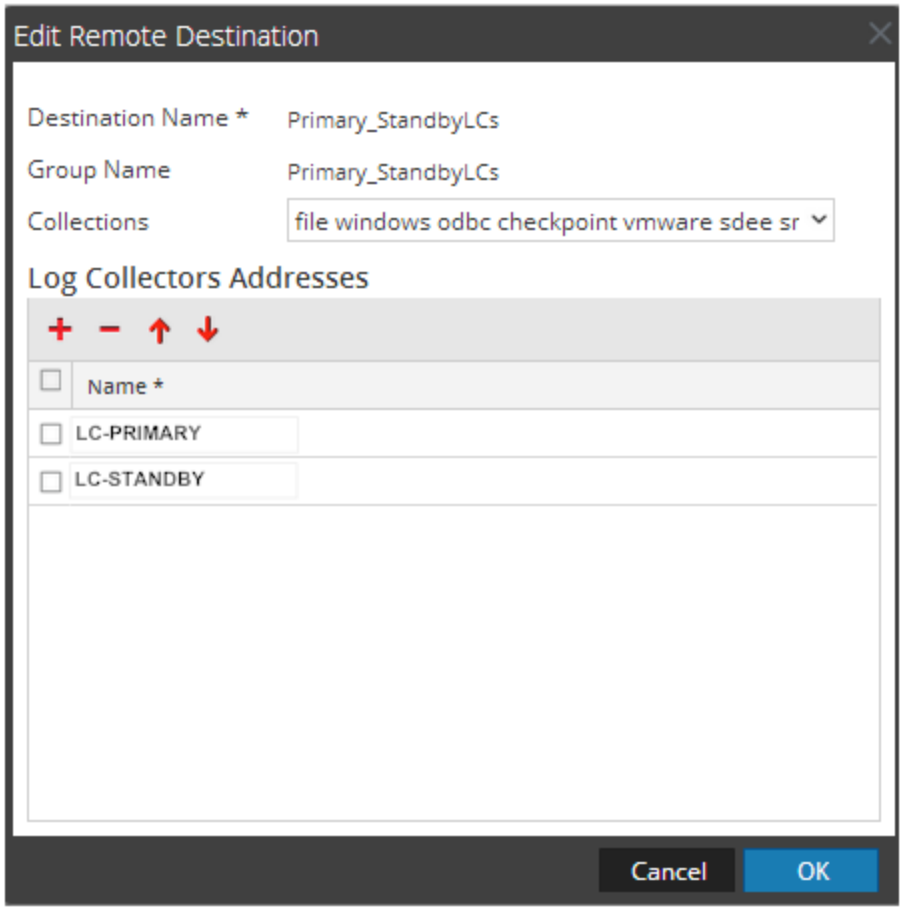
   Se muestra el cuadro de diálogo Agregar destino remoto.
6. Configure un grupo de destino y seleccione un Local Collector primario (por ejemplo, **LC-PRIMARY**).



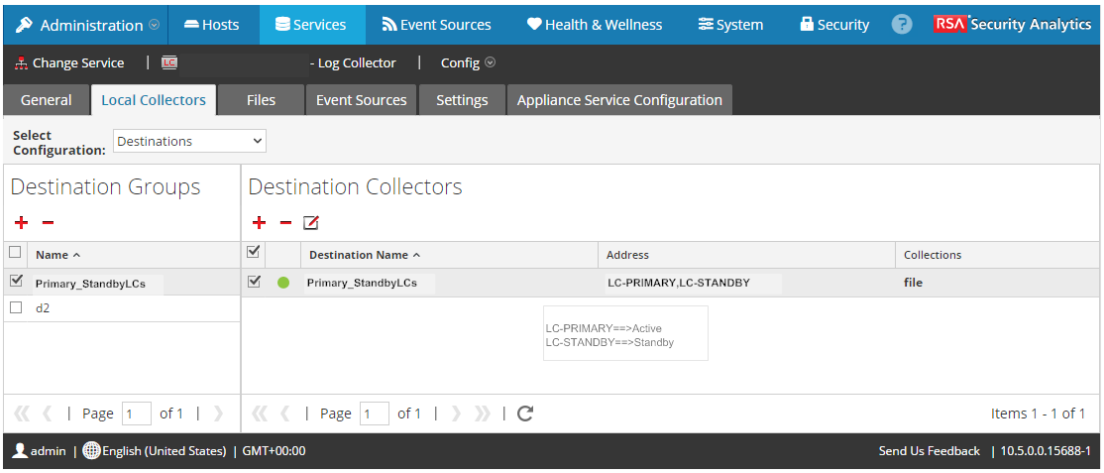
7. Seleccione el grupo (por ejemplo, **Primary_Standby_LCs**) en el panel Grupos de destino y haga clic en  .

El grupo que seleccionó se muestra en el panel Local Collectors.

8. Agregue el Local Collector de conmutación por error (por ejemplo, **LC-STANDBY**).



En los siguientes ejemplos se muestran los Local Collectors primario y de conmutación por error que acaba de agregar. El primario se muestra como **Activo** y el Local Collector de conmutación por error, como **En standby**. Se resalta el Local Collector activo (por ejemplo, **LC-PRIMARY**).



9. (Opcional) Agregue, elimine y cambie el orden de los Local Collectors en cada destino remoto.

   a. Haga clic en + para agregar un Log Collector como destino remoto de failover.

   b. Cuando se conecte a un destino remoto, el Remote Collector intentará conectarse a cada Local Collector de esta lista en orden, hasta que establezca una conexión correcta.

   c. Seleccione un Local Collector y use ↑ ↓ (botones de flecha hacia arriba y abajo) para cambiar el orden de conexión.

   d. Seleccione uno o más Local Collectors y haga clic en − para quitarlos de la lista.

   Los Local Collectors seleccionados se agregan a la sección Log Collector. Cuando un Remote Collector comienza a recopilar datos, migra datos a estos Log Collectors.

Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Configurar el Remote Collector de failover

En este tema se indica cómo configurar un Remote Collector de failover para un Remote Collector.

Después de completar este procedimiento, habrá configurado un destino compuesto por Remote Collectors de tal manera que cuando el Remote Collector primario esté inaccesible, el Remote Collector intente conectarse a cada Remote Collector en este destino hasta que establezca una conexión correcta.

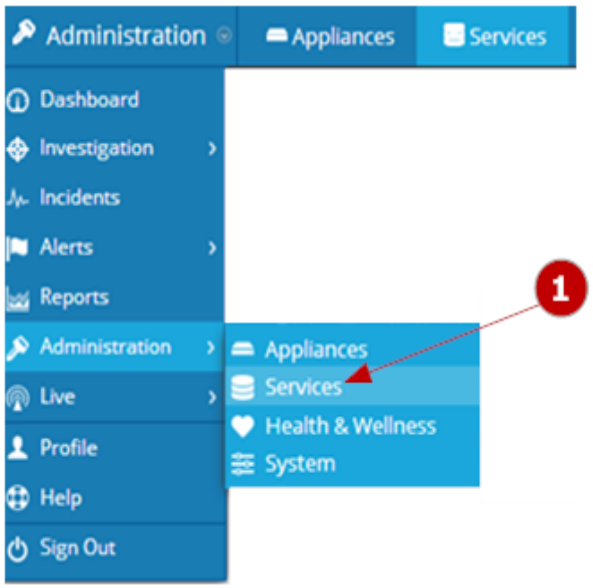
Volver a Procedimientos

Procedimientos

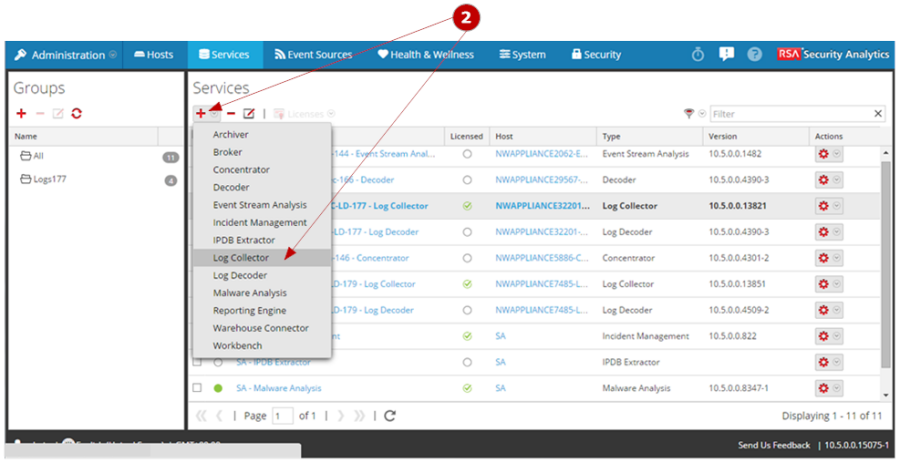
Configurar un Remote Collector de conmutación por error

Puede configurar un Remote Collector de conmutación por error al cual Security Analytics conmutará por error si el Remote Collector primario deja de funcionar por algún motivo.

En la siguiente figura se muestra cómo configurar un Remote Collector de conmutación por error.

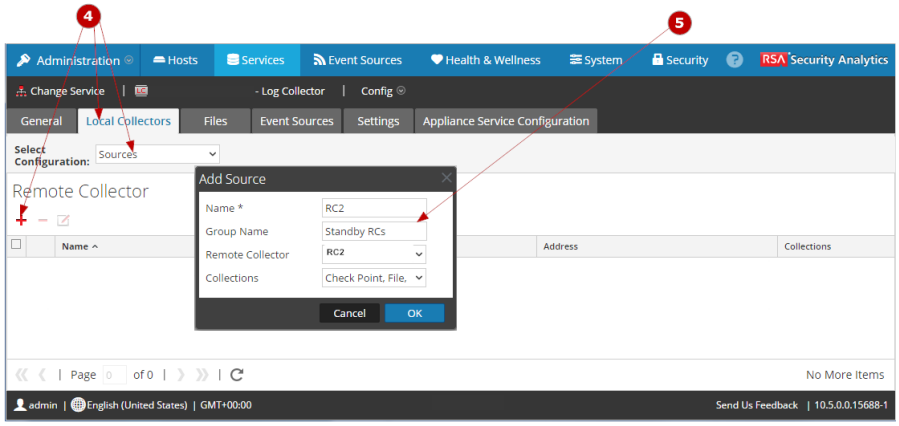


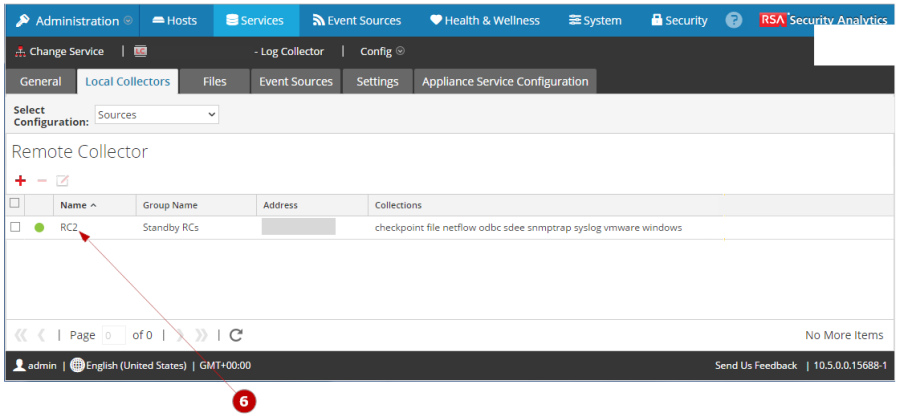
1 Acceda a la vista **Servicios**.



2 Seleccione un Remote Collector.

3 Haga clic en bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.





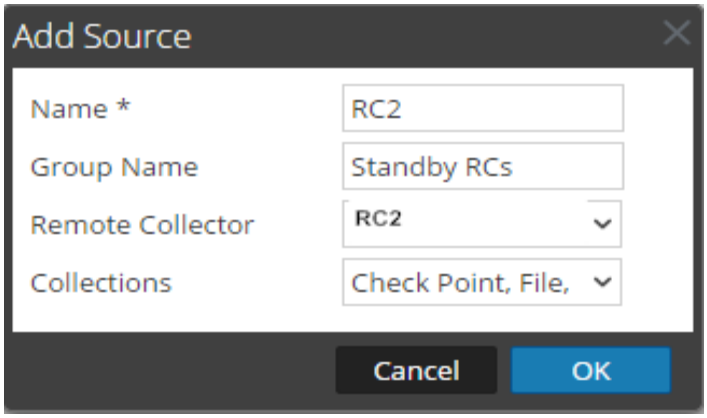
4 Seleccione la pestaña **Local Collectors**, elija **Orígenes** en el menú desplegable **Seleccionar configuración** y haga clic en + para mostrar el cuadro de diálogo **Agregar origen**.

5 Agregue un Remote Collector en espera.

6 El Remote Collector en espera que acaba de agregar se muestra en la pestaña **Local Collector**.

Configure un Remote Collector de conmutación por error:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un **Remote Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.
5. Seleccione **Orígenes** en el menú desplegable **Seleccionar configuración**.
6. Haga clic en para mostrar el cuadro de diálogo **Agregar origen**.
7. Defina el Remote Collector de conmutación por error y haga clic en **Aceptar**.



Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Configurar la replicación

En este tema se indica cómo replicar los datos de eventos que envía un Remote Collector.

Una vez finalizado este procedimiento, habrá configurado Security Analytics para que replique los datos de eventos de un Remote Collector en varios grupos de destino de Local Collector.

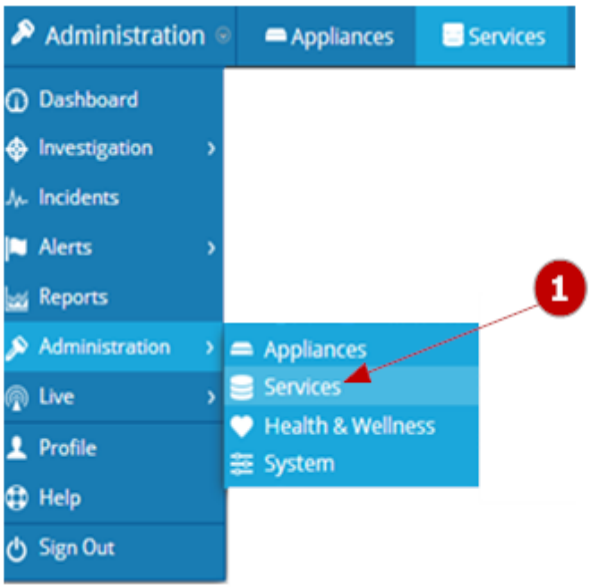
Volver a Procedimientos.

Procedimientos

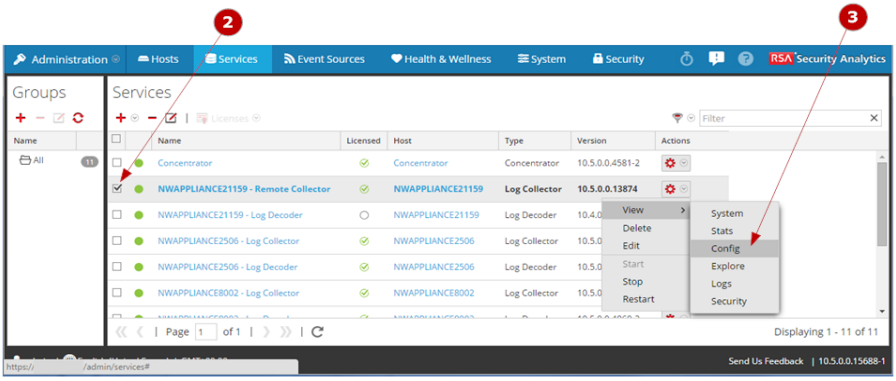
Replicar mensajes de eventos

Puede especificar varios grupos de destino para que los datos de eventos se repliquen en cada grupo.

En la siguiente figura se muestra cómo replicar datos de eventos en varios Local Collectors.

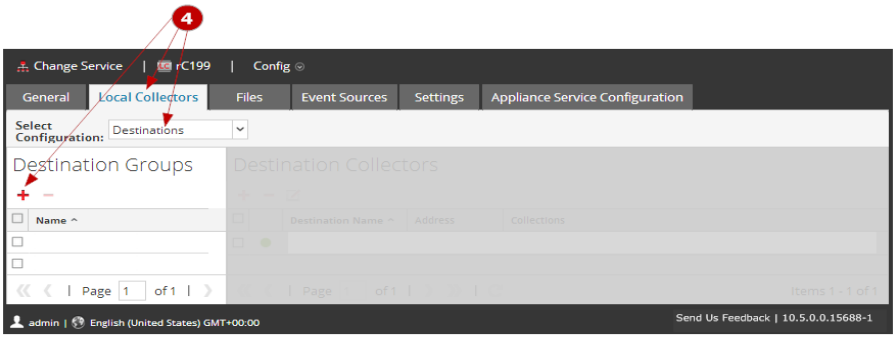


1 Acceda a la vista **Servicios**.

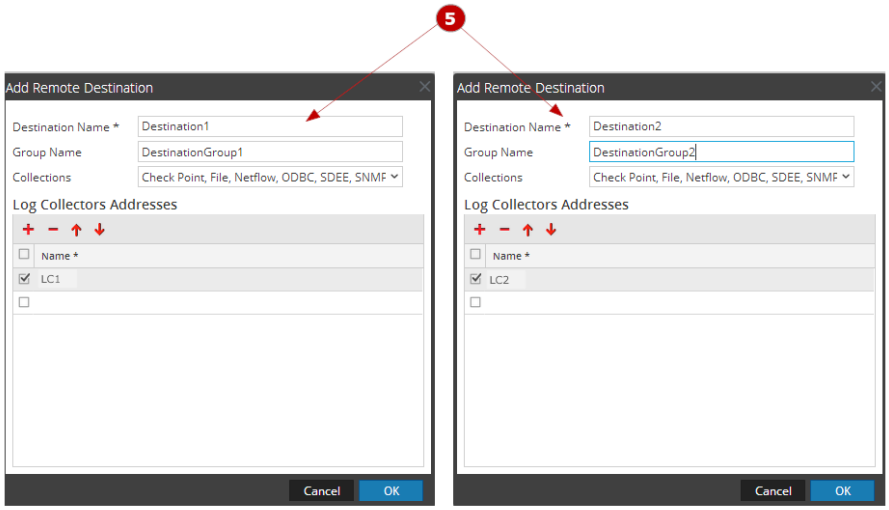


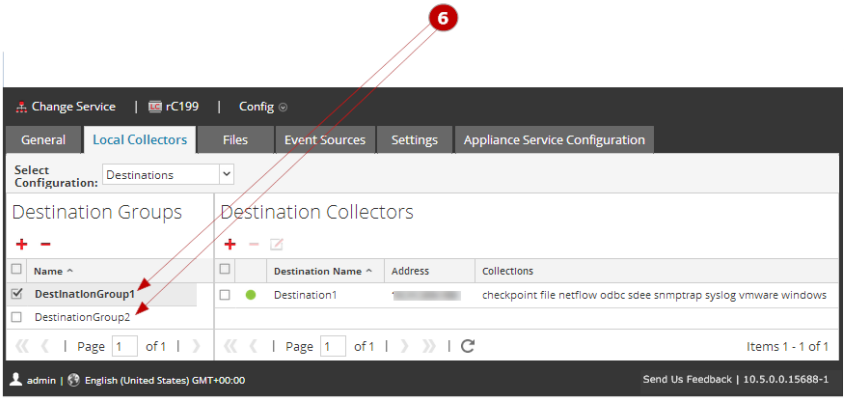
2 Seleccione un Remote Collector.

3 Haga clic en ⌄ bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



4 Seleccione la pestaña **Local Collectors**, seleccione **Destinos** en el menú desplegable **Seleccionar configuración** y haga clic en + en **Grupos de destino** para mostrar el cuadro de diálogo **Agregar destinos remotos**.





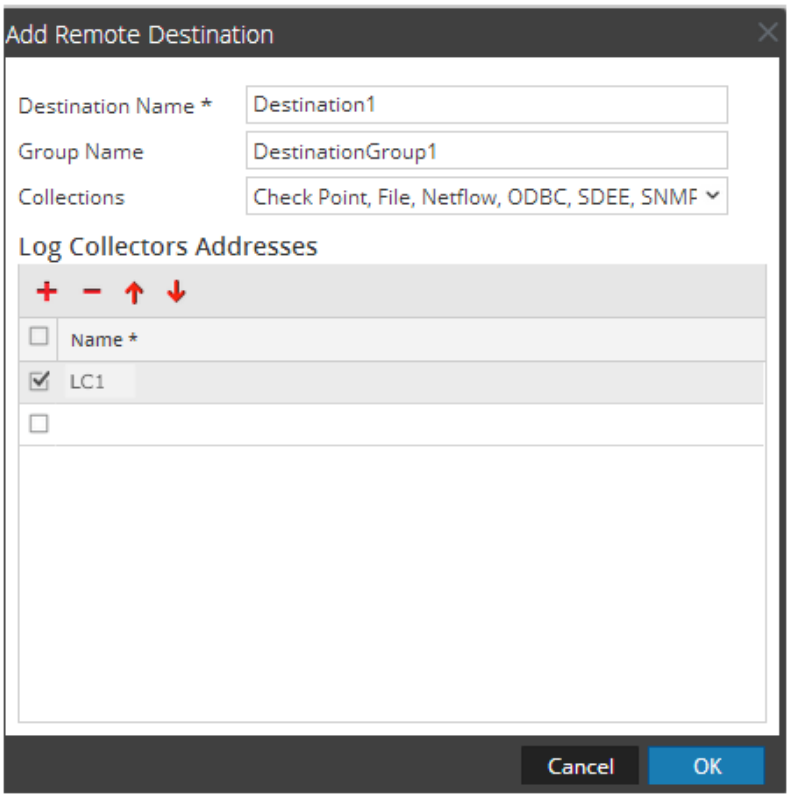
5 Configurar los **Grupos de destino** para facilitar la replicación

6 Los grupos de destino de replicación que acaba de agregar se muestran en la pestaña **Local Collector**.

Replicar datos de eventos en varios Local Collectors

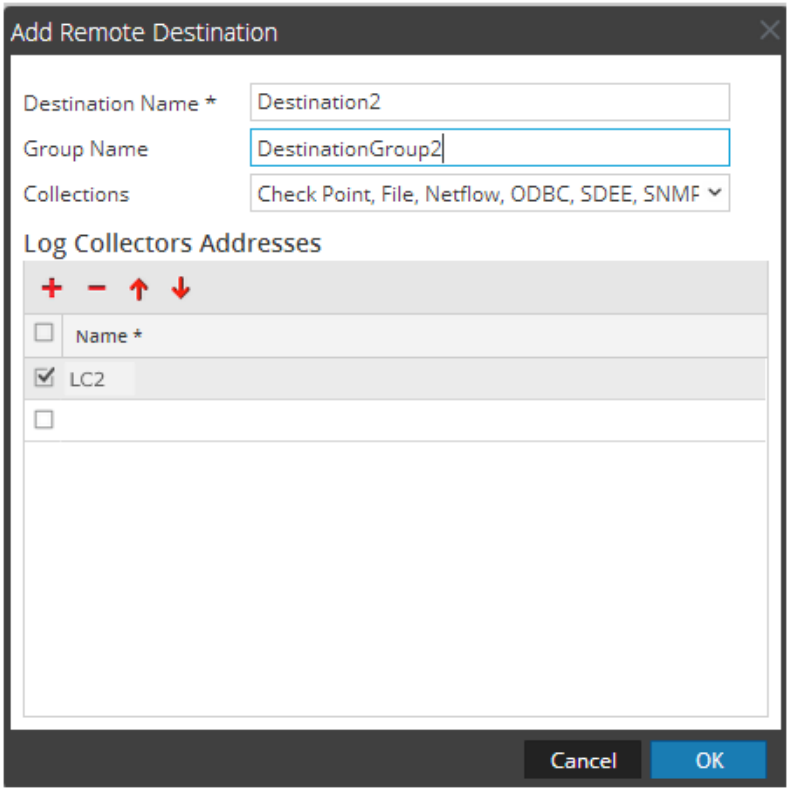
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un **Remote Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.
5. En la sección del panel **Grupos de destino**, haga clic en .
   Se muestra el cuadro de diálogo **Agregar destino remoto**.
6. Configure un destino por separado para cada Local Collector y especifique los protocolos para los cuales desea migrar mensajes de eventos a ese Local Collector. En los siguientes ejemplos se muestra la adición de dos Local Collectors de destino (**Destination1** y **Destination2**) para los protocolos de recopilación
   Punto de control, **Archivo**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog** y **Windows**:
   a. Escriba el **Nombre del destino**.
   b. Escriba el **Nombre del grupo**. Si no escribe un Nombre del grupo, el Nombre del destino se toma como el Nombre del grupo.
   c. Seleccione los protocolos de recopilación en la lista desplegable.
   d. Seleccione un Local Collector (por ejemplo, **LC1**).

e. Haga clic en **Aceptar**.

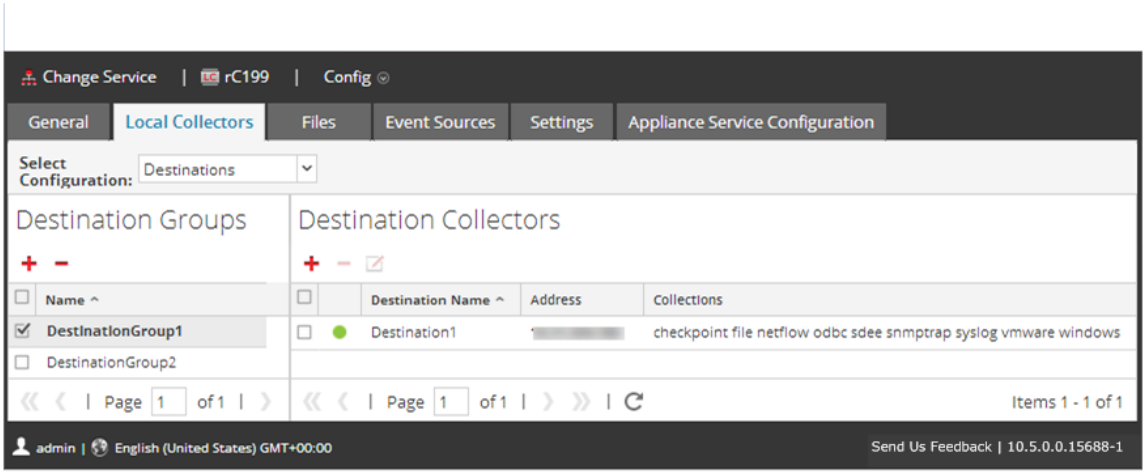


f. Seleccione el nuevo grupo (por ejemplo, **DestinationGroup2**) en el panel **Grupos de destino** y haga clic en + en el panel **Local Collector**.

g. En el panel **Local Collector**, haga clic en + y complete el cuadro de diálogo **Agregar destino remoto**, como se muestra en la siguiente figura.



Los protocolos de recopilación **Punto de control**, **Archivo**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog** y **Windows** se envían a dos Local Collectors (**LC1** y **LC2**). Ambos Local Collectors están activos y recopilan datos de eventos.



Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Configurar el enrutamiento de registros para protocolos específicos

En este tema se indica cómo definir el enrutamiento de los mensajes de eventos de protocolo específicos mediante la configuración de varios Local Collectors en un grupo de destino. Esto puede ayudarlo a dirigir datos de eventos a ubicaciones específicas según el tipo de protocolo.

Después de completar este procedimiento, habrá configurado varios destinos, de un grupo de destinos, a los cuales Security Analytics distribuye los datos de eventos de protocolo.

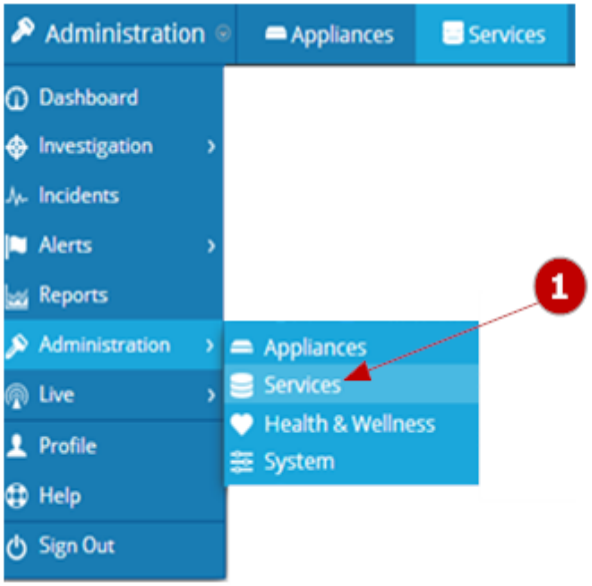
Volver a Procedimientos

Procedimiento

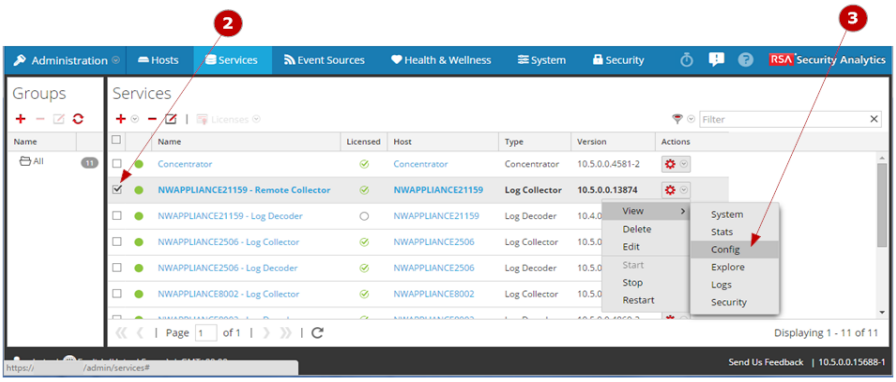
Definir el enrutamiento de datos de eventos de protocolo

Cuando se migra a más de un Local Collector, puede optar por enrutar datos de eventos de protocolo específicos a varios Local Collectors mediante la especificación de varios destinos dentro de un grupo de destinos. Un grupo de destinos es un conjunto de Local Collectors que permite que los datos de eventos se distribuyan a todos los miembros del grupo.

En la siguiente figura se muestra cómo enrutar los mensajes de eventos de un protocolo de recopilación.

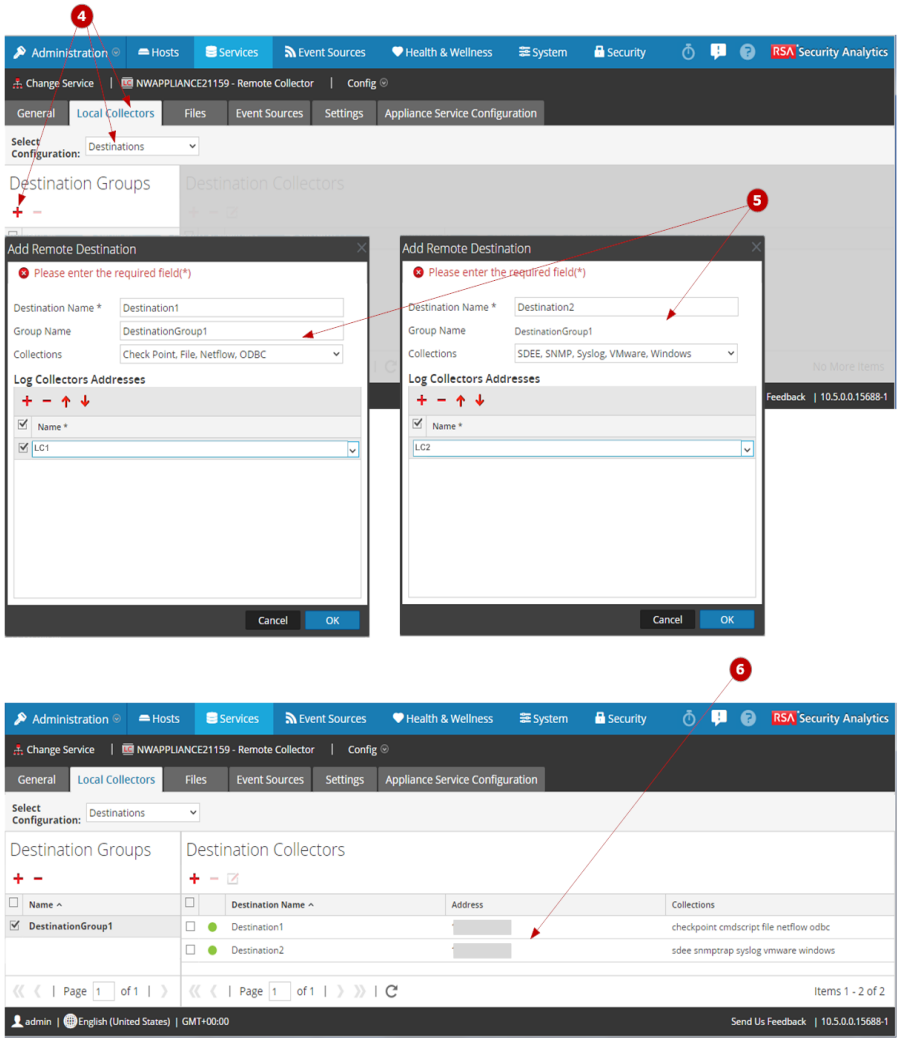


1 Acceda a la vista **Servicios**.



2 Seleccione un Remote Collector.

3 Haga clic en bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



4 Seleccione la pestaña **Local Collectors**, seleccione **Destinos** en el menú desplegable **Seleccionar configuración** y haga clic en + en **Grupos de destino** para mostrar el cuadro de diálogo **Agregar destinos remotos**.

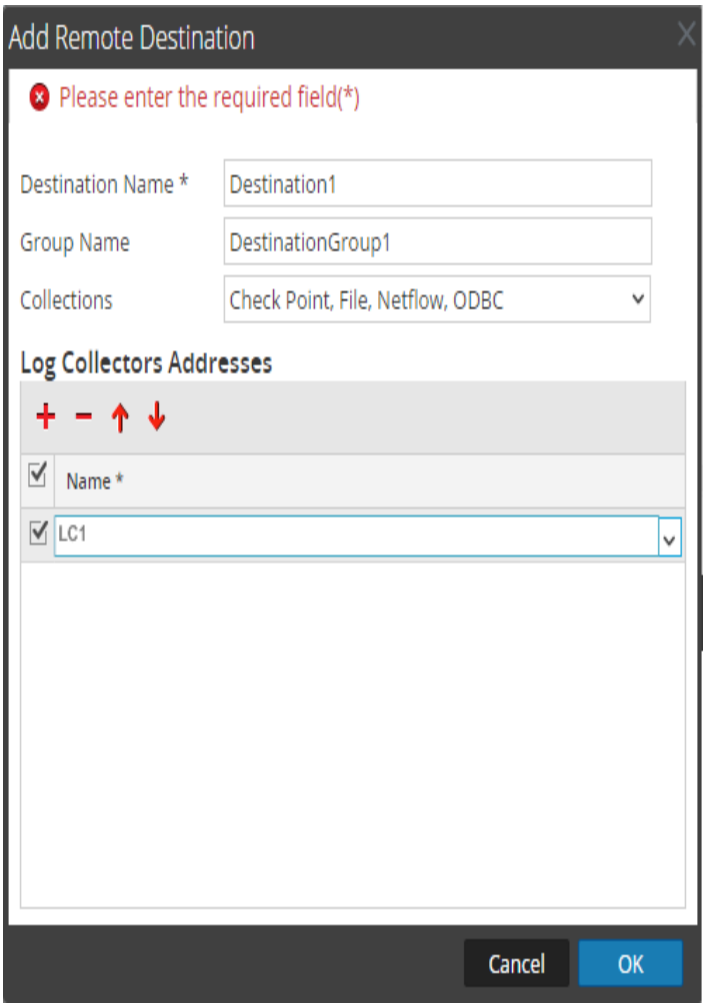
5 Configure un destino por separado para cada Local Collector y especifique los protocolos para los cuales desea migrar mensajes de eventos a ese Local Collector.

6 La configuración de Local Collector primario y con balanceo de carga que acaba de agregar se muestra en la pestaña **Local Collector**.

Configurar el enrutamiento de mensajes de eventos desde un protocolo de recopilación

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un **Remote Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.
5. En el panel **Grupos de destino**, haga clic en .
   Se muestra el cuadro de diálogo **Agregar destino remoto**.
6. Configure un destino por separado para cada Local Collector y especifique los protocolos para los cuales desea migrar mensajes de eventos a ese Local Collector. En los siguientes ejemplos se muestra la adición de dos Local Collectors de destino (**Destination1** y **Destination2**). Esta configuración envía:
   - Datos de eventos de **Punto de comprobación**, **Archivo y ODBC** a **Destination1**.
   - Datos de eventos de **Syslog** y **Windows** a **Destination2**.

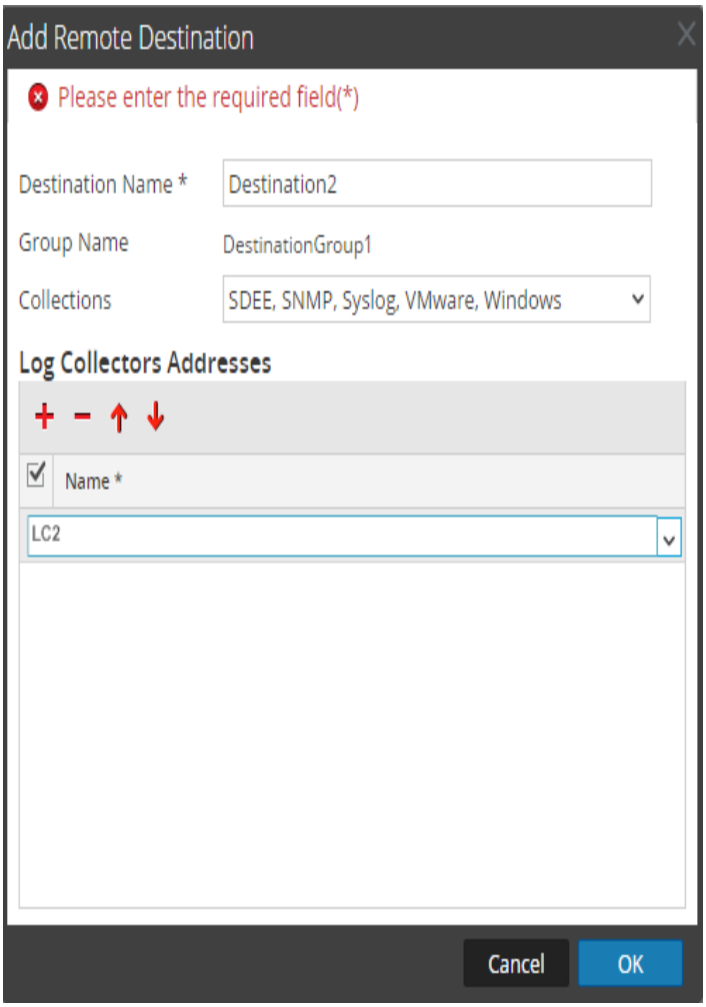
   a. Escriba el **Nombre del destino**.
   b. Escriba el **Nombre del grupo**. Si no escribe un Nombre del grupo, el Nombre del destino se toma como el Nombre del grupo.
   c. Seleccione el protocolo de recopilación en la lista desplegable.
   d. Seleccione un Local Collector (por ejemplo, **LC1**)



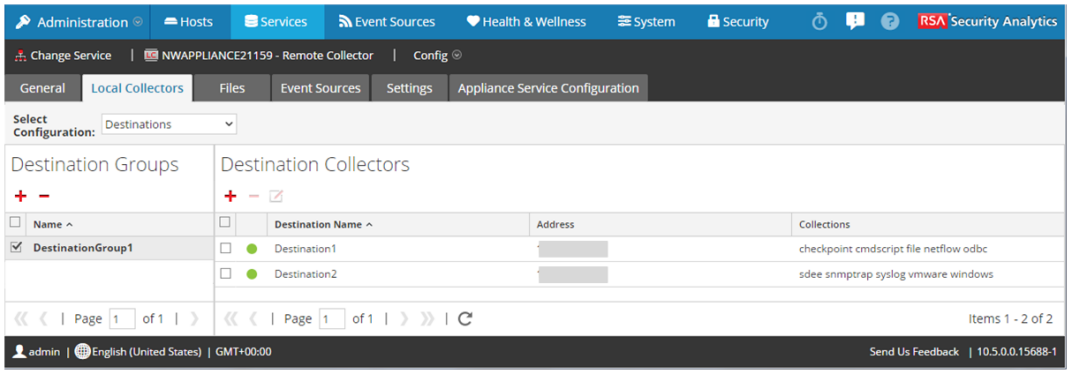
e. Haga clic en **Aceptar**. **Destination1** se crea y se muestra en el panel **Grupos de destino**.

f. Seleccione el nuevo grupo (por ejemplo, **Destination1**) en el panel **Grupos de destino** y haga clic en + en el panel **Local Collector**.

g. En el panel **Local Collector**, haga clic en + y complete el cuadro de diálogo **Agregar destino remoto**, como se muestra en la siguiente figura.



Se balancea la carga de los protocolos de recopilación **Punto de control**, **Archivo**, **ODBC**, **Syslog** y **Windows** entre dos Local Collectors (LC1 y LC2). Ambos Local Collectors están activos y recopilan datos de eventos.



Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Configurar una cadena de Remote Collectors

En este tema se describe cómo encadenar Remote Collectors (a los cuales también se denomina VLC).

Puede configurar una cadena de Remote Collectors para migrar datos de eventos a un Remote Collector o puede configurar un Remote Collector para extraer datos de eventos desde una cadena de Remote Collectors.

- Remote Collectors para migrar datos de eventos a un Remote Collector.
- Un Remote Collector para extraer datos de eventos de uno o más Remote Collectors.

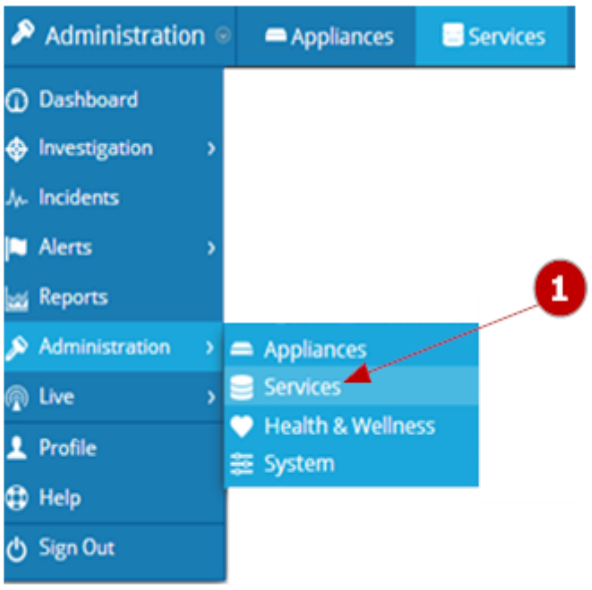
Nota: Para el encadenamiento de Remote Collector, solo puede:
Migrar datos desde un Remote Collector 10.4 o superior a otros Remote Collectors 10.4 o superiores o Local Collectors 10.4 o superiores.
Usar un Remote Collector 10.4 o superior para extraer datos desde uno o más Remote Collectors 10.4 o superiores.

Procedimientos

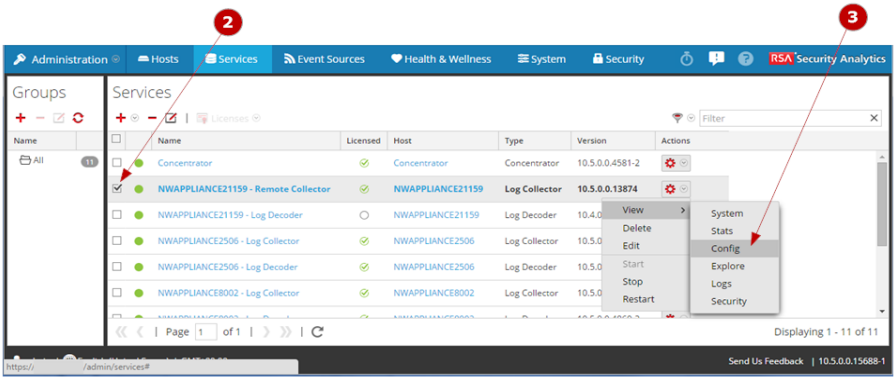
Configurar un Remote Collector para migrar datos de eventos a un Remote Collector

Puede configurar un Remote Collector para migrar datos de eventos a un Remote Collector.

En la siguiente figura se muestra cómo configurar un Remote Collector para migrar datos de eventos a un Remote Collector.

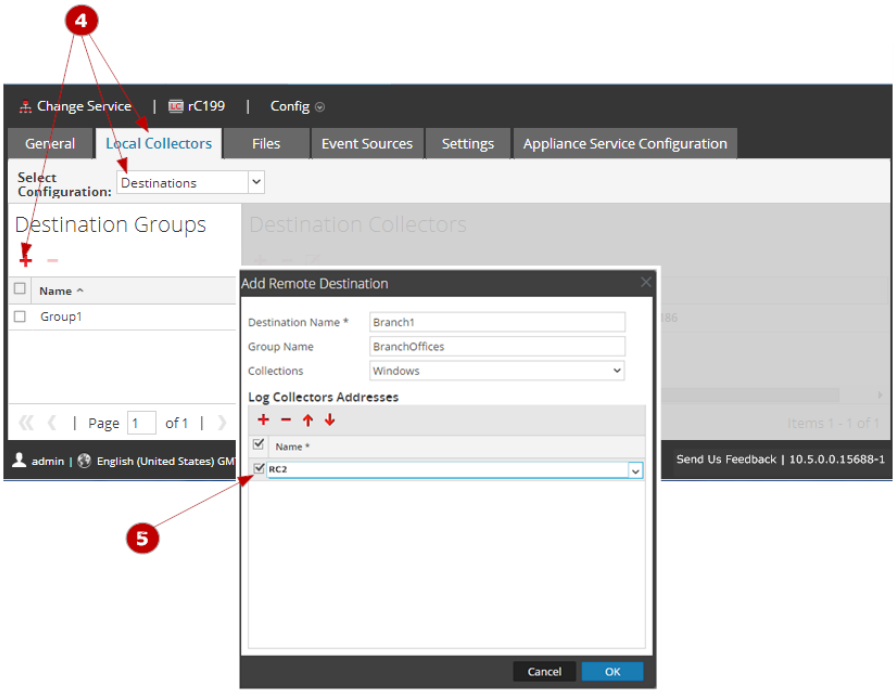


1. Acceda a la vista **Servicios**.



2. Seleccione un Remote Collector.

3. Haga clic en ⌄ bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.

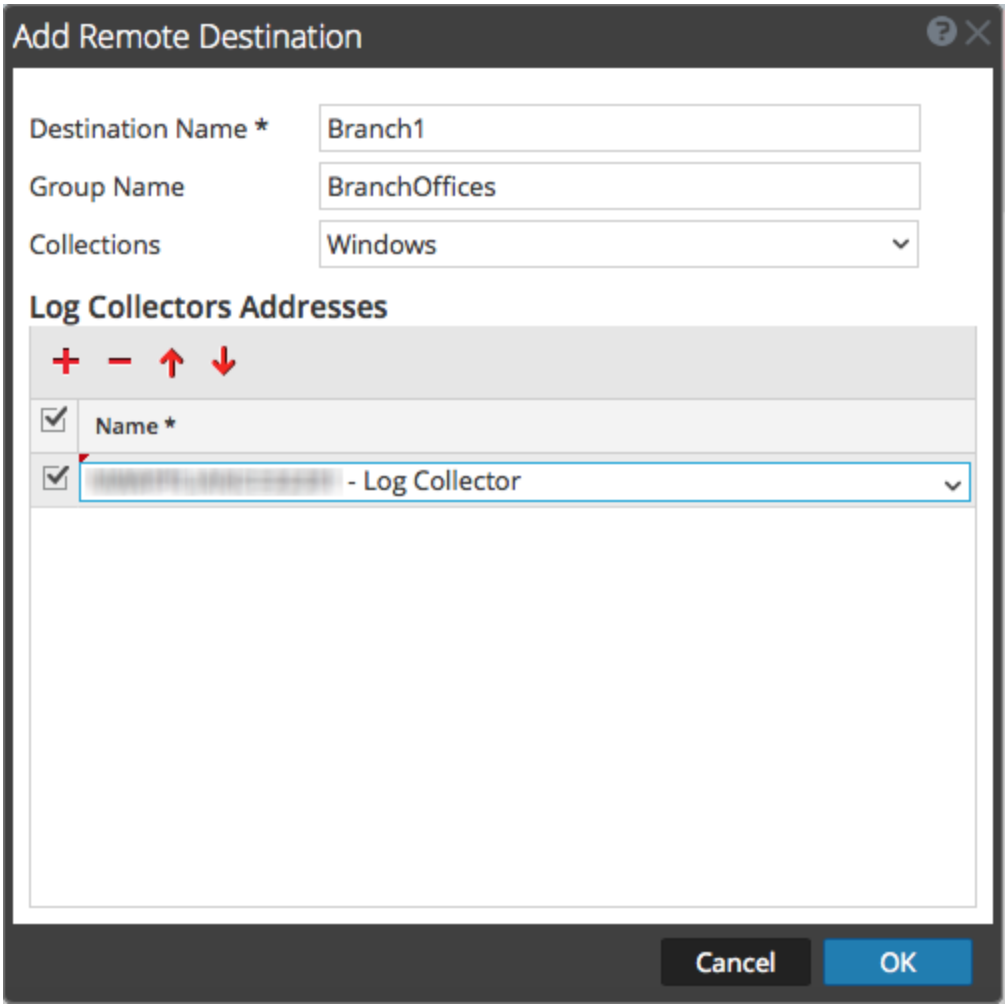


4. Seleccione la pestaña **Local Collectors**, seleccione **Destinos** en el menú desplegable **Seleccionar configuración** y haga clic en + en **Grupos de destino** para mostrar el cuadro de diálogo **Agregar destinos remotos**.

5 Configure los grupos de destino.

Configurar el Remote Collector seleccionado para migrar eventos a un Remote Collector especificado

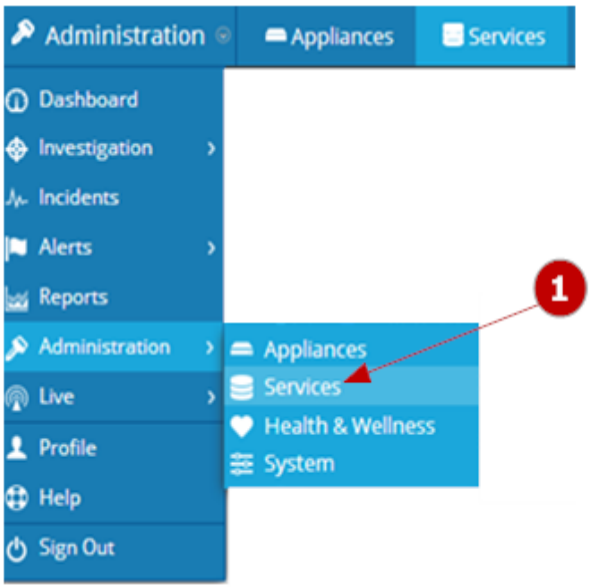
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un **Remote Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio Log Collector** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.
5. Seleccione **Destinos** en el menú desplegable **Seleccionar configuraciones**.
6. En la sección del **panel Grupos de destino**, seleccione .
   Se muestra el cuadro de diálogo **Agregar destino remoto**.
7. Configure un **grupo de destino**:
   a. Ingrese un **Nombre de destino**.
   b. (Opcional) **Ingrese un Nombre del grupo**. Si deja Nombre del grupo en blanco, Security Analytics lo establece en el valor que especificó en Nombre del destino.
   c. Seleccione uno o más protocolos de recopilación en la lista desplegable **Recopilaciones**.
   d. En **Direcciones de Log Collector**, haga clic en para seleccionar un Remote Collector.



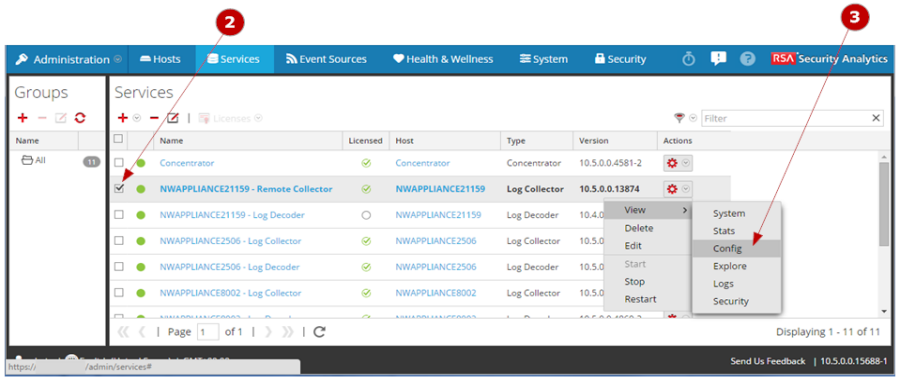
Nota: Si no selecciona un protocolo de recopilación, el Remote Collector migra todos los protocolos de recopilación a los Remote Collectors.

Configurar un Remote Collector para extraer datos de eventos de un Remote Collector

En la siguiente figura se muestra cómo configurar un Remote Collector para extraer eventos de un Remote Collector especificado.

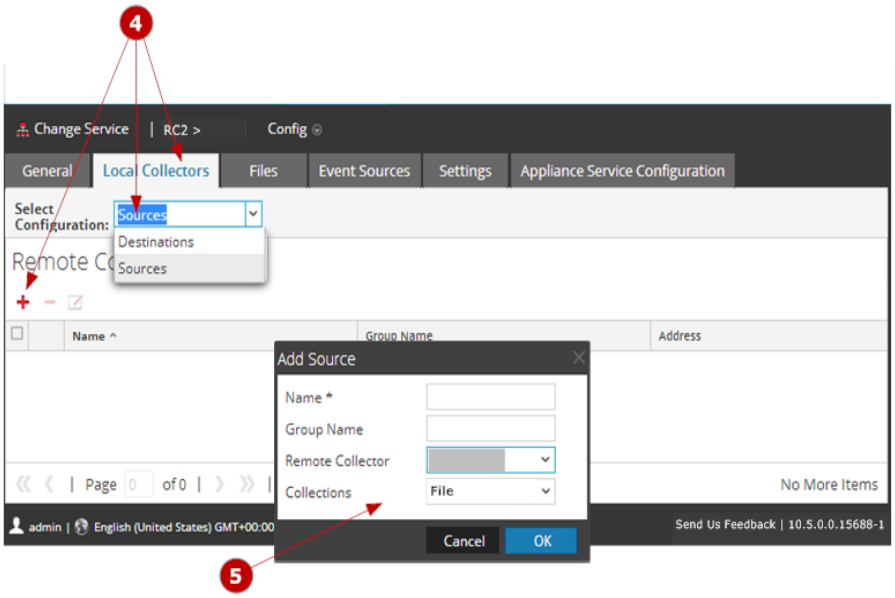


1 Acceda a la vista **Servicios**.



2 Seleccione un Remote Collector.

3 Haga clic en bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



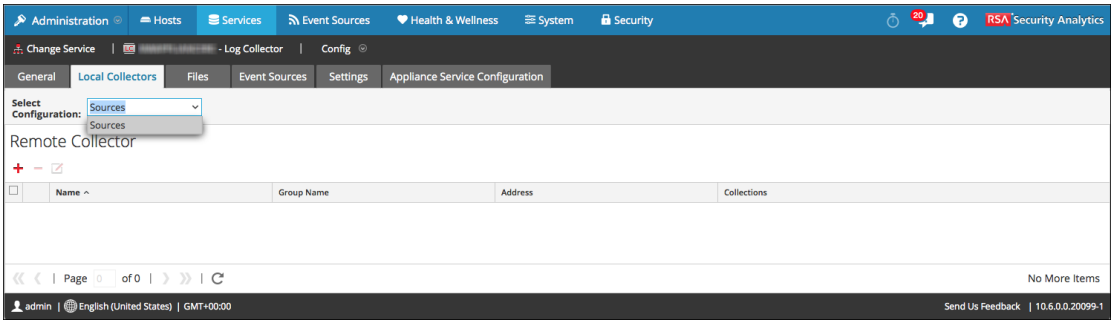
4 Seleccione la pestaña **Local Collectors**, elija **Orígenes** en el menú desplegable **Seleccionar configuraciones** y haga clic en + en **Remote Collectors** para mostrar el cuadro de diálogo **Agregar origen**.

5 En el cuadro de diálogo **Agregar origen**, seleccione el Remote Collector desde el cual desea extraer eventos.

Configurar el Remote Collector seleccionado para extraer eventos de un Remote Collector especificado

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un **Remote Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.

5. Seleccione **Orígenes** en el menú desplegable **Seleccionar configuraciones**.



6. En el panel **Remote Collectors**, seleccione  .

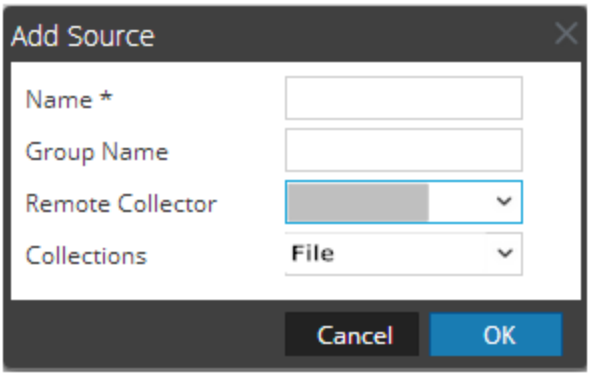
   Se muestra el cuadro de diálogo **Agregar origen**.

7. En el cuadro de diálogo **Agregar origen**:

   a. Seleccione uno o más protocolos de recopilación.

      Si no selecciona un protocolo de recopilación, el Remote Collector extrae todos los protocolos de recopilación desde el Remote Collector.

   b. Haga clic en **Aceptar**.



   El Remote Collector se agrega a la sección Remote Collector. Cuando el Log Collector comienza a recopilar datos, extrae datos de eventos de este Remote Collector.

Parámetros

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

Regular un Remote Collector al ancho de banda del Local Collector

Para mejorar el rendimiento, puede regular el ancho de banda con el fin de controlar la velocidad a la cual el Remote Collector envía datos de eventos al Local Collector o entre intermediadores de mensajes. Para ello, configure el filtrado del kernel de Linux y la funcionalidad IpTable.

Esto funciona en las configuraciones de migración y extracción de Remote Collector. El script de shell **set-shovel-transfer-limit.sh** que se encuentra en **/opt/netwitness/bin** automatiza la configuración del filtro de kernel y las iptables relacionadas con este puerto.

Contexto

Después de leer este tema, sabe cómo regular el ancho de banda de Remote Collector a Local Collector con el script de shell **set-shovel-transfer-limit.sh** mediante la revisión de:

- La ayuda de la línea de comandos de script de shell **set-shovel-transfer-limit.sh** .

> **Nota:** El valor del filtro que necesita establecer depende de la velocidad a la que colector de registro remoto envía eventos al Local Collector.

- Un ejemplo que establece el filtro en 4.096 kilobits por segundo.

Volver a Procedimientos

Ayuda de la línea de comandos set-shovel-transfer-limit.sh

Emita el comando `-h` para mostrar la ayuda para el script de shell `set-shovel-transfer-limit.sh`.

```
cd /opt/netwitness/bin
./set-shovel-transfer-limit.sh
```

```
Usage: set-shovel-transfer-limit.sh -s|-c|-d|[-i interface] [-r rate]
```

donde:

-c = clear existing

-d = display filter

-s = set new values

-i = interface is the name of the network interface. default=eth0

-r = rate is the bandwidth rate. default=256kbps
Bandwidths or rates can be specified in:
nolimit = disables throttling
kbit = Kilobits per second
mbit = Megabits per second
kbps = Kilobytes per second
mbps = Megabytes per second
bps = Bytes per second

Establecer el filtro en 4.096 kilobits por segundo.

[root@<hostname> bin]# ./set-shovel-transfer-limit.sh -s -r 4096kbit

RATE=4096kbit
PORTNUMBER=5671
DEVICE_INTERACE=eth0

iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[OK]

Current/new values...

```
iptables -t mangle -n -v -L
 Chain PREROUTING (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target  prot opt in  out  source    destination
 Chain INPUT (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target prot opt in out   source    des-
tination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in out   source    destination
Chain OUTPUT (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source    destination
   0  0 MARK   tcp -- *  eth0   0.0.0.0/0   0.0.0.0/0
multiport dports 5671 MARK set 0xa
   0  0 MARK   tcp -- *  eth0   0.0.0.0/0  0.0.0.0/0  multiport
sports 5671 MARK set 0xa
Chain POSTROUTING (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source    destination
tc -s -d class show dev eth0
 class htb 1:1 root rate 10000Kbit ceil 10000Kbit burst 1600b/8
mpu 0b overhead 0b cburst 1600b/8 mpu 0b overhead 0b level 7
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 20000 ctokens: 20000
class htb 1:2 parent 1:1 prio 0 quantum 51200 rate 4096Kbit ceil
4096Kbit burst 1599b/8 mpu 0b overhead 0b cburst 1599b/8 mpu 0b
overhead 0b level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 48828 ctokens: 48828
```

Referencia: Interfaz de parámetros de configuración de los Remote/Local Collectors

En este tema se presenta la interfaz del usuario para configurar los parámetros de la implementación de la recopilación de registros

La vista Configuración de servicios permite mantener todos los parámetros de la recopilación de registros. La pestaña en la cual se mantienen los parámetros de la implementación que se mencionan en esta guía es la pestaña **Remote/Local** Collectors:

- Si está configurando un Local Collector, Security Analytics muestra la pestaña **Remote Collectors** para que pueda configurar el Local Collector de modo que extraiga eventos de Remote Collectors.
- Si está configurando un Remote Collector, Security Analytics muestra la pestaña **Local Collectors** para que pueda configurar el Remote Collector de modo que migre eventos a un Local Collector.

En este tema se presentan las funciones de la **vista Configuración de servicios > pestaña Remote Collectors/Local Collectors**

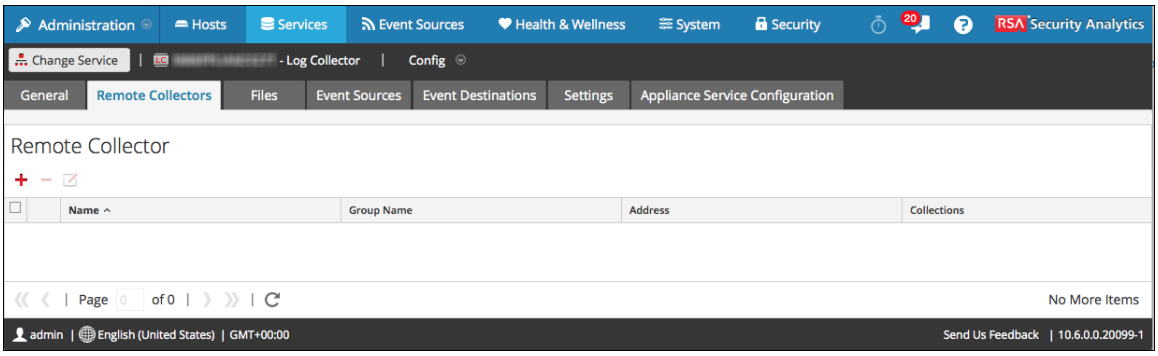
Pestaña Remote/Local Collectors

Si implementa Remote Collectors, el administrador de RSA Security Analytics debe configurar el método de envío al Local Collector de los eventos que recopilan los Remote Collectors.

Para acceder a esta pestaña:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Remote Collectors**.

En la siguiente figura se muestra la pestaña **Remote Collectors** de un Local Collector configurado para extraer eventos de un Remote Collector. Security Analytics muestra esta pestaña si se seleccionó un Local Collector en **Administration > Servicios**.

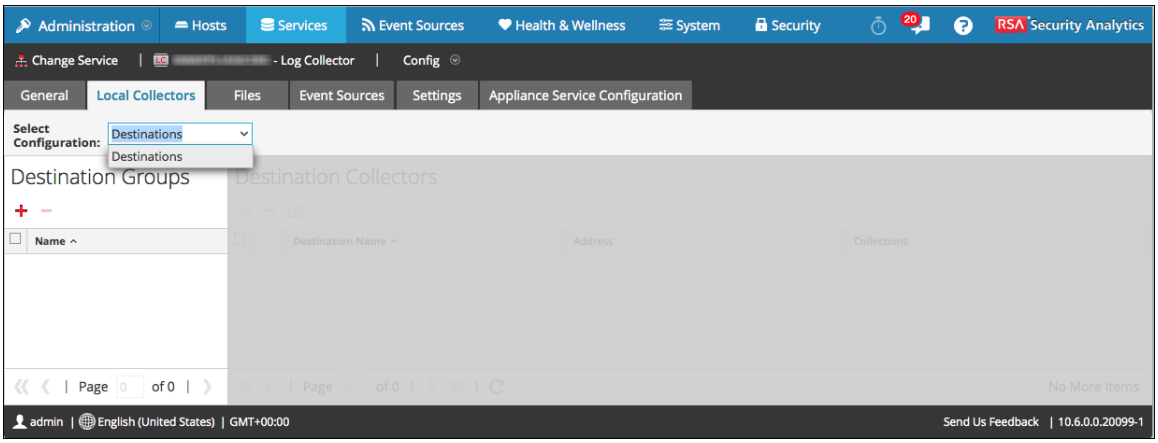


Pestaña Local Collectors para un Remote Collector

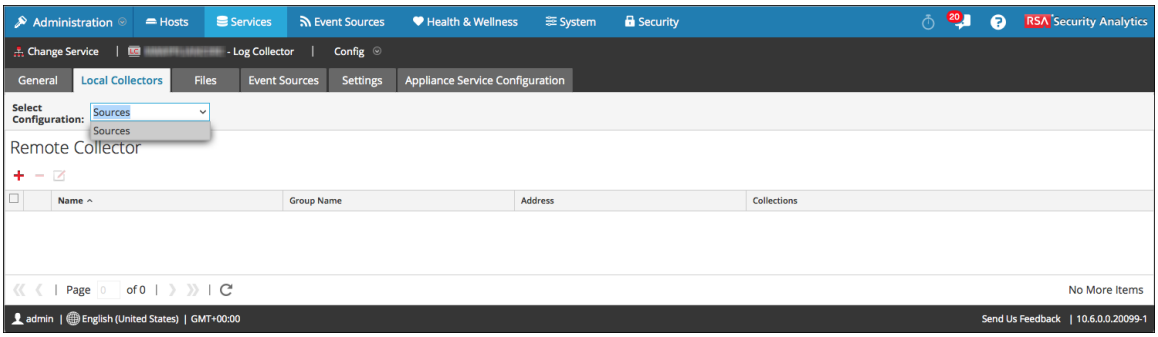
Para acceder a esta pestaña:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.

En la siguiente figura se muestra una pestaña **Local Collectors** de un Remote Collector configurado para migrar eventos a un Local Collector o a otro Remote Collector.



En la siguiente figura se muestra la pestaña Local Collectors de un Remote Collector configurado para extraer eventos de un Remote Collector. Security Analytics muestra esta pestaña si se seleccionó un Remote Collector en **Administration > Servicios**.



Pestaña Remote Collectors

En un Local Collector, el panel Remote Collectors proporciona una manera de agregar o eliminar Remote Collectors desde donde el Local Collector extrae eventos.

Panel Remote Collector

Columna	Descripción
	Muestra el cuadro de diálogo **Agregar origen** que permite seleccionar los Remote Collectors desde los cuales desea que el Local Collector extraiga eventos.
	Elimina el Remote Collector desde el panel Remote Collectors del Local Collector.
	Muestra el cuadro de diálogo **Editar origen** para el Remote Collector seleccionado.
	Selecciona Remote Collectors.
Nombre	Nombres de los Remote Collectors desde los cuales el Local Collector extrae eventos actualmente.
Dirección	Direcciones IP de los Remote Collectors desde los cuales el Local Collector extrae eventos actualmente.

Columna	Descripción
Recopilaciones	Elija los protocolos de recopilación que el Remote Collector migra a un Local Collector: **Punto de comprobación** **Archivo** **Flujo de red** **ODBC** **Plug-ins** **SDEE** **SNMP** **VMware** **Windows** **Windows existente** Puede seleccionar cualquier combinación de protocolos. Si no selecciona un protocolo, Security Analytics los selecciona todos.

Pestaña Local Collector

En un Remote Collector, el panel Local Collector proporciona una manera de agregar o eliminar los Local Collectors a los cuales desea que el Remote Collector migre eventos.

Seleccione el **Destino** o el **Origen** en el menú desplegable **Seleccionar configuración**.

- **Destino** muestra el cuadro de diálogo **Agregar destino remoto**.
- Origen muestra el cuadro de diálogo **Agregar origen**.

En la siguiente tabla se describe el cuadro de diálogo Agregar origen.

Columna	Descripción
	Muestra el cuadro de diálogo **Agregar origen** que permite seleccionar los Remote Collectors desde los cuales desea que el Local Collector extraiga eventos.
	Elimina el Remote Collector desde el panel Remote Collectors del Local Collector.

Columna	Descripción
	Muestra el cuadro de diálogo **Editar origen** para el Remote Collector seleccionado.
	Selecciona Remote Collectors.
Nombre	Nombres de los Remote Collectors desde los cuales el Local Collector extrae eventos actualmente.
Dirección	Direcciones IP de los Remote Collectors desde los cuales el Local Collector extrae eventos actualmente.

En la siguiente tabla se describe el panel Local Collectors.

Columna	Descripción
	Muestra el cuadro de diálogo **Agregar destino remoto** correspondiente al grupo que seleccionó. Debe agregar Local Collectors de destino para este grupo a los cuales desea que el Remote Collector migre eventos.
	Elimina el Log Collector de destino del grupo.
	Muestra el cuadro de diálogo **Editar destino remoto** para el Local Collector de destino seleccionado.
	Selecciona un Local Collector de destino.
Nombre del destino	Muestra el nombre del Local Collector de destino.
Dirección	Muestra la dirección IP del Local Collector de destino.

Columna	Descripción
Recopilaciones	Elija los protocolos de recopilación que el Local Collector extrae de un Remote Collector: **Punto de comprobación** **Archivo** **Flujo de red** **ODBC** **Plug-ins** **SDEE** **SNMP** **VMware** **Windows** **Windows existente** Puede seleccionar cualquier combinación de protocolos. Si no selecciona un protocolo, Security Analytics los selecciona todos.

Tareas

Configurar Local y Remote Collectors

Solucionar problemas de la implementación de la recopilación de registros

En este tema se sugiere cómo resolver los problemas que puede encontrar durante la implementación

Security Analytics le informa sobre problemas o posibles problemas de Log Collector de las dos maneras siguientes:

- Archivos de registro.
- Vista Monitoreo de Estado y condición

Archivos de registro

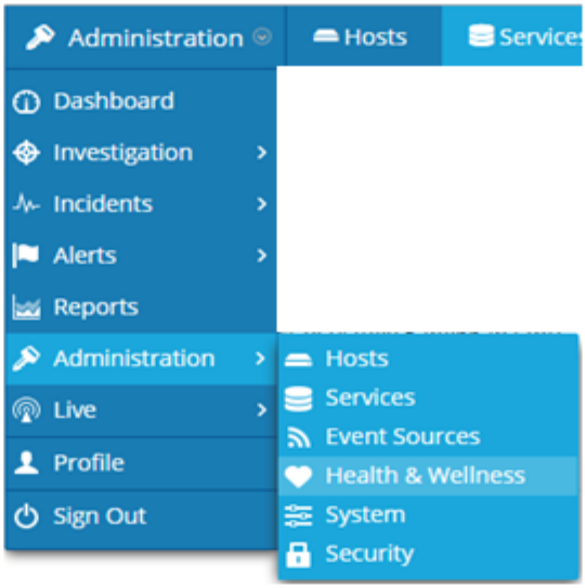
Si un protocolo de recopilación de orígenes de eventos específico presenta problemas, puede revisar los registros de depuración para investigarlos. Cada origen de eventos posee un parámetro de Depuración que puede activar (configurar en Activado o Detallado) para capturar estos registros.

Active la depuración solamente si este origen de eventos presenta problemas y necesita investigarlos. Si activa la depuración en todo momento, esta afectará negativamente al rendimiento de Log Collector.

Security Analytics tiene un conjunto de mensajes de error asociados con la recopilación de registros que incluye en archivos de registro.

Monitoreo del estado y la condición

El monitoreo del estado y la condición le permite informarse oportunamente de posibles problemas de hardware y software de modo que pueda evitar interrupciones. RSA recomienda monitorear los campos estadísticos de Log Collector para asegurarse de que el servicio funcione de manera eficiente y que no se encuentre en los valores máximos configurados ni cerca de estos. Puede monitorear las estadísticas que se describen en la vista **Administration > Estado y Condición**.



Guía de configuración de la recopilación de registros

En esta guía se indica cómo configurar la recopilación de registros después de su implementación (es decir, después de haber configurado Local y Remote Collectors).

Esta guía le indica:

- La función de la recopilación de registros y una descripción general de su funcionamiento con diagramas de implementación generales.
- Cómo comenzar a recopilar eventos.
- Dónde encontrar instrucciones para configurar implementaciones más complejas.
- Cómo iniciar, poner en pausa y detener cualquier protocolo de recopilación.
- Cuál es la estructura de la interfaz del usuario de configuración de la recopilación de registros.
- Qué herramientas se deben usar para solucionar problemas de la recopilación de registros, con una lista de instrucciones globales de solución de problemas.
- Cómo ajustar y personalizar la recopilación de registros en un ambiente.

Esta guía no le indica cómo:

- Dar los primeros pasos con la creación de la implementación y la configuración mínimas y básicas. Esta información se encuentra en la Guía de introducción a la recopilación de registros.
- Implementar la recopilación de registros en múltiples ubicaciones con alta disponibilidad y balanceo de carga. Esta información se encuentra en la Guía de implementación de la recopilación de registros.
- Configure protocolos de recopilación individuales. Las instrucciones se encuentran en las guías de recopilación de registros individuales:

- Guía de configuración de la recopilación de AWS (CloudTrail)
- Guía de configuración de la recopilación de punto de comprobación
- Guía de configuración del protocolo de recopilación de archivos
- Guía de configuración de la recopilación de Netflow
- Guía de configuración de la recopilación de ODBC
- Guía de configuración de la recopilación de SDEE
- Guía de configuración de la recopilación de SNMP
- Guía de configuración de la recopilación de VMware
- Guía de configuración de la recopilación de Windows
- Guía de configuración de la recopilación de Windows existente y NetApp
- Las guías de configuración de cada origen de eventos compatible están disponibles en la página Orígenes de eventos compatibles.

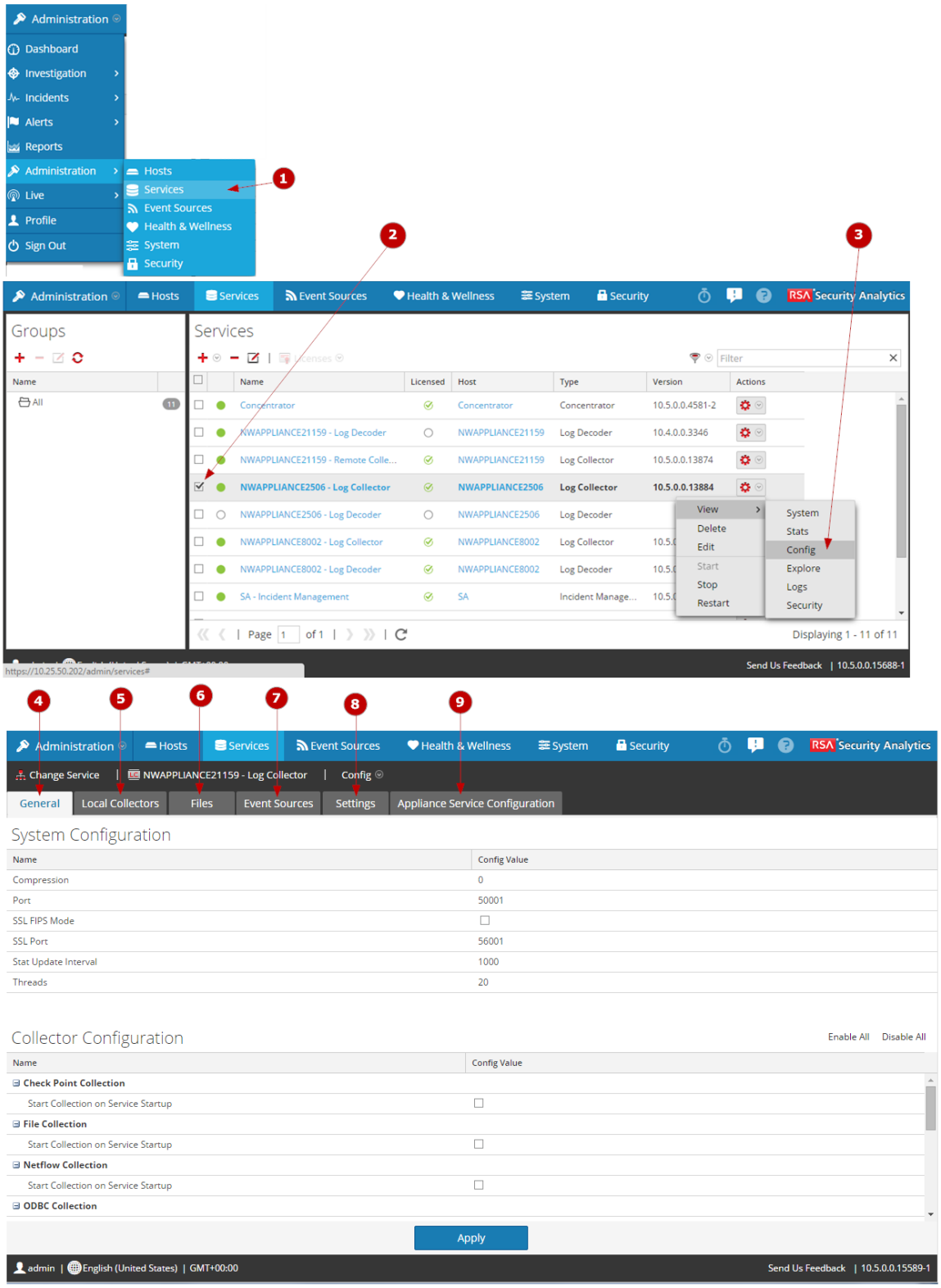
Conceptos básicos

En este tema se describe el proceso de configuración y se muestra cómo realizar esta configuración mediante la interfaz del usuario de Security Analytics.

Configuración de la recopilación de registros

Después de implementar la recopilación de registros, debe configurar los parámetros de cada servicio Log Collector que se ejecuta de forma local o remota. Realice esta configuración en las vistas de servicio de configuración de recopilación de registros.

Interfaz de parámetros de configuración



1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios** , seleccione el servicio Log Collector que desea configurar.
3. En la barra de herramientas, seleccione **Ver > Configurar**.
4. Haga clic en la pestaña **General** para revisar los parámetros generales del sistema y habilitar o deshabilitar el inicio automático de los protocolos de recopilación.
5. Haga clic en la pestaña **Remote Collectors/Local Collectors** para configurar el método de envío al Local Collector de los eventos que recopilan los Remote Collectors.
6. Haga clic en la pestaña **Archivos** para editar los archivos de configuración de servicios para Log Decoder como archivos de texto.
7. Haga clic en la pestaña **Orígenes de evento** para configurar parámetros para los protocolos de recopilación compatibles.
8. Haga clic en la pestaña **Configuración** para configurar el lockbox y administrar los certificados.
9. Haga clic en la pestaña **Configuración del servicio Appliance** para analizar las estadísticas del host de Log Decoder.

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para la recopilación de registros, con vínculos a cada paso de configuración.

Los pasos de configuración para Log Collector deben realizarse en la secuencia específica que se indica en la siguiente tabla. Cuando se completan estos pasos, Log Collector está operativo y la única configuración adicional que se requeriría sería debido a actualizaciones del sistema o del software.

Lista de verificación de la configuración

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Descripción	√
Paso 1. Descargar el contenido más reciente de LIVE	
Paso 2. Configurar ajustes (Configuración de seguridad de lockbox y certificados)	
Paso 3. Configurar orígenes de eventos en Security Analytics	
Paso 4. Configurar los orígenes de eventos para enviar eventos a Security Analytics	
Paso 5. Iniciar y detener servicios para los protocolos configurados	
Paso 6. Verificar que la recopilación de registros esté funcionando	

Paso 1. Descargar el contenido más reciente de LIVE

Descripción general

En este tema se le dirige a la documentación de Contenido y recursos de RSA, donde encontrará instrucciones para recuperar contenido de la recopilación de registros.

Contexto

LIVE es el sistema de administración de contenido de Security Analytics que permite descargar el contenido más reciente. Los dos tipos de recursos que se usan para descargar contenido de recopilación de registros son:

- **RSA Log Collector**: Contenido que permite recopilar tipos de orígenes de eventos.
- **RSA Log Device**: los últimos analizadores de orígenes de eventos compatibles. Consulte **Adición o actualización de analizadores de registros de orígenes de eventos compatibles** en la *Guía de contenido y recursos de RSA*.

Requisitos previos de un feed de identidad

Para crear un feed de identidad, debe tener:

- Un servicio Log Collector con la recopilación de Windows configurada y habilitada

- Debe haber creado y configurado un feed de identidad en LIVE. Consulte **Crear un feed de identidad** en la *Guía de administración de recursos de Live* para obtener instrucciones sobre cómo crear un feed de identidad en el sistema de administración de contenido de LIVE.

Paso 2. Configurar ajustes

Descripción general

En este tema, se presentan los ajustes que puede configurar para la recopilación de registros.

Contexto

Después de realizar este procedimiento, habrá seleccionado los ajustes de Log Collector que desea configurar.

Procedimiento

Para seleccionar los ajustes de Log Collector que desea configurar:

1. Seleccione un servicio Log Collector en la pestaña **Orígenes de evento** de la vista **Administration >Servicios > Ver > Configuración**.

   Se muestra la vista **Parámetros de configuración de Log Collector**.

2. Haga clic en la pestaña **Configuración del origen de eventos** y elija una de las dos opciones siguientes:

   - Lockbox
   - Certificados

Parámetros:

Pestaña Configuración de recopilación de registros

Configurar ajustes de seguridad de Lockbox

En este tema, se explica cómo cambiar la configuración de seguridad de lockbox. Una nueva estadística de Lockbox corresponde a una notificación de alarma de uso inmediato que monitorea el estado del Lockbox.

Después de realizar este procedimiento, habrá:

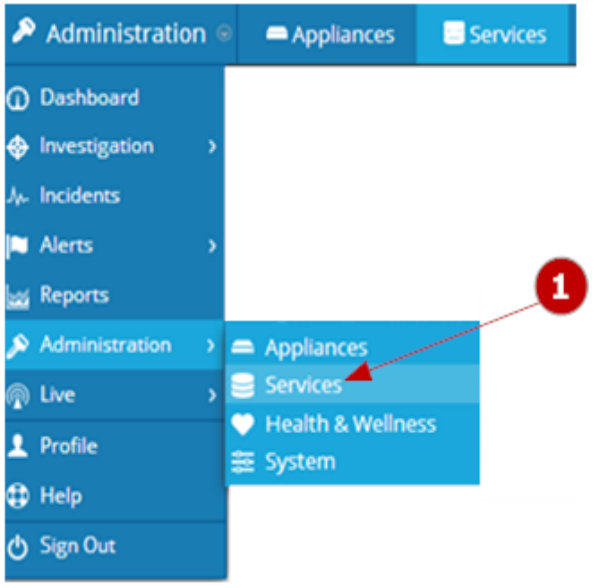
- Definido la contraseña de Lockbox
- Cambiado la contraseña de Lockbox
- Restablecido el valor de sistema estable

- Generado una nueva clave de cifrado
- Mostrado una estadística de Lockbox

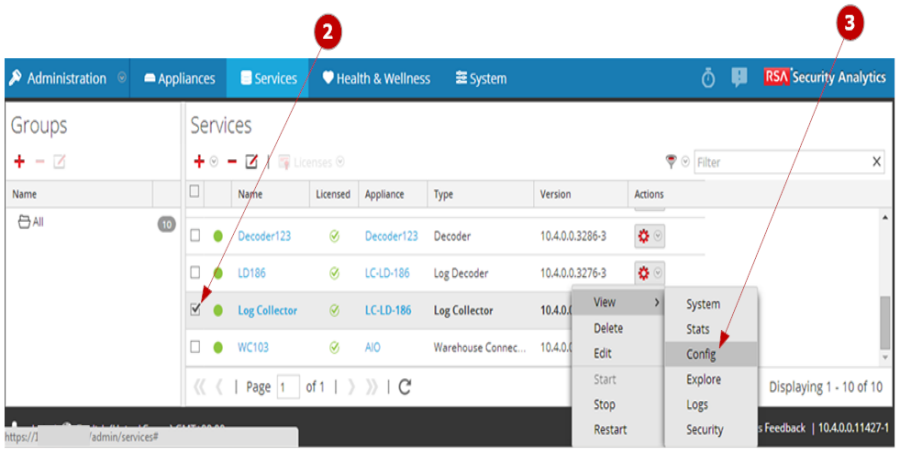
Nota: Puede configurar Estado y condición para que informe cuando hay un problema durante la configuración de Lockbox.

Volver a Procedimientos

En la siguiente figura se muestra cómo configurar los ajustes de seguridad de Lockbox.

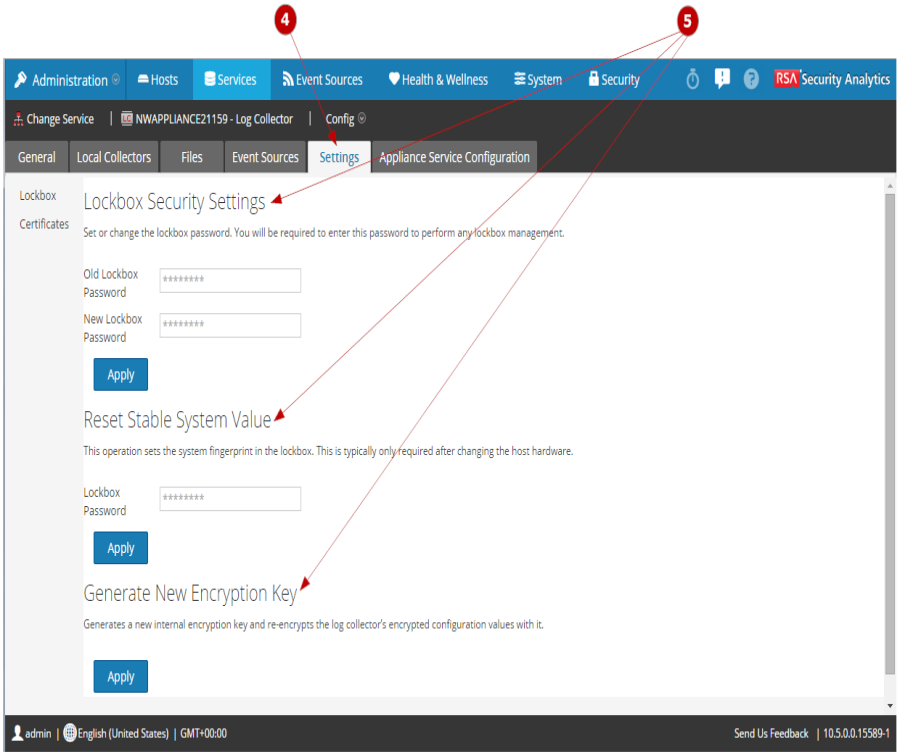


1 Acceda a la vista **Servicios**.



2 Seleccione un servicio de **recopilación de registros**.

3 Haga clic en bajo **Acciones** y seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.



4 Seleccione la pestaña **Configuración**.

5 Modifique los parámetros de **Lockbox**.

Procedimientos

Definir la contraseña de lockbox

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.

4. Haga clic en la pestaña **Configuración**.
5. En el panel de opciones, seleccione **Lockbox** para mantener la configuración de Lockbox.
6. En **Configuración de seguridad de lockbox**, ingrese una contraseña en el campo **Nueva contraseña de Lockbox** y haga clic en **Aplicar**.

Cambiar la contraseña de lockbox

En el menú de **Security Analytics**, seleccione **Administration > Servicios**.

1. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
2. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
3. Haga clic en la pestaña **Configuración**.
4. En el panel de opciones, seleccione **Lockbox** para mantener la configuración de Lockbox.
5. Ingrese la contraseña actual en el campo **Contraseña de Lockbox anterior**.
6. Ingrese una contraseña nueva en el campo **Nueva contraseña de Lockbox**.
7. Haga clic en **Aplicar**.
   Security Analytics cambia la contraseña anterior a la contraseña nueva.

Crear un nuevo Lockbox

Precaución: Si olvidó la contraseña actual, no podrá recuperarla desde el lockbox. Esto significa que debe volver a crear el lockbox. Si vuelve a crear el Lockbox, tendrá una nueva clave de cifrado. Esto significa que ya no se podrán descifrar las contraseñas de los orígenes de eventos existentes. Posteriormente debe restablecer la contraseña para cada origen de eventos.

Puede ser necesario crear un nuevo Lockbox si olvida su contraseña o si se produce un evento catastrófico.

Para crear un nuevo Lockbox:

1. En el dispositivo Log Collector, quite todos los archivos del directorio **/etc/netwitness/ng/vault**.
2. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
3. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
4. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
5. Haga clic en la pestaña **Configuración**.
6. En el panel de opciones, seleccione **Lockbox** para mantener la configuración de Lockbox.

7. Ingrese una contraseña nueva en el campo **Nueva contraseña de Lockbox**.

Nota: Su contraseña no se necesita para crear un nuevo Lockbox.

8. Haga clic en **Aplicar**.

Restablecer el valor de sistema estable

Precaución: Si varios valores de sistema estables cambian debido a actualizaciones del sistema, debe actualizar la huella digital del sistema host. Si no actualiza la huella digital del sistema host, Log Collector no podrá abrir el Lockbox y esto afectará a la recopilación de registros.

Para restablecer la contraseña de lockbox para el nuevo hardware de dispositivo (definir la huella digital del sistema en el nuevo hardware), haga lo siguiente:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Configuración**.
5. En **Restablecer valor de sistema estable**, ingrese una contraseña en el campo **Contraseña de lockbox** y haga clic en **Aplicar**.

Generar nueva clave de cifrado

Si genera una nueva clave de cifrado, las contraseñas para cualquier origen de eventos existente ya no se podrán descifrar, por lo que deberá restablecer la contraseña para cada origen de eventos.

Para generar una nueva clave de cifrado que se aplique a sus parámetros de contraseña de origen de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Configuración**.
5. En **Generar nueva clave de cifrado**, haga clic en **Aplicar**.

Mostrar una estadística de Lockbox

La estadística de Lockbox refleja el estado del Lockbox y si hay orígenes de eventos que lo usan. Hay una alarma asociada con la estadística del Lockbox que monitorea el estado del Lockbox. Se produce una condición de alarma cuando el Lockbox está en un estado No se encontró o Mensaje de error.

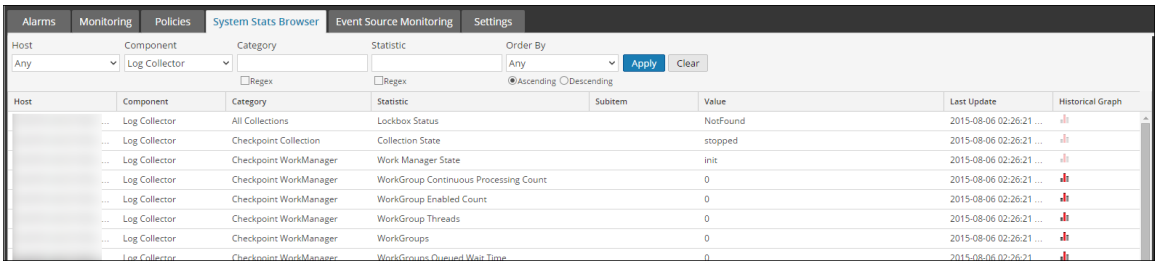
La estadística del Lockbox puede ser uno de los siguientes valores:

- *OK*
- *Not Required*
- *Not Found*
- *Error Message*

Para mostrar la estadística del Lockbox:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Navegador de estadísticas del sistema**.

En la siguiente figura se muestra un Lockbox que está en un estado **No se encontró**, el cual activa una condición de alarma.



Parámetros:

Parámetros de configuración de Lockbox

Configurar certificados

Este tema le enseña a agregar certificados.

Después de realizar este procedimiento, habrá agregado un certificado.

Volver a Procedimientos

Procedimiento

Para agregar un certificado:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Configuración**.
5. En el panel de opciones, seleccione **Certificados**.
6. Haga clic en en la barra de herramientas **Certificados**.
   Se muestra el cuadro de diálogo **Agregar certificado**.
7. Haga clic en **Navegar** y seleccione un certificado (***.PEM**) de la red.
8. Especifique una contraseña (si se requiere).

9. Haga clic en **Guardar**.

Parámetros

Parámetros de configuración de los certificados

Paso 3. Configurar orígenes de eventos en Security Analytics

Guía de configuración del protocolo de recopilación

Volver a Procedimientos

Use estas guías para configurar los protocolos de recopilación de los orígenes de eventos que tiene en su red empresarial.

