RSA NETWITNESS® PLATFORM

Notas de la versión

para RSA NetWitness Platform 11.3

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 11.3.0.0. Lea este documento antes de implementar o actualizar a RSA NetWitness® Platform 11.3.0.0.

Novedades

RSA NetWitness® Platform 11.3.0.0 proporciona nuevas funciones y mejoras para cada función en el centro de operaciones de seguridad. Entre ellas, se incluyen las siguientes:

- Funcionalidades adicionales de análisis de hosts y archivos para actividades maliciosas o sospechosas.
- Mejoras de usabilidad para facilitar el trabajo de los encargados de respuesta ante incidentes y buscadores de amenazas.
- Mejoras de política y licencia para ayudar a los administradores a administrar sus ambientes de manera más eficiente.

NetWitness Endpoint

Agente de Endpoint

En 11.3, el agente es compatible con las funcionalidades de detección y respuesta de Endpoint (EDR), junto con la recopilación de registros de Windows.

El agente avanzado (con licencia) proporciona funcionalidades de EDR con monitoreo continuo de actividades en el host para una visibilidad profunda y análisis de todos los procesos y comportamientos en el terminal. El agente registra datos acerca de cada acción crítica, como procesos, archivos, modificaciones de registro y conexiones de red, y las envía como eventos, casi en tiempo real, al servidor. El agente puede detectar anomalías, como enlaces de imágenes, enlaces de kernel, discrepancias de registro e hilos sospechosos. Además, recopila registros de Windows. Para obtener más información, consulte la *Guía del usuario de NetWitness Endpoint*.

Las siguientes son funcionalidades clave:

- Las interacciones de la consola del usuario son fundamentales para investigar los ataques de malware que utilizan archivos legítimos de Windows, como `cmd.exe` o `powershell.exe`, para ejecutar comandos en un host comprometido.

- Visibilidad de las cadenas de argumentos completas de la línea de comandos, importantes para las investigaciones forenses.
- Detección de scripts basados en archivos o sin archivos mediante la creación de informes de scripts a partir de los eventos de proceso, en lugar de motores de script. Los motores compatibles actualmente incluyen `powershell`, `cmd`, `cscript`, `wscript`, `rundll32`, `mshtml` y `javascript`.
- Agente a prueba de alteración: las claves de registro y los archivos `exe` y `sys` de los agentes en modo de usuario y en modo de kernel están protegidos.

Los agentes de Endpoint pueden operar en Insights o modo avanzado según la configuración de la política. Para obtener más información acerca de las políticas, consulte la *Guía de configuración de NetWitness Endpoint*.

Mejoras clave en agentes 11.3 en comparación con agentes NetWitness Endpoint heredados

- Dependencias desacopladas con estructuras internas del kernel.
- Mejoras en el rendimiento en el bloqueo de archivos con un gran aumento en la cantidad de hashes que se pueden bloquear.
- Aumento de los límites de captura de eventos. Los eventos ya no están vinculados a executable-hash, sino que a la cadena de creación completa.
- Mejor compatibilidad e interoperabilidad con aplicaciones de otros fabricantes.

Sistemas operativos de agentes compatibles

Ahora se admiten los siguientes sistemas operativos:

- Windows Server 2019
- Windows 10 (32 y 64 bits) (hasta la versión 1809)
- Red Hat Linux 7.x
- macOS 10.13 (High Sierra)
- macOS 10.14 (Mojave)

Los agentes también se pueden instalar en la infraestructura de escritorios virtuales (VDI) en entornos VMware. Para obtener más información, consulte la *Guía de instalación de agente de NetWitness Endpoint*.

Implementaciones escalables y distribuidas

Puede escalar su implementación mediante la adición de múltiples Endpoint Log Hybrid, según la cantidad, la ubicación, la distribución de agentes y los datos recopilados de los terminales. Instale Endpoint Broker para obtener una vista consolidada de todos los servidores de Endpoint de la implementación. Para obtener más información, consulte la *Guía del usuario de NetWitness Endpoint* y la *Guía de configuración de NetWitness Endpoint*.

