RSA NETWITNESS® SUITE

Guía de instalación de hosts virtuales

para la versión 11.0.0.0

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

febrero 2018

Contenido

Guía de instalación de hosts virtuales

En este documento se proporcionan instrucciones sobre la instalación y la configuración de los hosts de RSA NetWitness® Suite que se ejecutan en un ambiente virtual.

Implementación virtual básica

Este tema presenta reglas y requisitos generales para la implementación de RSANetWitness Suite11.0.0.0 en un ambiente virtual.

Abreviaturas que se utilizan en la Guía de implementación virtual

Abreviaturas	Descripción
CPU	Unidad central de procesamiento
EPS	Eventos por segundo
VMware ESX	Hipervisor tipo 1 de clase empresarial; versiones compatibles: 6.5, 6.0 y 5.5
GB	Gigabyte. 1 GB = 1,000,000,000 de bytes
Gb	Gigabit. 1 Gb = 1,000,000,000 de bits.
Gb/s	Gigabits por segundo o mil millones de bits por segundo. Mide el ancho de banda en un medio de transmisión de datos digital, como la fibra óptica.
GHz	GigaHertz 1 GHz = 1,000,000,000 de Hz
IOPS	Operaciones de entrada/salida por segundo
Mb/s	Megabits por segundo o un millón de bits por segundo. Mide el ancho de banda en un medio de transmisión de datos digital, como la fibra óptica.
NAS	Almacenamiento conectado en red
OVF	Formato de virtualización de código abierto
OVA	Dispositivo virtual abierto. Para los fines de esta guía, OVA significa host virtual abierto.
RAM	Memoria de acceso aleatorio (también conocida como memoria)
SAN	Red de área de almacenamiento
Disco duro SSD/EFD	Disco duro de estado sólido/Enterprise Flash Drive

Abreviaturas	Descripción
SCSI	Small Computer System Interface
SCSI (SAS)	Protocolo serie de punto a punto que transfiere datos hacia y desde dispositivos de almacenamiento de computadoras, como discos duros y unidades de cinta.
vCPU	Unidad central de procesamiento virtual (también conocida como un procesador virtual)
vRAM	Memoria de acceso aleatorio virtual (también conocida como memoria virtual)

Hosts virtuales compatibles

Puede instalar los siguientes hosts de NetWitness Suite en el ambiente virtual como un host virtual y heredar características que proporciona el ambiente virtual:

- Servidor de NetWitness
- Event Stream Analysis: ESA primario y ESA secundario
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector

Debe conocer los siguientes conceptos de la infraestructura de VMware:

- VMware vCenter Server
- VMware ESXi
- Máquina virtual

Para obtener información sobre los conceptos de VMware, consulte la documentación del producto VMware.

Los hosts virtuales se proporcionan como un OVA. Debe implementar el archivo OVA como máquina virtual en su infraestructura virtual.

Medios de instalación

Los medios de instalación se encuentran en la forma de paquetes de OVA, los cuales están disponibles para descarga e instalación en Download Central (https://download.rsasecurity.com). Como parte del cumplimiento de pedidos, RSA le brinda acceso al OVA.

Recomendaciones para ambientes virtuales

Los dispositivos virtuales instalados con los paquetes de OVA tienen la misma funcionalidad que los hosts de hardware de NetWitness Suite. Esto significa que, cuando implemente hosts virtuales, debe tener en cuenta el hardware de back-end. RSA recomienda realizar las siguientes tareas durante la configuración del ambiente virtual.

- Según los requisitos de recursos de los diferentes componentes, siga las mejores prácticas para utilizar el sistema y el almacenamiento exclusivo de forma correcta.
- Asegúrese de que las configuraciones de disco de back-end proporcionen una velocidad de escritura un 10 % superior a la captura sostenida y la tasa de recopilación requeridas para la implementación.
- Para OVA, se requieren 32 GB de RAM por dispositivo de host.
- Cree directorios de Concentrator para las bases de datos de metadatos e índice en discos duros SSD/EFD.
- Si los componentes de la base de datos están separados de los componentes del sistema operativo (SO) instalado (es decir, en un sistema físico por separado), proporcione conectividad directa con:
  - Dos puertos SAN Fibre Channel de 8 Gb/s por host virtual,
    o
  - Conectividad de disco SAS de 6 GB/s.

Nota: 1.) Actualmente, NetWitness Suite no es compatible con el almacenamiento conectado en red (NAS) para las implementaciones virtuales.
2.) Decoder permite cualquier configuración de almacenamiento que pueda cumplir con el requisito de rendimiento sostenido. El vínculo Fibre Channel de 8 Gb/s estándar a una SAN no es suficiente para leer y escribir datos de paquetes a 10 Gb. Debe usar múltiples conexiones Fibre Channel cuando configura la conexión desde **Decoder 10G** a la SAN.

Requisitos del sistema recomendados para un host virtual

En la siguiente tabla se señalan los requisitos recomendados de vCPU, vRAM e IOPS de lectura y escritura para los hosts virtuales en función de los EPS o la tasa de captura para cada componente.

- La asignación del almacenamiento se explica en el paso 3 “Configurar las bases de datos para adaptarse a NetWitness Suite”.
- Las recomendaciones de vRAM y vCPU pueden variar según las tasas de captura, la configuración y el contenido habilitado.
- Las recomendaciones se probaron a tasas de recopilación de hasta 25,000 EPS para los registros y dos Gb/s para los paquetes, para no SSL.
- Las especificaciones de vCPU para todos los componentes que se enumeran en las siguientes tablas son
  CPU Intel Xeon a 2.59 GHz.
- Todos los puertos se prueban para SSL a 15,000 EPS para los registros y a 1.5 Gb/s para los paquetes.

Nota: Los valores recomendados anteriores podrían ser distintos para la instalación de 11.0.0.0 en el momento de instalar y probar las nuevas características y mejoras.

Escenario uno

Los requisitos que se muestran en estas tablas se calcularon en las siguientes condiciones.

- Todos los componentes estaban integrados.
- El flujo de registros incluía un Log Decoder, un Concentrator y un Archiver.
- El flujo de paquetes incluía un Packet Decoder y un Concentrator.
- La carga en segundo plano incluía informes diarios y por hora.
- Los gráficos estaban configurados.

Log Decoder

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
2,500	6 o 15.60 GHz	32 GB	50	75
5,000	8 o 20.79 GHz	32 GB	100	100
7,500	10 o 25.99 GHz	32 GB	150	150

Packet Decoder

Mb/s	CPU	Memoria	IOPS de lectura	IOPS de escritura
50	4 o 10.39 GHz	32 GB	50	150
100	4 o 10.39 GHz	32 GB	50	250
250	4 o 10.39 GHz	32 GB	50	350

Concentrator: Flujo de registros

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
2,500	4 o 10.39 GHz	32 GB	300	1,800
5,000	4 o 10.39 GHz	32 GB	400	2,350
7,500	6 o 15.59 GHz	32 GB	500	4,500

Concentrator: Flujo de paquetes

Mb/s	CPU	Memoria	IOPS de lectura	IOPS de escritura
50	4 o 10.39 GHz	32 GB	50	1,350
100	4 o 10.39 GHz	32 GB	100	1,700
250	4 o 10.39 GHz	32 GB	150	2,100

Archiver

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
2,500	4 o 10.39 GHz	32 GB	150	250
5,000	4 o 10.39 GHz	32 GB	150	250
7,500	6 o 15.59 GHz	32 GB	150	350

Escenario dos

Los requisitos que se muestran en estas tablas se calcularon en las siguientes condiciones.

- Todos los componentes estaban integrados.
- El flujo de registros incluía un Log Decoder, un Concentrator, un Warehouse Connector y un Archiver.
- El flujo de paquetes incluía un Packet Decoder, un Concentrator y un Warehouse Connector.
- Event Stream Analysis agregaba a 90,000 EPS desde tres Hybrid Concentrators.
- Incident Management recibía alertas de Reporting Engine y Event Stream Analysis.
- La carga en segundo plano incluía informes, gráficos, alertas, investigation e incident management.
- Las alertas estaban configuradas.

Log Decoder

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
10,000	16 o 41.58 GHz	50 GB	300	50
15,000	20 o 51.98 GHz	60 GB	550	100

Packet Decoder

Mb/s	CPU	Memoria	IOPS de lectura	IOPS de escritura
500	8 o 20.79 GHz	40 GB	150	200
1,000	12 o 31.18 GB	50 GB	200	400
1,500	16 o 41.58 GHz	75 GB	200	500

Concentrator: Flujo de registros

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
10,000	10 o 25.99 GHz	50 GB	1,550 + 50	6,500
15,000	12 o 31.18 GB	60 GB	1,200 + 400	7,600

Concentrator: Flujo de paquetes

Mb/s	CPU	Memoria	IOPS de lectura	IOPS de escritura
500	12 o 31.18 GB	50 GB	250	4,600
1,000	16 o 41.58 GHz	50 GB	550	5,500
1,500	24 o 62.38 GHz	75 GB	1,050	6,500

Warehouse Connector: Flujo de registros

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
10,000	8 o 20.79 GHz	30 GB	50	50
15,000	10 o 25.99 GHz	35 GB	50	50

Warehouse Connector: Flujo de paquetes

Mb/s	CPU	Memoria	IOPS de lectura	IOPS de escritura
500	6 o 15.59 GHz	32 GB	50	50
1,000	6 o 15.59 GHz	32 GB	50	50
1,500	8 o 20.79 GHz	40 GB	50	50

Archiver: Flujo de registros

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
10,000	12 o 31.18 GB	40 GB	1,300	700
15,000	14 o 36.38 GHz	45 GB	1,200	900

Event Stream Analysis (ESA) con Context Hub

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
90,000	32 u 83.16 GHz	94 GB	50	50

Servidor de NetWitness y componentes colocalizados

Servidor de NetWitness, Jetty, Broker, Incident Management y Reporting Engine se encuentran en la misma ubicación.

CPU	Memoria	IOPS de lectura	IOPS de escritura
12 o 31.18 GB	50 GB	100	350

Escenario tres

Los requisitos que se muestran en estas tablas se calcularon en las siguientes condiciones.

- Todos los componentes estaban integrados.
- El flujo de registros incluía un Log Decoder y un Concentrator.
- El flujo de paquetes incluía un Packet Decoder y el Concentrator.
- Event Stream Analysis agregaba a 90,000 EPS desde tres Hybrid Concentrators.
- Incident Management recibía alertas de Reporting Engine y Event Stream Analysis.
- La carga en segundo plano incluía informes diarios y por hora.
- Los gráficos estaban configurados.

Log Decoder

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
25,000	32 u 83.16 GHz	75 GB	250	150

Packet Decoder

Mb/s	CPU	Memoria	IOPS de lectura	IOPS de escritura
2,000	16 o 41.58 GHz	75 GB	50	650

Concentrator: Flujo de registros

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
25,000	16 o 41.58 GHz	75 GB	650	9,200

Concentrator: Flujo de paquetes

Mb/s	CPU	Memoria	IOPS de lectura	IOPS de escritura
2,000	24 o 62.38 GHz	75 GB	150	7,050

Log Collector (local y remoto)

El Remote Log Collector es un servicio Log Collector que se ejecuta en un host remoto y el Remote Collector se implementa de manera virtual.

EPS	CPU	Memoria	IOPS de lectura	IOPS de escritura
15,000	8 o 20.79 GHz	8 GB	50	50
30,000	8 o 20.79 GHz	15 GB	100	100

Reglas de dimensionamiento de los recopiladores de Windows existente

Consulte *Actualización e instalación de la recopilación de Windows existente de RSA NetWitness Suite* para conocer las reglas de dimensionamiento del Recopilador de Windows existente.

Instalar el host virtual de NetWitness Suite en un ambiente virtual

Realice los siguientes procedimientos de acuerdo con su secuencia numerada para instalar RSA NetWitness® Suite en un ambiente virtual.

Requisitos previos

Asegúrese de contar con:

- Un VMware ESX Server que cumpla los requisitos descritos en Descripción general de dispositivos virtuales. Las Versiones compatibles son 6.5, 6.0 y 5.5.
- vSphere 4.1 Client o vSphere 5.0 Client instalados para iniciar sesión en VMware ESX Server.
- Derechos de administrador para crear las máquinas virtuales en VMware ESX Server.

Paso 1. Implementar el host virtual

Complete los siguientes pasos para implementar el archivo OVA en vCenter Server o ESX Server mediante vSphere Client.

Requisitos previos

Asegúrese de contar con:

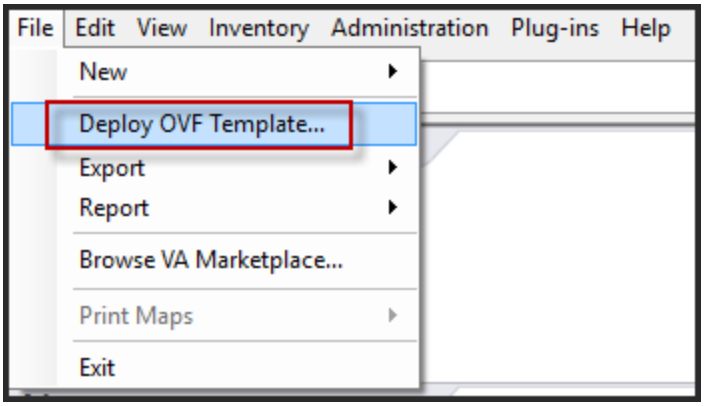
- Direcciones IP de red, máscara de red y direcciones IP de gateway para el host virtual.
- Nombres de red de todos los hosts virtuales, si está creando un clúster.
- Información de DNS o host.
- Contraseña para el acceso de los hosts virtuales. El nombre de usuario predeterminado es `root` y la contraseña predeterminada es `netwitness`.
- El archivo de paquete del host virtual de NetWitness Suite. (Este paquete se descarga desde Download Central [https://community.rsa.com]).

Procedimiento

Nota: En las siguientes instrucciones se ilustra un ejemplo de la implementación de un host OVA en el ambiente ESXi. Las pantallas que ve pueden ser diferentes a las de este ejemplo.