- *Guía de configuración de la recopilación de AWS (CloudTrail)*
- *Guía de configuración de la recopilación de punto de comprobación*
- *Guía de configuración de archivo*

- *Guía de configuración de la recopilación de Netflow*
- *Guía de configuración de la recopilación de ODBC*
- *Guía de configuración de la recopilación de SDEE*
- *Guía de configuración de la recopilación de SNMP*
- *Configurar orígenes de eventos de syslog para Remote Collector*
- *Configurar filtros de eventos de syslog para Remote Collector*
- *Guía de configuración de la recopilación de VMware*
- *Guía de configuración de la recopilación de Windows*
- *Guía de configuración de Windows existente y NetApp*
- *Orígenes de eventos compatibles*

Agregar certificados y contraseñas

Este tema le enseña a agregar certificados.

Después de realizar este procedimiento, habrá agregado un certificado.

Volver a Procedimientos

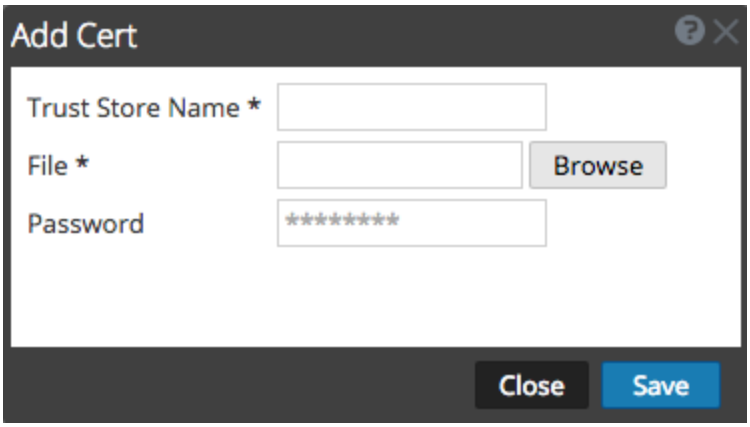
Procedimiento

Para agregar un certificado:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Configuración**.
5. En el panel de opciones, seleccione **Certificados**.
6. Haga clic en  en la barra de herramientas **Certificados**.
   Se muestra el cuadro de diálogo **Agregar certificado**.

   Nota: Asegúrese de que el certificado que agrega sea un certificado válido.

7. Haga clic en **Navegar** y seleccione un certificado (***.PEM**) de la red.
8. Especifique una contraseña (si se requiere).



9. Haga clic en **Guardar**.

Parámetros

Parámetros de configuración de los certificados

Importar, exportar y editar orígenes de eventos de manera masiva

En este tema, se explica cómo importar, exportar y editar orígenes de eventos de forma masiva.

Puede usar la opción de exportación en masa para exportar los detalles de orígenes de eventos de la configuración actual y almacenarlos. Estos datos se pueden importar en masa cuando se presenta un problema relacionado con la configuración actual y se necesitan los datos de orígenes de eventos que se tenían.

Puede usar la función de edición en masa cuando tiene múltiples orígenes de eventos que requieren una modificación específica. Puede seleccionar todos los orígenes y aplicar la opción de edición simultáneamente en ellos, lo cual evita tener que aplicarla origen por origen.

Después de realizar este procedimiento, habrá...

- Importado orígenes de eventos en masa.
- Exportado orígenes de eventos en masa.
- Editado orígenes de eventos en masa.

Volver a Procedimientos

Consulte también

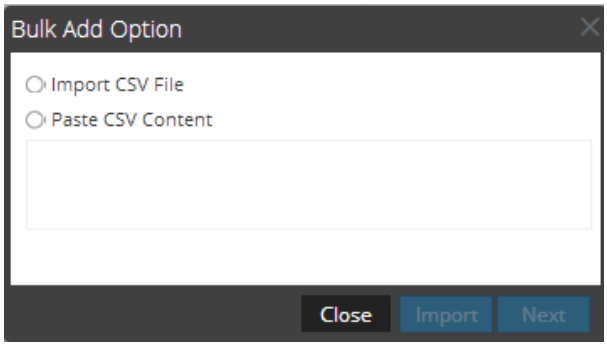
Están disponibles procedimientos similares en el módulo **Orígenes de eventos** (Administration > Orígenes de eventos). Para obtener detalles, consulte los siguientes temas en la *Guía de administración de orígenes de eventos*:

- **Importar orígenes de eventos**
- **Exportar orígenes de eventos**
- **Atributos de edición masiva de origen de evento**

Importar orígenes de eventos de forma masiva

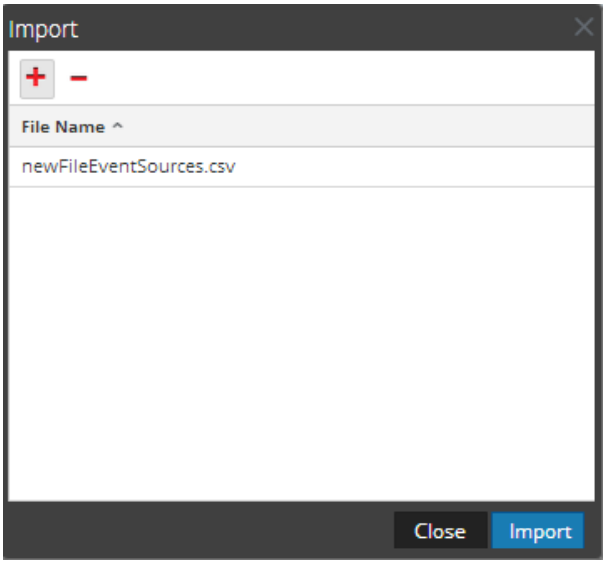
Para importar varios orígenes de eventos de una vez:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Seleccione la pestaña **Orígenes de evento** y elija **AWS (CloudTrail)**, **Punto de control**, **Archivo**, **Netflow**, **ODBC**, **SDEE**, **Syslog (solo para Remote Collectors)**, **VMware**, **Windows** y **Windows heredado** (SNMP no tiene una función de importación).
5. En la barra de herramientas del panel **Orígenes**, haga clic en **Importar origen**.
   Se muestra el cuadro de diálogo **Opción Adición en masa**.



6. Seleccione **Importar archivo CSV** o **Pegar contenido CSV**. Si selecciona:
   - Importar archivo CSV:
     a. Haga clic en **Siguiente**.
        Se muestra el cuadro de diálogo **Importar**.

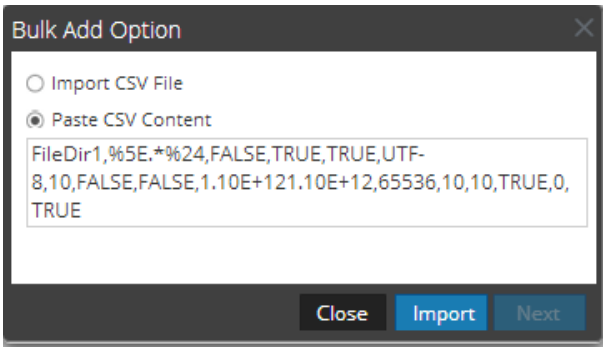
b. Haga clic en **Agregar** y seleccione un archivo **.csv** de la red.



c. Haga clic en **Importar**.
Los orígenes de eventos se agregan a la lista **Origen de evento**.

- Pegar contenido CSV:

a. Copie el contenido del archivo **.csv** y péguelo en el cuadro de diálogo.

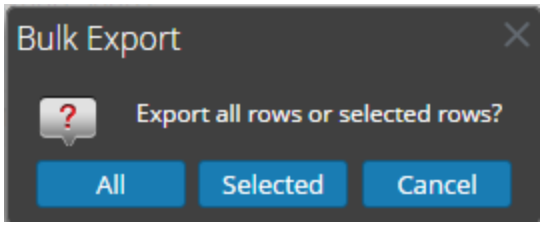


b. Haga clic en **Importar**.
Los orígenes de eventos se agregan a la **lista Origen de evento**.

Exportar orígenes de eventos de forma masiva

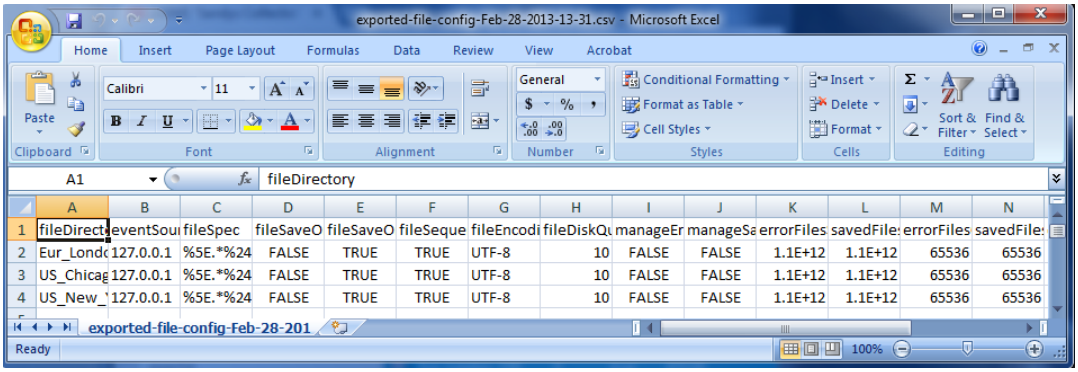
- En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
- En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
- Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.

- Seleccione la pestaña **Orígenes de evento** y elija **AWS (CloudTrail)**, **Punto de control**, **Archivo**, **Netflow**, **ODBC**, **SDEE**, **VMware**, **Windows** y **Windows heredado** (SNMP no tiene una función de exportación).
- En el panel **Orígenes**, seleccione uno o varios orígenes de eventos y haga clic en **Exportar origen**.
  Se muestra el cuadro de diálogo **Exportación masiva**.



- Si selecciona:
  - **Todo**, Security Analytics exporta todos los orígenes de eventos a un archivo CSV con registro de fecha y hora.
  - **Seleccionado**, Security Analytics exporta el o los orígenes de eventos que seleccionó a un archivo CSV con registro de fecha y hora.
  - **Cancelar**, Security Analytics cancela la exportación.

    El archivo CSV con registro de fecha y hora (por ejemplo, **exported-file-config-Feb-28-2013-13-31.csv**) con los orígenes de eventos que seleccionó en la lista.

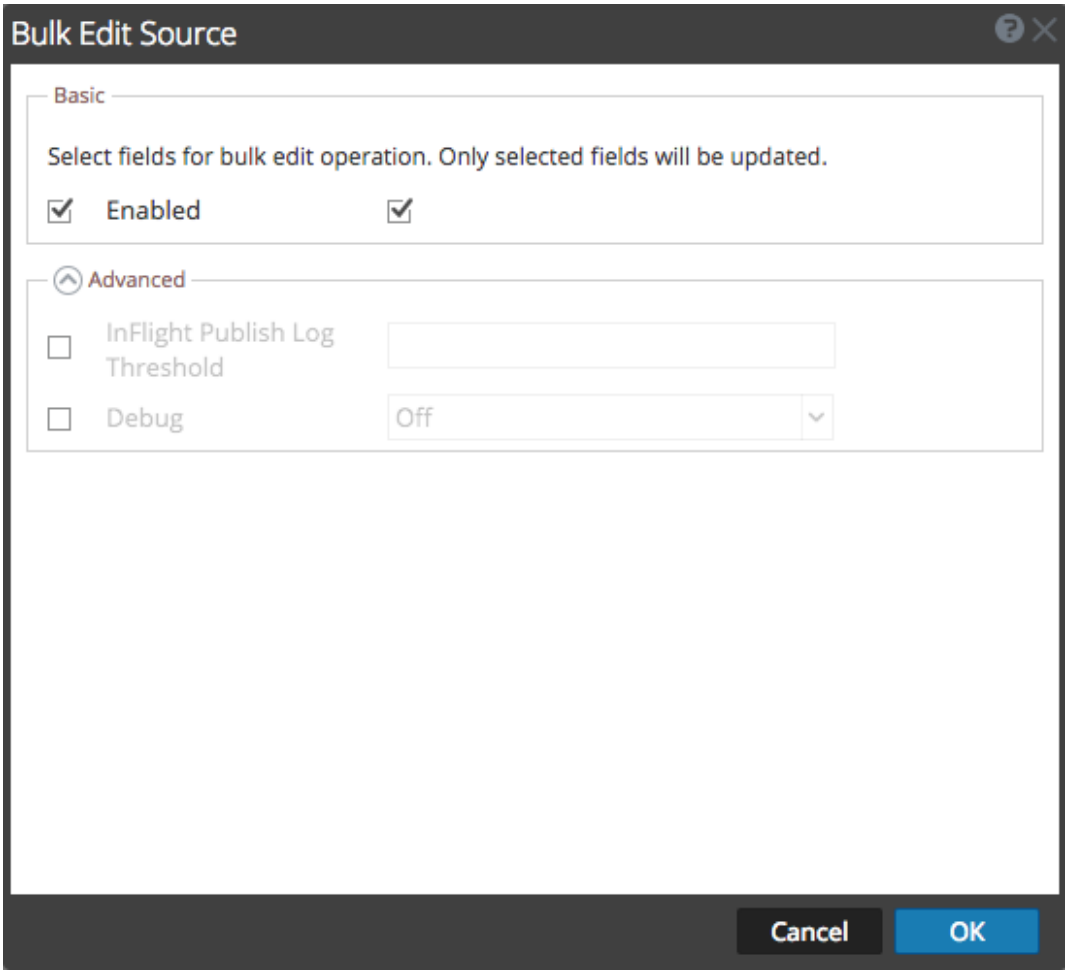


Editar orígenes de eventos de forma masiva

Para editar varios orígenes de eventos de una vez:

1. En la pestaña **Orígenes de evento del Log Collector**, seleccione **AWS (CloudTrail)**, **Punto de control**, **Archivo**, **Netflow**, **ODBC**, **SDEE**, **Syslog**, **VMware**, **Windows** o **Windows heredado** (SNMP no tiene una función de edición).

2. En el panel **Orígenes**, seleccione varios orígenes de eventos y haga clic en (ícono de edición).
   Se muestra el cuadro de diálogo **Edición masiva** correspondiente al origen de eventos seleccionado. La siguiente figura es un ejemplo del cuadro de diálogo **Edición en masa de origen** para los parámetros del origen de eventos de archivo.



3. Seleccione la casilla de verificación a la izquierda de los campos que desea modificar (por ejemplo, **Depurar**).
4. Modifique los parámetros seleccionados (por ejemplo, cambie Depurar de **Desactivado** a **Activado**).
5. Haga clic en **Aceptar**.
   Security Analytics aplica el mismo cambio de valores de parámetros a todos los orígenes de eventos seleccionados.

Parámetros

AWS (CloudTrail)
Punto de comprobación
Origen de eventos de archivo
Flujo de red
Open Database Connectivity (ODBC)
SDCC
Syslog
VMware
Windows

Probar conexiones de orígenes de eventos de manera masiva

En este tema, se explica cómo importar, exportar y editar orígenes de eventos de forma masiva.

Puede usar la opción de exportación en masa para exportar los detalles de orígenes de eventos de la configuración actual y almacenarlos. Estos datos se pueden importar en masa cuando se presenta un problema relacionado con la configuración actual y se necesitan los datos de orígenes de eventos que se tenían.

Puede usar la función de edición en masa cuando tiene múltiples orígenes de eventos que requieren una modificación específica. Puede seleccionar todos los orígenes y aplicar la opción de edición simultáneamente en ellos, lo cual evita tener que aplicarla origen por origen.

Después de realizar este procedimiento, habrá...

- Importado orígenes de eventos en masa.
- Exportado orígenes de eventos en masa.
- Editado orígenes de eventos en masa.

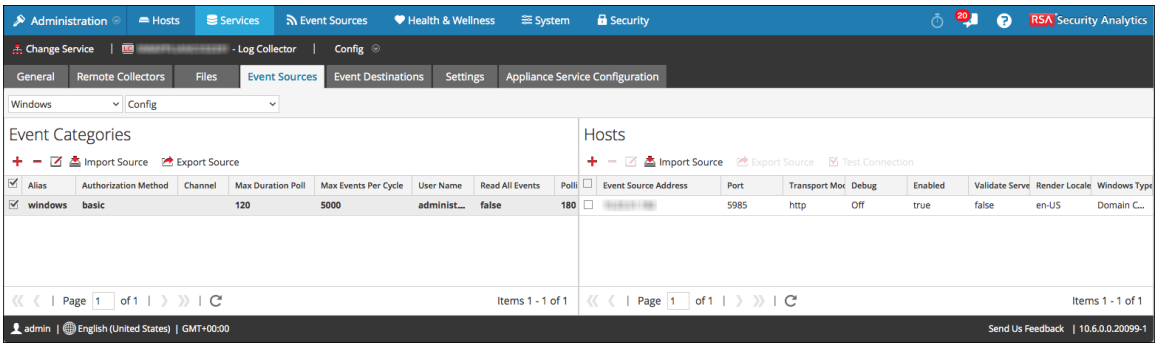
Volver a Procedimientos

Procedimiento

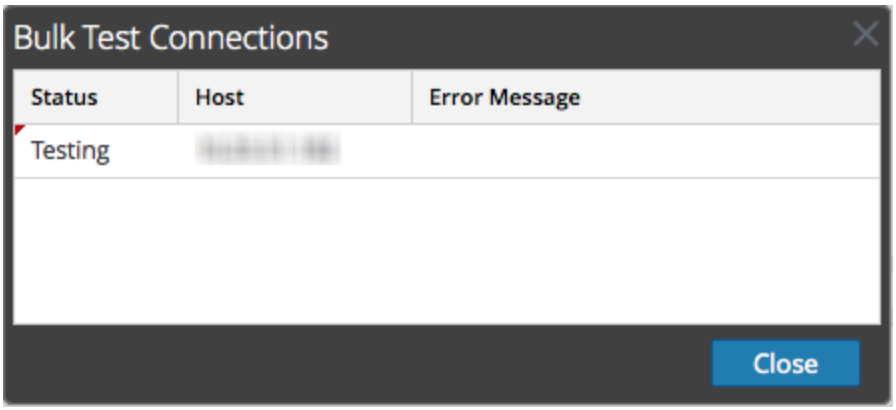
Para probar varias conexiones de orígenes de eventos simultáneamente:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Seleccione la pestaña **Orígenes de evento** y elija **Plug-ins**, **ODBC** y **Windows** (los otros protocolos no tienen una función de prueba en masa de conexiones).
5. Seleccione uno o más:

- orígenes en el panel **Orígenes** para **Plug-ins** u **ODBC**
- hosts en el panel **Hosts** para **Windows**
  El botón **Probar conexión** está habilitado.



6. Haga clic en Test Connection.
   Se muestra el cuadro de diálogo **Prueba en masa de conexiones**, en el cual aparece el estado actual de la prueba para cada origen. El estado puede ser esperando, probando, aprobado o fallido.
   Si decide cerrar la prueba antes de que se complete, la prueba se detiene y se cierra el cuadro de diálogo **Prueba en masa de conexiones**.
   Una vez que se complete la prueba, los resultados se muestran en el cuadro de diálogo **Prueba en masa de conexiones**.



Parámetros

AWS (CloudTrail)
Open Database Connectivity (ODBC)
Windows

Configurar orígenes de eventos de syslog para Remote Collector

En este tema se indica cómo configurar los orígenes de eventos de syslog para el Log Collector.

Después de realizar este procedimiento, habrá:

- Configurado un origen de eventos de syslog
- Modificado un origen de eventos de syslog

> **Precaución:** No configure la recopilación de syslog para los Log Collectors locales. Solo debe configurar la recopilación de syslog para los Remote Collectors.

Volver a Procedimientos

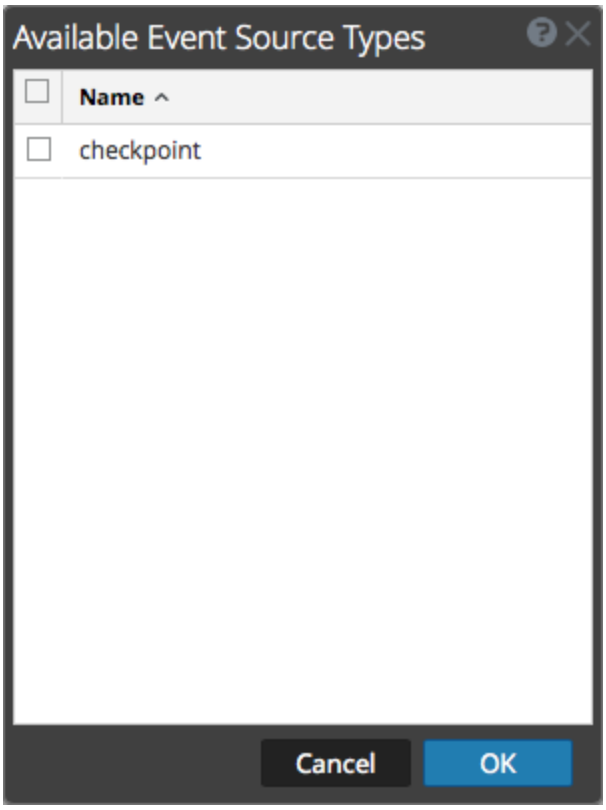
Procedimientos

Configurar un origen de eventos de syslog

> **Nota:** El Log Decoder recopila mensajes de syslog directamente desde los orígenes de eventos del sitio local. Esto significa que solo debe completar los siguientes procedimientos si está recopilando mensajes de syslog desde un sitio remoto mediante un Remote Collector.

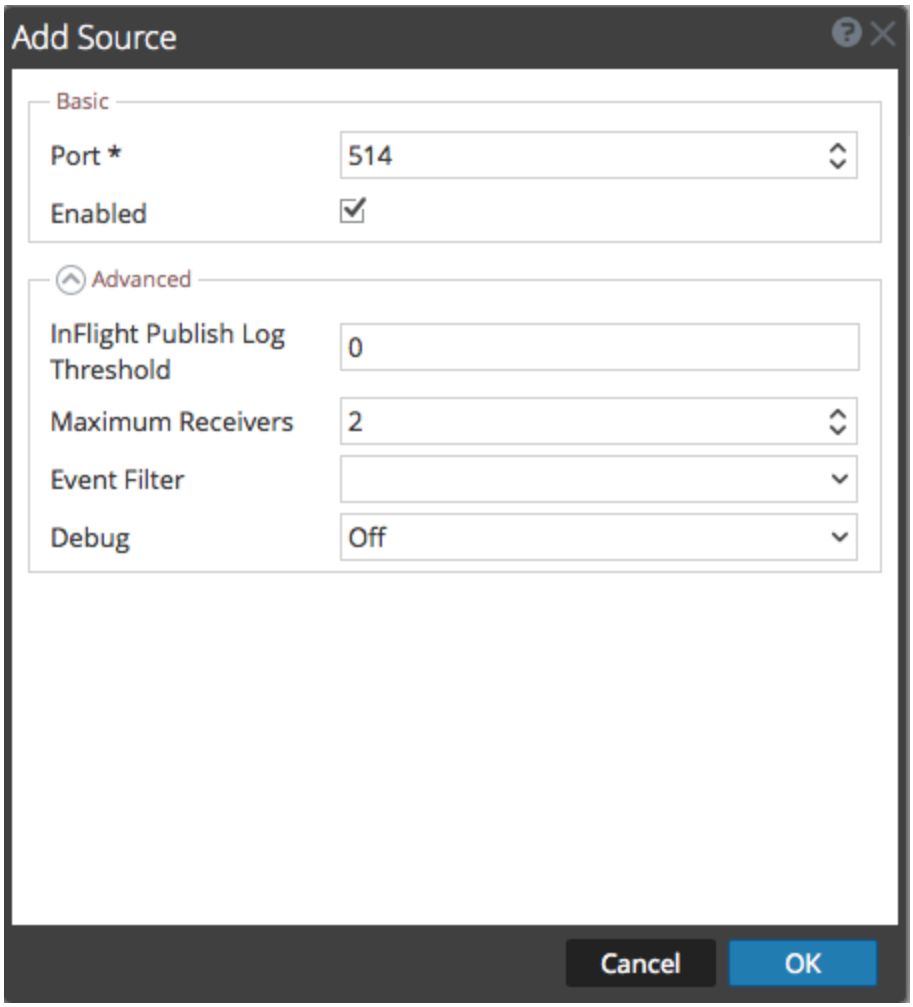
Para configurar un origen de eventos de syslog:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Syslog/Configurar** en el menú desplegable.
   En el panel **Categorías de evento** se muestran los orígenes de eventos de syslog que están configurados, si los hay.
5. En la barra de herramientas del panel **Categorías de evento**, haga clic en  .
   Se muestra el cuadro de diálogo **Tipos de origen de evento disponibles**.

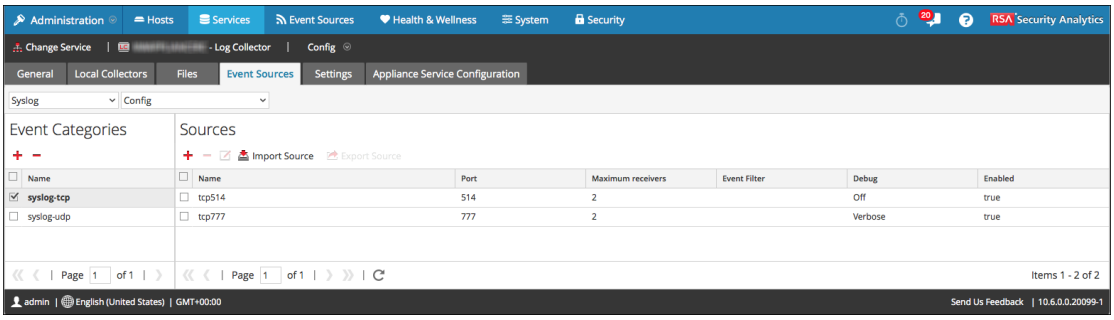


6. Seleccione un tipo de origen de eventos (por ejemplo, **syslog-tcp**) y haga clic en **Aceptar**.
   El tipo de origen de eventos recién agregado se muestra en el panel **Categorías de evento**.

7. Seleccione el nuevo tipo en el panel **Categorías de evento** y haga clic en + en la barra de herramientas del panel **Orígenes**.
   Se muestra el cuadro de diálogo **Agregar origen**.



8. Modifique cualquiera de los ajustes de los parámetros y haga clic en **Aceptar**.
   El origen de eventos de syslog se agrega al panel **Orígenes**.

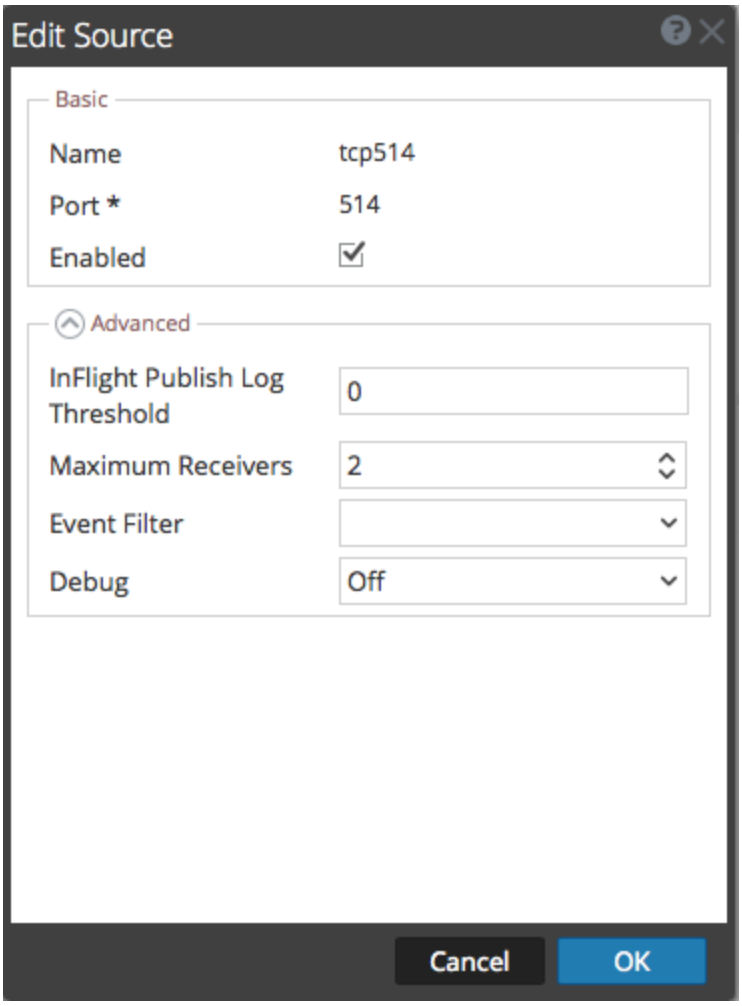


Modificar un origen de eventos de syslog

Para modificar un origen de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Syslog/Configurar** en el menú desplegable.
5. Seleccione un tipo de origen de eventos (por ejemplo, **syslog-tcp**) y haga clic en **Aceptar**.
6. En el panel **Origen**, seleccione un origen de eventos (por ejemplo, **tcp514**) y haga clic en .

   Se muestra el cuadro de diálogo **Editar origen**.



5. Modifique los parámetros que necesiten cambios y haga clic en **Aceptar**.
   Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado

Parámetros

Parámetros de configuración del origen de eventos de syslog para Remote Collector

Configurar filtros de eventos de syslog para Remote Collector

En este tema se indica cómo crear y mantener filtros de eventos para el protocolo de recopilación de syslog.

Después de realizar este procedimiento, habrá:

- Configurado un filtro de eventos de syslog
- Modificado reglas de filtros de eventos de syslog.

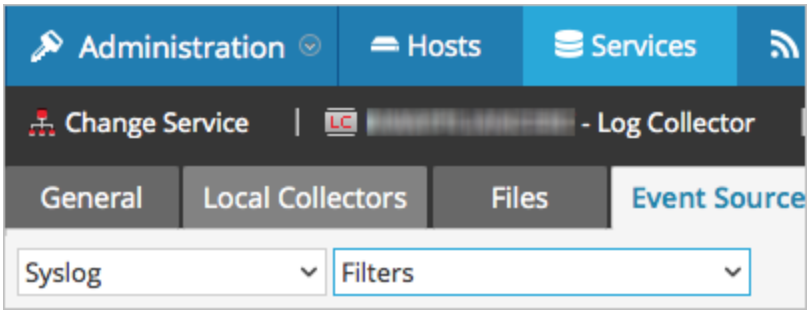
Precaución: No configure la recopilación de syslog para los Log Collectors locales. Solo debe configurar la recopilación de syslog para los Remote Collectors. Consulte Acceder a Local y Remote Collectors para obtener información de configuración adicional.

Volver a Procedimientos

Configurar un filtro de eventos de syslog

Para configurar un origen de eventos de archivo:

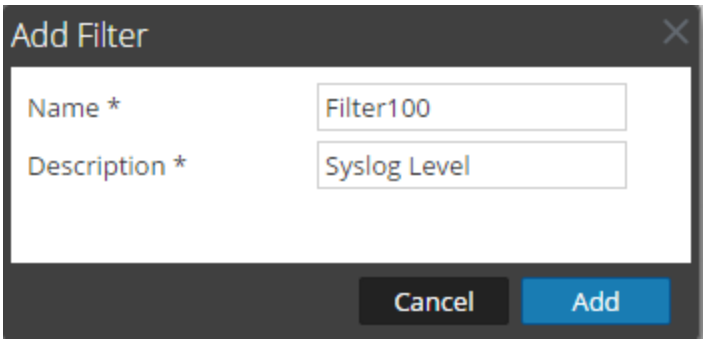
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Syslog/Filtros** en los menús desplegables.



   En la vista **Filtros** se muestran los filtros de **Syslog** que están configurados, si los hay.

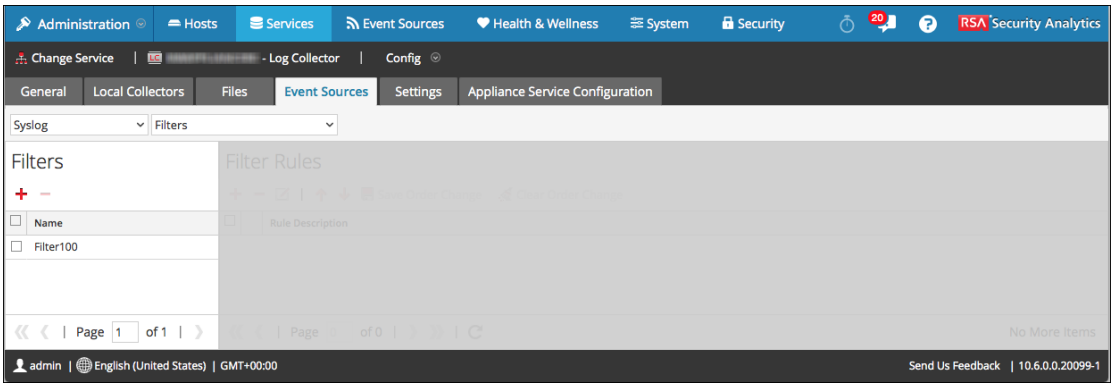
5. En la barra de herramientas del panel **Filtros**, haga clic en  .

   Se muestra el cuadro de diálogo **Agregar filtro**.



6. Ingrese un nombre y una descripción para el nuevo filtro y haga clic en **Agregar**.

   El nuevo filtro se muestra en el panel **Filtro**.

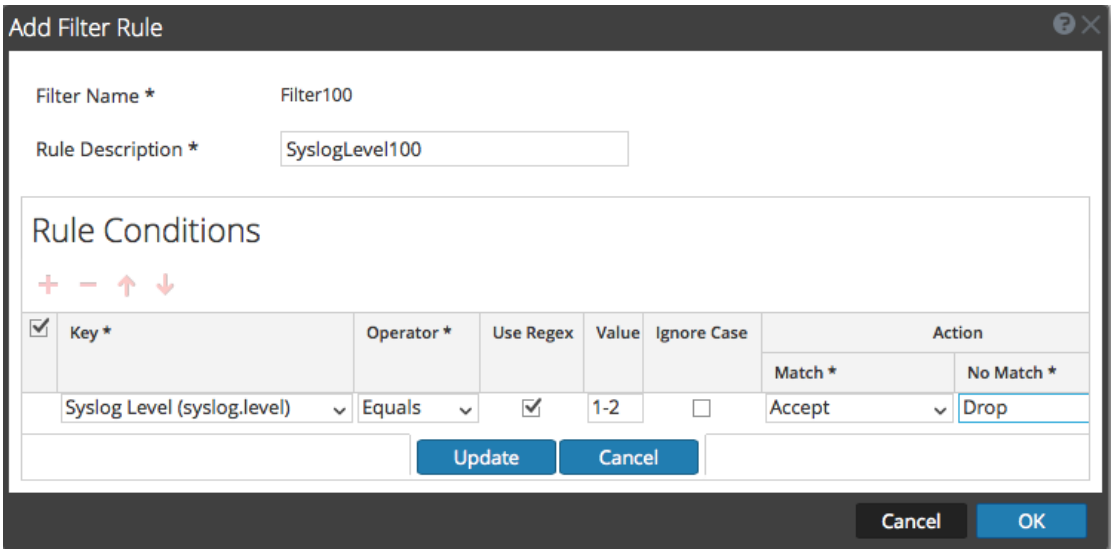


7. Seleccione el nuevo filtro en el panel **Filtros** y haga clic en + en la barra de herramientas del panel **Filtrar reglas**.

   Se muestra el cuadro de diálogo **Agregar regla de filtro**.

8. Haga clic en + bajo **Condiciones de la regla**.

9. Agregue los parámetros para esta regla y haga clic en **Actualizar** > **Aceptar**.



Security Analytics actualiza el filtro con la regla que definió.

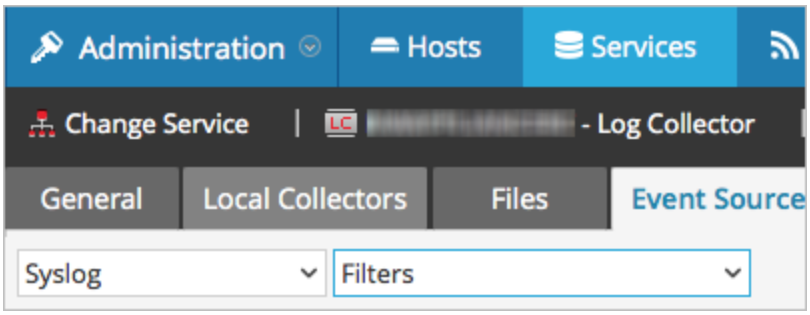
Campo	Descripción
Clave	Los valores válidos son: • Nivel de syslog • Dirección IP de origen • Evento crudo
Operador	Los valores válidos son: • Contiene • Es igual a
Usar regex	Opcional. Puede seleccionar esta opción si desea usar regex.
Valor	El valor depende del valor de la clave que seleccionó. Por ejemplo, si elige **Nivel de syslog** para Clave, el valor será un número que denota el nivel de syslog.
Omitir mayúsculas y minúsculas	Opcional. Seleccione esta opción para no hacer caso de la distinción de mayúsculas de minúsculas.

Campo	Descripción
Acción	Si hay una coincidencia, puede elegir las acciones aceptar, descartar, condición siguiente o regla siguiente. Si no hay una coincidencia, puede elegir las acciones aceptar, descartar, condición siguiente o regla siguiente.

Modificar reglas de filtro

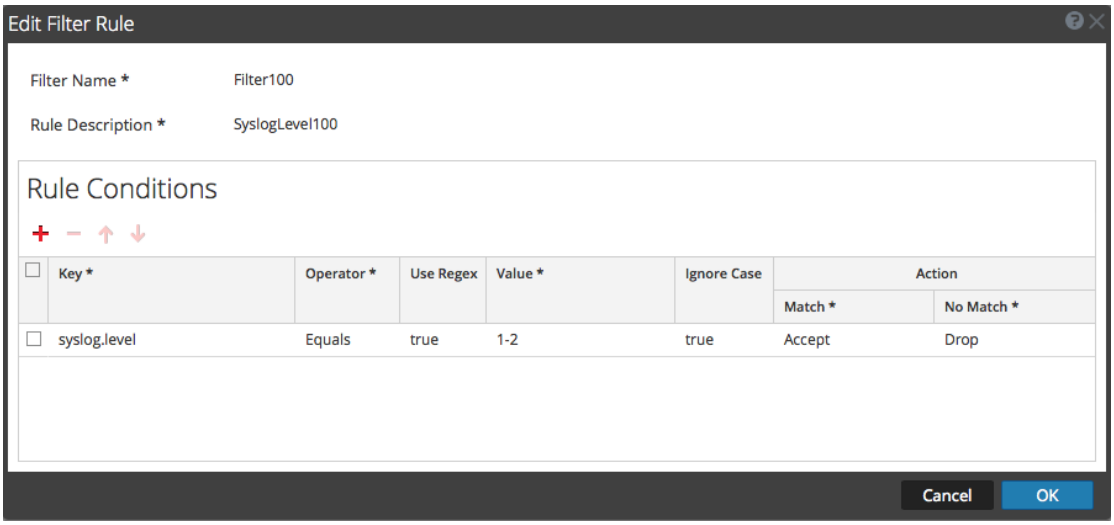
Para modificar un origen de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Syslog/Filtros** en el menú desplegable.

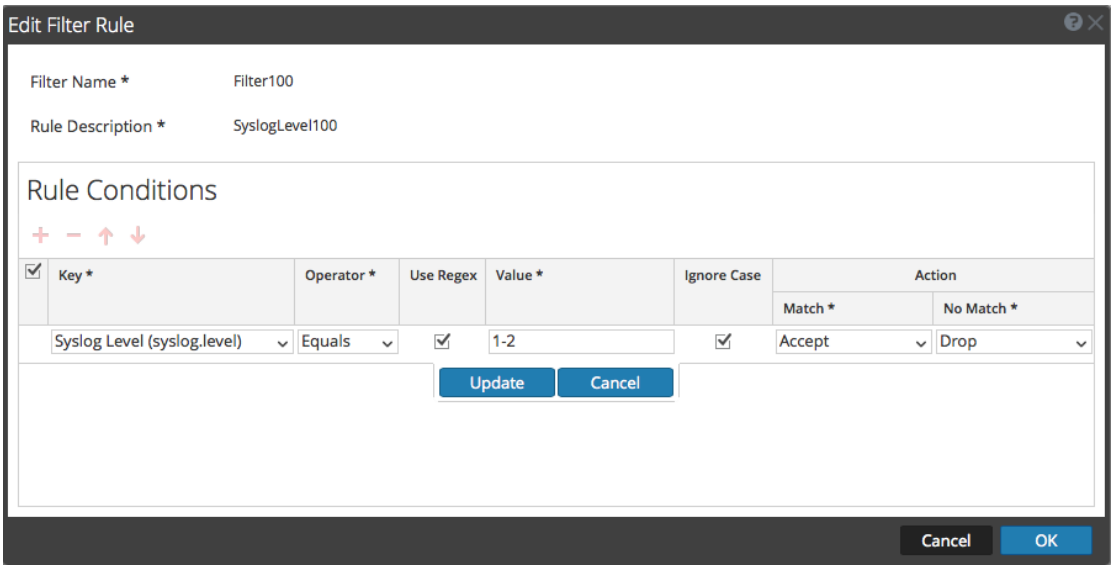


5. En la vista **Filtros** se muestran los filtros de **Syslog** que están configurados, si los hay.
6. En la lista **Filtrar reglas**, seleccione una regla y haga clic en .

   Se muestra el cuadro de diálogo **Editar regla de filtro**.



7. Seleccione la condición de la regla que desea modificar.



8. Modifique los parámetros de condición que necesiten cambios y haga clic en **Actualizar** > **Aceptar**.

Security Analytics aplica los cambios en los parámetros de condición a la regla de filtro seleccionada.

Parámetros

Vista Filtros de eventos de syslog para Remote Collector

Paso 4. Configurar los orígenes de eventos para enviar eventos a Security Analytics

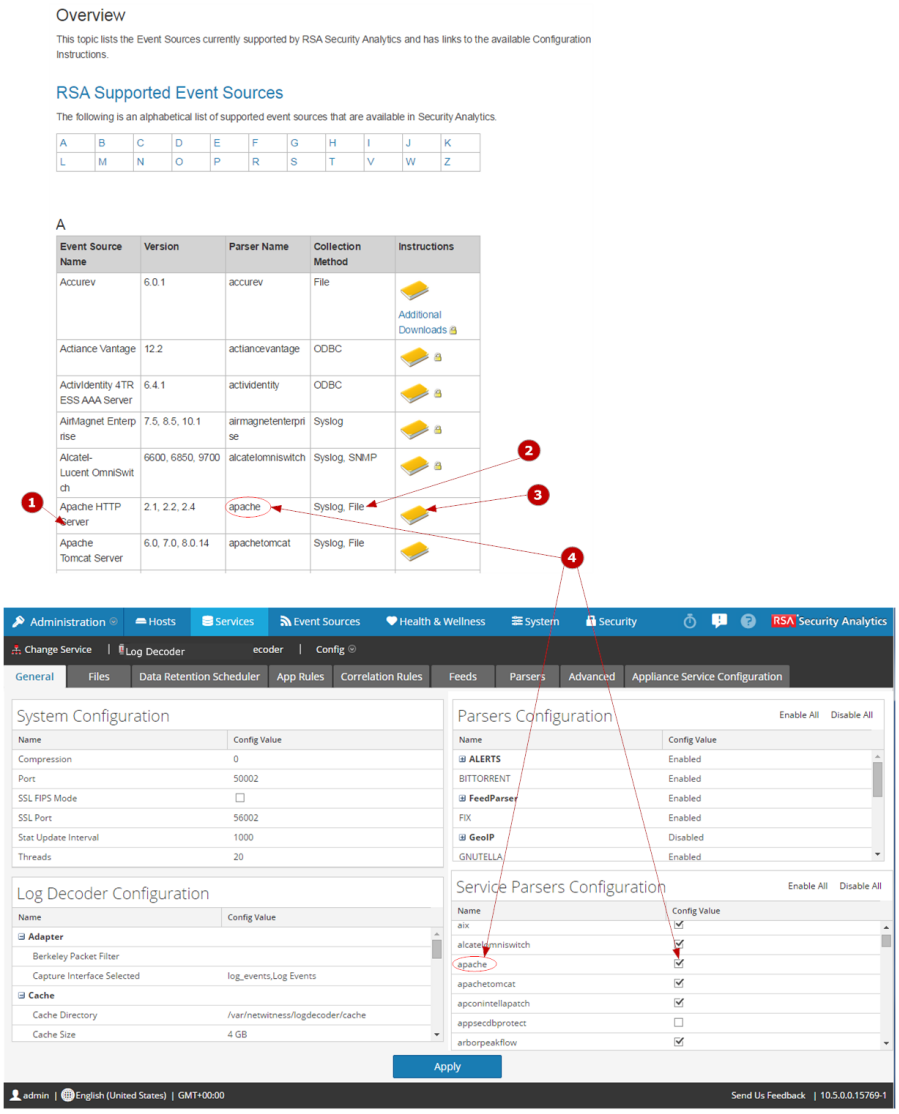
Descripción general

En este tema se incluye una tabla con vínculos a las instrucciones de configuración de cada origen de eventos compatible con Security Analytics.

Orígenes de eventos compatibles de RSA Security Analytics

Volver a Procedimientos

En la siguiente ilustración se muestra la primera sección de la tabla que será parte del contenido insertado en esta guía.



1. Busque el nombre del origen de eventos (por ejemplo, **servidor Apache HTTP**).
2. Verifique que sea compatible con el protocolo de recopilación (por ejemplo, el protocolo de recopilación de **archivos**).
3. Haga clic en  para ver las instrucciones de configuración del origen de eventos.
4. Verifique que haya descargado el analizador correcto (por ejemplo, apache) desde LIVE a Log Decoder y que lo haya habilitado.

Paso 5. Iniciar y detener servicios para los protocolos configurados

En este tema se indica cómo iniciar un servicio de recopilación y cómo habilitar el inicio automático de uno de estos servicios.

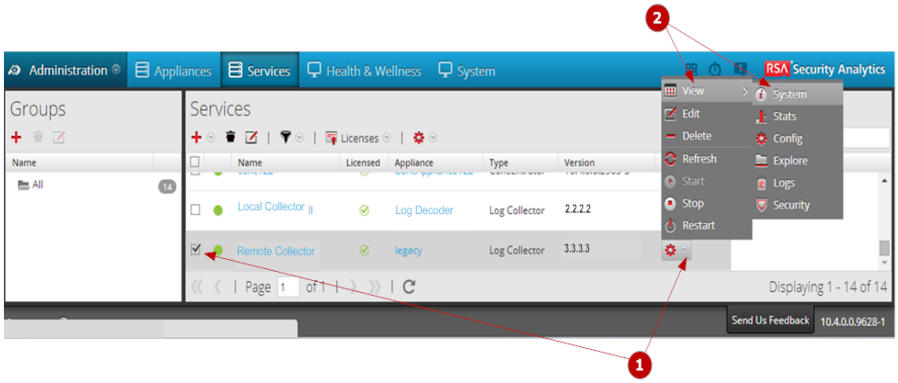
Contexto

Si un servicio de recopilación se detiene, puede ser necesario iniciarlo nuevamente o tal vez desee habilitar su inicio automático.

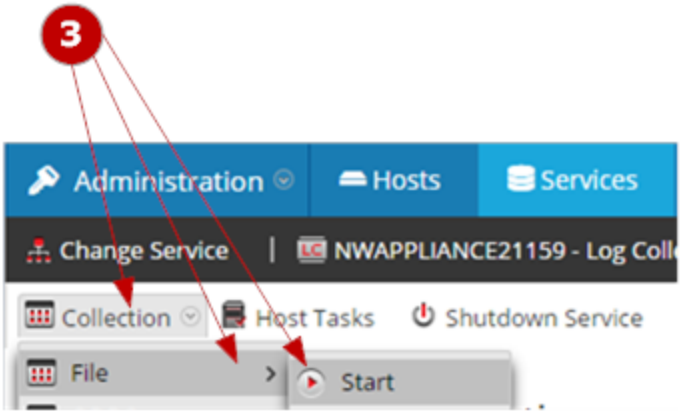
Iniciar un servicio de recopilación

Volver a Procedimientos

En la siguiente figura se muestra cómo iniciar un servicio de recopilación.



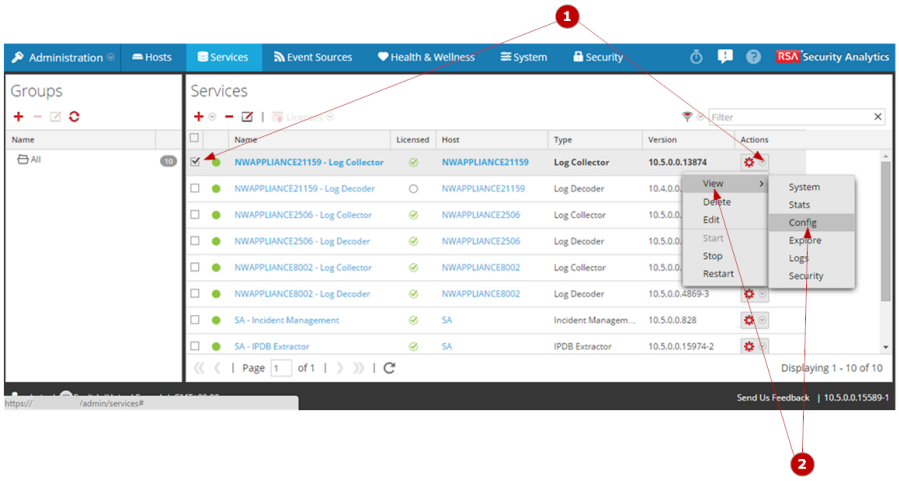
1. Seleccione un servicio Log Collector y haga clic en  bajo **Acciones**.
2. Haga clic en **Ver > Sistema**.



Haga clic en **Recopilación** > ***servicio*** (por ejemplo, **Windows heredado**) y, a continuación, haga clic en **Iniciar**.

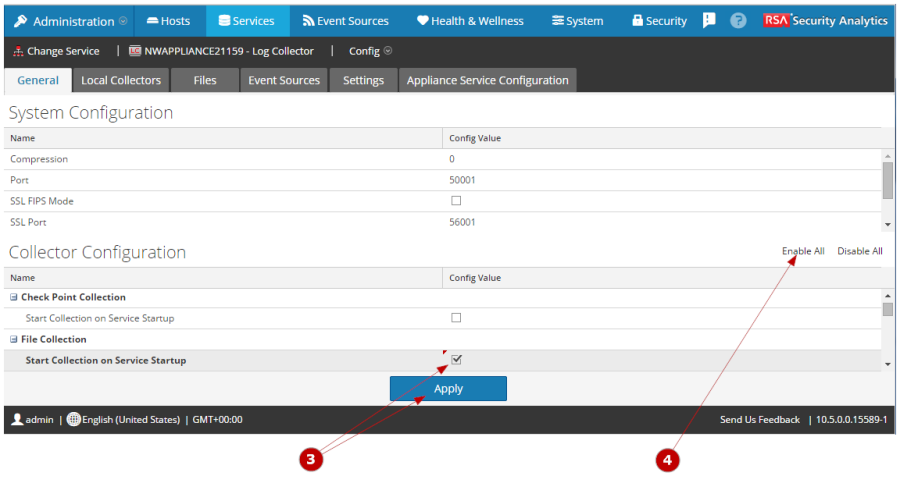
Habilitar el inicio automático de servicios individuales

En la siguiente figura se muestra cómo habilitar el inicio automático de un servicio de recopilación.



1 Seleccione un servicio Log Collector y haga clic en ⌄ bajo **Acciones**.

2 Haga clic en **Ver** > **Configuración**.



3 Seleccione la casilla de verificación **Iniciar la recopilación en el arranque del servicio** para un servicio de recopilación (por ejemplo, **Windows heredado**) y haga clic en **Aplicar**.

4 (Opcional) Puede hacer clic en **Activar todo** y, a continuación, en **Aplicar** para establecer el inicio de cada servicio de recopilación en el arranque del servicio Log Collector.

Paso 6. Verificar que la recopilación de registros esté funcionando

En este tema se indica cómo verificar la correcta configuración de la recopilación de registros.

Debe verificar que la recopilación de registros esté configurada correctamente; de lo contrario, podría no funcionar

Procedimiento

Volver a Procedimientos

Los siguientes métodos permiten verificar que la recopilación de registros esté funcionando.

- Verifique que haya actividad de evento en la pestaña **Monitoreo de orígenes de eventos** de la vista **Administration > Estado y condición**.
- Verifique que haya analizadores en el campo **device.type** de la columna **Detalles** de **Investigation > vista Eventos** para el protocolo de recopilación que configuró.

Consulte los pasos para verificar que el protocolo esté configurado correctamente en la guía de configuración de cada protocolo de recopilación.

Referencia: Interfaz de parámetros de configuración

La vista **Configuración del servicio Log Collector** es la vista en la cual se mantienen todos los parámetros de Log Collector.

Pestaña **General** = Parámetros de alto nivel que rigen la operación del servicio Log Collector y cada protocolo de recopilación.

Orígenes de eventos = Orígenes de eventos compatibles (punto de comprobación, archivo, ODBC, Netflow, plug-ins, SDEE, SNMP, Syslog, VMware, Windows y Windows existente)

Pestaña Configuración = Configuración de seguridad de lockbox y administración de certificados.

Consulte las pestañas **Archivos** y **Configuración del servicio Appliance** en la *Guía de configuración de hosts y servicios* para obtener información sobre los parámetros de configuración en estas pestañas.

Pestaña General de la recopilación de registros

En este tema se presentan las funciones de la vista Configuración de servicios > pestaña General que se relacionan específicamente con Log Collector.

El administrador de RSA Security Analytics debe configurar orígenes de eventos para enviar registros a los recopiladores. Cuando los orígenes de eventos están configurados, sondean orígenes de eventos, recuperan registros y envían los datos de eventos a Security Analytics. En la vista Configuración de servicios > pestaña General, puede ejecutar las siguientes acciones:

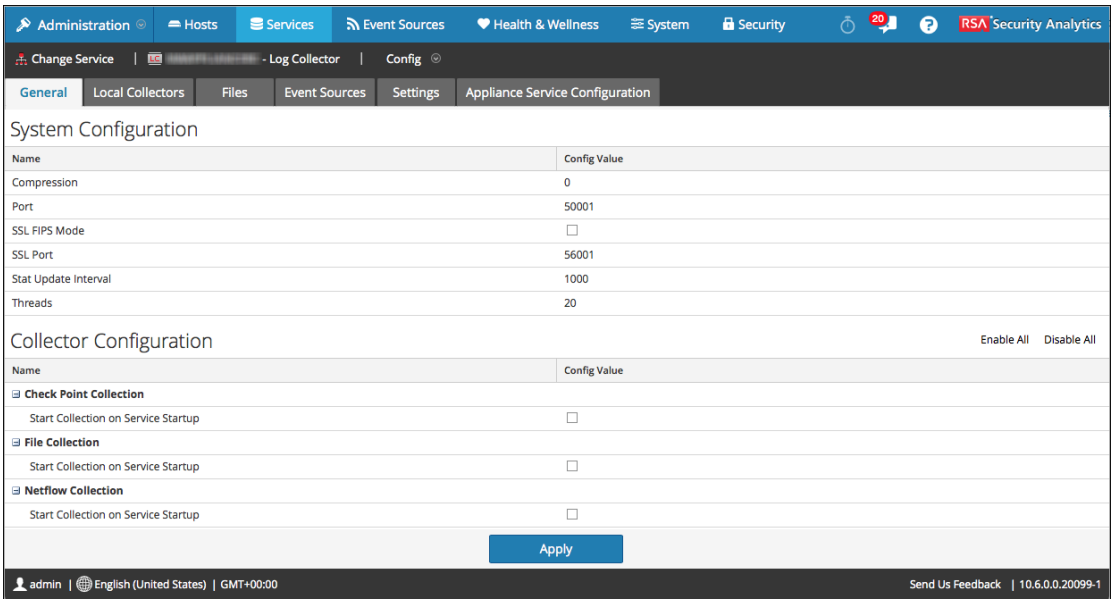
- Ajuste los parámetros de configuración del sistema, si es necesario, en el panel Configuración del sistema.
- Configure el inicio automático de la recopilación de registros por tipo de origen de eventos en el panel Configuración de Log Collector:
  - Punto de comprobación
  - Archivo
  - Flujo de red
  - ODBC
  - Plug-ins (AWS CloudTrail)
  - SDEE
  - SNMP
  - VMware

- Windows
- Windows existente

Para acceder a la pestaña General de la recopilación de registros:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.

   La vista **Configuración del servicio** se muestra con la pestaña **General** de Log Collector abierta.



Panel Configuración del sistema

El panel Configuración del sistema administra la configuración de un servicio de Security Analytics. Cuando un servicio se agrega por primera vez, se aplican valores predeterminados. Puede editar estos valores para ajustar el rendimiento. Consulte la pestaña **General** para obtener una descripción de estos parámetros.

La sección Configuración del sistema tiene estos parámetros.

Parámetro	Descripción
Compresión	La cantidad mínima de bytes que se deben transmitir por respuesta antes de la compresión. Si se define en 0, se deshabilita la compresión. El valor predeterminado es **0**. Un cambio en el valor se aplica de inmediato en todas las conexiones subsiguientes.
Puerto	El puerto en el cual escucha el servicio. Los puertos son: • 50001 para Log Collectors • 50002 para Log Decoders • 50003 para Brokers • 50004 para Decoders • 50005 para Concentrators • 50007 para otros servicios
Modo SSL FIPS	Cuando se habilita (**activado**), la seguridad de la transmisión de datos se administra mediante el cifrado de información y la entrega de autenticación mediante certificados SSL. El valor predeterminado es **off**.
Puerto SSL	El puerto SSL de Security Analytics Core en el cual escucha el servicio. Los puertos son: • 56001 para Log Collectors • 56002 para Log Decoders • 56003 para Brokers • 56004 para Decoders • 56005 para Concentrators • 56007 para otros servicios
Intervalo de actualización de estadísticas	La cantidad de milisegundos entre las actualizaciones de estadísticas del sistema. Los números más bajos permiten actualizaciones frecuentes y pueden retrasar otros procesos. El valor predeterminado es **1,000**. Un cambio en el valor se aplica de inmediato.

Parámetro	Descripción
Hilos	El número de hilos de ejecución en el pool de hilos de ejecución para manejar solicitudes entrantes. Si se define en 0, se permite que el sistema decida. El valor predeterminado es 15. Un cambio se aplica tras el reinicio del servicio.

Panel Configuración de recopilador

El panel Configuración de recopilador proporciona una manera de activar el inicio automático de recopilación de registros por tipo de origen de eventos: Punto de comprobación, archivo, ODBC, SDEE, SNMP, Syslog, VMware y Windows.

Nombre	Valor de configuración
Activar todo Desactivar todo	Activa o desactiva la recopilación automática de todos los tipos de eventos. • **Activar todo** = inicia la recepción de eventos y la recopilación de registros para todos los tipos de evento cuando se inicia el servicio Log Collector. • **Desactivar todo** = (valor predeterminado) no recibe datos de eventos para ningún tipo de evento hasta que usted inicia explícitamente la recopilación.
Iniciar la recopilación en el arranque del servicio	Habilita el inicio automático, por tipo de origen de eventos, de la recopilación de registros cuando se inicia el servicio Log Collector. Los valores válidos son: • Seleccionado = inicia la recopilación de registros cuando se inicia el servicio Log Collector. • No seleccionado = (predeterminado) no recopila datos de eventos hasta que usted inicia explícitamente la recopilación.
Aplicar	Haga clic en Aplicar para guardar los cambios realizados en los valores de los parámetros.

Tareas

Consulte la *Guía de introducción a la recopilación de registros* para obtener más información acerca de la habilitación o la deshabilitación del inicio automático de la recopilación o del inicio y la detención de protocolos de recopilación de registros.

Pestaña Destinos de evento de la recopilación de registros

Use la pestaña Destinos de evento de la vista Configuración del servicio de recopilación de registros para configurar el destino de los datos de eventos que recopila el Log Collector:

- Log Decoders
- Feed de identidad

Requisitos previos

Debe implementar la siguiente configuración para crear un feed de identidad.

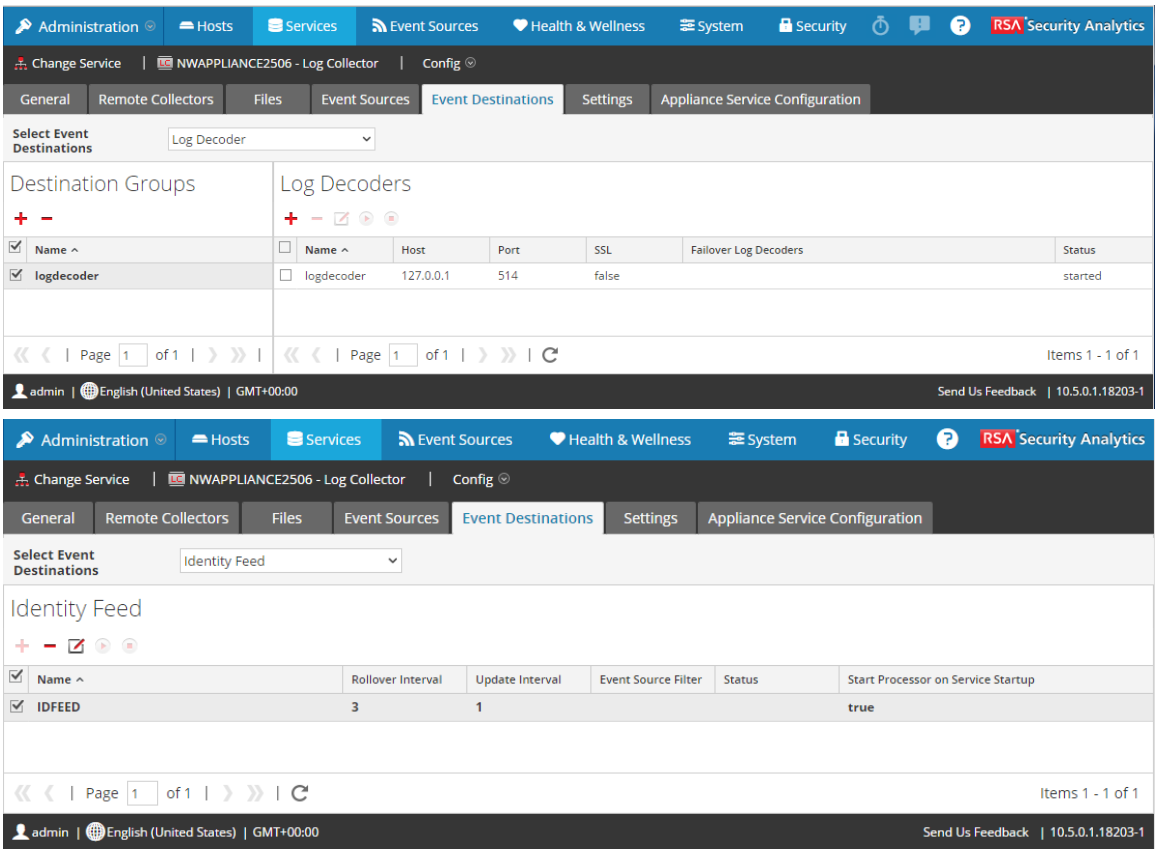
- Un servicio Log Collector con un procesador de eventos de feed de identidad
- Un servicio Log Collector con la recopilación de Windows configurada y habilitada

Nota: Consulte el tema Crear un feed de identidad de la Guía de administración de recursos de Live para obtener más información sobre cómo crear e investigar acerca de un feed de identidad.

El permiso requerido para acceder a esta vista es Administrar servicios.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Destinos de evento**.
5. En el menú desplegable **Seleccionar destinos de evento**:
   - Seleccione **Log Decoder** para configurar destinos de Log Decoder para los datos de eventos que recopila el Log Collector.

     Nota: Debe seleccionar un servicio Log Decoder en el cuadro de diálogo Agregar destino de Log Decoder, pero el resto de la configuración se realiza automáticamente.
   - Seleccione **Feed de identidad** para configurar un destino de feed de identidad para los datos de eventos que recopila Log Collector.



Parámetros de la recopilación de registros

La vista Configuración de la recopilación de registros permite mantener todos los parámetros de la recopilación de registros.

Pestaña Orígenes de evento de la recopilación de registros

En este tema se presentan los parámetros de configuración de servicios disponibles en la pestaña Orígenes de evento de la vista Configurar del servicio de recopilación de registros.

Use la pestaña Orígenes de evento de la vista Configuración del servicio Log Collector para configurar los orígenes de eventos de AWS (CloudTrail), Punto de comprobación, Archivo, ODBC, SDEE, Syslog, SNMP, VMware, Windows y Windows heredado.

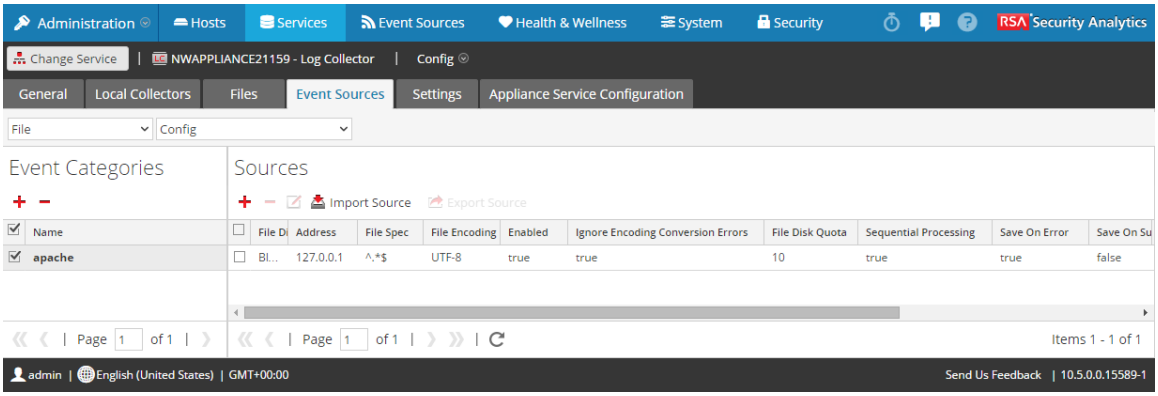
Para acceder a la pestaña Orígenes de evento de la recopilación de registros:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.

   La vista **Configuración del servicio** se muestra con la pestaña **General** de Log Collector

abierta.

4. Haga clic en la pestaña **Orígenes de evento**.



Características

La vista Archivo/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Menú Tipos de origen de evento

La pestaña Orígenes de evento de Log Collector tiene un menú desplegable de dos casillas en las cuales se selecciona el protocolo de recopilación y cualquier parámetro de apoyo para ese protocolo.

En la casilla izquierda, seleccione uno de los siguientes protocolos: Punto de comprobación, Archivo, ODBC, Plug-ins, SDEE, SNMP, SNMP, VMware, Windows y Windows existente.

En la casilla derecha, seleccione:

- Configurar para configurar los parámetros genéricos del origen de eventos para el tipo que seleccionó en la lista desplegable de la izquierda. Todos los paneles Config tienen una barra de herramientas con estas opciones:
  - Agregar, Editar y Eliminar
  - Importar (también Importar origen, Importar DSN)
  - Exportar (también Exportar origen, Exportar DSN)
- En el caso de ODBC, SNMP y Windows solamente:
  - Para la recopilación de ODBC, seleccione los DSN que se configurarán.
  - Para SNMP, Administrador de usuarios de SNMP v3

- Para configuración de Windows, dominios de Kerberos

- En el caso de Syslog solo en Remote Collectors, Syslog y Filtros

Cuando selecciona una opción, aparece un panel de configuración donde puede configurar los parámetros de recopilación de los orígenes de eventos. Los paneles de configuración de los orígenes de eventos tienen algunas diferencias leves y se describen por separado.

En el siguiente menú desplegable se muestran los parámetros de configuración seleccionados para Punto de comprobación.

Tareas

Paso 3. Configurar orígenes de eventos en Security Analytics

Vista Filtros de eventos de syslog para Remote Collector

En este tema se describen los parámetros de la vista Filtros de syslog.

Para acceder a la vista Filtros de syslog:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Syslog/Filtros** en los menús desplegables.
   En la vista **Filtros** se muestran los filtros de **Syslog** que están configurados, si los hay.

Características

En la siguiente tabla se describen los parámetros de la vista Filtros de syslog.

Campo	Descripción
Clave	Los valores válidos son: • Nivel de syslog • Dirección IP de origen • Evento crudo

Campo	Descripción
Operador	Los valores válidos son: • Contiene • Es igual a
Usar regex	Opcional. Puede seleccionar esta opción si desea usar regex.
Valor	El valor depende del valor de la clave que seleccionó. Por ejemplo, si elige Nivel de syslog para Clave, el valor será un número que denota el nivel de syslog.
Omitir mayúsculas y minúsculas	Opcional. Seleccione esta opción para no hacer caso de la distinción de mayúsculas de minúsculas.
Acción	Si hay una coincidencia, puede elegir las acciones aceptar, descartar, condición siguiente o regla siguiente. Si no hay una coincidencia, puede elegir las acciones aceptar, descartar, condición siguiente o regla siguiente.

Tareas

Procedimientos

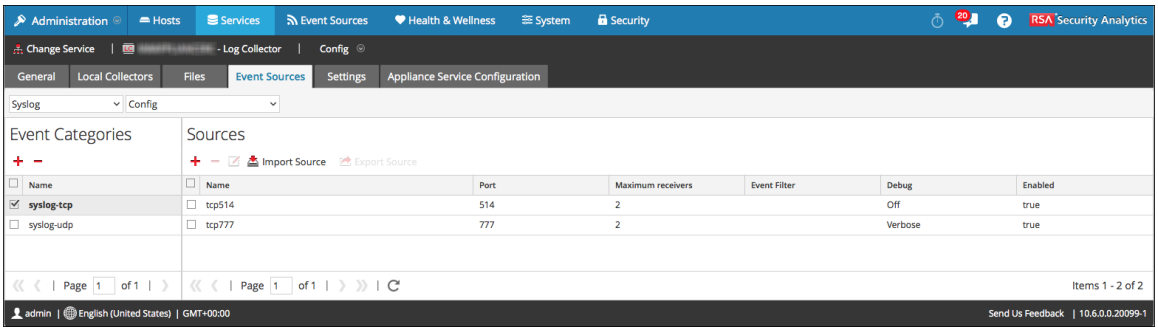
Parámetros de configuración del origen de eventos de syslog para Remote Collector

En este tema se describen los parámetros de la vista Orígenes de eventos de syslog.

Precaución: No configure la recopilación de syslog para los Log Collectors locales. Solo debe configurar la recopilación de syslog para los Remote Collectors.

Para acceder a la pestaña Orígenes de evento para un Remote Log Collector:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Syslog/Configurar** en el menú desplegable.



La vista **Syslog/Configuración** de la pestaña **Orígenes de evento** tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar los tipos de orígenes de eventos correspondientes.

Característica	Descripción
+	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
−	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.
☐	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de tipos de orígenes de eventos compatibles.

Característica	Descripción
☐	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.

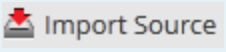
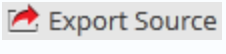
Característica	Descripción
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

Panel Orígenes

Use este panel para revisar, agregar, modificar y eliminar orígenes de eventos y sus parámetros para el tipo de origen de eventos que seleccionó en el panel Categorías de evento.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar origen, en el cual puede definir los parámetros para un host de firewall.
	Elimina el host que seleccionó.
	Abre el cuadro de diálogo Editar origen, en el cual puede editar los parámetros del origen de eventos seleccionado. Seleccione varios orígenes de eventos y haga clic en  para abrir el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar hosts de forma masiva desde un archivo de valores separados por comas (CSV). Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo .csv que contiene los parámetros de los hosts seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.

Cuadro de diálogo Agregar/Modificar orígenes

En este cuadro de diálogo, se agrega o se modifica un origen de eventos del tipo de origen de eventos seleccionado.

Característica	Descripción
Parámetros de origen	Muestra los parámetros completados con los valores predeterminados. Ingrese o modifique los valores apropiados.
Cancelar	Cierra el cuadro de diálogo sin agregar un origen de eventos ni guardar los valores de los parámetros del origen de eventos seleccionado.
OK	En el cuadro de diálogo Agregar orígenes, agrega el origen de eventos y sus parámetros. En el cuadro de diálogo Editar origen, aplica los cambios en los valores de los parámetros del origen de eventos seleccionado.

Parámetros de origen

En la siguiente tabla se proporcionan descripciones de los parámetros del origen.

Nombre	Descripción
	Básico
Puerto*	El puerto predeterminado es **514**.
Activado	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
Avanzado	
Número máximo de receptores	Cantidad máxima de recursos de receptor que se usan para procesar los eventos de syslog recopilados. El valor predeterminado es **2**.

Nombre	Descripción
Umbral de registro de publicación en trans-ferencia	Establece un umbral que, cuando se alcanza, Seguridad Analytics genera un mensaje de registro para ayudarle a resolver problemas de flujo de eventos. El umbral es el tamaño de los mensajes de eventos de syslog que fluyen actualmente desde el origen de eventos a Security Analytics. Los valores válidos son: • **0** (valor predeterminado): deshabilita el mensaje de registro • **Entre 100 y 100,000,000**: Genera un mensaje de registro cuando los mensajes de eventos de syslog que fluyen actualmente desde el origen de eventos a Security Analytics están en el rango de 100 a 100,000,000 bytes.
Filtro de eventos	Seleccione un filtro. Consulte Configurar un filtro de eventos de syslog para obtener instrucciones sobre cómo definir filtros.
Depurar	**Precaución:** Active la depuración (defina este parámetro en "Activado" o "Detallado") solamente si tiene un problema con un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa/desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar).
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega los parámetros del origen de eventos.

Tareas

Procedimientos

Configurar un filtro de eventos de syslog

Pestaña Configuración de recopilación de registros

En este tema se describen los parámetros de configuración de servicio disponibles en la pestaña Ajustes de configuración de la vista Configuración del servicio Log Collector.

La pestaña Configuración se usa para:

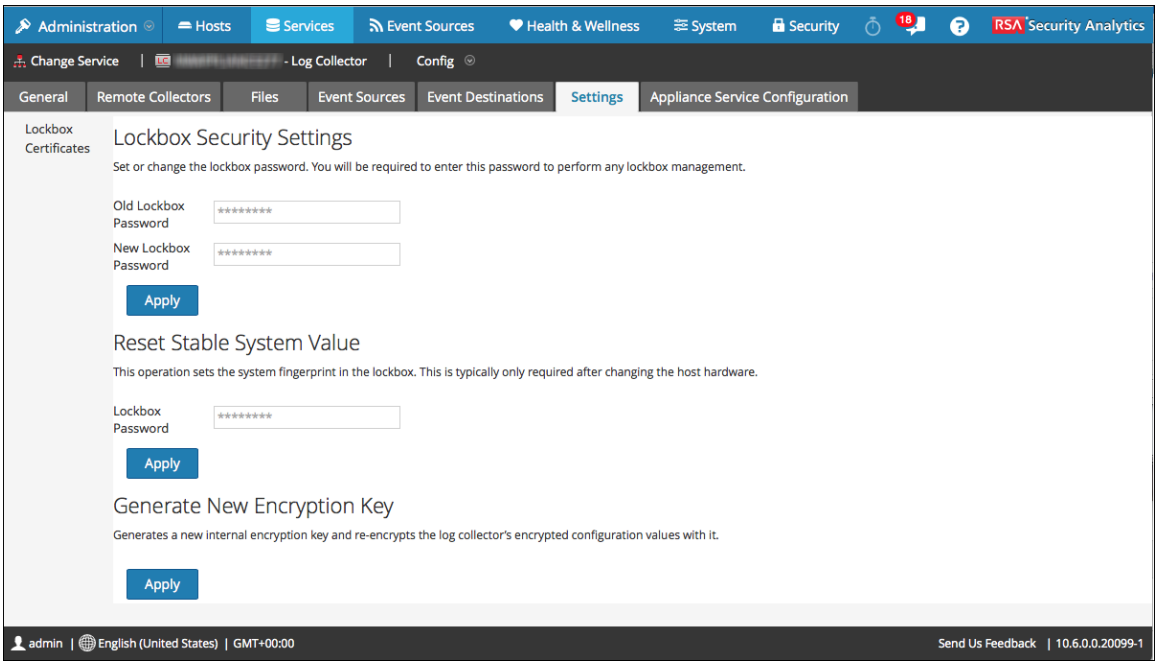
- Configurar un lockbox
- Restablecer valor de sistema estable

> **Precaución:** Si el nombre del host donde está instalado el Log Collector se cambia después de la instalación, el Log Collector no recopilará eventos de los orígenes de eventos. Si cambia el nombre del host, debe restablecer los valores de sistema estable.

- Administrar certificados.

Para acceder a la pestaña Configuración de recopilación de registros:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En el panel de opciones, seleccione:
   - Lockbox para mantener la configuración de Lockbox.
   - Certificados para agregar o eliminar certificados.



Parámetros de configuración de Lockbox

Este tema describe la configuración de seguridad de lockbox.

Un Lockbox es un archivo cifrado que se usa para almacenar información confidencial sobre una aplicación. Security Analytics Lockbox almacena una clave de cifrado para el Log Collector.

La clave de cifrado cifra todas las contraseñas de orígenes de eventos y la contraseña del intermediador de eventos, pero las contraseñas de orígenes de eventos reales no se almacenan en el Lockbox.

Cuando crea el Lockbox, debe:

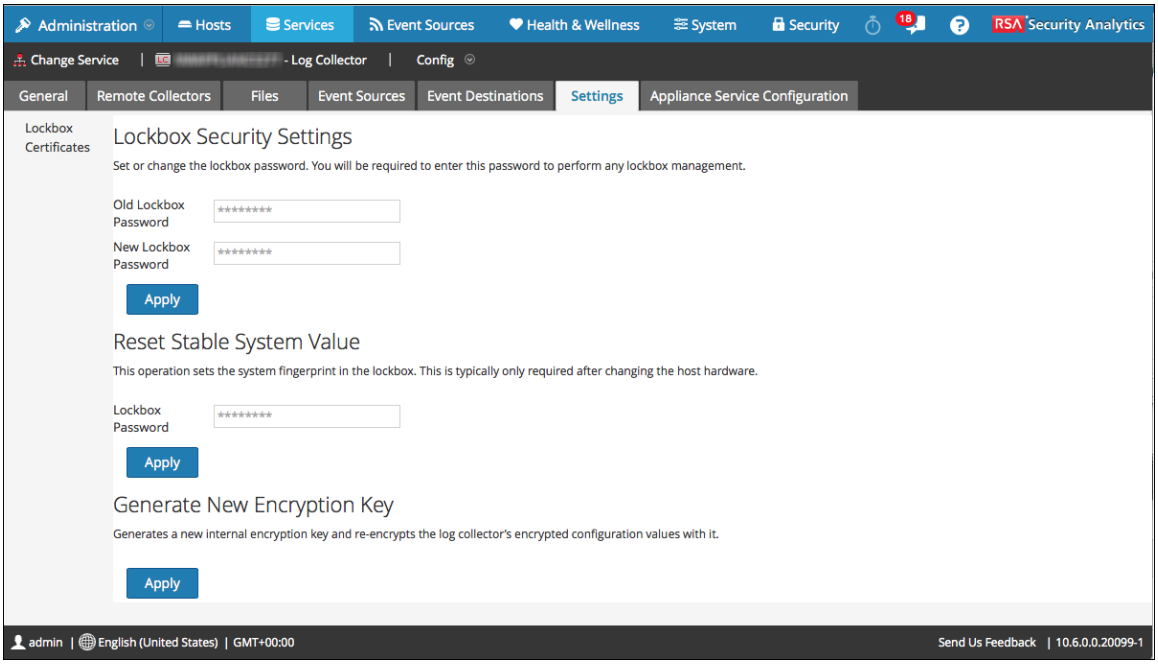
1. Definir una contraseña para el Lockbox.
2. Establecer una huella digital del sistema de host basada en valores estables del sistema.

Durante la recopilación de datos, Log Collector usa el Lockbox en un modo que no requiere que se especifique la contraseña (Log Collector usa en su lugar la huella digital del sistema host). Debe utilizar la contraseña de Lockbox de la siguiente manera:

- Cambie la contraseña de lockbox.
- Restablezca los valores estables del sistema
- Genere una nueva clave de cifrado.

Para acceder a Parámetros de configuración de Lockbox:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Configuración**.
5. En el panel de opciones, seleccione **Lockbox** para mantener la configuración de Lockbox.



Características

La vista Lockbox de la pestaña Configuración tiene tres secciones: Configuración de seguridad de lockbox, Restablecer valor de sistema estable y Generar nueva clave de cifrado.

Configuración de seguridad de lockbox

Antes de configurar los orígenes de eventos del Log Collector, debe configurar un Lockbox. Las reglas generales para la configuración de lockbox son:

- Solo será necesario definir una contraseña del lockbox una vez.
- Defina la contraseña antes de configurar orígenes de eventos.
- Después de definir la contraseña, el lockbox se configura para cualquier origen de eventos que agregue.

Los siguientes son los ajustes de seguridad de lockbox.

Característica	Descripción
Contraseña anterior de lockbox	Cuando configure un lockbox por primera vez, este campo estará en blanco. Security Analytics completa este campo una vez que se ingresa una Nueva contraseña de Lockbox y se hace clic en Aplicar.
Nueva contraseña de lockbox	Contraseña inicial o nueva del lockbox. **Nota:** Para maximizar la seguridad del Lockbox, especifique una contraseña que tenga ocho o más caracteres de longitud con al menos un carácter numérico, un carácter en mayúsculas y un carácter que no sea alfanumérico, como # o !
Aplicar	Haga clic en Aplicar para guardar los cambios realizados en la contraseña del lockbox.

Restablecer valor de sistema estable

Estos son los ajustes de Restablecer valor de sistema estable.

Característica	Descripción
Contraseña de lockbox	Cuando configure un lockbox por primera vez, este campo estará en blanco. Especifique la misma contraseña de lockbox que ingresó en Configuración de seguridad de lockbox. Generalmente, solo se necesita restablecer esta contraseña si cambia el hardware del host.
Aplicar	Haga clic en Aplicar para definir la huella digital del sistema en el lockbox.

Generar nueva clave de cifrado

Esta opción genera una nueva clave de cifrado interna y vuelve a cifrar los valores de los parámetros de configuración cifrados de Log Collector (generalmente, contraseñas). La opción se activa cuando hace clic en Aplicar.

Tareas

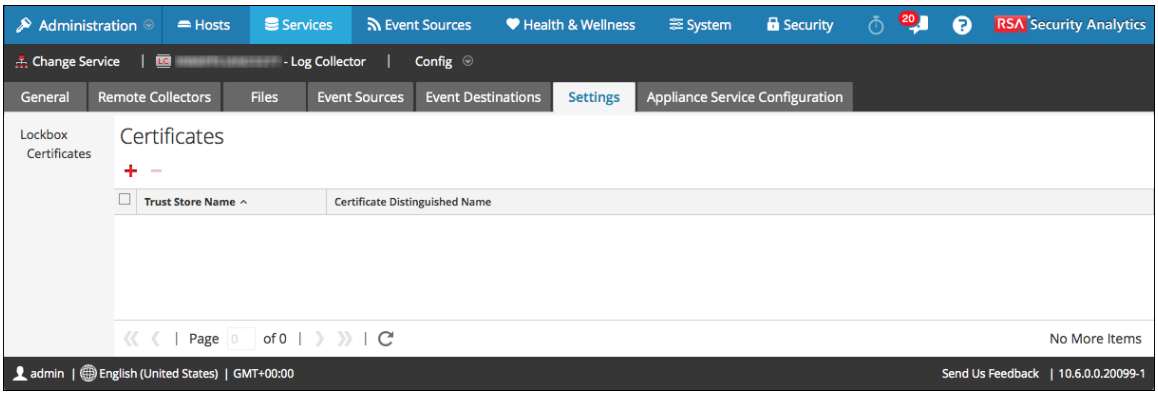
Procedimientos

Parámetros de configuración de los certificados

En este tema se describen los parámetros de configuración de certificados.

Para acceder a los parámetros de configuración de certificados:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Configuración**.
5. En el panel de opciones, seleccione **Certificados** para agregar o eliminar certificados.



Características

La vista Certificados de la pestaña Configuración tiene una sección: Certificados.

Certificados

Los certificados se administran mediante la creación de almacenes de confianza en el Log Collector. El Log Collector hace referencia a estos almacenes de confianza para determinar si los orígenes de eventos son de confianza o no.

Campo	Descripción
	Abre el cuadro de diálogo Agregar certificado, donde puede agregar un certificado y una contraseña.
	Elimina los certificados seleccionados.
	Selecciona certificados.

Campo	Descripción
Nombre del área de almacenamiento de confianza	Muestra el nombre del área de almacenamiento de confianza.
Nombre distinguido de certificado	Solamente para un origen de eventos de punto de comprobación, muestra el nombre distinguido del certificado.
Nombre de contraseña del certificado	Solamente para un origen de eventos de punto de comprobación, muestra el nombre de la contraseña del certificado.

Cuadro de diálogo Agregar certificado

Estos son los campos del cuadro de diálogo Agregar certificado.

Campo	Descripción
Nombre del área de almacenamiento de confianza	Escriba un nombre para el área de almacenamiento de confianza.
Archivo	Haga clic en Navegar para seleccionar un archivo de certificado (archivo *.PEM) en su red
Contraseña	Especifique la contraseña para este certificado.
Cerrar	Cierra el cuadro de diálogo sin agregar el certificado.
Guarda	Agrega el certificado.

Tareas

Procedimiento

Solucionar problemas de la configuración de la recopilación de registros

En este tema se señalan posibles problemas que puede encontrar en la configuración de la recopilación de registros y las soluciones que se sugieren para ellos.

Solucionar problemas de configuración de Remote Collector

Los mensajes de registro de la siguiente tabla se envían a:

- Para la configuración de Migración: **C:\NetWitness\ng\logcollector\rabbitmq\log\logcollector@localhost.log** en el servidor del recopilador de Windows heredado.
- Para la configuración de Extracción: **/var/log/rabbitmq/sa@localhost.log** en el servidor del host de Log Decoder en el cual se ejecuta Local Collector.

Log Mensajes	Mensaje de registro con "certificate expired" como parte del mensaje. Por ejemplo:
	`Any =ERROR REPORT==== 7-Apr-2015::11:02:07 ===`
	`SSL: cipher: tls_connection.erl:375:Fatal error: certificate expired`
	`=ERROR REPORT==== 7-Apr-2015::11:02:07 ===`
	`Shovel failed to connect to Host: "10.31.204.240" Port: 5671 VirtualHost: <<"logcollection">>: error: {badmatch,{error,`
	`{tls_alert,`
	`"certificate expired"}}}`

Causas posibles	La causa general de un mensaje de registro certificate expired es que el reloj (fecha/hora) del host del servicio SA y los relojes de uno o más hosts que ejecutan el servicio logcollector no están sincronizados. Los siguientes escenarios pueden causar este error. Los relojes del host del servicio SA y del host de Local Collector están sincronizados, pero el reloj del colector de Windows existente (WLC) está: • Causa 1: adelantado (en el futuro) con respecto al host de Local Collector y al host de SA. • Causa 2: atrasado (en el pasado) con respecto al host de Local Collector y al host de SA. El escenario del reloj de WLC en el pasado funciona si WLC está configurado para Migrar eventos al Local Collector. Sin embargo, si el Local Collector está configurado para Extraer eventos desde el WLC, este lee el certificado del Local Collector como no válido debido a que su fecha está adelantada (en el futuro) con respecto a la del WLC.

Soluciones	Para ambas causas, asegúrese de que los relojes del host de SA y de todos los hosts de Remote Collector y Local Collector estén sincronizados. • Causa 1: para un Remote Collector de Windows existente, puede ser necesario realizar una operación "rekey" si el certificado se creó en un momento que está "en el futuro" en comparación con Local Collector y Security Analytics. Para ello, realice lo siguiente: a. Seleccione el servicio **Log Collector** para el **Remote Collector de Windows heredado** en la vista **Servicios**. b. Haga clic en **Ver > Explorar**. c. Haga clic con el botón secundario en **/event-broker/ssl** y haga clic en **Propiedades**. Se muestra el cuadro de diálogo **Propiedades**. d. Vuelva a generar el certificado con el comando **rekey** en el cuadro de diálogo **Propiedades**. e. Intercambie el nuevo certificado con Security Analytics, para lo cual debe quitar y volver a agregar el servicio logcollector de Windows heredado en Security Analytics. • Causa 2: sincronice el WLC con el LC.

Solucionar problemas de recopilación

Consulte las instrucciones de solución de problemas correspondientes a cada protocolo de recopilación para conocer problemas relacionados con esos protocolos.

Guía de configuración de la recopilación de AWS (CloudTrail)

El protocolo de recopilación de Amazon Web Service (AWS) CloudTrail recopila eventos de Amazon Web Services (AWS) CloudTrail. CloudTrail registra llamadas API de AWS para una cuenta. Los eventos contienen la identidad del llamador de la API, la hora de la llamada API, la dirección IP de origen del llamador de la API, los parámetros de la solicitud y los elementos de respuesta que devolvió el servicio AWS. El historial de llamadas API de AWS que proporcionan los eventos de CloudTrail permite el análisis de seguridad, el rastreo del cambio de recursos y la auditoría del cumplimiento de normas. CloudTrail usa Amazon S3 para el almacenamiento y la distribución de archivos de registro. Security Analytics copia los archivos de registro desde la nube (depósito S3) y envía los eventos incluidos en los archivos a Log Collector.

Antes de configurar el protocolo de recopilación de AWS, debe implementar la recopilación de registros.

Conceptos básicos

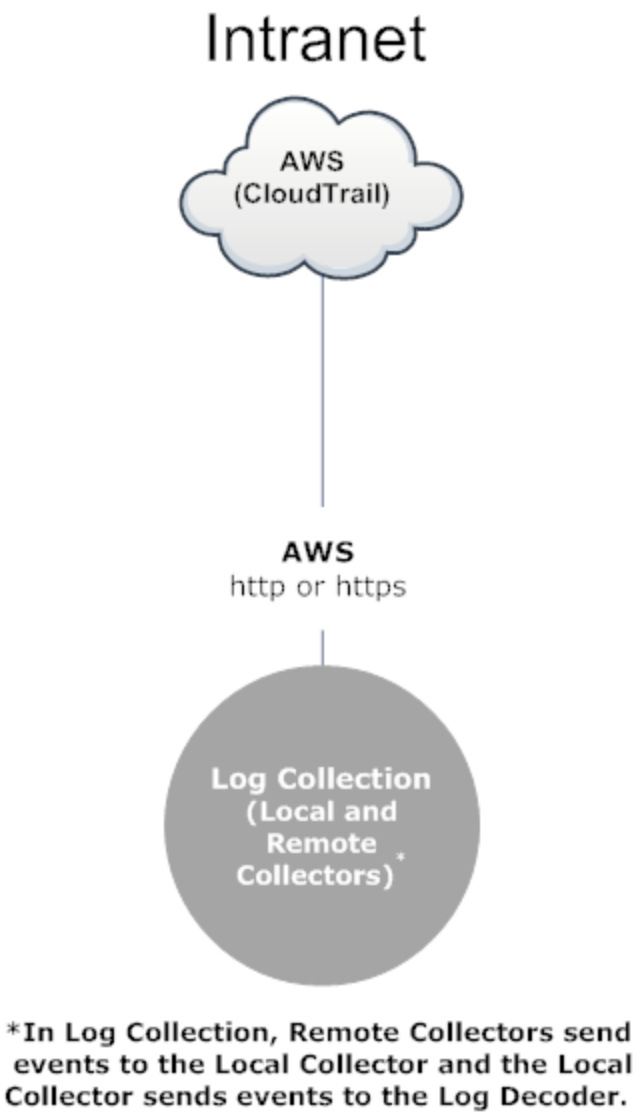
En esta guía se indica cómo configurar el protocolo de recopilación de AWS (CloudTrail), el cual recopila eventos de Amazon Web Services (AWS) CloudTrail.

Cómo funciona la recopilación de AWS

El servicio Log Collector recopila eventos de Amazon Web Services (AWS) CloudTrail. CloudTrail registra llamadas API de AWS para una cuenta. Los eventos contienen la identidad del llamador de la API, la hora de la llamada API, la dirección IP de origen del llamador de la API, los parámetros de la solicitud y los elementos de respuesta que devolvió el servicio AWS. El historial de llamadas API de AWS que proporcionan los eventos de CloudTrail permite el análisis de seguridad, el rastreo del cambio de recursos y la auditoría del cumplimiento de normas. CloudTrail usa Amazon S3 para el almacenamiento y la distribución de archivos de registro. Security Analytics copia los archivos de registro desde la nube (depósito S3) y envía los eventos incluidos en los archivos a Log Collector.

Escenario de implementación

En la siguiente figura se ilustra cómo implementar el protocolo de recopilación de AWS (CloudTrail) en Security Analytics.



