RSA NETWITNESS® PLATFORM

Guía de instalación de hosts físicos

para la versión 11.2

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

febrero 2019

Contenido

Introducción

Las instrucciones de esta guía se aplican a los hosts físicos exclusivamente. Consulte la *Guía de instalación de hosts virtuales* de RSA *NetWitness Platform* para obtener instrucciones sobre cómo configurar hosts virtuales en 11.2.

Hardware compatible

Serie 4, serie 4S y serie 5.

Consulte las guías de configuración de hardware de RSA *NetWitness Platform* para obtener información detallada sobre cada tipo de serie (https://community.rsa.com/community/products/netwitness/hardware-setup-guides).

Especificaciones de hardware del host de Endpoint Hybrid o Endpoint Log Hybrid

Debe instalar los nuevos hosts de Endpoint Hybrid o Endpoint Log Hybrid en el hardware de la serie 5 (Dell R730) o de la serie 6 (Dell R740). Consulte "(Opcional) Tarea 2: Instalar Endpoint Hybrid o Endpoint Log Hybrid" en Tareas posteriores a la instalación para obtener instrucciones sobre cómo instalar Endpoint Hybrid y Endpoint Log Hybrid.

Especificaciones de hardware del host de RSA NetWitness UEBA

Debe instalar el nuevo host de NetWitness UEBA en el hardware de S5 (dispositivo Dell R630). Consulte "(Opcional) Tarea 3: Instalar NetWitness UEBA" en Tareas posteriores a la instalación para obtener instrucciones sobre cómo instalar NetWitness UEBA.

ESPECIFICACIONES DE LA SERIE 5 (DELL R630)

Especificación	Capacidad
Modelo	Dell PowerEdge R630xl
Tipo de procesador	Intel Xeon E5-2680v3
Velocidad del procesador	2.5 GHz
Caché	30 MB
N.º de cores	12
Cantidad de procesadores	2
Cantidad de hilos de ejecución	24
Memoria total	256 GB
Controladora de disco interna	Dell PERC H730
Controladora de disco externa	Dell PERC H830
Conectividad SAN (HBA): opcional	N/D

Especificación	Capacidad
Tarjeta de administración remota	iDRAC8 Enterprise
Unidades	Total: 6 unidades 2 discos duros de 1 TB, 2.5 in 4 discos duros de 2 TB, 2.5 in
Chasis	1U
Peso	18.4 kg (40.5 lb)
Tarjeta NIC*	Incorporada 2 de cobre de 10 Gb 2 de cobre de 10 Gb y 2 de 1 Gb (Están disponibles otras opciones)
Dimensiones	Alt.: 4.28 cm (1.68 in) x Anch.: 48.23 cm (18.98 in) x Prof.: 75.51 cm (29.72 in)
Alimentación	1100 W redundante
BTU/h	4,100 BTU/h (máx.)
Amperios (espec.)	1,100 W/220 V CA = 5 A
Consumo real en amperios (después del arranque)	2.1 amperios
Eventos por segundo (EPS)	100,000 EPS
Rendimiento	N/D

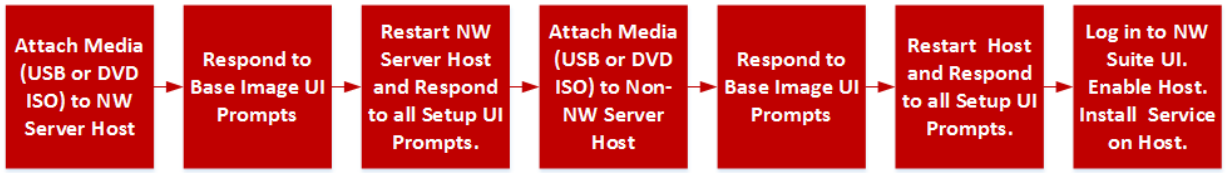
* Están disponibles opciones de tarjeta NIC para intercambiar con tarjeta secundaria incorporada o complementaria.

Almacenamiento de conexión externa

Si uno o más dispositivos de almacenamiento externo (por ejemplo, DAC o PowerVault) están conectados a un host físico, consulte las Guías de instalación de hardware para obtener información sobre cómo configurar este almacenamiento en RSA Link (https://community.rsa.com/community/products/netwitness/hardware-setup-guides).

Flujo de trabajo de instalación de hosts físicos

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



Póngase en contacto con el servicio al cliente

Consulte la página de contacto con el servicio al cliente de RSA (https://community.rsa.com/docs/DOC-1294) en RSA Link para obtener instrucciones sobre cómo obtener ayuda acerca de RSA NetWitness Platform 11.2.

Preparación para la instalación: Abrir los puertos del firewall

En el tema “Arquitectura y puertos de red” de la *RSA NetWitness® Platform Guía de implementación* se enumeran todos los puertos en una implementación. 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.

Tareas de instalación

Este tema contiene las tareas que debe realizar para instalar NetWitness Platform 11.2 en hosts físicos.

Existen dos tareas principales que debe realizar en el orden que se muestra.

Tarea 1: Instalar 11.2 en el host del servidor de NetWitness (servidor de NW)

Tarea 2: Instalar 11.2 en todos los demás hosts de componentes

Tarea 1: Instalar 11.2 en el host del servidor de NetWitness (servidor de NW)

Para el servidor de NW, esta tarea:

- Crea una imagen base.
- Configura el host del servidor de NW 11.2.

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

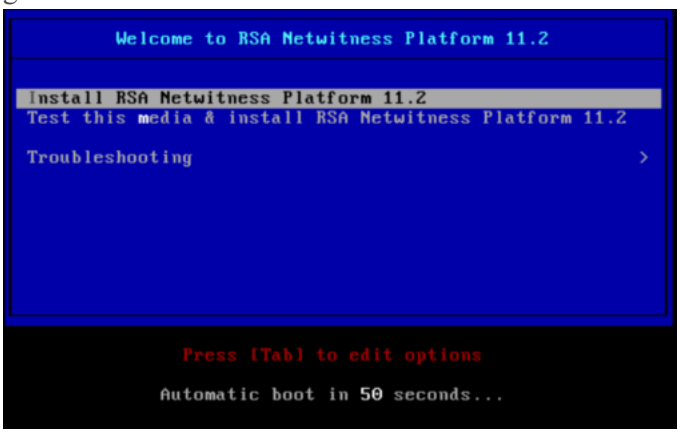
1. Cree una imagen base en el host:
   a. Conecte los medios (ISO) al host.
   Para obtener más información, consulte las *Instrucciones para una unidad de compilación de RSA NetWitness Platform*.
      - Instalaciones de hipervisor: Use la imagen ISO.
      - Medios físicos: Use el archivo ISO para crear medios de disco flash de arranque mediante la herramienta de instalación Universal Netboot (UNetbootin) u otra herramienta de digitalización adecuada. Consulte las *Instrucciones para una unidad de compilación de RSA NetWitness® Platform* para obtener información sobre cómo crear una unidad de compilación desde la imagen ISO. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
      - Instalaciones de iDRAC: El tipo de medios virtuales es:
        - **Disquete virtual** para discos flash mapeados.
        - **CD virtual** para dispositivos de medios ópticos o archivos ISO mapeados.

   b. Inicie sesión en el host y reinícielo.

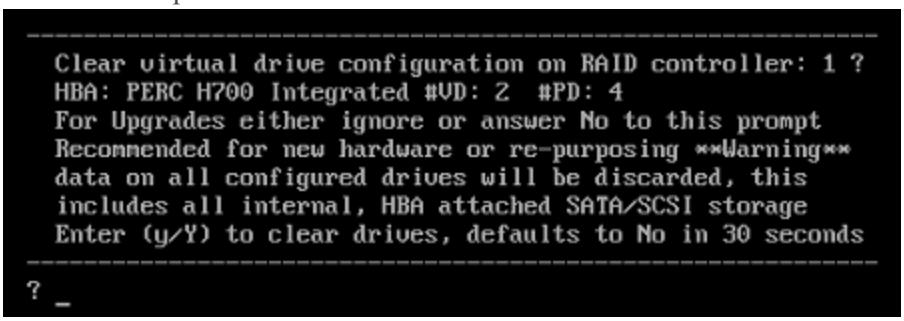
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

   c. Seleccione **F11 (menú de arranque)** durante el reinicio para seleccionar un dispositivo de arranque y arrancar desde los medios conectados.
   Después de algunas comprobaciones del sistema durante el arranque, se muestra el siguiente menú de instalación **Bienvenido a RSA NetWitness Platform 11.2**. Los gráficos del menú se

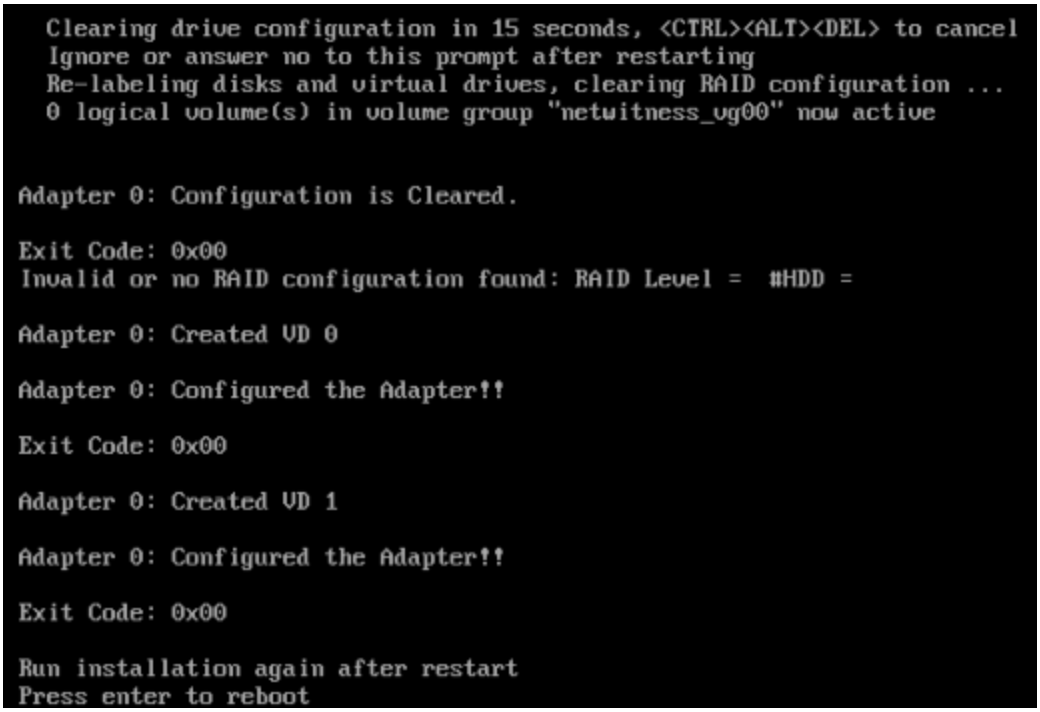
generarán de manera diferente si usa un medio flash USB físico.



