



# Guía de configuración de NetWitness Respond

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](https://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

---

<b>Acerca de este documento</b> .....	<b>5</b>
Descripción general de la configuración de NetWitness Respond .....	5
<b>Configuración de NetWitness Respond</b> .....	<b>7</b>
Paso 1. Configurar orígenes de alertas para mostrar alertas en la vista Respond .....	8
Requisitos previos .....	8
Configurar Reporting Engine para mostrar alertas que activó Reporting Engine en la vista Respond .....	8
Configurar Malware Analytics para ver las alertas que activó Malware Analytics en la vista Respond .....	9
Configurar NetWitness Endpoint para ver las alertas que activó NetWitness Endpoint en la vista Respond .....	9
Configurar NetWitness Endpoint para mostrar alertas de NetWitness Endpoint .....	10
Paso 2. Asignar permisos de visualización de Respond .....	12
Servidor de Respond .....	13
Incidentes .....	15
Paso 3. Crear una regla de agregación para alertas .....	17
<b>Procedimientos adicionales para la configuración de Respond</b> .....	<b>19</b>
Configurar un período de retención para alertas e incidentes .....	19
Requisitos previos .....	20
Procedimiento .....	20
Resultado .....	21
Ocultar datos privados .....	22
Requisitos previos .....	22
Procedimiento .....	23
Administrar incidentes en NetWitness SecOps Manager .....	24
Requisitos previos .....	24
Procedimiento .....	24
Configurar el contador para alertas e incidentes con coincidencia .....	26
Configurar una base de datos para el servicio servidor de Respond .....	28
Requisitos previos .....	28
Procedimiento .....	28

<b>Referencia de la configuración de NetWitness Respond .....</b>	<b>31</b>
Vista Configurar .....	31
Pestaña Reglas de agregación .....	32
¿Qué desea hacer? .....	32
Temas relacionados .....	32
Reglas de agregación .....	32
Pestaña Nueva regla .....	35
¿Qué desea hacer? .....	35
Temas relacionados .....	35
Nueva regla .....	35

## Acerca de este documento

---

En esta guía se proporciona una descripción general de NetWitness Respond, instrucciones detalladas sobre cómo configurar NetWitness Respond en la red, procedimientos adicionales que se usan en otros momentos y materiales de referencia que describen la interfaz del usuario para configurar NetWitness Respond en la red.

### Temas

- [Descripción general de la configuración de NetWitness Respond](#)
- [Configuración de NetWitness Respond](#)
- [Procedimientos adicionales para la configuración de Respond](#)
- [Referencia de la configuración de NetWitness Respond](#)

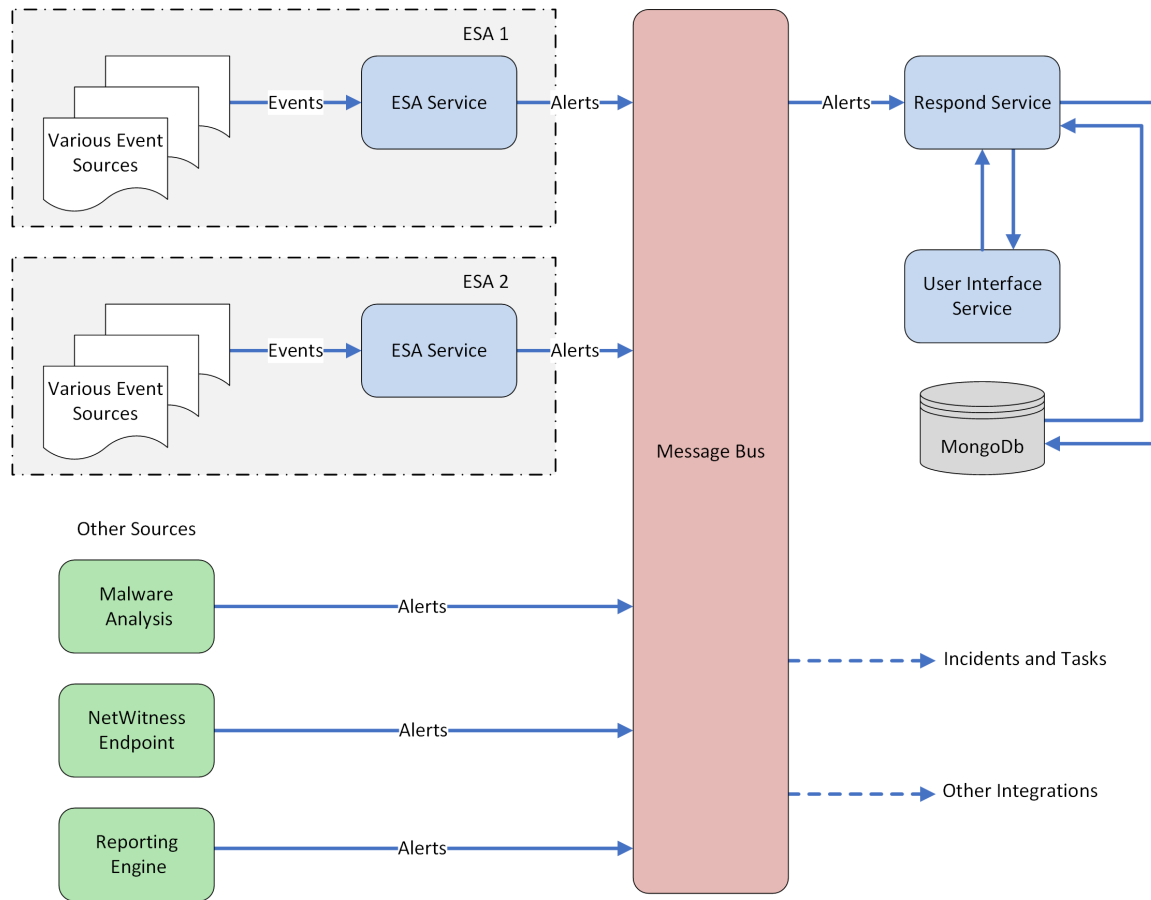
## Descripción general de la configuración de NetWitness Respond

RSA NetWitness® Suite NetWitness Respond consume datos de alerta de diversos orígenes a través del bus de mensajes y muestra estas alertas en la interfaz del usuario de NetWitness Suite. El Servicio servidor de Respond permite agrupar las alertas de manera lógica e iniciar un flujo de trabajo de NetWitness Respond para investigar y corregir los problemas de seguridad planteados.

El Servicio servidor de Respond consume alertas del bus de mensajes y normaliza los datos a un formato común (conservando los datos originales) para permitir un procesamiento más simple de las reglas. Ejecuta periódicamente las reglas para agregar múltiples alertas en un incidente y establecer algunos atributos del incidente (por ejemplo, severidad, categoría, etc.). Servicio servidor de Respond hace persistir los incidentes en MongoDB. Los incidentes también se publican en el bus de mensajes para que otros sistemas los consuman (por ejemplo, la integración de Archer).

**Nota:** NetWitness Respond requiere un servidor de ESA primario que contenga MongoDB. El servidor de Respond hace persistir los registros de alertas, incidentes y tareas en MongoDB.

En el siguiente diagrama se ilustra el flujo de alertas general.



Debe configurar diversos orígenes desde los cuales el Servicio servidor de Respond recopila y agrega las alertas.

## Configuración de NetWitness Respond

---

En este tema se proporcionan tareas generales necesarias para configurar el Servicio servidor de Respond. El administrador debe completar los pasos en la secuencia que se indica.

### Temas

- [Paso 1. Configurar orígenes de alertas para mostrar alertas en la vista Respond](#)
- [Paso 2. Asignar permisos de visualización de Respond](#)
- [Paso 3. Crear una regla de agregación para alertas](#)

## Paso 1. Configurar orígenes de alertas para mostrar alertas en la vista Respond

Este procedimiento es necesario para que las alertas de los orígenes de alertas se muestren en NetWitness Respond. Tiene la opción de habilitar o deshabilitar las alertas que se completan en la vista Respond. De forma predeterminada, esta opción está deshabilitada en Reporting Engine, Malware Analytics y NetWitness Endpoint, y solo está habilitada en Event Stream Analysis. Por lo tanto, cuando instala el Servicio servidor de Respond, debe habilitar esta opción en Reporting Engine, Malware Analytics y NetWitness Endpoint para completar las alertas correspondientes en la vista Respond.



