RSA NETWITNESS® PLATFORM

Guía de actualización de hosts virtuales

para la versión 10.6.6 a 11.2

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de Dell, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por Dell.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

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

febrero 2019

Contenido

Introducción

Las instrucciones de esta guía se aplican a la actualización de los hosts virtuales a RSA NetWitness Platform11.2 exclusivamente. Consulte la *Guía de actualización de hosts virtuales* de *RSA NetWitness Platform* para obtener instrucciones sobre cómo actualizar los hosts virtuales 10.6.6.x a 11.2. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

NetWitness Platform 11.2 es una versión principal que afecta a todos los productos de la suite NetWitness Platform. Los componentes de la plataforma son NetWitness Server (servidor de Admin, servidor de Config, servidor de Integration, servidor de Investigate, servidor de Orchestration, servidor de Respond, servidor de Security y servidor de Source), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA primario, ESA secundario, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, UEBA, Warehouse Connector y Workbench.

Consulte la *Guía de introducción de NetWitness Platform* para familiarizarse con los principales cambios a la interfaz del usuario de 11.x. Consulte la *Guía de implementación de NetWitness Platform* para familiarizarse con los principales cambios de plataforma en 11.x.

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

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

Actualización de CentOS6 a CentOS7

NetWitness Platform 11.2 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 11.2 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® Platform 11.2

La primera ruta de actualización a RSA NetWitness® Platform 11.2 compatible es Security Analytics 10.6.6.x. Si ejecuta una versión de NetWitness Platform anterior a 10.6.6.x, debe actualizar a 10.6.6.x antes de poder actualizar a 11.2. Consulte la *Guía de actualización a RSA Security Analytics 10.6.6* (https://community.rsa.com/docs/DOC-85119) en RSA Link.

Ruta de actualización a host compatible

Debe actualizar un host al mismo tipo de host:

- De dispositivo físico RSA de la misma serie a dispositivo físico RSA de la misma serie (es decir, de serie 4 a serie 4, de serie 5 a serie 5).
  RSA no admite hosts físicos de otros fabricantes en 11.2.
- De host virtual en las instalaciones a host virtual en las instalaciones

Precaución: La actualización a 11.2 no admite actualizaciones de plataformas mixtas (por ejemplo, no admite actualizaciones físicas a actualizaciones virtuales).

Hardware, implementaciones, servicios y características no compatibles en 11.2

RSA no admite la actualización de los siguientes hardware, implementaciones, servicios y características a 11.2.

- Dispositivo RSA All-in-One (AIO)
- Implementación de múltiples NetWitness Server
- Servicio IPDB
- Servicio Malware Analysis colocalizado en el servidor de SA (la actualización de Malware Analysis Enterprise es compatible con 11.2).
- Servicio Warehouse Connector independiente (la actualización de un Warehouse Connector colocalizado es compatible con 11.2).
- Política de Estado y condición personalizada en 10.6.x para el servicio Context Hub
  Después de que se realiza la actualización a NetWitness 11.2, 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 11.2.
- 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® Platform 11.2, RSA cambió la manera en que las reglas de correlación de ESA almacenan y transmiten las alertas que genera el sistema. En 11.2, ESA envía todas las alertas a un sistema central de alerta. Se quitó el almacenamiento de MongoDB local en ESA 10.6.6.x.

Precaución: Si no usa Incident Management en 10.6.6.x, considere cuidadosamente si desea actualizar o no a la versión 11.2.

Las siguientes reglas lo ayudarán a determinar si actualizar o no los hosts de ESA a 11.2.

En la implementación de 10.6.6.x:

- Si tiene un host de ESA, ya sea que tenga configurado o no Incident Management: Actualice a 11.2.
- Si tiene múltiples hosts de ESA configurados para usar Incident Management: El sistema continuará agregando alertas centralmente. Si el sistema está dimensionado correctamente y está operando según lo previsto en 10.6.6.x, puede actualizar a la versión 11.2.
- 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 11.2.

Nota: Si no usó Incident Management en 10.6.6.x, no puede ver las alertas de ESA para 10.6.6.x en el componente Respond 11.2 sin ejecutar un script de migración. Use el script Migración de alertas de ESA para migrar estas alertas a la ubicación en 11.2 que permitirá que Respond las vea. Consulte el artículo de la base de conocimientos *Instrucciones sobre la migración de alertas de ESA* (https://community.rsa.com/docs/DOC-84102) en RSA Link para obtener instrucciones sobre cómo ejecutar este script.

Fases de actualización

RSA recomienda escalonar las actualizaciones de los hosts como se describe en esta sección. La actualización a CentOS7 y la necesidad de un acceso físico o un acceso a iDRAC hacen que la actualización a 11.2 demore más tiempo que la mayoría de las actualizaciones.

Precaución: Si escalona la actualización:
• Primero debe actualizar los hosts en la fase 1, en el orden que se indica.
• Es posible que no todas las funciones estén operativas hasta que actualice la implementación completa.
• No tendrá funciones administrativas de servicios disponibles hasta que actualice todos los hosts en la implementación.

Fase 1

Realice primero la fase 1. Debe actualizar los hosts en el siguiente orden:

1. Host del servidor de Security Analytics
2. Hosts de Event Stream Analysis
3. Hosts de Malware Analysis

4. Hosts de Broker (si no tiene un host de Broker, actualice los hosts de Concentrator)
   El servidor de NW 11.2 no puede comunicarse con los servicios principales de 10.6.6.x para la nueva funcionalidad Investigate. Es por esto que debe actualizar los hosts de Broker o Concentrator en la fase 1.

Fase 2

Actualice el resto de los hosts.

RSA recomienda seguir el orden de la fase 2 para reducir:

- La pérdida de funcionalidad durante la investigación.
- El tiempo de inactividad que genera la pérdida de captura de red y registros.

Nota: Excepto los hosts de recopilación de registros con destinos de evento descendentes, no hay ningún motivo técnico para actualizar los hosts en el siguiente orden en la fase 2.

Este es el orden de actualización de los hosts en la fase 2 que recomienda RSA.

1. Hosts de Decoder
2. Hosts de Concentrator
3. Hosts de Archiver
4. Hosts de recopilación de registros: Log Collectors en hosts de Log Decoder (LD), Virtual Log Collectors (VLC) y Recopiladores de Windows existente (LWC)
   Antes de actualizar un host de recopilación de registros, debe prepararlo para la actualización. Parte de esta preparación garantiza que no queden datos de eventos en las líneas de espera. Esto requiere que mantenga los destinos de datos de eventos descendentes (Log Collectors, Virtual Log Collectors y Log Decoders) funcionando correctamente.

   Si tiene destinos de datos de eventos descendentes desde Log Decoder, debe preparar y actualizar los Log Collectors en el siguiente orden.

   a. LD (un LD a la vez)

   b. VLC y LWC

   Si no tiene destinos de datos de eventos descendentes desde Log Decoder, puede preparar y actualizar juntos múltiples LD, VLC y LWC.
5. Todos los demás hosts

Consulte “Ejecución en modo mixto” en “Aspectos básicos” de la *Guía de introducción de hosts y servicios* de *RSA NetWitness Platform* para:

- Brechas de funcionalidad encontradas durante la ejecución en este modo.
- Ejemplos de actualizaciones escalonadas.

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

Investigate en modo mixto

Se produce un modo mixto cuando algunos servicios están actualizados a 11.2 y otros aún están en 11.0.0.x o 10.6.6.x. Esto sucede cuando actualiza a 11.2 en fases.

Nota: Debe seguir la secuencia de actualización de hosts como se muestra en Fases de actualización para garantizar la funcionalidad completa de Investigate. El servidor de Investigate 11.2 se instala cuando actualiza el servidor de SA, pero los hosts de Broker se deben actualizar a 11.2 para acceder a la vista Análisis de eventos. Si el Broker no está actualizado, los analistas ven un icono de advertencia junto al Broker y no se puede mostrar ninguno de los datos agregados a ese Broker.

Después de actualizar todos los servicios a 11.2, cuando un analista realiza una investigación, el Control de acceso basado en funciones (RBAC) de las descargas funciona de manera coherente para limitar el acceso a los datos restringidos.

En el modo mixto (es decir, algunos servicios están actualizados a 11.2 y otros aún están en 11.0.0.x o 10.6.6.x), cuando un analista realiza una investigación, el RBAC no se aplica de manera uniforme a la visualización y las descargas.

Si la configuración de `sdk.packets` no se ha deshabilitado en los servicios de 10.6.6.x u 11.0.0.x, los analistas con permisos de funciones y metadatos de SDK para restringir la visualización y la reconstrucción del contenido de un evento pueden descargar la PCAP de un evento que tenga restricciones de contenido. Otros tipos de descargas parecen ser correctas, las que posteriormente generan errores debido a permisos insuficientes y a que los datos aún están protegidos.

Durante una actualización en fases, puede deshabilitar la configuración de `sdk.packets` en los servicios de 10.6.6.x y 11.0.x.x para impedir que el analista descargue PCAP o registros durante el modo mixto. Después de actualizar todos los servicios a 11.2 y volver a habilitar `sdk.packets`, RBAC funciona de manera coherente en todos los servicios.

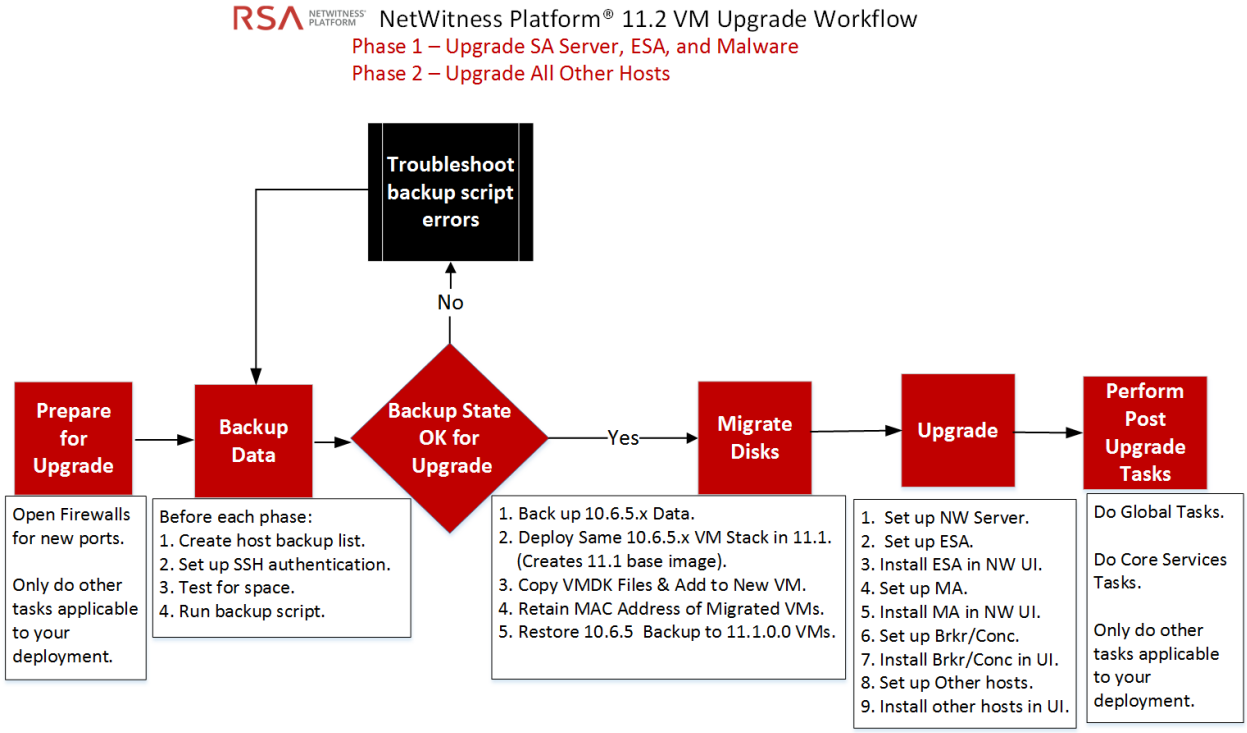
En la siguiente tabla se identifica lo que puede ver y descargar en Investigate cuando su servidor de NW en la versión 11.2 está conectado a servicios en una versión inferior.

Versión de servicio de conexión	Vista afectada	Función de usuario con contenido restringido	Puede ver	Puede descargar contenido restringido correctamente	Puede descargar contenido restringido con errores
Broker 11.2 -> Concentrator 10.6.6.x -> Network Decoder/Log Decoder 10.6.6.x	Vista Eventos	Analista	Elementos permitidos de RBAC	PCAP	El archiving de archivos se descargó, pero no se puede descomprimir
	Vista Reconstrucción de evento	Analista	Elementos permitidos de RBAC	PCAP	El archiving de archivos se descargó, pero no se puede descomprimir
	Vista Análisis de eventos	Analista	Elementos permitidos de RBAC	PCAP	Error al recuperar la carga útil del servicio para Carga útil, Carga útil de la solicitud, Carga útil de la respuesta
Broker 11.2 -> Concentrator 11.2 -> Decoder/Log Decoder 11.2	Vista Reconstrucción de evento	Analista y encargado de la privacidad de datos	Elementos permitidos de RBAC	PCAP	El archiving se descargó, pero no se puede descomprimir Las PCAP y los registros se descargan como cero bytes

Versión de servicio de conexión	Vista afectada	Función de usuario con contenido restringido	Puede ver	Puede descargar contenido restringido correctamente	Puede descargar contenido restringido con errores
Broker 11.2 -> Concentrator 11.0.0.x -> Network Decoder/Log Decoder 11.0.0.x	Vista Eventos	Analista	Elementos permitidos de RBAC	Ninguno	El archiving de archivos se descargó, pero no se puede descomprimir Las PCAP y los registros se descargan como cero bytes
	Vista Reconstrucción de evento	Analista	Elementos permitidos de RBAC	Ninguno	El archiving de archivos se descargó, pero no se puede descomprimir Las PCAP y los registros se descargan como cero bytes
	Vista Análisis de eventos	Analista	Elementos permitidos de RBAC	Ninguno	Error al recuperar la carga útil del servicio para Carga útil, Carga útil de la solicitud, Carga útil de la respuesta Las PCAP y los registros se descargan como cero bytes

Flujo de trabajo de actualización de hosts virtuales

En el siguiente diagrama se ilustra el flujo de trabajo de actualización de hosts virtuales de RSA NetWitness® Platform 11.2.



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 Platform 11.2.

Tareas de preparación para la actualización

Realice las siguientes tareas para preparar la actualización a NetWitness Platform 11.2. Estas tareas se organizan en las siguientes categorías.

Global

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

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

En las siguientes tablas se enumeran los puertos nuevos de 11.2.

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
Estación de trabajo de administrador	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Hosts de NW	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ

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

Endpoint Hybrid o Endpoint Log Hybrid

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

Todos los puertos principales de NetWitness Platform se enumeran en el tema “Arquitectura y puertos de red” de la *Guía de implementación* de *RSA NetWitness® Platform* en caso de que necesite reconfigurar los firewalls y los servicios NetWitness Platform. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Tarea 2: Registrar la contraseña de `admin user` 10.6.6.x

Registre la contraseña de `admin user` 10.6.6.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).

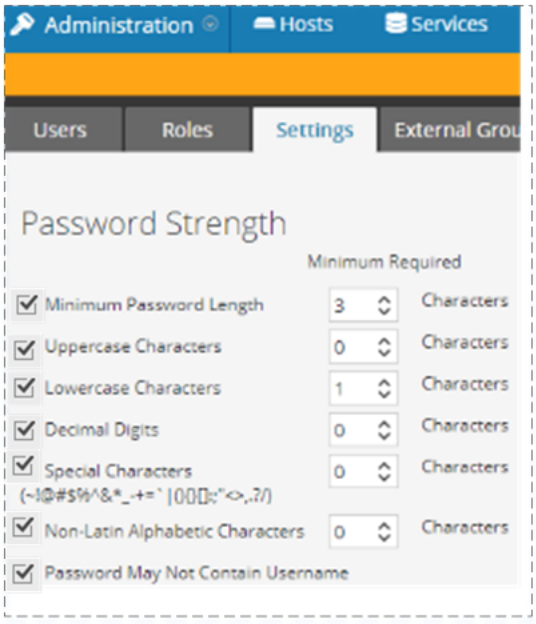
Nota: Este archivo se necesita para restaurar una VM con montajes a un almacenamiento externo.

Tarea 4: Asegurarse de que las casillas de verificación Configuración de seguridad de las contraseñas estén marcadas en 10.6.6.x

La casilla de verificación a la izquierda de **Configuración de seguridad de las contraseñas** en **Administración** > **Seguridad** > pestaña **Ajustes de configuración** debe estar marcada en 10.6.6.x o esta configuración no se migrará a 11.2.

Realice la siguiente tarea para asegurarse de que las casillas de verificación Configuración de seguridad de las contraseñas estén marcadas en 10.6.6.x.

1. En Security Analytics 10.6.6.x, vaya a **Administración** > **Seguridad** > pestaña **Ajustes de configuración**.
2. Asegúrese de que todas las casillas de verificación a la izquierda de **Configuración de seguridad de las contraseñas** estén marcadas. Si no lo están, márquelas y haga clic en **Aplicar**.
   En el siguiente ejemplo se muestran todas las casillas de verificación marcadas (es obligatorio en 10.6.6.x antes de la actualización a 11.2).



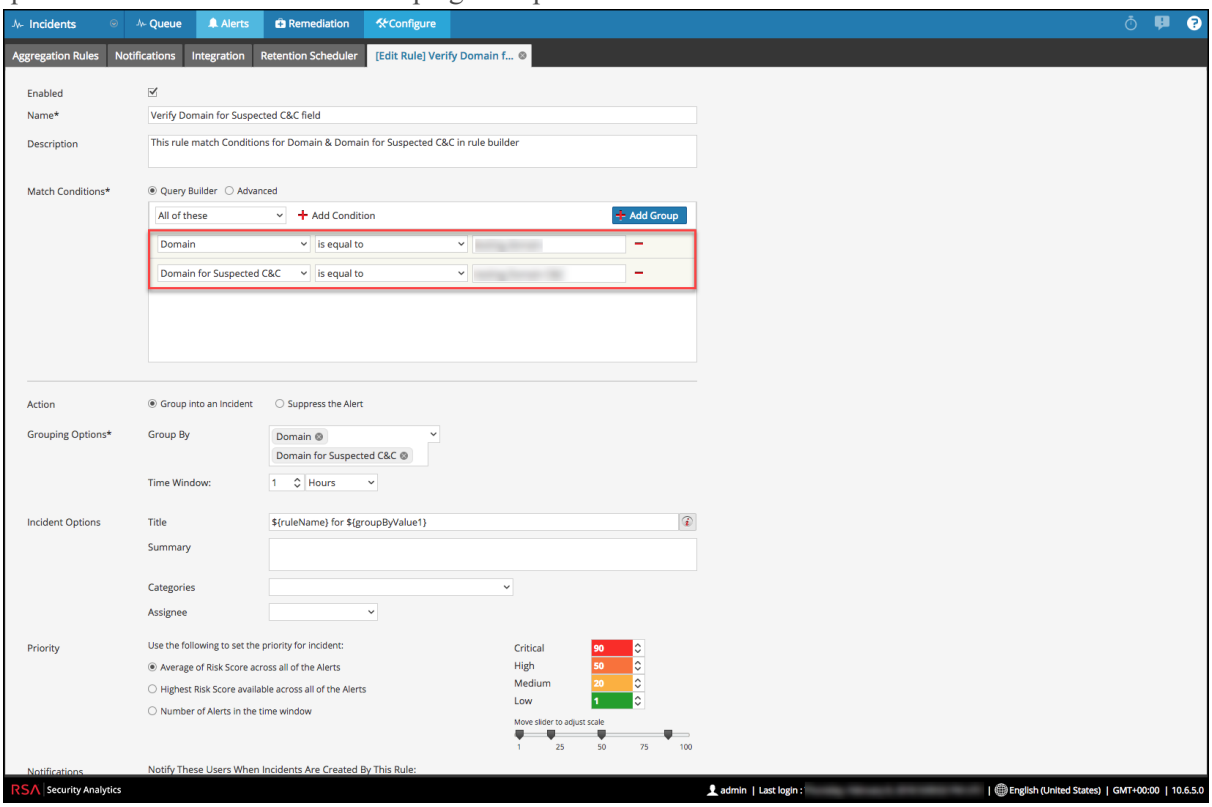
Respond

Tarea 5: Comprobar las condiciones de coincidencia de las reglas de agregación para “Dominio” o “Dominio para Sospecha de C&C”

Tome nota de cualquier regla de agregación de Incident Management que tenga condiciones de coincidencia mediante Dominio o Dominio para Sospecha de C&C en la lista desplegable del generador de reglas. En NetWitness Platform 11.2, tendrá que volver a agregar estas condiciones después de actualizar a 11.2 como se describe en Tareas posteriores a la actualización de Respond.

Compruebe lo siguiente para cada regla de agregación:

1. En el menú de Security Analytics 10.6.6.x, vaya a **Incidentes** > **Configurar** > pestaña **Reglas de agregación** y edite las reglas para ver las condiciones de coincidencia.
2. En la sección **Condiciones de coincidencia**, busque **Dominio** o **Dominio para Sospecha de C&C** que se encuentran en las listas desplegables para ver las condiciones.



