RSA NETWITNESS® SUITE

Guía de configuración de Context Hub

para la versión 11.0

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

febrero 2018

Contenido

5

Cómo funciona Context Hub 6

Descripción general de configuración de Context Hub 7

Configurar ajustes de orígenes de datos de Context Hub 8

Importar o exportar listas para Context Hub 13

Importar una lista 13

Importar lista de única columna 13

Importar valores a una lista existente 15

Exportar una lista para Context Hub 15

Configurar el mapeo de tipo de metadatos para Context Hub 17

Referencias de Context Hub 21

Pestaña Orígenes de datos de Context Hub 22

Flujo de trabajo 22

¿Qué desea hacer? 22

Temas relacionados 23

Vista rápida 23

Pestaña Listas de Context Hub 26

Flujo de trabajo 26

¿Qué desea hacer? 27

Temas relacionados 27

Vista rápida 27

Solución de problemas 31

Posibles problemas 31

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 Suite y proporcionan datos enriquecidos cuando se configuran.

Listas- 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.

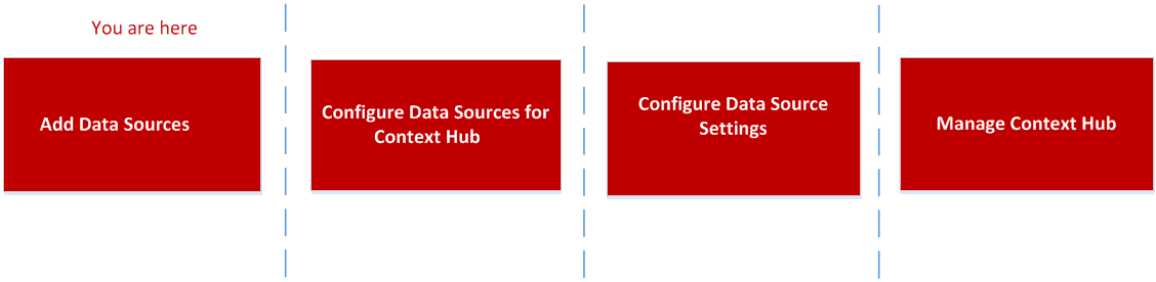
Respond: Proporciona información contextual de metadatos específicos disponible en Respond y permite que un analista responda más rápido en función de los datos de contexto.

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 **ADMIN**> **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 Suite.

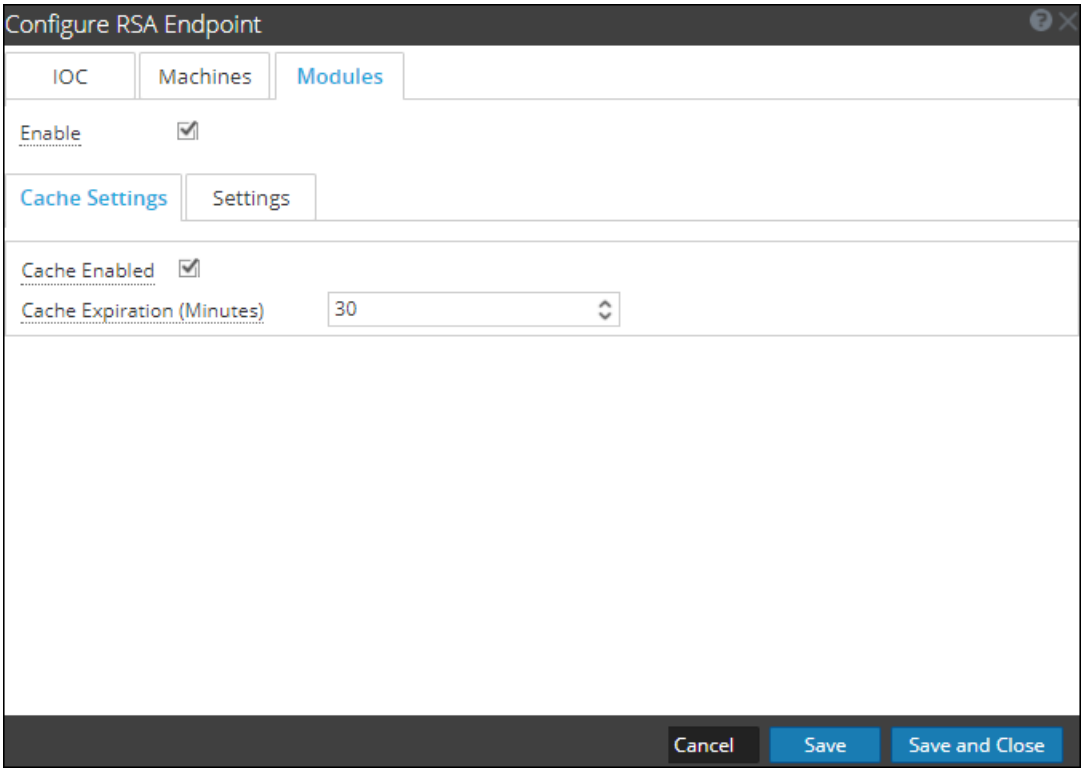
Nota: Solo puede tener una instancia del servicio Context Hub habilitada en su implementación de NetWitness Suite. Si hay varios servicios ESA en NetWitness Suite, debe elegir el host de ESA apropiado para Context Hub. Se requiere un mínimo de 8 GB de espacio para configurar Context Hub en el host de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

