RSA NETWITNESS® SUITE

Guía de implementación de AWS

para la versión 11.0

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

febrero 2018

Contenido

Descripción general de la implementación de AWS 5

Recomendaciones para ambientes AWS 5

Abreviaturas y otra terminología que se usan en esta guía 6

Escenarios de implementación de AWS 10

Visibilidad de VPC de plataforma completa de NetWitness Suite (paquete de soluciones) 10

Implementación de Hybrid: Decoder y Log Decoder (paquete de soluciones) 12

Implementación de Hybrid: Decoder, Log Decoder y Concentrator (paquete de soluciones) 13

Requisitos previos 13

Servicios compatibles 13

Implementación de AWS 15

Reglas 15

Lista de verificación 15

Establecer el ambiente AWS 16

Buscar AMI de NetWitness Suite 16

Iniciar una instancia y configurar un host 17

Tareas de instalación 22

Configurar hosts (instancias) en NetWitness Suite 37

Configurar la captura de paquetes 37

Integrar Gigamon GigaVUE con el Packet Decoder 37

Integrar f5® BIG-IP con el Packet Decoder 40

Recomendaciones de configuración de instancias de AWS 43

Archiver 44

Broker 46

Concentrator: Flujo de registros 47

Soluciones de flujo de paquetes 48

Concentrator: Solución de Gigamon 48

Concentrator: Solución de f5 BIG-IP 48

Decoder: Solución de Gigamon 49

Decoder: Solución de f5 BIG-IP 49

ESA y Context Hub en base de datos de Mongo 51

Log Collector (Syslog, Netflow y protocolos de recopilación de archivos) 52
Log Decoder 53
Servidor de NetWitness, Reporting Engine, Respond y Estado y condición 54

Descripción general de la implementación de AWS

Antes de que pueda implementar RSA NetWitness® Suite en Amazon Web Services (AWS), debe:

- Entender los requisitos de su empresa.
- Conocer el alcance de una implementación de NetWitness Suite.

Cuando esté preparado para comenzar la implementación:

- Asegúrese de tener una licencia de "Rendimiento" de NetWitness Suite.
- Para la captura de paquetes en AWS, puede comprar cualquiera de las siguientes soluciones de otros fabricantes. Si se comunica con uno de estos terceros, le asignarán un representante de cuentas y un ingeniero de servicios profesionales que trabajarán en estrecha coordinación con el personal RSA.
  - Gigamon® GigVUE 5.0
  - f5BIG-IP 12.1.0

Recomendaciones para ambientes AWS

Las instancias de AWS tienen la misma funcionalidad que los hosts de hardware de NetWitness Suite. RSA recomienda realizar las siguientes tareas durante la configuración del ambiente AWS.

- Según los requisitos de recursos de los diferentes componentes, siga las mejores prácticas para usar el sistema y los volúmenes de Elastic Block Store (EBS) de almacenamiento exclusivos de forma correcta.
- Asegúrese de que la capacidad de procesamiento proporcione una velocidad de escritura un 10 % superior a la captura sostenida y la tasa de recopilación requeridas para la implementación.
- Cree un directorio de Concentrator para una base de datos de índice en el disco SSD de IOPS aprovisionado.

Abreviaturas y otra terminología que se usan en esta guía

Abreviaturas	Descripción
AMI	Imagen de máquina de Amazon
AWS	Amazon Web Services
BYOL	Traiga su propia licencia
CPU	Unidad central de procesamiento
Instancia exclusiva	Las instancias exclusivas de AWS se ejecutan en una VPC en hardware que está destinado a un solo cliente. Las instancias exclusivas están aisladas físicamente en el nivel de hardware del host de las instancias que pertenecen a otras cuentas de AWS. Las instancias exclusivas pueden compartir hardware con otras instancias de la misma cuenta de AWS que no sean instancias exclusivas. Consulte la documentación "Instancia exclusiva de Amazon EC2" de AWS (https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/) para obtener más información sobre las instancias exclusivas.
Optimización de EBS	Una instancia optimizada para Amazon EBS usa una plataforma de configuración optimizada y proporciona capacidad adicional y exclusiva para las I/O de Amazon EBS. Esta optimización proporciona el mejor rendimiento para los volúmenes de EBS, porque minimiza la contención entre las I/O de Amazon EBS y otro tráfico proveniente de su instancia. Consulte la documentación "Instancias optimizadas para Amazon EBS" de AWS (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html) para obtener más información sobre las instancias optimizadas para EBS.

Abreviaturas	Descripción
Volumen de EBS	El volumen de Elastic Block Store (EBS) es un volumen de almacenamiento de alta disponibilidad y confiabilidad que se puede conectar a cualquier instancia en ejecución que se encuentre en la misma zona de disponibilidad. Consulte la documentación "Volúmenes de Amazon EBS" de AWS (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html) para obtener más información sobre los volúmenes de EBS.
Instancia de EC2	Servidor virtual en Elastic Compute Cloud (EC2) de AWS para la ejecución de aplicaciones en la infraestructura de AWS. Consulte también **Instancia**.
Redes mejoradas habilitadas	Las redes mejoradas proporcionan mayor ancho de banda, mayor rendimiento de paquetes por segundo y latencias entre instancias constantemente más bajas. Si su tasa de paquetes por segundo parece haber alcanzado su límite, debe considerar la posibilidad de cambiarse a redes mejoradas, porque probablemente haya alcanzado los umbrales superiores del driver de la interfaz de red de máquina virtual (VIF). Consulte la documentación "Cómo habilito y configuro redes mejoradas en mis instancias de EC2" de AWS (https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/) para obtener más información sobre las redes mejoradas.
EPS	Eventos por segundo
GB	Gigabyte. 1 GB = 1,000,000,000 de bytes
Gb	Gigabit. 1 Gb = 1,000,000,000 de bits.
Gb/s	Gigabits por segundo o mil millones de bits por segundo. Mide el ancho de banda en un medio de transmisión de datos digital, como la fibra óptica.

Abreviaturas	Descripción
GHz	GigaHertz 1 GHz = 1,000,000,000 de Hz
Disco duro	Disco duro
Instancia	Un host virtual en AWS (es decir, una máquina virtual o un servidor en la infraestructura de AWS en que se ejecutan servicios o aplicaciones). Consulte también **Instancia de EC2**.
Tipo de instancia	Especifica la CPU y la RAM requeridas para una instancia. Consulte la documentación "Tipos de instancia de Amazon EC2" de AWS (https://aws.amazon.com/ec2/instance-types/) para obtener más información sobre los tipos de instancia.
IOPS	Operaciones de entrada/salida por segundo
Mb/s	Megabits por segundo o un millón de bits por segundo. Mide el ancho de banda en un medio de transmisión de datos digital, como la fibra óptica.
En las instalaciones	Los hosts en las instalaciones están instalados y se ejecutan en computadoras en las instalaciones (en el edificio) de la organización mediante el uso de hosts, en lugar de en AWS.
PPS	Paquetes por segundo
RAM	Memoria de acceso aleatorio (también conocida como memoria)
Grupo de seguridad	Conjunto de reglas de firewall. Consulte la documentación "Arquitectura y puertos de red" en RSA Link (https://community.rsa.com/docs/) para obtener una lista completa de los puertos que debe configurar para todos los componentes de NetWitness Suite.
Disco SSD	Disco de estado sólido

Abreviaturas	Descripción
Etiqueta	Un identificador significativo para la instancia de AWS.
Proveedor Tap	Proveedor tapping de red
vCPU	Unidad central de procesamiento virtual (también conocida como un procesador virtual)
VM	Máquina virtual
VPC	Nube pública virtual
vRAM	Memoria de acceso aleatorio virtual (también conocida como memoria virtual)

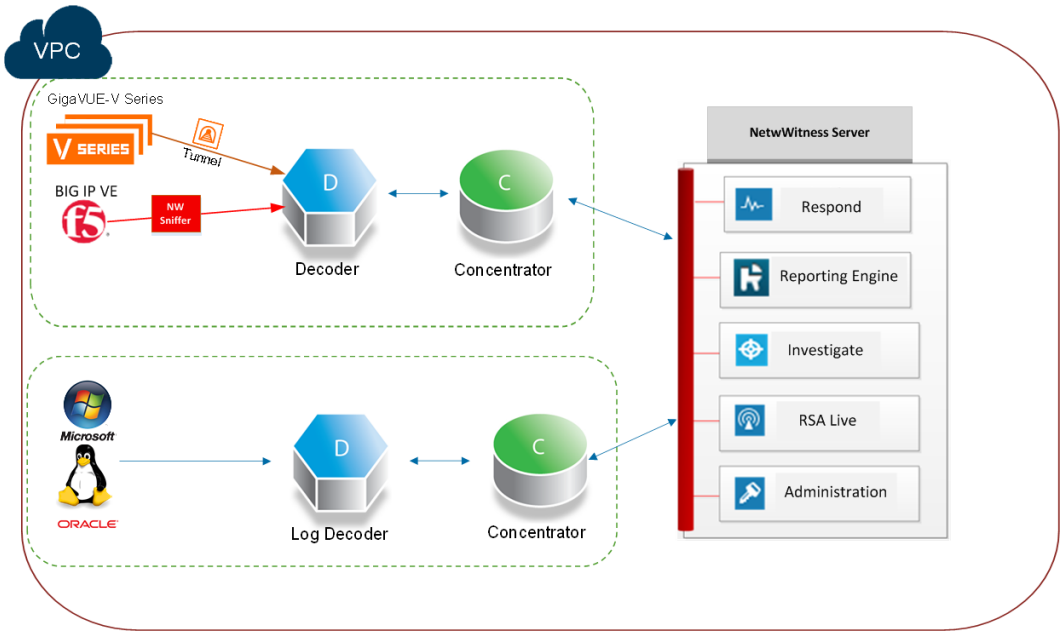
Escenarios de implementación de AWS

En los siguientes diagramas se muestran algunos escenarios de implementación de AWS comunes. En los diagramas:

- **Serie GigaVUE** (solución de Gigamon®) es una solución basada en agentes que usa **Tunelización** (que implementa el administrador de NetWitness Suite) para facilitar la captura de datos de paquetes en AWS.
- **BIG-IP** (solución de f5®) es una solución de balanceo de carga que usa un Packet Decoder que actúa como un sniffer (que personaliza el administrador de NetWitness Suite) para facilitar la captura de paquetes en AWS.
- El **Decoder** recopila datos de paquetes. El **Decoder** captura, analiza y reconstruye todo el tráfico de red de las capas 2 a 7.
- El **Log Decoder** recopila registros. El **Log Decoder** recopila eventos de registro de cientos de dispositivos y orígenes de eventos.
- El **Concentrator** indexa los metadatos extraídos de los datos de red o del registro y los pone a disposición para la analítica en tiempo real y la creación de consultas de toda la empresa y, al mismo tiempo, facilita la creación de informes y alertas.
- El Servidor de NetWitness aloja a **Respond**, **Reporting**, **Investigate**, **Live Content Management**, **Administration** y a otros aspectos de la interfaz del usuario.