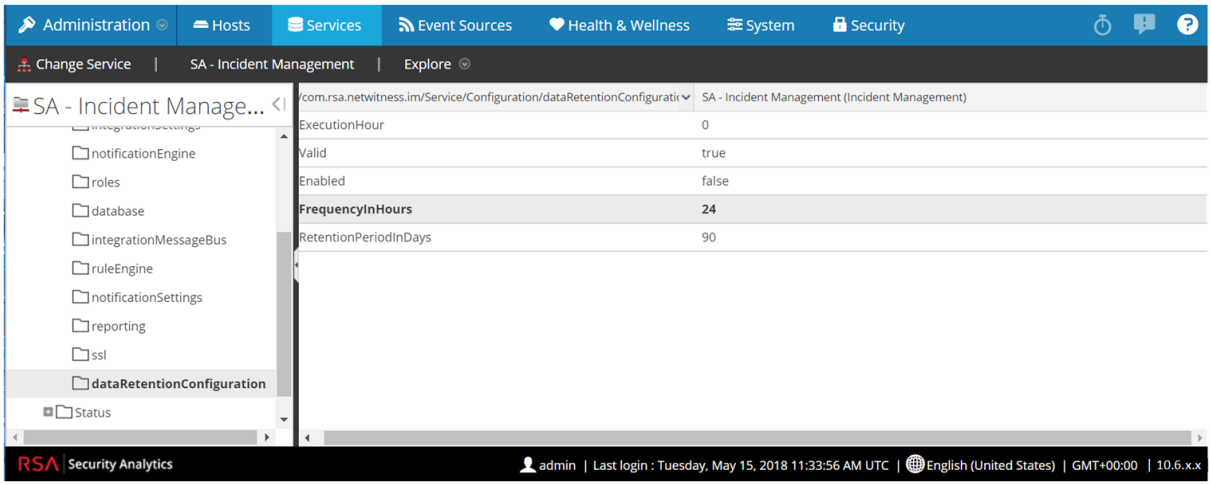
3. Tome nota del nombre de la regla y la condición completa que usa **Dominio** o **Dominio para Sospecha de C&C**, incluidos los operadores y los valores.

Tarea 6: Configurar el intervalo de ejecución de retención de datos en ≥ 24 horas

En Security Analytics 10.6.x, el intervalo de ejecución de retención de datos no tiene ninguna comprobación de valor mínimo. En 11.2, RSA agregó una comprobación de validación para asegurarse de que se ejecute al menos cada 24 horas. Al actualizar a 11.2, si este valor es menos de 24 horas, el servicio Respond no se iniciará.

Realice la siguiente tarea para asegurarse de que el servicio Respond se inicie después de actualizar a 11.2.

1. En Security Analytics 10.6.6.x, vaya a **ADMINISTRAR** > **Servicios**.
2. Seleccione el servicio **Incident Management** y elija  > **Ver** > **Explorar**.
3. En la vista **Explorar** de Incident Management, vaya a `Service` > `Configuration` > `dataRetentionConfiguration`.
4. Asegúrese de que el parámetro `FrequencyInHours` sea ≥ **24**.



Reporting Engine

(Condicional) Tarea 7: 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`

Instrucciones para respaldo

El respaldo de los datos de configuración de todos los hosts de 10.6.6.x es el primer paso en la actualización de versiones de Security Analytics 10.6.6.x a NetWitness Platform 11.2.

Nota: 1.) 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 11.2, 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. 2.) Deshabilite la configuración de Public Key Infrastructure (PKI) antes de iniciar el respaldo.

Precaución: Estos servicios no son compatibles en el proceso de respaldo y actualización de 10.6.6.x.
- IPDB
- Servidores todo en uno
- Malware Analysis colocalizado en el servidor de Security Analytics
- Warehouse Connector independiente
- Warehouse Analytics (ciencia de datos)

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

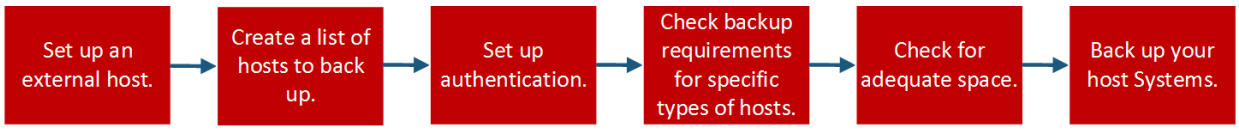
- **Servidor de Admin de Security Analytics**
- **Malware Analysis independiente**
- **Archiver**
- **Broker**
- **Event Stream Analysis** (incluida la base de datos de Context Hub e Incident Management)
- **Concentrator**
- **Log Decoder** (incluidos Local Log Collector y Warehouse Connector, si están instalados)
- **Log Hybrid**
- **Network Decoder** (incluido Warehouse Connector, si está instalado)
- **Network Hybrid**
- **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 11.2.” 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*.

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 Security Analytics.

Nota: Si no puede usar un host externo para respaldar archivos, Póngase en contacto con el servicio al cliente de RSA (https://community.rsa.com/docs/DOC-1294) para obtener ayuda.

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-v4.1.zip` o superior) de RSA Link en esta ubicación: https://community.rsa.com/docs/DOC-81514 y copiarlo en el sistema de respaldo CentOS 6. 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 servidores de Security Analytics y los sistemas del host que se respaldarán.

Precaución: Cuando realice una actualización en modo mixto, conserve una copia maestra de la actualización del archivo `all-systems` hasta que todos los hosts de la implementación se hayan actualizado a 11.2. No puede ejecutar `get-all-systems.sh` una segunda vez porque el servidor de NW, el primer host que se debe actualizar en modo mixto, tendrá CentOS7 como un sistema operativo.

- `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.
- `azure-mac-retention.ps1`: Se aplica solo si está usando AZURE. Para obtener más información, consulte la *Guía de implementación de AZURE*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

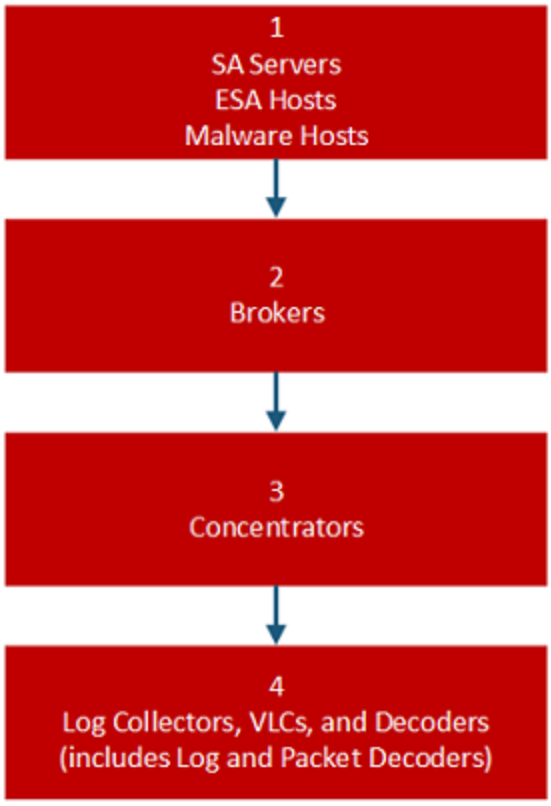
Nota: Si ha utilizado las versiones 10.6.x de los scripts de respaldo y restauración en los hosts 10.6.6, es necesario que ejecute todos los scripts que se enumeran aquí.

Nota: NO utilice los scripts en el archivo `nw-backup-v4.1.zip` para los respaldos periódicos. Estos scripts están diseñados específicamente para la actualización de 10.6.6.x a 11.2.

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-SA-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. RSA recomienda que agregue un comentario en los hosts que no desea respaldar (agregue el signo de número (#) al principio de la línea que contiene el host que no se respaldará).
   En los siguientes ejemplos se muestra cómo dejar como comentario el servidor de Security Analytics 10.6.6:
   `loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fa1d18d8,10.6.6.0`
   `#nwserver,nwserv106,172.31.255.23,67a9a0eb-1300-4fba-838f-7be4d8cf5e65,10.6.6.0`

   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,10.6.6.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.6.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.6.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.6.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.6.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.6.0
```

Y este es un ejemplo de un archivo `all-systems` que se podría utilizar en la primera sesión de respaldo, en que solo se respaldan el servidor de Security Analytics, el host de ESA y el host de Malware Analysis:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.6.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.6.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.6.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.6.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.6.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.6.0
```

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 que en cada versión del archivo se enumeren solo aquellos hosts que se están respaldando actualmente y que los demás hosts queden como comentario. 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 Security Analytics. 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 Security Analytics, RSA recomienda usar la interfaz del usuario de Security Analytics 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 Security Analytics 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 Security Analytics. (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`.

Complete la siguiente tarea para configurar la autenticación entre los hosts de respaldo y destino.

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 hosts.

1. En el servidor de Security Analytics, 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 11.2, 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 al servidor de Security Analytics y ejecute las siguientes cadenas de comandos para realizar las conversiones que se enumeran.
   Convertir un archivo DER (.crt .cer .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 ESA con bases de datos de Mongo

La contraseña predeterminada de la base de datos de Mongo 10.6.x es `netwitness`. Si personalizó esta contraseña, podría encontrar un error al ejecutar el script de respaldo. Puede utilizar su contraseña personalizada de la base de datos de Mongo durante el respaldo o podría volver a cambiar esa contraseña a `netwitness` antes de ejecutar el script `nw-backup.sh`.

1. Averigüe si la contraseña de la base de datos de Mongo es `netwitness` o si se modificó.
2. Si se modificó, vuelva a cambiarla a `netwitness` o asegúrese de saber cuál es la contraseña personalizada para que pueda ingresarla durante el respaldo.

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 “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

Complete la siguiente tarea para preparar Log Collectors y Virtual Log Collectors 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 11.2.
   - 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, Archer Cyber Incident & Breach Response o NetWitness Endpoint, enumerar nombres de usuario y contraseñas de RabbitMQ

En el host del servidor de Security Analytics 10.6.6.x, debe obtener una lista de todos los nombres de usuario y las contraseñas de RabbitMQ, de modo que después de realizar la actualización a 11.2, 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 10.6.6.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 10.6.6.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.

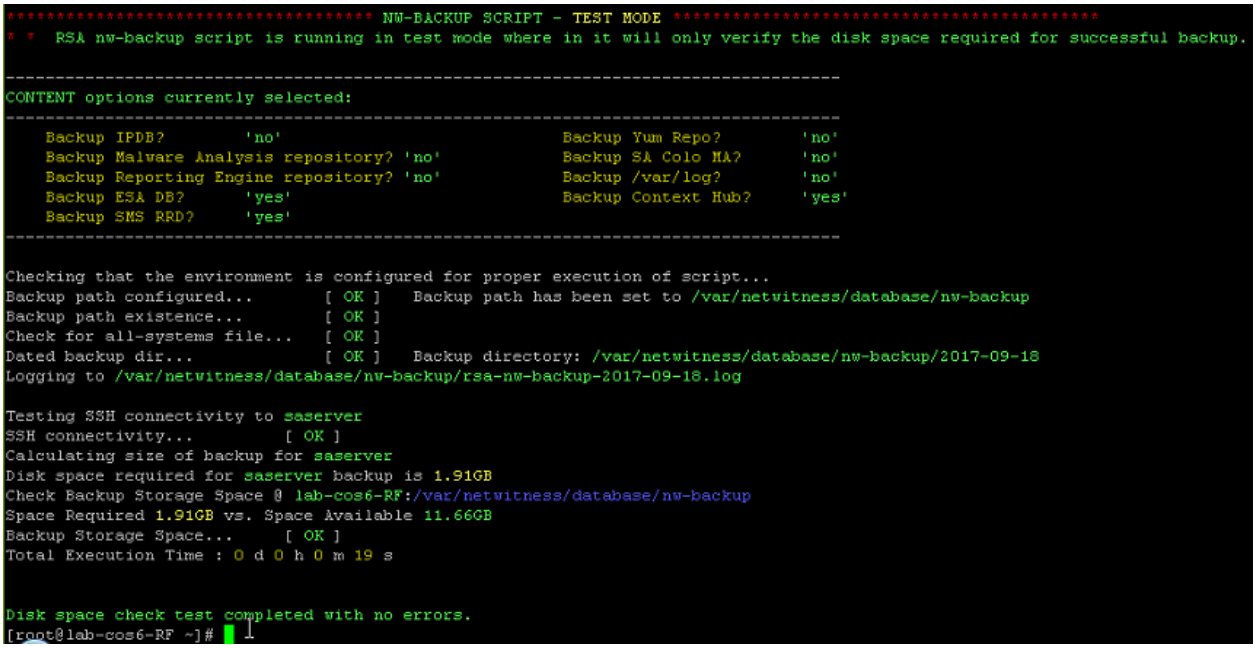
Complete la siguiente tarea para comprobar si hay suficiente espacio en disco.

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 11.2.

> **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.

Uso

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

Opciones generales

```
-u : This option is required for upgrading to 11.2. Enables the upgrade flag to run backup for upgrading to 11.2. 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 11.2, please use the default location! Default: (/var/netwitness/database/nw-backup)
```

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

Nota: Cuando ejecuta un respaldo con la opción `-u`, todos los servicios se detienen. Si necesita seguir utilizando la máquina 10.6.x después de ejecutar el respaldo, reinicie el sistema 10.6.x, de modo que se reinicien los servicios.

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 11.2. 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: El script `nw-backup` de RSA respalda los archivos de configuración, los datos y los registros en las opciones que se proporcionan en el script. Crea un archivo tar del contenido, con opciones para almacenar los archivos de respaldo en el servidor de respaldo, transferirlos o copiarlos a almacenamiento externo en un punto de montaje (USB/NFS/SMB), o transferirlos mediante SCP de regreso al host de destino.
Este script de respaldo cumple los requisitos de las siguientes versiones de Security Analytics: 10.6.6.x
Es posible que el uso de este script en cualquier otra versión del producto no produzca los resultados esperados y que no reciba soporte del servicio al cliente de RSA.
Nota: Todos los archivos personalizados, los scripts, los cronjobs y otros archivos importantes que no son de RSA se deben colocar en `/root`, `/home/'user'` O `/etc` con el fin de incluirlos en el respaldo.

Complete la siguiente tarea 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`

   Nota: Debe usar la opción `-u` para que los archivos se restauren correctamente durante la actualización a 11.2. NO realice cambios en el encabezado del script de respaldo para la ruta de respaldo porque la ruta es específica de la actualización y esos datos deben estar en un lugar específico.

   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-2018-03-15.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 servidores de Security Analytics:
<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 Security Analytics (específicamente, el servicio Admin) a 11.2.

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 11.2. 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 el servidor de Security Analytics y los hosts 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 servidor de Security Analytics.

- `<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 11.2., asegúrese de que existan los archivos apropiados en los hosts que está actualizando, como se describe en las siguientes listas.

Nota: Las rutas predeterminadas para los archivos de respaldo son:
- Servidores de Security Analytics:`/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 NetWitness Server

- `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 Platform)

Migrar unidades de disco de 10.6.6.x a 11.2

Estas instrucciones indican cómo actualizar los hosts virtuales de 10.6.6.x a 11.2.

Precaución: 1) No puede realizar la migración si tiene una instantánea para su VM.
2). Ejecute el respaldo inmediatamente antes de actualizar los hosts para cada fase, de modo que los datos no estén obsoletos.
3.) Esta guía se aplica exclusivamente a las actualizaciones de hosts virtuales. Si tiene hosts físicos y hosts virtuales en la implementación, consulte las *Instrucciones de actualización de hosts físicos RSA NetWitness® Platform 11.2* para ver cuáles son los pasos que debe completar para actualizar los hosts físicos. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Nota: Las máquinas deben estar en VMware ESX.

Hay cinco tareas que debe realizar para migrar sus unidades de disco de implementación de máquinas virtuales (VM) de 10.6.6.x a 11.2:

Tarea 1: Respaldar datos en las VM 10.6.6.x.

Tarea 2: Implementar la misma plataforma de VM 10.6.6.x en 11.2.

Tarea 3: Copiar los archivos VMDK y agregarlos como un disco duro a las nuevas VM.

Tarea 4: Conservar la dirección MAC de la VM del servidor de SA actualizada.

Tarea 5: Restaurar los datos de respaldo de 10.6.6.x en las VM 11.2.

Tarea 1: Respaldar datos en las VM 10.6.6.x

1. Prepare el Log Collector para la migración:
   a. Inicie sesión en el Log Collector con las credenciales raíz.
   b. Vaya al directorio `/opt/rsa/nwlogcollector/nwtools/` y ejecute el siguiente comando.
   `sh prepare-for-migrate.sh --prepare`
   Consulte Host de Virtual Log Collector (VLC) para obtener instrucciones detalladas sobre cómo actualizar el VLC.
2. Descargue el archivo `.zip` que contiene los scripts de respaldo de 10.6.6.x en RSA Link https://community.rsa.com/docs/DOC-81514)) al host de respaldo externo.

   Nota: 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 Platform.

3. Ejecute los siguientes comando desde el directorio `nw-backup/scripts` (consulte Instrucciones para respaldo para ver descripciones detalladas de los scripts de respaldo).
   `./get-all-systems.sh <SA-IP>`
   `./ssh-propagate.sh <path-to-backup-directory/all-systems>`
   `./nw-backup.sh -u`

(si dispone de una VM de Malware, sustituya `-m -u` por `-u` en esta cadena de comandos (por ejemplo, `./nw-backup.sh -m -u`).

Tarea 2: Implementar la misma plataforma de VM 10.6.6.x en 11.2

Debe configurar la misma plataforma de host virtual en 11.2 que la que tenía en 10.6.6.x. Consulte la *Guía de instalación de hosts virtuales* de *RSA NetWitness® Platform* 11.2 para obtener instrucciones.Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Los siguientes son los pasos generales sobre cómo implementar un host OVA en el ambiente ESXi.

Descargue OVA 11.2 desde RSA Link Download Central a un directorio local.

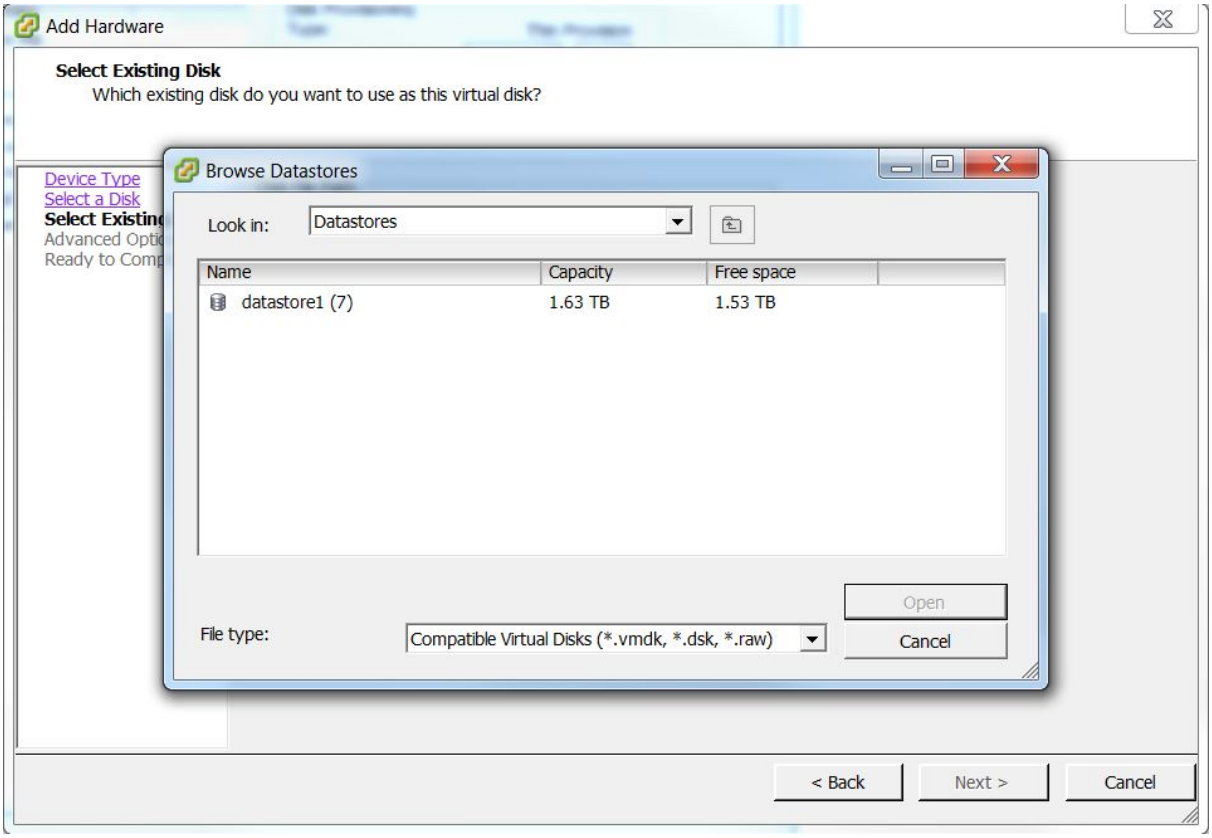
1. Inicie sesión en el ambiente ESXi.
2. En el menú desplegable **Archivo**, seleccione **Implementar plantilla OVF**.