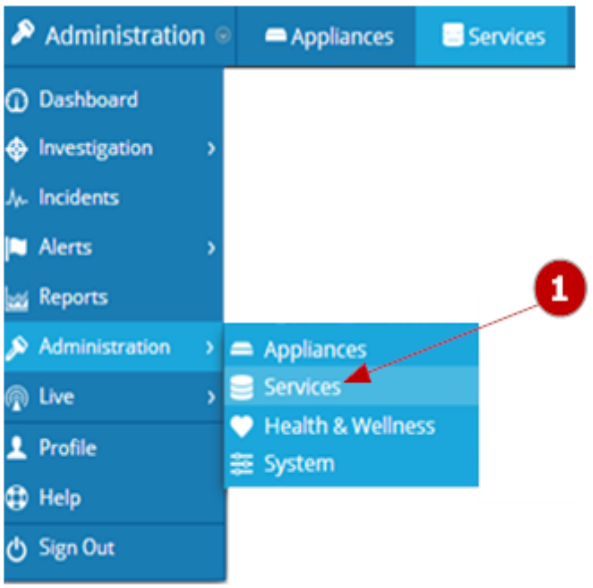
Procedimientos

Configurar el protocolo de recopilación de AWS (CloudTrail) en Security Analytics

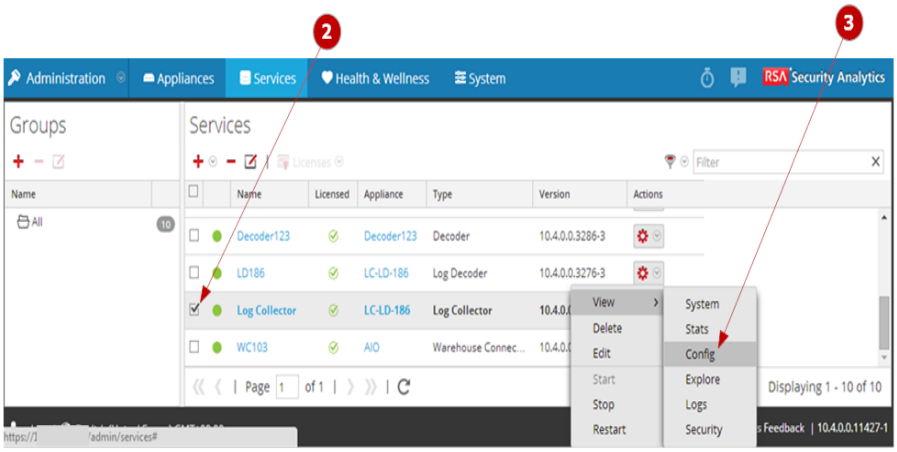
Puede configurar Log Collector para usar la recopilación de AWS (CloudTrail) para un origen de eventos en la pestaña Origen de eventos de la vista de parámetros de Log Collector. En la siguiente figura se muestra el flujo de trabajo básico para configurar un origen de eventos para la recopilación de AWS (CloudTrail) en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de AWS (CloudTrail) en Security Analytics para obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de AWS.

- Referencias: Parámetros de configuración de la recopilación de AWS (CloudTrail) para obtener una descripción detallada de cada parámetro del protocolo de recopilación de AWS (CloudTrail).

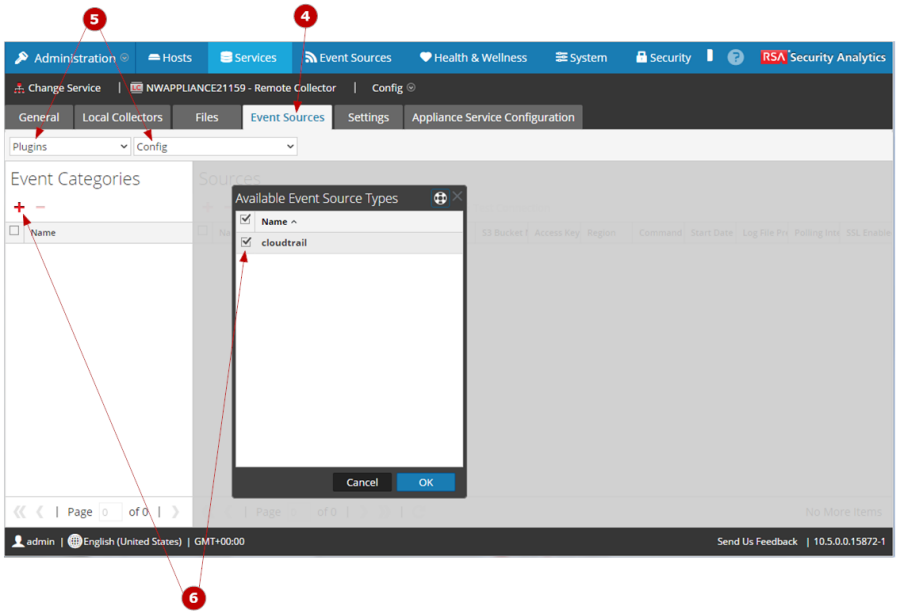


1 En el menú de **Security Analytics**, seleccione **Administration > Servicios**.



2 Seleccione un servicio de **recopilación de registros**.

3 Haga clic en ⌄ bajo **Acciones** y seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.

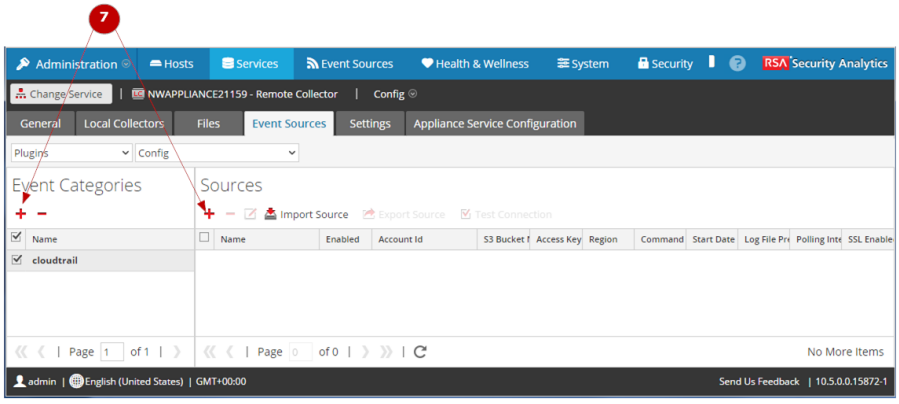


4 Haga clic en la pestaña **Orígenes de evento**.

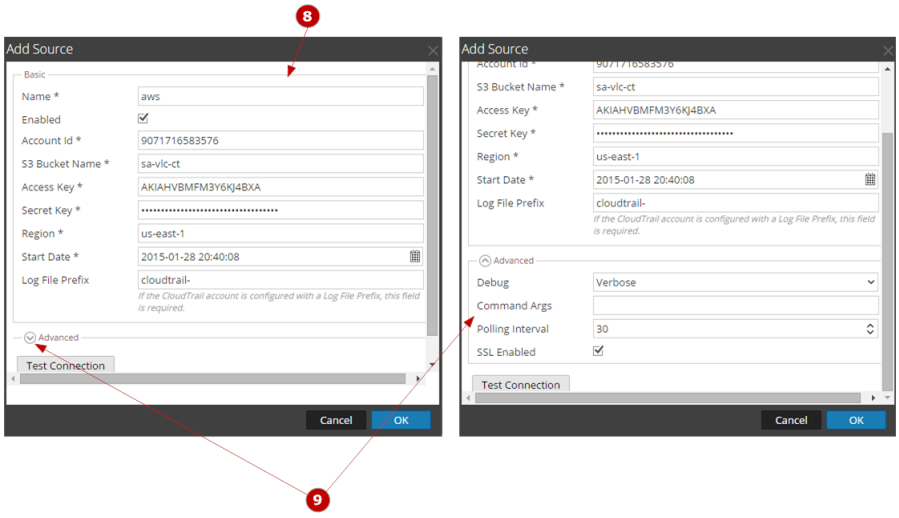
5 Seleccione **Plug-ins** como el protocolo de recopilación y elija **Configuración**.

6 Haga clic en + y seleccione **cloudtrail** como la categoría de origen de eventos.

La categoría de origen de eventos es parte del contenido que descargó de LIVE.



7 Seleccione la categoría **AWS (CloudTrail)** y haga clic en +.



8 Especifique los parámetros básicos requeridos para el origen de eventos de AWS (CloudTrail).

9 Haga clic en y especifique parámetros adicionales que mejoran la manera en que el protocolo de AWS (CloudTrail) maneja la recopilación de eventos para el origen de eventos.

Configurar orígenes de eventos de modo que usen el protocolo de recopilación de AWS (CloudTrail)

Debe configurar cada origen de eventos que usa el protocolo de recopilación de AWS (CloudTrail) para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de AWS (CloudTrail) para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de AWS (CloudTrail), con una lista de verificación que contiene cada paso de configuración.

Los pasos de configuración del protocolo de recopilación de AWS (CloudTrail) se deben realizar en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de la configuración de AWS (CloudTrail)

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de AWS (CloudTrail) en Security Analytics.	
2	Configurar orígenes de eventos de AWS (CloudTrail) para enviar eventos a Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de AWS (CloudTrail) configurado.	
4	Verificar que la recopilación de AWS (CloudTrail) esté funcionando.	

Paso 1. Configurar orígenes de eventos de AWS (CloudTrail) en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de AWS (CloudTrail) para Log Collector.

Después de realizar este procedimiento, habrá...

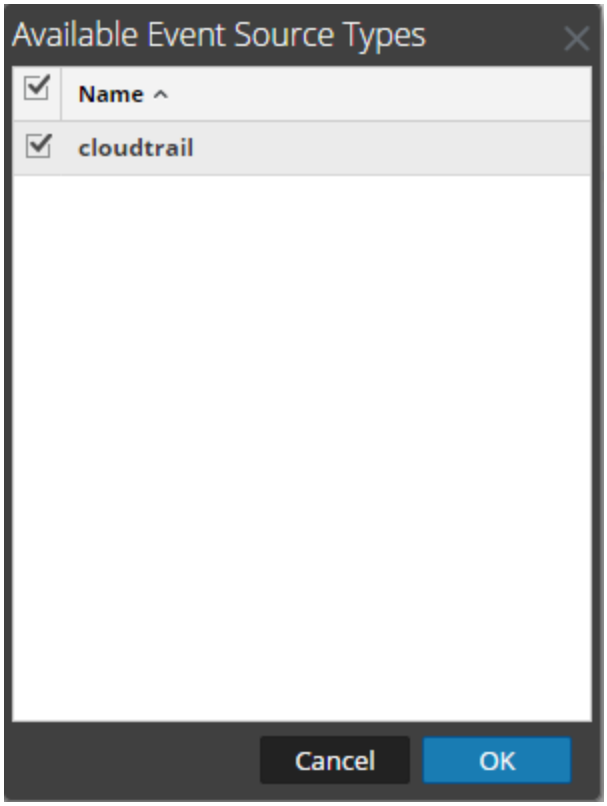
- Configurado un origen de eventos de AWS (CloudTrail).
- Modificado un origen de eventos de AWS (CloudTrail).
- Extraído un certificado para un origen de eventos de AWS (CloudTrail).

Volver a Procedimientos

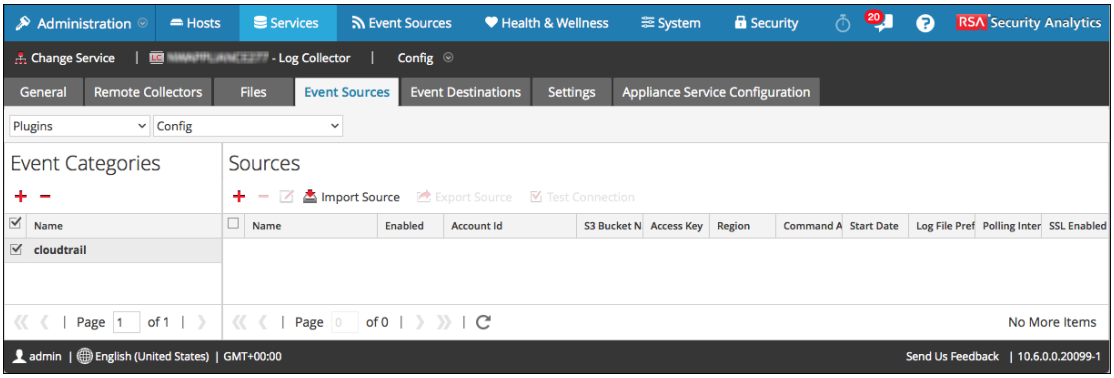
Procedimientos

Configurar un origen de eventos de AWS (CloudTrail)

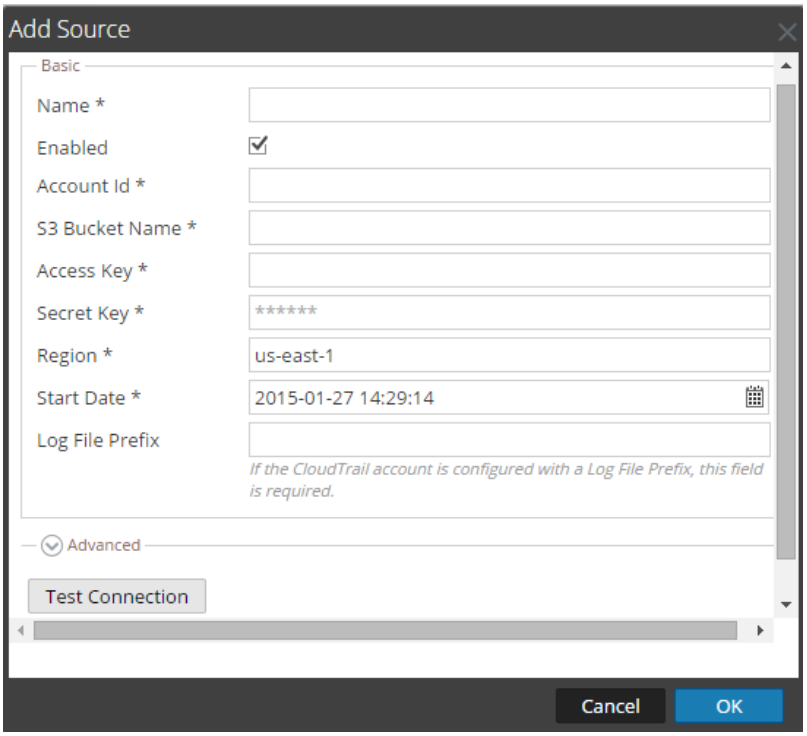
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Plug-ins/Configurar** en el menú desplegable.
5. En la barra de herramientas del panel **Categorías de evento**, haga clic en  .
   Se muestra el cuadro de diálogo **Tipos de origen de evento disponibles**.
6. Seleccione un tipo de origen de eventos (por ejemplo, **cloudtrail**) y haga clic en **Aceptar**.



El tipo de origen de eventos recién agregado se muestra en el panel **Categorías de evento**.



7. Seleccione el nuevo tipo en el panel **Categorías de evento** y haga clic en + en la barra de herramientas **Orígenes**.
   Se muestra el cuadro de diálogo **Agregar origen**.

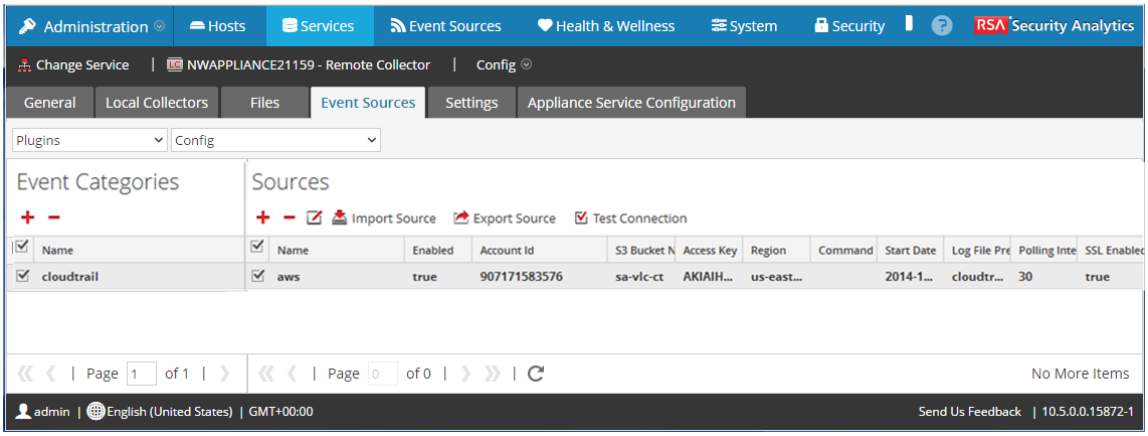


8. Definir valores de parámetros (consulte Referencias: Parámetros de configuración de la recopilación de AWS (CloudTrail) para ver definiciones de cada parámetro).

9. Haga clic en **Probar conexión**.
   El resultado de la prueba se muestra en el cuadro de diálogo. Si el resultado de la prueba no fue satisfactorio, edite la información del dispositivo o del servicio e inténtelo nuevamente. Log Collector tarda aproximadamente 60 segundos en devolver los resultados de la prueba.

Si se excede el límite de tiempo, se agota el tiempo de espera de la prueba y Security Analytics muestra un mensaje de error.

10. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**.
    El nuevo origen de eventos se muestra en el panel **Orígenes**.

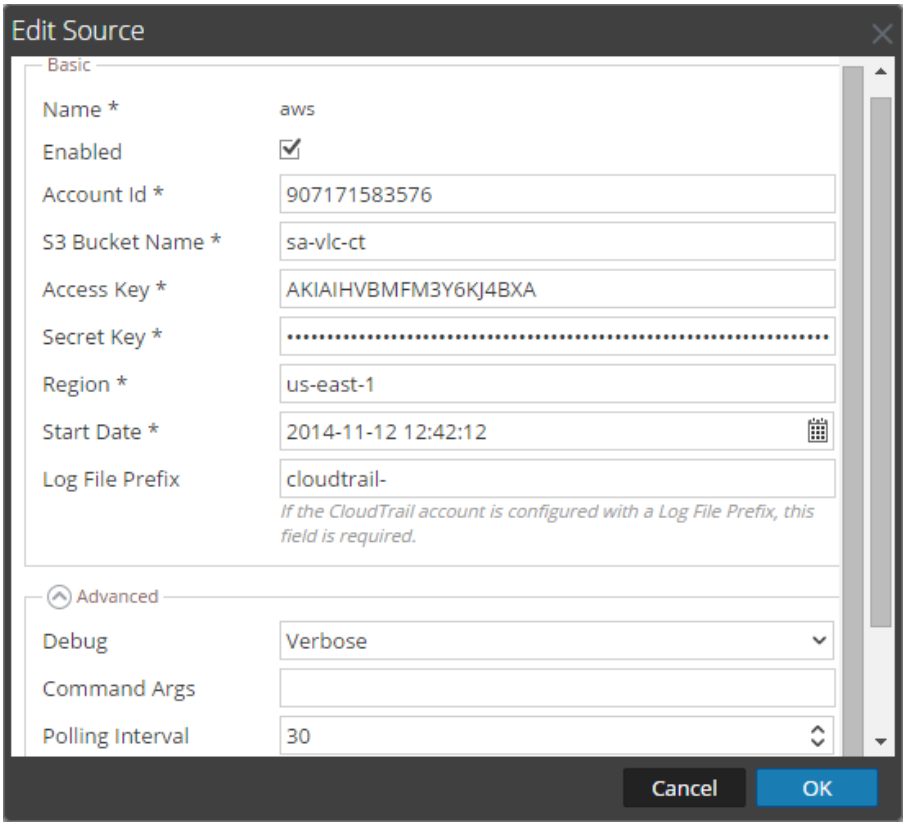


Modificar un origen de eventos de AWS (CloudTrail)

Para modificar un origen de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Plug-ins/Configurar** en el menú desplegable.
   En el panel **Categorías de evento** se muestran los orígenes de eventos que están configurados, si los hay.
5. Seleccione un tipo de origen de eventos en el panel **Categorías de evento**.
   Los orígenes de eventos de este tipo se muestran en el panel **Orígenes**.
6. Seleccione un origen y haga clic en  en la barra de herramientas.
   Se muestra el cuadro de diálogo **Editar origen**.

7. Modifique los parámetros que requieren cambios.



8. Haga clic en **Probar conexión**.
   El resultado de la prueba se muestra en el cuadro de diálogo. Si el resultado de la prueba no es satisfactorio, edite la información del dispositivo y del servicio y vuelva a intentarlo.
   Log Collector tarda aproximadamente 60 segundos en devolver los resultados de la prueba. Si se excede el límite de tiempo, se agota el tiempo de espera de la prueba y Security Analytics muestra un mensaje de error.
9. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**.
   Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado.

Parámetros

Referencias: Parámetros de configuración de la recopilación de AWS (CloudTrail)

Paso 2. Configurar orígenes de eventos de AWS (CloudTrail) para enviar eventos a Security Analytics

En este tema se indica dónde encontrar los orígenes de eventos que son compatibles actualmente con la recopilación de AWS (CloudTrail) y las instrucciones de configuración disponibles para cada origen de eventos

Volver a Procedimientos

Consulte Paso 1. Configurar orígenes de eventos de AWS (CloudTrail) en Security Analyticspara obtener instrucciones sobre cómo configurar un origen de eventos de CloudTrail.

Paso 3. Iniciar el servicio para el protocolo de recopilación de AWS (CloudTrail) configurado

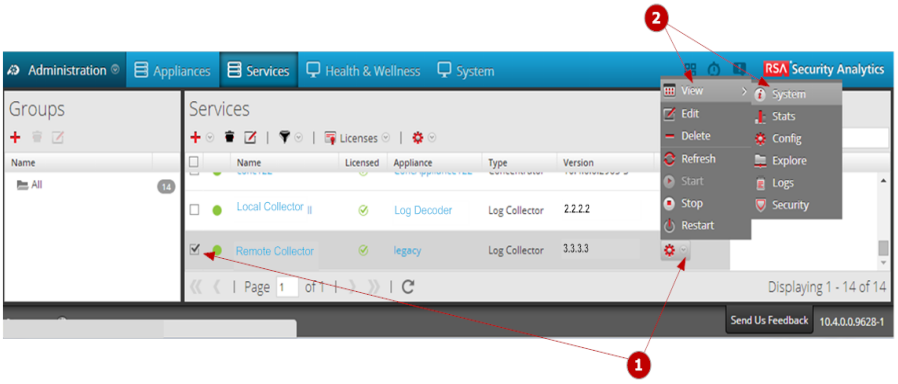
En este tema se indica cómo iniciar un servicio de recopilación de plug-ins detenido.

Volver a Procedimientos

Si el servicio de recopilación de Plug-ins se detiene, tendrá que iniciarlo nuevamente para que funcione. También puede consultar el tema Habilitar el inicio automático de servicios individuales de la Guía de configuración de la recopilación de registros si desea que el servicio se inicie automáticamente.

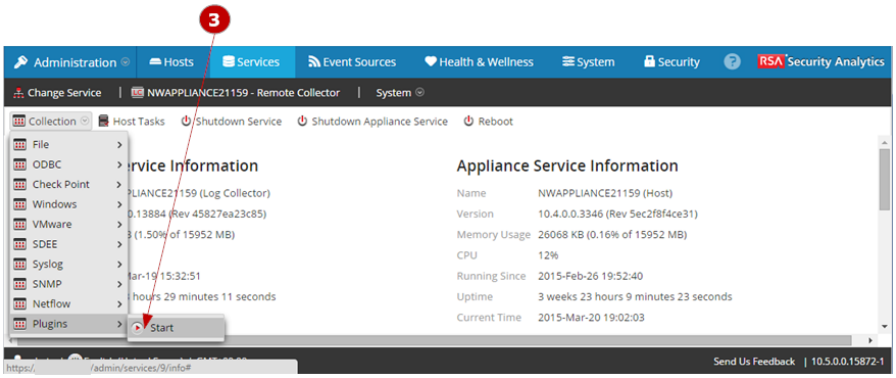
Procedimiento

En la siguiente figura se muestra cómo iniciar un servicio de recopilación.



1 En el menú de **Security Analytics**, seleccione **Administration > Servicios**.

2 Seleccione un servicio **Log Collector** y haga clic en bajo **Acciones**. Haga clic en **Ver > Sistema**.



3 Haga clic en **Recopilación > Plug-ins** y, a continuación, haga clic en **Iniciar**.

Paso 4. Verificar que la recopilación de AWS (CloudTrail) esté funcionando

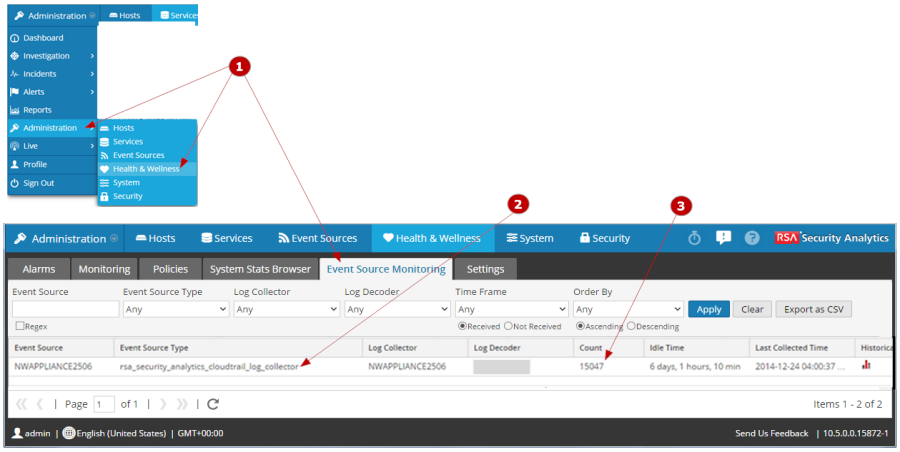
En este tema se indica qué comprobar en Security Analytics para verificar que la recopilación de AWS (CloudTrail) se configuró correctamente.

Volver a Procedimientos

Si la recopilación de AWS no se configura correctamente, no funcionará. Para asegurarse de que la recopilación funcione, puede verificarla en la vista **Estado y condición**.

Procedimiento

En la siguiente figura se ilustra cómo puede verificar que la recopilación de AWS (CloudTrail) esté funcionando desde **Administration > Estado y Condición > pestaña Monitoreo de orígenes de eventos**.



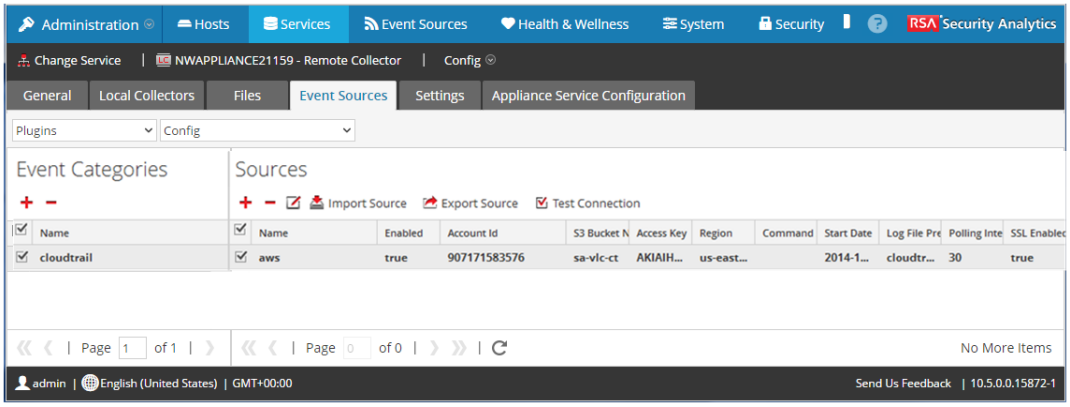
1. Acceda a la pestaña **Monitoreo de orígenes de eventos** desde la vista **Administration > Estado y condición**.
2. Busque **rsa_security_analytics_aws_log_collector** en la columna **Tipo de origen de evento**.
3. Busque actividad en la columna **Conteo** para verificar que la recopilación de AWS (CloudTrail) esté aceptando eventos.

Referencias: Parámetros de configuración de la recopilación de AWS (CloudTrail)

En este tema se describen los parámetros de configuración del origen de eventos de AWS (CloudTrail).

Para acceder a los parámetros de configuración de la recopilación de AWS:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Plug-ins/Configurar** en el menú desplegable.



La vista Plug-ins/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar los tipos de orígenes de eventos correspondientes.

Característica	Descripción
	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.
	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de tipos de orígenes de eventos compatibles.

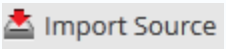
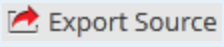
Característica	Descripción
	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

Panel Orígenes

En el panel Orígenes de AWS (CloudTrail) se muestra una lista de los orígenes de eventos de firewall de AWS (CloudTrail) existentes. Utilice esta sección para agregar o eliminar orígenes de eventos y parámetros de comunicación asociados.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar origen, en el cual puede definir los parámetros para un host de firewall de AWS (CloudTrail).
	Elimina el host que seleccionó.
	Abre el cuadro de diálogo Editar origen, en el cual puede editar los parámetros del origen de eventos de AWS (CloudTrail) seleccionado. Seleccione varios orígenes de eventos y haga clic en  para abrir el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar hosts de AWS (CloudTrail) de forma masiva desde un archivo de valores separados por comas (CSV). Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo **.csv** que contiene los parámetros de los hosts de AWS (CloudTrail) seleccionados. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Valida los parámetros de configuración de los hosts de firewall de AWS (CloudTrail) seleccionados. *Consulte la Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo probar conexiones de orígenes de eventos en masa.

Cuadro de diálogo Agregar/Editar origen

Los cuadros de diálogo Agregar origen y Editar origen contienen la misma información.

Valida la conexión a la dirección del origen de eventos.

Parámetro	Descripción
Parámetro	**Descripción**
	Básico
Nombre *	Nombre del origen de eventos.
Activado 	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
ID de cuenta *	Código de identificación de la cuenta del depósito S3

Parámetro	Descripción
Nombre de depósito S3 *	Nombre del depósito S3 de AWS (CloudTrail). Los nombres del depósito Amazon S3 son únicos globalmente, sin importar la región de AWS (CloudTrail) en la cual se crea el depósito. El nombre se especifica en el momento en que se crea el depósito. Los nombres de depósito deben cumplir con las convenciones de asignación de nombres de DNS. Las reglas para nombres de depósito que cumplen con DNS son: • Los nombres de depósito deben tener por lo menos tres caracteres de largo y no más de 63. • Los nombres de depósito deben ser una serie de una o más etiquetas. Las etiquetas adyacentes se separan mediante un único punto “.”. Los nombres de depósito pueden incluir letras en minúscula, números y guiones. Cada etiqueta debe comenzar y terminar con una letra en minúscula o un número. • Los nombres de depósito no deben tener el formato de una dirección IP (por ejemplo, 192.168.5.4). Los siguientes ejemplos son nombres de depósito **válidos**: • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** Los siguientes ejemplos son nombres de depósito **no válidos**: • **.myawsbucket**: un nombre de depósito no debe comenzar con un punto “.”. • **myawsbucket.** : un nombre de depósito no debe terminar con un punto “.”. • **my..examplebucket**: solo se debe usar un punto entre las etiquetas.
Clave de acceso *	Clave que se usa para acceder al depósito S3. Las claves de acceso se usan para realizar solicitudes del protocolo REST o de consulta seguras a cualquier API del servicio AWS. Consulte Manage User Credentials en el sitio de soporte de Amazon Web Services para obtener más información sobre las claves de acceso.

Parámetro	Descripción
Clave secreta *	Clave secreta que se usa para acceder al depósito S3.
Región *	Región del depósito S3. **us-east-1** es el valor predeterminado.
Fecha de inicio *	Fecha y hora de inicio en que la recopilación de AWS (CloudTrail) se inicia por primera vez.
Prefijo de archivo de registro	Prefijo de los archivos que se procesarán. **Nota:** Si estableció un prefijo cuando configuró el servicio CloudTrail, asegúrese de ingresar el mismo prefijo en este parámetro.
Avanzado	
Depurar	**Precaución:** Habilite la depuración (defina este parámetro en Activado o Detallado) solamente si hay un problema en un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa/desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar).
Argumentos de comando	Argumentos que se agregan al script.

Parámetro	Descripción
Intervalo de sondeo	El intervalo (cantidad de tiempo en segundos) entre cada encuesta. El valor predeterminado es 60. Por ejemplo, si especifica 60, el recopilador calendariza un sondeo del origen de eventos cada 60 segundos. Si aún se está realizando el ciclo de sondeo anterior, esperará hasta que ese ciclo termine. Si está sondeando una gran cantidad de orígenes de eventos, es posible que el sondeo tarde más de 60 segundos en comenzar, porque los hilos de ejecución están ocupados.
SSL habilitado 	Seleccione la casilla de verificación para establecer la comunicación mediante SSL. La seguridad de la transmisión de datos se administra mediante el cifrado de la información y el suministro de autenticación con certificados SSL. La casilla de verificación está seleccionada de manera predeterminada.
Probar conexión	Valida que los parámetros de configuración especificados en este cuadro de diálogo estén correctos. Por ejemplo, esta prueba valida que: • Security Analytics se puede conectar al depósito S3 en AWS con el uso de las credenciales especificadas en este cuadro de diálogo. • Security Analytics puede descargar un archivo de registro desde el depósito (la conexión de prueba fallaría si no hubiera archivos de registro para todo el depósito, pero esto sería extremadamente improbable).
Cancelar	Cierra el cuadro de diálogo sin agregar el origen de eventos AWS (CloudTrail).
OK	Agrega los valores de los parámetros actuales como un nuevo origen de eventos AWS (CloudTrail).

Tareas

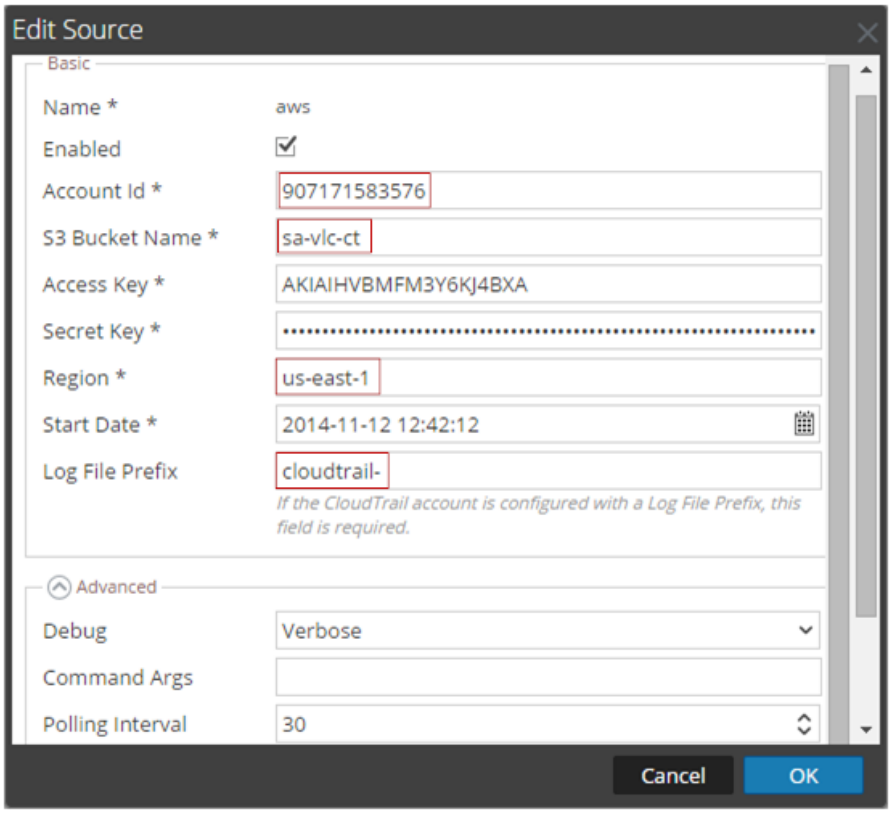
Paso 1. Configurar orígenes de eventos de AWS (CloudTrail) en Security Analytics

Solucionar problemas de la recopilación de AWS (CloudTrail)

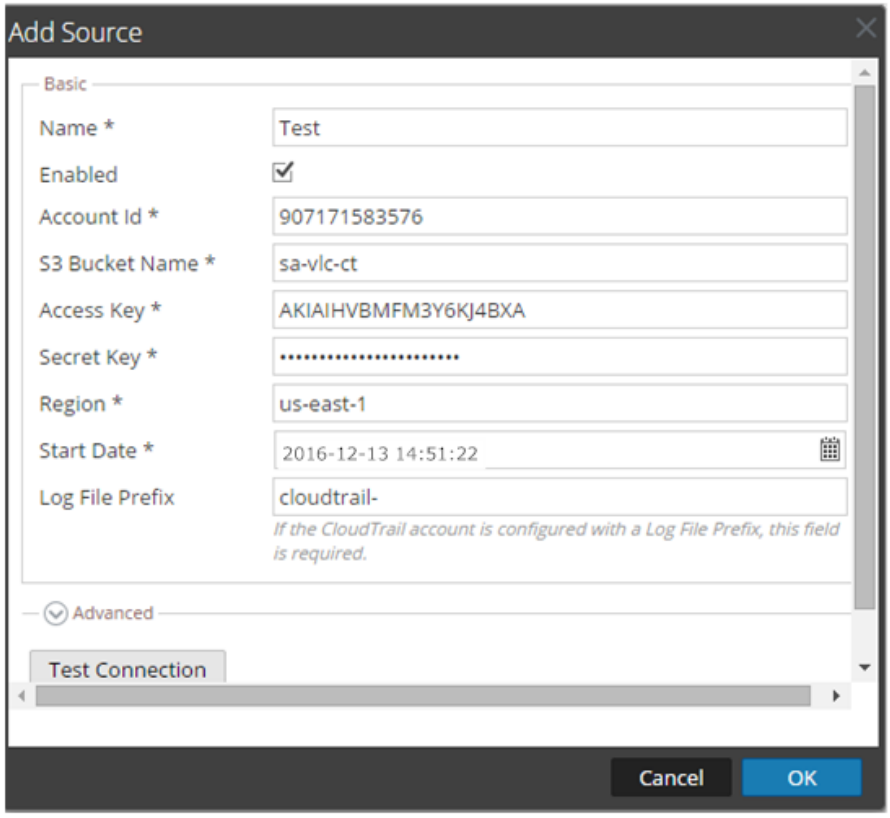
En este tema se señalan posibles problemas que puede encontrar en la recopilación de AWS (CloudTrail) y las soluciones que se sugieren para ellos.

Nota: En general, se reciben mensajes de registro más confiables cuando se desactiva SSL.

Mensaje de registro/ Problema	No se encontró ninguna clave de depósito bajo “arn:aws:s3:::bucket-name/AWSLogs/account-id/CloudTrail/region/”. Determine si el “Nombre de depósito S3” para CloudTrail está configurado y si “ID de cuenta” y “Región” están correctos. Determine también si la cuenta de CloudTrail está configurada con un “Prefijo de archivo de registro” y, si es así, si está definida correctamente para este origen de eventos.
Causa posible	El parámetro Nombre de depósito S3 y sus parámetros asociados no están configurados correctamente.
Solución	Para el origen de eventos que devolvió este mensaje: 1. Asegúrese de haber especificado un Nombre de depósito S3. 2. Asegúrese de haber especificado el ID de cuenta y la Región correctos. 3. Si la cuenta de CloudTrail tiene un Prefijo de archivo de registro, asegúrese de haberlo especificado correctamente. Por ejemplo:



Mensaje de registro/ Problema	Cuando intenta crear un origen de eventos de plug-ins, recibe el siguiente mensaje de error: `Parameter start_date: Invalid dateTime 2015-03-16T23:36:52.000Z :` Time must be specified in the past. Compruebe que la hora esté sincronizada en los dispositivos o especifique una hora en el pasado.
Causa posible	Seleccionó una fecha inicial no válida, una fecha que, de acuerdo con Security Analytics, no estaba en el pasado. Por ejemplo:



Esto ocurrió por dos motivos:

- Seleccionó una fecha de inicio que estaba en el futuro.
- La hora no está sincronizada en los hosts.

Solución

Asegúrese de que la hora esté sincronizada en los hosts. Seleccione una fecha en el pasado para la **Fecha inicial**.

Pages 191 - 226 Deleted May 8, 2017.

Configurar e implementar el servicio Remote Log Collector en AWS

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para implementar un servicio de recopilación remota de registros (VLC) en un ambiente Amazon Web Services (AWS) con una lista de verificación que contiene cada paso de configuración.

Nota: Security Analytics versión 10.6 debe estar instalado en el sistema con el fin de configurar e implementar correctamente un servicio de recopilación remota de registros en AWS.

Los pasos de configuración para implementar un servicio de recopilación remota de registros en un ambiente AWS deben realizarse en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de la configuración del servicio Remote Log Collector

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Iniciar sesión en AWS y crear una instancia.	
2	Configurar el servicio Remote Log Collector en AWS.	
	• Acceder a los recursos web de Amazon EC2	
	• Crear una instancia	
	• Seleccionar una AMI	
	• Elegir un tipo de instancia	
	• Configurar los detalles de la instancia	
	• Agregar almacenamiento	
	• Configurar el grupo de seguridad	

Paso	Descripción	√
	• Revisar el inicio de la instancia	
3	Implementar el servicio Remote Log Collector en AWS.	
	Implementar Remote Log Collector mediante scripts	
	• Iniciar sesión mediante el protocolo SSH	
	• Deshabilitar el repositorio base de CentOS	
	• Descargar los scripts de AWS	
	• Usar WinSCP para copiar los scripts descargados	
	• Configurar permisos de firewall	
	• Sincronizar la hora	
	• Implementar el contenido de Log Collector	
	Implementar manualmente Remote Log Collector	
	• Iniciar sesión mediante el protocolo SSH	
	• Deshabilitar el repositorio base de CentOS	
	• Configurar el usuario raíz	
	• Configurar la comunicación en el lado de AWS	
	• Configurar permisos de firewall	
	• Habilitar Remote Log Collector en el servidor de Security Analytics	
	• Configurar la comunicación en el lado de NetWitness	
	• Implementar el contenido de Log Collector	

Paso 1: Iniciar sesión en AWS y crear una instancia

Procedimiento: Iniciar sesión en AWS

Nota: RSA NetWitness 10.6 debe estar instalado en el sistema para realizar la implementación en AWS.

En este tema se indica cómo crear una instancia. Una instancia es un servidor virtual en Elastic Compute Cloud (EC2) de Amazon que ejecuta una aplicación en la infraestructura de Amazon Web Services.

Nota: Una cuenta de RSA Live es requisito previo para crear una instancia en AWS.

Para iniciar sesión en AWS:

1. Desde el navegador, vaya a http://aws.amazon.com.
2. Seleccione **Iniciar sesión en la consola**.
3. Ingrese las credenciales de nombre de usuario y contraseña.

4. Seleccione **Iniciar sesión**.

Procedimiento: Crear una instancia

Debe crear una instancia antes de configurar el servicio Remote Log Collector.

Para crear una instancia, realice las siguientes tareas.

- Descargue la plantilla CentOS 6 (x86_64) - with Updates HVM.
- Acceda a los **recursos web de Amazon EC2**.
- Inicie la nueva instancia en AWS.
- Cree un par de claves.

Descargar la plantilla CentOS 6 (x86_64) - with Updates HVM

Realice los siguientes pasos para descargar la plantilla CentOS 6 (x86_64) - with Updates HVM desde Amazon Marketplace.

Nota: Solo debe descargar la plantilla CentOS 6 (x86_64) - with Updates HVM una vez y puede utilizarla posteriormente para crear varias instancias.

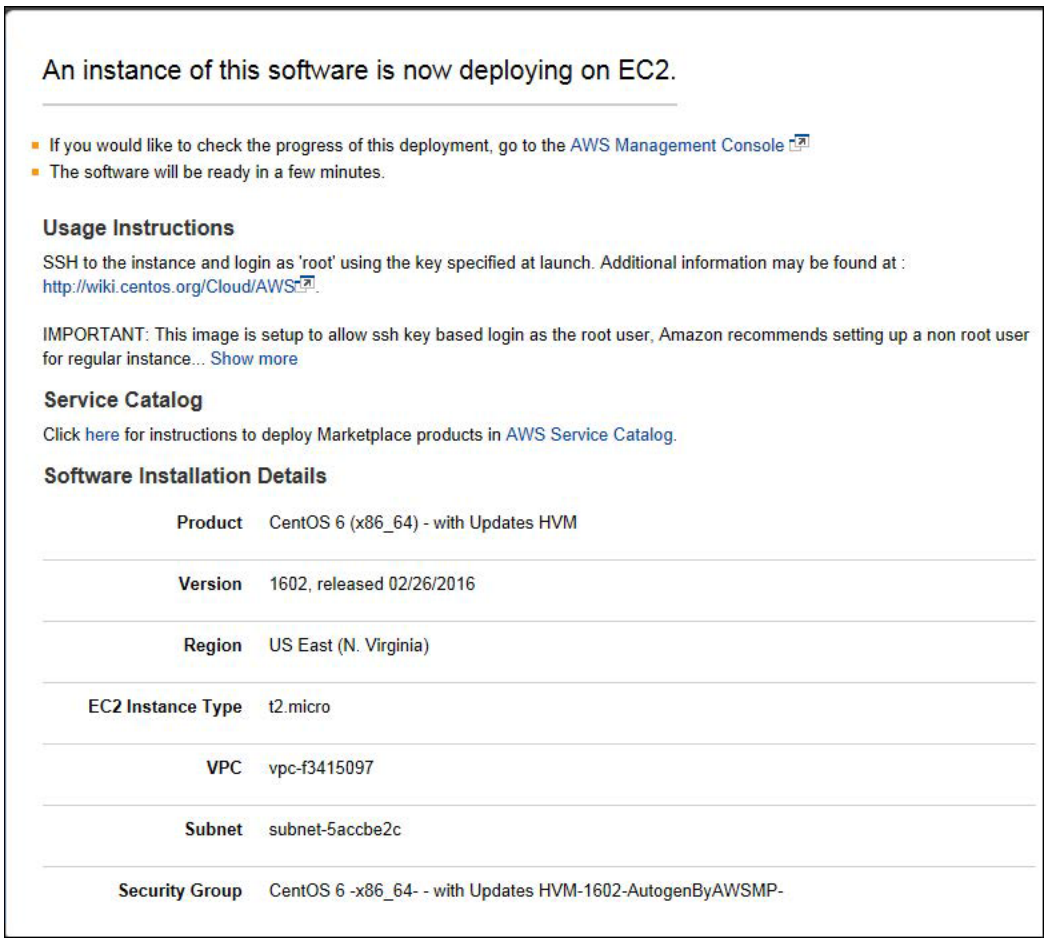
1. En la página de inicio de AWS, seleccione **AWS Marketplace** en la parte inferior de la página.

   Se muestra la página **AWS Marketplace**.

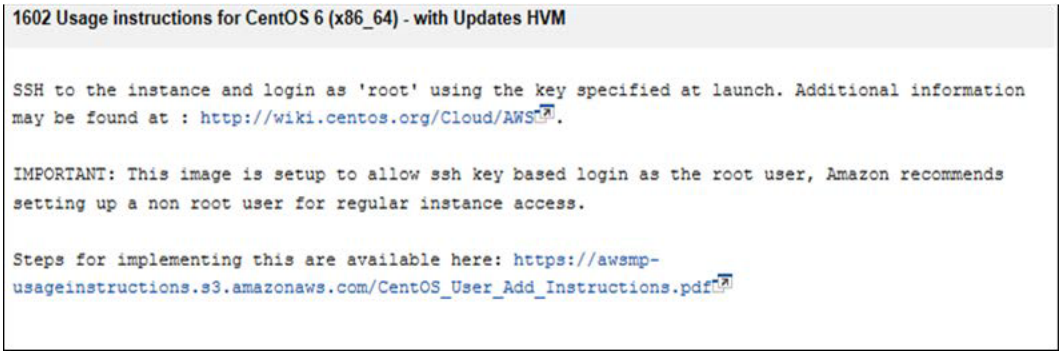
2. En la ventana **Search**, ingrese **CentOS 6** para buscar la plantilla **CentOS 6 (x86_64) - with Updates HVM**. Haga clic en **Ir**.
3. Haga clic en **CentOS 6 (x86_64) - with Updates HVM**.
   Se muestra la siguiente pantalla.

4. Haga clic en **Accept Software Terms & Launch with 1-Click** para descargar la plantilla. Se muestra el siguiente cuadro de diálogo.



5. Haga clic en **X** para cerrar este cuadro de diálogo.
6. Haga clic en **Instrucciones de uso**.

Se muestra el siguiente cuadro de diálogo.

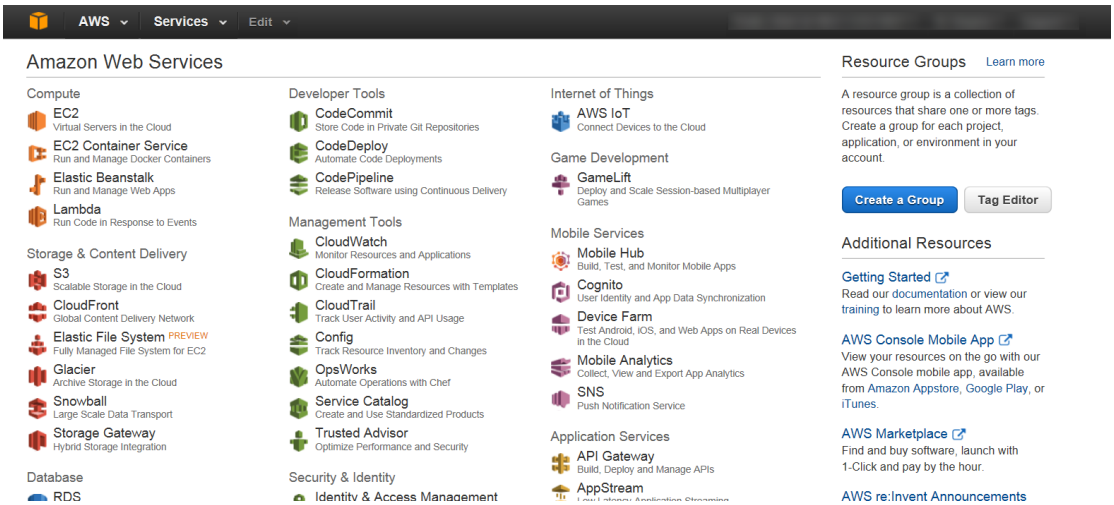


Antes de crear una instancia, debe acceder a los **recursos web de Amazon EC2**.

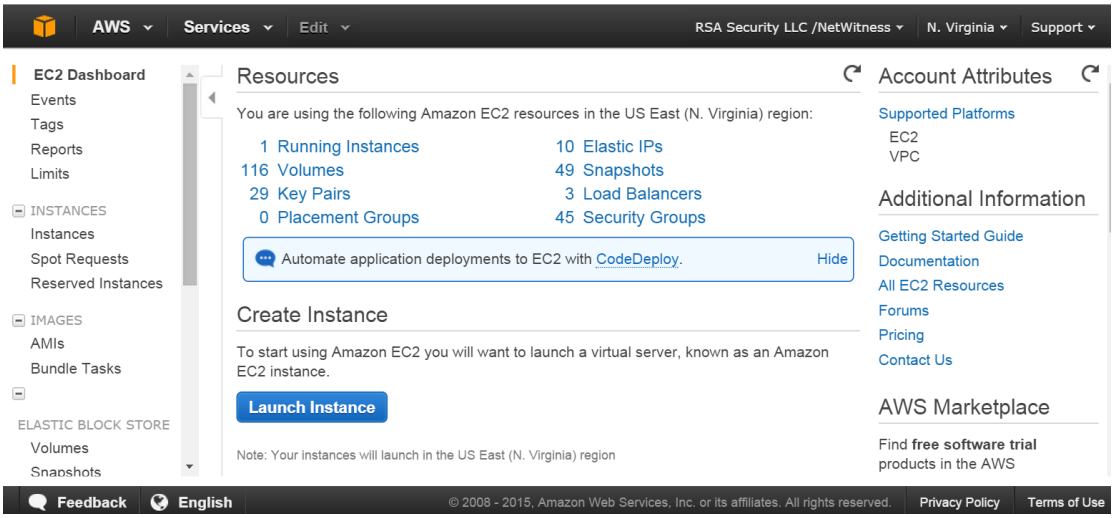
Acceder a los recursos web de Amazon EC2

Realice los siguientes pasos para acceder a los recursos web de Amazon EC2 en Marketplace.

1. Seleccione Servicios de **EC2** para acceder a los recursos web de Amazon EC2.



Se muestra la siguiente pantalla.

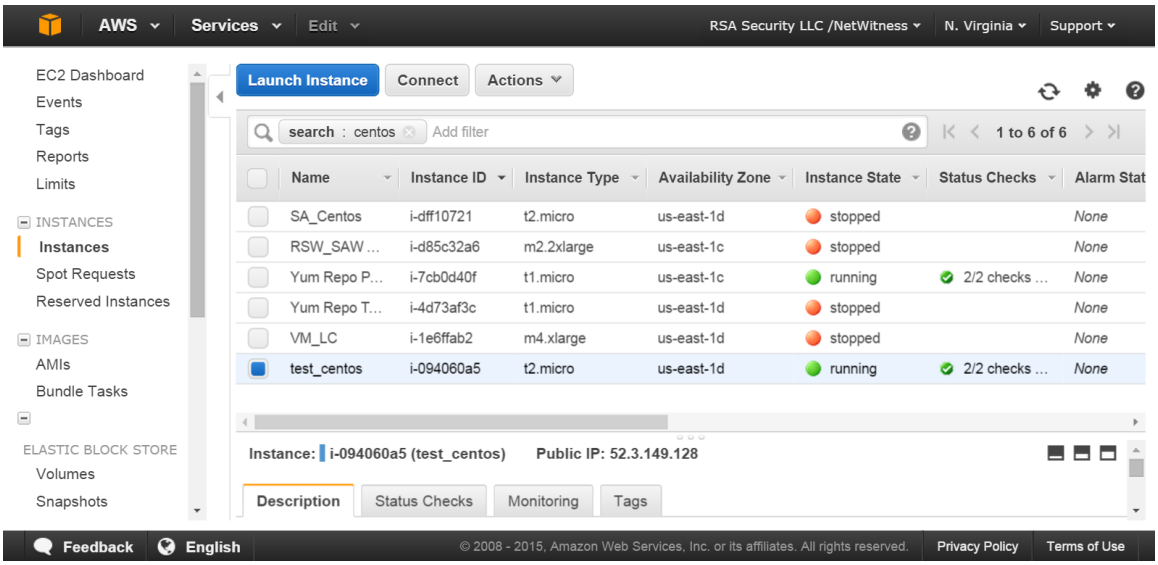


2. Seleccione **Instances** en el panel izquierdo.

Realice los siguientes pasos para iniciar la nueva instancia.

1. Seleccione la plantilla **CentOS6 (x86_64) - with Updates HVM5**.
2. Vaya a **Acciones > Estado de la instancia > Iniciar**.

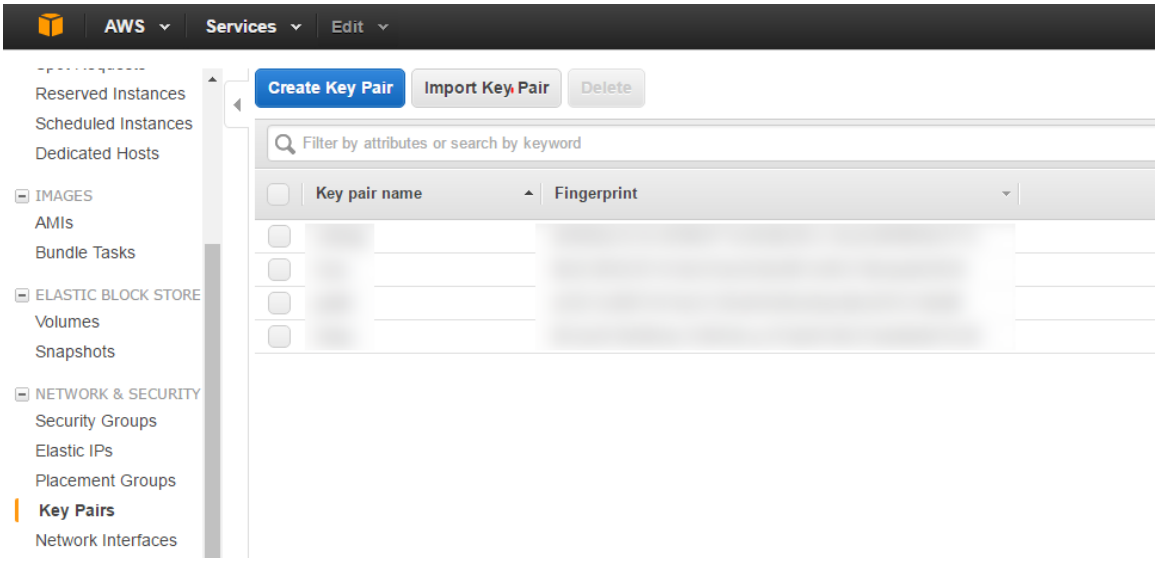
   Si la plantilla **CentOS 6 (x86_64) - with Updates HVM** está en un **estado de instancia detenida**, cambie el estado de la instancia de **Detener** a **Iniciar**.
3. Seleccione **Iniciar instancia**.



Crear un par de claves

Para crear un par de claves, siga estos pasos:

1. Seleccione **Servicios de EC2**.
2. En el panel izquierdo, seleccione **Pares de claves** bajo **Red y seguridad**.
3. Seleccione **Crear par de claves** e ingrese el nombre del par de claves.



4. Después de ingresar el nombre del par de claves, el archivo **<keypair name>.pem** se descarga en la máquina.
5. Utilice un cliente de otros fabricantes, como PuTTygen, para generar el **Archivo de clave privada puTTy** (**.ppk**). Este archivo se usa para conectarse a una instancia de AWS mediante el protocolo SSH o WinSCP.

Para obtener instrucciones detalladas sobre cómo configurar el servicio de recopilación remota de registros en el ambiente Amazon Web Services (AWS), consulte Paso 2: Configurar el servicio Remote Log Collector

Para obtener instrucciones detalladas sobre cómo implementar el servicio de recopilación remota de registros en el ambiente Amazon Web Services (AWS), consulte Paso 3: Implementar el servicio Remote Log Collector en AWS

Paso 2: Configurar el servicio Remote Log Collector

En este tema se indica cómo configurar el servicio de recopilación remota de registros en un ambiente Amazon Web Services (AWS).

Una vez que haya descargado la plantilla CentOS 6 (x86_64) - with Updates HVM y creado una instancia, en el próximo paso de configuración debe elegir una imagen de máquina de Amazon (AMI) y un tipo de instancia.

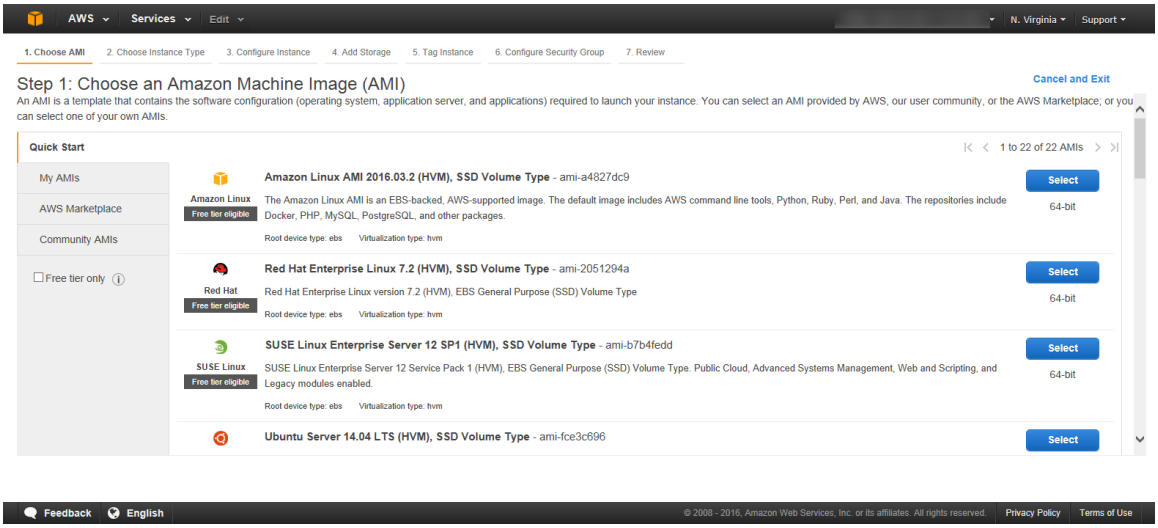
Nota: Solo debe descargar la plantilla CentOS 6 (x86_64) - with Updates HVM una vez y puede utilizarla posteriormente para crear varias instancias.

Elegir una imagen de máquina de Amazon

Una AMI es una plantilla que contiene la configuración de software necesaria para iniciar una instancia.

Realice los siguientes pasos para elegir un tipo de instancia.

1. Seleccione una AMI en la lista que se muestra en la pantalla.
2. Haga clic en el botón **Seleccionar** para completar su selección.



Elegir un tipo de instancia

Un tipo de instancia consta de diversas combinaciones de capacidad de CPU, memoria, almacenamiento y red que brindan la flexibilidad para elegir una combinación adecuada de recursos para sus aplicaciones. Cada tipo de instancia incluye uno o más tamaños de instancia que le permiten escalar sus recursos a los requisitos de su carga de trabajo.

Realice los siguientes pasos para elegir un tipo de instancia.

1. Seleccione un tipo de instancia en la lista desplegable.
2. Seleccione **Generación actual** o **Todas las generaciones** en la lista desplegable.

   Para obtener información detallada, consulte las siguientes tablas.

   Para obtener el mejor rendimiento, Amazon Web Services recomienda usar los tipos de instancia de la **generación actual** cuando se inician nuevas instancias.

   Amazon Web Services ofrece instancias de la **generación anterior** a los usuarios que optimizaron sus aplicaciones en torno a ellas y que aún deben actualizarlas.
3. Seleccione **Siguiente: Configurar los detalles de la instancia**.

En la siguiente tabla se describen los campos que se muestran en la figura anterior.

Campo	Descripción
Familia	Una agrupación de tipo de instancia general que utiliza capacidad de almacenamiento o CPU.
Tipo	Una especificación que define la capacidad de memoria, CPU y almacenamiento, así como el costo por hora de una instancia. Algunos tipos de instancia están diseñados para aplicaciones estándares, mientras que otros lo están para aplicaciones con un alto consumo de CPU y memoria.
vCPU	La cantidad de CPU virtuales para la instancia.
Memory (GiB)	La cantidad de memoria que se utiliza para la instancia.
Almacenamiento de la instancia (GB)	Los volúmenes del área de almacenamiento de la instancia local que están disponibles para la instancia. Los datos de un área de almacenamiento de instancia no son permanentes; solo persisten el tiempo que dura la instancia.

Campo	Descripción
Optimizada para EBS	Indica si el tipo de instancia es compatible con la optimización de EBS. Una instancia optimizada para EBS proporciona rendimiento adicional y exclusivo para los I/O de Amazon EBS. Esto ofrece un mejor rendimiento de los volúmenes de Amazon EBS y permite que las instancias utilicen los IOPS aprovisionados por completo.
Rendimiento de la red	Indica el nivel de rendimiento de la velocidad de transferencia de datos.

En la siguiente tabla se indican las especificaciones recomendadas para el CPU, la memoria y el tamaño de disco para Remote Log Collector en función de los eventos por segundo (EPS).

Tasa	Cantidad de CPU	RAM	Disco
30,000 EPS	8	15 GB	150 GB
15,000 EPS	4	7.5 GB	150 GB
2,500 EPS	2	3.75 GB	150 GB

Configurar los detalles de la instancia

Realice los siguientes pasos para configurar los detalles de la instancia. Consulte las descripciones detalladas en la siguiente tabla.

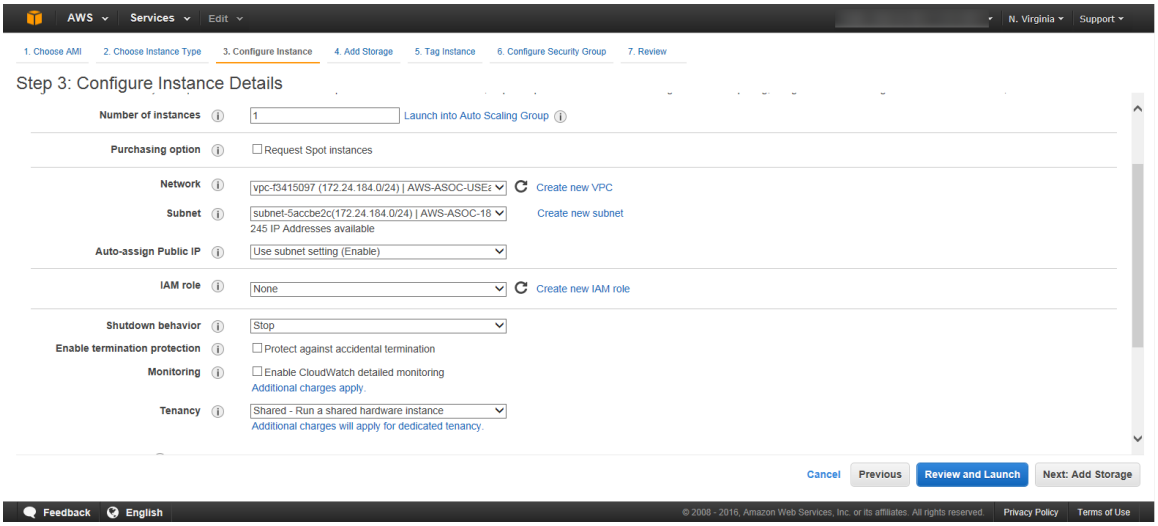
Nota: Consulte al administrador de AWS las selecciones adecuadas de Configurar instancia.

1. Seleccione **Cantidad de instancias** en la lista desplegable.

   Nota: Puede iniciar más de una instancia por vez.

2. (Opcional) En la opción **Compra**, seleccione la casilla de verificación **Solicitar instancias de subasta**.
3. Seleccione una **Red** en la lista desplegable.
4. Seleccione una **Zona de disponibilidad** en la lista desplegable.
5. Seleccione una **Función de IAM** en la lista desplegable.
   Tenga en cuenta que el valor predeterminado es **Ninguno**.
6. Seleccione **Comportamiento en apagado** en la lista desplegable.

7. (Opcional) En **Habilitar protección de terminación**, seleccione la casilla de verificación **Protección contra la terminación accidental**.
8. (Opcional) En **Monitoreo**, seleccione la casilla de verificación **Habilitar monitoreo detallado de CloudWatch**.
9. Haga clic en **Siguiente: Agregar almacenamiento**.



En la siguiente tabla se proporciona información relacionada con las diversas opciones de configuración de la instancia.

Campo	Descripción
Cantidad de instancias	Ingrese la cantidad de instancias que desea configurar. Tenga en cuenta que puede configurar más de una instancia por vez.
(Opcional) Opción Compra: Solicitar instancias de subasta	Las instancias de subasta permiten hacer ofertas por instancias de EC2 sin uso, lo cual puede disminuir considerablemente los costos de Amazon EC2. Amazon EC2 establece el precio por hora de una instancia de subasta (de cada tipo de instancia en cada zona de disponibilidad), y este varía conforme a la oferta y la demanda de instancias de subasta. La instancia de subasta se ejecuta cada vez que su oferta supera el precio de mercado actual. Seleccione esta opción de compra si puede admitir flexibilidad en relación con la ejecución de sus aplicaciones y si estas se pueden interrumpir, como cuando se ejecutan trabajos por lotes y tareas de procesamiento en segundo plano.

Campo	Descripción
Red	La selección de una red le permite iniciar su instancia en Amazon Virtual Private Cloud (VPC). Puede crear una VPC y seleccionar su propio rango de direcciones IP, crear subredes, configurar tablas de enrutamiento y configurar gateways de red.
Subred	Un rango de direcciones IP en su VPC que se puede usar para aislar distintos recursos de EC2 entre sí o de Internet. Cada subred reside en una zona de disponibilidad.
Zona de disponibilidad (el valor predeterminado es sin preferencia)	Una ubicación diferente dentro de una región que está diseñada para estar aislada en caso de fallas de otras zonas de disponibilidad, la cual proporciona conectividad de red económica y de baja latencia para otras zonas de disponibilidad de la misma región.
Seleccione una función de IAM (el valor predeterminado es ninguna)	Una función de IAM es una identidad de AWS con políticas de permisos que determinan lo que la identidad puede y no puede hacer en AWS. En lugar de estar asociada únicamente a una persona, cualquier persona que necesite una función puede adoptarla. Además, una función no tiene credenciales (contraseña o claves de acceso) asociadas. Si se asigna una función a un usuario, se crean claves de acceso de forma dinámica y se le proporcionan.
Comportamiento en apagado	Especifique el comportamiento de la instancia cuando se lleva a cabo un apagado en el nivel del sistema operativo. Las instancias se pueden finalizar o detener.
(Opcional) Habilitar protección de terminación	Puede proteger las instancias contra la terminación accidental. Cuando se habilite, no podrá terminar esta instancia a través de la API ni de la consola de administración de AWS hasta que la protección de terminación se haya deshabilitado.

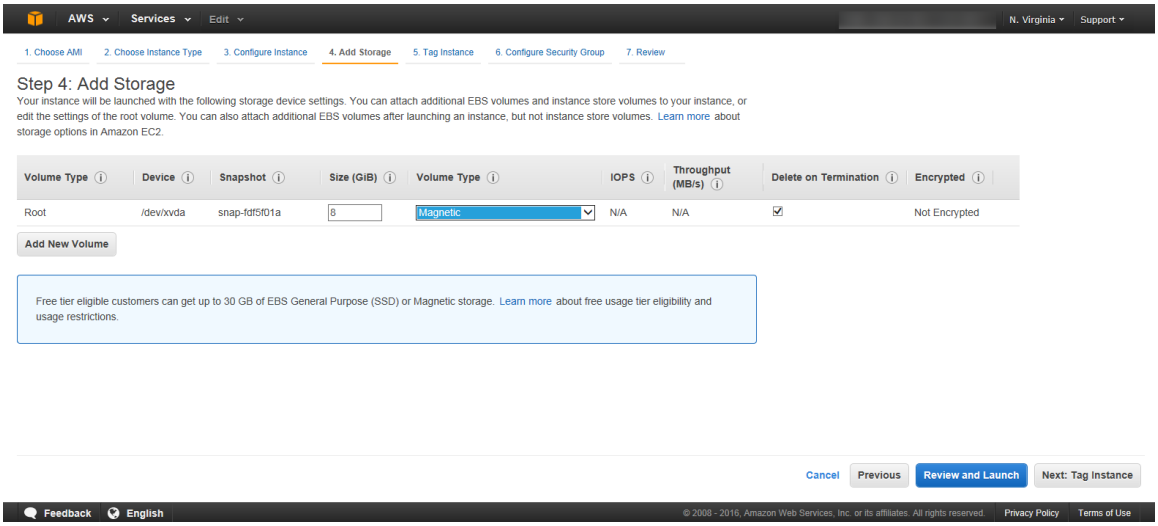
Campo	Descripción
(Opcional) Monitoreo: Habilitar monitoreo detallado de CloudWatch	Permite monitorear, recopilar y analizar métricas sobre sus instancias mediante Amazon CloudWatch. Si habilita esta opción, se aplican cargos adicionales.
Grupos de usuarios	Puede optar por ejecutar sus instancias en servidores físicos completamente exclusivos para su uso. El uso de grupos de usuarios de host le exige iniciar instancias en hosts exclusivos, mientras que con el uso de grupos de usuarios exclusivos, las instancias se iniciarán como instancias exclusivas. Puede iniciar una instancia con un grupo de usuarios de host o de manera exclusiva en una Amazon Virtual Private Cloud (VPC) exclusiva.

Agregar almacenamiento

Amazon EC2 permite asignar opciones flexibles de almacenamiento de datos para sus instancias.

Realice los siguientes pasos para configurar los ajustes de almacenamiento para su instancia:

1. Ingrese el tamaño del almacenamiento en el campo **Tamaño**.
   El tamaño del volumen debe ser mayor que cero o que el tamaño del snapshot utilizado. Los volúmenes de IOPS (disco SSD) aprovisionados deben tener un tamaño de al menos 4 GB.
2. Seleccione **Tipo de volumen magnético** en la lista desplegable.
3. Haga clic en **Siguiente: Etiquetar instancia**.



En la siguiente tabla se describen los campos de la pantalla Agregar almacenamiento.

Campo	Descripción
Tipo	Amazon EBS es un volumen de almacenamiento de nivel de bloque que persiste de manera independiente de la duración de una instancia de EC2, de modo que puede detener y reiniciar la instancia con posterioridad. Los volúmenes de área de almacenamiento de instancias efímeras se conectan físicamente a la computadora host. Los datos de un área de almacenamiento de instancia persisten solo mientras dura la instancia.
Dispositivo	Los nombres de dispositivo disponibles para el volumen. Según el controlador del dispositivo de bloques del kernel de AMI seleccionado, el dispositivo se puede conectar con un nombre diferente al que usted especifica.
Snapshot	Un snapshot es un respaldo de un volumen de EC2 que se almacena en S3. Puede crear un volumen nuevo mediante los datos almacenados en un snapshot si ingresa el ID del snapshot Puede buscar snapshots públicos si escribe texto en el campo Snapshot. Las descripciones distinguen mayúsculas de minúsculas.
Tamaño	El tamaño del volumen debe ser mayor que cero o que el tamaño del snapshot utilizado. Los volúmenes de IOPS (disco SSD) aprovisionados deben tener un tamaño de al menos 4 GB.
Tipo de volumen	Los volúmenes magnéticos ofrecen un promedio de 100 IOPS y pueden brindar ráfagas de hasta cientos de IOPS. Esta es una opción de bajo costo recomendada. Los volúmenes de Uso general (disco SSD) pueden brindar picos de hasta 3,000 IOPS y ofrecen una base constante de 3 IOPS/GB. Los volúmenes de IOPS (disco SSD) aprovisionados pueden ofrecer hasta 20,000 IOPS y son más aptos para las instancias optimizadas para EBS.

Campo	Descripción
IOPS	**Nota:** Los requisitos que se enumeran a continuación no se requieren para los volúmenes magnéticos recomendados. La cantidad solicitada de IOPS compatible con el volumen. Para los volúmenes de IOPS (disco SSD) aprovisionados, puede aprovisionar un máximo de 30 IOPS por GB. Para los volúmenes de uso general (disco SSD) de menos de 1,000 GB, se obtiene un rendimiento de base de 3 IOPS por GB con picos de hasta 3,000 IOPS. Para los volúmenes de uso general (disco SSD) de más de 1,000 GB, se obtiene un rendimiento de base de 3 IOPS por GB hasta un máximo de 10,000 IOPS.
Eliminar tras terminación	Los volúmenes de EBS persisten de manera independiente del ciclo de vida de ejecución de una instancia de EC2. Sin embargo, puede optar por eliminar automáticamente un volumen de EBS cuando se termina la instancia asociada.
Cifrado	Los volúmenes que se crean a partir de snapshots cifrados se cifran automáticamente y aquellos que se crean a partir de snapshots sin cifrar se descifran automáticamente. Si no se selecciona ningún snapshot, puede optar por cifrar el volumen.

Configurar la etiqueta de la instancia

Una etiqueta permite administrar las instancias y consta de un par clave-valor que distingue mayúsculas de minúsculas.

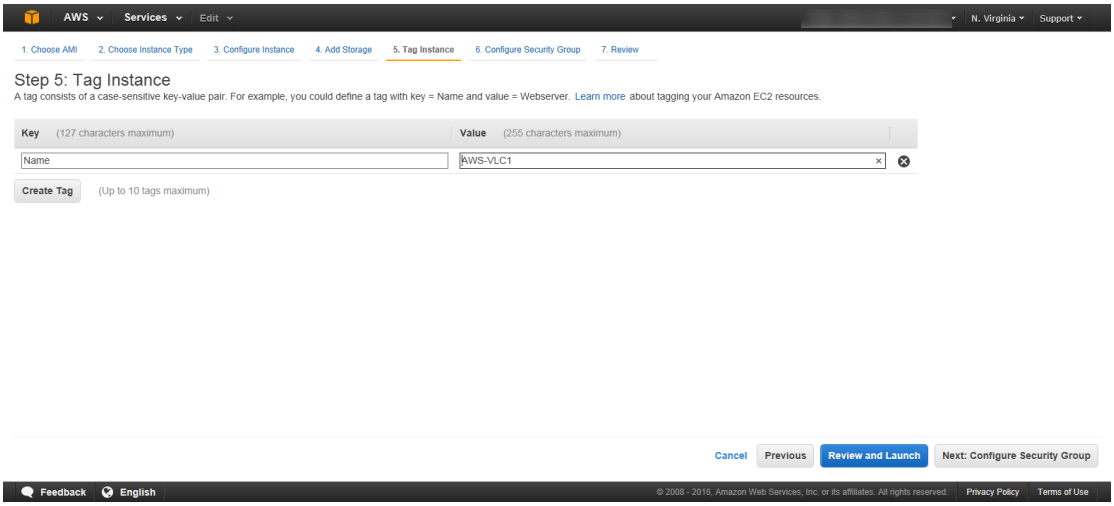
Realice los siguientes pasos para configurar una etiqueta de instancia.

1. Ingrese un nombre y un valor, como **AWS-VLC1**.

   Las siguientes restricciones se aplican a las etiquetas:

   - Las claves y los valores de las etiquetas distinguen mayúsculas de minúsculas.
   - La cantidad máxima de etiquetas por recurso es **10**.
   - La longitud máxima de la clave es **127 caracteres Unicode en UTF-8**.
   - La longitud máxima del valor es **255 caracteres Unicode en UTF-8**.
   - Evite usar el prefijo **aws:** en los nombres y los valores de las etiquetas, ya que su uso está reservado para Amazon Web Services.

2. Haga clic en **Siguiente: Configurar el grupo de seguridad**.



Configurar el grupo de seguridad

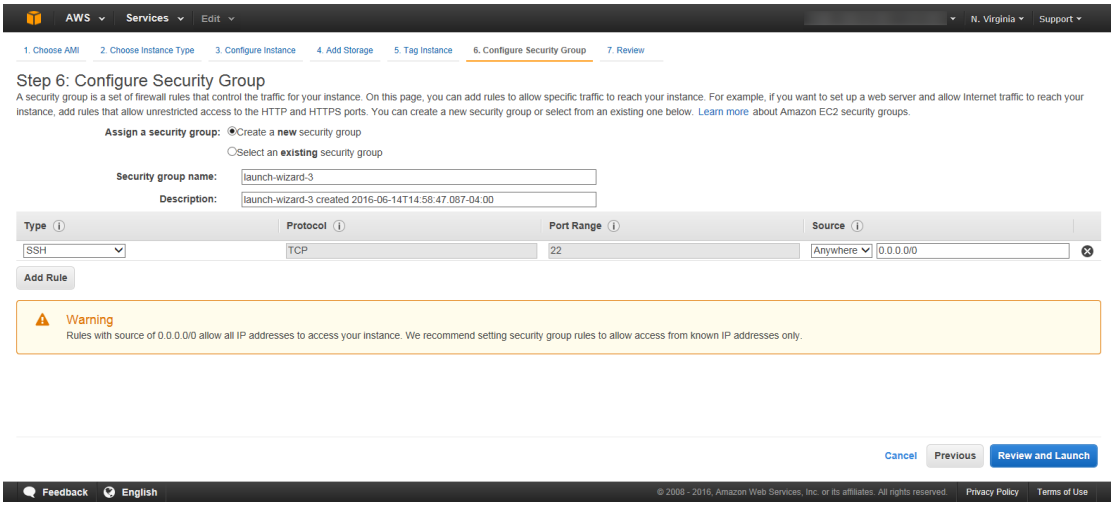
Puede configurar un grupo de seguridad, el cual actúa como un firewall virtual que controla el tráfico de una o más instancias. Puede agregar reglas a su grupo de seguridad, las cuales permiten tráfico hacia y desde sus instancias asociadas.

Campo	Descripción
Tipo	El protocolo para abrirse al tráfico de red. Puede elegir un protocolo común, como el protocolo SSH (para una instancia de Linux) y RDP (para una instancia de Windows), así como HTTP y HTTPS para permitir que el tráfico de Internet llegue a su instancia. También puede ingresar manualmente un puerto personalizado o rangos de puertos.
Protocolo	El tipo de protocolo; por ejemplo, TCP o UDP. Brinda una selección adicional para ICMP.
Rango de puertos	Para las reglas y los protocolos personalizados, puede ingresar manualmente un número de puerto o un rango de puertos. Consulte la siguiente tabla para obtener una lista de puertos de servicio.

Campo	Descripción
Source	Determina el tráfico que puede llegar a su instancia. Especifique una única dirección IP o un rango de direcciones IP en notación CIDR (por ejemplo, **203.0.113.5/32**). Si se conecta detrás de un firewall, necesita el rango de direcciones IP que usan las computadoras cliente. Puede especificar el nombre o el ID de otro grupo de seguridad de la misma región. Para especificar un grupo de seguridad en otra cuenta de AWS (solo EC2-Classic), use como prefijo el ID de cuenta y una barra diagonal; por ejemplo: **111122223333/OtherSecurityGroup**.

Realice los siguientes pasos para crear un grupo de seguridad.

1. Seleccione **Crear un nuevo grupo de seguridad** o **Seleccionar un grupo de seguridad existente**.
2. Seleccione un **tipo de protocolo** en la lista desplegable.
3. Ingrese un **protocolo**.
4. Especifique un **rango de puertos**.
5. Haga clic en **Revisar** e **Iniciar**.



Nota: El grupo de seguridad en AWS debe configurar puertos entrantes y salientes conectados a Remote Log Collector.

Categoría	Protocolo	Número de puerto	Dispositivos	Dirección

Protocolo SSH	TCP	22	Remote Log Collector (AWS)	Entrante
RabbitMQ	TCP	15671	Remote Log Collector (AWS)	Entrante y saliente
AMQP	TCP	5671/5672	Remote Log Collector (AWS) hacia y desde Remote Log Collector (corporativo)	Entrante y saliente
Puppet	TCP	8140	Remote Log Collector (AWS) hacia el servidor de Security Analytics	Saliente
Log Collector	TCP	50001/56001	Remote Log Collector (AWS) hacia y desde el servidor de Security Analytics	Entrante y saliente
Syslog	TCP	514	Origen de eventos hacia Remote Log Collector (AWS)	Entrante
Syslog	UDP	514	Origen de eventos hacia Remote Log Collector (AWS)	Entrante
Flujo de red	UDP	9995	Origen de eventos hacia Remote Log Collector (AWS)	Entrante
SNMP	UDP	162	Origen de eventos hacia Remote Log Collector (AWS)	Entrante
Windows	TCP	5985	Remote Log Collector (AWS) hacia el origen de eventos	Saliente Saliente

ODBC	TCP	Varios	Remote Log Collector (AWS) hacia el origen de eventos	Saliente
SDEE	TCP	443	Remote Log Collector (AWS) hacia el origen de eventos	Saliente

Configurar los permisos de firewall para permitir la comunicación

Configure el o los firewalls para permitir la comunicación entre Remote Log Collector y AWS, y los componentes de NetWitness que se enumeran en la tabla anterior.

Nota: Es necesario abrir puertos entre el Remote Log Collector y el servidor de Security Analytics, y también entre el Log Collector en el Log Decoder.

En la siguiente tabla se muestran los hosts de Security Analytics y sus respectivos puertos de servicio:

De host	A Local Collector en AWS	A puertos (protocolo)	Comentarios
Servidor de Security Analytics	Remote Log Collector	56001 (TCP) o 50001 (TCP)	SSL No SSL
Servidor de Security Analytics	Remote Log Collector	50101	REST (Opcional)
Servidor de Security Analytics	Remote Log Collector	5672 (TCP)	RabbitMQ
Servidor de Security Analytics	Remote Log Collector	50055 (TCP)	RSA-SMS
Servidor de Security Analytics	Remote Log Collector	50056 (TCP)	RSA-SMS
Remote Log Collector	Servidor de Security Analytics	8140 (TCP)	Puppet

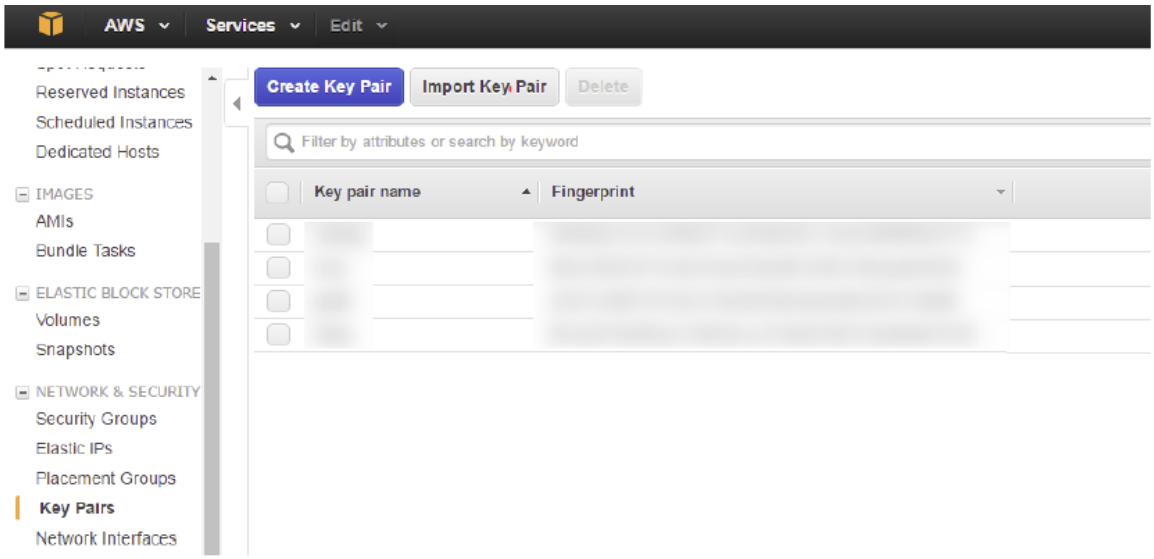
De host	A Local Collector en AWS	A puertos (protocolo)	Comentarios
Servidor de Security Analytics	Remote Log Collector	61614 (TCP)	MCollective
Remote Log Collector	Servidor de Security Analytics	61614 (TCP)	MCollective
Servidor de Security Analytics	Remote Log Collector	15671 (TCP)	Puppet
Remote Log Collector	Servidor de Security Analytics	15671 (TCP)	Puppet
En el modo de extracción:			
Log Collector (en Log Decoder)	Remote Log Collector	5671 (TCP)	RabbitMQ
En el modo de migración:			
Remote Log Collector	Log Collector (en Log Decoder)	5671 (TCP)	RabbitMQ

El vínculo general que indica qué puertos deben estar abiertos en qué dispositivo se puede encontrar en https://community.rsa.com/docs/DOC-54917.

Revisar inicio de instancia

Antes de completar el proceso de inicio de la instancia, tiene la oportunidad de revisar y editar su AMI. Si no desea realizar cambios en su AMI, seleccione **Iniciar**. Si selecciona **Editar AMI**, puede realizar cambios y elegir **Iniciar** después de completarlos.

Después de seleccionar **Iniciar**, se muestra el siguiente cuadro de diálogo en la pantalla.



Cuando inicia una instancia, debe especificar el nombre del par de claves que piensa usar para conectarse a esta. Si no especifica el nombre de un par de claves existente cuando inicia una instancia, no podrá conectarse a la instancia. Cuando se conecta a la instancia, debe especificar la clave privada que corresponde al par de claves que especificó cuando inició la instancia.

Haga clic en **Iniciar instancias** para completar el **proceso de inicio de la instancia**.

Consulte Paso 3: Implementar el servicio Remote Log Collector en AWS para obtener instrucciones detalladas sobre cómo implementar un servicio de recopilación remota de registros en un ambiente AWS.

Paso 3: Implementar el servicio Remote Log Collector en AWS

En este tema se indica cómo implementar el servicio de recopilación remota de registros en un ambiente AWS mediante scripts automatizados y también cómo implementarlo manualmente.

Uso de scripts para implementar el servicio Remote Log Collector

Después de configurar el servicio Remote Log Collector, debe implementarlo en una máquina virtual (VM) mediante los pasos que se proporcionan a continuación.

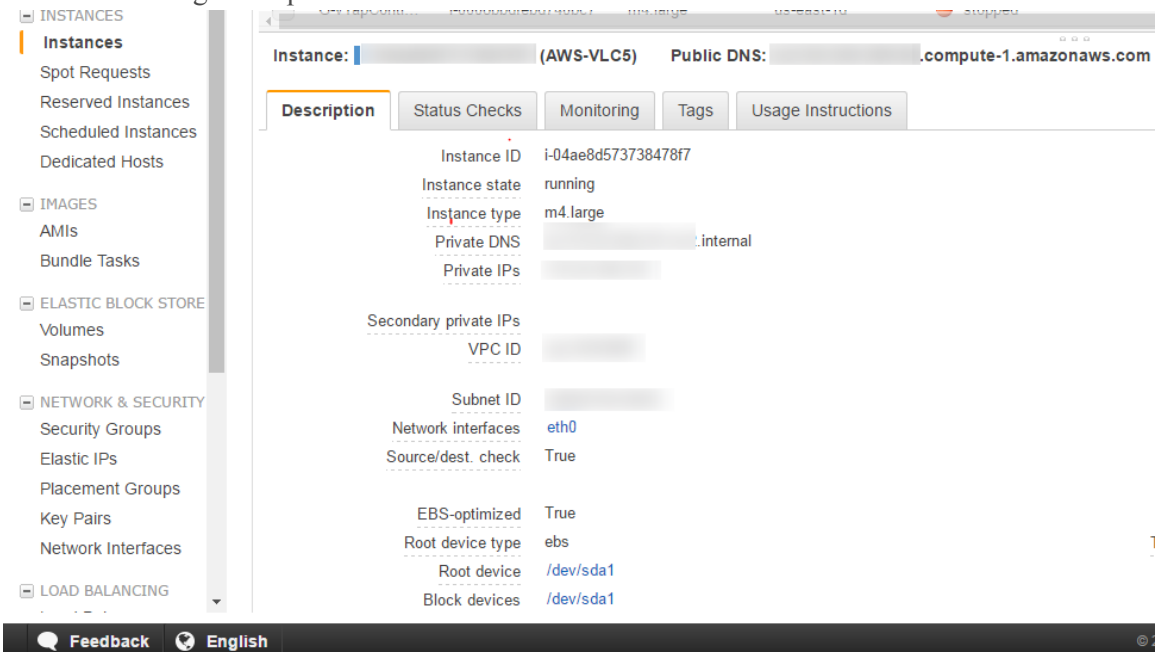
Nota: Se recomienda usar scripts. Si está utilizando scripts, siga los pasos que se señalan a continuación. O bien, para implementar manualmente el servicio Remote Log Collector, consulte los pasos de la sección **Implementar manualmente el servicio Remote Log Collector**.

Iniciar sesión mediante el protocolo SSH

Antes de descargar scripts, debe acceder a la máquina virtual mediante el protocolo SSH después de encontrar la dirección IP a través de los siguientes pasos.

1. Para obtener la dirección IP, seleccione el nombre de la instancia virtual implementada.
2. En la pestaña **Descripción**, ingrese la dirección IP privada de esa instancia virtual específica.

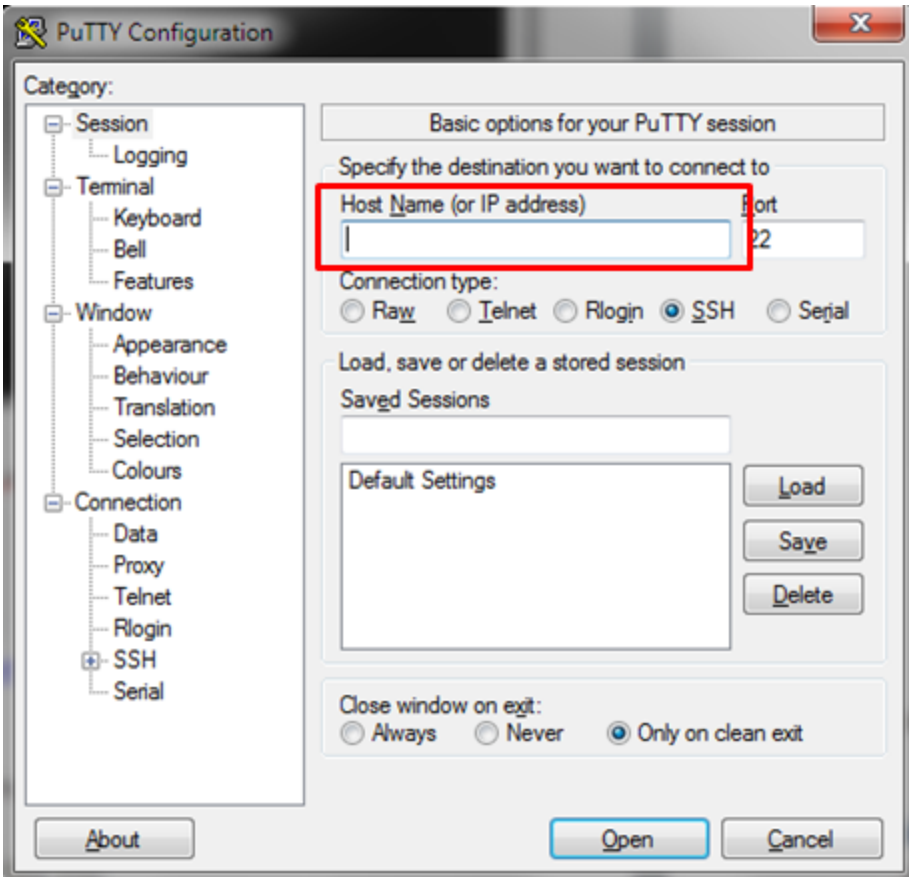
Se muestra la siguiente pantalla.



