RSA NETWITNESS® SUITE

Notas de la versión

para la versión 11.0.0.0

Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

Contenido

Introducción

En este documento se indican las novedades y los cambios en RSA NetWitness Suite 11.0.0.0, así como las soluciones alternativas a los problemas conocidos. Lea este documento antes de implementar o actualizar RSA NetWitness Suite 11.0.0.0.

RSA NetWitness Suite 11.0.0.0 incorpora algunas de las funciones principales de la versión clásica de Security Analytics, así como herramientas de detección de amenazas avanzadas que permiten a los analistas de todos los niveles descubrir y responder ante amenazas de seguridad.

Novedades

RSA NetWitness Suite 11.0.0.0 ofrece mejoras considerables en el flujo de trabajo del analista, junto con funciones que facilitan la búsqueda para los analistas de todos los niveles de experiencia. Los administradores se benefician del soporte Plus, así como de los servicios simplificados y las funciones de mantenimiento de hosts. NetWitness Suite 11.0.0.0 incluye las siguientes funciones y mejoras nuevas.

Interfaz del usuario

Navegación basada en funciones. La interfaz del usuario se divide en cinco áreas funcionales principales: Respond, Investigate, Monitor, Configurar y Admin, lo cual tiene como objetivo alinearse con las funciones típicas del centro de operaciones de seguridad. La interfaz se actualizó para brindar mayor modernidad y mejorar el flujo de trabajo para los analistas y los buscadores de amenazas. Para obtener más información sobre la navegación nueva y consejos importantes para familiarizarse con NetWitness Suite 11.0.0.0, consulte la *Guía de introducción de NetWitness Suite*.

Respond

- **Mejor experiencia para los analistas**. NetWitness Suite 11.0.0.0 proporciona una nueva manera de administrar los incidentes. Respond reemplaza a Incident Management de la versión 10.6. Para obtener más información acerca de Respond, consulte la *Guía del usuario de NetWitness Respond*.
- **Nueva vista Respond**. La vista Respond ayuda a los analistas y a los encargados de respuesta ante incidentes a comprender el alcance completo de un incidente y a realizar tareas de triage en ellos de manera rápida y eficiente.
- **Alertas consolidadas**. Los analistas pueden ver todas las alertas de amenazas que recibió RSA NetWitness Suite 11.0.0.0 en una sola ubicación. Esto puede incluir alertas como reglas de correlación de ESA, Detección de amenazas automatizadas de ESA, Malware Analytics y alertas de Reporting.
- **Lista de incidentes ordenados por prioridad**. La Lista de incidentes presenta a los analistas una línea de espera de incidentes en orden de gravedad para los cuales deben realizar tareas de triage.
- **Agregar indicadores relacionados según demanda**. Los analistas pueden encontrar indicadores relacionados y agregarlos a un incidente.

- **Rastrear las tareas de los incidentes hasta su finalización**. Los analistas pueden crear tareas dentro de incidentes y administrar todas ellas desde una ubicación central.
- **Colaborar con otros analistas**. Los analistas pueden publicar notas y revisar el historial de actividad de un incidente.
- **Argumento de los incidentes consolidado**. Una lista cronológica de indicadores (alertas) muestra eventos y enriquecimientos de varios orígenes de datos.
- **Gráfico de nodos interactivo que muestra relaciones entre entidades**. Puede desglosar a detalles de hosts o usuarios y cambiar a la vista Investigate para realizar una investigación más detallada.
- **Información contextual según demanda en la vista Respond**. Los analistas pueden reducir el tiempo necesario para las tareas de detección y respuesta con el uso de información contextual de orígenes de datos, como listas, RSA Archer, Active Directory, RSA NetWitness Endpoint, alertas, incidentes y Live Connect. Los analistas pueden colocar el cursor sobre entidades subrayadas para ver mensajes de globo de contexto. Estos mensajes de globo muestran un resumen rápido del tipo de datos contextuales disponible para la entidad seleccionada y proporcionan vínculos a acciones investigativas adicionales. También puede acceder a un panel de búsqueda de contexto que muestra información contextual más detallada para la entidad seleccionada.

Investigar

- **Visibilidad de datos de Endpoint**. Cuando NetWitness Suite está configurado para consumir datos de RSA NetWitness Endpoint, los analistas pueden ver los datos de Endpoint en Investigate. Con esta mejora, se exponen tres tipos de eventos (red, registro y terminal) en Investigate y todos ellos se pueden investigar de la misma manera. Para obtener más información, consulte la *Guía del usuario de Investigate y Malware Analysis*.
- **Análisis de eventos**. La funcionalidad Análisis de eventos proporciona a los analistas más formas de analizar eventos cuando los reconstruyen como un análisis de texto, paquetes o archivos. Para obtener más información, consulte “Analizar eventos en la vista Análisis de eventos” en la *Guía del usuario de Investigate y Malware Analysis*.
- **Funcionalidades de análisis de paquetes**.
  - Los atributos del encabezado y el pie de página de un paquete en formato hexadecimal y ASCII se resaltan en azul; cuando coloca el cursor sobre un atributo resaltado, se

muestra información adicional en un cuadro activado con el cursor.

- Las firmas de archivos comunes se resaltan con un fondo de color naranja; cuando coloca el cursor sobre el texto resaltado, se activa un cuadro que muestra la descripción de la firma del posible tipo de archivo.
- Hay cuatro opciones de descarga: el evento como una PCAP, todas las cargas útiles, solo las cargas útiles de solicitud y solo las cargas útiles de respuesta.
- El sombreado de caracteres en la carga útil del paquete permite diferenciar los caracteres hexadecimales para ayudar a los analistas a encontrar patrones.
- Capacidad de ver cargas útiles solo mediante la eliminación de los encabezados y los pies de página de los paquetes en la representación del evento.

- **Funcionalidades de análisis de texto**.
  - Capacidad de descargar un evento de registro o un evento de terminal en varios formatos.
  - Vea la codificación y la decodificación URL y Base64 en un cuadro activado con el cursor cuando se selecciona el texto. También puede copiar el texto seleccionado.
  - Vea el texto comprimido o sin comprimir de una sesión de red HTTP.
  - Resalte los pares de clave de metadatos/valor de metadatos (no distingue mayúsculas de minúsculas) en el análisis de texto.
- **Funcionalidades de análisis de archivos**. Cuando descarga archivos, estos se exportan como un archiving zip protegido por contraseña. La contraseña predeterminada es `netwitness`. La exportación de los archivos de esta forma garantiza que el software antivirus no ponga en cuarentena el archiving. Además, garantiza que la aplicación predeterminada no abra ni ejecute automáticamente los archivos potencialmente dañinos.

Reporting

- **Origen de datos predeterminado para gráficos**. Los gráficos se ejecutan en un origen de datos predeterminado si no se especifica uno. De forma predeterminada, todos los tableros preconfigurados también se ejecutan en el origen de datos predeterminado, a menos que se especifique un origen de datos.
- **Creación de informes basados en la base de datos de Respond**. Puede ejecutar y ver informes acerca de los datos de Respond para lograr una mejor visibilidad durante el

proceso de detección. Todos los datos de alertas e incidentes clave están disponibles en la vista Respond con fines de creación de informes.

- **Corrección automática de la sintaxis de las reglas de NWDB**. Los analizadores principales de NWDB utilizan un analizador estricto (espera un uso correcto de las comillas en la sintaxis de las consultas), lo que permite una validación estricta de la sintaxis de las reglas de NWDB. Para lograr una experiencia de actualización transparente, las reglas con sintaxis no válida se corrigen automáticamente durante la primera ejecución después de una actualización. Para obtener más información, consulte la *Guía de Reporting para la versión 11.0*.

Tableros

- **Nuevos tableros preconfigurados (de uso inmediato)**. Los tableros preconfigurados proporcionan valor inmediato a los administradores del SOC, los analistas y los administradores del sistema, y están disponibles como parte de la instalación de NetWitness. En esta versión se incorporaron los siguientes tableros preconfigurados:
  - Investigation
  - Operaciones: Análisis de archivos
  - Operaciones: Análisis de protocolos
  - Amenaza: Indicadores de malware
- **Mejora en la funcionalidad para los tableros**. Los administradores pueden crear y administrar tableros con facilidad mediante la interfaz del usuario intuitiva:
  - Puede vincular Valores principales de Investigation y dashlets Gráfica en tiempo real con un tablero relacionado para ver información detallada. Está disponible una opción Ver más en los dashlets seleccionados. Para obtener más información, consulte la *Guía de introducción de NetWitness Suite*.
  - Agregue un dashlet como un gráfico de mapa geográfico para obtener una vista rápida de la ubicación geográfica. Se muestra el estado y el tráfico de la red. Entre las funciones de los gráficos de mapa geográfico se incluyen el acercamiento, el alejamiento y la exportación del gráfico.
  - Personalice la apariencia del tablero mediante la adición, la eliminación y la reorganización de los dashlets.
  - Habilite o deshabilite dashlets individuales según sus requisitos.

- Filtre los valores de los gráficos en el tablero durante 24 horas o de manera permanente si el analista desea ocultar algunos valores obvios para una hora específica con el fin de concentrarse en los demás valores.
- Configure el diseño del tablero mediante la selección de anchos disponibles para los dashlets (1/2, 1/3, 2/3 y 1).
- Administre tableros mediante la configuración del tablero completo, cambie las horas pasadas y actualice la configuración del intervalo.
- Vea las horas pasadas y la última información actualizada para el dashlet Gráfico de Reporter.
- Exporte o importe tableros con las entidades dependientes en un formato .zip para evitar la importación o la exportación por separado de dependientes.

