RSA NETWITNESS® PLATFORM

Guía de configuración de Context Hub

para la versión 11.2

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.

February 2019

Contenido

Cómo funciona Context Hub

El servicio Context Hub proporciona funcionalidad de búsqueda de enriquecimiento en las vistas Respond e Investigate. Un administrador puede configurar el servicio Context Hub y los orígenes de datos para permitir que un analista realice la búsqueda de contexto de los orígenes de datos requeridos.

De forma predeterminada, el servicio Context Hub es compatible con búsquedas de enriquecimiento para tipos de metadatos como dirección IP, usuario, dominio, dirección MAC, nombre de archivo, hash de archivo y host.

Los siguientes orígenes de datos son compatibles con NetWitness Platform y proporcionan datos enriquecidos cuando se configuran.

Lists- Proporciona información contextual de una lista de listas negras, listas blancas o listas de seguimiento.

RSA Archer: Proporciona información de criticidad de un dispositivo o un recurso específico en función de la dirección IP o del host que necesita monitoreo constante.

Active Directory: Proporciona información contextual de un usuario para ayudar a determinar si el usuario es sospechoso o no.

RSA NetWitness® Endpoint-Proporciona información de contexto para indicadores de módulos y máquinas de Endpoint y para ayudar a determinar si alguno de los dispositivos de Endpoint está en riesgo.

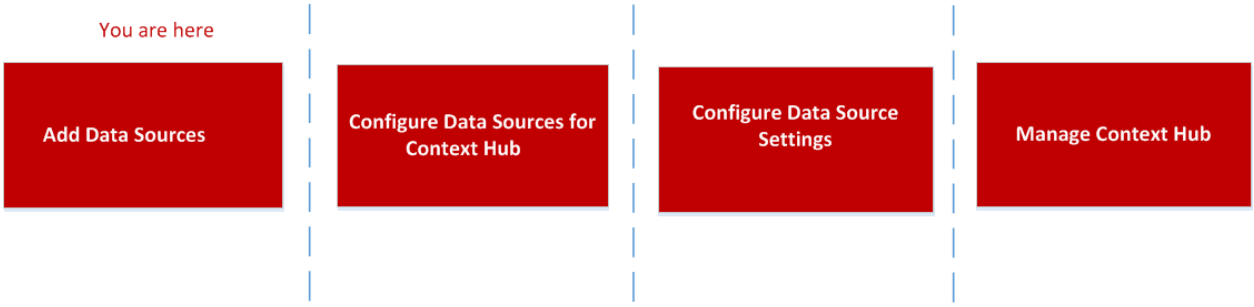
Respond: Proporciona información contextual de metadatos específicos disponible en Respond y permite que un analista responda más rápido en función de los datos de contexto.

Live Connect: Proporciona información contextual para direcciones IP, dominios y hashes de archivo desde el servidor de la comunidad de inteligencia de amenazas de RSA Live Connect.

Descripción general de configuración de Context Hub

El administrador debe ejecutar cada paso en la secuencia correcta para configurar que los servicios realicen la búsqueda de contexto de manera eficaz. En el **ADMINISTRAR**> **Servicios**. En la vista Configuración de servicios del servicio Context Hub, un administrador puede configurar orígenes de datos para el servicio Context Hub. El administrador puede configurar búsquedas de contexto para claves de metadatos personalizadas si es necesario y también puede importar o exportar listas.

El flujo de trabajo que se muestra a continuación describe cómo se puede configurar el servicio Context Hub:



El servicio Context Hub está preinstalado en el host de ESA primario y se agrega automáticamente a NetWitness Platform.

Nota: Solo puede tener una instancia del servicio Context Hub habilitada en su implementación de NetWitness Platform. Si hay varios servicios ESA en NetWitness Platform, debe elegir el host de ESA apropiado para Context Hub. Se requiere un mínimo de 8 GB de espacio para configurar Context Hub en el host de ESA.

Configurar listas como un origen de datos

Las listas como un origen de datos usan el servicio Context Hub para obtener información contextual para los tipos de metadatos que son compatibles con la búsqueda de contexto. Puede crear una o más listas y agregar en ellas valores de lista pertinentes. Asegúrese de crear listas significativas, como direcciones IP en lista negra, direcciones IP en lista blanca, etc. Las listas pueden contener entidades compatibles, como dirección IP, dirección MAC, nombre de usuario, nombre de host, nombre de dominio, nombre de archivo o hash de archivo. Puede importar una lista de única columna o una lista de múltiples columnas en la pestaña Origen de datos. Además, todos los feeds (excepto los feeds STIX) que se crean se convierten en listas y se muestran en la búsqueda de contexto. Si Context Hub no está configurado o el servicio está inactivo, los feeds quedarán disponibles cuando Context Hub esté en funcionamiento. Para obtener más información sobre cómo crear feeds, consulte la *Guía de administración de servicios de Live*.

Nota: Cuando se crea un feed, se genera automáticamente una lista con el mismo nombre que el feed. Si el nombre de la lista ya existe, al nombre de la lista nueva se le agrega el número "2" como sufijo. Por ejemplo, si el nombre del feed existente es test1.csv, la lista nueva se denominará test2.csv.

Los valores de lista están en formato CSV disponible en una ubicación externa y se puede acceder a estos a través de los dos siguientes métodos:

- **Almacén de archivo local**: Puede compartir un archivo desde una ubicación local.
- **HTTP(S)**: Puede compartir un archivo mediante una ubicación del servidor web.

Nota: También puede configurar un trabajo recurrente para buscar datos en intervalos regulares mediante el uso de la configuración Búsqueda previa al configurar el mapeo de metadatos.

Requisitos previos

Antes de configurar el origen de datos de Lists, asegúrese de que:

- El usuario tenga permisos de Admin.
- El servicio Context Hub esté disponible en la vista **ADMIN**> **Servicios** de NetWitness Platform.
- Si usa el servidor de Almacén de archivo local o HTTP(S), la ruta mencionada debe contener el archivo CSV.
  En el caso de Almacén de archivo local remoto, el archivo se debe montar o colocar en la ubicación de la unidad local `/var/lib/netwitness/contexthub-server/data`.
- El usuario de NetWitness tenga permiso de lectura para acceder al archivo.

Precaución: Si está creando una lista de Context Hub para utilizarla como origen de enriquecimiento en ESA, el nombre de la lista no puede incluir espacios ni caracteres especiales, ni comenzar con un número. Si no sigue esta convención de asignación de nombres, cuando intente agregar la lista como un origen de enriquecimiento en ESA, se mostrará un mensaje de error y no se le permitirá agregarla.

Agregar el origen de datos de Lista mediante Almacén de archivo local

Para agregar una lista como un origen de datos:

1. Vaya a **ADMINISTRAR > Servicios**.

   Se muestra la vista Servicios.

2. Seleccione el servicio Context Hub y haga clic en > **Ver** > **Configuración**.

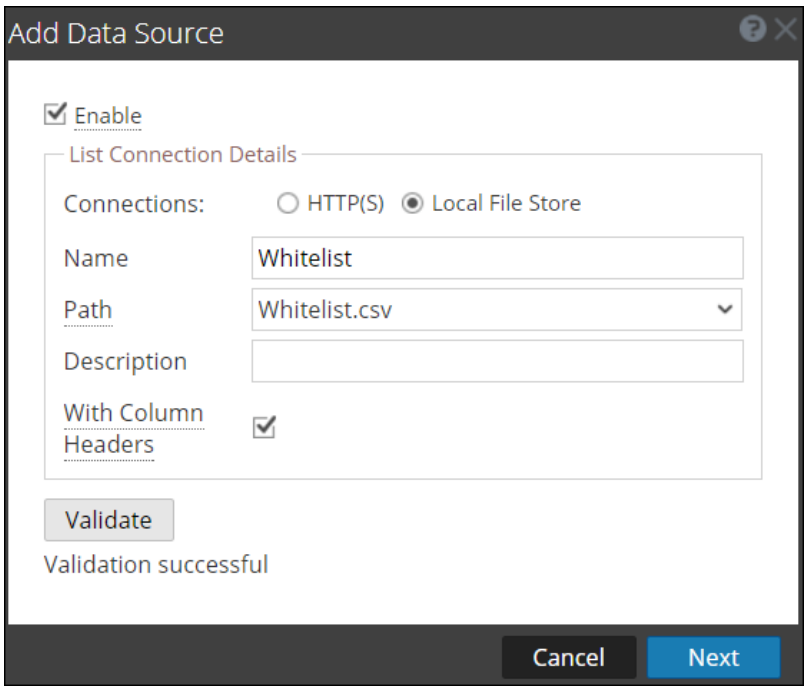
   Se muestra la vista Configuración de servicios de Context Hub.

3. En la pestaña **Orígenes de datos**, haga clic en > **LISTAS**.

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

4. La casilla de verificación **Habilitar** está seleccionada de manera predeterminada. Si esta opción está deseleccionada, el botón guardar está deshabilitado, no se puede agregar el origen de datos, no se puede ver la lista en la pestaña lista y no se puede ver la información contextual.

5. Seleccione el tipo de conexión **Almacén de archivo local**.



6. Proporcione los siguientes detalles de conexión de la base de datos. Ingrese los siguientes campos para el tipo de conexión Almacén de archivo local:

   - **Nombre:** Proporcione un nombre para el origen de datos de lista.
   - **Ruta:** En este campo se muestran todos los archivos de datos disponibles en la carpeta de datos `/var/lib/netwitness/contexthub-server/data`, donde se ejecuta el servicio Context Hub. Seleccione el nombre de archivo en la lista desplegable.
     Se admite un máximo de 32 columnas del archivo CSV que cumplen con los estándares de RFC1480.

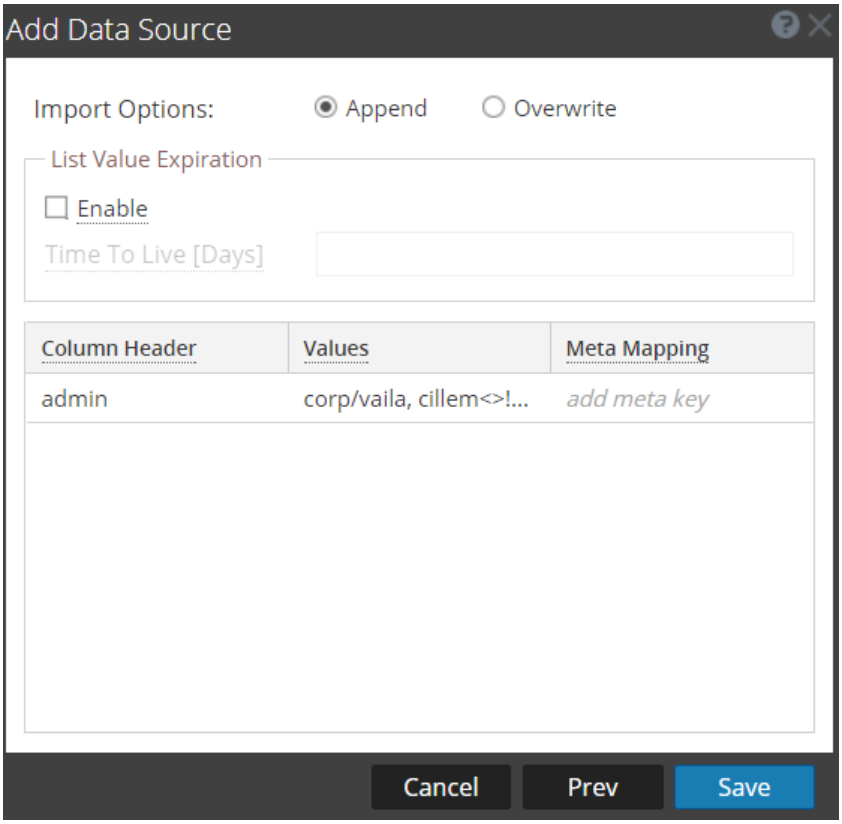
- (Opcional) **Descripción**: Agregue una descripción para el archivo seleccionado.
- **Con encabezados de columna**: Seleccione esta opción para considerar la primera fila como el encabezado de columna del archivo CSV. Si no selecciona esta opción, debe ingresar los encabezados de columna en la pantalla siguiente.

7. Haga clic en **Validar**.

   Si la validación falla, no puede agregar el origen de datos.

8. Haga clic en **Siguiente**.

   Se muestra el siguiente cuadro de diálogo.



9. Seleccione una de las siguientes opciones:
   - **Agregar**: Seleccione esta opción para agregar los valores importados a una lista existente.
   - **Sobrescribir**: Seleccione esta opción para reemplazar los valores en una lista existente por los valores importados.
10. En la sección **Vencimiento de valores de lista**, la opción **Habilitar** está deseleccionada de manera predeterminada. Si desea almacenar los valores de lista buscados en la caché durante una cantidad especificada de días, seleccione la casilla de verificación **Habilitar** e ingrese la cantidad de días en el campo **Tiempo de disponibilidad (días)** para que se conserven los valores de lista.
11. En la siguiente pantalla, mapee al menos una clave de metadatos con uno o más tipos de metadatos mediante el mapeo de un encabezado de columna con metadatos. La descripción de cada campo es el siguiente:

- **Encabezado de columna**: Muestra los encabezados del archivo CSV que se deben mapear a un tipo de metadatos.
- **Mapeo de metadatos**: Mapea un campo de encabezado de columna a un tipo de metadatos.
- **Valores**: Muestra los primeros tres valores de la lista importada.

12. Haga clic en **Guardar**.

Agregar el origen de datos de Lista mediante HTTP(S)

Para agregar Lista como un origen de datos:

1. Seleccione **ADMINISTRAR** > **Servicios**.

   Se muestra la vista Servicios.