2. Acceda a la instancia virtual mediante el protocolo SSH a través de un cliente de este protocolo, como PuTTY. Se proporcionan instrucciones para PuTTY, pero puede utilizar cualquier cliente del protocolo SSH.
3. Si está usando PuTTY, ejecute el siguiente comando para conectarse a un Remote Log Collector:

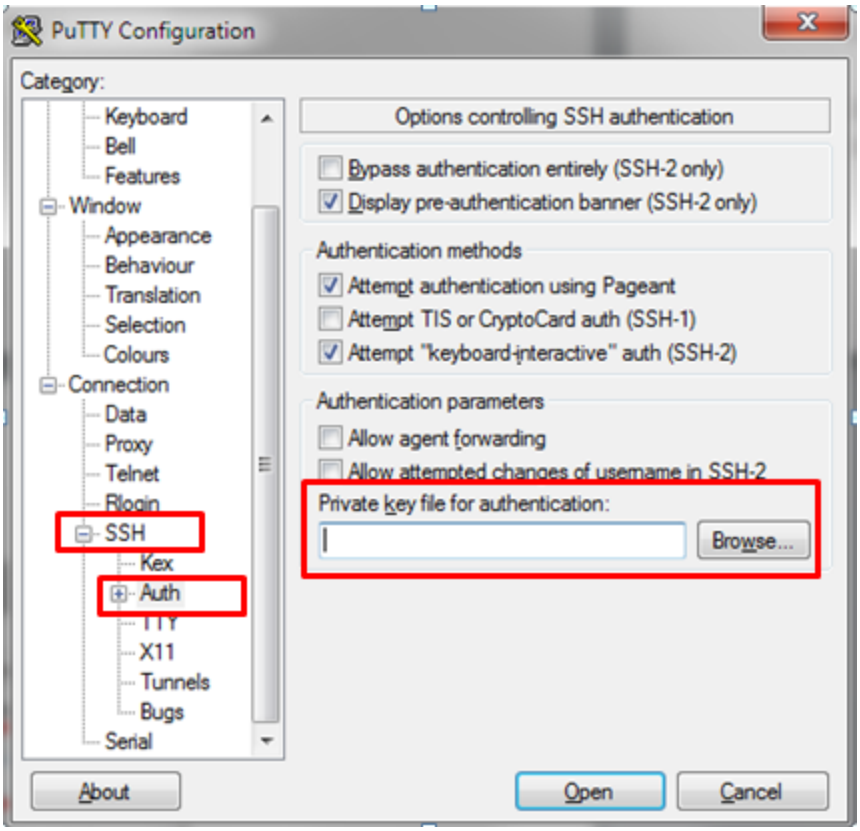
   ```
   putty.exe
   ```

Se muestra la siguiente pantalla.



3. Ingrese la dirección IP. Debe usar la dirección IP privada de la pantalla anterior.
4. En **Tipo de conexión**, seleccione **Protocolo SSH**.
5. Haga clic en **Abrir**.

Se muestra la siguiente pantalla.



7. Seleccione **Conexión > protocolo SSH > Autenticación**.
8. Seleccione **Navegar** para buscar el archivo de **Clave privada**.
9. Haga clic en **Abrir** para conectarse a la instancia virtual.

Deshabilitar el repositorio base de CentOS

Para deshabilitar el repositorio base de CentOS:

1. Ejecute el siguiente comando:
   ```
   sudo vi /etc/yum.repos.d/CentOS-Base.repo
   ```
2. Asegúrese de que en el contenido del archivo **CentOS-Base.repo** en el directorio **/etc/yum.repos** se incluyan secciones con **enabled=0**
   El contenido del archivo debe ser similar al siguiente ejemplo:
   ```
   [base]
   name=CentOS-$releasever - Base
   mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$ba
   search&repo
   =os
   #baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
   gpgcheck=1
   ```

```
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
enabled=0
```

Descargar los scripts de AWS

Nota: Cada script requiere que ingrese sus credenciales de nombre de usuario y contraseña en https://community.rsa.com.

Puede descargar los scripts de AWS a su máquina desde las siguientes ubicaciones:

aws_vlc_preinstall.sh - https://community.rsa.com/docs/DOC-53180
aws_vlc_postinstall.sh - https://community.rsa.com/docs/DOC-53201
aws_vlc_start_services.sh - https://community.rsa.com/docs/DOC-53202

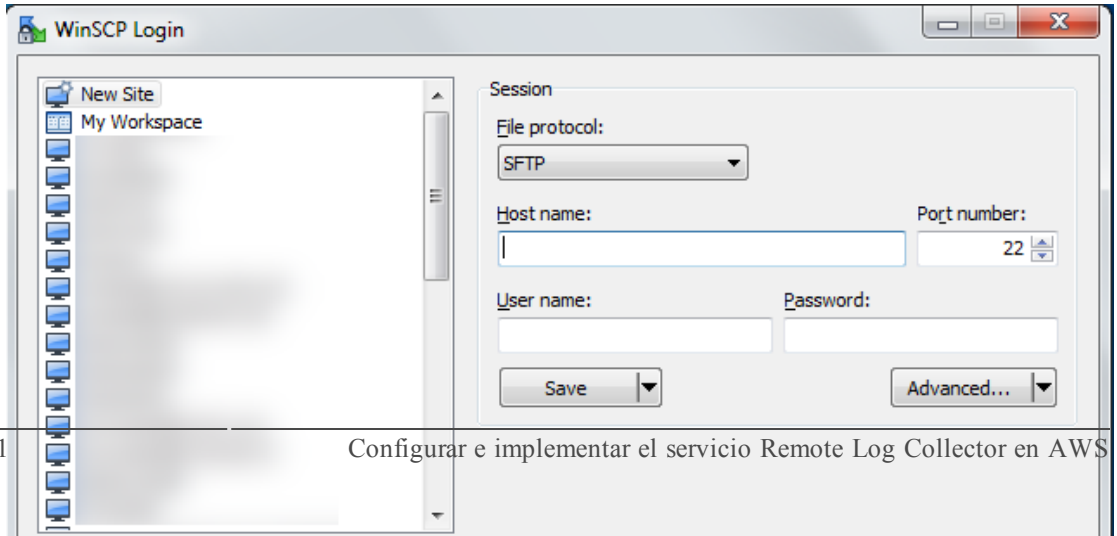
Instrucciones de WinSCP para copiar los scripts descargados

Cuando haya descargado los scripts de AWS a la máquina local, debe acceder a la máquina virtual mediante SFTP a través de un cliente SFTP, como WinSCP, de modo que pueda transferir los scripts al Log Collector de AWS.

Para conectarse a una instancia de la máquina virtual con SFTP, inicie WinSCP mediante las instrucciones que se presentan a continuación.

En el cuadro de diálogo de inicio de sesión de WinSCP:

1. Asegúrese de que la opción **Nuevo nodo de sitio** esté seleccionada.
2. En el campo **Nuevo nodo de sitio**, seleccione el protocolo **SFTP**.
3. Ingrese el **Nombre de host**.
4. Ingrese el nombre de usuario predeterminado.
5. Deje el campo de contraseña en blanco.
6. Haga clic en el botón **Guardar** para guardar la configuración.
7. Haga clic en el botón **Conectar** para iniciar sesión.
8. Verifique la clave del host, para lo cual debe consultar la clave que creó en la sección **Crear un par de claves** del Paso 1: Iniciar sesión en AWS y crear una instancia.



9. Copie los scripts que descargó desde la laptop al directorio principal del Remote Log Collector.
10. Utilice las instrucciones del protocolo SSH para acceder a la máquina de AWS mediante este protocolo, como se describe en la sección Iniciar sesión mediante el protocolo SSH.
11. Cambie el usuario al directorio principal mediante el siguiente comando:
    ```
    cd ~
    ```
12. Utilice el siguiente comando para proporcionar permisos de ejecución antes de ejecutar estos scripts:
    ```
    sudo chmod +x aws_vlc_preinstall.sh
    sudo chmod +x aws_vlc_preinstall.sh
    sudo chmod +x aws_vlc_start_services.sh
    ```

Configurar los permisos de firewall para permitir la comunicación

Nota: Es necesario abrir puertos entre el Remote Log Collector y el servidor de Security Analytics, y también entre el Log Collector en el Log Decoder.

Configure el o los firewalls para permitir la comunicación entre Remote Log Collector y AWS, y los componentes de NetWitness que se enumeran en la siguiente tabla.

De host	A host	A puertos (protocolo)	Comentarios
Servidor de Security Analytics	Remote Log Collector	56001 (TCP) o 50001 (TCP)	SSL o No SSL
Servidor de Security Analytics	Remote Log Collector	50101 (TCP)	REST (opcional)
Servidor de Security Analytics	Remote Log Collector	5672 (TCP)	RabbitMQ
Servidor de Security Analytics	Remote Log Collector	50055 (TCP)	RSA-SMS
Servidor de Security Analytics	Remote Log Collector	50056 (TCP)	RSA-SMS
Remote Log Collector	Servidor de Security Analytics	8140 (TCP)	Puppet

Servidor de Security Analytics	Remote Log Collector	61614 (TCP)	MCollective
Remote Log Collector	Servidor de Security Analytics	61614 (TCP)	MCollective
Servidor de Security Analytics	Remote Log Collector	15671 (TCP)	Puppet
Remote Log Collector	Servidor de Security Analytics	15671 (TCP)	Puppet
En el modo de extracción:			
Log Collector (en Log Decoder)	Remote Log Collector	5671 (TCP)	RabbitMQ
En el modo de migración:			
Remote Log Collector	Log Collector (en Log Decoder)	5671 (TCP)	RabbitMQ

Ejecutar los scripts de AWS

Para usar los scripts con el fin de configurar el servicio Remote Log Collector en AWS, realice los siguientes pasos.

1. Cambie al directorio principal mediante el siguiente comando:
   `cd ~`

Nota: Cada script requiere que ingrese sus credenciales de nombre de usuario y contraseña de la comunidad de RSA, como lo haría en https://community.rsa.com.

2. Configure un usuario raíz mediante los siguientes comandos:
   `sudo password root`
   `Passwd` (ingrese su contraseña y vuelva a escribirla)
3. Inicie sesión como **raíz** e ingrese el siguiente comando:
   `su root`
4. Ejecute el script **aws_vlc_preinstall.sh**.
   Este script crea un archivo **sa.repo** que instala toda las dependencias y los paquetes

requeridos.

Una vez que ejecuta el script, debe ingresar los siguientes tres parámetros como entrada:

-**Nombre de usuario de la cuenta de Live**

-Contraseña de la cuenta de Live

-**Versión** del Log Collector que desea instalar

5. Ejecute el script mediante el siguiente comando:
   `./aws_vlc_preinstall.sh`

5. Ejecute el script **aws_vlc_postinstall.sh**. Este script cambia el **Nombre de host** y permite configurar la dirección del servidor de Security Analytics.
   Debe ingresar dos parámetros como entrada: **Nombre de host** y **Dirección IP de Security Analytics**. Asegúrese de ingresar los parámetros de entrada entre comillas simples separadas por un espacio, como se muestra en el siguiente comando:
   `./aws_vlc_postinstall.sh '<hostname>' '<IP Address of the Security Analytics Server>'`

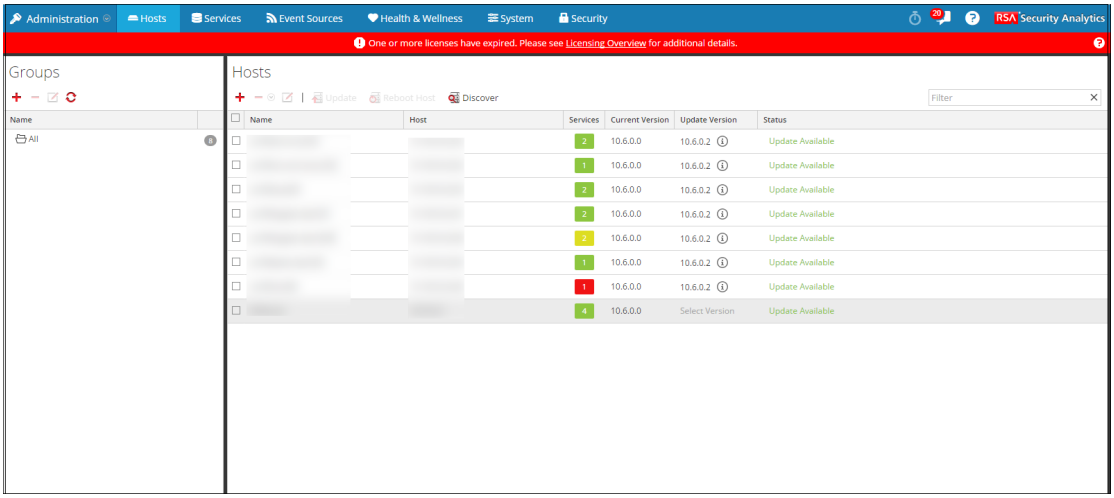
6. Vuelva a iniciar sesión en Remote Log Collector a medida que la máquina virtual se reinicia automáticamente después de la ejecución del script **aws_vlc_postinstall.sh**.

7. Después del reinicio de la máquina virtual, debe sincronizar la hora entre Remote Log Collector de AWS y el servidor de Security Analytics mediante los siguientes pasos:
   - Acceda a la máquina virtual mediante el protocolo SSH de acuerdo con las instrucciones que se proporcionan en

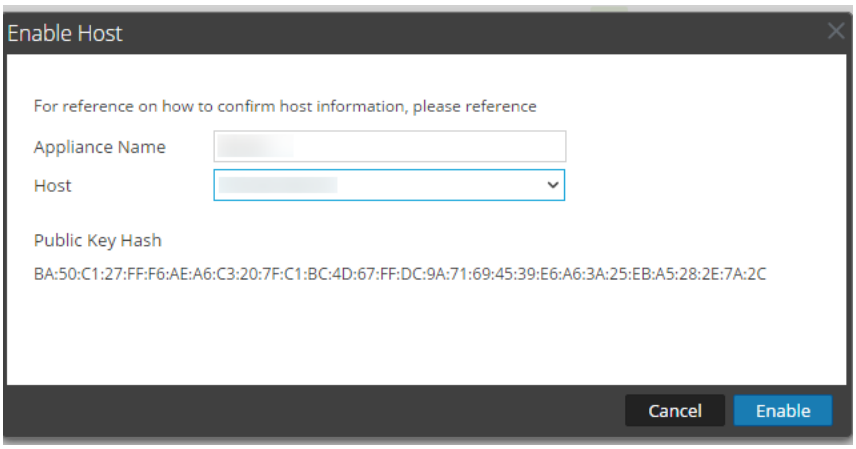
Sincronizar la hora

Después del reinicio de la máquina virtual, debe sincronizar la hora entre Remote Log Collector de AWS y el servidor de Security Analytics mediante los siguientes pasos:

1. Acceda a la máquina virtual mediante el protocolo SSH de acuerdo con las instrucciones que se proporcionan en Iniciar sesión mediante el protocolo SSH.
2. Cambie los usuarios al directorio principal mediante el siguiente comando:
   ```
   cd ~
   ```
3. Vuelva a iniciar sesión y ejecute el siguiente comando:
   ```
   su root
   ```
4. Para sincronizar la hora y la fecha entre el servicio de recopilación remota de registros de AWS y el servidor de Security Analytics, siga estos pasos:
   a. Obtenga la fecha y la hora actuales en el servidor de Security Analytics y en Remote Log Collector mediante la ejecución del siguiente comando.
   ```
   date
   ```
   b. Si la fecha y la hora no están sincronizadas, ejecute los siguientes comandos para establecerlas en Remote Log Collector de AWS:
   ```
   date --set="MM/DD/YYYY"
   date --set="HH:MM:SS"
   ```
5. Ejecute el script **aws_vlc_start_services.sh**. Este script inicia todos los servicios requeridos.
   ```
   ./aws_vlc_start_services.sh
   ```
6. Inicie sesión en el servidor de Security Analytics. En el menú de **Security Analytics**, vaya a **Administration > Hosts**.
7. Haga clic en **Descubrir**.



Cuando hace clic en **Descubrir**, se muestra la siguiente pantalla.



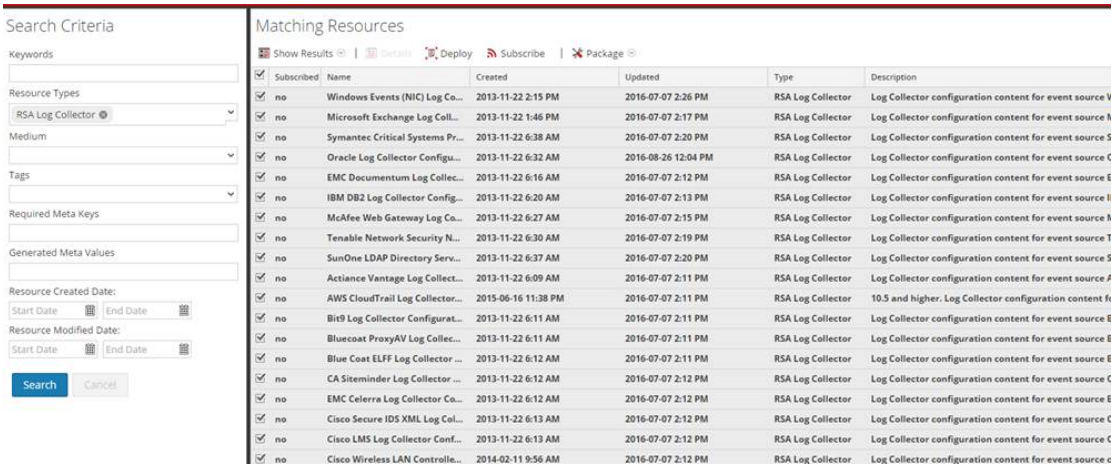
7. Seleccione un dispositivo y un host y, a continuación, haga clic en **Habilitar** para habilitar el dispositivo.

Nota: Consulte la sección **Solución de problemas** si se producen errores durante el aprovisionamiento.

Implementar el contenido de Log Collector

En el servidor de Security Analytics, debe implementar el Log Collector **nwlogcollectorcontent** en el Remote Log Collector (AWS) mediante Live.

1. En el menú de **Security Analytics**, seleccione **Live > Buscar**.
2. En el menú desplegable **Tipos de recursos**, seleccione **RSA Log Collector**.
3. Seleccione **Search**.



El Remote Log Collector (AWS) ahora debe estar operativo y esto se puede verificar en la página **Administration > Servicios**.

Para obtener más información, consulte la Guía de servicios de Live, disponible en RSA Link en la siguiente ubicación:

https://community.rsa.com/docs/DOC-41548.

Implementar manualmente el servicio Remote Log Collector

Para implementar manualmente el servicio Remote Log Collector, siga estos pasos.

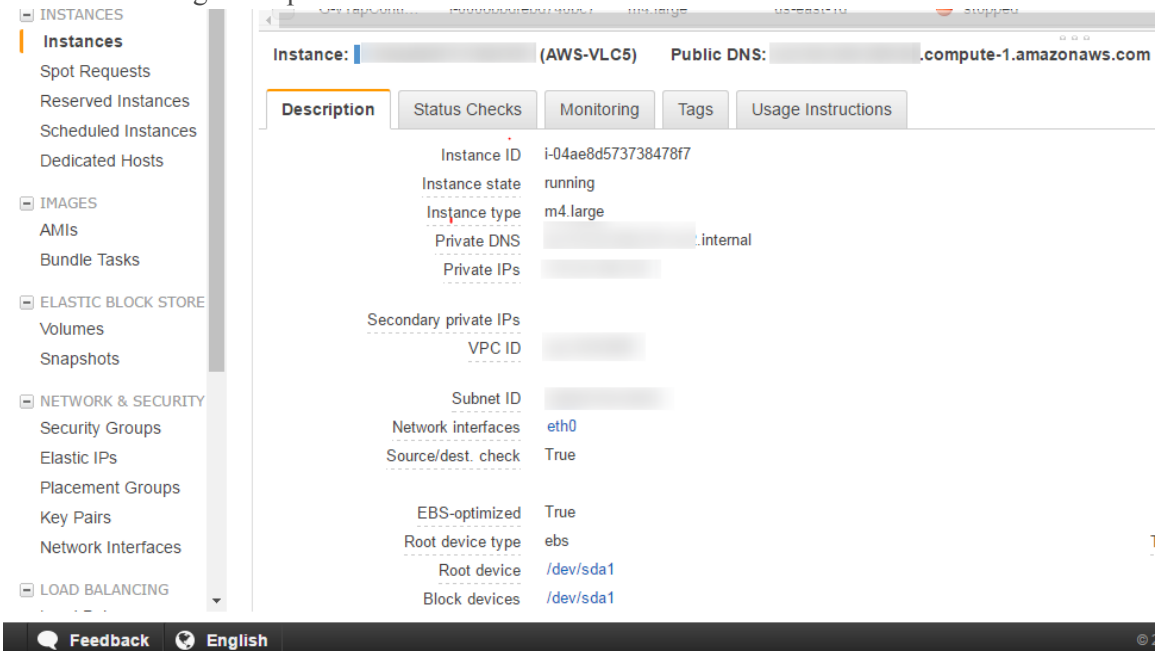
Nota: Se recomienda la implementación mediante el script.

Iniciar sesión mediante el protocolo SSH

Antes de descargar scripts, debe acceder a la máquina virtual mediante el protocolo SSH después de encontrar la dirección IP a través de los siguientes pasos.

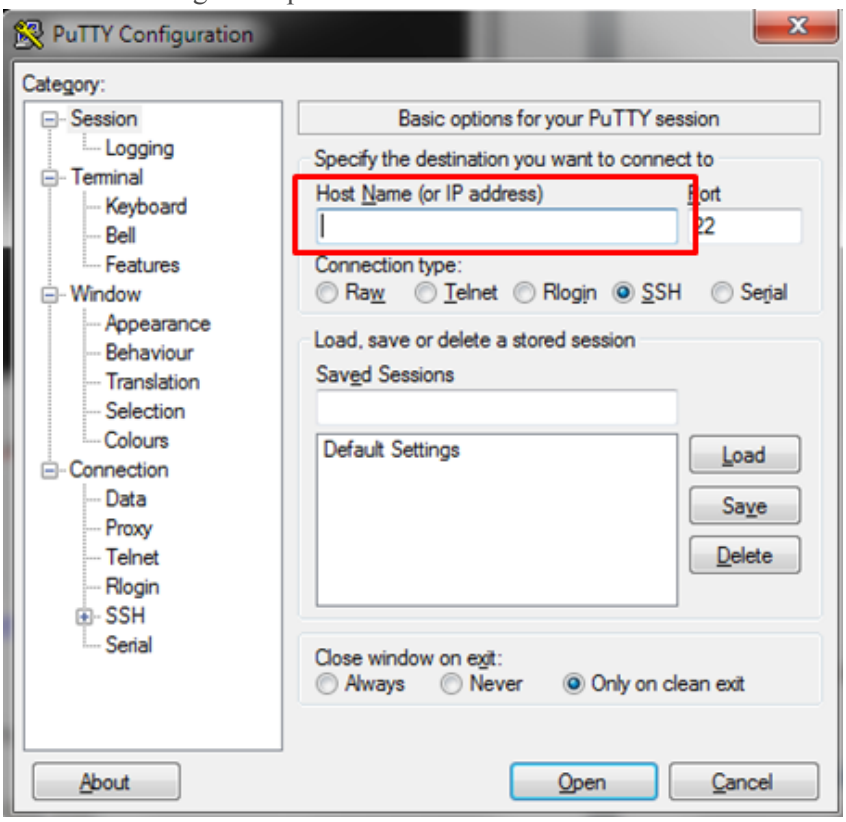
1. Para obtener la dirección IP, seleccione el nombre de la instancia virtual implementada.
2. Una vez que selecciona la instancia virtual, en la pestaña **Descripción**, seleccione la dirección IP privada de esa instancia virtual específica.

Se muestra la siguiente pantalla.



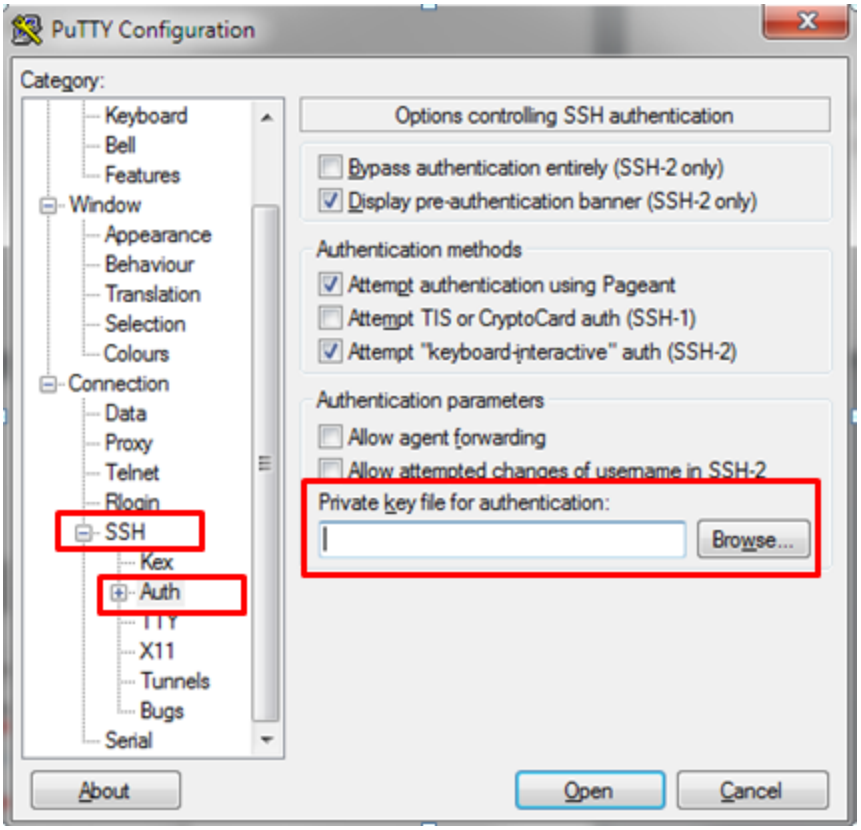
3. Acceda a la instancia virtual mediante el protocolo SSH a través de un cliente de este protocolo, como PuTTY. Se proporcionan instrucciones para PuTTY, pero puede utilizar cualquier cliente del protocolo SSH.
4. Si está usando PuTTY, ejecute el siguiente comando para conectarse a una máquina Linux:
   `putty.exe`

Se muestra la siguiente pantalla.



5. Ingrese la dirección IP. Debe usar la dirección IP privada de la pantalla anterior.
6. En **Tipo de conexión**, seleccione **Protocolo SSH**.
7. En **Cerrar la ventana al salir**, seleccione una de las opciones disponibles.
8. Haga clic en **Abrir**.

Se muestra la siguiente pantalla.



9. Seleccione **Conexión > protocolo SSH > Autenticación**.
10. Seleccione **Navegar** para buscar el archivo de **Clave privada**.
11. Haga clic en **Abrir** para conectarse a la instancia virtual.

Deshabilitar el repositorio base de CentOS

Para deshabilitar el repositorio base de CentOS:

1. Ejecute el siguiente comando:
   ```
   sudo vi /etc/yum.repos.d/CentOS-Base.repo
   ```
2. Asegúrese de que en el contenido del archivo **CentOS-Base.repo** en el directorio **/etc/yum.repos** se incluyan secciones con **enabled=0**
   El contenido del archivo debe ser similar al siguiente ejemplo:
   ```
   [base]
   name=CentOS-$releasever - Base
   mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$ba
   search&repo
   =os
   #baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
   ```

```
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
enabled=0
```

Configurar el usuario raíz

Para implementar manualmente el Remote Log Collector, siga estos pasos:

1. Configure un usuario raíz mediante los siguientes comandos:
   `sudo passwd root`
   `password` (Ingrese su contraseña y vuelva a escribirla).
2. Inicie sesión como **raíz** mediante el siguiente comando:
   `su root`
3. Use los siguientes comandos para configurar un archivo **repo**
   `cd /etc/yum.repos.d`
   `vi sa.repo`

Nota: Copie el siguiente contenido y péguelo en el archivo **repo de Security Analytics**. Debe reemplazar el nombre de usuario y la contraseña de cuenta de Live por sus credenciales de cuenta de Live.

```
[sa]
name=SA Yum Repo
baseurl=https://<LiveAccountUsername>:<LiveAccountPassword>@smcupdate
.emc.com/nw10/rpm/
enabled = 1
protect = 0
gpgcheck = 0
sslVerify = 1
metadata_expire = 1d
failovermethod=priority
```

4. Guarde el archivo **sa.repo**.
Presione **<Escape>:wq!** para guardar los cambios que realizó en el archivo.

5. Ejecute los siguientes comandos para descargar e instalar las dependencias.

```
yum install nwconsole
yum install nwappliance
yum install nwsdk
yum install nwlogcollector
```

```
yum install nwsupport-script
yum install (res-protobuffs,rsa-audit-rt,rsa-collectd,rsasa-
sshconfig,rsa-sms-runtime-rt,rsa-sa-tools,rsa-gpgpubkeys,
rsa-mcollective-agents)
yum install mcollective-*
yum install puppet
```

Configurar la comunicación (en el lado de AWS)

Para configurar la comunicación en el lado de AWS:

1. Edite el archivo **hostname** para agregar el nombre de host en dos lugares, como se muestra a continuación.
   ```
   vi /etc/hostname
   vi /etc/sysconfig/network
   ```
2. Presione **<Escape>:wq!** para guardar los cambios que realizó en los archivos.
3. Editar el archivo **Hosts** y agregue el nombre de host que agregó en el archivo **Nombre de host**. Agregue también el servidor IP de Security Analytics como **puppetmaster.local** mediante la ejecución del siguiente comando:
   ```
   vi /etc/hosts
   ```
   El contenido del archivo debe ser similar a lo que se muestra en el siguiente ejemplo:
   ```
   127.0.0.1 <hostname> localhost.localdom localhost
   ::1 < hostname> localhost.localdom localhost ip6-localhost ip6-
   loopback
   <SA IP> puppetmaster.local
   ```
4. En los siguientes pasos, necesitará el ID del nodo. Ejecute el siguiente comando para obtener el ID del nodo:
   ```
   /etc/puppet/scripts/node_id.py
   ```
5. Edite el archivo **puppet.conf** y agregue las líneas `certname=node_id` y `server=puppetmaster.local`. Debe reemplazar node_id por el del paso anterior.
   ```
   vi /etc/puppet/puppet.conf
   ```
   El contenido del archivo debe ser similar a lo que se muestra en el siguiente ejemplo:
   ```
   [main]
   rundir = /var/run/puppet
   logdir = var/log/puppet
   ssldir = $vardir/ssl
   certname = <node_id>
   [agent]
   localconfig = $vardir/localconfig
   ```

```
classfile = $vardir/classes.txt
server = puppetmaster.local
```

6. Cree un archivo **csr_attributes.yaml** mediante la ejecución del siguiente comando. Debe reemplazar el nombre de host y la dirección IP de Remote Log Collector:
   ```
   vi /etc/puppet/csr_attributes.yaml
   ```
   El contenido del archivo debe corresponder exactamente a lo que se muestra en el siguiente ejemplo:
   ```
   custom_attributes:
   1.2.840.113549.1.9.7: fqdn=<hostname>, ipaddress=<ip of the system
   (awsvlc)>,type=base
   ```
7. Ejecute el siguiente comando para reiniciar el sistema.
   ```
   reboot
   ```
8. Inicie sesión en Remote Log Collector mediante las instrucciones para el protocolo SSH de la sección Iniciar sesión mediante el protocolo SSH anterior.
9. Inicie sesión como **raíz** e ingrese el siguiente comando:
   ```
   su root
   ```
10. Ejecute el siguiente comando para asegurarse de que el Log Collector esté configurado como un Remote Log Collector y que todos los servicios estén en ejecución:
    ```
    vi / etc/netwitness/ng/logcollection/logCollectionType
    ```
    El contenido del archivo debe ser igual a la siguiente línea:
    ```
    RC
    ```
11. Para sincronizar la hora y la fecha entre el servicio de recopilación remota de registros de AWS y el servidor de Security Analytics, siga estos pasos:
    a. Obtenga la fecha y la hora actuales en el servidor de Security Analytics y en Remote Log Collector mediante la ejecución del siguiente comando.
    ```
    date
    ```
    b. Si la fecha y la hora no están sincronizadas, ejecute los siguientes comandos para establecerlas en Remote Log Collector de AWS:
    ```
    date --set="MM/DD/YYYY"
    date --set="HH:MM:SS"
    ```
12. Ejecute los siguientes comandos para iniciar los servicios requeridos:
    ```
    service rabbitmq-server start
    service puppet start
    service mcollective start
    start nwlogcollector
    ```

Configurar permisos de firewall

Nota: Es necesario abrir puertos entre el Remote Log Collector y el servidor de Security Analytics, y también entre el Log Collector en el Log Decoder.

Configure el o los firewalls para permitir la comunicación entre Remote Log Collector y AWS, y los componentes de NetWitness que se enumeran en la siguiente tabla.

De host	A host	A puertos (protocolo)	Comentarios
Servidor de Security Analytics	Remote Log Collector	56001 (TCP) o 50001 (TCP)	SSL o No SSL
Servidor de Security Analytics	Remote Log Collector	50101 (TCP)	REST (opcional)
Servidor de Security Analytics	Remote Log Collector	5672 (TCP)	RabbitMQ
Servidor de Security Analytics	Remote Log Collector	50055 (TCP)	RSA-SMS
Servidor de Security Analytics	Remote Log Collector	50056 (TCP)	RSA-SMS
Remote Log Collector	Servidor de Security Analytics	8140 (TCP)	Puppet
Servidor de Security Analytics	Remote Log Collector	61614 (TCP)	MCollective
Remote Log Collector	Servidor de Security Analytics	61614 (TCP)	MCollective
Servidor de Security Analytics	Remote Log Collector	15671 (TCP)	RabbitMQ
Remote Log Collector	Servidor de Security Analytics	15671 (TCP)	RabbitMQ

En el modo de extracción:			
Log Collector (en Log Decoder)	Remote Log Collector	5671 (TCP)	RabbitMQ
En el modo de migración:			
Remote Log Collector	Log Collector (en Log Decoder)	5671 (TCP)	RabbitMQ

El vínculo general que indica qué puertos deben estar abiertos en qué dispositivo se puede encontrar en https://community.rsa.com/docs/DOC-54917.

Habilitar Remote Log Collector en el servidor de Security Analytics

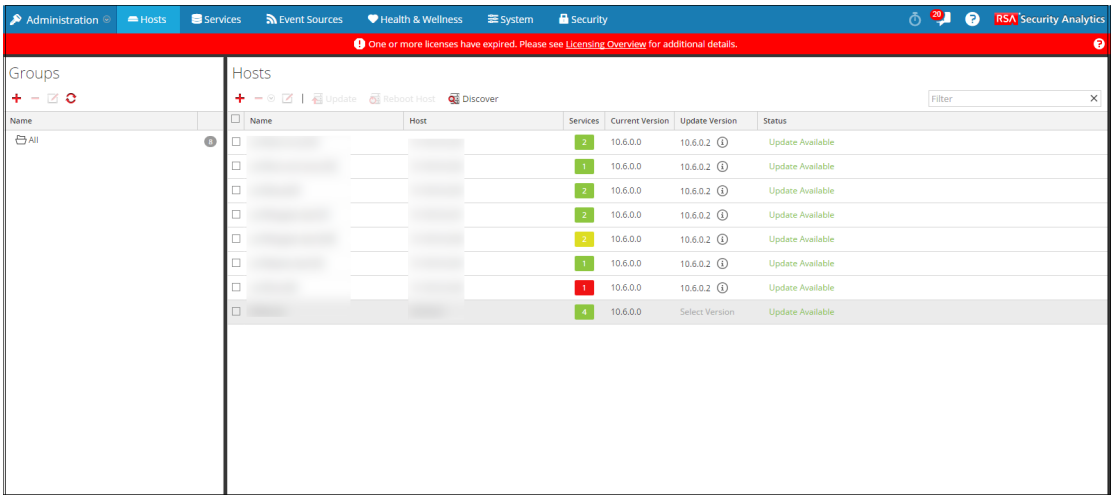
1. Ejecute el siguiente comando para habilitar Remote Log Collector en el servidor de Security Analytics:

```
puppet agent -t --waitforcert 30
```

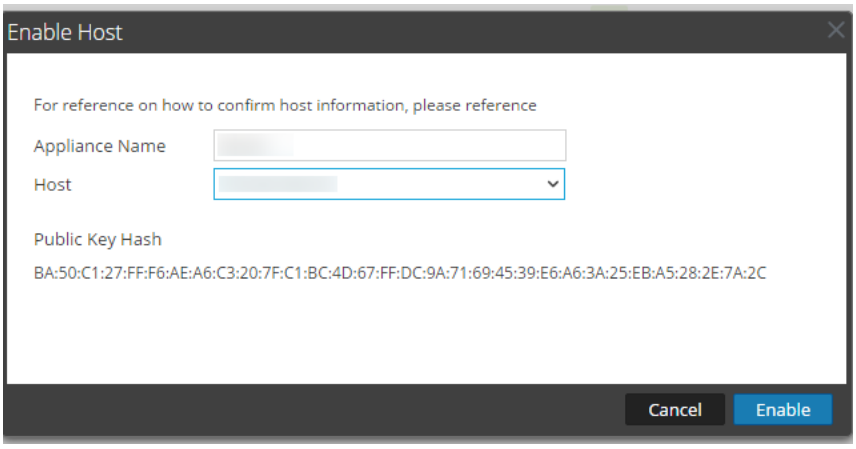
Configurar la comunicación (en el lado de NetWitness)

Para configurar la comunicación en el lado de NetWitness, siga estos pasos:

1. Inicie sesión en el servidor de Security Analytics.
   En el menú de **Security Analytics**, vaya a **Administration > Hosts**.
2. Haga clic en **Descubrir**.



Se muestra la siguiente pantalla.

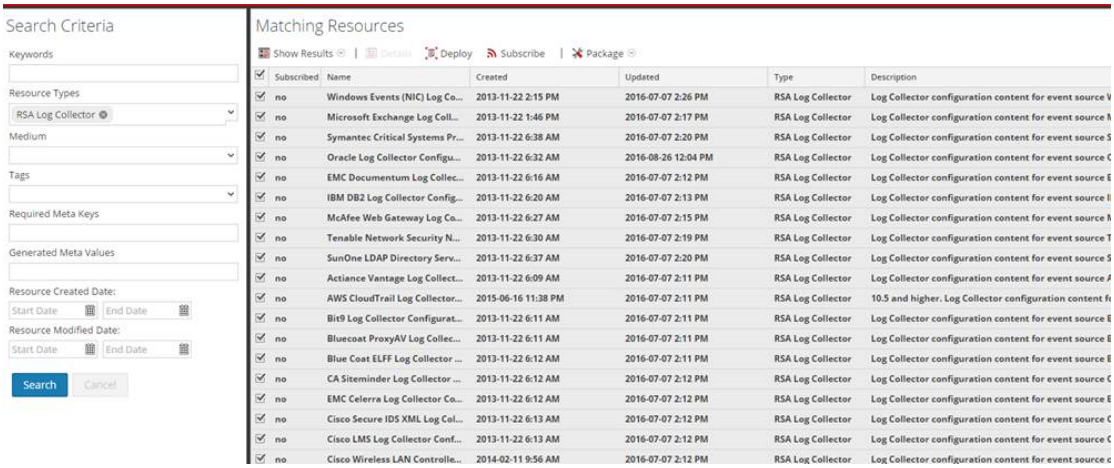


2. Seleccione un dispositivo y un host y, a continuación, haga clic en **Habilitar**.

Implementar el contenido de Log Collector

En el servidor de Security Analytics, debe implementar el Log Collector **nwlogcollectorcontent** en el Remote Log Collector (AWS) mediante Live.

1. En el menú de **Security Analytics**, seleccione **Live > Tipos de recursos.**
2. En el menú desplegable **Tipos de recursos**, seleccione **RSA Log Collector**.
3. Seleccione **Search**.



El Remote Log Collector (AWS) ahora debe estar operativo y esto se puede verificar en la página **Administration > Servicios**.

Para obtener más información, consulte la Guía de servicios de Live, disponible en RSA Link en la siguiente ubicación:

https://community.rsa.com/docs/DOC-41548.

Guía de configuración de la recopilación de punto de comprobación

Este protocolo recopila eventos desde los orígenes de eventos de punto de comprobación mediante OPSEC LEA. OPSEC LEA es la API de exportación de registros de seguridad de operaciones de punto de comprobación que facilita la extracción de registros.

Debe implementar Log Collection antes de poder configurar el protocolo de recopilación de punto de comprobación.

Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Conceptos básicos

Descripción general

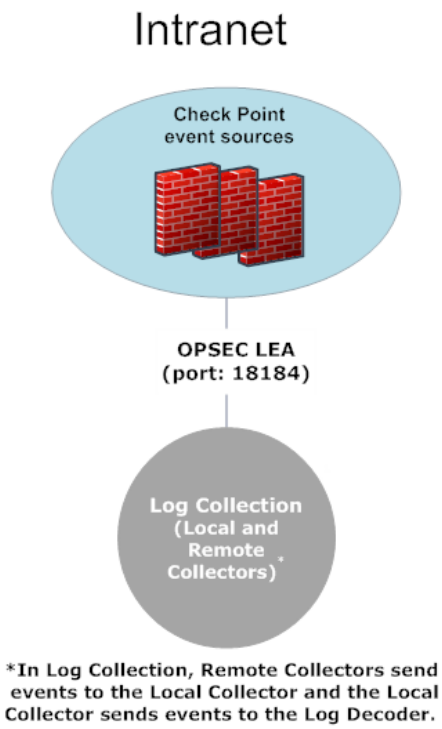
En esta guía se indica cómo configurar el protocolo de recopilación de punto de comprobación que recopila eventos desde un origen de eventos de punto de comprobación como un firewall o administrador de registro de punto de comprobación.

Cómo funciona la recopilación de punto de comprobación

el servicio de Log Collector recopila eventos de los orígenes de eventos de punto de comprobación utilizando OPSEC LEA. OPSEC LEA es la API de exportación de registros de seguridad de operaciones de punto de comprobación que facilita la extracción de registros.

Escenario de implementación

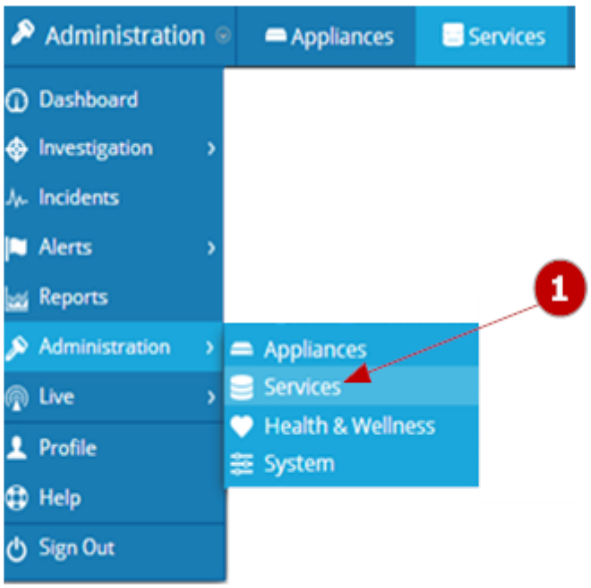
En la siguiente figura se ilustra cómo debe implementar el protocolo de recopilación de punto de control en Security Analytics.



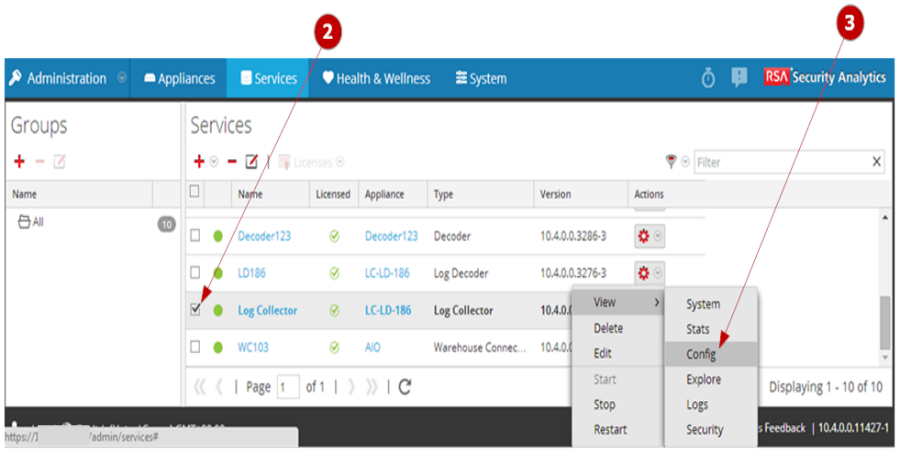
Configurar el protocolo de recopilación de punto de control en Security Analytics

Debe configurar el Log Collector para usar la recopilación de punto de comprobación para un origen de eventos en la pestaña Origen de eventos de la vista Parámetro de Log Collector. En la siguiente figura se muestra el flujo de trabajo básico para configurar un origen de eventos para la recopilación de punto de control en Security Analytics. Consulte:

- Paso 2. Configurar orígenes de eventos de punto de control en Security Analyticspara obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de punto de control.
- Recopilación de punto de control: Parámetros de configuraciónpara obtener una descripción detallada de cada parámetro del protocolo de recopilación de punto de control.

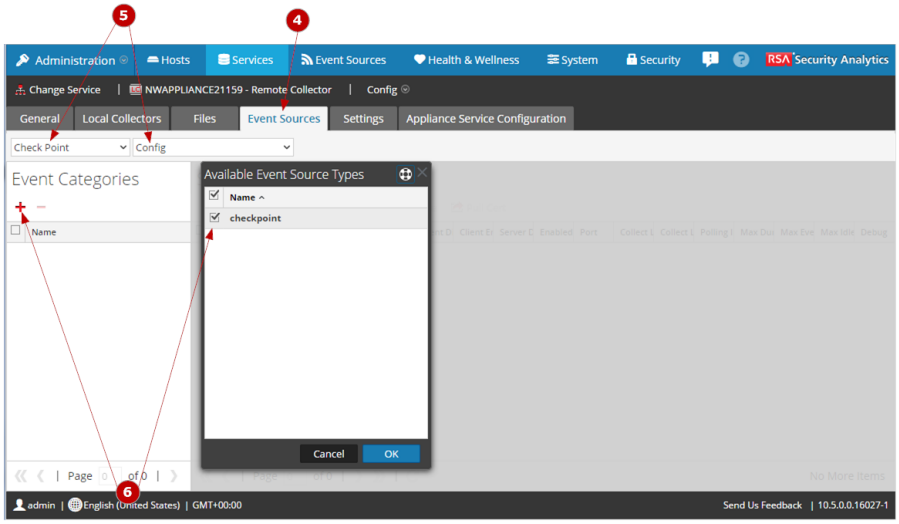


1 Acceda a la vista **Servicios**.



2 Seleccione un servicio de **recopilación de registros**.

3 Haga clic en ⌄ bajo **Acciones** y seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.

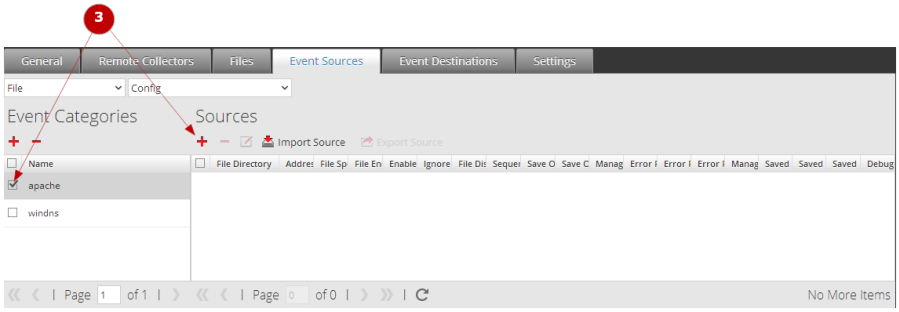


4 Haga clic en la pestaña **Orígenes de evento**.

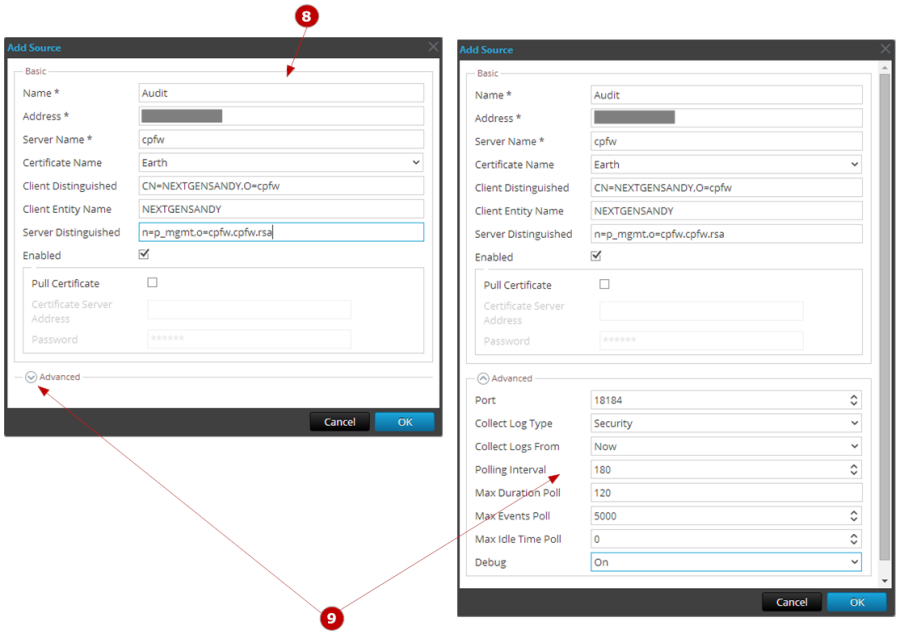
5 Seleccione **Punto de comprobación** como el protocolo de recopilación y seleccione **Configuración**.

6 Haga clic en + y seleccione **Punto de comprobación** como categoría de origen de eventos.

La categoría de origen de eventos es parte del contenido que descargó de LIVE.



7 Seleccione la categoría de **Punto de comprobación** y haga clic en +.



8 Especifique los parámetros básicos requeridos para el origen de eventos de **punto de control**.

9 Haga clic en y especifique parámetros adicionales que mejoran la manera en que el protocolo de **punto de control** maneja la recopilación de eventos para el origen de eventos.

Configurar los orígenes de eventos para usar el protocolo de recopilación de punto de comprobación

Debe configurar cada origen de eventos que usa el protocolo de recopilación de punto de control para que se comunique con Security Analytics (consulte Paso 1. Configurar orígenes de eventos de punto de control para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de punto de comprobación con una lista de verificación que contiene cada paso de configuración.

Contexto

Los pasos de configuración para el protocolo de recopilación de punto de comprobación deben realizarse en la secuencia específica que se indica en la siguiente tabla.

Lista de comprobación de configuración de punto de comprobación

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de punto de control para enviar eventos a Security Analytics.	
2	Configurar orígenes de eventos de punto de control en Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de punto de comprobación configurado.	
4	Verificar que la recopilación de punto de comprobación esté funcionando.	

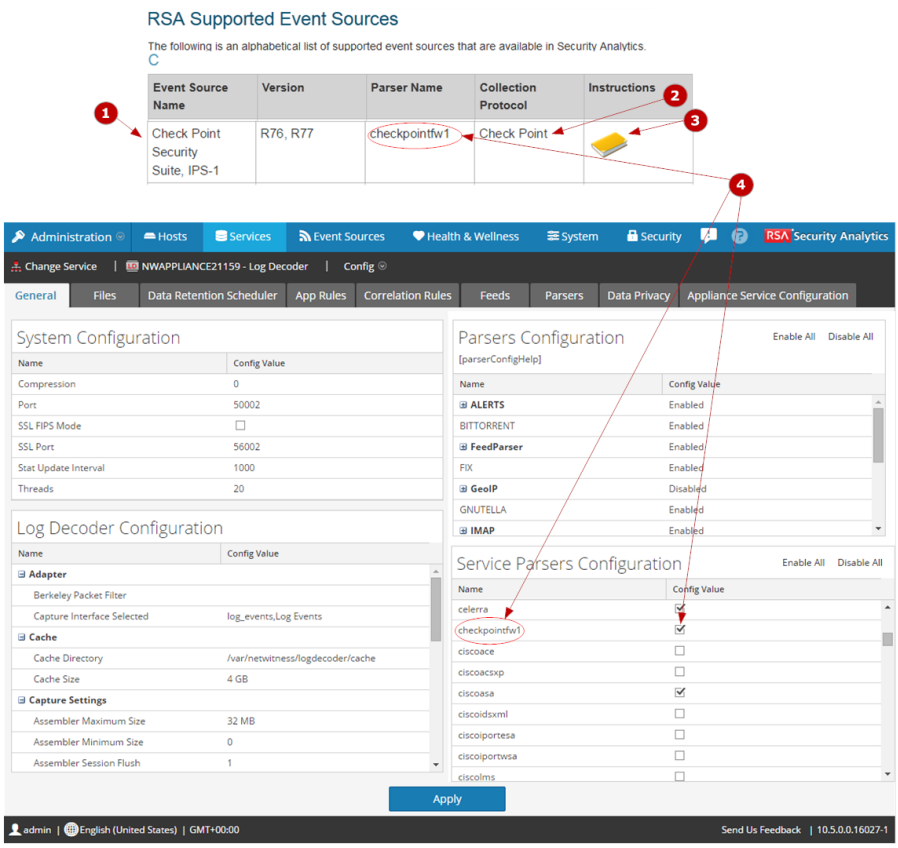
Paso 1. Configurar orígenes de eventos de punto de control para enviar eventos a Security Analytics

En este tema se indica dónde encontrar los orígenes de eventos que son compatibles actualmente con la recopilación de punto de comprobación y las instrucciones de configuración disponibles para cada origen de eventos.

Lista de orígenes de eventos compatibles

Volver a Procedimientos

La lista de orígenes de eventos compatibles de RSA es una lista alfabética de todos los orígenes de eventos que son compatibles actualmente con Security Analytics, la cual identifica los orígenes de eventos que puede usar con la recopilación de punto de comprobación.



1 Busque el nombre del origen de eventos.

2 Verifique que sea compatible con el protocolo de **recopilación de punto de control**.

3 Haga clic en  para ver las instrucciones de configuración del origen de eventos.

4 Verifique que haya descargado el analizador de origen de eventos correcto (por ejemplo, **checkpointfw1**) desde LIVE a Log Decoder y que lo haya activado.

Ejemplo de instrucciones de configuración

La siguiente ilustración se toma de las instrucciones de configuración de Check Point Security Suite, IPS-1.

RSA Security Analytics

Event Source Log Configuration Guide

Check Point Security Suite, IPS-1

Last Modified: Thursday, February 19, 2015

Event Source Product Information:

Vendor: Check Point
Event Source: Check Point Security Suite, IPS-1
Versions: R76, R77
Supported Platforms: Check Point Appliances, SecuredBy Check Point partner appliances, Check Point SecurePlatform running on Open Servers, and Check Point software running on supported Operating Systems like Windows, Red Hat and Solaris

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: checkpointfw1
Collection Method: Check Point LEA API
Event Source Class.Subclass: Security.Firewall

Paso 2. Configurar orígenes de eventos de punto de control en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de punto de comprobación para el Log Collector.

Después de realizar este procedimiento, habrá...

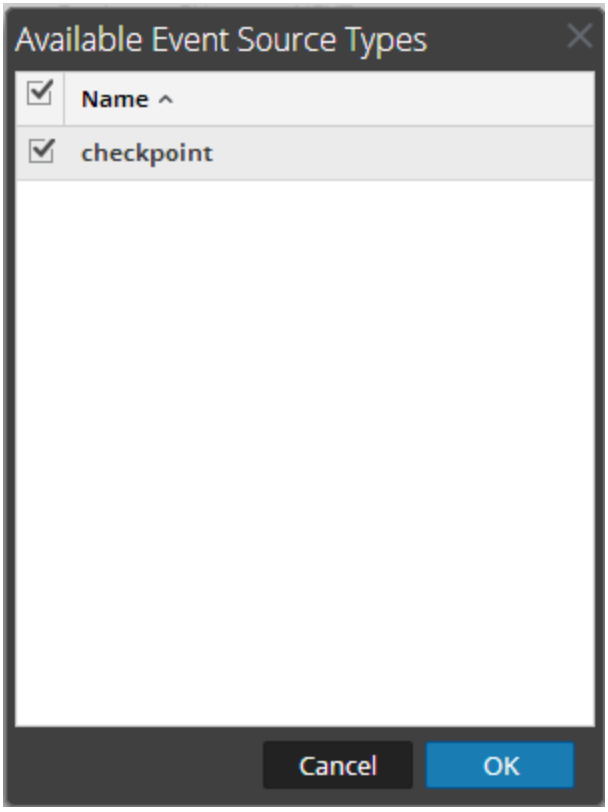
- Configurado un origen de eventos de punto de comprobación.
- Modificado un origen de eventos de punto de comprobación.
- Extraído un certificado para un origen de eventos de punto de comprobación.

Volver a Procedimientos

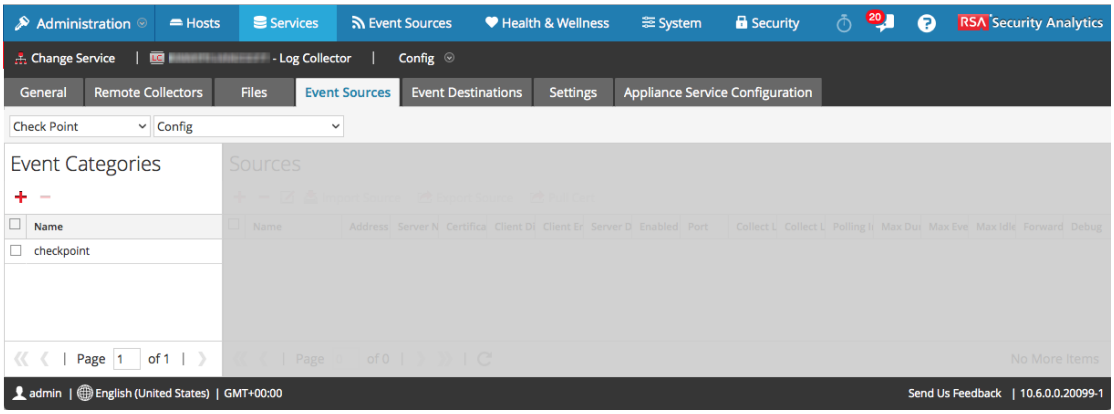
Procedimientos

Configurar origen de eventos de punto de comprobación

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Punto de comprobación/Configurar** en el menú desplegable.
5. En la barra de herramientas del panel **Categorías de evento**, haga clic en .
   Se muestra el cuadro de diálogo **Tipos de origen de evento disponibles**.
6. Seleccione un tipo de origen de eventos (por ejemplo, punto de comprobación) y haga clic en Aceptar.

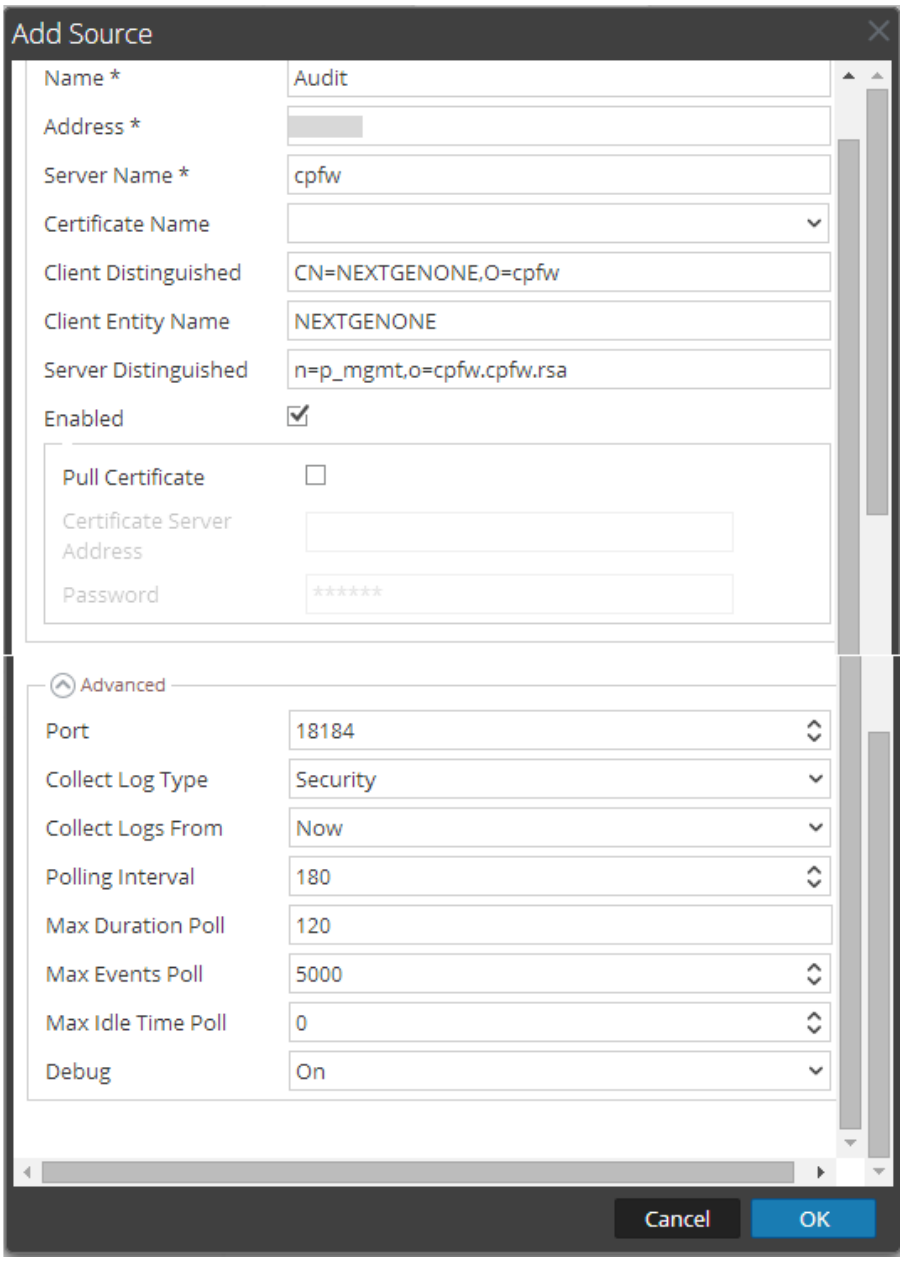


El tipo de origen de eventos recién agregado se muestra en el panel **Categorías de evento**.



7. Seleccione el nuevo tipo en el panel **Categorías de evento** y haga clic en + en la barra de herramientas **Orígenes**.
   Se muestra el cuadro de diálogo **Agregar origen**.
8. Definir valores de parámetros (consulte Recopilación de punto de control: Parámetros de configuraciónpara ver definiciones de cada parámetro).

Nota: Se utilizan menos recursos del sistema cuando se establece una conexión que solo permanece abierta para el volumen de tiempo y eventos que especificó o para una conexión transitoria. De forma predeterminada, los parámetros se configuran para una conexión transitoria, de la siguiente manera:
Máximo de eventos de encuesta = 0
Intervalo de sondeo = 0
Duración máxima de encuesta = 0
Intervalo de sondeo = -1
Especifique la cantidad de eventos y el período que desea que la conexión permanezca abierta en los parámetros **Máximo de eventos**, **Intervalo de sondeo**, **Duración máxima de encuesta** e **Intervalo de sondeo**. Para orígenes de eventos de punto de comprobación muy activos, una buena práctica consiste en configurar una conexión que permanezca abierta hasta que se detenga la recopilación (conexión persistente). Esto garantiza que la recopilación de punto de comprobación mantiene el ritmo de los eventos que generan estos orígenes de eventos activos. La conexión persistente evita reinicios y demoras en la conexión e impide que la recopilación de punto de comprobación retrase la generación de eventos. Para establecer una conexión persistente para un origen de eventos de punto de comprobación, configure los siguientes parámetros en los siguientes valores:
Intervalo de sondeo = 180 (3 minutos)
Duración máxima de encuesta = 120 (2 minutos)
Máximo de eventos de encuesta = 0



9. Seleccione **Extraer certificado** para extraer un certificado por primera vez. Esto permite que el certificado esté disponible en el área de almacenamiento de confianza.
10. Haga clic en **Aceptar**.

El nuevo origen de eventos se muestra en el panel **Orígenes**.

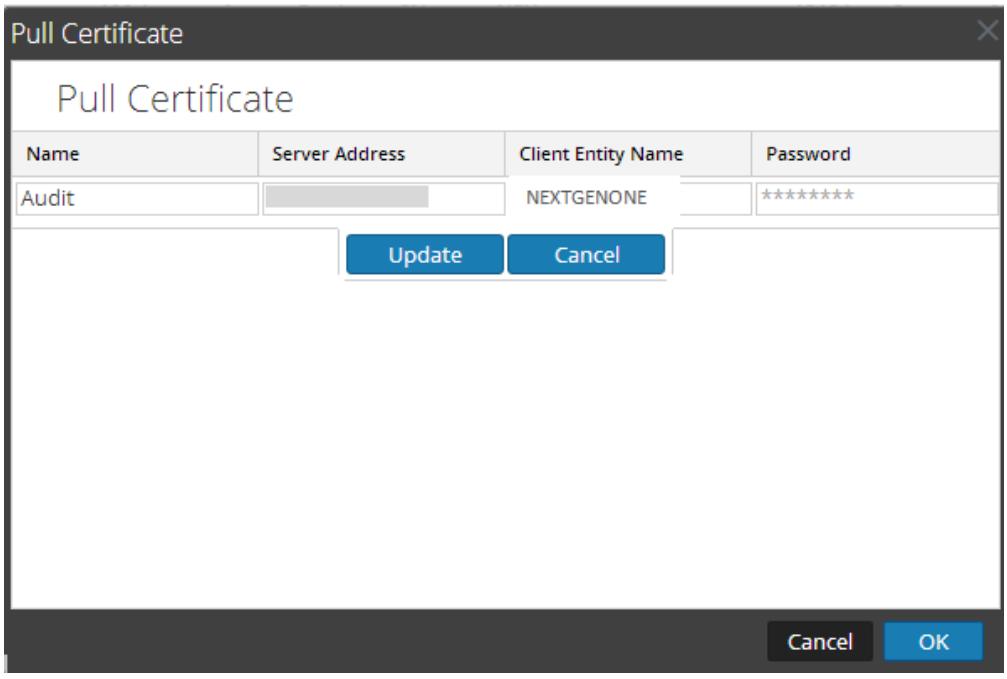
Extraer certificado

Realice el siguiente procedimiento si:

- no extrajo un certificado cuando configuró un origen de eventos Punto de comprobación, o
- necesita volver a extraer un certificado.

Para extraer un certificado:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Punto de comprobación/Configurar** en el menú desplegable.
5. Seleccione un tipo de origen de eventos en el panel Categorías de evento.
   Los orígenes de este tipo se muestran en el panel **Orígenes**.
6. Seleccione uno o más orígenes y haga clic en Pull Cert.
   Se muestra la configuración del servidor de punto de comprobación desde el cual puede extraer certificados.
7. Haga clic en el cuadro de texto bajo **Contraseña**.
   Todos los campos pasan a ser editables.



8. Ingrese una contraseña y haga clic en **Actualizar** y, a continuación, en **Aceptar**.

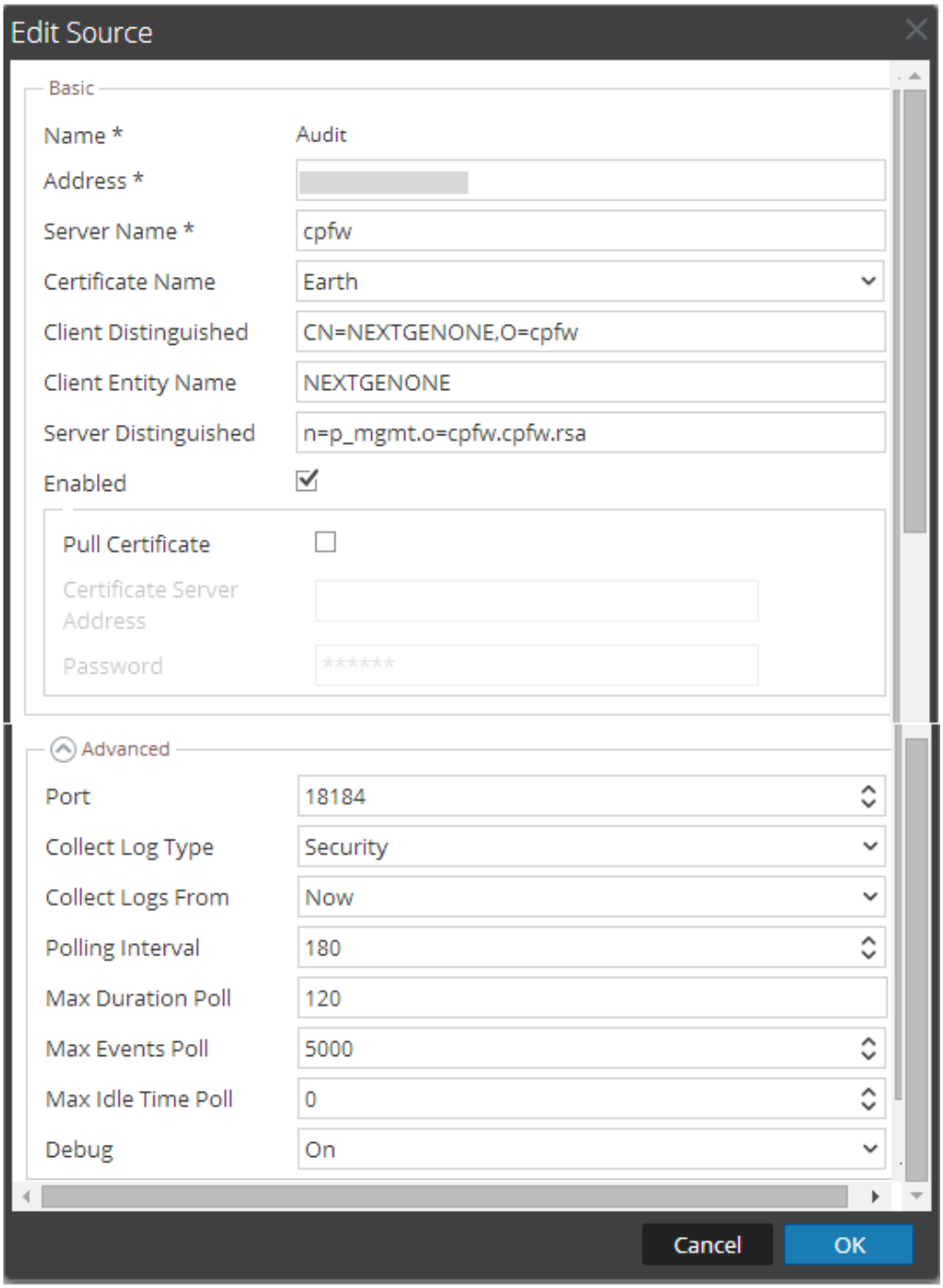
> **Nota:** Debe especificar una contraseña. Si necesita modificar los otros parámetros de certificado de servidor de punto de comprobación (Auditoría, Dirección de servidor y Nombre de entidad del cliente), tiene esa opción.

Security Analytics extrae el certificado.

Modificar un origen de eventos de punto de comprobación

Para modificar un origen de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Punto de comprobación/Configurar** en el menú desplegable.
   En el panel **Categorías de evento** se muestran los orígenes de eventos que están configurados, si los hay.
5. Seleccione un tipo de origen de eventos en el panel **Categorías de evento**.
   Los orígenes de eventos de este tipo se muestran en el panel **Orígenes**.
6. Seleccione un origen y haga clic en  en la barra de herramientas.
   Se muestra el cuadro de diálogo **Editar origen**.
7. Modifique los parámetros que necesiten cambios y haga clic en **Guardar**.



Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado.

Parámetros

Recopilación de punto de control: Parámetros de configuración

Paso 3. Iniciar el servicio para el protocolo de recopilación de punto de comprobación configurado

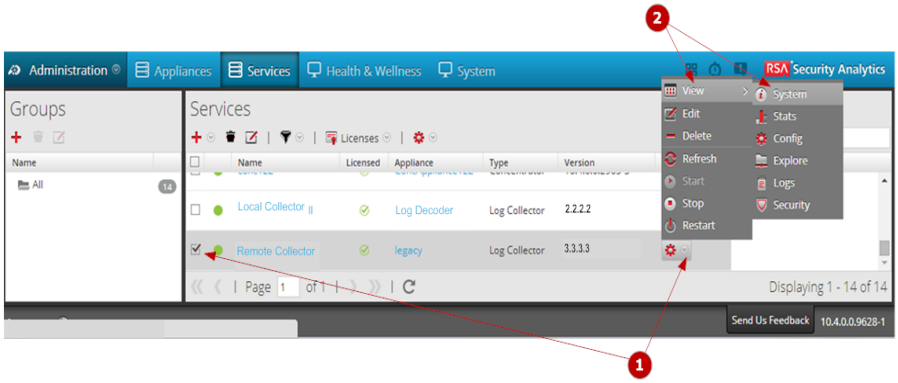
En este tema se indica cómo iniciar un servicio de recopilación de punto de comprobación detenido.

Volver a Procedimientos

Puede ser necesario iniciar un servicio de recopilación detenido o habilitar el inicio automático de un servicio individual.

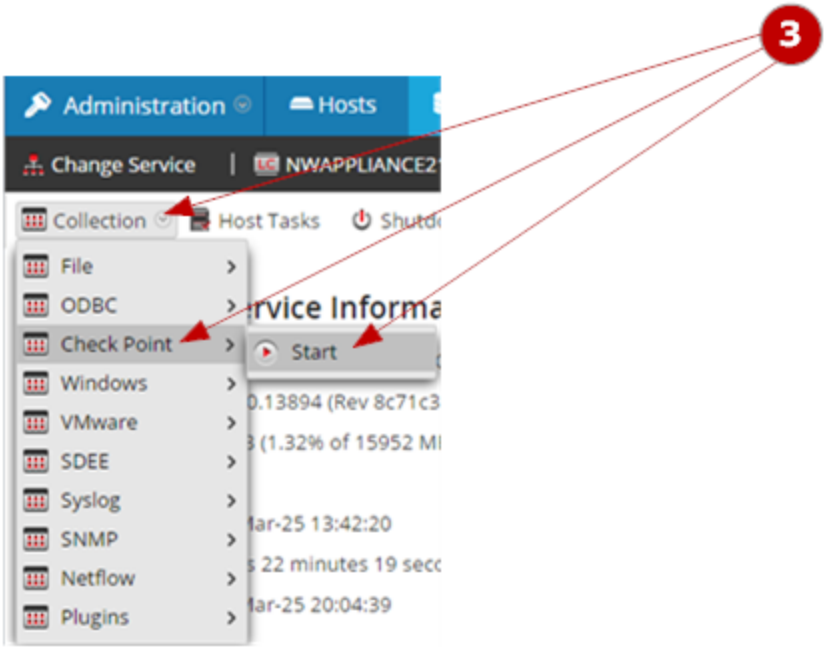
Procedimiento

En la siguiente figura se muestra cómo iniciar un servicio de recopilación. Consulte el tema **Habilitar el inicio automático de servicios individuales** de la *Guía de configuración de la recopilación de registros* si desea que el servicio se inicie automáticamente.



1 Seleccione un servicio **Log Collector** y haga clic en bajo **Acciones**.

2 Haga clic en **Ver > Sistema**.



3 Haga clic en **Recopilación > Punto de comprobación** y, a continuación, haga clic en **Iniciar**.

Paso 4. Verificar que la recopilación de punto de comprobación esté funcionando

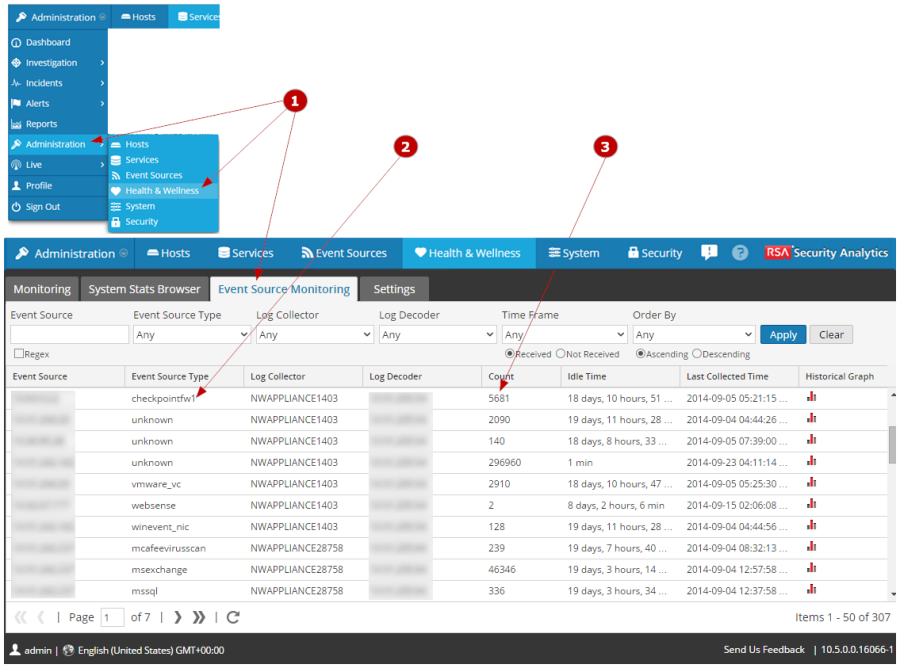
En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de punto de comprobación se configuró correctamente.

Volver a Procedimientos

Puede ser necesario verificar que la recopilación de punto de comprobación esté configurada correctamente; de lo contrario, no funcionará.

Procedimiento

En la siguiente figura se ilustra cómo puede verificar que la recopilación de punto de control esté funcionando desde **Administration > Estado y Condición > pestaña Monitoreo de orígenes de eventos**.

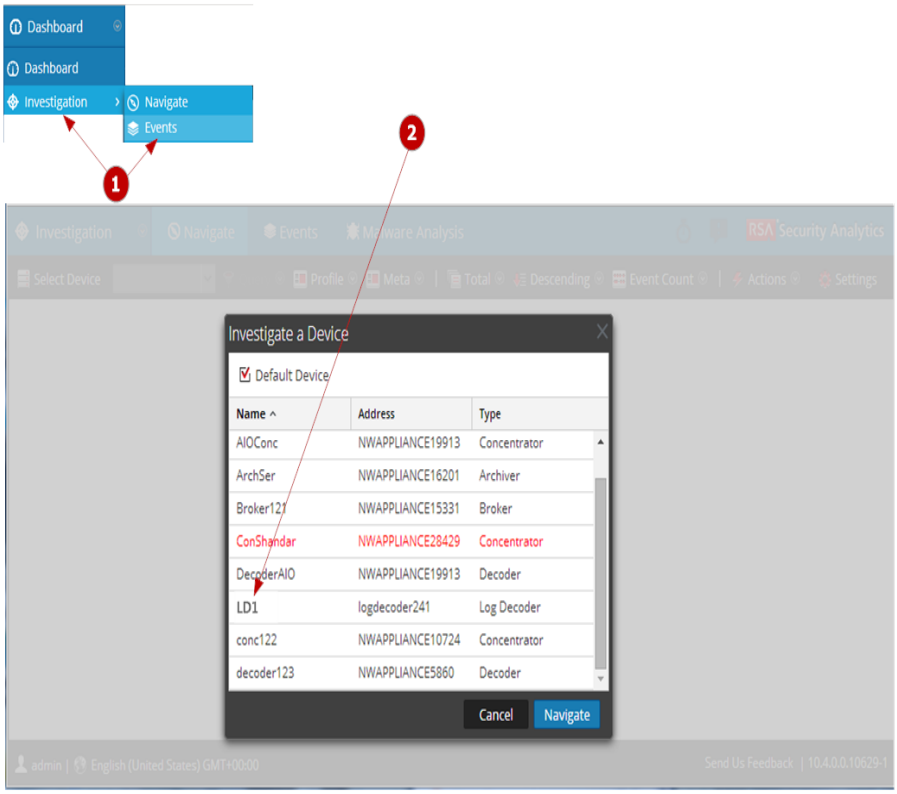


1 Acceda a la **pestaña Monitoreo de orígenes de eventos** desde la vista **Administration > Estado y condición**.

2 Busque **checkpointfw1** en la columna **Tipo de origen de evento**.

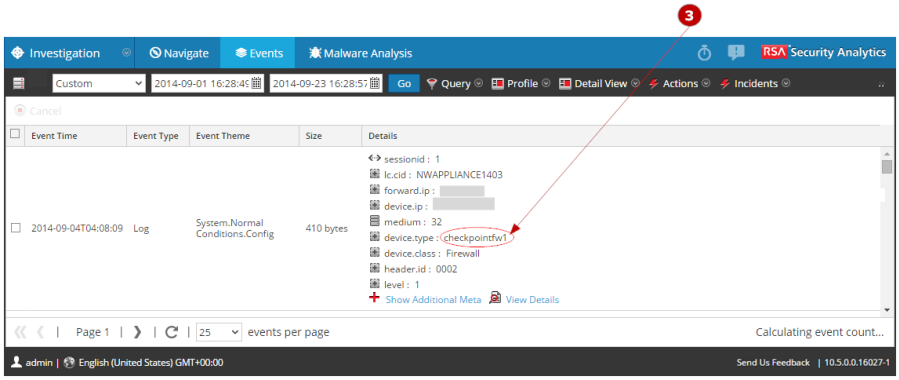
3 Busque actividad en la columna **Conteo** para verificar que la recopilación de punto de control acepte eventos.

En la siguiente figura se ilustra cómo puede verificar que la recopilación de punto de control esté funcionando desde **Investigation > vista Eventos**.



1 Acceda a **Investigation > vista Eventos**.

2 Seleccione eventos de punto de comprobación de la recopilación de Log Decoder (por ejemplo, **LD1**) en el cuadro de diálogo **Investigar un dispositivo**.



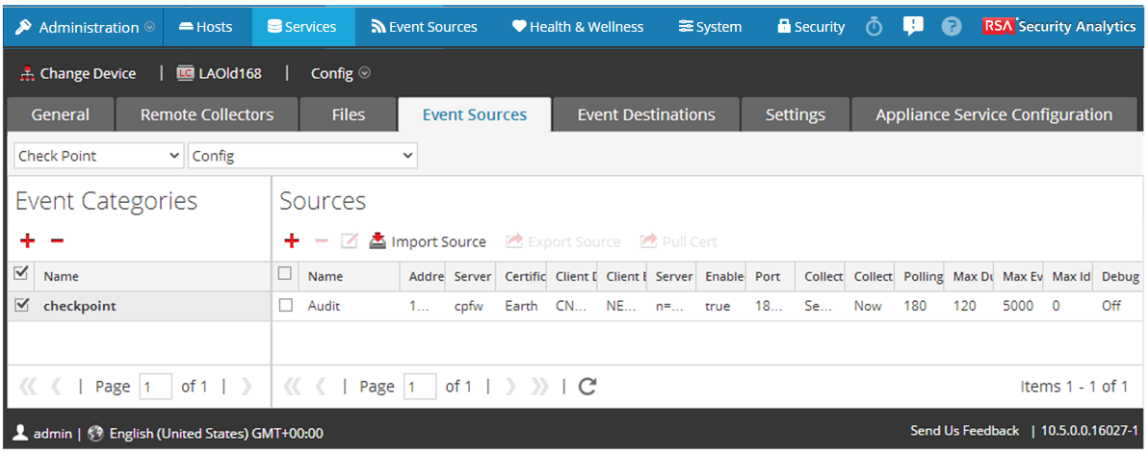
3 Busque un analizador de origen de eventos de punto de control (por ejemplo, **checkpointfw1**) en el campo **device.type** de la columna **Detalles** para verificar que la recopilación de punto de control esté aceptando eventos.

Recopilación de punto de control: Parámetros de configuración

Este tema describe los parámetros de configuración del origen de eventos de punto de comprobación

Para acceder a los parámetros de configuración de la recopilación de punto de comprobación:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Punto de comprobación/Configurar** en el menú desplegable.



La vista Punto de comprobación/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar los tipos de orígenes de eventos correspondientes.

Característica	Descripción
+	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
−	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.

Característica	Descripción
	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de tipos de orígenes de eventos compatibles.

Característica	Descripción
	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

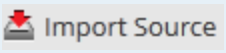
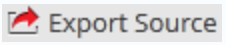
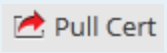
Panel Orígenes

El panel Orígenes de punto de comprobación muestra una lista de los orígenes de eventos de firewall de punto de comprobación existentes. Utilice esta sección para agregar o eliminar orígenes de eventos y parámetros de comunicación asociados.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar origen, en el cual puede definir los parámetros para un host de firewall de punto de comprobación.
	Elimina el host que seleccionó.

Característica	Descripción
	Abre el cuadro de diálogo Editar origen, en el cual puede editar los parámetros del origen de eventos de punto de comprobación seleccionado. Seleccione varios orígenes de eventos y haga clic en  para abrir el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar hosts de punto de comprobación de forma masiva desde un archivo de valores separados por comas (CSV). Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo .csv que contiene los parámetros de los hosts de punto de comprobación seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Extraer certificado. Use este cuadro de diálogo para extraer un certificado desde el servidor del punto de comprobación para este host.

Cuadro de diálogo Agregar/Editar origen

Los cuadros de diálogo Agregar origen y Editar origen contienen la misma información.

Parámetro	Descripción
Básico	
Nombre*	Nombre del origen de eventos.
Dirección de servidor*	Dirección IP del servidor del punto de comprobación.
Nombre del servidor*	Nombre del servidor del punto de comprobación.

Parámetro	Descripción
Nombre del certificado	El nombre del certificado que las conexiones seguras deben utilizar cuando el modo de transporte sea https. Si está definido, el certificado debe existir en el área de almacenamiento de confianza de certificados que creó usando la pestaña Configuración. Seleccione un certificado en la lista desplegable. La convención de nombres de archivos para los certificados de origen de eventos de punto de comprobación es checkpoint_name-of-event-source.
Cliente distinguido	Ingrese el nombre del cliente distinguido del servidor del punto de comprobación.
Nombre de entidad de cliente	Ingrese el nombre de entidad de cliente del servidor del punto de comprobación.
Servidor distinguido	Ingrese el nombre del servidor distinguido del servidor del punto de comprobación.
Extraer certificado	Seleccione la casilla de verificaciónpara extraer un certificado por primera vez. La extracción de un certificado hace que esté disponible desde el área de almacenamiento de confianza.
Dirección del servidor de certificados	Dirección IP del servidor en el cual reside el certificado.
Contraseña	Solo está activa cuando selecciona la casilla de verificación Extraer certificado por primera vez. Contraseña necesaria para extraer el certificado. La contraseña es la clave de activación que se crea cuando se agrega una aplicación OPSEC al punto de comprobación en el servidor del punto de comprobación.

Parámetro	Descripción
Activado	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
Avanzado	
Nota: se usan menos recursos del sistema cuando se configura una conexión de origen de eventos de punto de comprobación de modo que permanezca abierta durante un momento específico y para un volumen de eventos específico (conexión transitoria). Security Analytics se configura de forma predeterminada en los siguientes parámetros de conexión que establecen una conexión transitoria: Intervalo de sondeo = 180 (3 minutos) Duración máxima de encuesta = 120 (2 minutos) Máximo de eventos de encuesta = 5,000 (5,000 eventos por intervalo de sondeo) Tiempo máximo de inactividad de encuesta = 0 Para orígenes de eventos de punto de comprobación muy activos, una buena práctica consiste en configurar una conexión que permanezca abierta hasta que se detenga la recopilación (conexión persistente). Esto garantiza que la recopilación de punto de comprobación mantiene el ritmo de los eventos que generan estos orígenes de eventos activos. La conexión persistente evita reinicios y demoras en la conexión e impide que la recopilación de punto de comprobación retrase la generación de eventos. Para establecer una conexión persistente para un origen de eventos de punto de comprobación, configure los siguientes parámetros en los siguientes valores: Intervalo de sondeo = -1 Duración máxima de encuesta = 0 Máximo de eventos de encuesta = 0 Tiempo máximo de inactividad de encuesta = 0	
Puerto	Puerto del servidor del punto de control al cual se conecta Log Collector. El valor predeterminado es 18184.

Parámetro	Descripción
Recopilar tipo de registro	Tipo de registros que desea recopilar: Los valores válidos son: • **Auditoría**: recopila eventos de auditoría. • **Seguridad**: recopila eventos de seguridad. Si desea recopilar tanto eventos de auditoría como de seguridad, debe crear un origen de eventos duplicado. Por ejemplo, primero debe crear un origen de eventos con la opción Auditoría seleccionada para extraer un certificado hacia el área de almacenamiento de confianza de este origen de eventos. A continuación, debe crear otro origen de eventos con los mismos valores, pero en la opción Recopilar tipo de registro debe seleccionar Seguridad, en Nombre del certificado debe seleccionar el mismo certificado que extrajo cuando configuró el primer conjunto de parámetros de este origen de eventos y debe asegurarse de que la opción Extraer certificado no esté seleccionada.
Recopilar registros desde	Cuando configura un origen de eventos de punto de control, Security Analytics recopila eventos desde el archivo de registro actual. Los valores válidos son: • **Ahora**: comenzar a recopilar registros ahora (en este momento en el archivo de registro actual). • **Comienzo del tiempo**: recopilar registros desde el comienzo del archivo de registro actual. Si selecciona “Comienzo del tiempo” para este valor de parámetro, puede recopilar una cantidad muy grande de datos de acuerdo con el tiempo que el archivo de registro actual ha estado recopilando eventos.
Intervalo de sondeo	El intervalo (cantidad de tiempo en segundos) entre cada encuesta. El valor predeterminado es **180**. Por ejemplo, si especifica 180, el recopilador programa un sondeo del origen de eventos cada 180 segundos. Si aún se está realizando el ciclo de sondeo anterior, esperará hasta que ese ciclo termine. Si está sondeando una gran cantidad de orígenes de eventos, es posible que el sondeo tarde más de 180 segundos en comenzar porque los subprocesos están ocupados.

Parámetro	Descripción
Duración máxima de encuesta	La duración máxima del ciclo de sondeo (cuánto tiempo dura el ciclo) en segundos.
Máximo de eventos de encuesta	La cantidad máxima de eventos por ciclo de sondeo (cuántos eventos se recopilan por ciclo de sondeo).
Tiempo máximo de inactividad de encuesta	Tiempo de inactividad máximo, en segundos, de un ciclo de sondeo. 0 indica que no hay límite.**> 300** es el valor predeterminado.
Depurar	**Precaución:** Active la depuración (defina este parámetro en "Activado" o "Detallado") solamente si tiene un problema con un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa y desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar).
Cancelar	Cierra el cuadro de diálogo sin agregar el host de firewall de punto de comprobación.

Parámetro	Descripción
OK	Agrega los valores de parámetros actuales como un nuevo host de punto de comprobación.

Cuadro de diálogo Extraer certificado

En la siguiente tabla se proporcionan descripciones de los parámetros del cuadro de diálogo Extraer certificado.

Parámetro	Descripción
Nombre	Muestra el nombre del origen de eventos
Dirección de servidor	Muestra la dirección IP del servidor del punto de comprobación.
Nombre de entidad de cliente	Muestra el nombre de la entidad de cliente que adquiere cuando configura el origen de eventos de punto de control para Security Analytics.
Contraseña	Clave de activación que se crea cuando se agrega una aplicación OPSEC al punto de comprobación. Debe volver a ingresar esta contraseña para extraer el certificado del servidor del punto de comprobación.
Actualizar	(Solo aparece en el modo de edición; haga clic en el campo Contraseña) Aplica las ediciones que hace en los parámetros del host.
Cancelar	(Solo aparece en modo de edición; haga clic en el campo Contraseña) Cierra el modo de edición sin aplicar los cambios.
Cancelar	Cierra el cuadro de diálogo sin extraer ningún certificado.
OK	Extrae el certificado.

Tareas

Paso 2. Configurar orígenes de eventos de punto de control en Security Analytics

Solucionar problemas de la recopilación de punto de comprobación

Descripción general

En este tema se destacan los posibles problemas que puede encontrar con la recopilación de punto de comprobación y se sugieren soluciones a estos problemas.

Solucionar problemas de la recopilación de punto de comprobación

En general, se reciben mensajes de registro más confiables cuando se desactiva SSL.

Mensaje de registro/ Problema	La recopilación de punto de comprobación no mantiene el ritmo en el que el origen de eventos de punto de comprobación envía eventos.
Causa posible	No ha configurado los parámetros para este origen de eventos de modo que tenga una conexión persistente.
Solución	Para establecer una conexión persistente para un servidor de punto de comprobación, configure los siguientes parámetros de origen de eventos en los siguientes valores: • **Intervalo de sondeo** = -1 • **Duración máxima de encuesta** = 0 • **Máximo de eventos de encuesta** = 0 • **Tiempo máximo de inactividad de encuesta** = 0

Guía de configuración del protocolo de recopilación de archivos

Esta guía le indica cómo configurar el protocolo Recopilación de archivos. Este protocolo recopila eventos desde archivos de registro.

Debe implementar la recopilación de registros antes de poder configurar el protocolo Recopilación de archivos.

Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Para configurar el recopilador de agente de SFTP, consulte los siguientes temas:

- Para configurar el agente de SFTP en Windows, consulte Instalar y actualizar el agente de SFTP.
- Para configurar el agente de SFTP en Linux, consulte Configurar la transferencia de archivos del script de shell de SFTP.

Conceptos básicos

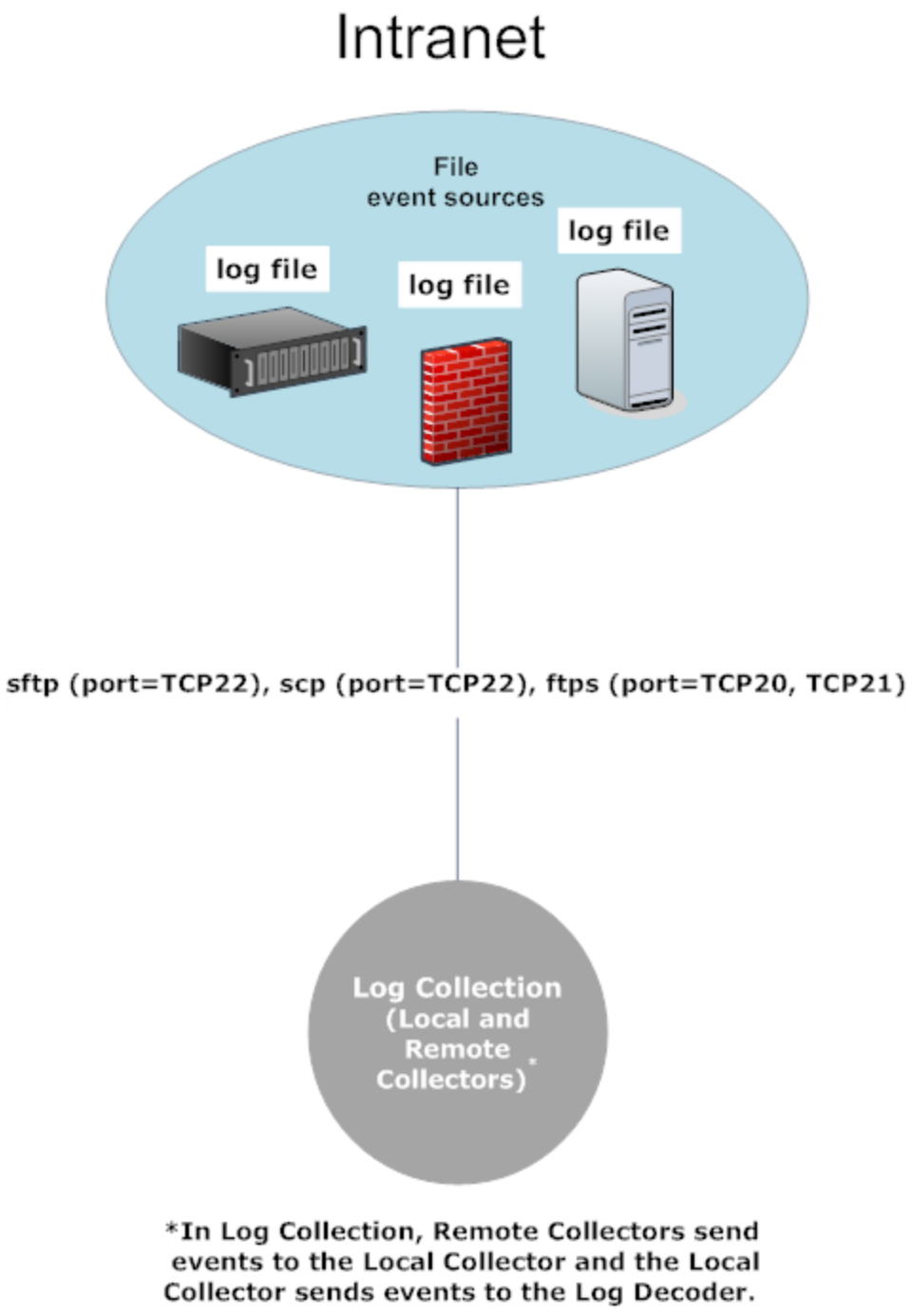
Esta guía le indica cómo configurar el protocolo de recopilación de archivos que recopila eventos desde archivos de registro. Los orígenes de eventos para este protocolo generan archivos de registro que se transfieren al servicio de Log Collector a través de un método de transferencia segura de archivos.

Cómo funciona la recopilación de archivos

El servicio de Log Collector recopila eventos desde archivos de registro. Los orígenes de eventos generan archivos de registro que se transfieren al host de Log Decoder que ejecuta el servicio de Log Collector a través de un método de transferencia segura de archivos.

Escenario de implementación

El protocolo de recopilación de archivos recopila datos de eventos desde archivos de registro.

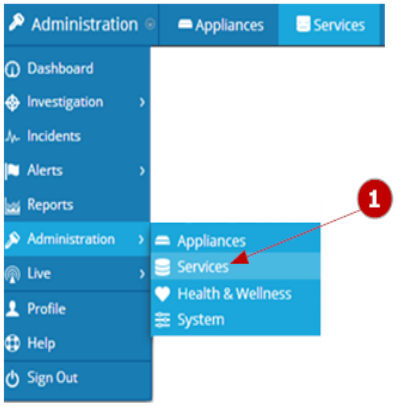

Intranet
File
event sources
log file
log file
log file
sftp (port=TCP22), scp (port=TCP22), ftps (port=TCP20, TCP21)
Log Collection
(Local and
Remote
Collectors)*
*In Log Collection, Remote Collectors send
events to the Local Collector and the Local
Collector sends events to the Log Decoder.

Procedimientos

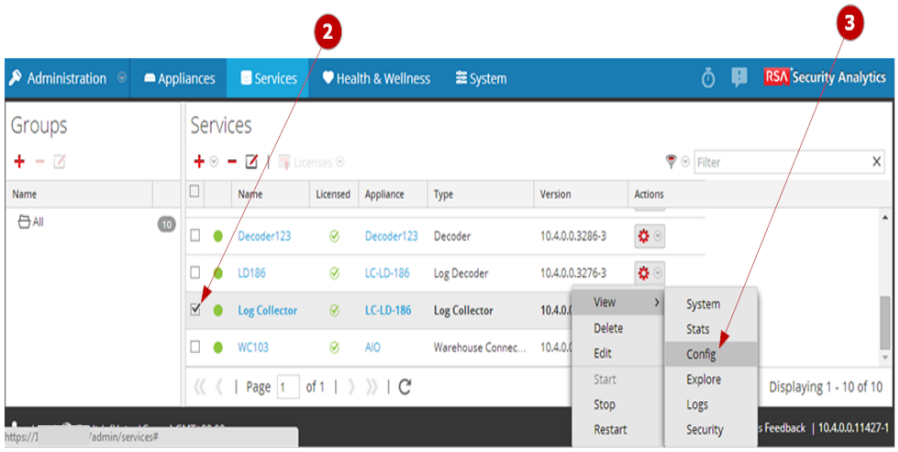
Configurar el protocolo de recopilación de archivos en Security Analytics

Debe configurar el Log Collector para usar la recopilación de archivos para un origen de eventos en la pestaña Origen de evento de la vista de parámetros de Log Collector. En la siguiente figura se representa el flujo de trabajo básico para configurar un origen de eventos para la recopilación de archivos en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de archivo en Security Analytics para obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de archivos.
- Recopilación de archivos: Parámetros de configuración para obtener una descripción detallada de cada parámetro del protocolo de recopilación de archivos.

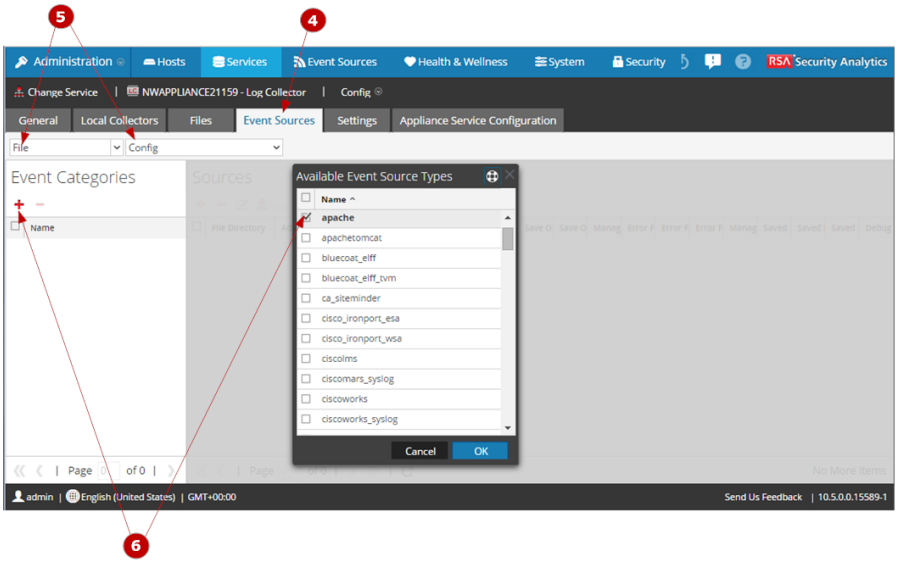


1. Acceda a la vista **Servicios**.



2. Seleccione un servicio de recopilación de registros.

3. Haga clic en  bajo **Acciones** y seleccione **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.

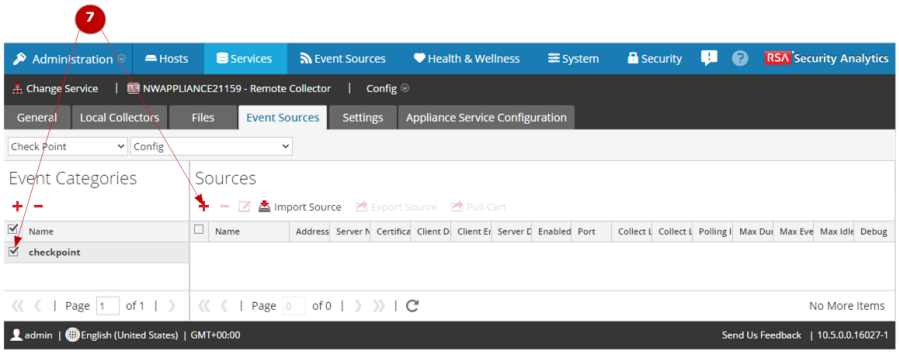


4. Haga clic en la pestaña **Orígenes de evento**.

5. Seleccione **Archivo** como el protocolo de recopilación y elija **Configuración**.

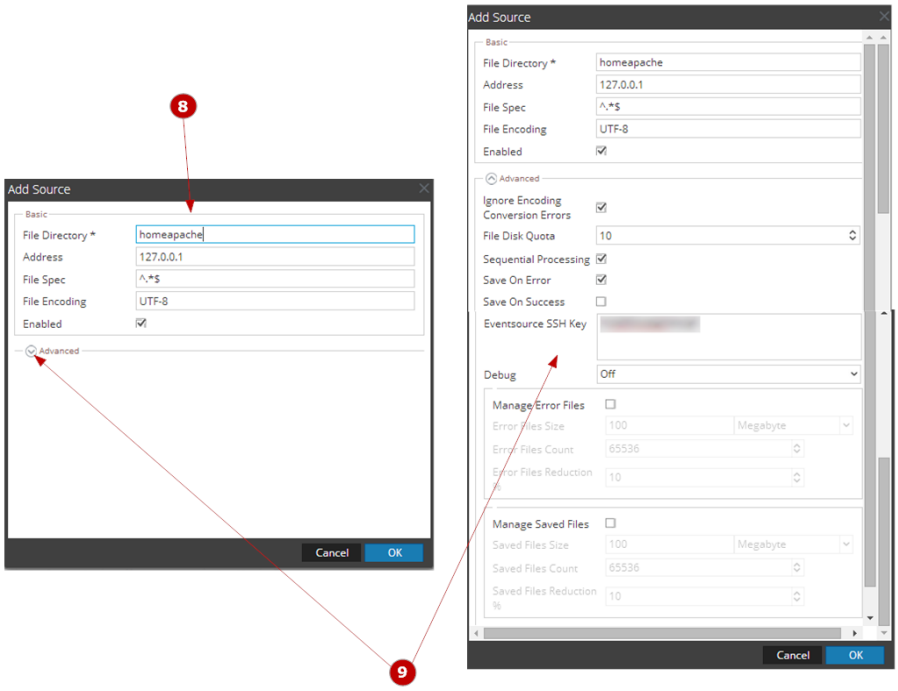
6. Haga clic en + y seleccione un tipo de origen de eventos (por ejemplo, **apache**) como la categoría de origen de eventos.

La categoría de origen de eventos es parte del contenido que descargó de LIVE.



7. Seleccione la categoría recién agregada (por ejemplo, **apache**).

Haga clic en +.



8. Especifique los parámetros básicos requeridos para el origen de eventos.

9. Haga clic en ⌄ y especifique parámetros adicionales que mejoran la manera en que el protocolo maneja la recopilación de eventos para el origen de eventos.

Configurar orígenes de eventos para usar el protocolo de recopilación de archivos

Debe configurar cada origen de eventos que utilice el protocolo de recopilación de archivos para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de archivo para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de archivos, con una lista de verificación que contiene cada paso de configuración

Los pasos de configuración del protocolo de recopilación de archivos se deben realizar en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de la configuración de la recopilación de archivos

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de archivo en Security Analytics.	
2	Configurar orígenes de eventos de archivo para enviar eventos a Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de archivos configurado.	
4	Verificar que la recopilación de archivos esté funcionando.	

Paso 1. Configurar orígenes de eventos de archivo en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de archivo en Security Analytics.

Después de realizar este procedimiento, habrá...

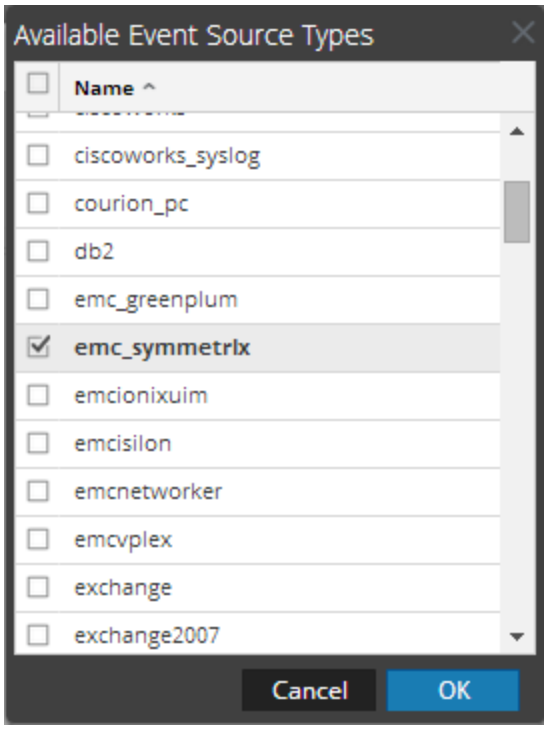
- Configurado la recopilación de archivos para un origen de eventos en Security Analytics.
- Modificado la recopilación de archivos para un origen de eventos en Security Analytics.
- Verificado que se haya habilitado el analizador correcto en el Log Decoder para analizar los eventos del registro del nuevo origen de eventos.

Volver a Procedimientos

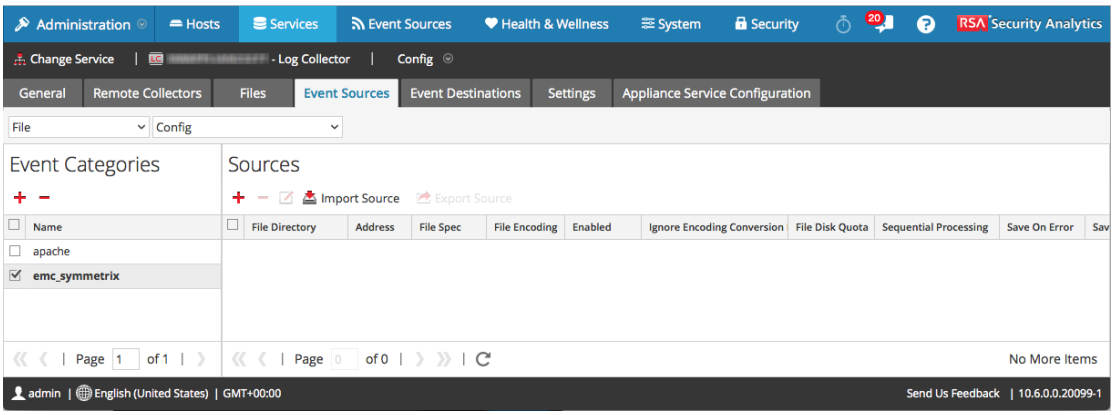
Procedimientos

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Archivo/Configurar** en el menú desplegable.

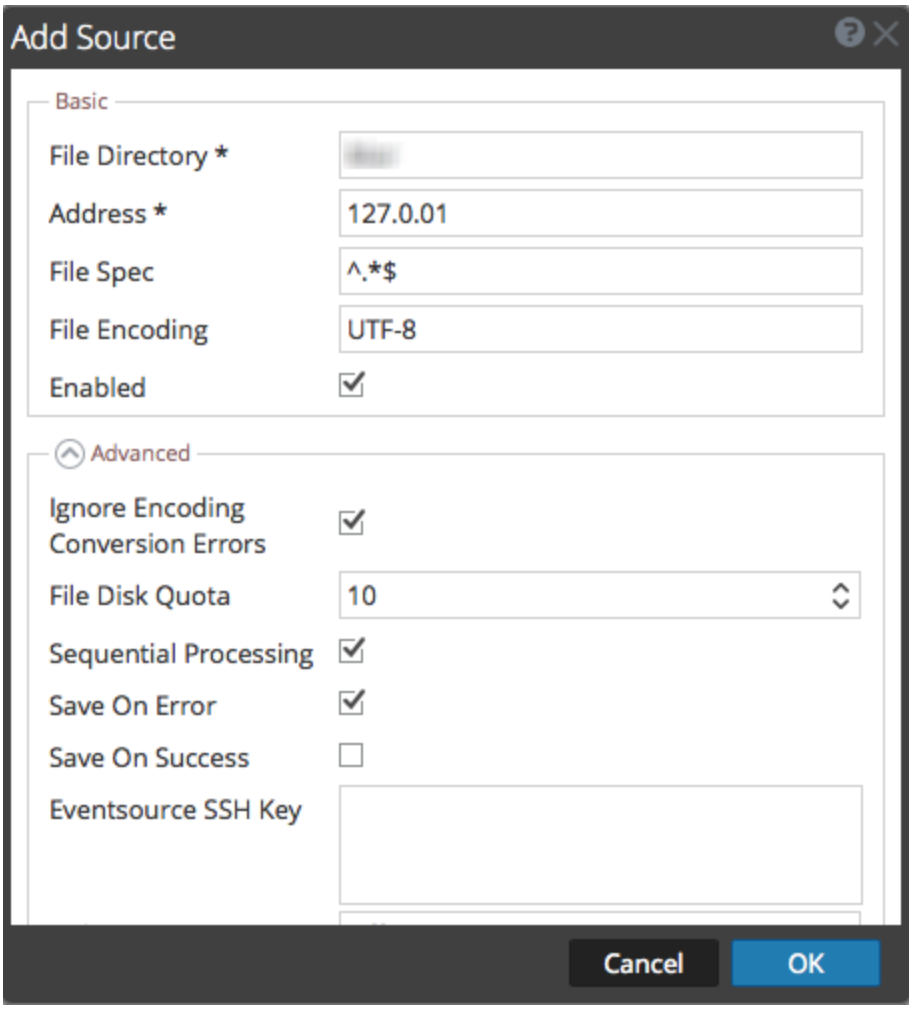
5. En la barra de herramientas del panel **Categorías de evento**, haga clic en  .



6. Seleccione un tipo de origen de eventos (por ejemplo, **emc_symmetrix**) y haga clic en **Aceptar**.
   El tipo de origen de eventos recién agregado se muestra en el panel Categorías de evento.



7. Seleccione el nuevo tipo en el panel **Categorías de evento** y haga clic en  en la barra de herramientas Orígenes.
   Se muestra el cuadro de diálogo **Agregar origen**.
8. Agregue un nombre de **directorio de archivo** y modifique cualquier otro parámetro que requiera cambios.



9. Para obtener la clave pública e ingresarla en el cuadro de diálogo, realice lo siguiente:
   a. Seleccione y copie la clave pública desde el origen de eventos mediante la ejecución de: **cat ~/.ssh/id_rsa.pub**
   b. Pegue la clave pública en el campo **Clave del protocolo SSH del origen de eventos**.
10. Haga clic en **Aceptar**.

Para que sus cambios surtan efecto, debe reiniciar la recopilación de archivos.

Configurar los directorios de carga de Security Analytics

Después de haber agregado y configurado el origen de eventos mediante la GUI de Security Analytics, debe configurar correctamente los directorios de carga.

1. Cambie al **directorio /var/netwitness/logcollector**.
2. Cambie el propietario del directorio de carga al usuario sftp:
   chown sftp /var/netwitness/logcollector/upload

3. Cambie el grupo del directorio de carga al usuario sftp:
   chgrp -R sftp /var/netwitness/logcollector/upload
4. Asegúrese de que el directorio /upload tenga los permisos correctos:
   chmod -R 775 /var/netwitness/logcollector/upload
5. Opcional: Configure un trabajo **cron** para ejecutar el script en los intervalos de tiempo que desee. Si configura un trabajo cron, asegúrese de ejecutarlo como el usuario sftp

Detener y reiniciar la recopilación de archivos

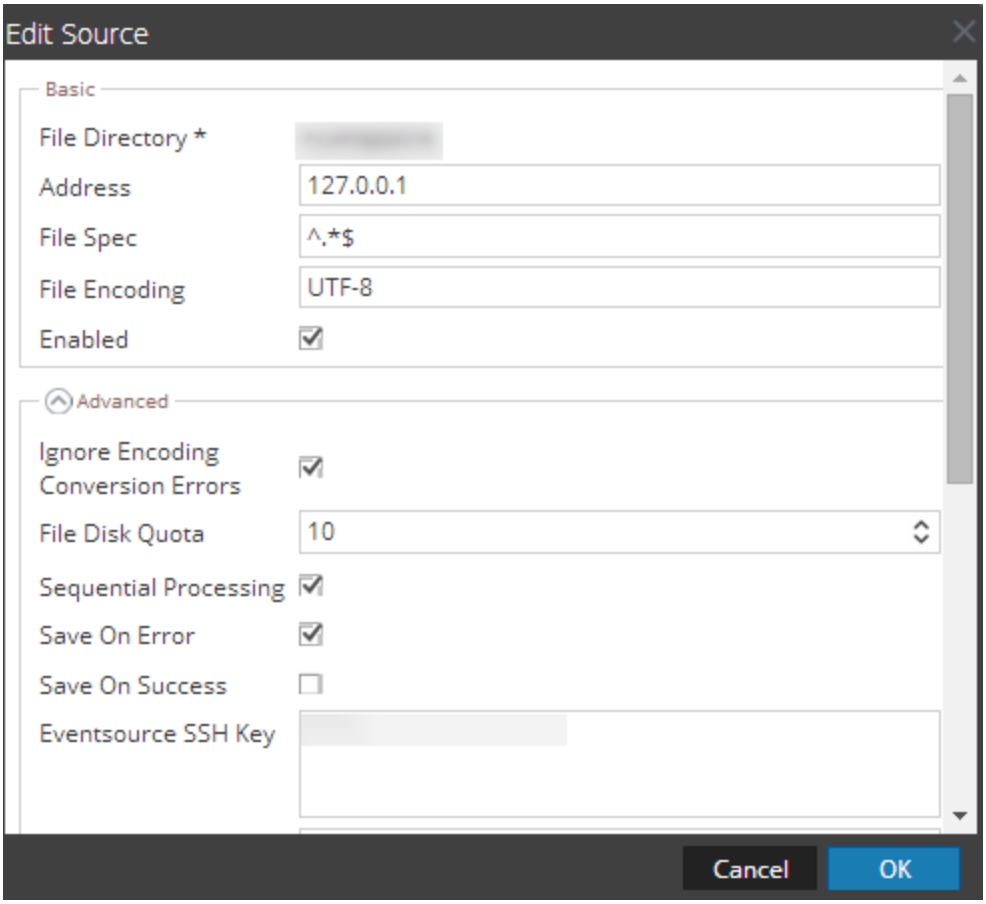
Después de agregar un nuevo origen de eventos que usa la recopilación de archivos, debe detener y reiniciar el servicio de recopilación de archivos de Security Analytics. Esto es necesario para agregar la clave al nuevo origen de eventos.

Modificar la recopilación de archivos para un origen de eventos en Security Analytics

Para modificar un origen de eventos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Archivo/Configurar** en el menú desplegable.
5. Seleccione un tipo de origen de eventos (por ejemplo, **emc_symmetrix**) en el panel **Categorías de evento** y haga clic en **Aceptar**.
6. En el panel **Orígenes**, seleccione un origen de eventos y haga clic en  .
   Se muestra el cuadro de diálogo **Editar origen**.

7. Modifique los parámetros que necesiten cambios y haga clic en **Aceptar**.



8. Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado.

Parámetros

Recopilación de archivos: Parámetros de configuración

(Opcional) Crear un archivo typespec de contenido personalizado para la recopilación de archivos

En este tema se indica cómo crear un archivo typespec personalizado para la recopilación de archivos.

Contexto

En este tema se indica cómo crear un archivo typespec personalizado para Log Collector. En el tema se incluye:

- Procedimiento Crear un archivo typespec personalizado
- Sintaxis de typespec para la recopilación de archivos
- Ejemplo de recopilación de archivos

Volver a Procedimientos

Procedimiento

Para crear un archivo **typespec** personalizado:

1. Copie un archivo typespec existente y guárdelo en el mismo directorio.
   Por ejemplo, copie el archivo **apache.xml** desde **/etc/netwitness/ng/logcollection/content/collection/file** y guárdelo con un nombre nuevo en el mismo directorio.
2. Modifique el archivo de acuerdo con los requisitos.
3. Reinicie Log Collector.
4. No podrá ver el nuevo tipo de dispositivo en Security Analytics hasta que reinicie Log Collector.

Sintaxis de typespec para la recopilación de archivos

Sintaxis	Descripción
`<?xml version="1.0" encoding="UTF-8"?>`	No modifique esta línea.
`<typespec>`	No modifique esta línea.

Sintaxis	Descripción
`<name>eventsource</name>`	<event source="source" name.="name." replace="replace"> Reemplace eventsource por el nombre del origen de eventos de archivo (por ejemplo, apache). Security Analytics muestra este nombre en el panel Orígenes de la pestaña Ver > Configuración > Orígenes de eventos. </event> Un valor válido es una cadena alfanumérica. No puede usar - (guiones), _ (guiones bajos) ni espacios. El nombre debe ser único entre todos los archivos typespec en la carpeta.
`<type>file</type>`	Tipo de origen de eventos (archivos, ODBC, Windows, etc.). No modifique esta línea.

Sintaxis	Descripción
<prettyName>event-source-name</prettyName>	Nombre definido por el usuario para el origen de eventos. Puede usar el mismo valor comonombre (por ejemplo, apache) o usar un nombre más descriptivo.
<version>1.0</version> <</td>	Versión de este archivo typespec. El valor predeterminado es 1.0.
<author>author-name</author>	Persona que creó el archivo typespec. Reemplace author-name por su nombre.
<description>formal-description</description>	Descripción formal del origen de eventos. Reemplace formal-description por su descripción del origen de eventos.
<dispositivo>	No modifique esta línea.
<name>event-source</name>	Nombre del origen de eventos. Reemplace event-source por el nombre del origen de eventos de archivo (por ejemplo, apache).
</device>	No modifique esta línea.

Sintaxis	Descripción
<configuración> </configuration>	No se utiliza en la recopilación de archivos.
<recopilación>	No modifique esta línea.
<file>	La sintaxis en <file> se usa para la recopilación y el procesamiento de eventos.
<parserId>file.event-source-name</parserId>	“Reservado para una versión futura”.
<processorType>processor-type</processorType>	Tipo de procesador. Como ejemplo de processor-type tenemos generic, xml, tagvalmap y oracle. Los tipos de procesador son similares a controladores en RSA enVision.<</p>
<dataStartLine>n</dataStartLine>	n es el número de línea en el archivo de registro en el cual Security Analytics comienza a recopilar eventos. El valor predeterminado es 1.

Sintaxis	Descripción
`<fieldDelim>x</fieldDelim>`	Especifique el delimitador que se usará para separar los campos. Especifique cualquiera de los siguientes valores para x: • || (barra vertical) • ^ (intercalación) • , (coma) • : (dos puntos) • 0x20 (para un espacio)
`<idField>n</idField>`	Número de campo de Msg ID (ID de mensaje). Por ejemplo, especifique 6 para n para identificar el sexto campo desde el evento delimitado por espacio como Msg ID.
`<lineDelim>x</lineDelim>`	El delimitador de línea que detecta el fin de un evento. Por ejemplo, especifique \n para x para proporcionar valores en hexadecimal para CR y LF.

Sintaxis	Descripción
`<eventGroups>`	La sintaxis en <eventGroups> solo se usa cuando processorType = xml.
`<eventGroup>`	No modifique esta línea.
`<globalInfo></globalInfo>`	xpath de globalInfo. Lee información de nodo principal y la agrega a cada nivel.
`<eventXPath>//Audit/AuditRecord</eventXPath>`	xpath de eventos
`</eventGroup>`	No modifique esta línea.
`</eventGroups>`	Fin de etiquetas de tipo de procesador xml. No modifique esta línea.
La recopilación de archivos usa las siguientes etiquetas durante la transformación de eventos:	
`<transformPrefixTag>prefix</transformPrefixTag>`	Inserta el prefijo especificado frente al evento transformado. Por ejemplo, si especifica **APACHE**, Security Analytics inserta **%APACHE** como prefijo.

Sintaxis	Descripción
`<transformReplaceFieldDelim>n </transformReplaceFieldDelim>`	Reemplazar/no reemplazar delimitador durante el indicador de transformación. Los valores válidos para n son: • **0** (predeterminado) = no reemplazar • **1** = reemplazar
`<transformPrefixFilename>n </transformPrefixFilename>`	Agregar/no agregar prefijo (por ejemplo, **APACHE**) para el nombre de archivo durante la marca de transformación. Los valores válidos para ***n*** son: • **0** (predeterminado) = no agregar • **1** = agregar

Sintaxis	Descripción
`<transformMultipleDelimiterAsOne>n </transformMultipleDelimiterAsOne>`	Combinar/no combinar múltiples delimitadores secuenciales en uno. Los valores válidos para ***n*** son: • **0** = no combinar • **1** (predeterminado) = combinar
`<transformReplacementFieldDelim>x </transformReplacementFieldDelim>`	Reemplace los delimitadores de campo crudo por los valores dados (x) si el indicador transformReplaceFieldDelim = 1.
`</file>`	No modifique esta línea.
`</collection>`	No modifique esta línea.
`</typespec>`	No modifique esta línea.

Ejemplo de archivo typespec de recopilación de archivos

```
-# Sample apache typespec , file collection

<&lt;?xml>

  <typespec>
  <name>apache</name>
```

```
  <type>file</type>

  <prettyName>apache</prettyName>

  <version>1.0</version>

  <author>administrator</author>

  <description>FileCollection specification for eventsource
type "Apache Web Server" using file handler type
"APACHE"</description>

    <dispositivo>

    <name>apache</name>



<   >

  </configuration>

  <recopilación>

    <file>
```

-# below tags are used for event collection and processing

```
    <parserId>file.apache</parserId>
        <processorType>generic</processorType>
    <dataStartLine>1</dataStartLine>
        <fieldDelim>0x20</fieldDelim>
    <idField>6</idField>
```

```
<lineDelim>\n</lineDelim>
  -# below tags are used only when processorType = xml
<eventGroups>

<eventGroup>

  <globalInfo></globalInfo>

  <eventXPath>//Audit/AuditRecord</eventXPath>

</eventGroup>

</eventGroups>

-# xml processortype specific tags ends

-# below tags are used during event transformation

  <transformPrefixTag>APACHE</transformPrefixTag>

  <transformReplaceFieldDelim>0</transformReplaceFieldDelim>

  <transformPrefixFilename>0</transformPrefixFilename>

  <transformMultipleDelimiterAsOne>1</transformMultipleDelimiterAsOne>

  <transformReplacementFieldDelim></transformReplacementFieldDelim>

</file>

</collection>
</typespec>
```

Paso 2. Configurar orígenes de eventos de archivo para enviar eventos a Security Analytics

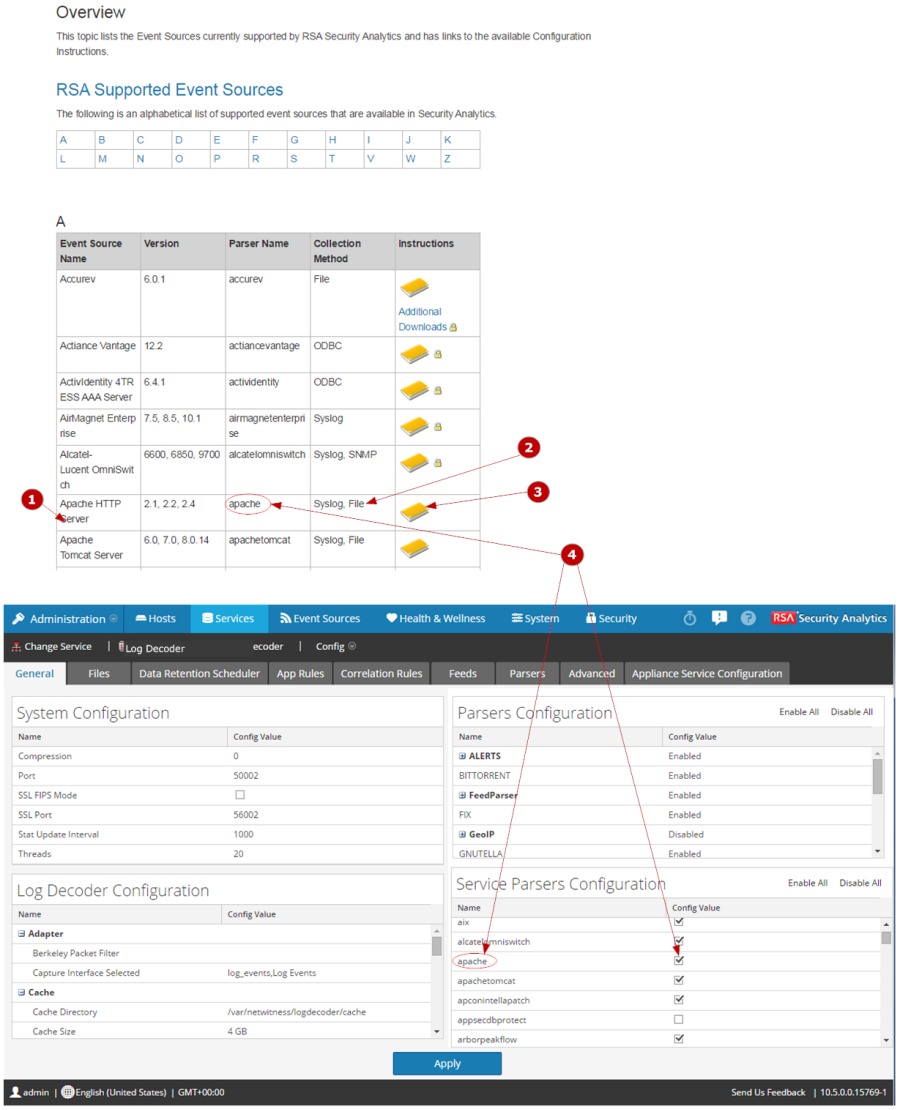
En este tema se indica dónde encontrar los orígenes de eventos que son compatibles actualmente con la recopilación de archivos y las instrucciones de configuración disponibles para cada origen de eventos

La lista de Orígenes de eventos compatibles de RSA es una lista alfabética de todos los orígenes de eventos que son compatibles actualmente con Security Analytics, en la cual se identifican los orígenes de eventos que puede usar con la recopilación de archivos.

Volver a Procedimientos

Procedimiento

Para verificar que los orígenes de eventos estén configurados correctamente:



1 Busque el nombre del origen de eventos.

2 Verifique que sea compatible con el **protocolo de recopilación de archivos** 3 Haga clic en  para ver las instrucciones de configuración del origen de eventos.

4 Verifique que haya descargado el analizador correcto (por ejemplo, apache) desde LIVE a Log Decoder y que lo haya habilitado.

Ejemplo de instrucciones de configuración

La siguiente ilustración se toma de las instrucciones de configuración de Apache HTTP Server.

RSA Security Analytics

Event Source Log Configuration Guide

RSA

Apache HTTP Server

Last Modified: Thursday, February 19, 2015

Event Source Product Information:

Vendor: Apache
Event Source: HTTP Server
Versions: 2.1, 2.2, 2.4
Additional Downloads: sftpagent.conf.apache, nicsftpagent.conf.apache

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: apache
Collection Method: File, Syslog
Event Source Class.Subclass: Host.Web Logs

Paso 3. Iniciar el servicio para el protocolo de recopilación de archivos configurado

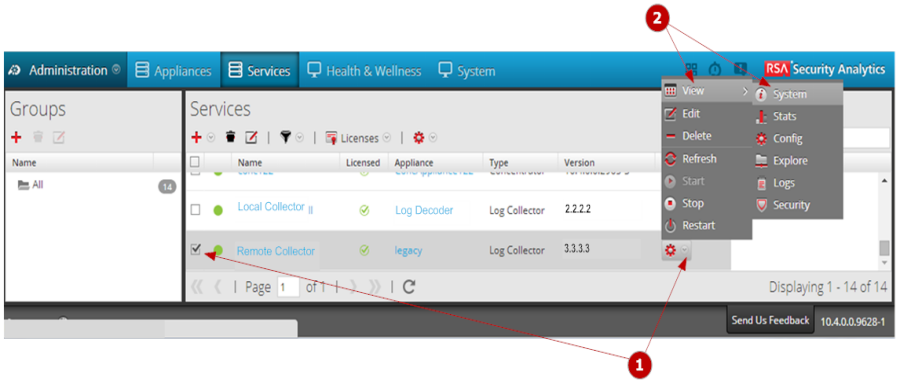
En este tema se indica cómo iniciar un servicio de recopilación de archivos detenido.

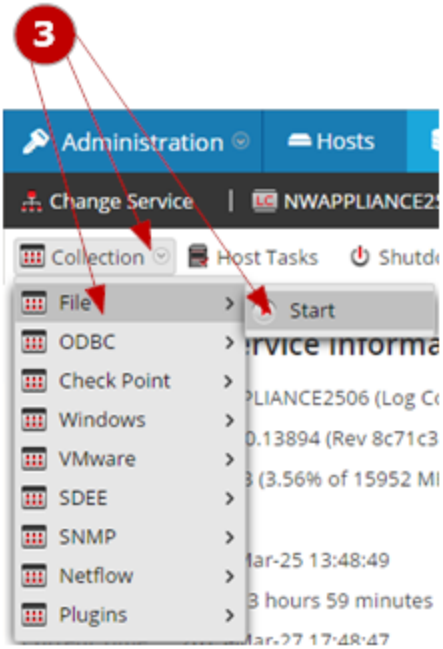
Si un servicio de recopilación de archivos se detuvo, tal vez deba iniciarlo nuevamente.

Volver a Procedimientos

Procedimiento

En la siguiente figura se muestra cómo iniciar un servicio de recopilación. Consulte el tema **Habilitar el inicio automático de servicios individuales** de la *Guía de configuración de la recopilación de registros* si desea que el servicio se inicie automáticamente.





1. Seleccione un servicio Log Collector y haga clic en  bajo **Acciones**.
2. Haga clic en **Ver > Sistema**.
3. Haga clic en **Recopilación > Archivo** y, a continuación, en **Iniciar**.

Paso 4. Verificar que la recopilación de archivos esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de archivos se configuró correctamente.

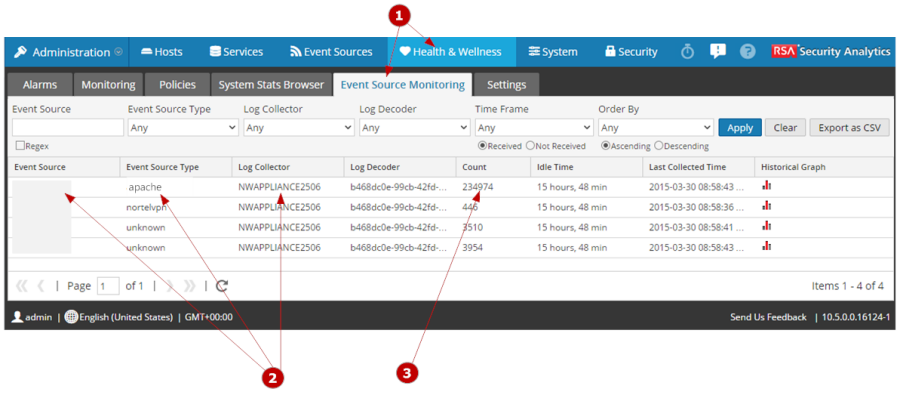
Volver a Procedimientos

Contexto

Debe verificar que la recopilación de archivos se haya configurado correctamente para asegurarse de que funcione.

Procedimiento

En la siguiente figura se ilustra cómo verificar que la recopilación de archivos esté funcionando desde la pestaña **Administration > Estado y condición >Monitoreo de orígenes de eventos**.

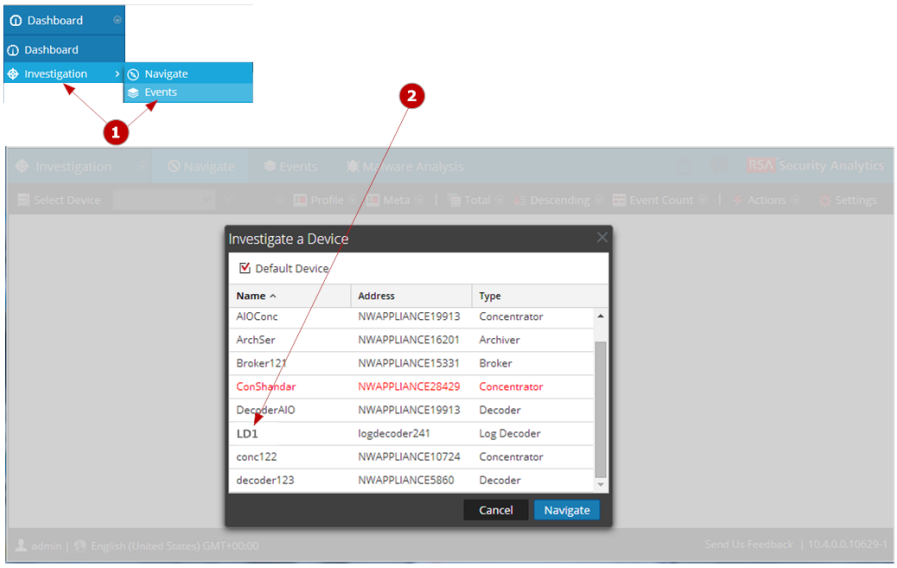


1 Acceda a la pestaña **Monitoreo de orígenes de eventos** desde la vista **Administration > Estado y condición**.

2 Busque Log Decoder, Origen de eventos y Tipo de origen de evento (por ejemplo, **apache**).

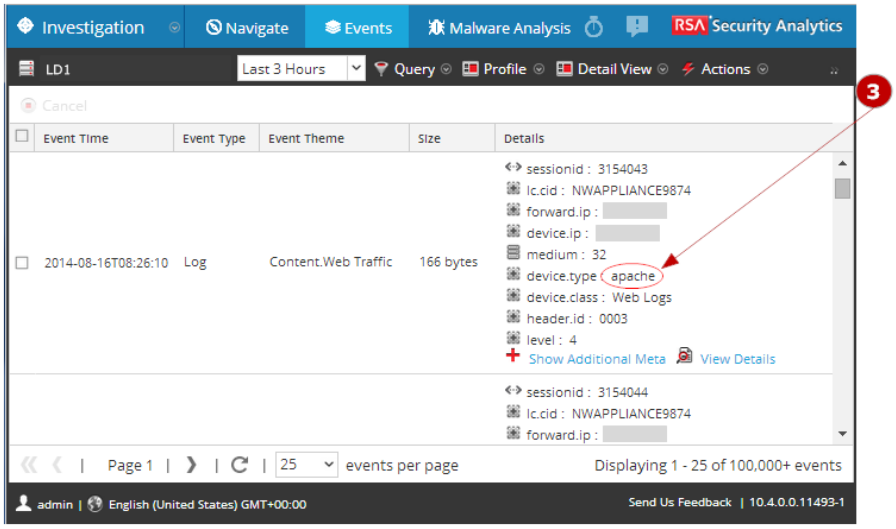
3 Busque actividad en la columna **Conteo** para verificar que la recopilación de archivos esté aceptando eventos.

En la siguiente figura se ilustra cómo puede verificar que la recopilación de archivos esté funcionando desde **Investigation > vista Eventos**.



1 Acceda a **Investigation > vista Eventos**.

2 Seleccione los eventos de recopilación de archivos del Log Decoder (por ejemplo, **LD1**) en el cuadro de diálogo **Investigar un dispositivo**.



3 Busque un analizador de orígenes de eventos de archivos (por ejemplo, **apache**) en la columna **Tipo de dispositivo** para verificar que la recopilación de archivos esté aceptando eventos.

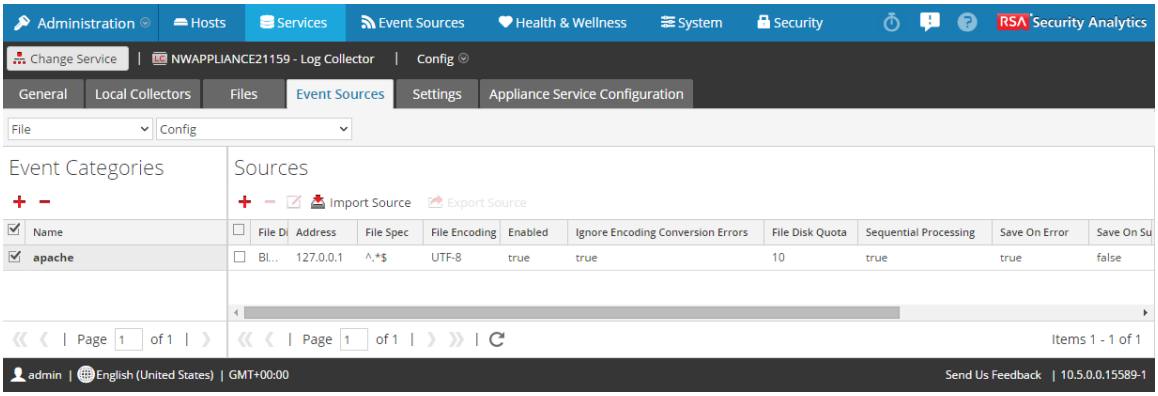
Recopilación de archivos: Parámetros de configuración

En este tema se describe la interfaz del usuario para configurar la recopilación de archivos.

Use esta sección cuando busque descripciones de la interfaz del usuario de recopilación de archivos y definiciones de las funciones de la interfaz del usuario.

Para acceder a los parámetros de configuración de la recopilación de archivos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Archivo/Configurar** en el menú desplegable.



La vista Archivo/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar los tipos de orígenes de eventos correspondientes.

Característica	Descripción
	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.

Característica	Descripción
	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de tipos de orígenes de eventos compatibles.

Característica	Descripción
	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

Nota: El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de los tipos de orígenes de eventos compatibles que se han descargado desde el archivo Especificación de tipo de lector de archivos genérico (GFTS). Si no ve ningún tipo de origen de eventos en esta lista, no cargó el contenido disponible con la actualización de Log Collector para esta versión.

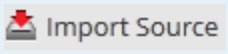
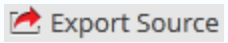
Panel Orígenes

Use este panel para revisar, agregar, modificar y eliminar los directorios de archivo de origen de eventos y sus parámetros del tipo de origen de eventos que seleccionó en el panel Categorías de evento.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar origen, en el cual puede definir los parámetros para un host de firewall.

Característica	Descripción
	Elimina el host que seleccionó.
	Abre el cuadro de diálogo Editar origen, en el cual puede editar los parámetros del origen de eventos seleccionado. Seleccione varios orígenes de eventos y haga clic en  para abrir el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar hosts de forma masiva desde un archivo de valores separados por comas (CSV). Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo .csv que contiene los parámetros de los hosts seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.

Cuadro de diálogo Agregar/Modificar origen

En este cuadro de diálogo, se agrega o modifica un directorio de archivos del origen de eventos seleccionado.

Característica	Descripción
Parámetros del origen Netflow	Muestra los parámetros de origen de eventos de Netflow completados con los valores predeterminados. Ingrese o modifique los valores apropiados.
Cancelar	Cierra el cuadro de diálogo sin agregar un directorio de archivo ni guardar los valores de los parámetros del directorio de archivos seleccionado.
OK	En el cuadro de diálogo Agregar origen, agrega el directorio de archivos y sus parámetros. En el cuadro de diálogo Editar origen, aplica los cambios en los valores de los parámetros del directorio de archivos seleccionado.

Parámetros del directorio de archivos

En la siguiente tabla se proporcionan descripciones de los parámetros del origen.

Nombre	Descripción
	Básico
Directorio de archivos*	Directorio de recopilación (por ejemplo, **Eur_London100**) en el cual el origen de eventos de archivos coloca sus archivos. El valor válido es una cadena de caracteres que utiliza la siguiente expresión regular: **[_a-zA-Z][_a-zA-Z0-9]*** Esto significa que el directorio de archivos debe comenzar con una letra seguida de números, letras y guiones bajos. No modifique este parámetro una vez que haya comenzado a recopilar datos de eventos. Después de crear la recopilación, el Log Collector crea los subdirectorios de trabajo, guardado y error debajo del directorio de recopilación.
Dirección*	Dirección IP del origen de eventos. El valor válido es una **dirección IPv4**, una **dirección IPv6** o un **nombre de host** que incluye un nombre de dominio calificado.
Especificación de archivo	Expresión regular. Por ejemplo, **^.*$** = procesa todo.
Codificación de archivo	Codificación del archivo de internacionalización. Ingrese el método de codificación de archivo. Las siguientes cadenas son ejemplos de métodos válidos: • UTF-8 (valor predeterminado) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US

Nombre	Descripción
Activado	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
	Avanzado
Omitir errores de conversión de codificación	Seleccione la casilla de verificación para omitir errores de conversión de codificación y datos no válidos. La casilla de verificación está seleccionada de manera predeterminada. **Precaución:** Esto puede provocar errores de análisis y transformación.
Cuota de disco de archivo	Determina cuándo dejar de guardar archivos independientemente de los ajustes de los parámetros **Guardar con error** y **Guardar con éxito**. Por ejemplo, un valor de 10 indica que cuando hay menos de un 10 % de disco restante disponible, el Log Collector deja de guardar archivos para reservar espacio suficiente para el procesamiento normal estimado de la recopilación. **Precaución:** disco disponible se refiere a una partición donde se monta el directorio de recopilación de base. Si el servidor de Log Decoder tiene un tamaño de disco de 10 TB y se asignan 2 TB al directorio de recopilación base, la definición de este valor en 10 hace que la recopilación de registros se detenga cuando quedan menos de 0.2 TB (10 % de 2 TB) de espacio. No significa 10 % de 10 TB. Un valor válido es un número en el rango de **0** a **100**. **10** es el valor predeterminado.
Procesamiento secuencial	Indicador de procesamiento secuencial: • Seleccione la casilla de verificación (valor predeterminado) para procesas los archivos de origen de eventos en el orden de recopilación. • No seleccione la casilla de verificación para procesar en paralelo los archivos de origen de eventos.
Guardar con error	Indicador de guardar con error. Seleccione la casilla de verificación para conservar el archivo de **recopilación de origen de eventos** cuando Log Collector encuentra un error. La casilla de verificación está seleccionada de manera predeterminada.

Nombre	Descripción
Guardar con éxito	Guarda el archivo de **recopilación de origen de eventos** después de procesar el indicador. Seleccione la casilla de verificación para guardar la recopilación de origen de eventos después de procesarla. De forma predeterminada, la casilla de verificación no está seleccionada.
Clave del protocolo SSH del origen de eventos	Clave pública del protocolo SSH que se usa para cargar archivos para este origen de eventos. Consulte Generar un par de claves en el origen de eventos e importar la clave pública a Log Collector para obtener instrucciones sobre la generación de claves. **Nota:** Si la recopilación de archivos se detiene, Security Analytics no actualiza el archivo authorized_keys con la clave pública del protocolo SSH que usted agrega o modifica en este parámetro. Debe reiniciar la recopilación de archivos para actualizar la clave pública. Puede agregar o modificar el valor de la clave pública en este parámetro en varios orígenes de eventos de archivo sin ejecutar la recopilación de archivos, pero Security Analytics no actualizará el archivo **authorized_keys** hasta que se reinicie la recopilación de archivos.
Administrar archivos de error	De manera predeterminada, el Log Collector usa el parámetro **Cuota de disco de archivo** para asegurarse de que el disco no se llene con archivos de error. Si define este parámetro en **verdadero**, puede especificar una de las siguientes opciones: • Espacio máximo asignado para archivos de error en el parámetro **Tamaño de archivos de error**. • Cantidad máxima de archivos de error permitida en el parámetro **Conteo de archivos de error**. También se especifica un porcentaje de reducción, el cual indica al sistema cuánto reducir cuando se alcanza el máximo. Seleccione la casilla de verificación para administrar los archivos de error. De forma predeterminada, la casilla de verificación no está seleccionada.

Nombre	Descripción
Tamaño de archivos de error	Solo es válido si los parámetros **Administrar archivos de error** y **Guardar con error** están definidos en verdadero. Especifica hasta qué punto Security Analytics guarda archivos de error. El valor que especifica es el tamaño total máximo de todos los archivos en el directorio de error. Un valor válido es un número dentro del rango entre **0** y **281474976710655**. Estos valores se especifican en **kilobyte**s, **megabyte**s o **gigabyte**s. **100 megabytes** es el valor predeterminado. Si cambia este parámetro, el cambio no se implementa hasta que reinicie la recopilación o el servicio de Log Collector.
Conteo de archivos de error	Solo es válido si los parámetros **Administrar archivos de error** y **Guardar con error** están definidos en verdadero. La cantidad máxima de archivos de error en el directorio de error. Un valor válido es un número en el rango de **0** a **65536**. **65536** es el valor predeterminado. Si cambia este parámetro, el cambio no se implementa hasta que reinicie la recopilación o el servicio de Log Collector.
% de reducción de archivos de error	Porcentaje por tamaño o conteo de archivos de error que el servicio Log Collector quita cuando se alcanza el tamaño o el conteo máximos. El servicio elimina los archivos más antiguos primero. Un valor válido es un número en el rango de **0** a **100**. **10** es el valor predeterminado.
Administrar archivos guardados	Seleccione la casilla de verificación para administrar los archivos guardados. De forma predeterminada, la casilla de verificación no está seleccionada. De manera predeterminada, el Log Collector usa el parámetro **Cuota de disco de archivo** para asegurarse de que el disco no se llene con archivos guardados. Si selecciona esta casilla de verificación, puede especificar una de las siguientes opciones: • Espacio máximo asignado para archivos guardados en el parámetro **Tamaño de archivos guardados**. • Cantidad máxima de archivos guardados permitida en el parámetro **Conteo de archivos guardados**. También se especifica un porcentaje de reducción, el cual indica al sistema cuánto reducir cuando se alcanza el máximo.

Nombre	Descripción
Tamaño de archivos guardados	Solo es válido si los parámetros **Administrar archivos guardados** y **Guardar con éxito** se definen en verdadero. El tamaño total máximo de todos los archivos en el directorio de almacenamiento. Un valor válido es un número en el rango de **0** a **281474976710655**. Estos valores se especifican en **kilobyte**s, **megabyte**s o **gigabyte**s. **100 megabytes** es el valor predeterminado. Si cambia este parámetro, el cambio no se implementa hasta que reinicie la recopilación o el servicio de Log Collector.
Conteo de archivos guardados	Solo es válido si los parámetros **Administrar archivos guardados** y **Guardar con éxito** se definen en verdadero. La cantidad máxima de archivos guardados en el directorio de almacenamiento. Un valor válido es un número en el rango de **0** a **65536**. **65536** es el valor predeterminado. Si cambia este parámetro, el cambio no se implementa hasta que reinicie la recopilación o el servicio de Log Collector.
% de reducción de archivos guardados	Porcentaje por tamaño o conteo de archivos guardados que el servicio Log Collector quita cuando se alcanza el tamaño o el conteo máximos. El servicio elimina los archivos más antiguos primero. Un valor válido es un número en el rango de **0** a **100**. **10** es el valor predeterminado.
Depurar	**Precaución:** Habilite la depuración (defina este parámetro en **Activado** o **Detallado**) solamente si hay un problema en un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa/desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar).

Nombre	Descripción
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega los parámetros del origen de eventos.

Tareas:

Paso 1. Configurar orígenes de eventos de archivo en Security Analytics

Paso 2. Configurar orígenes de eventos de archivo para enviar eventos a Security Analytics

Recopilación de archivos: solución de problemas

Security Analytics le informa sobre problemas o posibles problemas de Log Collector de las dos maneras siguientes.

- Archivos de registro.
- Vistas de monitoreo del estado y la condición.

Archivos de registro

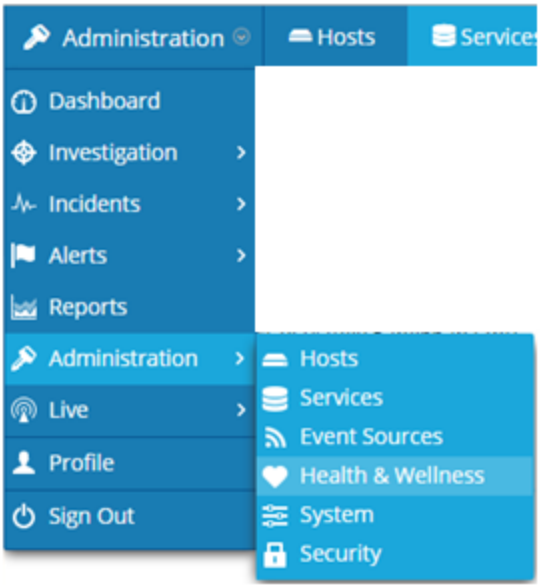
Si un protocolo de recopilación de orígenes de eventos específico presenta problemas, puede revisar los registros de depuración para investigarlos. Cada origen de eventos posee un parámetro de Depuración que puede activar (configurar en Activado o Detallado) para capturar estos registros.

Active la depuración solamente si este origen de eventos presenta problemas y necesita investigarlos. Si activa la depuración en todo momento, esta afectará negativamente al rendimiento de Log Collector.

Security Analytics tiene un conjunto de mensajes de error asociados con la recopilación de registros que incluye en archivos de registro. Para acceder a estos archivos:

Monitoreo del estado y la condición

El monitoreo del estado y la condición le permite informarse oportunamente de posibles problemas de hardware y software de modo que pueda evitar interrupciones. RSA recomienda monitorear los campos estadísticos de Log Collector para asegurarse de que el servicio funcione de manera eficiente y que no se encuentre en los valores máximos configurados ni cerca de estos. Puede monitorear las siguientes estadísticas que se describen en la vista **Administration > Estado y condición**.


Administration
Hosts
Service
Dashboard
Investigation
Incidents
Alerts
Reports
Administration
Live
Profile
Sign Out
Hosts
Services
Event Sources
Health & Wellness
System
Security

Guía de configuración de la recopilación de Netflow

En esta guía se indica cómo configurar el protocolo de recopilación de Netflow. Este protocolo recopila eventos de Netflow v5 y Netflow v9.

Antes de configurar el protocolo de recopilación de Netflow, debe implementar la recopilación de registros.

Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Conceptos básicos

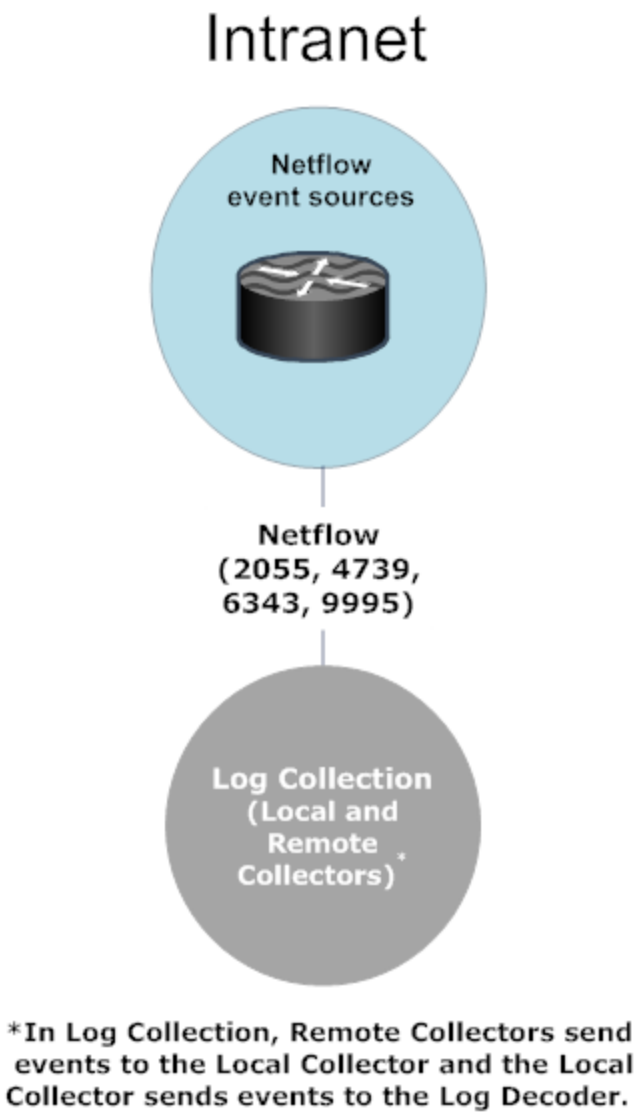
En esta guía se explica cómo configurar el protocolo de recopilación de Netflow que acepta eventos de Netflow v5 y Netflow v9. Este protocolo se usa para aceptar eventos con fines de seguridad, no con fines de rendimiento de la red. Esto significa que debe escoger aceptar eventos solo de puntos estratégicos seleccionados en su red (no de cualquier parte).

Cómo funciona la recopilación de Netflow

El servicio Log Collector recopila eventos de Netflow v5 y Netflow v9.

Escenario de implementación

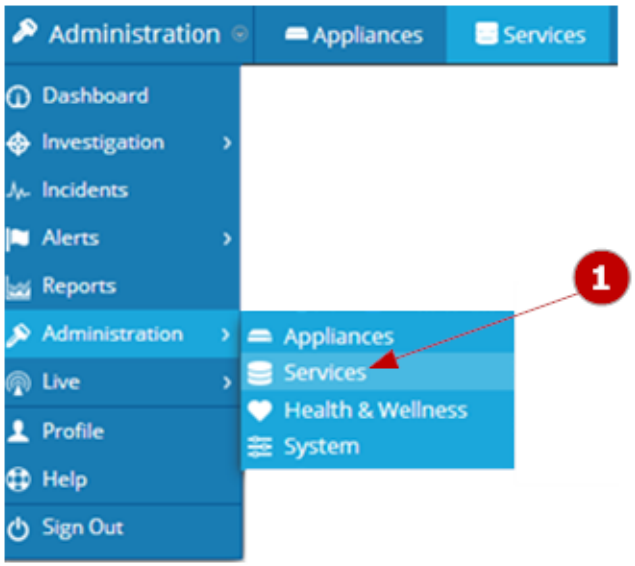
En la siguiente figura se ilustra cómo debe implementar el protocolo de recopilación de Netflow en Security Analytics.



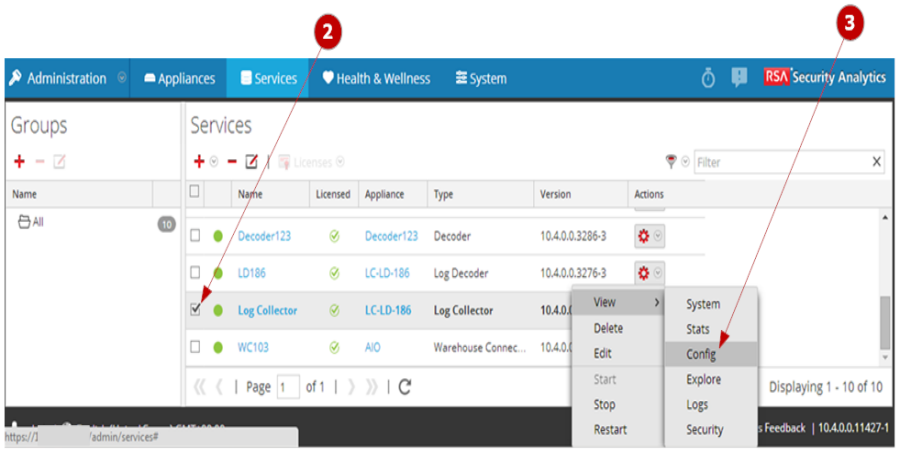
Configurar el protocolo de recopilación de Netflow en Security Analytics

Debe configurar el Log Collector para usar la recopilación de Netflow para un origen de eventos en la pestaña Origen de eventos de la vista Parámetro de Log Collector. En la siguiente figura se representa el flujo de trabajo básico para configurar un origen de eventos para la recopilación de Netflow en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de Netflow en Security Analytics para obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de Netflow.
- Referencias: Parámetros de configuración de la recopilación de Netflow para obtener una descripción detallada de cada parámetro del protocolo de recopilación de Netflow.

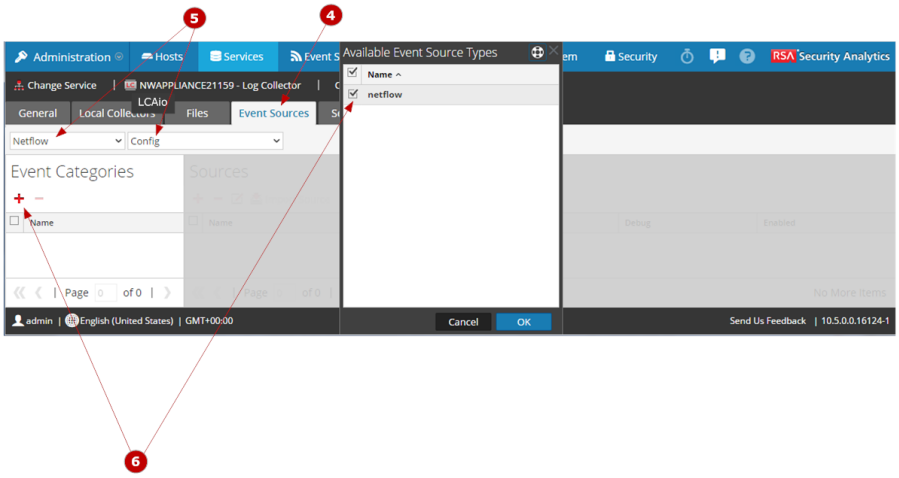


1 Acceda a la vista **Servicios**.



2 Seleccione un servicio de **recopilación de registros**.

3 Haga clic en bajo **Acciones** y seleccione **Ver> Configuración** para mostrar las pestañas de **parámetros de configuración de la recopilación de registros**.

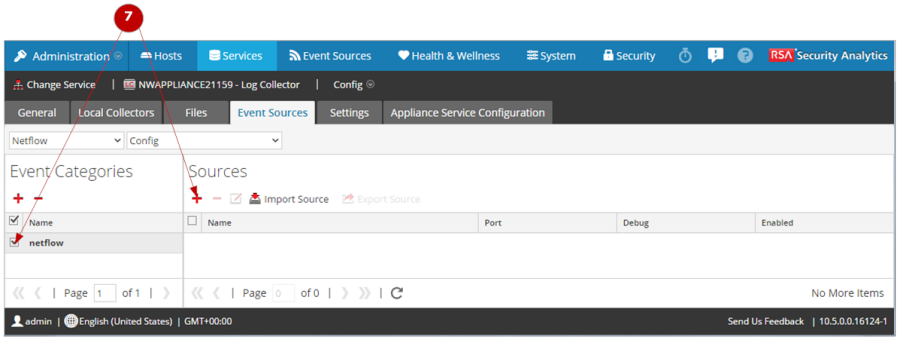


4 Haga clic en la pestaña **Orígenes de evento**.

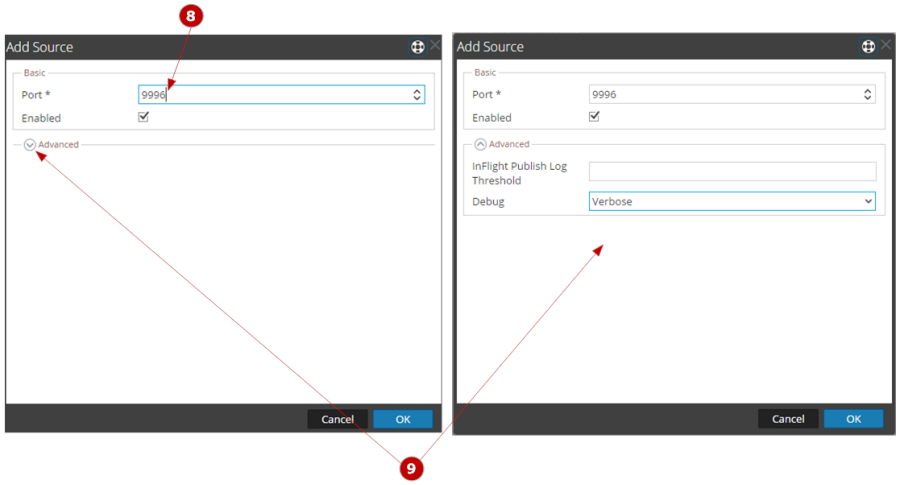
5 Seleccione **Netflow** como el protocolo de recopilación y seleccione **Configuración**.

6 Haga clic en + y seleccione **Netflow** en la categoría de orígenes de eventos.

La categoría de origen de eventos es parte del contenido que descargó de LIVE.



7 Seleccione **Netflow** como la categoría y haga clic en +.



8 Especifique los parámetros básicos requeridos para el origen de eventos de Netflow.

9 Haga clic en y especifique parámetros adicionales que mejoran la manera en que el protocolo de Netflow maneja la recopilación de eventos para el origen de eventos.

Configurar los orígenes de eventos para usar el protocolo de recopilación de Netflow

Debe configurar cada origen de eventos que utilice el protocolo de recopilación de Netflow para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de Netflow para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de Netflow, con una lista de verificación que contiene cada paso de configuración.

Los pasos de configuración del protocolo de recopilación de Netflow se deben realizar en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de la configuración de la recopilación de Netflow

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de Netflow en Security Analytics.	
2	Configurar orígenes de eventos de Netflow para enviar eventos a Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de Netflow configurado.	
4	Verificar que la recopilación de Netflow esté funcionando.	

Paso 1. Configurar orígenes de eventos de Netflow en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de Netflow para Log Collector.

Después de realizar este procedimiento, habrá...

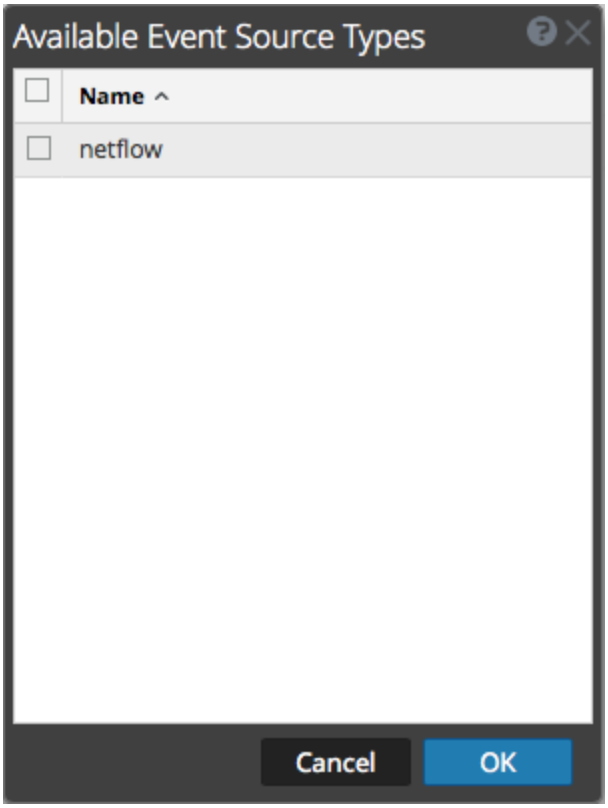
- Configurado un origen de eventos de Netflow.
- Modificado un origen de eventos de Netflow.

Volver a Procedimientos

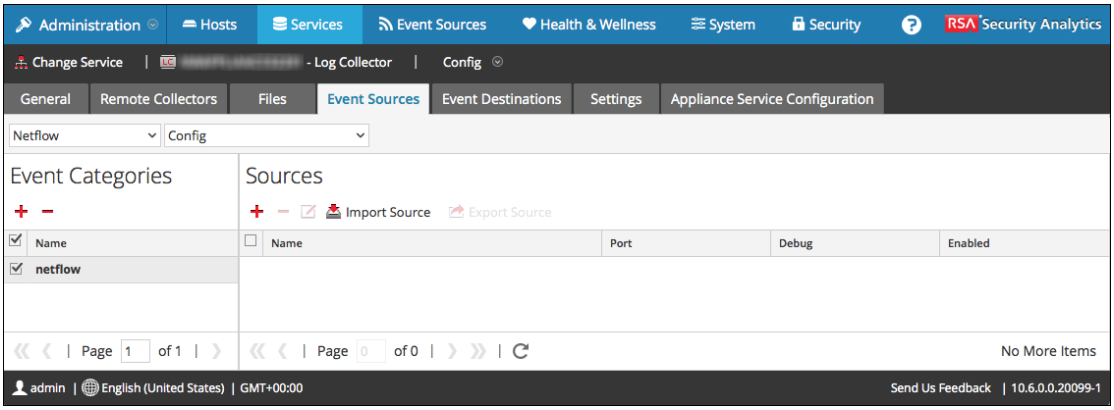
Procedimientos

Paso 1. Configurar orígenes de eventos de Netflow en Security Analytics

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Netflow/Configurar** en los menús desplegables.
5. En la barra de herramientas del panel **Categorías de evento**, haga clic en .

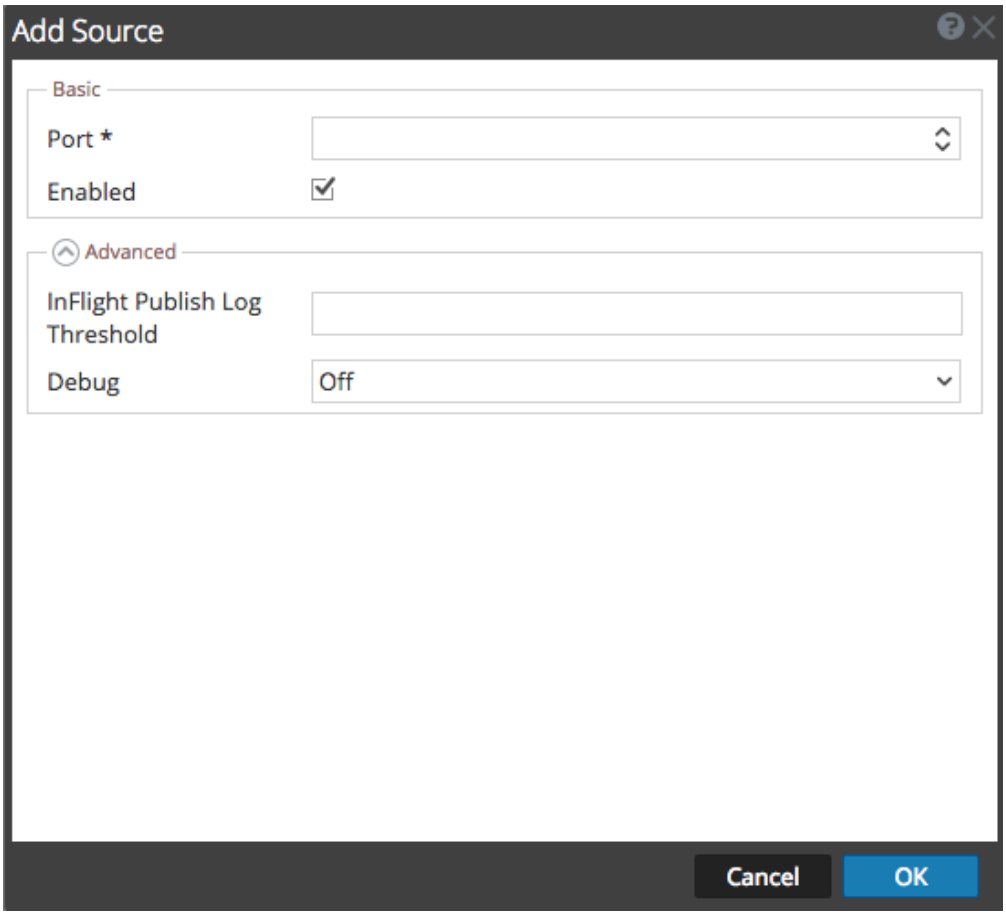


6. Seleccione un tipo de origen de eventos (por ejemplo, netflow) y haga clic en **Aceptar**.
   El tipo de origen de eventos recién agregado se muestra en el panel **Categorías de evento**.



7. Seleccione el nuevo tipo en el panel **Categorías de evento** y haga clic en + en la barra de herramientas **Orígenes**.
   Se muestra el cuadro de diálogo **Agregar origen**.
8. Especifique el puerto, modifique cualquier otro parámetro que requiera cambios y haga clic en **Aceptar**.

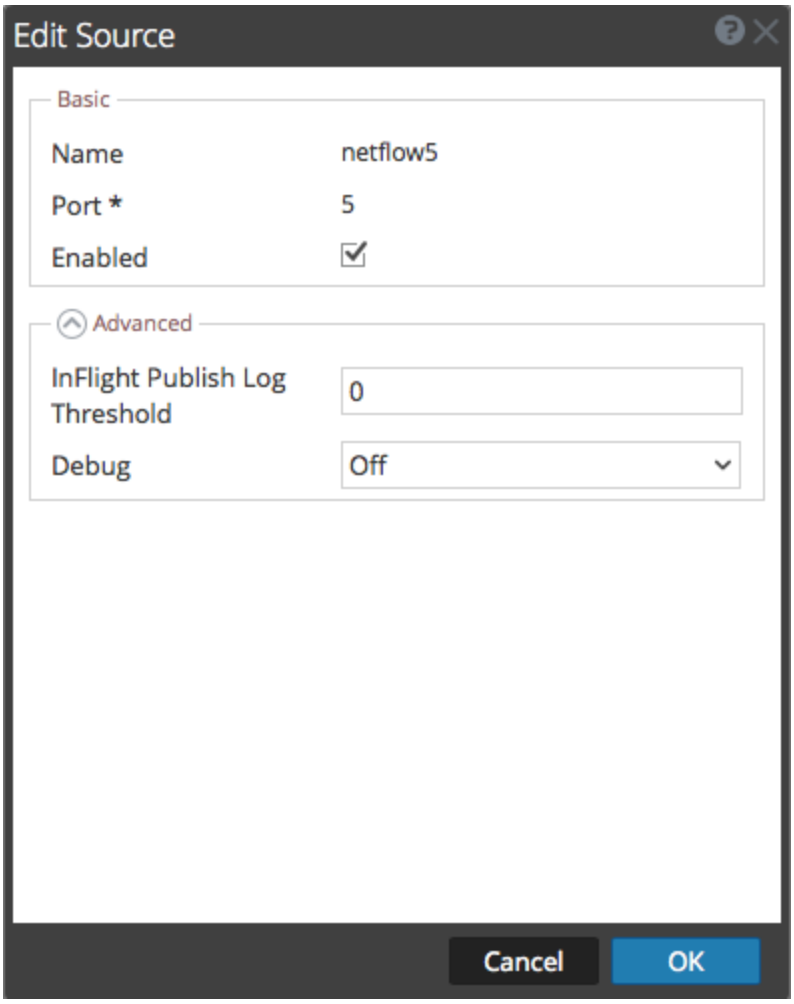
> **Nota:** Security Analytics abre los puertos 2055, 4739, 6343 y 9995 en el firewall de manera predeterminada. Puede abrir otros puertos para Netflow si es necesario.



El nuevo origen de eventos se muestra en la lista.

Modificar un origen de eventos de Netflow

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Netflow/Configurar** en el menú desplegable.
5. Seleccione **netflow** para el tipo de origen de eventos en el panel **Categorías de evento** y haga clic en **Aceptar**.
6. En el panel **Orígenes**, seleccione un origen de eventos y haga clic en .
   Se muestra el cuadro de diálogo **Editar origen**.
7. Modifique los parámetros que necesiten cambios y haga clic en **Aceptar**.



Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado.

Parámetros:

Referencias: Parámetros de configuración de la recopilación de Netflow

Paso 2. Configurar orígenes de eventos de Netflow para enviar eventos a Security Analytics

Descargar y configurar el analizador rsaflow o cef desde Live.

Verifique que haya descargado el analizador rsaflow o cef desde LIVE al Log Decoder y que lo haya habilitado.

Procedimiento

1. En el menú de **Security Analytics**, vaya a **Administration > Servicios**.
2. Seleccione un servicio **Log Decoder** y elija > **Ver** > **Configuración**.

3. En la pestaña **General**, bajo el panel **Configuración de analizadores de servicio**, verifique que la opción **rsaflow** esté seleccionada.

Paso 3. Iniciar el servicio para el protocolo de recopilación de Netflow configurado

En este tema se indica cómo iniciar un servicio de recopilación de NetFlow detenido.

Volver a Procedimientos

Contexto

En este tema se indica cómo iniciar un servicio de recopilación. Consulte el tema **Habilitar el inicio automático de servicios individuales** de la *Guía de configuración de la recopilación de registros* si desea que el servicio se inicie automáticamente.

Procedimiento

Para iniciar un servicio de recopilación de Netflow detenido:

1. En el menú de **Security Analytics**, vaya a **Administration > Servicios**.
2. Seleccione un **Log Collector** y elija  **> Ver > Sistema**.
3. Haga clic en **Recopilación > Netflow > Iniciar**.

Paso 4. Verificar que la recopilación de Netflow esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de Netflow se configuró correctamente.

Volver a Procedimientos

Contexto

Puede verificar que la recopilación de Netflow esté funcionando en Administration > Estado y condición > pestaña Monitoreo de orígenes de eventos.

Procedimiento

Para verificar que la recopilación de Netflow esté funcionando:

1. En el menú de **Security Analytics**, seleccione **Administration > Estado y condición**.
2. Haga clic en la pestaña **Monitoreo de orígenes de eventos**.
3. En la cuadrícula, busque **Log Decoder**, **Origen de eventos** y **Tipo de origen de evento** (es decir, **rsaflow**).
4. Busque actividad en la columna **Conteo** para verificar que la recopilación de Netflow esté aceptando eventos.

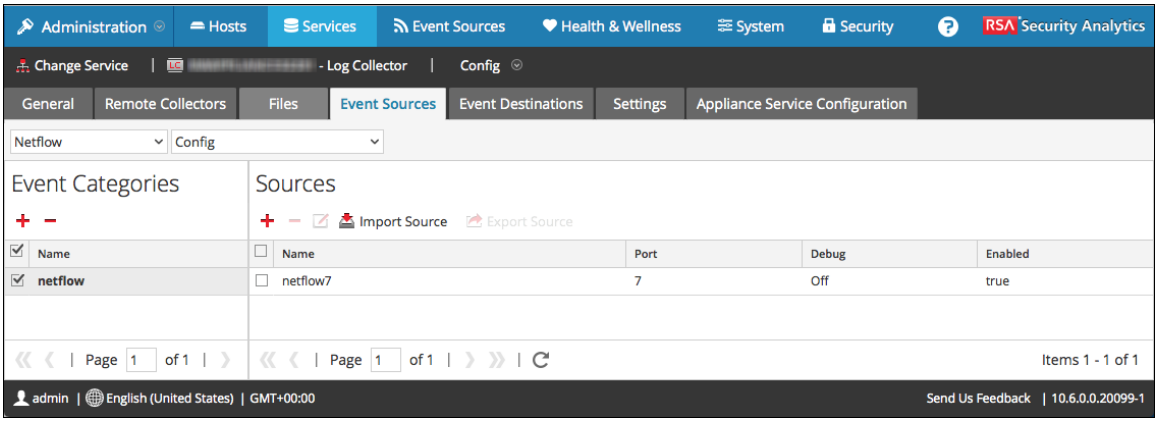
Referencias: Parámetros de configuración de la recopilación de Netflow

En este tema se describe la interfaz del usuario para establecer la configuración de Netflow.

Use esta sección cuando busque descripciones de la interfaz del usuario de recopilación de Netflow y definiciones de las funciones de la interfaz del usuario.

Para acceder a los parámetros de configuración de la recopilación de Netflow:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Netflow/Configurar** en el menú desplegable.



La vista Netflow/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar los tipos de orígenes de eventos correspondientes.

Característica	Descripción
	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.
	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de tipos de orígenes de eventos compatibles.

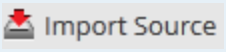
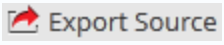
Característica	Descripción
	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

Panel Orígenes

Use este panel para revisar, agregar, modificar y eliminar los parámetros de origen de eventos para el tipo de origen de eventos que seleccionó en el panel Categorías de evento.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Opción	Descripción
	Abre el cuadro de diálogo Agregar origen, en el cual se agrega un directorio de archivos para el tipo de origen de eventos que seleccionó en el panel Categorías de evento.
	Elimina los directorios de archivo seleccionados.
	Abre el cuadro de diálogo Editar origen en el cual se modifican los parámetros de configuración del directorio de archivos seleccionado. Cuando selecciona varios orígenes de eventos, se abre el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los directorios de archivos seleccionados. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar parámetros del directorio de archivos de origen de eventos masivamente desde un archivo con valores separados por coma (CSV). Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo **.csv** que contiene los parámetros de los directorios de archivos seleccionados. Consulte la **Guía de configuración de la recopilación de registros** para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.

Cuadro de diálogo Agregar/Modificar origen

En este cuadro de diálogo, se agrega o modifica un directorio de archivos del origen de eventos seleccionado.

Característica	Descripción
Parámetros del origen Netflow	Muestra los parámetros de origen de eventos de Netflow completados con los valores predeterminados. Ingrese o modifique los valores apropiados.

Característica	Descripción
Cancelar	Cierra el cuadro de diálogo sin agregar un directorio de archivo ni guardar los valores de los parámetros del directorio de archivos seleccionado.
OK	En el cuadro de diálogo Agregar origen, agrega el directorio de archivos y sus parámetros. En el cuadro de diálogo Editar origen, aplica los cambios en los valores de los parámetros del directorio de archivos seleccionado.

Parámetros del origen Netflow

En la siguiente tabla se proporcionan descripciones de los parámetros del origen.

Nombre	Descripción
	Básico
Puerto	Especifique el número de puerto configurado para el origen de eventos de Netflow. De forma predeterminada, Security Analytics abre los puertos 2055, 4739, 6343 y 9995 para Netflow. Puede abrir otros puertos para Netflow si es necesario.
Activado	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
	Avanzado

Nombre	Descripción
Umbral de registro de publicación en trans-ferencia	Establece un umbral que, cuando se alcanza, Seguridad Analytics genera un mensaje de registro para ayudarle a resolver problemas de flujo de eventos. El umbral es el tamaño de los mensajes de eventos de Netflow que fluyen actualmente desde el origen de eventos a Security Analytics. Los valores válidos son: • **0** (valor predeterminado): deshabilita el mensaje de registro. • **100-100000000**: genera un mensaje de registro cuando este Log Collector ha procesado la cantidad especificada de eventos de Netflow. Por ejemplo, si establece este valor en 100, Security Analytics genera un mensaje de registro cuando se han procesado 100 eventos de Netflow de la versión de Netflow específica (v5 o v9).
Depurar	**Precaución:** Habilite la depuración (defina este parámetro en Activado o Detallado) solamente si hay un problema en un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa/desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar).
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega los parámetros del origen de eventos.

Tareas:

Paso 1. Configurar orígenes de eventos de Netflow en Security Analytics

Paso 2. Configurar orígenes de eventos de Netflow para enviar eventos a Security Analytics

Solucionar problemas de la recopilación de Netflow

En este tema se destacan los posibles problemas que puede encontrar con la recopilación de Netflow y proporciona soluciones sugeridas a estos problemas.

Solucionar problemas de la recopilación de Netflow

En general, se reciben mensajes de registro más confiables cuando se desactiva SSL.

Mensaje de registro/ Problema	Log Collector no recibe tráfico de Netflow.
Causa posible	Se configuró el puerto equivocado.
Solución	Asegúrese de haber configurado el puerto de firewall correcto (es decir, 2055, 4739, 6343 o 9995).
Mensaje de registro/ Problema	El registro de problemas de Log Collector le envía un mensaje para indicarle que hay un encabezado o número de versión incompatible o no coincidente.
Causa posible	La información de evento de Netflow v10 se envió al Log Collector.
Solución	No haga caso: Netflow v10 no es compatible con Security Analytics 10.4. Solo recopilación de Netflow acepta eventos de Netflow v5 y Netflow v9.

Guía de configuración de la recopilación de ODBC

En esta guía se indica cómo configurar el protocolo de recopilación de ODBC. Este protocolo recopila eventos de orígenes de eventos que almacenan datos de auditoría en una base de datos con el uso de la interfaz de software Open Database Connectivity (ODBC).

Debe implementar Log Collection antes de poder configurar el protocolo de recopilación de ODBC.

Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

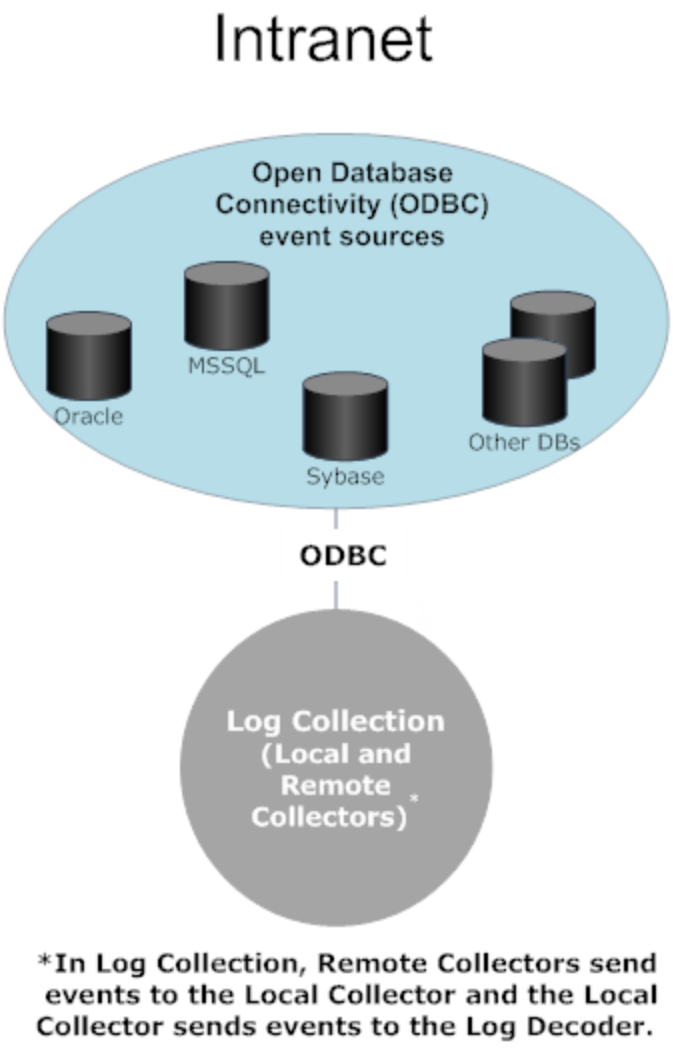
Conceptos básicos

Descripción general

En esta guía se explica cómo configurar el protocolo de recopilación de ODBC que recopila eventos de orígenes de eventos que almacenan datos de auditoría en una base de datos mediante la interfaz de software de Open Database Connectivity (ODBC).

Escenario de implementación

En la siguiente figura se ilustra cómo implementar el protocolo de recopilación de ODBC en Security Analytics.



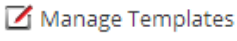
Procedimientos

Configurar el protocolo de recopilación de ODBC en Security Analytics

Debe configurar el Log Collector para usar la recopilación de ODBC para un origen de eventos en la pestaña Origen de evento de la vista de parámetros de Log Collector. En el siguiente procedimiento se explica el flujo de trabajo básico para configurar un origen de eventos para la recopilación de ODBC en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de ODBC en Security Analytics para obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de ODBC.
- Parámetros de configuración del origen de eventos de ODBC para obtener una descripción detallada de cada parámetro del protocolo de recopilación de ODBC.

Para configurar el Log Collector de modo que use el protocolo de recopilación de ODBC:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio de **recopilación de registros**.
3. Seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de la recopilación de registros.
4. En la pestaña **Orígenes de evento**, seleccione **ODBC** como el protocolo de recopilación y elija **Configurar**.
5. Haga clic en  y seleccione una categoría de origen de eventos (por ejemplo, **mssql**).
6. La categoría de origen de eventos es parte del contenido que descargó de LIVE.
7. Seleccione **DSN** en la lista desplegable y haga clic en  .
8. Seleccione una plantilla de par de valores de DSN, ingrese un nombre de DSN y agregue o elimine pares de valores, si es necesario.
   Si es necesario, haga clic en  para agregar o eliminar plantillas de DSN.
9. Seleccione **Configurar**.
10. Seleccione la categoría **ODBC** y haga clic en  en el panel **Orígenes**.
11. Especifique los parámetros básicos requeridos para el origen de eventos de ODBC.
12. Haga clic en  y especifique parámetros adicionales que mejoran la manera en que el protocolo de ODBC maneja la recopilación de eventos para el origen de eventos.

