RSA NETWITNESS® SUITE

Guía de introducción de hosts y servicios

para la versión 11.1

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 Dell, 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 Dell.

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

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

julio 2018

Contenido

Aspectos básicos de hosts y servicios

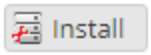
En esta guía se proporciona a los administradores los procedimientos estándares para agregar y configurar hosts y servicios en NetWitness Suite. Después de presentar el propósito básico de los hosts y los servicios y cómo funcionan dentro de la red de NetWitness Suite, en esta guía se aborda lo siguiente:

- Las tareas que debe realizar para configurar los hosts y los servicios en la red
- Los procedimientos adicionales que completa en función de las necesidades operacionales a largo plazo y diarias de una empresa.
- Temas de referencia que describen la interfaz del usuario

Qué es un host

Un host es la máquina en la cual se ejecuta un servicio y puede ser una máquina física o virtual. Consulte el "Diagrama detallado de implementación de hosts de RSA NetWitness Suite" de la *Guía de implementación de RSA NetWitness Suite* para ver una ilustración de cómo se implementan los hosts. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Qué es un tipo de host

Un tipo de host asigna un servicio o servicios a un host cuando se instala un host desde la vista Hosts. Elija un **Tipo de host** en el cuadro de diálogo **Instalar servicios**, el cual se muestra cuando se selecciona un host en la vista Hosts, y haga clic en 

(icono de instalación). En la siguiente tabla se enumeran cada host de tipo y el servicio o los servicios que instala. Consulte el "Diagrama detallado de implementación de hosts de RSA NetWitness Suite" de la *Guía de implementación de RSA NetWitness Suite* para ver una ilustración de cómo se implementan los hosts. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Tipo de host	Servicios instalados
Archiver	Workbench y Archiver
Broker	Broker
Cloud Gateway	Cloud Gateway
Concentrator	Concentrator

Tipo de host	Servicios instalados
Endpoint Hybrid	Log Decoder, Endpoint y Concentrator
Endpoint Log Hybrid	Log Collector, Log Decoder, Endpoint y Concentrator
ESA primario	Context Hub, Entity Behavior Analysis y Event Stream Analysis
ESA secundario	Entity Behavior Analysis y Event Stream Analysis
Log Collector	Log Collector
Log Decoder	Log Collector y Log Decoder
Log Hybrid	Log Collector, Log Decoder y Concentrator
Malware Analysis	Malware Analysis y Broker
Packet Decoder	Decoder
Packet Hybrid	Concentrator y Decoder
Warehouse Connector	Warehouse Connector

Qué es un servicio

Un servicio realiza una función única, como recopilar registros o archivar datos. Cada servicio se ejecuta en un puerto exclusivo y se modela como un plug-in para habilitarse o inhabilitarse de acuerdo con la función del host.

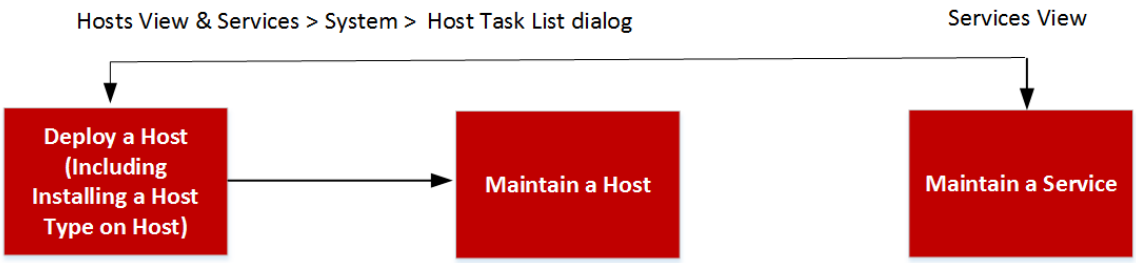
En primer lugar, debe configurar los siguientes servicios Core:

- Decoder
- Concentrator
- Broker
- Log Decoder

A continuación se enumeran todos los servicios y cada uno, con excepción de Log Collector, tiene su propia guía o comparte una en *Guías de configuración de hosts y servicios*. El Log Collector tiene su propio conjunto de guías de configuración para manejar la configuración de todos los protocolos de recopilación de eventos compatibles. Para obtener información sobre Log Collector, consulte *Guías de recopilación de registros*.

- Archiver
- Broker
- Cloud Gateway
- Concentrator
- Context Hub
- Decoder (Packets)
- Endpoint
- Entity Behavior Analysis
- Event Stream Analysis
- Investigate
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Respond
- Warehouse Connector
- Workbench

Debe configurar hosts y servicios para la comunicación entre estos y con la red de modo que puedan ejecutar sus funciones, como el almacenamiento o la captura de datos.



Configuración de un host

La vista Host se usa para agregar un host a NetWitness Suite. Consulte Paso 1. Implementar un host para obtener instrucciones detalladas.

Mantenimiento de hosts

La vista Host principal se usa para agregar, editar, eliminar y realizar otras tareas de mantenimiento para los hosts en la implementación. Use el cuadro de diálogo Lista de tareas para realizar tareas relacionadas con un host y sus comunicaciones con la red. Consulte Procedimientos de hosts y servicios para obtener instrucciones detalladas.

Después de la implementación inicial de NetWitness Suite, la tarea principal que realiza en la vista Host es la actualización de la implementación de NetWitness Suite a una nueva versión.

Convención de asignación de nombres de las versiones de actualización

Puede usar la vista Hosts para aplicar las actualizaciones de versiones más recientes desde el repositorio de actualización local (consulte el tema **Administrar las actualizaciones de NetWitness Suite** en *Mantenimiento del sistema* para obtener más información sobre el repositorio de actualización local). Debe comprender la convención de asignación de nombres de versiones de actualización para saber qué versión debe aplicar al host. La convención de asignación de nombres es ***major-release.minor-release.service-pack.patch***. Por ejemplo, si elige 11.6.1.2, aplicaría la siguiente versión al host.

- 11 = versión principal
- 6 = versión secundaria
- 1 = service pack
- 2 = parche

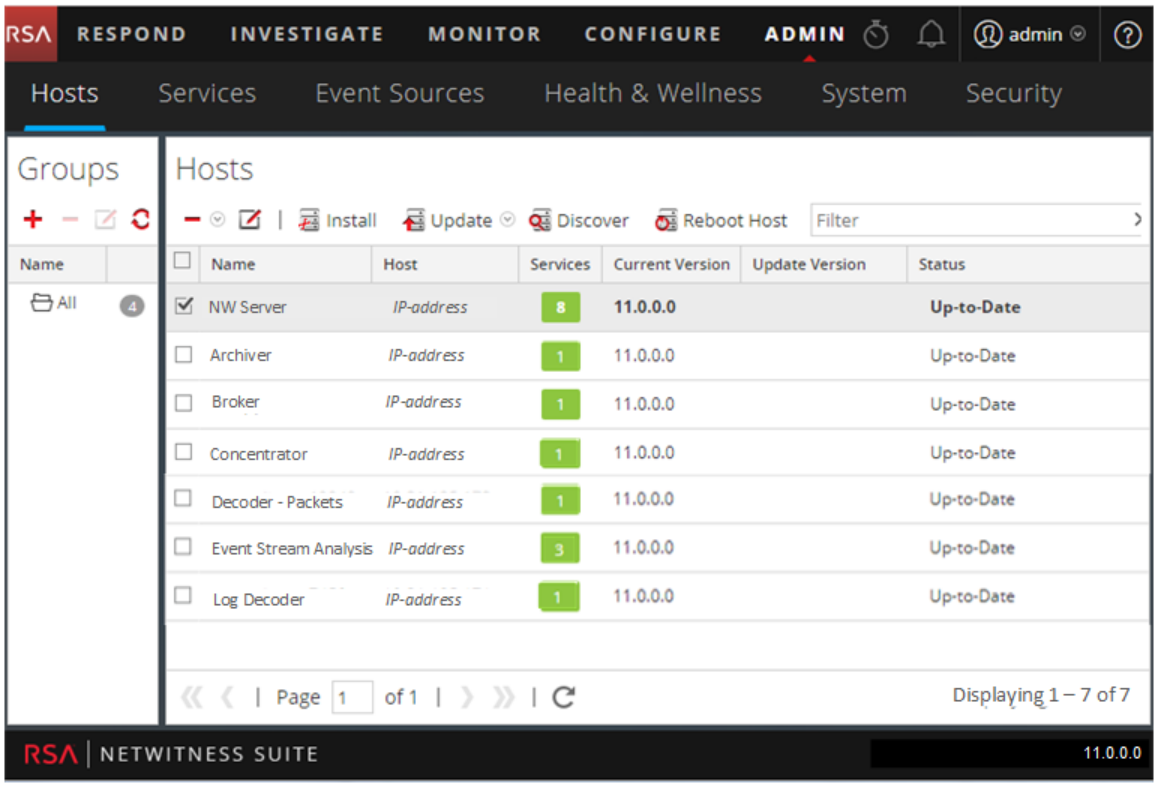
NetWitness Suite es compatible con múltiples versiones en su implementación. En primer lugar se actualiza Servidor de NetWitness (host del servidor de NW) y los demás hosts deben tener la misma versión que el host de Servidor de NW o una anterior.

Nota: En primer lugar se actualiza el host de Servidor de NW y los demás hosts tienen la misma versión que el host de Servidor de NW o una anterior.

El siguiente es un ejemplo de una implementación de múltiples versiones:

- Las actualizaciones de versiones disponibles actualmente en el repositorio de actualización local son 11.0.2.0 y 11.0.1.0 para los hosts de Broker, LC/LD y Log Decoder.
- El host de Servidor de NW y los demás hosts están actualizados a 11.0.2.0.

Esto significa que tiene la opción de actualizar los hosts de Broker, LC/LD y Log Decoder a 11.0.2.0 u 11.0.2.0.



Mantenimiento de los servicios

La vista Servicios se usa para agregar, editar, eliminar, monitorear y realizar otras tareas de mantenimiento para los servicios en su implementación. Consulte Procedimientos de hosts y servicios para obtener instrucciones detalladas.

Servicios que se implementan con el Servidor de NetWitness

Los servicios que aparecen en la siguiente tabla se implementan cuando implementa el Servidor de NW para admitir:

- la expansión de las plataformas de implementación física y virtual, y las mejoras en el mantenimiento de hosts y servicios.
- las mejoras a la funcionalidad Investigate y Respond.

Precaución: No es necesario configurar estos servicios para implementar NetWitness Suite. RSA recomienda monitorear el estado operativo de estos servicios mediante Estado y condición. No intente modificar los parámetros en la vista Explorar sin ponerse en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

Servicio	Propósito
Admin	El servidor de Administration (**servidor de Admin**) es el servicio de back-end para las tareas administrativas en la interfaz del usuario de NetWitness Suite. Resume la autenticación, la administración de preferencias globales y el soporte de autorización para la interfaz del usuario. El **servidor de Admin** requiere que el **servidor de Config** y el **servidor de Security** estén en línea para realizar su función.
Configuración	El servidor de Configuration (**servidor de Config**) almacena y administra los conjuntos de configuración. Un conjunto de configuración es cualquier grupo de configuración lógica que se administra de manera independiente. El **servidor de Config** facilita el uso compartido de las propiedades entre los servicios, proporciona funcionalidades de respaldo y restauración de configuración y rastrea los cambios en las propiedades.
Integración	El servidor de Integration administra las interacciones con los sistemas externos. El servicio maneja los siguientes canales de salida o de entrada. • Puerta de enlace de API REST: puerta de enlace a los clientes REST externos que asigna las llamadas a la interfaz de programación de aplicaciones de NetWitness. • Distribuidor de notificaciones: distribuidor centralizado para todas las notificaciones de salida que se originan en la implementación de NetWitness.
Investigate	El servidor de Investigate está colocalizado en el host del servidor de NW con el **servidor de Admin**, **servidor de Config**, **servidor de Integration,** **servidor de Orchestration**, **servidor de Respond** y **servidor de Security**. El servidor de Investigate está colocalizado en el host del servidor de NW con el servidor de Admin, servidor de Config, servidor de Integration, servidor de Orchestration, servidor de Respond y servidor de Security. Para obtener más información, consulte la *Guía del usuario de Investigate y Malware Analysis de RSA NetWitness Suite*. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Servicio	Propósito
Orchestration	El servidor de Investigate es un servicio de administración del sistema interna que se ejecuta en el Servidor de NW para aprovisionar, instalar y configurar todos los servicios en la implementación de NetWitness Suite.
Respond	El servidor de Respond está colocalizado en el host del servidor de NW con el **servidor de Admin**, **servidor de Config**, **servidor de Investigate**, **servidor de Orchestration** y **servidor de Security**. Para obtener más información, consulte la *Guía de configuración de RSA NetWitness Suite Respond*. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.
Security	El servidor de Security de NetWitness Suite (**servidor de Security**) administra la infraestructura de seguridad de una implementación de NetWitness Suite. Maneja las siguientes inquietudes relacionadas con la seguridad. • Usuarios y cuentas de autenticación • Control de acceso basado en funciones (RBAC) • Infraestructura de PKI de la implementación Una implementación de NetWitness Suite tiene usuarios con cuentas de autenticación. Independientemente de cómo verifique la identidad del analista (por ejemplo, Active Directory), NetWitness Suite debe mantener el estado del usuario que no todos los proveedores de autenticación proporcionan (por ejemplo, última hora de inicio de sesión, intentos de inicio de sesión fallidos y funciones). El concepto de un usuario es independiente de la identificación asociada con el usuario y el **servidor de Security** los mantiene como entidades de usuario y de cuenta por separado. Además de las cuentas de NetWitness locales de uso inmediato disponibles para todas las implementaciones de NetWitness, el servidor es compatible con proveedores de autenticación externa. El **servidor de Security** también implementa RBAC mediante la administración de las entidades de función y de permisos. Los permisos se pueden asignar a las funciones y las funciones, a los usuarios. En conjunto, estos permiten una política de autorización flexible para la implementación. El servidor también administra la generación de tokens criptográficamente seguros que codifican la autorización correspondiente para un usuario. Estos tokens forman la base para la autorización en toda la implementación.

Ejecución en modo mixto

El modo mixto se produce cuando se actualizan algunos de los servicios a la versión más reciente y algunos todavía están en las versiones anteriores. Esto sucede cuando actualiza los hosts en su implementación a la versión más reciente en fases (o si escalona la actualización).

Brechas de funcionalidad que se detectaron en las actualizaciones escalonadas

Si escalona la actualización:

- Es posible que no todas las funciones estén operativas hasta que actualice la implementación completa.
- No tendrá funciones administrativas de servicios disponibles hasta que actualice todos los hosts en la implementación.
- Es probable que durante un período de tiempo no capture datos.

Ejemplos de actualizaciones escalonadas

En los ejemplos siguientes, todos los hosts se encuentran en 11.1.0.x y desea escalonar las actualizaciones de hosts a la versión 11.1.1.0.

Ejemplo 1. Varios Decoders y Concentrators, alternativa 1

En este ejemplo, la implementación de 11.1.0.x incluye 1 host del servidor de NW, 2 hosts de Decoder, 2 hosts de Concentrator, 1 host de Archiver, 1 host de Broker, 1 host de Event Stream Analysis y 1 host de Malware Analysis.

Debe completar la fase 1 en primer lugar y actualizar los hosts en el orden que se indica para la fase 1.

RSA recomienda que actualice los hosts de la fase 2 en el orden que se indica para la fase 1

Fase 1: sesión 1

1. Actualice el host del servidor de Security Analytics.
2. Actualice el host de Event Stream Analysis.
3. Actualice el host de Malware Analysis.
4. Host de Broker o Concentrator.

Fase 2: sesión 2

1. Actualice 2 hosts de Decoder.
2. Actualice 2 hosts de Concentrators y el host de Archiver.

Fase 2: sesión 3

1. Actualice el resto de los hosts.

Ejemplo 2. Varios Decoders y Concentrators, alternativa 2

En este ejemplo, la implementación de 11.1.0.x incluye 1 host del servidor de NW, 2 hosts de Decoder, 2 hosts de Concentrator, 1 host de Broker, 1 host de Event Stream Analysis y 1 host de Malware Analysis. RSA recomienda que actualice los hosts de la fase 2 en la siguiente secuencia (debe completar la fase 1 en primer lugar y actualizar los hosts en el orden indicado).

Fase 1: sesión 1

1. Actualice el host del servidor de Security Analytics.
2. Actualice el host de Event Stream Analysis.
3. Actualice el host de Malware Analysis.
4. Actualice el host de Broker.

Fase 2: sesión 2

1. Actualice 1 host de Decoder y 1 host de Concentrator.
   Transcurre tiempo durante el cual NetWitness Suite procesa una gran cantidad de datos.

Fase 2: sesión 3

1. Actualice 1 host de Decoder, 1 host de Concentrator y el host de Broker.
2. Log Decoders
   Actualice todos los hosts de Log Decoder antes de actualizar Virtual Log Collectors
3. Actualice el resto de los hosts.

Ejemplo 3. Varias regiones

En este ejemplo, la implementación de 11.1.0.x incluye 1 host del servidor de NW, 1 host de Event Stream Analysis, 1 host de Malware Analysis, 4 hosts de Decoder, 4 hosts de Concentrator, 2 hosts de Broker (2 sitios, cada uno con 2 Decoders, 2 Concentrators y 1 Broker).

Fase 1: actualizar el sitio 1

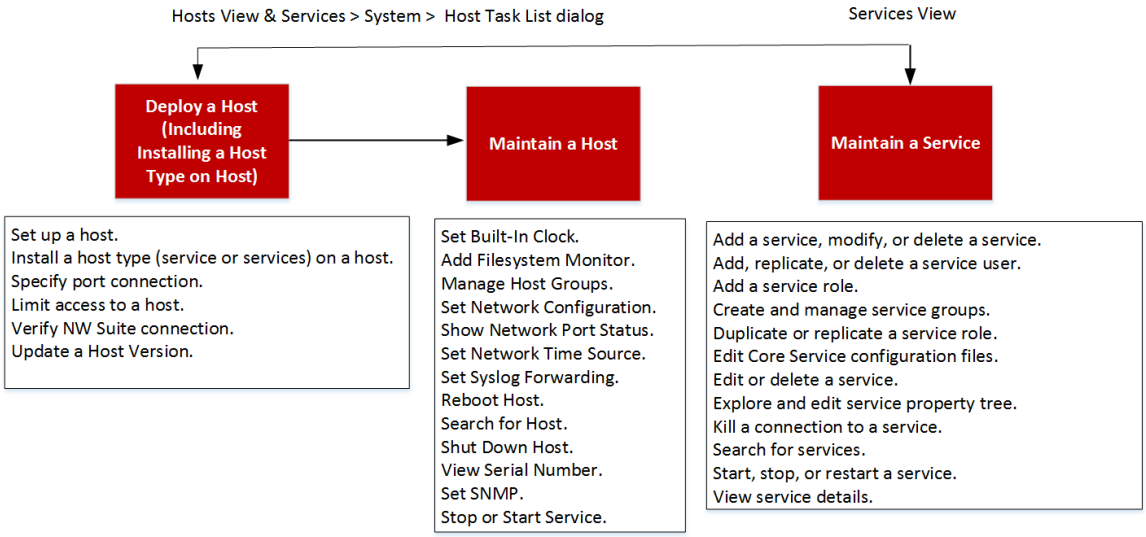
1. Actualice el host del servidor de NW.
2. Actualice el host de Event Stream Analysis.
3. Actualice el host de Malware Analysis.
4. Actualice 1 host de Broker, 2 hosts de Decoder y 2 hosts de Concentrator.
5. Actualice el resto de los hosts.

Fase 2: actualizar el sitio 2

1. Actualice los hosts de Broker.
2. Actualice 2 hosts de Decoder.
3. Actualice 2 hosts de Concentrator.
4. Actualice el resto de los hosts.

Introducción de hosts: Procedimientos de hosts y servicios

Cada servicio requiere un host. Después de configurar un host, puede asignar servicios hacia y desde este host a otros hosts de la implementación de NetWitness Suite.



Tarea general	Descripción
Configurar un host	Realice las siguientes tareas en el orden en que se muestran para configurar un host. Paso 1. Implementar un host. Paso 2. Instalar un servicio en un host. Paso 3. Revisar los puertos SSL para las conexiones de confianza. Paso 4. Administrar el acceso a un servicio.

Tarea general	Descripción

Mantener un host: aspectos básicos	Las siguientes tareas de mantenimiento no se requieren y se muestran en orden alfabético.
	• Aplicar actualizaciones de versión a un host.
	  • Completar el repositorio de actualización local
	  • Configurar un repositorio externo con actualizaciones de RSA y del SO
	• Crear y administrar grupos de hosts.
	• Buscar hosts.
	• Definir configuración de red.
	• Definir origen de tiempo de red.
	• Mostrar estado de puerto de red.
	• Mostrar número de serie.
	• Apagar un host.
	• Detener e iniciar un servicio en un host.

Tarea general	Descripción
Mantener un host desde el cuadro de diálogo Lista de tareas del host	El cuadro de diálogo Lista de tareas del host se usa para administrar las tareas relacionadas con un host y sus comunicaciones con la red. Varias opciones de configuración de servicios y hosts están disponibles para los hosts principales. • Ejecutar una tarea de la Lista de tareas del host. • Agregar y eliminar un monitor del sistema de archivos. • Reiniciar un host. • Definir reloj integrado de host. • Definir configuración de red. • Definir origen de tiempo de red. • Configurar SNMP. • Definir reenvío de syslog. • Mostrar estado de puerto de red. • Mostrar número de serie. • Apagar host. • Detener e iniciar un servicio en un host.

Tarea general	Descripción
Mantener un servicio	Los siguientes procedimientos describen cómo mantener servicios. • Agregar, replicar o eliminar un usuario de servicio. • Agregar una función de usuario de servicio. • Cambiar una contraseña de usuario de servicio. • Crear y administrar grupos de servicios. • Duplicar o replicar una función de servicio. • Editar los archivos de configuración de servicios principales. • Editar o eliminar un servicio. • Explorar y editar el árbol de propiedades de servicios. • Interrumpir una conexión a un servicio. • Buscar servicios. • Iniciar, detener o reiniciar un servicio. • Ver detalles de servicios.

Paso 1. Implementar un host

1. Implementar un host.
   Puede implementar un host físico (dispositivo RSA), un host virtual en las instalaciones, un host virtual en AWS o un host virtual en Azure. Consulte las siguientes guías para obtener instrucciones sobre cómo implementar los hosts.
   - *Guía de implementación del host físico de RSA NetWitness® Suite*
   - *Guía de implementación del host virtual de RSA NetWitness® Suite*
   - *Guía de implementación de AWS de RSA NetWitness® Suite*
   - *Guía de implementación de Azure de RSA NetWitness® Suite*
2. Vaya a **Administration** > **Hosts**.
   El cuadro de diálogo **Nuevos hosts** se muestra con los hosts que implementó.
3. Seleccione los hosts que desea habilitar.
   La opción de menú **Habilitar** se activa.

4. Haga clic en **Habilitar**.

5. Seleccione el host que habilitó.

   El host se muestra en la vista Hosts. En este punto, puede instalar un servicio en el host.

Paso 2. Instalar un servicio en un host

Cada servicio se modela como un plug-in para habilitarse o deshabilitarse según la función del host.

Requisitos previos

Se deben instalar equipos que puedan ser físicos o virtuales: Servidor de NetWitness, Broker, Concentrator, Decoder, Log Decoder, Archiver, Warehouse, servidor de Malware Analysis o servidor de Event Stream Analysis.

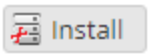
Procedimiento

Realice los siguientes pasos para agregar un servicio a un host:

1. En NetWitness Suite, vaya a **ADMIN > Hosts**.

   Se muestra la vista **Hosts**.

2. Seleccione el host en el que desea instalar el servicio (por ejemplo, **Event Stream Analysis**).

3. Haga clic en 

(ícono Instalar) en la barra de herramientas.

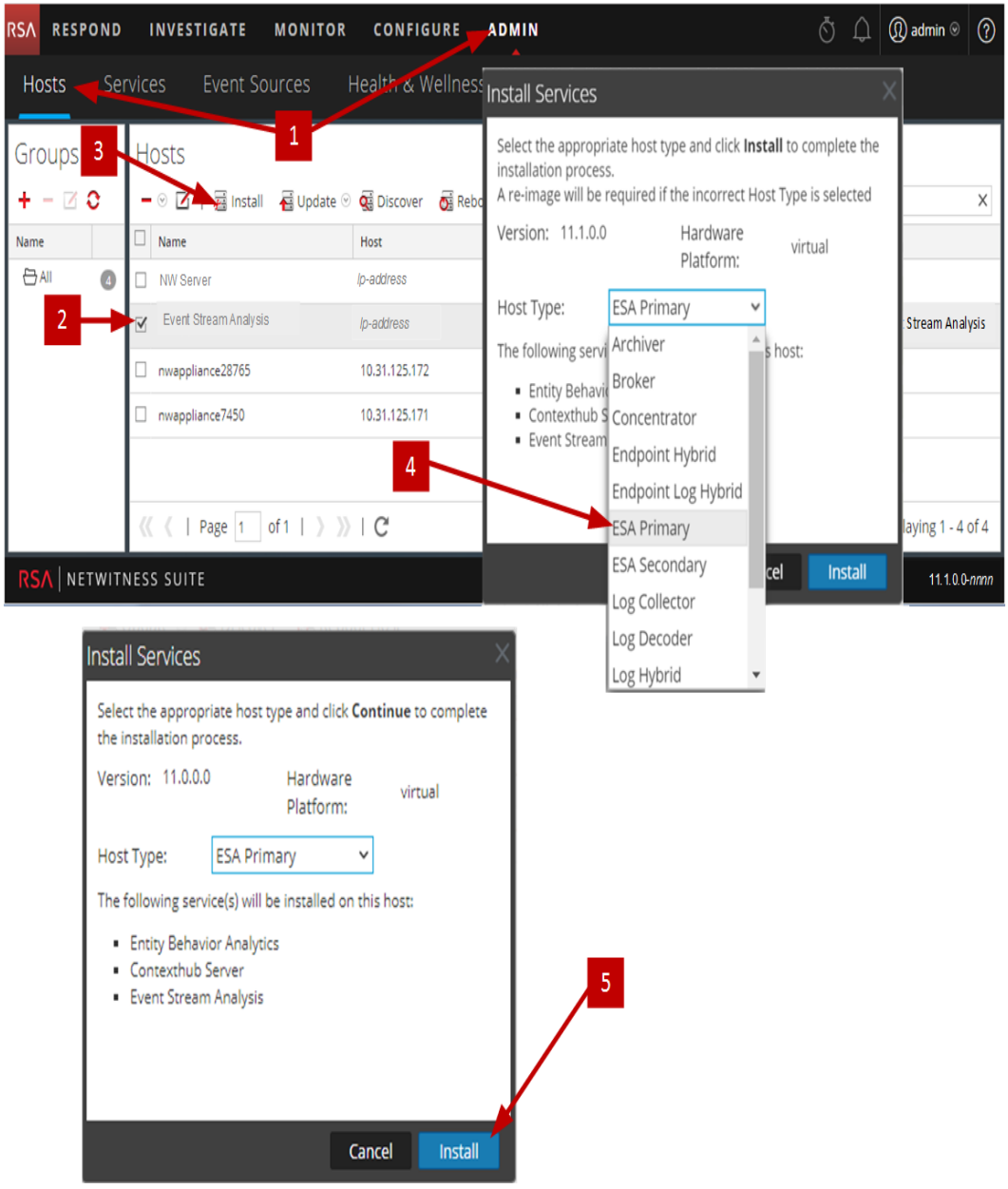
   Se muestra el cuadro de diálogo **Instalar servicios**.

4. Seleccione un servicio en la lista desplegable **Tipo de host** (por ejemplo, **ESA primario**).

(botón del comando Instalar) se activa en el cuadro de diálogo **Instalar servicios**.

5. Haga clic en Install (botón del comando Instalar).



Paso 3. Revisar puertos SSL para conexiones de confianza

Para ofrecer compatibilidad con conexiones de confianza, cada servicio principal tiene dos puertos, un puerto no SSL no cifrado y un puerto SSL cifrado. Las conexiones de confianza requieren el puerto SSL cifrado.

Requisito previo

Para establecer una conexión de confianza, cada servicio de NetWitness Suite Core se debe actualizar a 10.4 o superior. Las conexiones de confianza no tienen compatibilidad con las versiones de NetWitness Suite Core 10.3.x o anteriores.

Puertos SSL cifrados

Cuando instala o actualiza a 10.4 o superior, las conexiones de confianza se establecen de manera predeterminada con dos configuraciones:

1. SSL está activado.
2. El servicio principal está conectado a un puerto SSL cifrado.

Cada servicio de NetWitness Suite Core tiene dos puertos:

- **Puerto no SSL** no cifrado
  Ejemplo: Archiver 50008
- **Puerto SSL** cifrado
  Ejemplo: Archiver 56008

El puerto SSL es el puerto no SSL + 6000.

En la siguiente tabla se indican todos los servicios de NetWitness Suitecon sus respectivos puertos y se muestra que cada servicio principal tiene dos puertos. Todos los números de puerto señalados son TCP.

Servicio	Puerto no SSL no cifrado	Puerto SSL cifrado	Notas
Archiver	50008	56008	
Broker	50003	56003	
Cloud Gateway	N/D	N/D	
Concentrator	50005	56005	
Context Hub	N/D	50022	
Decoder (Packets)	50004	56004	
Endpoint	N/D	N/D	

Servicio	Puerto no SSL no cifrado	Puerto SSL cifrado	Notas
Entity Behavior Analysis	N/D	N/D	
Event Stream Analysis	N/D	50030	
Investigate	N/D	N/D	Se implementa con el servidor de NW.
Log Collector	50001	56001	
Log Decoder	50002	56002	
Malware Analysis	N/D	60007	
Reporting Engine	N/D	N/D	Se implementa con el servidor de NW.
Respond	N/D	N/D	Se implementa con el servidor de NW.
Warehouse Connector	50020	56020	
Workbench	50007	56007	

Paso 4. Administrar el acceso a un servicio

En una conexión de confianza, un servicio confía explícitamente en el Servidor de NW para administrar y autenticar usuarios. Con esta confianza, los servicios en **ADMINISTRAR > Servicios** ya no requieren credenciales para poder definirse para cada servicio de NetWitness Suite Core. En lugar de eso, los usuarios autenticados por el servidor pueden acceder al servicio sin ingresar otra contraseña.

Probar una conexión de confianza

REQUISITOS PREVIOS

1. Se debe asignar una función al usuario.

   Para obtener detalles, consulte **Agregar un usuario y asignar una función** en la *Guía de administración de usuarios y seguridad del sistema*.

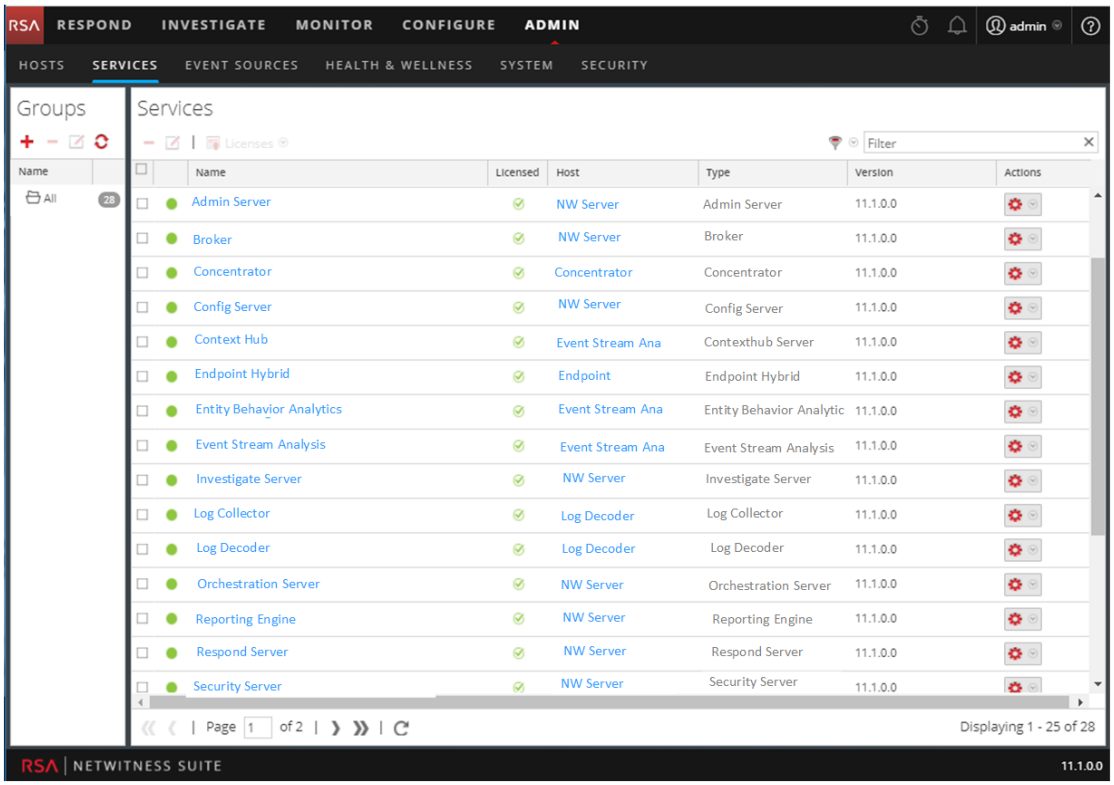
2. El usuario debe:

   - Iniciar sesión en NetWitness Suite para que el servidor lo autentique
   - Tener acceso al servicio

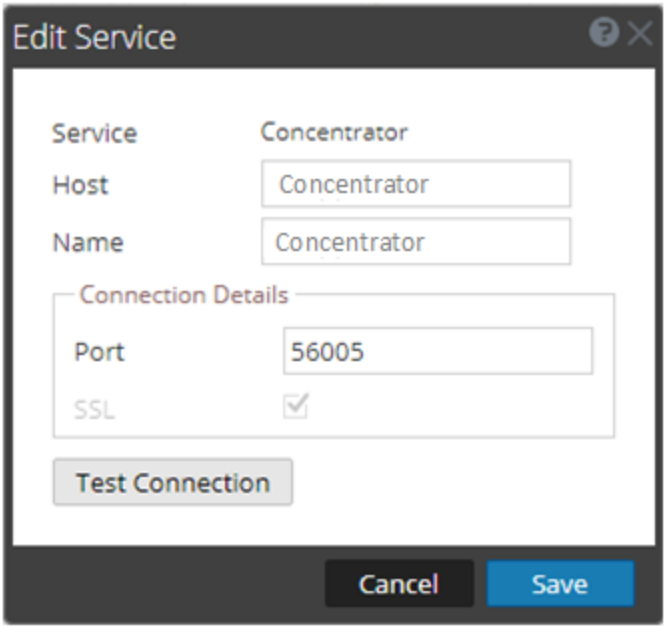
PROCEDIMIENTO

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.

   Se muestra la vista Servicios.

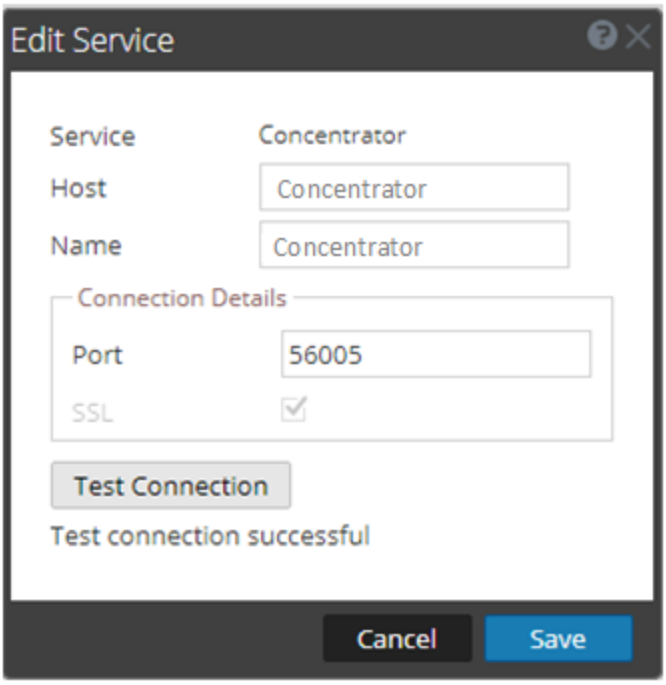


2. Seleccione el servicio (por ejemplo, un Concentrator) que desea probar y haga clic en .
   Se muestra el cuadro de diálogo **Editar servicio**.



3. Si realizó una instalación nueva de 11.0.0.0, el puerto está correcto. No se requiere ninguna acción en el campo **Puerto**. Vaya al paso siguiente.
   Si actualizó a 11.0.0.0 o tiene un ambiente mixto de un servidor 11.0.0.0 y hosts 10.3, debe actualizar el **puerto** mediante la deselección y la selección de **SSL**. Entonces, el número de **puerto** cambia al puerto SSL cifrado para el servicio.
4. Elimine el **nombre de usuario** para probar la conexión sin credenciales.

5. Haga clic en **Probar conexión**.



   El mensaje **La conexión de prueba se estableció correctamente** confirma que se estableció la conexión de confianza.
   El usuario previamente autenticado puede acceder al servicio sin escribir el nombre de usuario y la contraseña en el servicio.

6. Haga clic en **Guardar**.

Aplicar actualizaciones de versión a un host

Realice las siguientes tareas para actualizar un host a una nueva actualización de versión.

Puede usar dos métodos para aplicar actualizaciones de versión a un host.

Nota: Si cambió la ubicación del repositorio, consulte Configurar un repositorio externo con actualizaciones de RSA y del SO para obtener instrucciones.

- Aplicar actualizaciones desde la vista Hosts (acceso a la Web)
- Aplicar una actualización desde la línea de comandos (sin acceso a la Web)

Aplicar actualizaciones desde la vista Hosts (acceso a la Web)

Tarea 1. Completar el repositorio local o configurar un repositorio externo

Cuando configura el servidor de NW, debe seleccionar el repositorio local o un repositorio externo. La vista Hosts recupera las actualizaciones de versión desde el repositorio que se selecciona.

Si seleccionó el repositorio local, no es necesario configurarlo, pero debe asegurarse de que se complete con las actualizaciones de versión más recientes. Consulte Completar el repositorio local para obtener instrucciones sobre cómo completarlo con la actualización de versión.

Nota: Si seleccionó un repositorio externo, debe configurarlo. Consulte Configurar un repositorio externo con actualizaciones de RSA y del SO para obtener instrucciones sobre cómo configurar un repositorio externo.

Tarea 2. Aplicar actualizaciones desde la vista Hosts a cada host

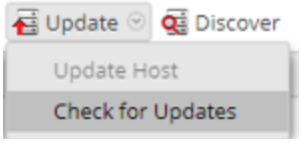
En la vista Hosts se muestran las actualizaciones de versiones de software disponibles en el repositorio de actualización local y se le permite elegir y aplicar las actualizaciones que desea.

Precaución: Si intenta actualizar servidores que no son de NW a parches de 11.0.0.x después de la actualización del servidor de NW a 11.1, la actualización del host de servidores que no son de NW estará en un estado fallido. Consulte “Actualización para <host>”, “Error al preparar el host <hostname> para su actualización a la versión 11.0.0.x. Compruebe los registros.” en Introducción de hosts: Solución de problemas de instalaciones y actualizaciones de versión para obtener más información.

En este procedimiento se indica cómo actualizar un host a una versión nueva de NetWitness Suite.

Nota: En este tema se utiliza NetWitness Suite 11.0.x.x a 11.1.0.0 como ejemplo.

1. Inicie sesión en NetWitness Suite.
2. Vaya a **ADMINISTRAR > HOSTS**.
3. (Condicional) Busque las actualizaciones más recientes.

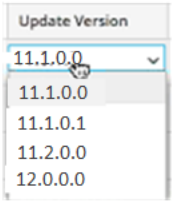


4. Seleccione uno o más hosts.

   En primer lugar, debe actualizar el servidor de NW a la versión más reciente. Puede actualizar los demás hosts en la secuencia que prefiera, pero RSA recomienda seguir las

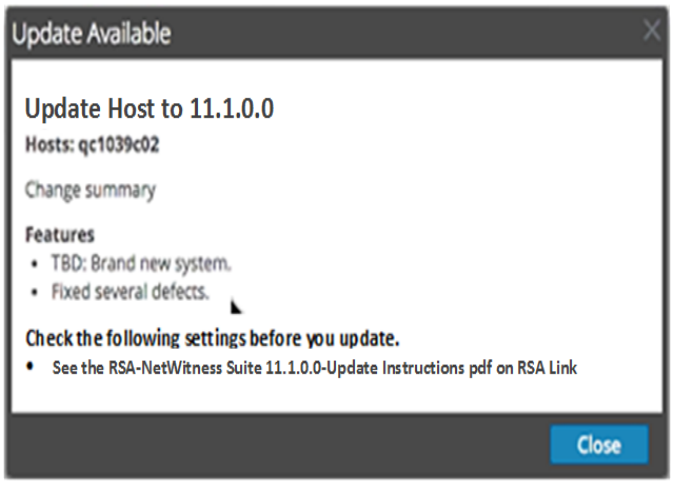
reglas que aparecen en “Ejecución en modo mixto” en la *Guía de introducción de hosts y servicios de RSA NetWitness Suite* para obtener más información.
Se muestra Actualización disponible en la columna **Estado** si hay una actualización de versión en el repositorio de actualización local para los hosts seleccionados.

5. Seleccione la versión que desea aplicar en la columna **Versión de actualización**.



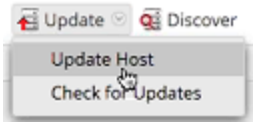
Si:

- Si desea actualizar más de un host a esa versión, después de actualizar el host de servidor de NW, seleccione la casilla de verificación a la izquierda de los hosts. Solo se enumeran las versiones de actualización compatibles actualmente.
- Desea ver un cuadro de diálogo con las principales funciones de la actualización e información sobre las actualizaciones, haga clic en el icono de información ( ) a la derecha del número de versión de actualización. El siguiente es un ejemplo de este cuadro de diálogo.

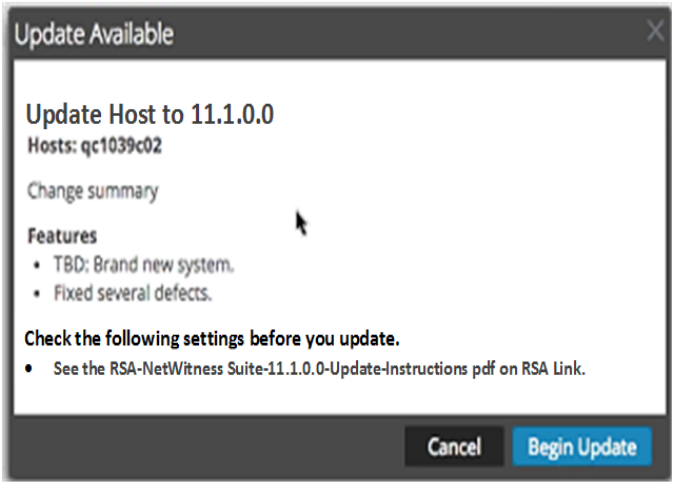


- No puede encontrar la versión que desea, seleccione **Actualizar > Buscar actualizaciones** para buscar las actualizaciones disponibles en el repositorio. Si hay una actualización disponible, se muestra el mensaje “Están disponibles nuevas actualizaciones” y la columna **Estado** se actualiza automáticamente para mostrar Actualización disponible. De forma predeterminada, solo se muestran las actualizaciones compatibles para el host seleccionado.

6. Haga clic en **Actualizar > Actualizar host** en la barra de herramientas.



Se muestra un cuadro de diálogo con información sobre la actualización seleccionada. Haga clic en **Iniciar actualización**.



En la columna **Estado** se indica lo que está sucediendo en cada una de las siguientes etapas de la actualización:

- Etapa 1: **Descargando paquetes de actualización**: Descarga al servidor de NW los artefactos del repositorio que se aplican a los servicios en el host que eligió.
- Etapa 2: **Configurando los paquetes de actualización**: Configura los archivos de actualización en el formato correcto.
- Etapa 3: **Actualización en curso**: Actualiza el host a la nueva versión.

7. Cuando vea **Actualización en curso**, actualice el navegador.
   Esto puede hacer que se dirija a la pantalla Iniciar sesión de NetWitness. Si esto sucede, inicie sesión y regrese a la vista Host.
   Después de la actualización del host, NetWitness Suite le solicita que ejecute la acción **Reiniciar host**.
8. Haga clic en **Reiniciar host** en la barra de herramientas.
   NetWitness Suite muestra el estado como **Reiniciando…** hasta que el host vuelve a estar en línea. Una vez que el host vuelve a estar en línea, en **Estado** se muestra **Actualizado**.
   Póngase en contacto con Atención al cliente si el host no vuelve a estar en línea.

Nota: Si la STIG de la DISA está habilitada, la apertura de los servicios principales puede tardar aproximadamente entre cinco y 10 minutos. La generación de los nuevos certificados es la causa de este retraso.

Aplicar actualizaciones desde la línea de comandos (sin acceso a la Web)

Si su implementación de RSA NetWitness Suite no tiene acceso a la Web, realice el siguiente procedimiento para aplicar una actualización de versión.

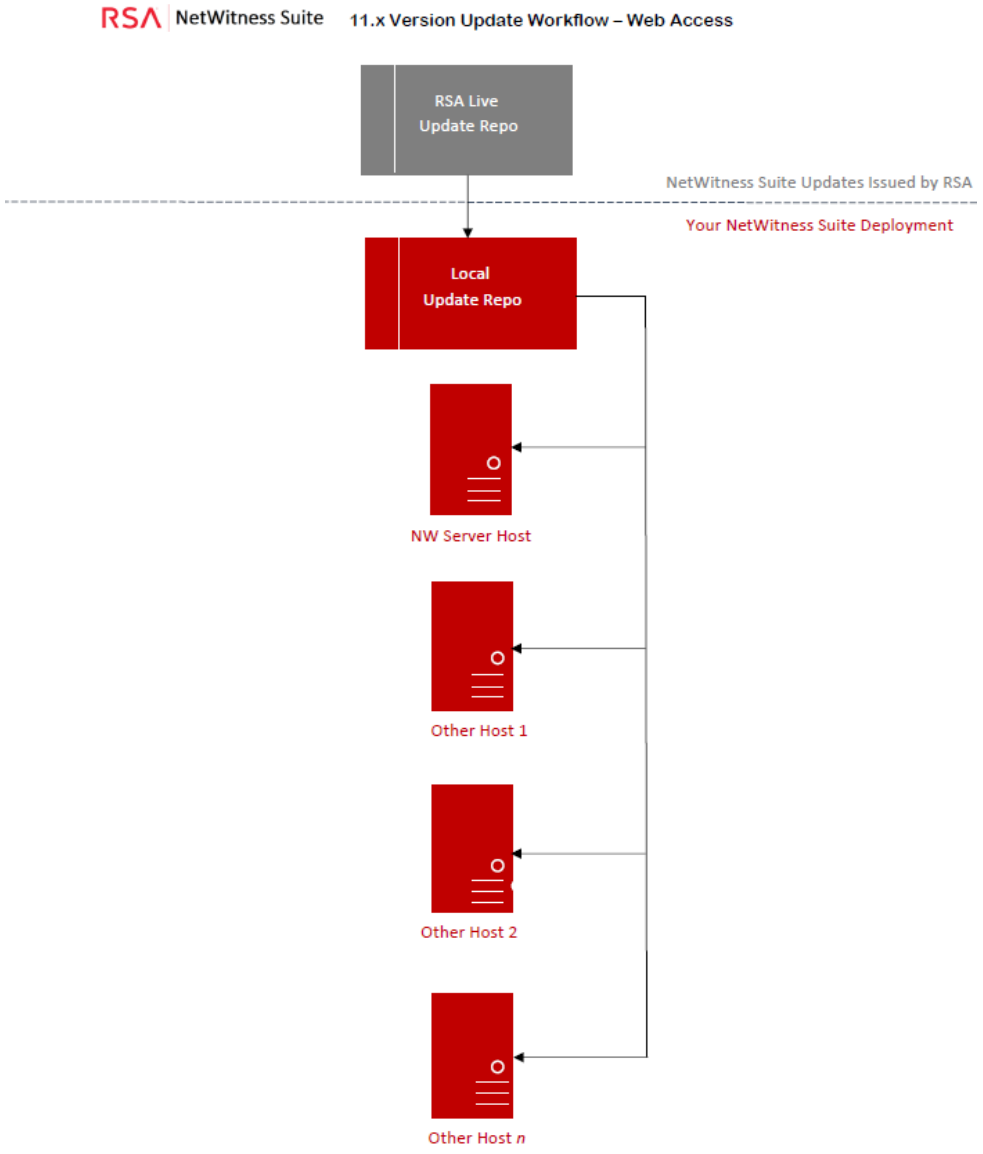
Nota: En el siguiente procedimiento, 11.1.0.0 es la actualización de versión que se usa como ejemplo en las cadenas de código.

1. Descargue el paquete de actualización de `.zip` correspondiente a la versión que desea (por ejemplo, `netwitness-11.1.0.0.zip`) desde RSA Link a un directorio local.
2. Acceda mediante el protocolo SSH al host del servidor de NW.
3. Cree un directorio de almacenamiento provisional `tmp/upgrade/<version>` para la versión que desea (por ejemplo, `tmp/upgrade/11.1.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.1.0.0
   ```
4. Descomprima el paquete en el directorio de almacenamiento provisional que creó (por ejemplo, `tmp/upgrade/11.1.0.0`).
   ```
   cd /tmp/upgrade/11.1.0.0
   unzip /tmp/upgrade/11.1.0.0/netwitness-11.1.0.0.zip
   ```
5. Inicialice la actualización en el servidor de NW.
   ```
   upgrade-cli-client --init --version 11.1.0.0 --stage-dir
   /tmp/upgrade/
   ```
6. Aplique la actualización al servidor de NW.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version
   11.1.0.0
   ```
7. Inicie sesión en NetWitness Suite y reinicie el host del servidor de NW en la vista Host.
8. Aplique la actualización a cada uno de los hosts de servidores que no son de NW.
   ```
   upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> -
   -version 11.1.0.0
   ```
   La actualización está completa cuando finaliza el sondeo.
9. Inicie sesión en NetWitness Suite y reinicie el host en la vista Host.
   Puede verificar la versión que se aplicó al host mediante el siguiente comando:
   ```
   upgrade-cli-client --list
   ```

Completar el repositorio de actualización local

NetWitness Suite envía actualizaciones de versión al repositorio de actualización local desde el repositorio de actualización de Live. El acceso al repositorio de actualización de Live requiere y usa las credenciales de la cuenta de Live configuradas en **ADMINISTRAR > SISTEMA > Live**. Además, debe seleccionar la casilla de verificación `Automatically download information about new updates every day` en **ADMINISTRAR > SISTEMA > Actualizaciones** para completar el repositorio local diariamente.

En el siguiente diagrama se ilustra la manera de obtener actualizaciones de versión si la implementación de NetWitness Suite tiene acceso a la Web.



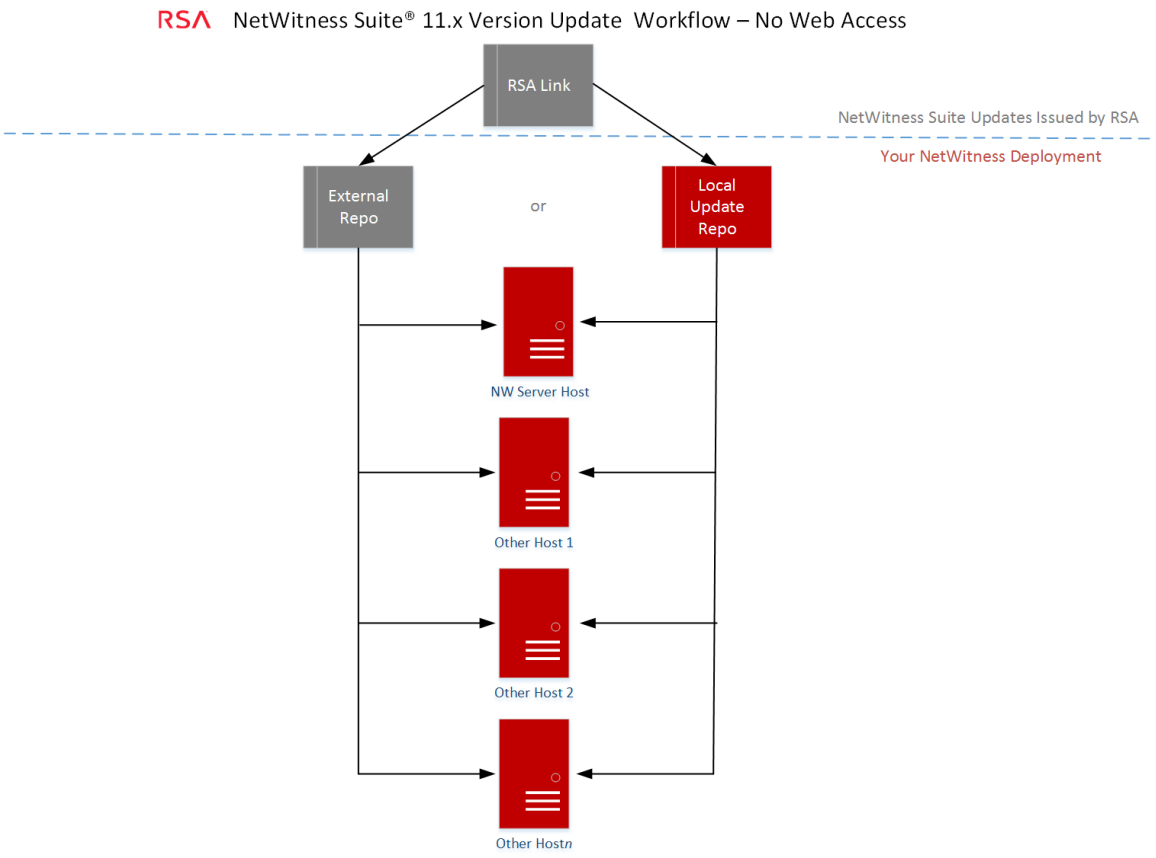
Nota: Cuando establezca la conexión inicial al repositorio de actualización de Live, accederá a todos los paquetes del sistema CentOS 7 y a los paquetes de producción de RSA. Esta descarga de más de 2.5 GB de datos tardará una cantidad indeterminada de tiempo de acuerdo con la conexión a Internet del servidor de NW y el tráfico del repositorio de RSA. El uso del repositorio de actualización de Live NO es obligatorio. Como alternativa, puede usar un repositorio externo como se describe en "Configuración de un repositorio externo".

Para conectarse al repositorio de actualización de Live, navegue a la vista **ADMINISTRAR > SISTEMA**, seleccione **Live** en el panel de opciones y asegúrese de que las credenciales estén configuradas (la luz de **Conexión** debería ser de color verde). Si no es verde, haga clic en **Iniciar sesión** y conéctese.

Nota: Si necesita usar un proxy para establecer conexión al repositorio de actualización de Live, puede configurar valores en Host proxy, Nombre de usuario de proxy y Contraseña de proxy. Consulte "Configurar el proxy deNetWitness Suite" en la *Guía de configuración del sistema de NetWitness Suite 1.1*.Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Consulte "Aplicar actualizaciones desde la línea de comandos" si la implementación de NetWitness Suite no tiene acceso a la Web.

En el siguiente diagrama se ilustra la manera de obtener actualizaciones de versión si la implementación de NetWitness Suite no tiene acceso a la Web.



Configurar un repositorio externo con actualizaciones de RSA y del SO

Nota: En el siguiente procedimiento, 11.1.0.0 es la actualización de versión que se usa como ejemplo en las cadenas de código.

Realice el siguiente procedimiento para configurar un repositorio externo (repositorio).

Nota: 1.) Para realizar este procedimiento, debe estar instalada una utilidad de descompresión en el host. 2.) Debe saber cómo crear un servidor web antes de realizar el siguiente procedimiento.

1. (Condicional) Complete este paso si tiene un repositorio externo y desea reemplazarlo.
   - Caso 1: Inició el host desde un repositorio externo y desea actualizar con un repositorio local en el servidor de Admin.

a. Cree el archivo `/etc/netwitness/platform/repobase`.
   `vi /etc/platform/netwitness/repobase`

b. Edite el archivo `repobase` para que la siguiente dirección URL sea la única información en el archivo.
   `https://nw-node-zero/nwrpmrepo`

c. Complete las instrucciones sobre cómo ejecutar la actualización usando la herramienta `upgrade-cli-client` .
   Consulte para obtener instrucciones.