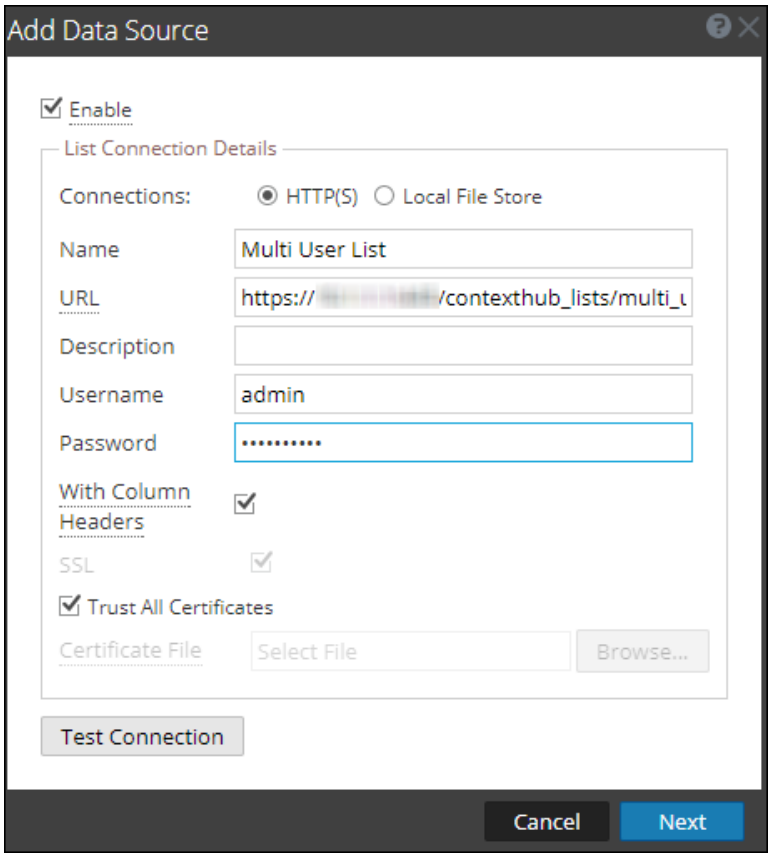
2. Seleccione el servicio Context Hub y haga clic en > **Ver** > **Configuración**.

   Se muestra la vista Configuración de servicios de Context Hub.

3. En la pestaña **Orígenes de datos**, haga clic en > **LISTAS**.

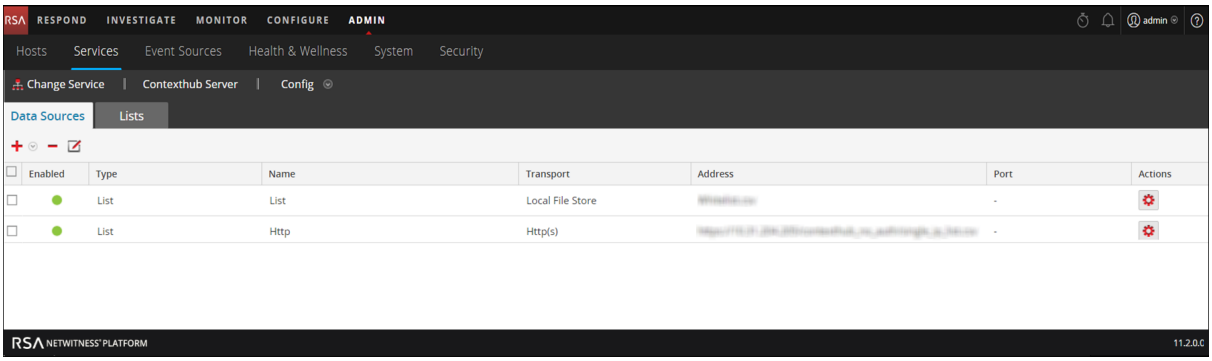
   Se muestra el cuadro de diálogo **Agregar origen de datos**.

4. Seleccione el tipo de conexión HTTP(S).



- Ingrese los siguientes campos para el tipo de conexión HTTP(S):
  - **Nombre:** Proporcione un nombre para el origen de datos de lista.
  - **URL**: Ingrese la ruta del archivo CSV disponible en la ubicación de HTTP(S), junto con el nombre de host o la dirección IP de la máquina remota donde se almacena la lista. El formato de la dirección URL debe ser: `https://<Hostname or IP-address of the HTTP(S)server>:<Port on which the HTTP(S) server is hosted>/<Absolute path of CSV file>`Por ejemplo, `https://10.1.1.1:443/contexthub_lists/multi_user_list.csv`
  - (Opcional) **Descripción**: Agregue una descripción para el archivo seleccionado.
  - (Opcional) **Nombre de usuario:** Ingrese el nombre de usuario para conectarse al servidor de HTTP(S) que requiere autenticación básica.
  - (Opcional) **Contraseña:** Ingrese la contraseña para conectarse al servidor de HTTP(S) que requiere autenticación básica.
  - **Con encabezados de columna**: Seleccione esta opción si desea importar un archivo CSV con encabezados. Si se selecciona esta opción e importa el archivo CSV sin encabezados, la primera fila se considerará como un encabezado que se puede editar.
  - **SSL:** Si ingresa una dirección URL con HTTPS en este campo, esta opción se selecciona automáticamente. Si ingresa una dirección URL con HTTP, esta casilla de verificación no está seleccionada.
  - **Confiar en todos los certificados**: Seleccione esta casilla de verificación para agregar el origen de datos sin validar el certificado. Si deselecciona esta opción, debe cargar un certificado válido del servidor de HTTP(S) con formato cer o .crt para que la conexión sea correcta.
5. Haga clic en **Probar conexión** para probar la conexión entre Context Hub y el origen de datos.
6. Haga clic en **Guardar** para guardar la configuración.

   Lista se agrega como un origen de datos para el Context Hub configurado y se muestra en la pestaña **Orígenes de datos**.



Próximos pasos:

- Agregue, edite o quite valores de una lista específica.
- Configure los ajustes de origen de datos para determinar los campos de origen de datos que se mostrarán en el panel Contexto. Para obtener instrucciones, consulte Configurar ajustes de orígenes de datos de Context Hub .
- Importe o exporte una lista. Para obtener más información, consulte Importar o exportar listas para Context Hub.
- Vea los datos contextuales en el panel Resumen de contexto de la vista Respond o la vista Investigate. Para obtener más información, consulte la *Guía del usuario de RSA NetWitness Respond* y la *Guía de RSA NetWitness Investigation y Malware Analysis*.

Configurar Archer como un origen de datos

Puede configurar Archer como un origen de datos para Context Hub y usar el servicio Context Hub para obtener información contextual desde Archer. Use los procedimientos de este tema para agregar Archer como un origen de datos para el servicio Context Hub y configurar los ajustes (si es necesario) para Archer.

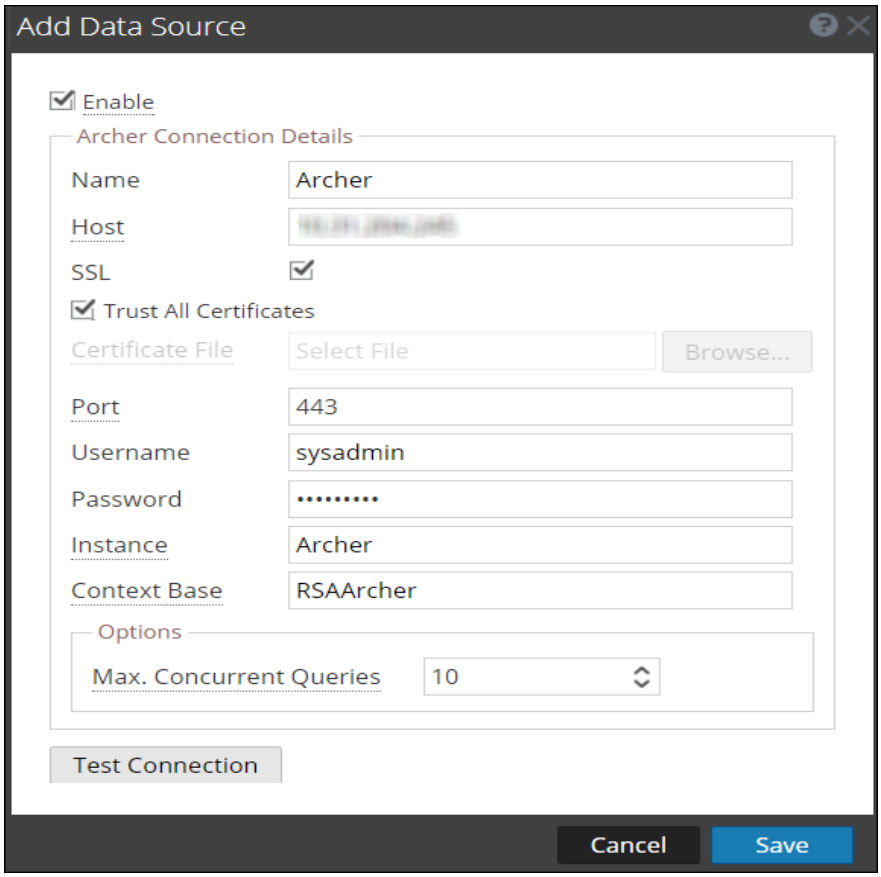
Requisitos previos

Antes de configurar el origen de datos de Archer, asegúrese de que:

- El servicio Context Hub esté disponible en la vista **ADMINISTRAR** > **Servicios** de NetWitness Platform.
- Archer esté instalado con la aplicación de dispositivos con licencia.

Para agregar Archer como un origen de datos para Context Hub:

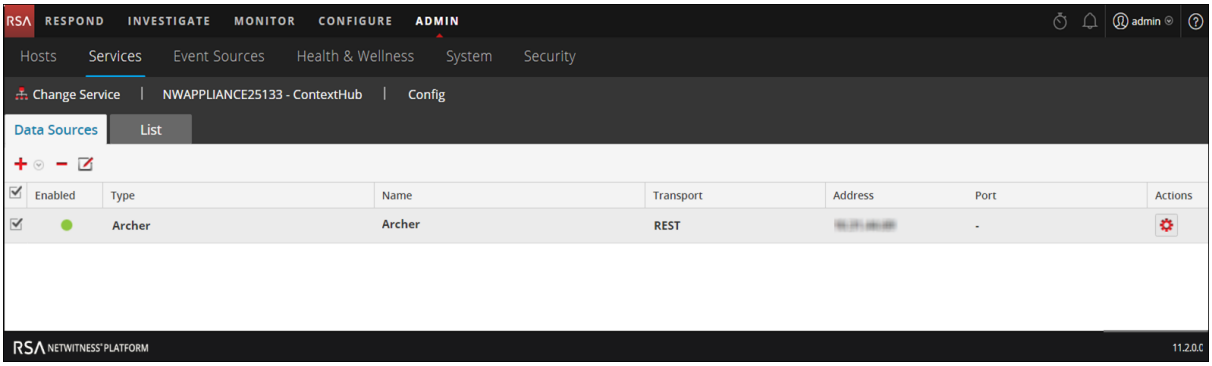
1. Vaya a **ADMIN** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione el servicio Context Hub y haga clic en  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de Servicios.
3. En la pestaña **Orígenes de datos**, haga clic en  > **Archer**.
   Se muestra el cuadro de diálogo **Agregar origen de datos**.



4. Proporcione la siguiente información:

- La casilla de verificación **Habilitar** está seleccionada de manera predeterminada. Si esta opción está deseleccionada, el botón guardar está deshabilitado, no se puede agregar el origen de datos y no se puede ver la información contextual.
- Ingrese los siguientes campos:
  - **Nombre**: Ingrese un nombre para el origen de datos de Archer.
  - **Host**: Ingrese el nombre de host o la dirección IP donde está instalado el servidor de Archer.
  - **SSL**: De forma predeterminada, esta opción está seleccionada y habilita la comunicación de SSL con Archer.
  - **Confiar en todos los certificados**: Seleccione esta casilla de verificación para agregar el origen de datos sin validar el certificado. Si deselecciona esta opción, debe cargar un certificado válido del servidor de Endpoint para que la conexión sea correcta.
  - **Puerto:** El puerto predeterminado es 443.
  - **Nombre de usuario**: Ingrese el nombre de usuario del servidor de Archer.
  - **Contraseña**: Ingrese la contraseña del servidor de Archer.
  - **Instancia**: Ingrese el nombre de la instancia desde la cual desea extraer los datos. Una instancia de RSA Archer es una sola configuración que incluye contenido único de una base de datos, la conexión a la base de datos, la interfaz y el inicio de sesión. Puede haber instancias individuales para cada región o ubicación de oficina o bien para los ambientes de desarrollo, prueba y producción. La base de datos de instancia almacena el contenido de RSA Archer correspondiente a una instancia concreta.
  - **Base de contexto**: Ingrese el nombre del directorio virtual donde se almacenan los archivos. Por ejemplo: rsaarcher que se encuentra en la dirección web de RSA Archer https://archer.company.com/**rsaarche**r/default.aspx. Si los archivos se almacenan en la dirección web predeterminada de IIS https://archer.company.com/default.aspx, este campo debe estar vacío.
  - **Máx. de consultas simultáneas**: Puede configurar la cantidad máxima de consultas simultáneas que define el servicio Context Hub y que se ejecutarán contra los orígenes de datos configurados. El valor predeterminado es 10.
5. Haga clic en **Probar conexión** para probar la conexión entre Context Hub y el origen de datos de Archer.

6. Haga clic en **Guardar**.
   Archer se agrega como un origen de datos para Context Hub y se muestra en la pestaña **Orígenes de datos**.



Después de agregar el origen de datos, puede configurar sus ajustes. Para obtener instrucciones, consulte Configurar ajustes de orígenes de datos de Context Hub . También puede ver los datos contextuales en el panel Resumen de contexto de la vista Respond o la vista Investigate. Para obtener instrucciones, consulte la *Guía del usuario de NetWitness Respond* y la *Guía del usuario de Investigation y Malware Analysis*.