   Se muestra el cuadro de diálogo Deploy OVA Template.
3. Busque en su directorio local los OVA 11.2 que descargó.
4. Seleccione para implementarlo en el ambiente virtual y haga clic en **Next**.
5. Seleccione la configuración adecuada para la VM y haga clic en **Next**.
6. Encienda la VM, vaya a Console e inicie sesión en la máquina.
   La VM ahora tiene la imagen base 11.2 requerida para ejecutar el programa de instalación (es decir, `nwsetup-tui`).

Tarea 3: Copiar los archivos VMDK y agregarlos como un disco duro a las nuevas VM

1. Apague las VM 10.6.6.x y 11.2.
2. Vaya al servidor de ESX deseado y haga clic en la pestaña **Configuration** > **Storage**.

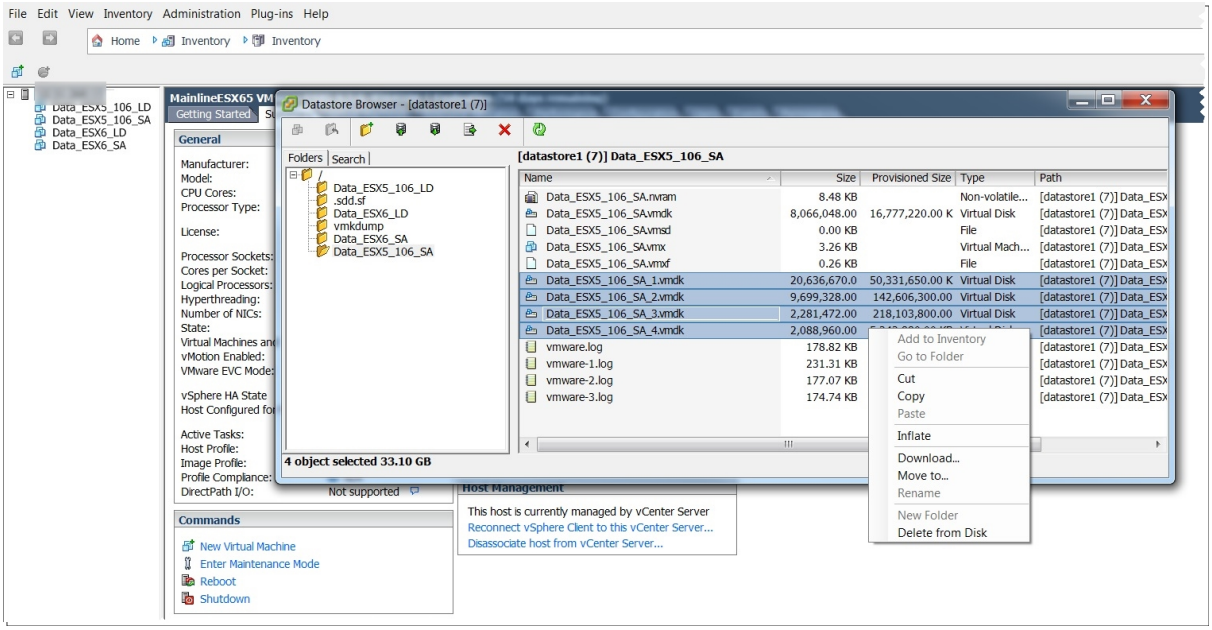
3. Haga clic con el botón secundario en el almacén de datos requerido y haga clic en **Browse Datastore**.



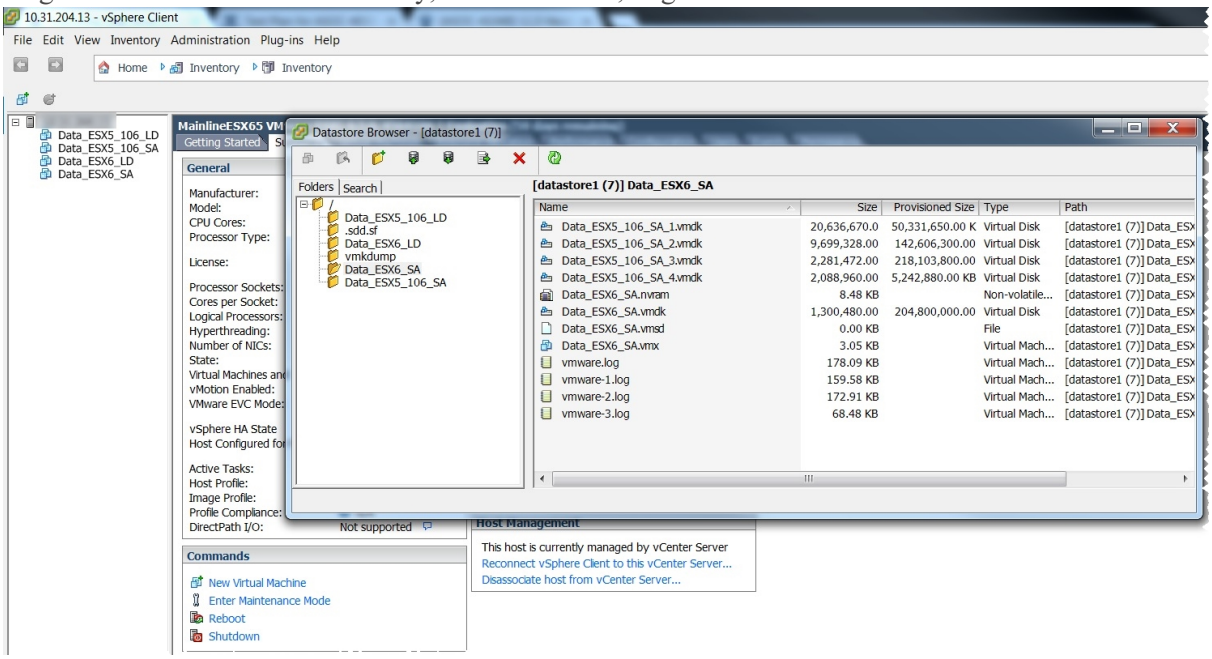
4. Navegue a la VM 10.6.6.x existente en el almacén de datos.

5. Seleccione todos los archivos VMDK en el almacén de datos, haga clic con el botón secundario y, a continuación, haga clic en **Copy**.

> **Precaución:** No copie el archivo VMDK base (por ejemplo, `Data_106_SA`) porque contiene CentOS6.
>
> Debe copiar todos los archivos VMDK numerados. Por ejemplo, si el nombre de la VM 10.6.6.x es `Data_106_SA`, copiaría todos los archivos `Data_106_SA_1`, `Data_106_SA_2`, `Data_106_SA_3`, etc.



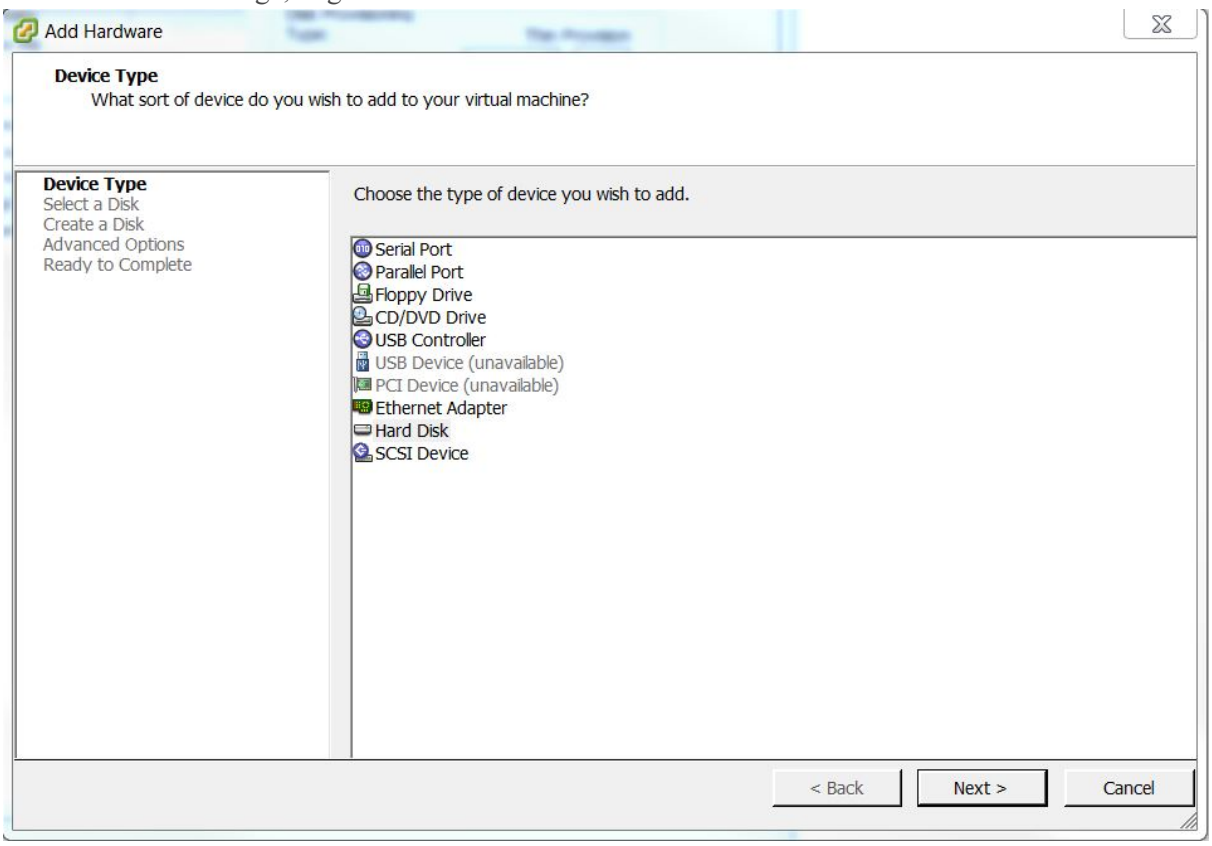
6. Navegue a la nueva VM 11.2 en el almacén de datos.
7. Haga clic con el botón secundario y, a continuación, haga clic en **Paste**.



Nota: Debe esperar hasta que todos los archivos VMDK de la VM anterior se hayan copiado por completo en el almacén de datos de la nueva VM.

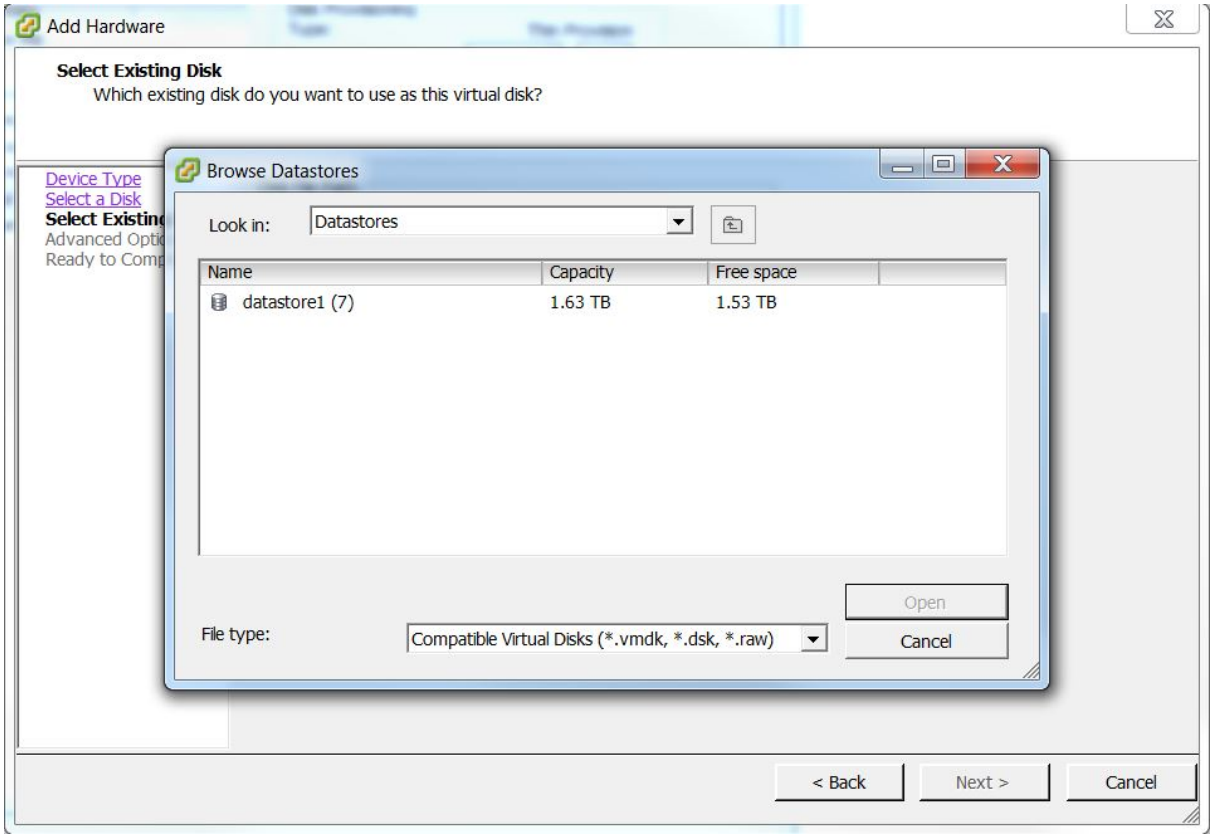
8. Seleccione la VM 11.2 y haga clic en **Edit Settings** > **Add**.

9. En el cuadro de diálogo, haga clic en **HardDisk** > **Next**.

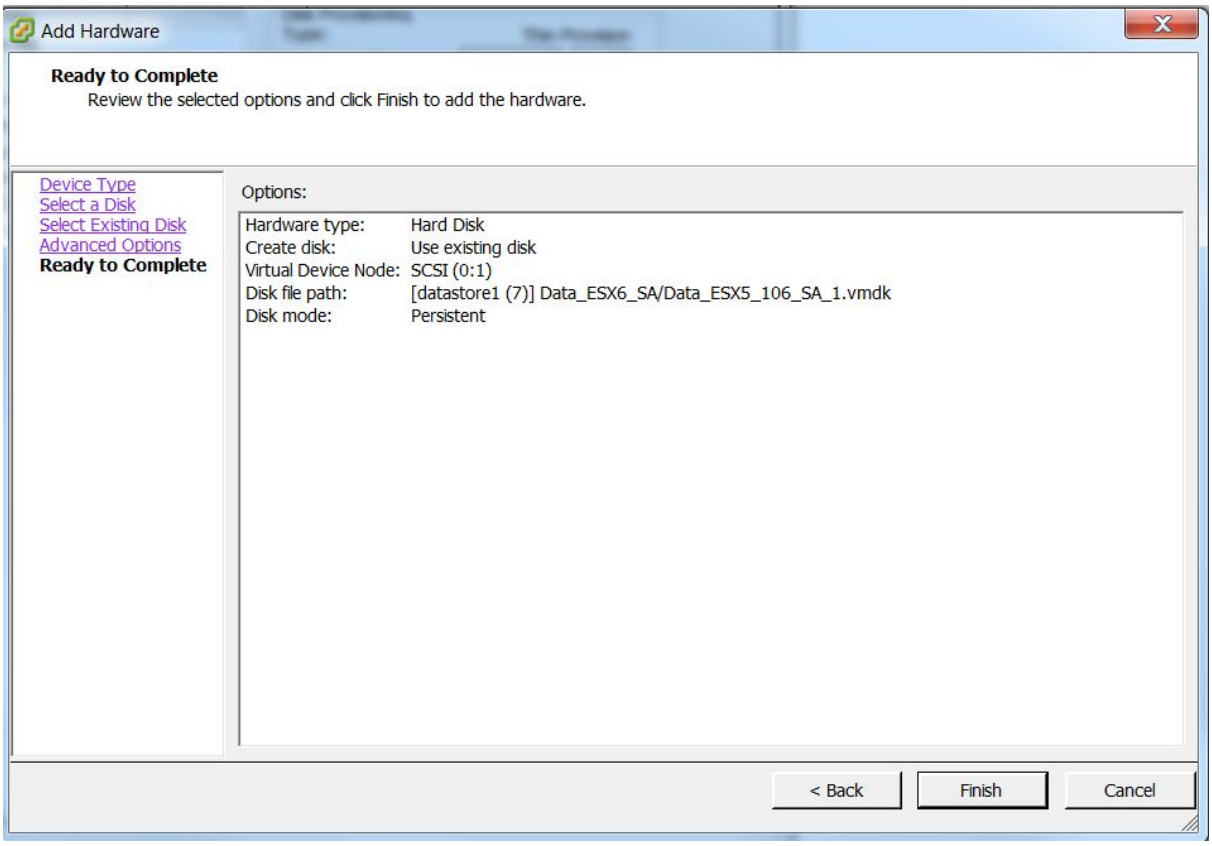


10. Haga clic en **Already existing hard disk** > **Next**.

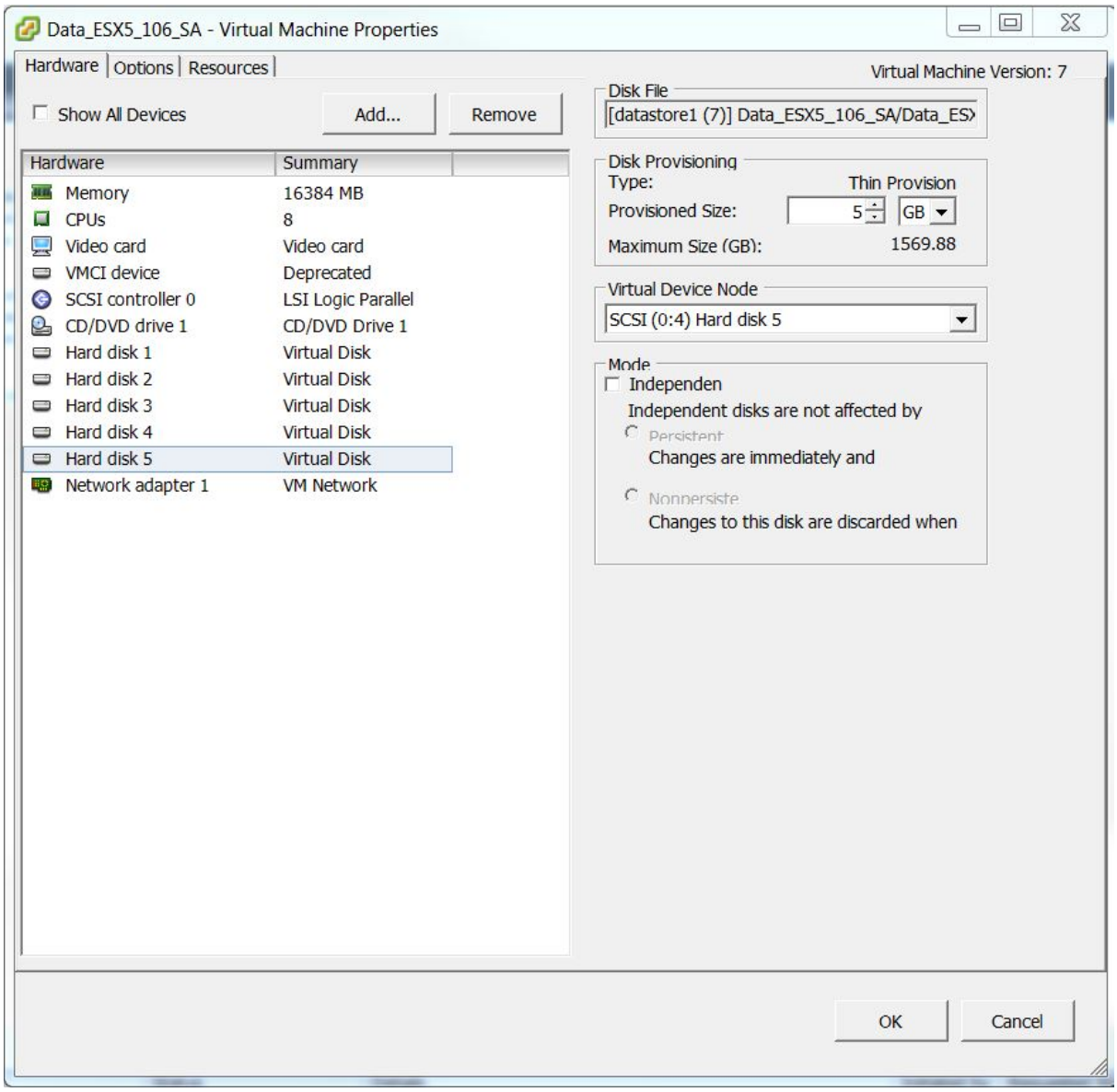
11. Haga clic en **Browse** y navegue hasta la ubicación del almacén de datos en que copió los archivos VMDK.