Configurar orígenes de eventos de modo que usen el protocolo de recopilación de ODBC

Debe configurar cada origen de eventos que usa el protocolo de recopilación de ODBC para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de ODBC para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de ODBC, con una lista de verificación que contiene cada paso de configuración.

Los pasos para el protocolo de recopilación de ODBC deben realizarse en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de configuración de la recopilación de ODBC

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de ODBC en Security Analytics.	
2	Configurar orígenes de eventos de ODBC para enviar eventos a Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de ODBC configurado.	
4	Verificar que la recopilación de ODBC esté funcionando.	

Paso 1. Configurar orígenes de eventos de ODBC en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de ODBC para el Log Collector.

Después de realizar este procedimiento, habrá...

- Configurado un origen de eventos de ODBC.
- Modificado un origen de eventos de ODBC

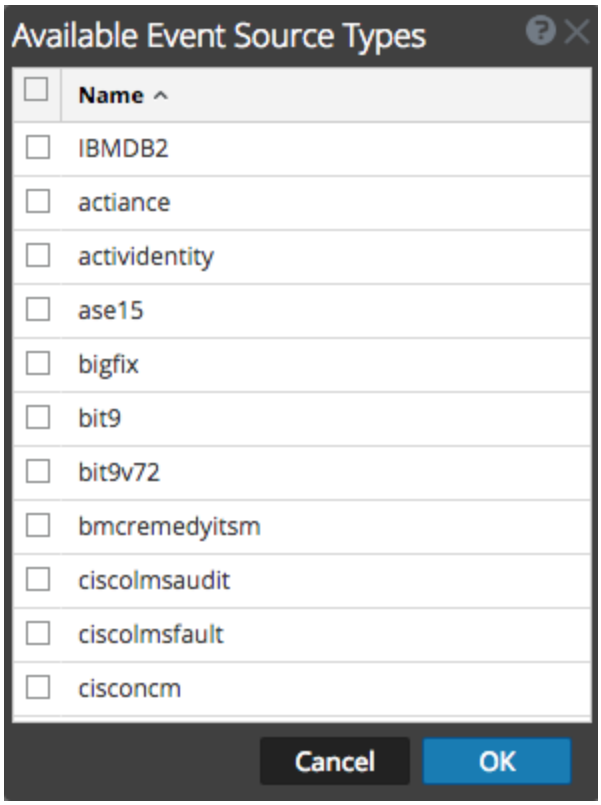
Volver a Procedimientos

Procedimientos

Configurar un origen de eventos de ODBC

1. Asegúrese de haber configurado la combinación de pares de DSN/valor (consulte Paso 1. Configurar orígenes de eventos de ODBC en Security Analytics) para las categorías de eventos de ODBC que desea configurar.
2. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
3. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
4. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
5. En la pestaña **Orígenes de evento** de Log Collector, seleccione **ODBC/Configurar** en el menú desplegable. En el **panel Categorías de evento** se muestran los orígenes de eventos de ODBC que están configurados, si los hay.
6. Haga clic en  .

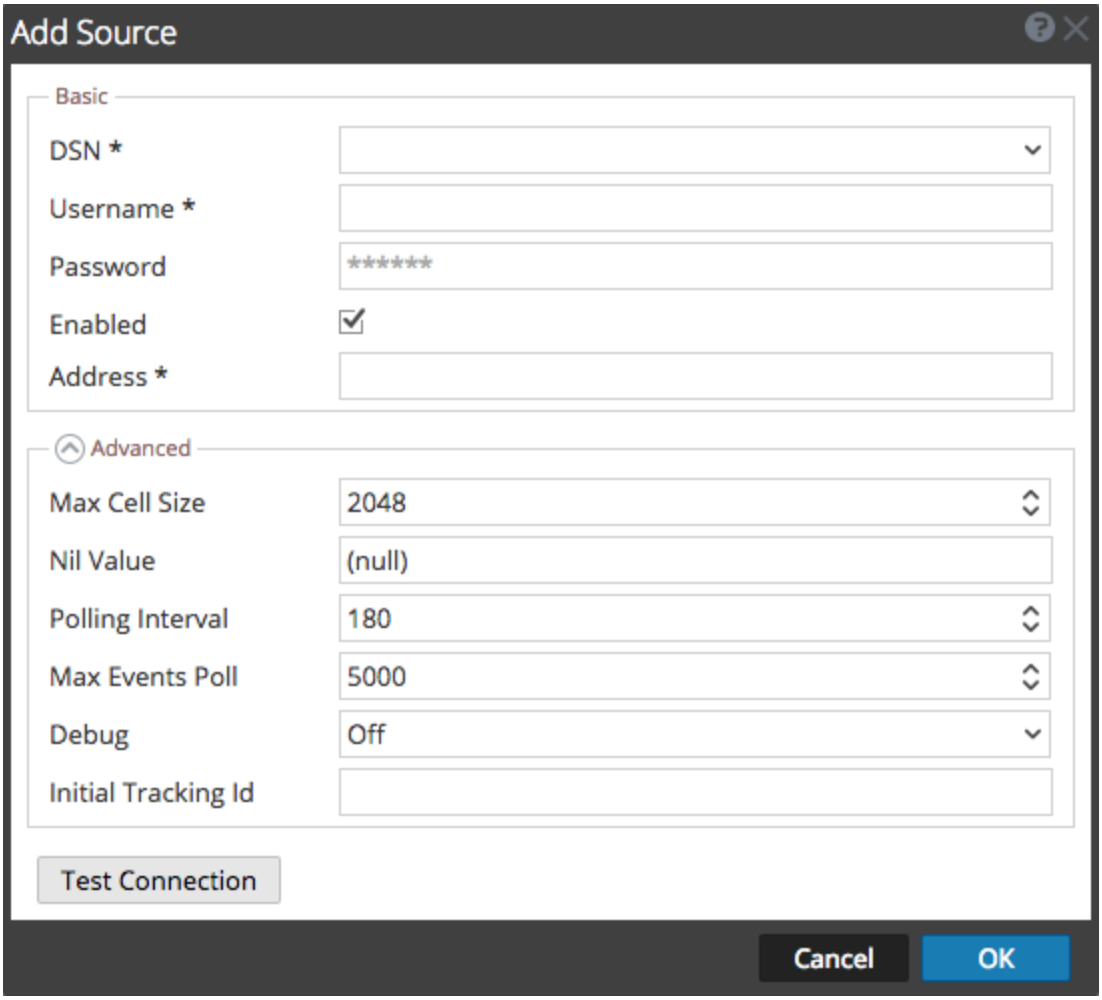
   Se muestra el cuadro de diálogo **Tipos de origen de evento disponibles**.



7. Seleccione un tipo de origen de eventos (por ejemplo, **mssql**) y haga clic en **Aceptar**.
   El tipo de origen de eventos de ODBC recién agregado se muestra en el panel **Categorías de evento**.

8. Seleccione el nuevo tipo en el **panel Categorías de evento** y haga clic en + en la barra de herramientas del panel de la **lista de DSN**.
   Se muestra el cuadro de diálogo **Agregar DSN**.

9. Seleccione un DSN en la lista desplegable, especifique o modifique los otros parámetros según sea necesario y haga clic en **Aceptar**.
   Los nombres de DSN se definieron en la lista desplegable en Configurar nombres de orígenes de datos que identifica las combinaciones de pares de DSN/valor.



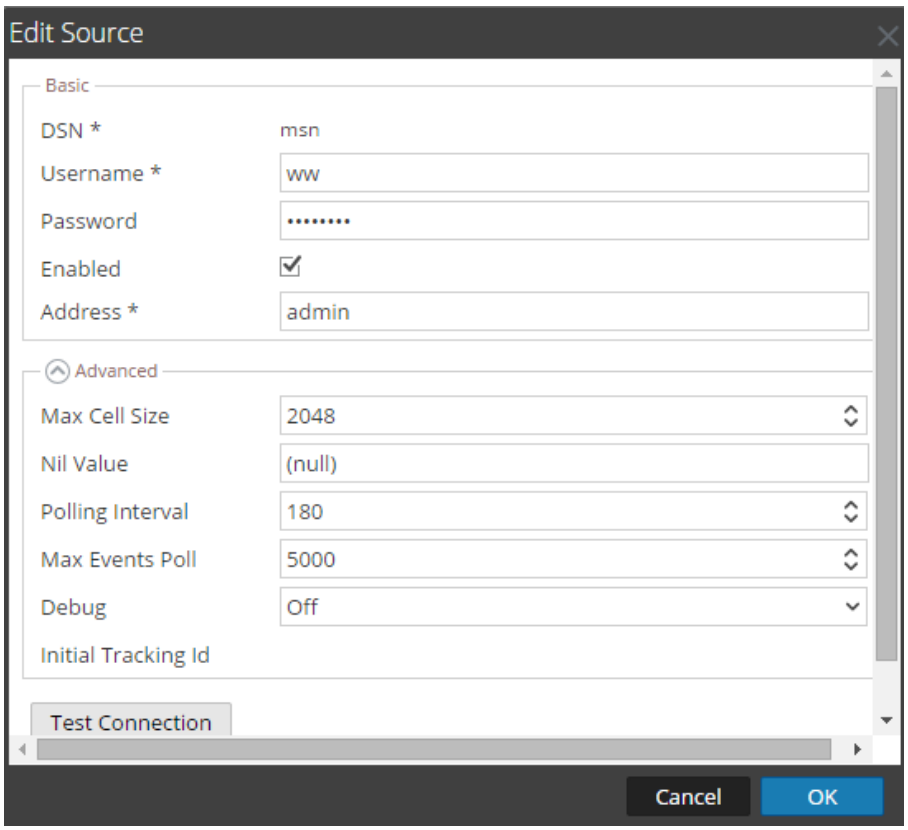
10. Haga clic en **Probar conexión**.
    El resultado de la prueba se muestra en el cuadro de diálogo. Si el resultado de la prueba no es satisfactorio, edite la información de DSN y vuelva a intentarlo.
    Log Collector tarda aproximadamente 60 segundos en devolver los resultados de la prueba.

Si se excede el límite de tiempo, se agota el tiempo de espera de la prueba y el servidor de Security Analytics muestra un mensaje de error.

11. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**.
    El DSN definido recientemente se muestra en el panel **Orígenes**.

Modificar un origen de eventos de ODBC

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **ODBC/Configurar** en el menú desplegable.
5. En el panel **Orígenes**, seleccione un origen de eventos y haga clic en  .
   Se muestra el cuadro de diálogo **Editar DSN**



6. Modifique los parámetros que requieren cambios.
7. Haga clic en **Probar conexión**.
   El resultado de la prueba se muestra en el cuadro de diálogo. Si el resultado de la prueba no

es satisfactorio, edite la información de DSN y vuelva a intentarlo.
Log Collector tarda aproximadamente 60 segundos en devolver los resultados de la prueba. Si se excede el límite de tiempo, se agota el tiempo de espera de la prueba y Security Analytics muestra un mensaje de error.

8. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**.
Security Analytics aplica los cambios de parámetros al DSN seleccionado.

Parámetros

Referencias: Parámetros de configuración de la recopilación de ODBC

Parámetros de configuración del origen de eventos de DSN de ODBC

Configurar nombres de orígenes de datos (DSN)

Descripción general

En este tema, se explica cómo crear y mantener DSN para la recopilación de ODBC.

Contexto

Los orígenes de eventos de Open Database Connectivity (ODBC) requieren los Nombres de origen de datos (DSN); de modo que debe definir DSN con sus pares de valores asociados para la configuración de origen de eventos de ODBC.

Después de realizar este procedimiento, habrá…

- Agregado una plantilla DSN.
- Agregado un DSN.
- Editado un DSN.

Volver a Procedimientos

Procedimientos

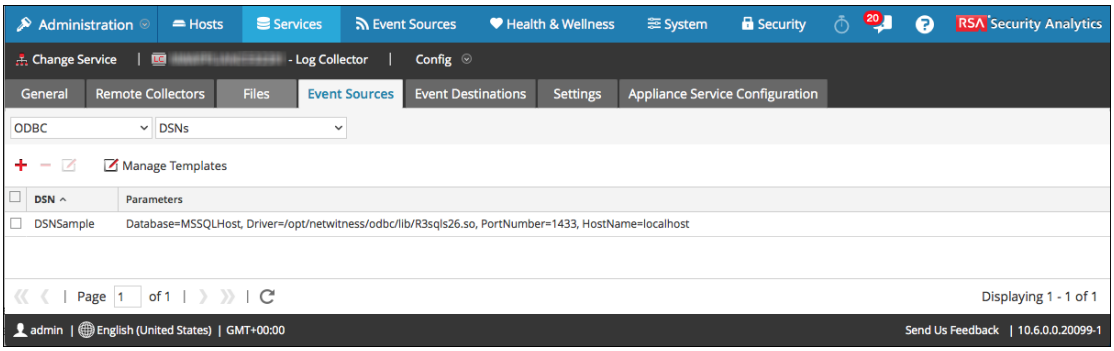
Agregar una plantilla DSN

Puede agregar plantillas DSN para usarlas la próxima vez que agregue un DSN.

Para agregar una plantilla DSN:

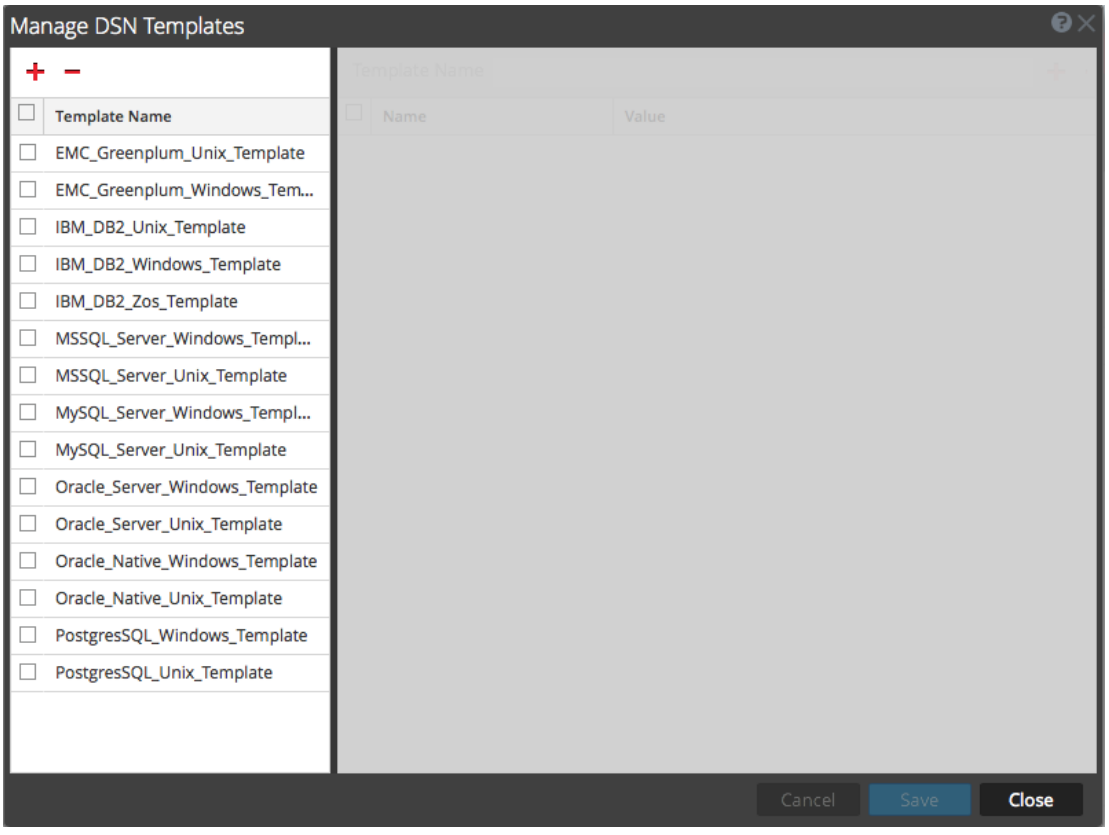
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.

4. En la pestaña **Orígenes de evento de Log Collector**, seleccione **ODBC/DSN** en el menú desplegable.
   El panel **DSN** se muestra con los DSN que se agregaron, si los hay.



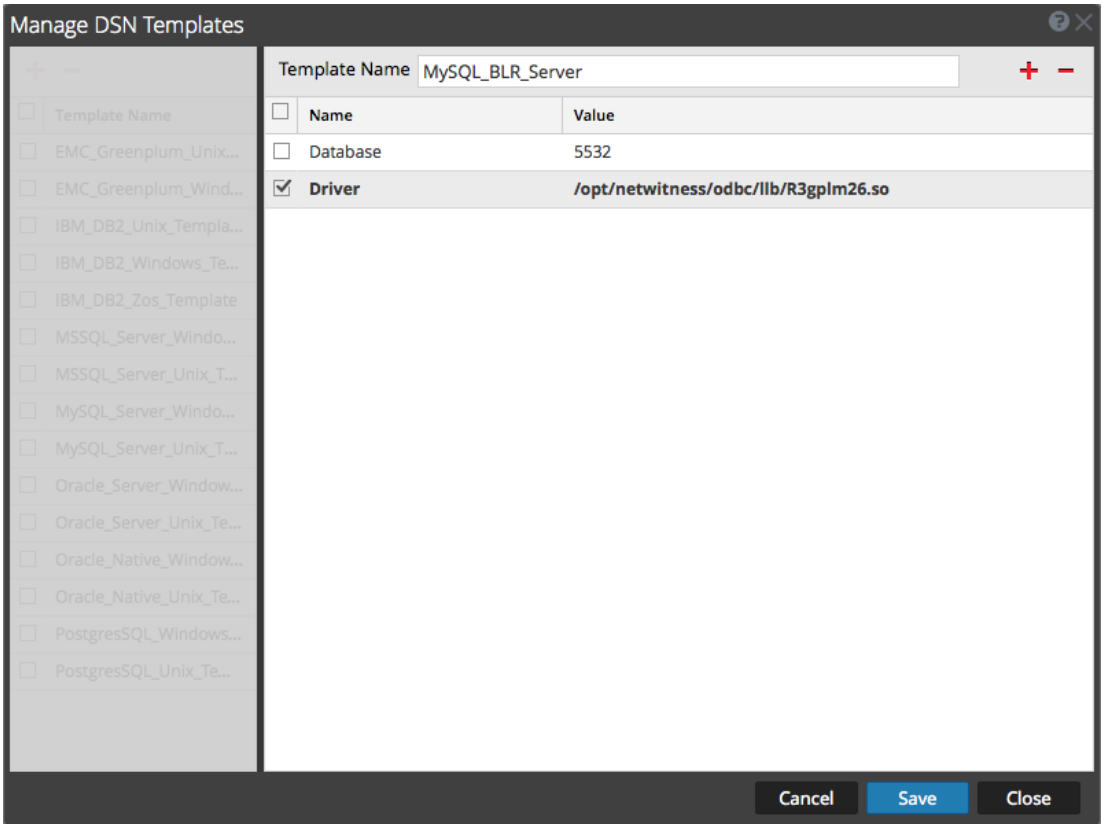
5. Haga clic en 

   Se muestra el cuadro de diálogo **Administrar plantillas DSN**.



Nota: RSA proporciona plantillas predeterminadas en el panel del lado izquierdo que puede usar mientras agrega un nuevo DSN.

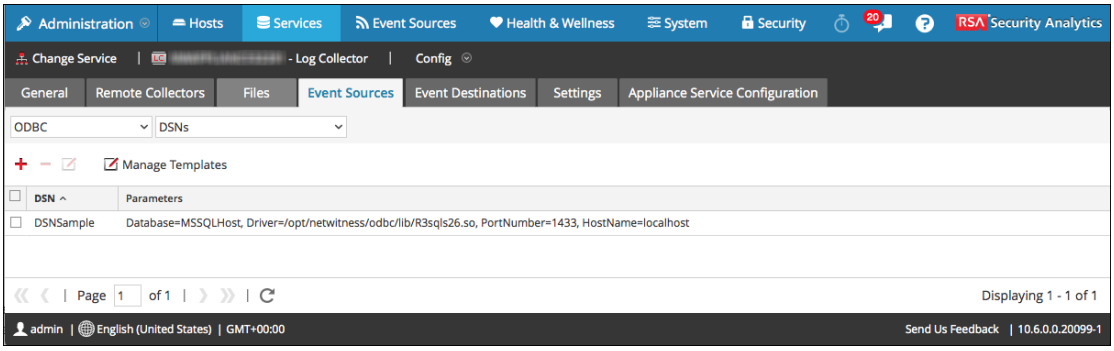
6. Haga clic en +.
   El panel derecho se activa.
7. Especifique un nombre de plantilla y haga clic en +, en el panel derecho para agregar parámetros.
8. Especifique los parámetros. Haga clic en **Guardar**.



La nueva plantilla DSN se agrega en la lista **Administrar plantillas DSN**.

Agregar un DSN

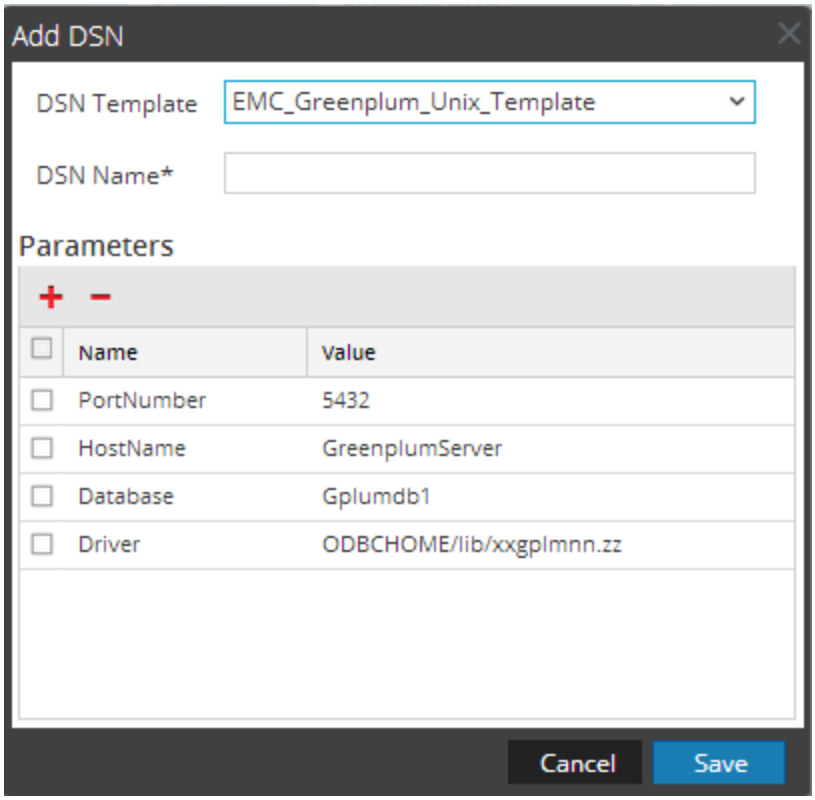
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento de Log Collector**, seleccione **ODBC/DSN** en los menús desplegables.
   El panel **DSN** se muestra con los DSN que se agregaron, si los hay.



5. Haga clic en  .

- Mediante la plantilla DSN

a. Seleccione una plantilla DSN en la lista desplegable del campo **Plantilla DSN**.
Se muestran los parámetros predeterminados.



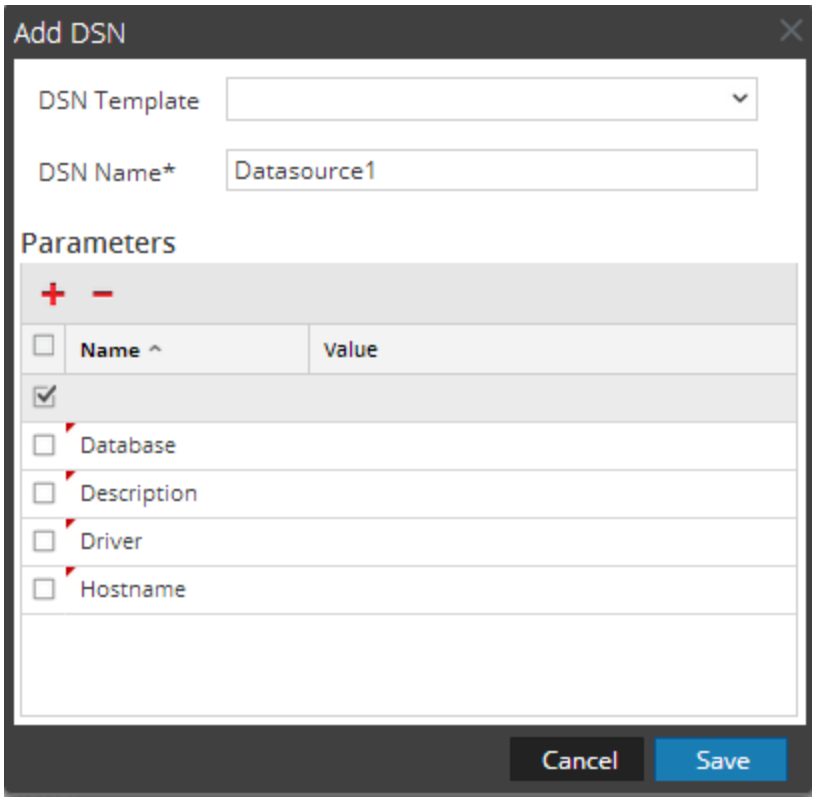
b. Especifique un nombre en el campo **Nombre de DSN**.

c. Agregue, elimine o edite los parámetros predeterminados y haga clic en **Guardar**.
El DSN recién agregado y sus pares de nombre-valor se muestran en el panel DSN.

- Incorporación manual de parámetros

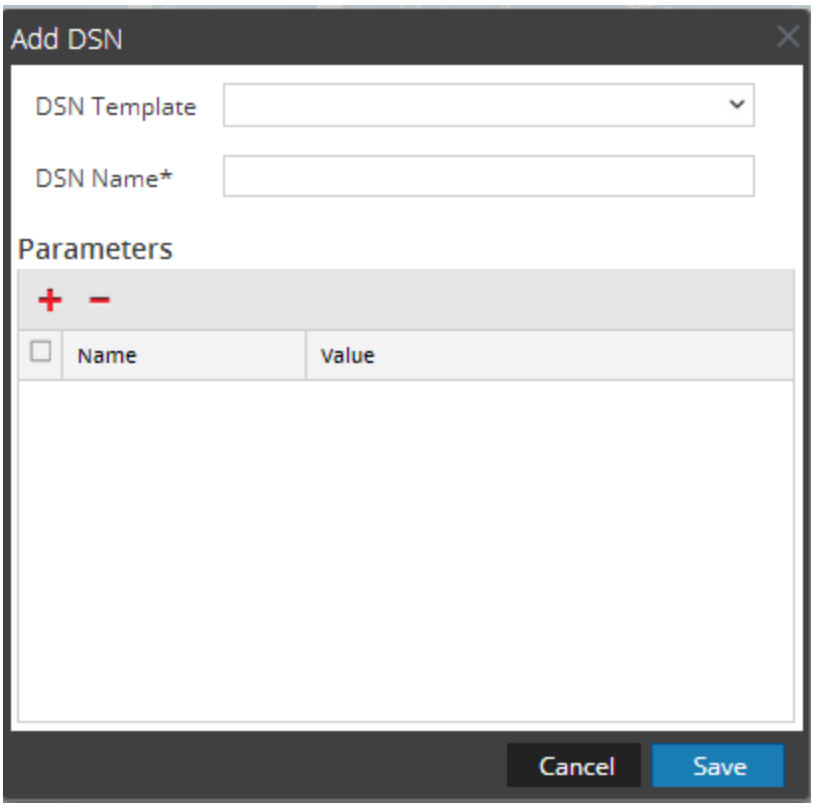
  a. Especifique un nombre en el campo **Nombre de DSN**.

  b. Haga clic en + para agregar parámetros.



  c. Especifique los pares de valores en el cuadro de diálogo y haga clic en **Guardar**.
  El DSN recién agregado y sus pares de nombre-valor se muestran en el panel **DSN**.

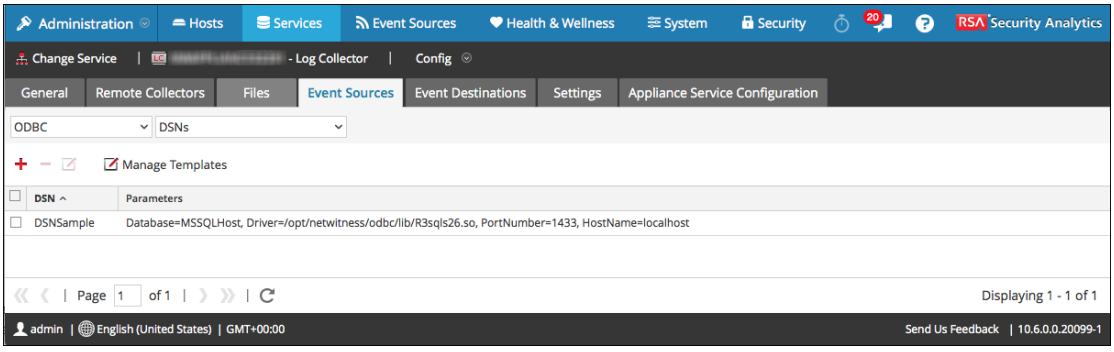
6. Se muestra el cuadro de diálogo **Agregar DSN**.



Puede agregar un DSN de dos maneras:

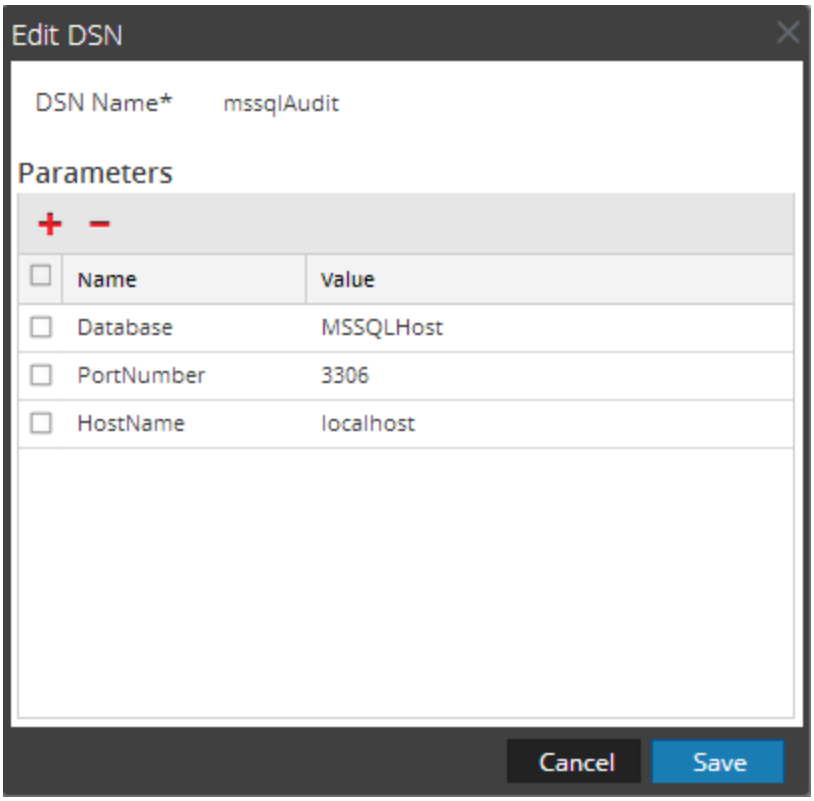
Editar un DSN

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento de Log Collector**, seleccione **ODBC/DSN** en los menús desplegables.
   El panel **DSN** se muestra con los DSN que se agregaron, si los hay.



5. Seleccione un DSN.
6. Haga clic en  .

   Se muestra el cuadro de diálogo **Editar DSN**.
7. Modifique los parámetros que necesiten cambios y haga clic en **Guardar**.



Los pares de nombre-valor modificados se muestran en el panel **DSN**.

Parámetros

Parámetros de configuración del origen de eventos de DSN de ODBC

Parámetros de configuración del origen de eventos de ODBC

Crear un archivo typespec de contenido personalizado para la recopilación de ODBC

En este tema se indica cómo crear un archivo typespec personalizado para Log Collector. En el tema se incluye:

- Procedimiento Crear un archivo typespec personalizado
- Sintaxis de typespec para la recopilación de ODBC
- Ejemplo de archivo typespec para la recopilación de ODBC

Volver a Procedimientos

Procedimiento

Para crear un archivo typespec personalizado:

1. Copie un archivo typespec existente y guárdelo en el mismo directorio.

   Por ejemplo, recopilación de ODBC, copie el archivo **actividentity.xml** desde **/etc/netwitness/ng/logcollection/content/collection/odbc** y guárdelo con un nuevo nombre en el mismo directorio.

2. Modifique el archivo de acuerdo con los requisitos.
3. Reinicie Log Collector.

   No podrá ver el nuevo tipo de dispositivo en Security Analytics hasta que reinicie Log Collector.

Sintaxis de typespec para la recopilación de ODBC

Sintaxis	Descripción
`<?xml version="1.0" encoding="UTF-8"?>`	No modifique esta línea.
`<typespec>`	No modifique esta línea.
`<name>event-source</name>`	Nombre del origen de eventos. Reemplace event-source por el nombre del origen de eventos de ODBC (por ejemplo, actividentity). Security Analytics muestra este nombre en el panel **Orígenes** de la pestaña **Ver > Configuración > Orígenes de evento**.
`<type>odbc</type>`	Tipo de origen de eventos (archivos, ODBC, Windows, etc.). No modifique esta línea.

Sintaxis	Descripción
`<prettyName>event-source -name</-prettyName>`	Nombre definido por el usuario para el origen de eventos. Puede usar el mismo valor que name (por ejemplo, actividentity) o usar un nombre más descriptivo.
`<version>1.0</version>`	Versión de este archivo typespec. El valor predeterminado es 1.0.
`<author>author-name</author>`	Persona que creó el archivo typespec. Reemplace author-name por su nombre.
`<description>formal-description</description>`	Descripción formal del origen de eventos. Reemplace formal-description por su descripción del origen de eventos.
`<device>`	No modifique esta línea.
`<name>device</name>`	Reemplace device por el nombre de la información del dispositivo (por ejemplo, **ActivIdentity ActivCard AAA Server**).
`<maxVersion>n</maxVersion`	Reemplace n por el número de versión del dispositivo (por ejemplo, **6.4.1**).
`<description>description</description>`	Descripción del dispositivo. Reemplace description por su descripción del dispositivo.
`</device>`	No modifique esta línea.

Sintaxis	Descripción
`<configuration>` `</configuration>`	La recopilación de ODBC no utiliza esto.
`<collection>`	No modifique esta línea.
`<odbc>`	La sintaxis en `<odbc>` se usa para la recopilación y el procesamiento de eventos. Puede proporcionar múltiples consultas para el mismo tipo de origen de eventos si agrega etiquetas `<query>`.
`<query>`	No modifique esta línea.
`<tag>prefix</tag>`	Reemplace prefix por la etiqueta de prefijo que desea agregar a los eventos durante la transformación (por ejemplo, ActivIdentity).
`<outputDelimiter>x</outputDelimiter>`	Especifique el delimitador que usará para separar los campos durante la transformación. Especifique cualquiera de los siguientes valores para x: || (barra vertical) ^ (intercalación) , (coma) : (dos puntos) 0x20 (para un espacio)
`<interval>n</interval>`	Especifique la cantidad de segundos entre eventos para **n**. El valor predeterminado es **60**.

Sintaxis	Descripción
`<dataQuery>SQL-syntax</dataQuery>`	Especifique la consulta para buscar datos desde la base de datos de origen de eventos de ODBC para SQL-syntax. Por ejemplo: `SELECT accepedrejected, servername, serveripa, sdate, millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG WHERE sdate > '%TRACKING%' ORDER BY sdate`
`<maxTrackingQuery>SQL-syntax</maxTrackingQuery>`	Especifique la consulta para buscar nuevos datos para SQL-syntax. Por ejemplo: `SELECT MAX (sdate) FROM A_AHLOG`
`<addressColumn>source-address-col-value </addressColumn>`	Reemplace **source-address-col-value** por el valor de la columna de la base de datos de la dirección de origen para cada evento (por ejemplo, **serverIPA**).
`<trackingColumn>col-value</-trackingColumn>`	Reemplace **col-value** por el valor de la columna de rastreo cuando el colector de ODBC extraiga un nuevo conjunto de eventos.
`</query>`	No modifique esta línea.

Sintaxis	Descripción
`</odbc>`	No modifique esta línea.
`</collection>`	No modifique esta línea.
`</typespec>`	No modifique esta línea.

Ejemplo de archivo typespec para la recopilación de ODBC

```
-# Sample actividentity typespec , odbc collection <?xml version="1.0"
encoding="UTF-8"?>
<typespec>
    <name>actividentity</name>
    <type>odbc</type>
    <prettyName>ACTIVIDENTITY</prettyName>
    <version>1.0</version>
    <author>Administrator</author>
    <description>Collects events from ActivIdentity ActivCard AAA
Server</description>
    <device>
        <name>ActivIdentity ActivCard AAA Server</name>
        <maxVersion>6.4.1</maxVersion>
        <description></description>
    </device>
    <configuration>
    </configuration>
    <collection>
        <odbc>
            <query>
                <tag>ActivIdentity</tag>
                <outputDelimiter>||</outputDelimiter>   <interval>60</interval>
                <dataQuery>
                    SELECT acceptedrejected, servername, serveripa, sdate,
millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG
WHERE sdate > '%TRACKING%' ORDER BY sdate
                </dataQuery>
                <maxTrackingQuery>
                    SELECT MAX(sdate) FROM A_AHLOG
                </maxTrackingQuery>
                <addressColumn>serverIPA</addressColumn>
                <trackingColumn>sdate</trackingColumn>
            </query>
            <query>
                <tag>ActivIdentity</tag>
                <outputDelimiter>||</outputDelimiter>
                <interval>60</interval>
                <dataQuery>                    SELECT object, suid, sdate,
objname, operation, opdetail, param1, param2, param3, param4 FROM A_AUDIT WHERE
sdate > '%TRACKING%' ORDER BY sdate
                </dataQuery>
                <maxTrackingQuery>
                    SELECT MAX(sdate) FROM A_AUDIT
                </maxTrackingQuery>
                <addressColumn></addressColumn>
                <trackingColumn>sdate</trackingColumn>
            </query>
        </odbc>
    </collection>
</typespec>
```

Paso 2. Configurar orígenes de eventos de ODBC para enviar eventos a Security Analytics

En este tema se indica dónde encontrar los orígenes de eventos que son compatibles actualmente con la recopilación de ODBC y las instrucciones de configuración disponibles para cada origen de eventos.

Es posible que necesite ver los orígenes de eventos que son compatibles actualmente con la recopilación de ODBC, así como las instrucciones de configuración disponibles para cada uno de ellos. En la lista de orígenes de eventos compatibles se proporciona información sobre los orígenes de eventos que están disponibles actualmente para la recopilación de ODBC.

Procedimiento

Volver a Procedimientos

La lista de orígenes de eventos compatibles de RSA es una lista alfabética de todos los orígenes de eventos que son compatibles actualmente con Security Analytics, en la cual se identifican los orígenes de eventos que puede usar con la recopilación de ODBC. Para verificar que el origen de eventos sea compatible:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un Log Decoder y haga clic en  **> Ver > Configuración**.
   La vista **Configuración de servicios** se muestra con la pestaña **General** abierta.
3. En la pestaña **General**, bajo el panel **Configuración de analizadores de servicio**, busque el nombre del origen de eventos.
4. Verifique que sea compatible con el protocolo de recopilación de ODBC. Haga clic en  en la lista de **orígenes de eventos compatibles** para mostrar las instrucciones de configuración del origen de eventos.
5. Verifique que haya descargado el analizador de origen de eventos correcto (por ejemplo, **mssql**) desde Live a Log Decoder y que lo haya habilitado.

Ejemplo de instrucciones de configuración

La siguiente ilustración se toma de las instrucciones de configuración de ODBC Security Suite, IPS-1.

RSA Security Analytics

Event Source Log Configuration Guide

Microsoft SQL Server

Last Modified: Monday, June 09, 2014

Event Source Product Information:

Vendor: Microsoft
Event Source: SQL Server
Versions: 2000, 2005, 2008, 2012, and MS SQL Express

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: mssql
Collection Method: ODBC, File, and Windows event logs
Event Source Class.Subclass: Storage.Database

Paso 3. Iniciar el servicio para el protocolo de recopilación de ODBC configurado

En este tema se indica cómo iniciar un servicio de recopilación de ODBC detenido.

Si un servicio de recopilación de ODBC se detiene, debe iniciarlo nuevamente para que funcione. También puede habilitar el inicio automático de servicios individuales si desea que el servicio se inicie automáticamente.

Procedimiento

Volver a Procedimientos

En el siguiente procedimiento se explica cómo iniciar un servicio de recopilación. Consulte el tema **Habilitar el inicio automático de servicios individuales** de la *Guía de configuración de la recopilación de registros* si desea que el servicio se inicie automáticamente.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un Log Collector y elija  **> Ver > Sistema**.

   Se muestra la vista Sistema de servicios.

3. Seleccione **Recopilación > ODBC > Iniciar**.

Paso 4. Verificar que la recopilación de ODBC esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de ODBC se configuró correctamente

Debe verificar que la recopilación de ODBC esté configurada correctamente; de lo contrario, no funcionará.

Procedimiento

Volver a Procedimientos

En el siguiente procedimiento se explica cómo puede verificar que la recopilación de ODBC esté funcionando desde **Administration > Estado y condición > pestaña Monitoreo de orígenes de eventos**.

1. En el menú de **Security Analytics**, seleccione **Administration > Estado y condición.**
   La vista **Estado y condición** se muestra con la pestaña **Monitoreo** abierta.
2. En la pestaña **Monitoreo de orígenes de eventos**, busque un tipo de origen de eventos de ODBC (por ejemplo, **msql**) en la columna **Tipo de origen de evento**.
3. Busque actividad en la columna **Conteo** para verificar que la recopilación de ODBC esté aceptando eventos.

Referencias: Parámetros de configuración de la recopilación de ODBC

Este tema describe los parámetros de configuración del origen de eventos de ODBC.

Los parámetros del origen de eventos de ODBC tienen dos partes y parámetros de vista, ODBC y DSN por separado.

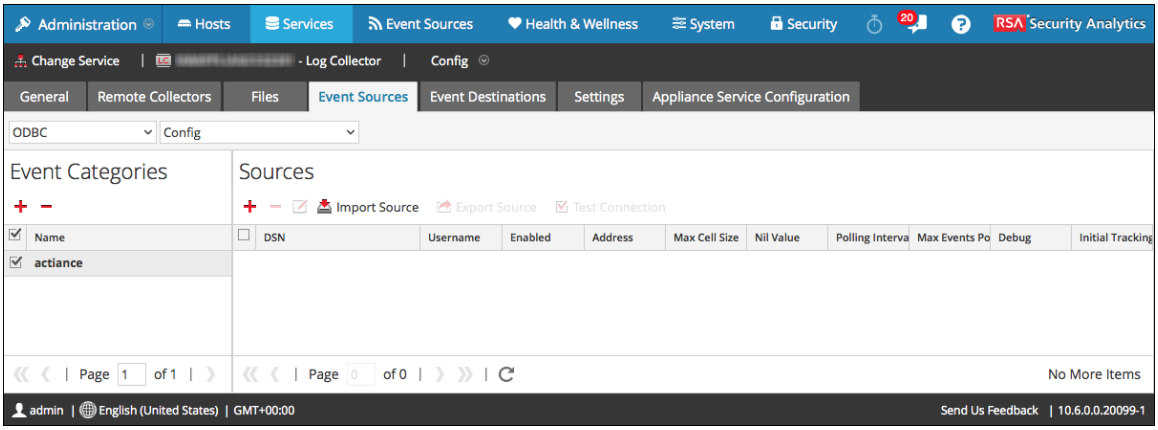
Parámetros de configuración del origen de eventos de ODBC

Este tema describe los parámetros de configuración del origen de eventos de ODBC.

Para acceder a los parámetros de configuración del origen de eventos de ODBC:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.

3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General** de Log Collector abierta.
4. En la pestaña **Orígenes de evento** de Log Collector, seleccione **ODBC/Configurar** en el menú desplegable.



Características

La vista ODBC/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

El panel Categorías de evento proporciona una manera de agregar o eliminar tipos de orígenes de eventos.

Característica	Descripción
+	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
−	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.
☐	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

En este cuadro de diálogo, puede seleccionar el tipo de origen de eventos para el cual desea definir parámetros.

Este cuadro de diálogo contiene la lista de tipos de orígenes de eventos descargados de la lista de tipos de orígenes de eventos del archivo Especificación de tipo de ODBC genérico (GOTS). Si no ve ningún tipo de origen de eventos en esta lista, no cargó el contenido disponible con la actualización de Log Collector para esta versión.

Característica	Descripción
	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

Panel Orígenes

Use el panel Orígenes para revisar, agregar, modificar y eliminar parámetros de Nombre de origen de datos (DSN).

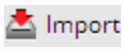
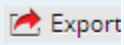
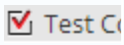
Un DSN de ODBC le indica al Log Collector cómo comunicarse con el terminal de ODBC. Cuando configura un nombre de origen de datos con información tal como qué controlador de ODBC debe usar o el nombre de host y el puerto del terminal de ODBC, hace referencia al DSN de ODBC.

Una DSN ODBC es una secuencia de pares de valor de nombre. Para obtener información sobre los nombres válidos de un tipo de origen de datos de ODBC determinado, como Sybase, Microsoft SQL Server u Oracle, descargue la *Guía del usuario de DataDirect Connect Series for ODBC* en la biblioteca de Progress DataDirect Documentation.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Opción	Descripción
	Abre el cuadro de diálogo Agregar DSN, en el cual se agrega un origen de eventos para el tipo de origen de eventos que seleccionó en el panel Categorías de evento.
	Elimina los orígenes de eventos seleccionados.

	Abre el cuadro de diálogo Editar DSN, en el cual se modifican los parámetros de configuración del origen de eventos seleccionado. Cuando selecciona varios orígenes de eventos, esta opción abre el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los directorios de archivos seleccionados. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar parámetros de DSN masivamente desde un archivo con valores separados por coma (CSV). El cuadro de diálogo Opción Adición en masa tiene las siguientes dos opciones. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo **.csv** que contiene los parámetros de los DSN seleccionados. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Valida los parámetros de configuración de la base de datos de ODBC seleccionada. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo probar conexiones de orígenes de eventos en masa.

Cuadro de diálogo Agregar/Editar DSN

En este cuadro de diálogo, se agrega o modifica un origen de eventos del origen de eventos seleccionado.

Nombre	Descripción

Básico	
DSN*	El nombre del origen de datos (DSN) que define la base de datos desde la cual se recopilan eventos. Seleccione un DSN existente en la lista desplegable. Los valores de esta lista se mantienen en los Parámetros de configuración del origen de eventos de DSN de ODBC.
Nombre de usuario*	Nombre de usuario que usa el nombre del origen de datos para conectarse con la base de datos. Debe especificar el nombre de usuario cuando cree el origen de eventos.
Contraseña	Contraseña que usa el nombre del origen de datos para conectarse con la base de datos. **Precaución:** La contraseña se cifra internamente y se muestra en su forma cifrada.
Activado	Seleccione la casilla de verificación para habilitar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
Dirección*	Este campo no se usa para ODBC. El Log Collector utiliza la dirección que aparece en el archivo **ODBC.ini**.
Avanzado	
Tamaño máximo de celda	Tamaño máximo en bytes de los datos que el Log Collector puede extraer de una celda de la base de datos. El valor predeterminado es **2048**.
Valor nulo	Cadena de caracteres que el Log Collector muestra cuando se devuelve NULO para una celda de la base de datos. Valor predeterminado: **“”** (nulo).

Intervalo de sondeo	El intervalo (cantidad de tiempo en segundos) entre cada encuesta. El valor predeterminado es **180**. Por ejemplo, si especifica 180, el recopilador programa un sondeo del origen de eventos cada 180 segundos. Si aún se está realizando el ciclo de sondeo anterior, el recopilador espera a que ese ciclo termine. Si está sondeando una gran cantidad de orígenes de eventos, es posible que el sondeo tarde más de 180 segundos en comenzar porque los subprocesos están ocupados.
Máximo de eventos de encuesta	La cantidad máxima de eventos por ciclo de sondeo (cuántos eventos se recopilan por ciclo de sondeo).
Depurar	**Precaución:** Habilite la depuración (defina este parámetro en Activado o Detallado) solamente si hay un problema en un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa o desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar). El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento.
Identificador de rastreo inicial	Código de identificación inicial que el Log Collector asigna a este origen de eventos si la recopilación no se inicia. Si no hay ningún valor para este parámetro, el Log Collector comienza al final de la tabla y solo extrae filas después del final de la tabla a medida que se agregan. El valor predeterminado es "" (nulo).

Nombre del archivo	Solamente para orígenes de eventos de Microsoft SQL Server, la ubicación del directorio de archivos de rastreo (por ejemplo, **C:\MyTraceFiles**). Consulte la Guía de configuración del origen de eventos de Microsoft SQL Server de RSA, que se encuentra en RSA Secure Care Online (SCOL), para obtener información detallada sobre cómo crear este directorio con los permisos correctos.
Probar conexión	Comprueba los parámetros de configuración especificados en este cuadro de diálogo para asegurarse de que estén correctos.
Cancelar	Cierra este cuadro de diálogo sin agregar ni modificar parámetros de DSN.
OK	Agrega o modifica los parámetros de DSN.

Tareas

Paso 1. Configurar orígenes de eventos de ODBC en Security Analytics

Parámetros de configuración del origen de eventos de DSN de ODBC

En este tema se describen los parámetros de configuración de DSN de nombres de origen de datos.

Los orígenes de eventos de Open Database Connectivity (ODBC) requieren los Nombres de origen de datos (DSN); de modo que debe definir DSN con sus pares de valores asociados para la configuración de origen de eventos de ODBC. En este tema se describen los parámetros de configuración de DSN.

Para acceder a los parámetros de configuración del origen de eventos de DSN de ODBC:

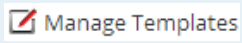
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **ODBC/DSN** en los menús desplegables.

Características

La vista ODBC/DSN en Orígenes de evento tiene un panel: el panel DSN.

Panel DSN

El panel DSN permite agregar, eliminar o editar DSN y los pares de nombre-valor de DSN para orígenes de eventos de ODBC.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar DSN, donde define un DSN y sus parámetros.
	Elimina los DSN seleccionados.
	Muestra el cuadro de diálogo Editar DSN, donde puede editar los pares de nombre-valor del DSN seleccionado.
	Muestra el cuadro de diálogo Administrar plantillas DSN que permite agregar o eliminar plantillas de pares de nombre-valor de DSN.
	Selecciona DSN.
DSN	Nombre del DSN que agregó.
Parámetros	**<name-value for="" p="" pairs="" the=""> </name-value>**

Cuadro de diálogo Agregar/Editar DSN

En este cuadro de diálogo, se agrega o modifica un directorio de archivos del origen de eventos seleccionado.

Característica	Descripción
Plantilla DSN	Seleccione una plantilla predefinida de pares de nombre-valor de valores de DSN para DSN.

Característica	Descripción
Nombre de DSN*	Agregue el nombre del DSN. No puede editar un nombre de DSN después de agregarlo. Este valor debe corresponder a una entrada de DSN en el archivo ODBC.ini. El valor válido es una cadena de caracteres restringida a los siguientes caracteres: `[_a-zA-Z][_a-zA-Z0-9]*` Esto significa que el directorio de archivos debe comenzar con una letra seguida de números, letras y guiones bajos (por ejemplo, oracle_executive_compensation).
Parámetros	Agrega una fila donde puede definir un par de nombre-valor de parámetro. Elimina el par de nombre-valor de parámetro seleccionado. Selecciona pares de nombre-valor de parámetro. Nombre: Ingrese o modifique el nombre del parámetro. Valor: Ingrese o modifique el valor asociado con el nombre del parámetro.
Cancelar	Cierra el cuadro de diálogo sin agregar el DSN y sus pares de nombre-valor o sin guardar las modificaciones en los pares de nombre-valor.
Guardar	Agrega el DSN y sus pares de nombre-valor o guarda las modificaciones en los pares de nombre-valor.

Cuadro de diálogo Administrar plantillas DSN

En este cuadro de diálogo, puede agregar o eliminar plantillas de pares de nombre-valor de DSN.

Característica	Descripción
Panel Selección de plantillas	

Característica	Descripción
	Abre el panel Agregar plantilla, en el cual puede agregar una plantilla de pares de nombre-valor de DSN.
	Elimina la plantilla seleccionada.
	Selecciona una plantilla para eliminación o modificación.
Panel Agregar plantilla	
	Agrega una fila de pares de valores.
	Elimina una fila de pares de valores.
	Selecciona una fila de pares de valores.
Nombre	Ingrese el nombre del parámetro.
Valor	Ingrese el valor asociado con el nombre del parámetro.
Cancelar	Cancela los cambios que realizó en el cuadro de diálogo.
Guardar	Agrega el DSN y sus pares de nombre-valor o guarda las modificaciones en los pares de nombre-valor.
Cerrar	Cierra el cuadro de diálogo sin agregar el DSN y sus pares de nombre-valor o sin guardar las modificaciones en los pares de nombre-valor.

Tareas

Parámetros de configuración del origen de eventos de DSN de ODBC

Paso 1. Configurar orígenes de eventos de ODBC en Security Analytics

Solucionar problemas de la recopilación de ODBC

En este tema se sugiere cómo resolver problemas que pueda encontrar con el protocolo de recopilación de ODBC.

Solucionar problemas de la recopilación de ODBC

Puede solucionar problemas y monitorear la recopilación de ODBC revisando los mensajes informativos, de advertencia y de error del registro del colector de ODBC durante la ejecución de la recopilación.

Cada mensaje de registro de ODBC incluye:

- Timestamp
- Categoría: `debug`, `info`, `warning` o `failure`
- Método de recopilación = `OdbcCollection`
- Tipo de origen de eventos de ODBC (GOTS-name) = nombre de especificación de tipo de ODBC genérico que configuró para el origen de eventos.
- Función de recopilación completada o intentada (por ejemplo, `[processing]`)
- Nombre del origen de eventos de ODBC (DSN-name) = nombre de origen de datos que configuró para el origen de eventos.
- descripción (por ejemplo, cuántos eventos recopiló el Log Collector)
- ID de rastreo = la posición de Log Collector en la tabla de base de datos de destino.

En el siguiente ejemplo se ilustra el mensaje que recibiría tras la recopilación correcta de un evento de ODBC:

```
2014-July-25 17:21:25 info (OdbcCollection) : [event-source]
[processing] [event-source] Published 100 ODBC events: last
tracking id: 2014-July-25 13:22:00.280
```

En el siguiente ejemplo se ilustra un mensaje que podría recibir si un evento de ODBC se recopila incorrectamente:

Mensaje de registro	`timestamp failure (OdbcCollection: [event-source] [processing][event-source-type] Failed during doWork: Unable to prepare statement: state: S0002; error-code:208; description: [RSA] [ODBC-driver] [event-source-type]Invalid object name 'object-name'.`
Causa posible	La recopilación de ODBC falló cuando estaba accediendo al controlador de ODBC o a la base de datos de destino.
Soluciones	Valide los pares de DSN/valores para el origen de eventos.

Guía de configuración de la recopilación de SDEE

En esta guía se indica cómo configurar el protocolo de recopilación de SDEE. Este protocolo recopila eventos de un sistema de detección de intrusiones (IDS) y mensajes de un servicio de prevención de intrusiones (IPS).

Antes de configurar el protocolo de recopilación de SDEE, debe implementarla recopilación de registros.

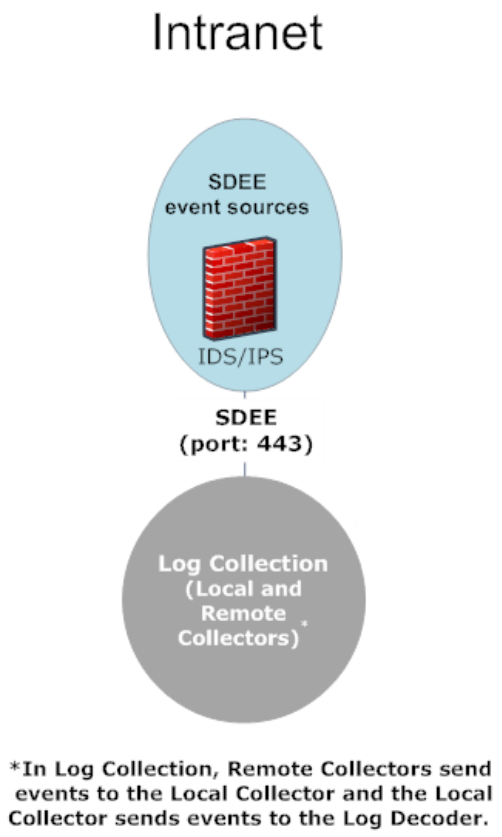
Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Conceptos básicos

En esta guía se indica cómo configurar el protocolo de recopilación de SDEE que recopila eventos de un sistema de detección de intrusiones (IDS) y mensajes de un servicio de prevención de intrusiones (IPS).

Escenario de implementación

En la siguiente figura se ilustra cómo debe implementar el protocolo de recopilación de SDEE en Security Analytics.

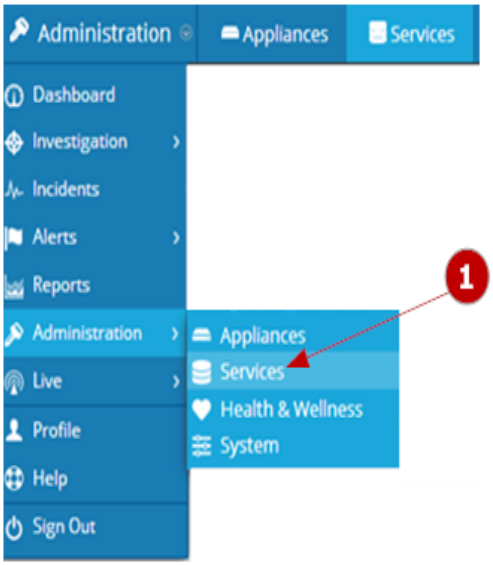


Procedimientos

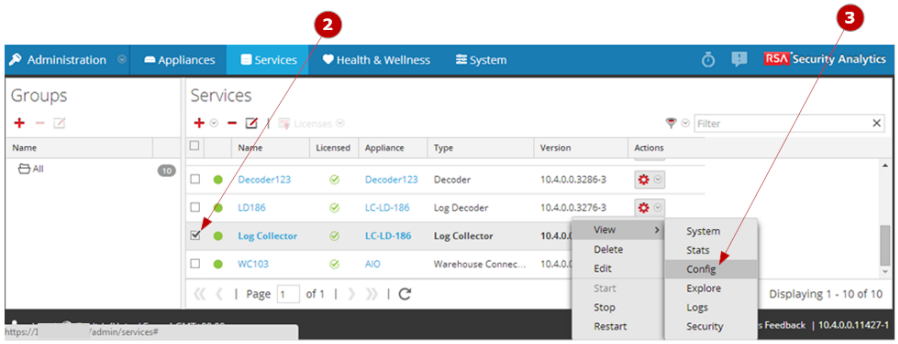
Configurar el protocolo de recopilación de SDEE en Security Analytics

Debe configurar el Log Collector para usar la recopilación de SDEE para un origen de eventos en la pestaña Origen de eventos de la vista Parámetro de Log Collector. En la siguiente figura se representa el flujo de trabajo básico para configurar un origen de eventos para la recopilación de SDEE en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de SDEE en Security Analyticspara obtener instrucciones paso a paso acerca de cómo configurar orígenes de eventos en Security Analytics que utilizan el protocolo de recopilación de SDEE.
- Referencia: Parámetros de configuración del origen de eventos de SDEE para obtener una descripción detallada de cada parámetro del protocolo de recopilación de SDEE.

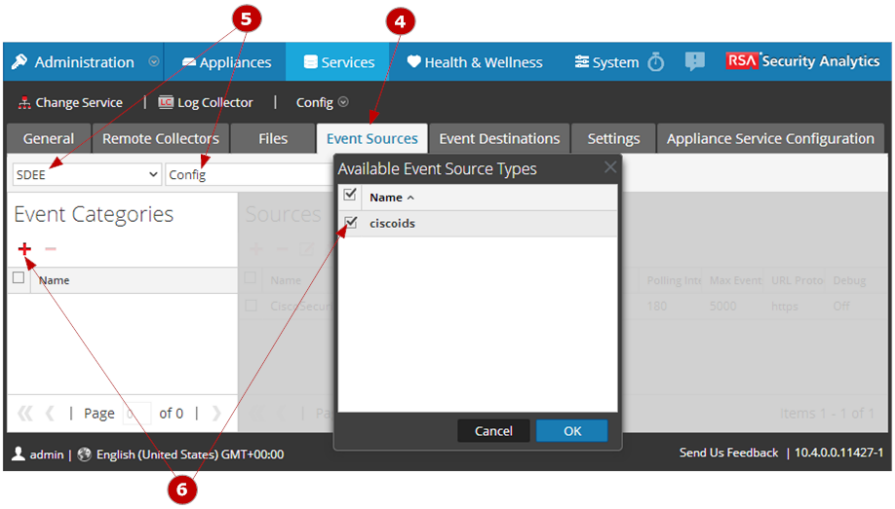


1 Acceda a la vista **Servicios**.



2 Seleccione un servicio de **recopilación de registros**.

3 Haga clic en ⌄ bajo **Acciones** y seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de la **recopilación de registros**.

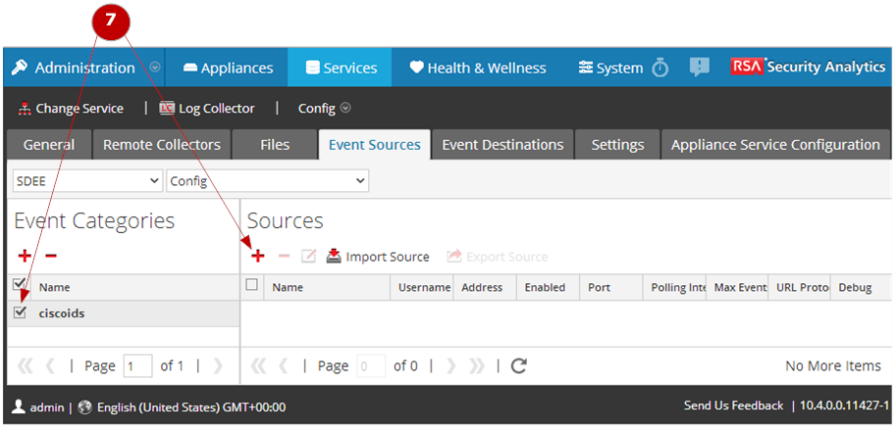


4 Haga clic en la pestaña **Orígenes de evento**.

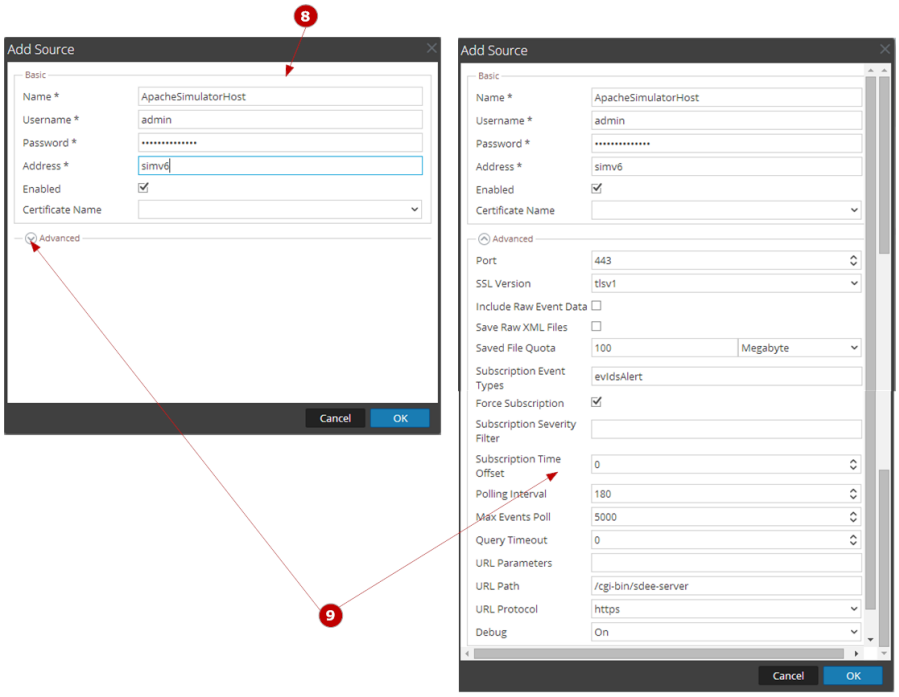
5 Seleccione **SDEE** como el protocolo de recopilación y seleccione **Configuración**.

6 Haga clic en + y seleccione **SDEE** en la categoría de orígenes de eventos.

La categoría de origen de eventos es parte del contenido que descargó de LIVE.



7 Seleccione la categoría **SDEE** y haga clic en +.



8 Especifique los parámetros básicos requeridos para el origen de eventos de SDEE.

9 Haga clic en y especifique parámetros adicionales que mejoran la manera en que el protocolo de SDEE maneja la recopilación de eventos para el origen de eventos.

Configurar los orígenes de eventos para usar el protocolo de recopilación de SDEE

Debe configurar cada origen de eventos que utilice el protocolo de recopilación de SDEE para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de SDEE para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de SDEE, con una lista de verificación que contiene cada paso de configuración

Los pasos de configuración del protocolo de recopilación de SDEE se deben realizar en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de configuración de la recopilación de SDEE

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de SDEE en Security Analytics.	
2	Configurar orígenes de eventos de SDEE para enviar eventos a Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de SDEE configurado.	
4	Verificar que la recopilación de SDEE esté funcionando.	

Paso 1. Configurar orígenes de eventos de SDEE en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de SDEE para el Log Collector.

Después de realizar este procedimiento, habrá...

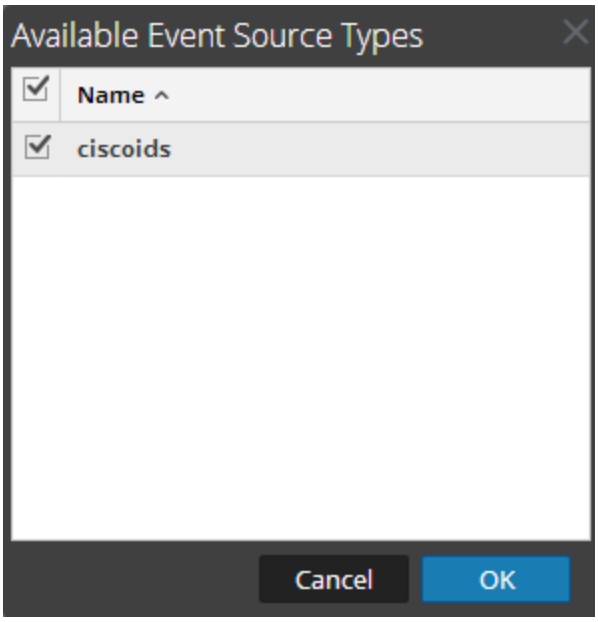
- Configurado un origen de eventos de SDEE.
- Modificado un origen de eventos de SDEE.

Volver a Procedimientos

Procedimientos

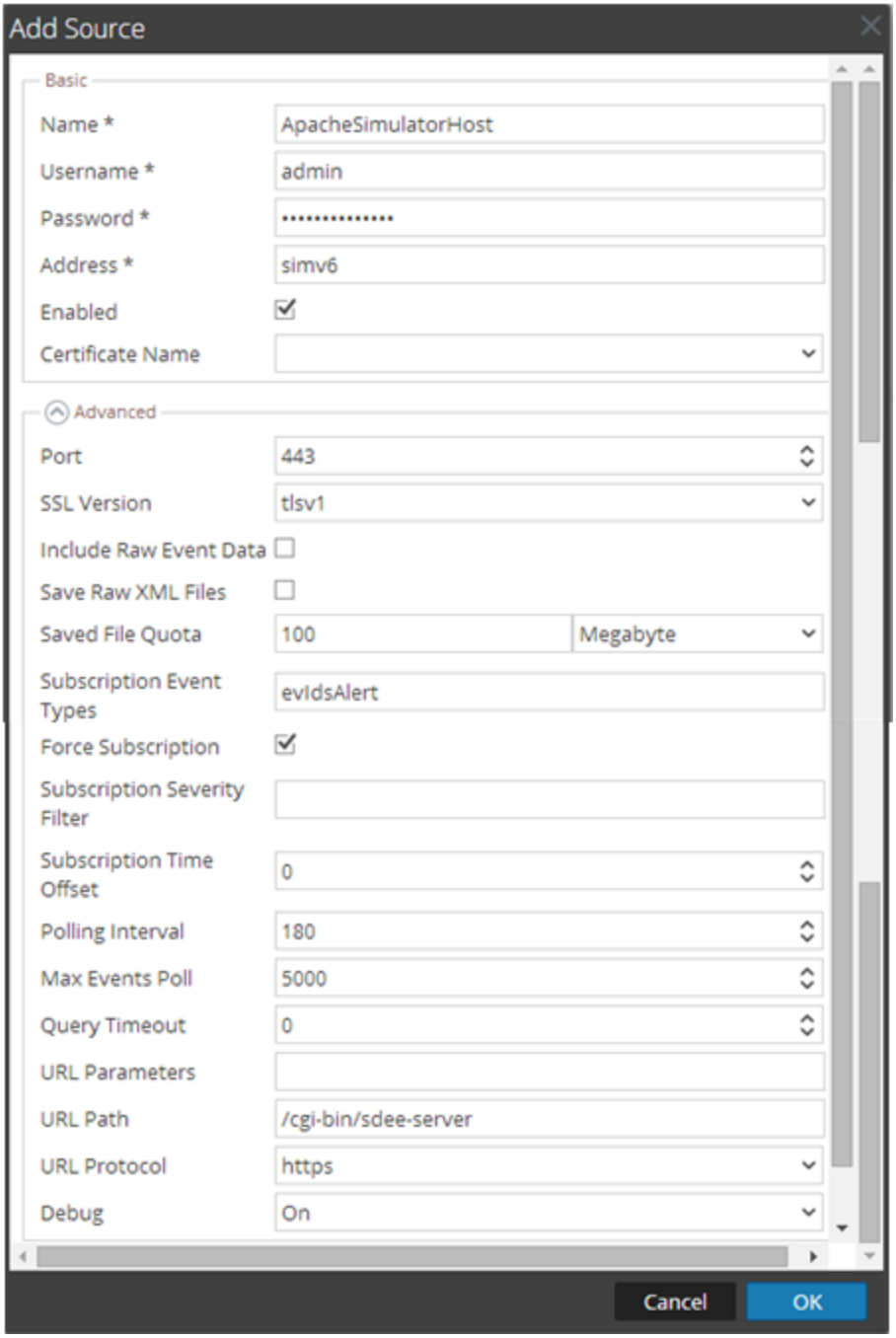
Configurar un origen de eventos de SDEE

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **SDEE/Configuración** en el menú desplegable.
   En el panel **Categorías de evento** se muestran los orígenes de eventos de SDEE que están configurados, si los hay.
5. En la barra de herramientas del panel **Categorías de evento**, haga clic en  .



Si no ve ningún tipo de origen de eventos en esta lista, no cargó el contenido que obtuvo de Atención al cliente como parte de la actualización de Log Collector a esta versión.

6. Seleccione un tipo de origen de eventos (por ejemplo, **ciscoids**) y haga clic en **Aceptar**.
   El tipo de origen de eventos recién agregado se muestra en el panel **Categorías de evento**.
7. Seleccione el nuevo tipo en el panel **Categorías de evento** y haga clic en + en la barra de herramientas Orígenes.
   Se muestra el cuadro de diálogo **Agregar origen**.
8. Agregue un **nombre**, un **nombre de usuario**, una **dirección** y una **contraseña**, modifique cualquier otro parámetro que sea necesario cambiar y haga clic en **Aceptar**.

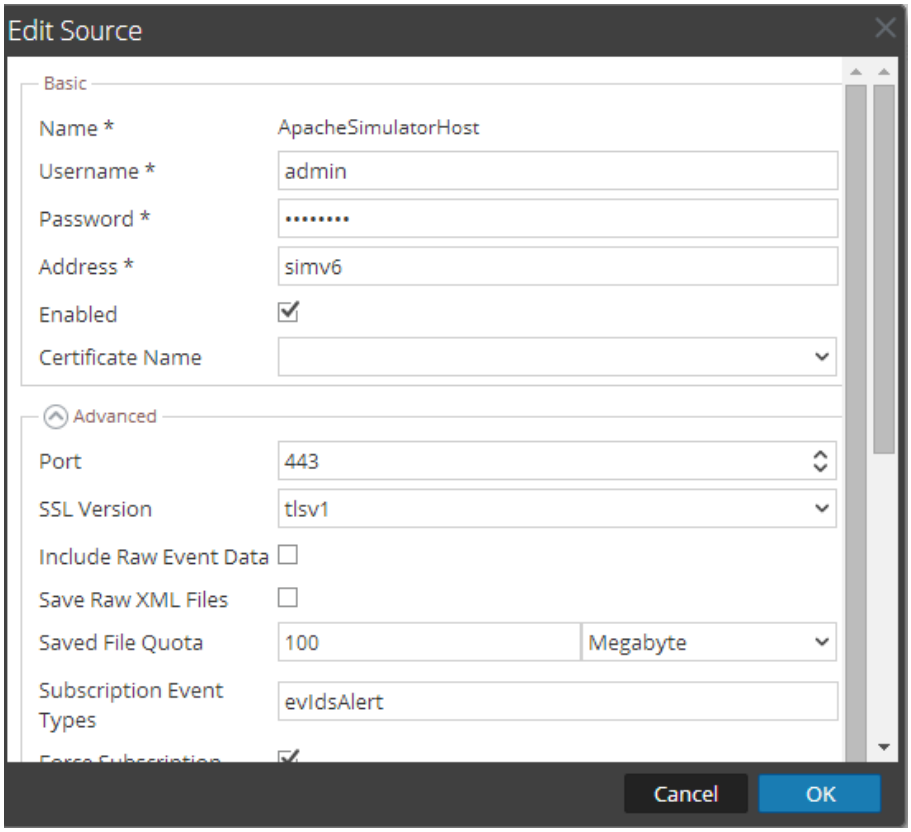


El nuevo origen de eventos se muestra en la lista.

Modificar un origen de eventos de SDEE

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.

4. En la pestaña **Orígenes de evento**, seleccione **SDEE/Configuración** en el menú desplegable.
5. Seleccione un tipo de origen de eventos en el panel Categorías de evento.
6. En el panel **Orígenes**, seleccione un origen de eventos y haga clic en  .
   Se muestra el cuadro de diálogo **Editar origen**.



7. Modifique los parámetros que necesiten cambios y haga clic en **Aceptar**.
8. Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado.

Parámetros

Referencia: Parámetros de configuración del origen de eventos de SDEE

Paso 2. Configurar orígenes de eventos de SDEE para enviar eventos a Security Analytics

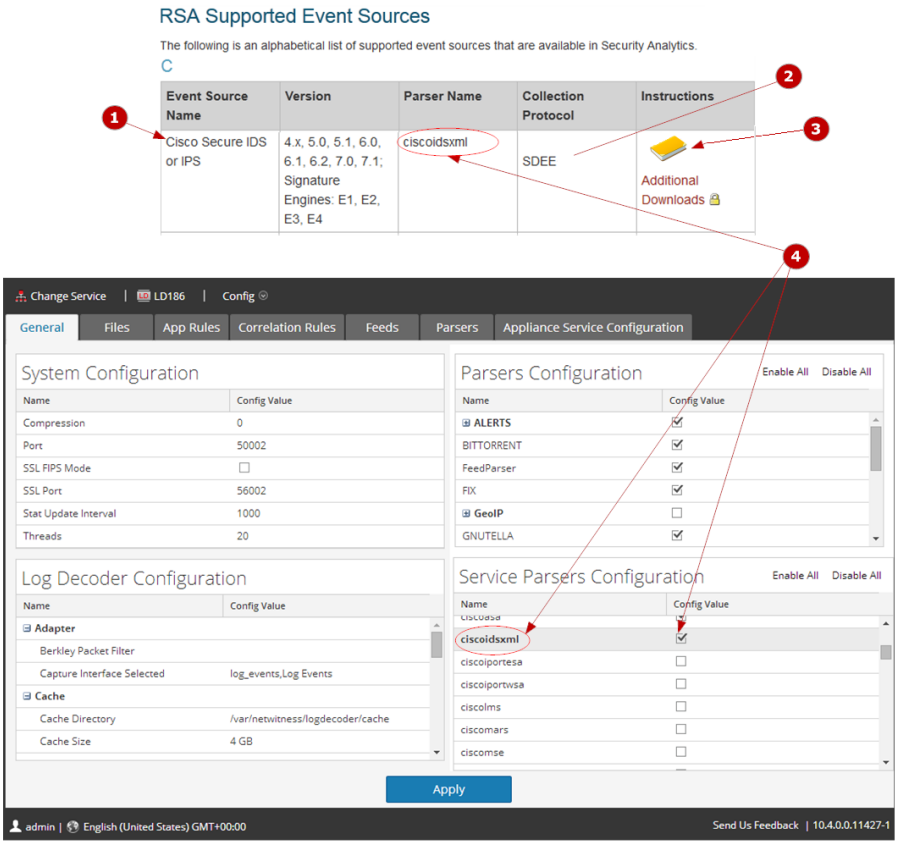
En este tema se indica dónde encontrar los orígenes de eventos que son compatibles actualmente con la recopilación de SDEE y las instrucciones de configuración disponibles para cada origen de eventos.

Volver a Procedimientos

Los orígenes de eventos actualmente compatibles con la recopilación de SDEE están disponibles en la lista de orígenes de eventos compatibles.

Procedimiento

La lista de orígenes de eventos compatibles de RSA es una lista alfabética de todos los orígenes de eventos que son compatibles actualmente con Security Analytics, en la cual se identifican los orígenes de eventos que puede usar con la recopilación de SDEE.



1 Busque el nombre del origen de eventos.

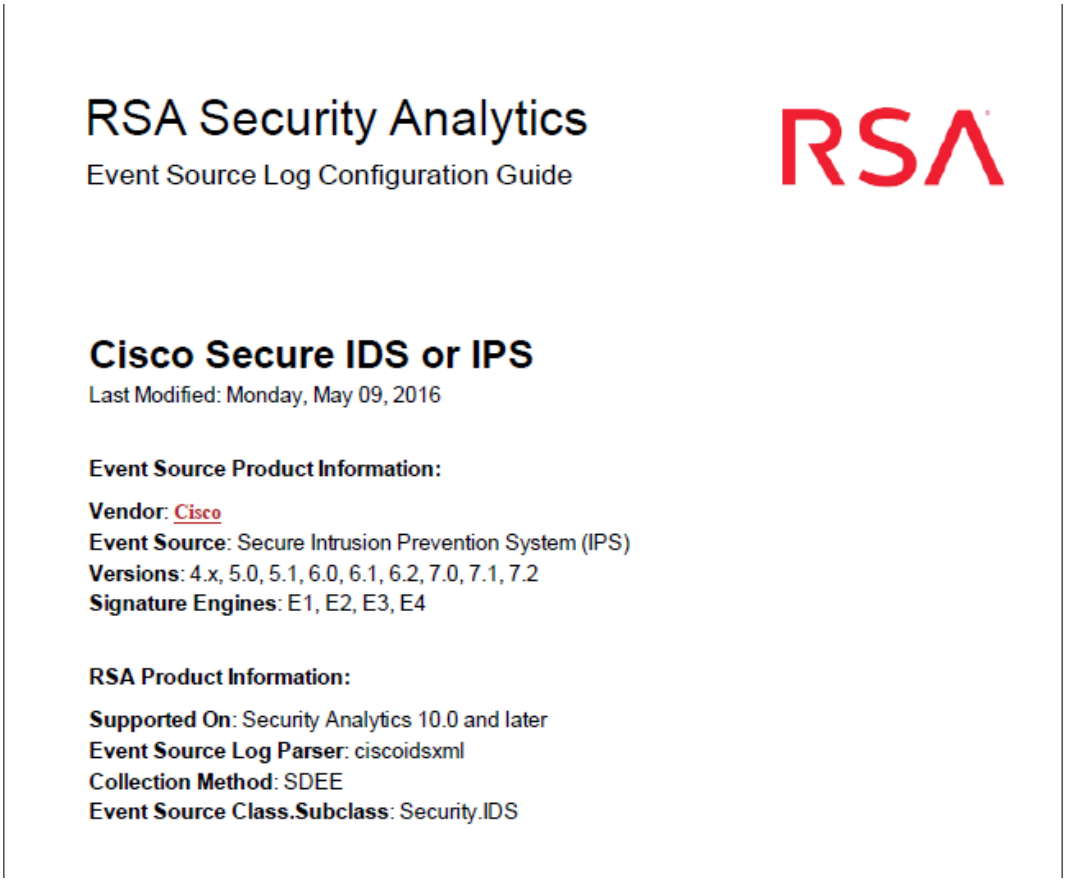
2 Verifique que sea compatible con el protocolo de recopilación de SDEE.

3 Haga clic en  para recuperar las instrucciones de configuración del origen de eventos.

4 Verifique que haya descargado el analizador de origen de eventos correcto (por ejemplo, **ciscoidsxml**) desde LIVE a Log Decoder y que lo haya activado.

Ejemplo de instrucciones de configuración

La siguiente ilustración se toma de las instrucciones de configuración de Cisco Secure IDS o IPS.



RSA Security Analytics

Event Source Log Configuration Guide

RSA

Cisco Secure IDS or IPS

Last Modified: Monday, May 09, 2016

Event Source Product Information:

Vendor: Cisco
Event Source: Secure Intrusion Prevention System (IPS)
Versions: 4.x, 5.0, 5.1, 6.0, 6.1, 6.2, 7.0, 7.1, 7.2
Signature Engines: E1, E2, E3, E4

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: ciscoidsxml
Collection Method: SDEE
Event Source Class.Subclass: Security.IDS

Paso 3. Iniciar el servicio para el protocolo de recopilación de SDEE configurado

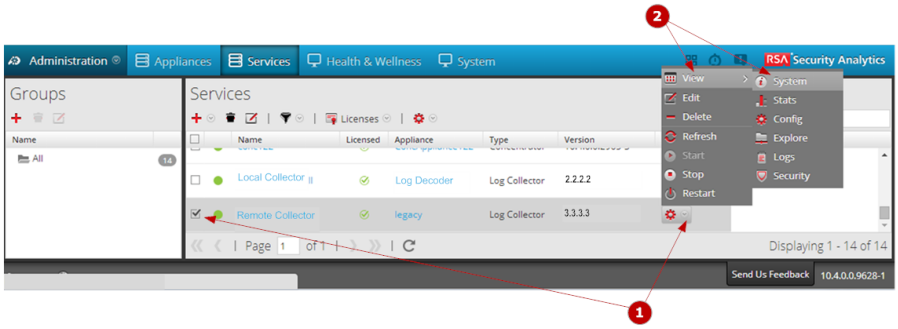
En este tema se indica cómo iniciar un servicio de recopilación de SDEE detenido.

Volver a Procedimientos

Si un servicio de recopilación de SDEE se detuvo, puede ser necesario reiniciarlo o habilitar el inicio automático de un servicio individual

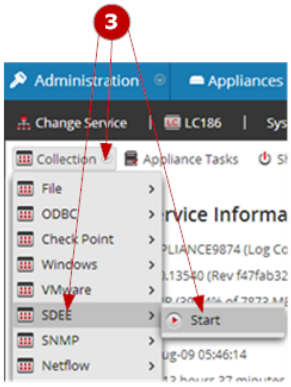
Procedimiento

En la siguiente figura se muestra cómo iniciar un servicio de recopilación. Consulte el tema **Habilitar el inicio automático de servicios individuales** de la *Guía de configuración de la recopilación de registros* si desea que el servicio se inicie automáticamente.



1 Seleccione un servicio **Log Collector** y haga clic en ⚙ bajo **Acciones**.

2 Haga clic en **Ver > Sistema**.



3 Haga clic en **Recopilación > SDEE** y, a continuación, en **Iniciar**.

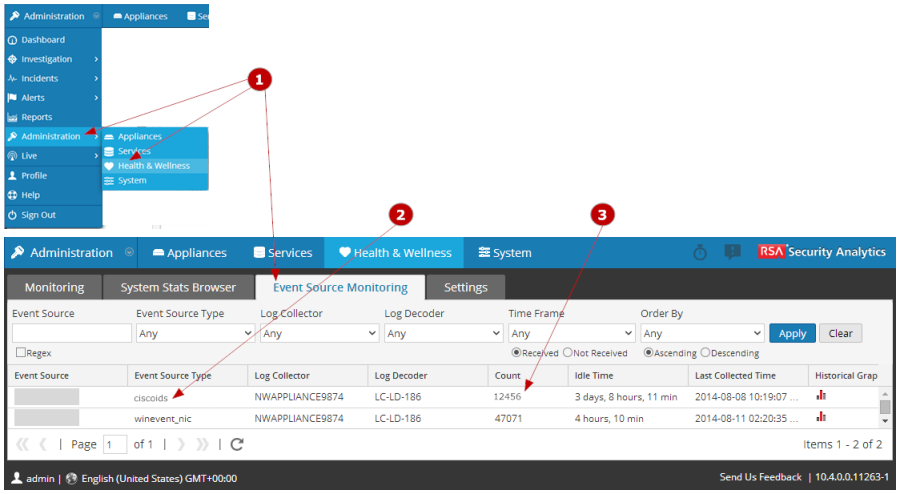
Paso 4. Verificar que la recopilación de SDEE esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de SDEE se configuró correctamente. Debe verificar que la recopilación de SDEE esté configurada correctamente; de lo contrario, no funcionará.

Volver a Procedimientos

Procedimiento

En la siguiente figura se ilustra cómo puede verificar que la recopilación de SDEE esté funcionando desde **Administration > Estado y condición > pestaña Monitoreo de orígenes de eventos**.

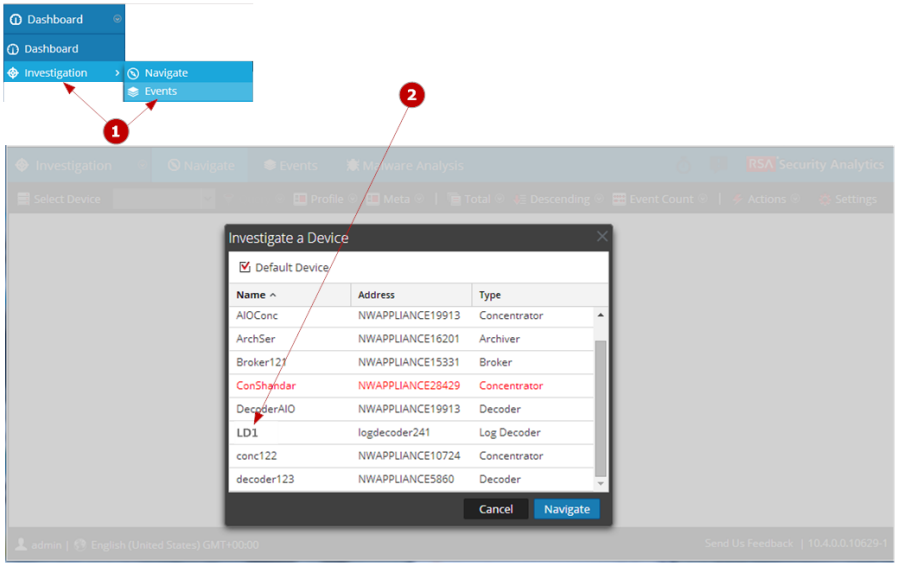


1 Acceda a la pestaña **Monitoreo de orígenes de eventos** desde la vista **Administration > Estado y condición**.

2 Busque un tipo de origen de eventos de SDEE (por ejemplo, **ciscoids**) en la columna **Tipo de origen de evento**.

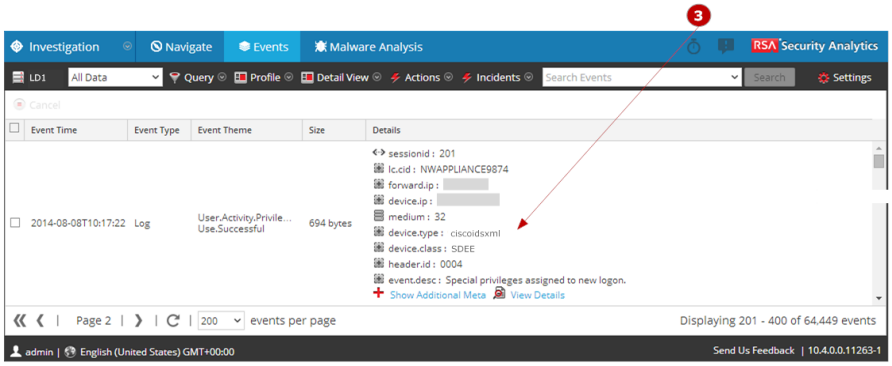
3 Busque actividad en la columna **Conteo** para verificar que la recopilación de SDEE esté aceptando eventos.

En la siguiente figura se ilustra cómo puede verificar que la recopilación de SDEE esté funcionando desde **Investigation > vista Eventos**.



1 Acceda a **Investigation > vista Eventos**.

2 Seleccione el Log Decoder (por ejemplo, **LD1**) que recopila eventos de SDEE en el cuadro de diálogo **Investigar un dispositivo**.



3 Busque un analizador de orígenes de eventos de SDEE (por ejemplo, **ciscoidsxml**) en la columna **Tipo de dispositivo** para verificar que la recopilación de SDEE esté aceptando eventos.

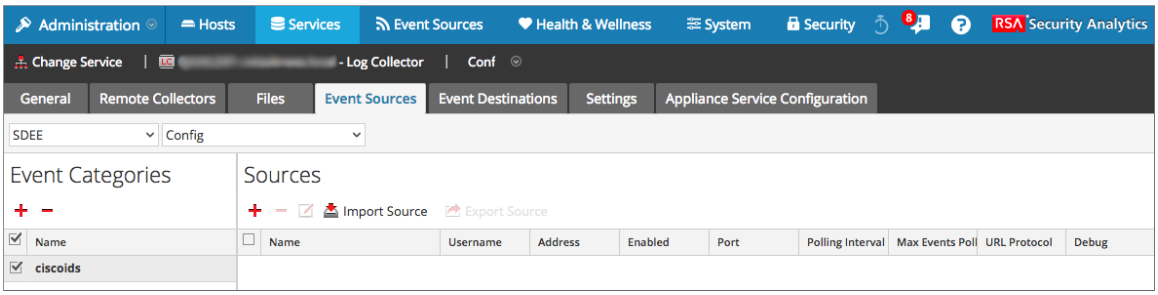
Referencia: Parámetros de configuración del origen de eventos de SDEE

En este tema se describen los parámetros del origen de eventos del intercambio de eventos de dispositivos de seguridad (SDEE).

Use la opción SDEE de la pestaña Ver orígenes de eventos en la Configuración de Log Collector para agregar y mantener parámetros de configuración para la recopilación de datos de un sistema de detección de intrusiones (IDS) (por ejemplo, mensajes de Cisco Secure IDS) formateados conforme al estándar SDEE.

Para acceder a los parámetros de configuración del origen de eventos de SDEE:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **SDEE/Configuración** en el menú desplegable.



La vista SDEE/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar los tipos de orígenes de eventos correspondientes.

Característica	Descripción
+	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
−	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.
☐	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de tipos de orígenes de eventos compatibles.

Característica	Descripción
☐	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.

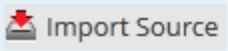
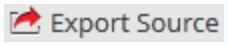
Característica	Descripción
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

Panel Orígenes

Use este panel para revisar, agregar, modificar y eliminar orígenes de eventos.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar origen, en el cual puede definir los parámetros para un host de firewall.
	Elimina el host que seleccionó.
	Abre el cuadro de diálogo Editar origen, en el cual puede editar los parámetros del origen de eventos seleccionado. Seleccione varios orígenes de eventos y haga clic en  para abrir el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar hosts de forma masiva desde un archivo de valores separados por comas (CSV). Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo .csv que contiene los parámetros de los hosts seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.

Cuadro de diálogo Agregar/Modificar origen

En este cuadro de diálogo, se agrega o modifica un directorio de archivos del origen de eventos seleccionado.

Característica	Descripción
Parámetros de origen	Muestra los parámetros completados con los valores predeterminados. Ingrese o modifique los valores apropiados.
Cancelar	Cierra el cuadro de diálogo sin agregar un directorio de archivo ni guardar los valores de los parámetros de los orígenes de eventos seleccionados.
OK	En el cuadro de diálogo Agregar origen, agrega el directorio de archivos y sus parámetros. En el cuadro de diálogo Modificar orígenes, aplica los cambios en los valores de los parámetros del origen de eventos seleccionado.

