RSA NETWITNESS® PLATFORM

Notas de la versión

para la versión 11.2.0.1

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

Notas de la versión

En este documento se indican las reparaciones realizadas en NetWitness Platform 11.2.0.1. Lea este documento antes de implementar o actualizar NetWitness Platform 11.2.0.1

Problemas resueltos

En este documento se indican los problemas resueltos en NetWitness Platform 11.2.0.1.

Reparaciones en el servidor

Número de rastreo	Descripción
ASOC-64089	El idioma de configuración de la aplicación se restablece cuando la localización está habilitada. En NetWitness Platform 11.2.0.0, no puede configurar francés, alemán o japonés como la preferencia de idioma.

Reparaciones en Malware Analysis

Número de rastreo	Descripción
SACE-9874	Cuando utiliza una versión anterior de la llamada URL hash, Malware Analysis no muestra los detalles del proveedor de antivirus.

Reparaciones en Administración de orígenes de eventos

Número de rastreo	Descripción
ASOC-62575	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`.

Reparaciones en servicios principales

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

Número de rastreo	Descripción
SACE-10191	El servicio Log Decoder se regenera cuando save.session.count está configurado en Automático.
SACE-10283	MetaDB en Log Decoder se regenera debido a una estructura incorrecta del directorio del analizador.
SACE-10336	Network Decoder presenta una falla general debido al controlador de tarjeta de red 10G.

Números de compilación

En la siguiente tabla se muestran los números de compilación de los diversos componentes de NetWitness Platform 11.2.0.1.

Componente	Número de versión
NetWitness Platform Decoder	11.2.0.1-9473.5
NetWitness Platform Concentrator	11.2.0.1-9473.5
NetWitness Platform Broker	11.2.0.1-9473.5
NetWitness Platform Log Decoder	11.2.0.1-9473.5
NetWitness Platform Archiver (Workbench)	11.2.0.1-9473.5
NetWitness Platform Event Stream Analysis Server	11.2.0.1-448.5
NetWitness Platform Appliance	11.2.0.1-9473.5
NetWitness Platform Archiver	11.2.0.1-9473.5
NetWitness Platform Console	11.2.0.1-9473.5
NetWitness Platform Legacy Web Server	11.2.0.1-181010193532.5
NetWitness Platform Log Player	11.2.0.1-9473.5
NetWitness Platform SDK	11.2.0.1-9473.5

Instrucciones para la actualización

Debe leer la información y seguir estos procedimientos para actualizar NetWitness Platform versión 11.2.0.1.

Las siguientes rutas de actualización son compatibles con NetWitness Platform 11.2.0.1:

- NetWitness Platform 11.2.0.0 a 11.2.0.1
- NetWitness Platform 11.1.0.3 a 11.2.0.1

Para conocer las rutas de actualización compatibles con 11.2.0.0, consulte la *Guía de actualización para la versión 11.0.x.x u 11.1.x.x a 11.2*.

Puede actualizar el parche de 11.2.0.1 mediante una de las siguientes opciones:

- Si el servidor de NetWitness tiene conexión a Internet con Servicios de Live, es posible usar la interfaz del usuario de NetWitness Platform para aplicar el parche.
- Si el servidor de NetWitness no tiene conexión a Internet con Servicios de Live, es posible usar la interfaz de la línea de comandos (CLI) para aplicar el parche.

Tareas de actualización

Tarea 1: Deshabilitar los servicios de Decoder

Antes de actualizar a 11.2.0.1, debe deshabilitar AutoStart de la captura en los servicios Network Decoder y Network Hybrid.

Para deshabilitar el campo AutoStart de la captura:

1. Vaya a **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione un servicio Network Decoder o Network Hybrid y elija  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios para el Network Decoder o el Network Hybrid seleccionados.
3. En el panel **Configuración de Decoder**, deseleccione el campo **AutoStart de la captura** y haga clic en **Aplicar**.

Tarea 2: Actualizar el parche

Puede elegir uno de los siguientes métodos de actualización en función de la conexión a Internet.

