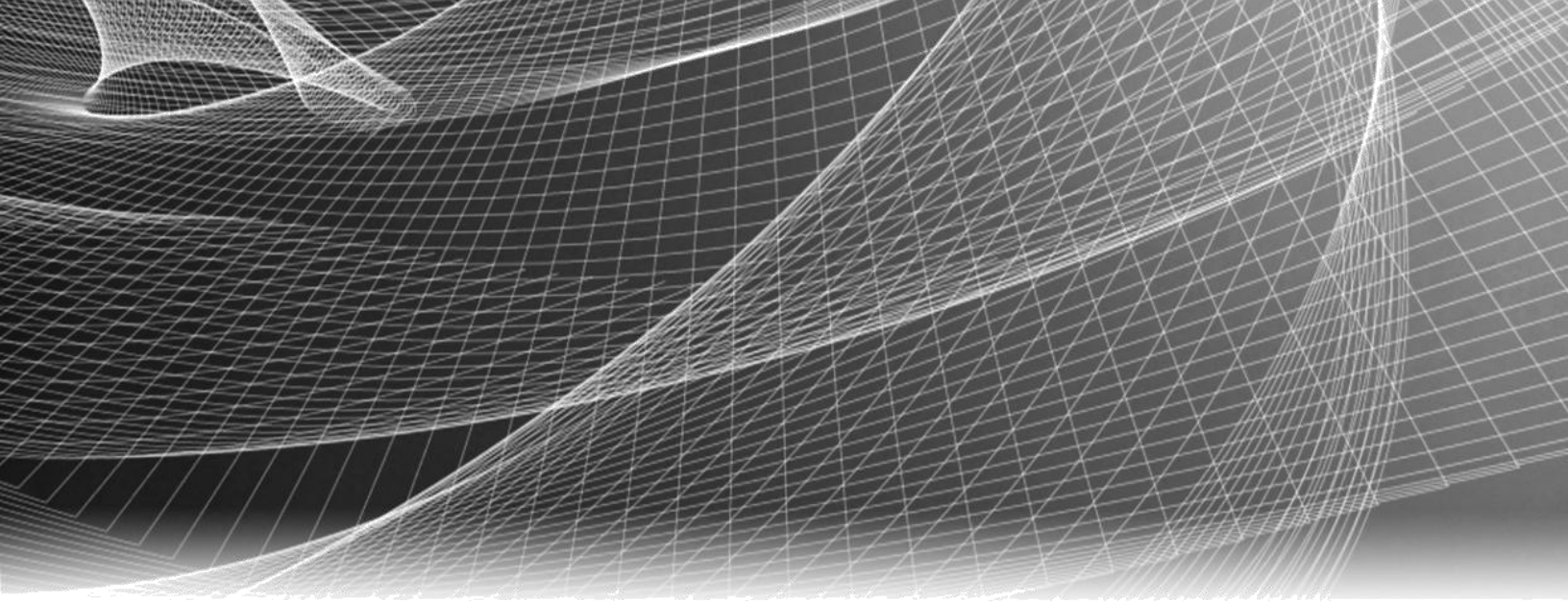

RSA Security Analytics

Notas de la versión 10.6

RSA

EMC²

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 COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Notas de la versión de Security Analytics 10.6

Introducción

En este documento se indican las novedades y los cambios de RSA® Security Analytics, así como las soluciones alternativas a problemas conocidos. Lea este documento antes de implementar o actualizar RSA Security Analytics.

Números de compilación

En la siguiente tabla se muestran los números de compilación de los diversos componentes de RSA Security Analytics versión 10.6.

Componente	Número de versión
Security Analytics Web Server	10.6.0.0.22075
Security Analytics Decoder	10.6.0.0.6993
Security Analytics Concentrator	10.6.0.0.6993
Security Analytics Broker	10.6.0.0.6993
Security Analytics Log Decoder	10.6.0.0.6993
Security Analytics Log Collector	10.6.0.0.14466
Security Analytics IPDB Extractor	10.6.0.0.17259
Security Analytics Incident Management	10.6.0.0.1037
Security Analytics Reporting Engine	10.6.0.0.5489
Security Analytics Warehouse Connector	10.6.0.0.1972
Security Analytics Archiver (Workbench)	10.6.0.0.6993

Última modificación: 18 de febrero de 2016, 14:12 h

Componente	Número de versión
Security Analytics Event Stream Analysis	10.6.0.0.1536
Security Analytics Malware Analysis	10.6.0.0.8522
Security Analytics Context Hub	10.6.0.0.521

Documentación del producto

Con esta versión se proporciona la siguiente documentación.

Documento	Ubicación
Ayuda en línea de RSA Security Analytics 10.6	https://sadocs.emc.com
Lista de verificación para la actualización de RSA Security Analytics 10.6	https://knowledge.rsasecurity.com
Instrucciones de actualización de RSA Security Analytics 10.6	https://knowledge.rsasecurity.com
Actualización del colector de Windows existente	https://knowledge.rsasecurity.com
Guía de instalación de Decoder 10G de RSA Security Analytics 10.6	https://knowledge.rsasecurity.com

Cambios de la terminología en 10.6

En la siguiente tabla se enumeran los términos nuevos incorporados en 10.6 con los términos reemplazados de las versiones anteriores y una descripción de cada término.

10.6.0.0	Antes de 10.6.0.0	Descripción
Repositorio dinámico de actualizaciones	Repositorio Yum, SMCUPDATE	Repositorio dinámico en el cual RSA publica las actualizaciones de las versiones de software de Security Analytics de manera habitual.
Repositorio de actualización local	Repositorio del servidor de SA, repositorio Yum de SA	Repositorio local en su implementación de Security Analytics desde el cual se aplican las actualizaciones de las versiones de software a un host. Tiene dos opciones para completar el repositorio de actualización local en su implementación de Security Analytics: • Opción 1: Conectarse al repositorio dinámico de actualizaciones. • Opción 2: Descargar actualizaciones de versiones desde SecureCare Online (SCOL) y cargarlas en el repositorio de actualización local.
Host que no es de servidor de SA	Host que no es de SA	Cualquier host de la implementación de Security Analytics distinto de un host del servidor de SA. Consulte **Host del servidor de Security Analytics**.

10.6.0.0	Antes de 10.6.0.0	Descripción
Host del servidor de Security Analytics	Host de SA, dispositivos de SA	**Nota:** Se abrevia **host del servidor de SA** en los mensajes y en los gráficos donde hay restricciones de espacio. Host en el cual reside el servidor de Security Analytics. El servidor de Security Analytics contiene la interfaz del usuario y el servicio de administración de servicios (SMS). Cuando actualiza a una versión nueva, el servidor de Security Analytics se debe actualizar primero. Si tiene una implementación de Security Analytics con versiones combinadas, el servidor de Security Analytics debe tener la versión más reciente en su implementación. Según su implementación, puede alojar los siguientes servicios en el host del servidor de Security Analytics además del servidor de Security Analytics y SMS: • Administración de orígenes de eventos • Reporting Engine • Malware Analysis • IPDB Extractor • Incident Management • Intermediador

Novedades

RSA Security Analytics versión 10.6 incluye las siguientes funciones y mejoras nuevas.

Seguridad

En esta sección se describen las nuevas funciones y mejoras de seguridad de RSA Security Analytics.

- **Mejoras en la seguridad.** Consulte Reparaciones y mejoras en la seguridad.

Archiver

En esta sección se describen las nuevas funciones y mejoras de RSA Security Analytics Archiver.

- **Retención selectiva de registros.** Security Analytics le permite conservar los registros con el uso de varias recopilaciones de acuerdo con sus requisitos de retención. Por ejemplo, puede crear una recopilación de cumplimiento de normas para los registros que desea mantener durante un periodo prolongado, una recopilación de bajo valor para los registros que desea mantener durante un par de semanas y una recopilación sin valor para los registros que desea eliminar después de algunos días.

  La retención selectiva de registros brinda las siguientes ventajas:

  - Le permite separar los registros en recopilaciones que requieren distintos criterios de retención, como el tiempo y el tamaño
  - Le permite eliminar registros legalmente confidenciales apenas se permite
  - Automatiza la eliminación de los registros que no se necesitan
  - Proporciona flexibilidad para almacenar registros, lo cual puede generar ahorros considerables en el almacenamiento

Plataforma

En esta sección se describen las nuevas funciones y mejoras de la plataforma RSA Security Analytics.

- **Flujo de trabajo optimizado para las actualizaciones.** Se agregó un flujo de trabajo coherente para la actualización de hosts en Security Analytics con la capacidad de realizar la actualización completa a través de la interfaz del usuario.
- **Información y controles adicionales para las actualizaciones.** En el proceso del flujo de trabajo de actualización se incorporaron comentarios y controles que proporcionan al administrador advertencias e información mucho mejores durante la actualización. Security Analytics cuenta con verificaciones para asegurarse de que el kernel sea compatible con la ruta de actualización y que esté disponible el espacio de archivos adecuado.
- **Proceso consolidado para actualizaciones de servidores de Security Analytics.** Ahora hay un único proceso para actualizar el host del servidor de Security Analytics. Este aún se realiza a través de la línea de comandos para los clientes que aún no actualizan a la versión 10.5.1, pero es un proceso de un paso para el administrador.
- **Compatibilidad con múltiples versiones.** El repositorio dinámico de actualizaciones y el repositorio local de actualizaciones se optimizaron y ahora son compatibles con varias versiones de Security Analytics.

Log Collector

En esta sección se describen las nuevas funciones y mejoras de RSA Security Analytics Log Collector.

- **Monitoreo de Lockbox.** Se agregaron mejoras de Lockbox y se habilitó el monitoreo de estadísticas, reglas y alarmas para garantizar que las actualizaciones de software o los parches de seguridad no causen interrupciones en la recopilación de registros.

