RSA NETWITNESS® PLATFORM

Guía de inicio rápido de NetWitness UEBA

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 Dell, 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 Dell.

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

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

junio 2019

¿Qué es NetWitness UEBA?

RSA NetWitness UEBA (User and Entity Behavior Analytics) es una solución de analítica avanzada para descubrir, investigar y monitorear comportamientos riesgosos en todos los usuarios y todas las entidades del ambiente de red. NetWitness UEBA se utiliza para lo siguiente:

- Detección de usuarios maliciosos y deshonestos
- Detección de comportamientos de alto riesgo
- Descubrimiento de ataques
- Investigación de amenazas de seguridad emergentes
- Identificar actividad potencial de atacantes

Acerca de esta guía

En esta guía se proporcionan instrucciones de punto a punto para configurar NetWitness Platform UEBA y para utilizar las funciones de UEBA.

Documentación en línea de RSA NetWitness Platform 11.3 en RSA Link

La documentación del producto NetWitness Platform está organizada en líneas funcionales. Si se busca una versión o una guía específica, esta información está disponible en la Tabla de contenidos principal de la versión 11.x.

Utilice estos enlaces para ver la documentación de RSA NetWitness Platform 11.3. Ambos enlaces proporcionan la misma documentación en estos dos formatos:

- Las guías HTML incluyen la información más reciente acerca de las versiones 11. x soportadas actualmente: Documentación en línea de RSA NetWitness Platform 11.x.
- Las guías PDF proporcionan la información correspondiente a una versión específica: PDF de RSA NetWitness Platform 11.3.

Utilice estos enlaces para obtener acceso a documentación que no está relacionada con una versión específica del software:

- Guías de configuración de hardware: https://community.rsa.com/community/products/netwitness/hardware-setup-guides.
- Documentación de contenido de RSA, como feeds, analizadores, reglas de aplicación e informes: https://community.rsa.com/community/products/netwitness/rsa-content.

Introducción

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	
Ver información acerca de las actualizaciones del producto, las mejoras y los problemas conocidos.	Notas de la versión
Comprender NetWitness UEBA	*Guía del usuario de RSA NetWitness UEBA*

Instalación y configuración

Instalación independiente

Las siguientes tareas deben realizarse en la siguiente secuencia.

Descripción	Referencias
	
Revisar el hardware soportado.	Tema “Requisitos del sistema” en la *Guía de instalación independiente de UEBA*
Revisar la implementación de UEBA.	Tema “Instalación independiente de RSA NetWitness UEBA” en la *Guía de instalación independiente de UEBA*
Configurar puertos en el firewall.	Tema “Instalación independiente de RSA NetWitness UEBA" en la *Guía de instalación independiente de UEBA*
Instalar el host del servidor de NetWitness	Tema “Tareas de instalación” en la *Guía de instalación independiente de UEBA*
Instalar Log Host Hybrid 11.3.	Tema “Tareas de instalación” en la *Guía de instalación independiente de UEBA*
Instalar y configurar NetWitness UEBA.	Tema “Tareas de instalación” en la*Guía de instalación independiente de UEBA*
Asignar las funciones UEBA_Analysts y Analysts a los usuarios de UEBA.	“Permisos de función” en la Guía de administración de usuarios y de la seguridad del sistema de

Instalación nueva

Las siguientes tareas deben realizarse en la siguiente secuencia.

Descripción	Referencias
	
Revisar el hardware soportado.	"Hardware compatible" en la *Guía de instalación de hosts físicos*
Revisar la arquitectura de UEBA.	Tema "Diagrama de la arquitectura de red de NetWitness Platform" en la *Guía de implementación*
Configurar puertos en el firewall.	Tema "Puertos y arquitectura de red" de la *Guía de implementación*
Instalar el host del servidor de NetWitness y otros componentes.	"Tarea 1: Instalar 11.3 en el host del servidor de NetWitness (servidor de NW)" y "Tarea 2: Instalar 11.3 en otros hosts de componentes" en la *Guía de instalación de hosts físicos* "Instalar el host virtual de NetWitness Platform en un entorno virtual" en la *Guía de instalación de hosts virtuales*
Instalar UEBA.	"RSA NetWitness® UEBA" en la *Guía de instalación de hosts físicos*
Asignar las funciones UEBA_Analysts y Analysts a los usuarios de UEBA.	"Permisos de función" en la *Guía de administración de usuarios y de la seguridad del sistema de* .

Actualización

Las siguientes tareas deben realizarse en la siguiente secuencia.

Descripción	Referencias
	
Implementar el paquete de Endpoint desde RSA Live, que contiene Analizador Lua de categoría de archivos para la integración de UEBA con Endpoint.	Durante la implementación, se debe especificar el servicio Log Decoder de Endpoint Log Hybrid En el caso de contar con varios servidores de Endpoint, seleccione todos los servicios Log Decoder de Endpoint Log Hybrid

Descripción	Referencias
Habilitar orígenes de datos de Endpoint, como procesos y registros, para generar alertas en UEBA.	"Activar orígenes de datos de Endpoint" en las *Instrucciones de actualización*
Habilitar el reenviador de indicador de UEBA para transferir los indicadores de UEBA al servidor de NetWitness Respond y al servidor de correlación para crear incidentes de .	"Habilitar el reenviador de indicadores UEBA" en las *Instrucciones de actualización*
Después de la actualización a la plataforma NetWitness 11.3, se modifican los UUID de Broker o Concentrator. Se debe actualizar los servicios principales de NetWitness Platform y actualizar el UUID de Broker o Concentrator.	"Actualizar el UUID de Broker o Concentrator" en las *Instrucciones de actualización*
Actualizar la configuración del flujo de aire.	"Actualizar la configuración del flujo de aire" en las *Instrucciones de actualización*
Reiniciar el servicio del programador de flujo de aire después de que el DAG de presidio_upgrade se haya ejecutado correctamente.	"Reiniciar el servicio del programador de flujo de aire" en las *Instrucciones de actualización*

Investigación

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	
Investigar a los usuarios de alto riesgo.	Tema "Investigar usuarios de alto riesgo" en la *Guía del usuario de RSA NetWitness UEBA*
Investigar las alertas principales.	Tema "Investigar las alertas principales" en la *Guía del usuario de RSA NetWitness UEBA*

Monitoreo

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	
Revisar métricas de NetWitness UEBA en Estado y condición.	Tema "Ver métricas de NetWitness UEBA en Estado y condición" en la Guía del usuario de RSA NetWitness UEBA
Monitorear el estado y la condición de UEBA.	Tema “Monitorear el estado y la condición de UEBA” de la Guía del usuario de RSA NetWitness UEBA