



Guía de instalación de hosts virtuales

para la versión 11.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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

Guía de instalación de hosts virtuales	5
Implementación virtual básica	6
Abreviaturas que se utilizan en la Guía de implementación virtual	6
Hosts virtuales compatibles	7
Medios de instalación	7
Recomendaciones para ambientes virtuales	7
Requisitos del sistema recomendados para un host virtual	8
Escenario uno	8
Escenario dos	10
Escenario tres	13
Escenario cuatro	15
Reglas de dimensionamiento de los recopiladores de Windows existente	15
Instalar el host virtual de NetWitness Platform en un ambiente virtual	17
Requisitos previos	17
Paso 1. Implementar el host virtual para crear VM	17
Requisitos previos	17
Procedimiento	17
Paso 2. Configurar la red	21
Requisitos previos	21
Procedimiento	21
Revisar los puertos del firewall abiertos	21
Paso 3. Configurar las bases de datos para adaptarse a NetWitness Platform	21
Tarea 1. Revisar la configuración inicial del almacén de datos	22
Espacio inicial asignado a PacketDB	22
Tamaño inicial de la base de datos	22
Punto de montaje de PacketDB	23
Tarea 2. Revisar la configuración óptima del espacio del almacén de datos	24
Tasas de espacio de unidad virtual	25
Tarea 3. Agregar un volumen nuevo y extender los sistemas de archivos existentes	26
AdminServer	29
ESAPrimary/ESASSecondary/Malware	30
LogCollector	30
LogDecoder	30
Concentrator	32

Archiver	34
Decoder	35
Instalar RSA NetWitness Platform	37
Paso 4. Configurar parámetros específicos del host	54
Configurar recopilación de registros en el ambiente virtual	54
Configurar una captura de paquetes en el ambiente virtual	55
Uso de un Tap virtual de otros fabricantes	55
Paso 5. Tareas posteriores a la instalación	56
General	56
RSA NetWitness Endpoint Insights	56
Habilitación de FIPS	58
NetWitness User Entity Behavior Analytics (UEBA)	59
Apéndice A. Solución de problemas	65
Interfaz de la línea de comandos (CLI)	66
Respaldo (script nw-backup)	67
Event Stream Analysis	69
Servicio Log Collector (nwlogcollector)	70
Servidor de NW	72
Orchestration	72
Servicio Reporting Engine	73
NetWitness UEBA	74
Apéndice B. Crear un repositorio externo	75
Historial de revisiones	77

Guía de instalación de hosts virtuales

En este documento se proporcionan instrucciones sobre la instalación y la configuración de los hosts de RSA NetWitness® Platform 11.2.0.0 que se ejecutan en un ambiente virtual.

Implementación virtual básica

Este tema presenta reglas y requisitos generales para la implementación de RSANetWitness Platform 11.2.0.0 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
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)
RSA NetWitness UEBA	RSA NetWitness User and Entity Behavior Analysis

Hosts virtuales compatibles

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

- NetWitness Server
- Event Stream Analysis: ESA primario y ESA secundario
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Endpoint Hybrid
- Endpoint Log Hybrid
- User and Entity Behavior Analysis (UEBA)

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 Platform. 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.
- 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 Platform 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 Platform”.
- 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 11.2.0.0 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 Network 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

Network 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 Network Decoder, un Concentrator y un Warehouse Connector.
- Event Stream Analysis agregaba a 90,000 EPS desde tres Hybrid Concentrators.
- Respond recibía alertas de Reporting Engine y Event Stream Analysis.
- La carga en segundo plano incluía informes, gráficos, alertas, Investigation y Respond.
- 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

Network 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 GHz	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 GHz	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 GHz	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 GHz	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

NWS1: servidor de NetWitness y componentes colocados

NetWitness Server, Jetty, Broker, Respond y Reporting Engine se encuentran en la misma ubicación.

CPU	Memoria	IOPS de lectura	IOPS de escritura
12 o 31.18 GHz	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 Network Decoder y el Concentrator.
- Event Stream Analysis agregaba a 90,000 EPS desde tres Hybrid Concentrators.
- Respond 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

Network 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

Escenario cuatro

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

- Todos los componentes estaban integrados.
- El servidor de Endpoint está instalado.
- El flujo de registros incluía un Log Decoder y un Concentrator.

Endpoint Hybrid

Agentes	CPU	Memoria	Valores de IOPS		
			IOPS de lectura	IOPS de escritura	
5,000	16 o 42 GHz	32 GB	Log Decoder	250	150
			Concentrator	150	7,050
			MongoDb	250	150

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 Platform* para conocer las reglas de dimensionamiento del Recopilador de Windows existente.

UEBA

CPU	Memoria	IOPS de lectura	IOPS de escritura
16 o 2.4 GHz	64 GB	500	500

Nota: RSA recomienda implementar UEBA únicamente en un host virtual si el volumen de recopilación de registros es bajo. Si el volumen de recopilación de registros es de moderado a alto, RSA recomienda implementar UEBA en el host físico que se describe en “Especificaciones de hardware del host de RSA NetWitness UEBA” en la Guía de instalación de hosts físicos. Póngase en contacto con el servicio al cliente (<https://community.rsa.com/docs/DOC-1294>) para obtener asesoría sobre la elección del host, virtual o físico, que debe utilizar para UEBA.

Instalar el host virtual de NetWitness Platform en un ambiente virtual

Realice los siguientes procedimientos de acuerdo con su secuencia numerada para instalar RSA NetWitness® Platform 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, vSphere 5.0 Client o vSphere 6.0 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 para crear VM

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

Requisitos previos

Asegúrese de contar con:

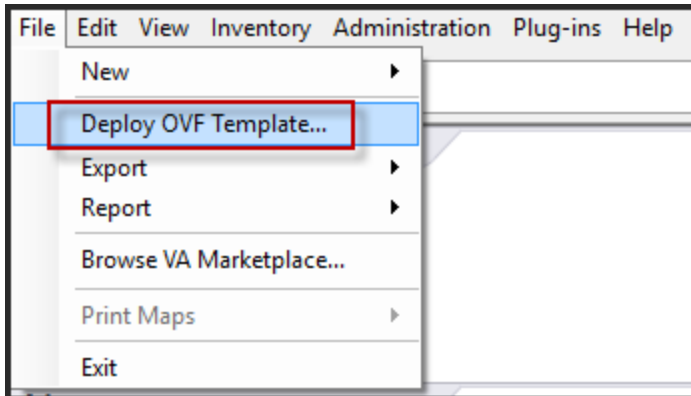
- Direcciones IP de red, máscara de red y direcciones IP de gateway para el host virtual.
- Nombres de red de todos los hosts virtuales, si está creando un clúster.
- Información de DNS o host.
- Contraseña para el acceso de los hosts virtuales. El nombre de usuario predeterminado es `root` y la contraseña predeterminada es `netwitness`.
- El archivo de paquete del host virtual de NetWitness Platform, por ejemplo, `rsanw-11.2.0.xxxx.e17-x86_64.ova`. (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.

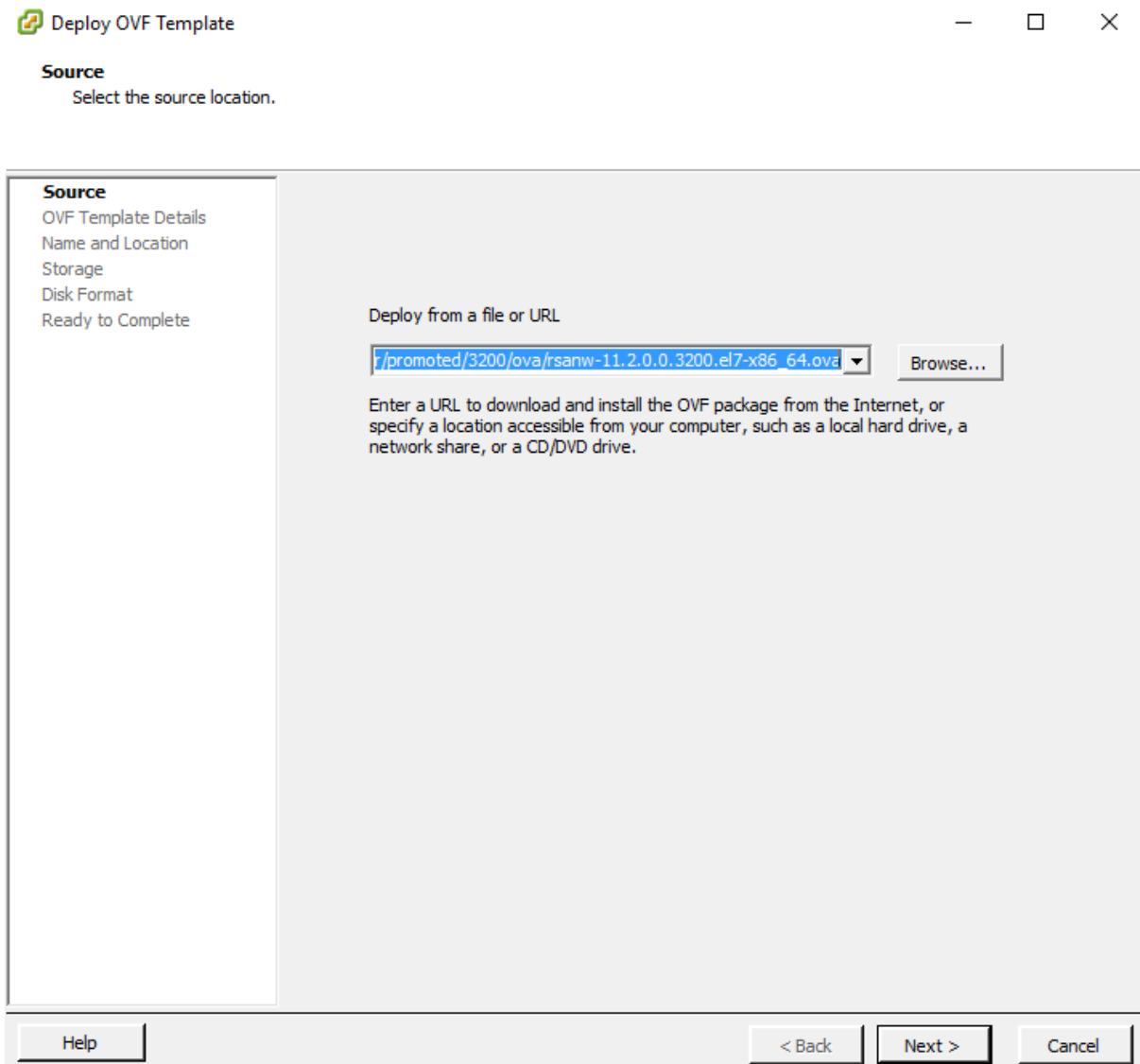
Para implementar el host OVA:

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 **Deploy OVF Template**, seleccione el OVF del host que desea implementar en el ambiente

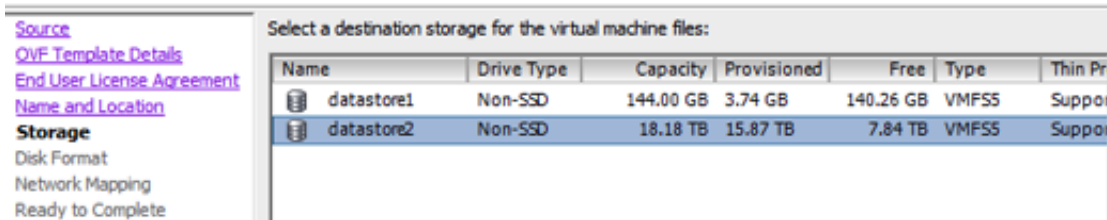
virtual (por ejemplo, V11.2 GOLD\rsanw-11.2.0.0.1948.el7-x86_64.ova) y haga clic en **Next**.



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.

Storage

Where do you want to store the virtual machine files?



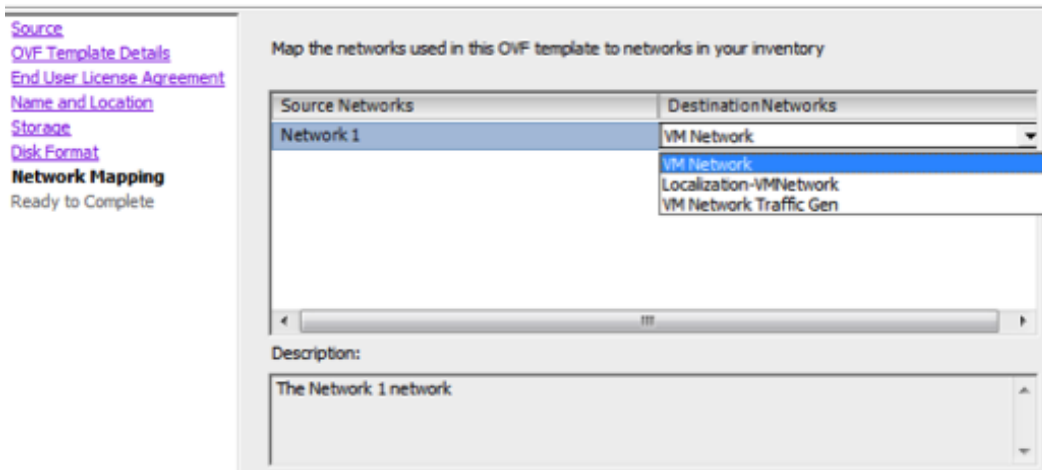
6. En las opciones de almacenamiento, designe la ubicación del almacén de datos para el host virtual.