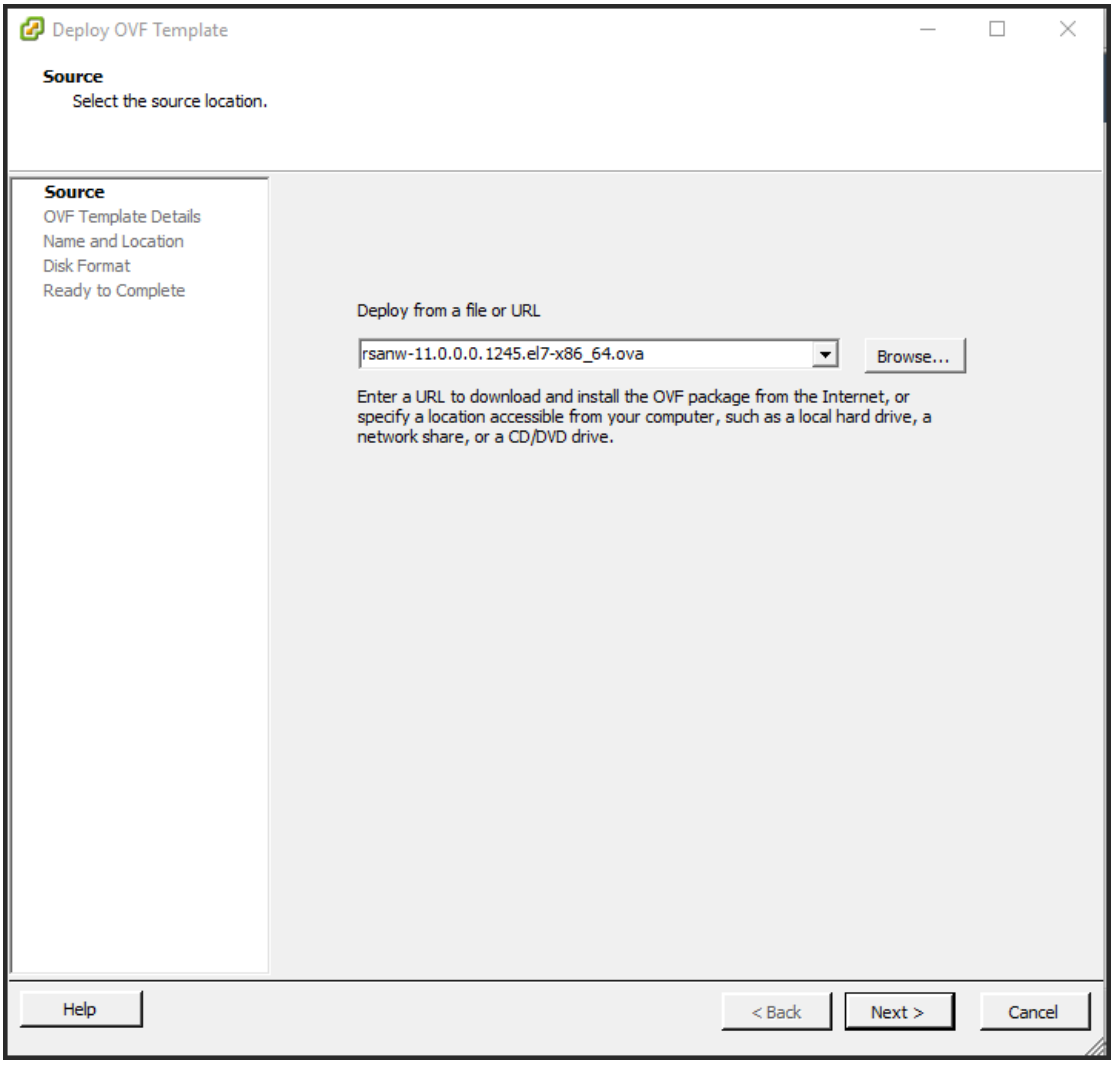
Para implementar el host OVA:

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

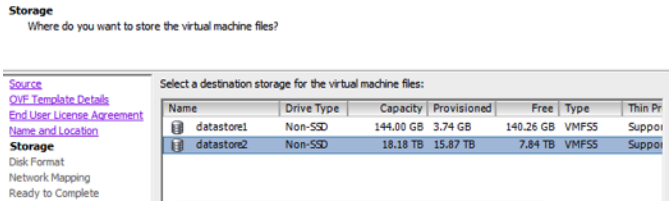


3. Aparecerá el cuadro de diálogo Implementar plantilla OVF. En el cuadro de diálogo **Implementar plantilla OVF**, seleccione el OVF del host que desea implementar en el ambiente virtual (por ejemplo, **V11.0 GOLD\OVFImge\v11_SA_OVF\nwreuax_**

OVF11.ovf) y haga clic en **Siguiente**.



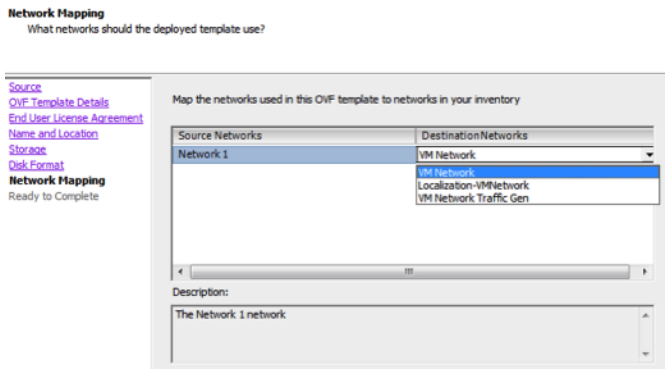
4. Aparece el cuadro de diálogo Nombre y Ubicación. El nombre designado no refleja el nombre de host del servidor. El nombre que aparece es útil como referencia del inventario desde dentro de ESXi.
5. Anote el nombre y haga clic en **Siguiente**.
   Aparecen las opciones de almacenamiento.



6. En las opciones de almacenamiento, designe la ubicación del almacén de datos para el host virtual.

Nota: Esta ubicación es exclusivamente para el sistema operativo (SO) del host. No se requiere que sea el mismo almacén de datos que se necesita cuando se instalan y configuran volúmenes adicionales para las bases de datos de NetWitness Suite en ciertos hosts (los cuales se analizan en las secciones siguientes).

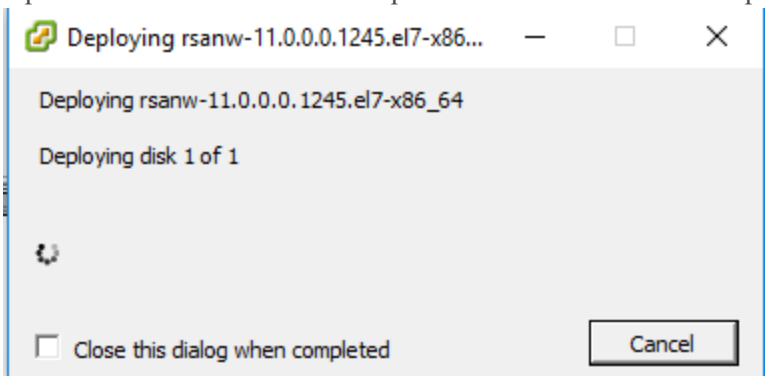
7. Haga clic en **Siguiente**.
   Aparece la opción Mapeo de red.



8. Deje los valores predeterminados y haga clic en **Siguiente**.

Nota: Si desea configurar Mapeo de red ahora, puede seleccionar opciones, pero RSA recomienda conservar los valores predeterminados y configurarlo después de configurar el OVA. El OVA se configura en el Paso 4: Configurar parámetros específicos del host.

Aparece una ventana de estado que muestra el estado de la implementación.



Después de finalizar el proceso, se presenta el nuevo OVA en el pool de recursos designado visible en ESXi desde vSphere. En este punto, el host virtual principal se instala, pero aún no se configura.

Paso 2. Configurar la red e instalar RSA NetWitness Suite

Realice los siguientes pasos para configurar la red del dispositivo virtual.

Requisitos previos

Asegúrese de contar con:

- Direcciones IP de red, máscara de red y direcciones IP de gateway para el host virtual.
- Nombres de red de todos los hosts virtuales, si está creando un clúster.
- Información de DNS o host.

Procedimiento

Ejecute los siguientes pasos para hacer que todos los hosts virtuales accedan a la red.

Revisar los puertos del firewall abiertos

Revise el tema ***Arquitectura y puertos de red*** de la ***Guía de implementación*** en la ayuda de NetWitness Suite, de modo que pueda configurar los servicios NetWitness Suite y los firewalls.

Precaución: No realice la instalación hasta que los puertos del firewall estén configurados.

Existen dos tareas principales que debe realizar en el orden en que se muestra para instalar NetWitness Suite 11.0.0.0

Tareas de instalación

Tarea 1: Instalar 11.0.0.0 en el Servidor de NetWitness (nodo 0)

Tarea 2: Instalar 11.0.0.0 en otros componentes de NetWitness Suite (nodo x)

Tarea 1: Instalar 11.0.0.0 en el Servidor de NetWitness (nodo 0)

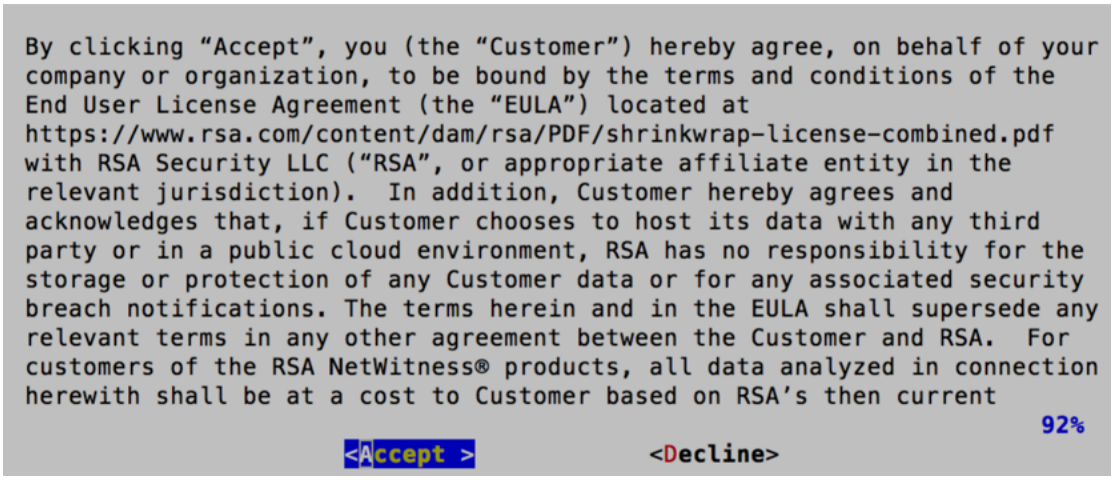
En el host que implementó para el servidor de NW (nodo 0), esta tarea instala:

- La plataforma ambiental del servidor de NW 11.0.0.0.
- Los componentes del servidor de NW (es decir, los servicios Admin, Config, Orchestration, Service Management y Security).
- Un repositorio con los archivos RPM requeridos para instalar los otros componentes o servicios funcionales.

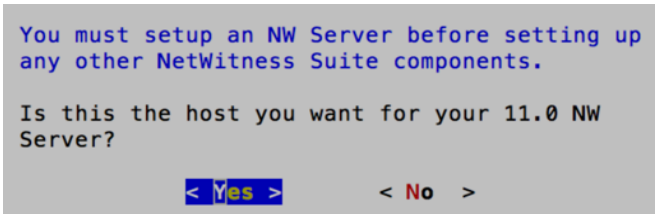
1. Implemente el ambiente 11.0.0.0:
   a. Aprovisione los hosts.
   b. Configure el almacenamiento.
   c. Configure los firewalls.

2. 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 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.
3.) Si especifica servidores DNS durante la ejecución del programa de instalación (`nwsetup-tui`), DEBEN ser válidos (válido en este contexto significa válido durante la configuración) y ser accesibles para que `nwsetup-tui` pueda continuar. Los servidores DNS configurados erróneamente hacen que la configuración falle. Si después de la configuración necesita acceder a un servidor DNS al que no se pudo acceder durante la configuración (por ejemplo, para reubicar un host después de la configuración que tenga un conjunto diferente de servidores DNS), consulte Tarea 1. Volver a configurar servidores DNS después de 11.0.0.0 en Tareas posteriores a la instalación.
Si no especifica servidores DNS durante `nwsetup-tui` , debe seleccionar **1 El repositorio local (en el servidor de NW)** en el indicador **Repositorio de actualizaciones** de **NetWitness Suite** en el paso 12 (los servidores DNS no están definidos, de modo que el sistema no puede acceder al repositorio externo).



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

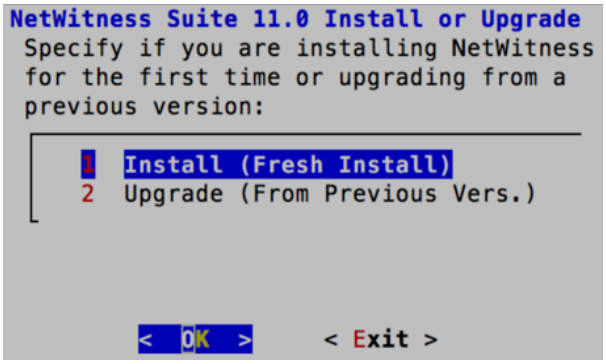


4. Use la tecla de tabulación para ir a **Sí** y presione Intro.

   Elija **No** si ya instaló 11.0.0.0 en el servidor de NW.

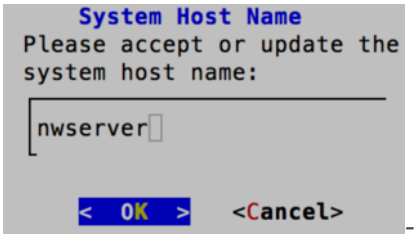
   Precaución: Si elige el host incorrecto para el servidor de NW y completa la configuración, debe iniciar el programa de instalación (paso 3) y completar todos los pasos subsiguientes para corregir este error.

