RSA NETWITNESS® SUITE

Guía de actualización de AWS

para la versión 11.0.0.0

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

marzo 2018

Contenido

Introducción

Las instrucciones de esta guía se aplican a la actualización de AWS para RSA NetWitness Suite 10.6.4.x a 11.0.0.0 exclusivamente. Consulte la *Guía de actualización de hosts virtuales* de *RSA NetWitness Suite* para obtener instrucciones sobre cómo actualizar los hosts virtuales 10.6.4.x a 11.0. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0. En este documento se presupone que los dispositivos están en la nube de AWS.

NetWitness Suite 11.0 es una versión principal que afecta a todos los productos de la suite NetWitness Suite. Los componentes de la suite son Servidor de NetWitness (servidor de NW), Archiver, Broker, Concentrator, Context Hub, Decoder, Entity Behavior Analytics, Event Stream Analysis, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response y Workbench.

Actualización de CentOS6 a CentOS7

NetWitness Suite 11.0 es una versión principal que implica la actualización a una versión más reciente del sistema operativo (de CentOS6 a CentOS7). Además, al ambiente de la plataforma 11.0 se le realizaron mejoras considerables para que se adapte a los tipos de implementaciones físicas y virtuales actuales y futuras. Estos cambios requieren una actualización al nuevo ambiente y una actualización de la funcionalidad.

Ruta de actualización a RSA NetWitness® Suite 11.0

La ruta de actualización a RSA NetWitness® Suite 11.0 admitida es Security Analytics 10.6.4.x. Si ejecuta una versión de NetWitness Suite anterior a 10.6.4.x, debe actualizar a 10.6.4.x antes de poder actualizar a 11.0. Consulte la *Guía de actualización a RSA Security Analytics 10.6.4* (https://community.rsa.com/docs/DOC-79055) en RSA Link.

Precaución: Hay un problema conocido si tiene usuarios de Active Directory configurados en 10.6.4.x. Tiene dos opciones para solucionar este problema:
• Aplicar el parche de 10.6.4.2 antes de respaldar los datos para la actualización a 11.0.

Hardware, implementaciones, servicios y características no compatibles en 11.0

RSA no admite la actualización de los siguientes hardware, implementaciones, servicios y características a 11.0.

- Dispositivo RSA All-in-One (AIO)
- Implementación de múltiples Servidor de NetWitness
- Servicio IPDB
- Servicio Malware Analysis colocalizado en el servidor de SA (la actualización de Malware Analysis Enterprise se admite en 11.0).
- Política de Estado y condición personalizada en 10.6.x para el servicio Context Hub Después de que se realiza la actualización a NetWitness 11.0, su política personalizada ya no está presente. En su lugar, se encuentra la Política de monitoreo del servidor de Context Hub de uso inmediato en la interfaz del usuario, que es específica para la versión 11.0.
- La Guía de información técnica de seguridad de la Agencia de Sistemas de Información de Defensa (DISA-STIG) reforzó las implementaciones.
- Warehouse Analytics (ciencia de datos)

Consideraciones de actualización de Event Stream Analysis (ESA)

En RSA NetWitness® Suite 11.0, RSA cambió la manera en que las reglas de correlación de ESA almacenan y transmiten las alertas que genera el sistema. En 11.0, ESA envía todas las alertas a un sistema central de alerta. Se quitó el almacenamiento de Mongo local en ESA 10.6.4.x.

Precaución: Si no usa Incident Management en 10.6.4.x, considere cuidadosamente si desea actualizar o no a la versión 11.0.

Las siguientes reglas lo ayudarán a determinar si actualizar o no los hosts de ESA a 11.0.

En la implementación de 10.6.4.x:

- Si tiene un host de ESA, ya sea que tenga configurado o no Incident Management, actualice a 11.0.
- Si hay múltiples hosts de ESA configurados para usar Incident Management, el sistema continuará agregando alertas de manera centralizada. Si el sistema está dimensionado correctamente y está operando según lo previsto en 10.6.4.x, puede actualizar a la versión 11.0.
- Si tiene múltiples hosts de ESA sin configuración para usar Incident Management y se está conectando a hosts de ESA individuales para ver las alertas, no actualice a la versión 11.0.

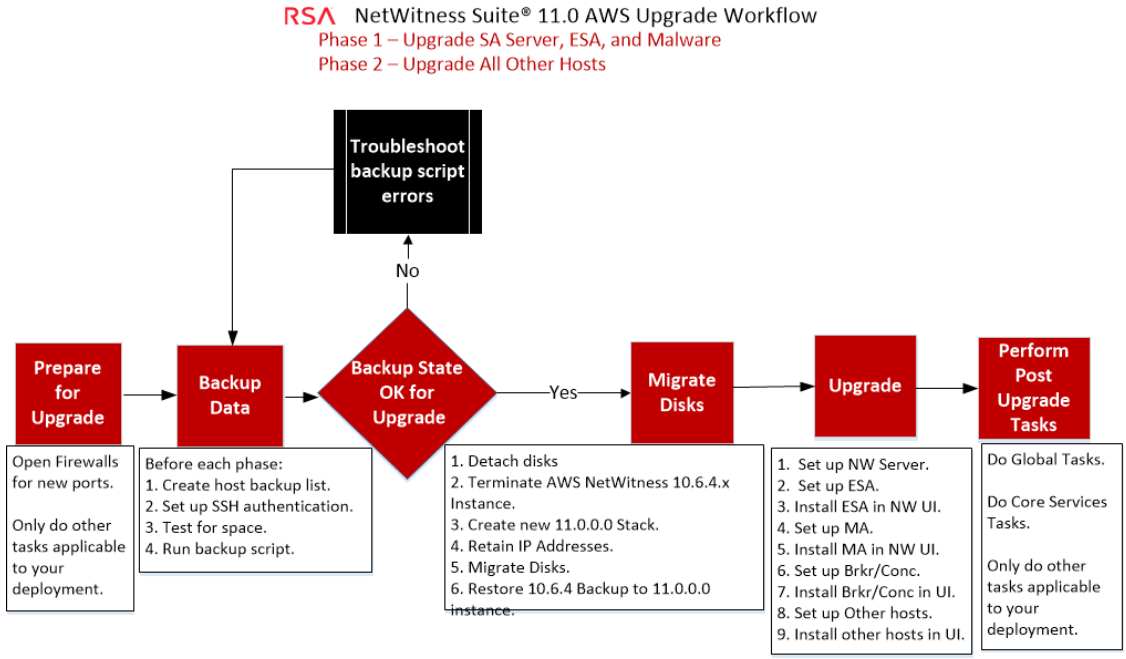
Nota: Si no usó Incident Management en 10.6.4.x, no puede ver las alertas de ESA para 10.6.4.x en el componente Respond 11.0 sin ejecutar un script de migración. Use el script Migración de alertas de ESA para migrar estas alertas a la ubicación en 11.0 que permitirá que Respond las vea. Consulte el artículo de la base de conocimientos *Instrucciones sobre la migración de alertas de ESA de 10.6.4.x a 11.0* (https://community.rsa.com/docs/DOC-81680) en RSA Link para obtener instrucciones sobre cómo ejecutar este script.

Cambios de atributos de usuario y de función que afectan a Investigate

Los siguientes cambios afectan la forma en que NetWitness Suite 11.0 maneja los atributos de usuario y de función en el componente Investigate.

- Atributos de usuario
  Cuando actualiza a 11.0, los atributos de usuario (prefijo de consulta, tiempo de espera de sesión agotado y umbral de consulta) disponibles en SA 10.6.4.x ya no existen. Los mismos atributos están disponibles en el nivel de función para su uso.
- Atributos de usuario y de función (prefijo de consulta) no se aplica a Análisis de eventos de Investigate. Los atributos de usuario y de función y, lo que es más importante, el prefijo de consulta, no se aplican al nuevo Análisis de eventos de Investigate. Cualquier usuario puede modificar la dirección URL en el navegador para acceder a los datos cuya vista se debe

restringir incluso cuando se aplica el prefijo de consulta.



Póngase en contacto con el servicio al cliente

Consulte la página de contacto con el servicio al cliente de RSA (https://community.rsa.com/docs/DOC-1294) en RSA Link para obtener instrucciones sobre cómo obtener ayuda acerca de RSA NetWitness Suite 11.0.

Tareas de preparación para la actualización

Realice las siguientes tareas para preparar la actualización a NetWitness Suite 11.0. Estas tareas se organizan en las siguientes categorías.

- Global
- Reporting Engine
- Respond e Incident Management

Global

Debe realizar estas tareas, independientemente de cómo implemente NetWitness Suite y qué componentes use.

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

En la siguiente tabla se enumeran los puertos nuevos en 11.0.

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.

Host del servidor de NW

Host de origen	Host de destino	Puertos de destino	Comentarios
Hosts de NW	Servidor de NW	TCP 4505, 4506	Puertos maestros de valor de sal
Hosts de NW	Servidor de NW	TCP 27017	MongoDB

Host de ESA

Host de origen	Host de destino	Puertos de destino	Comentarios
Servidor de NW, NW Endpoint, ESA secundario	ESA primario	TCP 27017	MongoDB

Todos los puertos principales de NetWitness Suite se enumeran en el tema “Arquitectura y puertos de red” de la *Guía de implementación* de *RSA NetWitness® Suite* en caso de que necesite reconfigurar los firewalls y los servicios NetWitness Suite. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Tarea 2: Registrar la contraseña de `admin user` 10.6.4.x

Registre la contraseña de `admin user` 10.6.4.x. La necesitará para completar la actualización.

Tarea 3: Crear un respaldo del archivo `/etc/fstab`

Copie el archivo `/etc/fstab` desde todas las VM en su máquina local (host de respaldo o máquina remota).

Nota: Este archivo se necesita para restaurar una VM con montajes a un almacenamiento externo.

Reporting Engine

(Condicional) Tarea 4: Desvincular el almacenamiento externo

Si Reporting Engine tiene almacenamiento externo [como red de almacenamiento SAN o almacenamiento conectado en red (NAS) para almacenar informes], debe realizar los siguientes pasos para desvincular el almacenamiento.

En estos pasos:

- `/home/rsasoc/rsa/soc/reporting-engine/` es el directorio principal de Reporting Engine.
- `/externalStorage/` es donde se monta el almacenamiento externo.

1. Acceda mediante el protocolo SSH al host de Reporting Engine e inicie sesión con sus credenciales `root` .
2. Detenga el servicio Reporting Engine.
   `stop rsasoc_re`
3. Cambie al usuario `rsasoc`.
   `su rsasoc`
4. Cambie al directorio principal de Reporting Engine.
   `cd /home/rsasoc/rsa/soc/reporting-engine/`
5. Desvincule el directorio `resultstore` montado a un almacenamiento externo.
   `unlink /externalStorage/resultstore`
6. Desvincule el directorio `formattedReports` montado a un almacenamiento externo.
   `unlink /externalStorage/formattedReports`

Respond e Incident Management

(Condicional) Tarea 5: Deshabilitar la retención de datos de Incident Management

Realice el siguiente procedimiento para deshabilitar los trabajos de retención de datos de Incident Management en 10.6.4.x

1. Inicie sesión en RSA Security Analytics 10.6.4.x.
2. Vaya a **Incident Management** > **Configurar** > **Calendarizador de retención**.
3. Deseleccione la casilla de verificación **Activar el calendarizador de retención de datos** y haga clic en **Aplicar**.

Instrucciones para respaldo

El respaldo de los datos de configuración de todos los hosts de 10.6.4.x es el primer paso en la actualización de versiones de 10.6.4.x a 11.0.0.0.

Nota: Es importante que coloque los archivos de certificado personalizado y cualquier otro archivo de autoridad de certificación (CA) en la carpeta `/root/customcerts` para asegurarse de que estos archivos de certificado se respalden. Los archivos de certificado personalizado que se colocan en este directorio se restaurarán automáticamente durante el proceso de actualización. Después de actualizar a 11.0.0.0, los archivos de certificado personalizado se encontrarán en `/etc/pki/nw/trust/import`. Para obtener más información acerca del respaldo de estos tipos de archivo, consulte el paso 1 en Para todos los tipos de host

Precaución: 1) Estos servicios no son compatibles en el proceso de respaldo y actualización de 10.6.4.x.
- IPDB
- Servidores de todo en uno
- Malware Analysis colocalizado en el servidor de NetWitness
- Warehouse Connector independiente

2) Hay un problema conocido si hay configurados usuarios de Active Directory en 10.6.4.x. Tiene dos opciones para solucionar este problema:
• Aplicar el parche de 10.6.4.2 antes de respaldar los datos para la actualización a 11.0.
• Si no pudo aplicar el parche de 10.6.4.2, puede aplicar el parche de 11.0.0.1 inmediatamente después de actualizar a 11.0.

Los siguientes tipos de host se pueden respaldar y se restauran de forma automática durante el proceso de actualización:

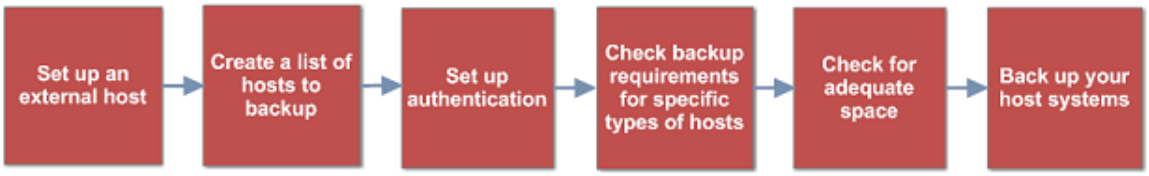
- **Servidor de NetWitness** (se pueden incluir Malware Analysis, NetWitness Respond, Estado y condición y Reporting Engine)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (incluida la base de datos de Context Hub y NetWitness Respond)
- **Concentrator**
- **Log Decoder**
- **Packet Decoder**
- **Virtual Log Collector**

Los siguientes tipos de archivos se respaldan automáticamente, pero se deben restaurar de manera manual después del proceso de actualización:

- Archivos de configuración de PAM: Para obtener información sobre la restauración de los archivos de configuración de PAM, consulte “Tarea 5: Reconfigurar módulo de autenticación con capacidad para conectarse (PAM) en 11.0.0.0” en la sección “Global” de Tareas posteriores a la actualización.
- `/etc/pfring/mtu.conf` y `/etc/init.d/pf_ring`: Para restaurar estos archivos, debe recuperarlos manualmente. Los archivos `/etc/pfring/mtu.conf` se encontrarán en `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf` y los archivos `/etc/init.d/pf_ring`, en `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. Para obtener información sobre cómo restaurar estos archivos, consulte “(Condicional) Tarea 2: Restaurar los archivos para Decoder 10G” en la sección “Tareas relacionadas con hardware" de Tareas posteriores a la actualización.

Nota: Si tiene problemas durante los procesos de respaldo o de actualización y pierde datos, puede recuperar los datos y volver a iniciar el proceso. Para obtener información sobre la recuperación de datos perdidos, consulte “Recuperar datos después de una falla del sistema” en la *Guía de mantenimiento del sistema.*

En el siguiente diagrama se muestra el flujo de tareas general de los pasos que debe realizar para respaldar sus hosts.



En las siguientes secciones se describe cada una de estas tareas:

- Tarea 1: Configurar un host externo para respaldar archivos
- Tarea 2: Crear una lista de hosts para respaldo
- Tarea 3: Configurar la autenticación entre los hosts de respaldo y de destino
- Tarea 4: Comprobar cuáles son los requisitos de respaldo para tipos específicos de hosts
- Tarea 5: Comprobar si hay espacio suficiente para el respaldo
- Tarea 6: Respaldar los sistemas del host
- Tareas posteriores al respaldo

Tarea 1: Configurar un host externo para respaldar archivos

Debe configurar un host externo para usarlo con el fin de respaldar archivos. El host debe ejecutar CentOS 6 con conectividad mediante el protocolo SSH a la plataforma de hosts de NetWitness Suite.

Asegúrese de que los nombres de host para los sistemas que se deben respaldar puedan resolverse en la máquina del host de respaldo, ya sea mediante DNS o una lista en el archivo `/etc/hosts`.

Nota: Estos scripts están diseñados para ejecutarse solamente en CentOS 6. Debe ejecutar estos scripts en máquinas de CentOS 6.

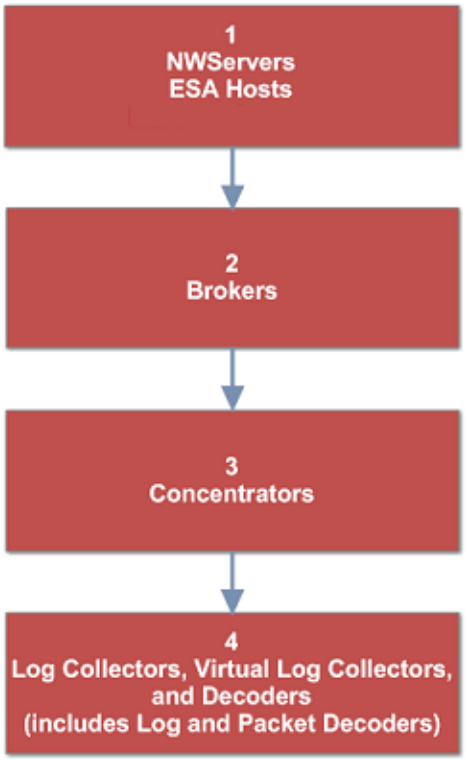
Existen varios scripts que se ejecutan durante el proceso de respaldo. Debe descargar el archivo zip que contiene los scripts (`nw-backup-v3.0.zip`) de RSA Link en esta ubicación: https://community.rsa.com/docs/DOC-81514 y copiarlo en el sistema de respaldo CentOS 6. Haga clic en el vínculo **Script de respaldo de RSA NetWitness Logs & Packets 11.0 (nw-backup-v3.0.sh)** y extraiga el archivo zip para acceder a los scripts. Los scripts son los siguientes:

- `get-all-systems.sh`: Crea el archivo `all-systems`, que contiene una lista de todos los Servidor de NetWitness y los sistemas del host que se respaldarán.
- `ssh-propagate.sh`: Automatiza las claves de uso compartido entre los sistemas que está respaldando y el sistema del host de respaldo, de modo que las contraseñas no se le solicitarán varias veces.
- `nw-backup.sh`: Realiza el respaldo de los hosts.

