RSA NETWITNESS® PLATFORM

Guía de implementación

para RSA NetWitness® Platform 11.3

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.

julio 2019

Contenido

Conceptos básicos

En esta guía se describen los requisitos básicos de una implementación de NetWitness Platform y se presentan escenarios opcionales para abordar las necesidades de su empresa. Incluso en redes pequeñas, la planificación puede garantizar que todo funcione correctamente cuando esté listo para poner los hosts en línea.

Nota: En este documento se hace referencia a documentación adicional disponible en RSA Link. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Existen muchos factores que debe tener en cuenta antes de implementar NetWitness Platform. Los siguientes elementos son solo algunos de estos factores. Cuando considere estos factores, debe calcular los requisitos de crecimiento y almacenamiento

- El tamaño de su empresa (es decir, la cantidad de ubicaciones y personas que utilizarán NetWitness Platform.
- El volumen de registros y datos de red que debe procesar.
- El rendimiento que necesita cada función de usuario de NetWitness Platform para desempeñar su trabajo de manera eficaz.
- La prevención del tiempo fuera (es decir, cómo evitar un punto único de falla).
- El entorno en el cual planea ejecutar NetWitness Platform
  - Hosts físicos de RSA (software que se ejecuta en hardware que proporciona RSA)
    Consulte la *Guía de instalación de hosts físicos de RSA NetWitness® Platform*para obtener instrucciones detalladas sobre cómo implementar hosts físicos de RSA.
  - Software solo proporcionado por RSA:
    - Hosts virtuales en las instalaciones
      Consulte la *RSA NetWitness® Platform Guía de instalación de hosts virtuales de* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en las instalaciones.
    - VCloud:
      - Amazon Web Services (AWS)
        Consulte la *Guía de instalación de AWS de RSA NetWitness® Platform* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en AWS.
      - Azure
        Consulte la *Guía de instalación de Azure de RSA NetWitness® Platform* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en Azure.

Implementación básica

Antes de que pueda implementar NetWitness Platform, necesita:

- Considerar los requisitos de su empresa y comprender el proceso de implementación.
- Tener un panorama general de la complejidad y el alcance de una implementación de NetWitness Platform.

Proceso

Los componentes y la topología de una red de NetWitness Platform pueden variar en gran medida entre las instalaciones y se deben planear cuidadosamente antes del inicio del proceso. La planificación inicial incluye:

- Consideración de los requisitos del sitio y los requisitos de seguridad.
- Revisión de la arquitectura de red y el uso de puertos.
- Compatibilidad con la agregación de grupos en Archivers y Concentrators, y hosts virtuales.

Cuando esté listo para dar inicio a la implementación, la secuencia general es:

- Para los hosts físicos de RSA:
  1. Instalación de hosts físicos y conexión a la red, como se describe en las Guías de configuración de hardware de RSA NetWitness® Platform y en la *Guía de instalación de hosts físicos* de *RSA NetWitness® Platform*.
  2. Configure la licencia de NetWitness Platform, como se describe en la *Guía de licencia de RSA NetWitness® Platform*.
  3. Configure los hosts físicos y servicios individuales, como se describe en la *Guía de introducción de hosts y servicios de RSA NetWitness® Platform*. Esta guía también describe los procedimientos para aplicar actualizaciones y prepararse para las actualizaciones de versión.
- Para los hosts virtuales en las instalaciones, siga las instrucciones de la *Guía de instalación de hosts virtuales de RSA NetWitness® Platform*.
- Para AWS, siga las instrucciones de la *Guía de instalación de AWS* de *RSA NetWitness® Platform*.
- Para Azure, siga las instrucciones de la *Guía de instalación de Azure* de *RSA NetWitness® Platform*.

Cuando actualice los hosts y los servicios, siga las reglas recomendadas en el tema “Ejecución en modo mixto” de la *Guía de introducción de hosts y servicios de RSA NetWitness Platform*.

También debería familiarizarse con hosts, tipos de hosts y servicios como se usan en el contexto de NetWitness Platform, lo que también se describe en la *Guía de introducción de hosts y servicios de RSA NetWitness Platform*.

Diagrama de implementación general de NetWitness Platform

El siguiente diagrama ilustra una implementación básica de NetWitness Platform de múltiples sitios.

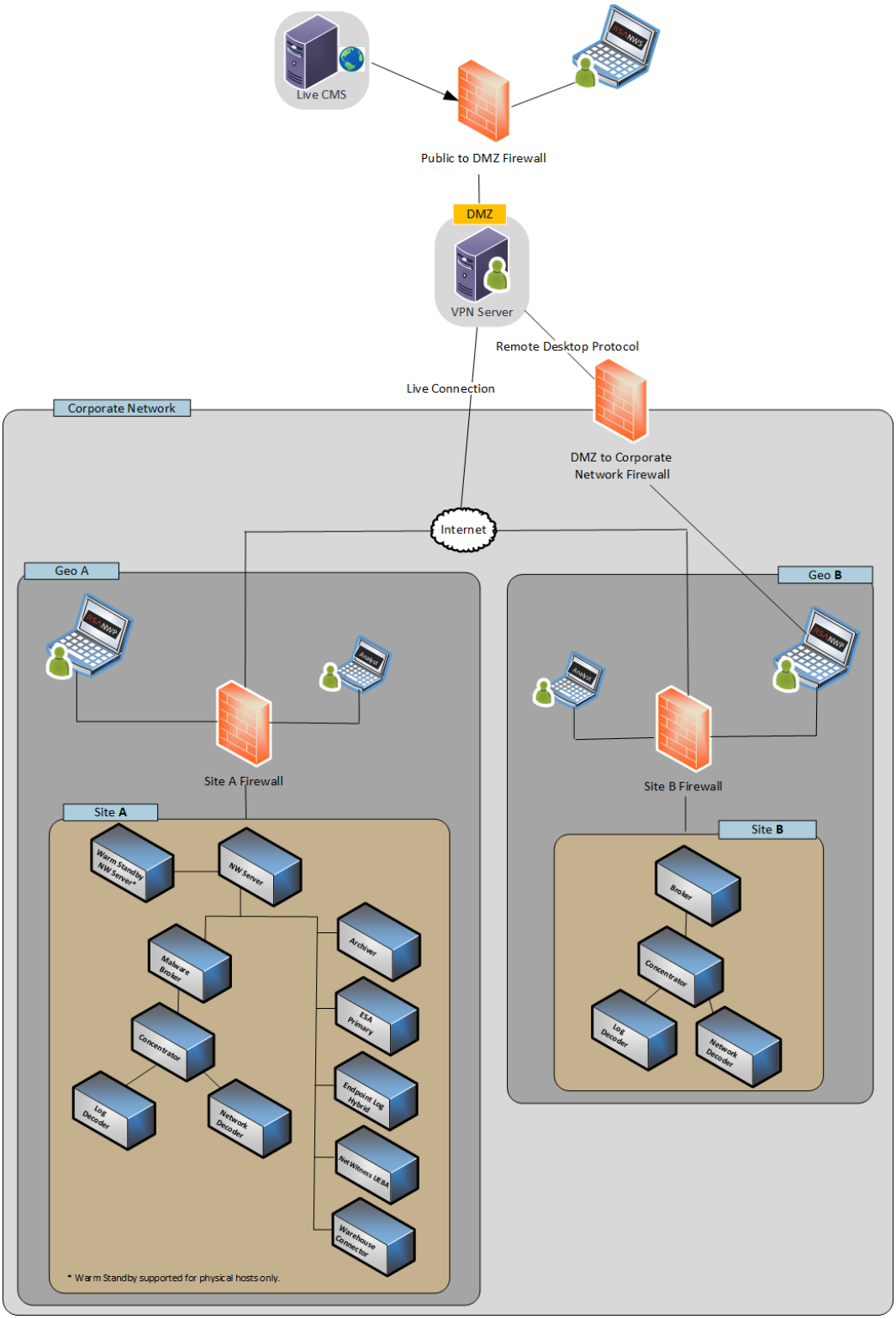
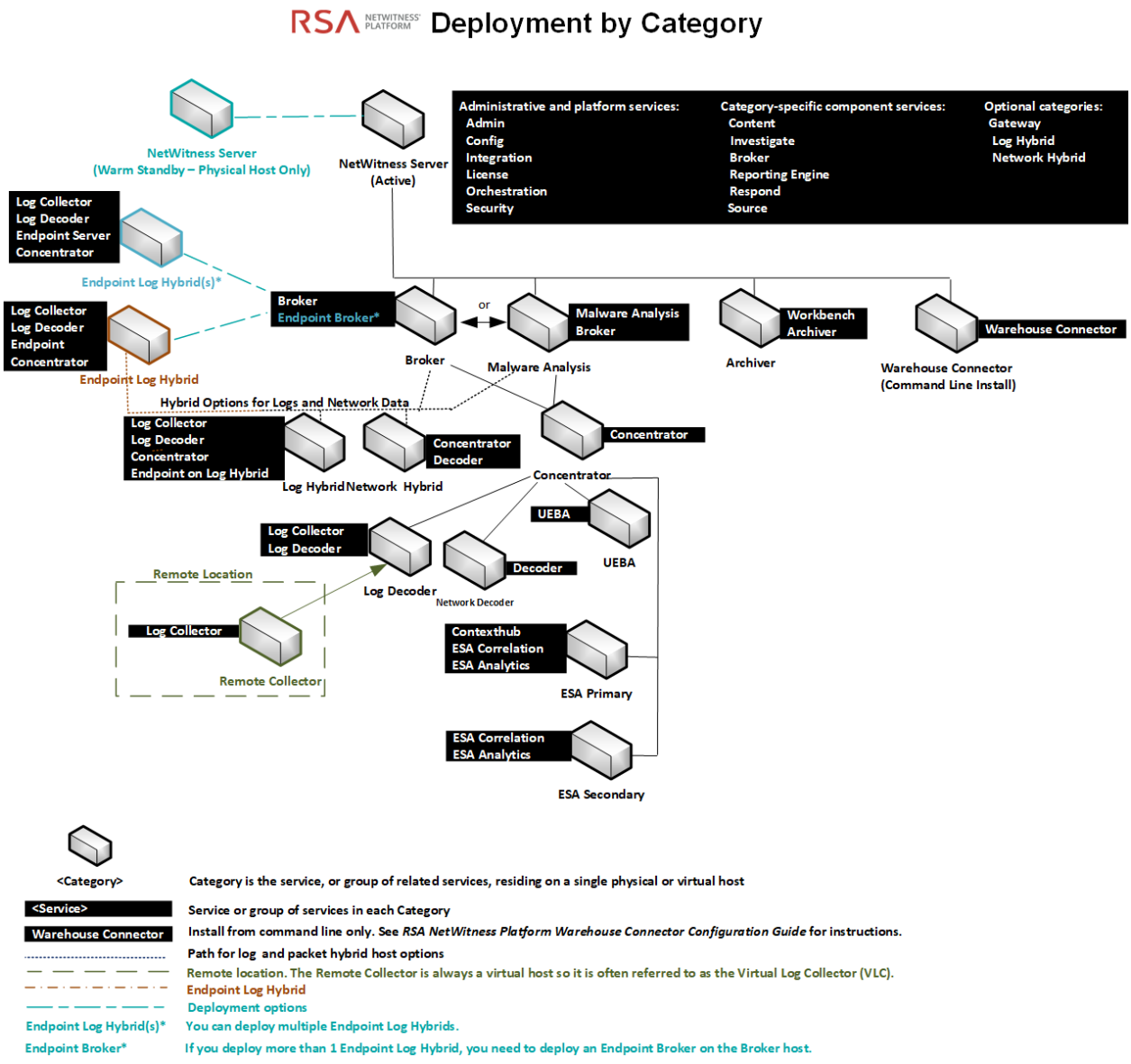


Diagrama detallado de implementación de hosts de RSA NetWitness Platform

El siguiente diagrama es un ejemplo de una implementación de NetWitness Platform alojada en máquinas físicas o virtuales. Para obtener instrucciones sobre cómo instalar NetWitness Platform, consulte la *Guía de instalación de hosts físicos*, la *Guía de instalación de hosts virtuales*, la *Guía de instalación de AWS* o la *Guía de instalación de Azure*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.



Opciones de implementación

RSA NetWitness Platform se implementa con las siguientes opciones.

- Agregación de grupos
- Segundo servidor Endpoint
- Host del servidor de NW semiactivo en espera
- Categorías híbridas en el servidor de NW

Consulte Procedimientos de configuración opcional de la implementación para obtener instrucciones.

Procedimientos de configuración opcional de la implementación

Agregación de grupos

La agregación de grupos se usa para configurar varios servicios Archiver o Concentrator como un grupo y compartir las tareas de agregación entre ellos. Puede configurar varios servicios Archiver o Concentrator para que agreguen de manera eficiente desde varios servicios Log Decoder con el fin de mejorar el rendimiento de las consultas en los datos:

- Almacenados en el Archiver.
- Procesados a través del Concentrator.

