RSA NETWITNESS® PLATFORM

Notas de la versión

para la versión 11.2

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 mejoras y las reparaciones realizadas en RSA NetWitness® Platform 11.2.0.0. Lea este documento antes de implementar o actualizar a RSA NetWitness® Platform 11.2.0.0.

Novedades

La versión 11.2.0.0 de RSA NetWitness® Platform proporciona nuevas funciones y mejoras para la investigación en registros, paquetes y terminales. Como parte de esta versión, se incorpora la analítica del comportamiento de usuarios y entidades para detectar e investigar los ataques y las anomalías basadas en identidades.

NetWitness User and Entity Behavior Analysis (UEBA)

RSA NetWitness® UEBA es ahora parte de RSA NetWitness® Platform. NetWitness UEBA proporciona analítica integral del comportamiento de usuarios y entidades que mejora la detección, la investigación y la respuesta a los ataques internos y las anomalías basadas en identidades.

NetWitness UEBA tiene las siguientes funciones:

- Aprovecha la analítica estadística y dinámica de valores atípicos para la conformación de una base de comportamiento, el modelado del comportamiento y la analítica de grupos de pares con el fin de descubrir el comportamiento anómalo, el movimiento lateral, las amenazas internas y la extracción de datos.
- Identifica anomalías sospechosas basadas en el comportamiento que aprovechan algoritmos de aprendizaje automático no supervisados.
- Genera un modelo de puntaje de riesgo de identidades y alertas para elevar la gravedad y la prioridad únicamente en los indicadores de alto riesgo, lo que reduce la fatiga por alertas y los falsos positivos.

Implementación del servicio NetWitness UEBA. NetWitness UEBA se puede configurar e implementar desde el servidor de NetWitness Platform Admin. El servidor de NetWitness UEBA captura los datos de registros de Windows desde los servicios de NetWitness Platform, procesa los datos y muestra los resultados en la GUI de NetWitness. Si se implementa el agente de NetWitness Insights Endpoint, también se analizan los datos de registros de Windows recopilados. Para obtener información sobre la implementación de UEBA, consulte la *Guía de instalación de hosts físicos* y la *Guía de instalación de hosts virtuales*.

En la versión 11.2, UEBA es compatible de manera nativa con varios orígenes de registro de Windows, como los siguientes:

- Windows Active Directory
- Actividad de inicio de sesión y autenticación de Windows
- Servidor de archivos de Windows

Conformación de una base de comportamiento de identidad. Se aplican modelos de aprendizaje automático a datos históricos y en tiempo real para la creación de bases de comportamiento que ayudan a identificar valores atípicos y que proporcionan visibilidad de métricas organizacionales e individuales. La política de modelado estándar ejecuta un período de capacitación de 30 días. Si se almacenan datos históricos adicionales más allá de ese punto, el período de capacitación se puede modificar para que su ejecución sea en un intervalo de tiempo anterior. Solamente los comportamientos anormales a estas bases generan anomalías o indicadores de riesgo.

Investigación de alertas principales y usuarios de alto riesgo. Los analistas pueden aprovechar un tablero de uso inmediato predefinido e informes para investigar las alertas principales (las alertas que desencadena una secuencia de indicadores en el período de hora completa) y usuarios de alto riesgo (los usuarios con un puntaje de alto riesgo). Los analistas pueden ver a los usuarios que requieren atención inmediata, realizar investigaciones más profundas y reducir los puntajes de riesgo.

Licencia de NetWitness UEBA. La licencia de NetWitness UEBA se basa en la cantidad total de usuarios en una organización. Los usuarios son personas que tienen acceso a la red y credenciales de inicio de sesión. Si la cantidad de usuarios supera el cinco por ciento (5 %) de la licencia adquirida, debe adquirir nuevas licencias. Para obtener más información, póngase en contacto con el administrador de cuentas de RSA. Para obtener más información sobre la licencia, consulte la *Guía de administración de licencia*.

Para obtener más información sobre UEBA, consulte la *Guía del usuario de NetWitness User Entity and Behavior Analytics*.

NetWitness Respond

Acceso a Análisis de eventos directamente desde la vista Detalles de incidente. Puede acceder sin problemas a Análisis de eventos en la vista Investigate desde el argumento del panel Indicadores de un incidente. Para seguir investigando un incidente, puede hacer clic en el hipervínculo de un tipo de evento en un evento del argumento con el fin de abrir la vista Análisis de eventos en Respond.

Se agregó la capacidad de enviar incidentes desde NetWitness Respond a RSA Archer. Si RSA Archer está configurado como un origen de datos en Context Hub, puede enviar incidentes a Incidente cibernético y respuesta ante vulneración de Archer. Cuando está configurado, verá un botón Enviar a Archer y un estado Enviado a Archer en NetWitness Respond. También tendrá la opción de filtrar la lista de incidentes para los incidentes enviados a Archer. Cuando envía un incidente a Archer, el sistema crea automáticamente una entrada en el registro para el incidente.

Cambio a RSA Archer desde incidentes. Puede cambiar a RSA Archer con el fin de obtener detalles de dispositivos y otra información en Incidente cibernético y respuesta ante vulneración de RSA Archer® para entidades específicas. Estas entidades son dirección IP, host y dirección Mac. En el panel Búsqueda de contexto, puede ver los atributos de la entidad subrayada, como valores de unidades de negocios, nombre de dispositivo, tipo de dispositivo, etc. Para obtener más información, consulte la *Guía del usuario de NetWitness Respond*.

Se mejoró la creación manual de incidentes desde la vista Lista de alertas. Puede agregar una prioridad, un usuario asignado y categorías cuando crea un incidente manualmente a partir de alertas.

Se agregó la capacidad de ocultar los tipos de nodos en el gráfico de nodos. Para seguir estudiando las interacciones entre las entidades del gráfico de nodos, puede seleccionar los tipos de nodos que desea incluir en este gráfico. Esto puede ser especialmente útil si un gráfico de nodos contiene más de 100 nodos.