Grupos y políticas

Para administrar y actualizar de manera eficiente las configuraciones de agentes de Endpoint, los administradores pueden agrupar agentes y administrar su comportamiento mediante políticas. Los administradores pueden usar políticas predeterminadas o personalizadas. Se puede habilitar la configuración del registro de Windows mediante la política de registro de Windows en lugar de generarla a través del empaquetador de agentes. Para obtener más información, consulte la *Guía de configuración de NetWitness Endpoint*.

Analizar archivos y hosts mediante el puntaje de riesgo

Las cuentas con función de analista pueden investigar un archivo o host con puntajes de riesgo que van de 1 a 100. El contexto detallado de los colaboradores de riesgos (alertas y eventos) está disponible para facilitar la investigación expedita de actividad sospechosa o maliciosa. Para obtener más información, consulte la *Guía del usuario de NetWitness Endpoint*.

Visualización de procesos

Para mejorar la experiencia de los analistas durante una investigación de proceso, se presenta una interfaz del usuario intuitiva que permite lo siguiente:

- Comprender toda la cadena de eventos de proceso, las relaciones de elementos primarios y secundarios de proceso y todos los eventos asociados en una vista de tiempo.
- Analizar atributos importantes de proceso, como el nombre de usuario, los argumentos de inicio, la reputación, el estado de archivo, el firmante, la firma y la ruta de archivo.

Para obtener más información, consulte la *Guía del usuario de NetWitness Endpoint*.

Análisis y respuesta de archivos

Los analistas pueden:

- Analizar archivos mediante la reputación de archivos (por ejemplo, correcto conocido, no válido o sospechoso) desde Context Hub, puntaje de riesgo y estado del certificado.
- Realizar una búsqueda externa mediante Google o VirusTotal.
- Descargue un archivo y realice un análisis de archivo más detallado, como búsqueda de cadena y contenido de texto para scripts.

Después de la investigación, los analistas pueden:

- Asignar estados a archivos para categorizarlos en listas negras, listas blancas, etcétera.
- Corregir amenazas mediante el bloqueo de archivos maliciosos o infectados.

Para obtener más información, consulte la *Guía del usuario de NetWitness Endpoint*.

Reglas de aplicación para IIOC existentes

Los IIOC existentes de NetWitness Endpoint 4.4.0.x están disponibles como reglas de aplicación listas para usar en NetWitness Platform 11.3. Para obtener más información, consulte la *Guía de configuración de NetWitness Endpoint*.

Reglas de puntaje de riesgo de terminal agregadas en ESA

Además de las reglas de ejemplo de ESA, NetWitness Platform ahora incluye un paquete de puntuación de riesgo de terminal con aproximadamente 400 reglas. Estas reglas generan alertas que se utilizan para calcular los puntajes de riesgo de los archivos sospechosos y los hosts que cruzan los umbrales de puntaje de riesgo definidos. De tener NetWitness Endpoint, es posible agregar este paquete de reglas a una implementación de regla de ESA de la misma manera que se agregan reglas de ESA. Sin embargo, se debe especificar los orígenes de datos de terminales (Concentrator) durante las implementaciones de reglas de ESA. Para obtener más información, consulte la *Guía de configuración de ESA*.

Actualizaciones de la vista Investigate > Vista de análisis de eventos para eventos de Endpoint

- El análisis de texto de eventos de Endpoint proporciona texto significativo que explica el evento. También puede ver los metadatos con valores mayores de 255 caracteres.
- Para cada sesión, se puede ver el evento en el análisis de procesos o ver los detalles del host asociado con el evento al cambiar a la vista Detalles de hosts.

NetWitness Respond

Cambio de diseño de la lista de eventos para eventos de NetWitness Endpoint

Para mejorar la experiencia de los analistas e incorporar eventos de Endpoint en NetWitness Respond, la lista de eventos rediseñadas tiene un diseño flexible que mejora la representación de distintos tipos de datos. La lista rediseñada entrega facultades a los analistas para comprender y hacer triage rápidamente a los eventos con una vista previa de evento más escaneable, que está personalizada para los detalles de los eventos en lista y para NetWitness Endpoint. Para obtener más información, consulte la *Guía del usuario de NetWitness Respond*.

Se mejoró el filtro de lista de alertas para NetWitness Endpoint

Al filtrar la lista de alertas para el origen de Endpoint, se incluye las alertas de NetWitness Endpoint 4.4.x y NetWitness Endpoint 11.x.