Recomendaciones para la implementación de la agregación de grupos de RSA

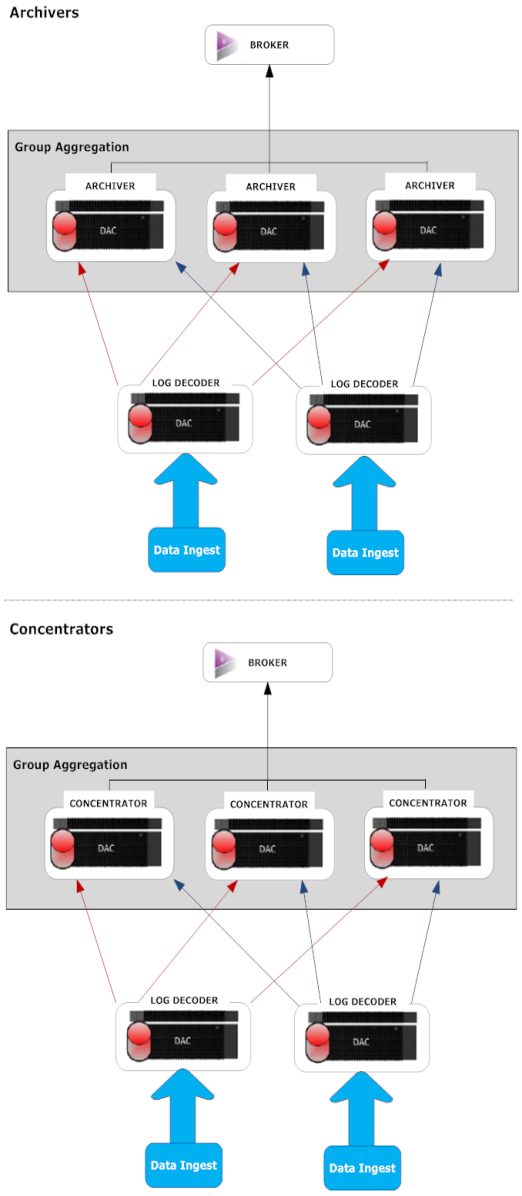
RSA recomienda la siguiente implementación para la agregación de grupos:

- Entre uno y dos Log Decoders
- Entre tres y cinco Archivers o Concentrators

Ventajas de usar la agregación de grupos

- Aumenta la velocidad de las consultas de RSA NetWitness® Platform.
- Mejora el rendimiento de las consultas agregadas (Count y Sum) en el ambiente.
- Mejora el rendimiento del servicio de investigación.
- Ofrece la opción de almacenar datos durante más tiempo con fines de investigación.

En el siguiente diagrama se ilustra la agregación de grupos.



Puede haber una cantidad indefinida de Archivers o Concentrators agrupados, los cuales forman un grupo de agregación. Los servicios Archiver o Concentrator del grupo dividen toda la sesión agregada entre ellos de acuerdo con la cantidad de sesiones definidas en el parámetro Sesiones máximas de agregación.

Por ejemplo, en un grupo de agregación que contiene dos servicios Archiver o dos servicios Concentrator con el parámetro Sesiones máximas de agregación configurado en 10,000, los servicios dividirían la sesión entre ellos como se ilustra en la siguiente tabla.

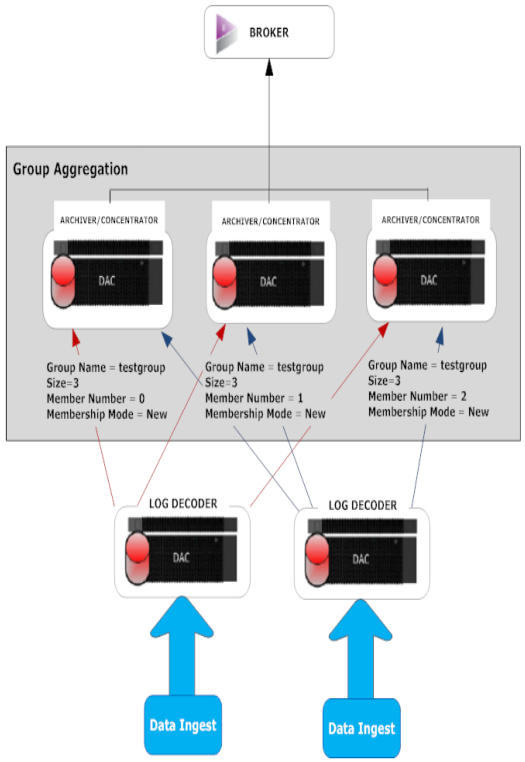
Archiver 0 o Concentrator 0	Archiver 1 o Concentrator 1
1 - 9,999	10,000 - 19,999
20,000 a 29,999	30,000 a 39,999
40,000 a 49,999	50,000 a 59,999

Configurar la agregación de grupos

Complete este procedimiento para configurar múltiples servicios Archiver o Concentrator como un grupo y compartir las tareas de agregación entre ellos.

Requisitos previos

Planee el diseño de la red para la agregación de grupos. La siguiente figura es un ejemplo de una configuración de agregación de grupos.



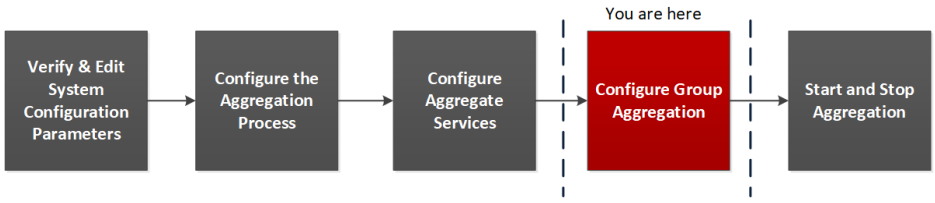
Asegúrese de comprender los parámetros de agregación de grupos de la siguiente tabla y de crear un plan de agregación de grupos.

Parámetro	Descripción
Nombre del grupo	Determina el grupo al cual pertenece el Archiver o el Concentrator. Puede agregar cualquier número de datos de agregación de grupos desde un Log Decoder. Log Decoder utiliza el parámetro Nombre del grupo para identificar los servicios Archiver o Concentrator que están trabajando juntos. Todos los servicios Archiver o Concentrator en el grupo deben tener el mismo nombre de grupo.
Tamaño	Determina la cantidad de servicios Archiver o Concentrator en el grupo de agregación.
Número de miembro	Determina la posición del Archiver o del Concentrator en el grupo de agregación. En el caso de un grupo de tamaño N, se debe configurar el número de miembro de 0 a N-1 en cada uno de los servicios Archiver o Concentrator del grupo de agregación. Por ejemplo: Si el tamaño del grupo de agregación es 2, el número de miembro de uno de los servicios Archiver o Concentrator se debe configurar en 0 y el del otro Archiver o Concentrator, en 1.
Modo de membresía	Hay dos modos de membresía: • Nuevo: Adición de un nuevo servicio Archiver o Concentrator como miembro del grupo de agregación existente o creación de un grupo de agregación. El servicio Archiver o Concentrator no agrega ninguna sesión existente desde el servicio, ya que otros miembros del grupo ya habrían agregado en él todas las sesiones. Este servicio Archiver o Concentrator agregará solamente nuevas sesiones a medida que aparecen en el servicio. • Reemplazo: Reemplazo de un miembro del grupo de agregación existente. El Archiver o el Concentrator comenzarán la agregación a partir de la sesión más antigua disponible en el servicio desde el cual realiza la agregación.

Nota: El parámetro de modo de membresía tiene efecto solamente cuando no se han agregado sesiones desde el servicio. Después de agregar algunas sesiones este parámetro no tiene ningún efecto.

Configurar la agregación de grupos

En este flujo de trabajo se muestran los procedimientos que se realizan para configurar la agregación de grupos.



Complete los pasos siguientes para configurar la agregación de grupos.

1. Configure varios servicios Archiver o Concentrator en el ambiente. Asegúrese de agregar el mismo Log Decoder como origen de datos en todos los servicios.
2. Realice lo siguiente en todos los servicios de Archiver o Concentrator que desea que formen parte

del grupo de agregación:

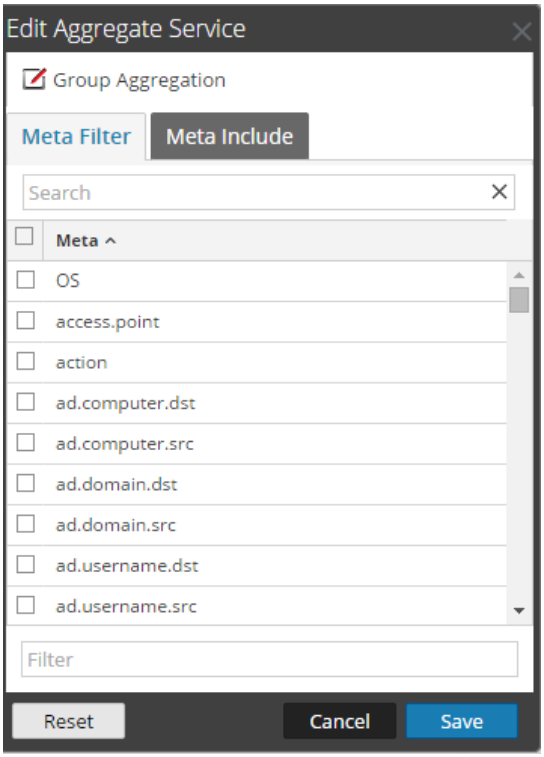
a. Vaya a **ADMINISTRAR > Servicios**.

b. Seleccione el servicio Archiver o Concentrator y, en la columna **Acciones**, seleccione **Ver > Configuración**.
Se muestra la vista Configuración del servicio de Archiver o Concentrator.

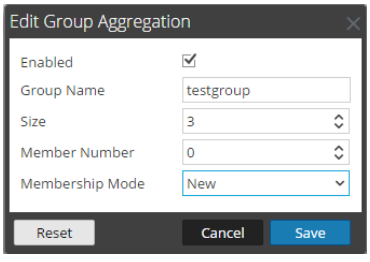
c. En la sección **Servicios agregados**, seleccione **Log Decoder**.

d. Haga clic en Toggle Service para cambiar el estado de Log Decoder a offline si se encuentra en línea.

e. Haga clic en .
Se muestra el cuadro de diálogo **Editar servicio agregado**.



f. Haga clic en Group Aggregation.
Se muestra el cuadro de diálogo **Editar agregación de grupos**.



g. Seleccione la casilla de verificación **Activado** y configure los siguientes parámetros:

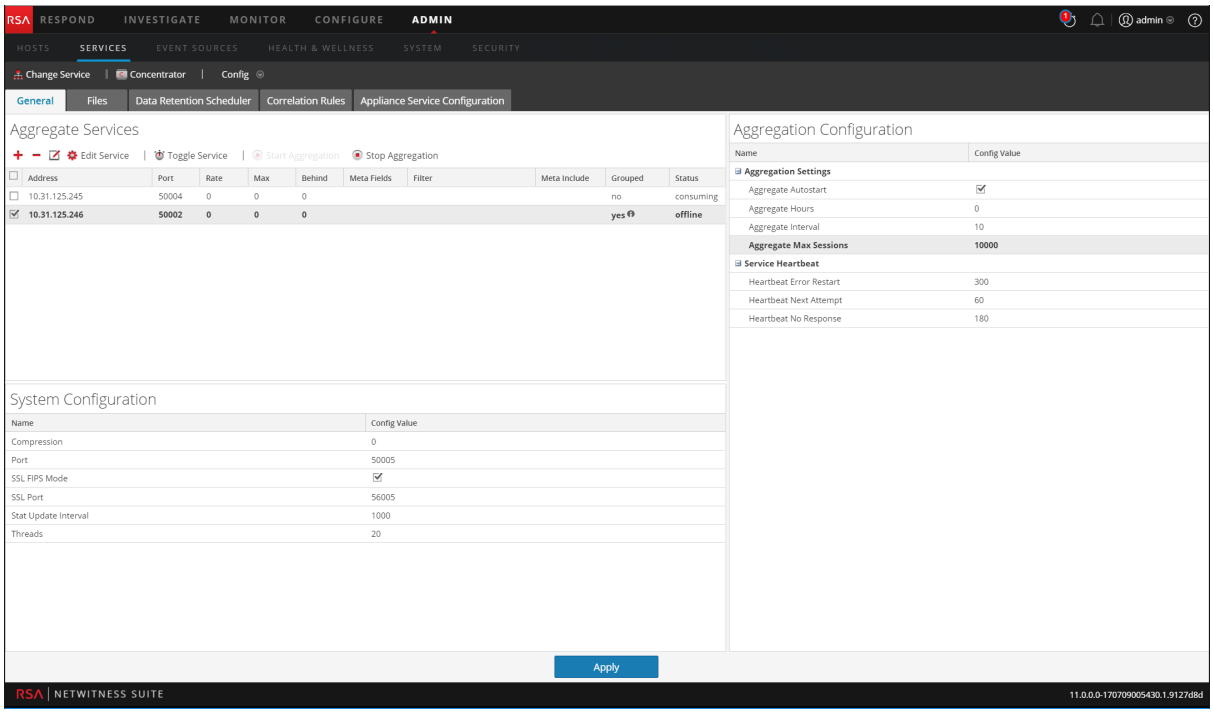
- En el campo **Nombre del grupo**, escriba el nombre del grupo.
- En el campo **Tamaño**, seleccione la cantidad de servicios Archiver o Concentrator en el grupo de agregación.
- En el campo **Número de miembro**, seleccione la posición de Archiver o Concentrator en el grupo de agregación.
- En el menú desplegable **Modo de membresía**, seleccione el modo.

h. Haga clic en **Guardar**.

i. En la página Vista de configuración del servicio, haga clic en **Aplicar**.

j. Realice del **paso b** al **paso i** en todos los demás servicios Archiver o Concentrator que deben ser parte de la agregación de grupos.

3. En la sección **Configuración de agregación**, configure el parámetro **Sesiones máximas de agregación** en **10000**.



Categorías híbridas en el servidor de NW

Se puede instalar categorías híbridas, como las categorías de servicio Log Hybrid y Network (Packet), en un host físico serie 6 (R640). Esto le brinda la capacidad de conectar varios dispositivos de almacenamiento externo de PowerVault al host físico de la serie 6 (R640).

Segundo servidor Endpoint

Complete el siguiente procedimiento para implementar un segundo servidor Endpoint.

