RSA NETWITNESS® SUITE

Guía de actualización

para la versión 11.0.x a 11.1

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 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.

julio 2018

Contenido

Introducción

RSA NetWitness® Suite11.1.0.0 proporciona reparaciones para todos los productos de la suite. Los componentes de la suite son Servidor de NetWitness (servidor de Admin, servidor de Config, servidor de Integration, servidor de Investigate, servidor de Orchestration, servidor de Respond y servidor de Security), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA primario, ESA secundario, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector y Workbench.

Nota: Reporting Engine se instala en el host del servidor de NW, Workbench se instala en el host de Archiver y Warehouse Connector se puede instalar en el host de Decoder o el host de Log Decoder.

Las instrucciones de esta guía se aplican a los hosts físicos y virtuales (que incluyen nube pública de AWS y Azure), salvo que se indique lo contrario.

Ruta de actualización

Las siguientes rutas de actualización son compatibles con NetWitness Suite 11.1.0.0:

- 11.0.0.0 a 11.1.0.0
- 11.0.0.1 a 11.1.0.0
- 11.0.0.2 a 11.1.0.0
- 10.6.5.x a 11.1.0.0

  Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

  Consulte la *Guía de actualización de hosts físicos de RSA NetWitness Suite 10.6.5.x a 11.1* y la *Guía de actualización de hosts virtuales de RSA NetWitness Suite 10.6.5.x a 11.1* para obtener instrucciones sobre cómo actualizar de 10.6.5.x a 11.1.0.0.

Ejecución en modo mixto

La ejecución en modo mixto se produce cuando se actualizan algunos de los servicios a la versión más reciente y algunos todavía están en las versiones anteriores. Consulte “Ejecución en modo mixto” en la *Guía de introducción de hosts y servicios de RSA NetWitness Suite* para obtener más información.

Tareas de preparación para la actualización

Complete las siguientes tareas para preparar la actualización a NetWitness Suite 11.1.0.0. Estas tareas se organizan en las siguientes categorías.

General

Tarea 1: Revisar los puertos principales y abrir los puertos del firewall

En las siguientes tablas se enumeran los puertos nuevos en 11.1.0.0.

Precaución: Asegúrese de que los puertos nuevos se implementen y se prueben antes de actualizar, de modo que la actualización no falle debido a la falta de puertos.

Endpoint Hybrid o Endpoint Log Hybrid

Host de origen	Host de destino	Puertos de destino	Comentarios
Endpoint Hybrid o Endpoint Log Hybrid	Servidor de NW	TCP 5672	Bus de mensajes
Servidor de Endpoint	Servidor de NW	TCP 27017	MongoDB

Tarea 2: Respaldar el archivo de configuración de Malware Analysis en otro directorio

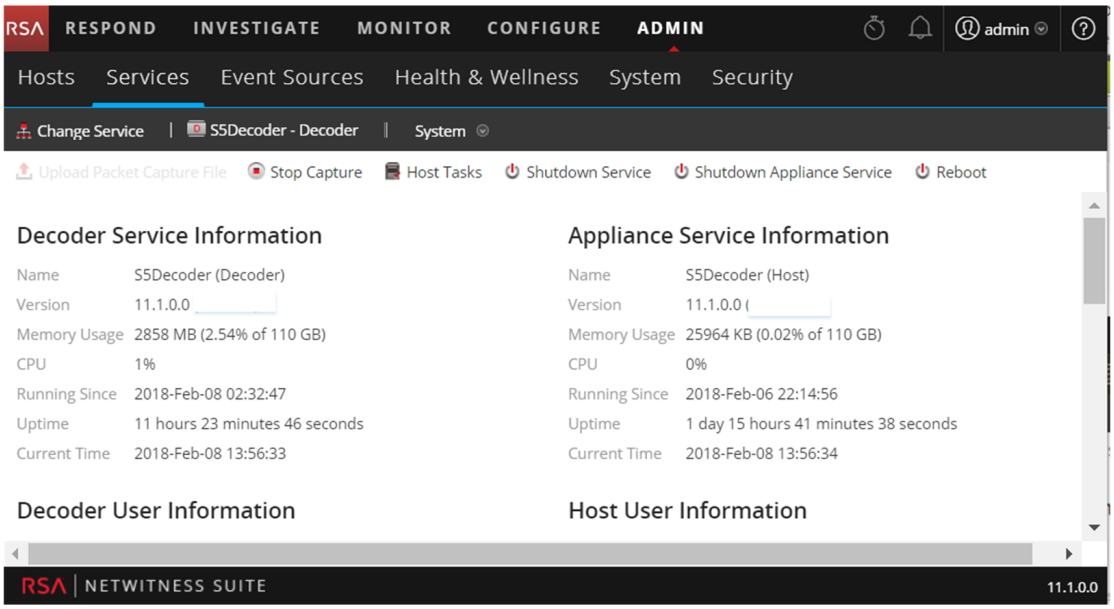
1. Realice un respaldo de los siguientes archivos en otro directorio seguro.
   `/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`
   Debe recuperar los valores de parámetros personalizados desde este respaldo después de actualizar el host de Malware Analysis a 11.1.0.0. La actualización crea un archivo de configuración nuevo con todos los parámetros configurados en los valores predeterminados.
2. Elimine el siguiente archivo.
   `/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`

Tarea 3: Detener la captura y la agregación de datos

Detener la captura de paquetes

Para detener la captura de paquetes:

1. Inicie sesión en NetWitness Suite 11.0.x y vaya a **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione cada servicio **Decoder**.



3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en 

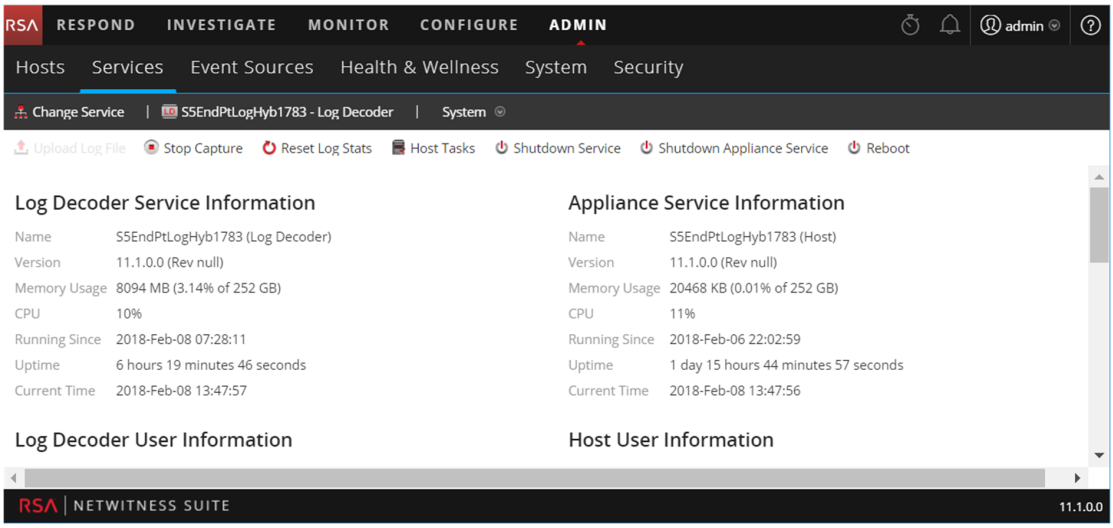
.