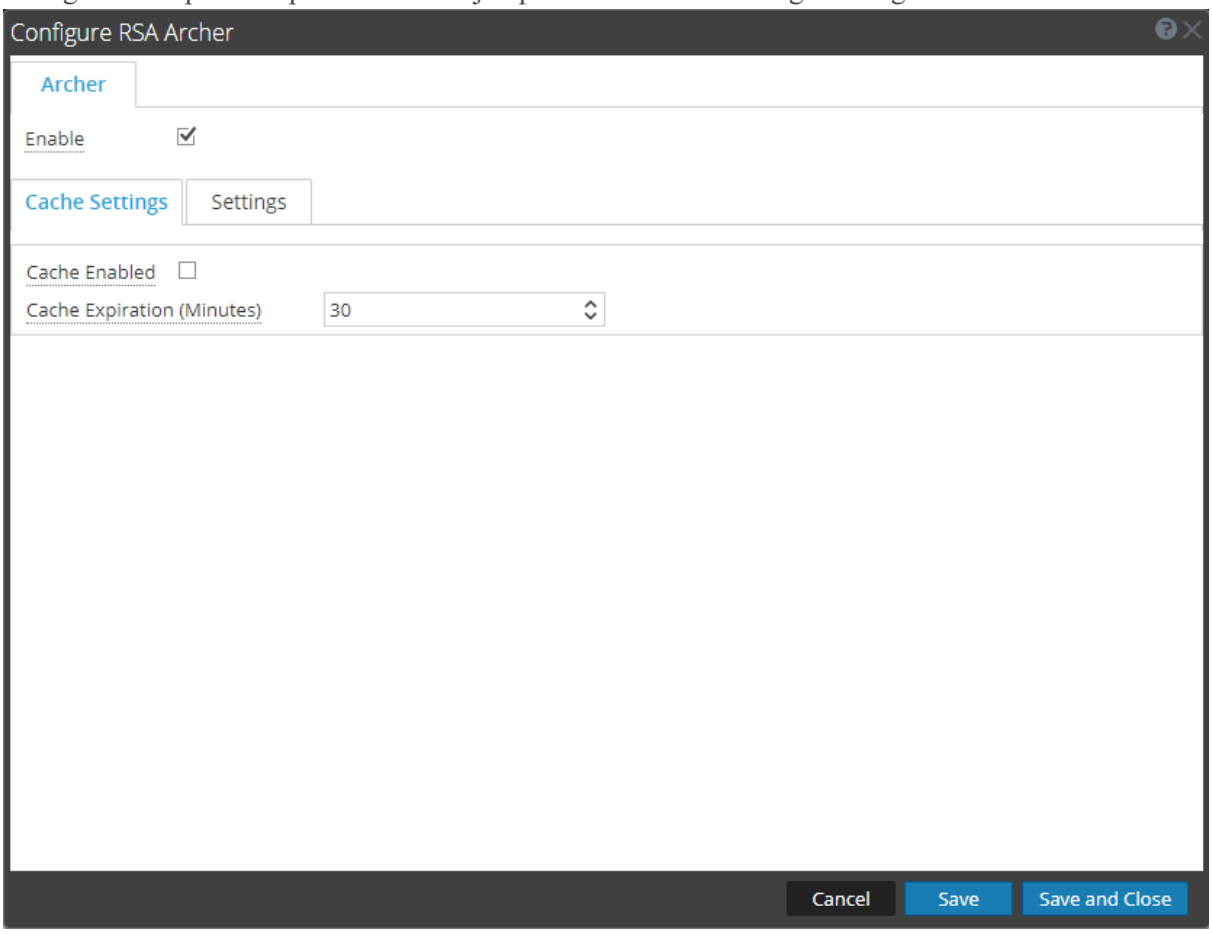
Configurar el origen de datos de Archer

Después de configurar los orígenes de datos requeridos, puede personalizar la configuración de estos de acuerdo con sus requisitos.

Para acceder y configurar los ajustes:

1. Vaya a **ADMIN**> **Servicios**.
   Se muestra la vista Servicios.
2. En el panel Servicios, seleccione el servicio Context Hub y haga clic en **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios de Context Hub.
3. Seleccione el origen de datos cuyos ajustes desea configurar y haga clic en  en la columna Acciones.

La siguiente captura de pantalla es un ejemplo del cuadro de diálogo Configurar de RSA Archer:

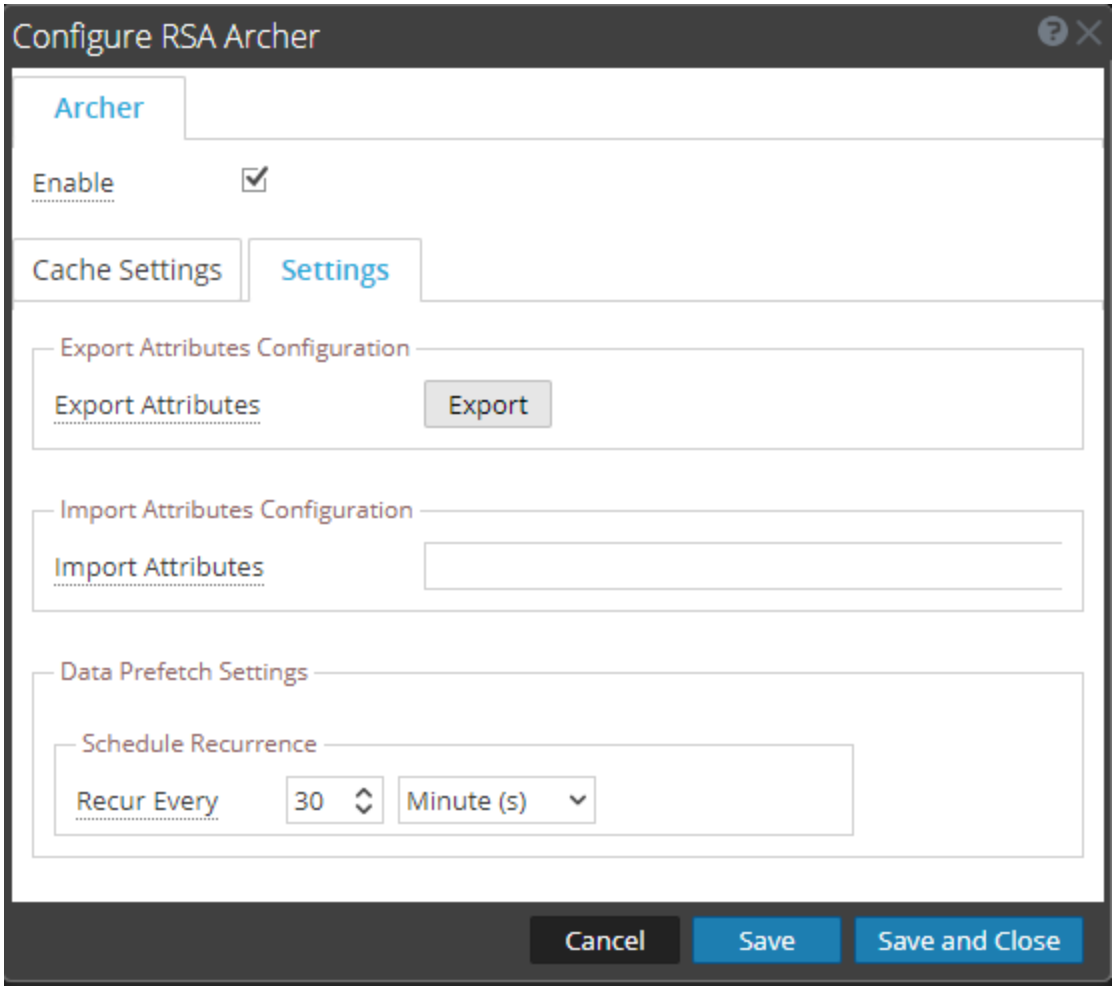


4. En la pestaña **Configuración**. Configure los siguientes campos:

Campo	Descripción
Habilitar	Esta opción está habilitada de manera predeterminada (seleccionada) y se puede utilizar para habilitar o deshabilitar la respuesta desde el origen de datos seleccionado.

Campo	Descripción
Configuración de la caché	Cualquier búsqueda desde Context Hub se puede almacenar en la caché de Context Hub durante un tiempo configurado. La respuesta a cualquier solicitud posterior coincidente se recuperará desde la caché de Context Hub. Use esta sección para definir los siguientes ajustes de caché para la búsqueda de la consulta: • **La caché está habilitada**: Esta casilla de verificación está seleccionada de manera predeterminada y la respuesta a la consulta se almacena en caché. • **Vencimiento de la caché (minutos)**: El tiempo máximo que la búsqueda de la consulta se conserva en la caché. El tiempo predeterminado es 30 minutos y el máximo que puede configurar es 7,200 minutos.

5. Haga clic en **Configuración de la caché**. Configure los siguientes campos



Campo	Descripción
Exportar configuración de atributos	En **Ajustes de configuración**, **Exportar configuración de atributos**, haga clic en **Exportar** para exportar la configuración de atributos de Archer. Estos son los atributos visibles en Búsqueda de contexto mientras se observan detalles de Archer para una dirección IP, un host o una dirección Mac. Se descarga un archivo de configuración JSON, en el cual se mantiene el orden de los atributos sincronizados con la lista en el panel de contexto.
Importar configuración de atributos	Si desea actualizar o editar los ajustes de configuración, en **Ajustes de configuración**, **Importar configuración de atributos**, haga clic en **Navegar**. Seleccione el archivo JSON que contiene los atributos de configuración. Los atributos aparecen en el panel Búsqueda de contexto cuando un usuario ve el contexto, en el orden en que se importaron. **Nota**: Puede respaldar los atributos anteriores antes de importar los cambios realizados en los atributos existentes.
Configuración de búsqueda previa de datos	En **Ajustes de configuración**, **Configuración de búsqueda previa de datos** permite realizar una búsqueda previa de los datos. Configure la **Recurrencia del programa** para proporcionar datos con mayor rapidez cuando coloca el cursor sobre la entidad prevista en Respond.
Recurrencia del programa	En el campo **Repetir cada**, ingrese un valor o utilice la lista desplegable para configurar la recurrencia de la búsqueda previa. En la lista desplegable se puede seleccionar la duración de tiempo predeterminada para configurar la duración de la recurrencia. Los valores disponibles son minutos, horas, días o semanas.

6. Haga clic en cualquiera de las siguientes opciones:
   - **Cancelar**: Seleccione esta opción para cancelar los cambios.
   - **Guardar**: Seleccione esta opción para guardar los cambios.
   - **Guardar y cerrar**: Seleccione esta opción para guardar y cerrar el cuadro de diálogo.

Nota: Después de configurar los ajustes de los orígenes de datos, puede establecer los parámetros de configuración de Context Hub, para lo cual debe navegar a **ADMIN**> **Servicios**> **Ver** > vista **Explorar**. Asegúrese de reiniciar el servicio Context Hub si realiza cambios en la configuración en la vista Explorar.

Configurar Active Directory como un origen de datos

Puede configurar Active Directory (AD) como un origen de datos para Context Hub y usar el servicio Context Hub para obtener información contextual desde AD. Use los procedimientos de este tema para agregar AD como un origen de datos para el servicio Context Hub y configurar los ajustes (si es necesario) para AD.

Requisitos previos

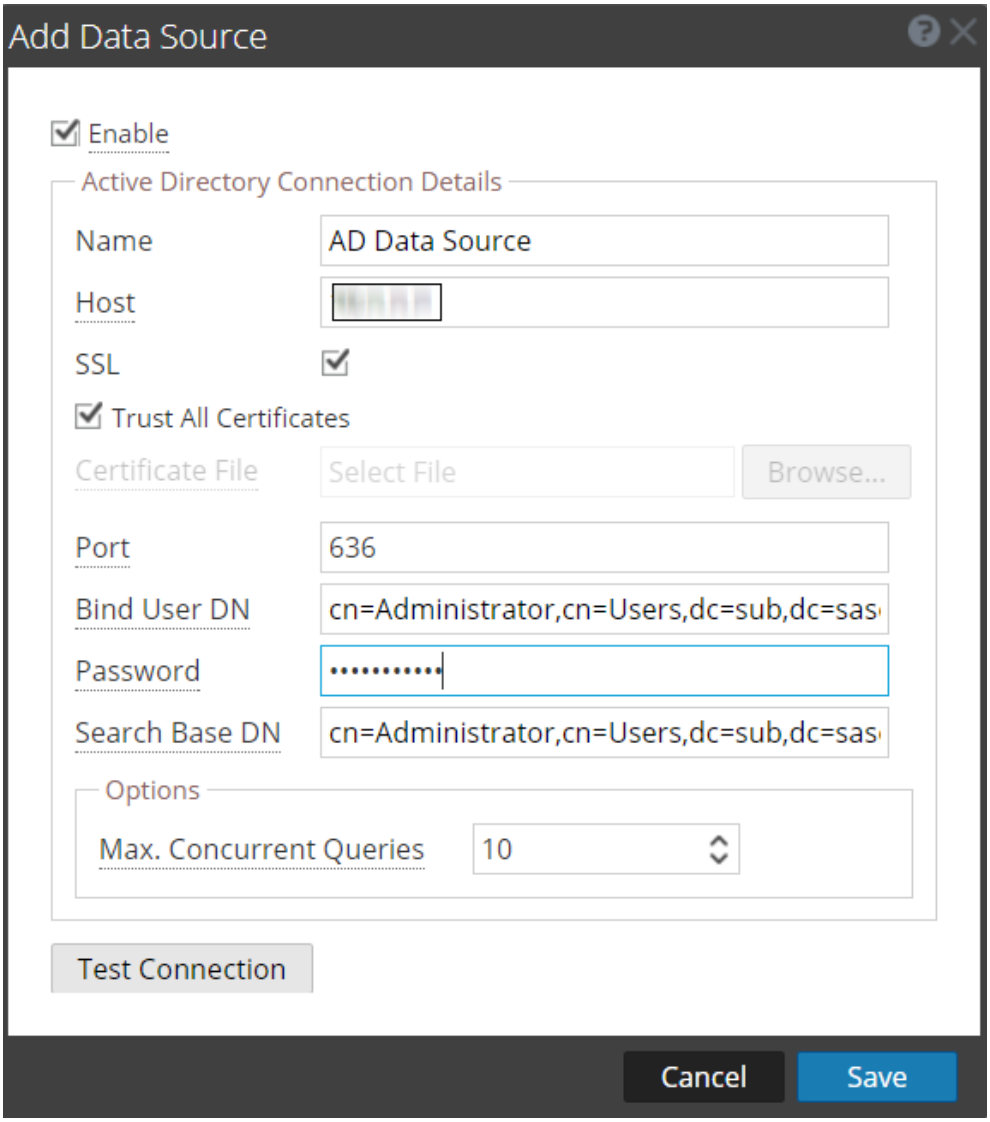
Antes de configurar el origen de datos de Active Directory, asegúrese de que:

- El servicio Context Hub esté disponible en la vista **ADMINISTRAR** > **Servicios** de NetWitness Platform.
- AD esté disponible y se ejecute en Windows versiones 2003, 2008 y 2012 que son compatibles.

Para agregar AD como un origen de datos para Context Hub:

1. Vaya a **ADMIN** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione el servicio Context Hub y haga clic en  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios de Context Hub.

3. En la pestaña **Orígenes de datos**, haga clic en + > **AD**.
   Se muestra el cuadro de diálogo **Agregar origen de datos**.