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 Platform en ciertos hosts (los cuales se analizan en las secciones siguientes).

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

Network Mapping

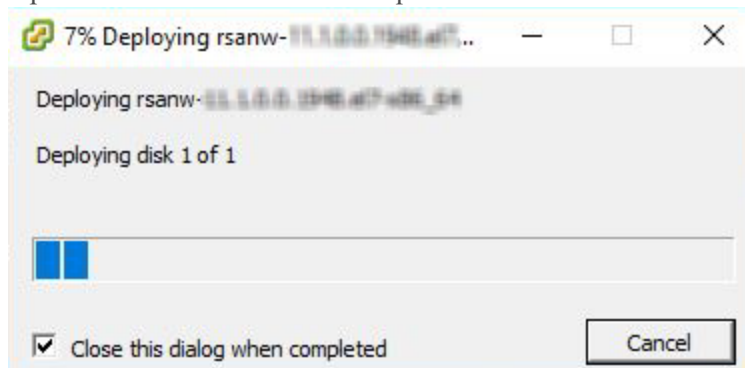
What networks should the deployed template use?



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

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 Platform, de modo que pueda configurar los servicios NetWitness Platform y los firewalls. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

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

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

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 NetWitness Server. Debe revisar el estado de los almacenes

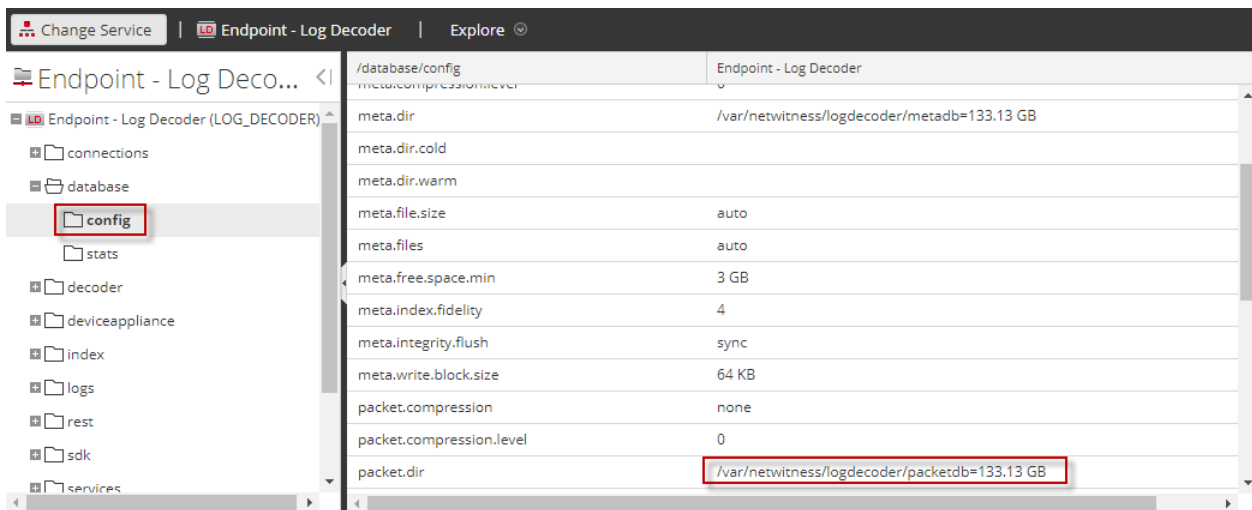
de datos después de la implementación inicial y expandirlos.

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 de alrededor de 133.13 GB). En el siguiente ejemplo de la vista Explorar de NetWitness Platform 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@LogDecoder ~]# df -kh
Filesystem                Size      Used Avail Use% Mounted on
/dev/mapper/netwitness_vg00-root  30G    3.0G   27G  10% /
devtmpfs                  16G         0   16G   0% /dev
tmpfs                     16G     12K   16G   1% /dev/shm
tmpfs                     16G     25M   16G   1% /run
tmpfs                     16G         0   16G   0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome  10G    33M   10G   1% /home
/dev/mapper/netwitness_vg00-varlog   10G    42M   10G   1% /var/log
/dev/mapper/netwitness_vg00-nwhome  141G   396M  140G   1% /var/netwitness
/dev/sda1                 1014M    73M   942M   8% /boot
tmpfs                     3.2G         0   3.2G   0% /run/user/0
[root@LogDecoder ~]#
```

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.

```
[root@LogDecoder ~]# vgs
VG                #PV #LV #SN Attr   VSize   VFree
netwitness_vg00   1   5   0 wz--n- <194.31g 100.00m
```

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.

```
[root@LogDecoder ~]# pvs
PV                VG                Fmt Attr PSize   PFree
/dev/sda2         netwitness_vg00  lvm2 a--  <194.31g 100.00m
```

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.

```
[root@LogDecoder ~]# vgs
VG          #PV #LV #SN Attr   VSize   VFree
netwitness_vg00  1   5   0 wz--n- <194.31g 100.00m
```

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 Platform. 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 PlatformCore](#) 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

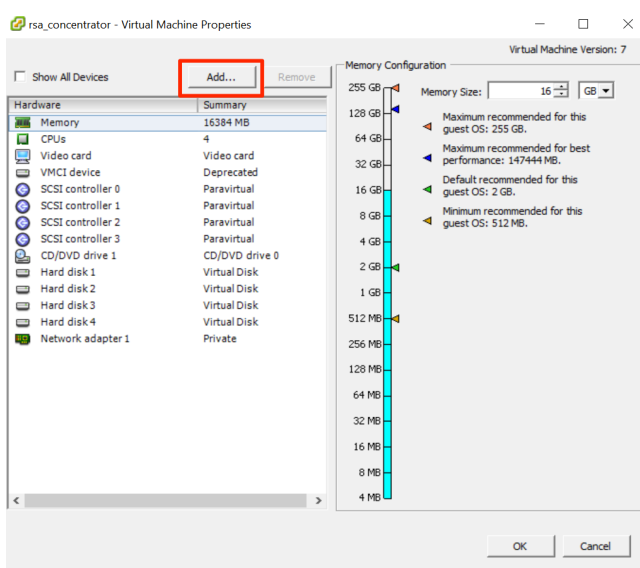
6. Iniciar los servicios
7. Asegurarse de que los servicios estén en ejecución
8. Volver a configurar los parámetros de Log Decoder

Agregar un disco nuevo

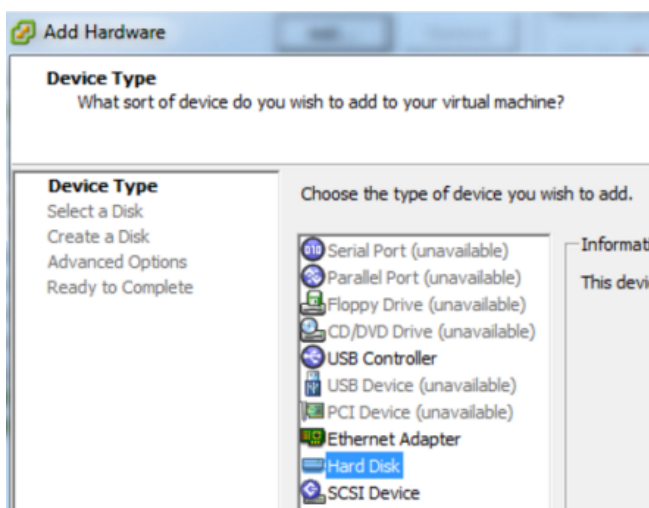
En este procedimiento se muestra cómo agregar un disco de 100 GB nuevo en el mismo almacén de datos.

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

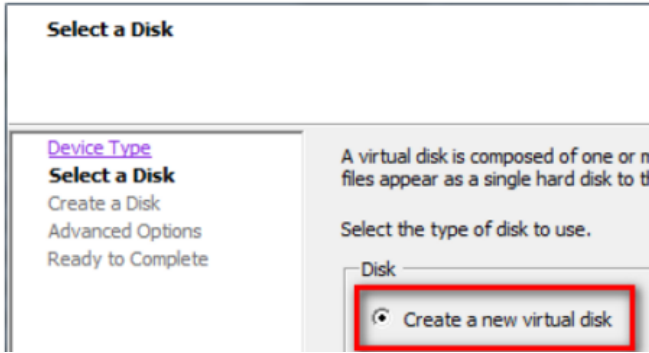
1. Apague la máquina, edite las **Propiedades de máquinas virtuales**, haga clic en la pestaña **Hardware** y, a continuación, en **Agregar**.



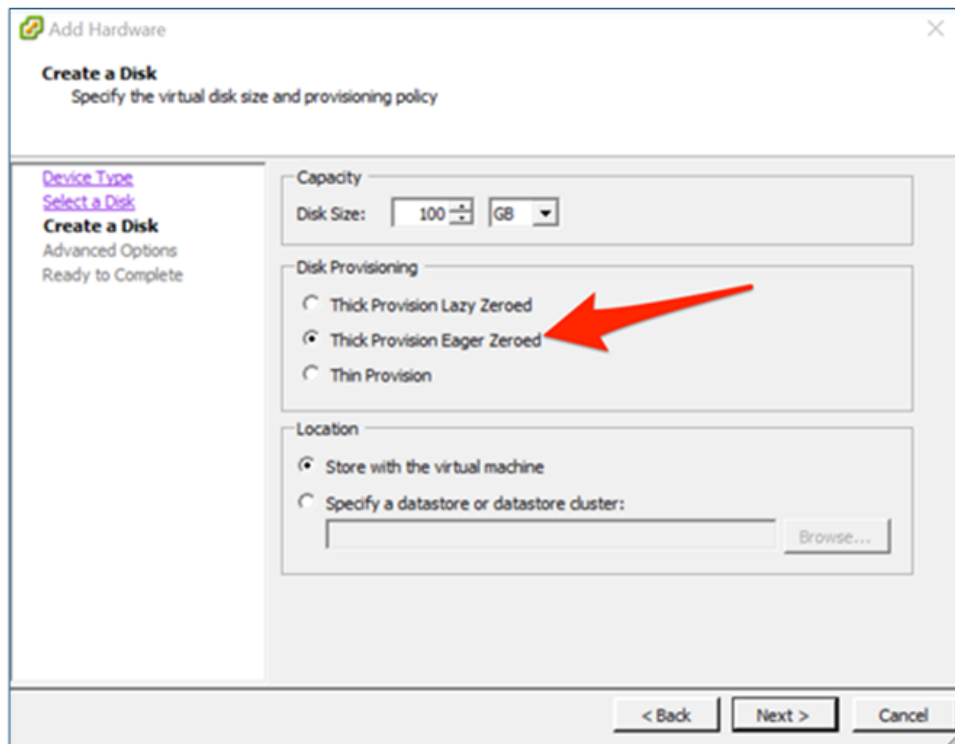
2. Seleccione **Disco duro** como el tipo de dispositivo.



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

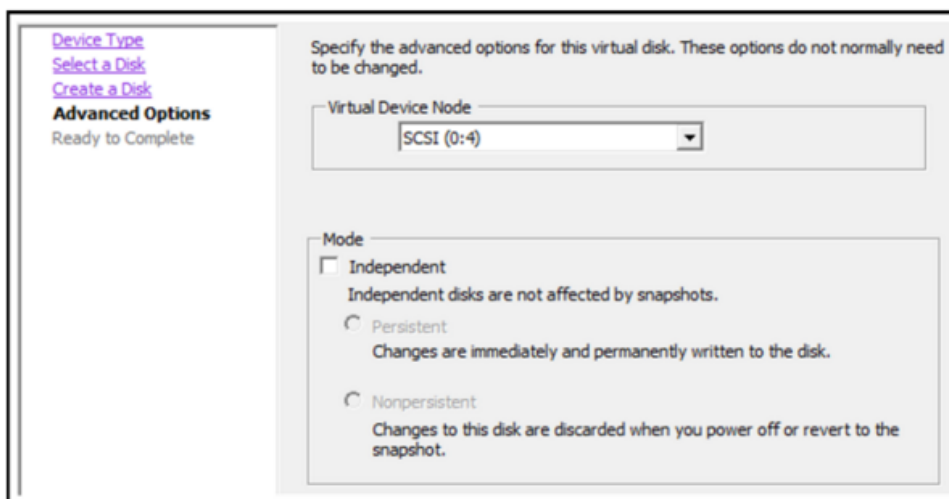


4. Seleccione el tamaño del disco nuevo y dónde desea crearlo (en el mismo almacén de datos o en otro).



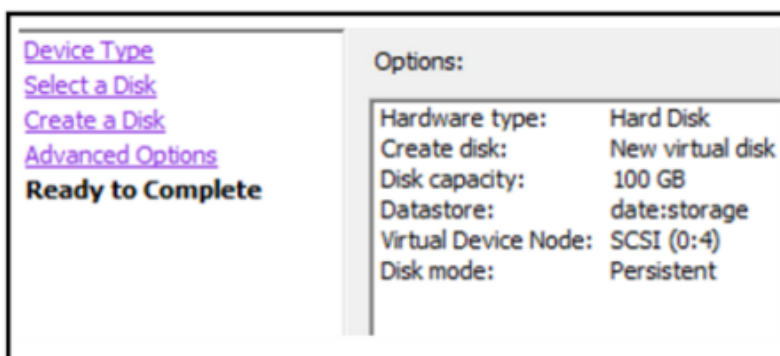
Precaución: Por motivos de rendimiento, asigne todo el espacio.

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.



Extending File Systems

Follow the instructions provided to extend the file systems for the various components.

AdminServer

Attach external disk for extension of `/var/netwitness/` (refer to the steps in attaching the disk) partition. Create an additional disk with suffix as `nwhome`.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk.
2. `pvccreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for AdminServer (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	2TB	SSD	Read/Write

ESAPrimary/ESASecondary/Malware

Attach external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
2. `pvccreate <pv_name> . ex suppose the PV name is /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for ESAPrimary/ESASecondary (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	6TB	HDD	Read/Write

LogCollector

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

1. Execute `lsblk` and get the physical volume name, for example if you attach one 500GB disk
2. `pvccreate <pv_name> . ex suppose the PV name is /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 600G /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for LogCollector (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	500GB	HDD	Read/Write

LogDecoder

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome, attach other external disks for Logdecoder database partition. For extending /var/netwitness partition follow these steps:

Nota: No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Other partitions are also required. Create the following four partitions on volume group logdecodersmall

Folder	LVM	Volume Group
<code>/var/netwitness/logdecoder</code>	decoroot	logdecodersmall
<code>/var/netwitness/logdecoder/index</code>	index	logdecodersmall
<code>/var/netwitness/logdecoder/metadb</code>	metadb	logdecodersmall
<code>/var/netwitness/logdecoder/sessiondb</code>	sessiondb	logdecodersmall

Follow these steps to create the partitions:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecodersmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lvm_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecoderssmall/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

The following four partitions should be on volume group logdecoder and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/logdecoder/packetdb</code>	packetdb	logdecoder

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 logdecoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb logdecoder`
5. `mkfs.xfs /dev/logdecoder/packetdb`

RSA recommends below sizing partition for LogDecoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HD D	Read/Write
/dev/logdecoderssmall/decoroot	/var/netwitness/logdecoder	10GB	HD D	Read/Write
/dev/logdecoderssmall/index	/var/netwitness/logdecoder/index	30GB	HD D	Read/Write
/dev/logdecoderssmall/metadb	/var/netwitness/logdecoder/metadb	370GB	HD D	Read/Write
/dev/logdecoderssmall/sessiondb	/var/netwitness/logdecoder/sessiondb	3TB	HD D	Read/Write
/dev/logdecoder/packetdb	/var/netwitness/logdecoder/packetdb	18TB	HD D	Read/Write

Create each directory and mount the LVM on it in a serial manner, except /var/netwitness which will be already created.

Nota: Create the folder /var/netwitness/logdecoder and mount on /dev/logdecoderssmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using mount -a.

