RSA NETWITNESS® SUITE

Guía de configuración de la recopilación de registros

para la versión 11.0

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

febrero 2018

Contenido

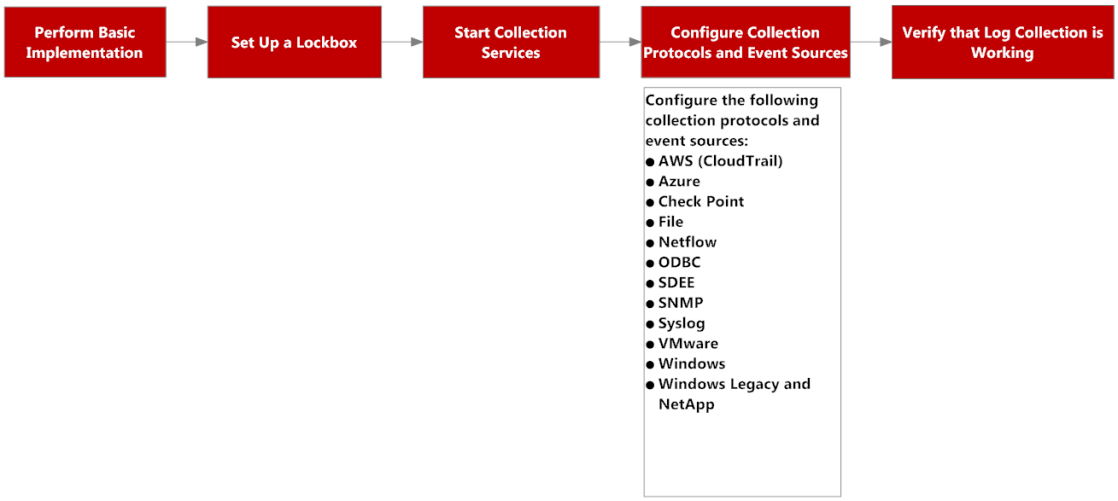
Acerca de recopilación de registros

En esta guía se describen los pasos generales y las subtareas para configurar la recopilación de registros de orígenes de eventos que incluyen:

- 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.
- Cómo configurar protocolos de recopilación individuales. Las instrucciones se encuentran en las secciones de recopilación de registros individuales.

Flujo de trabajo

Este flujo de trabajo contiene las tareas básicas necesarias para comenzar a recopilar eventos mediante la recopilación de registros.



Procedimiento general

De manera general, estos son los procedimientos que debe seguir para la recopilación de registros:

I. Agregar Local y Remote Collectors a RSA NetWitness Suite.

   Configurar un Log Collector localmente en un Log Decoder (es decir, un Local Collector). También puede configurar Log Collector en tantas ubicaciones remotas (es decir, Remote Collectors) como requiera una empresa. Para obtener más información, consulte Implementación básica.

II. Descargar el contenido más reciente de Live. Esta es una tarea que se realiza periódicamente, a medida que el contenido que se proporciona en Live se actualiza regularmente.

   LIVE es el sistema de administración de contenido de RSA NetWitness® Suite 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.

   También puede suscribirse al contenido de Live. Para obtener más información, consulte la *Guía de administración de servicios de Live*.

III. Configurar ajustes: configurar el Lockbox y los certificados.

   Para obtener más información, consulte Configurar un Lockbox y Configurar certificados.

IV. Configurar orígenes de eventos.

   Puede configurar todos los orígenes de eventos en la red para enviar su información de registro a RSA NetWitness Suite. Cada vez que agrega nuevos orígenes de eventos, debe realizar este procedimiento. Todas las guías de configuración de origen de eventos se encuentran en el espacio Orígenes de eventos compatibles de RSA en RSA Link.

V. Iniciar y detener servicios para los protocolos configurados. Ocasionalmente, es posible que deba detener y reiniciar los servicios en función de los nuevos orígenes de eventos que agrega a RSA NetWitness Suite.

VI. Verifique que la recopilación de registros funcione.

   Cada vez que configura un nuevo origen de eventos o agrega un nuevo protocolo de recopilación, debe verificar que se envían los registros correctos a RSA NetWitness Suite.

Arquitectura de recopilación de registros

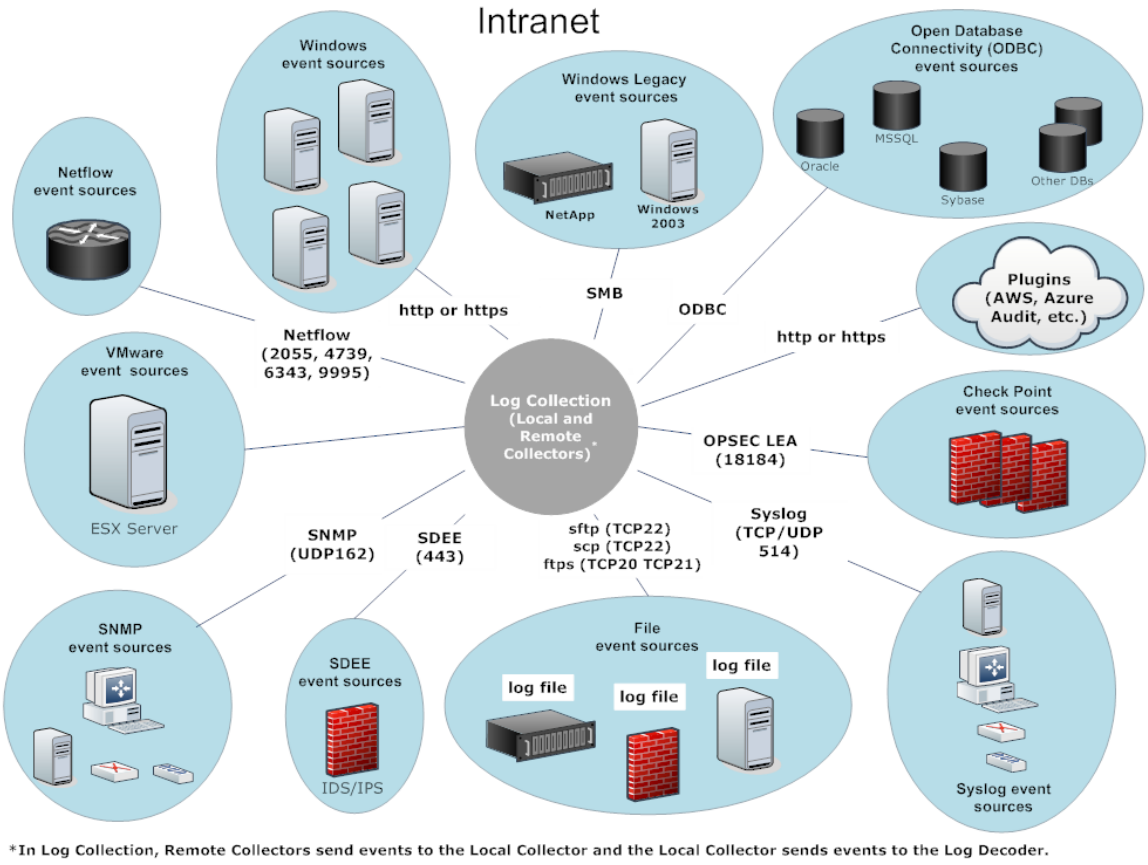
En este tema se describe cómo NetWitness Suite realiza la recopilación de registros.

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 implica la recopilación de eventos mediante NetWitness Suite Log Collector.



*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

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 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:

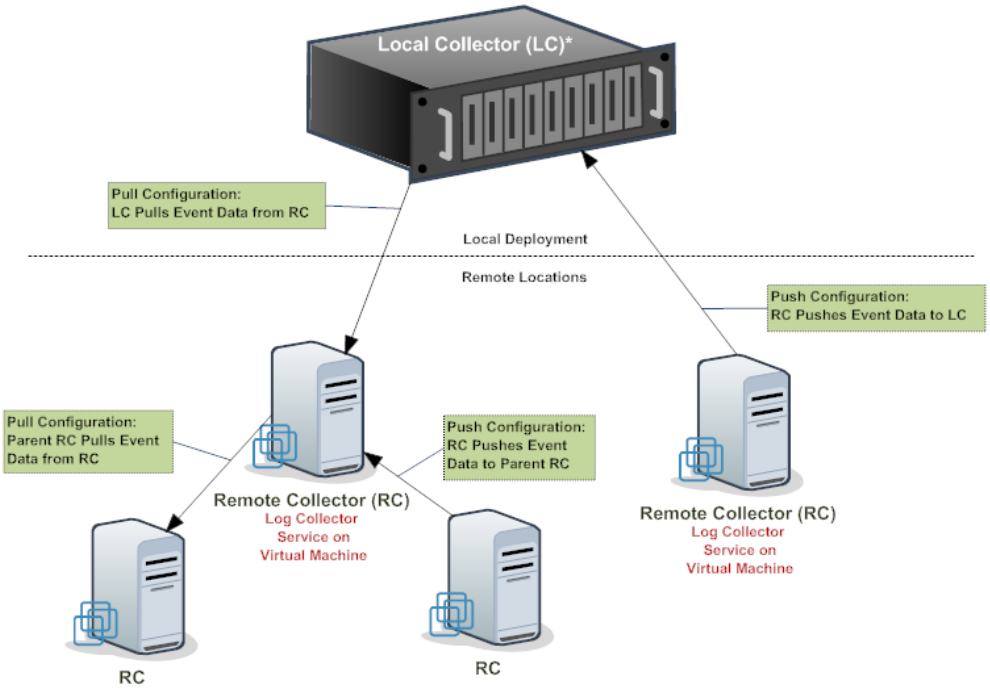
- **Extraer configuración**: en un Local Collector, seleccione los Remote Collectors desde los cuales desea extraer eventos.
- **Migrar configuración**: en un Remote Collector, seleccione el Local Collector al cual desea migrar eventos.

Nota: El caso de uso típico es Migrar. La extracción está disponible si tiene una DMZ en su ambiente. No se permite que los segmentos de red menos seguros establezcan conexiones a los segmentos de red más seguros. Con la extracción, el Log Collector (o Virtual Log Collector) en la red segura inicia la conexión al VLC en la red menos segura y, a continuación, se transfieren los registros sin romper las reglas de conexión.

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.

Además, puede configurar 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 desde uno o varios Remote Collectors.



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

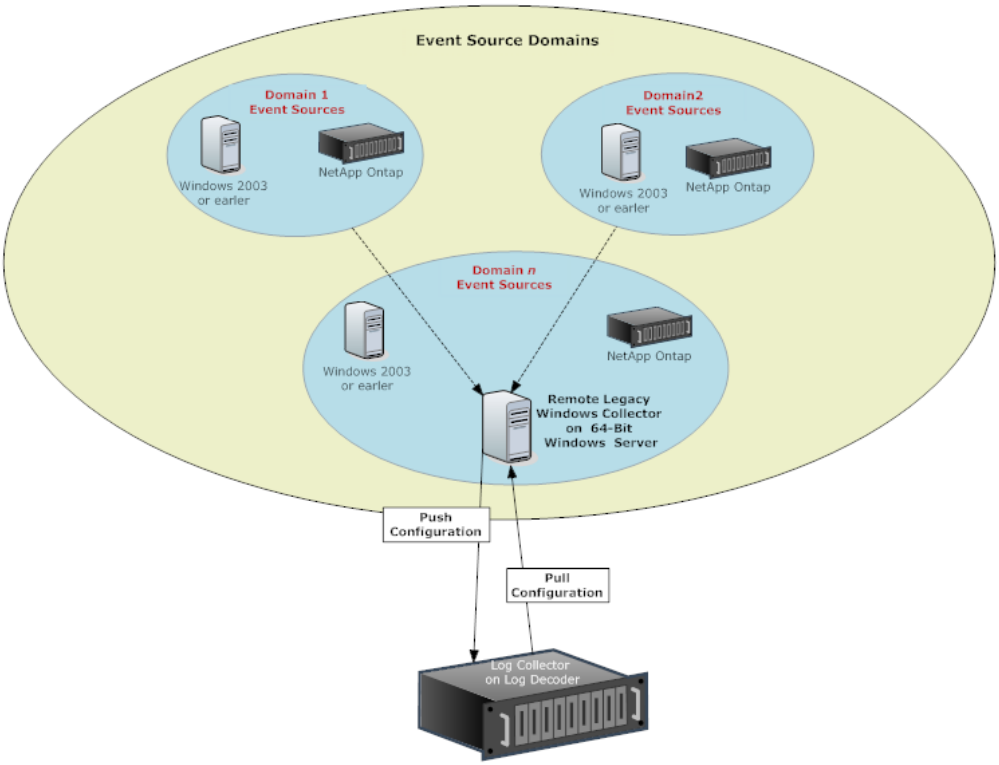
Remote Collector de Windows existente

El recopilador de Windows existente de RSA NetWitness® Suite es un Remote Log Collector (RC) que se basa en Microsoft Windows y que se puede instalar en un dominio de Windows.

Es compatible con la recopilación desde:

- Orígenes de eventos de Windows 2003 y versiones anteriores
- Archivos evt del host ONTAP de NetApp

En la siguiente figura se ilustra la implementación que se requiere para recopilar eventos desde orígenes de eventos de Windows existente.


Event Source Domains
Domain 1
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain2
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain n
Event Sources
Windows 2003
or earlier
NetApp Ontap
Remote Legacy
Windows Collector
on 64-Bit
Windows Server
Push
Configuration
Pull
Configuration
Log Collector
on Log Decoder

Configuración

Implementación básica

En este tema se indica cómo realizar la configuración inicial de Local Collectors y Remote Collectors.

Requisitos previos

Verificar que el Log Decoder esté configurado:

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

Funciones de los Local y Remote Collectors

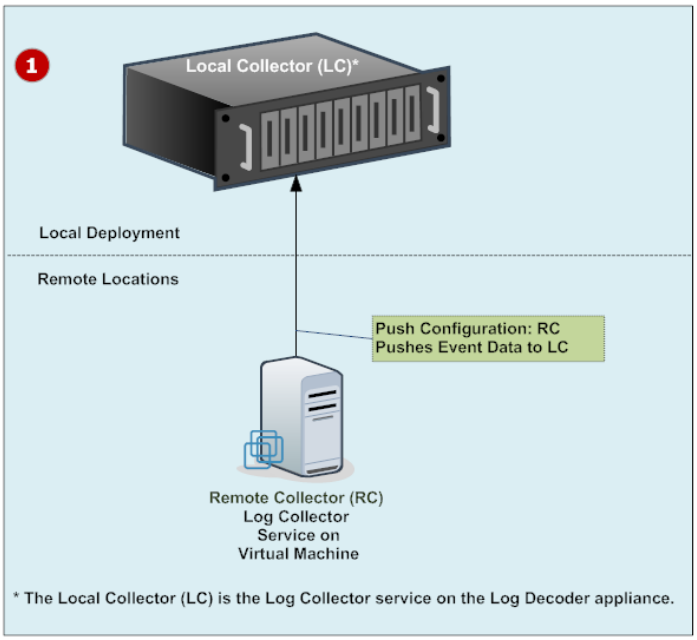
Un Local Collector (LC) es un servicio Log Collector que se ejecuta en un host de Log Decoder. En un escenario de implementación local, el servicio Log Collector se implementa en un host de Log Decoder con el servicio Log Decoder. La recopilación de registros de varios protocolos, como Windows, ODBC, 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

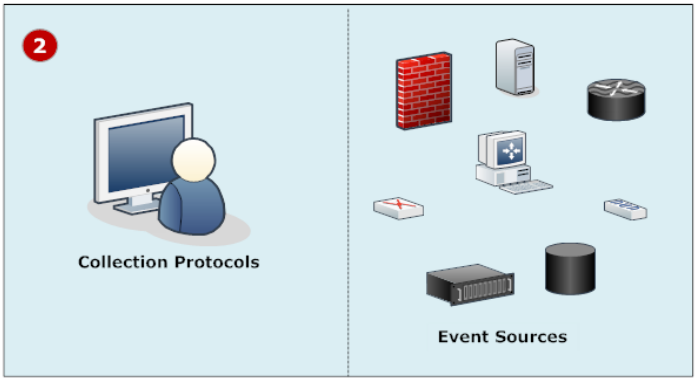
En la siguiente figura se ilustran las tareas básicas que debe realizar para implementar y configurar la recopilación de registros. Para implementar la recopilación de registros, debe configurar un Local Collector. También puede implementar uno o más Remote Collectors. Después de implementar la recopilación de registros, debe configurar los orígenes de eventos en NetWitness Suite y en los propios orígenes de eventos. En el siguiente diagrama se muestra el Local Collector con un Remote Collector que envía eventos al Local Collector.



1 Configure Local Collectors y Remote Collectors.

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

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



2 Configure orígenes de eventos:

- Configurar protocolos de recopilación en NetWitness Suite.
- Configurar cada origen de eventos para comunicarse con el NetWitness Suite Log Collector.

Adición de Local Collector y Remote Collector a NetWitness Suite

Para agregar un Local Collector y un Remote Collector a NetWitness Suite:

1. Vaya a **ADMIN > Servicios**.
2. Haga clic en + y seleccione **Log Collector** en el menú.

   Se muestra 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.

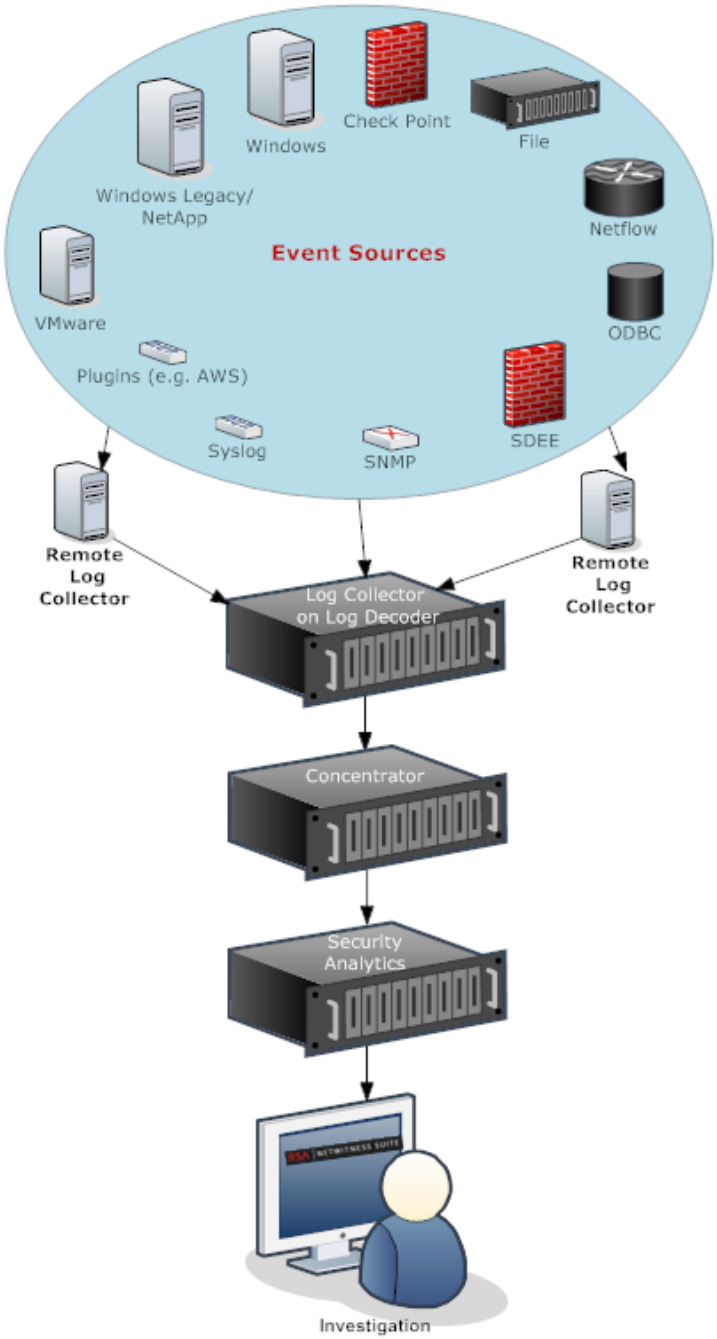
Configuración de la recopilación de registros

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. Vaya a **ADMIN > 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 Log Collection.
4. Defina los parámetros globales de recopilación de registros en la pestaña **General**.
5. Para un:
   - Local Collector,NetWitness Suite muestra la pestaña **Remote Collectors**. En esta pestaña, seleccione los Remote Collectors desde los cuales el Local Collector extrae eventos.
   - Remote Collector, NetWitness Suite muestra los **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 eventos**.
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 del registro 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 NetWitness Suite hasta Investigation.



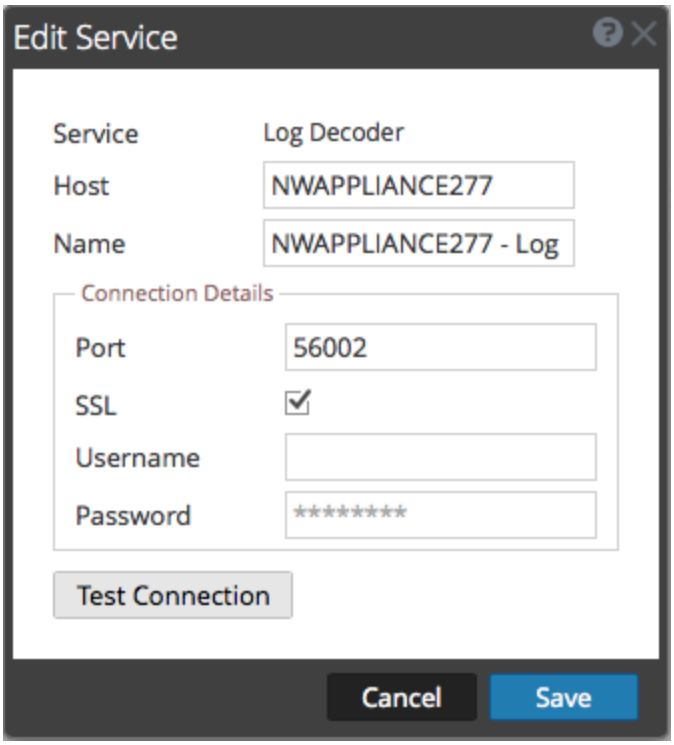
Aprovisionar Local y Remote Collectors

El servidor de NetWitness Suite verifica si un dispositivo tiene un servicio Log Decoder. Si no hay un servicio Log Decoder, se convierte en un Local Collector. Si no hay 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 Servidor de NW identifica un recopilador de Windows existente como un Remote Collector.

Para editar un Local Collector o un Remote Collector:

1. Vaya a **ADMIN > 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.

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 NetWitness Suite 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.
(Opcional) Contraseña	Escriba la contraseña del Local Collector.

4. Haga clic en **Probar conexión** para determinar si NetWitness Suite 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.

Este tema le indica cómo:

- Configurar Local Collector para extraer eventos de Remote Collector
  Si desea que un Local Collector extraiga eventos de Remote Collector, realice esta configuración en la pestaña Remote Collectors de la vista Configuración del Local Collector.
- Configurar 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 Local Collector de conmutación por error para 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 realiza una conexión correcta.

- Configurar la replicación

  Debe configurar varios grupos de destino para que NetWitness 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

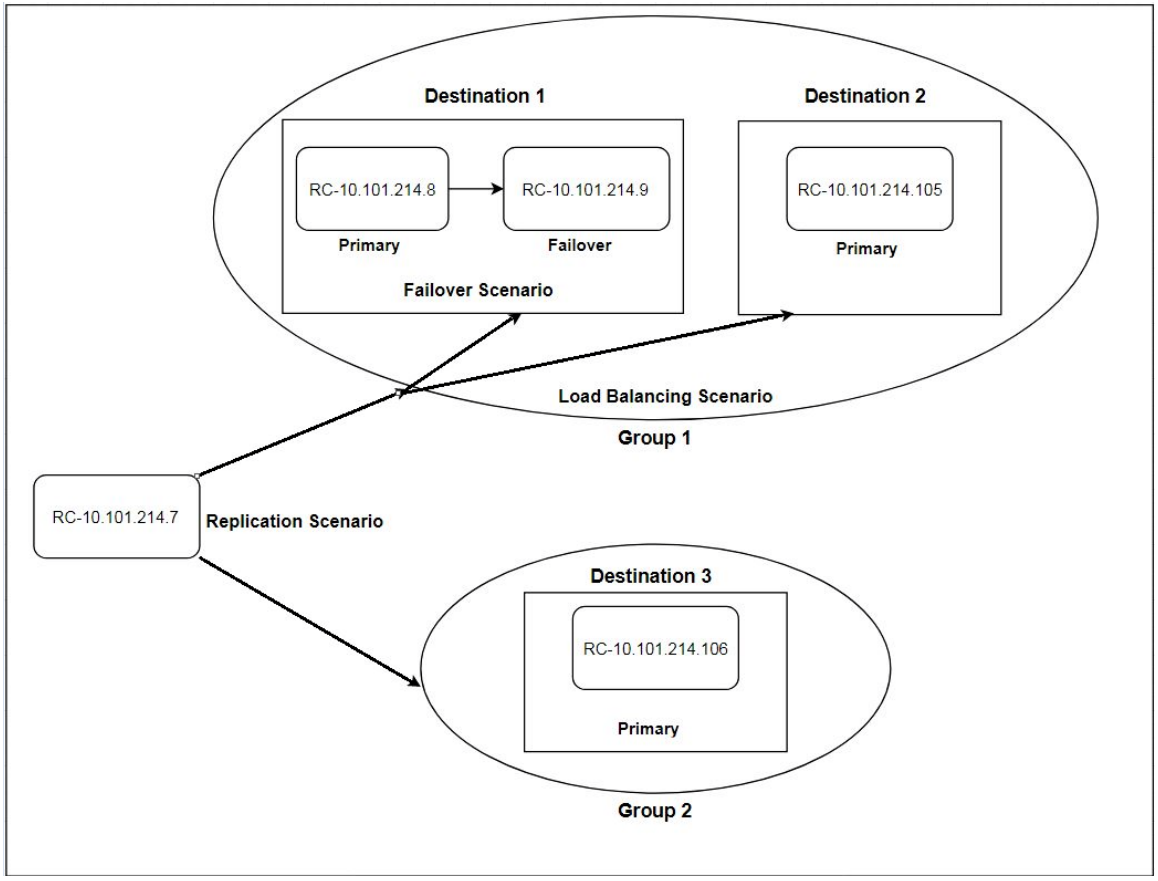
  Puede configurar una cadena de Remote Collectors para migrar datos de eventos a un Local Collector o puede configurar un Local Collector para extraer datos de eventos desde una cadena de Remote Collectors.

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

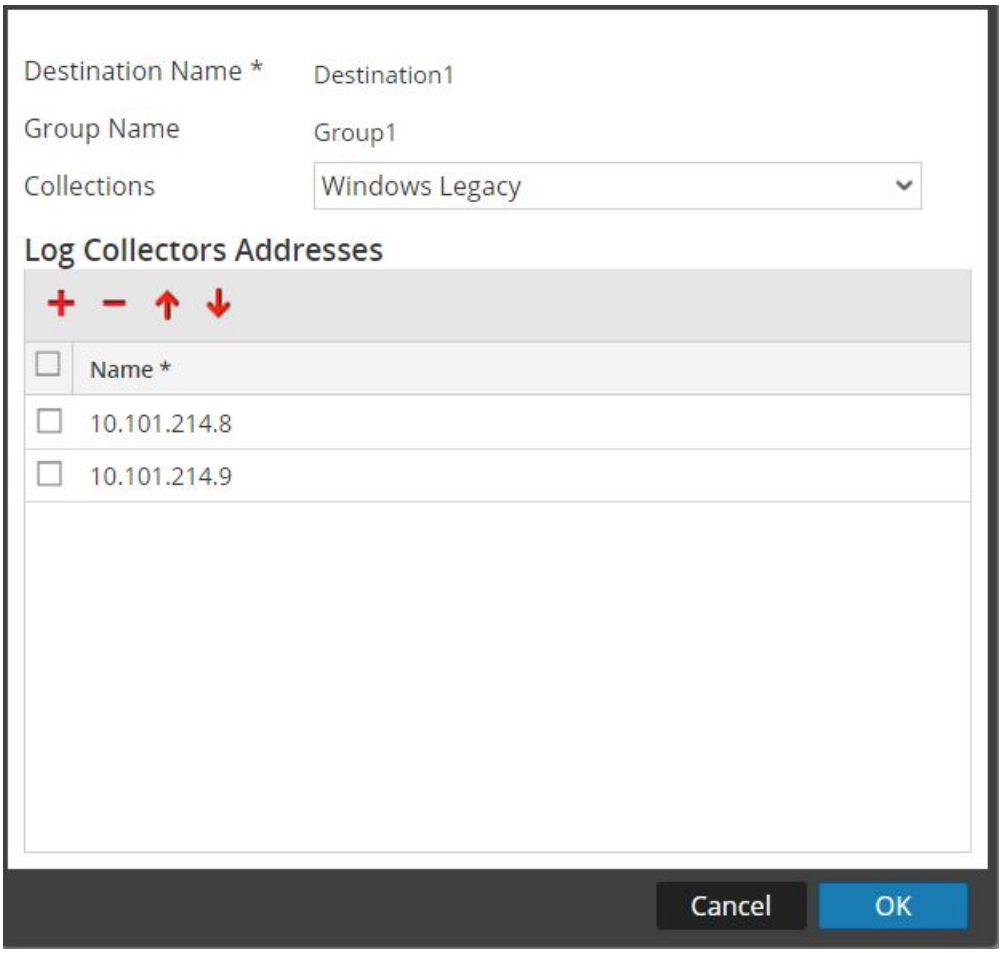
Conmutación por error, replicación y el balanceo de carga

En esta sección se describe el trabajo de conmutación por error, replicación y balanceo de carga en RSA NetWitness Suite.

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

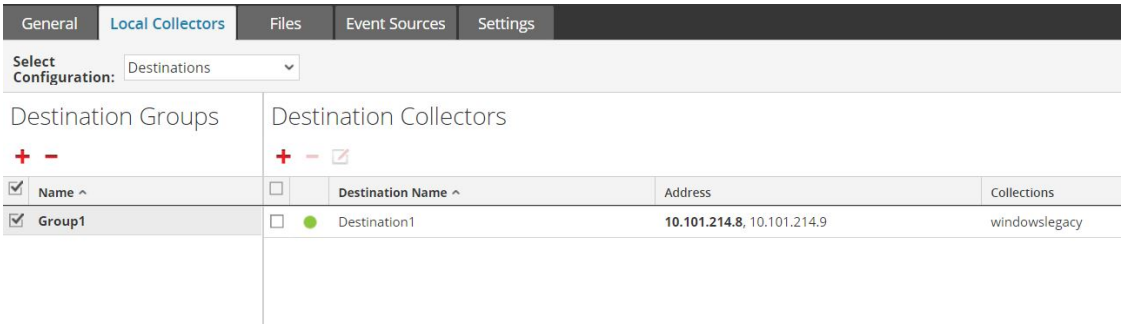


- **La conmutación por error** se logra mediante la configuración de varios recopiladores en el mismo destino. El destino 1 tiene un recopilador primario y, en segundo lugar, un recopilador de conmutación por error. Esto se realiza en NetWitness Suite mediante la adición de varios Log Collectors al mismo destino.



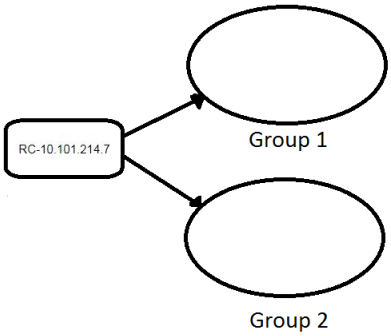
Dado que 10.101.214.8 se enumera en primer lugar, se convierte en el recopilador principal y 10.101.214.9 se convierte en la conmutación por error. Para que 10.101.214.9 sea el primario, use la flecha hacia arriba para cambiar el orden.

A continuación, puede ver los dos recopiladores que aparecen en el destino 1. El primario (10.101.214.8) está en negrita.

