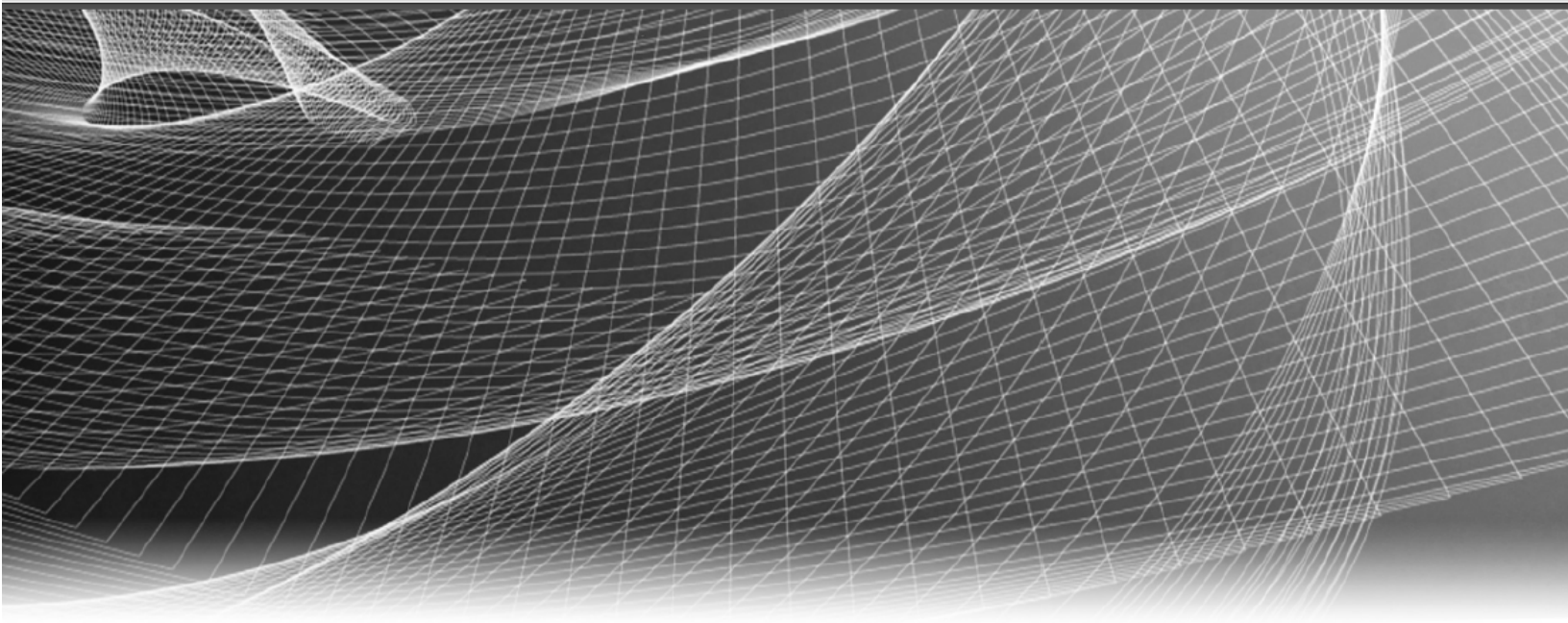


RSA Security Analytics

Guía de instalación de hosts virtuales

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Guía de instalación de hosts virtuales

Este documento se aplica exclusivamente a la instalación y la configuración de hosts de Security Analytics que se ejecutan en un ambiente virtual.

Implementación virtual básica

Este tema presenta reglas y requisitos generales para la implementación de Security Analytics en un ambiente virtual.

Abreviaturas que se utilizan en la Guía de implementación virtual

Abreviaturas	Descripción
CPU	Unidad central de procesamiento
EPS	Eventos por segundo
VMware ESX	Hipervisor tipo 1 de clase empresarial
GB	Gigabyte. 1 GB = 1,000,000,000 de bytes
Gb	Gigabit. 1 Gb = 1,000,000,000 de bits.
Gb/s	Gigabits por segundo o mil millones de bits por segundo. Mide el ancho de banda en un medio de transmisión de datos digital, como la fibra óptica.
GHz	GigaHertz 1 GHz = 1,000,000,000 de Hz
IOPS	Operaciones de entrada/salida por segundo
IPDB	Operaciones de entrada/salida por segundo
Mb/s	Megabits por segundo o un millón de bits por segundo. Mide el ancho de banda en un medio de transmisión de datos digital, como la fibra óptica.
NAS	Almacenamiento conectado en red
OVF	Formato de virtualización de código abierto
OVA	Dispositivo virtual abierto. Para los fines de esta guía, OVA significa host virtual abierto.
RAM	Memoria de acceso aleatorio (también conocida como memoria)

Abreviaturas	Descripción
SAN	Red de área de almacenamiento
Disco duro SSD/EFD	Disco duro de estado sólido/Enterprise Flash Drive
SCSI	Small Computer System Interface
SCSI (SAS)	Protocolo serie de punto a punto que transfiere datos hacia y desde dispositivos de almacenamiento de computadoras, como discos duros y unidades de cinta.
vCPU	Unidad central de procesamiento virtual (también conocida como un procesador virtual)
vRAM	Memoria de acceso aleatorio virtual (también conocida como memoria virtual)