   Se muestra el indicador Instalar o Actualizar.



5. Presione Intro (la opción Instalar está seleccionada de manera predeterminada).

   Se muestra el indicador “Nombre del host”.



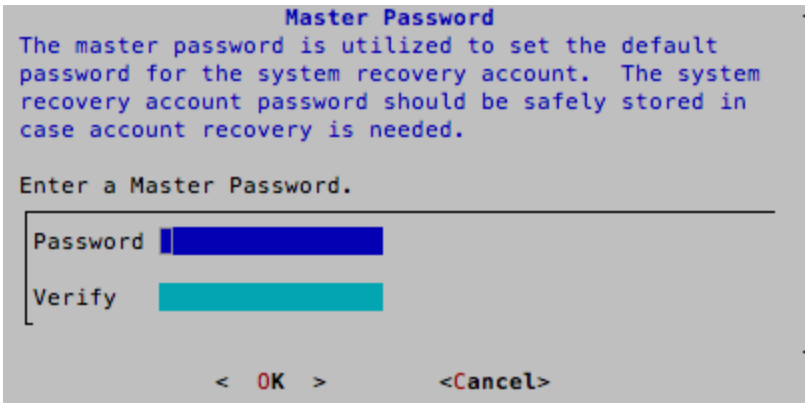
6. Presione Intro si desea mantener este nombre. Si no edita el nombre del host, use la tecla de tabulación para ir a **Aceptar** y presione Intro para cambiarlo.

   Se muestra el indicador “Contraseña maestra”.

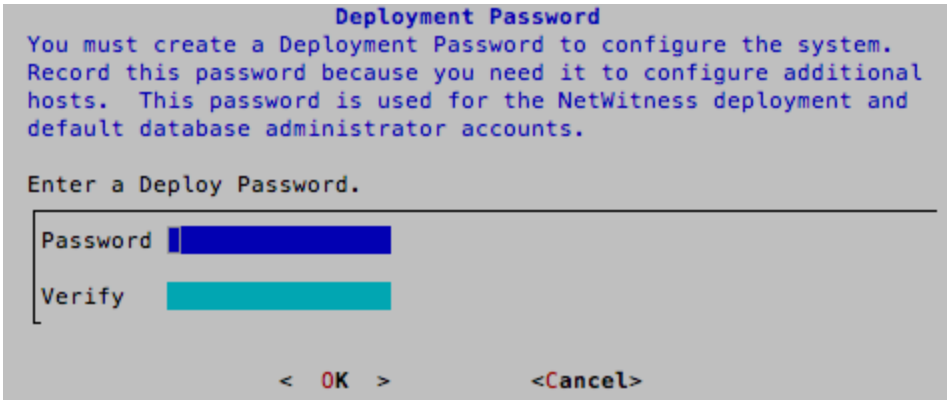
   Los caracteres de la siguiente lista son compatibles para Contraseña maestra y Contraseña de implementación:

   - 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 { } [ ] ( ) / \ ' " ` ~ , ; : . < > -).



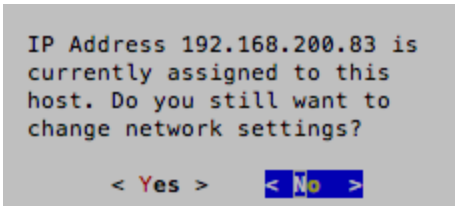
7. Use la flecha hacia abajo para desplazarse hasta **Contraseña** y escriba una contraseña, use la flecha hacia abajo para desplazarse hasta **Verificar** y vuelva a escribir la contraseña, use la tecla de tabulación para ir a **Aceptar** y presione Intro.
   Se muestra el indicador "Contraseña de implementación".



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

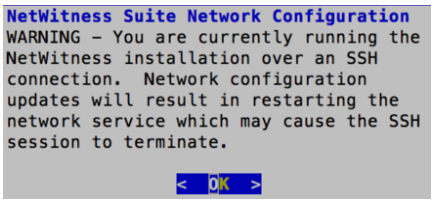
Indicadores condicionales:

- Si el programa de instalación encuentra una dirección IP válida para este host, se muestra el siguiente indicador.



  Presione Intro si desea usar esta dirección IP y evitar cambiar la configuración de red. Use la tecla de tabulación para ir a **Sí** y presione Intro si desea cambiar la configuración de IP que se encontró en el host.

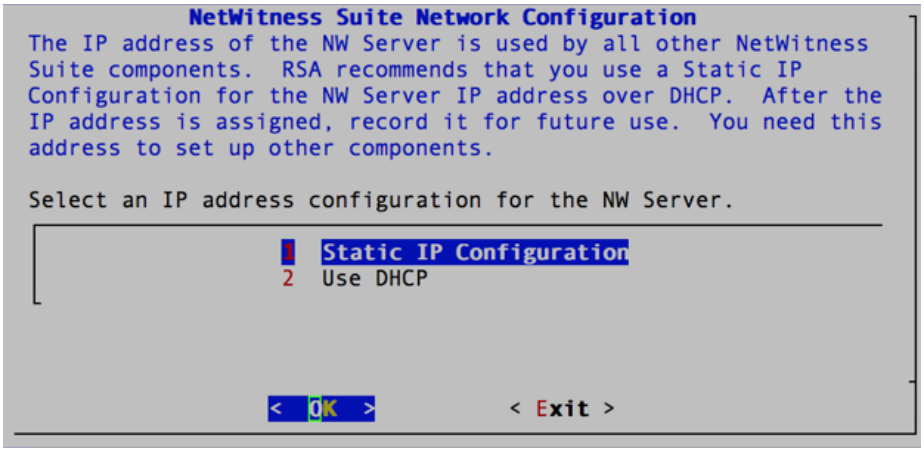
- Si está usando una conexión de protocolo SSH, se muestra la siguiente advertencia.



  Presione Intro para cerrar el indicador de advertencia.

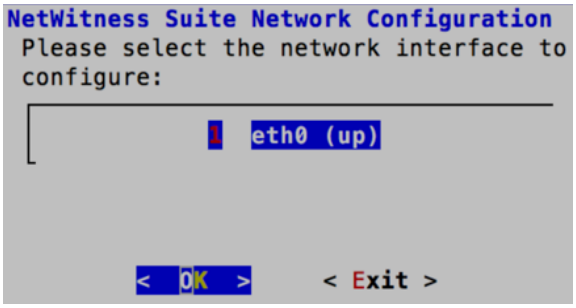
Si el programa de instalación encontró una configuración de IP y usted decidió usarla, se muestra el indicador Repositorio de actualizaciones. Vaya al paso 12 para completar la instalación.

Si no se encontró ninguna configuración de IP o si decidió cambiar la configuración de IP existente, se muestra el indicador Configuración de redes.



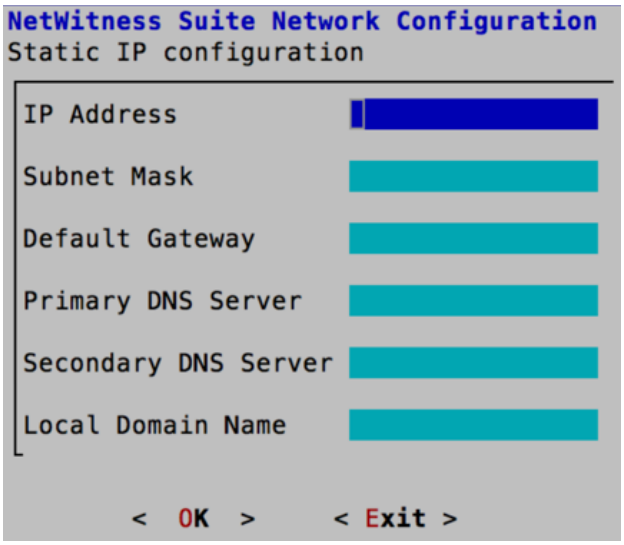
9. Use la tecla de tabulación para ir a **Aceptar** y presione Intro para usar **Dirección IP estática**.
   Si desea usar **DHCP**, use la flecha hacia abajo para desplazarse hasta 2 Usar DHCP y presione Intro.

Se muestra el indicador Configuración de redes.



10. Use la flecha hacia abajo para desplazarse hasta la interfaz de red que desea, use la tecla de tabulación para ir a **Aceptar** y presione Intro. Si no desea continuar, use la tecla de tabulación para ir a **Salir**

    Se muestra el indicador Configuración de IP estática.



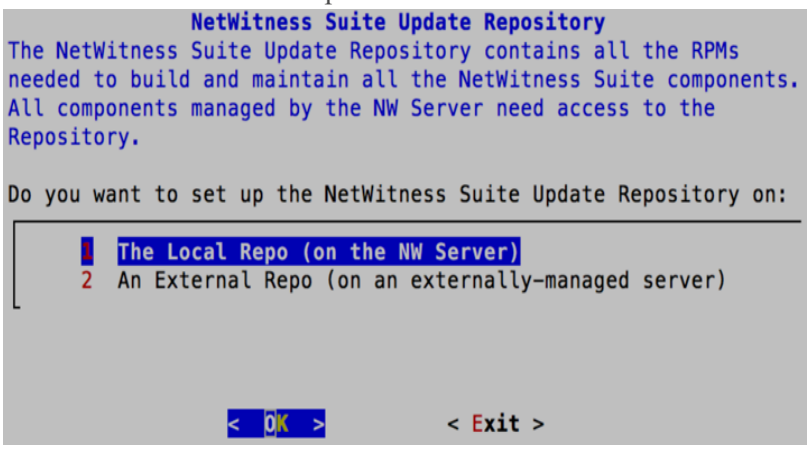
11. Escriba los valores de configuración (con la flecha hacia abajo para desplazarse de un campo a otro), use la tecla de tabulación para ir a **Aceptar** y presione Intro.

    Si no completa todos los campos obligatorios, se muestra un mensaje de error Todos los campos son obligatorios (los campos **Servidor DNS principal**, **Servidor DNS secundario** y **Nombre de dominio local** no son obligatorios).

    Si usa la sintaxis o la longitud de caracteres incorrectas para alguno de los campos, se muestra un mensaje de error *field-name* no válido.

    Precaución: Si selecciona un servidor DNS, asegúrese de que sea el servidor DNS correcto y que el host pueda acceder a él antes de continuar con la instalación.

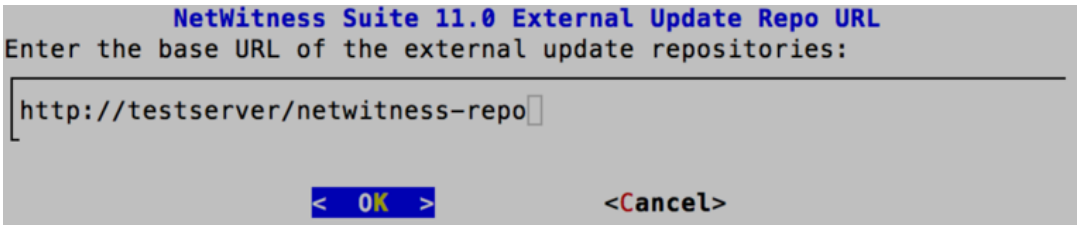
Se muestra el indicador Repositorio de actualizaciones.



12. Presione Intro para elegir **Repositorio local** en el servidor de NW.
    Si desea usar un repositorio externo, use la flecha hacia abajo para desplazarse hasta **Repositorio externo**, use la tecla de tabulación para ir a **Aceptar** y presione Intro.

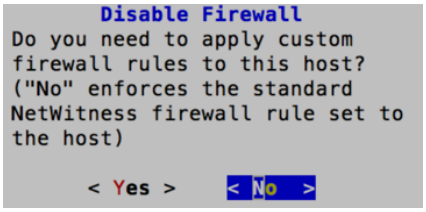
    - Si selecciona **1 El repositorio local (en el servidor de NW)**, el programa de instalación se asegura de que estén conectados los medios adecuados al host (es decir, una unidad de compilación o un DVD), desde los cuales puede recuperar la instalación o la actualización de los hosts a NetWitness Suite 11.0.0.0. Si el programa no puede encontrar los medios conectados, se muestra el siguiente indicador.

    - Si selecciona **2 Un repositorio externo (en un servidor administrado externamente)**, la interfaz del usuario le solicita que indique una dirección URL. Los repositorios otorgan acceso a las actualizaciones de RSA y a las actualizaciones de CentOS.



      Ingrese la dirección URL base del repositorio externo de NetWitness Suite y haga clic en **Aceptar.** Se muestra el indicador Iniciar instalación.

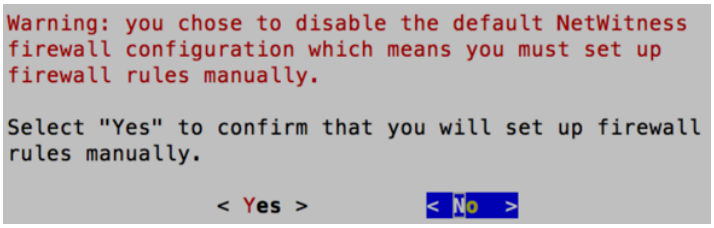
Se muestra el indicador Deshabilitar el firewall.



13. Para:

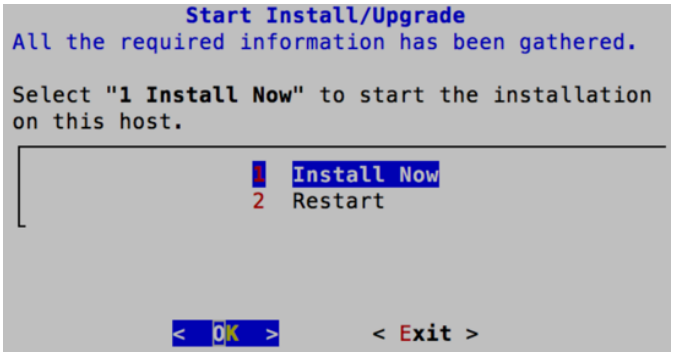
- Aplicar la configuración del firewall estándar, presione Intro.
- Deshabilitar la configuración estándar, use la tecla de tabulación para ir a **Sí** y presione Intro.