Debe configurar el esquema de Active Directory para replicar los siguientes atributos para ver los datos en la página RESPONDER:

- ID de empleado
- Departamento
- Empresa
- Título
- Código postal

Todos los demás atributos se replican automáticamente.

6. Proporcione los siguientes detalles de conexión de la base de datos:

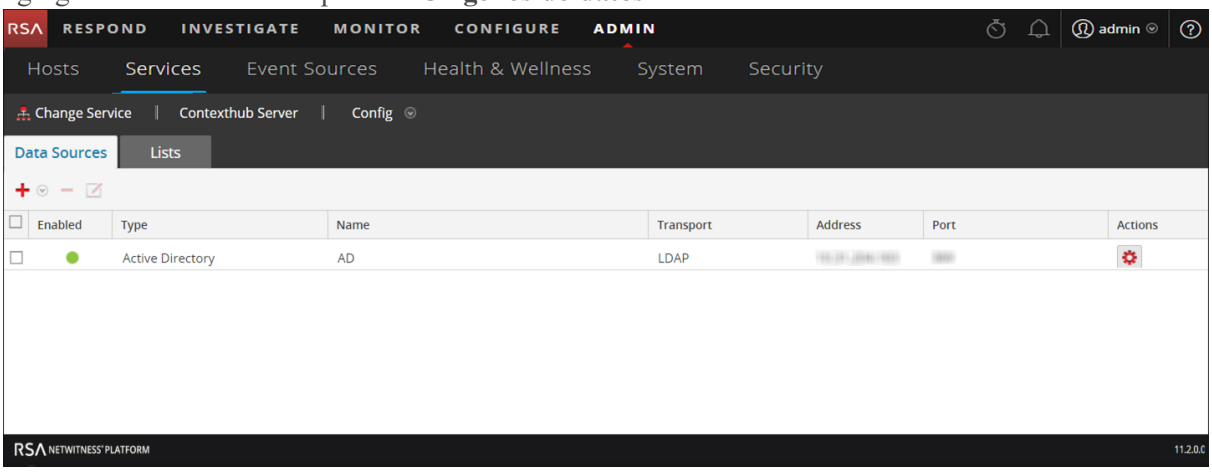
- La casilla de verificación **Habilitar** está seleccionada de manera predeterminada. Si esta opción está deseleccionada, el botón guardar está deshabilitado, no se puede agregar el origen de datos y no se puede ver la información contextual.
- Ingrese los siguientes campos.
  - **Nombre:** Ingrese un nombre para el origen de datos de AD.
  - **Host:** Ingrese el nombre de host o la dirección IP de AD.
  - **SSL:** De forma predeterminada, esta opción estará seleccionada con el número de puerto 636 que se conectará al origen de datos mediante la conexión de capa de conexión segura (SSL).
  - **Confiar en todos los certificados**: Seleccione esta casilla de verificación para agregar el origen de datos sin validar el certificado. Si deselecciona esta opción, debe cargar un certificado válido del servidor de Active Directory con formato cer o .crt para que la conexión sea correcta. Si agrega múltiples orígenes de datos de AD con SSL, debe configurar todos los orígenes de datos con un certificado válido o con la opción Confiar en todos los certificados.
  - **Puerto:** El puerto predeterminado es 636 con protocolo SSL y 389 sin protocolo SSL. Si desea buscar datos en dominios múltiples, puede configurar un único origen de datos con el puerto de catálogo Global (3269 con SSL o 3268 sin SSL).

    Como alternativa, para dominios múltiples, puede configurar un único origen de datos para cada dominio con el puerto predeterminado (389 con SSL o 636 sin SSL).

    Bosques múltiples es un conjunto de dominios múltiples. Si desea buscar datos en bosques múltiples, debe configurar cada bosque con el puerto de catálogo Global (3269 con SSL o 3268 sin SSL).
  - **Contraseña:** Ingrese la contraseña del DN de usuario que se usó para la vinculación con AD.
  - **DN de usuario de vinculación:** El nombre distintivo del usuario que se autenticará en el directorio de búsqueda. Por ejemplo, cn=Administrator,cn=Users,dc=sub,dc=saserver,dc=local.
  - **Buscar DN base:** El nombre distintivo base, o DN base, identifica la entrada en el directorio desde el cual se inician las búsquedas; el DN base a menudo se conoce como la base de búsqueda. Por ejemplo, dc=sub,dc=saserver,dc=local.

7. Haga clic en **Probar conexión** para probar la conexión entre Context Hub y el origen de datos.
8. Haga clic en **Guardar**.
   AD se agrega como un origen de datos para el Context Hub configurado. El origen de datos de AD

agregado se muestra en la pestaña **Orígenes de datos**.



Después de agregar el origen de datos, puede configurar sus ajustes. Para obtener instrucciones, consulte Configurar ajustes de orígenes de datos de Context Hub .

Próximos pasos

Después de completar la configuración, puede ver los datos contextuales en el panel Resumen de contexto de la vista Respond o la vista Investigate. Para obtener instrucciones, consulte el tema **Navegar al panel Resumen de contexto y ver contexto adicional** de la *Guía de Investigation y Malware Analysis*.

Configurar NetWitness Endpoint como un origen de datos

Puede configurar NetWitness Endpoint como un origen de datos para Context Hub y usar el servidor de Context Hub para obtener información contextual desde NetWitness Endpoint. Use los procedimientos de este tema para agregar NetWitness Endpoint como un origen de datos para el servicio Context Hub y configurar los ajustes (si es necesario) para NetWitness Endpoint.

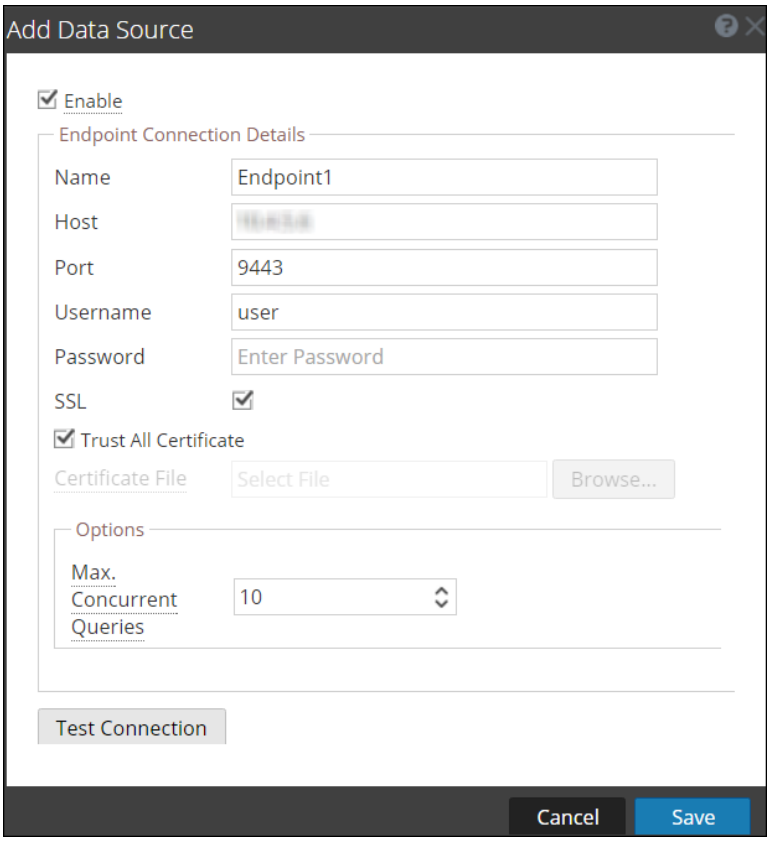
Requisitos previos

Antes de configurar el origen de datos de NetWitness Endpoint, asegúrese de que:

- El servicio Context Hub esté disponible en la vista **Admin** > **Servicios** de NetWitness Platform.
- NetWitness Endpoint (v4.1.1 a 4.3.0.5) esté instalado y configurado.
  Para obtener más información sobre cómo instalar y configurar NetWitness Endpoint, además de obtener información detallada sobre este, consulte los documentos de NetWitness Endpoint disponibles en RSA Link.

Para agregar NetWitness Endpoint como un origen de datos para Context Hub:

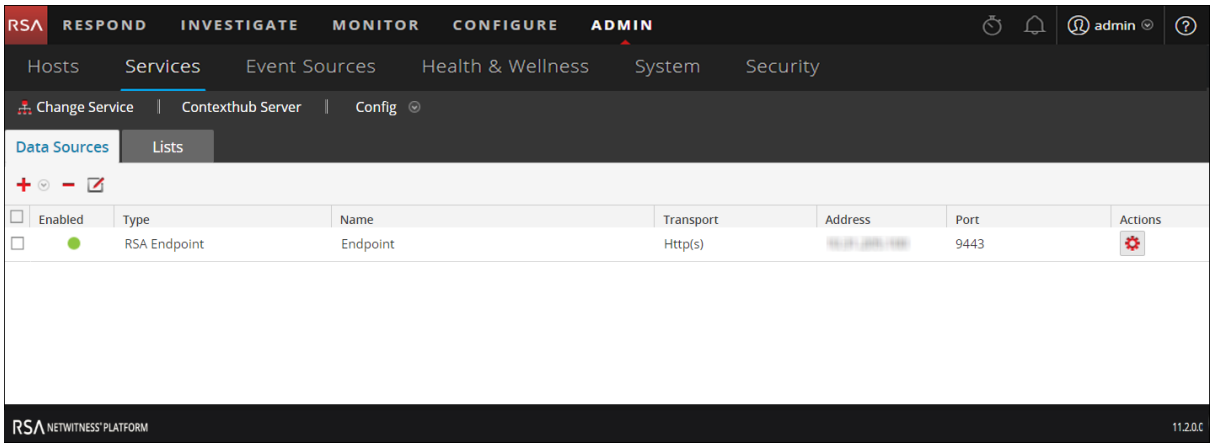
1. Vaya a **Admin** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione el servicio Context Hub y haga clic en > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios.
3. En la pestaña **Orígenes de datos**, haga clic en > **RSA Endpoint**.
   Se muestra el cuadro de diálogo **Agregar origen de datos**.



4. Proporcione la siguiente información:

- La casilla de verificación **Habilitar** está seleccionada de manera predeterminada. Si esta opción está deseleccionada, el botón guardar está deshabilitado, no se puede agregar el origen de datos y no se puede ver la información contextual.
- Ingrese los siguientes campos:
  - **Nombre**: Ingrese un nombre para el origen de datos de NetWitness Endpoint.
  - **Host**: Ingrese el nombre de host o la dirección IP donde está instalado el servidor API de NetWitness Endpoint.
  - **Puerto:** El puerto predeterminado es 9443.
  - **SSL**: Seleccione SSL si desea que NetWitness Platform se comunique con el host mediante SSL. Esta opción está activada de manera predeterminada.
  - **Nombre de usuario**: Ingrese el nombre de usuario del servidor API de NetWitness Endpoint.
  - **Contraseña**: Ingrese la contraseña del servidor API de NetWitness Endpoint.
  - **Confiar en todos los certificados**: Seleccione esta casilla de verificación para agregar el origen de datos sin validar el certificado. Si deselecciona esta opción, debe cargar un servidor válido generado o un certificado de CA para autenticar la conexión con los formatos compatibles de .cer o .crt de codificación en Base64 [PEM] o DER.
  - **Máx. de consultas simultáneas**: Puede configurar la cantidad máxima de consultas simultáneas que se ejecutarán contra los orígenes de datos configurados. El valor predeterminado es 10.

5. Haga clic en **Probar conexión** para probar la conexión entre Context Hub y NetWitness Endpoint.
6. Haga clic en **Guardar**.
   NetWitness Endpoint se agrega como un origen de datos para Context Hub y se muestra en la pestaña **Orígenes de datos**.



Próximos pasos

Después de agregar el origen de datos, puede configurar los ajustes. Para obtener más información, consulte Configurar ajustes de orígenes de datos de Context Hub .

También puede ver los datos contextuales en el panel Resumen de contexto de la vista Respond o la vista Investigate. Para obtener más información, consulte la *Guía del usuario de RSA NetWitness Respond* y la *Guía de RSA NetWitness Investigation y Malware Analysis*.

Configurar Respond como un origen de datos

Puede configurar Respond como un origen de datos para Context Hub y usar el servicio Context Hub para obtener información contextual desde el servicio Respond. Si el servicio Respond ya está configurado, los detalles de configuración se completan automáticamente al agregar Respond como un origen de datos. Use los procedimientos de este tema para agregar Respond como un origen de datos para el servicio Context Hub y configurar los ajustes.

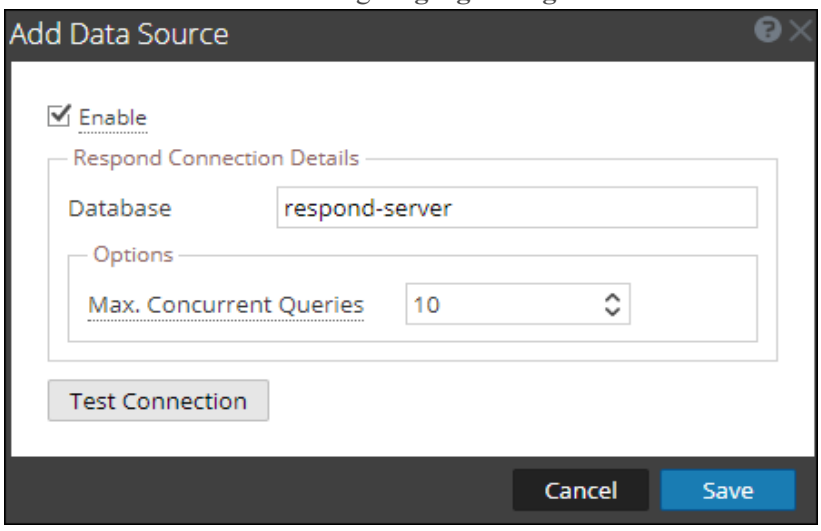
Requisitos previos

Antes de configurar el origen de datos de Respond, asegúrese de que:

- El servicio Context Hub esté disponible en la vista **ADMIN**> **Servicios** de NetWitness Platform.
- El servicio Respond esté disponible.

