



RSA | Security Analytics

Guía de configuración de Incident Management
para la versión 10.6

Marcas comerciales

RSA, el logotipo de RSA y EMC son marcas registradas o marcas comerciales de EMC Corporation en los Estados Unidos y en otros países. Todas las demás marcas comerciales utilizadas en este documento pertenecen a sus respectivos propietarios. Para obtener una lista de las marcas comerciales de EMC, visite mexico.emc.com/legal/emc-corporation-trademarks.htm (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 del acuerdo de licencia que se aplica al software de otros fabricantes en este producto puede encontrarse en el archivo [thirdpartylicenses.pdf](#).

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

El uso, la copia y la distribución de cualquier software de EMC descrito en esta publicación requieren una licencia de software correspondiente. 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.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA "TAL CUAL". EMC CORPORATION NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIALIZACIÓN O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Contenido

Guía de configuración de Incident Management	4
Descripción general de Incident Management	5
Configurar Incident Management	7
Paso 1. Agregar el servicio Incident Management	8
Requisitos previos	8
Procedimiento	8
Paso 2. Configurar una base de datos para el servicio Incident Management	10
Consideraciones para elegir el host para la base de datos de ESA	10
Requisitos previos	10
Procedimiento	11
Paso 3. Configurar orígenes de alertas para mostrar alertas en Incident Management	12
Requisitos previos	12
Configurar Reporting Engine para mostrar alertas que activó Reporting Engine en la vista Incident Management	12
Configurar Malware Analytics para ver las alertas que activó Malware Analytics en la vista Incident Management	13
Configurar ECAT para ver las alertas que activó ECAT en la vista Incident Management	13
Configurar ECAT para mostrar alertas de ECAT	14
Configurar el contador para alertas e incidentes con coincidencia	16
Vista Sistema de servicios de Incident Management	18
Acceder a la vista	18
Información de servicio	18

Guía de configuración de Incident Management

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

Temas

- [Descripción general de Incident Management](#)
- [Configurar Incident Management](#)
- [Configurar el contador para alertas e incidentes con coincidencia](#)
- [Vista Sistema de servicios de Incident Management](#)