Live

- **Compatibilidad con el servidor de TAXII**. El servidor de TAXII se admite para recopilar información de amenazas con formato STIX en NetWitness Suite. Los siguientes servidores de TAXII cumplen los requisitos de NetWitness Suite:
  - Hail a TAXII
  - Anomali Limo
  - Soltra Edge
  - OpenTAXII
- **Servidor con SSL habilitado**. Puede habilitar el protocolo de enlace SSL/TLS para servidores de TAXII y REST.
- **Limpieza automática de datos de TAXII**. En el campo Quitar datos de STIX más antiguos que, puede especificar un período de vencimiento, de modo que los paquetes de STIX extraídos del servidor de TAXII que son anteriores a los días especificados se eliminan de MongoDB. Esto limita la cantidad de indicadores obsoletos en NetWitness Suite.
- **Mejora en la interfaz de categorías**. Puede recorrer las categorías de contenido disponibles a través de Live para ver el contenido que está disponible en función del caso de uso. Para obtener más información, consulte la *Guía de administración de servicios de Live*.

Event Stream Analysis y ESA Analytics

- **Se agregó un nuevo servicio de ESA Analytics (Servidor de ESA Analytics)**. Ahora hay dos servicios que se pueden ejecutar en un host de ESA:
  - Event Stream Analysis (ESA Correlation Rules)
  - Event Stream Analytics Server (ESA Analytics) El servicio ESA Analytics se usa para Detección de amenazas automatizadas. Para obtener más información sobre la detección automática de amenazas avanzadas, consulte la *Guía de Detección de amenazas automatizadas de NetWitness Suite* y la sección "Configurar ESA Analytics" de la *Guía de configuración de ESA*.
- **Los módulos de ESA Analytics preconfigurados no requieren conocimiento de las reglas de ESA**. Actualmente, hay dos módulos disponibles en Detección de amenazas automatizadas: Comando y control (C2) para paquetes y C2 para registros.
- **Mapee todos los módulos ESA Analytics a orígenes de datos de Concentrator desde una ubicación central (ADMIN > Sistema)**. Los módulos ESA Analytics están configurados en el nivel del sistema para que pueda administrar mejor las implementaciones y las actualizaciones de los mapeos de los módulos.
- **Las alertas ahora se encuentran en la vista Respond (RESPOND > Alertas)**. La Lista de alertas de la vista Respond muestra todas las alertas y los indicadores de amenazas que recibió NetWitness Suite. Puede filtrar la Lista de alertas por el tipo de origen "Event Stream Analysis" para ver solo las alertas de ESA. Para los usuarios de 10.6, la vista Alertas > Resumen ya no está disponible.
- **Se agregó una interfaz del usuario nueva para configurar el servicio Búsqueda de Whois (ADMIN > Sistema > Whois)**. Los analistas deben configurar el servicio Búsqueda de Whois en la interfaz del usuario de NetWitness Suite y no en la vista Explorar. Una vez que se configura, Whois está disponible para todos los módulos ESA Analytics.
- **Las conexiones a orígenes de datos externos a ESA ahora requieren TLSv1.2**. Por motivos de seguridad, las conexiones internas y externas en NetWitness Suite 11.0.0.0 requieren TLSv1.2. Si está utilizando un origen de datos externo, como MS SQL-Server, MongoDB, MySQL o Postgres para los datos de enriquecimiento (Configurar > Reglas de ESA > Ajustes de configuración), asegúrese de que el servidor del origen de datos sea compatible con TLSv1.2.

Servicios principales

- **Nuevos servicios**. Los siguientes servicios se incorporaron en NetWitness Suite 11.0.0.0. Para obtener más información, consulte la *Guía de hosts y servicios*:
  - **Servidor de Admin**. El servidor de NetWitness Administration es el servicio de back-end para las tareas administrativas en la interfaz del usuario de NetWitness. Resume la autenticación, la administración de preferencias globales y el soporte de autorización para la interfaz del usuario.
  - **Servidor de Configuration**. El servidor de NetWitness Configuration es responsable de almacenar y manipular las recopilaciones de configuración. Un conjunto de configuración es cualquier agrupación lógica de configuración que se debe administrar de manera independiente.
  - **Servidor de Orchestration**. El servidor de NetWitness Orchestration es responsable de aprovisionar, instalar y configurar todos los servicios que constituyen una implementación de NetWitness. Sirve para abstraer la lógica de implementación de la plataforma de los propios servicios de NetWitness.
  - **Servidor de Security**. El servidor de NetWitness Security administra la infraestructura de seguridad de una implementación de NetWitness. Es responsable de todas las inquietudes relacionadas con la seguridad, entre las cuales se incluyen:
    - Usuarios y cuentas de autenticación
    - Control de acceso basado en funciones
    - Infraestructura de PKI de la implementación
  - **Servidor de Investigate**. El servidor de NetWitness Investigate es responsable de la investigación.
  - **Servidor de Respond**. El servidor de Respond reemplaza al servicio Incident Management.
- **Descifrado de paquetes entrantes a un Decoder**. El comando `sslKeys` admite la carga de claves de cifrado privadas a un Decoder para descifrar los paquetes entrantes antes del paso de análisis, de modo que los analizadores habilitados vean la carga útil de los paquetes sin cifrar y creen metadatos según corresponda. Para obtener más información, consulte la *Guía de configuración de Decoder y Log Decoder*.

- **Mejora en las opciones de analizadores**: `decoder/parsers/config/parsers.option`. Este nodo de configuración es una serie de StringParams, donde se da al analizador una lista de opciones, como pares de nombre = "valor". El nuevo nodo de configuración está disponible para el analizador Entropy nativo y para los analizadores Lua. Para obtener más información, consulte la *Guía de ajuste de la base de datos de Core*.
- **Los analizadores que ya no proporcionan valor se quitaron de Decoder**. Los analizadores incorporados anteriores que se describen a continuación se quitaron de los Decoders.
  - Estos analizadores nativos se quitaron de los Decoders debido a que ya no proporcionan valor: LotusNotes, MSN, SAMETIME, YMSG, AIM, Net2Phone, YCHAT y WEBMAIL.
  - Los analizadores AIM nativos se quitaron porque AIM_Lua cubre esa funcionalidad.
  - El analizador WebMail se quitó porque ya no es pertinente y porque está cifrado; no hay ningún reemplazo de Lua. La función del analizador WebMail era quitar el formato HTML de gmail, yahoo y hotmail, y extraer metadatos de interés. Los proveedores de estas aplicaciones WebMail cambian su HTML tan a menudo que el analizador no ofrece ninguna utilidad.
- **Nuevo analizador Entropy nativo**. El analizador Entropy analiza todas las sesiones de red de forma nativa en el Decoder para calcular las funciones relacionadas con Entropy. Como resultado, se obtienen varios números que brindan información valiosa acerca de si el tráfico se cifró o se puso en riesgo, o si se ajusta a una distribución de bytes prevista. La entropía es una medida de la aleatoriedad de los datos. Un valor alto para la entropía de una solicitud o una respuesta indicaría que es probable que el tráfico esté cifrado o comprimido y que una sesión de red intenta ocultar información. Para obtener más información, consulte "Configuración del analizador Entropy nativo" en la *Guía de configuración de Decoder y Log Decoder*.
- **Reindexación en segundo plano de la base de datos mientras el servicio principal está en línea**. En una operación normal, los cambios realizados en la configuración del índice solo se aplican a los datos nuevos que ingresan a la recopilación. La reconstrucción del índice en todos los datos de la recopilación es un proceso lento debido a que requiere que todo el almacenamiento de la base de datos de metadatos se lea desde el disco. A partir de la versión 11.0.0.0, es posible reconstruir el índice mientras el servicio principal está en línea. Los servicios de la versión 11.0.0.0 reconstruyen los índices en segundo plano cada

vez que el servicio detecta que parte de las bases de datos de sesión y metadatos no está indexada. Para obtener más información, consulte la *Guía de ajuste de la base de datos de Core*.

- **Validación de archivos de configuración del índice del servicio antes del guardado o el reinicio**. Se realiza una comprobación estricta de los archivos del índice para validar todos los elementos y los atributos cuando se guardan los archivos y cuando se inicia el servicio. Cuando intenta guardar un archivo de configuración del índice que no está formado correctamente, este se rechaza; se muestra un mensaje en la interfaz del usuario y el archivo no se guarda. La comprobación estricta también ocurre cuando se inicia un servicio. Sin embargo, para evitar problemas en la actualización desde 10.x, los errores se registran como advertencias. Si intenta editar un archivo del índice con advertencias registradas desde la interfaz del usuario, el guardado del archivo del índice se rechazará hasta que se hayan resuelto los problemas.
- **Nuevas estadísticas de uso de CPU de contenido.** A partir de esta versión, el Decoder proporciona estadísticas de uso de CPU para todo el contenido instalado. Los nuevos monitores de utilización de CPU revelan cuánto tiempo de CPU usan los analizadores, los feeds, las reglas de aplicación y el análisis léxico. Las estadísticas se pueden ver como nodos de estadísticas en el árbol de servicios en la vista Explorador cuando `/decoder/parsers/config/detailed.stats` está habilitado y el Decoder está capturando las estadísticas. Cada contenido se considera como un valor de porcentaje único (0 a 100) independientemente del número de subprocesos de análisis que se ejecutan. El porcentaje representa un promedio del uso de CPU para el contenido a través de todos los subprocesos.
- **Mejora en la funcionalidad RBAC**. En RSA Security Analytics 10.6, el control de acceso basado en funciones (RBAC) para el comando `/sdk packets` se activaba o se desactivaba por usuario. En general, el acceso se quitaba para los usuarios restringidos, por lo que la generación de PCAP desde Investigation no se permitía incluso para las sesiones que no tenían restricciones. En RSA NetWitness Suite 11.0.0.0, el RBAC solo funciona para los paquetes. Las sesiones que están restringidas se omitirán durante la generación de PCAP en Investigate. Se devolverán paquetes para las sesiones permitidas. Para obtener más información acerca del RBAC, consulte la *Guía de administración de usuarios y seguridad del sistema.*
- **Nueva capacidad de analizar las sesiones web comprimidas**. Los Decoders pueden realizar un análisis adicional de las sesiones HTTP con el lenguaje del analizador Lua. Los analizadores LUA pueden solicitar la descompresión de instancias individuales de

compresión en una sesión HTTP. Esto se asemeja a la funcionalidad que ofrecen los analizadores Flex anteriores.