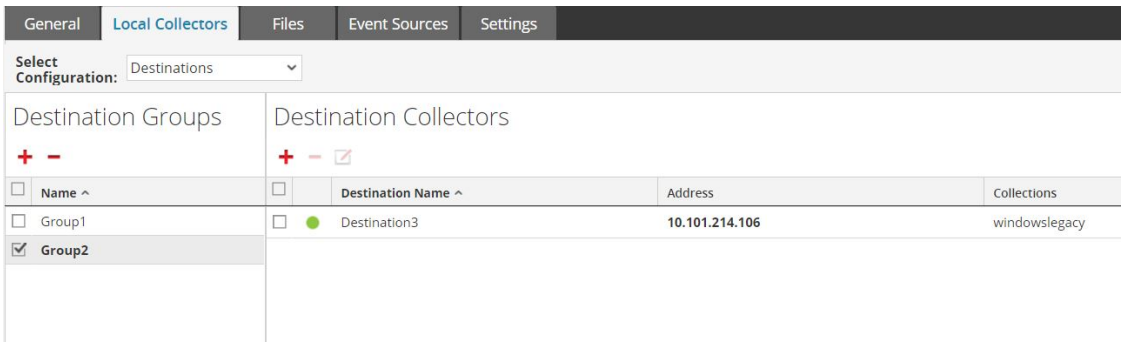


- La **replicación** se logra con varios grupos de destino: cada grupo recibe todo el conjunto de

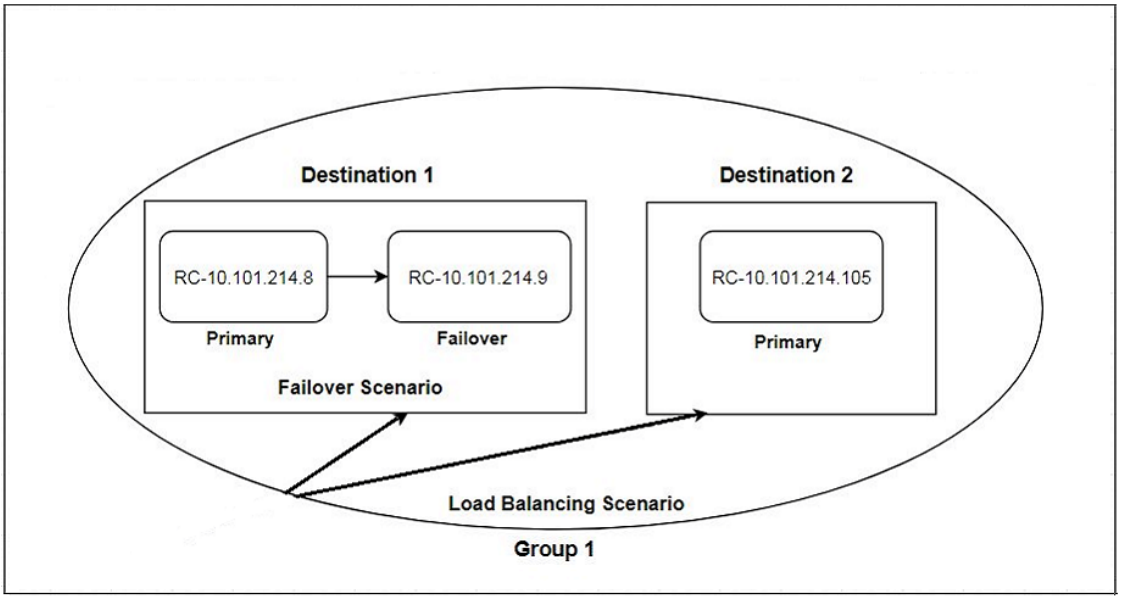
datos del mensaje.



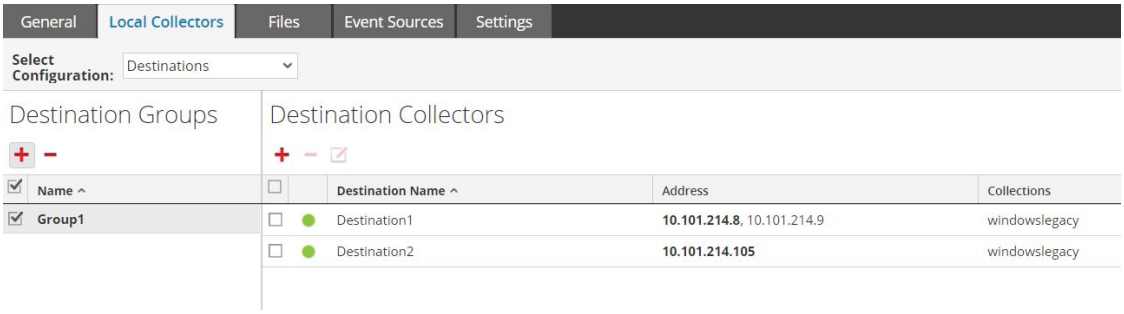
En la siguiente pantalla, puede ver que los datos del mensaje se envían a los recopiladores en el grupo 1 *y* el grupo 2.



- El **balanceo de carga** se logra mediante la configuración de varios destinos dentro de un grupo.



En la siguiente pantalla puede ver que el grupo 1 tiene dos destinos: destino 1 y destino 2. Los datos del mensaje se dividen de manera equitativa entre los destinos del grupo.



Con dos destinos, cada destino recibe la mitad de los datos del mensaje. Con tres de los destinos, cada uno de ellos recibiría 1/3 de los datos del mensaje total. Continúe agregando destinos para reducir aún más la carga en los recopiladores en cada destino.

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

Configurar un Local Collector o un Remote Collector

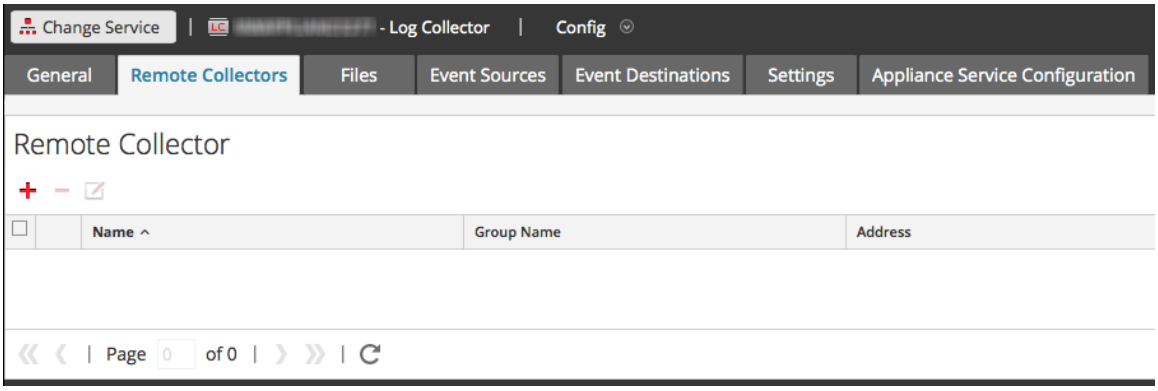
Debe elegir el Log Collector, es decir un Local Collector (LC) o un Remote Collector (RC), para el cual desea definir parámetros de implementación en la vista Servicios. En el siguiente procedimiento se muestra cómo navegar a la vista Servicios, seleccionar un Local Collector o un Remote Collector y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

Para configurar un Local Collector o un Remote Collector:

1. Vaya a **ADMIN > Servicios**.
2. Seleccione un servicio de recopilación de registros local o remoto.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Según su selección en el paso 2:
   - Si ha seleccionado un Local Collector, se muestra la pestaña **Remote Collectors**. En esta pestaña, seleccione los Remote Collectors desde los cuales el Local Collector extrae eventos.
   - Si seleccionó un Remote Collector, se muestran los**Local Collectors**. En esta pestaña, seleccione los Local Collectors a los cuales el Remote Collector migra eventos.

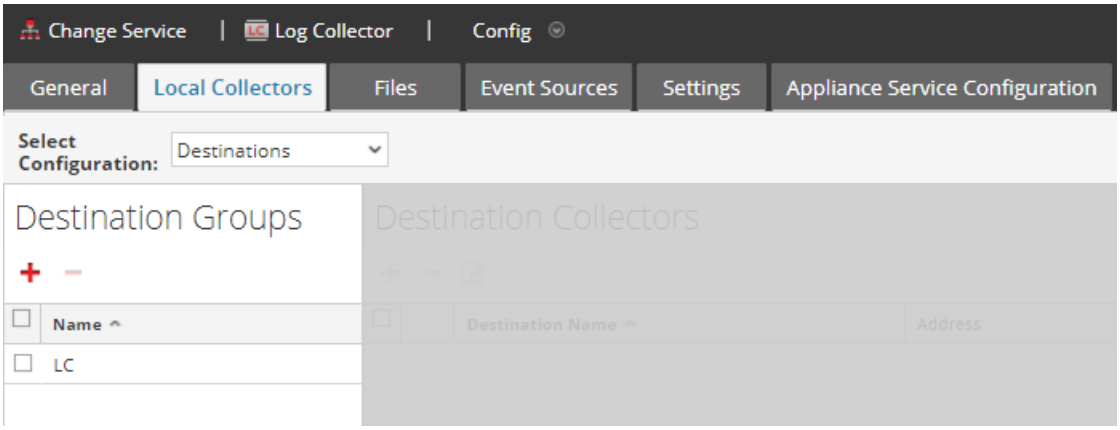
Pestaña Remote Collectors

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

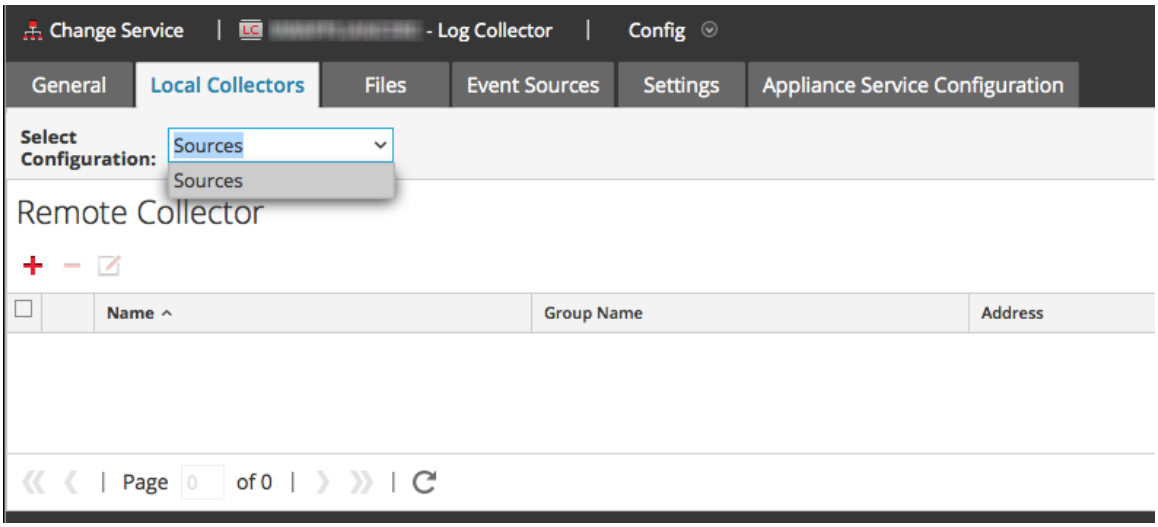


Pestaña Local Collectors para un Remote Collector

En la siguiente figura se muestra una pestaña **Local Collectors** de un Remote Collector configurado para migrar eventos a un Local Collector u 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. NetWitness Suite muestra esta pestaña si se seleccionó un Remote Collector en **Admin > Servicios**.



Parámetros

Parámetros de configuración de Remote/Local Collectors

Configurar Local Collector de conmutación por error

En este tema se indica cómo configurar un Local Collector o un Remote Collector de conmutación por error.

Configurar un Local Collector de conmutación por error

Puede configurar un Local Collector de conmutación por error al cual RSA NetWitness® Suite realizará una conmutación por error si el Local Collector primario deja de funcionar por algún motivo.

1. Vaya a **ADMIN>Servicios**.
2. En **Servicios**, seleccione un servicio de 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. Local Collector se muestra como **activo** y el Local Collector de conmutación por error como **en espera**. 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 conmutación por error.

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

   c. Seleccione un Local Collector y use los botones de flecha hacia arriba ( ) y hacia 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 el Remote Collector comienza a recopilar datos, migra datos a estos Local Collectors.

Configurar un Remote Collector de conmutación por error

Puede configurar un Remote Collector de conmutación por error al cual RSA NetWitness® Suite realizará una conmutación por error si el Remote Collector primario deja de funcionar por algún motivo.

1. Vaya a **ADMIN > Servicios**.
2. En **Servicios**, seleccione un servicio de 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

Parámetros de configuración de Remote/Local Collectors

Configurar la replicación

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

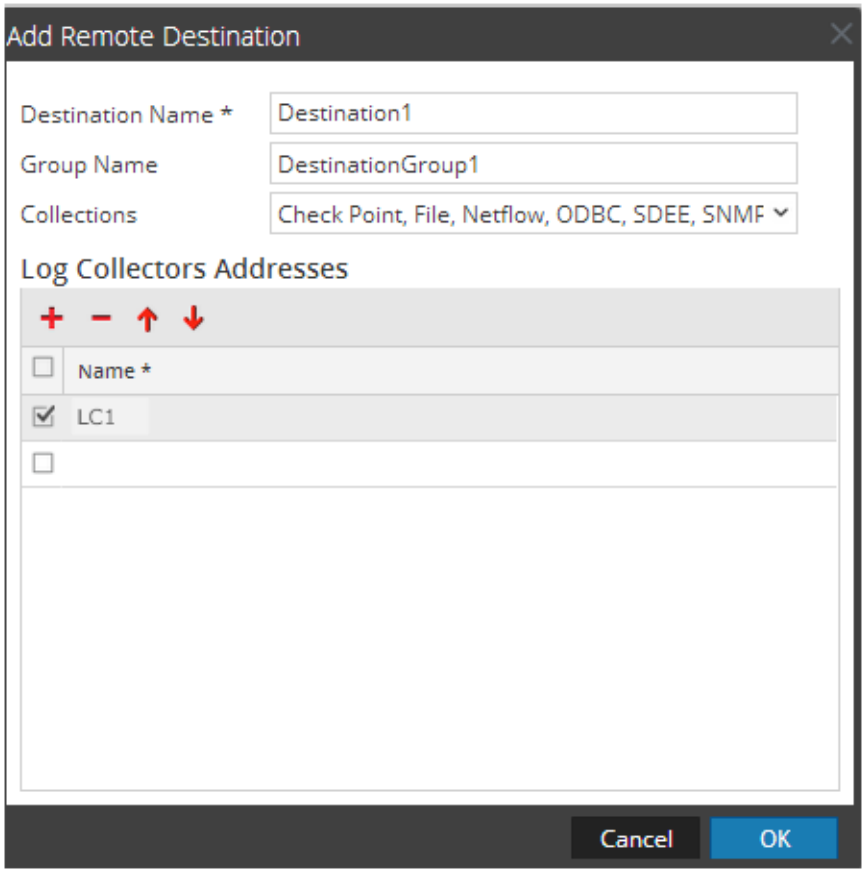
Puede especificar varios grupos de destino para que los datos de eventos se repliquen en cada grupo.

Para replicar datos de eventos en varios Local Collectors:

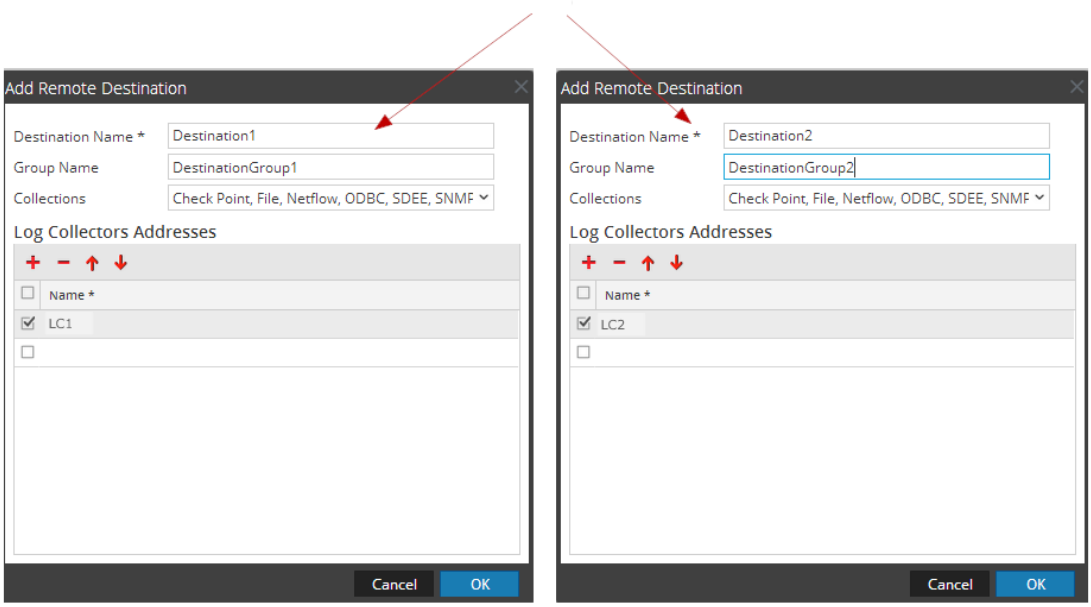
1. Vaya a **ADMIN > Servicios.**
2. Seleccione un servicio de recopilación de registros remoto.
3. En Acciones, seleccione  **> Ver > Configuración**.

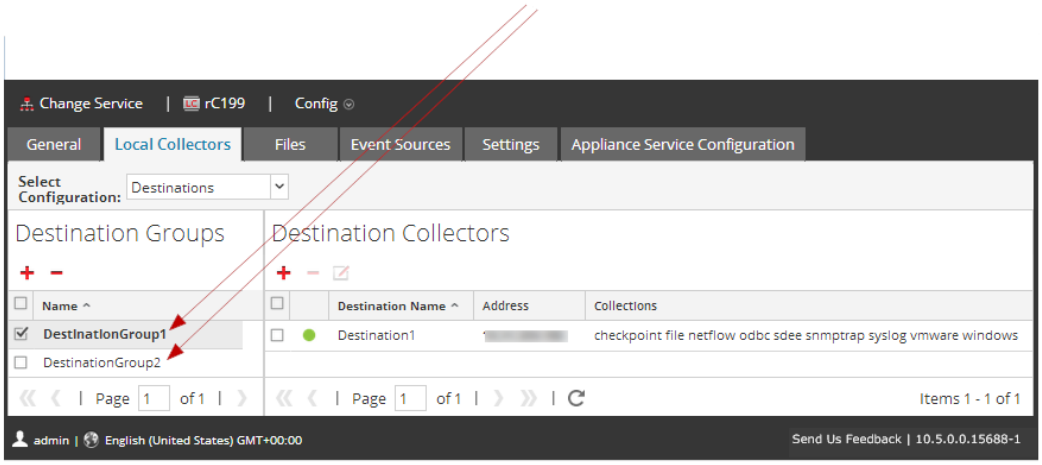
   La vista Configuración del servicio se muestra con la pestaña **General de Log Collector** abierta.
4. Seleccione la pestaña **Local Collectors**.
5. En la sección del panel **Grupos de destino**, haga clic en  .

   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.

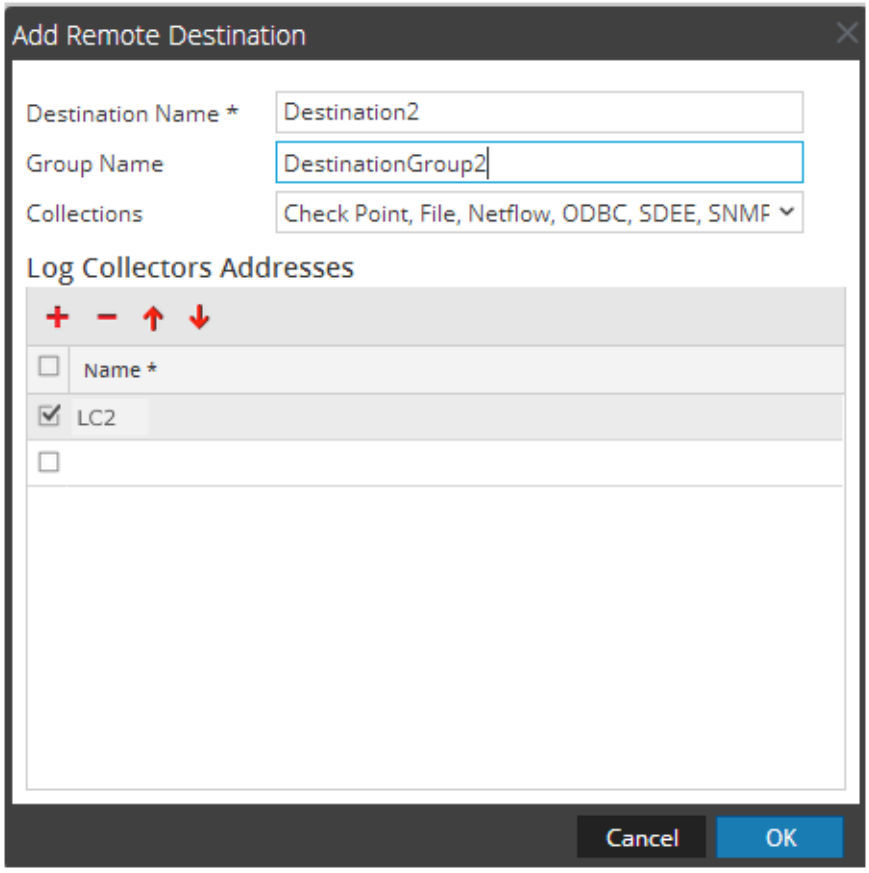
d. Seleccione un Local Collector (por ejemplo, **LC1**).

e. Haga clic en **Aceptar**.

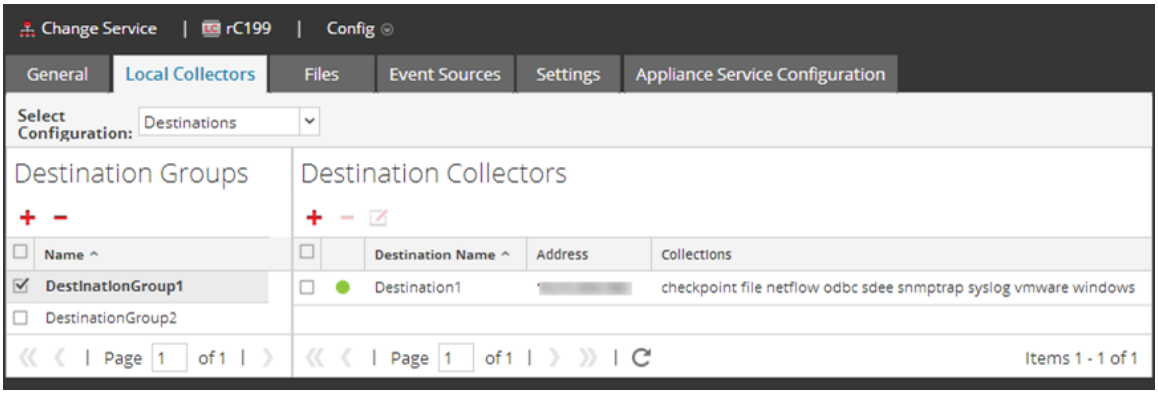
f. Seleccione el nuevo grupo (por ejemplo, **DestinationGroup2**) en el panel **Grupos de destino** y haga clic en + en el panel **Local Collector**.

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.



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.** Migrar datos desde un Remote Collector a otros Remote Collectors o Local Collectors.
- **Remote Collector para extraer datos.** Use un Remote Collector para extraer datos desde uno o varios Remote Collectors.

Configurar Remote Collector para migrar datos de eventos a Remote Collector

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

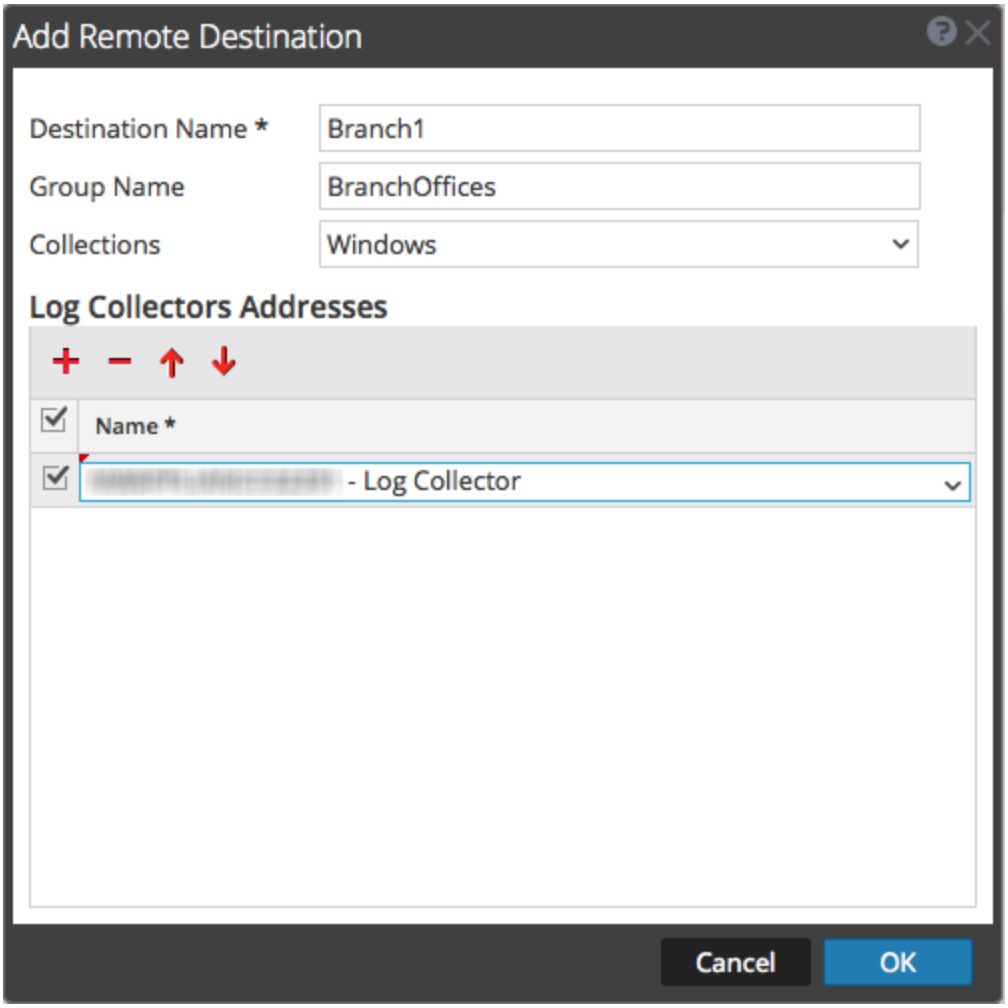
Configurar un Remote Collector para migrar eventos a un Remote Collector especificado

1. Vaya a **ADMIN > Servicios.**
2. En **Servicios**, seleccione un **Remote Collector**.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

   La vista **Log CollectorConfiguración del servicio** se muestra con la pestaña **Log CollectorGeneral** 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, NetWitness Suite lo configura 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.

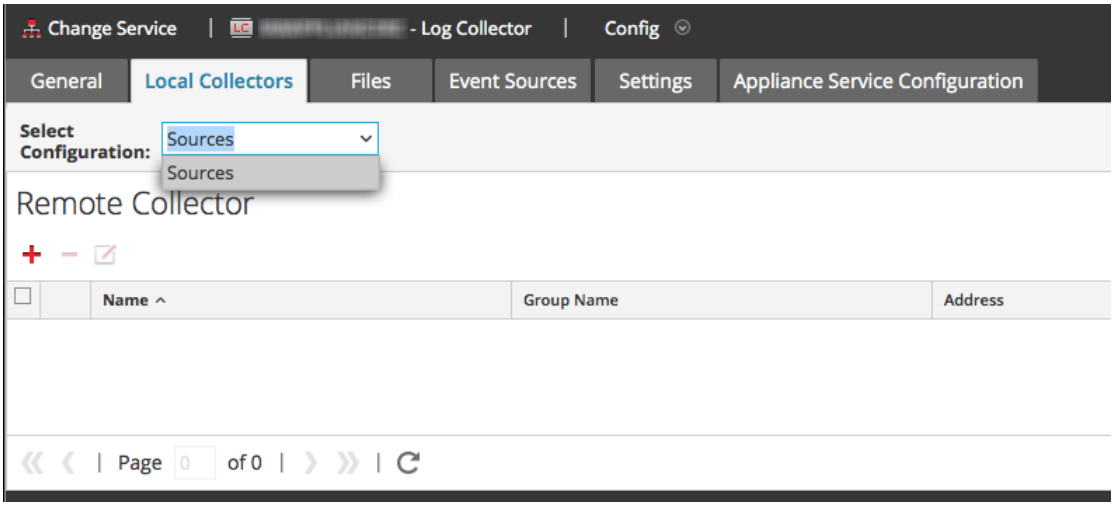
Configurar Remote Collector para extraer datos de eventos de un Remote Collector

Configurar el Remote Collector seleccionado para extraer eventos del Remote Collector especificado

1. Vaya a **ADMIN > Servicios.**
2. En **Servicios**, seleccione un **Remote Collector**.
3. En Acciones, seleccione > **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

   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.

Regular el ancho de banda de Remote Collector a 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.

En este tema se describe cómo regular el ancho de banda de Remote Collector a Local Collector mediante el script de shell **set-shovel-transfer-limit.sh**. Incluye las siguientes secciones:

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

  Nota: El valor del filtro que necesita configurar depende de la velocidad a la que el Remote Log Collector envía eventos al Local Collector.

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

Ayuda de la línea de comandos para configurar el script de límite de transferencia de shovel

Ejecute 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
```

Uso:

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

donde:

- -c = clear existing
- -d = display filter
- -s = set new values
- -i = interfaz es el nombre de la interfaz de red. El valor predeterminado es **eth0**
- -r = tasa es la tasa de ancho de banda. El valor predeterminado es **256 kbps**

Los anchos de banda y las tasas se pueden especificar en:

- **nolimit**: deshabilita la regulación
- **kbit**: Kilobits por segundo
- **mbit**: Megabits por segundo
- **kbps**: Kilobytes por segundo
- **mbps**: Megabytes por segundo
- **bps**: Bytes por segundo

Establecer el filtro en 4.096 kilobits por segundo.

En este ejemplo se configura 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          destination

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
```

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. El Lockbox de NetWitness Suite 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).

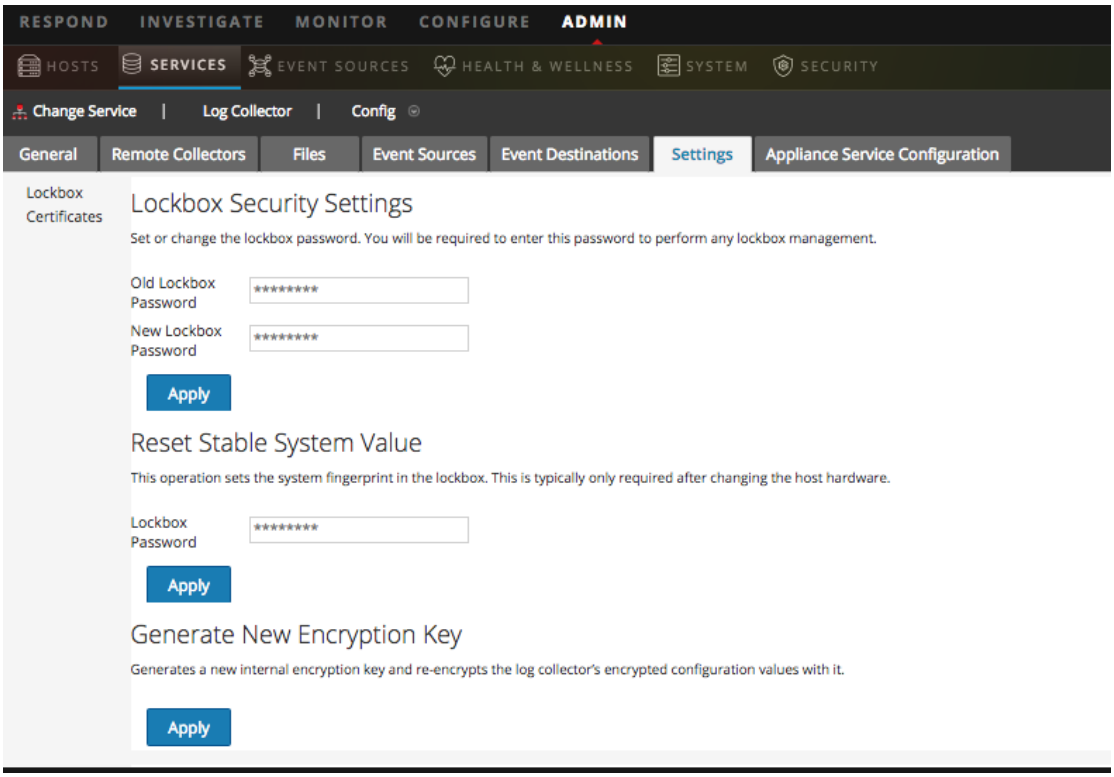
Los siguientes son los ajustes de seguridad de lockbox.