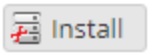
1. Configure un nuevo host en NetWitness Platform.
   - Para un host físico, complete los pasos del 1 al 14, ambos inclusive, en la sección "Tarea 2: Instalar 11.3 en otros hosts de componentes", en "Tareas de instalación" de la *Guía de instalación de hosts físicos*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
   - En el caso de un host virtual, siga las instrucciones de la *Guía de instalación de hosts virtuales* de la sección “Tarea 2: Instalar 11.3 en otros hosts de componentes” en el “Paso 4. Instalar RSA NetWitness Platform”.
2. Acceda mediante el protocolo SSH al host que se configuró en el paso 1.
3. Ejecute la siguiente cadena de comandos.
   `mkdir -p /etc/pki/nw/nwe-ca`

   Nota: No es necesario modificar los permisos.
4. Copie los siguientes dos archivos desde el servidor de Endpoint implementado anteriormente al servidor Endpoint nuevo/segundo:
   `/etc/pki/nw/nwe-ca/nwerootca-cert.pem`
   `/etc/pki/nw/nwe-ca/nwerootca-key.pem`
5. Instale Endpoint 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, Endpoint Server II) y haga clic en

      .
      Se muestra el cuadro de diálogo **Instalar servicios**.

   d. Seleccione **Endpoint** en **Tipo de host** y haga clic en **Instalar**.

Host del servidor de NW semiactivo en espera

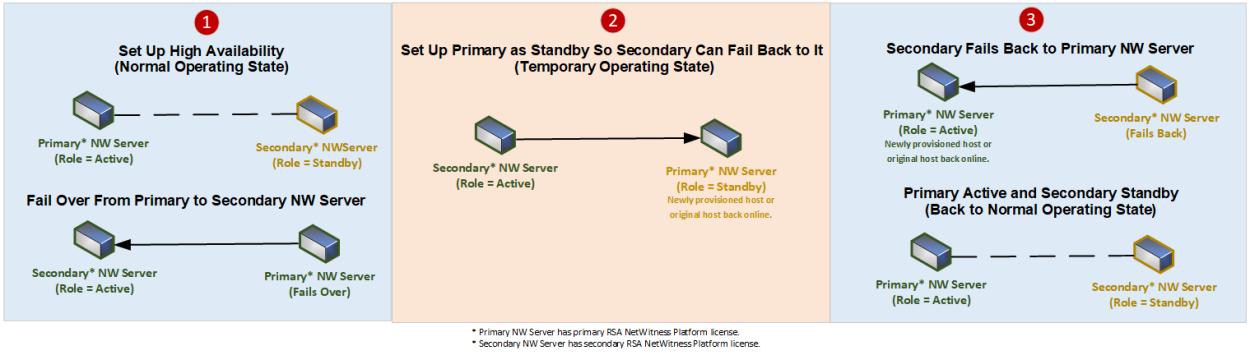
El servidor de NW semiactivo en espera duplica los componentes críticos y las configuraciones del host del servidor de NW activo para aumentar la confiabilidad.

Un servidor de NW secundario permanece en la función en espera y, cuando está configurado, recibe respaldos del servidor de NW primario en la función activa en intervalos regulares. Si el servidor de NW primario falla (se desconecta), se debe ejecutar el procedimiento de conmutación por error, lo que permite que el servidor de NW secundario asuma la función activa.

Al configurar un servidor de NW secundario como semiactivo en espera, se hace referencia a una falla o un switch programado desde el servidor de NW primario al servidor de NW secundario como una conmutación por error. Puede realizar una conmutación por recuperación para volver al estado operativo normal (es decir, servidor de NW primario en la función activa y el servidor de NW secundario en la función en espera).

En el siguiente diagrama se ilustra el proceso de conmutación por error y conmutación por recuperación.

1. Configure el servidor de NW secundario como en espera (configuración inicial). Este es el estado normal de funcionamiento.
2. El servidor de NW primario realiza una conmutación por error al servidor de NW secundario. Después de la conmutación por error, vuelva a poner en línea el servidor de NW primario y configúrelo en la función en espera. Este es un estado operativo temporal.
3. Vuelva a generar una conmutación por error del servidor de NW secundario al primario. El servidor de NW primario regresa a la función activa y el secundario regresa a la función en espera. Este es el estado normal de funcionamiento.



IMPORTANTE: Durante una conmutación por recuperación, se debe asignar la misma dirección IP que el servidor de NW primario al servidor de NW secundario, de modo que pueda asumir la función activa.

Procedimientos

Complete la siguiente tarea para configurar un servidor de NW secundario en la función en espera para conmutación por error:

- Configure un servidor de NW secundario en la función en espera.

Cuando sea necesario, complete las siguientes tareas para mantener la alta disponibilidad.

- Realice una conmutación por error del servidor de NW primario al servidor de NW secundario.
- Realice una conmutación por recuperación del servidor de NW secundario al servidor de NW primario.

Escenario planificado de conmutación por recuperación

Este escenario se produce cuando se programa una conmutación por error (consulte **Conmutación por error planificada** en el paso 3 del procedimiento Conmutación por error de servidor de NW primario a servidor de NW secundario). No es necesario hacer nada después de que se complete la conmutación por error.

Escenario de conmutación por error requerido sin sustitución de hardware

Este escenario ocurre cuando falla el servidor de NW primario (consulte el tema *Conmutación por error necesaria* en el paso 3 del tema Conmutación por error de servidor de NW primario a servidor de NW secundario), pero se puede recuperar fácilmente sin necesidad de volver a crear una imagen (como, por ejemplo, si el servidor de NW activo está dañado o no cuenta con suficiente RAM). No es necesario ejecutar `nwsetup-tui` y no es necesario que se ponga en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294) para restablecer correctamente el licenciamiento cuando:

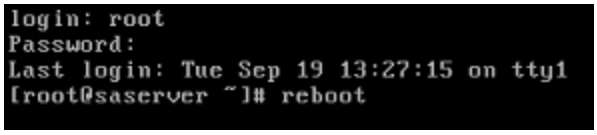
1. El servidor activo (servidor de NW primario) realiza una conmutación por error al servidor en espera (servidor de NW secundario) y ese host secundario asume temporalmente la función del servidor de NW activo.
2. Puede corregir el problema con el servidor de NW primario (por ejemplo, instalar RAM adicional) y realizar una conmutación por recuperación desde el host secundario.

Escenario de conmutación por error requerido con sustitución de hardware

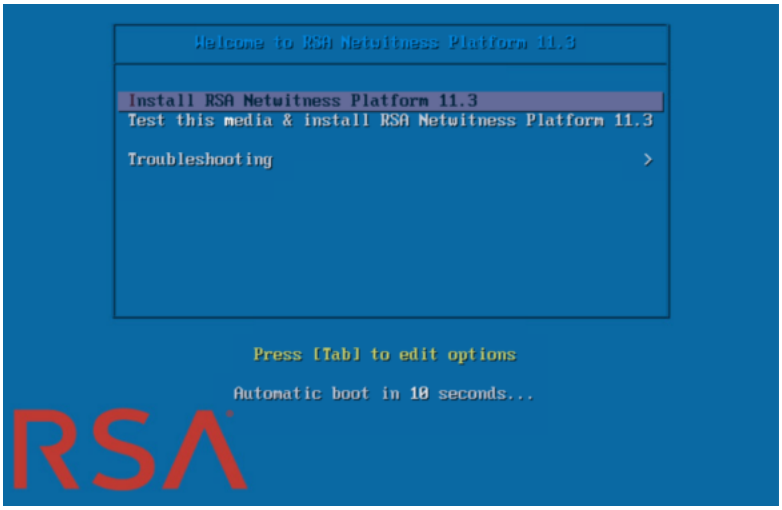
Este escenario ocurre cuando el servidor de NW activo falla completamente y el hardware requiere sustitución; por ejemplo, recibirá una autorización de devolución de mercancías (RMA). Debe ejecutar la reconfiguración del host con `nwsetup-tui` y ponerse en contacto con el servicio al cliente (https://community.rsa.com/docs/DOC-1294) para restablecer correctamente el licenciamiento. Si se opta por reconstruir el host sustituto como uno en espera temporal (por ejemplo, hasta que se produzca una conmutación por recuperación programada), se debe responder "**Sí**" al indicador **Modo de recuperación de host en espera** `nw-setup-tui` al configurar el host como uno temporal en espera para conmutación por recuperación (consulte el paso 4 del procedimiento Configurar el servidor de NW secundario en la función en espera para el contexto de este indicador).

Configurar el servidor de NW secundario en la función en espera

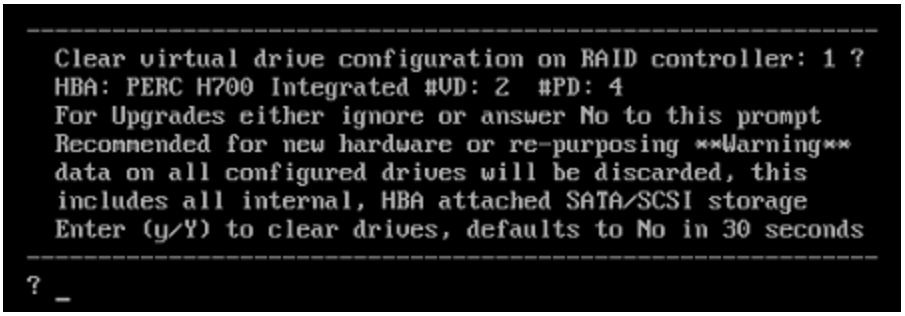
1. Antes de instalar un host del servidor de NW secundario para la función en espera, asegúrese de lo siguiente:
   a. el servidor de NW primario está ejecutando 11.3.
   b. Todos los hosts de componentes ejecutan 11.3
   En el caso de lo siguiente:
   - Instalación de NetWitness Platform 11.3, siga las instrucciones de la *Guía de instalación de hosts físicos de RSA NetWitness Platform para la versión 11.3* o la *Guía de instalación de hosts virtuales de RSA NetWitness Platform para la versión 11.3*.
   - Actualización de 10.6.x a 11.3, siga las instrucciones de la *Guía de actualización de hosts físicos de RSA NetWitness Platform de la versión 10.6.6.x a 11.3* o la *Guía de instalación de hosts virtuales de RSA NetWitness Platform para la versión 11.3*
   - Actualización de 11.x a 11.3, siga las instrucciones de la *Guía de actualización de RSA NetWitness Platform de la versión 11.x a 11.3*.
   Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.
2. Cree una imagen base en el servidor de NW secundario:
   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 unidad flash de arranque mediante **Etcher®** u otras herramientas de digitalización adecuada, de modo de grabar un sistema de archivos Linux en la unidad USB. Consulte las *RSA NetWitness® PlatformInstrucciones para una unidad de compilación* para obtener información sobre cómo crear una unidad de compilación desde la imagen ISO. Etcher está disponible en: https://etcher.io.
   - 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.



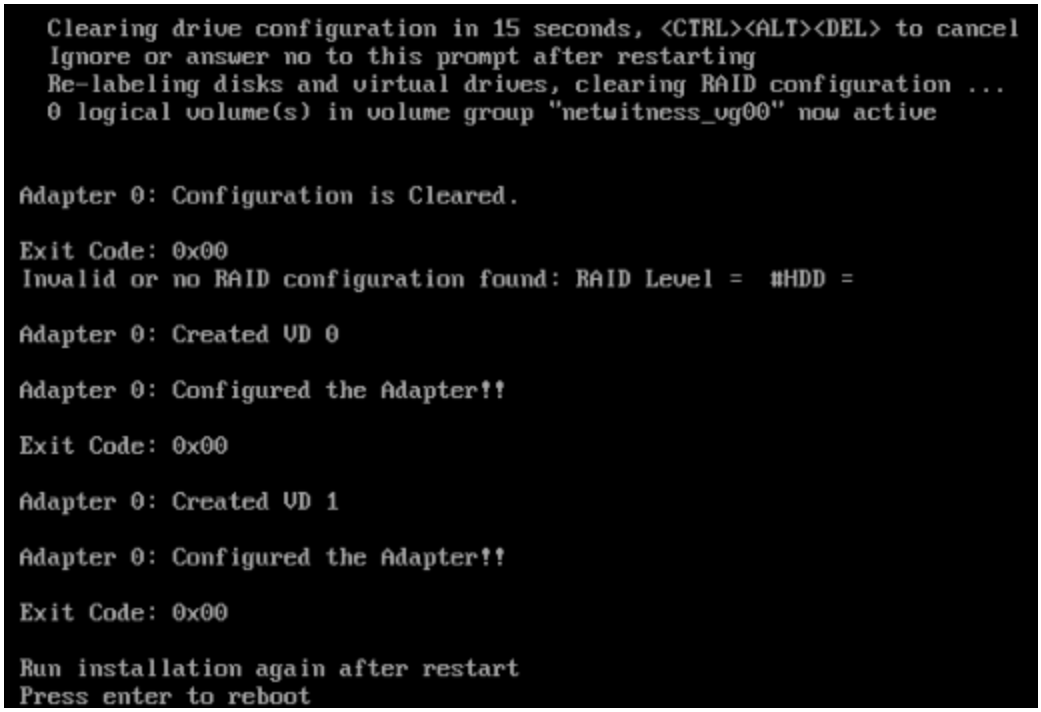
c. Seleccione **F11** (menú de arranque) durante el reinicio para seleccionar un dispositivo de arranque y arrancar desde los medios conectados.
Después de algunas comprobaciones del sistema durante el arranque, se muestra el siguiente menú de instalación **Bienvenido a RSA NetWitness Platform 11.3**. Los gráficos del menú se generarán de manera diferente si usa un medio flash USB físico.