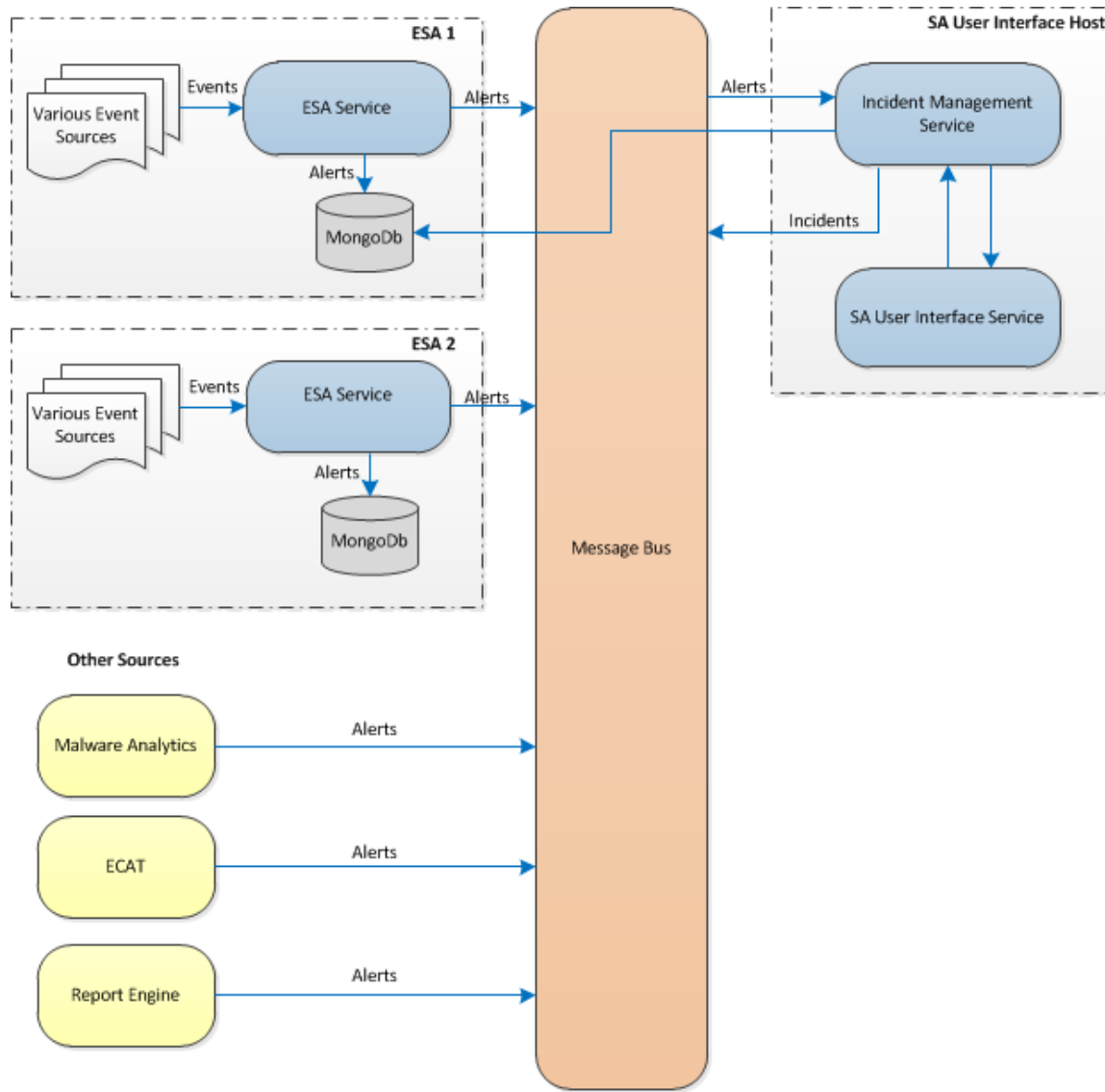
Descripción general de Incident Management

Security Analytics Incident Management consume datos de alerta de diversos orígenes a través del bus de mensajes y muestra estas alertas en la interfaz del usuario de Security Analytics. El servicio Incident Management permite agrupar las alertas de manera lógica e iniciar un flujo de trabajo de respuesta ante incidentes para investigar y corregir los problemas de seguridad planteados.

Este servicio 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.). El servicio Incident Management 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: El servicio Incident Management hace persistir los registros de alertas en MongoDB. En Security Analytics 10.4 y superior, la instancia de MongoDB se instala en uno de los hosts de ESA. ESA es un componente requerido para Incident Management.

En la siguiente figura se ilustra un diagrama de flujo de datos general:



Debe configurar diversos orígenes desde los cuales el servicio Incident Management recopila y agrega las alertas.

Configurar Incident Management

En este tema se proporcionan tareas generales necesarias para configurar el servicio Incident Management. El administrador debe completar los pasos en la secuencia que se indica.

Temas

- [Paso 1. Agregar el servicio Incident Management](#)
- [Paso 2. Configurar una base de datos para el servicio Incident Management](#)
- [Paso 3. Configurar orígenes de alertas para mostrar alertas en Incident Management](#)

Paso 1. Agregar el servicio Incident Management

En este tema se proporciona información sobre la forma de agregar el servicio Incident Management en un host.

Requisitos previos

Asegúrese de haber instalado un host en el cual desea ejecutar el servicio Incident Management. Consulte **Paso 1: Agregar o actualizar un host** en la *Guía de introducción de hosts y servicios* para conocer el procedimiento necesario para agregar un host.