Se agregó una regla de incidentes de UEBA

Está disponible una nueva regla de incidentes predeterminada de User Entity Behavior Analytics (UEBA), la cual captura el comportamiento de la entidad de usuario agrupada por ID de clasificador para crear incidentes a partir de alertas.

Actualización de la regla de incidentes de NetWitness Endpoint

De tener NetWitness Endpoint, las alertas de alto riesgo se comportarán del siguiente modo: La regla de incidentes predeterminada de NetWitness Endpoint captura alertas generadas por NetWitness Endpoint con un puntaje de riesgo alto o crítico. Ahora, esta regla agrupa las alertas en incidentes por nombre de host. Para obtener más información, consulte la *Guía de configuración de NetWitness Respond*.

Se agregó la capacidad de crear automáticamente incidentes de puntaje de riesgo de Endpoint

De tener NetWitness Endpoint, se puede configurar los ajustes de umbral de puntaje de riesgo de Endpoint para crear incidentes de puntaje de riesgo automáticamente para archivos y hosts sospechosos que superan los umbrales de puntaje de riesgo definidos. Para obtener más información acerca de la configuración de los ajustes de umbral de puntaje de riesgo, consulte la *Guía de configuración de NetWitness Respond*. Para obtener más información acerca de NetWitness Endpoint, consulte la *Guía de configuración de NetWitness Endpoint*.

Cambie a las vistas Investigate > Hosts y Archivos desde la vista Respond

Para una investigación detallada de un incidente, los analistas pueden acceder a la vista Investigate > Hosts y Archivos a través de la información de herramientas contextual en la vista Respond.

Buscar el estado y la información de reputación de archivos en la vista Respond

En la vista Respond y en las vistas de Investigate donde Context Hub está integrado en NetWitness Platform, los analistas pueden colocar el cursor sobre una entidad de hash de archivo para abrir información contextual sobre herramientas, la cual muestra el estado de reputación del archivo. Los analistas también pueden hacer clic en el botón Ver contexto, el cual abre el panel Búsqueda de contexto con información de archivo adicional.

NetWitness UEBA

Analítica avanzada mediante RSA NetWitness Endpoint

UEBA se integra con NetWitness Endpoint para mejorar la cobertura de detección actual en NetWitness Platform. El propósito de esta integración es identificar actividad de potenciales atacantes. Esto se centra en dos orígenes de datos primarios:

- Ejecución de los procesos
- Cambios en el registro

Para obtener más información, consulte la *Guía del usuario de NetWitness UEBA*.

Acceder a detalles de hosts o analizar vistas de procesos desde la vista Perfil de usuario

Un analista puede cambiar a la vista Detalles del host o a la vista Analizar proceso de la vista Perfil de usuario para buscar información más detallada sobre procesos anómalos o hosts asociados a riesgo del usuario. Para obtener más información, consulte la *Guía del usuario de NetWitness UEBA*.

Soporte para origen de datos adicional

NetWitness UEBA ahora es compatible con RSA SecurID como origen de datos.

NetWitness Investigate

Los analistas pueden ver una gran cantidad de eventos de forma simultánea en la lista de eventos de la vista Análisis de eventos.

Se cargan hasta 50,000 eventos en la lista de eventos en orden ascendente según la hora de recolección. Un indicador de número de fila cada 100 filas facilita la navegación a través de la lista. Las funciones de la interfaz del usuario lo ayudan a comprender lo que se muestra y el orden de clasificación. Para obtener información detallada, consulte “Análisis de eventos en la vista Análisis de eventos” en la *Guía del usuario de NetWitness Investigate*.

Los analistas pueden ver el estado detallado de una consulta en la vista Análisis de eventos

Al hacer clic en el ícono de información (ⓘ) ubicado en el generador de consultas de la vista Análisis de eventos, se abre la consola de consultas, una nueva función de interfaz de usuario que proporciona una barra de estado, advertencias, errores y otros detalles acerca de lo que está sucediendo mientras se ejecuta una consulta. Al completar una consulta, la consola de consultas muestra el rango de tiempo, la consulta, los servicios consultados, cualquier servicio que no se pudo consultar y la cantidad de tiempo que tardó cada servicio para buscar los resultados y recuperar eventos en función de la consulta. Es posible copiar la consulta completa como texto. Para obtener más información, consulte “Filtrar datos en la vista Análisis de eventos” en la *Guía del usuario de NetWitness Investigate*.