- Caso 2: Inició el host desde un repositorio local en el servidor de Admin (host del servidor de NW) y desea usar un repositorio externo para la actualización.

a. Cree el archivo `/etc/netwitness/platform/repobase`.
   `vi /etc/platform/netwitness/repobase`

b. Edite el archivo `repobase` para que la siguiente dirección URL sea la única información en el archivo.
   `https://<webserver-ip>/<alias-for-repo>`

c. Complete las instrucciones sobre cómo ejecutar la actualización usando la herramienta `upgrade-cli-client`.
   Las instrucciones se encuentran en “Aplicar actualizaciones desde la línea de comandos” en el tema.

2. Configure el repositorio externo.

a. Iniciar sesión en el host del servidor web

b. Cree el directorio para alojar el repositorio de NW (`netwitness-11.1.0.0.zip`), por ejemplo `ziprepo` bajo `web-root` del servidor web. Por ejemplo, si /var/netwitness es la raíz web, ejecute la siguiente cadena de comandos.
   `mkdir -p /var/netwitness/<your-zip-file-repo>`

c. Cree el directorio 11.1.0.0 bajo `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`

d. Cree los directorios `OS` y `RSA` bajo `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`

e. Descomprima el archivo `netwitness-11.1.0.0.zip` en el directorio `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-`

repo>/11.1.0.0

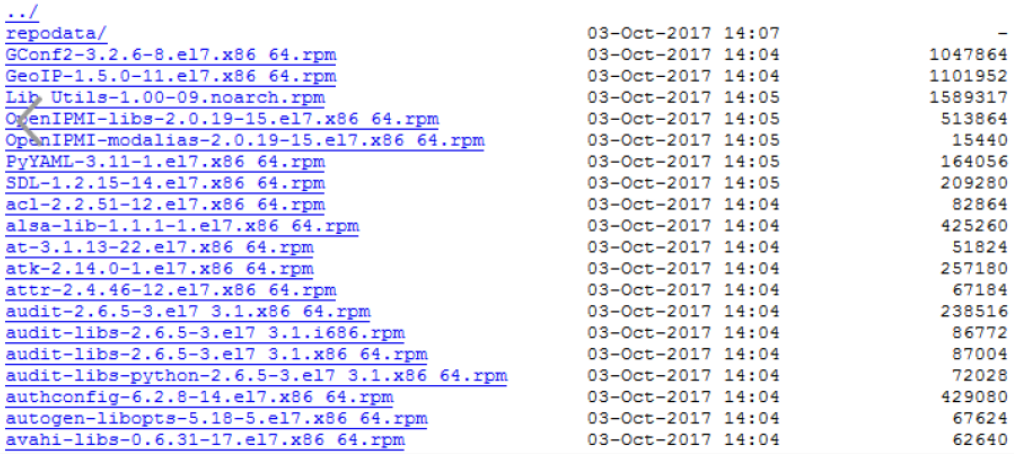
Con la descompresión de netwitness-11.1.0.0.zip se obtienen dos archivos zip (OS-11.1.0.0.zip y RSA-11.1.0.0.zip) y algunos otros archivos.

f. Descomprima

1. OS-11.1.0.0.zip en el directorio /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS.

   unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS

   En el siguiente ejemplo se ilustra la forma en que aparecerá la estructura de archivos del sistema operativo (SO) después de descomprimir el archivo.



../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

2. RSA-11.1.0.0.zip en el directorio /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA.

   unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA

   En el siguiente ejemplo se ilustra la forma en que aparecerá la estructura de archivos

de actualización de la versión de RSA después de descomprimir el archivo.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

La dirección URL externa del repositorio es `http://<web server IP address>/<your-zip-file-repo>`.

g. (Condicional: para Azure) Siga estos pasos para la actualización de Azure

i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

ii. `unzip nw-azure-11.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`

iv. `createrepo .`

h. Use `http://<web server IP address>/<your-zip-file-repo>` en respuesta al indicador **Ingrese la dirección URL base de los repositorios de actualización externos** del programa de instalación de NW 11.1.0.0 (`nwsetup-tui`).

Crear y administrar grupos de hosts

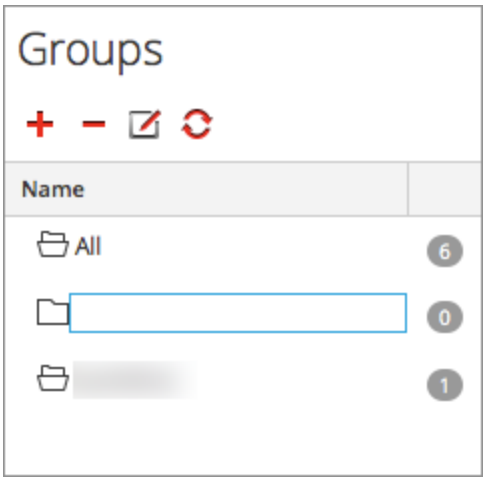
La vista Hosts ofrece opciones para crear y administrar grupos de hosts. La barra de herramientas del panel Grupos incluye opciones para crear, editar y eliminar grupos de hosts. Una vez que se crean los grupos, puede arrastrar hosts individuales desde el panel Hosts a un grupo.

Los grupos pueden reflejar un principio funcional, geográfico, orientado a un proyecto o cualquier principio de la organización que sea útil. Un host puede pertenecer a más de un grupo. Aquí hay algunos ejemplos de posibles agrupamientos:

- Agrupe diferentes tipos de hosts para facilitar la configuración y el monitoreo de todos los Brokers, Decoders o Concentrators.
- Agrupe hosts que formen parte del mismo flujo de datos; por ejemplo, un Broker y todos los Concentrators y los Decoders asociados.
- Agrupe hosts según su región geográfica y su ubicación dentro de la región. Si ocurre una interrupción de energía importante en una ubicación, los hosts posiblemente afectados se pueden identificar fácilmente.

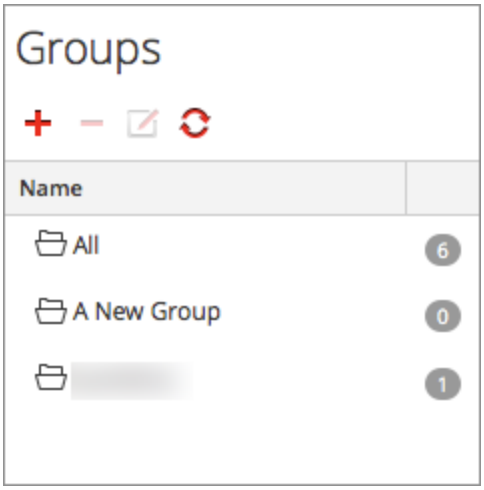
Crear un grupo

1. Seleccione **ADMIN** > **Hosts**.
   Se muestra la vista Hosts.
2. En la barra de herramientas del panel **Grupos**, haga clic en +.
   Se abre un campo para el grupo nuevo con un cursor parpadeante.



3. Escriba el nombre del grupo nuevo en el campo (por ejemplo, **Un grupo nuevo**) y presione **Intro**.
   El grupo se crea como una carpeta en el árbol. El número junto al grupo indica la cantidad

de hosts en ese grupo.



Cambiar el nombre de un grupo

1. En el panel **Grupos** de la vista Hosts, haga doble clic en el nombre de grupo o seleccione el grupo y haga clic en .

   El campo de nombre de abre con un cursor parpadeante.

2. Escriba el nuevo nombre del grupo y presione **Intro**.

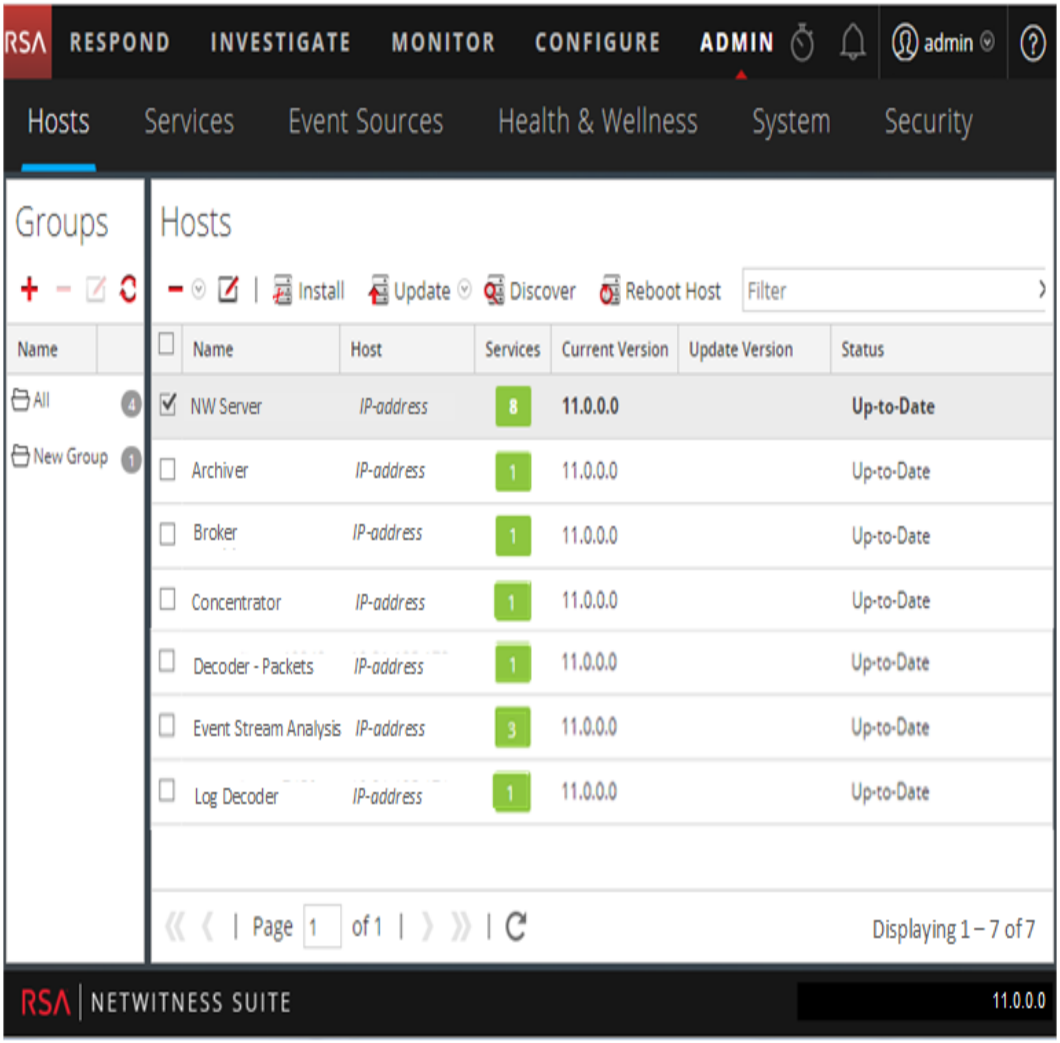
   El campo de nombre se cierra y el nuevo nombre del grupo se muestra en el árbol.

Agregar un host a un grupo

En el panel **Hosts** de la vista Hosts, seleccione un host y arrástrelo a una carpeta de grupo del panel Grupos.
El host se agrega al grupo.

Ver los hosts de un grupo

Para ver los hosts de un grupo, haga clic en el grupo en el panel **Grupos**.
En el **panel Hosts** se muestran los hosts de ese grupo.



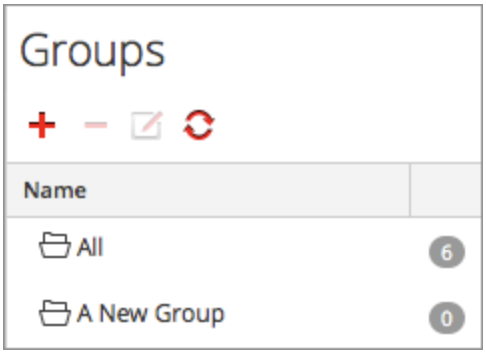
Eliminar un host de un grupo

1. En el **panel Grupos** de la vista Hosts, seleccione el grupo que contiene el host que desea eliminar. Los hosts de ese grupo aparecen en el panel Hosts.
2. En el **panel Hosts**, seleccione uno o más hosts que desee quitar del grupo y, en la barra de herramientas, seleccione > **Eliminar degrupo**.

   Los hosts seleccionados se quitan del grupo, pero no se quitan de la interfaz del usuario de NetWitness Suite. La cantidad de hosts en el grupo, que se indica cerca del nombre del grupo, disminuye según la cantidad de hosts eliminados del grupo. El grupo **Todo** contiene los hosts que se quitaron del grupo.

   En el siguiente ejemplo, el grupo de hosts denominado **Un grupo nuevo** no contiene ningún

host, ya que el host de ese grupo se quitó.



Eliminar un grupo

1. En el **panel Grupos** de la vista Hosts, seleccione el grupo que desea eliminar.
2. Haga clic en .

   El grupo seleccionado se quita del panel Grupos. Los hosts que estaban en el grupo no se quitan de la interfaz del usuario de NetWitness Suite. El grupo **Todo** contiene los hosts del grupo eliminado.

Buscar hosts

Puede buscar hosts desde una lista de hosts en la vista Hosts. La vista Hosts permite filtrar rápidamente la lista de hosts por Nombre y Host. Pueden estar en uso varios hosts de NetWitness Suite para distintos propósitos. En lugar de desplazarse por la lista de hosts, puede filtrar rápidamente esta lista para localizar los hosts que desea administrar.

En la vista Servicios, puede buscar un servicio y encontrar rápidamente el host que lo ejecuta.

Buscar un host

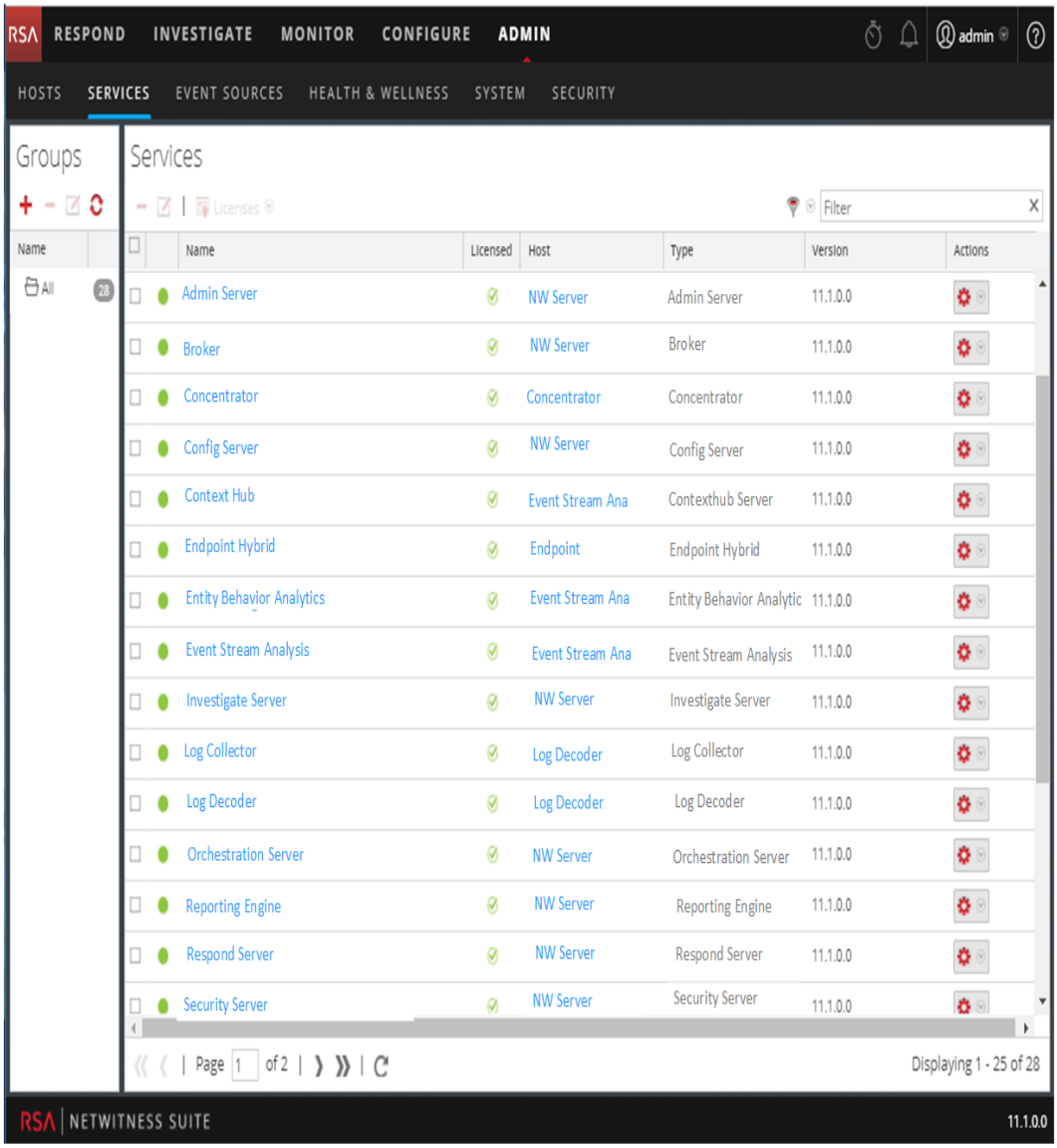
1. Seleccione **ADMIN** > **Hosts**.
2. En la barra de herramientas del **panel Hosts**, escriba un **Nombre** o el **Nombre del host** en el campo **Filtro**.

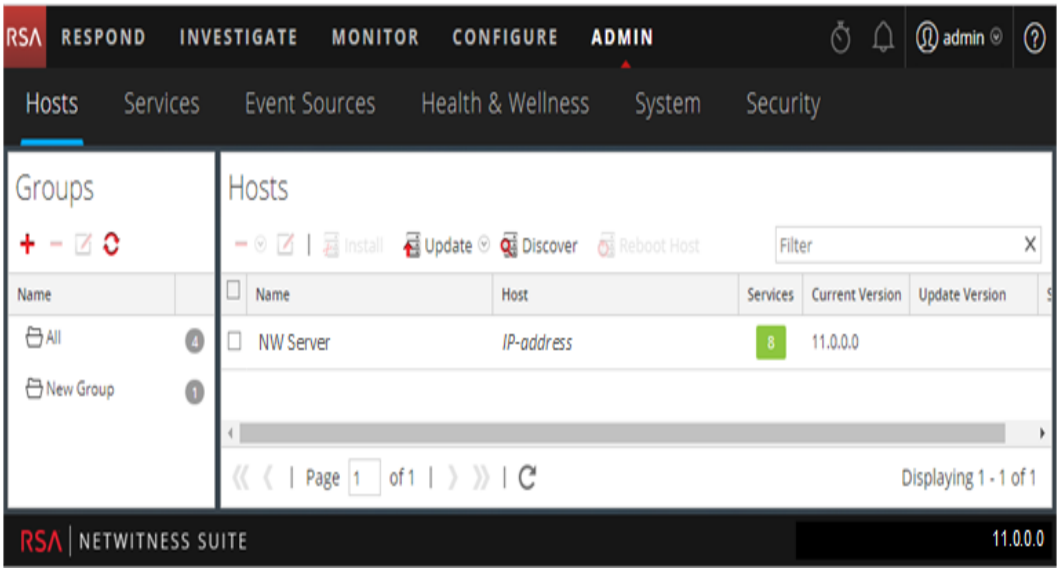
   En el panel Hosts se enumeran los hosts que coinciden con los nombres ingresados en el campo Filtro.

Buscar el host que ejecuta un servicio

1. Seleccione **ADMINISTRAR > Servicios**.
2. En la vista Servicios, seleccione un servicio. El host asociado se muestra en la columna **Host** de ese servicio.



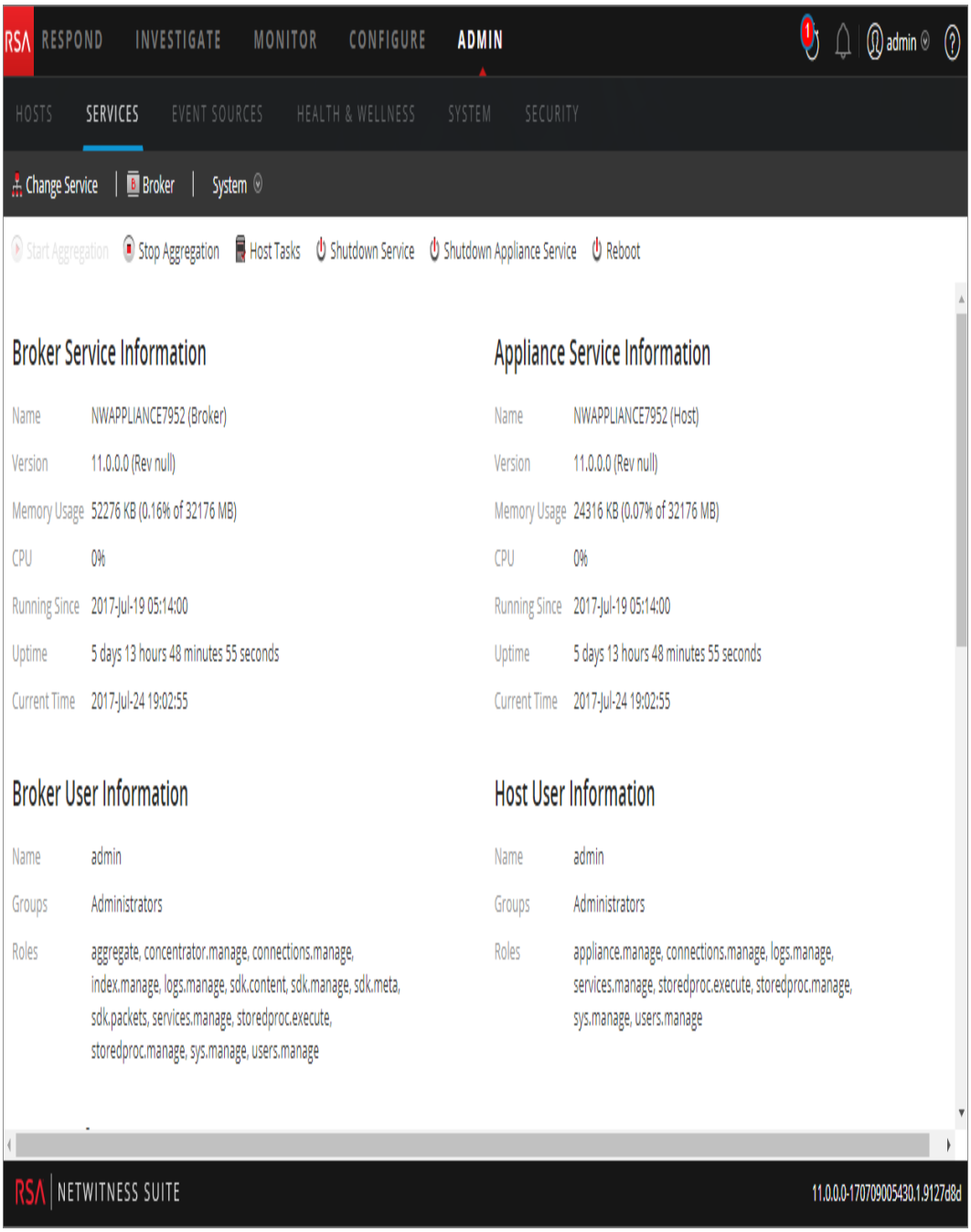
3. Para administrar el host en la vista Hosts, haga clic en el vínculo de la columna **Host** de ese servicio. El host asociado con el servicio seleccionado se muestra en la vista Hosts.



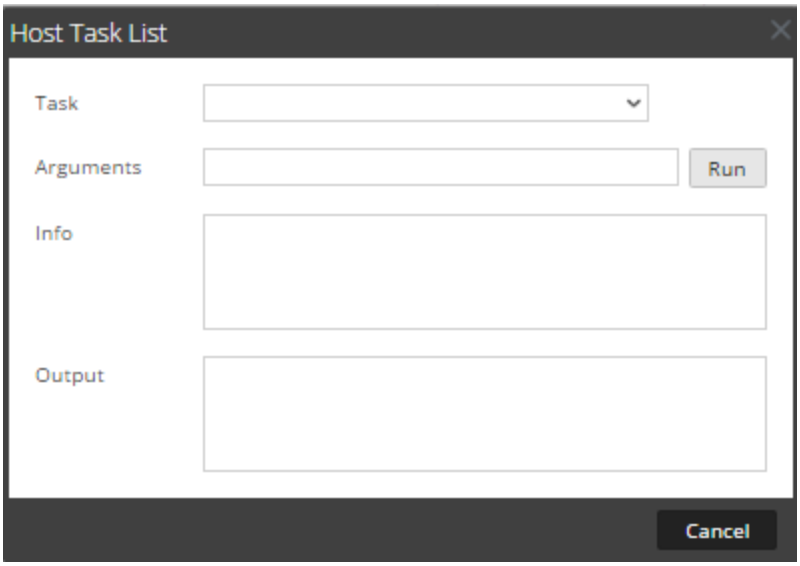
Ejecutar una tarea de la Lista de tareas del host

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en > **Ver** > **Sistema**.

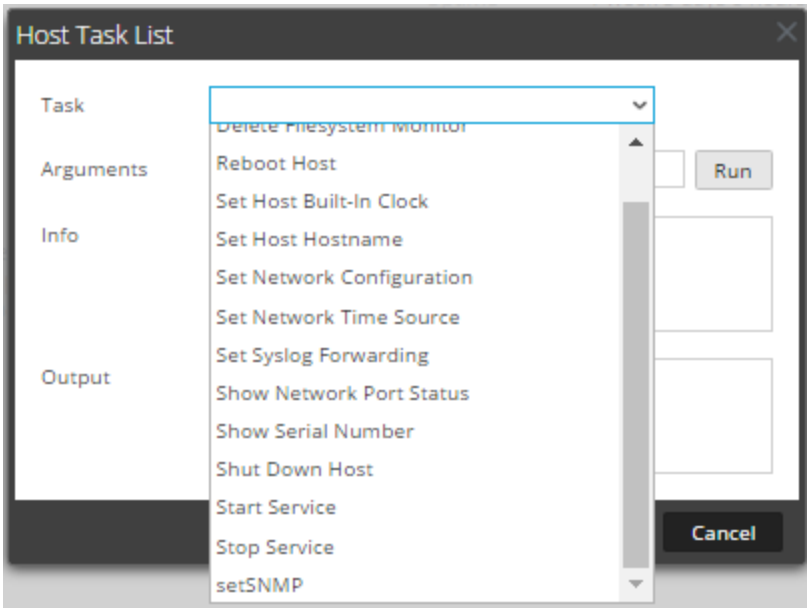
Nota: Los servicios Admin, Config, Orchestration, Security, Investigate y Respond tienen acceso a la vista Sistema. Solo tienen acceso a la vista Explorar.
Se muestra la vista Sistema del servicio.


RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN
admin
HOSTS SERVICES EVENT SOURCES HEALTH & WELLNESS SYSTEM SECURITY
Change Service | Broker | System
Start Aggregation Stop Aggregation Host Tasks Shutdown Service Shutdown Appliance Service Reboot
Broker Service Information
Name NWAPPLIANCE7952 (Broker)
Version 11.0.0.0 (Rev null)
Memory Usage 52276 KB (0.16% of 32176 MB)
CPU 0%
Running Since 2017-Jul-19 05:14:00
Uptime 5 days 13 hours 48 minutes 55 seconds
Current Time 2017-Jul-24 19:02:55
Appliance Service Information
Name NWAPPLIANCE7952 (Host)
Version 11.0.0.0 (Rev null)
Memory Usage 24316 KB (0.07% of 32176 MB)
CPU 0%
Running Since 2017-Jul-19 05:14:00
Uptime 5 days 13 hours 48 minutes 55 seconds
Current Time 2017-Jul-24 19:02:55
Broker User Information
Name admin
Groups Administrators
Roles aggregate, concentrator.manage, connections.manage, index.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, 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
RSA | NETWITNESS SUITE
11.0.0.0-170709005430.1.9127d8d

3. En la barra de herramientas de la vista **Sistema de servicios**, haga clic en Host Tasks.

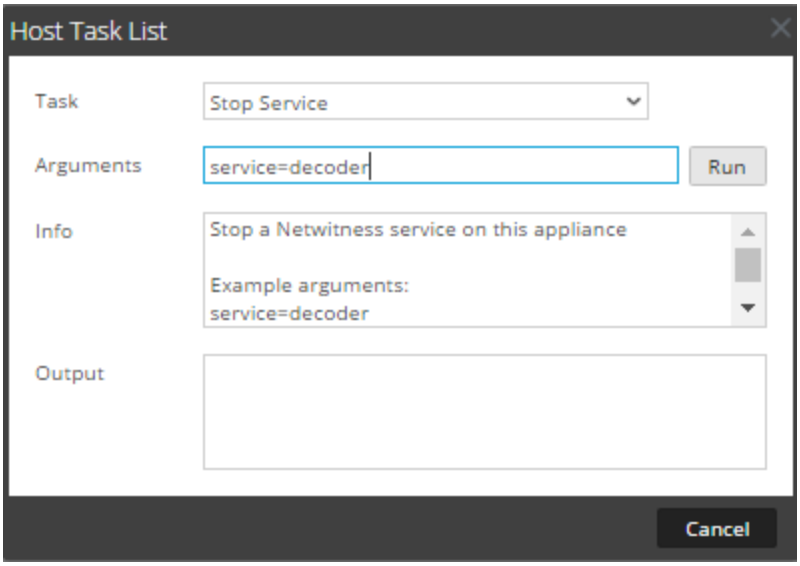


4. En la **Lista de tareas del host**, haga clic en el campo **Tarea** para ver una lista desplegable de las tareas que se ejecutan en un host.



5. Seleccione una tarea, por ejemplo, haga clic en **Detener servicio**.
   La tarea aparece en el campo **Tarea** y la descripción de la tarea, argumentos de ejemplo,

funciones de seguridad y parámetros se muestran en el área **Información**.



6. Ingrese argumentos, si es necesario, y haga clic en **Ejecutar**.
   El comando se ejecuta y el resultado aparece en la sección **Salida**.

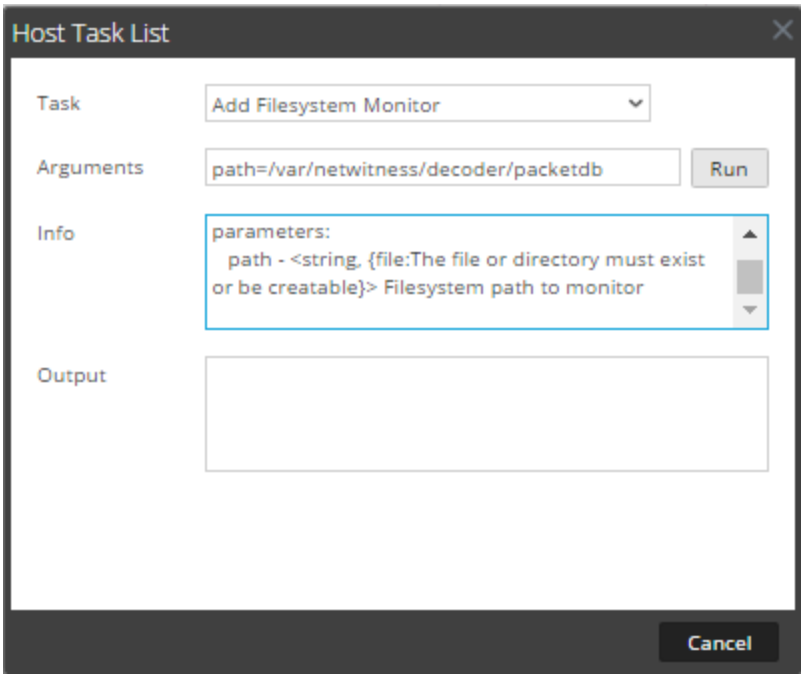
Agregar y eliminar un monitor del sistema de archivos

Cuando desee que un servicio monitoree tráfico en un sistema de archivos específico, puede seleccionar el servicio y, a continuación, especificar la ruta. Security Analytics agrega un monitor del sistema de archivos. Una vez que se agrega un monitor de sistema de archivos a un servicio, el servicio continúa monitoreando el tráfico en esa ruta hasta que el monitor se elimina.

Configurar el monitor de sistema de archivos

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en > **Ver** > **Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas del host**, seleccione **Agregar monitor de sistema de archivos**.
   En el área **Información**, se muestra una breve explicación de la tarea y sus argumentos.
5. Para identificar el sistema de archivos que desea monitorear, escriba la ruta en el campo **Argumentos**. Por ejemplo:

path=/var/netwitness/decoder/packetdb

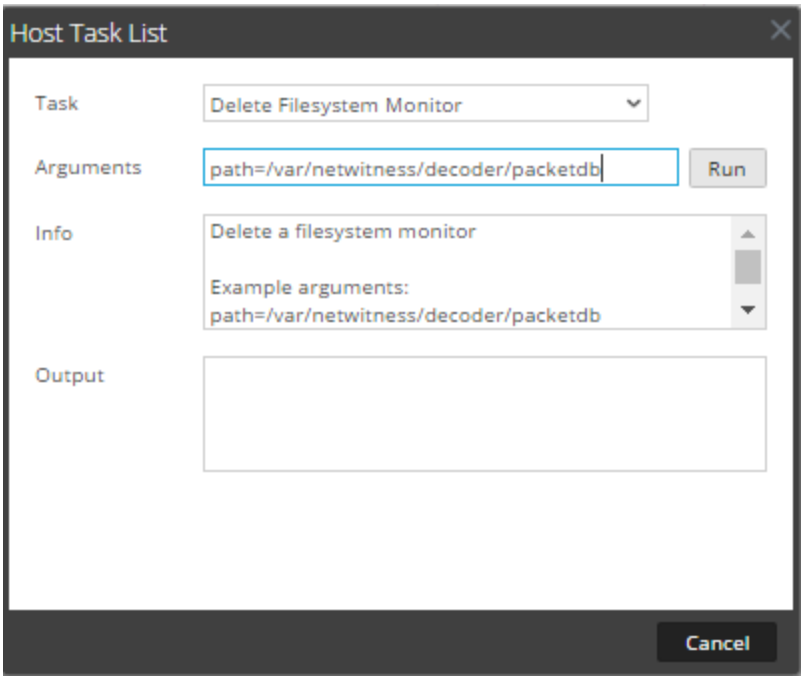


6. Haga clic en **Ejecutar**.
   El resultado se muestra en el área **Salida**. El servicio comienza a monitorear el sistema de archivos y continúa haciéndolo hasta que se elimina.

Eliminar un monitor de sistema de archivos

1. Navegue al cuadro de diálogo **Lista de tareas del host**.
2. En la **Lista de tareas del host**, seleccione **Eliminar monitor de sistema de archivos**.
   En el área **Información**, se muestra una breve explicación de la tarea y sus argumentos.
3. Para identificar el sistema de archivos que desea dejar de monitorear, escriba la ruta en el campo **Argumentos**. Por ejemplo:

path=/var/netwitness/decoder/packetdb



4. Haga clic en **Ejecutar**.
   El resultado se muestra en el área **Salida**. El servicio deja de monitorear el sistema de archivos.

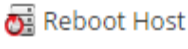
Reiniciar un host

En ciertas condiciones es necesario reiniciar un host, por ejemplo, después de instalar una actualización de software. Este procedimiento usa un mensaje de la Lista de tareas del host para apagar y reiniciar un host.

Security Analytics también ofrece otras opciones para apagar un host:

- Para apagar y reiniciar un host a través de un servicio conectado, vaya a la vista Hosts desde un servicio en la vista Servicios (consulte Buscar hosts) y, a continuación, siga el procedimiento *Apagar y reiniciar un host desde la vista Hosts* que se indica a continuación.
- Para apagar el host físico sin reiniciar, consulte Apagar host.

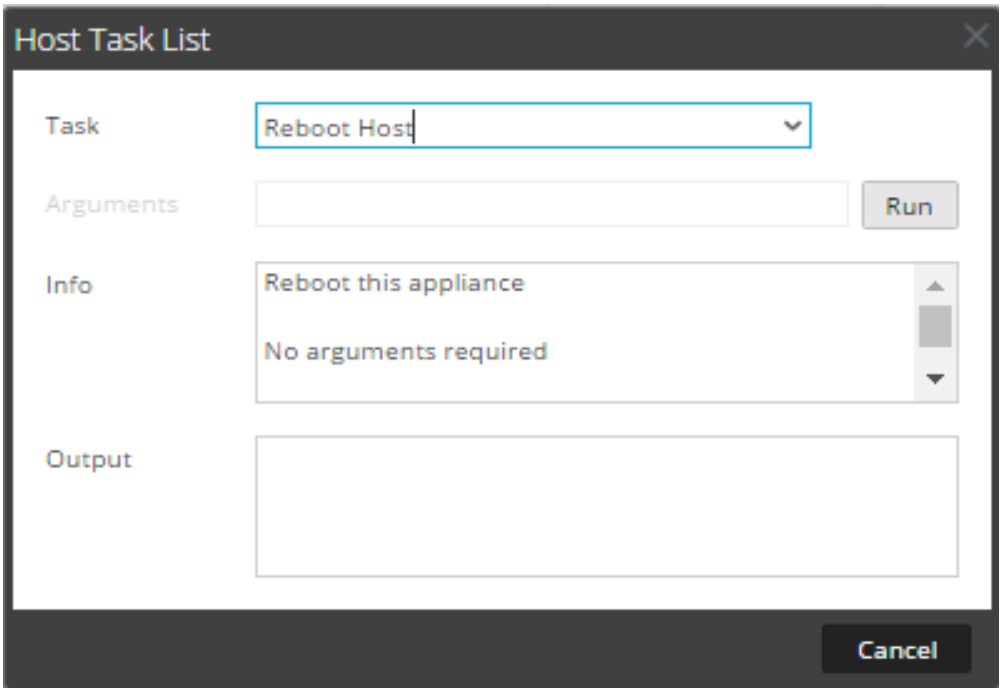
Apagar y reiniciar un host desde la vista Hosts

1. Seleccione **ADMIN > Hosts**.
2. En el panel **Hosts**, seleccione un host.
3. Seleccione 

en la barra de herramientas.

Apagar y reiniciar un host desde la Lista de tareas del host

1. Seleccione **ADMIN** > **Servicios**.
2. En el panel **Servicios**, seleccione un servicio y haga clic en > **Ver** > **Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas del host**, seleccione **Reiniciar host** en el campo **Tarea**
   .No se requieren argumentos.



5. Haga clic en **Ejecutar**.
   El host se reinicia y el resultado se muestra en el área **Salida**.

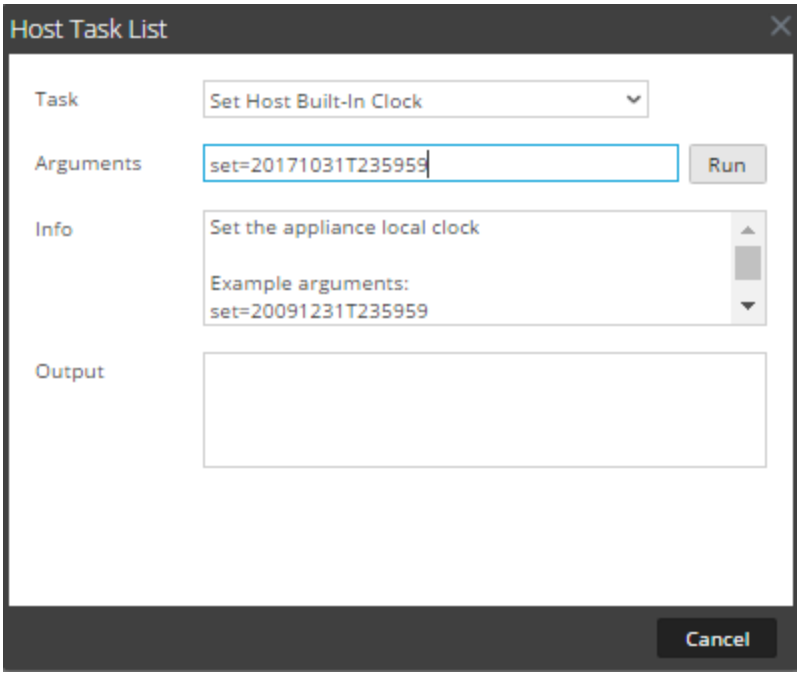
Definir reloj integrado de host

Después de un apagado o de una falla de la batería, puede ser necesario configurar el reloj local en un host. La tarea Definir reloj integrado de host restablece la hora del reloj.

Configurar la hora en el reloj local

1. Seleccione **ADMIN** > **Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y > **Ver** > **Sistema**.
   Se muestra la vista Sistema del servicio.

3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas del host**, seleccione **Definir reloj integrado de host**. La ayuda para la tarea aparece en el área **Información**.
5. Ingrese los argumentos de fecha y hora en el campo **Argumentos**; por ejemplo, para especificar 31 de octubre de 2017 a las 23:59:59 h, ingrese:
   set=20171031T235959



6. Haga clic en **Ejecutar**.
   El reloj se configura en la hora especificada y se muestra un mensaje en el área **Salida**.

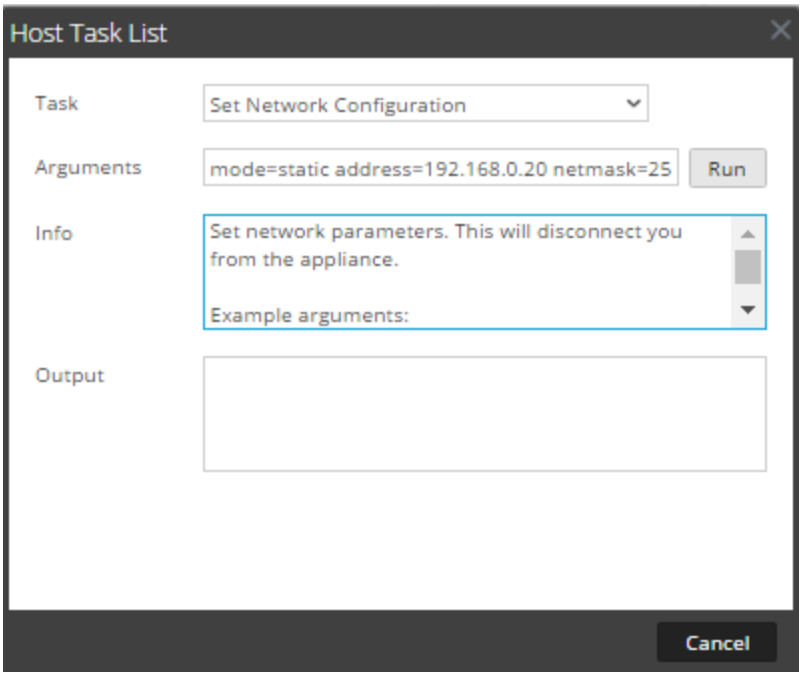
Definir configuración de red

Cuando es necesario cambiar la dirección de un host Core configurado, puede configurar una nueva dirección de red, una máscara de subred y un gateway para el host con el mensaje **Definir configuración de red** de la **Lista de tareas del host**.

Precaución: El cambio se aplica de inmediato y el host se desconecta de Security Analytics. Debe volver agregar el host a Security Analytics con el uso de la nueva dirección de red.

Especificar la dirección de red para un host

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en > **Ver** > **Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas del host**, haga clic en **Definir configuración de red**.
   La tarea se muestra en el campo **Tarea** y la ayuda, en el área **Información**.
5. Escriba los argumentos en el campo **Argumentos**. Por ejemplo:
   mode=static address=192.168.0.20 netmask=255.255.255.0 gateway=192.168.0.1



6. Haga clic en **Ejecutar.**
   La tarea se ejecuta y el resultado aparece en el área **Resultado**. El host se desconecta de Security Analytics. Debe volver a agregarlo con la nueva dirección.

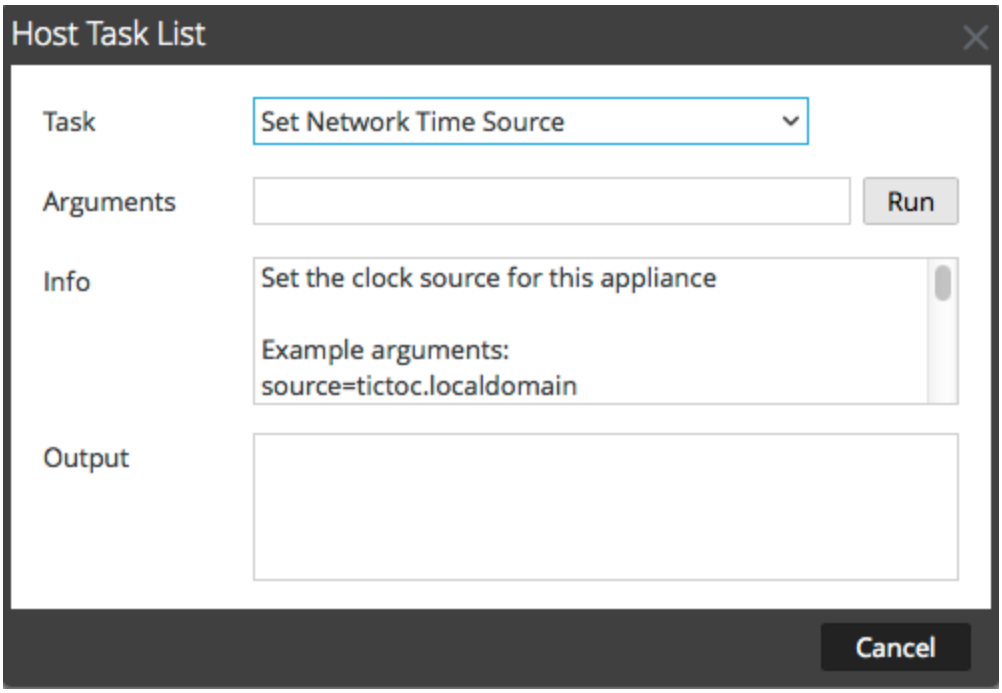
Nota: si el modo es DHCP, es posible que no haya manera de determinar la nueva dirección. Es posible que deba conectarse al host directamente para determinarla.

Definir origen de tiempo de red

Cuando configure el origen del reloj para un host, defina el nombre de host o la dirección de un servidor NTP que será el origen del reloj de red para el host. Si el host está utilizando un origen del reloj local, debe especificar **local** aquí para permitir que se aplique la configuración de **Definir el origen del reloj local**.

Especificar al origen del reloj de red

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en **Ver > Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas del host**, seleccione **Definir origen de tiempo de red**.



5. Realice una de las siguientes acciones:
   - Ingrese el nombre de host o la dirección del servidor NTP que se usarán como el origen del reloj para este host; por ejemplo: **source=tictoc.localdomain**
   - Si desea utilizar el reloj del host como un origen del reloj, ingrese: **source=local**
6. Haga clic en **Ejecutar**.
   Se define el origen del reloj y aparece un mensaje en el área **Resultado**.

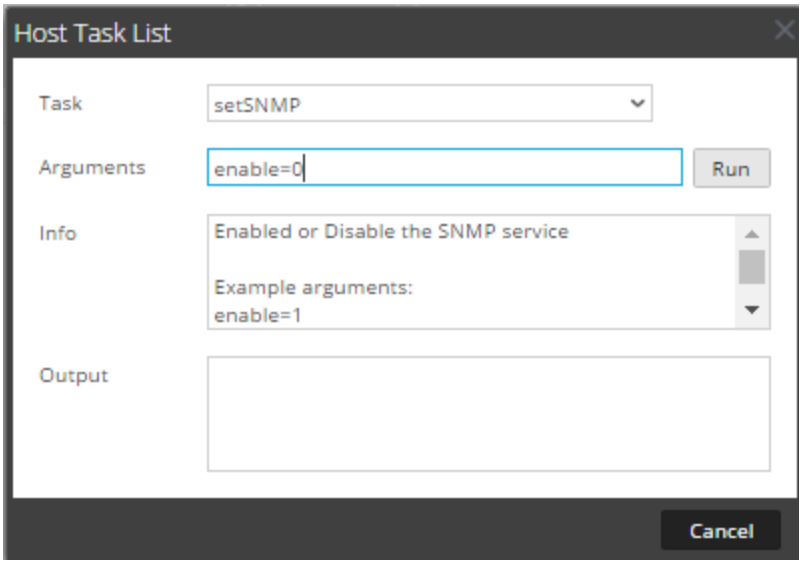
Nota: Si especificó un origen del reloj NTP **local**, el reloj del host se usa como el origen del reloj y la hora se configura mediante Definir reloj integrado de host.

Configurar SNMP

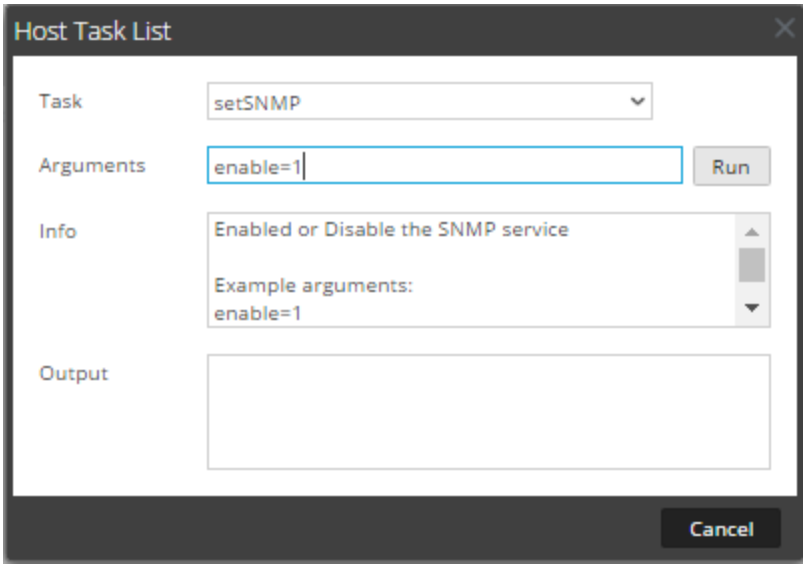
La configuración de SNMP en la Lista de tareas del host habilita o deshabilita el servicio SNMP en un host. Para que un host reciba notificaciones de SNMP, el servicio SNMP debe estar habilitado. Si no está utilizando SNMP para notificaciones de NetWitness Suite, no es necesario habilitar el servicio.

Alternar el servicio SNMP en el host

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en > **Ver** > **Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas del host**, seleccione **setSNMP**.
   En el área **Información**, se muestra una breve explicación de la tarea y sus argumentos.
5. Realice una de las siguientes acciones:
   - Si desea deshabilitar el servicio, ingrese **enable=0** en el campo **Argumentos**.



- Si desea habilitar el servicio, ingrese **enable=1** en el campo **Argumentos**.



6. Haga clic en **Ejecutar**.
   El resultado se muestra en el área **Salida**.

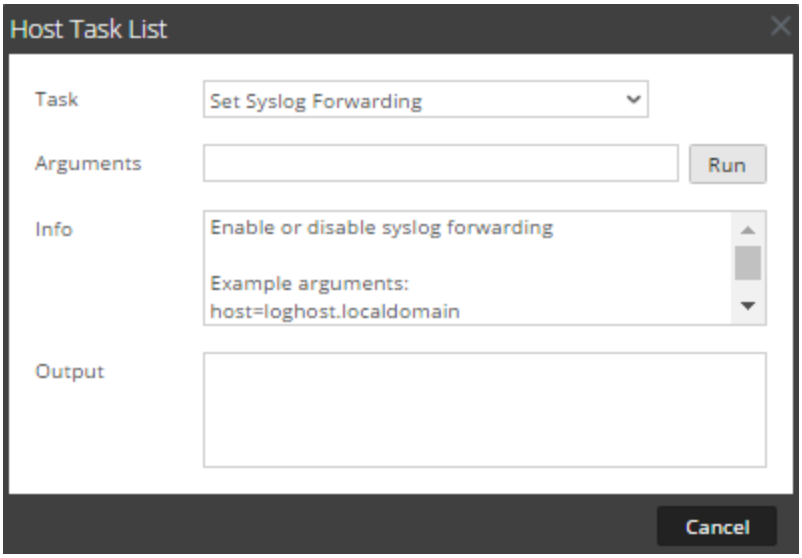
Definir reenvío de syslog

Puede configurar el reenvío de syslog para reenviar los registros del sistema operativo de los hosts de NetWitness Suite a un servidor de syslog remoto. Puede utilizar la tarea Definir reenvío de syslog de la Lista de tareas del host para habilitar o deshabilitar el reenvío de syslog.

Configurar e iniciar el envío de syslog

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en > **Ver** > **Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.

4. En la **Lista de tareas del host**, seleccione **Definir reenvío de syslog**.
   En el área **Información**, se muestra una breve explicación de la tarea y sus argumentos.



5. En el campo **Argumentos**, realice una de las siguientes acciones.
   - Para habilitar el reenvío de syslog, especifique cualquiera de los siguientes formatos:
     - **host=<loghost>.<localdomain>** (por ejemplo, host=syslogserver.local).
     - **host=<loghost>.<localdomain>:<port>** (por ejemplo, host=syslogserver.local:514).
     - **host=<IP>** (por ejemplo, host=10.31.244.244).
     - **host=<IP>:<port>** (por ejemplo, host=10.31.244.244:514).
       En la siguiente tabla se enumeran los parámetros que se usan para habilitar el reenvío de syslog y sus descripciones.

Parámetro	Descripción
loghost	El nombre de host del servidor de syslog remoto.
localdomain	El dominio del servidor de syslog remoto.
puerto	Dirección IP del servidor de syslog remoto.
IP	El número de puerto en el cual el servidor de syslog remoto recibe los mensajes de syslog.

   - Para deshabilitar el reenvío de syslog, escriba **host=disable**.
6. Haga clic en **Ejecutar**.
   El resultado se muestra en el área **Salida**.

Una vez que el reenvío de syslog se habilita o se deshabilita, el archivo `/etc/rsyslog.conf` se actualiza automáticamente para habilitarlo o deshabilitarlo al destino de syslog remoto y el servicio de syslog se reinicia.

Si habilita el reenvío de syslog, los registros del servicio configurado se reenvían al servidor de syslog definido y el reenvío continúa hasta que se inhabilita.

Nota: Ahora puede iniciar sesión en el servidor de syslog remoto y verificar si se reciben mensajes de los servicios de NetWitness Suite configurados para el reenvío de syslog.

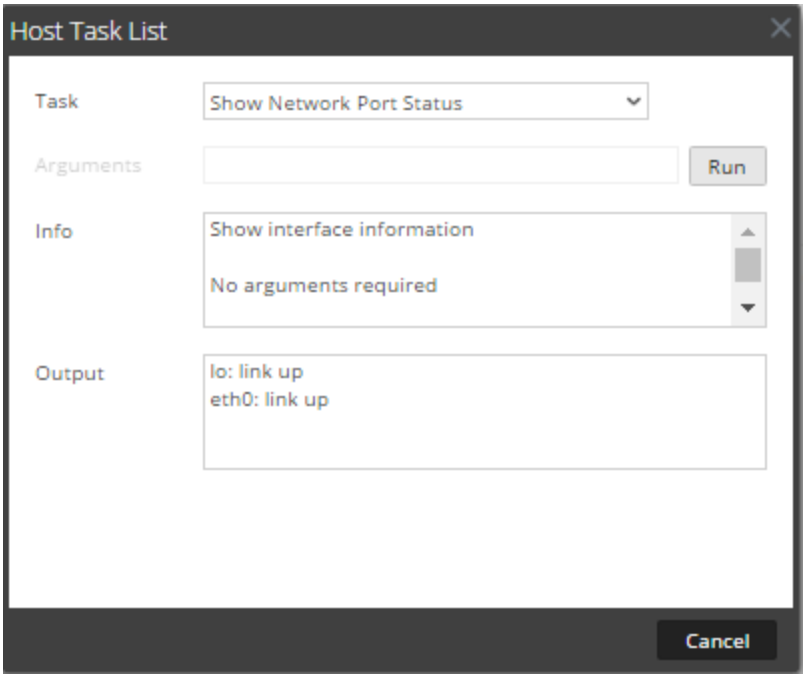
Mostrar estado de puerto de red

La tarea Mostrar estado de puerto de red en la Lista de tareas del host presenta el estado de todos los puertos configurados en el host.