Detener la captura de registros

Para detener la captura de registros:

1. Inicie sesión en NetWitness Suite 11.0.x y vaya a **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios.

2. Seleccione cada servicio **Log Decoder**.



3. En  (acciones), seleccione **Ver** > **Sistema**.

4. En la barra de herramientas, haga clic en  .

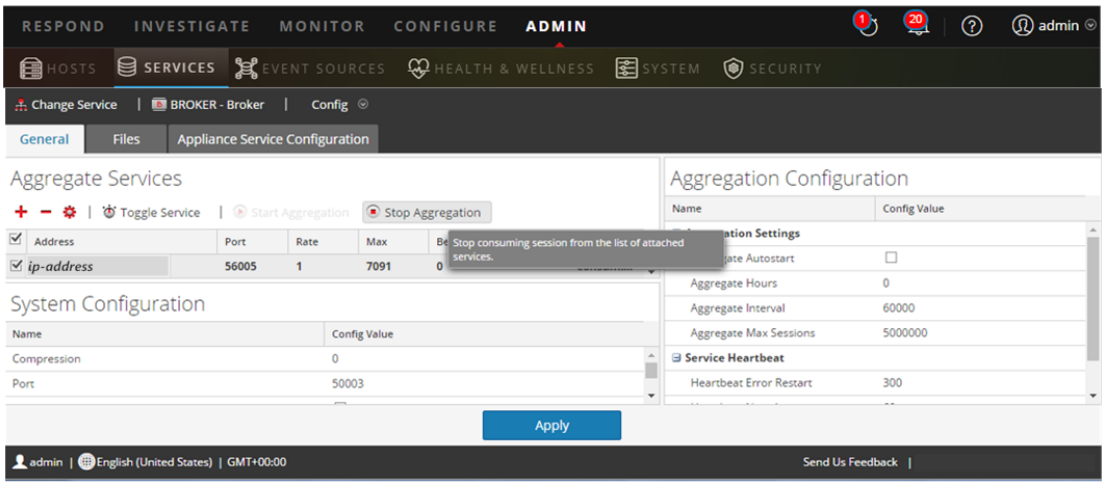
Detener agregación

1. Inicie sesión en NetWitness Suite 11.0.x y vaya a **ADMINISTRAR** > **Servicios**.

2. Seleccione el servicio **Broker**.

3. En  (acciones), seleccione **Ver** > **Configuración**.

4. Se muestra la pestaña **General**.



5. En **Servicios agregados** haga clic en  .

Tarea 4: Asegurarse de que la información de identificación de `deploy_admin` siga siendo válida (no esté vencida)"

La información de identificación de `deploy_admin` debe ser válida (no estar vencida) para actualizar a 11.1.

Parte I. Verificar el estado de vencimiento de la información de identificación de `deploy_admin`

Realice el siguiente procedimiento para determinar si la información de identificación de `deploy_admin` está vencida.

1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**.
2. Asegúrese de que `deploy_admin` no esté vencida.
   - Si aún es válida, puede continuar con la actualización.
   - Si está vencida, realice la Parte II de esta tarea.

(Condicional) Parte II. Restablecer la información de identificación de `deploy_admin` vencida

Realice el siguiente procedimiento para restablecer la información de identificación de `deploy_admin` vencida.

1. Seleccione `deploy_admin` y haga clic en **Restablecer contraseña**.
2. (Condicional) Si NetWitness Suite le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos.
   a. Ingrese la contraseña de `deploy_admin` vencida.
   b. Deseleccione la casilla de verificación Forzar cambio de contraseña en el próximo inicio de sesión.
   c. Haga clic en **Guardar**.
3. (Condicional) Si NetWitness Suite no le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo Restablecer contraseña, realice los siguientes pasos.
   a. Restablezca `deploy_admin` para utilizar una contraseña nueva.
   b. En todos los hosts del servidor de NW y en todos los demás hosts en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` nueva.
   `/opt/rsa/saTools/bin/set-deploy-admin-password`
   c. En el host en el cual falló la instalación/coordinación, ejecute nwsetup-tui y use la contraseña de `deploy_admin` nueva.

Reporting Engine

Tarea 5: Configurar Reporting Engine para los gráficos de uso inmediato

Para que los gráficos de uso inmediato se ejecuten después de la actualización, debe configurar el origen de datos predeterminado en la página Configuración de Reporting Engine antes de ejecutar la actualización. Si no ejecuta esta tarea, debe configurar manualmente el origen de datos después de la actualización. Para obtener más información sobre los orígenes de datos de Reporting Engine, consulte la *Guía de configuración de Reporting Engine de NetWitness Suite 11.1*. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

En este punto, puede continuar con las instrucciones de actualización.

Respond

Tarea 6: (Condicional) Restaurar las claves personalizadas del servicio Respond

Si agregó claves personalizadas en `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` para su uso en la cláusula groupBy en 11.0, copie y guarde las claves personalizadas en un archivo.

Tarea 7: Restaurar scripts de normalización del servicio Respond personalizados

Los scripts de normalización del servicio Respond refactorizados de RSA se almacenan en el directorio `/var/lib/netwitness/respond-server/scripts` en 11.1.0.0. Debe respaldarlos en 11.0.x antes de actualizar a 11.1.0.0, de modo que pueda restaurarlos en 11.1.0.0 como se describe en Tareas posteriores a la actualización de Respond.