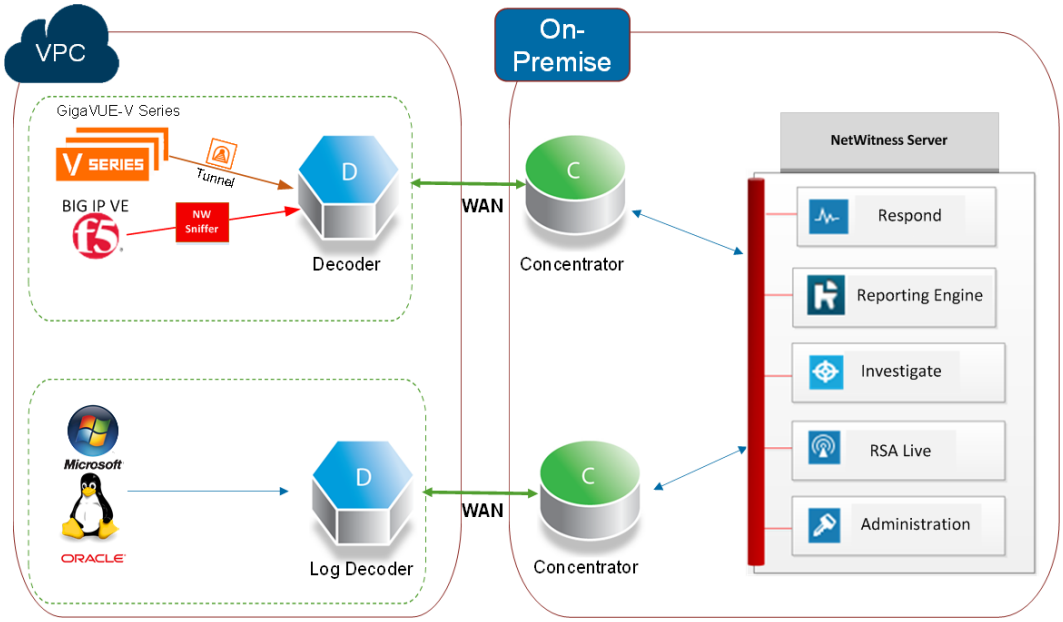
Visibilidad de VPC de plataforma completa de NetWitness Suite (paquete de soluciones)

En este diagrama se muestran todos los componentes de NetWitness Suite (plataforma completa) implementados en AWS.


VPC
GigaVUE-V Series
V SERIES
Tunnel
BIG IP VE
NW Sniffer
D
Decoder
C
Concentrator
NetwWitness Server
Respond
Reporting Engine
Investigate
RSA Live
Administration
Microsoft
ORACLE
D
Log Decoder
C
Concentrator

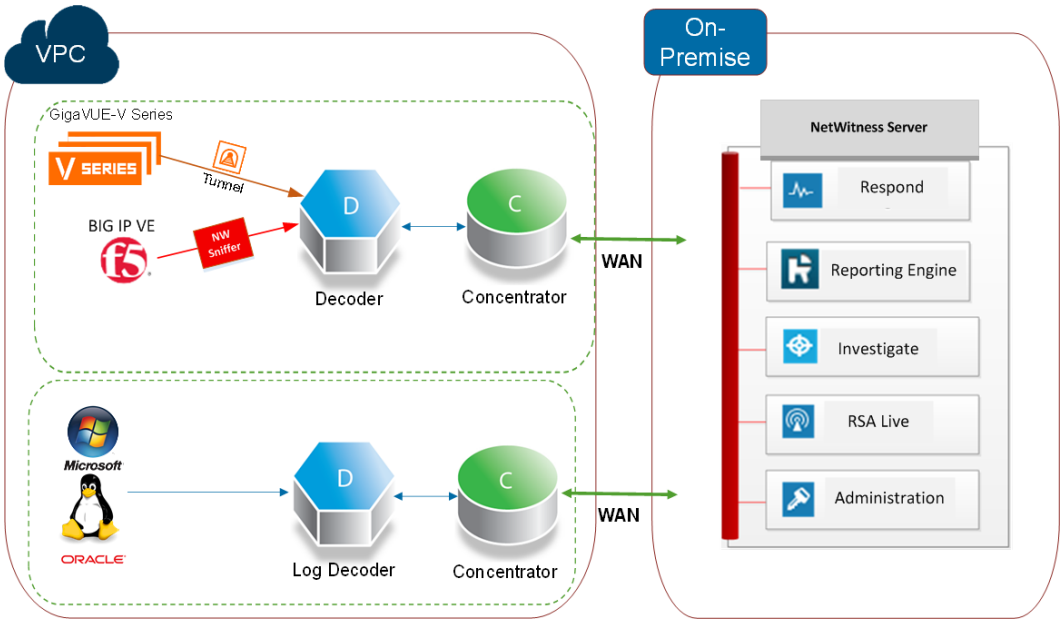
Implementación de Hybrid: Decoder y Log Decoder (paquete de soluciones)

En este diagrama se muestran el Decoder y el Log Decoder implementados en AWS con todos los demás componentes de NetWitness Suite implementados en sus instalaciones.



Implementación de Hybrid: Decoder, Log Decoder y Concentrator (paquete de soluciones)

En este diagrama se muestran el Decoder, el Log Decoder y el Concentrator implementados en AWS con todos los demás componentes de NetWitness Suite implementados en sus instalaciones.



Requisitos previos

Necesita los siguientes elementos antes de comenzar el proceso de integración:

- Acceso a la consola de AWS
- Red enrutable (y grupos de seguridad de AWS adecuados) para que los contenedores transfieran los datos al NetWitness Suite Decoder.

Servicios compatibles

RSA ofrece los siguientes servicios NetWitness Suite.

- Servidor de NetWitness
- Archiver
- Broker
- Concentrator

- Event Stream Analysis
- Log Decoder
- Decoder
- Remote Log Collector

Implementación de AWS

En este tema se incluyen las reglas y las tareas generales que debe seguir para implementar los componentes de RSA NetWitness® Suite en AWS.

Reglas

Debe cumplir con las siguientes reglas cuando se implementa NetWitness Suite en AWS.

- Acceda mediante el protocolo SSH a la instancia de NetWitness Suite al menos una vez después de la implementación para inicializar el sistema.
- Antes de habilitar los tableros de uso inmediato (OOTB), configure el origen de datos predeterminado en la página de configuración de Reporting Engine.
- Si reinicia la instancia de Packet Decoder, no se conserva el túnel. Cree de nuevo el túnel en el Packet Decoder y reinicie el servicio Decoder.
- Siempre use direcciones IP privadas cuando aprovisione instancias de NetWitness Suite de AWS.

Nota: Si asigna una dirección IP pública al host del servidor de Netwitness, actualice el archivo de configuración /etc/nginx/conf.d/nginx.conf de la siguiente manera:

```
location /nwrpmrepo
{
alias /var/lib/netwitness/common/repo;
index index.html index.htm;
allow <Subnet-Gateway>/Subnet mask ;
#example
# allow 10.0.0.1/25;
deny all;
autoindex on;
}
```

Lista de verificación

Paso	Descripción	√
1	Establecer el ambiente AWS	
2	Buscar AMI de NetWitness Suite	

Paso	Descripción	√
3	Iniciar una instancia y configurar un host	
4	Configurar hosts (instancias) en NetWitness Suite	
5	Configurar la captura de paquetes	

Establecer el ambiente AWS

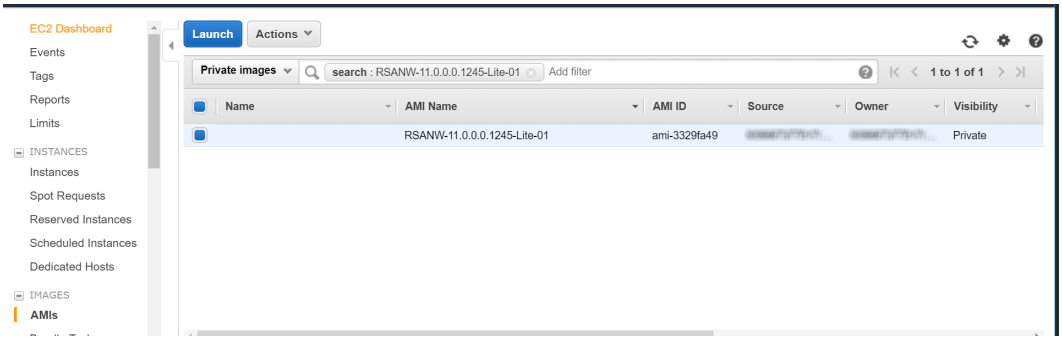
1. Asegúrese de tener un ambiente AWS con la capacidad de cumplir o superar las reglas de rendimiento de NetWitness Suite que se describen en los Recomendaciones de configuración de instancias de AWS .
2. Vaya a Buscar AMI de NetWitness Suite.

Buscar AMI de NetWitness Suite

Busque archivos AMI de NW dentro del repositorio público/compartido/de comunidad. Use "RSANW" como una palabra clave para buscar los archivos AMI.

Nota: Consulte la documentación **Búsqueda de AMI compartidos** de AWS (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingsharedamis-finding.html) para obtener instrucciones adicionales.

1. Abra la consola de Amazon EC2 (nueva cuenta de suscriptor) en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMIs.
3. En el primer filtro, elija Public images.
4. Escriba "RSANW" en el campo de búsqueda para buscar los AMI de NetWitness Suite.



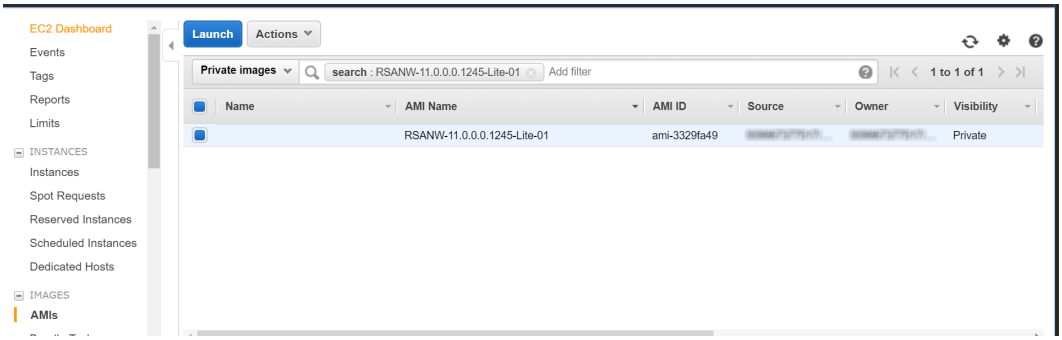
Nota: Póngase en contacto con el servicio al cliente de RSA (https://community.rsa.com/docs/DOC-1294) para acceder a **RSANW-11.0.0.0.1245-Full-01**.

5. Vaya a Iniciar una instancia y configurar un host.

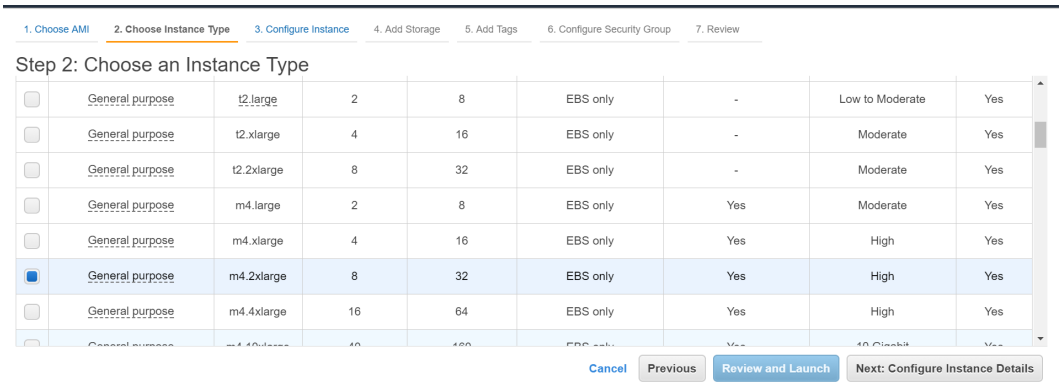
Iniciar una instancia y configurar un host

Nota: Consulte la documentación "Inicio de una instancia" de AWS (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html) para obtener instrucciones adicionales.

1. Seleccione una instancia de la cuadrícula (por ejemplo, **RSA-NW-Concentrator-11.0.0.0-01**) y haga clic en **Iniciar**.