### Requisitos previos

Garantice que:

- El Servicio servidor de Respond esté instalado y en ejecución en NetWitness Suite.
- Una base de datos esté configurada para el Servicio servidor de Respond.
- NetWitness Endpoint esté instalado y en ejecución.

### Configurar Reporting Engine para mostrar alertas que activó Reporting Engine en la vista Respond

De forma predeterminada, las alertas de Reporting Engine no se muestran en la vista Respond. Para mostrar y ver las alertas de Reporting Engine, debe habilitar las alertas de NetWitness Respond en la vista Configuración de servicios > pestaña General para Reporting Engine.

1. Vaya a **ADMIN > Servicios**, seleccione un servicio Reporting Engine y elija   > **Ver > Configuración**.

La vista Configuración de servicios se muestra con la pestaña General de Reporting Engine abierta.

2. Seleccione **Configuración del sistema**.
3. Seleccione la casilla de verificación **Reenviar alertas a Respond**.  
Reporting Engine ahora reenvía las alertas a NetWitness Respond.

Para obtener detalles acerca de los parámetros de la pestaña General, consulte el tema “Pestaña General de Reporting Engine” de la *Guía de configuración de Reporting Engine*.



## Configurar Malware Analytics para ver las alertas que activó Malware Analytics en la vista Respond

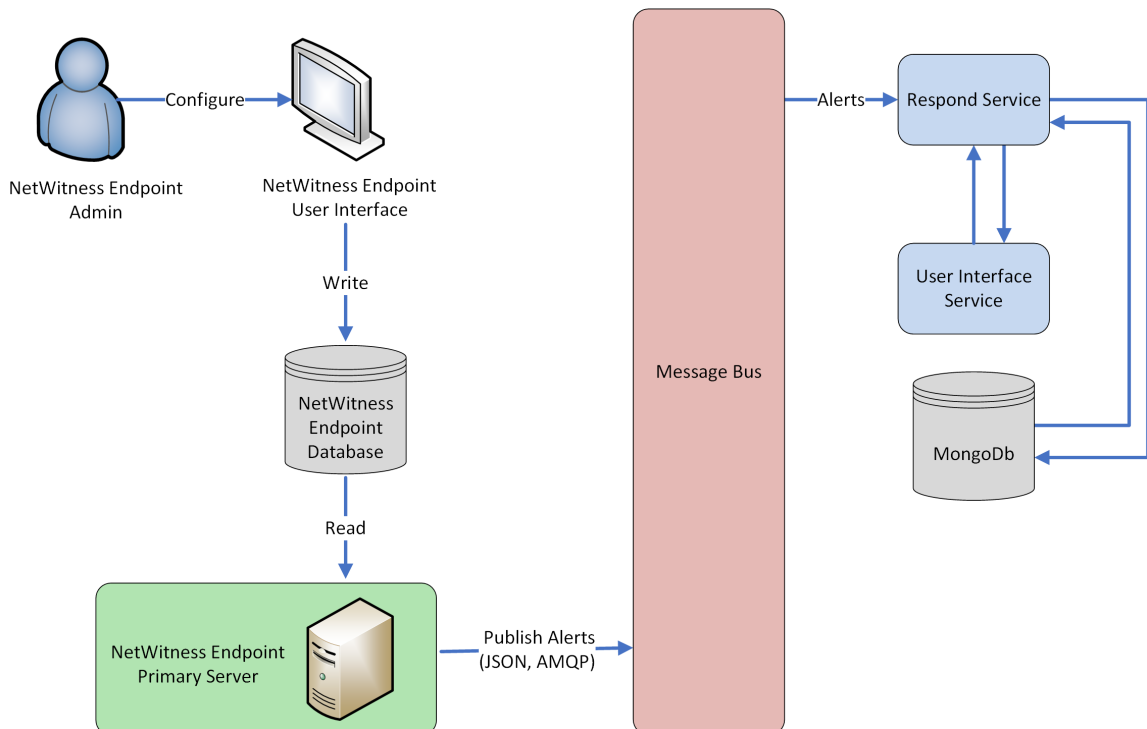
La visualización de alertas de NetWitness Respond es una función de auditoría en Malware Analysis. El procedimiento para habilitar alertas de NetWitness Respond se describe en el tema “(Opcional) Configurar la auditoría en un host de Malware Analysis” de la *Guía de configuración de Malware Analysis*.

## Configurar NetWitness Endpoint para ver las alertas que activó NetWitness Endpoint en la vista Respond

Este procedimiento se requiere para integrar NetWitness Endpoint con NetWitness Suite de modo que el componente NetWitness Respond de NetWitness Suite recopile las alertas de NetWitness Endpoint y las muestre en la vista **RESPOND > Alertas**.

**Nota:** RSA es compatible con NetWitness Endpoint versiones 4.3.0.4, 4.3.0.5 o superior para la integración de NetWitness Respond. Para obtener información detallada, consulte el tema “Integración de RSA NetWitness Suite” en la *Guía del usuario de NetWitness Endpoint*.

En el siguiente diagrama se representa el flujo de alertas de NetWitness Endpoint al NetWitness Suite Servicio servidor de Respond y su visualización en la vista **RESPOND > Alertas**.

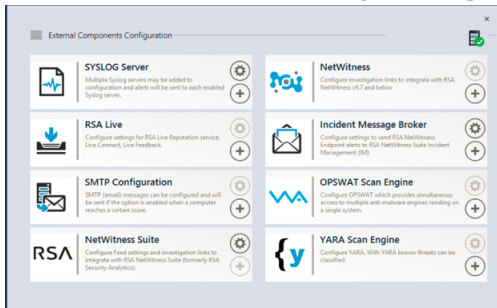


## Configurar NetWitness Endpoint para mostrar alertas de NetWitness Endpoint

Para configurar NetWitness Endpoint de manera que muestre alertas de NetWitness Endpoint en la interfaz del usuario de NetWitness Suite:

1. En la interfaz del usuario de NetWitness Endpoint, haga clic en **Configurar > Monitoreo y componentes externos**.

Se muestra el cuadro de diálogo **Configuración de componentes externos**.



2. En los componentes enumerados, seleccione **Intermediador de mensajes de incidentes** y haga clic en + para agregar un nuevo intermediador de IM.
3. Ingrese los siguientes campos:
  - a. **Nombre de instancia:** Escriba un nombre único para identificar al intermediador de IM.
  - b. **Nombre de host o dirección IP del servidor:** Escriba la dirección IP o el DNS del host del intermediador de IM (Servidor de NetWitness).
  - c. **Número de puerto:** El puerto predeterminado es 5671.
4. Haga clic en **Guardar**.
5. Navegue al archivo **ConsoleServer.exe.Config** en **C:\Program Files\RSA\ECAT\Server**.
6. Modifique las configuraciones del host virtual en el archivo de la siguiente manera:
 

```
<add key="IMVirtualHost" value="/rsa/system" />
```

**Nota:** En NetWitness Suite 11.0, el host virtual es “/rsa/system”. En la versión 10.6.x y anteriores, el host virtual es “/rsa/sa”.

7. Reinicie el servidor de API y de la consola.
8. Para configurar SSL para las alertas de Respond, realice los siguientes pasos en el servidor de la consola primaria de NetWitness Endpoint con el fin de establecer las comunicaciones de SSL:

- a. Exporte el certificado de CA de NetWitness Endpoint al formato .CER (X.509 con codificación Base 64) desde el almacén de certificados personales de la computadora local (sin seleccionar la clave privada).
- b. Genere un certificado de cliente para NetWitness Endpoint mediante el certificado de CA de NetWitness Endpoint. (DEBE configurar Nombre de CN en ecat).

```
makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NWECA" -is MY -ir LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -cy end -sy 12 client.cer
```

**Nota:** En el código de ejemplo anterior, si actualizó a Endpoint versión 4.3 desde una versión anterior y no generó nuevos certificados, debe sustituir “EcatCA” por “NWECA”.