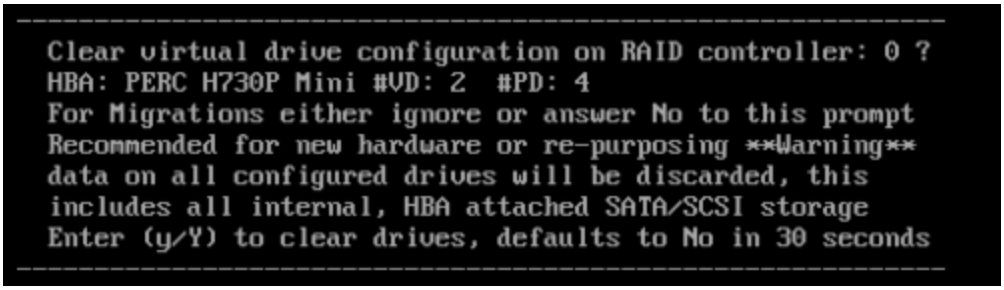
d. Seleccione **Instalar RSA Netwitness Platform 11.2** (selección predeterminada) y presione **Intro**.
El programa de instalación se ejecuta y se detiene en el indicador **Ingresar (s/S) para borrar las unidades** que le solicita formatear las unidades.



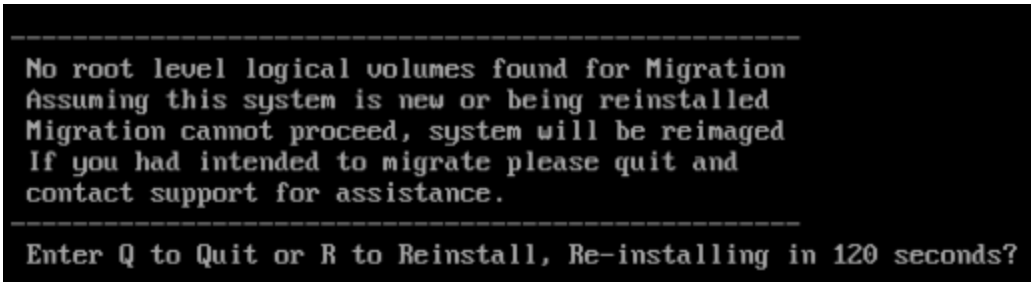
e. Escriba **S** para continuar.
La acción predeterminada es No, de modo que si pasa por alto el indicador, se seleccionará No en 30 segundos y las unidades no se borrarán. Se muestra el indicador **Presione Intro para reiniciar**.



f. Presione **Intro** para reiniciar el host.
El programa de instalación le vuelve a solicitar que borre las unidades.



g. Escriba **N** porque ya borró las unidades.
Se muestra el indicador **Ingresar Q (Salir) o R (Reinstalar)**.



h. Escriba **R** para instalar la imagen base.
El programa de instalación muestra los componentes a medida que se instalan, lo que varía según el dispositivo, y reinicia.

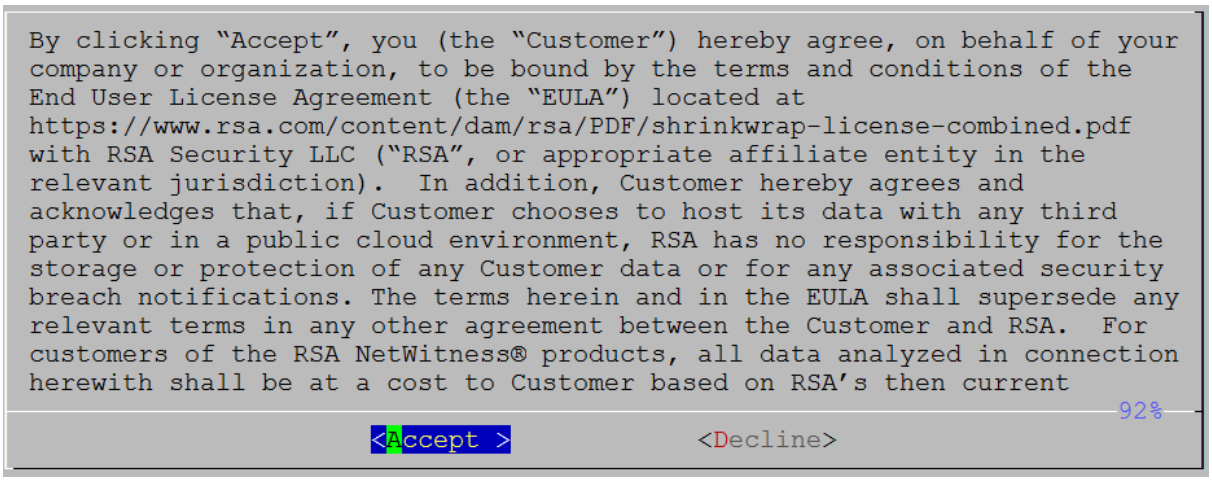
Precaución: No reinicie los medios conectados (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación).

i. Inicie sesión en el host con las credenciales `root` .

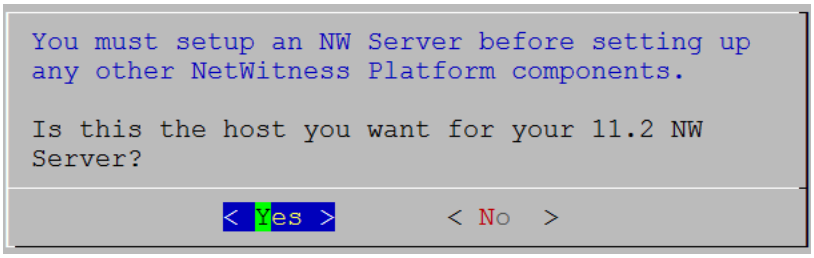
2. Ejecute el comando `nwsetup-tui` para configurar el host.

Esto inicia `nwsetup-tui` (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 los comandos y desde estos (como **<Sí>**, **<No>**, **<Aceptar>** y **<Cancelar>**). Presione **Intro** para registrar la respuesta de los comandos y pasar al siguiente indicador.
2.) El programa de instalación adopta la combinación de colores del escritorio o de la consola que se 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 el proceso (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 la configuración (`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).



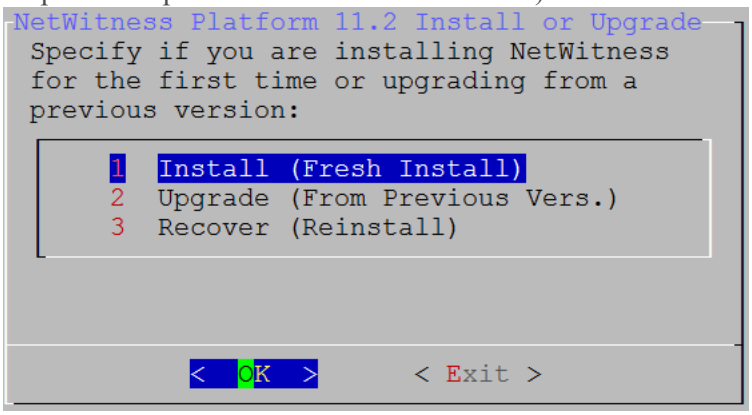
3. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador **¿Es este el host que desea para el servidor de NW 11.2?**.



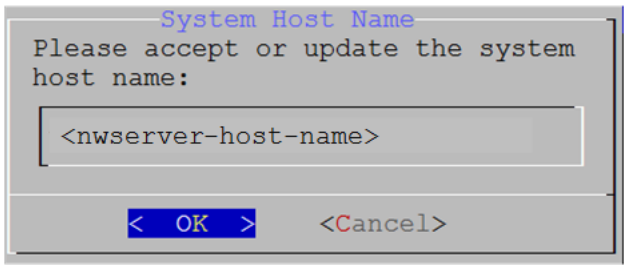
4. Use la tecla de tabulación para ir a **Sí** y presione **Intro**.
   Elija **No** si ya instaló 11.2 en el servidor de NW.

   Precaución: Si elige el host incorrecto para el servidor de NW y completa la configuración, debe reiniciar el programa de instalación y completar los pasos del 2 al 14 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).



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



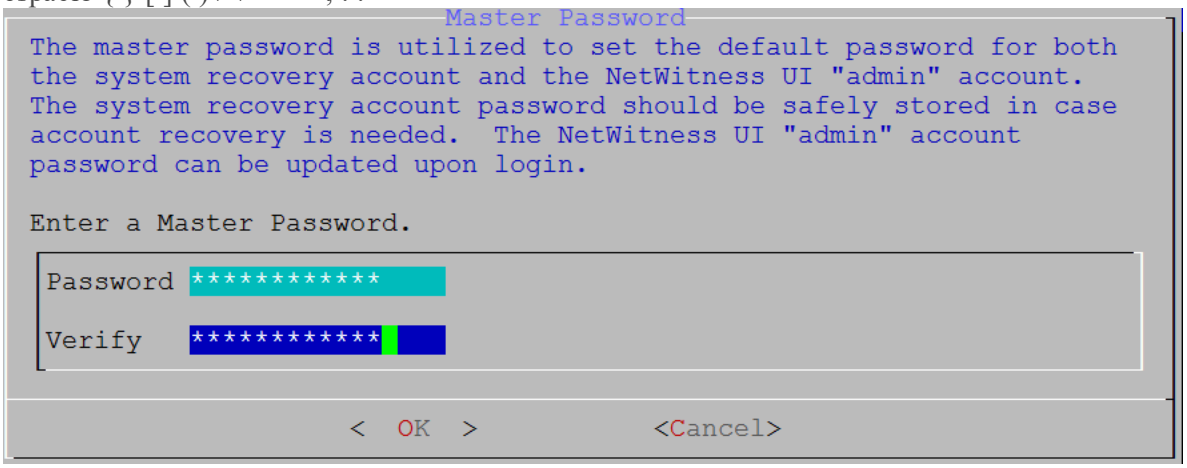
Precaución: Si incluye “.” en un nombre de host, el nombre de host también debe incluir un nombre de dominio válido.

Se muestra el indicador **Contraseña maestra**.

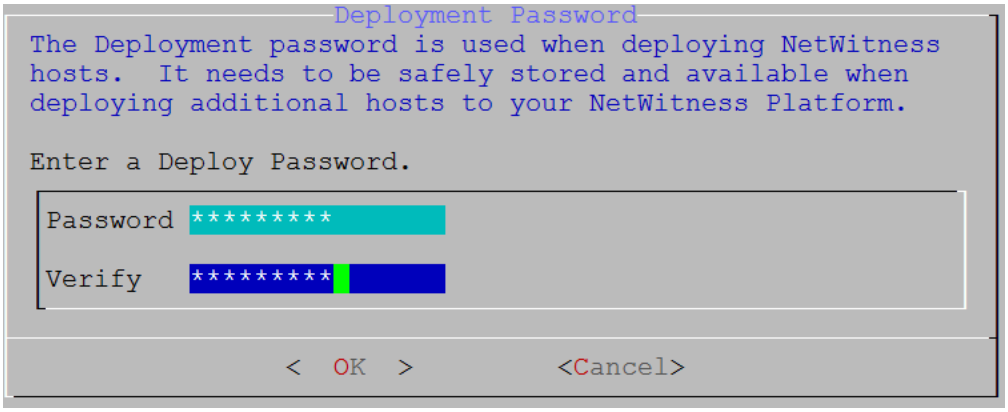
6. Presione **Intro** si desea mantener este nombre. Si no edita el nombre del host, use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para cambiarlo.
   Los caracteres de la siguiente lista son compatibles para Contraseña maestra y Contraseña de implementación:

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

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

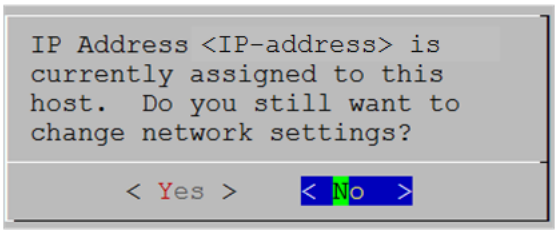


7. Escriba la **Contraseña**, use la flecha hacia abajo para desplazarse hasta **Verificar**, vuelva a escribir la contraseña, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador **Contraseña de implementación**.