Nota: Los scripts de respaldo no admiten el respaldo de datos para hosts de reforzamiento STIG.

Tarea 2: Crear una lista de hosts para respaldo

El script que se usa para respaldar sus archivos depende de los archivos `all-systems` y `all-systems-master-copy`, que contienen una lista de los hosts que desea respaldar. El archivo `all-systems-master-copy` contiene una lista de todos sus hosts. El archivo `all-systems` se usa para cada sesión de respaldo y contiene solamente los hosts que se han respaldado para una sesión determinada. El script `get-all-systems.sh` se ejecuta para generar estos archivos. RSA recomienda que respalde los hosts en grupos y no todos al mismo tiempo. El orden y la agrupación de hosts que se recomiendan para sesiones de respaldo se muestran en el siguiente diagrama:



Limite cada sesión de respaldo a cinco hosts para asegurarse de que no se agote el espacio para los archivos de respaldo. Para crear los archivos `all-systems` para las sesiones de respaldo, use el archivo `all-systems-master-copy` como referencia y edite de forma manual el archivo `all-systems` para que contenga hosts específicos.

Para generar los archivos `all-systems` y `all-systems-master-copy`:

1. En el host en que ejecuta el proceso de respaldo, ejecute el siguiente comando para que el script `get-all-systems.sh` se pueda ejecutar:
   ```
   chmod u+x get-all-systems.sh
   ```
2. En el nivel de raíz, ejecute el script `get-all-systems.sh`:
   ```
   ./get-all-systems.sh <IP-Address-of-NetWitness-Admin-Server>
   ```
   Se le solicitará que ingrese la contraseña para cada sistema del host, una vez por host.

Este script guarda el archivo `all-systems` y el archivo `all-systems-master-copy` en `/var/netwitness/database/nw-backup/`.

3. Valide que los archivos `all-systems` y `all-systems-master-copy` se hayan generado y que contengan los hosts correctos.
4. Edite el archivo `all-systems` para que contenga solo los sistemas que está respaldando. Para hacer esto, use el archivo `all-systems-master-copy` como referencia, abra el archivo `all-systems` en un editor (por ejemplo, vi) y modifíquelo para incluir solo los sistemas que desea respaldar.

> **Nota:** Si usa vi, asegúrese de incluir la ruta a la ubicación del archivo `all-systems`.

Este es un ejemplo de un archivo `all-systems-master-copy`:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.4.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.4.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.4.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.4.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.4.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.4.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.4.0
```

Y este es un ejemplo de un archivo `all-systems` basado en el archivo `all-systems-master-copy` que se podría usar en la primera sesión de respaldo:

```
saserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.4.0
```

Información de solución de problemas

- Asegúrese de guardar copias de los archivos `all-systems` y `all-systems-master-copy` en una ubicación segura. Siga estas recomendaciones:

  - No edite el archivo `all-systems-master-copy`.
  - Si crea varias versiones distintas del archivo `all-systems` (por ejemplo, para varias sesiones de respaldo), asegúrese de quitar las entradas preexistentes del archivo, de modo que el archivo contenga solamente aquellos hosts que se están respaldando actualmente. Para obtener más información, consulte Tareas posteriores al respaldo.

- Si alguno de los sistemas del host está inactivo mientras se está ejecutando el script `get-all-systems.sh`, el script crea una lista de hosts para los cuales no puede encontrar información. Después de que finalice el script y se cree el archivo `all-systems`, debe editar el archivo `all-systems` manualmente y agregar la información que falta para estos hosts.

- El script `get-all-systems.sh` genera una lista de hosts que se definieron en la interfaz del usuario de NetWitness Suite. Asegúrese de que todos los hosts y los servicios se aprovisionen correctamente. Si algún host o servicio no se aprovisiona correctamente, no se podrá respaldar. Cuando agregue hosts y servicios a NetWitness Suite, RSA recomienda usar la interfaz del usuario de NetWitness Suite para asegurarse de que se aprovisionen correctamente. Sin embargo, si hay algún host o servicio que no se haya definido en la interfaz del usuario, debe agregarlo al archivo `all-systems` manualmente.

- Al final del script `get-all-systems.sh`, el script comprobará si existe alguna diferencia entre los sistemas que el Servidor de NetWitness ha enumerado y aquellos para los cuales el script pudo encontrar toda la información requerida. Si algún ID de nodo o nombre del sistema se enumera como faltante, verifique la existencia de esos sistemas, que todos los servicios estén en ejecución y que se estén comunicando correctamente con el Servidor de NetWitness. (No se agregará ningún Recopilador de Windows existente o Recopilador de nube de AWS al archivo `all-systems`, porque esto puede producir discrepancias. **NO agregue manualmente estos elementos al archivo `all-systems`**).
- Si la sintaxis en el archivo `all-systems` está incorrecta, el script fallará. Por ejemplo, si hay un espacio adicional al principio o al final de una entrada de host, el script fallará.

Tarea 3: Configurar la autenticación entre los hosts de respaldo y de destino

RSA recomienda ejecutar el script `ssh-propagate.sh` para automatizar las claves de uso compartido entre el host de respaldo y los sistemas del host.

Nota: Si tiene claves del protocolo SSH que están protegidas con frases de contraseña, puede usar `ssh-agent` para ahorrar tiempo. Para obtener más información, consulte la página de los manuales de `ssh-agent`.

1. En el sistema del host de respaldo externo, ejecute el siguiente comando para que el script `ssh-propagate.sh` se pueda ejecutar:
   `chmod u+x ssh-propagate.sh`
2. En el directorio raíz, ejecute el siguiente comando, donde `<path-to-all-systems-file>` es la ruta al directorio donde se almacena el archivo `all-systems`:
   `ssh-propagate.sh <path-to-all-systems-file>`
3. Se le solicitará la contraseña una vez por host, pero no será necesario ingresarla reiteradamente más adelante durante el proceso de respaldo.

Tarea 4: Comprobar cuáles son los requisitos de respaldo para tipos específicos de hosts

Después de crear el archivo `all-systems` que desea usar para el respaldo, debe comprobar para ver si alguno de los hosts que aparecen en el archivo tiene requisitos que se deben cumplir antes de ejecutar el proceso de respaldo.

Para todos los tipos de host

Realice los siguientes pasos para todos los tipos de host:

1. En el Servidor de NetWitness, coloque los archivos de certificado personalizado y cualquier otro archivo de autoridad de certificación (CA) en la carpeta `/root/customcerts` para asegurarse de que estos archivos de certificado se respalden. Los archivos de certificado personalizado que se colocan en este directorio se restaurarán automáticamente durante el proceso de actualización. Después de actualizar a 11.0.0.0, los archivos de certificado personalizado se encontrarán en `/etc/pki/nw/trust/import`.
   Puede convertir los certificados y las claves de CA a diferentes formatos para que sean compatibles con tipos específicos de servidores o de software mediante OpenSSL. Por ejemplo, puede convertir un archivo PEM normal que funcionaría con Apache a un archivo

PFX (PKCS#12) y usarlo con Tomcat o IIS. Para convertir los archivos, acceda mediante el protocolo SSH a Servidor de NetWitness y ejecute las siguientes cadenas de comandos para realizar las conversiones que se enumeran.

Convertir un archivo DER (.crt, .cer o .der) a PEM

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Convertir un archivo PEM a DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convertir un archivo de certificado PEM y una clave privada a PKCS#12 (.pfx o .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

Convertir un archivo PKCS#12 (.pfx o .p12) que contenga una clave privada y certificados a PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Nota:** Agregue el siguiente calificador a la cadena de comandos para:
> `-nocerts` convertir exclusivamente claves privadas.
> `-nokeys` convertir exclusivamente certificados.

2. Registre manualmente todas las configuraciones personalizadas que se realizan a CentOS 6 (por ejemplo, personalizaciones de driver) para la restauración después de actualizar a CentOS 7. Las configuraciones personalizadas a CentOS 6 no se respaldan ni se restauran automáticamente.

Para hosts de Decoder, Concentrator o Broker: Detener la captura y la agregación de datos

Además de las tareas que se describen en Para todos los tipos de host, para los hosts de Decoder, Concentrator o Broker, detenga la captura y la agregación de datos en todos los sistemas que está respaldando. Para obtener instrucciones, consulte el Apéndice B. Detención y reinicio de la captura y la agregación de datos .

Log Collectors (LC) y Virtual Log Collectors (VLC): Ejecute `prepare-for-migrate.sh`

> **Precaución:** Esta tarea detiene la recopilación de registros, de modo que debe realizar este paso inmediatamente antes de la actualización para minimizar la pérdida de recopilación de eventos. Realice esta tarea de acuerdo con las tareas de respaldo y actualización de esta guía.

Requisitos previos

Necesita la siguiente información antes de preparar LC y VLC para la actualización.

- Si Lockbox se inicializó en el LC y VLC, debe conocer la contraseña de Lockbox. Es necesario reconfigurar Lockbox después de la actualización.
- Si configura la contraseña para el usuario `logcollector` de RabbitMQ, debe conocer la contraseña para que pueda configurarla nuevamente después de la actualización.

Preparar LC y VLC para la actualización

1. Acceda mediante el protocolo SSH a Log Collector.
2. Ejecute la siguiente cadena de comandos.
   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```
   Este comando:
   - Detiene el servicio de agente puppet.
   - Deshabilita las cuentas de recopilación de archivos (“sftp” y todos los usuarios en el grupo “upload”) que se usan para cargar los archivos de registro en Log Collector. Los archivos de registro se acumulan en los orígenes de eventos hasta que el Log Collector se actualiza a 11.0.0.0.
   - Detiene todos los protocolos de recopilación en el servicio Log Collector.
   - Guarda la lista de cuentas de Plug-in y RabbitMQ.
   - Configura el servidor de RabbitMQ para que los nuevos eventos no se puedan publicar más en él. Los consumidores de eventos en las líneas de espera, por ejemplo, shovels y procesadores de eventos de Log Decoder, continuarán ejecutándose.
   - Espera hasta que las líneas de espera de Log Collector están vacías.
   - Detiene el servicio Log Collector.
   - Crea un archivo de marcador que indica que el Log Collector se preparó correctamente para la actualización.

Información de solución de problemas

El script `prepare-for-migrate.sh` :

- Envía mensajes informativos, de advertencia y de error a la consola.
- Guarda un registro de sesión en el directorio `/var/log/backup/`.

Debe reparar cualquiera de los siguientes errores y reanudar la preparación. Póngase en contacto con el servicio al cliente de RSA (https://community.rsa.com/docs/DOC-1294) para obtener ayuda.

- Hay líneas de espera de Log Collector con eventos, pero sin consumidores.
- No se puede detener el servicio de agente puppet.

- No se puede detener un protocolo de recopilación en el servicio Log Collector.
- No se pueden bloquear los publicadores de eventos para el servidor de RabbitMQ.
- No se pueden consumir los eventos en línea de espera o su consumo tarda mucho. El script realiza 30 intentos para que los eventos se consuman. Después de cada intento, queda en reposo durante 30 segundos.
- No se puede detener el servicio Log Collector.

Para obtener más información acerca de la solución de problemas, consulte el Apéndice A. Solución de problemas.

Para integraciones con Web Threat Detection, NetWitness SecOps Manager o NetWitness Endpoint: Enumerar nombres de usuario y contraseñas de RabbitMQ

En el host 10.6.4.x, en el host de Servidor de NetWitness, debe obtener una lista de todos los nombres de usuario y las contraseñas de RabbitMQ, de modo que después de realizar la actualización a 11.0.0.0, pueda restaurar las cuentas de usuario de RabbitMQ.

Para obtener una lista de los nombres de usuario y las contraseñas de RabbitMQ, ejecute el siguiente comando:

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

Para restaurar las cuentas de usuario de RabbitMQ, consulte *Tarea 2: Para integraciones con Web Threat Detection, NetWitness SecOps Manager o NetWitness Endpoint, configurar SSL autenticado mutuamente* en Tareas posteriores a la actualización.

Para orígenes de eventos de Bluecoat

Los orígenes de eventos de Bluecoat ProxySG usan el protocolo FTPS para cargar archivos de registro en Log Collector (LC) y Virtual Log Collector (VLC). La documentación de origen de eventos contiene los pasos para configurar el servicio VSFTPD en LC y VLC.

- Si existe material de clave en el directorio `/root/vsftpd/` en 10.6.4.x, esta área de material se respaldará y se restaurará. **Si el material está en otra ubicación, debe respaldarlo y restaurarlo manualmente.**
- Si el archivo `/etc/vsftpd/vsftpd.conf` se cierra en 10.6.4.x, se respalda y se restaura.

Tarea 5: Comprobar si hay espacio suficiente para el respaldo

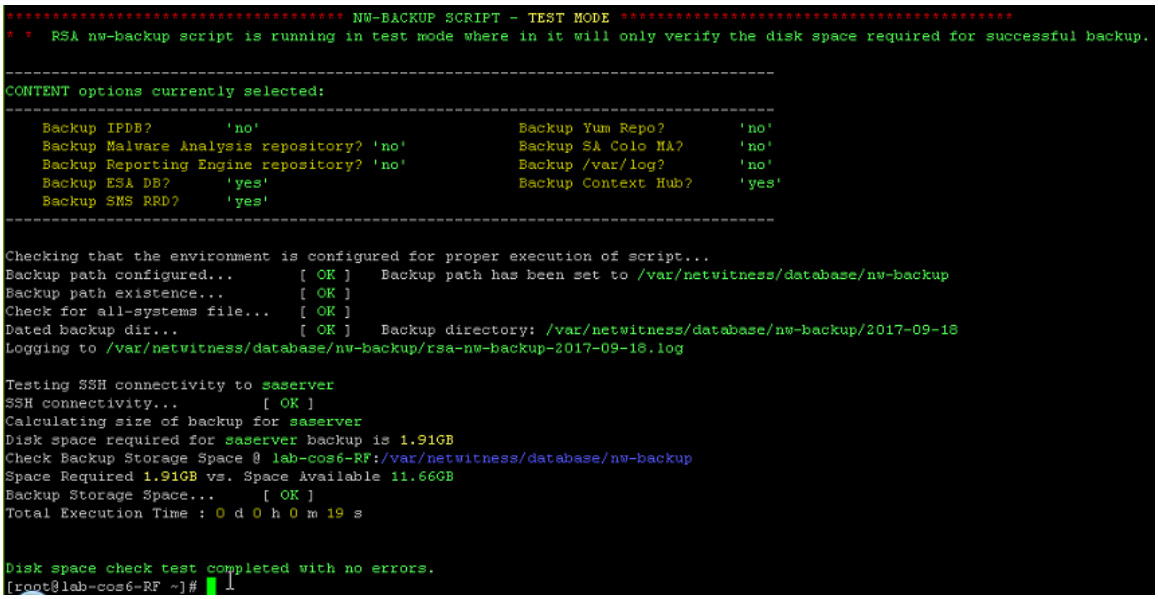
Puede ejecutar el script de prueba de respaldo para comprobar la cantidad de espacio en disco que se requiere para el respaldo mediante la opción `-t` que se describe en Opciones de prueba. Ejecute el script sin respaldar realmente los archivos ni detener algún servicio. RSA recomienda realizar este paso para asegurarse de que proporcione un espacio suficiente para el respaldo, de modo que el respaldo capture todos los datos.

Para comprobar si hay espacio suficiente en disco:

1. Ejecute el siguiente comando para que el script de respaldo se pueda ejecutar:
   `chmod u+x nw-backup.sh`
2. Ejecute el siguiente comando en el nivel del directorio raíz:
   `./nw-backup.sh -t`
   La salida muestra la cantidad de espacio en disco que se requiere para el respaldo.

> **Nota:** El comando `./nw-backup.sh -t` se ejecuta con la opción `-d` de manera predeterminada. Sin embargo, si desea obtener resultados más precisos sobre el espacio en disco, reemplace la opción `-d` por `-D`. Con la opción `-D`, se muestra cuánto espacio se requiere en cada host para los datos que deben respaldarse, pero no se muestra cuánto espacio hay disponible. Si no hay suficiente espacio disponible, la opción `-D` producirá un error. Si desea saber cuánto espacio hay disponible en el host de destino, debe ejecutar el comando`df -h` en el host.

En la siguiente figura se muestra un ejemplo de la salida mediante la opción `-t`.



Tarea 6: Respaldar los sistemas del host

Antes de ejecutar el script de respaldo para realizar el respaldo real, asegúrese de que haya una gran cantidad de espacio. Para respaldar los hosts, ejecute el script `nw-backup.sh` mediante la opción `-u`. Esta opción se requiere para la actualización a 11.0.0.0.

Nota: El script detendrá los servicios cuando se ejecute. Sin embargo, puede detener los servicios manualmente antes de ejecutar el script, si es necesario.

Cuando se ejecuta el script de respaldo, puede elegir entre varias opciones que se describen en las siguientes secciones.

Sintaxis:
`./nw-backup.sh [-u -t -d -D -u -l -x -e <external-mnt> -b <backup file path>`

Opciones generales

`-u : This option is required for upgrading to 11.0. Enables the upgrade flag to run backup for upgrading to 11.0. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

`-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)`

`-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)`

`-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)`

`-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)`

`-x : move all backup files to an external mount point. Default: (no) - COPY`

`-b <path to write backups> : path to the location for storing backup files on a backup server.` **`For upgrading to 11.0, please use the default location!`** `Default: (/var/netwitness/database/nw-backup)`

Nota: No cambie la ruta de respaldo en el modo de actualización (-u).

Opciones avanzadas de selección de contenido

`-c : back up Colocated Malware Analysis on SA servers. Default: (no)`

`-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)`

`-m : back up Malware Analysis File Repository. Default: (no)`

`-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)`

`-v : back up system logs (/var/log). Default: (no)`