```

/dev/logdecoderssmall/decoroot /var/netwitness/logdecoder xfs noatime,nosuid 1 2
/dev/logdecoderssmall/index /var/netwitness/logdecoder/index xfs noatime,nosuid 1 2
/dev/logdecoderssmall/metadb /var/netwitness/logdecoder/metadb xfs noatime,nosuid 1 2
/dev/logdecoderssmall/sessiondb /var/netwitness/logdecoder/sessiondb xfs noatime,nosuid 1 2
/dev/logdecoder/packetdb /var/netwitness/logdecoder/packetdb xfs noatime,nosuid 1 2

```

Concentrator

Attach external disk for extension of /var/netwitness/ partition, Create an external disk with suffix as nwhome, attach other external disks for Concentrator database partition. If there are multiple disks, create a Raid 0 array.

For extending /var/netwitness partition follow below steps:

Nota: No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partition are also required on volume group concentrator and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator</code>	Root	Concentrator
<code>/var/netwitness/ concentrator /sessiondb</code>	index	Concentrator
<code>/var/netwitness/ concentrator /metadb</code>	metadb	Concentrator

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 concentrator /dev/md0`
4. `lvcreate -L <disk_size> -n <lvm_name> concentrator`
5. `mkfs.xfs /dev/concentrator/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below four partitions should be on volume group index and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator/index</code>	index	index

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md1`
3. `vgcreate -s 32 index /dev/md1`
4. `lvcreate -L <disk_size> -n index index`
5. `mkfs.xfs /dev/index/index`

RSA recommends below sizing partition for Concentrator (Can be changed based on the retention days)

LVM	Folder	Size	Dis k Typ e	Cachin g
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HD D	Read/Wr ite
/dev/concentrator/decoroot	/var/netwitness/concentrator	10G B	HD D	Read/Wr ite
/dev/concentrator/metadb	/var/netwitness/concentrator/ metadb	370G B	HD D	Read/Wr ite
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb	3TB	HD D	Read/Wr ite
/dev/index/index	/var/netwitness/concentrator/ index	2TB	SSD	Read/Wr ite

Create each directory and mount the LVM on it in a serial manner, except /var/netwitness which will be already created.

Nota: Create the folder /var/netwitness/concentrator and mount on /dev/concentrator/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order

```
/dev/concentrator/root /var/netwitness/concentrator xfs noatime,nosuid 1 2
/dev/concentrator/sessiondb /var/netwitness/concentrator/sessiondb xfs
noatime,nosuid 1 2
/dev/concentrator/metadb /var/netwitness/concentrator/metadb xfs
noatime,nosuid 1 2 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
```

Archiver

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome, attach other external disks for Archiver database partition. If there are multiple disks, create a Raid 0 array.

For extending /var/netwitness partition follow these steps:

Nota: No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partitions are required on volume group archiver and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/archiver	Archiver	archiver

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 archiver /dev/md0`
4. `lvcreate -L <disk_size> -n archiver archiver`
5. `mkfs.xfs /dev/archiver/archiver`

RSA recommends below sizing partition for archiver (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD	Read/Write
/dev/archiver/archiver	/var/netwitness/archiver	4TB	HDD	Read/Write

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/archiver/archiver /var/netwitness/archiver xfs noatime,nosuid 1 2
```

Decoder

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for decoder database partition. For extending `/var/netwitness` partition follow these steps:

Nota: No other partition should reside on this partition, only to be used for `/var/netwitness/partition`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name> . ex suppose the PV name is /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Below four partition should be on volume group `decodersmall`

Folder	LVM	Volume Group
/var/netwitness/decoder	decoroot	decoderssmall
/var/netwitness/decoder/index	index	decoderssmall
/var/netwitness/decoder/metadb	metadb	decoderssmall
/var/netwitness/decoder/sessiondb	sessiondb	decoerssmall

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecoderssmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lvm_name> logdecoderssmall`
5. `mkfs.xfs /dev/logdecoderssmall/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below partition should be on volume group logdecoder and should be in single RAID 0 array

Below four partition should be on volume group logdecoder and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/logdecoder/packetdb	packetdb	decoder

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 decoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb decoder`
5. `mkfs.xfs /dev/decoder/packetdb`

RSA recommends below sizing partition for Decoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness	1TB	HDD	Read/Write
/dev/decoderssmall/decoroot	/var/netwitness/decoder	10GB	HDD	Read/Write

LVM	Folder	Size	Disk Type	Caching
/dev/decodersmall/index	/var/netwitness/decoder/index	30GB	HDD	Read/Write
/dev/decoderssmall/metadb	/var/netwitness/decoder/metadb	370GB	HDD	Read/Write
/dev/decoderssmall/sessiondb	/var/netwitness/decoder/sessiondb	3TB	HDD	Read/Write
/dev/decoder/packetdb	/var/netwitness/decoder/packetdb	18TB	HDD	Read/Write

Create each directory and mount the LVM on it in serial manner, except /var/netwitness which will be already created.

Nota: Create the folder /var/netwitness/decoder and mount on /dev/decoderssmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using mount -a.

```

/dev/decoderssmall/decoroot /var/netwitness/decoder xfs noatime,nosuid 1 2
/dev/decoderssmall/index /var/netwitness/decoder/index xfs noatime,nosuid 1 2
/dev/decoderssmall/metadb /var/netwitness/decoder/metadb xfs noatime,nosuid 1 2
/dev/decoderssmall/sessiondb /var/netwitness/decoder/sessiondb xfs noatime,nosuid 1 2
/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2
    
```

Instalar RSA NetWitness Platform

Existen dos tareas principales que debe realizar en el orden en que se enumeran a continuación para instalar NetWitness Platform 11.2

1. Tarea 1: Instalar 11.2.0.0 en el host del servidor de NetWitness (NW)
2. Tarea 2: Instalar 11.2.0.0 en otros hosts de componentes

Tarea 1: Instalar 11.2.0.0 en el host del servidor de NW

En el host que implementó para el servidor de NW, esta tarea instala:

- La plataforma ambiental del servidor de NW 11.2.0.0.

- Los componentes del servidor de NW (es decir, servidor de Admin, servidor de Config, servidor de Orchestration, servidor de Integration, Broker, servidor de Investigate, Reporting Engine, servidor de Respond y servidor de Security).
- Un repositorio con los archivos RPM requeridos para instalar los otros componentes o servicios funcionales.

1. Implemente el ambiente 11.2.0.0:
 - a. Agregue una nueva VM.
 - 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 [\(Opcional\) Tarea 1: Volver a configurar servidores DNS después de 11.2](#) en Tareas posteriores a la instalación.

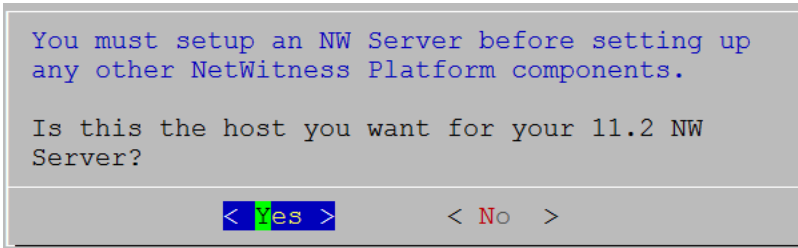
Si no especifica servidores DNS durante `nwsetup-tui`, debe seleccionar **1 El repositorio local (en el servidor de NW)** en el indicador **Repositorio de actualizaciones de NetWitness Platform** en el paso 12 (los servidores DNS no están definidos, de modo que el sistema no puede acceder al repositorio externo).

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>

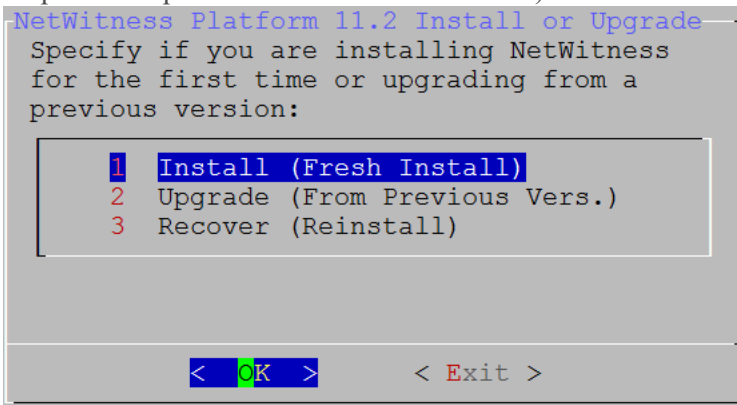
- Use la tecla de tabulación para ir a **Aceptar** y presione Intro.
Se muestra el indicador **¿Es este el host que desea para el servidor de NW 11.2?**.



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

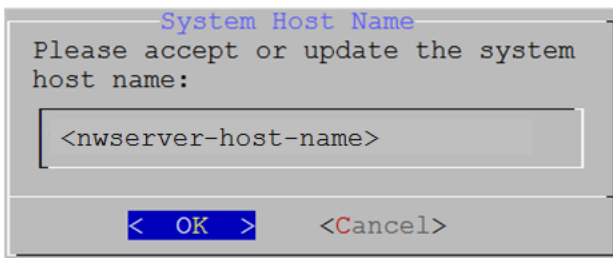
Precaución: Si elige el host incorrecto para el servidor de NW y completa la configuración, debe iniciar el programa de instalación (paso 3) y completar todos los pasos subsiguientes para corregir este error.

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



- Presione **Intro**. La opción **Instalar (instalación nueva)** está seleccionada de manera predeterminada.

Se muestra el indicador **Nombre del host**.



Precaución: Si incluye “.” en un nombre de host, el nombre de host también debe incluir un nombre de dominio válido.

- 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.