Se ajustó el filtro de incidentes para los incidentes asignados y sin asignar. En el panel Filtros de la lista de incidentes, ya no puede filtrar por usuarios asignados e incidentes sin asignar al mismo tiempo. Si selecciona "Mostrar solo los incidentes sin asignar", ahora la lista desplegable del filtro Usuario asignado se deshabilita. Si selecciona un Usuario asignado en la lista desplegable, ahora la opción "Mostrar solo los incidentes sin asignar" se deshabilita.

Se mejoró la experiencia del usuario en relación con el orden de la lista de incidentes. Puede hacer clic en cualquier parte del encabezado de columna de la lista para alternar el orden. Ya no es necesario hacer clic en las flechas hacia arriba o hacia abajo para ordenar la lista.

Para obtener más información, consulte la *Guía del usuario de NetWitness Respond* y la *Guía de configuración de NetWitness Respond*.

NetWitness Investigate

Información contextual para un valor de metadatos en la vista Análisis de eventos. El panel Búsqueda de contexto, que estaba disponible anteriormente en las vistas Navegar y Eventos, se agregó a la vista Análisis de eventos. Este panel muestra detalles acerca de los elementos asociados con un evento (dirección IP, usuario, host, dominio, dirección MAC, nombre de archivo y hash de archivo) en Context Hub. Puede interactuar con los valores de metadatos de un evento para obtener más información valiosa, como incidentes relacionados, alertas, listas personalizadas, recursos de RSA Archer, detalles de Active Directory y el cliente grueso de NetWitness Endpoint. Para obtener más información, consulte "Ver el contexto adicional de un punto de datos" en la *Guía del usuario de NetWitness Investigate*.

Cambio a Archer desde valores de metadatos en la vista Análisis de eventos. Ahora puede cambiar a RSA Archer desde estas entidades subrayadas (dirección IP, dirección Mac y host) en Análisis de eventos con el fin de ver detalles de los dispositivos.

Consultas en formato libre en la vista Análisis de eventos. El Modo de formato libre es una alternativa al modo de consulta básica (Guiado) disponible en versiones anteriores. En el Modo de formato libre, los analistas pueden ingresar consultas de texto complejas y cambiar entre este modo y el Modo guiado. Para obtener más información, consulte "Filtrar los resultados en la vista Análisis de eventos" en la *Guía del usuario de NetWitness Investigate*.

Entre las mejoras de los perfiles se incluyen los grupos de perfiles y los perfiles nuevos y actualizados, así como la consulta previa para un perfil en la ruta de navegación. Para obtener más información, consulte "Usar perfiles para encapsular vistas personalizadas" en la *Guía del usuario de NetWitness Investigate*.

- Los grupos de perfiles permiten organizar los perfiles en grupos lógicos; por ejemplo, diferentes grupos de perfiles para distintos casos de uso o para distintos usuarios. Puede transferir perfiles existentes y nuevos a grupos de perfiles.

- Un nuevo perfil de uso inmediato llamado Análisis de terminales de RSA utiliza una consulta previa de `device.type=nwendpoint` y el grupo de metadatos y los grupos de columnas de Análisis de terminales de RSA.
- En el perfil de Análisis de amenazas de RSA, se reemplazan las tres claves de metadatos siguientes:
  `risk.warning` ahora es `behavior of compromise (boc)`
  `risk.suspicious` ahora es `indicator of compromise (ioc)`
  `risk.informational` ahora es `enabler of compromise (eoc)`
- Cuando se selecciona un perfil en las vistas Navegar o Eventos, la consulta previa del perfil se muestra en la ruta de navegación.

Se mejoró la configuración de opciones de búsqueda. El menú para configurar opciones de búsqueda se reorganizó con el fin de facilitar la comprensión y la selección. Para obtener más información, consulte "Configurar la vista Navegar y la vista Eventos" en la *Guía del usuario de NetWitness Investigate*.

Mejoras en el panel Análisis de texto. En la vista Análisis de eventos, varias mejoras abordan la facilidad de uso en la visualización de datos.

- Los nuevos controles de paginación permiten una mayor flexibilidad en la paginación a través de una lista de eventos.
- Si un evento reconstruido en el panel Análisis de texto tiene una solicitud o una respuesta que superan el límite máximo de cantidad de bytes, el encabezado indica que el mensaje se truncó. Esto proporciona la mayor cantidad de datos posible cuando se ve el Análisis de texto de un evento que es demasiado grande para representar.

Administración de orígenes de eventos

Identificación de orígenes de eventos inactivos. Este nuevo atributo muestra la cantidad de días desde que se recibió por última vez un registro de cada origen de eventos. Puede utilizar este atributo para agrupar los orígenes de eventos que han estado inactivos durante un tiempo especificado (por ejemplo, 90 días) con fines de revisión o eliminación en masa.

Context Hub

Opción para importar o exportar atributos. Ahora, los atributos del panel Búsqueda de contexto se pueden administrar para ayudar a los usuarios a ver aquellos atributos destinados a detalles de dispositivos de RSA Archer. Puede configurar el atributo de interés desde la aplicación para el dispositivo de RSA Archer y ver estos atributos en el panel de contexto. Para realizar esto, puede exportar los atributos existentes, agregar el nuevo atributo e importar el conjunto de atributos actualizado. Estos atributos se reflejan en el orden en que se importan en el panel Búsqueda de contexto cuando se ve el contexto de un incidente o un evento en la vista Análisis de eventos. Para obtener más información, consulte la *Guía de configuración de Context Hub*.

Servicios implementados con el servidor de NetWitness

Nuevo servicio Content. El nuevo servicio **Content** administra las reglas de analizadores que proporciona RSA y que crea el usuario. Ahora puede agregar reglas de analizadores en la interfaz del usuario. El servicio Content se utiliza en la pestaña Reglas de analizadores de registros, lo que se describe en la sección Análisis de registros más adelante en este documento.