- c. Tome nota de la huella digital del certificado de cliente que se generó en el paso b. Ingrese el valor de la huella digital del certificado de cliente en la sección IMBrokerClientCertificateThumbprint del archivo ConsoleServer.Exe.Config como se muestra.

```
<add key="IMBrokerClientCertificateThumbprint" value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```
9. En el Servidor de NetWitness, copie el archivo de certificado de CA de NetWitness Endpoint en formato .CER en la carpeta de importación:

```
/etc/pki/nw/trust/import
```
10. Emita el siguiente comando para iniciar la ejecución de Chef necesaria:

```
orchestration-cli-client --update-admin-node
```

Esto agrega todos esos certificados al almacén de confianza.
11. Reinicie el servidor de RabbitMQ:

```
systemctl restart rabbitmq-server
```

La cuenta de NetWitness Endpoint debe estar disponible en RabbitMQ de forma automática.
12. Importe los archivos `/etc/pki/nw/ca/nwca-cert.pem` y `/etc/pki/nw/ca/ssca-cert.pem` desde Servidor de NetWitness y agréguelos a los almacenes de Certificación raíz de confianza en el servidor de Endpoint.

## Paso 2. Asignar permisos de visualización de Respond

Agregue usuarios con los permisos requeridos para investigar los incidentes y las alertas en NetWitness Respond. Los usuarios con acceso a la vista Respond necesitan permisos de Incidentes y de Servidor de Respond.

Las siguientes funciones preconfiguradas tienen permisos en la vista Respond:

- **Analistas:** Los Analistas del centro de operaciones de seguridad (SOC) tienen acceso a Alerting, NetWitness Respond, Investigation y Reporting, pero no a las configuraciones del sistema.
- **Analistas de malware:** Los Analistas de malware tienen acceso a los eventos de investigaciones y malware.
- **Operadores:** Los Operadores tienen acceso a las configuraciones, pero no a Investigation, ESA, Alerting, Reporting y NetWitness Respond.
- **SOC\_Managers:** Los administradores del SOC tienen el mismo acceso que poseen los analistas, además de los permisos adicionales para manejar incidentes y configurar NetWitness Respond.
- **Data\_Privacy\_Officers:** Los Encargados de la privacidad de datos (DPO) cumplen una función similar a la de los Administradores, pero tienen un enfoque adicional en opciones de configuración que administran el ocultamiento y la visualización de datos confidenciales dentro del sistema. Consulte *Administración de la privacidad de datos* para obtener información adicional.
- **Respond\_Administrator:** El Administrador de Respond tiene acceso completo a NetWitness Respond.
- **Administradores:** Los Administradores tienen acceso completo al sistema a NetWitness Suite y cuentan con todos los permisos de manera predeterminada.

Los permisos predeterminados de NetWitness Respond se muestran en las siguientes tablas. Debe asignar permisos de usuario desde las pestañas **Incidentes** y **Servidor de Respond**, que son los nombres de la pestaña Permisos en los cuadros de diálogo Agregar o Editar funciones de la vista ADMIN > Seguridad. Es posible agregar permisos de usuario adicionales para Alerting, Context Hub, Investigate, Servidor de Investigate y Reports.

## Servidor de Respond

Permisos	Analistas	Administradores de SOC	DP O	Administradores de Respond	Operadores	M A
respond-server.alert.delete			Sí*	Sí*		
respond-server.alert.manage	Sí	Sí	Sí*	Sí*		Sí
respond-server.alert.read	Sí	Sí	Sí*	Sí*		Sí
respond-server.alertrule.manage		Sí	Sí*	Sí*		
respond-server.alertrule.read		Sí	Sí*	Sí*		
respond-server.configuration.manage			Sí*	Sí*		
respond-server.health.read			Sí*	Sí*		
respond-server.incident.delete			Sí*	Sí*		
respond-server.incident.manage	Sí	Sí	Sí*	Sí*		Sí
respond-server.incident.read	Sí	Sí	Sí*	Sí*		Sí

Permisos	Analistas	Administradores de SOC	DP O	Administradores de Respond	Operadores	M A
respond-server.journal.manage	Sí	Sí	Sí*	Sí*		Sí
respond-server.journal.read	Sí	Sí	Sí*	Sí*		Sí
respond-server.logs.manage			Sí*	Sí*		
respond-server.metrics.read			Sí*	Sí*		
respond-server.process.manage			Sí*	Sí*		
respond-server.remediation.manage	Sí	Sí	Sí*	Sí*		Sí
respond-server.remediation.read	Sí	Sí	Sí*	Sí*		Sí
respond-server.security.manage			Sí*	Sí*		
respond-server.security.read			Sí*	Sí*		

\* Los Encargados de la privacidad de datos y los Administradores de Respond tienen el permiso **responder-server.\***, que les otorga todos los permisos del servidor de Respond.

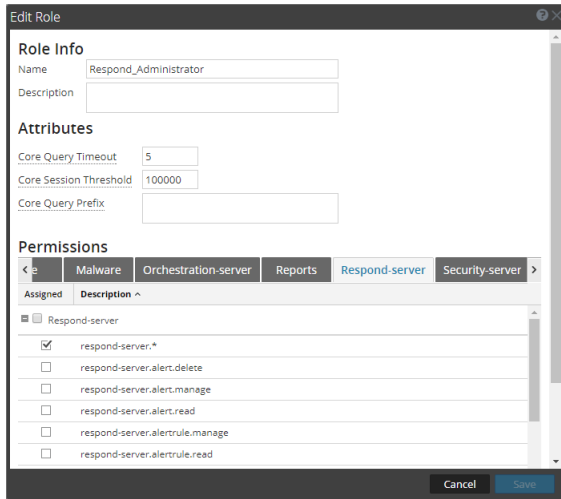
## Incidentes

Permisos	Analistas	Administradores de SOC	DP O	Administradores de Respond	Operadores	M A
Acceder al módulo Incident	Sí	Sí	Sí	Sí		Sí
Configuración de la integración de Incident Management		Sí	Sí	Sí		
Eliminar alertas e incidentes			Sí	Sí		
Administración de las reglas del manejo de alertas		Sí	Sí	Sí		
Ver y administrar incidentes	Sí	Sí	Sí	Sí		Sí

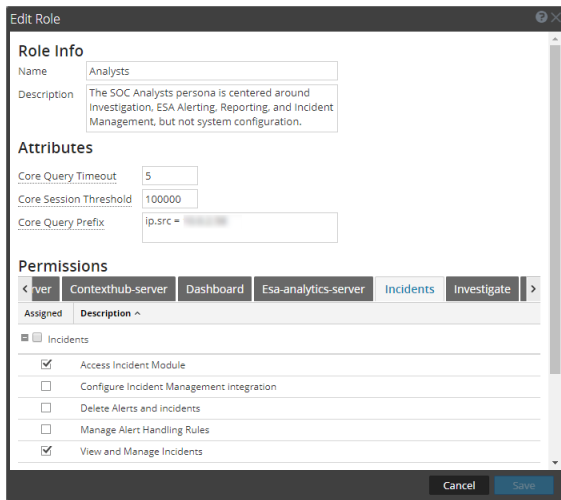
El Administrador de Respond tiene todos los permisos de Servidor de Respond e Incidentes.

**Precaución:** Es muy importante que asigne los permisos de usuario equivalentes TANTO desde la pestaña Servidor de Respond COMO desde la pestaña Incidentes.

En la siguiente figura se muestran los permisos de Servidor de Respond para la función Administrador de Respond predeterminada. La función Administrador de Respond contiene todos los permisos de NetWitness Respond.



En la siguiente figura se muestran los permisos de incidentes para la función Analistas predeterminada:



Para obtener más información, consulte “Permisos de funciones” y “Administrar usuarios con funciones y permisos” en la guía *Administración de usuarios y de la seguridad del sistema*.



### Paso 3. Crear una regla de agregación para alertas

Puede crear reglas de agregación con diversos criterios para automatizar el proceso de creación de incidentes. Las alertas que cumplen con los criterios de la regla se agrupan para formar un incidente. Esto es útil cuando se sabe que un conjunto específico de alertas se puede agrupar en un incidente y se puede configurar una regla de agregación que se encargue de agrupar las alertas en lugar de desperdiciar tiempo en crear manualmente un incidente y agregar en él las alertas de manera individual. Para crear incidentes automáticamente, debe crear una regla de agregación.

Para crear una regla de agregación:

1. Vaya a **CONFIGURAR > Reglas de incidentes**.

Se muestra la vista **Reglas de agregación**.

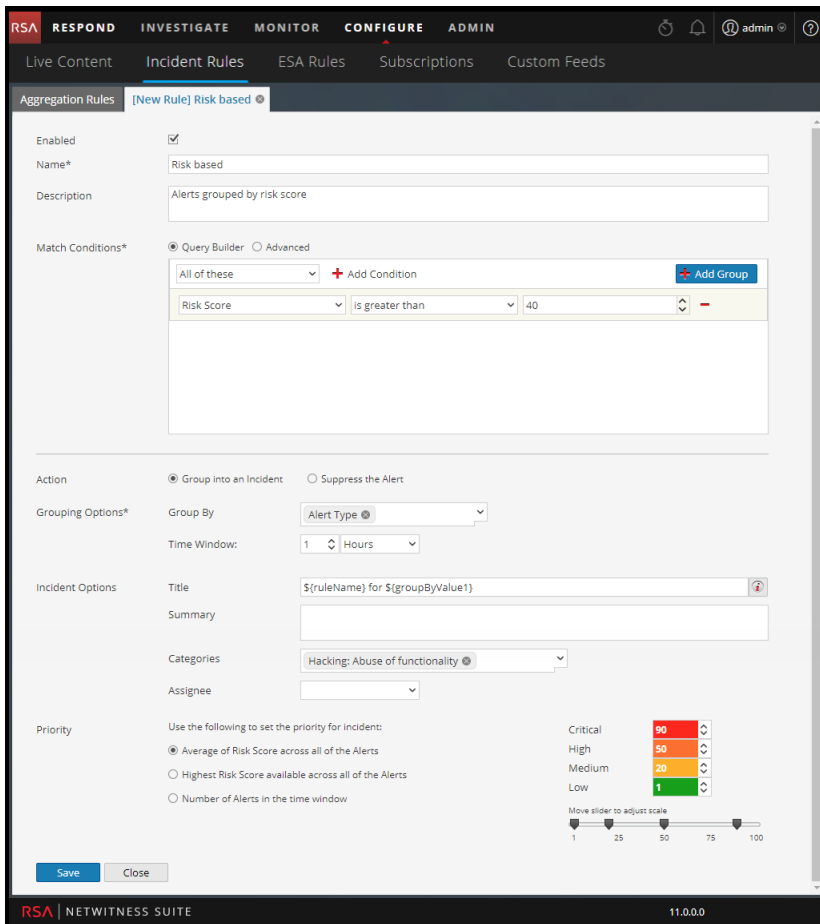
	Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
<input type="checkbox"/>	1	●	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication wi...		0	0
<input type="checkbox"/>	2	●	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA ...		0	0
<input type="checkbox"/>	3	●	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA ...		0	0
<input type="checkbox"/>	4	●	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA ...	2017-08-11 18:2...	2510	62