- **Se mejoró el manejo del vencimiento para los tiempos de espera de consulta**. El comportamiento del vencimiento predeterminado para todas las consultas RESTful se cambió a ilimitado, de modo que la mecánica normal de cancelación de consultas maneja el vencimiento. Con la eliminación del vencimiento de la sesión de la API REST, el vencimiento que envía la configuración de `query.timeout` en la sesión del usuario será el factor determinante para los tiempos de espera de consulta.
- **Captura del Decoder de VLAN en varias interfaces de red mediante packet_mmap**. Se agregó la capacidad de seleccionar cualquier subconjunto de interfaces de captura mediante la adición de configuración al parámetro de configuración `/decoder/config/capture.device.params` Para obtener más información, consulte "Configurar ajustes de captura" en la *Guía de configuración de Decoder y Log Decoder*.
- **Captura de paquetes desde F5 BIG-IP VE en AWS**. Cuando implementa un Decoder para la captura de red en la nube, el administrador puede configurar Decoders con el fin de recopilar datos de red desde la infraestructura de nube de AWS mediante F5 BIG-IP Virtual Edition.
- **Comparación de claves de metadatos en reglas de aplicación**. Las reglas de aplicación en Decoders pueden comparar valores de distintas claves de metadatos en una sesión. Ahora, las claves de metadatos se pueden usar en el lado derecho de los operadores binarios. Los operadores compatibles incluyen los operadores relacionales (`=, !=,<, <=, >, >=`), así como `contains`, `begins`, `ends`, `count`, `ucount` y `length`. Para obtener más información, consulte "Sintaxis de reglas de captura" en la *Guía de configuración de Decoder y Log Decoder*.
- **Mejora en el lenguaje de reglas y consultas para los rangos de tiempo relativos**. Los puntos de tiempo relativos permiten que una cláusula `where` haga referencia a un valor en algún desplazamiento fijo relativo a los elementos de metadatos de tiempo más tempranos o más recientes observados en la recopilación. Para obtener más información acerca de los cambios en la sintaxis de las consultas, consulte la *Guía de ajuste de la base de datos de Core*.
- **Mejora en la indexación del texto de los registros**. Se define el nivel base de análisis de registros de modo que se escanee el texto de todos los registros no analizados en busca de estos elementos de entidades clave, incluso cuando no hay analizadores habilitados: registro de fecha y hora de syslog, registro de fecha y hora de RFC 3339, direcciones IP, direcciones de correo electrónico, componentes de URL y nombres de dominio. Todo lo que se pueda identificar de manera razonable como estos tipos de datos se etiqueta

automáticamente con el elemento de metadatos correspondiente.

- **Capacidad de reconstruir el flujo de red desde varias sesiones**. Mejora la combinación de sesiones divididas. El Decoder rastrea el flujo de red mientras cuenta con recursos de memoria para hacerlo. Por lo tanto, cuando llegan más paquetes en el mismo flujo de red, el Decoder agrega elementos de metadatos divididos a las sesiones posteriores. Mediante una combinación de los metadatos divididos y la clave de flujo, es posible volver a construir el flujo de red a partir de múltiples sesiones.

Security

- Se agregó compatibilidad con autoridades de certificación intermedias.
- Mejora en la postura de seguridad
- FIPS está habilitado de manera predeterminada en todos los servicios, excepto en Log Collector y Log Decoder. FIPS no se puede deshabilitar en ningún servicio, excepto en Log Collector, Log Decoder y Decoder.
- Los módulos criptográficos con certificación FIPS 140-2 están habilitados para todos los servicios que realizan operaciones criptográficas. Para los siguientes servicios, aunque se aprovecha el módulo criptográfico FIPS, el uso de suites de cifrado FIPS no se aplica:
  - NTP: Puerto UDP 123
  - TCP: Puerto del protocolo SSH 22
  - TCP: Puerto de loopback de API de valor de sal 8000
  - CollectD
  - Log Collector
  - Log Decoder

  Nota: De forma predeterminada, los dispositivos principales que no estaban en el modo de aplicación de FIPS en 10.6.4 tampoco lo estarán en 11.0.0.0 después de una actualización. Esto afecta a los servicios Log Decoder, Log Collector y Packet Decoder.

Plataforma

- **Configuración de Decoder 10G simplificada**. Puede instalar los RPM del Decoder y de pfring por separado y en cualquier orden. El orden en el cual se instalan los RPM no es

relevante. El Decoder puede localizar el adaptador de 10G e iniciar la captura.

Administration

- **Optimización del rendimiento y la escalabilidad** de NetWitness Suite con las siguientes mejoras:
  - Aprovisionamiento más rápido de hosts y servicios.
  - Funcionalidad de repositorio YUM externo que proporciona la capacidad de instalar software con rapidez.
  - Los servicios de terceros y NW se desvincularon para ofrecer opciones de escalamiento horizontal en versiones futuras.
- **Se simplificó el proceso de creación y mantenimiento de servicios y hosts**. Se agregó la funcionalidad de aprovisionamiento simultáneo de hosts desde la línea de comandos o la interfaz del usuario.
- **Se agregó compatibilidad con repositorios YUM administrados externamente**. Compatibilidad con repositorios YUM que se administran externamente.

Análisis de registros

Descubrimiento de orígenes de eventos. El descubrimiento de orígenes de eventos mejora la precisión del análisis de registros y proporciona un flujo de trabajo para encontrar y corregir orígenes de eventos no descubiertos de manera íntegra o correcta, el cual incluye:

- Lista única y centralizada de todos los orígenes de eventos
- Detalles para cada origen de eventos
  - Tipos de orígenes de eventos descubiertos
  - Probabilidad de que el tipo de origen de eventos se haya identificado correctamente
  - Permite que los administradores encuentren orígenes de eventos problemáticos
- Detalles para cada origen de eventos y tipo
  - Registros para cada tipo de origen de eventos
  - Atributos importados o configurados
  - Permite que el administrador determine si el origen de eventos está correcto
- Capacidad de confirmar o configurar tipos de orígenes de eventos correctos

- El cuadro de diálogo Administrar mapeos de analizadores permite que los administradores mapeen centralmente analizadores adecuados para las direcciones IP seleccionadas.

Context Hub

- **Se incorporaron nuevos orígenes de datos**
  - **RSA Archer**. Los datos de criticidad de recursos de RSA Archer se usan para dar prioridad a los eventos de seguridad según el impacto en el negocio y para moderar las amenazas más perjudiciales. El analista puede actuar en función de la calificación de criticidad. Para obtener más información, consulte la *Guía de configuración de Context Hub*.
  - **Active Directory**. Un analista usa información de identidad de Active Directory para acelerar la detección y la respuesta para un usuario seleccionado. Esta información se puede utilizar para realizar una investigación más a fondo de un usuario.
  - **Listas de múltiples columnas**. Los analistas pueden ver la información contextual cuando se configura una lista como un origen de datos. Por ejemplo, si el analista tiene una lista de direcciones IP en lista negra, esta se puede configurar como un origen de datos de lista de una o de múltiples columnas. Después de esto, los datos contextuales correspondientes a los datos importados se pueden recuperar y ver en las vistas Respond e Investigate. Esto permite realizar más acciones.
- **Indicador de contexto en línea**. Resumen rápido de datos contextuales para que un analista seleccione metadatos con el fin de realizar una investigación más a fondo en la vista de nodos y eventos de la vista Respond. Esta opción está disponible cuando un usuario coloca el cursor sobre los metadatos específicos. Además, brinda al analista las funciones Cambiar a Investigate, Cambiar a Endpoint y Agregar/eliminar de la lista.
- **Panel Búsqueda de contexto**. La información contextual para los orígenes de datos configurados se muestra para que los analistas realicen acciones investigativas adicionales.
- **Búsqueda de dominios y hashes de archivos**. Además de las direcciones IP, un analista puede buscar dominios y hashes de archivos dentro de Context Hub para obtener un contexto más amplio de una serie de tipos de indicadores durante una investigación.
- **Etiquetas de indicador de riesgo**. Además de la búsqueda en Live Connect, el analista puede obtener mayor información sobre el riesgo (evaluación del riesgo y motivos del riesgo). Esto incluye la magnitud del riesgo de un indicador, así como el motivo de la clasificación actual. Además, están disponibles nuevos atributos para cada uno de los tipos de indicador:

- Dirección IP
  - Identidad (ASN, país registrado y organización)
  - Archivos y dominios relacionados
- Dominio
  - Identidad (información de WHOIS: nombre del inscrito, organización, dirección, correo electrónico, etc.)
  - Las direcciones IP y los archivos relacionados
- Hash de archivo
  - Identidad (nombre de archivo, tamaño, descripción, MD5, SHA1 y fecha/hora de última modificación)
  - Información del certificado (emisor, fecha de inicio y vencimiento, información de firma, asunto, etc.)
  - Direcciones IP y dominios relacionados

- **Comentarios sobre la Evaluación del riesgo de Live Connect**. Un analista puede proporcionar comentarios en función de su nivel, la confianza y los indicadores de riesgo. Además, puede proporcionar comentarios adicionales acerca de un indicador en Live Connect. Los comentarios constan de: Etiquetas de indicador de riesgo (contexto sobre el motivo por el cual un indicador es sospechoso), confianza, estado de riesgo y nivel del analista (para proporcionar contexto sobre la manera en que se descubrió un indicador o en que se lo sometió a tareas de triage). Para obtener más información, consulte la Guía del usuario de NetWitness Respond.