Hosts virtuales compatibles

Puede instalar los siguientes hosts de Security Analytics en el ambiente virtual como un host virtual y heredar funciones que proporciona el ambiente virtual:

- Servidor de Security Analytics
- Archiver
- Broker
- Concentrator
- Event Stream Analysis
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Warehouse Connector

Debe conocer los siguientes conceptos de la infraestructura de VMware:

- VMware vCenter Server
- Host de VMware
- Máquina virtual

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

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

Medios de instalación

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

Recomendaciones para ambientes virtuales

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

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

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

Requisitos del sistema recomendados para un host virtual

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

- La asignación del almacenamiento se explica en el paso 3 “Configurar las bases de datos para adaptarse a la suite Security Analytics”.
- Las recomendaciones de vRAM y vCPU pueden variar según las tasas de captura, la configuración y el contenido habilitado.
- Las recomendaciones se probaron a tasas de recopilación de hasta 25,000 EPS para los registros y 2 GB/s para los paquetes.
- Las especificaciones de vCPU para todos los componentes que se enumeran en las siguientes tablas son
  CPU Intel Xeon a 2.59 Ghz.
- Todos los puertos son SSL.

Log Decoder

EPS	vCPU de labo-ratorio	vRAM de labo-ratorio	vCPU de pro-ducción	vRAM de pro-ducción	Lec-tura IOPS	Escri-tura IOPS
10,000	8	30 GB	16	50 GB	300	50
15,000	12	40 GB	20	60 GB	550	100

Packet Decoder

Mb/s	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
500	8	40 GB	8	40 GB	150	200
1,000	12	40 GB	12	50 GB	200	400
1,500	16	50 GB	16	75 GB	200	500

Concentrator para el flujo de registros

EPS	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
10,000	4	30 GB	10	50 GB	1,600	6,500
15,000	6	40 GB	12	60 GB	1,600	7,600

Concentrator para el flujo de paquetes

Mb/s	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
500	8	30 GB	12	50 GB	250	4,600
1,000	12	40 GB	16	50 GB	550	5500
1,500	16	50 GB	24	75 GB	1,050	6,500

Warehouse Connector para el flujo de registros

EPS	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
10,000	6	20 GB	8	30 GB	50	50
15,000	6	30 GB	10	35 GB	50	50

Warehouse Connector para el flujo de paquetes

Mb/s	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
500	6	20 GB	6	20 GB	50	50
1,000	6	30 GB	6	30 GB	50	50
1,500	8	40 GB	8	40 GB	50	50

Archiver para el flujo de registros

EPS	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
10,000	8	10 GB	12	40 GB	1,300	700
15,000	12	20 GB	14	45 GB	1,200	900

Event Stream Analysis (ESA) con Context Hub

EPS	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
90,000	12	50 GB	32	94 GB	50	50

Servidor de Security Analytics (NW)

vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
8	50 GB	12	50 GB	100	50

Broker

vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
4	10 GB	4	10 GB	100	350

Log Collector (local y remoto)

EPS	vCPU de laboratorio	vRAM de laboratorio	vCPU de producción	vRAM de producción	Lectura IOPS	Escritura IOPS
15,000	8	8 GB	8	8 GB	50	50
30,000	8	15 GB	8	15 GB	100	100

Reglas de dimensionamiento de los recopiladores de Windows heredado

Consulte la documentación de *Actualización e instalación de la recopilación de Windows heredado de RSA Security Analytics* para conocer las reglas de dimensionamiento del recopilador de Windows heredado.

Instalar el host virtual de Security Analytics en un ambiente virtual

Complete los siguientes procedimientos de acuerdo con su secuencia numerada para instalar Security Analytics en un ambiente virtual.

Requisitos previos

Asegúrese de haber:

- Un VMware ESX Server que cumpla los requisitos descritos en Descripción general de dispositivos virtuales.
- vSphere 4.1 Client o vSphere 5.0 Client instalados para iniciar sesión en VMware ESX Server.
- Derechos de administrador para crear las máquinas virtuales en VMware ESX Server.

Paso 1. Implementar el host virtual

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

Requisitos previos

Asegúrese de haber:

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

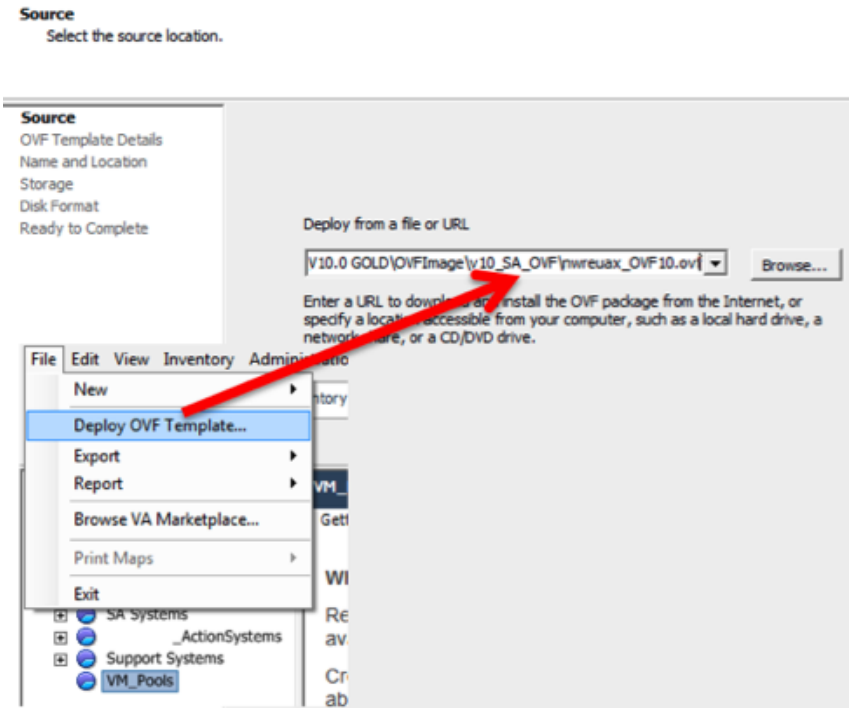
Nota: Cuando inicia sesión, se ejecuta un script que le solicita la dirección IP del host del servidor de Security Analytics (servidor de SA). Presione **Intro**, sin dirección IP, o **Ctrl-C** para salir de este script. Una vez que complete la configuración del host actual y que el host del servidor de SA esté en línea y listo para aceptar hosts, ingrese la dirección IP de Security Analytics en este indicador mediante el cierre y el inicio de una sesión.

Procedimiento

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

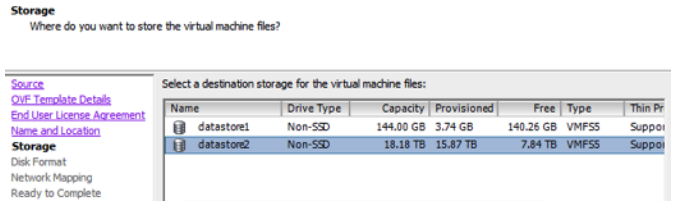
Para implementar el host OVA:

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



3. En el cuadro de diálogo **Implementar plantilla OVF**, seleccione el OVF del host que desea implementar en el ambiente virtual (por ejemplo, **V10.0 GOLD\OVFImge\v10_SA_OVF\nwreuax_OVF10.ovf**) y haga clic en **Siguiente**.
   Aparece el cuadro de diálogo Nombre y Ubicación. El nombre designado no refleja el nombre de host del servidor. El nombre que aparece es útil como referencia del inventario desde dentro de ESXi.

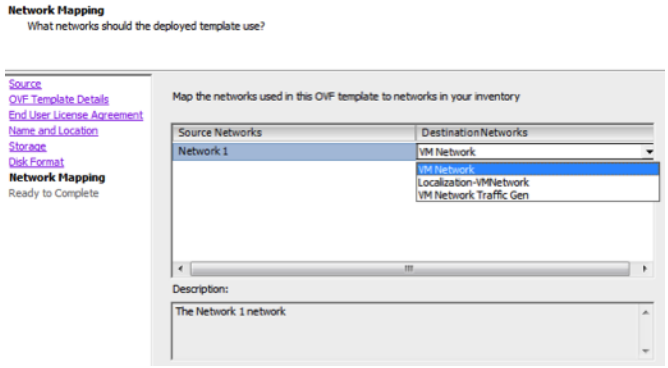
4. Anote el nombre y haga clic en **Siguiente**.
   Aparecen las opciones de almacenamiento.



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

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

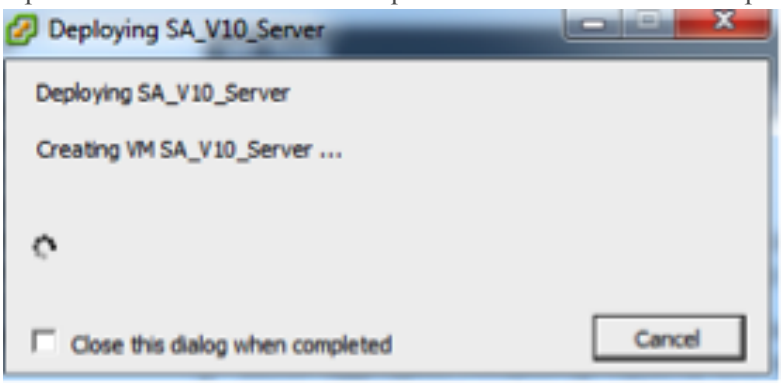
6. Haga clic en **Siguiente**.
   Aparece la opción Mapeo de red.



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

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

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



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

Paso 2. Configurar la red

Consulte "Conectar el dispositivo y configurar parámetros de red" en la *Guía de instalación de los dispositivos NetWitness serie 5* para obtener instrucciones detalladas sobre cómo configurar los parámetros de red.