<input type="checkbox"/>	5	●	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ...	2017-08-12 20:0...	105464	1236
<input type="checkbox"/>	6	●	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addr...		0	0
<input type="checkbox"/>	7	●	User Watch List: Activity Detected	This incident rule captures alerts generated by network ...		0	0
<input type="checkbox"/>	8	●	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of w...		0	0
<input type="checkbox"/>	9	●	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common l...		0	0
<input type="checkbox"/>	10	●	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert desig...		0	0
<input type="checkbox"/>	11	●	Web Threat Detection	This incident rule captures alerts generated by the RSA ...		0	0

Se muestra una lista de 11 reglas predefinidas. Puede realizar una de las siguientes acciones:

- agregar una regla nueva
  - editar una regla existente
  - clonar una regla
2. Para agregar una nueva regla, seleccione **+**.

Se muestra la pestaña **Nueva regla**.

En el siguiente ejemplo se muestra la agrupación de alertas en un incidente en función del puntaje de riesgo.



### 3. Haga clic en **Guardar**.

La regla se muestra en la pestaña **Reglas de agregación**. La regla se activa y comienza a crear incidentes de acuerdo con las alertas entrantes que coinciden con los criterios seleccionados.

#### Consulte también:

- Para obtener detalles sobre los diversos parámetros que se pueden configurar como criterios para una regla de agregación, consulte [Pestaña Nueva regla](#).
- Para obtener detalles sobre las descripciones de los parámetros y los campos en la pestaña Reglas de agregación, consulte [Pestaña Reglas de agregación](#).

## Procedimientos adicionales para la configuración de Respond

---

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

- [Configurar un período de retención para alertas e incidentes](#)
- [Ocultar datos privados](#)
- [Administrar incidentes en NetWitness SecOps Manager](#)
- [Configurar el contador para alertas e incidentes con coincidencia](#)
- [Configurar una base de datos para el servicio servidor de Respond](#)

### Configurar un período de retención para alertas e incidentes

En ocasiones, los encargados de la privacidad de datos desean conservar datos durante cierto periodo y después eliminarlos. Un periodo de retención más breve libera espacio en disco antes. En algunos casos, el periodo de retención debe ser breve. Por ejemplo, las leyes de Europa establecen que los datos confidenciales no se pueden conservar durante más de 30 días. Después de 30 días, los datos se deben ocultar o eliminar.

La configuración de un periodo de retención para los datos es un procedimiento opcional. El momento en que NetWitness Respond recibe alertas y crea un incidente determina cuándo comienza la retención. Los periodos de retención varían entre 30 y 365 días. Si configura un periodo de retención, los datos se eliminan de manera definitiva un día después de la finalización del periodo.

La retención se basa en el momento en que NetWitness Respond recibe las alertas y en la hora de creación del incidente.

**Precaución:** Los datos que se eliminan después del periodo de retención no se pueden recuperar.

Cuando vence el periodo de retención, los siguientes datos se **eliminan de manera definitiva**:

- Alertas
- Incidentes
- Tareas
- Entradas del registro

Los registros rastrean la retención y la eliminación manual, de modo que pueda ver lo que se ha eliminado. Puede ver los registros del Servidor de Respond en las siguientes ubicaciones:


- **Registro de servicio de Servidor de Respond:** /var/log/netwitness/respond-server/respond-server.log
- **Registro de auditoría de Servidor de Respond:** /var/log/netwitness/respond-server/respond-server.audit.log

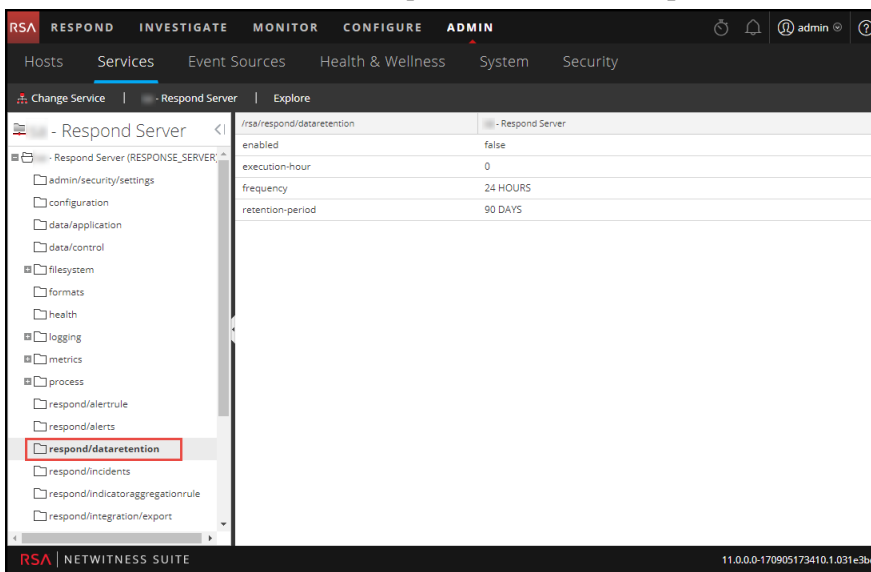
El período de retención de datos que configuró aquí no se aplica a Archer ni a otras herramientas de SOC de otros fabricantes. Las alertas y los incidentes de otros sistemas se deben eliminar por separado.

## Requisitos previos

Se le debe asignar la función de administrador.

## Procedimiento

1. Vaya a **ADMIN > Servicios**, seleccione Servicio servidor de Respond y elija  > **Ver > Explorar**.
2. En la lista de nodos de la vista Explorar, seleccione **respond/dataretention**.



3. En el campo **habilitado**, seleccione **verdadero** para eliminar las alertas y los incidentes más antiguos que el período de retención.

El programador se ejecuta cada 24 horas a las 23:00 h.

Verá un aviso que indica que la configuración se actualizó correctamente.

4. En el campo **retention-period**, escriba la cantidad de días que se conservarán los incidentes y las alertas. Por ejemplo, escriba 30 DÍAS, 60 DÍAS, 90 DÍAS, 120 DÍAS, 365 DÍAS o cualquier cantidad de días.

Verá un aviso que indica que la configuración se actualizó correctamente.

## **Resultado**

24 horas después del fin del período de retención, el programador elimina de manera definitiva de NetWitness Respond todas las alertas y los incidentes más antiguos que el período especificado. Las entradas del registro y las tareas de corrección asociadas a los incidentes eliminados también se eliminan.

## Ocultar datos privados

La función Encargado de la privacidad de datos (DPO) puede identificar claves de metadatos que contienen datos confidenciales y que deben mostrar datos ocultos. En este tema se explica la forma en que el administrador mapea esas claves de metadatos para mostrar un valor al que se aplicó hash en lugar del valor real.

Para los valores de metadatos a los cuales se aplicó hash se aplican las siguientes advertencias:

- NetWitness Suite es compatible con dos métodos de almacenamiento para valores de metadatos a los cuales se aplicó hash, hexadecimal (predeterminado) y cadena.
- Cuando una clave de metadatos está configurada para mostrar un valor al cual se aplicó hash, todas las funciones de seguridad ven únicamente el valor con hash en el módulo Incidentes.
- Los valores a los cuales se aplicó hash se usan de la misma manera en que se usan los valores reales. Por ejemplo, cuando usa un valor al cual se aplicó hash en criterios de regla, los resultados son los mismos que si usa el valor real.

En este tema se explica cómo ocultar datos privados en NetWitness Respond. Consulte el tema **Descripción general de la administración de la privacidad de datos** en la guía *Administración de la privacidad de datos* para obtener información adicional acerca de la privacidad de datos.

### Archivo de mapeo para ocultar claves de metadatos

En NetWitness Respond, el archivo de mapeo para el ocultamiento de datos es `data_privacy_map.js`. En él, se escribe un nombre de clave de metadatos oculta y se mapea al nombre de clave de metadatos real.

En el siguiente ejemplo se muestran los mapeos para ocultar datos de dos claves de metadatos, `ip.src` y `user.dst`:

```
'ip.src.hash' : 'ip.src',  
'user.dst.hash' : 'user.dst'
```

Usted determina la convención de asignación de nombres para los nombres de claves de metadatos ocultas. Por ejemplo, `ip.src.hash` podría ser `ip.src.private` o `ip.src.bin`. Debe elegir una convención de asignación de nombres y usarla coherentemente en todos los hosts.

### Requisitos previos

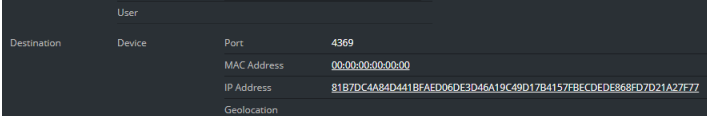
- La función DPO debe especificar qué claves de metadatos requieren ocultamiento de datos.
- La función de administrador debe mapear las claves de metadatos para el ocultamiento de datos.

## Procedimiento

1. Abra el archivo de mapeo de privacidad de datos:  
`/var/lib/netwitness/respond-server/scripts/data_privacy_map.js`
2. En la variable `obfuscated_attribute_map`, escriba el nombre de una clave de metadatos que tendrá datos ocultos. A continuación, mápela a la clave de metadatos que no contiene datos ocultos de acuerdo con este formato:  
`'ip.src.hash' : 'ip.src'`
3. Repita el paso 2 para cada clave de metadatos que deba mostrar un valor al cual se aplicó hash.
4. Use la misma convención de asignación de nombres que en el paso 2 y aplíquela coherentemente en todos los hosts.
5. Guarde el archivo  
.Todas las claves de metadatos mapeadas mostrarán valores a los cuales se aplicó hash en lugar de valores reales.

En la siguiente figura, un valor al cual se aplicó hash muestra la dirección IP de destino en

Detalles de eventos:



User	
Destination	Port 4369
Device	MAC Address 00:00:00:00:00:00
	IP Address 81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBCED0E6868FD7D21A27E77
	Geolocation

Las nuevas alertas mostrarán datos ocultos.

**Nota:** Las alertas existentes continuarán mostrando datos confidenciales. Este procedimiento no es retroactivo.

## Administrar incidentes en NetWitness SecOps Manager

Si desea administrar incidentes en RSA NetWitness® SecOps Manager en lugar de NetWitness Respond, debe configurar los ajustes de integración de sistemas en la vista Explorar del Servicio servidor de Respond. Después de configurar Configuración de integración de sistemas, todos los incidentes se administran en NetWitness SecOps Manager. Los incidentes que se crearon antes de la integración no se administrarán en NetWitness SecOps Manager.


**Precaución:** Si está administrando incidentes en NetWitness SecOps Manager en lugar de NetWitness Respond, no use lo siguiente en la vista Respond: vista Lista de incidentes, vista Detalles de incidente y vista Lista de tareas. No cree incidentes desde la vista Lista de alertas de Respond o desde Investigate.

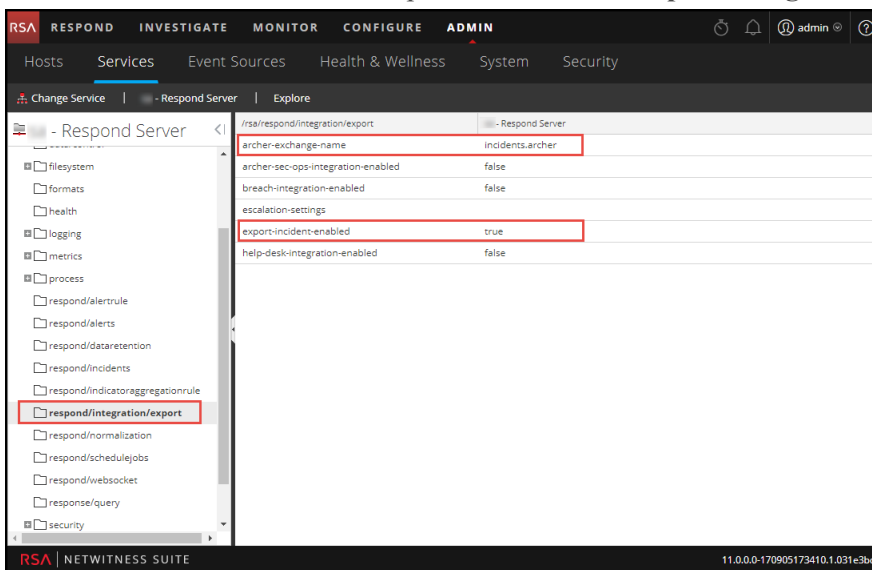
### Requisitos previos

- NetWitness SecOps Manager 1.3.1.2 (NetWitness Suite 11.0 solamente funcionará con NetWitness SecOps Manager 1.3.1.2).

### Procedimiento

Siga este procedimiento para configurar los ajustes del servicio servidor de Respond para administrar incidentes en NetWitness SecOps Manager.

1. Vaya a **ADMIN > Servicios**, seleccione Servicio servidor de Respond y elija  > **Configuración > Explorar**.
2. En la lista de nodos de la vista Explorar, seleccione **respond/integration/export**.





3. En el campo **archer-exchange-name**, escriba NetWitness SecOps Manager exchange name.  
Verá un aviso que indica que la configuración se actualizó correctamente.
4. En el campo **archer-sec-ops-integration-enabled**, seleccione **verdadero**.  
Verá un aviso que indica que la configuración se actualizó correctamente.  
Los incidentes se administrarán exclusivamente en NetWitness SecOps Manager.

## Configurar el contador para alertas e incidentes con coincidencia

Este procedimiento es opcional. Los administradores pueden usarlo para cambiar el momento en el cual el conteo de alertas con coincidencia se restablece a 0. La pestaña Reglas de agregación muestra estos conteos en las columnas de la derecha.

Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
1	●	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication wi...		0	0
2	●	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA ...		0	0
3	●	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA ...		0	0
4	●	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA ...	2017-08-11 18:2...	2510	62
5	●	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ...	2017-08-12 20:0...	105464	1236
6	●	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addre...		0	0
7	●	User Watch List: Activity Detected	This incident rule captures alerts generated by network ...		0	0
8	●	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of w...		0	0
9	●	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common l...		0	0
