RSA NETWITNESS® SUITE

Guía de configuración de Endpoint Insights

para la versión 11.1

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

julio 2018

Contenido

Descripción general de NetWitness Endpoint Insights

Nota: La información de esta guía se aplica a la versión 11.1 y superior.

RSA NetWitness Endpoint recopila datos de terminales de hosts Windows, Mac o Linux, los que se pueden utilizar para investigar e informar, generar alertas y realizar análisis. Los analistas pueden ejecutar escaneos instantáneos para obtener información valiosa detallada sobre el comportamiento del host en cualquier punto en el tiempo. Además, Endpoint puede recopilar registros de hosts de Windows. NetWitness Endpoint Insights introduce dos tipos de hosts: Endpoint Hybrid y Endpoint Log Hybrid. Solo puede instalar una instancia del tipo de host en su implementación. Esto significa que puede implementar ya sea una instancia de Endpoint Hybrid o una de Endpoint Log Hybrid. No puede cambiar el tipo una vez que se ha implementado.

Endpoint Hybrid: Recopila y administra datos de terminales (hosts). Genera metadatos para investigación, análisis, alertas e informes. Su configuración y administración son similares a las de Log o Packet Decoder. Endpoint Hybrid se ejecuta en un servidor Nginx (en un modo de proxy inverso) que recibe datos desde el agente de Endpoint. En Endpoint Hybrid se ejecutan los siguientes servicios:

- Servidor de Endpoint: Administra los datos que se reciben a través de Nginx, los almacena en la base de datos de Mongo y envía metadatos al Log Decoder.
- Log Decoder: Captura datos desde el servidor de Endpoint y procesa los metadatos.
- Concentrator: Agrega metadatos desde el Log Decoder y los pone a disposición de todos los componentes ascendentes, como Investigate, Event Stream Analysis y Reporting Engine, de manera similar a otra instalación de NetWitness Decoder y Concentrator.

Endpoint Log Hybrid: Captura datos de terminales y datos del registro. Además de los servicios que se ejecutan en el Endpoint Hybrid, un servicio Log Collector se ejecuta en el Endpoint Log Hybrid. Recopila registros de hosts de Windows y todos los demás orígenes de eventos que son compatibles con la recopilación de registros en NetWitness Suite.

En la *Guía de introducción de hosts y servicios*, se proporciona la información que necesita para comprender e instalar todos los servicios de NetWitness Suite.

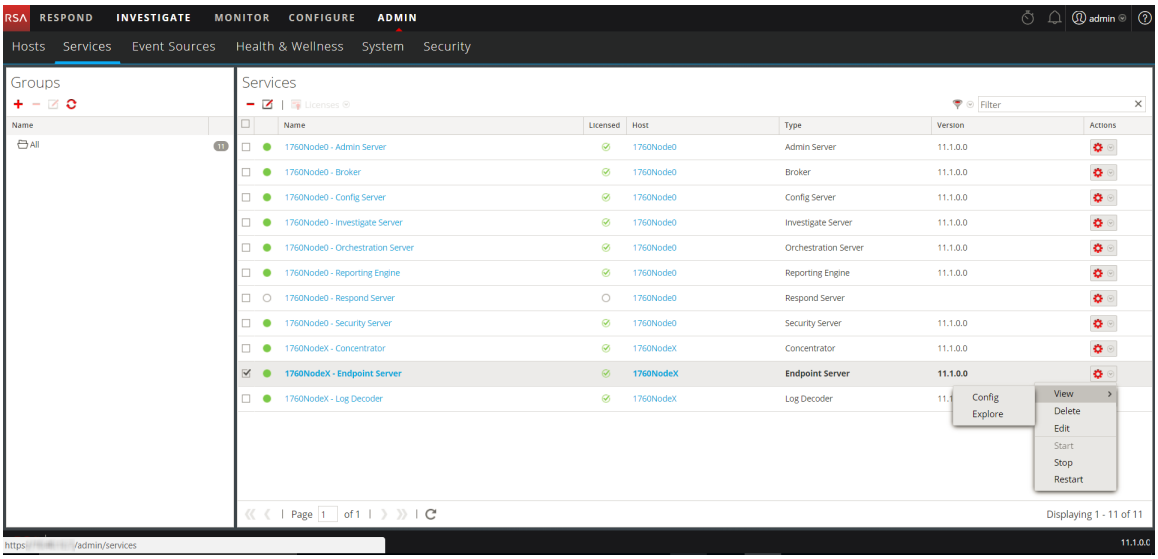
La **configuración básica** implica:

- Instalar agentes en hosts
- Configurar el reenvío de metadatos de terminales, los escaneos programados y las políticas

de retención

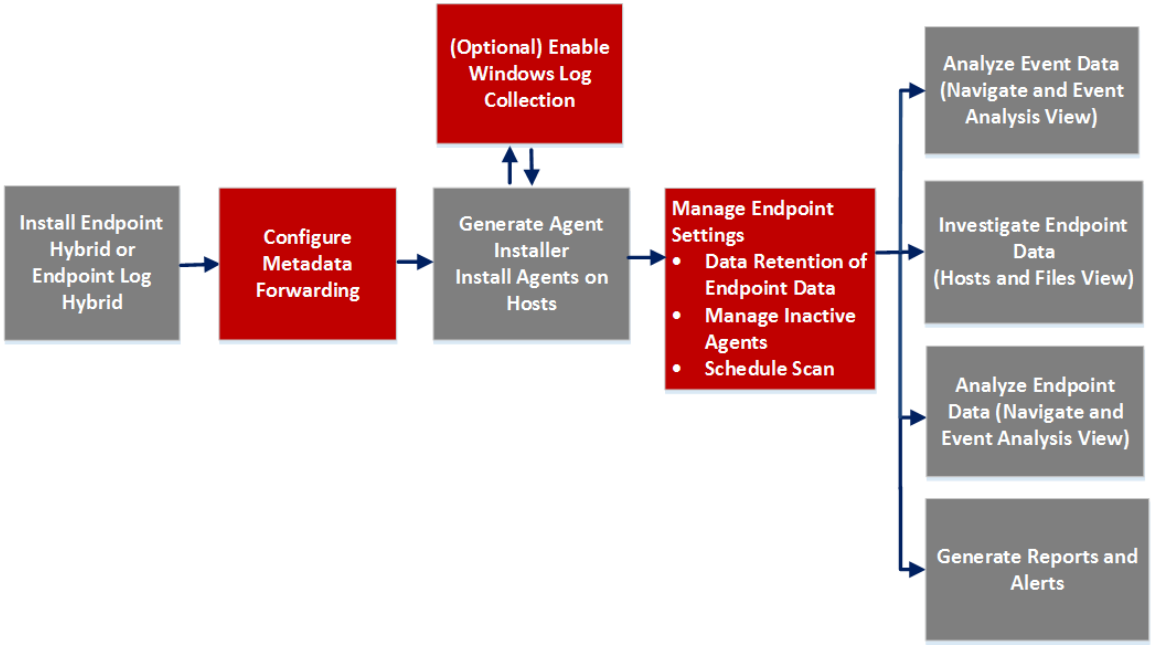
- Definir políticas de estado y condición para monitorear el servidor de Endpoint.

Puede configurar los ajustes necesarios mediante las opciones de la interfaz del usuario de NetWitness Suite en la vista Configuración de Servicios de Administration (**ADMINISTRAR > Servicios > Servidor de Endpoint > Configuración**).



Configuración del servidor de Endpoint

En este tema se proporcionan tareas generales necesarias para configurar el servicio Servidor de Endpoint.



Tareas	Descripción

Instalar Endpoint Hybrid o Endpoint Log Hybrid	Consulte *Guía de instalación de hosts físicos* y *Guía de instalación de hosts virtuales*.
	Nota: Después de instalar Endpoint Hybrid o Endpoint Log Hybrid, registre la dirección IP del host del servidor de Endpoint con el servidor de NW de la siguiente manera:
	1. Acceda mediante el protocolo SSH al servidor de NW.
	2. Vaya al directorio `/opt/rsa/saTools/bin`.
	`cd /opt/rsa/saTools/bin`
	3. Ejecute el script `register-endpoint`, en el cual debe especificar la dirección IP del host de Endpoint.
	`./register-endpoint-ip -v --host-addr <ip-address>`
	El script tarda algunos minutos en actualizar la dirección IP del servidor de Endpoint.

Tareas	Descripción
Configurar el reenvío de metadatos para los agentes de NetWitness Endpoint 11.1	De manera similar a los registros y los paquetes, puede ver los metadatos de terminales en las vistas Navegar y Análisis de eventos. También puede generar informes y alertas para los datos de Endpoint. De forma predeterminada, la opción Metadatos de Endpoint está deshabilitada. Para el reenvío de metadatos, el agente debe estar instalado con la opción Metadatos de Endpoint habilitada.
Instalar agentes en hosts	El instalador de agentes de Endpoint se genera mediante la pestaña Empaquetador en **ADMINISTRAR > Servicios > Configuración > Servidor de Endpoint** desde la interfaz del usuario de NetWitness Suite. El empaquetador es un archivo zip que contiene archivos ejecutables y archivos de configuración para generar el instalador de agentes para los sistemas operativos Linux, Mac y Windows. Puede instalar únicamente una versión del agente en un host. Si está instalada una versión anterior de un agente (por ejemplo, 4.4), desinstale este agente para instalar al agente 11.1. Una vez que se instala el agente, este aparece en la vista **Investigar > Hosts**. De forma predeterminada, los datos de Endpoint se registran por primera vez. Para recopilar datos de Endpoint subsiguientes, debe programar un escaneo o realizar un escaneo ad hoc. Este recupera datos como los controladores, los procesos, los archivos DLL, los archivos (ejecutables), los servicios, las ejecuciones automáticas, la información de seguridad, las configuraciones del sistema y los scripts que se encuentran en el host. Si el agente está configurado para la recopilación de registros, recopila registros de hosts de Windows y los reenvía a un Log Decoder o un Remote Log Collector. Para obtener más información sobre la instalación de agentes de Endpoint, consulte *Guía de instalación de agentes de Endpoint Insights*.
Investigar datos de Endpoint	Puede investigar los datos de Endpoint en las vistas **Investigar > Hosts** e **Investigar > Archivos**. Para obtener más información, consulte la *Guía del usuario de Investigate*.
Configurar un programa de escaneo	Programe un escaneo para que se ejecute de manera diaria o semanal.

Tareas	Descripción
Configurar una política de retención de datos	Defina políticas de retención de datos para almacenar y administrar de manera óptima los datos de Endpoint según la antigüedad de estos o el tamaño del almacenamiento. De forma predeterminada, se conservan 30 días de datos de los agentes.
Administrar agentes inactivos	De forma predeterminada, los agentes (incluidos todos los datos de Endpoint recopilados) que no se han comunicado con el servidor de Endpoint durante 90 días se eliminarán automáticamente.