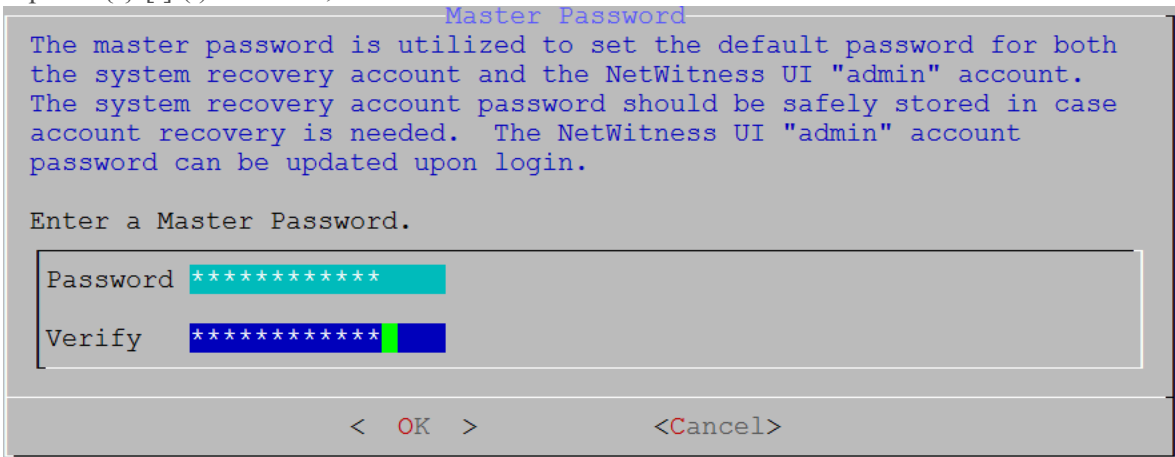
7. Se muestra el indicador **Contraseña maestra**.

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



8. Se muestra el indicador **Contraseña maestra**.

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

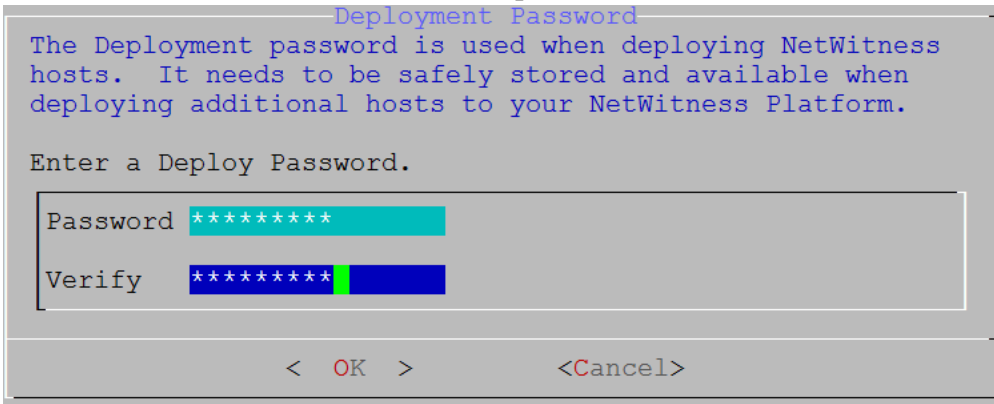
- Símbolos: ! @ # % ^ + ,
- Números: 0-9
- Caracteres en minúscula: a-z
- Caracteres en mayúscula: A-Z

Ningún carácter ambiguo es compatible para Contraseña maestra y Contraseña de implementación. Por ejemplo:

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

9. 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.

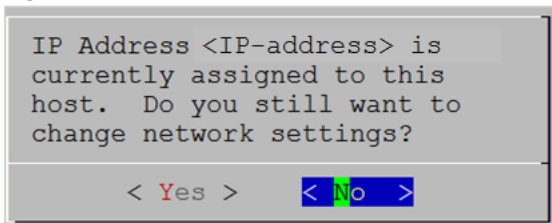
Se muestra el indicador **Contraseña de implementación.**



10. 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 uno de los siguientes indicadores condicionales.

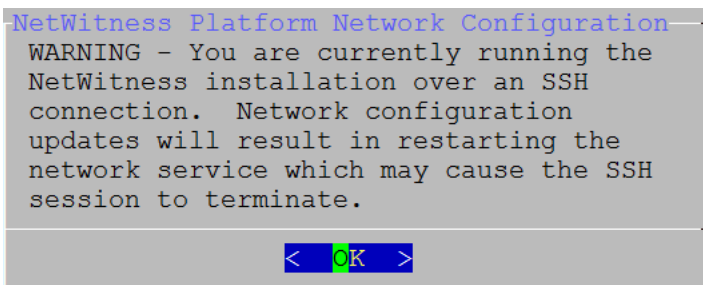
- Si el programa de instalación encuentra una dirección IP válida para este host, se muestra el siguiente indicador.



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.

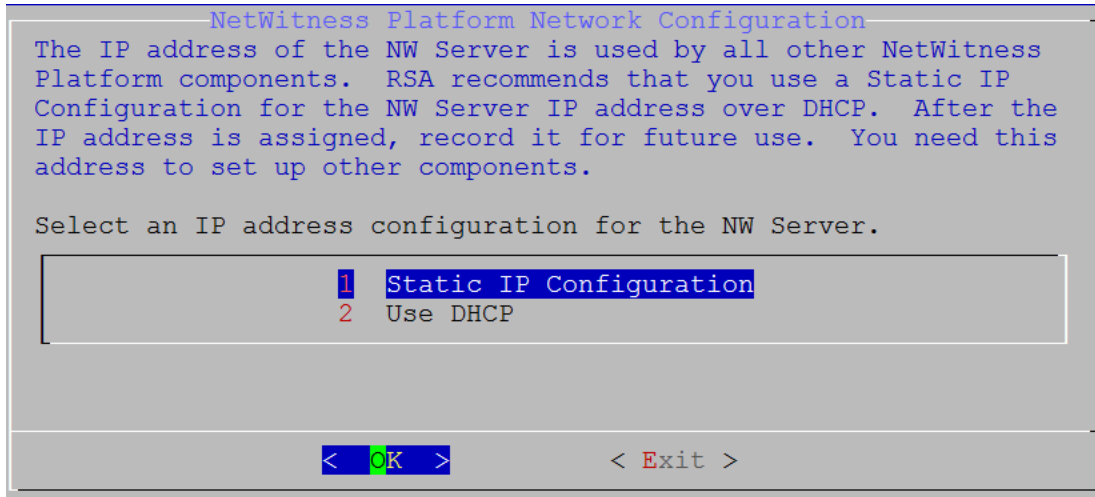
Nota: Si se conecta directamente desde la consola del host, no se mostrará la siguiente advertencia.



Presione **Intro** para cerrar el indicador de advertencia.

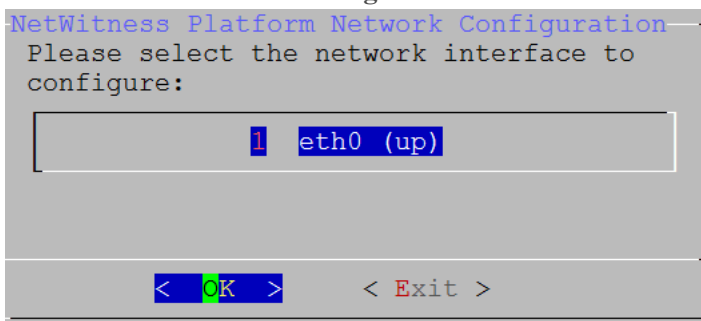
Nota: Si se conecta directamente desde la consola del host, no se mostrará la advertencia mencionada anteriormente.

- 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 red**.



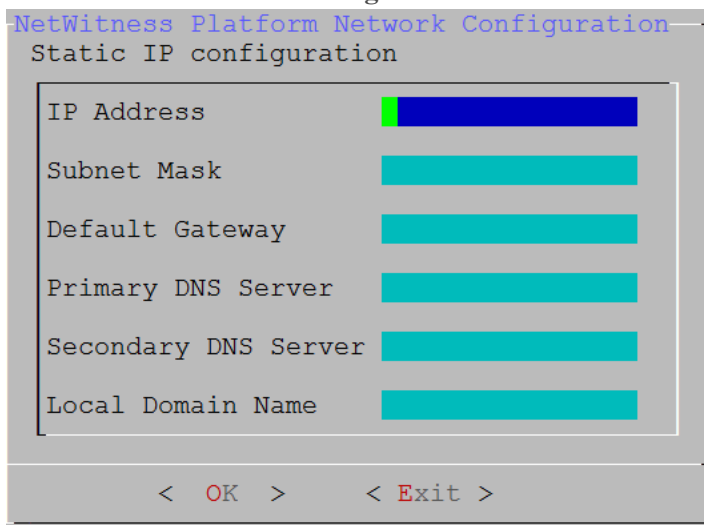
11. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para usar **Dirección IP estática**. Si desea usar **DHCP**, use la flecha hacia abajo para desplazarse hasta 2 Usar DHCP y presione **Intro**.

Se muestra el indicador **Configuración de red**.



12. 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**.

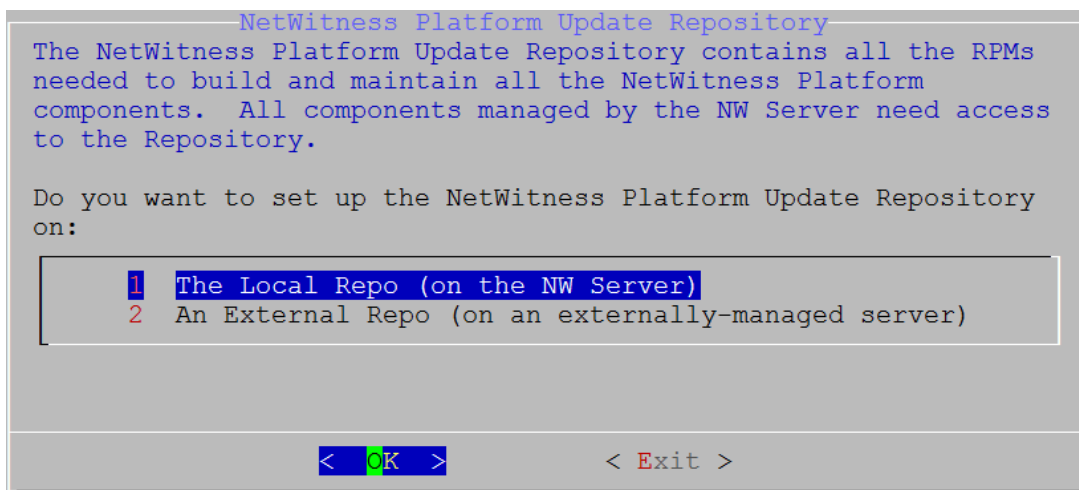


13. Escriba los valores de configuración (con la flecha hacia abajo para desplazarse de un campo a otro), use la tecla de tabulación para ir a **Aceptar** y presione **Intro**. Si no completa todos los campos obligatorios, se muestra un mensaje de error *All fields are required* (los campos **Servidor 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**.

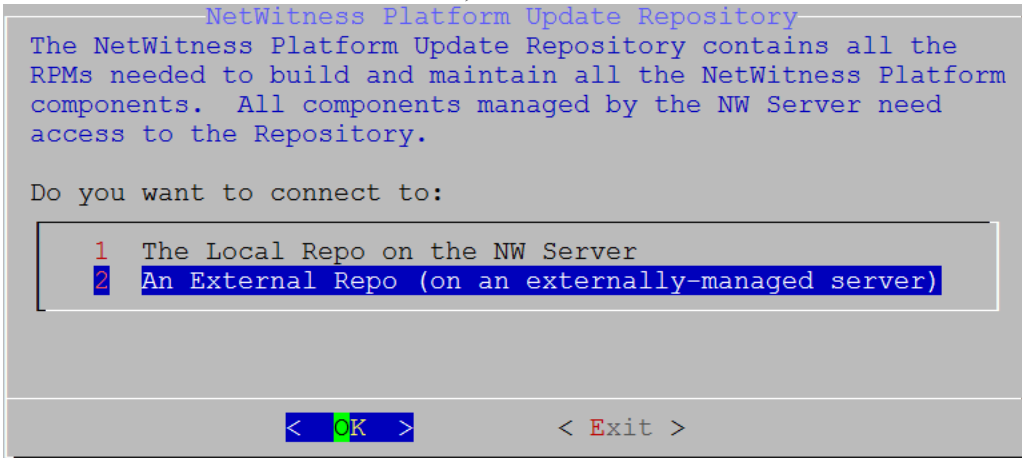
14. Seleccione el mismo repositorio que seleccionó cuando instaló el host del servidor de NW para todos los hosts.



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)** en el programa de instalación, asegúrese de que estén conectados los medios adecuados al host (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación) desde los cuales puede instalar NetWitness Platform 11.2.0.0.