Procedimiento

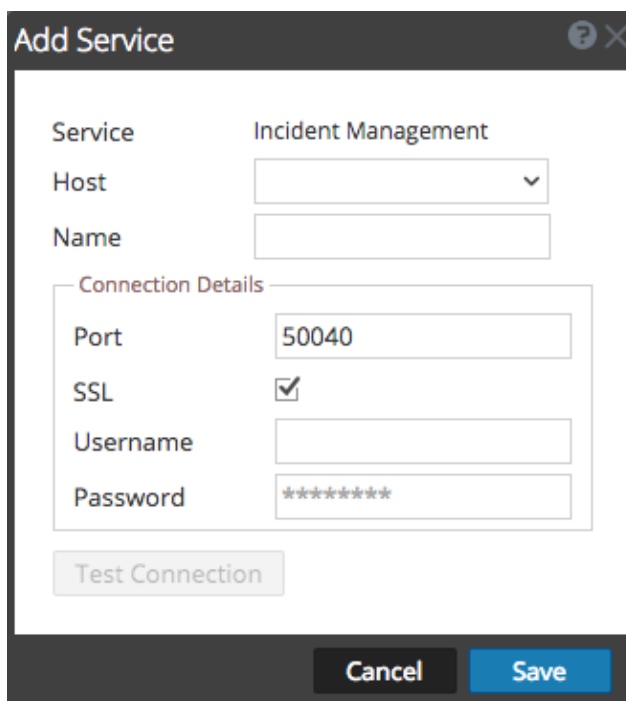
Para agregar el servicio Incident Management:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.

Se muestra la vista Servicios.

2. En el panel Servicios, seleccione **+** > **Incident Management**.

Se muestra el cuadro de diálogo **Agregar servicio**.



The screenshot shows a dialog box titled "Add Service" with a question mark icon and a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Service:** A dropdown menu with "Incident Management" selected.
- Host:** A dropdown menu with a downward arrow.
- Name:** A text input field.
- Connection Details:** A section with a minus sign icon, containing:
 - Port:** A text input field with "50040" entered.
 - SSL:** A checkbox that is checked.
 - Username:** A text input field.
 - Password:** A text input field with "*****" entered.
- Test Connection:** A button.
- Cancel:** A button.
- Save:** A button.

3. Ingrese los siguientes detalles:

Campo	Descripción
Host	Seleccione el host en el cual está instalado el servidor de IM.
Nombre	Escriba un nombre para el servicio.
Puerto	El puerto predeterminado es 50040.
SSL	<p>Seleccione SSL si desea que Security Analytics se comunice con el host mediante SSL. La seguridad de la transmisión de datos se administra mediante el cifrado de la información y el suministro de autenticación con certificados SSL. Esto se requiere de manera predeterminada.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Nota: si selecciona SSL, asegúrese de que este protocolo esté activado en el panel Configuración del sistema.</p> </div>
Nombre de usuario	Escriba el nombre de usuario del host.
Contraseña	Escriba la contraseña del host.

4. Haga clic en **Probar conexión** para determinar si Security Analytics se conecta al servicio.

5. Cuando el resultado sea satisfactorio, haga clic en **Guardar**.

El servicio agregado ahora se muestra en el panel Servicios.

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

Paso 2. Configurar una base de datos para el servicio Incident Management

Para que el servicio se pueda utilizar, debe configurar la base de datos para el servicio Incident Management. La instalación de ESA crea y asegura una instancia de base de datos para el servicio Incident Management. Tiene que seleccionar uno de los servidores de ESA para que actúe como host de la base de datos del servicio Incident Management.

Consideraciones para elegir el host para la base de datos de ESA

Este tema se aplica si habilita la correlación entre sitios en ESA.

En ESA, la correlación entre sitios permite crear una implementación que incluye un conjunto de reglas y varios servicios de ESA. Estas son las funciones principales de una implementación con correlación entre sitios:

1. Hay un servicio de ESA central.
2. Cuando implementa reglas, los servicios de ESA reenvían los eventos pertinentes al servicio de ESA central.
3. El servicio de ESA central ejecuta las reglas y genera alertas.