10	●	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert desig...		0	0
11	●	Web Threat Detection	This incident rule captures alerts generated by the RSA ...		0	0

En estas columnas se proporciona la siguiente información para una regla:

- La columna **Última coincidencia** muestra la hora en que la regla coincidió por última vez con alertas.
- La columna **Alertas con coincidencia** muestra la cantidad de alertas con coincidencia para la regla.
- La columna **Incidentes** muestra la cantidad de incidentes que creó la regla.

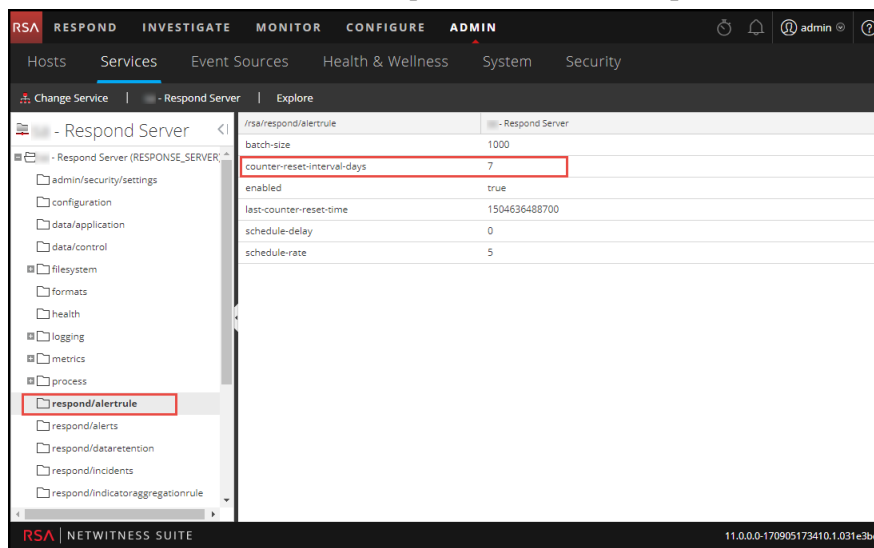
De manera predeterminada, estos valores se restablecen a cero cada siete días. Según el tiempo durante el cual desea que continúen los conteos, puede cambiar la cantidad predeterminada de días.


**Nota:** Cuando el contador se restablece a cero, solo los números de las tres columnas cambian a cero. No se elimina ninguna alerta ni incidente.

### Para configurar un contador para alertas e incidentes con coincidencia:

1. Vaya a **ADMIN > Servicios**, seleccione Servicio servidor de Respond y elija  > **Ver > Explorar**.

2. En la lista de nodos de la vista Explorar, seleccione **respond/alertrule**.



3. En el panel de la derecha, escriba la cantidad de días en el campo **counter-reset-interval-days**.
4. Reinicie el Servicio servidor de Respond para que se aplique la nueva configuración. Para hacerlo, vaya a **ADMIN > Servicios**, seleccione el Servicio servidor de Respond y elija  > **Reiniciar**.

## Configurar una base de datos para el servicio servidor de Respond


Este procedimiento se requiere solo si necesita cambiar la configuración de la base de datos para el servidor de Respond después de la implementación de los hosts de NetWitness o ESA primario y sus servicios correspondientes. Tiene que seleccionar el servidor de ESA primario para que actúe como el host de base de datos para los datos de las aplicaciones de NetWitness Respond, como alertas, incidentes y tareas. También debe seleccionar el servidor de NetWitness para que actúe como el host de base de datos para los datos de control de NetWitness Respond, como reglas de agregación y categorías.

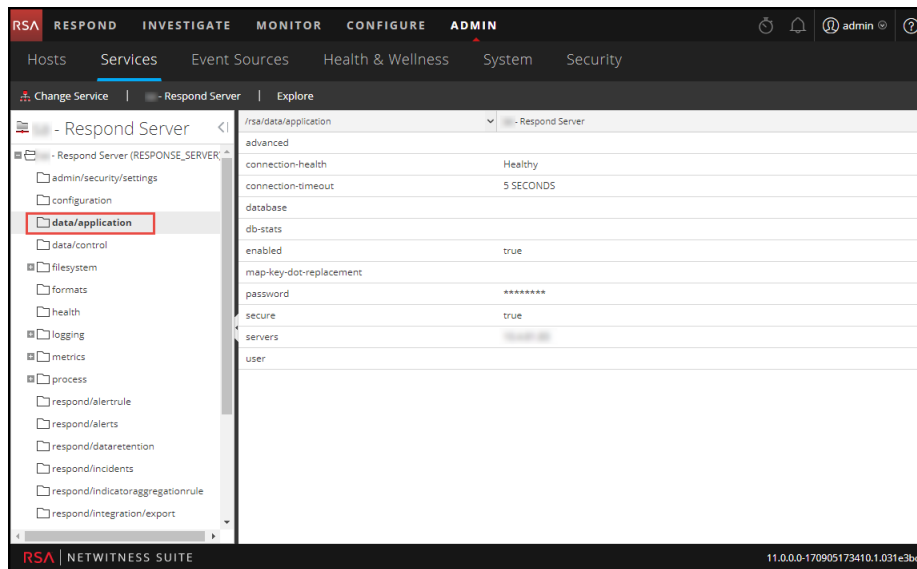
### Requisitos previos

Garantice que:

- Haya instalado un host en el cual desea ejecutar el Servicio servidor de Respond. Consulte “Paso 1: Implementar un host” de la *Guía de introducción de hosts y servicios* para conocer el procedimiento necesario para agregar un host.
- El Servicio servidor de Respond esté instalado y en ejecución en NetWitness Suite.
- Un host de ESA esté instalado y configurado.

### Procedimiento

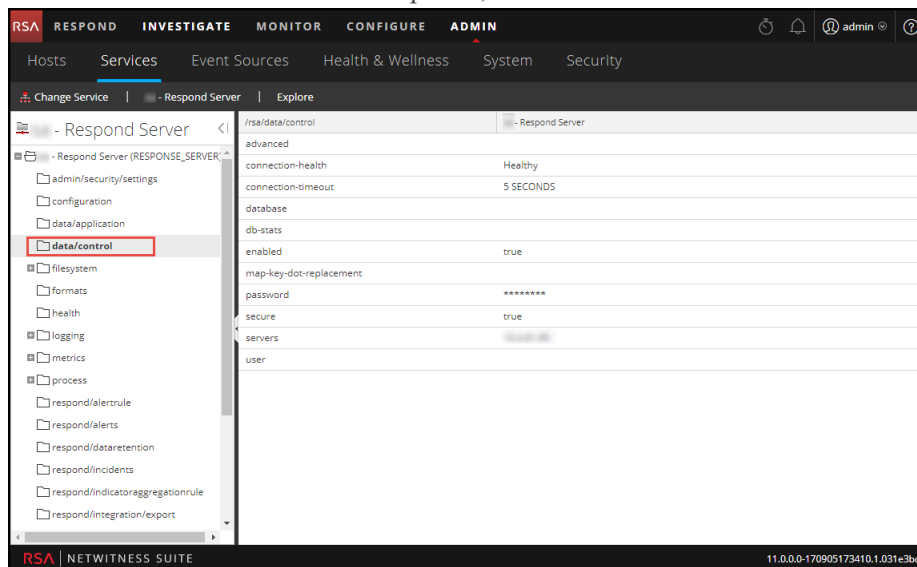
1. Vaya a **ADMIN > Servicios**.  
Se muestra la vista Servicios.
2. En el panel Servicios, seleccione el servicio **Servidor de Respond** y elija  > **Ver > Explorar**.
3. En la lista de nodos de la vista Explorar, seleccione **data/application**.





4. Proporcione la siguiente información:

- **base de datos:** El nombre de la base de datos. El valor predeterminado es respond-server.
- **contraseña:** La contraseña que se usa para la implementación del servidor de ESA primario (contraseña de usuario `deploy_admin`).
- **servidores:** El nombre de host o la dirección IP del **servidor de ESA primario** para que actúe como el host de base de datos para los datos de las aplicaciones de NetWitness Respond datos de aplicaciones, como alertas, incidentes y tareas.
- **usuario:** Ingrese `deploy_admin`.

5. En la lista de nodos de la vista Explorar, seleccione **data/control**.



6. Proporcione la siguiente información:

- **base de datos:** El nombre de la base de datos. El valor predeterminado es respond-server.
  - **contraseña:** La contraseña que se usa para la implementación del Servidor de NetWitness (contraseña de usuario deploy\_admin).
  - **servidores:** El nombre de host o la dirección IP del **Servidor de NetWitness** para que actúe como el host de base de datos para los datos de control de NetWitness Respond, como reglas de agregación y categorías.
  - **usuario:** Ingrese **deploy\_admin**.
7. Reinicio del Servicio servidor de Respond. Para hacerlo, vaya a **ADMIN > Servicios**, seleccione el Servicio servidor de Respond y elija   > **Reiniciar**.

**Nota:** Es importante reiniciar el Servicio servidor de Respond para que se complete la configuración de la base de datos.

## Referencia de la configuración de NetWitness Respond

---

Esta sección contiene información de referencia para la configuración de NetWitness Respond.

### Vista Configurar

La vista Configurar permite configurar la funcionalidad de NetWitness Respond.