Función	Descripción
Contraseña anterior de lockbox	Cuando configure un Lockbox por primera vez, este campo estará en blanco. NetWitness Suite lo completa 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. Vaya a **ADMIN > Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Ajustes de 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**.

Iniciar servicios de recopilación

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

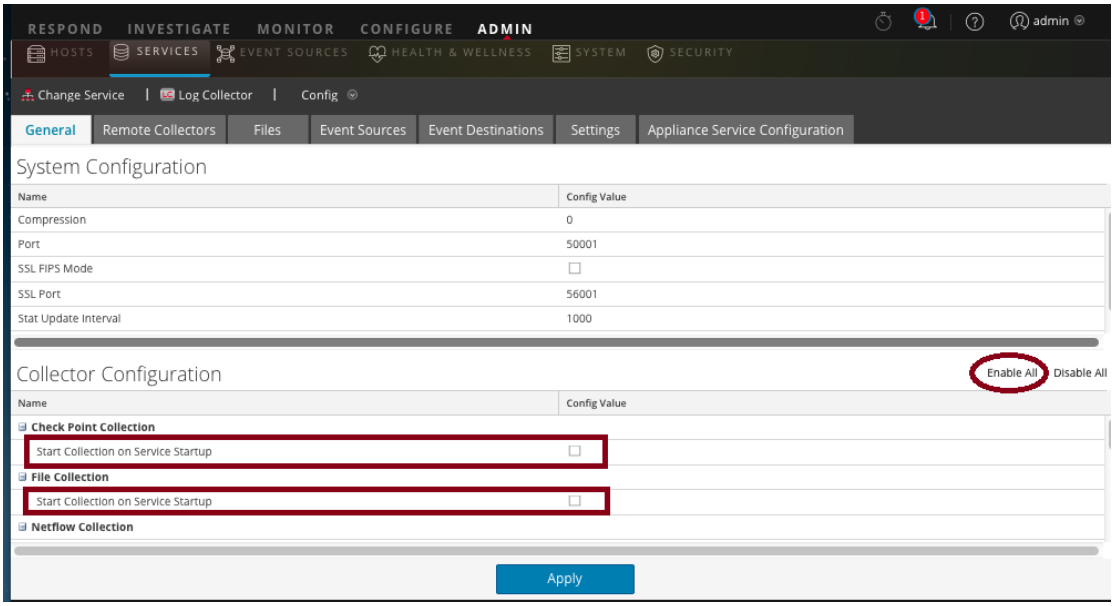
Iniciar un servicio de recopilación

1. Vaya a **ADMIN > Servicios**.
2. Seleccione un servicio Log Collector y haga clic en  bajo **Acciones**.
3. Haga clic en **Ver** > **Sistema**.
4. Haga clic en **Recopilación** > ***servicio*** (por ejemplo, **Archivo**) y, a continuación, haga clic en **Iniciar**.

Habilitar el inicio automático de servicios de recopilación

1. Vaya a **Admin > Servicios**.
2. Seleccione un servicio Log Collector y haga clic en  bajo **Acciones**.
3. Haga clic en **Ver** > **Configuración**.

   Se muestra la pestaña General.
4. En el panel Configuración de Collector, seleccione **Iniciar la recopilación en el arranque del servicio** para los servicios de recopilación individuales que desea que se inicien automáticamente. Como alternativa, seleccione **Activar todo** para iniciar automáticamente todos los servicios de recopilación.



5. Haga clic en **Aplicar** para que se apliquen los cambios.

Verificar que la recopilación de registros esté funcionando

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

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

- Verifique que haya actividad de eventos 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 la vista **Investigation > Eventos** para el protocolo de recopilación que configuró.

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

Configurar 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.

Agregar un certificado

Para agregar un certificado:

1. Vaya a **ADMIN >Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio de **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Ajustes de 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**.

Panel Certificados

En la siguiente tabla se describen los botones y las columnas disponibles en el panel Certificados.

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

En la siguiente tabla se describen los parámetros disponibles en el 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.
Guardar	Agrega el certificado.

Aspectos básicos 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 NetWitness Suite. Los logs 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 NetWitness Suite configura el servicio Log Collector para sondear orígenes de eventos y recuperar sus registros. En consecuencia, Log Collector recibe todos los registros en su forma original.

Protocolos de recopilación

RSA NetWitness Suite puede recopilar registros desde una amplia variedad de orígenes de eventos. Cuando configura la recopilación de registros para un origen de eventos específico, debe conocer, en primer lugar, el protocolo que se usa para recopilar los registros.

Protocolo de recopilación	Descripción
Punto de control	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 Configurar orígenes de eventos de punto de comprobación en NetWitness Suite.
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 Configurar orígenes de eventos de archivos en NetWitness Suite.
Netflow	Acepta eventos de Netflow v5 y Netflow v9. Para obtener más información, consulte Configurar orígenes de eventos de Netflow en NetWitness Suite.

Protocolo de recopilación	Descripción
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 Configurar orígenes de eventos de ODBC en NetWitness Suite.
Plug-ins	La recopilación de plug-ins es una infraestructura de recopilación genérica para recopilar eventos mediante scripts externos que se escriben en otros idiomas. Actualmente, RSA proporciona recopilación de Amazon Web Services (AWS) CloudTrail y Microsoft Azure. • **AWS**: Recopila eventos desde Amazon Web Services (AWS) CloudTrail. Específicamente, CloudTrail registra llamadas API de AWS para una cuenta. Para obtener más información, consulte Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite • **Azure**: Recopila eventos de Microsoft Azure. Para obtener más información, consulte Configurar orígenes de eventos de Azure en NetWitness Suite. Los clientes pueden usar esta infraestructura para desarrollar protocolos de recopilación propios.
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 Configurar orígenes de eventos de SDEE en NetWitness Suite.
SNMP Trap	Acepta SNMP traps. Para obtener más información, consulte Configurar orígenes de eventos de SNMP en NetWitness Suite.
Syslog	Acepta mensajes de orígenes de eventos que emiten mensajes de syslog. Para obtener más información, consulte Configurar orígenes de eventos de syslog para Remote Collector. **Nota:** No configure la recopilación de syslog para los Log Collectors locales. Solo debe configurar la recopilación de syslog para los Remote Collectors.
VMware	Recopila eventos de una infraestructura virtual de VMware. Para obtener más información, consulte Configurar orígenes de eventos de VMware en NetWitness Suite.

Protocolo de recopilación	Descripción
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 Configurar orígenes de eventos de Windows en NetWitness Suite.
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 Configuración de la recopilación de Windows existente y NetApp. **Nota:** El recopilador de Windows existente de NetWitness Suite se instala en un servidor Windows 2008 R2 SP1 de 64 bits físico o virtual mediante el archivo **SALegacyWindowsCollector-*version-number*.exe**.

Procedimiento básico

El procedimiento básico es el mismo para todos los protocolos de recopilación compatibles.

1. **Configurar el origen de eventos para la recopilación.** Cada origen de eventos compatible tiene un documento de configuración disponible en el espacio Orígenes de eventos compatibles de RSA en RSA Link
   a. Navegue al espacio Orígenes de eventos compatibles de RSA en RSA Link.
   b. Encuentre las instrucciones del origen de eventos.

      En la página Descripción general se enumeran todos los orígenes de eventos actualmente compatibles, así como información sobre el método de recopilación, la clase de dispositivo y las versiones compatibles.
   c. Descargue las instrucciones de configuración para el origen de eventos y sígalas.

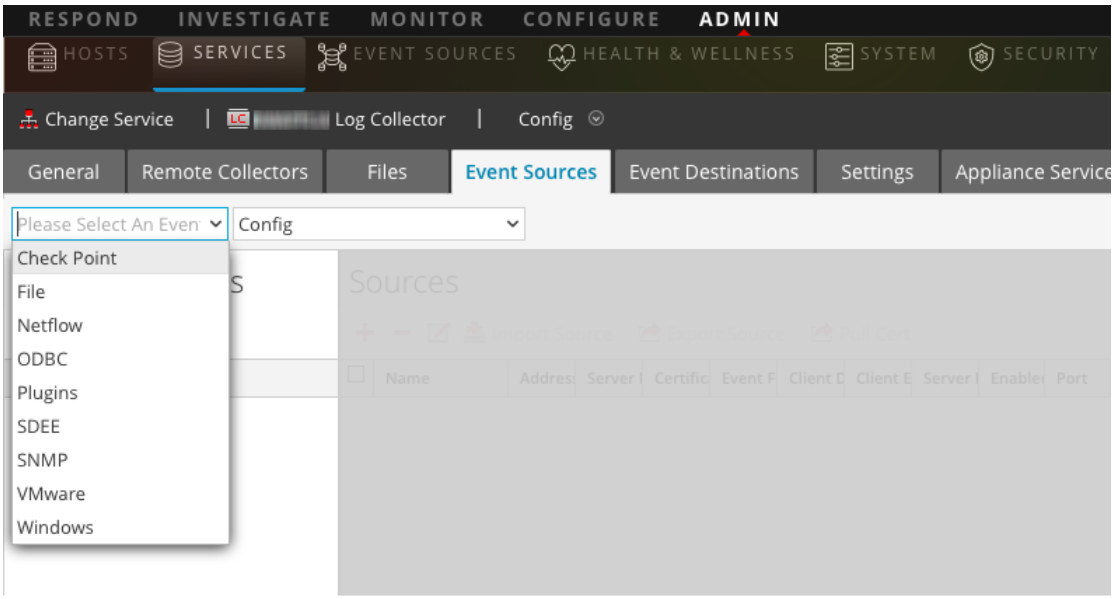
2. **Configurar la recopilación en RSA NetWitness Suite.** La Guía de configuración del origen de eventos contiene estas instrucciones. Sin embargo, en esta guía también se proporcionan estas instrucciones, según el método de recopilación que usa el origen de eventos. Para obtener más información, consulte Protocolos de recopilación.
3. **Iniciar el servicio para el método de recopilación.** Por lo general, solo debe realizar esto para el primer origen de eventos que usa este método de recopilación. Por ejemplo, la primera vez que configura un origen de eventos que usa la recopilación de archivos, puede que necesite iniciar el servicio de archivos en NetWitness Suite.
4. **Verificar que la recopilación funcione para el origen de eventos.**

En el resto de este tema se describen los pasos 2, 3 y 4 más detalladamente.

Configurar la recopilación en RSA NetWitness Suite

El proceso para configurar orígenes de eventos depende del método de recopilación que usen. Sin embargo, tenga en cuenta que son muy similares. El siguiente procedimiento es genérico: puede obtener más detalles de los métodos de recopilación individuales en los temas que abarcan los detalles de cada método de recopilación específico.

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione > **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. En la pestaña **Orígenes de evento de Log Collector**, seleccione el método de recopilación en el menú desplegable.
6. 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.
7. Seleccione un tipo de origen de eventos y haga clic en **Aceptar**.

   El tipo de origen de eventos 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 Orígenes.

   Se muestra el cuadro de diálogo **Agregar origen**.
9. Ingrese valores para los parámetros disponibles.

   Consulte la sección Parámetros del método de recopilación específico que está configurando.
10. Haga clic en **Aceptar**.

Iniciar el servicio para el método de recopilación

Iniciar el servicio para el método de recopilación, realice lo siguiente:

1. Vaya a **Admin > Servicios**.
2. Seleccione un **Log Collector** y elija  **> Ver > Sistema**.
3. Haga clic en **Recopilación >** ***protocolo*****> Iniciar**

   donde ***protocolo*** es el protocolo que desea iniciar, por ejemplo **Netflow**.

Verificar que la recopilación funcione para el origen de eventos

Puede verificar que un método de recopilación está funcionando en **Admin > Estado y condición > pestaña Monitoreo de orígenes de eventos**.

Para verificar que la recopilación funcione para un origen de eventos:

1. Vaya a **ADMIN > Estado y condición**
2. Haga clic en la pestaña **Monitoreo de orígenes de eventos**.
3. En la cuadrícula, busque el **Log Decoder**, **origen de evento** y **tipo de origen de evento**.
4. Busque actividad en la columna **Conteo** para que un origen de evento verifique que la recopilación está aceptando eventos.

Configurar filtros de eventos para un Log Collector

En este tema se indica cómo crear y mantener filtros de eventos en todos los protocolos de recopilación.

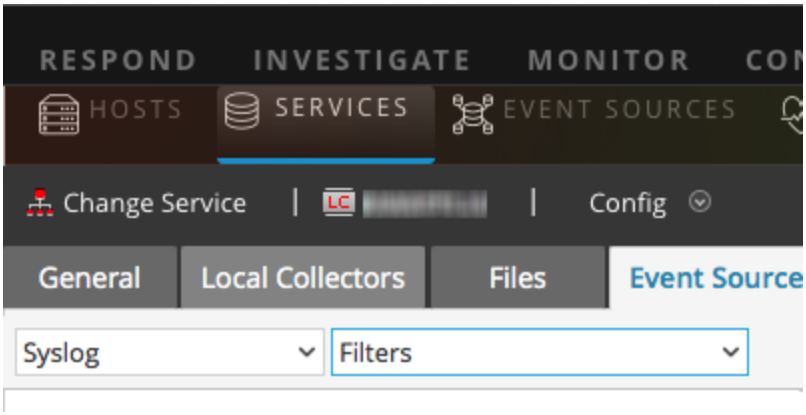
Nota: No puede configurar la recopilación de syslog para los Log Collectors locales. Solo debe configurar la recopilación de syslog para los Remote Collectors. Consulte Configurar Local y Remote Collectors para obtener información de configuración adicional.

Configurar un filtro de eventos

Para configurar un origen de eventos:

1. Vaya a **ADMIN > Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.
5. En la pestaña **Orígenes de evento**, seleccione cualquier método de recopilación/**filtro**en los menús desplegables.

   En la siguiente pantalla se muestra el **Syslog** seleccionado.

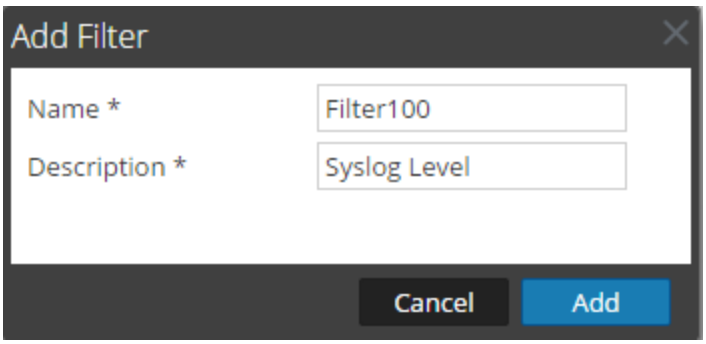


   Nota: La configuración de syslog solo está disponible en Remote Collectors: si está trabajando con un servicio Local Collector, **Syslog** no está disponible en el menú desplegable.

   En la vista **Filtros** se muestran los filtros que están configurados para el método de recopilación seleccionado, si los hay.

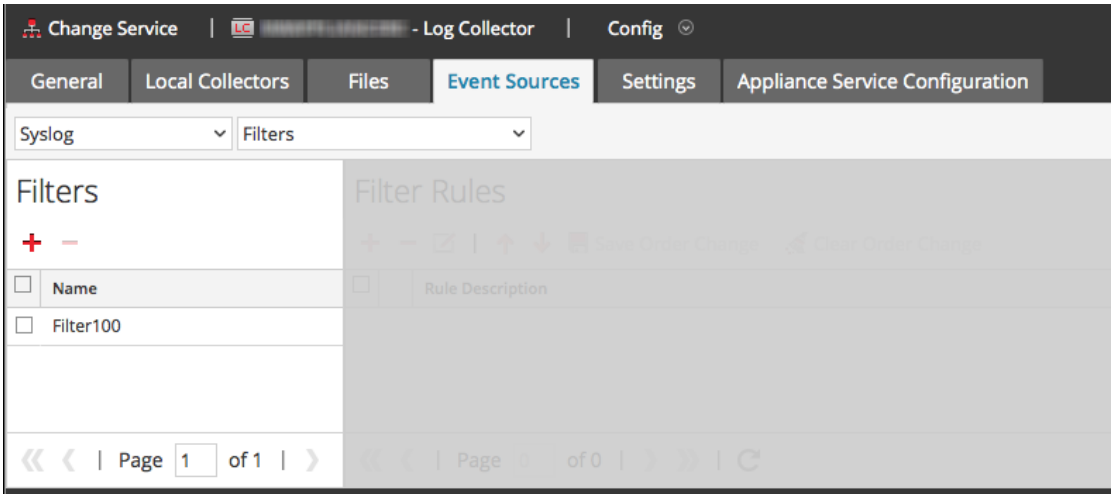
6. En la barra de herramientas del panel **Filtros**, haga clic en +.

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



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

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

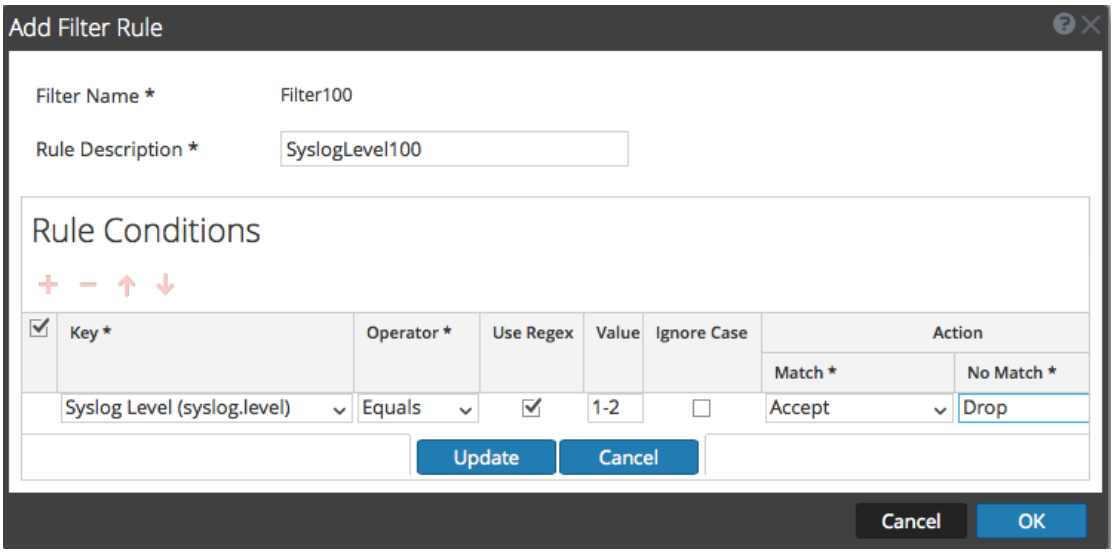


8. Seleccione el nuevo filtro en el panel **Filtros** y haga clic en + en la barra de herramientas del panel **Filtrar reglas**.

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

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

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



NetWitness Suite actualiza el filtro con la regla que definió.

Nota: Las reglas se procesan en orden de arriba hacia abajo hasta que un tipo de acción anula el procesamiento o se comprueba la regla final. El comportamiento predeterminado es aceptar la regla si no se encuentran coincidencias.

En las siguientes tablas se describen los parámetros para agregar una regla de filtro.

Parámetro de "clave" de regla de filtro de eventos

El método de recopilación al cual se aplica el filtro depende de los valores del campo Clave.

Método de recopilación	Los valores del campo *Clave*
Punto de control, archivo, Netflow, Plug-in, SDEE SNMP y VMware	• Todos los campos de datos • Tipo de origen de evento • Nombre del origen de eventos • Dirección IP de origen • Evento crudo

Método de recopilación	Los valores del campo *Clave*
ODBC	• Todos los campos de datos • Tipo de origen de evento • Nombre del origen de eventos • Dirección IP de origen • ID de mensaje • Nivel de mensaje
Syslog	• Todos los campos de datos • Tipo de origen de evento • Nombre del origen de eventos • Dirección IP de origen • Nivel de syslog • Evento crudo
Windows	• Todos los campos de datos • Tipo de origen de evento • Nombre del origen de eventos • Dirección IP de origen • ID del evento • Proveedor • Canal • Computadora • UserName • DomainName

Método de recopilación	Los valores del campo *Clave*
Windows existente	• Todos los campos de datos • Tipo de origen de evento • Nombre del origen de eventos • Dirección IP de origen • ID del evento

Otros parámetros de regla de filtro de eventos

En la siguiente tabla se describen todos los demás campos disponibles para la creación de una regla de filtro de eventos.

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.

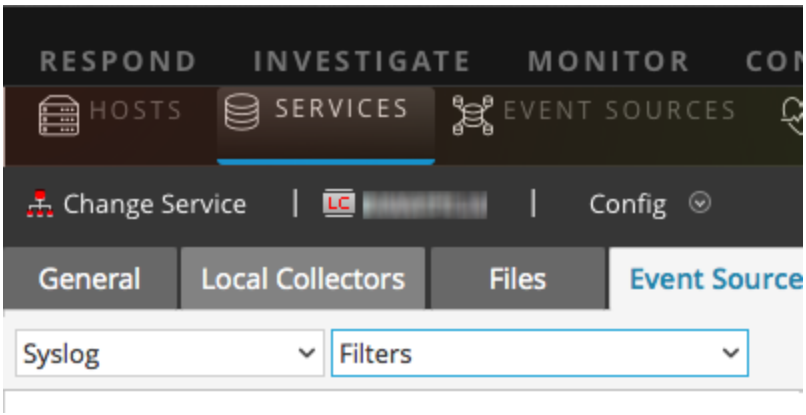
Campo	Descripción
Acción	Si hay una coincidencia, puede elegir las acciones aceptar, descartar, condición siguiente o regla siguiente: • **Aceptar**: los eventos que coinciden con los ID proporcionados se incluirán en los registros de eventos y se mostrarán en la interfaz del usuario de analítica de los sistemas. • **Descartar**: los eventos que coinciden con los ID proporcionados no se incluirán en los registros de eventos y no se mostrarán en la interfaz del usuario. • **Condición siguiente**: el filtro omitirá los eventos con los ID que coincidan y se moverá a la condición de regla siguiente. • **Regla siguiente**: el filtro omitirá los eventos con los ID que coincidan y se moverá a la 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. Vaya a **ADMIN >Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.
5. En la pestaña **Orígenes de evento**, seleccione cualquier método de recopilación/**filtro**en los menús desplegables.

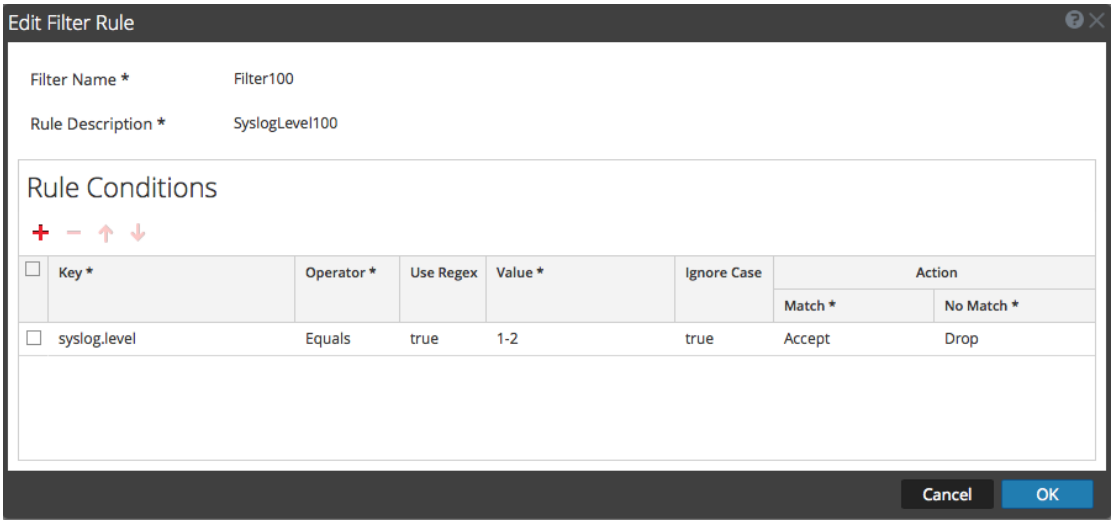
   En la siguiente pantalla se muestra **Punto de comprobación** seleccionado.



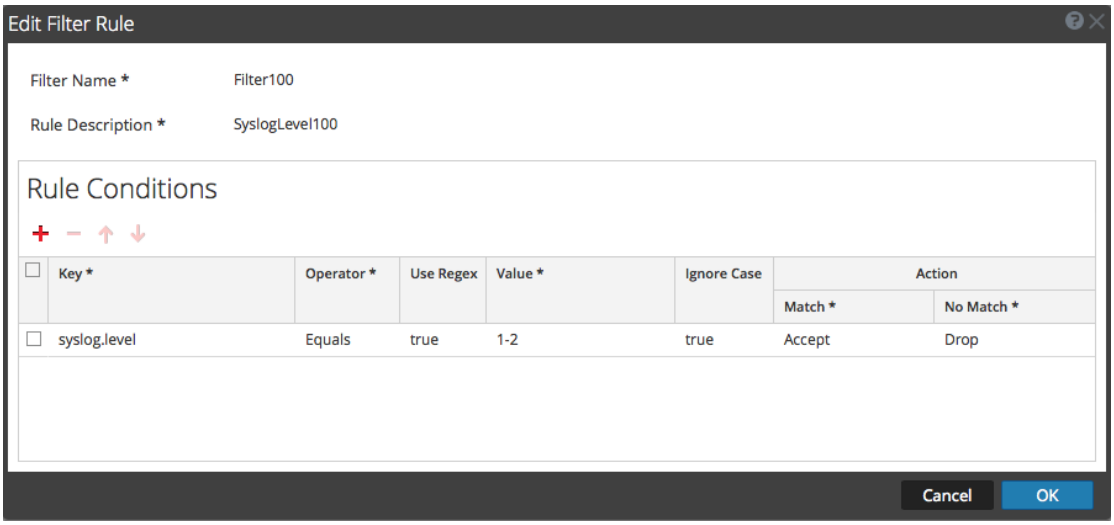
En la vista **Filtros** se muestran los filtros que están configurados para el método de recopilación seleccionado, si los hay.

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**.

NetWitness Suite aplica los cambios en los parámetros de condición a la regla de filtro seleccionada.

Importar, exportar, editar y probar orígenes de eventos de manera masiva

En este tema, se describe cómo importar, exportar, editar y probar orígenes de eventos de manera 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.

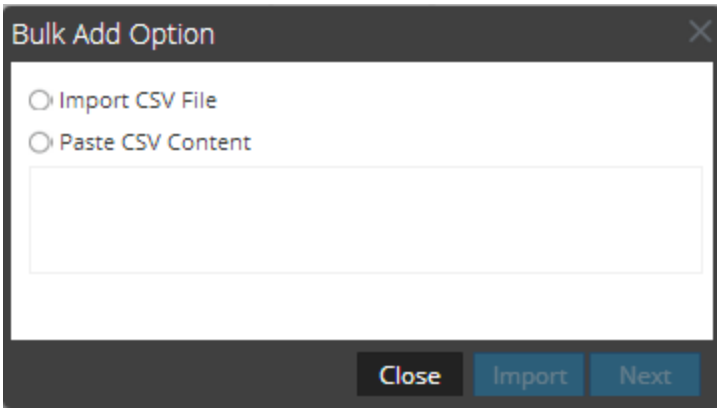
Importar orígenes de eventos de forma masiva

Advertencia: Cuando se usa un programa de hoja de cálculo para editar un archivo CSV de origen de eventos exportado, a algunos campos de datos, como números y fechas, se les puede cambiar el formato a los tipos de campos nativos del programa de hoja de cálculo. Esto puede causar problemas en el momento de volver a importar esta información, porque algunos campos de datos podrían estar ilegibles o formateados incorrectamente. Para evitar esto, importe el archivo CSV al programa de hoja de cálculo y especifique todos los campos de datos como valores de texto.

Para importar varios orígenes de eventos de una vez:

1. Vaya a **Admin > Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.
5. Seleccione **Punto de comprobación**, **Archivo**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE**, **(Syslog para Remote Collectors) solamente**, **VMware**, **Windows** o **Windows existente** (SNMP no tiene una función de importación).
6. En la barra de herramientas del panel **Orígenes**, haga clic en **Importar origen**.

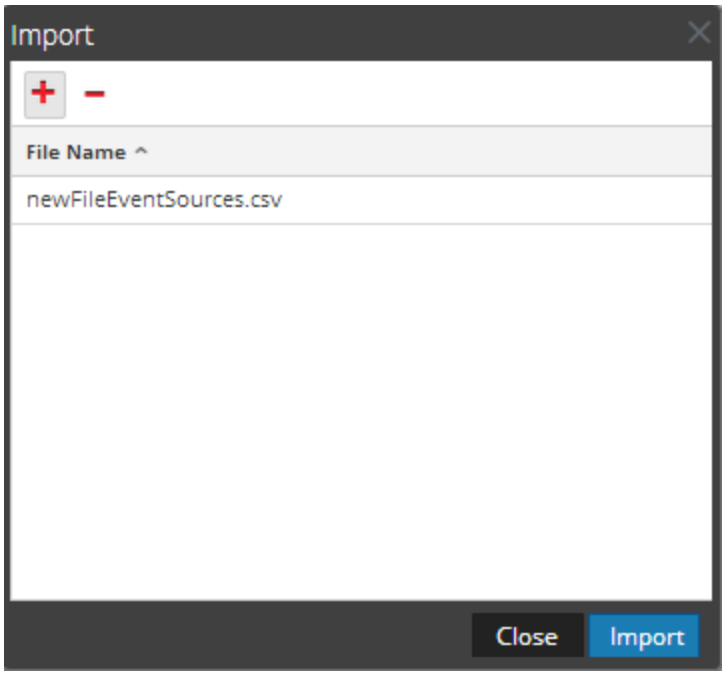
   Se muestra el cuadro de diálogo **Opción Adición en masa**.



7. 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.

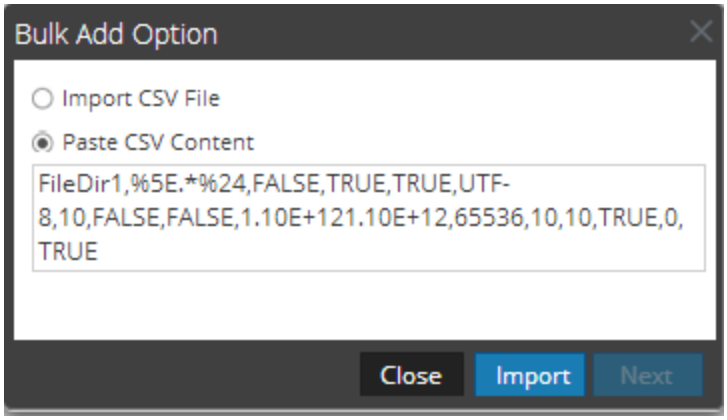


c. Haga clic en **Importar**.