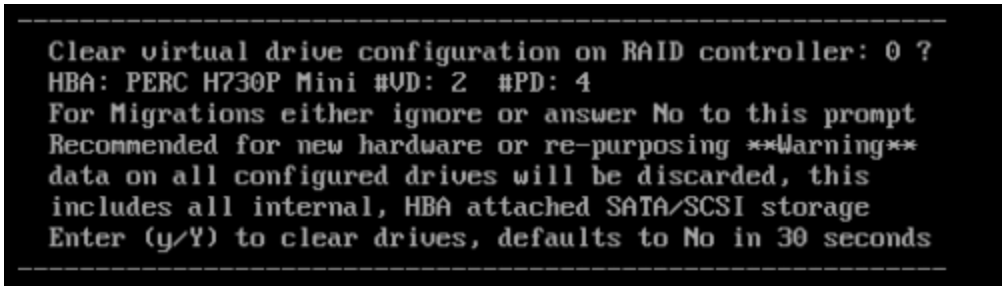
d. Seleccione **Instalar RSA Netwitness Platform 11.3** (selección predeterminada) y presione **Intro**.
El programa de instalación se ejecuta y se detiene en el indicador **Ingresar (s/S) para borrar las unidades** que le solicita formatear las unidades.



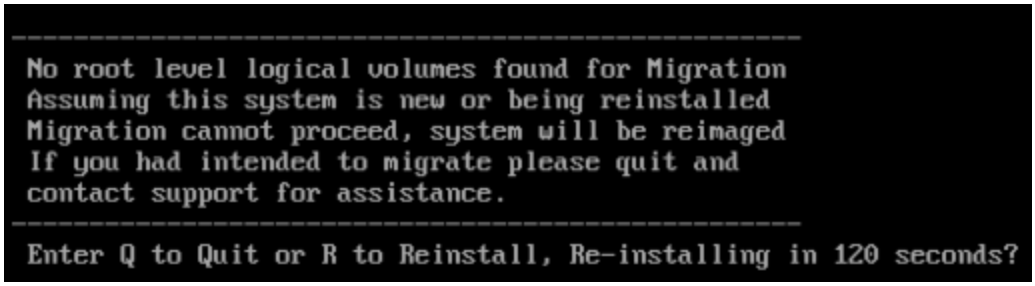
e. Escriba **S** para continuar.
La acción predeterminada es No, de modo que si pasa por alto el indicador, se seleccionará No en 30 segundos y las unidades no se borrarán. Se muestra el indicador **Presione Intro para reiniciar**.



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.

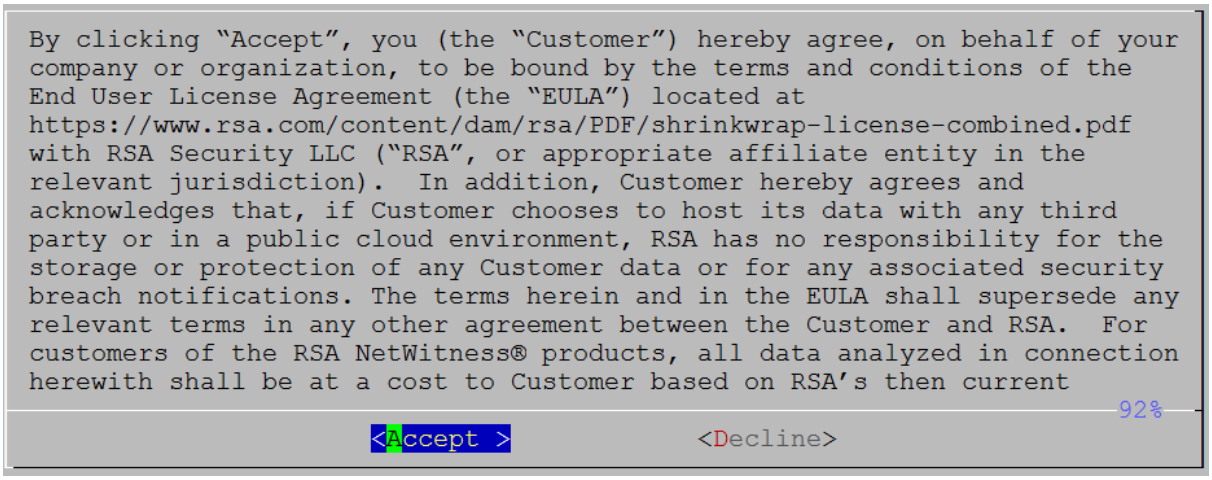
Precaución: No reinicie los medios conectados (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación).

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

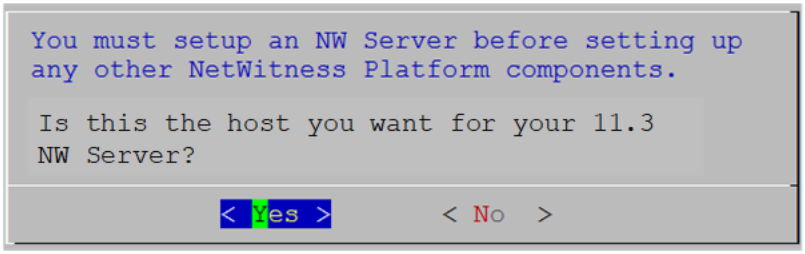
2. Ejecute el comando `nwsetup-tui`.

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.) Durante el programa de instalación, cuando se le solicite la configuración de red del host, asegúrese de especificar la misma configuración de red que se utilizó para la instalación original de 11.x en este host (debe ser exactamente la misma).

Esto inicia `nwsetup-tui` (programa de instalación) y se muestra el EULA.

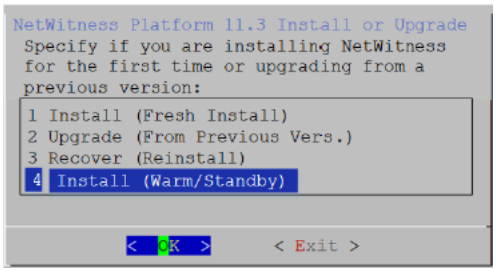


3. Use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador **¿Es este el host que desea para el servidor de NW 11.3?**.

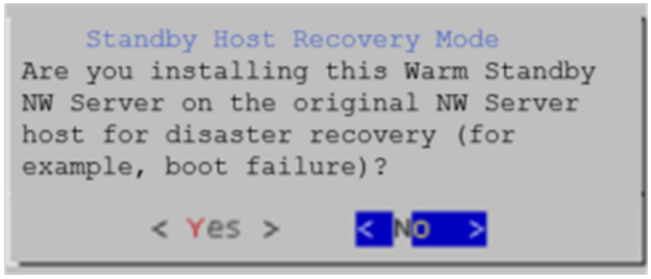


   Su respuesta a este indicador identifica un host como el primario o el secundario durante una instalación nueva (y la respuesta seleccionada se mantiene constante, independientemente de la función actual o futura, que está activa o en espera para el host).

4. Use la tecla de tabulación para ir a **Sí** y presione **Intro**.
   Se muestra el indicador **Instalar o Actualizar**.

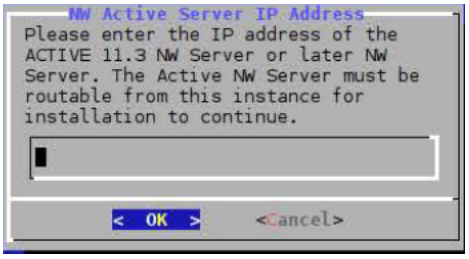


5. Use la tecla de tabulación para desplazarse a **4 Instalar (en espera semiactiva)** y presione **Intro**.
   Se muestra el indicador Modo de recuperación de host en espera.

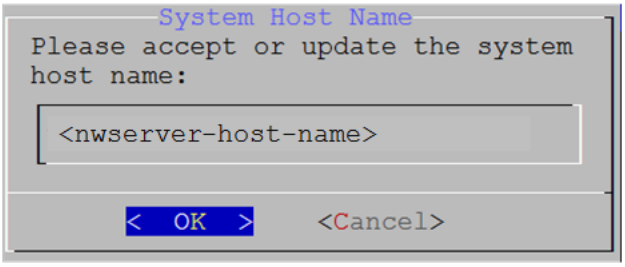


6. Use la tecla de tabulación para desplazarse a:
   - **No** y presione **Intro** para configurar un servidor de NW secundario con la función en espera (en la mayoría de los escenarios comunes).
   - **Sí** y presione **Intro** para configurar un host que se usaba anteriormente como servidor de NW primario con la función en espera, de modo que pueda ejecutar una conmutación por error y conmutación por recuperación (un escenario menos común).

   Se muestra el indicador Dirección IP del servidor de NW activo.



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

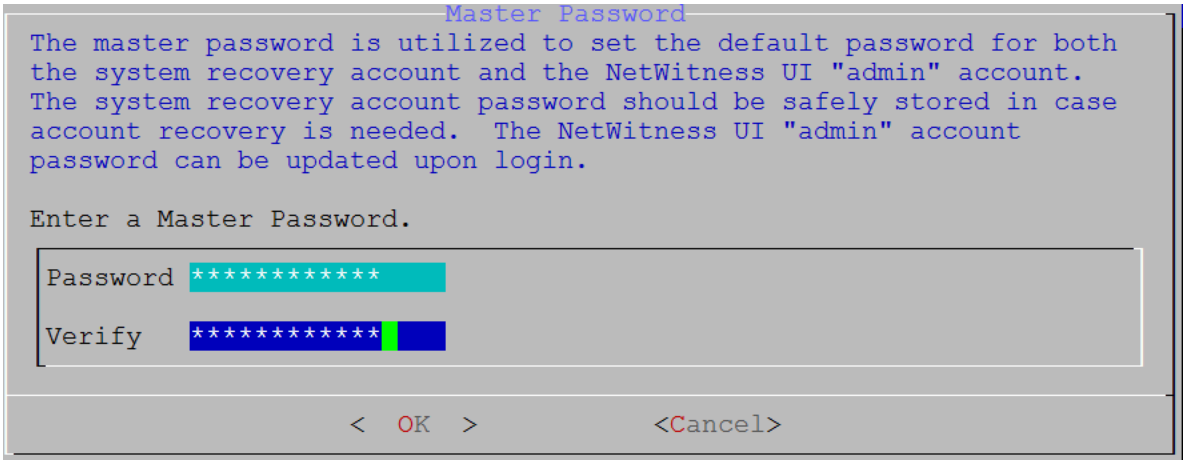
8. Presione **Intro** si desea mantener este nombre. Si no edita el nombre del host, use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para cambiarlo.
   Se muestra el indicador **Contraseña maestra**.

   Nota: Se debe usar las mismas credenciales de administrador maestro y de implementación en el host del servidor de NW semiactivo en espera que se utilizó para el host del servidor de NW activo.

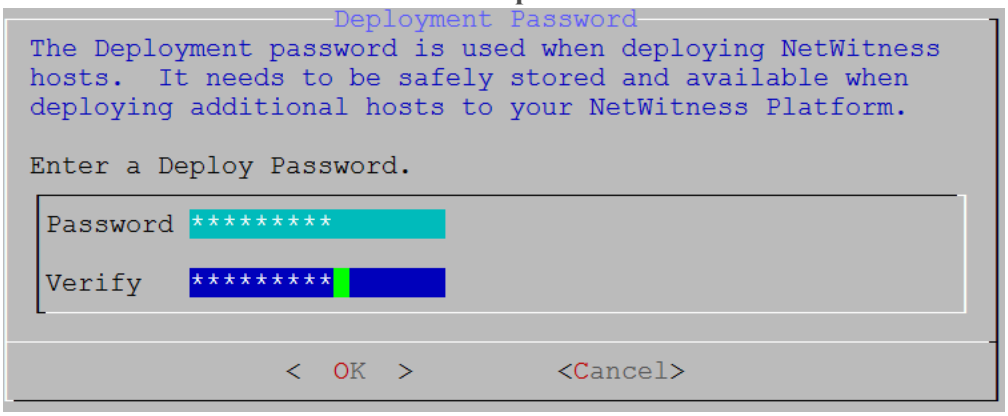
   Los caracteres de la siguiente lista son compatibles para Contraseña maestra y Contraseña de implementación:

   - Símbolos: ! @ # % ^ +
   - 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 { } [ ] ( ) / \ ' " ` ~ ; : .< > -

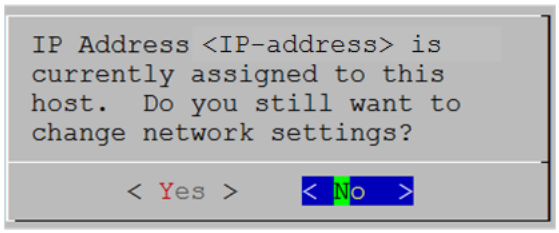


9. Escriba la **Contraseña**, use la flecha hacia abajo para desplazarse hasta **Verificar**, vuelva a escribir la contraseña, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.
   Se muestra el indicador **Contraseña de implementación**.



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.

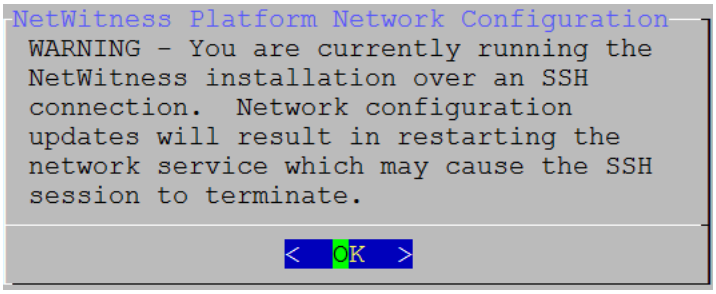
    - Si el programa de instalación encuentra una dirección IP válida para este host, se muestra el siguiente indicador.

      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.