Puede configurar reglas de agregación con el objeto de automatizar el flujo de trabajo de Respond para crear incidentes automáticamente.

## Pestaña Reglas de agregación

La pestaña Reglas de agregación permite crear y administrar reglas de agregación para automatizar el proceso de creación de incidentes. NetWitness Suite proporciona 11 reglas preconfiguradas. Puede agregar estas reglas y ajustarlas para su propio ambiente.

### ¿Qué desea hacer?

Función	Deseo...	Mostrarme cómo
Analista, experto en contenido, administrador del SOC	Crear una regla de agregación.	<a href="#">Paso 3. Crear una regla de agregación para alertas</a>
Encargados de respuesta ante incidentes, analistas, expertos en contenido, administrador del SOC	Ver los resultados de mi regla de agregación (Ver amenazas detectadas).	Consulte “Respuesta ante incidentes” en la <i>Guía del usuario</i> de <i>NetWitness Respond</i> .

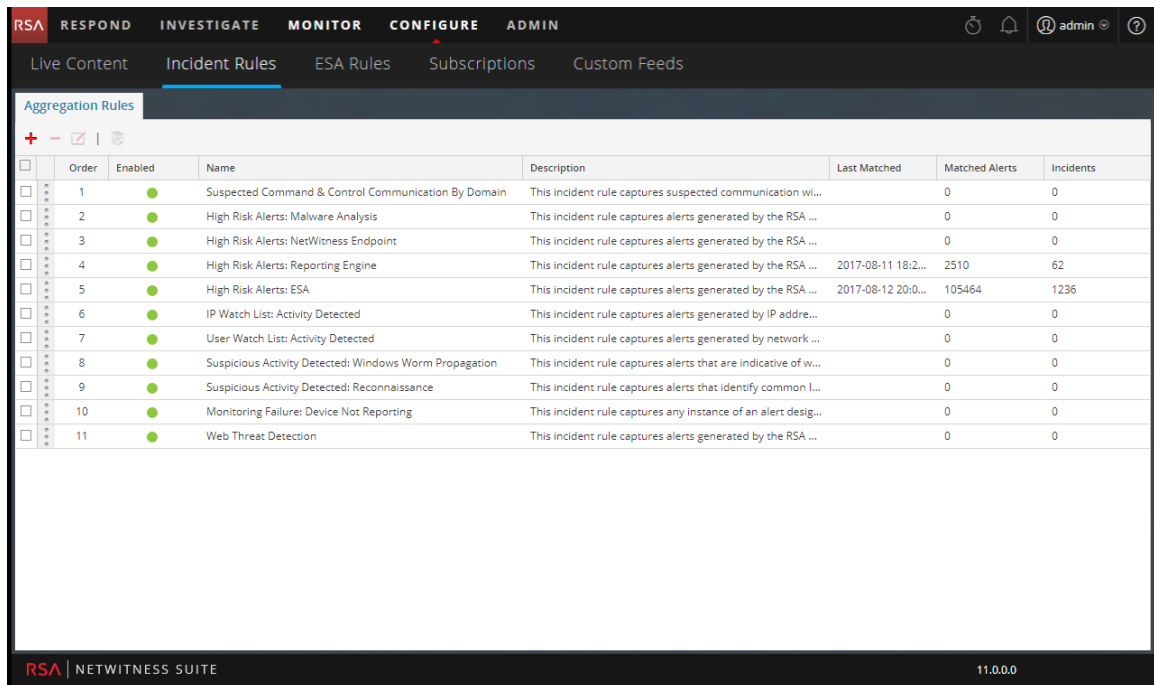
### Temas relacionados

- [Pestaña Nueva regla](#)

### Reglas de agregación

Para acceder a la pestaña Reglas de agregación, vaya a **CONFIGURAR > Reglas de incidentes > pestaña Reglas de agregación**.





La pestaña Reglas de agregación consta de una lista y una barra de herramientas.

### Lista Reglas de agregación





En la siguiente tabla se describen las columnas de la lista Reglas de agregación.

Columna	Descripción
Seleccionar	Permite seleccionar una regla con el fin de realizar una acción, como Clonar o Eliminar.
Orden	Muestra el orden en que se coloca la regla. El orden de la regla determina cuál regla se aplica si los criterios de varias reglas coinciden con la misma alerta. Si dos reglas coinciden con una alerta, solo se evalúa la que tiene la prioridad más alta.
Nombre	Muestra el nombre de la regla.
Habilitado	Muestra si la regla está o no habilitada. ● especifica que la regla está activada.
Descripción	Muestra la descripción de la regla.

Columna	Descripción
Última coincidencia	Muestra la hora en que se hizo coincidir correctamente una alerta con la regla. Este valor se reinicia una vez por semana.
Alertas con coincidencia	Muestra la cantidad de alertas con coincidencia. Este valor se restablece una vez por semana. Para cambiar la configuración, consulte <a href="#">Configurar el contador para alertas e incidentes con coincidencia</a> .
Incidentes	Muestra la cantidad de incidentes que creó la regla. Este valor se restablece una vez por semana. Para cambiar la configuración, consulte <a href="#">Configurar el contador para alertas e incidentes con coincidencia</a> .

### Barra de herramientas de Reglas de agregación

En la siguiente tabla se muestran las operaciones que se pueden realizar en la pestaña Reglas de agregación.

Opción	Descripción
	Le permite agregar una regla nueva.
	Le permite editar una regla.
	Le permite eliminar una regla.
	Permite duplicar una regla.

## Pestaña Nueva regla

La pestaña Nuevas reglas permite crear reglas de agregación personalizadas para automatizar el proceso de creación de incidentes. En este tema se describe la información que se requiere cuando se crea una nueva regla.

### ¿Qué desea hacer?

Función	Deseo...	Mostrarme cómo
Analista, experto en contenido, administrador del SOC	Crear una regla de agregación.	<a href="#">Paso 3. Crear una regla de agregación para alertas</a>
Encargados de respuesta ante incidentes, analistas, expertos en contenido, administrador del SOC	Ver los resultados de mi regla de agregación (Ver amenazas detectadas).	Consulte “Respuesta ante incidentes” en la <i>Guía del usuario</i> de <i>NetWitness Respond</i> .

### Temas relacionados

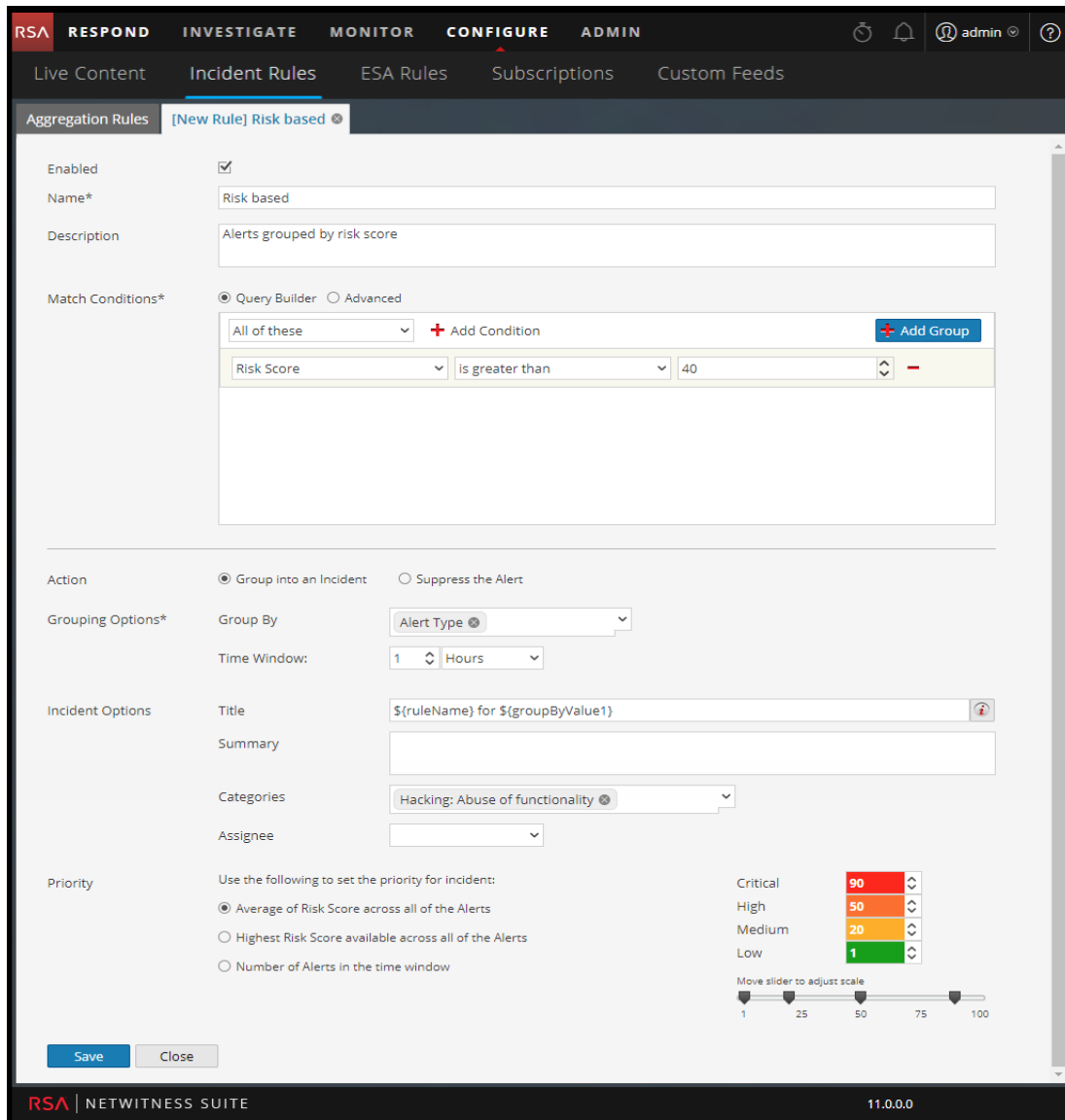
- [Pestaña Reglas de agregación](#)

### Nueva regla

Para acceder a la vista de la pestaña Nueva regla:

1. Vaya a **CONFIGURAR > Reglas de incidentes > pestaña Reglas de agregación**.
2. Haga clic en **+**.

Se muestra la pestaña **Nueva regla**.



En la siguiente tabla se describen las opciones disponibles cuando se crean reglas de agregación personalizadas.

Campo	Descripción
Habilitado	Seleccione esta opción para activar la regla.
Nombre*	Nombre de la regla. Este campo es obligatorio.
Descripción	Descripción de la regla que permite formarse una idea de las alertas que se agregan.

Campo	Descripción