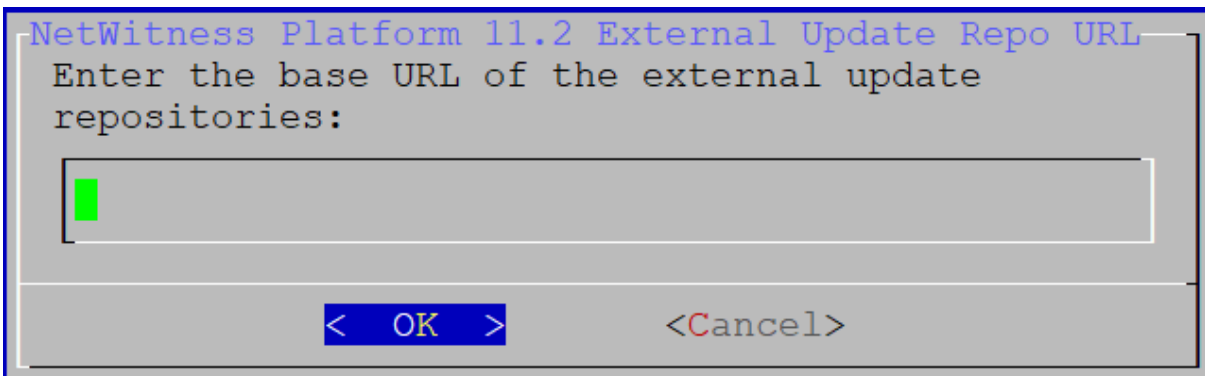
- Use las flechas hacia abajo y hacia arriba para seleccionar **2 Un repositorio externo (en un servidor administrado externamente)**.



Se muestra el indicador **URL de repositorio de actualización externo**.

Consulte [Apéndice B. Crear un repositorio externo](#) para obtener instrucciones sobre cómo configurar un repositorio externo. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

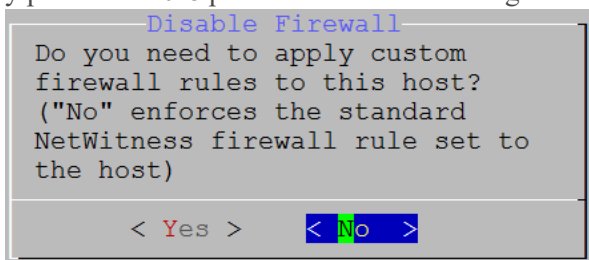
- Ingrese la dirección URL base del repositorio externo de NetWitness Platform que aparece en las instrucciones que se siguieron en el [Apéndice B. Crear un repositorio externo](#) (por ejemplo, <http://testserver/netwitness-repo>) y haga clic en **Aceptar**.



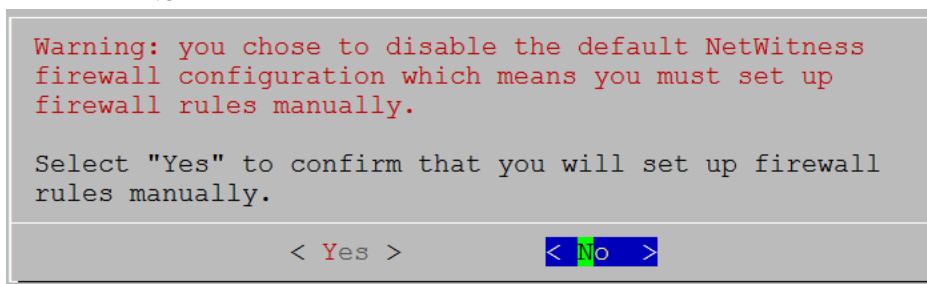
Se muestra el indicador **Deshabilitar** o usar la configuración estándar del **firewall**.

- 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.

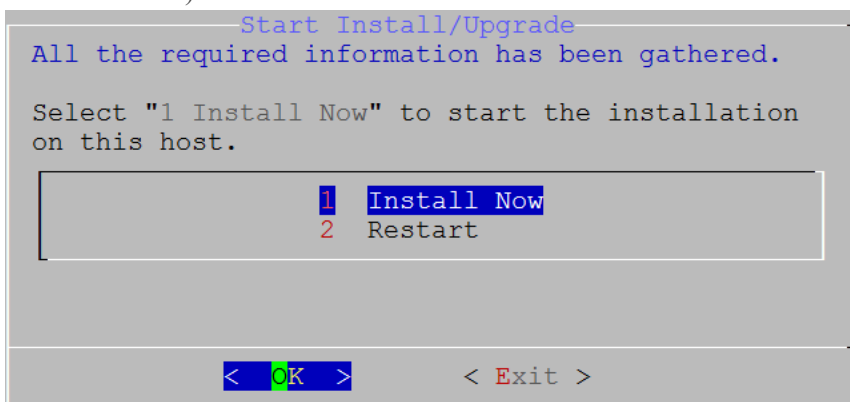


- Si selecciona **Sí**, confirma su selección. Si desea usar la configuración del firewall estándar, seleccione **No**.



Se muestra el indicador **Iniciar instalación/actualización**.

18. Presione **Intro** para instalar 11.2.0.0 en el servidor que no es de NW (el valor predeterminado es **Instalar ahora**).



Cuando se muestra **Instalación completa**, ya actualizó el servidor de NW 10.6.6 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)
```

Tarea 2: Instalar 11.2 en otros hosts de componentes

Para un servicio funcional, realice las siguientes tareas en un host de servidor que no es de NW.

- Instale la plataforma ambiental de 11.2.0.0.
 - Aplique los archivos RPM 11.2.0.0 al servicio desde el repositorio de actualizaciones del servidor de NW.
1. Implemente OVA 11.2.0.0.
 2. 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 [\(Opcional\) Tarea 1: Volver a configurar servidores DNS después de 11.2](#) 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 Platform** en el paso 12 (los servidores DNS no están definidos, de modo que el sistema no puede acceder al repositorio externo).