Paso 3. Configurar las bases de datos para adaptarse a Security Analytics

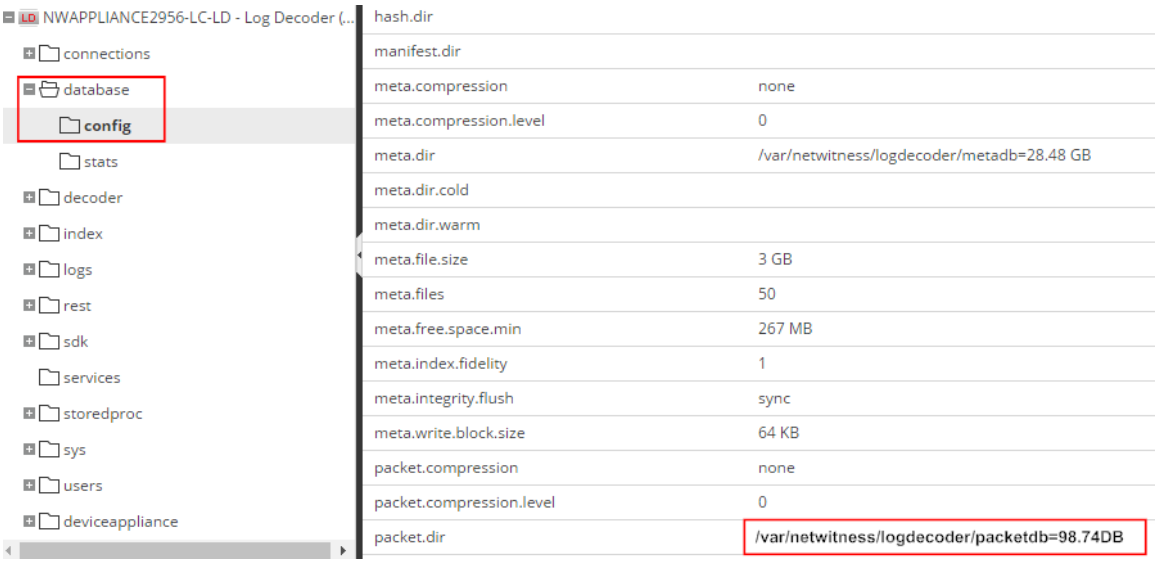
Cuando implementa bases de datos desde OVA, es posible que la asignación inicial de espacio de la base de datos no sea suficiente para admitir Security Analytics. Debe revisar el estado de los almacenes de datos después de la implementación inicial y expandirlos.

Tarea 1. Revisar la configuración inicial del almacén de datos

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

Espacio inicial asignado a PacketDB

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



Tamaño inicial de la base de datos

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

[root@LogDecoderGM ~1}# df -k

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

```
/dev/mapper/VolGroup01-logcoll
                      67076096   42652   67033444   1%
/var/netwitness/logcollector
/dev/mapper/VolGroup01-packetdb
                      108994564   37152  108957412   1%
/var/netwitness/logdecoder/packetdb
```

Punto de montaje de PacketDB

La base de datos se monta en el volumen lógico `packetdb` del grupo de volúmenes `VolGroup01`, y es aquí donde comienza la planificación de la expansión para el sistema de archivos.

Estado inicial de VolGroup01

Complete los siguientes pasos para revisar el estado de `VolGroup01`.

1. Acceda al host de Log Decoder mediante el protocolo SSH.
2. Ingrese la cadena de comandos `lvs` (mostrar volúmenes lógicos) para determinar los volúmenes lógicos que están agrupados en `VolGroup1`.

```
[root@LogDecoderGM ~1}# lvs VolGroup01.
```

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

```
LV      VG       Attr      LSize   Pool Origin Data%  Move Log Cpy%Sync
Convert
decoroot VolGroup01  -wi-ao---  20.00g
index  VolGroup01  -wi-ao---  10.00g
logcoll  VolGroup01  -wi-ao---  64.00g
metadb    VolGroup01  -wi-ao---  44.00g
packetdb VolGroup01  -wi-ao--- 104.00g
sessiondb  VolGroup01  -wi-ao---  30.00g
```

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

   ```
   [root@LogDecoderGM ~1}# pvs
   ```

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

   ```
   PV      VG    Fmt  Attr  PSize   PFree
   /dev/sdb1  VolGroup00 lvm2 a--   32.00g  0
   /dev/sdc1  VolGroup01 lvm2 a--   104.00g
   /dev/sdd1  VolGroup01 lvm2 a-- 168.00g 0
   ```

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

   ```
   [root@LogDecoderGM ~1}# vgs
   ```

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

   ```
   VG      #PV #LV #SN Attr   VSize   VFree
   VolGroup00   1   7   0   wz--n-  32.00g  0
   VolGroup01  2   6   0   wz--n-  32.00g  0
   ```

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

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

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

Tasas de espacio de unidad virtual

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

Decoder			
Persistente Áreas de almacenamiento de datos	Almacén de datos de caché		
PacketDB	SessionDB	MetaDB	Index
100 % según el cálculo de Sizing & Scoping Calculator	6 GB por 100 Mb/s de tráfico sostenido proporcionan cuatro horas de caché	60 GB por 100 Mb/s de tráfico sostenido proporcionan cuatro horas de caché	3 GB por 100 Mb/s de tráfico sostenido proporcionan cuatro horas de caché

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

Log Decoder			
Persistente Áreas de almacenamiento de datos	Áreas de almacenamiento de datos en caché		
PacketDB	SessionDB	MetaDB	Index
100 % según el cálculo de Sizing & Scoping Calculator	1 GB por 1,000 EPS de tráfico sostenido proporcionan ocho horas de caché	20 GB por 1,000 EPS de tráfico sostenido proporcionan ocho horas de caché	0.5 GB por 1,000 EPS de tráfico sostenido proporciona cuatro horas de caché

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

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

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

Realice estas tareas en el siguiente orden.