1. Vaya al directorio `/var/lib/netwitness/respond-server/scripts`.
2. Respalde los siguientes archivos:

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_wtd_alerts.js
utils.js
```

3. (Condicional) Si agregó alguna lógica personalizada en 11.0.x o en alguna versión anterior, copie y guarde esta lógica de los scripts respaldados, de modo que pueda restaurarla en 11.1.0.0.

Tarea 8: (Condicional; para Azure Stack)

Completar el repositorio con los paquetes adicionales.

1. Si utiliza un repositorio local, extraiga el archivo zip de Azure mediante los siguientes pasos en el servidor de Admin:

a. Ejecute como raíz: `mkdir -p /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

b. Descomprima en el directorio anterior: `unzip nw-azure-11.1-extras.zip -d /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

2. Si está utilizando un repositorio externo, siga estos pasos:

a. Después de configurar el contenido de 11.1.0.0 en el repositorio externo, descomprima nw-azure-11.1-extras.zip en la carpeta <base-directory>11.1.0.0/OS/other del directorio del repositorio externo.

b. Ejecute createrepo desde el directorio 11.1.0.0/OS del repositorio externo.

Tareas de actualización

Complete las siguientes tareas para preparar la actualización de NetWitness Suite 11.0.x.x a 11.1.0.0.

Puede usar dos métodos para aplicar actualizaciones de versión a un host.

Nota: Si planea usar un repositorio de actualización (repositorio) para NetWitness Suite 11.1.0.0 que sea distinto al repositorio ahora tiene configurado para 11.0.x.x, consulte Apéndice C. Configurar un repositorio externo para obtener instrucciones.

- Aplicar actualizaciones desde la vista Hosts (acceso a la Web)
- Aplicar una actualización desde la línea de comandos (sin acceso a la Web)

Aplicar actualizaciones desde la vista Hosts (acceso a la Web)

Existen dos tareas que debe realizar para aplicar las actualizaciones desde la vista Hosts:

- Tarea 1. Completar el repositorio local o configurar un repositorio externo: Asegúrese de tener las actualizaciones de versión más recientes.
- Tarea 2. Aplicar actualizaciones desde la vista Hosts a cada host.

Tarea 1. Completar el repositorio local o configurar un repositorio externo

Cuando configura el servidor de NW en 11.1.0.0, debe seleccionar el repositorio local o un repositorio externo. La vista Hosts recupera las actualizaciones de versión desde el repositorio que se selecciona.

Si seleccionó el repositorio local, no es necesario configurarlo, pero debe asegurarse de que se complete con las actualizaciones de versión más recientes. Consulte Apéndice B. Completar el repositorio local para obtener instrucciones sobre cómo completarlo con la actualización de versión.

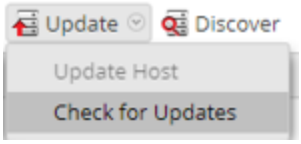
Si seleccionó un repositorio externo, debe configurarlo. Consulte Apéndice C. Configurar un repositorio externo para obtener instrucciones sobre cómo configurar un repositorio externo.

Tarea 2. Aplicar actualizaciones desde la vista Hosts a cada host

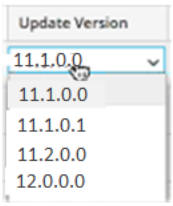
En la vista Hosts se muestran las actualizaciones de versiones de software disponibles en el repositorio de actualización local y se le permite elegir y aplicar las actualizaciones que desea.

En este procedimiento se indica cómo actualizar un host a una versión nueva de NetWitness Suite.

1. Inicie sesión en NetWitness Suite.
2. Vaya a **ADMIN > HOSTS**.
3. (Condicional) Busque las actualizaciones más recientes.



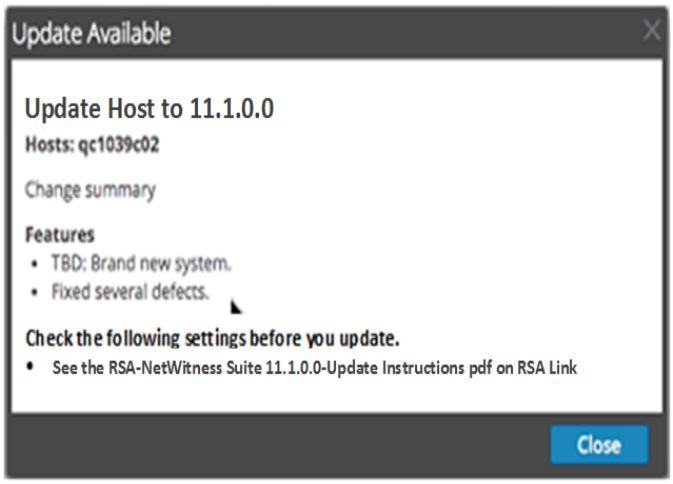
4. Seleccione uno o más hosts.
   En primer lugar, debe actualizar el servidor de NW a la versión más reciente. Puede actualizar los demás hosts en la secuencia que prefiera, pero RSA recomienda seguir las reglas que aparecen en "Ejecución en modo mixto" en la *Guía de introducción de hosts y servicios de RSA NetWitness Suite* para obtener más información.
   Se muestra Actualización disponible en la columna **Estado** si tiene una actualización de versión en el repositorio de actualización local para los hosts seleccionados.
5. Seleccione la versión que desea aplicar en la columna **Versión de actualización**.



   Si:

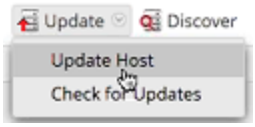
   - Si desea actualizar más de un host a esa versión, después de actualizar el host de servidor de NW, seleccione la casilla de verificación a la izquierda de los hosts. Solo se enumeran las versiones de actualización compatibles actualmente.
   - Desea ver un cuadro de diálogo con las principales funciones de la actualización e información sobre las actualizaciones, haga clic en el icono de información ( ) a la derecha del número de versión de actualización. El siguiente es un ejemplo de este cuadro

de diálogo.

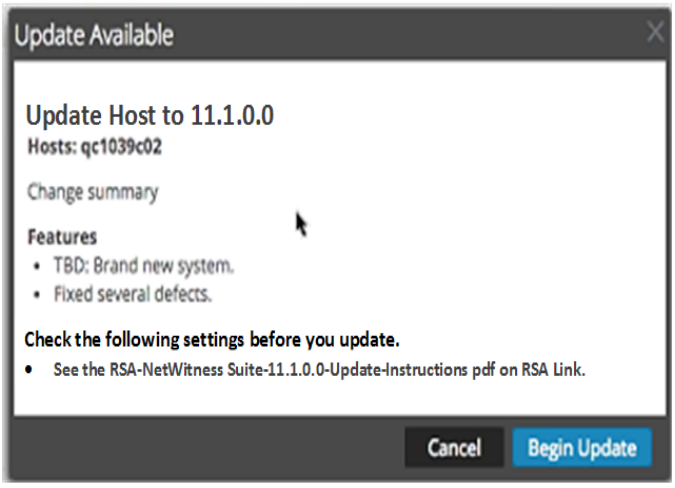


- No puede encontrar la versión que desea, seleccione **Actualizar > Buscar actualizaciones** para buscar las actualizaciones disponibles en el repositorio. Si hay una actualización disponible, se muestra el mensaje "Están disponibles nuevas actualizaciones" y la columna **Estado** se actualiza automáticamente 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.



Se muestra un cuadro de diálogo con información sobre la actualización seleccionada. Haga clic en **Iniciar actualización**.



En la columna **Estado** se indica lo que está sucediendo en cada una de las siguientes etapas

de la actualización:

- Etapa 1: **Descargando paquetes de actualización**: Descarga al servidor de NW los artefactos del repositorio que se aplican a los servicios en el host que eligió.
- Etapa 2: **Configurando los paquetes de actualización**: Configura los archivos de actualización en el formato correcto.
- Etapa 3: **Actualización en curso**: Actualiza el host a la nueva versión.

7. Cuando vea **Actualización en curso**, actualice el navegador.
   Esto puede hacer que se dirija a la pantalla Iniciar sesión de NetWitness. Si esto sucede, inicie sesión y regrese a la vista Host.
   Después de la actualización del host, NetWitness Suite le solicita que ejecute la acción **Reiniciar host**.
8. Haga clic en **Reiniciar host** en la barra de herramientas.
   NetWitness Suite muestra el estado como **Reiniciando…** hasta que el host vuelve a estar en línea. Una vez que el host vuelve a estar en línea, en **Estado** se muestra **Actualizado**.
   Póngase en contacto con Atención al cliente si el host no vuelve a estar en línea.

Nota: Si la STIG de la DISA está habilitada, la apertura de los servicios principales puede tardar aproximadamente entre cinco y 10 minutos. La generación de los nuevos certificados es la causa de este retraso.

Aplicar actualizaciones desde la línea de comandos (sin acceso a la Web)

Si su implementación de RSA NetWitness Suite no tiene acceso a la Web, realice el siguiente procedimiento para aplicar una actualización de versión.

1. Descargue el paquete de actualización de `.zip` correspondiente a la versión que desea (por ejemplo, `netwitness-11.1.0.0.zip`) desde RSA Link a un directorio local.
2. Acceda mediante el protocolo SSH al host del servidor de NW.
3. Cree un directorio de almacenamiento provisional `tmp/upgrade/<version>` para la versión que desea (por ejemplo, `tmp/upgrade/11.1.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.1.0.0
   ```
4. Descomprima el paquete en el directorio de almacenamiento provisional que creó (por ejemplo, `tmp/upgrade/11.1.0.0`).
   ```
   cd /tmp/upgrade/11.1.0.0
   unzip /tmp/upgrade/11.1.0.0/netwitness-11.1.0.0.zip
   ```
5. Inicialice la actualización en el servidor de NW.
   ```
   upgrade-cli-client --init --version 11.1.0.0 --stage-dir
   /tmp/upgrade/
   ```
6. Aplique la actualización al servidor de NW.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version
   11.1.0.0
   ```
7. Inicie sesión en NetWitness Suite y reinicie el host del servidor de NW en la vista Host.
8. Aplique la actualización a cada uno de los hosts de servidores que no son de NW.
   ```
   upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> -
   -version 11.1.0.0
   ```
   La actualización está completa cuando finaliza el sondeo.