Flujo de trabajo de analistas mejorado en la vista Navegar, Eventos y Análisis de eventos

Para facilitar la realización de investigaciones a los analistas, se implementaron las siguientes mejoras:

- Al cambiar entre páginas en la vista Eventos, los eventos de registro se cargan más rápidamente debido al almacenamiento en caché de los resultados de las consultas.
- Se usa el rango de tiempo utilizado en Navegar cuando se realiza la transición a la vista Eventos.
- En la vista Navegar, se muestra una descripción de la clave de metadatos facil de entender junto al nombre de la clave de metadatos. Para obtener información detallada, consulte “Vista Navegar” en la *Guía del usuario de NetWitness Investigate*.
- Se agregó una entrada de rango de tiempo personalizada en la vista Análisis de eventos. Además de las ventanas de tiempo predefinidas, se puede ingresar un rango de tiempo personalizado y, a continuación, hacer clic en el mes, el día, el año, la hora y el minuto para editar el rango de tiempo directamente en la ruta de navegación. Para obtener más información, consulte “Filtrar datos en la vista Análisis de eventos” en la *Guía del usuario de NetWitness Investigate*.

Se muestra información detallada acerca de los eventos cargados en la vista Eventos en el pie de página

El mensaje en el pie de página ayuda a los analistas a entender lo que se ve en la vista Eventos. Si no se cargan eventos, se muestra este mensaje: "0 coincidencias de evento". Otros mensajes permiten saber si se alcanzó el límite de los resultados o el límite de escaneo que configuró el administrador se cumplen y cuales servicios tienen resultados visualizados. Por ejemplo, el siguiente mensaje le permite saber que se alcanzó el límite de escaneo y que hay más datos disponibles para escanear: “Visualizando 1-25 de más de 100,000 coincidencias de eventos (se alcanzó el límite de escaneo de 100,000 eventos)." Para obtener información detallada, consulte “Vista Eventos”, consulte la *Guía del usuario de NetWitness Investigate*.

Búsqueda y consultas más rápidas en la vista Navegar y Eventos

Cuando los analistas que trabajan en la vista Navegar consultan un Broker o un Concentrator, las consultas subsiguientes que comparten todos o algunos de los criterios de una consulta anterior devuelven resultados con mayor rapidez mediante la nueva incorporación de almacenamiento en caché en los servicios. En la vista Eventos, las consultas que utilizan operaciones complejas con valores de texto se almacenan en caché, de modo que las consultas subsiguientes que comparten todos o algunos de los resultados de los criterios de la consulta anterior se devuelven más rápidamente.

Nuevas funcionalidades del generador de consultas en la vista Análisis de eventos

- Se puede crear filtros complejos en el generador de consultas de Modo guiado mediante el filtro Formulario libre en el submenú Opciones avanzadas, que se encuentra en todos los menús desplegables del Modo guiado. El modo Forma libre aún está disponible si desea pegar una consulta larga y compleja.
- Al enviar una consulta que contiene filtros de forma libre, estos filtros se validan en el lado del servidor antes de su ejecución. Si alguno de los filtros no es válido, la consulta no se ejecutará.
- Durante la ejecución de una consulta, se puede cancelar la consulta en curso. Cuando se cancela una consulta, el conteo de eventos del panel Eventos, el mensaje del pie de página y la consola de consulta reflejan la cantidad de eventos recuperados en lugar de la cantidad total de eventos que se encuentran.

Para obtener información detallada, consulte “Filtrado de eventos en la vista Análisis de eventos” en la *Guía del usuario de NetWitness Investigate*.

Claves de metadatos actualizadas en el grupo de columnas Análisis de Endpoint

El grupo de columnas Análisis de Endpoint se actualiza para incluir nuevas claves de metadatos para la investigación de Endpoint, las cuales se muestran al visualizar un evento de Endpoint en la vista Eventos y en la vista Análisis de eventos.