8. 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.

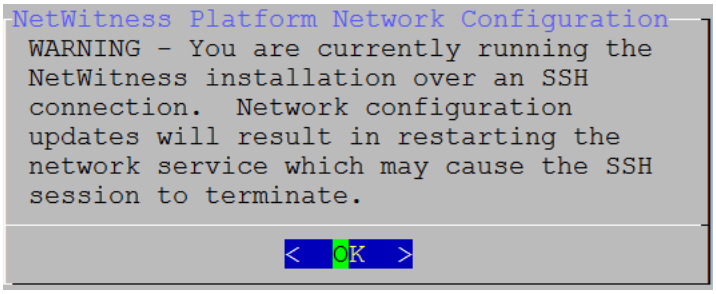
   - Si el programa de instalación encuentra una dirección IP válida para este host, se muestra el siguiente indicador.

     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.

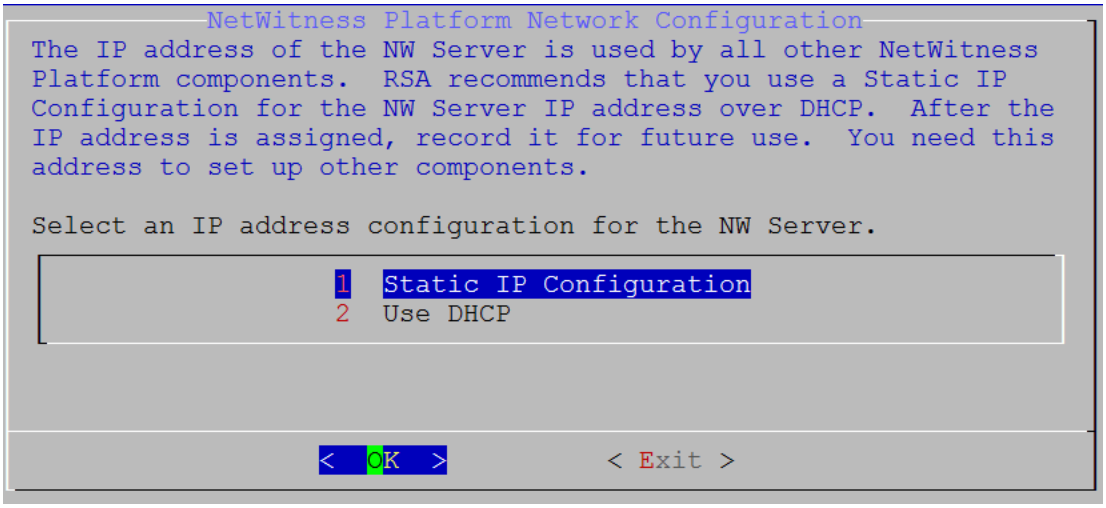
     Nota: Si se conecta directamente desde la consola del host, no se mostrará la siguiente advertencia.

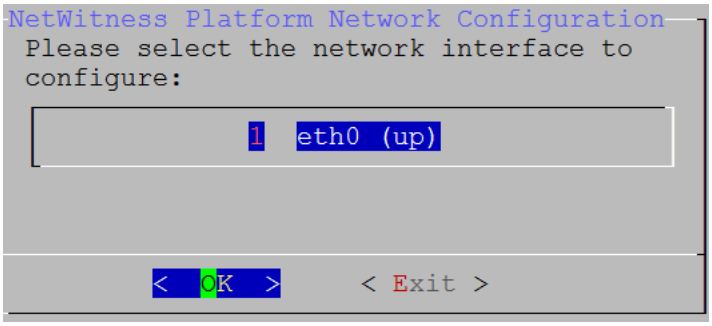
     Presione **Intro** para cerrar el indicador de advertencia.

   - 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.

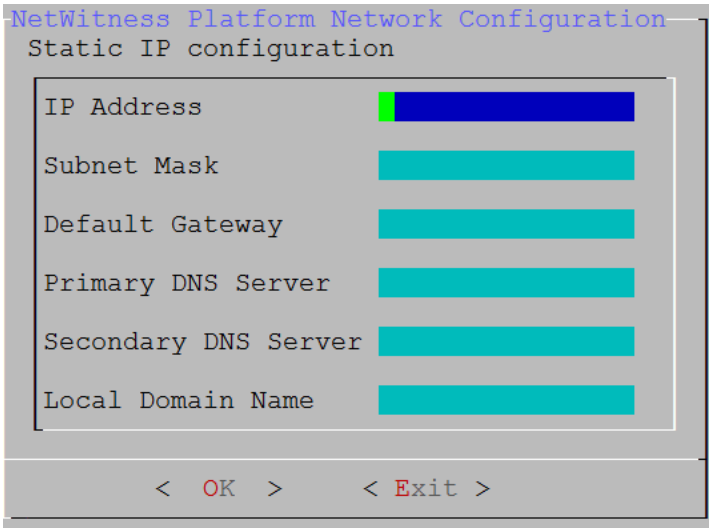
- Si el programa de instalación no encontró una configuración de IP o usted decidió cambiar la configuración de IP existente, se muestra el indicador **Configuración de red**.



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



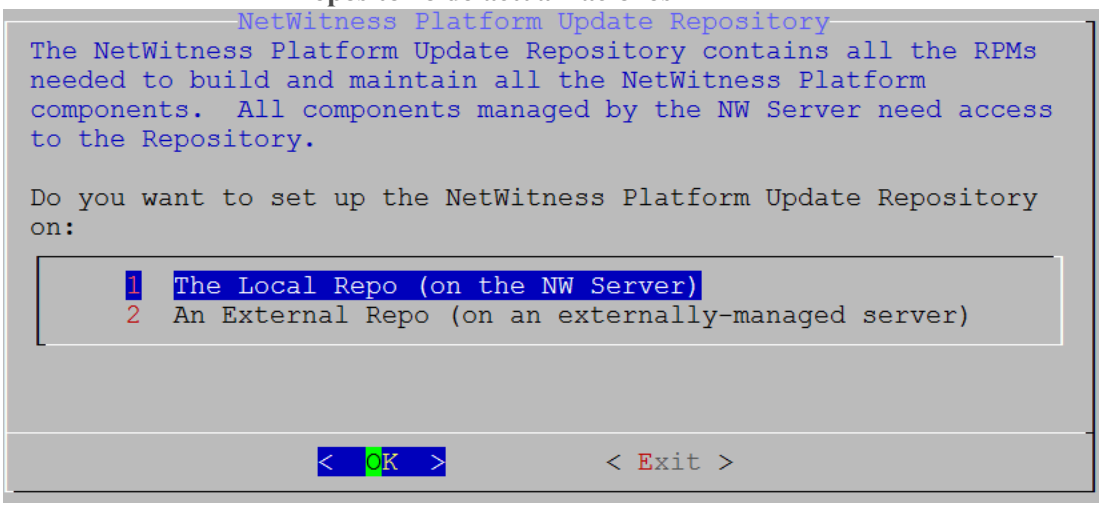
10. Use la flecha hacia abajo para desplazarse hasta la interfaz de red que desea, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**. Si no desea continuar, use la tecla de tabulación para ir a **Salir.**
    Se muestra el siguiente indicador **Configuración de IP estática**.



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

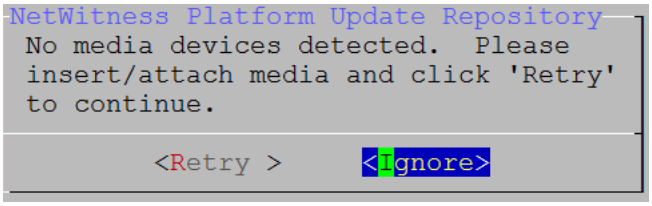
Precaución: Si selecciona un **servidor DNS**, asegúrese de que sea el servidor DNS correcto y que el host pueda acceder a él antes de continuar con la instalación.

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

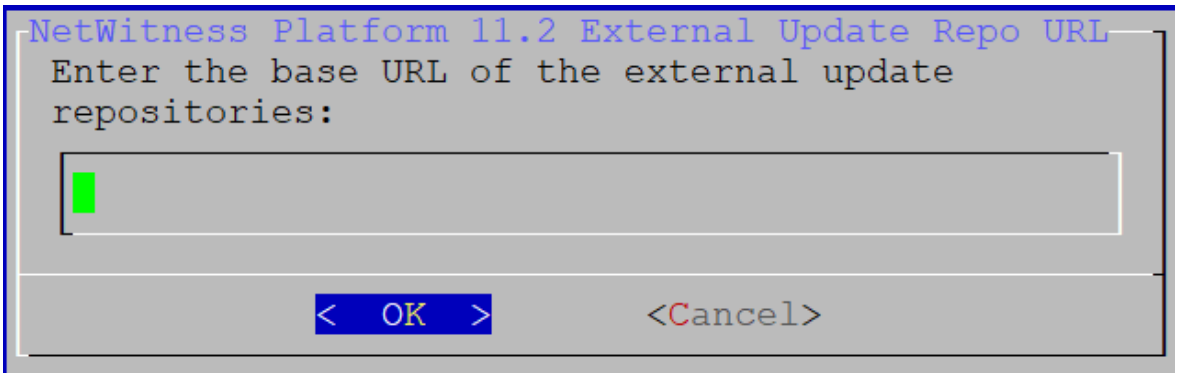


12. Presione **Intro** para elegir **Repositorio local** en el servidor de NW.
Si desea usar un repositorio externo, use la flecha hacia abajo para desplazarse hasta **Repositorio externo**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

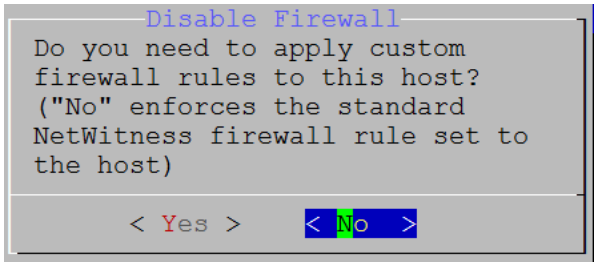
- Si selecciona **1 El repositorio local (en el servidor de NW)** en el programa de instalación, asegúrese de que estén conectados los medios adecuados al host (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación) desde los cuales puede instalar NetWitness Platform 11.2.0.0. Si el programa no puede encontrar los medios conectados, se muestra el siguiente indicador.



- Si selecciona **2 Un repositorio externo (en un servidor administrado externamente)**, la interfaz del usuario le solicita que indique una dirección URL. Los repositorios otorgan acceso a las actualizaciones de RSA y a las actualizaciones de CentOS. Consulte Apéndice B. Crear un repositorio externo para obtener instrucciones sobre cómo crear este repositorio y la dirección URL correspondiente del repositorio externo, de modo que pueda ingresarla en el siguiente indicador.