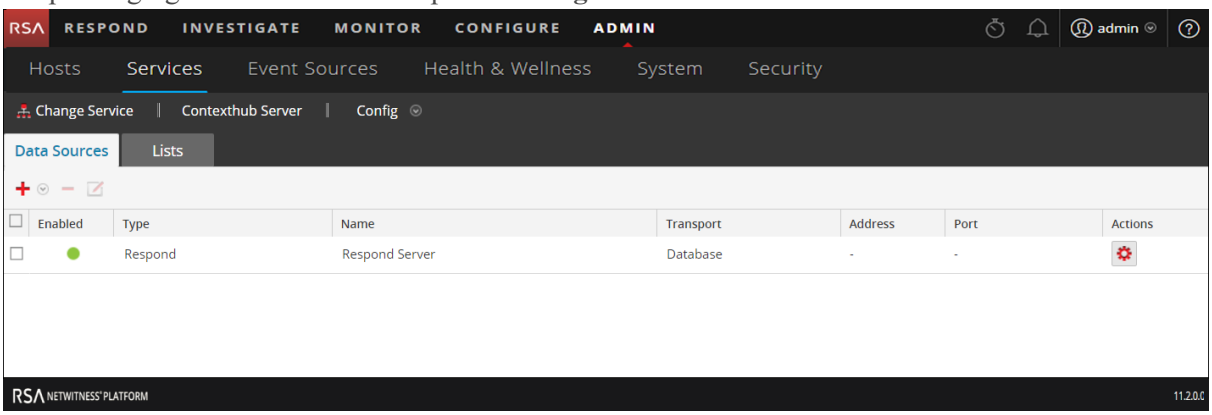
Para agregar Respond como un origen de datos para Context Hub:

1. Vaya a **Admin** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione el servicio Context Hub y haga clic en > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios de Context Hub.
3. En la pestaña **Orígenes de datos**, haga clic en > **Respond**.
   Se muestra el cuadro de diálogo **Agregar origen de datos**.



   Los campos requeridos para configurar el origen de datos de Respond se actualizan automáticamente.
4. Haga clic en **Probar conexión** para probar la conexión entre Context Hub y el origen de datos.
5. Haga clic en **Guardar**.
   Respond se agrega como un origen de datos para el Context Hub configurado. El origen de datos de

Respond agregado se muestra en la pestaña **Orígenes de datos**.



Después de agregar el origen de datos, puede configurar los ajustes. Para obtener más información, consulte Configurar ajustes de orígenes de datos de Context Hub .

Próximos pasos

Después de completar la configuración, puede ver los datos contextuales en el panel Resumen de contexto de la vista Respond o la vista Investigate. Para obtener más información, consulte la *Guía del usuario de RSA NetWitness Respond* y la *Guía de RSA NetWitness Investigation y Malware Analysis*.

Configurar Live Connect como un origen de datos para Context Hub

En este tema se describe el procedimiento para configurar orígenes de datos de Live Connect para Context Hub.

RSA Live Connect es un servicio de inteligencia de amenazas basado en la nube. Este servicio recopila, analiza y evalúa datos de inteligencia de amenazas, como direcciones IP, dominios y archivos recopilados desde diversos orígenes, incluida la comunidad de clientes de RSA NetWitness® Platform y RSA NetWitness® Endpoint.

RSA Live Connect forma parte de los servicios de Live y se puede configurar desde la vista Sistema > panel Configuración de servicios de Live. Para obtener más información sobre la configuración de los servicios de Live, consulte el tema **Configurar los ajustes de servicios de Live** de la *Guía de configuración del sistema*.

Información valiosa de amenazas de RSA Live Connect proporciona a los analistas la oportunidad de extraer datos de inteligencia de amenazas, como información relacionada con direcciones IP, desde el servicio Live Connect para que los analistas los aprovechen durante el proceso de investigación. De manera predeterminada, **Información valiosa de amenazas** está habilitada en **Servicios adicionales de Live**. Si se configura el servicio Context Hub, Live Connect se agrega automáticamente como un origen de datos para Context Hub.

Requisitos previos

Garantice que:

- Context Hub esté habilitado y el servicio esté disponible en la vista Admin > Servicios de NetWitness Platform.
- La cuenta de RSA Live esté disponible.

Nota: Para crear una cuenta de Live, consulte el tema **Paso 1. Crear una cuenta de Live** en la *Guía de administración de servicios de Live*.

De manera predeterminada, **Información valiosa de amenazas** está habilitada en la sección **Servicios adicionales de Live**. Antes de configurar el origen de datos de Live Connect, asegúrese de haber iniciado sesión en su cuenta de Live con sus credenciales de la cuenta de Live y que Context Hub esté habilitado. Live Connect se agrega automáticamente como un origen de datos para Context Hub.

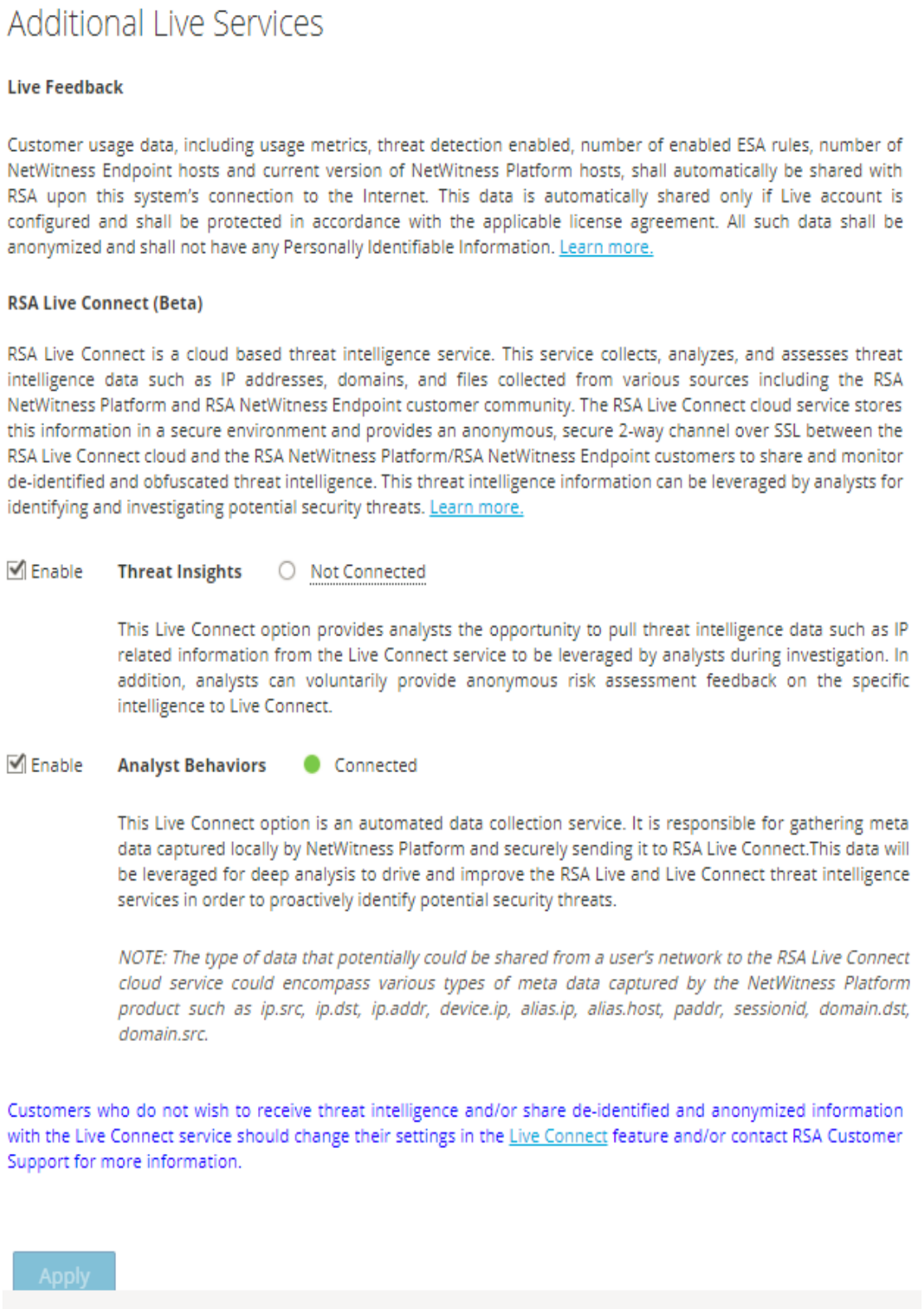
Para obtener información sobre la configuración de la cuenta de Live y los servicios de Live, consulte el tema **Configurar los ajustes de servicios de Live** de la *Guía de configuración del sistema*.

Para obtener información sobre cómo configurar el servicio Context Hub, consulte el tema **Paso 1. Agregar el servicio Context Hub** de la *Guía de configuración de Context Hub*.

Habilitar o deshabilitar el origen de datos de Live Connect

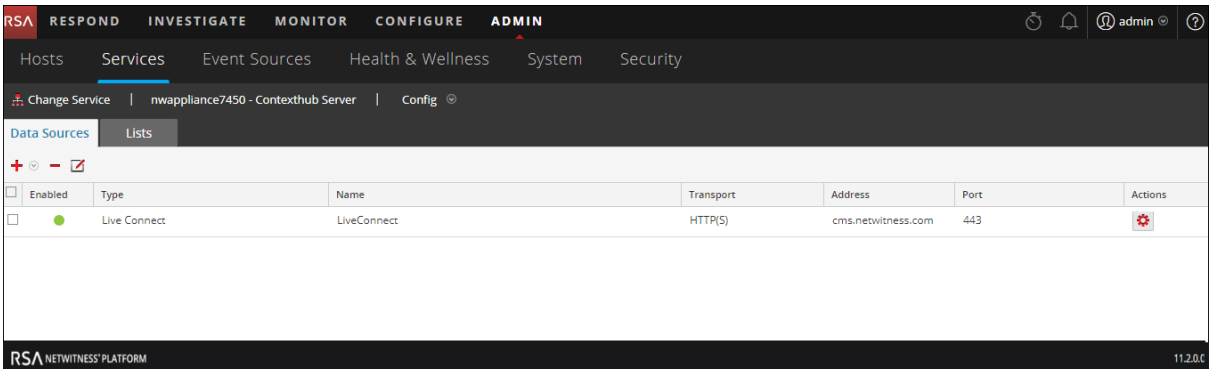
Para habilitar o deshabilitar el origen de datos de Live Connect para Context Hub:

1. Vaya a **ADMIN > Sistema**.
2. En el panel de navegación izquierdo, seleccione **Servicios de Live**.
3. En la sección **Servicios adicionales de Live**, habilite **Información valiosa de amenazas**.



4. Haga clic en **Aplicar**.
   El origen de datos de Live Connect está habilitado para el servicio Context Hub.

5. Para verificar, vaya a la pestaña **Orígenes de datos** y vea los orígenes disponibles.
   El origen de Live Connect debe agregarse a la lista de orígenes disponibles y el campo **Habilitado** debe tener un círculo verde ( ).



6. Para deshabilitar el origen de datos de Live Connect, deshabilite **Información valiosa de amenazas** en el panel Servicios adicionales de Live y haga clic en **Aplicar**.

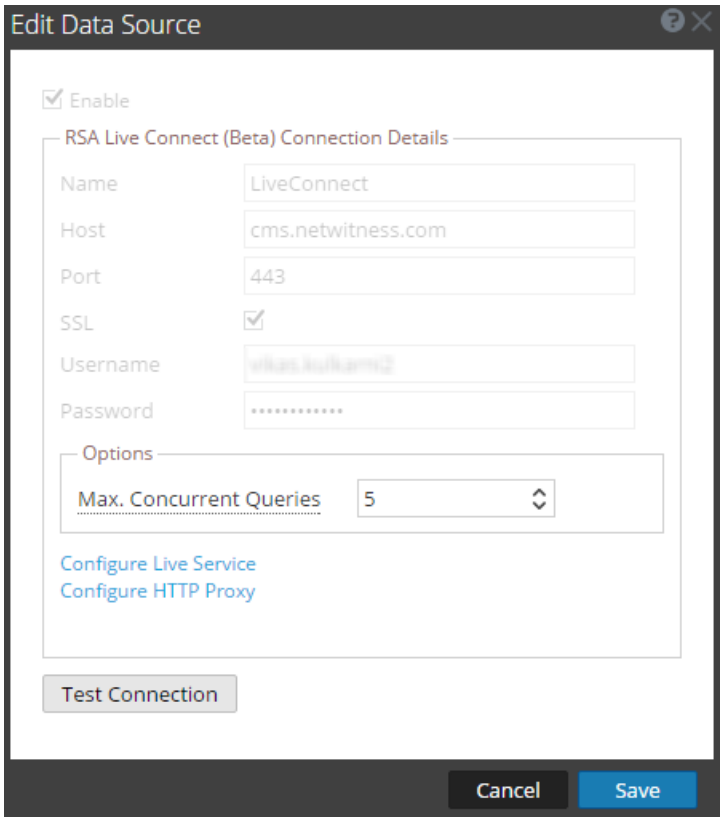
   El origen de datos de Live Connect está deshabilitado para el servicio Context Hub.

   Nota: Si Información valiosa de amenazas está deshabilitada, el panel Búsqueda de contexto para Live Connect (en la vista Navegar y la vista Eventos de Investigation) muestra un mensaje para configurar el origen de datos de Live Connect. Para ver datos contextuales de Live Connect, debe habilitar Información valiosa de amenazas.

Editar configuración de orígenes de datos de Live Connect

Para editar el origen de datos de Live Connect para Context Hub:

1. En el menú principal, seleccione **Admin > Servicios**.
   Se muestra la vista Servicios.
2. En el panel **Servicios**, seleccione el servicio Context Hub y elija > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios.
3. En la pestaña **Orígenes de datos**, seleccione el origen de datos de Live Connect y haga clic en .
   Se muestra el cuadro de diálogo **Editar origen de datos**.



4. Edite los campos obligatorios:

Campo	Descripción
Máx. de consultas simultáneas	Puede configurar la cantidad máxima de consultas simultáneas que define el servicio Context Hub y que se ejecutarán contra los orígenes de datos configurados. El valor predeterminado es 25.

5. Para editar la configuración de Live Connection y Proxy, realice lo siguiente:
   - Para editar la configuración de Conexión de Live, consulte el tema **Panel de configuración de servicios de Live** de la *Guía de configuración del sistema*.
   - Para editar la configuración de proxy, consulte el tema **Panel Configuración de proxy HTTP** de la *Guía de configuración del sistema*.
6. Haga clic en **Probar conexión** para probar la conexión entre Context Hub y el origen de datos.
7. Haga clic en **Guardar** para guardar la configuración.