Parámetros de Agregar/Editar origen

En la siguiente tabla se proporcionan descripciones de los parámetros del origen.

Nombre	Descripción
Básico	
Nombre *	Nombre del origen de eventos.
Nombre de usuario*	Nombre de usuario para autenticarse con el origen de eventos.
Contraseña *	Contraseña para autenticarse con el origen de eventos. **Precaución:** La contraseña se cifra internamente y se muestra en su forma cifrada.
Dirección *	Dirección IP del origen de eventos, que es el sensor de IDS.
Activado	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.

Nombre	Descripción
Nombre del certificado	El nombre del certificado que las conexiones seguras deben utilizar cuando el modo de transporte sea https. Los valores válidos son los certificados que existen actualmente en su área de almacenamiento de confianza que creó usando la pestaña Configuración. **Nota:** Si deja este campo en blanco, Security Analytics no ejecuta la validación.
Avanzado	
Puerto	Número de puerto. Un número de puerto válido es cualquier número dentro del rango de 1 a 65535 (el valor predeterminado es 443).
Versión de SSL	Versión de SSL a través de la cual está configurada la comunicación del origen de eventos. Los valores válidos son: • tlsv1 (valor predeterminado) • sslv2 • sslv3 • sslv2
Incluir datos de evento crudo	Seleccione la casilla de verificación para incluir datos XML crudos para el evento que devuelve el origen de eventos de SDEE en los datos de eventos que se envían a Log Decoder. De forma predeterminada, la casilla de verificación no está seleccionada. **Nota:** este parámetro solo se admite para datos de contenido 3.0.
Guardar archivos XML crudos	Seleccione la casilla de verificación para enviar datos crudos a **/var/netwitness/logcollector/runtime/sdee/saved_raw_events**. De forma predeterminada, la casilla de verificación no está seleccionada.
Cuota de archivo guardada	Cantidad de espacio disponible para los archivos XML guardados. El valor válido es la cantidad de megabytes, kilobytes o gigabytes de espacio que desea asignar. Security Analytics se configura de forma predeterminada en **100** megabytes.

Nombre	Descripción
Tipos de eventos de suscripción	(Solo se aplica cuando realiza una solicitud de suscripción inicial.) Filtra eventos de los tipos de eventos de suscripción especificados (por ejemplo, alertas de IDS). El valor predeterminado es **evIdsAlert**.
Forzar suscripción	(Solo se aplica cuando realiza una solicitud de suscripción inicial.) Seleccione la casilla de verificación si desea que el servidor de SDEE cree una suscripción incluso cuandoestá abierta la cantidad máxima de suscripciones. La casilla de verificación está seleccionada de manera predeterminada. **Nota:** el servidor cierra la suscripción existente para acomodar la nueva.
Filtro de severidad de suscripción	(Solo se aplica cuando realiza una solicitud de suscripción inicial.) A todos los eventos que genera un origen de eventos de SDEE se les asigna un nivel de severidad. Use este parámetro para filtrar los mensajes de eventos por severidad. Si deja este campo en blanco, Security Analytics recopila todos los eventos independientemente del nivel de severidad. Por ejemplo, si desea recopilar eventos exclusivamente con niveles de gravedad media y alta, debe especificar la siguiente cadena de caracteres en este parámetro: **medium+high**
Compensación de tiempo de suscripción	(Solo se aplica cuando realiza una solicitud de suscripción inicial.) Valor predeterminado (tiempo de suscripción activado). Este parámetro le permite especificar desde cuánto tiempo hacia atrás (en segundos) comenzar a extraer eventos.
Intervalo de sondeo	El intervalo (cantidad de tiempo en segundos) entre cada encuesta. El valor predeterminado es **180**. Por ejemplo, si especifica **180**, el recopilador programa un sondeo del origen de eventos cada **180** segundos. Si aún se está realizando el ciclo de sondeo anterior, el recopilador espera a que ese ciclo termine. Si está sondeando una gran cantidad de orígenes de eventos, es posible que el sondeo tarde más de **180** segundos en comenzar porque los subprocesos están ocupados.
Máximo de eventos de encuesta	La cantidad máxima de eventos por ciclo de sondeo (cuántos eventos se recopilan por ciclo de sondeo).

Nombre	Descripción
Tiempo de espera agotado de consulta	Valor (en segundos) que se transmite al origen de eventos de SDEE y que indica al servidor cuánto tiempo debe esperar cuando no hay datos.
Parámetros de URL	Anexa parámetros a la cadena de URL (por ejemplo, **/cgi-bin/sdee-server.cgi**).
Ruta de URL	Ruta de URL del servidor de SDEE.
Protocolo de URL	Los valores válidos son: • **http** • **https**
Depurar	**Precaución:** Active la depuración (defina este parámetro en "Activado" o "Detallado") solamente si tiene un problema con un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa o desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar). El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento.

Tareas

Paso 1. Configurar orígenes de eventos de SDEE en Security Analytics

Solucionar problemas de la recopilación de SDEE

En este tema se señalan posibles problemas que puede encontrar en la recopilación de SDEE y las soluciones que se sugieren para ellos.

Solucionar problemas de la recopilación de SDEE

En general, se reciben mensajes de registro más confiables cuando se desactiva SSL.

Puede seleccionar el parámetro de configuración Guardar archivos XML crudos para guardar los archivos XML crudos desde el servidor a **/var/netwitness/logcollector/runtime/sdee/saved_sdee_files** para investigar más los problemas de SDEE. El nombre de estos archivos contiene el nombre del origen de eventos y el registro de fecha y hora. Puede controlar la cantidad de archivos (datos) que almacena Security Analytics con el parámetro de configuración Cuota de archivo guardada. El valor que ingresa para la cuota es la cantidad de bytes que almacena Security Analytics en kilobytes, megabytes o gigabytes.

Guía de configuración de la recopilación de SNMP

En esta guía se indica cómo configurar el protocolo de recopilación de SNMP. Este protocolo acepta SNMP traps.

Debe implementar Log Collection antes de poder configurar el protocolo de recopilación de punto de comprobación.

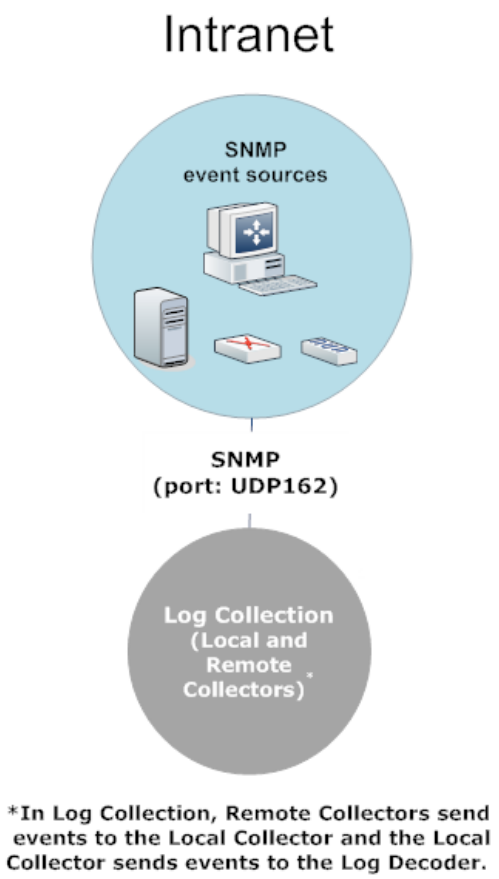
Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Conceptos básicos

En esta guía se indica cómo configurar el protocolo de recopilación de SNMP que acepta SNMP traps.

Escenario de implementación

En la siguiente figura se ilustra cómo implementar el protocolo de recopilación de SNMP en Security Analytics.



Procedimientos

Configurar el protocolo de recopilación de SNMP en Security Analytics

Log Collector se configura para usar la recopilación de SNMP para un origen de eventos en la pestaña Origen de evento de la vista de parámetros de Log Collector. En la siguiente figura se representa el flujo de trabajo básico para configurar un origen de eventos para la recopilación de SNMP en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de SNMP en Security Analyticspara obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de SNMP.
- Referencias: Parámetros de configuración de la recopilación de SNMPpara obtener una descripción detallada de cada parámetro del protocolo de recopilación de SNMP.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. En la cuadrícula **Servicios**, seleccione un servicio de **recopilación de registros**.

3. Seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de la **recopilación de registros**.
4. Haga clic en la pestaña **Orígenes de evento**.
5. Seleccione **SNMP** como el protocolo de recopilación y elija **Configurar**.
6. Haga clic en  y seleccione **SNMP** como la categoría de origen de eventos.
   La categoría de origen de eventos es parte del contenido que descargó de Live.
7. Seleccione **SNMP** como el protocolo de recopilación y elija **Administrador de usuarios de SNMP v3**.
8. Haga clic en  para mostrar el cuadro de diálogo **Agregar usuario SNMP**.
9. Defina los parámetros del **usuario SNMP** y haga clic en **Guardar**.

Configurar orígenes de eventos de modo que usen el protocolo de recopilación de SNMP

Debe configurar cada origen de eventos que usa el protocolo de recopilación de SNMP para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de SNMP para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de SNMP, con una lista de verificación que contiene cada paso de configuración.

Los pasos de configuración del protocolo de recopilación de SNMP se deben realizar en la secuencia específica en la cual se presentan los procedimientos.

Lista de verificación de la configuración de la recopilación de SNMP

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de SNMP en Security Analytics.	
2	Configurar orígenes de eventos de SNMP para enviar eventos a Security Analytics.	

Paso	Descripción	√
3	Iniciar el servicio para el protocolo de recopilación de SNMP configurado.	
4	Verificar que la recopilación de SDEE esté funcionando.	

Paso 1. Configurar orígenes de eventos de SNMP en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de SNMP para el Log Collector.

Después de realizar este procedimiento, habrá...

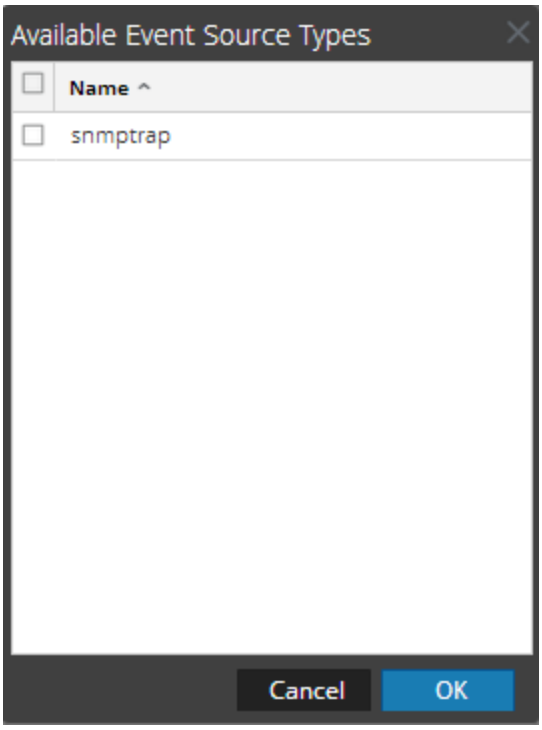
- Configurado un origen de eventos de SNMP.
- Modificado un origen de eventos de SNMP.

Volver a Procedimientos

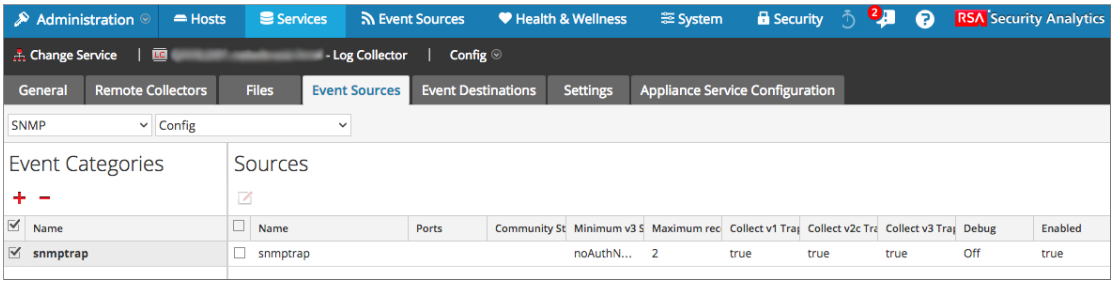
Procedimientos

Configurar un origen de eventos de SNMP

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración >**.
4. En la pestaña **Orígenes de evento**, seleccione **SNMP/Configuración** en el menú desplegable.
   En el panel **Categorías de evento** se muestran los orígenes de eventos de SNMP que están configurados, si los hay.
5. En la barra de herramientas del panel **Categorías de evento**, haga clic en  .
   Se muestra el cuadro de diálogo **Tipos de origen de evento disponibles**.



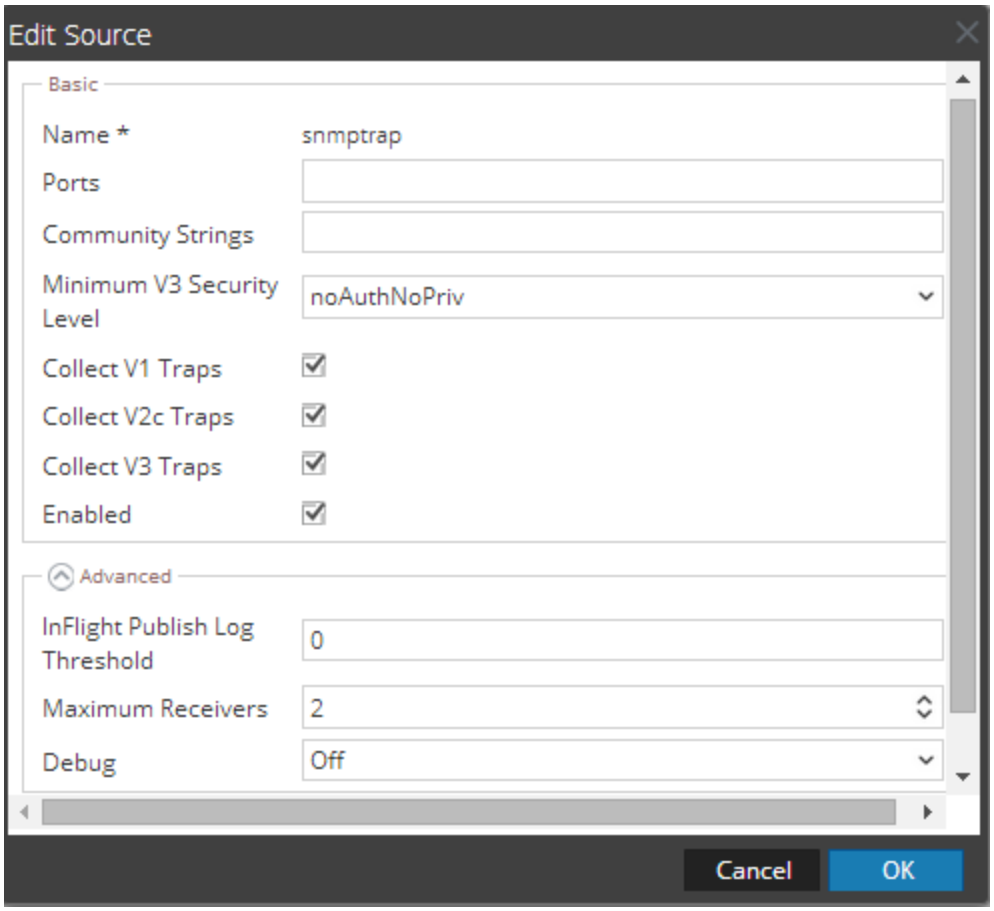
6. Seleccione un tipo de origen de eventos (por ejemplo, **snmptrap**) y haga clic **Aceptar**.
   El tipo de origen de eventos recién agregado se muestra en el panel **Categorías de evento**.
7. Seleccione el nuevo tipo en el panel **Categorías de evento**.
   El nuevo origen de SNMP se muestra en el panel **Orígenes**.



Modificar un origen de eventos de SNMP

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración >**.
4. En la pestaña **Orígenes de evento**, seleccione **SNMP/Configuración** en el menú desplegable.

5. Seleccione un tipo de origen de eventos (por ejemplo, **snmptrap**) en el panel **Categorías de evento** y haga clic en **Aceptar**.
6. En el panel **Origen**, seleccione un origen de eventos y haga clic en  .
   Se muestra el cuadro de diálogo **Editar origen**.



7. Modifique los parámetros que necesiten cambios y haga clic en **Aceptar**.
   Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado.

Parámetros

Paso 1. Configurar orígenes de eventos de SNMP en Security Analytics

Parámetros de configuración del administrador de usuarios de SNMP v3

Paso 2. Configurar orígenes de eventos de SNMP para enviar eventos a Security Analytics

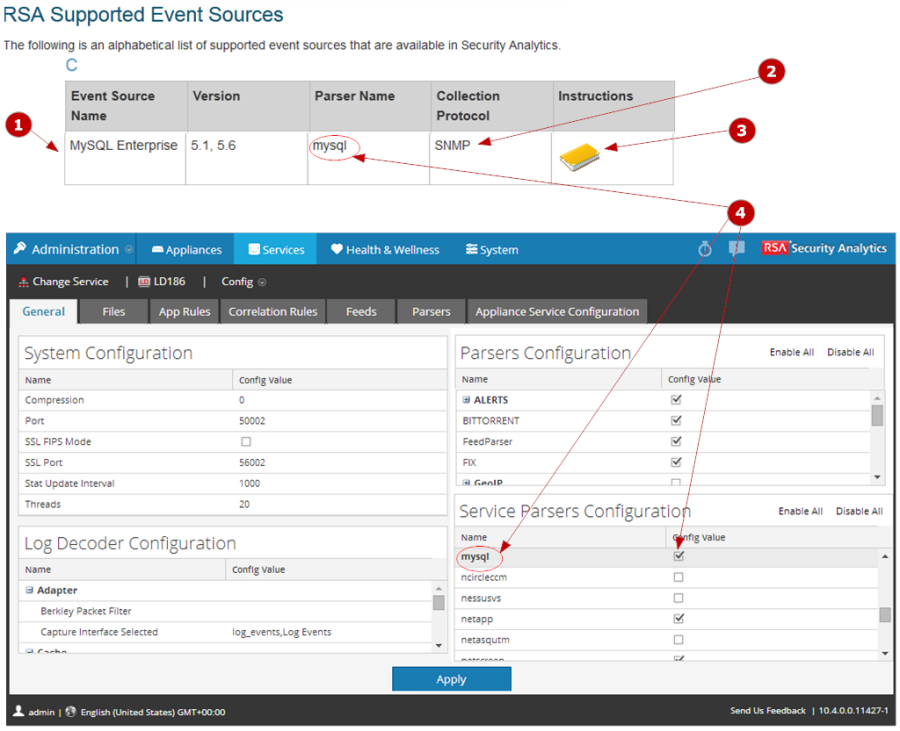
En este tema se indica dónde puede encontrar los orígenes de eventos que son actualmente compatibles con la recopilación de SNMP y las instrucciones de configuración disponibles para cada origen de eventos.

Para conocer los orígenes de eventos que son compatibles actualmente con la recopilación de SNMP, consulte la lista de orígenes de eventos compatibles. A continuación se proporcionan ejemplos de instrucciones de configuración.

Procedimiento

Volver a Procedimientos

La lista de orígenes de eventos compatibles de RSA es una lista alfabética de todos los orígenes de eventos que son compatibles actualmente con Security Analytics, en la cual se identifican los orígenes de eventos que puede usar con la recopilación de SNMP.



1. Busque el nombre del origen de eventos.
2. Verifique que sea compatible con el protocolo de recopilación de SNMP.
3. Haga clic en para ver las instrucciones de configuración del origen de eventos.

4 Verifique que haya descargado el analizador de origen de eventos correcto (por ejemplo, **mysql**) desde LIVE a Log Decoder y que lo haya activado.

Ejemplo de instrucciones de configuración

La siguiente ilustración se toma de las instrucciones de configuración de MySQL Enterprise.


RSA Security Analytics

Event Source Log Configuration Guide

RSA

MySQL Enterprise

Last Modified: Monday, June 09, 2014

Event Source Product Information:

Vendor: MySQL
Event Source: MySQL Enterprise
Versions: 5.1 and 5.6

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: mysql
Collection Method: SNMP
Event Source Class.Subclass: Storage.Database

Paso 3. Iniciar el servicio para el protocolo de recopilación de SNMP configurado

En este tema se indica cómo iniciar un servicio de recopilación de SNMP detenido.

Debe iniciar un servicio de recopilación de SNMP detenido para hacer que vuelva a funcionar. También tiene la opción de habilitar el inicio automático de protocolos individuales si desea que estos se inicien automáticamente.

Procedimiento

Volver a Procedimientos

En el siguiente procedimiento se indica cómo iniciar un protocolo de recopilación. Consulte el tema **Habilitar el inicio automático de protocolos individuales** de la *Guía de configuración de la recopilación de registros* si desea que el protocolo se inicie automáticamente.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector** y elija  **> Ver > Sistema**.
   Se muestra la vista **Sistema de servicios**.
3. Haga clic en **Recopilación > SNMP > Iniciar**.

Paso 4. Verificar que la recopilación de SNMP esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de SNMP se configuró correctamente.

Volver a Procedimientos

Debe verificar que la recopilación de SNMP esté configurada correctamente; de lo contrario, no funcionará.

Procedimiento

En el siguiente procedimiento se indica cómo puede verificar que la recopilación de SNMP esté funcionando desde **Administration > Estado y Condición > pestaña Monitoreo de orígenes de eventos**.

1. En el menú de **Security Analytics**, seleccione **Administration > Estado y condición**.
2. Haga clic en la pestaña **Monitoreo de orígenes de eventos**.
3. Busque **SNMP** en la columna **Tipo de origen de evento**.
4. Busque actividad en la columna **Conteo** para verificar que la recopilación de SNMP esté aceptando eventos.

Referencias: Parámetros de configuración de la recopilación de SNMP

En este tema se describen los parámetros de configuración del origen de eventos de SNMP.

Cada parámetro de configuración del origen de eventos de recopilación de SNMP tiene dos partes con una vista por separado, parámetros de SNMP y del administrador de usuarios de SNMP v3.

Parámetros de configuración del origen de eventos de SNMP

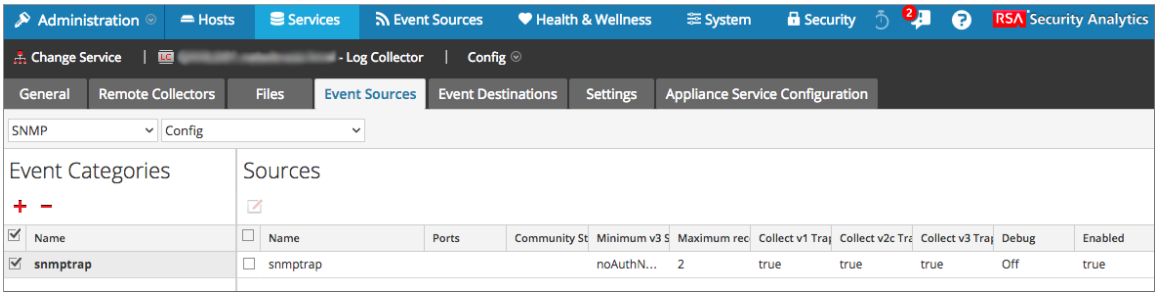
En este tema se describen los parámetros de origen de eventos del protocolo simple de administración de red (SNMP).

El protocolo simple de administración de red (SNMP) es un conjunto de estándares de Internet para la administración de servicios de red. Incluye un protocolo, un esquema de definición de datos y conjuntos de datos conocidos como Management Information Bases (MIB). Las MIB incluyen estándares de Internet y estándares específicos de proveedores/servicios. Las entidades de SNMP incluyen agentes y administradores. Los agentes son servicios administrados que preparan diversas MIB y hacen que los datos estén disponibles para los administradores. Los administradores pueden recuperar los datos desde los servicios administrados. Los servicios administrados también pueden enviar notificaciones a los administradores de manera asíncrona mediante un trap.

Existen tres versiones de SNMP que se usan de manera generalizada: versión 1, versión 2c y versión 3. La versión 3 incluye funciones de control de seguridad y acceso.

Para acceder a los parámetros de configuración del origen de eventos de SNMP:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **SNMP/Configuración** en el menú desplegable.



Características

La vista SNMP/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar tipos de orígenes de eventos de SNMP.

Característica	Descripción
	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros. **Nota:** Security Analytics solo es compatible con un único origen de eventos, que es snmptrap, y agrega snmptrap automáticamente cuando se agrega el tipo de origen de eventos.
	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.
	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de origen de evento disponibles

SNMP tiene un solo tipo de origen de eventos (categoría) llamado snmptrap. Una vez que agrega snmptrap al panel Categorías de evento, Security Analytics también genera un origen de eventos llamado snmptrap en el panel Orígenes. Solo se admite un único origen de eventos. No puede agregarlo ni eliminarlo. Solo se puede agregar o eliminar el tipo de origen de eventos (o categoría).

Característica	Descripción
	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

Panel Orígenes

Use este panel para analizar, agregar, modificar y eliminar los orígenes de eventos y sus parámetros para el tipo de origen de eventos que seleccionó en Orígenes de evento.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Opción	Descripción
	Abre el cuadro de diálogo Modificar origen, en el cual se modifican los parámetros de configuración del origen de eventos seleccionado. Cuando selecciona varios orígenes de eventos, se abre el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Después de guardar los cambios en el origen de eventos de SNMP, Security Analytics solicita reiniciar la recopilación de SNMP. Cuando reinicia la recopilación de SNMP, Security Analytics utiliza los valores de parámetro modificados.
	Selecciona el tipo de origen de eventos que desea editar.

Cuadro de diálogo Editar origen

En este cuadro de diálogo, se agrega o modifica un origen de eventos del origen de eventos seleccionado.

Característica	Descripción
Parámetros de origen de SNMP	Muestra los parámetros completados con los valores predeterminados. Ingrese o modifique los valores apropiados.
Cancelar	Cierra el cuadro de diálogo sin agregar un origen de eventos ni guardar los valores de los parámetros del origen de eventos seleccionado.
OK	En el cuadro de diálogo Agregar orígenes, agrega el origen de eventos y sus parámetros. En el cuadro de diálogo Modificar orígenes, aplica los cambios en los valores de los parámetros del origen de eventos seleccionado.

Parámetros de origen de SNMP

En la siguiente tabla se proporcionan descripciones de los parámetros del origen de SNMP.

Opción	Descripción
Básico	
Nombre *	El nombre del origen de SNMP (por ejemplo, snmptrap).
Puertos *	Los números de puerto UDP yUDP/IPv6. Un número de puerto válido es cualquier número dentro del rango de 1 a 65535. 162 es el puerto predeterminado. Puede ingresar varios puertos separando cada uno con una coma. Si cambia este parámetro, el cambio no se implementa hasta que reinicie la recopilación o el servicio de Log Collector.
Nivel de seguridad v3 mínimo	Nivel de seguridad mínimo requerido en los traps v3 recibidos. Los valores válidos son: • **noAuthNoPriv**: sin autenticación y sin privacidad. • **authNoPriv**: autenticación pero sin privacidad. Security Analytics omite cualquier trap con un nivel de seguridad de noAuthNoPriv. • **authPriv**: autenticación y privacidad. Security Analytics omite cualquier trap con un nivel de seguridad de noAuthNoPriv o authNoPriv.
Recopilación de traps v1	Seleccione la casilla de verificación para recopilar SNMP traps versión 1. La casilla de verificación está seleccionada de manera predeterminada. Si no selecciona este parámetro, Security Analytics omite los SNMP traps v1.
Recopilar traps v2c	Seleccione la casilla de verificación para recopilar SNMP traps versión 2c. La casilla de verificación está seleccionada de manera predeterminada. Si no selecciona este parámetro, Security Analytics omite los SNMP traps v2c.
Recopilar traps v3	Seleccione la casilla de verificación para recopilar SNMP traps versión 3. La casilla de verificación está seleccionada de manera predeterminada. Si no selecciona este parámetro, Security Analytics omite los SNMP traps v3.

Activado	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
Cadenas de comunidad	Lista de cadenas de comunidad separadas por coma. De manera predeterminada, este parámetro no contiene valores. • **sin valores especificados**: Security Analytics recopila todos los SNMP traps. • **valores especificados**: Si la cadena de comunidad del trap recibido no está en la lista especificada, Security Analytics omite el trap.
Avanzado	
Número máximo de receptores	Número máximo de recursos de receptores dentro del rango de 1 a 50. El valor predeterminado es condicional según el tipo (categoría) de SNMP y usa 2 de manera predeterminada para el tipo snmp. Si cambia este parámetro, el cambio no se implementa hasta que reinicie la recopilación o el servicio de Log Collector.
Umbral de registro de publicación en transferencia	El valor de umbral en los eventos publicados en los cuales Security Analytics crea un mensaje informativo. Los valores válidos son: • **0** = desactivar el mensaje • **100-100000000** = umbral de evento publicado

Depurar	**Precaución:** Active la depuración (defina este parámetro en "Activado" o "Detallado") solamente si tiene un problema con un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa/desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar).

Tareas

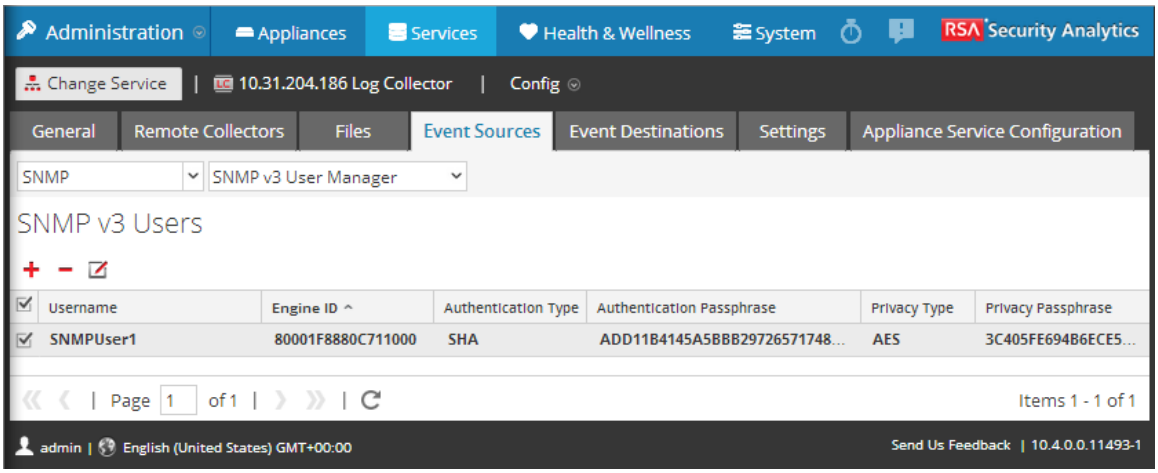
Paso 1. Configurar orígenes de eventos de SNMP en Security Analytics

Parámetros de configuración del administrador de usuarios de SNMP v3

En este tema, se describen los parámetros de configuración del administrador de usuarios de SNMP v3.

Para acceder a los parámetros de configuración del administrador de usuarios de SNMP v3:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en ⚙ bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Administrador de usuarios de SNMP/SNMP v3** en el menú desplegable.



La vista Administrador de usuarios de SNMP/SNMP v3 de la pestaña Orígenes de evento tiene un panel: Usuarios de SNMP v3.

Usuarios de SNMP v3

En el panel Usuarios de SNMP v3, puede agregar, eliminar o editar usuarios de SNMP v3.

Característica	Descripción
+	Muestra el cuadro de diálogo Agregar SNMP, donde define los parámetros de un usuario de SNMP v3.
−	Elimina los usuarios de SNMP v3 seleccionados.
✎	Muestra el cuadro de diálogo Editar SNMP, donde edita los parámetros de un usuario de SNMP v3. Después de guardar los cambios en la configuración de usuario de SNMP, Security Analytics solicita reiniciar la recopilación de SNMP. Cuando reinicia la recopilación de SNMP, Security Analytics utiliza los valores de parámetro modificados.
☐	Selecciona usuarios de SNMP v3.

Característica	Descripción
Parámetros de usuario de SNMP v3	Muestra a cada usuario de SNMP v3 que ha agregado con sus parámetros.

Cuadro de diálogo Agregar/Editar usuario de SNMP

En este cuadro de diálogo, puede agregar o modificar los parámetros de usuario de SNMP v3.

Característica	Descripción
Nombre de usuario*	Nombre de usuario (o, más precisamente, en terminología de SNMP, nombre de seguridad). Security Analytics usa este parámetro y el parámetro de ID del motor para crear una entrada de usuario en el motor de SNMP del servicio de recopilación. La combinación de Nombre de usuario e ID del motor debe ser única (por ejemplo, **logcollector**).
ID del motor	(Opcional) ID del motor del origen de eventos. Para todos los orígenes de eventos que envían SNMP v3 traps a este servicio de recopilación, debe agregar el nombre de usuario e ID del motor del origen de eventos remitente. Para todos los orígenes de eventos que envían informes de SNMPv3, debe agregar solo el nombre de usuario con un ID del motor en blanco. Por ejemplo, **Nombre de usuario = logcollector** e **ID del motor = 80001F8880C7110000410449510000**.
Tipo de autenticación	(Opcional) Protocolo de autenticación. Los valores válidos son: • **Ninguno (valor predeterminado)**: Solamente el nivel de seguridad de noAuthNoPriv puede usarse para traps que se envían a este servicio • **SHA**: algoritmo hash seguro • **MD5:** algoritmo de recopilación de mensaje
Frase de contraseña de autenticación	Opcional si no tiene el Tipo de autenticación definido. Frase de contraseña de autenticación.

Característica	Descripción
Tipo de privacidad	(Opcional) Protocolo de privacidad. Solo puede configurar este parámetro si el parámetro Tipo de autenticación está configurado. Los valores válidos son: • **Ninguno (valor predeterminado)** • **AES:** Advanced Encryption Standard (Estándar de cifrado avanzado) • **DES:** Data Encryption Standard (Estándar de cifrado de datos)
Privacy Passphrase	Opcional si no tiene el Tipo de privacidad definido. Frase de contraseña de privacidad
Cerrar	Cierra el cuadro de diálogo sin agregar el usuario de SNMP v3ni guardar las modificaciones en los parámetros.
Guardar	Agrega los parámetros de usuario de SNMP v3 o guarda las modificaciones de los parámetros.

Tareas

Configurar usuarios de SNMP v3

Solucionar problemas de la recopilación de SNMP

En este tema se señalan posibles problemas que puede encontrar en la recopilación de SNMP y las soluciones que se sugieren para ellos.

Solucionar problemas de la recopilación de SNMP

Para recuperar eventos de SNMP, debe configurar los parámetros para que verifiquen y descifren SNMPv3 traps y mensajes de informes desde los orígenes de eventos.

- Para mensajes de informes, debe especificar el usuario (nombre de seguridad, en la terminología de SNMPv3) sin un ID de motor.
- Para mensajes de trap, debe especificar el usuario con el ID de motor del remitente del evento.

Debe establecer el parámetro Depurar en **Detallado** para recuperar mensajes no válidos de trap y de registros de informes.

Security Analytics devuelve los siguientes tipos de mensajes de error en los archivos de registro para el protocolo de recopilación de SNMP.

Mensajes de registro	(d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmpv3_parse: (d) 2013-May-02 13:43:38 [SnmpTrapCollection (TraceLog)] Net-SNMP: msgMaxSize 65507 received (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing begun... (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Unknown Engine ID. (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing has begun (offset 55) (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: getting user (d) 2013-May-02 13:43:38 [SnmpTrapCollection (TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing completed. (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmpv3_parse: (d) 2013-May-02 13:43:38 [SnmpTrapCollection (TraceLog)] Net-SNMP: msgMaxSize 65507 received (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing begun... (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Unknown User(logcollector) (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing has begun (offset 55) (d) 2013-May-02 13:43:38 [SnmpTrapCollection (TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: getting user logcollector (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing completed.
Causa posible	Falta el nombre de usuario o el ID de motor para SNMP trap
Soluciones	Asegúrese de que el origen de eventos envíe el nombre de usuario y el ID de motor que configuró para el origen de eventos en los Parámetros de configuración del administrador de usuarios de SNMP v3.

Mensajes de registro	(d) 2013-May-02 16:47:26 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmptrapd: (d) 2013-May-02 16:47:26 [SnmpTrapCollection(TraceLog)] Net-SNMP: Running global handlers (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmpv3_parse: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: msgMaxSize 65507 received (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing begun... (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: match on user logcollector (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Verification succeeded. (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing completed. (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmp_parse: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Parsed SNMPv3 message (secName:logcollector, secLevel:authPriv): ASN.1 parse error in message
Causa posible	El tipo de autenticación o la contraseña utilizada por el origen de eventos fueron distintos de los valores que configuró.
Soluciones	Asegúrese de que el tipo de autenticación y la frase de contraseña de autenticación que envió el origen de eventos coincidan con los parámetros que configuró para el origen de eventos en los Parámetros de configuración del administrador de usuarios de SNMP v3.

Guía de configuración de la recopilación de VMware

En esta guía se indica cómo configurar el protocolo de recopilación de VMware. Este protocolo recopila eventos de una infraestructura virtual de VMware.

Debe implementar Log Collection antes de poder configurar el protocolo de recopilación de punto de comprobación.

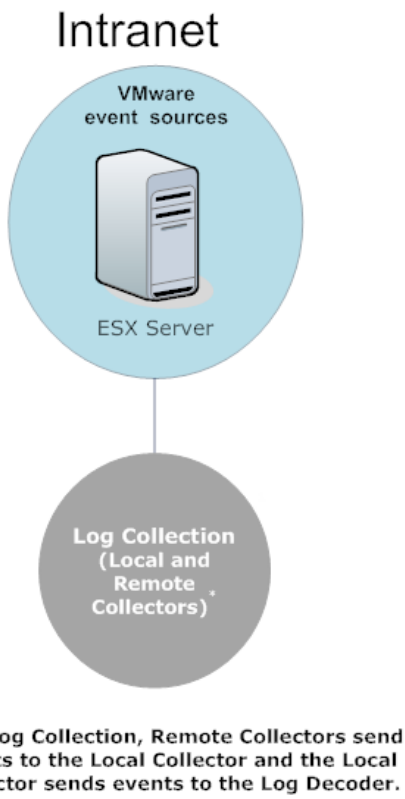
Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Conceptos básicos

En esta guía se indica cómo configurar el protocolo de recopilación de VMware, el cual recopila eventos de una infraestructura virtual de VMware.

Escenario de implementación

En la siguiente figura se ilustra cómo implementar el protocolo de recopilación de VMware en Security Analytics.



Procedimientos

Configurar el protocolo de recopilación de VMware en Security Analytics

Debe configurar el Log Collector para usar la recopilación de VMware para un origen de eventos en la pestaña Origen de evento de la vista de parámetros de Log Collector. En el siguiente procedimiento se explica el flujo de trabajo básico para configurar un origen de eventos para la recopilación de VMware en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de VMware en Security Analytics para obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de VMware.
- Referencias: Parámetros de configuración del origen de eventos de VMware para obtener una descripción detallada de cada parámetro del protocolo de recopilación de VMware.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio de recopilación de registros.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
   Se muestra la vista **Configuración de Log Collector**.

4. Haga clic en la pestaña **Orígenes de evento**.
5. Seleccione **VMware** como el protocolo de recopilación y elija **Configurar**.
6. Haga clic en  y seleccione el nombre de la categoría del origen de eventos (por ejemplo, **vmware-events**). La categoría de origen de eventos es parte del contenido que descargó de LIVE.
7. Seleccione una categoría y haga clic en en la barra de herramientas del panel **Orígenes**.
8. Especifique los parámetros básicos requeridos para el origen de eventos de VMware.
9. Haga clic en  y especifique parámetros adicionales que mejoran la manera en que el protocolo de VMware maneja la recopilación de eventos para el origen de eventos.

Configurar orígenes de eventos de modo que usen el protocolo de recopilación de VMware

Debe configurar cada origen de eventos que usa el protocolo de recopilación de VMware para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de VMware para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de VMware, con una lista de verificación que contiene cada paso de configuración.

Los pasos de configuración del protocolo de recopilación de VMware deben realizarse en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de la configuración de la recopilación de VMware

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de VMware en Security Analytics.	

Paso	Descripción	√
2	Configurar orígenes de eventos de VMware para enviar eventos a Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de VMware configurado.	
4	Verificar que la recopilación de VMware esté funcionando.	

Paso 1. Configurar orígenes de eventos de VMware en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de VMware para el Log Collector.

Después de realizar este procedimiento, habrá...

- Configurado un origen de eventos de VMware.
- Modificado un origen de eventos de VMware.

Volver a Procedimientos

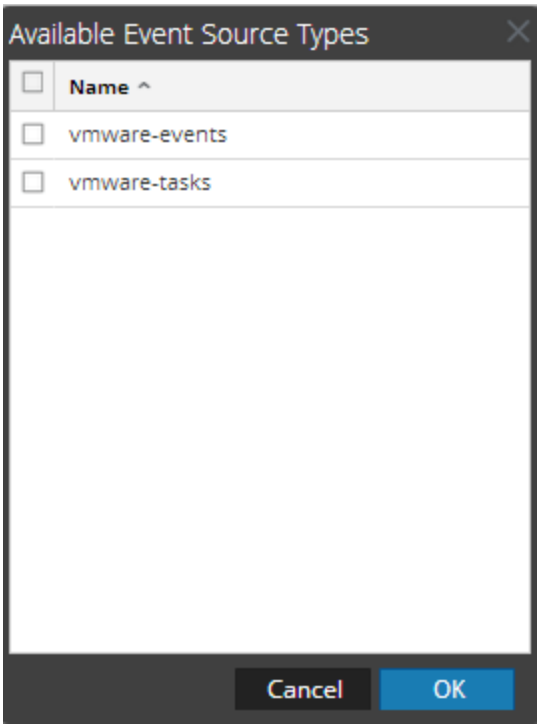
Procedimientos

Configurar un origen de eventos de VMware

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **VMware/Configuración** en el menú desplegable.

En el panel **Categorías de evento** se muestran los orígenes de eventos de VMware que están configurados, si los hay.

5. En la barra de herramientas del panel **Categorías de evento**, haga clic en  .

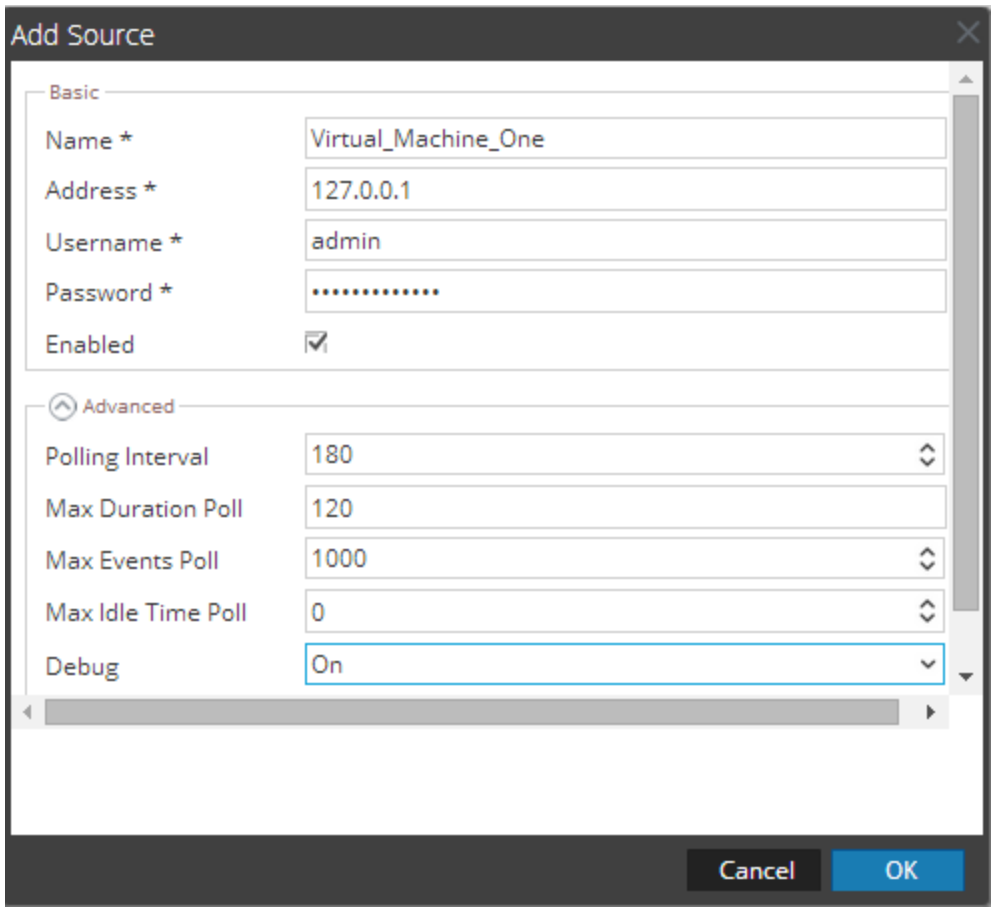


El tipo de origen de eventos recién agregado se muestra en el panel **Categorías de evento**.

6. Seleccione el nuevo tipo en el panel **Categorías de evento** y haga clic en  en la barra de herramientas **Orígenes**.
Se muestra el cuadro de diálogo **Agregar origen**.

7. Agregue un **nombre**, un **nombre de usuario** y una **contraseña**, modifique cualquier otro parámetro que requiera cambios y haga clic en **Aceptar**.

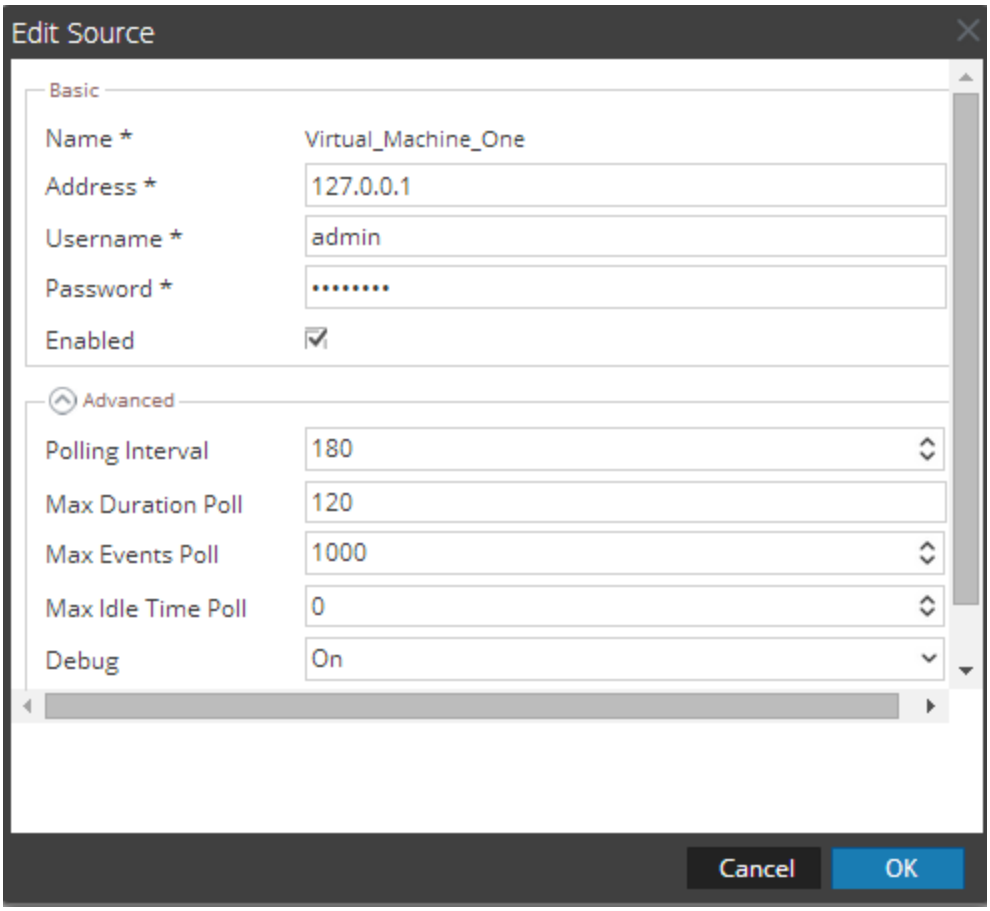
Precaución: Si debe ingresar el nombre de dominio como parte del Nombre de usuario, debe utilizar dos barras invertidas como separador. Por ejemplo, si el dominio|nombre de usuario es corp\smithj, debe especificar corp\\smithj.



El nuevo origen de eventos se muestra en la lista.

Modificar un origen de eventos de VMware

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
4. Seleccione **VMware/Configuración** en el menú desplegable.
5. En la lista **Origen de evento**, seleccione un origen de eventos y haga clic en .
   Se muestra el cuadro de diálogo **Editar origen**.



6. Modifique los parámetros que necesiten cambios y haga clic en **Aceptar**.
   Security Analytics aplica los cambios de parámetros al origen de eventos seleccionado.

Parámetros

Referencias: Parámetros de configuración del origen de eventos de VMware

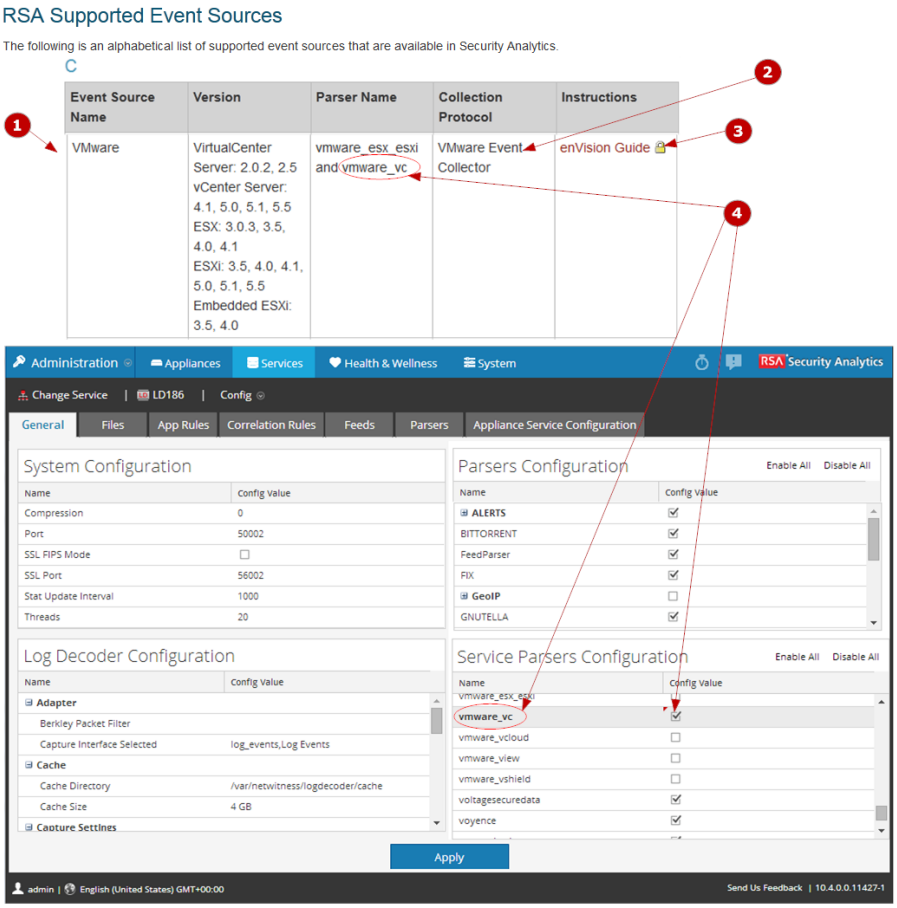
Paso 2. Configurar orígenes de eventos de VMware para enviar eventos a Security Analytics

En este tema se indica dónde encontrar los orígenes de eventos que son compatibles actualmente con la recopilación de VMware y las instrucciones de configuración disponibles para cada origen de eventos.

Lista de orígenes de eventos compatibles

Volver a Procedimientos

La lista de orígenes de eventos compatibles de RSA es una lista alfabética de todos los orígenes de eventos que son compatibles actualmente con Security Analytics, la cual identifica los orígenes de eventos que puede usar con la recopilación de VMware.



1 Busque el nombre del origen de eventos.

2 Verifique que sea compatible con el protocolo de recopilación de VMware.

3 Haga clic en para recuperar las instrucciones de configuración del origen de eventos.

4 Verifique que haya descargado el analizador de origen de eventos correcto (por ejemplo, **vmare_vc**) desde LIVE a Log Decoder y que lo haya habilitado.

Ejemplo de instrucciones de configuración

La siguiente ilustración se toma de las instrucciones de configuración de VMware Collector Service.


RSA enVision VMware Collector Service Installation and Configuration Guide

RSA
The Security Division of EMC

1

RSA enVision VMware Collector Service Overview

- About RSA enVision VMware Collector Service
- Using RSA enVision VMware Collector Service to Collect Events
- Deployment Model

About RSA enVision VMware Collector Service

You can use RSA enVision VMware Collector Service to collect events generated from a VMware virtual infrastructure.

A VMware infrastructure typically consists of multiple VMware VirtualCenter Servers that connect to several ESX, ESXi, and embedded ESXi servers. Each of these servers generates tasks and events, which are collected and managed by the VMware VirtualCenter Server. For information about the VMware infrastructure, see the product documentation.

Note: The term VirtualCenter refers to all VMware management console products such as vCenter Server.

VMware Collector Service retrieves the events from the VMware VirtualCenter Server and stores the events in the Internet Protocol Database (IPDB).

Paso 3. Iniciar el servicio para el protocolo de recopilación de VMware configurado

En este tema se indica cómo iniciar un servicio de recopilación de VMware detenido.

Si un servicio de recopilación de VMware se detuvo, tendrá que iniciarlo nuevamente para que funcione. También puede consultar el tema Habilitar el inicio automático de servicios individuales de la Guía de configuración de la recopilación de registros si desea que el servicio se inicie automáticamente.

Procedimiento

Para iniciar un servicio de recopilación:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. Seleccione un servicio Log Collector y, en la columna **Acciones**, haga clic en > **Ver** > **Sistema**.
   Se muestra la vista **Sistema de servicios**.

3. En la barra de herramientas, haga clic en **Recopilación > VMware** y, a continuación, haga clic en **Iniciar**.

Paso 4. Verificar que la recopilación de VMware esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de VMware se configuró correctamente.

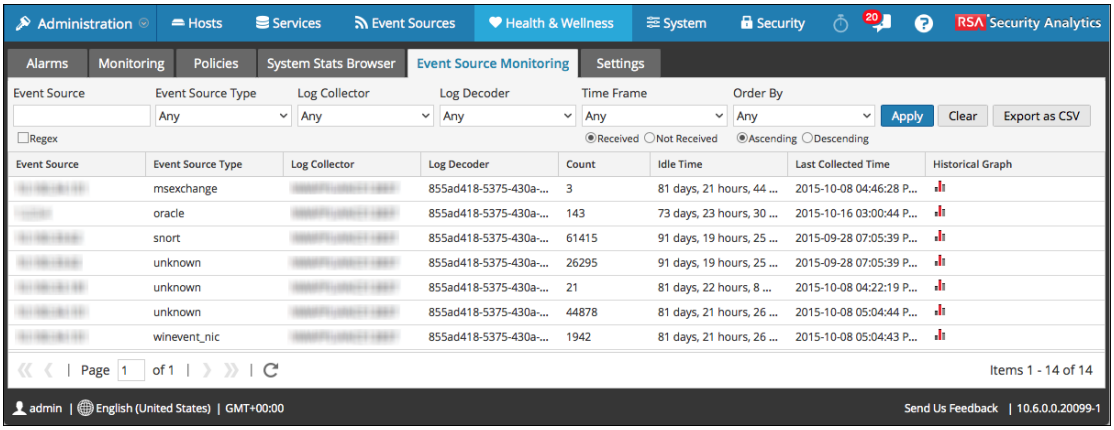
Si la recopilación de VMware no se configura correctamente, no funcionará. Puede verificar su funcionamiento en la vista Estado y condición.

Procedimiento

Volver a Procedimientos

Para verificar que la recopilación de VMware esté funcionando:

1. En el menú de **Security Analytics**, seleccione **Administration > Estado y condición.** La vista **Estado y condición** se muestra con la pestaña **Alarmas** abierta.
2. Haga clic en la pestaña **Monitoreo de orígenes de eventos**.



3. Busque un origen de eventos de VMware (por ejemplo, **vmware_vc**) en la columna **Tipo de origen de evento**.
4. Busque actividad en la columna **Conteo** para verificar que la recopilación de VMware esté aceptando eventos.

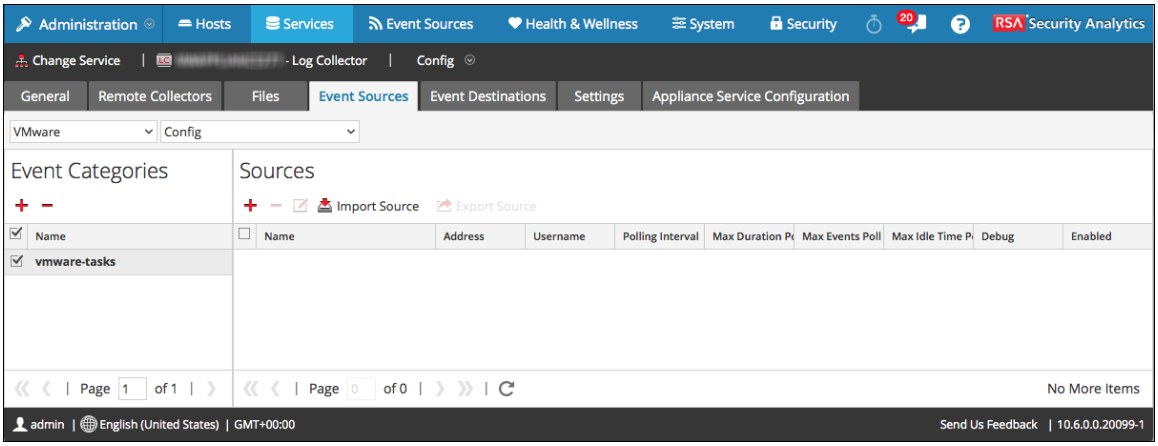
Referencias: Parámetros de configuración del origen de eventos de VMware

Este tema describe los parámetros de origen evento de VMware.

Puede usar la opción de VMware que aparece en la pestaña Ver orígenes de eventos en la Configuración de Log Collector para agregar y mantener parámetros de configuración de los orígenes de eventos de VMware. Estos orígenes de eventos generan eventos desde una infraestructura virtual de VMware. La infraestructura consta generalmente de múltiples servidores de VMware vCenter que se conectan a diversos servidores ESX Server, servidores ESXi Server y servidores ESXi Server incorporados. Cada uno de los servidores de vCenter recopila y administra tareas y eventos. Los eventos pueden ser cualquier mensaje generado por un origen de eventos de VMware (por ejemplo, una alarma). Las tareas son trabajos cuya ejecución se calendariza.

Para acceder a los parámetros de configuración del origen de eventos de VMware:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio Log Collector.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración**.
   La vista **Configuración del servicio** se muestra con la pestaña **General** abierta.
4. Haga clic en la pestaña **Orígenes de evento**.
5. Seleccione VMware en el menú desplegable.



La vista VMware de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

En el panel Categorías de evento, puede agregar o eliminar los tipos de orígenes de eventos correspondientes.

Característica	Descripción
	Muestra el cuadro de diálogo Tipos de origen de evento disponibles en el cual se selecciona el tipo de origen para el cual desea definir parámetros.
	Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.
	Selecciona los tipos de orígenes de eventos.
Nombre	Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Cuadro de diálogo Tipos de orígenes de eventos disponibles

El cuadro de diálogo Tipos de origen de evento disponibles muestra la lista de tipos de orígenes de eventos compatibles.

Característica	Descripción
	Selecciona el tipo de origen de eventos que desea agregar.
Tipo	Muestra los tipos de orígenes de eventos disponibles para agregar.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega el tipo de origen de eventos seleccionado al panel Categorías de evento.

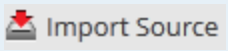
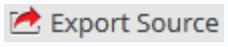
Panel Orígenes

Use este panel para revisar, agregar, modificar y eliminar orígenes de eventos y sus parámetros para el tipo de origen de eventos que seleccionó en el panel Categorías de evento.

Precaución: Para la recopilación de eventos de VMware, Security Analytics extrae todos los eventos existentes actualmente la primera vez que comienza a recopilar eventos de VMware.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar origen, en el cual puede definir los parámetros para un host de firewall.
	Elimina el host que seleccionó.
	Abre el cuadro de diálogo Editar origen, en el cual puede editar los parámetros del origen de eventos seleccionado. Seleccione varios orígenes de eventos y haga clic en  para abrir el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar hosts de forma masiva desde un archivo de valores separados por comas (CSV). Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo .csv que contiene los parámetros de los hosts seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.

Cuadro de diálogo Agregar/Modificar orígenes

En este cuadro de diálogo, se agrega o modifica un origen de eventos del origen de eventos seleccionado.

Característica	Descripción
Parámetros de origen	Muestra los parámetros completados con los valores predeterminados. Ingrese o modifique los valores apropiados.
Cancelar	Cierra el cuadro de diálogo sin agregar un origen de eventos ni guardar los valores de los parámetros del origen de eventos seleccionado.

Característica	Descripción
OK	En el cuadro de diálogo **Agregar orígenes**, agrega el origen de eventos y sus parámetros. En el cuadro de diálogo **Modificar orígenes**, aplica los cambios en los valores de los parámetros del origen de eventos seleccionado.

Parámetros de origen

En la siguiente tabla se proporcionan descripciones de los parámetros del origen.

Nombre	Descripción
	Básico
Nombre *	Nombre del servidor donde se ejecuta VMware.
Dirección *	Dirección IP del servidor de VMware (127.0.0.1 es el valor predeterminado).
Nombre de usuario*	Nombre de usuario que usa el Log Collector para conectarse al servidor de VMware. Debe especificar el nombre de usuario cuando cree el origen de eventos. **Precaución:** Si debe ingresar el nombre de dominio como parte del Nombre de usuario, debe utilizar una barra invertida como separador. Por ejemplo, si el **dominio\nombre de usuario** es **corp\smithj**, debe especificar **corp\\smithj**.
Contraseña *	Contraseña que usa el Log Collector para conectarse al servidor de VMware. **Precaución:** La contraseña se cifra internamente y se muestra en su forma cifrada.
Activado	Seleccione la casilla de verificación para activar la configuración del origen de eventos con el fin de iniciar la recopilación. La casilla de verificación está seleccionada de manera predeterminada.
	Avanzado

Intervalo de sondeo	El intervalo (cantidad de tiempo en segundos) entre cada encuesta. El valor predeterminado es **180**. Por ejemplo, si especifica **180**, el recopilador programa un sondeo del origen de eventos cada **180** segundos. Si aún se está realizando el ciclo de sondeo anterior, el recopilador espera a que ese ciclo termine. Si está sondeando una gran cantidad de orígenes de eventos, es posible que el sondeo tarde más de **180** segundos en comenzar porque los subprocesos están ocupados.
Duración máxima de encuesta	La duración máxima del ciclo de sondeo (cuánto tiempo dura el ciclo) en segundos.
Tiempo máximo de inactividad de encuesta	Tiempo de inactividad máximo, en segundos, de un ciclo de sondeo. **0** indica que no hay límite. **300** es el valor predeterminado.
Máximo de eventos de encuesta	La cantidad máxima de eventos por ciclo de sondeo (cuántos eventos se recopilan por ciclo de sondeo).

Depurar	**Precaución:** Active la depuración (defina este parámetro en "Activado" o "Detallado") solamente si tiene un problema con un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa o desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar). El registro de depuración es detallado, por lo que se debe limitar la cantidad de orígenes de eventos para minimizar el impacto en el rendimiento.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
OK	Agrega los parámetros del origen de eventos.

Tareas

Paso 2. Configurar orígenes de eventos de VMware para enviar eventos a Security Analytics

Solucionar problemas de la recopilación de VMware

En este tema se sugiere cómo resolver los problemas que puede en el protocolo de recopilación de VMware.

Security Analytics le informa sobre problemas o posibles problemas de Log Collector de las dos maneras siguientes:

- Archivos de registro.
- Vista Monitoreo de Estado y condición

Archivos de registro

Si un protocolo de recopilación de orígenes de eventos específico presenta problemas, puede revisar los registros de depuración para investigarlos. Cada origen de eventos posee un parámetro de Depuración que puede activar (configurar en Activado o Detallado) para capturar estos registros.

Active la depuración solamente si este origen de eventos presenta problemas y necesita investigarlos. Si activa la depuración en todo momento, esta afectará negativamente al rendimiento de Log Collector.

Security Analytics tiene un conjunto de mensajes de error asociados con la recopilación de registros que incluye en archivos de registro. Para acceder a estos archivos:

Monitoreo del estado y la condición

El monitoreo del estado y la condición le permite informarse oportunamente de posibles problemas de hardware y software de modo que pueda evitar interrupciones. RSA recomienda monitorear los campos estadísticos de Log Collector para asegurarse de que el servicio funcione de manera eficiente y que no se encuentre en los valores máximos configurados ni cerca de estos. Puede monitorear las estadísticas que se describen en la vista **Administration > Estado y condición**.

Guía de configuración de la recopilación de Windows

Esta guía le indica cómo configurar el protocolo de recopilación de Windows. Este protocolo recopila los eventos de los equipos de Windows que son compatibles con el modelo de Microsoft Windows.

Debe implementar Log Collection antes de poder configurar el protocolo de recopilación de Windows.

Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Conceptos básicos

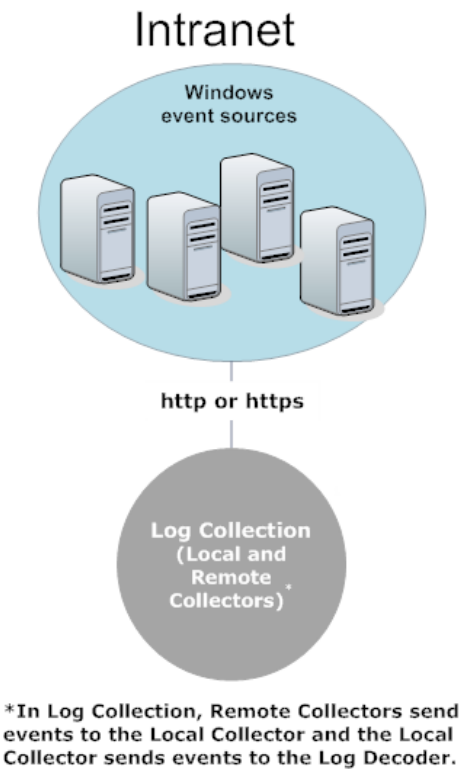
En esta guía se indica cómo configurar el protocolo de recopilación de Windows que recopila eventos de máquinas con Windows que son compatibles con el modelo de Microsoft Windows. Windows 6.0 es una plataforma de rastreo y registro de eventos que se incluye en el sistema operativo a partir de Microsoft Windows Vista y Windows Server 2008.

Cómo funciona la recopilación de Windows

El servicio Log Collector recopila eventos de orígenes de eventos de Microsoft Windows.

Escenario de implementación

En la siguiente figura se ilustra cómo implementar el protocolo de recopilación de Windows en Security Analytics.



Procedimientos

Configurar el protocolo de recopilación de Windows en Security Analytics

Debe configurar el Log Collector para usar la recopilación de Windows para un origen de eventos en la pestaña Origen de evento de la vista de parámetros de Log Collector. En el siguiente procedimiento se explica el flujo de trabajo básico para configurar un origen de eventos para la recopilación de Windows en Security Analytics. Consulte:

- Paso 1. Configurar orígenes de eventos de Windows en Security Analyticspara obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de Windows.
- Parámetros de configuración del origen de eventos de Windows para obtener una descripción detallada de cada parámetro del protocolo de recopilación de Windows.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. Seleccione un servicio de **recopilación de registros**.
3. Haga clic en > Ver > **Configurar**.
   Se muestran las pestañas de parámetros de configuración de la recopilación de registros.

4. Haga clic en la pestaña **Orígenes de evento**.
5. Seleccione **Windows** como el protocolo de recopilación y elija **Configurar**.
6. Haga clic en  y defina un alias de Windows (**Agregar origen**).
7. Seleccione el alias y haga clic en  .
8. Defina un host de Windows.
9. Haga clic en **Probar conexión** para validar la conexión con el origen de eventos de Windows.

Configurar los orígenes de eventos para usar el protocolo de recopilación de Windows

Debe configurar cada origen de eventos que usa el protocolo de recopilación de Windows para que se comunique con Security Analytics (consulte Paso 2. Configurar orígenes de eventos de Windows para enviar eventos a Security Analytics).

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de Windows, con una lista de verificación que contiene cada paso de configuración.

Los pasos de configuración del protocolo de recopilación de Windows deben realizarse en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de configuración de la recopilación de Windows

Nota: los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar orígenes de eventos de Windows en Security Analytics.	

Paso	Descripción	√
2	Configurar orígenes de eventos de Windows para enviar eventos a Security Analytics.	
3	Iniciar el servicio para el protocolo de recopilación de Windows configurado.	
4	Verificar que la recopilación de Windows esté funcionando.	

Paso 1. Configurar orígenes de eventos de Windows en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de Windows para el Log Collector.

Después de realizar este procedimiento, habrá:

- Configurado un origen de eventos de Windows.
- Modificado un origen de eventos de Windows.
- Determinado el nombre del canal y agregado este al origen de eventos de Windows.

Volver a Procedimientos

Procedimientos

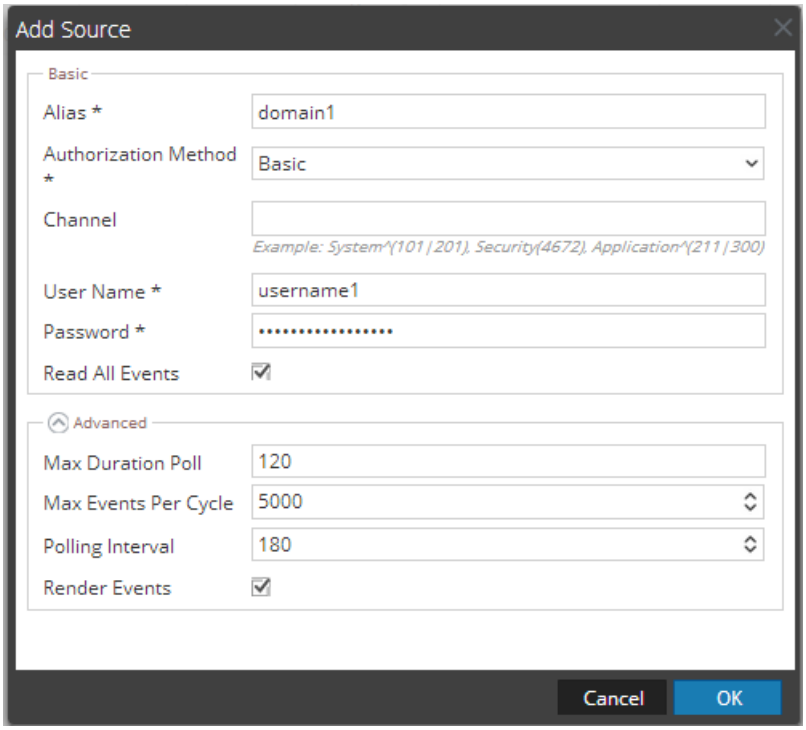
Configurar un origen de eventos de Windows

Agregar un origen de eventos de Windows

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Windows/Configuración** en el menú desplegable.
   Se muestra el panel **Categorías de evento** con los orígenes de eventos de Windows que están configurados, si los hay.

Configurar un origen de eventos (alias)

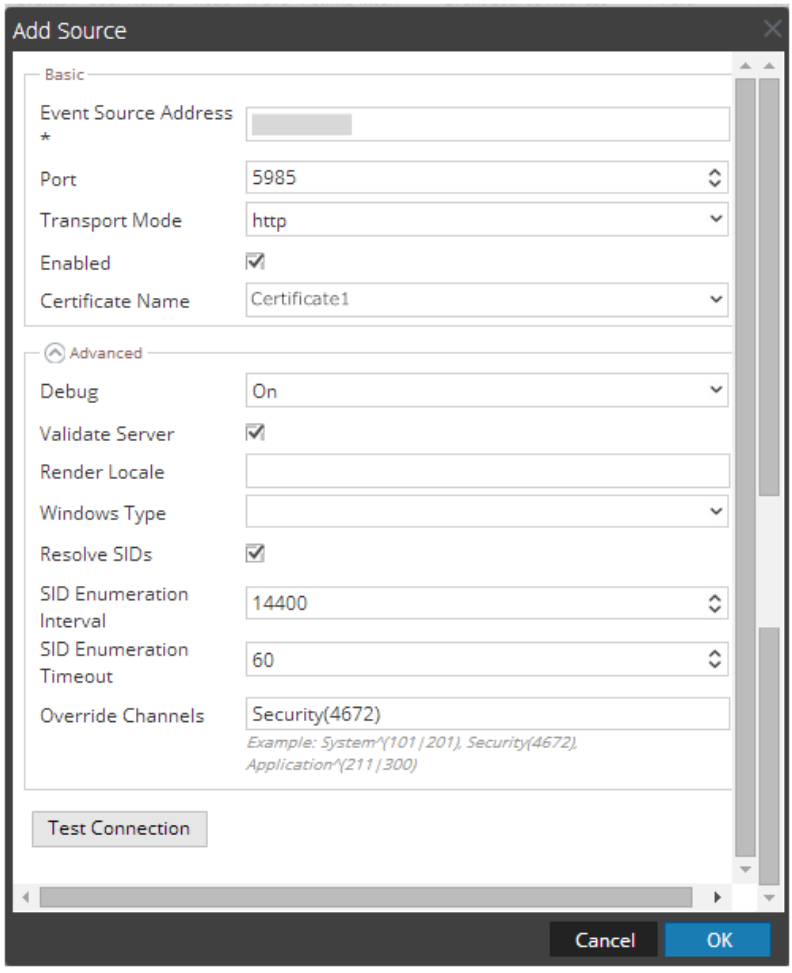
1. Haga clic en  en la barra de herramientas del panel **Categorías de evento**.
   Se muestra el cuadro de diálogo **Agregar origen de evento**.
2. Especifique valores para los parámetros y haga clic en **Aceptar**.



El origen de eventos de Windows recién agregado se muestra en el panel **Categorías de evento**.

Agregar host de origen de eventos

1. Seleccione el nuevo origen de eventos (alias) en el panel **Categorías de evento**.
   El panel **Hosts** está activado.
2. Haga clic en + en la barra de herramientas del panel **Hosts**.
   Se muestra el cuadro de diálogo **Agregar origen**.
3. Especifique los valores para los parámetros de **Host**.



4. Haga clic en **Probar conexión**.
   El resultado de la prueba se muestra en el cuadro de diálogo. Si el resultado de la prueba no fue satisfactorio, edite la información del dispositivo o del servicio e inténtelo nuevamente.

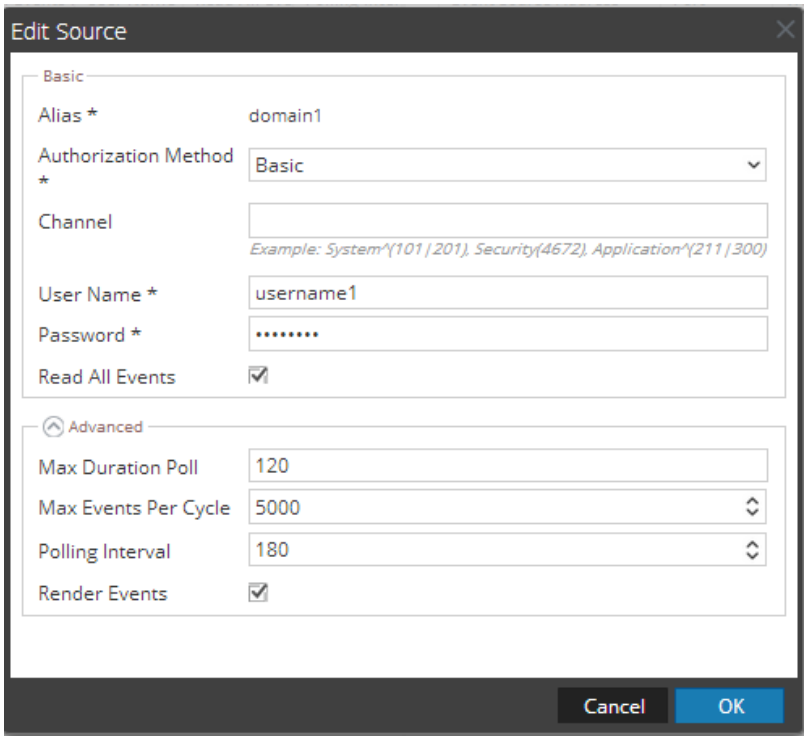
Nota: Log Collector tarda aproximadamente 60 segundos en devolver los resultados de la prueba. Si se excede el límite de tiempo, se agota el tiempo de espera de la prueba y Security Analytics muestra un mensaje de error.

5. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**. El host agregado recientemente se muestra en el panel **Hosts**.

Modificar un origen de eventos de Windows

Para modificar un origen de eventos de Windows:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver > Configuración.**
4. En la pestaña **Orígenes de evento**, seleccione **Windows/Configuración** en el menú desplegable.
5. Modifique los parámetros de origen.
   a. En el panel **Categorías de evento**, seleccione un origen y haga clic en .
      Se muestra el cuadro de diálogo **Editar origen**.
   b. Modifique los parámetros de origen que necesiten cambios y haga clic en **Aceptar**.



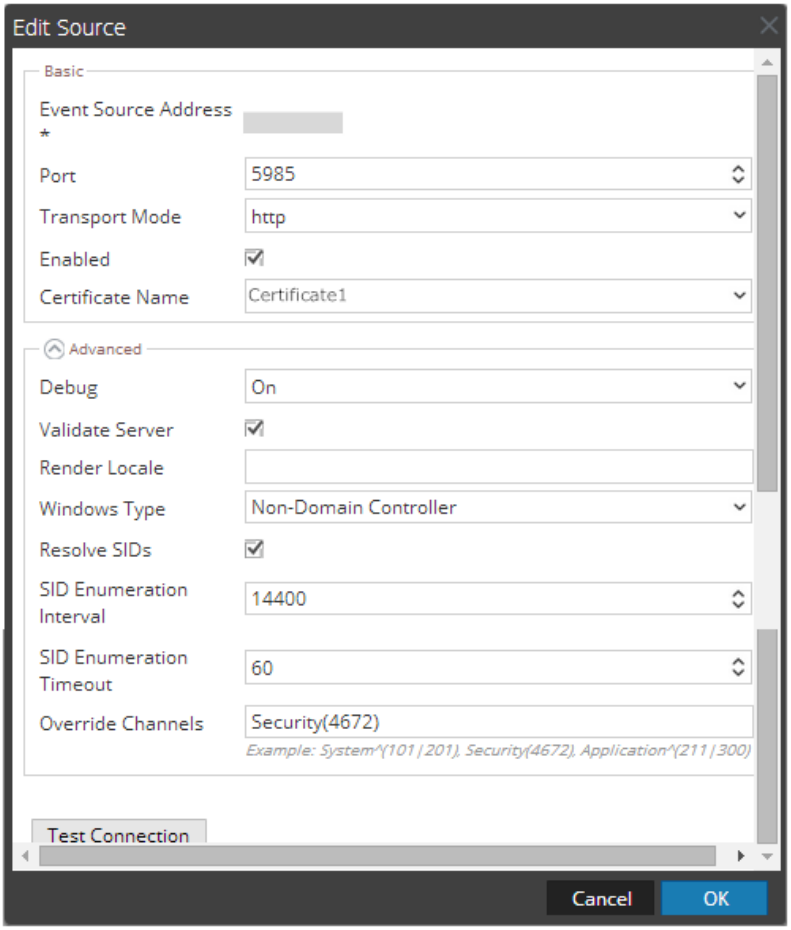
Security Analytics aplica los cambios de parámetros al origen seleccionado.

6. Modificar el host de origen de eventos:

   a. En el panel **Hosts**, seleccione un host y haga clic en  .

      Se muestra el cuadro de diálogo **Editar origen**.

   b. Modifique los parámetros de host que necesiten cambios y haga clic en **Aceptar**.

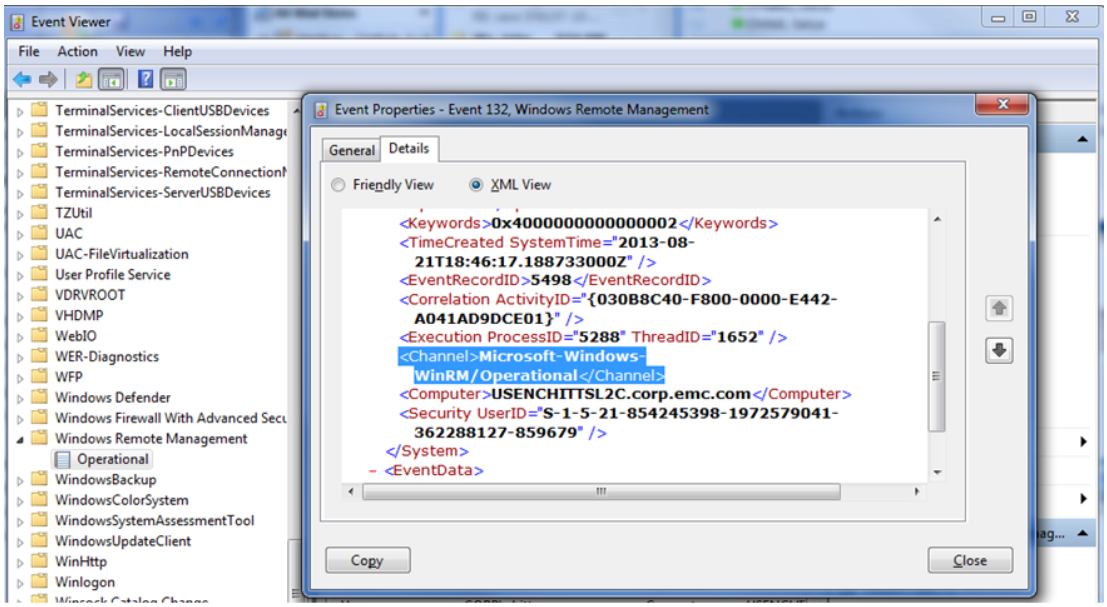


   Security Analytics aplica los cambios de parámetros al host seleccionado.

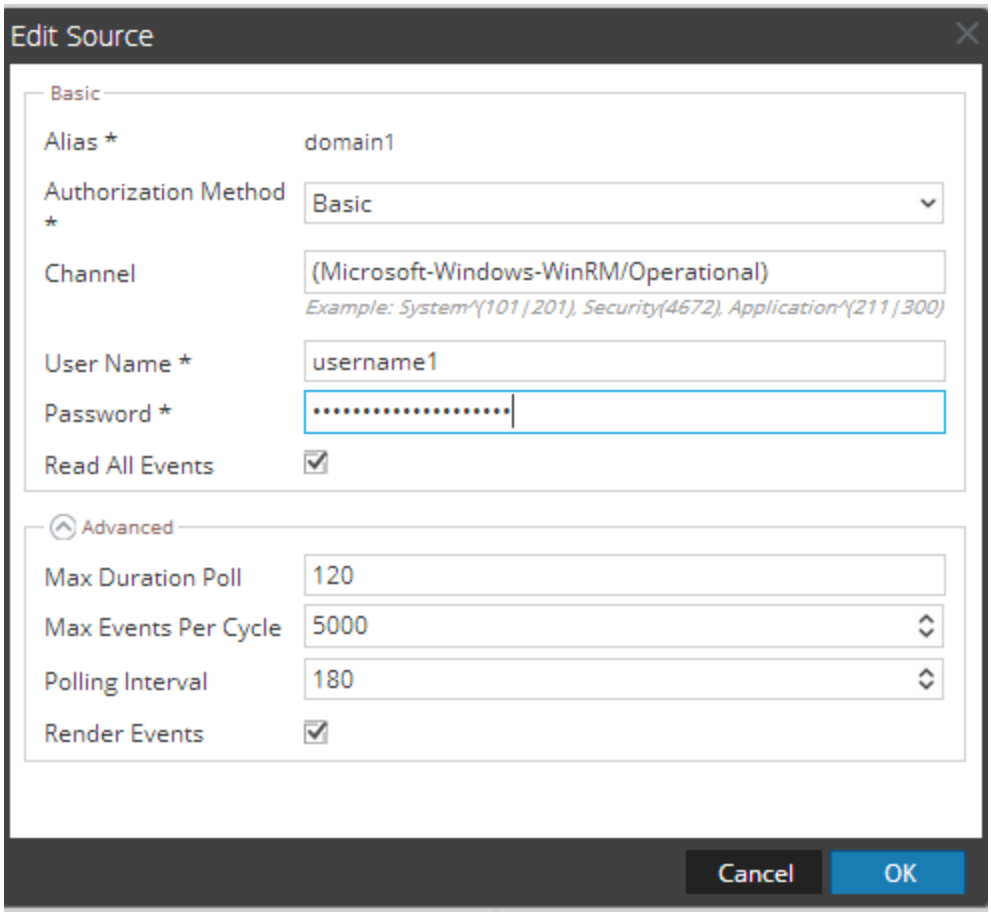
Determinar el nombre del canal y agregarlo al origen de eventos de Windows

Para buscar un nombre del canal desconocido y agregarlo al origen de eventos de Windows, haga lo siguiente:

1. Seleccione el canal que desea en el origen de eventos de Windows.
2. Haga clic en la pestaña **Detalles** y busque el campo del canal que sea el nombre del canal (por ejemplo, **Microsoft-Windows-WinRM/Operational**).



3. Edite el origen de eventos en Security Analytics, agregue el canal al parámetro **Canal** y haga clic en **Aceptar**. Por ejemplo:



Parámetros

Parámetros de configuración del origen de eventos de Windows

Configurar un dominio de Kerberos

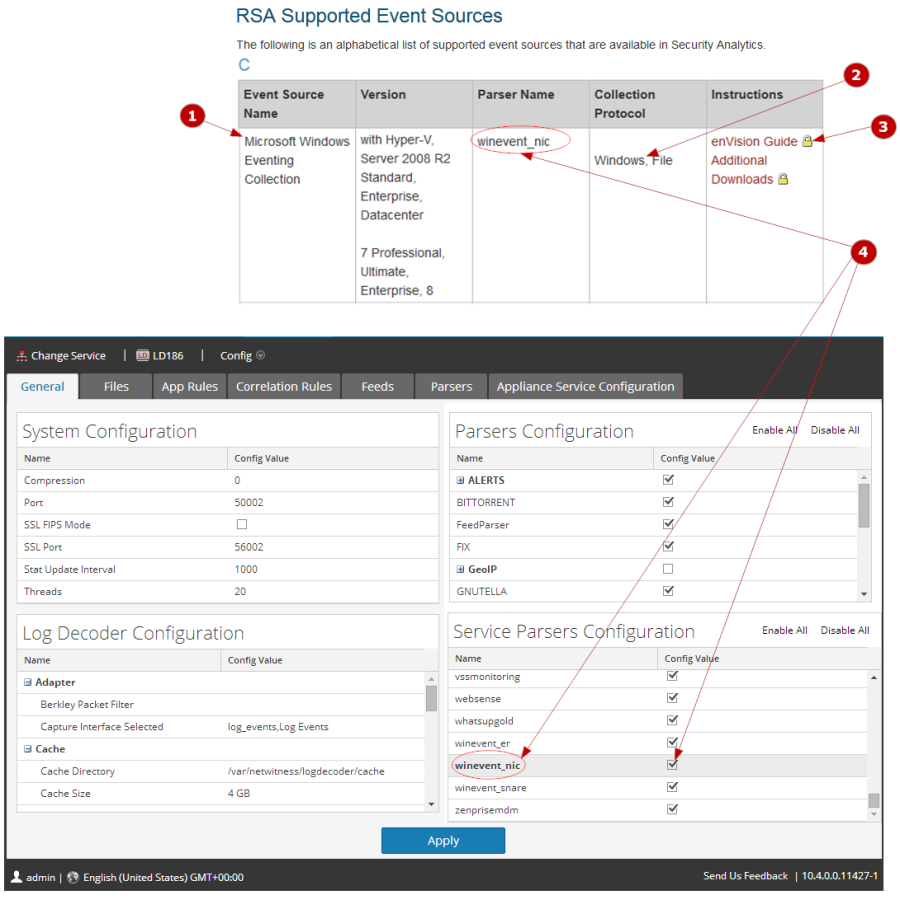
Paso 2. Configurar orígenes de eventos de Windows para enviar eventos a Security Analytics

En este tema se indica dónde encontrar los orígenes de eventos que son compatibles actualmente con la recopilación de Windows y las instrucciones de configuración disponibles para cada origen de eventos.

Lista de orígenes de eventos compatibles

Volver a Procedimientos

La lista de orígenes de eventos compatibles de RSA es una lista alfabética de todos los orígenes de eventos
que son compatibles actualmente con Security Analytics, en la cual se identifican los orígenes de eventos que puede usar con la recopilación de Windows.



1 Busque el nombre del origen de eventos.

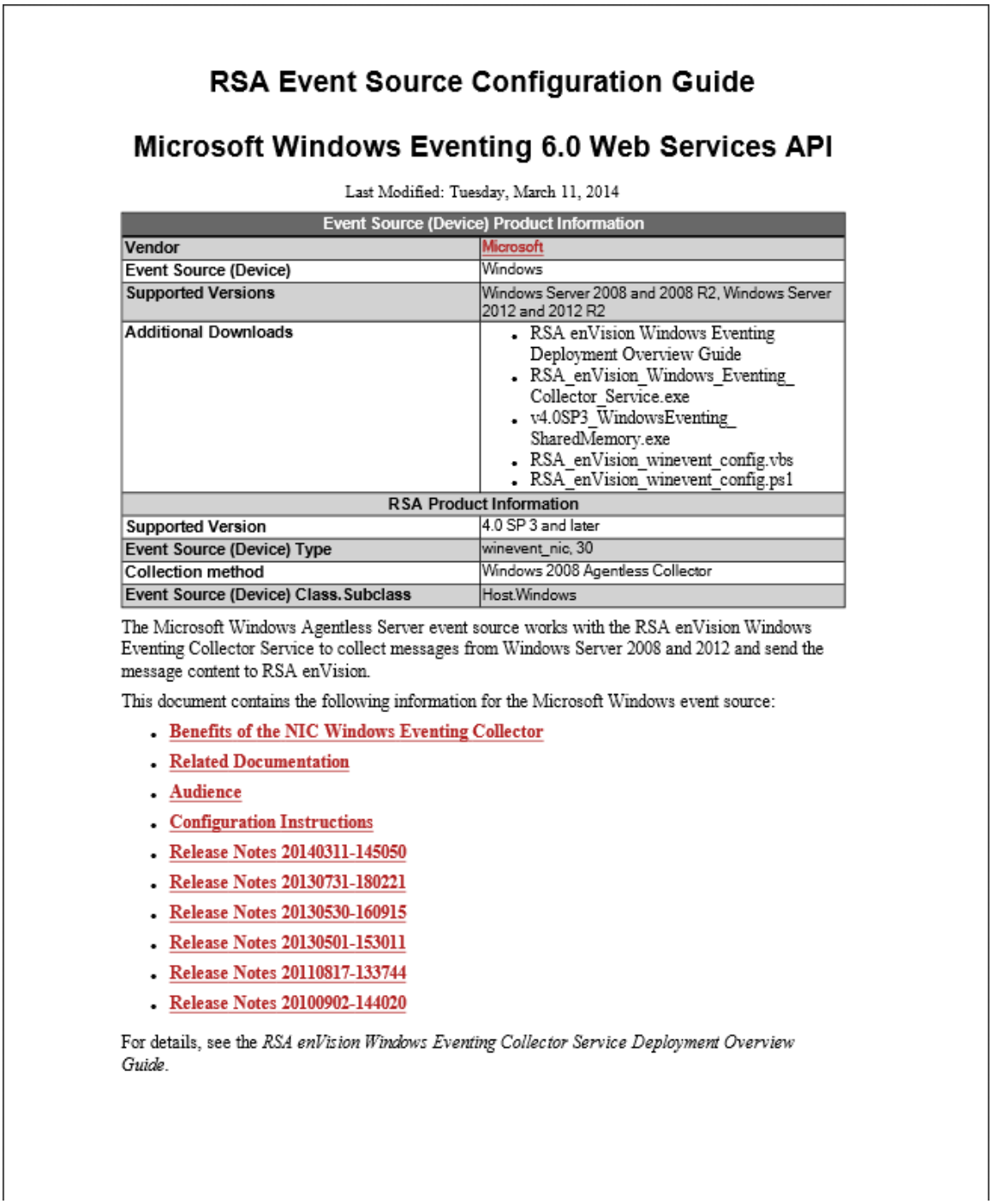
2 Verifique que sea compatible con el protocolo de recopilación de Windows.

3 Haga clic en para recuperar las instrucciones de configuración del origen de eventos.

4 Verifique que haya descargado el analizador de origen de eventos correcto (por ejemplo, **winevent_nic**) desde LIVE a Log Decoder y que lo haya habilitado.

Ejemplo de instrucciones de configuración

La siguiente ilustración se extrajo de las instrucciones de configuración de Microsoft Windows Eventing 6.0 Web Services API.