```
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
```

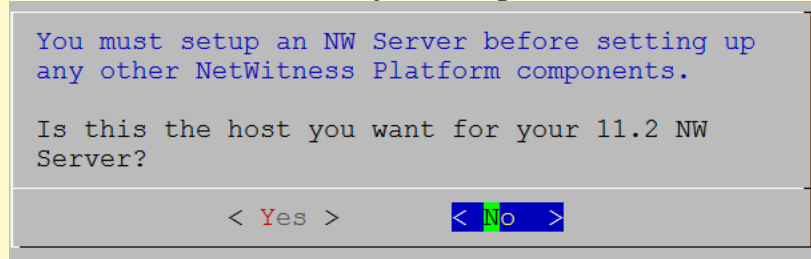
92%

<Accept >

<Decline>

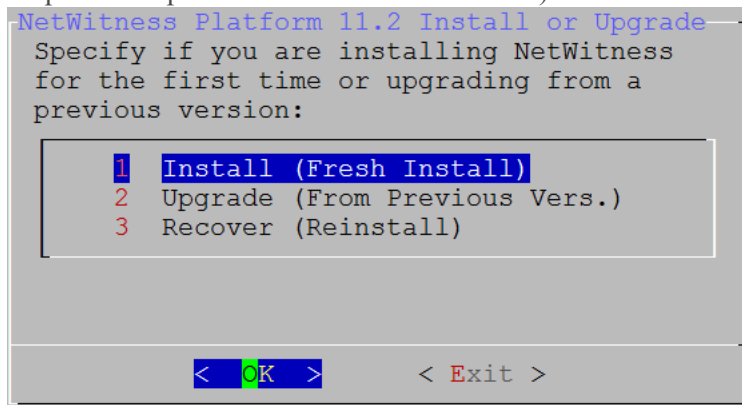
3. Use la tecla de tabulación para ir a **Aceptar** y presione Intro. Se muestra el indicador **¿Es este el host que desea para el servidor de NW 11.2?**.

Precaución: Si elige el host incorrecto para el servidor de NW y completa la instalación, debe reiniciar el programa de instalación y completar los pasos del 2 al 14 de [Tarea 1: Instalar 11.2.0.0 en el host del servidor de NW](#) para corregir este error.

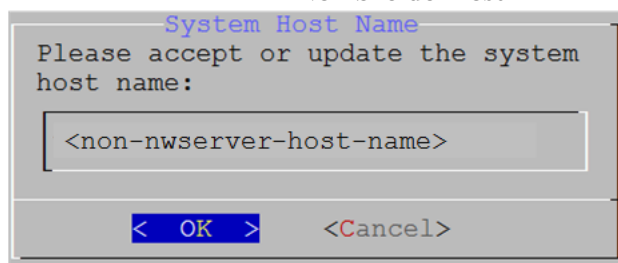


4. Presione **Intro** (No).

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



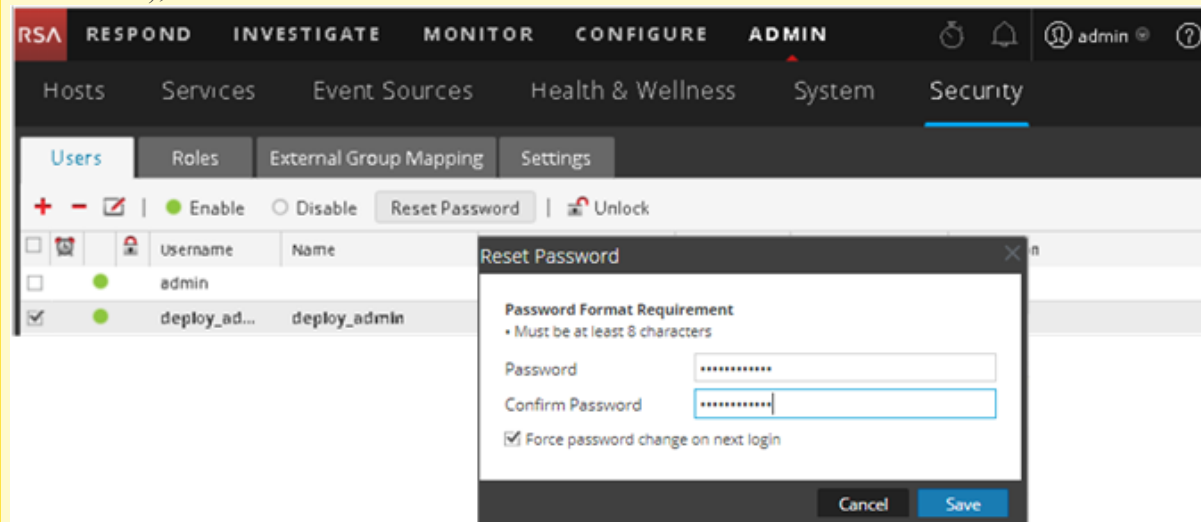
5. Presione Intro. La opción **Instalar (instalación nueva)** está seleccionada de manera predeterminada. Se muestra el indicador **Nombre del host**.



Precaución: Si incluye “.” en un nombre de host, el nombre de host también debe incluir un nombre de dominio válido.

6. Si desea mantener este nombre, presione **Intro**. Si desea cambiar este nombre, edítelo, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**

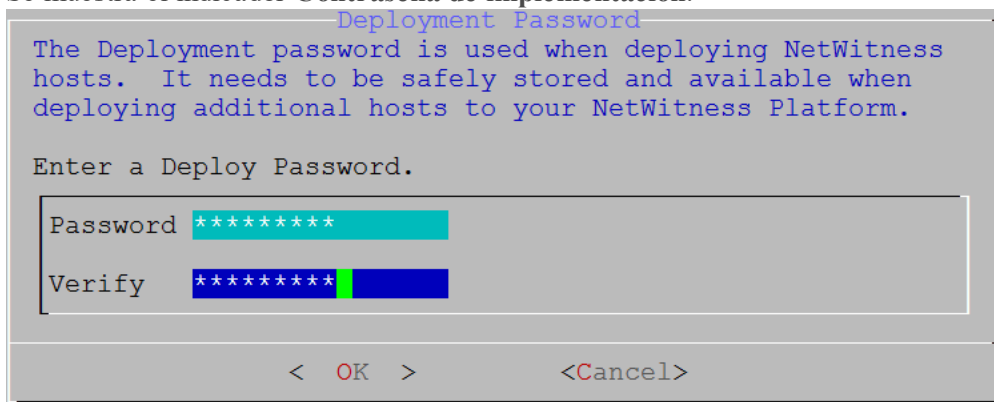
Precaución: Si cambia la contraseña de usuario **deploy_admin** en la interfaz del usuario de NetWitness Platform (**ADMIN>Seguridad >Seleccionar deploy-admin - Restablecer contraseña**),



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 instalar cualquier host nuevo que no es de servidor de NW.
4. 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.
5. Escribir la contraseña porque podría necesitarla para consultarla más adelante en la instalación.

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

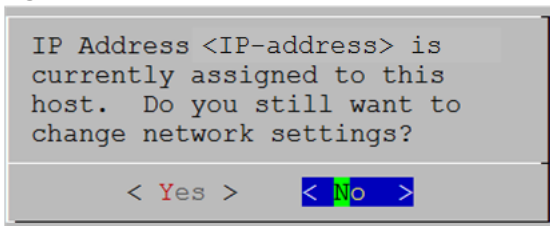


Nota: Debe usar la misma contraseña de implementación que usó cuando instaló el servidor de NW.

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**.

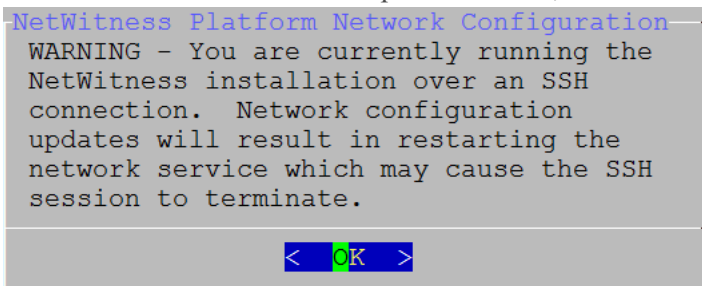
Se muestra uno de los siguientes indicadores condicionales.

- 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.

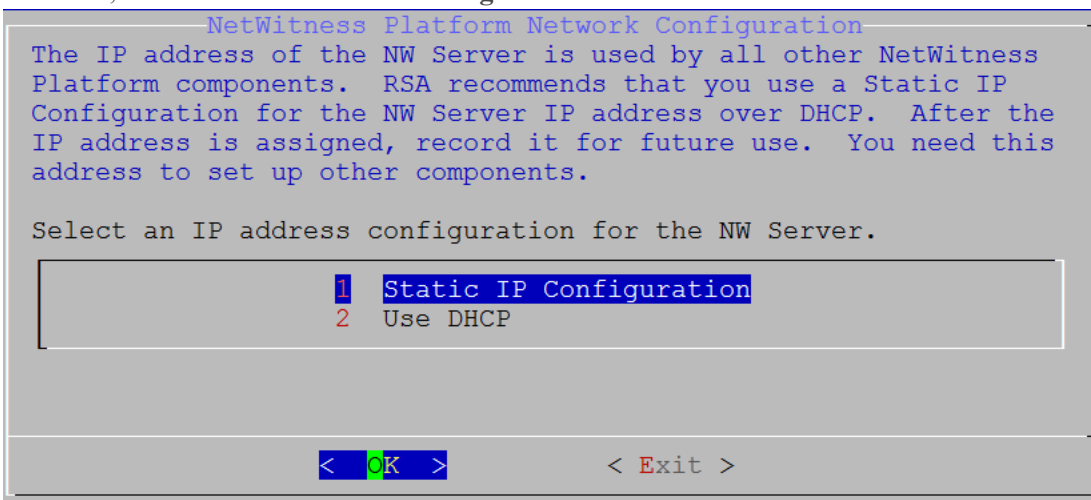
- Si está usando una conexión de protocolo SSH, se muestra la siguiente advertencia.



Presione **Intro** para cerrar el indicador de advertencia.

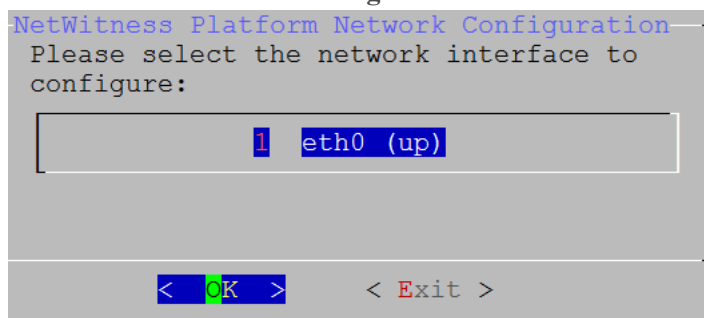
Nota: Si se conecta directamente desde la consola del host, no se mostrará la advertencia mencionada anteriormente.

- 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 red**.



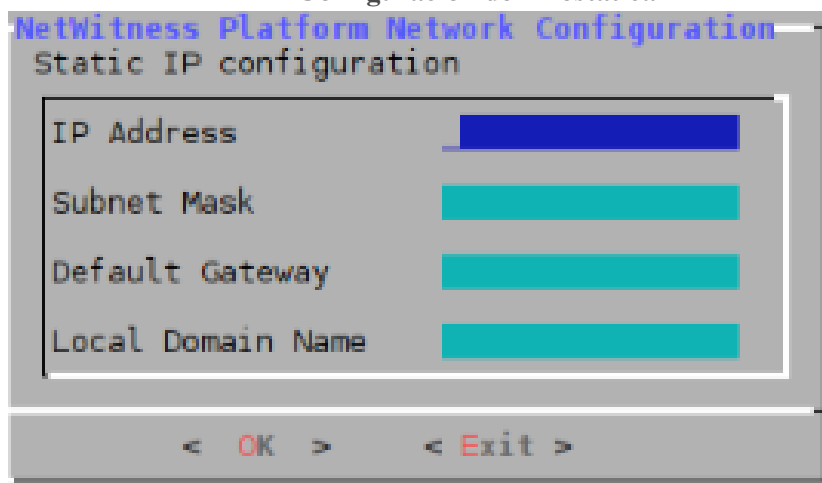
8. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para usar **Dirección IP estática**. Si desea usar **DHCP**, use la flecha hacia abajo para desplazarse hasta **2 Usar DHCP** y presione **Intro**.

Se muestra el indicador **Configuración de red**.



9. 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**.

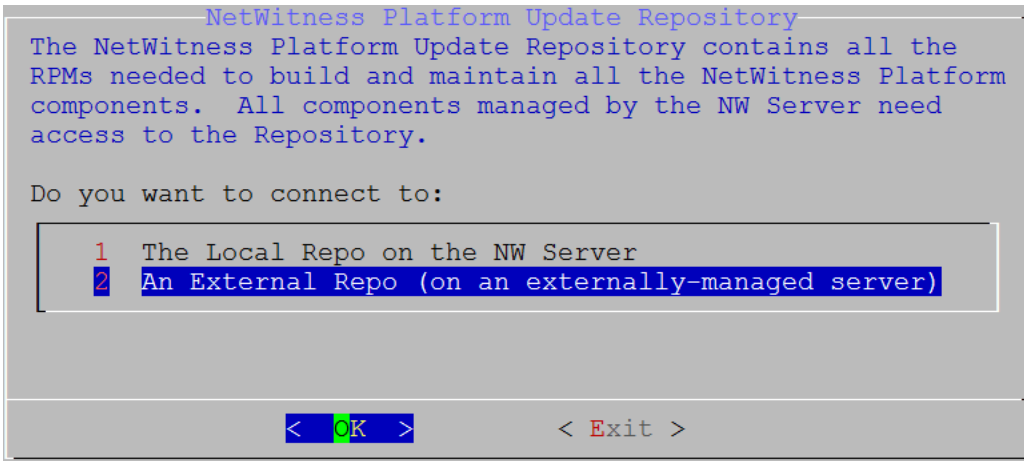


10. Escriba los valores de configuración (con la flecha hacia abajo para desplazarse de un campo a otro), use la tecla de tabulación para ir a **Aceptar** y presione **Intro**. Si no completa todos los campos obligatorios, se muestra un mensaje de error `All fields are required` (los campos **Servidor 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 `Invalid <field-name> .`

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**.

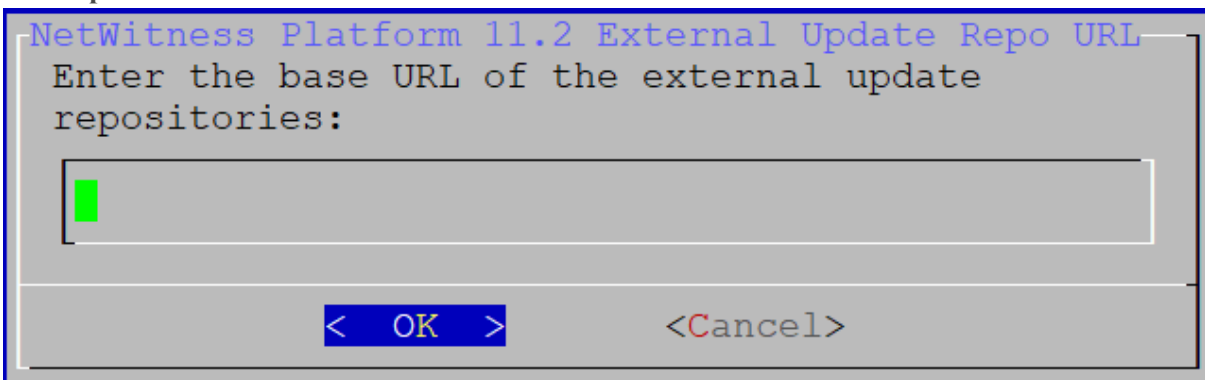
11. Use las flechas hacia abajo y hacia arriba para seleccionar **2 Un repositorio externo (en un servidor administrado externamente)**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.



Se muestra el indicador **URL de repositorio de actualización externo**.

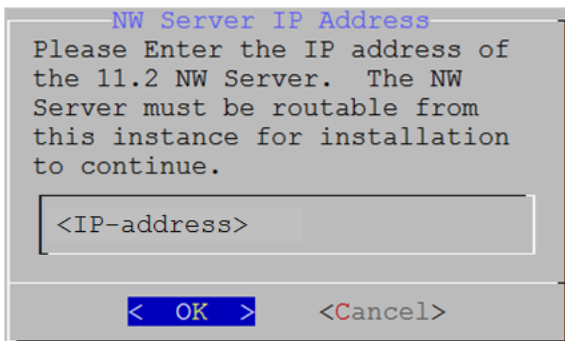
Los repositorios otorgan acceso a las actualizaciones de RSA y a las actualizaciones de CentOS.

12. Ingrese la URL base del repositorio externo de NetWitness Platform que se usó para configurar el servidor de NW en la sección anterior (por ejemplo, **http://testserver/netwitness-repo**) y haga clic en **Aceptar**.



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

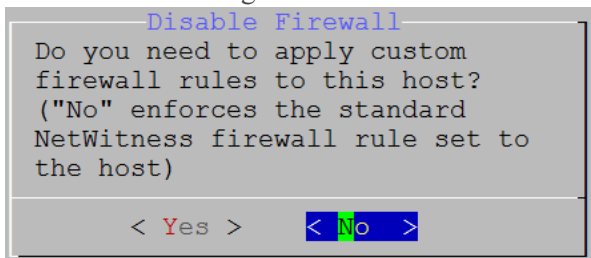
13. Escriba la dirección IP del servidor de NW, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.



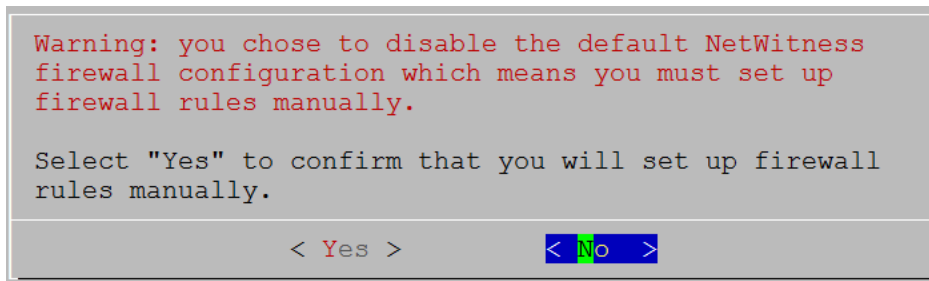
Se muestra el indicador de **deshabilitación** o uso de la configuración del **firewall** estándar.

14. 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.



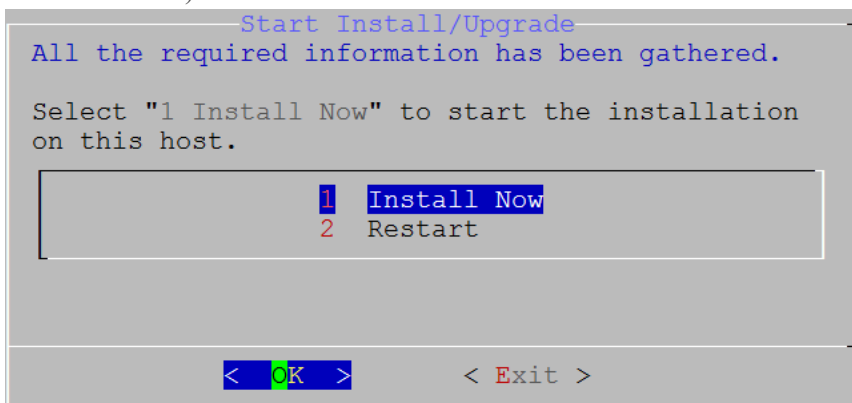
- Si selecciona **Sí**, confirme su selección.



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

Se muestra el indicador **Iniciar instalación**.

15. Presione **Intro** para instalar 11.2.0.0 en el servidor que no es de NW (el valor predeterminado es **Instalar ahora**).




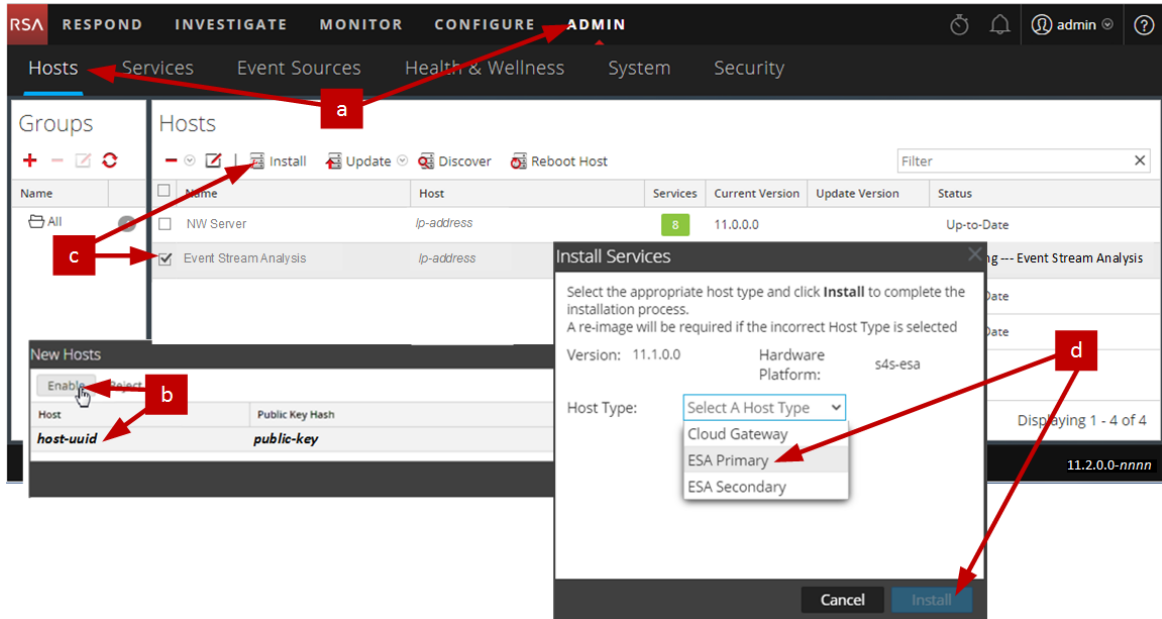
Cuando se muestra **Instalación completa**, tiene un host genérico con un sistema operativo compatible con NetWitness Platform 11.2.0.0.

16. Instale un servicio de componentes en el host de servidor que no es de NW.
 - 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. Seleccione el host en el cuadro de diálogo **Nuevos hosts** y 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 (por ejemplo, **Event Stream Analysis**) y haga clic en  **Install**.
- Se muestra el cuadro de diálogo **Instalar servicios**.
- d. Seleccione el tipo de host adecuado (por ejemplo, **ESA primario**) en **Tipo de host** y haga clic en **Instalar**.



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

- 17. Complete los requisitos de licencia para los servicios instalados.
 Consulte la *Guía de administración de licencia de NetWitness Platform 11.2* para obtener más información. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
- 18. Complete los pasos del 1 al 16 para el resto de los componentes que no son de servidor de NW de NetWitness Platform.

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 Platform maneja su desencapsulado.

Paso 5. Tareas posteriores a la instalación

En este tema se enumeran las tareas que debe completar después de instalar 11.2.

- General
- RSA NetWitness® Endpoint Insights
- Habilitación de FIPS
- RSA NetWitness User Entity Behavior Analytics (UEBA)

General

(Opcional) Tarea 1: Volver a configurar servidores DNS después de 11.2

En NetWitness Server, realice los siguientes pasos para volver a configurar los servidores DNS en NetWitness Platform 11.2.

1. Inicie sesión en el host del servidor con sus credenciales `root`.
2. Edite el archivo `/etc/netwitness/platform/resolv.dnsmasq`:
 - a. Reemplace la dirección IP correspondiente a `nameserver`.
Si es necesario reemplazar ambos servidores DNS, reemplace las entradas IP para ambos hosts por direcciones válidas.

En el siguiente ejemplo se muestran dos entradas de DNS modificadas.