Próximos pasos

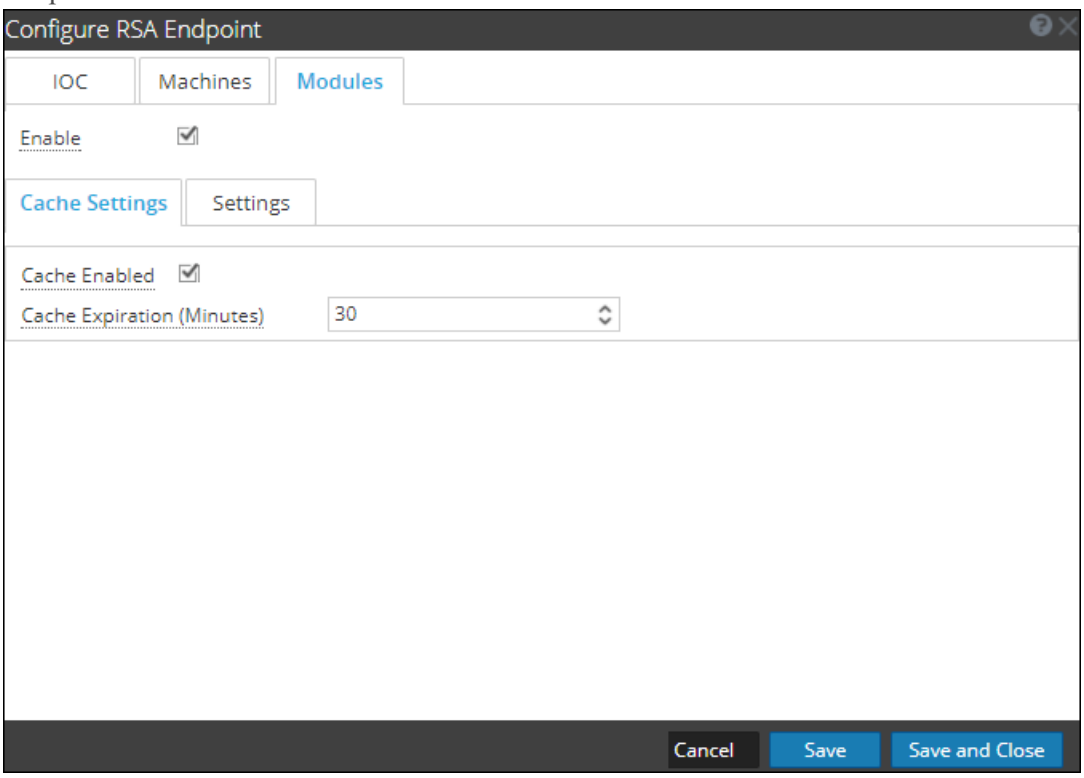
Después de completar la configuración, puede ver los datos contextuales en el panel Resumen de contexto de la vista Respond o la vista Investigate. Para obtener más información, consulte la *Guía del usuario de RSA NetWitness Respond* y la *Guía de RSA NetWitness Investigation y Malware Analysis*.

Configurar ajustes de orígenes de datos de Context Hub

Después de configurar los orígenes de datos requeridos, puede personalizar la configuración de estos de acuerdo con sus requisitos.

Para acceder y configurar los ajustes:

1. Vaya a **ADMIN**> **Servicios**.
   Se muestra la vista Servicios.
2. En el panel Servicios, seleccione el servicio Context Hub y haga clic en **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios de Context Hub.
3. Seleccione el origen de datos cuyos ajustes desea configurar y haga clic en  en la columna Acciones.
   La siguiente captura de pantalla es un ejemplo del cuadro de diálogo de configuración de NetWitness Endpoint:



4. Configure los siguientes campos:

Campo	Descripción
Habilitar	Esta opción está habilitada de manera predeterminada (seleccionada) y se puede utilizar para habilitar o deshabilitar la respuesta desde el origen de datos seleccionado.
Configuración de la caché	Cualquier búsqueda desde Context Hub se puede almacenar en la caché de Context Hub durante un tiempo configurado. La respuesta a cualquier solicitud posterior coincidente se recuperará desde la caché de Context Hub. Use esta sección para definir los siguientes ajustes de caché para la búsqueda de la consulta: • **La caché está habilitada**: Esta casilla de verificación está seleccionada de manera predeterminada y la respuesta a la consulta se almacena en caché. • **Vencimiento de la caché (minutos)**: El tiempo máximo que la búsqueda de la consulta se conserva en la caché. El tiempo predeterminado es 30 minutos y el máximo que puede configurar es 7,200 minutos.
Vencimiento de valores de lista	**Habilitar**: Seleccione Habilitar para definir la cantidad de días que deben estar disponibles los valores de la lista. Esta opción está deshabilitada de manera predeterminada y los valores se conservan. **Tiempo de disponibilidad (días)**: Ingrese la cantidad de días que desea que se conserven los valores de la lista.
Mapeo de metadatos	Cualquier lista almacenada en Context Hub debe estar disponible para una búsqueda. La búsqueda en Context Hub se realiza según el tipo de metadatos o las entidades. Ejemplos: IP, HOST, MAC ADDRESS, DOMAIN, FILE_NAME, FILE_HASH, USER. **Tipo de metadatos**: Entidades disponibles en Context Hub. **Campos de Context Hub**: Encabezados de columna del archivo CSV que usted agregó cuando creó una lista.
Puntaje de IIOC mínimo	El puntaje de IIOC mínimo que se considerará para buscar información contextual sobre los módulos de NetWitness Endpoint.
Consultar últimos (días)	La duración (en días) para la cual se deben consultar los datos de contexto.
Límite	La cantidad máxima de registros que se mostrarán cuando se realice una búsqueda de contexto.
Repetir cada	Configure un programa recurrente para buscar y almacenar datos contextuales para los intervalos requeridos.

5. Haga clic en cualquiera de las siguientes opciones:
   - **Cancelar**: Seleccione esta opción para cancelar los cambios.
   - **Guardar**: Seleccione esta opción para guardar los cambios.

- **Guardar y cerrar**: Seleccione esta opción para guardar y cerrar el cuadro de diálogo.

Según el origen de datos que seleccione, los grupos de respuestas difieren. En la siguiente tabla se describen los grupos de respuestas para cada origen de datos.

Origen de datos (conexión)	Grupos de respuestas compatibles	Configuración de campos
 Lista	Lista	Mapeo de metadatos Tipo de metadatos Campos de Context Hub Ajustes de configuración Configuración de búsqueda previa de datos Recurrencia del programa Vencimiento de valores de lista Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos) [el mínimo es 30 minutos y el máximo, 7,200 minutos]
 RSA Archer	Archer	Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos) Ajustes de configuración Exportar configuración de atributos Exportar atributos Configuración de búsqueda previa de datos Recurrencia del programa

Origen de datos (conexión)	Grupos de respuestas compatibles	Configuración de campos
Active Directory	Usuarios	Mapeo de metadatos Tipo de metadatos Campos de Context Hub Ajustes de configuración Configuración de búsqueda previa de datos Recurrencia del programa Vencimiento de valores de lista Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos) [el mínimo es 30 minutos y el máximo, 7,200 minutos]
RSA Endpoint	IOC Máquinas Módulos	Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos) Ajustes de configuración Configuración del panel de contexto Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos) Ajustes de configuración Configuración del panel de contexto Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos) Ajustes de configuración Puntaje de IIOC mínimo Configuración del panel de contexto
Respond	Alertas Incidentes	Configuración del panel de contexto Configuración de búsqueda previa de datos Consultar últimos (días) Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos)

Origen de datos (conexión)	Grupos de respuestas compatibles	Configuración de campos
Live Connect	Dominio Archivo IP	Configuración de la caché La caché está habilitada Vencimiento de la caché (minutos) Ajustes de configuración Configuración del panel de contexto

Nota: Después de configurar los ajustes de los orígenes de datos, puede establecer los parámetros de configuración de Context Hub, para lo cual debe navegar a **ADMIN**> **Servicios**> **Ver** > vista **Explorar**. Asegúrese de reiniciar el servicio Context Hub si realiza cambios en la configuración en la vista Explorar.

Importar o exportar listas para Context Hub

Como administrador, puede importar o exportar una lista que esté configurada en el servicio Context Hub para que un analista la utilice. El archivo que se importará o se exporta es un archivo CSV y se pueden agregar múltiples listas como orígenes de datos.

Requisitos previos

Asegúrese de que Context Hub esté habilitado y que el servicio esté disponible en la vista **Admin** > **Servicios** de NetWitness Platform.

Importar una lista

Después de haber importado una lista, puede realizar las siguientes tareas:

- Importar valores a una lista existente
- Agregar una fila a una lista
- Editar el nombre y la descripción de una lista
- Editar un valor de una lista
- Eliminar una lista
- Eliminar una fila de una lista

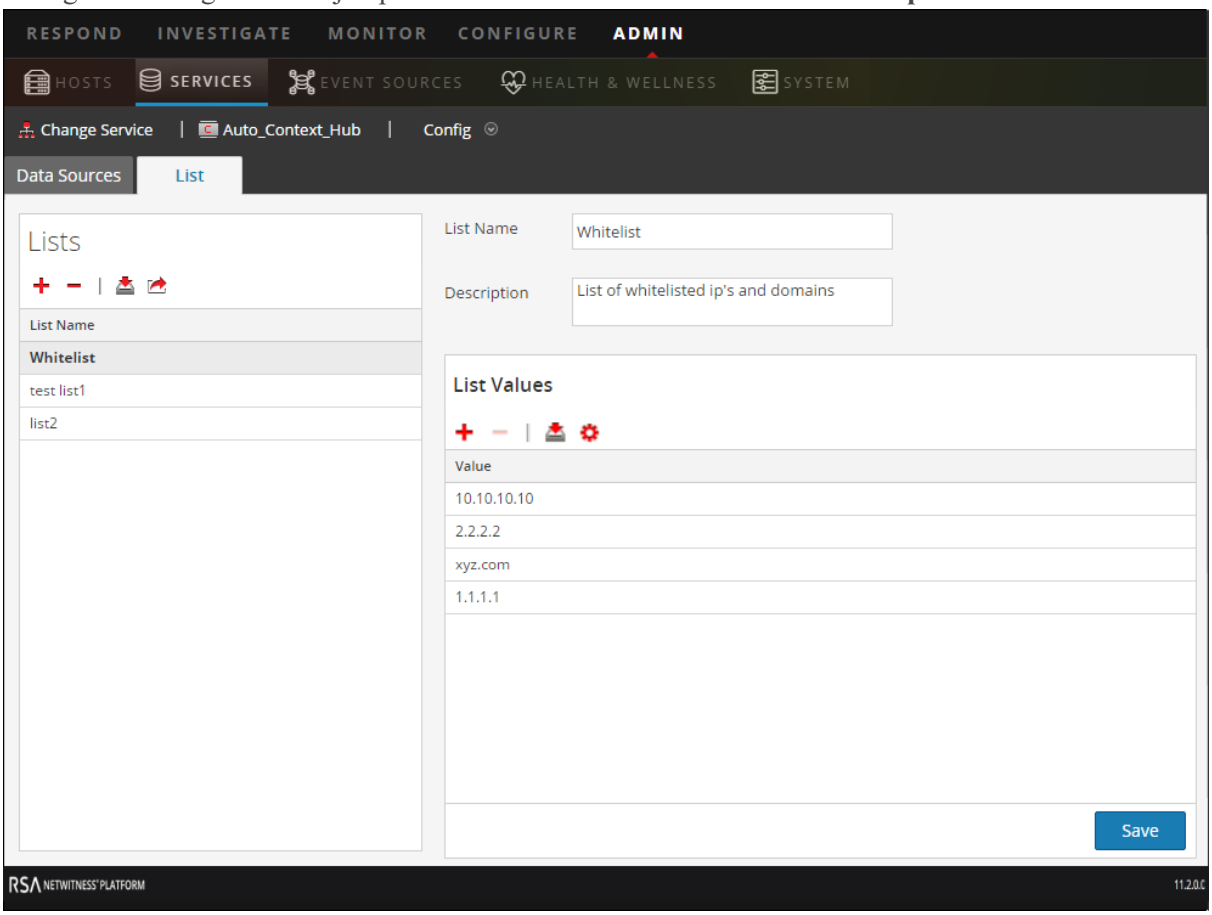
Nota: Debe hacer los mismos cambios al archivo .CSV pertinente, para que los cambios se vean reflejados la próxima vez que se repita el programa. De lo contrario, cuando importe valores a una lista existente de una columna o de múltiples columnas, los datos del archivo de origen se sobrescribirán cuando se repita el programa. En el caso de una lista de feeds personalizados, si el feed se edita o se elimina, la lista de Context Hub correspondiente también se edita o se elimina.

Importar lista de única columna

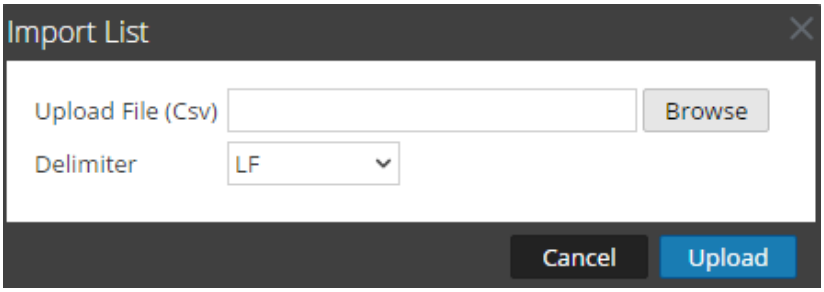
Para importa una lista:

1. Seleccione ADMINISTRAR > **Servicios**.
   Se muestra la vista Servicios.
2. En el panel **Servicios**, seleccione el servicio Context Hub y haga clic en  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios del servicio Context Hub.
3. Haga clic en la pestaña **Listas**.
   La pestaña Listas consta de los paneles **Listas** y **Valores de lista**.

La siguiente imagen es un ejemplo de una lista de una columna. **<need an updated screenshot>**



4. Haga clic en  en el panel **Listas**.
   Se muestra el cuadro de diálogo **Importar lista**.



5. En el cuadro de diálogo **Importar lista**, realice los siguientes pasos:
   a. En el campo **Cargar archivo .CSV)**, navegue y seleccione el archivo `CSV`.
   b. En el campo **Delimitador**, seleccione el delimitador para separar los valores de una lista entre las opciones: **Coma**, **CR** (Retorno de carro) y **LF** (Salto de línea).
6. Haga clic en **Cargar** para cargar el archivo CSV en Context Hub.