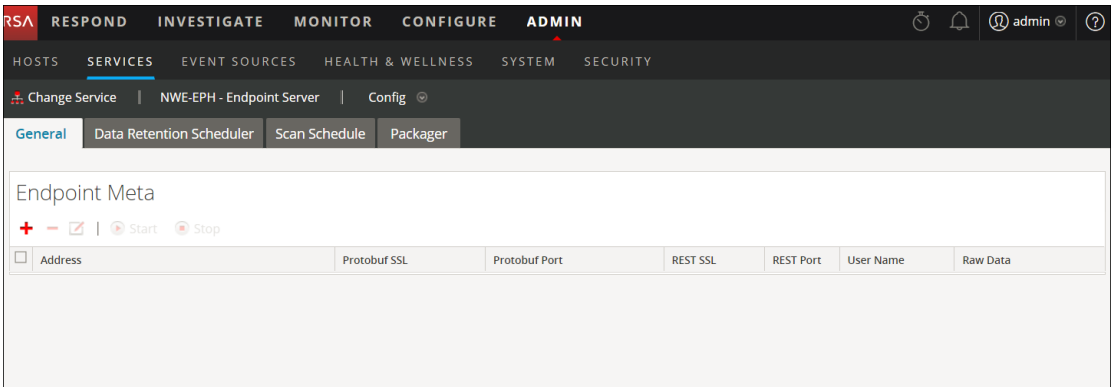
Configurar el reenvío de metadatos para los agentes de NetWitness Endpoint 11.1

Puede ver los metadatos de terminales en NetWitness Suite Investigate (vistas **Navegar** y **Análisis de eventos**), de manera similar a los registros y los paquetes. Debe habilitar el reenvío de metadatos para reenviar las siguientes categorías:

Sistema operativo	Categorías
Windows	Archivo, servicio, archivo DLL, proceso, tarea, ejecución automática y máquina
Linux	Archivo, biblioteca cargada, Systemd, proceso, Cron, Initd y máquina
Mac	Archivo, demonio, proceso, tarea, Dylib, ejecución automática y máquina

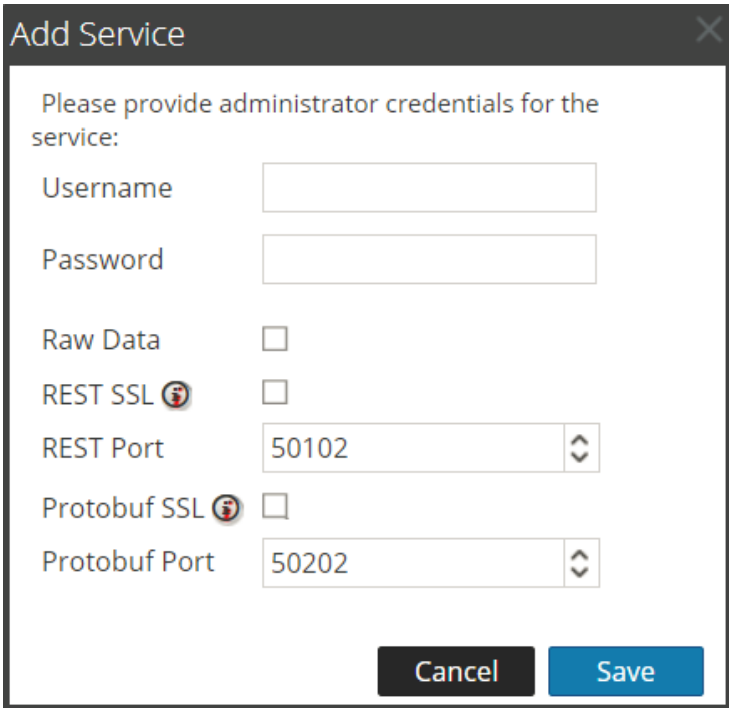
Configuración del reenvío de metadatos

1. Vaya a **ADMINISTRAR** > **Servicios**.
2. En la vista Servicios, seleccione el servicio **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **General**.



5. Haga clic en + en la barra de herramientas.
   Se muestra el cuadro de diálogo Servicios disponibles.

6. Seleccione el servicio Log Decoder y haga clic en **Aceptar**.
   Se muestra el cuadro de diálogo Agregar servicio. Puede agregar únicamente un servicio Log Decoder.



7. Ingrese las credenciales de administrador para la autenticación.
8. (Opcional) Si habilita Datos crudos, se envía un breve resumen de la sesión junto con los metadatos.
9. (Opcional) Si habilitó SSL en el puerto REST en el Log Decoder, seleccione la opción **SSL REST**. De forma predeterminada, el puerto REST cuando no se utiliza SSL es 50202 y cuando se utiliza, 56202.
10. Seleccione la opción **SSL Protobuf** para habilitar SSL en Protobuf. De forma predeterminada, el puerto Protobuf es 50202.
11. Haga clic en **Guardar**.

Después de configurar el reenvío de metadatos, asegúrese de realizar lo siguiente:

- Iniciar la captura en el Log Decoder
- Iniciar la agregación en el Concentrator
- Agregar el Log Decoder como un servicio en el **Concentrator**

Inicio del reenvío de metadatos al Log Decoder

1. En la vista de configuración Metadatos de Endpoint, seleccione el servicio.
2. Haga clic en Start

   El servidor de Endpoint comienza a reenviar los metadatos al Log Decoder.

Detención del reenvío de metadatos al Log Decoder

1. En la vista de configuración Metadatos de Endpoint, seleccione el servicio.
2. Haga clic en Stop.

   El servidor de Endpoint deja de reenviar los metadatos al Log Decoder.

Eliminación del reenvío de metadatos

Nota: Asegúrese de detener el servicio antes de quitar el reenvío de metadatos.

1. En la vista de configuración Metadatos de Endpoint, seleccione el servicio.
2. Haga clic en .
3. Haga clic en **Aplicar**.

Mapeos de metadatos de terminales

Puede ver los mapeos de metadatos predeterminados o modificar los mapeos de metadatos de los terminales.

Esquema JSON para mapeos de metadatos

Todos los mapeos de metadatos se configuran mediante el esquema JSON. El siguiente es un ejemplo del esquema JSON:

```
{
"metaKeyPairs" : [
     {
     "metaKeyPairsCategory" : "",
     "keyPairs" : [
          {
          "endpointJpath" : "",
```

```
            "metaName" : "",
            "type" : "",
            "enabled" : true
            },
            {
            "endpointJpath" : "",
            "metaName" : "",
            "type" : "",
            "enabled" : true
            }
        ]
        }
]
}
```

Las siguientes API se usan para ver o modificar los mapeos de metadatos:

- `get-default`: Devuelve las configuraciones predeterminadas de los mapeos de metadatos de terminales.
- `get-custom`: Devuelve las configuraciones personalizadas de los mapeos de metadatos de terminales.
- `set-custom`: Puede personalizar los mapeos de metadatos de terminales.

Visualización de los mapeos de metadatos

Para ver los mapeos de metadatos de terminales:

1. En el servidor de NW, ejecute el comando `nw-shell` desde la línea de comandos.
2. Ejecute el comando `login` e ingrese las credenciales.
3. Conéctese al servidor de Endpoint mediante el siguiente comando:
   `connect --host <IP address> --port <number>`

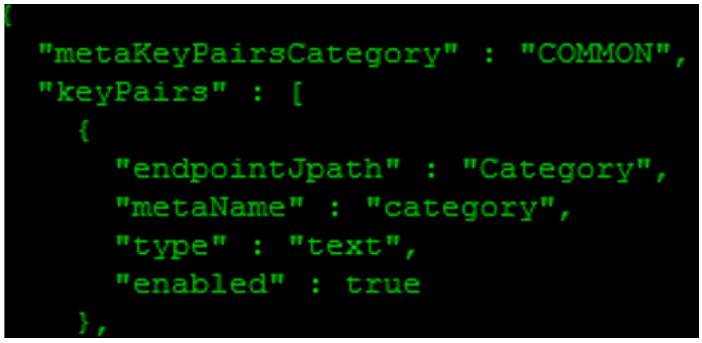
   Nota: El puerto predeterminado es 7050.
4. Ejecute los siguientes comandos:
   ```
   cd endpoint/meta
   cd get-default
   invoke
   ```

En la siguiente pantalla se muestran los mapeos de metadatos predeterminados:

Para deshabilitar un mapeo de metadatos predeterminado:

Ingrese el mismo valor de endpointJpath y configure el parámetro enabled en `false`.

Por ejemplo, si endpointJpath es `Category` y el parámetro enabled es `true`, ingrese el mismo valor de endpointJpath y configure el parámetro enabled en `false`.



Nota: No modifique metaKeyPairsCategory en el esquema; “COMMON”, “COMMON_MACHINE”, “COMMON_MACHINE_FOR_EVENTS”.

Para cambiar el nombre o el tipo de los metadatos:

Ingrese el mismo valor de endpointJpath y especifique valores para metaName y type.

Nota: El valor de metaName debe existir en table-map.xml del Log Decoder, en index-concentrator.xml o en el archivo index-concentrator-custom.xml del Concentrator para que el valor de metaName aparezca en la vista Investigar.

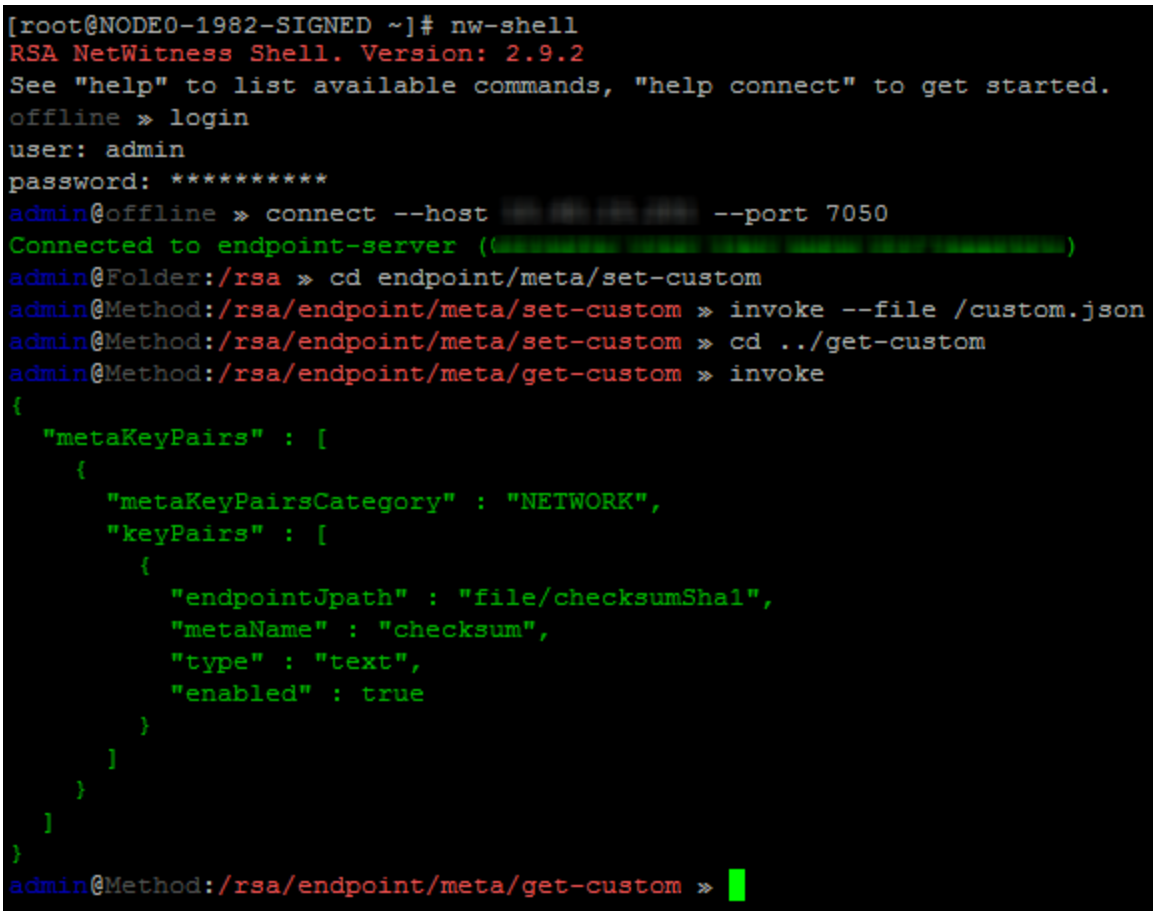
Adición o modificación de mapeos de metadatos

Para agregar o modificar los mapeos de metadatos, ejecute la API `set-custom`. La configuración de metaKeyPairs que se proporciona en el archivo JSON debe coincidir con el esquema JSON de la configuración predeterminada que se recibió a través de la API `get-default`.