Log Decoder y Network Decoder

Compatibilidad con archivos pcapng estándares. Para proporcionar un formato de base de datos más abierto, Network Decoder ahora puede escribir archivos pcapng estándares. Esta funcionalidad está habilitada de manera predeterminada si 11.2 se instala directamente. Si actualiza desde una versión anterior a 11.2, debe habilitar manualmente los archivos de base de datos con formato pcapng, lo que puede dar lugar a una disminución aproximada del 4 % en el espacio en disco (ya que los archivos pcapng requieren más espacio que los archivos nwdb). También puede utilizar el formato pcapng con captura de 10 Gbps, lo que no reduce considerablemente el rendimiento (<1 %).

Para habilitar el nuevo nodo de configuración:
`/database/config/packet.file.type = 'netwitness' or 'pcapng'`

Nuevo analizador GeoIP2. El nuevo analizador GeoIP2 convierte direcciones IP en ubicaciones geográficas, proporciona el paquete MaxMind GeoIP más reciente y es compatible tanto con direcciones IPv6 como IPv4. El analizador GeoIP2 lee desde `ip.src`, `ip.dst`, `ipv6.src` y `ipv6.dst` para generar información de GeoIP, y está habilitado en el Decoder de manera predeterminada. Para obtener más información, consulte "Analizadores GeoIP2 y GeoIP" en la *Guía de configuración de Decoder y Log Decoder*.

Búsquedas de GeoIP en metadatos IPv4 e IPv6. Ahora puede realizar búsquedas de GeoIP en metadatos IPv4 o IPv6 para que pueda comprender la información geográfica en escenarios cuando `ip.src` y `ip.dst` no son el enfoque del análisis.

- Existe una nueva API de Lua que proporciona a los analizadores Lua acceso completo a cualquier información de GeoIP2. La API de Lua devuelve la información solicitada de la base de datos de GeoIP2. Posteriormente, el analizador es libre de utilizar esta información para crear metadatos o para realizar su propio análisis.
- Puede configurar el analizador de GeoIP2 nativo para generar metadatos de GeoIP2 en cualquier clave IPv4 o IPv6 mediante el nodo `parsers.options` de `config`.

Para obtener más información, consulte "Analizadores GeoIP2 y GeoIP" en la *Guía de configuración de Decoder y Log Decoder*.

Aplicación de hash al certificado TLS. El Network Decoder puede producir hashes de certificados que se ven en el flujo de paquetes. Estos hashes son el valor SHA-1 de cualquier certificado con codificación DER encontrado durante un protocolo de enlace TLS. Los datos con algoritmo hash se escriben en la clave `cert.checksum`. Los hashes producidos se pueden utilizar para comparar el tráfico de red con hashes de listas negras SSL públicas. Para obtener más información, consulte "Aplicación de hash al certificado TLS" en la *Guía de configuración de Decoder y Log Decoder*.

Interfaz del usuario

Se cambió la ubicación de la pestaña Reglas de analizadores de registros. La pestaña Reglas de analizadores de registros, ubicada en ADMINISTRAR > Orígenes de eventos para la versión 11.1, se cambió a CONFIGURAR para la versión 11.2.

Se agregó compatibilidad con un idioma adicional. En las Preferencias de usuario, hay una nueva opción Idioma, la que permite seleccionar otro idioma disponible. El idioma seleccionado modifica el texto en todo NetWitness Platform. Para obtener más información, consulte la *Guía de introducción de NetWitness Platform*.

Cambio de marca de NetWitness. Hubo un cambio de marca relacionado con el producto NetWitness 11.2 en toda la interfaz del usuario, la documentación y otras apariciones pertinentes de la siguiente manera:

1. RSA NetWitness® Suite a RSA NetWitness® Platform
2. RSA NetWitness® Packets a RSA NetWitness® Network
3. RSA NetWitness® Logs and Packets a RSA NetWitness® Logs & Network
4. Tipo de host de Packet Hybrid a tipo de host de Network Hybrid
5. Tipo de host de Packet Decoder a tipo de host de Network Decoder
6. RSA NetWitness® SecOps Manager a Incidente cibernético y respuesta ante vulneración de RSA Archer®

Administración

Acciones del menú contextual configurables en Investigate. Las acciones al hacer clic con el botón secundario disponibles en Investigate ahora se pueden configurar mediante la interfaz del usuario Acciones del menú contextual con el uso de distintos campos y grupos. Puede crear nuevas acciones del menú contextual y administrarlas mediante el panel Acciones del menú contextual, disponible en ADMINISTRAR > Sistema. Las acciones del menú contextual configuradas con la interfaz del usuario se pueden ver como una acción al hacer clic con el botón secundario en claves de metadatos en la pestaña Investigación de las vistas Navegar, Eventos y Análisis de eventos. En Análisis de eventos, las acciones al hacer clic con el botón secundario también son compatibles en claves de metadatos.

Está disponible un anuncio de inicio de sesión mejorado. Ahora, el anuncio de inicio de sesión cuenta con texto totalmente personalizable y mayores medidas de seguridad.

Análisis de registros

Se mejoró la pestaña Reglas de analizadores de registros. RSA agregó la capacidad de ampliar los analizadores de registros existentes, agregar analizadores de registros personalizados y actualizar las reglas para los analizadores de registros. Las reglas de analizadores de registros cambian la manera en que se extrae información de metadatos desde los registros de orígenes de eventos. Puede agregar reglas de analizadores de registros que amplían los analizadores de registros existentes en el sistema, así como al analizador de registros predeterminado, el cual extrae metadatos desde los mensajes que, de otra manera, podrían aparecer como desconocidos. Para obtener más detalles, consulte la *Guía de personalización de analizadores de registros* disponible en RSA Link. En 11.1, las reglas de analizadores de registros eran de solo lectura.

Instrucciones para la actualización

Las siguientes rutas de actualización son compatibles con RSA NetWitness® Platform 11.2.0.0:

- RSA NetWitness® Platform 10.6.6.x a 11.2.0.0
- RSA NetWitness® Platform 11.0.x u 11.1.x a 11.2.0.0

Para obtener más información sobre cómo actualizar a 11.2.0.0, consulte las instrucciones de actualización en la sección Instalación y actualización.

