RSA NETWITNESS® PLATFORM

Guía de inicio rápido de NetWitness Endpoint

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 Endpoint?

RSA NetWitness Endpoint es una herramienta de respuestas y de detección de terminales que monitorea continuamente los terminales en una red, a fin de proporcionar una visibilidad detallada y un análisis sólido de todos los ejecutables y procesos. Ayuda a detectar ataques nuevos, desconocidos y dirigidos, resalta la actividad sospechosa para su investigación, expone comportamientos anormales y determina el alcance de la vulneración para ayudar a los analistas a responder a las amenazas avanzadas con mayor rapidez.

Acerca de esta guía

Esta guía proporciona instrucciones de punto a punto para configurar NetWitness Platform Endpoint y utilizar las funciones de Endpoint.

Documentación de RSA NetWitness Platform 11.3 en RSA Link

La documentación del producto de NetWitness Platform está organizada en líneas funcionales. Si se busca una versión o una guía específica, vaya a la Tabla de contenido 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 que se soportan actualmente: Documentación 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
	

Descripción	Referencias
Ver información acerca de las actualizaciones del producto, las mejoras y los problemas conocidos.	Notas de la versión
Comprender NetWitness Endpoint.	“Introducción a NetWitness Platform" e "Investigate" en la *Guía de introducción de NetWitness Platform*

Configuración e instalación

Instalación nueva

Las siguientes tareas se deben realizar en la secuencia indicada.

Descripción	Referencias
	
Obtener una licencia de Endpoint Log Hybrid.	Guía de administración de licencia
Revisar el hardware compatible.	“Hardware compatible” en la *Guía de instalación de hosts físicos*
Revise la arquitectura de Endpoint. Planee la implementación en función de la cantidad de terminales, la distribución y la ubicación de estos terminales. y elija una de las siguientes implementaciones: • Servidor único de Endpoint • Múltiples servidores de Endpoint	“Arquitectura de NetWitness Endpoint” en la *Guía de implementación*
Configurar los puertos en el firewall.	“Puertos y arquitectura de red” de la *Guía de implementación*
Instalar NetWitness Server y otros componentes. Para una implementación de un solo servidor de Endpoint, se debe instalar NetWitness Server, Endpoint Log Hybrid y ESA. Para un servidor con varias instancias de Endpoint, además de los componentes anteriormente mencionados, se debe instalar Endpoint Log Hybrid adicionales y NetWitness Broker con Endpoint Broker instalado en este.	- *Guía de instalación de hosts físicos* para obtener instrucciones sobre cómo configurar hosts físicos - *Guía de instalación de hosts virtuales* para obtener instrucciones sobre cómo configurar hosts virtuales

Descripción	Referencias
Instalar Endpoint Log Hybrid.	"RSA NetWitness Endpoint" en la *Guía de instalación de hosts físicos*
Revisar los servicios instalados.	*Guía de introducción de hosts y servicios*
Nota: Revise las políticas predeterminadas y modifíquelas según corresponda. Instalar el agente de Endpoint en los hosts.	Tema "Orígenes de Endpoint" en la *Guía de configuración de Endpoint* *Guía de instalación de agentes de NetWitness Endpoint*

Actualización

Las siguientes tareas se deben realizar en la secuencia indicada.

Descripción	Referencias
	
Actualización de 10.6.5 a 11.3: Después de la actualización de NetWitness Platform a 11.3, instale Endpoint Log Hybrid y otros componentes de Endpoint.	- *Guía de actualización de hosts físicos* para obtener instrucciones sobre la actualización de hosts físicos - *Guía de actualización de hosts virtuales* para obtener instrucciones sobre la actualización de hosts virtuales
Actualizar los hosts de 11.x a 11.3: Actualice el servidor y los agentes de Endpoint.	*Guía de actualización*
Actualizar los agentes de Endpoint de 11.1.x y 11.2.x a 11.3.	"Agentes de actualización" en la *Guía de instalación de agente de Endpoint*
Migrar NetWitness Endpoint 4.4.0.x a NetWitness Platform.	*Guía de migración de NetWitness Endpoint 4.4.0.x a RSA NetWitness Platform 11.3*

Configuración

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	

Descripción	Referencias
Comprender las tareas de NetWitness Endpoint y de alto nivel que se requieren para la configuración.	"Descripción general de NetWitness Endpoint y configuración del servidor de Endpoint" en la *Guía de configuración de Endpoint*
Revisar los grupos y las políticas de agentes.	Tema "Orígenes de Endpoint" en la *Guía de configuración de Endpoint*
Configurar la cuenta de RSA Live y verificar si el contenido de ESA y las reglas de aplicación para Endpoint están disponibles. **Nota:** El servicio de reputación de archivos se activa automáticamente en RSA Live.	*Guía de administración de servicios de Live*
Crear control de acceso basado en funciones (RBAC).	"Permisos de función" en la Guía de administración de usuarios y de la seguridad del sistema de
Configurar una política de retención de datos.	"Configurar la retención de datos" en la *Guía de configuración de Endpoint*
Administrar agentes inactivos	"Administrar agentes inactivos" en la *Guía de configuración de Endpoint*

Investigación

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	
Comprender cómo funciona la investigación.	"Cómo funciona NetWitness Investigate" en la *Guía del usuario de NetWitness Investigate*.
Configurar las vistas de Investigate.	"Configuración de vistas y preferencias de NetWitness Investigate" en la *Guía del usuario de NetWitness Investigate*
Comenzar una investigación en distintas vistas de Investigate.	"Iniciar una investigación" en la *Guía del usuario de NetWitness Investigate*
Revise las mejores prácticas para los archivos y los hosts y configure la vista Investigate para la investigación.	"Mejores prácticas" en investigación de archivos y de hosts en la *Guía del usuario de NetWitness Endpoint*

Descripción	Referencias
Investigar los archivos.	"Investigación de archivos" en la *Guía del usuario de NetWitness Endpoint*
Investigar los hosts	"Investigación de hosts" en la *Guía del usuario de NetWitness Endpoint*
Investigar el proceso.	"Investigación de hosts" en la *Guía del usuario de NetWitness Endpoint*
Analizar los archivos descargados.	"Análisis de archivos descargados" en la *Guía del usuario de NetWitness Endpoint*
Cambiar el estado del archivo y realizar una corrección.	"Cambiar estado o corrección de archivo" en la *Guía del usuario de NetWitness Endpoint*
Analizar eventos.	"Análisis de eventos" en la *Guía del usuario de NetWitness Endpoint* "Análisis de datos crudos y metadatos en la vista análisis de eventos", "Investigación de metadatos en la vista Navegar" y "Análisis de eventos crudos en la vista Eventos" en la *Guía del usuario de NetWitness Investigate*

Respond y Reporting

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	
Responder a los incidentes de Endpoint.	*Guía del usuario de NetWitness Respond*
Ver informes relacionados con datos de Endpoint.	*Guía del usuario de Reporting*

Mantenimiento

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	
Monitorear estado y condición.	Guía de mantenimiento del sistema

Integración (para NetWitness Endpoint legados)

Las siguientes tareas se pueden realizar en cualquier secuencia.

Descripción	Referencias
	
Configure los metadatos de NetWitness Endpoint 4.4.x con NetWitness Platform.	Tema “Integración de NetWitness Endpoint 4.4.0.2 o superior con NetWitness Platform" de la *Guía de configuración de Endpoint*
Configure la operación integrada de NetWitness Endpoint 4.4.x con NetWitness Platform.	*Guía de integración de RSA NetWitness Endpoint*