Nueva opción de preferencias para controlar la actualización automática del rango de tiempo en la ruta de navegación

En la vista Análisis de eventos, una nueva preferencia en el cuadro de diálogo Preferencias de evento controla la actualización automática del rango de tiempo en la ruta de navegación. Durante la visualización de los resultados de un rango de tiempo específico, el servicio se sondea en intervalos de un minuto para detectar la presencia de nuevos resultados, pero los resultados nuevos no se cargan en la vista actual. De forma predeterminada, la ventana de rango de tiempo en la ruta de navegación permanece sincronizada con la búsqueda actual. Se puede optar por actualizar automáticamente la ventana de rango de tiempo en la ruta de navegación cuando el servicio indica que existen resultados más recientes al seleccionar la casilla de verificación **Actualizar ventana de tiempo automáticamente**. Cuando se actualiza el rango de tiempo mientras el botón Enviar consulta está activado, se puede obtener los resultados actualizados.

Acceda a UEBA desde la vista Investigate > Detalles del host

Si NetWitness UEBA está instalado, se puede analizar los riesgos asociados con los usuarios que iniciaron sesión en el host, en la vista Usuarios. Para obtener más información, consulte la *Guía del usuario de NetWitness UEBA*.

Event Stream Analysis (ESA)

Se presentó un servicio de correlación de ESA nuevo y mejorado para las reglas de correlación de ESA

El servicio de correlación de ESA en NetWitness Platform 11.3 sustituye el servicio Event Stream Analysis que se encuentra en las versiones anteriores. De forma similar al servicio Event Stream Analysis, el servicio de correlación de ESA se instala en los tipos de host primario y secundario de ESA.

Hay dos servicios de ESA que se pueden ejecutar en un host de ESA:

- Correlación de ESA (reglas de correlación de ESA)
- Event Stream Analytics Server (ESA Analytics)

El servicio del servidor de Context Hub, que proporciona la funcionalidad de búsqueda de enriquecimiento en las vistas Respond e Investigate, solo se ejecuta en un host de ESA primario.

Compatibilidad con diferentes orígenes de datos para las reglas de correlación de ESA

En lugar de agregar orígenes de datos, como Concentrator, a todo el servicio, se puede especificar diferentes orígenes de datos para cada implementación de reglas de ESA. Por ejemplo, en un caso donde se desea usar Concentrator con datos de paquetes HTTP en una implementación y Concentrator con datos de registro HTTP en otra implementación. Para obtener más información, consulte la *Guía del usuario de creación de alertas con reglas de correlación de ESA*.

Para consideraciones de actualización de implementaciones de reglas de ESA, consulte las instrucciones de actualización aplicables, así como la *Guía de configuración de ESA*.

Compatibilidad con ajustes de nivel de compresión de los Concentrator en ESA

Al configurar la implementación de una regla de ESA y configurar un Concentrator para usarlo como origen de datos, tiene la opción de especificar el nivel de compresión de datos para el concentrator en ESA. Para obtener más información, consulte la *Guía del usuario de creación de alertas con reglas de correlación de ESA*.

Habilitar o deshabilitar el reenvío de alertas de reglas de ESA individuales a la vista Respond

Se puede activar o desactivar las alertas para las reglas de ESA individuales. Para obtener más información, consulte la *Guía de configuración de ESA*.

Actualización de la versión de ESPER desde la versión 5.3 a 7.1

Se actualizó ESPER a la versión más reciente, 7.1.

Log Collectors

Lista ordenada de Log Collectors y Virtual Log Collectors (VLC)

En el caso de los servicios Log Collector, Local Collectors y Remote Collectors, los menús desplegables se ordenan alfabéticamente para facilitar la localización del recopilador que desea ver:

- En un Local Collector, en la pestaña Remote Collectors, el campo Remote Collectors en el cuadro de diálogo Agregar origen está ordenado.
- En un Virtual Log Collector, la pestaña Local Collectors tiene campos ordenados para destinos y orígenes.

Lista ordenada de Log Collectors y Log Decoders

En la vista ADMINISTRAR > Estado y condición > Monitoreo de orígenes de eventos, los menús desplegables de Log Collectors y Log Decoders se ordenan alfabéticamente para facilitar la localización de los elementos que desea ver.