Método en línea (conexión a Servicios de Live): Actualización mediante la interfaz del usuario de NetWitness

Puede usar este método si el Servidor de NetWitness está conectado a los Servicios de Live y se puede obtener el paquete.

Nota: Está disponible una actualización de 11.1.0.3 a 11.2.0.1 mediante el método en línea. Si está actualizando de 11.1.0.x a 11.2.0.1, primero debe actualizar a NetWitness Platform 11.2.0.0 y, a continuación, a 11.2.0.1.

Nota: Si el Servidor de NetWitness no tiene acceso a los Servicios de Live, use el Método offline (sin conexión a Servicios de Live): Actualización mediante la interfaz de la línea de comandos .

Requisitos previos

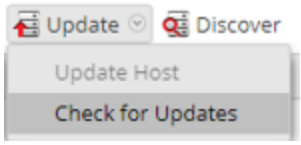
Asegúrese de:

1. La opción “Descargar automáticamente información acerca de actualizaciones nuevas cada día” debe estar seleccionada y aplicada en **ADMINISTRAR** > **Sistema** > **Actualizaciones** .
2. Debe ir a **ADMINISTRAR** > **Hosts** > **Actualizar** > **Buscar actualizaciones** para buscar actualizaciones. La página Host muestra el estado **Actualización disponible**.
3. 11.2.0.1 debe estar disponible en la columna “Versión de actualización”.

Nota: Si tiene certificados personalizados, transfiéralos desde el directorio `/etc/pki/nw/trust/import/` a `/root/cert`. Siga estos pasos para transferir los certificados:
1.) `mkdir /root/cert.`
2.) `mv /etc/pki/nw/trust/import/* /root/cert.`

Procedimiento

1. Vaya a **ADMINISTRAR** > **HOSTS**.
2. Seleccione el host del servidor de NetWitness (nw-server).
3. Busque las actualizaciones más recientes.



4. Se muestra Actualización disponible en la columna **Estado** si tiene una actualización de versión en el repositorio de actualización local para el host seleccionado.
5. Seleccione **11.2.0.1** en la columna **Versión de actualización**.
   Si:

- Desea ver un cuadro de diálogo con las principales funciones de la actualización e información sobre las actualizaciones, haga clic en el icono de información () a la derecha del número de versión de actualización.
- No puede encontrar la versión que desea, seleccione **Actualizar > Buscar actualizaciones** para buscar las actualizaciones disponibles en el repositorio. Si hay una actualización disponible, se muestra el mensaje "Están disponibles nuevas actualizaciones" y la columna **Estado** se actualiza automáticamente para mostrar Actualización disponible. De forma predeterminada, solo se muestran las actualizaciones compatibles para el host seleccionado.

6. Haga clic en **Actualizar** > **Actualizar host** en la barra de herramientas.
7. Haga clic en **Iniciar actualización**.
8. Haga clic en **Reiniciar host**.
9. Repita los pasos del 6 al 8 para otros hosts.

Nota: Puede seleccionar varios hosts para actualizar a la vez únicamente después de actualizar y reiniciar el servidor de NetWitness Admin. Todos los hosts de ESA, Endpoint Insights y Malware Analysis se deben actualizar a la misma versión que la del servidor de NW Admin o servidor de NetWitness Admin.

Nota: No todos los componentes se cambiaron para 11.2.0.1. Por lo tanto, después de realizar los pasos de actualización, es normal ver algunos componentes con números de versión distintos. Para obtener una lista de los componentes que se actualizaron para esta versión, consulte Números de compilación.

Método offline (sin conexión a Servicios de Live): Actualización mediante la interfaz de la línea de comandos

Puede usar este método si el Servidor de NetWitness no está conectado a los Servicios de Live.

Requisitos previos

Asegúrese de:

- Haber descargado el siguiente archivo, que contiene todos los archivos de actualización de NetWitness Platform 11.2.0.1, desde RSA Link (https://community.rsa.com/) > NetWitness Platform > RSA NetWitness Logs and Network > Downloads > RSA Dowloads a un directorio local: `netwitness-11.2.0.1.zip`

Procedimiento

Debe realizar los pasos de actualización para los servidores de NW Admin y para los servidores de componentes.