2. Elija la RAM y las CPU mediante la selección de tipo de instancia.
   Consulte Recomendaciones de configuración de instancias de AWS para obtener reglas sobre cómo configurar la instancia de EC2 según los requisitos del componente de NetWitness Suite (es decir, servicio) para el cual está iniciando una instancia. En el siguiente ejemplo se muestra el tipo de instancia **m4.2xlarge** seleccionado con **8** CPU y **32** GB de RAM.

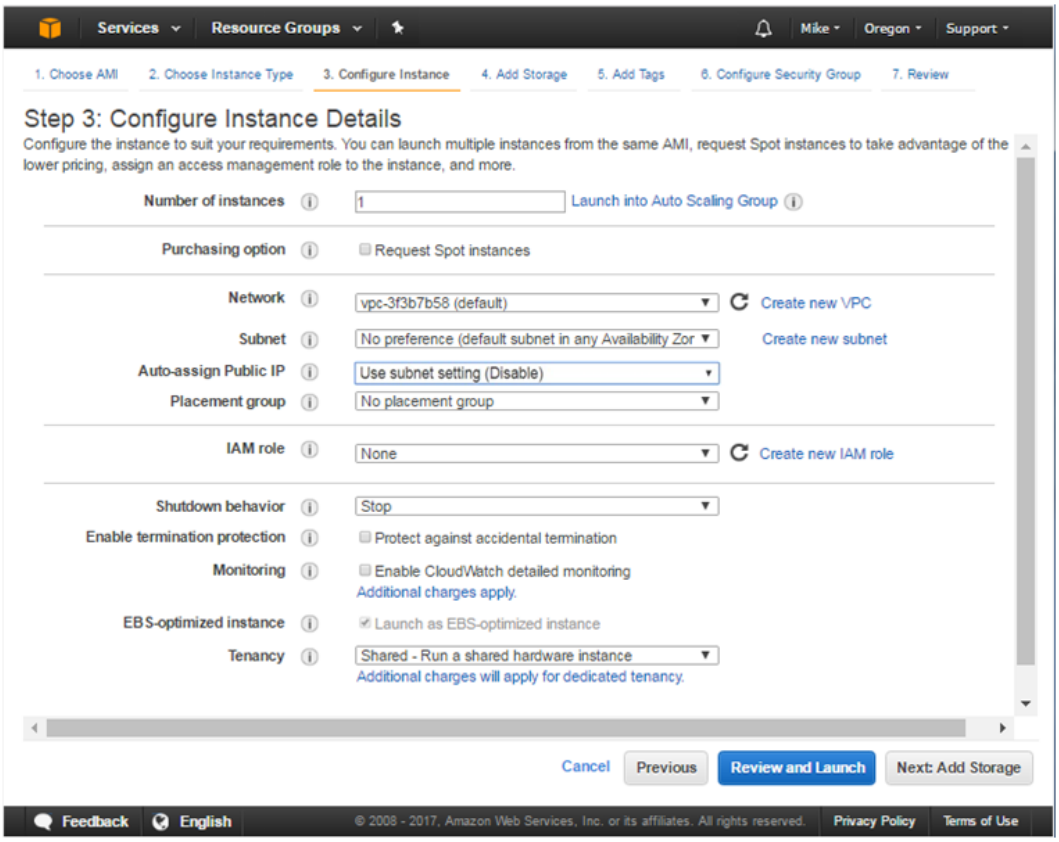


	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes

3. Haga clic en **Siguiente: Configurar los detalles de la instancia** en la parte inferior derecha de la página **Paso 2: Elegir un tipo de instancia**.

   Se muestra la página **Paso 3. Configurar los detalles de la instancia**.

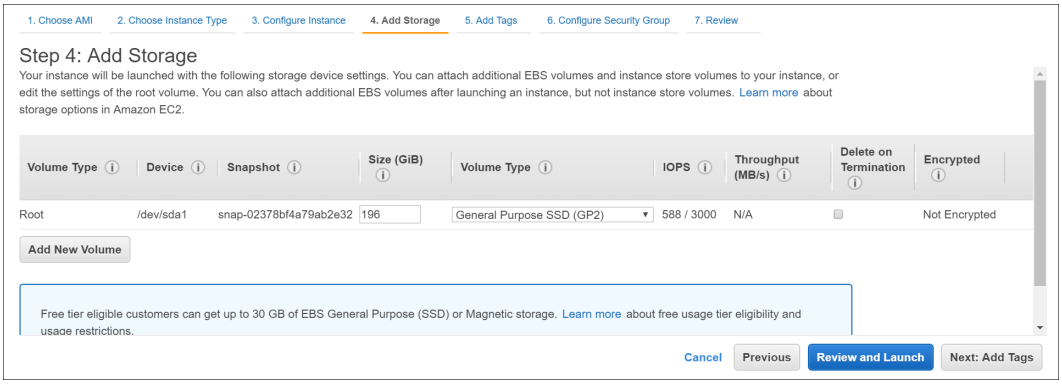
   Para NetWitness Suite, la subred y la VPC están configuradas de manera predeterminada en los valores del siguiente ejemplo.



4. Haga clic en **Siguiente: Agregar almacenamiento** en la parte inferior derecha de la página **Paso 3: Configurar los detalles de la instancia**.

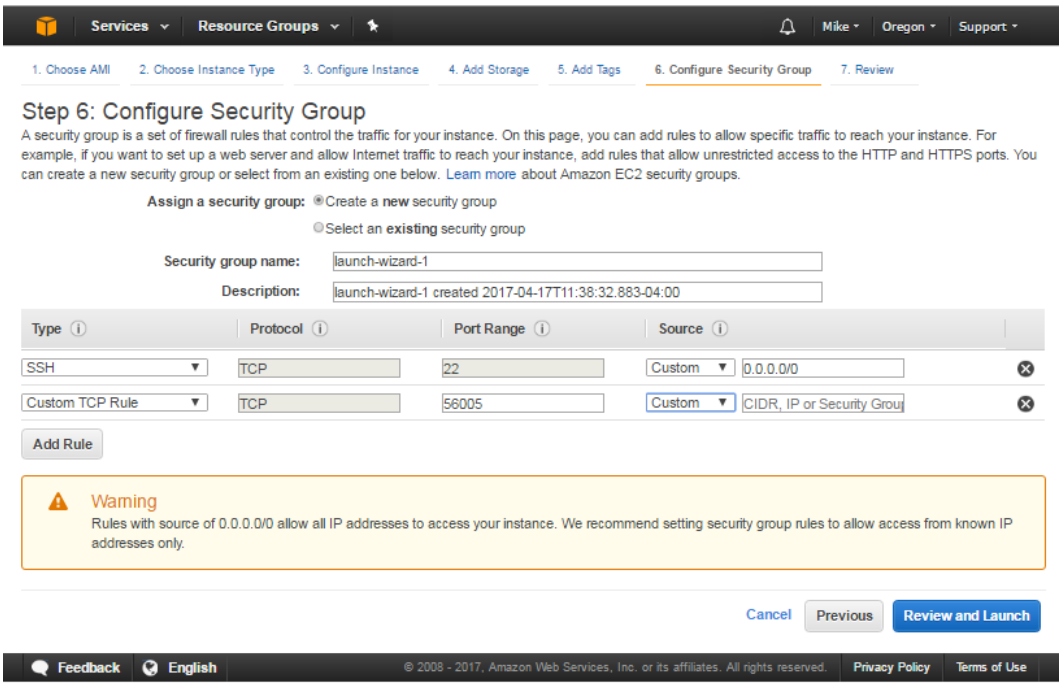
   Se muestra la página **Paso 4. Agregar almacenamiento**.

Consulte Recomendaciones de configuración de instancias de AWS para obtener reglas sobre cómo configurar el almacenamiento según los requisitos del componente de NetWitness Suite (es decir, servicio) para el cual está iniciando una instancia.



5. Haga clic en **Siguiente: Agregar etiquetas** en la parte inferior derecha de la página **Paso 4: Agregar almacenamiento**.
   Se muestra la página **Paso 5. Agregar etiquetas**. Ingrese el nombre de la instancia.
6. Haga clic en **Siguiente: Configurar el grupo de seguridad** en la parte inferior derecha de la página **Paso 5: Agregar etiquetas**.
   Se muestra la página **Paso 6. Configurar el grupo de seguridad**.
   a. Seleccione el botón de opción “Crear un **nuevo** grupo de seguridad”.
   b. Cree una regla que abra todo el firewall para el componente de NetWitness Suite. Debe configurar correctamente el grupo de seguridad para configurar la instancia (host) desde la interfaz del usuario de NetWitness Suite y acceder mediante el protocolo SSH a ella.

   Nota: Consulte la documentación “Arquitectura y puertos de red” en RSA Link (https://community.rsa.com/docs/DOC-83050) para obtener una lista completa de los puertos que debe configurar para todos los componentes de NetWitness Suite.

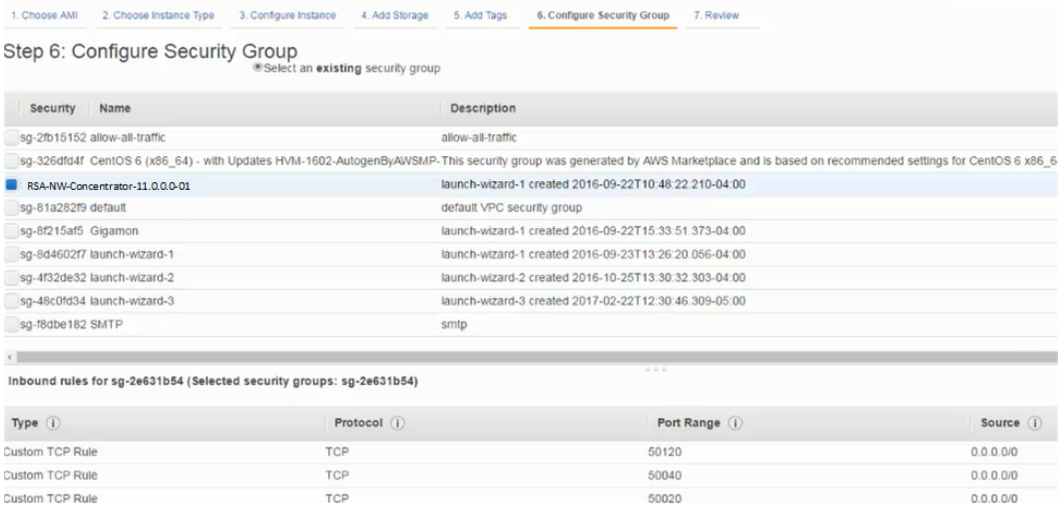


Nota: Después de configurar un grupo de seguridad, puede cambiarlo en cualquier momento.

7. Haga clic en **Revisar e iniciar** en la parte inferior derecha de la página **Paso 6: Configurar el grupo de seguridad**.
   Se muestra la página **Paso 7. Revisar inicio de instancia**.
8. Haga clic en **Iniciar** en la parte inferior derecha de la página **Paso 7. Revisar inicio de instancia**.
   Se muestra el cuadro de diálogo **Seleccionar un par de claves existente o crear un par de claves nuevo**.
9. Elija **Continuar sin par de claves**.

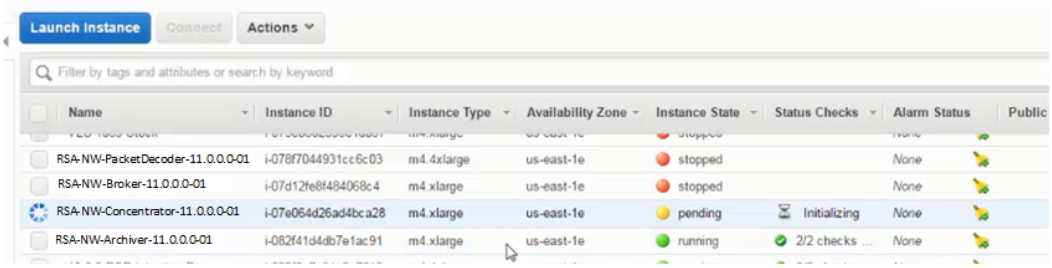
10. Haga clic en **Iniciar instancia**.

    AWS muestra la siguiente información a medida que se crea la instancia.



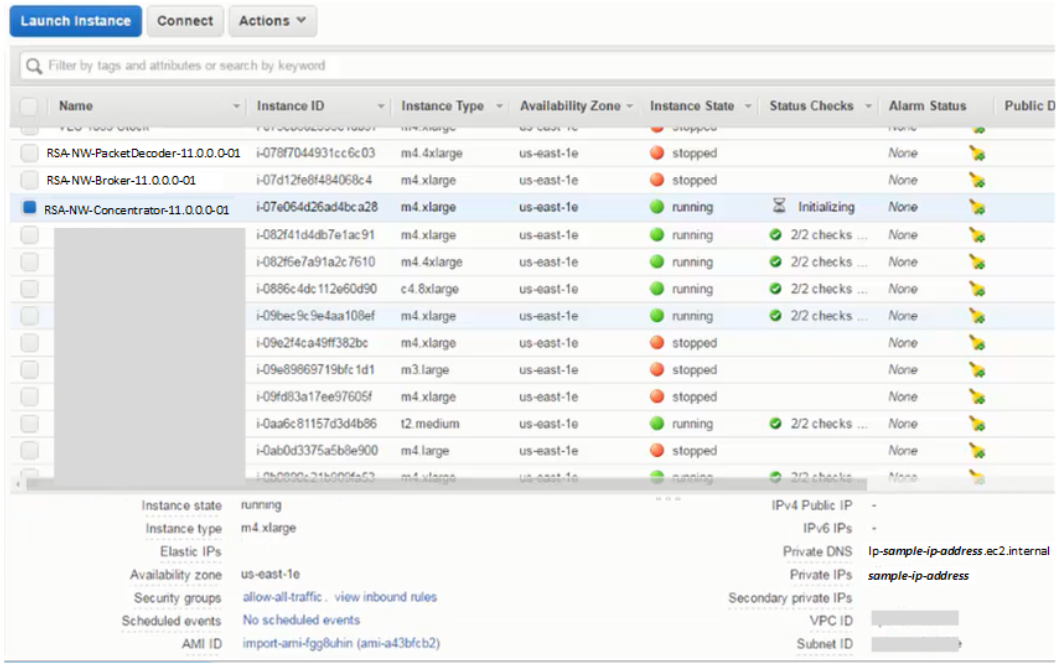
11. Haga clic en **Ver instancias**.

12. Seleccione **Instancias** en el panel de navegación izquierdo para revisar todas las instancias que AWS está inicializando (por ejemplo, **NW-Concentrator**).



    La dirección IP para el nuevo host de **RSA-NW-Concentrator-11.0.0.0-01** es ***sample-ip-***

address.



13. Acceda mediante el protocolo SSH a la instancia recién creada con las credenciales de NetWitness Suite predeterminadas.
14. Vaya a Configurar hosts (instancias) en NetWitness Suite.

Tareas de instalación

Tarea 1: Instalar 11.0.0.0 en el host del servidor de NetWitness (servidor de NW)

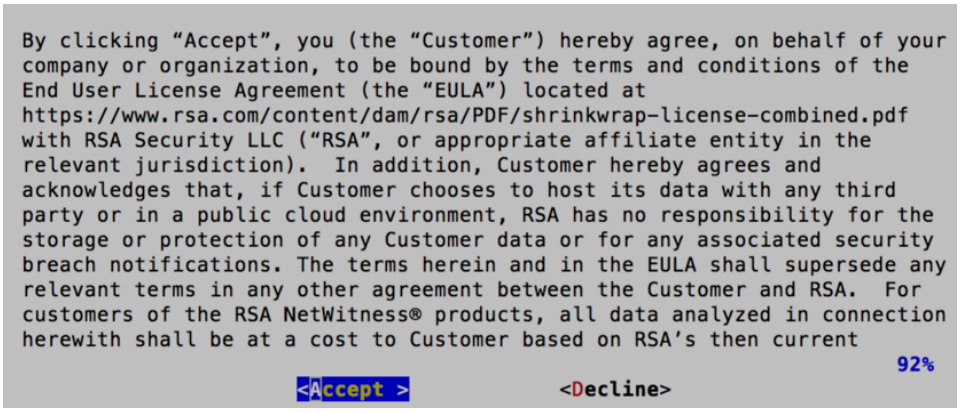
Nota: Puede realizar esta tarea para la instancia de RSANW-11.0.0.0.1245-Full-01.

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

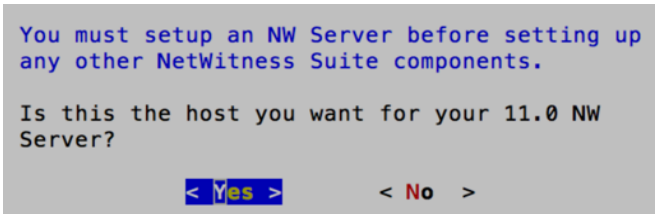
Esto inicia el programa de instalación y se muestra el EULA.

Nota: 1.) Cuando navegue por los indicadores del programa de instalación, use las flechas hacia abajo y hacia arriba para desplazarse entre los campos y use la tecla de tabulación para desplazarse hacia y desde los comandos (como **<Sí>**, **<No>**, **<Aceptar>** y **<Cancelar>**). Presione **Intro** para registrar la respuesta de los comandos y moverse al siguiente indicador.
2.) El programa de instalación adopta la combinación de colores del escritorio o de la consola que usa para acceder al host.
3.) Si especifica servidores DNS durante la ejecución del programa de instalación (`nwsetup-tui`), DEBEN ser válidos (válido en este contexto significa válido durante la configuración) y ser accesibles para que `nwsetup-tui` pueda continuar. Los servidores DNS configurados erróneamente hacen que la configuración falle. Si después de la configuración necesita acceder a un servidor DNS al que no se pudo acceder durante la configuración (por ejemplo, para reubicar un host después de la configuración que tenga un conjunto diferente de servidores DNS), consulte 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 Suite** en el paso 12 (los servidores DNS no están definidos, de modo que el sistema no puede acceder al repositorio externo).

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



3. Se muestra el indicador "Este es el servidor de NW".



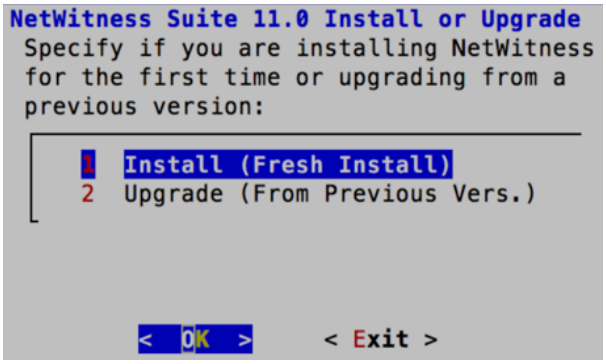
Use la tecla de tabulación para ir a **Sí** y presione **Intro**.

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

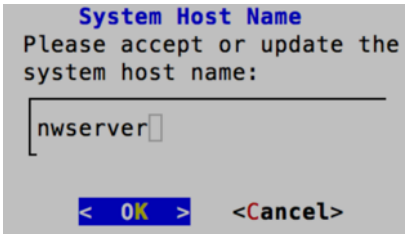
Precaución: Si elige el host incorrecto para el servidor de NW y completa la configuración, debe reiniciar el programa de instalación (paso 2) y completar todos los pasos subsiguientes para corregir este error.

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

   Se muestra el indicador Instalar o Actualizar.



5. Se muestra el indicador “Nombre del host”.



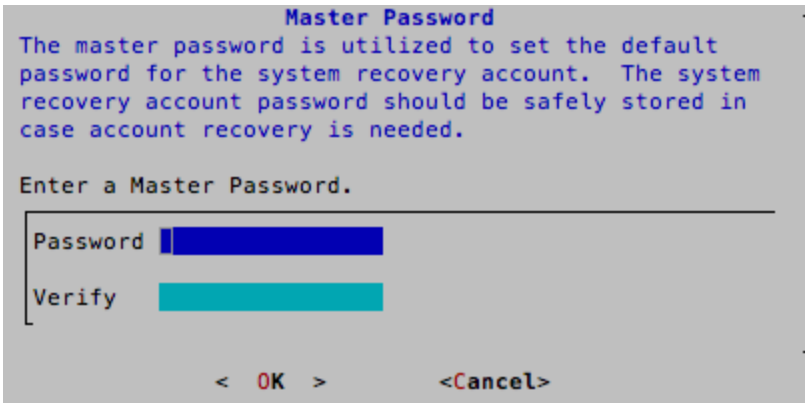
   Presione **Intro** si desea mantener este nombre. Si no edita el nombre del host, use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para cambiarlo.

   Se muestra el indicador “Contraseña maestra”.

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

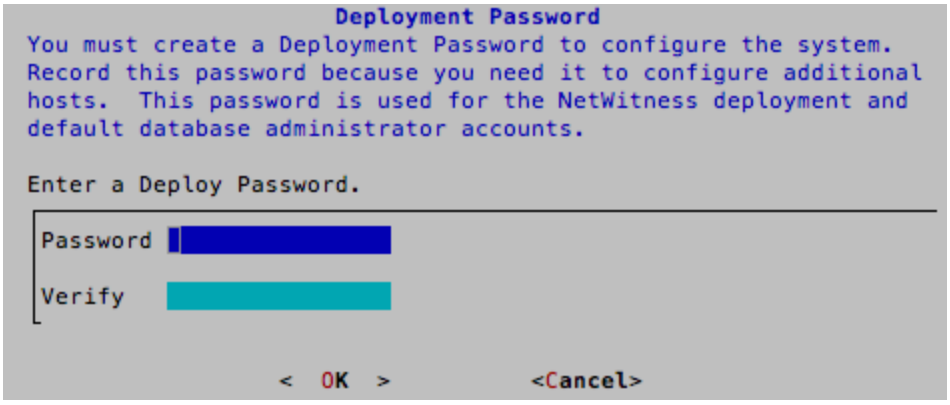
   - Símbolos: ! @ # % ^ +
   - Números: 0-9
   - Caracteres en minúscula: a-z
   - Caracteres en mayúscula: A-Z

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



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**.

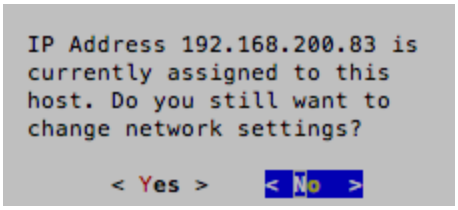
7. Se muestra el indicador "Contraseña de implementación".



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**.

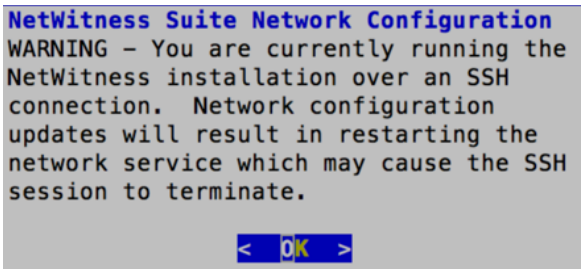
8. Si:

- 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.

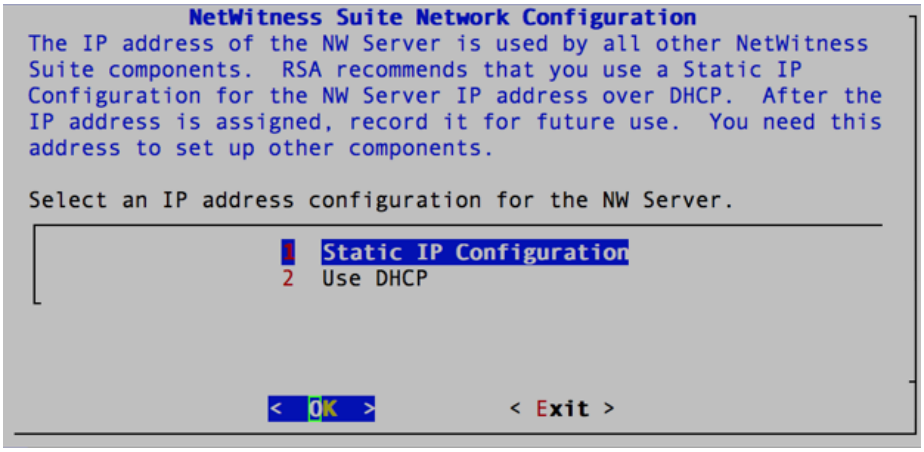
- Está usando una conexión de protocolo SSH, se muestra la siguiente advertencia.



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

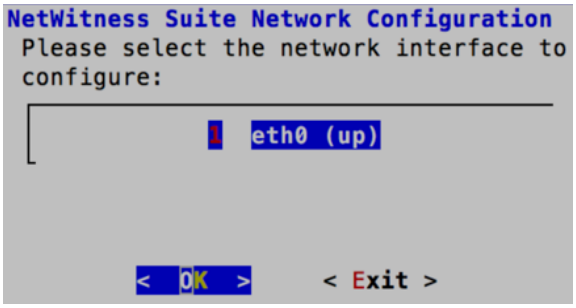
- El programa de instalación encontró una configuración de IP y usted decidió usarla, se muestra el indicador Repositorio de actualizaciones. Vaya al paso 12 para completar la instalación.

- 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 redes.



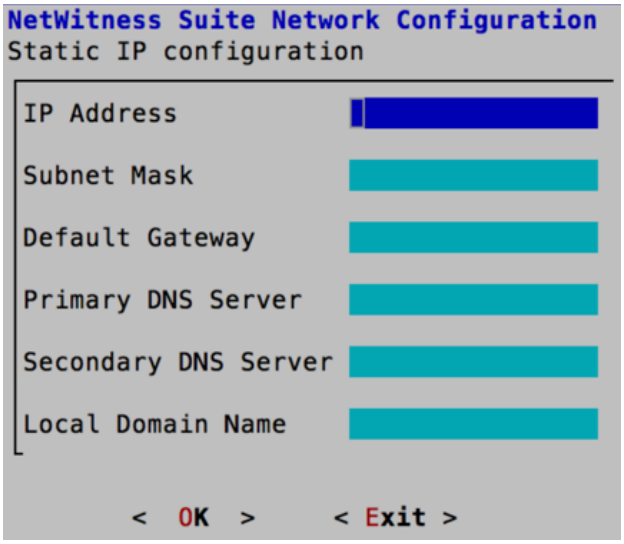
  Use la tecla de tabulación para ir a **Aceptar** y presione **Intro** para usar **Dirección IP estática**.
  Si desea usar **DHCP**, use la flecha hacia abajo para desplazarse hasta 2 Usar DHCP y presione **Intro**.

9. Se muestra el indicador Configuración de redes.



  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**.

10. Se muestra el indicador Configuración de IP estática.



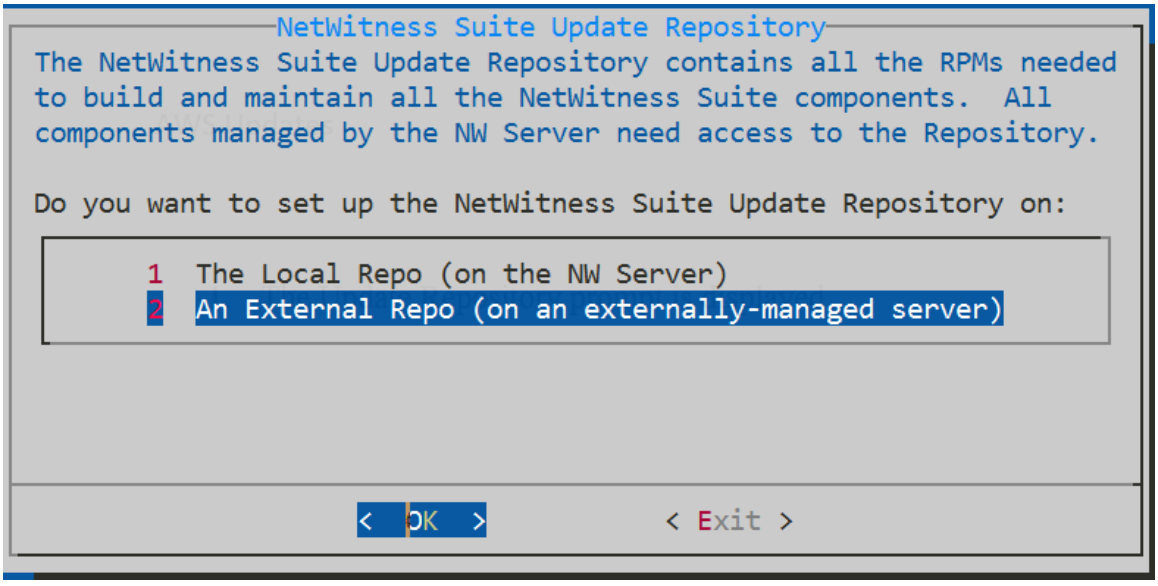
Escriba los valores de configuración (con la flecha hacia abajo para desplazarse de un campo a otro), use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

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

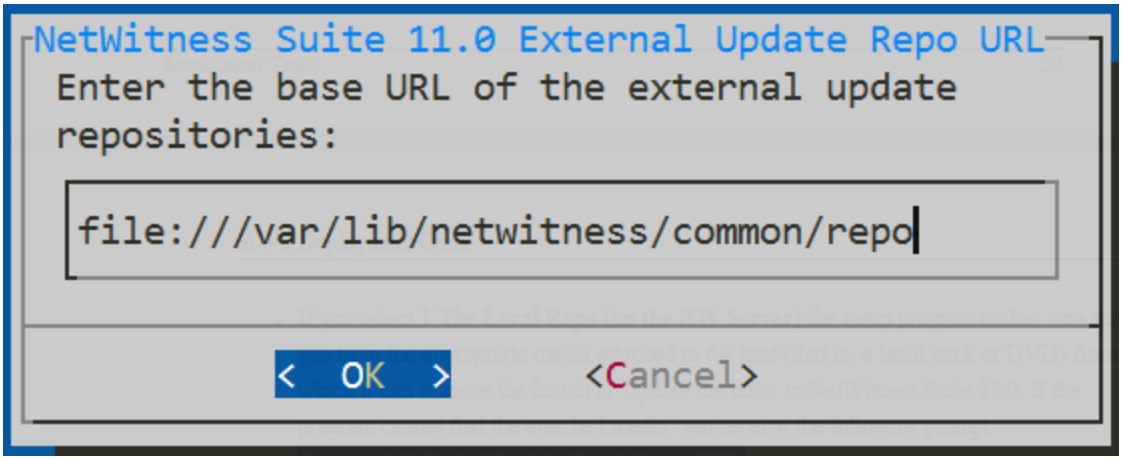
Si usa la sintaxis o la longitud de caracteres incorrectas para alguno de los campos, se muestra un mensaje de error *field-name* no válido.

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

11. Se muestra el indicador Repositorio de actualizaciones.



Seleccione **2 Un repositorio externo (en un servidor administrado externamente)**. La interfaz del usuario le solicita que indique una dirección URL.

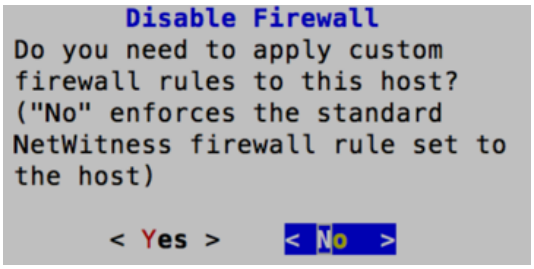


Use la dirección URL predeterminada del repositorio externo de NetWitness Suite y haga clic en **Aceptar**.

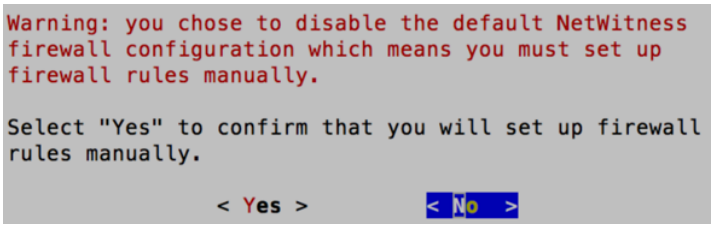
12. Aplique la configuración del firewall estándar y presione **Intro**.

    - Deshabilite la configuración estándar; use la tecla de tabulación para ir a **Sí** y presione **Intro**.

      Se muestra el indicador Deshabilitar el firewall.

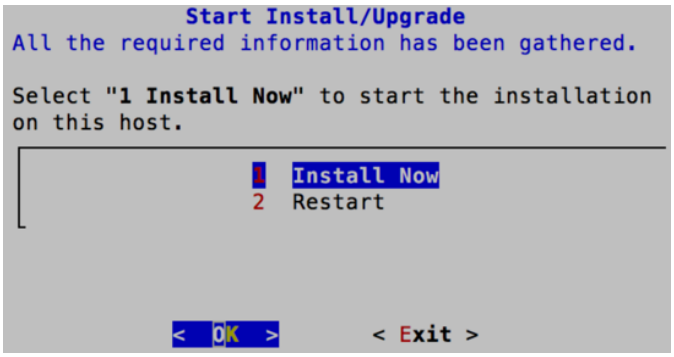
      Se muestra el indicador de confirmación de deshabilitación de la configuración del firewall.

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

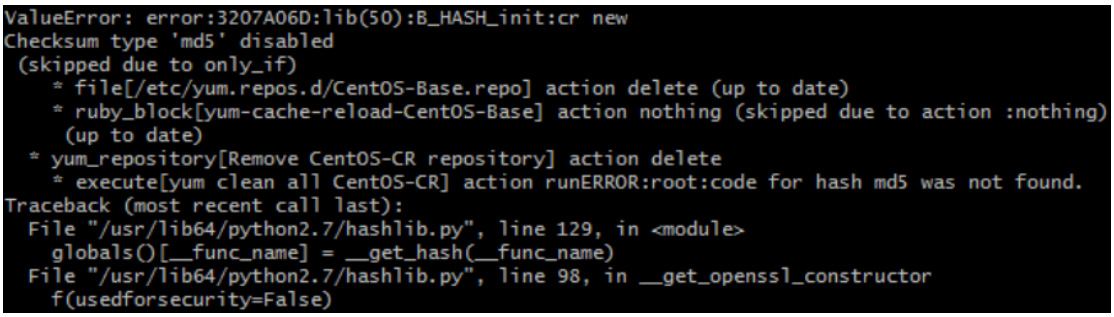
13. Presione **Intro** para instalar 11.0.0.0 en el servidor de NW.

    Se muestra el indicador Iniciar instalación.



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

Nota: Pase por alto los errores de código hash similares a los errores que se muestran en la siguiente captura de pantalla que aparecen cuando inicia el comando `nwsetup-tui`. Yum no usa MD5 para ninguna de las operaciones de seguridad, de modo que no afectan la seguridad del sistema.



Tarea 2: Instalar 11.0.0.0 en otros hosts de componentes

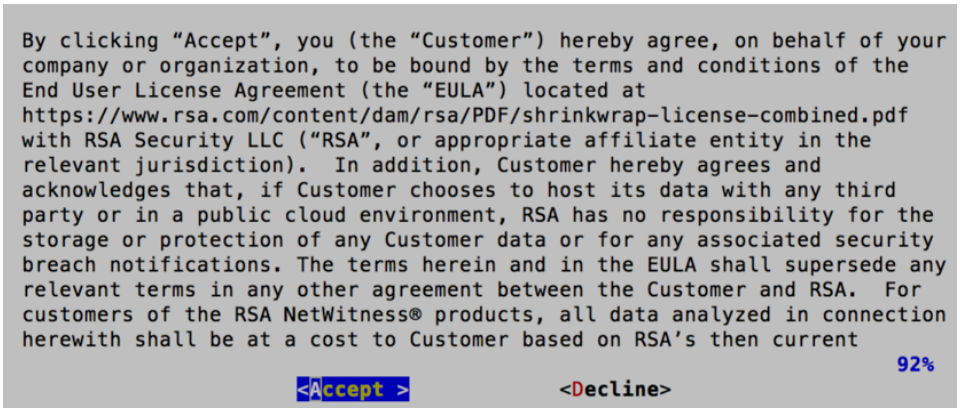
Nota: Puede realizar esta tarea para la instancia de RSANW-11.0.0.0.1245-Lite-01.

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

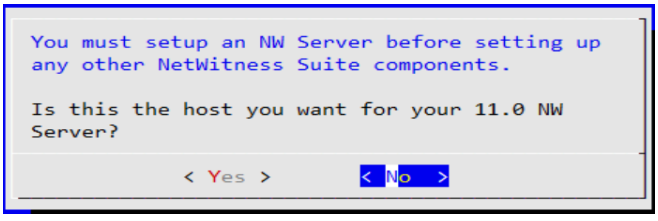
Esto inicia el programa de instalación y se muestra el EULA.

Nota: 1.) Cuando navegue por los indicadores del programa de instalación, use las flechas hacia abajo y hacia arriba para desplazarse entre los campos y use la tecla de tabulación para desplazarse hacia y desde los comandos (como **<Sí>**, **<No>**, **<Aceptar>** y **<Cancelar>**). Presione **Intro** para registrar la respuesta de los comandos y moverse al siguiente indicador.
2.) El programa de instalación adopta la combinación de colores del escritorio o de la consola que usa para acceder al host.
3.) Si especifica servidores DNS durante la ejecución del programa de instalación (`nwsetup-tui`), DEBEN ser válidos (válido en este contexto significa válido durante la configuración) y ser accesibles para que `nwsetup-tui` pueda continuar. Los servidores DNS configurados erróneamente hacen que la configuración falle. Si después de la configuración necesita acceder a un servidor DNS al que no se pudo acceder durante la configuración (por ejemplo, para reubicar un host después de la configuración que tenga un conjunto diferente de servidores DNS), consulte 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 Suite** en el paso 12 (los servidores DNS no están definidos, de modo que el sistema no puede acceder al repositorio externo).

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



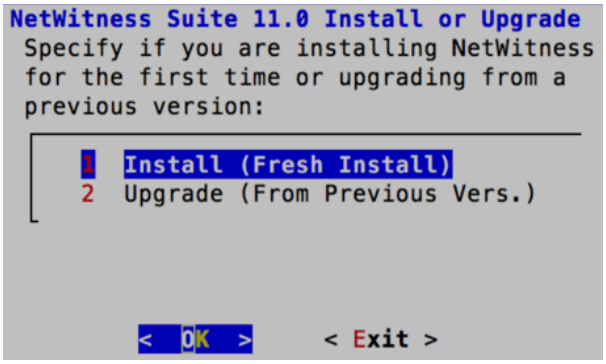
3. Se muestra el indicador "Este es el servidor de NW".



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

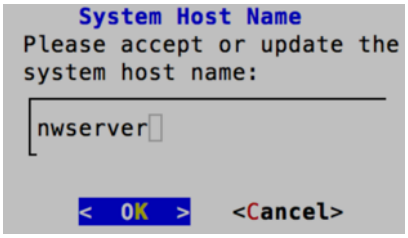
Precaución: Si elige el host incorrecto para el servidor de NW y completa la configuración, debe reiniciar el programa de instalación (paso 2) y completar todos los pasos subsiguientes para corregir este error.

4. Se muestra el indicador Instalar o Actualizar.



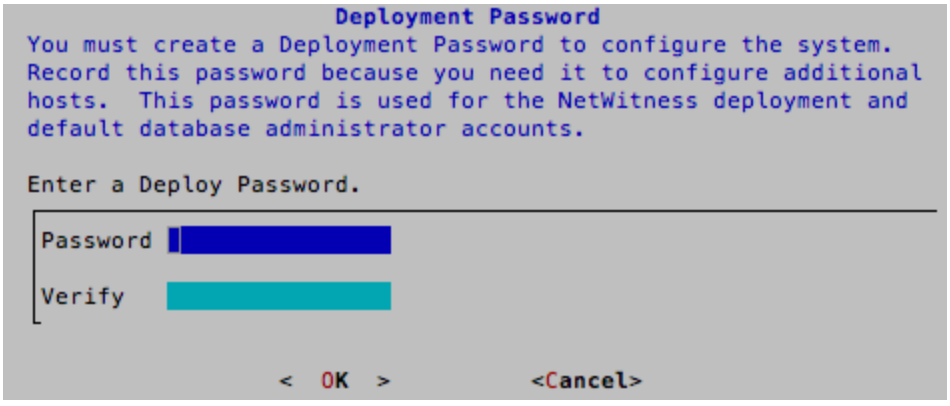
Presione **Intro** (la opción Instalar está seleccionada de manera predeterminada).

5. Se muestra el indicador "Nombre del host".



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.

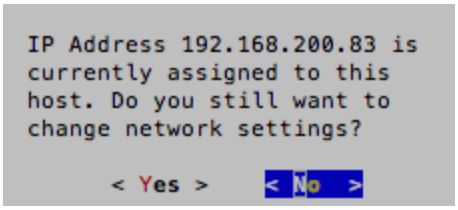
6. Se muestra el indicador "Contraseña de implementación".



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**.

7. Si:
   El programa de instalación encuentra una dirección IP válida para este host, se muestra el

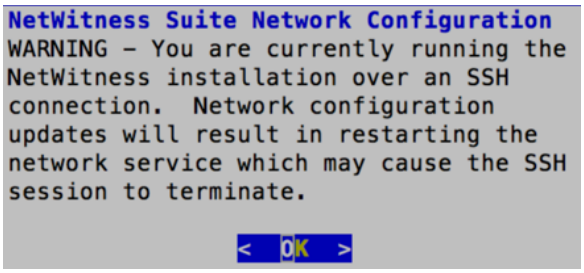
siguiente indicador.



Presione **Intro** si desea usar esta dirección IP y evitar cambiar la configuración de red.

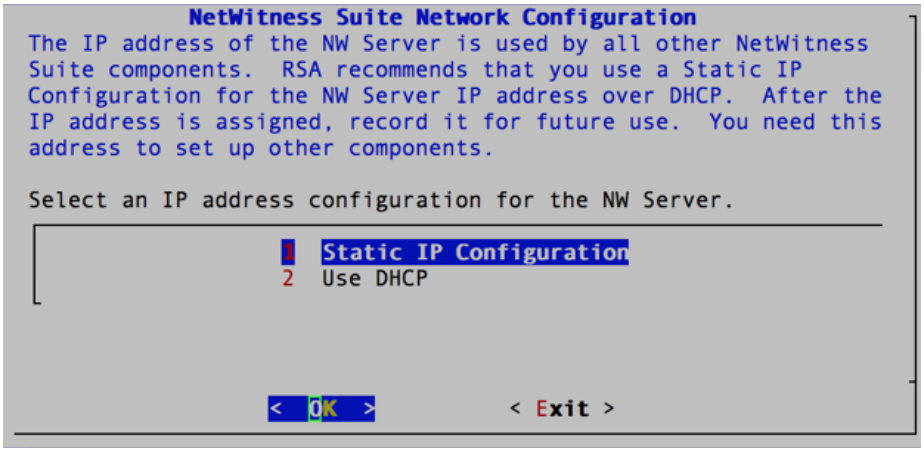
Use la tecla de tabulación para ir a **Sí** y presione **Intro** si desea cambiar la configuración de IP que se encontró en el host.

Está usando una conexión de protocolo SSH, se muestra la siguiente advertencia.



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

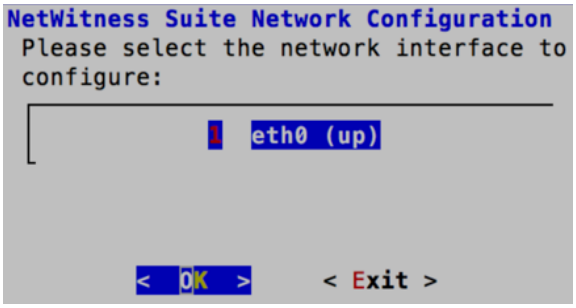
El programa de instalación no encontró una configuración de IP o usted decidió cambiar la configuración de IP existente, se muestra el indicador Configuración de redes.



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

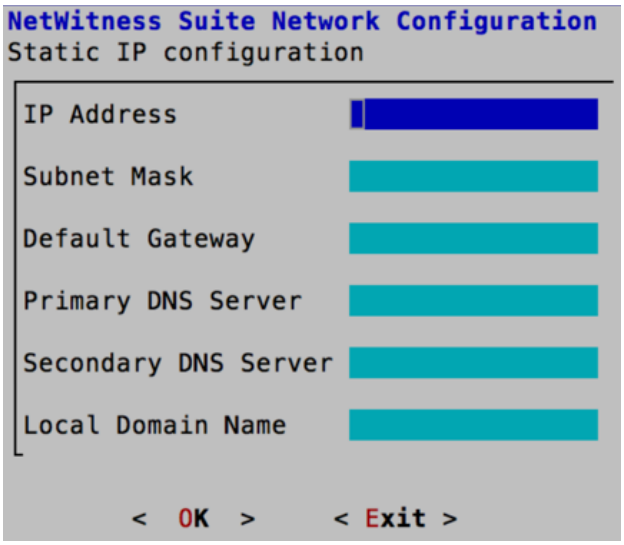
Si desea usar **DHCP**, use la flecha hacia abajo para desplazarse hasta 2 Usar DHCP y presione **Intro**.

8. Se muestra el indicador Configuración de redes.



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**.

9. Se muestra el indicador Configuración de IP estática.

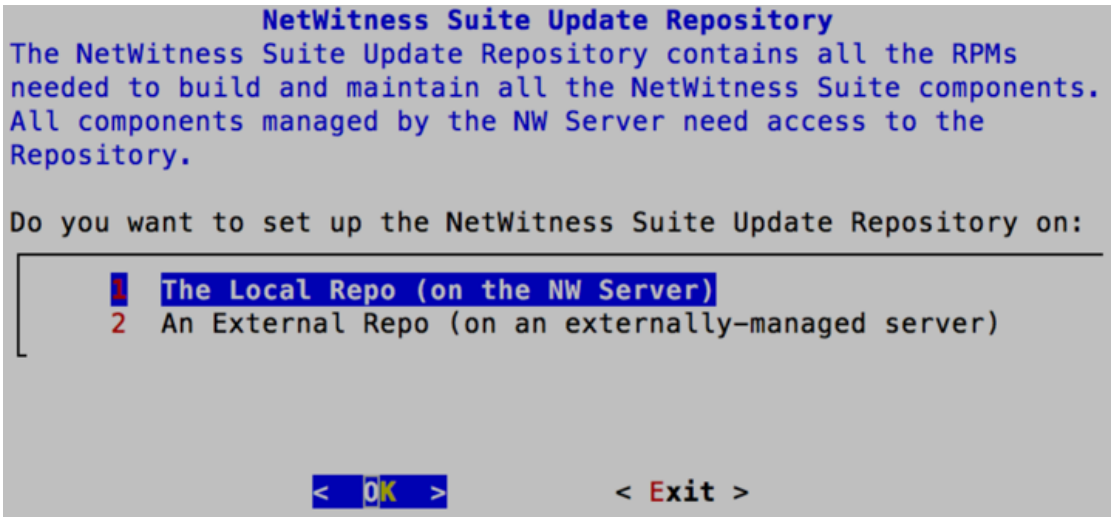


Escriba los valores de configuración (con la flecha hacia abajo para desplazarse de un campo a otro), use la tecla de tabulación para ir a **Aceptar** y presione **Intro**.

10. Si no completa todos los campos obligatorios, se muestra un mensaje de error Todos los campos son obligatorios (los campos **Servidor DNS principal**, **Servidor DNS secundario** y **Nombre de dominio local** no son obligatorios).
Si usa la sintaxis o la longitud de caracteres incorrectas para alguno de los campos, se muestra un mensaje de error *field-name* no válido.

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

11. Se muestra el indicador Repositorio de actualizaciones.

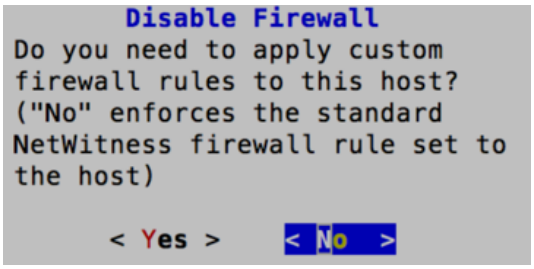


Presione **Intro** para elegir **Repositorio local** en el servidor de NW.

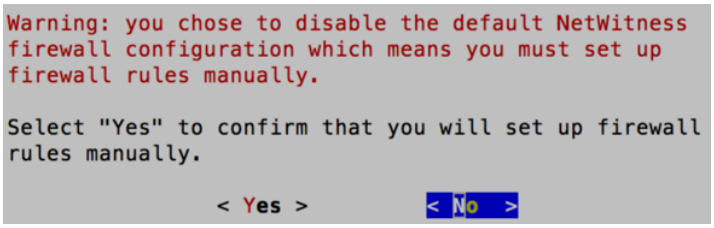
12. Para:

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

    Se muestra el indicador Deshabilitar el firewall.

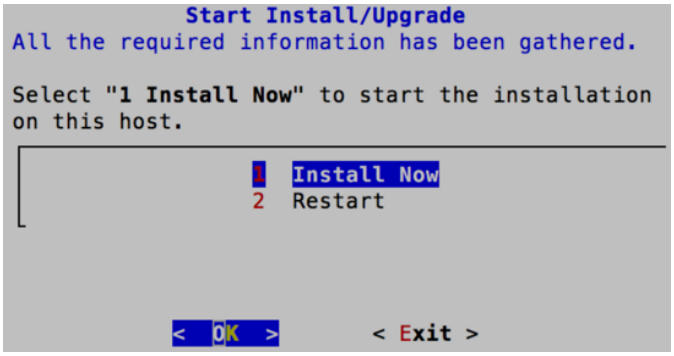


    Se muestra el indicador de confirmación de deshabilitación de la configuración del firewall.



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

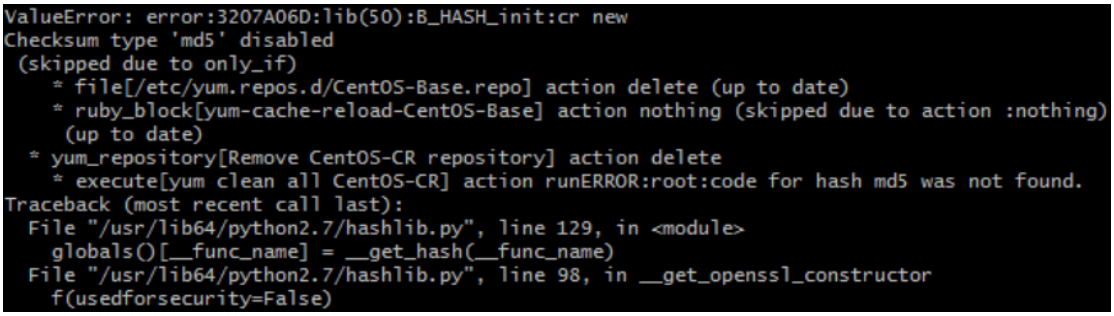
13. Se muestra el indicador Iniciar instalación.



    Presione **Intro** para instalar 11.0 en el servidor de NW.

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

Nota: Pase por alto los errores de código hash similares a los errores que se muestran en la siguiente captura de pantalla que aparecen cuando inicia el comando `nwsetup-tui`. Yum no usa MD5 para ninguna de las operaciones de seguridad, de modo que no afectan la seguridad del sistema.



Configurar hosts (instancias) en NetWitness Suite

Configure los hosts y los servicios individuales, como se describe en la *Guía de configuración de hosts y servicios* de RSA NetWitness® Suite. Esta guía también describe los procedimientos para aplicar actualizaciones y prepararse para las actualizaciones de versión.

Nota: Después de iniciar correctamente una instancia, AWS le asigna un nombre de host predeterminado. Consulte la documentación "Cambiar el nombre y el nombre de host de un host" en RSA Link (https://community.rsa.com) para obtener instrucciones sobre cómo cambiar un nombre de host.

Configurar la captura de paquetes

Puede integrar cualquiera de las siguientes soluciones de otros fabricantes con el Packet Decoder para capturar paquetes en la nube de AWS:

- Gigamon® GigaVUE
- f5® BIG-IP

Integrar Gigamon GigaVUE con el Packet Decoder

Existen dos tareas principales para configurar la solución de captura de paquetes de proveedores Tap de otros fabricantes Gigamon®:

Tarea 1. Integrar la solución Gigamon®.

Tarea 2. Configurar un túnel en el Packet Decoder.

Tarea 1. Integrar la solución Gigamon

La plataforma de visibilidad de Gigamon® en AWS estará disponible en AWS Marketplace y se activará mediante una licencia BYOL. También está disponible una prueba gratuita de treinta días.

Para obtener más información sobre la solución Gigamon®, consulte la “Hoja de datos de la plataforma de visibilidad de Gigamon® para AWS” (https://www.gigamon.com/sites/default/files/resources/datasheet/ds-gigamon-visibility-platform-for-aws-4095.pdf).

Para obtener los detalles de implementación, consulte la “Guía de introducción de la plataforma de visibilidad de Gigamon® para AWS” (https://www.gigamon.com/sites/default/files/resources/deployment-guide/dg-visibility-platform-for-aws-getting-started-guide-4111.pdf).

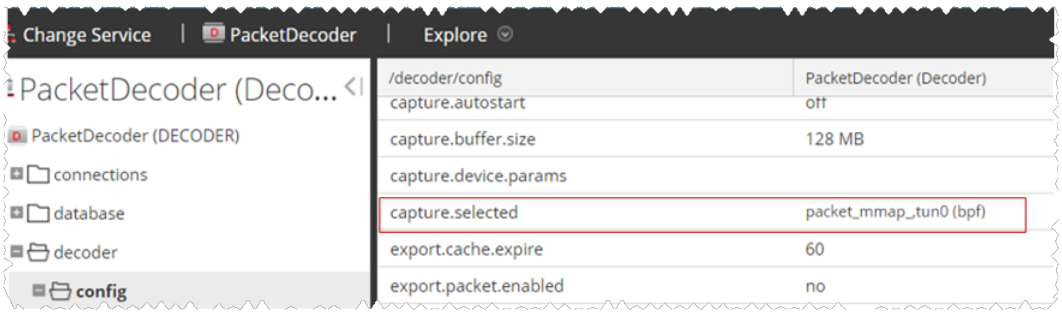
Después de implementada la “Sesión de monitoreo” dentro de Gigamon GigaVUE-FM, puede configurar el túnel del Packet Decoder.

Tarea 2. Configurar un túnel en el Packet Decoder

1. Acceda mediante el protocolo SSH a Decoder.
2. Ejecute las siguientes cadenas de comandos.

```
$ sudo ip link add tun0 type gretap local any remote <ip_address_of_
VSERIES_NODE_TUNNEL_INTERFACE> ttl 255

$ sudo ip link set tun0 up mtu <MTU-SIZE>

$ sudo ifconfig (to verify if the tunnel tun0 is being listed in the
list of interfaces)

$ sudo lsmod | grep gre ( to make sure if the below kernel modules
are running:

ip_gre 18245 0

ip_tunnel 25216 1)

If they are not running then execute the below commands to enable the
modules

$ sudo modprobe act_mirred

$ sudo modprobe ip_gre
```

3. Cree una regla de firewall en el Packet Decoder para permitir el tráfico a través del túnel.
   a. Abra el archivo `iptables`.
      `vi /etc/sysconfig/iptables`
   b. Agregue la línea `-A INPUT -p gre -j ACCEPT` antes de la declaración `commit`.
   c. Reinicie `iptables` mediante la ejecución de los siguientes comandos.
      `service iptables restart`
4. Configure la interfaz en el Packet Decoder.
   a. Inicie sesión en NetWitness Suite y seleccione el nodo `decoder/config` en la vista Explorador para el servicio Packet Decoder.
   b. Configure `capture.selected` en `packet_mmap_,tun0`.



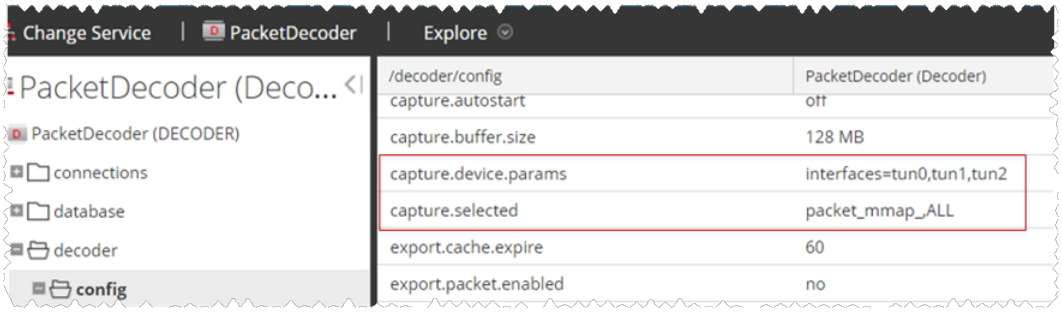
5. (Condicional): Si tiene múltiples túneles en el Packet Decoder.

   a. Reinicie el servicio Decoder después de crear el túnel en el Packet Decoder.

   b. Inicie sesión en NetWitness Suite, seleccione el nodo `decoder/config` en la vista Explorador para el servicio Packet Decoder y configure los siguientes parámetros.

   ```
   capture.device.params = interfaces=tun0,tun1,tun2
   ```

   ```
   capture.selected = packet_mmap_,All
   ```



6. Reinicie el servicio Decoder.

   ```
   $ sudo restart nwdecoder
   ```

   El usuario debe realizar todas las configuraciones correspondientes para capturar el tráfico de red en el Decoder.

Realice los siguientes pasos para crear un nuevo proyecto y obtener la clave del proyecto.

Integrar f5® BIG-IP con el Packet Decoder

IG-IP Virtual Edition (VE) es un servidor virtual y un balanceador de carga en línea. Un caso de uso común sería que la computadora f5® sea un servidor web virtual que presenta una sola dirección IP o un solo nombre de host que administra las solicitudes a un pool de servidores web en la nube.

Todo el tráfico a RSA NetWitness® Suite fluye a través del servidor virtual de f5® BIG-IP VE.

Las funciones de servidor virtual de BIG-IP clonan todo el tráfico a una computadora designada, lo que se logra mediante la reescritura de direcciones MAC y su carga en una subred que comparte con el sniffer de destino. Esta guía describe cómo configurar el Decoder como el sniffer.

Información de implementación de f5® BIG-IP VE

f5® BIG-IP VE en AWS estará disponible en AWS Marketplace y se activará mediante una licencia BYOL. También está disponible una prueba gratuita de treinta días.

Para obtener más información sobre esta solución, consulte la Hoja de datos de DNS de f5® BIG-IP (https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf).

Tarea 1: Configurar una instancia del servidor virtual BIG-IP VE

Configure una instancia de servidor virtual de BIG-IP VE según las instrucciones de "BIG-IP Virtual Edition 12.1.0 and Amazon Web Services: Multi-NIC Manual" (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-multi-nic-setup-amazon-ec2-12-1-0.html). Realice todo el proceso hasta el último paso, "Creación de un servidor virtual".

En este servidor virtual se ejecuta la captura de paquetes. Es posible que deba crear múltiples servidores virtuales según su volumen.

Como parte de la creación del servidor virtual, debe tener al menos un servidor en el dominio de NetWitness Suite para manejar el tráfico que se enruta mediante el servidor virtual (por ejemplo, puede crear otra instancia en AWS para alojar el servidor interno).

Tarea 2: Crear un pool de clones

1. Asegúrese de que la instancia de Decoder tenga una interfaz de red en la misma subred que una de las interfaces de red en la instancia de BIG-IP VE.
   El pool de clones envía paquetes al Decoder mediante la reescritura de direcciones MAC y su envío a una interfaz de red. La reescritura de direcciones MAC puede utilizarse para enrutar paquetes a otra subred.
2. Configure el pool de clones dentro del servidor virtual de BIG-IP VE según las instrucciones del artículo "K13392: Configuración del sistema de BIG-IP para enviar tráfico a un sistema de detección de intrusiones (11.x - 13.x)" (https://support.f5.com/kb/en-us/solutions/public/13000/300/sol13392.html).
   Este documento explica cómo crear el pool de clones y cómo hacer que un servidor virtual existente copie tráfico en el pool de clones. En este caso, la instancia de Decoder se colocará en el pool de clones.

Reglas

Las siguientes reglas lo ayudarán a configurar la captura de paquetes correctamente mediante BIG-IP VE.

- La instancia de Decoder debe tener su propia dirección IP en una de las mismas subredes que BIG-IP VE. BIG-IP usa esa dirección IP para identificar el Decoder como parte del pool de clones.
- Cuando se agrega la instancia de Decoder al pool de clones, BIG-IP solicita un número de puerto, además de la dirección IP. Este número de puerto no es relevante para el tráfico clonado. El Decoder recibirá todo el tráfico clonado, independientemente del número de puerto que se usa aquí.

- De forma predeterminada, la subred AWS que comparten el Decoder y BIG-IP VE no permitirá que el tráfico clonado viaje desde la interfaz de BIG-IP VE a la interfaz de Decoder. Debe deshabilitar **`source/dest. check`** en el Decoder y en las interfaces de red de BIG-IP VE en AWS.
- La instancia de Decoder debe tener una sola interfaz de red, eth0, de manera predeterminada. El Decoder captura el tráfico en esta interfaz, pero también puede recibir el tráfico administrativo en ella. RSA recomienda usar reglas de red para filtrar el tráfico del protocolo SSH y nwdecoder del flujo de captura. Estos son los puertos 22 (protocolo SSH) y 50004/56004 (nwdecoder).

Consejos para la solución de problemas

Hay áreas para solucionar problemas si el Decoder no acepta los paquetes.

- Asegúrese de que el BIG-IP VE esté enviando los paquetes fuera de la interfaz correcta. La instancia de BIG-IP VE contiene tcpdump. Úsela para verificar que los paquetes clonados se envían fuera de la interfaz esperada. Si no es así, existe un problema en la configuración del pool de clones o el servidor virtual.
- Asegúrese de que el Decoder esté recibiendo paquetes.
  El Decoder tiene instalado `tcpdump`. Úselo para verificar que el Decoder está recibiendo paquetes. Si el Decoder no está capturando paquetes, asegúrese de que
  - AWS **`source/dest. check`** esté apagado.
  - El Decoder esté en la misma subred que la interfaz que BIG-IP VE está usando para clonar los paquetes.

Recomendaciones de configuración de instancias de AWS

Nota: Estas recomendaciones satisfacen las condiciones de RSA Security Analytics versión 10.6.3. Se pueden utilizar como base para 11.0.0.0 y ajustar según sea necesario.

Nota: Para obtener una descripción de los términos y las abreviaturas que se usan en este tema, consulte Abreviaturas y otra terminología que se usan en esta guía.

En este tema se enumeran los ajustes de configuración mínimos recomendados de la instancia de AWS para los componentes de la plataforma virtual de RSA NetWitness® Suite.

- Instancia de EC2:
  - Tipo de instancia mínimo: **m4-2xlarge** es el tipo de instancia mínimo requerido para que cualquier AMI de componente de NetWitness Suite pueda funcionar.
  - Ajustes de tipo de instancia: Debe ajustar los tipos de instancia según la tasa de recopilación, el contenido y los analizadores, los informes de tablero, los informes programados, las investigaciones y los usuarios activos.
  - Configuración recomendada: La configuración recomendada en las tablas de instancia de componente de SA que aparece a continuación se calculó en las siguientes condiciones.
    - Se usaron tasas de recopilación de 15,000 EPS y 1.5 Gb/s.
    - Todos los componentes estaban integrados.
    - El flujo de registros incluía un Log Decoder, un Concentrator y un Archiver.
    - El flujo de paquetes incluía un Packet Decoder y un Concentrator.
    - Respond recibía alertas de Reporting Engine y Event Stream Analysis.
    - La carga en segundo plano incluía informes, gráficos, alertas, investigation y respond.
- Volúmenes de EBS (almacenamiento)

  Póngase en contacto con el servicio al cliente de RSA (https://community.rsa.com/docs/DOC-1294) para obtener ayuda sobre cómo aumentar el número de volúmenes en función de sus requisitos de almacenamiento mediante Sizing & Scoping Calculator de RSA.

  Nota: El volumen de índice del Concentrator se debe asignar en el disco SSD de IOPS aprovisionado.

- Índice
- Metadatos
- Sesión
- Packet

Archiver

Instancia de EC2			
EPS	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
5,000	m4.xlarge N.º de CPU: 4 Memoria: 16 GB	No	Sí
10,000	m4.2xlarge N.º de CPU: 8 Memoria: 32 GB	No	Sí
15,000	m4.4xlarge N.º de CPU: 16 Memoria: 64 GB	No	Sí

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
archiver	/dev/sdg	Disco duro de rendimiento optimizado	240 MB/s

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
Workbench	/dev/sdh	Disco duro de rendimiento optimizado	N/D

Broker

Instancia de EC2		
Tipo de instancia	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
m4.xlarge N.º de CPU: 4 Memoria: 16 GB	No	Sí

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
broker	/dev/sdg	Disco SSD de propósito general	N/D

Concentrator: Flujo de registros

Instancia de EC2			
EPS	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
5,000	m4.xlarge N.º de CPU: 4 Memoria: 16 GB	No	Sí
10,000	m4.2xlarge N.º de CPU: 8 Memoria: 32 GB	No	Sí
15,000	m4.4xlarge N.º de CPU: 16 Memoria: 64 GB	No	Sí

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
index, session	/dev/sdg	IOPS aprovisionadas	10,000
metadb	/dev/sdh	Disco duro de rendimiento optimizado	240 MB/s

Soluciones de flujo de paquetes

Concentrator: Solución de Gigamon

Instancia de EC2			
Mb/s/Gb/s	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
500 Mb/s	c4.4xlarge N.º de CPU: 16 Memoria: 30 GB	No	Sí
1,000 Mb/s	c4.8xlarge N.º de CPU: 36 Memoria: 60 GB	No	Sí
1.5 Gb/s	m4.10xlarge N.º de CPU: 40 Memoria: 160 GB	No	Sí

Concentrator: Solución de f5 BIG-IP

Se actualizará cuando se completen las pruebas de rendimiento de f5 BIG-IP.

Instancia de EC2			
Mb/s/Gb/s	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
230 Mb/s	m4.4xlarge N.º de CPU: 16 Memoria: 64 GB	No	No

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
index, session	/dev/sdg	IOPS aprovisionadas	15,000
metadb	/dev/sdh	Disco duro de rendimiento optimizado	240 MB/s

Decoder: Solución de Gigamon

Instancia de EC2			
Mb/s/Gb/s	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
500 Mb/s	c4.2xlarge N.º de CPU: 8 Memoria: 15 GB	Sí	Sí
1,000 Mb/s	c4.4xlarge N.º de CPU: 16 Memoria: 30 GB	Sí	Sí
1.5 Gb/s	c4.8xlarge N.º de CPU: 36 Memoria: 60 GB	Sí	Sí

Decoder: Solución de f5 BIG-IP

Se actualizará cuando se completen las pruebas de rendimiento de f5 BIG-IP.

Instancia de EC2			
Mb/s/Gb/s	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
230 Mb/s	m4.4xlarge N.º de CPU: 16 Memoria: 64 GB	No	No

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
index, session, meta	/dev/sdg	Disco duro de rendimiento optimizado	240 MB/s
packet	/dev/sdh	Disco duro de rendimiento optimizado	240 MB/s

ESA y Context Hub en base de datos de Mongo

	Instancia de EC2		
EPS	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
9,000	m4.2xlarge N.º de CPU: 8 Memoria: 32 GB	No	Sí
18,000	r4.2xlarge N.º de CPU: 8 Memoria: 61 GB	No	Sí
30,000 Tasa de agregación	r4.4xlarge N.º de CPU: 16 Memoria: 122 GB	No	Sí

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
apps (/opt/rsa)	/dev/sdg	Disco SSD de propósito general	N/D

Log Collector (Syslog, Netflow y protocolos de recopilación de archivos)

Instancia de EC2			
EPS	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
30,000 NO SSL	c4.2xlarge N.º de CPU: 8 Memoria: 15 GB	No	Sí

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
logcollector	/dev/sdg	Disco SSD de propósito general	N/D

Log Decoder

Instancia de EC2			
EPS	**Tipo de instancia**	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
5,000	c4.2xlarge N.º de CPU: 8 Memoria: 15 GB	Sí	Sí
10,000	c4.4xlarge N.º de CPU: 16 Memoria: 30 GB	Sí	Sí
15,000	c4.8xlarge N.º de CPU: 36 Memoria: 60 GB	Sí	Sí

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
index, session, meta	/dev/sdg	Disco duro de rendimiento optimizado	240 MB/s
packet	/dev/sdh	Disco duro de rendimiento optimizado	240 MB/s

Servidor de NetWitness, Reporting Engine, Respond y Estado y condición

Instancia de EC2		
Tipo de instancia	**Redes mejoradas habilitadas**	**Tipo de multiusuario: exclusivo; Ejecutar una instancia exclusiva**
m4.2xlarge N.º de CPU: 8 Memoria: 32 GB	No	Sí
m4.4xlarge N.º de CPU: 16 Memoria: 64 GB	No	Sí

Volúmenes de EBS (almacenamiento)			
Volúmenes	**Dispositivo**	**Tipo de volumen**	**IOPS/Rendimiento de base**
/ (root)	/dev/sda1	Disco SSD de propósito general	N/D
usr, var, opt, home, tmp	/dev/sdf	Disco SSD de propósito general	N/D
uax, ipdb	/dev/sdg	Disco SSD de propósito general	N/D
redb, rehome	/dev/sdh	Disco SSD de propósito general	N/D