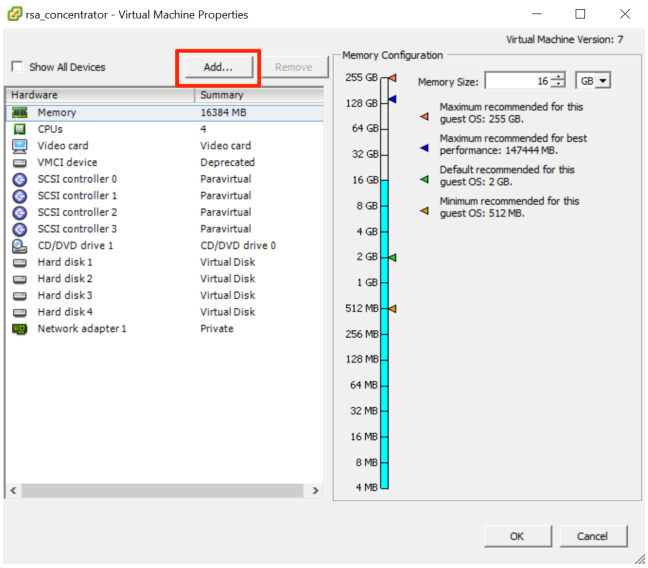
1. Agregar un disco nuevo
2. Crear volúmenes nuevos en el disco nuevo
3. Crear un volumen físico de LVM en la partición nueva
4. Extender el grupo de volúmenes con el volumen físico
5. Expandir el sistema de archivos
6. Iniciar los servicios
7. Asegurarse de que los servicios estén en ejecución
8. Volver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

Agregar un disco nuevo

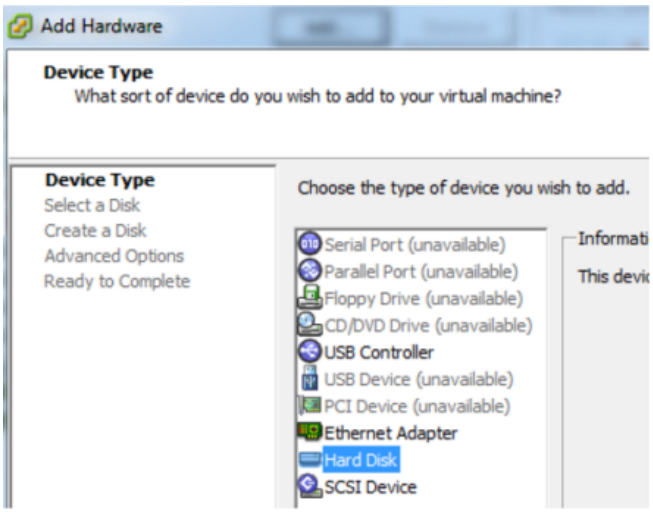
En este procedimiento se muestra cómo agregar un disco de 100 GB nuevo en el mismo almacén de datos.

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

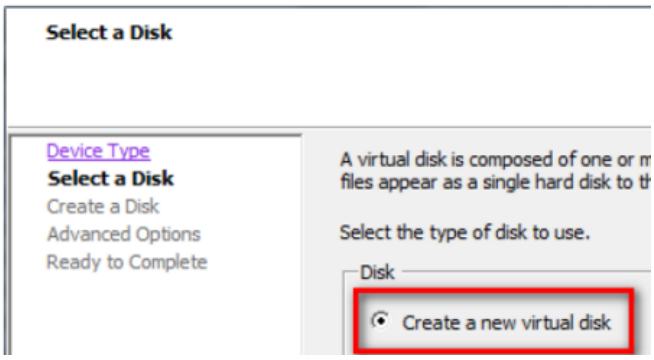
1. Apague la máquina, edite las **Propiedades de máquinas virtuales**, haga clic en la pestaña **Hardware** y, a continuación, en **Agregar**.



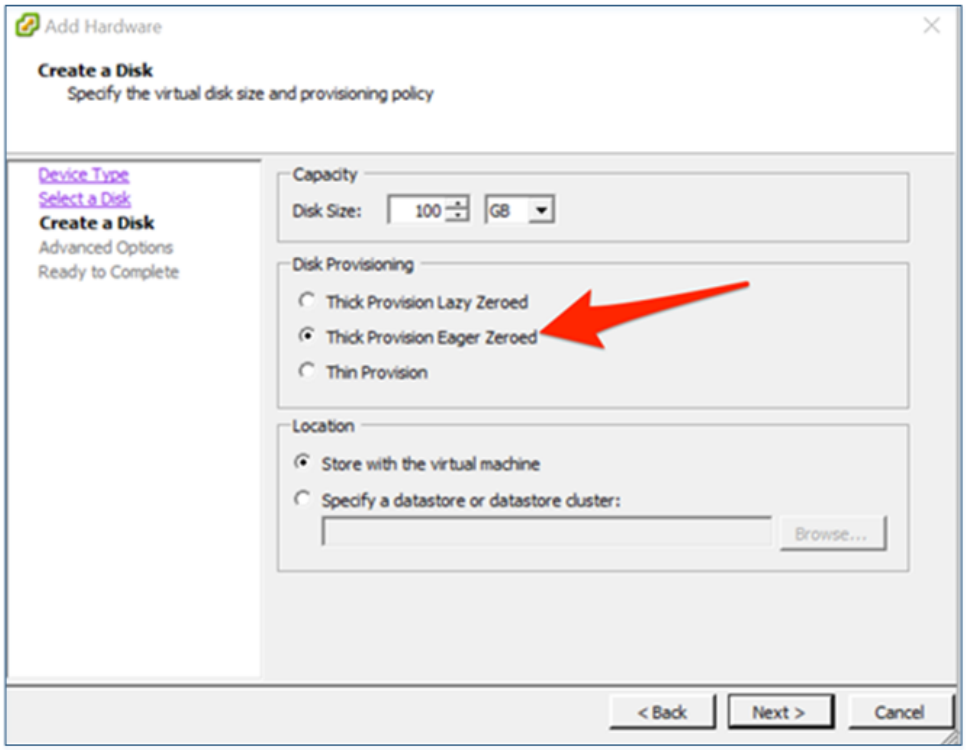
2. Seleccione **Disco duro** como el tipo de dispositivo.