```
-y : back up YUM Web Server & RPM Repository. Default: (no)

-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)

-C : If set: DISABLES back up of Context-Hub configuration and database.
Default: (not-set)

-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)
```

Opciones de prueba

```
 -t : performs script test run for disk space check only. Services are
not stopped and excludes execution of backup. Can be combined with (-d)
or (-D) and other flags. Default: (-t)
```

Por ejemplo, el comando:
`./nw-backup.sh`
ejecutaría el respaldo con opciones configuradas en el Encabezado del script mismo.
O, el comando:
`./nw-backup.sh -ue /mnt/external_backup`
podría ejecutar un respaldo normal mediante la ruta de respaldo definida en el script, con las siguientes opciones:

```
-u : enables the upgrade flag to run backup for upgrading to 11.0. It
also enables disk space check (-d), backing up reporting engine reports
(-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on
/mnt/external_backup

For Help: ./nw-backup.sh -h
```

Cuando se ejecuta el script, se muestra el siguiente texto en la parte superior del script:

Precaución:
```
RSA nw-backup script backs up configuration files, data, and
logs on the options provided in the script. It tars the content, with
options to store the backup files on the backup server, move or copy
them to external storage on a mount point (USB/NFS/SMB), or SCP them
back to the target host.
This backup script has been qualified on the following versions of
Security Analytics:
10.6.3.x and 10.6.4.x
Use of this script on any other versions of the product may not give
expected results and may not be supported by RSA Customer
Service.Note: All non-RSA custom files, scripts, Cronjobs and other
important files should be placed in /root, /home/'user', OR /etc to be
included in the backup.
```

Para ejecutar el script de respaldo para respaldar los hosts:

1. Asegúrese de que el archivo `all-systems` contenga solo los hosts que se respaldarán. Para obtener información, consulte Tarea 2: Crear una lista de hosts para respaldo.

2. Ejecute el siguiente comando para que el script de respaldo se pueda ejecutar:
   `chmod u+x nw-backup.sh`
3. Inicie el proceso de respaldo mediante la ejecución del siguiente comando en el nivel de directorio raíz:
   `./nw-backup.sh -u <additional options as needed>`

   Nota: Debe usar la opción `-u` para que los archivos se restauren correctamente durante la actualización a 11.0.0.0.

   Cuando se muestra el texto "`Backup completed with no errors`", el respaldo se completó correctamente.

   En el directorio de respaldo se crea un archivo de registro, con un nombre similar al siguiente ejemplo, el cual proporciona información sobre los archivos que se respaldan:
   `rsa-nw-backup-2017-03-15.log`
4. Cuando haya completado el respaldo, para asegurarse de que se hayan respaldado los archivos previstos, puede ejecutar el siguiente comando para ver una lista de todos los archivos que se respaldaron:

   `tar -tzvf hostname-ip-address-backup.tar.gz`

   Se crean los siguientes archivos de archiving:

   Para todos los hosts:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   archivos `tar checksum`

   `<hostname-IPaddress>-network.info.txt`

   Para Servidor de NetWitness:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   archivos `tar checksum`

   `<hostname-IPaddress>-network.info.txt`

   Para hosts de ESA:

   `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   `<hostname-IPaddress>-controldata-mongodb.tar.gz`

   archivos `tar checksum`

   `<hostname-IPaddress>-network.info.txt`

Los archivos archivados se encuentran en el directorio `/var/netwitness/database/nw-backup`. Si alguno de los archivos tar se ve más pequeño de lo esperado, debe abrirlo para asegurarse de que los archivos se hayan respaldado correctamente.

Tareas posteriores al respaldo

Tarea 1: Guardar una copia del archivo `all-systems` y de los archivos tar de respaldo

Realice copias del archivo `all-systems`, el archivo `all-systems-master-copy` y los archivos tar de respaldo, y colóquelas en una ubicación segura. No puede volver a generar estos archivos después de actualizar el Servidor de NetWitness (específicamente, el servicio Admin) a 11.0.0.0.

Tarea 2: Asegurarse de que se hayan generado los archivos de respaldo requeridos

Después de ejecutar los scripts de respaldo, se generan varios archivos. Estos archivos se requieren para el proceso de actualización a 11.0.0.0. Antes de comenzar el proceso de actualización, debe asegurarse de que los archivos de respaldo requeridos estén en los hosts que se están actualizando y de realizar las siguientes tareas.

Los siguientes archivos se generan en todos los hosts mediante los scripts de respaldo:

- `all-systems`
- `all-systems-master-copy`
- `appliance_info`
- `service_info`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

Además de los archivos mencionados anteriormente, se generarán los siguientes archivos en los hosts de Servidor de NetWitness y de ESA:

- *<hostname>-<host IP address>*`-mongodb.tar.gz`
- *<hostname>-<host IP address>*`-mongodb.tar.gz.sha256`

El script de respaldo también genera los siguientes archivos `controldata-mongodb.tar.gz`.

Nota: El script de respaldo copia los siguientes archivos desde todos los hosts de ESA a la ruta de respaldo del host de Servidor de NetWitness.

- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz`
- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256`

Tarea 3: (Condicional) Para múltiples hosts de ESA, copiar archivos `mongodb tar` en host de ESA primario

Si tiene múltiples sistemas del host de ESA en su empresa, copie los siguientes dos archivos desde cada host de ESA al directorio `/opt/rsa/database/nw-backup/` del sistema de host de ESA primario (el host en que se ejecuta el servicio Context Hub):

- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Tarea 4: Asegurarse de que todos los archivos de respaldo requeridos estén en cada host

Antes de actualizar a 11.0.0.0, asegúrese de que existan los archivos apropiados en los hosts que está actualizando, como se describe en las siguientes listas.

There should be note here mentioning default backup path locations for that user knows where to go and check these files.

Nota: Las rutas predeterminadas para los archivos de respaldo son las siguientes:
- Hosts de Servidor de NetWitness:`/var/netwitness/database/nw-backup`
- Hosts de ESA:`/opt/rsa/database/nw-backup`
- Hosts de Malware: `/var/lib/rsamalware/nw-backup`

Archivos requeridos para los Servidor de NetWitness

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256

Archivos requeridos para los hosts de ESA

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

Archivos requeridos para todos los demás hosts

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

Nota: Los siguientes archivos se encuentran en el archivo tar <hostname>-<host-IP-address>-backup.tar.gz en todos los hosts:
appliance_info
service_info

Nota: Las rutas a la ubicación de los archivos de respaldo y restauración para tablas de IP, las configuraciones de NAT, las cuentas de usuario y las entradas de crontab se muestran en la siguiente lista:

Rutas de respaldo:

`BUPATH=/opt/rsa/database/nw-backup` para el motor de correlación de ESA

`BUPATH=/var/lib/rsamalware/nw-backup` para el servicio Malware

`BUPATH=/var/netwitness/database/nw-backup` para todos los demás servicios

Ubicaciones de restauración:

`BUPATH/restore/etc/sysconfig` para las reglas Iptable

`BUPATH/restore/etc/sysconfig` para las configuraciones de NAT

`BUPATH/restore/etc` para las entradas de Crontab

`BUPATH/restore/etc` para las cuentas de usuario (los usuarios se encuentran en el archivo `passwd` y los grupos, en el archivo `group`). Estos no se restauran durante el proceso de actualización, pero se pueden restaurar manualmente.

`BUPATH/restore/etc/ntp.conf` para las configuraciones de NTP (deben restaurarse utilizando con la interfaz del usuario de NetWitness Suite)

Migrar unidades de disco de 10.6.4.x a 11.0

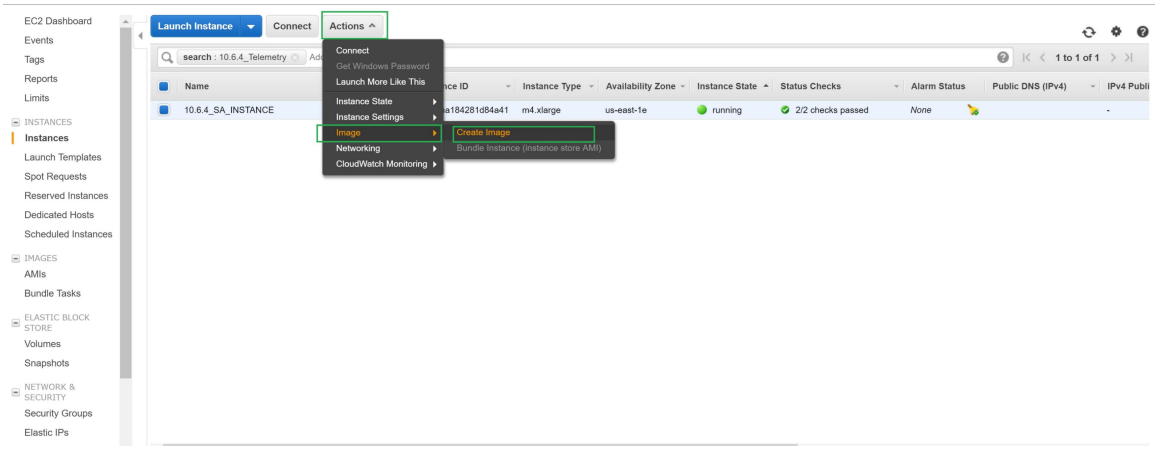
Estas instrucciones indican cómo actualizar los hosts virtuales de 10.6.4.x a 11.0.

Precaución: 1.) Ejecute el respaldo inmediatamente antes de actualizar los hosts para cada fase, de modo que los datos no estén obsoletos.
2.) Esta guía se aplica exclusivamente a las actualizaciones de hosts de AWS. Si tiene hosts físicos y hosts virtuales en la implementación, consulte las *Instrucciones de actualización de hosts físicos 11.0* de *RSA NetWitness® Suite* para ver cuáles son los pasos que debe completar para actualizar los hosts físicos. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Debe completar ocho tareas para migrar de 10.6.4.x a 11.0:

Tarea 1. Respaldar el dispositivo de EC2 10.6.4.x

Seleccione la instancia de EC2 10.6.4.x y desplácese a Acciones. Haga clic en Imagen y, a continuación, seleccione Crear imagen.



(Opcional) Tarea 2. Ejecutar el script de respaldo para obtener los datos de respaldo de la instancia de 10.6.4.x

Nota: Si no realizó el respaldo de la instancia de 10.6.4.x, siga estos pasos; de lo contrario, vaya a Tarea 3. Parar las instancias y desconectar los volúmenes de instancias de 10.6.4.x.

Si la pila contiene LogCollector, prepare **Log Collector** para la migración:

1. Vaya a `/opt/rsa/nwlogcollector/nwtools/` y ejecute el comando siguiente:

```
sh prepare-for-migrate.sh --prepare
```

2. Descargue los scripts de respaldo de GitHub (https://github.rsa.lab.emc.com/asoc/nw-backup, maintenance-11.0) y colóquelos en cualquier ubicación de una computadora que ejecute una distribución de Linux basada en RPM (RHEL o CentOS, por ejemplo) y tenga gran cantidad de espacio libre en el disco duro. En muchos casos, basta con el servidor de SA. Después, desplácese al directorio `scripts` de "`nw-backup-master`" y ejecute los comandos siguientes:

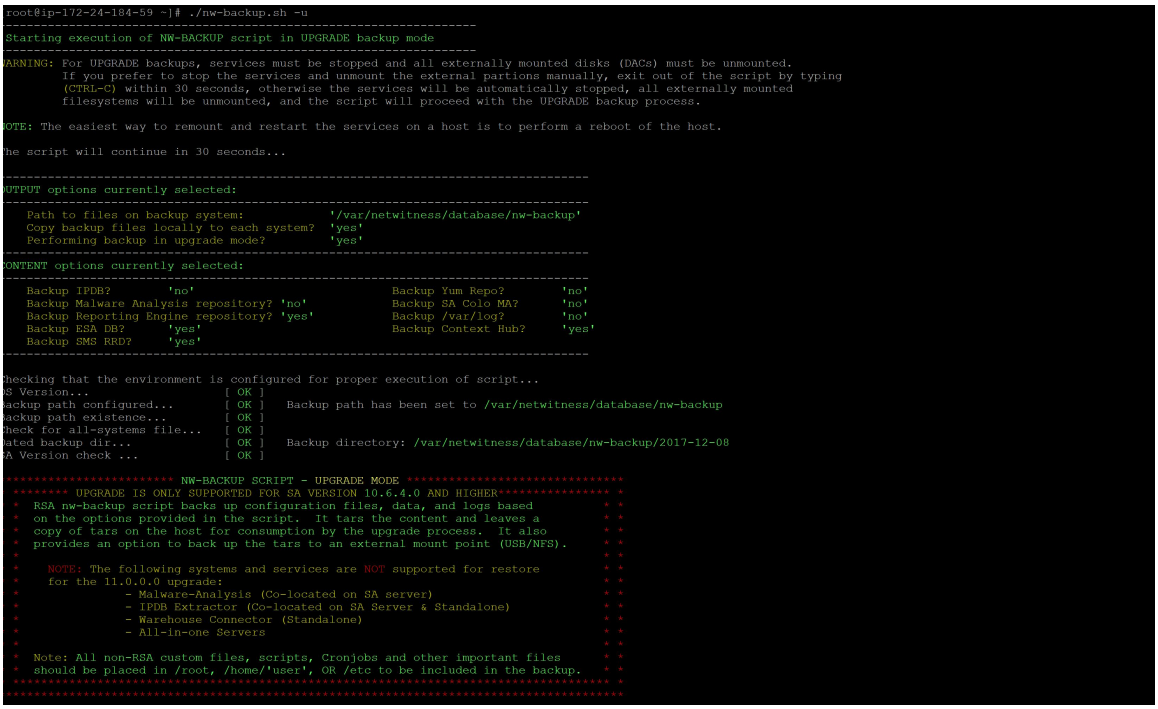
```
./get-all-systems.sh <SA server-IP>
```