   Los orígenes de eventos se agregan a la lista **Origen de evento**.

- Pegar contenido de CSV

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



b. Haga clic en **Importar**.

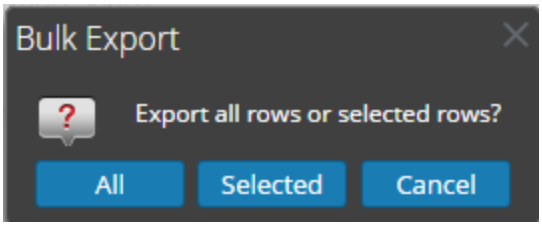
   Los orígenes de eventos se agregan a la **lista Origen de evento**.

Exportar orígenes de eventos de forma masiva

Advertencia: Cuando se usa un programa de hoja de cálculo para editar un archivo CSV de origen de eventos exportado, a algunos campos de datos, como números y fechas, se les puede cambiar el formato a los tipos de campos nativos del programa de hoja de cálculo. Esto puede causar problemas en el momento de volver a importar esta información, porque algunos campos de datos podrían estar ilegibles o formateados incorrectamente. Para evitar esto, importe el archivo CSV al programa de hoja de cálculo y especifique todos los campos de datos como valores de texto.

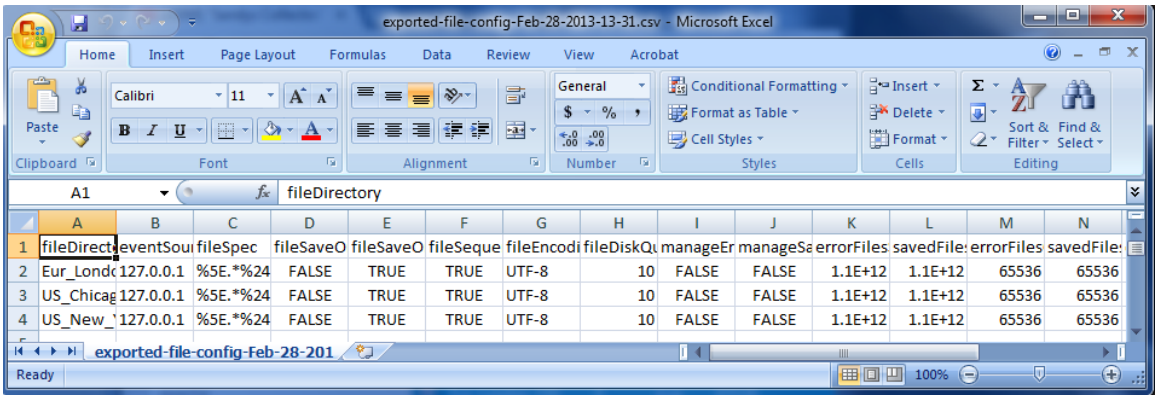
1. Vaya a **Admin** > **Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  > **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.
5. Seleccione **Punto de comprobación**, **Archivo**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE**, **(Syslog para Remote Collectors) solamente**, **VMware**, **Windows** o **Windows existente** (SNMP no tiene una función de exportación).
6. 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**.

7. Según su selección:
   - **Todo**, NetWitness Suite exporta todos los orígenes de eventos a un archivo CSV con registro de fecha y hora.
   - **Seleccionado**, NetWitness Suite exporta los orígenes de eventos que seleccionó a un archivo CSV con registro de fecha y hora.
   - **Cancelar**, NetWitness Suite cancela la exportación.

   El siguiente es un ejemplo de un archivo CSV con registro de fecha y hora que se crea con los orígenes de evento que seleccionó en la lista.

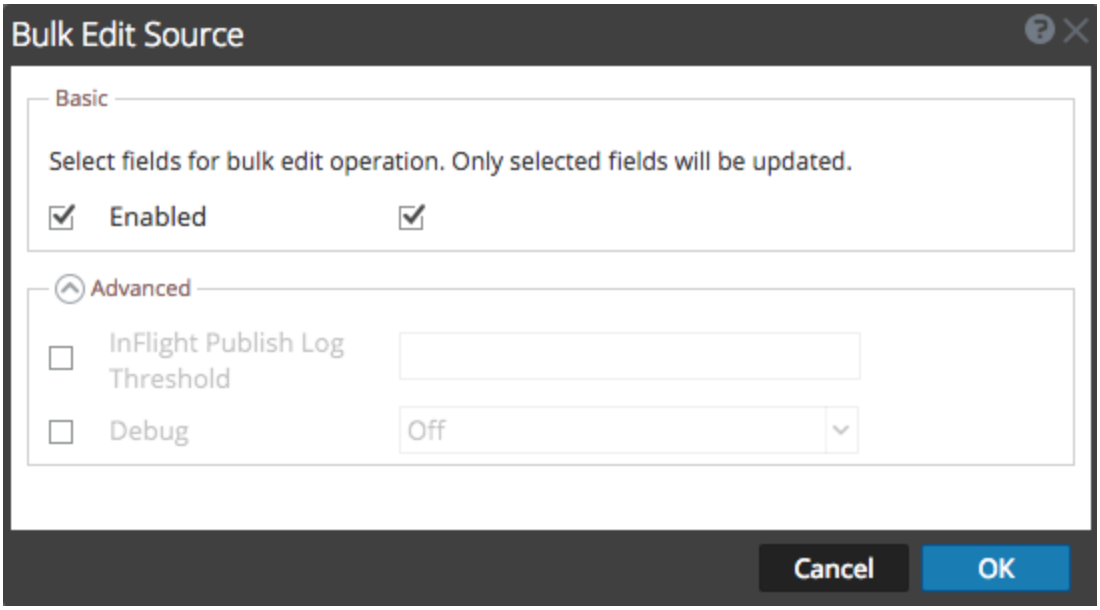


Editar orígenes de eventos de forma masiva

Para editar varios orígenes de eventos de una vez:

1. En la pestaña **Orígenes de evento de Log Collector**, seleccione **Punto de comprobación**, **Archivo**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE**, **Syslog**, **VMware**, **Windows** o **Windows existente** (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**.

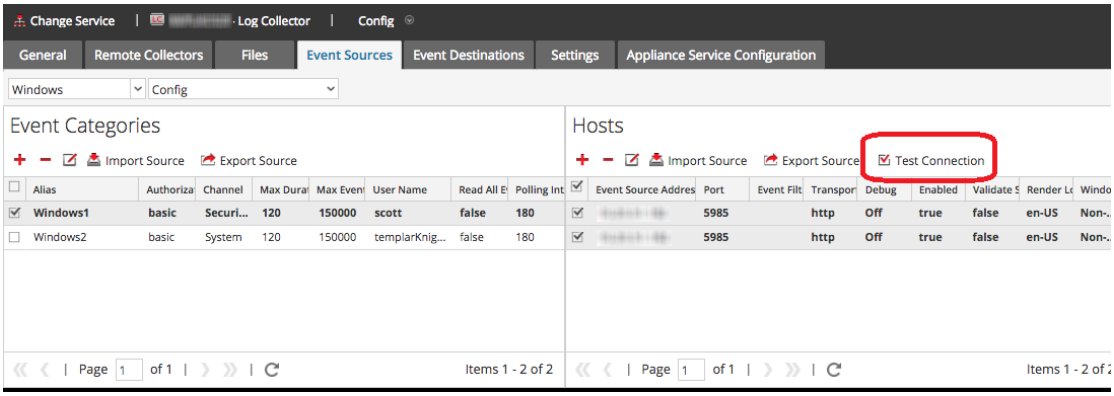
   NetWitness Suiteaplica el mismo cambio de valores de parámetros a todos los orígenes de eventos seleccionados

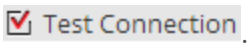
Probar conexiones de orígenes de eventos de manera masiva

Para probar varias conexiones de orígenes de eventos simultáneamente:

1. Vaya a **Admin** > **Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. En Acciones, seleccione  > **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Seleccione la pestaña **Orígenes de evento** y elija **Plug-ins**, **ODBC** o **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  .

   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**.

Consulte también

Puede usar el módulo **Orígenes de evento** (Administration > Orígenes de evento) para crear grupos de orígenes de eventos, por lo general, se importan desde una CMDB y para monitorear orígenes de eventos en función de esos grupos. Para obtener detalles, consulte los siguientes temas en la *Guía de administración de orígenes de eventos*:

- Importar orígenes de eventos
- Exportar orígenes de eventos
- Edición en masa de atributos de orígenes de eventos

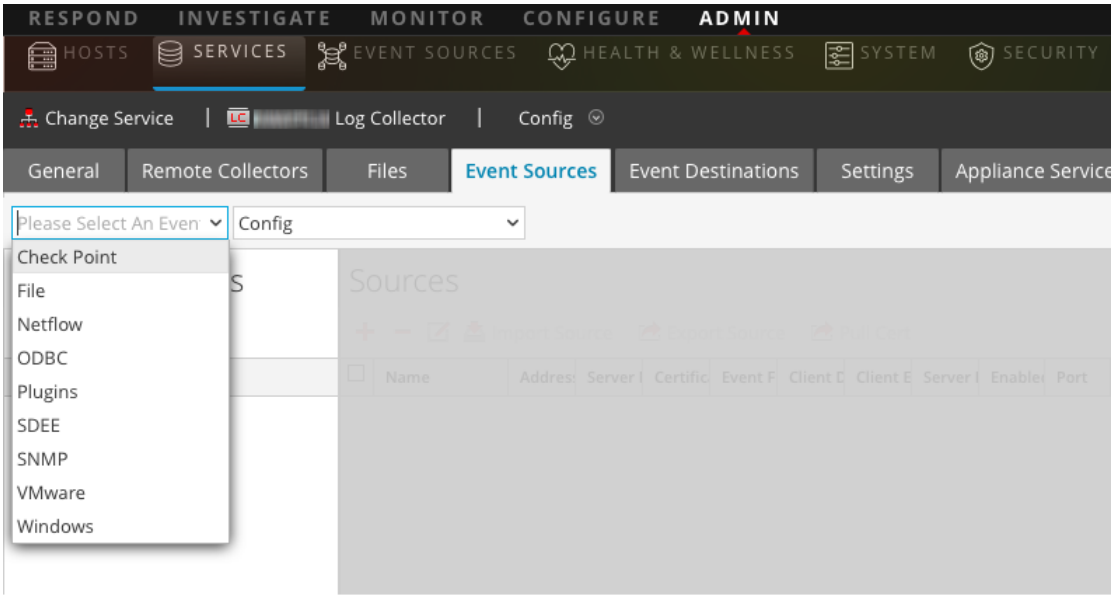
Configurar protocolos y orígenes de eventos de recopilación

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.

Para configurar un protocolo de recopilación:

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
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 un origen de eventos.
7. Seleccione la categoría que recién se agregó y haga clic en +.
8. Especifique los parámetros del origen de eventos. Para obtener detalles, consulte los temas de cada protocolo de recopilación.

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

Para configurar protocolos de recopilación individuales, consulte los siguientes temas:

- Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite
- Configurar orígenes de eventos de Azure en NetWitness Suite
- Configurar orígenes de eventos de punto de comprobación en NetWitness Suite
- Configurar orígenes de eventos de archivos en NetWitness Suite
- Configurar orígenes de eventos de Netflow en NetWitness Suite
- Configurar orígenes de eventos de ODBC en NetWitness Suite
  - Configurar nombres de orígenes de datos (DSN)
  - Crear un archivo typespec personalizado para la recopilación de ODBC
  - Parámetros de configuración del origen de eventos de ODBC
  - Parámetros de configuración del origen de eventos de DSN de ODBC
- Configurar orígenes de eventos de SDEE en NetWitness Suite
- Configurar orígenes de eventos de SNMP en NetWitness Suite
- Configurar orígenes de eventos de syslog para Remote Collector
- Configurar orígenes de eventos de VMware en NetWitness Suite
- Configurar orígenes de eventos de Windows en NetWitness Suite
- Configuración de la recopilación de Windows existente y NetApp
  - Configurar el recopilador de Windows existente
  - Configurar orígenes de eventos de Windows existente y de NetApp
  - Solucionar problemas de la recopilación de Windows existente y NetApp

Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite

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

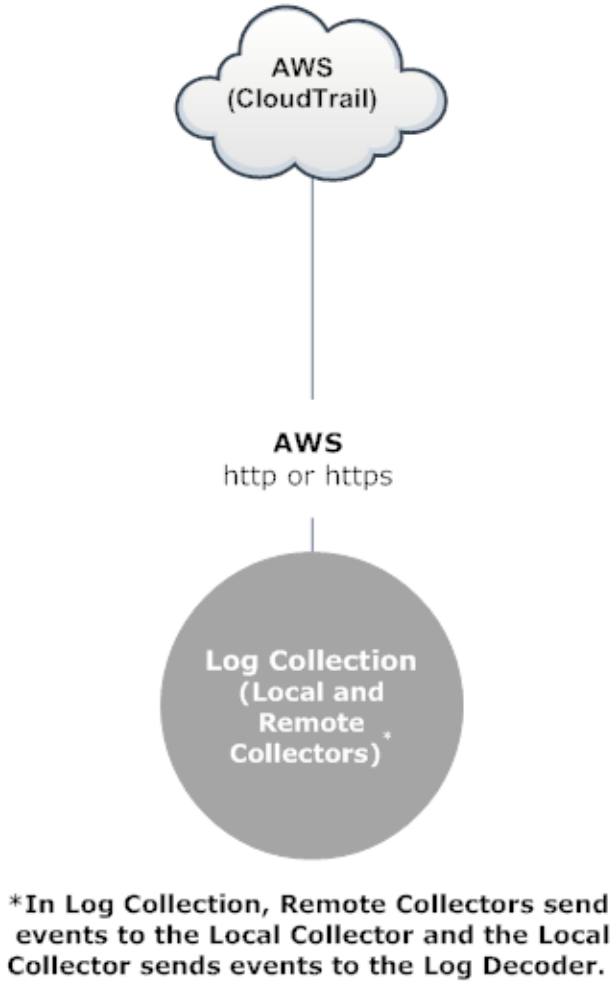
Nota: El plug-in de AWS está diseñado únicamente para la recopilación desde registros de AWS CloudTrail y no para la recopilación desde registros arbitrarios en depósitos S3 (en directorios arbitrarios). Los registros de AWS CloudTrail se envían en formato JSON, como se describe en la documentación de AWS que se encuentra en la siguiente dirección: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html.

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. NetWitness Suite 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 debe implementar el protocolo de recopilación de AWS en NetWitness Suite.

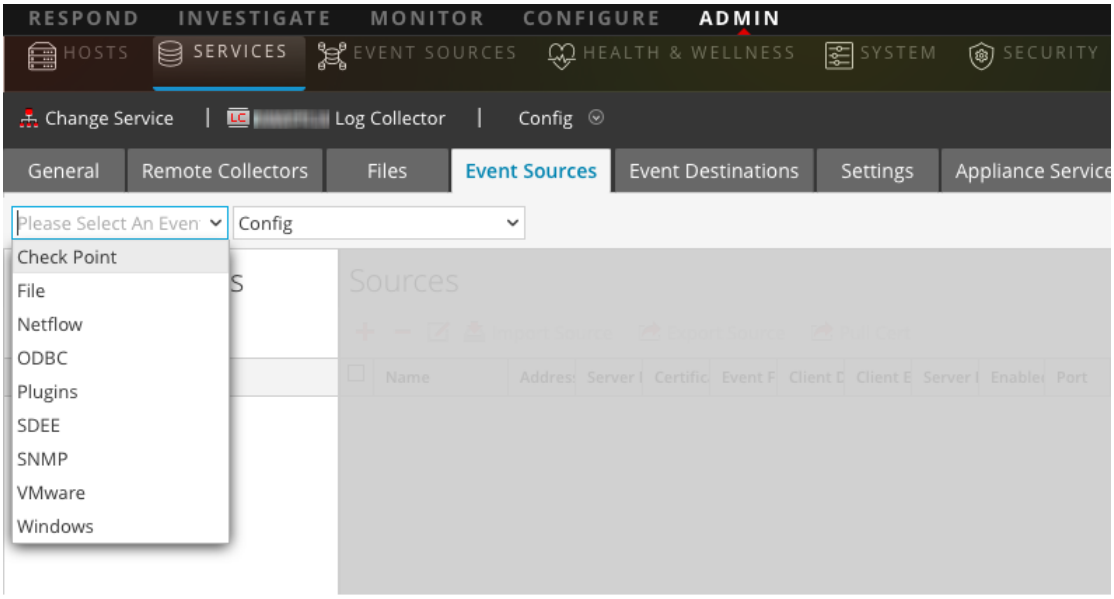


Configuración

Para configurar un origen de eventos de AWS (CloudTrail):

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

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



5. En la pestaña **Orígenes de eventos**, seleccione **Plug-ins/Configuración** en el menú desplegable.
6. 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**.
7. Seleccione **cloudtrail** y haga clic en **Aceptar**.

   El tipo de origen de eventos 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 **Orígenes**.

   Se muestra el cuadro de diálogo **Agregar origen**.
9. Definir valores de parámetros. Para obtener más información, consulte Parámetros de AWS a continuación.
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 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 supera el límite de tiempo, se agota el tiempo de espera de la prueba y NetWitness Suite muestra un mensaje de error.
11. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**.

    El nuevo origen de eventos se muestra en el panel **Orígenes**.

Parámetros de AWS

En la siguiente tabla se describen los parámetros de configuración disponibles para la recopilación de AWS.

Parámetro	Descripción
Parámetro	**Descripción**
	Básico
Nombre *	Nombre del origen de eventos.
Habilitado 	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.
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.
Terminal de región	Especifica el nombre de host de AWS CloudTrail. Por ejemplo, para una nube pública de AWS para la región este de EE. UU., el Terminal de región sería s3.amazonaws.com. Encontrará más información en http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. Este parámetro es necesario para recopilar registros CloudTrail de nubes gubernamentales o privadas de AWS.
Usar proxy	Habilite **Usar proxy** para configurar el proxy para el servidor de AWS. De manera predeterminada, está deshabilitada.
Servidor proxy	Ingrese el nombre de proxy que desea conectar para acceder al servidor de AWS.
Puerto proxy	Ingrese el número de puerto que se conecta al servidor proxy para acceder al servidor de AWS.
Usuario de proxy	Ingrese el nombre de usuario para autenticar con el servidor proxy.
Contraseña de proxy	Ingrese la contraseña para autenticarse con el puerto de proxy.
Fecha de inicio *	Inicia la recopilación de AWS (CloudTrail) a partir de la cantidad especificada de días en el pasado, que se miden a contar del registro de fecha y hora actual. El valor predeterminado es 0, que se inicia a partir de hoy. El rango es de 0 a 89 días.
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.
Opciones avanzadas	

Parámetro	Descripción
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. Habilita o deshabilita el registro de depuración del origen de eventos. Los valores válidos son: • **Desactivado** = (predeterminado) deshabilitado • **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.
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 programa 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 subprocesos 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.

Parámetro	Descripción
Probar conexión	Valida que los parámetros de configuración especificados en este cuadro de diálogo estén correctos. Por ejemplo, esta prueba valida que: • NetWitness se pueda conectar al depósito S3 en AWS con el uso de las credenciales especificadas en este cuadro de diálogo. • NetWitness pueda 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).
Aceptar	Agrega los valores de los parámetros actuales como un nuevo origen de eventos AWS (CloudTrail).

Configurar orígenes de eventos de Azure en NetWitness Suite

En este tema se indica cómo configurar el protocolo de recopilación de Azure. Microsoft Azure es una plataforma y una infraestructura de cómputo en la nube que permite crear, implementar y administrar aplicaciones y servicios mediante una red global de centros de datos que administra Microsoft.

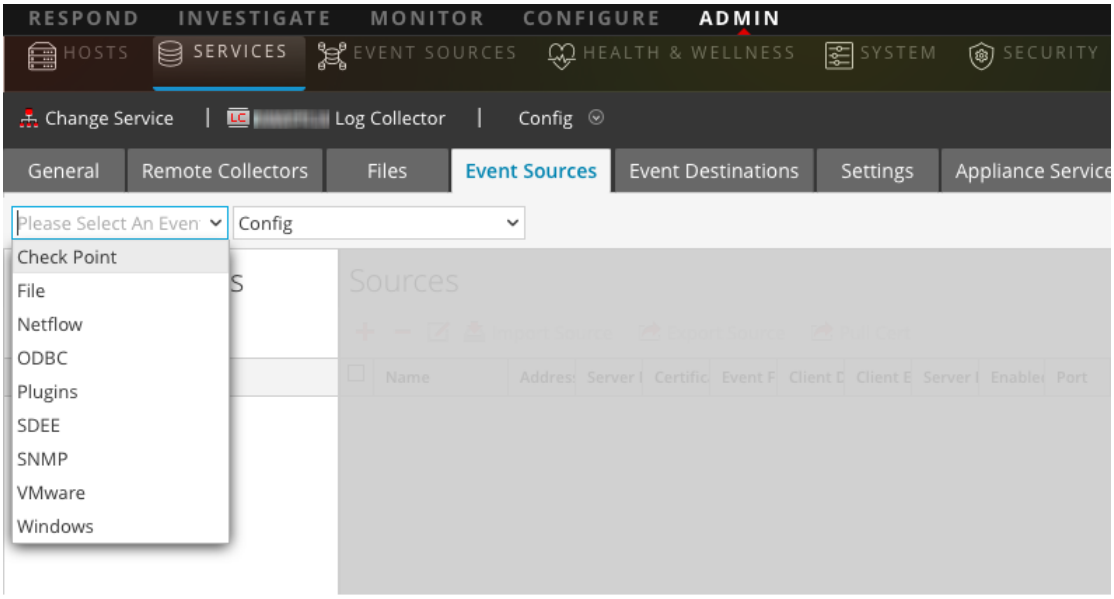
Configuración en NetWitness Suite

Para obtener información detallada acerca de la configuración de Azure como un origen de eventos, consulte la Guía de configuración del origen de eventos de Azure, disponible en RSA Link.

Para configurar un origen de eventos de Azure:

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

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



5. En la pestaña **Orígenes de evento**, seleccione **Plug-ins/Configurar** en el menú desplegable.
6. 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**.
7. Seleccione **azureaudit** y haga clic en **Aceptar**.

   El tipo de origen de eventos 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 **Orígenes**.

   Se muestra el cuadro de diálogo **Agregar origen**.
9. Definir valores de parámetros. Para obtener más información, consulte Parámetros de Azure a continuación.
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 fue satisfactorio, edite la información del dispositivo o del servicio e inténtelo nuevamente.

    Log Collectortarda aproximadamente 60 segundos en devolver los resultados de la prueba. Si se supera el límite de tiempo, se agota el tiempo de espera de la prueba y NetWitness Suite muestra un mensaje de error.
11. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**.

    El nuevo origen de eventos se muestra en el panel **Orígenes**.

Parámetros de Azure

En esta sección se describen los parámetros de configuración del origen de eventos de Azure.

Nota: Se requieren elementos seguidos de un asterisco (*).

Parámetros básicos

Nombre	Descripción
Nombre *	Ingrese un nombre descriptivo alfanumérico para el origen. Este valor solo se usa para mostrar el nombre en esta pantalla.
Habilitado	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.
ID de cliente *	El ID de cliente se encuentra en la pestaña Configuración de la aplicación de Azure. Desplácese hacia abajo hasta que lo vea.
Seña secreta del cliente *	Cuando configure el origen de eventos, la seña secreta del cliente aparecerá en el momento en que cree una clave y seleccione una duración de validación. Asegúrese de guardarla, ya que solo podrá verla una vez y no se puede recuperar más adelante.
URL base de recursos de API *	Ingrese `https://management.azure.com/`. Asegúrese de incluir la barra diagonal final (/).
Terminal de metadatos de federación *	En la aplicación de Azure, haga clic en el botón **Ver terminales** (cerca de la parte inferior del panel). Existen muchos vínculos que comienzan con la misma cadena. Compare las direcciones URL y busque la cadena común con la que comienza la mayoría de ellas. Esta cadena común es el terminal que debe ingresar aquí.
ID de suscripción *	Puede encontrarlo en el tablero de Microsoft Azure: haga clic en Suscripciones en la parte inferior de la lista a la izquierda.
Dominio de grupo de usuarios *	Vaya a Active Directory y haga clic en el directorio. En la dirección URL, el dominio de grupo de usuarios es la cadena que viene directamente después de **manage.windowsazure.com/**. El dominio de grupo de usuarios es la cadena que incluye hasta **.com**.

Nombre	Descripción
Nombres del grupo de recursos *	En Azure, seleccione los grupos Recurso en el panel de navegación izquierdo y luego elija su grupo.
Fecha de inicio *	Elija la fecha a partir de la cual iniciar la recopilación. La fecha actual es el valor predeterminado.
Probar conexión	Comprueba los parámetros de configuración especificados en este cuadro de diálogo para asegurarse de que estén correctos.

Parámetros avanzados

Haga clic en  junto a **Opciones avanzadas** para ver y editar los parámetros avanzados, si es necesario.

Nombre	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, 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, en segundos, de un ciclo de sondeo. Un valor cero indica que no hay un límite.
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	La duración máxima, en segundos, de un ciclo de sondeo. Un valor cero indica que no hay un límite.
Argumentos de comando	Los argumentos opcionales que se agregarán a la invocación de script.

Nombre	Descripción
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. **Precaución:** Habilita o deshabilita el registro de depuración del origen de eventos. Los valores válidos son: • **Desactivado** = (predeterminado) deshabilitado • **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.

Configurar orígenes de eventos de punto de comprobación en NetWitness Suite

En este tema se indica cómo configurar el protocolo de recopilación de punto de control que recopila eventos desde un origen de eventos de punto de control.

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.

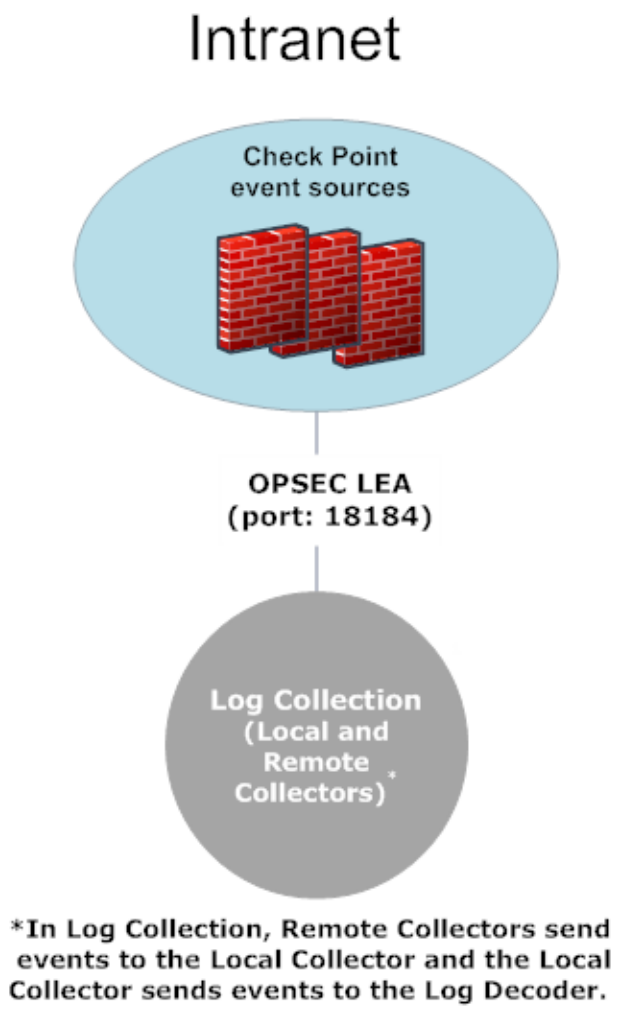
Cómo funciona la recopilación de punto de comprobación

El servicio Log Collector 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.

Nota: OPSEC LEA (API de exportación de registros) admite la extracción de registros de orígenes de eventos de punto de control configurados con un certificado SHA-256 o SHA-1.

Escenario de implementación

En la siguiente figura se ilustra cómo debe implementar el protocolo de recopilación de punto de comprobación en NetWitness Suite.

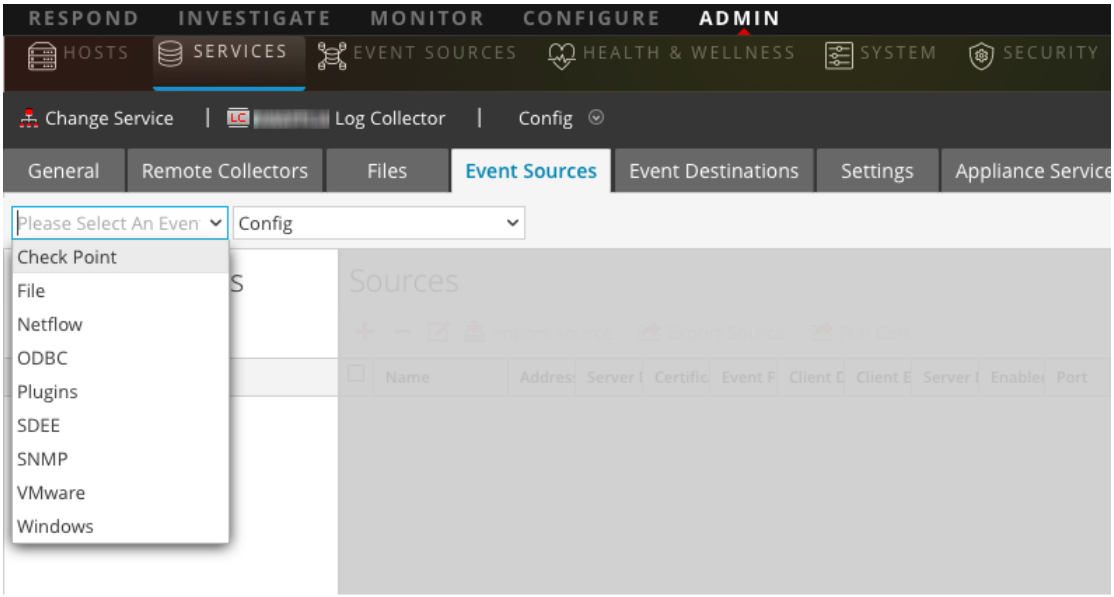


Configuración en NetWitness Suite

Para configurar un origen de eventos de punto de control:

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

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



5. En la pestaña **Orígenes de evento**, seleccione **Punto de comprobación/Configurar** en el menú desplegable.
6. 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**.
7. Seleccione un tipo de origen de eventos de punto de control y haga clic en **Aceptar**.

   El tipo de origen de eventos 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 **Orígenes**.

   Se muestra el cuadro de diálogo **Agregar origen**.
9. Definir valores de parámetros. Para obtener más información, consulte Parámetros de punto de control a continuación.
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 fue satisfactorio, edite la información del dispositivo o del servicio e inténtelo nuevamente.

    Log Collectortarda aproximadamente 60 segundos en devolver los resultados de la prueba. Si se supera el límite de tiempo, se agota el tiempo de espera de la prueba y NetWitness Suite muestra un mensaje de error.
11. Si la prueba se ejecuta correctamente, haga clic en **Aceptar**.

    El nuevo origen de eventos se muestra en el panel **Orígenes**.

Parámetros de punto de control

En esta sección se describen los parámetros de configuración del origen de eventos de punto de control.

Parámetros básicos

Parámetro	Descripción
Nombre*	Nombre del origen de eventos.
Dirección*	Dirección IP del servidor del punto de comprobación.
Nombre del servidor*	Nombre del servidor del punto de comprobación.
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.
Habilitado	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.
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.

Parámetro	Descripción
Dirección del servidor de certificados	Dirección IP del servidor en el cual reside el certificado. El valor predeterminado es la dirección de origen de eventos.
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.

Determinar los valores de los parámetros avanzados para la recopilación de punto de control

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). RSA NetWitness Suite 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**

Parámetro	Descripción
Puerto	Puerto del servidor del punto de control al cual se conecta Log Collector. El valor predeterminado es 18184.
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 logs desde	Cuando configura un origen de eventos de punto de control, NetWitness 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). • **Inicio de log**: Recopilar registros desde el comienzo del archivo de registro actual. Si selecciona “Inicio de log” 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. Tenga en cuenta que esta opción es eficaz únicamente para la primera sesión de recopilación.
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.
Reenviador	Habilita o deshabilita el servidor del punto de control como un reenviador. De manera predeterminada, está deshabilitada.
Tipo de registro (par de nombre/valor)	Registros desde el origen de eventos en formato nombre/valor. De manera predeterminada, está deshabilitada.