Ver el estado de puerto de red

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y elija  **> Ver> Sistema**.
   Se muestra la vista Sistema del servicio seleccionado.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas** del host**, haga clic en** Mostrar estado de puerto de red
   .La tarea se muestra en el campo **Tarea** y la información acerca de la tarea, en el área **Información**.

5. Para ejecutar la tarea, haga clic en **Ejecutar**.
   El estado de cada puerto en el host se muestra en el área **Salida**.



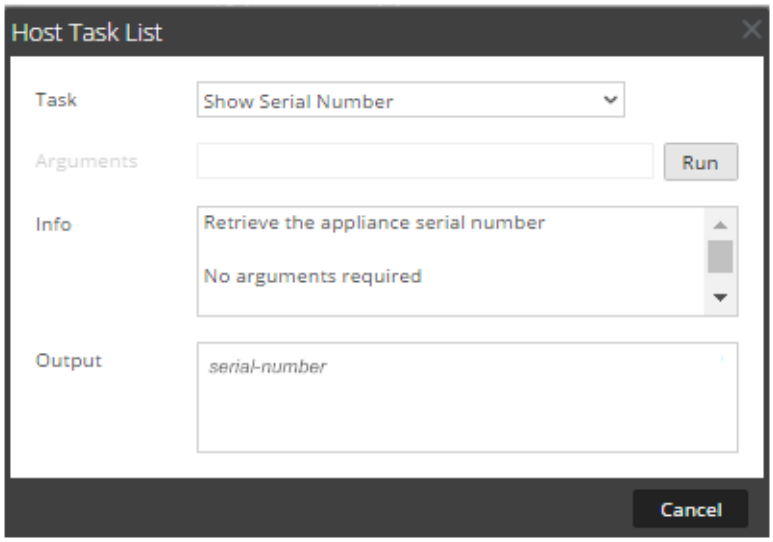
Mostrar número de serie

La tarea Mostrar número de serie de la Lista de tareas del host permite obtener el número de serie de un host.

Mostrar el número de serie

1. Seleccione **ADMIN > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en > **Ver**> **Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas** del host**, seleccione** Mostrar número de serie
   .En el área **Información**, se muestra una breve explicación de la tarea y sus argumentos.

5. No se requieren argumentos para esta tarea. Haga clic en **Ejecutar**.
   El número de serie del host seleccionado se muestra en el área **Salida**.



Apagar host

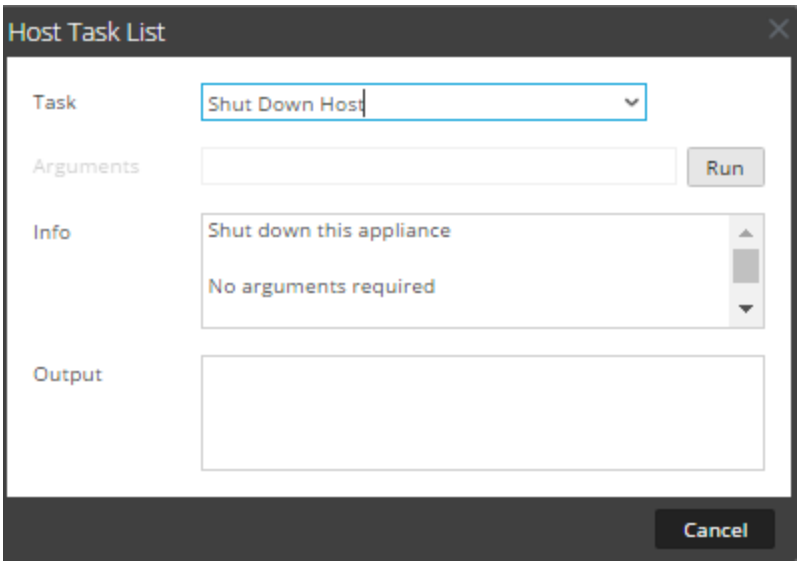
En algunas circunstancias, como una actualización de hardware o una interrupción prolongada de la alimentación que supera la capacidad de alimentación de respaldo, puede ser necesario apagar un host físico. Cuando apaga un host, se detienen todos los servicios que se ejecutan en él y se apaga el host físico.

El host físico no se reinicia automáticamente; se debe reiniciar mediante el switch de encendido. Una vez que se reinicia el host físico, el host y los servicios están configurados para reiniciarse automáticamente.

Reiniciar un host para iniciar y detener un host sin apagarlo.

Apagar el host

1. En el cuadro de diálogo Lista de tareas del host, seleccione **Apagar host** en el campo **Tarea**.



2. Para ejecutar la tarea, haga clic en **Ejecutar**.
   El host se apaga.

Detener e iniciar un servicio en un host

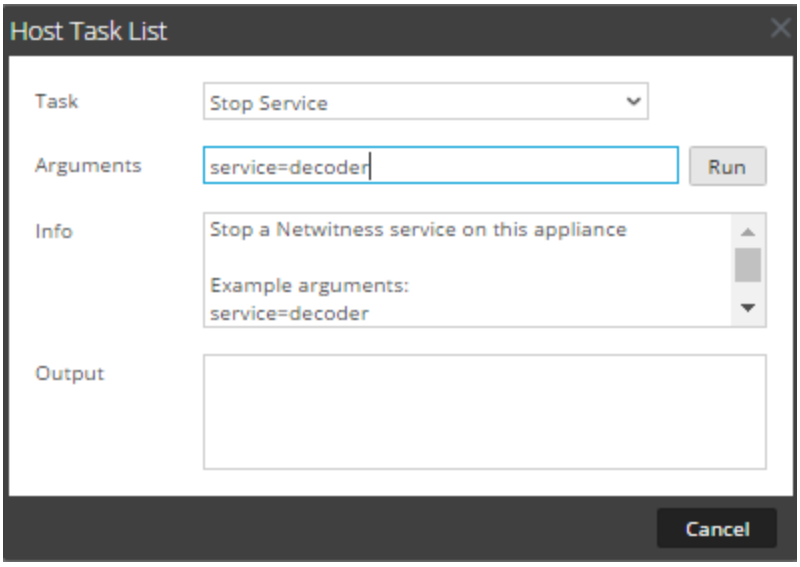
La Lista de tareas del host tiene dos opciones para detener e iniciar un servicio en un host. Cuando detiene un servicio con el mensaje **Detener servicio**, todos los procesos del servicio se detienen y se desconecta a los usuarios conectados al servicio. A menos que haya un problema con el servicio, este se reinicia automáticamente. Es igual que la opción **Apagar servicio** en la vista Sistema de servicios.

Si un servicio no se reinicia automáticamente después de detenerse, puede reiniciarlo manualmente con el mensaje **Iniciar servicio**.

Detener un servicio en un host

1. Seleccione **ADMIN** > **Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio y haga clic en > **Ver**> **Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
4. En la **Lista de tareas del host**, haga clic en **Detener servicio**.
   La tarea se muestra en el campo **Tarea** y la información acerca de la tarea, en el área **Información**.

5. Especifique el servicio (decoder, concentrator, broker, logdecoder o logcollector) que se detendrá en el campo **Argumentos**; por ejemplo, **service=decoder**.

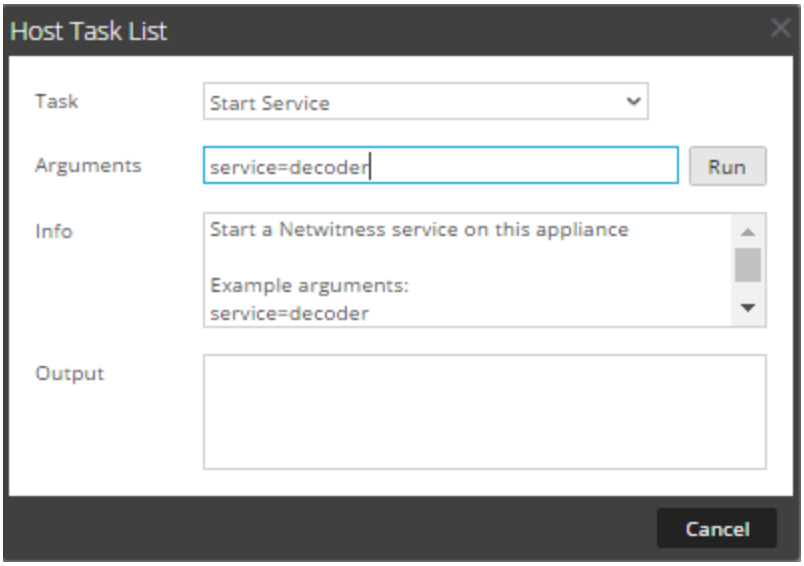


6. Para ejecutar la tarea, haga clic en **Ejecutar**.
   El servicio se detiene y el estado aparece en el área **Salida**. Todos los procesos del servicio se detienen y se desconecta a todos los usuarios conectados a él. A menos que haya un problema con el servicio, este se reinicia automáticamente.

Iniciar un servicio en un host

1. En la **Lista de tareas del host**, seleccione **Iniciar servicio** en el menú desplegable Tarea. La tarea se muestra en el campo **Tarea** y la información acerca de la tarea, en el área **Información**.
2. Especifique el servicio (decoder, concentrator, broker, logdecoder o logcollector) que se iniciará en el campo **Argumentos**; por ejemplo,

service=decoder



3. Para ejecutar la tarea, haga clic en **Ejecutar**.
   El servicio se inicia y el estado aparece en el área **Resultado**.

Agregar, replicar o eliminar un usuario de servicio

Debe agregar un usuario a un servicio para:

- Agregación
- Acceso al servicio con:
  - Cliente grueso
  - API REST

Nota: Este tema no se aplica a usuarios que acceden a servicios mediante la interfaz del usuario en el Servidor de NetWitness. Debe agregar estos usuarios al sistema, no a un servicio. Para obtener detalles, consulte el tema **Configurar un usuario** en *Administración de usuarios y de la seguridad del sistema.*

Para cada usuario de servicio, puede:

- Configurar la autenticación de usuario y las propiedades de manejo de consultas para el servicio
- Hacer al usuario miembro de una función, la que tiene un conjunto de permisos que recibe el usuario

- Replicar la cuenta de usuario en otros servicios
- Cambiar la contraseña del usuario en los servicios seleccionados

En Cambiar una contraseña de usuario de servicio se proporcionan instrucciones para cambiar la contraseña del usuario en varios servicios.

Consideraciones de replicación y migración

Cuando se replica un usuario desde un servicio NetWitness Suite 10.5 o superior a un servicio NetWitness Suite 10.4, Tiempo de espera agotado de consulta migra a Nivel de consulta en función del nivel más cercano. Por ejemplo, si un usuario tiene un tiempo de espera agotado de consulta de 15 minutos, este recibe un nivel de consulta de 3 después de la migración. Si un usuario tiene un tiempo de espera agotado de consulta de 35 minutos, este recibe un nivel de consulta de 2 después de la migración. Si un usuario tiene un tiempo de espera agotado de consulta de 45 minutos, este recibe un nivel de consulta de 2 después de la migración.

Cuando un usuario se migra o se replica desde un servicio de NetWitness Suite 10.4 a un servicio de NetWitness Suite 10.5 o superior, el Nivel de consulta migra a Tiempo de espera agotado de consulta en función de las siguientes definiciones:

- Nivel de consulta 1 = 60 minutos
- Nivel de consulta 2 = 40 minutos
- Nivel de consulta 3 = 20 minutos

Procedimientos

ACCEDER A LA VISTA SEGURIDAD

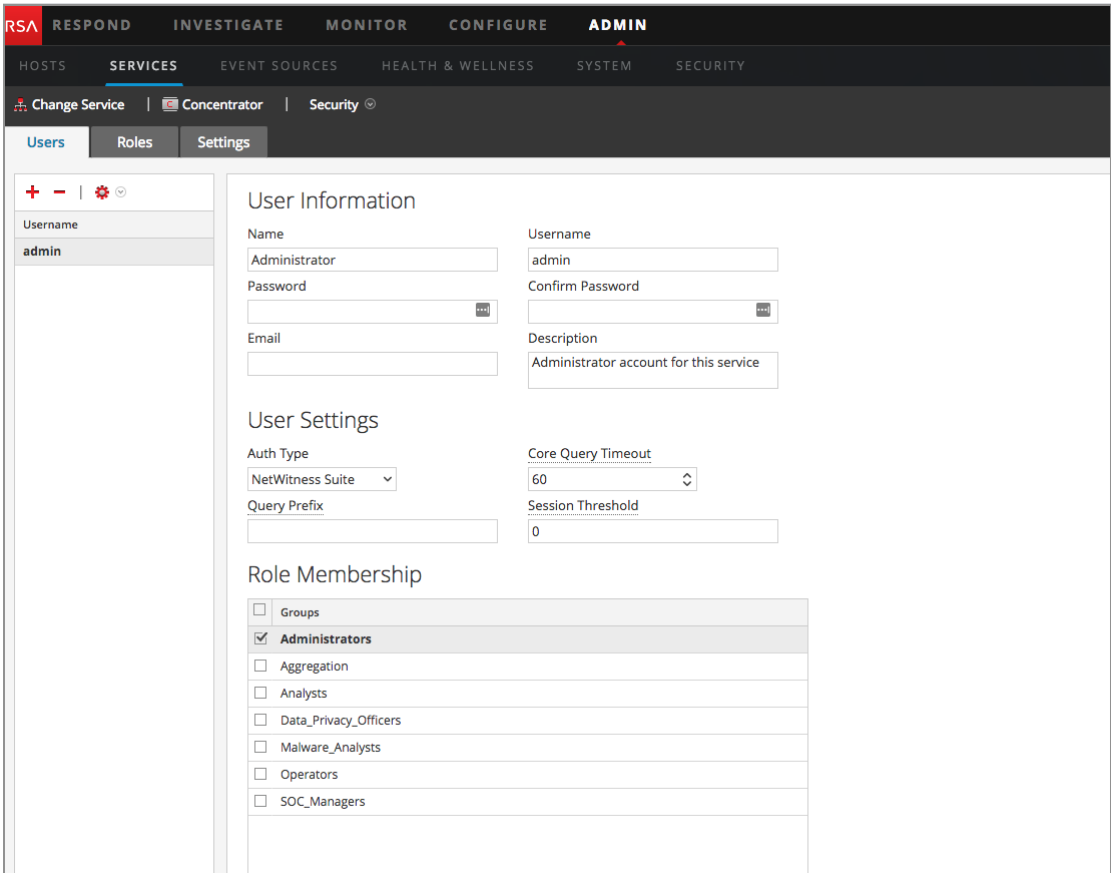
Cada uno de los siguientes procedimientos comienza en la vista Seguridad de servicios.

Para navegar a la vista Seguridad de servicios:

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.

2. Seleccione un servicio y haga clic en  > **Ver** > **Seguridad**.

   La vista Seguridad del servicio seleccionado se muestra con la pestaña Usuarios abierta.



Nota: En el servicio de NetWitness Suite versión 10.4 y anteriores, en la sección Configuración de usuario, se muestra el campo **Nivel de consulta** en lugar de **Tiempo de espera agotado de consulta de Core**.

AGREGAR UN USUARIO DE SERVICIO

1. En la pestaña **Usuarios**, haga clic en +.
2. Escriba el nombre de usuario para acceder al servicio y, a continuación, presione **Intro**.
   La sección Información del usuario muestra el nombre de usuario y el resto de los campos están disponibles para su edición.
3. Escriba la contraseña para iniciar sesión en el servicio en los campos **Contraseña** y **Confirmar contraseña**.
4. (Opcional) Proporcione información adicional:

- **Nombre** para iniciar sesión en NetWitness Suite
- Dirección de **Correo electrónico**
- **Descripción** del usuario

5. En la sección Configuración de usuario, seleccione la siguiente información:
   - **Tipo de autenticación**
     - Si NetWitness Suite autentica al usuario, seleccione NetWitness.
     - Si Active Directory o PAM están configurados en el Servidor de NetWitness para autenticar al usuario, seleccione Externo.

Nota: En 10.4 y superior, las conexiones de confianza hacen que no sea necesario configurar cuentas de usuario externas en el servicio. Toda configuración externa se centraliza en el Servidor de NetWitness.

   - **Tiempo de espera agotado de consulta de Core** es la cantidad máxima de minutos que un usuario puede ejecutar una consulta en el servicio. Este campo se aplica al servicio de NetWitness Suite versión 10.5 y superiores y no aparece para la versión 10.4 y anteriores.

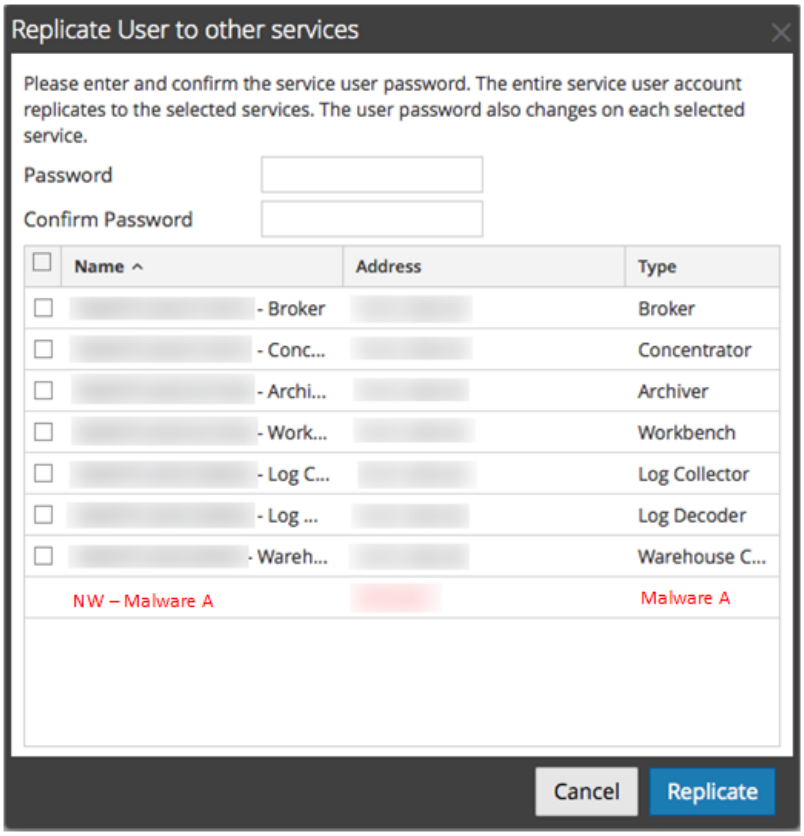
6. (Opcional) Especifique criterios adicionales de consulta:
   - **Prefijo de consulta** filtra las consultas. Escriba un prefijo para restringir los resultados que ve el usuario.
   - **Umbral de sesión** controla la forma en que el servicio escanea los valores de metadatos para determinar los conteos de sesiones. Cualquier valor de metadatos con un conteo de sesiones que está por sobre el umbral detiene su determinación del conteo de sesiones verdadero.

7. En la sección **Membresía en función**, seleccione cada función para asignar al usuario. Cuando un usuario es un miembro de una función en un servicio, el usuario tiene los permisos asignados a la función.
8. Para activar el nuevo usuario de servicio, haga clic en **Aplicar**.

Se agrega el usuario al servicio inmediatamente.

REPLICAR UN USUARIO EN OTROS SERVICIOS

1. En la pestaña Usuarios, seleccione un usuario y haga clic en  > **Replicar**.
   Se muestra el cuadro de diálogo Replicar usuarios a otros servicios.



2. Escriba y confirme la **contraseña** del usuario.
3. Seleccione cada servicio para los que está replicando el usuario.
4. Haga clic en **Replicar**.

Se agrega la cuenta de usuario a cada servicio seleccionado.

ELIMINAR UN USUARIO DE SERVICIO

1. En la pestaña **Usuarios**, seleccione el **Nombre de usuario** y haga clic en .
   NetWitness Suite solicita confirmar la intención de eliminar al usuario seleccionado.
2. Para confirmar, haga clic en **Sí**.

Se elimina el usuario del servicio inmediatamente.

Agregar una función de usuario de servicio

Existen funciones preconfiguradas en NetWitness Suite que están instaladas en el servidor y en cada servicio. También puede agregar funciones personalizadas. En la siguiente tabla se enumeran las funciones preconfiguradas del sistema y sus permisos.

Función	Permiso
Administradores	Acceso completo al sistema
Operadores	Acceso a configuraciones, pero no a metadatos ni a contenido de sesiones
Analistas	Acceso a metadatos y contenido de sesiones, pero no a configuraciones
SOC_Managers	El mismo acceso que poseen los analistas, además del permiso adicional para manejar incidentes
Malware_ Analysts	Acceso a eventos de malware y a metadatos y contenido de sesiones
Data_Privacy_ Officers	Acceso a metadatos y contenido de sesiones, así como a opciones de configuración que administran el ocultamiento y la visualización de datos confidenciales en el sistema (consulte Administración de la privacidad de datos).

Debe agregar una función de servicio cuando ha agregado:

- Un usuario o usuarios de **servicio** que requieren un nuevo conjunto de permisos.
- Una **función personalizada en el Servidor de NetWitness**, ya que las conexiones de confianza requieren que exista la misma función personalizada en el servidor y en cada servicio al que accederá la función personalizada. Los nombres deben ser idénticos. Por ejemplo, si agrega una función Junior Analysts en el servidor, debe agregar una función Junior Analysts en cada servicio al cual accederá la función. Para obtener más información, consulte el tema **Agregar una función y asignar permisos** en *Administración de usuarios y de la seguridad del sistema*.

También hay una función de servicio **Agregación** preconfigurada. En Función Agregación y Funciones y permisos de los usuarios de servicios se proporciona información adicional.

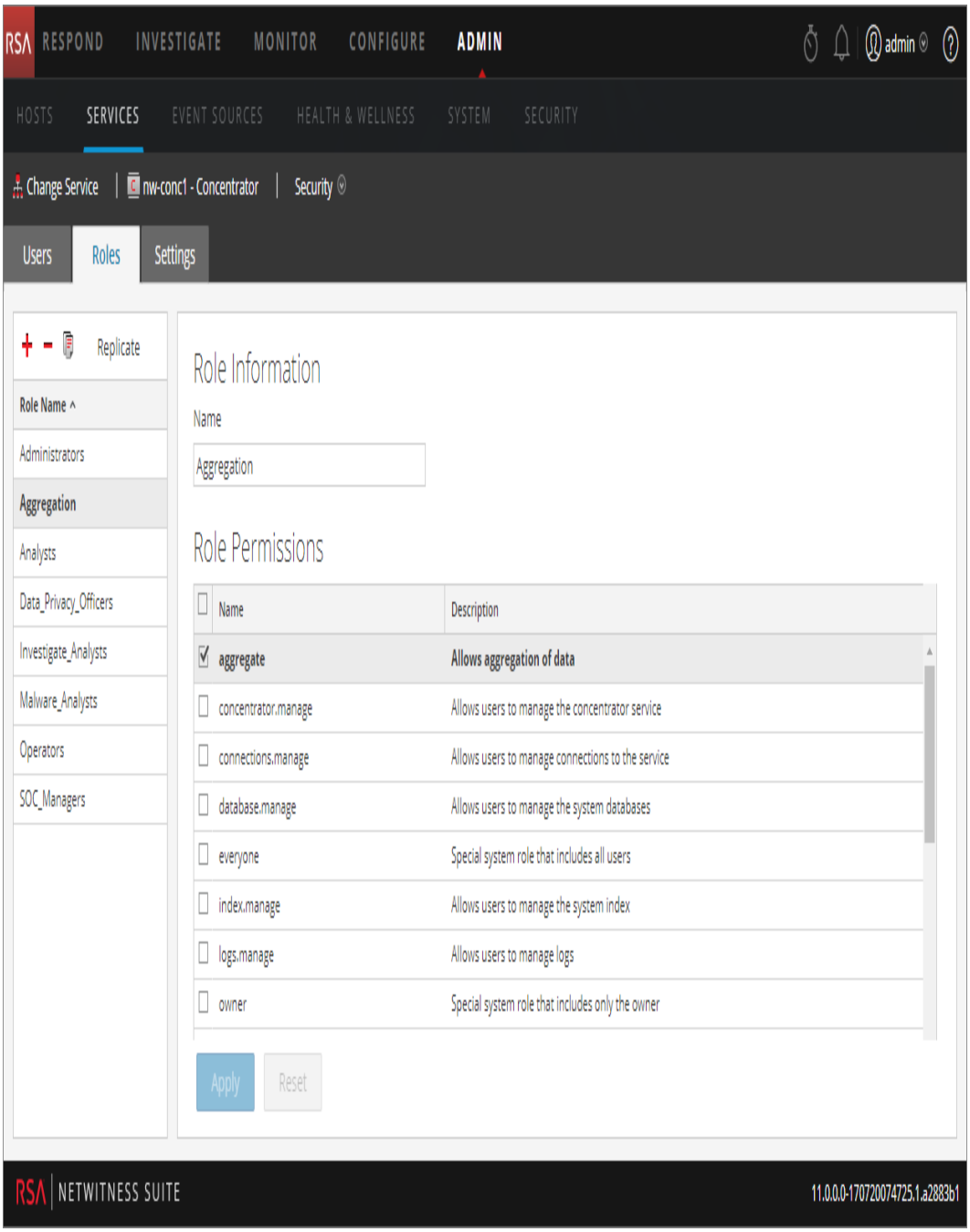
Procedimiento

Para agregar una función de usuario de servicio y asignarle permisos:

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y elija  **> Ver > Seguridad**.
   La vista Seguridad del servicio seleccionado se muestra con la pestaña Usuarios abierta.

3. Seleccione la pestaña **Funciones** y haga clic en +.

   La vista Seguridad de servicios se muestra con cinco funciones preconfiguradas que ya están enumeradas.



4. Haga clic en +, escriba el **Nombre de la función** y presione **Intro**.

   El Nombre de la función se muestra sobre una lista de **Permisos de función**.

5. Seleccione cada permiso que tendrá la función en el servicio.

6. Haga clic en **Aplicar**.

La función se agrega inmediatamente al servicio. Puede agregar usuarios de servicio en la pestaña **Usuarios**.

Cambiar una contraseña de usuario de servicio

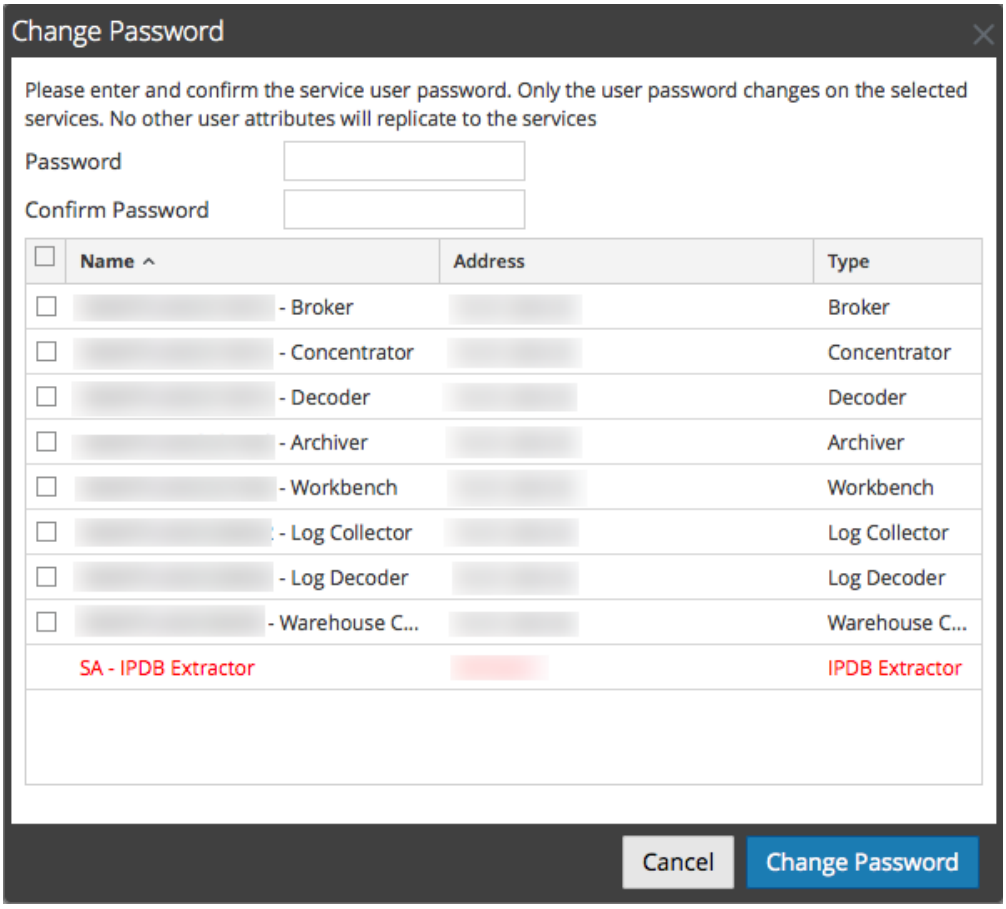
Este procedimiento permite que los administradores cambien la contraseña de un usuario de servicios y que repliquen la contraseña nueva a todos los servicios principales en los cuales está definida esa cuenta de usuario. Solo el cambio de contraseña se replica a los servicios principales seleccionados y no la cuenta de usuario completa. Los administradores también pueden cambiar la contraseña de la cuenta de **administrador** en los servicios principales.

Nota: la opción Cambiar contraseña no se aplica a los usuarios externos.

Para cambiar la contraseña de un usuario de servicios:

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione un servicio y haga clic en  **> Ver > Seguridad**.
   Se muestra la vista Seguridad para los servicios seleccionados.
3. En la pestaña **Usuarios**, seleccione un usuario y elija **Cambiar contraseña** en el ícono de acciones.

Se muestra el cuadro de diálogo **Cambiar contraseña**.



4. Escriba la contraseña nueva del usuario y confírmela.
5. Seleccione los servicios en los cuales desea cambiar la contraseña del usuario.
6. Haga clic en **Cambiar contraseña**.
   Se muestra el estado del cambio de contraseña en los servicios seleccionados.

Crear y administrar grupos de servicios

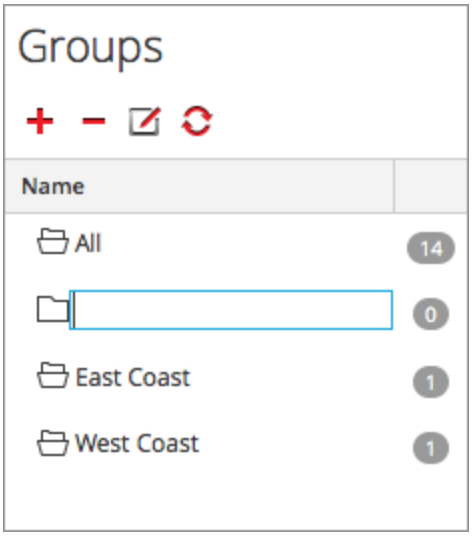
La vista Servicios de Administration proporciona opciones para crear y administrar grupos de servicios. La barra de herramientas de panel Servicios incluye opciones para crear, editar y eliminar grupos de servicios. Una vez que se crean los grupos, puede arrastrar servicios individuales desde el panel Servicios a un grupo.

Los grupos pueden reflejar un principio funcional, geográfico, orientado a un proyecto o cualquier principio de la organización que sea útil. Un servicio puede pertenecer a más de un grupo. Aquí hay algunos ejemplos de posibles agrupamientos.

- Agrupe diferentes tipos de servicios para facilitar la configuración y el monitoreo de todos los Brokers, Decoders o Concentrators.
- Agrupe servicios que sean parte del mismo flujo de datos; por ejemplo, un Broker y todos los Concentrators y Decoder asociados.
- Agrupe servicios según su región y ubicación geográfica dentro de la región. Si ocurre una interrupción de energía importante en una ubicación, los servicios posiblemente afectados son fácilmente identificables.

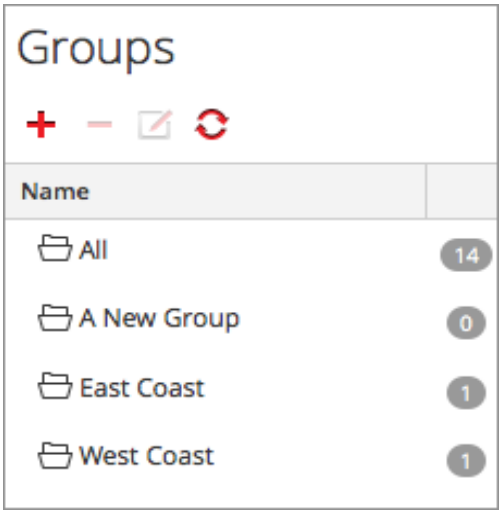
Crear un grupo

1. En NetWitness Suite, vaya a **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios de Administration.
2. En la barra de herramientas del panel **Grupos**, haga clic en +.
   Se abre un campo para el grupo nuevo con un cursor parpadeante.



3. Escriba el nombre del grupo nuevo en el campo (por ejemplo, **Un grupo nuevo**) y presione **Intro**.
   El grupo se crea como una carpeta en el árbol. El número junto al grupo indica la cantidad

de servicios en ese grupo.



Cambiar el nombre de un grupo

1. En el panel **Grupos** de la vista **Servicios**, haga doble clic en el nombre de grupo o seleccione el grupo y haga clic en . El campo de nombre se abre con un cursor parpadeante.
2. Escriba el nuevo nombre del grupo y presione **Intro**.
   El campo de nombre se cierra y el nuevo nombre del grupo se muestra en el árbol.

Agregar un servicio a un grupo

En el panel **Servicios** de la vista Servicios, seleccione un servicio y arrástrelo a una carpeta de grupo en el panel de grupos; por ejemplo, **Log Collectors**.
El servicio se agrega al grupo.

Ver los servicios en un grupo

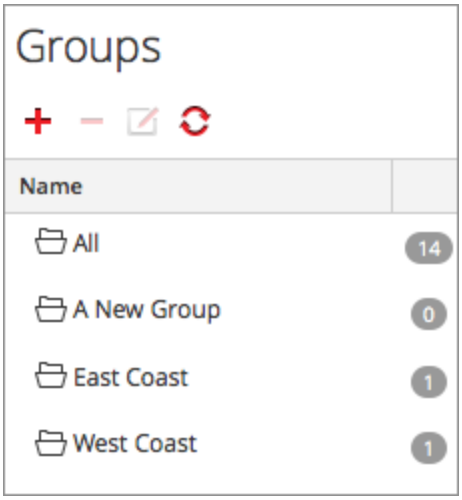
Para ver los servicios en un grupo, haga clic en el grupo en el panel **Grupos**.

El panel **Servicios** indica los servicios en ese grupo.

Eliminar un servicio de un grupo

1. En el **panel Grupos** de la vista Servicios, seleccione el grupo que contiene el servicio que desea eliminar. Los servicios de ese grupo aparecen en el panel Servicios.
2. En el panel **Servicios**, seleccione uno o más servicios que desee quitar del grupo y, en la barra de herramientas, seleccione > **Eliminar de grupo**.
   Los servicios seleccionados se quitan del grupo, pero no se quitan de la interfaz del usuario

de NetWitness Suite. La cantidad de servicios en el grupo, que se indica cerca del nombre del grupo, disminuye según la cantidad de servicios eliminados de un grupo. El grupo **Todo** contiene los servicios que se quitaron del grupo.
En el siguiente ejemplo, el grupo de servicios llamado **Un grupo nuevo** no contiene ningún servicio, ya que se quitó el servicio en ese grupo.



Eliminar un grupo

1. En el **panel Grupos** de la vista Servicios, seleccione el grupo que desea eliminar.
2. Haga clic en .
   El grupo seleccionado se quita del panel Grupos. Los servicios que estaban en el grupo no se quitan de la interfaz del usuario de NetWitness Suite. El grupo **Todo** contiene los servicios del grupo eliminado.

Duplicar o replicar una función de servicio

Una forma eficiente de agregar una nueva función de servicio es duplicar una función similar, guardarla con un nuevo nombre y revisar los permisos que ya están asignados. Por ejemplo, podría duplicar la función Analistas. Después, puede guardarla como **JuniorAnalysts** y modificar los permisos.

La forma rápida de agregar una función existente a otros servicios es replicar la función. Por ejemplo, podría replicar la función **JuniorAnalysts** que existe en un Broker a un Concentrator y un Log Decoder.

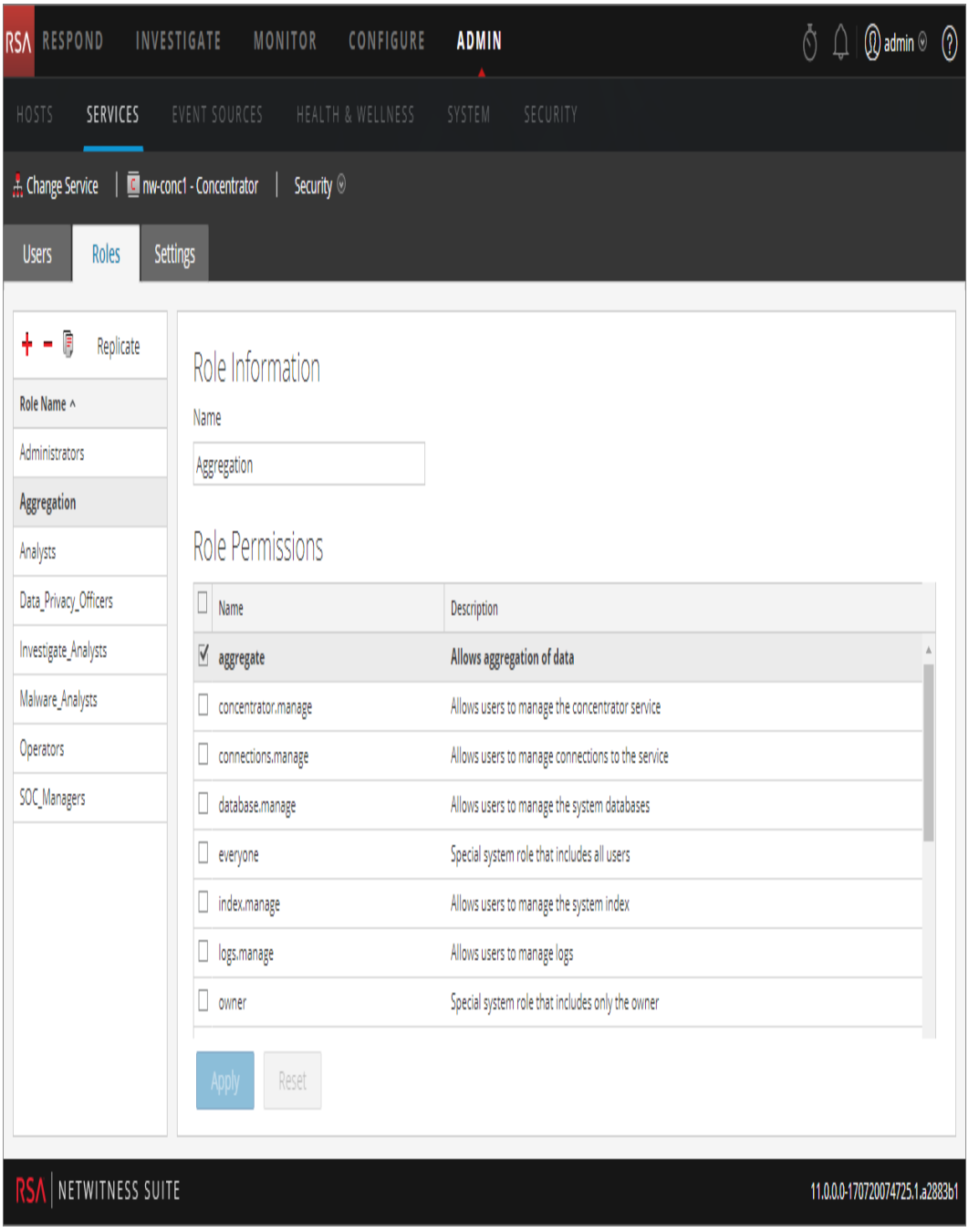
Cada uno de los siguientes procedimientos comienza en la vista Seguridad de servicios.

Para navegar a la vista Seguridad de servicios:

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y haga clic en  **> Ver > Seguridad**.
   La vista Seguridad del servicio seleccionado se muestra con la pestaña Usuarios abierta.
3. Seleccione la pestaña **Funciones**.

Duplicar una función de servicio

1. En la pestaña Funciones, seleccione la función que desea duplicar.



2. Haga clic en **Duplicar función.**
3. Escriba un nombre nuevo y haga clic en **Aplicar**.
4. Seleccione la nueva función.

5. En la sección **Permisos de función**, seleccione o deseleccione permisos para modificar lo que puede hacer la nueva función.

La función duplicada se agrega de inmediato al servicio.

Replicar una función

1. En la pestaña **Funciones**, seleccione la función que desea replicar y haga clic en **Replicar**.
2. En el cuadro de diálogo **Replicar función a otros servicios**, seleccione cada servicio en el cual desea agregar la función.
3. Haga clic en **Replicar**.

La función replicada se agrega de inmediato a cada servicio seleccionado.

Editar los archivos de configuración de servicios principales

Los archivos de configuración de los servicios Decoder, Log Decoder, Broker, Concentrator, Archiver y Workbench se pueden editar como archivos de texto. La vista Configuración de servicios > pestaña Archivos permite:

- Ver y editar un archivo de configuración de servicio que el sistema NetWitness Suite utiliza actualmente.
- Recuperar y restaurar el respaldo más reciente del archivo que está editando.
- Migrar el archivo abierto a otros servicios.
- Guardar cambios realizados en un archivo.

Los archivos disponibles para editar varían según el tipo de servicio que se configura. Los archivos comunes a todos los servicios Core son:

- El archivo del índice del servicio.
- El archivo de netwitness.
- El archivo del generador de informes de fallas.
- El archivo del programador.

Además, el Decoder tiene archivos que configuran los analizadores, las definiciones de feed y un adaptador de LAN inalámbrica.

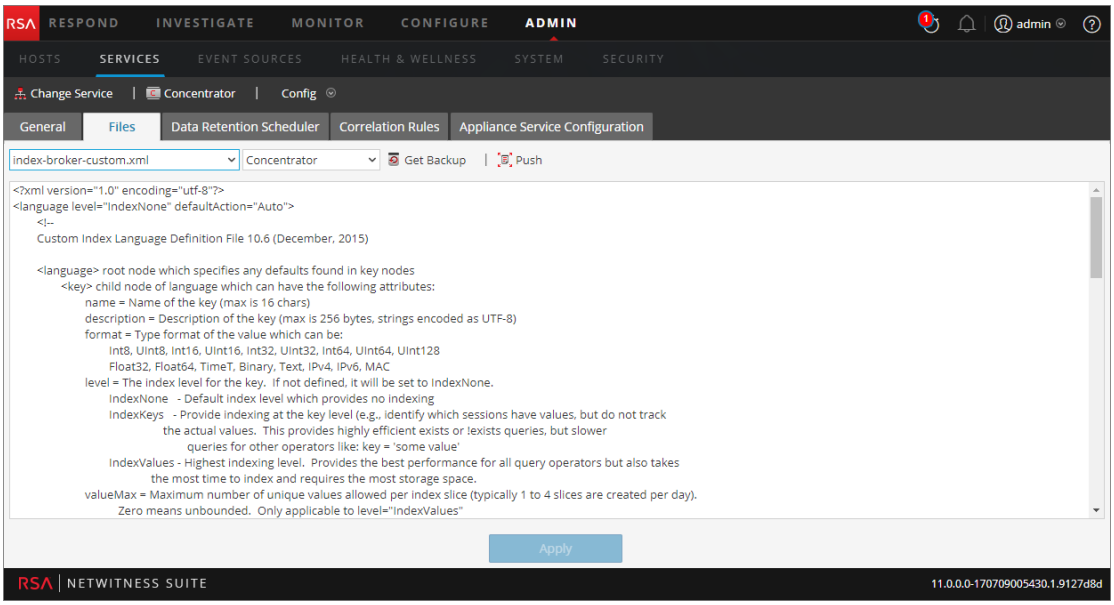
Nota: Los valores predeterminados en estos archivos de configuración son, por lo general, aptos para las situaciones más comunes. Sin embargo, es necesario realizar tareas de edición para los servicios opcionales, como el generador de informes de fallas generales o el programador. Solo los administradores que comprenden ampliamente las redes y los factores que afectan la forma en que los servicios recopilan y analizan datos deben realizar cambios en estos archivos en la pestaña Archivos.

Para obtener más detalles sobre los parámetros de configuración de servicios, consulte Ajustes de configuración de servicios.

Editar el archivo de configuración de un servicio

Para editar un archivo:

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
2. En la cuadrícula Servicios, seleccione un servicio.
3. Seleccione  **> Ver > Configuración**.
   La vista Configuración de servicios se muestra con la pestaña General abierta.
4. Haga clic en la pestaña **Archivos**.
   El servicio seleccionado, como Concentrator, aparece en la lista desplegable de la derecha.
5. (Opcional) Para editar un archivo para el host en lugar del servicio, seleccione **Host** en la lista desplegable.
6. Elija un archivo en la lista desplegable **Seleccione un archivo a editar**.
   El contenido del archivo se muestra en modo de edición.



7. Edite el archivo y haga clic en **Aplicar**.

El archivo actual se sobrescribe y se crea un archivo de respaldo. Los cambios se aplican tras el reinicio del servicio.

Revertir a una versión de respaldo de un archivo de configuración de servicio

Después de hacer cambios en un archivo de configuración, guarde el archivo y reinicie el servicio, un archivo de respaldo está disponible. Para revertir a un respaldo de un archivo de configuración:

1. Seleccione un archivo de configuración, para lo cual debe realizar los pasos del 1 al 6 del procedimiento **Editar el archivo de configuración de un servicio** al principio de este tema.
2. Haga clic en Get Backup.

   El archivo de respaldo se abre en el editor de texto.
3. Para revertir a la versión de respaldo, haga clic en **Guardar**.

Los cambios se aplican tras el reinicio del servicio.

Migrar un archivo de configuración a otros servicios

Después de editar un archivo de configuración de servicio, puede migrar la misma configuración a otros servicios del mismo tipo.

1. Seleccione un archivo de configuración, para lo cual debe realizar los pasos del 1 al 6 del procedimiento **Editar el archivo de configuración de un servicio** al principio de este tema.

2. Haga clic en 

. Se muestra el cuadro de diálogo Seleccionar servicios.
3. Seleccione cada servicio para migrar a estos el archivo de configuración.
   Cada servicio debe ser del mismo tipo que el que seleccionó en la vista Servicios.

   Precaución: si decide no migrar el archivo de configuración, haga clic en **Cancelar**.
4. Para migrar el archivo de configuración a todos los servicios seleccionados, haga clic en **Aceptar**.

El archivo se migra a todos los servicios seleccionados.

CONFIGURAR EL PROGRAMADOR DE TAREAS

Archivo del programador

Puede editar el archivo del **programador** en la vista Configuración de servicios > pestaña Archivos. Este archivo configura el programador de tarea incorporado de un servicio. El programador de tareas puede enviar mensajes automáticamente a intervalos predefinidos o en momentos específicos del día.

Sintaxis de tareas de programador

Una línea de tarea en el archivo de programador contiene la siguiente sintaxis, donde no tiene espacios:

```
<ParamName>=<Value>
```

si **<Value>** tiene espacios, esta es la sintaxis:

```
<ParamName>="<Value>"
```

En cada línea de tarea, se aplican estas reglas:

- Se requiere el parámetro **tiempo** o uno de los parámetros de intervalo (**segundos**, **minutos** u **horas**).
- En los caracteres especiales se debe usar el carácter de escape \ (barra invertida).

Parámetros de línea de tarea

El programador acepta los siguientes parámetros de línea de tarea.

Sintaxis	Descripción
daysOfWeek: <string, optional, {enum-any:sun|mon|tue|wed|thu|fri|sat|all}>	Los días de la semana para ejecutar una tarea. El valor predeterminado es **all**.

Sintaxis	Descripción
deleteOnFinish: <bool, optional>	Eliminar la tarea cuando haya finalizado correctamente.
hours: <uint32, optional, {range:1 to 8760}>	La cantidad de horas entre ejecuciones.
logOutput: <string, optional>	Generar la respuesta en el registro con el uso del nombre de módulo especificado.
minutes: <uint32, optional, {range:1 to 525948}>	La cantidad de minutos entre ejecuciones.
msg: <string>	El mensaje para enviar el nodo.
params: <string, optional>	Los parámetros para el mensaje.
pathname: <string>	La ruta del nodo que recibe el mensaje.
seconds: <uint32, optional, {range:1 to 31556926}>	El número de segundos entre ejecuciones.
time: <string>	La hora de ejecución en formato HH::MM:SS (hora local de este servidor).
timesToRun: <uint32, optional>	Cuántas veces se ejecuta desde el inicio del servicio; el valor **0** indica que no hay límite (valor predeterminado).

Mensajes

Las siguientes son las cadenas de mensaje que se utilizan en el parámetro **msg** del programador de tareas.

Mensaje	Descripción
addInter	Agrega una tarea para ejecutarse en un intervalo definido. Por ejemplo, este mensaje ejecuta el comando **/index save** cada 6 horas: addInter hours=6 pathname=/index msg=save
addMil	Agrega una tarea que se ejecutará en un momento específico del día o incluso durante los días de la semana. Por ejemplo, este mensaje ejecuta el comando **/index save** a la 01:00 h cada día laborable: addMil time= 01:00:00 pathname=/index msg=save daysOfWeek=mon,tue,wed,thu,fri
delSched	Elimina una tarea programada existente. El parámetro **id** de la tarea debe recuperarse del mensaje de impresión.
print	Imprime todas las tareas programadas.
replace	Asigna todas las tareas programadas en un mensaje, eliminando cualquier tarea existente.
save	Le indica a un nodo que guarde

Ejemplo de línea de tarea

El siguiente ejemplo de línea de tarea en el archivo de programador descarga el archivo de paquetes de feeds (**feeds.zip**) al Decoder seleccionado cada 120 minutos desde el servidor de host de feeds:

```
minutes=120 pathname=/parsers msg=feed params="type\=wget
file\=http://feedshost/nwlive/feeds.zip"
```

EDITAR UN ARCHIVO DE ÍNDICE DE SERVICIOS

En este tema se proporciona información y reglas importantes para configurar archivos de índice personalizados de servicios, los cuales se pueden editar en la vista Configuración del servicio > pestaña Archivos.

El archivo de índice, junto con otros archivos de configuración, controla la operación de cada servicio principal. El acceso al archivo de índice a través de la vista Configuración de servicios en NetWitness Suite abre el archivo en un editor de texto, donde puede editarlo.

Nota: Solo los administradores con un conocimiento integral y completo de la configuración del servicio principal cumplen los requisitos para realizar cambios en un archivo de índice, que es uno de los archivos de configuración principales para el servicio del dispositivo. Los cambios que se hacen deben ser coherentes en todos los servicios principales. Las entradas no válidas o un archivo configurado erróneamente pueden impedir que se inicie el sistema y es posible que requiera la ayuda de RSA Support para lograr que el sistema vuelva a un estado funcional.

Estos son los archivos de índice:

- `index-broker.xml` y `index-brokercustom.xml`
- `index-concentrator.xml` y `index-concentratorcustom.xml`
- `index-decoder.xml` y `index-decodercustom.xml`
- `index-logdecoder.xml` y `index-logdecodercustom.xml`
- `index-archiver.xml` y `index-archivercustom.xml`
- `index-workbench.xml` y `index-workbenchcustom.xml`

Archivos de índice y archivos de índice personalizados

Todos los cambios de índice específicos del cliente se realizan en**`index-<service>-custom.xml`**. Este archivo reemplaza cualquier ajuste en `index-<service>.xml`, el cual está bajo el control exclusivo de RSA.

Nota: Los clientes que usaban versiones de NetWitness Suite anteriores a 10.1 tenían que personalizar los archivos de índice mediante su edición y guardado, y este método dependía de que NetWitness Suite creara un respaldo del archivo de índice actual después del reinicio del servicio. Utilizando este proceso, se sobrescribe el archivo actual y se crea un archivo de respaldo. La opción de la barra de herramientas proporciona una manera de revertir a una versión de respaldo del archivo de índice.
Durante las actualizaciones de software, el archivo `index-<service>.xml` no se conserva, ya que se sobrescribe con los cambios que hace el equipo de contenido de RSA. Sin embargo, se crea un respaldo en el mismo directorio, el cual se denomina `index-<service>.xml.rpm_pre_save`. Si es necesario, se puede hacer referencia al archivo `index-<service>.xml.rpm_pre_save` para crear el archivo **`index-<service>-custom.xml`** específico del cliente, lo cual solo es necesario hacer una vez. A partir de ahí, el nuevo sistema permite a RSA realizar cambios de índice sin modificar los cambios específicos existentes del cliente.

El archivo de índice personalizado, **`index-<service>-custom.xml`**, permite crear definiciones personalizadas o reemplazos de sus propias claves de idioma que no se sobrescriben durante el proceso de actualización.

- Las claves que se definen en `index-<service>-custom.xml` reemplazan a las definiciones que se encuentran en `index-<service>.xml`.
- Las claves que se agregan a `index-<service>custom.xml` y que no se encuentran en `index <service>.xml` se agregan al idioma como una clave nueva.

Algunas aplicaciones comunes para editar el archivo de índice son:

- Agregar las nuevas claves de metadatos personalizadas para agregar nuevos campos a la interfaz del usuario de NetWitness Suite.
- Configurar claves de metadatos protegidas como parte de una solución de privacidad de datos, como se describe en la guía *Administración de la privacidad de datos*.
- Ajustar el rendimiento de consultas de la base de datos de NetWitness Suite Core, como se describe en la *Guía de ajuste de la base de datos de NetWitness Suite Core*.

Nota: Para NetWitness Suite 10.1 y superior, no hay necesidad de editar el archivo de índice personalizado de Broker, con excepción de los escenarios de implementación de la privacidad de datos y las funciones del sistema. El Broker combina automáticamente las claves de todos los servicios agregados para crear un idioma integral. Se utiliza el idioma alternativo definido en `index-broker.xml` y **`indexbroker-custom.xml`** si no hay servicios o si todos los servicios están offline.

Precaución: Nunca configure el nivel de índice en `IndexKeys` o `IndexValues` en un Decoder si tiene un Concentrator o un Archiver que realizan agregación desde el Decoder. El tamaño de la partición del índice es demasiado pequeño para ofrecer compatibilidad con cualquier indexación más allá de la clave de metadatos `time` predeterminada.

HABILITAR EL SERVICIO DEL GENERADOR DE INFORMES DE FALLAS

El generador de informes de fallas es un servicio opcional para servicios de NetWitness Suite. Cuando se activa para cualquiera de los servicios principales, el generador de informes de fallas crea automáticamente un paquete de información que se utilizará para diagnosticar y solucionar el problema que causó la falla en el servicio. El paquete se envía automáticamente a RSA para el análisis. Los resultados se envían al servicio de soporte de RSA para cualquier acción adicional.

El paquete de información que se envía a RSA no contiene datos capturados. Este paquete consta de la siguiente información:

- Rastreo de paquete de discos
- Registros
- Ajustes de configuración

- Versión de software
- Información de CPU
- RPM instalados
- Geometría de discos

El análisis de fallas generales del generador de informes de fallas generales se puede activar para cualquier producto Core.

El archivo crashreporter.cfg

Uno de los archivos disponibles para edición en la vista Configuración de servicios > pestaña Archivos es **crashreporter.cfg**, el archivo de configuración del servidor de cliente del generador de informes de fallas.

El script que comprueba, actualiza y crea informes de fallas generales en el host utiliza este archivo. La lista de productos para monitorear puede incluir Decoders, Concentrators, hosts y Brokers.

En esta tabla se muestran las configuraciones para el archivo **crashreporter.cfg**.

Configuración	Descripción
applicationlist=decoder, concentrator, host	Definir la lista de productos para monitorear.
sitedir=/var/crashreporter	Ubicación del directorio de sitio para el informe.
webdir=/usr/share/crashreporter/Web	Ubicación del directorio web.
devdir=/var/crashreporter/Dev	Ubicación del directorio de desarrollo.
datadir=/var/crashreporter/data	Ubicación de los archivos de datos del almacenamiento de directorios.
perldir=/usr/share/crashreporter/perl	Ubicación de los archivos Perl.
bindir=/usr/share/crashreporter/bin	Ubicación de los archivos ejecutables binarios.