  Se muestra el indicador de confirmación de deshabilitación de la configuración del firewall.



Use la tecla de tabulación para ir a **Sí** y presione Intro para confirmar (presione Intro para usar la configuración del firewall estándar).

Se muestra el indicador Iniciar instalación.



14. Presione Intro para instalar 11.0.0.0 en el servidor de NW.

    Cuando se muestra “Instalación completa”, terminó de instalar el servidor de NW 11.0.0.0 en este host.

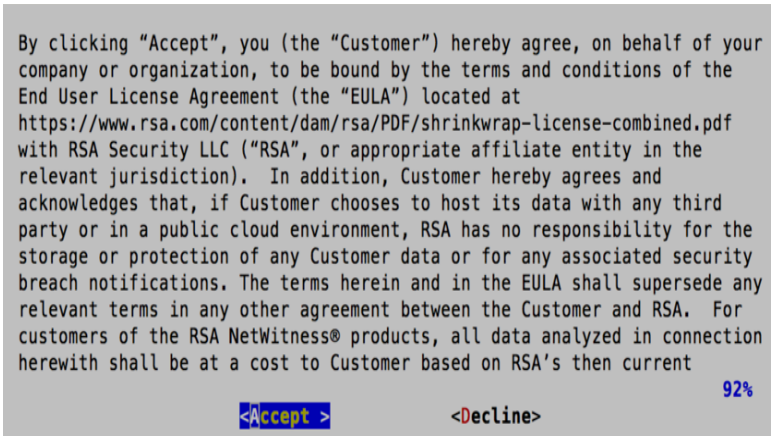
Tarea 2: Instalar 11.0 en otros componentes de NetWitness Suite (nodo x)

Para un host de servicio funcional (nodo x), esta tarea:

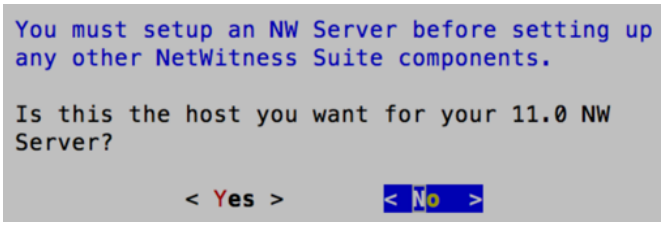
- Instala la plataforma ambiental 11.0.0.0.
- Aplica los archivos RPM al servicio desde el repositorio de actualizaciones del servidor de NW.

1. Conecte la unidad de compilación al host.
   Consulte “Unidad de compilación de RSA NetWitness® Suite” para obtener instrucciones sobre cómo crear una unidad de compilación.
2. Instale CentOS7 como el sistema operativo (SO) del host.
   Consulte el Apéndice A. Instalar CentOS7 en el host para obtener instrucciones.
3. Ejecute el comando `nwsetup-tui` para configurar el host.
   Esto inicia el programa de instalación y se muestra el EULA.

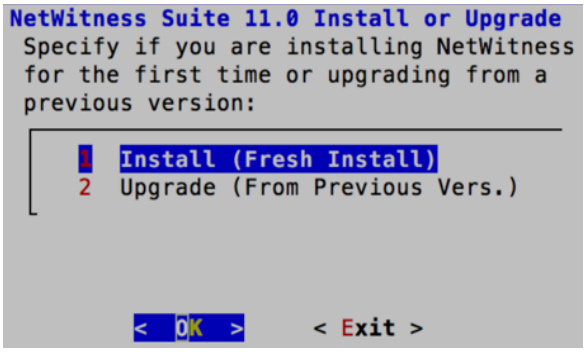
   Nota: Si especifica servidores DNS durante la ejecución del programa de instalación (`nwsetup-tui`), DEBEN ser válidos (válido en este contexto significa válido durante la configuración) y ser accesibles para que `nwsetup-tui` pueda continuar. Los servidores DNS configurados erróneamente hacen que la configuración falle. Si después de la configuración necesita acceder a un servidor DNS al que no se pudo acceder durante la configuración (por ejemplo, para reubicar un host después de la configuración que tenga un conjunto diferente de servidores DNS), consulte Volver a configurar servidores DNS después de 11.0.0.0.
   Si no especifica servidores DNS durante `nwsetup-tui` , debe seleccionar **1 El repositorio local (en el servidor de NW)** en el indicador **Repositorio de actualizaciones** de **NetWitness Suite** en el paso 12 (los servidores DNS no están definidos, de modo que el sistema no puede acceder al repositorio externo).



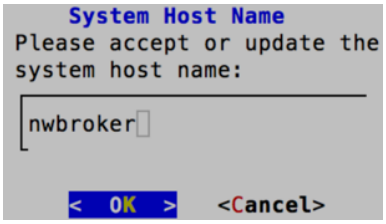
4. Use la tecla de tabulación para ir a **Aceptar** y presione Intro.
   Se muestra el indicador "Este es el servidor de NW".



5. Presione Intro (No).
   Se muestra el indicador Instalar o Actualizar.

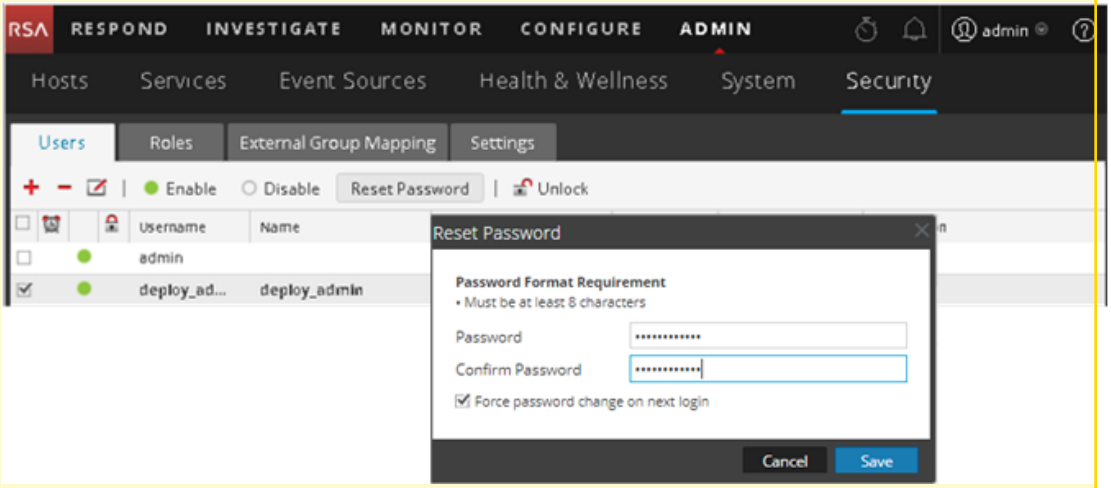


6. Presione Intro (la opción Instalar está seleccionada de manera predeterminada).
   Se muestra el indicador "Nombre del host".



7. Presione Intro si desea mantener este nombre. Si no edita el nombre del host, use la tecla de tabulación para ir a **Aceptar** y presione Intro para cambiarlo.

Precaución:
Escenario 1
Después de actualizar el servidor de NW a 11.0.0.0, si cambia la contraseña de usuario **deploy_admin** en la interfaz del usuario de NetWitness Suite (**ADMIN**>**Seguridad** >Seleccionar **deploy-admin - Restablecer contraseña**),

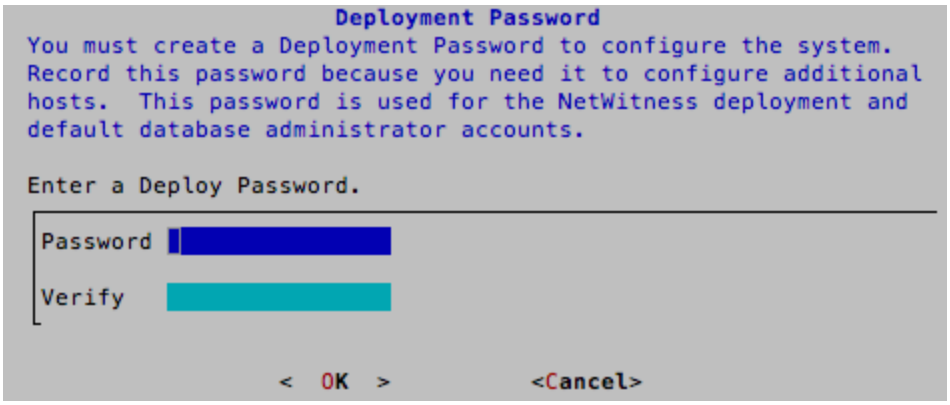


debe:
1. Acceder mediante el protocolo SSH al host del servidor de NW.
2. Ejecutar el script `(/opt/rsa/saTools/bin/set-deploy-admin-password`.
3. Usar la nueva contraseña en el momento de actualizar cualquier host nuevo que no es de servidor de NW.

Escenario 2
Después de actualizar el servidor de NW y actualizar cualquier número de versión de los hosts que no son de servidor de NW a 11.0.0.0, si cambia la contraseña de usuario **deploy_admin** en la interfaz del usuario de NetWitness Suite, debe:

1. Ejecutar el script `(/opt/rsa/saTools/bin/set-deploy-admin-password` en todos los hosts que no son de servidor de NW en su implementación.
2. Escribir la contraseña porque podría necesitarla para consultarla más adelante en la instalación.

Se muestra el indicador “Contraseña de implementación”.

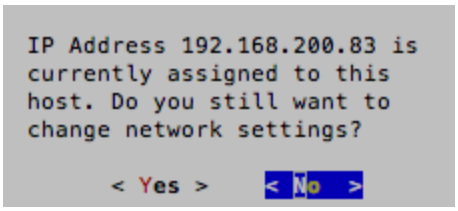


Nota: Debe usar la misma contraseña de implementación que usó cuando actualizó el servidor de NW.

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

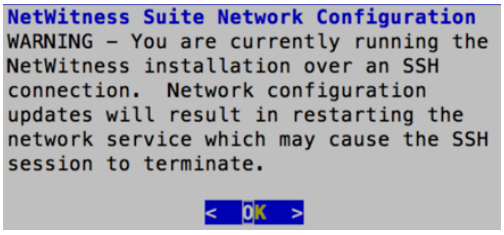
   Indicadores condicionales:

   - Si el programa de instalación encuentra una dirección IP válida para este host, se muestra el siguiente indicador.

     Presione Intro si desea usar esta dirección IP y evitar cambiar la configuración de red. Use la tecla de tabulación para ir a **Sí** y presione Intro si desea cambiar la configuración de IP que se encontró en el host.

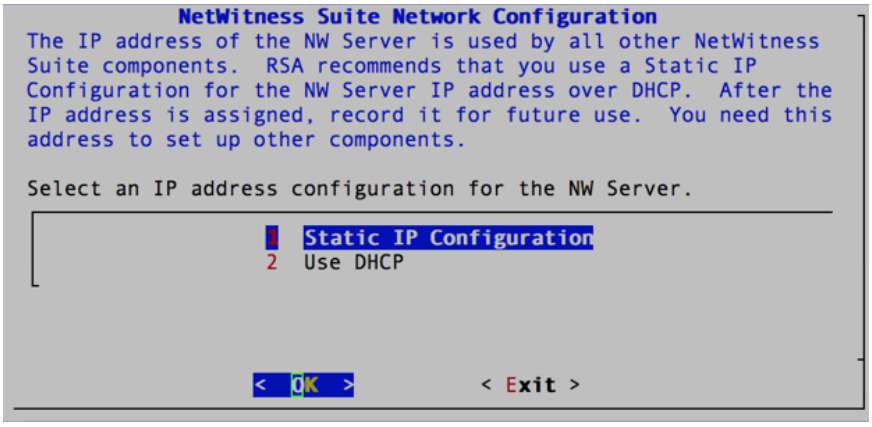
   - Si está usando una conexión de protocolo SSH, se muestra la siguiente advertencia.

     Presione Intro para cerrar el indicador de advertencia.

   Si el programa de instalación encontró una configuración de IP y usted decidió usarla, se muestra el indicador Repositorio de actualizaciones. Vaya al paso 11 para completar la instalación.

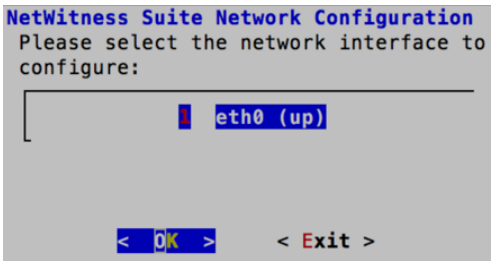
Si no se encontró ninguna configuración de IP o si decidió cambiar la configuración de IP existente, se muestra el indicador Configuración de redes.



9. Use la tecla de tabulación para ir a Aceptar y presione Intro para usar **Dirección IP estática**.

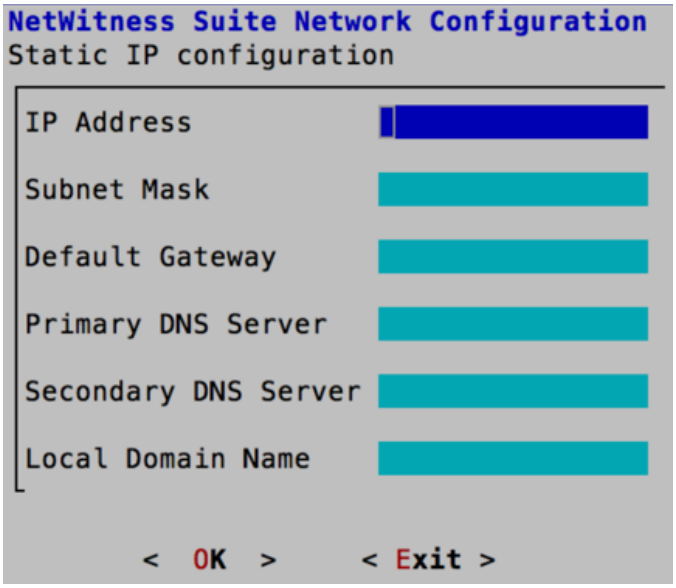
   Si desea usar **DHCP**, use la flecha hacia abajo para desplazarse hasta 2 Usar DHCP y presione Intro.