Notas sobre la actualización

Las siguientes rutas de actualización son compatibles con RSA NetWitness Suite 11.0.0.0:

- RSA NetWitness Suite 10.6.4.x a 11.0.0.0

Para obtener más información sobre cómo actualizar a 11.0.0.0, consulte las instrucciones de actualización en la sección Documentación del producto.

Problemas resueltos

Esta sección enumera los problemas resueltos desde la última versión principal de .

Reparaciones en el servidor

Número de rastreo	Descripción
SATCE-1477/ASOC-24080	La configuración de alternancia del analizador de CEF se borra cuando se cambia la configuración del analizador en la interfaz del usuario
SACE-7121/ASOC-30636	Los feeds personalizados con contenido CSV no coinciden con los valores de metadatos y las comillas no se muestran correctamente.

Reparaciones en Estado y condición

Número de rastreo	Descripción
ASOC-9225	Error Página no mostrada durante el inicio de sesión mediante el navegador IE 10
SACE-6720	Se quitan todos los filtros en la página Monitoreo

Reparaciones en Log Collector

Número de rastreo	Descripción
SAENG-2476	Se muestran mensajes de error repetidos si el nombre del dominio no se puede resolver desde la computadora de LWCS
ASOC-9586	Se genera un mensaje inexacto para un error de la recopilación de AWS
ASOC-26826	No funciona la configuración del filtro de recopilación de archivos

Reparaciones en Event Stream Analysis

Número de rastreo	Descripción
ASOC-6633	En la configuración de las reglas de prueba, se limitan los valores que exceden el límite

Reparaciones en servicios principales

Entre los servicios principales se incluyen Broker, Concentrator, Decoder y Log Decoder.

Número de rastreo	Descripción
ASOC-18044	Los feeds Metacallback no son compatibles con los índices en rango (rango de direcciones IP o CIDR)

Funciones no compatibles

En las siguientes tablas se proporciona información acerca de las funciones que ya no son compatibles en RSA NetWitness Suite 11.0.0.0 ni en versiones superiores.

Funciones no compatibles en 11.0.0.0 ni en versiones superiores

No.	Función	Notas
1	Malware colocalizado	Malware colocalizado no es compatible en 11.0.0.0 ni en versiones superiores. Malware Analysis es compatible con el uso de Malware Analysis independiente.
2	Implementación de All-In-One (AIO)	La implementación de All-In-One no es compatible. La instalación nueva de AIO se quitó.
3	Warehouse Connector independiente en Decoders	De manera predeterminada, Warehouse Connector no se instala en Decoders y Log Decoders. Warehouse Connector se debe instalar y configurar después de que se configura el Decoder.
4	Características de administración	1. Olvidé mi contraseña. 2. Notificación por correo electrónico al usuario cuando vence la contraseña. 3. El cambio del anuncio de inicio de sesión no es compatible. 4. Probar/buscar usuario de AD.
5.	Pivotal	Pivotal no es compatible. Se proporciona soporte de HortonWorks.

Funciones disponibles en versiones futuras

Las siguientes funciones no están disponibles en 11.0.0.0 y estarán disponibles en una versión futura.

No.	Función	Notas
1	Creación de informes de IPDB	El servicio IPDB Extractor no es compatible en 11.0.0.0 y estará disponible en versiones superiores.
2	STIG	Si tiene un host con reforzamiento STIG, no puede actualizar a 11.0.0.0, ya que los scripts de respaldo no son compatibles con esta acción.
3	Compatibilidad con múltiples de servidores de Security Analytics (servidor de NetWitness)	La implementación de múltiples servidores no es compatible.
4	Autenticación de PKI	La función Autenticación de PKI no está disponible en 11.0.0.0.
5	Warehouse Analytics	Warehouse Analytics no es compatible en 11.0.0.0 y estará disponible en versiones superiores.

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.

Problemas conocidos durante la actualización a 11.0.0.0

Los siguientes problemas conocidos ocurren durante la actualización de la versión 10.6.x a 11.0.0.0:

Después de la actualización de 10.6.4.x a 11.0.0.0, las licencias offline no se conservan.

Número de rastreo: ASOC-41757

Problema: Incluso si carga un BIN file de respuesta nuevo desde Download Central, las licencias offline no funcionan. A pesar de que los archivos antiguos se restauran en `/var/lib/fneserver`, las licencias permanecen desactivadas.

Solución alternativa: Realice los siguientes pasos para restaurar las licencias:

1. Genere un BIN file de respuesta nuevo desde Download Central.
2. Inicie sesión en el servidor de NetWitness 11.0.0.0 (AdminServer).
3. Quite los archivos ra* (3 archivos) de `/var/lib/fneserver/`
4. Inicie sesión en la interfaz del usuario de RSA NetWitness 11.0.0.0 con información del usuario administrador y navegue a Admin > Sistema > pestaña Descripción general de la licencia.
5. En Acciones de licencia, haga clic en Actualizar licencias.
6. Ahora, cargue el archivo de respuesta que recibió de Download Central en Admin > Sistema > Licencia > pestaña Ajustes de configuración > Cargar respuesta.

Nota: La actualización mediante el modo en línea (RSA NetWitness Suite 11.0.0.0 conectado a Internet) funciona correctamente y todas las licencias se restauran después de la actualización a 11.0.0.0.

Los atributos de usuario o de función para restringir el acceso a datos a través del prefijo de consulta no son compatibles

Número de rastreo: ASOC-42734

Problema: Si configuró atributos de usuario o de función para restringir el acceso a datos a través de un prefijo de consulta en 10.6.4.x y actualiza a 11.0, esta operación no funciona.

Solución alternativa: Debe aplicar el parche de RSA NetWitness Suite 11.0.0.1 para resolver esta configuración.

Después de actualizar a 11.0, los usuarios configurados con Active Directory no podrán iniciar sesión en la interfaz del usuario de NetWitness Suite

Número de rastreo: ASOC-42738

Problema: Si hay usuarios de Active Directory configurados para nombres de inicio de sesión del usuario externos en 10.6.4.1 o anterior y actualiza a 11.0, estos usuarios no podrán iniciar sesión en la interfaz del usuario de NetWitness Suite.

Solución alternativa: Realice uno de los siguientes pasos:

- Aplique el parche de 10.6.4.2 antes de actualizar a 11.0.0.0.
- Si el parche de 10.6.4.2 no se aplica por algún motivo, aplique el parche de 11.0.0.1 y, a continuación, realice la Migración de autenticación externa.

Error al iniciar sesión del usuario

Número de rastreo: ASOC-43523

Problema: Los usuarios no pueden iniciar sesión en la interfaz del usuario de NetWitness Suite durante la instalación de 11.0.0.0 o la actualización a 11.0.0.0. Esto se debe a que la interfaz del usuario no puede recuperar información de la cuenta de usuario de MongoDB.

Solución alternativa: Debe aplicar el parche de RSA NetWitness Suite 11.0.0.1.

Después de actualizar a 11.0.0.0, no se pueden agregar orígenes de eventos nuevos en una implementación de modo mixto.

Número de rastreo: ASOC-41867

Problema: Después de actualizar a 11.0.0.0 y de conectarse a Log Collectors 10.6.4, las conexiones de prueba fallan en interfaz del usuario de Editar. Esto es porque la interfaz del usuario convierte el valor de Fecha de inicio (int.) de la recopilación al formato de fecha de cadena “1970-01-01 00:00:00”. Usted continuará recopilando eventos desde el origen de eventos existente, pero no podrá agregar un origen de eventos nuevo. Sin embargo, en el caso de una conexión de prueba masiva, todos los valores se obtienen directamente de la interfaz de REST y “Probar conexión” se pasa correctamente.

Solución alternativa: Utilice la interfaz de REST para agregar un origen de eventos nuevo en un modo mixto.

FIPS está deshabilitado de forma predeterminada para el servicio Log Collector

Número de rastreo: ASOC-41841

Problema: FIPS está deshabilitado de forma predeterminada para el servicio Log Collector, incluso si se habilitó en 10.6.4.

Nota: Incluso si FIPS se habilitó en 10.6.4, se deshabilita después de la migración.

Solución alternativa: Para habilitar FIPS en el servicio Log Collector, realice lo siguiente:

1. Detenga el servicio Log Collector.
2. Abra el archivo `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf`.
3. Cambie el valor de la siguiente variable a **off** como se describe aquí:

   ```
   Environment="OWB_ALLOW_NON_FIPS=on"
   ```
   a
   ```
   Environment="OWB_ALLOW_NON_FIPS=off"
   ```
4. Vuelva a cargar el demonio del sistema mediante la ejecución del comando `systemctl daemon-reload`.
5. Reinicie el servicio Log Collector.
6. Configure el modo FIPS para el servicio Log Collector en la interfaz del usuario:

   Nota: Este paso no es necesario en caso de una actualización si FIPS se habilitó en 10.6.4.

   a. Vaya a ADMIN > Servicios.

   b. Seleccione el servicio Log Collector y vaya a Ver > Configuración.

   c. En el modo SSL FIPS, seleccione la casilla de verificación en Valor de configuración y haga clic en **Aplicar**.

   Nota: Para habilitar Log Decoder y Packet Decoder, en `/sys/config`, configure `ssl.fips` en ON y reinicie el servicio.

Los vínculos de investigación están deshabilitados para los gráficos estáticos

Número de rastreo: ASOC-42136

Problema: El vínculo de investigación está deshabilitado para el gráfico estático (el resultado del informe está en formato de gráfico) cuyo origen de datos es NetWitness Suite-Broker (este servicio está disponible de forma predeterminada).