9. Inicie sesión en NetWitness Suite y reinicie el host en la vista Host.
   Puede verificar la versión que se aplicó al host mediante el siguiente comando:
   ```
   upgrade-cli-client --list
   ```

Actualizar o instalar la recopilación de Windows existente

Consulte la *Guía de recopilación de Windows existente de RSA NetWitness*. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Nota: Después de actualizar o instalar la recopilación de Windows existente, reinicie el sistema para asegurar el correcto funcionamiento de la recopilación de registros.

Tareas posteriores a la actualización

Complete las siguientes tareas después de la actualización a NetWitness Suite 11.1.0.0.

General

Estas tareas se aplican a todos los clientes de NetWitness Suite 11.1.0.0.

Tarea 1: Iniciar la captura y la agregación de datos

Reinicie la captura y la agregación de paquetes y registros después de la actualización a 11.1.0.0.

Iniciar la captura de paquetes

Para iniciar la captura de paquetes:

1. En el menú **NetWitness Suite**, seleccione **ADMIN** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione cada servicio **Decoder**.
3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en 

.

Iniciar la captura de registros

Para iniciar la captura de registros:

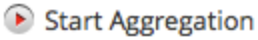
1. En el menú **NetWitness Suite**, seleccione **ADMIN** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione cada servicio **Log Decoder**.

3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en 

.

Iniciar agregación

Para iniciar agregación:

1. En el menú **NetWitness Suite**, seleccione **ADMIN** > **Servicios**.
   Se muestra la vista Servicios.
2. Para cada servicio Concentrator y Broker.
   a. Seleccione el servicio
   .
   b. En  (acciones), seleccione **Ver** > **Configuración**.
   c. En la barra de herramientas, haga clic en 

.

Servidor de NW

Tarea 2: (Condicional) Corregir las plantillas del registro de auditoría que no están actualizadas en el archivo de configuración de salida de Logstash

Problema: Cuando un usuario actualiza de 11.0.0.0 a 11.1.0.0, si está configurada una auditoría global, las plantillas del registro de auditoría no se actualizan en el archivo de configuración de salida de Logstash.

Solución alternativa: Si la auditoría global está configurada, debe editar una de las entradas de syslog en los servidores de notificaciones globales y hacer clic en Guardar para aplicar la configuración del registro de auditoría más reciente.

Si la auditoría global estaba configurada en 11.0.x, debe completar el siguiente procedimiento para aplicar la configuración de la auditoría global más reciente.

1. En el menú de **NetWitness Suite**, seleccione **ADMINISTRAR** > **Sistema** > **Notificaciones globales**.
   Se muestra la vista **Notificaciones globales**.
2. Haga clic en la pestaña **Servidores** y seleccione cualquier servidor de syslog.
3. Haga clic en  (icono de edición) y, a continuación, haga clic en **Guardar**.

(Condicional) Tarea 3: Reconfigurar la autenticación de Radius en PAM

Si configuró la autenticación de Radius en PAM en 11.0.x.x con el paquete `pam_radius`, debe reconfigurarla en 11.1.0.0 mediante el `pam_radius_auth package` para lograr un mejor rendimiento. Para obtener instrucciones, consulte "Configurar la funcionalidad de inicio de sesión PAM" en la *Guía de administración de usuarios y de la seguridad del sistema de RSA NetWitness® Suite 11.1*. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

RSA NetWitness® Endpoint

Tarea 4: Reconfigurar un feed recurrente configurado desde Endpoint heredado debido a un cambio en la versión de Java

Debe reconfigurar el feed recurrente de Endpoint heredado debido al cambio de la versión de Java. Realice el siguiente paso para corregir este problema.

- Importe el certificado de CA de NetWitness Endpoint en el almacén de confianza de NetWitness Suite, como se describe en "Exportar el certificado SSL de NetWitness

Endpoint" en el tema "Configurar datos contextuales desde Endpoint a través de un feed recurrente" de la *Guía de integración de RSA NetWitness Endpoint 11.1* para importar el certificado.

Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

RSA NetWitness® Endpoint Insights

(Opcional) Tarea 5: Instalar Endpoint Hybrid o Endpoint Log Hybrid

Consulte:

Guía de instalación de hosts físicos de RSA NetWitness Suite 11.1 para obtener instrucciones acerca de la instalación en un host físico.

Guía de instalación de hosts virtuales de RSA NetWitness Suite 11.1 para obtener instrucciones acerca de la instalación en un host virtual.

Event Stream Analysis

Estas tareas se aplican a todos los clientes de NetWitness Suite 11.1.0.0 que usan Event Stream Analysis.

(Condicional) Tarea 6: Reconfigurar la regla de agregación "Comunicación de comando y control sospechosa por dominio" para la detección de amenazas automatizadas

En 11.0, la condición Agrupar por "Dominio para Sospecha de C&C" de la regla de agregación "Comunicación de comando y control sospechosa por dominio" no funcionaba como se esperaba y se tuvo que cambiar a "Dominio" para agregar alertas y habilitar los incidentes que se crearán para "Sospecha de C&C". La condición "Dominio para Sospecha de C&C" funciona correctamente en 11.1.0.0 y se debe usar como la condición Agrupar por para la regla de agregación "Comunicación de comando y control sospechosa por dominio" (como regla de incidentes en 11.1.0.0).

Si cambió la condición Agrupar por de la regla de agregación "Comunicación de comando y control sospechosa por dominio" a "Dominio" para 11.0, deberá cambiarla de nuevo a "Dominio para Sospecha de C&C" para 11.1.0.0.

1. Inicie sesión en NetWitness Suite 11.1.0.0.
2. Vaya a **CONFIGURAR** > **Reglas de incidentes**.

3. En la lista Reglas de incidentes, busque la regla Comunicación de comando y control sospechosa por dominio y haga clic en el vínculo del campo NOMBRE para abrirla.
4. En la sección Opciones de agrupación de la vista Detalles de regla de incidentes, configure el campo Agrupar por en Dominio para Sospecha de C&C y haga clic en Guardar.

Para obtener más información, consulte la Guía de Detección de amenazas automatizadas de NetWitness Suite y la

sección “Configurar ESA Analytics” de la Guía de configuración de NetWitness Suite ESA. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Respond

Tarea 7: (Condicional) Obtener la versión más reciente del esquema de la regla de agregación y restaurar todas las claves personalizadas del servicio Respond

Realice el siguiente procedimiento para obtener la versión más reciente del esquema de la regla de agregación y restaurar todas las claves personalizadas del servicio Respond.

1. Elimine el archivo `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`.
2. Reinicie el servidor de Respond para obtener la versión más reciente del archivo `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` .
   ```
   systemctl restart rsa-nw-respond-server
   ```
3. Si agregó claves personalizadas en el archivo `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` para su uso en la cláusula groupBy para 11.0, modifique el archivo `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` y agregue las claves personalizadas que guardó anteriormente como una tarea de preparación de la actualización.

Nota: Se agregaron nuevos campos Agrupar por a Respond en 11.1.0.0. Los nuevos campos Agrupar por no estarán visibles en la interfaz del usuario de NetWitness Suite si no obtiene la versión más reciente del archivo en el servidor.

Tarea 8: Obtener la versión más reciente de los scripts de normalización del servicio Respond y restaurar todos los scripts de normalización del servicio Respond personalizados

RSA refactorizó los scripts de normalización del servicio Respond en el directorio `/var/lib/netwitness/respond-server/scripts` en 11.1.0.0. Debe reemplazar las versiones anteriores.

Antes de la actualización a 11.1.0.0, respaldó los siguientes archivos del directorio `/var/lib/netwitness/respond-server/scripts` .

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_wtd_alerts.js
utils.js
```