Estas listas se consideran orígenes de datos para la recuperación de información contextual. Pero puede anexar a una lista de múltiples columnas existente. Los datos se agregarán solo si coinciden con el número de columnas.

Nota: No puede crear una nueva lista de múltiples columnas mediante la importación directa de un archivo CSV. Sin embargo, todos los feeds que se convierten en listas de múltiples columnas se muestran en la pestaña Lista. Para obtener información sobre cómo importar una lista de múltiples columnas, consulte Configurar listas como un origen de datos.

Importar valores a una lista existente

Cuando importe valores a una lista de múltiples columnas existente, los datos del archivo de origen se sobrescribirán cuando se repita el programa.

Para importar valores a una lista:

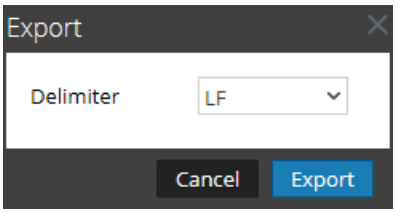
1. Vaya a **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione un servicio y haga clic en  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios del servicio Context Hub.
3. Haga clic en la pestaña **Listas**.
   La pestaña Listas consta de los paneles **Listas** y **Valores de lista**.
4. En el panel Listas, seleccione una lista para la cual desee importar valores.
5. Haga clic en  en el panel **Valores de lista**.
   Se muestra el cuadro de diálogo **Importar lista**.
6. En el cuadro de diálogo **Importar lista**, realice los siguientes pasos:
   a. En el campo **Cargar archivo (Csv)**, navegue y seleccione el archivo `CSV`.
   b. En el campo **Delimitador**, seleccione el delimitador para separar los valores de una lista entre las opciones: **Coma**, **CR**(Retorno de carro) y **LF**(Salto de línea).
7. Haga clic en **Cargar** para cargar el archivo CSV en NetWitness Platform.

Los valores de lista se importan a la lista seleccionada. Estas listas se consideran orígenes de datos para la recuperación de información contextual. Pero puede anexar una lista de múltiples columnas existente. Los datos se agregarán solo si coinciden con el número de columnas.

Exportar una lista para Context Hub

Para exportar una lista:

1. En la pestaña **Listas** de la vista Configuración de servicios del servicio Context Hub, haga clic en  .
   Se muestra el cuadro de diálogo **Exportar**.



2. En el campo **Delimitador**, seleccione el delimitador para separar los valores de una lista exportada en la lista desplegable [**Coma**, **CR** (Retorno de carro) y **LF** (Salto de línea)].
3. Haga clic en **Exportar**.

En el caso de una lista de única columna, puede seleccionar el delimitador. Y, en el caso de una lista de múltiples columnas, la lista se exporta como un archivo .CSV a la máquina local.

Nota: Cuando un feed personalizado se convierte en una lista de Context Hub, debe mapear al menos una clave de metadatos con uno o más mapeos de entidades para un encabezado de columna con un valor de metadatos. Sin embargo, si desea agregar o editar más entidades, puede hacerlo haciendo clic en ⚙.

Configurar el mapeo de tipo de metadatos para Context Hub

Como administrador, puede administrar el mapeo de los tipos de metadatos de Context Hub con claves de metadatos de NetWitness.

El servicio Context Hub proporciona búsqueda de contexto para valores de metadatos en las vistas Respond e Investigation. Estos valores de metadatos se agrupan en tipos de metadatos según la categoría a la cual pertenecen. Por ejemplo, las claves de metadatos de NetWitness Platform Respond e Investigation, como `ip.src` y `ip.dst`, se agrupan en el tipo de metadatos `IP` en Context Hub. A la vez, el tipo de metadatos `IP` se mapea a metadatos como `alert.events.source.device.ip_address` y `alert.events.destination.device.ip_address` en la base de datos de RESPONDER.

En la vista **ADMINISTRAR**> **Sistema** > **Investigation**, la pestaña Búsqueda de contexto permite al administrador configurar el mapeo de claves de metadatos y tipos de metadatos de NetWitness. El administrador puede agregar claves de metadatos a la lista de tipos de metadatos compatibles con Context Hub o quitarlas de ella.

El servicio Context Hub está preconfigurado con un mapeo predeterminado de tipos de metadatos y claves de metadatos, el cual debería funcionar en la mayoría de las implementaciones, a menos que se creen algunos mapeos personalizados para su implementación específica.

Nota: No puede agregar un tipo de metadatos nuevo.

A continuación se muestra el mapeo predeterminado:

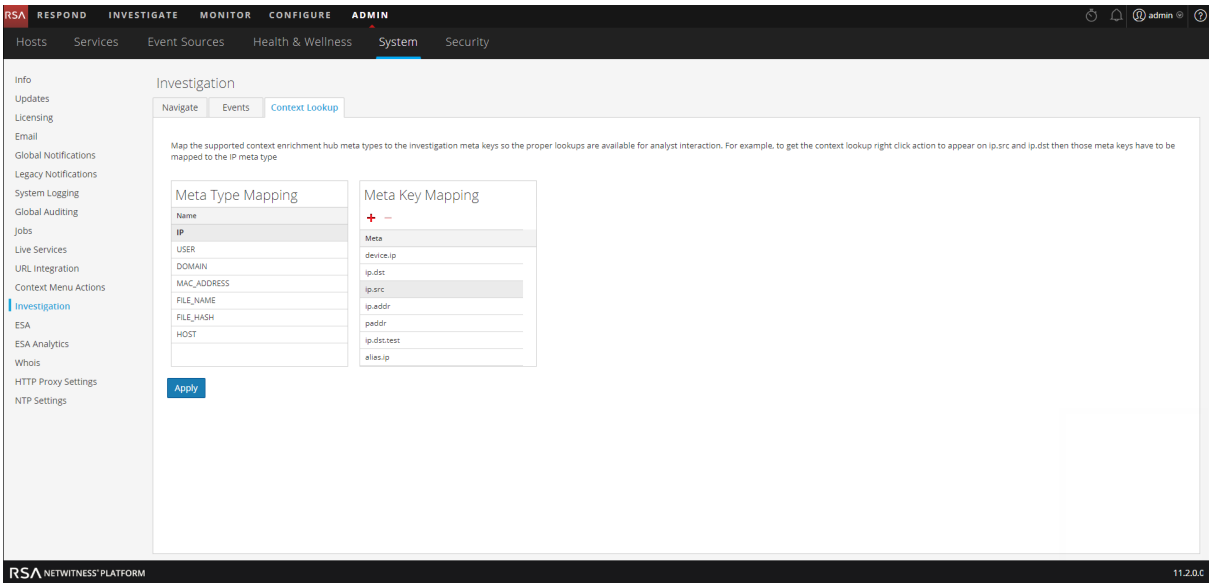
Nombre de tipo de metadatos	Claves de metadatos
IP	device.ip, ip.src, ip.dst, ip.addr,ipv6.src, alias.ip, ipv6.addr, device.ipv6,forward.ip, forward.ipv6,ipv6.dst, ipv6.addr, stransaddr, transaddr
USER	user.src, user.dst, username, event user
DOMAIN	domain.src, domain.dst,fqdn, web.domain, domain, sdomain, ddomain
MAC_ADDRESS	eth.dst, eth.src, alias.mac
FILE_NAME	filename, sourcefile
FILE_HASH	checksum
HOST	device.host, alias.host, host.src, host.dst

Procedimiento

Para administrar el mapeo de claves de metadatos de Investigation:

1. Vaya a ADMINISTRAR > **Sistema**.
2. En el panel de opciones, seleccione **Investigation**.

   Se muestra el panel Configuración de Investigation.
3. Seleccione la pestaña **Búsqueda de contexto**.



4. Seleccione un tipo de metadatos para ver las claves de metadatos predeterminadas que están mapeadas con este tipo de metadatos.
5. Para agregar una clave de metadatos, haga clic en + e ingrese la clave de metadatos.
6. Para eliminar una clave de metadatos, seleccione la clave de metadatos y haga clic en −.
7. Para guardar los cambios, haga clic en **Aplicar**.
8. Para agregar nuevos metadatos, se deben incluir en el archivo de índice personalizado del Concentrator. Por ejemplo, si desea agregar metadatos "**fqdn**", debe agregar una nueva entrada:**<key name="fqdn" description="Fully Qualified Domain Name="IndexValues" form-at="Text" valueMax="100" />** en el archivo de índice. Para obtener más información sobre cómo incluir nuevos metadatos en el archivo de índice, consulte el tema Personalización del índice de la *Guía de ajuste de la base de datos de Core*. Después de agregar los nuevos metadatos, haga clic en la opción Cambiar a Investigate de la vista Responder para ver la información contextual.

En caso de que se agregue una clave de metadatos nueva, la opción de menú Búsqueda de contexto se habilita para los valores de metadatos bajo esa clave de metadatos. Para obtener más información, consulte el tema “Panel Configuración de Investigation“ de la *Guía de configuración del sistema*

Referencias de Context Hub

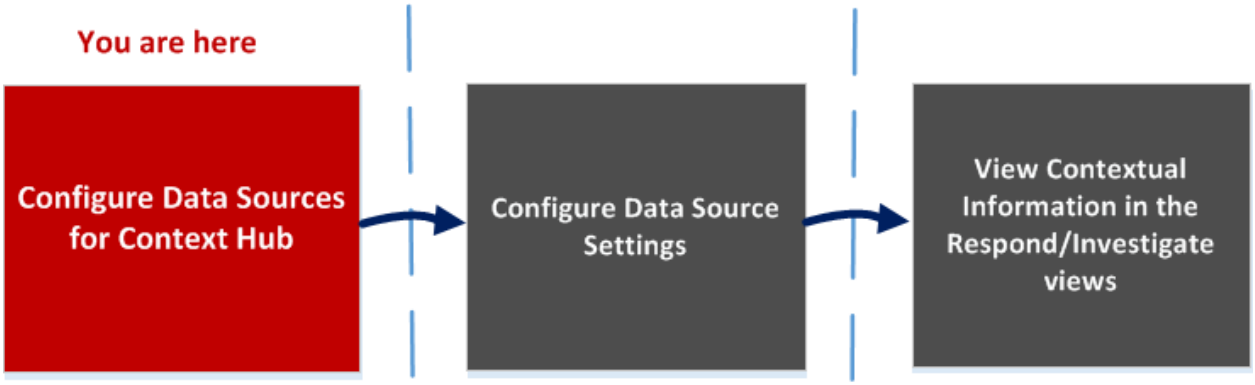
Después de configurar el servicio Context Hub y el origen de datos requerido, puede administrar la configuración para cada origen de datos. Todo esto ayudará a optimizar y personalizar los resultados de búsqueda.

Pestaña Orígenes de datos de Context Hub

La pestaña **Orígenes de datos** permite configurar uno o más orígenes de datos para el servicio Context Hub. Navegue a **ADMIN** > **SERVICIOS** > seleccione el servicio Context Hub > **Ver** > **Configuración** > pestaña **Orígenes de datos**.

Flujo de trabajo

En este flujo de trabajo se muestra el procedimiento para configurar orígenes de datos para el servicio Context Hub con el fin de ver información contextual en las vistas Respond/Investigate.



- La primera tarea consiste en agregar un origen de datos
- La segunda tarea consiste en configurar los ajustes de los orígenes de datos con el fin de mejorar la implementación. Esta tarea es opcional, debido a que la configuración de cada origen de datos ya está establecida con valores predeterminados que ofrecen un rendimiento óptimo.
- Y la tercera tarea consiste en ver y analizar la información contextual en el panel Resumen de contexto de las vistas Respond o Investigate.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar orígenes de datos para Context Hub*	Configurar listas como un origen de datos Configurar Archer como un origen de datos Configurar Active Directory como un origen de datos Configurar NetWitness Endpoint como un origen de datos Configurar Respond como un origen de datos Configurar Live Connect como un origen de datos para Context Hub

Función	Deseo…	Mostrarme cómo
Administrador	Configurar ajustes de datos de Context Hub*	Configurar ajustes de orígenes de datos de Context Hub
Analista	Ver información contextual en la vista Respond	Consulte la *Guía del usuario de NetWitness Respond.*
Analista	Agregar, crear y eliminar una lista de la vista Respond o Investigate	Consulte la *Guía del usuario de NetWitness Respond.* Consulte la *Guía del usuario de Investigation y Malware Analysis*.
Analista	Agregar o eliminar una entrada de una lista existente	Consulte la *Guía del usuario de NetWitness Respond.*

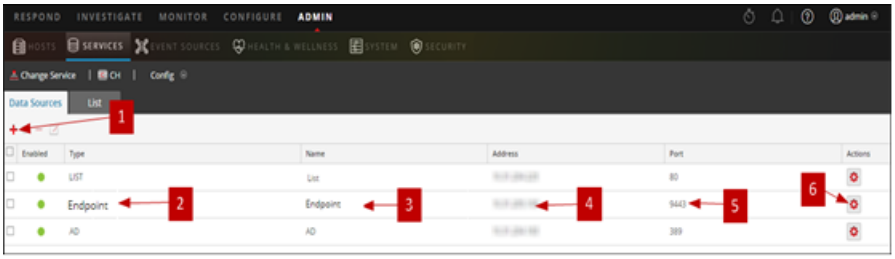
*Puede realizar esta tarea aquí (es decir, en la pestaña Orígenes de datos de Context Hub).

Temas relacionados

- Configurar listas como un origen de datos
- Configurar Archer como un origen de datos
- Configurar Active Directory como un origen de datos
- Configurar NetWitness Endpoint como un origen de datos
- Configurar Respond como un origen de datos
- Configurar Live Connect como un origen de datos para Context Hub

Vista rápida

En el siguiente ejemplo se ilustra cómo agregar un origen de datos para el servicio Context Hub.



1. Haga clic en + para mostrar el cuadro de diálogo **Agregar origen de datos**.
2. Muestra el tipo de origen de datos.
3. Nombre que identifica el origen de datos.
4. La dirección IP o el nombre de host del origen de datos.
5. El puerto de conexión para el origen de datos.
6. Abre el cuadro de diálogo **Establecer configuración**. Puede ver y editar la configuración que se mostrará en el panel Resumen de contexto de las vistas Respond o Investigate.
7. Haga clic en **Probar conexión** para verificar que el host esté conectado al servicio Context Hub.