Última modificación: 18 de febrero de 2016, 14:12 h

- **Monitoreo del colector de Windows existente.** En Estado y condición se agregaron estadísticas y alarmas para el colector de Windows existente.
- **Determinación automática de Local o Remote Log Collector.** Se eliminó la casilla de verificación Remote/Local Log Collector. El servidor de Security Analytics determina automáticamente si se trata de un Local Log Collector o de un Remote Log Collector.
- **Monitoreo de RabbitMQ.** Las estadísticas y las alarmas de RabbitMQ se pueden monitorear a través de Estado y condición.

Investigation

En esta sección se describen las nuevas funciones y mejoras de RSA Security Analytics Investigation.

- **Mejoras en la búsqueda de registros crudos.** Security Analytics ahora permite buscar rápidamente los registros no analizados. Log Decoder ahora tokeniza los registros no analizados y crea elementos de metadatos que forman una indexación de texto completo en los servicios descendentes, como Concentrators y Archivers. Cuando selecciona la opción Buscar en índices en las preferencias de búsqueda, la búsqueda utiliza automáticamente el índice de texto. Esto le permite buscar de manera rápida y eficiente en los registros analizados y no analizados.

  Estas mejoras en la búsqueda de registros crudos proporcionan visibilidad de los registros no analizados. Por ejemplo, ahora puede tener visibilidad de todo lo que está haciendo un usuario, incluso si los registros no están analizados.

  El tokenizador de registros no analizados está habilitado de forma predeterminada en Log Decoders, Concentrators y Archivers. Cuando se actualiza el Archiver, puede ser necesario agregar el metadato `word` al filtro de inclusión de metadatos para aprovechar estas mejoras. Para obtener más información, consulte el tema de la ayuda en línea de Security Analytics 10.6 “Agregar Log Decoder como un origen de datos en Archiver” en la *Guía de configuración de Archiver*.

- **Mejoras en la búsqueda de eventos.** El cuadro Buscar eventos ahora puede aprovechar todos los índices en el nivel de valores presentes en Concentrators y Archivers. Las búsquedas mediante el cuadro de texto Buscar eventos hacen uso implícitamente de los índices que ya están presentes en Security Analytics. Por lo tanto, las búsquedas en la vista Evento se ejecutan más rápido, incluso cuando abarcan una gran cantidad de eventos.
- **Búsqueda de eventos en las vistas Navegar y Eventos.** Además de la búsqueda de eventos en la vista Eventos, ahora también puede buscar eventos en la vista Navegar de Investigation. En la vista Navegar, puede hacer clic en un valor de metadatos, como HTTP, para desglosar a los datos y, a continuación, ingresar una cadena de búsqueda en el campo Buscar para buscar eventos en ese subconjunto de datos. La búsqueda abre una pestaña en la vista Eventos, presenta el desglose y el rango de tiempo hacia delante y muestra los resultados de búsqueda. También puede desglosar a los datos mediante consultas antes de iniciar una búsqueda.
- **Enriquecimiento automático del contexto en línea.** Guía los flujos de trabajo de investigación mediante el resaltado automático de ciertos valores de metadatos para indicar que está disponible más información contextual de orígenes adicionales (ECAT, Incident Management y listas personalizadas).
- **Búsquedas de enriquecimiento de contexto según demanda.** Proporciona una vista centralizada de contexto relacionado con cualquier valor de metadatos seleccionado en vistas de Investigation.
- **Listas personalizadas.** Grupos de valores generados o importados que son útiles para rastrear elementos durante una investigación. Las listas personalizadas se transforman automáticamente en orígenes de datos para la indicación en línea de valores de metadatos, así como búsquedas de enriquecimiento según demanda.

Servicio Context Hub

Un nuevo servicio de RSA Security Analytics 10.6 que ofrece enriquecimiento de contexto automático y según demanda en las vistas de Security Analytics Investigation. Los analistas aprovechan los datos de enriquecimiento personalizables que gestiona Context Hub a fin de proporcionar información contextual de alto nivel. El servicio Context Hub viene preinstalado en el host de ESA, pero está inhabilitado de forma predeterminada. Debe habilitar este servicio para utilizar la funcionalidad de búsqueda de enriquecimiento.

Última modificación: 18 de febrero de 2016, 14:12 h

Malware Analysis

En esta sección se describen las nuevas funciones y mejoras de RSA Security Analytics Malware Analysis.

- **Mejora en syslog.** Además de MD5, Malware Analysis ahora también externaliza los hashes SHA1 y SHA256 mediante el formato CEF de syslog.

Informes

En esta sección se describen las nuevas funciones y mejoras de creación de informes de RSA Security Analytics.

- **Mejoras en la creación de informes.** Consulte Reparaciones y mejoras en la creación de informes.

Administration

En esta sección se describen las nuevas funciones y mejoras de RSA Security Analytics Administration.

- **Cambios en la vista Hosts.** La vista Hosts se usa para actualizar un host a una versión nueva. Se hicieron varios cambios a esta vista en 10.6. Cuando hay actualizaciones de versiones disponibles para un host, se muestra Actualización disponible en la columna Estado y la actualización se elije en la columna Seleccionar versión. En la columna Estado se presenta información sobre el proceso de actualización y se le solicitan acciones en caso de ser necesarias. Consulte el tema de la ayuda en línea de Security Analytics 10.6 “Actualización de una versión de host” en la sección “Conceptos básicos” de la *Guía de introducción de hosts y servicios* para obtener más información sobre la vista Hosts en 10.6 y el proceso de actualización mejorado.

  Nota: La información sobre Memoria total, CPU, SO y Tiempo de actividad ya no se muestra en la vista Hosts. Puede monitorear esta información en Administration > Estado y condición > Navegador de estadísticas del sistema si selecciona el host y especifica la estadística (por ejemplo, Memoria total).

Estado y condición

En esta sección se describen las nuevas funciones y mejoras de Estado y condición de RSA Security Analytics.

- **Monitoreo del colector de Windows existente.** En Estado y condición se agregaron estadísticas y alarmas para el colector de Windows existente.
- **Mejora en la eliminación de alarmas.** Las alarmas de Estado y condición se pueden eliminar de la página Alarmas.
- **Mejora en las estadísticas del sistema.** El Navegador de estadísticas del sistema muestra texto atenuado para las estadísticas que no se han actualizado en los últimos 30 minutos.
- **Monitoreo de RabbitMQ.** Las estadísticas y las alarmas de RabbitMQ ahora se monitorean a través de Estado y condición.

Administración de orígenes de eventos

En esta sección se describen las nuevas funciones y mejoras de Administración de orígenes de eventos de RSA Security Analytics.

- **Pestaña Alarmas.** La nueva pestaña Alarmas de Administration > vista Orígenes de eventos permite ver los detalles de las alarmas de ESM que se han generado.
- **Monitoreo automático (BETA).** Las alertas y el monitoreo automáticos permiten recibir alertas automáticas en función de las desviaciones del comportamiento de base de sus orígenes de eventos, sin necesidad de configurar numerosos umbrales y políticas de grupo.

Última modificación: 18 de febrero de 2016, 14:12 h

- **Pestaña Ajustes de configuración.** La nueva pestaña Ajustes de configuración de Administration > vista Orígenes de eventos permite configurar las alertas y el monitoreo automáticos.

Nota: Las alertas automáticas y su configuración son una función BETA en Security Analytics 10.6.

Live

En esta sección se describen las nuevas mejoras de los servicios RSA Security Analytics Live.

- **Live Feedback.** Live Feedback recopila automáticamente información, como los datos de uso de licencias y el número de versión, de los hosts del servidor de Security Analytics, la cual se puede analizar para mejorar las versiones futuras de Security Analytics.
- **Live Connect Threat Data Sharing (BETA).** Esta es la parte inicial de la plataforma de inteligencia de amenazas basada en la comunidad Live Connect. Su objetivo es compartir datos de inteligencia de amenazas potenciales en el servicio de nube de RSA Live Connect con fines de análisis. Se puede recopilar cualquier tipo de metadatos según la implementación, la configuración, la actividad de red y la interacción de los analistas con Security Analytics. De manera predeterminada, este servicio está activado. Sin embargo, durante la instalación o la actualización, se solicitará a los administradores que acepten o descarten el servicio.

Nota: Live Connect Threat Data Sharing es una función BETA en Security Analytics 10.6.

Event Stream Analysis

En esta sección se describen las nuevas mejoras de RSA Security Analytics Event Stream Analysis.

- **Detección avanzada de amenazas.** Detección de amenazas automatizadas es un servicio nuevo que se implementa en la instalación de ESA y que examina el tráfico HTTP para identificar actividad que posiblemente se trate de malware de control y comando (C2). Automated Threat genera puntajes en función de diversos aspectos del comportamiento del tráfico (como la frecuencia y la regularidad con las cuales se establece contacto con un determinado dominio). Si estos puntajes alcanzan un umbral establecido, se genera una alerta de ESA que contiene puntajes de C2 (comando y control).

  Las comunicaciones de comando y control se producen cuando el malware ha puesto en riesgo un sistema y realiza tareas de señalización. La señalización ocurre cuando el malware envía comunicaciones al servidor de comando y control para informarle que se ha puesto en riesgo una máquina y que espera más instrucciones. La capacidad de detectar el malware en esta etapa de riesgo puede alertar a los responsables de una respuesta antes de que se produzcan otros daños y se pase a una etapa crítica en la “cadena de ataques”.

  Esta función resuelve varios problemas que se producen cuando se busca malware:

  - **Capacidad de utilizar los modelos de ciencia de datos en lugar de las firmas.** Dado que los comportamientos del malware cambian con frecuencia, la detección de malware con firmas es todo un reto. Detección de amenazas automatizadas utiliza modelos de perfiles de comportamientos para detectar el malware de manera rápida y eficaz.
  - **Capacidad de automatizar la búsqueda.** La búsqueda manual en los datos es muy lenta. La automatización de este proceso permite que un analista use su tiempo con mayor eficacia.
  - **Capacidad de detectar un ataque en tiempo real.** En lugar de la creación de lotes y el posterior análisis de los datos, Detección de amenazas automatizadas los analiza a medida que Security Analytics los recopila, lo cual permite la detección de los ataques casi en tiempo real.
- **Pool de memoria.** Cuando desee crear reglas que abarquen un amplio intervalo de tiempo o que sean muy complejas, se recomienda utilizar un pool de memoria para manejar la memoria de manera más eficiente. Cuando utiliza un pool de memoria, en lugar de que todos los eventos estén en la memoria, se pueden escribir en el disco.