   Se muestra el indicador Configuración de redes.



10. Use la flecha hacia abajo para desplazarse hasta la interfaz de red que desea, use la tecla de tabulación para ir a **Aceptar** y presione Intro. Si no desea continuar, use la tecla de tabulación para ir a **Salir**

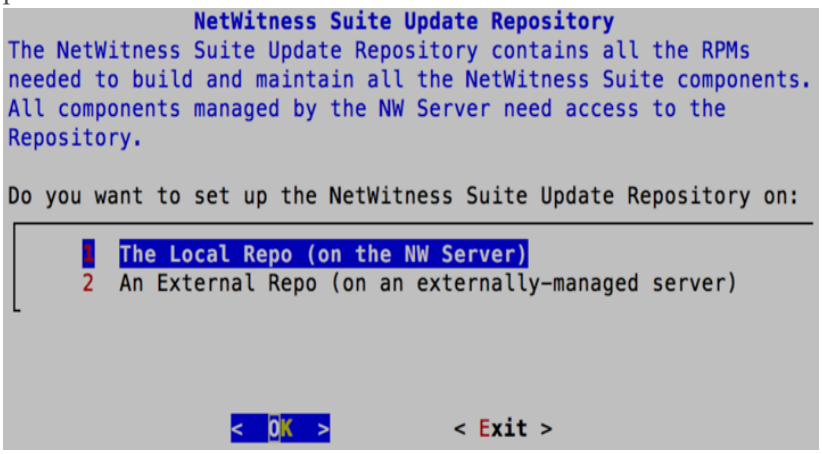
Se muestra el indicador Configuración de IP estática.



11. Escriba los valores de configuración (con la flecha hacia abajo para desplazarse de un campo a otro), use la tecla de tabulación para ir a **Aceptar** y presione Intro.
Si no completa todos los campos obligatorios, se muestra un mensaje de error Todos los campos son obligatorios (los campos Servidor DNS principal, Servidor DNS secundario y Nombre de dominio local no son obligatorios).
Si usa la sintaxis o la longitud de caracteres incorrectas para alguno de los campos, se muestra un mensaje de error *field-name* no válido.

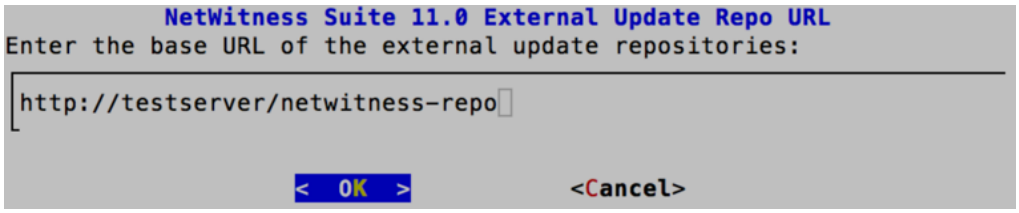
Precaución: Si selecciona un servidor DNS, asegúrese de que sea el servidor DNS correcto y que el host pueda acceder a él antes de continuar con la instalación.

Se muestra el indicador Repositorio de actualizaciones.
Seleccione el mismo repositorio que seleccionó cuando actualizó el host del servidor de NW para todos los hosts.

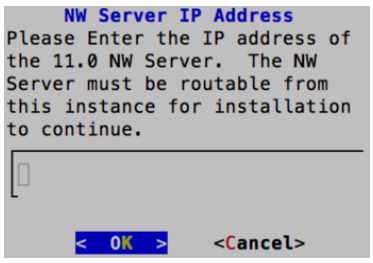


12. Presione Intro para elegir **Repositorio local** en el servidor de NW.
    Si desea usar un repositorio externo, use la flecha hacia abajo para desplazarse hasta **Repositorio externo**, use la tecla de tabulación para ir a **Aceptar** y presione Intro.

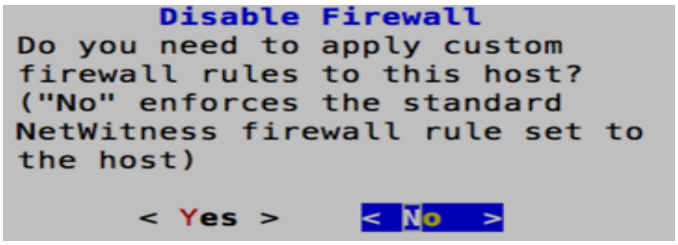
    - Si selecciona **1 El repositorio local (en el servidor de NW)**, el programa de instalación se asegura de que estén conectados los medios adecuados al host (es decir, una unidad de compilación o un DVD), desde los cuales puede recuperar la instalación o la actualización de los hosts a NetWitness Suite 11.0.0.0.
    - Si selecciona **2 Un repositorio externo (en un servidor administrado externamente)**, la interfaz del usuario le solicita que indique una dirección URL. Los repositorios otorgan acceso a las actualizaciones de RSA y a las actualizaciones de CentOS.

      Ingrese la dirección URL base del repositorio externo de NetWitness Suite y haga clic en **Aceptar.**
      Se muestra el indicador Dirección IP del servidor de NW.

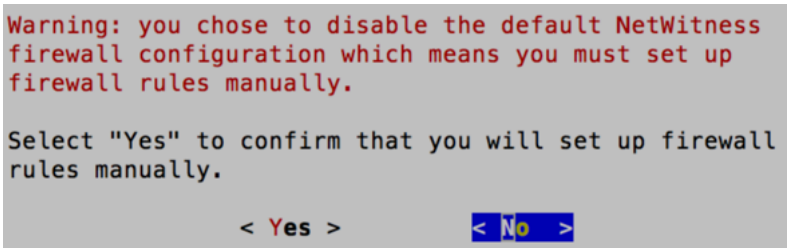
13. Escriba la dirección IP del servidor de NW. Use la tecla de tabulación para ir a **Aceptar** y presione Intro.
    Se muestra el indicador Deshabilitar el firewall.

14. Para:

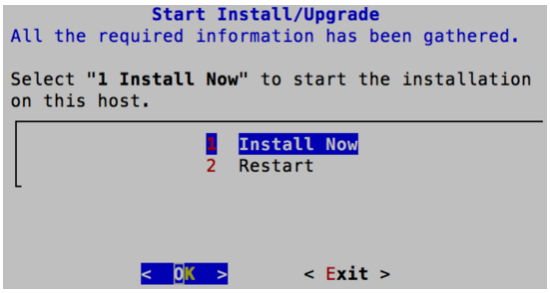
    - Aplicar la configuración del firewall estándar, presione Intro.
    - Deshabilitar la configuración estándar, use la tecla de tabulación para ir a **Sí** y presione Intro.

      Se muestra el indicador de confirmación de deshabilitación de la configuración del firewall.

      Use la tecla de tabulación para ir a **Sí** y presione Intro para confirmar (presione Intro para usar la configuración del firewall estándar).

    Se muestra el indicador Iniciar instalación.

15. Presione Intro para instalar 11.0.0.0 en el servidor de NW.

    Cuando se muestra “Instalación completa”, tiene un host genérico (nodo x) con un sistema operativo compatible con NetWitness Suite 11.0.0.0.

16. Instale un servicio de componentes en el host de nodo x.

    a. Haga clic en **ADMIN** > **Hosts**.

       El cuadro de diálogo **Nuevos hosts** se muestra con la vista **Hosts** atenuada en segundo plano.

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

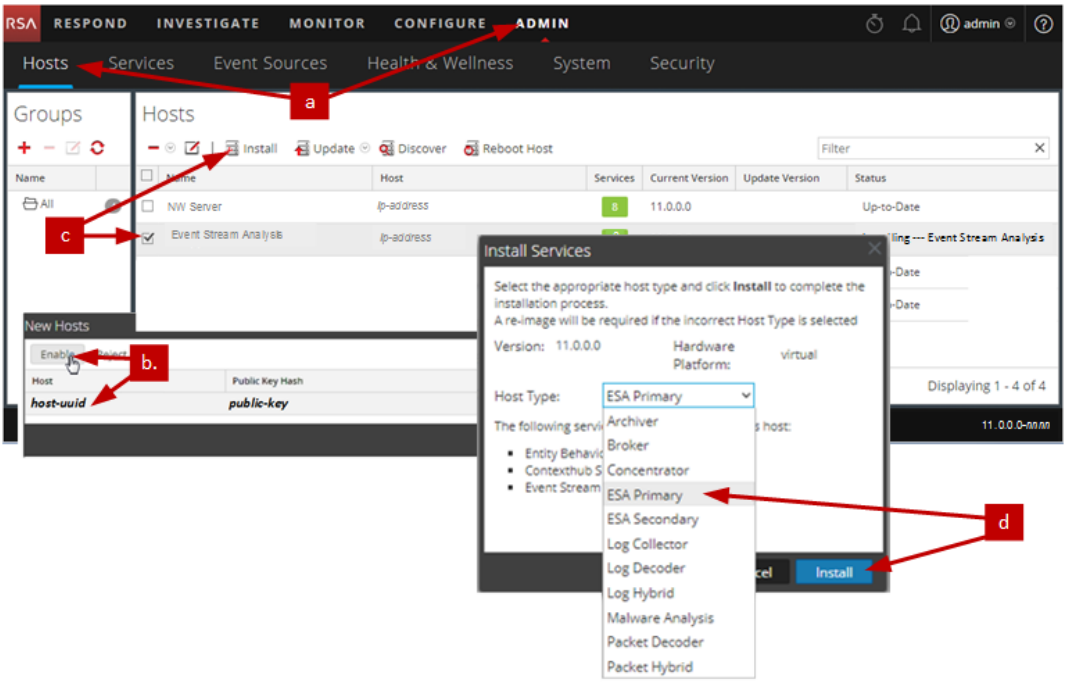
    b. Seleccione un host que no es de servidor de NW en la vista **Hosts**.

    c. 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**.

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

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



Se completó la instalación del host que no es de servidor de NW en NetWitness Suite.

17. Complete los pasos del 1 al 15 para el resto de los componentes que no son de servidor de NW de NetWitness Suite.

Paso 3. Configurar las bases de datos para adaptarse a NetWitness Suite

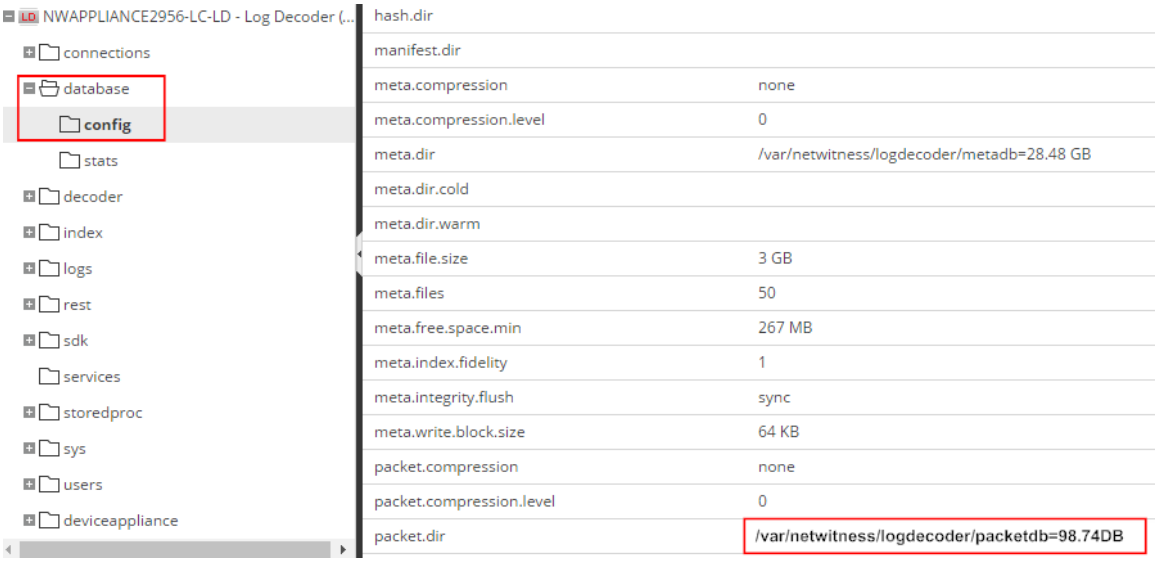
Cuando implementa bases de datos desde OVA, es posible que la asignación inicial de espacio de la base de datos no sea suficiente para admitir Servidor de NetWitness. Debe revisar el estado de los almacenes de datos después de la implementación inicial y expandirlos.

Tarea 1. Revisar la configuración inicial del almacén de datos

Revise la configuración del almacén de datos después de la implementación inicial con el fin de determinar si el espacio en las unidades es suficiente para adaptarse a las necesidades de su empresa. Por ejemplo, en este tema se revisa la configuración del almacén de datos de PacketDB en el host de Log Decoder después de que se implementa por primera vez desde un archivo de virtualización abierta (OVA).

Espacio inicial asignado a PacketDB

El espacio asignado para PacketDB es muy pequeño (alrededor de 98 GB). En el siguiente ejemplo de la vista Explorar de NetWitness Suite se muestra el tamaño de PacketDB después de su implementación inicial desde un OVA.