Configuración	Descripción
libdir=/usr/share/crashreporter/lib	Ubicación de las bibliotecas binarias.
cfgdir=/etc/crashreporter	Ubicación de los archivos de configuración.
logdir=/var/log/crashreporter	Ubicación de los archivos de registro.
scriptdir=/usr/share/crashreporter/scripts	Ubicación del directorio que contiene scripts.
workdir=/var/crashreporter/work	Ubicación del directorio de trabajo de procesos.
sqldir=/var/crashreporter/sql	Ubicación donde se sitúan los archivos SQL creados.
reportdir=/var/crashreporter/reports	Ubicación donde se crean los informes temporales.
packagedir=/var/crashreporter/packages	Ubicación de los archivos de paquete creados.
gdbconfig=/etc/crashreporter/crashreporter.gdb	Ubicación del archivo de configuración gdb.
corewaittime=30	Defina la cantidad de segundos que se deben esperar después de buscar un core para determinar si el core aún se está escribiendo.
cyclewaittime=10	Defina la cantidad de minutos que se deben esperar entre los ciclos de búsqueda.

Configuración	Descripción
deletecores=1	Especifique si los archivos principales se deben eliminar después del informe. 0 = No 1 = Sí **NOTA:** Hasta que se elimina, el archivo principal se informa cada vez que se reinicia el generador de informes de fallas.
deletereportdir=1	Especifique si el directorio de informes debe eliminarse después del informe. Útil para ver informes principales en el cuadro. 0 = No 1 = Sí **NOTA:** Si no se elimina, el directorio se incluirá en cada paquete subsiguiente.

Configuración	Descripción
debug=1	Especifique si los mensajes de depuración están activados o desactivados en la salida de registro del **generador de informes de fallas**. 0 = No 1 = Sí
posturl=https://www.netwitnesslive.com/crash…ter/submit.php	Defina la URL de publicación del servidor web.
postpackages=0	Especifique si los paquetes deben publicarse en el servidor web. 0 = No 1 = Sí
deletepackages=1	Especifique si los paquetes deben eliminarse después de publicarse en el servidor web. 0 = No 1 = Sí

Configurar el servicio del generador de informes de fallas.

Para configurar el servicio del generador de informes de fallas.

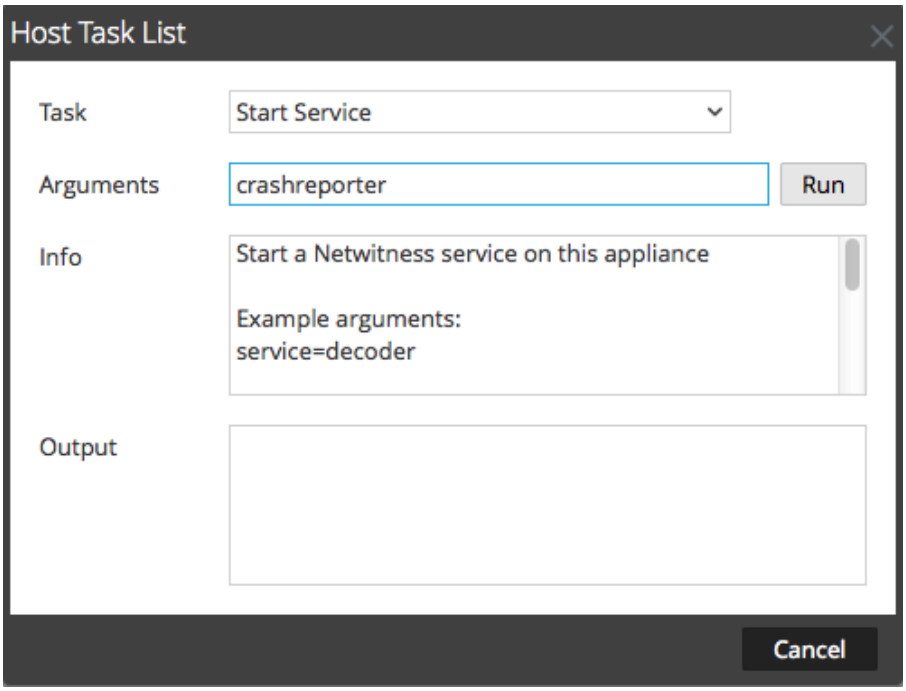
1. Seleccione **ADMIN > Servicios**.
2. Seleccione un servicio y haga clic en  **> Ver > Configuración**.

3. Seleccione la pestaña **Archivos**.
4. Edite **crashreporter.cfg**.
5. Haga clic en **Guardar**.
6. Para mostrar la vista Sistema de servicios, seleccione **Configurar > Sistema**.
7. Para reiniciar el servicio, haga clic en Shutdown Service.
   El servicio se apaga y se reinicia.

Iniciar y detener el servicio del generador de informes de fallas

Para iniciar el servicio de generador de informes de fallas:

1. Seleccione **ADMIN > Servicios**.
2. Seleccione un servicio y haga clic en > **Ver > Sistema**.
3. En la barra de herramientas, haga clic en Host Tasks.
   Se muestra la Lista de tareas del host.
4. En la lista desplegable Tarea, seleccione **Iniciar servicio**.
5. En el campo Argumentos, escriba **crashreporter** y haga clic en **Ejecutar**.



El servicio de generador de informes de fallas se activa y permanece así hasta que se detiene.

Para detener el servicio del generador de informes de fallas, seleccione **Detener servicio** en la lista desplegable Tarea.

MANTENER LOS ARCHIVOS DE MAPA DE TABLAS

El archivo de mapeo de tablas que proporciona RSA, `table-map.xml`, es una parte muy importante de Log Decoder. Es un archivo de definición de metadatos que también mapea las claves que se usan en un analizador de registros a las claves de metadb.

No edite el archivo `table-map.xml`. Si desea hacer cambios en el mapa de tablas, hágalos en el archivo `table-map-custom.xml`. El archivo `table-map.xml` más reciente está disponible en Live y RSA lo actualiza si es necesario. Si hace cambios en el archivo `table-map.xml`, estos se pueden sobrescribir durante una actualización de servicio o contenido.

En `table-map.xml`, algunas claves de metadatos están configuradas en `Transient` y otras en `None`. Para almacenar e indexar una clave de metadatos específica, esta se debe configurar en `None`. Para realizar cambios en el mapeo, debe crear una copia del archivo, denominada `table-map-custom.xml`, en Log Decoder y configurar las claves de metadatos en `None`.

Para la indexación de claves de metadatos:

- Cuando una clave está marcada como `None` en el archivo `table-map.xml` en el Log Decoder, está indexada.
- Cuando una clave está marcada como `Transient` en el archivo **`table-map.xml`** en el Log Decoder, no está indexada. Para indexar la clave, copie la entrada en el archivo `table-map-custom.xml` y cambie la palabra clave `flags="Transient"` a `flags="None"`.
- Si una clave no existe en el archivo `table-map.xml`, agregue una entrada al archivo `table-map-custom.xml` en el Log Decoder.

Precaución: No actualice el archivo `table-map.xml` porque una actualización puede sobrescribirlo. Agregue todos los cambios que desea hacer en el archivo **`table-map-custom.xml`** .

Requisitos previos

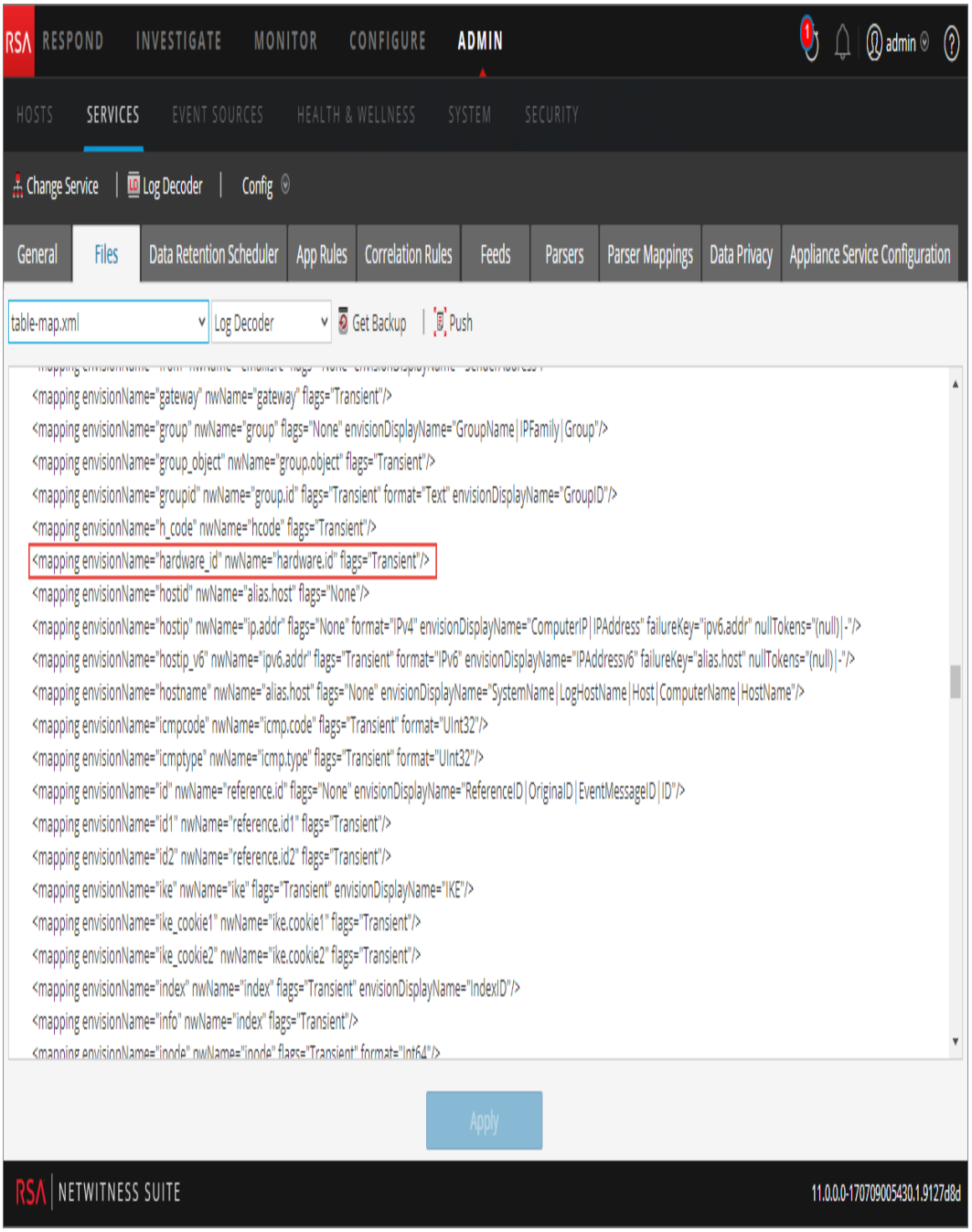
Si no tiene un archivo `table-map-custom.xml` en el Log Decoder, cree una copia de `table-map.xml` y cambie su nombre a `table-map-custom.xml`.

Procedimiento

Para verificar y actualizar el archivo de mapeo de tablas:

1. Vaya a **ADMINISTRAR** > **Servicios**.
2. En la cuadrícula Servicios, seleccione un Log Decoder y haga clic en  > **Ver** > **Configuración**.

3. Haga clic en la pestaña **Archivos** y seleccione el archivo **`table-map.xml`**.



4. Verifique que las palabras clave flags estén configuradas correctamente en `Transient` o `None`.

5. Si necesita cambiar una entrada, no cambie el archivo `table-map.xml` . En su lugar, copie la entrada, seleccione el archivo `table-map-custom.xml`, busque la entrada en el archivo `table-map-custom.xml` y cambie la palabra clave flags de `Transient` a `None`.
   Por ejemplo, la siguiente entrada para la clave de metadatos `hardware.id` en el archivo

`table-map.xml` no está indexada y la palabra clave flags aparece como `Transient`:

```
<mapping envisionName="hardware_id" nwName="hardware.id"
flags="Transient"/>
```

Para indexar la clave de metadatos `hardware.id`, cambie la palabra clave flags de `Transient` a `None` en `table-map-custom.xml`:

```
<mapping envisionName="hardware_id" nwName="hardware.id"
flags="None"/>
```

6. Si una entrada no existe en el archivo `table-map.xml`, agregue una entrada en el archivo `table-map-custom.xml`.
7. Cuando haya hecho los cambios en el archivo `table-map-custom.xml`, haga clic en **Aplicar**.

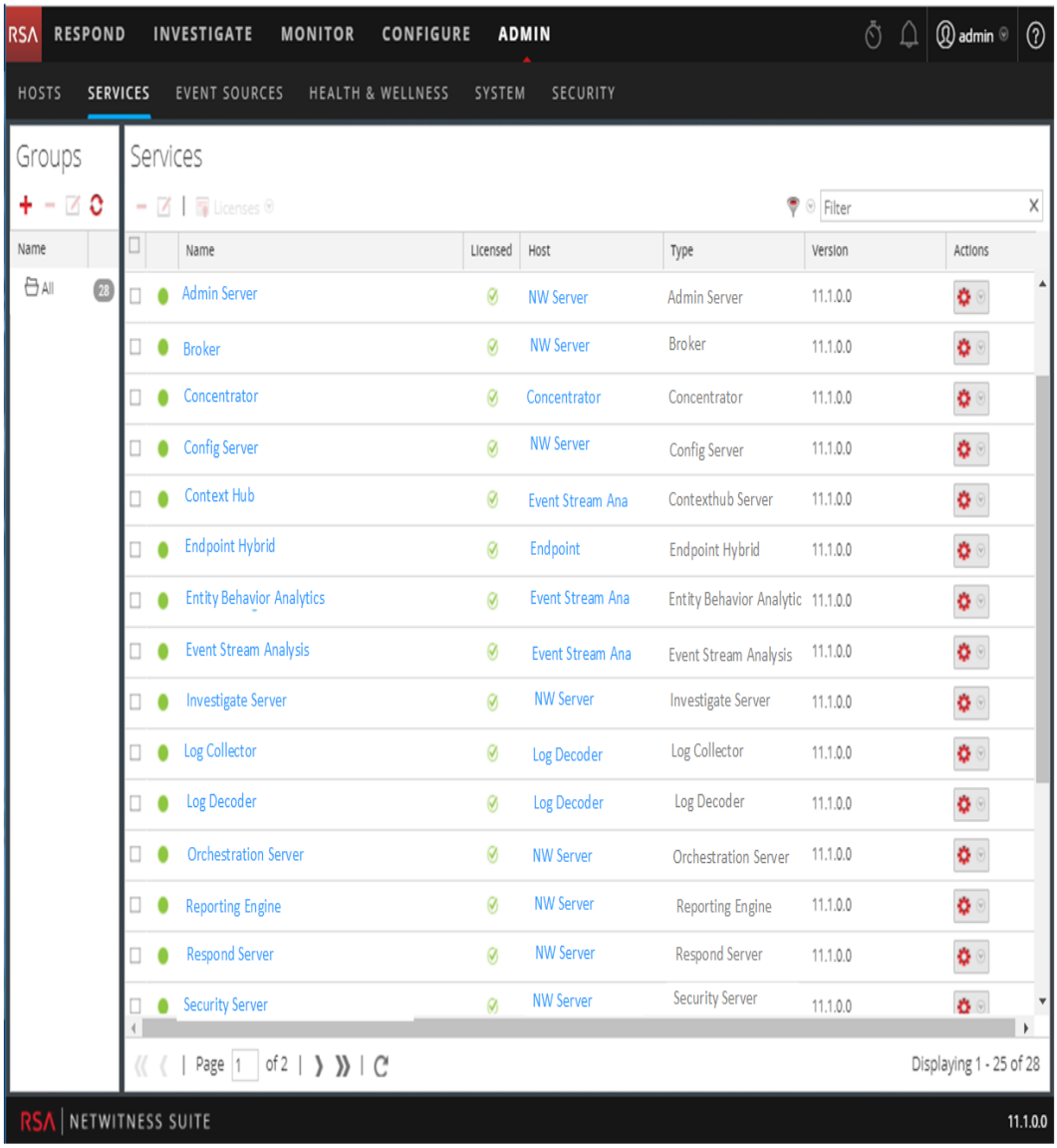
Precaución: Antes de modificar los archivos de mapeo de tablas, considere cuidadosamente el efecto de cambiar el índice de `Transient` a `None`, ya que esto puede afectar el almacenamiento disponible y el rendimiento del Log Decoder. Por esta razón, solo ciertas claves de metadatos vienen indexadas. Utilice el archivo `table-map-custom.xml` para diferentes casos de uso.

Editar o eliminar un servicio

Puede editar la configuración de un servicio, como cambiar el nombre de host o el número de puerto, o eliminar un servicio que ya no necesite.

Cada uno de los siguientes procedimientos comienza en la vista Servicios.

Para navegar a la vista Servicios, en NetWitness Suite, vaya a **ADMIN > Servicios**.

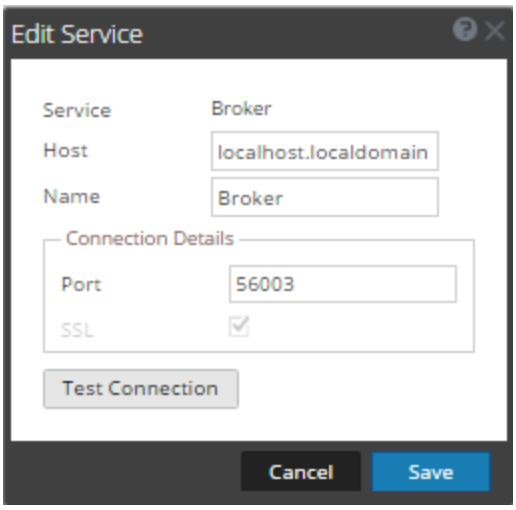


Procedimientos

EDITAR UN SERVICIO

1. En la vista Servicios, seleccione un servicio y haga clic en o > **Editar**.

   Se muestra el cuadro de diálogo **Editar servicio**. Solo muestra los campos que se aplican al servicio seleccionado.



2. Edite los detalles del servicio, para lo cual debe cambiar cualquiera de los siguientes campos:
   - **Nombre**
   - **Puerto**: cada servicio principal tiene dos puertos, SSL y no SSL. Para conexiones de confianza, debe usar el puerto SSL.
   - **SSL**: para conexiones de confianza, debe usar SSL.
   - **Nombre de usuario** y **Contraseña**: Use estas credenciales para probar la conexión a un servicio.
     a. Si usa una conexión de confianza, elimine el nombre de usuario.
        Si no utiliza una conexión de confianza, escriba el nombre de usuario y la contraseña.
     b. Haga clic en **Probar conexión**.
3. (Opcional) Si el servicio requiere una licencia, seleccione Conferir autorizaciones al servicio. Esta opción se muestra solo para los servicios que requieren una licencia.
4. Haga clic en **Guardar**.

Los cambios se hacen efectivos inmediatamente.

ELIMINAR UN SERVICIO

1. En la vista Servicios, seleccione uno o más servicios y haga clic en − o  > **Eliminar**.
2. Un cuadro de diálogo solicita confirmación. Para eliminar el servicio, haga clic en **Sí**.

El servicio eliminado ya no está disponible para los módulos de NetWitness Suite.

Explorar y editar el árbol de propiedades de servicios

Puede obtener un acceso y un control avanzados de la funcionalidad del servicio en la vista Explorar servicios, que se compone de dos partes. La lista Nodo muestra la funcionalidad de servicio en carpetas en estructura de árbol. El panel Monitor muestra las propiedades de la carpeta o el archivo seleccionado en la lista Nodos.

Cada uno de los siguientes procedimientos comienza en la vista Explorar.

Para navegar hasta la vista Explorar:

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y elija  **> Ver > Explorar**.

   Se muestra la vista Explorar. La lista Nodo está a la izquierda y el panel Monitor está a la

derecha.

Procedimientos

MOSTRAR O EDITAR UNA PROPIEDAD DE SERVICIO

Para mostrar una propiedad de servicio:

1. Haga clic con el botón secundario en un archivo en la lista Nodo o en el panel Monitorear.
2. Haga clic en **Properties**.

Para editar el valor de una propiedad de servicio:

1. En el **panel Monitorear**, seleccione un valor de propiedad editable.
2. Escriba un nuevo valor.

ENVIAR UN MENSAJE A UN NODO

1. En el cuadro de diálogo Propiedades, seleccione un **tipo de mensaje**. Las opciones varían de acuerdo con el archivo seleccionado en la lista Nodo.
   Se muestra una descripción del tipo de mensaje seleccionado en el campo **Ayuda de mensaje**.
2. (Opcional) si el mensaje así lo requiere, escriba los **parámetros**.
3. Haga clic en **Enviar**.
   Se muestra el valor o el formato en el campo **Salida de respuesta**.

Interrumpir una conexión a un servicio

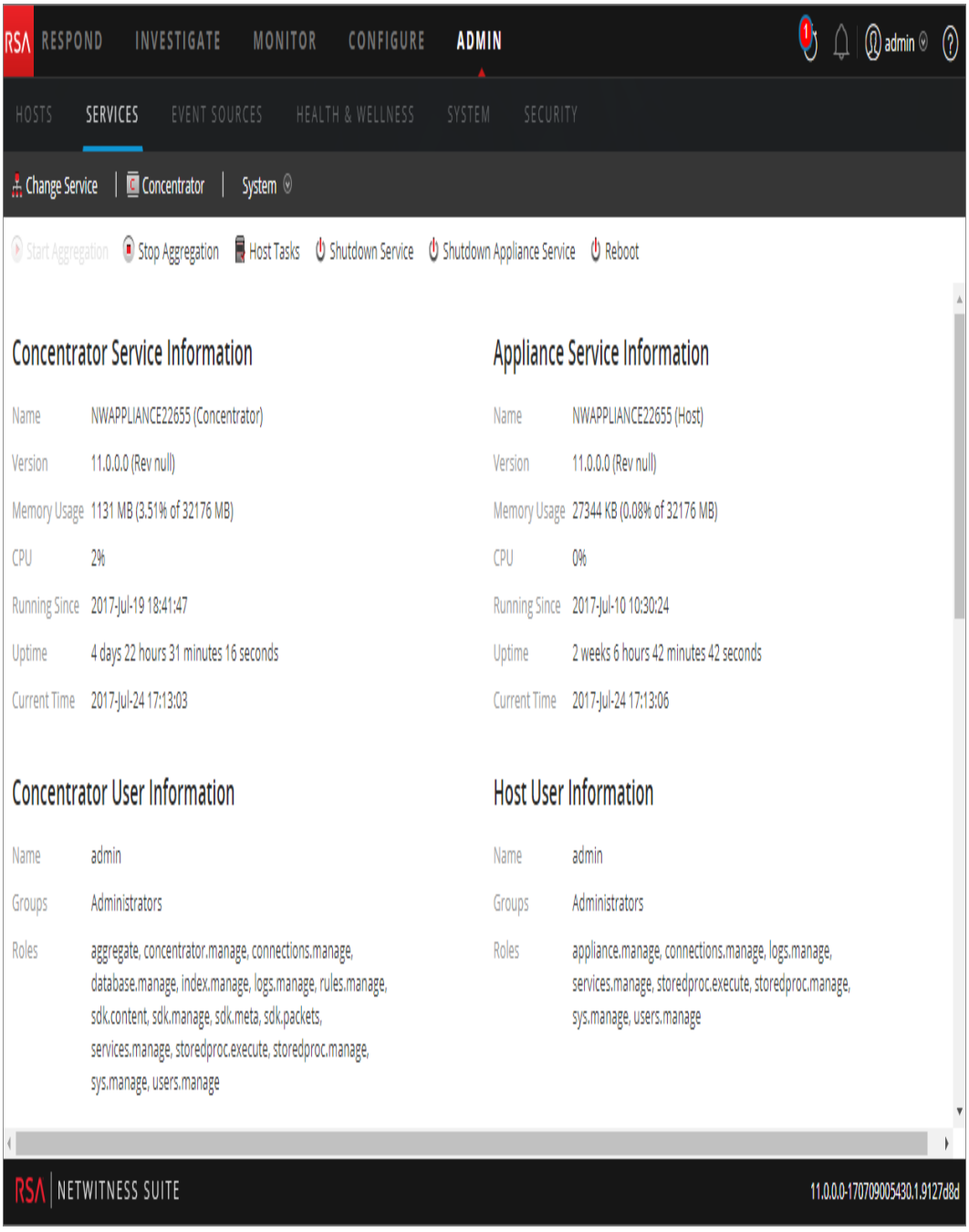
Puede ver sesiones que estén en ejecución en un servicio en la vista Sistema de servicios. En la lista de sesiones, puede terminar la sesión y finalizar las consultas activas en una sesión.

Finalizar una sesión en un servicio

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
   Se muestra la vista Servicios de Admin.

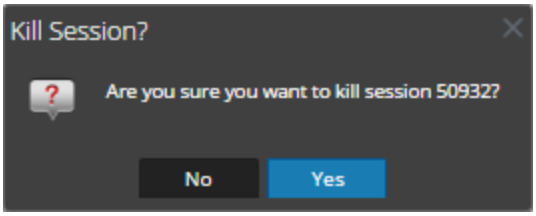
2. Seleccione un servicio y elija  **> Ver > Sistema**.

   Se muestra la vista Sistema de servicios.



3. En la parte inferior de la cuadrícula **Información de sesión**, haga clic en un ***número de sesión***.

Se muestra el siguiente cuadro de diálogo de confirmación.

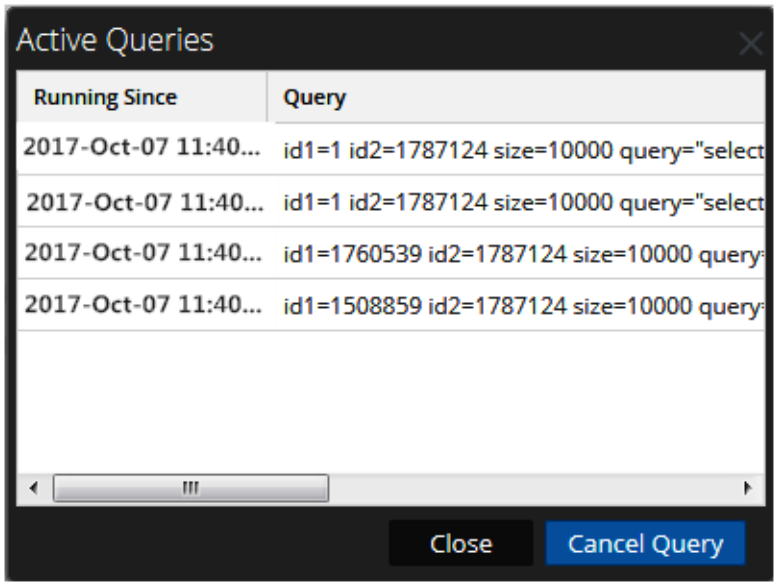


4. Haga clic en **Sí**.

La sesión termina y se elimina de la cuadrícula.

Finalizar una consulta activa en una sesión

1. Desplácese hacia abajo de la cuadrícula **Sesiones**.
2. En la columna **Consultas activas**, haga clic en un conteo distinto de cero de consultas activas de una sesión. No puede hacer clic en él si no hay consultas activas.
   Se mostrará el cuadro de diálogo Consultas activas.



3. Seleccione una consulta y haga clic en **Cancelar consulta**.
   Se detiene la consulta y se actualiza la columna Consultas activas.

Buscar servicios

Puede buscar servicios en la lista de servicios de la vista Servicios. La vista Servicios permite filtrar rápidamente la lista de servicios por nombre, host y tipo de servicio. Puede usar el menú desplegable Filtro y el campo Filtro de forma separada o a la misma vez para filtrar la vista Servicios.

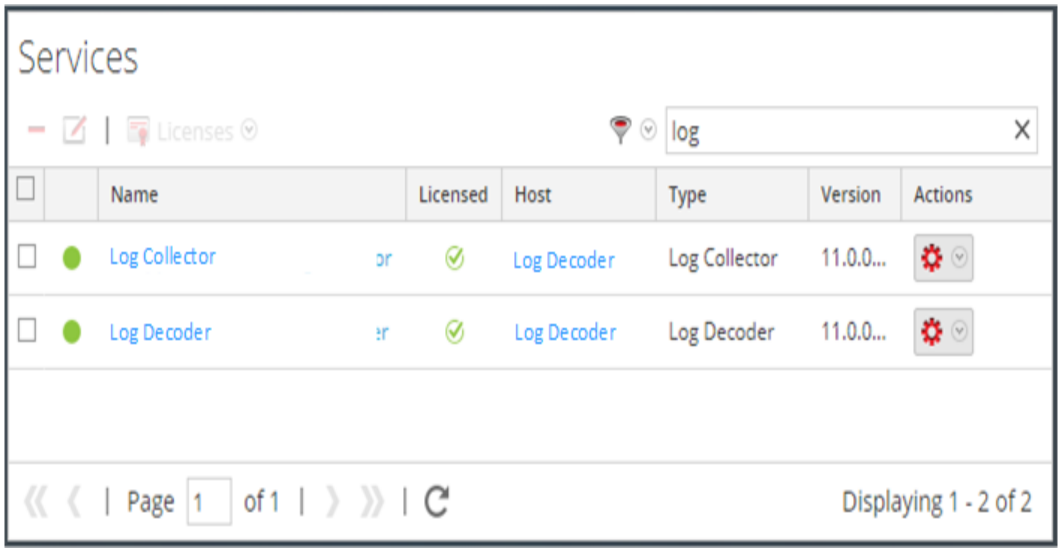
Además de poder localizar los servicios para un host en la vista Servicios, también puede buscar rápidamente los servicios que se ejecutan en un host en la vista Hosts.

Buscar un servicio

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
2. En la barra de herramientas del panel **Servicios**, escriba el **Nombre** o el **Host** de un servicio en el campo **Filtro**.

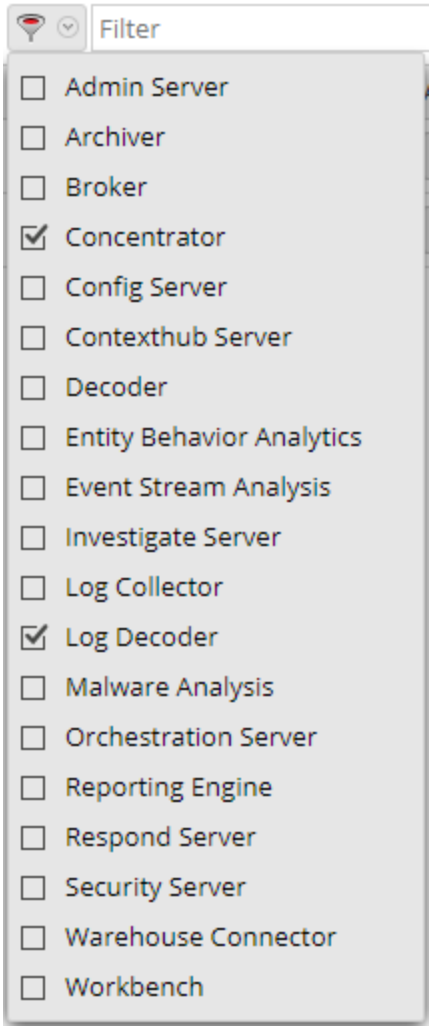
   

   En el panel Servicios se enumeran los servicios que coinciden con los nombres ingresados en el campo Filtro. En el siguiente ejemplo se muestran los resultados de búsqueda una vez que se comienza a escribir **log** en el campo Filtro.

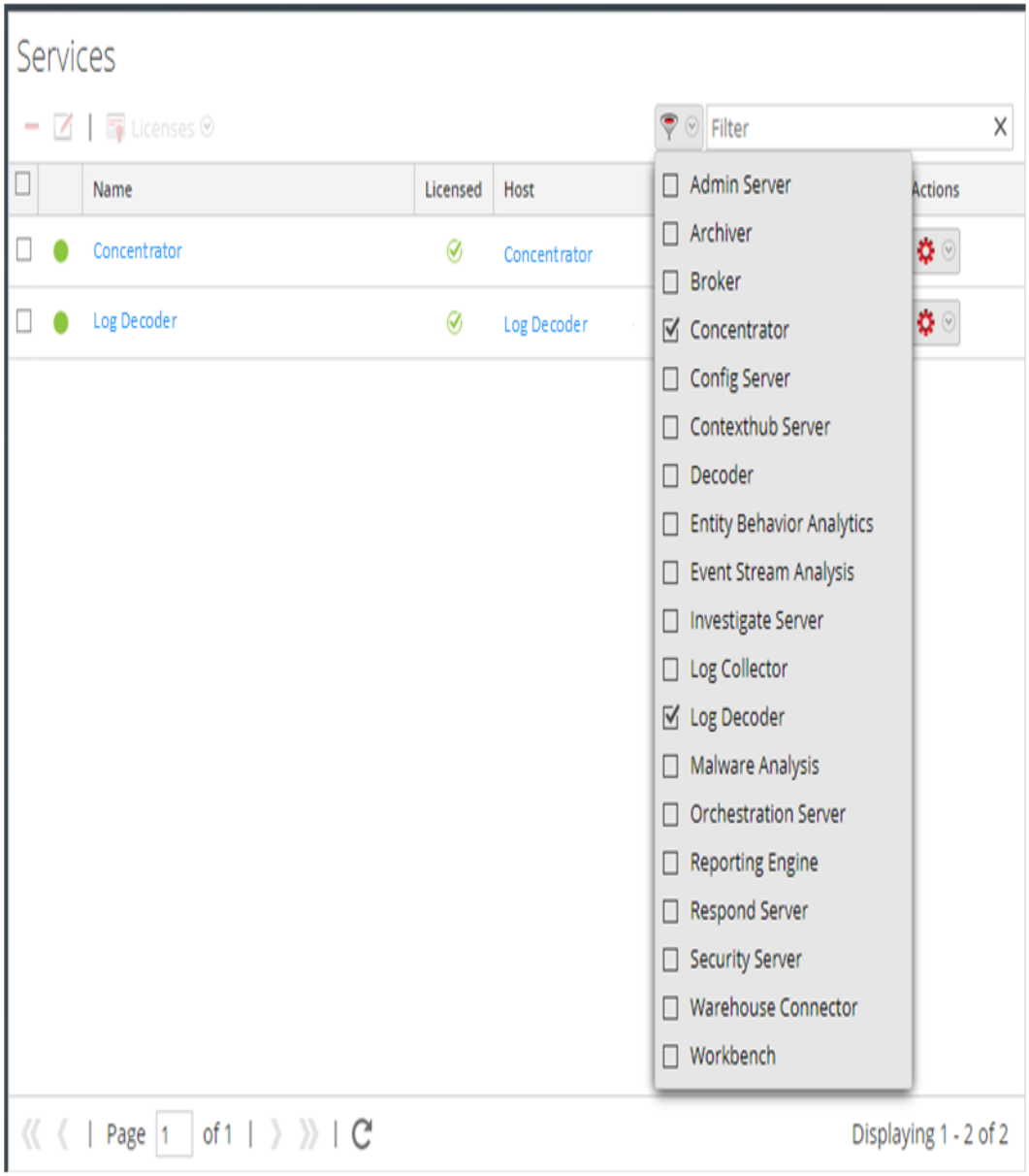
   

Filtrar servicios por tipo

1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
2. En la vista Servicios, haga clic en y seleccione los tipos de servicios que le gustaría que aparezcan en la vista Servicios.



Los tipos de servicio seleccionados aparecen en la vista Servicios. En el siguiente ejemplo se muestra la vista Servicios filtrada por Concentrator y Log Decoder.

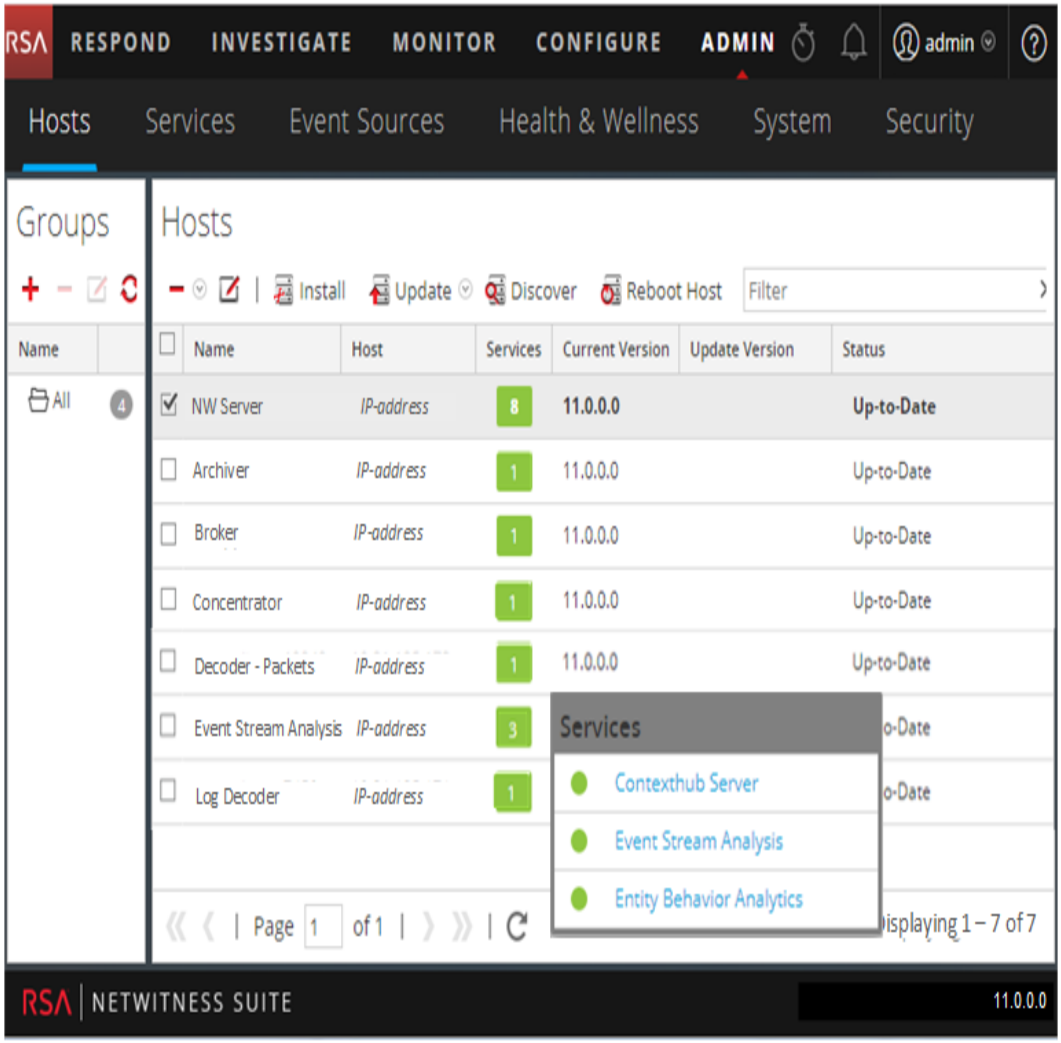


Buscar los servicios en un host

Además de poder localizar los servicios para un host en la vista Servicios, también puede buscar rápidamente los servicios que se ejecutan en un host en la vista Hosts.

1. En NetWitness Suite, vaya a **ADMIN > Hosts**.
2. En la vista Hosts, seleccione un host y haga clic en el cuadro que contiene un número (el número de servicios) en la columna **Servicios**.
   Se muestra una lista de los servicios en el host seleccionado.

En el siguiente ejemplo se enumera una lista de tres servicios en el host seleccionado después de que se hace clic en el cuadro que contiene el número 3.



3. Puede hacer clic en los vínculos del servicio para ver los servicios en la vista Servicios.

Iniciar, detener o reiniciar un servicio

Estos procedimientos solo se aplican a servicios principales.

Cada uno de los siguientes procedimientos comienza en la vista Servicios. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.

Iniciar un servicio

Seleccione un servicio y haga clic en  > **Iniciar**.

Detener un servicio

Cuando detiene un servicio, todos los procesos se detienen y los usuarios activos se desconectan de él.

Para detener un servicio:

1. Seleccione un servicio y haga clic en  > **Detener**.
2. Un cuadro de diálogo solicita confirmación. Para detener el servicio, haga clic en **Sí**.

Reiniciar un servicio

A veces, tiene que reiniciar un servicio para que los cambios surtan efecto. Cuando cambia un parámetro que requiere un reinicio, NetWitness Suite muestra un mensaje.

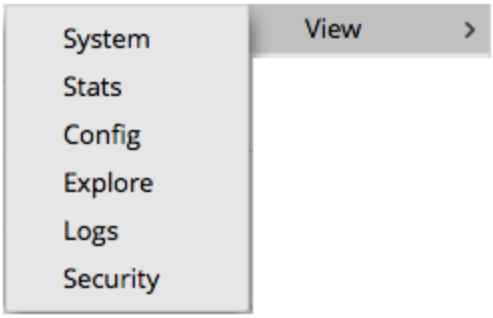
Para reiniciar un servicio:

1. Seleccione un servicio y haga clic en  > **Reiniciar**.
2. Un cuadro de diálogo solicita confirmación. Para detener el servicio, haga clic en **Sí**.

El servicio se detiene y se reinicia automáticamente.

Ver detalles de servicios

Puede ver y editar información sobre los servicios mediante las opciones del menú Ver de un servicio.



Objetivo de cada vista Servicio

Cada vista muestra una parte funcional de un servicio y se describe detalladamente en su propia sección:

- En la vista Sistema se muestra un resumen de información de servicio, servicio de dispositivo, usuario del host, licencia y sesión.

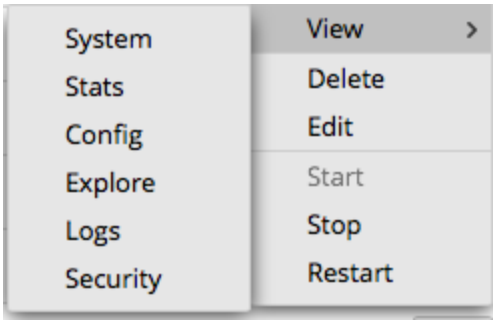
- La vista Estadísticas de servicios proporciona una forma de monitorear las operaciones y el estado de un servicio.
- La vista Configuración de servicios permite configurar todos los aspectos de un servicio.
- La vista Explorar de servicios permite ver y editar las configuraciones de hosts y servicios.
- El panel Registro de sistema muestra registros de servicios en los cuales se puede buscar.
- La vista Seguridad de servicios es una forma de agregar cuentas de usuario de Security Analytics Core para agregación, usuarios de clientes gruesos y usuarios de la API REST.

Acceder a la vista Servicios

Para acceder a una vista de un servicio:

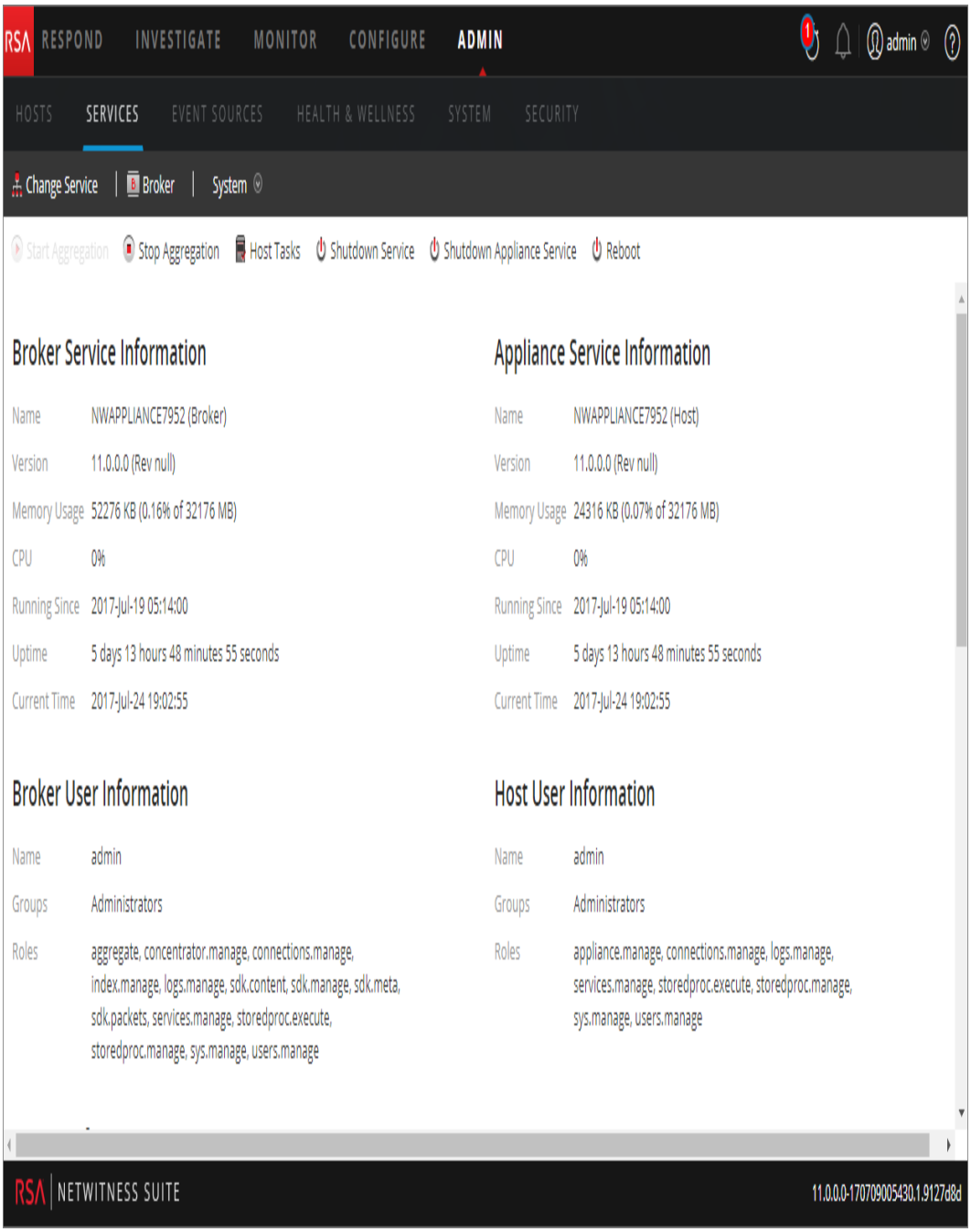
1. En NetWitness Suite, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y haga clic en  **> Ver**.

   Aparece el menú Ver.

3. En las opciones de la izquierda, seleccione una vista.

   Esta es una vista Sistema correspondiente a un Broker.

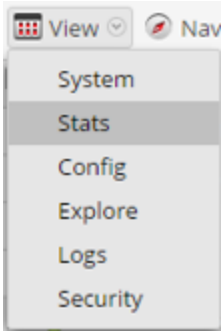


4. Use la barra de herramientas para navegar:

   a. Haga clic en **Cambiar servicio** para seleccionar otro servicio.
      Se muestra el cuadro de diálogo **Administrar servicio**.

   b. Seleccione la casilla de verificación a la izquierda del servicio que desea.

c. Seleccione la vista que desea para el servicio que seleccionó en el menú desplegable Ver.



Se muestra la vista nueva (por ejemplo, Estadísticas) para el servicio que seleccionó.

Referencias de las vistas Hosts y Servicios

Este tema es una referencia a las funciones de la interfaz del usuario de NetWitness Suite ADMIN.

Este tema describe las funciones disponibles en la interfaz del usuario de NetWitness Suite Admin. El módulo Admin extrae las actividades de NetWitness Suite Admin a una única vista para monitorear y administrar los hosts (dispositivos), los servicios, las tareas y la seguridad.

Temas

Vista Hosts

La máquina física o virtual en la cual se ejecutan los servicios de NetWitness Suite se configura y se mantiene en la vista **Hosts**.

Importante: Consulte Solución de problemas de instalaciones y actualizaciones de versión para obtener ayuda sobre cómo resolver los errores que recibe durante la instalación y la actualización de la versión.

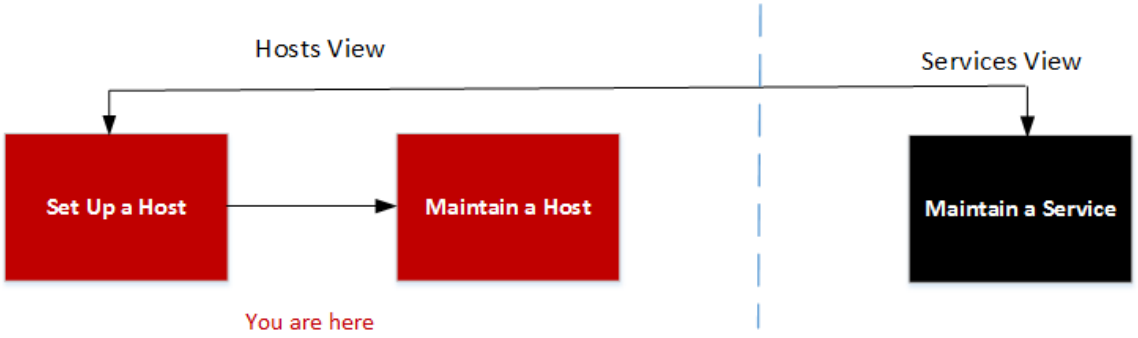
Un servicio realiza una función única, como recopilar registros o archivar datos. Cada servicio se ejecuta en un puerto exclusivo y se modela como un plug-in para habilitarse o deshabilitarse de acuerdo con la función del host. En primer lugar, debe configurar los siguientes servicios Core:

Principal	Otros	Otros	Otros
Decoder	Log Decoder	Context Hub	Reporting Engine
Concentrator	Archiver	Log Collector	Warehouse Connector
Broker	Event Stream Analysis	Malware Analysis	Workbench

Debe configurar hosts y servicios para la comunicación entre estos y con la red de modo que puedan ejecutar sus funciones, como el almacenamiento o la captura de datos.

Flujo de trabajo

En este flujo de trabajo se muestran los procedimientos que se realizan para configurar, mantener y actualizar un host con las versiones nuevas de NetWitness Suite. La configuración de un host es la primera tarea de este flujo de trabajo. Los hosts con servicios principales se configuran de manera inmediata. Después de eso, puede configurar hosts adicionales con el fin de mejorar la implementación de NetWitness Suite. Las otras dos tareas, el mantenimiento de un host y la actualización de versiones para un host, se realizan cuando son necesarias y no se deben ejecutar en un orden específico.

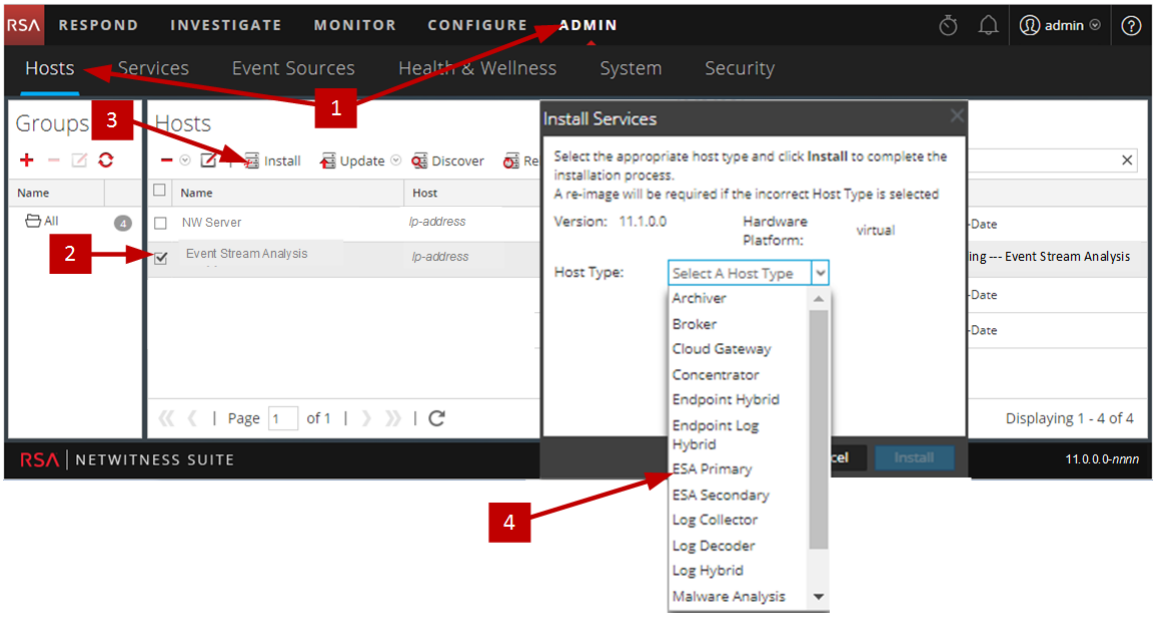


¿Qué desea hacer?

Consulte Introducción de hosts: Procedimientos de hosts y servicios con el fin de obtener instrucciones detalladas para las siguientes tareas.

Función	Deseo…
Administrador	Configurar un host.
Administrador	Mantener un host.
Administrador	Aplicar actualizaciones de versión a un host.

Vista rápida



En el siguiente ejemplo se muestra cómo configurar un host.

1. Seleccione ADMIN > Hosts.
2. Seleccione el host que implementó (por ejemplo, **Event Stream Analysis**).
3. Haga clic en Install (ícono Instalar).
4. Seleccione el servicio que se instalará en el cuadro de diálogo **Instalar servicios** (por ejemplo, **ESA primario**). Este tipo de host instala los servicios Entity Behavior Analytics, Context Hub y Event Stream Analysis en este host.

Barra de herramientas del panel Hosts

La barra de herramientas de la vista Hosts contiene las herramientas que se usan para mantener los hosts en la implementación de NetWitness Suite.

En NetWitness Suite, vaya a **Admin** > **Hosts** para acceder a la vista Hosts. La barra de herramientas del panel Hosts se encuentra en la parte superior de la cuadrícula Hosts en la vista Hosts.

Funciones

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

Funciones	Descripción
	**Eliminar de grupo**: Si el host es parte de un grupo de hosts, puede eliminar lo del grupo.
	Abra el cuadro de diálogo Editar host, en el cual edita la configuración básica de comunicación e identificación de un host o un servicio. Este cuadro de diálogo tiene las mismas características que el cuadro de diálogo Agregar host. Procedimientos relacionados: Paso 1. Implementar un host
Instalación	Se abre el cuadro de diálogo **Instalar servicios** desde el cual puede instalar un servicio en un host implementado. Procedimientos relacionados: Paso 2. Instalar un servicio en un host

Funciones	Descripción
Actualizar	• **Actualizar**: Actualiza el o los hosts que haya seleccionado con la versión que se selecciona en la columna **Versión de actualización**. • **Buscar actualizaciones**: Busca el repositorio de actualización local para obtener las actualizaciones más recientes disponibles en RSA. Procedimientos relacionados: Aplicar actualizaciones de versión a un host
Descubrir	La mayor parte del tiempo, la función Descubrir se ejecuta automáticamente y no es necesario hacer clic en el botón Descubrir. En el caso de una instalación nueva, haga clic en Descubrir para acceder al cuadro de diálogo Aprovisionar de modo que pueda completar la fase de aprovisionamiento. Después de la fase de aprovisionamiento, NetWitness Suite descubre automáticamente los servicios que se ejecutan en el host y no es necesario hacer clic en el botón Descubrir. En el caso de una instalación nueva, haga clic en **Descubrir** para acceder al cuadro de diálogo **Aprovisionar** de modo que pueda completar la fase de aprovisionamiento. Después de la fase de aprovisionamiento, NetWitness Suite descubre automáticamente los servicios que se ejecutan en el host.
Reiniciar host	Reinicie el host.
Filtro	Filtre los hosts por nombre o host.

Barra de herramientas del panel de grupos

En la barra de herramientas del panel Grupos se proporcionan opciones para administrar grupos de hosts. Utilice la barra de herramientas para crear, editar y eliminar grupos. Una vez que crea un grupo, puede arrastrar hosts individuales desde el panel Hosts a ese grupo.

Use grupos para organizar los hosts por función, ubicación geográfica, proyecto o cualquier otro principio de organización que sea útil. Un host puede pertenecer a más de un grupo.

En NetWitness Suite, vaya a **ADMIN > Hosts**. La barra de herramientas del panel Grupos está en la parte superior de la cuadrícula Grupos en la vista Hosts.

En el panel Grupos se proporciona un modo de crear grupos lógicos de hosts. Una vez que los hosts están agrupados, es más fácil ejecutar operaciones en varios de ellos mediante la interacción con cada uno de manera grupal, en lugar de interactuar con hosts individuales en una lista desagrupada.

Nota: En NetWitness Live, los grupos pueden suscribirse a recursos, no así los hosts individuales.

El panel Grupos consta de una cuadrícula completada con una lista de grupos de hosts definidos y la barra de herramientas del panel Grupos.