```
./ssh-propagate.sh <path-to-backup-directory/all-systems>
```

```
./nw-backup.sh -u
```

Puede copiar un respaldo de los conjuntos tar creados en `/var/netwitness/database` en alguna ubicación segura (no es obligatorio).

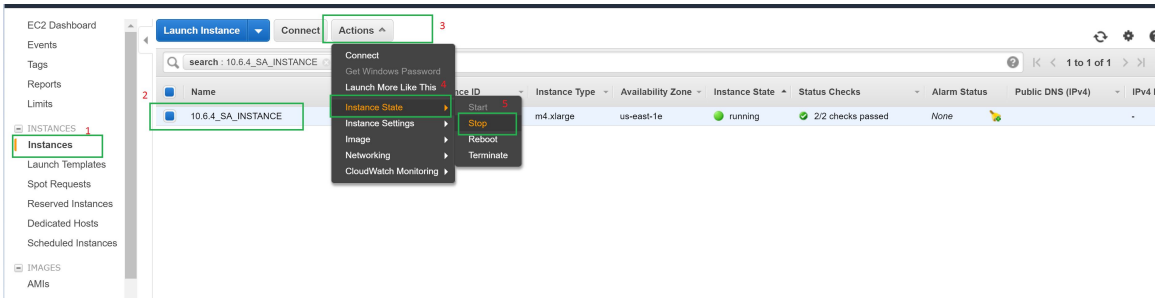
Antes de iniciar el proceso de restauración, si dispone de la implementación de ESA, copie los archivos `<hostname>-<IP>-controldata-mongodb.tar.gz` y `<hostname>-<IP>-controldata-mongodb.tar.gz.sha256` de la ubicación `/opt/rsa/database/nw-backup` de la VM de ESA en la ubicación `/var/netwitness/database/nw-backup/` de la VM de SA.



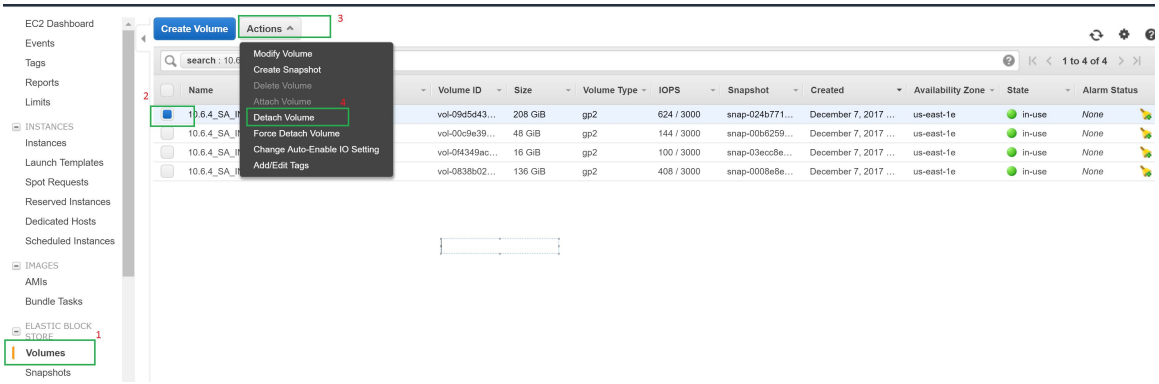
Tarea 3. Parar las instancias y desconectar los volúmenes de instancias de 10.6.4.x

Nota: Si falla la desconexión de algún volumen, fuércela en él.

Seleccione la instancia de EC2 10.6.4.x, desplácese a Acciones y haga clic en Detener.



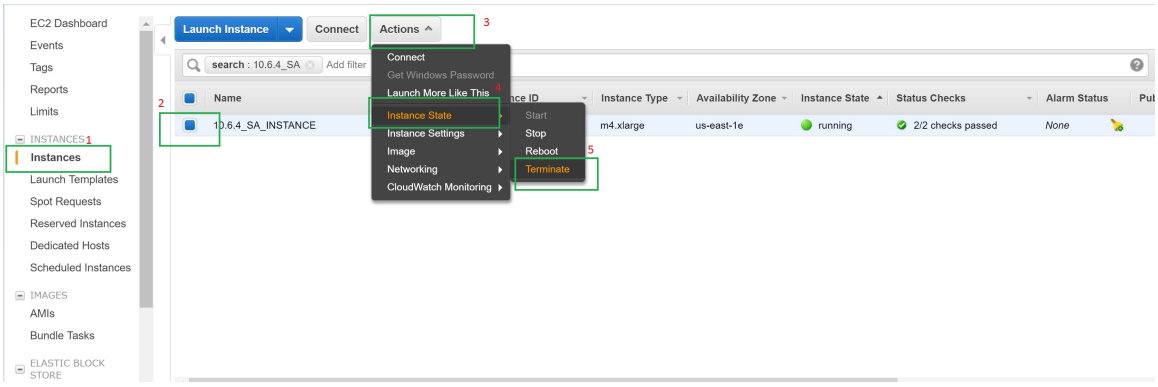
Haga clic en Volúmenes y seleccione los volúmenes de las instancias de 10.6.4.x que deben desconectarse; a continuación, en Acciones, seleccione Desconectar volumen.


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
1
Create Volume
Actions
3
Modify Volume
Create Snapshot
Delete Volume
Attach Volume
4
Detach Volume
Force Detach Volume
Change Auto-Enable IO Setting
Add/Edit Tags
2
1 to 4 of 4
Name
Volume ID
Size
Volume Type
IOPS
Snapshot
Created
Availability Zone
State
Alarm Status
vol-09d5d43…
208 GiB
gp2
624 / 3000
snap-024b771…
December 7, 2017 …
us-east-1e
in-use
None
vol-00c9e39…
48 GiB
gp2
144 / 3000
snap-00b6259…
December 7, 2017 …
us-east-1e
in-use
None
vol-0f4349ac…
16 GiB
gp2
100 / 3000
snap-03ecc8e…
December 7, 2017 …
us-east-1e
in-use
None
vol-0838b02…
136 GiB
gp2
408 / 3000
snap-0008e8e…
December 7, 2017 …
us-east-1e
in-use
None

Tarea 4. Anotar las direcciones IP de las instancias de 10.6.4.x y, a continuación, terminar las instancias de EC2

Nota: Es precisa la terminación para liberar la dirección IP.

1. Haga clic en Instancias y, a continuación, seleccione la instancia.
2. Haga clic en Acciones y navegue hasta Estado de la instancia.
3. Haga clic en Finalizar.

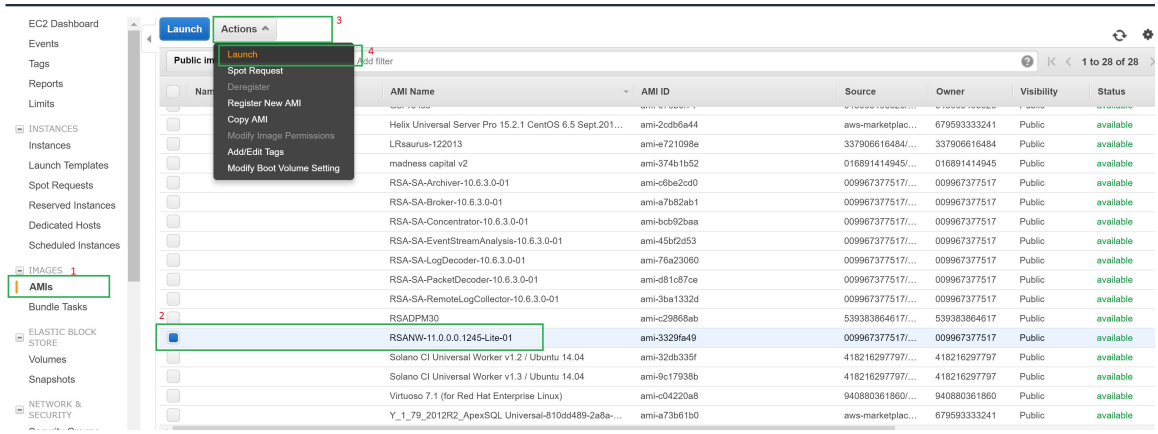


Tarea 5. Crear instancias de 11.0 mediante AMI de 11.0 (retención de IP)

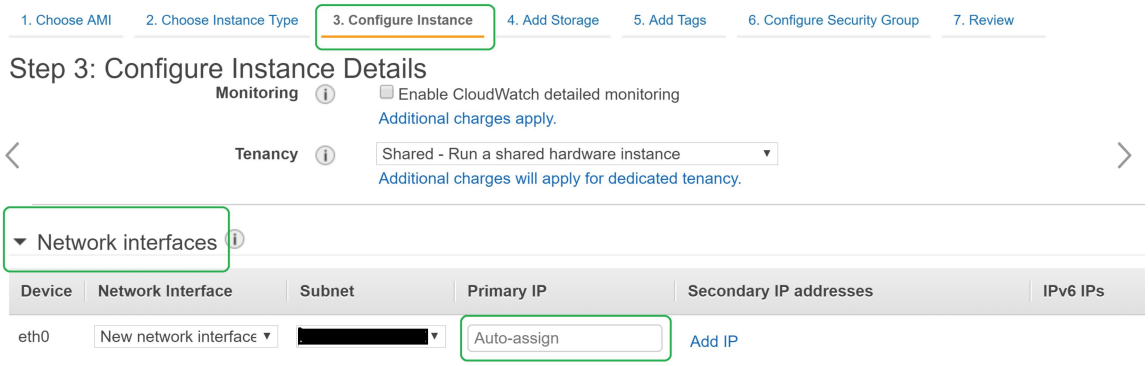
1. Durante la creación de la instancia de EC2, proporcione la dirección IP de la tarea 4. Haga clic en AMI y seleccione AMI 11.0.

Nota: Para instalar RSA NetWitness Suite 11.0.0.0, consulte la *Guía de implementación de AWS para la versión 11.0.*

2. Haga clic en Acciones y, a continuación, en Iniciar.



3. Asigne la IP conservada a las instancias adecuadas (retención de IP). Por ejemplo, si la IP de la instancia 10.6.4.xSA es 172.24.184.63, asigne la misma IP (172.24.184.63) a la instancia 11.0.



Nota: Para implementar otros componentes que no sean NW, seleccione la imagen (RSANW-11.0.0.0.1245-Lite-01) que se encuentra disponible en la sección de AMI de la comunidad.

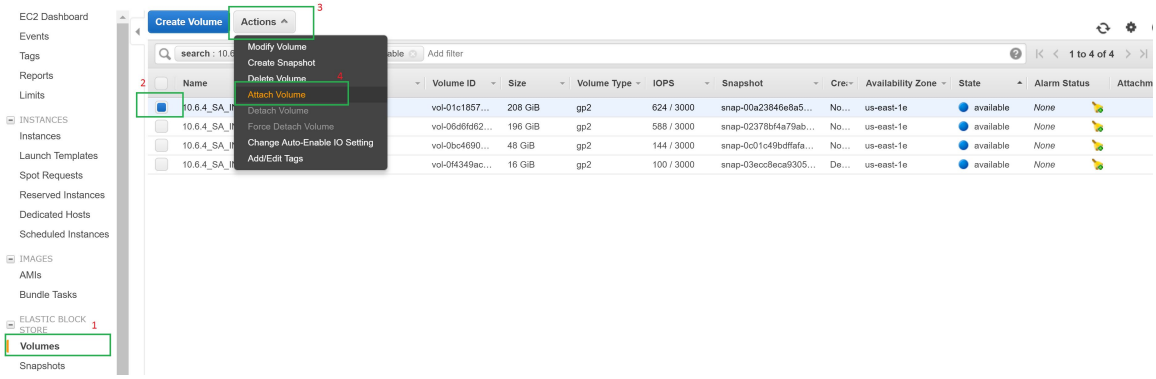
Tarea 6. Conectar los volúmenes a la instancia de 11.0 que corresponda

Después de implementar la instancia de NW 11.0, pare la instancia 11.0 y conecte los volúmenes 10.6.4.x disponibles (excepto “Disco del SO”) a las instancias 11.0.

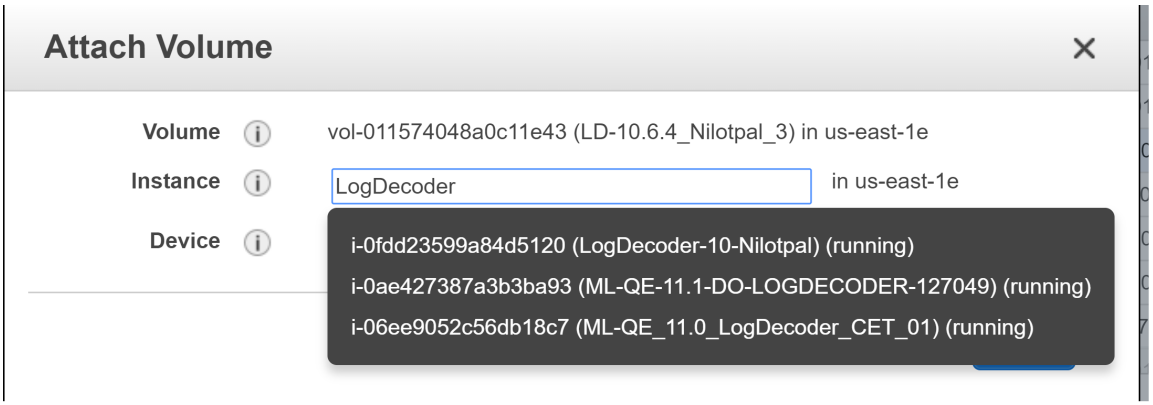
1. Haga clic en Volumes.

2. Seleccione el volumen de la instancia 10.6.4.x que debe conectarse.

3. Haga clic en Acciones y, a continuación, seleccione Conectar volumen.



4. Ingrese el ID de la instancia 11.0 a la que debe conectarse el volumen.



5. Encienda todas las instancias 11.0 cuando estén conectados todos los discos.

Tarea 7. Restaurar los datos de respaldo de 10.6.4.x en las instancias de 11.0 (restauración de datos)

Ejecute los pasos siguientes para copiar los datos de respaldo en SA, LC/LD, PD, Concentrator, Archiver y Broker:

1. Cree un directorio en `/tmp/` con el nombre `nwhome`.
2. Monte `VolGroup00-nwhome` en `/tmp/nwhome/` y asegúrese de que esté presente el directorio `/var/netwitness/database/`.

```
mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

3. Copie el contenido del directorio `/tmp/nwhome/` en `/var/netwitness/`.
4. Desmonte `VolGroup00-nwhome` de `/tmp/nwhome/`.

```
umount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

Siga estos pasos para **ESA**:

1. Cree un directorio en `/tmp/` con el nombre `apps`.
2. Monte `VolGroup01-apps` temporalmente en `/tmp/apps/`:

```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
```

3. Copie el directorio `nw-backup` de aquí en `/var/netwitness`:

```
cp /tmp/apps/database/nw-backup /var/netwitness
```

4. Desmonte `VolGroup01-apps` de `/tmp/apps/`.

```
umount /dev/mapper/VolGroup01-apps /tmp/apps
```

Agregue las entradas siguientes a `/etc/fstab` para `mounts`(montaje de discos):

Para **SA**:

```
/dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs
defaults,noatime,nosuid 1 2
```

Para **LogDecoder o LogCollector**:

```
/dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb
xfs defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb xfs
defaults,noatime,nosuid 1 2
```

Para **PacketDecoder**:

```
dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb xfs
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb xfs
defaults,noatime,nosuid 1 2
```

Para **Concentrator**:

```
/dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4
defaults,noatime,nosuid 1 2

/dev/mapper/VolGroup01-sessiondb /var/netwitness/concentrator/sessiondb
xfs defaults,nosuid,noatime 1 2

/dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs
defaults,noatime,nosuid 1 2
```

```
/dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb xfs
defaults,noatime,nosuid 1 2
```

Para **Archiver**:

```
/dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs
defaults,nosuid,noatime 1 2
```

```
/dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs
defaults,nosuid,noatime 1 2
```

Para **Broker**:

```
/dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
defaults,nosuid,noatime 1 2
```

Tarea 8. Reiniciar el dispositivo y ejecutar el script nwsetup-tui

Nota: Después del inicio, proporcione los nombres de host adecuados para todas las instancias 11.0. (Para saber los nombres de las instancia 10.6.4.x, consulte el archivo all-systems-master-copy, que contiene los nombres de las instancias 10.6.4.x con la dirección IP).

Ejecute este comando para configurar el nombre de host: `hostnamectl set-hostname <hostname>`.

Inicie sesión en la CLI del servidor de SA y ejecute el script `nwsetup-tui` para que se complete el resto del proceso.

Ejecute “nwsetup-cli” en el resto de los componentes para realizar el encendido y la coordinación. Para obtener más información, consulte la sección Configurar hosts virtuales en 11.0.

Configurar hosts virtuales en 11.0

Existen dos fases para configurar la plataforma virtual 11.0 que debe completar en el orden en que se muestran.

- Fase 1: Configurar los hosts del servidor de NW, Event Stream Analysis, Malware Analysis y Broker o Concentrator

  Nota: Para Event Stream Analysis, si tiene módulos C2 habilitados en 10.6.4.x, los módulos ingresarán a un período de preparación después de actualizar el servicio Event Stream Analysis a 11.0 y no estarán disponibles hasta que este período se complete.

- Fase 2: Configurar el resto de los hosts de componentes

Fase 1: Configurar los hosts del servidor de NW, Event Stream Analysis, Malware Analysis y Broker o Concentrator

Tarea 1: Configurar Servidor de NetWitness 11.0

Siga las instrucciones de Configurar un host del servidor de NW 11.0.

Tarea 2: Configurar ESA 11.0

Precaución: Si tiene módulos C2 habilitados en 10.6.4.x, los módulos ingresarán a un período de preparación después de actualizar el servicio Event Stream Analysis a 11.0 y no estarán disponibles hasta que este período se complete.

Siga las instrucciones de Configurar un host que no es de servidor de NW 11.0 para configurar los hosts de ESA.

1. Configure el host de ESA primario a través del programa de instalación e instale **ESA primario** en el host en la interfaz del usuario en la vista **Hosts de Admin**.

   Nota: Si tiene múltiples hosts de ESA en su empresa, primero debe actualizar el host de ESA primario, donde se encuentran todos los archivos tar de respaldo `mongodb` (base de datos de Mongo) antes de actualizar los hosts de ESA secundario.

2. (Condicional) Si tiene un host de ESA secundario, configúrelo a través del programa de instalación e instale **ESA secundario** en el host en la interfaz del usuario en la vista **Hosts de Admin**.

Tarea 3: Configurar Malware Analysis 11.0

Siga las instrucciones de Configurar un host que no es de servidor de NW 11.0.

Tarea 4: Configurar Broker o Concentrator 11.0

Siga las instrucciones de Configurar un host que no es de servidor de NW 11.0.

Nota: Si no tiene un Broker, actualice los hosts de Concentrator. El servidor de NW 11.0 no se puede comunicar con los servicios principales de 10.6.4.x para la nueva funcionalidad Investigate. Es por esto que debe actualizar los hosts de Broker o Concentrator en la fase 1.

Fase 2: Configurar el resto de los hosts de componentes

Consulte Apéndice B. Detención y reinicio de la captura y la agregación de datos para obtener instrucciones sobre cómo parar y reiniciar la captura y la agregación de datos cuando se actualizan los hosts de Decoder, Concentrator y Log Collection.

Hosts de Decoder y Concentrator

1. Detenga la captura y la agregación de datos.
2. Realice los pasos de Configurar un host que no es de servidor de NW 11.0.
3. Reinicie la captura y la agregación de datos.

Host de Log Decoder

1. Asegúrese de haber preparado Log Collector como se describe en *Log Collectors (LC) y Virtual Log Collectors (VLC): Ejecute prepare-for-migrate.sh* en **Instrucciones para respaldo**.
2. Detenga la captura de datos en Log Decoder.
3. Realice los pasos de Configurar un host que no es de servidor de NW 11.0.
4. Reinicie la captura de datos en Log Decoder.

Nota: Después de la actualización, reiniciará la recopilación de registros tras completar la Tarea 11: Restablecer valores de sistema estables para Log Collector después de la actualización en **Tareas posteriores a la actualización**.

Host de Virtual Log Collector

1. Asegúrese de haber preparado Virtual Log Collector como se describe en *Log Collectors (LC) y Virtual Log Collectors (VLC): Ejecute prepare-for-migrate.sh*.
2. Respalde su VLC 10.6.4.x mediante la edición del archivo `all-systems` en el host donde

se realizó el respaldo.

a. Asegúrese de que el contenido del archivo `all-systems` tenga esta información antes de realizar este paso.
`vlc,<host-name>,<IP-address>,<UUID>,10.6.4.0`

b. Ejecute el siguiente comando para crear un respaldo.
`./nw-backup.sh -u`
Consulte Instrucciones para respaldo para conocer los procedimientos detallados sobre cómo respaldar el host.

3. Asegúrese de que el host de respaldo contenga el respaldo del VLC en el siguiente formato.
`<hostname>-<IPaddress>-root.tar.gz`
`<hostname>-<IPaddress>-root.tar.gz.sha256`
`<hostname>-<IPaddress>-backup.tar.gz`
`<hostname>-<IPaddress>-backup.tar.gz.sha256`
`<hostname-IPaddress>-network.info.txt`
`all-systems-master-copy`

4. Apague el VLC 10.6.4.x, de modo que se pueda crear una nueva VM 11.0 con la misma configuración de red.

5. Implemente un host que no es de servidor de NW nuevo mediante el OVA de NetWitness Suite 11.0.

6. Conéctese a la consola de VM del VLC nuevo.

7. Actualice la configuración de red para que sea la misma que la del VLC 10.6.4.x. Esta información se almacena en el archivo de respaldo del VLC `<hostname-IPaddress>-network.info.txt` 10.6.4.x.

Nota: Asegúrese de que IPv6 esté deshabilitado.

a. Edite el archivo `/etc/sysconfig/network-scripts/ifcfg-eth0` y actualice la configuración. El contenido de `ifcfg-eth0` debe ser el siguiente.
```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
```

```
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

b. Ejecute la siguiente cadena de comandos.

```
systemctl restart network.service
```

8. Cree el directorio de respaldo.

```
# mkdir -p /var/netwitness/database/nw-backup/
```

9. Copie el respaldo del host de respaldo desde `/var/netwitness/database/nw-backup` al VLC nuevo en el directorio `/var/netwitness/database/nw-backup`.