Configurar 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 al agregar el origen de datos de lista.
Puntaje de IIOC mínimo	El puntaje de IIOC mínimo que se considerará para buscar información contextual sobre los módulos de NetWitness Endpoint.

Campo	Descripción
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)

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

Origen de datos (conexión)	Grupos de respuestas compatibles	Configuración de campos
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)
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, que un analista puede usar. 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 Suite.

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

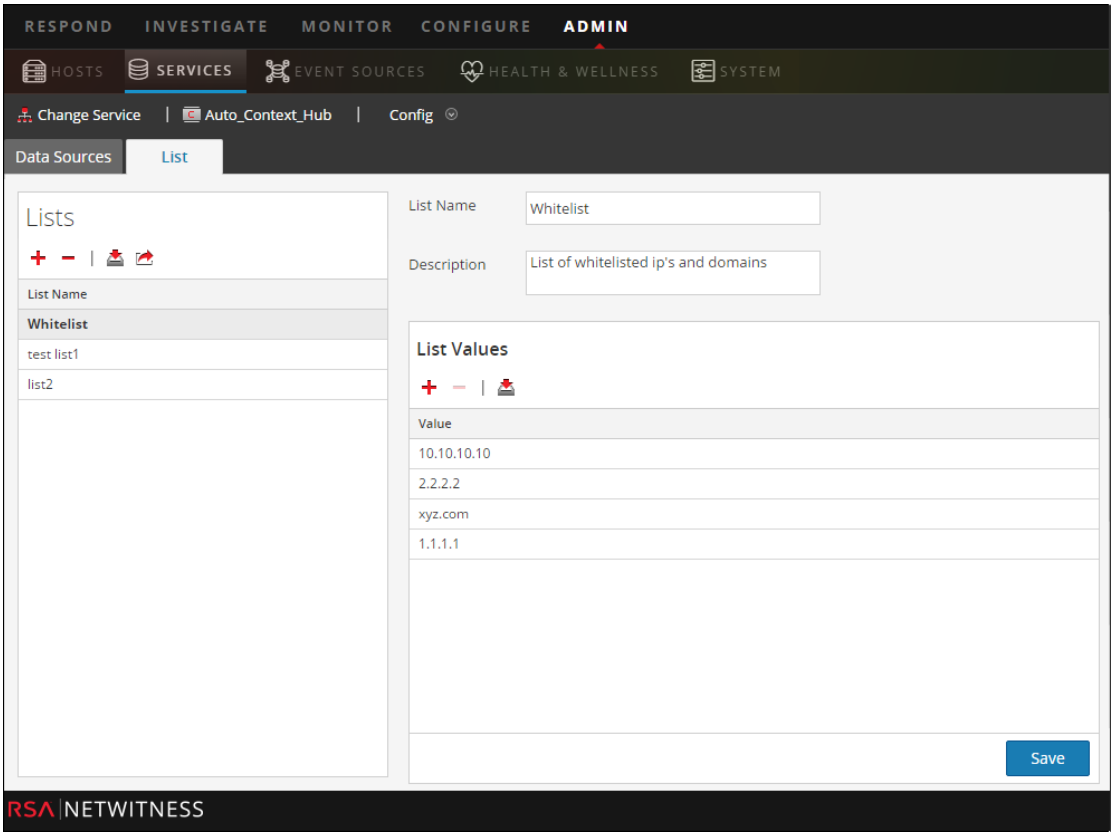
Nota: Debe hacer los mismos cambios al archivo .CSV pertinente, para que los cambios se vean reflejados la próxima vez que se repita el programa. De lo contrario, cuando importe valores a una lista de única columna existente o a una lista de múltiples columnas existente, los datos del archivo de origen se sobrescribirán la próxima vez que se repita el programa.