Última modificación: 18 de febrero de 2016, 14:12 h

- **Orden por hora.** ESA ahora es compatible con el orden de las sesiones en función de la hora de captura (la hora a la cual el evento de registro o el paquete llegaron a los Decoders). Esta función es útil si está correlacionando eventos desde dos o más Concentrators. Cuando tiene dos o más Concentrators como orígenes, el orden por hora garantiza que sus sesiones se correlacionen según la hora. Esto asegura la correlación de las sesiones capturadas a la misma hora y garantiza que las alertas sean coherentes con las expectativas del usuario, incluso cuando se producen demoras en la transmisión. Si cualquiera de los orígenes queda offline o tarda en enviar las sesiones, ESA hace una pausa para asegurarse de que las sesiones con la misma hora de registro de captura se correlacionen.
- **Actualizaciones al generador de reglas.** Se hicieron varios cambios en el generador de reglas con el fin de aumentar los tipos de reglas que se pueden crear y la funcionalidad del generador de reglas:
  - **Compatibilidad con operadores de comparación numéricos.** Se agregó la capacidad de crear reglas de ESA que evalúan valores de metadatos numéricos para comparación, incluidos mayor que (>), mayor o igual que (>=), menor que (<) y menor o igual que (< =).
  - **Compatibilidad con el operador no es nulo.** El operador no es nulo permite asegurarse de que un campo devuelva un valor. Este campo se puede usar cuando una regla depende de un campo específico que devuelve un valor.
  - **Compatibilidad con la coincidencia estricta de patrones.** Si especifica una coincidencia estricta, esto significa que el patrón se debe producir en la secuencia exacta que se especificó, sin eventos adicionales entremedio.
  - **Compatibilidad con agrupar por en múltiples campos.** Se agregó la capacidad de agrupar por en múltiples campos.
  - **Simplificación del uso de enriquecimientos GeoIP.** Para facilitar el uso, ahora ciertos campos se completan automáticamente.
  - **Compatibilidad con la omisión de mayúsculas y minúsculas.** Este campo está diseñado para su uso con cadenas y matrices de valores de cadena. Cuando se selecciona el campo Omitir mayúsculas y minúsculas, la consulta trata todo el texto de la cadena como un valor en minúscula.
  - **Simplificación del comportamiento de claves CSV.** De forma predeterminada, la primera columna de un archivo CSV se trata como la clave que se usa para las búsquedas. Esto simplifica el trabajo con archivos .CSV.

Servicios principales

En esta sección se describen las nuevas mejoras de los servicios de RSA Security Analytics Core (Archiver, Broker, Concentrator, Decoder y Log Decoder).

- **Aplicación de sintaxis de analizador moderno a fin de evitar resultados inesperados de reglas ambiguas.** Para proporcionar una mejor experiencia del usuario con mensajes de error mejorados e información sobre fallas en el análisis de consultas, Security Analytics ahora aplica el análisis estricto a las reglas de aplicación, red y correlación nuevas. Ahora debe usar la sintaxis correcta para los valores de metadatos que incluye en las consultas a cualquiera de los servicios principales. Todas las consultas y las condiciones de regla en los servicios de Security Analytics Core deben seguir estas pautas:

  > **Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los números ni las direcciones MAC e IP.**

  Por ejemplo:

  - `extension = 'torrent'`
  - `time='2015-jan-01 00:00:00'`
  - `service=80`
  - `ip.src = 192.168.0.1`

  El analizador antiguo de las generaciones anteriores, ahora obsoleto, permite una sintaxis ambigua que puede dar lugar a resultados imprevistos. Solo para las actualizaciones a Security Analytics 10.6, las reglas anteriores a 10.6 existentes con sintaxis obsoleta continúan funcionando y registrando errores. Las reglas anteriores a 10.6 que edita y las que crea en 10.6 deben seguir la sintaxis del análisis estricto.

  Para las actualizaciones a Security Analytics 10.6 o a ambientes combinados, consulte Notas sobre la actualización. Para obtener detalles adicionales, consulte el tema de la ayuda en línea de Security Analytics 10.6 “Guía de reglas y consultas”.

Última modificación: 18 de febrero de 2016, 14:12 h

- **NwConsole mejorada.** NwConsole contiene ahora un sistema de ayuda y completado mediante la tecla de tabulación para los comandos de la consola. La tecla de tabulación proporciona el completado contextual de la mayoría de los comandos y sus parámetros. Por ejemplo, para ver el tema de ayuda Conexión a un servicio, puede escribir `man con` en la línea de comandos y, a continuación, presionar la tecla de tabulación. NwConsole completa el comando por usted: `man Conexión a un servicio`. En el tema de la ayuda en línea de Security Analytics 10.6 “Acceder a NwConsole y a la ayuda” se proporciona información sobre cómo acceder a NwConsole y ver la ayuda interna dentro de NwConsole.

Notas sobre la actualización

Las siguientes rutas de actualización son compatibles con Security Analytics 10.6:

- 10.4.1.x a 10.6.
- 10.5.0.x a 10.6.
- 10.5.1.x a 10.6.

Nota: Las versiones 10.5.2 y superiores no son compatibles como rutas de actualización a 10.6.

Para obtener información detallada y procedimientos para realizar la actualización a 10.6, consulte las instrucciones de actualización en la sección Documentación del producto.

(Condicional: solo para 10.4.1.x a 10.6) Certificados de servidor web personalizados

Cuando actualiza desde 10.4.1.x a 10.6, si creó certificados de servidor web personalizados (es decir `keystore`) y los guarda en `/opt/rsa/jetty9/etc`, debe:

- Respaldar `keystore` en otra ubicación.
- Restaurar `keystore` en `/opt/rsa/jetty9/etc` después de completar la actualización.

Configuración del modo estricto para Security Analytics 10.6

Desde 10.2 en adelante, Security Analytics ha utilizado un analizador moderno para las reglas y las consultas, el cual define estrictamente la sintaxis válida. Cuando un servicio principal encuentra sintaxis obsoleta, escribe una advertencia acerca de esta en los registros de Security Analytics. Security Analytics ahora aplica el análisis estricto a las reglas de aplicación, red y correlación nuevas. El analizador antiguo de las generaciones anteriores, ahora obsoleto, permite una sintaxis ambigua que puede dar lugar a resultados imprevistos.

Nota: Security Analytics continuará siendo compatible con la sintaxis obsoleta en 10.6.x.x, pero no lo será en las versiones posteriores.

RSA recomienda corregir las reglas anteriores a 10.6 con sintaxis obsoleta antes de la actualización a 10.6. Sin embargo, puede corregirlas antes o después de acuerdo con su preferencia.

Después de la actualización a Security Analytics 10.6, las reglas con sintaxis obsoleta se resaltan en la interfaz del usuario. En el Editor de regla se proporcionan mensajes de globo adicionales. Después de corregir las reglas, los elementos resaltados desaparecen.

Las estadísticas **/decoder/config/rules/rule.errors** y **/concentrator/config/rules/rule.errors** que se incorporaron en 10.6 contienen el conteo de reglas con errores. Si **rule.errors** es distinto de cero, Security Analytics genera una alerta de Estado y condición para indicar que debe corregir las reglas.

Además, existe una ruta de migración para las consultas desde Reporting e Investigation. Después de una actualización desde una versión anterior, el sistema funciona en el modo obsoleto (lo controla **/sdk/config/query.parse**). En el modo obsoleto, el servicio continúa utilizando el analizador antiguo para todas las consultas que no pasan el análisis estricto. Los errores se registran y se envía un mensaje al cliente en el cual se informa la falla del análisis estricto. Pero la consulta se ejecuta y devuelve resultados como en las versiones anteriores. Debe monitorear los registros y los clientes externos en busca de informes, tableros, reglas, etc. que estén escritos con sintaxis obsoleta y resolver esos problemas a medida que surgen.

Después de resolver los problemas, puede cambiar todos los servicios principales (Decoders, Log Decoders, Concentrators, Brokers y Archivers) al modo estricto y monitorearlos en busca de problemas. En el modo estricto no se utiliza el analizador antiguo y cualquier infracción en el análisis devuelve errores. Esta tarea se debe ejecutar antes de cualquier actualización principal después de 10.6, porque el analizador antiguo se puede eliminar en versiones futuras y no existiría la opción de funcionamiento en el modo obsoleto.

De manera predeterminada, todas las instalaciones funcionan en el modo estricto. Si planea agregar un dispositivo nuevo a una infraestructura existente que se ejecuta en el modo obsoleto, en la vista Explorar (Administration > Servicios > seleccione un servicio y, en el menú Acciones, seleccione Ver > Explorar), puede cambiar **/sdk/config/query.parse** al modo obsoleto hasta que la plataforma completa se haya cambiado al modo estricto.

En Security Analytics 10.6, toda la validación de reglas funcionará siempre en el modo estricto para impedir la creación de problemas de sintaxis.

Para obtener información adicional, consulte Servicios principales y el tema de la ayuda en línea de Security Analytics 10.6 “Guía de reglas y consultas”.

Problemas resueltos

En esta sección se enumeran los problemas resueltos desde la última versión principal de Security Analytics.

Reparaciones y mejoras en la seguridad

En esta versión de RSA Security Analytics se incorporaron las siguientes mejoras en la seguridad.