Puertos de syslog de Local Log Collectors

En 11.3, los Local Log Collector (Log Collectors ubicados en los dispositivos Log Decoder) tienen capacidades de recibir syslog en puertos distintos de 514 y 6514 a fin de admitir la recepción de mensajes de syslog con diferentes codificaciones, como EUC-KR, ISO8897-9, etcétera. El servicio Log Decoder sigue siendo el punto de recopilación para la recepción de registros ASCII/UTF-8 en el puerto 514 y 6514.

"Lógica de paso" mejorada para syslog fuera de estándar

Los Remote Log Collectors ahora aceptan todos los mensajes de syslog que están fuera de norma, excepto aquellos con encabezados o cuerpos de mensaje vacíos. Los mensajes no deseados se deben filtrar en la recolección de syslog mediante los filtros de eventos. Para obtener más información, consulte la sección "Configurar filtros de eventos para un recopilador" en la *Guía de recopilación de registros*. Consulte RFC3164 y RFC5424 de syslog para obtener más información sobre el formato syslog (https://www.ietf.org/standards/rfcs/).

Servicios principales

Analizador Snort con compatibilidad con UDM

La compatibilidad con el analizador Snort se actualizó con una nueva opción, `udm=true`, que utiliza el conjunto de claves del modelo de datos unificado (UDM) alineado. Para obtener más información, consulte "Analizador Snort" en la *Guía de configuración de Decoder y Log Decoder*.

Descifrado de SMTP seguro

NetWitness Platform es compatible con el descifrado oportunista de SSL/TLS, orientado a RFC 3207 (https://tools.ietf.org/html/rfc3207). Se puede agregar una opción de analizador HTTPS que proporcione una lista con formato de valores separados por comas (.csv) de los puertos de destino de la sesión en la que se buscará el comando de STARTTLS, con al menos una clave de cifrado que se haya cargado. Esto habilita la funcionalidad de STARTTLS. Para obtener más información, consulte "Descifrado de la *Guía de configuración de Decoder y Log Decoder*.

El analizador de GeoIP ya no es compatible; se sustituye con el analizador GeoIP2

No se admite el analizador de GeoIP original. El nuevo analizador GeoIP2 que se incorporó en 11.2 lo sustituye por completo. El analizador GeoIP2 admite todas las funcionalidades anteriores, así como el nuevo paquete Maxmind, incluidas las conversiones IPv4 e IPv6.

Limitar el uso de memoria de la consulta con el parámetro SDK max.query.memory

El parámetro `max.where.clause.sessions` se usa para imponer un límite en la cantidad de sesiones que se puede escanear en una única consulta. Por ejemplo, si un usuario selecciona todos los metadatos de la base de datos, esta deja de procesar los resultados una vez que la cantidad de sesiones leídas para la consulta alcanza este valor de configuración. Este parámetro quedará obsoleto en una versión futura. El parámetro `max.query.memory` se puede usar para limitar el uso total de memoria en la consulta.

Se puede usar SED PowerVault para almacenamiento externo

Ahora se puede configurar SED (unidades con cifrado automático) PowerVault para su uso como almacenamiento externo con el fin de almacenar datos de registros y paquetes para su recuperación.

Los índices N-Gram ofrecen un mejor rendimiento que las referencias en 11.2, lo que mejora las búsquedas de texto completo

Se han realizado mejoras en la tasa de inserción de índices de N-Gram para las búsquedas de texto completo. Los índices de modo N-Gram presentan aproximadamente el doble de la velocidad para las actualizaciones, lo que significa que se pueden aprovechar en más Concentrator sin impacto en el rendimiento de la agregación. Esta función está deshabilitada de forma predeterminada. Para obtener información sobre los índices N-Gram, consulte "Personalización de índices" en la *Guía de ajuste de la base de datos principal de NetWitness Platform*.

Nueva función `avglen` en la sintaxis de consulta de base de datos

La función `avglen` se agregó a la sintaxis de consulta. Devuelve un único valor, que es la longitud promedio de un valor de metadatos dentro de una función.