Realice el siguiente procedimiento para obtener la versión más reciente de los scripts de normalización.

1. Después de respaldar los archivos mencionados anteriormente, elimine el directorio `/var/lib/netwitness/respond-server/scripts` y su contenido.
2. Reinicie el servidor de Respond.
   ```
   systemctl restart rsa-nw-respond-server
   ```
3. (Condicional) Edite los nuevos archivos para incluir cualquier lógica personalizada de los scripts 11.0 que se respaldaron.

Nota: Los siguientes archivos cambiaron con la versión 11.1.0.0:

```
normalize_alerts.js
normalize_core_alerts.js
normalize_ma_alerts.js
```

Tarea 9: Agregar permisos de configuración de notificaciones de Respond

Los permisos de configuración de notificaciones de Respond permiten que los administradores de Respond, los encargados de la privacidad de datos y los administradores del SOC accedan a Configuración de notificaciones de Respond (**CONFIGURAR** > **Notificaciones** de **Respond**), con lo que pueden enviar notificaciones por correo electrónico cuando se crean o se actualizan incidentes.

Para acceder a esta configuración, necesitará agregar permisos adicionales a las funciones de usuario incorporadas existentes de NetWitness Suite. También deberá agregar permisos a sus funciones personalizadas. Consulte el tema “Permisos de configuración de notificaciones de Respond” de la *Guía de configuración de NetWitness Respond*. Para obtener información detallada sobre los permisos de usuario, consulte la *Guía de administración de usuarios y de la seguridad del sistema*. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Tarea 10: Actualizar los valores de Agrupar por de las reglas de incidentes predeterminadas

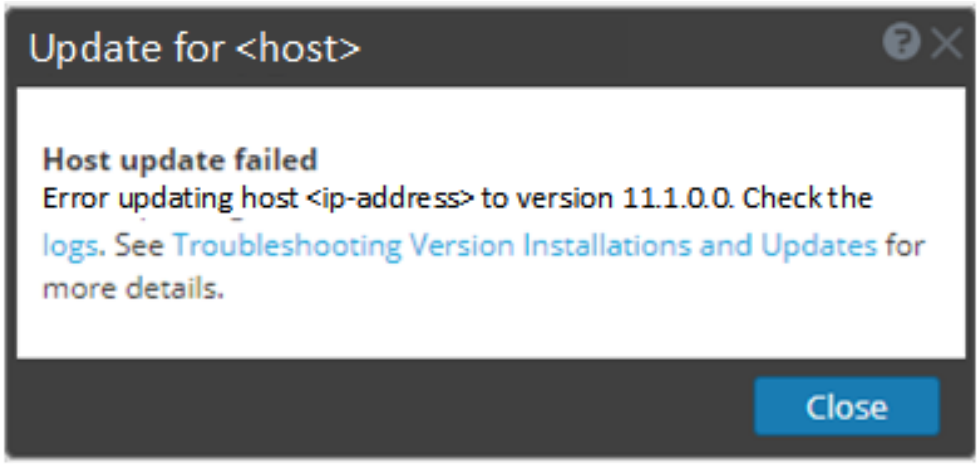
Ahora, cuatro de las reglas de incidentes predeterminadas utilizan “Dirección IP de origen” como el valor de Agrupar por. Para actualizar las reglas predeterminadas, cambie el valor de Agrupar por de las siguientes reglas predeterminadas a “Dirección IP de origen”:

- Alertas de alto riesgo: Reporting Engine
- Alertas de alto riesgo: Malware Analysis
- Alertas de alto riesgo: NetWitness Endpoint
- Alertas de alto riesgo: ESA

1. Vaya a **CONFIGURAR** > **Reglas de incidentes** y haga clic en el vínculo de la columna **Nombre** correspondiente a la regla que desea actualizar. Se muestra la vista Detalles de regla de incidentes.
2. En el campo **Agrupar por**, seleccione el nuevo valor de Agrupar por.
3. Haga clic en **Guardar** para actualizar la regla.

Apéndice A. Solución de problemas de instalaciones y actualizaciones de versión

En esta sección se describen los mensajes de error que se muestran en la vista **Hosts** cuando se producen problemas durante la actualización de versiones de hosts y la instalación de servicios en hosts en la vista **Hosts**. Si no puede resolver algún problema de actualización o instalación con los siguientes métodos de solución de problemas, póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

Mensaje de error	
Problema	Cuando selecciona una versión de actualización y hace clic en **Actualizar** > **Actualizar host**, el proceso de descarga se realiza correctamente, pero el proceso de actualización falla.

Solución	1. **Intente volver a aplicar la actualización de versión al host**.
	A menudo, esto es todo lo que debe hacer.
	2. Si aún no puede aplicar la actualización de versión nueva:
	a. Monitoree los siguientes registros en el servidor de NW a medida que avanza (por ejemplo, envíe la cadena de comandos `tail -f` desde la línea de comandos):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-`

`stacktrace.out`

El error aparecerá en uno o más de estos registros.

b. Intente solucionar el problema y vuelva a aplicar la actualización de versión.

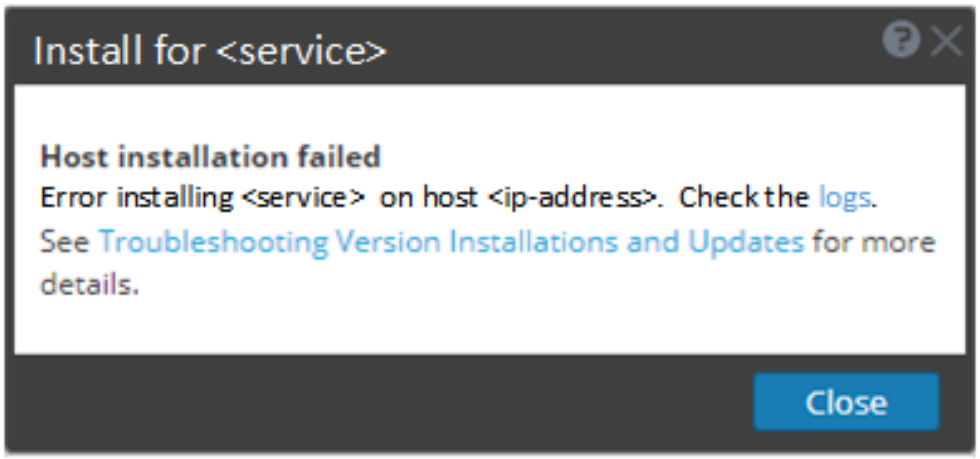
- Causa 1: La contraseña de `deploy_admin` venció.
  Solución: Restablezca su contraseña de `deploy_admin`.
  Realice los siguientes pasos para resolver la causa 1.

  1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**.
  2. Seleccione `deploy_admin` y haga clic en **Restablecer contraseña**.
  3. (Condicional) Si NetWitness Suite no le permite restablecer una contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos.
     a. Restablezca `deploy_admin` para utilizar una contraseña nueva.
     b. En todos los hosts de servidores que no son de NW en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` coincidente desde el host del servidor de NW.
     `/opt/rsa/saTools/bin/set-deploy-admin-password`

- Causa 2: La contraseña de `deploy_admin` se cambió en el host del servidor de NW, pero no se cambió en hosts de servidores que no son de NW.
  Realice el siguiente paso para resolver la causa 2.