12. Seleccione el archivo VMDK de la VM 11.2 que desea agregar como un disco.



13. Repita los pasos 8 al 12 para cada disco que desee agregar.



14. Haga clic en **Aceptar**.

Tarea 4: Conservar la dirección MAC de la VM del servidor de SA actualizada

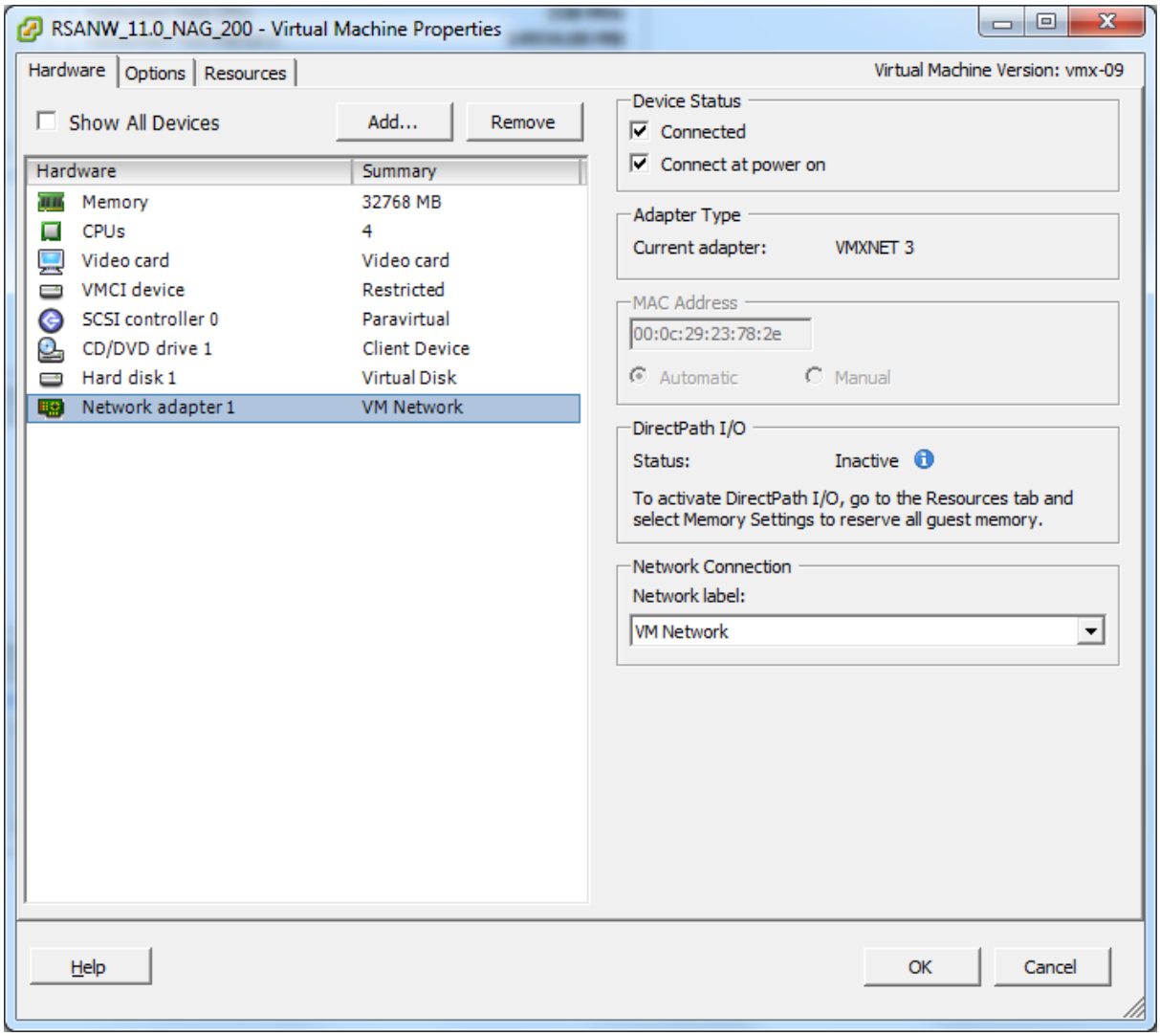
Para conservar la dirección MAC de la máquina virtual (VM) del servidor de Security Analytics (SA) migrada:

Nota: Estos pasos se aplican a la VM del servidor de SA (que se crea con la opción "Automático" de la asignación de direcciones MAC seleccionada) para el servidor de NetWitness 11.2. Para las VM con una dirección MAC estática, vaya a Edit Settings para una VM y escriba la dirección MAC para cambiar la dirección MAC.

1. Inicie sesión en vCenter Server.

   Nota: Las versiones compatibles de vCenter son las versiones 5.5 a 6.5, ambas inclusive.

2. (Condicional) Si están encendidas, **apague** ambas VM (NetWitness 10.6.6.x y 11.2).
3. Haga clic en la pestaña **Summary**, haga clic con el botón secundario en **Datastore** y busque la ubicación del almacén de datos.
4. Vaya a la carpeta VM y descargue el archivo `.vmx` de 10.6.6.x y 11.2 al repositorio local.
   De forma predeterminada, la VM generada con la dirección MAC se crea en el formato (como se muestra en la siguiente figura).



Nota: 00:0c:29:XX:YY:ZZ – 00:0c:29 es el identificador único de una dirección MAC generada automáticamente. **00:50:56:XX:YY:ZZ – 00:50:56** es el identificador único de una dirección MAC estática o generada manualmente. Esta opción solo es válida si vCenter no está implementado. Si vCenter está implementado, esta dirección MAC denota el identificador único para una dirección MAC generada automáticamente.

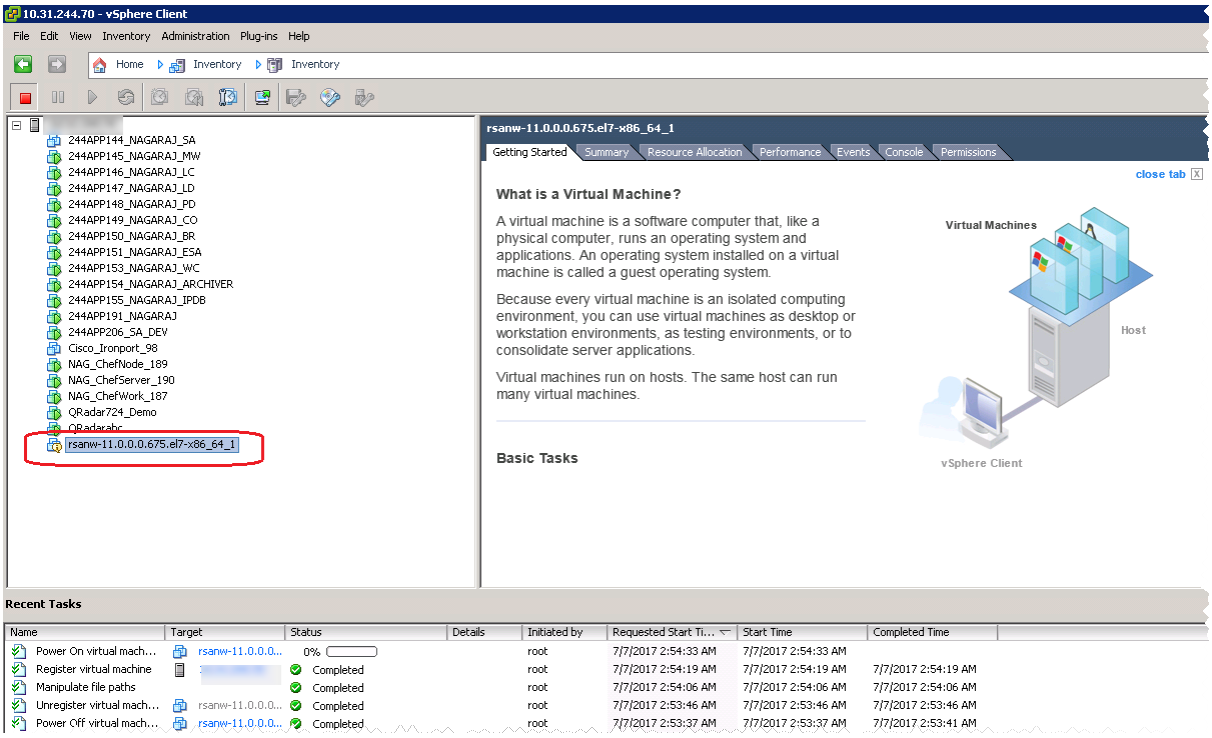
5. Con un editor de texto, copie los valores `uuid.location` y `ethernet0.generatedAddress` desde el archivo **.vmx** 10.6.6.x al archivo **.vmx** 11.2.

   Nota: Si implementó la plataforma 10.6.6.x directamente en el servidor ESX (no a través de VCenter), debe copiar el valor para `uuid.bios`, junto con `uuid.location` y `ethernet0.generatedAddress` desde el archivo **.vmx** 10.6.6.x al archivo **.vmx** 11.2.

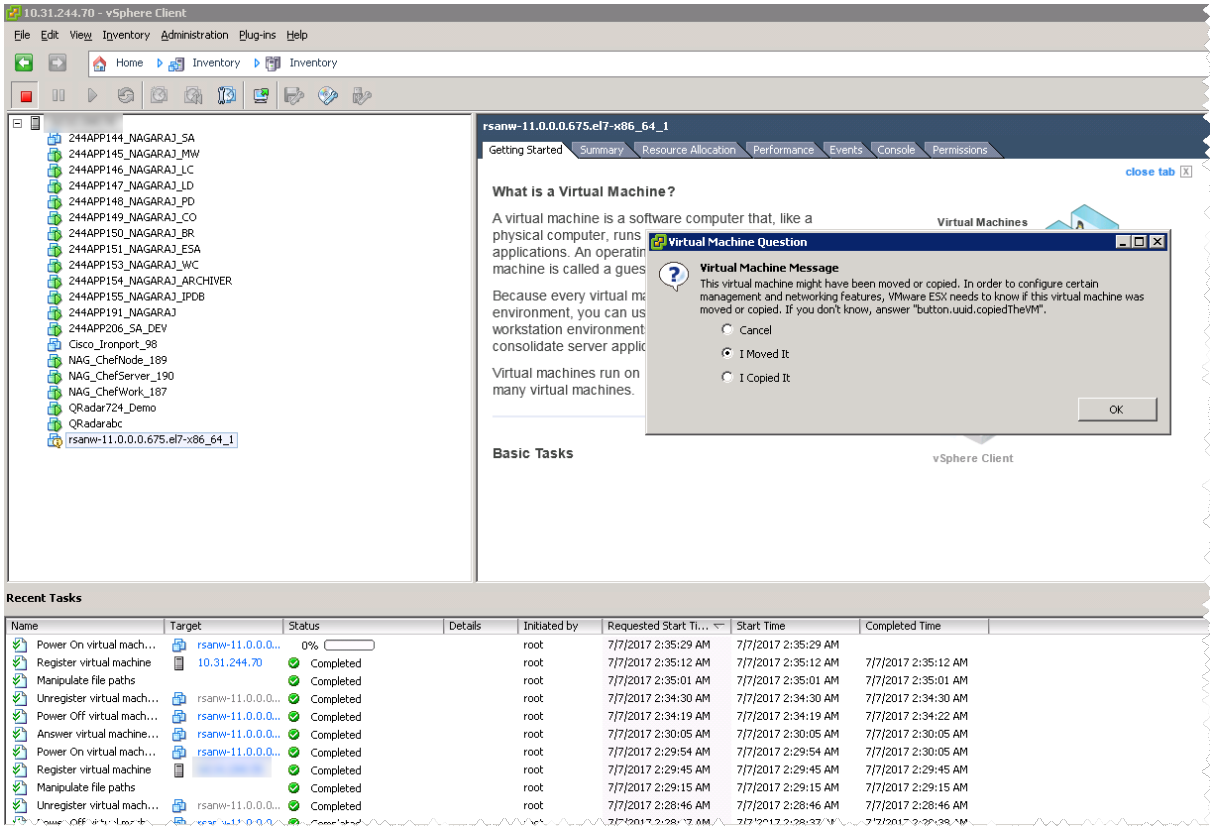
6. Quite las VM 10.6.6.x y 11.2 del inventario.
   a. Navegue a vCenter Server.
   b. Haga clic con el botón secundario en las VM 10.6.6.x y 11.2.

c. Seleccione Remove from Inventory.

7. Cargue el archivo **.vmx** 11.2 modificado en la ubicación de almacén de datos mediante el reemplazo de este por el archivo **.vmx** existente.
8. En el almacén de datos, haga clic con el botón secundario en el archivo **.vmx** 11.2 y seleccione Add to Inventory.
9. Navegue a vCenter Server y **encienda** la VM 11.2.
   Aparece el siguiente mensaje:
   The virtual machine might have been moved or copied. In order to configure certain management and networking features, VMware ESX needs to know if this virtual machine was moved or copied. If you don't know, answer "I Copied it."



10. Haga clic con el botón secundario en la VM y seleccione **Guest** > **Answer Question**.
    Se muestra la siguiente figura.



11. Seleccione **I Moved It**.
12. Haga clic en **Aceptar**.
    La dirección MAC se conserva en la dirección MAC de 10.6.6.x a 11.2.

Tarea 5: Restaurar los datos de respaldo de 10.6.6.x en las VM 11.2

Realice los siguientes pasos para **encender** la VM 11.2.

1. Copie los datos respaldados desde el directorio `nw-backup` a las VM 11.2.
   - Para el servidor de NW (servidor de SA en 10.6.6.x):

     Nota: Consulte Host de Virtual Log Collector (VLC) para obtener instrucciones detalladas sobre cómo actualizar el VLC.

     a. Cree el directorio `nwhome` en `/tmp`.

     b. Monte `VolGroup00-nwhome` en `/tmp/nwhome/`.
     ```
     mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
     ```

     c. Copie el contenido del directorio `/tmp/nwhome/` en `/var/netwitness/`.
     ```
     cp -r /tmp/nwhome/* /var/netwitness/
     ```

     d. Monte `VolGroup02-redb` en `/var/netwitness/database`.
     ```
     mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
     ```

     Nota: Asegúrese de que el directorio `/var/netwitness/database/nw-backup` exista con los archivos tarball de respaldo del dispositivo.

     e. Desmonte `VolGroup00-nwhome` de `/tmp/nwhome/`.
     ```
     umount /tmp/nwhome
     ```

   - Para Archiver, Broker, Concentrator, Log Decoder/Log Collector y Network Decoder:

     Nota: Si el Decoder o el Log Decoder 10.6.6.x tuvieran múltiples interfaces de red:
     1. **Apague** la VM de Decoder o Log Decoder 11.2 de la VM 11.2.
     2. Vaya a **Edit Settings** para la VM y agregue la cantidad requerida de adaptadores Ethernet.
     3. **Encienda** la VM.
     4. Agregue los adaptadores Ethernet antes de restaurar los datos de respaldo.

     a. Cree el directorio `nwhome` en `/tmp`.

     b. Cree un montaje temporal `VolGroup00-nwhome` en `/tmp/nwhome/`.
     ```
     mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
     ```

     c. Copie el contenido del directorio `/tmp/nwhome/` en `/var/netwitness/`.
     ```
     cp -r /tmp/nwhome/* /var/netwitness/
     ```

     d. Desmonte `VolGroup00-nwhome` de `/tmp/nwhome/`.
     ```
     umount /tmp/nwhome
     ```

   - Para Malware Analysis (Malware colocalizado no es compatible con la actualización a 11.2):

     a. Cree el directorio `apps` en `/tmp/`.

     b. Cree un montaje temporal `VolGroup01-apps` en `/tmp/apps/`.
     ```
     mount /dev/mapper/VolGroup01-apps /tmp/apps/
     mkdir /var/netwitness/database
     ```

     c. Copie el directorio `nw-backup` en `/var/netwitness/`.
     ```
     cp -r /tmp/apps/nw-backup /var/netwitness/database
     ```

d. Desmonte `VolGroup01-apps` de `/tmp/apps/`.
```
umount /tmp/apps
```

- Para Event Stream Analysis:

a. Cree el directorio `apps` en `/tmp/`

b. Cree un montaje temporal `VolGroup01-apps` en `/tmp/apps/`.
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. Copie el directorio `nw-backup` en `/var/netwitness`.
```
cp -r /tmp/apps/nw-backup /var/netwitness
```

d. Desmonte `VolGroup01-apps` de `/tmp/apps/`.
```
umount /tmp/apps
```

2. Monte los discos.

Nota: Si configuró algún punto de montaje externo en las VM en la plataforma para cualquiera de los siguientes directorios, vuelva a montar los puntos de montaje externos en el lugar de los siguientes montajes.

- Para el servidor de NW:
```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

Nota: Asegúrese de que el directorio `/var/netwitness/database/nw-backup` exista con los archivos tarball de respaldo del dispositivo.

- Para el Log Decoder/Log Collector:

Nota: Los siguientes montajes no se requieren para el Virtual Log Collector.

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder
mount /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index
mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb
mount /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
mount /dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb
```

- Para el Network Decoder:
```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder
mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/decoder/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb
mount /dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb
```

- Para el Concentrator:
```
mount /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb
```

- Para el Archiver:
  ```
  mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
  mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
  ```
- Para el Broker:
  ```
  mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
  ```

3. Agregue las siguientes entradas de montaje a `/etc/fstab`.
   - Para el servidor de NW:
     ```
     /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 el Log Decoder/Log Collector:

     Nota: Los siguientes montajes no se requieren para el Virtual Log Collector.

     ```
     /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 el Network Decoder:
     ```
     /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 el 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 el 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 el Broker:
  ```
  /dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
  defaults,nosuid,noatime 1 2
  ```

Configurar hosts virtuales en 11.2

Existen dos fases para configurar la plataforma virtual 11.2 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 10.6.6.x, los módulos ingresarán a un período de preparación después de actualizar el servicio Event Stream Analysis a 11.2 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 NetWitness Server 11.2

Siga las instrucciones de Configurar un host del servidor de NW 11.2.

Tarea 2: Configurar ESA 11.2

Precaución: Si tiene módulos C2 habilitados en 10.6.6.x, los módulos ingresarán a un período de preparación después de actualizar el servicio Event Stream Analysis a 11.2 y no estarán disponibles hasta que este período se complete.

Siga las instrucciones de Configurar un host de servidor que no es de NW 11.2 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 11.2

Siga las instrucciones de Configurar un host de servidor que no es de NW 11.2.

Tarea 4: Configurar Broker o Concentrator 11.2

Siga las instrucciones de Configurar un host de servidor que no es de NW 11.2.

Nota: Si no tiene un Broker, actualice los hosts de Concentrator. El servidor de NW 11.2 no se puede comunicar con los servicios principales de 10.6.6.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 el Apéndice B. Detención y reinicio de la captura y la agregación de datos para obtener instrucciones sobre cómo detener 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 de servidor que no es de NW 11.2.
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): Ejecutar 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 de servidor que no es de NW 11.2.
4. Reinicie la captura de datos en Log Decoder.

Nota: Después de la actualización, reiniciará la recopilación de registros tras completar la Tarea 30: Actualizar las reglas de incidentes identificadas en la tarea de preparación para la actualización Dominio en las condiciones de coincidencia 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): Ejecutar prepare-for-migrate.sh" en **Instrucciones para respaldo**.
2. Respalde su VLC 10.6.6.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>,10.6.6.x`
   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 10.6.6.x, de modo que se pueda crear una nueva VM 11.2 con la misma configuración de red.
5. Implemente un host de servidor que no es de NW nuevo mediante el OVA de NetWitness Platform 11.2.
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 10.6.6.x.
   Esta información se almacena en el archivo de respaldo del VLC `<hostname-IPaddress>-network.info.txt` 10.6.6.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 11.2 para el resto de los componentes de NetWitness Platform. Asegúrese de seleccionar **Log Collector** para el servicio en el paso 12.

Configurar un host del servidor de NW 11.2

Asegúrese de haber respaldado los datos de 10.6.6.x para el host del servidor de SA. **Debe seguir las instrucciones de Instrucciones para respaldo para respaldar el host.**

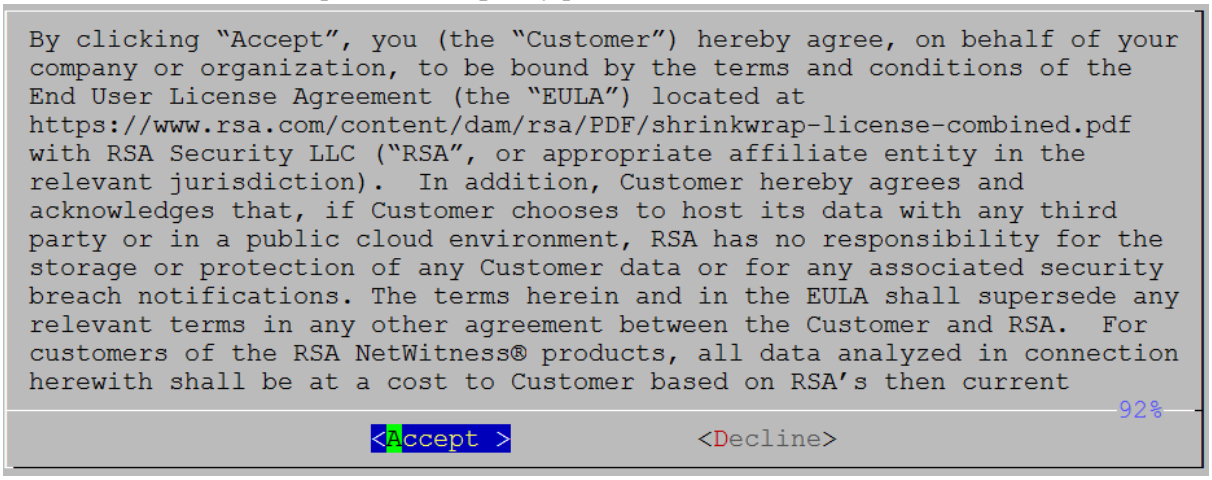
Precaución: Ejecute el respaldo inmediatamente antes de actualizar el servidor de SA a 11.2, de modo que los datos sean lo más recientes posible. Debe crear el archivo **all-systems** antes de actualizar el servidor de SA, porque no podrá hacer esto después de que el servidor de SA se haya actualizado a 11.2.