Parámetro	Descripción
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: • **Desactivado** = (predeterminado) deshabilitado • **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).

Verificar que la recopilación de punto de control esté funcionando

En el siguiente procedimiento se ilustra cómo puede verificar que la recopilación de punto de control esté funcionando en **Administration > Estado y condición > pestaña Monitoreo de orígenes de eventos**.

1. Acceda a la **pestaña Monitoreo de orígenes de eventos** en 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 comprobación acepte eventos.

En la siguiente figura se ilustra cómo puede verificar que la recopilación de punto de control esté funcionando en la vista **Investigation > Eventos**.

1. Acceda a la vista **Investigation > 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.

Nota: Si los registros del servidor de firewall de punto de control de VSX se recopilan mediante el servicio de punto de control de Log Collector, para convertir la IP VSX de los registros en metadatos **ip.orig**, debe agregar el nombre de host VSX y la dirección IP de VSX en el archivo `/etc/hosts` de Log Collector.

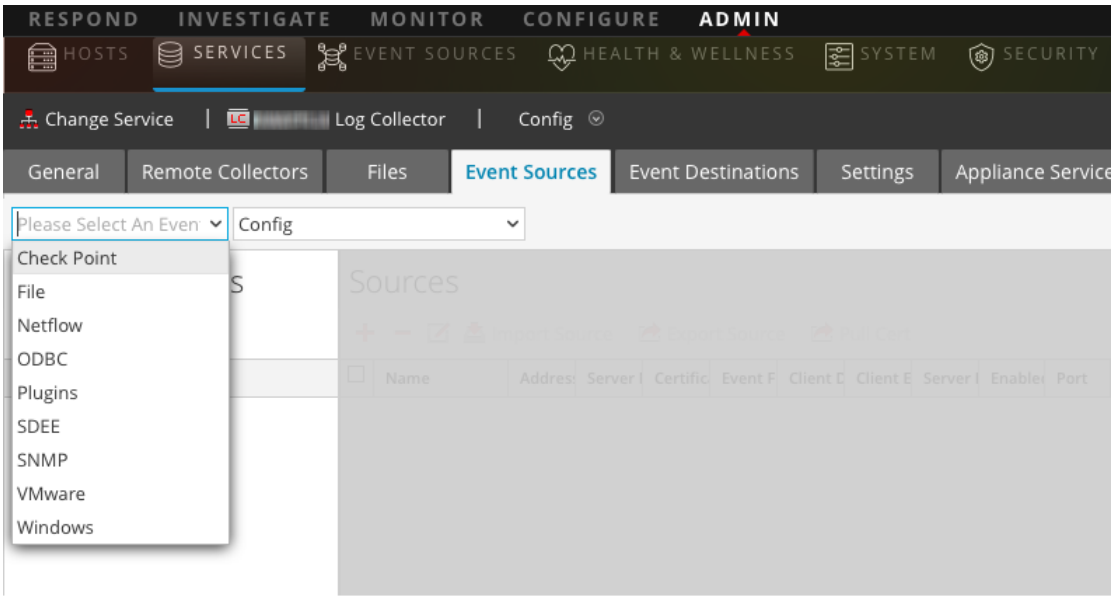
Configurar orígenes de eventos de archivos en NetWitness Suite

En esta guía se describe cómo configurar el protocolo de recopilación de archivos.

Para configurar un origen de eventos de archivo

Para configurar un origen de eventos de archivo:

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. En la pestaña **Orígenes de evento**, seleccione **Archivo/Configuración** en el menú desplegable.

6. 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**.

7. Seleccione un tipo de origen de eventos de archivo y haga clic en **Aceptar**.

   El tipo de origen de eventos 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 **Orígenes**.

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

9. Agregue un nombre de **directorio de archivo** y modifique cualquier otro parámetro que requiera cambios. Para obtener más información, consulte Parámetros de la recopilación de registros a continuación.

10. 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**.

11. Haga clic en **Aceptar**.

Para que sus cambios surtan efecto, debe reiniciar la recopilación de archivos.

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 NetWitness Suite. Esto es necesario para agregar la clave al nuevo origen de eventos.

Parámetros de la recopilación de registros

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

Nombre	Descripción
Básico	

Nombre	Descripción
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
Habilitado	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.
Opciones avanzadas	

Nombre	Descripción
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 su procesamiento de recopilación normal estimado. **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.
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.

Nombre	Descripción
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 la sección *Generar un par de claves en el origen de eventos e importar la clave pública a Log Collector* en la Guía de instalación y actualización del agente de SFTP para obtener instrucciones sobre la generación de claves. **Nota:** Si la recopilación de archivos se detiene, NetWitness Suite 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 NetWitness Suite 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.
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 NetWitness Suite 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 se reinicia la recopilación o el servicio Log Collector.

Nombre	Descripción
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 se reinicia la recopilación o el servicio Log Collector.
% de reducción de archivos de error	Porcentaje por tamaño o conteo de archivos de error que el servicio Log Collector elimina 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.
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 se reinicia la recopilación o el servicio Log Collector.

Nombre	Descripción
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 se reinicia la recopilación o el servicio Log Collector.
% de reducción de archivos guardados	Porcentaje por tamaño o conteo de archivos guardados que el servicio Log Collector elimina 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 habilitación de la depuración afectará negativamente el rendimiento del Log Collector. Habilita/deshabilita el registro de depuración del origen de eventos. Los valores válidos son: • **Desactivado** = (predeterminado) deshabilitado • **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.
Aceptar	Agrega los parámetros del origen de eventos.

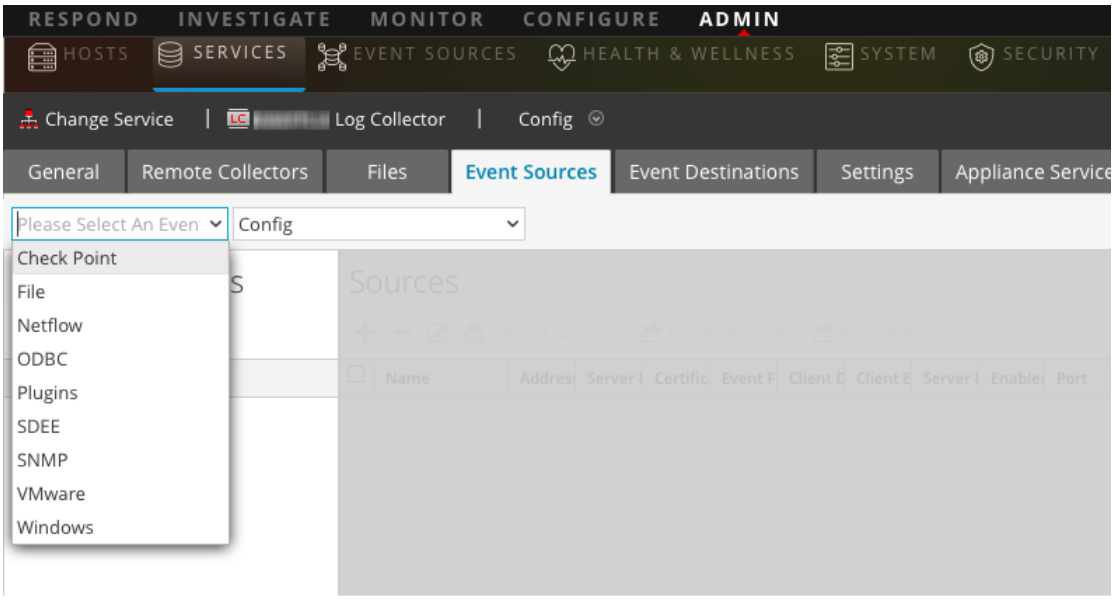
Configurar orígenes de eventos de Netflow en NetWitness Suite

En este tema se describe cómo configurar el protocolo de recopilación de Netflow.

Configurar un origen de eventos de Netflow

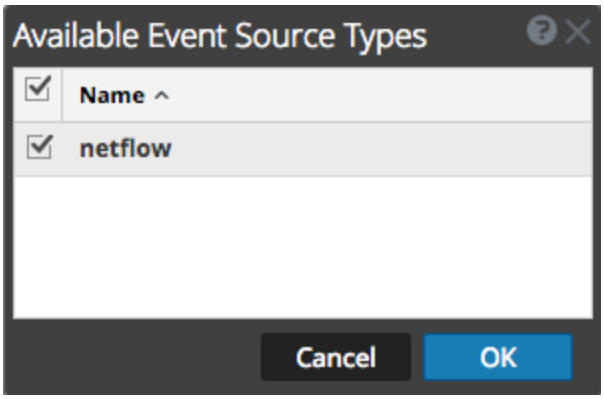
Para configurar un origen de eventos de Netflow:

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. En la pestaña **Orígenes de evento**, seleccione **Netflow/Configuración** en el menú desplegable.
6. 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**.
7. Seleccione el tipo de origen de eventos **netflow** y haga clic en **Aceptar**.



El tipo de origen de eventos 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 **Orígenes**.

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

9. Ingrese un número de puerto en el campo **Puerto** y asegúrese de que esté seleccionada la casilla Habilitado.

   Nota: NetWitness Suite abre los puertos 2055, 4739, 6343 y 9995 en el firewall de manera predeterminada. Puede abrir otros puertos para Netflow si es necesario.

   Para obtener detalles de otros parámetros, consulte Parámetros de recopilación de Netflow a continuación.

10. Haga clic en **Aceptar**.

El nuevo origen de eventos se muestra en la lista.

Parámetros de recopilación de Netflow

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

Nombre	Descripción
	Básico
Puerto	Especifique el número de puerto configurado para el origen de eventos de Netflow. NetWitness Suite abre los puertos 2055, 4739, 6343 y 9995 para Netflow de forma predeterminada. Puede abrir otros puertos para Netflow si es necesario.

Nombre	Descripción
Habilitado	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.
	Opciones avanzadas
Umbral de registro de publicación en transferencia	Establece un umbral y, cuando se alcanza, NetWitness Suite genera un mensaje de registro para ayudarlo a resolver problemas relacionados con el flujo de eventos. El umbral es el tamaño de los mensajes de eventos de netflow que fluyen actualmente desde el origen de eventos a NetWitness Suite. Los valores válidos son: • **0 (valor predeterminado)**: Deshabilita el mensaje de registro. • **100-100,000,000**: 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, NetWitness Suite 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 habilitación de la depuración afectará negativamente el rendimiento del Log Collector. Habilita o deshabilita el registro de depuración del origen de eventos. Los valores válidos son: • **Desactivado** = (predeterminado) deshabilitado • **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.
Aceptar	Agrega los parámetros del origen de eventos.

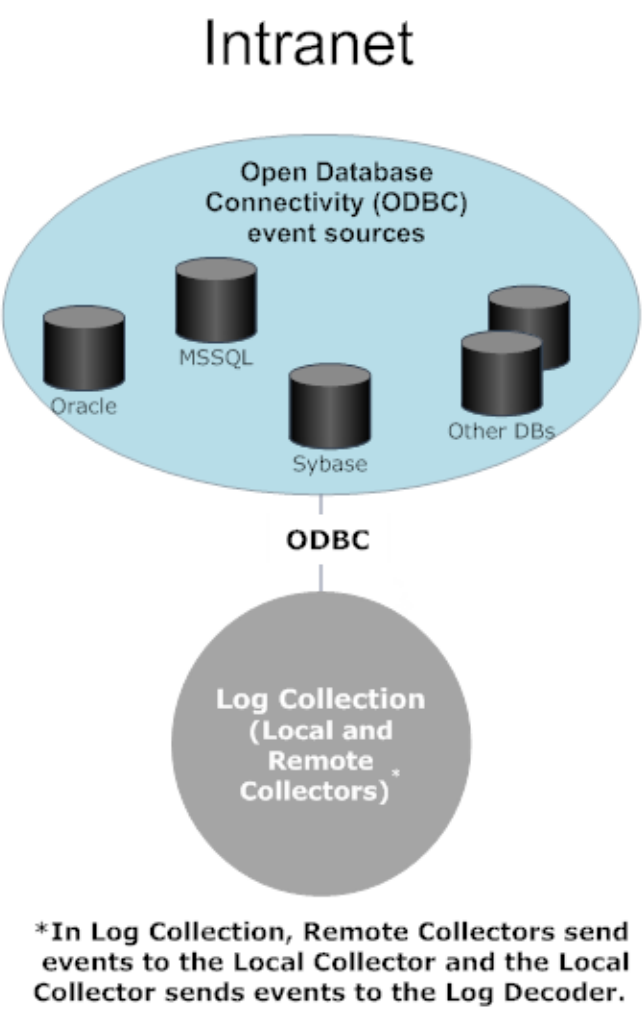
ODBC

Configurar orígenes de eventos de ODBC en NetWitness Suite

En este tema 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 NetWitness Suite.



Configurar un origen de eventos de ODBC

Para configurar un origen de eventos de ODBC, debe configurar un tipo de origen de eventos y elegir una plantilla DSN.

Configurar un DSN

En el siguiente procedimiento se describe cómo agregar un DSN desde una plantilla DSN existente. Para otros procedimientos relacionados con DSN, consulte Configurar nombres de orígenes de datos (DSN).

Configurar un DSN (nombre de origen de datos):

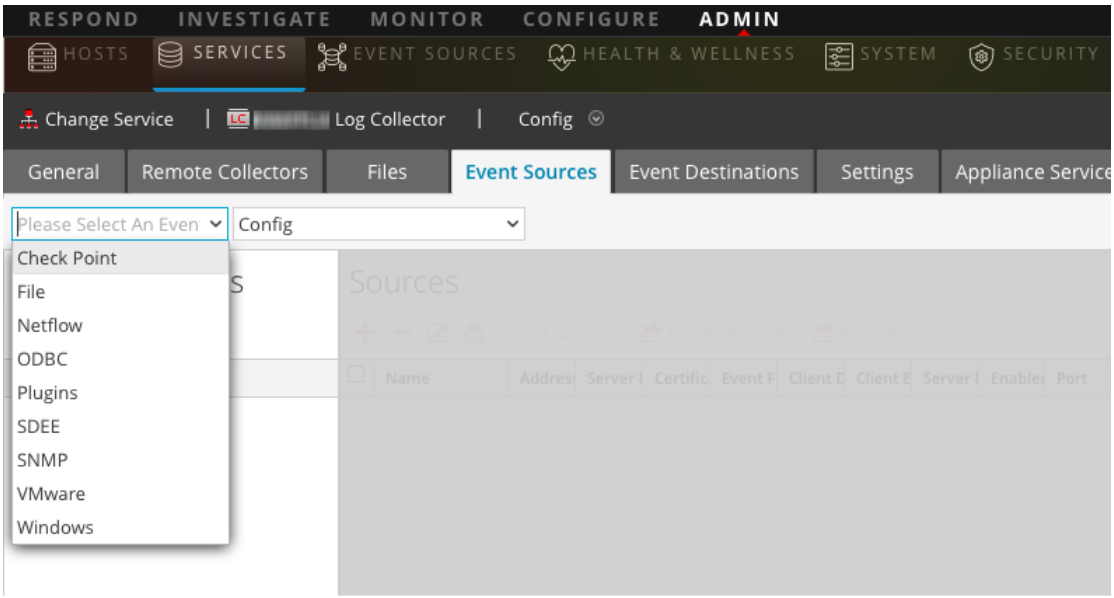
1. Vaya a **Administration** > **Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Collector**.
3. Haga clic en bajo **Acciones** y seleccione **Ver** > **Configuración**.

4. En la pestaña **Orígenes de evento de Log Collector**, seleccione **ODBC/DSN** en el menú desplegable.
5. El panel DSN se muestra con los DSN que existen, si los hay.
6. Haga clic en + para abrir el cuadro de diálogo **Agregar DSN**.
7. Elija una plantilla DSN en el menú desplegable y escriba un nombre para el DSN. (Use el nombre cuando configure el tipo de origen de eventos de ODBC). Si es necesario, haga clic en Manage Templates para agregar o eliminar plantillas DSN.
8. Rellene los parámetros y haga clic en **Guardar**.

Agregar un tipo de origen de eventos

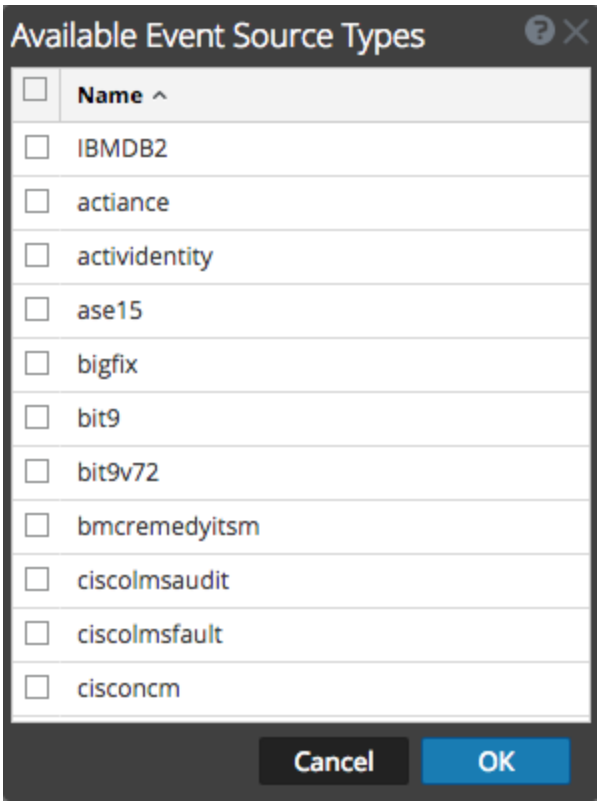
Para configurar un tipo de origen de eventos de ODBC:

1. Vaya a **ADMIN >Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione > **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. En la pestaña **Orígenes de evento**, seleccione **ODBC/Configuración** en el menú desplegable.
6. 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**.

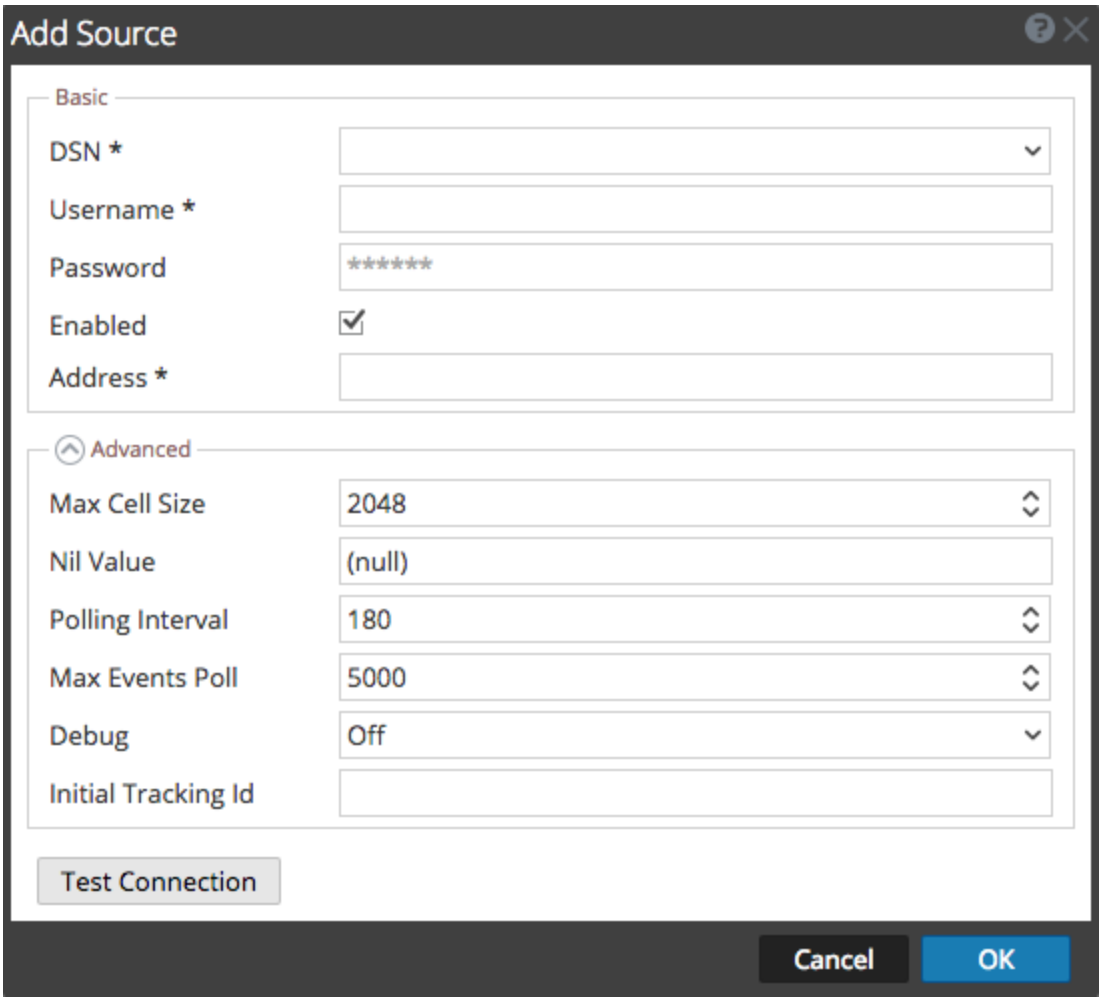


7. Seleccione una categoría de origen de eventos, por ejemplo, **mssql**, y haga clic en **Aceptar**.

   El tipo de origen de eventos 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 **Orígenes**.

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



9. Seleccione un DSN en la lista desplegable, especifique o modifique los otros parámetros según sea necesario y haga clic en **Aceptar**.
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.

    Nota: Log Collectortarda aproximadamente 60 segundos en devolver los resultados de la prueba. Si se supera el límite de tiempo, se agota el tiempo de espera de la prueba y el servidor de NetWitness Suite 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**.

Parámetros de recopilación de ODBC

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

Configurar nombres de orígenes de datos (DSN)

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.

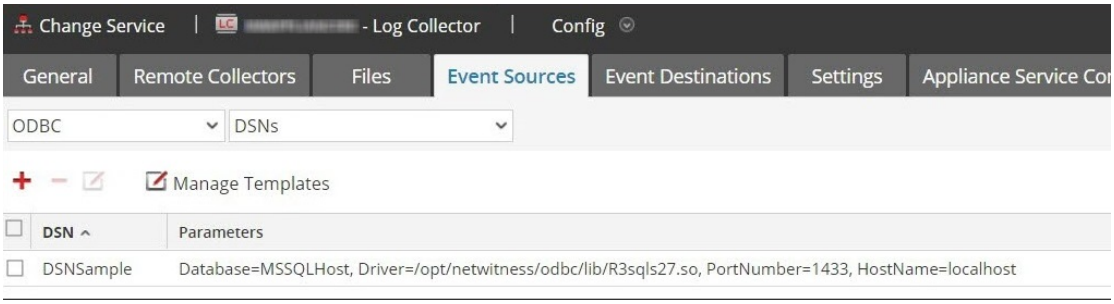
Navegue al Panel DSN

Para agregar o editar DSN o plantillas DSN, navegue a la pantalla adecuada.

Para navegar al panel de plantillas DSN:

1. Vaya a **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio de **Log Collector**.
3. Haga clic en  bajo **Acciones** y seleccione **Ver > Configuración**.
4. En la pestaña **Orígenes de evento deLog Collector**, seleccione **ODBC/DSN** en el menú desplegable.

   El panel **DSN** se muestra con los DSN que se agregaron, si los hay.



En esta pantalla puede realizar las siguientes acciones:

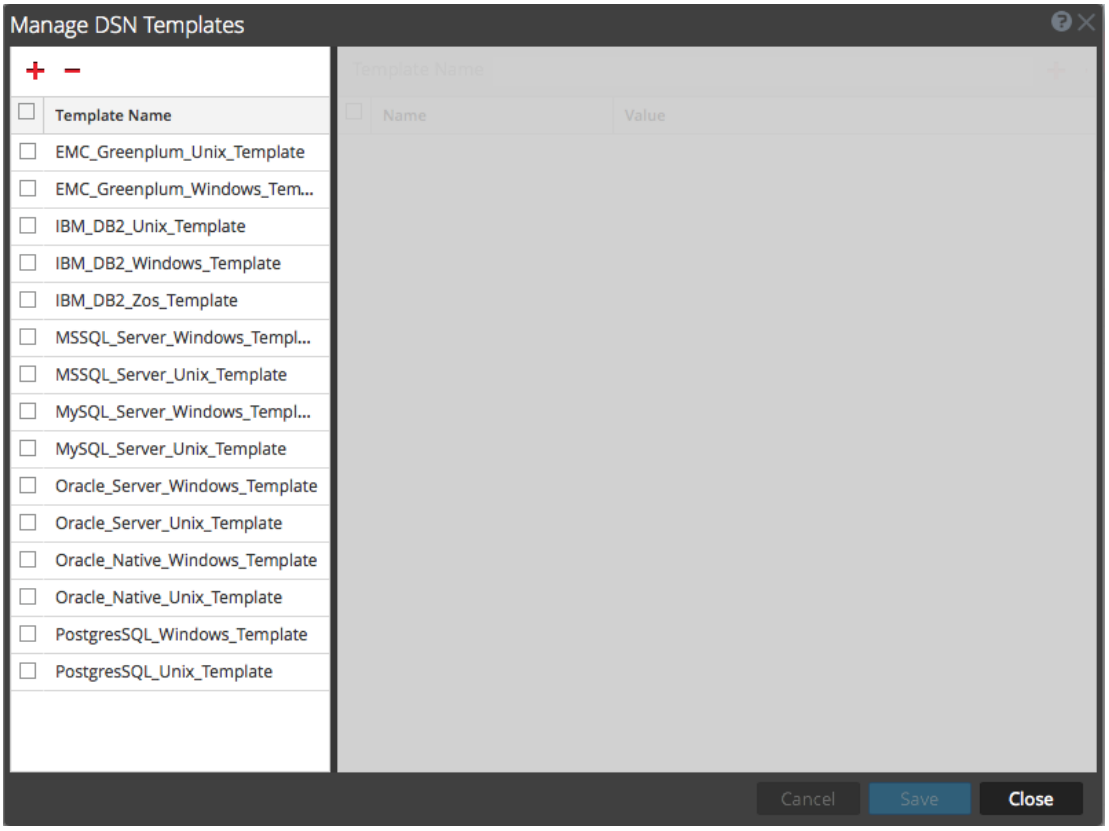
- Agregar una plantilla DSN nueva
- Agregar un DSN de una plantilla existente
- Agregar un DSN mediante la edición de una plantilla DSN existente
- Quitar un DSN o una plantilla DSN

Agregar una plantilla DSN nueva

Si ninguna de las plantillas DSN predefinidas satisface sus necesidades, use este procedimiento para agregar una plantilla DSN.

1. En el panel DSN, haga clic en Manage Templates.

   Se muestra el cuadro de diálogo **Administrar plantillas DSN**.



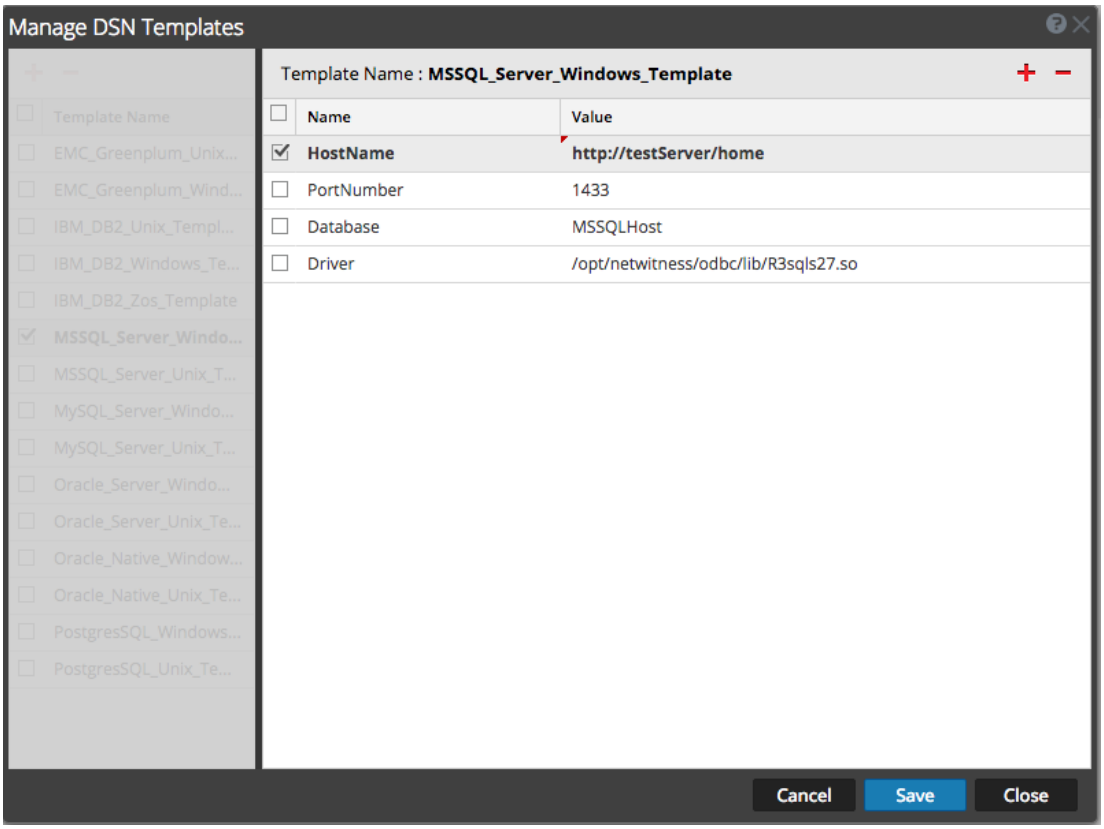
   Nota: RSA proporciona plantillas predeterminadas en el panel del lado izquierdo que puede usar mientras agrega un nuevo DSN.

2. Haga clic en +.

   El panel derecho se activa.

3. Especifique un nombre de plantilla y haga clic en +, en el panel derecho para agregar parámetros.

4. Especifique los parámetros. Haga clic en **Guardar**.



La nueva plantilla DSN se agrega en la lista **Administrar plantillas DSN**.

Agregar un DSN de una plantilla existente

Puede seleccionar una plantilla existente y rellenar los parámetros según sus necesidades.

1. En el panel DSN, haga clic en + para abrir el cuadro de diálogo Agregar DSN.

   Se muestra el cuadro de diálogo **Agregar DSN** con los DSN existentes, si los hay

2. Elija una plantilla DSN en el menú desplegable y escriba un nombre para el DSN. (Use el nombre cuando configure el tipo de origen de eventos de ODBC).
3. Rellene los parámetros y haga clic en **Guardar**.