  - En todos los hosts de servidores que no son de NW en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` coincidente desde el host del servidor de NW.
    `/opt/rsa/saTools/bin/set-deploy-admin-password`

3. Si aún no puede aplicar la actualización, reúna los registros del paso 2 y póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

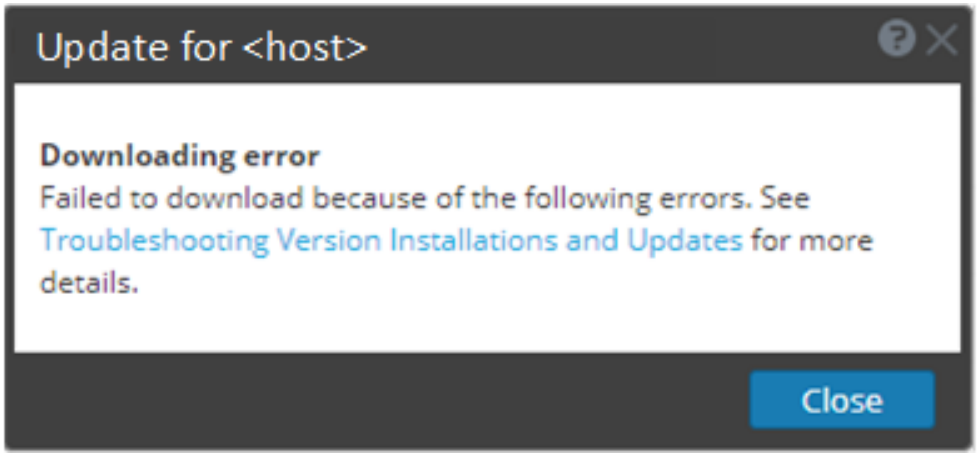
Mensaje de error	
Problema	Cuando selecciona un host y hace clic en **Instalar**, el proceso del servicio de instalación falla.

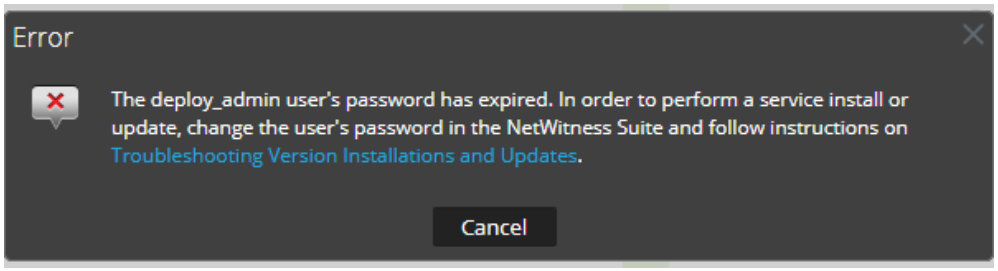
Solución	1. **Intente volver a instalar el servicio.**.
	A menudo, esto es todo lo que debe hacer.
	2. Si aún no puede instalar el servicio:
	a. Monitoree los siguientes registros en el servidor de NW a medida que avanza (por ejemplo, envíe la cadena de comandos `tail -f` desde la línea de comandos):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	El error aparecerá en uno o más de estos registros.
	b. Intente solucionar el problema y reinstale el servicio.
	• Causa 1: Se ingresó una contraseña de `deploy_admin` incorrecta en nwsetup-tui.
	Solución: Recupere su contraseña de `deploy_admin` .
	Realice los siguientes pasos para resolver la causa 1.
	1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**.

2. Seleccione `deploy_admin` y haga clic en **Restablecer contraseña**.
3. (Condicional) Si NetWitness Suite no le permite restablecer una contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos.
   a. Acceda mediante el protocolo SSH al host del servidor de NW.
   ```
   security-cli-client --get-config-prop --prop-hierarchy
   nw.security-client --prop-name
   platform.deployment.password –quiet
   ```
   b. Acceda mediante el protocolo SSH al host en el cual falló la instalación/coordinación.
   c. Vuelva a ejecutar nwsetup-tui con el uso de la contraseña de `deploy_admin` correcta.

- Causa 2: La contraseña de `deploy_admin` venció.
  Realice el siguiente paso para resolver la causa 2.
  1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**.
  2. Seleccione `deploy_admin` y haga clic en **Restablecer contraseña**.
  3. (Condicional) Si NetWitness Suite le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos.
     a. Ingrese la contraseña de `deploy_admin` vencida.
     b. Deseleccione la casilla de verificación Forzar cambio de contraseña en el próximo inicio de sesión.
     c. Haga clic en **Guardar**.
  4. (Condicional) Si NetWitness Suite no le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo Restablecer contraseña, realice los siguientes pasos.
     a. Restablezca `deploy_admin` para utilizar una contraseña nueva.
     b. En todos los hosts del servidor de NW y en todos los demás hosts en 11.x, ejecute el siguiente comando con el uso de la

	contraseña de `deploy_admin` nueva. `/opt/rsa/saTools/bin/set-deploy-admin-password` c. En el host en el cual falló la instalación/coordinación, ejecute nwsetup-tui y use la contraseña de `deploy_admin` nueva. 3. Si aún no puede aplicar la actualización, reúna los registros del paso 2 y póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

Mensaje de error	
Problema	Cuando selecciona una versión de actualización y hace clic en **Actualizar** >**Actualizar host**, la descarga comienza, pero no se completa.
Causa	Los archivos de descarga de versiones pueden ser grandes y su descarga puede tardar mucho tiempo. Si se producen problemas de comunicación durante la descarga, esta fallará.
Solución	1. Intente volver a descargarlo. 2. Si la descarga continúa fallando, intente descargarlo fuera de NetWitness Suite, como se describe en Aplicar actualizaciones desde la línea de comandos (sin acceso a la Web). 3. Si aún no puede descargar el archivo de actualización, póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