Solución alternativa: Hay dos soluciones alternativas para este problema:

- Las reglas que tienen el resultado en el gráfico estático se pueden ver en formato tabular y la investigación funciona según lo previsto.
- También puede realizar los siguientes pasos para solucionar el problema:
  1. Elimine y agregue NetWitness Suite-Broker nuevamente como el origen de datos en Reporting Engine con el mismo nombre.

2. Si los informes que incluyen el gráfico estático son informes programados, el vínculo de investigación funcionará según lo previsto en la siguiente ejecución.
3. Si el informe es un informe ad hoc, vuelva a ejecutarlo para obtener los vínculos de investigación.

Error de instalación en la interfaz del usuario después de la coordinación de Warehouse Connector o de la actualización de 11.0 a 11.0.0.1 para una instancia de Log Collector/Log Decoder

Problema: En una instancia de Log Collector/Log Decoder, cuando WC se coordina o si se actualiza

de 11.0 a 11.0.0.1, el estado se puede mostrar como fallido en la consola y se muestra un error de instalación

en la interfaz del usuario.

Solución alternativa: Para obtener instrucciones sobre cómo solucionar este problema, consulte este artículo de la

base de conocimientos: https://community.rsa.com/docs/DOC-84635.

Warehouse Connector no está instalado en Decoders

Problema: De manera predeterminada, Warehouse Connector no está instalado en Decoders.

Solución alternativa: Después de una actualización, si hay necesidad de volver a establecer una conexión a Warehouse, se proporciona una utilidad para reinstalar el servicio. La utilidad se implementa durante la fase de bootstrap. Para instalar Warehouse Connector, debe ejecutar el siguiente comando y especificar el host por ID (--host-id), nombre (--host-name) o dirección (--host-addr). La última versión disponible se instalará de forma predeterminada, a menos que se especifique una versión concreta con --version. Para instalar Warehouse Connector en un host, ejecute el siguiente comando en el servidor de Admin:

```
[root]warehouse-installer --host-id <uuid of the host>
Details about the command:
Location: /usr/bin
Utility Name: warehouse-installer
```

Uso:

```
[root@nw11pds5 bin]# warehouse-installer --help
Warehouse Connector Installer
warehouse-installer [options]
Install options:
--host-id <id> Specify host to install (by ID)
--host-name <name> Specify host to install (by name)
--host-addr <address> Specify host to install (by address)
```

```
--version <#.#.#.#> Install version (defaults to latest)
General options:
-v, --verbose Enable verbose output
```

Se agregan claves de metadatos para investigación y búsqueda al archivo de índice de Concentrator predeterminado.

Número de rastreo: ASOC-22338, ASOC-22895, ASOC-19406

Problema: Si agregó las siguientes claves de metadatos como personalizadas al archivo index-concentrator-custom.xml, se pueden quitar después de la actualización y ahora están presentes como claves de metadatos estándares dentro del archivo index-concentrator.xml. Las claves de metadatos son las siguientes: direction, netname, ioc, eoc, boc, analysis.file, analysis.session, analysis.service, inv.category e inv.context.

Solución alternativa: Quite las claves enumeradas del archivo index-concentrator-custom.xml.

Tableros duplicados para indicadores de amenazas.

Número de rastreo: ASOC-41701

Problema: El tablero Amenaza: Indicadores se actualizó para crear informes respecto de nuevas claves de metadatos de búsqueda y su nombre se cambió a Amenaza: Indicadores de malware. En la actualización, ambos aparecen en la interfaz del usuario y el antiguo no se reemplaza.

Solución alternativa: Habilite los gráficos y el tablero del informe Amenaza: Indicadores de malware y deshabilite el tablero Amenaza: Indicadores antiguo.

En la actualización, las políticas personalizadas de Estado y condición para el servidor de Context Hub no están disponibles.

Número de rastreo: ASOC-41826

Problema: Cuando actualiza a NetWitness Suite 11.0.0.0, las políticas personalizadas de Estado y condición configuradas para el servidor de Context Hub no estarán disponibles.

Solución alternativa: Debe definir estas políticas personalizadas en 11.0.0.0.

Después de una actualización a 11.0, las recopilaciones creadas desde un Workbench 10.4 muestran valores de Rango de fechas y Fecha de creación en blanco

Número de rastreo: ASOC-9035

Problema: Las recopilaciones creadas desde un Workbench 10.4 muestran valores de Rango de fechas y Fecha de creación en blanco después de la actualización a 11.0.0.0.

Solución alternativa: Ninguna.

En la actualización, el dashlet Geomap no se puede crear mediante un gráfico preconfigurado (de uso inmediato).

Número de rastreo: ASOC-41896

Problema: Cuando actualiza a NetWitness Suite 11.0.0.0, el dashlet Geomap no se puede crear mediante un gráfico preconfigurado (de uso inmediato). Esto sucede si un tablero personalizado utiliza un dashlet Geomap, el cual se crea mediante un gráfico preconfigurado (de uso inmediato).

Solución alternativa: El origen de datos se debe actualizar manualmente para ese gráfico de uso inmediato que se debe usar en el dashlet con Geomap. O bien, cree un gráfico nuevo mediante la misma regla preconfigurada (de uso inmediato) y use el gráfico nuevo en el dashlet con Geomap.

El servicio Warehouse Connector muestra que SSL FIPS está deshabilitado.

Número de rastreo: ASOC-41930

Problema: Cuando actualiza desde la configuración no FIPS de 10.6.x a 11.0.0.0, a pesar de que el servicio Warehouse Connector está en ejecución en FIPS, la interfaz del usuario muestra que SSL FIPS está deshabilitado.

Solución alternativa: Seleccione SSL FIPS en la página Configuración (interfaz del usuario) y reinicie el servicio Warehouse Connector.

Context Hub

OutOfMemoryError en el servicio Context Hub

Número de rastreo: ASOC-41664

Problema: El servicio Context Hub se ejecuta en OutOfMemoryError y deja de responder si se configura una gran cantidad de feeds TAXII para obtener datos.

Solución alternativa: Reinicie el servicio Context Hub y asegúrese de que el rango de tiempo que selecciona para obtener feeds TAXII desde el servidor de TAXII no sea superior a 6 meses. Si el problema persiste incluso después de actualizar el rango de tiempo, consulte el tema Solución de problemas de la *Guía de administración de servicios de Live*.

La opción Cambiar a Investigate en la vista Respond no navega al vínculo correcto.

Número de rastreo: ASOC-40944

Problema: Cada vez que detiene y reinicia el servidor de RabbitMQ, la opción Cambiar a Investigate disponible en la pantalla de Respond no está visible. Y el panel de contexto para Cambiar a Investigate vuelve a abrir la misma página.

Solución alternativa: Reinicie el servicio Jetty en el servidor de NetWitness, inicie sesión en el host del servidor de NetWitness e ingrese el comando de reinicio del servicio Jetty.

El aumento de la configuración del límite para alertas e incidentes produce un error en la búsqueda.

Número de rastreo: ASOC-40246

Problema: De forma predeterminada, la configuración del límite para ver la cantidad de alertas e incidentes está establecida en 50. Si se aumenta el límite y se obtiene un error en la búsqueda, esto se debe a una gran cantidad de incidentes y alertas. Esto sucede debido a una restricción de la base de datos interna.

Solución alternativa: Limite y vea un máximo de 50 alertas e incidentes.

Las listas de una sola columna y de múltiples columnas agregadas desde la pestaña Origen de datos no son compatibles con Agregar a lista y Quitar de lista.

Número de rastreo: ASOC-37998

Problema: Cuando realiza una búsqueda en metadatos de contexto específicos en la vista Investigation, Eventos o Respond, los nombres de lista que se muestran son aquellos que tienen valores coincidentes.

Cuando hace clic con el botón secundario en metadatos específicos y selecciona la opción Agregar o quitar lista, los nombres de lista de una sola columna y de múltiples columnas agregados desde la pestaña Origen de datos no se muestran. Solo se muestran las listas agregadas desde la interfaz del usuario mediante la pestaña Lista.

Solución alternativa: Debe agregar manualmente los valores que se agregaron desde la pestaña Origen de datos al archivo CSV específico. De este modo, la próxima vez que se ejecute el programador, los valores del archivo CSV actualizado estarán disponibles en las listas específicas.

Se importó una lista vacía

Número de rastreo: ASOC-34187

Problema: Cuando importa una lista en la cual faltan comillas, “172.16.0.0, la lista se guarda sin datos. Esto se debe al error de Apache (CSV-141), en el cual el archivo CSV con un formato incorrecto no se analiza.

Solución alternativa: Importe una lista en la cual las comillas se usen correctamente. Por ejemplo, “172.16.0.0”, “host.mycompany.com”, etc.

El protocolo de enlace SSL con certificado de RSA Archer falla cuando se agrega como un origen de datos

Número de rastreo: ASOC-32654

Problema: Cuando intenta agregar RSA Archer como un origen de datos con credenciales válidas, la conexión de prueba falla (ARCHER-37085). Esto sucede cuando se deselecciona la opción “Confiar en todos los certificados” y se intenta cargar un certificado de confianza de RSA Archer.

Solución alternativa: Seleccione la casilla de verificación “Confiar en todos los certificados” y no cargue un certificado.

Problemas generales de la plataforma

La interfaz del usuario de NetWitness Suite puede dejar de responder

Número de rastreo: SACE-7751

Problema: La interfaz del usuario de NetWitness Suite puede dejar de responder cuando el sistema intenta leer registros de Live Connect de gran volumen.

Solución alternativa: Este problema se puede resolver temporalmente mediante el reinicio de jettysrv.

Problema con la exportación de metadatos

Número de rastreo: SACE-8116

Problema: A pesar de que la exportación funciona, si hay más de un valor de metadatos en una sesión, la funcionalidad actual solo exportará uno de ellos. Por ejemplo, si tiene una sesión con 100 valores de metadatos alias.host, solo se exporta uno de ellos.