Problemas resueltos

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

Security

Número de rastreo	Descripción
ASOC-58379	Actualización de seguridad de glibc de CentOS 7 con impacto moderado https://access.redhat.com/errata/RHSA-2018:0805
ASOC-58373	Actualización de seguridad del kernel de CentOS 7 https://access.redhat.com/errata/RHSA-2018:1629
ASOC-58376	Actualización de seguridad de dhcp: https://access.redhat.com/errata/RHSA-2018:1453
ASOC-58374	Actualización de seguridad de procps-ng https://access.redhat.com/errata/RHSA-2018:1700
ASOC-58381	Actualización de seguridad de ntp https://access.redhat.com/errata/RHSA-2018:0855
ASOC-58384	Actualización de seguridad de gcc https://access.redhat.com/errata/RHSA-2018:0849
ASOC-58380	Actualización de seguridad de krb5 https://access.redhat.com/errata/RHSA-2018:0666
ASOC-50151	Actualización de seguridad de openssh https://access.redhat.com/errata/RHSA-2018:0980
ASOC-58367	Actualización de seguridad de openjdk https://access.redhat.com/errata/RHSA-2018:1649
ASOC-58377	Actualización de seguridad de libvorbis https://access.redhat.com/errata/RHSA-2018:1058

Número de rastreo	Descripción
ASOC-52448	Actualización de seguridad de Authconfig https://access.redhat.com/errata/RHSA-2017:2285
ASOC-52439	Actualización de seguridad de Libx11 https://access.redhat.com/errata/RHSA-2017:1865
ASOC-52443	Actualización de seguridad de NetworkManager https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52444	Actualización de seguridad de Bash https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52445	Actualización de seguridad de Openldap https://access.redhat.com/errata/RHSA-2017:1852
ASOC-49815	Actualización de seguridad de Systemd https://access.redhat.com/errata/RHSA-2018:0260

Problemas generales de las aplicaciones

Número de rastreo	Descripción
ASOC-46483	El sistema cierra la sesión de los usuarios inactivos en Respond y en algunas vistas de Investigate

Investigate

Número de rastreo	Descripción
ASOC-51011	Tres grupos de metadatos nuevos para 11.0 y los mismos grupos de columnas para 11.1 no se crean cuando se actualiza de 10.6.5 a 11.x: Análisis de terminales de RSA, HTTP de salida de RSA y Protocolos SSL/TLS de salida de RSA.
ASOC-50702	Después de la actualización a 11.1, hay tipos de datos que no coinciden entre las definiciones de Log Decoder (table-map.xml) y Concentrator (index-concentrator.xml).

Número de rastreo	Descripción
ASOC-50924	El intento de realizar una consulta directa, o una consulta a través de un vínculo, que utiliza un valor de metadatos IPv6 con caracteres especiales no compatibles genera un error en las vistas Análisis de eventos y Navegar.
ASOC-50771	Si accede a Análisis de eventos desde la vista Eventos, tanto si hizo clic en el vínculo Análisis de eventos como si hizo clic con el botón secundario en uno de los eventos, las opciones del botón secundario en valores de metadatos no funcionan.
ASOC-49854	El indicador giratorio del selector de Servicio se queda cargando infinitamente.
ASOC-50712	Las entidades de metadatos no se pueden agregar a un grupo de columnas personalizado en la vista Eventos cuando la opción Optimizar cargas de la página Investigation está deshabilitada.
ASOC-50349	En la vista Eventos se pueden crear grupos de columnas personalizados que contienen entidades de metadatos, pero cuando el grupo de columnas personalizado se utiliza en la vista Análisis de eventos, las claves de metadatos incluidas en la entidad de metadatos no se pueden ver en los resultados.
ASOC-50041	Cuando hace clic con el botón secundario en un valor de metadatos que contiene punto y coma en la vista Análisis de eventos e intenta aplicar el desglose en una nueva pestaña en la vista Navegar, se produce un error: No se puede crear la visualización.
ASOC-45198	Cuando se modifica la dirección URL y la nueva dirección URL corresponde a un evento restringido, el contenido reconstruido de la consulta anterior persiste en la vista Análisis de eventos y no se muestra ningún mensaje de error.
ASOC-48945	Cuando ingresa una consulta a una sesión para la cual no tiene acceso en la vista Análisis de eventos, no se muestran datos y no aparece ningún mensaje de error.
ASOC-48710	Cuando realiza una investigación en la vista Análisis de eventos, se muestra el siguiente mensaje de error: “Se produjo un error inesperado”.

Respond

Número de rastreo	Descripción
ASOC-40749	El administrador de Respond no puede consultar Investigate ni ver dashlets de Live en el tablero.
ASOC-41891	El vínculo de Security Analytics Incident Management en NetWitness SecOps Manager 1.3.1.2 no es válido en NetWitness Suite 11.1.0.0.
ASOC-46834	No se puede seleccionar Dominio para Sospecha de C&C y Dominio en el generador de reglas
ASOC-50911	La agregación se detiene después de la reconexión a Mongo
ASOC-51480	La regla de incidentes de Endpoint no agrega eventos de Endpoint con una dirección IP de detector ni crea incidentes con la condición de coincidencia de la regla de incidentes predeterminada actual. Consulte el tema “Configurar y verificar reglas de incidentes predeterminadas” en la *Guía de configuración de NetWitness Respond*.

Event Stream Analysis (ESA)

Número de rastreo	Descripción
ASOC-50201	Cuando se implementan nuevas reglas de ESA en la vista Estado y condición, y se crea una nueva política en Event Stream Analytics mediante la estadística de uso de memoria de la regla de ESA, no se enumeran todas las reglas de ESA implementadas.

Funciones no compatibles

En las siguientes tablas se proporciona información acerca de las funciones que ya no son compatibles en RSA NetWitness® Platform 11.1 ni en versiones superiores.