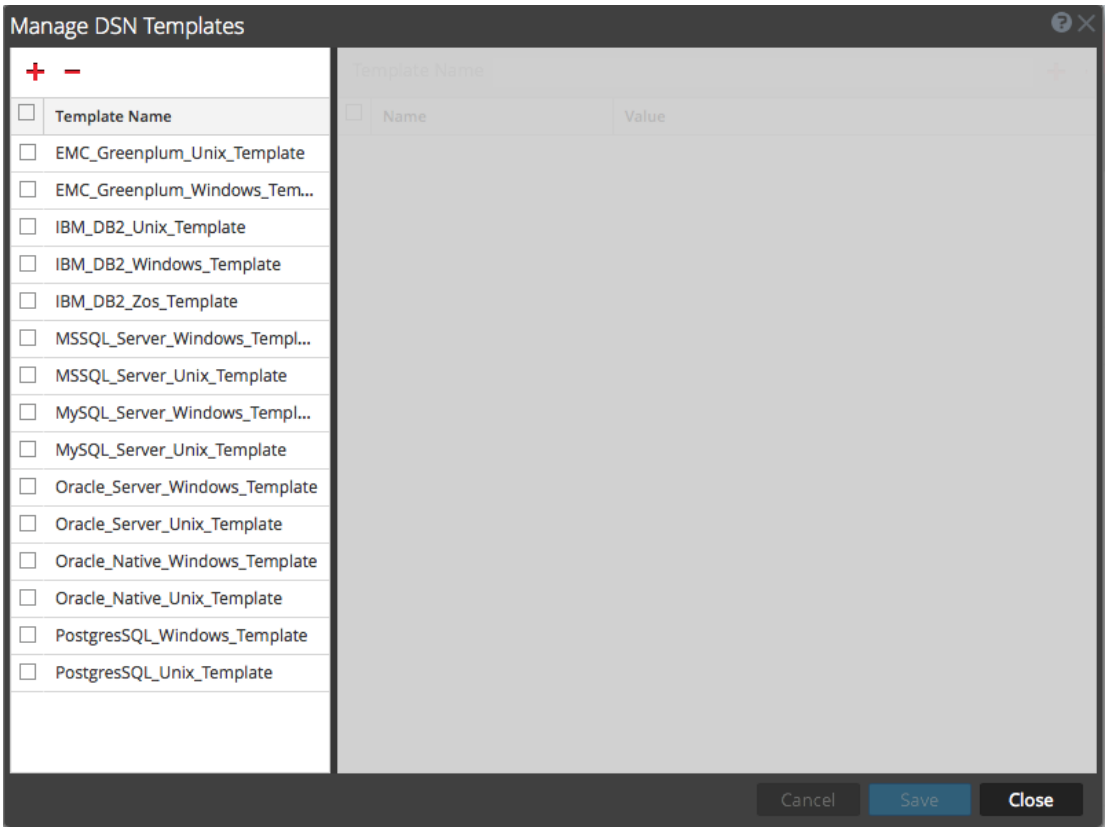
El DSN se agrega a la lista de DSN.

Agregar un DSN nuevo mediante la edición de una plantilla DSN existente

Puede agregar un DSN actualizando una plantilla DSN existente para satisfacer sus necesidades.

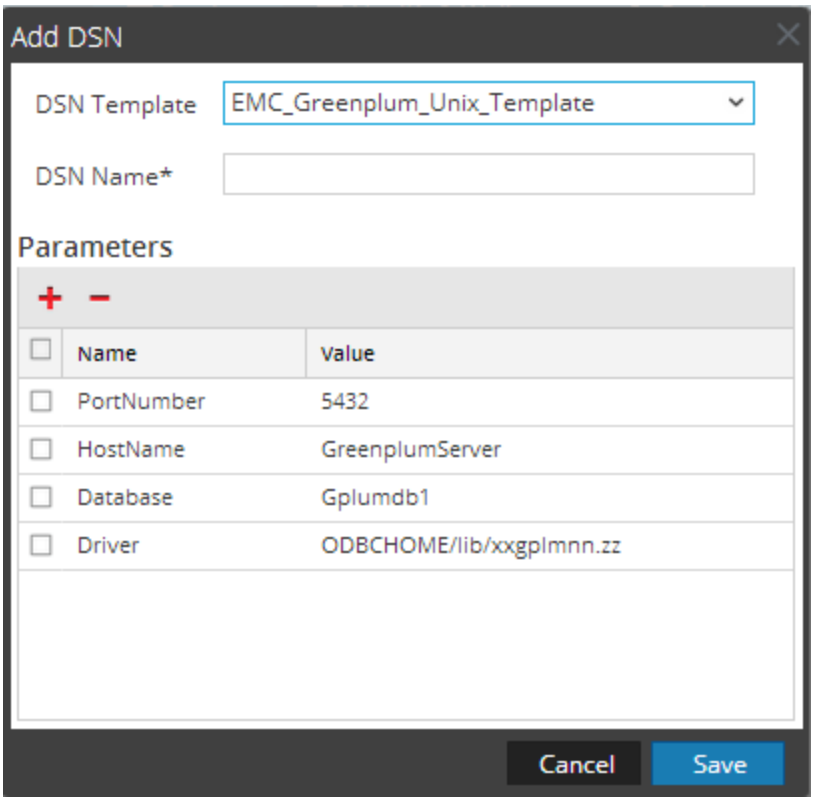
1. En el panel DSN, haga clic en Manage Templates.

   Se muestra el cuadro de diálogo **Administrar plantillas DSN**.



2. Seleccione la plantilla existente que desea modificar.

   El panel derecho se activa y se muestran los parámetros predeterminados para la plantilla seleccionada.



3. Especifique un nombre en el campo **Nombre de DSN**.
4. Agregue, elimine o edite los parámetros predeterminados.
5. Una vez que tenga el conjunto de parámetros requeridos, haga clic en **Guardar** y, a continuación, en **Cerrar**.
6. En el menú desplegable, elija la plantilla DSN que actualizó y escriba un nombre para el DSN. (Use el nombre cuando configure el tipo de origen de eventos de ODBC).
7. Rellene los parámetros y haga clic en **Guardar**.

El DSN se agrega a la lista de DSN.

Quitar un DSN o una plantilla DSN

Si ya no se usa un DSN o una plantilla DSN, puede quitarlo del sistema.

Para quitar un DSN existente:

1. En el panel DSN, seleccione un DSN existente.
2. Haga clic en —.

   Aparece un mensaje de advertencia, que le pregunta si está seguro de que desea eliminar el DSN.

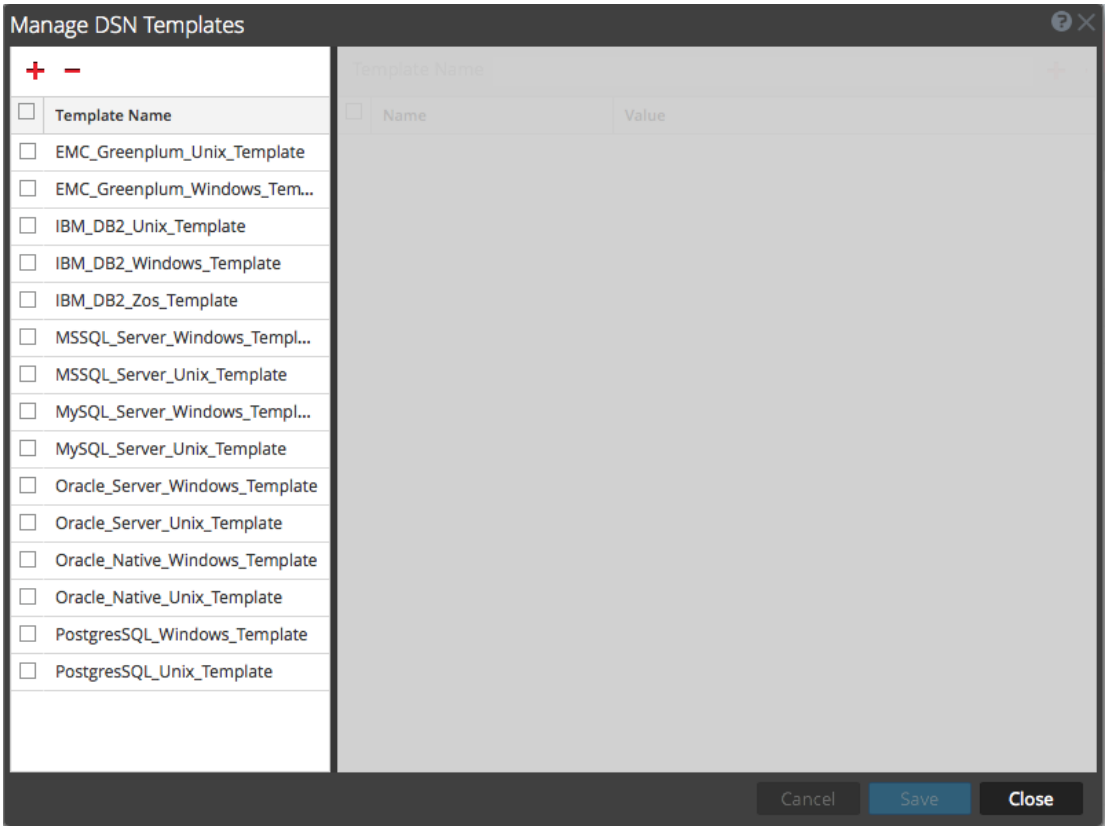
3. Haga clic en **Sí** para eliminar el DSN. Alternativamente, para cancelar la eliminación, haga clic en **No**.

Si confirma la eliminación, el DSN seleccionado se quita del sistema.

Para quitar una plantilla DSN existente:

1. En el panel DSN, haga clic en Manage Templates.

   Se muestra el cuadro de diálogo **Administrar plantillas DSN**.



2. En el panel DSN, seleccione una plantilla DSN existente.
3. Haga clic en −.

   Aparece un mensaje de confirmación, que le pregunta si está seguro de que desea eliminar la plantilla DSN.

4. Haga clic en **Sí** para eliminar la plantilla DSN. Alternativamente, para cancelar la eliminación, haga clic en **No**.

Si confirma la eliminación, la plantilla DSN seleccionada se quita del sistema.

Crear un archivo typespec 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 archivos typespec para la recopilación de ODBC

Crear un archivo typespec personalizado

Para crear un archivo typespec personalizado:

1. Abra un cliente SFTP (por ejemplo, WinSCP) y conéctese a un Log Collector o un Log Collector remoto.
2. Navegue a **/etc/netwitness/ng/logcollection/content/collection/odbc** y copie un archivo existente, por ejemplo **bit9.xml**.
3. Modifique el archivo de acuerdo con los requisitos. Consulte Sintaxis de typespec para la recopilación de ODBC para obtener detalles.
4. Cambie el nombre del archivo y guárdelo en el mismo directorio.
5. Reinicie el Log Collector.

Nota: No podrá ver el nuevo tipo de origen de eventos en NetWitness Suite hasta que reinicie Log Collector.

Sintaxis de typespec para la recopilación de ODBC

En la siguiente tabla se describen los parámetros de typesec.

Parámetro	Descripción
name	El nombre para mostrar del origen de eventos de ODBC (por ejemplo, **activeidentity**). NetWitness Suite muestra este nombre en el panel **Orígenes** de **Ver > Configuración > pestaña Orígenes de eventos**. Un valor válido es unacadena alfanumérica. No puede usar - (guiones), _ (guiones bajos) ni espacios. El nombre debe ser único entre todos los archivos typespec en la carpeta.
type	Tipo de origen de eventos: **odbc**. No modifique esta línea.

Parámetro	Descripción
prettyName	Nombre definido por el usuario para el origen de eventos. Puede usar el mismo valor que name (por ejemplo, apache) o usar un nombre más descriptivo.
version	Versión de este archivo typespec. El valor predeterminado es 1.0.
author	Persona que creó el archivo typespec. Reemplace author-name por su nombre.
descripción	Descripción formal del origen de eventos. Reemplace formal-description por su descripción del origen de eventos.
	Sección <device>
parser	Este parámetro opcional contiene el nombre del analizador de registros. Este valor hace que el Log Decoder utilice el analizador de registros especificado durante el análisis de registros desde este origen de eventos. **Nota:** Deje el campo en blanco cuando no esté seguro del analizador de registros que se utilizará.
name	Nombre del origen de eventos de ODBC (por ejemplo, **ActivIdentity ActivCard AAA Server**).
maxVersion	El número de versión del origen de eventos (por ejemplo, **6.4.1**).
descripción	Descripción del origen de eventos.
	Sección <collection>
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	Esta sección contiene los detalles de la consulta que se usa para recopilar información desde el origen de eventos.
tag	La etiqueta de prefijo que desea agregar a los eventos durante la transformación (por ejemplo, **ActivIdentity**).

Parámetro	Descripción
outputDelimiter	Especifique el delimitador que se usará para separar los campos. Especifique cualquiera de los siguientes valores: • || (barra vertical) • ^ (intercalación) • , (coma) • : (dos puntos) • **0x20** (para representar un espacio)
interval	Especifique la cantidad de segundos entre eventos. El valor predeterminado es **60**.
dataQuery	Especifique la consulta para buscar datos desde la base de datos de origen de eventos de ODBC para SQL-syntax. Por ejemplo: `SELECT acceptedrejected, servername, serveripa, sdate, millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG WHERE sdate > '%TRACKING%' ORDER BY sdate`
maxTrackingQuery	La consulta que se usa en la extracción inicial de eventos para identificar el punto de partida en el conjunto de datos desde el cual se comienzan a extraer registros. Después de la extracción inicial, esta consulta ya no se utiliza, a menos que se haya restablecido o modificado el valor **maxTracking**. Por ejemplo: `SELECT MAX(Event_Id) from ExEvents`
trackingColumn	El valor de la columna de rastreo que se usa cuando el recopilador de ODBC extrae un nuevo conjunto de eventos.

Ejemplo de archivos typespec para la recopilación de ODBC

En el siguiente ejemplo se muestra el archivo typespec para el origen de eventos de IBM ISS SiteProtector.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>siteprotector4_x</name>
   <type>odbc</type>
   <prettyName>SITEPROTECTOR4_X</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
```

```
   <description>Collects events from SiteProtector</description>

   <device>
      <name>Internet Security Systems, Inc. RealSecure SiteProtector v 2.0</name>
      <maxVersion>2.0</maxVersion>
      <description></description>
      <parser>iss</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag></tag>
            <outputDelimiter></outputDelimiter>
            <interval></interval>
            <dataQuery></dataQuery>
            <maxTrackingQuery></maxTrackingQuery>
            <trackingColumn></trackingColumn>
            <levelColumn></levelColumn>
            <eventIdColumn></eventIdColumn>
            <addressColumn></addressColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

En el siguiente ejemplo se muestra el archivo typespec para el origen de eventos de Bit9 Security Platform.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>bit9</name>
   <type>odbc</type>
   <prettyName>BIT9</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Bit9 Events</description>

   <device>
```

```
      <name>Bit9</name>
      <parser>bit9</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag>BIT9</tag>
            <outputDelimiter>||</outputDelimiter>
            <interval>10</interval>
            <dataQuery>
            SELECT
            Timestamp,
            Event_Id,
            Computer_Id,
            File_Catalog_Id,
            Root_File_Catalog_Id,
            Priority,
            Type,
            Subtype,
            IP_Address,
            User_Name,
            Process,
            Description
            FROM
            ExEvents
            WHERE
            Event_Id > '%TRACKING%'
            </dataQuery>
            <trackingColumn>Event_Id</trackingColumn>
            <maxTrackingQuery>SELECT MAX(Event_Id) from
ExEvents</maxTrackingQuery>
            <eventIdColumn></eventIdColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

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:

- Registro de fecha y hora
- 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.

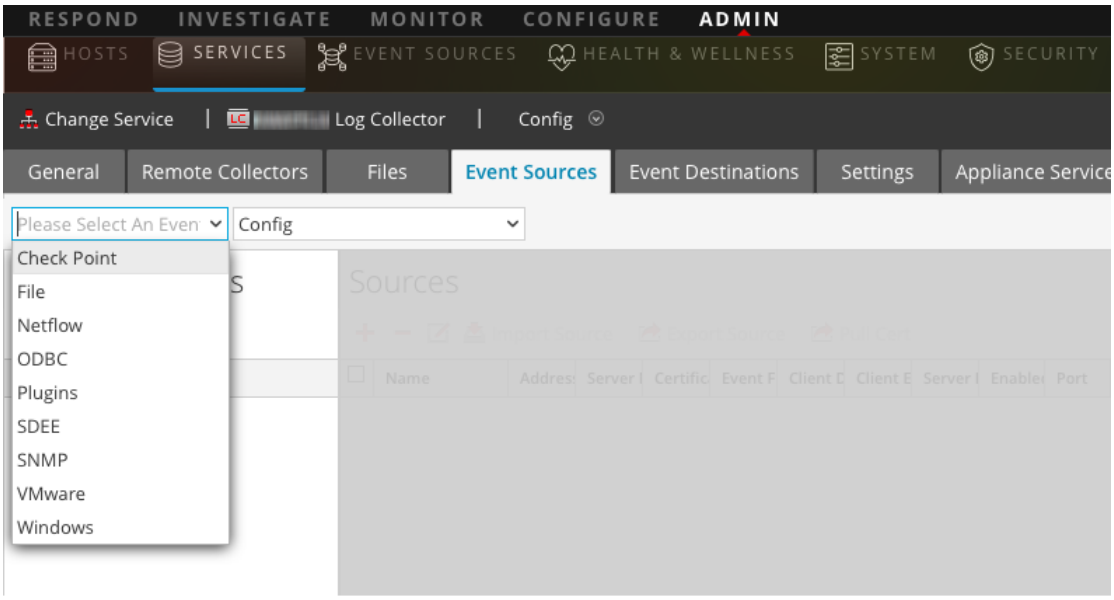
Configurar orígenes de eventos de SDEE en NetWitness Suite

En este tema se indica cómo configurar el protocolo de recopilación de SDEE.

Configurar un origen de eventos de SDEE

Para agregar un origen de eventos de SDEE:

1. Vaya a **ADMIN >Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. 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.

6. En la barra de herramientas del panel **Categorías de evento**, haga clic en  .

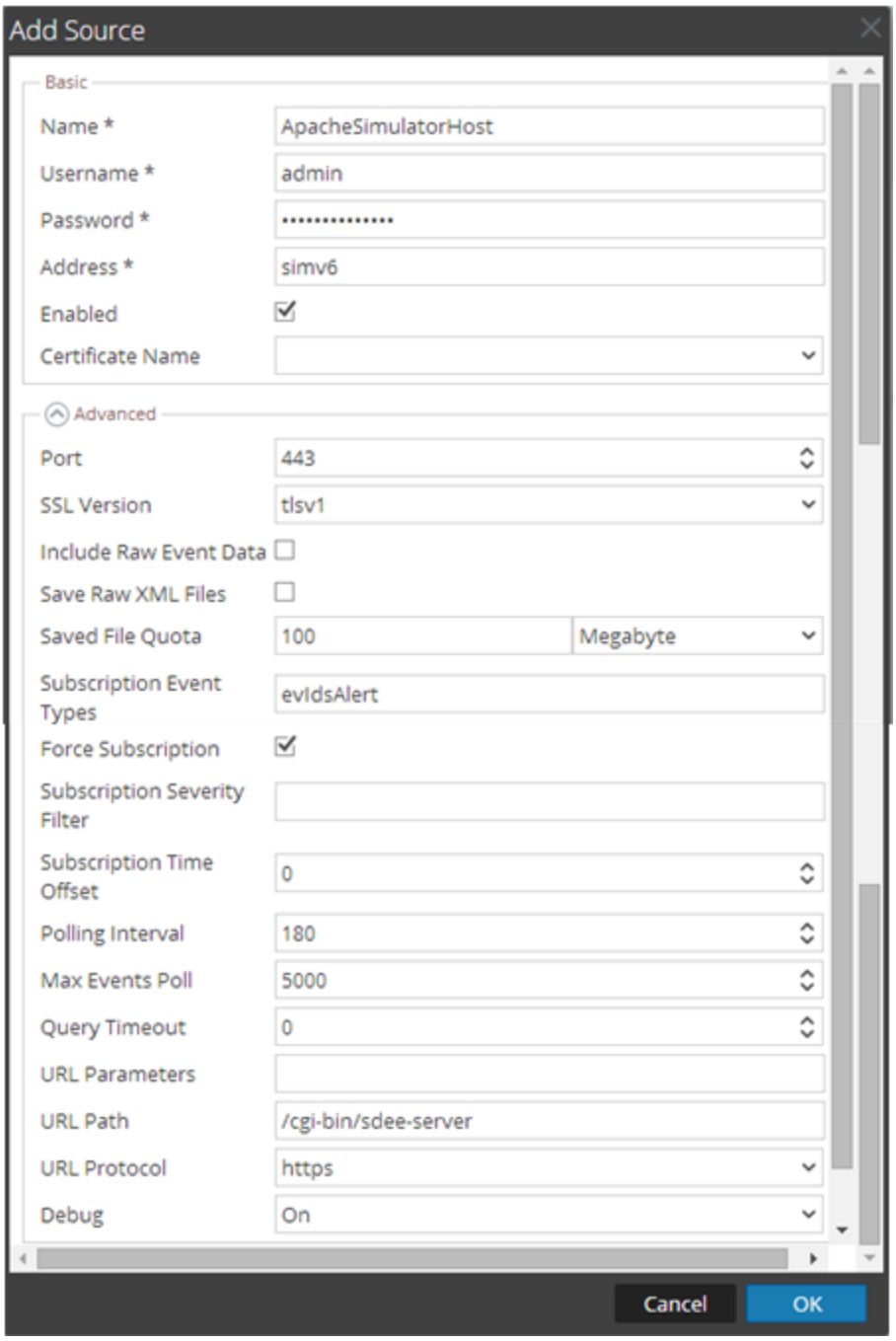
   Se muestra el cuadro de diálogo **Tipos de origen de evento disponibles**.

7. Seleccione un tipo de origen de eventos y haga clic en **Aceptar**.

   El tipo de origen de eventos 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 Orígenes.

   Se muestra el cuadro de diálogo Agregar origen.



9. 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**.

Configurar orígenes de eventos de SNMP en NetWitness Suite

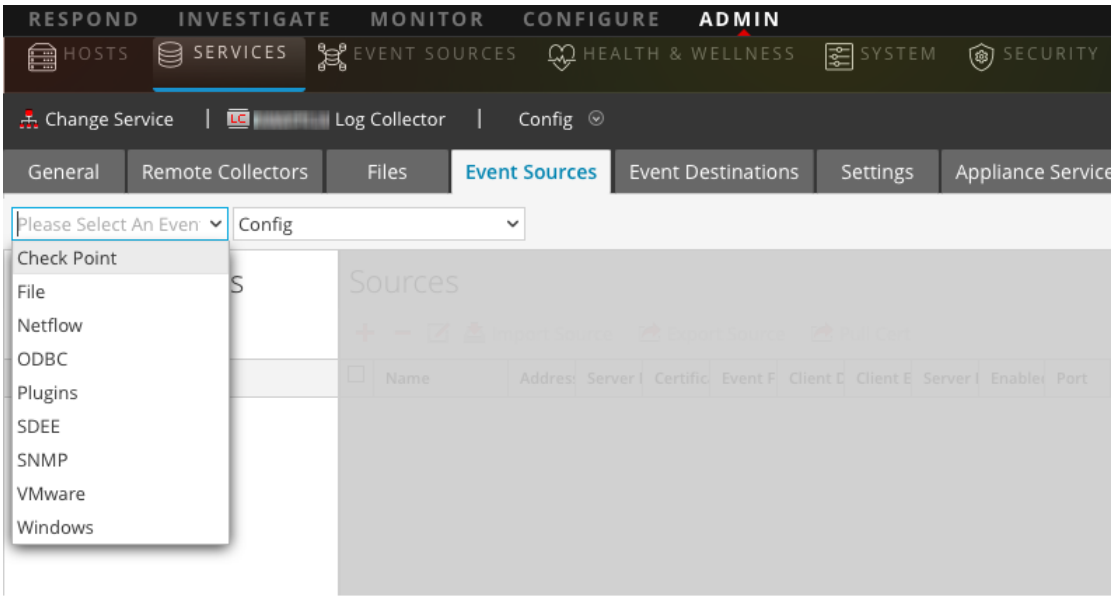
En este tema se describe cómo configurar el protocolo de recopilación de SNMP.

Configurar el origen de eventos de SNMP trap

Para agregar el origen de eventos de SNMP:

Nota: Si anteriormente agregó el tipo **snmptrap**, no puede volver a agregarlo. Puede editarlo o administrar usuarios.

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione > **Ver** > **Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. En la pestaña **Orígenes de evento**, seleccione **SNMP/Configuración** en el menú desplegable.
6. 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**.
7. Seleccione el tipo de origen de eventos **snmptrap** y haga clic **Aceptar**.

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

8. Seleccione **snmptrap** en el panel Categorías de evento.
9. Seleccione **snmptrap** en el panel Orígenes y haga clic en el icono de edición, , para editar los parámetros.
10. Actualice cualquiera de los parámetros que necesita cambiar y haga clic en **Aceptar**.

(Opcional) Configurar usuarios de SNMP

Si usa SNMPv3, siga este procedimiento para actualizar y mantener los usuarios de SNMP v3.

Configurar usuarios de SNMP v3

1. Vaya a **Admin** > **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 **Administrador de usuarios de SNMP/SNMP v3** en el menú desplegable.

   El panel de usuario SNMP v3 se muestra con los usuarios existentes, si los hay.
5. Haga clic en para abrir el cuadro de diálogo **Agregar usuario SNMP**.
6. Rellene el cuadro de diálogo con los parámetros necesarios. A continuación se describen los parámetros disponibles.

Parámetros de usuario de SNMP

En la siguiente tabla se describen los parámetros que debe ingresar al crear un usuario de SNMP v3.

Parámetro	Descripción
Nombre de usuario*	Nombre de usuario (o, más precisamente, en terminología de SNMP, nombre de seguridad). NetWitness Suite usa este parámetro y el parámetro **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.

Parámetro	Descripción
Tipo de autenticación	(Opcional) Protocolo de autenticación. Los valores válidos son los siguientes: • **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 mensajes **NO USE: no seleccione MD5, porque entra en conflicto con Log Collector que se ejecuta en modo FIPS.**
Frase de contraseña de autenticación	Opcional si no tiene el **Tipo de autenticación** definido. Frase de contraseña de autenticación.
Tipo de privacidad	(Opcional) Protocolo de privacidad. Solo puede configurar este parámetro si el parámetro Tipo de autenticación está configurado. Los valores válidos son los siguientes: • **Ninguno** (valor predeterminado) • **AES:** Advanced Encryption Standard (Estándar de cifrado avanzado) • **DES**: estándar de cifrado de datos **NO USE: no seleccione DES, porque entra en conflicto con Log Collector que se ejecuta en modo FIPS.**
Frase de contraseña de privacidad	Opcional si no tiene configurado el **Tipo de privacidad**. Frase de contraseña de privacidad.
Cerrar	Cierra el cuadro de diálogo sin agregar el usuario de SNMP v3 ni guardar las modificaciones en los parámetros.
Guardar	Agrega los parámetros de usuario de SNMP v3 o guarda las modificaciones de los parámetros.

Configurar orígenes de eventos de syslog para Remote Collector

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

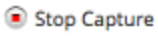
No configure la recopilación de syslog para los Log Collectors locales. Solo debe configurar la recopilación de syslog para los Remote Collectors.

Configurar un origen de eventos de syslog

Nota: Solo debe configurar la recopilación de Syslog la primera vez que configura un origen de eventos que usa Syslog para enviar sus resultados a RSA NetWitness Suite.

Debe configurar el Log Decoder o el Remote Log Collector para Syslog. No es necesario configurar ambos.

Para configurar el Log Decoder para la recopilación de Syslog:

1. Vaya a **Admin > Servicios**.
2. Seleccione un Log Decoder en la cuadrícula Servicios y en el menú Acciones, elija  > **Ver > Sistema**.
3. Realice una de las siguientes acciones de acuerdo con el ícono que ve:
   - Si ve  , haga clic en el ícono para iniciar la captura de Syslog.
   - Si ve  , no es necesario hacer nada; este Log Decoder ya está capturando Syslog.

Para configurar el Remote Log Collector para la recopilación de Syslog:

1. Vaya a **Admin > Servicios**.
2. En la cuadrícula Servicios, seleccione un Remote Log Collector y, en el menú Acciones, elija  > **Ver > Orígenes de evento**.
3. Seleccione **Syslog/Configuración** en el menú desplegable.

   En el panel Categorías de evento se muestran los orígenes de eventos de Syslog que están configurados, si los hay.
4. 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.
5. Seleccione **syslog-tcp** o **syslog-udp**. Puede configurar uno o ambos, según las necesidades de su organización.
6. 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.
7. Ingrese **514** para el puerto y seleccione **Habilitado**. De manera opcional, configure cualquiera de los parámetros avanzados según sea necesario.

   Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo.

Una vez que configura uno o ambos tipos de syslog, el Log Decoder o el Remote Log Collector recopila esos tipos de mensajes de todos los orígenes de eventos disponibles. Por lo tanto, puede continuar agregando orígenes de eventos de Syslog a su sistema sin necesidad de realizar otra configuración de RSA NetWitness Suite.

Parámetros de Syslog

En la siguiente tabla se describen los parámetros disponibles para la configuración de Syslog.

Nombre	Descripción
Básico	
Avanzado	
Aceptar	Agrega los parámetros del origen de eventos.
Cancelar	Cierra el cuadro de diálogo sin agregar el tipo de origen de eventos.
Puerto*	El puerto predeterminado es **514**.
Umbral de registro de publicación en transferencia	Establece un umbral y, cuando se alcanza, NetWitness genera un mensaje de registro para ayudarlo a resolver problemas relacionados con el flujo de eventos. El umbral es el tamaño de los mensajes de eventos de syslog que fluyen actualmente desde el origen de eventos a NetWitness. Los valores válidos son: • **0** (valor predeterminado): deshabilita el mensaje de registro • **100 a 100,000,000**: genera un mensaje de registro cuando los mensajes de eventos de syslog que fluyen actualmente desde el origen de eventos a NetWitness están en el rango de 100 a 100,000,000 bytes.
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
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: • **Desactivado** = (predeterminado) deshabilitado • **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).
Filtro de eventos	Seleccione un filtro. Consulte Configurar filtros de eventos para un Log Collector para obtener instrucciones sobre cómo definir filtros.
Habilitado	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.

Configurar orígenes de eventos de VMware en NetWitness Suite

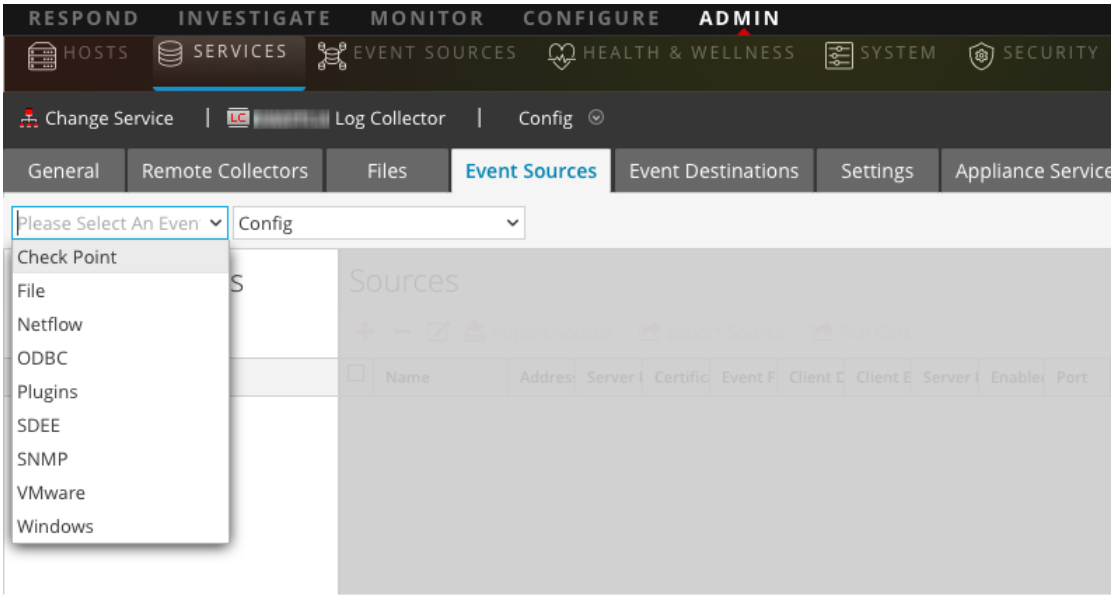
En este tema se indica cómo configurar el protocolo de recopilación de VMware.