10. Complete los pasos 2 al 12, ambos inclusive, en Configurar un host que no es de servidor de SA 11.0 para el resto de los componentes de NetWitness Suite. Asegúrese de seleccionar **Log Collector** para el servicio en el paso 12.

Configurar un host del servidor de NW 11.0

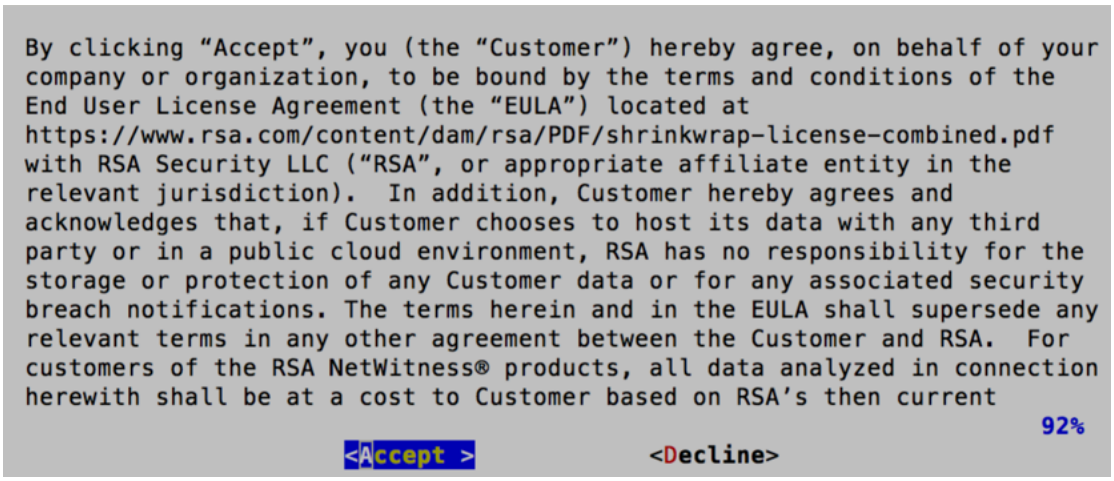
Asegúrese de haber respaldado los datos de 10.6.4.x para el host del servidor de SA. **Debe seguir las instrucciones de** Instrucciones para respaldo **para respaldar el host.**

Precaución: Ejecute el respaldo inmediatamente antes de actualizar el servidor de SA a 11.0, de modo que los datos sean lo más recientes posible. Debe crear el archivo **all-systems** antes de actualizar el servidor de SA, porque no podrá hacer esto después de que el servidor de SA se haya actualizado a 11.0.

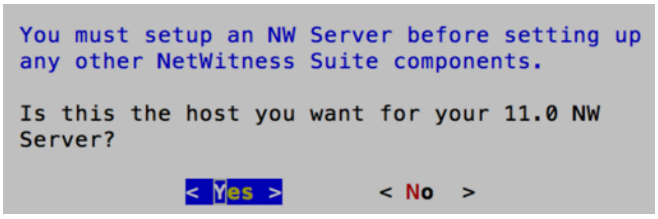
Realice los siguientes pasos para configurar el host del servidor de NW 11.0.

1. Encienda la VM del servidor de NW y ejecute el comando `nwsetup-tui`.
   Esto inicia el programa de instalación y se muestra el EULA.

Nota: 1.) Cuando navegue por los indicadores del programa de instalación, use las flechas hacia abajo y hacia arriba para desplazarse entre los campos y use la tecla de tabulación para desplazarse hacia y desde los comandos (como **<Sí>**, **<No>**, **<Aceptar>** y **<Cancelar>**). Presione la tecla Intro para registrar la respuesta de los comandos y moverse al siguiente indicador.
2.) El programa de instalación adopta la combinación de colores del escritorio o de la consola que usa para acceder al host.

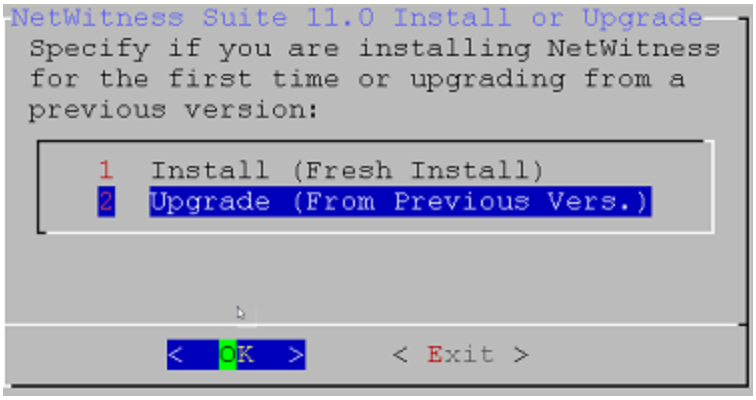


2. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador "Este es el servidor de NW".



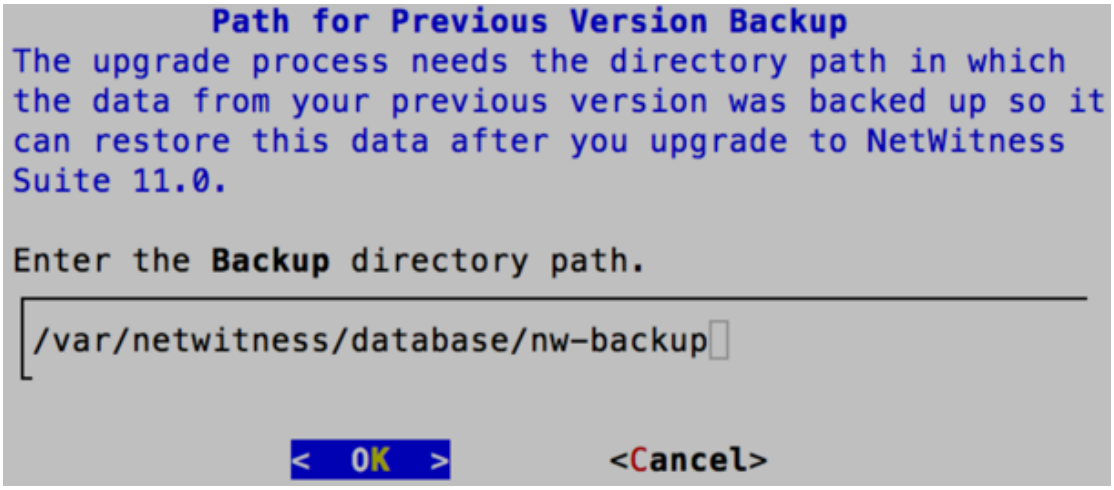
Precaución: Si elige el host incorrecto para el servidor de NW y completa la actualización, debe repetir los pasos 1 al 11 de Configurar un host del servidor de NW 11.0 para corregir este error.

3. Use la tecla de tabulación para ir a **Sí** y presione **Intro**.
   Elija No si ya actualizó el servidor de NW a 11.0.
   Se muestra el indicador Instalar o Actualizar.



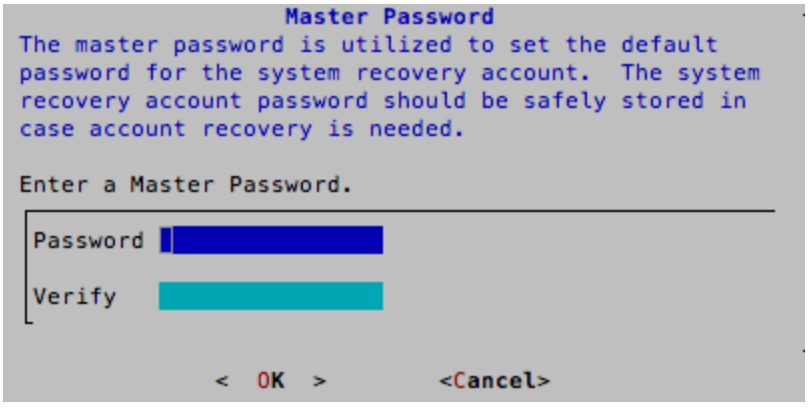
4. Use la flecha hacia abajo para seleccionar **2 Actualizar (de versión anterior)**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

Se muestra el indicador de ruta de respaldo.



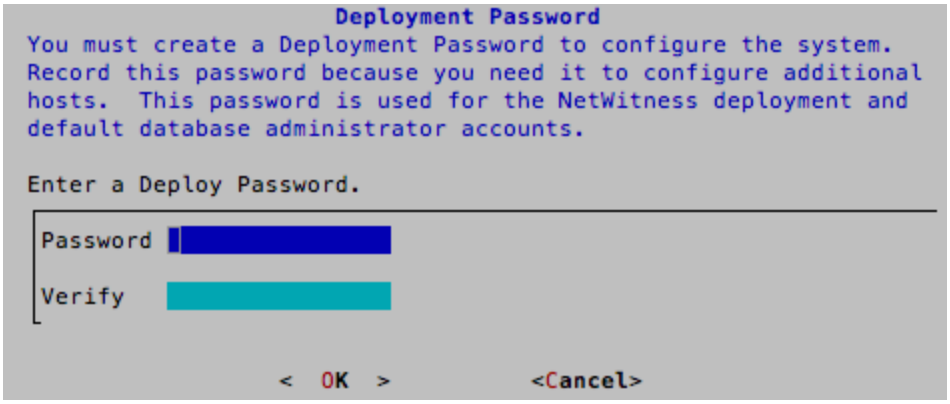
5. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro** si desea mantener esta ruta. Si no desea hacerlo, edite la ruta, use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para cambiarla.
   Se muestra el indicador Contraseña maestra.
   Los caracteres de la siguiente lista son compatibles para Contraseña maestra y Contraseña de implementación:
   - Símbolos: ! @ # % ^ +
   - Números: 0-9
   - Caracteres en minúscula: a-z
   - Caracteres en mayúscula: A-Z

   Ningún carácter ambiguo es compatible para Contraseña maestra y Contraseña de implementación (por ejemplo: espacio { } [ ] ( ) / \ ' " ` ~ , ; : . < > -).

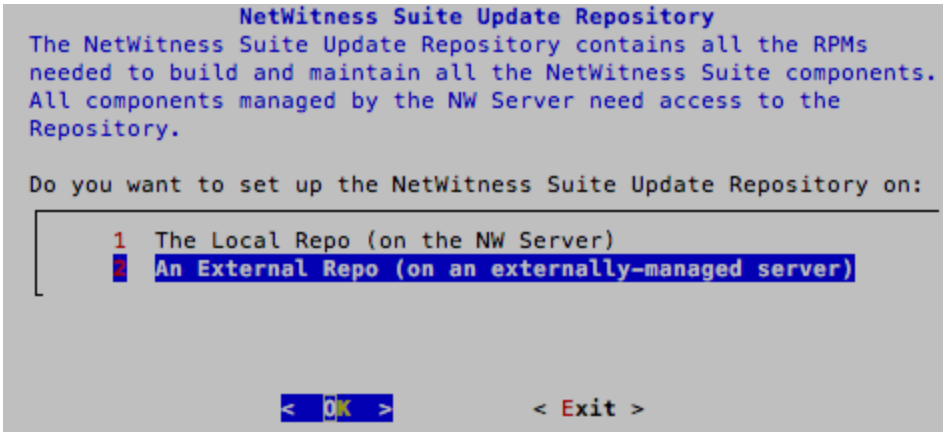


6. Escriba la **Contraseña**, use la flecha hacia abajo para desplazarse hasta **Verificar**, vuelva a escribir la contraseña, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

Se muestra el indicador Contraseña de implementación.

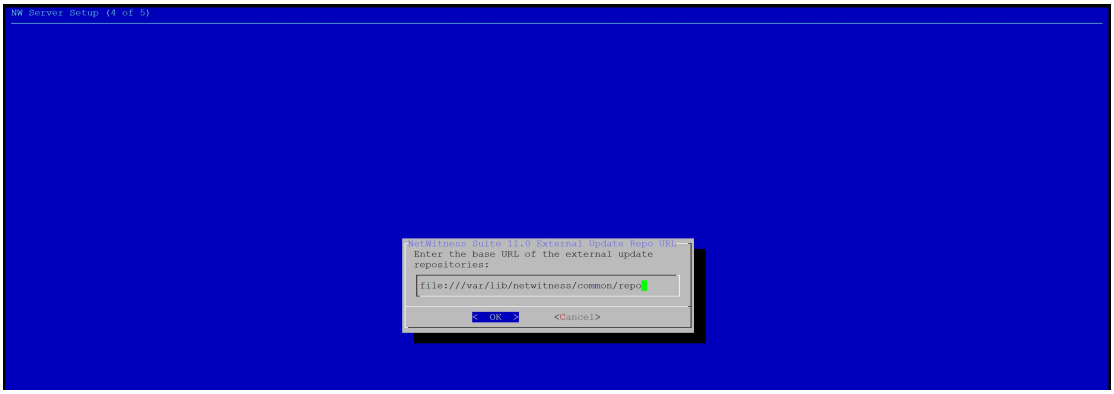


7. Escriba la **Contraseña**, use la flecha hacia abajo para desplazarse hasta **Verificar**, vuelva a escribir la contraseña, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador Repositorio de actualizaciones.



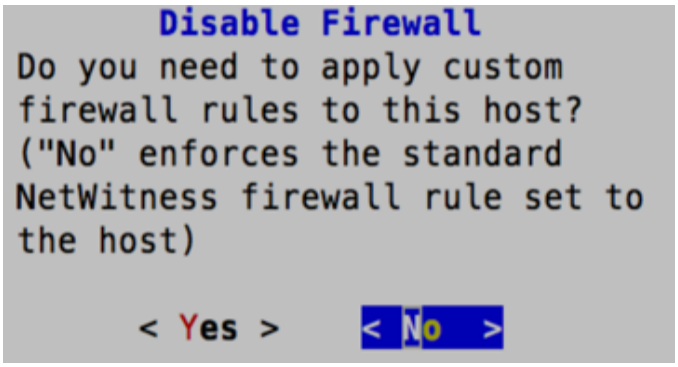
   Debe usar para todos los hosts el mismo repositorio que usó para los hosts del servidor de NW.

8. Use las flechas hacia abajo y hacia arriba para seleccionar **2 Un repositorio externo (en un servidor administrado externamente)**; la interfaz del usuario le solicita que indique una dirección URL.



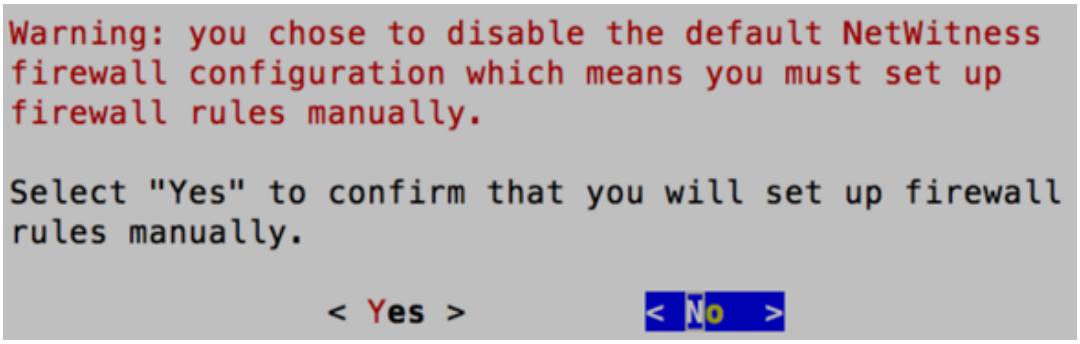
Consulte “Configurar un repositorio externo con actualizaciones de RSA y del SO” en “Procedimientos de hosts y servicios” en la *Guía de introducción de hosts y servicios de RSA NetWitness Suite 11.0* para obtener instrucciones. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

9. Ingrese la dirección URL base del repositorio externo de NetWitness Suite y haga clic en **Aceptar**.
   Se muestra el indicador de deshabilitación o uso de la configuración del firewall estándar.



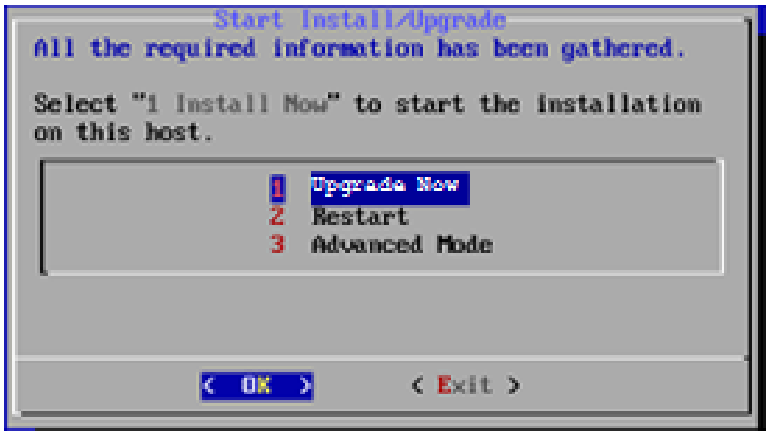
10. Use la tecla de tabulación para ir a **No** y presione **Intro** para usar la configuración del firewall estándar. Use la tecla de tabulación para ir a **Sí** y presione **Intro** para deshabilitar la configuración del firewall estándar.

    - Si selecciona Sí, confirme su selección.



    - Si selecciona No, se aplica la configuración del firewall estándar.