Funciones no compatibles en 11.1.0.0 ni en versiones superiores

No.	Función	Notas
1	Malware colocalizado	Malware colocalizado no es compatible en 11.1.0.0 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	Warehouse Connector independiente no es compatible.
4	Características de administración	1. Olvidé mi contraseña. 2. Notificación por correo electrónico al usuario cuando vence la contraseña. 3. Probar/buscar usuario de AD.
5.	Pivotal	Pivotal no es compatible.
6.	Warehouse Analytics	Warehouse Analytics no es compatible.

Funciones disponibles en versiones futuras

Las siguientes funciones no están disponibles en 11.2 y pueden estar disponibles en una versión futura.

No.	Función	Notas
1	Creación de informes de IPDB	El servicio IPDB Extractor no es compatible en 11.2.0.0 y estará disponible en versiones superiores.

No.	Función	Notas
2	STIG	Si tiene un host con reforzamiento STIG, no puede actualizar a 11.2.0.0, 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 11.2.0.0.
6	Analítica en Endpoint	La analítica, por ejemplo, el puntaje de riesgo o un cálculo de IOC, no es compatible con los datos de escaneo de terminales.
7	Corrección en Endpoint	La funcionalidad de respuesta (contención/bloqueo) no es compatible.
8	Rastreo en Endpoint	El rastreo de eventos de red no es compatible.
9	Modo Kernel en Endpoint	El agente de Endpoint funciona actualmente en el modo Usuario y no es compatible con la detección del modo Kernel.
10	Reputación de archivos en Endpoint	La reputación de archivos, como las búsquedas en OPSWAT, YARA y Reversing Lab, no es compatible y, por lo tanto, los archivos no se pueden poner en listas blancas o negras.

Problemas conocidos

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

Problemas conocidos durante la actualización a 11.2

Los siguientes problemas conocidos ocurren durante la actualización de 10.6.6 a 11.2 o la actualización de 11.1 u 11.1.x a 11.2.

El feed recurrente de STIX falla durante la actualización de 10.6.6 a 11.2

Número de rastreo: ASOC-61227

Problema: Cuando Security Analytics 10.6.6 se actualiza a NetWitness Platform 11.2, el feed recurrente de STIX que se creó con el uso de una URL HTTPS no funciona. Esto se debe a que, en 10.6.x, de manera predeterminada, todos los certificados son de confianza. Sin embargo, esto no es así en 11.2. En 11.2 se proporciona la opción Confiar en todos los certificados, la que está deshabilitada de manera predeterminada.

Solución alternativa: Navegue a Configurar > Feeds personalizados y edite el feed fallido. Habilite la opción Confiar en todos o cargue un certificado SSL válido para resolver el problema. Si tiene alguna otra consulta, póngase en contacto con el servicio al cliente de RSA.

Durante la actualización a NetWitness Platform 11.2, los detalles de la licencia no se conservan en la nube de AWS

Número de rastreo: ASOC-61614

Problema: Cuando Security Analytics 10.6.6 se actualiza a NetWitness Platform 11.2, el ID del servidor de licencias no se conserva. Por lo tanto, el servidor de administración no puede obtener los detalles del servidor de licencias desde el sistema de back-end externo, razón por la cual no se puede habilitar la licencia para los servicios.

Solución alternativa: Siga los pasos que se proporcionan en los temas “Acceder a Download Central” y “Registrar el servidor (en línea)” de la *Guía de administración de licencia* para obtener los detalles de la licencia desde el sistema de back-end externo y registrar el nuevo ID del servidor de licencias.

Después de la actualización de 10.6.6 a 11.2.0.0, 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. Acceda mediante el protocolo SSH a un host de servidor de NetWitness 11.2.0.0 (AdminServer).

3. Quite los archivos ra* (3 archivos) de `/var/lib/fneserver/`
4. Inicie sesión en la interfaz del usuario de RSA NetWitness 11.2.0.0 con información del usuario administrador y vaya a **ADMINISTRAR** > **Sistema** > pestaña **Detalles de licencia**.
5. Haga clic en **Actualizar licencias**.
6. Cargue el archivo de respuesta que recibió de Download Central. Vaya a **ADMINISTRAR** > **Sistema** > **Licencia** > pestaña **Ajustes de configuración**
7. Haga clic en **Cargar respuesta**.

Nota: La actualización mediante el modo en línea (RSA NetWitness Suite 11.2.0.0 conectado a Internet) funciona correctamente y todas las licencias se restauran después de la actualización a 11.2.0.0.

Los vínculos de investigación se deshabilitan para los gráficos estáticos durante las tareas posteriores a la actualización de 10.6.6 a 11.2

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 un 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 un 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 restaurar los vínculos de investigación.

Durante la actualización de 10.6.6 a 11.2, 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 11.2.0.0, el dashlet Geomap no se puede crear mediante un gráfico preconfigurado. Esto sucede si un tablero personalizado utiliza un dashlet Geomap, el cual se crea mediante un gráfico preconfigurado.

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

Durante la actualización de 11.x a 11.2, si ha usado el analizador de entropía y ha indexado la carga útil, deberá agregar la marca de depósito al archivo del índice de modo que el analizador de entropía pueda usar depósitos del índice

Número de rastreo: ASOC-45721

Problema: Cuando actualiza de la versión 11.0 a la versión 11.2, si ha usado el analizador de entropía en el Decoder (solamente paquetes) e indexa la carga útil, debe agregar la marca de depósito al archivo del índice para aprovechar la nueva función de depósitos del índice.

Nota: Si está actualizando desde la versión 11.1 o superior a la versión 11.2, no es necesario realizar este cambio.