Número de rastreo	Descripción
ASOC-10139	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-1081.html
ASOC-5121	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2014-1997.html

Última modificación: 18 de febrero de 2016, 14:12 h

Número de rastreo	Descripción
ASOC-7634 ASOC-8885	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-0674.html
ASOC-11044 ASOC-13435	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-1221.html
ASOC-11294	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-1272.html
ASOC-15717	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-0087.html
ASOC-8881 ASOC-9260 ASOC-12468	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-0864.html
ASOC-12315	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-1623.html
ASOC-15792	Actualización de seguridad del kernel: https://rhn.redhat.com/errata/RHSA-2015-2636.html
ASOC-14288	Actualización de seguridad de java-1.8.0-openjdk: https://rhn.redhat.com/errata/RHSA-2015-1919.html
ASOC-9256	Actualización de seguridad de java-1.7.0-openjdk: https://rhn.redhat.com/errata/RHSA-2015-0806.html
ASOC-11122	Actualización de seguridad de java-1.8.0-openjdk: https://rhn.redhat.com/errata/RHSA-2015-1228.html
ASOC-11123	Actualización de seguridad de java-1.7.0-openjdk: https://rhn.redhat.com/errata/RHSA-2015-1229.html
ASOC-14287	Actualización de seguridad de java-1.7.0-openjdk: https://rhn.redhat.com/errata/RHSA-2015-1920.html
ASOC-8883 ASOC-13489	Actualización de seguridad de glibc: https://rhn.redhat.com/errata/RHSA-2015-0863.html
ASOC-8478	Actualización de corrección de errores de chkconfig: https://rhn.redhat.com/errata/RHBA-2015-0671.html
ASOC-12079	Actualización de seguridad de SQLite: https://rhn.redhat.com/errata/RHSA-2015-1634.html
ASOC-12080	Actualización de seguridad de los paquetes net-snmp del protocolo simple de administración de red (SNMP): https://rhn.redhat.com/errata/RHSA-2015-1636.html
ASOC-12081	Actualización de seguridad del paquete Pluggable Authentication Modules (PAM): https://rhn.redhat.com/errata/RHSA-2015-1640.html
ASOC-13303	Actualización de seguridad de cups: https://rhn.redhat.com/errata/RHSA-2015-1123.html
ASOC-13452	Actualización de seguridad de openldap: https://rhn.redhat.com/errata/RHSA-2015-1840.html
ASOC-13453	Actualización de seguridad de libXfont: https://rhn.redhat.com/errata/RHSA-2015-1708.html

Número de rastreo	Descripción
ASOC-13485	Actualización de seguridad de bind: https://rhn.redhat.com/errata/RHSA-2015-0672.html
ASOC-13454	Actualización de seguridad de bind: https://rhn.redhat.com/errata/RHSA-2015-1705.html
ASOC-15390	Actualización de seguridad de postgresql: https://rhn.redhat.com/errata/RHSA-2015-2081.html
ASOC-13477	Actualización de seguridad de postgresql: https://rhn.redhat.com/errata/RHSA-2015-0750.html
ASOC-13478	Actualización de seguridad de krb5: https://rhn.redhat.com/errata/RHSA-2015-0794.html
ASOC-13507	Actualización de seguridad de postgresql: https://rhn.redhat.com/errata/RHSA-2015-1194.html
ASOC-13479	Actualización de seguridad de flac: https://rhn.redhat.com/errata/RHSA-2015-0767.html
ASOC-13509	Actualización de seguridad de openssl: https://rhn.redhat.com/errata/RHSA-2015-1072.html
ASOC-13484	Actualización de seguridad de openssl: https://rhn.redhat.com/errata/RHSA-2015-1115.html
ASOC-16367	Actualización de seguridad de openssl: https://rhn.redhat.com/errata/RHSA-2015-2617.html
ASOC-14286	Actualización de seguridad de ntp: https://rhn.redhat.com/errata/RHSA-2015-1930.html
ASOC-13505	Actualización de seguridad de ntp: https://rhn.redhat.com/errata/RHSA-2015-1459.html
ASOC-13513	Actualización de seguridad de grep: https://rhn.redhat.com/errata/RHSA-2015-1447.html
ASOC-14475	Actualización de seguridad de nss-softokn: https://rhn.redhat.com/errata/RHSA-2015-1699.html
ASOC-13508	Actualización de seguridad de nss: https://rhn.redhat.com/errata/RHSA-2015-1185.html
ASOC-13515	Actualización de seguridad de sudo: https://rhn.redhat.com/errata/RHSA-2015-1409.html
ASOC-16193	Actualización de seguridad de libxml2: https://rhn.redhat.com/errata/RHSA-2015-2549.html
ASOC-13516	Actualización de seguridad de libxml2: https://rhn.redhat.com/errata/RHSA-2015-1419.html
ASOC-13517	Actualización de seguridad de net-snmp: https://rhn.redhat.com/errata/RHSA-2015-1385.html
ASOC-13518	Actualización de seguridad de curl: https://rhn.redhat.com/errata/RHSA-2015-1254.html
ASOC-16195	Actualización de seguridad de libpng: https://rhn.redhat.com/errata/RHSA-2015-2594.html

Número de rastreo	Descripción
ASOC-13968	Actualización de seguridad de gdk-pixbuf2: https://rhn.redhat.com/errata/RHSA-2015-1694.html
ASOC-15395	Actualización de lighttpduax de la versión 1.4.35 a la versión 1.4.37
ASOC-11378	Actualización de seguridad de PFRing: https://rhn.redhat.com/errata/RHSA-2015-1272.html
ASOC-15473	El servidor de Security Analytics muestra páginas de error detalladas para indicar el seguimiento regresivo de Java en el cual falla un elemento de la aplicación web.
ASOC-15263	La actualización de la biblioteca Apache Commons Collections (ACC) de la versión 3.2.1 a la versión 3.2.2
ASOC-15482	La interfaz del usuario muestra la ruta absoluta de los archivos del lado del servidor
ASOC-6938	El certificado personalizado en el servidor web de SA no se conserva después de la actualización a 10.4/10.5
ASOC-16418 SACE-3775	Redireccionamiento de HTTP a HTTPS
ASOC-14888	Envío de las credenciales de la cuenta del servicio Active Directory al usuario
ASOC-2255	Security Analytics ya no es compatible con el conjunto de aplicaciones de cifrado *RC4* en los protocolos TLS/SSL

Reparaciones generales

Número de rastreo	Descripción
ASOC-11521	Cuando inicia sesión en Security Analytics mediante un navegador Internet Explorer 10, algunas páginas no se cargan correctamente. El problema está actualmente solucionado.

Reparaciones en Log Collector

Número de rastreo	Descripción
ASOC-15761	Se muestra un mensaje de error de LDEP aunque las líneas de espera vacías se eliminaron.
ASOC-13424	Desvinculación de identificador y/o eliminación de línea de espera correctos cuando se elimina un feed de identidad o LDEP.
ASOC-15283	Se muestran entradas duplicadas en el panel Detalles del navegador de estadísticas.
ASOC-15203	La eliminación parcial de LDEP envía mensajes de advertencia al registro.
ASOC-13954	El servidor de Security Analytics determina automáticamente si se trata de un Local Log Collector o de un Remote Log Collector.

Reparaciones en Malware Analysis

Número de rastreo	Descripción
ASOC-10478	Un servicio Malware independiente que se ejecuta en un ambiente virtual tardará aproximadamente 20 minutos en abrirse después de la habilitación de FIPS. El problema está actualmente solucionado.
ASOC-15468	El registro de auditoría de syslog de Malware Analysis no muestra todos los valores de metadatos. El problema está actualmente solucionado.

Reparaciones en Incident Management

Número de rastreo	Descripción
ASOC-11726	Se agregaron datos de contexto útiles de Incident Management que permiten tomar decisiones más informadas. Entre los datos nuevos se incluyen: número de incidente, nombre/descripción de incidente, prioridad de incidente, estado de incidente, hora de creación de incidente, origen de incidente, puntaje de riesgo de incidente, cantidad de alertas asociadas y metadatos (host y usuario) en una alerta asociada con un incidente.
ASOC-11882	Ahora se utiliza una regla de agregación de Incident Manager para combinar varias alertas de puntaje de indicadores de detección de amenazas para un dominio en un incidente. La regla busca una alerta generada a partir del puntaje de agregación de C2 y, a continuación, recopila todas las alertas relacionadas con el dominio sospechoso que se generan durante la semana siguiente.
ASOC-12106	Cuando se crea una regla nueva, la opción Dominio ahora está disponible en la lista desplegable Agrupar por en Incidentes > Configurar.
ASOC-12683	Aparecen valores no válidos en el campo Días abierta en Incidentes> Corrección> Tareas de corrección cuando la interfaz del usuario se establece en una configuración regional distinta de inglés. El problema está actualmente solucionado.
ASOC-14183	Se agregaron los elementos Dominio, datos de registro de dominio y puntaje de indicador C2 a la pantalla Ver detalles de incidente. Esta información ahora se incluye cuando se observan detalles de incidentes.
ASOC-14342	La versión predeterminada de Java está configurada en 1.7, lo cual hace que falle el inicio de jettysrv durante la actualización de 10.5.1 a 10.6.
ASOC-15105	Las alertas ahora se enumeran en orden de severidad en lugar de puntaje de riesgo para brindar una experiencia similar a la de Incident Management en el panel de contexto. De esta manera, el usuario no se confunde en relación con la forma en que se da prioridad a los elementos. De manera predeterminada en Incident Management, las alertas se muestran inicialmente por severidad y no por puntaje de riesgo.
ASOC-15581	En la pestaña Datos de contexto, el nombre de usuario debe ser igual que el valor de metadatos del registro crudo.