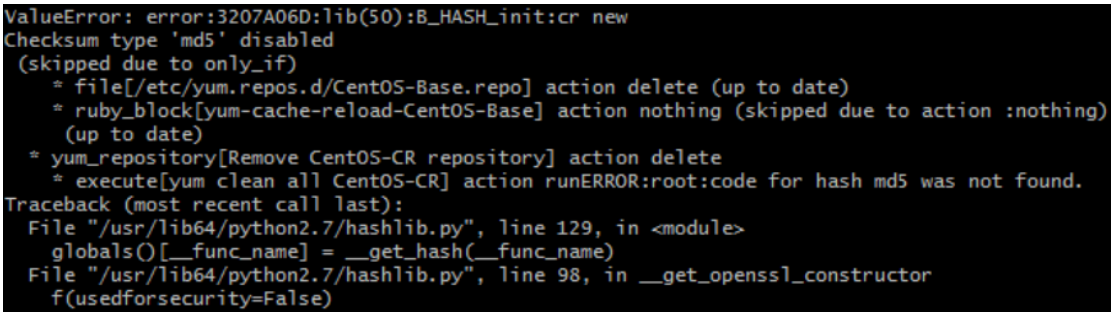
Se muestra el indicador Iniciar actualización.



11. Seleccione 1 **Actualizar ahora**, use la tecla de tabulación para ir a **Aceptar** y presione Intro.

    Cuando se muestra “Instalación completa”, ya actualizó el servidor de SA 10.6.4.x al servidor de NW 11.0.

> **Nota:** Pase por alto los errores de código hash similares a los errores que se muestran en la siguiente captura de pantalla que aparecen cuando inicia el comando `nwsetup-tui`. Yum no usa MD5 para ninguna de las operaciones de seguridad, de modo que no afectan la seguridad del sistema.



Configurar un host que no es de servidor de NW 11.0

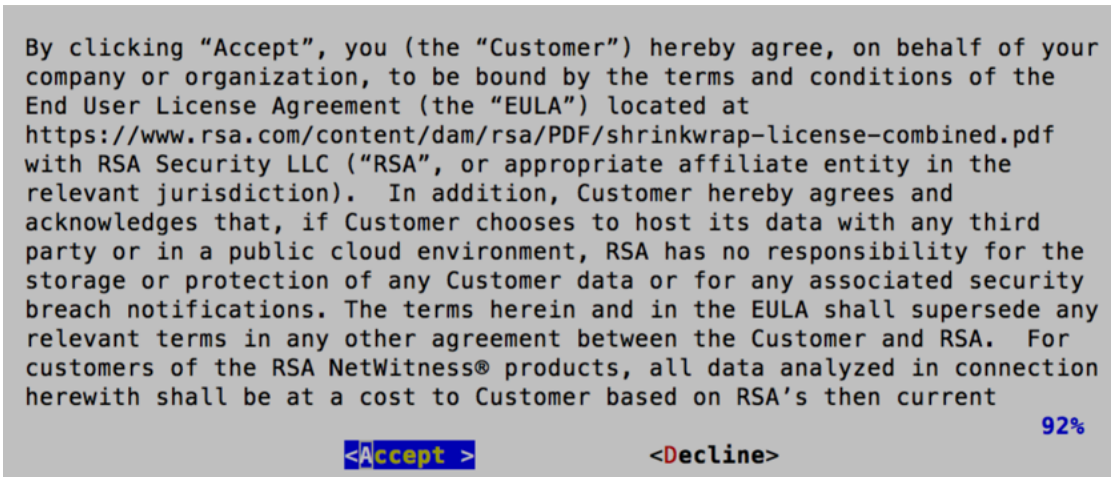
Asegúrese de respaldar los datos de 10.6.4.x para el host. **Debe seguir las instrucciones de** Instrucciones para respaldo **para respaldar el host.**

> **Precaución:** Ejecute el respaldo inmediatamente antes de actualizar el host a 11.0, de modo que los datos sean lo más recientes posible.

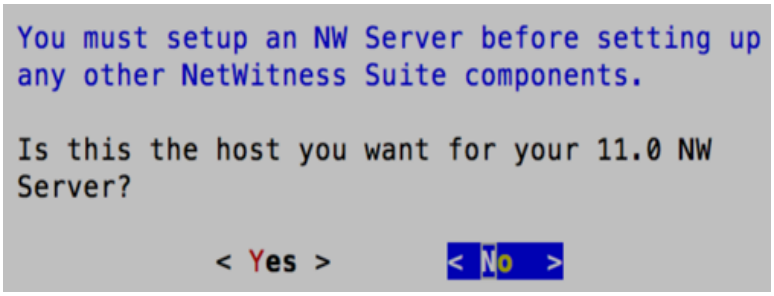
Realice los siguientes pasos para configurar un host que no es de servidor de NW 11.0.

1. **Encienda** la VM que no es de servidor de NW y ejecute el comando `nwsetup-tui`.

   Esto inicia el programa de instalación y se muestra el EULA.

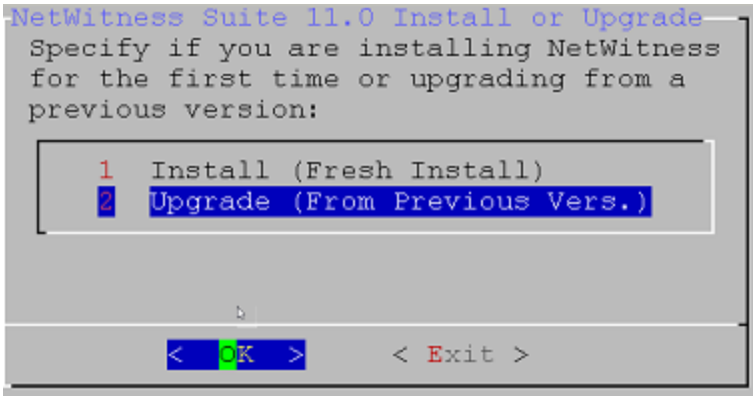


2. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador "Este es el servidor de NW".



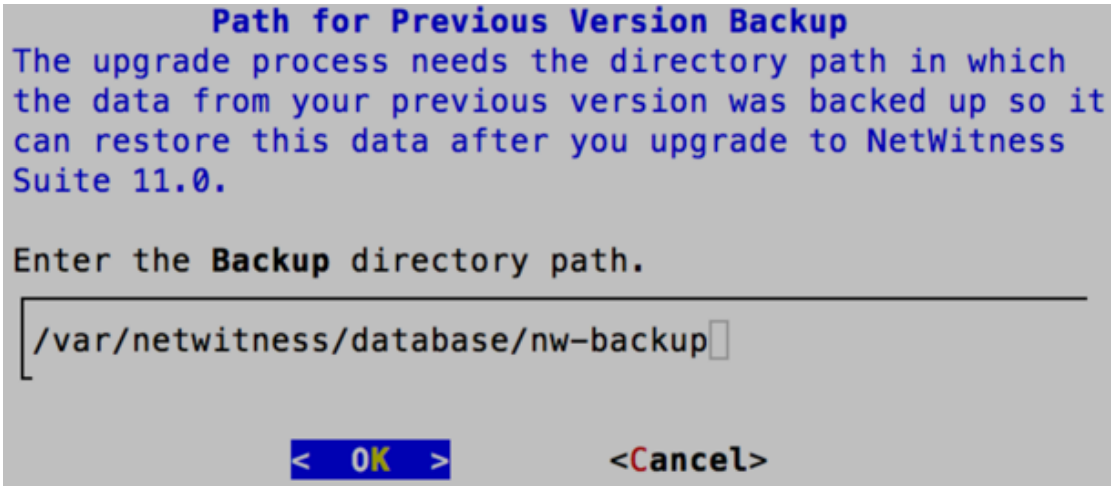
Precaución: Si elige el host incorrecto para el servidor de NW y completa la actualización, debe repetir los pasos 1 al 11 de Configurar un host del servidor de NW 11.0 para corregir este error.

3. Use la tecla de tabulación para ir a **No** y presione **Intro**.
   Se muestra el indicador Instalar o Actualizar.



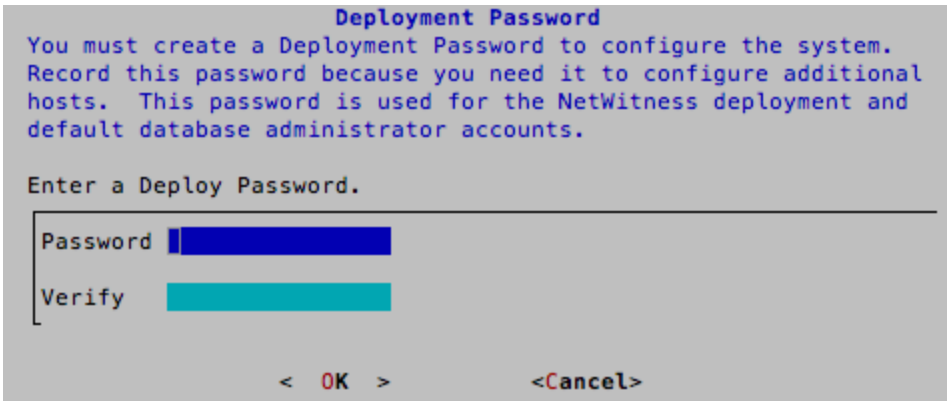
4. Use la flecha hacia abajo para seleccionar **2 Actualizar (de versión anterior)**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

Se muestra el indicador de ruta de respaldo.



5. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro** si desea mantener esta ruta. Si no desea hacerlo, edite la ruta, use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para cambiarla.

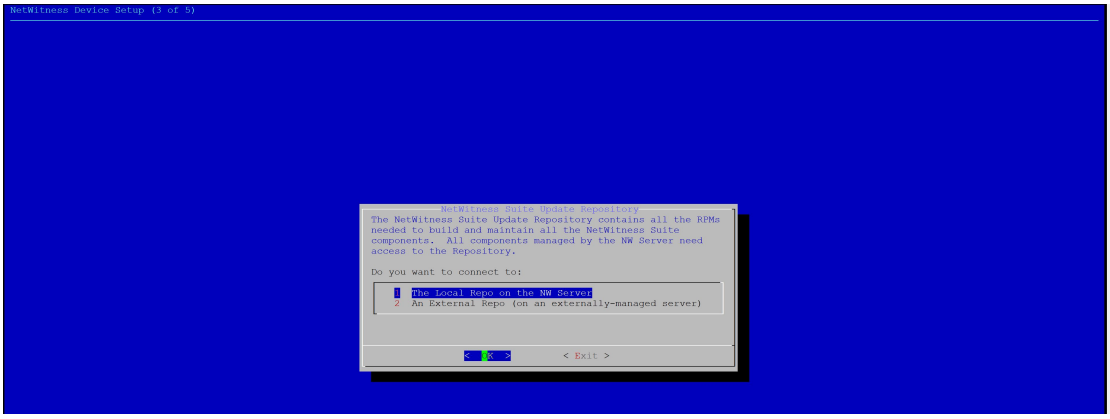
   Se muestra el indicador Contraseña de implementación.



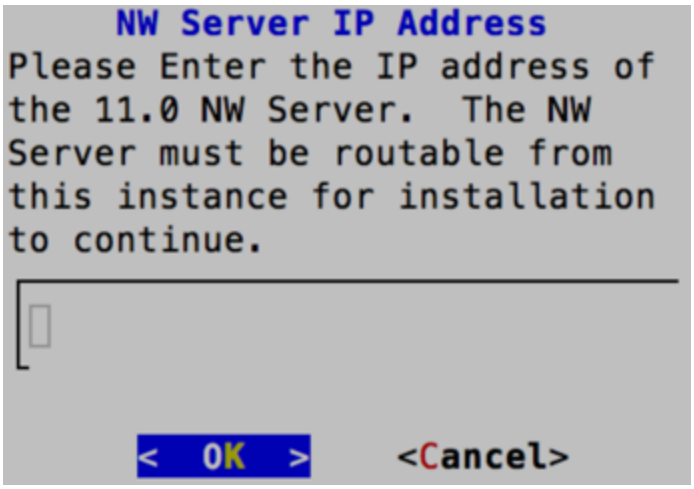
> **Nota:** Debe usar la misma contraseña de implementación que usó cuando actualizó el servidor de NW.

6. Escriba la **Contraseña**, use la flecha hacia abajo para desplazarse hasta **Verificar**, vuelva a escribir la contraseña, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

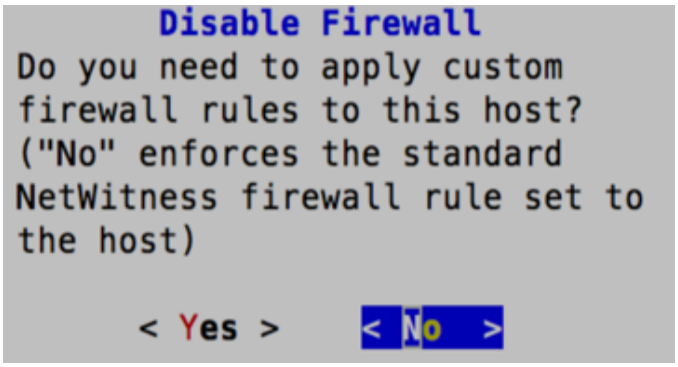
Se muestra el indicador Repositorio de actualizaciones.



7. Use las flechas hacia abajo y hacia arriba para seleccionar **1 El repositorio local (en el servidor de NW)**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
8. Se muestra la dirección IP del servidor de NW.

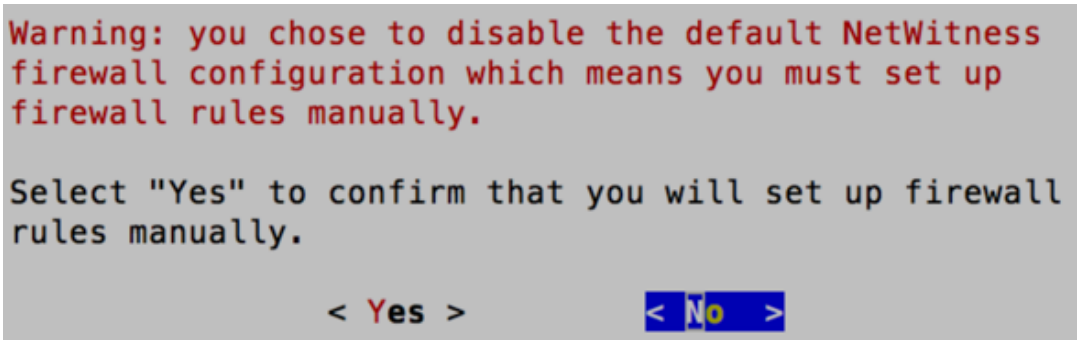


9. Escriba la dirección IP del servidor de NW, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador de deshabilitación o uso de la configuración del firewall estándar.



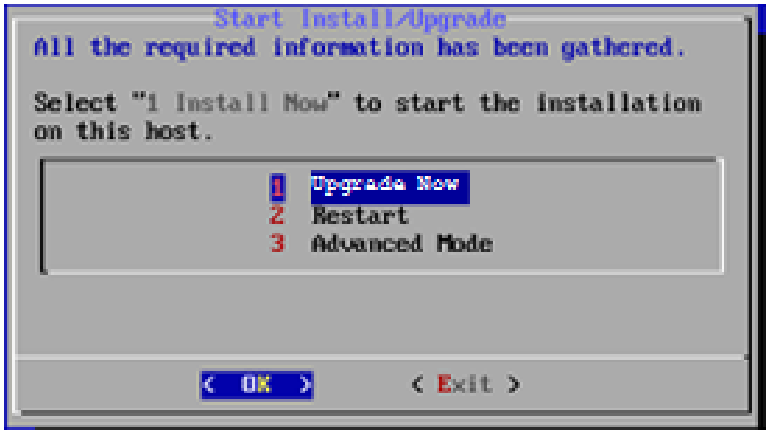
10. Use la tecla de tabulación para ir a **No** y presione Intro para usar la configuración del firewall estándar. Use la tecla de tabulación para ir a **Sí** y presione **Intro** para deshabilitar la configuración del firewall estándar.

    - Si selecciona **Sí**, confirme su selección.

    - Si selecciona **No**, se aplica la configuración del firewall estándar.

    Se muestra el indicador Iniciar actualización.

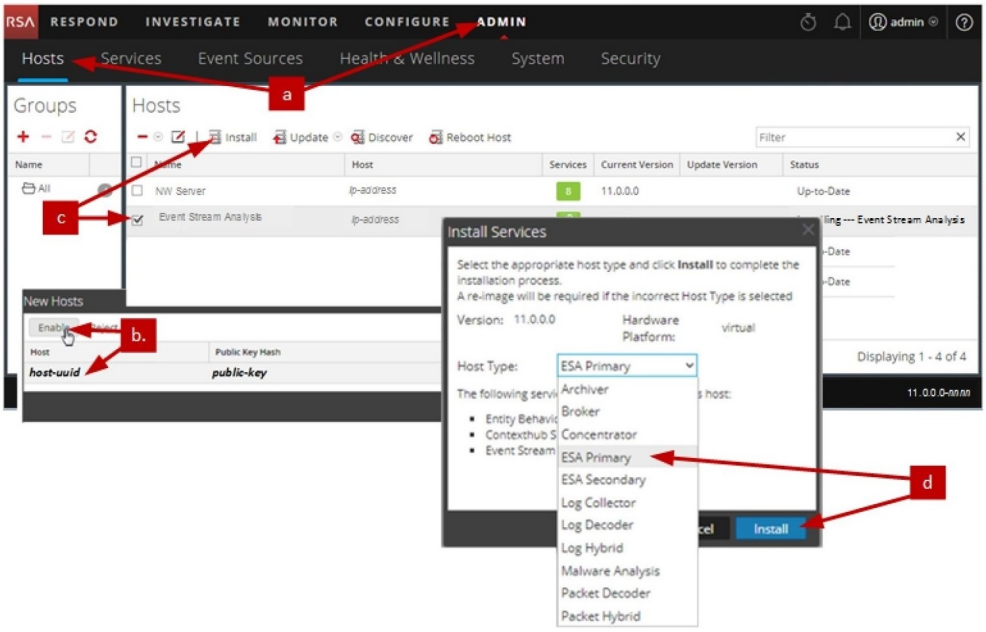
11. Seleccione 1 **Actualizar ahora**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

    Cuando se muestra “Instalación completa”, ya actualizó el host a 11.0.