1. En el servidor de NW, ejecute el comando `nw-shell` desde la línea de comandos.
2. Ejecute el comando `login` e ingrese las credenciales.
3. Conéctese al servidor de Endpoint mediante los siguientes comandos:
   `connect --host <IP address> --port <number>`

   Nota: El número de puerto predeterminado es 7050)
4. Ejecute los siguientes comandos:
   ```
   cd endpoint/meta
   cd set-custom
   invoke –file <json file>
   ```

Puede agregar nuevos valores de metaKeys con la adición de entradas en el archivo que se cargarán mediante la API `set-custom`. En el siguiente ejemplo se muestra cómo agregar un nuevo mapeo de metadatos:



Visualización de los mapeos de metadatos personalizados

Para ver los mapeos de metadatos personalizados, ejecute la API `get-custom`.

Nota: La API `get-custom` devolverá valores únicamente si los mapeos de metadatos se modifican mediante la API `set-custom`.

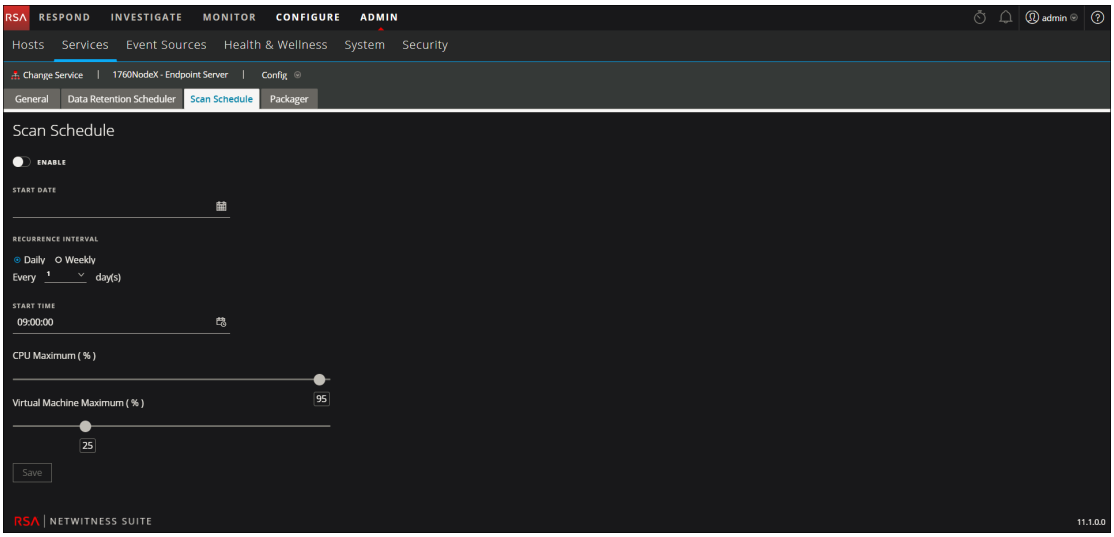
Configurar un programa de escaneo

Puede programar un escaneo para que se ejecute de manera diaria o semanal.

Nota: Se puede configurar únicamente un programa, el cual se aplica a todos los agentes.

Para configurar un programa de escaneo:

1. Vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione el servicio **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **Programa de escaneo**.



5. Haga clic en el switch de alternancia **Habilitar** para configurar el escaneo.
6. Seleccione la **Fecha de inicio**.
7. Seleccione el intervalo de recurrencia: Diariamente o Semanalmente.

   Nota: Los valores ingresados son específicos de la zona horaria del agente.

8. Para un escaneo diario:
   - Seleccione el intervalo de recurrencia **Diariamente**.
   - Especifique la frecuencia de escaneo en días.

9. Para un escaneo semanal:
   - Seleccione el intervalo de recurrencia **Semanalmente**.
   - Especifique la frecuencia de escaneo en semanas.
   - Seleccione el día de la semana.
10. Ingrese la hora de inicio del escaneo.
11. Configure el valor Máximo de CPU mediante el control deslizante. Esto garantiza el límite de CPU del agente de NetWitness Endpoint. Si los agentes se ejecutan en máquinas virtuales, configure el valor Máximo de máquinas virtuales mediante el control deslizante.
12. Haga clic en **Guardar** para guardar la configuración.

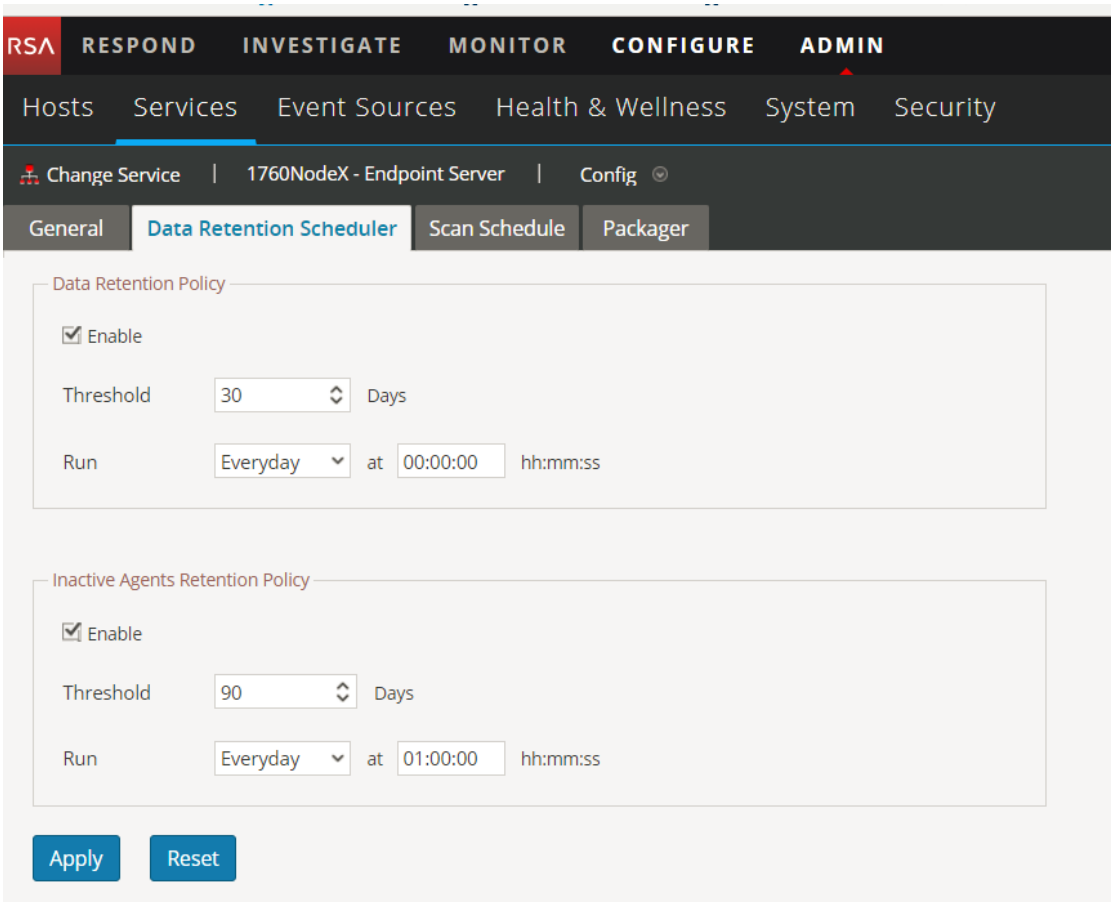
Nota: Si un agente no puede realizar el escaneo en el momento programado debido a que la máquina está apagada o a que el servicio del agente está detenido, el escaneo siguiente se basa en la diferencia horaria entre la hora actual y la hora del siguiente escaneo programado. Por ejemplo, si hay un escaneo programado para ejecutarse todos los miércoles a las 18:00 h y el servicio del agente se detuvo antes de la hora de inicio del escaneo, y si el servicio está activo el jueves a las 10:00 h, el agente esperará hasta que el sistema esté completamente en funcionamiento y ejecutará un escaneo de inmediato.
Pero, si el servicio está activo el siguiente lunes a las 13:00 h, el escaneo se ejecutará el siguiente miércoles a las 18:00 h.

Configurar una política de retención de datos

Un administrador puede configurar las políticas de retención para conservar los datos de Endpoint según la antigüedad o el tamaño del almacenamiento. De forma predeterminada, las políticas de retención basadas en días y en tamaño están habilitadas.

Para cambiar la configuración de la retención basada en antigüedad:

1. Vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione el servicio **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **Calendarizador de retención de datos**.

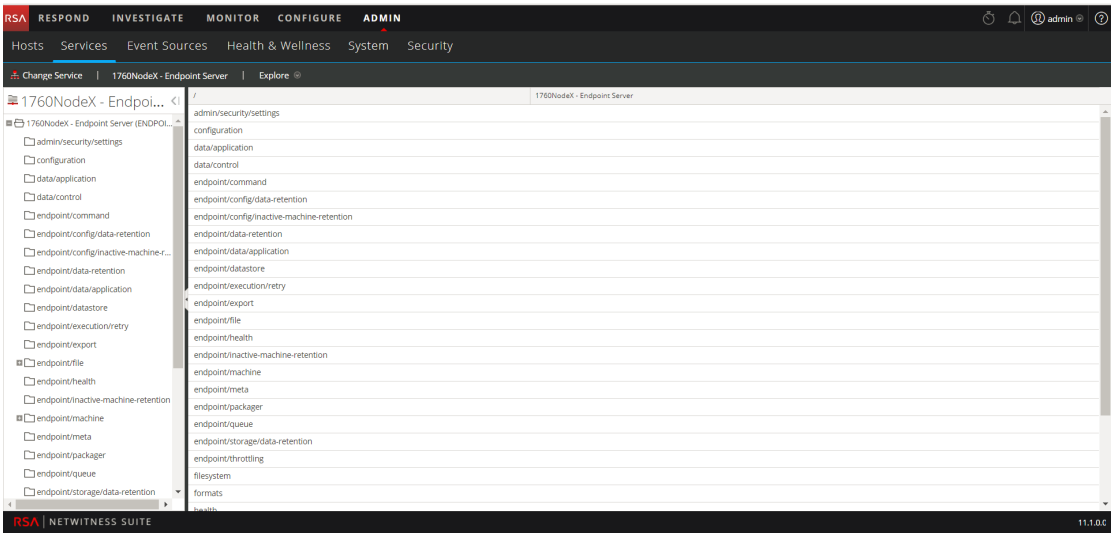


5. De forma predeterminada, en el panel **Política de retención de datos**, el **Umbral** está configurado en 30 días y **Ejecutar**, en Todos los días. Esto significa que solo se retienen 30 días de datos de Endpoint y que los datos más antiguos se eliminan de la base de datos.
6. Haga clic en **Aplicar**.