```
root@nw11sas5:~#
# Generated by NetworkManager
nameserver nn.nn.55.15
nameserver nn.nn.55.17
search netwitness.local
```

En el siguiente ejemplo se muestran los nuevos valores de DNS.

```
root@nw11sas5:~#
# Generated by NetworkManager
nameserver nn.nn.44.37
nameserver nn.nn.66.17
search netwitness.local
```

- b. Guarde el archivo `/etc/netwitness/platform/resolv.dnsmasq`.
- c. Reinicie el DNS interno ejecutando el siguiente comando:
`systemctl restart dnsmasq`

RSA NetWitness Endpoint Insights



(Opcional) Tarea 2: Instalar Endpoint Hybrid o Endpoint Log Hybrid

Debe instalar uno de los siguientes servicios para instalar NetWitness Platform Endpoint Insights en la implementación:

- Endpoint Hybrid
- Endpoint Log Hybrid

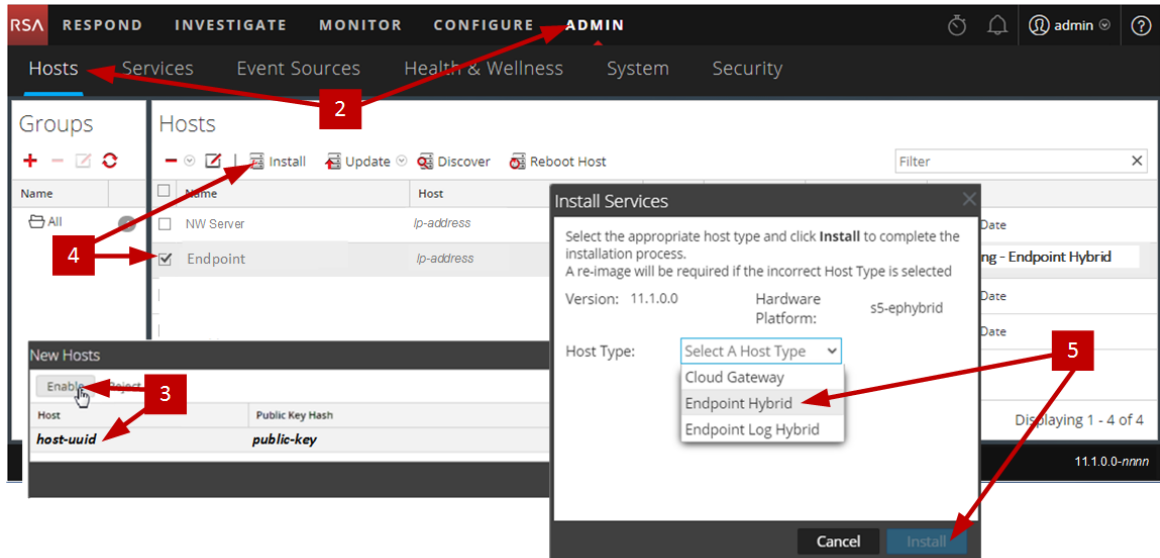
Precaución: Solamente puede instalar una instancia de los servicios anteriores en la implementación.

Nota: Debe instalar Endpoint Hybrid o Endpoint Log Hybrid en el dispositivo serie 5 o Dell R730.

1. Complete los pasos del 1 al 14 para el host físico o los pasos del 1 al 15 para los hosts virtuales como se describe en “Tarea 2: Instalar 11.2 en otros hosts de componentes” en la sección “Tareas de instalación” de la *Guía de instalación de hosts físicos de NetWitness Platform para la versión 11.2*. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
2. 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.
3. Seleccione el host en el cuadro de diálogo **Nuevos hosts** y haga clic en **Habilitar**.
El cuadro de diálogo Nuevos hosts se cierra y el host se muestra en la vista Hosts.
4. Seleccione ese host en la vista **Hosts** (por ejemplo, **Endpoint**) y haga clic en  **Install** .
Se muestra el cuadro de diálogo Instalar servicios.

5. Seleccione el servicio adecuado, ya sea **Endpoint Hybrid** o **Endpoint Log Hybrid**, y haga clic en **Instalar**.

Endpoint Hybrid se usa como un ejemplo en la siguiente captura de pantalla.



6. Asegúrese de que todos los servicios Endpoint Hybrid o Endpoint Log Hybrid estén en ejecución.
7. Configure el reenvío de metadatos de terminales.
Consulte la *Guía de configuración de Endpoint Insights* para obtener instrucciones sobre cómo configurar el reenvío de metadatos de terminales. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
8. Instale el agente de Endpoint Insights.
Consulte la *Guía de instalación de agentes de Endpoint Insights* para obtener instrucciones detalladas sobre cómo instalar el agente. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Habilitación de FIPS

(Opcional) Tarea 3: Habilitar el modo FIPS

El estándar de procesamiento de información federal (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 acerca de cómo habilitar FIPS para estos servicios, consulte el tema “Activar o desactivar FIPS” en 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.

NetWitness User Entity Behavior Analytics (UEBA)

(Opcional) Tarea 3: Instalar NetWitness UEBA

Requisito previo: Aumentar el almacenamiento para la implementación virtual

De manera predeterminada, las máquinas virtuales se implementan con aproximadamente 104 GB en el montaje de almacenamiento. Para instalar NetWitness UEBA, debe aumentar el espacio de almacenamiento en el ambiente virtual a al menos 800 GB.

Instalar NetWitness UEBA

Para configurar NetWitness UEBA en NetWitness Platform 11.2, debe instalar y configurar el servicio NetWitness UEBA.



En el siguiente procedimiento se muestra cómo instalar el servicio NetWitness UEBA en un tipo de host de NetWitness UEBA y cómo configurar el servicio.

1. Complete los pasos del 1 al 14 para el host físico o los pasos del 1 al 15 para los hosts virtuales como se describe en “Tarea 2: Instalar 11.2 en otros hosts de componentes” en la sección “Tareas de instalación” de la *Guía de instalación de hosts físicos de NetWitness Platform para la versión 11.2*. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

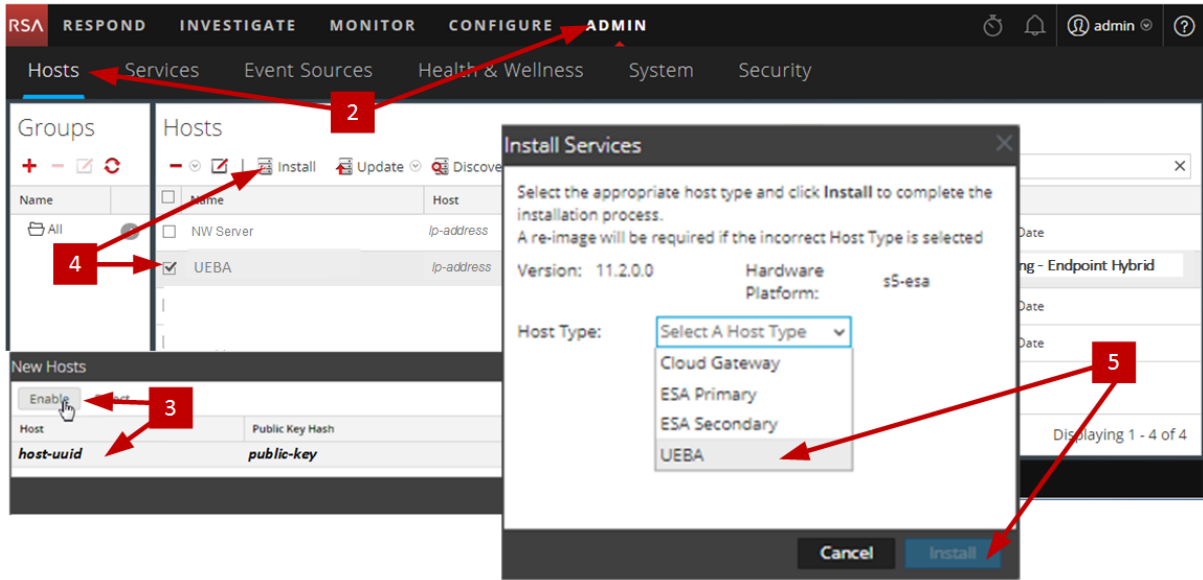
Nota: La contraseña de la interfaz del usuario del servidor Web de Kibana y Ariflow es la misma que la contraseña de administrador de la implementación. Asegúrese de registrar esta contraseña y de guardarla en un lugar seguro.

2. Inicie sesión en NetWitness Platform y vaya a **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.

3. Seleccione el host en el cuadro de diálogo **Nuevos hosts** y haga clic en **Habilitar**. El cuadro de diálogo Nuevos hosts se cierra y el host se muestra en la vista Hosts.
4. Seleccione ese host en la vista **Hosts** (por ejemplo, **UEBA**) y haga clic en  **Install** . Se muestra el cuadro de diálogo Instalar servicios.

5. Seleccione el tipo de host **UEBA** y haga clic en **Instalar**.



6. Asegúrese de que el servicio UEBA esté en ejecución.

7. Complete los requisitos de licencia para NetWitness UEBA.

Consulte la *Guía de administración de licencia de NetWitness Platform 11.2* para obtener más información. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Nota: NetWitness Platform es compatible con la licencia de User and Entity Behavior Analytics (UEBA). Esta licencia se utiliza en función de la cantidad de usuarios. La licencia de prueba de uso inmediato es una licencia de prueba de 90 días. En el caso de las licencias de UEBA, el período de prueba de 90 días comienza desde el momento en que el servicio UEBA se implementa en el producto NetWitness Platform.


8. Configure NetWitness UEBA.

Debe configurar un origen de datos (Broker o Concentrator), la fecha de inicio de la recopilación de datos históricos y los esquemas de datos.

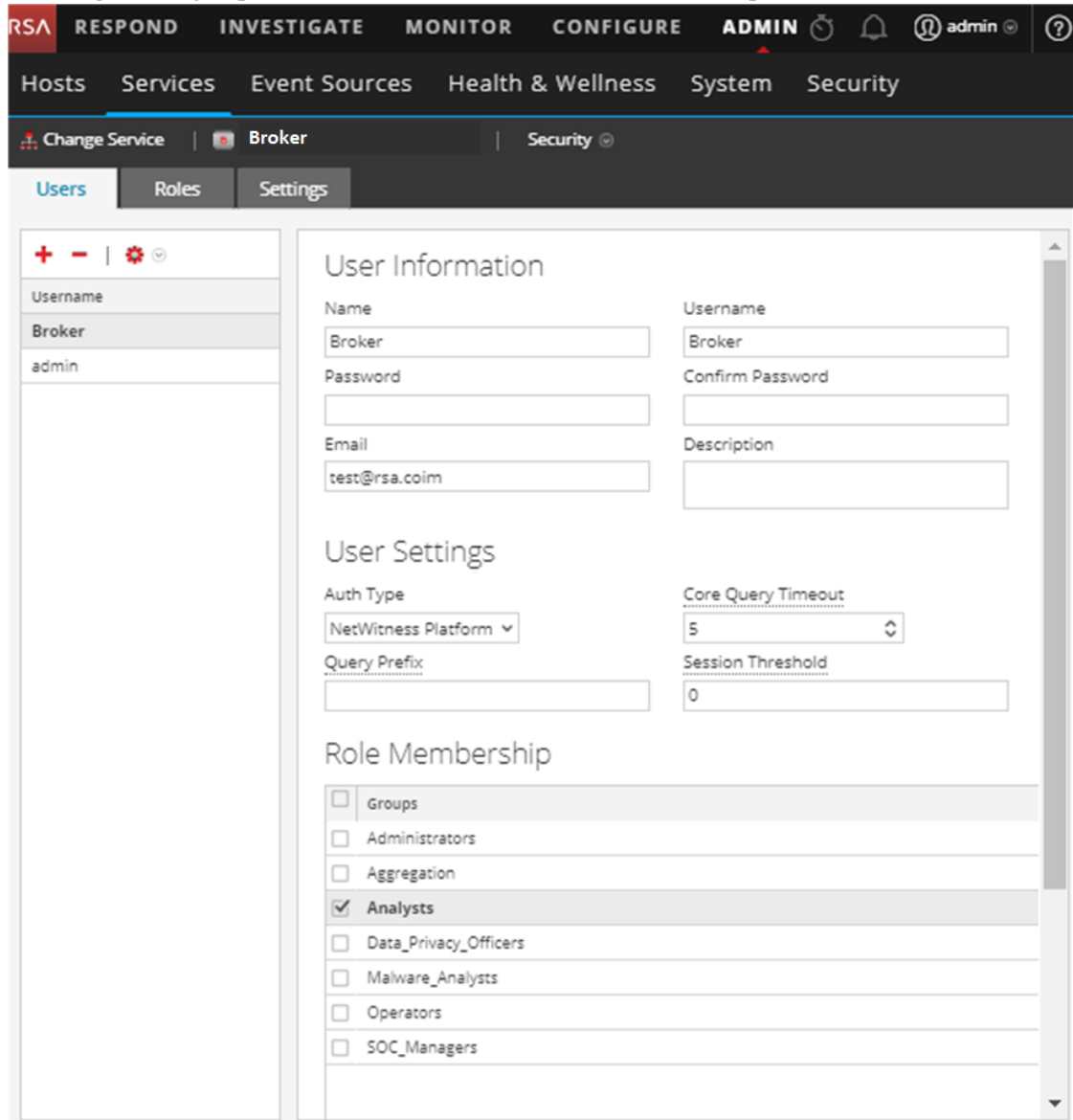
IMPORTANTE: Si la implementación tiene varios Concentrators, RSA recomienda asignar el Broker en la parte superior de la jerarquía de implementación para el origen de datos NetWitness UEBA.

- a. Determine la primera fecha en la NWDB del esquema de datos que planea elegir (AUTHENTICATION, FILE, ACTIVE_DIRECTORY o cualquier combinación de estos esquemas) para especificar en `startTime` en el paso c. Si planea especificar varios esquemas, utilice la primera fecha entre todos los esquemas. Si no está seguro del esquema de datos que debe elegir, puede especificar los tres esquemas de datos (es decir, AUTHENTICATION, FILE y ACTIVE_DIRECTORY) para que UEBA ajuste los modelos con los que puede ser compatible en función de los registros de Windows disponibles. Puede utilizar uno de los siguientes métodos para determinar la fecha del origen de datos.

- Utilice la fecha de retención de datos (es decir, si la duración de la retención de datos es 48 horas, `startTime = <48 horas antes de la hora actual>`).
 - Busque la primera fecha en la NWDB.
- b. Cree una cuenta de usuario para el origen de datos (Broker o Concentrator) para autenticarse en el origen de datos.
- i. Inicie sesión en NetWitness Platform.
 - ii. Vaya a **Administrar > Servicios**.
 - iii. Localice el servicio del origen de datos (Broker o Concentrator).

Seleccione ese servicio y elija  (Acciones) > **Ver > Seguridad**.
 - iv. Cree un nuevo usuario y asígnele la función “Analistas”.

En el siguiente ejemplo se muestra una cuenta de usuario creada para un Broker.



c. Acceda mediante el protocolo SSH al host del servidor de NetWitness UEBA.

d. Ejecute los siguientes comandos.