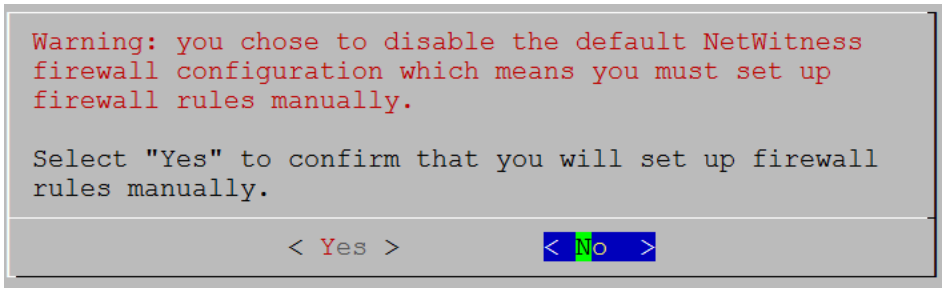


Ingrese la dirección URL base del repositorio externo de NetWitness Platform y haga clic en **Aceptar**. Se muestra el indicador **Iniciar instalación**.
Consulte "Configurar un repositorio externo con actualizaciones de RSA y del SO" en la sección "Procedimientos de hosts y servicios" de la *Guía de introducción de hosts y servicios de RSA NetWitness Platform* para obtener instrucciones. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
Se muestra el indicador Deshabilitar el firewall.

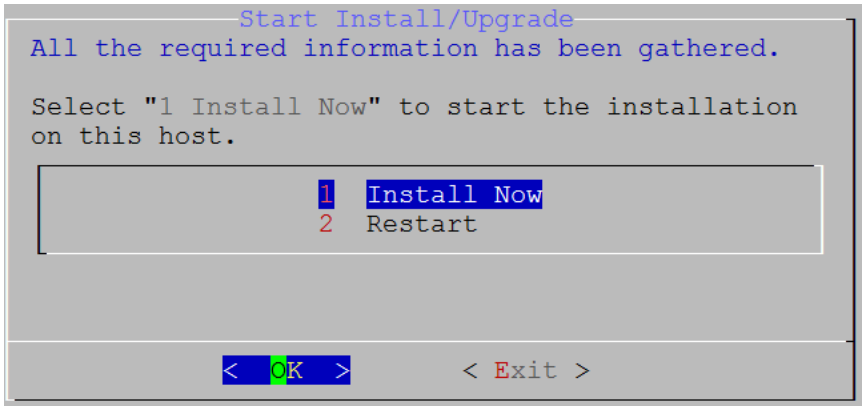


13. Use la tecla de tabulación para ir a **No** (valor predeterminado) y presione **Intro** para usar la configuración del firewall estándar. Use la tecla de tabulación para ir a **Sí** y presione **Intro** para deshabilitar la configuración del firewall estándar.

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

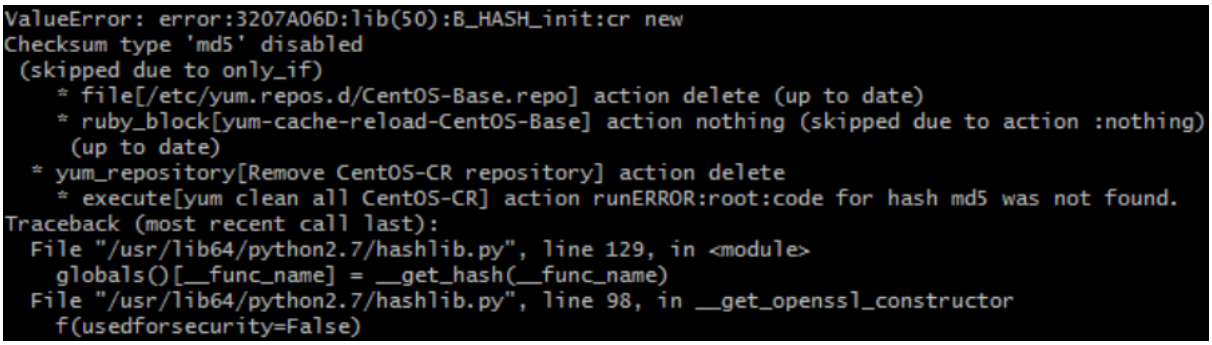


Se muestra el indicador **Iniciar instalación/actualización**.



14. Presione **Intro** para instalar 11.2 en el servidor de NW.
    Cuando se muestra **Instalación completa**, terminó de instalar el servidor de NW 11.2 en este host.

> **Nota:** Pase por alto los errores de código hash, similares a los errores que se muestran en la siguiente figura, 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.



Tarea 2: Instalar 11.2 en otros hosts de componentes

Para un host que no es de servidor de NW, esta tarea:

- Crea una imagen base.
- Configura el host que no es de servidor de NW 11.2.

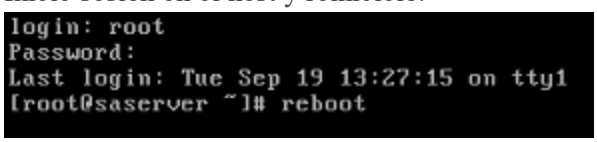
Para los hosts de ESA:

- Instale el host de ESA primario e instale el servicio **ESA primario** en este después de completar el programa de instalación en la interfaz del usuario de la vista **ADMINISTRAR > Hosts**.
- (Condicional) Si tiene un host de ESA secundario, instale el servicio **ESA secundario** en este después de completar el programa de instalación en la interfaz del usuario de la vista **ADMINISTRAR > Hosts**.

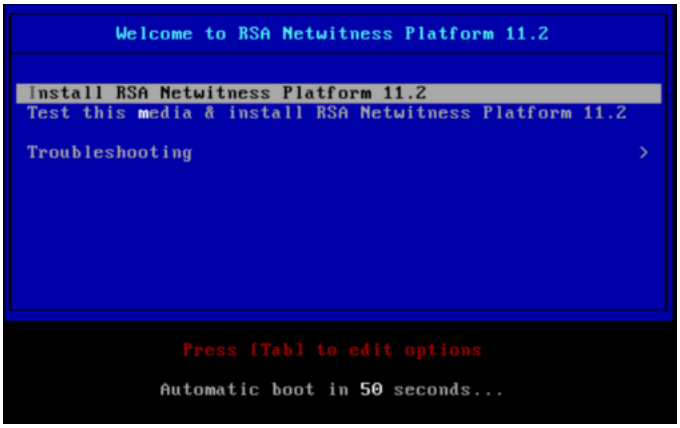
Realice los siguientes pasos para instalar NetWitness Platform 11.2 en un host que no es de servidor de NW.

1. Cree una imagen base en el host:
   a. Conecte los medios (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación) al host.
   Para obtener más información, consulte las *Instrucciones para una unidad de compilación de RSA NetWitness Platform*.
      - Instalaciones de hipervisor: Use la imagen ISO.
      - Medios físicos: Use el archivo ISO para crear medios de disco flash de arranque mediante la herramienta de instalación Universal Netboot (UNetbootin) u otra herramienta de digitalización adecuada. Consulte las *Instrucciones para una unidad de compilación* de *RSA NetWitness® Platform* para obtener información sobre cómo crear una unidad de compilación desde el archivo ISO. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
      - Instalaciones de iDRAC: El tipo de medios virtuales es:
         - **Disquete virtual** para discos flash mapeados.
         - **CD virtual** para dispositivos de medios ópticos o archivos ISO mapeados.

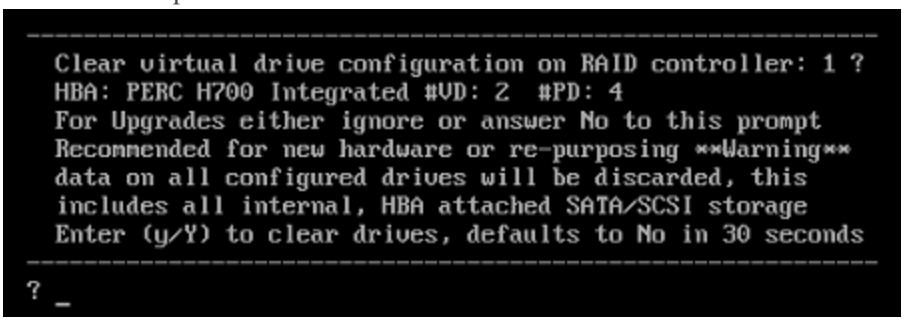
      Para obtener más información, consulte las *Instrucciones para una unidad de compilación de RSA NetWitness Platform*.
   b. Inicie sesión en el host y reinícielo.



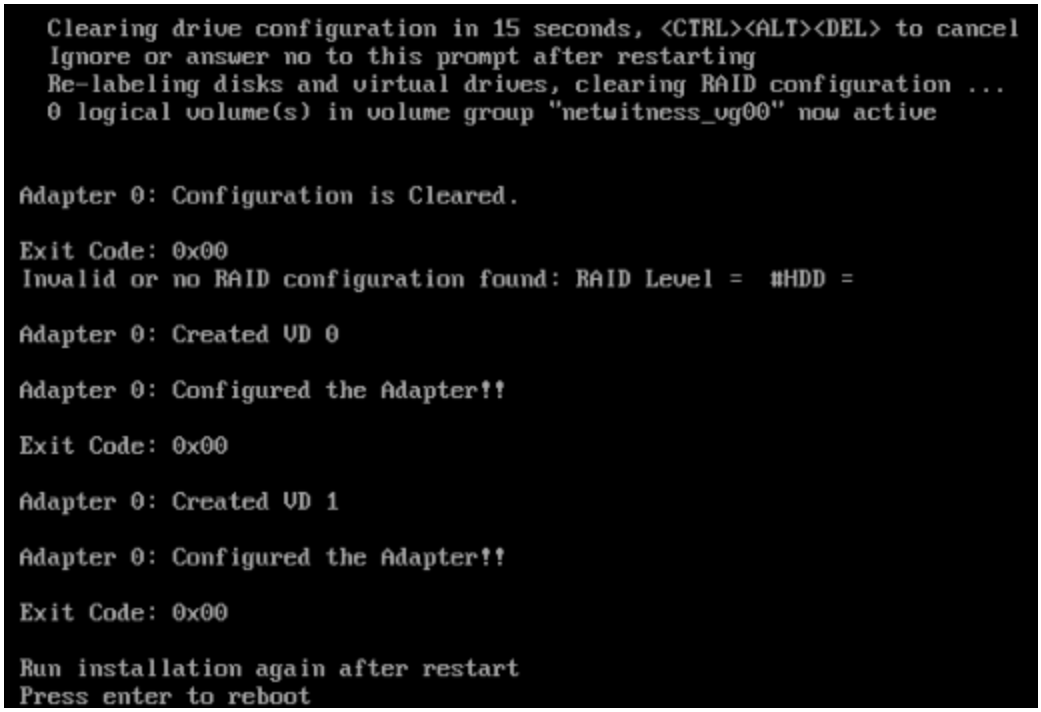
c. Seleccione **F11 (menú de arranque)** durante el reinicio para seleccionar un dispositivo de arranque y arrancar desde los medios conectados.
Después de algunas comprobaciones del sistema durante el arranque, se muestra el siguiente menú de instalación **Bienvenido a RSA NetWitness Platform 11.2**. Los gráficos del menú se generarán de manera diferente si usa un medio flash USB físico.



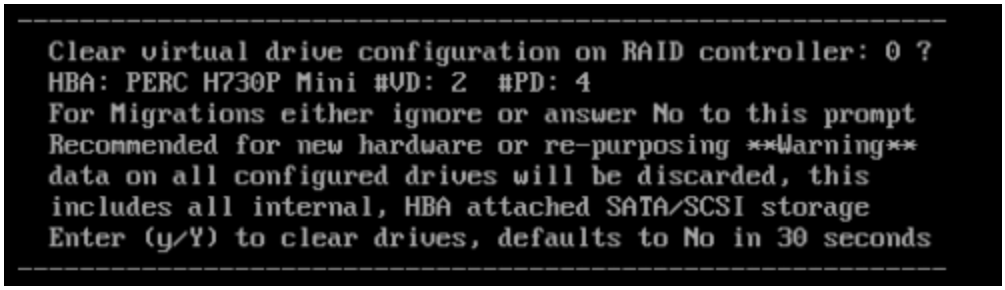
d. Seleccione **Instalar RSA Netwitness Platform 11.2** (selección predeterminada) y presione **Intro**.
El programa de instalación se ejecuta y se detiene en el indicador **Ingresar (s/S) para borrar las unidades** que le solicita formatear las unidades.