Si habilita la correlación entre sitios, hay factores que se deben considerar cuando elige el servicio de ESA que se usará con Incident Management:

- Elija un servicio ESA que comparta ubicación con Security Analytics para limitar la latencia para el acceso a MongoDB.
- Elija el servicio de ESA que recibe la menor cantidad de tráfico.

Nota: no elija el servicio de ESA central porque recopila su propio tráfico y recibe eventos reenviados de otros servicios de ESA.


De manera predeterminada, la correlación entre sitios no está habilitada. Para habilitar la correlación entre sitios, debe consultar a RSA Professional Services con el fin de participar en el Programa de prueba de campo de la correlación entre sitios.

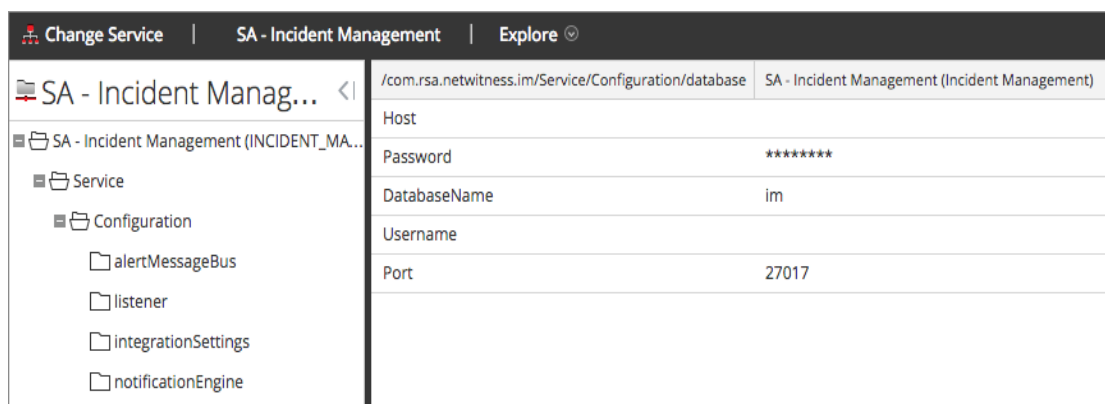
Requisitos previos

Asegúrese de que un host de ESA esté instalado y configurado.

Procedimiento

Para configurar una base de datos para el servicio Incident Management:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
Se muestra la vista Servicios.
2. En el panel Servicios, seleccione el servicio Incident Management y elija  > **Ver > Explorar**.
Se muestra la vista Explorar de los servicios.
3. En el panel de opciones, seleccione **Servicio > Configuración > base de datos**.
La vista de la base de datos se muestra en el panel derecho.



4. Proporcione la siguiente información:
 - **Host:** nombre de host o dirección IP del host de ESA seleccionado como una base de datos
 - **DatabaseName:** im (este es el valor predeterminado)
 - **Puerto:** 27017 (este es el valor predeterminado)
 - **Nombre de usuario:** nombre de usuario de la cuenta de usuario para la base de datos de IM (ESA crea un usuario im con los privilegios correctos)
 - **Contraseña:** la contraseña que seleccionó para el usuario im
5. Reinicie el servicio Incident Management mediante el siguiente comando:
`service rsa-im restart`

Nota: Es importante reiniciar el servicio Incident Management para que se complete la configuración de la base de datos.

Paso 3. Configurar orígenes de alertas para mostrar alertas en Incident Management

Este procedimiento es necesario para que las alertas de los orígenes de alertas se muestren en Incident Management. Tiene la opción de activar o desactivar las alertas que se completan en la vista Incident Management. De forma predeterminada, esta opción está inhabilitada en Reporting Engine, Malware Analytics y ECAT, y solo está habilitada en Event Stream Analysis. Por lo tanto, cuando instala el servicio Incident Management, debe habilitar esta opción en Reporting Engine, Malware Analytics y ECAT para completar las alertas correspondientes en la vista Incident Management.