Para cambiar la configuración de la retención basada en tamaño:

De forma predeterminada, para la retención basada en tamaño, el valor `rollover-after` está configurado en 80 y `rollover-chunk-size`, en 10. Esto significa que, cuando el tamaño del almacenamiento supera el 80 % del espacio asignado a la partición del disco, el 10 % de los datos más antiguos de Endpoint se elimina de la base de datos. Sin embargo, puede cambiar estos valores de la siguiente manera:

1. En el menú principal, vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione el servicio **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Explorar**. Se muestra la vista Explorar:



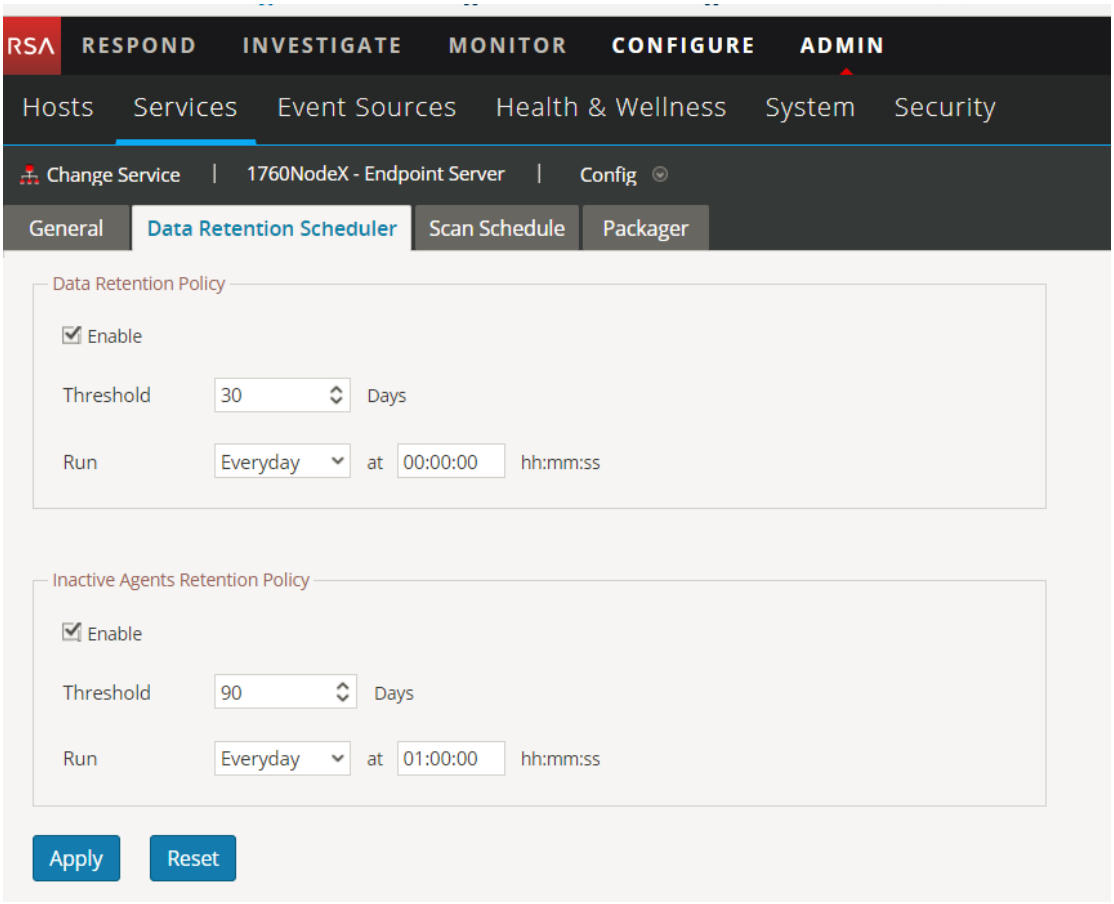
4. En el panel izquierdo, seleccione **endpoint/config/data-retention**.
5. Edite las configuraciones en función de sus requisitos.

Administrar agentes inactivos

Un administrador puede configurar la política de retención de los agentes inactivos para eliminar del servidor de Endpoint los datos de los agentes que están inactivos. Tras la eliminación, el servidor de Endpoint deja de recopilar datos de estos agentes. De manera predeterminada, esta opción está activada.

Para configurar la política de retención de agentes inactivos:

1. Vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **Calendarizador de retención de datos**.



5. De forma predeterminada, en el panel **Política de retención de agentes inactivos**, el **Umbral** está configurado en 90 días y **Ejecutar**, en Todos los días. Esto significa que los datos de los agentes que no se han comunicado con el servidor de Endpoint durante 90 días

se eliminan de la base de datos.

6. Haga clic en **Aplicar**.

Nota: La política de retención de agentes inactivos no se aplica a los agentes de NetWitness Endpoint 4.4.0.2 o superior.

Integración de NetWitness Endpoint 4.4.0.2 o superior con NetWitness Endpoint 11.1

Puede configurar los metadatos de terminales para NetWitness Endpoint 4.4.0.2 de una de las siguientes maneras:

- **(Opción 1) Integrar el servidor de la consola de NetWitness Endpoint 4.4.0.2 en un Endpoint Hybrid o un Endpoint Log Hybrid**: Los datos de los agentes de NetWitness Endpoint 4.4.0.2 o superior estarán disponibles en las vistas **Investigar > Hosts** y **Archivos**, y usted puede ver los metadatos de terminales en las vistas **Investigar > Navegar** y **Análisis de eventos**. Para esta opción, asegúrese de que el servidor de Endpoint esté configurado para el reenvío de metadatos.
- **(Opción 2) Integrar el servicio Meta Integrator en NetWitness Endpoint 4.4.0.2 directamente en un Log Decoder**: Puede ver los metadatos de terminales en las vistas **Investigar > Navegar** y **Análisis de eventos**. Los datos de agentes de NetWitness Endpoint 4.4 no estarán disponibles en las vistas **Investigar > Hosts** y **Archivos**.

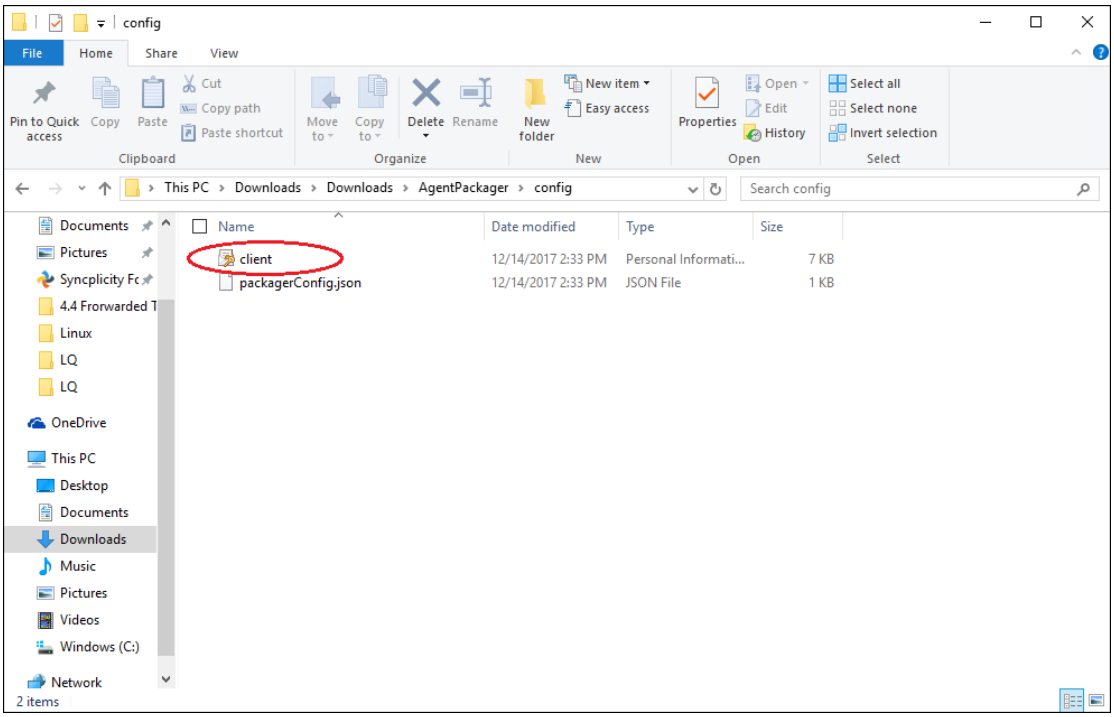
Además de las categorías mencionadas para los agentes de NetWitness Endpoint 11.1, las siguientes categorías también se reenvían para los agentes de NetWitness Endpoint 4.4.0.2 o superior: eventos de archivos, eventos de red, eventos del registro y eventos de procesos.

Configuración del servidor de la consola de NetWitness Endpoint 4.4.0.2

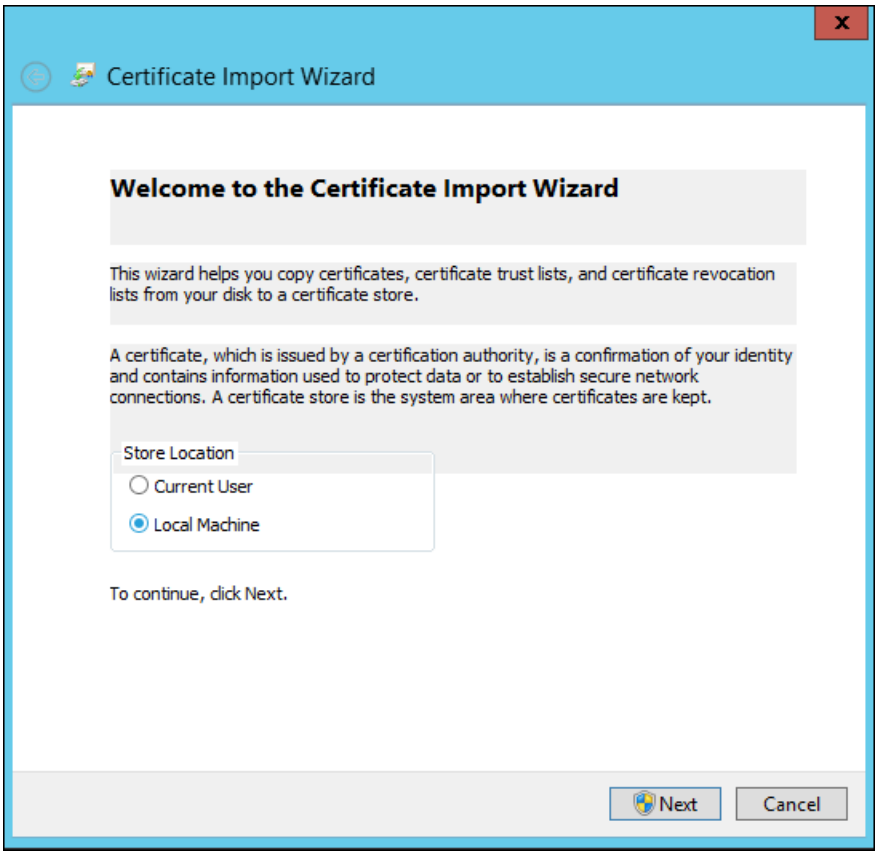
Configuración del certificado de cliente en el servidor de la consola de NetWitness Endpoint 4.4.0.2 (para la opción 1)

El servidor de la consola de NetWitness Endpoint 4.4.0.2 debe usar el mismo certificado de cliente que usan los agentes de NetWitness Endpoint 11.1 para reenviar los metadatos al servidor de Endpoint.