<p>Condiciones de coincidencia*</p>	<p><b>Generador de consultas:</b> seleccione si desea crear una consulta con diversas condiciones que se pueden agrupar. También puede tener grupos de condiciones anidados.</p> <p>Condiciones de coincidencia: puede configurar el valor en <b>Todas estas</b>, <b>Cualquiera de estas</b> o <b>Ninguna de estas</b>. De acuerdo con la selección, se buscan coincidencias con los tipos de criterios especificados en las condiciones y el grupo de condiciones para agrupar las alertas.</p> <p><b>Por ejemplo</b>, si configura la condición de coincidencia en Todas estas, las alertas que coinciden con los criterios mencionados en las condiciones y el grupo de condiciones se agrupan en un incidente.</p> <ul style="list-style-type: none"> <li>• Agregue una condición para la cual se buscarán coincidencias mediante un clic en <b>+</b> <b>Agregar condición</b>.</li> <li>• Agregue un grupo de condiciones mediante un clic en <b>+</b> <b>Agregar grupo</b> y agregue condiciones mediante un clic en <b>+</b> <b>Agregar condición</b>.</li> </ul> <p>Puede incluir múltiples condiciones y grupos de condiciones para los cuales se pueden buscar coincidencias conforme a los criterios establecidos con el fin de agrupar las alertas entrantes en incidentes.</p> <p><b>Avanzado:</b> seleccione si desea agregar un generador de consultas avanzado. Puede agregar una condición específica que se deba hacer coincidir de acuerdo con la opción de coincidencia seleccionada.</p> <p><b>Por ejemplo:</b> puede ingresar el formato del generador de criterios <code>{"\$and": [{"alert.severity" : {"\$gt":4}]}</code> para agrupar alertas que tienen una gravedad mayor que 4.</p> <p>Para conocer la sintaxis avanzada, consulte <a href="http://docs.mongodb.org/manual/reference/operator/query/">http://docs.mongodb.org/manual/reference/operator/query/</a> o <a href="http://docs.mongodb.org/manual/reference/method/db.collection.find/">http://docs.mongodb.org/manual/reference/method/db.collection.find/</a></p>
<p>Acción</p>	<p><b>Agrupar en un incidente:</b> si esta opción está activada, las alertas que coinciden con los criterios establecidos se agrupan en una alerta.</p> <p><b>Suprimir la alerta:</b> si esta opción está activada, las alertas que coinciden con los criterios se suprimen.</p>

Campo	Descripción
Opciones de agrupación*	<p><b>Agrupar por:</b> Criterios para agrupar las alertas según la categoría especificada. Puede usar un máximo de dos atributos para agrupar las alertas. Puede agruparlas con uno o dos atributos. Ya no las puede agrupar con atributos que no tienen valores (atributos vacíos). El agrupamiento según un atributo significa que todas las alertas coincidentes que contienen el mismo valor para ese atributo se agrupan juntas en el mismo incidente.</p> <p><b>Ventana de tiempo:</b> El rango de tiempo especificado para agrupar alertas. Por ejemplo, si la ventana de tiempo se configura en una hora, todas las alertas que coinciden con los criterios establecidos en el campo Agrupar por y que llegan con una hora de diferencia unas de otras se agrupan en un incidente.</p>
Opciones de incidente	<p><b>Título:</b> (Opcional) Título del incidente. Puede proporcionar marcadores de posición basados en los atributos que agrupó. Los marcadores de posición son opcionales. Si no usa marcadores de posición, todos los incidentes que crea la regla tendrán el mismo título.</p> <p>Por ejemplo, si las agrupó según el origen, el incidente resultante se puede llamar Alertas para <b>\${groupByValue1}</b> y el incidente para todas las alertas de NetWitness Endpoint tendría el nombre <b>Alertas para NetWitness Endpoint</b>.</p> <p><b>Resumen:</b> (opcional) resumen del incidente.</p> <p><b>Categoría:</b> (opcional) categoría del incidente creado. Un incidente se puede clasificar por más de una categoría.</p> <p><b>Usuario asignado:</b> (opcional) nombre del usuario asignado a quien se asigna el incidente.</p>

Campo	Descripción
Prioridad	<p><b>Promedio de puntaje de riesgo en todas las alertas:</b> toma el promedio de los puntajes de riesgo en todas las alertas para establecer la prioridad del incidente creado.</p> <p><b>Puntaje de riesgo más alto disponible en todas las alertas:</b> toma el puntaje más alto disponible en todas las alertas para establecer la prioridad del incidente creado.</p> <p><b>Cantidad de alertas en la ventana de tiempo:</b> toma el conteo de la cantidad de alertas en la ventana de tiempo seleccionada para establecer la prioridad del incidente creado.</p> <p><b>Crítica, Alta, Media y Baja:</b> especifique el umbral de prioridad de los incidentes con coincidencia. Los valores predeterminados son:</p> <ul style="list-style-type: none"> <li>• Crítica: 90</li> <li>• Alta: 50</li> <li>• Media: 20</li> <li>• Baja: 1</li> </ul> <p>Por ejemplo, con la prioridad Crítica configurada en 90, a los incidentes con un puntaje de riesgo de 90 o más se les asignará una prioridad Crítica para esta regla.</p> <p>Puede cambiar estos valores predeterminados mediante la modificación manual de las prioridades o el uso del control deslizante bajo <b>Mover control deslizante para ajustar escala</b>.</p>