Realice los siguientes pasos para configurar el host del servidor de NW 11.2.

1. Inicie sesión en la consola de la VM del servidor de NW 11.2 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.

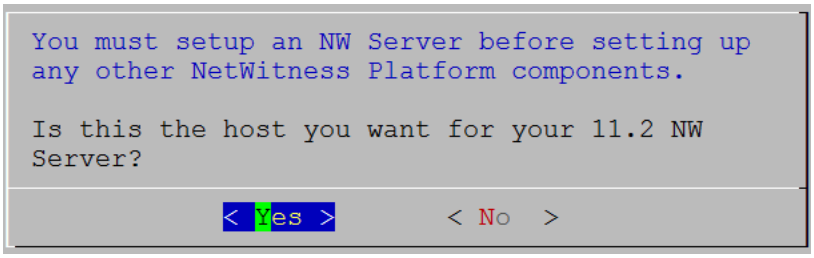
2. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.



   Se muestra el indicador **¿Es este el host que desea para el servidor de NW 11.2?**.

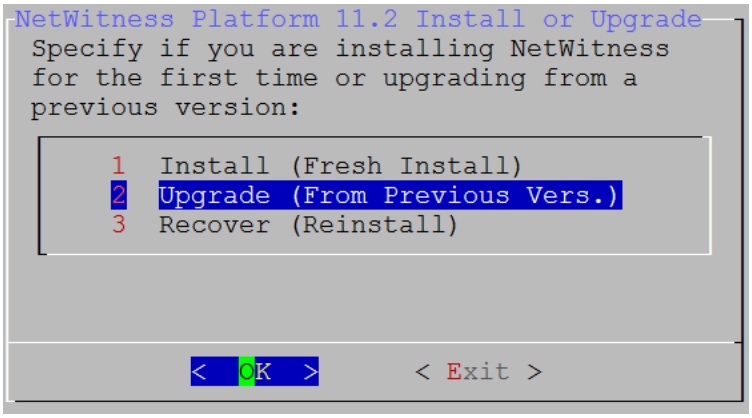
   Precaución: Si elige el host incorrecto para el servidor de NW y completa la actualización, debe repetir los pasos del 1 al 11 de Configurar un host del servidor de NW 11.2 para corregir este error.

3. Use la tecla de tabulación para ir a **Sí** y presione **Intro**.



Elija **No** si ya actualizó el servidor de NW a 11.2.
Se muestra el indicador **Instalar o Actualizar**.

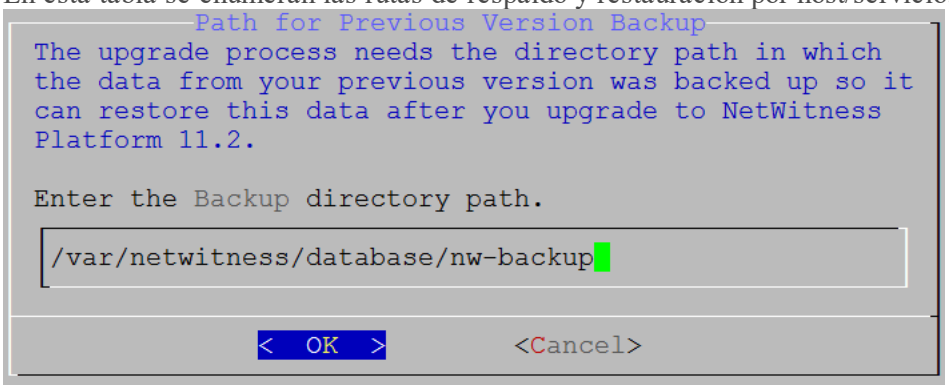
4. Use la flecha hacia abajo para seleccionar **2 Actualizar (de versión anterior)**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.



Se muestra el indicador de ruta de **respaldo**.

Precaución: La ruta de respaldo en el indicador siguiente debe ser igual que la ruta donde se almacena el respaldo. Por ejemplo, el script de respaldo asigna **/var/netwitness/database/nw-backup** como la ruta predeterminada. Si utilizó la ruta de respaldo predeterminada durante el respaldo y no la cambió posteriormente, debe mantener **/var/netwitness/database/nw-backup** como la ruta en el indicador siguiente.

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.
En esta tabla se enumeran las rutas de respaldo y restauración por host/servicio.



Host	Ruta de respaldo	Ruta de restauración
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore

Host	Ruta de respaldo	Ruta de restauración
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

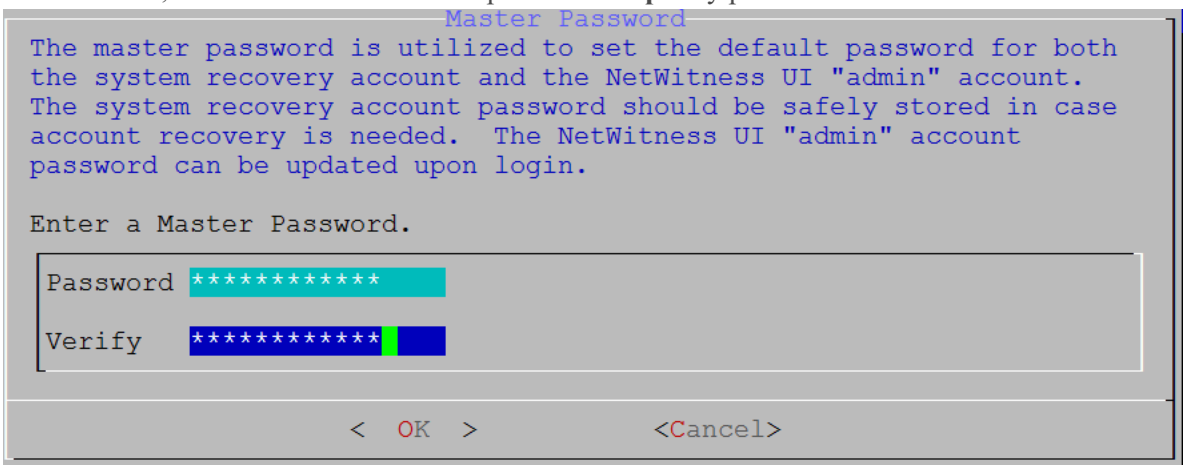
Se muestra el indicador **Contraseña maestra**.

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

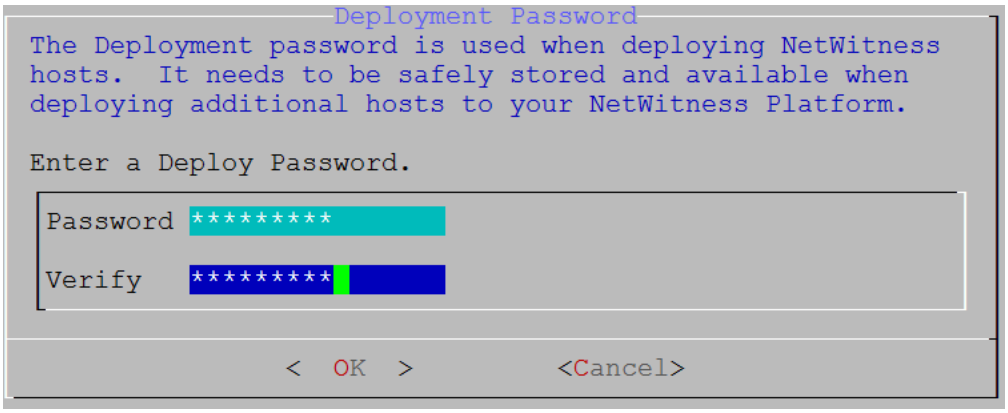
Ningún carácter ambiguo es compatible para Contraseña maestra y Contraseña de implementación. Por ejemplo:
espacio { } [ ] ( ) / \ ' " ` ~ ; : . < > -

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**.



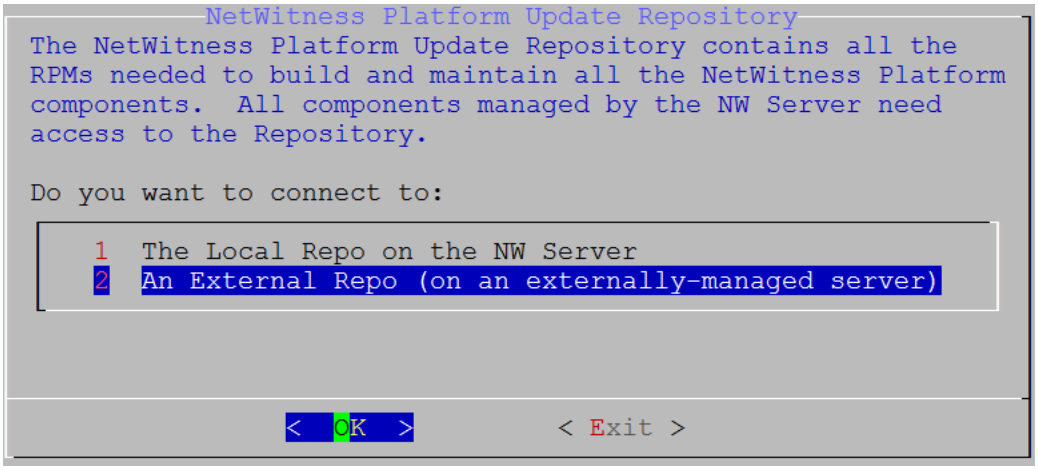
Se muestra el indicador **Contraseña de implementación**.

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**.



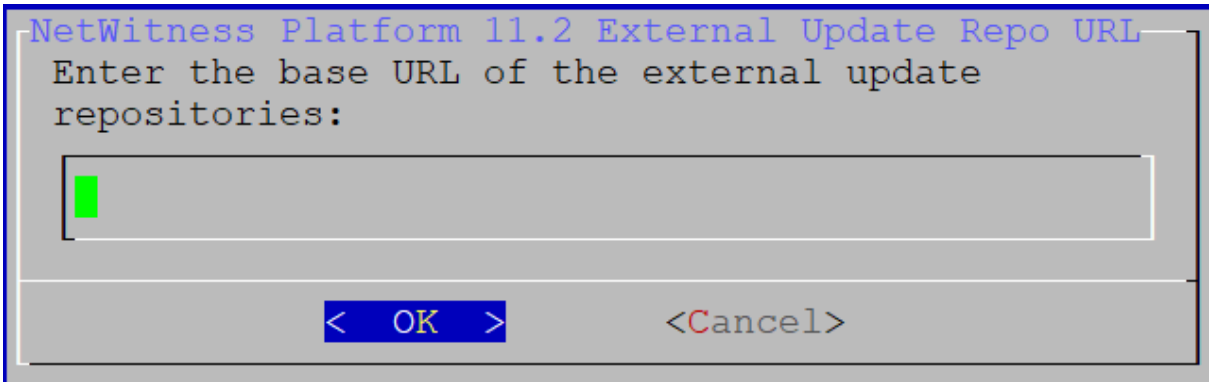
Se muestra el indicador **Repositorio de actualizaciones**.
Debe usar para todos los hosts el mismo repositorio que usó para los hosts del servidor de NW.

8. Use las flechas hacia abajo y hacia arriba para seleccionar **2 Un repositorio externo (en un servidor administrado externamente)**.



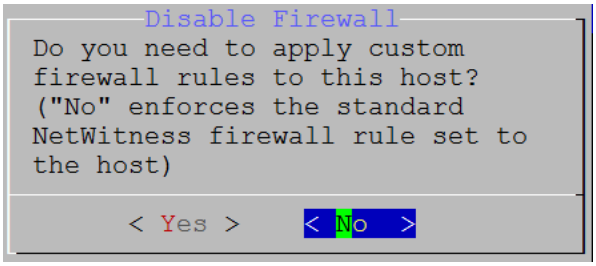
Se muestra el indicador **URL de repositorio de actualización externo**.
Consulte Apéndice D. Crear un repositorio externo para obtener instrucciones. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

9. Ingrese la URL base del repositorio externo de NetWitness Platform (por ejemplo, **http:/testserver/netwitness-repo**) y haga clic en **Aceptar**.

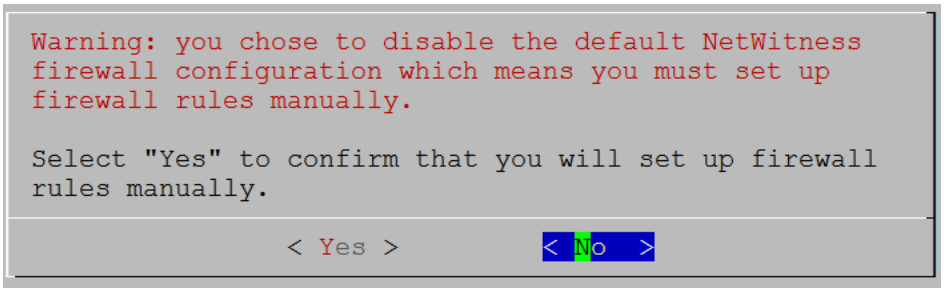


Se muestra el indicador de **deshabilitación** o uso de la configuración del **firewall** estándar.

10. Use la tecla de tabulación para ir a **No** (valor predeterminado) 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.

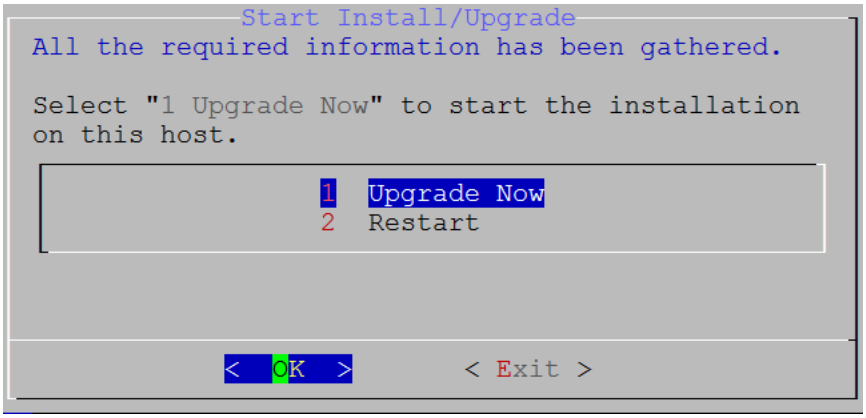


- Si selecciona **Sí**, confirma su selección. Si desea usar la configuración del firewall estándar, seleccione **No**.



Se muestra el indicador **Instalar** o **Actualizar** (la opción **Recuperar** no se aplica a la instalación. Es para Recuperación ante desastres en 11.2).

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 10.6.6.x al servidor de NW 11.2.

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.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
     (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

12. Complete las Servidor de NW antes de actualizar cualquiera de los hosts que no son de servidores de SA a 11.2.

Configurar un host de servidor que no es de NW 11.2

Asegúrese de respaldar los datos de 10.6.6.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 11.2, de modo que los datos sean lo más recientes posible.

Realice los siguientes pasos para configurar un host de servidor que no es de NW 11.2.