Configurar un origen de eventos de VMware

Para agregar un origen de eventos de VMware:

1. Vaya a **ADMIN >Servicios**.
2. Seleccione un servicio de recopilación de registros.

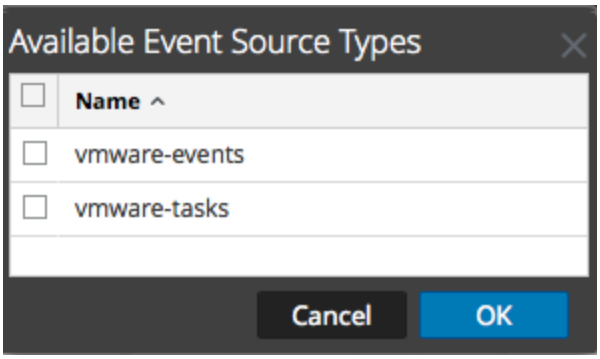
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. En la pestaña **Orígenes de evento** de Log Collector, seleccione **VMware/Configurar** en el menú desplegable.

   En el panel Categorías de evento se muestran los orígenes de eventos de VMware que están configurados, si los hay.

6. Haga clic en  para abrir el cuadro de diálogo **Tipos de origen de evento disponibles**.



7. Seleccione **vmware-events** o **vmware-tasks** en el cuadro de diálogo Tipos de origen de evento disponibles y haga clic en **Aceptar**.

   Los tipos de origen de evento disponibles de VMware son los siguientes:

   - **vmware-events:** configure vmware-events para recopilar eventos desde vCenter Server y ESX/ESXi Server.

- **vmware-tasks:** (Opcional) configure vmware-tasks para recopilar tareas desde vCenter Server.

8. Seleccione el nuevo tipo en el panel Categorías de evento y haga clic en + en la barra de herramientas Orígenes.
9. Agregue un nombre, un nombre de usuario y una contraseña, y modifique cualquier otro parámetro que requiera cambios.

   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**.

10. Haga clic en **Aceptar** para guardar los cambios.

Configurar orígenes de eventos de Windows en NetWitness Suite

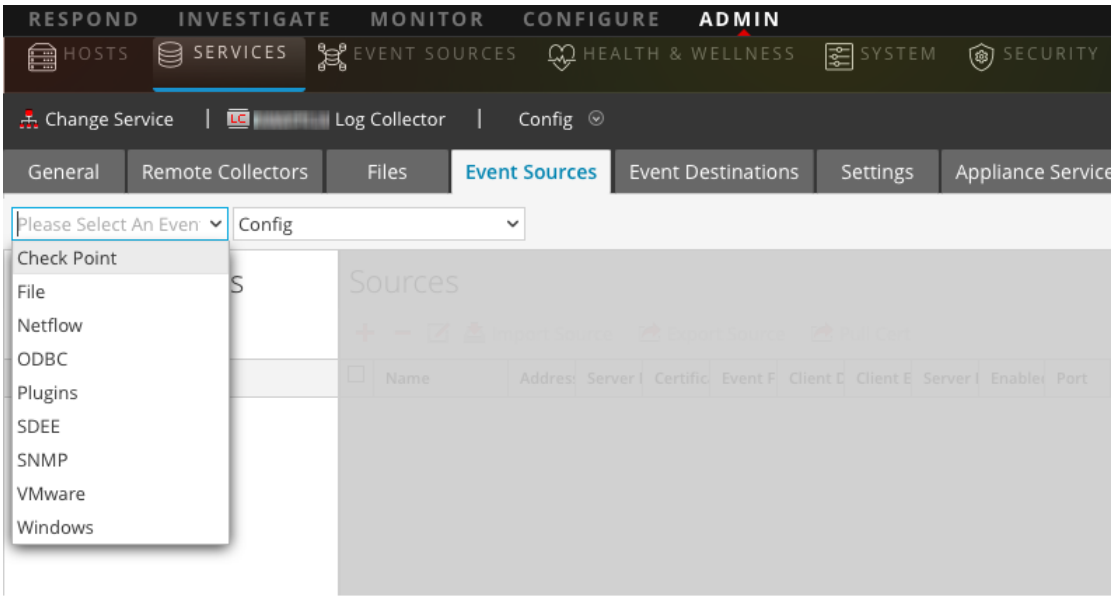
En este tema se describe cómo configurar el protocolo de recopilación de Windows.

Configurar un origen de eventos de Windows

En RSA NetWitness Suite, debe configurar el dominio Kerberos y, a continuación, agregar el tipo de origen de eventos de Windows.

Para configurar el dominio Kerberos para la recopilación de Windows:

1. Vaya a **ADMIN > Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.



5. Seleccione **Dominio Windows/Kerberos** en el menú desplegable.
6. En la barra de herramientas del panel de configuración del dominio Kerberos, haga clic en + para agregar un dominio nuevo.

   Se muestra el cuadro de diálogo Agregar dominio Kerberos.
7. Rellene los parámetros con las siguientes reglas.

Parámetro	Detalles
Nombre de dominio Kerberos	Ingrese el nombre de dominio, todo en mayúsculas. Por ejemplo, DSNETWORKING.COM. Tenga en cuenta que el parámetro Mapeos se rellena automáticamente con variaciones en el nombre de dominio.
Nombre de host KDC	Ingrese el nombre de la controladora de dominio. ***No*** use un nombre completamente calificado aquí: solo el nombre de host para la DC. **Nota:** Asegúrese de que el Log Collector esté configurado como un cliente DNS para el servidor DNS corporativo. De lo contrario, el Log Collector no sabrá cómo encontrar el dominio Kerberos.
Servidor de Admin	(Opcional) El nombre del servidor de administración de Kerberos en formato de nombre de dominio calificado.

8. Haga clic en **Guardar** para agregar el dominio Kerberos.

Para agregar un origen de eventos de Windows:

1. Vaya a **ADMIN > Servicios**.
2. Seleccione un servicio de recopilación de registros.

3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.
5. En la pestaña **Orígenes de evento** de Log Collector, seleccione **Windows/Configurar** en el menú desplegable.

   En el panel Categorías de evento se muestran los orígenes de eventos de VMware que están configurados, si los hay.

A continuación, siga desde la pantalla actual para agregar un tipo y una categoría de evento de Windows.

Para configurar el tipo de evento de Windows:

1. Seleccione **Windows/Configuración** en el menú desplegable.
2. En la barra de herramientas del panel Categorías de evento, haga clic en  para agregar un origen.

   Se muestra el cuadro de diálogo Agregar origen.
3. Rellene los parámetros con las siguientes reglas.

Parámetro	Detalles
Alias	Ingrese un nombre descriptivo.
Método de autorización	Elija **Negociar**.
Canal	En el caso de la mayoría de los orígenes de eventos que usan la recopilación de Windows, desea recopilar los canales de **seguridad**, **sistema** y **aplicación**.
Nombre de usuario	Ingrese el nombre de cuenta para la cuenta de usuario de Windows que configuró anteriormente para la comunicación con NetWitness. Tenga en cuenta que debe ingresar el nombre de cuenta completo, que incluye el dominio. Por ejemplo, **rsalog@DSNETWORKING.COM**.
Contraseña	Ingrese la contraseña correcta para la cuenta de usuario.
Máximo de eventos por ciclo	(Opcional). RSA recomienda configurar este valor en 0, lo cual recopila todo.
Intervalo de sondeo	(Opcional). Para la mayoría de los usuarios, un valor de **60** debe funcionar bien.

4. Haga clic en **Aceptar** para agregar el origen.

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

5. Seleccione el nuevo origen de eventos en el panel Categorías de evento.

   El panel **Hosts** está activado.

6. Haga clic en + en la barra de herramientas del panel Hosts.

7. Rellene los parámetros con las siguientes reglas.

Parámetro	Detalles
Dirección de origen de evento	Ingrese la dirección IP del host de Windows.
Puerto	Acepte el valor predeterminado, **5985**.
Modo de transporte	Ingrese **http**.
Habilitado	Asegúrese de que esté seleccionada la casilla.

8. Haga clic en **Probar conexión**.

   Nota: Podrá probar correctamente la conexión, incluso si no se ejecuta el servicio de Windows.

Para obtener más información sobre cualquiera de los pasos anteriores, consulte los siguientes temas de ayuda en la Guía del usuario de NetWitness Suite:

- Configurar la recopilación de Windows: https://community.rsa.com/docs/DOC-43410
- Guía de configuración de WinRM de Microsoft: https://community.rsa.com/docs/DOC-58163
- Guía de prueba y solución de problemas de WinRM de Microsoft: https://community.rsa.com/docs/DOC-58164

Configuración de la recopilación de Windows existente y NetApp

Este protocolo de **Windows existente** recopila eventos de Windows existente (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.

Cómo funciona la recopilación de Windows existente y NetApp

El protocolo de recopilación de Windows heredado se utiliza para configurar NetWitness Suite 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 Guía de configuración de origen de eventos de ONTAP de datos de dispositivo de red en RSA Link para obtener más información. 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.

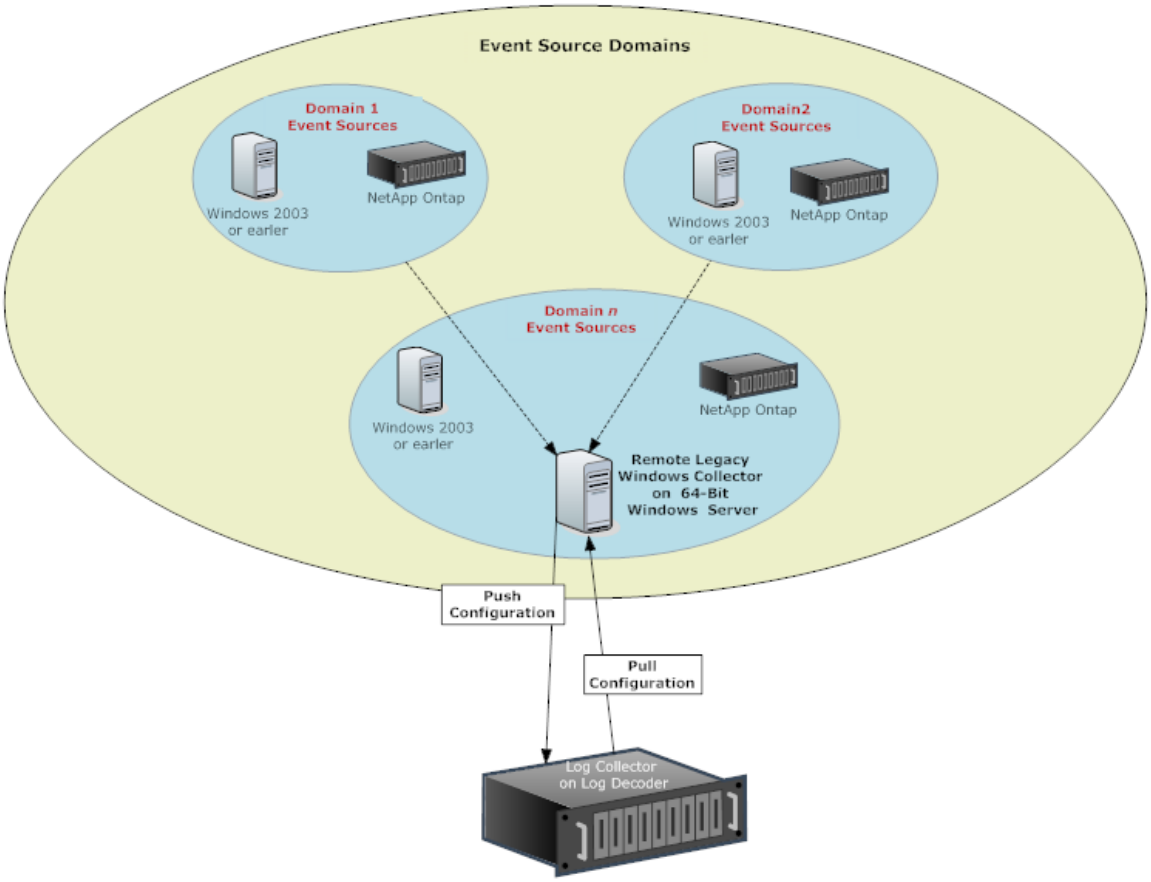
- **Ruta de directorio de eventos**: el dispositivo NetApp genera datos de eventos y los guarda en archivos .evt en un directorio que se puede compartir en el dispositivo NetApp. NetWitness Suite requiere que especifique esta ruta de directorio en el parámetro Ruta de directorio de eventos
- **Prefijo de archivo de evento**: de manera similar a la ruta de directorio de eventos, NetWitness Suite requiere que especifique el prefijo (por ejemplo, adtlog.) de los archivos .evt de datos de eventos de modo que NetWitness Suite pueda procesar estos datos.

En cada ciclo de sondeo, NetWitness Suite 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. NetWitness Suite:

- 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 NetWitness Suite encuentra un archivo procesado parcialmente, omite los eventos ya procesados.

Escenario de implementación

El protocolo de recopilación de Windows heredado recopila datos de eventos de Windows 2003 o versiones anteriores, y orígenes de datos del dispositivo ONTAP de NetApp. El Remote Collector de Windows existente es el recopilador de Windows existente de SA instalado en un servidor Windows 2008 de 64 bits físico o virtual en su dominio de origen de eventos.



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.

El recopilador de Windows existente de NetWitness Suite se instala en un servidor Windows 2008 R2 SP1 de 64 bits físico o virtual mediante el archivo **NWLegacyWindowsCollector-11.*version-number.exe***. Descargue el archivo **NWLegacyWindowsCollector-11.*version-number.exe*** en RSA Link. Consulte *Instrucciones de actualización e instalación de la recopilación de Windows existente de NetWitness 11.x* para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows existente.

Nota: Microsoft Management Console (MMC) debe estar cerrada durante el proceso de instalación.

Configurar orígenes de eventos de Windows existente y de NetApp

En este tema se indica cómo configurar los orígenes de eventos de Windows existente en NetWitness Suite.

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.

Requisitos previos

Antes de configurar un origen de eventos de Windows existente, asegúrese de haber:

1. Instalado el NetWitness Suite de Windows existente de Remote Collector en un servidor Windows 2008 de 64 bits físico o virtual.
2. Agregado este Remote Collector de Windows existente a NetWitness Suite.

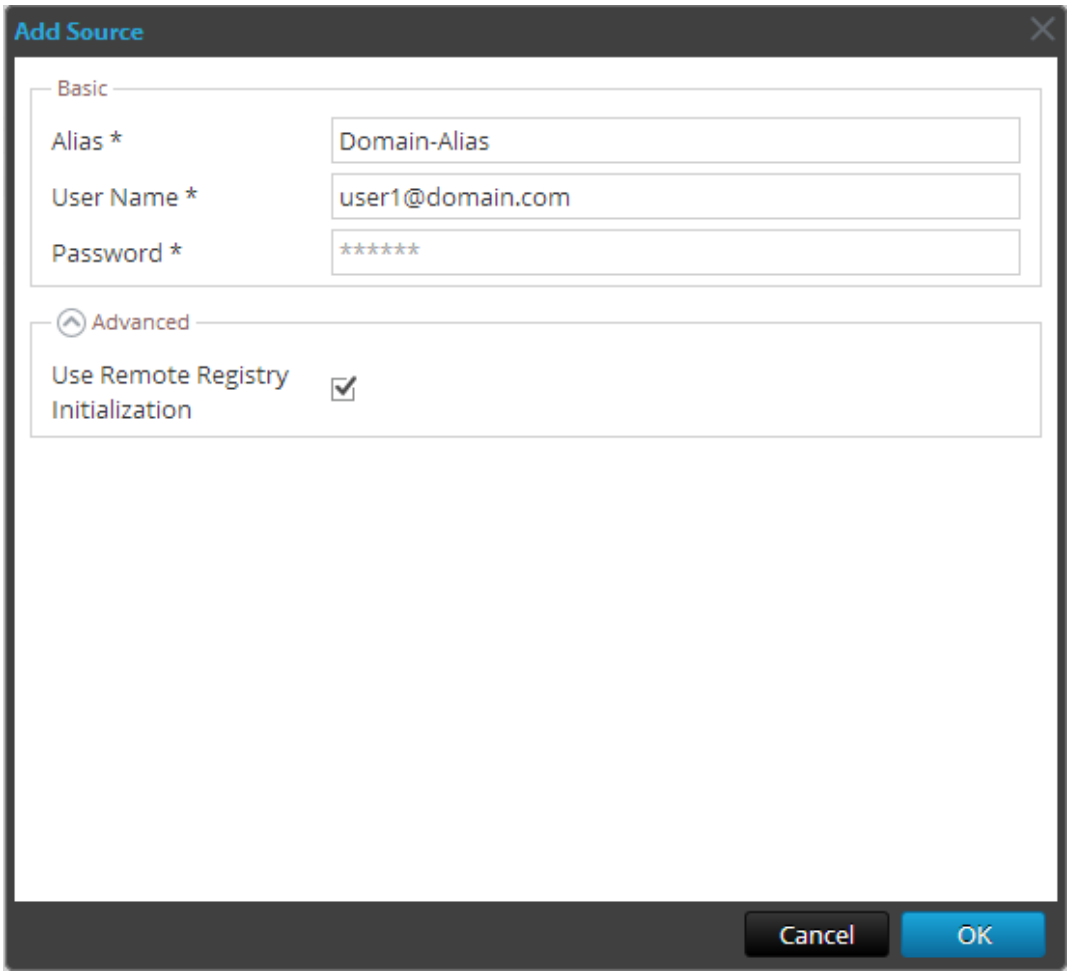
Agregar un origen de eventos de Windows existente

1. Acceda a la vista Servicios, para lo cual debe seleccionar **Admin > Servicios** en el menú de NetWitness Suite.
2. En la cuadrícula **Servicios**, seleccione un servicio **Log Decoder de Windows existente**.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
4. Haga clic en la pestaña **Orígenes de evento**.
5. En la pestaña **Orígenes de evento**, seleccione una de las siguientes opciones en el menú desplegable.
    - Windows existente/Windows.
    - Windows existente/NetApp.
6. 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**.



Nota: De forma predeterminada, se selecciona **Inicialización del registro remoto**. Para obtener más información, consulte Acceso al registro remoto a continuación.

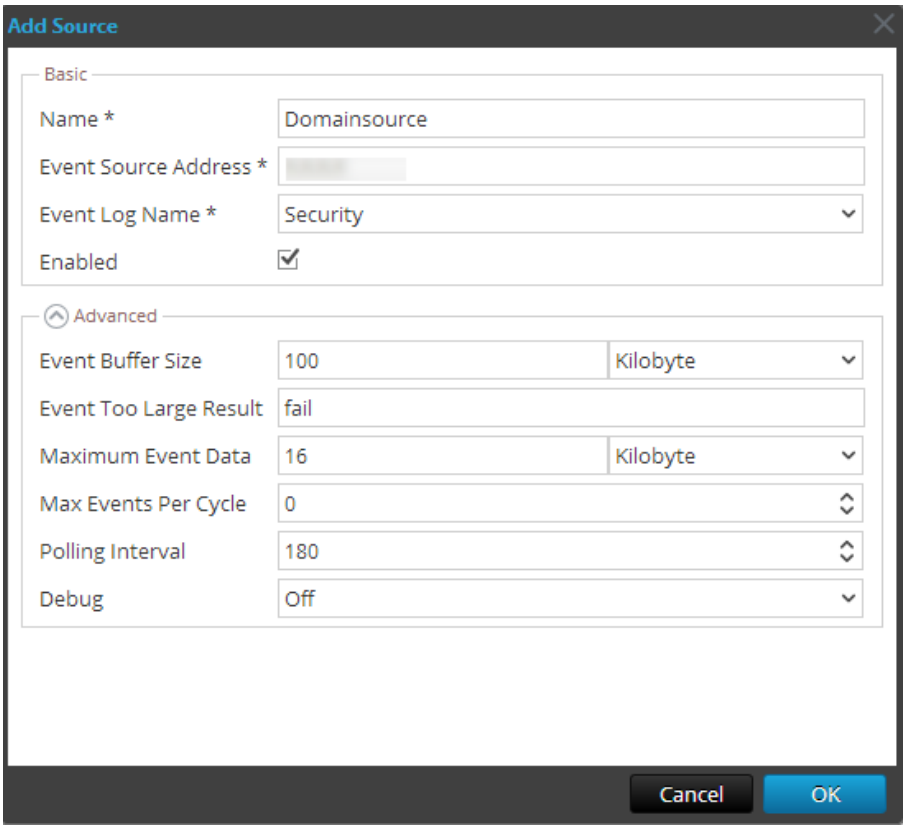
El tipo de origen de eventos de **Windows** agregado recientemente se muestra en el panel Categorías de evento.

7. 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**.

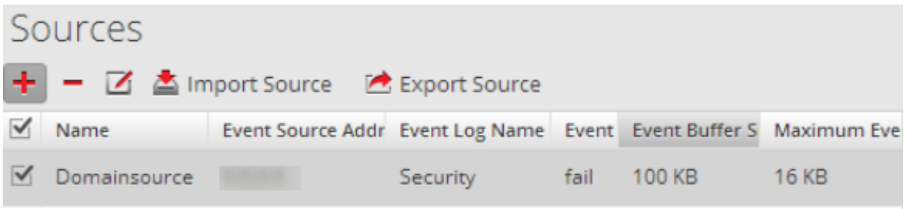
   Se muestra el cuadro de diálogo **Agregar origen**.

b. Especifique valores para los parámetros de orígenes de eventos y haga clic en **Aceptar**.



Para obtener más información, consulte Parámetros de configuración de Windows existente a continuación.

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



Acceso al registro remoto

El recopilador de Windows existente ejecuta una verificación inicial del origen de eventos antes de recopilar datos. De forma predeterminada, el colector de Windows existente usa el método Instrumental de administración de Windows (WMI) para realizar esta verificación inicial. Si habilita el método de acceso remoto al registro, el recopilador de Windows existente ejecuta una consulta remota al registro para verificar el origen de eventos.

Parámetros de configuración de Windows existente

En la siguiente tabla se describen los parámetros de un origen de eventos de Windows existente.

Función	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 incluye un nombre de dominio calificado. NetWitness Suite se configura de forma predeterminada en **127.0.0.1**. Log Collector convierte el nombre de host en letras minúsculas para evitar las 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.
Habilitado	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.

Función	Descripción
Ruta de directorio de eventos	Ruta del directorio de archivos NetApp **.evt o .evtx**. Debe ser la ruta UNC. NetApp genera datos de eventos y los guarda en archivos .evt o .evtx 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. • En cada ciclo de sondeo, Log Collector navega por la ruta compartida de NetApp configurada para los archivos **.evtx** 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.evtx** 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**.

Función	Descripción
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).
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.

Función	Descripción
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 habilitación 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: • **Desactivado** = (predeterminado) deshabilitado • **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.
Aceptar	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 existente (LWC) y las soluciones que se sugieren para ellos.

Nota: 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 existente se reinicia, pero NetWitness Suite no recibe eventos.	El servicio logcollector está detenido.	Reinicie el servicio **logcollector**. 1. Inicie sesión en el **Remote Collector de Windows existente**. 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 NetWitness Suite muestra excepciones debido a una falla de la conexión con el recopilador de Windows existente.	Este problema se soluciona automáticamente después del reinicio del servicio de Windows existente.

Problema	Posibles síntomas	Soluciones

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 NetWitness Suite.	Las páginas de la interfaz del usuario de NetWitness Suite no funcionan.	Reinicie el servicio RabbitMQ.

Problema	Posibles síntomas	Soluciones
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 NetWitness Suite y un host remoto" con el host de LWC como la IP remota.	El script **federate.bat** no se ejecutó correctamente.	Si la ejecución del script **Federate.bat** no fue correcta, ejecútelo de forma manual como se describió anteriormente.

Referencia

Parámetros de AWS

En este tema se proporciona una descripción general de los parámetros de configuración de la recopilación de AWS para implementar un servicio de recopilación remota de registros (VLC) en un ambiente Amazon Web Services (AWS).

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Configurar los parámetros de recopilación de AWS.	Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

Temas relacionados

- Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite

En la siguiente tabla se describen los parámetros de configuración disponibles para la recopilación de AWS.

Parámetro	Descripción
Parámetro	**Descripción**
	Básico
Nombre *	Nombre del origen de eventos.

Parámetro	Descripción
Habilitado 	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.
ID de cuenta *	Código de identificación de la cuenta del depósito S3
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.

Parámetro	Descripción
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.
Clave secreta *	Clave secreta que se usa para acceder al depósito S3.
Región *	Región del depósito S3. **us-east-1** es el valor predeterminado.
Terminal de región	Especifica el nombre de host de AWS CloudTrail. Por ejemplo, para una nube pública de AWS para la región este de EE. UU., el Terminal de región sería s3.amazonaws.com. Encontrará más información en http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. Este parámetro es necesario para recopilar registros CloudTrail de nubes gubernamentales o privadas de AWS.
Usar proxy	Habilite **Usar proxy** para configurar el proxy para el servidor de AWS. De manera predeterminada, está deshabilitada.
Servidor proxy	Ingrese el nombre de proxy que desea conectar para acceder al servidor de AWS.
Puerto proxy	Ingrese el número de puerto que se conecta al servidor proxy para acceder al servidor de AWS.
Usuario de proxy	Ingrese el nombre de usuario para autenticar con el servidor proxy.
Contraseña de proxy	Ingrese la contraseña para autenticarse con el puerto de proxy.
Fecha de inicio *	Inicia la recopilación de AWS (CloudTrail) a partir de la cantidad especificada de días en el pasado, que se miden a contar del registro de fecha y hora actual. El valor predeterminado es 0, que se inicia a partir de hoy. El rango es de 0 a 89 días.

Parámetro	Descripción
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.
	Opciones avanzadas
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. Habilita o deshabilita el registro de depuración del origen de eventos. Los valores válidos son: • **Desactivado** = (predeterminado) deshabilitado • **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.
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 programa 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 subprocesos están ocupados.

Parámetro	Descripción
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: • NetWitness se pueda conectar al depósito S3 en AWS con el uso de las credenciales especificadas en este cuadro de diálogo. • NetWitness pueda 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).
Aceptar	Agrega los valores de los parámetros actuales como un nuevo origen de eventos AWS (CloudTrail).

Parámetros de Azure

Microsoft Azure es una plataforma y una infraestructura de cómputo en la nube que permite crear, implementar y administrar aplicaciones y servicios mediante una red global de centros de datos que administra Microsoft.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Configurar parámetros de orígenes de eventos de Azure.	Configurar orígenes de eventos de Azure en NetWitness Suite

Temas relacionados

- Configurar orígenes de eventos de Azure en NetWitness Suite

Parámetros de configuración del origen de eventos de Azure

En este tema se describen los parámetros de configuración del origen de eventos de Azure.

Nota: Se requieren elementos seguidos de un asterisco (*).

Parámetros básicos

Nombre	Descripción
Nombre *	Ingrese un nombre descriptivo alfanumérico para el origen. Este valor solo se usa para mostrar el nombre en esta pantalla.
Habilitado	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.

Nombre	Descripción
ID de cliente *	El ID de cliente se encuentra en la pestaña Configuración de la aplicación de Azure. Desplácese hacia abajo hasta que lo vea.
Seña secreta del cliente *	Cuando configure el origen de eventos, la seña secreta del cliente aparecerá en el momento en que cree una clave y seleccione una duración de validación. Asegúrese de guardarla, ya que solo podrá verla una vez y no se puede recuperar más adelante.
URL base de recursos de API *	Ingrese `https://management.azure.com/`. Asegúrese de incluir la barra diagonal final (/).
Terminal de metadatos de federación *	En la aplicación de Azure, haga clic en el botón **Ver terminales** (cerca de la parte inferior del panel). Existen muchos vínculos que comienzan con la misma cadena. Compare las direcciones URL y busque la cadena común con la que comienza la mayoría de ellas. Esta cadena común es el terminal que debe ingresar aquí.
ID de suscripción *	Puede encontrarlo en el tablero de Microsoft Azure: haga clic en Suscripciones en la parte inferior de la lista a la izquierda.
Dominio de grupo de usuarios *	Vaya a Active Directory y haga clic en el directorio. En la dirección URL, el dominio de grupo de usuarios es la cadena que viene directamente después de **manage.windowsazure.com/**. El dominio de grupo de usuarios es la cadena que incluye hasta **.com**.
Nombres del grupo de recursos *	En Azure, seleccione los grupos Recurso en el panel de navegación izquierdo y luego elija su grupo.
Fecha de inicio *	Elija la fecha a partir de la cual iniciar la recopilación. La fecha actual es el valor predeterminado.
Probar conexión	Comprueba los parámetros de configuración especificados en este cuadro de diálogo para asegurarse de que estén correctos.

Parámetros avanzados

Haga clic en  junto a **Opciones avanzadas** para ver y editar los parámetros avanzados, si es necesario.

Nombre	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, 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, en segundos, de un ciclo de sondeo. Un valor cero indica que no hay un límite.
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	La duración máxima, en segundos, de un ciclo de sondeo. Un valor cero indica que no hay un límite.
Argumentos de comando	Los argumentos opcionales que se agregarán a la invocación de script.
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. **Precaución:** Habilita o deshabilita el registro de depuración del origen de eventos. Los valores válidos son: • **Desactivado** = (predeterminado) deshabilitado • **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.

Parámetros de punto de control

El protocolo de recopilación de punto de control recopila eventos desde los 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.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Configurar parámetros de punto de control.	Configurar orígenes de eventos de punto de comprobación en NetWitness Suite

Temas relacionados

- Configurar orígenes de eventos de punto de comprobación en NetWitness Suite

Parámetros de configuración de la recopilación de punto de comprobación

Parámetros básicos

Parámetro	Descripción
Nombre*	Nombre del origen de eventos.
Dirección*	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.
Habilitado	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.
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. El valor predeterminado es la dirección de origen de eventos.
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.

Determinar los valores de los parámetros avanzados para la recopilación de punto de control

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). RSA NetWitness Suite 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**

Parámetro	Descripción
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 logs desde	Cuando configura un origen de eventos de punto de control, NetWitness 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). • **Inicio de log**: Recopilar registros desde el comienzo del archivo de registro actual. Si selecciona “Inicio de log” 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. Tenga en cuenta que esta opción es eficaz únicamente para la primera sesión de recopilación.
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.
Duración máxima de encuesta	La duración máxima del ciclo de sondeo (cuánto tiempo dura el ciclo) en segundos.

Parámetro	Descripción
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.
Reenviador	Habilita o deshabilita el servidor del punto de control como un reenviador. De manera predeterminada, está deshabilitada.
Tipo de registro (par de nombre/valor)	Registros desde el origen de eventos en formato nombre/valor. De manera predeterminada, está deshabilitada.
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: • **Desactivado** = (predeterminado) deshabilitado • **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).

Parámetros de archivo

En este tema se describen los parámetros de configuración de la recopilación de archivos.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Configurar parámetros de orígenes de recopilación de archivos.	Configurar orígenes de eventos de archivos en NetWitness Suite

Temas relacionados

- Configurar orígenes de eventos de archivos en NetWitness Suite

Parámetros de orígenes de eventos de recopilación de archivos

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

Nombre	Descripción
Básico	

Nombre	Descripción
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
Habilitado	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.
Opciones avanzadas	

Nombre	Descripción
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 su procesamiento de recopilación normal estimado. **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.
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.

Nombre	Descripción
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 la sección *Generar un par de claves en el origen de eventos e importar la clave pública a Log Collector* en la Guía de instalación y actualización del agente de SFTP para obtener instrucciones sobre la generación de claves. **Nota:** Si la recopilación de archivos se detiene, NetWitness Suite 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 NetWitness Suite 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.
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 NetWitness Suite 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 se reinicia la recopilación o el servicio Log Collector.

Nombre	Descripción
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 se reinicia la recopilación o el servicio Log Collector.
% de reducción de archivos de error	Porcentaje por tamaño o conteo de archivos de error que el servicio Log Collector elimina 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.
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 se reinicia la recopilación o el servicio Log Collector.

Nombre	Descripción
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 se reinicia la recopilación o el servicio Log Collector.
% de reducción de archivos guardados	Porcentaje por tamaño o conteo de archivos guardados que el servicio Log Collector elimina 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 habilitación de la depuración afectará negativamente el rendimiento del Log Collector. Habilita/deshabilita el registro de depuración del origen de eventos. Los valores válidos son: • **Desactivado** = (predeterminado) deshabilitado • **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.
Aceptar	Agrega los parámetros del origen de eventos.

Vista Sistema de servicios de Log Collection

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.