Administración

Capacidad de configurar componentes híbridos en dispositivos principales (permite el uso de varios PowerVault para componentes híbridos)

Se puede instalar categorías híbridas, como las categorías de servicio Log Hybrid y Network (Packet), en un host físico serie 6 (R640). Esto le brinda la capacidad de conectar varios dispositivos de almacenamiento externo de PowerVault al host físico de la serie 6 (R640).

Autenticación Public Key Infrastructure (PKI)

La autenticación de PKI permite a los usuarios autenticarse y acceder a la interfaz del usuario de NetWitness Platform mediante certificados digitales. Para obtener más información, consulte la sección Autenticación de PKI en la *Guía de administración de usuarios y de la seguridad del sistema.*

Compatibilidad con DISA STIG

RSA es compatible con todas las reglas de auditoría en el grupo de control de Guía de implementación técnica de seguridad de la Agencia de sistemas de información de defensa (DISA STIG) en la versión 11.3. Para obtener información detallada sobre STIG compatible en 11.3, consulte la *Guía de mantenimiento del sistema.*

Comando de emisión de certificados

RSA agregó el comando `cert-reissue` y sus argumentos, de modo que pueda volver a emitir certificados de host. Después de actualizar todos los hosts a 11.3, se debe volver a emitir certificados para todos ellos tan pronto como sea posible para evitar que venzan. Si los certificados vencen, la implementación de NetWitness pasará a un estado irrecuperable. Para obtener información detallada sobre cómo resolver certificados en 11.3, consulte la *Guía de configuración del sistema.*

Host de servidor de NW semiactivo en espera (para conmutación por error/alta disponibilidad): solo host físico

El servidor de NW semiactivo en espera duplica los componentes críticos y las configuraciones del host del servidor de NW activo para aumentar la confiabilidad. El servidor de NW en espera semiActivo puede configurarse para permanecer en modo en espera y recibir respaldos del host del servidor de NW activo a intervalos regulares. Si el servidor de NW activo falla (se desconecta), se puede ejecutar el procedimiento de conmutación por error y el servidor de NW en espera se activa. Para obtener información detallada sobre cómo configurar y administrar un servidor de NW en espera semiactivo en 11.3, consulte la NetWitness Platform *Guía de implementación*.

Nueva herramienta para consolidación de datos de configuración de hosts y servicios en una sola instancia

La herramienta NW-Consolidator está disponible para clientes selectivos de 10.6.6 que desean migrar la configuración y los datos de 10.6.6 a NetWitness Platform 11.3. Esta herramienta se puede usar si la implementación tiene varias instancias de Security Analytics y Reporting Engine y desea consolidar los datos y la configuración de hosts y servicios en una única instancia. También se puede consolidar los datos relacionados con los usuarios, los grupos, las funciones, los feeds y los informes.

Licencia

(Compatibilidad con licencias de servidores de correlación de terminales y ESA y consolidación de todos los derechos para las licencias de rendimiento

La interfaz del usuario de licencias mejorada facilita a los administradores la visualización de la información de licencia. La página Detalles de licencia muestra el rendimiento agregado para diferentes derechos con tendencias de uso de rendimiento. Los administradores pueden ver todas las licencias de la implementación, incluidas las de Endpoint y del servidor de correlación de ESA. Además, los administradores pueden configurar las licencias para varios servidores de NetWitness y servidores activos y semiactivos. Para obtener más información, consulte la *Guía de administración de licencia*.

Autenticación con reconocimiento de amenazas

Integración de NetWitness Platform con RSA SecurID Access

La integración de NetWitness Platform con RSA SecurID Access permite identificar usuarios sospechosos en NetWitness Platform y elevar los niveles de acceso o bloquear a los usuarios en RSA Secure ID Access según el nivel de seguridad y las políticas definidas en Secure ID. El servidor de NetWitness Respond envía identificadores de correo electrónico de usuarios sospechosos de incidentes a RSA SecurID Access. Para configurar esta integración en el servidor de Respond, consulte la *Guía de configuración de Respond*.

Problemas resueltos

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

Security

Número de rastreo	Descripción
ASOC-59254	Actualización de seguridad del kernel https://access.redhat.com/errata/RHSA-2018:1965.
ASOC-58383	Actualización de seguridad de policycoreutils https://access.redhat.com/errata/RHSA-2018:0913.
ASOC-58382	Actualización de seguridad de Openssl https://access.redhat.com/errata/RHSA-2018:0998.