Última modificación: 18 de febrero de 2016, 14:12 h

Reparaciones en Event Stream Analysis

Número de rastreo	Descripción
ASOC-10429	El campo Reglas activadas de la pestaña Alertas > Servicios no mostraba el conteo de reglas correcto. Ahora, el campo Reglas activadas muestra el conteo correcto de reglas habilitadas.
ASOC-12259	En versiones anteriores, el parámetro **ServerCertificateValidateEnable** de Event Stream Analysis estaba configurado en false de manera predeterminada. El certificado del cliente para el modo TCP seguro se obtenía del área de almacenamiento de confianza de ESA. Ahora, puede configurarlo en true y agregar los certificados al área de almacenamiento de confianza de Security Analytics. ⚠ **Precaución:** Si seleccionó el modo TCP seguro para la notificación de syslog, debe asegurarse de que el parámetro **ServerCertificateValidateEnable** se configure en true. Los certificados para el cliente de syslog se deben agregar al almacenamiento de claves java de ESA para habilitar la notificación de syslog seguro.
ASOC-14724 ASOC-15888	Anteriormente, en la página Resumen de alertas > sección Metadatos adicionales, había vínculos rotos a la página Investigaciones. Ahora, cuando se hace clic en un vínculo de la sección Metadatos adicionales, la página Investigaciones se carga en una pestaña del navegador nueva.

Reparaciones y mejoras en la creación de informes

Número de rastreo	Descripción
ASOC-13175	En la pantalla Ver informe, puede seleccionar para cada regla la cantidad de registros que desea ver por página, como 10, 30, 50,100, 250 y 500.
ASOC-12022	Se implementó un gráfico histórico para los gráficos de Live. Puede extraer datos antes de la fecha de habilitación del gráfico. También puede optar por una notificación una vez que se haya completado la búsqueda. El widget de fecha y hora también se modificó con algunos cambios de etiqueta para los tipos de gráficos.
ASOC-11611	Después de la habilitación del gráfico, los datos del gráfico para las últimas tres a seis horas, según el intervalo de tiempo, se obtendrán automáticamente para el usuario.
ASOC-9549 SATCE-923	Durante la creación de un dashlet de gráfico de Live, se agregó un nuevo botón Navegar que permite ver los grupos de gráficos completos y el nombre del gráfico.
ASOC-2163	El widget Rango de tiempo de Ver gráfico cambió y se conservará el último rango de tiempo seleccionado cuando se abra el mismo informe de gráfico.
ASOC-2164	Las etiquetas del gráfico de resumen y del gráfico de serie de tiempo ahora coinciden con su definición real.
ASOC-9548 SATCE-908	Se mejoraron las leyendas de modo que fueran más legibles y se les agregó un botón de desplazamiento.

Reparaciones en los servicios principales

Entre los servicios de Security Analytics Core se incluyen Archiver, Broker, Concentrator, Decoder y Log Decoder.

Número de rastreo	Descripción
SACE-4853	Se corrigieron varios problemas relacionados con RESTful API que causaban interbloqueos o fallas generales del proceso en todos los servicios principales.

Problemas conocidos

En esta sección se describen los problemas que permanecen pendientes en esta versión. Si está disponible una solución alternativa o una reparación, esto se indica o se menciona en detalle.

Nota: Los problemas conocidos de las versiones anteriores de Security Analytics se pueden solucionar en los service packs. Consulte las notas de la versión de los service packs correspondientes que están disponibles en SecurCare Online: https://knowledge.rsasecurity.com.

Instalación y actualización

La actualización falla si el parche de seguridad no está instalado

Número de rastreo: ASOC-9062

Problema: Cuando se actualiza de 10.4.x a 10.5.1 y el parche de seguridad del segundo trimestre de 2015 o anterior no está instalado, la comprobación de la actualización no identifica algunas actualizaciones y la actualización falla.

Solución alternativa: Cuando se complete la actualización, busque una actualización y vuelva a aplicarla (si la hay).

Cuando se actualiza de 10.4.1 a 10.6, la actualización puede fallar

Número de rastreo: ASOC-13369

Problema: Cuando se actualiza de 10.4.1 a 10.6, la actualización puede fallar. Esto se debe a que se usa el repositorio de CentOS para obtener las actualizaciones.

Solución alternativa: Debe actualizar 10.4.1 a 10.4.1.1 o 10.4.1.2 antes de actualizar a 10.6, ya que este problema se resolvió en 10.4.1.1 o en las versiones superiores.

Después de la actualización de 10.4.x a 10.6, FIPS se inhabilita

Número de rastreo: ASOC-13748

Problema: Si FIPS está habilitado y se realiza una actualización de 10.4.x a 10.6, se inhabilita. Esto se debe a la actualización de la versión de Java (1.7 a 1.8).

Solución alternativa: Debe volver a habilitar FIPS.

Última modificación: 18 de febrero de 2016, 14:12 h

El servicio Malware Colo está inactivo inmediatamente después de la implementación

Número de rastreo: ASOC-15732

Problema: Inmediatamente después de la implementación de un ISO u OVA, Malware Colo está inactivo, ya que el almacenamiento de claves Carlos no está configurado correctamente.

Solución alternativa: Después de la implementación, espere 30 minutos (para que Puppet se ejecute y configure correctamente el almacenamiento de claves Carlos) y reinicie el servicio Malware (`restart rsaMalwareDevice`).

Después de la actualización a 10.6.0.0, la agregación no se inicia si las reglas de correlación están escritas en sintaxis obsoleta

Número de rastreo: ASOC-15695

Problema: Después de la actualización a 10.6.0.0, las reglas de correlación escritas en sintaxis obsoleta pueden hacer que los Decoders o los Concentrators se inicien en un estado fallido. Las reglas que coinciden con el formato estricto no causan este problema.

Solución alternativa: Cambie las reglas de correlación con sintaxis obsoleta a la sintaxis de formato estricto. Compruebe las reglas de correlación en **Administration > Servicios** (seleccione un Decoder, un Log Decoder o un Concentrator) **> Configuración > pestaña Reglas de correlación**. Las reglas con sintaxis obsoleta aparecen resaltadas. Para cada regla obsoleta, edite la regla, corrija la sintaxis en el campo **Condición** y haga clic en **Guardar**. Cuando haya corregido todas las reglas de correlación, reinicie el servicio.

Problemas generales de las aplicaciones

Error Página no mostrada durante el inicio de sesión mediante el navegador IE 10

Número de rastreo: ASOC-9225

Problema: Cuando inicia sesión en Security Analytics mediante un navegador Internet Explorer 10, se puede mostrar el siguiente mensaje de error: `La página no se puede mostrar`.
Esto se puede deber a que el protocolo TLS 1.2 no está habilitado en su navegador.

Solución alternativa: Además de los otros protocolos, habilite el protocolo TLS 1.2 en el navegador de la siguiente manera:

1. Navegue a **Opciones de Internet > Opciones avanzadas > Configuración > Seguridad**.
2. Asegúrese de que el protocolo TLS 1.2 esté habilitado.
3. Haga clic en **Aplicar** y vuelva a cargar la página.

Problemas generales de la plataforma

No está disponible una opción Cancelar para las tareas de Analítica de warehouse

Número de rastreo: SAENG-4706

Problema: Una vez que se inicia la tarea de Analítica de warehouse, no hay ninguna opción que permita cancelarla.

Solución alternativa: Debe interrumpir manualmente la tarea. Los siguientes son los pasos necesarios para interrumpir la tarea:

Para MapR:

1. Obtenga el Jobid en los logs de la tarea.
2. Inicie sesión en la interfaz del usuario de jobtracker y busque el Jobid que interrumpirá bajo “Tareas en ejecución”. Ejemplo de URL: http://<job-tracker-host>:50030/jobtracker.jsp
3. Interrumpa el Jobid:
   - Seleccione **Jobid en Trabajos en ejecución** y haga clic en **Interrumpir trabajos seleccionados**.

     (o)

   - Haga clic en el enlace Jobid, desplácese hacia abajo y haga clic en el enlace **Interrumpir esta tarea**.

Para Pivotal:

1. Obtenga el Jobid en los logs de la tarea.
2. Interrumpa el Jobid.
   Por ejemplo:
   ```
   mapred job -list
   mapred job -kill job_1406294496331_0385
   ```
   o
   ```
   yarn application -list
   yarn application -kill application_1406294496331_0385
   ```

Autorizaciones

La licencia medida no regresa de inmediato a la condición de cumplimiento de normas cuando no hay servicios conectados a ella

Número de rastreo: ASOC-9078

Problema: Por ejemplo, si hay una licencia medida disponible para un Log Decoder y bajo esta se enumera un Log Decoder, pueden ocurrir las siguientes condiciones:

- Superó el uso autorizado y se señala que está en una condición de incumplimiento de normas.
- Decide cambiar el Log Decoder a una licencia basada en servicios disponible.
- Bajo la licencia medida no hay ningún servicio.
- La licencia medida regresa a un estado de cumplimiento de normas después de siete días.

Solución alternativa: Ninguna.

El informe de uso agregado se genera cada vez que se conecta un servicio a una licencia y se selecciona “Todo” mientras se exportan estadísticas de uso

Número de rastreo: ASOC-10079

Problema: Para cualquier tipo de licencia (Todo/Medidas/Basadas en servicio), el archivo PDF/CSV agregado se debe generar solo cuando se enumera más de un servicio bajo cualquier tipo de licencia.

Solución alternativa: Ninguna.

Cuando se cambia el tipo de licencia de un servicio, el uso que se muestra contra el servicio después del cambio incluye el uso pasado para ese día.

Número de rastreo: ASOC-10685

Problema: Para cualquier servicio cuyo tipo de licencia se cambia, el uso que se muestra contra el servicio después del cambio continúa incluyendo el uso pasado para ese día.

Solución alternativa: Ninguna.

Log Collector

Se muestran mensajes de error repetidos si el nombre del dominio no se puede resolver desde la computadora de LWCS

Número de rastreo: SAENG-2476

Problema: Cuando se intenta acceder a registros de Windows desde la máquina A en un dominio/grupo de trabajo que está en otro dominio, y si LWCS no resuelve el nombre del dominio de la máquina A, se muestra un mensaje de error para cada evento recopilado.

Solución alternativa: Agregue la entrada del dominio al archivo de host de la computadora existente que no se puede resolver.

Falta la función DPO en Log Collector

Número de rastreo: ASOC-7937

Problema: La nueva función Encargado de la privacidad de datos no existe en Log Collector.