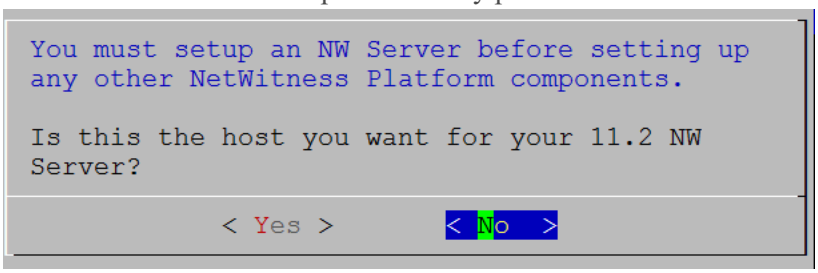
1. Inicie sesión en la consola de la VM que no es de servidor de NW 11.2 y ejecute el comando `nwsetup-tui`.
   Esto inicia el programa de instalación y se muestra el EULA.
2. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
                                                                      92%
                    <Accept >            <Decline>
```

   Se muestra el indicador **¿Es este el host que desea para el servidor de NW 11.2?**.

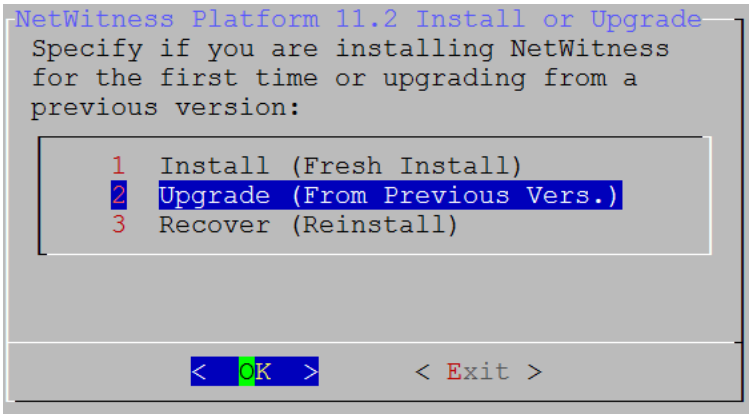
   Precaución: Si elige el host incorrecto para el servidor de NW y completa la actualización, debe repetir los pasos del 1 al 11 de Configurar un host del servidor de NW 11.2 para corregir este error.

3. Use la tecla de tabulación para ir a **No** y presione **Intro**.



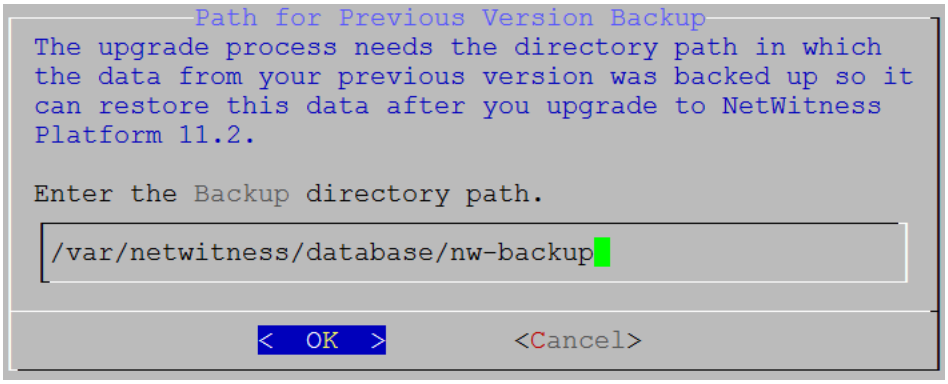
Se muestra el indicador **Instalar** o **Actualizar** (la opción **Recuperar** no se aplica a la instalación. Es para Recuperación ante desastres en 11.2).

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.



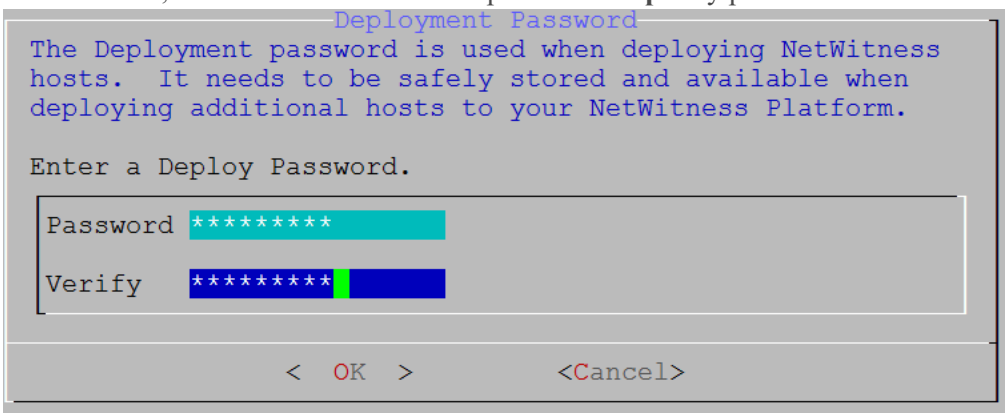
En esta tabla se enumeran las rutas de respaldo y restauración por host/servicio.

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

Se muestra el indicador **Contraseña de implementación**.

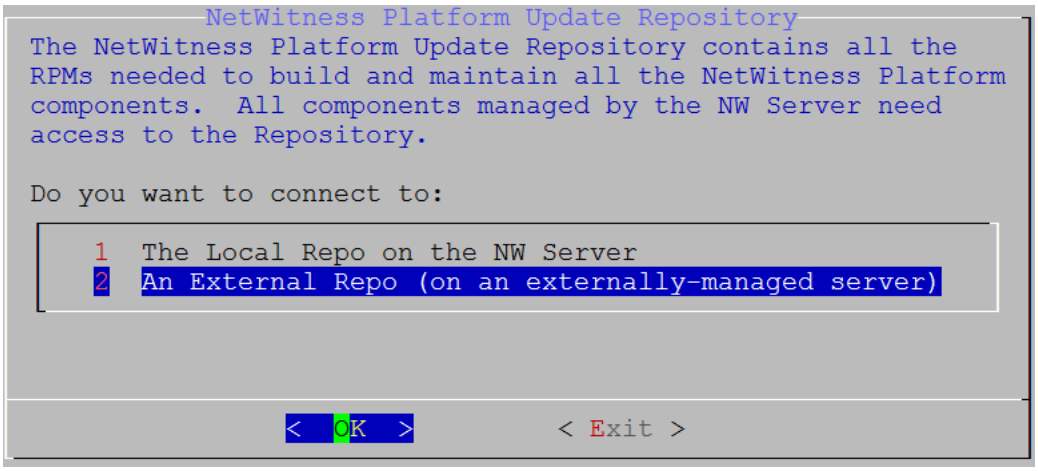
Nota: Debe usar la misma contraseña de implementación que usó cuando actualizó el servidor de NW.

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**.



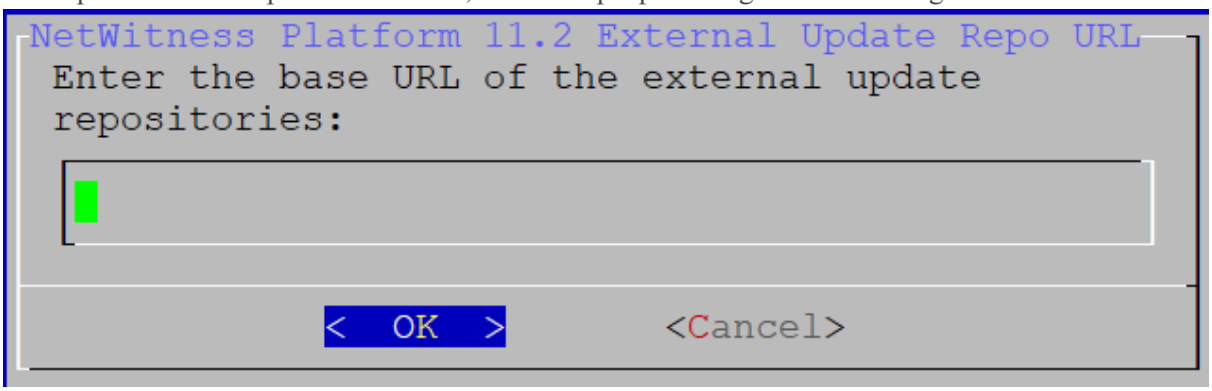
Se muestra el indicador **Repositorio de actualizaciones**.

7. Use las flechas hacia abajo y hacia arriba para seleccionar **2 Un repositorio externo (en un servidor administrado externamente)**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.



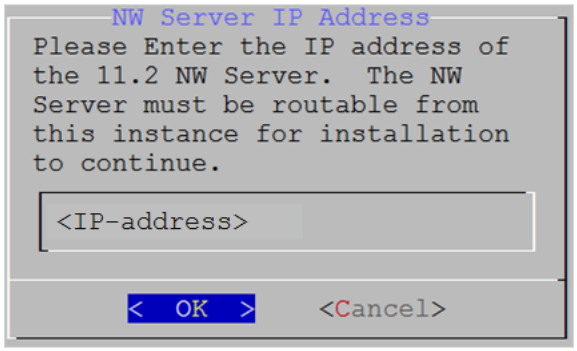
Se muestra el indicador **URL de repositorio de actualización externo**.
Los repositorios otorgan acceso a las actualizaciones de RSA y a las actualizaciones de CentOS.

8. Ingrese la URL base del repositorio externo de NetWitness Platform (por ejemplo, **http://testserver/netwitness-repo**) y haga clic en **Aceptar**. Consulte Apéndice D. Crear un repositorio externo para obtener instrucciones sobre cómo crear este repositorio y la dirección URL correspondiente del repositorio externo, de modo que pueda ingresarla en el siguiente indicador.



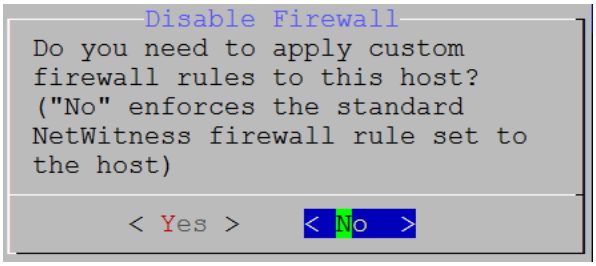
Se muestra la **dirección IP del servidor de NW**.

9. Escriba la dirección IP del servidor de NW, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

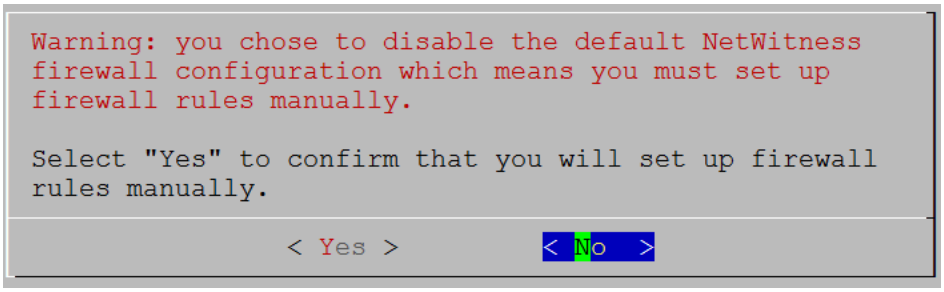


Se muestra el indicador de **deshabilitación** o uso de la configuración del **firewall** estándar.

10. Use la tecla de tabulación para ir a **No** (valor predeterminado) 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.



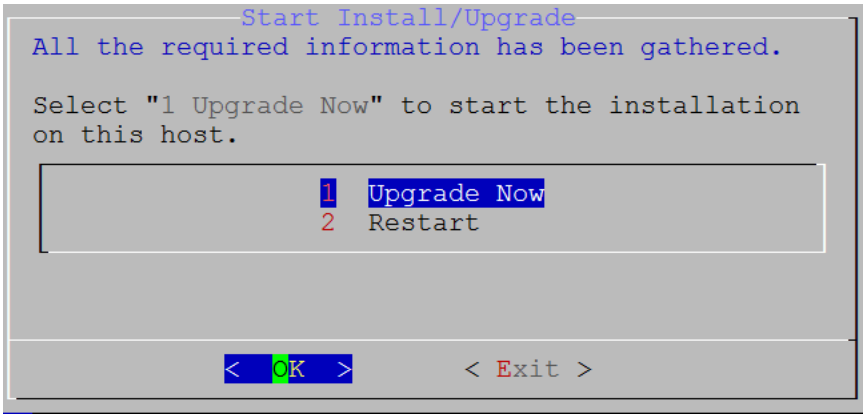
- Si selecciona **Sí**, confirme su selección.



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

Se muestra el indicador **Instalar** o **Actualizar** (la opción **Recuperar** no se aplica a la instalación. Es para Recuperación ante desastres en 11.2).

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 11.2.

12. Instale el servicio en este host:

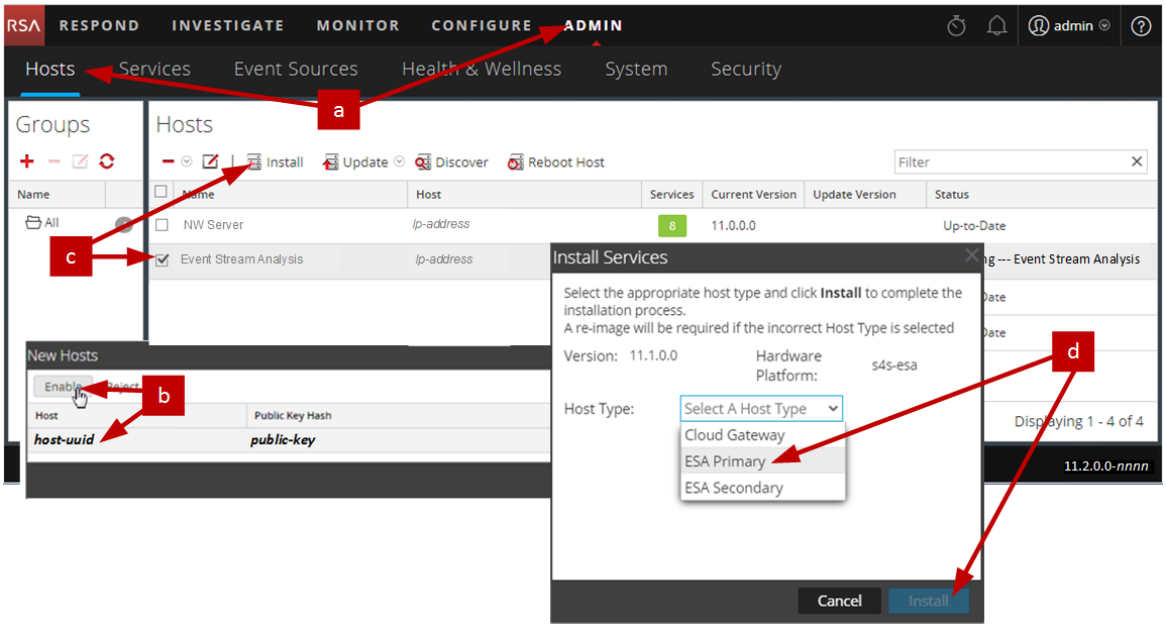
    a. Inicie sesión en NetWitness Platform y haga clic en **ADMINISTRAR** > **Hosts**.
    El cuadro de diálogo **Nuevos hosts** se muestra con la vista **Hosts** atenuada en segundo plano.

    Nota: Si no se muestra el cuadro de diálogo **Nuevos hosts**, haga clic en **Descubrir** en la barra de herramientas de la vista Hosts.

b. 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**.

c. Seleccione ese host en la vista **Hosts** (por ejemplo, **Event Stream Analysis**) y haga clic en Install
Se muestra el cuadro de diálogo **Instalar servicios**.

d. Seleccione el servicio adecuado (por ejemplo, **ESA primario**) y haga clic en **Instalar**.



Se completó la actualización del host que no es de servidor de NW en NetWitness Platform.

Nota: Cuando actualiza un host de Respond de 10.6.6.x a 11.2, tarda un tiempo para que Respond vuelva a estar en línea. Esto se debe a la indexación de datos de Respond mientras se restaura. El tamaño de los datos en la base de datos de Mongo determinará el tiempo.

Actualizar o instalar la recopilación de Windows existente

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

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

Tareas posteriores a la actualización

En este tema se enumeran las tareas que debe completar después de actualizar los hosts de 10.6.6.x a 11.2. Estas tareas se organizan en las siguientes categorías.

General

Tarea 1: Asegurarse de que el puerto 15671 esté configurado correctamente

El puerto 15671 es nuevo en 11.x, pero no es necesario abrir un firewall para él. Asegúrese de que 15671, y todos los puertos, estén configurados como se muestra en el tema "Arquitectura y puertos de red" de la ***Guía de implementación de*** *RSA NetWitness® Platform*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

(Condicional) Tarea 2: Restaurar las funciones personalizadas de analista

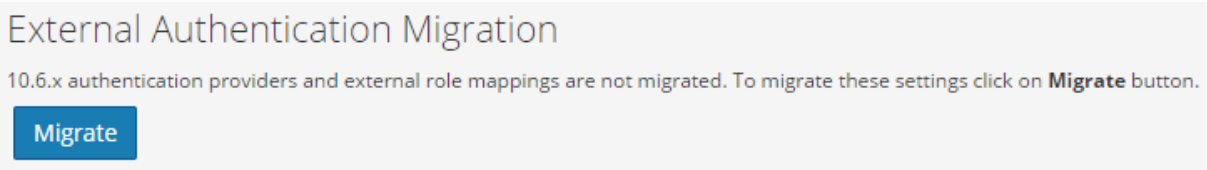
Si tenía funciones personalizadas de analista en 10.6.6.x, debe restablecerlas en 11.2. Consulte "Agregar una función y asignar permisos" en la *Guía de administración de usuarios y de la seguridad del sistema* de RSA *NetWitness Platform*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Servidor de NW

Tarea 3: Migrar Active Directory (AD)

La primera vez que inicia sesión en la interfaz del usuario de NetWitness Platform 11.2, debe hacer clic en el botón Migrar para completar la migración de AD.

1. Inicie sesión en NetWitness Platform 11.2 con las credenciales de `admin user`.
2. En el menú de **NetWitness Platform** 11.2, seleccione **ADMINISTRAR** > **SEGURIDAD** y 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 4: Modificar la configuración de AD migrada para cargar el certificado

Si se autenticó a través del servidor de Active Directory (AD) y habilitó SSL para la conexión de AD en 10.6.6.x, debe modificar la configuración de AD migrada para cargar el certificado del servidor de Active Directory.

Realice el siguiente procedimiento para modificar la configuración de AD migrada con el fin de cargar el certificado.

1. En el menú de **NetWitness Platform** 11.2, seleccione **ADMINISTRAR** > **Seguridad** y haga clic en la pestaña **Ajustes de configuración**.
2. En **Configuración de Active Directory**, seleccione una configuración de AD y haga clic en .
   Se muestra el cuadro de diálogo Editar configuración.
3. Vaya al campo **Archivo de certificado**, haga clic en **Navegar** y seleccione un certificado de la red.
4. Haga clic en **Guardar**.

Tarea 5: Reconfigurar el módulo de autenticación con capacidad para conectarse (PAM) en 11.2

Debe reconfigurar PAM después de actualizar a 11.2. 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® Platform*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Puede consultar los archivos de configuración de PAM 10.6.6.x en el directorio **/etc** en los datos de respaldo de 10.6.6.x para obtener orientación.

Tarea 6: Restaurar los servidores NTP

Debe usar la interfaz del usuario de NetWitness Platform 11.2 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® Platform* para obtener instrucciones detalladas sobre cómo agregar servidores NTP. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Tarea 7: 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 Platform. Consulte "Paso 1. Registrar el servidor de NetWitness" en la *Guía de administración de licencia de RSA NetWitness Platform* para obtener instrucciones sobre cómo volver a descargar las licencias. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Tarea 8: Volver a mapear la licencia del servidor de NW virtual a la dirección MAC de 10.6.6.x

Si está actualizando un servidor de Security Analytics que se ejecuta en una máquina virtual, cambie el host virtual del servidor de NW 11.2 a la dirección MAC de 10.6.6.x para conservar la licencia. Consulte "Licencia: Paso 1. Registrar el servidor de NetWitness" en la *Guía de administración de licencia de RSA NetWitness Platform* para obtener instrucciones sobre cómo volver a mapear una licencia a una nueva dirección MAC. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

(Condicional) Tarea 9: 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 10: 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:

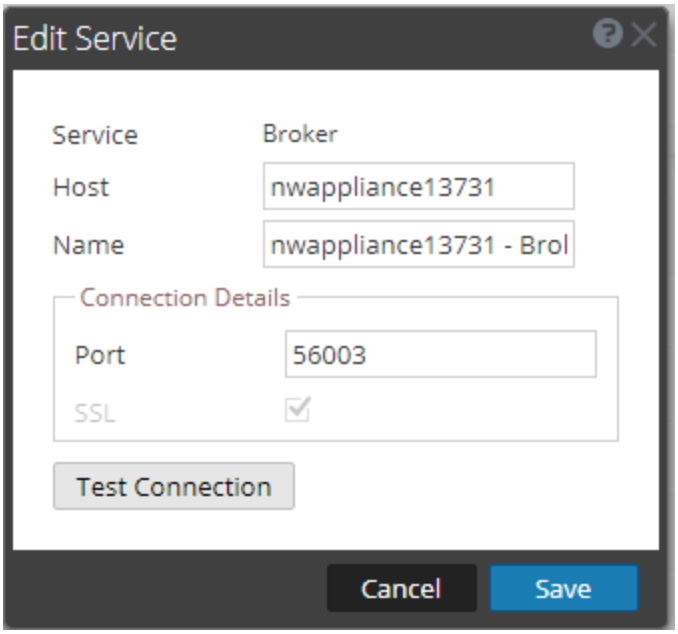
- Usó la imagen ISO base para 10.3.2 o anterior.
- Actualizó el sistema mediante RPM exclusivamente para llegar a 10.6.6.

NetWitness Platform 11.2 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. En el menú de **NetWitness Platform** 11.2, seleccione **ADMINISTRAR** > **Servicios**.
2. 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

3. Haga clic en (Editar) en la barra de herramientas de la vista **Servicios**.
   Se muestra el cuadro de diálogo Editar servicio.
4. 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).



Tarea 11: (Condicional) Corregir las plantillas del registro de auditoría que no están actualizadas en el archivo de configuración de salida de Logstash

Problema: Cuando un usuario actualiza de 10.6.6 a 11.2 y de 11.0.0.0 a 11.2, si está configurada una auditoría global, las plantillas del registro de auditoría no se actualizan en el archivo de configuración de salida de Logstash.

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

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

1. En el menú de **NetWitness Platform** 11.2, seleccione **ADMINISTRAR** > **Sistema** > **Notificaciones globales**.
   Se muestra la vista **Notificaciones globales**.
2. Haga clic en la pestaña **Servidores** y seleccione cualquier servidor de syslog.
3. Haga clic en  (icono de edición) y, a continuación, haga clic en **Guardar**.

RSA NetWitness® Endpoint

Tarea 12: 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 Platform 11.2, el host virtual es `/rsa/system`. Para 10.6.6.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.

Tarea 13: Reconfigurar un feed recurrente configurado desde Endpoint heredado debido a un cambio en la versión de Java

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

1. Importe el certificado de CA de NetWitness Endpoint en el almacén de confianza de NetWitness Platform, como se describe en "Exportar el certificado SSL de NetWitness Endpoint" en el tema "Configurar datos contextuales desde Endpoint a través de un feed recurrente" de la *Guía de integración de RSA NetWitness Endpoint* para importar el certificado.
   Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

RSA NetWitness® Endpoint Insights

(Opcional) Tarea 14: Instalar Endpoint Hybrid o Endpoint Log Hybrid

Consulte:

Guía de instalación de hosts físicos de RSA NetWitness Platform 11.2 para obtener instrucciones acerca de la instalación en un host físico.

Guía de instalación de hosts virtuales de RSA NetWitness Platform 11.2 para obtener instrucciones acerca de la instalación en un host virtual.

Tareas de Event Stream Analysis (ESA)

Tarea 15: Reconfigurar Detección de amenazas automatizadas para ESA

Si usó Detección de amenazas automatizadas en 10.6.6.x, debe completar los siguientes pasos para reconfigurarla mediante el servicio ESA Analytics en 11.2.

1. En el menú de **NetWitness Platform** 11.2, seleccione **ADMINISTRAR** > **Sistema** > **ESA Analytics**.
   Los módulos Suspicious Domains, Command and Control (C2) for Network Data y C2 for Logs requieren una lista blanca denominada "**domains_whitelist**".
2. Condicional: Si aparece la lista blanca de Detección de amenazas automatizadas anterior en la pestaña **Listas** del servicio Context Hub:
   a. Haga clic en **ADMINISTRAR** > **Servicios**, seleccione el servicio Context Hub y, en el menú desplegable de comandos de acción (), haga clic en **Ver** > **Configuración** > pestaña **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 Platform* y la sección "Configurar ESA Analytics" de la *Guía de configuración de NetWitness Platform ESA*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Tarea 16: Para integraciones con Web Threat Detection, Archer Cyber Incident & Breach Response o NetWitness Endpoint, configurar SSL autenticado mutuamente

Si se integra con Web Threat Detection, Archer Cyber Incident & Breach Response 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 10.6.6.x (consulte Instrucciones para respaldo).

1. Cree un usuario en el sistema host que debe integrarse con NetWitness Platform mediante el inicio de sesión en el host y la ejecución del 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 17: Habilitar el Tablero Amenaza: Indicadores de malware

En 11.2.0, el nombre **Tablero Amenaza: Indicadores** de 10.6.6.x se cambió a **Tablero Amenaza: Indicadores de malware**. Si usó este tablero en 10.6.6.x, debe:

1. Habilitar el **Tablero Amenaza: Indicadores de malware** en 11.2.
2. Configurar el origen de datos para los dashlets nuevos.
   Consulte "Dashlets" en RSA Link (https://community.rsa.com/docs/DOC-81463) para obtener una descripción de los dashlets en el contexto de NetWitness Platform.

Investigate