Tamaño inicial de la base de datos

De forma predeterminada, el tamaño de la base de datos se establece en un 95 % del tamaño del sistema de archivos en el cual reside. Acceda al host de Log Decoder mediante el protocolo SSH e ingrese la cadena de comandos `df -k` para ver el sistema de archivos y su tamaño. La siguiente salida es un ejemplo de la información que devuelve esta cadena de comandos.

```
[root@nwappliance32431 ~]# df -k
Filesystem                          1K-blocks     Used Available Use% Mounted on
/dev/mapper/netwitness_vg00-root     31441920 3148972  28292948  11% /
devtmpfs                             16462812       0  16462812   0% /dev
tmpfs                                16474132      12  16474120   1% /dev/shm
tmpfs                                16474132   41492  16432640   1% /run
tmpfs                                16474132       0  16474132   0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome  10475520   32984  10442536   1% /home
/dev/mapper/netwitness_vg00-varlog   10475520   72868  10402652   1% /var/log
/dev/mapper/netwitness_vg00-nwhome  146950036  399908 146550128   1% /var/netwitness
/dev/sda1                             1038336   88448    949888   9% /boot
tmpfs                                 3294828       0   3294828   0% /run/user/0
```

Punto de montaje de PacketDB

La base de datos se monta en el volumen lógico `packetdb` del grupo de volúmenes `netwitness_vg00`. `netwitness_vg00` y esto es donde se inicia su planificación de expansión para el sistema de archivos.

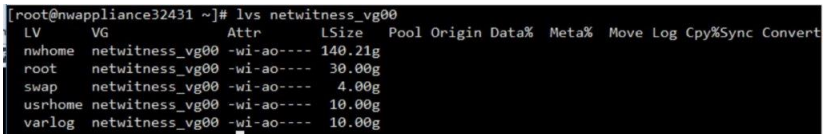
Estado inicial de netwitness_vg00

Complete los siguientes pasos para revisar el estado de `netwitness_vg00`.

1. Acceda al host de Log Decoder mediante el protocolo SSH.
2. Ingrese la cadena de comandos `lvs` (mostrar volúmenes lógicos) para determinar los volúmenes lógicos que están agrupados en `netwitness_vg00`.

   `[root@nwappliance32431 ~}# lvs netwitness_vg00.`

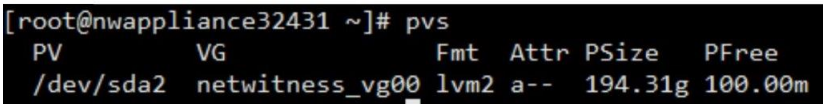
   La siguiente salida es un ejemplo de la información que devuelve esta cadena de comandos.



3. Ingrese la cadena de comandos pvs (mostrar volúmenes físicos) para determinar los volúmenes físicos que pertenecen a un grupo específico.

   `[root@nwappliance32431 ~}# pvs`

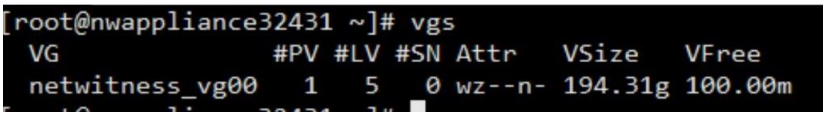
   La siguiente salida es un ejemplo de la información que devuelve esta cadena de comandos.



4. Ingrese la cadena de comandos `vgs` (mostrar grupos de volúmenes) para mostrar el tamaño total del grupo de volúmenes específico.

   `[root@nwappliance32431 ~}# vgs`

   La siguiente salida es un ejemplo de la información que devuelve esta cadena de comandos.



Tarea 2. Revisar la configuración óptima del espacio del almacén de datos

Debe revisar las opciones de configuración del espacio del almacén de datos para los diferentes hosts con el fin de obtener el rendimiento óptimo de la implementación virtual de NetWitness Suite. Las áreas de almacenamiento de datos se requieren para la configuración de los hosts virtuales y el tamaño correcto depende del host.

Nota: (1.) Consulte el tema "**Técnicas de optimización**" de la Guía de ajuste de la base de datos de RSA NetWitness SuiteCore para obtener recomendaciones sobre cómo optimizar el espacio del almacén de datos. (2.) Póngase en contacto con Atención al cliente con el fin de obtener ayuda para configurar sus unidades virtuales y utilizar Sizing & Scoping Calculator.

Tasas de espacio de unidad virtual

En la siguiente tabla se proporcionan configuraciones óptimas para hosts de paquetes y registros. Se proporcionan ejemplos de particionamiento y dimensionamiento para la captura de paquetes y ambientes de recopilación de registros al final de este tema.

Decoder			
Almacenes de datos persistentes	Almacén de datos de la caché		
PacketDB	SessionDB	MetaDB	Índice
100 % según el cálculo de Sizing & Scoping Calculator	6 GB por 100 Mb/s de tráfico sostenido proporcionan 4 horas de caché	60 GB por 100 Mb/s de tráfico sostenido proporcionan 4 horas de caché	3 GB por 100 Mb/s de tráfico sostenido proporcionan 4 horas de caché

Concentrator		
Almacenes de datos persistentes	Almacenes de datos de la caché	
MetaDB	SessionDB Índice	Índice
Se calcula como el 10 % de la PacketDB requerida para una tasa de retención de 1:1	30 GB por 1 TB de PacketDB para implementaciones de red multiprotocolo estándar como se ven en gateways de Internet típicas.	5 % de la MetaDB calculada en Concentrator. Disco SSD o ejes de alta velocidad recomendados para acceso rápido

Log Decoder			
Almacenes de datos persistentes	Almacenes de datos de la caché		
PacketDB	SessionDB	MetaDB	Índice
100 % según el cálculo de Sizing & Scoping Calculator	1 GB por 1,000 EPS de tráfico sostenido proporcionan ocho horas de caché	20 GB por 1,000 EPS de tráfico sostenido proporcionan ocho horas de caché	0.5 GB por 1,000 EPS de tráfico sostenido proporciona 4 horas de caché

Log Concentrator		
Almacenes de datos persistentes	**Almacenes de datos de la caché**	
MetaDB	**SessionDB** **Índice**	**Índice**
Se calcula como el 100 % de la PacketDB requerida para una tasa de retención de 1:1	3 GB por 1,000 EPS de tráfico sostenido por día de retención	5 % de la MetaDB calculada en Concentrator. Disco SSD o ejes de alta velocidad recomendados para acceso rápido

Tarea 3. Agregar un volumen nuevo y extender los sistemas de archivos existentes

Después de revisar la configuración inicial del almacén de datos, puede determinar que debe agregar un volumen nuevo. En este tema se utiliza un host virtual de Packet/Log Decoder como ejemplo.

Realice estas tareas en el siguiente orden.

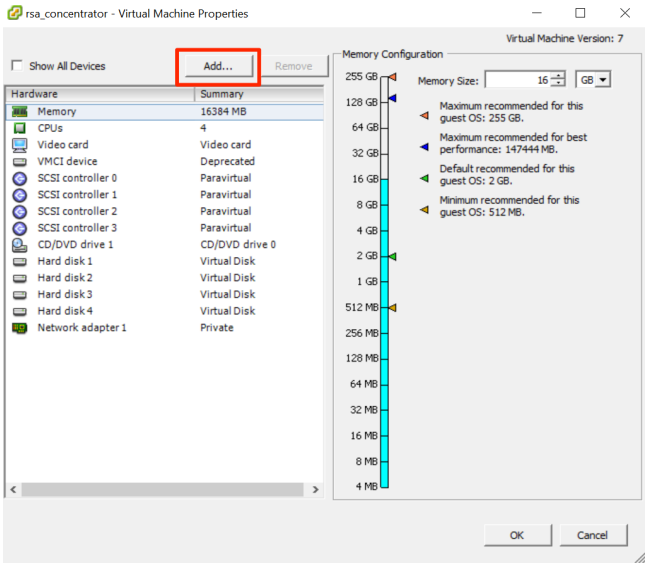
1. Agregar un disco nuevo
2. Crear volúmenes nuevos en el disco nuevo
3. Crear un volumen físico de LVM en la partición nueva
4. Extender el grupo de volúmenes con el volumen físico
5. Expandir el sistema de archivos
6. Iniciar los servicios
7. Asegurarse de que los servicios estén en ejecución
8. Volver a configurar los parámetros de Log Decoder

Agregar un disco nuevo

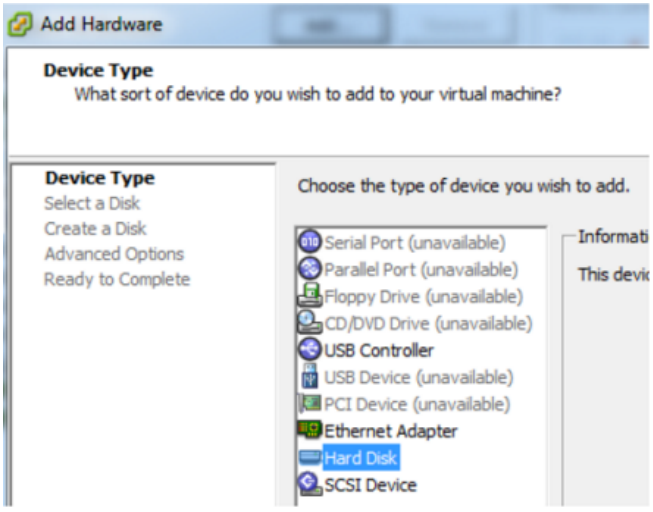
En este procedimiento se muestra cómo agregar un disco de 100 GB nuevo en el mismo almacén de datos.

Nota: El procedimiento para agregar un disco en otro almacén de datos es similar al procedimiento que se muestra aquí.

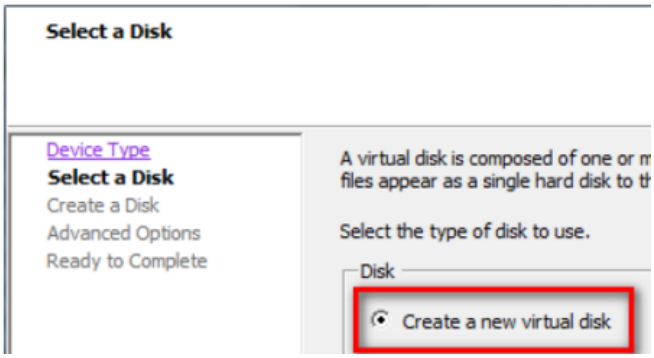
1. Apague la máquina, edite las **Propiedades de máquinas virtuales**, haga clic en la pestaña **Hardware** y, a continuación, en **Agregar**.



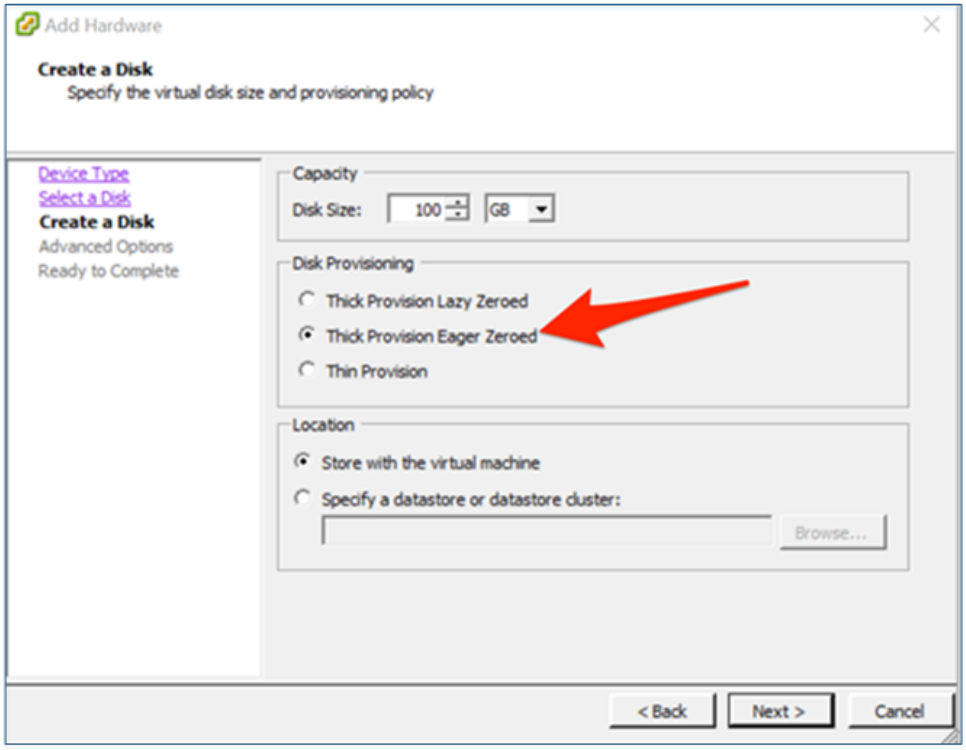
2. Seleccione **Disco duro** como el tipo de dispositivo.



3. Seleccione **Crear un nuevo disco virtual**.

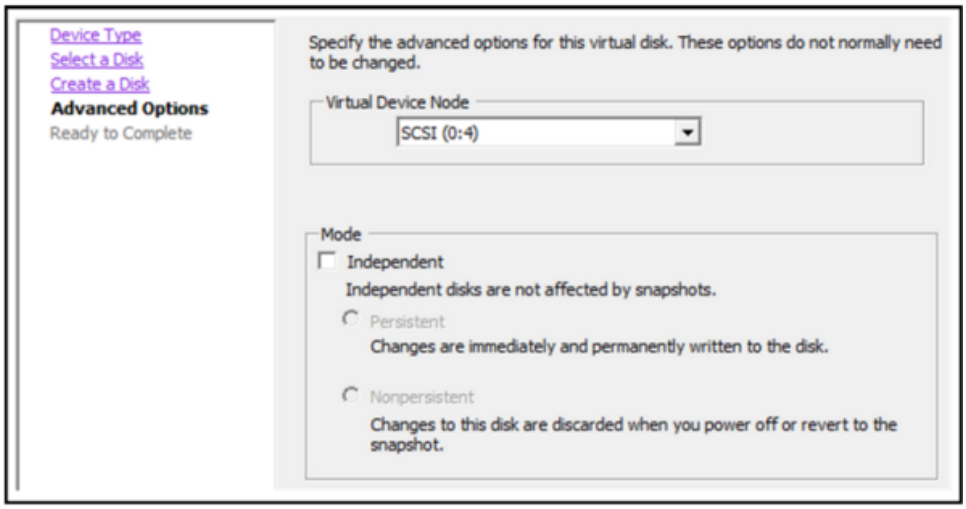


4. Seleccione el tamaño del disco nuevo y dónde desea crearlo (en el mismo almacén de datos o en otro).



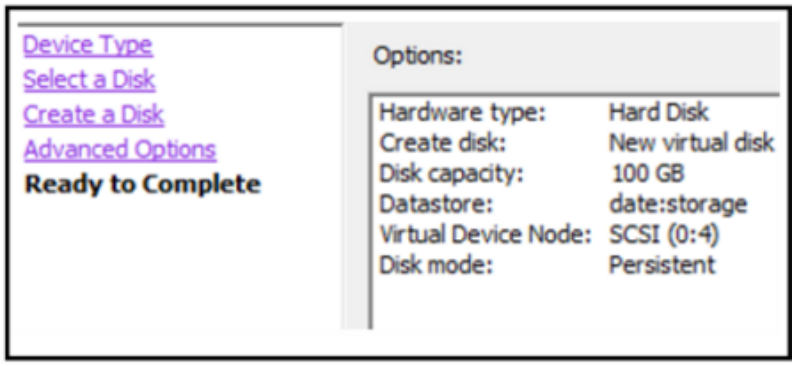
Precaución: Por motivos de rendimiento, asigne todo el espacio.