Nota: Si está actualizando de 11.1.0.3 a 11.2.0.1, debe descargar los archivos de NetWitness Platform 11.2.0.0, netwitness-11.2.0.0.zip, y configurarlos en la carpeta de almacenamiento provisional junto con los archivos de 11.2.0.1. Si está actualizando de 11.1.0.x a 11.2.0.1, primero debe actualizar a NetWitness Platform 11.2.0.0 y, a continuación, a 11.2.0.1.

Nota: Si copia y pega los comandos desde el archivo PDF al terminal del protocolo SSH de Linux, los caracteres no funcionarán. Se recomienda escribirlos.

1. Almacene provisionalmente 11.2.0.1 mediante la creación de un directorio en el servidor de NetWitness en `/tmp/upgrade/11.2.0.1` y extraiga el paquete zip.
   `unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1`

   Nota: Si copió el archivo .zip al directorio de almacenamiento provisional creado para descomprimirlo, asegúrese de eliminar el archivo .zip inicial que copió en la ubicación de almacenamiento provisional después de extraerlo.

2. Inicialice la actualización mediante el siguiente comando:
   `upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade`
3. Actualice el servidor de NetWitness mediante el siguiente comando:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.0.1`
4. Cuando la actualización del host de componentes se realice correctamente, reinicie el host desde la interfaz del usuario de NetWitness.
5. Repita los pasos 3 y 4 para cada host de componentes, pero cambie la dirección IP a la del host de componentes que se actualiza.

Nota: Puede comprobar las versiones de todos los hosts mediante el comando `upgrade-cli-client --list` en el servidor de NetWitness. Si desea ver el contenido de la ayuda de `upgrade-cli-client`, utilice el comando `upgrade-cli-client --help`.

Nota: Si aparece el siguiente error durante el proceso de actualización:

```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```

el parche se instalará correctamente. No se necesita realizar ninguna otra acción. Si se producen errores adicionales durante la actualización de un host a una nueva versión, póngase en contacto con el servicio al cliente (Contacto con atención al cliente).

Instrucciones para el repositorio externo para la actualización mediante la CLI

Nota: El repositorio externo que se va a configurar debe tener el repositorio de 11.2.0.1 configurado en el mismo directorio que 11.2.0.0.

1. Almacene provisionalmente 11.2.0.1 mediante la creación de un directorio en el servidor de NetWitness en `/tmp/upgrade/11.2.0.1` y extraiga el paquete zip.
   `unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1`

   Nota: Si copió el archivo .zip al directorio de almacenamiento provisional creado para descomprimirlo, asegúrese de eliminar el archivo .zip inicial que copió en la ubicación de almacenamiento provisional después de extraerlo.

2. Inicialice la actualización mediante el siguiente comando:
   `upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade`
3. Actualice el servidor de NetWitness mediante el siguiente comando:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.0.1`
4. Cuando la actualización del host de componentes se realice correctamente, reinicie el host desde la interfaz del usuario de NetWitness.
5. Repita los pasos 3 y 4 para cada host de componentes, pero cambie la dirección IP a la del host de componentes que se actualiza.

Nota: Puede comprobar las versiones de todos los hosts mediante el comando `upgrade-cli-client --list` en el servidor de NetWitness. Si desea ver el contenido de la ayuda de `upgrade-cli-client`, utilice el comando `upgrade-cli-client --help`.

Nota: Si aparece el siguiente error durante el proceso de actualización:

```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```

el parche se instalará correctamente. No se necesita realizar ninguna otra acción. Si se producen errores adicionales durante la actualización de un host a una nueva versión, póngase en contacto con el servicio al cliente (Contacto con atención al cliente).

Tareas posteriores a la actualización

Tarea 1 (opcional): Transferir los certificados personalizados

Transfiera los certificados personalizados del directorio externo al directorio `/etc/pki/nw/trust/import`.