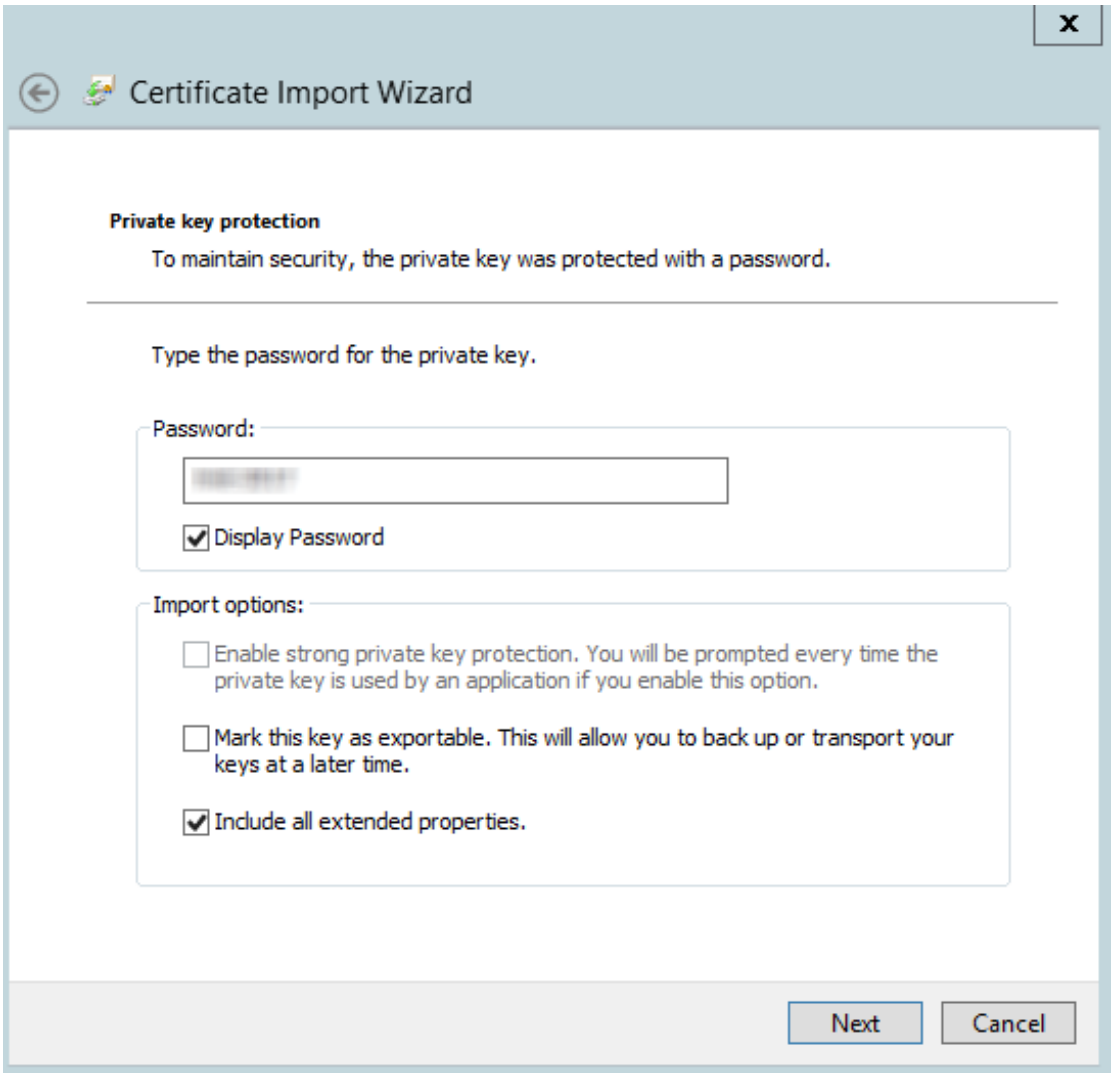
1. Descargue el empaquetador de agentes. Para obtener más información, consulte la *Guía de instalación de agentes de Endpoint Insights*.
2. Extraiga **AgentPackager.zip** y, desde la carpeta Config, obtenga el certificado de cliente.
3. Copie el certificado de cliente en el servidor de la consola de NetWitness Endpoint 4.4.



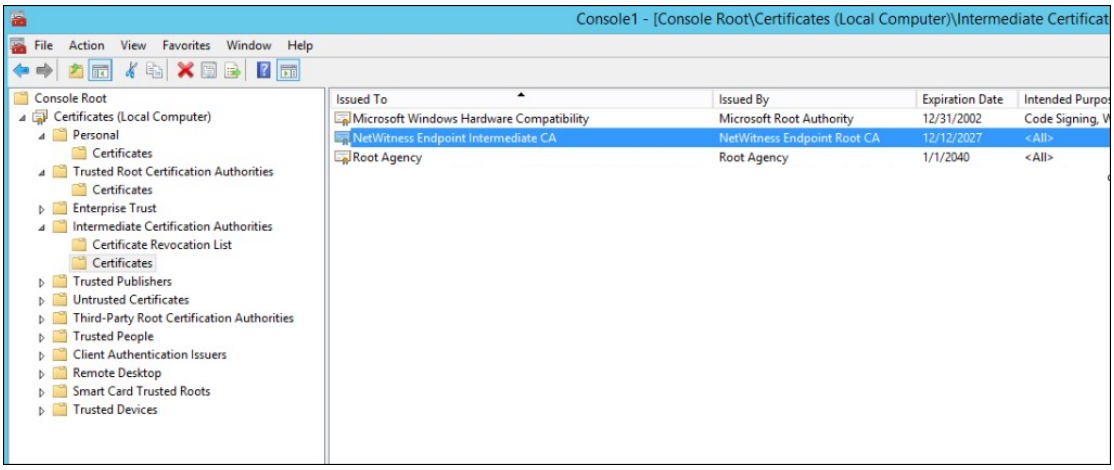
4. Haga doble clic en el archivo **client**.
   Se muestra el cuadro de diálogo **Asistente de importación de certificados**.
5. Seleccione la ubicación del almacén **Máquina local** y haga clic en **Siguiente**.



6. Navegue al archivo que desea importar y haga clic en **Siguiente**.
7. Ingrese la misma contraseña que se usa al generar el empaquetador de agentes.



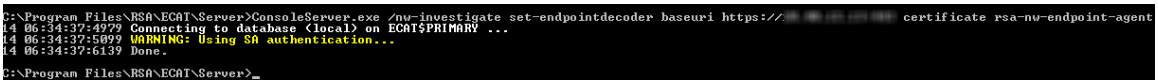
8. Haga clic en **Siguiente** y en **Finalizar**.
   El certificado se enumera en **Personal**, **Autoridades de certificación intermedias** > **Certificado** y **Autoridades de certificación de raíz de confianza** en el servidor de la consola.



Habilitación del reenvío de metadatos en NetWitness Endpoint 4.4.0.2 (para la opción 1)

Para habilitar el reenvío de metadatos para los agentes de NetWitness Endpoint 4.4.0.2 seleccionados, ejecute el siguiente comando:

`ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri <ENDPOINT HOST> certificate <CERTIFICATE DISPLAY NAME>.`



Por ejemplo, `ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://<Ip Address>:443 certificate rsa-nw-endpoint-agent`

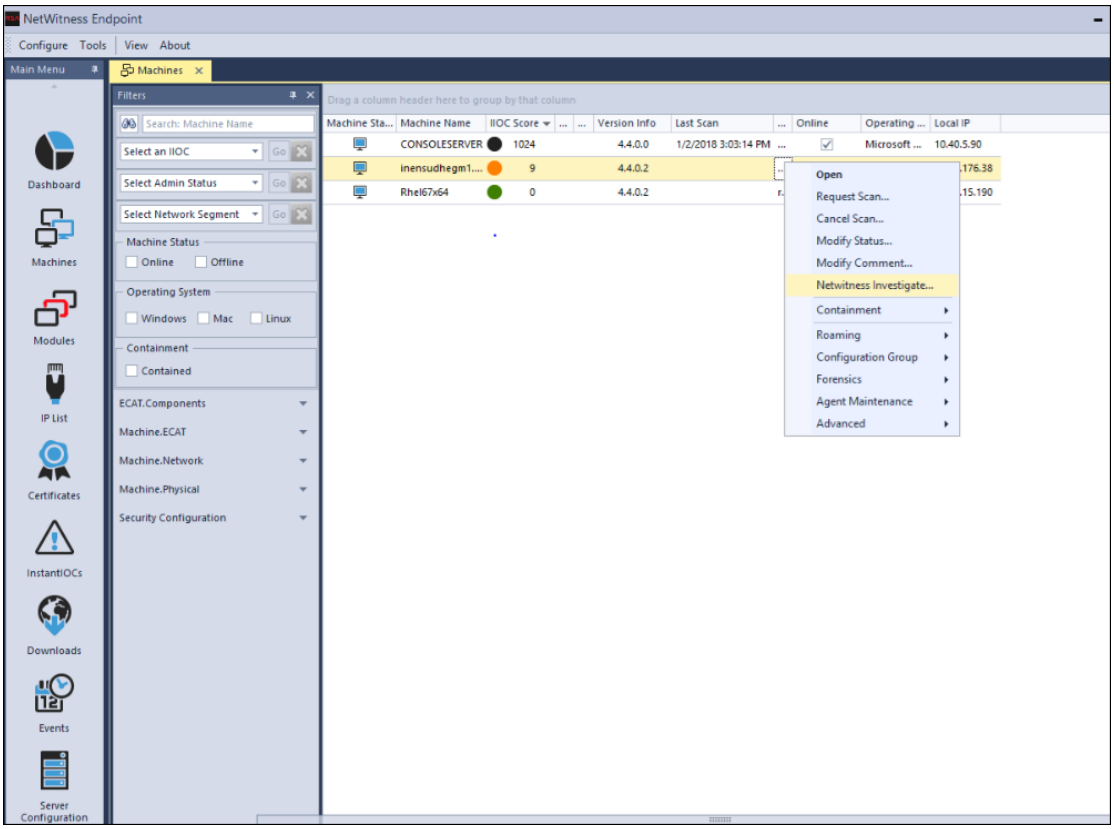
Habilitar el reenvío de metadatos de NetWitness Endpoint 4.4.0.2 al Log Decoder (para la opción 2)

Para habilitar el servicio Metadata Integrator para los agentes de NetWitness Endpoint 4.4.0.2 seleccionados, ejecute el siguiente comando:
`ConsoleServer.exe /nw-investigate enable.`