Solución alternativa: Agregue la marca de depósito al archivo del índice para que el analizador de entropía pueda utilizar los depósitos del índice, como se indica a continuación:

1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione cada servicio Concentrator que agregue tráfico desde los Decoders.
3. En  (acciones), seleccione **Ver** > **Configuración** y elija la pestaña **Archivos**.
4. Seleccione el `index-concentrator-custom.xml file` y configure la marca `bucket` en `true` para `payload.req` y `payload.res`. Por ejemplo:
   ```
   <key description="Payload Size Request" format="UInt 32"
   level="IndexNone" bucket="true" name="payload.req"
   valueMax="500000"/>
   <key description="Payload Size Response" format=UInt32"
   level="IndexNone" bucket="true" name="payload.res"
   valueMaz="500000"/>
   ```
5. Haga clic en **Aplicar**.
6. Para que los cambios en el archivo `index-concentrator-custom.xml` surtan efecto, debe reiniciar el servicio Concentrator:
   ```
   systemctl restart nwconcentrator
   ```

UEBA

Cuando el proxy está configurado, en el caso de las actualizaciones, los detalles de la licencia no se actualizan automáticamente

Número de rastreo: ASOC-52366

Problema: Cuando el proxy está configurado, en el caso de las actualizaciones, los detalles de la licencia no se actualizan automáticamente, ni siquiera después de que se hace clic en el botón Actualizar de la vista Detalles de licencia. Esto se debe a que la comunicación con el servidor de licencias no está establecida.

Solución alternativa: El administrador debe descargar manualmente los detalles de la licencia utilizando el modo offline y cargar los detalles más recientes a través de la interfaz del usuario de NetWitness Platform. Para obtener más información, consulte la *Guía de administración de licencia*.

Endpoint

Nginx rechaza solicitudes post que superan el tamaño de solicitud de 1 MB

Número de rastreo: ASOC-56236

Problema: El servidor de Nginx se actualiza y el tamaño de carga útil predeterminado se configura en 1 MB. Esto hace que cualquier solicitud post de datos superior a 1 MB falle.

Solución alternativa: Agregue la siguiente configuración al archivo de configuración de Nginx (`/etc/nginx/conf.d/nginx.conf`) y reinicie el servidor de Nginx.

```
client_max_body_size 100M
```

La generación y la copia del archivo *nwelcfg no actualiza el registro de fecha y hora

Número de rastreo: ASOC-49847

Problema: Después de instalar el agente de Endpoint Insights, si el administrador desea actualizar una nueva configuración de la recopilación de registros a través de cualquiera de los métodos de copia o la herramienta de administración de Endpoint de otros fabricantes, el registro de fecha y hora continúa siendo la hora del servidor de Endpoint y no la del agente. En consecuencia, si el agente de Endpoint está en una zona horaria distinta a la del servidor de Endpoint, el registro de fecha y hora no se actualiza correctamente.

Solución alternativa: Después de copiar el archivo de configuración, ejecute en el agente de Endpoint el comando: `copy /b <filename.nwelcfg> +,,` desde la carpeta %programdata%\NWEAgent\ donde se encuentra el archivo nwelcfg.

Respond

Cuando se eliminan todas las alertas para una regla de alerta, el filtro de la regla no se quita correctamente

Número de rastreo: ASOC-59243

Problema: En la vista Lista de alertas (Responder > Alertas), puede filtrar las alertas por Nombre de alerta y, a continuación, eliminar todas las alertas que tengan ese nombre. Si no quita el filtro de nombre de alerta después de eliminar las alertas, la próxima vez que se cargue la vista Lista de alertas, el filtro continuará vigente, pero ya no estará visible como una casilla de verificación en el panel Filtros debido a la eliminación de todas las alertas con ese nombre. Cuando visite la vista Lista de alertas, continuará sin obtener resultados.

Solución alternativa: Antes de actualizar o volver a cargar la vista Lista de alertas, puede quitar el filtro deseleccionado la casilla de verificación por el nombre de la alerta. Si ya actualizó o volvió a cargar la vista Lista de alertas, la única manera de quitar el filtro oculto es presionar el botón **Restablecer filtros**, lo que quita todos los filtros, incluido el filtro de nombre de alerta oculto.

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

Número de rastreo: ASOC-52428

Problema: Los valores de metadatos en los valores activados con el puntero no se resaltan cuando las alertas se han agregado manualmente a un incidente en Respond. En cambio, las alertas que se agregan automática o dinámicamente a un incidente se muestran en un cuadro activado con el puntero.

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 muestran correctamente en la vista Respond.

Solución alternativa: Ninguna.

Las reglas de ESA con gravedad Alta o Baja no se completan en la interfaz del usuario de RSA Archer

Número de rastreo: ARCHER-47101

Problema: Cuando las alertas de ESA con gravedad Alta o Baja se reenvían a RSA Archer, el campo Prioridad de la alerta de seguridad no se completa en la interfaz del usuario de RSA Archer.

Solución alternativa: Ninguna.

Los incidentes y las tareas continúan disponibles cuando está habilitada la integración de Incidente cibernético y respuesta ante vulneración de RSA Archer

Número de rastreo: ASOC-39886

Problema: Después de habilitar la integración de Incidente cibernético y respuesta ante vulneración de Archer (NetWitness SecOps Manager) en el servicio del servidor de Respond, todos los incidentes se administran en Incidente cibernético y respuesta ante vulneración de Archer. En las versiones anteriores, cuando SecOps se habilitaba, los incidentes y las tareas de corrección se ocultaban. En NetWitness Platform 11.0.0.x, los usuarios aún pueden acceder a los incidentes y las tareas en la vista de Respond (RESPONDER > Incidentes y RESPONDER > Tareas). Tampoco se les impide crear incidentes en NetWitness Platform. Si crean incidentes desde la vista Lista de alertas de Respond (RESPONDER > Alertas) o desde Investigate, esos incidentes no se dirigen a Incidente cibernético y respuesta ante vulneración de Archer.

Solución alternativa: Si habilitó la integración de Incidente cibernético y respuesta ante vulneración de Archer (NetWitness 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 es el comportamiento normal en NetWitness Platform 11.0.0.x y superior. (Para acceder al panel Descripción general, vaya a Responder > 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.

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.