Cuando el script “nwsetup-cli” se ejecute correctamente en todos los componentes, siga los pasos que aparecen a continuación para completar la actualización o la migración a NW 11.0:

1. Inicie sesión en NetWitness Suite. (Escriba `https://<NW-Server-IP-Address>/login` en el navegador para ir a la pantalla de conexión de NetWitness Suite).
2. Haga clic en ADMIN > Hosts. El cuadro de diálogo Nuevos hosts se muestra con la vista Hosts atenuada en segundo plano. Nota: Si no se muestra el cuadro de diálogo Nuevos hosts, haga clic en Descubrir en la barra de herramientas de la vista Hosts.

3. Haga clic en el host en el cuadro de diálogo Nuevos hosts y, a continuación, haga clic en Habilitar. El cuadro de diálogo Nuevos hosts se cierra y el host se muestra en la vista Hosts.
4. Seleccione ese host (por ejemplo, Event Stream Analysis) y haga clic en .Se muestra el cuadro de diálogo Instalar servicios.



Actualización o instalación de recopilaciones de Windows existentes

Consulte la *Guía de recopilación de Windows existente de RSA NetWitness 11.0* en RSA Link (https://community.rsa.com/docs/DOC-75593) para obtener detalles sobre cómo instalar o actualizar la recopilación de Windows existente.

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

En este tema se enumeran las tareas que debe completar después de actualizar los hosts de 10.6.4.x a 11.0. Estas tareas se organizan en las siguientes categorías.

- Global
- NetWitness Endpoint
  RSA solo admite las versiones 4.3.0.4, 4.3.0.5 y 4.4 de NetWitness Endpoint con NetWitness Suite 11.0.
- Event Stream Analysis
- Recopilación de registros
- Reporting Engine
- Respond
- NetWitness SecOps Manager
- Seguridad

Tareas globales

Tarea 1: Quitar los archivos relacionados con respaldo de los directorios locales de los hosts

Precaución: (1) Debe conservar una copia de todos los archivos de respaldo en un host externo. (2) Valide que restauró en 11.0 todos los datos desde su respaldo antes de quitar los archivos relacionados con el respaldo de los directorios locales de sus hosts 11.0.

Archivos `.tar` de respaldo

Después de que todos los hosts se actualizan a 11.0, debe quitar:

- los archivos de respaldo de los directorios locales de los hosts.
- todos los archivos de los directorios `nw-backup` y `restore` de los hosts.

Host	Ruta de respaldo	Ruta de restauración
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`

Host	Ruta de respaldo	Ruta de restauración
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
Servidor de NW	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
Todos los demás hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Tarea 2: Restaurar los servidores NTP

Debe usar la interfaz del usuario de NetWitness Suite 11.0 para restaurar las configuraciones del servidor NTP. La información de configuración del servidor NTP se encuentra en `$BUPATH/restore/etc/ntp.conf`. Use el nombre del servidor NTP y el nombre de host que aparecen en el archivo `/var/netwitness/restore/etc/ntp.conf`. Consulte "Configurar servidores NTP" en la *Guía de configuración del sistema* de *RSA NetWitness® Suite* 11.0 para obtener instrucciones detalladas sobre cómo agregar los servidores NTP. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Tarea 3: Restaurar licencias para ambientes sin acceso a FlexNet Operations On-Demand

Si su ambiente no tiene acceso a FlexNet Operations On-Demand, debe volver a descargar las licencias de NetWitness Suite. Consulte "Paso 1. Registrar el servidor de NetWitness" en la *Guía de administración de licencia de RSA NetWitness Suite* para obtener instrucciones sobre cómo volver a descargar las licencias. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

(Condicional) Tarea 5: Agregar tablas de IP personalizadas si deshabilitó la configuración del firewall estándar

Durante la actualización, tiene la opción de usar estas reglas o deshabilitarlas. Si las deshabilitó, siga estas instrucciones como una base para crear un conjunto de reglas de firewall administrado por el usuario en todos los hosts para los cuales se deshabilitó la configuración del firewall estándar.

Nota: Puede consultar `$BUPATH/restore/etc/sysconfig/iptables` y `$BUPATH/restore/etc/sysconfig/ip6tables` en la carpeta de restauración del respaldo para actualizar los archivos `ip6tables` y `iptables`. El archivo `/etc/netwitness/firewall.cfg` contiene las reglas estándares del firewall `iptables`.

1. Acceda mediante el protocolo SSH a cada host e inicie sesión con sus credenciales raíz.
2. Actualice los siguientes archivos `ip6tables` y `iptables` con las reglas de firewall personalizadas.
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```
3. Vuelva a cargar los servicios `iptables` y `ip6tables`.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Condicional) Tarea 6: Especificar puertos SSL si nunca configuró conexiones de confianza

Realice esta tarea solo si nunca configuró conexiones de confianza. Es probable que no haya configurado conexiones de confianza si:

- Usó la imagen ISO base para 10.3.2 o anterior.
- Actualizó el sistema mediante RPM exclusivamente para llegar a 10.6.4.

NetWitness Suite 11.0 no puede comunicarse con los servicios principales para estos clientes porque usan un puerto 500XX no SSL. Debe actualizar los puertos de servicio principales a un puerto SSL en el cuadro de diálogo Editar servicio.

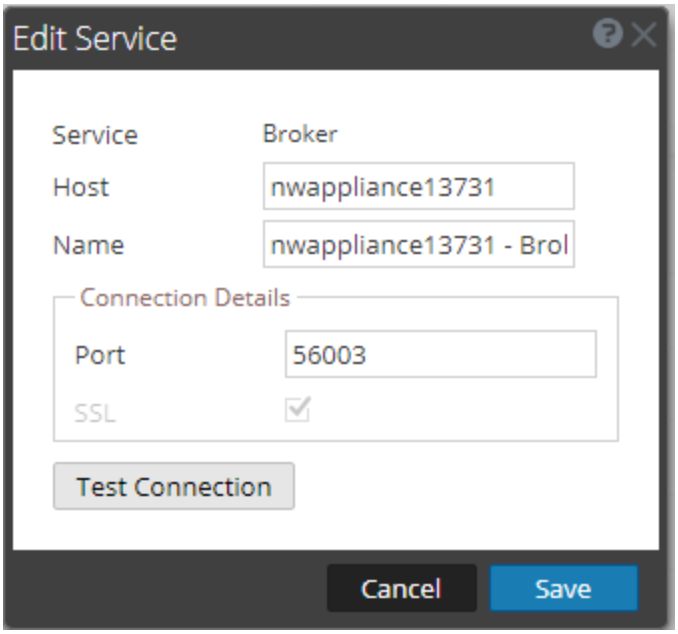
1. Inicie sesión en NetWitness Suite.
2. Vaya a **ADMIN** > **Servicios**.
3. Seleccione cada servicio principal y cambie ahí los puertos de puertos no SSL a puertos SSL.

Servicio	No SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

4. Haga clic en (Editar) en la barra de herramientas de la vista **Servicios**.

   Se muestra el cuadro de diálogo Editar servicio.

5. Cambie el puerto de No SSL a SSL, como se muestra en la tabla, y haga clic en **Guardar** (por ejemplo, cambie el puerto de Broker de 50003 a 56003).



NetWitness Endpoint

Tarea 7: Reconfigurar alertas de Endpoint mediante el bus de mensajes

1. En el servidor de NetWitness Endpoint, modifique la configuración del host virtual en el archivo `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` para que se refleje la siguiente configuración.
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Nota: En NetWitness Suite 11.0, el host virtual es `/rsa/system`. Para 10.6.4.x y versiones anteriores, el host virtual es `/rsa/sa`.

2. Reinicie el servidor de API y de la consola.
3. Acceda mediante el protocolo SSH al servidor de NW e inicie sesión con las credenciales `root`.
4. Ejecute el siguiente comando para agregar todos los certificados al almacén de confianza.
   `orchestration-cli-client --update-admin-node`
5. Ejecute el siguiente comando para reiniciar el servidor RabbitMQ.
   `systemctl restart rabbitmq-server`
   La cuenta de NetWitness Endpoint debe estar disponible en RabbitMQ de forma automática.
6. Importe los archivos `/etc/pki/nw/ca/nwca-cert.pem` y `/etc/pki/nw/ca/ssca-cert.pem` desde el servidor de NW y agréguelos a los almacenes de Certificación raíz de confianza en el servidor de Endpoint.

Tareas de Event Stream Analysis (ESA)

Tarea 8: Reconfigurar Detección de amenazas automatizadas para ESA

Si usó Detección de amenazas automatizadas en 10.6.4.x, debe completar los siguientes pasos para reconfigurarla mediante el servicio ESA Analytics en 11.0.

1. Inicie sesión en NetWitness Suite 11.0.
2. Haga clic en **ADMIN** > **Sistema** > **ESA Analytics**.
   Los módulos Suspicious Domains, Command and Control (C2) for Packets y C2 for Logs requieren una lista blanca denominada "**domains_whitelist**".
3. Condicional: Si aparece la lista blanca de Detección de amenazas automatizadas anterior en la pestaña **Listas** del servicio Context Hub:

a. Haga clic en **ADMIN**> **Servicios**, seleccione el servicio Context Hub y, en el menú desplegable de comandos de acción (), haga clic en la pestaña **Ver** > **Configuración** > **Listas**.

b. Cambie el nombre de la lista blanca de Detección de amenazas automatizadas anterior a "`domains_whitelist`" para el módulo Suspicious Domains.

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 la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Tarea 9: Para integraciones con Web Threat Detection, NetWitness SecOps Manager o NetWitness Endpoint, configurar SSL autenticado mutuamente

Si se integra con Web Threat Detection, NetWitness SecOps Manager o NetWitness Endpoint, debe configurar SSL autenticado mutuamente en cada sistema integrado, de modo que la aplicación pueda autenticarse a sí misma en el momento de conectarse al bus de mensajes de RabbitMQ.

Nota: Use los nombres de usuario y las contraseñas de RabbitMQ que se obtuvieron cuando respaldó los datos de 10.6.4.x (consulte Instrucciones para respaldo).

1. Cree un usuario en el sistema del host que debe integrarse con NetWitness Suite iniciando sesión en el host y ejecutando el siguiente comando `rabbitmqctl`.

   ```
   > rabbitmqctl add_user <username> <password>
   ```

   Por ejemplo:

   ```
   > rabbitmqctl add_user wtd-incidents incidents
   ```

2. Configure permisos para los usuarios mediante la ejecución del siguiente comando (use el nombre de usuario del paso 1):