Solución alternativa: Ninguna.

La recopilación de punto de comprobación no funciona y se muestra el error “el par terminó la sesión”

Número de rastreo: ASOC-8351

Problema: La recopilación de punto de comprobación no funciona y los registros muestran el error: **el par terminó la sesión**

Solución alternativa: Para resolver este problema:

1. Realice un respaldo y elimine el archivo de posición del punto de comprobación (**/var/netwitness/logcollector/runtime/checkpoint/ eventsources/checkpoint.CP_Security.xml**).
2. Reinicie el servicio para volver a generar el archivo.
3. (Opcional) Si la opción **Tiempo máximo de inactividad de encuesta** está configurada en 0, configúrela en 5.

Se genera un mensaje inexacto para un error de la recopilación de AWS

Número de rastreo: ASOC-9586

Problema:

En la recopilación de Amazon Web Service (AWS) CloudTrail, cuando falta el archivo de transformación en `/etc/netwitness/ng/logcollection/content/transform/cmdscript`, Security Analytics muestra el siguiente mensaje de error inexacto:

Error: no se pudo encontrar el tipo de archivo compatible en el archivo /etc/netwitness/ng/logcollection/content/collection/cmdscript/ cloudtrail_transform.xml

La ruta correcta es `etc/netwitness/ng/logcollection/content/`**`transform`**`/cmdscript/cloudtrail_transform.xml.`

Solución alternativa:

1. Verifique la falta de `etc/netwitness/ng/logcollection/content/transform/cmdscript/cloudtrail_transform.xml`.
2. Recupere el contenido más reciente de **RSA Log Collector** e impleméntelo.

Error en la regulación del ancho de banda de un Remote Collector a un Local Collector

Número de rastreo: ASOC-16717

Problema:

Los cambios en la configuración de la regulación del ancho de banda para controlar la velocidad a la cual el Remote Collector envía datos de eventos a un Local Collector no persisten después de un reinicio.

El script `set-shoveltransfer-limit.sh` se utiliza para configurar la regulación del ancho de banda para los datos de eventos que se transfieren desde un Remote Collector a un Local Collector. El script utiliza reglas iptables y filtros de conformación de tráfico del kernel de Linux para controlar el ancho de banda de carga que usa el puerto RabbitMQ en las transferencias a un colector ascendente. El script funciona correctamente cuando se ejecuta, pero no conserva los valores de los filtros de conformación de tráfico una vez que el dispositivo se reinicia.

Solución alternativa:

Agregue la ejecución del script a `/etc/rc.local` en el Remote Collector, como se muestra en el siguiente ejemplo:

```
"/opt/netwitness/bin/set-shovel-transfer-limit.sh -s -r 4096kbit"
```

Investigation

La opción Ver > Correo electrónico de la reconstrucción de evento con presentación De arriba abajo no muestra información de respuesta.

Número de rastreo: ASOC-5690

Problema: Ver correo electrónico de la reconstrucción de eventos con presentación De arriba abajo no muestra información de respuesta si no hay datos de correo para mostrar en esa vista.

Solución alternativa: La información de error se muestra en la vista de respuesta cuando se selecciona la presentación En paralelo.

La extracción de PCAP puede llenar la carpeta del calendarizador y esto hace que el servidor de Security Analytics se apague

Número de rastreo: ASOC-6874

Problema: A medida que transcurre el tiempo, los analistas que ejecutan extracciones de archivos pueden llenar la partición de la línea de espera de trabajos en el servidor de Security Analytics y hacer que este se apague.

Solución alternativa: Utilice las políticas de uso inmediato de Estado y condición para monitorear el volumen de disco y enviar una alerta antes de que la partición de la línea de espera de trabajos se llene.

El desglose a la vista Investigation desde un informe causa un error cuando el valor de metadatos termina en comillas

Número de rastreo: ASOC-7053

Problema: Si el valor de metadatos termina en comillas (por ejemplo, si el valor para el metadato `filename` es `'$%&'()*+^^- .'`), el desglose desde un informe muestra el siguiente error: **Falta comilla de cierre: se encontró comilla de inicio sin comilla de cierre…**

Solución alternativa: Ninguna.

El botón Siguiente no queda inhabilitado para el último evento en la vista Reconstrucción

Número de rastreo: ASOC-7577

Problema: El uso de los botones Siguiente < > para ir de un evento a otro en la ventana Reconstrucción de evento no indica cuándo se llega al último evento.

Solución alternativa: Ninguna.

Las claves de metadatos no se actualizan correctamente cuando se navega entre múltiples perfiles

Número de rastreo: ASOC-7743 (SACE-2881)

Problema: Las claves de metadatos que se indexan se muestran como no indexadas cuando el usuario cambia entre múltiples perfiles.

Solución alternativa: Cambie del perfil de metadatos actual al perfil de metadatos anterior y nuevamente al actual.

La visualización de coordenadas paralelas no muestra correctamente los caracteres especiales

Número de rastreo: ASOC-9346

Problema: Cuando se configura la clave de metadatos `content type` como uno de los metadatos para el eje, si el valor de metadatos contiene caracteres especiales, los valores no se muestran correctamente.

Solución alternativa: Ninguna.

La búsqueda en el valor de LISTA muestra la misma LISTA dos veces en el panel Búsqueda de Investigation

Número de rastreo: ASOC-16573

Problema: Cuando se realiza una búsqueda de contexto en valores de metadatos con una entrada de lista, la búsqueda muestra la misma lista dos veces en el panel Búsqueda de Investigation. Este problema ocurre de manera inconstante.

Solución alternativa: Reinicie el servicio Context Hub.

La utilización del CPU se dispara cuando la búsqueda de contexto se realiza con listas que tienen más de 5,000 valores

Número de rastreo: ASOC-16460

Problema: Si se crean listas personalizadas grandes, el servicio Context Hub puede consumir un gran porcentaje (p. ej., un 70 %) de los ciclos de procesamiento en Event Stream Analysis, lo cual hace que los resultados de la búsqueda para las listas sean mucho más lentos que lo normal.

Solución alternativa: Para minimizar la posible carga de recursos, se recomienda que la cantidad de entradas en una lista sea menor que 5,000.

Los incidentes no se marcan cuando un usuario agrega manualmente las alertas a un incidente existente

Número de rastreo: ASOC-16640

Problema: Los valores de Investigation no se resaltan cuando se han agregado alertas manualmente a un incidente en Incident Management. Las alertas que se agregan de manera dinámica a un incidente se resaltan.

Solución alternativa: Ninguna

Workbench

El rango de datos no se muestra para una recopilación si el servicio Workbench o Jettysrv se reinician mientras la restauración está en curso

Número de rastreo: ASOC-6822

Problema: El rango de fechas no se muestra para una recopilación si el servicio Workbench o Jettysrv se reinician mientras la restauración está en curso.

Solución alternativa: Ninguna.

Se crea una recopilación vacía si la restauración falla debido a la detención o el reinicio del servicio Workbench

Número de rastreo: ASOC-6859

Problema: Se muestra una recopilación vacía en la pestaña Recopilaciones si el servicio Workbench se detiene o se reinicia durante el proceso de restauración

Solución alternativa: Ninguna.

La creación de una recopilación en Workbench 10.4 desde la interfaz del usuario de 10.5 o superior no crea ninguna entrada de trabajo y la recopilación solo aparece en la interfaz del usuario después que se actualiza la página

Número de rastreo: ASOC-8368

Problema: Si crea una recopilación en un Workbench 10.4 desde una interfaz del usuario de 10.5 o superior, no se crea ninguna entrada de trabajo en la página Trabajos y la recopilación solo aparece en la interfaz del usuario después de que se actualiza la página.

Solución alternativa: Ninguna.

En todas las recopilaciones de restauración creadas en 10.4 habrá valores de Rango de fechas y Fecha de creación en blanco después de la actualización a 10.5 o superior

Número de rastreo: ASOC-9035

Problema: Las recopilaciones creadas en un Workbench 10.4 mostrarán valores de Rango de fechas y Fecha de creación en blanco después de la actualización a 10.5 o superior.

Solución alternativa: Ninguna.

En las recopilaciones de restauración creadas en la vista Explorador habrá un rango de fechas en blanco en la pestaña Recopilaciones de la interfaz del usuario

Número de rastreo: ASOC-9087

Problema: Una recopilación de restauración que no se crea a través de la interfaz del usuario de Security Analytics mostrará un rango de fechas vacío en la interfaz del usuario.

Solución alternativa: Ninguna.

Última modificación: 18 de febrero de 2016, 14:12 h

Malware Analysis

No es posible realizar escaneos según demanda de Malware Analysis mediante conexiones de confianza

Número de rastreo: SAENG-5485

Problema: No es posible realizar escaneos según demanda de Malware Analysis mediante conexiones de confianza debido a que Malware Analysis espera un nombre de usuario/contraseña, pero esta información no existe para las conexiones de confianza.

Solución alternativa: Vuelva a ejecutar el proceso de conexiones de confianza en Concentrator:

1. Desactive las conexiones de confianza para Concentrator.
2. Ejecute la prueba de la conexión y guarde.
3. Edite el servicio Concentrator y active las conexiones de confianza (elimine las credenciales).
4. Ejecute la prueba de la conexión y guarde.

Los usuarios que tienen la función Analista no pueden ejecutar un escaneo de malware según demanda

Número de rastreo: ASOC-5425

Problema: Un usuario al que se asignó la función Analista tiene acceso a los módulos Investigation y Malware Analysis. Sin embargo, cuando el usuario intenta ejecutar el escaneo de Malware Analysis según demanda desde la pantalla Investigation, este falla y muestra un error de nombre de usuario no válido. El trabajo se envía, pero falla debido a las credenciales.

Solución alternativa: Ninguna.

Si el dispositivo principal no está configurado con una dirección IP, la opción Ver sesión de red se inhabilita para eventos de Malware Analysis.