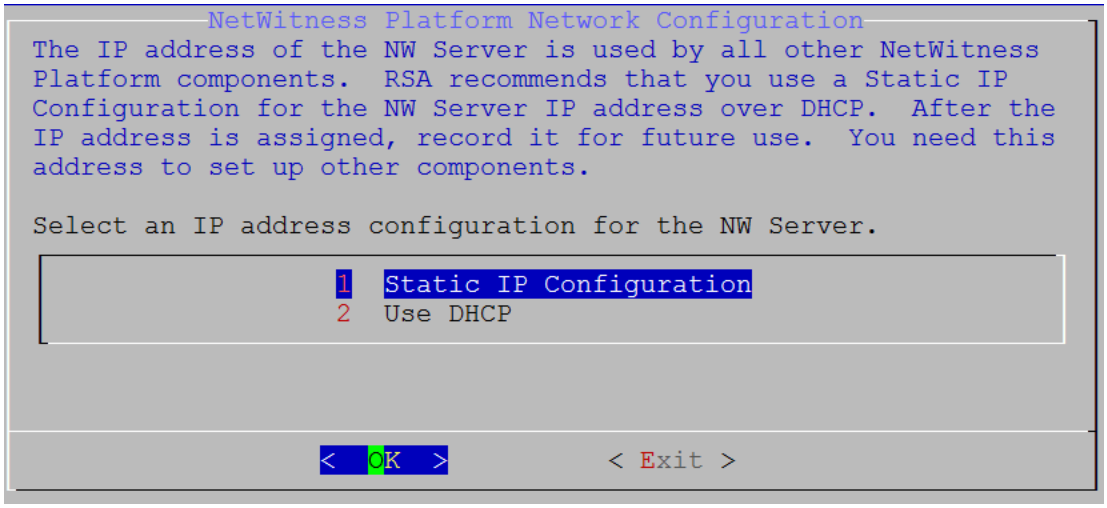
      Nota: Si se conecta directamente desde la consola del host, no se mostrará la siguiente advertencia.

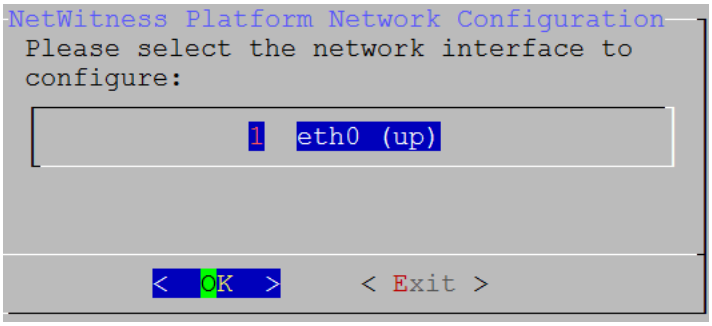
      Presione **Intro** para cerrar el indicador de advertencia.

    - 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.

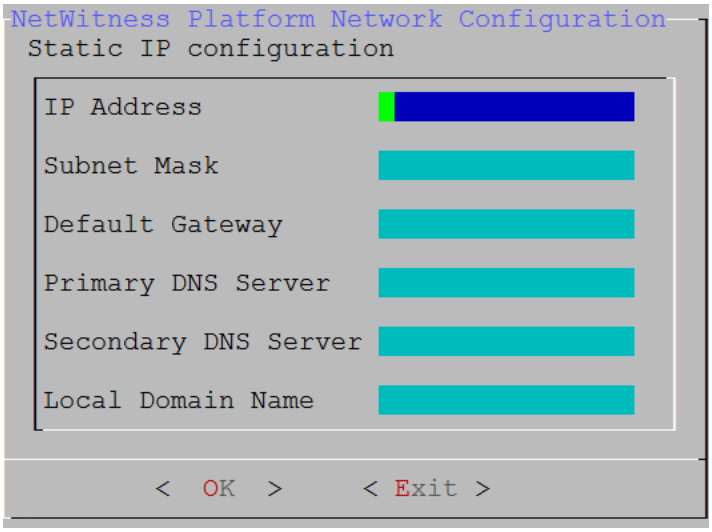
- Si el programa de instalación no encontró una configuración de IP o usted decidió cambiar la configuración de IP existente, se muestra el indicador **Configuración de red**.



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**.



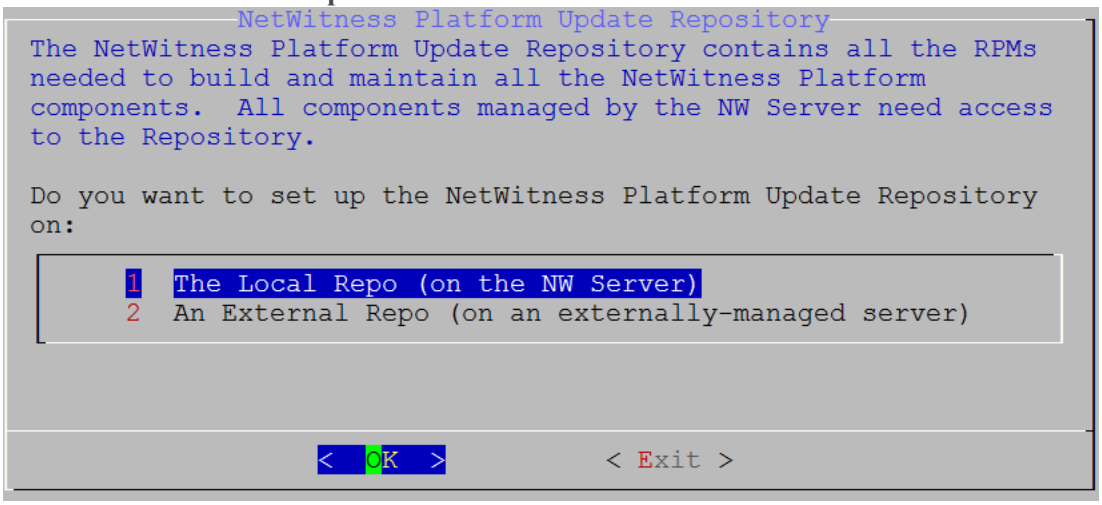
12. Use la flecha hacia abajo para desplazarse hasta la interfaz de red que desea, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**. Si no desea continuar, use la tecla de tabulación para ir a **Salir**
    .Se muestra el siguiente indicador **Configuración de IP estática**.



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 `Invalid <field-name>`.

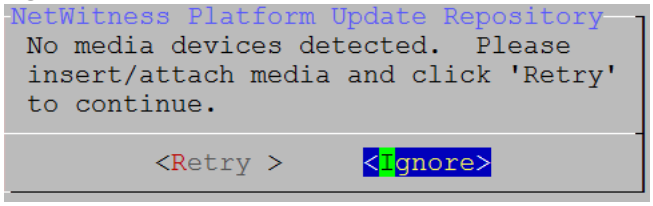
    Precaución: Si selecciona un **servidor DNS**, asegúrese de que sea el servidor DNS correcto y que el host pueda acceder a él antes de continuar con la instalación.

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

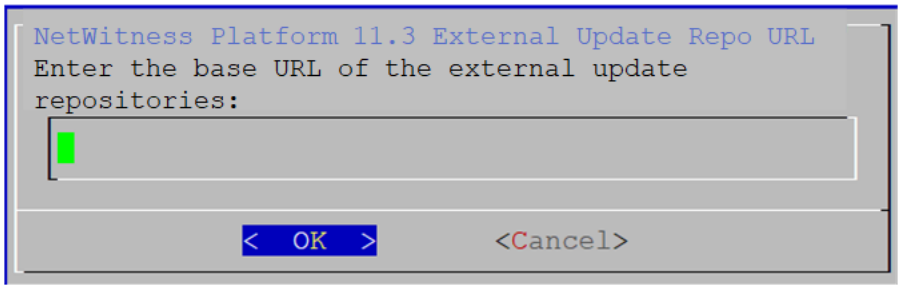


14. Presione **Intro** para elegir **Repositorio local** en el servidor de NW.
    Si desea usar un repositorio externo, use la flecha hacia abajo para desplazarse hasta **Repositorio externo**, use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

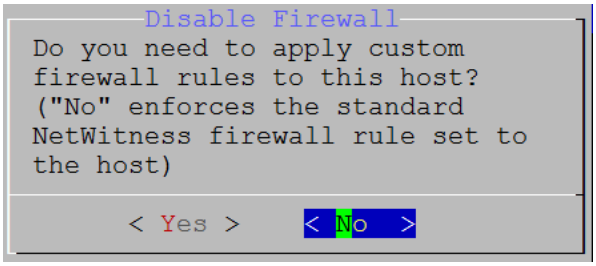
    - Si selecciona **1 El repositorio local (en el servidor de NW)** en el programa de instalación, asegúrese de que estén conectados los medios adecuados al host (medios que contienen el archivo ISO, por ejemplo, una unidad de compilación) desde los cuales puede instalar NetWitness Platform 11.2.0.0. Si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



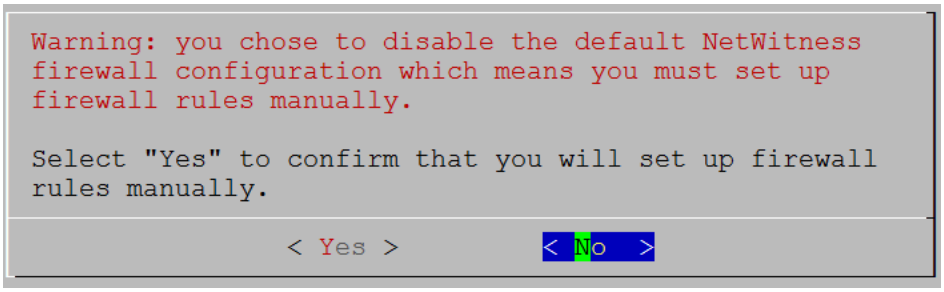
- Si selecciona **2 Un repositorio externo (en un servidor administrado externamente)**, la interfaz del usuario le solicita que indique una dirección URL. Los repositorios otorgan acceso a las actualizaciones de RSA y a las actualizaciones de CentOS. Consulte Apéndice B. Crear un repositorio externo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



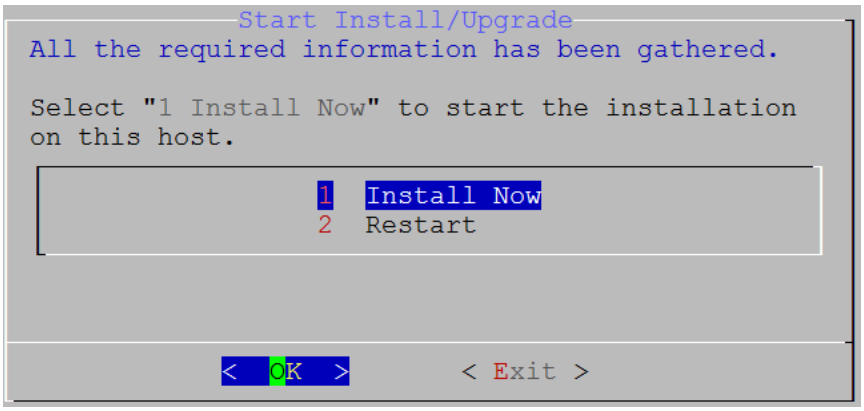
Ingrese la dirección URL base del repositorio externo de NetWitness Platform y haga clic en **Aceptar**. Se muestra el indicador **Iniciar instalación**.
Consulte "Configurar un repositorio externo con actualizaciones de RSA y del SO" en la sección "Procedimientos de hosts y servicios" de la *Guía de 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.



15. 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**, se confirma su selección (seleccione **Sí** nuevamente). Si desea usar la configuración del firewall estándar, seleccione **No**.

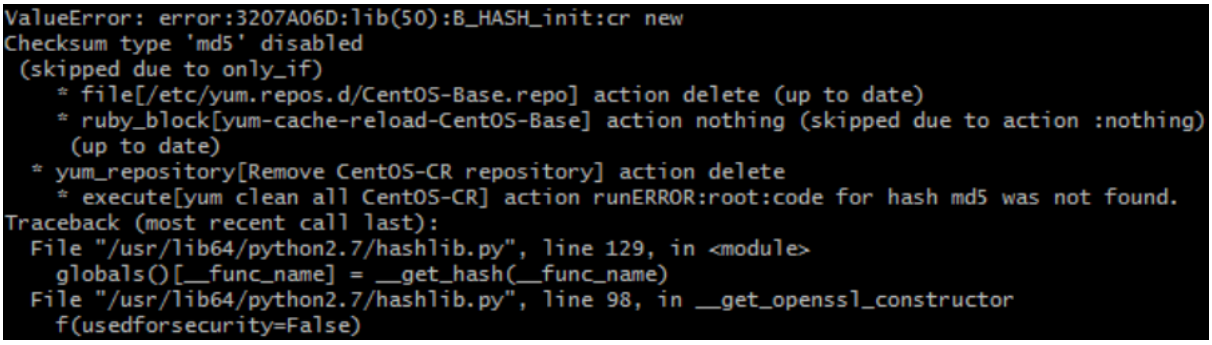


Se muestra el indicador **Iniciar instalación/actualización**.



16. Presione **Intro** para instalar 11.3 en el servidor de NW.
    Cuando se muestra **Instalación completa**, terminó de instalar el servidor de NW 11.3 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.



