RSA NETWITNESS® PLATFORM

Notas de la versión

para la versión 11.2.1

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 NetWitness Platform 11.2.1.0. Lea este documento antes de implementar o actualizar a NetWitness Platform 11.2.1.0.

Novedades

La versión 11.2.1.0 de NetWitness Platform proporciona la siguiente mejora.

NetWitness User and Entity Behavior Analysis (UEBA)

Compatibilidad con el modelo de acceso remoto. Ahora, UEBA modela el acceso de usuarios a computadoras remotas mediante el protocolo de escritorio remoto. Este modelo define las computadoras remotas a las que accede comúnmente cada usuario y marca cualquier acceso anormal. Para obtener más información, consulte la *Guía del usuario de RSA NetWitness UEBA*.

Problemas resueltos

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

Security

Número de rastreo	Descripción
ASOC-61704	Actualización de seguridad de yum-utils https://access.redhat.com/errata/RHSA-2018:2285
ASOC-61929	Actualización de seguridad del kernel https://access.redhat.com/errata/RHSA-2018:2384
ASOC-60399	Actualización de seguridad de Openjdk https://access.redhat.com/errata/RHSA-2018:2242
ASOC-59638	Actualización de seguridad de Gnupg2 https://access.redhat.com/errata/RHSA-2018:2181

Número de rastreo	Descripción
ASOC-62742	Actualización de seguridad de postgresql https://access.redhat.com/errata/RHSA-2018:2557
ASOC-62744	Actualización de seguridad de Bind https://access.redhat.com/errata/RHSA-2018:2570
ASOC-59640	Actualización de seguridad de Python https://access.redhat.com/errata/RHSA-2018:2123

Servidor

Número de rastreo	Descripción
SACE-10385/ SACE-10364	La vista Estado y condición no muestra las páginas actualizadas.
SACE-9850	En la vista Gráficos, el orden ascendente y descendente no muestra resultados.

Reporting

Número de rastreo	Descripción
SACE-10456	En la vista Reglas, cuando se define una cláusula WHERE, se agrega automáticamente espacio adicional después de cada condición.

Investigate

Número de rastreo	Descripción
SACE-10329	Cuando se realiza una consulta en la vista Investigación, el cuadro de diálogo de la consulta no permite ingresar más de seis caracteres.
SACE-10162	La consulta de Investigación con grupos de metadatos no es compatible con direcciones IP en el formato CIDR.

Número de rastreo	Descripción
SACE-10060	Las claves de metadatos con tipo entero no muestran opciones para los operadores en la lista desplegable Intelli Sense.

Estado y condición

Número de rastreo	Descripción
SACE-10237	Cuando exporta orígenes de eventos, se crea un archivo CSV no válido.

Event Stream Analysis

Número de rastreo	Descripción
SACE-9793	Se produce un error cuando se configura el servicio Whois.

Servicios principales

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

Número de rastreo	Descripción
SACE-10222	El archivo de salida carece de registros cuando se reinicia el Concentrator.

Números de compilación

En la siguiente tabla se muestran los números de compilación de los diversos componentes de NetWitness Platform 11.2.1.0.

Componente	Número de versión
NetWitness Platform Web Server	11.2.1-x
NetWitness Platform Decoder	11.2.1-x

NetWitness Platform Concentrator	11.2.1-x
NetWitness Platform Broker	11.2.1-x
NetWitness Platform Log Decoder	11.2.1-x
NetWitness Platform Archiver (Workbench)	11.2.1-x
NetWitness Platform Event Stream Analysis Server	11.2.1-x
NetWitness Platform Appliance	11.2.1-x
NetWitness Platform Archiver	11.2.1-x
NetWitness Platform Cloud Gateway Server	11.2.1-x
NetWitness Platform Concentrator	11.2.1-x
NetWitness Platform Console	11.2.1-x
NetWitness Platform Endpoint Server	11.2.1-x
NetWitness Platform Investigate Server	11.2.1-x
NetWitness Platform Legacy Web Server	11.2.1-x
NetWitness Platform Log Player	11.2.1-x
NetWitness Platform Respond Server	11.2.1-x
NetWitness Platform SDK	11.2.1-x

Instrucciones para la actualización

Las siguientes rutas de actualización son compatibles con NetWitness Platform 11.2.1.0:

- RSA NetWitness® Platform 11.1.0.0 a 11.2.1.0
- RSA NetWitness® Platform 11.1.0.1 a 11.2.1.0
- RSA NetWitness® Platform 11.1.0.2 a 11.2.1.0
- RSA NetWitness® Platform 11.1.0.3 a 11.2.1.0

- RSA NetWitness® Platform 11.2.0.0 a 11.2.1.0
- RSA NetWitness® Platform 11.2.0.1 a 11.2.1.0

Para obtener más información sobre cómo actualizar a 11.2.1.0, consulte las instrucciones de actualización en la sección Instalación y actualización.

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.

Nota: Los problemas conocidos de las versiones anteriores de 11.2.1.0 se pueden solucionar en las versiones de parche. Consulte las notas de la versión respectivas de los parches que están disponibles en RSA Link: https://community.rsa.com/.

UEBA

Bajo la política de UEBA se enumeran estadísticas duplicadas.

Número de rastreo: ASOC-70119

Problema: Después de que se crea una regla bajo la política de UEBA, se muestran valores duplicados en la lista desplegable Estadísticas.

Solución alternativa:

1. Inicie sesión en MongoDB utilizando el siguiente comando:
   ```
   mongo admin -u deploy_admin -p {Ingrese la contraseña}
   ```
2. Ejecute el siguiente comando en MongoDB
   ```
   use sms;
   db.getCollection('sms_statdefinition').find({componentId
   :"presidioairflow"})
   db.getCollection('sms_statdefinition').deleteMany({componentId
   :"presidioairflow"})
   ```

El servicio UEBA muestra una versión incorrecta.

Número de rastreo: ASOC-69605

Problema: Después de la actualización de NetWitness Platform a 11.2.1, la vista **ADMINISTRAR > Hosts** muestra la versión incorrecta de UEBA.

Solución alternativa: Debe actualizar el servicio UEBA.

1. Vaya a **ADMINISTRAR > Hosts**.
2. Seleccione un host de UEBA.
3. Haga clic en **Actualizar** > **Actualizar host** en la barra de herramientas.
4. Haga clic en **Iniciar actualización**.

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

Comentarios sobre la documentación del producto

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

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	17/12/2018	Segunda versión preliminar