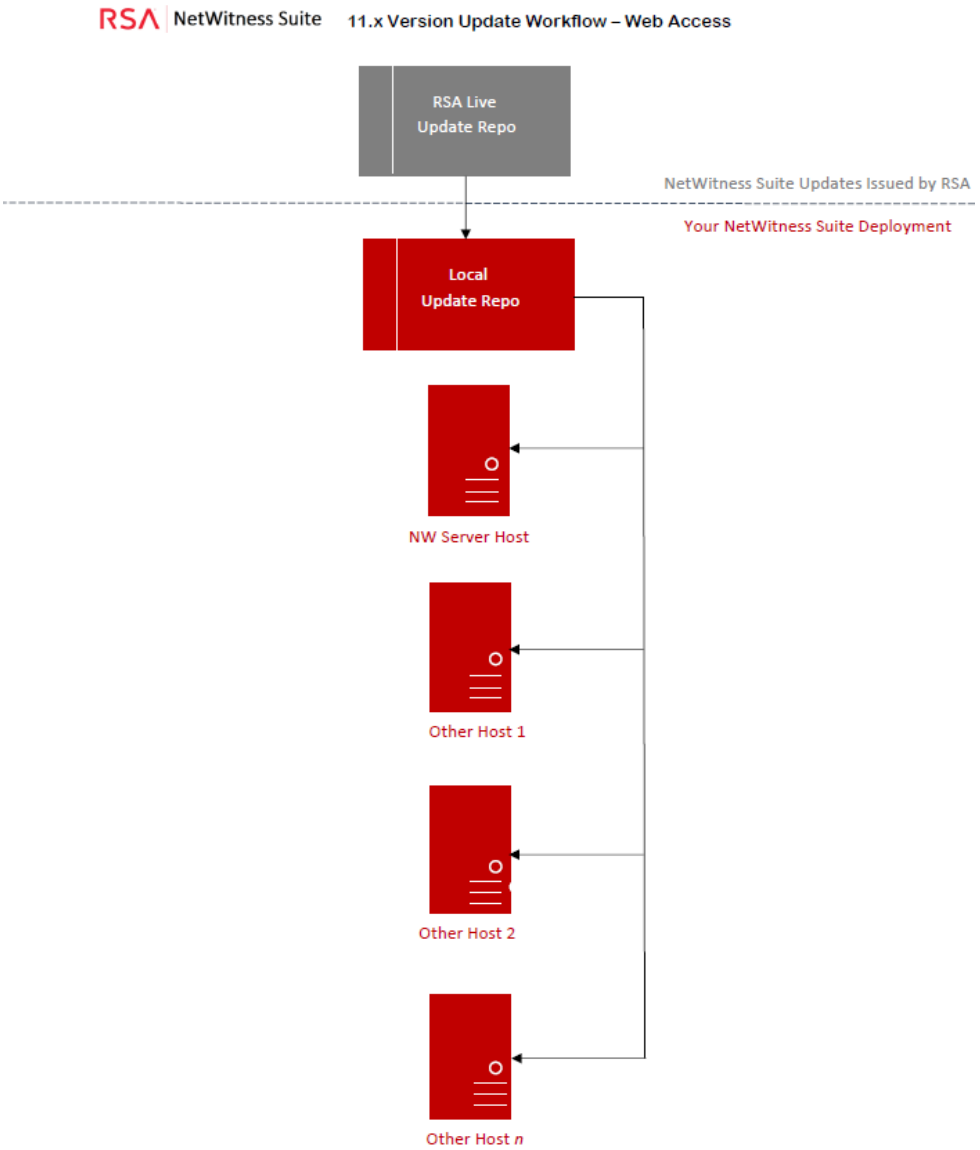
Mensaje de error	
Causa	La contraseña del usuario `deploy_admin` venció.
Solución	Restablezca la contraseña de `deploy_admin`. 1. En el menú de NetWitness Suite, seleccione **ADMINISTRAR** > **Seguridad** > pestaña **Usuarios**. 2. Seleccione **deploy_admin** y haga clic en **Restablecer contraseña**. • Si NetWitness Suite le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**, realice los siguientes pasos. a. Ingrese la contraseña de `deploy_admin` vencida. b. Deseleccione la casilla de verificación **Forzar cambio de contraseña en el próximo inicio de sesión**. c. Haga clic en **Guardar**. • Si NetWitness Suite no le permite ingresar la contraseña de `deploy_admin` vencida en el cuadro de diálogo **Restablecer contraseña**. a. En el host del servidor de NW y en todos los demás hosts en 11.x, ejecute el siguiente comando con el uso de la contraseña de `deploy_admin` nueva. `/opt/rsa/saTools/bin/set-deploy-admin-password` b. En el host en el cual falló la instalación/coordinación, ejecute nwsetup-tui y use la contraseña de `deploy_admin` nueva.

Mensaje de error	`/var/log/netwitness/orchestration-server/orchestration-server.log` tiene un error similar al siguiente: `API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgument Exception::Version '11.0.0.n' is not supported`
Problema	Después de actualizar el host del servidor de NW a 11.1, la única ruta de actualización para los hosts de servidores que no son de NW es 11.1. Si intenta actualizar cualquier host de servidor que no es de NW a un parche de 11.0.0.n (por ejemplo, de 11.0.0.0 a 11.0.0.3), se mostrará este mensaje de error.
Solución	Tiene dos opciones: • Actualice el host de servidor que no es de NW a 11.1 o • No actualice el host de servidor que no es de NW (mantenga su versión actual).

Apéndice B. Completar el repositorio local

NetWitness Suite envía actualizaciones de versión al repositorio de actualización local desde el repositorio de actualización de Live. El acceso al repositorio de actualización de Live requiere y usa las credenciales de la cuenta de Live configuradas en **ADMINISTRAR > SISTEMA > Live**. Además, debe seleccionar la casilla de verificación `Automatically download information about new updates every day` en **ADMINISTRAR > SISTEMA > Actualizaciones** para completar el repositorio local diariamente.

En el siguiente diagrama se ilustra la manera de obtener actualizaciones de versión si la implementación de NetWitness Suite tiene acceso a la Web.



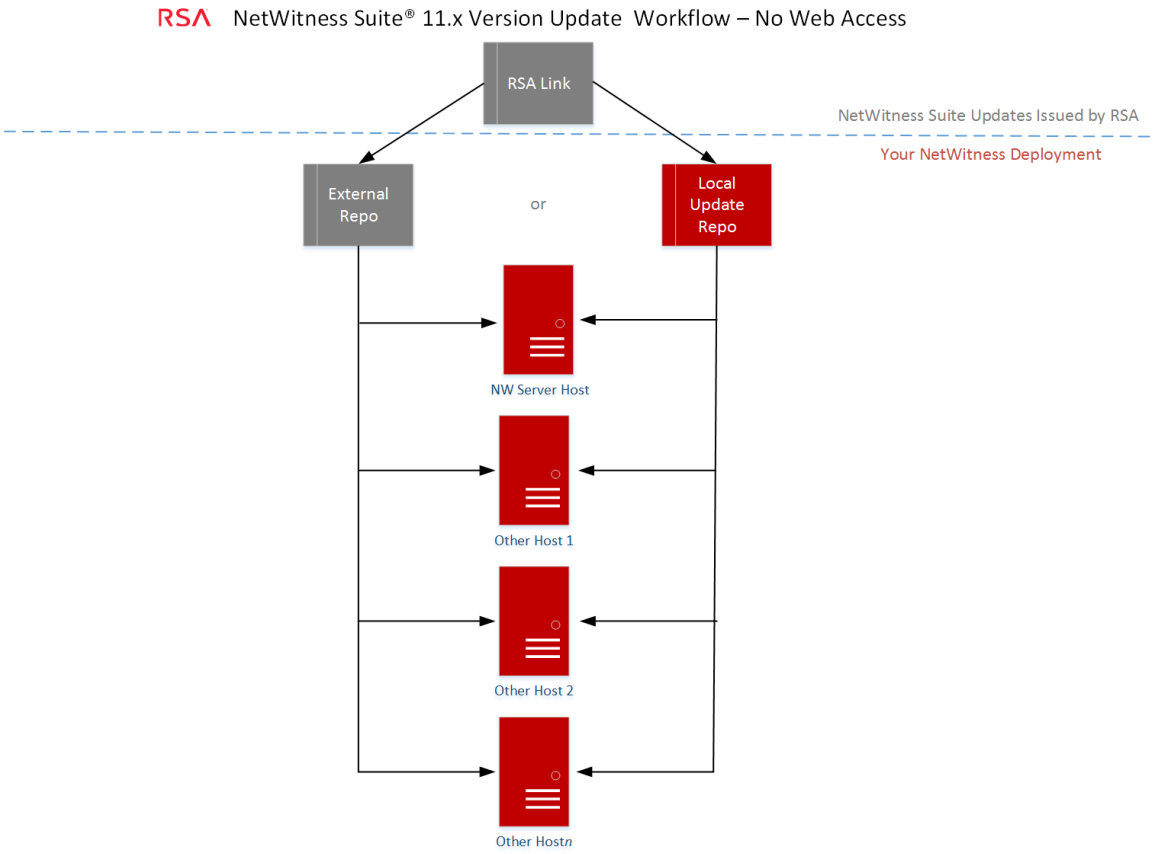
Nota: Cuando establezca la conexión inicial al repositorio de actualización de Live, accederá a todos los paquetes del sistema CentOS 7 y a los paquetes de producción de RSA. Esta descarga de más de 2.5 GB de datos tardará una cantidad indeterminada de tiempo de acuerdo con la conexión a Internet del servidor de NW y el tráfico del repositorio de RSA. El uso del repositorio de actualización de Live NO es obligatorio. Como alternativa, puede usar un repositorio externo como se describe en "Configuración de un repositorio externo".