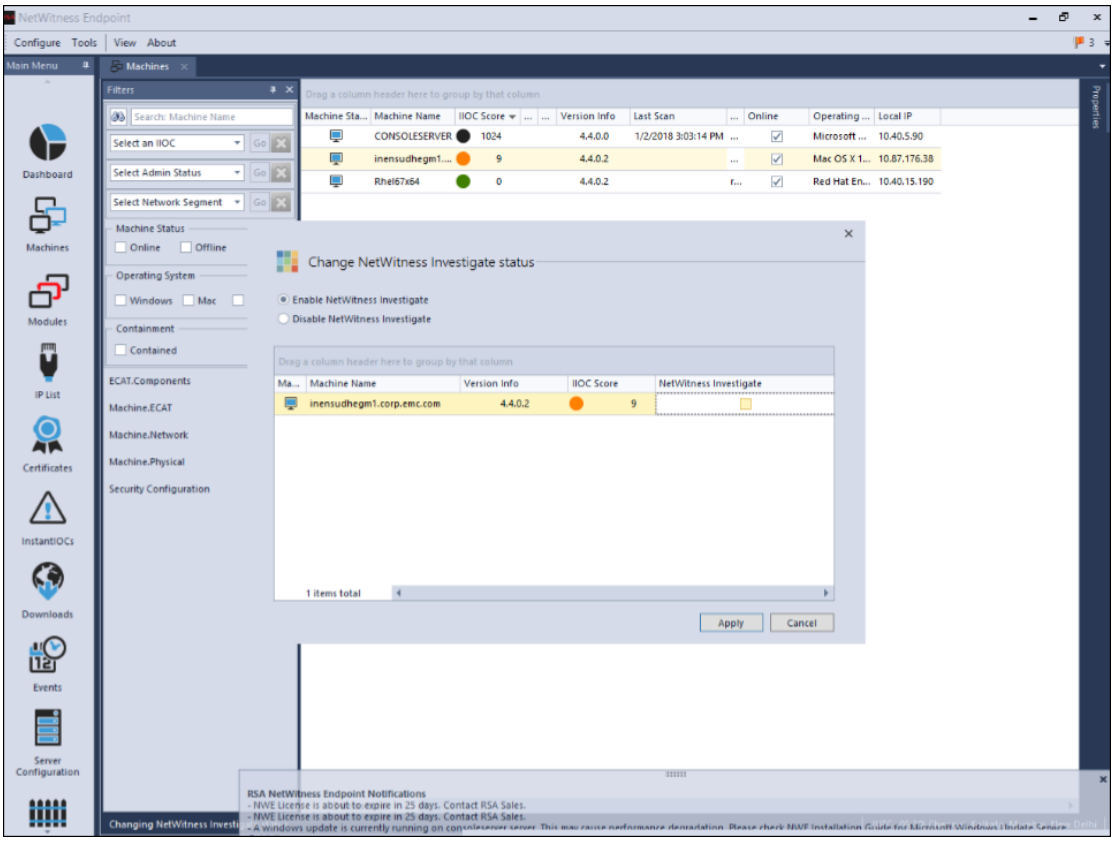
Habilitación de máquinas para reenviar metadatos desde NetWitness Endpoint 4.4.0.2 al servidor de NetWitness Endpoint (para las opciones 1 y 2)

Después de habilitar el reenvío de metadatos mediante cualquiera de las opciones anteriores, realice lo siguiente para habilitar las máquinas de modo que puedan reenviar metadatos.

1. Abra la interfaz del usuario de NetWitness Endpoint 4.4.0.2.
2. Haga clic en **Máquinas** en el panel izquierdo. Se muestra la lista de máquinas disponibles.



3. Seleccione las máquinas para las cuales desea reenviar metadatos al servidor de NetWitness Endpoint.
4. Haga clic con el botón secundario y seleccione la opción **NetWitness Investigate**.
   Se muestra el cuadro de diálogo Cambiar el estado de NetWitness Investigate.



5. Seleccione la opción **Habilitar NetWitness Investigate**.
6. Haga clic en **Aplicar**.
7. Para verificar si la opción **Habilitar NetWitness Investigate** está activada, repita el paso 4.

Referencias de Endpoint

El objetivo de esta sección es ayudarlo a comprender el propósito de la vista Configuración de servicios para el servidor de Endpoint. Para cada configuración, hay una breve introducción y una tabla Qué desea hacer que incluye vínculos a procedimientos relacionados. Además, incluyen secciones de flujos de trabajo y vistas rápidas para resaltar las funciones importantes de la interfaz del usuario.

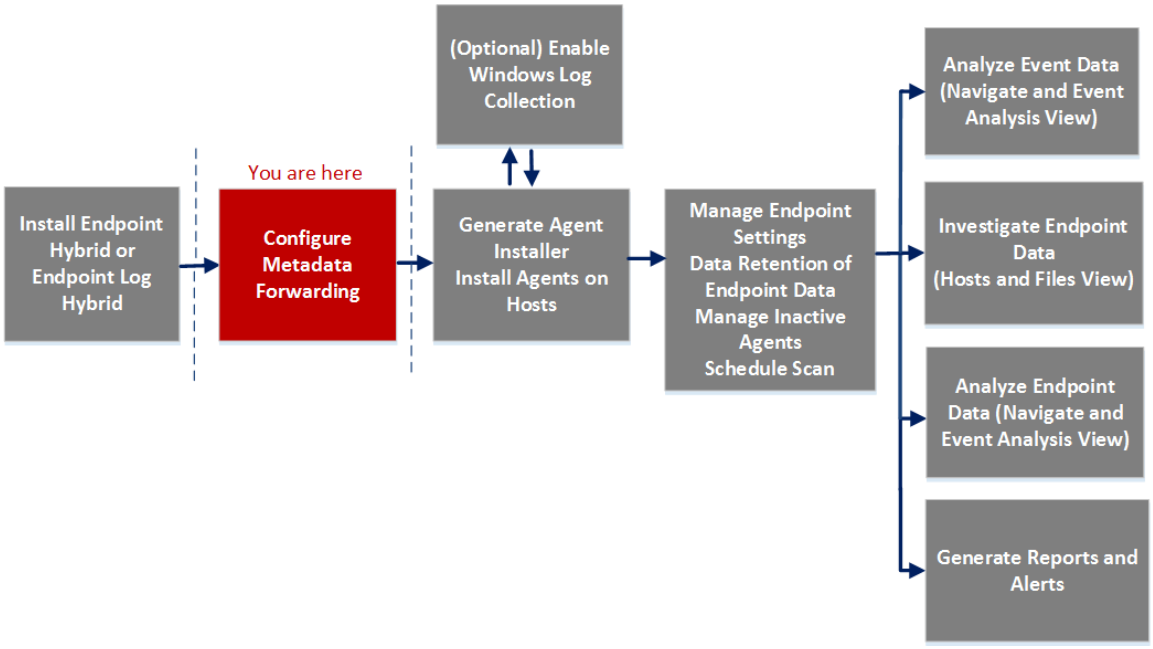
Puede ver los nodos de servicios completos en forma de árbol en la vista Explorar de servicios. Para obtener más información, consulte el tema “Vista Explorar de servicios” de la *Guía de introducción de hosts y servicios*.

Pestaña General

En la pestaña **General**, puede configurar el reenvío de metadatos de terminales. Para acceder a esta vista:

1. Vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **General**.

Flujo de trabajo



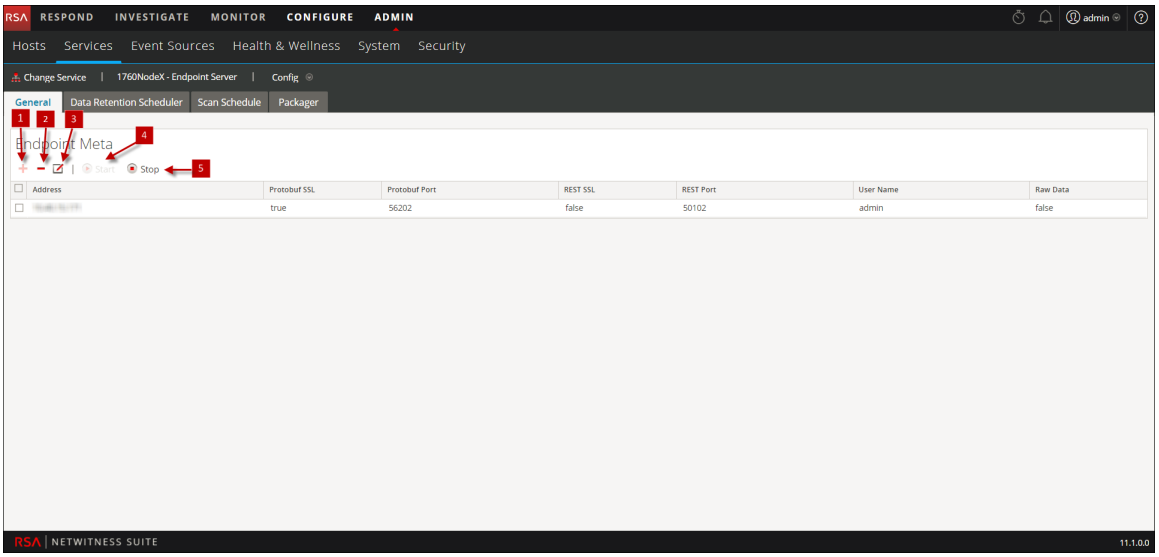
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar el reenvío de metadatos de terminales para los agentes de NetWitness Endpoint 11.1	Configuración del reenvío de metadatos
Administrador	Configurar el reenvío de metadatos de terminales para los agentes de NetWitness Endpoint 4.4.0.2 o superior	Integración de NetWitness Endpoint 4.4.0.2 o superior con NetWitness Endpoint 11.1

*Puede realizar esta tarea en la vista actual.

Vista rápida

En la siguiente figura se muestra un ejemplo de la pestaña General.



1. Haga clic en + para ver el cuadro de diálogo **Servicios disponibles**.
2. Haga clic en − para eliminar el servicio agregado.

3. Haga clic en  para editar la información del servicio agregado.
4. Haga clic en  para iniciar el reenvío de metadatos de terminales.
5. Haga clic en  para detener el reenvío de metadatos de terminales.

En la siguiente tabla se describen los campos de la pestaña General.