Importar lista de única columna

Para importa una lista:

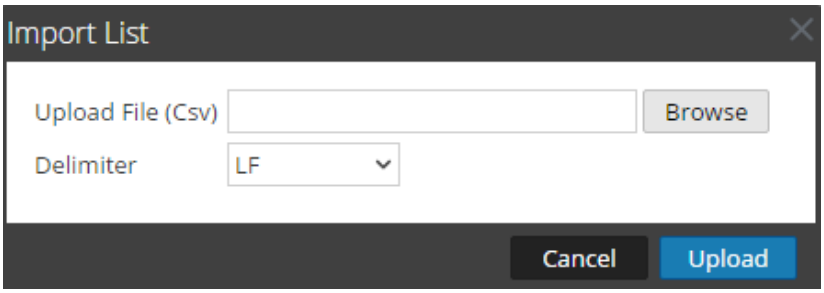
1. Seleccione ADMIN > **Servicios**.
   Se muestra la vista Servicios.
2. En el panel **Servicios**, seleccione el servicio Context Hub y haga clic en  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios del servicio Context Hub.
3. Haga clic en la pestaña **Listas**.
  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

La siguiente imagen es un ejemplo de lista de única columna.



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 importación. Para obtener información sobre cómo importar una lista de múltiples columnas, consulte Configurar el origen de datos Listas para Context Hub.

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 **ADMIN** > **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 Suite.

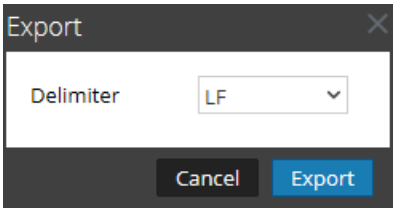
Los valores de lista se importan a la lista seleccionada. Estas listas se consideran orígenes de datos para la recuperación de información contextual. Pero puede anexar una lista de múltiples columnas existente. Los datos se agregarán solo si coinciden con el número de columnas.

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.

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 Suite 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 RESPOND.

En la vista **ADMIN**> **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

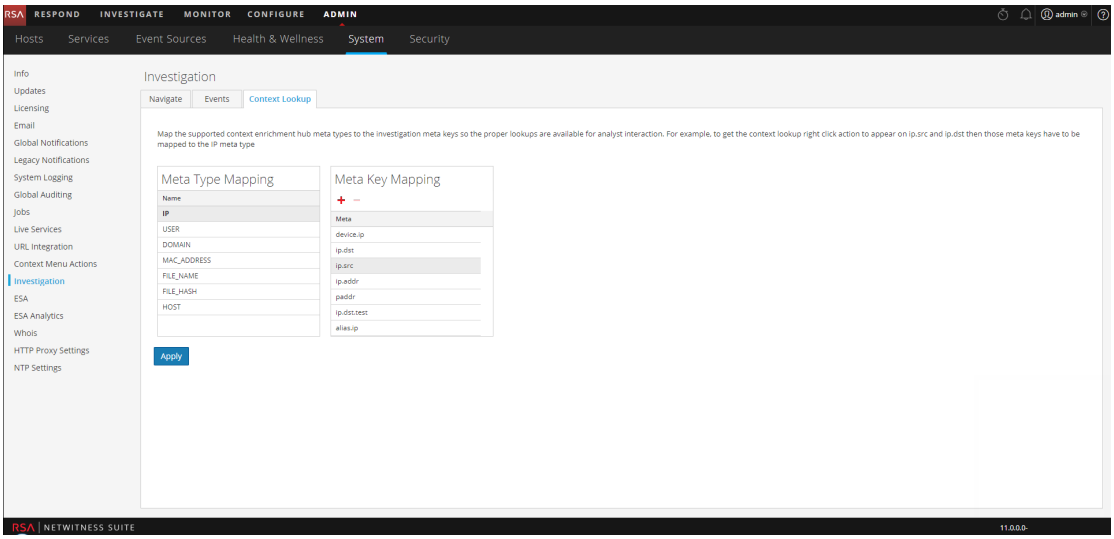
Nombre de tipo de metadatos	Claves de metadatos
HOST	device.host, alias.host, host.src, host.dst