Número de rastreo: ASOC-5571

Problema: Debido al nuevo ID del servicio y a cambios en Agrupación de dispositivos y servicios (ASG), Malware Analysis no muestra la opción Ver sesión de red desde el Resumen de eventos de Malware. Parece que el ID del dispositivo llega nulo.

Solución alternativa: Ninguna.

Última modificación: 18 de febrero de 2016, 14:12 h

El Resumen de eventos de Malware Analysis no carga todos los dashlets, a menos que el usuario vuelva a actualizar la página.

Número de rastreo: ASOC-5959

Problema: En la carga inicial, el Resumen de eventos de Malware no carga todos los dashlets.

Solución alternativa: Se cargan cuando el usuario vuelve a actualizar la página.

La carga de un trabajo de escaneo no se envía a Colo Malware si también está presente Malware independiente en Security Analytics

Número de rastreo: ASOC-9821

Problema: Cuando Malware Analysis independiente y en la misma ubicación existen en un ambiente Security Analytics, los comandos de escaneo de archivos se enviarán a Malware Analysis independiente y no a Malware Analysis en la misma ubicación.

Solución alternativa: Ninguna.

La habilitación o inhabilitación de TODOS los indicadores de riesgo no tiene un comportamiento correcto

Número de rastreo: ASOC-13857

Problema: Cuando se inhabilitan o habilitan indicadores de riesgo (IOC) en Malware Analysis, se requiere un comando de actualización del navegador antes de que se siga el comando.

Solución alternativa: Utilice el botón de actualización del navegador para ver la lista de IOC actualizada.

Incident Management

Problema del paquete Java cuando se actualiza a 10.6

Número de rastreo: ASOC-12411

Problema: El servicio puppet se podría bloquear cuando se actualiza a 10.6. La versión de Java se restablece a 1.7 y no se vuelve a configurar en 1.8, incluso después de un reinicio del sistema.

Solución alternativa: Ninguna.

Ver evento original devuelve el seguimiento de pila cuando no hay ningún Concentrator disponible.

Número de rastreo: ASOC-14266

Problema: Cuando un usuario no tiene el Concentrator en línea que se enumeraba en la alerta, hace clic en el engranaje de un evento bajo los detalles de la alerta en el servicio Incident Management y, a continuación, elige **"Ver evento original"**, el usuario recibe un seguimiento de pila. Esto se debe a que el Concentrator no está funcionando.

Solución alternativa: Ninguna.

Las reglas de agregación de uso inmediato en Incident Management se duplican después de la actualización a 10.6

Número de rastreo: ASOC-15031

Problema: Después de la actualización a Security Analytics 10.6, hay dos conjuntos de las mismas reglas de agregación de uso inmediato para Incident Management. Esto puede causar ambigüedad si se habilitan ambos conjuntos de estas reglas.

Solución alternativa: Cuando habilite reglas, asegúrese de no habilitar las reglas de agregación de uso inmediato duplicadas de Incident Management.

Después de la configuración de MongoDB, el servicio se debe reiniciar

Número de rastreo: SAIM-355

Problema: Para configurar MongoDB en Incident Management (IM), el servicio Incident Management debe señalar a una base de datos en el host de ESA. Los cambios no se aplican de inmediato.

Solución alternativa: Después de la configuración de MongoDB para Incident Management, debe reiniciar el servicio Incident Management.

Event Stream Analysis

El orden que distingue mayúsculas de minúsculas no funciona correctamente en la cuadrícula Todas las reglas de ESA.

Número de rastreo: SAENG-3605

Problema: Cuando los nombres de regla comienzan con letras en minúsculas y mayúsculas, el orden no funciona correctamente en la columna Nombre de la regla de la cuadrícula Todas las reglas de ESA. Por ejemplo, a "Regla 1" no le sigue "Regla 2" cuando se ordena por nombre.

Solución alternativa: Ninguna.

La implementación (denominada sincronización en 10.4 y anterior) falla si se implementa esta regla desde RSA Live: No se detectó tráfico de registros desde un dispositivo en un intervalo de tiempo determinado

Número de rastreo: SAENG-5888

Problema: La implementación, anteriormente denominada sincronización, falla para la regla “No se detectó tráfico de registros desde un dispositivo en un intervalo de tiempo determinado” que se implementó desde Live. Este problema no se observa si implementa las reglas desde Live en una configuración de 10.4 y realiza la sincronización. El problema se observa si actualiza el sistema desde una versión anterior a 10.4 en la cual las reglas se implementan desde Live con ID de módulo incorrectos.

Solución alternativa: Elimine las reglas con ID de módulo incorrectos y vuelva a implementarlas desde Live.

La implementación falla si el servidor que aloja una base de datos queda inactivo

Número de rastreo: ASOC-9011

Problema: Una conexión de base de datos se configura para usar la base de datos como un origen de enriquecimiento para una regla. Se implementa una referencia a la base de datos en cada ESA, incluso si ESA no implementa ninguna regla que usa la base de datos. Si el servidor que aloja la base de datos queda inactivo, cualquier implementación nueva fallará.

Solución alternativa: Reinicie el servidor que aloja la base de datos.

El panel de alertas no se carga cuando el tamaño de MongoDB es demasiado grande

Número de rastreo: ASOC-9026

Problema: En Security Analytics 10.4, el panel de alertas no se carga cuando el tamaño de MongoDB es demasiado grande.

Solución alternativa: Debe habilitar al mantenimiento automatizado del almacenamiento de ESA para reducir el tamaño de MongoDB.

El nombre de la regla de reenvío no se actualiza cuando cambia el nombre de una regla avanzada

Número de rastreo: ASOC-9585

Problema: Para una implementación entre sitios, la regla de reenvío no cambia junto con el cambio de nombre de una regla avanzada. Esto puede dar lugar a una regla huérfana, la cual puede continuar con el reenvío de eventos.

Solución alternativa: Para cambiar el nombre de una regla avanzada entre sitios, cree una regla nueva y elimine la anterior.

Última modificación: 18 de febrero de 2016, 14:12 h

Falla de una regla con Agrupar por que usa metadatos de múltiples valores

Número de rastreo: ASOC-15802

Las reglas que contienen una declaración agrupar por con metadatos de múltiples valores (como alias_host) fallan.

Solución alternativa: Ninguna.

La regla de ESA no activa una alerta para el contenido actualizado del enriquecimiento en la memoria utilizado en la regla

Número de rastreo: ASOC-16396

Cuando una regla se crea y se implementa mediante un enriquecimiento en la memoria y posteriormente se quitan o se agregan filas del archivo .CSV, si la regla correspondiente se implementa, las alertas no se activan según lo previsto.

Solución alternativa: Si se agregan filas al archivo .CSV, elimine la regla de la implementación y vuelva a implementarla. Sin embargo, si se eliminan filas esta solución no funciona. En el caso de las filas eliminadas, puede aplicar una solución alternativa para este problema si elimina el origen de enriquecimiento existente (por medio de Alertas > Configurar > Ajustes de configuración > Orígenes de enriquecimiento) y carga el archivo .CSV actualizado con otro nombre. A continuación, agregue manualmente el enriquecimiento en la regla a la regla y vuelva a implementar la regla.

La configuración de WhoIsHTTPSProxy no se guarda si se usa sintaxis incorrecta

Número de rastreo: ASOC-16494

Cuando se configura el ajuste WhoisHTTPSProxy del servicio WhoIs, si el formato que se usa no corresponde a http://<host>:<port> o https://<host>:<port>, el mensaje indica erróneamente que la configuración se guardó de manera correcta. Cuando el usuario vuelva a cargar la página, el ajuste regresará a la configuración anterior.

Solución alternativa: Ninguna.

Cuando se configura el orden por hora de la captura (flujo habilitado), las estadísticas de uso de la memoria se muestran de manera incorrecta en Estado y condición

Número de rastreo: ASOC-16613

Si configuró el orden por hora de la captura (mediante Explorador > Flujo de trabajo > Origen > nextgenAggregationSource y estableció StreamEnabled en true), las estadísticas para rastrear el uso de la memoria muestran un valor de 0 en las estadísticas de Estado y condición.

Solución alternativa: El atributo asociado con cada una de estas reglas se puede examinar en el registro de ESA desde Tablero > Host > Visualizaciones > Registros o en el host de ESA (/opt/rsa/esa/logs/esa.log). Las entradas relacionadas se pueden buscar con el uso de “Bytes de memoria de estimados” y las estadísticas en un nivel de regla se enumeran como “TYPE=MDUL”. De forma predeterminada, el nivel de registro para las métricas de la memoria está configurado en “Módulo”.

Última modificación: 18 de febrero de 2016, 14:12 h

Reporting Engine

Algunos informes de cumplimiento de normas no se pueden implementar desde Live

Número de rastreo: SAENG-1334

Problema: Si las dependencias de ciertos informes de cumplimiento de normas en Live no se implementan antes que los propios informes, la implementación de estos falla.

Solución alternativa: Vuelva a intentar la implementación. Si el problema persiste, intente implementar primero las dependencias de regla o de lista y, a continuación, implemente los informes.

Algunas alertas de Reporting pueden fallar o retrasarse si la conexión RabitMQ está bloqueada

Número de rastreo: SAENG-5329

Problema: Si la opción **Reenviar alertas a IM** está habilitada y las conexiones de RabbitMQ a Incident Management están bloqueadas, algunos de los hilos de ejecución de Reporting Engine se pueden bloquear.

Solución alternativa: Inhabilite la opción **Reenviar alertas a IM** hasta que el intermediador de RabbitMQ en el servidor de Security Analytics en Incident Management se haya iniciado y pueda aceptar las conexiones.

Las actualizaciones a los parámetros de conexión en la página Servicio no se reflejan en los orígenes de datos de Reporting

Número de rastreo: ASOC-8149

Problema: Si hay cambios o actualizaciones a nombres de servicio, puertos o parámetros en la página Servicio, estos no se propagan a los orígenes de datos correspondientes agregados en Reporting Engine.