Requisitos previos

Garantice que:

- El servicio Incident Management está instalado y en ejecución en Security Analytics.
- Hay una base de datos configurada para el servicio Incident Management.
- ECAT está instalado y en ejecución.

Configurar Reporting Engine para mostrar alertas que activó Reporting Engine en la vista Incident Management

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

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. Seleccione el servicio Reporting Engine y elija  > **Ver > Configuración**.
La vista Configuración de servicios se muestra con la pestaña General de Reporting Engine abierta.
3. Seleccione **Configuración del sistema**.
4. Seleccione la casilla de verificación **Reenviar alertas a IM**.
Reporting Engine ahora reenvía las alertas a Incident Management.

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 Incident Management

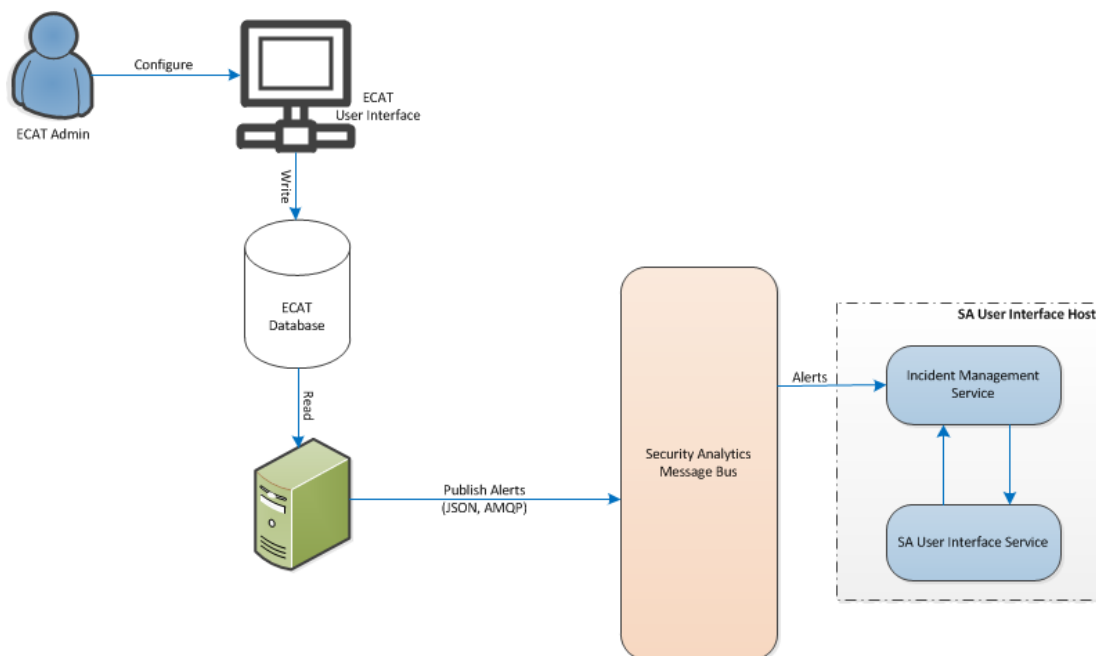
La visualización de alertas de Incident Management es una función de auditoría en Malware Analysis. El procedimiento para habilitar alertas de IM se describe en el tema **(Opcional) Configurar la auditoría en un host de Malware Analysis** de la *Guía de configuración de Malware Analysis*.

Configurar ECAT para ver las alertas que activó ECAT en la vista Incident Management

Este procedimiento se requiere para integrar ECAT con Security Analytics de modo que el componente Incident Management de Security Analytics recopile las alertas de ECAT y las muestre en la vista **Incidente > Alertas**.

Nota: En el tema **Integración de RSA ECAT** de la *Guía de integración de RSA ECAT* se proporciona una descripción general de las funcionalidades de integración de ECAT en Security Analytics, así como procedimientos detallados para configurar la integración de ECAT con Security Analytics a través del bus de mensajes.