Procedimiento

Para administrar el mapeo de claves de metadatos de Investigation:

1. Vaya a ADMIN > **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

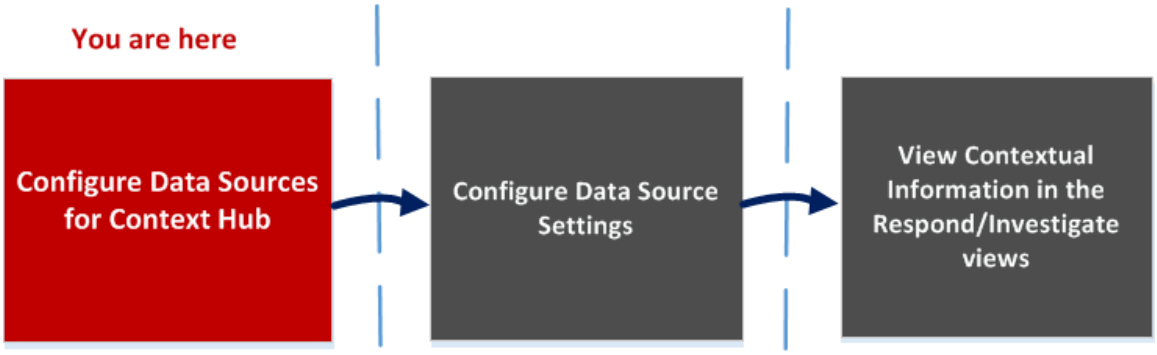
Después de configurar el servicio Context Hub y el origen de datos requerido, puede administrar la configuración para cada origen de datos. Todo esto ayudará a optimizar y personalizar los resultados de búsqueda.

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 orígenes de datos para Context Hub
Administrador	Configurar ajustes de datos de Context Hub*	Configurar ajustes de orígenes de datos de Context Hub

Función	Deseo…	Mostrarme cómo
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.*

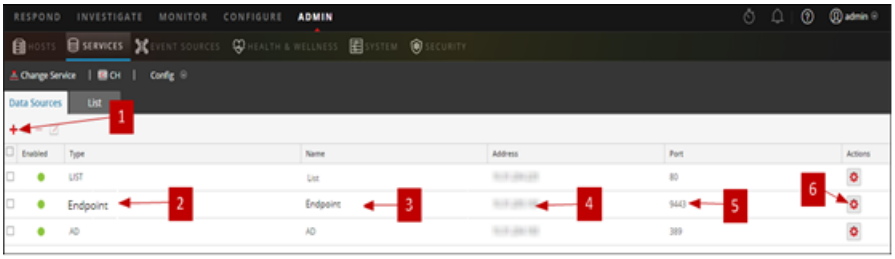
*Puede realizar esta tarea aquí (es decir, en la pestaña Orígenes de datos de Context Hub).

Temas relacionados

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

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 orígenes de datos para Context Hub.
	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 orígenes de datos para Context Hub.
	Abre el cuadro de diálogo Establecer configuración. Puede ver y editar la configuración de los orígenes de datos. Para conocer la descripción de cada campo del cuadro de diálogo Configurar respuestas, consulte Configurar ajustes de orígenes de datos.

Configuraciones de orígenes de datos

En la siguiente tabla se describen las configuraciones enumeradas.

Función	Descripción
Habilitado	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**.

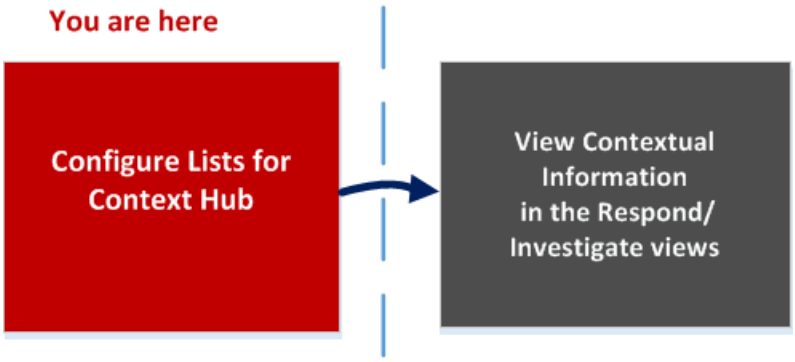
La pestaña Listas del servicio Context Hub permite crear una o más listas y agregar en ellas valores de lista pertinentes. Estas listas se consideran automáticamente como orígenes de datos para el servicio Context Hub.