Columna	Descripción
	Muestra una nueva fila en la cuadrícula Grupo donde puede ingresar el nombre de un nuevo grupo.
	Solicita confirmación para eliminar el grupo o el host. Puede confirmar o cancelar la eliminación.
	Abre el campo de nombre en una fila de la cuadrícula Grupo para que pueda ingresar un nuevo nombre para un grupo existente.
	Actualiza el grupo seleccionado.
Nombre	Nombre del grupo de hosts. Haga clic en el nombre del grupo en el panel Grupos para enumerar los hosts de ese grupo en el panel Hosts.
<En blanco>	Indica la cantidad de hosts en el grupo. Haga clic en la cantidad de hosts del grupo en el panel Grupos para enumerar los hosts de ese grupo en el panel Hosts.

Introducción de hosts: Vista Servicios

Los servicios de NetWitness Suite se configuran y se mantienen en la vista **Servicios**. La vista Servicios le permite:

- Buscar y ubicar rápidamente un servicio o tipo de servicio específico, como Log Decoder o Warehouse Connector
- Usar accesos directos para llegar a tareas de administración
- Agregar, editar y eliminar servicios
- Administrar licencias y ver el estado de la licencia de un servicio (con o sin licencia)
- Ordenar los servicios por nombre y host
- Filtrar servicios por tipo y por nombre y host
- Iniciar, detener o reiniciar servicios

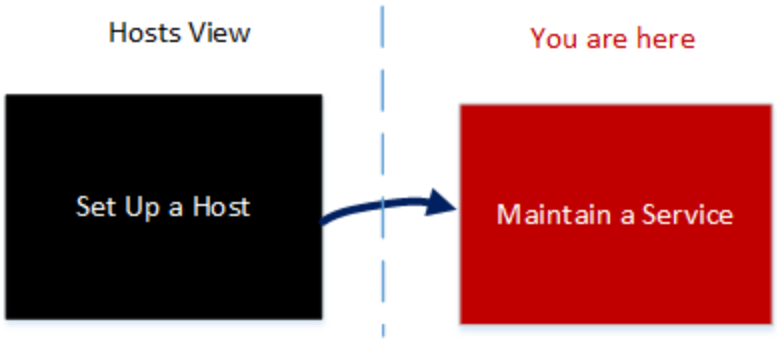
Un servicio realiza una función única, como recopilar registros o archivar datos. Cada servicio se ejecuta en un puerto exclusivo y se modela como un plug-in para habilitarse o deshabilitarse de acuerdo con la función del host. En primer lugar, debe configurar los siguientes servicios Core:

Principal	Otros	Otros	Otros
Decoder	Archiver	IPDB Extractor	Warehouse Connector
Concentrator	Event Stream Analysis	Log Collector	Workbench
Broker	Context Hub	Malware Analysis	
Log Decoder	Incident Management	Reporting Engine	

Debe configurar hosts y servicios para la comunicación entre estos y con la red de modo que puedan ejecutar sus funciones, como el almacenamiento o la captura de datos.

Flujo de trabajo

En este flujo de trabajo se muestran los procedimientos que debe completar para configurar y mantener un servicio. La adición de un servicio a un host es la primera tarea de este flujo de trabajo. Los hosts con servicios principales se configuran de manera inmediata. Después de eso, puede configurar servicios adicionales en hosts con el fin de mejorar la implementación de NetWitness Suite.



¿Qué desea hacer?

Consulte Introducción de hosts: Procedimientos de hosts y servicios con el fin de obtener instrucciones detalladas para las siguientes tareas.

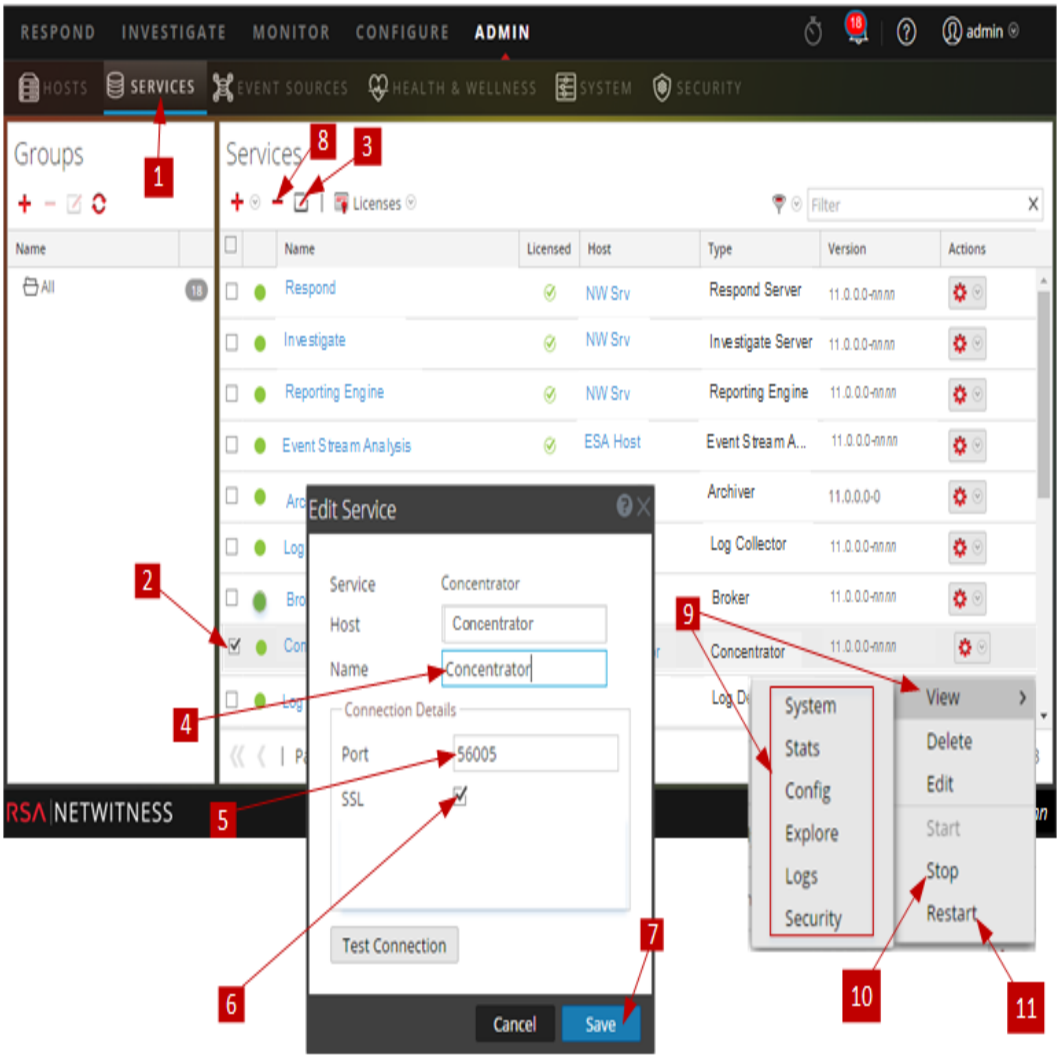
Función	Deseo...
Administrador	Mantener un servicio.
Administrador	Configurar un host.

Temas relacionados

- Mejores prácticas
- Solucionar problemas de actualizaciones de hosts

Vista rápida

En el siguiente ejemplo se muestra cómo mantener un servicio.



Seleccione un servicio.

1	Vaya a **ADMINISTRAR** > vista **Servicios**.
2	Haga clic en la casilla de verificación a la izquierda del servicio que desea seleccionar.

Edite el nombre del servicio y la conexión.

3	Haga clic en (de manera alternativa, seleccione Editar en (menú desplegable Acción).
4	Edite el nombre del **host**.
5	Edite el **nombre** del servicio.
6	Edite el número de **puerto**.
7	Deseleccione o seleccione la conexión de la comunicación SSL.

8 Haga clic en **Probar conexión**.

Elimine un servicio.

9 **Seleccione un servicio** y haga clic en ícono Eliminar.

Ver estadísticas de un servicio y configurar sus parámetros

10 Realice los siguientes pasos para ver las estadísticas de un servicio y configurar sus parámetros.

a. **Seleccione un servicio** y haga clic en ícono Acciones.

b. Haga clic en **Ver** y seleccione:

- **Sistema** para:
  - Ver información general actual sobre el servicio y su host.
  - Acceder a la barra de herramientas de la vista Sistema.
- **Estadísticas** para ver las estadísticas detalladas del servicio.
- **Configuración** para ver y configurar los parámetros del servicio.
- **Explorar** para ver y configurar los parámetros del servicio en la vista Explorar de NetWitness Suite.
- **Registros** para ver los mensajes de registro que emite el servicio.

10 **Seleccione un servicio**, haga clic en el ícono Acciones y haga clic en **Detener** para detener un servicio que está en ejecución.

11 **Seleccione un servicio**, haga clic en el ícono Acciones y haga clic en **Reiniciar** para reiniciar un servicio detenido.

Temas

Consulte las siguientes guías de RSA NetWitness Suite para obtener información detallada acerca de cada servicio. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Guía de configuración de Archiver

Guía de configuración de Broker y Concentrator

Guía de configuración de Cloud Behavioral Analytics Gateway

Guía de configuración de Context Hub

Guía de configuración de Decoder y Log Decoder

Guía de configuración de Endpoint Insights

Guía de configuración de Event Stream Analysis (ESA)

Guía del usuario de Investigate y Malware Analysis

Guía de configuración de la recopilación de registros

Guía de configuración de Malware Analysis

Guía del usuario de Reporting Engine

Guía de configuración de Respond

Guía de configuración de Workbench

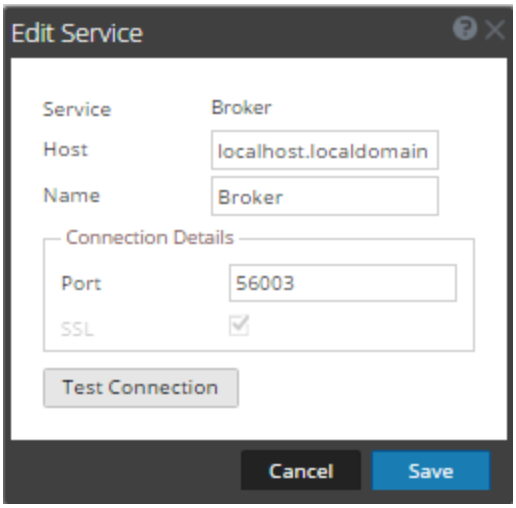
Guía de configuración de Warehouse Connector

Cuadro de diálogo Editar servicio

En este tema se presenta el cuadro de diálogo Editar servicio, al cual se accede desde la vista Servicios de ADMINISTRAR (ADMINISTRAR > Servicios).

Los servicios de NetWitness Suite se descubren automáticamente en NetWitness Suite.

Puede usar el cuadro de diálogo Editar servicio para modificar servicios. Para acceder al cuadro de diálogo Editar servicio, vaya a **ADMIN > Servicios** y seleccione **Editar** ( ) en la barra de herramientas del panel **Servicios**.



Los procedimientos relacionados con los servicios se describen en Introducción de hosts: Procedimientos de hosts y servicios.

Funciones

En esta tabla se describen las funciones de los cuadros de diálogo Agregar servicio o Editar servicio.

Campo u Opción	Descripción
Servicio	Muestra el tipo de servicio. Puede agregar los siguientes servicios: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector y Workbench.
Host	Especifica el host en el cual reside el servicio.

Campo u Opción	Descripción
Nombre	Especifica el nombre que se usa para identificar el servicio; por ejemplo, **Broker**. Una convención de asignación de nombres comprensible puede facilitar las tareas administrativas. A algunos administradores también les resulta conveniente utilizar el nombre de host o la dirección IP (especificada en el campo **Host**) como el **Nombre**.
Puerto	Especifica el puerto utilizado para comunicarse con este servicio. El puerto predeterminado basado en el tipo de servicio seleccionado en el campo **Servicio** se completa automáticamente aquí. Si selecciona **SSL** a continuación, este puerto se convierte en un puerto SSL. Si no selecciona **SSL**, se convierte en un puerto no SSL. Puede personalizar este puerto si abre un firewall para el puerto que agrega. Para obtener información sobre puertos, consulte **Arquitectura y puertos de red** en la *Guía de implementación*.
SSL	Indica que NetWitness Suiteutiliza SSL para comunicaciones con este servicio.
Nombre de usuario	Especifica el nombre de usuario utilizado para iniciar sesión con este servicio. El nombre de usuario predeterminado es **admin**.
Contraseña	Especifica la contraseña utilizada para iniciar sesión con este servicio. La contraseña predeterminada es **netwitness**.
Conferir autorizaciones al servicio	(Opcional) Asigna licencias desde el servidor de licencias local (LLS) a los servicios seleccionados. Para obtener más información, consulte el tema **Ver autorizaciones actuales** en la *Guía de licencia*.
Probar conexión	Al hacer clic en este botón, se realiza la prueba de conexión de un servicio que esté agregando.

Campo u Opción	Descripción
Cancelar	Cuando se hace clic en este botón, se cierra el cuadro de diálogo Agregar servicio o Editar servicio. Si no guarda el servicio antes de cerrar el cuadro de diálogo, el servicio no se agrega o no se edita.
Guardar	Al hacer clic en este botón, se guarda el nuevo servicio.

Barra de herramientas del panel de grupos

En este tema se presentan las funciones y las opciones de **ADMIN > vista Servicios** > barra de herramientas del panel **Grupos**.

La barra de herramientas del panel Grupos proporciona opciones para administrar grupos de servicios. La barra de herramientas incluye opciones para crear, editar y eliminar grupos. Una vez que se crean los grupos, puede arrastrar servicios individuales desde el panel Servicios a un grupo.

Los grupos pueden reflejar un principio funcional, geográfico, orientado a un proyecto o cualquier principio de la organización que sea útil. Un servicio puede pertenecer a más de un grupo.

Para acceder a la vista Servicios, en **NetWitness Suite**, vaya a **ADMIN > Servicios.** La barra de herramientas del panel Grupos está en la parte superior de la cuadrícula Grupos de la vista Servicios.

Funciones

Esta tabla describe funcionalidades de la barra de herramientas.

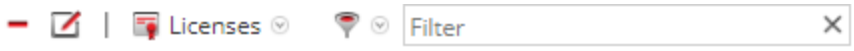
Opción	Descripción
+	Muestra una nueva fila en la cuadrícula Grupo donde puede ingresar el nombre de un nuevo grupo.
−	Solicita confirmación si desea eliminar el grupo o servicio. Puede confirmar o cancelar la eliminación.
	Abre el campo de nombre en una fila de la cuadrícula Grupo para que pueda ingresar un nuevo nombre para un grupo existente.
	Actualiza el grupo seleccionado.

Barra de herramientas del panel Servicios

En este tema se presentan las opciones de la barra de herramientas del panel Servicios para agregar, editar, eliminar y otorgar licencia a los servicios. También puede filtrar los servicios que se indican en el panel Servicios.

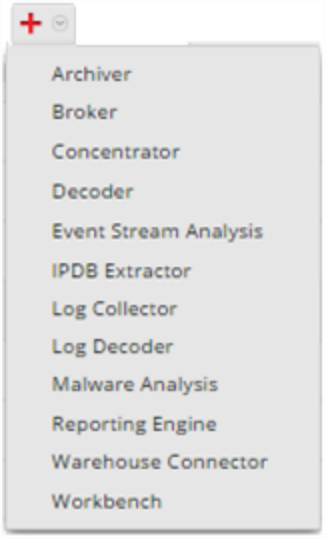
La barra de herramientas de panel Servicios incluye opciones para agregar, eliminar, editar y otorgar licencia a los servicios. Puede filtrar los servicios que se indican en función de uno o más tipos de servicios, nombre de servicio y host.

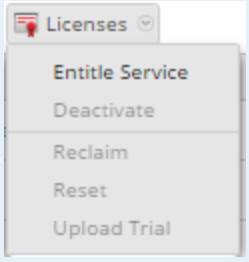
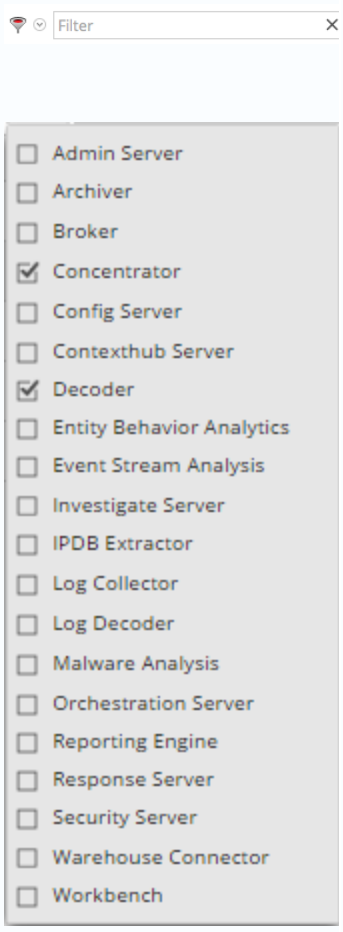
Para acceder a la vista Servicios de Administration, en **NetWitness Suite**, vaya a **ADMIN > Servicios.** La barra de herramientas del panel Servicios se encuentra en la parte superior de la cuadrícula Servicios de la vista Servicios.



Funciones

En la tabla se describen las funciones de la barra de herramientas del panel Servicios.

Función	Descripción
	Agrega un servicio para que lo administre esta instancia de RSA NetWitness Suite (consulte Paso 2. Instalar un servicio en un host).
	Elimina un servicio de esta instancia de NetWitness Suite (consulte Editar o eliminar un servicio).
	Edita la identificación del servicio y la configuración básica de la comunicación.

Función	Descripción
	• Conferir autorizaciones al servicio: Asigna licencias de Local License Server (LLS) a los servicios seleccionados (consulte el tema **Pestaña Descripción general** de la *Guía de licencia*). • Desactivar: No se usa en NetWitness Suite 10.6. • Recuperar: Recupera una licencia desactivada desde LLS para el servicio seleccionado. • Restablecer: No se usa en NetWitness Suite 10.6. • Cargar prueba: No se usa en NetWitness Suite 10.6.
	Filtra los servicios que se indican en la vista Servicios. En el menú desplegable Filtro, puede filtrar los servicios por uno o más tipos de servicio seleccionados. En este ejemplo, cuando selecciona Concentrator y Decoder, solo aparecen los servicios de Concentrator y Decoder en la vista Servicios. En el campo Filtro, puede filtrar los servicios por nombre y host. Puede usar el menú desplegable Filtro y el campo Filtro al mismo tiempo para filtrar los servicios que se indican en la vista Servicios.

Vista Configuración de servicios

En este tema se presentan las funcionalidades y funciones de la vista Configuración de servicios.

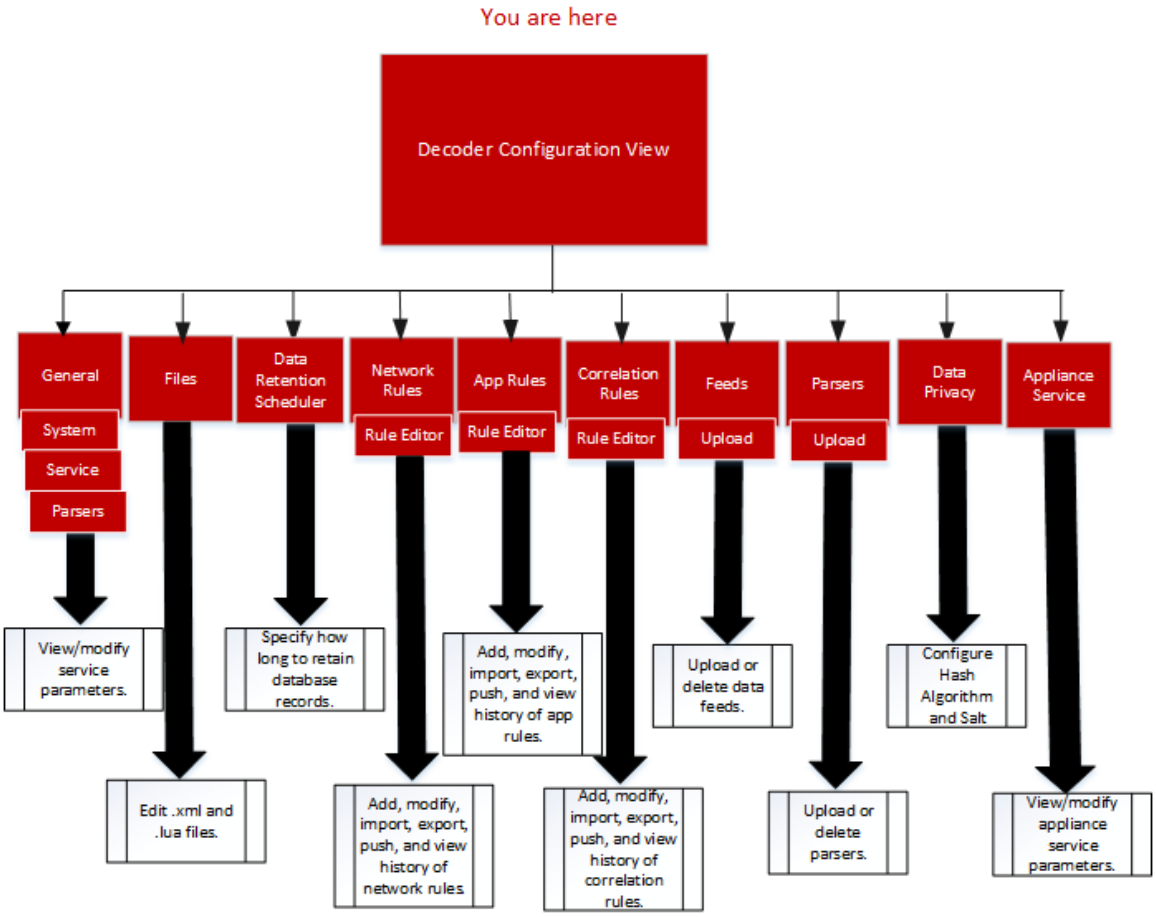
La vista Configuración de servicios es una de las vistas disponibles en **Servicios** > menú Acciones (). Proporciona una interfaz del usuario para configurar todos los aspectos de un servicio principal o un servicio de NetWitness Suite.

Las opciones de configuración en la vista Configuración de servicios se organizan en pestañas y cada pestaña proporciona una vista de un conjunto de parámetros relacionados. A diferencia de la vista Explorar de servicios, la cual ofrece un acceso directo a todos los archivos de configuración de un servicio, estas pestañas contienen los parámetros que se modifican con mayor frecuencia en la configuración de servicios a través de una vista fácil de usar.

Debido a los requisitos de configuración de los distintos servicios, cada tipo de servicio tiene variaciones en las pestañas y los parámetros de configuración disponibles en esta vista. Cada tema describe los parámetros de configuración que son específicos de un host (Brokers y Concentrators, Decoders y Log Decoders) o de un servicio (por ejemplo, Reporting Engine, IPDB Extractor, Log Collector y Warehouse Connector).

Flujos de trabajo

En el siguiente flujo de trabajo se muestran las tareas de configuración del servicio Decoder como un ejemplo de esta vista. Consulte las guías de configuración de cada servicio (por ejemplo, la *Guía de configuración de Broker y Concentrator* de *RSA NetWitness® Suite*) para obtener detalles sobre sus vistas **ADMIN > Servicios > Configuración**.

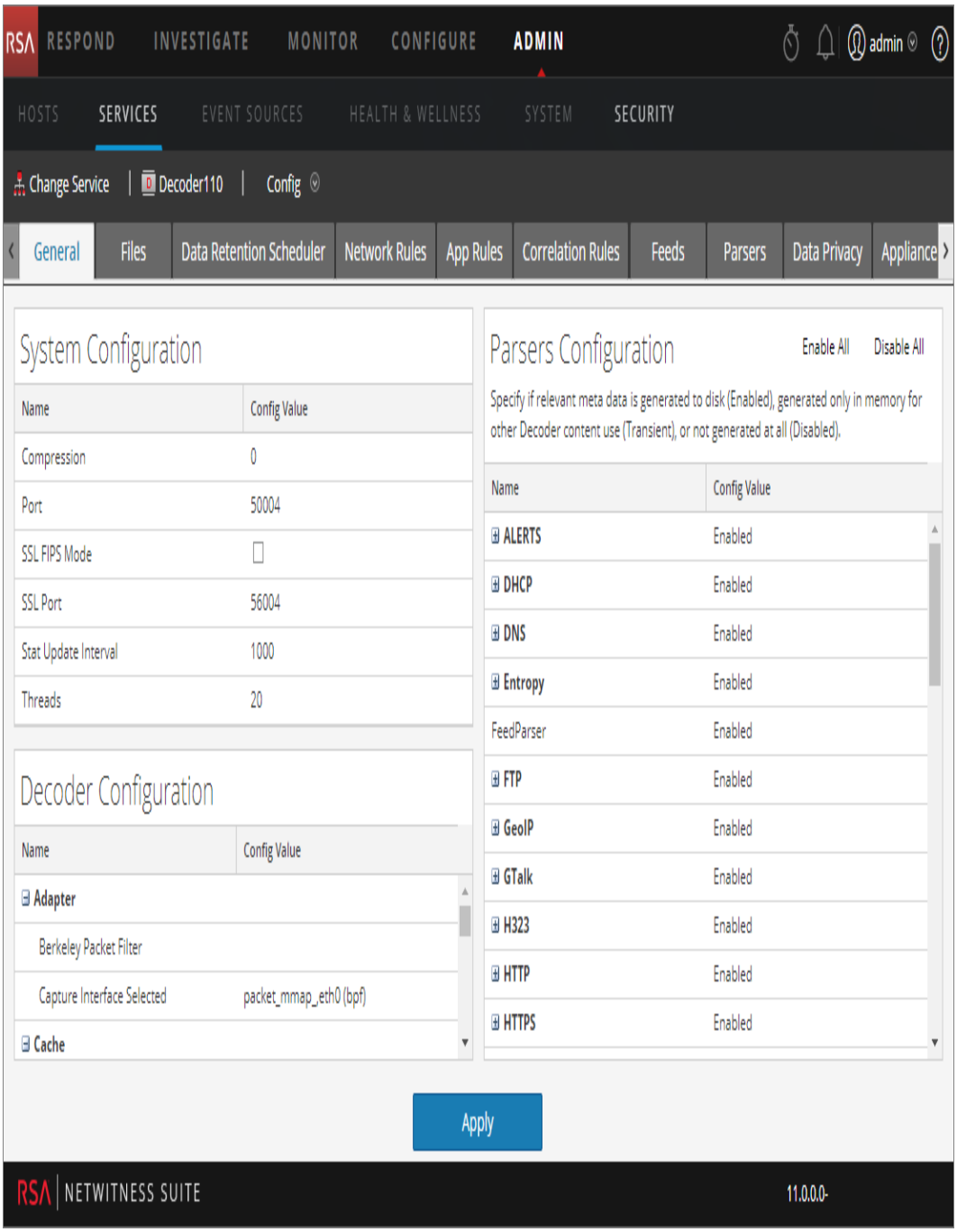


Para acceder a la vista Configuración de servicios:

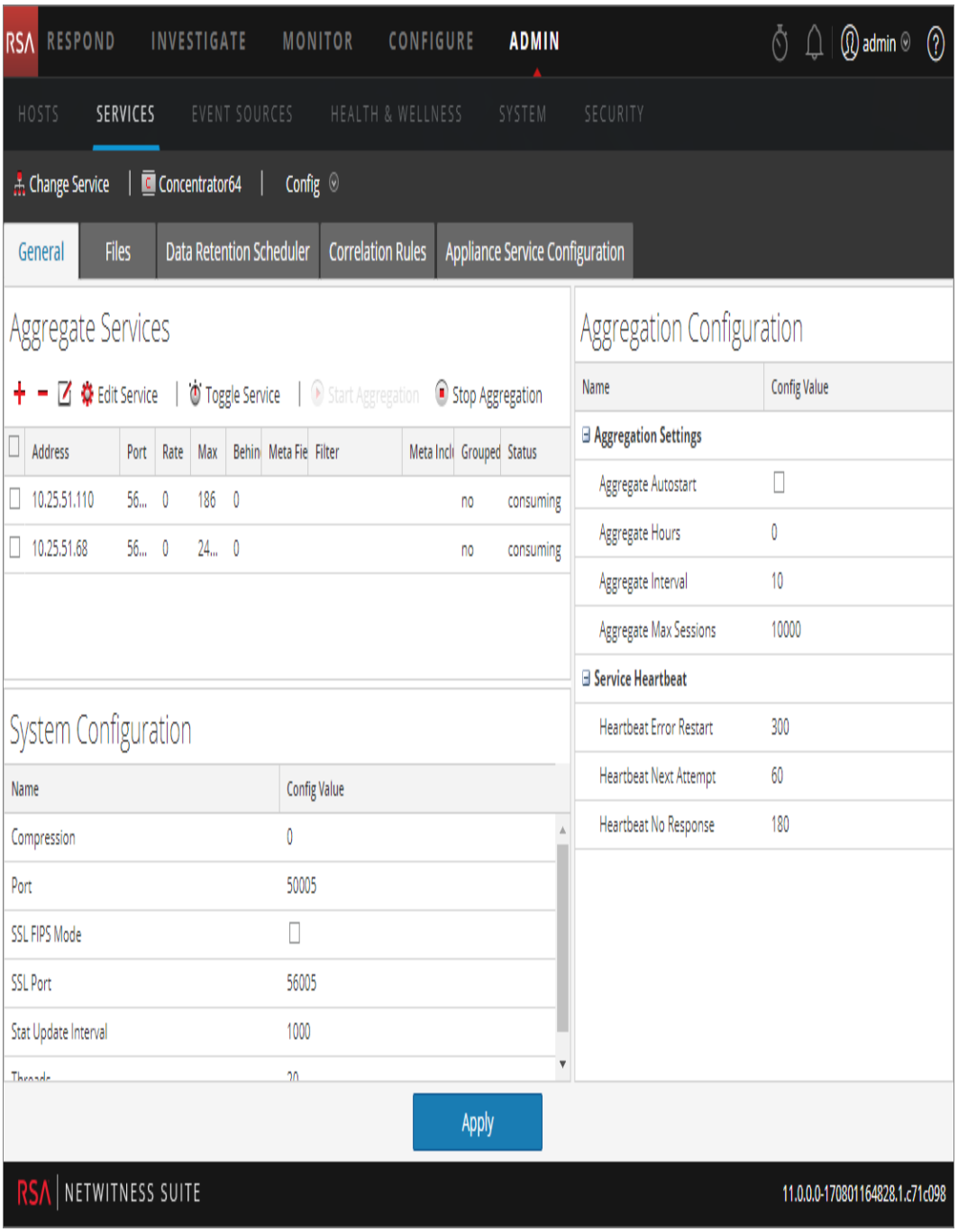
1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione un servicio y elija  **>Ver > Configuración**.
   Se muestra la vista Configuración de servicios del servicio seleccionado.

Vista rápida

Este es un ejemplo de la vista Configuración de servicios de un Decoder.



Este es un ejemplo de la vista Configuración de servicios de un Concentrator.



Temas

- Tema
- Funciones
- Editar el archivo de configuración de un servicio

Pestaña Configuración de servicios de dispositivos

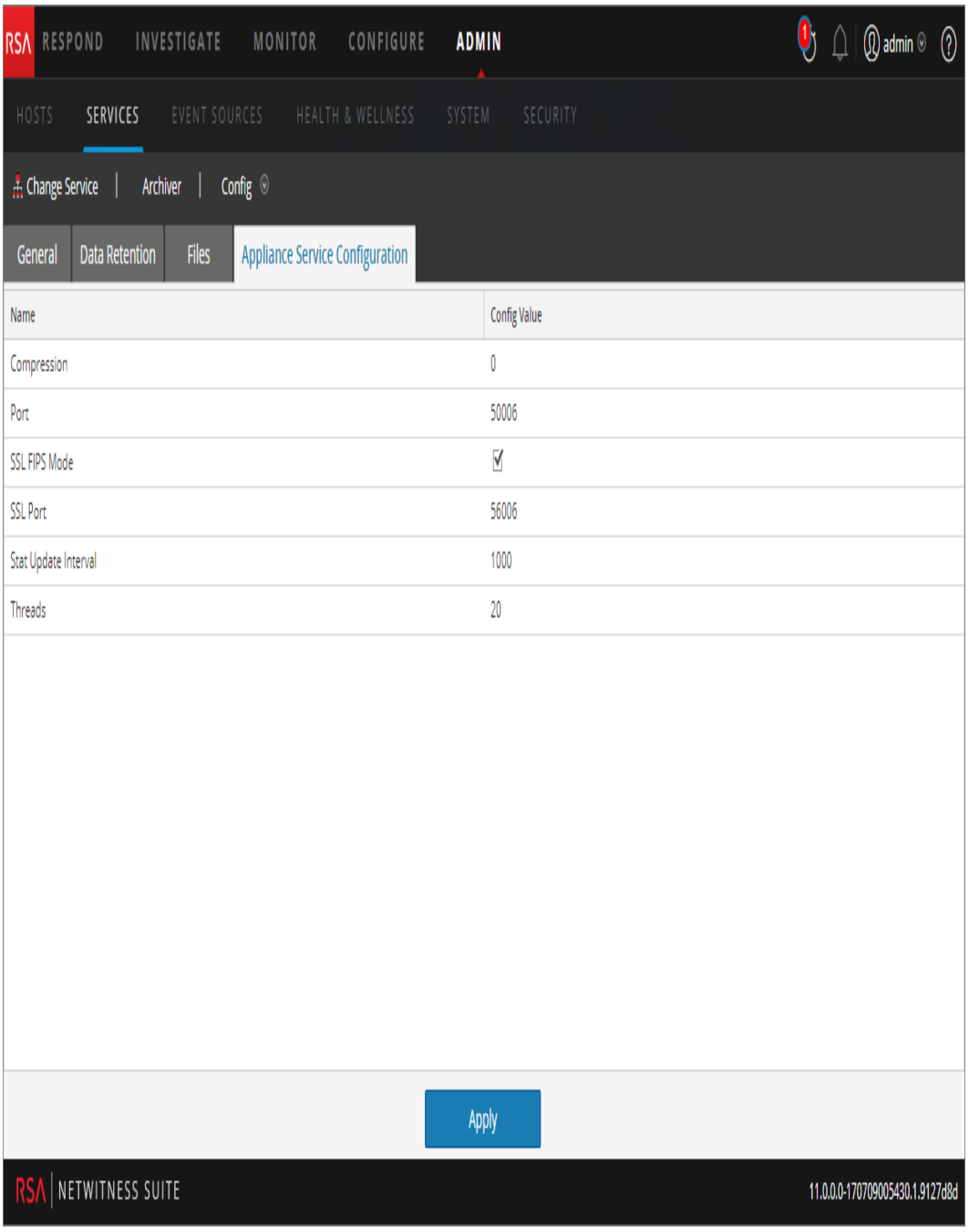
En este tema se enumeran y se describen los parámetros de configuración disponibles para el servicio NetWitness Suite Core Appliance. El servicio NetWitness Suite Core Appliance permite el monitoreo del hardware en hardware NetWitness heredado.

En la vista Configuración de los servicios Archiver, Broker, Concentrator, IPDB Extractor, Decoder, Log Collector o Log Decoder se incluye una pestaña Configuración de servicios de dispositivos.

Para acceder a la pestaña Configuración de servicios de dispositivos:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione un servicio y elija  **>Ver > Configuración**.
   Se muestra la vista Configuración de Servicios correspondiente al servicio Archiver.
3. Haga clic en la pestaña **Configuración de servicios de dispositivos**.

Este es un ejemplo de la pestaña Configuración de servicios de dispositivos correspondiente a un Archiver.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Archiver
Config
General
Data Retention
Files
Appliance Service Configuration
Name
Config Value
Compression
0
Port
50006
SSL FIPS Mode
SSL Port
56006
Stat Update Interval
1000
Threads
20
Apply
NETWITNESS SUITE
11.0.0.0-170709005430.1.9127d8d

Nombre	Descripción del valor de configuración	Cuándo surten efecto los cambios
Compresión	Comprime un mensaje cuando alcanza el número positivo (en bytes) que usted especifica.	La próxima vez que se conecta a este servicio.
Puerto	Puerto de escucha sin cifrar. **0** indica que el puerto está deshabilitado.	Después del reinicio del servicio.
Modo SSL FIPS	Uno de los parámetros que necesita para habilitar o deshabilitar los estándares de procesamiento de información federal (FIPS). Consulte “Activar o desactivar FIPS” en la Guía de mantenimiento del sistema RSA NetWitness® Suite para obtener instrucciones detalladas.	Después del reinicio del servicio.
Puerto SSL	Puerto de escucha de SSL (capa de conexión segura). **0** indica que el puerto está deshabilitado. SSL es la tecnología de seguridad estándar para establecer un vínculo cifrado entre un servidor web y un navegador. Este vínculo comprueba que todos los datos que se transmiten entre el servidor web y los navegadores mantengan sus características de privacidad e integridad.	Después del reinicio del servicio.

Nombre	Descripción del valor de configuración	Cuándo surten efecto los cambios
Intervalo de actualización de estadísticas	La frecuencia (en milisegundos) con la que el sistema actualiza los nodos de estadísticas para monitorear el estado y la condición.	De inmediato.
Subprocesos	Subprocesos en el pool de subprocesos que se deben usar para el manejo de solicitudes. El parámetro **Subprocesos** funciona en conjunto con el parámetro **Intervalo de sondeo** para los subprocesos de eventos y registros.	De inmediato.

Tema

Parámetros de configuración del servicio Appliance

Pestaña Calendarizador de retención de datos

En este tema se describen las opciones configurables de la pestaña Calendarizador de retención de datos para Decoder, Log Decoder y Concentrator.

La pestaña Calendarizador de retención de datos permite definir los criterios para quitar registros de bases de datos del almacenamiento primario en los servicios Decoder, Log Decoder y Concentrator, y programar el momento en que se comprobará el umbral.

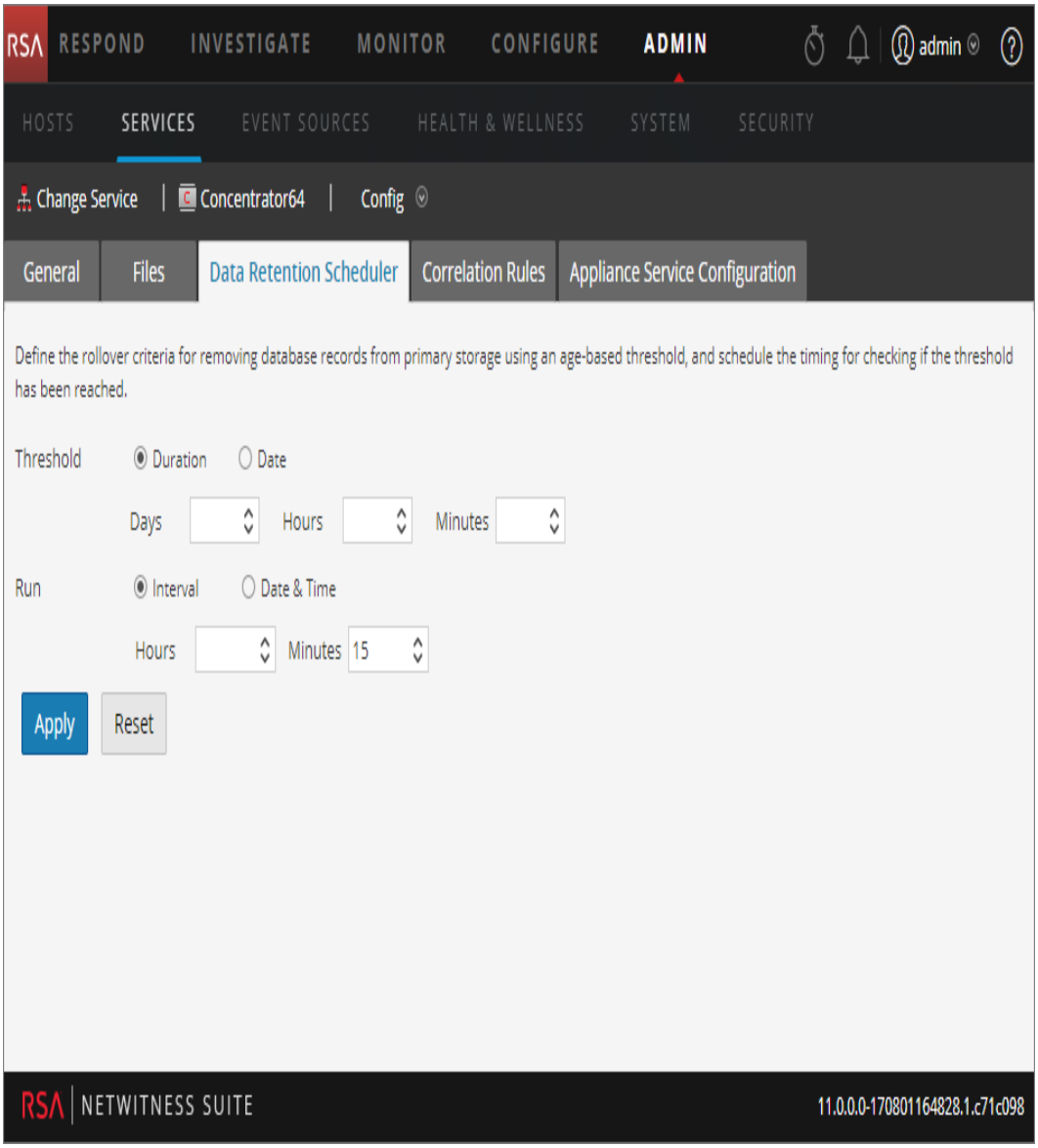
Para obtener información sobre la pestaña Retención de datos para Archiver, consulte el tema **Pestaña Retención de datos: Archiver** de la *Guía de configuración de Archiver*.

Nota: Si se necesita personalización adicional, se puede realizar mediante el Calendarizador de la pestaña Archivos en la vista Configuración de Servicios. Por ejemplo, si está disponible más almacenamiento para guardar los datos crudos que para los metadatos, puede tener más sentido usar Capacidad como el umbral y configurar distintos umbrales por base de datos (metadatos frente a paquete).

Para acceder a la pestaña Calendarizador de retención de datos:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un Decoder, un Log Decoder o un Concentrator y, a continuación, elija  **> Ver > Configuración**.
3. En la vista **Configuración de Servicios** correspondiente al servicio, haga clic en la pestaña **Calendarizador de retención de datos**.

En la siguiente figura se ilustran los parámetros de la pestaña Calendarizador de retención de datos de un Concentrator.



Funciones

La pestaña Calendarizador de retención de datos tiene secciones que permiten especificar los ajustes de los umbrales y de la ejecución. En la siguiente tabla se enumeran los parámetros compatibles con la configuración de la retención de datos.

Parámetro	Descripción
Umbral	El umbral se basa en la antigüedad de los datos, la cantidad de tiempo que han estado almacenados o la fecha en que se almacenaron. La fecha proviene del archivo de la base de datos, no de la hora de sesión real. • **Duration**: La cantidad de tiempo que pueden estar almacenados los datos antes de la eliminación. Especifica la cantidad de días (un máximo de 365), horas (un máximo de 24) y minutos (un máximo de 60) que han transcurrido desde el registro de fecha y hora en los datos. • **Fecha**: la eliminación de datos según la fecha del registro de fecha y hora. Especifique la fecha y la hora mensuales en los campos **Calendario** y **Hora**.
Ejecutar	El calendario para ejecutar el trabajo que comprueba los criterios de transferencia. • **Intervalo**: calendarice la comprobación de la base de datos para que se produzca en un intervalo regular. Especifique las **Horas** y los **Minutos** entre las comprobaciones calendarizadas. • **Fecha y hora**: Calendarice la comprobación de la base de datos para que se produzca en un día y una hora regulares. Especifica el día en la lista desplegable y la hora del reloj del sistema en formato `hh:mm:ss`. Los valores posibles para el día son **Todos los días**, **Días de la semana**, **Fines de semana** y **Personalizado**. La opción **Personalizado** permite seleccionar uno o más días específicos de la semana.
Aplicar	Sobrescribe cualquier programa anterior para este servicio y aplica la nueva configuración de inmediato. **Precaución:** una vez que se aplica esta configuración y se alcanza el umbral, los datos antiguos se eliminan de la base de datos y ya no se puede acceder a ellos.

Parámetro	Descripción
Restablecer	Restablece el calendario al último estado aplicado.

Pestaña Archivos

En este tema se describen los archivos de configuración de servicios que se pueden ver en la vista Configuración de servicios > pestaña Archivos.

La pestaña Archivos de la vista Configuración de servicios es la interfaz del usuario para editar archivos de configuración de servicios, por ejemplo, Decoders, Log Decoders, Brokers, Archivers y Concentrators, como archivos de texto.

Los archivos disponibles para editar varían según el tipo de servicio que se configura. Los archivos comunes a todos los servicios Core son:

- El archivo del índice del servicio.
- El archivo de netwitness.
- El archivo del generador de informes de fallas.
- El archivo del programador.
- El archivo de definiciones de feeds.

Además, el Decoder tiene archivos que configuran los analizadores, las definiciones de feed y un adaptador de LAN inalámbrica.

Nota: Los valores predeterminados en estos archivos de configuración son, por lo general, aptos para las situaciones más comunes. Sin embargo, es necesario realizar tareas de edición para los servicios opcionales, como el generador de informes de fallas generales o el programador. Solo los administradores que comprenden ampliamente las redes y los factores que afectan la forma en que los servicios recopilan y analizan datos deben realizar cambios en estos archivos en la pestaña Archivos.

Encontrará más detalles sobre los parámetros de configuración de servicios en Ajustes de configuración de servicios.

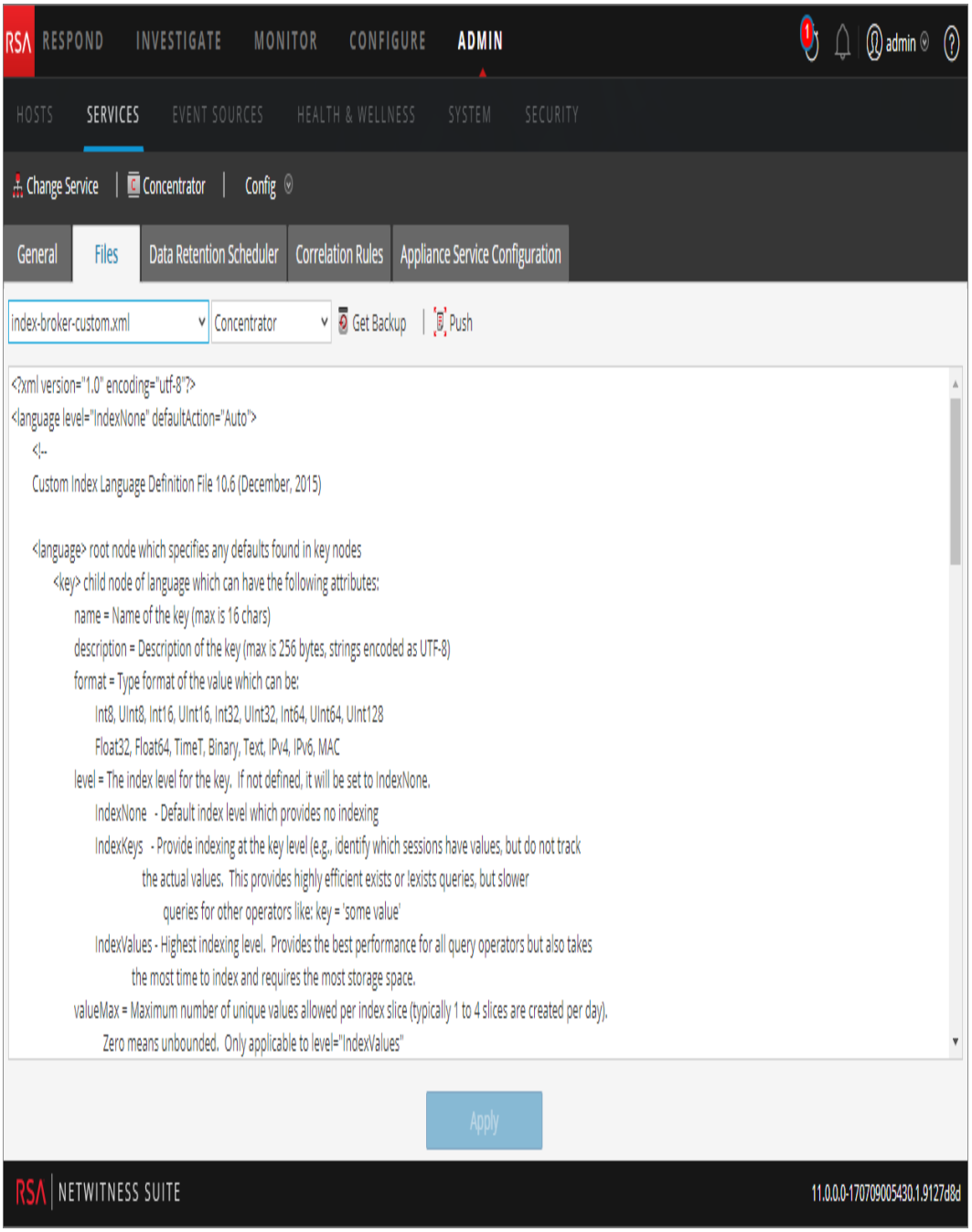
Para acceder a la pestaña Archivos:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y elija  **> Ver > Configuración**.
   La vista Configuración de servicios se muestra con la pestaña **General** abierta.
3. Haga clic en la pestaña **Archivos**.

Función	Deseo…
Administrador	Editar el archivo de configuración de un servicio.

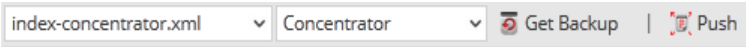
Editar el archivo de configuración de un servicio

Este es un ejemplo de la pestaña Archivos.



Barra de herramientas de la pestaña Archivos

La pestaña Archivos tiene una barra de herramientas y una ventana de edición. Este es un ejemplo de la barra de herramientas.



Estas son las funcionalidades de la barra de herramientas de la pestaña Archivos.

Función	Descripción
Lista desplegable **Archivo**	Muestra una lista de archivos que el sistema está utilizando actualmente. Cuando selecciona un archivo, el texto del archivo aparece en la ventana de edición de texto. En la ventana de texto, puede editar el archivo y guardar los cambios o crear archivos alternativos para utilizar.
Lista desplegable **Servicio/Host**	Muestra el tipo de servicio y el host. Puede abrir un archivo desde el servicio o desde el host para editarlo.
Get Backup	Recupera el respaldo del archivo actual más reciente, que puede resultar útil si ha hecho cambios y desea volver a la versión anterior del archivo. El respaldo no reemplaza el archivo actual a menos que haga clic en **Guardar**.
Push	Muestra un cuadro de diálogo donde puede seleccionar servicios del mismo tipo y migrar el archivo que se ve actualmente a los servicios.
Aplicar	Sobrescribe el archivo actual, crea un archivo de respaldo.

Vista Explorar de Servicios

En este tema se presentan las funciones de la vista Explorar de Servicios de NetWitness Suite, una interfaz del usuario eficiente y flexible para ver y editar configuraciones de hosts y servicios.

La vista Explorar de los servicios ofrece acceso y control avanzados de todos los hosts y los servicios de NetWitness Suite. Todos los servicios muestran su funcionalidad mediante una serie de nodos en forma de árbol, similar a la vista del Explorador de Windows del sistema de archivos. Aquí puede:

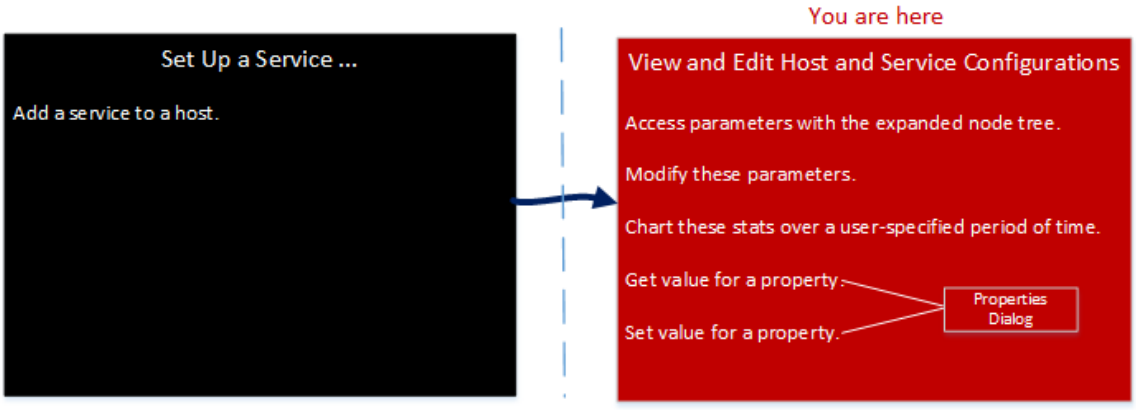
- Ver un árbol de directorios que muestra los archivos comunes de todos los servicios seleccionados.
- Navegar por el directorio hasta un archivo.
- Abrir el mismo archivo para cada servicio y mostrar los contenidos lado a lado.
- Seleccionar una entrada en el archivo y editar el valor.
- Aplicar un valor de propiedad de un servicio a otros servicios.

La vista Explorar de los servicios también puede mostrar un cuadro de diálogo Propiedades, una interfaz simple para ver las propiedades de cualquier nodo del sistema y enviar mensajes al nodo, como se muestra en la siguiente figura.

Precaución: cuando se edita en esta vista, se requiere una buena compresión de los nodos y los parámetros. Los ajustes incorrectos pueden provocar problemas de rendimiento.

Flujo de trabajo

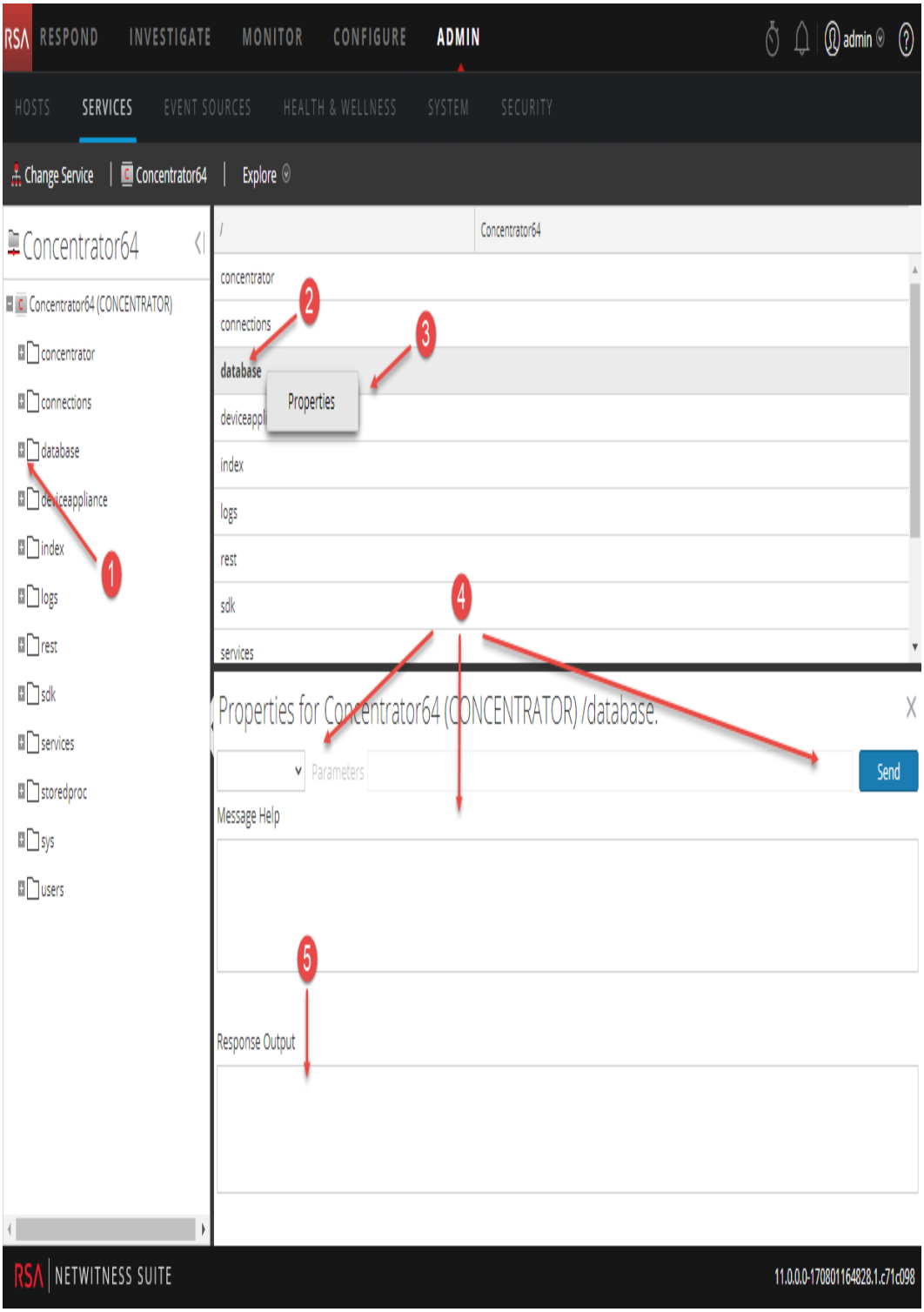
En este flujo de trabajo se muestran las tareas que se realizan en la vista Explorar.



Vista rápida

Para acceder a la vista Explorar servicios:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y elija > **Ver** > **Explorar**.



1. Expanda el nodo para mostrar sus categorías de parámetros.
2. Haga clic en una propiedad (por ejemplo, **meta.dir**) para seleccionarla.
3. Haga clic con el botón secundario en un nodo o en una categoría y, a continuación, haga clic en **Propiedades** para mostrar el cuadro de diálogo Propiedades.
4. Realice una operación en un nodo o una categoría:
   a. Seleccione un comando en la lista desplegable.
   b. Escriba una cadena de comandos (si es necesario).
   c. Haga clic en **Enviar**.
5. Revise la salida.

Funciones

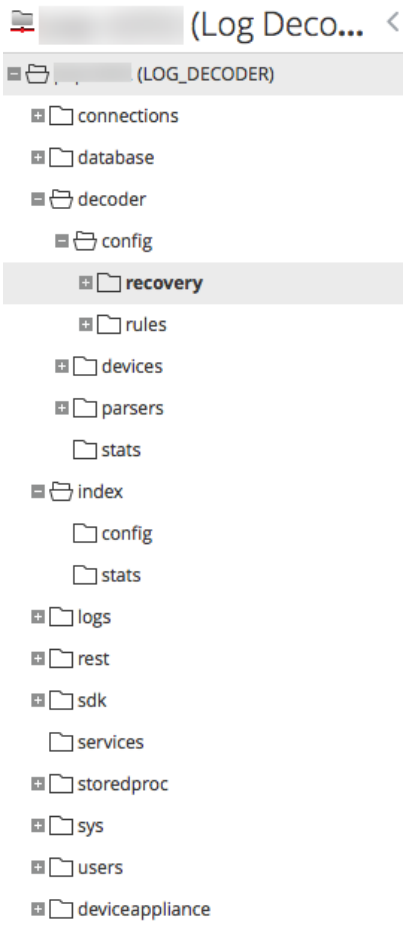
La **vista Explorar servicios** tiene dos paneles principales:

- La lista Nodo
- El panel Monitor

Puede acceder a las Propiedades de cualquier archivo si hace clic con el botón secundario en el archivo y selecciona Propiedades.

La lista Nodo

La lista Nodo muestra los servicios como una serie de nodos y carpetas en forma de árbol. Los niveles en la lista Nodo se expanden y contraen para mostrar la jerarquía completa.



Cada carpeta raíz se nombra según la funcionalidad que expone. Por ejemplo, la carpeta **/conexiones** muestra todas las direcciones IP conectadas. Debajo de cada **Dirección IP/puerto** hay dos carpetas, **sesiones** y **estadísticas**.

- La carpeta **sesiones** muestra todas las sesiones de usuario autenticadas que se originan desde la dirección IP/puerto.
- La carpeta **estadísticas** muestra los valores, como la cantidad de mensajes enviados/recibidos, los bytes enviados/recibidos y otros valores establecidos por el servicio. No se pueden editar.

Cuando se selecciona cualquier carpeta en la vista de árbol, se muestran sus objetos secundarios en el panel **Monitor**. Cada nodo del árbol se monitorea de manera activa, por lo que cuando un nodo de estadísticas o configuración cambia de valor, se refleja inmediatamente en el árbol y el panel de monitor.

El panel Monitor

El panel **Monitor** muestra las propiedades y los valores de un nodo seleccionado (como el **índice**) y una carpeta secundaria (como **configuración**). Hay dos formas de editar valores:

- Hacer clic en el valor y escribir un valor nuevo
- Enviar un mensaje **set** en el cuadro de diálogo Propiedades

/Index/Config	(Concentrator)
index.dir	/var/netwitness/concentrator/index=7.08 GB
index.dir.cold	
index.dir.warm	
page.compression	huffhybrid
save.session.count	0

Temas

- Funciones
- Introducción de hosts: Parámetros de configuración del servicio Log Decoder

Cuadro de diálogo Propiedades

En este tema se explica cómo enviar mensajes a un nodo de sistema en la vista Explorar servicios > cuadro de diálogo Propiedades.

El cuadro de diálogo Propiedades se abre debajo del panel Monitor cuando selecciona Propiedades en el menú contextual. El cuadro de diálogo Propiedades proporciona una herramienta de mensajería fácil de usar para comunicarse con los nodos de sistema. Esto es útil para obtener y establecer valores de una propiedad para varios servicios.

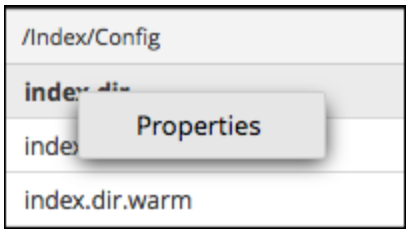
Todos los nodos soportan el mensaje de ayuda, el cual contiene:

- Una descripción del nodo.
- La lista de mensajes soportados con su descripción correspondiente.
- Las funciones de seguridad necesarias para obtener acceso a los mensajes.

Los mensajes disponibles pueden variar según el servicio y la carpeta raíz. También se puede acceder a muchos de estos mensajes como opciones con un tablero o vista de NetWitness Suite.

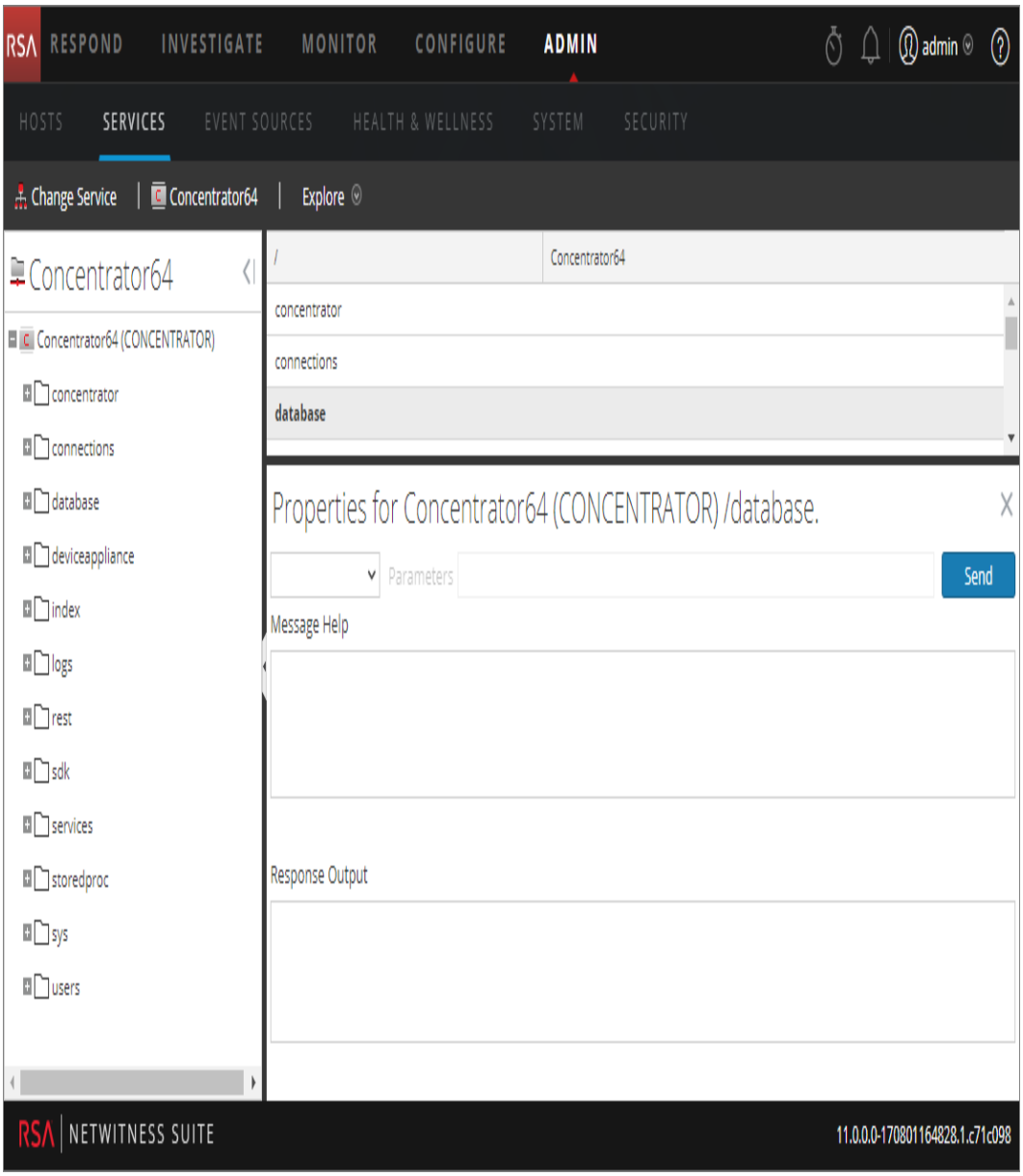
Para obtener acceso al cuadro de diálogo Propiedades:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y elija  **> Ver > Explorar**.
3. En la lista **Nodo**, seleccione un archivo.
4. En el panel **Monitor**, haga clic con el botón secundario en una propiedad y seleccione **Propiedades**.



Se muestra el cuadro de diálogo Propiedades. También puede hacer clic con el botón secundario en cualquier archivo de la lista Nodo para mostrar el cuadro de diálogo Propiedades.

El siguiente es un ejemplo del cuadro de diálogo Propiedades con ayuda para un mensaje (**información**) que se muestra.



Funciones

El cuadro de diálogo Propiedades tiene las siguientes funcionalidades.

Función	Descripción
Lista desplegable **Mensaje**	Muestra todos los mensajes disponibles para un nodo actual. Seleccione un mensaje para enviar a un nodo.
Campo de entrada **Parámetros**	Escriba los parámetros de mensaje en este campo.
Botón **Enviar**	Envía el mensaje al nodo.
Ayuda de mensaje	Muestra el texto de ayuda para el mensaje actual.
Salida de respuesta	Muestra la respuesta a un mensaje o resultado desde un mensaje.

Vista Registros de servicios

En este tema se presenta la vista Registros de servicios.

La vista Registros de servicios proporciona la capacidad para ver y buscar los registros de un servicio específico. La vista Registros de servicios es idéntica al panel Registro de sistema con dos excepciones:

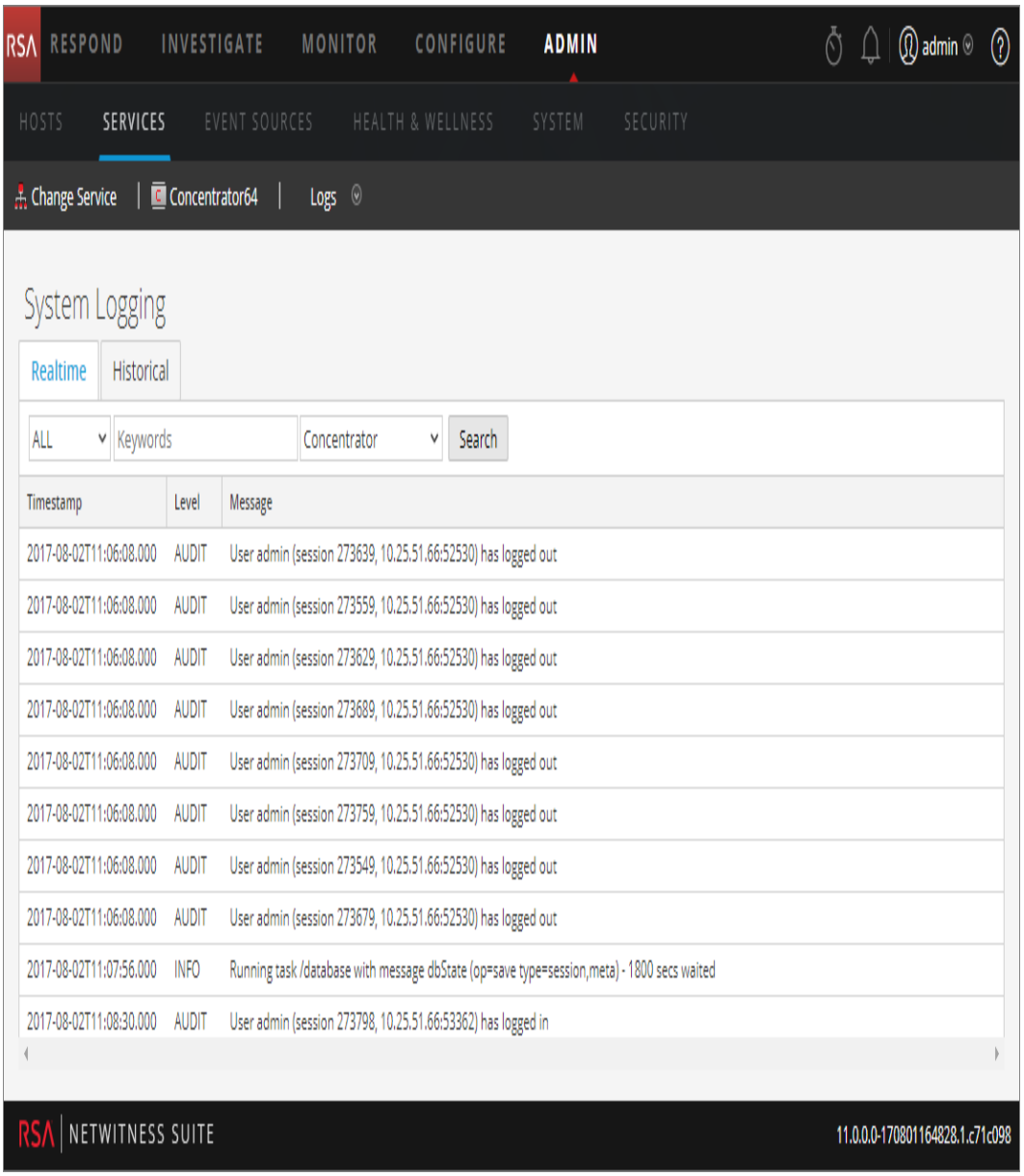
- La vista Registros de servicios tiene un filtro adicional para seleccionar mensajes del servicio o del host.
- El panel Registro de sistema tiene una pestaña adicional para Configuración.

Consulte Panel Registro de sistema para ver una descripción completa de las funciones del registro de NetWitness Suite.

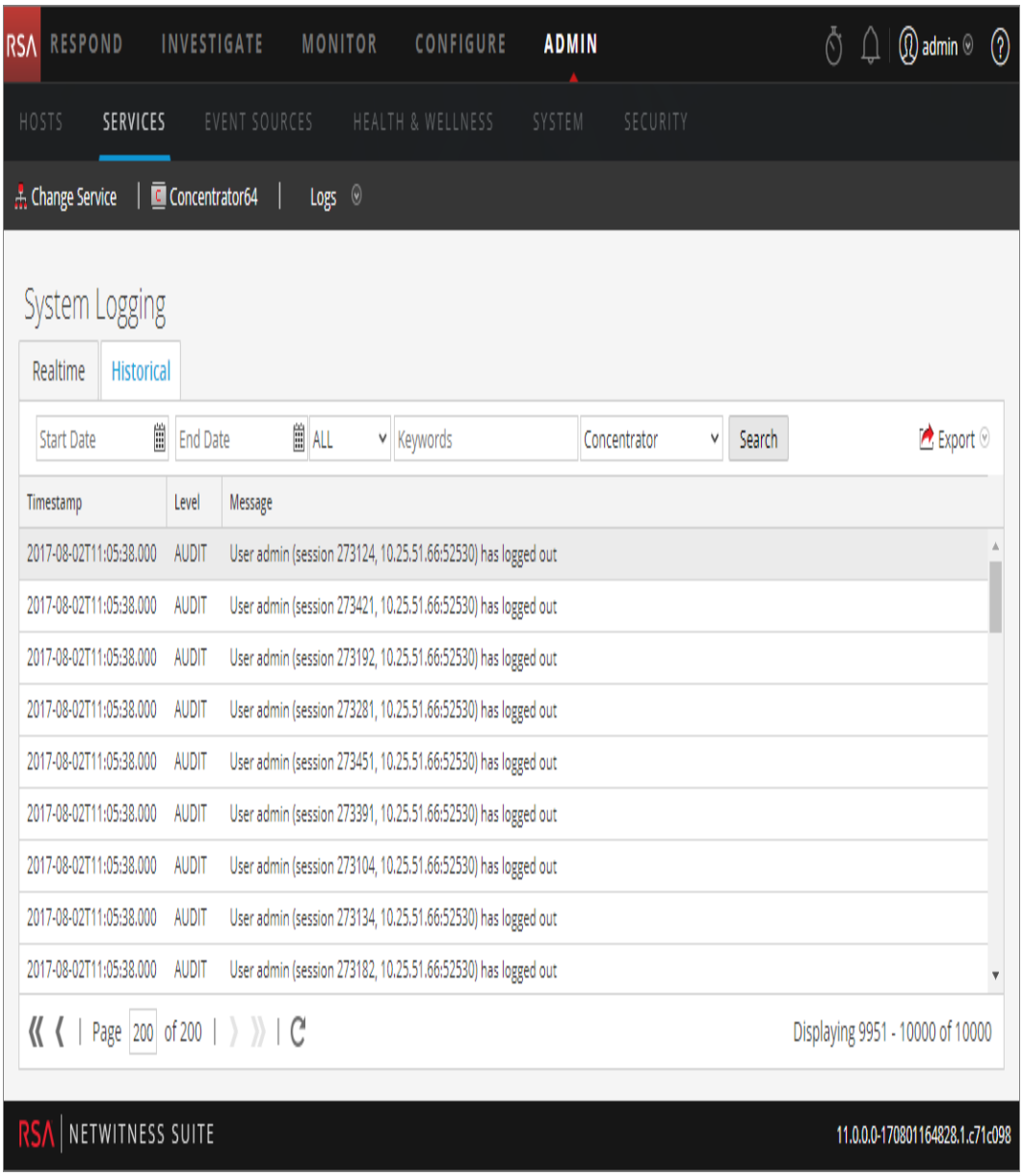
Para ver un registro de servicio:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y elija  **>Ver > Registros**.

En la siguiente figura se muestra la pestaña Tiempo real de la vista Registros de servicios.



En la siguiente figura se muestra la pestaña Historial de la vista Registros de servicios.



Funciones

El panel Registro de sistema tiene las siguientes pestañas y las funciones de registro se describen como parte del mantenimiento del sistema (consulte **Monitorear el estado y la condición de Security Analytics** en la guía *Mantenimiento del sistema*).

Función	Descripción
Pestaña Tiempo real	Este es el modo monitor del registro de servicio.
Pestaña Historial	Esta es una vista que se puede buscar del registro de servicio.

Vista Seguridad de servicios

En este tema, se proporciona una descripción general de la administración de seguridad del servicio en la vista Seguridad de servicios.

En NetWitness Suite, cada servicio tiene una configuración independiente de los usuarios, las funciones y los permisos de función, los cuales se administran en la vista Seguridad de servicios.

Para acceder a información sobre los servicios y realizar operaciones de servicios mediante NetWitness Suite, un usuario debe pertenecer a una función que tenga permisos para ese servicio. Para los servicios NetWitness Suite Core 10.4 o superiores que usan conexiones de confianza, ya no es necesario crear cuentas de usuario de NetWitness Suite Core para los usuarios que inician sesión a través del cliente web. Solo debe crear cuentas de usuario de NetWitness Suite Core para agregación, usuarios de clientes gruesos y usuarios de la API REST.

Nota: Solo el usuario administrador predeterminado en NetWitness Suite se crea de manera predeterminada en todos los servicios. Como requisito previo para administrar la seguridad de un servicio, la cuenta de usuario administrador predeterminada debe estar presente en Administration > vista Servicios de NetWitness Suite. Para el resto de los usuarios, debe configurar el acceso a cada servicio en especial por medio de NetWitness Suite.

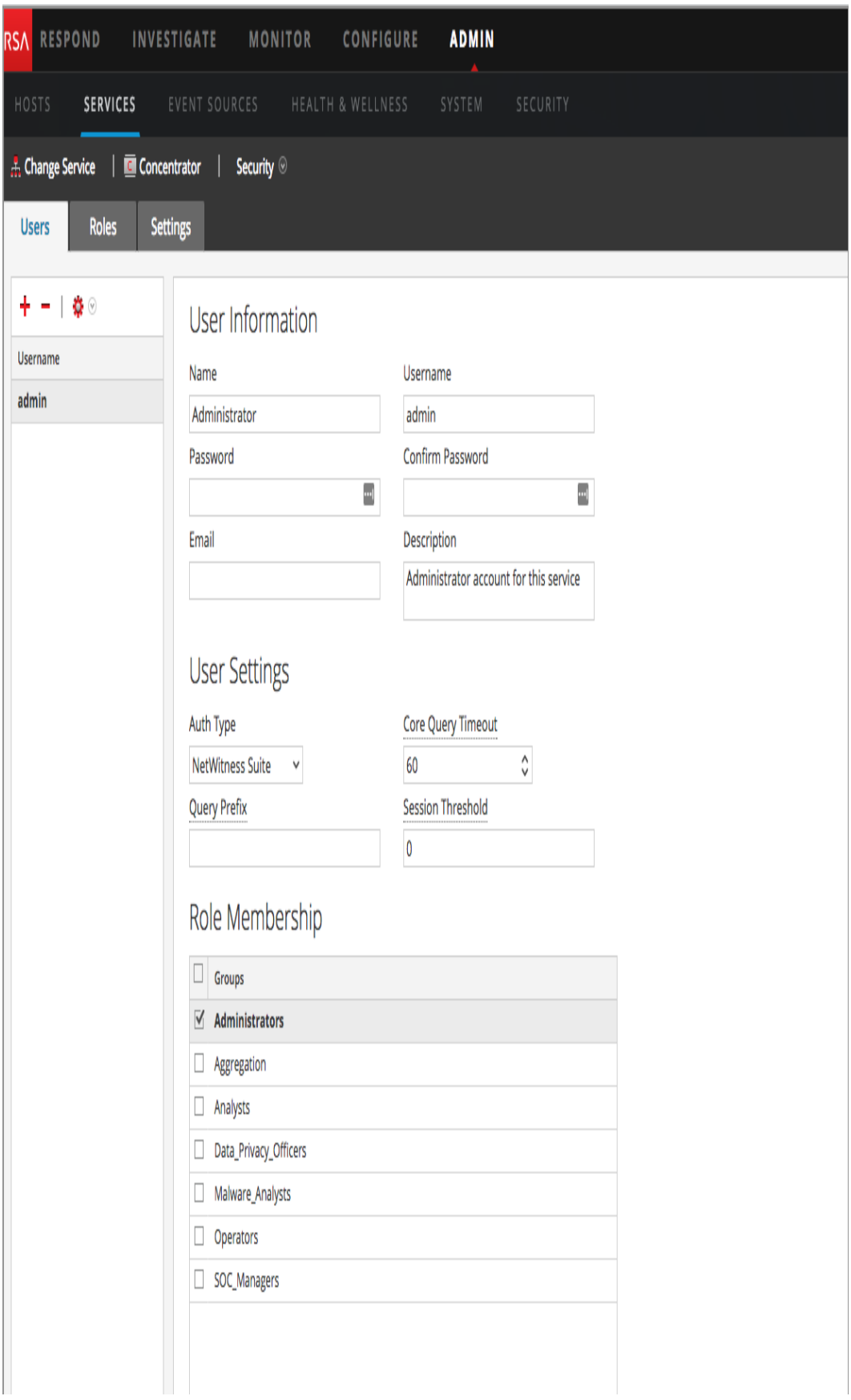
Los procedimientos relacionados con esta pestaña se describen en Introducción de hosts: Procedimientos de hosts y servicios.

Para acceder a la vista Seguridad de servicios:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios.**

2. Seleccione un servicio y elija  > **Ver > Seguridad**.

   Se muestra la vista Seguridad de Servicios correspondiente al servicio seleccionado.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Concentrator
Security
Users
Roles
Settings
Username
admin
User Information
Name
Administrator
Username
admin
Password
Confirm Password
Email
Description
Administrator account for this service
User Settings
Auth Type
NetWitness Suite
Core Query Timeout
60
Query Prefix
Session Threshold
0
Role Membership
Groups
Administrators
Aggregation
Analysts
Data_Privacy_Officers
Malware_Analysts
Operators
SOC_Managers

Funciones

La vista Seguridad de servicios tiene tres pestañas, la pestaña Usuarios, la pestaña Funciones y la pestaña Configuración.

Funciones y acceso al servicio

Las consideraciones primarias para configurar la seguridad del servicio son definir las funciones y asignar usuarios a las funciones. La vista Seguridad del servicio separa estas dos funciones en la pestaña Usuarios y la pestaña Funciones.

- En la pestaña Funciones, puede crear funciones y asignar permisos a las funciones para un servicio seleccionado.
- La pestaña Usuarios permite agregar un usuario, editar la configuración del usuario, cambiar la contraseña del usuario y editar la membresía en función del usuario para un servicio seleccionado. Aunque seleccione un único servicio en la vista Seguridad de servicios, puede aplicar la configuración de un servicio a otros servicios.

Temas

- Pestaña Funciones
- Funciones y permisos de los usuarios de servicios
- Función Agregación
- Pestaña Ajustes de configuración
- Pestaña Usuarios

Pestaña Funciones

En este tema se presentan las funcionalidades de la vista Seguridad de servicios > pestaña Funciones.

La pestaña **Funciones** permite crear funciones y asignar permisos. Cada función puede tener diferentes permisos para diferentes servicios. Por ejemplo, la función Analistas puede tener diferentes permisos de función basados en el servicio seleccionado.

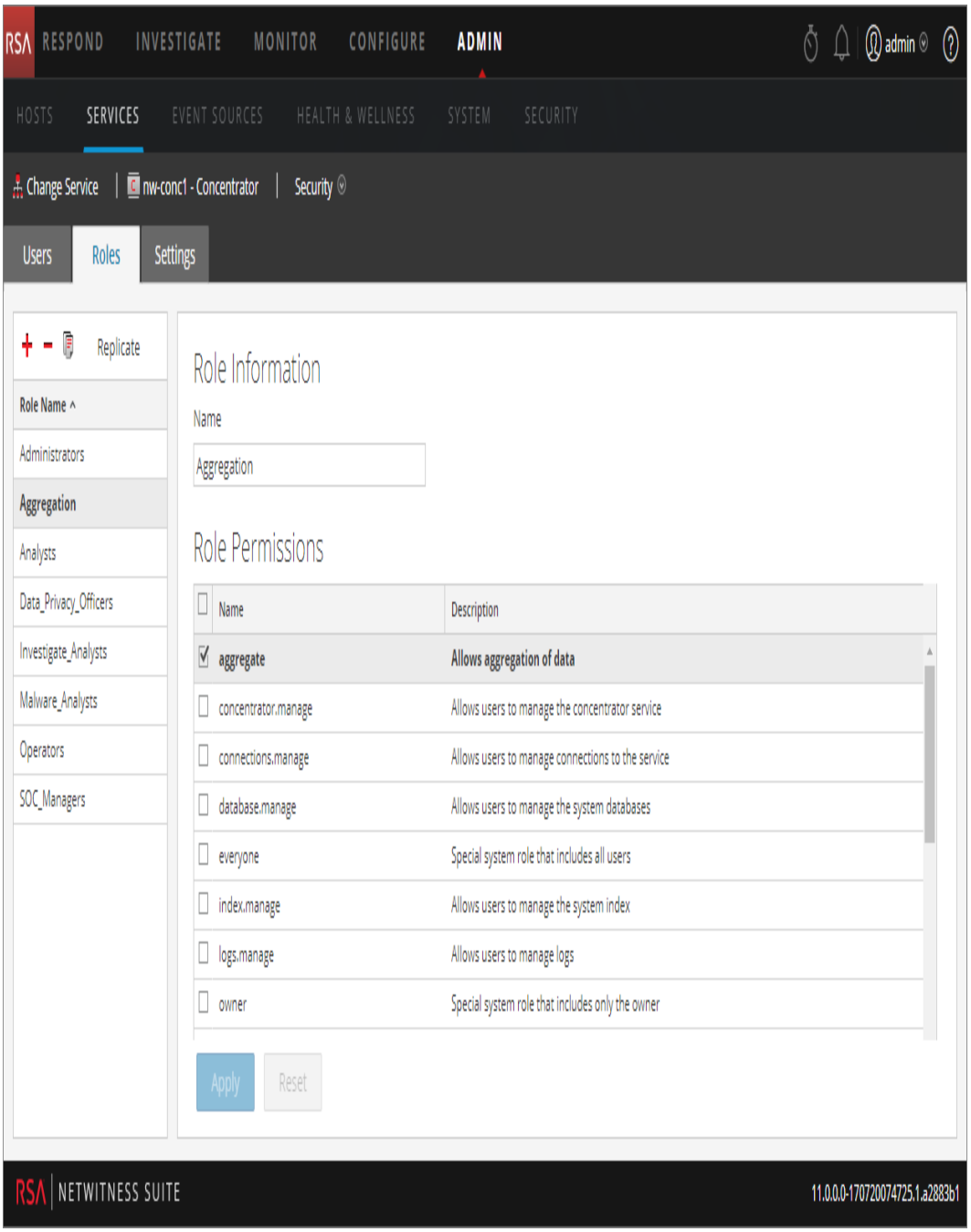
Antes de agregar usuarios a funciones, es necesario definir las funciones de los usuarios, por lo general por funcionalidad, y asignar permisos a las funciones.

Los procedimientos relacionados con esta pestaña se describen en Introducción de hosts: Procedimientos de hosts y servicios.

Para mostrar la **vista Seguridad de servicios > pestaña Funciones**:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios.**
2. Seleccione un servicio en el cual desee agregar un usuario y elija  **> Ver > Seguridad**.
3. Seleccione la pestaña **Funciones**.

En la figura siguiente se muestra la pestaña Funciones de la vista Seguridad de servicios.



Funciones

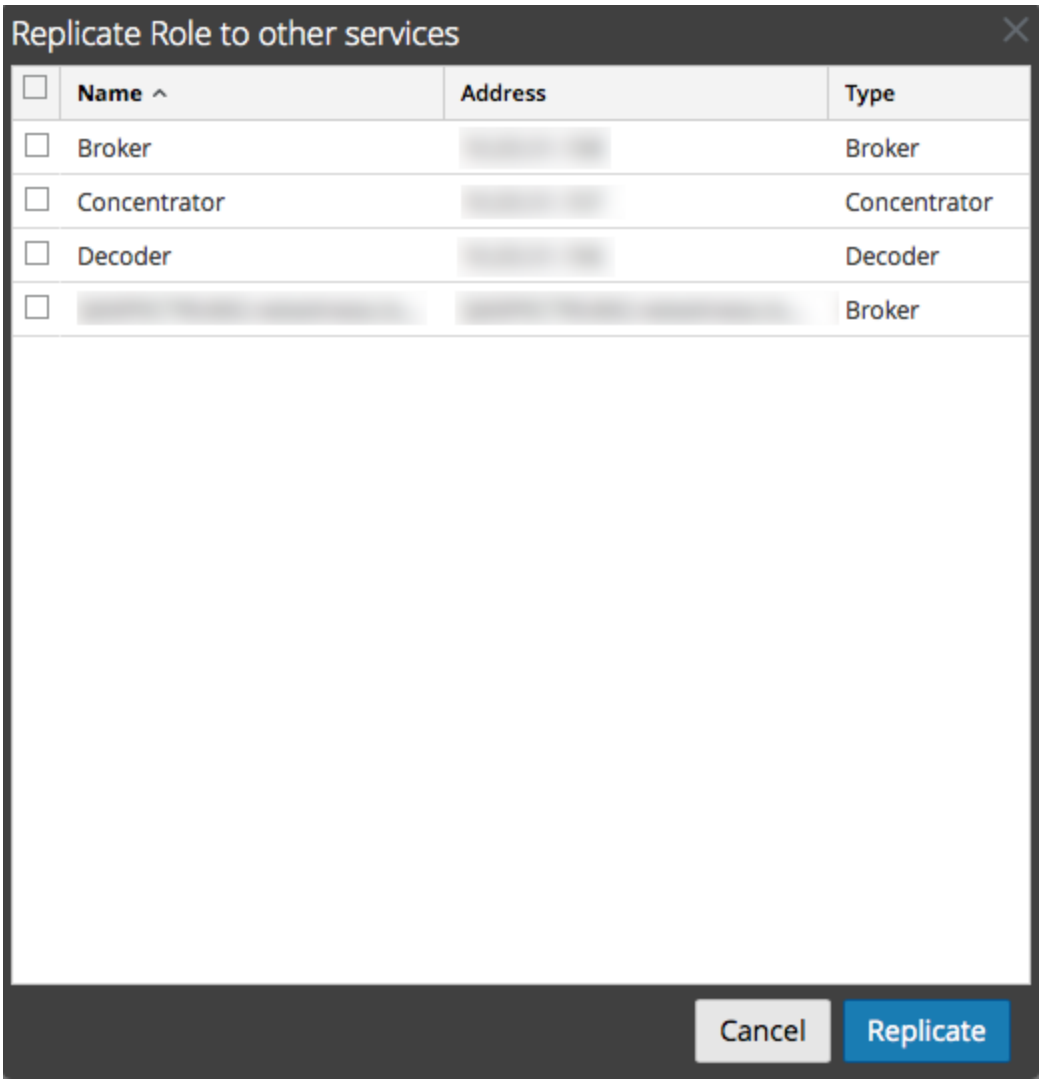
La pestaña Funciones contiene el panel **Nombre de la función** a la izquierda. Cuando selecciona un nombre de función, se muestra el panel **Información de la función** para la función seleccionada a la derecha.

Panel Nombre de la función

El panel **Nombre de la función** tiene las siguientes funciones.

Función	Descripción
	Agrega un grupo nuevo al servicio actual.
	Elimina el grupo seleccionado del servicio actual.
	Copia una función y los permisos asignados en una función nueva. El nombre de la función nueva debe ser único. Por ejemplo, puede copiar la función **Analistas** y crear otra función con un nombre nuevo, como **Analyst_Managers**.
Replicar	Migra una función y los permisos asignados a otros servicios. Después de seleccionar una función y hacer clic en **Replicar**, se muestra el cuadro de diálogo **Replicar función a otros servicios**. En el cuadro de diálogo, puede seleccionar los servicios en los que desea replicar la función.

En la siguiente figura se muestra el cuadro de diálogo **Replicar función a otros servicios**.



Panel Información de la función y permisos

El panel **Información de la función y permisos** define permisos de función.

Existen dos botones:

- El botón **Aplicar** guarda los cambios realizados en el panel Permisos de función y se implementan de inmediato.
- Si no ha guardado los cambios en el panel Permisos de función, el botón **Restablecer** restablece todos los campos y ajustes a sus valores previos a la edición.

Funciones y permisos de los usuarios de servicios

En este tema se describen las funciones y los permisos preconfigurados de los usuarios de servicios.

La pestaña Funciones de la vista Seguridad de los servicios permite crear funciones de usuarios de servicios y asignar permisos. También puede usar funciones preconfiguradas que se incluyen con NetWitness Suite para asignar permisos de usuario.

Funciones de usuarios de servicios

NetWitness Suite incluye las siguientes funciones preconfiguradas de usuarios de servicios.

Función	Permisos asignados	Personal/cuenta
Administradores	Todos los permisos	Administrador del sistema NetWitness Suite
Agregación	aggregate sdk.content sdk.meta sdk.packets	Puede usar esta función para crear una cuenta de agregación. Esta función proporciona los permisos mínimos necesarios para ejecutar la agregación de datos. Solo está disponible en servicios de NetWitness Suite 10.5 y superiores.
Analistas, Malware_ Analysts y SOC_Managers	sdk.meta sdk.content sdk.packets storedproc.execute	Los usuarios pueden usar aplicaciones específicas, ejecutar consultas y ver contenido con fines de análisis.
Data_Privacy_ Officers	sys.manage users.manage sdk.meta sdk.content sdk.packets sdk.manage logs.manage database.manage index.manage dpo.manage	Encargado de la privacidad de datos Los Encargados de la privacidad de datos tienen el permiso dpo.manage en Decoders y Log Decoders.

Función	Permisos asignados	Personal/cuenta
Operadores	sys.manage services.manage connections.manage users.manage logs.manage parsers.manage rules.manage database.manage index.manage sdk.manage decoder.manage archiver.manage concentrator.manage storedproc.manage	Los operadores son responsables de la operación diaria de los servicios.

Permisos de usuarios de servicios

Puede asignar muchos permisos a una función de servicio en NetWitness Suite. Los usuarios pueden tener distintos permisos en cada servicio según sus asignaciones de funciones y los permisos seleccionados para cada función. En esta tabla se describen los permisos que puede asignar a una función.

Permiso	Definición
sys.manage	Permite que el usuario edite los ajustes de configuración de los servicios.
services.manage	Permite que el usuario administre las conexiones a otros servicios.
connections.manage	Permite que el usuario administre las conexiones al servicio.
users.manage	Permite que el usuario cree usuarios individuales y funciones de usuario, y que especifique permisos de usuario.

Permiso	Definición
aggregate	Permite que el usuario ejecute la agregación de datos.
sdk.meta	Permite que el usuario ejecute consultas en las aplicaciones Investigation y Reporting, y que vea los metadatos que devuelve la consulta.
sdk.content	Permite que el usuario acceda a registros y paquetes crudos desde cualquier aplicación cliente (Investigation y Reporting).
sdk.packets	Permite que los usuarios accedan a registros y paquetes crudos desde cualquier aplicación cliente.
appliance.manage	Permite que el usuario administre las tareas del dispositivo (host). El servicio Appliance requiere este permiso.
decoder. manage	Permite que el usuario edite los ajustes de configuración del servicio Decoder.
concentrator.manage	Permite que el usuario edite los ajustes de configuración del servicio Concentrator/Broker.
logs.manage	Permite que el usuario vea los registros del servicio y que edite los ajustes de configuración del registro para el servicio especificado.
parsers.manage	Permite que el usuario administre todos los atributos bajo el nodo parsers.
rules.manage	Permite que el usuario agregue y elimine todas las reglas.
database.manage	Permite que el usuario configure ubicaciones de bases de datos, tamaños y los diversos ajustes de configuración para la sesión, los metadatos y/o las bases de datos de paquete/registros.
index.manage	Permite que el usuario administre todos los atributos relacionados con índices.

Permiso	Definición
sdk.manage	Permite que el usuario vea y configure todos los elementos de configuración de SDK.
storedproc.execute	Permite que el usuario ejecute un procedimiento almacenado Lua.
storedproc.manage	Permite que el usuario administre procedimientos almacenados Lua.
archiver.manage	Permite que el usuario modifique la configuración de Archiver.
dpo.manage	Permite que el usuario administre la configuración de la transformación y las claves aplicables.

Función Agregación

En este tema se describe la función Agregación y los permisos con los cuales los usuarios de servicios pueden ejecutar una agregación.

La función Agregación es una función de usuario de servicios destinada únicamente a la agregación de datos. Tiene los permisos de función mínimos necesarios para ejecutar una agregación:

- aggregate
- sdk.meta
- sdk.packets
- sdk.content

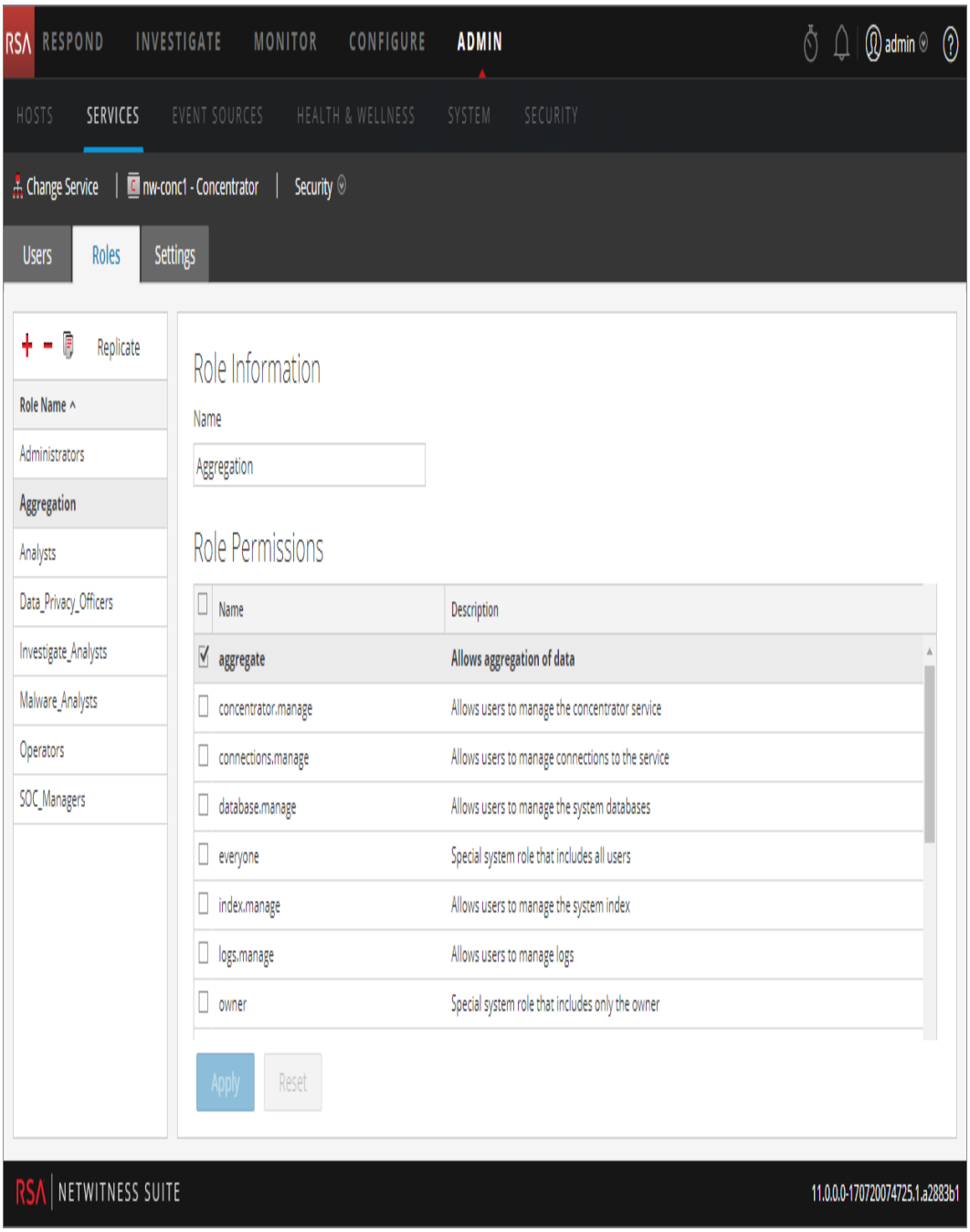
La función Agregación está disponible solo en servicios de NetWitness Suite 10.5 y superiores, y se puede usar para una cuenta de agregación. Los miembros de esta función o los usuarios de servicios con estos permisos pueden ejecutar la agregación en Decoders, Concentrators, Archivers y Brokers. El permiso **aggregate** permite que los usuarios de servicios ejecuten la agregación de sesiones y metadatos junto con registros y paquetes crudos.

Puede usar los permisos decoder.manage, concentrator.manage y archiver.manage, pero los permisos de la función Agregación permiten únicamente la agregación e impiden las otras operaciones disponibles.

Se accede a las funciones de servicio desde ADMIN > Servicios (seleccione un servicio) > Acciones > Ver > Seguridad > pestaña Funciones.

Los procedimientos pertinentes a las funciones se describen en Introducción de hosts: Procedimientos de hosts y servicios. En Funciones y permisos de los usuarios de servicios se proporciona información detallada sobre las funciones preconfiguradas.

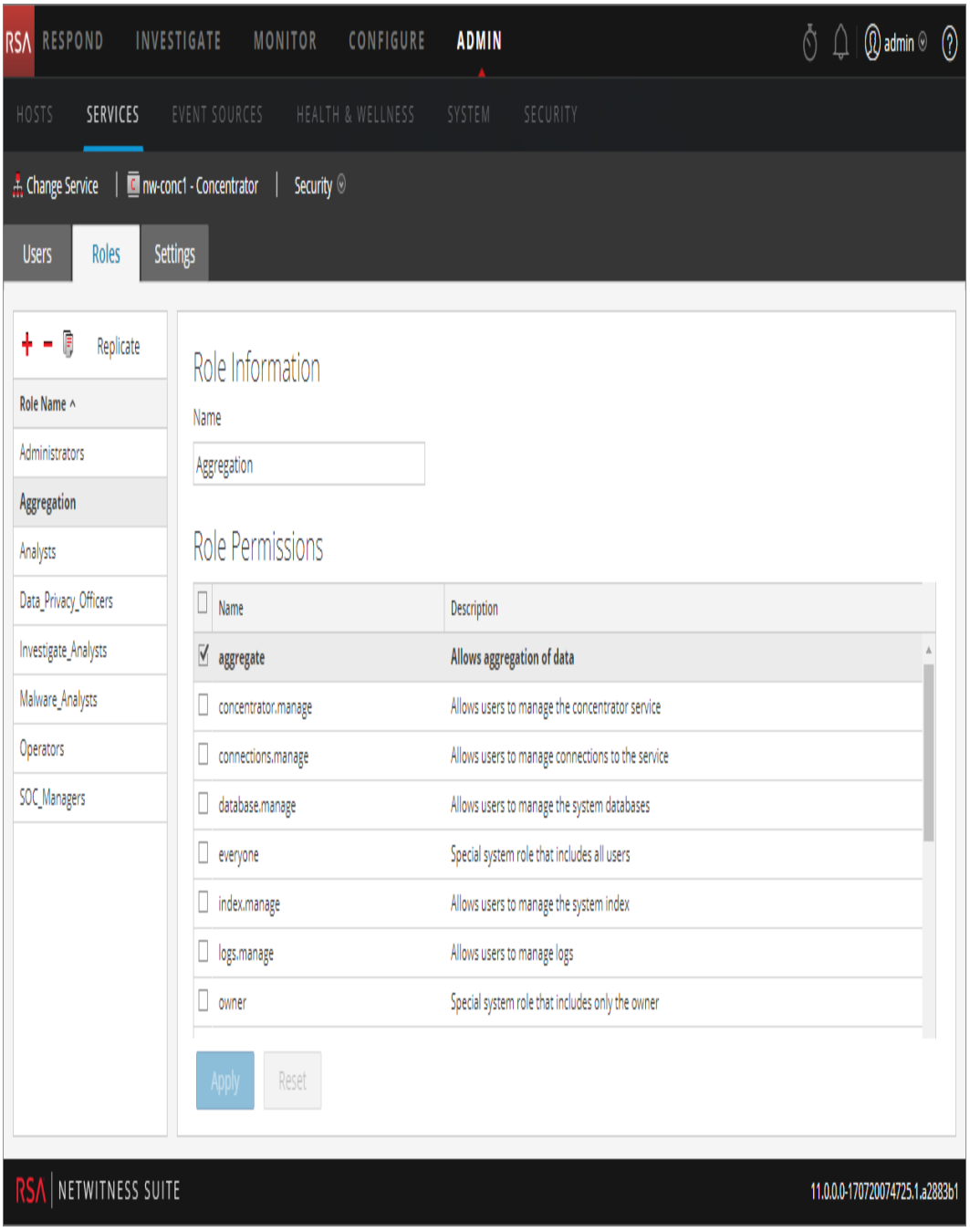
En la siguiente figura se muestran los permisos de la función Agregación.



Pestaña Ajustes de configuración

En este tema se describen las funciones de la vista Seguridad de servicios > pestaña Configuración.

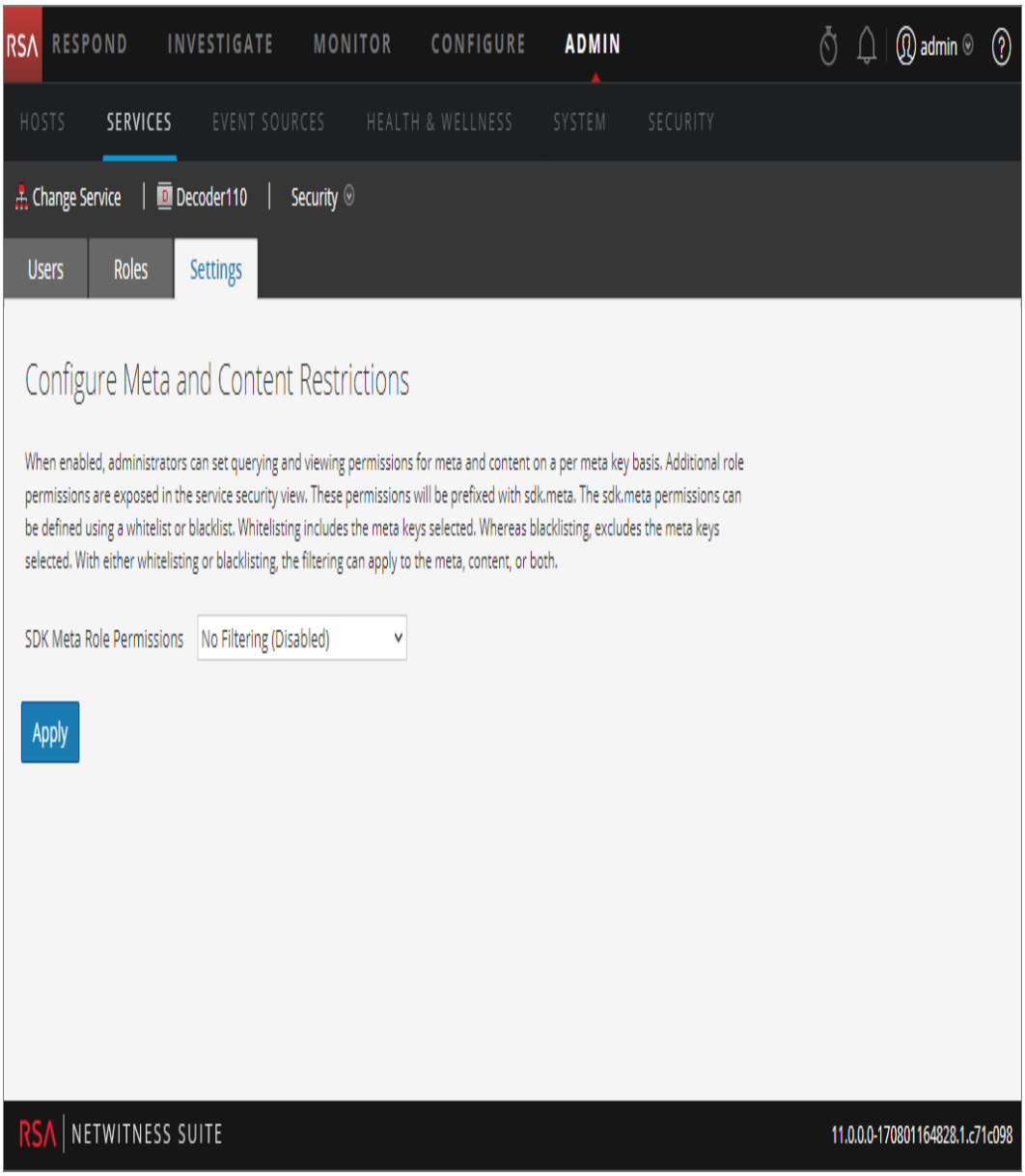
En la pestaña Ajustes de configuración de la vista Seguridad de servicios, los administradores pueden habilitar y configurar funciones del sistema que definen permisos por clave de metadatos para Brokers, Concentrators, Decoders y Log Decoders individuales. La configuración de esta función agrega claves de metadatos configurables a la vista Seguridad de servicios > pestaña Funciones de modo que las claves de metadatos individuales se puedan aplicar a funciones específicas en un servicio específico. En la siguiente figura se ilustra esto.



Esta configuración suele ser parte de un plan de privacidad de datos que se implementa para asegurarse de que tipos específicos de contenido que consume o agrega un servicio se mantengan seguros mediante la limitación de la visibilidad de los metadatos y el contenido a usuarios con privilegios (consulte *Administración de la privacidad de datos*).

Para mostrar la pestaña:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio Decoder o Log Decoder, haga clic en  **> Ver > Seguridad** y haga clic en la pestaña **Ajustes de configuración**.



Funciones

La pestaña incluye dos funciones.

Función	Descripción
Campo Permisos de función de metadatos de SDK	Proporciona la opción de inhabilitar o configurar restricciones de claves de metadatos y contenido. Se describen las opciones de filtrado.
Botón Aplicar	Aplica de inmediato la configuración seleccionada. Si no está inhabilitado, las claves de metadatos se agregan a la pestaña Funciones para que se puedan aplicar a funciones específicas.

Opciones de Permisos de función de metadatos de SDK

En la siguiente tabla se muestran las opciones de filtrado disponibles en la lista de selección Permisos de función de metadatos de SDK, así como los valores numéricos que se usan para inhabilitar (0) y los tipos de filtrado (del 1 al 6).

Nota: No hay necesidad de conocer el valor numérico, a menos que la visibilidad de metadatos y contenido en el nodo system.roles se configure manualmente.

Valor del nodo system.roles	Opción de la pestaña Configuración	Descripción
0	Sin filtrado (ideshabilitado	Las funciones del sistema que definen permisos por clave de metadatos están deshabilitadas.
1	Ingresar en lista blanca metadatos y contenido	Los metadatos y el contenido para las funciones de metadatos de SDK especificadas se ingresan en lista blanca o están visibles para los usuarios que tienen asignada la función del sistema.
2	Ingresar en lista blanca solo metadatos	Los metadatos para las funciones de metadatos de SDK especificadas se ingresan en lista blanca o están visibles para los usuarios que tienen asignada la función del sistema.

Valor del nodo system.roles	Opción de la pestaña Configuración	Descripción
3	Ingresar en lista blanca solo contenido	El contenido para las funciones de metadatos de SDK especificadas se ingresa en lista blanca o están visibles para los usuarios que tienen asignada la función del sistema.
4	Ingresar en lista negra metadatos y contenido	Los metadatos y el contenido para las funciones de metadatos de SDK especificadas se ingresan en lista negra o no están visibles para los usuarios que tienen asignada la función del sistema.
5	Ingresar en lista negra solo metadatos	Los metadatos para las funciones de metadatos de SDK especificadas se ingresan en lista negra o no están visibles para los usuarios que tienen asignada la función del sistema.
6	Ingresar en lista negra solo contenido	El contenido para las funciones de metadatos de SDK especificadas se ingresa en lista negra o no están visibles para los usuarios que tienen asignada la función del sistema.

Pestaña Usuarios

En este tema se explican las funciones de la vista Seguridad de servicios > pestaña Usuarios.

En la vista Seguridad de servicios, la pestaña Usuarios permite configurar los siguientes aspectos de un servicio:

- Agregar cuentas de usuario.
- Cambiar las contraseñas de los usuarios de servicios.
- Configurar las propiedades de autenticación de usuarios y las propiedades de manejo de consultas del servicio.
- Especificar la membresía en funciones de usuario, la cual especifica las funciones a las que pertenece el usuario en el servicio seleccionado.

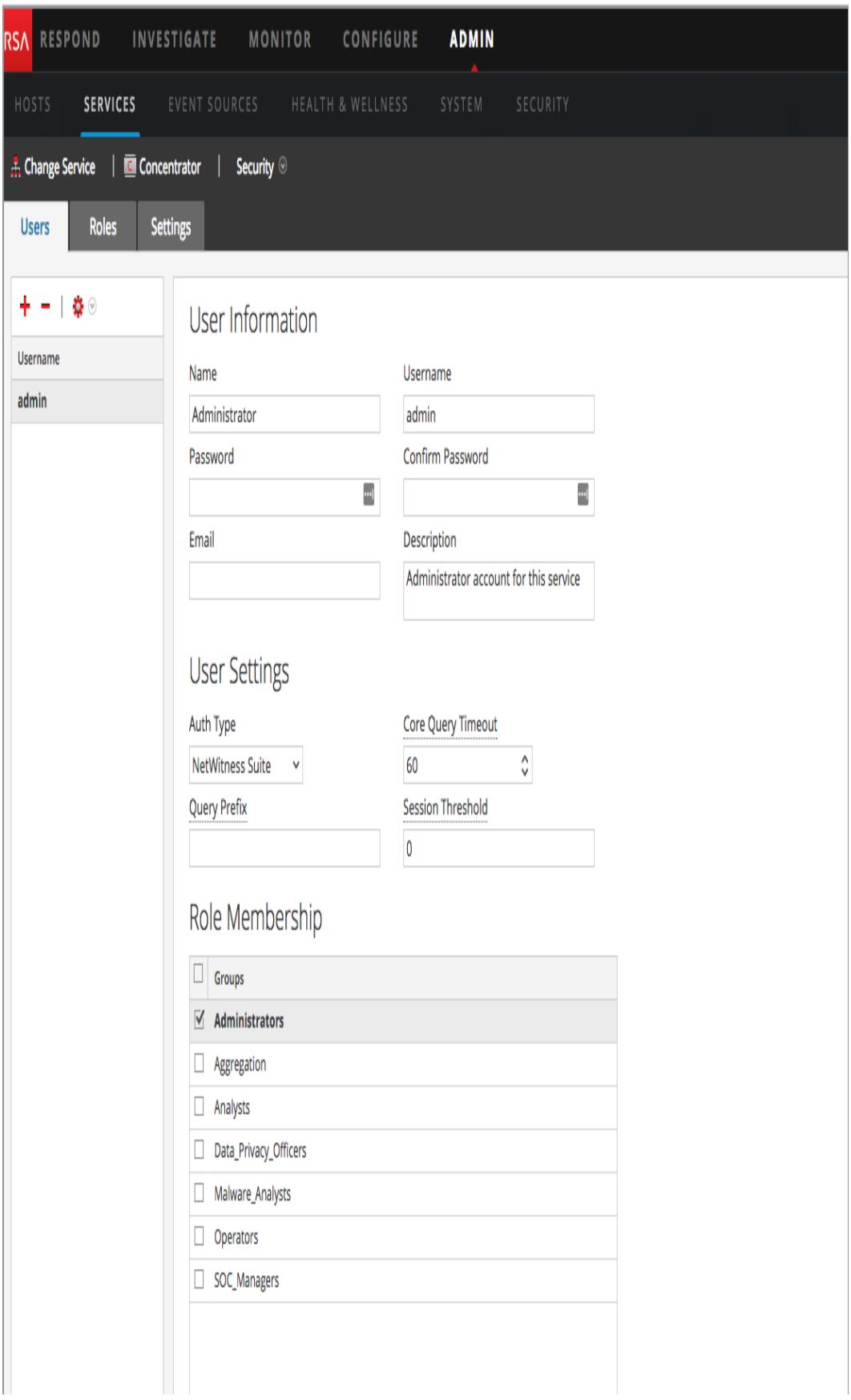
Nota: Para los servicios NetWitness Suite Core 10.4 o superior que usan conexiones de confianza, ya no es necesario crear cuentas de usuario de NetWitness Suite Core para los usuarios que inician sesión a través del cliente web. Solo debe crear cuentas de usuario de NetWitness Suite Core para agregación, usuarios de clientes gruesos y usuarios de la API REST.

Los procedimientos relacionados con esta pestaña se describen en Introducción de hosts: Procedimientos de hosts y servicios.

Para acceder a la vista Seguridad de servicios > pestaña Usuarios:

1. En **NetWitness Suite**, vaya a **ADMINISTRAR > Servicios.**

2. Seleccione un servicio en el cual desee agregar un usuario y elija  **> Ver >** **Seguridad**.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Concentrator
Security
Users
Roles
Settings
Username
admin
User Information
Name
Administrator
Username
admin
Password
Confirm Password
Email
Description
Administrator account for this service
User Settings
Auth Type
NetWitness Suite
Core Query Timeout
60
Query Prefix
Session Threshold
0
Role Membership
Groups
Administrators
Aggregation
Analysts
Data_Privacy_Officers
Malware_Analysts
Operators
SOC_Managers

Funciones

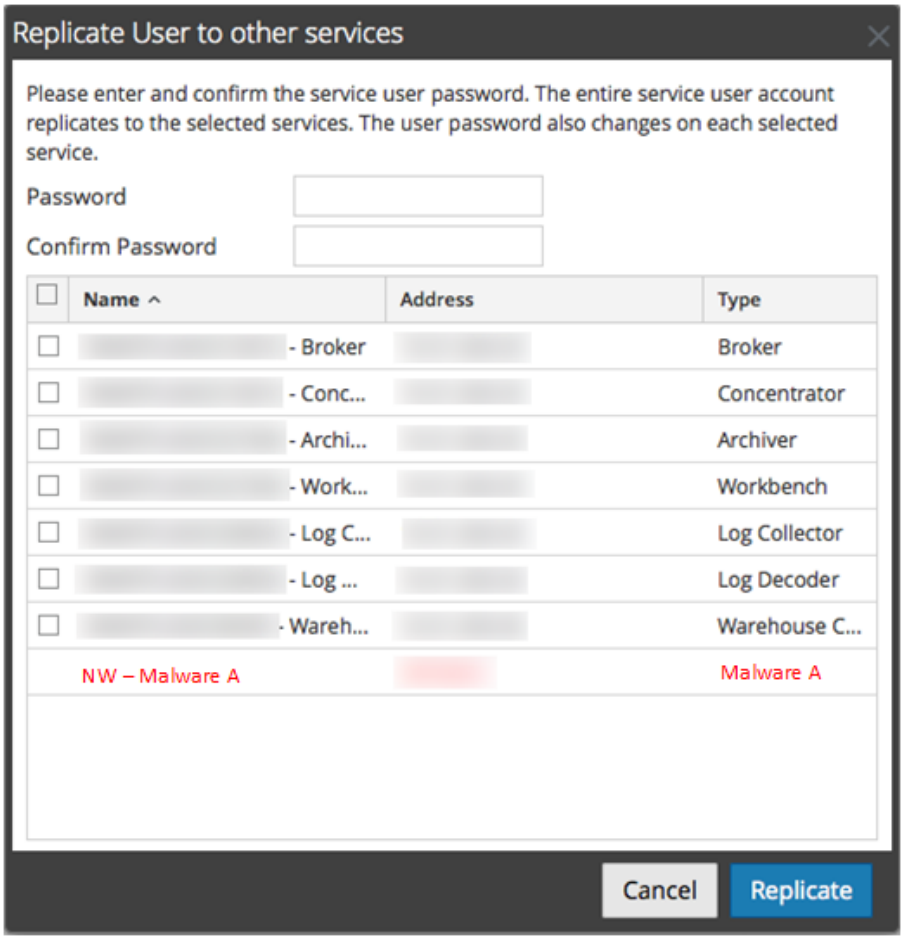
La pestaña Usuarios contiene el panel Lista de usuarios a la izquierda. Si selecciona un nombre de usuario, el panel Definición de usuario estará disponible a la derecha.

Panel Lista de usuarios

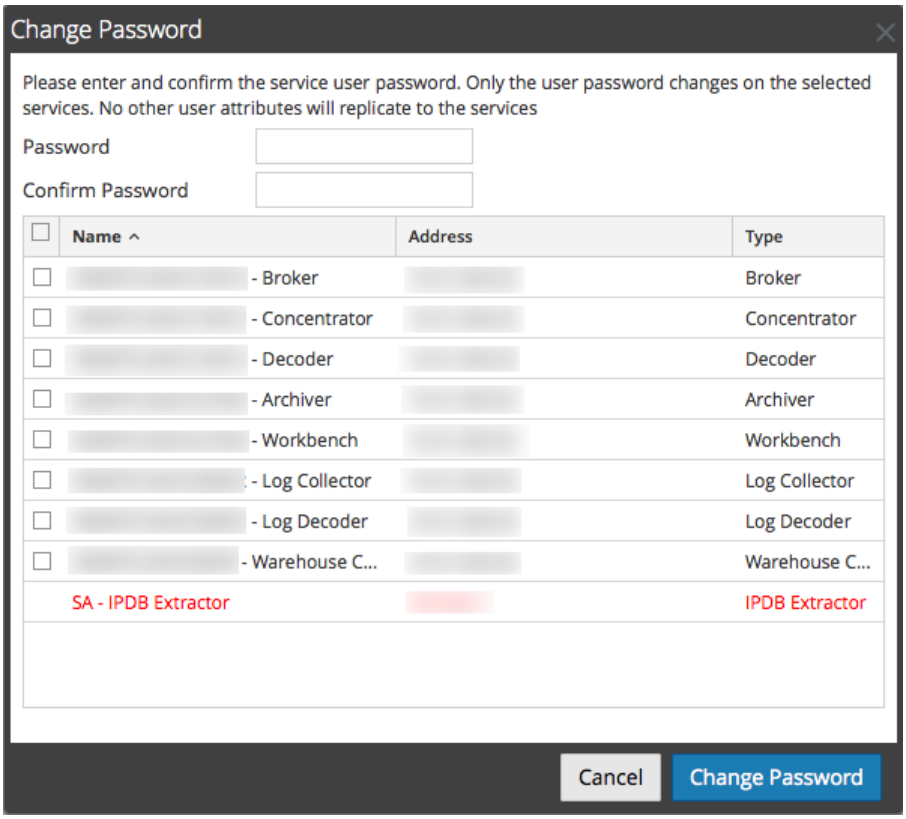
El panel Lista de usuarios tiene las siguientes funciones.

Función	Descripción
	Agrega un nuevo usuario al servicio actual.
	Elimina los usuarios seleccionados del servicio.
	Realiza una de las siguientes acciones en la cuenta de usuario de servicios seleccionada: • **Replicar:** replica la cuenta de usuario de servicios completa a los servicios seleccionados. • **Cambiar contraseña:** cambia la contraseña de un usuario de servicios y replica la contraseña nueva a los servicios principales en los cuales está definida esa cuenta de usuario. Con la opción Cambiar contraseña, solo el cambio de contraseña se replica a los servicios principales seleccionados y no la cuenta de usuario completa.
Nombre de usuario	Los nombres de usuario de todas las cuentas de usuario que acceden al servicio. El nombre de usuario debe ser uno que se utilice para iniciar sesión en NetWitness Suite.

En la siguiente figura se muestra el cuadro de diálogo **Replicar usuario a otros servicios**.



En la siguiente figura se muestra el cuadro de diálogo **Cambiar contraseña**.



Panel Definición de usuario

El panel Definición de usuario tiene tres secciones:

- Información del usuario identifica el usuario según se creó en la vista Seguridad de Administration.
- Configuración de usuario define los parámetros que se aplican al acceso de este usuario al servicio.
- Membresía en función define las funciones de usuario a las cuales pertenece el usuario.

Existen dos botones:

- El botón **Guardar** guarda los cambios realizados en el panel Definición de usuario y los aplica de inmediato.
- Si no ha guardado los cambios en el panel Definición de usuario, el botón **Restablecer** restablece todos los campos y los ajustes a sus valores previos a la edición.

Información del usuario

La sección Información del usuario tiene las funcionalidades siguientes.

Campo	Descripción
Nombre	El nombre del usuario.
Nombre de usuario	El nombre de usuario que este usuario ingresa para iniciar sesión en el servicio. Este es el nombre de usuario de NetWitness Suite que se generó cuando el administrador agregó el usuario y las credenciales asociadas en la vista **Seguridad de Administration** (Administration > Seguridad).
Contraseña (y **Confirmar contraseña**)	La contraseña que el usuario ingresa para iniciar sesión en el servicio. Esta es la contraseña de NetWitness Suite que se generó cuando el administrador agregó el usuario y las credenciales asociadas en la vista **Seguridad de Administration**. La contraseña de la cuenta de NetWitness Suite y la contraseña del servicio deben coincidir para permitir que el usuario se conecte al servicio a través de NetWitness Suite.
Correo electrónico	(Opcional) La dirección de correo electrónico del usuario.
Descripción	(Opcional) Un campo de descripción general que describe a este usuario.

Configuración de usuario

La sección Configuración de usuario tiene las funcionalidades siguientes.

Campo	Descripción
Tipo de autenticación	El esquema de autenticación para este usuario. La línea de productos soporta autenticación interna y externa. • **NetWitness** especifica la autenticación interna y está activado de manera predeterminada. En este modo, todos los usuarios deben autenticarse con la cuenta de usuario y las contraseñas que se generan cuando el administrador utiliza la vista Seguridad de Administration de NetWitness Suite (Administration > Seguridad) para crear el usuario y sus credenciales asociadas. • **Externo** especifica que la autenticación está habilitada a través de la interfaz del host mediante PAM (Pluggable Authentication Modules). Para obtener más información, consulte el tema **Configurar la funcionalidad de inicio de sesión PAM** de la guía *Administración de usuarios y de la seguridad del sistema*.
Prefijo de consulta	(Opcional) Siempre anexa la sintaxis de consulta a todas las consultas realizadas por este usuario. Por ejemplo, la adición del prefijo de consulta **email != 'ceo@company.com'** impide que los resultados de ese correo electrónico se muestren en las sesiones.

Campo	Descripción
Tiempo de espera agotado de consulta de SA Core	**Nota:** Este campo se aplica al servicio NetWitness Suite versión 10.5 y superiores y no aparece para el servicio versión 10.4 y anteriores. Los servicios NetWitness Suite versión 10.4 y anteriores usan Nivel de consulta en lugar de Tiempo de espera agotado de consulta de SA Core. Especifica la cantidad máxima de minutos que un usuario puede ejecutar una consulta en el servicio. Si este valor se configura en cero (0), el tiempo de espera agotado de consulta no se impone para el usuario en el servicio. Cuando se replica un usuario desde un servicio NetWitness Suite 10.5 o superior a un servicio NetWitness Suite 10.4, Tiempo de espera agotado de consulta migra a Nivel de consulta en función del nivel más cercano. Por ejemplo, si un usuario tiene un tiempo de espera agotado de consulta de 15 minutos, este recibe un nivel de consulta de 3 después de la migración. Si un usuario tiene un tiempo de espera agotado de consulta de 35 minutos, este recibe un nivel de consulta de 2 después de la migración. Si un usuario tiene un tiempo de espera agotado de consulta de 45 minutos, este recibe un nivel de consulta de 2 después de la migración.
Umbral de sesión	(Opcional) Controla el comportamiento de la aplicación cuando escanea los valores de metadatos para determinar los conteos de sesiones. Cualquier valor de metadatos con un conteo de sesión que está por sobre el umbral establecido detiene su determinación del conteo de sesiones verdadero cuando se alcanza el umbral. Si se establece un umbral para una sesión, la vista Navegación muestra que el umbral se alcanzó y el porcentaje del tiempo de consulta utilizado para alcanzarlo.

Membresía en función

La sección Membresía en función muestra las funciones de las cuales es miembro un usuario para el servicio seleccionado.

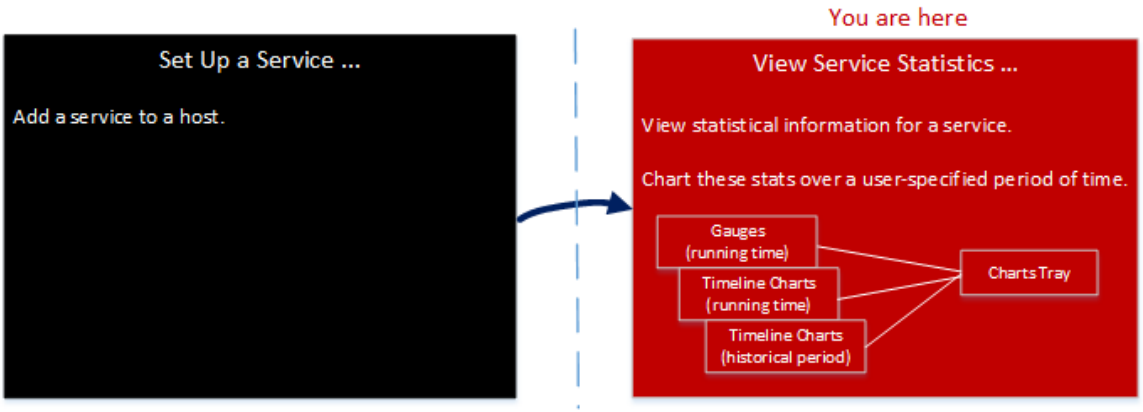
Vista Estadísticas de servicios

En este tema se describen las funciones disponibles en la vista Estadísticas de Servicios de NetWitness Suite.

La vista Estadísticas de servicios proporciona un modo para monitorear el estado y las operaciones de un servicio. Esta vista muestra estadísticas clave, información del sistema del servicio e información del sistema del host de un servicio. Además, hay más de 80 estadísticas disponibles para visualizar en forma de medidor y en gráficos de cronograma. En los gráficos de cronograma históricos, solo se pueden ver estadísticas de tamaño de sesión, sesiones y paquetes.

Flujo de trabajo

En este flujo de trabajo se muestran las tareas que se realizan en la vista Estadísticas.

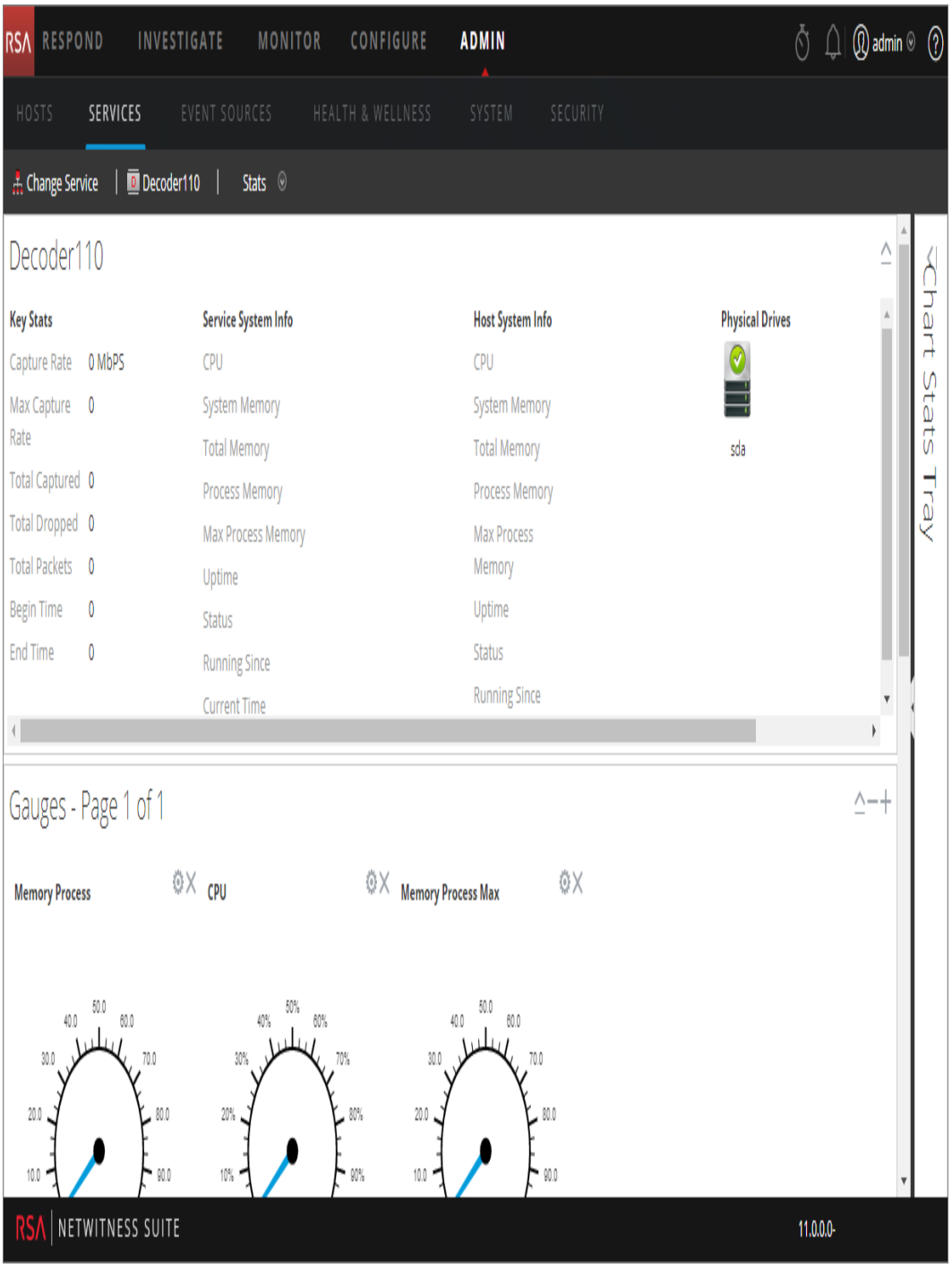


La vista Estadísticas permite personalizar las estadísticas monitoreadas de cada servicio.

En el siguiente ejemplo se muestra cómo usar la vista Estadísticas de un Decoder. La vista Estadísticas de todos los servicios brinda la misma información para cada servicio.

Para acceder a la vista Estadísticas de servicios:

1. En **NetWitness Suite** , vaya a **ADMINISTRAR > Servicios**.
   Se muestra la vista Servicios.
2. Seleccione un servicio y elija  **> Ver > Estadísticas.**



Funciones

Aunque hay diferentes estadísticas disponibles para los distintos tipos de servicios, hay ciertos elementos en común en la vista Estadísticas de servicios para cualquier servicio Core:

- Sección Estadísticas de resumen
- Sección Medidores
- Sección Cronogramas
- Sección Cronogramas históricos
- Bandeja de estadísticas de gráfico

Sección Estadísticas de resumen

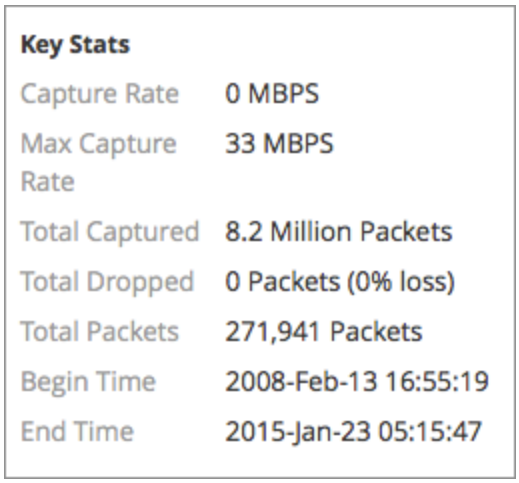
La sección Estadísticas de resumen está en la parte superior de la vista predeterminada y no tiene campos que se puedan editar.

Hay cinco paneles en la sección Estadísticas de resumen. En el panel **Estadísticas clave** se muestran diferentes estadísticas para distintos tipos de servicios. Los paneles restantes de la sección Estadísticas de resumen son los mismos para todos los tipos de servicios.

Estadísticas clave

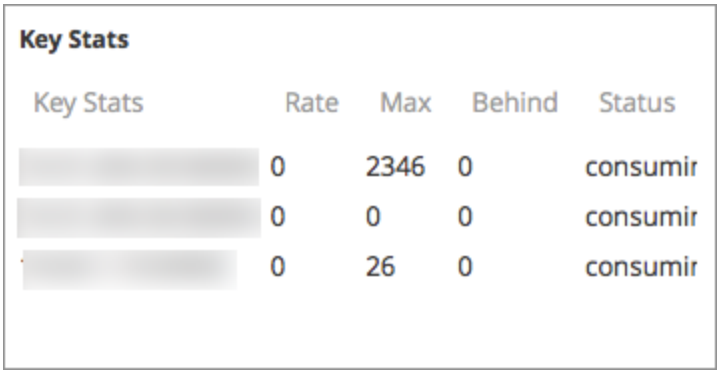
En el panel Estadísticas clave se muestran diferentes estadísticas para distintos tipos de servicios.

- En un Decoder o un Log Decoder, las estadísticas clave incluyen las estadísticas de captura, como la velocidad de captura, la cantidad total de paquetes o registros capturados, la cantidad total de paquetes o registros descartados y la hora de inicio y finalización de la captura de datos.



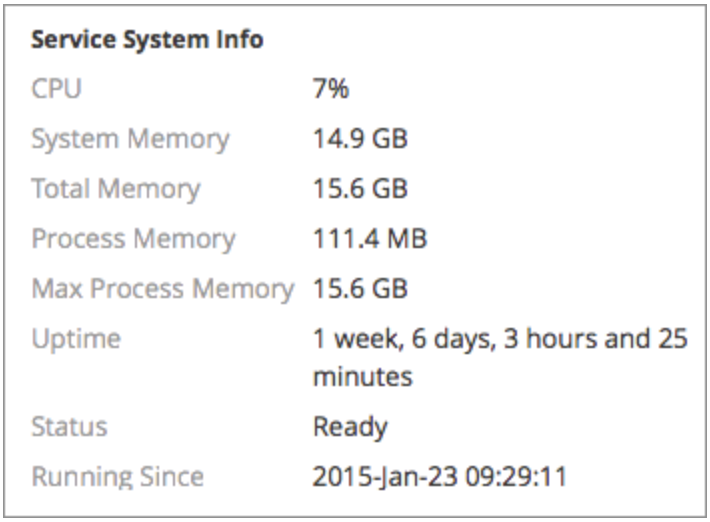
- Un Broker o un Concentrator agrega datos de varios servicios. Por lo tanto, las estadísticas clave de todos los dispositivos agregados se muestran en una cuadrícula. Las columnas de la cuadrícula proporcionan el nombre del servicio, la velocidad de captura, la velocidad de captura máxima, la cantidad de sesiones retrasadas (que se deben agregar) y el estado del

servicio.

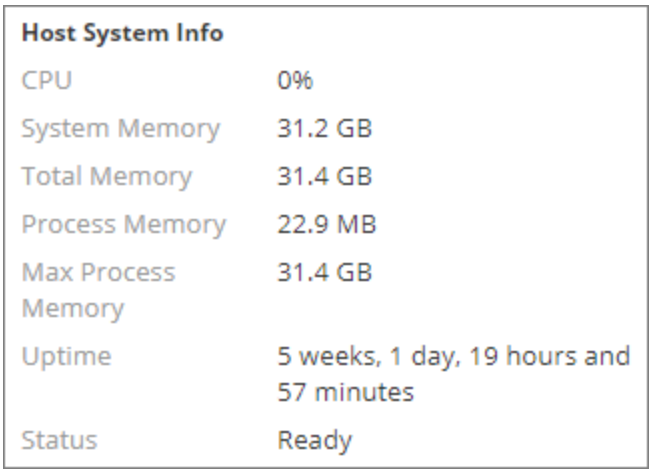


Información del sistema del servicio

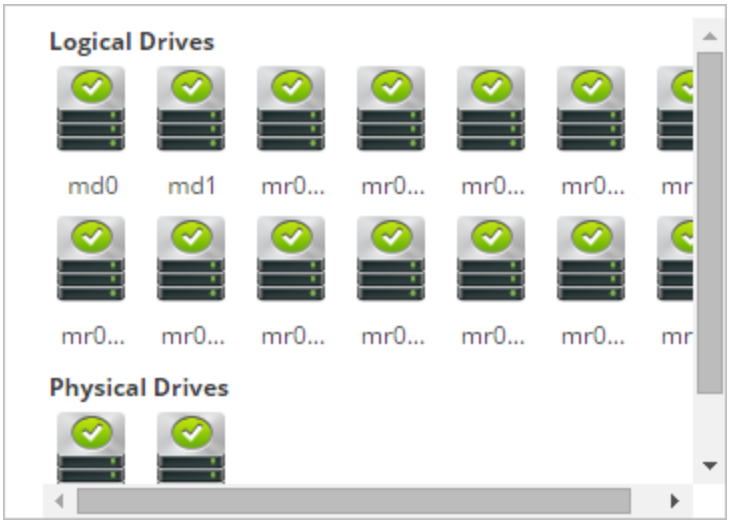
El panel Información del sistema del servicio incluye el porcentaje de CPU que utiliza el servicio, las estadísticas del uso de memoria (sistema, total, proceso y proceso máximo), el tiempo de actividad del servicio, el estado, la hora de inicio de la ejecución y la hora actual.



Información del sistema del host incluye el porcentaje de CPU que utiliza el host, las estadísticas de uso de la memoria (sistema, total, proceso y máximo), el tiempo de actividad del host, el estado, la hora de inicio de la ejecución y la hora actual.



Las **Unidades lógicas** y las **Unidades físicas** se muestran con un ícono para el nombre y el estado de la unidad. A continuación se enumeran los tipos de unidad que se usan en los nombres y en las opciones de estado de la unidad.



Tipos y estados de unidades

Tipo de unidades	Descripción	Comentario	Opciones de estado
sd	Dispositivo de bloques de SCSI	Volúmenes de discos SAS, discos SATA MegaRAID conectados directamente	CORRECTO (verde) FALLA (rojo)

Tipo de unidades	Descripción	Comentario	Opciones de estado
ld	Volumen MegaRAID lógico	Definido en BIOS o con la herramienta MegaCLI	CORRECTO (verde) DEGRADADO (amarillo) EN CONSTRUCCIÓN (amarillo) FALLA (rojo)
pd	Discos MegaRAID físicos	No está expuesto directamente a Linux	CORRECTO (verde) FALLA (rojo)
md	Volumen RAID de software Linux		CORRECTO (verde) DEGRADADO (amarillo) EN CONSTRUCCIÓN (amarillo) FALLA (rojo)

Medidores

La sección Medidores en la vista Estadísticas muestra las estadísticas en la forma de medidores analógicos. Consulte Funciones para obtener los detalles sobre la configuración de los medidores.

Cronogramas

Los gráficos de cronograma muestran las estadísticas seleccionadas en un cronograma en ejecución centrándose en la hora actual. Esto es lo mismo para todos los tipos de servicios y solamente se puede editar el nombre para mostrar del cronograma. Consulte Gráficos de cronograma para obtener los detalles sobre la configuración de cronogramas.

Cronogramas históricos

Los gráficos de cronograma histórico muestran las estadísticas del tamaño de la sesión, las sesiones y los paquetes en un cronograma histórico. Esto es igual en todos los tipos de servicios, y se proporcionan un nombre para mostrar, una fecha de inicio y una fecha de finalización que se pueden editar. Consulte Gráficos de cronograma para obtener los detalles sobre la configuración de cronogramas.

Nota: Los gráficos de cronograma históricos quedaron obsoletos para los servicios Log Collector, Virtual Log Collector (VLC) y recopilador de Windows existente.

Bandeja de estadísticas de gráfico

La Bandeja de estadísticas de gráfico muestra todas las estadísticas disponibles del tipo de servicio seleccionado. Diferentes servicios tienen diferentes estadísticas para monitorear. Consulte Componentes para obtener una descripción detallada.

Temas

- Componentes
- Funciones
- Gráficos de cronograma

Bandeja de estadísticas de gráfico

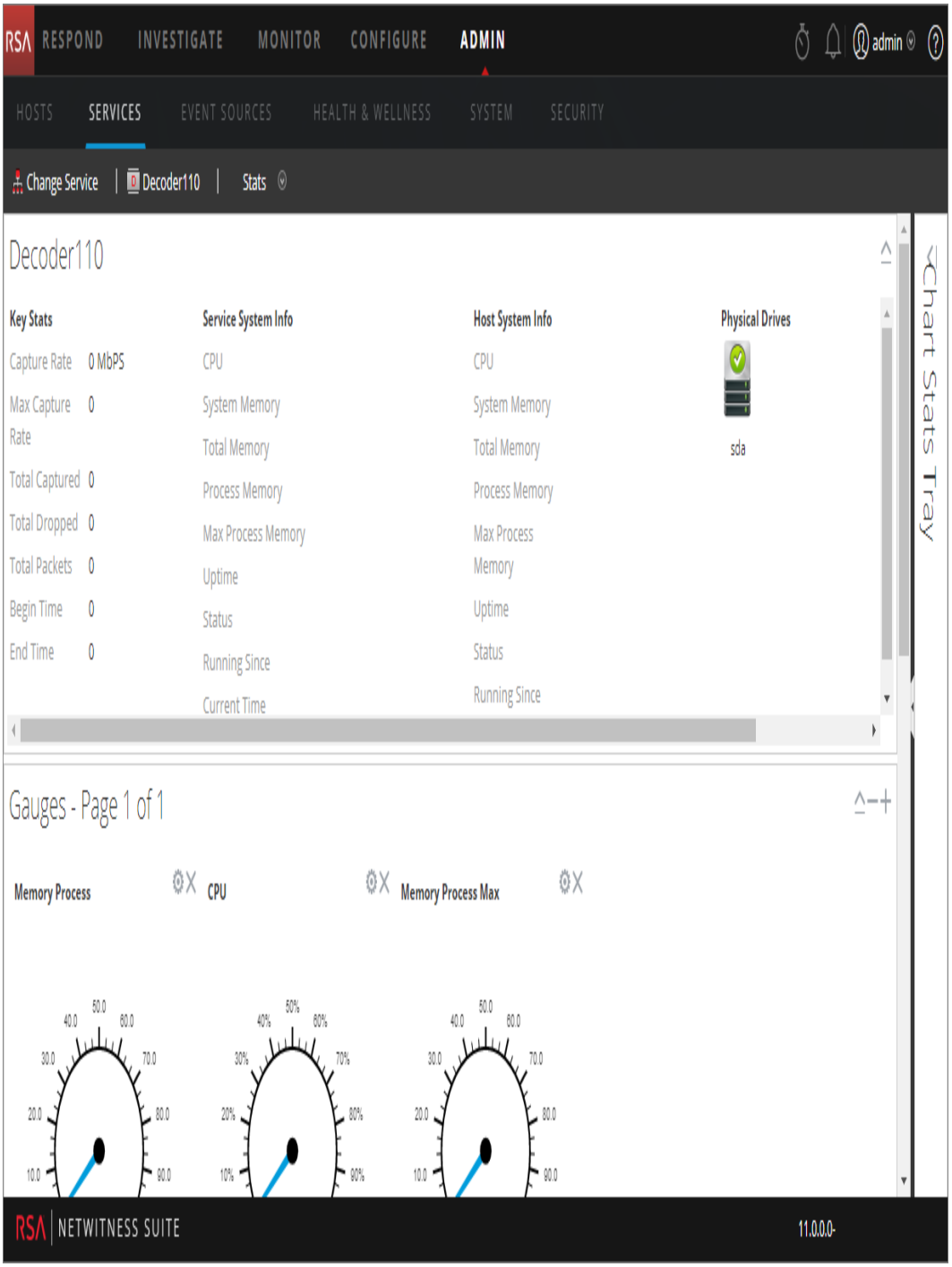
En este tema se describe la Bandeja de estadísticas de gráfico de la vista Estadísticas de servicios.

En la vista Estadísticas de servicios, la Bandeja de estadísticas de gráfico proporciona una manera de personalizar las estadísticas monitoreadas de cada servicio. La Bandeja de estadísticas de gráfico muestra todas las estadísticas disponibles para el servicio. La cantidad de estadísticas varía según el tipo de servicio que se monitorea. Cualquier estadística en la Bandeja de estadísticas de gráfico se puede mostrar en un gráfico de cronograma o tipo velocímetro. Solo las estadísticas del tamaño de la sesión, las sesiones y los paquetes son visibles en los gráficos de cronograma histórico.

Para acceder a la vista Estadísticas de servicios:

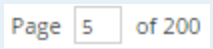
1. En el menú de **NetWitness Suite**, seleccione **ADMIN > Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione un servicio y elija  **> Ver > Estadísticas.**
   La Bandeja de estadísticas de gráfico aparece en el lado derecho.
3. Si la bandeja está contraída, haga clic en  para ver la lista de estadísticas disponibles.

En el siguiente ejemplo se muestra la vista Estadísticas de servicios de un Decoder. La Bandeja de estadísticas de gráfico está contraída.



Componentes

La Bandeja de estadísticas de gráfico tiene diferentes estadísticas de los distintos tipos de servicios. En el ejemplo anterior, hay 111 estadísticas disponibles para Decoder. En la siguiente tabla se describen las funciones de la Bandeja de estadísticas de gráfico.

Función	Descripción
	Haga clic para ampliar el panel horizontalmente.
	Haga clic para contraer el panel horizontalmente.
Buscar	Escriba un término para buscar en el campo y presione **DEVOLVER**. Las estadísticas que coinciden se muestran con la palabra de coincidencia destacada.
	Haga clic para ir a la primera página.
	Haga clic para ir a la página anterior.
	Escriba un número de página en el campo Página.
	Haga clic para ir a la página siguiente.
	Haga clic para ir a la última página.
	Haga clic para actualizar la vista.
Stats 1 - 12 of 111	Muestra el rango de estadísticas que se muestra. La cantidad total de estadísticas varía según el tipo de servicio.

Medidores

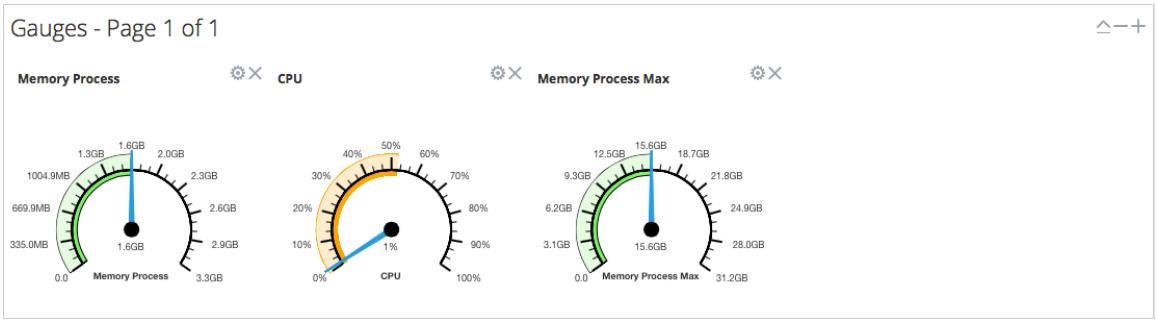
En este tema se presentan las funcionalidades de la sección Medidores en la vista Estadísticas de servicios.

La sección Medidores en la vista Estadísticas de servicios presenta las estadísticas en forma de un medidor analógico. Puede arrastrar cualquier estadística disponible en la Bandeja de estadísticas de gráfico a la sección Medidores. Es posible editar las propiedades de cada medidor individual; todos los medidores tienen un título que se puede editar y algunos tienen propiedades adicionales que también se pueden editar.

Para acceder a la vista Estadísticas de servicios:

1. En el menú de **NetWitness Suite**, seleccione **ADMIN > Servicios**
   Se muestra la vista Servicios de Administration.
2. Seleccione un servicio y elija  **> Ver > Estadísticas**.
   La vista Estadísticas de servicios incluye la sección Medidores.

La siguiente figura muestra los medidores predeterminados de la vista Estadísticas de servicios para un Log Decoder.



Funciones

Los medidores predeterminados muestran estas estadísticas:

- El uso de memoria del proceso
- Uso de CPU
- Cantidad máxima de memoria utilizada en el proceso

Los controles en la barra de título Medidores y en cada medidor son los controles estándar de un dashlet.

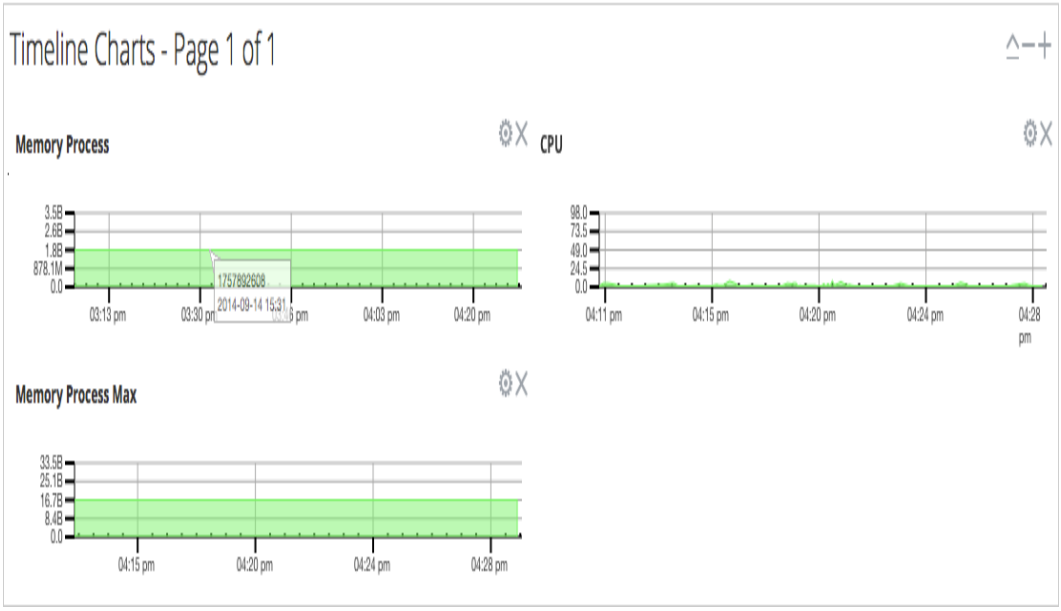
- En la barra de título Medidores, puede contraer y expandir la sección y la página hacia delante o hacia atrás.
- En cada medidor, puede editar las propiedades (⚙) y eliminar (✕) el medidor.

Gráficos de cronograma

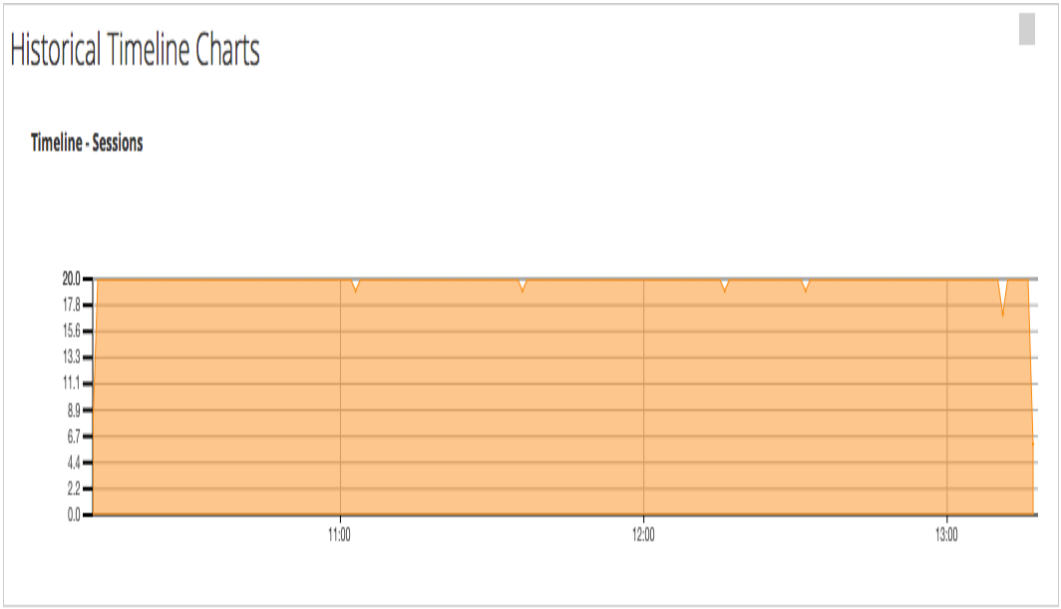
En este tema se describen las funciones de los gráficos de cronograma en la vista Estadísticas de servicios.

Los gráficos muestran las estadísticas en un cronograma de ejecución. La vista Estadísticas de servicios incluye dos tipos de cronogramas: cronograma actual e histórico. Puede arrastrar cualquier estadística disponible en la Bandeja de estadísticas de gráfico a la sección Gráficos de cronograma. Solo las estadísticas del tamaño de la sesión, las sesiones y los paquetes son visibles en los gráficos de cronograma histórico. Es posible editar las propiedades de un gráfico de cronograma individual; todos los gráficos de cronograma tienen un título que se puede editar y algunos tienen propiedades adicionales que también se pueden editar.

La siguiente figura es un ejemplo de un gráfico de cronograma actual que muestra el valor y el registro de fecha y hora de un punto de datos.



La siguiente figura es un ejemplo de un gráfico de cronograma histórico.



Los gráficos de cronograma actual predeterminados muestran estas estadísticas:

- Proceso de memoria
- CPU
- Poseso de memoria máximo

Los gráficos de cronograma histórico muestran estas estadísticas:

- Sessions
- Paquetes
- Tamaño de sesión

Los controles en la barra de título Gráficos de cronograma y en cada cronograma son los controles estándar de un dashlet.

- En la barra de título Gráficos de cronograma, puede contraer y expandir la sección y la página hacia delante o hacia atrás.
- En cada cronograma, puede editar las propiedades ( ) y eliminar ( ) el cronograma.
- Cuando mantiene el mouse sobre un punto de datos en el gráfico, se muestra el valor y el registro de fecha y hora del punto seleccionado.

Vista del sistema

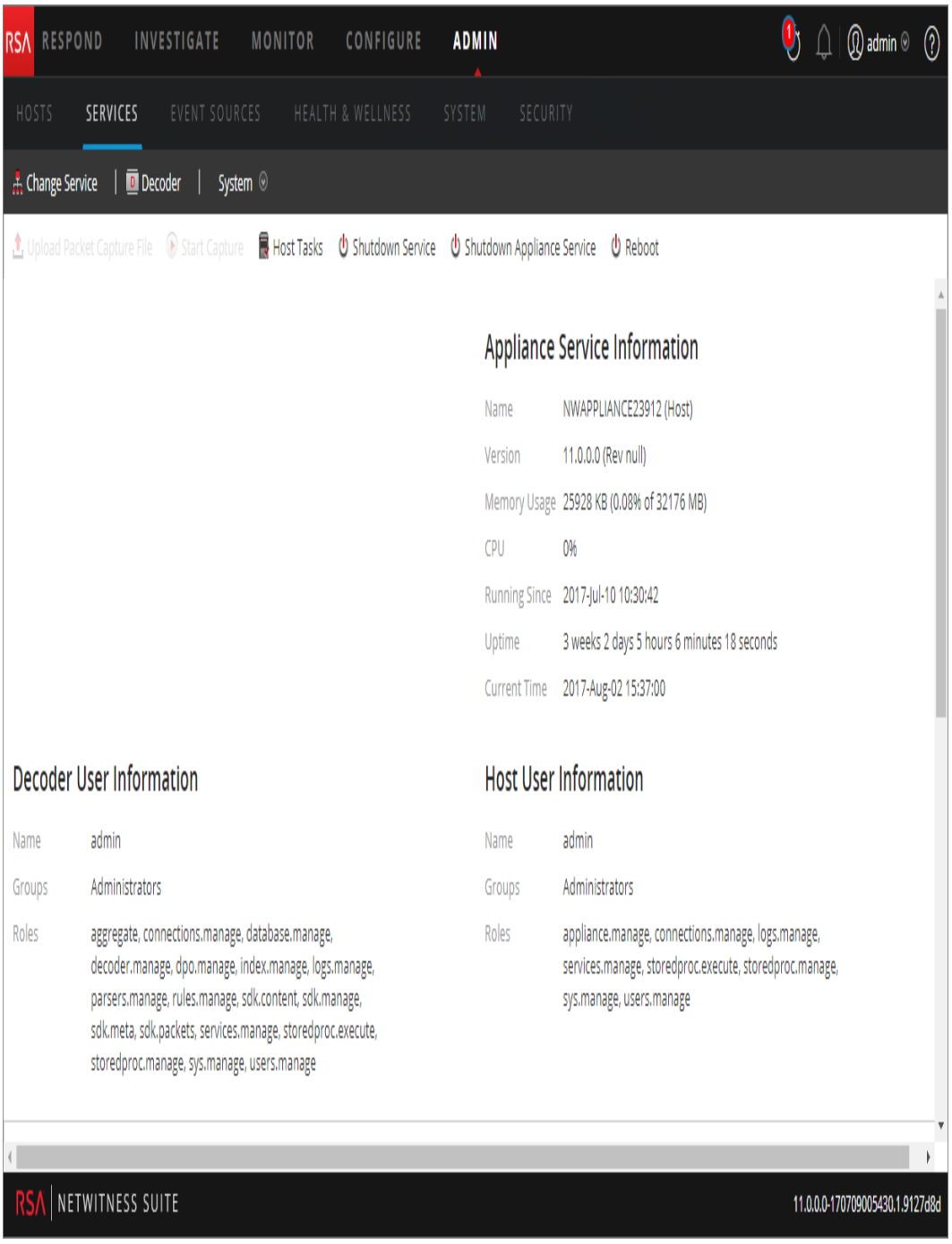
En este tema se presentan las funciones de la vista Sistema con el uso de Decoder y Log Decoder como ejemplo. Consulte las guías de configuración de cada servicio (por ejemplo, la *Guía de configuración de Broker y Concentrator* de *RSA NetWitness® Suite*) para obtener detalles sobre sus vistas **ADMIN > Servicios > Sistema**.

Un Log Decoder es un tipo especial de Decoder y se configura y administra de manera similar a un Decoder. Por lo tanto, la mayor parte de la información en esta sección se refiere a ambos tipos de Decoders. Se especifican las diferencias para los Log Decoders.

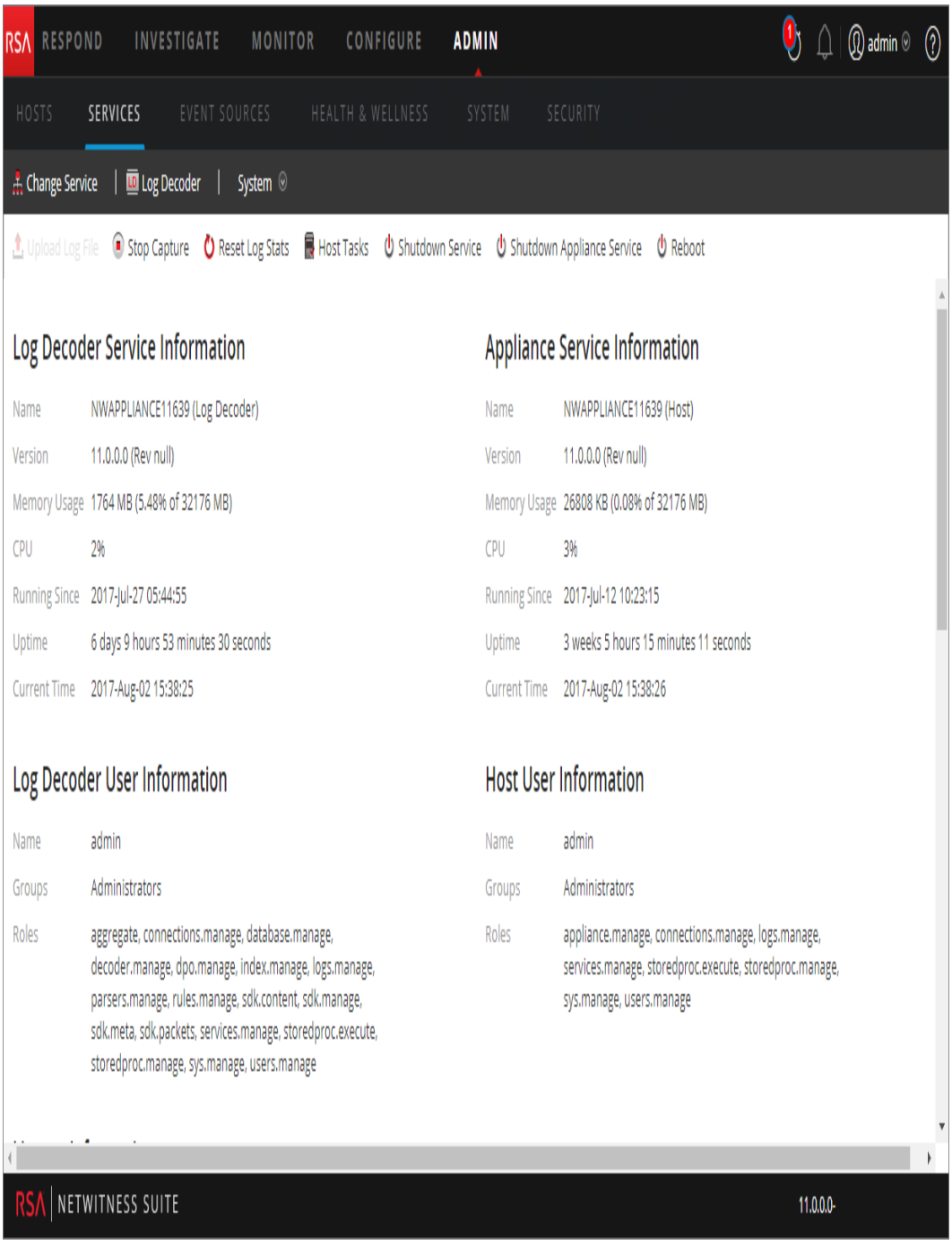
Para acceder a la vista Sistema de servicios de un Decoder:

1. En **NetWitness Suite** , vaya a **ADMINISTRAR > Servicios**.
   Se muestra la vista Servicios.
2. Seleccione un servicio y elija  **> Ver> Sistema**.

En la siguiente figura se muestra un ejemplo de la vista Sistema de servicios de un Decoder.



En la siguiente figura se muestra la vista Sistema de servicios de un Log Decoder.



Funciones

Barra de herramientas de información de los servicios

En las siguientes barras de herramientas se muestran las opciones específicas de Log Decoders y Decoders.

Además de las opciones comunes de la barra de herramientas de la vista Sistema de servicios, puede iniciar y detener la captura de paquetes o registros. Las opciones para cargar archivos son distintas en los Decoder estándar (archivo de captura de paquetes) y el Log Decoder (archivo de registro).

Acción	Descripción
Cargar archivo de captura de paquete	Muestra un cuadro de diálogo que proporciona una manera de seleccionar un archivo de captura de paquetes (.pcap) para cargar en el Decoder seleccionado. Para obtener más información, consulte el tema **Cargar archivo de captura de paquete** de la *Guía de configuración de Decoder y Log Decoder*. **Nota:** Esta opción no se aplica a los Log Decoders.
Cargar archivo de log	Muestra un cuadro de diálogo que proporciona una manera de seleccionar un archivo de registro (.log) para cargar en el Log Decoder seleccionado. Para obtener más información, consulte el tema **Cargar un archivo de registro en un Log Decoder** de la *Guía de configuración de Decoder y Log Decoder*.
Iniciar/detener captura	Inicia la captura de un paquete en el Decoder seleccionado. Cuando la captura de un paquete está en curso, la opción en la barra de herramientas cambia a Detener captura y la opción para cargar un archivo no está disponible.

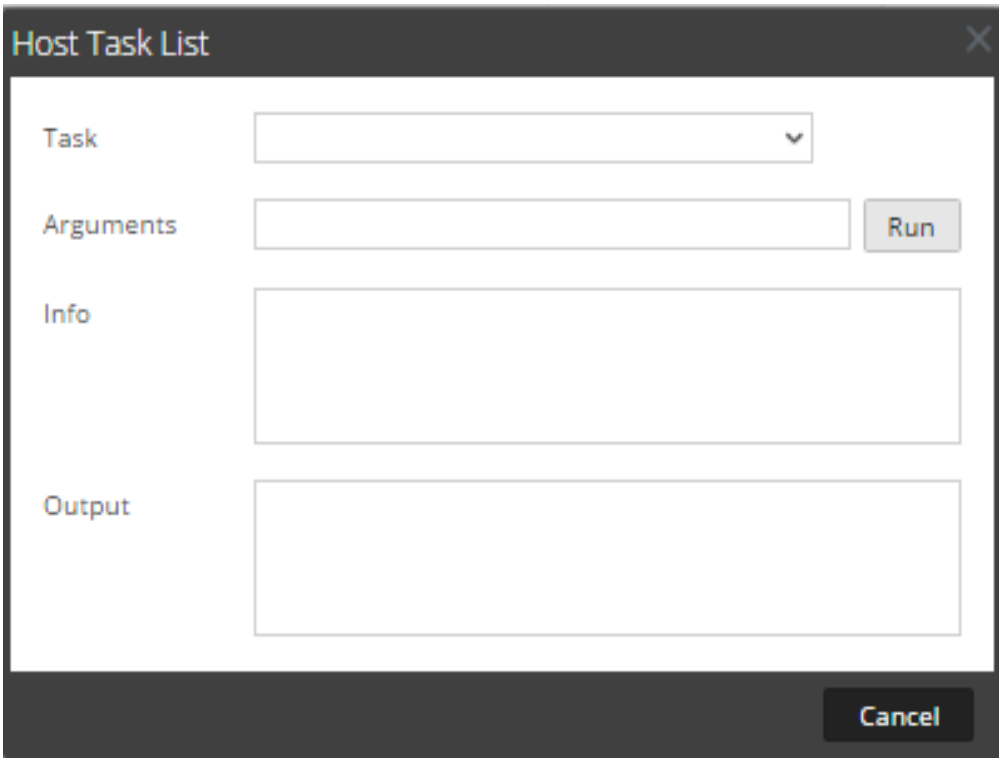
Cuadro de diálogo Lista de tareas del host

En este tema se presenta la vista Sistema de servicios > cuadro de diálogo Lista de tareas del host.

En la vista Sistema de servicios de RSA NetWitness Suite, puede usar la opción Tareas de host para administrar las tareas relacionadas con un host y sus comunicaciones con la red. Hay varias opciones de configuración de servicios y hosts disponibles para los servicios Core.

Para acceder al cuadro de diálogo Tareas de host:

1. En **NetWitness Suite**, seleccione **ADMIN > Servicios**.
2. Seleccione un servicio y elija  > **Ver> Sistema**.
   Se muestra la vista Sistema del servicio.
3. En la barra de herramientas de la **vista Sistema de servicios**, haga clic en **Tareas de host**.
   Se muestra el cuadro de diálogo Lista de tareas del host. La lista **Tarea** proporciona una lista de mensajes compatibles con el host asociado.



Funciones

La siguiente tabla describe las funcionalidades del cuadro de diálogo.

Campo	Descripción
Tarea	Un campo de entrada en el cual puede escribir o seleccionar un mensaje para un host de Core. Cuando hace clic en este campo, se muestra una lista desplegable de las tareas del host disponibles.
Argumentos	Un campo de entrada en el cual se ingresan los argumentos del mensaje, si los hay.
Ejecutar	Ejecuta la tarea y los argumentos en los campos de entrada.
Información	Información acerca del propósito y la sintaxis del mensaje.
Salida	El resultado de una tarea ejecutada.
Cancelar	Cierra el cuadro de diálogo Lista de tareas del host.

Lista de selección de tareas del host

Estas tareas se muestran como una lista desplegable en el campo Tarea. La función de seguridad requerida para ejecutar la opción regula las opciones disponibles.

Tarea	Descripción
Agregar monitor de sistema de archivos	Inicia el monitoreo de los servicios de almacenamiento conectados al sistema de archivos especificado (consulte Agregar y eliminar un monitor del sistema de archivos).
Eliminar monitor de sistema de archivos	Detiene el monitoreo de los servicios de almacenamiento conectados al sistema de archivos especificado.
Reiniciar host	Apaga y reinicia el host (consulte Reiniciar un host).
Definir reloj integrado de host	Configura el reloj local del host (consulte Definir reloj integrado de host).

Tarea	Descripción
Definir nombre del host	Este método de cambio del nombre de host está obsoleto en NetWitness Suite 10.6; lo reemplazó el procedimiento que se describe en Introducción de hosts: Procedimientos de hosts y servicios
Definir configuración de red	Establece los parámetros de dirección de red (consulte Definir configuración de red).
Definir origen de tiempo de red	Define el origen del reloj de este host (consulte Definir origen de tiempo de red).
Definir reenvío de syslog	Activa o desactiva el reenvío de syslog desde un servidor remoto hacia el dispositivo seleccionado (consulte Definir reenvío de syslog).
Mostrar estado de puerto de red	Muestra la información de la interfaz de red de un host (consulte Mostrar estado de puerto de red).
Mostrar número de serie	Obtiene el número de serie del host (consulte Mostrar número de serie).
Apagar host	Apaga el host físico y el host permanece apagado (consulte Apagar host).
Iniciar servicio	Inicia un servicio en este host (consulte Iniciar, detener o reiniciar un servicio).
Detener servicio	Detiene un servicio en este host.
setSNMP	Habilita o deshabilita el servicio SNMP en un host (consulte Configurar SNMP).

Ajustes de configuración de servicios

En este tema se presentan los ajustes de configuración de servicios disponibles para los servicios de RSA NetWitness Suite Core.

Los servicios de NetWitness Suite Core incluyen Brokers, Concentrators, Decoders, Log Decoders, Archivers y el servicio Appliance. Los parámetros de configuración de servicios que se enumeran en estas tablas constituyen todos los parámetros visibles y configurables. Algunos parámetros se pueden configurar en varias secciones de la interfaz del usuario de NetWitness Suite y otros solo se pueden ver o configurar en la vista Explorar de Servicios.

Parámetros de configuración del servicio Appliance

En este tema se enumeran y se describen los parámetros de configuración disponibles para el servicio NetWitness Suite Core Appliance.

El servicio NetWitness Suite Core Appliance permite el monitoreo del hardware en hardware NetWitness heredado.

En esta tabla se describen los parámetros de configuración de Appliance.

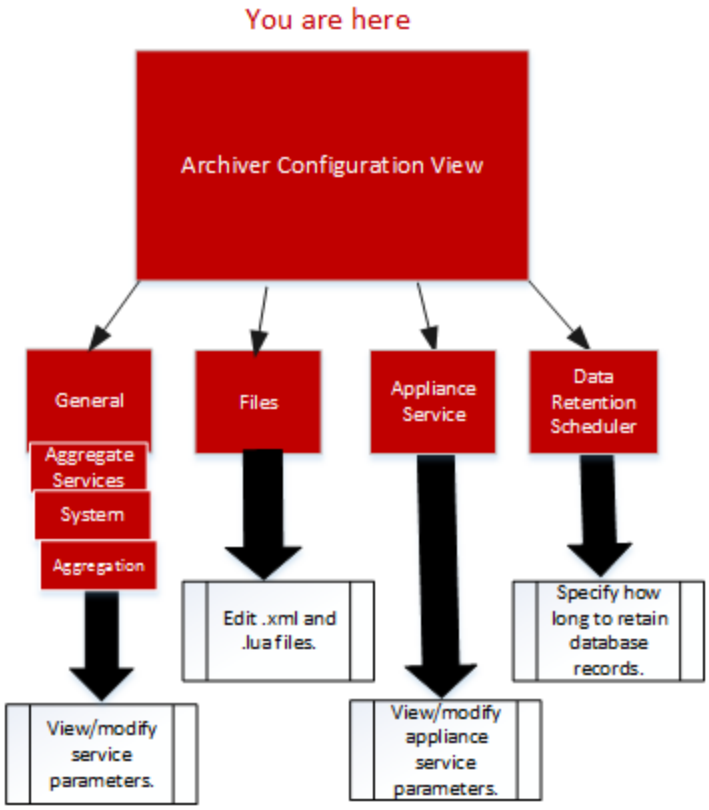
Campo de parámetros de Appliance	Descripción
Registros	/logs/config, consulte Parámetros de configuración del registro de los servicios principales
REST	/rest/config, consulte Parámetros de configuración de la interfaz REST
Servicios	/services/<service name>/config, consulte Parámetros de configuración de servicio principal a servicio principal
Sistema	/sys/config, consulte Parámetros de configuración del sistema de servicios principales

Vista Configuración del servicio Archiver

En este tema se enumeran y se describen los ajustes de configuración disponibles para NetWitness Suite Archivers.

Flujo de trabajo

En el siguiente flujo de trabajo se muestran las tareas de configuración correspondientes al servicio Archiver.



Función	Deseo…
Administrador	Configurar filtros de metadatos para agregación. Consulte "(Opcional) Configurar filtros de metadatos para agregación" en la *Guía de configuración de Archiver de RSA NetWitness Suite* para obtener instrucciones.
Administrador	Configurar la agregación de grupos. Consulte "Configurar la agregación de grupos" en la *Guía de implementación de RSA NetWitness Suite* para obtener instrucciones.

Vista rápida

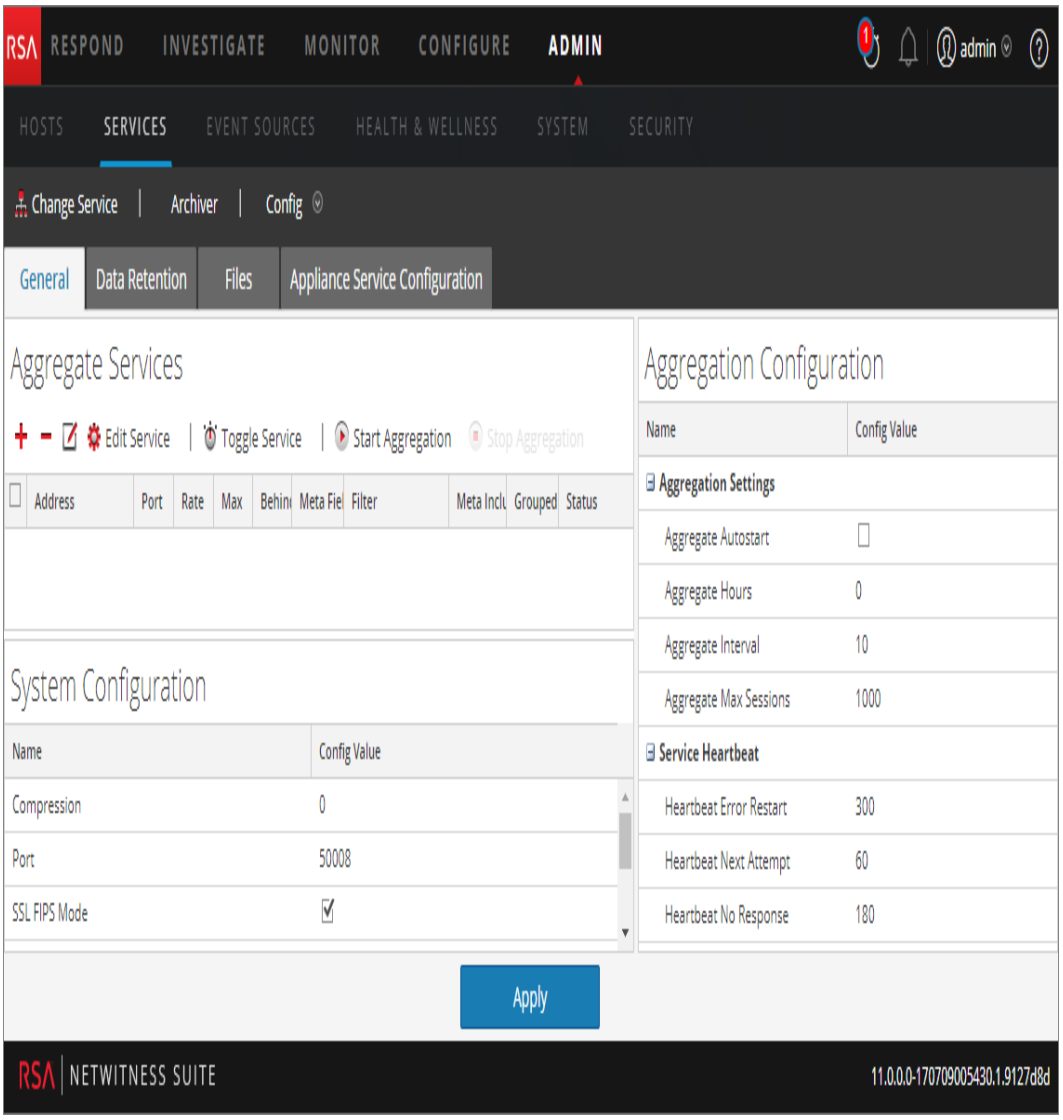
Para acceder a la vista Configuración de servicios:

1. En **NetWitness Suite**, seleccione **ADMIN > Servicios**.
   Se muestra la vista Servicios de Administrar.

2. Seleccione un servicio Archiver y elija  **>Ver > Configuración**.

   Se muestra la vista Configuración de Servicios correspondiente al servicio Archiver.

Este es un ejemplo de la vista Configuración de Servicios de un Archiver.



Parámetros de configuración del servicio Broker

En este tema se enumeran y se describen los parámetros de configuración de NetWitness Suite Brokers.

En esta tabla se enumeran y se describen los parámetros de configuración de Broker.

Campo de parámetro de Broker	Descripción
Broker	/broker/config, consulte Parámetros de configuración de agregación
aggregate.interval.behind	Cantidad mínima de milisegundos antes de que se solicite otra ronda de agregación cuando el proceso de agregación se está retrasando en el Broker. El cambio se aplica de inmediato.
Base de datos	/database/config, consulte el tema **Nodos de configuración de la base de datos** de la *Guía de ajuste de la base de datos de servicios NetWitness Suite Core*
Índice	/index/config
index.dir	Directorio donde se almacenan los archivos de mapeo del dispositivo de Broker. El cambio se aplica tras el reinicio del servicio.
language.filename	Especificación del lenguaje de índice (XML) que se carga en el inicio. El cambio requiere el reinicio del servicio.
Registros	/logs/config, consulte Parámetros de configuración del registro de los servicios principales
REST	/rest/config, consulte Parámetros de configuración de la interfaz REST
SDK	/sdk/config, consulte el tema **Nodos de configuración de SDK** de la *Guía de ajuste de la base de datos de servicios NetWitness Suite Core* y Introducción de hosts: Modos system.roles de servicios Core de NetWitness Platform
Servicios	/services/<service name>/config, consulte Parámetros de configuración de servicio principal a servicio principal
Sistema	/sys/config, consulte Parámetros de configuración del sistema de servicios principales

Parámetros de configuración de agregación

En este tema se enumeran y se describen los parámetros de configuración disponibles que son comunes a los servicios que ejecutan la agregación, como NetWitness Suite Concentrators y Archivers.

En esta tabla se enumeran y se describen los parámetros que controlan la agregación en un servicio de agregación.

Ruta de configuración	/concentrator/config o /archiver/config
aggregate.autostart	Reinicia automáticamente la agregación después de un reinicio del servicio, si está activado. El cambio se aplica de inmediato.
aggregate.buffer.size	Muestra el tamaño del buffer (la unidad predeterminada es KB) que se usa por ronda de agregación. Los buffers más grandes pueden mejorar el rendimiento de la agregación, pero podrían afectar el rendimiento de la consulta. El cambio se aplica después del reinicio de la agregación.
aggregate.crc	Si está activado, todos los flujos de agregación contarán con validación de CRC. El cambio se aplica de inmediato.
aggregate.hours	Muestra la cantidad máxima de horas de anticipación en las cuales un servicio podrá iniciar la agregación. El cambio se aplica de inmediato.
aggregate.interval	Indica la cantidad mínima de milisegundos antes de solicitar otra ronda de agregación. El cambio se aplica de inmediato.
aggregate.meta.page.factor	Indica la cantidad asignada de páginas de metadatos por sesión utilizada para la agregación. El cambio se hace efectivo con el reinicio del servicio.
aggregate.meta.perpage	Indica la cantidad asignada de metadatos almacenados en una página de datos. El cambio se hace efectivo con el reinicio del servicio.

Ruta de configuración	/concentrator/config o /archiver/config
aggregate.precache	Determina si el Concentrator almacenará previamente en caché la siguiente ronda de agregación para los servicios upstream. Puede mejorar el rendimiento de la agregación, pero podría afectar el rendimiento de la consulta. El cambio se aplica de inmediato.
aggregate.sessions.max	Indica la cantidad de sesiones que se van a agregar a cada ronda. El cambio se aplica después del reinicio de la agregación.
aggregate.sessions.perpage	Indica la cantidad de sesiones almacenadas en una página de datos. El cambio se hace efectivo con el reinicio del servicio.
aggregate.time.window	Muestra la ventana de tiempo máximo +/-, en segundos, dentro de la que deben estar todos los servicios antes de solicitar otra ronda de agregación. Cero desactiva la ventana de tiempo. El cambio se aplica de inmediato.
consume.mode	Determina si el Concentrator solo puede agregar localmente o en red, según las restricciones de licencia. El cambio se hace efectivo con el reinicio del servicio.
export.enabled	Permite la exportación de datos de sesiones, si está activada. El cambio se hace efectivo con el reinicio del servicio.
export.expire.minutes	Indica la cantidad de minutos antes de que los archivos de la caché de exportación venzan y se eliminen. El cambio se aplica de inmediato.
export.format	Determina el formato de archivo que se usó durante la exportación de datos. El cambio se hace efectivo con el reinicio del servicio.

Ruta de configuración	/concentrator/config o /archiver/config
export.local.path	Muestra la ubicación local para almacenar en caché los datos exportados. Tamaño máximo asignado opcional (=#unit); las unidades son: t de TB, g de GB y m de MB. El cambio se hace efectivo con el reinicio del servicio.
export.meta.fields	Determina los campos de metadatos que se exportan. Lista de campos separada por comas. Asterisco significa todos los campos. Asterisco más lista de campos significa todos los campos, SALVO los enumerados. Solo lista de campos indica que solo se incluyen esos campos. El cambio se aplica de inmediato.
export.remote.path	Muestra el protocolo remoto (nfs://) y ubicación para exportar datos. El cambio se hace efectivo con el reinicio del servicio.
export.rollup	Determina el intervalo de acumulación para los archivos de exportación. El cambio se hace efectivo con el reinicio del servicio.
export.session.max	Muestra el máximo de sesiones por archivo exportado. Para los tipos de archivos de exportación que se almacenan en caché, esto determina los tamaños de memoria almacenados en caché. Cero significa sin límite. El cambio se aplica de inmediato.
export.size.max	Muestra la cantidad máxima de bytes por archivo exportado. Para los tipos de archivos de exportación que se almacenan en caché, esto determina los tamaños de memoria almacenados en caché. Cero significa sin límite. El cambio se aplica de inmediato.
export.usage.max	Muestra el porcentaje máximo de espacio de caché usado antes de la detención de la agregación. Cero significa sin límite. El cambio se aplica de inmediato.

Ruta de configuración	/concentrator/config o /archiver/config
heartbeat.error	Indica la cantidad de segundos que se debe esperar después de un error de servicio antes de intentar volver a conectar el servicio. El cambio se aplica de inmediato.
heartbeat.interval	Indica la cantidad de milisegundos entre comprobaciones de servicio de latido. El cambio se aplica de inmediato.
heartbeat.next.attempt	Indica la cantidad de segundos que se debe esperar antes de intentar volver a conectar el servicio. El cambio se aplica de inmediato.
heartbeat.no.response	Indica la cantidad de segundos que se debe esperar antes de dejar offline un servicio que no responde. El cambio se aplica de inmediato.

Parámetros de configuración del servicio Concentrator

En este tema se enumeran y se describen los parámetros de configuración disponibles para NetWitness Suite Concentrators.

En esta tabla se enumeran y se describen los parámetros de configuración de Concentrator.

Campo de parámetro de Concentrator	Descripción
Concentrator	/concentrator/config, consulte Parámetros de configuración de agregación
Base de datos	/database/config, consulte el tema **Nodos de configuración de la base de datos** de la *Guía de ajuste de la base de datos de NetWitness Suite Core*
Índice	/index/config, consulte el tema **Nodos de configuración de índices** de la *Guía de ajuste de la base de datos de NetWitness Suite Core*
Registros	/logs/config, consulte Parámetros de configuración del registro de los servicios principales

Campo de parámetro de Concentrator	Descripción
REST	/rest/config, consulte Parámetros de configuración de la interfaz REST
SDK	/sdk/config, consulte el tema **Nodos de configuración de SDK** de la *Guía de ajuste de la base de datos de NetWitness Suite Core* y Introducción de hosts: Modos system.roles de servicios Core de NetWitness Platform
Servicios	/services/<service name>/config, consulte Parámetros de configuración de servicio principal a servicio principal
Sistema	/sys/config, consulte Parámetros de configuración del sistema de servicios principales

Parámetros de configuración del registro de los servicios principales

En este tema se enumeran y se describen los parámetros de configuración del registro para todos los servicios de NetWitness Suite Core.

La configuración del registro es la misma en todos los servicios de NetWitness Suite Core.

En la siguiente tabla se describen los parámetros de configuración de registros:

Carpeta de configuración de registros	/logs/config
log.dir	Muestra el directorio donde se almacena la base de datos de registros. El tamaño máximo asignado opcional (=#) se expresa en MB. El cambio se hace efectivo con el reinicio del servicio.
log.levels	Controla los tipos de mensajes de registro que se almacenan (separados por comas). La configuración específica del módulo se define así: <Module>= [debug|info|audit|warning|failure|all|none]. El cambio se aplica de inmediato.

Carpeta de configuración de registros	/logs/config
log.snmp.agent	Establece un agente de recepción de SNMP trap remoto.
snmp.trap.version	Establece la versión de SNMP que se usará para gets y traps (2c o 3).
snmpv3.engine.boots	Muestra el conteo de encendidos del motor SNMPv3. Este campo se incrementa automáticamente en el arranque y normalmente no deber requerir que el usuario lo configure.
snmpv3.engine.id	Establece el ID del motor SNMPv3, que es un número de entre 10 y 64 dígitos hexadecimales opcionalmente antecedido por 0x. Puede agregar valores de sufijo al final del ID del motor para cada uno de los servicios SA Core que se ejecutan en el mismo host. Por ejemplo, si el ID de motor generado para un host de SA Core es 0x1234512345, puede establecer el ID de motor para el servicio Decoder en 0x123451234501 y en 0x123451234504 para el servicio Appliance.
snmpv3.trap.auth.local.key	Establece la clave local de autenticación SNMPv3 trap, que es un número de 16 o 20 dígitos hexadecimales (según el protocolo de autenticación que se use) antecedido por 0x. Para MD5, la clave tiene 16 dígitos hexadecimales, mientras que SHA usa 20 dígitos hexadecimales. Puede usar cualquier algoritmo deseado para generar las claves locales. Se recomienda usar un método de generación que implique aleatoriedad en lugar de seleccionar valores clave manualmente.
snmpv3.trap.auth.protocol	Muestra el protocolo de autenticación SNMPv3 trap (ninguno, MD5 o SHA).

Carpeta de configuración de registros	/logs/config
snmpv3.trap.priv.local.key	Establece la clave local de privacidad SNMPv3 trap, que es un número de 16 dígitos hexadecimales antecedido por 0x.
snmpv3.trap.priv.protocol	Muestra el protocolo de privacidad SNMPv3 trap (ninguno o AES).
snmpv3.trap.security.level	Muestra el nivel de seguridad SNMPv3 trap, el cual indica si la autenticación y la privacidad se usan o no. Los posibles valores son noAuthNoPriv, authNoPriv o authPriv.
snmpv3.trap.security.name	Establece el nombre de seguridad SNMPv3 trap que se usa durante la autenticación SNMPv3 trap
syslog.size.max	Muestra el tamaño máximo de un registro enviado a syslog (algunos demonios de syslog tienen problemas con los mensajes muy grandes). Cero significa sin límite. El cambio se aplica de inmediato.

Parámetros de configuración de servicio principal a servicio principal

En este tema se enumeran y se describen los parámetros de configuración que controlan la forma en que un servicio principal se conecta a otro servicio principal. Por ejemplo, cuando un Concentrator se conecta a un Decoder, esta configuración controla los parámetros de esa conexión.

Cada vez que un servicio principal establece una conexión a otro servicio principal, el servicio que actúa como el **cliente** crea una nueva subcarpeta en la carpeta /services del árbol de configuración. El nombre de la subcarpeta corresponde al nombre del servicio y tiene el formato `host:port`. Por ejemplo, la carpeta de conexión de servicio para una conexión de Concentrator a un Decoder podría ser `/services/reston-va-decoder:50004`. Dentro de cada carpeta de conexión de servicio, hay una subcarpeta `config` que contiene parámetros configurables.

En la siguiente tabla se describen los parámetros de configuración de servicio:

Servicios	/services/host:port/config

Servicios	/services/host:port/config
allow.nonssl.to.ssl	Cuando se configura en true, permite que una conexión no SSL se conecte a un servicio SSL. De lo contrario, si se configura en false, las conexiones no seguras a seguras se rechazarán. El cambio se aplica de inmediato.
Compresión	Muestra un nodo de configuración que determina si los datos se comprimen antes de enviarlos. Un valor positivo determina la cantidad de bytes que se deben enviar antes de que se compriman. Cero significa sin compresión.
crc.checksum	Muestra un nodo de configuración que determina si los flujos de datos se validan con una suma de comprobación de CRC. Un valor positivo determina la cantidad de bytes que se deben enviar antes de que se les aplique validación CRC. Cero significa sin validación CRC.
ssl	Muestra un nodo de configuración que habilita o inhabilita el cifrado de SSL en la conexión.

Parámetros de configuración del sistema de servicios principales

En este tema se enumeran y se describen los parámetros de configuración que son comunes a todos los servicios de NetWitness Suite Core.

En la siguiente tabla se describen los parámetros de configuración del sistema:

Carpeta de configuración del sistema	/sys/config
Compresión	Muestra la cantidad mínima de bytes antes de que se comprima un mensaje, cuando se define en un valor positivo. Cero significa sin compresión para ningún mensaje. El cambio se aplica en las conexiones subsiguientes.

Carpeta de configuración del sistema	/sys/config
crc.checksum	Muestra la cantidad mínima de bytes antes de que se envíe un mensaje a través de la red con una suma de comprobación de CRC (que el cliente validará), cuando se define en un valor positivo. Cero significa sin validación de suma de comprobación de CRC con ningún mensaje. El cambio se aplica en las conexiones subsiguientes.
unidades	Muestra unidades en las cuales se monitorearán las estadísticas de uso. El cambio se hace efectivo con el reinicio del servicio.
puerto	Muestra el puerto en el cual escuchará este servicio. El cambio se hace efectivo con el reinicio del servicio.
scheduler	Muestra la carpeta de las tareas calendarizadas.
service.name.override	Muestra un nombre de servicio opcional que usan los servicios upstream para la agregación en lugar del nombre de host.
ssl	Cifra todo el tráfico mediante SSL, si está activado. El cambio se hace efectivo con el reinicio del servicio.
stat.compression	Comprime las estadísticas a medida que se escriben en la base de datos, si está activado. El cambio se hace efectivo con el reinicio del servicio.
stat.dir	Muestra el directorio donde se almacena la base de datos de estadísticas históricas (separe múltiples directorios con punto y coma). Tamaño máximo asignado opcional (=#unit); las unidades son: t de TB, g de GB y m de MB. El cambio se hace efectivo con el reinicio del servicio.

Carpeta de configuración del sistema	/sys/config
stat.exclude	Indica los nombres de rutas de acceso de estadísticas que se excluirán de la base de datos de estadísticas. Se permiten los siguientes comodines: ? se hace coincidir cualquier carácter, * se hace coincidir cero o más caracteres con el delimitador /, ** se hace coincidir cero o más caracteres, incluido el delimitador. El cambio se aplica de inmediato.
stat.interval	Determina la frecuencia (en milisegundos) con la cual se actualizan los nodos de estadísticas en el sistema. El cambio se aplica de inmediato.
threads	Indica la cantidad de hilos de ejecución en el pool de hilos de ejecución para manejar solicitudes entrantes. El cambio se aplica de inmediato.

Parámetros de configuración del servicio Decoder

En este tema se enumeran y se describen los parámetros de configuración disponibles para NetWitness Suite Decoders.

En esta tabla se enumeran y se describen los parámetros de configuración de Decoder.

Campo de parámetro de Decoder	Descripción
Decoder	/decoder/config consulte Parámetros de configuración de Decoder y Log Decoder
Base de datos	/database/config, consulte el tema **Nodos de configuración de la base de datos** de la *Guía de ajuste de la base de datos de NetWitness Suite Core*

Campo de parámetro de Decoder	Descripción
Índice	/index/config, consulte el tema **Nodos de configuración de índices** de la *Guía de ajuste de la base de datos de NetWitness Suite Core*
Registros	/logs/config, consulteParámetros de configuración del registro de los servicios principales
REST	/rest/config, consulte Parámetros de configuración de la interfaz REST
SDK	/sdk/config, consulte el tema **Nodos de configuración de SDK** de la *Guía de ajuste de la base de datos de NetWitness Suite Core* y Introducción de hosts: Modos system.roles de servicios Core de NetWitness Platform
Sistema	/sys/config, consulte Parámetros de configuración del sistema de servicios principales

Parámetros de configuración de Decoder y Log Decoder

En este tema se enumeran y se describen los parámetros de configuración que son idénticos en los servicios Packet Decoder y Log Decoder.

Ajustes de configuración de Decoder

En esta tabla se enumeran y se describen los parámetros de configuración compartidos de Decoder y Log Decoder.

Ruta de configuración de Decoder	/decoder/config

Ruta de configuración de Decoder	/decoder/config
aggregate.buffer.size	Muestra el tamaño del buffer (la unidad predeterminada es KB) que se usa por ronda de agregación. Los buffers más grandes pueden mejorar el rendimiento de la agregación, pero podrían afectar el rendimiento de la captura. El cambio se aplica después del reinicio de la captura.
aggregate.precache	Determina si el Decoder almacenará previamente en caché la siguiente ronda de agregación para los servicios upstream. Puede mejorar el rendimiento de la agregación, pero podría afectar el rendimiento de la captura. El cambio se aplica de inmediato.
assembler.pool.ratio	Muestra el porcentaje de páginas del pool que el ensamblador administra y usa en el proceso de ensamblaje. El cambio se hace efectivo con el reinicio del servicio.
assembler.session.flush	Elimina las sesiones cuando se completan (1) o las elimina cuando se analizan (2). El cambio se hace efectivo con el reinicio del servicio.
assembler.session.pool	Indica la cantidad de entradas del pool de sesiones. El cambio se hace efectivo con el reinicio del servicio.
assembler.size.max	Indica el tamaño máximo que obtendrá una sesión. Una configuración de 0 elimina el límite del tamaño de sesión. El cambio se aplica de inmediato.
assembler.size.min	Indica el tamaño mínimo que una sesión debe tener antes de persistir. El cambio se aplica de inmediato.
assembler.timeout.packet	Indica la cantidad de segundos que transcurren antes de que se agote el tiempo de espera de los paquetes. El cambio se aplica de inmediato.

Ruta de configuración de Decoder	/decoder/config
assembler.timeout.session	Indica la cantidad de segundos que transcurren antes de que se agote el tiempo de espera de las sesiones. El cambio se aplica de inmediato.
assembler.voting.weights	Muestra las ponderaciones utilizadas para determinar qué flujo de sesiones está marcado como cliente y servidor. El cambio se aplica de inmediato.
capture.autostart	Determina si la captura comienza automáticamente cuando se inicia el servicio. El cambio se hace efectivo con el reinicio del servicio.
capture.buffer.size	Muestra el tamaño de asignación del buffer de la memoria de captura (la unidad predeterminada es MB). El cambio se hace efectivo con el reinicio del servicio.
capture.device.params	Muestra parámetros específicos del servicio de captura. El cambio se hace efectivo con el reinicio del servicio. Los parámetros que entiende este campo son específicos del dispositivo de captura seleccionado actualmente. Si el dispositivo de captura actual no reconoce ninguno de los parámetros, no se hace caso de ellos. En Log Decoders, solo existe el dispositivo de captura de eventos de registro. Este acepta algunos parámetros opcionales. • **uso-envision-time**: Si se establece en 1, se importarán los metadatos de hora para cada evento desde el flujo de Log Collector. Si es 0 o no se establece, la hora del evento importado se almacenará en el metadato event.time. • **port**: Este parámetro se puede establecer en un valor numérico para reemplazar al escucha del puerto de syslog predeterminado, 514.

Ruta de configuración de Decoder	/decoder/config
capture.selected	Muestra la interfaz y el servicio de captura actuales. El cambio se aplica de inmediato.
export.expire.minutes	Indica la cantidad de minutos antes de que los archivos de la caché de exportación venzan y se eliminen. El cambio se aplica de inmediato.
export.packet.enabled	Permite la exportación de datos de paquetes, si está activada. El cambio se hace efectivo con el reinicio del servicio.
export.packet.local.path	Muestra la ubicación local para almacenar en caché los datos exportados de paquetes. Tamaño máximo asignado opcional (=#unit); las unidades son: t de TB, g de GB y m de MB. El cambio se hace efectivo con el reinicio del servicio.
export.packet.max	Muestra el máximo de paquetes por archivo exportado. Para los tipos de archivos de exportación que se almacenan en caché, esto determina los tamaños de memoria almacenados en caché. Cero significa sin límite. El cambio se aplica de inmediato.
export.packet.remote.path	Indica el protocolo remoto (nfs://) y la ubicación para exportar datos. El cambio se hace efectivo con el reinicio del servicio.
export.packet.size.max	Muestra el máximo de bytes de paquetes por archivo exportado. Para los tipos de archivos de exportación que se almacenan en caché, esto determina los tamaños de memoria almacenados en caché. Cero significa sin límite. El cambio se aplica de inmediato.
export.rollup	Determina el intervalo de acumulación para los archivos de exportación. El cambio se hace efectivo con el reinicio del servicio.

Ruta de configuración de Decoder	/decoder/config
export.session.enabled	Permite la exportación de datos de sesiones, si está activada. El cambio se hace efectivo con el reinicio del servicio.
export.session.format	Determina el formato de archivo que se usa durante la exportación de sesiones. El cambio se hace efectivo con el reinicio del servicio.
export.session.local.path	Muestra la ubicación local para almacenar en caché los datos exportados de sesiones. Tamaño máximo asignado opcional (=#unit); las unidades son: t de TB, g de GB y m de MB. El cambio se hace efectivo con el reinicio del servicio.
export.session.max	Muestra el máximo de sesiones por archivo exportado. Para los tipos de archivos de exportación que se almacenan en caché, esto determina los tamaños de memoria almacenados en caché. Cero significa sin límite. El cambio se aplica de inmediato.
export.session.meta.fields	Determina los campos de metadatos que se exportan. Lista de campos separada por comas. Asterisco significa todos los campos. Asterisco más lista de campos significa todos los campos, SALVO los enumerados. Solo lista de campos indica que solo se incluyen esos campos. El cambio se aplica de inmediato.
export.session.remote.path	Muestra el protocolo remoto (nfs://) y ubicación para exportar datos. El cambio se hace efectivo con el reinicio del servicio.
export.session.size.max	Indica el máximo de bytes de sesión por archivo exportado. Para los tipos de archivos de exportación que se almacenan en caché, esto determina los tamaños de memoria almacenados en caché. Cero significa sin límite. El cambio se aplica de inmediato.

Ruta de configuración de Decoder	/decoder/config
export.usage.max	Indica el máximo de bytes de sesión por archivo exportado. Para los tipos de archivos de exportación que se almacenan en caché, esto determina los tamaños de memoria almacenados en caché. Cero significa sin límite. El cambio se aplica de inmediato.
parse.threads	Indica la cantidad de hilos de ejecución de análisis que se usan para el análisis de sesiones. Cero significa que el servidor decide. El cambio se hace efectivo con el reinicio del servicio.
pool.packet.page.size	Muestra el tamaño de una página de paquetes (el valor predeterminado es KB). El cambio se hace efectivo con el reinicio del servicio.
pool.packet.pages	Indica la cantidad de páginas de paquetes que asignará y usará el Decoder. El cambio se hace efectivo con el reinicio del servicio.
pool.session.page.size	Muestra el tamaño de una página de sesiones (el valor predeterminado es KB). El cambio se hace efectivo con el reinicio del servicio.
pool.session.pages	Indica la cantidad de páginas de sesiones que asignará y usará el Decoder. El cambio se hace efectivo con el reinicio del servicio.

Introducción de hosts: Parámetros de configuración del servicio Log Decoder

En este tema se enumeran y se describen los parámetros de configuración disponibles para RSA NetWitness Suite Log Decoders.

Ajustes de configuración de Log Decoder

En este tema se enumeran y se describen los ajustes de configuración de Log Decoder.

Campo Configuración de Log Decoder	Descripción
Base de datos	/database/config, consulte el tema **Nodos de configuración de la base de datos** de la *Guía de ajuste de la base de datos de NetWitness Suite Core*.
Decoder	/decoder/config, consulte Parámetros de configuración de Decoder y Log Decoder
Índice	/index/config, consulte el tema **Nodos de configuración de índices** de la *Guía de ajuste de la base de datos de NetWitness Suite Core*.
Registros	/logs/config, consulte Configuración del registro de los servicios principales.
REST	/rest/config, consulte Configuración de la interfaz de REST
SDK	/sdk/config, consulte el tema **Nodos de configuración de SDK** de la *Guía de ajuste de la base de datos de NetWitness Suite Core* y Modos system.roles de los servicios principales.
Sistema	/sys/config, consulte Configuración del sistema de servicios principales.

Ajustes de configuración del tokenizador de registros

El Log Decoder tiene un conjunto de elementos de configuración que controlan la manera en que el tokenizador de registros crea elementos de metadatos a partir de registros no analizados. El tokenizador de registros se implementa como un conjunto de analizadores incorporados, donde cada uno analiza un subconjunto de tokens reconocibles. En la siguiente tabla se muestra la funcionalidad de cada uno de estos analizadores nativos. Estos elementos word forman una indexación de texto completo cuando se transfieren al motor de indexación en el Concentrator y el Archiver. Mediante la manipulación de la entrada de configuración parsers.disabled, es posible controlar los tokenizadores de registros que están habilitados.

Nombre del analizador	Descripción	Parámetros de configuración
Tokens de registros	Escanea en busca de ejecuciones de caracteres consecutivos para producir elementos de metadatos “word”.	token.device.types, token.char.classes, token.max.length, token.min.length, token.unicode
IPSCAN	Escanea en busca del texto que parece ser una dirección IPv4 para producir los elementos de metadatos “ip.addr”.	token.device.types
IPV6SCAN	Escanea en busca del texto que parece ser una dirección IPv6 para producir los elementos de metadatos “ipv6”.	token.device.types
URLSCAN	Escanea en busca del texto que parece ser un URI para producir los elementos de metadatos “alias.host”, “filename”, “username” y “password”.	token.device.types

Nombre del analizador	Descripción	Parámetros de configuración
DOMAINSCAN	Escanea en busca del texto que parece ser un nombre de dominio para producir los elementos de metadatos “alias.host”, “tld”, “cctld” y “sld”.	token.device.types
EMAILSCAN	Escanea en busca del texto que parece ser una dirección de correo electrónico para producir los elementos de metadatos “email” y “username”.	token.device.types
SYSLOGTIMESTAMPSCAN	Escanea en busca del texto que parece ser registros de fecha y hora con formato de syslog. Syslog carece de la zona horaria y el año. Cuando se encuentra dicho texto, se normaliza en la hora UTC para crear elementos de metadatos “event.time”.	token.device.types
INTERNETTIMESTAMPSCAN	Escanea en busca del texto que parece ser registros de fecha y hora con formato RFC 3339 para crear elementos de metadatos “event.time”.	token.device.types

Estos son los parámetros de configuración del tokenizador de registros.

Campo Configuración de analizador de Log Decoder	Descripción
token.device.types	El conjunto de tipos de dispositivos que se escanearán en busca de tokens de texto crudo. De forma predeterminada, se establece en `unknown`, lo cual significa que solo los registros que no se analizaron se escanearán en busca de texto crudo. Aquí puede agregar tipos de registros adicionales para enriquecer los registros analizados con información de token de texto. Si este campo está vacío, la Tokenization de registros se deshabilita.
token.char.classes	Este campo controla el tipo de tokens que se generan. Puede ser cualquier combinación de los valores `alpha`, `digit`, `space` y `punct`. El valor predeterminado es `alpha`. • **alpha**: los tokens pueden contener caracteres alfabéticos • **digit**: los tokens pueden contener números • **space**: los tokens pueden contener espacios y tabulaciones • **punct**: los tokens pueden contener signos de puntuación
token.max.length	Este campo pone un límite a la longitud de los tokens. El valor predeterminado es cinco caracteres. El ajuste de longitud máxima permite que el Log Decoder limite el espacio necesario para almacenar los metadatos word. El uso de tokens más largos requiere más espacio para la base de datos de metadatos, pero puede proporcionar búsquedas de texto crudo un poco más rápidas. El uso de tokens más cortos hace que el solucionador de consultas de texto deba realizar más lecturas desde los registros crudos durante las búsquedas, pero tiene el efecto de usar mucho menos espacio en la base de datos de metadatos y el índice.

Campo Configuración de analizador de Log Decoder	Descripción
token.min.length	Es la longitud mínima de un token de texto con capacidad de búsqueda. La longitud mínima del token corresponderá a la cantidad mínima de caracteres que un usuario puede escribir en el cuadro de búsqueda para encontrar los resultados. El valor recomendado es el predeterminado, 3.
token.unicode	Este ajuste booleano controla si se aplican las reglas de clasificación unicode durante la clasificación de caracteres según la configuración de token.char.classes. Si se establece en true, cada registro se trata como una secuencia de puntos de código codificados con UTF-8 y la clasificación se realiza después de la decodificación de UTF-8. Si este valor se establece en false, cada registro se trata como caracteres ASCII y solo se realiza la clasificación de caracteres ASCII. La clasificación de caracteres Unicode requiere más recursos de CPU en el Log Decoder. Si la indexación de texto distinto del inglés no se requiere, puede deshabilitar esta configuración para reducir la utilización de CPU en el Log Decoder. Está activada de forma predeterminada.

Parámetros de configuración de la interfaz REST

En este tema se enumeran y se describen los parámetros de configuración disponibles para la interfaz REST incorporada en todos los servicios de NetWitness Suite Core.

Ajustes de configuración

En la siguiente tabla se enumeran y se describen los parámetros de configuración de REST:

Ruta de configuración de REST	/rest/config
cache.dir	Muestra el directorio del host que se usa para la creación y el almacenamiento temporal de archivos. El cambio se hace efectivo con el reinicio del servicio.
cache.size	Muestra el tamaño máximo total (la unidad predeterminada es MB) de todos los archivos en el directorio de caché antes de que se eliminen los más antiguos. El cambio se hace efectivo con el reinicio del servicio.
enabled	Cambia para activar o desactivar los servicios REST: 1 es activado y 0 es desactivado. El cambio se hace efectivo con el reinicio del servicio.
puerto	Muestra el puerto en el cual escuchará el servicio REST. El cambio se hace efectivo con el reinicio del servicio.
ssl	Cifra todo el tráfico REST mediante SSL, si está activado. El valor predeterminado “system” significa que se usa la configuración de /sys/config/ssl. El cambio se hace efectivo con el reinicio del servicio.

Introducción de hosts: Modos system.roles de servicios Core de NetWitness Platform

Todos los servicios Core de NetWitness Platform ofrecen modos de autorización basada en funciones. En este tema se describen los modos que están disponibles y cómo se configuran dentro de cada servicio.

El nodo de configuración `/sdk/config/system.roles` establece los permisos de consulta y visualización para metadatos y contenido clave por clave. Este parámetro es compatible con la función de administración de la privacidad de datos y, cuando se habilita con el uso de uno de los valores distintos de cero, ayuda a un encargado de la privacidad de datos a controlar el acceso a claves de metadatos y contenido específicos. Este parámetro se puede configurar en la interfaz del usuario de NetWitness Platform (consulte el tema **Pestaña Privacidad de datos** de la *Guía de administración de la privacidad de datos* para obtener detalles). Cuando se edita el valor, el cambio se aplica de inmediato.

Cero significa que los permisos de servicios basados en claves de metadatos de SDK están inhabilitados.

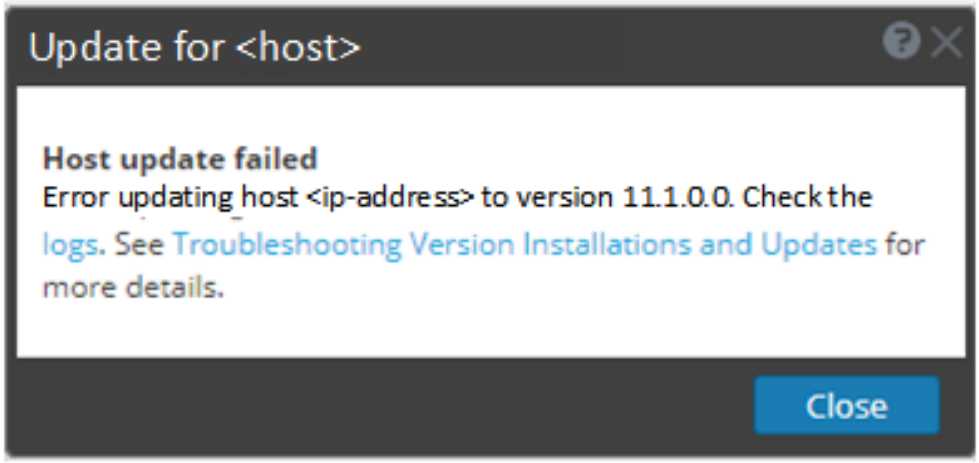
- 0: desactivado

Cuando se especifica uno de los valores distintos de cero, el encargado de la privacidad de datos puede seleccionar una clave de metadatos para poner en lista blanca o negra la presentación de los metadatos o el contenido (o ambos) asociados para una función de usuario específica en un servicio.

- 1: poner en lista blanca metadatos y contenido filtrados
- 2: poner en lista blanca metadatos filtrados
- 3: poner en lista blanca contenido filtrado
- 4: poner en lista negra metadatos y contenido filtrados
- 5: poner en lista negra metadatos filtrados
- 6: poner en lista negra contenido filtrado

Introducción de hosts: Solución de problemas de instalaciones y actualizaciones de versión

En esta sección se describen los mensajes de error que se muestran en la vista **Hosts** cuando se producen problemas durante la actualización de versiones de hosts y la instalación de servicios en hosts en la vista **Hosts**. Si no puede resolver algún problema de actualización o instalación con los siguientes métodos de solución de problemas, póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

Mensaje de error	
Problema	Cuando selecciona una versión de actualización y hace clic en **Actualizar** > **Actualizar host**, el proceso de descarga se realiza correctamente, pero el proceso de actualización falla.

Solución	1. **Intente volver a aplicar la actualización de versión al host**.
	A menudo, esto es todo lo que debe hacer.
	2. Si aún no puede aplicar la actualización de versión nueva:
	a. Monitoree los siguientes registros en el servidor de NW a medida que avanza (por ejemplo, envíe la cadena de comandos `tail -f` desde la línea de comandos):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`

El error aparecerá en uno o más de estos registros.

b. Intente solucionar el problema y vuelva a aplicar la actualización de versión.

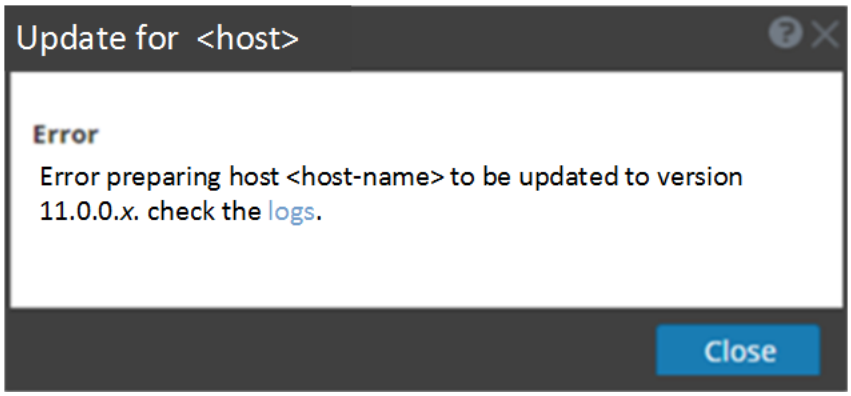
- Causa 1: La contraseña de `deploy_admin` venció.
  Solución: Restablezca su contraseña de `deploy_admin`.
  Realice los siguientes pasos para resolver la causa 1.

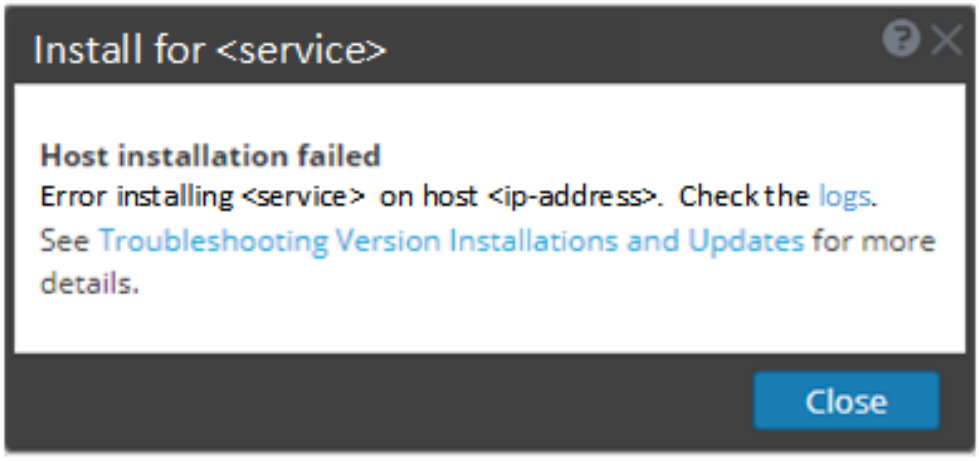
  1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**.
  2. Seleccione `deploy_admin` y haga clic en **Restablecer contraseña**.
  3. (Condicional) Si NetWitness Suite no le permite restablecer una contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos.
     a. Restablezca `deploy_admin` para utilizar una contraseña nueva.
     b. En todos los hosts de servidores que no son de NW en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` coincidente desde el host del servidor de NW.
     `/opt/rsa/saTools/bin/set-deploy-admin-password`

- Causa 2: La contraseña de `deploy_admin` se cambió en el host del servidor de NW, pero no se cambió en hosts de servidores que no son de NW.
  Realice el siguiente paso para resolver la causa 2.

  - En todos los hosts de servidores que no son de NW en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` coincidente desde el host del servidor de NW.
    `/opt/rsa/saTools/bin/set-deploy-admin-password`

3. Si aún no puede aplicar la actualización, reúna los registros del paso 2 y póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

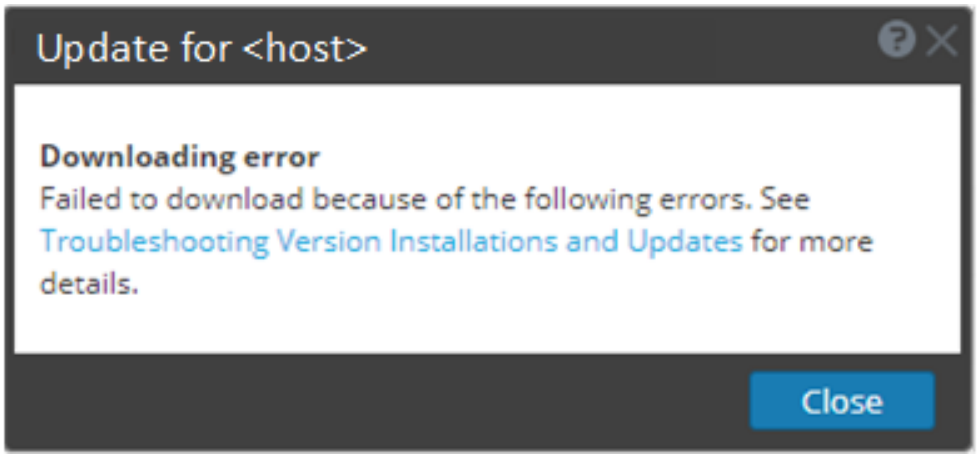
Mensaje de error	 `/var/log/netwitness/orchestration-server/orchestration-server.log` tiene un error similar al siguiente: `API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.0.0.x' is not supported`
Problema	Después de actualizar el host del servidor de NW a 11.1, la única ruta de actualización para los hosts de servidores que no son de NW es 11.1. Si intenta actualizar cualquier host de servidor que no es de NW a un parche de 11.0.0.n (por ejemplo, de 11.0.0.0 a 11.0.0.3), obtendrá este mensaje de error en /var/log/netwitness/orchestration-server/orchestration-server.log.
Solución	Actualice el host de servidor que no es de NW a 11.1.

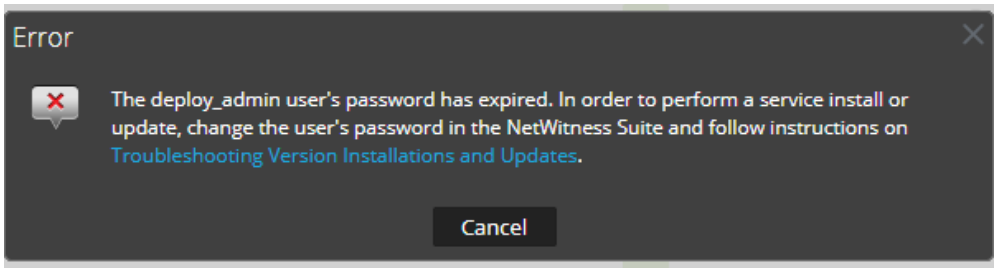
Mensaje de error	
Problema	Cuando selecciona un host y hace clic en **Instalar**, el proceso del servicio de instalación falla.

Solución	1. **Intente volver a instalar el servicio.**.
	A menudo, esto es todo lo que debe hacer.
	2. Si aún no puede instalar el servicio:
	a. Monitoree los siguientes registros en el servidor de NW a medida que avanza (por ejemplo, envíe la cadena de comandos `tail -f` desde la línea de comandos):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	El error aparecerá en uno o más de estos registros.
	b. Intente solucionar el problema y reinstale el servicio.
	• Causa 1: Se ingresó una contraseña de `deploy_admin` incorrecta en nwsetup-tui.
	Solución: Recupere su contraseña de `deploy_admin` .
	Realice los siguientes pasos para resolver la causa 1.
	1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**.
	2. Seleccione `deploy_admin` y haga clic en **Restablecer contraseña**.
	3. (Condicional) Si NetWitness Suite no le permite restablecer una contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos.
	a. Acceda mediante el protocolo SSH al host del servidor de NW.
	`security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name platform.deployment.password -quiet`
	b. Acceda mediante el protocolo SSH al host en el cual falló la instalación/coordinación.
	c. Vuelva a ejecutar nwsetup-tui con el uso de la contraseña de `deploy_admin` correcta.

- Causa 2: La contraseña de `deploy_admin` venció.
  Realice el siguiente paso para resolver la causa 2.
  1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**.
  2. Seleccione `deploy_admin` y haga clic en **Restablecer contraseña**.
  3. (Condicional) Si NetWitness Suite le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos.
     a. Ingrese la contraseña de `deploy_admin` vencida.
     b. Deseleccione la casilla de verificación Forzar cambio de contraseña en el próximo inicio de sesión.
     c. Haga clic en **Guardar**.
  4. (Condicional) Si NetWitness Suite no le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo Restablecer contraseña, realice los siguientes pasos.
     a. Restablezca `deploy_admin` para utilizar una contraseña nueva.
     b. En todos los hosts del servidor de NW y en todos los demás hosts en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` nueva.
     `/opt/rsa/saTools/bin/set-deploy-admin-password`
     c. En el host en el cual falló la instalación/coordinación, ejecute nwsetup-tui y use la contraseña de `deploy_admin` nueva.

3. Si aún no puede aplicar la actualización, reúna los registros del paso 2 y póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

Mensaje de error	
Problema	Cuando selecciona una versión de actualización y hace clic en **Actualizar** >**Actualizar host**, la descarga comienza, pero no se completa.
Causa	Los archivos de descarga de versiones pueden ser grandes y su descarga puede tardar mucho tiempo. Si se producen problemas de comunicación durante la descarga, esta fallará.
Solución	1. Intente volver a descargarlo. 2. Si la descarga continúa fallando, intente descargarlo fuera de NetWitness Suite, como se describe en Aplicar actualizaciones desde la línea de comandos (sin acceso a la Web). 3. Si aún no puede descargar el archivo de actualización, póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

Mensaje de error	
Causa	La contraseña del usuario `deploy_admin` venció.
Solución	Restablezca la contraseña de `deploy_admin`. 1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**. 2. Seleccione **deploy_admin** y haga clic en **Restablecer contraseña**. • Si NetWitness Suite le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos. a. Ingrese la contraseña de `deploy_admin` vencida. b. Deseleccione la casilla de verificación **Forzar cambio de contraseña en el próximo inicio de sesión**. c. Haga clic en **Guardar**. • Si NetWitness Suite no le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**. a. En el host del servidor de NW y en todos los demás hosts en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` nueva. `/opt/rsa/saTools/bin/set-deploy-admin-password` b. En el host en el cual falló la instalación/coordinación, ejecute nwsetup-tui y use la contraseña de `deploy_admin` nueva.