5. Apruebe el nodo del dispositivo virtual propuesto.



Nota: El nodo del dispositivo virtual puede variar, pero es pertinente a los mapeos de `/dev/sdX`.

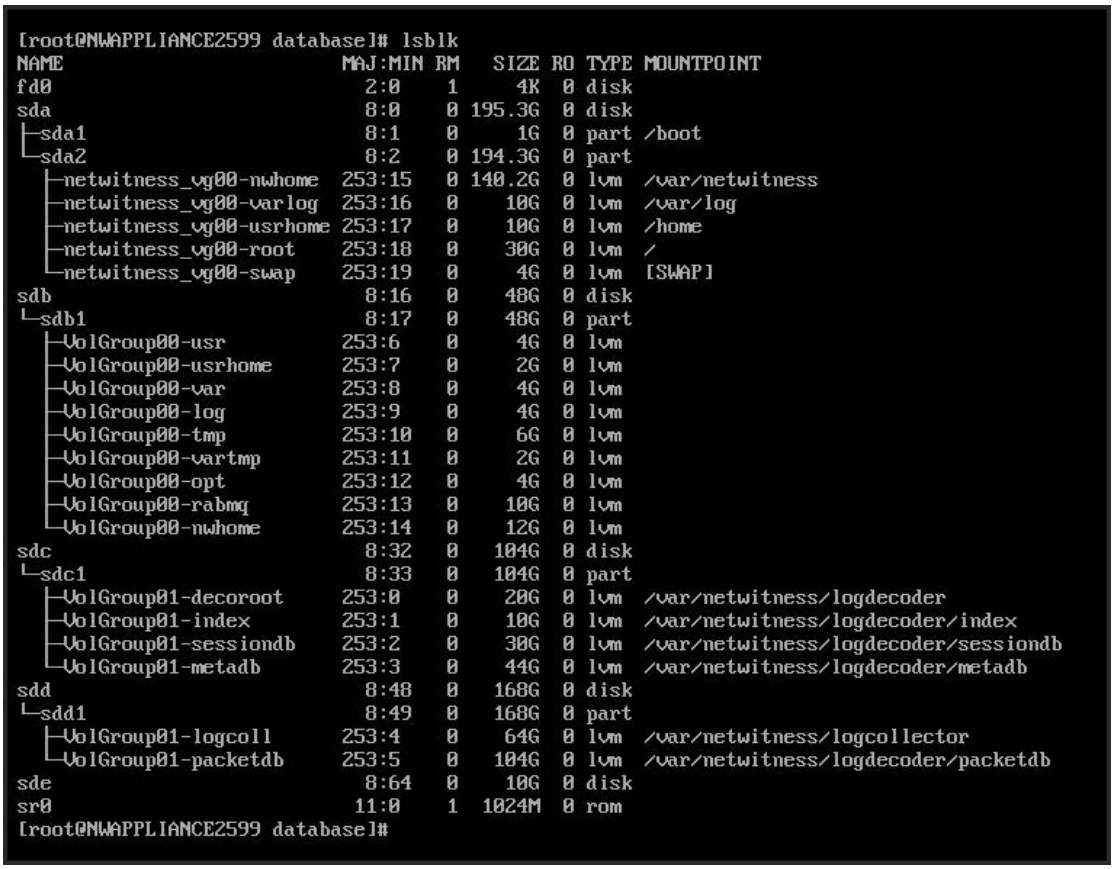
6. Confirme los ajustes.



7. Inicie la máquina virtual.
8. Acceda a la máquina mediante el protocolo SSH.
9. Reinicie la máquina y escriba el siguiente comando.

   ```
   lsblk
   ```

   Se muestra la siguiente salida, en la cual se presenta el disco nuevo.



Nota: 1.) Recibirá un error de **tabla de partición desconocida** debido a que el disco nuevo no se ha inicializado. 2.) El valor **sd 2:0:4:0** tiene relación con el nodo del dispositivo virtual **SCSI:0:4** que apareció cuando agregó el dispositivo nuevo. 3.) Es dispositivo de disco nuevo es **sde** (o `/dev/sde`).

10. Para detener el servicio, escriba el siguiente comando.

    `root@LogDecoderGM ~] # service nwlogcollector stop; service nwlogdecoder stop`.

    Este procedimiento utiliza el Log Decoder como ejemplo.

    Si desea detener los servicios en un Concentrator, debe escribir:

    `service nwconcentrator stop`

    Si desea detener los servicios en un Packet Decoder, debe escribir:

    `service nwdecoder stop`

Crear volúmenes en el disco nuevo

1. Acceda al host de Log Decoder mediante el protocolo SSH.
2. Cree una partición en el nuevo disco y cambie su tipo a LVM de Linux.

```
[root@NWAPPLIANCE2599 ~]# fdisk /dev/sde
```

Se muestra la información y el indicador siguientes.

```
[root@NWAPPLIANCE2599 database]# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x7cab96b5.

Command (m for help): _
```

3. Escriba `p`.

   Se muestra la siguiente información.

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System

Command (m for help):
```

   El tipo de partición predeterminado es **Linux (83)**. Debe cambiarlo a **LVM (8e)** de Linux.

4. Escriba `n`.

   Se muestra el siguiente indicador.

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set

Command (m for help): _
```

Se configura Partición 1 de tipo Linux y de tamaño de 10 GB

1. En el indicador `Command m for help:`, escriba `t`.

   Se muestra la información y el indicador siguientes.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help):
```

2. Escriba `8e`.

   Se muestra la información y el indicador siguientes.

```
Changed system type of partition 1 to 8e (Linux LVM).

Command (m for help):
```

3. Escriba `p`.

   Se muestra la siguiente información.

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1            2048    20971519    10484736   8e  Linux LVM

Command (m for help):
```

4. En el indicador `Command (m for help):`, escriba `w`.

   La tabla de partición nueva se escribe en el disco y fdisk sale al shell de raíz.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
[ 9838.504920]  sde: sde1
Syncing disks.
[root@NWAPPLIANCE2599 database]# _
```

   La partición `/dev/sde1` nueva se crea en el disco nuevo.

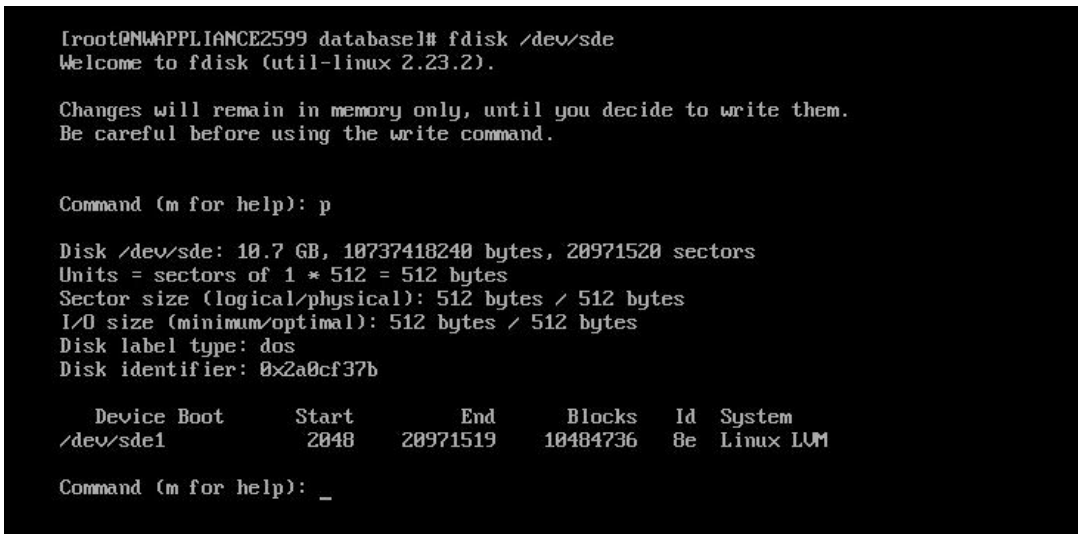
5. Realice uno de los siguientes pasos para verificar que la partición nueva exista.

- Escriba `dmesg | tail`.

  Se muestra la siguiente información.

- Escriba `fdisk /dev/sde`.
- Escriba `p`.

  Se muestra la siguiente información.



Crear un volumen físico de LVM en la partición nueva

1. Acceda al host de Log Decoder mediante el protocolo SSH.
2. Ingrese la siguiente cadena de comandos para crear un volumen físico del Administrador de volúmenes lógicos (LVM) en la partición nueva.

   ```
   [root@LogDecoderGM ~]# pvcreate /dev/sdel
   ```

3. Se muestra la siguiente información.

```
[root@NWAPPLIANCE2599 database]# pvcreate /dev/sde1
  Physical volume "/dev/sde1" successfully created.
[root@NWAPPLIANCE2599 database]#
```

Extender el grupo de volúmenes con el volumen físico

1. Acceda al host de Log Decoder mediante el protocolo SSH.
2. Ingrese la siguiente cadena de comandos para crear un volumen físico del Administrador de volúmenes lógicos (LVM) en la partición nueva.

   ```
   [root@LogDecoderGM ~]# pvs
   ```

   Se muestra la siguiente información.

```
[root@NWAPPLIANCE2599 database]# pvs
  PV         VG              Fmt  Attr PSize   PFree
  /dev/sda2  netwitness_vg00 lvm2 a--  194.31g 100.00m
  /dev/sdb1  VolGroup00      lvm2 a--   48.00g      0
  /dev/sdc1  VolGroup01      lvm2 a--  104.00g      0
  /dev/sdd1  VolGroup01      lvm2 a--  168.00g      0
  /dev/sde1                  lvm2 ---   10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

   `netwitness_vg00` consta de los volúmenes físicos (PV) `/dev/sdc1`y `/dev/sdd1` y del sistema LVM. Tenga en cuenta que el volumen`/dev/sde1` nuevo tiene 10 GB de espacio libre.

3. Para agregar el volumen físico a `netwitness_vg00`.
   a. Ingrese `vgextend netwitness_vg00 /dev/sde1`.

      Se muestra la siguiente información.

      ```
      Volume group "netwitness_vg00" successfully extended
      ```

   b. Ingrese pvs.

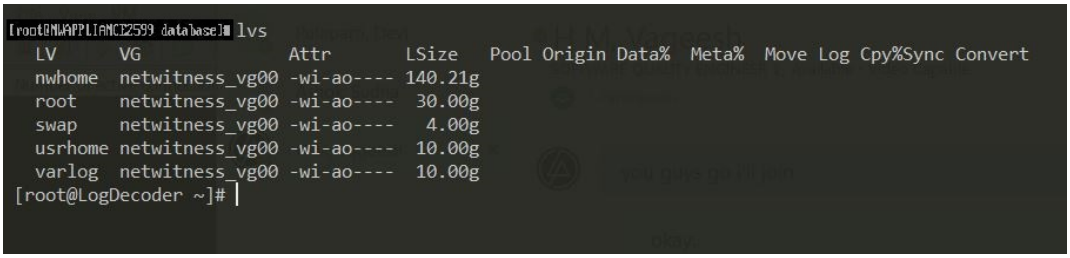
      Se muestra la siguiente información.

```
[root@NWAPPLIANCE2599 database]# vgextend netwitness_vg00 /dev/sde1
  Volume group "netwitness_vg00" successfully extended
[root@NWAPPLIANCE2599 database]# pvs
  PV         VG              Fmt  Attr PSize   PFree
  /dev/sda2  netwitness_vg00 lvm2 a--  194.31g 100.00m
  /dev/sdb1  VolGroup00      lvm2 a--   48.00g      0
  /dev/sdc1  VolGroup01      lvm2 a--  104.00g      0
  /dev/sdd1  VolGroup01      lvm2 a--  168.00g      0
  /dev/sde1  netwitness_vg00 lvm2 a--   10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

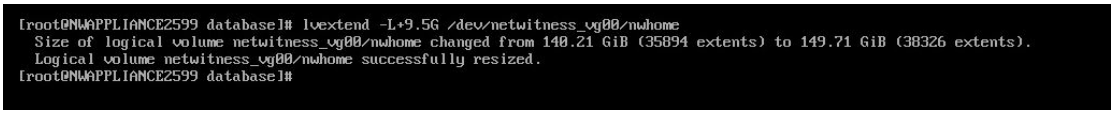
      El volumen se agregó a `netwitness_vg00`, pero aún no se extiende (aún tiene 10 GB de espacio libre). Hay varios volúmenes lógicos en `netwitness_vg00`; este ejemplo involucra a PacketDB.

4. Para extender el volumen lógico PacketDB de modo que use los 10 GB de espacio libre.

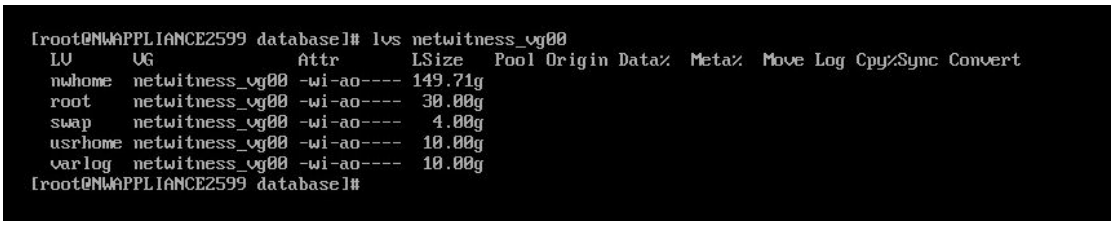
   a. Ingrese `lvs netwitness_vg00`.
   Se muestra la siguiente información.



   b. Ingrese `lvextend -L+9.5G /dev/netwitness_vg00/nwhome`.
   Se muestra la siguiente información.



   c. Ingrese `lvs netwitness_vg00`.
   Se muestra la siguiente información.



El volumen lógico `packetdb` se extendió a 149.71 GB, pero el sistema de archivos `/var/netwitness` aún tiene 140.21 GB.

Expandir el sistema de archivos

1. Acceda al host de Log Decoder mediante el protocolo SSH.
2. Ingrese la siguiente cadena de comandos para crear un volumen físico del Administrador de volúmenes lógicos (LVM) en la partición nueva.
   `[root@LogDecoderGM ~]# xfs_growfs /var/netwitness/`

Se muestra la siguiente información.