En el siguiente diagrama se representa el flujo de alertas de ECAT para la línea de espera de Incident Management de Security Analytics y su visualización en la vista **Incidente > Alertas**.



Configurar ECAT para mostrar alertas de ECAT

Para configurar ECAT de manera que muestre alertas de ECAT en la interfaz del usuario de Security Analytics:

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

Se muestra el cuadro de diálogo **Monitoreo y componentes externos**.

2. Haga clic con el botón secundario en cualquier lugar del cuadro de diálogo y seleccione **Agregar componente**.

Se muestra el cuadro de diálogo **Agregar componente**.

3. Proporcione la siguiente información:

- Seleccione intermediador de IM como el **Tipo de componente** en las opciones del menú desplegable.
- Escriba un nombre de usuario para identificar al intermediador de IM.
- Escriba la **Dirección IP o el DNS del host** del intermediador de IM.
- Escriba el **Número de puerto**. El puerto predeterminado es 5671.

4. Haga clic en **Guardar y cerrar** para cerrar todos los cuadros de diálogo.

5. Para configurar SSL para las alertas de IM, realice los siguientes pasos en ECAT con el fin de establecer las comunicaciones SSL:

- a. En el servidor de consola primario de ECAT, exporte el certificado de CA de ECAT al formato cer (X.509 con codificación Base 64) desde el área de almacenamiento de certificados personales de la computadora local (sin seleccionar la clave privada).
- b. En el servidor de consola primario de ECAT, genere un certificado de cliente para ECAT mediante el certificado de CA de ECAT. (El nombre de CN se debe configurar 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 "EcatCA" -is MY -ir  
LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -  
cy end -sy 12 client.cer
```

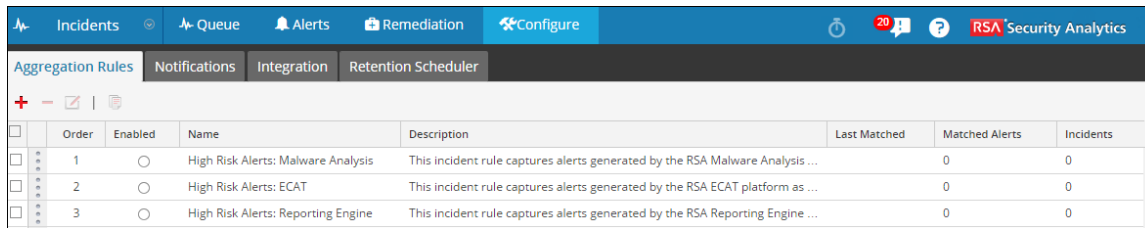
- c. En el servidor de la consola primaria de ECAT, tome nota de la huella digital del certificado de cliente generado en el paso b. Ingrese el valor de la huella digital del certificado de cliente en la sección IMBrokerClientCertificateThumbprint del archivo ConsoleServer.Exe.Config como se muestra.