```
/opt/rsa/saTools/ueba-server-config -u <user> -p <password> -h <host> -o <type> -t <startTime> -s <schemas> -v
```

Donde:

Argumento	Variable	Descripción
-u	<user>	Nombre de usuario de las credenciales para la instancia de Broker o Concentrator que está utilizando como origen de datos.
-p	<password>	<p>Contraseña de las credenciales para la instancia de Broker o Concentrator que está utilizando como origen de datos. Los siguientes caracteres especiales son compatibles en una contraseña.</p> <pre>!"#\$%&()*+,-.:;<=>?@[\\]^_`{ }</pre> <p>Si desea incluir uno o más caracteres especiales, debe delimitar la contraseña con un apóstrofo; por ejemplo:</p> <pre>sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '! "UHfz?@ExMn#\$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY' -o broker -v</pre>
-h	<host>	Dirección IP del Broker o el Concentrator que se utilizan como orígenes de datos. Actualmente, solo es compatible un origen de datos.
-o	<type>	Tipo del host del origen de datos (broker o concentrator).
-t	<startTime>	<p>Hora de inicio histórica a partir de la cual se comienzan a recopilar datos del origen de datos en formato AAAA-MM-DDTHH-MM-SSZ (por ejemplo, 2018-08-15T00:00:00Z).</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Nota: El script interpreta la hora que ingresa como UTC (hora universal coordinada) y no la ajusta a la zona horaria local.</p> </div>

Argumento	Variable	Descripción
-s	<schemas>	Matriz de esquemas de datos. Si desea especificar varios esquemas, utilice un espacio para separar cada esquema (por ejemplo, 'AUTHENTICATION FILE ACTIVE_DIRECTORY'). Nota: Si especifica los tres esquemas de datos (es decir, AUTHENTICATION, FILE y ACTIVE_DIRECTORY), UEBA ajusta los modelos con los que puede ser compatible en función de los registros de Windows disponibles.
-v		Modo detallado.

9. Complete la configuración de NetWitness UEBA de acuerdo con las necesidades de la organización. Consulte la *Guía del usuario de RSA NetWitness UEBA* para obtener más información. Vaya a la [Tabla maestra de contenido](#) para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

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	<p>La interfaz de la línea de comandos (CLI) muestra: “La operación de coordinación falló.”</p> <pre>Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log</pre>
Causa	<p>Ingresó la contraseña de <code>deploy_admin</code> incorrecta en <code>nwsetup-tui</code>.</p>
Solución	<p>Recupere su contraseña de <code>deploy_admin</code>.</p> <ol style="list-style-type: none"> 1. Acceda mediante el protocolo SSH al host del servidor de NW. <pre>security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password</pre> <p>Acceda mediante el protocolo SSH al host que falló.</p> 2. Vuelva a ejecutar <code>nwsetup-tui</code> con el uso de la contraseña de <code>deploy_admin</code> correcta.
Mensaje de error	<pre>ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service</pre>
Causa	<p>NetWitness Platform ve el servicio de administración de servicios (SMS) como inactivo después de la actualización correcta aunque el servicio esté en ejecución.</p>
Solución	<p>Reinicie el servicio SMS.</p> <pre>systemctl restart rsa-sms</pre>
Mensaje de error	<p>Usted recibe un mensaje en la interfaz del usuario que le solicita reiniciar el host después de actualizar y reiniciar el host offline.</p> 
Causa	<p>No puede utilizar la CLI para reiniciar el host. Debe utilizar la interfaz del usuario.</p>
Solución	<p>Reinicie el host en la vista Host de la interfaz del usuario.</p>

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	<p>Respalde los errores ocasionados por la configuración del atributo <code>immutable</code>. Este es un ejemplo de un error que puede aparecer:</p> <pre>Backing up NetWitness Config (/etc/netwitness) files from: saserver1 WARNING: Errors occurred while backing up NetWitness Configuration files. Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1</pre>
Causa	Si tiene algún archivo con la marca <code>immutable</code> 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 <code>immutable</code> configurada, ejecute el siguiente comando para quitar la configuración de <code>immutable</code> de los archivos: <code>chattr -i <filename></code>

Error	<p>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: <code>/etc/sysconfig/network-scripts/ifcfg-em1</code> Verifique el contenido de <code>/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt</code></p>
Causa	<p>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.</p>
Solución	<p>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 <code><hostname>-<hostip>-network.info.txt</code> y debe contener las siguientes entradas:</p> <pre> 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 </pre>

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	<ol style="list-style-type: none"> 1. Acceda mediante el protocolo SSH al host de ESA primario e inicie sesión. 2. En el archivo <code>/opt/rsa/esa/conf/wrapper.conf</code>, reemplace la siguiente línea: <code>wrapper.java.additional.5=-</code> <code>Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore</code> por: <code>wrapper.java.additional.5=-</code> <code>Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore</code> 3. Ejecute el siguiente comando para reiniciar ESA. <code>systemctl restart rsa-nw-esa-server</code> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Nota: Si tiene múltiples hosts de ESA y encuentra ese mismo problema, repita los pasos 1 al 3 en cada host de ESA secundario.</p> </div>

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	<code><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.</code>
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 <i>Guía de configuración de la recopilación de registros</i> . Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Mensaje de error	<code><timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
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 <i>Guía de configuración de la recopilación de registros</i> . 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 <i>Guía de configuración de la recopilación de registros</i> . 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	<p>Después de la actualización, observa que los registros de auditoría no se reenvían a la configuración de auditoría global definida</p> <p>o</p> <p>El siguiente mensaje se muestra en <code>sa.log</code>. <code>Syslog Configuration migration failed. Restart jetty service to fix this issue</code></p>
Causa	<p>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.</p>
Solución	<ol style="list-style-type: none"> 1. Acceda mediante el protocolo SSH al servidor de NW. 2. Ejecute el siguiente comando. <code>orchestration-cli-client --update-admin-node</code>

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	<ol style="list-style-type: none"> 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.
Causa	<p>Verá el siguiente mensaje en <code>orchestration-server.log</code>. <code>''file' _virtual_ returned False: cannot import name HASHES''</code></p> <p>Salt minion se puede haber actualizado y nunca se reinició en el host fallido que no es de servidor de NW</p>
Solución	<ol style="list-style-type: none"> 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. <code>systemctl unmask salt-minion</code> <code>systemctl restart salt-minion</code> 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	<code><timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [><existing-GB] is less than the required space [<required-GB>]</code>
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 <i>Guía de configuración de Reporting Engine</i> 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	<p>Realice los siguientes pasos para quitar el servicio de NetWitness UEBA adicional.</p> <ol style="list-style-type: none"> 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. <pre># 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</pre> 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): <pre># orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output></pre> 4. Ejecute el siguiente comando para actualizar el nodo 0 con el fin de restaurar NGINX: <pre># orchestration-cli-client --update-admin-node</pre> 5. Inicie sesión en NetWitness Platform, vaya a ADMINISTRAR > Hosts y quite el host de NetWitness UEBA extra.

Apéndice B. 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
fineserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11	1.3M
httpd-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
1.1	29/11/2018	Se agregó una nota acerca de la licencia de prueba de UEBA.	IDD