```
[root@NWAPPLIANCE2599 database]# xfs_growfs /var/netwitness/
meta-data=/dev/mapper/netwitness_vg00-nwhome isize=256    agcount=4, agsize=9188864 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=36755456, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal               bsize=4096   blocks=17947, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 36755456 to 39245824
[root@NWAPPLIANCE2599 database]# _
```

Iniciar los servicios

Ingrese la siguiente cadena de comando para iniciar los servicios en el host de Log Decoder.

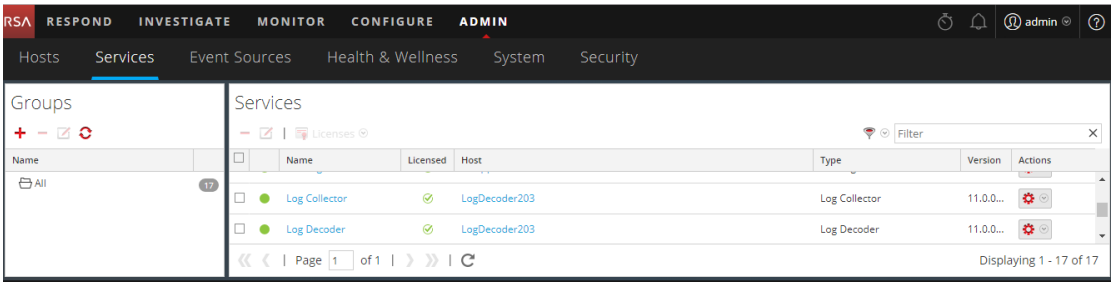
```
[root@LogDecoderGM ~]# service nwlogcollector start; service
nwlogdecoder start
```

Se muestra la siguiente información.

```
nwlogcollector start/running, process 4069
nwlogdecoder start/running, process 4069
```

Asegurarse de que los servicios estén en ejecución

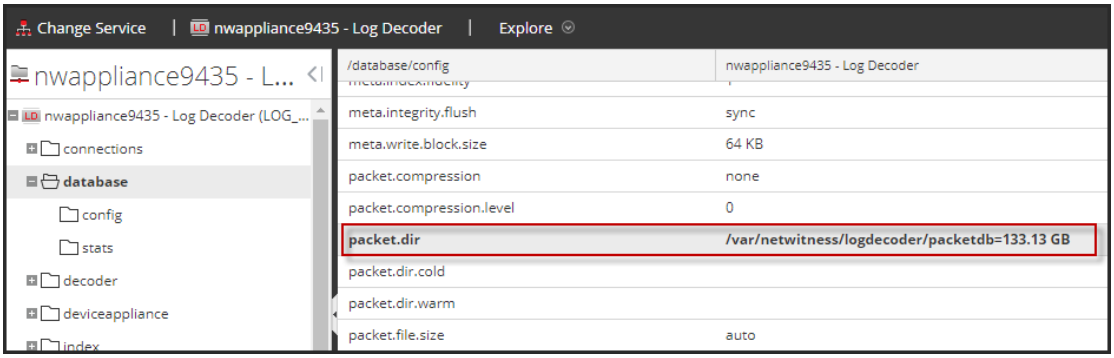
1. Inicie sesión en NetWitness Suite.
2. Haga clic en **Administration** > **Servicios**.
3. Asegúrese de que los servicios Log Collector y Log Decoder estén en ejecución.



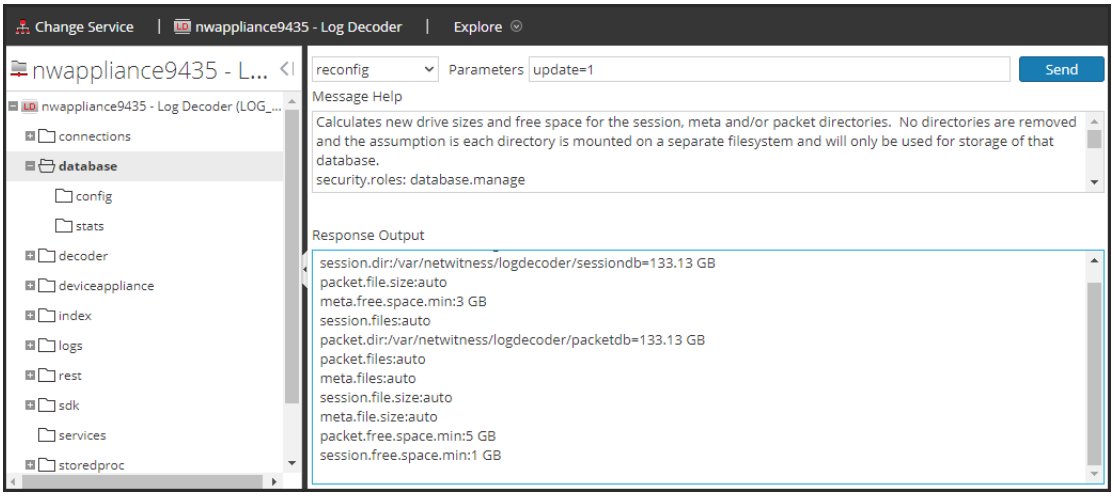
Volver a configurar los parámetros de Log Decoder

1. Inicie sesión en NetWitness Suite.
2. Haga clic en **Administration** > **Servicios**.
3. Seleccione el servicio Log Decoder.
4. En Acciones, seleccione Ver > Explorar.

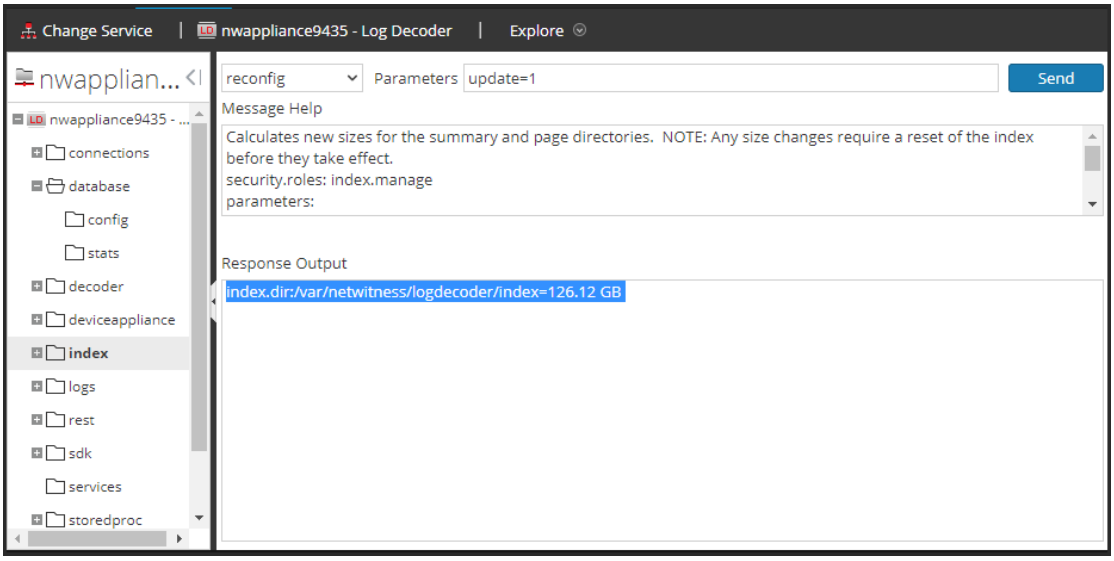
5. Haga clic en `database > config > packet.dir`.



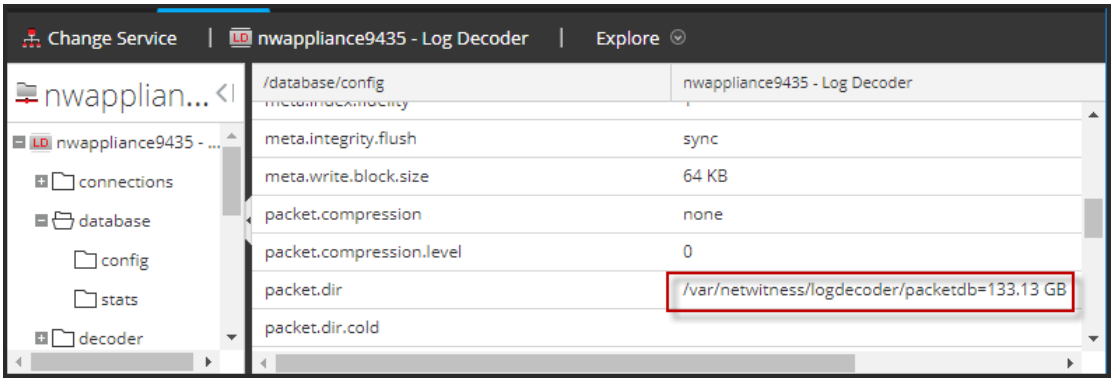
6. Haga clic con el botón secundario en `database`, haga clic en **Propiedades**, seleccione el comando **reconfig**, especifique **update=1** en **Parámetros** y haga clic en **Enviar**.
El valor del parámetro `packetdb` cambió de 98.74 GB a 133.13 GB.



7. Haga clic con el botón secundario en `index`, haga clic en **Propiedades**, seleccione el comando **reconfig**, especifique **update=1** en **Parámetros** y haga clic en **Enviar**.



8. Cierre el cuadro de diálogo Propiedades para volver a la vista Explorar. El valor del parámetro `packet.dir` ahora es 133.13 GB (95 % de 203 GB).



Paso 4. Configurar parámetros específicos del host

Ciertos parámetros específicos de las aplicaciones se requieren para configurar la recopilación de registros y la captura de paquetes en el ambiente virtual.

Configurar recopilación de registros en el ambiente virtual

La recopilación de registros se puede llevar a cabo fácilmente mediante el envío de los registros a la dirección IP que especificó para el Decoder. La interfaz de administración del Decoder permite seleccionar la interfaz adecuada para escuchar el tráfico si aún no se selecciona una de forma predeterminada.

Configurar una captura de paquetes en el ambiente virtual

Existen dos opciones para la captura de paquetes en un ambiente VMware. Lo primero es configurar el vSwitch en modo promiscuo y lo segundo es utilizar un tap virtual de otros fabricantes.

Configurar un vSwitch en modo promiscuo

La opción de poner un switch, ya sea virtual o físico, en modo promiscuo, el cual también se describe como un puerto SPAN (servicios de Cisco) y espejeado de puertos, no está exenta de limitaciones. Ya sea virtual o física, según la cantidad y el tipo de tráfico que se está copiando, la captura de paquetes puede llevar fácilmente a la sobresuscripción del puerto, lo cual significa la pérdida de paquetes. Los taps, ya sean físicos o virtuales, están diseñados y destinados para capturar el 100 % del tráfico deseado, sin pérdida.

El modo promiscuo está desactivado de manera predeterminada y no debe activarse a menos que se necesite específicamente. El software que se ejecuta en una máquina virtual puede ser capaz de monitorear todo el tráfico que pasa por un vSwitch si se le permite ingresar al modo promiscuo y causar pérdida de paquetes debido a la sobresuscripción del puerto.

Para configurar un grupo de puertos o switch virtual para permitir el modo promiscuo:

1. Inicie sesión en el host ESXi/ESX o vCenter Server mediante vSphere Client.
2. Seleccione el host ESXi/ESX en el inventario.
3. Seleccione la pestaña **Configuración**.
4. En la sección **Hardware**, haga clic en **Redes**.
5. Seleccione **Propiedades** del switch virtual para el cual desea activar el modo promiscuo.
6. Seleccione el switch virtual o grupo de puertos que desea modificar y haga clic en **Editar**.
7. Haga clic en la pestaña **Seguridad**. En el menú desplegable **Modo promiscuo**, seleccione **Aceptar**.

Uso de un Tap virtual de otros fabricantes

Los métodos de instalación de un tap virtual varían según el proveedor. Consulte la documentación de su proveedor para obtener instrucciones sobre la instalación. Por lo general, los taps virtuales son fáciles de integrar, y la interfaz del usuario del tap simplifica la selección y el tipo de tráfico que se copiará.

Los taps virtuales encapsulan el tráfico capturado en un túnel GRE. Según el tipo que seleccione, cualquiera de estos escenarios puede aplicarse:

- Se requiere un host externo para terminar el túnel y el host externo dirige el tráfico a la interfaz de Decoder.

- El túnel envía el tráfico directamente a la interfaz de Decoder, donde NetWitness Suite maneja su desencapsulado.