Investigate

Número de rastreo	Descripción
ASOC-61230	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.
ASOC-60941	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.
ASOC-50196	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).
ASOC-49427	El generador de consultas de la vista Análisis de eventos no responde a los filtros que contienen un espacio.

Respond

Número de rastreo	Descripción
ASOC-59243	Cuando se eliminan todas las alertas para una regla de alerta, el filtro de la regla no se quita correctamente.
ASOC-37533	Al crear una tabla en la memoria personalizada y se agrega como un origen de enriquecimiento en ESA, esa información no se muestra para las alertas de ESA.

Event Stream Analysis (ESA)

Número de rastreo	Descripción
ASOC-60511	Las reglas de CH de ESA se deshabilitan durante la actualización o el reinicio del host de ESA
ASOC-60367	Las reglas de ESA con claves de metadatos personalizados no se implementan en el servidor de ESA
ASOC-26481	No se puede establecer el nivel de compresión de ESA como en otros dispositivos.
ASOC-14157	ESA muestra una advertencia para los operadores de arreglo.

Servicios principales

Número de rastreo	Descripción
ASOC-41902	Se debe deshabilitar ell modo SSL FIPS (casilla de verificación) para Broker, Concentrator y Archiver se debe deshabilitar.

Actualización

Número de rastreo	Descripción
ASOC-49843	Las plantillas de registro de auditoría no se actualizan en el archivo de conf de salida de Logstash durante la actualización a 11.x.

Número de rastreo	Descripción
ASOC-42136	Después de la actualización, los vínculos de investigación están deshabilitados para los gráficos estáticos.

Notas sobre la actualización

Las siguientes rutas de actualización son compatibles con RSA NetWitness® Platform 11.3.0.0:

- RSA NetWitness® Platform 10.6.6.x a 11.3.0.0
- RSA NetWitness® Platform 11.0.x, 11.1.x o 11.2.x a 11.3.0.0

Para obtener más información sobre la instalación y la actualización a 11.3.0.0, consulte las guías de instalación y actualización en https://community.rsa.com/community/products/netwitness/113 > Installation and Upgrade Guides.

Documentación del producto

Con esta versión se proporciona la siguiente documentación.

Documentación	Dirección URL de ubicación
Documentación en línea de RSA NetWitness Platform 11.3	https://community.rsa.com/community/products/netwitness/documentation
Instrucciones de actualización y listas de comprobación de RSA NetWitness Platform 11.3	https://community.rsa.com/community/products/netwitness/documentation
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

Problemas conocidos

Los problemas que permanecen pendientes en esta versión se documentan aquí: https://community.rsa.com/community/products/netwitness/documentation/known-issues. Si está disponible una solución alternativa, esto se indica o se menciona en detalle.

Comentarios sobre la documentación del producto

Puede enviar un correo electrónico a sahelpfeedback@rsa.com para proporcionar comentarios sobre la documentación de RSA NetWitness Platform.

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.

No.	Función	Notas
7.	Algunas características del servicio Event Stream Analysis de 11.2 y versiones anteriores	Las funciones del servicio Event Stream Analysis (11.2 y anteriores) que no están en el servicio de correlación de ESA 11.3: 1. Instantánea de la memoria para las reglas de prueba 2. Método de notificación de SNMP de ESA 3. Base de datos como origen de enriquecimiento (se sustituye por la lista de Context Hub) 4. Warehouse Analytics como origen de enriquecimiento (se sustituye por la lista de Context Hub) 5. Conexión de la base de datos como origen de enriquecimiento (se sustituye por la lista de Context Hub) 6. Deshabilitar ordenamiento por hora de captura 7. Pool de memoria
8.	Endpoint Hybrid	El tipo de host Hybrid Endpoint no es compatible en 11.3.0.0 ni en versiones superiores.

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.

Si tiene preguntas o necesita ayuda, siga las instrucciones que se proporcionan aquí:
https://community.rsa.com/docs/DOC-1294

Historial de revisiones

Revisión	Fecha	Descripción
1.0	13-Mar-19	Liberación a Operaciones