Para conectarse al repositorio de actualización de Live, navegue a la vista **ADMINISTRAR > SISTEMA**, seleccione **Live** en el panel de opciones y asegúrese de que las credenciales estén configuradas (la luz de **Conexión** debería ser de color verde). Si no es verde, haga clic en **Iniciar sesión** y conéctese.

Nota: Si necesita usar un proxy para establecer conexión al repositorio de actualización de Live, puede configurar valores en Host proxy, Nombre de usuario de proxy y Contraseña de proxy. Consulte "Configurar el proxy deNetWitness Suite" en la *Guía de configuración del sistema de NetWitness Suite 1.1*.Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Consulte "Aplicar actualizaciones desde la línea de comandos" si la implementación de NetWitness Suite no tiene acceso a la Web.

En el siguiente diagrama se ilustra la manera de obtener actualizaciones de versión si la implementación de NetWitness Suite no tiene acceso a la Web.


NetWitness Suite® 11.x Version Update Workflow – No Web Access
RSA Link
NetWitness Suite Updates Issued by RSA
Your NetWitness Deployment
External Repo
or
Local Update Repo
NW Server Host
Other Host 1
Other Host 2
Other Hostn

Apéndice C. Configurar un repositorio externo

Realice el siguiente procedimiento para configurar un repositorio externo (repositorio).

Nota: 1.) Para realizar este procedimiento, debe estar instalada una utilidad de descompresión en el host. 2.) Debe saber cómo crear un servidor web antes de realizar el siguiente procedimiento.

1. (Condicional) Complete este paso si tiene un repositorio externo y desea reemplazarlo.
   - Caso 1: Inició el host desde un repositorio externo y desea actualizar con un repositorio local en el servidor de Admin.
     a. Cree el archivo `/etc/netwitness/platform/repobase`.
        `vi /etc/platform/netwitness/repobase`
     b. Edite el archivo `repobase` para que la siguiente dirección URL sea la única información en el archivo.
        `https://nw-node-zero/nwrpmrepo`
     c. Complete las instrucciones sobre cómo ejecutar la actualización usando la herramienta `upgrade-cli-client` .
        Consulte para obtener instrucciones.
   - Caso 2: Inició el host desde un repositorio local en el servidor de Admin (host del servidor de NW) y desea usar un repositorio externo para la actualización.
     a. Cree el archivo `/etc/netwitness/platform/repobase`.
        `vi /etc/platform/netwitness/repobase`
     b. Edite el archivo `repobase` para que la siguiente dirección URL sea la única información en el archivo.
        `https://<webserver-ip>/<alias-for-repo>`
     c. Complete las instrucciones sobre cómo ejecutar la actualización usando la herramienta `upgrade-cli-client`.
        Las instrucciones se encuentran en “Aplicar actualizaciones desde la línea de comandos” en el tema.
2. Configure el repositorio externo.
   a. Iniciar sesión en el host del servidor web
   b. Cree el directorio para alojar el repositorio de NW (`netwitness-11.1.0.0.zip`), por ejemplo `ziprepo` bajo `web-root` del servidor web. Por ejemplo, si /var/netwitness es

la raíz web, ejecute la siguiente cadena de comandos.

```
mkdir -p /var/netwitness/<your-zip-file-repo>
```

c. Cree el directorio 11.1.0.0 bajo `/var/netwitness/<your-zip-file-repo>`.

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0
```

d. Cree los directorios `OS` y `RSA` bajo `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

e. Descomprima el archivo `netwitness-11.1.0.0.zip` en el directorio `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.

```
unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0
```

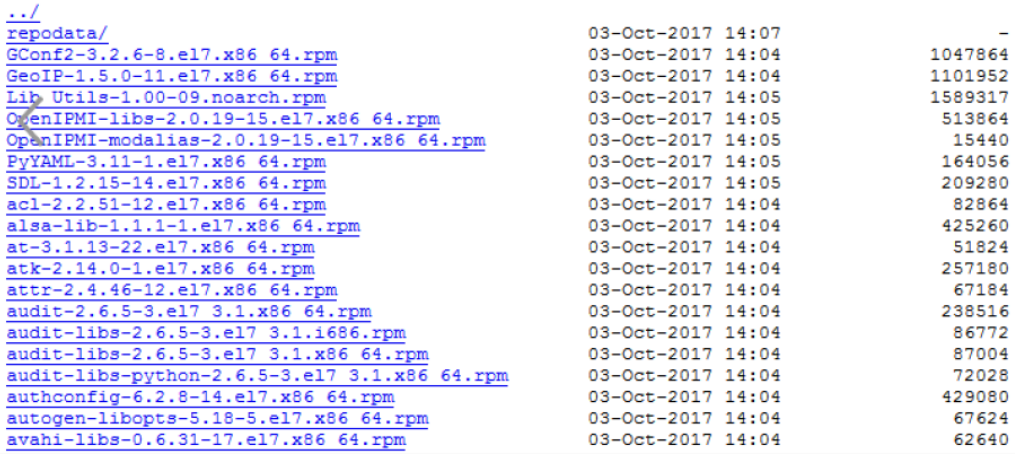
Con la descompresión de `netwitness-11.1.0.0.zip` se obtienen dos archivos zip (`OS-11.1.0.0.zip` y `RSA-11.1.0.0.zip`) y algunos otros archivos.

f. Descomprima

1. `OS-11.1.0.0.zip` en el directorio `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
```

En el siguiente ejemplo se ilustra la forma en que aparecerá la estructura de archivos del sistema operativo (SO) después de descomprimir el archivo.



../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

2. `RSA-11.1.0.0.zip` en el directorio `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-
11.1.0.0.zip -d /var/netwitness/<your-zip-file-
repo>/11.1.0.0/RSA
```

En el siguiente ejemplo se ilustra la forma en que aparecerá la estructura de archivos de actualización de la versión de RSA después de descomprimir el archivo.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

La dirección URL externa del repositorio es `http://<web server IP address>/<your-zip-file-repo>`.

g. (Condicional: para Azure) Siga estos pasos para la actualización de Azure

i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

ii. `unzip nw-azure-11.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`

iv. `createrepo .`

h. Use `http://<web server IP address>/<your-zip-file-repo>` en respuesta al indicador **Ingrese la dirección URL base de los repositorios de actualización externos** del programa de instalación de NW 11.1.0.0 (`nwsetup-tui`).

Historial de revisiones

Revisión	Fecha	Descripción	Autor
1.0	08/03/2018	Liberación a Operaciones (RTO)	IDD
1.1	12/03/2017	Se realizó un cambio a una nota al comienzo de Tareas de actualización en relación con un repositorio externo.	IDD
1.2	12/04/2018	Se agregó “Tarea 4: Asegurarse de que la información de identificación de `deploy_admin` siga siendo válida (no esté vencida)” a Tareas de preparación para la actualización.	IDD