   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*", ".*"
   ```

   Por ejemplo:

   ```
   > rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*", ".*", ".*"
   ```

Tarea 10: Habilitar el Tablero Amenaza: Indicadores de malware

En 11.0.0, el nombre **Tablero Amenaza: Indicadores** de 10.6.4.x se cambió a **Tablero Amenaza: Indicadores de malware**. Si usó este tablero en 10.6.4.x, debe:

1. Habilitar el **Tablero Amenaza: Indicadores de malware** en 11.0.
2. Configurar el origen de datos para los dashlets nuevos.

   Consulte "Dashlets" en RSA Link (https://community.rsa.com/docs/DOC-81463).

Recopilación de registros

Tarea 11: Restablecer valores de sistema estables para Log Collector después de la actualización

Realice las siguientes tareas para restablecer los valores de sistema estables para el Log Collector después de actualizarlo a 11.0 para asegurarse de que todos los protocolos de recopilación reanuden la operación normal.

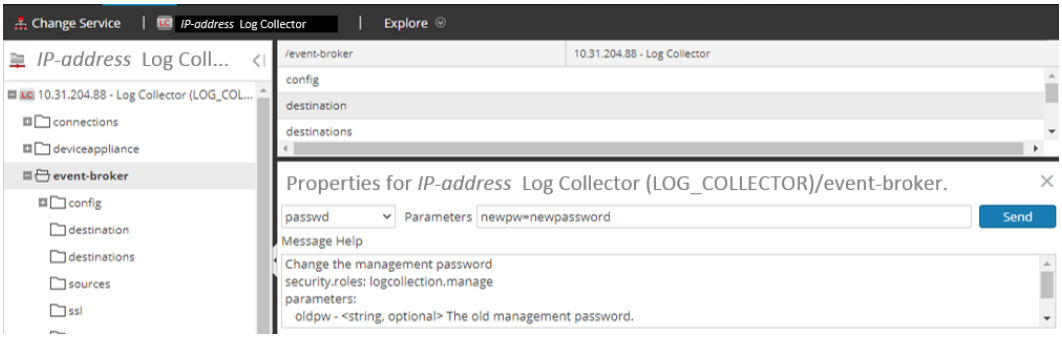
Restablecer valores de sistema estables para Lockbox

El Lockbox almacena la clave para cifrar el origen de eventos y otras contraseñas para el Log Collector. El servicio Log Collector no puede abrir el Lockbox debido a los cambios de los valores de sistema estables. Como resultado, debe restablecer los valores de sistema estables para Lockbox. Consulte "Recopilación de registros: Paso 3. Configurar un Lockbox" en la *Guía de configuración de la recopilación de registros* de *RSA NetWitness® Suite* para obtener instrucciones.Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Actualizar la contraseña de la cuenta de usuario de RabbitMQ del servicio Log Collector

Si se cambió la contraseña de la cuenta de usuario de RabbitMQ del servicio logcollector, debe volver a ingresarla después de la actualización a 11.0.

1. Inicie sesión en NetWitness Suite.
2. Haga clic en **ADMIN > Servicios**.
3. Seleccione el servicio Log Collector.
4. Haga clic en  (Acciones) > **Ver** > **Explorar**.
5. Haga clic con el botón secundario en `event-broker` > **Propiedades**.
6. Seleccione `passwd` en la lista desplegable, ingrese `newpw=><newpassword>` en Parámetros (donde `<newpassword>` es la contraseña de la cuenta de usuario de RabbitMQ) y haga clic en **Enviar**.



(Opcional para las actualizaciones desde 10.6.4.x en que FIPS está habilitado para Log Collectors, Log Decoders y Packet Decoders) Tarea 12: Habilitar el modo FIPS

FIPS está habilitado en todos los servicios, excepto en Log Collector, Log Decoder y Decoder. FIPS no se puede deshabilitar en ningún servicio, excepto en Log Collector, Log Decoder y Decoder. Para obtener información sobre cómo habilitar FIPS para estos servicios, consulte el tema "Mantenimiento del sistema: Activar o desactivar FIPS" de la *Guía de mantenimiento del sistema de RSA NetWitness® Suite*. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Reporting Engine

Tarea 13: Restaurar los certificados de CA para los servidores de syslog externos para Reporting Engine

Debe restaurar los certificados de CA después de la actualización del respaldo que realizó antes de la actualización. El script de respaldo respalda los certificados de CA de 10.6.4.x en el directorio `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts`.

Realice el siguiente procedimiento para restaurar los certificados de CA en 11.0.

1. Acceda mediante el protocolo SSH al host del servidor de NW.
2. Exporte los certificados de CA.
   ```
   keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
   ```
3. Copie el archivo PEM de CA en el directorio `/etc/pki/nw/trust/import`.

(Condicional) Tarea 14: Restaurar el almacenamiento externo para Reporting Engine

Si tiene almacenamiento externo para Reporting Engine (por ejemplo, SAN o NAS para almacenar informes), debe restaurar el montaje que desvinculó antes de la actualización. Consulte "Reporting Engine: Agregar espacio adicional para informes grandes" en la *Guía de configuración de Reporting Engine* de *RSA NetWitness® Suite* para obtener instrucciones. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Respond

Tarea 15: Restaurar las claves personalizadas del servicio Respond

En 10.6.4.x, si agregó una clave personalizada para su uso en la cláusula groupBy, se modificó el archivo `alert_rules.json`. El archivo `alert_rules.json` contiene el esquema de la regla de agregación. RSA transfirió el archivo `alert_rules.json` a la siguiente ubicación nueva:
`/var/lib/netwitness/respond-server/scripts`

1. Copie las claves personalizadas desde el archivo `/opt/rsa/im/fields/alert_rules.json` en el directorio de respaldo.
   Este directorio está en la ubicación en la que se restaura el archivo `alert_rules.json` desde el respaldo de 10.6.4.x.
2. Vaya a `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` en 11.0.
   Este es el nuevo archivo para 11.0.
3. Edite `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` para incluir las claves personalizadas que copió en el paso uno.

Tarea 16: Restaurar scripts de normalización del servicio Respond personalizados

RSA refactorizó los scripts de normalización del servicio Respond en 11.0 y los transfirió a la siguiente ubicación nueva:
`/var/lib/netwitness/respond-server/scripts`
Si personalizó estos scripts en 10.6.4.x, debe:

1. Ir al directorio `/opt/rsa/im/scripts`.
   Este directorio es donde se restauran los siguientes scripts de normalización del servicio Respond desde el respaldo de 10.6.4.x.
   `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`
2. Copiar cualquier lógica personalizada desde los scripts de 10.6.4.x.
3. Ir al directorio `/var/lib/netwitness/respond-server/scripts`.
   Este directorio es donde NetWitness Suite 11.0 almacena los scripts refactorizados.
4. Editar los scripts nuevos para incluir la lógica personalizada que se copió en el paso 2 desde los scripts de 10.6.4.x.
5. Copiar cualquier lógica personalizada desde el archivo `/opt/rsa/im/fields/alert_rules.json`.
   El archivo `alert_rules.json` contiene el esquema de la regla de agregación.

(Condicional) Tarea 17: Habilitar la retención de datos de Incident Management 10.6.4.x deshabilitada

Realice el siguiente procedimiento para habilitar los trabajos de retención de datos de Incident Management que deshabilitó antes de la actualización.

1. Inicie sesión en RSA NetWitness® Suite.
2. Vaya a **ADMIN** > **Servicios** y seleccione el **servidor de Respond**.
3. Haga clic en  (Acciones), **Ver** > **Explorar**.
4. Vaya al nodo `respond/dataretention`.
5. Configure el parámetro `enable` en `true`.

(Condicional) Tarea 18: Restaurar las funciones personalizadas de analista

Si tenía funciones personalizadas de analista en 10.6.4.x, debe restablecerlas en 11.0. Consulte *Adición de funciones y asignación de permisos para las funciones* en la *Guía de RSA NetWitness Suite Warehouse Analytics*. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

NetWitness SecOps Manager

Tarea 19: Reconfigurar la integración de NW SecOps Manager

Para obtener información sobre cómo reconfigurar NW SecOps para Event Stream Analysis, Reporting Engine y Respond, consulte la *Guía de integración de RSA Archer*. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

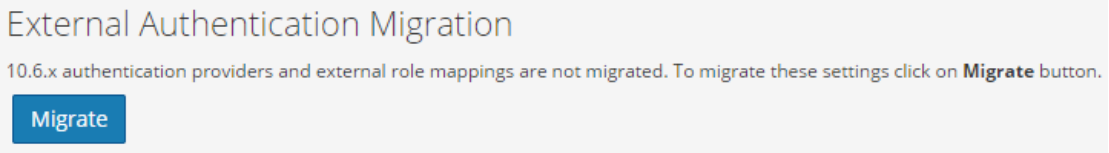
Seguridad

Tarea 20: Migrar Active Directory (AD)

La primera vez que inicia sesión en la interfaz del usuario de NetWitness Suite 11.0, debe hacer clic en el botón Migrar para completar la migración de AD.

Precaución: Si no actualizó desde 10.6.4.2, debe aplicar el parche de 11.0.0.1 inmediatamente antes de iniciar sesión por primera vez en NetWitness Suite 11.0 y migrar Active Directory. No es necesario aplicar el parche de 11.0.0.1 si actualizó a 11.0 desde 10.6.4.2.

1. Inicie sesión en NetWitness Suite con las credenciales de `admin user`.
2. Haga clic en **ADMIN** > **SEGURIDAD** y, a continuación, haga clic en la pestaña **Ajustes de configuración**.
   Se muestra el siguiente cuadro de diálogo.



3. Haga clic en **Migrar**.
   El cuadro de diálogo se cierra cuando la migración está completa.

Tarea 21: Modificar la configuración de AD migrado para cargar el certificado

Si usó un certificado autofirmado en el servidor de Active Directory (AD) y habilitó SSL para la conexión de AD en 10.6.4.x, debe modificar la configuración de AD migrado para cargar el certificado (el certificado autofirmado o el certificado de CA).

Realice el siguiente procedimiento para modificar la configuración de AD migrado con el fin de cargar el certificado (el certificado autofirmado o el certificado de CA).

1. Inicie sesión en NetWitness Suite.
2. Haga clic en **ADMIN** > **Seguridad** y, a continuación, haga clic en la pestaña **Ajustes de configuración**.
3. En **Configuración de Active Directory**, seleccione una configuración de AD y haga clic en  .

   Se muestra el cuadro de diálogo Editar configuración.
4. Vaya al campo **Archivo de certificado**, haga clic en **Navegar** y seleccione un certificado de la red.
5. Haga clic en **Guardar**.

Tarea 22. Resolver una falla de autenticación en 11.0

Los usuarios no pueden iniciar sesión en la interfaz del usuario de NetWitness Suite después de la actualización a 11.0 debido a que la interfaz no puede recuperar información de la cuenta del usuario de MongoDB.

- Aplique el parche de 11.0.0.1 para corregir este problema inmediatamente después de actualizar a 11.0.

Tarea 23: Reconfigurar el módulo de autenticación con capacidad para conectarse (PAM) en 11.0

Debe reconfigurar PAM después de actualizar a 11.0. 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*. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Puede consultar los archivos de configuración de PAM 10.6.4.x en el directorio **/etc** en los datos de respaldo de 10.6.4.x para obtener orientación.

Apéndice A. Solución de problemas

En esta sección se describen los problemas que podría encontrar durante la actualización con las soluciones. En la mayoría de los casos, NetWitness Suite crea mensajes de registro cuando encuentra estos problemas.

Nota: Si no puede resolver algún problema de actualización con los siguientes métodos de solución de problemas, póngase en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294).

Esta sección incluye documentación sobre la solución de problemas para los siguientes servicios, características y procesos.

- Programa de instalación 11.0 (`nwsetup-tui`)
- Respaldo
- Event Stream Analysis
- General
- Servicio Log Collector (`nwlogcollector`)
- Servidor de NW
- Reporting Engine

Programa de instalación 11.0 (`nwsetup-tui`)

Problema	El programa de instalación de hosts (`nwsetup-tui`) se cierra y crea el siguiente mensaje de error en `/var/log/netwitness/bootstrap/launch/security-server/security-server.log`:
	`<yyyy-mm-dd hh:mm:ss,nnn> [ main] ERROR SystemOperation|Service startup failed. Running in safe mode org.h2.jdbc.JdbcSQLException: The database is read only [90097-193]`
	`at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) ...`
	`at org.springframework.jdbc.datasource.AbstractDriverBasedDataSource.getConnection(AbstractDriverBasedDataSource.java:159)`
	`at com.rsa.asoc.security.upgrade.legacy.MigrationDatabase.<init>(MigrationDatabase.java:113)`

Causa	La base de datos H2 necesita permiso de escritura para completar la configuración del host.

Solución	Desde la línea de comandos del servidor de NW, proporcione permiso de escritura a `H2.db`, reinicie el servidor de NW y reinicie el programa de instalación nwsetup-tui.
	`chmod o+w /var/lib/netwitness/uax/db/platform.h2.db`
	`systemctl restart rsa-nw-security-server.service`
	`nwsetup-tui`

Respaldo (script `nw-backup`)

Mensaje	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Causa	La contraseña de administrador de ESA Mongo contiene caracteres especiales (por ejemplo, '!@#$%^qwerty').
Solución	Vuelva a cambiar la contraseña de administrador de ESA Mongo al valor predeterminado original de "netwitness" antes de ejecutar el respaldo. Consulte "Configuración de ESA: Cambiar la contraseña de MongoDB para la cuenta de administrador" en la *Guía de configuración de Event Stream AnalysisVaya a la* Tabla maestra de contenido *para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.* de *RSA NetWitness® Suite*.

Event Stream Analysis

Problema	El servicio ESA falla después de actualizar a 11.0 desde una configuración de FIPS habilitado.
Causa	El servicio ESA está apuntando a un almacenamiento de claves no válido.

Solución	1. Acceda mediante el protocolo SSH al host de ESA primario e inicie sesión.
	2. En el archivo `/opt/rsa/esa/conf/wrapper.conf`, reemplace la siguiente línea:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	por:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Ejecute el siguiente comando para reiniciar ESA.
	`systemctl restart rsa-nw-esa-server`
	Nota: Si tiene múltiples hosts de ESA y encuentra ese mismo problema, repita los pasos 1 al 3 en cada host de ESA secundario.

General

Los registros que se mencionan en esta sección se publican en `/var/log/install/install.log` en el host del servidor de NW.

Mensaje	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Causa	NetWitness Suite ve el servicio de administración de servicios (SMS) como inactivo después de la actualización correcta aunque el servicio esté en ejecución.
Solución	Reinicie el servicio SMS mediante el siguiente comando. `systemctl restart rsa-sms`

Mensaje	`<timestamp> <host>: SMS_PostInstall: INFO: Free disk space on /opt is nGB` `<timestamp> <host>: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space nGB is less than the recommended minimum disk space of 10GB.`
Causa	Se asignó espacio en disco bajo o insuficiente para el servicio SMS.
Solución	RSA recomienda proporcionar un mínimo de 10 GB de espacio en disco para que el servicio SMS se ejecute de manera óptima.

Problema	Después de ejecutar el programa de instalación para un host que no es de servidor de NW, debe ir a la interfaz del usuario, habilitar el host e instalar el servicio en el host desde la vista Hosts. Si aparece "Error en la instalación Ver detalles" en la columna **Estado** de la vista Hosts, el host perdió conectividad debido a problemas de red.
Solución	Vuelva a instalar el servicio en el host desde la vista Hosts.

Servicio Log Collector (`nwlogcollector`)

Los registros de Log Collector se publican en `/var/log/install/nwlogcollector_install.log` en el host que ejecuta el servicio `nwlogcollector` .

Mensaje	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Causa	El Lockbox de Log Collector no se pudo abrir después de la actualización.
Solución	Inicie sesión en NetWitness Suite y restablezca la huella digital del sistema mediante el restablecimiento de la contraseña de valor de sistema estable para el Lockbox como se describe en el tema “Restablecer el valor de sistema estable” bajo el tema “Configurar ajustes de seguridad de Lockbox” en la *Guía de configuración de la recopilación de registros*. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Mensaje	*timestamp* `NwLogCollector_PostInstall: Lockbox Status : Not Found`
Causa	El Lockbox de Log Collector no se configuró después de la actualización.
Solución	(Condicional) Si utiliza un Lockbox de Log Collector, inicie sesión en NetWitness Suite y configure el Lockbox como se describe en el tema “Configurar ajustes de seguridad de Lockbox” de la *Guía de configuración de la recopilación de registros*. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Mensaje	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Causa	Debe restablecer el campo de umbral de valor estable para el Lockbox de Log Collector.
Solución	Inicie sesión en NetWitness Suite y restablezca la contraseña de valor de sistema estable para el Lockbox como se describe en el tema “Restablecer el valor de sistema estable” bajo el tema “Configurar ajustes de seguridad de Lockbox” en la *Guía de configuración de la recopilación de registros*. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Problema	Preparó un Log Collector para actualización y ya no desea actualizarlo en este momento.
Causa	Retraso en la actualización.
Solución	Use la siguiente cadena de comandos para revertir un Log Collector que fue preparado para actualización con el propósito de que reanude su operación normal. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

Servidor de NW

Estos registros se publican en `/var/netwitness/uax/logs/sa.log` en el host del servidor de NW.

Problema	Después de la actualización, observa que los registros de auditoría no se reenvían a la configuración de auditoría global definida o El siguiente mensaje se muestra en sa.log. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Causa	La migración de la configuración de auditoría global del servidor de NW de 10.6.4 a 11.0 no se pudo realizar.
Solución	1. Acceda mediante el protocolo SSH al servidor de NW. 2. Ejecute el siguiente comando. `orchestration-cli-client --update-admin-node`

Servicio Reporting Engine

Los registros de actualización de Reporting Engine se publican en el archivo `/var/log/re_install.log` en el host que ejecuta el servicio Reporting Engine.

Mensaje	`<timestamp> : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ existing-GB ] is less than the required space [ required-GB ]`
Causa	La actualización de Reporting Engine falló debido a que no hay espacio en disco suficiente.
Solución	Libere el espacio en disco requerido según se muestra en el mensaje de registro. Consulte el tema “Agregar espacio adicional para informes grandes” de la *Guía de configuración de Reporting Engine* para obtener instrucciones sobre cómo liberar espacio en disco. Vaya a la Tabla maestra de contenido para la versión 11.0 para buscar los documentos de NetWitness Suite 11.0.

Apéndice B. Detención y reinicio de la captura y la agregación de datos

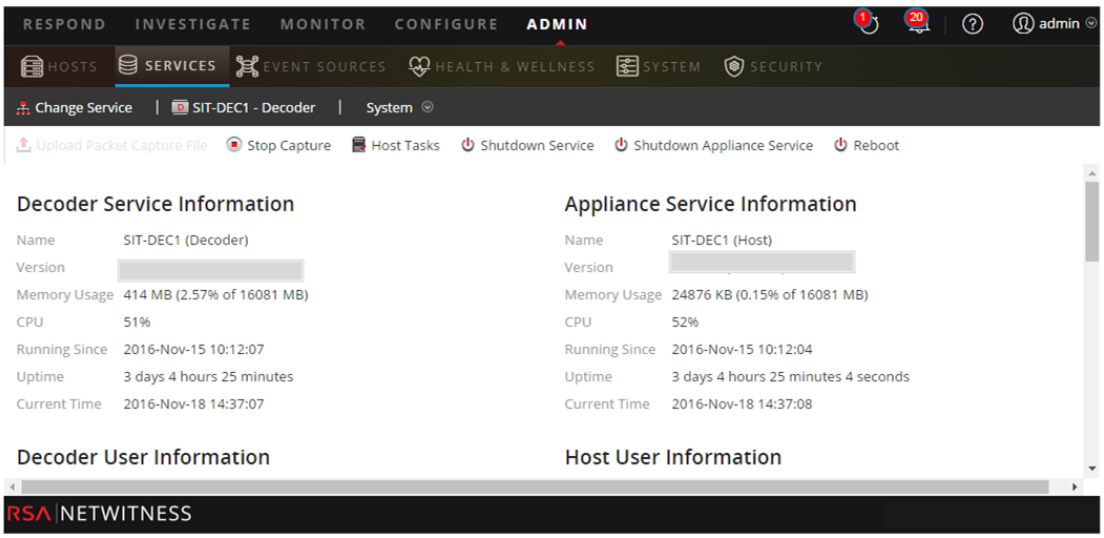
RSA recomienda detener la captura y la agregación de paquetes y registros antes de actualizar un host de Decoder, Concentrator y Broker a 11.0. Si hace esto, debe reiniciar la captura y la agregación de paquetes y registros después de actualizar estos hosts.

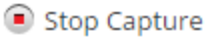
Detener la captura y la agregación de datos

Detener la captura de paquetes

Para detener la captura de paquetes:

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



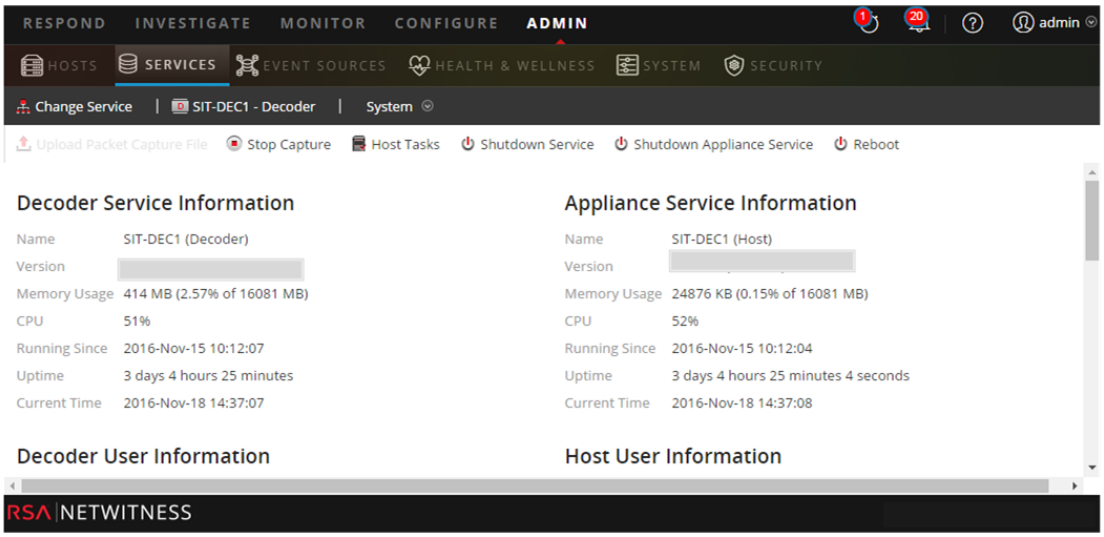
3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en  .

Detener la captura de registros

Para detener la captura de registros:

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

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



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

4. En la barra de herramientas, haga clic en 

.

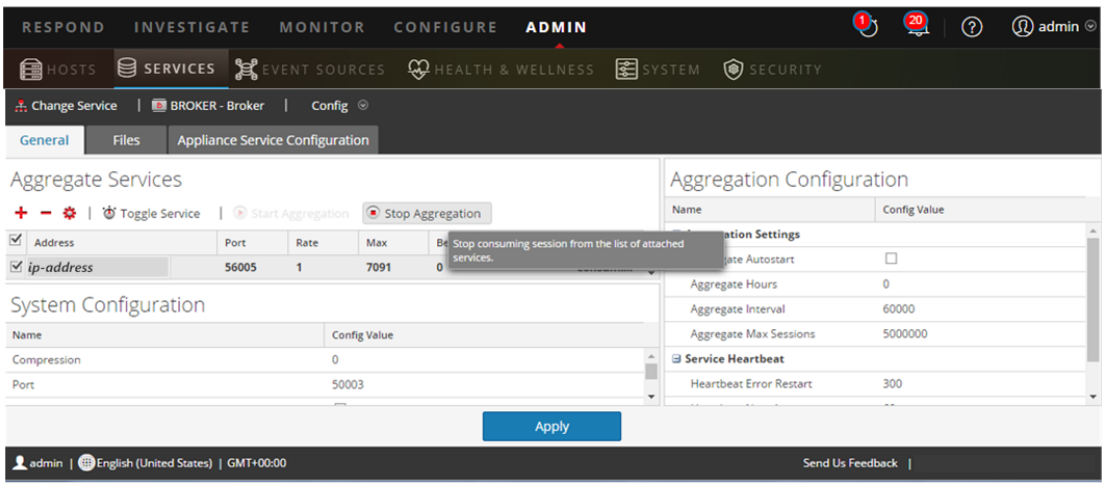
Detener agregación

1. Inicie sesión en NetWitness Suite y vaya a **ADMIN** > **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 

.

Iniciar la captura y la agregación de datos

Reinicie la captura y la agregación de paquetes y registros después de la actualización a 11.0.

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

.

Iniciar agregación

Durante la actualización de 10.6.4.x a 11.0, el servicio Broker se reinicia y esto inicia automáticamente la agregación.

Historial de revisiones

Revisión	Fecha	Descripción	Autor
1.0	26/12/2017	Publicación en RSA Link	IDD