Solución alternativa: Ninguna.

El usuario decide extraer metadatos, pero no se descarga ningún dato

Número de rastreo: ASOC-35600

Problema: Si decide exportar metadatos para un evento, el archivo de exportación se descarga y se guarda con el nombre de archivo especificado, pero el archivo descargado no contiene datos.

Solución alternativa: Ninguna.

Se muestra un cuadro de diálogo emergente vacío en la interfaz del usuario de NW para un archivo STIX no válido

Número de rastreo: ASOC-36138

Problema: Si intenta cargar un archivo STIX no válido, se debe mostrar un mensaje de error, pero en su lugar se muestra un cuadro de diálogo emergente vacío.

Solución alternativa: Ninguna.

La exportación del registro siempre se exporta en formato de registro

Número de rastreo: ASOC-38270

Problema: En la interfaz del usuario de Investigation, si selecciona Extraer registros desde el servidor de NetWitness, el registro se exportará siempre en formato de “registro”.

Solución alternativa: Ninguna.

Problemas generales de las aplicaciones

Las páginas clásicas de la interfaz del usuario de NetWitness Suite no se cargan cuando el sistema se usa de manera intensiva

Número de rastreo: ASOC-41999

Problema: Las páginas clásicas de la interfaz del usuario de NetWitness Suite no se cargarán cuando el sistema se encuentre en un período de uso intensivo y se mostrará el error “`OutOfMemoryError: Metaspace`”.

Solución alternativa: Cambie "`-XX:MaxMetaspaceSize=256m`" a "`-XX:MaxMetaspaceSize=512m`" en el archivo `/etc/default/jetty` en el nodo de Admin. Una vez que se guarden los cambios, reinicie el servicio Jetty (`systemctl restart jetty`).

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 "Todos" mientras se exportan estadísticas de uso

Número de rastreo: ASOC-10079

Problema: para cualquier tipo de licencia (Todos/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.

Respond

Cuando se realiza una actualización, la regla de agregación para la condición Agrupar por de las alertas de C2 es incorrecta

Número de rastreo: ASOC-41934

Problema: Cuando se actualiza 11.0.0.0, la regla de agregación de C2 que usa Detección de amenazas automatizadas tiene un valor diferente para la condición Agrupar por.

Solución alternativa: Después de actualizar a 11.0.0.0, edite la regla de agregación "Comunicación de comando y control sospechosa por dominio" y cambie la condición Agrupar por a "Dominio". (Para hacer esto, vaya a CONFIGURAR > Reglas de incidentes > Reglas de agregación y haga doble clic en la regla Comunicación de comando y control sospechosa para editarla). Esto agregará alertas y se crearán incidentes para "Sospecha de C&C".

No es posible crear un incidente con el uso de 1,000 alertas

Número de rastreo: ASOC-41855

Problema: Cuando intenta crear manualmente un incidente con más de 400 alertas seleccionadas en la vista Lista de alertas, puede experimentar problemas.

Solución alternativa: No seleccione más de 400 alertas cuando cree un incidente.

El administrador de Respond no puede consultar Investigate ni ver dashlets de Live en el tablero

Número de rastreo: ASOC-40749

Problema: La función Respond_Administrator no tiene permiso para consultar Investigate. Esto es necesario para que el administrador de Respond pueda ir a Investigate o crear incidentes a partir de eventos. La función Respond_Administrator tampoco tiene el permiso Live: Acceso a módulo Live, el cual se requiere para ver dashlets de Live en el tablero.

Solución alternativa:

1. Cree manualmente la función Respond_Administrator en los servicios principales. Para hacerlo, vaya a ADMIN > Servicios, seleccione un servicio principal y, a continuación, en la lista desplegable Acciones, seleccione Ver > Seguridad > pestaña Funciones. Haga clic en + para agregar la función Respond_Administrator. Agregue los siguientes permisos a la función Respond_Administrator:

- sdk.content
- sdk.meta
- sdk.packets
- storedproc.execute

Replique la función Respond_Administrator a otros servicios principales que pueden usar los usuarios.

2. En ADMIN > Seguridad > pestaña Función, agregue el permiso Live: Acceso a módulo Live a la función Respond_Administrator.

Cuando se mapea la licencia medida o basada en servicios, los días con licencia y la fecha de inicio se muestran incorrectamente.

Número de rastreo: ASOC-26334

Problema: Cuando se mapea la licencia medida o basada en servicios, los días con licencia y la fecha de inicio se muestran incorrectamente en la interfaz del usuario. Esto ocurre debido a un problema en el sistema de licencia y si se mapea una licencia nueva o cuando esto sucede. Sin embargo, los datos correctos (días con licencia y la fecha de inicio) se reflejan en la interfaz del usuario después de algunos días.

Solución alternativa: Ninguna.

El nombre de archivo de eventos de malware con caracteres coreanos no se muestra correctamente en la vista Respond

Número de rastreo: ASOC-40159

Problema: Si hay caracteres coreanos en una alerta que se recibe de Malware Analysis, estos no se mostrarán correctamente en la vista Respond.

Solución alternativa: Ninguna.

No es posible consultar un domino en source/destination.device.geolocation

Número de rastreo: ASOC-39938

Problema: Una ubicación geográfica que proviene de las reglas de correlación de ESA no está disponible en el panel Indicadores relacionados de la vista Detalles de incidente. (Para acceder al panel Indicadores relacionados, vaya a RESPOND > Incidentes y, en la Lista de incidentes, haga clic en el vínculo ID o NOMBRE del incidente. En la barra de herramientas de la vista Detalles de incidente, haga clic en el ícono Registro, Tareas y Relacionado. El registro se muestra a la derecha. Haga clic en la pestaña Relacionado).

Solución alternativa: Ninguna. Se trata de una funcionalidad nueva, por lo tanto, solo son datos en los que no se puede buscar.

El vínculo de Security Analytics Incident Management en NetWitness SecOps Manager 1.3.1.2 no es válido en NetWitness Suite 11.0.0.0

Número de rastreo: ASOC-41891

Problema: NetWitness Suite 11.0.0.0 solo funciona con NetWitness SecOps Manager 1.3.1.2. Sin embargo, el vínculo de Security Analytics Incident Management en NetWitness SecOps Manager 1.3.1.2 navega a la página heredada de Security Analytics Incident Management, la cual no es válida en NetWitness Suite 11.0.0.0.

Solución alternativa: Ninguna.

Los incidentes y las tareas continúan disponibles cuando se habilita la integración de RSA NetWitness SecOps Manager

Número de rastreo: ASOC-39886

Problema: Después de habilitar la integración de NetWitness SecOps Manager en el servicio del servidor de Respond, todos los incidentes se administran en NetWitness SecOps Manager. En las versiones anteriores, cuando SecOps se habilitaba, los incidentes y las tareas de corrección se ocultaban. En NetWitness Suite 11.0.0.0, los usuarios aún pueden acceder a los incidentes y las tareas en la vista Respond (RESPOND > Incidentes y RESPOND > Tareas). Tampoco se les impide crear incidentes en NetWitness Suite. Si crean incidentes desde la vista Lista de alertas de Respond (RESPOND > Alertas) o desde Investigate, esos incidentes no se dirigen a NetWitness SecOps Manager.

Solución alternativa: Si habilitó la integración de SecOps Manager en el servicio del servidor de Respond, no utilice lo siguiente en la vista Respond: vista Lista de incidentes, vista Detalles de incidente y vista Lista de tareas. Además, no cree incidentes desde la vista Lista de alertas de Respond o desde Investigate.

Para los incidentes migrados, el conteo de eventos siempre se muestra como 0 en el panel Descripción general

Número de rastreo: ASOC-38026

Problema: En el campo Catalizadores del panel Descripción general de incidentes, la cantidad de eventos para los incidentes migrados siempre se muestra como 0 (cero). Este comportamiento es normal en NetWitness Suite 11.0.0.0 (para acceder al panel Descripción general, vaya a Respond > Incidentes. Si hace clic en un incidente en la Lista de incidentes, el panel Descripción general aparece a la derecha. Si hace clic en un vínculo en el campo ID o Nombre en la Lista de incidentes, la vista Detalles de incidente se abre con el panel Descripción general a la izquierda).

Solución alternativa: Ninguna.

No se puede cambiar a Investigate en todos los valores de nombre de usuario, nombre de archivo y dominio cuando hay valores múltiples.

Número de rastreo: ASOC-37997

Problema: Si los campos de nombre de usuario contienen comas que no representan delimitadores entre los valores, tal vez no pueda cambiar a Investigate en ciertos metadatos si hay más de un valor en el campo.

Solución alternativa: Puede consultar o cambiar a otros datos, o realizar una investigación manual de los metadatos. Puede continuar accediendo a los metadatos a través de Investigate.

La información de enriquecimiento de tabla en la memoria no se muestra para las alertas de ESA

Número de rastreo: ASOC-37533

Problema: No puede ver enriquecimientos personalizados para reglas de correlación de ESA en la vista Alertas de Respond.

Solución alternativa: Ninguna.

Los metadatos DOMAIN y HOST no se muestran correctamente en la vista Respond

Número de rastreo: ASOC-37232

Problema: Los metadatos Domain y Host se pueden etiquetar incorrectamente en la vista Detalles de incidente de Respond cuando alias.host contiene distintos tipos de datos. El comportamiento del campo Dominio es incoherente y se puede completar con nombres de host.

Solución alternativa: Ninguna. En el campo Dominio continuará habiendo múltiples tipos de información.

Después de la actualización, no se pueden filtrar incidentes mediante el campo Usuario asignado

Número de rastreo: ASOC-36973

Problema: Después de la actualización de incidentes de 10.6.x a 11.0.0.0, los analistas no pueden filtrar los incidentes migrados mediante el campo Usuario asignado (RESPOND > Incidentes: panel Filtro).