RSA Event Source Configuration Guide

Microsoft Windows Eventing 6.0 Web Services API

Last Modified: Tuesday, March 11, 2014

Event Source (Device) Product Information	
Vendor	Microsoft
Event Source (Device)	Windows
Supported Versions	Windows Server 2008 and 2008 R2, Windows Server 2012 and 2012 R2
Additional Downloads	• RSA enVision Windows Eventing Deployment Overview Guide • RSA_enVision_Windows_Eventing_ Collector_Service.exe • v4.0SP3_WindowsEventing_ SharedMemory.exe • RSA_enVision_winevent_config.vbs • RSA_enVision_winevent_config.ps1
RSA Product Information	
Supported Version	4.0 SP 3 and later
Event Source (Device) Type	winevent_nic, 30
Collection method	Windows 2008 Agentless Collector
Event Source (Device) Class.Subclass	Host.Windows

The Microsoft Windows Agentless Server event source works with the RSA enVision Windows Eventing Collector Service to collect messages from Windows Server 2008 and 2012 and send the message content to RSA enVision.

This document contains the following information for the Microsoft Windows event source:

- Benefits of the NIC Windows Eventing Collector
- Related Documentation
- Audience
- Configuration Instructions
- Release Notes 20140311-145050
- Release Notes 20130731-180221
- Release Notes 20130530-160915
- Release Notes 20130501-153011
- Release Notes 20110817-133744
- Release Notes 20100902-144020

For details, see the *RSA enVision Windows Eventing Collector Service Deployment Overview Guide*.

Paso 3. Iniciar el servicio para el protocolo de recopilación de Windows configurado

En este tema se indica cómo iniciar un servicio de recopilación de Windows detenido.

Si un servicio de recopilación de Windows se detiene, tendrá que iniciarlo nuevamente para que funcione. También puede consultar el tema **Habilitar el inicio automático de servicios individuales** de la *Guía de configuración de la recopilación de registros* si desea que el servicio se inicie automáticamente.

Procedimiento

Volver a Procedimientos

1. Para iniciar un servicio de recopilación:
2. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
3. Seleccione un servicio Log Collector y elija > **Ver** > **Sistema**.
   Se muestra la vista **Sistema de servicios**.
4. Haga clic en **Recopilación > Windows > Iniciar** en la barra de herramientas.

Paso 4. Verificar que la recopilación de Windows esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de Windows se configuró correctamente.

Si la recopilación de Windows no se configura correctamente, no funcionará. Puede comprobar si está funcionando en la vista Estado y condición o en la vista Investigation.

Procedimiento

Volver a Procedimientos

Para verificar que la recopilación de Windows esté funcionando:

1. En el menú de **Security Analytics**, seleccione **Administration > Estado y condición**.
2. En la pestaña **Monitoreo de orígenes de eventos**, busque un tipo de origen de eventos de Windows (por ejemplo, **winevent_nic**) en la columna **Tipo de origen de evento**.
3. Busque actividad en la columna **Conteo** para verificar que la recopilación de Windows esté aceptando eventos.

En la siguiente figura se ilustra cómo puede verificar que la recopilación de Windows esté funcionando desde **Investigation > vista Eventos**.

1. En el menú de **Security Analytics**, seleccione **Investigation > Eventos**.
2. Seleccione el Log Decoder que recopila eventos de **Windows** en el cuadro de diálogo **Investigar un servicio**.
3. Busque un tipo de servicio de Windows en la columna **Detalles** para verificar que la recopilación de Windows esté aceptando eventos.

Referencias: Parámetros de configuración de la recopilación de Windows

En este tema se describen los parámetros de configuración del origen de eventos de Windows.

Los parámetros de configuración del origen de eventos de recopilación de Windows tienen dos vistas: parámetros de **Windows** y de **dominio Kerberos**.

- Parámetros de configuración del origen de eventos de Windows
- Parámetros de configuración de Windows Kerberos

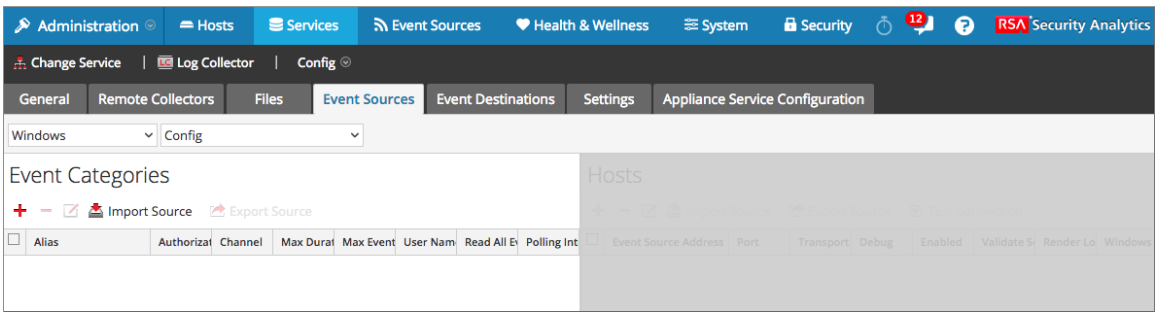
Parámetros de configuración del origen de eventos de Windows

En este tema se indica cómo configurar los orígenes de eventos de Windows para el Log Collector.

La opción Windows/Configuración de la vista Configuración del servicio Log Collector > pestaña Orígenes de evento muestra los parámetros que se especifican para configurar orígenes de eventos de Windows.

Para acceder a los parámetros de configuración del origen de eventos de Windows:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. En la columna **Acciones**, seleccione  **> Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione **Windows/Configuración** en los menús desplegables.



Características

La vista Windows/Configurar de la pestaña Orígenes de evento tiene dos paneles: Categorías de evento y Hosts.

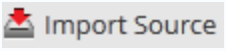
Panel Categorías de evento

El panel Categorías de evento proporciona una lista de alias de orígenes de eventos de Windows existentes. Use esta sección para agregar o eliminar alias de orígenes de eventos de Windows.

El dominio de Windows, conocido como alias, es el parámetro de configuración que Log Collector usa para agrupar orígenes de eventos. Generalmente, el alias define a un solo dominio, porque las credenciales (es decir, nombre de usuario y contraseña) y los canales se aplican a todo el dominio. En ocasiones, es necesario definir varias entradas de alias para el mismo dominio si se necesita personalizar los ajustes de diferentes grupos de orígenes de eventos.

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Opción	Descripción
	Muestra el cuadro de diálogo **Agregar origen de evento**, en el cual se definen los parámetros de un nuevo origen de eventos de Windows.
	Elimina los alias de origen de eventos de Windows seleccionados.
	Muestra el cuadro de diálogo **Editar origen de evento**, en el cual se editan los parámetros del origen de eventos de Windows seleccionado. Cuando se seleccionan varios orígenes de eventos, se abre el cuadro de diálogo **Edición en masa de origen**, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte Importar, exportar y editar orígenes de eventos de manera masiva en la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo usar esta función.
	Abre el cuadro de diálogo **Opción Adición en masa** en el cual puede importar parámetros de host de origen de eventos de manera masiva desde un archivo con valores separados por comas (CSV). Consulte Importar, exportar y editar orígenes de eventos de manera masiva en la Guía de configuración de la recopilación de registros para conocer los pasos detallados sobre cómo usar esta función.

Export Source	Crea un archivo **.csv** que contiene los parámetros de los hosts seleccionados. Consulte Importar, exportar y editar orígenes de eventos de manera masiva en la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo usar esta función.
Test Connection	Valida los parámetros de configuración para los hosts seleccionados. Consulte la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo probar conexiones de orígenes de eventos en masa.

Cuadro de diálogo Agregar origen de eventos

En este cuadro de diálogo puede definir parámetros para un nuevo origen de eventos de Windows.

Característica	Descripción
Básico	
Alias*	El dominio de Windows, conocido como alias, es el parámetro de configuración que Log Collector usa para agrupar orígenes de eventos. Estos grupos de tipos de orígenes de eventos (por ejemplo, **domain2**, **domain3** y **domain4**) categorizan los orígenes de eventos que ha configurado.
Método de autorización*	El método de autenticación. Los valores válidos son: • Básico (valor predeterminado) • Negociar: negocia la autenticación entre Kerberos y NTLM (Microsoft Windows NT LAN Manager). Por motivos de seguridad, Security Analytics es compatible exclusivamente con Kerberos.

Característica	Descripción
Channel	Lista separada por comas de canales desde los cuales Security Analytics recopila eventos. Sistema, Aplicación y Seguridad es el valor predeterminado para este parámetro. Consulte “Determinar el nombre del canal en el origen de eventos de Windows” en Paso 1. Configurar orígenes de eventos de Windows en Security Analytics para conocer los nombres de canal apropiados que se deben usar para definir este parámetro. Puede utilizar paréntesis para incluir y excluir ID de evento. El filtro de exclusión debe tener un carácter ^ entre el nombre del canal y el ID de evento. Los ID de evento se deben separar con un carácter |. Por ejemplo, **Application^(211|300), System(1010|1012)** excluye los eventos Application 211 y 300 e incluye los eventos System 1010 y 1012. Un canal es un flujo de eventos con nombre que los transporta desde un editor de eventos a un archivo de registro de eventos. Existen muchos canales de Windows predefinidos. Los siguientes son algunos ejemplos de esos canales: **Sistema**: Aplicaciones que se ejecutan bajo cuentas de servicio del sistema (servicios del sistema instalados), drivers o un componente o aplicación que tiene eventos relacionados con el estado del sistema. **Aplicación**: todas las aplicaciones de nivel de usuario. Este canal no es seguro y está abierto a cualquier aplicación. Si una aplicación tiene mucha información, es recomendable definir un canal de aplicación específico para ella. **Seguridad**: el registro de auditoría de Windows (registro de eventos) que se usa exclusivamente para la Autoridad de seguridad local de Windows. Consulte http://msdn.microsoft.com/en-us/subscriptions/aa385225(v=vs.85).aspx para obtener información adicional sobre los canales de Windows.

Característica	Descripción
Nombre de usuario *	Nombre de usuario de origen de eventos. Para la autenticación negociada, debe ser el nombre del principal de Kerberos en el formato name@kerberosdomain. Por ejemplo, **logcollector@LAB30.LOCAL**.
Contraseña *	Contraseña de origen de eventos. La contraseña se cifra internamente y se muestra en su forma cifrada.
Leer todos los eventos	Seleccione esta casilla de verificación para leer todos los datos de eventos históricos de un canal. Los valores válidos son: • **Seleccionada**: Log Collector recopila información de todos los datos de eventos históricos de un canal específico. • **Deseleccionada (valor predeterminado)**: Log Collector no recopila información de todos los datos de eventos históricos de un canal específico.
Avanzado	
Duración máxima de encuesta	La duración máxima del ciclo de sondeo (cuánto tiempo dura el ciclo) en segundos.
Máximo de eventos por ciclo	La cantidad máxima de eventos por ciclo de sondeo (cuántos eventos se recopilan por ciclo de sondeo).
Intervalo de sondeo	El intervalo (cantidad de tiempo en segundos) entre cada encuesta. El valor predeterminado es **180**. Por ejemplo, si especifica 180, el recopilador programa un sondeo del origen de eventos cada 180 segundos. Si aún se está realizando el ciclo de sondeo anterior, esperará hasta que ese ciclo termine. Si está sondeando una gran cantidad de orígenes de eventos, es posible que el sondeo tarde más de 180 segundos en comenzar porque los subprocesos están ocupados.

Característica	Descripción
Generar eventos	Seleccione esta casilla de verificación para solicitar la generación de eventos desde el origen de eventos. • **Seleccionada (valor predeterminado)**: Log Collector solicita los eventos generados desde el origen de eventos. • **Deseleccionada**: Log Collector no solicita los eventos generados desde el origen de eventos.
Cancelar	Cierra el cuadro de diálogo sin agregar el origen de eventos de Windows.
OK	Agrega los valores de los parámetros actuales como un nuevo origen de eventos.

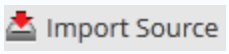
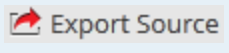
Panel Hosts

El panel Hosts muestra una lista de hosts de orígenes de eventos de Windows existentes. Use esta sección para agregar o eliminar hosts de origen de eventos de Windows (es decir, la dirección del origen de eventos de Windows y los parámetros de comunicación asociados).

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Opción	Descripción
	Muestra el cuadro de diálogo Agregar host, en el cual puede definir los parámetros de un host para el origen de eventos que seleccionó en el panel Categorías de evento.
	Elimina el host de origen de eventos seleccionado.

	Muestra el cuadro de diálogo Editar host, en el cual se editan los parámetros del origen de eventos de Windows seleccionado. Cuando se seleccionan varios orígenes de eventos, se abre el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los hosts seleccionados. Consulte Importar, exportar y editar orígenes de eventos de manera masiva en la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo usar esta función.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar orígenes de eventos masivamente desde un archivo con valores separados por coma (CSV). El cuadro de diálogo Opción Adición en masa tiene las siguientes dos opciones. Consulte Importar, exportar y editar orígenes de eventos de manera masiva en la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo usar esta función.
	Crea un archivo **.csv** que contiene los parámetros de los orígenes de eventos seleccionados. Consulte Importar, exportar y editar orígenes de eventos de manera masiva en la *Guía de configuración de la recopilación de registros* para conocer los pasos detallados sobre cómo usar esta función.
	Valida la Dirección de origen de evento para los hosts seleccionados.

Cuadro de diálogo Agregar host

En la siguiente tabla se proporcionan descripciones de las funciones del cuadro de diálogo Agregar host.

Columna	Descripción
Básico	

Dirección de origen de evento*	Dirección IP del origen de eventos. El valor válido es una dirección IPv4, una dirección IPv6 o un nombre de host que incluya un nombre de dominio calificado. Log Collector convierte el nombre de host en letras minúsculas para evitar que haya entradas duplicadas.
Puerto	Número de puerto. Un número de puerto válido es cualquier número dentro del rango de 1 a 65535. • WinRM 2.0 (Vista y superior) usa los puertos 5985 para HTTP y 5986 para HTTPS como los puertos predeterminados. • WinRM 1.1 (Windows 2003) usa los puertos 80 para HTTP y 443 para HTTPS como los puertos predeterminados.
Modo de transporte	modo de transporte [por ejemplo, http (valor predeterminado)]. Los modos de transporte válido son: • **HTTP** (valor predeterminado): conexión no segura • **HTTPS**: conexión segura
Activado	Seleccione esta casilla de verificación para recopilar desde este origen de eventos. Si no selecciona esta casilla de verificación, Log Collector no recopila eventos desde este origen de eventos.
Nombre del certificado	Nombre del certificado que se debe usar cuando el modo de transporte es HTTPS. Si está definido, el certificado debe existir en el área de almacenamiento de confianza de certificados. Los certificados se agregan al área de almacenamiento de confianza en el panel **Certificados** de la pestaña Configuración.
Avanzado	

Depurar	**Precaución:** Habilite la depuración (defina este parámetro en **Activado** o **Detallado**) solamente si hay un problema en un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa o desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar). Limite la cantidad de orígenes de eventos para los que utiliza depuración Detallada para minimizar el impacto en el rendimiento.
Validar servidor	Seleccione esta casilla de verificación para validar el Sujeto del certificado del servidor. El Sujeto del certificado del servidor debe coincidir con la dirección del origen de eventos.
Generar configuración regional	Especifique la ubicación donde se reproducen los eventos. Si no especifica un valor, el origen de eventos usa la configuración regional predeterminada. En la mayoría de los casos, la configuración regional predeterminada es en-US. El origen de eventos omite una configuración regional no compatible y la suscripción falla si la configuración regional no es válida.

Tipo de Windows	(Configuración opcional) Indica si el origen de eventos configurado y desde el cual está recopilando es o no una controladora de dominio. Security Analytics usa este parámetro para determinar si debe o no enviar la información al procesador de eventos de identidad (IDEP). Si no especifica este parámetro, todos los datos se envían al IDEP. Los valores válidos son: • **No está configurado**: Se envían todos los datos al IDEP. • **Controladora no de dominio**: El origen de eventos configurado desde el cual está recopilando es una controladora no de dominio. • **Controladora de dominio**: El origen de eventos configurado desde el cual está recopilando es una controladora de dominio.
Resolver SID	Resolver códigos de identificación del sistema (SID) Seleccione esta casilla de verificación para resolver SID de cuenta en atributos pertinentes en los eventos recopilados en los nombres de cuenta. Esta casilla de verificación está seleccionada de manera predeterminada.
Intervalo de enumeración de SID	Intervalo, en segundos, en el cual cada origen de eventos enumera los SID de cuenta. El valor válido está en el rango de **0 a 86400**. El valor predeterminado es **14400**.
Tiempo de espera agotado de enumeración de SID	Ingrese el tiempo, en segundos, para las operaciones de enumeración de SID. El valor válido está en el rango de **10 a 600**. El valor predeterminado es **60**.

Reemplazar canales	Este parámetro reemplaza al parámetro Canal del alias que configuró en el cuadro de diálogo **Agregar origen** para todos los hosts definidos para un alias de Windows (origen de eventos). Si deja el parámetro en blanco, Security Analytics usa el parámetro **Canal** del alias. Lista separada por comas de canales desde los cuales Security Analytics recopila eventos. **Sistema**, **Aplicación** y **Seguridad** es el valor predeterminado para este parámetro. Consulte "Determinar el nombre del canal en el origen de eventos de Windows" en Paso 1. Configurar orígenes de eventos de Windows en Security Analyticspara conocer los nombres de canal apropiados que se deben usar para definir este parámetro. Puede utilizar paréntesis para incluir y excluir ID de evento. El filtro de exclusión debe tener un carácter ^ entre el nombre del canal y el ID de evento. Los ID de evento se deben separar con un carácter |. Por ejemplo, **Application^(211|300), System(1010|1012)** excluye los eventos Application 211 y 300 e incluye los eventos System 1010 y 1012. Un canal es un flujo de eventos con nombre que los transporta desde un editor de eventos a un archivo de registro de eventos. Existen muchos canales de Windows predefinidos. Los siguientes son algunos ejemplos de esos canales: **Sistema**: Aplicaciones que se ejecutan bajo cuentas de servicio del sistema (servicios del sistema instalados), drivers o un componente o aplicación que tiene eventos relacionados con el estado del sistema. **Aplicación**: todas las aplicaciones de nivel de usuario. Este canal no es seguro y está abierto a cualquier aplicación. Si una aplicación tiene mucha información, es recomendable definir un canal de aplicación específico para ella. **Seguridad**: el registro de auditoría de Windows (registro de eventos) que se usa exclusivamente para la Autoridad de seguridad local de Windows.
Probar conexión	Valida la conexión a la dirección del origen de eventos.
Cancelar	Cierra el cuadro de diálogo sin agregar el origen de eventos de Windows.
OK	Guarda los parámetros actuales como un nuevo origen de eventos.

Tareas

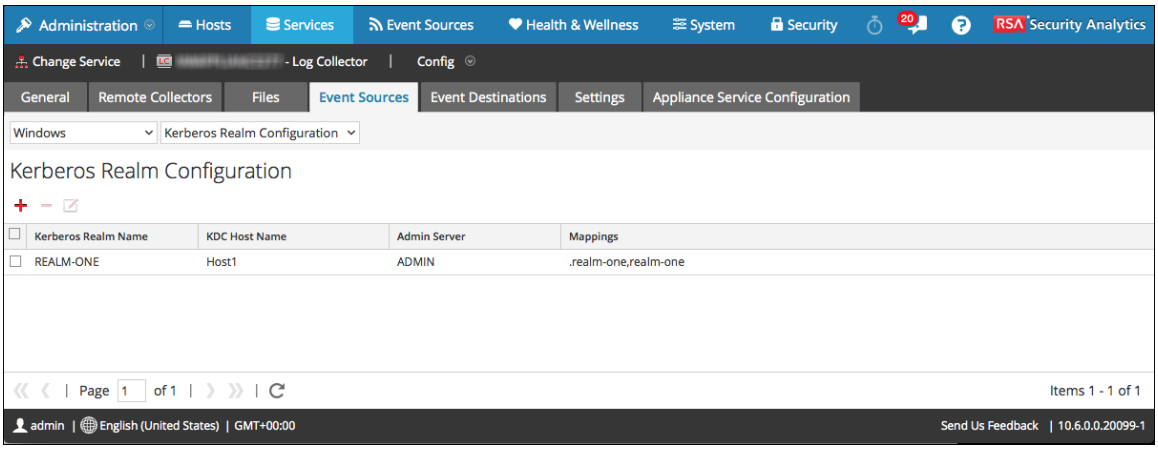
Paso 1. Configurar orígenes de eventos de Windows en Security Analytics

Parámetros de configuración de Windows Kerberos

Parámetros de configuración de Windows Kerberos

En este tema se describen los parámetros de configuración del dominio de Kerberos para Autenticación de Windows Kerberos.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. En la barra de herramientas, seleccione **Ver > Configuración > Orígenes de evento**.
4. En la pestaña **Orígenes de evento**, seleccione **Configuración de dominio Windows/Kerberos** en el menú desplegable.



Características

La vista Configuración de dominio Windows/Kerberos en la pestaña Orígenes de evento tiene un panel: Configuración de dominio Kerberos.

Panel Configuración de dominio Kerberos

El panel **Configuración de dominio Kerberos** permite **agregar**, **eliminar** o **editar** dominios de Kerberos.

Nota: Security Analytics completa previamente el parámetro Mapeos en función de los valores del parámetro Nombre de dominio Kerberos que ingresó.

Característica	Descripción
	Muestra el cuadro de diálogo **Agregar dominio de Kerberos**, en el cual se definen los parámetros del dominio de Kerberos.
	Elimina los dominios de Kerberos seleccionados.
	Muestra el cuadro de diálogo **Editar dominio Kerberos**, en el cual edita los parámetros del dominio Kerberos.
	Selecciona dominios de Kerberos.
Parámetros de dominio de Kerberos	Muestra los dominios que ha agregado con sus parámetros.

Cuadro de diálogo Agregar o Editar dominio Kerberos

En este cuadro de diálogo, puede agregar o modificar los parámetros del dominio de Kerberos.

Característica	Descripción
Nombre de dominio de Kerberos *	Nombre de dominio de Kerberos. Valor válido es un nombre que está completamente en letras mayúsculas y en formato de nombre de dominio calificado.
Nombre de host KDC *	Un nombre del centro de distribución de claves. Valor válido es un nombre que está en formato **.domain-name**. Si hay múltiples KDC disponibles, puede ingresarlos con comas como separador.
Servidor de administración	(Opcional) El nombre del servidor de administración de Kerberos en formato de **nombre de dominio calificado**.

Característica	Descripción
Mapeo	Mapeo desde hosts a dominios de Kerberos. **.domain,domain** es el valor predeterminado, donde domain es el dominio de Windows. Si su implementación requiere un mapeo adicional, puede ingresarlos con comas como separador. **Nota:** Security Analytics completa previamente el parámetro Mapeos en función de los valores del parámetro Nombre de dominio Kerberos que ingresó.
Cerrar	Cierra el cuadro de diálogo sin agregar el dominio ni guardar las modificaciones en los parámetros.
Guardar	Agrega los parámetros de dominio de Kerberos o guarda las modificaciones de los parámetros.

Tareas

Parámetros de configuración de Windows Kerberos

Parámetros de configuración del origen de eventos de Windows

Solucionar problemas de la recopilación de Windows

En este tema se señalan posibles problemas que puede encontrar en la recopilación de Windows y las soluciones que se sugieren para ellos.

Solucionar problemas de la recopilación de Windows

En general, se reciben mensajes de registro más confiables cuando se desactiva SSL.

Security Analytics devuelve los siguientes tipos de mensajes de error en los archivos de registro.

Mensajes de registro	(i) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.-bad-host_lab30_local] [processing] [LAB30.bad-host_lab30_local] Starting work (F) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] Error subscribing. Transport error code = 6/Could not resolve host (F) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] [processing] [LAB30.-bad-host_lab30_local] Unable to subscribe for events with Windows event source bad-host.lab30.local: Could not resolve host Possible causes: - DNS resolution failed or name/address (bad-host.lab30.local) incorrect. (i) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] [processing] [LAB30.bad-host_lab30_local] Finished work (F) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] [processing] [LAB30.-bad-host_lab30_local] windows:WrkUnit[1] Processing failed. (i) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Starting work (i) 2013-Nov-21 14:47:06[WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Enumerating SID information (F) 2013-Nov-21 14:47:09 [WindowsCollection] [LAB30.10_100_33_179] Error enumerating for account SIDs. Transport error code = 7/Could not connect (F) 2013-Nov-21 14:47:09 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Error enumerating for SID information: Could not connect

	(F) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] Error subscribing. Transport error code = 7/Could not connect (F) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Unable to subscribe for events with Windows event source 10.100.33.179: Could not connect Possible causes: - Event source not configured for collection with http. - Event source currently down. (i) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Finished work (F) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] windows:WrkUnit[2] Processing failed.
Causa posible	La recopilación de Windows no se puede conectar a WinRM.
Soluciones	La recopilación de Windows se conecta al servicio WinRM en el origen de eventos de Windows. Debe configurar el origen de eventos de Windows para permitir que la recopilación de los eventos. Puede hacer esto manualmente mediante el comando **winrm** en el origen de eventos o puede crear una política de grupo y migrarla a todos los orígenes de eventos de un dominio. Esta configuración crea un escucha de WinRM en el origen de eventos. También debe configurar el firewall en el origen de eventos para permitir las conexiones a él. De forma predeterminada, WinRM escucha en el puerto 5985 las conexiones HTTP y en el puerto 5986 las conexiones HTTPS. Consulte **Orígenes de eventos compatibles** en la *Guía de administración de recursos de Live* para obtener instrucciones sobre la configuración de orígenes de eventos.

Guía de configuración de la recopilación de Windows existente y NetApp

En esta guía se indica cómo configurar Windows existente y NetApp mediante el protocolo de recopilación de **Windows existente**.

Este protocolo recopila eventos de Windows heredado (orígenes de eventos de Windows 2003 o versiones anteriores) y eventos de auditoría de CIFS desde orígenes de eventos de NetApp ONTAP.

Debe implementar la recopilación de registros, es decir, configurar un Local Collector y un Remote Collector de Windows existente, antes de poder configurar el protocolo de recopilación de Windows existente.

Para obtener instrucciones sobre la implementación, consulte Guía de implementación de la recopilación de registros.

Conceptos básicos

En este tema se indica cómo funciona el protocolo de recopilación de Windows existente y cómo se implementa. También se brinda una descripción de alto nivel de la forma de configurar este protocolo.

Cómo funciona la recopilación de Windows existente y NetApp

El protocolo de recopilación de Windows existente se utiliza para configurar Security Analytics con el fin de que recopile eventos desde:

- Orígenes de eventos de Microsoft Windows existentes (orígenes de eventos de Windows 2003 y versiones anteriores)
- Orígenes de eventos de NetApp

Orígenes de eventos de Windows 2003 y versiones anteriores

Los orígenes de eventos de Windows existentes son versiones anteriores de Windows (como Windows 2000 y Windows 2003). El protocolo de recopilación de Windows existente recopila de orígenes de eventos de Windows que ya están configurados para la recopilación de enVision sin tener que volver a configurarlos. Puede configurar estos orígenes de eventos en el tipo de origen de eventos ventanas .

Orígenes de eventos de NetApp

Los dispositivos de NetApp que ejecutan Data ONTAP son compatibles con un marco de trabajo de auditoría nativo similar a Windows Servers. Cuando se configura, este marco de trabajo de auditoría genera y guarda eventos de auditoría en el formato de archivo .evt de Windows. El protocolo de recopilación de Windows existente es compatible con la recopilación de eventos desde dichos archivos .evt de NetApp. Puede configurar estos orígenes de eventos en el tipo de origen de eventos netapp_evt.

El dispositivo de Data ONTAP de NetApp está configurado para generar eventos de auditoría de CIFS y guardarlos periódicamente como archivos .evt en un formato que incluye el registro de fecha y hora en el nombre de archivo. Consulte la documentación de configuración de Orígenes de eventos de NetApp en SecurCare Online (SCOL) para obtener detalles. El protocolo de recopilación guarda el registro de fecha y hora del último nombre de archivo .evt procesado para hacer un seguimiento del estado de recopilación

Parámetros específicos de Net App

La mayoría de los parámetros que mantiene en el cuadro de diálogo Agregar/Editar origen se aplican a orígenes de eventos tanto de Windows existente como de Net App.

Los siguientes dos parámetros son únicos para los orígenes de eventos de NetApp.

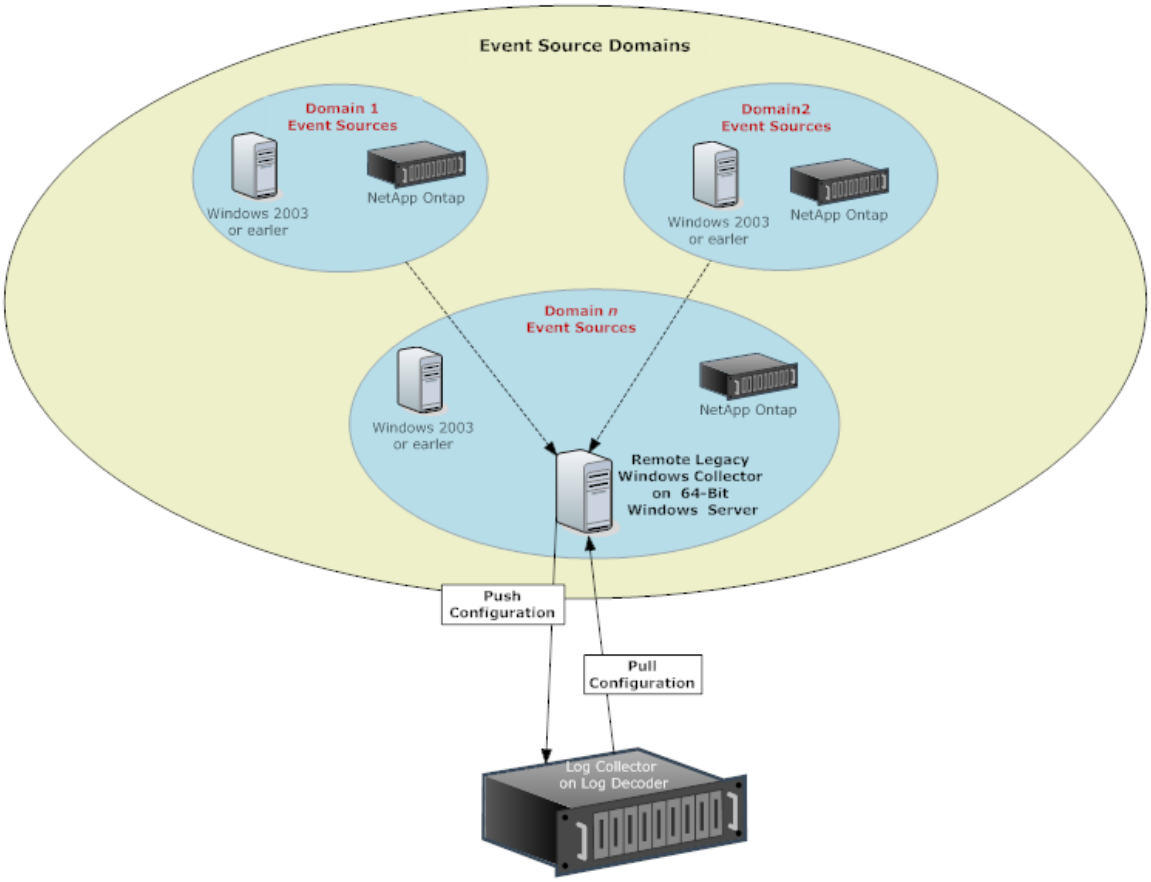
- **Ruta de directorio de eventos**: El dispositivo NetApp genera datos de eventos y los guarda en archivos .evt en un directorio que se puede compartir en este dispositivo. Security Analytics requiere que especifique esta ruta de directorio en el parámetro Ruta de directorio de eventos.
- **Prefijo de archivo de evento**: De manera similar a Ruta de directorio de eventos, Security Analytics requiere que se especifique el prefijo (por ejemplo, adtlog.) de los archivos .evt de datos de eventos de modo que pueda procesar estos datos.

En cada ciclo de sondeo, Security Analytics navega por la ruta compartida de NetApp configurada para los archivos **.evt** que identificó con los parámetros Ruta de directorio de eventos y Prefijo de archivo de evento. Security Analytics:

- Clasifica los archivos que coinciden con el formato event-file-prefix.YYMMDDhhmmss.evt en orden ascendente.
- Usa el registro de fecha y hora del último archivo procesado para determinar los archivos que aún requieren procesamiento. Si Security Analytics encuentra un archivo procesado parcialmente, omite los eventos ya procesados.

Escenario de implementación

El protocolo de recopilación de Windows existente recopila datos de eventos de Windows 2003 o versiones anteriores, y orígenes de datos del dispositivo ONTAP de NetApp. El Remote Collector de Windows heredado es el recopilador de Windows heredado de SA instalado en un servidor Windows 2008 de 64 bits físico o virtual en su dominio de origen de eventos.



Configurar el protocolo de recopilación de Windows heredado en Security Analytics

Puede configurar el Log Collector para usar la recopilación de Windows existente para un origen de eventos en la pestaña Origen de eventos de la vista del parámetro Log Collector. En la siguiente figura se muestra el flujo de trabajo básico para configurar un origen de eventos para la recopilación de Windows heredado en Security Analytics. Consulte:

- Paso 2. Configurar orígenes de eventos de Windows existente y NetApp en Security Analyticspara obtener instrucciones paso a paso sobre la configuración de orígenes de eventos en Security Analytics que usan el protocolo de recopilación de archivos.

- Parámetros de configuración del origen de eventos de Windows para obtener una descripción detallada de cada parámetro del protocolo de recopilación de archivos.

Procedimientos

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de Windows existente con una lista de verificación que contiene cada paso de configuración.

Los pasos de configuración para Log Collector deben realizarse en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de configuración de Windows heredado y NetApp

Nota: El recopilador de Windows heredado de Security Analytics se instala en un servidor Windows 2008 R2 SP1 de 64 bits físico o virtual mediante el archivo **SALegacyWindowsCollector-*version-number.exe*.** El archivo **SALegacyWindowsCollector-*version-number.exe*** se descarga desde SCOL [consulte Instrucciones de actualización e instalación de Windows heredado para SA-v10.6 en SCOL (https://knowledge.rsasecurity.com/)].

los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Configurar el recopilador de Windows heredado.	
2	Configurar orígenes de eventos de Windows heredado en Security Analytics.	
3	Iniciar el servicio para el protocolo Windows heredado configurado.	
4	Verificar que la recopilación de Windows existente esté funcionando.	

Paso 1. Configurar el recopilador de Windows existente

En este tema se indica dónde buscar el archivo ejecutable y se proporcionan las instrucciones requeridas para instalar o actualizar el recopilador de Windows existente en uno o más dominios de Windows existente.

Volver a Procedimientos

El recopilador de Windows heredado de Security Analytics se instala en un servidor Windows 2008 R2 SP1 de 64 bits físico o virtual mediante el archivo **SALegacyWindowsCollector-10.6.*version-number.exe***. Puede descargar **SALegacyWindowsCollector-10.6.*version-number.exe*** desde SCOL. Consulte *Instrucciones de actualización e instalación de la recopilación de Windows heredado de SA v10.6* en SCOL (https://knowledge.rsasecurity.com) para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows heredado.

Nota: Microsoft Management Console (MMC) debe estar cerrada durante el proceso de instalación.

Paso 2. Configurar orígenes de eventos de Windows existente y NetApp en Security Analytics

En este tema se indica cómo configurar los orígenes de eventos de Windows existente en Security Analytics.

El protocolo de recopilación de Windows existente recopila datos de eventos de orígenes de eventos de Windows 2003 o versiones anteriores y de orígenes de eventos de NetApp.

Después de realizar este procedimiento, habrá:

- Configurado un origen de eventos de Windows existente.
- Modificado un origen de eventos de Windows existente.

Volver a Procedimientos

Requisitos previos

Antes de configurar un origen de eventos de Windows existente, asegúrese de haber:

1. Instalado el Remote Collector de Windows heredado de Security Analytics en un servidor Windows 2008 de 64 bits físico o virtual.
2. Agregado este Remote Collector de Windows heredado a Security Analytics.

Procedimientos

Agregar un origen de eventos de Windows existente

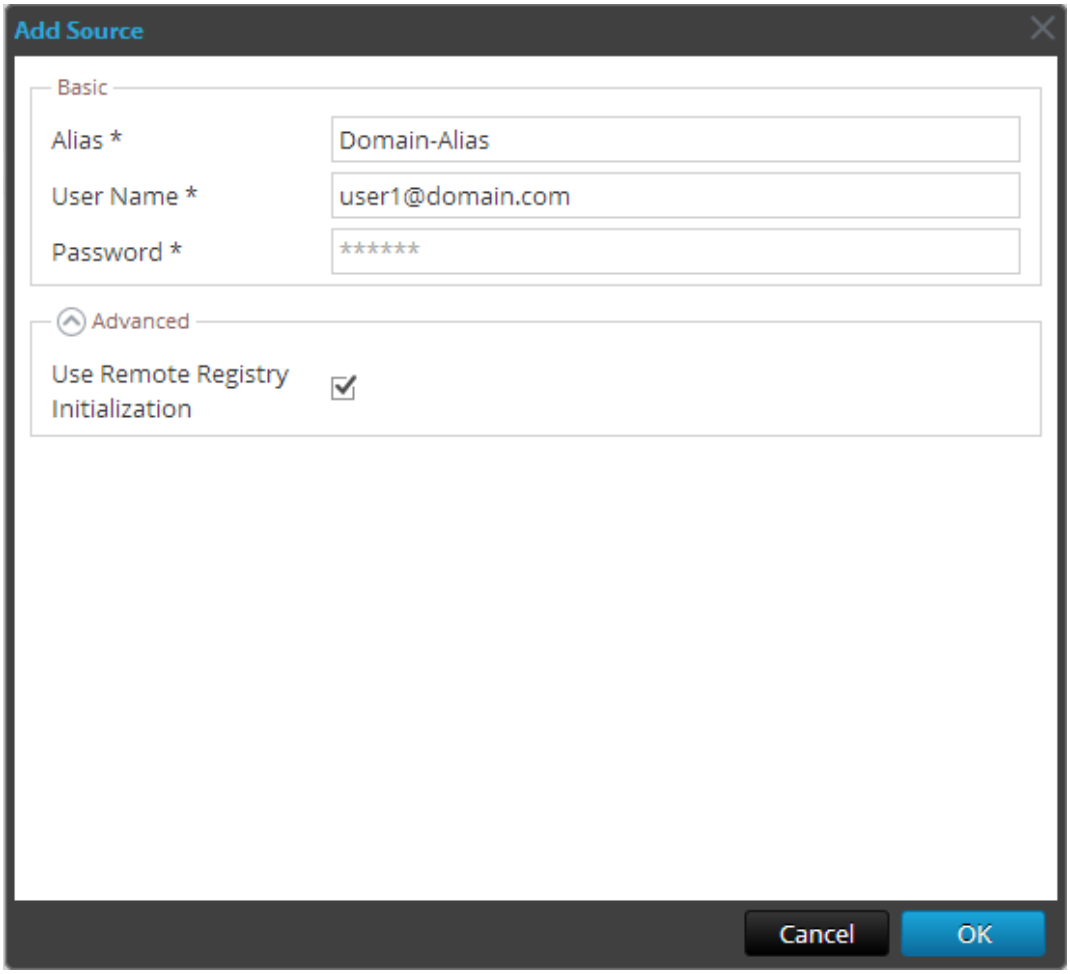
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector de Windows heredado**.
3. En la barra de herramientas, seleccione **Ver > Configuración > Orígenes de evento.**
4. En la pestaña **Orígenes de evento**, seleccione una de las siguientes opciones en el menú desplegable.

- Windows existente/Windows.
- Windows existente/NetApp.

5. Configure el alias:

   a. Haga clic en + en la barra de herramientas del panel **Categorías de evento**.
   Se muestra el cuadro de diálogo **Agregar origen**.

   b. Especifique valores para los parámetros y haga clic en **Aceptar**.

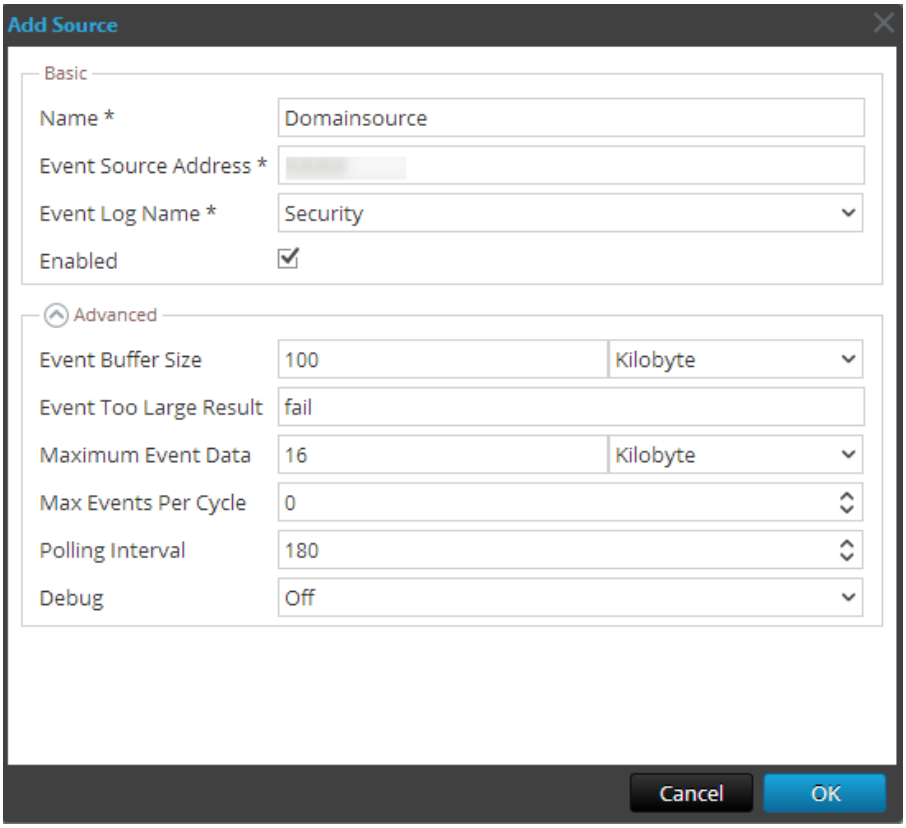


   El tipo de origen de eventos de **Windows** agregado recientemente se muestra en el panel Categorías de evento.

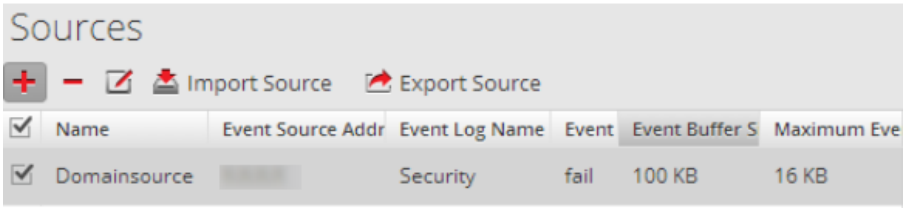
6. Agregar el origen de eventos:

   a. Seleccione el nuevo alias en el panel **Categorías de evento** y haga clic en + en la barra de herramientas del panel **Origen**.
   Se muestra el cuadro de diálogo **Agregar origen**.

b. Especifique valores para los parámetros de orígenes de eventos y haga clic en **Aceptar**.



El origen de eventos de Windows recién agregado se muestra en el panel **Categorías de evento**.

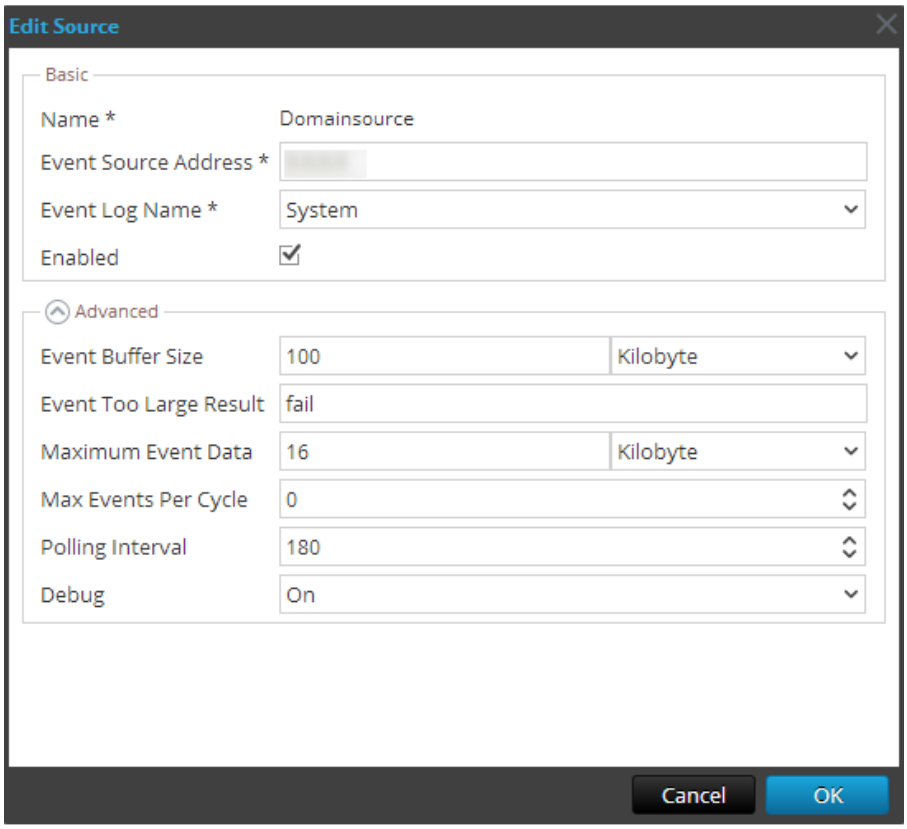


Modificar un origen de eventos de Windows existente

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. En el menú desplegable **Acciones**, seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento**, seleccione una de las siguientes opciones en el menú desplegable.

- Windows existente/Windows.
- Windows existente/NetApp

5. Modifique los parámetros de origen.
   a. En el panel **Categorías de evento**, seleccione un origen y haga clic en .
      Se muestra el cuadro de diálogo **Editar dominio**.
   b. Modifique los parámetros de origen que necesiten cambios y haga clic en **Guardar**.



6. Modificar los parámetros de un origen de eventos.
   a. En el panel **Origen**, seleccione un origen de eventos y haga clic en .
      Se muestra el cuadro de diálogo **Editar origen**.
   b. Modifique los parámetros de origen de eventos que necesiten cambios y haga clic en **Guardar**.
      Security Analytics aplica los cambios de parámetros al host seleccionado.

Parámetros

Referencias: Parámetros de configuración de la recopilación de Windows existente y NetApp

Paso 3. Iniciar el servicio para el protocolo de recopilación de Windows existente configurado

En este tema se indica cómo iniciar un servicio de recopilación de Windows existente detenido.

Si un servicio de recopilación de Windows existente se detiene, tal vez deba iniciarlo nuevamente.

Procedimiento

Volver a Procedimientos

En el siguiente procedimiento se muestra cómo iniciar un servicio de recopilación. Consulte el tema **Habilitar el inicio automático de servicios individuales** de la *Guía de configuración de la recopilación de registros* si desea que el servicio se inicie automáticamente.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. Seleccione un **Log Collector de Windows heredado** y, en la columna **Acciones**, seleccione  > **Ver > Sistema**.

   Se muestra la vista **Sistema de servicios**.
3. Haga clic en **Recopilación > Windows existente > Iniciar**.

Paso 4. Verificar que la recopilación de Windows existente esté funcionando

En este tema se indica lo que se debe comprobar en Security Analytics para verificar que la recopilación de Windows existente se configuró correctamente.

Este procedimiento es útil para verificar que configuró correctamente la recopilación de Windows existente. Si no se configura correctamente, no puede funcionar como debe.

Procedimiento

Volver a Procedimientos

En el siguiente procedimiento se explica cómo puede verificar que la recopilación de Windows heredado esté funcionando desde **Administration > Estado y condición > pestaña Monitoreo de orígenes de eventos**.

1. En el menú de **Security Analytics**, seleccione **Administration > Estado y condición.**
2. Haga clic en la pestaña **Monitoreo de orígenes de eventos**.
3. En la fila de la cuadrícula del tipo de origen de eventos de Windows existente, busque actividad en la columna **Conteo** para verificar que la recopilación de Windows existente esté aceptando eventos.

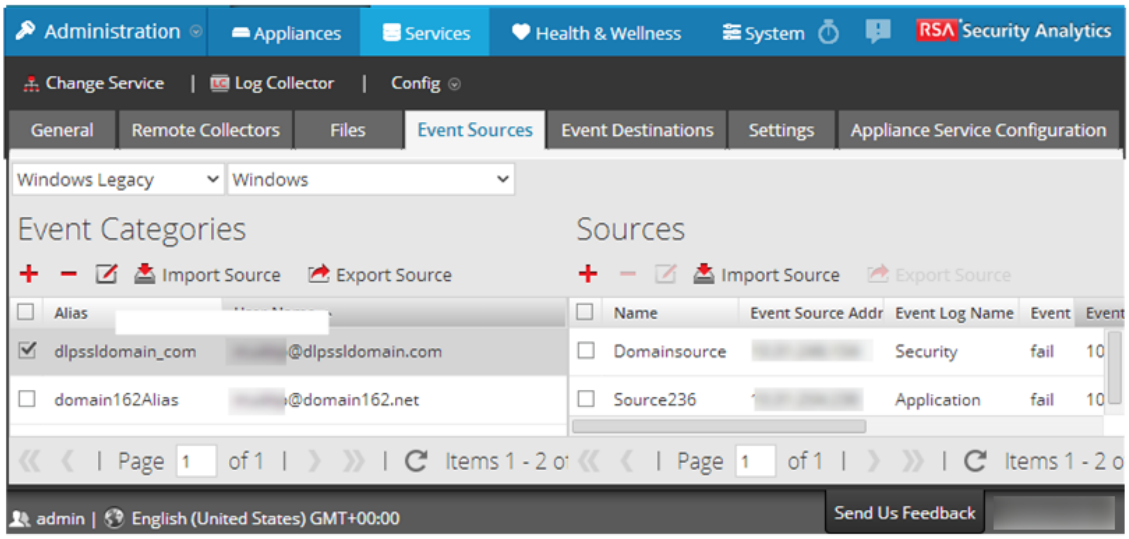
Referencias: Parámetros de configuración de la recopilación de Windows existente y NetApp

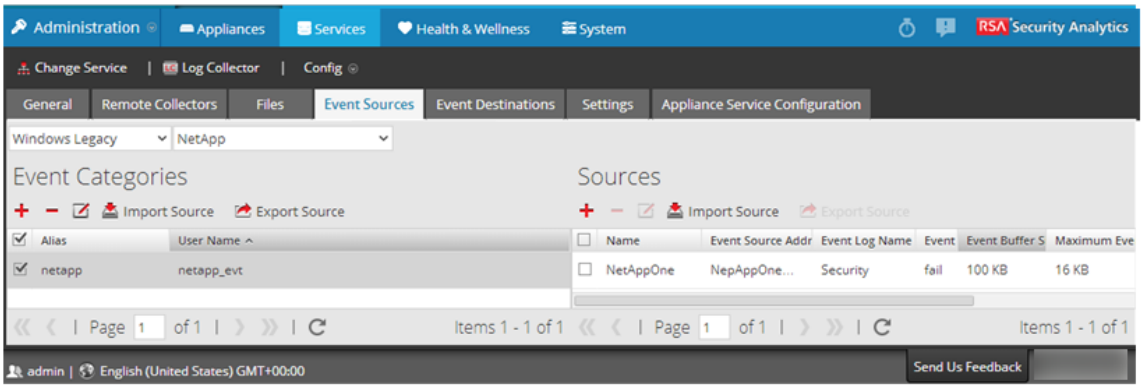
En este tema se describe la interfaz del usuario para configurar la recopilación de Windows existente.

Las opciones **Windows existente/Windows** o **Windows existente/NetApp** de la **vista Configuración > pestaña Orígenes de evento** del servicio Log Collector muestran los parámetros que se especifican para configurar orígenes de eventos de Windows heredado.

Para acceder a los parámetros de configuración de la recopilación de Windows existente y NetApp:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. En la columna **Acciones**, seleccione  > **Ver > Configuración** y haga clic en la pestaña **Orígenes de evento**.
4. En la pestaña **Orígenes de evento**, seleccione una de las siguientes opciones en el menú desplegable
   - **Windows existente/Windows**
   - **Windows existente/NetApp**





Características

La pestaña Orígenes de evento de Windows existente/Windows y Windows existente/NetApp tiene dos paneles: Categorías de evento y Orígenes.

Panel Categorías de evento

El panel Categorías de evento muestra los alias de orígenes de eventos de Windows existente actuales. Use esta sección para agregar o eliminar alias de orígenes de eventos de Windows existente.

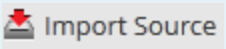
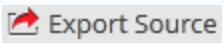
El dominio de Windows, conocido como alias, es el parámetro de configuración que Log Collector usa para agrupar orígenes de eventos. Generalmente, el alias define a un único dominio porque las credenciales (es decir, nombre de usuario y contraseña) y el nombre del registro de eventos se aplican a todo el dominio. En ocasiones, es necesario definir varias entradas de alias para el mismo dominio si se necesita personalizar los ajustes de diferentes grupos de orígenes de eventos.

Panel Orígenes

El panel Orígenes muestra una lista de orígenes de eventos de Windows existente actuales. Use esta sección para agregar o eliminar orígenes de eventos de Windows existente (es decir, la dirección del origen de eventos de Windows y los parámetros de comunicación asociados).

Barra de herramientas

En la siguiente tabla se proporcionan descripciones de las opciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Agregar origen, en el cual puede definir los parámetros para un host de firewall.
	Elimina el host que seleccionó.
	Abre el cuadro de diálogo Editar origen, en el cual puede editar los parámetros del origen de eventos seleccionado. Seleccione varios orígenes de eventos y haga clic en  para abrir el cuadro de diálogo Edición en masa de origen, en el cual puede editar los valores de los parámetros de los orígenes de eventos seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Abre el cuadro de diálogo Opción Adición en masa, en el cual puede importar hosts de forma masiva desde un archivo de valores separados por comas (CSV). Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.
	Crea un archivo .csv que contiene los parámetros de los hosts seleccionados. Consulte la Guía de configuración de la recopilación de registros para obtener información detallada sobre cómo importar, exportar y editar orígenes de eventos en masa.

Cuadro de diálogo Agregar origen

En este cuadro de diálogo puede definir parámetros para un nuevo origen de eventos de Windows existente.

Característica	Descripción
	Básico
Nombre*	Nombre del origen de eventos. Un valor válido es un nombre en el rango **[_a-zA-Z] [_a-zA-Z0-9]***. Puede usar un guion "**-**" como parte del nombre.
Dirección de origen de evento*	Dirección IP del origen de eventos. El valor válido es una dirección IPv4, una dirección IPv6 o un nombre de host que incluya un nombre de dominio calificado. Security Analytics se configura de forma predeterminada en **127.0.0.1**. Log Collector convierte el nombre de host en letras minúsculas para evitar que haya entradas duplicadas.
Nombre de registro de eventos	Nombre del registro de eventos desde el cual se recopilan datos de eventos (por ejemplo, **Sistema**, **Aplicación** o **Seguridad**). Los siguientes son algunos ejemplos de esos canales: • **Sistema**: Aplicaciones que se ejecutan bajo cuentas de servicio del sistema (servicios del sistema instalados), drivers o un componente o aplicación que tiene eventos relacionados con el estado del sistema. • **Aplicación**: todas las aplicaciones de nivel de usuario. Este canal no es seguro y está abierto a cualquier aplicación. Si una aplicación tiene mucha información, es recomendable definir un canal de aplicación específico para ella. • **Seguridad**: el registro de auditoría de Windows (registro de eventos) que se usa exclusivamente para la Autoridad de seguridad local de Windows.
Activado	Seleccione esta casilla de verificación para recopilar desde este origen de eventos. Si no selecciona esta casilla de verificación, Log Collector no recopila eventos desde este origen de eventos.

Característica	Descripción
Ruta de directorio de eventos	Ruta del directorio de archivos NetApp **.evt**. Debe ser la ruta UNC. NetApp genera datos de eventos y los guarda en archivos **.evt** en un directorio que se puede compartir en el dispositivo NetApp. En cada ciclo de sondeo, Log Collector navega por la ruta compartida de NetApp configurada para los archivos .evt que identificó con los parámetros Ruta de directorio de eventos y Prefijo de archivo de evento. Log Collector: • Clasifica los archivos que coinciden con el formato event-file-prefix.**YYMMDDhhmmss.evt** en orden ascendente. • usa el registro de fecha y hora del último archivo procesado para determinar los archivos que aún requieren procesamiento. Si Log Collector encuentra un archivo procesado parcialmente, omite los eventos ya procesados.
Prefijo de archivo de evento	Prefijo de los archivos **.evt** (por ejemplo, **adtlog.**) guardados en la **Ruta de directorio de eventos**.
Avanzado	
Tamaño de buffer de eventos	Tamaño máximo de los datos que Log Collector extrae del origen de eventos en cada solicitud. El valor válido es un número en el rango de **0** a **511 Kilobytes**. Este valor se especifica en **kilobytes**.
Resultado de evento demasiado grande	Indica a Log Collector qué hacer si un evento es demasiado grande para el búfer de eventos.
Máximo de datos de eventos	Tamaño máximo de los datos de eventos que se incluirán en la salida. El valor válido es un número en el rango de **0** a **511 Kilobytes**. Este valor se especifica en **kilobyte**s o **megabytes**. • 1 kilobyte - 100 megabytes • 0 = no se incluyen datos de eventos en la salida.
Máximo de eventos por ciclo	La cantidad máxima de eventos por ciclo de sondeo (cuántos eventos se recopilan por ciclo de sondeo).

Característica	Descripción
Intervalo de sondeo	El intervalo (cantidad de tiempo en segundos) entre cada encuesta. El valor predeterminado es **180**. Por ejemplo, si especifica 180, el recopilador programa un sondeo del origen de eventos cada 180 segundos. Si aún se está realizando el ciclo de sondeo anterior, esperará hasta que ese ciclo termine. Si está sondeando una gran cantidad de orígenes de eventos, es posible que el sondeo tarde más de 180 segundos en comenzar porque los subprocesos están ocupados.
Depurar	**Precaución:** Habilite la depuración (defina este parámetro en Activado o Detallado) solamente si hay un problema en un origen de eventos y necesita investigarlo. La activación de la depuración afectará negativamente el rendimiento del Log Collector. Activa o desactiva el registro de depuración del origen de eventos. Los valores válidos son: • **Apagado** = (predeterminado) desactivado • **Encendido** = activado • **Detallado** = activado en el modo detallado: agrega a los mensajes información del hilo de ejecución e información contextual del origen. Este parámetro esta diseñado para depurar y monitorear problemas aislados en la recopilación de orígenes de eventos. Si cambia este valor, el cambio se implementa inmediatamente (no es necesario reiniciar). Limite la cantidad de orígenes de eventos para los que utiliza depuración Detallada para minimizar el impacto en el rendimiento.
Cancelar	Cierra el cuadro de diálogo sin agregar el origen de eventos de Windows existente.
OK	Agrega los valores de los parámetros actuales como un nuevo origen de eventos

Solucionar problemas de la recopilación de Windows existente y NetApp

En este tema se señalan posibles problemas que puede encontrar en la recopilación de Windows heredado (LWC) y las soluciones que se sugieren para ellos.

Solucionar problemas de la recopilación de Windows existente y NetApp

En general, se reciben mensajes de registro más confiables cuando se desactiva SSL.

Problemas relacionados con el reinicio del protocolo

Problema	Causas posibles	Soluciones
El protocolo de recopilación de Windows heredado se reinicia, pero Security Analytics no recibe eventos.	El servicio logcollector está detenido.	Reinicie el servicio **logcollector**. 1. Inicie sesión en el **Remote Collector de Windows heredado**. 2. Vaya a **Inicio > Herramientas administrativas > Programador de tareas** y haga clic en **Biblioteca del Programador de tareas**. 3. En el panel derecho, busque la tarea **restartnwlogcollector** y asegúrese de que esté en ejecución. 4. Si no lo está, haga clic con el botón secundario en **restartnwlogcollector** y seleccione **Ejecutar**.

Problemas relacionados con la instalación

Si ve cualquiera de los siguientes mensajes en **MessageBroker.log**, es posible que existan problemas.

Mensajes de registro	Cualquier mensaje que contenga “rabbitmq”
Causa posible	Es posible que el servicio RabbitMQ no esté en ejecución. Puede que el puerto **5671** no esté abierto.
Soluciones	Asegúrese de que el servicio RabbitMQ esté en ejecución. Asegúrese de que el puerto **5671** esté abierto.

Mensajes de registro	Error: adición de la cuenta de usuario logcollector. Error: adición de la etiqueta de administrador a la cuenta logcollector. Error: adición del vhost de logcollection. Error: configuración de permisos para la cuenta logcollector en todos los vhosts.
Causa posible	**rabbitmq-server** no estaba en ejecución cuando el instalador intentó crear usuarios y vhosts.

Soluciones	Asegúrese de que el servicio **RabbitMQ** esté en ejecución y ejecute manualmente los siguientes comandos.
	`rabbitmqctl -q add_user logcollector netwitness`
	`rabbitmqctl -q set_user_tags logcollector administrator`
	`rabbitmqctl -q add_vhost logcollection`
	`rabbitmqctl -q set_permissions -p / logcollector ".*" ".*" ".*"`
	`rabbitmqctl -q set_permissions -p logcollection logcollector ".*" ".*" ".*"`

Problemas relacionados con el script de la federación de Windows heredado

Si ve cualquiera de los siguientes mensajes en el registro del script de la federación, es posible que existan problemas.

Problema	Posibles síntomas	Soluciones
El script de la federación se inició, pero el servicio LWC quedó inactivo.	El registro de Security Analytics muestra excepciones debido a una falla de la conexión con el recopilador de Windows heredado.	Este problema se soluciona automáticamente después del reinicio del servicio de Windows heredado.

LWC está en ejecución, pero el servicio RabbitMQ está inactivo o se está reiniciando.	El archivo de registro de la federación en Windows heredado muestra un mensaje de error sobre la inactividad del servicio RabbitMQ.
	El archivo de registro que se debe revisar es: **C:\NetWitness\ng\logcollector**
	Se registra el siguiente mensaje de error cuando RabbitMQ no está en ejecución:
	`"Unable to connect to node logcollector@localhost: nodedown"`
	Se muestran los siguientes mensajes de diagnóstico:
	`attempted to contact: [logcollector@localhost]`
	`logcollector@localhost:`
	`* connected to epmd (port 4369) on localhost`
	`* epmd reports: node 'logcollector' not running at all other nodes on localhost: ['rabbitmqctl-4084']`
	`* suggestion: start the node`
		Ejecute manualmente el script **federation.bat** en LWC.
		Para ejecutar manualmente el script **federate.bat**, realice los siguientes pasos:
		1. Vaya a la carpeta **C:\Program Files\NwLogCollector** donde está instalada la instancia de Windows heredado.
		2. Busque el archivo **federate.bat** en esta carpeta. Seleccione el archivo y haga clic con el botón secundario.
		3. Seleccione **Ejecutar como administrador**.
		4. Para monitorear el archivo de registro, navegue a **C:\NetWitness\ng\logcollector\federate.log** durante la ejecución del script **federate.bat**.
		Nota: Asegúrese de que el archivo de registro no muestre ningún error mientras se ejecuta el script.

El servicio RabbitMQ está inactivo en Security Analytics.	Las páginas de la interfaz del usuario de Security Analytics no funcionan.	Reinicie el servicio RabbitMQ.

No se muestran estadísticas de Estado y condición en la interfaz del usuario de Security Analytics.	El agente puppet no está en ejecución o está tardando bastante en publicar los certificados intercambiados.	Reinicie el agente puppet o espere varios minutos para completar el intercambio de los certificados.
El cliente recibe una notificación de Estado y condición o se muestra la siguiente alarma de Estado y condición: "Falla de comunicación entre el host maestro de Security Analytics y un host remoto" con el host de LWC como la IP remota.	1. El script **federate.bat** no se ejecutó correctamente. 2. Puppet agent no se ejecutó después de la ejecución correcta del script **federate.bat**.	1. Si la ejecución del script **federate.bat** no fue correcta, ejecútelo de forma manual como se describió anteriormente. 2. Si el script **federate.bat** se ejecutó correctamente y el agente puppet no realizó su ejecución programada, ejecútelo de forma manual mediante el siguiente comando en el servidor de Security Analytics: **puppet agent -t**

Instalar y actualizar el agente de SFTP

Descripción general

En este tema se indica cómo descargar el **agente de FTP seguro de RSA Security Analytics** y cómo realizar las modificaciones correspondientes para la recopilación de registros.

Debe utilizar el protocolo SFTP para cargar eventos desde orígenes de eventos de archivo a Log Collector. Consulte Guía de configuración del protocolo de recopilación de archivos para obtener más detalles acerca de la configuración de orígenes de eventos.

RSA recomienda utilizar el **agente de FTP seguro de RSA Security Analytics**, el cual puede descargar desde el sitio web de servicio al cliente de RSA SecurCare Online (SCOL). El agente de SFTP en SCOL consta de los archivos binarios para instalar el agente de SFTP. Estos binarios se configuran como se describe aquí, en este documento. Como parte del proceso de instalación, se genera un par de claves pública/privada.

Debe crear a una cuenta de usuario para la transferencia de archivos en cada origen de eventos de Windows que envía datos al Log Collector. Puede asignar cualquier nombre a las cuentas, pero la documentación supone que las cuentas se denominan **sftp**.

Instalar y actualizar el agente de SFTP de SA

Realice los siguientes pasos para configurar el agente de SFTP de SA en el origen de eventos:

I. Ejecute Microsoft Visual C++ 2005 Redistributable Package en el origen de eventos.

II. Instale el agente de SFTP de SA en el origen de eventos.

III. Genere un par de claves en el origen de eventos e importe la clave pública a Log Collector.

IV. Seleccione la cuenta de usuario para ejecutar el servicio de agente de SFTP de SA.

V. Almacene en caché las claves para la conexión.

VI. Configure el agente de SFTP de SA en el origen de eventos.

VII. Inicie el servicio de agente de SFTP de SA desde el panel de control de Servicios de Windows.

Ejecutar Microsoft Visual C++ 2005 Redistributable Package

Para ejecutar Microsoft Visual C++ 2005 Redistributable Package:

1. Descargue cualquiera de los siguientes paquetes al origen de eventos:
   - Microsoft Visual C++ 2005 Redistributable Package (x86):

     http://www.microsoft.com/downloads/details.aspx?familyid=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en
   - Microsoft Visual C++ 2005 SP1 Redistributable Package (x86):

     http://www.microsoft.com/downloads/details.aspx?familyid=200B2FD9-AE1A-4A14-984D-389C36F85647&displaylang=en
2. Haga clic en **Descargar** y ejecute **vcredist_x86.exe**.

Instalar el agente de SFTP de SA en el origen de eventos

Precaución: Debe usar el agente de FTP seguro de RSA Security Analytics.

Para instalar el agente de SFTP de SA en el origen de eventos:

1. Busque Agente de FTP seguro de RSA Security Analytics en RSA SecurCare Online (SCOL).
2. Seleccione su SO:
   - Para un cliente Windows, haga clic en **Agente de FTP seguro** para descargar los binarios.
   - Para un cliente Unix, haga clic en **Agente de FTP seguro de Unix** para descargar los binarios.
3. Complete el resto de estas instrucciones para instalar el agente de SFTP en el origen de eventos.

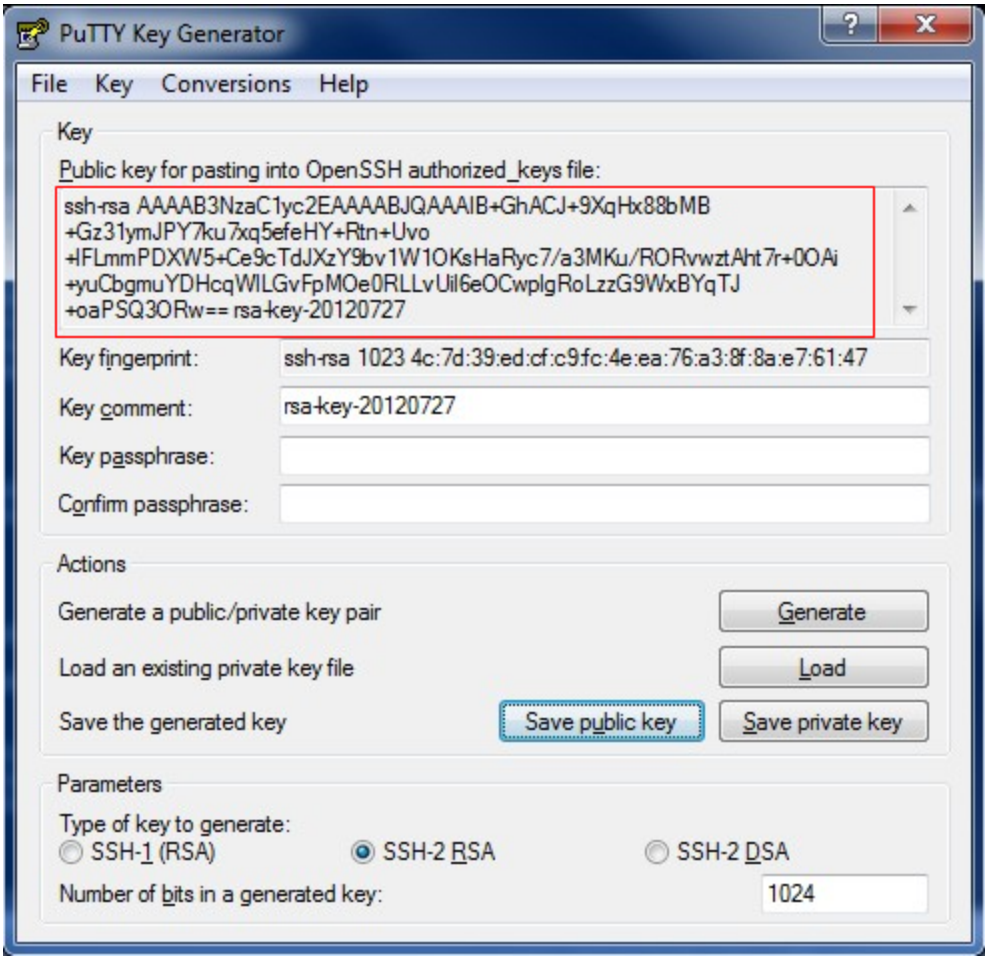
Generar un par de claves en el origen de eventos e importar la clave pública a Log Collector

Para generar un par de claves en el origen de eventos e importar la clave pública a Log Collector:

1. Haga doble clic en **puttygen.exe** en el directorio **C:\sasftpagent**. Se inicia PuTTY Key Generator.
2. Seleccione **SSH2 RSA** como el tipo de clave que desea generar.

3. Haga clic en **Generar** y mueva el mouse en la ventana de PuTTY Key Generator hasta que se genere la clave.
4. Guarde la clave privada:
   a. Haga clic en **Guardar clave privada**.
   b. Seleccione **Sí** para no usar una frase de contraseña.
   c. Guarde el archivo como **private.ppk** en el directorio **C:\sasftpagent**.
5. Agregue la clave pública en Log Collector:
   a. Copie la clave pública en el búfer para poder pegarla en el parámetro en Security Analytics, como se describe en el paso 5b.

      En el siguiente ejemplo, la clave pública se muestra dentro de un recuadro rojo.



   b. Pegue la clave pública desde el búfer al parámetro Clave del protocolo SSH del origen de eventos en Security Analytics. Para obtener detalles, consulte el tema **Configurar orígenes de eventos de archivo** de la *Guía de recopilación de registros de RSA Security Analytics*.

6. Cierre **puttygen**.

Seleccionar la cuenta de usuario para ejecutar el servicio de agente de SFTP

Después de importar la clave pública al Log Collector, debe realizar lo siguiente:

- Seleccione una cuenta de usuario existente, o
- Cree una cuenta de usuario en el origen de eventos para ejecutar el servicio de agente de SFTP.

Para crear una cuenta de usuario en el origen de eventos:

1. En el menú **Inicio** de Windows, haga clic en **Programas > Herramientas administrativas > Usuarios y equipos de Active Directory**.
2. Haga clic en **Acción > Nuevo > Usuario** y cree un usuario nuevo a nombre del cual desea que se ejecute el servicio.

   Nota: La cuenta de usuario debe ser miembro del grupo de administradores local. También debe tener acceso a los archivos que se envían a Log Collector.

3. Modifique el servicio de agente de SFTP de SA de modo que use esta cuenta de usuario:
   a. Haga clic con el botón secundario en Agente de SFTP de SA y seleccione **Propiedades**.
   b. Haga clic en la pestaña **Inicio de sesión**.
   c. Seleccione **This account**.
   d. Escriba el nombre de usuario y la contraseña de la cuenta que está usando para ejecutar el servicio de agente de SFTP.
   e. Haga clic en **Aceptar**.
4. Cierre la sesión en el origen de eventos e inicie sesión nuevamente con la cuenta de usuario nueva.

   Nota: La cuenta de usuario con la cual se ejecutan estos pasos debe ser la del usuario que ejecuta el servicio.

5. Almacene en caché las claves para la conexión.

Almacenar en caché las claves para la conexión

Tras crear la cuenta de usuario con la cual se ejecuta el servicio de agente de SFTP de SA, debe almacenar en caché las claves para conectar el origen de eventos al Log Collector.

Para almacenar en caché las claves en el origen de eventos, realice lo siguiente:

1. Inicie sesión en la máquina con la cuenta que seleccionó para el servicio de agente de SFTP de SA.
2. Ejecute el siguiente comando desde el directorio **C:\sasftpagent**:

   psftp -i ***private.ppk*** -l sftp -v ***ngc-ip***

   donde:

   - ***private.ppk*** es el archivo que contiene la clave privada
   - ***ngc-ip*** es la dirección IP de Log Collector

   En el sistema se muestra un mensaje que indica que la clave del host del servidor no está en el registro.
3. Escriba **Y** y presione INTRO para confiar en el host.
4. En el indicador `psftp`, escriba **quit** y presione INTRO.

Ahora, la clave está almacenada en la caché en el registro del origen de eventos.

Configurar el agente de SFTP de SA en el origen de eventos

Para configurar el agente de SFTP de SA en el origen de eventos:

1. Vaya al directorio de instalación del agente de SFTP de SA (el directorio predeterminado es **C:\sasftpagent**).
2. Los archivos de configuración de ejemplo están dentro del directorio sasftpagent. El nombre de estos ejemplos se determina según el origen de eventos correspondiente. Por ejemplo, el archivo de configuración de SFTP de ejemplo del origen de eventos de Microsoft IIS se denomina **sftpagent.conf.microsoftiis**.
3. Cree el archivo `C:\sasftpagent\sftpagent.conf` y use el archivo de ejemplo correspondiente que configurará de acuerdo con la siguiente leyenda.

Parámetro	Descripción
agent.logginhost	Nombre de host o dirección IP de Log Collector al cual se enviarán los registros.
dir0	Ubicación de los archivos de registro para los orígenes de eventos en el sistema Windows local.
dir0.filespec	Archivos que desea enviar al Log Collector desde la ubicación anterior. En este ejemplo, cualquier archivo con la extensión ***.log** se envía al Log Collector.

Parámetro	Descripción
dir0.interval	Cantidad de tiempo entre transferencias de archivos. Puede modificar este valor.
dir0.has_header	Si el registro tiene un encabezado en la parte superior del archivo de registro, configure este valor en **true**. Si el archivo de registro no tiene un encabezado, configúrelo en **false**.
dir0.compression	El valor puede ser **true** o **false**. • Configúrelo en **true** para utilizar compresión. Los archivos de registro se comprimen y se envían en formato **.gz** al Log Collector. • Configúrelo en **false** para no utilizar compresión de archivos.
dir0.enabled	El valor se configura en **true**. No modifique este valor porque si lo cambia a **false**, no enviará ningún archivo de registro al Log Collector.
dir0.ftp	***Log Collector-ip-address***,sftp,sftp,***publickey***,***//upload/event-source-type/filedirectory*** Esta ruta se puede encontrar en el Log Collector dentro de la siguiente ruta: /var/netwitness/logcollector/upload/ Al final de esa ruta está agregado el valor que usted ingresa para el parámetro **Directorio de archivos** cuando crea el origen de eventos en la interfaz del usuario de Security Analytics.
dir0.delete_ after_read	El valor es **true** o **false**. El valor **true** elimina los archivos después de que el agente envía los registros al destino.

4. Guarde el archivo y compruebe que el nombre permanezca sin cambios (es decir, asegúrese de que no se agregue una extensión **.txt** al archivo).

Iniciar el servicio de agente de SFTP de SA desde el panel de control de Servicios de Windows

1. Escriba `services.msc` en la línea de comandos.
2. Inicie el servicio de agente de SFTP de SA.

Archivos de configuración de ejemplo

Los siguientes son ejemplos del archivo sftpagent.conf para varios orígenes de eventos.

Un archivo de configuración de ejemplo para configurar un servidor de Microsoft IIS:

```
agent.logginghost=<ngc-ip>
dir0=C:\inetpub\logs\LogFiles\W3SVC1
dir0.filespec=*.log
dir0.interval=60
dir0.has_header=false
dir0.compression=false
dir0.enabled=true
dir0.ftp=<ngc-ip>,>,sftp,sftp,publickey,//upload/iis_tvm/IIS
dir0.delete_after_read=true
```

Un archivo de configuración de ejemplo para configurar un origen de eventos de Apache:

```
dir0=C:\Program Files\Apache Group\Apache2\logs
dir0.filespec=access_log*
dir0.interval=60
dir0.has_header=false
dir0.compression=true
dir0.enabled=true
dir0.ftp=enVisionIP,nic_sshd,publickey,APACHE_10.10.31.155
```

Solucionar problemas del agente de SFTP de SA

Para solucionar problemas, primero debe detener el servicio y, a continuación, ejecutar un comando para ver los mensajes de depuración.

Para solucionar problemas del agente de SFTP de SA:

1. Detenga el servicio del agente de SFTP de SA en la ventana Servicios de Windows.
2. Abra un nuevo shell de comandos y cambie al directorio de instalación del agente de SFTP de SA.
3. Escriba:

   ```
   sasftpagent -v
   ```

4. Revise los mensajes de depuración que se muestran.

En las siguientes secciones se describen algunos mensajes posibles y cómo solucionar los problemas correspondientes.

Error al abrir el archivo de configuración del agente de SFTP

Si falta el archivo de configuración de SFTP, recibirá el siguiente error:

Error al abrir el archivo: sftpagent.conf

Para resolver el problema, busque o cree nuevamente el archivo y transfiéralo al directorio de instalación del agente de SFTP de SA.

Problemas relacionados con la clave privada

Si la generación de los archivos de clave presenta un problema, es posible que reciba un mensaje similar al siguiente:

> **Leyendo el archivo de clave privada “private.ppk”**
> **No se puede usar este archivo de clave (no se puede abrir el archivo)**
> **No se puede usar el archivo de clave “private.ppk” (no se puede abrir el archivo)**

O bien, es posible que reciba un mensaje como el siguiente si la clave presenta un problema:

> **Se ofreció una clave pública**
> **El servidor rechazó nuestra clave**
> **El servidor rechazó la clave pública**

Para resolver el problema, vuelva a generar los pares de claves y migre la clave al Log Collector.

Configurar la transferencia de archivos del script de shell de SFTP

Descripción general

Use el script de shell **sasftpagent.sh** para transferir datos del registro basados en texto desde sistemas Linux. Este script toma segmentos de datos de archivos de registro activos, pero solo transfiere los datos nuevos cada vez que se ejecuta.

Programe el script en cron para que se ejecute con la frecuencia que desee enviar datos del registro a RSA Security Analytics Log Collector. El script usa el protocolo SFTP o SCP para transferir los datos.

Tenga en cuenta lo siguiente:

- Todas las conexiones se inician desde el sistema a Security Analytics.
- El script se ejecuta en todos los sistemas y shells Unix/Linux que cumplen con POSIX.

  Nota: Debe usar OpenSSH versión 4.4p1 o superior.

- RSA recomienda configurar un trabajo cron para ejecutar el script en los intervalos de tiempo especificados. Sin embargo, si configura un trabajo cron, asegúrese de ejecutarlo como un usuario que tenga acceso a los registros que se deben enviar a Security Analytics.

Este tema contiene la siguiente información:

- Mejoras en la versión 3 del agente
- Instrucciones para actualizar el agente: siga estos pasos si actualmente está ejecutando la versión 2.7 del agente
- Instrucciones para instalar el agente: siga estos pasos si va a descargar el agente por primera vez
- Detalles de los parámetros del script de shell
- Instrucciones para configurar RSA Security Analytics Log Collector de modo que reciba archivos de registro

Debe ejecutar los siguientes pasos para completar la instalación y la configuración del agente:

I. Instale o actualice al agente, en función de si lo está ejecutando o no.

II. Configure RSA Security Analytics Log Collector para que reciba archivos de registro.

Mejoras en la versión 3

- El script se ejecuta en todos los sistemas y shells Unix/Linux que cumplen con POSIX.
- Espera la configuración en `/etc/rsa/sasftpagent.conf`.
- Recomienda al usuario mantener la configuración por separado del origen del script. Si el usuario no cumple con esto, se registra una advertencia.
- El estado persistente se escribe en `/var/lib/rsa` de forma predeterminada.
- Se mejoró la interacción del usuario, como se indica a continuación:
  - Compatibilidad con la ejecución del script sin privilegios de raíz.
  - Ahora se pueden configurar muchos aspectos del agente, como la ejecución desde cualquier lugar y la creación de un directorio de estado persistente en cualquier lugar. Por ejemplo, los usuarios no raíz pueden hacer persistir la información de estado en su directorio principal mediante la especificación de un directorio de estado persistente alternativo en el archivo de configuración.
  - Una configuración especificada en el directorio principal de un usuario no raíz (p. ej., `~/sasftpgent.conf`) se recupera automáticamente durante la ejecución como un usuario no raíz.
  - Se agregaron opciones de la línea de comandos (`-C` o `--config`) para dirigir al agente a la configuración personalizada.
- Los registros se escriben en `/var/log/rsa/sasftpagent.log`. Se introdujeron niveles de registro, de modo que los registros se pueden filtrar para entradas de advertencia, error y graves como ayuda para la solución de problemas. Ahora, estas entradas del registro se pueden usar para solucionar problemas después de los hechos.
- Si el usuario olvida editar la configuración, se genera una entrada del registro de carácter grave. La entrada contiene un mensaje claro que indica que el usuario debe editar la configuración antes de que se pueda usar el script.

Actualizar el agente

Si usó una versión de **sasftpagent.sh** anterior a la versión 3, debe seguir las instrucciones de esta sección para realizar la actualización a la versión más reciente.

Los pasos principales son los siguientes:

I. Descargue el agente nuevo desde SCOL.

II. Transfiera la información de la configuración a `/etc/rsa/sasftpagent.conf`.

III. Descargue el script **mvpersinfo.sh**.

IV. Ejecute el script **mvpersinfo.sh** para transferir la información persistente a la ubicación que utilizaba la versión 3.

V. Ejecute la versión 3 del agente.

Transferir la información de la configuración

En la versión 2.7, la configuración del usuario se especificaba en una de las dos ubicaciones siguientes:

- La configuración se puede haber editado en línea dentro de `/usr/local/sa/sasftpapgent.sh` (o dondequiera que haya colocado el script).
- La configuración se puede haber especificado por separado; dondequiera que se establezca el parámetro **CONFIG_FILE** en el script sasftpagent.sh.

Debe transferir cualquier parámetro que haya editado dentro del script o que haya especificado en el archivo de configuración por separado a un archivo aparte en la siguiente ubicación: `/etc/rsa/sasftpagent.conf`.

Los siguientes son los parámetros que los usuarios suelen cambiar durante la configuración:

- SA
- DATA_DIRECTORY
- FILESPEC
- FLAG_REMOVE_AFTER_SEND (solo se configura si se desea quitar los archivos de datos automáticamente después de su transferencia a Log Collector).

Transferir la información persistente

En la versión 2.7, la información de estado persistente se mantiene en el directorio `/usr/local/sa` de forma predeterminada. También se puede especificar en el parámetro **PERSINFO_DIRECTORY**.

El directorio de información persistente contiene archivos de rastreo que incluyen la cantidad de líneas, para cada archivo de datos, que ya se transfirieron a Log Collector. El agente utiliza esta información para determinar las líneas de cada archivo que son nuevas desde la última vez que se ejecutó. A continuación, transfiere solo los datos nuevos y actualiza los archivos de rastreo según corresponda.

Es importante transferir estos archivos a la ubicación nueva antes de que se ejecute la versión 3.0.1 del agente. RSA proporciona un script, **mvpersinfo.sh**, para transferir la información persistente.

Ejecutar el script de transferencia

Realice los siguientes pasos para transferir la información persistente a su ubicación nueva:

1. Copie **mvpersinfo.sh** al sistema donde ejecuta la versión 2.7 del agente.
2. Abra **mvpersinfo.sh** con un editor de texto y compruebe que **OLD_PERSINFO_DIRECTORY** esté configurado en el valor establecido para **PERSINFO_DIRECTORY** en la configuración de 2.7.
3. Ejecute el script mediante el siguiente comando:

   ```
   sh mvpersinfo.sh
   ```

Si no hay ningún error y la ejecución es correcta, el script no genera ninguna salida.

Comprobar la transferencia de los archivos

Después de ejecutar el script, puede comprobar la transferencia correcta mediante el siguiente procedimiento:

1. Ejecute el siguiente comando para obtener una lista de los archivos de rastreo antiguos:

   ```
   find /usr/local/sa -name "*-*last.line"
   ```
2. Ejecute el siguiente comando para obtener una lista de los archivos de rastreo nuevos:

   ```
   find /var/lib/rsa/sasftpagent -name "*-*last.line"
   ```
3. Compare la salida de los dos comandos. La salida debe ser similar y tener como única diferencia las rutas a los archivos. El siguiente es un ejemplo de los resultados de la ejecución de estos comandos después de la transferencia de los archivos persistentes:

```
$ find /usr/local/sa -name "*-*last.line"

    /usr/local/sa/opt/log/bar.log-sa.last.line
    /usr/local/sa/opt/log/foo.log-sa.last.line
    usr/local/sa/var/log/foo.log-sa.last.line
    /usr/local/sa/var/log/fob.log-sa.last.line

$ find /var/lib/rsa/sasftpagent -name "*-*last.line"

    /var/lib/rsa/sasftpagent/track/opt/log/bar.test-last.line
    /var/lib/rsa/sasftpagent/track/opt/log/foo.test-last.line
    /var/lib/rsa/sasftpagent/track/var/log/foo.test-last.line
    /var/lib/rsa/sasftpagent/track/var/log/fob.test-last.line
```

Instalar y configurar el agente

Si no está realizando la actualización desde una versión anterior del agente, siga los pasos de esta sección para descargar, instalar y configurar el agente.

I. Descargar el agente

II. Crear o configurar una cuenta de usuario para ejecutar el agente

III. Crear y actualizar el archivo de configuración

IV. Programar el agente para que se ejecute periódicamente: Configure cron en el programador del SO para automatizar la ejecución del script en el intervalo deseado.

Descargar el agente

Siga estos pasos para descargar el agente de SFTP de SA (**sasftpagent.sh**) desde SCOL.

1. Inicie sesión en RSA SecurCare Online (SCOL).
2. En el cuadro Buscar, ingrese **Agentes de SFTP de RSA Security Analytics**.
3. Seleccione la página que devuelve la búsqueda, Agentes de SFTP de RSA Security Analytics.
4. Haga clic en **Agente de SFTP de Unix de RSA Security Analytics** y guarde el archivo en cualquier lugar en su sistema de archivos.
5. Configure permisos de ejecución en el archivo **sasftpagent.sh**. Por ejemplo, ejecute el siguiente comando:

   chmod 755 /usr/local/sa/sasftpagent.sh

Crear o configurar una cuenta de usuario para ejecutar el agente

La cuenta de usuario que ejecuta el agente necesita permiso de lectura a DATA_DIRECTORY que contiene los registros, y acceso de lectura/escritura a PERSINFO_DIRECTORY que usa el agente para el almacenamiento persistente.

Crear y actualizar el archivo de configuración

Cree el archivo de configuración aquí: `/etc/rsa/sasftpagent.conf`. Si no tiene un archivo de configuración, copie el archivo de script (**sasftpagent.sh**) y quite todo, salvo los parámetros de configuración. Actualice el archivo de configuración con la información correspondiente a su ambiente. Como referencia, consulte la tabla Parámetros a continuación.

Si está ejecutando el script por primera vez, ejecute el siguiente comando, donde ***collector-IP*** es la dirección IP de Security Analytics Log Collector:

sftp ***collector-IP***

Precaución: Es importante ejecutar este comando como el mismo usuario que lo ejecutará cuando esté automatizado.

Parámetros del script de shell

En la siguiente tabla se describen los parámetros más importantes que debe establecer cuando configure el script.

Parámetro	Valores	Descripción
SA	Nombre o dirección IP	El nombre o la dirección IP del host de RSA Security Analytics Log Collector.
DATA_DIRECTORY	Ruta o rutas del directorio, separadas por dos puntos (:).	El origen local de los datos del registro. Por ejemplo: DATA_DIRECTORY=/var/log:/var/log/audit Puede especificar una o más carpetas. **Nota:** Los nombres de archivo que proporciona en el parámetro FILESPEC se buscan en todas las carpetas que especifica.
FILESPEC	Nombre o nombres de archivo, separados por dos puntos (:).	Máscara de archivo que coincide con los archivos de registro que procesará el script. **Nota:** El script admite datos de texto línea por línea. Por lo tanto, .xml, .zip, .gz, .exe y otros formatos que no son de texto no se admiten. Por ejemplo, para procesar todos los archivos de la carpeta: FILESPEC=isi_webui.log:smb.log:/etc/logs/*.* **Nota:** Los archivos que especifica pueden residir en distintas carpetas. Asegúrese de enumerar todas las carpetas necesarias en el parámetro **DATA_DIRECTORY**.
SA_DIRECTORY	El nombre del directorio del host de Security Analytics Log Collector	El nombre de la carpeta de destino. Por ejemplo: /upload/apache/muditapache

Parámetro	Valores	Descripción
TRANSFER_METHOD	**SFTP** o **SCP**	SFTP es el protocolo de transferencia predeterminado (y recomendado)
USEHEAD	Un entero no negativo que representa la cantidad de líneas del encabezado	La cantidad de líneas en cada archivo de registro que se considerarán como un encabezado que se debe transferir a Log Collector en cada transferencia. Puede configurarlo en 0 para indicar que no hay líneas de encabezado.
DEPTH	Un entero positivo que representa la cantidad de niveles de carpeta	Controla en cuántos niveles de profundidad busca registros el script en el DATA_DIRECTORY configurado. Se configura de forma predeterminada en **DEPTH=1**, con lo cual el script busca archivos de datos directamente en los directorios configurados en DATA_DIRECTORY, pero no en subcarpetas.
Configuración de SFTP y SCP		
USERNAME	**sftp**	Ajuste predeterminado para el demonio del protocolo SSH en la plataforma Security Analytics.
IDENTITY	Ruta del archivo	Ubicación de la clave privada que se utiliza para conectarse a Security Analytics. Para obtener instrucciones sobre la generación de claves, consulte Instalar y actualizar el agente de SFTP. El valor predeterminado es el siguiente: $HOME/.ssh/id_rsa

Información del script de configuración

Todos los ajustes de configuración se pueden cargar mediante un archivo de configuración por separado del script. Este archivo debe contener un ajuste y un valor por línea (excepto DATA_DIRECTORY y FILESPEC, que pueden contener varias entradas separadas por dos puntos).

El archivo de configuración debe estar en el directorio que asigna SA_DIRECTORY en el script de shell o en la ruta del shell que llama al script. SA_DIRECTORY se puede reemplazar en el archivo de configuración, aunque el script de shell intentará usar su propio ajuste de SA_DIRECTORY para abrir el archivo de configuración.

Por ejemplo, un archivo de configuración podría contener la siguiente información:

```
SA=10.31.246.168
DATA_DIRECTORY=/var/log/httpd
SA_DIRECTORY=/upload/apache/muditapache
USERNAME=sftp
FILESPEC=*_log*
FLAG_REMOVE_FILE_AFTER_SEND=no
```

Configure RSA Security Analytics Log Collector para que reciba archivos de registro

Antes de configurar el Log Collector, recuerde ejecutar el siguiente comando en cualquier origen de eventos nuevo desde el cual Security Analytics no haya recopilado registros anteriormente mediante SFTP o SCP:

sftp ***collector-IP***

donde ***collector-IP*** es la dirección IP de Security Analytics Log Collector.

Para configurar Security Analytics de modo que reciba archivos de registro:

1. En el origen de eventos Unix o Linux, ejecute el siguiente comando para generar el par de claves pública/privada:

   ssh-keygen -b 1024 -t rsa

   Este comando crea id_rsa en el formato OpenSSH que usa RSA Security Analytics. Si el sistema Linux crea el formato IETF SECSH de forma predeterminada, ejecute el siguiente comando para convertirlo:

   ssh-keygen -f ~/.ssh/id_rsa.pub -i

2. Agregue la clave pública al Log Collector, como se describe en Instalar y actualizar el agente de SFTP.