La configuración de la integración para Incidente cibernético y respuesta ante vulneración de Archer se debe exponer en la interfaz del usuario

Número de rastreo: ASOC-25127

Problema: La configuración de la integración para el envío de todos los incidentes a Incidente cibernético y respuesta ante vulneración de Archer (NetWitness SecOps Manager) se debe exponer en la interfaz del usuario.

Solución alternativa: La interfaz del usuario para la integración parcial de Incidente cibernético y respuesta ante vulneración de Archer (NetWitness SecOps Manager) se quitó en 11.0.0.x. Los administradores pueden completar la integración desde la vista Explorar para el servicio del servidor de Respond.

Log Collector

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 11.2.0.0.

Nota: Incluso si FIPS se habilitó en 11.2.0.0, 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 11.2.0.0.

   a. Vaya a **ADMINISTRAR** > **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.

Investigate

Los perfiles de Investigate importados no se muestran en el menú desplegable Perfiles

Número de rastreo: ASOC-61230

Problema: Cuando importa perfiles a las vistas Navegar o Eventos mediante el cuadro de diálogo Administrar perfiles, los perfiles recién importados no se agregan al menú desplegable Perfiles.

Solución alternativa: Actualice la ventana del navegador para ver los perfiles agregados recientemente.

En la vista Análisis de eventos, los eventos de registro y red no se intercalan

Número de rastreo: ASOC-60941

Problema: Los eventos de red y registro se intercalan y se ordenan por hora en la vista Eventos, pero en la vista Análisis de eventos, se ordenan de otra manera. En la vista Análisis de eventos, los eventos no se intercalan como deberían; en lugar de esto, se muestran todos los eventos de registro ordenados por hora antes que todos los eventos de red ordenados por hora.

Solución alternativa: Utilice la vista Eventos para ver los eventos de red y registro intercalados.

Cuando se extrae un PCAP grande desde la vista Eventos, si se agota el tiempo de espera después de 5 minutos, el tiempo de la consulta se muestra como 8 horas en el mensaje de error de la bandeja de trabajos

Número de rastreo: ASOC-60464

Problema: Cuando se exporta una PCAP con aprox. 100,000 sesiones desde la vista Eventos utilizando Exportar > Exportar todas las PCAP, la descarga puede fallar debido al tiempo de espera de llamada de paquetes de 5 minutos. Si se agota el tiempo de espera de la llamada, el mensaje de error en la bandeja de trabajos muestra incorrectamente el tiempo de espera como 8 horas (28,800,000 de ms).

Solución alternativa: Ninguna.

Los usuarios a los que no se ha asignado el permiso investigate-server* no reciben el mensaje de error adecuado para explicarles por qué no tienen acceso a la vista Análisis de eventos

Número de rastreo: ASOC-60366

Problema: Si el administrador no ha asignado el permiso investigate-server* a un usuario, este debe ver el error de permiso denegado cuando intenta acceder a una sesión en la vista Análisis de eventos. En su lugar, se muestra un error interno del servidor.

Solución alternativa: Ninguna.

Los valores de metadatos de Active Directory en la vista Análisis de eventos, como el nombre de usuario, pueden tener datos de contexto disponibles, pero no se subrayan a modo de indicador

Número de rastreo: ASOC-58853

Problema: Los analistas que trabajan en la vista Análisis de eventos no verán un indicador que señala que los metadatos de Active Directory tienen enriquecimiento de contexto; deben colocar el cursor sobre un valor de metadatos de Active Directory para determinar si tiene contexto asociado y abrir el panel Búsqueda de contexto.

Solución alternativa: Coloque el cursor sobre un valor de metadatos o selecciónelo y haga clic en el botón **Ver contexto** para determinar si tiene contexto asociado para Active Directory.

Si la dirección URL de un punto de desglose es muy larga y se utilizar la consulta en la vista Análisis de eventos, se muestra un error (error de solicitud 414)

Número de rastreo: ASOC-50196

Problema: Varias situaciones crean una consulta muy larga que el navegador no puede manejar, especialmente si se utiliza Internet Explorer, el cual tiene un límite de caracteres mucho menor que la mayoría de los navegadores. El cambio a Análisis de eventos desde Reporting puede dar lugar a una consulta muy larga, al igual que una serie de cambios en la vista Navegar.

Solución alternativa: Continúe trabajando en las vistas Navegar o Eventos cuando la dirección URL sea demasiado larga como para representarla en la vista Análisis de eventos.

El generador de consultas de la vista Análisis de eventos no responde para los filtros que contienen un espacio

Número de rastreo: ASOC-49427

Problema: Cuando se agrega un filtro, si agrega un espacio adicional antes de <clave de metadatos>, entre <clave de metadatos> y <operador>, y después de <operador>, el generador de consultas deja de responder, el botón Eventos de consulta se deshabilita y no es posible continuar agregando filtros.

Solución alternativa: Haga clic en un filtro existente y, a continuación, haga clic en el generador de consultas. Si eso no funciona, actualice la página.

Feeds personalizados

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.

Event Stream Analysis (ESA)

Las reglas de CH de ESA se deshabilitan durante la actualización o el reinicio del host de ESA

Número de rastreo: ASOC-60511

Problema: Si el host de ESA se reinicia y hay reglas de Context Hub implementadas en ESA, estas pueden deshabilitarse. Esto sucede debido a una condición de carrera entre el orden de arranque de los servicios Event Stream Analysis y Context Hub en el host de ESA.

Solución alternativa: Para resolver este problema, realice una de las siguientes acciones:

- Vaya a la pestaña **CONFIGURAR > Reglas de ESA > Servicios** y habilite las reglas deshabilitadas que dependen de Context Hub.
- Reinicie el servicio Event Stream Analysis.

Las reglas de ESA con metadatos personalizados no se implementan en el servidor de ESA

Número de rastreo: ASOC-60367

Problema: Si agrega nuevas claves de metadatos personalizadas en 11.2, es posible que las reglas de ESA que utilizan esas claves de metadatos no se implementen. Esto sucede porque el servicio Event Stream Analysis necesita información desde Concentrator.