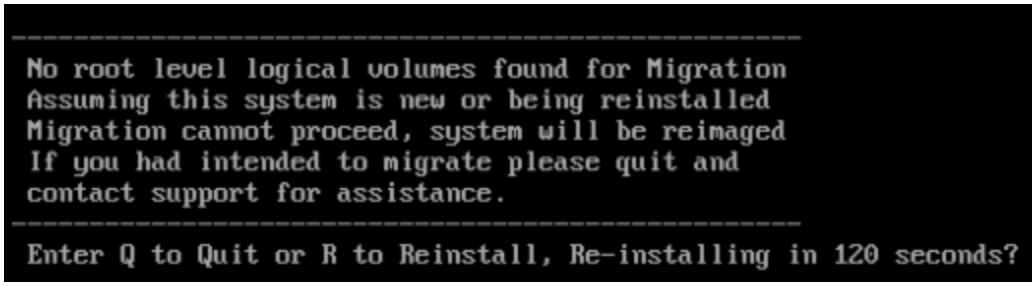
e. Escriba **S** para continuar.
La acción predeterminada es No, de modo que si pasa por alto el indicador, se seleccionará No en 30 segundos y las unidades no se borrarán. Se muestra el indicador **Presione Intro para reiniciar**.



f. Presione **Intro** para reiniciar el host.
El programa de instalación le vuelve a solicitar que borre las unidades.

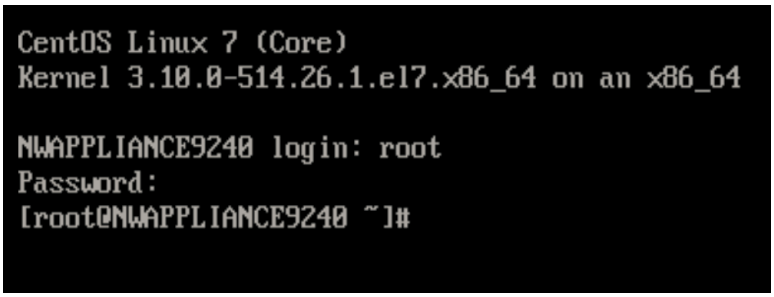


g. Escriba **N** porque ya borró las unidades.
Se muestra el indicador **Ingresar Q (Salir) o R (Reinstalar)**.



h. Escriba **R** para instalar la imagen base.
El programa de instalación muestra los componentes a medida que se instalan, lo que varía según el dispositivo, y reinicia.

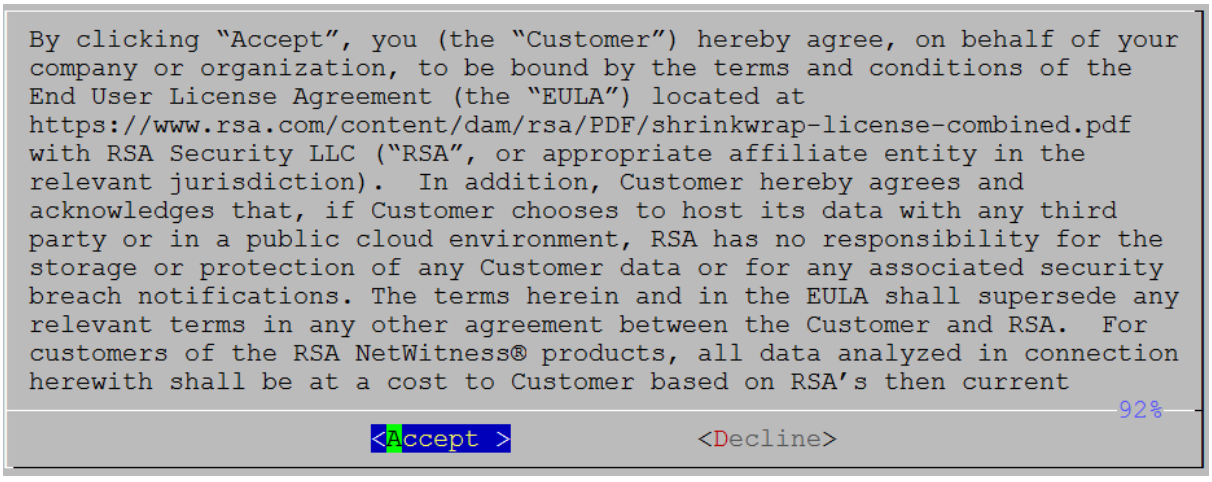
Precaución: No reinicie los medios conectados (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación).



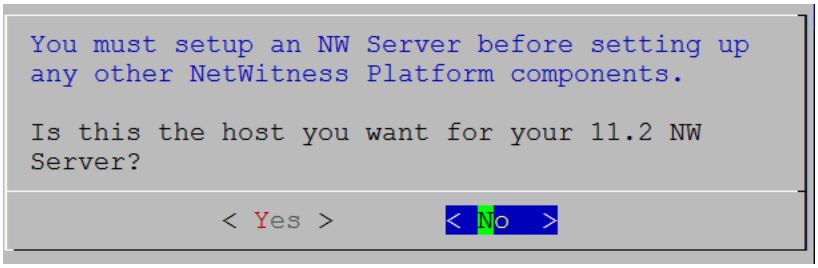
i. Inicie sesión en el host con las credenciales `root` .

2. Ejecute el comando `nwsetup-tui` para configurar el host.
Esto inicia `nwsetup-tui` (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 el proceso (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 11 (los servidores DNS no están definidos, de modo que el sistema no puede acceder al repositorio externo).

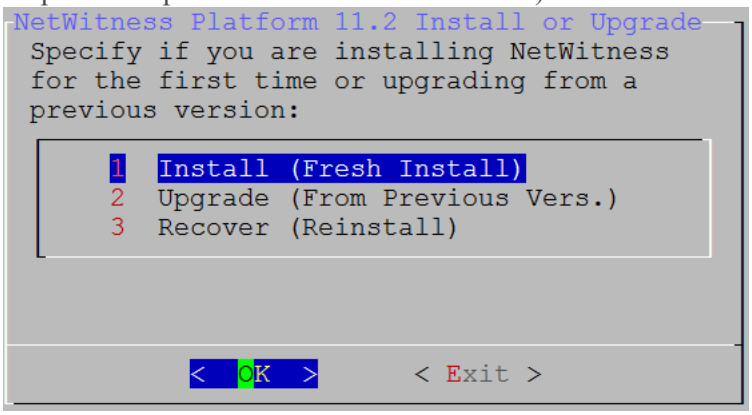


3. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador **¿Es este el host que desea para el servidor de NW 11.2?**.

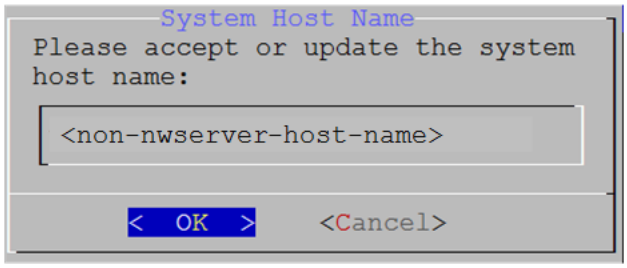


Precaución: Si elige el host incorrecto para el servidor de NW y completa la instalación, debe reiniciar el programa de instalación y completar los pasos del 2 al 14 de Tarea 1: Instalar 11.2 en el host del servidor de NetWitness (servidor de NW) para corregir este error.

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).



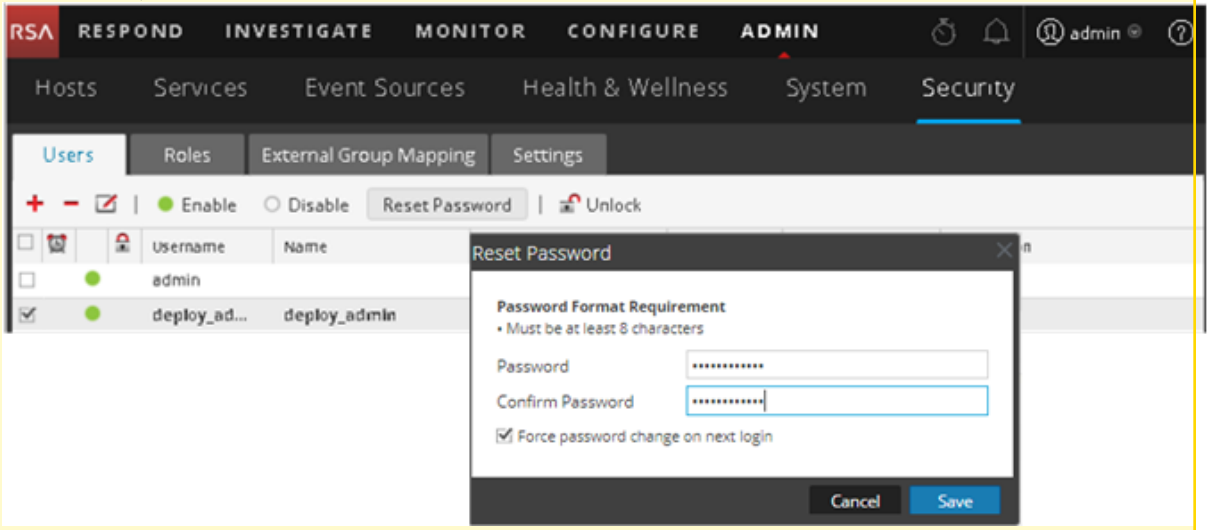
5. Presione **Intro**. La opción **Instalar (instalación nueva)** está seleccionada de manera predeterminada.
   Se muestra el indicador **Nombre del host**.



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

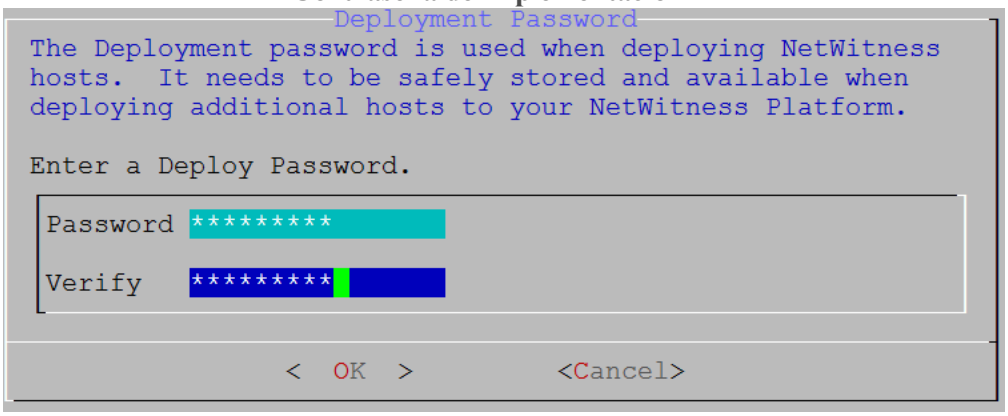
6. Si desea mantener este nombre, presione **Intro**. Si desea cambiar este nombre, edítelo, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador **Contraseña maestra**.