```
<add key="IMBrokerClientCertificateThumbprint"  
value="?896df0efacf0c976d955d5300ba0073383c83abc"/>
```

- d. En el servidor de SA, agregue el contenido del archivo de certificado de CA de ECAT en formato .cer (del paso a) a
`/etc/puppet/modules/rabbitmq/files/truststore.pem.`
- e. En el servidor de SA, ejecute puppet agent como se muestra (o espere 30 minutos hasta que se ejecute el servidor de SA).
`puppet agent -t`
- f. En el servidor de consola primario de ECAT, importe el archivo
`/var/lib/puppet/ssl/certs/ca.pem` desde el servidor de SA al almacén de autoridades de certificación raíz de confianza. Con esto se garantizará que ECAT, como cliente, pueda confiar en el certificado de servidor de IM.

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
<input type="checkbox"/>	1	<input type="radio"/>	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA Malware Analysis ...		0	0
<input type="checkbox"/>	2	<input type="radio"/>	High Risk Alerts: ECAT	This incident rule captures alerts generated by the RSA ECAT platform as ...		0	0
<input type="checkbox"/>	3	<input type="radio"/>	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reporting Engine ...		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.

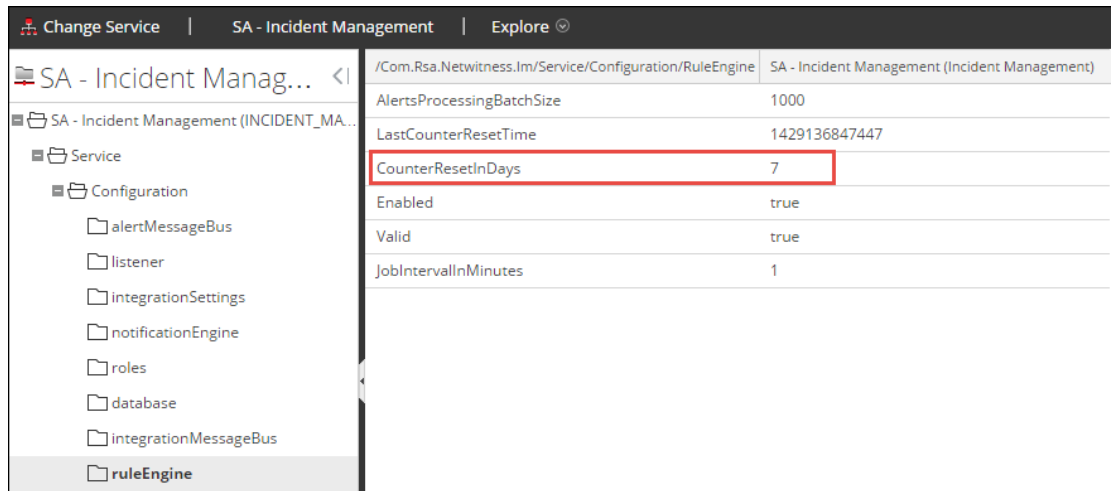
De manera predeterminada, estos valores se restablecen a cero cada siete días. Según el tiempo durante el cual desea que continúen los conteos, puede cambiar la cantidad predeterminada de días.


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. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. Seleccione un servicio Incident Management y, a continuación, elija  > **Ver > Explorar**.

3. En la vista Explorar de la izquierda, seleccione **Servicio > Configuración > ruleEngine**.





4. En el panel de la derecha, escriba la cantidad de días en el campo **CounterResetInDays**.
5. Reinicie el servicio para que se aplique la nueva configuración:
 - a. Seleccione **Servicios**.
 - b. Seleccione el servicio y haga clic en  > **Reiniciar**.

Vista Sistema de servicios de Incident Management