Tarea 18: Asegurarse de que las funciones de usuario personalizadas tengan permisos `Investigate-server` para el acceso a Análisis de eventos

Después de actualizar a 11.2.0.0, el permiso `investigate-server.*` de las funciones de usuario personalizadas no está habilitado de manera predeterminada. Realice el siguiente procedimiento para asegurarse de que las funciones de usuario correspondientes tengan permiso para acceder a Análisis de eventos.

1. Inicie sesión en NetWitness Platform 11.2.0.0 con sus credenciales de `Admin user` y vaya a **ADMINISTRAR** > **Seguridad**.
2. Haga clic en la pestaña **Funciones**.
3. Seleccione las funciones que necesitan permisos `investigate-server.*` y haga clic en (icono de edición).
4. Seleccione la pestaña **Servidor de Investigate** bajo **Permisos**.
5. Si la casilla de verificación **investigate-server** no está seleccionada, selecciónela para los usuarios que requieran acceso a Análisis de eventos.

6. Haga clic en **Guardar**.

Recopilación de registros

Tarea 19: 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 11.2 para asegurarse de que todos los protocolos de recopilación reanuden la operación normal.

Restablecer valores de sistema estables para Lockbox

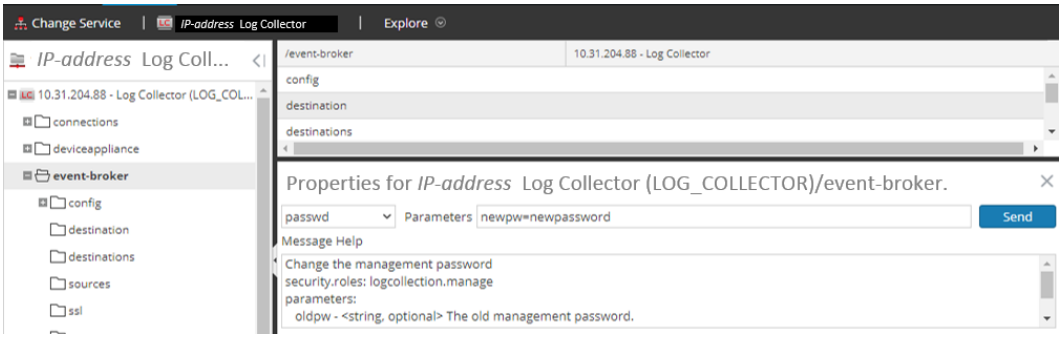
El Lockbox almacena la clave para cifrar el origen de eventos y otras contraseñas para el Log Collector. El servicio Log Collector no puede abrir el Lockbox debido a los cambios de los valores de sistema estables. Como resultado, debe restablecer los valores de sistema estables para Lockbox. Consulte "Recopilación de registros: Paso 3. Configurar un Lockbox" en la *Guía de configuración de la recopilación de registros* de *RSA NetWitness® Platform* para obtener instrucciones. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

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 11.2.

1. En el menú de **NetWitness Platform** 11.2, seleccione **ADMINISTRAR > Servicios**.
2. Seleccione el servicio Log Collector.
3. Haga clic en (Acciones) > **Ver** > **Explorar**.
4. Haga clic con el botón secundario en `event-broker` > **Propiedades**.

5. 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 10.6.6.x en que FIPS está habilitado para Log Collectors, Log Decoders y Network Decoders)

Tarea 20: 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® Platform*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Decoder y Log Decoder

(Condicional) Tarea 21: Habilitar metadatos para el analizador GeoIP2

De manera predeterminada, el analizador GeoIP2 genera menos metadatos que el analizador GeoIP. Después de la actualización a 11.2, si necesita cualquiera de los metadatos adicionales, debe habilitarlos (una sola vez) para cada decodificador. Esto también se puede modificar después de la actualización. Tenga en cuenta que los campos de metadatos `isp` y `org` suelen producir un valor equivalente a `domain`.

Para habilitar los metadatos:

1. Vaya a **ADMINISTRAR** > **Servicios**.
2. En la vista **Servicios de Administration**, seleccione un Log Decoder o un Decoder.
3. Haga clic en el icono de configuración () y seleccione **Ver** > **Configuración**. Se muestra el panel Configuración de analizadores, desde el que puede seleccionar **GeoIP2** para habilitar los metadatos deseados.

Para obtener más información acerca de los analizadores GeoIP2, consulte el tema "Analizadores GeoIP2 y GeoIP" en la *Guía de configuración de Decoder y Log Decoder*.

Reporting Engine

Tarea 22: 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 10.6.6.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 11.2.

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 23: 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® Platform* para obtener instrucciones. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Respond

Tarea 24: Restaurar las claves personalizadas del servicio Respond

En 10.6.6.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 10.6.6.x.
2. Vaya a `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` en 11.2.
   Este es el nuevo archivo para 11.2.
3. Edite `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` para incluir las claves personalizadas que copió en el paso uno.

Tarea 25: Restaurar scripts de normalización del servicio Respond personalizados

RSA refactorizó los scripts de normalización del servicio Respond en 11.2 y los transfirió a la siguiente ubicación nueva:
`/var/lib/netwitness/respond-server/scripts`
Si personalizó estos scripts en 10.6.6.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 10.6.6.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 10.6.6.x.
3. Ir al directorio `/var/lib/netwitness/respond-server/scripts`.
   Este directorio es donde NetWitness Platform 11.2 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 10.6.6.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.

Tarea 26: Agregar la configuración de notificaciones de Respond para las funciones personalizadas

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

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

Tarea 27: Establecer manualmente la configuración de notificaciones de Respond

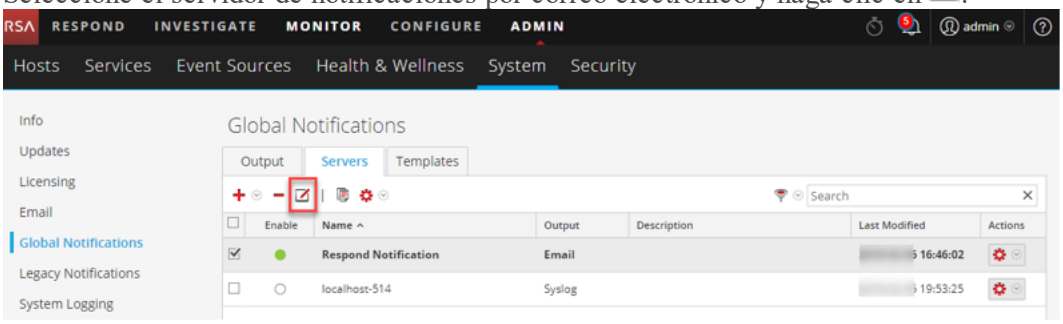
La configuración de notificaciones de Incident Management en NetWitness Platform 10.6.6.x a 11.2 es diferente de la configuración de notificaciones de Respond disponible en 11.2, razón por la cual la configuración existente de 10.6.6.x a 11.2 no se migrará a 11.2.

La configuración de notificaciones de NetWitness Respond permite el envío de notificaciones por correo electrónico a los administradores del SOC y al analista asignado a un incidente cuando este se crea o se actualiza.

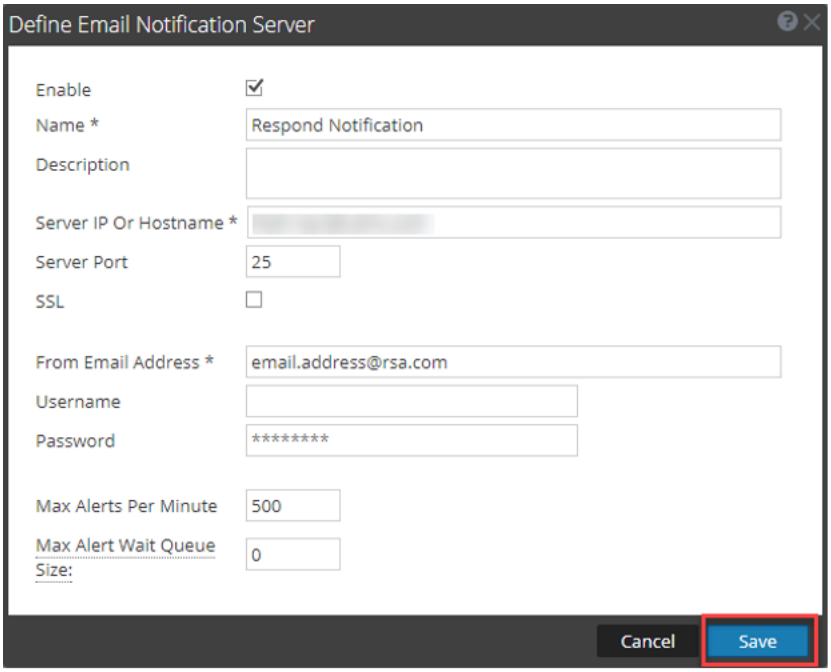
Para establecer manualmente la configuración de notificaciones de Respond, vaya a **CONFIGURAR** > **Notificaciones de Respond.** Consulte el procedimiento "Establecer la configuración de notificaciones por correo electrónico de Respond" en la *Guía de configuración de NetWitness Respond*.

Los servidores de notificaciones de 10.6.6.x a 11.2 no se muestran en la lista desplegable Servidor de correo electrónico. Los servidores de correo electrónico se deben editar y guardar en el panel Servidores de notificaciones globales (**ADMINISTRAR** > **Sistema** > **Notificaciones globales** > pestaña **Servidor**).

1. En el menú de **NetWitness Platform** 11.2, seleccione **ADMINISTRAR** > **Sistema** > **Notificaciones globales** > pestaña **Servidor**.
2. Vaya a **CONFIGURAR** > **Notificaciones de Respond**. Se muestra la vista Configuración de notificaciones de Respond.
3. Observe que los servidores de notificaciones por correo electrónico no aparecen en la lista desplegable SERVIDOR DE CORREO ELECTRÓNICO.
4. Haga clic en vínculo **Configuración de servidor de correo electrónico**. Verá el panel Notificaciones globales.
5. Haga clic en la pestaña **Servidores**.
6. Para cada uno de los servidores de notificaciones por correo electrónico:
   a. Seleccione el servidor de notificaciones por correo electrónico y haga clic en .



b. En el cuadro de diálogo Definir servidor de notificación de correo electrónico, haga clic en **Guardar**.



7. Vuelva a **CONFIGURAR** > **Notificaciones de Respond**. Los servidores aparecerán en la lista desplegable **SERVIDOR DE CORREO ELECTRÓNICO**.
   Las plantillas de notificación personalizadas de Incident Management no se pueden migrar a 11.2. 11.2 no es compatible con las plantillas personalizadas.

Tarea 28: Actualizar los valores de Agrupar por de las reglas de incidentes predeterminadas

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

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

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

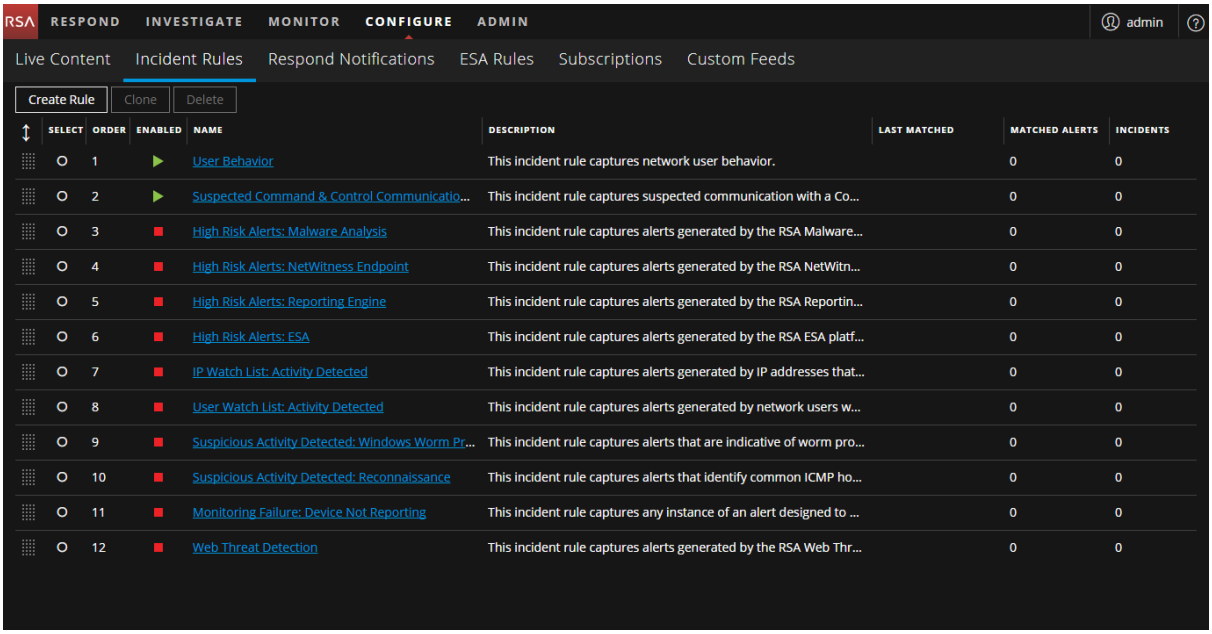
Tarea 29: Agregar el campo Agrupar por a las reglas de incidentes

El campo **Agrupar por** no se requiere en 10.6.6, pero sí en 11.2. Después de la actualización a

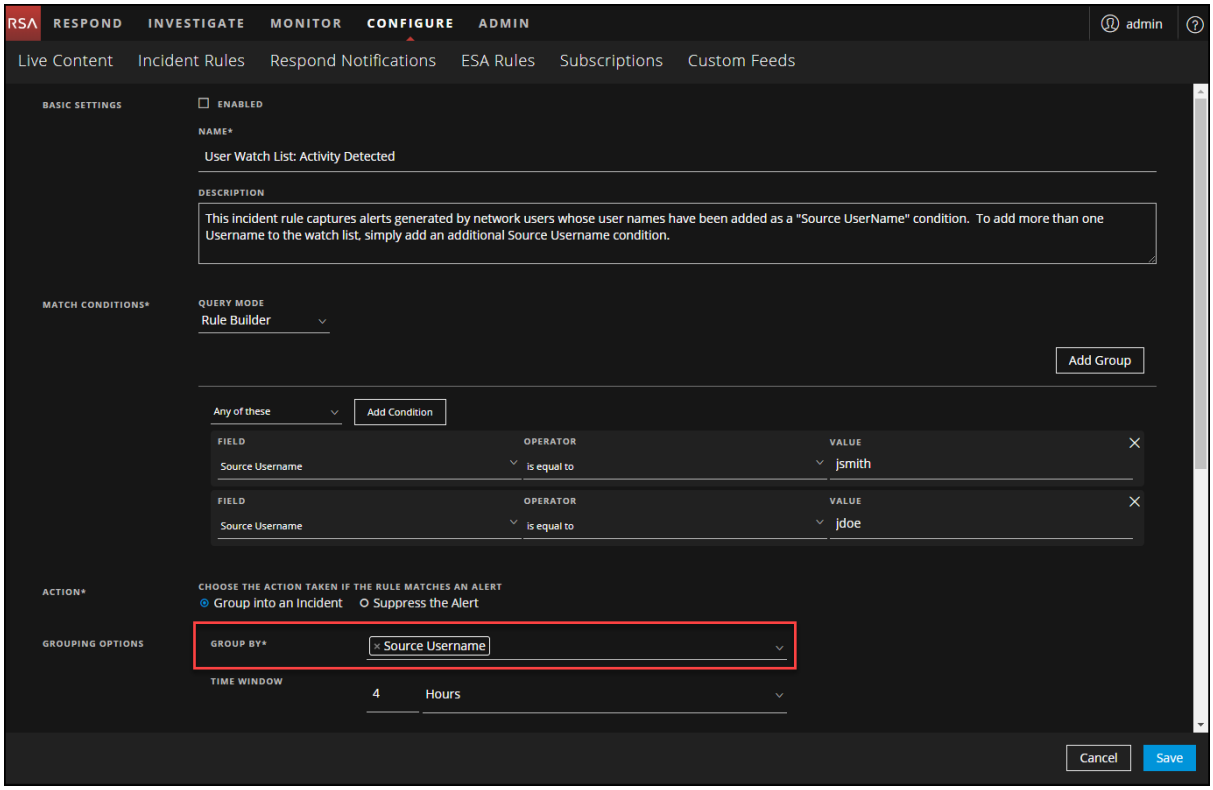
11.2, algunas reglas de incidentes no tendrán un campo **Agrupar por**, por lo que debe agregarlo a las reglas o estas no funcionarán y no crearán incidentes.

Realice los siguientes pasos para cada regla de incidentes:

1. En el menú de **NetWitness Platform** 11.2, vaya a **CONFIGURAR** > **Reglas de incidentes** y haga clic en el vínculo de la columna Nombre correspondiente a la regla que desea actualizar.



2. En el campo Agrupar por, verifique que esté seleccionado un valor de Agrupar por. Si no es así, seleccione un valor de Agrupar por.



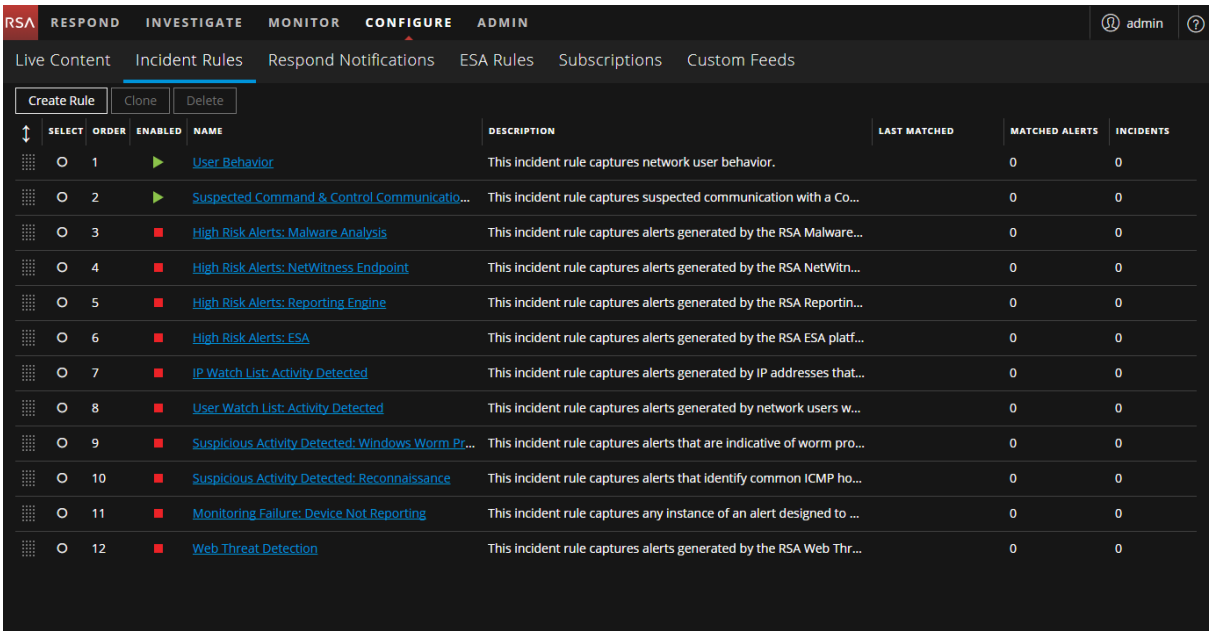
3. Haga clic en **Guardar** para actualizar la regla.
   Para obtener información sobre las reglas de incidentes, consulte la *Guía de configuración de NetWitness Respond*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Tarea 30: Actualizar las reglas de incidentes identificadas en la tarea de preparación para la actualización Dominio en las condiciones de coincidencia

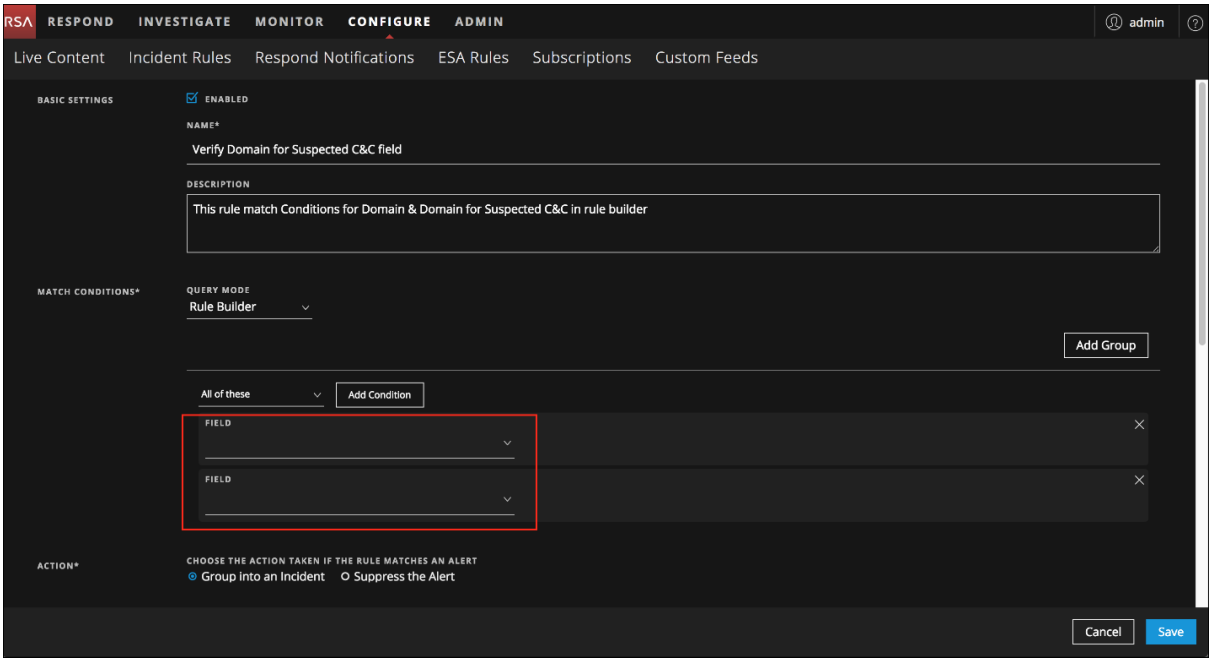
Modifique las reglas de incidentes que identificó en la tarea de preparación para la actualización Tarea 5: Comprobar las condiciones de coincidencia de las reglas de agregación para “Dominio” o “Dominio para Sospecha de C&C”, las cuales contenían Dominio o Dominio para Sospecha de C&C en las condiciones de coincidencia del generador de reglas.

Para cada regla que identificó anteriormente:

1. En el menú de **NetWitness Platform** 11.2, seleccione **CONFIGURAR** > **Reglas de incidentes** y haga clic en el vínculo de la columna Nombre correspondiente a la regla que desea actualizar.



2. En la sección **Condiciones de coincidencia**, en los campos en blanco, seleccione **Dominio** y **Dominio para Sospecha de C&C** en la lista desplegable y, a continuación, seleccione las condiciones que identificó anteriormente en las tareas previas a la actualización.



3. Haga clic en **Guardar** para actualizar la regla.
Para obtener información sobre las reglas de incidentes, consulte la *Guía de configuración de NetWitness Respond*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Incidente cibernético y respuesta ante vulneración de RSA Archer®

Tarea 31: Reconfigurar la integración de Incidente cibernético y respuesta ante vulneración de Archer®

Para obtener información sobre cómo reconfigurar Incidente cibernético y respuesta ante vulneración de Archer® para Event Stream Analysis, Reporting Engine y Respond, consulte la *Guía de integración de RSA Archer*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

User and Entity Behavior Analytics (UEBA)

(Opcional) Tarea 32: Instalar UEBA

UEBA es una nueva característica a partir de NetWitness Platform 11.2.

Consulte:

Guía de instalación de hosts físicos de RSA NetWitness Platform 11.2 para obtener instrucciones acerca de la instalación en un host físico.

Guía de instalación de hosts virtuales de RSA NetWitness Platform 11.2 para obtener instrucciones acerca de la instalación en un host virtual.

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

Respaldo

Tarea 33: Quitar los archivos relacionados con el 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 11.2 todos los datos desde su respaldo antes de quitar los archivos relacionados con el respaldo de los directorios locales de sus hosts 11.2.

Archivos `.tar` de respaldo

Después de que todos los hosts se actualizan a 11.2, 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`

Apéndice A. Solución de problemas

En esta sección se describen las soluciones a problemas que podría encontrar durante las instalaciones y las actualizaciones. En la mayoría de los casos, NetWitness Platform 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.

- Interfaz de la línea de comandos (CLI)
- Script de respaldo
- Event Stream Analysis
- Servicio Log Collector (`nwlogcollector`)
- Orchestration
- Servidor de NW
- Reporting Engine
- NetWitness UEBA

Interfaz de la línea de comandos (CLI)

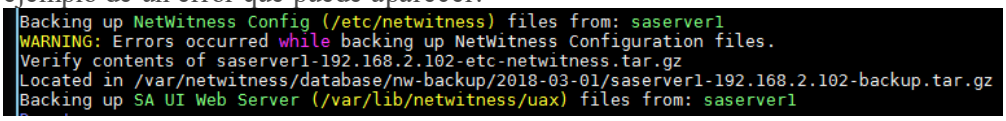
Mensaje de error	La interfaz de la línea de comandos (CLI) muestra: "La operación de coordinación falló." `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Causa	Ingresó la contraseña de `deploy_admin` incorrecta en `nwsetup-tui`.
Solución	Recupere su contraseña de `deploy_admin`. 1. Acceda mediante el protocolo SSH al host del servidor de NW. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` Acceda mediante el protocolo SSH al host que falló. 2. Vuelva a ejecutar `nwsetup-tui` con el uso de la contraseña de `deploy_admin` correcta.

Mensaje de error	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service`
Causa	NetWitness Platform 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. `systemctl restart rsa-sms`

Mensaje de error	Usted recibe un mensaje en la interfaz del usuario que le solicita reiniciar el host después de actualizar y reiniciar el host offline. 
Causa	No puede utilizar la CLI para reiniciar el host. Debe utilizar la interfaz del usuario.
Solución	Reinicie el host en la vista Host de la interfaz del usuario.

Respaldo (script `nw-backup`)

Mensaje de error	`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.

Error	Respalde los errores ocasionados por la configuración del atributo `immutable`. Este es un ejemplo de un error que puede aparecer: 
Causa	Si tiene algún archivo con la marca inmutable configurada (para impedir que el proceso Puppet sobrescriba un archivo personalizado), el archivo no se incluirá en el proceso de respaldo y se generará un error.