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

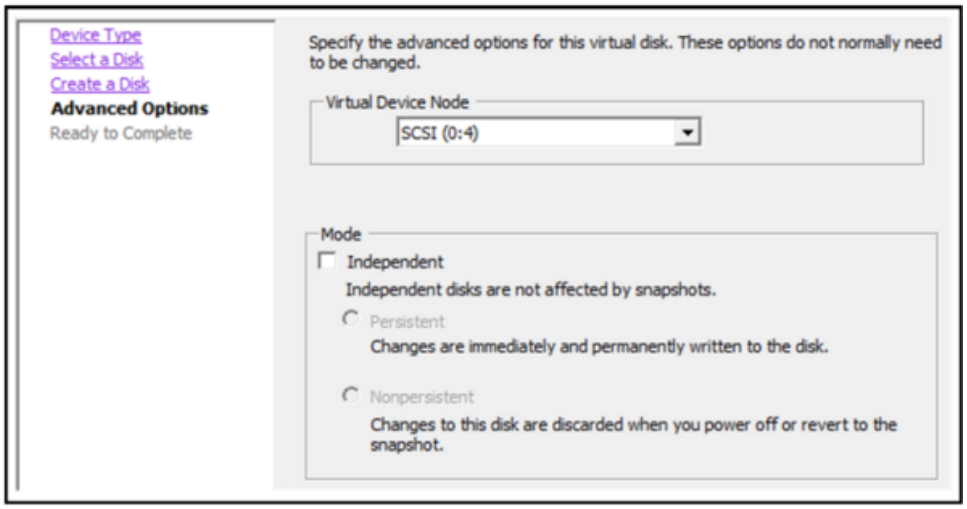


4. Seleccione el tamaño del disco nuevo y dónde desea crearlo (en el mismo almacén de datos o en otro).



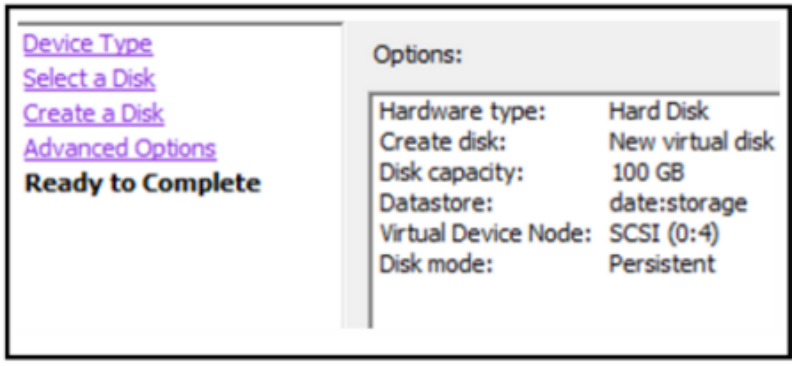
Precaución: Por motivos de rendimiento, asigne todo el espacio.

5. Apruebe el nodo del dispositivo virtual propuesto.



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

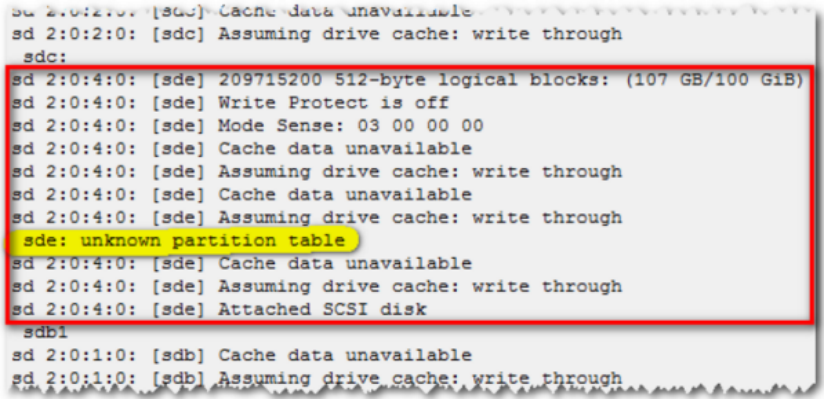
6. Confirme los ajustes.