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



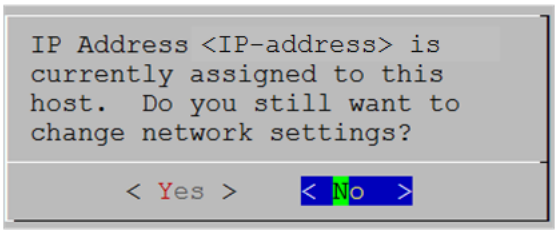
debe:
1. Acceder mediante el protocolo SSH al host del servidor de NW.
2. Ejecutar el script `(/opt/rsa/saTools/bin/set-deploy-admin-password`.
3. Usar la nueva contraseña en el momento de instalar cualquier host nuevo que no es de servidor de NW.
4. Ejecutar el script `(/opt/rsa/saTools/bin/set-deploy-admin-password`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



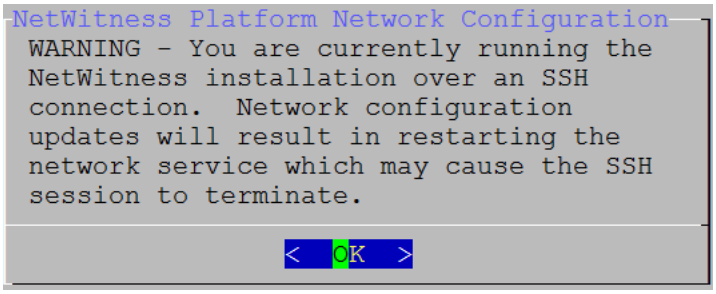
Nota: Debe usar la misma contraseña de implementación que usó cuando instaló el servidor de NW.

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

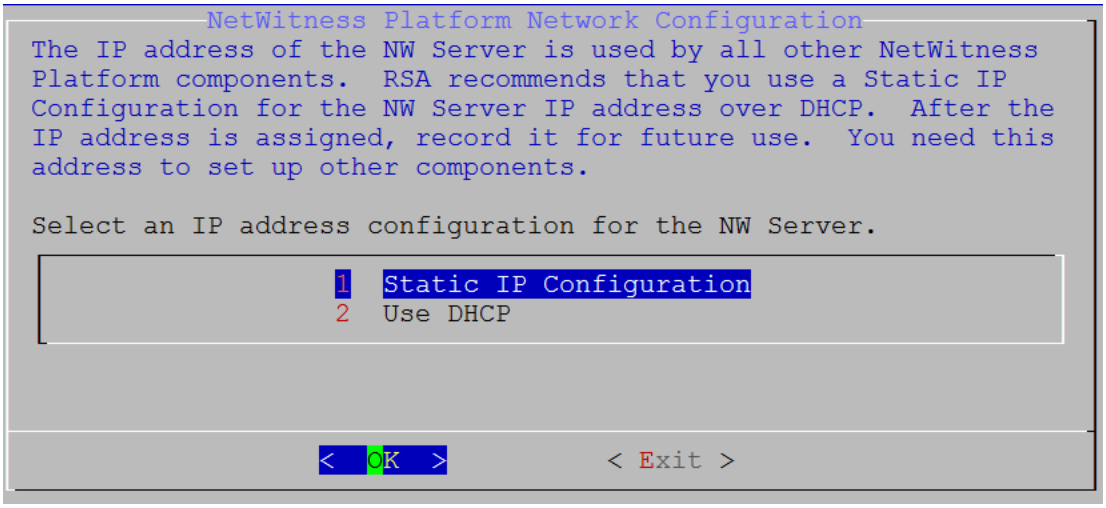
     Presione **Intro** si desea usar esta dirección IP y evitar cambiar la configuración de red. Use la tecla de tabulación para ir a **Sí** y presione **Intro** si desea cambiar la configuración de IP que se encontró en el host.
   - Si está usando una conexión de protocolo SSH, se muestra la siguiente advertencia.

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

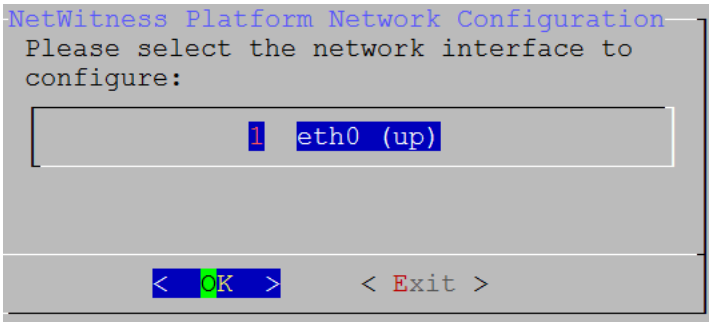
     

     Presione **Intro** para cerrar el indicador de advertencia.
   - Si el programa de instalación encontró una configuración de IP y usted decidió usarla, se muestra el indicador **Repositorio de actualizaciones**. Vaya al paso 11 para completar la instalación.

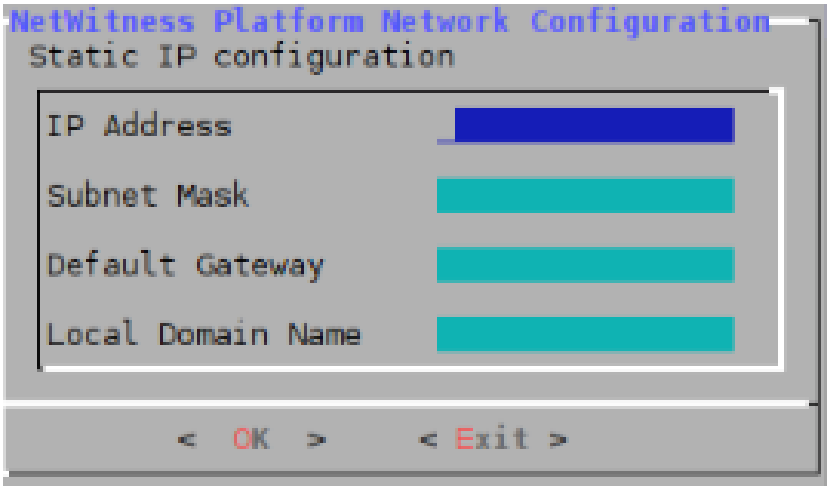
- Si el programa de instalación no pudo encontrar una configuración de IP o usted decidió cambiar la configuración de IP existente, se muestra el indicador **Configuración de red**.



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**.



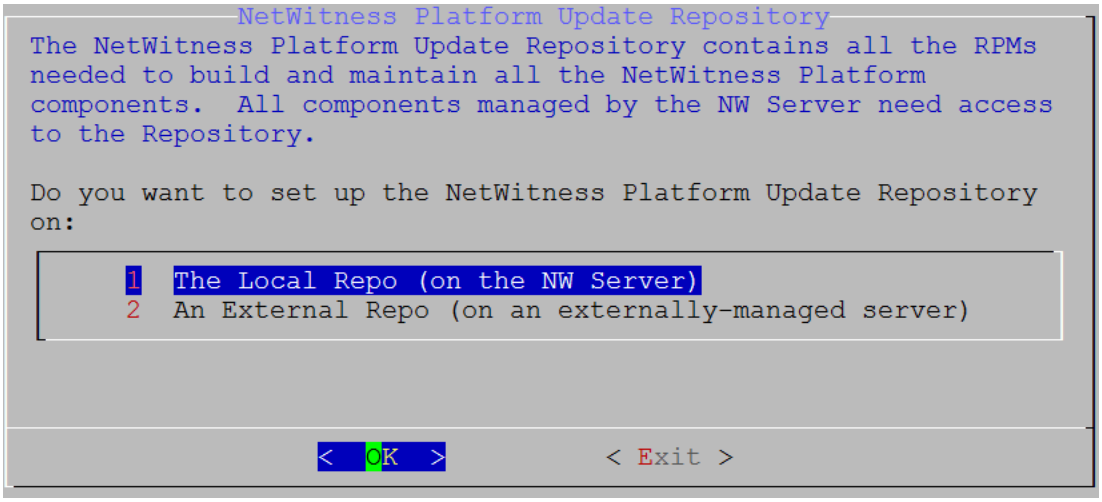
9. Use la flecha hacia abajo para desplazarse hasta la interfaz de red que desea, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**. Si no desea continuar, use la tecla de tabulación para ir a **Salir**.
   Se muestra el siguiente indicador **Configuración de IP estática**.



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>`.

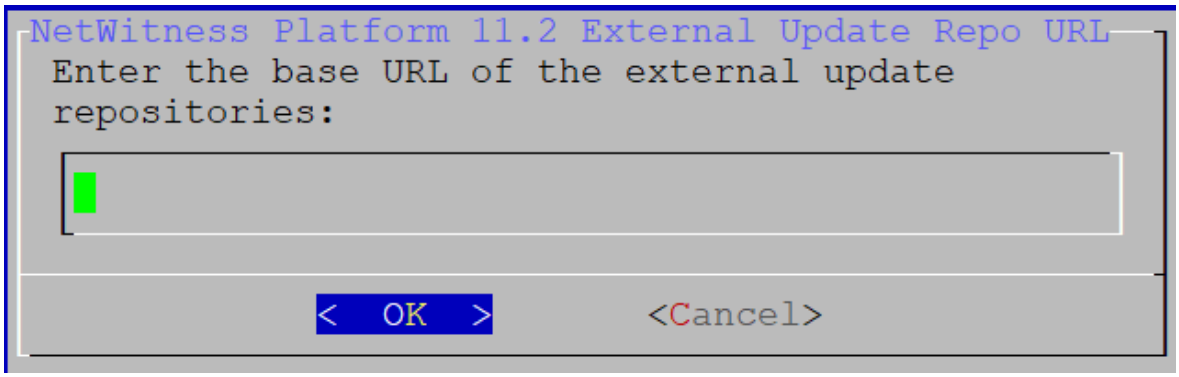
    Precaución: Si selecciona un **servidor DNS**, asegúrese de que sea el servidor DNS correcto y que el host pueda acceder a él antes de continuar con la instalación.

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

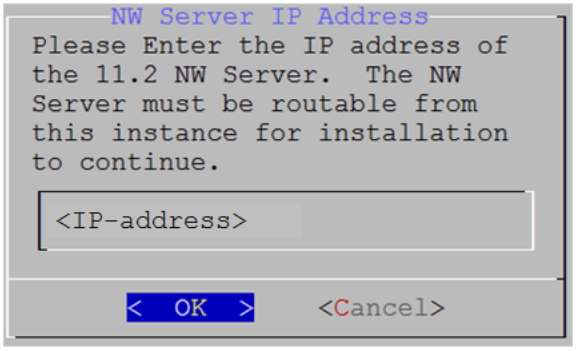


11. Presione **Intro** para elegir **Repositorio local** en el servidor de NW.
    Si desea usar un repositorio externo, use la flecha hacia abajo para desplazarse hasta **Repositorio externo**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

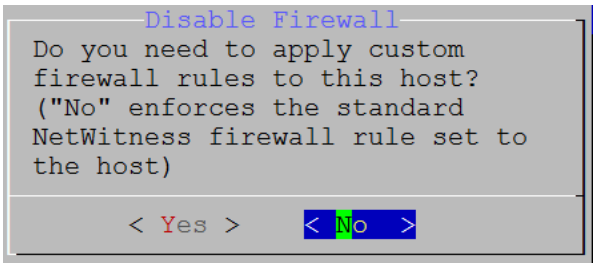
    - Si selecciona **1 El repositorio local (en el servidor de NW)** en el programa de instalación, asegúrese de que estén conectados los medios adecuados al host (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación) desde los cuales puede instalar NetWitness Platform 11.2.0.0.
    - Si selecciona **2 Un repositorio externo (en un servidor administrado externamente: no en el servidor de NW)**, la interfaz del usuario le solicita que indique una dirección URL. Los repositorios otorgan acceso a las actualizaciones de RSA y a las actualizaciones de CentOS. Consulte Apéndice B. Crear un repositorio externo para obtener instrucciones sobre cómo crear este repositorio y la dirección URL correspondiente del repositorio externo, de modo que pueda ingresarla en el siguiente indicador.