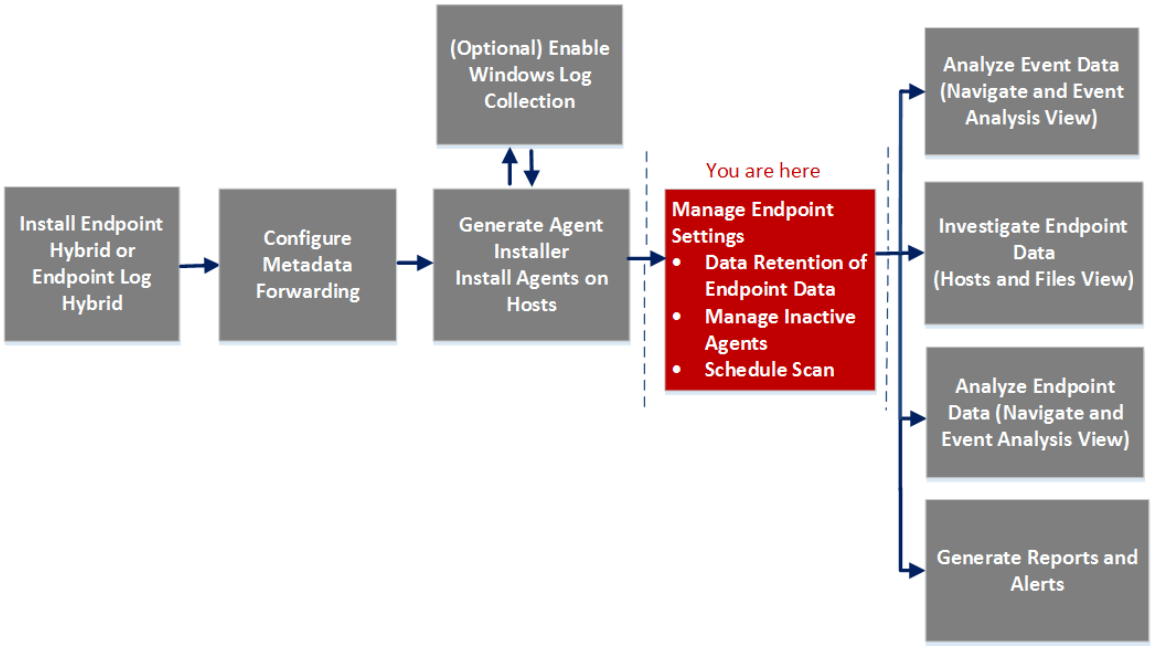
Campo	Descripción
Dirección	Muestra la dirección IP del Log Decoder.
SSL Protobuf	Indica si SSL está activado en Protobuf. De manera predeterminada, esta opción está deshabilitada.
Puerto Protobuf	Muestra el puerto que se usa para Protobuf. De manera predeterminada, el puerto es 50202.
SSL REST	Indica si SSL está activado en el puerto REST en el Log Decoder. De manera predeterminada, esta opción está deshabilitada.
Puerto REST	Muestra el puerto que se usa para la comunicación de REST. El valor predeterminado es 50202 (para protocolos distintos de SSL) y 56202 (para SSL).
Nombre de usuario	Muestra el nombre de usuario.
Datos crudos	Envía un breve resumen de la sesión junto con los metadatos, si están activados. De manera predeterminada, esta opción está deshabilitada.

Pestaña Calendarizador de retención de datos

En la pestaña **Calendarizador de retención de datos**, puede configurar la retención de datos y las políticas de agentes inactivos. Para acceder a esta vista:

1. Vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **Calendarizador de retención de datos**.

Flujo de trabajo



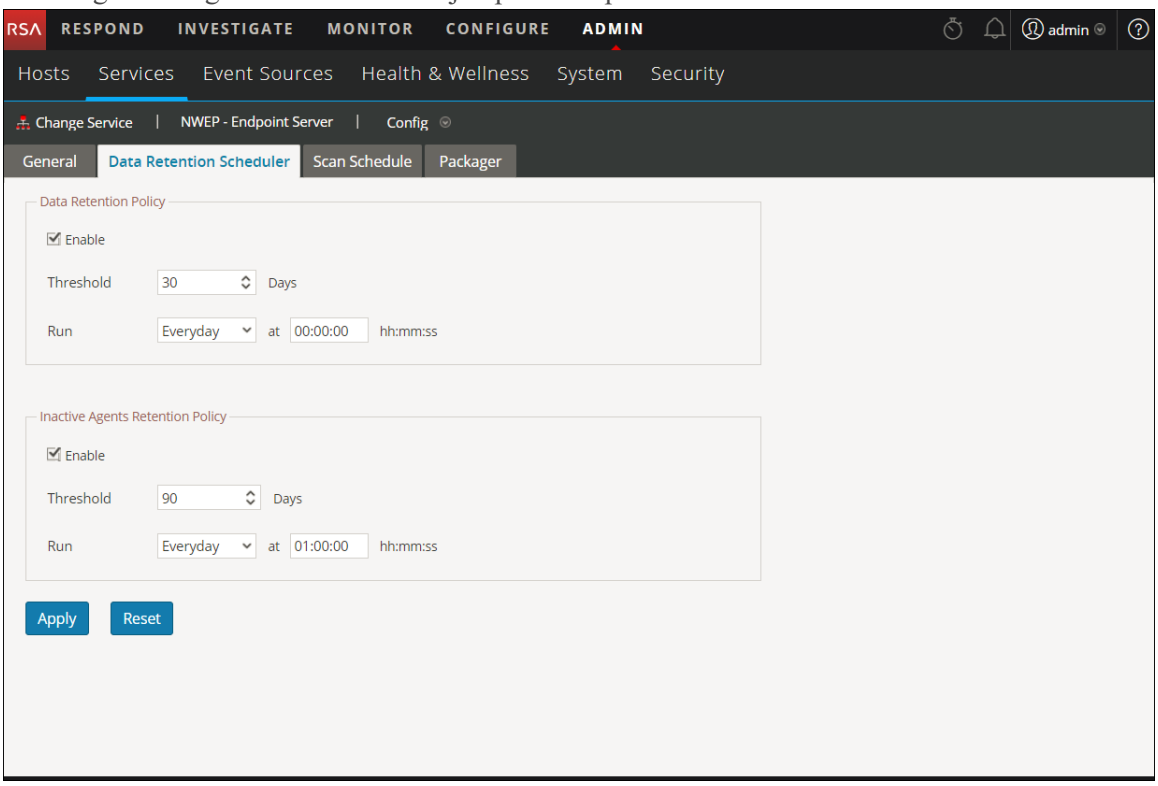
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar una política de retención de datos*	Configurar una política de retención de datos
Administrador	Configurar una política de agentes inactivos*	Administrar agentes inactivos

*Puede realizar esta tarea en la vista actual.

Vista rápida

En la siguiente figura se muestra un ejemplo de la pestaña Calendarizador de retención de datos.



Funciones

En la siguiente tabla se indican los campos para la política de retención de datos.

Campo	Descripción
Habilitar	Permite la configuración para la política de retención de datos. De manera predeterminada, esta opción está activada.
Umbral	Muestra la cantidad de días que se conservan los datos de Endpoint en la base de datos. De manera predeterminada, el umbral está configurado en 30 días. Los datos que tienen más de 30 días se eliminan de la base de datos.

Campo	Descripción
Ejecutar	Muestra el programa para ejecutar el trabajo de retención de datos. De manera predeterminada, la comprobación de la base de datos se realiza cada día a las 00:00:00 h. Puede seleccionar la frecuencia en la lista desplegable (Todos los días, Días de semana, Fines de semana o Personalizado, opción que permite seleccionar uno o más días de la semana específicos) y la hora a la que se ejecutará el trabajo.
Aplicar	Sobrescribe cualquier programa anterior para este servicio y aplica el nuevo programa de inmediato.
Restablecer	Restablece el programa a la configuración predeterminada.

En la siguiente tabla se indican los campos para la política de retención de agentes inactivos.

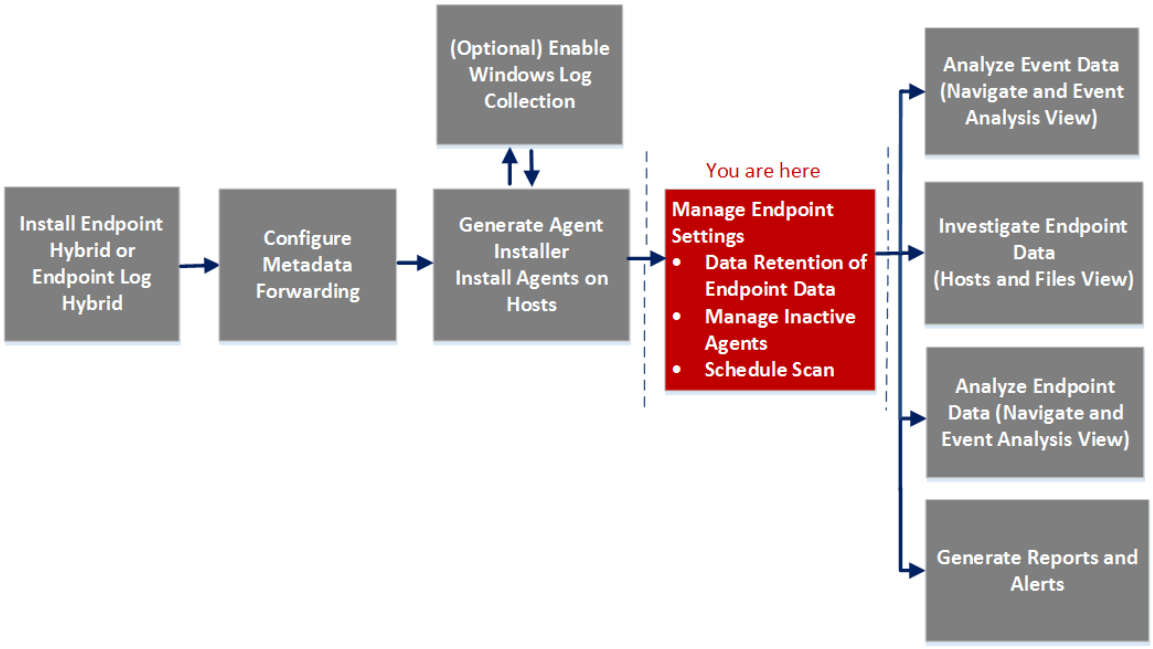
Campos	Descripción
Habilitar	Permite la configuración de la política de agentes inactivos. De manera predeterminada, esta opción está activada.
Umbral	Muestra la cantidad de días que se conservan los agentes inactivos en el Servidor de Endpoint. De manera predeterminada, el valor del umbral es 90 días.
Ejecutar	Muestra el programa para ejecutar el trabajo de retención de agentes inactivos. De manera predeterminada, la comprobación de la base de datos se realiza cada día a las 00:00:00 h. Puede seleccionar la frecuencia en la lista desplegable (Todos los días, Días de semana, Fines de semana o Personalizado, opción que permite seleccionar uno o más días de la semana específicos) y la hora a la que se ejecutará el trabajo.
Aplicar	Sobrescribe cualquier programa anterior para este servicio y aplica la nueva configuración de inmediato.
Restablecer	Restablece el programa a la configuración predeterminada.

Pestaña Programa de escaneo

En la pestaña **Programa de escaneo**, puede configurar los escaneos programados. Para acceder a esta vista:

1. Vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **Programa de escaneo**.

Flujo de trabajo



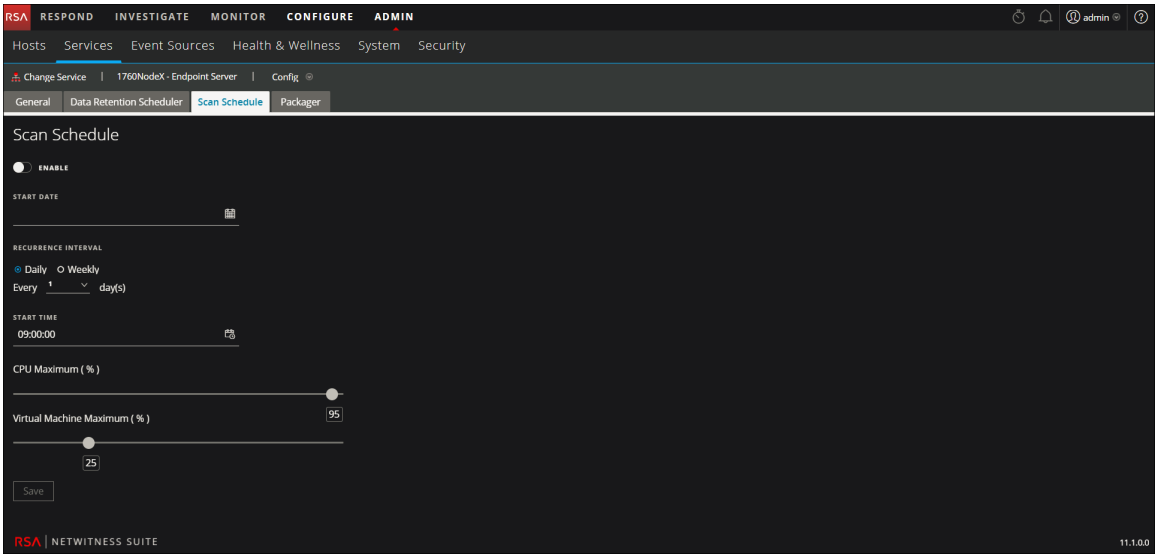
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar un programa de escaneo*	Configurar un programa de escaneo

*Puede realizar esta tarea en la vista actual.