Tarea 2 (condicional): Reconfigurar la autenticación de Radius en PAM

Si configuró la autenticación de Radius en PAM en 11.2.x.x con el paquete `pam_radius`, debe reconfigurarla en 11.2.0.1 mediante el paquete `pam_radius_auth`.

Debe ejecutar los siguientes comandos en el servidor de NW en cual reside el servidor de Admin.

Nota: Si configuró `pam_radius` en 11.x.x.x, realice los siguientes pasos para desinstalar la versión existente, o bien, puede continuar con el paso 2.

Paso 1: Verifique la página existente y desinstale `pam_radius` existente

```
rpm -qi |grep pam_radius
yum erase pam_radius
```

Paso 2: Para instalar el paquete `pam_radius_auth` , ejecute el siguiente comando

```
yum install pam_radius_auth
```

Paso 3: Edite el archivo de configuración de RADIUS `/etc/raddb/server` como se indica a continuación y agregue las configuraciones para el servidor de RADIUS:

```
# server[:port] shared_secret timeout (s)
server secret 3
```

Por ejemplo, 111.222.33.44 secret 1

Paso 4: Edite el archivo de configuración de NetWitness Server PAM `/etc/pam.d/securityanalytics` para agregar la siguiente línea. Si el archivo no existe, créelo y agregue la siguiente línea:

```
auth sufficient pam_radius_auth.so
```

Paso 5: Proporcione el permiso de escritura para los archivos `/etc/raddb/server` mediante el siguiente comando

```
chown netwitness:netwitness /etc/raddb/server
```

Paso 6: Para copiar la biblioteca de `pam_radius_auth`, ejecute el siguiente comando

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```

Paso 7: Reinicie el servidor jetty después de realizar los cambios en las configuraciones de `pam_radius_auth`. Ejecute el siguiente comando.

```
systemctl restart jetty
```

Tarea 3: Reiniciar el servidor de Respond

Reinicie el servidor de Respond:

```
systemctl restart rsa-nw-respond-server
```

Tarea 4: Actualizar la ubicación del controlador 10G

Debe actualizar el controlador 10G en la ubicación correcta en el kernel actual.

Paso 1: Si está utilizando el Decoder 10G, ejecute los siguientes comandos después de la actualización a 11.2.0.1 y reinicie el dispositivo Decoder. Haga clic en **Y** cuando se le solicite confirmar la sobrescritura.

- cp /var/lib/dkms/ixgbe-zc/5.3.7.14/$(uname -r)/x86_64/module/ixgbe_zc.ko.xz /lib/modules/$(uname -r)/extra/
- cp /var/lib/dkms/i40e-zc/2.4.6.14/$(uname -r)/x86_64/module/i40e_zc.ko.xz /lib/modules/$(uname -r)/extra/
- `cp /var/lib/dkms/pfring/6.5.0.14/$(uname -r)/x86_64/module/pf_ring.ko.xz /lib/modules/$(uname -r)/extra/`

Paso 2: Si deshabilitó el campo **AutoStart de la captura**, como se mencionó en Tarea 1: Deshabilitar los servicios de Decoder, debe volver a habilitar **AutoStart de la captura** en los servicios Network Decoder y Network Hybrid.

Para habilitar el campo AutoStart de la captura:

1. Vaya a **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione un servicio Network Decoder o Network Hybrid y elija  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios para el Network Decoder o el Network Hybrid seleccionados.
3. En el panel **Configuración de Decoder**, seleccione el campo **AutoStart de la captura** y haga clic en **Aplicar**.

Documentación del producto

Con esta versión se proporciona la siguiente documentación.

Documento	Ubicación
Documentación en línea de RSA NetWitness Platform 11.2.0.0	https://community.rsa.com/community/products/netwitness/112

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

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

RSA Link	https://community.rsa.com/
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/rsa-customer-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.

Preparación para ponerse en contacto con el servicio 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.

Historial de revisiones

Revisión	Fecha	Descripción
0.1	25/10	Versión preliminar final