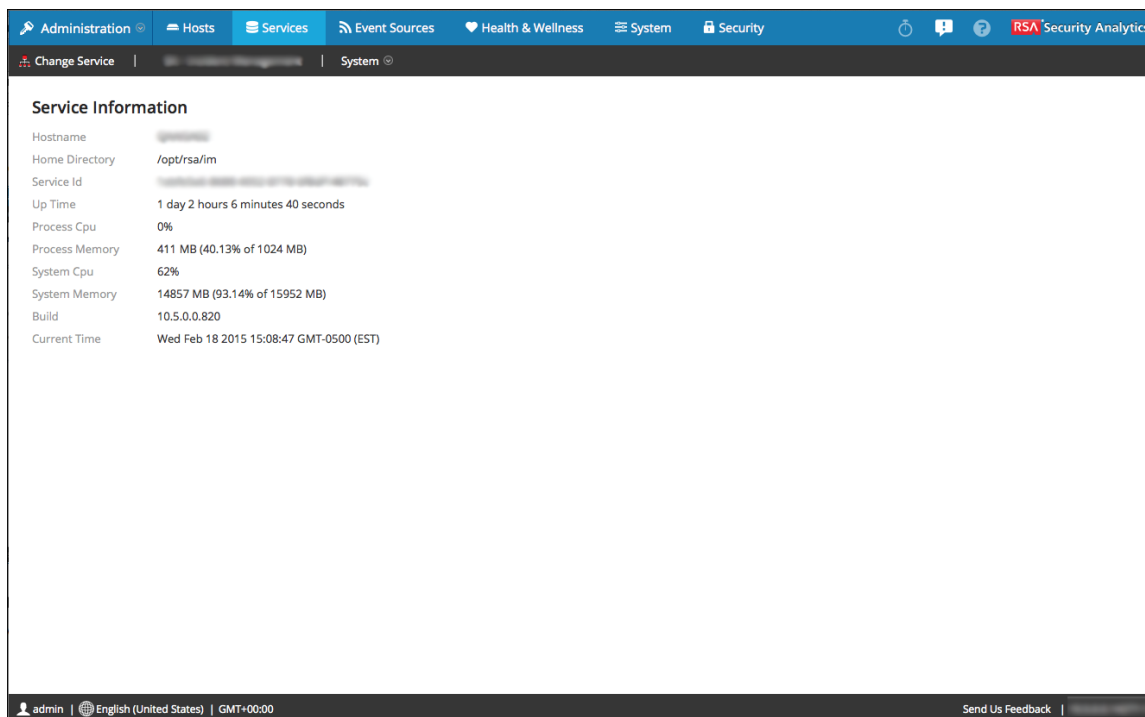
La vista Sistema de servicios permite ver información sobre el servicio Incident Management.

Acceder a la vista

Para acceder a esta vista:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio de Incident Management y elija   **> Ver > Sistema**.

Se muestra la vista Sistema de servicios de Incident Management.



The screenshot shows the 'Service Information' panel in the RSA Security Analytics interface. The panel displays the following details:

Hostname	[Redacted]
Home Directory	/opt/rsa/im
Service Id	[Redacted]
Up Time	1 day 2 hours 6 minutes 40 seconds
Process Cpu	0%
Process Memory	411 MB (40.13% of 1024 MB)
System Cpu	62%
System Memory	14857 MB (93.14% of 15952 MB)
Build	10.5.0.0.820
Current Time	Wed Feb 18 2015 15:08:47 GMT-0500 (EST)

Información de servicio

La vista Sistema contiene un panel: el panel Información de servicio. En el panel Información de servicio se proporciona un resumen del servicio, el cual difiere levemente de la vista Sistema de servicios genérica. En esta tabla se describe la información de servicio del panel.

Campo	Descripción
Hostname	Muestra el nombre del host. Por ejemplo: NWAPPLIANCE2682
Home	Muestra la ubicación del directorio principal de Incident Management. Por ejemplo: /opt/rsa/im
ID de servicio	Muestra el ID del servicio. Por ejemplo: 1694b15c-42c7-410d-9ba3-a7c48ba4722d
Tiempo de actividad	Muestra el tiempo que ha pasado desde que se inició el host. Por ejemplo: 0 5 horas 33 minutos 20 segundos
CPU del proceso	Muestra el porcentaje de CPU que usa el proceso. Por ejemplo: %0
Memoria del proceso	Muestra la memoria que usa el proceso. Por ejemplo: 86,285 KB (8.37 % de 1,024 MB)
CPU del sistema	Muestra el porcentaje de CPU que usa el sistema. Por ejemplo: %2
Memoria del sistema	Muestra la memoria que usa el sistema. Por ejemplo: 30,065 MB (31.05 % de 96,831 MB)
Compilación	Muestra el número de versión de Security Analytics. Por ejemplo: 10.6.0.0.1009
Hora actual	Muestra el día actual de la semana, la fecha y la hora. Por ejemplo: Jueves 14 de enero de 2016 11:15:23 UTC-05:00