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

   `dmesg`

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



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

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

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

   Este procedimiento utiliza el Log Decoder como ejemplo.

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

   `stop nwconcentrator`

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

   `stop nwdecoder`

Crear volúmenes en el disco nuevo

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

   ```
   [root@LogDecoderGM ~]# fdisk /f=dev/sde
   ```

   Se muestra la información y el indicador siguientes.

   ```
   Device contains neither a valid DOS partition table, nor Sun, SGI or
   OSF disklabel

   Building a new DOS disklabel with disk identifier 0xae709134.

   Changes will remain in memory only, until you decide to write them.

   After that, of course, the previous content won't be recoverable.

   Warning: invalid flag 0x0000 of partition table 4 will be
   cirrected by w(rite)

   WARNING: DOS-compatible mode is deprecated. It's strongly recommended
   to

      switch off the mode (command 'c') and change display units to

      sectors (command 'u').

   Command (m for help):
   ```

3. Escriba `n`.

   Se muestra el siguiente indicador.

   ```
   Command action

    e  extended(m for help):

    p  primary partition (1-4)
   ```

4. Escriba `p`.

   Se muestra la siguiente información.

   ```
   Disk /dev/sde: 107.4 GB, 107374182400 bytes

   255 heads, 63 sectors/track, 13054 cylinders

   Units = cylinders of 16065 * 512 bytes = 8225280 bytes

   Sector size (logical/physical): 512 bytes / 512 bytes

   I/O size (minimum/optimal): 512 bytes / 512 bytes

   Disk identifier: 0xae709134

    Device Boot  Start  End    Blocks      Id   System

    /dev/sde1     1     13054  104856223+   83  Linux
   ```

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

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

   Se muestra la información y el indicador siguientes.

   ```
   Selected partition 1
   Hex code (type L to list codes):
   ```

6. Escriba `8e`.

   Se muestra la información y el indicador siguientes.

   ```
   Changed system type of partition 1 to 8e (Linux LVM).
   Command (m for help):
   ```

7. Escriba `p`.

   Se muestra la siguiente información.

   ```
   Disk /dev/sde: 107.4 GB, 107374182400 bytes
   255 heads, 63 sectors/track, 13054 cylinders
   Units = cylinders of 16065 * 512 bytes = 8225280 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disk identifier: 0xae709134

    Device Boot  Start    End      Blocks  Id  System

      /dev/sde1      1  13054  104856223+  83  Linux

   Command (m for help):
   ```

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

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

   ```
   The partition table has been altered!
   Calling ioctl() to re-read partition table.
   Syncing disks.
   [root@LogDecoderGM ~]#
   ```

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

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

   - Escriba `dmesg | tail`.

     Se muestra la siguiente información.

```
lo: Disabled Privacy Extensions
 e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow
Control: None
 e1000: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow
Control: None
 eth0: no IPv6 routers present
 eth1: no IPv6 routers present
 coretemp coretemp.0: partition-name is assumed as 100 C!
 coretemp coretemp.1: partition-name is assumed as 100 C!
 sd 2:0:4:0: [sde] Cache data unavailable
 sd 2:0:4:0: [sde] Assuming drive cache: write through sde:
sde1 [root@LogDecoderGM ~]#
```

- Escriba `fdisk /dev/sde`.

  Se muestra la información y el indicador siguientes.

```
WARNING: DOS-compatible mode is deprecated. Tr's strongly
recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').

Command (m for help):
```

- Escriba `p`.

  Se muestra la siguiente información.

```
Disk /dev/sde: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 bytes = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xae709134

 Device Boot  Start    End      Blocks  Id  System

   /dev/sde1      1  13054  104856223+  83  Linux
```

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

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

Se muestra la siguiente información.

```
Physical volume "dev/sdel" successfully created
```

Extender el grupo de volúmenes con el volumen físico

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

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

   Se muestra la siguiente información.

   ```
     PV           VG     Fmt  Attr   PSize    PFree
   /dev/sdb1   VolGroup00 1vm2  a--   32.00g        0
   /dev/sdc1   VolGroup01 1vm2  a--  104.00g        0
   /dev/sdd1   VolGroup01 1vm2  a--  168.00g        0
   /dev/sde1              1vm2  a--  100.00g 100.00g
   ```

   `VolGroup01` consta de los volúmenes físicos (PV) `/dev/sdc1` y `/dev/sdd1` y del sistema LVM. Tenga en cuenta que el volumen `/dev/sde1` nuevo tiene 100 GB de espacio libre.
3. Para agregar el volumen físico a `VolGroup01`.
   a. Ingrese `vgextend VolGroup01 /dev/sde1`.

      Se muestra la siguiente información.

      ```
      Volume group "VolGroup01" successfully extended
      ```

   b. Ingrese pvs.

      Se muestra la siguiente información.

PV	VG	Fmt	Attr	PSize	PFree
/dev/sdb1	VolGroup00	1vm2	a--	32.00g	0
/dev/sdc1	VolGroup01	1vm2	a--	104.00g	0
/dev/sdd1	VolGroup01	1vm2	a--	168.00g	0
/dev/sde1	VolGroup01	1vm2	a--	100.00g	100.00g

      El volumen se agregó a `VolGroup01`, pero aún no se extiende (aún tiene 100 GB de espacio libre). Hay varios volúmenes lógicos en `VolGroup01`; este ejemplo involucra a PacketDB.