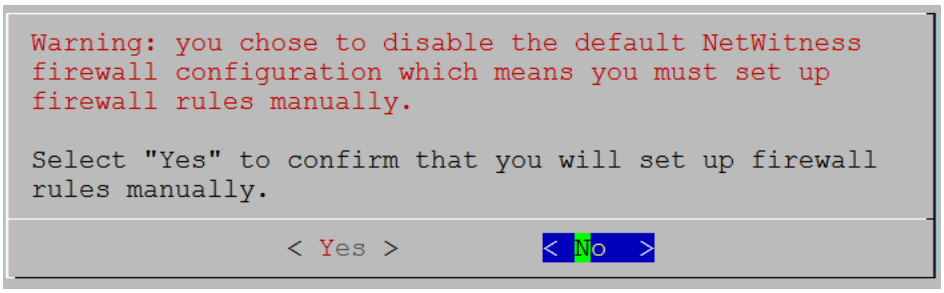
Ingrese la dirección URL base del repositorio externo de NetWitness Platform, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
Se muestra el indicador **Dirección IP del servidor de NW**.



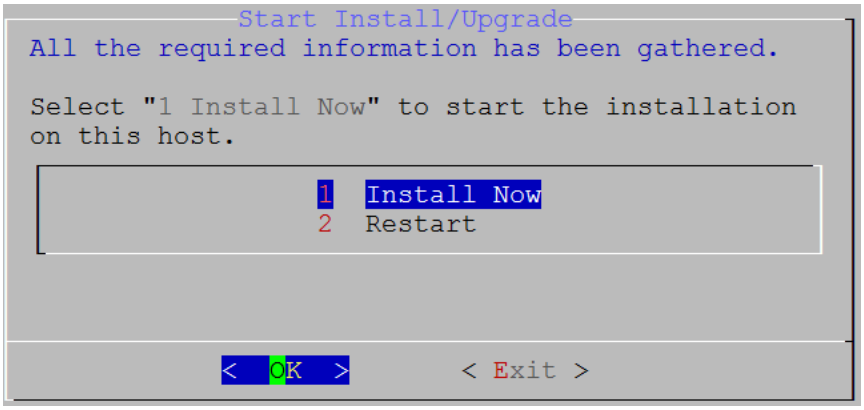
12. Escriba la dirección IP del servidor de NW. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
    Se muestra el indicador **Deshabilitar el firewall**.



13. 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**.

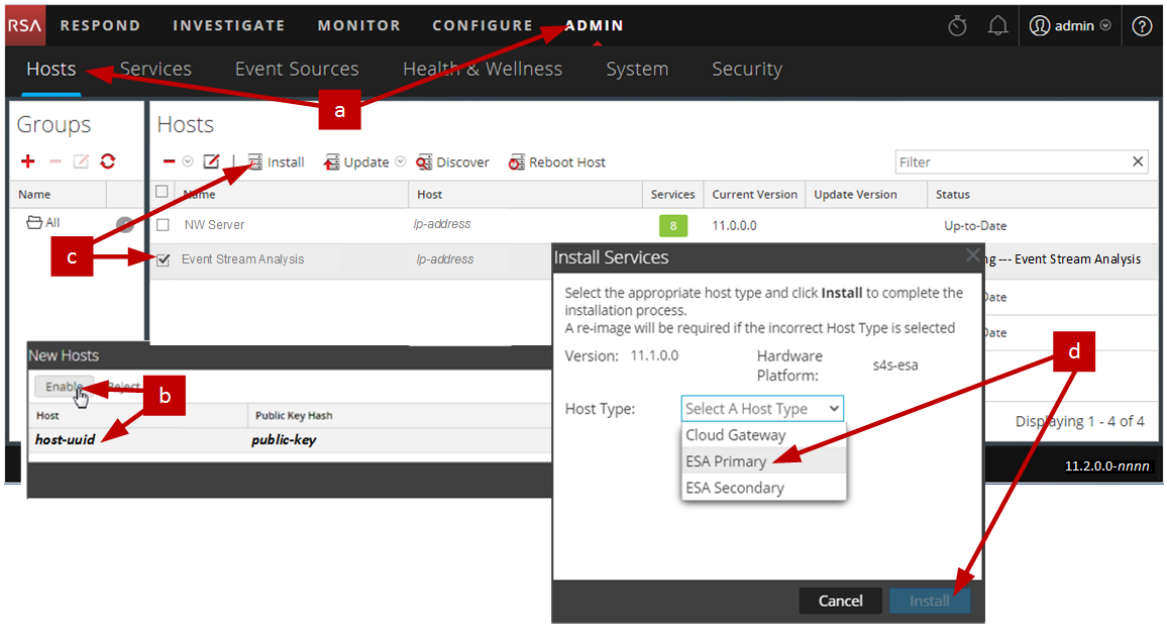


14. Presione **Intro** para instalar 11.2 en el servidor que no es de NW.
    Cuando se muestra **Instalación completa**, tiene un host de servidor genérico que no es de servidor de NW con un sistema operativo compatible con NetWitness Platform 11.2.
15. Instale un servicio de componentes en el host.
    a. 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.

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

d. Seleccione el 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.

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

Actualizar o instalar la recopilación de Windows existente

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

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

Tareas posteriores a la instalación

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

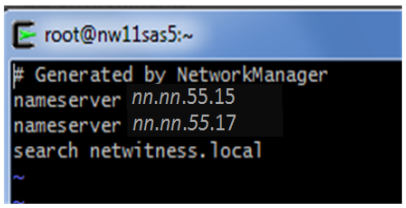
- General
- RSA NetWitness® Endpoint Insights
- Habilitación de FIPS
- RSA NetWitness® UEBA

General

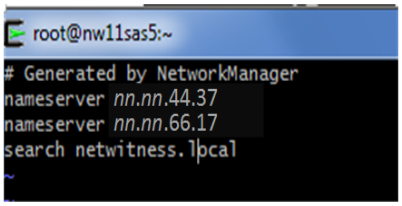
(Opcional) Tarea 1: Volver a configurar servidores DNS después de 11.2

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.



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



   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

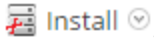
Debe instalar uno de los siguientes servicios para instalar NetWitness Platform Endpoint Insights en la implementación:

- Endpoint Hybrid
- Endpoint Log Hybrid

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

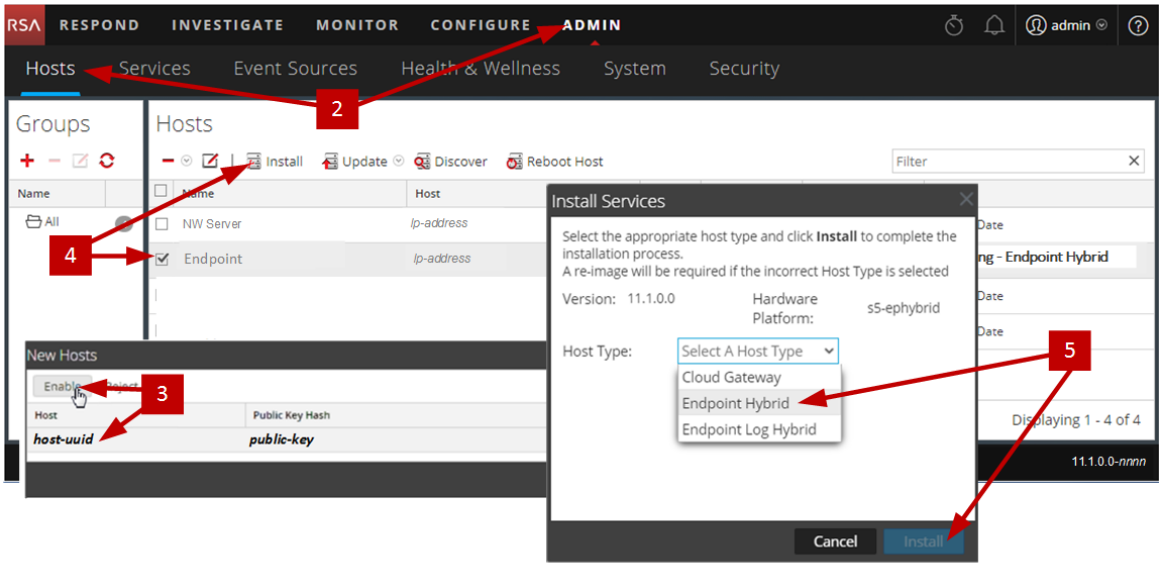
Nota: Debe instalar Endpoint Hybrid o Endpoint Log Hybrid en el dispositivo serie 5 o Dell R730.

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 

.
   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.

RSA NetWitness® UEBA

(Opcional) Tarea 4: 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.

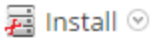
1. Complete los pasos del 1 al 14 para el host físico o los pasos del 1 al 15 para los hosts virtuales como se describe en "Tarea 2: Instalar 11.2 en otros hosts de componentes" en la sección "Tareas de instalación" de la *Guía de instalación de hosts físicos de NetWitness Platform para la versión 11.2*. 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.

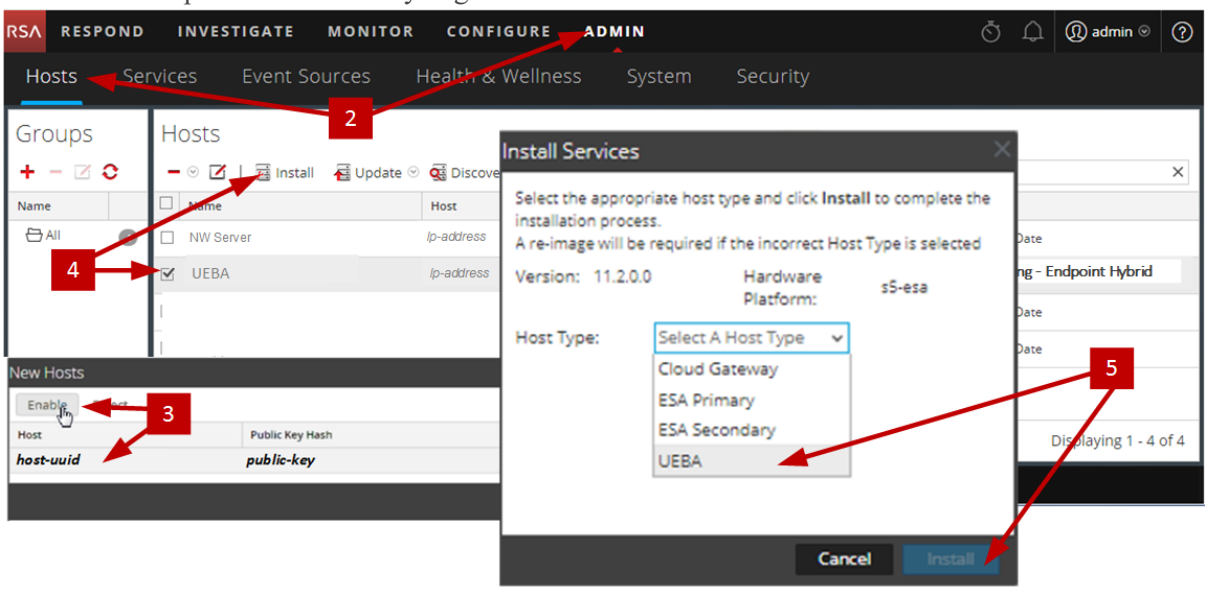
   Nota: Si no se muestra el cuadro de diálogo **Nuevos hosts**, haga clic en **Descubrir** en la barra de herramientas de la vista Hosts.