17. Obtenga una licencia para el servidor de NW secundario.
    a. Inicie sesión en la interfaz del usuario del servidor de NW secundario, haga clic en **ADMINISTRAR** > **Sistema** > **Info** y anote el **Indicador de servidor de licencia** en **Información de la versión**.
    b. Acceda mediante el protocolo SSH al servidor de NW primario.
    c. Edite el archivo `/opt/netwitness/flexnetls/local-configuration.yaml` y agregue `back up hostid` (es decir, el **Identificador del servidor de licencia**).
    Este es un ejemplo de la sección del archivo `local-configuration.yaml` antes de agregar el **Identificador de servidor de licencia**.

```
# Hostid of the backup server, if in fail over configuration.
#backup-hostid:
```

    Este es un ejemplo de la sección del archivo `local-configuration.yaml` después de agregar la dirección MAC (por ejemplo, `000c2918c80d`) del host del servidor de NW semiactivo en espera.

```
# Hostid of the backup server, if in fail over configuration.
backup-hostid: "000c2918c80d"
```

d. Reinicie los servicios de fneserver.
`systemctl restart flexnetls-RSALM`

e. (Condicional) Si se prohibe a la implementación de NetWitness Platform el acceso a Internet (sistema aislado), debe:

i. Descargar la solicitud de funcionalidad desde la interfaz del usuario de NetWitness Platform.

ii. Cargar la solicitud a FNO.

iii. Cargar la respuesta desde FNO a la interfaz del usuario de NetWitness Platform.

18. Programar el respaldo del servidor de NW primario y la copia de estos datos respaldados en el servidor de NW secundario.

a. Acceda mediante el protocolo SSH al servidor de NW primario.

b. Ejecute los siguientes comandos.
`/opt/rsa/saTools/bin/schedule-standby-admin-data-sync -di <warm-standby-admin-server-ip>`
Esto respalda los datos del servidor de NW primario y copia el archivo de copia de seguridad en el servidor de NW secundario a diario para su uso futuro durante la conmutación por error. También programa el respaldo y la copia para ejecutarse a diario. Puede mostrar la ayuda para el script `schedule-standby-admin-data-sync` con la siguiente cadena de comandos.
`/opt/rsa/saTools/bin/schedule-standby-admin-data-sync --help`
Esto regresa la siguiente ayuda, mediante la cual se puede personalizar la copia de seguridad de datos del host (como la frecuencia de respaldo).

```
Schedule Data Synch between AdminServer and Standby AdminServer
Script also executes a synchronization each time.

Usage:
schedule-standby-admin-data-sync command [options]

Commands:
-h, --help                          Display Help
-d, --daily                         Schedule daily data synchronization
-w, --weekly                        Schedule weekly data synchronization
-c, --custom <crontab formatted> Schedule custom data synchronization
                                    i.e. to schedule for midnight on 1st
                 -                  and 10th of the month: '0 0 1,10 * *'
-i, --standby-ip <ip address>   IP address of standby Admin Server
-v, --verbose                   Enable verbose output
```

Conmutación por error de un servidor de NW primario a un servidor de NW secundario

Inicialmente, el servidor de NW primario realiza una conmutación por error al servidor de NW secundario. Subsiguientemente, se hace una conmutación por error del servidor de NW secundario al servidor de NW primario, lo cual se denomina conmutación por recuperación. Complete el siguiente procedimiento para realizar una conmutación por recuperación desde el servidor de NW primario al servidor de NW secundario.

1. Acceda mediante el protocolo SSH al servidor de NW secundario.
2. Ejecute el script `nw-failover` con los argumentos correspondientes. Por ejemplo:
   `nw-failover --make-active --ip-address <active-nw-server-host-ip> --name <primary-nw-server-hostname>`
   Una vez que se completa el script, se muestra el siguiente mensaje.
   `*** Please update network ip and reboot host to complete the fail over process ***`
3. Actualice la configuración de red de CentOS para intercambiar las direcciones IP.
   - **Conmutación por error planificada:** El servidor de NW primario no falló:
     a. Acceda mediante el protocolo SSH al servidor de NW primario.
     b. Asigne una dirección IP no utilizada al servidor de NW primario.
     c. Ejecute el script de conmutación por error con los argumentos apropiados para asignar la función en espera al servidor de NW primario. Por ejemplo:
        `nw-failover --make-standby --ip-address <unused-ip-or-previous-standby-ip> --name <previous-standby-nw-server-hostname>`
     d. Apague el servidor de NW primario.
     e. Acceda mediante el protocolo SSH al servidor de NW secundario.
     f. Asigne la dirección IP del servidor de NW primario que registró al servidor de NW secundario.
   - **Conmutación por error requerida**: El servidor de NW primario no falló:
     a. Acceda mediante el protocolo SSH al servidor de NW secundario.
     b. Asigne la dirección IP del servidor de NW primario al servidor de NW secundario.

     > **Nota:** Si se enfrenta una falla catastrófica, es posible que se deba aprovisionar un nuevo host o volver a crear una imagen del servidor de NW primario y completar el procedimiento Configurar el servidor de NW secundario en espera para este host a fin de crear un nuevo servidor de NW primario, de modo que pueda realizar una conmutación por recuperación a él.
4. Reinicie el host.

5. Asegúrese de que la conmutación por error esté configurada correctamente.
   a. Acceda mediante el protocolo SSH al servidor de NW en espera.
   b. Asegúrese de que el servidor de NW activo:
      i. Puede resolver su UUID (identificador único universal).
      ```
      source /usr/lib/netwitness/bootstrap/resources/nwcommon 2>/dev/null > /dev/null
      nslookup $(getNodeID)
      ```
      `nslookup` debería devolver la dirección IP del servidor de NW activo actual.
      ii. Coincide con la misma dirección IP que se resolvió en el paso anterior

Conmutación por error del servidor de NW secundario al servidor de NW primario

Después de una conmutación por error del servidor de NW primario al servidor de NW secundario, se debe realizar una conmutación por recuperación a la configuración original del servidor de NW primario en la función activa y el servidor de NW secundario en la función en espera.

Esencialmente, se siguen los mismos pasos que se describen en Conmutación por error del servidor de NW primario al servidor de NW secundario para realizar una conmutación por recuperación a la configuración original (es decir, de servidor de NW primario activo y servidor de NW secundario en espera). La diferencia es que ahora se debe realizar una conmutación por error desde el servidor de NW secundario al servidor de NW primario.

Arquitectura y puertos de red

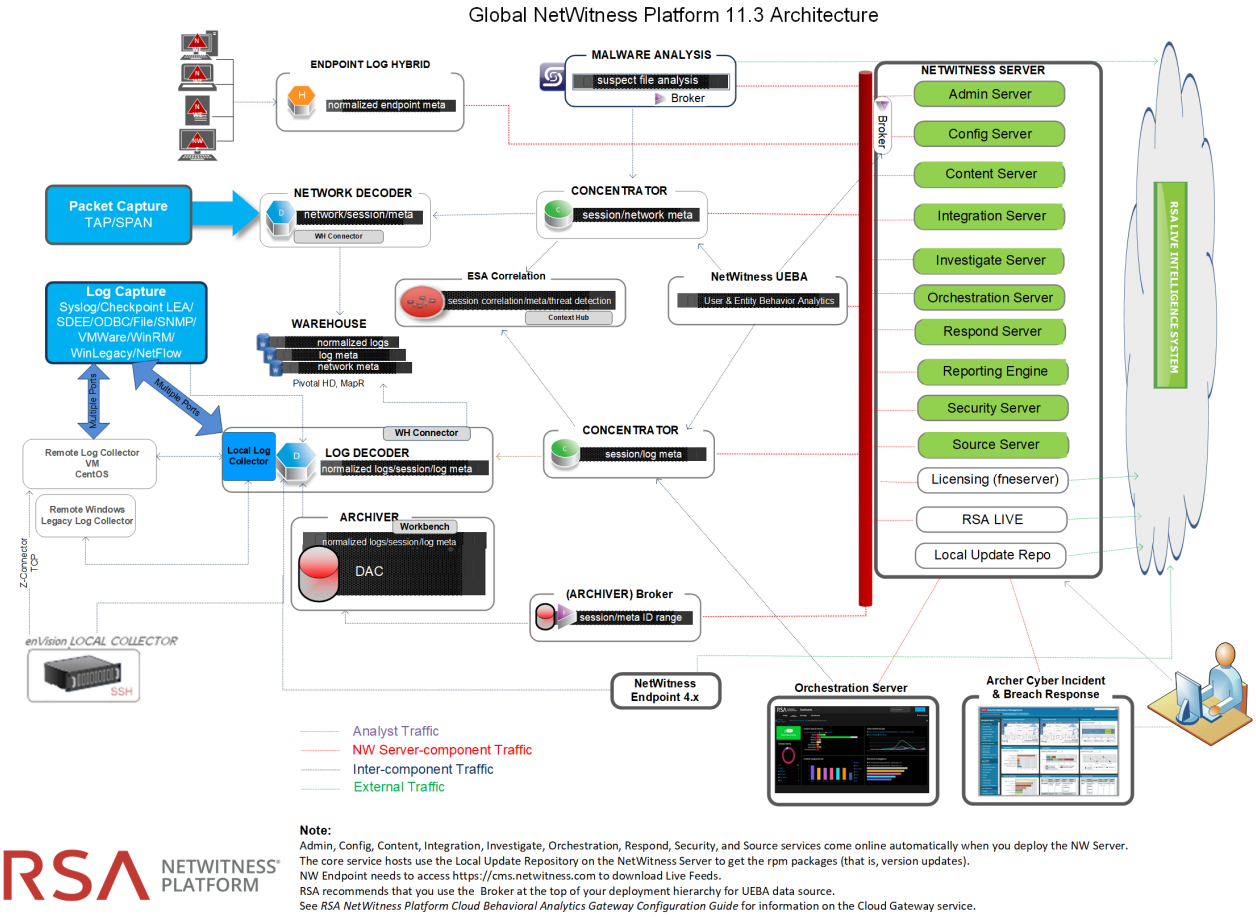
Consulte el diagrama y la tabla de puertos siguientes para asegurarse de que todos los puertos pertinentes estén abiertos para los componentes de la implementación de NetWitness Platform de modo que exista comunicación entre ellos.

Consulte Arquitectura de NetWitness Endpoint al final de este tema para ver los diagramas de arquitectura de Endpoint individuales.

Diagrama de la arquitectura de red de NetWitness Platform

En el siguiente diagrama se ilustra la arquitectura de red de NetWitness Platform, incluidos todos los productos que la componen.

Nota: Los hosts de NetWitness Platform Core deben ser capaces de comunicarse con el Servidor de NetWitness (servidor primario en una implementación de múltiples servidores) a través del puerto UDP 123 para la sincronización horaria de NTP.



Note:
Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server.
The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).
NW Endpoint needs to access https://cms.netwitness.com to download Live Feeds.
RSA recommends that you use the Broker at the top of your deployment hierarchy for UEBA data source.
See *RSA NetWitness Platform Cloud Behavioral Analytics Gateway Configuration Guide* for information on the Cloud Gateway service.

Diagrama de la arquitectura de red de NetWitness Network (packets)

En los siguientes diagramas se muestra la arquitectura de red de NetWitness Network (paquetes).

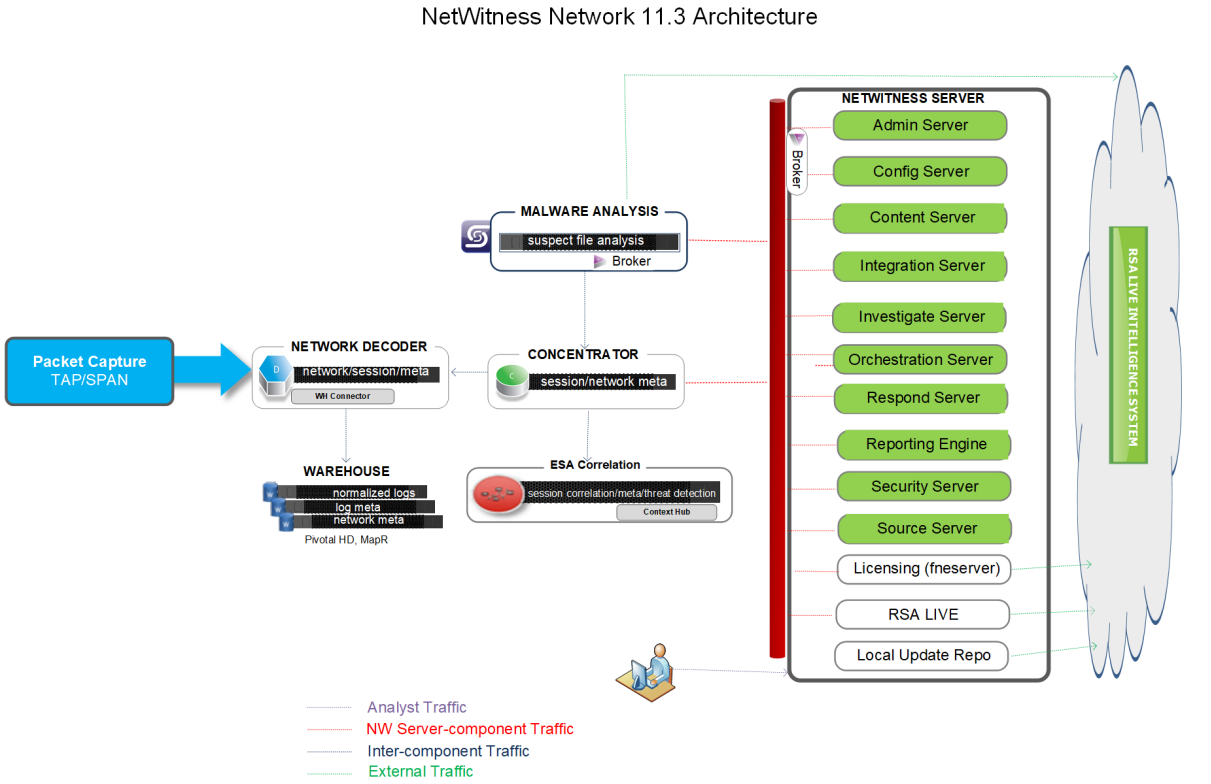
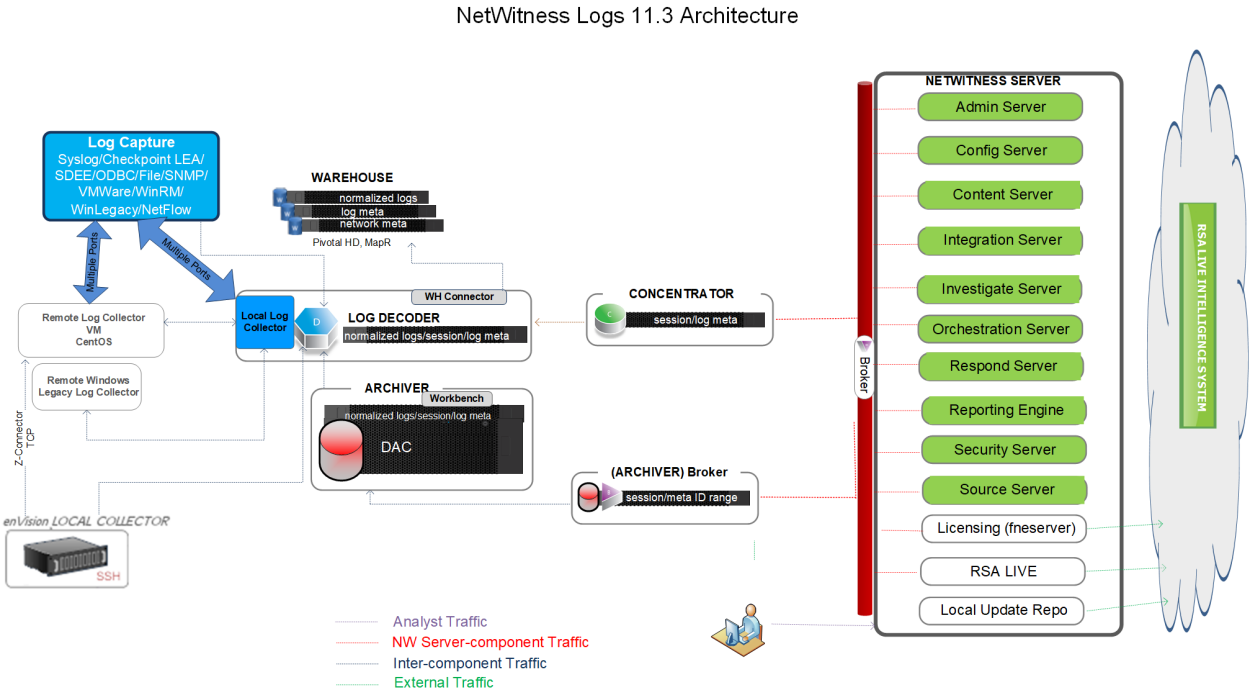