Solución alternativa: Para implementar una regla de correlación de ESA con metadatos personalizados, realice lo siguiente:

1. Agregue las claves no estándares al archivo index-concentrator-custom.xml (ADMINISTRAR > Servicios > Seleccione un Concentrator y, a continuación, seleccione Acciones > Ver > Configuración > pestaña Archivos).
2. Reinicie el Concentrator (ADMINISTRAR > Servicios > Seleccione un Concentrator y, a continuación, seleccione Acciones > Reiniciar).
3. Asegúrese de que el Concentrator esté configurado como un origen de datos para el servicio Event Stream Analysis (ADMINISTRAR > Servicios > Seleccione el servicio Event Stream Analysis y, a continuación, seleccione Acciones > Ver > Configuración > pestaña Orígenes de datos).
4. Reinicie el servicio Event Stream Analysis (Acciones > Reiniciar).
5. Asegúrese de que las nuevas claves de metadatos se enumeren en las Referencias de claves de metadatos (CONFIGURAR > Reglas de ESA > pestaña Ajustes de configuración > Referencias de claves de metadatos).
6. Implemente la regla de ESA con metadatos personalizados.

No se puede implementar una regla de ESA con metadatos de arreglo en enriquecimiento

Número de rastreo: ASOC-47584

Problema: Si un usuario configura una tabla en la memoria como un origen de enriquecimiento en ESA (donde el tipo de una columna de la tabla es cadena), crea una regla de ESA con una condición de lista blanca y mapea la columna de lista de cadena a una clave de metadatos de evento de arreglo de cadena, cuando se implementa la regla, esta se deshabilita, ya que no se permite la conversión de tipo de datos de String[] a String.

Solución alternativa: Ninguna.

Para las reglas de ESA que utilizan orígenes de enriquecimiento, la opción Omitir mayúsculas y minúsculas no funciona para la primera declaración

Número de rastreo: ASOC-49906

Problema: Cuando crea una regla de ESA que utiliza cualquier origen de enriquecimiento, si la opción Omitir mayúsculas y minúsculas está habilitada en la primera declaración de enriquecimiento, no se devuelve ningún resultado. Tenga en cuenta que este problema no se aplica a todas las declaraciones después de la primera (es decir, subdeclaraciones).

Solución alternativa: Ahora, cuando se crea una regla nueva, la opción Omitir mayúsculas y minúsculas está deshabilitada. Para las reglas existentes en las que la opción Omitir mayúsculas y minúsculas está activada para una declaración de enriquecimiento, la opción continúa activada, pero se solicitará a los usuarios que la deshabiliten cuando abran la regla en ESA y, a continuación, guarden la regla actualizada.

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 ADMINISTRAR > 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 Event Stream Analysis deja de responder cuando se usa la agregación basada en consultas en 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 las siguientes acciones:

1. Vaya a **Administración > Servicios > Event Stream Analysis> Explorar** 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 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.

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.

Reporting

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.

Administración de orígenes de eventos

La ventana Administrar mapeos de analizadores tiene un nombre para mostrar vacío para los analizadores de registros si el origen de eventos se creó manualmente

Número de rastreo: ASOC-53914

Problema: Cuando abre la ventana Administrar mapeos de analizadores desde ADMINISTRAR > Orígenes de eventos > vista Descubrimiento, el nombre para mostrar de los orígenes de eventos mapeados está vacío para los orígenes de eventos que se crearon manualmente.

Solución alternativa: Cierre la ventana de mapeo y vuelva a abrirla.

No se muestran todos los tipos para las direcciones mapeadas automáticamente

Número de rastreo: ASOC-48328

Problema: Si se agrega una nueva aplicación en un origen de eventos existente con mapeo automático, puede haber una demora en la aparición de ese tipo en la vista Descubrimiento de orígenes de eventos y en que este deje de aparecer como mapeado automáticamente.

Solución alternativa: Ninguna.

El servicio SMS tiene una falla general con un error de memoria insuficiente

Número de rastreo: ASOC-62575

Problema: En los sistemas con una gran cantidad de orígenes de eventos activos que no pueden seguir el ritmo del procesamiento de mensajes de estadísticas de registro, el servicio SMS puede tener una falla general con un error **java.lang.OutOfMemoryError: Java heap space**.

Solución alternativa: Si experimenta este problema, póngase en contacto con el soporte de RSA para obtener detalles sobre cómo abordarlo.

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.x o superior, 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.

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

Número de rastreo: ASOC-40867

Problema: NetWitness Platform 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.

Documentación del producto

Con esta versión se proporciona la siguiente documentación.

Documentación	Dirección URL de ubicación
Documentación en línea de RSA NetWitness Platform 11.2	https://community.rsa.com/community/products/netwitness/112
Instrucciones de actualización de RSA NetWitness Platform 11.2	https://community.rsa.com/community/products/netwitness/112/content?filterID=contentstatus%5Bpublished%5D~category%5Binstallation-upgrade%5D
Listas de verificación de la actualización de RSA NetWitness Platform 11.2	Lista de verificación de actualización de hosts virtuales para la versión 10.6.6.x a 11.2 Lista de verificación de actualización de hosts físicos para la versión 10.6.6.x a 11.2
Guías de configuración de hardware de RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/hardware-setup-guides

Documentación	Dirección URL de ubicación
Contenido de RSA para RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

Contacto con atención 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 Platform que está usando.
- El tipo de hardware que está usando.

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

RSA Link	https://community.rsa.com En el menú principal, haga clic en **My Cases**.
Teléfono	1 800 995 5095, opción 3
Contactos internacionales	http://mexico.emc.com/support/rsa/contact/phone-numbers.htm (visite el sitio web de su país correspondiente)
Comunidad	https://community.rsa.com/community/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.

Historial de revisiones

Revisión	Fecha	Descripción
1.0	15/8/2018	Liberación a Operaciones