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 

.
   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.

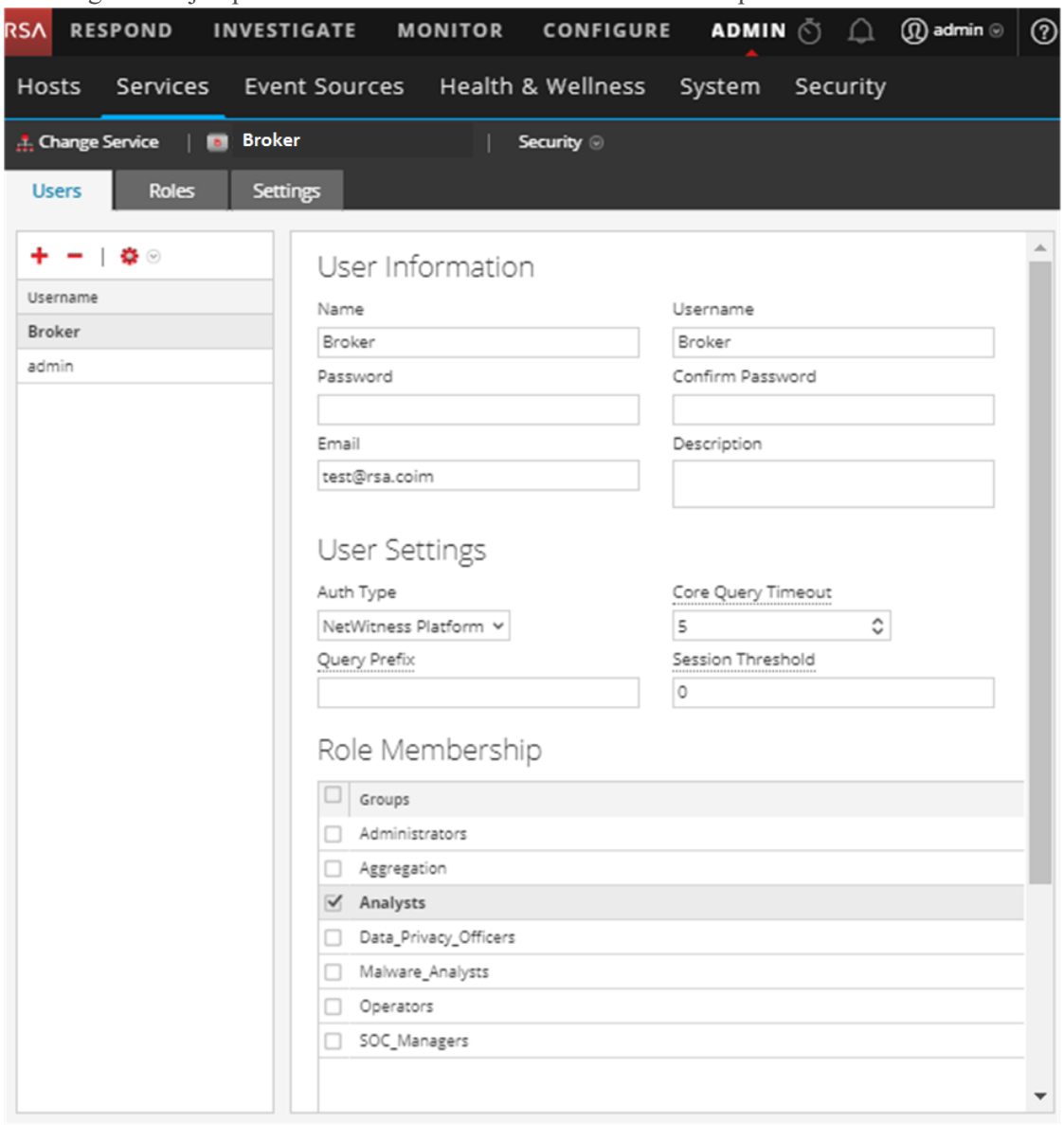
ii. Vaya a **Administrar** > **Servicios**.

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>`	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. `!"#$%&()*+,-:;<=>?@[\]^_`\{\|}` Si desea incluir uno o más caracteres especiales, debe delimitar la contraseña con un apóstrofo; por ejemplo: `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`
`-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>`	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`). **Nota:** El script interpreta la hora que ingresa como UTC (hora universal coordinada) y no la ajusta a la zona horaria local.

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)

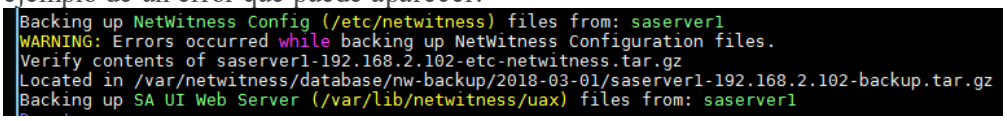
Mensaje de error	La interfaz de la línea de comandos (CLI) muestra: "La operación de coordinación falló." `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Causa	Ingresó la contraseña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

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

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

Respaldo (script `nw-backup`)

Mensaje de error	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Causa	La contraseña de administrador de ESA Mongo contiene caracteres especiales (por ejemplo, '!@#$%^qwerty').
Solución	Vuelva a cambiar la contraseña de administrador de ESA Mongo al valor predeterminado original de "netwitness" antes de ejecutar el respaldo.

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

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

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

Event Stream Analysis

Problema	El servicio ESA falla después de actualizar a 11.2.0.0 desde una configuración de FIPS habilitado.
Causa	El servicio ESA está apuntando a un almacenamiento de claves no válido.

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

Servicio Log Collector (`nwlogcollector`)

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

Mensaje de error	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Causa	El Lockbox de Log Collector no se pudo abrir después de la actualización.
Solución	Inicie sesión en NetWitness Platform y restablezca la huella digital del sistema mediante el restablecimiento de la contraseña de valor de sistema estable para el Lockbox como se describe en el tema “Restablecer el valor de sistema estable” bajo el tema “Configurar ajustes de seguridad de Lockbox” en la *Guía de configuración de la recopilación de registros*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Mensaje de error	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Causa	El Lockbox de Log Collector no se configuró después de la actualización.
Solución	Si utiliza un Lockbox de Log Collector, inicie sesión en NetWitness Platform y configure el Lockbox como se describe en el tema “Configurar ajustes de seguridad de Lockbox” de la *Guía de configuración de la recopilación de registros*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Mensaje de error	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Causa	Debe restablecer el campo de umbral de valor estable para el Lockbox de Log Collector.
Solución	Inicie sesión en NetWitness Platform y restablezca la contraseña de valor de sistema estable para el Lockbox como se describe en el tema "Restablecer el valor de sistema estable" bajo el tema "Configurar ajustes de seguridad de Lockbox" en la *Guía de configuración de la recopilación de registros*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

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

Servidor de NW

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

Problema	Después de la actualización, observa que los registros de auditoría no se reenvían a la configuración de auditoría global definida o El siguiente mensaje se muestra en `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Causa	La migración de la configuración de auditoría global del servidor de NW de 10.6.6.x a 11.2.0.0 no se pudo realizar.
Solución	1. Acceda mediante el protocolo SSH al servidor de NW. 2. Ejecute el siguiente comando. `orchestration-cli-client --update-admin-node`

Orchestration

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

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

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

Servicio Reporting Engine

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

Mensaje de error	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Causa	La actualización de Reporting Engine falló debido a que no hay espacio en disco suficiente.
Solución	Libere el espacio en disco requerido según se muestra en el mensaje de registro. Consulte el tema "Agregar espacio adicional para informes grandes" de la *Guía de configuración de Reporting Engine* para obtener instrucciones sobre cómo liberar espacio en disco. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

NetWitness UEBA

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

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

Apéndice B. Crear un repositorio externo

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

1. Inicie sesión en el host del servidor web.
2. Cree el directorio `ziprepo` para alojar el repositorio de NW (`netwitness-11.2.0.0.zip`) bajo `web-root` del servidor web. Por ejemplo, si `/var/netwitness` es la raíz web, ejecute la siguiente cadena de comandos.
   ```
   mkdir /var/netwitness/ziprepo
   ```
3. Cree el directorio 11.2.0.0 bajo `/var/netwitness/ziprepo`.
   ```
   mkdir /var/netwitness/ziprepo/11.2.0.0
   ```
4. Cree los directorios `OS` y `RSA` bajo `/var/netwitness/ziprepo/11.2.0.0`.
   ```
   mkdir /var/netwitness/ziprepo/11.2.0.0/OS
   mkdir /var/netwitness/ziprepo/11.2.0.0/RSA
   ```
5. Descomprima el archivo `netwitness-11.2.0.0.zip` en el directorio `/var/netwitness/ziprepo/11.2.0.0`.
   ```
   unzip netwitness-11.2.0.0.zip -d /var/netwitness/ziprepo/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/ziprepo/11.2.0.0/OS`.
      ```
      unzip /var/netwitness/ziprepo/11.2.0.0/OS-11.2.0.0.zip -d
      /var/netwitness/ziprepo/11.2.0.0/OS
      ```

   b. `RSA-11.2.0.0.zip` en el directorio `/var/netwitness/ziprepo/11.2.0.0/RSA`.
      ```
      unzip /var/netwitness/ziprepo/11.2.0.0/RSA-11.2.0.0.zip -d
      ```

`/var/netwitness/ziprepo/11.2.0.0/RSA`

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

La dirección URL externa del repositorio es `http://<web server IP address>/ziprepo`.

7. Use `http://<web server IP address>/ziprepo` en respuesta al indicador **Ingrese la dirección URL base de los repositorios de actualización externos** del programa de instalación de NW 11.2 (nwsetup-tui).

Historial de revisiones

Revisión	Fecha	Descripción	Autor
1.0	15/8/2018	Liberación a Operaciones	IDD

1.1	24/9/2018	Se actualizó la cadena de comandos del script de configuración de UEBA en Tareas posteriores a la instalación para evitar confusión y quitar la extensión `.sh` del script.
		Cadena de comandos incorrecta:
		`./ueba-server-config.sh -u <user> -p <password> -h <host> -o <type> -t`
		`<startTime> -s <schemas> -v`
		Cadena de comandos corregida:
		`/opt/rsa/saTools/ueba-server-config -u <user> -p <password> -h <host> -o <type> -t <startTime> -s <schemas> -v`
			IDD

1.2	10/10/2018	Se realizaron varios cambios en “Tarea 4: Instalar NetWitness UEBA” bajo Tareas posteriores a la instalación (consulte SADOCS-1592).	IDD
1.3	11/10/2018	Se agregó un tema sobre la configuración del almacenamiento de conexión externa para la mejora SADOCS-1597	IDD
1.4	29/11/2018	Se agregó una nota acerca de la licencia de prueba de UEBA.	IDD