Diagrama de la arquitectura de red de registros de NetWitness

En los siguientes diagramas se muestra la arquitectura de red de los registros de NetWitness.



RSA NETWITNESS LOGS

Note:
Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

Lista completa de hosts, servicios y puertos iDRAC de NetWitness Platform

Nota: Para los puertos que se usan en la recopilación de eventos a través del Registros de NetWitness, consulte "Aspectos básicos" en la *Guía de implementación de la recopilación de registros de RSA NetWitness Suite*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Esta sección contiene las especificaciones de puerto para los siguientes hosts.

Host del servidor de NW

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Servidor de NW	TCP 443, 80	nginx: Interfaz del usuario de NetWitness
Estación de trabajo de administrador	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Estación de trabajo de administrador	Servidor de NW	TCP 22	Protocolo SSH
Hosts de NW	Servidor de NW	TCP 53 UDP 53	DNS
Hosts de NW	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Hosts de NW	Servidor de NW	TCP 4505, 4506	Puertos maestros de valor de sal
Hosts de NW	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Hosts de NW	Servidor de NW	TCP 5671	RabbitMQ-amqp
Hosts de NW	Servidor de NW	UDP 123	NTP
Hosts de NW	Servidor de NW	TCP 27017	MongoDB
Servidor de NW	cloud.netwitness.com	TCP 443	Live
Servidor de NW	cms.netwitness.com	TCP 443	Live
Servidor de NW	smcupdate.emc.com	TCP 443	Live
Servidor de NW	Servidor NFS	TCP 111, 2049, UDP 111, 2049	Instalaciones de iDRAC
Servidor de NW	Hosts de NW	UDP 123	NTP
Servidor de NW	NW Endpoint	TCP 443, 9443	Para integraciones de NW Endpoint 4.x

Host de Archiver

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Archiver	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Archiver	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Archiver	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Archiver	TCP 22	Protocolo SSH
Servidor de NW	Archiver	TCP 56008 (SSL), 50108 (REST)	Puertos de aplicaciones de Archiver
Servidor de NW	Archiver	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Archiver	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Servidor de NW	Archiver	TCP 514, 6514, 56007 (SSL), 50107 (REST), UDP 514	Puertos de aplicaciones de Workbench
Archiver	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC

Host de Broker

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Broker	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Broker	Concentrator	TCP 56005	Puerto de aplicaciones de Concentrator
Broker	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Broker	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Broker	TCP 22	Protocolo SSH
Servidor de NW	Broker	TCP 56003 (SSL), 50103 (REST)	Puertos de aplicaciones de Broker
Servidor de NW	Broker	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Broker	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Broker	Servidor de NW	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC
Endpoint Broker	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA

Host de Concentrator

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Concentrator	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Concentrator	Log Decoder	TCP 56002	Puerto de aplicaciones de Concentrator
Concentrator	Network Decoder	TCP 56004	Puerto de aplicaciones de Concentrator
Concentrator	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Concentrator	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Concentrator	TCP 22	Protocolo SSH
Servidor de NW	Concentrator	TCP 56005 (SSL), 50105 (REST)	Puertos de aplicaciones de Concentrator
Malware	Concentrator	TCP 56005 (SSL)	Malware
Servidor de NW	Concentrator	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Concentrator	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Concentrator	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC

Endpoint Log Hybrid

Host de origen	Host de destino	Puertos de destino	Comentarios
Agente de Endpoint	Endpoint Log Hybrid	TCP 443 UDP 444	HTTPS de NGINX UDP de NGINX. Si el puerto UDP 444 no es aceptable en su entorno consulte Cómo cambiar el puerto UDP para Endpoint Log Hybrid.
Agente de Endpoint	Log Decoder o Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Recopilación de registros de Windows
Endpoint Log Hybrid	Log Decoder (externo)	TCP 50102 (REST) 56202 (Protobuf SSL) 50202 (Protobuf)	Para reenviar metadatos a un Log Decoder externo
Endpoint Log Hybrid	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Servidor de NW	Endpoint Log Hybrid	TCP 7050	Tráfico web de la interfaz de usuario
Endpoint Log Hybrid	Servidor de NW	TCP 5671	Bus de mensajes
Endpoint Log Hybrid	Servidor de NW	TCP 27017	MongoDB
Servidor de NW	Endpoint Log Hybrid	TCP 7054	Tráfico web de la interfaz de usuario
Servidor de NW	Servidor NFS	TCP 111, 2049 UDP 111, 2049	Instalaciones de iDRAC

Host de Event Stream Analysis (ESA)

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	ESA	TCP 15671	Interfaz del usuario de administración de RabbitMQ
ESA primario y secundario	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
ESA primario y secundario	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	ESA	TCP 22	Protocolo SSH
Servidor de NW, ESA secundario	ESA primario	TCP 27017	MongoDB
Servidor de NW	ESA primario	TCP 7005	Puerto de lanzamiento de Context Hub: (ESA primario)
Servidor de NW	ESA	TCP 50030 (SSL)	Puerto de aplicaciones de ESA
Servidor de NW	ESA	TCP 50035 (SSL)	Puerto de aplicaciones de ESA
Servidor de NW	ESA	TCP 50036 (SSL)	Puerto de aplicaciones de ESA
Servidor de NW	ESA	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
ESA primario y secundario	cms.netwitness.com	TCP 443	Live
ESA primario y secundario	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC
ESA primario y secundario	Active Directory	636 (SSL)/389 (no SSL)	
Servidor de NW	ESA	80 (HTTP)/ 443 (HTTPS)(REST)	
ESA primario	Archer	443 (SSL)/80 (no SSL)	
ESA primario	ESA primario	TCP 7007	Iniciar puerto

Puertos iDRAC

Puerto	Función	Comentarios
22*	Protocolo SSH	Puerto predeterminado configurable a través del cual iDRAC escucha las conexiones
443*	HTTP	Puerto predeterminado configurable a través del cual iDRAC escucha las conexiones
5900*	Teclado de consola virtual y redirección de mouse, medios virtuales, carpetas virtuales y uso compartido de archivos remotos.	Puerto predeterminado configurable a través del cual iDRAC escucha las conexiones
111, 2049	TCP	Hosts de NetWitness Platform para el servidor NFS
111, 2049	UDP	Hosts de NetWitness Platform para el servidor NFS

Host de Log Collector

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Log Collector	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Log Collector	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Log Collector	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Log Collector	TCP 22	Protocolo SSH
Log Collector	Orígenes de eventos de registro	Consulte *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.	
Orígenes de eventos de registro	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Puertos de recopilación de registros
Orígenes de eventos de registro	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Puertos FTP/S de recopilación de registros
Servidor de NW	Log Collector	TCP 56001 (SSL), 50101 (REST)	Puertos de aplicaciones de Log Collector
Servidor de NW	Log Collector	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Log Collector	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Log Collector	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC
Log Collector	Log Collector virtual	TCP 5671	En el modo de extracción

Host de origen	Host de destino	Puertos de destino	Comentarios
Log Collector virtual	Log Collector	TCP 5671	En el modo de migración

Host de Log Decoder

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Log Decoder	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Log Decoder	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Log Decoder	TCP 22	Protocolo SSH
Log Decoder	Orígenes de eventos de registro	Consulte *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.	
Orígenes de eventos de registro	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Puertos de recopilación de registros
Orígenes de eventos de registro	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Puertos FTP/S de recopilación de registros
Servidor de NW	Log Decoder	TCP 56001 (SSL), 50101 (REST)	Puertos de aplicaciones de Log Collector
Servidor de NW	Log Decoder	TCP 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Puertos de aplicaciones de Log Decoder
Servidor de NW	Log Decoder	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Log Decoder	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Log Decoder	Log Collector	TCP 6514	
Log Decoder	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC

Host de Log Hybrid

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Log Hybrid	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Log Hybrid	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Log Hybrid	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Log Hybrid	TCP 22	Protocolo SSH
Log Collector	Orígenes de eventos de registro	Consulte *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.	
Orígenes de eventos de registro	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Puertos de recopilación de registros
Orígenes de eventos de registro	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Puertos FTP/S de recopilación de registros
Servidor de NW	Log Hybrid	TCP 56001 (SSL), 50101 (REST)	Puertos de aplicaciones de Log Collector
Servidor de NW	Log Hybrid	TCP 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Puertos de aplicaciones de Log Decoder
Servidor de NW	Log Hybrid	TCP 56005 (SSL), 50105 (REST)	Puertos de aplicaciones de Concentrator
Servidor de NW	Log Hybrid	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance

Host de origen	Host de destino	Puertos de destino	Comentarios
Servidor de NW	Log Hybrid	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Log Hybrid	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC

Host de Malware

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Malware	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Malware	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Malware	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Malware	TCP 22	Protocolo SSH
Servidor de NW	Malware	TCP 60007	Puertos de aplicaciones de Malware
Servidor de NW	Malware	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Malware	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Servidor de NW	Malware	TCP 5432	Postgresql
Servidor de NW	Malware	TCP 56003 (SSL), 50103 (REST)	Puertos de aplicaciones de Broker
Malware	panacea.threatgrid.com	TCP 443	ThreatGrid
Malware	cloud.netwitness.com	TCP 443	Evaluación de la comunidad/Opswat
Malware	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC

Host de Network Decoder

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Network Decoder	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Network Decoder	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Network Decoder	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Network Decoder	TCP 22	Protocolo SSH
Servidor de NW	Network Decoder	TCP 56004 (SSL), 50104 (REST)	Puertos de aplicaciones de Network Decoder
Servidor de NW	Network Decoder	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Network Decoder	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Network Decoder	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC

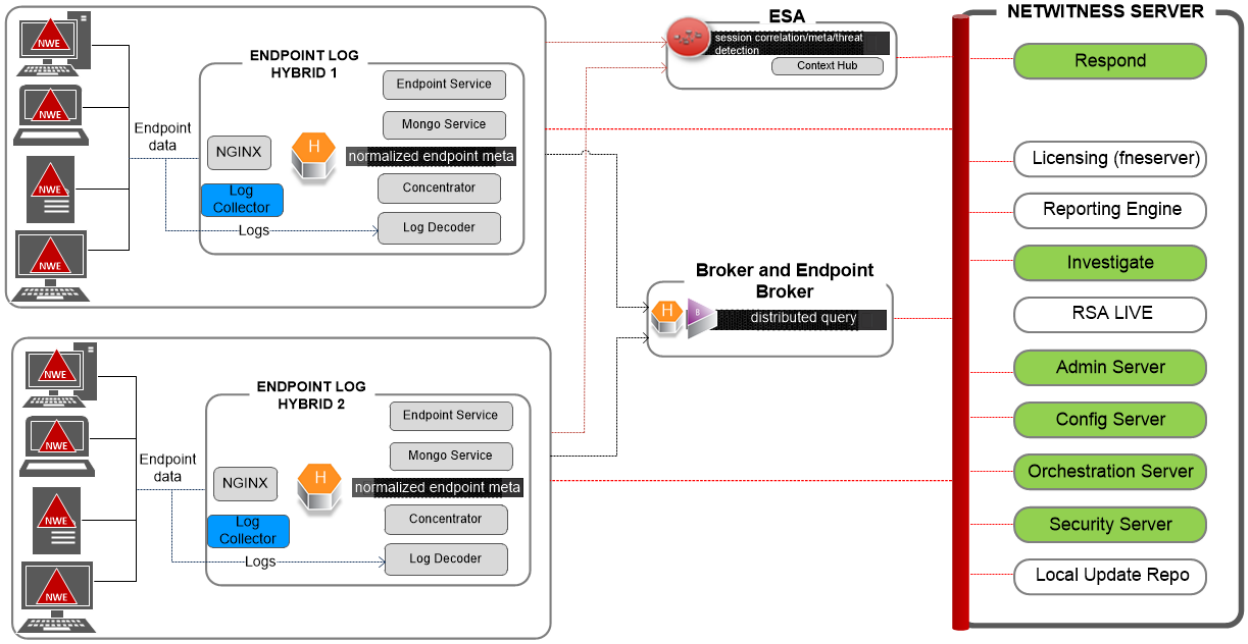
Host de Network Hybrid

Host de origen	Host de destino	Puertos de destino	Comentarios
Estación de trabajo de administrador	Network Hybrid	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Network Hybrid	Servidor de NW	TCP 15671	Interfaz del usuario de administración de RabbitMQ
Network Hybrid	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Estación de trabajo de administrador	Network Hybrid	TCP 22	Protocolo SSH
Servidor de NW	Network Hybrid	TCP 56004 (SSL), 50104 (REST)	Puertos de aplicaciones de Network Decoder
Servidor de NW	Network Hybrid	TCP 56005 (SSL), 50105 (REST)	Puertos de aplicaciones de Concentrator
Servidor de NW	Network Hybrid	TCP 56006 (SSL), 50106 (REST)	Puertos de NetWitness Appliance
Servidor de NW	Network Hybrid	TCP 5671	Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW.
Network Hybrid	Servidor NFS	TCP 111 2049 UDP 111 2049	Instalaciones de iDRAC

Host de UEBA

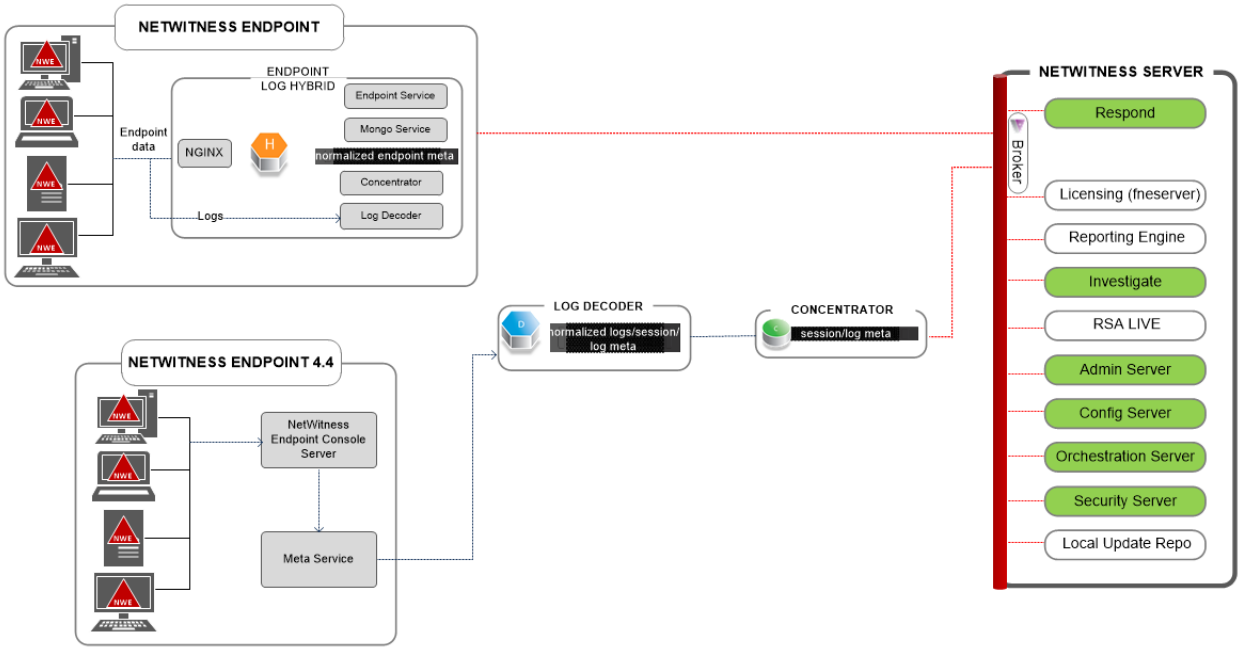
Host de origen	Host de destino	Puertos de destino	Comentarios
Servidor de UEBA	Servidor de NW	TCP 443	Repositorio de actualizaciones de RSA
Servidor de UEBA	Broker	TCP 56003 (SSL), 50103 (REST)	Puertos de aplicaciones de Broker
Servidor de UEBA	Concentrator	TCP 56005 (SSL), 50105 (REST)	Puertos de aplicaciones de Concentrator
Estación de trabajo de administrador	Servidor de UEBA	443	Monitoreo de UEBA
Estación de trabajo de administrador	Servidor de UEBA	22	Protocolo SSH
Servidor de UEBA	Servidor de NW	15671	Reenvío de alertas de UEBA a Respond
Servidor de NW	Servidor NFS	TCP 111, 2049 UDP 111, 2049	Instalaciones de iDRAC

Arquitectura de NetWitness Endpoint



Note: Log Collector collects Windows logs from event sources.

Integración de NetWitness Endpoint 4.4 con NetWitness Platform



Para obtener más información sobre los servicios que se ejecutan en Endpoint Hybrid, consulte la *Guía de configuración de RSA NetWitness Endpoint*.

Cómo cambiar el puerto UDP de Endpoint Log Hybrid

Los siguientes pasos indican cómo cambiar el puerto UDP predeterminado 444 de Endpoint Log Hybrid si no es aceptable en el entorno. Se usa el puerto 555 como ejemplo del procedimiento para sustituir el puerto UDP 444.
Hay dos tareas que se deben completar para cambiar el puerto UDP predeterminado 444 de Endpoint Log Hybrid:

Tarea 1: Indicar a todos los agentes que utilicen un nuevo puerto UDP

Tarea 2: Actualizar el puerto en todos los hosts de Endpoint Log Hybrid en el entorno

Nota: Si no se seleccionó la opción de reglas de firewall personalizadas al ejecutar nwsetup-tui, NetWitness Platform sobrescribirá las reglas de firewall después de un tiempo. Consulte el siguiente artículo de la base de conocimientos 00036446 (https://community.rsa.com/docs/DOC-93651) si este es el caso.

Tarea 1: Indicar a todos los agentes que utilicen un nuevo puerto UDP

Se deben completar los siguientes pasos para actualizar el puerto UDP en la política de replicación de datos empresariales (EDR) predeterminada y todas las demás políticas aplicadas, a fin de indicar a todos los agentes que utilicen un nuevo puerto UDP.

1. En el menú de **NetWitness Platform**, seleccione **ADMINISTRAR** > **Fuentes de Endpoint** > **Políticas**.
   Se muestra la vista **Políticas**.
2. Seleccione la **política de EDR predeterminada** y haga clic en **Editar** en la barra de herramientas.
3. desplácese hacia abajo hasta **PUERTO UDP** y cambie el valor (por ejemplo, cambie de **444** a **555**).
4. Haga clic en **Publicar política**, en la parte inferior de la vista.

Tarea 2: Actualizar el puerto en todos los hosts de Endpoint Log Hybrid en el entorno

Acceda mediante el protocolo SSH a cada host de Endpoint Log Hybrid en su entorno con las credenciales de `admin` y realice las siguientes actualizaciones.

1. Actualice las reglas de `iptables` para permitir `555` en lugar de `444`.
   a. En el siguiente archivo, reemplace la línea `444` por `555` .
      `vi /etc/sysconfig/iptables`
   b. Reinicie `iptables` con la siguiente cadena de comandos.
      `systemctl restart iptables`
   c. Verifique el cambio mediante la siguiente cadena de comandos.
      `iptables -L -n`
      A continuación se muestra un ejemplo de los elementos a visualizar para realizar correctamente el cambio.
      ```
      ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp multiport dports 555 /*
      EndpointNginxPort */ ctstate NEW
      ```

2. Actualice la política de SELinux. 555 es un puerto con privilegios, por lo que se debe actualizar la política de SELinux para permitir este puerto.
   a. Ejecute la siguiente cadena de comandos.
      `semanage port -a -t http_port_t -p udp 555`
      Si se recibió advertencias o errores de Python, omítalos.
   b. Verifique el cambio mediante la siguiente cadena de comandos.
      `semanage port -l | grep http_port_t`
      A continuación se muestra un ejemplo de los elementos a visualizar para realizar correctamente el cambio.
      `http_port_t udp 555, 444`
   c. (Opcional) Elimine `444`.
3. Actualice nginx config.
   a. Edite el siguiente archivo.
      `vi /etc/nginx/nginx.conf`
   b. Busque la siguiente cadena.
      `listen 444 udp;`
   c. Reemplace `444` por `555`.
   d. Reinicie nginx con la siguiente cadena de comandos.
      `systemctl restart nginx`
4. Verifique que los agentes se comuniquen a través del nuevo puerto.
   a. Ejecute la siguiente cadena de comandos.
      `tcpdump -i eth0 port 555`
   b. Espere 30 segundos, el puerto envía una señalizal cada 30 segundos. Si todo funciona correctamente, se mostrará información similar a la siguiente.
      ```
      09:20:12.571316 IP 10.40.15.103.60807 >
      NiranjanEPS1.rsa.lab.emc.com.dsf: UDP, length 20
      09:20:12.572433 IP NiranjanEPS1.rsa.lab.emc.com.dsf >
      10.40.15.103.60807: UDP, length 1
      ```
      Se deben devolver ambas líneas. Uno es la solicitud de tamaño (`20` bytes) y el otro es el tamaño de la respuesta (`1`byte).

Requisitos y seguridad del sitio

Asegúrese de leer este tema con detención y respete todas las advertencias y las precauciones antes de instalar o realizar el mantenimiento de los dispositivos de RSA.

Usos previstos de la aplicación

Este producto se evaluó como un equipo de tecnología de la información (ITE) que se puede instalar en oficinas, escuelas, salas de computadoras y ubicaciones interiores similares de tipo comercial. Este dispositivo no está diseñado para ningún tipo de conexión a un cable para exteriores.

Servicio

Este dispositivo no contiene componentes que el usuario pueda reparar. Si se produce un desperfecto, póngase en contacto con Atención al cliente. En una condición de falla, se pueden generar altas temperaturas dentro del sistema, las cuales pueden activar una señal de alarma. En caso de una señal de alarma, desconecte inmediatamente el dispositivo de la fuente de alimentación y póngase en contacto con Atención al cliente. El funcionamiento del dispositivo en estas condiciones será inseguro y puede causar lesiones o daños materiales.

Información sobre seguridad

Selección del sitio

El sistema está diseñado para funcionar en un ambiente de oficina típico. Elija un sitio que esté:

- Limpio, seco y libre de partículas transportadas por el aire (más allá del polvo normal de una habitación).
- Bien ventilado y lejos de fuentes de calor, entre ellas, luz solar directa y radiadores.
- Lejos de fuentes de vibración o de golpes físicos.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones susceptibles a tormentas eléctricas, se recomienda conectar el sistema a un supresor de sobretensión.
- Equipado con un tomacorriente de pared correctamente conectado a tierra.
- Provisto de espacio suficiente para acceder a los cables de la fuente de alimentación, debido a que actúan como el principal medio de desconexión del producto.

Prácticas de manejo de equipos

Reduzca el riesgo de lesiones o daño en los equipos mediante:

- El cumplimiento de requisitos locales de salud y seguridad ocupacionales cuando transfiera y levante equipos.
- El uso de asistencia mecánica u otra que sea apropiada cuando transfiera y levante equipos.
- La reducción del peso para lograr un manejo más sencillo gracias a la extracción de componentes fácilmente desmontables.

Advertencias eléctricas y de alimentación

Precaución: El botón de encendido, que se señala con una marca de alimentación en espera, NO apaga totalmente la alimentación AC del sistema; la alimentación en espera de 5 V permanece activa mientras el sistema está conectado. Para cortar la alimentación del sistema, debe desconectar los cables de alimentación AC del tomacorriente de pared.

- No intente modificar ni usar un cable de alimentación AC si no es el tipo exacto que se exige. Se requiere un cable de AC por separado para cada fuente de alimentación del sistema.
- Este producto no contiene componentes que el usuario pueda reparar. No abra el sistema.
- Cuando reemplace una fuente de alimentación de conexión en caliente, desconecte el cable de alimentación de la fuente de alimentación que se va a reemplazar antes de quitarla del servidor.

Advertencias sobre el montaje en rack

- El rack del equipo se debe anclar a un soporte fijo para evitar que se incline cuando se extienda desde él un servidor o un equipo. El rack del equipo se debe instalar de acuerdo con las instrucciones de su fabricante.
- El montaje del equipo en el rack se debe realizar sin que se presente una condición de peligro debido a una carga mecánica irregular.
- Extienda solo un equipo por vez desde el rack.
- Para evitar el riesgo de una posible descarga eléctrica, debe implementarse una conexión a tierra de seguridad adecuada para el rack y cada pieza de equipo instalada en él.

Enfriamiento y flujo de aire

La instalación del equipo se debe realizar de manera tal que no sea vea afectada la cantidad de flujo de aire que se necesita para el funcionamiento seguro del equipo.