Solución	En el host que contiene los archivos con la marca inmutable configurada, ejecute el siguiente comando para quitar la configuración de inmutable de los archivos: `chattr -i <filename>`

Error	Error al crear el archivo de información de configuración de red debido a entradas duplicadas o incorrectas en el archivo de configuración de red principal: `/etc/sysconfig/network-scripts/ifcfg-em1` Verifique el contenido de `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Causa	Existen entradas incorrectas o duplicadas para alguno de los siguientes campos: DEVICE, BOOTPROTO, IPADDR, NETMASK o GATEWAY, que se encontraron al leer el archivo de configuración de la interfaz de Ethernet principal desde el host que se respalda.

Solución	Cree manualmente un archivo en la ubicación de respaldo en el servidor de respaldo externo, así como en la ubicación de respaldo local en el host donde se han almacenado provisionalmente otros respaldos. El nombre de archivo debe tener el formato `<hostname>-<hostip>-network.info.txt` y debe contener las siguientes entradas:
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problema	El servicio ESA falla después de actualizar a 11.2.0.0 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.

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 de error	`<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 Platform 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 buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Mensaje de error	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Causa	El Lockbox de Log Collector no se configuró después de la actualización.
Solución	Si utiliza un Lockbox de Log Collector, inicie sesión en NetWitness Platform 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 buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Mensaje de error	`<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 Platform 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 buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

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 10.6.6.x a 11.2.0.0 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`

Orchestration

Los registros del servidor de Orchestration se publican en `/var/log/netwitness/orchestration-server/orchestration-server.log` en el host del servidor de NW.

Problema	1. Se intentó sin éxito actualizar un host que no es de servidor de NW. 2. La actualización de este host se reintentó y volvió a fallar. Verá el siguiente mensaje en `orchestration-server.log`. `"'file' _virtual_ returned False: cannot import name HASHES""`
Causa	Salt minion se puede haber actualizado y nunca se reinició en el host fallido que no es de servidor de NW

Solución	1. Acceda mediante el protocolo SSH al host que no es de servidor de NW que no se pudo actualizar.
	2. Ejecute los siguientes comandos.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Reintente la actualización del host que no es de servidor de NW.

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 de error	`<timestamp> : Available free space in /var/netwitness/re-server/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 buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

NetWitness UEBA

Problema	La interfaz del usuario no está accesible.
Causa	Tiene más de un servicio de NetWitness UEBA en la implementación de NetWitness y solamente puede tener uno.

Solución	Realice los siguientes pasos para quitar el servicio de NetWitness UEBA adicional.
	1. Acceda mediante el protocolo SSH al servidor de NW y ejecute los siguientes comandos para consultar la lista de servicios de NetWitness UEBA instalados.
	`# orchestration-cli-client --list-services|grep presidio-airflow`
	`... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`
	`... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`
	2. En la lista de servicios, determine qué instancia del servicio `presidio-airflow` se debe quitar (observando las direcciones de host).
	3. Ejecute el siguiente comando para quitar el servicio extra de Orchestration (utilice el ID de servicio coincidente de la lista de servicios):
	`# orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output>`
	4. Ejecute el siguiente comando para actualizar el nodo 0 con el fin de restaurar NGINX:
	`# orchestration-cli-client --update-admin-node`
	5. Inicie sesión en NetWitness Platform, vaya a **ADMINISTRAR** > **Hosts** y quite el host de NetWitness UEBA extra.

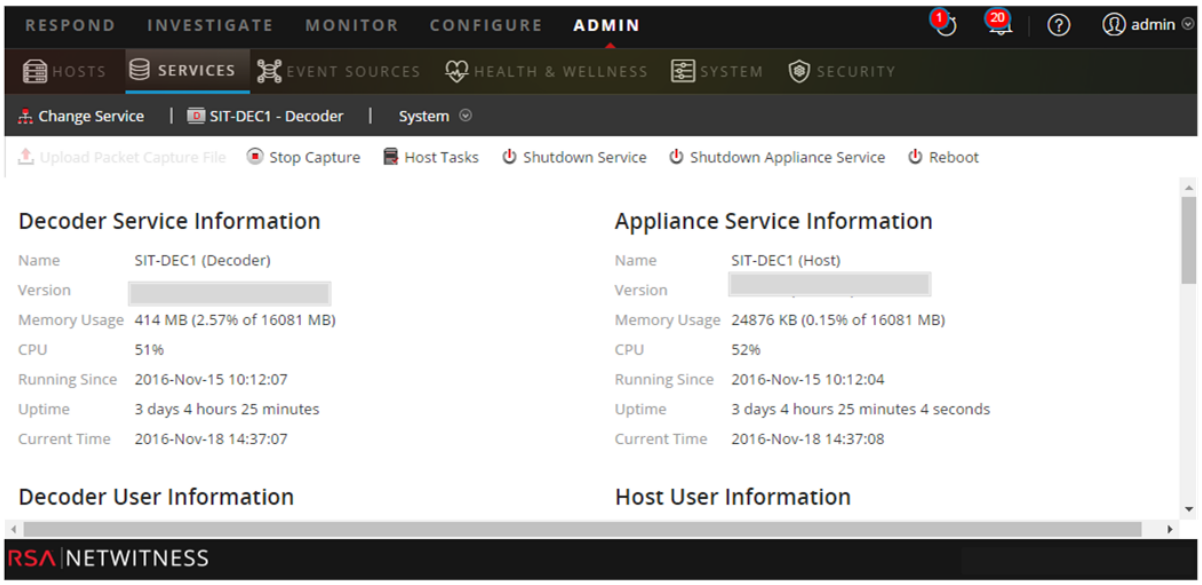
Apéndice B. Detención y reinicio de la captura y la agregación de datos

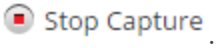
RSA recomienda detener la captura y la agregación de red y registros antes de actualizar un host de Decoder, Concentrator y Broker a 11.2.0.0. Si hace esto, debe reiniciar la captura y la agregación de red y registros después de actualizar estos hosts.

Detener la captura y la agregación de datos

Detener la captura de red

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



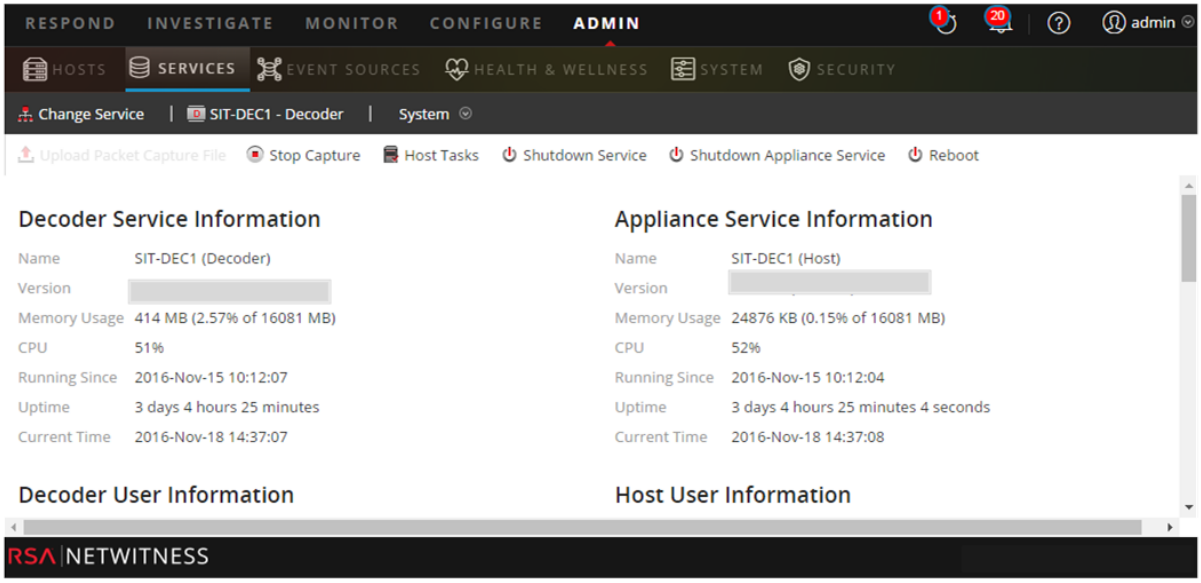
3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en 

.

Detener la captura de registros

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

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

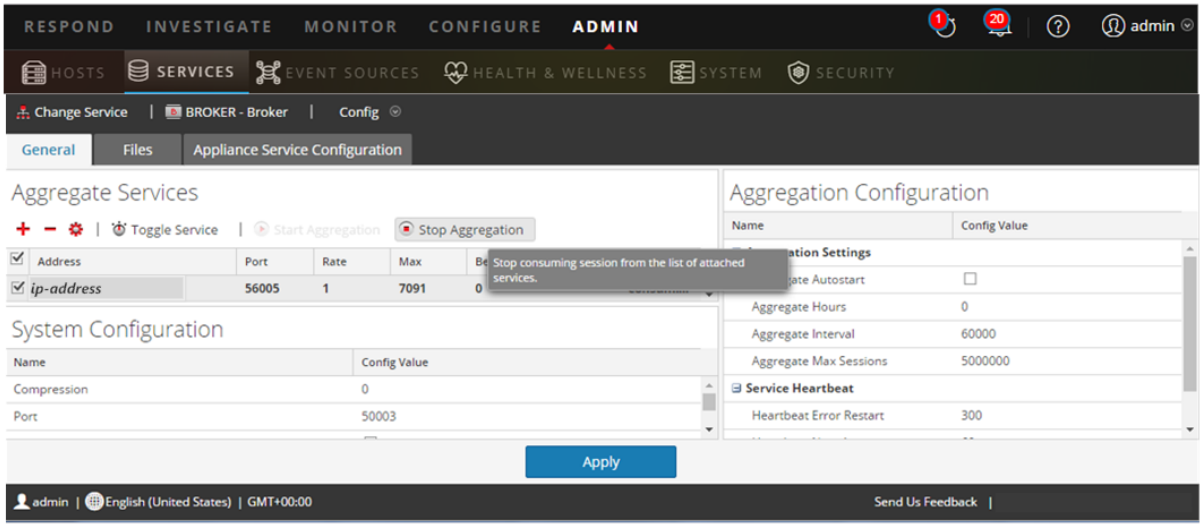


3. En  (acciones), seleccione **Ver** > **Sistema**.

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

Detener agregación

1. Inicie sesión en NetWitness Platform 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 red y registros después de la actualización a 11.2.0.0.

Iniciar la captura de red

1. Inicie sesión en **NetWitness Platform** y vaya a **ADMINISTRAR** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione cada servicio **Decoder**.
3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en 

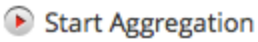
.

Iniciar la captura de registros

1. Inicie sesión en **NetWitness Platform** y vaya a **ADMIN** > **Servicios**.
   Se muestra la vista Servicios.
2. Seleccione cada servicio **Log Decoder**.
3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en 

.

Iniciar agregación

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

.

Apéndice C. Uso de iDRAC

Muchos clientes tienen sitios remotos con acceso físico limitado y ancho de banda limitado desde el escritorio del administrador. Si este es el caso, es posible que desee usar iDRAC con la imagen ISO compartida desde un recurso compartido de NFS que sea local para los dispositivos que se están actualizando o instalando. Esto también le permite usar un dispositivo NetWitness existente como el host de uso compartido.

Por ejemplo:

- Tiene un Concentrator y un Decoder en un sitio en una ubicación geográfica remota.
- El ancho de banda es relativamente bajo a ese sitio desde el sitio del administrador.
- No es práctico enviar una memoria USB y hacer que una persona la conecte a las computadoras mientras se ejecuta la actualización.

En esta situación, puede:

1. Instalar el archivo RPM nfs-utils.
2. Configurar el recurso compartido de NFS.
3. Configurar iDRAC para conectarse a ese recurso compartido.
   Asegúrese de actualizar los sistemas operativos Windows y Linux compatibles con el firmware de iDRAC. Descargue y ejecute los paquetes de actualización de Dell para sistemas operativos Windows y Linux compatibles desde el sitio web de soporte de Dell en http://www.support.dell.com. Para obtener más información, consulte el documento Dell Update Package User's Guide disponible en el sitio web de soporte de Dell en http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf.
4. Arrancar desde los medios virtuales que contienen el archivo ISO y continuar con la actualización.

Configurar el servidor NFS: archivo de configuración del servidor NFS

1. Instale NFS y sus utilidades comunes con yum.
   ```
   yum install nfs-utils
   ```
2. Configure el servicio de NFS para que se ejecute durante el arranque.
   ```
   chkconfig nfs on
   ```
3. Configure el servicio rpcbind para que se ejecute durante el arranque.
   NFS requiere este servicio y debe estar en ejecución antes de que NFS se pueda iniciar.
   ```
   chkconfig rpcbind on
   ```
4. Inicie el servicio rpcbind.
   ```
   service rpcbind start
   ```
5. Inicie el servicio de NFS.
   ```
   service nfs start
   ```
6. Cree un directorio para nuestra primera exportación.
   ```
   mkdir /exports/files
   ```

7. Abra el archivo de exportaciones de NFS en un editor de texto.
   `vi /etc/exports`
8. Para exportar el directorio a cualquier usuario con acceso de solo lectura, agregue la siguiente línea.
   `/exports/files *(ro)`
9. Guarde los cambios y salga del editor.
   `:wq!`
10. Exporte el directorio que se definió anteriormente.
    `exportfs -a`
11. Desactive las reglas de firewall durante la ejecución de las actualizaciones.
    `service iptables stop`
12. Copie los medios de instalación que contienen el archivo ISO en el directorio `/exports/files` .

Arrancar iDRAC desde la configuración de NFS

Nota: Debe verificar que el firmware de iDRAC sea al menos 1.57.57 para la serie 4 (R620).

1. Inicie sesión en la interfaz de iDRAC.
2. Conecte los medios a través del uso compartido de archivos remoto.
   `<server ip>:/export/files/11.2.0.0.iso`
   Por ejemplo: `10.10.10.10:/exports/files/rsa-11.2.0.0.1948.el7-usb.iso`
3. Haga clic en **Conectar**.
4. Inicie **Consola**.
5. En el menú **próximo arranque**, seleccione **DVD/CD virtual**.
6. Restablezca el dispositivo.

Apéndice D. Crear un repositorio externo

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

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

1. Inicie sesión en el host del servidor web.
2. Cree un directorio para alojar el repositorio de NW (`netwitness-11.2.0.0.zip`), por ejemplo `ziprepo` bajo `web-root` del servidor web. Por ejemplo, si `/var/netwitness` es la `web-root`, ejecute la siguiente cadena de comandos.
   `mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Cree el directorio 11.2.0.0 bajo `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0`
4. Cree los directorios `OS` y `RSA` bajo `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`
5. Descomprima el archivo `netwitness-11.2.0.0.zip` en el directorio `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.
   `unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0`
   Con la descompresión de `netwitness-11.2.0.0.zip` se obtienen dos archivos zip (`OS-11.2.0.0.zip` y `RSA-11.2.0.0.zip`) y algunos otros archivos.
6. Descomprima
   a. `OS-11.2.0.0.zip` en el directorio `/var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`.
      `unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
      En el siguiente ejemplo se ilustra la forma en que aparecerá la estructura de archivos del sistema operativo (SO) después de descomprimir el archivo.

Parent Directory		-
GeoIP-1.5.0-11.el7.x86_64.rpm	20-Nov-2016 12:49	1.1M
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 10:07	4.6M
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 10:05	1.5M
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	502K
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	15K
PyYAML-3.11-1.el7.x86_64.rpm	19-Dec-2017 12:30	160K
SDL-1.2.15-14.el7.x86_64.rpm	25-Nov-2015 10:39	204K
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 10:04	81K
adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm	13-Feb-2018 05:10	706K
alsa-lib-1.1.3-3.el7.x86_64.rpm	10-Aug-2017 10:52	421K
at-3.1.13-22.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	51K
atk-2.22.0-3.el7.x86_64.rpm	10-Aug-2017 10:53	258K
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 10:04	66K

b. `RSA-11.2.0.0.zip` en el directorio `/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`.
`unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`
En el siguiente ejemplo se ilustra la forma en que aparecerá la estructura de archivos de actualización de la versión de RSA después de descomprimir el archivo.

Parent Directory		-
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07	1.2M
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07	173K
bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03	203K
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07	52K
cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14	85K
device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	134K
dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36	277K
elasticsearch-5.6.9.rpm	17-Apr-2018 09:37	32M
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07	17K
fneserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11	1.3M
htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23	102K
i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08	399K
ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41	441K
iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20	51K
ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08	374K

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

7. Use `http://<web server IP address>/<your-zip-file-repo>` en respuesta al indicador **Ingrese la dirección URL base de los repositorios de actualización externos** del programa de instalación de NW 11.2.0.0 (`nwsetup-tui`).

Historial de revisiones

Revisión	Fecha	Descripción	Autor
1.0	17/08/2018	Liberación a Operaciones	IDD