Solución alternativa: Ninguna.

Respond: Crear incidentes a partir de alertas en la vista Lista de alertas de Respond

Número de rastreo: ASOC-35811

Problema: Cuando crea manualmente un incidente a partir de alertas en la vista Lista de alertas de Respond (RESPOND > Alertas) en 11.0.0.0, dispone de funcionalidad mínima para crear un incidente a partir de alertas. Solo puede proporcionar un nombre para el incidente y la prioridad se configura de manera predeterminada en Baja. Cuando crea manualmente un incidente, no tiene opciones adicionales, como la adición de una Prioridad, un Usuario asignado o una Categoría.

Solución alternativa: Puede actualizar campos adicionales mediante la edición manual del incidente después de crearlo, como el cambio de la prioridad de Baja a Alta. Sin embargo, no puede agregar una categoría a un incidente.

Agregar dominios a una lista blanca mientras los incidentes se cierran como falsos positivos

Número de rastreo: ASOC-25135

Problema: En 10.6.x, si un incidente de sospecha de C&C se marcaba como “Cerrado: falso positivo”, se realizaba una entrada en la lista “Dominios en lista blanca” desde Context Hub. Debería haber una funcionalidad similar en la vista Respond.

Solución alternativa: Los analistas pueden agregar dominios manualmente a una lista blanca en la vista Respond. Los procedimientos se proporcionan en la *Guía del usuario de NetWitness Respond*.

Los ajustes de integración de SecOps Manager se deben exponer en la interfaz del usuario

Número de rastreo: ASOC-25127

Problema: Los ajustes de integración para el envío de todos los incidentes a RSA NetWitness SecOps Manager se deben exponer en la interfaz del usuario.

Solución alternativa: La interfaz del usuario para la integración parcial de RSA NetWitness SecOps Manager se quitó en 11.0.0.0. Los administradores pueden completar la integración desde la vista Explorar para el servicio del servidor de Respond.

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 Respond. Las alertas que se agregan de manera dinámica a un incidente se resaltan.

Solución alternativa: Ninguna.

Log Collector

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 control no funciona y los registros muestran el error: **el par terminó la sesión**

Solución alternativa: Para resolver este problema:

1. Realice un respaldo y quite el archivo de posición del punto de control (**/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.

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

Los atributos de usuario y de función no se imponen en los flujos de trabajo nuevos de Análisis de eventos de Investigate.

Número de rastreo: ASOC-42735

Problema: NetWitness Suite 11.0 no impone atributos de usuario y de función en los flujos de trabajo nuevos de Análisis de eventos de Investigate.

Solución alternativa: Debe aplicar el parche de RSA NetWitness Suite 11.0.0.1 para resolver esta configuración.

En un ambiente de modo mixto, un analista con permisos suficientes puede descargar PCAP y registros desde un servicio 10.6.x en Investigate > vista Análisis de eventos, pero no archivos ni cargas útiles.

Número de rastreo: ASOC-41697, ASOC-41698

Problema: El control de acceso basado en funciones (RBAC) en el servidor de NW 11.0.0.0 no se aplica uniformemente a las descargas cuando se investigan servicios de 10.6.x. Si la configuración de sdk.packets no se ha deshabilitado, los analistas con permiso de funciones y metadatos de SDK en el lugar para restringir la visualización y la reconstrucción del contenido de un evento pueden descargar la PCAP y el registro de un evento que tenga restricciones de contenido. Otros tipos de descargas aparecen para descargar, las que posteriormente generan errores debido a permisos insuficientes y a que los datos aún están protegidos.

Solución alternativa: Deshabilite la configuración de sdk.packets en los servicios de 10.6.x para impedir que el analista descargue PCAP o registros durante la actualización en fases. Cuando se complete la actualización de todos los servicios, la experiencia de RBAC será coherente en todos ellos. Consulte la sección "Tareas de actualización" de la *Guía de actualización de hosts físicos* para obtener detalles.

En un ambiente de modo mixto, en la vista Reconstrucción de evento > Vista de archivos, se muestra la palabra "finalizado" en lugar de la lista de archivos.

Número de rastreo: ASOC-41703

Problema: La primera vez que un usuario administrador reconstruye un evento de service=other y un archivo .raw, en la vista Reconstrucción de evento se puede mostrar la palabra "finalizado" en lugar del archivo .raw.

Solución alternativa: Vaya a otro evento en la vista Eventos y regrese a este evento o borre la caché de servicios para ver el resultado correcto. Como alternativa, el usuario administrador puede ver el archivo en la vista Análisis de eventos. El problema ocurre únicamente durante la actualización en el modo mixto. Por lo tanto, la mejor solución alternativa es terminar de actualizar los servicios conectados a NW 11.0.0.0. Consulte la sección "Tareas de actualización" de la *Guía de actualización de hosts físicos* para obtener detalles.

En una red de modo mixto y en una red completamente 11.0.0.0, un analista con restricciones de contenido parece poder descargar contenido restringido, pero no puede descomprimir el archiving de archivos descargado debido a que el contenido restringido no está en el archivo zip.

Número de rastreo: ASOC-41698, ASOC-41696

Problema: Cuando un usuario no tiene permisos para los archivos de descarga de contenido, la restricción de contenido que se aplica mediante RBAC se mantiene, pero la experiencia del usuario no es coherente con la experiencia para otros tipos de descargas con permisos insuficientes. Esto se ve en un ambiente completamente 11.0.0.0 y en un ambiente 11.0.0.0/10.6.x de modo mixto. Un analista cuyos permisos restringen la visualización de contenido en la vista Reconstrucción de evento puede descargar contenido restringido en los servicios de 10.6.x conectados. El analista puede exportar archivos restringidos como Zip o GZip y la línea de espera de trabajos muestra una descarga correcta. Sin embargo, el archivo se descarga en formato Zip o Tar y el archivo no se descomprime. En cambio, se crea una copia como “cpgz”.

Solución alternativa: Ninguna. Cuando se complete la actualización de todos los servicios, la experiencia de RBAC será coherente en todos ellos. Consulte la sección “Tareas de actualización” de la Guía de actualización de hosts físicos para obtener detalles.

La acción de hacer clic con el botón secundario en la Vista de registro no inicia una Reconstrucción de evento ni un Análisis de eventos cuando usted hace clic en una columna Registros que se ajusta a más de una fila.

Número de rastreo: ASOC-37989

Problema: En la Vista de registro de un evento, la acción de hacer clic con el botón secundario para iniciar una Reconstrucción de evento o un Análisis de eventos no está disponible cuando la columna Registros en la Vista de registro se ajusta a más de una fila.

Solución alternativa: Los analistas pueden hacer clic con el botón secundario en otra columna que no tenga ajuste automático de línea en la misma fila del evento.

En Análisis de eventos, el mensaje Paquetes representados no se muestra para los eventos que tienen una carga útil pequeña, pero una gran cantidad de paquetes.

Número de rastreo: ASOC-37348

Problema: Cuando un evento tiene más de 2,500 paquetes, debe aparecer un mensaje en la parte inferior de los resultados con el fin de mostrar el conteo de paquetes representados. Este mensaje no se muestra para los eventos con 2,500 o más paquetes y una carga útil muy pequeña, debido a que en la vista se puede mostrar toda la carga útil.

Solución alternativa: Ninguna.

Problemas de descarga de PCAP y carga útil en la vista Análisis de eventos en un ambiente de modo mixto

Número de rastreo: ASOC-37309

Problema: El flujo de trabajo de Análisis de eventos requiere que todos los servicios ejecuten 11.0.0.0. Si el servidor de NW, Broker y Concentrator están ejecutando 11.0.0.0 y los Decoders ejecutan 10.6.x, el usuario administrador no podrá descargar archivos, registros, PCAP y cargas útiles.

Solución alternativa: Descargue los archivos desde Reconstrucción de evento.

Cuando ve un archiving de archivos en el panel Análisis de eventos: Análisis de archivos, no se muestran los nombres de archivo individuales en el archiving.

Número de rastreo: ASOC-35607

Problema: Puede ver el archiving, pero no los nombres de archivo que contiene.

Solución alternativa: Vea el evento en la vista Reconstrucción de evento de Investigate para que aparezcan los nombres de archivo individuales.

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.

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.

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.

Live

El estado de la barra de progreso del feed STIX está incompleto.

Número de rastreo: ASOC-40642

Problema: En algunos casos, el estado de la barra de progreso para algunos de los feeds STIX está incompleto, incluso si los feeds se migran correctamente a los Decoders.

Solución alternativa: Ninguna.

Malware Analysis

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 ASG, Malware Analysis no muestra la opción Ver sesión de red desde el Resumen de evento de Malware. Parece que el ID del dispositivo llega nulo.

Solución alternativa: Ninguna.

Event Stream Analysis

La implementación (denominada sincronización en 10.4 y anteriores) 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.

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.

No se puede establecer el nivel de compresión de ESA como en otros dispositivos

Número de rastreo: ASOC-26481

Problema: Los administradores no pueden establecer el nivel de compresión en ESA como lo hacen en otros dispositivos, incluso si utilizan la vista Explorador.

Solución alternativa: Elimine el origen Concentrator de ESA y vuelva a agregarlo para que los cambios en el nivel de compresión se reflejen:

1. Quite el origen de datos Concentrator de ESA. (Vaya a ADMIN > Servicios, seleccione el servicio Event Stream Analysis y, en el menú Acciones, seleccione Ver > Configuración. En la pestaña Orígenes de datos de vista Configuración, quite el origen de datos Concentrator).
2. Establezca el nivel de compresión en ESA. (Vaya a la vista Explorar y, en la lista de nodos, navegue a Workflow/Source/nextgenAggregationSource y establezca CompressionLevel).
3. Vuelva a agregar el origen de datos Concentrator a ESA. (Vuelva a la pestaña Orígenes de datos de la vista Configuración y agregue el origen de datos Concentrator).