Para acceder a la vista Sistema de servicios de Log Collection, vaya a ADMIN > Servicios, seleccione un servicio Log Collector y, a continuación, seleccione Ver > Sistema.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

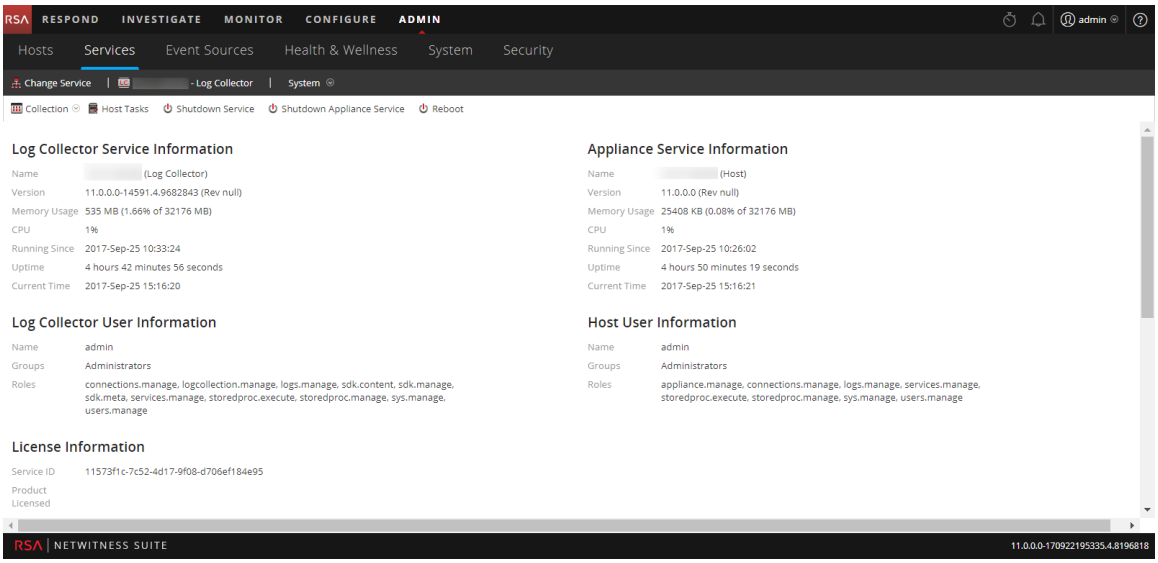
Función	Deseo…	Documentación
Administrador	Iniciar la recopilación de datos de eventos desde un protocolo detenido.	Iniciar servicios de recopilación
Administrador	Detener la recopilación de datos de eventos desde un protocolo iniciado.	Iniciar servicios de recopilación

Temas relacionados

- Iniciar servicios de recopilación

Vista rápida

En la barra de herramientas Información de servicio de Log Collector, puede administrar los datos de eventos mediante el ícono de recopilación para iniciar la recopilación de datos de eventos desde un protocolo detenido o detenerla desde un protocolo iniciado. En el ícono Tareas de host, puede seleccionar las tareas que desea ejecutar. También puede apagar el servicio y reiniciarlo desde la barra de herramientas Información de servicio.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Hosts
Services
Event Sources
Health & Wellness
System
Security
Change Service
- Log Collector
System
Collection
Host Tasks
Shutdown Service
Shutdown Appliance Service
Reboot
Log Collector Service Information
Name (Log Collector)
Version 11.0.0.0-14591.4.9682843 (Rev null)
Memory Usage 535 MB (1.66% of 32176 MB)
CPU 1%
Running Since 2017-Sep-25 10:33:24
Uptime 4 hours 42 minutes 56 seconds
Current Time 2017-Sep-25 15:16:20
Appliance Service Information
Name (Host)
Version 11.0.0.0 (Rev null)
Memory Usage 25408 KB (0.08% of 32176 MB)
CPU 1%
Running Since 2017-Sep-25 10:26:02
Uptime 4 hours 50 minutes 19 seconds
Current Time 2017-Sep-25 15:16:21
Log Collector User Information
Name admin
Groups Administrators
Roles connections.manage, logcollection.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
Host User Information
Name admin
Groups Administrators
Roles appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
License Information
Service ID 11573f1c-7c52-4d17-9f08-d706ef184e95
Product Licensed
RSA | NETWITNESS SUITE
11.0.0.0-170922195335.4.8196818

Parámetros de configuración del origen de eventos de ODBC

En este tema 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).

Acceder a los parámetros de configuración de ODBC

Para acceder a los parámetros de configuración del origen de eventos de ODBC:

1. Vaya a **Administration > Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

   La vista **Configuración del servicio** se muestra con la pestaña **General** de Log Collector abierta.
4. Haga clic en la pestaña **Orígenes de eventos** y seleccione **ODBC/Configuración** en el menú desplegable.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Ver o actualizar los parámetros de ODBC.	Configurar orígenes de eventos de ODBC en NetWitness Suite

Temas relacionados

- Configurar orígenes de eventos de ODBC en NetWitness Suite
- Configurar nombres de orígenes de datos (DSN)

- Solucionar problemas de la recopilación de ODBC
- Crear un archivo typespec personalizado para la recopilación de ODBC

Parámetros de nombre de origen de datos (DSN)

Use el panel Orígenes para revisar, agregar, modificar y eliminar parámetros de Nombre de origen de datos (DSN).

Panel Orígenes

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 *DataDirect Connect Series for ODBC User's Guide* en Progress DataDirect Document Library.

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.

Opción	Descripción
Import DSN	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.
Export DSN	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.
Test Connection	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. Para obtener detalles, consulte 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.

Nombre	Descripción
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.
Habilitado	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).

Nombre	Descripción
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 los siguientes: • **Desactivado** = (predeterminado) deshabilitado • **Activado** = habilitado • **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.
Aceptar	Agrega o modifica los parámetros de DSN.

Parámetros de configuración del origen de eventos de DSN de ODBC

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.

Acceder a los parámetros de configuración de ODBC

Para acceder a los parámetros de configuración del origen de eventos de ODBC:

1. Acceda a la vista Servicios, para lo cual debe seleccionar **Admin > Servicios** en el menú de NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

   La vista **Configuración del servicio** se muestra con la pestaña **General** de Log Collector abierta.
4. Haga clic en la pestaña **Orígenes de eventos** y seleccione **ODBC/DSN** en el menú desplegable.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Configurar los parámetros de configuración de DSN de nombres de orígenes de datos de ODBC.	Configurar nombres de orígenes de datos (DSN)

Temas relacionados

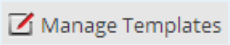
- Configurar orígenes de eventos de ODBC en NetWitness Suite
- Configurar nombres de orígenes de datos (DSN)

Parámetros de configuración de DSN de ODBC

En este tema se describen los parámetros de configuración de DSN de nombres de origen de datos.

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.

Función	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.

Función	Descripción
Plantilla DSN	Seleccione una plantilla predefinida de pares de nombre-valor de valores de DSN para DSN.
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.

Función	Descripción
	Panel Selección de plantillas
	Abre el panel Agregar plantilla, en el cual puede agregar una plantilla de pares de nombre-valor de DSN.

Función	Descripción
	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.

Parámetros de configuración de Remote/Local 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.

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

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Agregar o eliminar Local Collectors	Configurar Local y Remote Collectors
Administrador	Agregar o eliminar Remote Collectors.	Configurar Local y Remote Collectors

Temas relacionados

- Aprovisionar Local y Remote Collectors
- Configurar Local y Remote Collectors

Vista Configuración de servicios

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, NetWitness Suite 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, NetWitness Suite muestra la pestaña **Local Collectors** para que pueda configurar el Remote Collector de modo que migre eventos a un Local Collector.

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.

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.
Recopilaciones	Elija los protocolos de recopilación que el Remote Collector migra a un Local Collector. Puede seleccionar cualquier combinación de protocolos. Si no selecciona un protocolo, NetWitness Suite 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.
	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.

Columna	Descripción
	Seleccione 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.
Recopilaciones	Elija los protocolos de recopilación que el Local Collector extrae de un Remote Collector. Puede seleccionar cualquier combinación de protocolos. Si no selecciona un protocolo, NetWitness Suite los selecciona todos.

Pestañas de Log Collection

En este tema se describe las pestañas disponibles en la vista Log Collection.

Acceder a la vista Log Collection

1. Vaya a **ADMIN > Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione **Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.

   La vista **Configuración del servicio** se muestra con la pestaña **General** de Log Collector abierta.
4. Seleccione cualquiera de las pestañas disponibles para ver o actualizar los parámetros correspondientes.

Pestañas disponibles

Use la vista Admin > Servicios para mantener los parámetros de Log Collection. Tiene las siguientes pestañas:

- **General**: contiene parámetros generales que rigen la operación del servicio Log Collector y cada protocolo de recopilación. Consulte Pestaña General de la recopilación de registros para obtener más información.

- **Remote Collectors**: use esta pestaña para configurar Remote Collectors. Consulte Configurar Local y Remote Collectors para obtener más información.
- **Archivos**: proporciona una interfaz para editar archivos de configuración de Log Collector.
- **Orígenes de eventos**: use esta pestaña para configurar la recopilación de los orígenes de eventos. Consulte Pestaña Orígenes de eventos de Log Collection para obtener más información.
- **Destinos de evento**: Use la pestaña Destinos de evento de la vista Configuración del servicio Log Collection para configurar el destino de los datos de eventos que recopila el Log Collector. Consulte Pestaña Destinos de evento de la recopilación de registros para obtener más información.
- **Ajustes de configuración**: contiene parámetros para la configuración de seguridad de Lockbox y administración de certificados.
- **Configuración del servicio Appliance**: contiene parámetros de configuración para el servicio RSA NetWitness Suite Core Appliance.

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.

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

1. Vaya a **ADMIN> Servicios** en el menú NetWitness Suite.
2. Seleccione un servicio de recopilación de registros.
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.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Ajuste los parámetros de configuración del sistema, si es necesario, en el panel Configuración del sistema.	Implementación básica

Función	Deseo…	Documentación

Administrador	• 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 y Azure Audit)
	  • SDEE
	  • SNMP
	  • VMware
	  • Windows
	  • Windows existente
		• Configurar orígenes de eventos de punto de comprobación en NetWitness Suite
		• Configurar orígenes de eventos de archivos en NetWitness Suite
		• Configurar orígenes de eventos de ODBC en NetWitness Suite
		• Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite
		• Configurar orígenes de eventos de SDEE en NetWitness Suite
		• Configurar orígenes de eventos de Netflow en NetWitness Suite
		• Configurar orígenes de eventos de ODBC en NetWitness Suite
		• Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite
		• Configurar orígenes de eventos de SNMP en NetWitness Suite
		• Configurar orígenes de eventos de VMware en NetWitness Suite
		• Configurar orígenes de eventos de Windows en

Función	Deseo…	Documentación
		NetWitness Suite • Configuración de la recopilación de Windows existente y NetApp

Temas relacionados

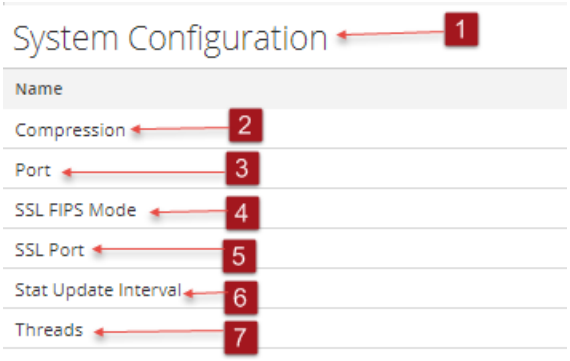
- Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite
- Configurar orígenes de eventos de punto de comprobación en NetWitness Suite
- Configurar orígenes de eventos de archivos en NetWitness Suite
- Configurar orígenes de eventos de Netflow en NetWitness Suite
- Configurar orígenes de eventos de ODBC en NetWitness Suite
- Configurar orígenes de eventos de SDEE en NetWitness Suite
- Configurar orígenes de eventos de SNMP en NetWitness Suite
- Configurar orígenes de eventos de syslog para Remote Collector
- Configurar orígenes de eventos de VMware en NetWitness Suite
- Configurar orígenes de eventos de Windows en NetWitness Suite
- Configuración de la recopilación de Windows existente y NetApp

Vista rápida

El administrador de RSA NetWitness Suite debe configurar orígenes de eventos para enviar registros a los recopiladores. Cuando están configurados, los orígenes de eventos sondean orígenes de eventos, recuperan registros y envían los datos de eventos a NetWitness Suite.

Panel Configuración del sistema

El panel Configuración del sistema administra la configuración de un servicio de NetWitness Suite. 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.

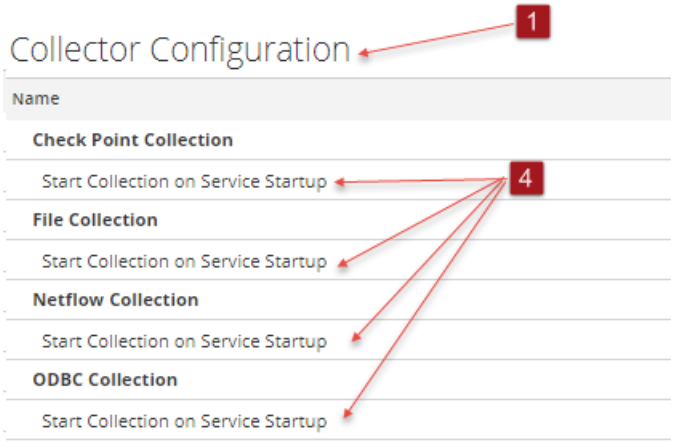


1	El panel Configuración del sistema administra la configuración de un servicio de NetWitness Suite.
2	Compresión: La cantidad mínima de bytes que se deben transmitir por respuesta antes de la compresión. Si se define en 0, se deshabilita la compresión. El valor predeterminado es **0**. Un cambio en el valor se aplica de inmediato en todas las conexiones subsiguientes.
3	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
4	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**.
5	Puerto SSL: El puerto SSL de NetWitness Suite 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
6	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.
7	Subprocesos: 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 habilitar el inicio automático de la recopilación de registros por tipo de origen de eventos.



1	El panel Configuración de recopilador proporciona una manera de habilitar el inicio automático de la recopilación de registros por tipo de origen de eventos.
2	Activar todo habilita 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 eventos cuando se inicia el servicio Log Collector.
3	Deshabilitar todo deshabilita la recopilación automática de todos los tipos de eventos. **Deshabilitar todo** = (valor predeterminado) no recibe datos de eventos para ningún tipo de evento hasta que usted inicia explícitamente la recopilación.
4	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 los siguientes:

- 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.

5 **Aplicar**: Haga clic en **Aplicar** para guardar los cambios realizados en los valores de los parámetros.

Pestaña Destinos de evento de la recopilación de registros

Use la pestaña Destinos de evento de la vista Configuración del servicio Log Collection 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.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

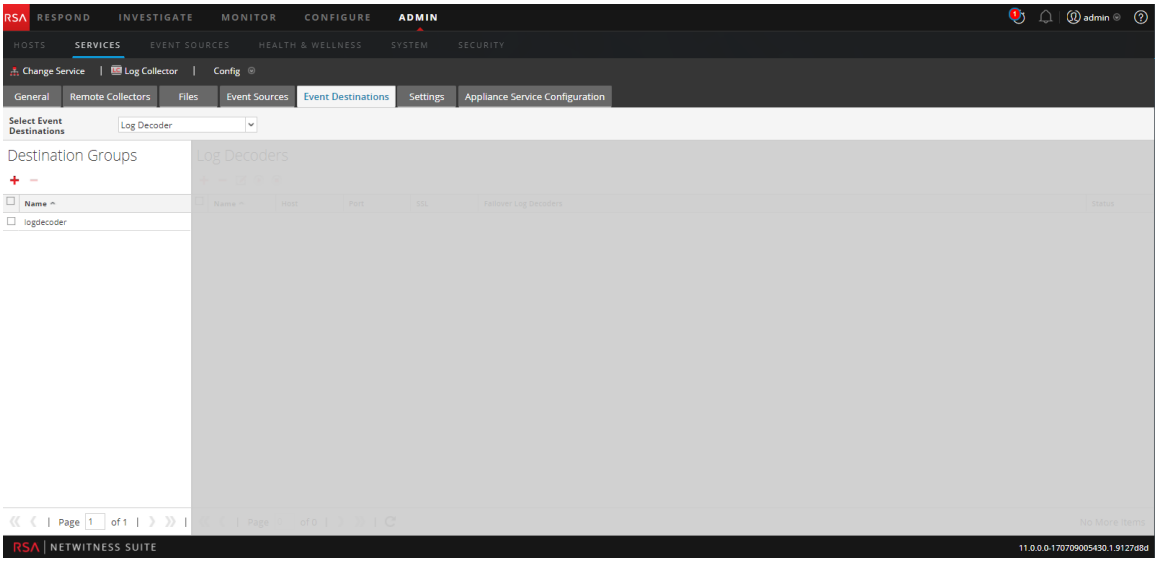
Función	Deseo…	Documentación
Administrador	Configurar el destino de los datos de eventos que recopila el Log Collector	Consulte las instrucciones que aparece a continuación.

Temas relacionados

- Consulte el tema **Crear un feed de identidad** en la *Guía de administración de recursos de Live*.

Vista rápida

La pestaña Destinos de evento de la vista Configuración del servicio Log Collection permite configurar el destino de los datos de eventos que recopila el Log Collector.

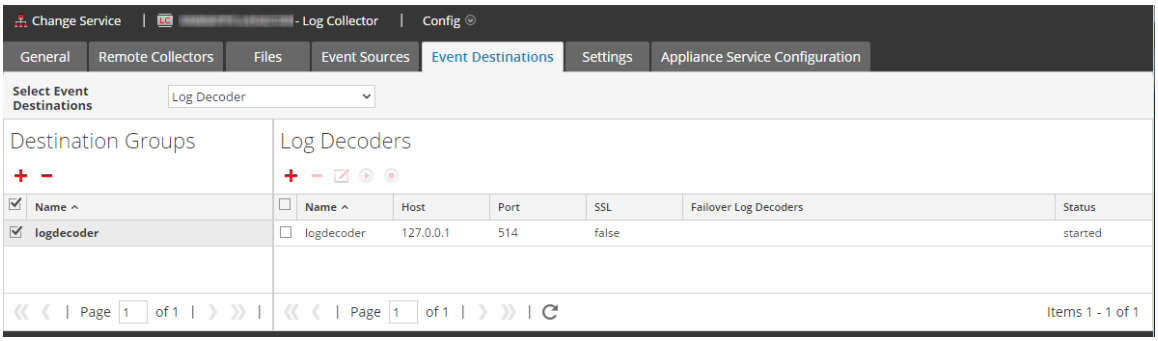


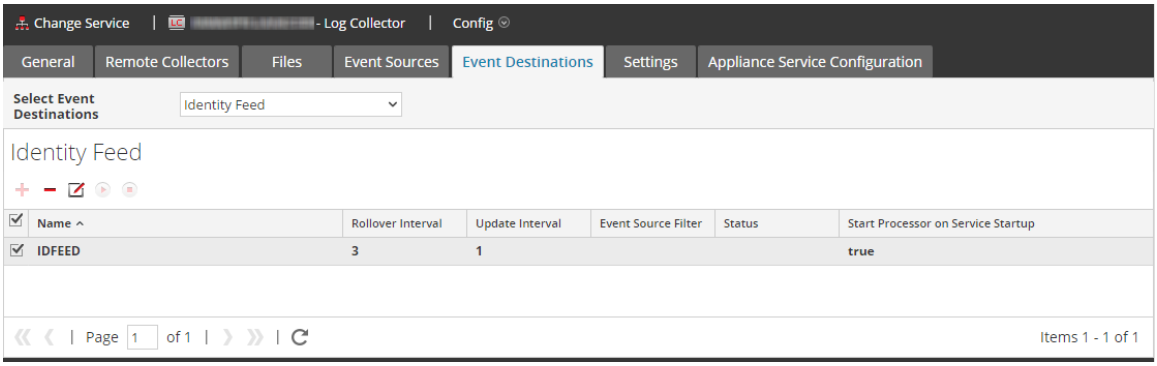
El permiso requerido para acceder a esta vista es Administrar servicios.

1. Vaya a **ADMIN> Servicios**.
2. Seleccione un servicio de recopilación de registros.
3. En Acciones, seleccione  **> Ver > Configuración** para mostrar las pestañas de parámetros de configuración de Log Collection.
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 CollectorLog Collector.


Change Service
- Log Collector
Config
General
Remote Collectors
Files
Event Sources
Event Destinations
Settings
Appliance Service Configuration
Select Event Destinations
Log Decoder
Destination Groups
Name
logdecoder
Log Decoders
Name
Host
Port
SSL
Failover Log Decoders
Status
logdecoder
127.0.0.1
514
false
started
Page 1 of 1
Items 1 - 1 of 1


Change Service
- Log Collector
Config
General
Remote Collectors
Files
Event Sources
Event Destinations
Settings
Appliance Service Configuration
Select Event Destinations
Identity Feed
Identity Feed
Name
Rollover Interval
Update Interval
Event Source Filter
Status
Start Processor on Service Startup
IDFEED
3
1
true
Page 1 of 1
Items 1 - 1 of 1

Pestaña Orígenes de eventos de Log Collection

Use la pestaña Orígenes de eventos para configurar los orígenes de eventos de AWS (CloudTrail), Punto de control, Archivo, ODBC, SDEE, SNMP, Syslog, VMware, Windows y Windows existente.

Para acceder a la pestaña Orígenes de eventos, vaya a ADMIN > Servicios > seleccione el servicio Log Collection > Ver > Configuración > Orígenes de eventos.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

Función	Deseo…	Documentación
Administrador	Configurar orígenes de eventos de AWS (CloudTrail).	Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite
Administrador	Configurar orígenes de eventos de punto de control.	Configurar orígenes de eventos de punto de comprobación en NetWitness Suite
Administrador	Configurar orígenes de eventos de archivos.	Configurar orígenes de eventos de archivos en NetWitness Suite
Administrador	Configurar orígenes de eventos de ODBC.	Configurar orígenes de eventos de ODBC en NetWitness Suite
Administrador	Configurar orígenes de eventos de SDEE.	Configurar orígenes de eventos de SDEE en NetWitness Suite
Administrador	Configurar orígenes de eventos de SNMP.	Configurar orígenes de eventos de SNMP en NetWitness Suite

Función	Deseo…	Documentación
Administrador	Configurar orígenes de eventos de syslog.	Configurar orígenes de eventos de syslog para Remote Collector
Administrador	Configurar orígenes de eventos de VMware.	Configurar orígenes de eventos de VMware en NetWitness Suite
Administrador	Configurar orígenes de eventos de Windows.	Configurar orígenes de eventos de Windows en NetWitness Suite
Administrador	Configurar orígenes de eventos de Windows existente.	Configuración de la recopilación de Windows existente y NetApp

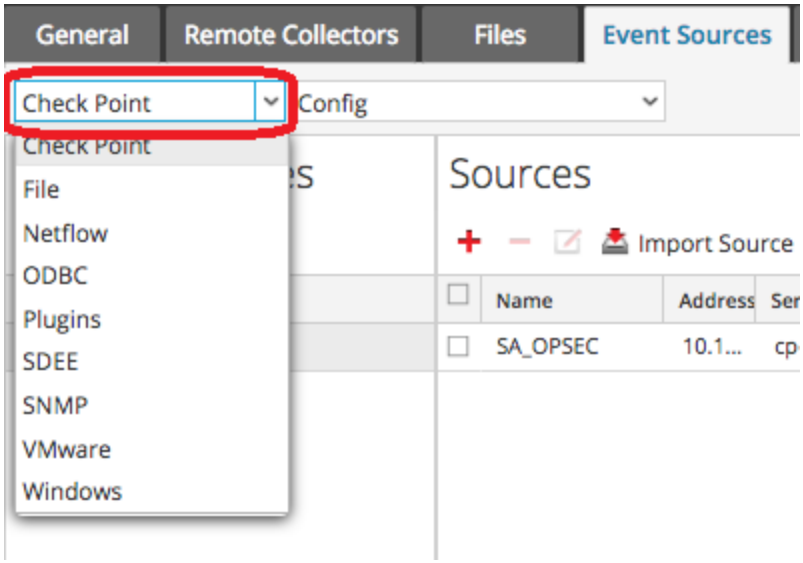
Temas relacionados

- Configurar orígenes de eventos de AWS (CloudTrail) en NetWitness Suite
- Configurar orígenes de eventos de punto de comprobación en NetWitness Suite
- Configurar orígenes de eventos de archivos en NetWitness Suite
- Configurar orígenes de eventos de ODBC en NetWitness Suite
- Configurar orígenes de eventos de SDEE en NetWitness Suite
- Configurar orígenes de eventos de SNMP en NetWitness Suite
- Configurar orígenes de eventos de syslog para Remote Collector
- Configurar orígenes de eventos de VMware en NetWitness Suite
- Configurar orígenes de eventos de Windows en NetWitness Suite
- Configuración de la recopilación de Windows existente y NetApp

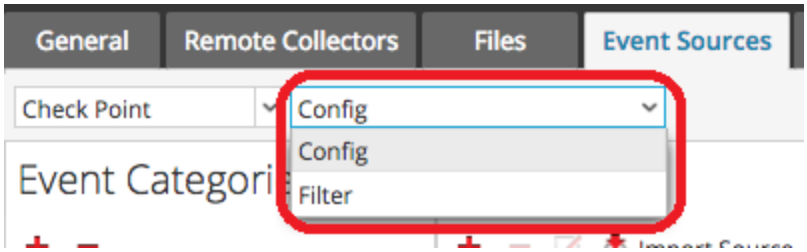
Vista rápida

La vista Configuración tiene dos menús desplegables:

- El menú de la izquierda enumera todos los protocolos de recopilación disponibles.



- El menú de la derecha tiene dos opciones: **Configuración** y **Filtro**.



La vista Configuración de la pestaña Orígenes de eventos tiene dos paneles: Categorías de evento y Orígenes.

Nota: Para obtener detalles acerca del elemento de menú Filtro, consulte Configurar filtros de eventos para un Log Collector.

Menú Tipos de origen de eventos

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.

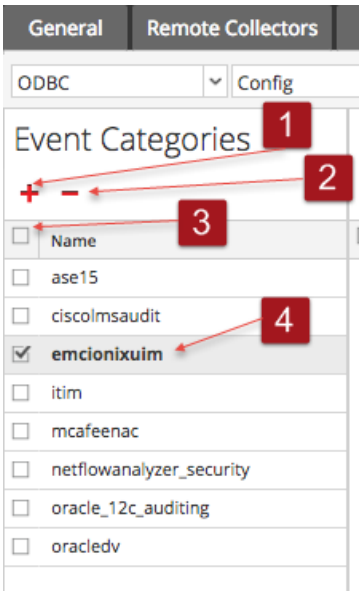
En la casilla derecha, seleccione:

- 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

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.

Panel Categorías de evento

Una vez que selecciona un protocolo de recopilación, el panel Categorías de evento se completa con todos los orígenes de eventos que configuró para ese protocolo. Por ejemplo, en la siguiente imagen se muestran los orígenes de eventos de ODBC que se configuraron:



El panel Categorías de evento proporciona una manera de agregar o eliminar tipos de orígenes de eventos.

1 Muestra el cuadro de diálogo Tipos de origen de evento disponibles, en el cual se

selecciona el tipo de origen de eventos para el cual desea definir parámetros.

2 Elimina los tipos de orígenes de eventos seleccionados en el panel Categorías de evento.

3 Selecciona los tipos de orígenes de eventos.

4 Muestra el nombre de los tipos de orígenes de eventos que ha agregado.

Panel Orígenes

En el panel Orígenes se enumeran los valores de los parámetros para el tipo de origen de eventos seleccionado. Para obtener detalles, consulte los temas de cada protocolo de recopilación.

Pestaña Ajustes de configuración de Log Collection

Use la pestaña Ajustes de configuración para:

- Configurar un lockbox
- Restablecer valor de sistema estable
- Administrar certificados

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.

Para acceder a la pestaña Ajustes de configuración de Log Collection, vaya a ADMIN > Servicios. En la cuadrícula Servicios, seleccione un servicio Log Collector. Haga clic en el menú Acciones recortado bajo Acciones y seleccione Ver > Configuración.

Flujo de trabajo

En este flujo de trabajo se ilustran las tareas básicas necesarias para comenzar a recopilar eventos mediante Log Collection.

¿Qué desea hacer?

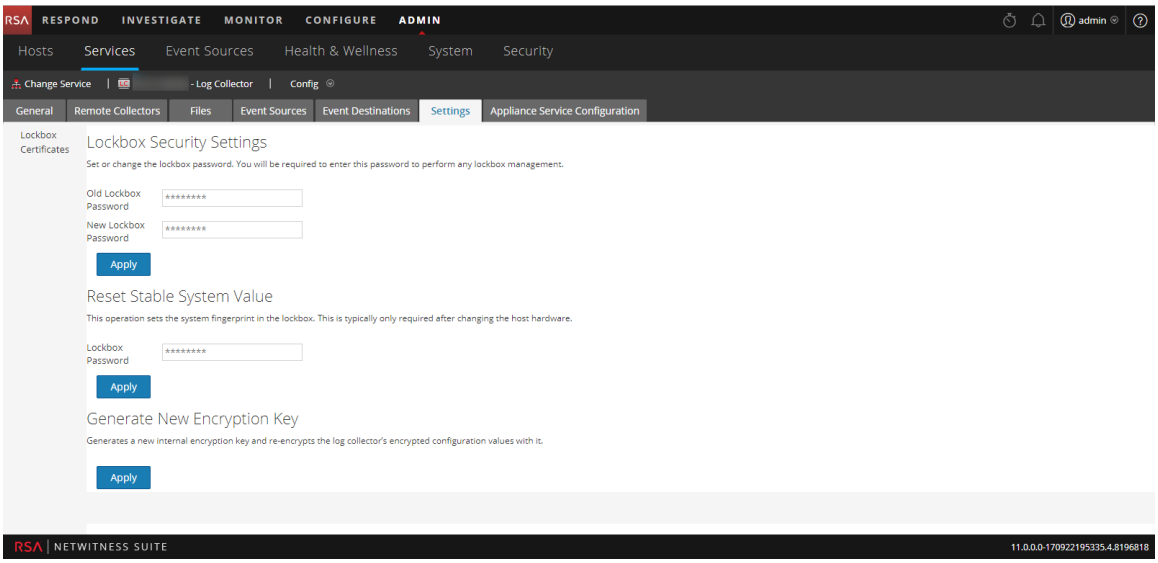
Función	Deseo…	Documentación
Administrador	Configurar un Lockbox para mantener la configuración de Lockbox.	Configurar un Lockbox
Administrador	Agregar o eliminar certificados.	Configurar certificados

Temas relacionados

- Consulte el tema “Crear un feed de identidad” en la *Guía de administración de recursos de Live*.

Vista rápida

Este es un ejemplo de la pestaña Ajustes de configuración.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Hosts
Services
Event Sources
Health & Wellness
System
Security
Change Service
- Log Collector
Config
General
Remote Collectors
Files
Event Sources
Event Destinations
Settings
Appliance Service Configuration
Lockbox Certificates
Lockbox Security Settings
Set or change the lockbox password. You will be required to enter this password to perform any lockbox management.
Old Lockbox Password
New Lockbox Password
Apply
Reset Stable System Value
This operation sets the system fingerprint in the lockbox. This is typically only required after changing the host hardware.
Lockbox Password
Apply
Generate New Encryption Key
Generates a new internal encryption key and re-encrypts the log collector's encrypted configuration values with it.
Apply
RSA | NETWITNESS SUITE
11.0.0.0-170922195335.4.8196818

Solucionar problemas de la recopilación de registros

En este tema se describe el formato y el contenido de la solución de problemas de recopilación de registros. NetWitness Suite informa sobre los problemas de Log Collector o sobre posibles problemas en las dos formas 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 habilitar (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 **Admin > Estado y condición**.

Ejemplo de formato de solución de problemas

RSA NetWitness Suite 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" systemctl="systemctl" 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$ systemctl status rabbitmq-server`
	`rabbitmq start/running, process 10916`
	2. Inicie el RabbitMQ Message Broker en el nodo event-broker en la vista Explorar: