RSA NETWITNESS® SUITE

Guía de configuración de Archiver

para la versión 11.0

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

febrero 2018

Contenido

Descripción general de Archiver

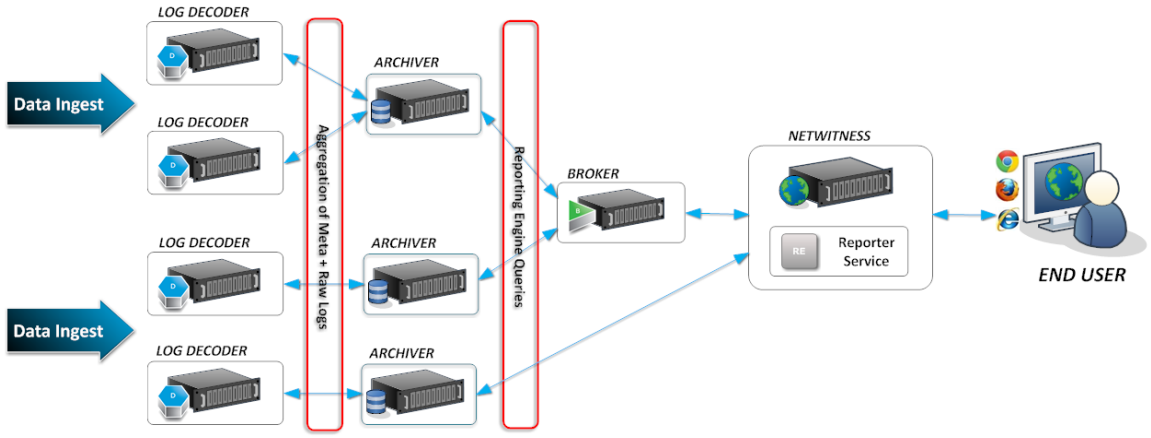
En esta guía se proporcionan instrucciones detalladas sobre cómo configurar Archiver en la red, procedimientos adicionales que se usan en otros momentos y materiales de referencia que describen la interfaz del usuario para configurar Archiver en la red.

NetWitness Suite Archiver es un dispositivo que permite el archiving de registros a largo plazo mediante la indexación y la compresión de datos del registro y su envío a almacenamiento de archiving. Posteriormente, el almacenamiento de archiving se optimiza para la retención de datos a largo plazo y la creación de informes de cumplimiento de normas.

Archiver almacena registros crudos y metadatos de registros de Log Decoders para la retención a largo plazo y utiliza capacidad de conexión directa (DAC) para el almacenamiento.

Nota: Los paquetes crudos y los metadatos de paquetes no se almacenan en Archiver.

En la siguiente figura se muestra la arquitectura de una red de NetWitness Suite que implementa Archiver.



Configuración de un Archiver

NetWitness Suite Archiver es un dispositivo que permite el archiving de registros a largo plazo mediante la indexación y la compresión de datos del registro y su envío a almacenamiento de archiving. Posteriormente, el almacenamiento de archiving se optimiza para la retención de datos a largo plazo y la creación de informes de cumplimiento de normas.

Archiver almacena registros crudos y metadatos de registros de Log Decoders para la retención a largo plazo y utiliza capacidad de conexión directa (DAC) para el almacenamiento.

Nota: Los paquetes crudos y los metadatos de paquetes no se almacenan en Archiver.

Requisitos previos

Asegúrese de haber:

- Instalado el host de Archiver en el ambiente de red.
- Instalado y configurado Log Decoder versión 11.0.0.0 en el ambiente de red.

Si desea configurar múltiples servicios Archiver o Concentrator como un grupo y compartir las tareas de agregación entre ellos, consulte **Agregación de grupos** en la *Guía de implementación*.

Flujo de trabajo

En este flujo de trabajo se ilustra el proceso de instalación y configuración de punto a punto para un Archiver.

En la siguiente tabla se describen los pasos básicos para configurar un Archiver. Las tareas se deben completar en la secuencia en que se presentan.

Paso de configuración	Descripción
Agregar el servicio Archiver	En este tema se proporciona información sobre cómo agregar un servicio Archiver en el host de Archiver y aplicarle una licencia.

Paso de configuración	Descripción
Agregar Log Decoder como un origen de datos en Archiver	Se proporcionan instrucciones sobre cómo agregar un Log Decoder en un Archiver.
Configurar el almacenamiento y la retención de registros de Archiver	Se proporcionan instrucciones sobre cómo configurar el almacenamiento y la retención de registros en un Archiver.
Agregar Archiver como un origen de datos en Reporting Engine	Se proporcionan instrucciones sobre cómo agregar un Archiver como un origen de datos en Reporting Engine para generar informes de los datos que recopila Archiver.
Configurar el monitoreo de Archiver	Se proporcionan instrucciones sobre cómo configurar el mecanismo de alerta relacionado con el almacenamiento de Archiver.

Agregar el servicio Archiver

Para agregar un servicio Archiver, asegúrese de haber instalado un host de Archiver en el cual desea ejecutar el servicio Archiver. Consulte **Paso 1: Agregar o actualizar un host** de la *Guía de introducción de hosts y servicios* para conocer el procedimiento que explica cómo agregar un host.

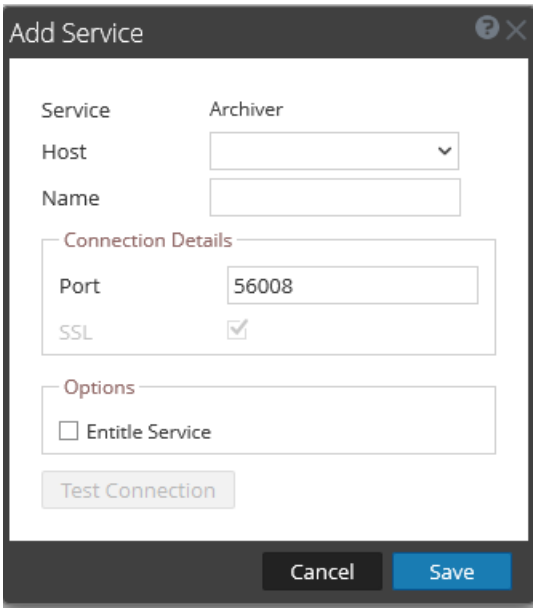
Después de instalar un host de Archiver, debe agregar un servicio Archiver y aplicarle una licencia, como se explica en el siguiente procedimiento.

Nota: Este procedimiento solo es necesario si el servicio Archiver no está instalado.

Realice los siguientes pasos para agregar el servicio Archiver:

1. Vaya a **ADMIN > Servicios**.
2. En la barra de herramientas del panel **Servicios**, seleccione + **> Archiver**.

   Se muestra el cuadro de diálogo Agregar servicio.



3. Ingrese los siguientes detalles.

Campo	Descripción
Host	Seleccione un host en el menú desplegable.
Nombre	Escriba un nombre para el servicio.
Puerto	El puerto predeterminado es 50008.

Campo	Descripción
SSL	Seleccione **SSL** si desea que NetWitness Suite se comunique con el servicio mediante SSL. La seguridad de la transmisión de datos se administra mediante el cifrado de la información y el suministro de autenticación con certificados SSL. **Nota:** si selecciona SSL, asegúrese de que este protocolo esté activado en el panel Configuración del sistema.
Nombre de usuario	(Opcional) Escriba el nombre de usuario para el servicio.
Contraseña	(Opcional) Escriba la contraseña para el servicio.
Conferir autorizaciones al servicio	Seleccione si desea aplicar las autorizaciones configuradas actualmente para este servicio. Para obtener más información, consulte el tema **Implementación de la funcionalidad de autorización** de la *Guía de licencia*.

4. Haga clic en **Probar conexión** para determinar si NetWitness Suite se conecta al servicio.
5. Cuando el resultado sea satisfactorio, haga clic en **Guardar**.

   El servicio agregado ahora se muestra en el panel Servicios.

   Nota: Si el resultado de la prueba no es satisfactorio, edite la información del servicio y vuelva a intentarlo.

6. Aplique la licencia al servicio Archiver.

   Consulte el tema **Sincronizar el servidor de Servidor de NetWitness** de la *Guía de licencia* para obtener detalles sobre el procedimiento para activar el servicio Archiver (aplicarle una licencia).

Agregar Log Decoder como un origen de datos en Archiver

Para agregar un Log Decoder como un origen de datos en Archiver, debe haber instalado el host de Archiver en el ambiente de red, haber instalado y configurado un Log Decoder en su ambiente de red y haber agregado el host de Archiver en NetWitness Suite, y debe asegurarse de que el servicio Archiver se muestre como activo y con licencia.

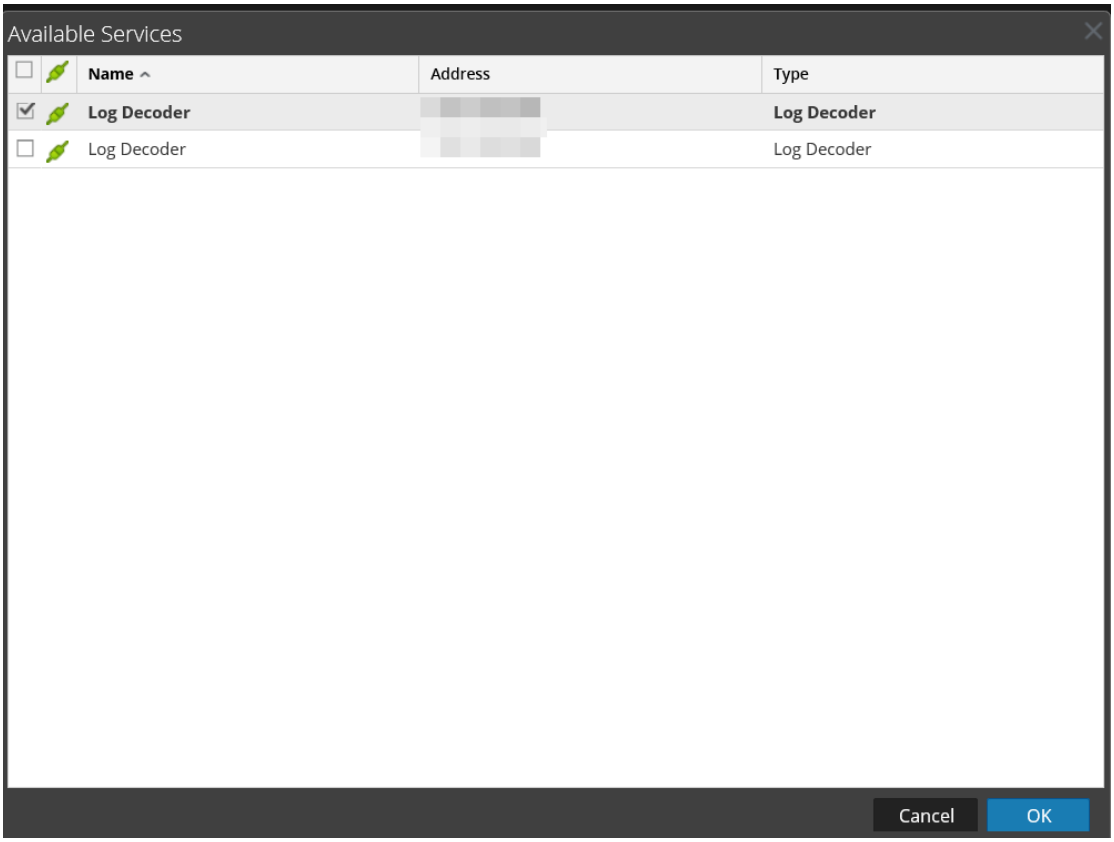
Agregar Log Decoder como un origen de datos en Archiver

Para agregar un Log Decoder como un origen de datos en un Archiver:

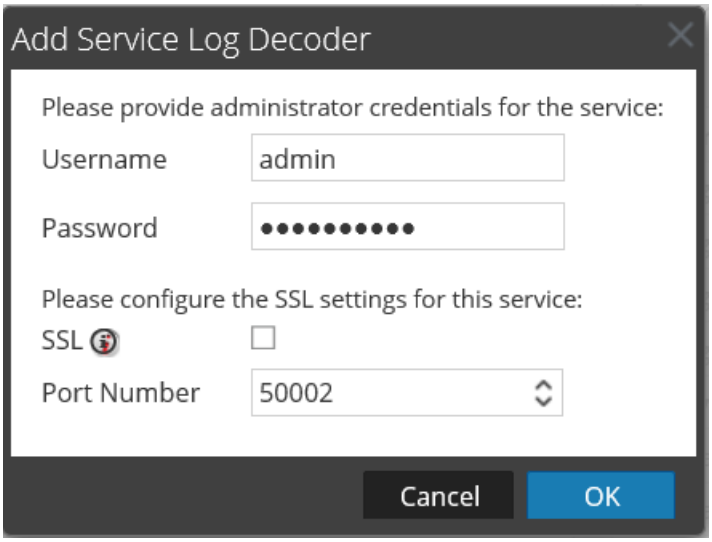
1. Vaya a **ADMIN > Servicios**.
2. Seleccione el servicio Archiver.
3. En la columna **Acciones**  , seleccione **Ver > Configuración**.

   Se muestra la vista Configuración de servicios de Archiver.
4. En la pestaña **General**, panel **Servicios agregados**, haga clic en +.

   Se muestra el cuadro de diálogo Servicios disponibles.



5. Seleccione el servicio Log Decoder que desea agregar como un origen de datos en Archiver y haga clic en **Aceptar**.
6. Si el Log Decoder está utilizando el modelo de confianza, aparece un cuadro de diálogo Agregar servicio.



7. Escriba el nombre de usuario y la contraseña del Log Decoder y configure los ajustes de SSL.
8. Haga clic en **Aceptar**.
   El servicio de Log Decoder seleccionado se muestra en el panel **Servicios agregados**.

Consideraciones de configuración de metadatos de Archiver

Para maximizar el tiempo de retención, los elementos de metadatos y el índice del Archiver se redujeron (en comparación con el Concentrator) con el fin de apoyar las necesidades comunes de creación de informes. Esto significa que, de forma predeterminada, tal vez no pueda ejecutar en el Archiver todos los informes que ejecuta en el Concentrator. Puede ver una lista de elementos de metadatos e índice actuales que utiliza el Archiver en las siguientes ubicaciones:

- **Vista Explorador**: En la ruta **/archiver/devices/<logdecoder>/config/options** en el campo **Inclusión de metadatos** se muestra la lista actual de elementos de metadatos.
- **Vista Configuración > pestaña Archivos**: El archivo **index-archiver.xml** muestra la configuración predeterminada del índice. El archivo **index-archiver-custom.xml** muestra las modificaciones.

Los elementos de metadatos y el índice de Archiver se pueden personalizar para apoyar necesidades de creación de informes específicas del cliente, sin embargo esto requerirá el soporte de almacenamiento, recursos de CPU y recursos de memoria adicionales y puede afectar el tiempo de retención. A medida que se agregan más elementos de metadatos al Archiver, disminuirá la tasa de agregación máxima y aumentará el tiempo de ejecución de los informes.

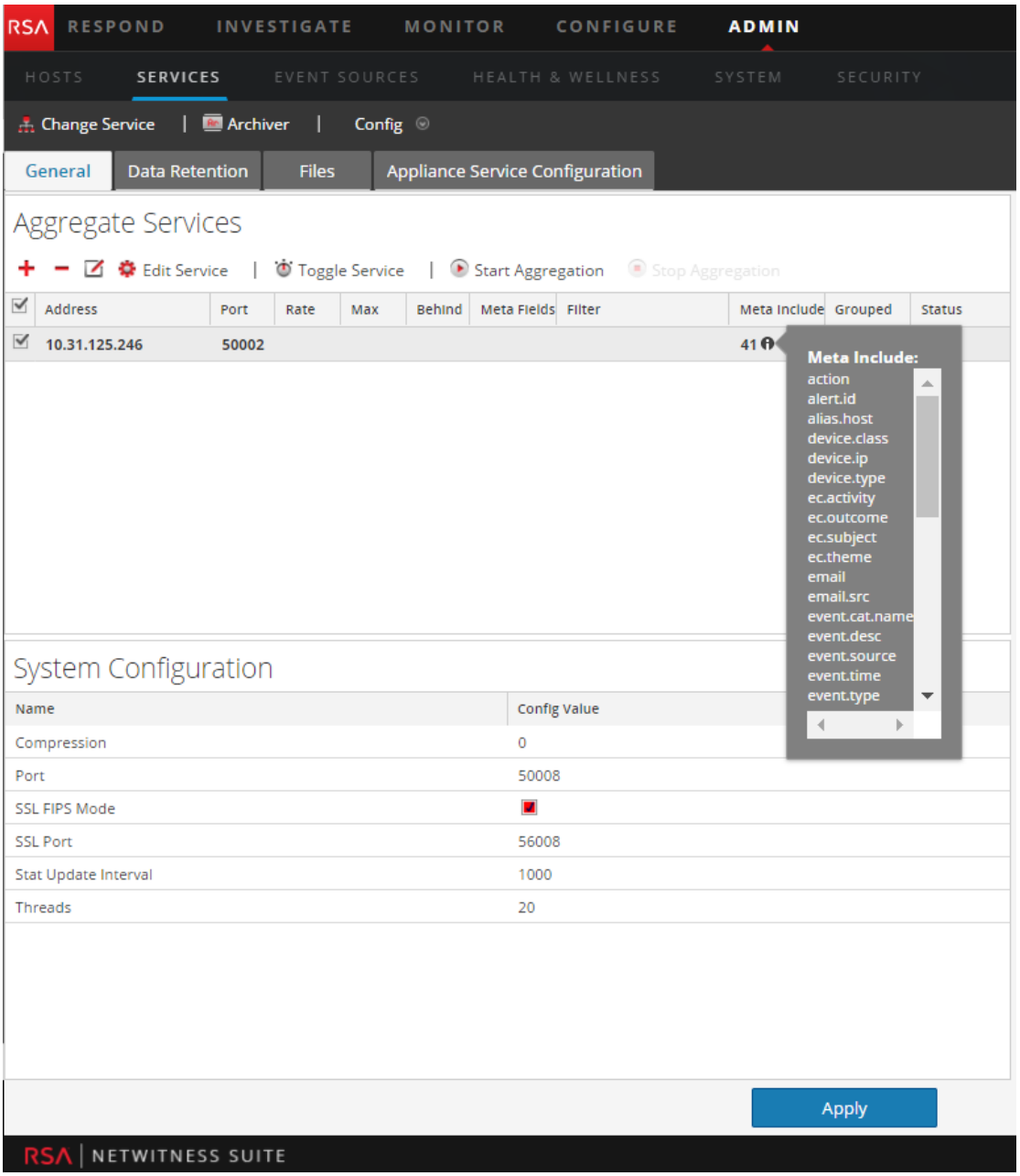
Consulte (Opcional) Configurar filtros de metadatos para agregación y (Opcional) Agregar entradas de índice para la creación de informes de Archiver para obtener información adicional.

(Opcional) Configurar filtros de metadatos para agregación

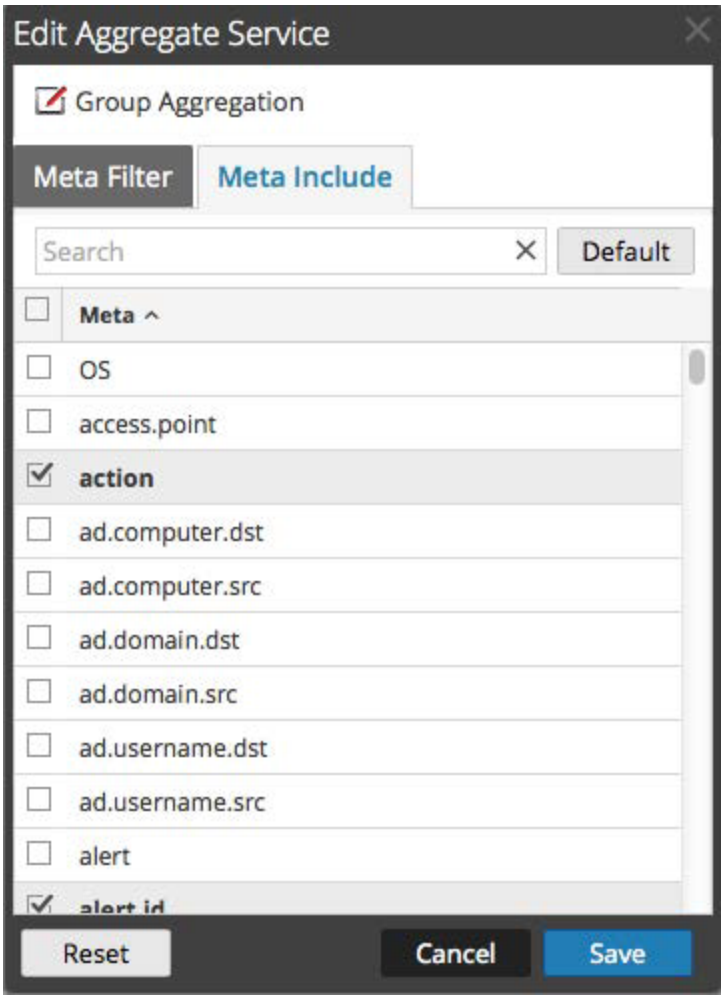
Siga este procedimiento para ver y agregar elementos de metadatos adicionales al Archiver.

Precaución: La adición de metadatos o índices requerirá el soporte de almacenamiento, recursos de CPU y recursos de memoria adicionales y puede afectar el tiempo de retención. A medida que se agregan más elementos de metadatos al Archiver, disminuirá la tasa de agregación máxima y aumentará el tiempo de ejecución de los informes.

1. Para ver los elementos de metadatos actuales, en el panel **Servicios agregados**, seleccione el servicio Log Decoder y haga clic en en el campo **Inclusión de metadatos**.



2. Para agregar elementos de metadatos adicionales, seleccione el servicio Log Decoder y haga clic en .



3. En el cuadro de diálogo Editar servicio agregado, seleccione los elementos de metadatos que se incluirán en la lista Inclusión de metadatos. Por ejemplo, puede considerar la inclusión de ip.srcport, tcp.srcport, udp.srcport, msg, url, query, bytes, alias.host, ip.dst, ip.dstport, ip.src, tcp.dstport, megabytes, time, event.desc y word.
4. Haga clic en **Guardar** y, a continuación, en **Aplicar**.
5. Consulte (Opcional) Agregar entradas de índice para la creación de informes de Archiver, a continuación, para obtener información sobre cómo indexar las claves de metadatos adicionales.

(Opcional) Agregar entradas de índice para la creación de informes de Archiver

Precaución: La adición de metadatos o índices requerirá el soporte de almacenamiento, recursos de CPU y recursos de memoria adicionales y puede afectar el tiempo de retención. A medida que se agregan más elementos de metadatos al Archiver, disminuirá la tasa de agregación máxima y aumentará el tiempo de ejecución de los informes.

La configuración predeterminada del índice del Archiver solo incluye índices de valores de las siguientes claves:

- time
- origen de Decoder (did)
- cuenta de usuario de destino (user.dst)
- ID de alerta (alert.id)
- dirección IP de dispositivo (device.ip)
- dirección IP de origen (ip.src)
- dirección IP de destino (ip.dst)
- descripción de evento (event.desc)
- clase de dispositivo (device.class)
- medium
- nombre de objeto (obj.name)
- palabra

Para obtener información sobre cómo personalizar esta lista, consulte **Personalización del índice** de la *Guía de ajuste de la base de datos de Core*.

Configurar el almacenamiento y la retención de registros de Archiver

En este tema se proporcionan instrucciones a los administradores para configurar el almacenamiento y la retención de registros en un Archiver.

Por motivos de cumplimiento de normas, suele ser necesario conservar algunos registros durante más tiempo que otros. Algunos registros son confidenciales desde el punto de vista legal y no se pueden conservar durante un período prolongado. Para otros registros existe el requisito de conservación durante años. Además del cumplimiento de normas, algunos registros son útiles para análisis forense histórico y otros tienen un valor pertinente mínimo o nulo en materia de seguridad u operacional, y se pueden eliminar después de un período breve.

Debido a que los requisitos de negocios varían, NetWitness Suite permite configurar recopilaciones, las cuales son conjuntos de retención de registros para almacenar datos del registro. Para cada recopilación, puede especificar la cantidad de espacio de almacenamiento total que se usará y los días durante los cuales se conservarán los registros en la recopilación. Para especificar el tipo de registros que se guardan en la recopilación, debe definir reglas de retención que se asocian con las recopilaciones. Las reglas de retención para todas las recopilaciones se ejecutan secuencialmente en un orden que usted define.

Para esto, primero debe definir el espacio de almacenamiento físico total para las recopilaciones. NetWitness Suite permite definir tres tipos de almacenamiento:

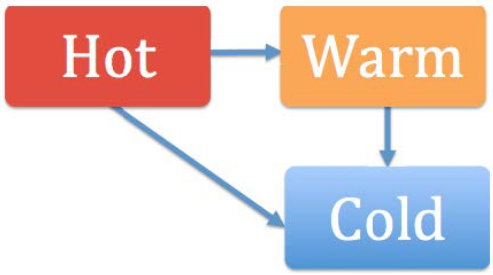
- **Almacenamiento del nivel activo**: Este almacenamiento contiene datos del registro que están en uso activo como parte del proceso de negocios. Los usuarios pueden acceder a estos registros con mayor rapidez que otros tipos de almacenamiento y pueden usarlos para la creación de informes y otras tareas. El almacenamiento activo suele ser almacenamiento de capacidad de conexión directa (DAC) o SAN.
- **Nivel de almacenamiento semiactivo**: (Opcional) Este almacenamiento contiene datos del registro más antiguos que agrega el Archiver. El acceso a los datos del registro es más lento que en el almacenamiento activo. Los usuarios también pueden utilizar estos registros para la creación de informes y otras tareas. El almacenamiento semiactivo suele ser almacenamiento conectado en red (NAS).
- **Nivel de almacenamiento inactivo**: (Opcional) Este almacenamiento contiene los datos del registro más antiguos que se requieren para la operación del negocio o que exigen los requisitos normativos. Los registros están offline y Archiver no puede acceder a ellos para la creación de informes y otras tareas. Sin embargo, si desea acceder a estos datos del registro, puede restaurarlos a las recopilaciones creadas en el servicio Archiver y usarlos posteriormente para la creación de informes. El almacenamiento inactivo suele ser

almacenamiento offline, como NAS, o almacenamiento temporal antes del archiving en cintas. Una vez que los datos se transfieren al nivel inactivo, Archiver deja de administrarlos. Cuando se transfieren, procesos externos se encargan de respaldarlos o de administrar ese espacio del nivel inactivo de modo que no alcance el 100 % de la capacidad. Si se alcanza la capacidad, Archiver detiene la agregación hasta que se resuelve el problema.

Los Archivers están preconfigurados para utilizar el almacenamiento activo disponible y una recopilación de registros predeterminada, de modo que no es necesario configurar el almacenamiento ni la retención de registros del Archiver si no se tienen requisitos de retención de registros complejos.

Los registros se pueden transferir de un tipo de almacenamiento a otro de las siguientes maneras:

- Almacenamiento activo > Almacenamiento inactivo
- Almacenamiento activo > Almacenamiento semiactivo > Almacenamiento inactivo



Cuando una recopilación llega a sus límites de retención para el almacenamiento activo y semiactivo, NetWitness Suite elimina los datos del registro desde el almacenamiento activo o semiactivo. Cuando se ha configurado almacenamiento inactivo, se deja una copia en el almacenamiento inactivo antes de que los registros se eliminen del almacenamiento activo o semiactivo. Por ejemplo, si tiene una recopilación con almacenamiento activo de 1 TB, almacenamiento semiactivo de 1 TB y almacenamiento inactivo habilitado, cuando los datos del registro alcanzan 1 TB de almacenamiento activo, los más antiguos se transfieren al almacenamiento semiactivo. Cuando los datos del registro en el almacenamiento semiactivo alcanzan 1 TB, los más antiguos se copian del almacenamiento semiactivo al inactivo antes de quitarse del almacenamiento semiactivo.

En el caso del almacenamiento activo y semiactivo, los ajustes del tamaño y el período de retención para una recopilación pueden reemplazarse mutuamente en función del criterio que se cumple primero (tamaño o tiempo). Por ejemplo, si tiene una recopilación con almacenamiento activo de 1 TB, sin almacenamiento semiactivo o inactivo y con un período de retención de 20 días, y los datos del registro superan 1 TB después de 11 días, los registros más antiguos por sobre 1 TB se eliminarán aunque la recopilación tenga un período de retención de 20 días.

Después de crear almacenamiento activo, semiactivo e inactivo, debe configurar recopilaciones de almacenamiento de retención de registros. Puede especificar el tamaño máximo del almacenamiento activo y semiactivo para la recopilación, si desea usar almacenamiento inactivo, la cantidad de días que se conservarán los registros en la recopilación, la compresión de datos y si desea usar un algoritmo hash para poder verificar la integridad de los datos de los archivos que se guardan.

Después de configurar las recopilaciones, debe definir reglas de retención para la recopilación. Estas reglas especifican el tipo de registros que se almacenarán en la recopilación. Cada recopilación debe tener al menos una regla de retención asociada para almacenar datos del registro.

Procedimiento

Realice las siguientes tareas en el orden que se muestra para configurar el almacenamiento y la retención de registros.

Tarea	Referencia
1. Configurar el almacenamiento activo, semiactivo e inactivo total.	Consulte Configurar el almacenamiento activo, semiactivo e inactivo.
2. Configurar recopilaciones de almacenamiento de retención de registros.	Consulte Configurar recopilaciones de almacenamiento de registros.
3. Definir reglas de retención para las recopilaciones y determinar el orden de ejecución de la lista general de reglas de retención.	Consulte Definir reglas de retención.

Configurar el almacenamiento activo, semiactivo e inactivo

En este tema se proporcionan instrucciones a los administradores para configurar el almacenamiento activo, semiactivo e inactivo total en un Archiver.

En un host de Archiver, el almacenamiento activo está preconfigurado en los valores predeterminados. Los administradores pueden configurar el almacenamiento activo, semiactivo e inactivo total para satisfacer sus requisitos de negocios específicos. En un Archiver, el almacenamiento activo total debe estar configurado, pero las configuraciones de almacenamiento semiactivo e inactivo son opcionales. NetWitness Suite no administra el almacenamiento inactivo.

Requisitos previos

Asegúrese de haber:

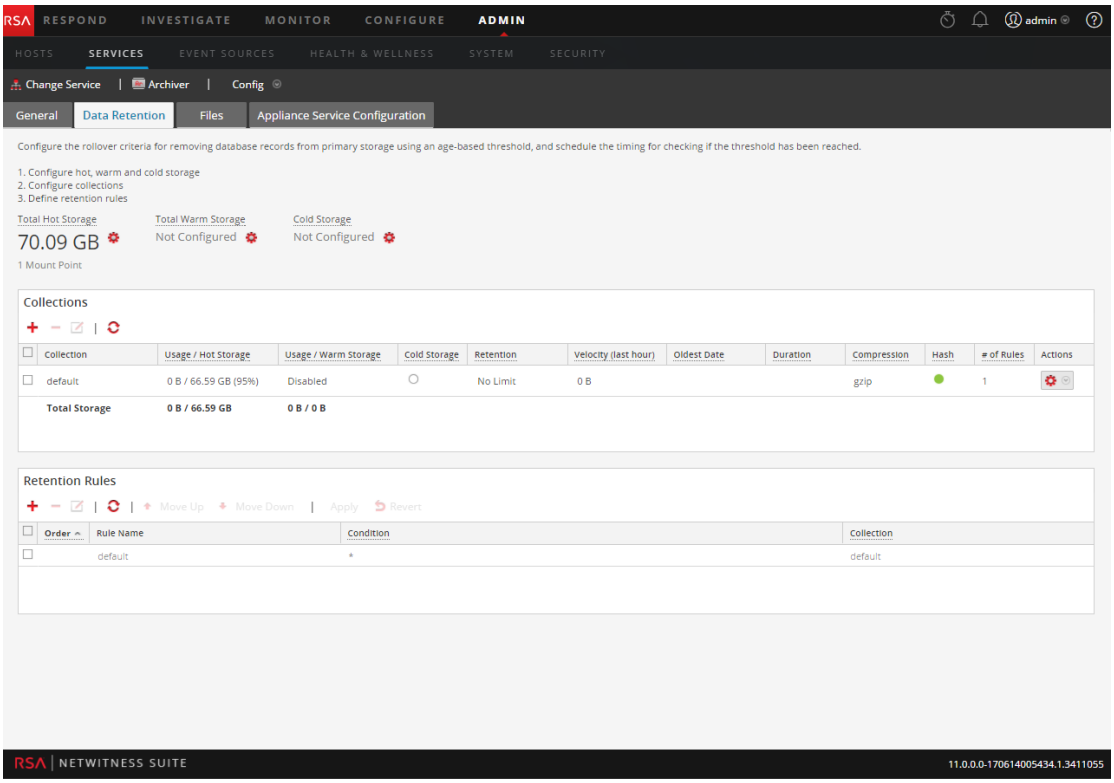
1. Instalado el host de Archiver en el ambiente de red.
2. Instalado y configurado Log Decoder en el ambiente de red.
3. Agregado Archiver como un servicio principal en la implementación de NetWitness Suite.
4. Agregado servicios Log Decoder como un origen de datos para Archiver.
5. Instalado y configurado DAC u otro almacenamiento físico en el ambiente de red.
6. Determinado los requisitos de retención y almacenamiento de registros.

Procedimientos

Configurar el almacenamiento activo total para un Archiver

1. Vaya a **ADMIN > Servicios**.
2. Seleccione el servicio Archiver y elija  **> Ver > Configuración**.

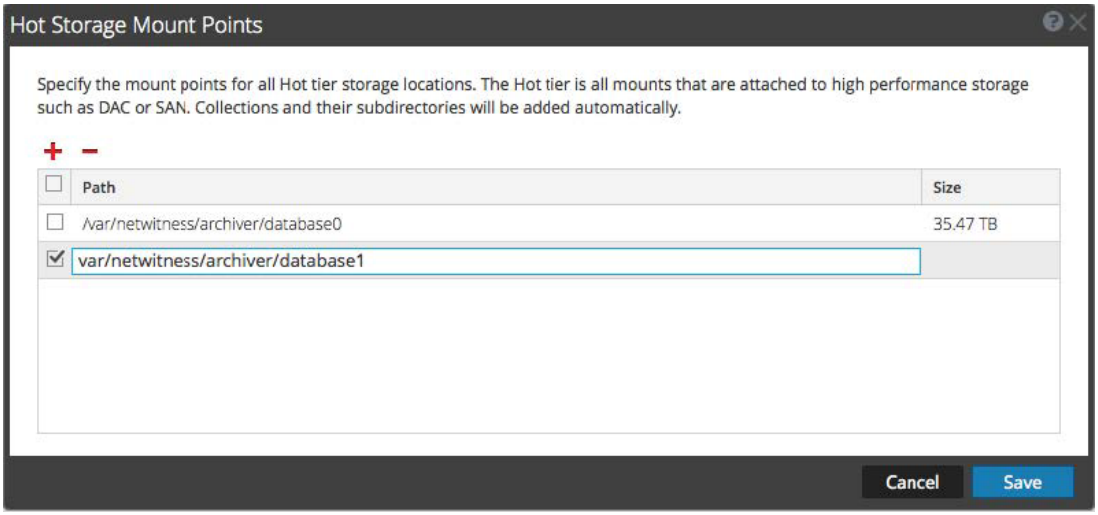
   Se muestra la vista Configuración de servicios de Archiver.
3. En la pestaña **Retención de datos**, en la sección **Almacenamiento activo total**, haga clic en  para configurar el almacenamiento activo total.



4. En el cuadro de diálogo **Puntos de montaje del almacenamiento activo**, agregue los puntos de montaje conectados al host de Archiver que desea incluir en Almacenamiento activo total.

   Estas son las rutas al almacenamiento de alto rendimiento, como el almacenamiento DAC y la SAN. No agregue recopilaciones ni subdirectorios a los puntos de montaje.

   Para agregar un punto de montaje, haga clic en + y escriba la ruta al punto de montaje.



5. Verifique que las rutas del punto de montaje estén correctas y haga clic en **Guardar**.

   NetWitness Suite creará automáticamente los directorios metadb, packetdb, sessiondb e

index para cada recopilación definida en el Archiver:
<storageLocation>/<CollectionName>/metadb
<storageLocation>/<CollectionName>/packetdb
<storageLocation>/<CollectionName>/sessiondb
<storageLocation>/<CollectionName>/index

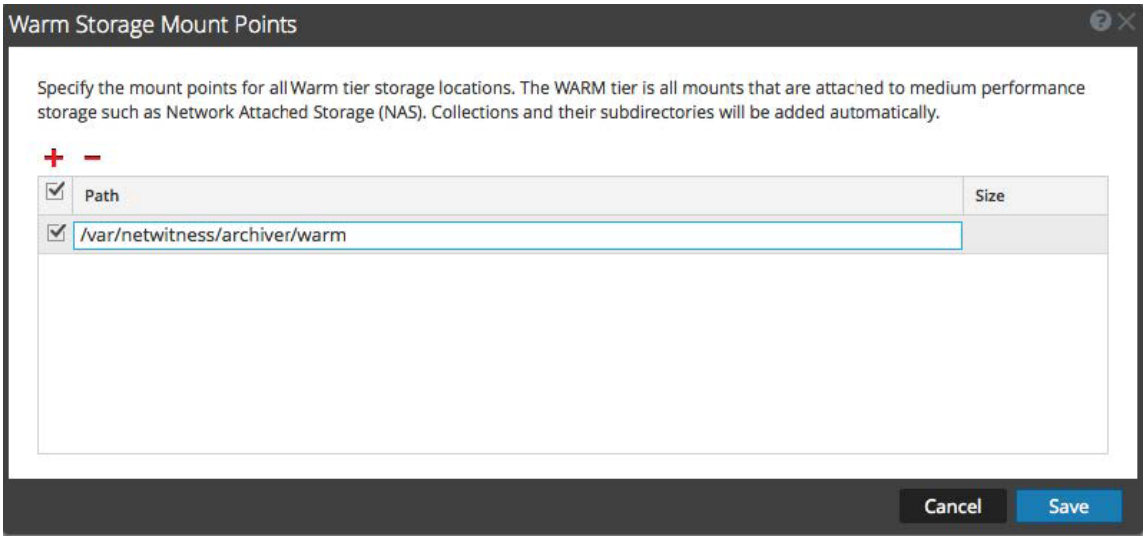
Por ejemplo, si el punto de montaje es /var/netwitness/archiver, se crearán los siguientes directorios para cada una de las recopilaciones:
/var/netwitness/archiver/<CollectionName>/metadb
/var/netwitness/archiver/<CollectionName>/packetdb
/var/netwitness/archiver/<CollectionName>/sessiondb
/var/netwitness/archiver/<CollectionName>/index

Tras el reinicio del servicio Archiver, los datos comenzarán a guardarse en las recopilaciones definidas. Asegúrese de que las recopilaciones de retención de registros estén correctas antes de reiniciar el servicio Archiver.

Precaución: Una vez que los datos se guardan en un punto de montaje, no se pueden eliminar de la interfaz del usuario.

Configurar el almacenamiento semiactivo total para un Archiver

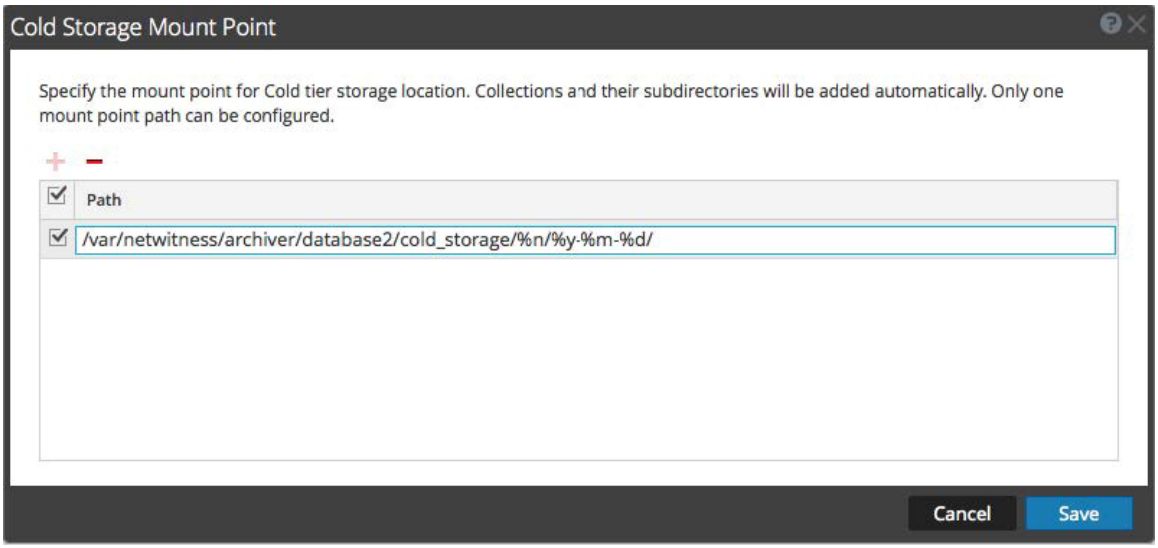
(Opcional) El procedimiento para configurar el almacenamiento semiactivo total para un Archiver es el mismo que para el almacenamiento activo total, con excepción de que debe hacer clic en en la sección Almacenamiento semiactivo total y agregar los puntos de montaje que desea usar para el almacenamiento semiactivo, los cuales son las rutas físicas al almacenamiento semiactivo, como el almacenamiento conectado en red (NAS).



Configurar el almacenamiento inactivo total para un Archiver

(Opcional) El procedimiento para configurar el almacenamiento inactivo total para un Archiver es el mismo que para el almacenamiento activo total, con excepción de que debe hacer clic en  en la sección Almacenamiento inactivo total y que solo debe agregar un punto de montaje para el almacenamiento inactivo. NetWitness Suite no administra el almacenamiento inactivo.

Debe incluir el especificador de formato de nombre de la recopilación `%n` en alguna parte del nombre de ruta del punto de montaje del almacenamiento inactivo para evitar conflictos de nombre de archivo entre recopilaciones.



Se permiten los siguientes especificadores de formato en la ruta:

Especificador de formato	Descripción
%n	nombre de la recopilación (obligatorio)
%y	año en que los datos se transfirieron al almacenamiento inactivo
%m	mes
%d	day
%h	hora

Especificador de formato	Descripción
%##r	bloque de horas para el día actual. Por ejemplo, si desea tres bloques de ocho horas, puede configurarlo en %8r. Las primeras 8 horas del día devuelven 0, las segundas 8 horas devuelven 1 y las últimas 8 horas del día devuelven 2.

Los cambios se hacen efectivos inmediatamente.

Por ejemplo, si tiene una recopilación llamada **compliance** y crea la siguiente ruta de almacenamiento inactivo:

```
/sa-cold-storage/%n/%y-%m-%d/
```

NetWitness Suite crea un directorio cada día con el siguiente formato:

/sa-cold-storage/compliance/2015-11-20/

Características de almacenamiento en niveles activo, semiactivo e inactivo

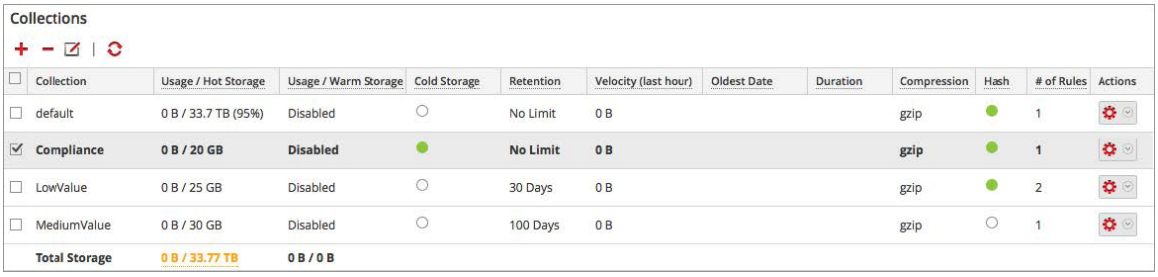
En la siguiente tabla se describen las características de los cuadros de diálogo del almacenamiento de los niveles activo, semiactivo e inactivo.

Función	Descripción
	Agrega un punto de montaje.
	Elimina un punto de montaje. No puede eliminar un punto de montaje que esté en uso, a menos que elimine las recopilaciones asociadas.
	Seleccione los puntos de montaje que desea incluir para el almacenamiento activo, semiactivo e inactivo total. Solo puede seleccionar un punto de montaje para el almacenamiento inactivo total.

Función	Descripción
Mount Point	Muestra la ruta al almacenamiento físico conectado. Por ejemplo: **/var/netwitness/archiver/database0**, que es la ubicación de la DAC del almacenamiento activo. No se deben agregar recopilaciones o subdirectorios a los puntos de montaje. NetWitness Suite creará automáticamente los directorios metadb, packetdb, sessiondb e index para cada recopilación definida en el Archiver: <storageLocation>/<CollectionName>/metadb <storageLocation>/<CollectionName>/packetdb <storageLocation>/<CollectionName>/sessiondb <storageLocation>/<CollectionName>/index Por ejemplo, si el punto de montaje del almacenamiento activo es /var/netwitness/archiver, se crearán los siguientes directorios para cada una de las recopilaciones: /var/netwitness/archiver/<CollectionName>/metadb /var/netwitness/archiver/<CollectionName>/packetdb /var/netwitness/archiver/<CollectionName>/sessiondb /var/netwitness/archiver/<CollectionName>/index Para el almacenamiento inactivo, debe incluir el especificador de formato de nombre de la recopilación `%n` en alguna parte del nombre de ruta del punto de montaje del almacenamiento inactivo para evitar conflictos de nombre de archivo entre recopilaciones.
Tamaño del almacenamiento	Muestra el tamaño del almacenamiento conectado. En la pestaña Retención de datos se muestra la cantidad total de almacenamiento para su referencia.

Recopilaciones

En la sección Recopilaciones se enumeran todas las recopilaciones de almacenamiento junto con el almacenamiento total para el almacenamiento activo y semiactivo.



Características de recopilaciones

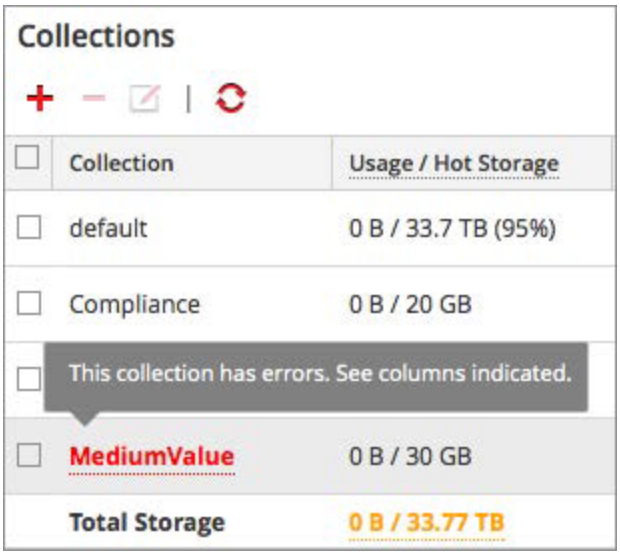
En la siguiente tabla se describen los íconos y las columnas de la sección Recopilaciones. Puede ocultar algunas de las columnas de acuerdo con sus requisitos.

Función	Descripción
	Abre el cuadro de diálogo Recopilaciones, en el cual puede agregar una recopilación de almacenamiento.
	Elimina la recopilación seleccionada. La eliminación de la recopilación quita de manera definitiva todos los datos almacenados de la recopilación, pero los directorios de datos vacíos permanecen.
	Abre el cuadro de diálogo Recopilaciones, en el cual puede editar la recopilación seleccionada.
	Actualiza la información de la recopilación
	Selecciona una recopilación. Por ejemplo, puede seleccionar una recopilación para editarla o eliminarla.
Collection	Muestra el nombre de la recopilación, como Default, Compliance, MediumValue y LowValue. Puede crear varias recopilaciones con distintos criterios para la retención de registros. Si no crea ninguna, se utiliza la recopilación Predeterminada. Si una recopilación tiene errores, el nombre de la recopilación y las columnas con errores aparecen en texto de color rojo.
Uso/almacenamiento activo	Muestra el uso del almacenamiento activo actual y el almacenamiento activo máximo para la recopilación. Cuando el tamaño de los registros alcanza la cantidad máxima del almacenamiento activo, los registros se quitan o se transfieren al siguiente nivel de almacenamiento disponible (semiactivo o inactivo).
Uso/almacenamiento semiactivo	Muestra el uso del almacenamiento semiactivo actual y el almacenamiento semiactivo máximo para la recopilación. Cuando el tamaño de los registros alcanza la cantidad máxima del almacenamiento semiactivo, los registros se quitan o se transfieren al almacenamiento inactivo disponible.

Función	Descripción
Almacenamiento inactivo	Indica si el almacenamiento inactivo está habilitado o deshabilitado. Un círculo verde indica que el almacenamiento inactivo está habilitado ( ). Un círculo blanco indica que el almacenamiento inactivo está deshabilitado.
Retención	Muestra la cantidad de días que se conservan los registros antes de que se quiten o se transfieran de manera opcional al almacenamiento inactivo. Sin límite indica que la retención de registros no se limita a una cantidad especificada de días. En el caso del almacenamiento activo y semiactivo, los ajustes del tamaño y el período de retención para una recopilación pueden reemplazarse mutuamente en función del criterio que se cumple primero (tamaño o tiempo).
Velocidad (última hora)	Muestra la cantidad de registros capturados durante la última hora.
Fecha más antigua	Muestra la fecha y la hora de la última captura de registros.
Duración	Muestra hace cuántos días se capturó el último registro. Por ejemplo: 20 días.
Compresión	Muestra el tipo de compresión utilizado para los metadatos y los datos crudos en la recopilación.
Hash	Muestra si hash está habilitado o deshabilitado. Cuando está habilitado, el algoritmo hash se usa para verificar la integridad de los datos de los archivos que se guardan. De forma predeterminada, los únicos datos a los cuales se aplica hash son los registros crudos y los archivos hash se guardan en el mismo directorio que los datos.

Función	Descripción
# of Rules	Muestra la cantidad de reglas aplicadas a la recopilación. Defina al menos una regla para cada recopilación. Una recopilación sin reglas asociadas muestra un cero en texto rojo como una advertencia: El nombre de la recopilación también aparece en texto de color rojo, lo cual indica un error en la recopilación. **Precaución:** Si una recopilación no tiene una regla, nunca ingresarán registros en ella.
Acciones	Permite ver las reglas asociadas con una recopilación en la sección Regla de retención cuando se selecciona <botón acciones> > **Seleccionar reglas**. En la sección Regla de retención, puede cambiar la prioridad general de las reglas de recopilación.
Almacenamiento total	Muestra el uso actual del almacenamiento activo total y el almacenamiento activo total máximo en la parte inferior de la columna **Uso/almacenamiento activo**. También muestra el uso actual del almacenamiento semiactivo total y el almacenamiento semiactivo total máximo en la parte inferior de la columna **Uso/almacenamiento semiactivo**.

Los errores en la recopilación aparecen en texto de color rojo. Un subrayado punteado indica que está disponible un mensaje de globo con información sobre el error.



Las recopilaciones con la edición deshabilitada (atenuada) también tienen mensajes de globo que proporcionan información sobre el problema.

Reglas de retención

En la sección Reglas de retención se indican todas las reglas de retención que se utilizan para las recopilaciones de almacenamiento enumeradas en el orden de ejecución de las reglas.

En la siguiente tabla se describen las funciones de la sección Regla de retención.

Función	Descripción
	Abre el cuadro de diálogo Definición de regla, en el cual puede agregar una regla de retención que se usará en una recopilación de almacenamiento.
	Elimina la regla de retención seleccionada. Para que las recopilaciones de registros recopilen y almacenen datos del registro, debe asociarlas al menos con una regla de retención.
	Abre el cuadro de diálogo Definición de regla, en el cual puede editar la regla de retención seleccionada.
	Actualiza la información de la regla de retención.
 Subir	Hace que la regla de retención seleccionada suba en la lista de prioridad de las reglas de retención. El orden de las reglas de retención es muy importante. NetWitness Suite evalúa las reglas de retención para todas las recopilaciones en orden numérico según el número que se indica en la columna Orden de la sección Regla de retención. También puede usar arrastrar y soltar para cambiar el orden de las reglas de retención.

Función	Descripción
Bajar	Hace que la regla de retención seleccionada baje en la lista de prioridad de las reglas de retención. El orden de las reglas de retención es muy importante. NetWitness Suite ejecuta las reglas de retención para todas las recopilaciones en orden numérico según el número que se indica en la columna Orden de la sección Regla de retención.
Aplicar	Guarda el cambio en el orden de las reglas.
Revertir	Revierte el cambio en el orden de las reglas.
	Selecciona o muestra una regla de retención seleccionada.
Orden	Muestra el orden de una regla en la lista general de reglas de retención.
Nombre de la regla	Muestra el nombre de la regla, como ComplianceDevices y GeneralWindowsLogs.
Condición	Muestra las condiciones para la regla. Estas condiciones especifican el tipo de registros que se incluirán en la recopilación. Definir reglas de retención presenta la regla que se aplica a todas las consultas y las condiciones de regla en los servicios principales.
Collection	Muestra el nombre de la recopilación y la cantidad de días que se conserva. Por ejemplo: MediumValue (30 días)

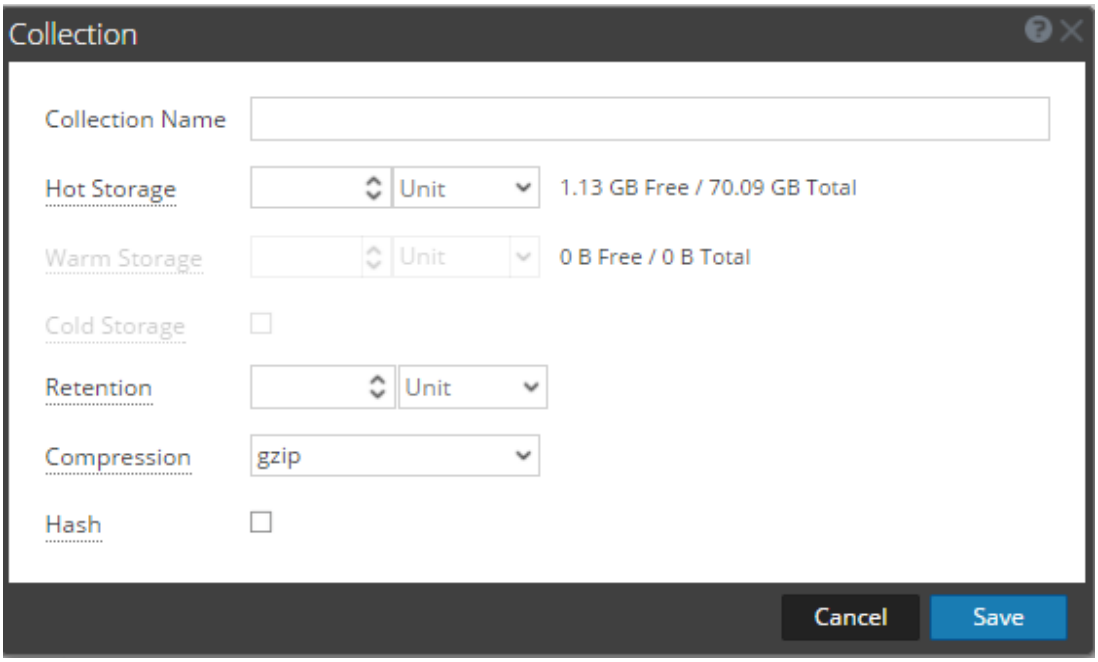
Cuadro de diálogo Recopilación

En ADMIN > Servicios > vista Configuración > pestaña Retención de datos de un Archiver, los administradores pueden definir los criterios para el almacenamiento y la retención de registros. En el cuadro de diálogo Recopilación, al cual se accede desde la sección Recopilaciones, puede definir las recopilaciones de almacenamiento individuales que se usarán para los distintos tipos de registros. Por ejemplo, tal vez desee crear recopilaciones por motivos de cumplimiento de normas o conservar registros importantes de manera selectiva.

Los procedimientos relacionados con este cuadro de diálogo se describen en Configurar el almacenamiento y la retención de registros de Archiver y Configurar recopilaciones de almacenamiento de registros.

Para acceder al cuadro de diálogo Recopilación:

1. Seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Archiver y elija >**Ver > Configuración**.
3. En la vista Configuración de servicios correspondiente al servicio, haga clic en la pestaña **Retención de datos**.
4. En la sección **Recopilaciones**, haga clic en + para agregar o editar la regla.
   Se muestra el cuadro de diálogo Recopilación.



En la siguiente tabla se describen los campos del cuadro de diálogo Recopilación.

Campo	Descripción
Nombre de recopilación	Especifique un nombre para la recopilación, como Compliance, MediumValue o LowValue.
Almacenamiento activo	Especifique el tamaño máximo o el porcentaje del almacenamiento activo que se usará para esta recopilación. El espacio libre disponible que se usará para el almacenamiento activo y el almacenamiento activo total se muestran junto a este campo. Cuando el tamaño de los registros alcanza el tamaño máximo del almacenamiento activo, los registros se quitan o se transfieren al siguiente nivel de almacenamiento disponible (semiactivo o inactivo).

Campo	Descripción
Almacenamiento semiactivo	(Opcional) Especifique el tamaño máximo o el porcentaje del almacenamiento semiactivo que se usará para esta recopilación. El espacio libre disponible que se usará para el almacenamiento semiactivo y el almacenamiento semiactivo total se muestran junto a este campo. Cuando los registros alcanzan el tamaño máximo del almacenamiento semiactivo, se quitan o se transfieren al almacenamiento inactivo disponible.
Almacenamiento inactivo	(Opcional) Especifique si desea usar almacenamiento inactivo para esta recopilación. Si utiliza almacenamiento inactivo para la recopilación, los registros que superan los límites de tamaño y retención especificados se transfieren al almacenamiento inactivo. Si no lo utiliza, los registros que superan estos límites se quitan.
Retención	(Opcional) Especifique la cantidad de días que se conservan los registros antes de que se quiten o se transfieran al almacenamiento inactivo. En el caso del almacenamiento activo y semiactivo, los ajustes del tamaño y el período de retención para una recopilación pueden reemplazarse mutuamente en función del criterio que se cumple primero (tamaño o tiempo).
Compresión	Especifique el tipo de compresión que se usará para los metadatos y los registros crudos en la recopilación. Puede comprimir los metadatos y los registros crudos mediante GZIP o LZMA para ahorrar espacio. GZIP es muy rápido para comprimir y descomprimir, pero no comprime tan bien como LZMA. LZMA ofrece una mejor compresión a expensas de la velocidad de descompresión (aproximadamente tres veces más lenta que la de GZIP). Las relaciones de compresión dependen en gran medida de los datos. La compresión predeterminada es GZIP.

Campo	Descripción
Hash	Especifique si desea habilitar o deshabilitar hash. Cuando está habilitado, el algoritmo hash se usa para verificar la integridad de los datos de los archivos que se guardan. De forma predeterminada, los únicos datos a los cuales se aplica hash son los registros crudos y los archivos hash se guardan en el mismo directorio que los datos.

Nota: Cuando se disminuyen las asignaciones de almacenamiento de recopilación o se reduce el tiempo de retención, pueden pasar varios minutos o varias horas antes de que se transfieran los datos y que el espacio esté disponible en función de la cantidad de datos que se transfieren. Los tiempos predeterminados son cada 20 minutos para una transferencia por tamaño y cada seis horas para una transferencia por tiempo.

Cuadro de diálogo Definición de regla

En ADMIN > Servicios > vista Configuración > pestaña Retención de datos de un Archiver, los administradores pueden definir los criterios para el almacenamiento y la retención de registros. En el cuadro de diálogo Definición de regla, al cual se accede desde la sección Reglas de retención, puede definir reglas de retención que se usarán para las recopilaciones de almacenamiento.

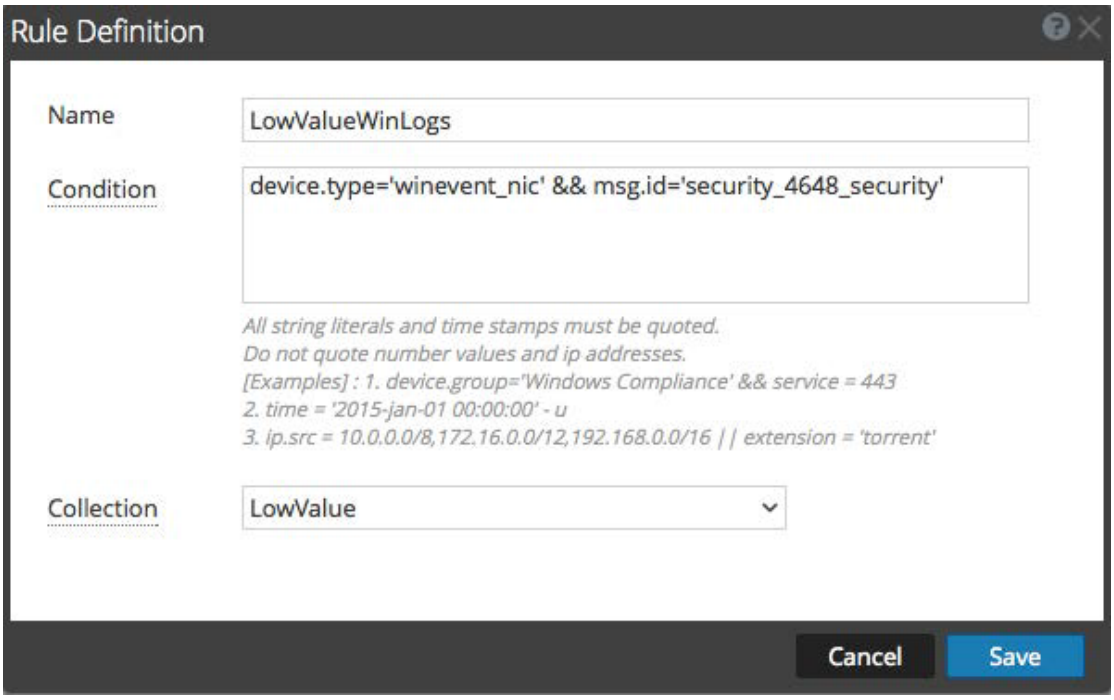
Los procedimientos relacionados con este cuadro de diálogo se describen en Configurar el almacenamiento y la retención de registros de Archiver y Definir reglas de retención.

Para acceder al cuadro de diálogo Definición de regla:

1. Seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Archiver y elija  **>Ver > Configuración**.
3. En la vista Configuración de servicios correspondiente al servicio, haga clic en la pestaña **Retención de datos**.

4. En la sección **Regla de retención**, haga clic en + o en .

   Se muestra el cuadro de diálogo Definición de regla.



En la siguiente tabla se describen los campos del cuadro de diálogo Definición de regla.

Campo	Descripción
Nombre	Especifique un nombre único para la regla de retención. Por ejemplo: ComplianceDevices
Condición	Especifique las condiciones para el tipo de registros que desea incluir en la recopilación. Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. Por ejemplo: `device.group='PCI Devices' || device.group='HIPPA Devices'`
Collection	Seleccione la recopilación en la cual desea aplicar esta regla. Por ejemplo: Cumplimiento de normas

Paso siguiente

Configurar recopilaciones de almacenamiento de registros.

Configurar recopilaciones de almacenamiento de registros

En este tema se proporcionan instrucciones a los administradores para configurar recopilaciones de almacenamiento de registros en un Archiver.

NetWitness Suite permite definir recopilaciones de almacenamiento individuales para distintos tipos de registros. Puede especificar el tamaño máximo del espacio de almacenamiento activo y semiactivo que usa la recopilación, si desea usar almacenamiento offline (almacenamiento inactivo), la cantidad de días que se conservarán los registros en la recopilación, la compresión de datos y si desea usar un algoritmo hash para poder verificar la integridad de los datos de los archivos que se guardan. Debe crear recopilaciones según sus requisitos de almacenamiento de retención de registros. Cada recopilación que crea debe asociarse con al menos una regla de retención.

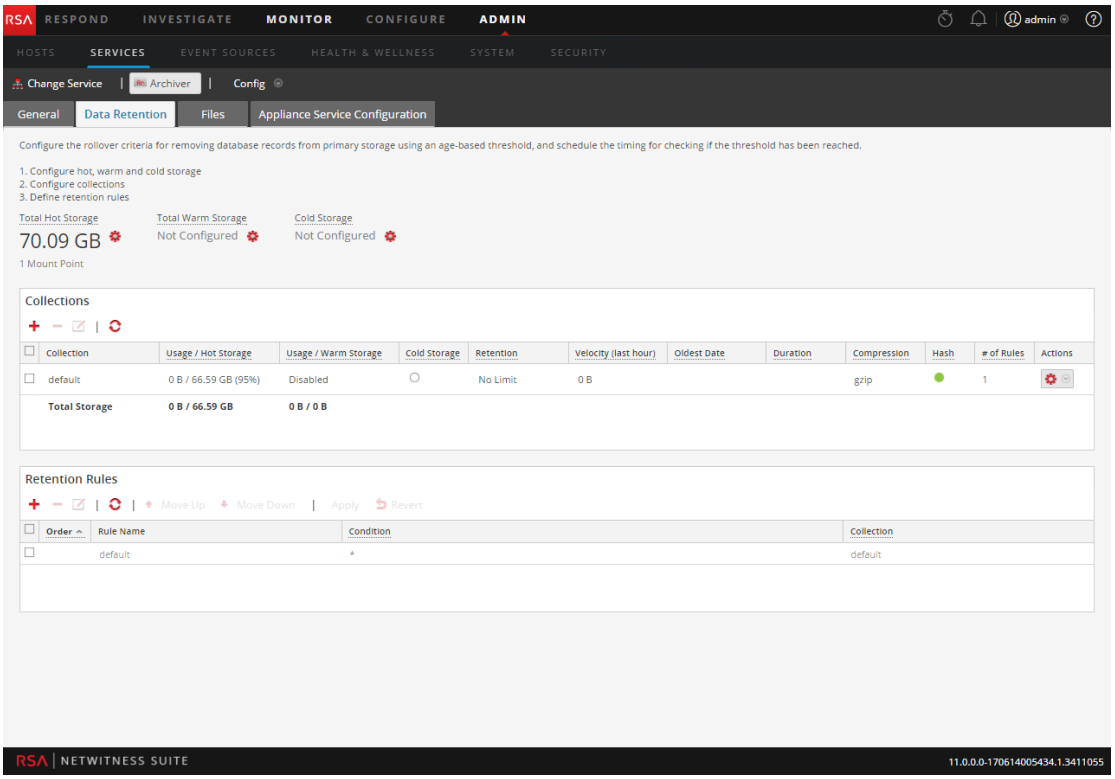
Requisitos previos

Antes de configurar recopilaciones de almacenamiento de retención de registros, configure el almacenamiento activo, semiactivo e inactivo total.

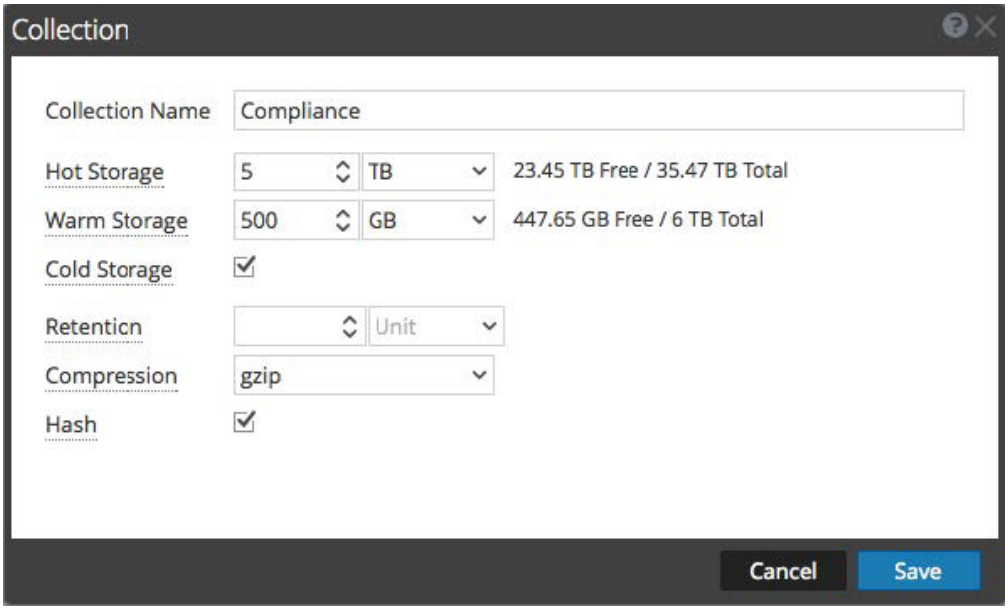
Configurar una recopilación de almacenamiento de registros

Para configurar una recopilación de almacenamiento de retención de registros en un Archiver:

1. Vaya a **ADMIN > Servicios**.
2. Seleccione el servicio Archiver y elija  **> Ver > Configuración**.
   Se muestra la vista Configuración de servicios de Archiver.
3. En la sección **Recopilaciones** de la pestaña **Retención de datos**, haga clic en  para agregar una recopilación.
   (Si decide hacer cambios en una recopilación existente, puede seleccionar la recopilación y hacer clic en  para cambiar la configuración).



Se muestra el cuadro de diálogo **Recopilación**.



4. Configure la recopilación como se describe en la siguiente tabla.

Campo	Descripción
Nombre de recopilación	Especifique un nombre único para su recopilación, como Compliance, MediumValue o LowValue.
Almacenamiento activo	Especifique el tamaño máximo o el porcentaje del almacenamiento activo que se usará para esta recopilación. El espacio libre disponible que se usará para el almacenamiento activo y el almacenamiento activo total se muestran junto a este campo.
Almacenamiento semiactivo	(Opcional) Especifique el tamaño máximo o el porcentaje del almacenamiento semiactivo que se usará para esta recopilación. El espacio libre disponible que se usará para el almacenamiento semiactivo y el almacenamiento semiactivo total se muestran junto a este campo.
Almacenamiento inactivo	(Opcional) Especifique si desea usar almacenamiento inactivo para esta recopilación. Si utiliza almacenamiento inactivo para la recopilación, los registros que superan los límites del almacenamiento se copian en el almacenamiento inactivo antes de que se eliminen del almacenamiento activo o semiactivo.
Retención	(Opcional) Especifique la cantidad de días que se conservan los registros antes de que se quiten o se transfieran al almacenamiento inactivo. En el caso del almacenamiento activo y semiactivo, los ajustes del tamaño y el período de retención para una recopilación pueden reemplazarse mutuamente en función del criterio que se cumple primero (tamaño o tiempo).

Campo	Descripción
Compresión	Especifique el tipo de compresión que se usará para los metadatos y los registros crudos en la recopilación. Puede comprimir los metadatos y los registros crudos mediante GZIP o LZMA para ahorrar espacio. GZIP es muy rápido para comprimir y descomprimir, pero no comprime tan bien como LZMA. LZMA ofrece una mejor compresión a expensas de la velocidad de descompresión (aproximadamente tres veces más lenta que la de GZIP). Las relaciones de compresión dependen en gran medida de los datos. La compresión predeterminada es GZIP.
Hash	Especifique si desea habilitar o deshabilitar hash. Cuando está habilitado, el algoritmo hash se usa para verificar la integridad de los datos de los archivos que se guardan. De forma predeterminada, los únicos datos a los cuales se aplica hash son los registros crudos y los archivos hash se guardan en el mismo directorio que los datos.

5. Haga clic en **Guardar**.
   Los errores en la recopilación aparecen en texto de color rojo. Un subrayado punteado indica que está disponible un mensaje de globo con información sobre el error. El nombre de la recopilación aparece en texto de color rojo hasta que se define al menos una regla de retención para la recopilación.
   Si hay una recopilación con la edición deshabilitada (atenuada), observe el mensaje de globo asociado para obtener más información.

Nota: Cuando se disminuyen las asignaciones de almacenamiento de recopilación o se reduce el tiempo de retención, pueden pasar varios minutos o varias horas antes de que se transfieran los datos y que el espacio esté disponible en función de la cantidad de datos que se transfieren. Los tiempos predeterminados son cada 20 minutos para una transferencia por tamaño y cada seis horas para una transferencia por tiempo.

Paso siguiente

Definir reglas de retención para las recopilaciones.

Definir reglas de retención

Los administradores pueden definir y ordenar las reglas de retención para las recopilaciones de almacenamiento de registros en un Archiver. Las reglas de retención especifican el tipo de registros que se almacenarán en la recopilación. Para que las recopilaciones de registros recopilen y almacenen datos del registro, debe asociarlas al menos con una regla de retención. Cuando configura una regla de retención, debe especificar una condición y una recopilación para esa regla. La condición (definición de regla) determina el tipo de registros almacenados en esa recopilación.

Para la condición, puede usar cualquier elemento que funcione en una cláusula `where` de una consulta normal.

Por ejemplo, para obtener registros de servicios de cumplimiento de normas, puede usar la siguiente condición:

```
device.group='PCI Devices' || device.group='HIPPA Devices'
```

Después de definir las reglas de retención para las recopilaciones, es importante que especifique el orden de las reglas de retención. NetWitness Suite evalúa las reglas de retención para todas las recopilaciones en orden numérico según el número que se indica en la columna Orden de la sección Regla de retención de la pestaña Retención de datos del Archiver (ADMIN > vista Configuración de servicios).

Precaución: El orden de las reglas es muy importante. Determina la prioridad de evaluación de los datos del registro para la retención del almacenamiento.

Requisitos previos

Antes de configurar las reglas de retención:

- Configure el almacenamiento activo, semiactivo e inactivo total
- Configure recopilaciones de almacenamiento de registros

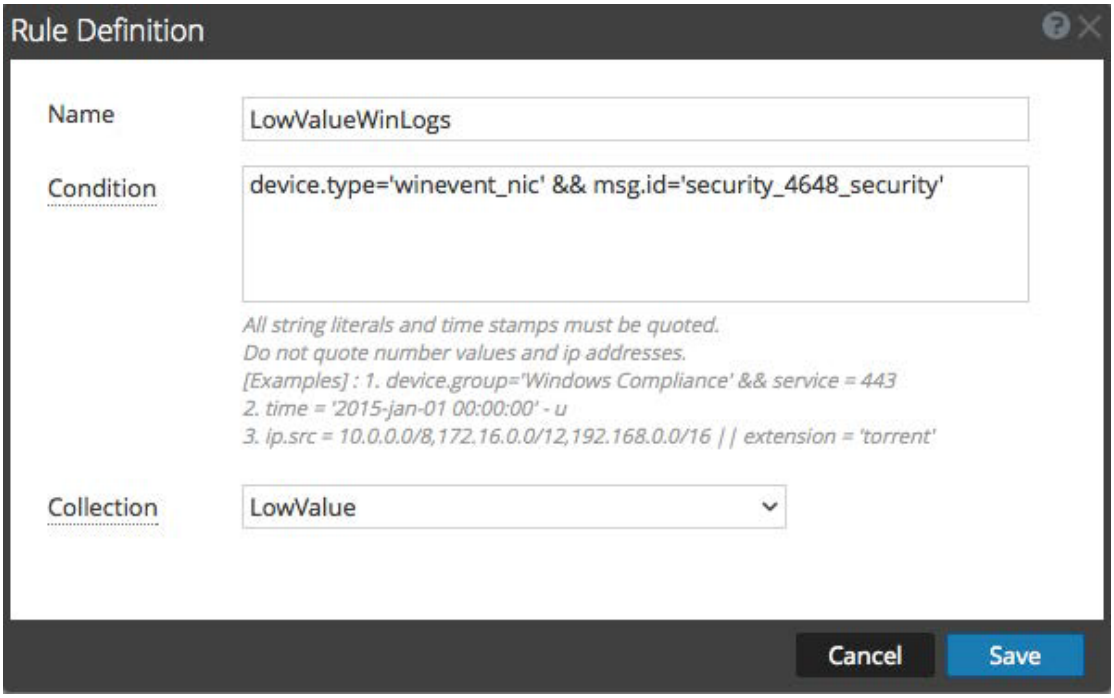
Procedimientos

Definir una regla de retención para una recopilación

1. Vaya a **ADMIN > Servicios**.
2. Seleccione el servicio Archiver y elija  **> Ver > Configuración**.

   Se muestra la vista Configuración de servicios de Archiver.

3. En la sección **Regla de retención** de la pestaña **Retención de datos**, haga clic en +.
   Se muestra el cuadro de diálogo **Definición de regla**.

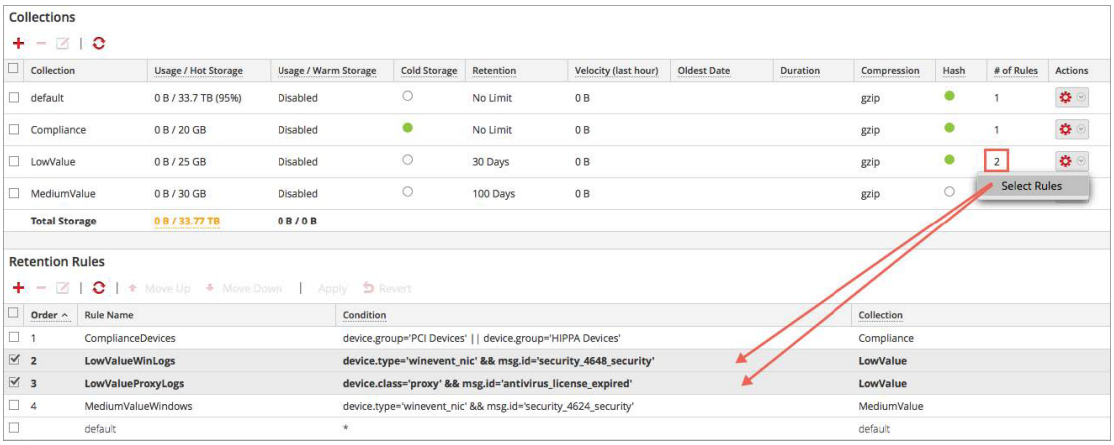


4. Configure los campos del cuadro de diálogo Definición de regla como se describe en la siguiente tabla:

Campo	Descripción
Nombre de la regla	Especifique un nombre único para la regla de retención. No puede incluir espacios. Por ejemplo: LowValueWinLogs
Condición	Especifique las condiciones para el tipo de registros que desea incluir en la recopilación. Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. Por ejemplo: `device.type='winevent_nic' && msg.id='security_4648_security'`

Campo	Descripción
Collection	Seleccione la recopilación en la cual desea aplicar esta regla. Por ejemplo: LowValue.

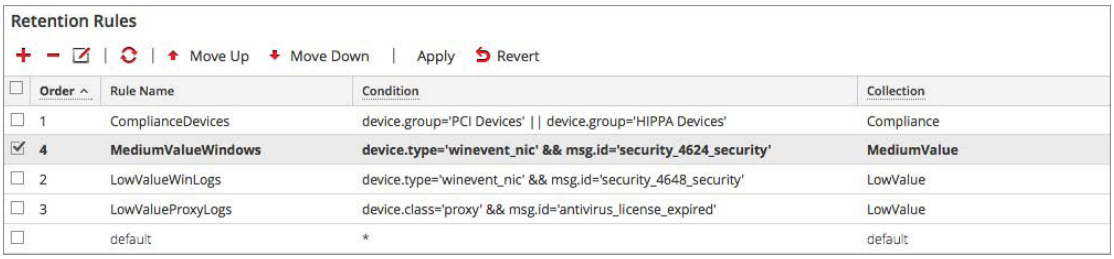
5. Haga clic en **Guardar**.
   La regla de retención que define se asocia con la recopilación que seleccionó. En la sección **Recopilaciones** de la pestaña **Retención de datos**, puede hacer clic en  > **Seleccionar reglas** en la columna **Acciones** para la recopilación seleccionada con el fin de ver las reglas de retención asociadas con la recopilación en la sección **Regla de retención**.



Especificar el orden de las reglas de retención

Para dar prioridad a la lista completa de todas las reglas de retención:

1. En la sección **Regla de retención** de la pestaña **Retención de datos**, seleccione una regla de retención y use arrastrar y soltar (o seleccione **Subir** y **Bajar**) para cambiar su orden en la lista de prioridad.



2. Haga clic en **Aplicar** para guardar el orden de las reglas de retención.

Precaución: El orden de las reglas es muy importante. Determina la prioridad de evaluación de los datos del registro para la retención del almacenamiento.

Paso siguiente

Agregar Archiver como un origen de datos en Reporting Engine.

Agregar Archiver como un origen de datos en Reporting Engine

En este tema se proporcionan instrucciones sobre cómo agregar Archiver como un origen de datos en Reporting Engine para generar informes acerca de los datos que recopila Archiver.

Requisitos previos

Asegúrese de haber:

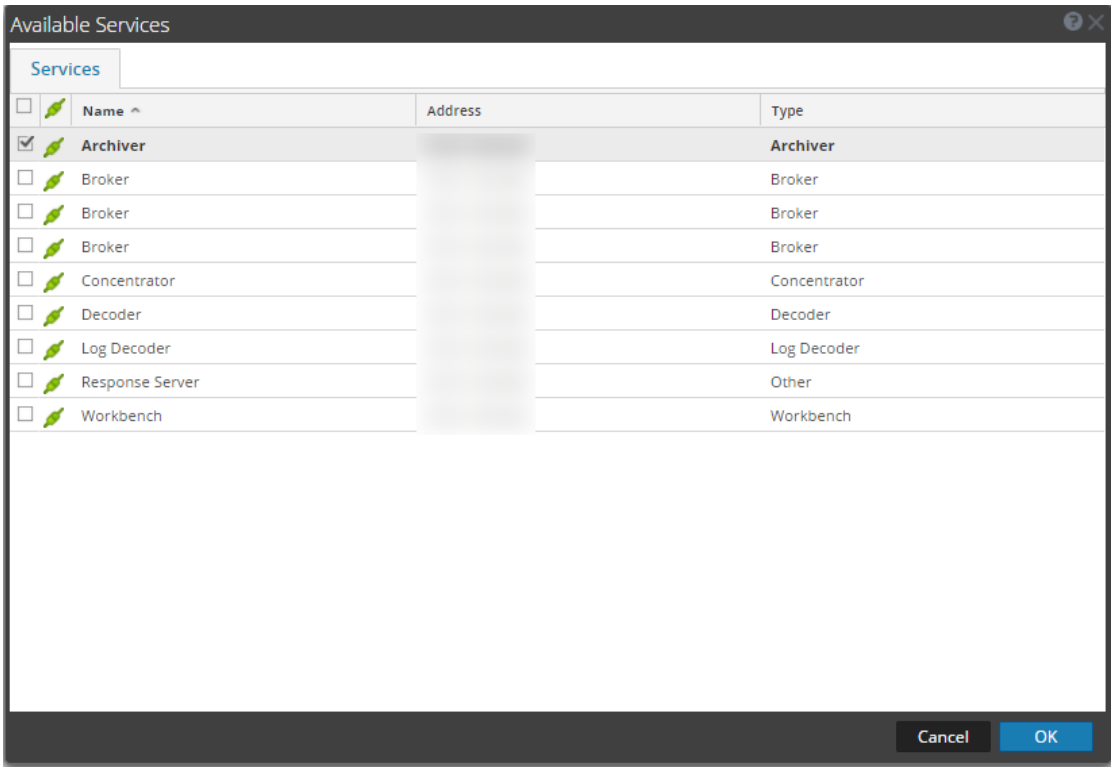
1. Instalado el host de Archiver en el ambiente de red.
2. Instalado y configurado Log Decoder Decoder en el ambiente de red.
3. Verificado que los servicios Reporting Engine y Archiver estén activos.

Procedimiento

Para asociar el origen de datos de Archiver con Reporting Engine:

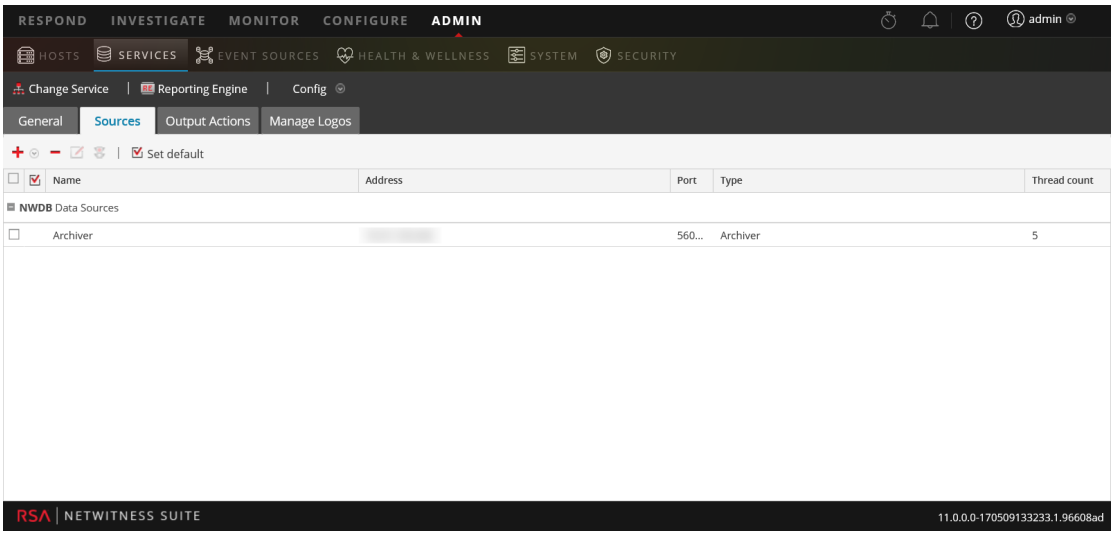
1. Vaya a **ADMIN > Servicios**.
2. En el panel **Servicios**, seleccione un servicio **Reporting Engine**.
3. En la columna **Acciones**, seleccione **Ver > Configuración**.
4. Seleccione la pestaña **Orígenes**.
5. Haga clic en + y seleccione **Servicios disponibles**.

   Se muestra el cuadro de diálogo Servicios disponibles.



6. Seleccione el Archiver que desea agregar como origen de datos al Reporting Engine y haga clic en **Aceptar**.
7. En el cuadro de diálogo Información de servicio, escriba el nombre de usuario y la contraseña para el Archiver.
8. Haga clic en **Aceptar**.

   El Archiver seleccionado se muestra en la categoría Orígenes de datos de NWDB.



Ahora puede crear informes sobre los datos que recopila Archiver.

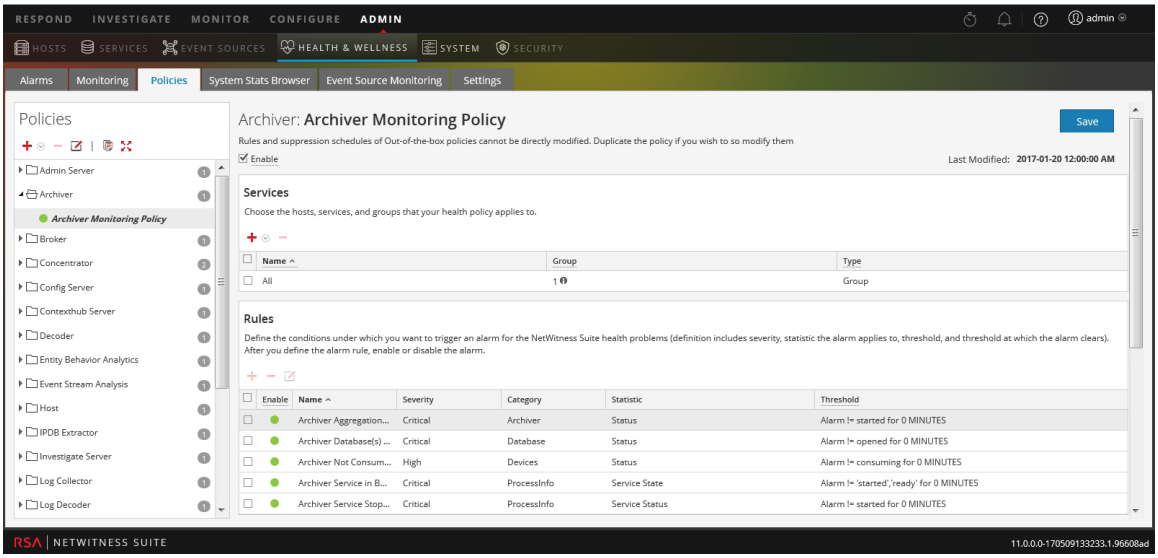
Paso siguiente

Configurar alertas para el almacenamiento para archivo.

Configurar el monitoreo de Archiver

Estado y condición permite la generación automática de notificaciones cuando se alcanzan los umbrales críticos.

Revise las políticas de Estado y condición para Archiver y el host en la sección Políticas de Estado y condición. Realice actualizaciones según sea necesario.



Para obtener información detallada, consulte **Administrar políticas** en la guía de *Mantenimiento del sistema*.

Configuración adicional de Archiver

Este tema es un conjunto de procedimientos individuales que un administrador puede ejecutar en cualquier momento, los cuales no son necesarios para llevar a cabo la configuración inicial de Archiver. Estos procedimientos se presentan en orden alfabético.

Use esta sección cuando busque instrucciones para realizar una tarea específica después de la configuración inicial de Archiver.

Temas

Configuración del respaldo y la restauración de datos

En este tema se proporciona información sobre la función de respaldo y restauración de datos para un Archiver. puede usar esta función para respaldar los datos de Archiver y recuperar los datos respaldados.

Puede respaldar los datos de las siguientes formas:

- Use scripts para copiar archivos desde las carpetas de respaldo de almacenamiento inactivo a un almacenamiento offline.
- Use software de respaldo para copiar archivos desde las carpetas de respaldo de almacenamiento inactivo a un almacenamiento offline.
- Ejecute EMC Networker u otro software de respaldo en Archiver y configúrelo para que realice un respaldo incremental diario de los archivos de la base de datos.

Nota: Para obtener detalles sobre el procedimiento de respaldo de datos mediante Networker, consulte la *Guía de administración de Networker*.

Una vez que haya respaldado los datos, debe ejecutar las siguientes tareas para restaurar los datos respaldados que están instalados en Archiver.

Acción	Descripción
1. Restaurar los datos en una ubicación a la que puede acceder Archiver.	Consulte Crear recopilación
2. Crear una recopilación en Archiver que usa esa ubicación.	Consulte el tema **Administrar recopilaciones** de la *Guía de configuración de Workbench*.
3. Agregue el servicio Archiver como origen de datos en Reporting Engine para generar informes de los datos restaurados en el servicio Archiver.	Consulte Agregar Archiver como un origen de datos en Reporting Engine

Agregar el servicio Archiver

El servicio NetWitness Suite Archiver permite crear recopilaciones con datos restaurados desde el almacenamiento offline (inactivo) de Archiver. Este procedimiento solo es necesario si el servicio Archiver no está instalado.

Requisitos previos

Asegúrese de haber agregado un host de Archiver y de haberle aplicado una licencia.

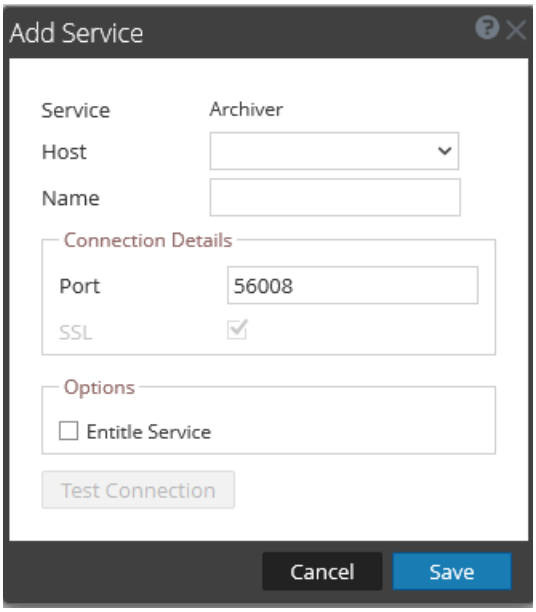
Procedimiento

Nota: Este procedimiento solo es necesario si el servicio Archiver no está instalado.

Realice los siguientes pasos para agregar el servicio Archiver:

1. Vaya a **ADMIN > Servicios**.
2. En el panel **Servicios**, seleccione + **>Archiver**.

   Aparece el cuadro de diálogo Agregar servicio, como se muestra a continuación.



3. Ingrese los siguientes detalles.

Campo	Descripción
Host	Seleccione un host de Archiver en el menú desplegable.
Nombre	Escriba un nombre para el servicio.
Puerto	El puerto predeterminado es 50007.
SSL	Seleccione **SSL** si desea que NetWitness Suite se comunique con el servicio mediante SSL. La seguridad de la transmisión de datos se administra mediante el cifrado de la información y el suministro de autenticación con certificados SSL. **Nota:** si selecciona SSL, asegúrese de que este protocolo esté activado en el panel Configuración del sistema.
Nombre de usuario	(Opcional) Escriba el nombre de usuario para el servicio.
Contraseña	(Opcional) Escriba la contraseña para el servicio.

4. Haga clic en **Probar conexión** para determinar si NetWitness Suite se conecta al servicio.
5. Cuando el resultado sea satisfactorio, haga clic en **Guardar**.
   El servicio agregado ahora se muestra en el panel Servicios.

Nota: si el resultado de la prueba no es satisfactorio, edite la información del servicio y vuelva a intentarlo.

Crear recopilación

En este tema se proporciona información sobre cómo crear una recopilación en un servicio Archiver.

Puede crear una recopilación con el uso de datos restaurados de los datos respaldados o de un subconjunto de datos existente. Cuando recupera los datos respaldados, debe colocarlos en la carpeta de la recopilación creada en el servicio Archiver para poder generar los informes requeridos para los datos recuperados. Por ejemplo, si respaldó los datos mediante EMC Networker en <*location*>, puede usar las opciones de restauración de Networker para restaurar los datos respaldados en la carpeta de la recopilación que se creó en el servicio Archiver. Para conocer el procedimiento de restauración mediante EMC Networker, consulte la *Guía de administración de Networker*.

Requisitos previos

Asegúrese de:

- Haber instalado el servicio Archiver en un host de Archiver.
- Que el servicio Archiver tenga espacio suficiente para dar cabida a la recopilación.
- Que los datos respaldados estén en una ubicación conocida en el host local, si va a crear una recopilación mediante el uso de los datos restaurados a partir de los datos respaldados.

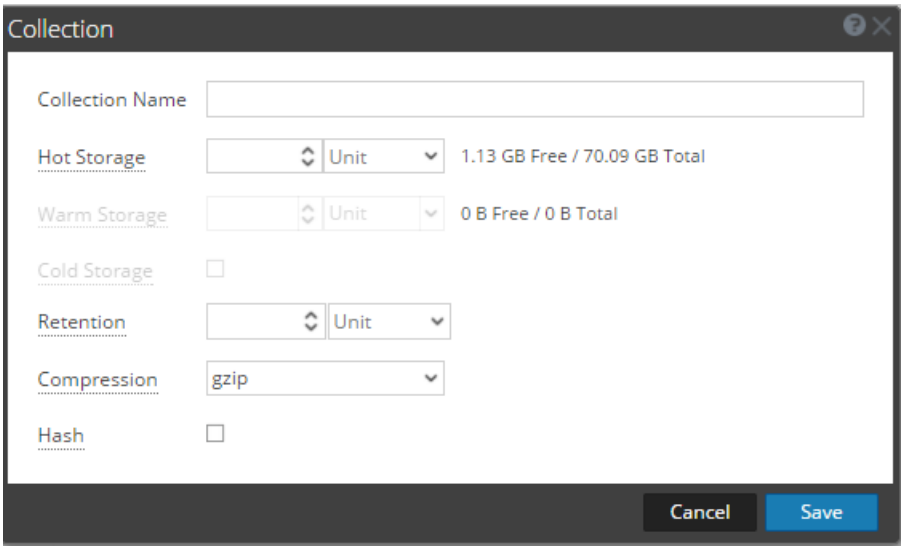
Procedimiento

La pestaña Retenciones de datos permite a los administradores restaurar y guardar datos que se restauraron a partir de un respaldo o de un conjunto de datos existente.

Nota: El administrador puede señalar la ruta de origen a la ubicación de los archivos de la base de datos y el comando restore los copia a Archiver. El administrador debe montar esos directorios en Archiver antes de que se pueda crear una recopilación de restauración.

Para crear una recopilación con el uso de datos restaurados de los datos respaldados o de un subconjunto de datos existente:

1. Vaya a **ADMIN > Servicios > Archiver**.
2. En la cuadrícula **Servicios**, seleccione  **>Ver > Configuración**.
   Se muestra la pestaña **General**.
3. Seleccione la pestaña **Retenciones de datos** y haga clic en  en el panel **Recopilaciones** para agregar una recopilación.
   Se muestra el cuadro de diálogo **Recopilación**.



4. Proporcione la siguiente información:

- **Nombre de recopilación:** Nombre de la recopilación de Archiver que desea restaurar.
- **Almacenamiento activo:** Ingrese la cantidad de archivos de base de datos de Archiver y el tamaño de unidad (gigabytes o terabytes) que se hayan transferido desde el almacenamiento inactivo.
- **Retención:** Seleccione la cantidad de días u horas que desea almacenar la recopilación.
- **Compresión:** Seleccione el tipo de compresión para la recopilación.

6. Haga clic en **Guardar** para restaurar la recopilación.

Nota: Destino es la ubicación en la cual se crea la recopilación.

Nota: Si la ruta de origen proporcionada para crear la recopilación de restauración no existe, se muestra el siguiente mensaje de error:
"La ruta de origen no existe "/xxx/xxx/"."
Si hay almacenamiento insuficiente para restaurar la recopilación, se muestra el siguiente error:
"Error durante la comprobación del espacio en disco. Espacio en disco insuficiente en la ubicación "/xxx/xxx"."

El cuadro de diálogo Programar trabajo se muestra con el siguiente mensaje:
"Restaurando datos en una nueva recopilación. Compruebe el progreso en la página de trabajos".

7. Haga clic en el ícono **Trabajos**  del área superior derecha del menú principal para expandir la lista de trabajos de recopilación de restauración con su estado actual.

Nota: Cuando se restaura una recopilación, mientras más grande sea el conjunto de datos que se debe restaurar, más tardará la restauración. Si va a restaurar una recopilación que contiene cientos de gigabytes o más, la restauración puede tardar varias horas.

Agregar el servicio Archiver como un origen de datos en Reporting Engine

En este tema se proporcionan instrucciones para agregar el servicio Archiver como un origen de datos en Reporting Engine con el fin de generar informes de los datos restaurados en el Archiver.

Requisitos previos

Asegúrese de:

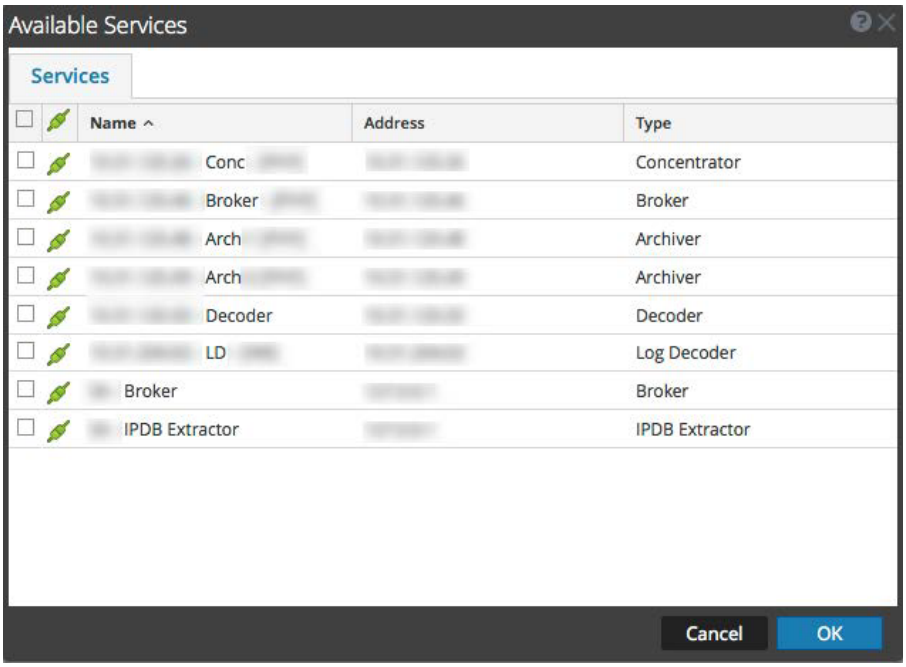
- Haber instalado el servicio Archiver en el host de Archiver.

- Haber agregado una recopilación en el servicio Archiver.

Procedimiento

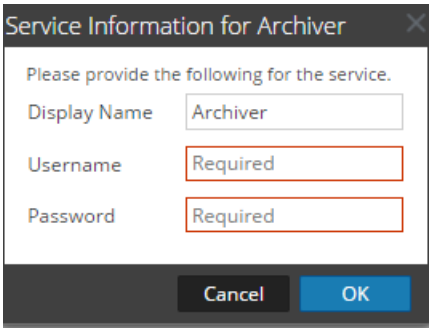
Realice los siguientes pasos para agregar el servicio Archiver como un origen de datos en Reporting Engine:

1. Seleccione **ADMIN > Servicios**.
2. En el panel **Servicios**, seleccione un servicio Reporting Engine.
3. En la columna **Acciones**, seleccione **Ver > Configuración**.
4. Seleccione la pestaña **Orígenes**.
5. Haga clic en + y seleccione **Servicios disponibles**.
   Se muestra el cuadro de diálogo Servicios disponibles.

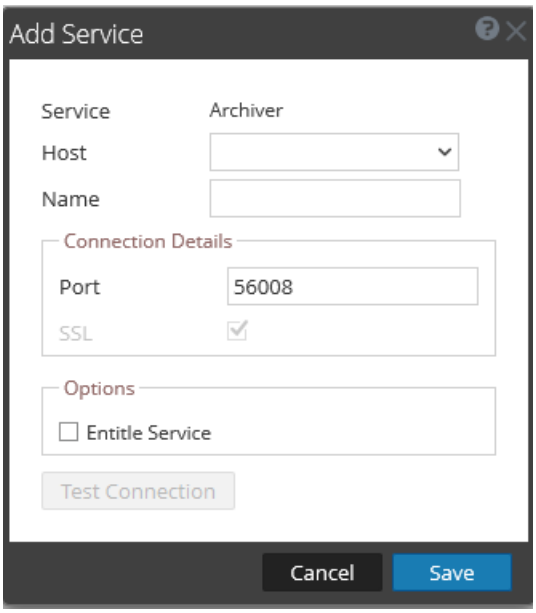


6. Seleccione el servicio Archiver y haga clic en **Aceptar**.
   Si el servicio Archiver usa un modelo de confianza, el cuadro de diálogo Información de servicio para el servicio seleccionado se muestra con los campos obligatorios de nombre de usuario y contraseña. Si el servicio no usa un modelo de confianza, estos campos serán

opcionales.



7. Escriba el nombre de usuario y la contraseña de las credenciales de administrador correspondientes al servicio.
8. Haga clic en **Aceptar**.
   Se muestra el cuadro de diálogo Agregar servicio.



9. Seleccione un host en la lista desplegable y haga clic en **Guardar**.
   El servicio Archiver se agrega como un origen de datos en Reporting Engine y se incluye en la lista Orígenes de datos de NWDB.

Nota: Este procedimiento se debe realizar para cada recopilación.

Un administrador puede crear y eliminar recopilaciones de Workbench y ver estadísticas y registros de Workbench. En este tema se proporcionan todos estos procedimientos y un procedimiento de ejemplo para restaurar una recopilación con fines de creación de informes e investigación.

- Montar directorios de Archiver
- Crear una recopilación
- Eliminar una recopilación
- Investigar una recopilación
- Ver estadísticas de recopilación de Workbench
- Ver registros de Workbench

Montar directorios de Archiver

Si los datos están en el almacenamiento offline o de nivel inactivo, debe montar los directorios de Archiver a fin de restaurar los datos con fines de creación de informes e investigación:

1. Vaya a **ADMIN > Servicios**.
2. Seleccione un **Archiver** en la cuadrícula Servicios y elija  **> Ver > Explorar**.
   Se muestra la vista Explorador para el Archiver.
3. Haga clic con el botón secundario en el nodo **Base de datos** del árbol de la izquierda y seleccione las propiedades de **Base de datos** para abrirlas en el panel de la derecha.
4. Ejecute el comando **manifest** para un rango de tiempo, por ejemplo, del 1.º de abril de 2015 al 10 de abril de 2015.
   La búsqueda devuelve todos los archivos que se deben restaurar para la consulta que seleccionó.

Crear una recopilación

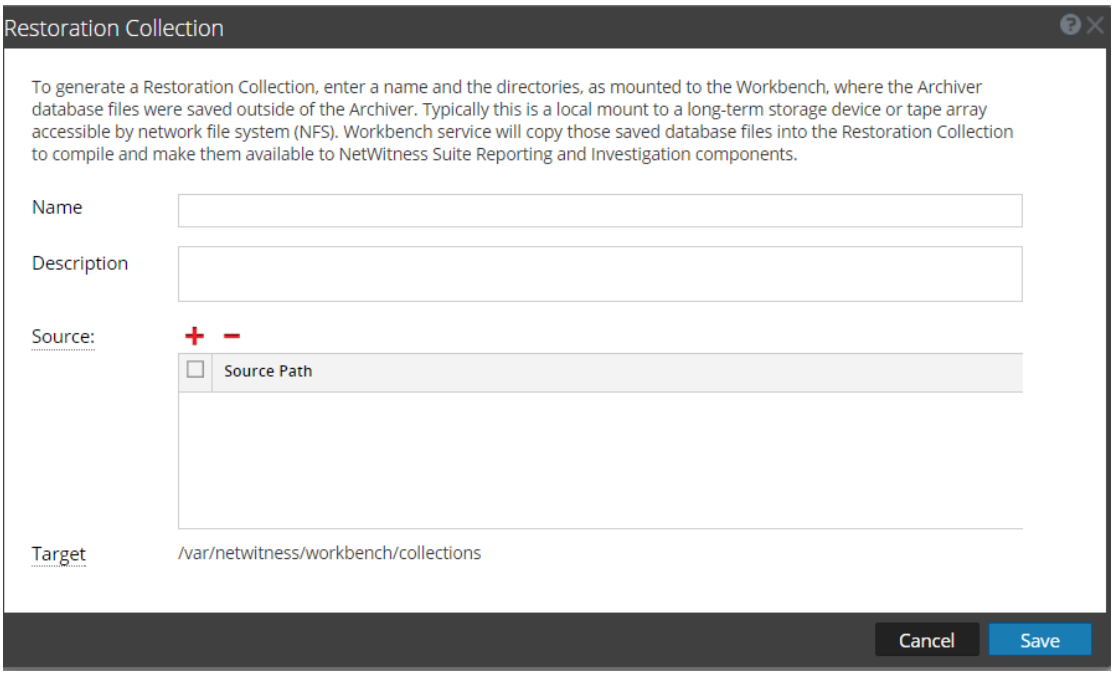
Los administradores pueden crear recopilaciones de los datos restaurados desde un respaldo o de un conjunto de datos existente.

Nota: Puede señalar la ruta de origen a la ubicación de los archivos de la base de datos y el comando restore los copia en Archiver. Debe montar esos directorios en Archiver (donde está instalado Workbench) antes de que pueda crear una recopilación de restauración.

Para crear una recopilación con el uso de datos restaurados de los datos respaldados o de un subconjunto de datos existente:

1. Vaya a **ADMIN > Servicios.**
2. En la vista Servicios, seleccione un **Workbench**, y, a continuación, elija  **> Ver > Configuración**.
   La vista Configuración de servicios se muestra con la pestaña General abierta.

3. Haga clic en la pestaña **Recopilaciones**.
   Se muestra la cuadrícula Recopilaciones.
4. Haga clic en + en la barra de herramientas.
   Se muestra el cuadro de diálogo Recopilación de restauración.



5. Proporcione la siguiente información:
   - **Nombre:** Nombre de la recopilación de Workbench que desea restaurar.
   - **Fuente:** ubicación donde se transfirieron los archivos de la base de datos de Archiver desde el almacenamiento inactivo.

   Nota: Destino es la ubicación en la cual se crea la recopilación.
6. Haga clic en **Guardar** para restaurar la recopilación.

   Nota: Si la ruta de origen proporcionada para crear la recopilación de restauración no existe, se muestra el siguiente mensaje de error:

```
The source path does not exist '/xxx/xxx/'.
```

Si hay almacenamiento insuficiente para restaurar la recopilación, se muestra el siguiente error:

```
Error during disk space checking. Insufficient disk space in
location '/xxx/xxx'.
```

El cuadro de diálogo Programar trabajo se muestra con el siguiente mensaje:

```
Restoring data into a new collection. Check the jobs page for
progress.
```

7. Haga clic en el ícono **Trabajos**  de la barra de herramientas de NetWitness Suite para expandir la lista de trabajos de recopilación de restauración con su estado actual.

Nota: la restauración de una recopilación de más de 550 GB puede tardar varias horas.

Eliminar una recopilación

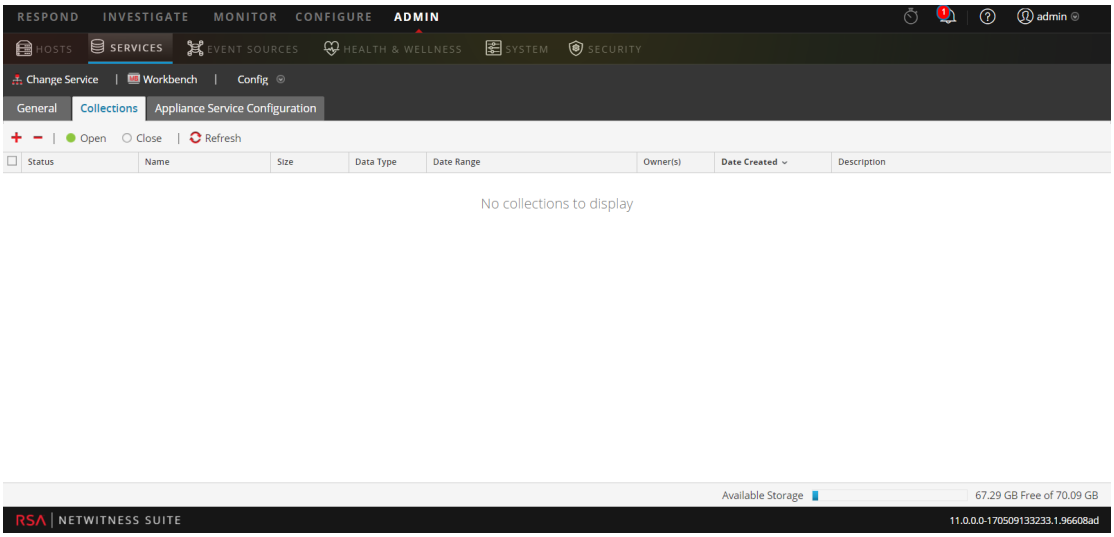
Los administradores pueden eliminar las recopilaciones del servicio Workbench.

Realice los siguientes pasos para eliminar una recopilación:

1. Vaya a **ADMIN > Servicios.**
2. En la vista Servicios, seleccione un **Workbench** y haga clic en  **> Ver > Configuración**.

   La vista Configuración de servicios se abre con la pestaña General abierta.
3. Seleccione la pestaña **Recopilaciones**.

   Se muestra la cuadrícula Recopilaciones.



4. En la cuadrícula Recopilaciones, seleccione la recopilación que desea eliminar.
5. Haga clic en en la barra de herramientas.

   Un cuadro de diálogo de advertencia solicita confirmación.
6. Si desea eliminar la recopilación, haga clic en **Sí**.

   La recopilación se quita del servicio Workbench.

Procedimiento de ejemplo: Cómo restaurar una recopilación con fines de creación de informes e investigación

En los siguientes pasos se ilustra cómo restaurar datos que están en el almacenamiento offline o de nivel inactivo con fines de creación de informes e investigación. En el siguiente ejemplo se restauran datos para el rango de tiempo del 1.º de abril de 2015 al 10 de abril de 2015.

Para restaurar datos con fines de creación de informes e investigación:

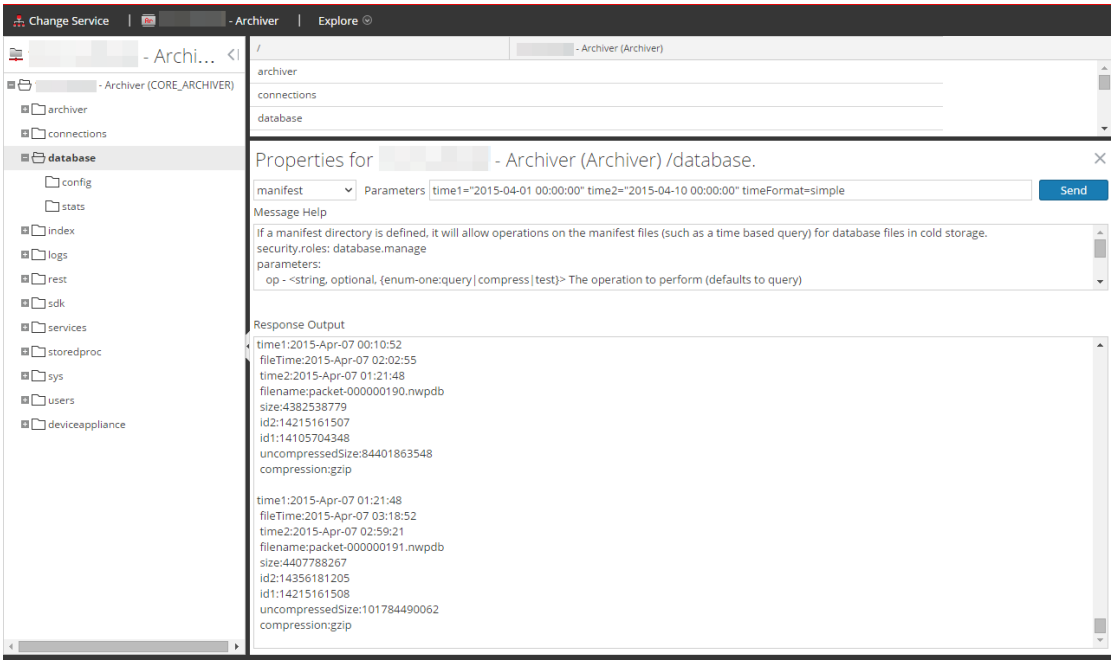
1. Vaya a **ADMIN > Servicios**.
2. Seleccione **Archiver**en la cuadrícula Servicios.
3. Navegue a la vista Explorador del dispositivo Archiver mediante la selección de > **Ver > Explorar**.

   Se muestra la vista Explorador para Archiver.
4. Haga clic con el botón secundario en el nodo **Base de datos** del árbol de la izquierda y seleccione las propiedades de **Base de datos** para abrirlas en el panel de la derecha.
5. Ejecute el comando **manifest** para el rango de tiempo seleccionado del 1.º de abril de 2015 al 10 de abril de 2015.

La búsqueda devuelve todos los archivos que se deben restaurar para la consulta que seleccionó.

Ejemplo de búsqueda:

```
time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
timeFormat=simple
```



6. Vaya a **ADMIN > Servicios**.
7. En la vista Servicios, seleccione un **Archiver** y, a continuación, elija  **> Ver > Configuración**.

   La vista Configuración de servicios se muestra con la pestaña General abierta.
8. Seleccione la pestaña **Recopilaciones.**
9. Cree una recopilación de restauración en la cual la ruta de origen señale a los archivos enumerados en la salida del comando manifest.
10. Guarde la recopilación.

    Una vez que haya creado correctamente una recopilación, puede usarla con fines de creación de informes e investigación.

Investigar una recopilación

Para realizar una investigación en función de una recopilación de Archiver:

1. Seleccione **Investigate**.
   Se muestra el cuadro de diálogo Investigate.

2. Haga clic en la pestaña **Recopilaciones** del cuadro de diálogo Investigar.
3. Seleccione un servicio Archiver en el panel de la izquierda.
4. Seleccione la recopilación que desea investigar en el panel de la derecha.
5. Haga clic en **Navegar**.

Aparece la vista Navegar, en la cual se muestran datos relacionados con la recopilación de Archiver que seleccionó.

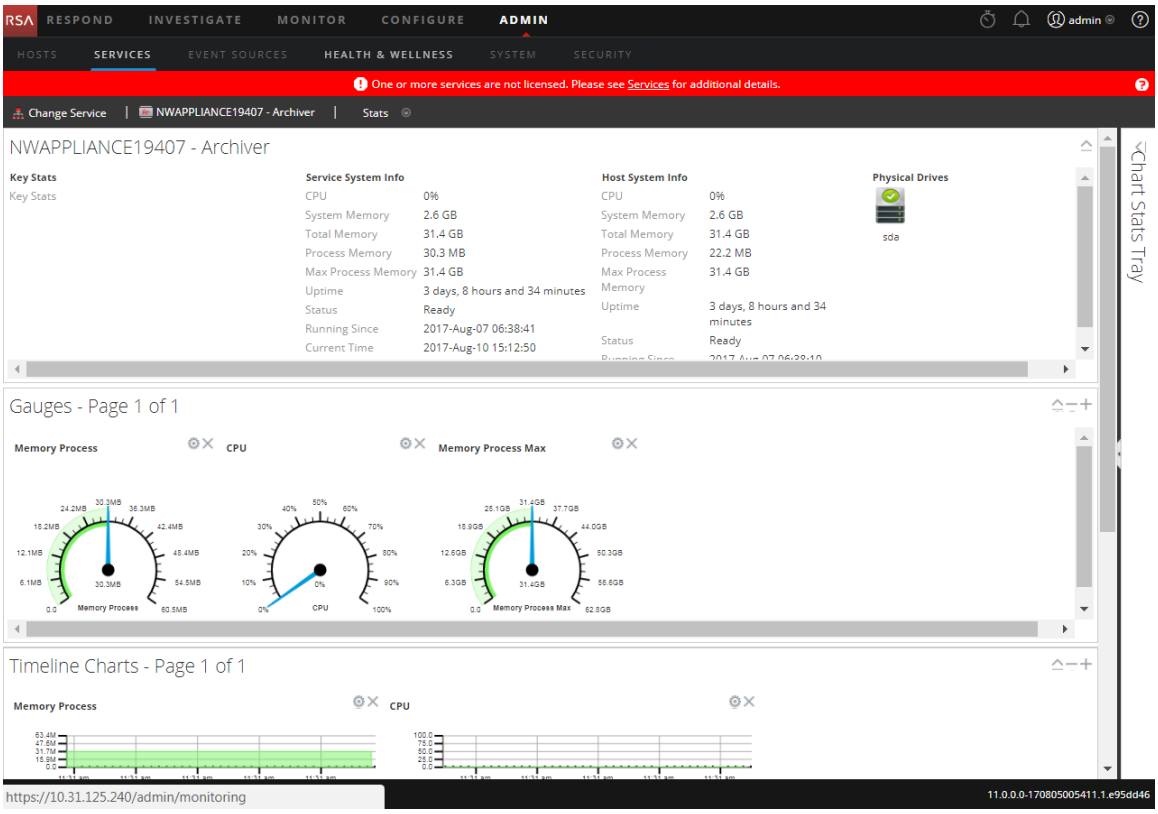
Nota: Para obtener información detallada sobre el uso de Investigation, consulte *Investigation y Malware Analysis*.

Ver estadísticas de recopilación de Archiver

Las mismas estadísticas disponibles para otros servicios se proporcionan para el servicio Archiver. En la vista Estadísticas de servicios se muestran estadísticas clave e información del sistema relacionadas con el servicio Archiver seleccionado. La información se muestra en varias secciones distintas dentro de la vista Estadísticas: Archiver, Medidores, Gráficos de cronograma y Bandeja de estadísticas de gráfico. La Bandeja de estadísticas de gráfico muestra todas las estadísticas disponibles para Archiver. Cualquier estadística en la Bandeja de estadísticas de gráfico se puede mostrar en un gráfico tipo velocímetro o de cronograma.

Realice los siguientes pasos para ver estadísticas de Archiver:

1. Vaya a **ADMIN > Servicios**.
2. En la vista Servicios, seleccione un Archiver y, a continuación, elija  **> Ver > Estadísticas**.
   Se muestra la vista Estadísticas de servicios.



Nota: Para obtener más información acerca de las estadísticas de Archiver, consulte *Guía de introducción de hosts y servicios*.

Ver registros de Archiver

Realice los siguientes pasos para ver registros en un servicio Archiver:

1. Vaya a **ADMIN > Servicios.**
2. En la vista Servicios, seleccione un **Archiver** y, a continuación, seleccione  **> Ver > Registros**.
   Se muestra la cuadrícula Registros de servicios.

Nota: Para obtener información sobre la visualización y la configuración de registros de auditoría, consulte **Configurar el registro de auditoría global** de la *Guía de configuración del sistema.*

Agregar el servicio Archiver como un origen de datos en Broker

La adición del servicio Archiver como un origen de datos en Broker es de utilidad cuando hay más de una recopilación y se desea generar un informe sobre los datos archivados. Para hacerlo, puede agregar más de una recopilación como un servicio descendente a un Broker y generar un informe sobre él.

Requisitos previos

Asegúrese de:

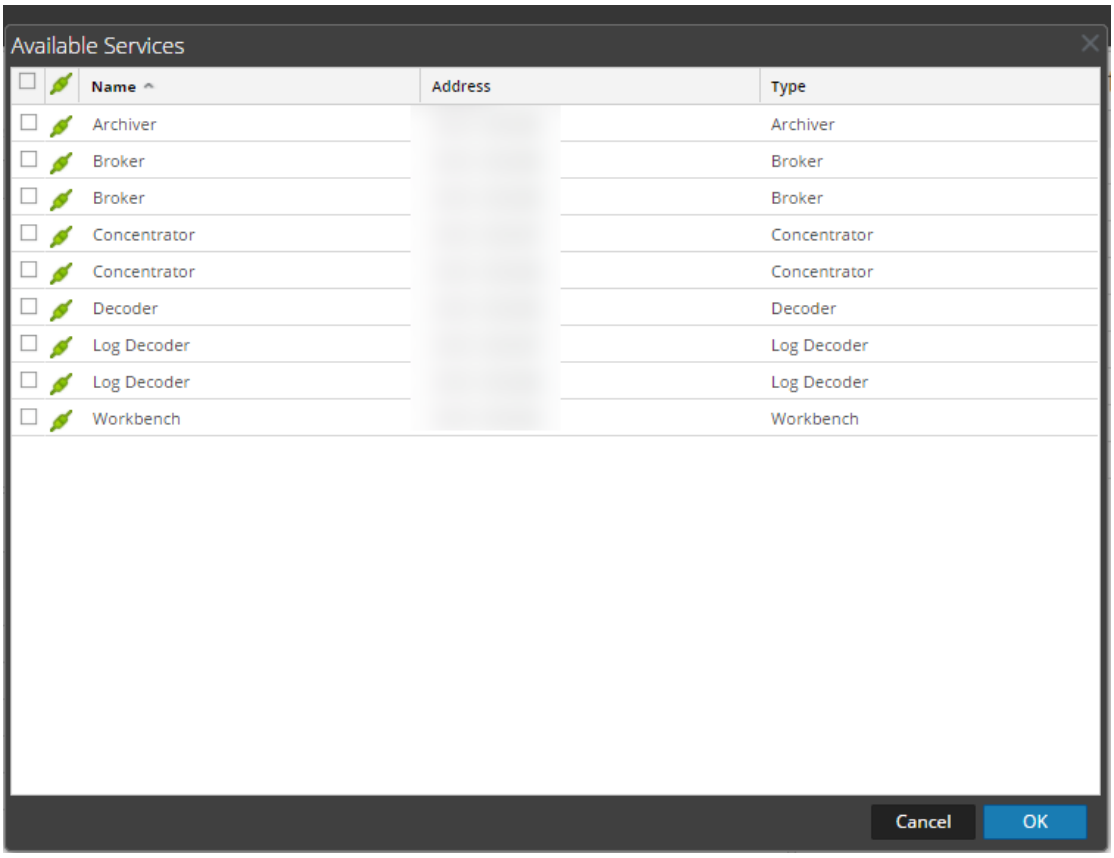
- Haber instalado el servicio Archiver en el host de Archiver.
- Haber agregado una recopilación en el servicio Archiver.

Procedimiento

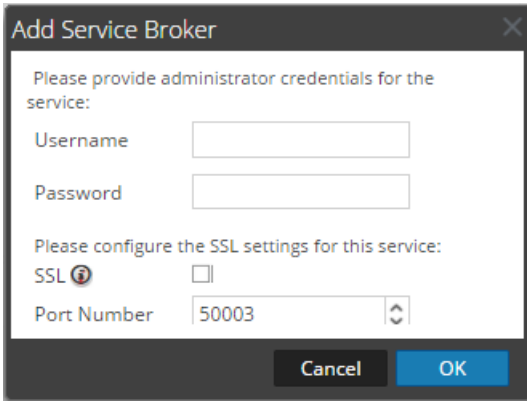
Para agregar un servicio Archiver como un origen de datos en el Broker:

1. Seleccione **ADMIN > Servicios**.
2. En el panel **Servicios**, seleccione un servicio Broker.
3. En la columna **Acciones**, seleccione  **> Ver > Configuración**.
   La vista Configurar se muestra con la pestaña General abierta.

4. En la sección **Servicios agregados**, haga clic en +.
   Se muestra el cuadro de diálogo Servicios disponibles.



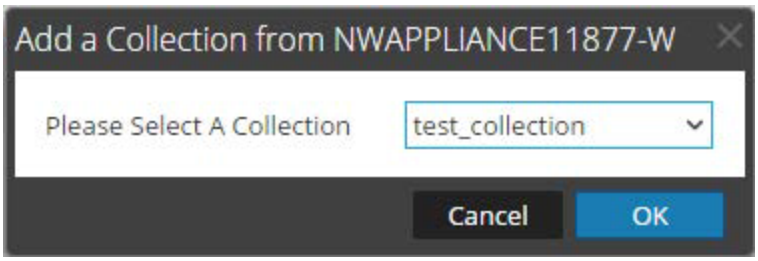
6. Seleccione el servicio Broker y haga clic en **Aceptar**.
7. Si el servicio Archiver usa un modelo de confianza, se muestra un cuadro de diálogo Información de servicio para el servicio seleccionado.



8. Escriba el nombre de usuario y la contraseña de las credenciales de administrador correspondientes al servicio.

9. Haga clic en **Aceptar**.

   Se muestra el cuadro de diálogo Agregar recopilación.



10. Seleccione una recopilación en la lista desplegable y haga clic en **Aceptar**.

    El servicio Archiver se agrega como un origen de datos en el Broker.

Nota: Este procedimiento se debe realizar para cada recopilación.

Recuperar información de hash

Archiver proporciona un comando, **hashInfo**, con el cual puede recuperar la información de hash de cada base de datos de sesiones, metadatos y paquetes que cumple con los criterios de lista de sesiones o rango de fechas. La información de hash recuperada tiene el formato de lista de parámetros de cadena, y cada parámetro de cadena corresponde a la información de hash de un único archivo de la base de datos. Puede recuperar la información de hash de los archivos de la base de datos mediante la vista Explorar servicio de Archiver o la interfaz de REST del servicio Archiver. La información de hash que se recupera de este modo se usa para comparar los archivos de la base de datos en la ubicación original y en la ubicación exportada con el fin de validar la integridad de los datos.

En la siguiente tabla se indican los criterios que puede usar para recuperar los archivos de hash de la base de datos.

Criterios	Descripción
sessions	Puede recuperar la información de hash de los archivos de la base de datos si especifica las sesiones que existen o que se leen desde la base de datos de sesiones para determinar el ID de metadatos y paquetes asociado que se necesita para establecer los archivos de las bases de datos de metadatos y paquetes requeridos para recuperar la información de hash. **Por ejemplo:** sessions=100: Recupera la información de hash de todos los archivos de la base de datos que contienen los componentes constitutivos (sesión, metadatos y contenido) de la sesión 100. sessions=100,500000: Recupera la información de hash de todos los archivos de la base de datos que contienen los componentes constitutivos (sesión, metadatos y contenido) de las sesiones 100 y 500,000.
beginDate	Puede especificar una fecha de inicio para filtrar los archivos de la base de datos. Con esto se busca la información de hash correspondiente a los archivos creados después de la fecha especificada. La fecha de inicio especificada debe estar en el formato AAAA-MM-DD HH:MM:SS.

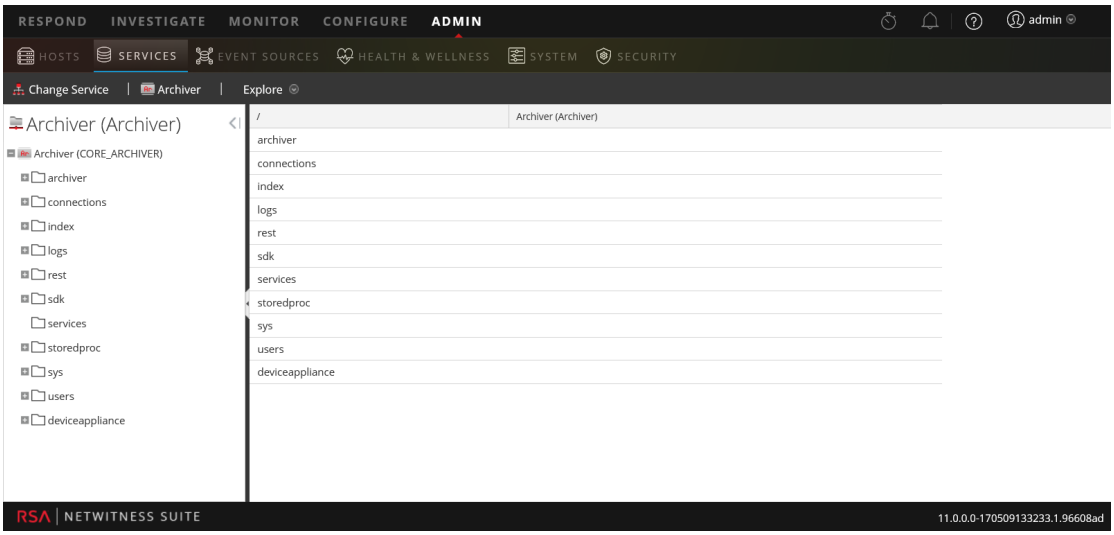
Criterios	Descripción
endDate	Puede especificar una fecha de finalización para filtrar los archivos de la base de datos. Con esto se busca la información de hash correspondiente a los archivos creados antes de la fecha especificada. La fecha de finalización especificada debe estar en el formato AAAA-MM-DD HH:MM:SS. **Por ejemplo:** beginDate: “2014-Mar-25 05:52:00” endDate=”2014-Mar-27 05:52:00”: Recupera la información de hash de todos los archivos de la base de datos entre el 25 de marzo de 2014 y el 27 de marzo de 2014 en el rango de horas especificado en esos días.
directorios	De forma predeterminada, los archivos de información de hash se almacenan con los archivos de la base de datos para los cuales se crearon. También puede almacenar el archivo de información de hash en otra ubicación si define varias ubicaciones en el parámetro de configuración hash.dir. Puede definir la ubicación como un filtro y recuperar los archivos de información de hash para la ubicación configurada. **Por ejemplo:** directories="/home/hash": Recupera la información de hash de los archivos de la base de datos desde la ubicación /home/hash.

Procedimiento

Para recuperar información de hash de los archivos de la base de datos:

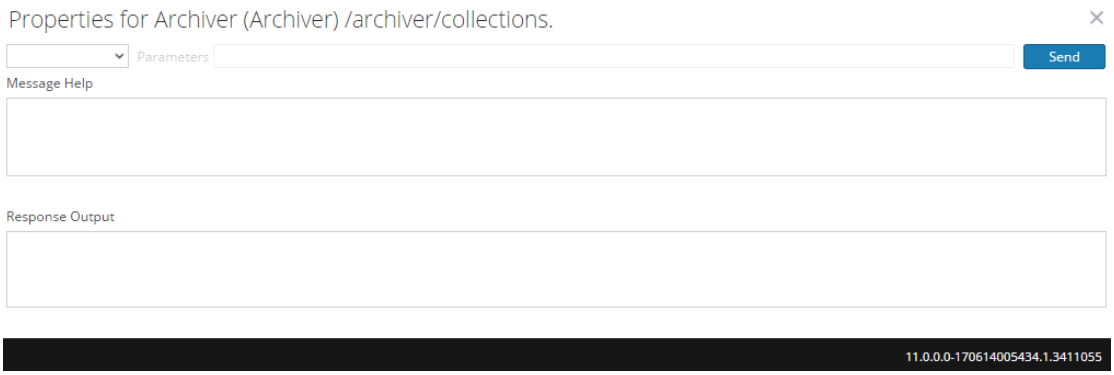
1. Seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Archiver.
3. En la columna **Acciones**, seleccione **Ver > Explorar**.

   Se muestra la vista Explorar del servicio Archiver.



4. En el árbol de nodos, haga clic con el botón secundario en **archiver** y seleccione **Propiedades**.

   Se muestra el cuadro de diálogo Propiedades.



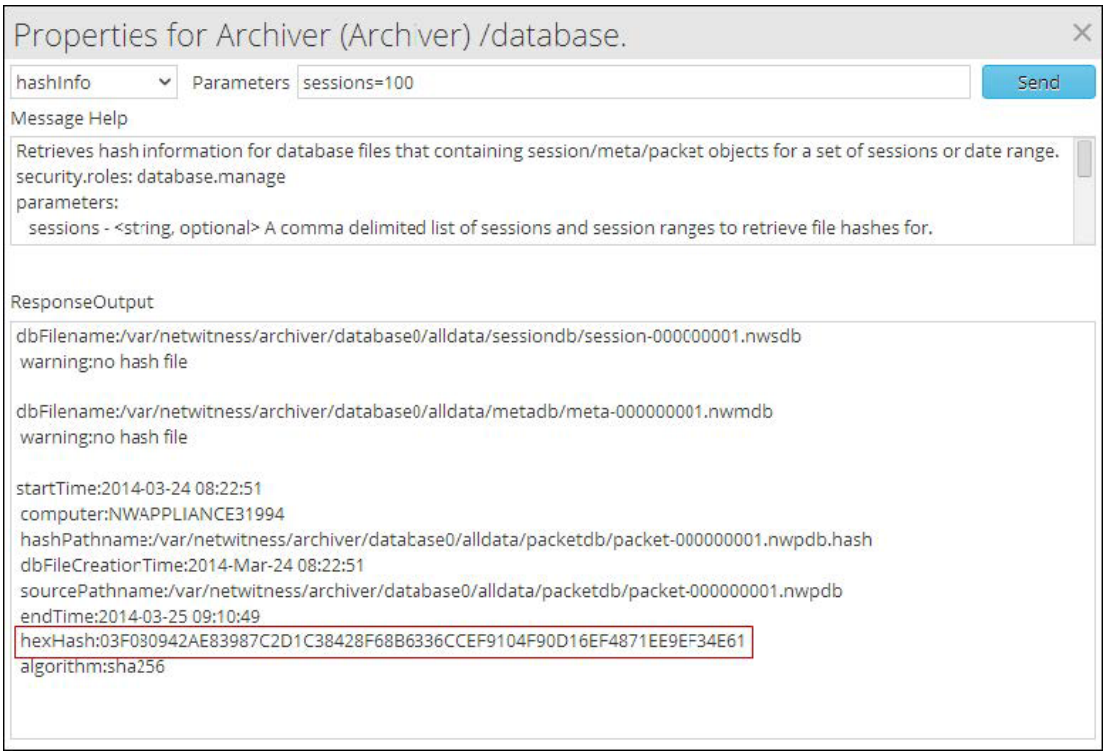
5. En el menú desplegable, seleccione **hashInfo**.
6. En el campo **Parámetros**, escriba los criterios que desea usar para recuperar la información de hash de la base de datos.
7. Haga clic en **Enviar**.

   La salida del comando se muestra en el cuadro de texto Salida de respuesta. En la salida, la información de hash se muestra en el parámetro hexHash. Puede usar esta información de hash para verificar manualmente la integridad de los datos.

Ejemplos

Recupere la información de hash de los archivos de la base de datos para las sesiones que existen.
Criterios: sessions=100

Salida

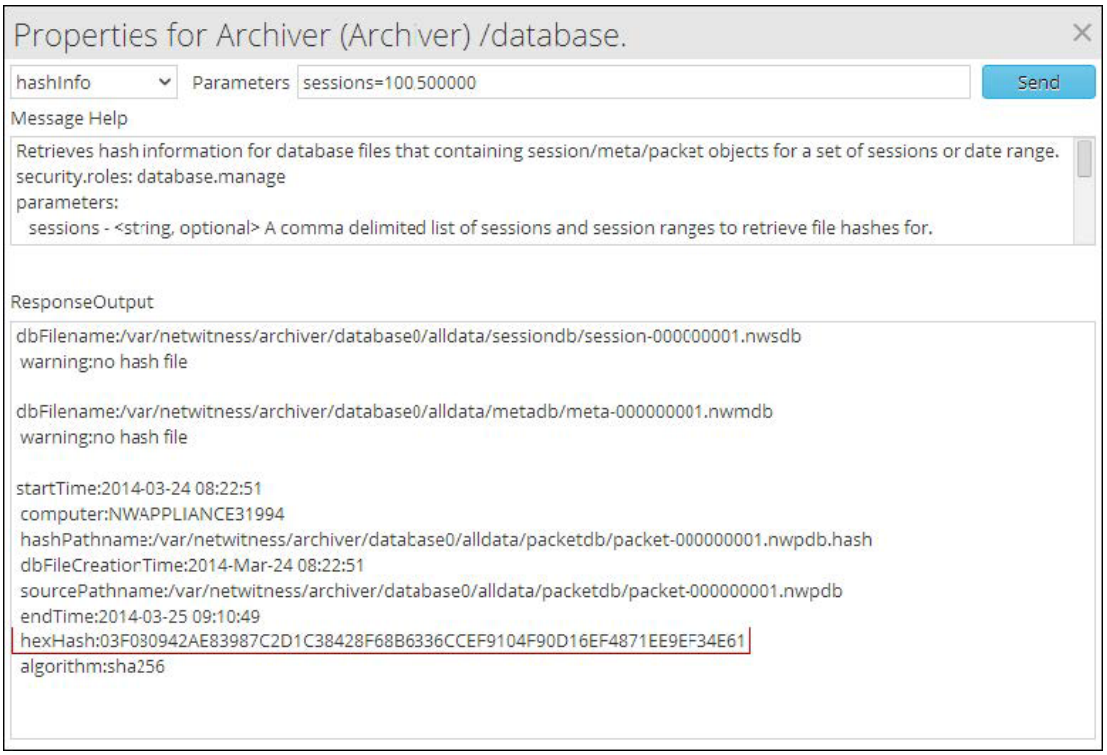


Se recupera la información de hash que se muestra en el parámetro hexHash y esta información se puede usar para verificar manualmente la integridad de los datos de la sesión 100.

Recupere la información de hash de los archivos de la base de datos para los rangos de sesiones que existen.

Criterios: sessions=100,500000

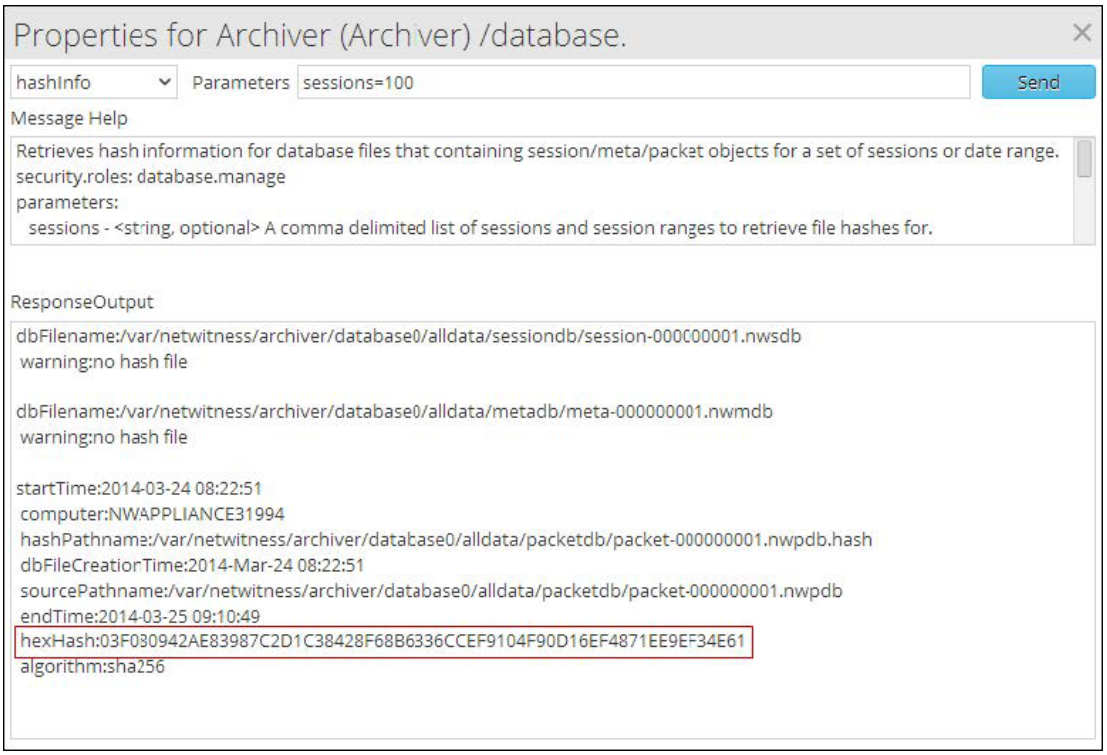
Salida



Se recupera la información de hash que se muestra en el parámetro hexHash y esta información se puede usar para verificar manualmente la integridad de los datos del rango de sesiones 100 a 500,000

Recupere la información de hash de los archivos de la base de datos creados en el rango de fechas especificado
Criterios: beginDate="2017-Mar-25 05:52:15" endDate="2017-Mar-27 05:52:15"

Salida



Se recupera la información de hash que se muestra en el parámetro hexHash y esta información se puede usar para verificar manualmente la integridad de los datos correspondientes al rango de fechas especificado.

Referencias

Este tema es un conjunto de referencias que describen la interfaz del usuario de Archiver en NetWitness Suite.

Temas

Cuadro de diálogo Recopilación de Archiver

En Administration > Servicios > vista Configuración > pestaña Retención de datos de un Archiver, los administradores pueden definir los criterios para el almacenamiento y la retención de registros. En el cuadro de diálogo Recopilación, al cual se accede desde la sección Recopilaciones, puede definir las recopilaciones de almacenamiento individuales que se usarán para los distintos tipos de registros. Por ejemplo, tal vez desee crear recopilaciones por motivos de cumplimiento de normas o conservar registros importantes de manera selectiva.

Flujo de trabajo

En este flujo de trabajo se ilustra el proceso de instalación y configuración de punto a punto para un Archiver.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo…
Administrador	Configurar recopilaciones de Archiver	Configurar el almacenamiento y la retención de registros de Archiver

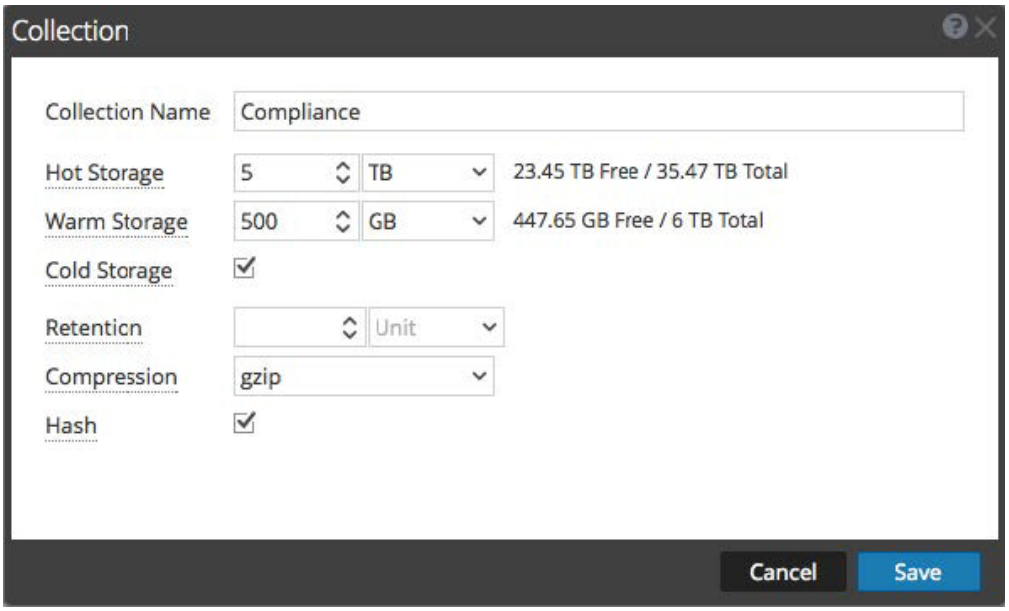
Temas relacionados

Configurar el almacenamiento y la retención de registros de Archiver

Vista rápida

Para acceder al cuadro de diálogo Recopilación:

1. Vaya a ADMIN >Servicios.
2. Seleccione un servicio Archiver y elija >  Ver > Configuración.
3. En la vista Configuración de servicios correspondiente al servicio, haga clic en la pestaña Retención de datos.
4. En la sección Recopilaciones, haga clic en  .
   Se muestra el cuadro de diálogo Recopilación.



Nota: Cuando se disminuyen las asignaciones de almacenamiento de recopilación o se reduce el tiempo de retención, pueden pasar varios minutos o varias horas antes de que se transfieran los datos y que el espacio esté disponible en función de la cantidad de datos que se transfieren. Los tiempos predeterminados son cada 20 minutos para una transferencia por tamaño y cada seis horas para una transferencia por tiempo.

En la siguiente tabla se describen los campos del cuadro de diálogo Recopilación.

Campo	Descripción
Nombre de recopilación	Especifique un nombre para la recopilación, como Compliance, MediumValue o LowValue.
Almacenamiento activo	Especifique el tamaño máximo o el porcentaje del almacenamiento activo que se usará para esta recopilación. El espacio libre disponible que se usará para el almacenamiento activo y el almacenamiento activo total se muestran junto a este campo. Cuando los registros alcanzan el tamaño máximo del almacenamiento activo, se quitan o se transfieren al siguiente nivel de almacenamiento disponible (semiactivo o inactivo).

Campo	Descripción
Almacenamiento semiactivo	(Opcional) Especifique el tamaño máximo o el porcentaje del almacenamiento semiactivo que se usará para esta recopilación. El espacio libre disponible que se usará para el almacenamiento semiactivo y el almacenamiento semiactivo total se muestran junto a este campo. Cuando los registros alcanzan el tamaño máximo del almacenamiento semiactivo, se quitan o se transfieren al almacenamiento inactivo disponible.
Almacenamiento inactivo	(Opcional) Especifique si desea usar almacenamiento inactivo para esta recopilación. Si utiliza almacenamiento inactivo para la recopilación, los registros que superan los límites de tamaño y retención especificados se transfieren al almacenamiento inactivo. Si no lo utiliza, los registros que superan estos límites se quitan.
Retención	(Opcional) Especifique la cantidad de días que se conservan los registros antes de que se eliminen o se transfieran al almacenamiento inactivo. En el caso del almacenamiento activo y semiactivo, los ajustes del tamaño y el período de retención para una recopilación pueden reemplazarse mutuamente en función del criterio que se cumple primero (tamaño o tiempo).

Campo	Descripción
Compresión	Especifique el tipo de compresión que se usará para los metadatos y los registros crudos en la recopilación. Puede comprimir los metadatos y los registros crudos mediante GZIP o LZMA para ahorrar espacio. GZIP es muy rápido para comprimir y descomprimir, pero no comprime tan bien como LZMA. LZMA ofrece una mejor compresión a expensas de la velocidad de descompresión (aproximadamente tres veces más lenta que la de GZIP). Las relaciones de compresión dependen en gran medida de los datos. La compresión predeterminada es GZIP.
Hash	Especifique si desea habilitar o deshabilitar hash. Cuando está habilitado, el algoritmo hash se usa para verificar la integridad de los datos de los archivos que se guardan.

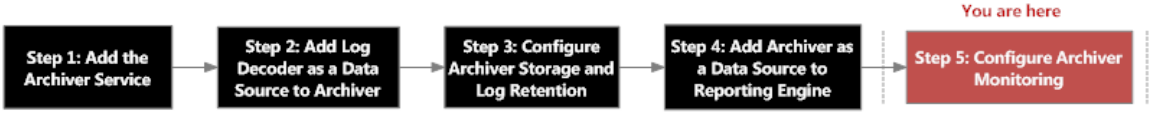
Vista Configuración de servicios de Archiver: Pestaña General

La pestaña General de un Archiver en la vista Configuración de servicios permite administrar la configuración básica de servicios, configurar el servicio agregado y configurar el proceso de agregación entre un Archiver y el servicio agregado.

Para acceder a la pestaña General, vaya a ADMIN > Servicios, seleccione un servicio Archiver y, a continuación, seleccione Ver > Configuración.

Flujo de trabajo

En este flujo de trabajo se ilustra el proceso de instalación y configuración de punto a punto para un Archiver.



La configuración de servicios agregados (cuyos datos se consumen y agregan) incluye:

- Adición, edición y eliminación de Archivers como servicios agregados
- Alternación de un servicio agregado de modo que funcione en línea y offline
- Estadísticas de monitoreo de servicios agregados
- Inicio y detención de una agregación

La configuración del proceso de agregación incluye los ajustes de:

- Inicio automático de una agregación
- Parámetros de tiempo y rendimiento, como la cantidad de sesiones por ronda de agregación y el tiempo entre rondas
- Las veces que se intenta reiniciar, reconectar o dejar offline un servicio agregado que no responde

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo…
Administrador	Iniciar y detener la agregación Agregar, editar, eliminar y alternar un servicio agregado	Sección Servicios agregados

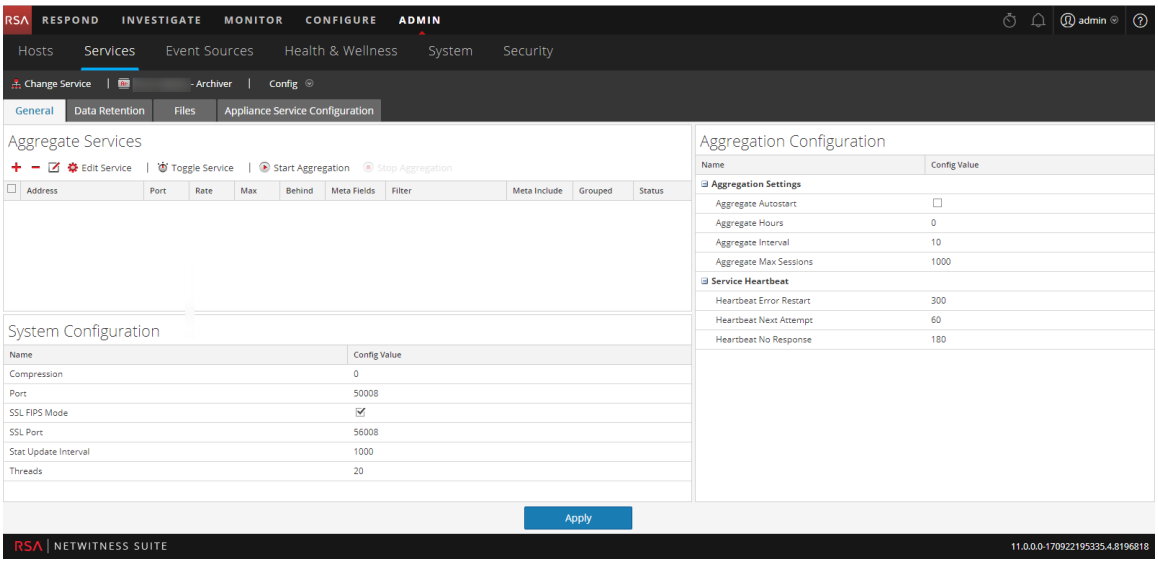
Función	Deseo…	Mostrarme cómo…
Administrador	Administrar la configuración del sistema	Sección Configuración del sistema

Temas relacionados

Configurar el monitoreo de Archiver

Vista rápida

Este es un ejemplo de la pestaña General.



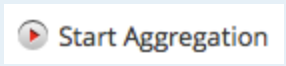
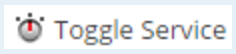
Estas son las tres secciones principales de la pestaña General de los Archivers:

- Servicios agregados
- Configuración del sistema
- Configuración de agregación

Sección Servicios agregados

La sección Servicios agregados proporciona una manera de iniciar y detener la agregación, así como agregar, editar, eliminar y alternar un servicio agregado. Este es un ejemplo de la sección Servicios agregados de un Concentrator.

La barra de herramientas de la sección Servicios agregados ofrece las siguientes opciones.

Opción	Descripción
	Abre un cuadro de diálogo donde puede agregar un Concentrator, Decoder o Log Decoder como servicio agregado.
	Elimina los servicios agregados seleccionados.
	Se abre un cuadro de diálogo para editar valores de **Campos de metadatos** y valores de **Filtro**.
	Cuando la agregación de datos está detenida o no se ha iniciado, se inicia desde el servicio en línea en la lista mediante el uso de las reglas definidas para el servicio.
	Cuando la agregación está en curso, detiene la agregación en el Broker o Concentrator. Esto detiene todos los servicios y elimina el índice, lo cual puede tardar varios minutos. Es necesario detener los servicios agregados para realizar diversos procedimientos administrativos.
	Alterna el estado de un servicio entre offline y en línea. Solo los datos de los servicios en línea se consumen durante la agregación.

La lista de la sección Servicios agregados tiene las siguientes columnas.

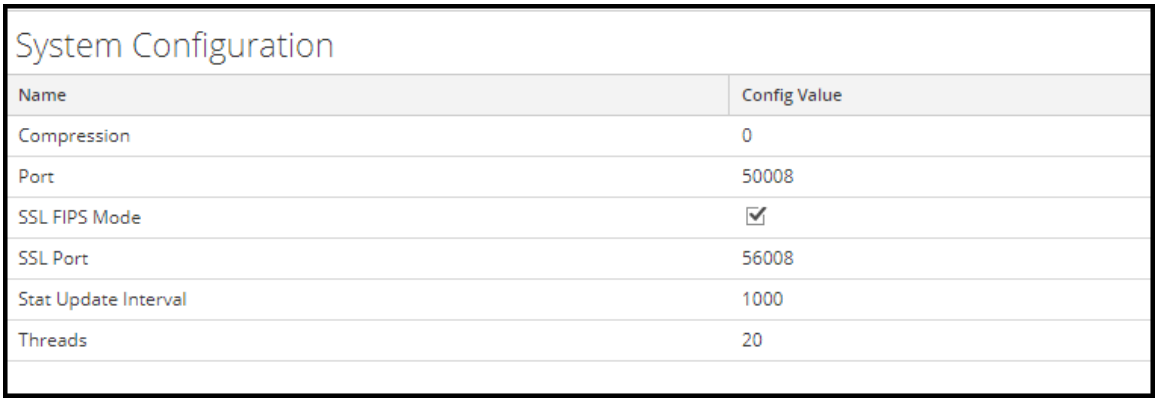
Columna	Descripción
Dirección	Muestra la dirección del servicio.

Columna	Descripción
Puerto	Muestra el puerto en el cual escucha el servicio. Los puertos predeterminados son: • 50001 para Log Collectors • 50002 para Log Decoders • 50003 para Brokers • 50004 para Decoders • 50005 para Concentrators • 50007 para otros servicios
Tasa	Muestra la cantidad de objetos de metadatos que se están escribiendo en la base de datos por segundo. Los valores son muestras de promedios móviles en un corto periodo de tiempo (10 segundos). Una vez que la captura se detiene, la tasa se restablece a **cero**.
Máx.	Indica la cantidad máxima de objetos de metadatos escritos en la base de datos por segundo desde que se inició la captura. Los valores son muestras de promedios móviles en un corto periodo de tiempo (10 segundos). Una vez que la captura se detiene, **Máx.** sigue mostrando el valor máximo durante la captura.
Atrás	Indica la cantidad de sesiones en el servicio que se deben agregar.
Recopilación	Solo para Brokers, indica la recopilación que se seleccionó cuando se agregó el servicio Archiver Workbench a la sección Servicios agregados.
Campos de metadatos	Solo para Concentrators, indica los tipos de metadatos que el servicio agregado está consumiendo.
Filtro	Solo para Concentrators, indica cualquier filtro que se esté aplicando a los metadatos que el servicio agregado está consumiendo.
Inclusión de metadatos	Solo para Concentrators, indica la cantidad de tipos de metadatos incluidos en el servicio agregado.

Columna	Descripción
Agrupado	Si el servicio agregado es parte de un grupo.
Estado	Indica el estado actual del servicio: • en línea = disponible para proporcionar datos para el consumo de Broker o Concentrator • offline = no disponible para proporcionar datos para el consumo de Broker o Concentrator • consumiendo = proporcionando datos para el consumo de Broker o Concentrator

Sección Configuración del sistema

La sección Configuración del sistema administra la configuración del servicio de un servicio. Cuando un servicio se agrega por primera vez, se aplican valores predeterminados. Puede editar estos valores para ajustar el rendimiento.


System Configuration

Name	Config Value
Compression	0
Port	50008
SSL FIPS Mode	☑
SSL Port	56008
Stat Update Interval	1000
Threads	20

La sección Configuración del sistema tiene estos parámetros.

Parámetro	Descripción
Compresión	La cantidad mínima de bytes que se deben transmitir por respuesta antes de la compresión. Si se define en **0**, se deshabilita la compresión. El valor predeterminado es **0**. Un cambio en el valor se aplica de inmediato en todas las conexiones subsiguientes.

Parámetro	Descripción
Puerto	El puerto en el cual escucha el servicio. Los puertos predeterminados son: • 50001 para Log Collectors • 50002 para Log Decoders • 50003 para Brokers • 50004 para Decoders • 50005 para Concentrators • 50007 para otros servicios
Modo SSL FIPS	Cuando se habilita (**activado**), la seguridad de la transmisión de datos se administra mediante el cifrado de información y la entrega de autenticación mediante certificados SSL. El valor predeterminado es **off**.
Puerto SSL	Indica el puerto SSL.
Intervalo de actualización de estadísticas	La cantidad de milisegundos entre las actualizaciones de estadísticas del sistema. Los números más bajos permiten actualizaciones frecuentes y pueden retrasar otros procesos. El valor predeterminado es **1,000**. Un cambio en el valor se aplica de inmediato.
Subprocesos	El número de hilos de ejecución en el pool de hilos de ejecución para manejar solicitudes entrantes. Si se define en **0**, se permite que el sistema decida. El valor predeterminado es **15**. Un cambio se aplica tras el reinicio del servicio.

Sección Configuración de agregación

La sección Configuración de agregación proporciona ajustes de configuración que afectan diversos aspectos del proceso de agregación. Cuando hace clic en **Aplicar**, los cambios se guardan; sin embargo, no todos los ajustes se aplican de inmediato. En las tablas de Configuración de agregación y Latido del servicio se proporcionan detalles.

Precaución: No edite ninguno de estos ajustes sin orientación del servicio al cliente.

Aggregation Configuration

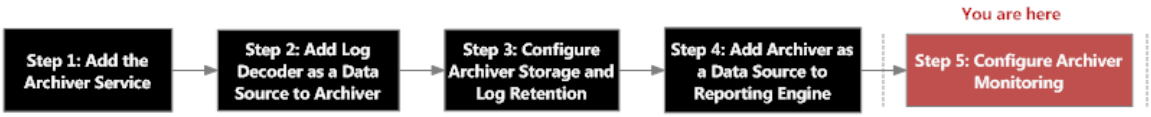
Name	Config Value
Aggregation Settings	
Aggregate Autostart	☐
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	1000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Configuración del servicio Archiver

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

Flujo de trabajo

En este flujo de trabajo se ilustra el proceso de instalación y configuración de punto a punto para un Archiver



¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo…
Administrador	Configurar los ajustes de Archiver.	/archiver/config
Administrador	Configurar los ajustes de la base de datos.	/database/config
Administrador	Configurar los ajustes del índice.	/index/config
Administrador	Configurar los ajustes de registros.	/logs/config
Administrador	Configurar los ajustes de REST.	/rest/config
Administrador	Configurar los ajustes de SDK.	/sdk/config
Administrador	Configurar los ajustes de servicios.	/services/<service name>/config
Administrador	Configurar los ajustes del sistema.	/sys/config

Temas relacionados

- Para obtener más información sobre cómo configurar los ajustes de la base de datos, consulte el tema “Nodos de configuración de la base de datos” en la *Guía de ajuste de la base de*

datos de RSA NetWitness Core.

- Para obtener más información sobre cómo configurar los ajustes del índice, consulte el tema "Nodos de configuración del índice" en la *Guía de ajuste de la base de datos de RSA NetWitness Core*.
- Para obtener más información sobre cómo configurar los ajustes de SDK, consulte el tema "Nodos de configuración de SDK" en la *Guía de ajuste de la base de datos de RSA NetWitness Core*.

Pestaña Retención de datos: Archiver

En Admin > Servicios > vista Configuración > pestaña Retención de datos de un Archiver, los administradores pueden definir los criterios para el almacenamiento y la retención de registros.

Flujo de trabajo

En este flujo de trabajo se ilustra el proceso de instalación y configuración de punto a punto para un Archiver. En la pestaña Retención de datos, puede configurar el almacenamiento activo, semiactivo e inactivo, y también varias recopilaciones de almacenamiento para la retención de datos.

¿Qué desea hacer?

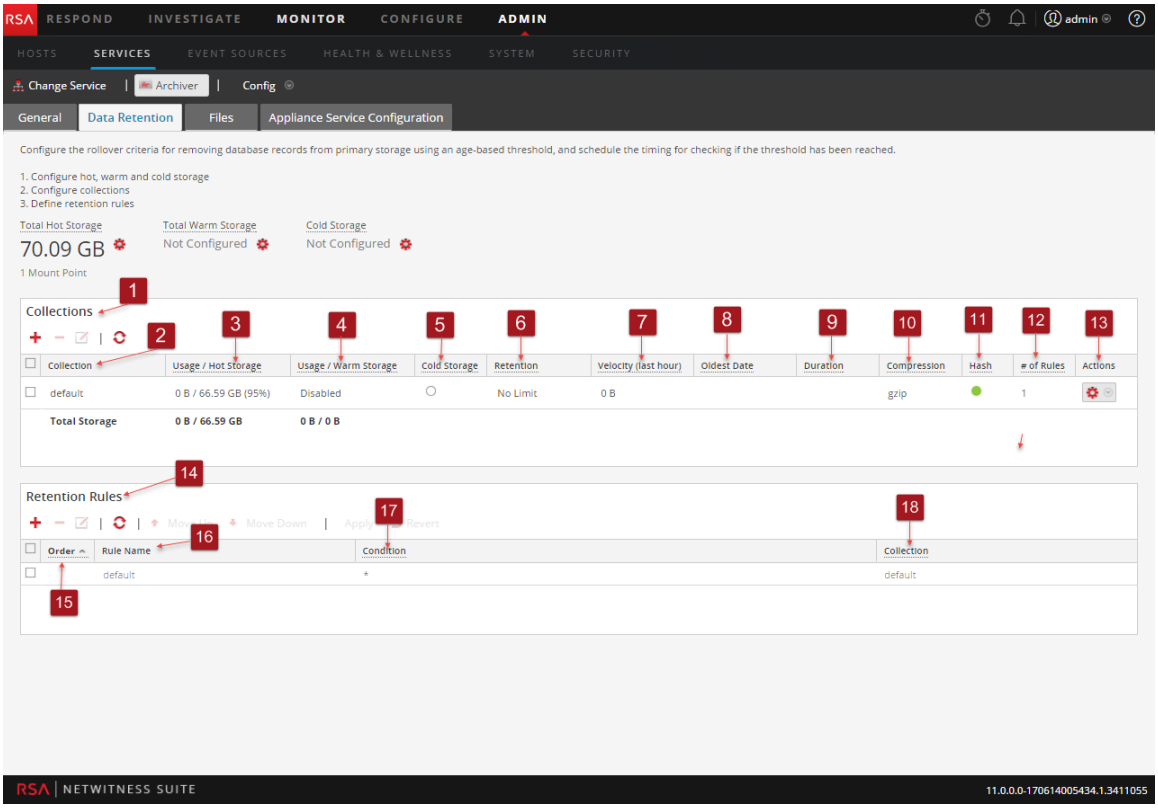
Función	Deseo…	Mostrarme cómo…
Administrador	Configurar el almacenamiento activo total	Configurar el almacenamiento activo, semiactivo e inactivo
Administrador	Configurar el almacenamiento semiactivo total (opcional)	Configurar el almacenamiento activo, semiactivo e inactivo
Administrador	Configurar el almacenamiento inactivo total (opcional)	Configurar el almacenamiento activo, semiactivo e inactivo
Administrador	Configurar recopilaciones	Configurar recopilaciones de almacenamiento de registros
Administrador	Configurar reglas de retención	Definir reglas de retención

Temas relacionados

- Configurar el almacenamiento activo, semiactivo e inactivo
- Configurar el almacenamiento y la retención de registros de Archiver
- Definir reglas de retención

Vista rápida

Como administrador, puede configurar el almacenamiento activo, semiactivo e inactivo, así como varias recopilaciones de almacenamiento con distintas ubicaciones y criterios para la retención de registros. Por ejemplo, puede crear una recopilación de cumplimiento de normas que almacena registros durante un período específico según lo exigen las normativas gubernamentales. Puede crear otra recopilación que almacena registros de valor bajo en el almacenamiento activo con un período de retención mucho más breve. La flexibilidad de estas recopilaciones permite que los requisitos generales del almacenamiento sean considerablemente menores.



1	Muestra el panel Recopilaciones con la pestaña Retención de datos abierta.
2	Permite ordenar las recopilaciones en orden ascendente o descendente.
3	Muestra el espacio de almacenamiento activo asignado para la recopilación, así como el uso actual aproximado.
4	Muestra el espacio de almacenamiento semiactivo asignado para la recopilación, así como el uso actual aproximado.
5	Muestra si la recopilación usa almacenamiento inactivo para el respaldo a largo plazo.
6	Muestra el rango de tiempo que se usa para determinar cuándo los datos se transfieren al almacenamiento inactivo o se descartan.

7	Muestra la cantidad de datos escritos en la recopilación en la última hora.
8	Muestra la fecha de los datos más antiguos almacenados en la recopilación.
9	Muestra la edad aproximada de los datos más antiguos almacenados en la recopilación.
10	Muestra el tipo de compresión que se usa en el almacenamiento de la recopilación.
11	Muestra si se usan o no valores hash cuando se almacenan datos en la recopilación.
12	Muestra la cantidad de reglas de retención que usa esta recopilación para almacenar datos.
13	Muestra el menú desplegable Acciones.
14	Muestra el panel Reglas de retención.
15	Muestra el orden en el cual se evalúan las reglas de retención en la cadena de ejecución.
16	Muestra el nombre de la regla de retención.
17	Los datos que satisfacen esta condición se almacenan en la recopilación correspondiente.
18	Muestra la recopilación que se usa para almacenar los datos que satisfacen esta condición de regla específica.

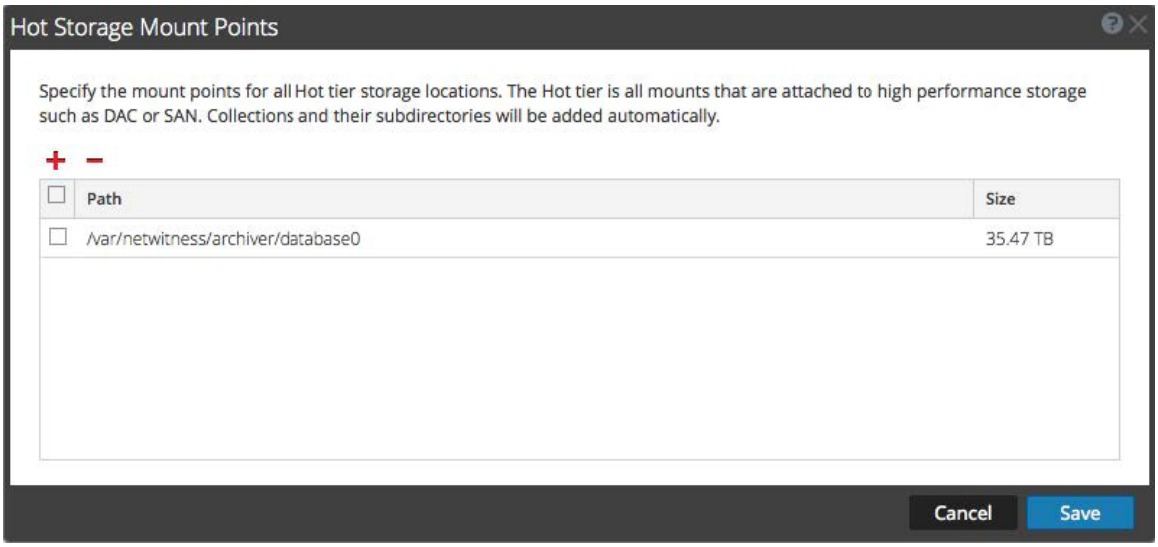
Almacenamiento activo, semiactivos e inactivo total

En la sección Almacenamiento activo total se muestra la cantidad total de almacenamiento activo disponible y la cantidad de puntos de montaje de almacenamiento activo. En la sección Almacenamiento semiactivo total se muestra la cantidad total de almacenamiento semiactivo disponible y la cantidad de puntos de montaje de almacenamiento semiactivo. En la sección Almacenamiento inactivo total se muestra la cantidad total de almacenamiento inactivo y el espacio libre restante disponible en el almacenamiento inactivo.

Cuadros de diálogo Puntos de montaje del almacenamiento activo, semiactivo e inactivo

En los cuadros de diálogo Puntos de montaje del almacenamiento activo, semiactivo e inactivo, puede especificar los puntos de montaje para las ubicaciones de almacenamiento. Puede especificar las partes de este almacenamiento que usará para las recopilaciones de almacenamiento de registros.

Para acceder a los cuadros de diálogo Puntos de montaje del almacenamiento activo, semiactivo e inactivo, haga clic en el ícono cerca de la sección correspondiente.

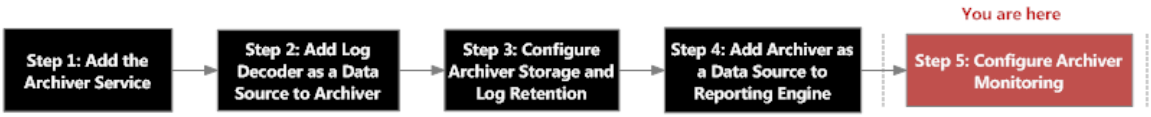

Hot Storage Mount Points
Specify the mount points for all Hot tier storage locations. The Hot tier is all mounts that are attached to high performance storage such as DAC or SAN. Collections and their subdirectories will be added automatically.
Path
Size
/var/netwitness/archiver/database0
35.47 TB
Cancel
Save

Vista Configuración de servicios: Archiver

La vista Configuración de servicios (ADMIN > Servicios > seleccione el servicio Archiver y elija >Ver > Configuración) proporciona una manera de administrar la configuración básica del servicio, configurar servicios agregados, configurar el almacenamiento y la retención de registros, editar archivos de configuración del servicio y configurar el servicio del dispositivo para un Archiver.

Flujo de trabajo

En este flujo de trabajo se ilustra el proceso de instalación y configuración de punto a punto para un Archiver.



¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo…
Administrador	*Agregar un Log Decoder como un servicio agregado.	Haga clic en en la sección Servicios agregados.
Administrador	*Quitar el servicio agregado seleccionado.	Haga clic en en la sección Servicios agregados.
Administrador	*Editar valores de Campos de metadatos y valores de Filtro del servicio agregado.	Haga clic en en la sección Servicios agregados. Puede especificar el tipo de metadatos que consume el Archiver desde este servicio. También puede especificar una regla para filtrar los datos que consume el Archiver desde este servicio.

Función	Deseo…	Mostrarme cómo…
Administrador	*Comunicarse con el Archiver.	Haga clic en Edit Service en la sección Servicios agregados. Esto permite ingresar las credenciales de administrador del servicio agregado seleccionado, de modo que se pueda comunicar con el Archiver.
Administrador	*Alternar el estado de un servicio entre offline y en línea.	Haga clic en Toggle Service en la sección Servicios agregados.
Administrador	*Agregar datos mediante las reglas definidas para el servicio.	Haga clic en Start Aggregation en la sección Servicios agregados. Tenga en cuenta que es necesario iniciar el servicio agregado una vez que se ha detenido la agregación.
Administrador	*Detener la agregación en el Archiver.	Haga clic en Stop Aggregation en la sección Servicios agregados. Esto detiene todos los servicios y elimina el índice, lo cual puede tardar varios minutos. Es necesario detener los servicios agregados para realizar diversos procedimientos administrativos.

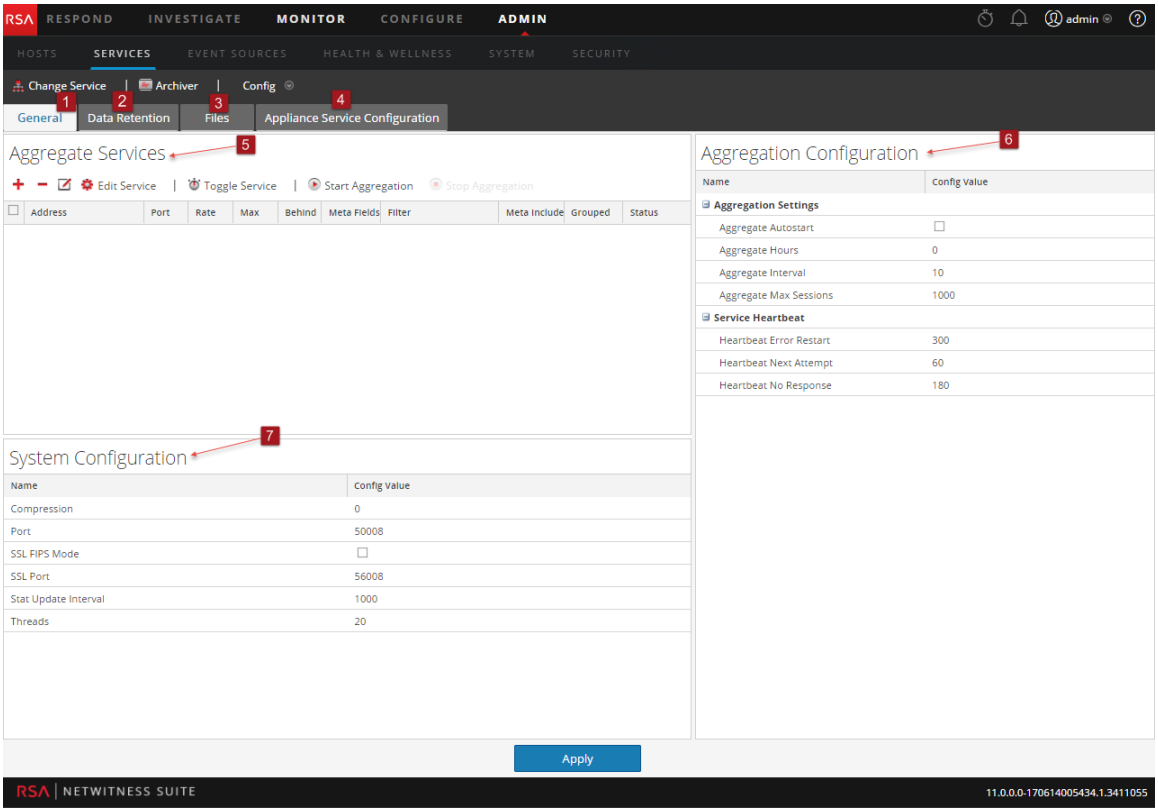
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Agregar Log Decoder como un origen de datos en Archiver
- Configurar el monitoreo de Archiver
- Configurar recopilaciones de almacenamiento de registros

Vista rápida

La vista Configuración de servicios tiene cuatro pestañas y tres paneles.



1	La pestaña General proporciona una manera de administrar la configuración básica del servicio Archiver.
2	La pestaña Retención de datos proporciona una manera de ver y editar las recopilaciones y las reglas de retención.
3	La pestaña Archivos permite editar los archivos de configuración del servicio para el Archiver como archivos de texto
4	La pestaña Configuración de servicios de dispositivos proporciona una manera de configurar un servicio Archiver.
5	El panel Servicios agregados proporciona una manera de iniciar y detener la agregación, así como agregar, editar, eliminar y alternar un servicio agregado.
6	El panel Configuración de agregación proporciona ajustes de configuración que afectan diversos aspectos del proceso de agregación.
7	El panel Configuración del sistema proporciona una manera de administrar la

configuración de un servicio Archiver.

General

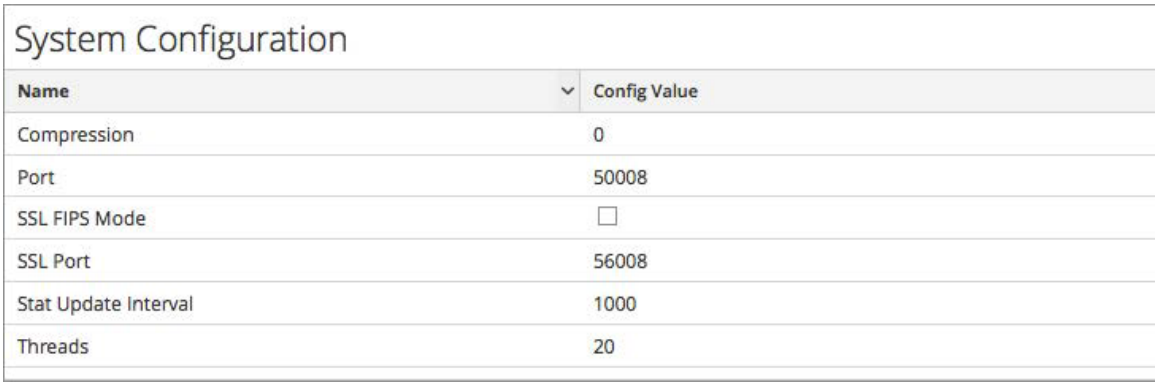
La pestaña General contiene las siguientes secciones:

- Servicios agregados
- Configuración del sistema
- Configuración de agregación

Servicios agregados

La sección Servicios agregados proporciona una manera de iniciar y detener la agregación, así como agregar, editar, eliminar y alternar un servicio agregado.

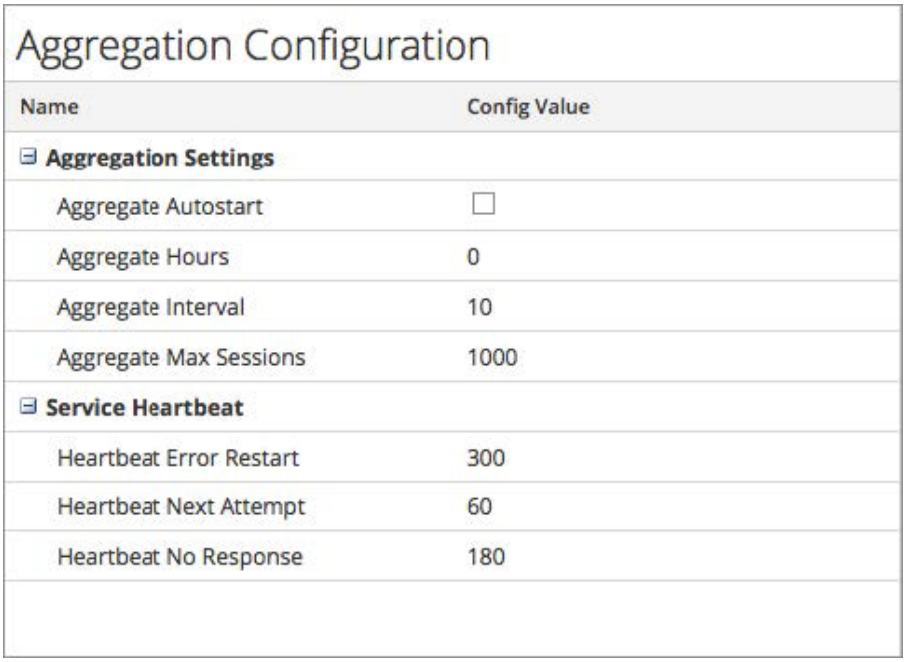
Configuración del sistema



Cuando agrega un servicio Archiver, se aplican valores predeterminados. RSA diseñó los valores predeterminados para adecuarse a la mayoría de los ambientes y recomienda no editarlos dado que esto podría afectar negativamente al rendimiento. La siguiente tabla describe los parámetros de configuración del sistema.

Tarea	Descripción
Compresión	Determina la cantidad mínima de bytes antes de que se comprima un mensaje. Si se configura en cero, los mensajes no se comprimen.
Puerto	Determina el puerto que usa el servicio. **Nota:** Si cambia el número de puerto, asegúrese de reiniciar el servicio.
Modo SSL FIPS	Si esta opción está activada, todos los datos transferidos en la red se cifrarán mediante SSL.
Puerto SSL	Indica el puerto que se usa para cifrar mediante SSL.
Intervalo de actualización de estadísticas	Determina la frecuencia (en milisegundos) con la cual se actualizan los nodos de estadísticas en el sistema.
Subprocesos	Determina la cantidad de hilos de ejecución en el pool de hilos de ejecución para manejar solicitudes entrantes.

Configuración de agregación



La sección Configuración de agregación contiene las siguientes secciones:

- Configuración de agregación
- Latido del servicio

Configuración de agregación

La sección Configuración de agregaciones tiene los siguientes parámetros.

Parámetro	Descripción
Inicio automático agregado	Si está activada, la agregación de datos se reinicia automáticamente después de un reinicio del servicio.
Horas de agregación	Determina la cantidad máxima de horas que se permite iniciar la agregación a un servicio.
Intervalo de agregación	Determina la cantidad mínima de milisegundos antes de solicitar otra ronda de agregación.
Sesiones máximas de agregación	Determina la cantidad de sesiones que se van a agregar a cada ronda.

Latido del servicio

La sección Latido del servicio tiene los siguientes parámetros.

Parámetros	Descripción
Reinicio en error de latido	Determina la cantidad de segundos que se debe esperar después de un error de servicio antes de intentar su reconexión.
Siguiente intento de latido	Determina la cantidad de segundos que se debe esperar antes de intentar la reconexión de un servicio.
Sin respuesta de latido	Determina la cantidad de segundos que se debe esperar antes de dejar offline un servicio que no responde.

Archivos

La pestaña **Archivos** de la vista Configuración de servicios permite editar los archivos de configuración de servicios para el Archiver como archivos de texto. Los archivos disponibles para editar varían según el tipo de servicio que se configura.

Los siguientes archivos son comunes a todos los servicios principales:

- Archivo del índice del servicio
- Archivo de NetWitness
- Archivo del generador de informes de fallas
- Archivo del programador
- Archivo de definiciones de feed

Para obtener más información sobre la pestaña **Archivos**, consulte el tema “Pestaña Archivos” de la *Guía de introducción de hosts y servicios*.