El servicio de *Event Stream Analysis deja de responder cuando se usa la agregación basada en consultas para la detección de amenazas automatizadas para los registros*

Número de rastreo: ASOC-25174

Problema: es posible que Event Stream Analysis deje de responder a causa del uso intensivo de recursos y que deba ajustarse la configuración del contenedor.

Solución alternativa: Quizá deba cambiar la configuración de tiempo de ping en el archivo `wrapper.conf`. Realice lo siguiente:

1. Vaya a **Administration > Servicios > Event Stream Analysis> Explorador** y navegue a la carpeta `/opt/rsa/esa/conf/ .`
2. Cambie la configuración a los valores siguientes:
   `wrapper.ping.timeout=300`
3. Agregue las siguientes líneas al final del archivo:
   `wrapper.restart.delay=40`
   `wrapper.ping.timeout.action=RESTART`
4. Reinicie el servicio de Event Stream Analysis.

ESA muestra una advertencia para los operadores de arreglo

Número de rastreo: ASOC-14157

Problema: Cuando se escribe una regla avanzada, los operadores de arreglo, como anyOf, fallan. Por ejemplo:

```
SELECT * FROM

Event(

alias_host.anyOf(i => i.length()>50)
```

```
);
```

produce un error similar al siguiente:

```
Logger name:
com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray

Thread: pipeline-sessions-0

Level : WARN

Message : Expected array-type input from property 'alias_host' but
received class java.util.Vector
```

Solución alternativa: Para hacer una comparación difusa, primero convierta el arreglo en una cadena. Por ejemplo:

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

Nota: Si usó operadores de arreglo en EPL desarrollado en las versiones 10.5, 10.5.0.1 y 10.6, tendrá que modificar el EPL para utilizar la solución alternativa anterior.

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.

La implementación falla si el servidor que aloja una base de datos externa 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.

En la configuración de las reglas de prueba, se limitan los valores que exceden el límite

Número de rastreo: ASOC-6633

Problema: Al configurar los parámetros de las reglas de prueba, puede configurar los valores siguientes:

- **MemoryCheckPeriod**: define el intervalo de sondeo para comprobar el consumo de memoria de ESA.

- **MemoryThresholdForTrialRules**: define el valor del umbral; cuando se alcanza, se deshabilitan todas las reglas de prueba.
  Si configura estos parámetros con valores que exceden el límite, los valores se limitan a los valores mínimo o máximo del sistema en lugar de a los valores definidos en los parámetros.

Solución alternativa: Ninguna.

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 RabbitMQ está bloqueada

Número de rastreo: SAENG-5329

Problema: Si la opción **Reenviar alertas a Respond** está habilitada y las conexiones de RabbitMQ al servidor de Respond están bloqueadas, algunos de los subprocesos de Reporting Engine se pueden bloquear.

Solución alternativa: Deshabilite la opción **Reenviar alertas a Respond** hasta que el intermediador de RabbitMQ en el servidor de NetWitness Suite en Respond 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 Investigación 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.

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.

Reporting

Los metadatos de categorías para la recopilación de incidentes no son compatibles.

Número de rastreo: ASOC-40851

Problema: Cuando se utilizan metadatos de categorías para la recopilación de incidentes, los resultados se presentan en un formato incorrecto. Por lo tanto, estos metadatos no se admiten y no puede usar metadatos de categorías en las cláusulas Select o Where. Además, no están disponibles para su selección en la lista de metadatos de la página Generador de reglas.

Solución alternativa: Ninguna.

Cuando se realiza una consulta en la base de datos de Respond, se muestran filas vacías.

Número de rastreo: ASOC-37846

Problema: Cuando se realiza una consulta en la base de datos de Respond, si los datos no están disponibles para las columnas solicitadas, se muestran filas vacías en la interfaz del usuario.

Solución alternativa: Ninguna.

Un gráfico con totales muestra datos incorrectos.

Número de rastreo: ASOC-37958

Problema: Un gráfico con totales muestra datos incorrectos cuando la cantidad total de valores es mayor que el límite del gráfico. Por ejemplo, si se recuperan 16 valores numéricos, es posible que en el gráfico solo se muestren los primeros 10 valores.

Solución alternativa: Ninguna.

Las opciones Ocultar e Investigar no son compatibles con los navegadores Google Chrome y Mozilla Firefox en el sistema operativo Windows 10.

Número de rastreo: ASOC-37590

Problema: Si está usando los navegadores Chrome o Firefox en un sistema operativo Windows 10 y hace clic en un punto de datos del gráfico, las opciones Ocultar e Investigar no se muestran. Sin embargo, estas opciones están disponibles cuando se usa el navegador Internet Explorer.

Solución alternativa: Deshabilite la función táctil en los navegadores Chrome y Firefox. Para deshabilitar esta opción en Chrome, use el siguiente procedimiento:

1. Navegue a - chrome://flags/ en el navegador Chrome o Firefox.
2. Seleccione la opción “Disable” para la marca “Touch Events API”.
3. Vuelva a iniciar el navegador.

Para deshabilitar esta opción en Firefox, use el siguiente procedimiento:

1. Navegue a - “about:config”.
2. Haga clic en “I accept the risk”.
3. Busque “Preference Name” - “dom.w3c_touch_events.enabled”.
4. Actualice la columna “Value” a 0.
5. Vuelva a iniciar el navegador.

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 programa 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.

Administration

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

Número de rastreo: ASOC-8889

Problema: El servidor de NetWitness Suite no captura el servicio de destino 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 NetWitness Suite y se importa, se exporta, se inicia sesión y se cierra sesión

Número de rastreo: ASOC-8916

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

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 NetWitness Suite, los registros de auditoría del servidor de NetWitness Suite 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 NetWitness Suite no menciona el nombre ni la dirección URL del servidor de NetWitness Suite que lo envió. Si hay varios servidores de NetWitness Suite, es posible que 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 NetWitness Suite 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 NetWitness Suite sin los permisos necesarios, los registros de auditoría no capturan los nombres de las páginas a las cuales accede el usuario.

Solución alternativa: Ninguna.

Administración de orígenes de eventos

El cambio del nombre de host de Log Collector o Log Decoder no se refleja en la vista Administrar de Orígenes de eventos

Número de rastreo: ASOC-9235

Problema: En la página **Administration > Host**, si edita el "nombre" del dispositivo Log Collector o Log Decoder, el cambio no se reflejará en la página **Administration > Orígenes de evento > Administrar** en las columnas Log Collector o Log Decoder.

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

1. Acceda mediante el protocolo SSH al dispositivo NetWitness Suite.
2. Reinicie el servicio SMS con la ejecución de este comando: service rsa-sms restart.
3. En la interfaz del usuario de NetWitness Suite, espere hasta que vuelva a aparecer la página **Administrar 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 orígenes de eventos eliminados, estos se vuelven a agregar automáticamente a la página Administración de orígenes de eventos con los nombres nuevos de Log Collector o Log Decoder.

Servicios principales

La casilla de verificación Modo SSL FIPS en la vista Configuración de servicios se debe deshabilitar para Brokers, Concentrators y Archivers debido a que el cambio del valor de la casilla de verificación no desactiva la imposición de FIPS para el servicio.

Número de rastreo: ASOC-41902

Problema: En 11.0.0.0, FIPS se impone siempre en Broker, Concentrator y Archiver, y el administrador no tiene la opción de alternar entre los modos FIPS y no FIPS. El administrador puede usar la casilla de verificación Modo SSL FIPS para activar y desactivar el modo FIPS en Log Decoder, Packet Decoder o Log Collector.

Solución alternativa: Ninguna.

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: Puede 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.

Configuración de feed personalizado: error no válido del archivo XML de opciones avanzadas para múltiples metacallback.

Número de rastreo: ASOC-40867

Problema: NetWitness Suite no es compatible con la carga de feeds para archivos XML cuando hay más de una devolución de llamada.

Solución alternativa: Es posible cargar el feed ad hoc con el uso de NwConsole o directamente mediante la dirección URL de REST del Decoder. Esto no se aplica a un feed recurrente.

Capacidad de crear feeds basados en dirección IP de origen y destino mediante CIDR o un rango

Número de rastreo: SATCE-628

Problema: Cuando crea un feed basado en origen y destino en un Log Decoder, este solo completa la clave de metadatos de origen. No puede utilizar feed de CIDR o basado en rango. Debe enumerar cada dirección IP.

Solución alternativa: Cree dos feeds distintos con el uso de direcciones IP. En ellos puede usar CIDR.

Documentación del producto

Con esta versión se proporciona la siguiente documentación.

Documento	Ubicación
Documentación en línea de RSA NetWitness Suite 11.0	https://community.rsa.com/community/products/netwitness/110
Instrucciones para la actualización de RSA NetWitness Suite 11.0	https://community.rsa.com/community/products/netwitness/110
Lista de verificación de la actualización a RSA NetWitness Suite 11.0	https://community.rsa.com/community/products/netwitness/110
Guías de configuración del hardware de RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
Contenido de RSA para RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

Contacto con atención al cliente

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	https://mexico.emc.com/support/rsa/contact/phone-numbers.htm (visite el sitio web de su país correspondiente)
Correo electrónico	nwsupport@rsa.com
Comunidad	https://community.rsa.com/community/rsa-customer-support
Soporte básico	El soporte técnico para resolver sus 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 gravedad 1 y 2.

Preparación para ponerse en 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:

- Número de versión de la aplicación o el producto RSA NetWitness Suite que está usando.
- El tipo de hardware que está usando.

Historial de revisiones

Revisión	Fecha	Descripción
1.0	24/10/2017	Disponibilidad general