Estas listas se pueden completar con elementos mediante la importación de archivos CSV 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 para Context Hub
Administrador/analista	Ver información contextual en la vista Respond	Consulte la *Guía del usuario de NetWitness Respond*.
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).

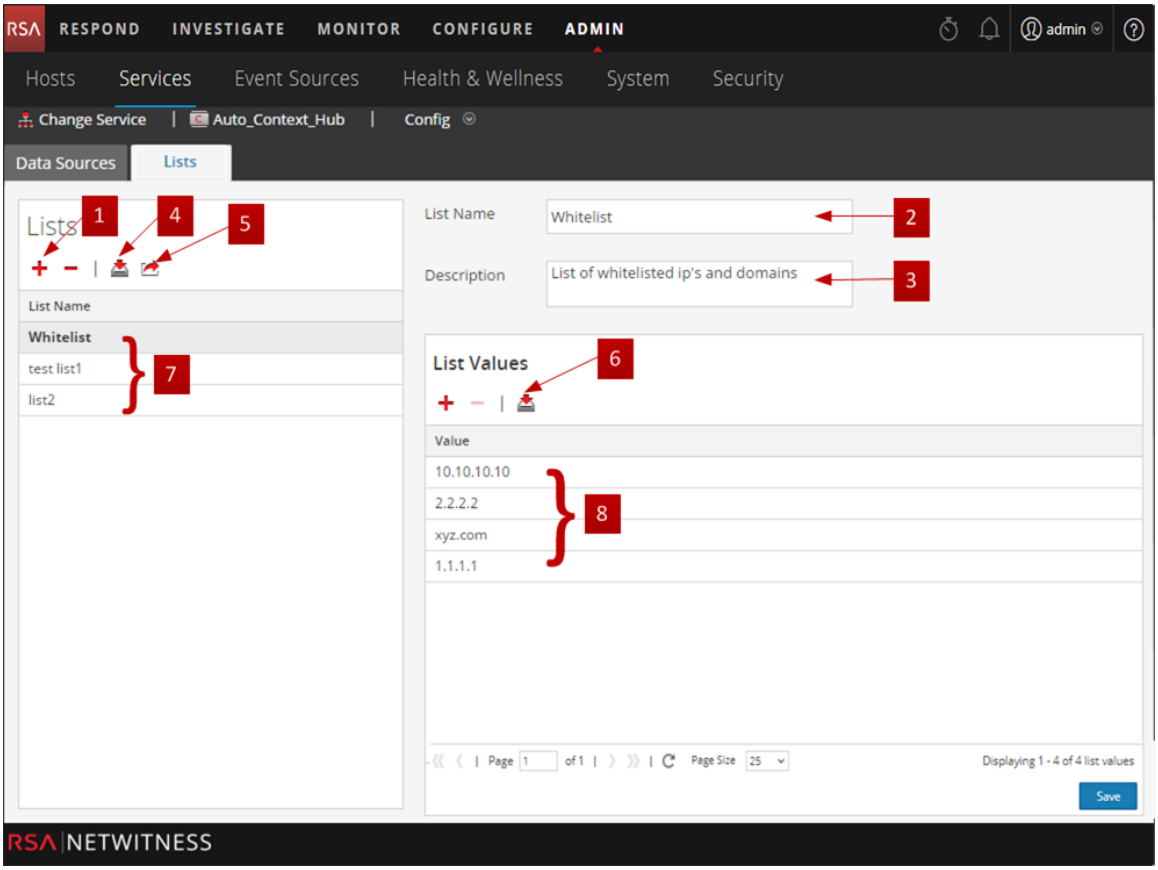
Temas relacionados

- Pestaña Orígenes de datos de Context Hub

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.
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	Muestra las listas personalizadas que se agregan a Context Hub.
8	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 los usuarios de NetWitness Suite pueden encontrar cuando configuran el servicio Context Hub en NetWitness Suite.

Posibles problemas

Problema	Soluciones
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 página Respond no navega al vínculo correcto.	Cuando detiene y reinicia el servidor de RabbitMQ, la opción Cambiar a Investigate disponible en la pantalla de Respond no está visible. Y el panel de contexto para Cambiar a Investigate vuelve a abrir la misma página. Debe reiniciar el servicio Jetty en el servidor de NetWitness, iniciar sesión en el host del servidor de NetWitness e ingresar el comando de reinicio del servicio Jetty.