Barra de herramientas

En la siguiente tabla se describen las acciones de la barra de herramientas.

Función	Descripción
	Se abre el cuadro de diálogo Agregar origen de datos, el cual permite agregar un origen de datos. Puede agregar solo un origen de datos de cada tipo, excepto en el caso de los orígenes de datos Listas y Active Directory, de los cuales se pueden agregar varios. Para obtener instrucciones detalladas sobre cómo agregar un origen de datos, consulte Configurar listas como un origen de datos.
	Eliminar un origen de datos. Si elimina un origen de datos, Context Hub no considera el servicio eliminado como un origen de datos. Toda la información contextual obtenida con anterioridad no estará disponible.
	Abre el cuadro de diálogo Editar origen de datos. Para obtener una descripción de cada campo del panel Editar origen de datos, consulte Configurar Live Connect como un origen de datos para Context Hub.
	Abre el cuadro de diálogo Establecer configuración. Puede ver y editar la configuración de los orígenes de datos. Para obtener una descripción de cada campo del cuadro de diálogo Configurar respuestas, consulte Configurar ajustes de orígenes de datos de Context Hub.

Configuraciones de orígenes de datos

En la siguiente tabla se describen las configuraciones enumeradas.

Función	Descripción
Activado	Indica si el origen de datos está habilitado o deshabilitado. Un círculo de color verde indica que el origen de datos está habilitado ( ). Un círculo de color blanco indica que está deshabilitado.
Tipo	El tipo de origen de datos. Por ejemplo, Listas, Archer, Active Directory, Endpoint, Respond o Live Connect.
Nombre	El nombre único para identificar el origen de datos. Por ejemplo, Respond \.
Dirección	La dirección IP o el nombre de host del origen de datos.
Puerto	El puerto de conexión para el origen de datos, el cual varía en función del origen de datos que se agrega. Por ejemplo, para Endpoint, el puerto es 9443, para Listas, el puerto es 80 y así sucesivamente.

Pestaña Listas de Context Hub

La pestaña **Listas** permite crear y configurar listas para Context Hub. Navegue a **ADMIN** > **SERVICIOS** > seleccione el servicio Context Hub > **Ver** > **Configuración** > pestaña **Listas**.

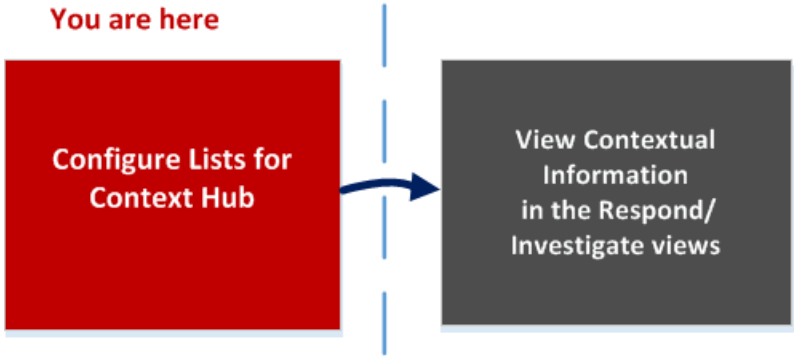
La pestaña Listas del servicio Context Hub permite crear una o más listas y agregar en ellas valores de lista pertinentes. Estas listas se consideran automáticamente como orígenes de datos para el servicio Context Hub.

Estas listas se pueden completar con elementos mediante la importación de archivos CSV de feeds personalizados o externos, o la adición de valores de metadatos a través de la opción Agregar/eliminar de la lista en las vistas de Investigation y Respond.

Nota: También puede crear listas y agregar valores de lista desde las vistas Respond e Investigation. Para obtener más información, consulte la *Guía del usuario de RSA NetWitness Respond* y la *Guía de RSA NetWitness Investigation y Malware Analysis*.

Flujo de trabajo

En este flujo de trabajo se muestra el procedimiento para configurar listas para el servicio Context Hub y para ver información contextual en las vistas Respond e Investigate.



La creación de una o más listas es la primera tarea de este flujo de trabajo. Las listas pueden contener metadatos compatibles, como dirección IP, usuario, host, dominio, dirección MAC, nombre de archivo o hash de archivo. La tarea siguiente consiste en analizar o usar los datos de las listas para ver datos contextuales en las vistas Respond e Investigate.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar el origen de datos Listas para Context Hub*	Configurar listas como un origen de datos
Administrador/analista	Ver información contextual en la vista Respond	Consulte la *Guía del usuario de NetWitness Respond*.

Función	Deseo…	Mostrarme cómo
Administrador/analista	Administrar listas y valores de lista en Investigation	Consulte la *Guía del usuario de Investigation y Malware Analysis*.
Administrador/analista	Crear una lista	Consulte la *Guía del usuario de NetWitness Respond* y la *Guía del usuario de Investigation y Malware Analysis*
Administrador/analista	Actualizar una lista	Consulte la *Guía del usuario de NetWitness Respond* y la *Guía del usuario de Investigation y Malware Analysis*
Administrador/analista	Eliminar lista	Consulte la *Guía del usuario de NetWitness Respond* y la *Guía del usuario de Investigation y Malware Analysis*
Administrador/analista	Importar una lista	Importar o exportar listas para Context Hub
Administrador/analista	Exportar lista	Importar o exportar listas para Context Hub

*Puede realizar esta tarea aquí (es decir, en la pestaña Listas de Context Hub).

Temas relacionados

- Pestaña Orígenes de datos de Context Hub
- "Solución de problemas de NetWitness Investigate" en la *Guía del usuario de NetWitness Investigate*

Vista rápida

En el siguiente ejemplo se ilustra cómo agregar listas para el servicio Context Hub.

La pestaña Lista consta de los paneles **Listas** y **Valores de lista**. El panel **Listas** tiene una barra de herramientas con opciones para agregar, eliminar, importar y exportar listas. Las entradas bajo **Nombre de lista** son listas que se agregan o se importan para el servicio Context Hub.

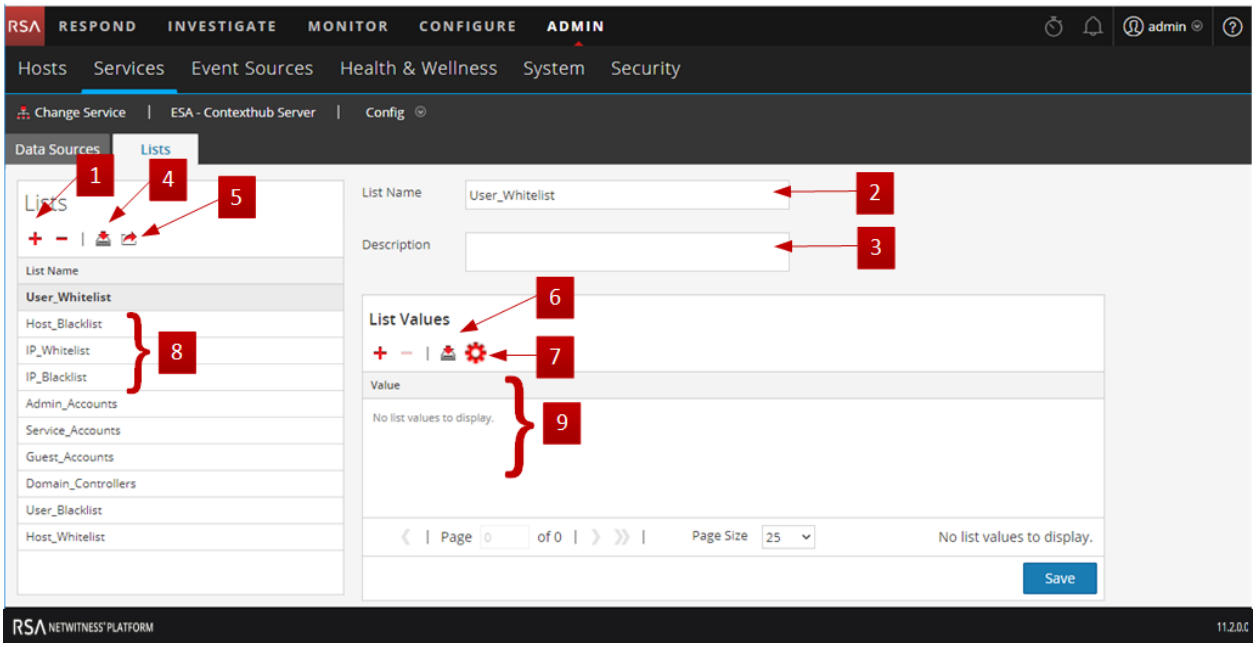
De manera predeterminada, están disponibles 10 listas de una sola columna vacías en RSA NetWitness Platform11.1. Estas listas están vacías y es necesario agregar información en ellas. Los 10 nombres de lista de uso inmediato se utilizan en reglas de ESA. Para obtener más información sobre las reglas de ESA, consulte la *Guía del usuario de Alertas con ESA Correlation Rules*. Los usuarios que actualizan desde versiones anteriores podrán ver estas listas nuevas además de sus listas creadas con anterioridad. Las listas disponibles de manera predeterminada son las siguientes:

- Admin_Accounts
- Guest_Accounts
- Service_Accounts
- User_Blacklist
- User_Whitelist
- Host_Whitelist

- Domain_Controllers
- IP_Blacklist
- IP_Whitelist
- Host_Blacklist

Nota: Si ya existe una lista con el mismo nombre antes de la actualización a RSA NetWitness Platform11.2 o su instalación, esa lista se conservará. Cambie el nombre de esa lista antes de actualizar a 11.1 o actualice el contenido de tal manera que se pueda usar en las reglas de ESA.

Las listas están disponibles en la pestaña Reglas de ESA en CONFIGURAR > Reglas de ESA > Ajustes de configuración > Orígenes de enriquecimiento. Para obtener más información sobre las reglas de ESA, consulte la *Guía de Alertas mediante ESA para la versión 11.1*.
El panel **Valores de lista** tiene una barra de herramientas con opciones para agregar, eliminar e importar valores de lista en la lista seleccionada. Las entradas bajo **Valor** identifican cada entrada de lista que se incluye en la lista.



1	Haga clic en + para agregar una lista nueva.
2	Nombre que identifica la lista.
3	Descripción de la lista.
4	Haga clic en para importar listas a Context Hub.
5	Haga clic en para exportar una lista a la máquina local.
6	Haga clic en para importar valores de lista a la lista seleccionada.

7 Haga clic en para agregar o editar el mapeo de entidades.

8 Muestra las listas personalizadas que se agregan a Context Hub.

9 Muestra los valores de lista que se agregan a la lista seleccionada.

Barra de herramientas

En la siguiente tabla se describen las acciones de la barra de herramientas.

Función	Descripción
	Agregar una nueva lista. Para obtener más información, consulte Configurar listas como un origen de datos.
	Eliminar una lista. Si elimina una lista de Context Hub, esta ya no se considera como un origen de datos para la recuperación de información contextual.
	Importar listas a Context Hub. Para obtener más información, consulte Importar o exportar listas para Context Hub.
	Exportar una lista a la máquina local. Para obtener más información, consulte Importar o exportar listas para Context Hub.

Opciones de la Vista de lista

En la siguiente tabla se describen las configuraciones de Listas.

Función	Descripción
Nombre de lista	Nombre único para identificar la lista.
Descripción	Descripción de la lista.
Guardar	Guarda los cambios realizados en la lista.

Próximos pasos

Después de completar la configuración, puede ver los datos contextuales en el panel Resumen de contexto de la vista Respond o la vista Investigate. Para obtener instrucciones, consulte **Navegar al panel Resumen de contexto y ver contexto adicional** de la *Guía del usuario de Investigation y Malware Analysis*.

Solución de problemas

En este tema se proporciona información sobre los posibles problemas que pueden encontrar los usuarios de NetWitness Platform cuando configuran el servicio Context Hub.

Posibles problemas

Problema	Solución
La búsqueda previa de una lista falla si la lista se crea en modo de adición. En el siguiente mensaje de error que se muestra en los registros, se indica que las entradas de la lista superan el máximo permitido. `Error setting data source entries com.rsa.asoc.contexthub.exception.ContextHubException: total.entries.exceed.max` Además, Estado y condición establece la siguiente estadística: `Contexthub.Datasource.Health.Data-Sources-Health` en `Unhealthy` y muestra los nombres de las listas para las cuales falló la búsqueda previa. Por ejemplo, la cantidad de entradas en la lista es 50,001 y la cantidad de registros en el archivo CSV es 50,001 porque el usuario no cambió el CSV desde la última búsqueda previa. El límite superior para la cantidad de entradas de la lista es 100,000. Ahora, en la búsqueda previa, Context Hub intentará agregar 50,001 entradas a la lista, pero dado que 50,001 + 50,001 > 100,000, la búsqueda previa fallará.	En el archivo CSV, agregue únicamente las entradas que desea agregar en el archivo CSV existente. Si no desea agregar ninguna entrada a la lista, realice una de estas opciones, según corresponda: • Si creó la lista con encabezados, quite todas las filas del archivo CSV, excepto el encabezado. • Si creó la lista sin encabezados, debe tener 0 filas en el archivo CSV.
El protocolo de enlace SSL con certificado de Archer falla cuando se agrega como un origen de datos.	Use un certificado generado por Archer con la opción Confiar en todos los certificados configurada.
La opción Cambiar a Investigate en la vista Respond no navega a la ubicación correcta.	Reinicie el servicio Jetty en el servidor de NetWitness, inicie sesión en el host del servidor de NetWitness e ingrese el comando `service jetty restart`.

Problema	Solución
Cuando importa una lista en la cual faltan comillas en los elementos de la lista, como 172.16.0.0, la lista se guarda sin datos para mostrar. Esto se debe al error de Apache CSV-141, en el cual los archivos CSV con formatos incorrectos no se analizan.	Importe una lista con un uso correcto de comillas para evitar mostrar un archivo vacío. Por ejemplo, “172.16.0.0”, “host.mycompany.com”, etc.
El aumento del límite para alertas e incidentes produce un error en la búsqueda. De manera predeterminada, la cantidad de alertas e incidentes que se pueden ver se limita a 50.	Si se aumenta el límite, la mayor cantidad de metadatos buscados para alertas e incidentes puede producir un error en la búsqueda debido a una restricción interna de la base de datos. Para resolver esto, revierta la configuración predeterminada que limita a 50 la cantidad de alertas e incidentes que se pueden ver.