Solución alternativa: Agregue los orígenes de datos con el servicio modificado y úselos. Además, si se modifican los nombres de los servicios existentes, los calendarios correspondientes se deben actualizar en Reporting.

No es posible navegar a Investigation desde los informes de NWDB si se actualizan los parámetros de conexión en la página Servicio

Número de rastreo: ASOC-8575

Problema: El vínculo Investigation para los valores de metadatos de los informes ejecutados no se muestra en la página de resultados de NWDB.

Solución alternativa: Ninguna. Se corregirá en una versión futura.

Última modificación: 18 de febrero de 2016, 14:12 h

Informes

Los resultados de Probar regla con datos grandes no se muestran en Internet Explorer 10

Número de rastreo: SAENG-3926

Problema: Cuando hace clic en **Probar regla** varias veces en rápida sucesión, es posible que los resultados con datos de entrada grandes no se muestren en Internet Explorer 10.

Solución alternativa: Si se presenta este problema, intente uno de los siguientes pasos:

- Cierre la ventana Probar regla en Internet Explorer 10 y vuelva a ejecutar la prueba.
- Use otros navegadores como Chrome o Mozilla Firefox para probar la ejecución de la regla.

No es posible agregar listas dinámicas cuando se edita un calendario de informes desde la página Ver todos los calendarios

Número de rastreo: SAENG-5837

Problema: No se puede agregar una lista dinámica a un calendario existente desde la opción Editar en la página “Ver todos los calendarios”.

Solución alternativa: Edite el calendario desde la página Calendario de informes para agregar una lista dinámica.

Se espera un mensaje de error apropiado para las reglas que se ejecutan con una lista vacía

Número de rastreo: ASOC-16271

Problema: Cuando se ejecuta una regla con valores de lista vacíos para los metadatos numéricos, de dirección IP y de dirección Mac, la ejecución de la regla falla con el siguiente mensaje de error ambiguo: **Se produjo un error al obtener datos del origen**.

Solución alternativa: Cree una lista válida que contenga valores y úsela para la regla. Si se usa una lista válida, el error no se muestra.

Administration

Cuando se navega desde las vistas Configurar de los servicios principales a Estadísticas en la pestaña Servicios, los íconos se ven desordenados

Número de rastreo: ASOC-8803

Problema: Navegue a cualquiera de las vistas Configurar de los servicios principales y, a continuación, diríjase a Estadísticas para el mismo servicio. En Cambiar servicio, seleccione otro servicio principal y elija Configurar. En Acciones, diríjase a Estadísticas y verá que los íconos están desordenados.

Solución alternativa: Ninguna.

El evento de auditoría de configuración que capturó SA no incluye contexto del servicio que se modificó

Número de rastreo: ASOC-8889

Problema: El servidor de Security Analytics no captura el servicio objetivo aplicable para los cambios en la configuración en los eventos de auditoría.

Solución alternativa: Ninguna.

Se registra un exceso de registros de auditoría cuando se accede a las páginas de la interfaz del usuario de SA y se importa, se exporta, se inicia sesión y se cierra sesión desde esta interfaz del usuario

Número de rastreo: ASOC-8916

Problema: Security Analytics crea una cantidad excesiva de registros de auditoría cuando sus usuarios inician sesión, cierran sesión, importan, exportan y acceden a páginas desde la interfaz del usuario de Security Analytics.

Solución alternativa: Ninguna.

Registros de auditoría: SA_SERVER no captura el valor de queryString

Número de rastreo: ASOC-8994

Problema: Cuando se cambia el contenido de un archivo de un servicio de Security Analytics, los registros de auditoría del servidor de Security Analytics no indican qué archivo modificó el usuario.

Solución alternativa: Ninguna.

El correo electrónico de vencimiento de la contraseña no incluye información de origen

Número de rastreo: ASOC-9187

Problema: El correo electrónico de vencimiento de la contraseña que envía el servidor de Security Analytics no menciona el nombre ni la dirección URL del servidor de Security Analytics que lo envió. Si hay múltiples servidores de Security Analytics, es posible que el usuario no sepa dónde dirigirse para actualizar su contraseña.

Solución alternativa: Ninguna.

Los registros de auditoría no informan la página (nombre) a la que se accedió cuando el usuario intenta acceder a páginas de SA para las cuales no tiene permisos

Número de rastreo: ASOC-9323

Problema: Cuando un usuario intenta acceder a páginas de la interfaz del usuario de Security Analytics sin los permisos necesarios, los registros de auditoría no capturan los nombres de las páginas a las cuales accede el usuario.

Solución alternativa: Ninguna.

Si PKI está habilitada y se ve la interfaz del usuario de Security Analytics por primera vez, las etiquetas no se muestran correctamente

Número de rastreo: ASOC-12619

Problema: Si PKI está habilitada y se ve la interfaz del usuario de Security Analytics por primera vez, las etiquetas no se muestran correctamente.

Solución alternativa: Debe actualizar la página.

Security Analytics no considera la fecha de vencimiento de CRL (Siguiente actualización el) y no invalida el archivo CRL

Número de rastreo: ASOC-12992

Problema: Security Analytics no respeta la fecha de vencimiento de CRL (Siguiente actualización el) y no invalida el archivo CRL.

Solución alternativa: El administrador debe rastrear manualmente la fecha de vencimiento de CRL, eliminar el archivo CRL vencido e importar el más reciente.

Administración de orígenes de eventos

Las alarmas automáticas de ESM no funcionan en un dispositivo All-in-One (AIO)

Número de rastreo: ASOC-16588

Problema: El monitoreo automático no funciona para los datos recopilados mediante Log Decoder en un AIO. Las alarmas de políticas continuarán funcionando correctamente.

Solución alternativa: Ninguna.

El cambio del nombre de host de Log Collector o Log Decoder no se refleja en Administración de orígenes de eventos

Número de rastreo: ASOC-9235

Problema: En **Administration** > **vista Host**, si edita el “nombre” del dispositivo Log Collector o Log Decoder, el cambio no se reflejará en **Administration** > **Orígenes de eventos** > **vista Administrar** en las columnas LogCollector o LogDecoder.

Solución alternativa: Una vez que actualice un nombre en la vista Host, realice los siguientes pasos:

1. Acceda mediante el protocolo SSH al dispositivo Security Analytics.
2. Reinicie el servicio SMS con la ejecución de este comando: `service rsa-sms restart`.
3. En la interfaz del usuario de Security Analytics, espere hasta que vuelva a aparecer la vista **Administración de orígenes de eventos** y elimine los orígenes de eventos que tienen los nombres anteriores de Log Collector o Log Decoder.

Si está recopilando eventos desde los orígenes de eventos eliminados, estos se vuelven a agregar automáticamente a la vista **Administración de orígenes de eventos** con los nuevos nombres de Log Collector o Log Decoder.

Servicios principales

Entre los servicios de Security Analytics Core se incluyen Archiver, Broker, Concentrator, Decoder y Log Decoder.

Sintaxis incorrecta en el archivo de índice personalizado de Concentrator causa errores de inicialización

Número de rastreo: ASOC-4195

Problema: Cuando se inicia un servicio Archiver, Broker, Concentrator, Decoder o Log Decoder, se muestra un error de inicialización. Esto puede ocurrir debido a la aplicación de la verificación de la sintaxis de XML.

Solución alternativa: Ahora, el archivo index-<SA Core component>-index.xml requiere sintaxis de XML correcta. Si experimenta este error, agregue el encabezado y el pie de página XML correctos al archivo XML para corregirlo.

En el archivo que se muestra a continuación se incluyen ejemplos de encabezados y pies de página correctos.

Ejemplo de Decoder o Log Decoder:

```
<?xml version="1.0" encoding="utf-8"?>

<language level="IndexNone" defaultAction="Auto?>

    <!-- *** Please insert your custom keys or modifications below this line *** -->

</language>
```

Ejemplo de Concentrator o Broker:

```
<?xml version="1.0" encoding="utf-8"?>

<language level="IndexValues" defaultAction="Auto?>

    <!-- *** Please insert your custom keys or modifications below this line *** -->

</language>
```

Las funciones del sistema Broker no muestran las claves de metadatos personalizadas definidas en Concentrator

Número de rastreo: ASOC-6749

Problema: Si se definieron claves de metadatos personalizadas, las mismas claves de metadatos deben aparecer en Broker. Sin embargo, las funciones del sistema Broker no muestran los metadatos personalizados.

Solución alternativa: Los usuarios pueden copiar el archivo de lenguaje de Concentrator y el archivo de índice personalizado (si existe) en Broker para agregar las funciones de claves de metadatos de SDK a las funciones del sistema.

Contacto con el servicio al cliente

Cuando se pone en contacto con el servicio al cliente, debe encontrarse en su computadora. Prepárese para proporcionar la siguiente información:

1. El número de versión del producto o la aplicación de RSA Security Analytics que está usando.
2. El tipo de hardware que está usando.

Use la siguiente información de contacto si tiene preguntas o necesita ayuda.

RSA SecurCare:	https://knowledge.rsasecurity.com
Teléfono:	1 800 995 5095, opción 3
Contactos internacionales:	http://mexico.emc.com/support/rsa/contact/phone-numbers.htm (visite el sitio web de su país correspondiente)
Correo electrónico:	nwsupport@rsa.com
Comunidad:	http://mexico.emc.com/security/security-analytics/security-analytics.htm (visite el sitio web de su país correspondiente)
Soporte básico:	El soporte técnico relacionado con problemas técnicos está disponible de lunes a viernes, de 8:00 h a 17:00 h (hora local).
Soporte Plus:	El soporte técnico está disponible por teléfono durante todo el año solo para los problemas de severidad 1 y 2.

Historial de revisiones

Fecha	Descripción
16 de febrero de 2016	RTO
18 de febrero de 2016	Se agregó el problema conocido de la instalación y la actualización ASOC-15695. Se eliminó el SMS de Security Analytics de la lista de números de compilación.

Última modificación: 18 de febrero de 2016, 14:12 h