Vista rápida

En la siguiente figura se muestra un ejemplo de la pestaña Programa de escaneo.



En la siguiente tabla se describen los campos de la pestaña Programa de escaneo. Los valores ingresados son específicos de la zona horaria del agente.

Campo	Descripción
Habilitar	Seleccione esta opción para configurar el escaneo. De manera predeterminada, esta opción está deshabilitada.
Fecha de inicio	Especifique la fecha en que se iniciará el escaneo.
Intervalo de recurrencia	Seleccione el valor Diariamente o Semanalmente como el intervalo de recurrencia y configure la frecuencia en días.
Hora de inicio	Especifique la hora en que se iniciará el escaneo.
Máximo de CPU	Configure el valor mediante el control deslizante. Esto garantiza el límite de CPU del agente de NetWitness Endpoint.
Máximo de VM	Configure el valor mediante el control deslizante. **Nota:** Use esta opción si los agentes se ejecutan en máquinas virtuales. Esto se aplica únicamente a los agentes de Windows.

Pestaña Empaquetador

En la pestaña **Empaquetador**, puede generar un empaquetador de agentes y un instalador de agentes. Para acceder a esta vista:

1. Vaya a **Administrar** > **Servicios**.
2. En la vista Servicios, seleccione **Servidor de Endpoint**.
3. Haga clic en  y seleccione > **Ver** > **Configuración**.
4. Haga clic en la pestaña **Empaquetador**.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Generar un empaquetador de agentes para la recopilación de datos de Endpoint*	*Guía de instalación de agentes de Endpoint Insights*
Administrador	Generar un empaquetador de agentes con la recopilación de registros de Windows*	
Administrador	Generar un instalador de agentes*	

*Puede realizar esta tarea en la vista actual.

Para obtener más información sobre cómo generar un agente, consulte la *Guía de instalación de agentes de Endpoint Insights*.

Solución de problemas

En esta sección se proporciona información sobre posibles problemas durante el uso de RSA NetWitness Endpoint Insights.

Problemas de comunicación de los agentes

Problema	El agente no puede comunicarse con el servidor de Endpoint.

Explicación	Podría deberse a una de las siguientes causas:
	• En el empaquetador de agentes:
	  • La IP del servidor es incorrecta
	  • El puerto especificado no está disponible para la comunicación con el servidor de Endpoint
	• El servidor de Endpoint o el servidor de Nginx no están en ejecución
	• Las reglas de firewall o tabla de IP están bloqueando la conexión entre el host y el servidor de Endpoint
	• El agente está inactivo o se eliminó manualmente de la interfaz del usuario

Solución	• Compruebe si el servidor de Endpoint y el servidor de Nginx están accesibles • Desinstale el agente, reinicie el host y vuelva a instalar el agente • Actualice las reglas de firewall o tabla de IP, si es necesario

Problema	El agente tarda mucho tiempo en escanear.
Explicación	Algunas veces, el escaneo de NetWitness Endpoint tarda mucho tiempo en completarse. Esto se debe al uso de la CPU que hacen otros programas antivirus (por ejemplo, Windows Defender, Mcafee, Norton, etc.) que pueden estar instalados en las máquinas de los agentes.
Solución	Se recomienda incluir en la lista blanca el archivo NWEAgent.exe en el conjunto de aplicaciones antivirus de Windows.

Problemas del empaquetador

Mensaje	`Failed to load the client certificate.`
Problema	La contraseña del certificado es incorrecta.
Explicación	En el momento de generar el instalador de agentes, la contraseña del certificado no coincide con la que se proporcionó durante la descarga del empaquetador de agentes desde la interfaz del usuario.
Solución	Especifique la contraseña correcta del certificado.

Mensaje	`An unexpected error has occurred attempting to retrieve this data.`
Problema	Al intentar acceder a la pestaña Empaquetador, se abre con el mensaje.
Explicación	El servidor de Endpoint puede estar inactivo o no accesible.
Solución	Compruebe el estado del servidor de Endpoint en **Administrar > Servicio**. Si el servicio no está en ejecución, inicie el servidor de Endpoint.

Problemas de programa de escaneo

Mensaje	`An unexpected error has occurred attempting to retrieve this data.`
Problema	Al intentar acceder a la pestaña Programa de escaneo, se abre con el mensaje.
Explicación	El servidor de Endpoint puede estar inactivo o no accesible.
Solución	Compruebe el estado del servidor de Endpoint en **Administrar > Servicio**. Si el servicio no está en ejecución, inicie el servidor de Endpoint.

Problemas de estado y condición

Comportamiento	Los metadatos de terminales no están disponibles en la vista **Investigar >**

	Navegar o **Análisis de eventos**.
Problema	La evaluación del estado de Meta-Ld-Buffer muestra **En mal estado** en Estado y condición, con las siguientes excepciones: `dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder`
Solución	Asegúrese de que: • La opción Captura esté activada en el Log Decoder • La opción Metadatos esté configurada correctamente

Comportamiento	Para NetWitness Endpoint 4.4.0.2, los metadatos no están teniendo acceso al servidor de Endpoint.
Problema	El estado de Meta-Ld-Buffer muestra **En mal estado** en Estado y condición, con las siguientes excepciones: `dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder`
Explicación	Asegúrese de que: • El certificado se obtenga y se importe al servidor de la consola de NetWitness 4.4.0.2 • La opción NetWitness Investigate esté activada en la interfaz del usuario de NetWitness Endpoint • El reenvío de metadatos esté configurado en el servidor de la consola de NetWitness 4.4.0.2

Comportamiento	La evaluación del estado de Data.Application.Connection-Health del servidor de Endpoint muestra **En mal estado**.
Problema	El servicio Mongo o Servidor de Endpoint están inactivos.
Explicación	Para conocer los detalles del error, consulte los registros del servidor de Endpoint en /var/log/netwitness/endpoint-server/endpoint-server.log.
Solución	Reinicie el servicio Mongo o Servidor de Endpoint.

Comportamiento	La evaluación del estado de la estadística Endpoint.Health.Overall-Health muestra **En mal estado**.
Problema	El servicio Mongo o Servidor de Endpoint están inactivos.
Explicación	Compruebe las estadísticas de estado del servidor de Endpoint (como, Data.Application.Connection-Health, Endpoint.Health.Ld-Buffer-Health) para identificar qué estadísticas muestran En mal estado. Si una de ellas está En mal estado, el estado general del servidor de Endpoint muestra En mal estado.
Solución	Consulte la solución para estas estadísticas en la sección Problemas de estado y condición.

Problema	El conteo de rechazos de agentes es mayor que el umbral de alarma.
Explicación	El conteo de agentes rechazados es mayor que un límite específico y se activa la política personalizada. Por ejemplo, el conteo de agentes rechazados de las últimas 5 horas corresponde al 10 % de los agentes implementados.
Solución	Compruebe el estado general del servidor de Endpoint y las reglas de dimensionamiento.

Problema	La estadística del tamaño del almacenamiento de la aplicación de datos superó el umbral de alarma.
Explicación	El tamaño del almacenamiento de la aplicación de datos superó el umbral (por ejemplo, el 75 %) y se activa la política personalizada. **Nota:** De manera predeterminada, el servidor elimina automáticamente los datos más antiguos cuando alcanza el 80 % del espacio en disco.
Solución	Compruebe el umbral establecido en la política de retención de datos.

Problema	La evaluación del estado de Data.Application.Connection-Health muestra En mal estado o Grave.

Explicación	El servicio Mongo está inactivo.
Solución	Compruebe si el servicio Mongo está en ejecución y si el servidor de Endpoint registra los detalles de errores.

Problema	El conteo de solicitudes de agentes muestra 0 para un umbral de alarma.

Explicación	El conteo de solicitudes de agentes muestra 0 para todo el día o toda la semana. Podría deberse a una de las siguientes causas:
	• En el empaquetador de agentes:
	  • La IP del servidor es incorrecta
	  • El puerto especificado no está disponible para la comunicación con el servidor de Endpoint
	• El servidor de Endpoint o el servidor de Nginx no están en ejecución
	• Las reglas de firewall o tabla de IP están bloqueando la conexión entre el host y el servidor de Endpoint
	• El agente está inactivo o se eliminó manualmente de la interfaz del usuario

Solución	• Compruebe si el servidor de Endpoint y el servidor de Nginx están accesibles • Desinstale el agente, reinicie el host y vuelva a instalar el agente • Actualice las reglas de firewall o tabla de IP, si es necesario

Problema de configuración de metadatos

Comportamiento	El servidor de la consola muestra un mensaje.
Problema	El servidor de la consola muestra el siguiente mensaje: *El servidor de la consola registrará el lote procesado como 1.“rsa-nw-endpoint-agent se usará para establecer la conexión SSL con NetWitness Suite.*
Explicación	Cuando se ejecuta un escaneo rápido en el servidor de NetWitness Endpoint 4.4 para un agente o una máquina, se muestra un mensaje.
Solución	Verifique la configuración de los metadatos.

Problemas de instalación

Comportamiento	NetWitness Suite permite que se instalen varias instancias de Endpoint Hybrid o Endpoint Log Hybrid.
Problema	Solo una instancia de Endpoint Hybrid o Endpoint Log Hybrid se puede usar para los datos de Endpoint.
Explicación	Aunque la instalación de Endpoint Hybrid o Endpoint Log Hybrid esté en curso, puede instalar otra instancia y la instalación se realizará correctamente.
Solución	Debe eliminar todas las instancias de Endpoint Hybrid o Endpoint Log Hybrid, excepto la que desee usar para los datos de Endpoint.

Problema de búsqueda de agentes inactivos

Problema	Un agente podría estar inactivo o no haberse comunicado con el servidor de Endpoint durante mucho tiempo.
Explicación	Una lista de agentes inactivos está disponible en la base de datos de Mongo con el ID de agente. Con esta información, puede buscar más detalles de los agentes inactivos.
Solución	Para buscar agentes inactivos en su implementación, realice lo siguiente: 1. Abra el archivo de registro del servidor de Endpoint en `/var/log/netwitness/endpoint-server/endpoint-server.log` y busque la cadena El <ID> de agente no existe. 2. Copie el ID de agente que aparece en el archivo de registro. 3. Busque el ID de agente en el archivo de registro de acceso a NGINX (`/var/log/nginx/access.log`) para recuperar los siguientes detalles de un agente inactivo: • Dirección IP • Fecha y hora en que el agente quedó inactivo • Ubicación