4. Para extender el volumen lógico PacketDB de modo que use los 100 GB de espacio libre.

   a. Ingrese `lvs VolGroup01`.
   Se muestra la siguiente información

LV	VG	Attr	LSize	Pool
decoroot	VolGroup01	-wi-ao---	20.00g	
index	VolGroup01	-wi-ao---	10.00g	
logcoll	VolGroup01	-wi-ao---	64.00g	
metadb	VolGroup01	-wi-ao---	44.00g	
packetdb	VolGroup01	-wi-ao---	104.00g	
Sessiondb	VolGroup01	-wi-ao---	30.00g	

   b. Ingrese `lvextend -L+100G /dev/VolGroup01/packetdb`.
   Se muestra la siguiente información.

```
Extending logical volume packetdb to 204.00 GiB
Insufficient free space: 25600 extents needed, but only 25599
available
```

   c. Ingrese `lvextend -L+99G /dev/VolGroup01/packetdb`.
   Se muestra la siguiente información.

```
Extending logical volume packetdb to 203.00 GiB
Logical volume packetdb successfully resized
```

   d. Ingrese `lvs VolGroup01`.
   Se muestra la siguiente información.

```
LV            VG         Attr       LSize  Pool
decoroot   VolGroup01  -wi-ao---    20.00g
index      VolGroup01  -wi-ao---   10.00g
logcoll    VolGroup01  -wi-ao---   64.00g
metadb     VolGroup01  -wi-ao---    44.00g
packetdb   VolGroup01  -wi-ao---   203.00g
Sessiondb  VolGroup01  -wi-ao---    30.00g
```

El volumen lógico `packetdb` se extendió a 203 GB, pero el sistema de archivos `/var/netwitness/logdecoder/packetdb` aún tiene 104 GB.

Expandir el sistema de archivos

1. Acceda al host de Log Decoder mediante el protocolo SSH.
2. Ingrese la siguiente cadena de comandos para crear un volumen físico del Administrador de volúmenes lógicos (LVM) en la partición nueva.
   ```
   [root@LogDecoderGM ~]# xfs_growfs /var/netwitness/logdecoder/packetdb
   ```
   Se muestra la siguiente información.
   ```
   meta-data=/dev/mapper/VolGroup01-packetdb isize=256  agcount=4,
   agsize=6815488 blks

            =           sectsz=512   attr=2, projid32bit=0

   data     =           bsize=4096   blocks=27261952, imaxpct=25

            =           sunit=0      swidth=0 blks

   naming   =version 2  bsize=4096   ascii-ci=0

   log      =internal    bsize=4096  blocks=13311, version=2

            =           sectsz=512   sunit=0blks, lazy-count=1

   lrealtime =none      extsz=4096   blocks=0, rtextents=0
   ```
   data blocks changed from 27261952 to 53214208
3. Ingrese `df -k /var/netwitness/loggdecoder/packetdb`.
   Se muestra la siguiente información.
   ```
   Filesystem   1K-blocks   Used Available Use % Mounted on
   /dev/mapper/VolGroup01-packetdb

     21280358   3641   21276717   1%  /var/netwitness/logdecoder/packetd
     8          6      2              b
   ```

Iniciar los servicios

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

```
[root@LogDecoderGM ~]# start nwlogcollector: start nwlogdecoder
```

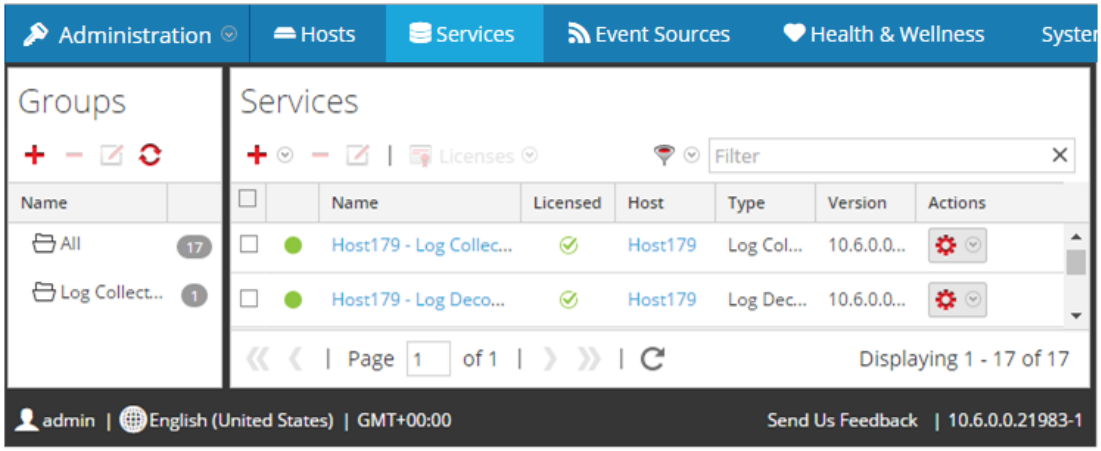
Se muestra la siguiente información.

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

Asegurarse de que los servicios estén en ejecución

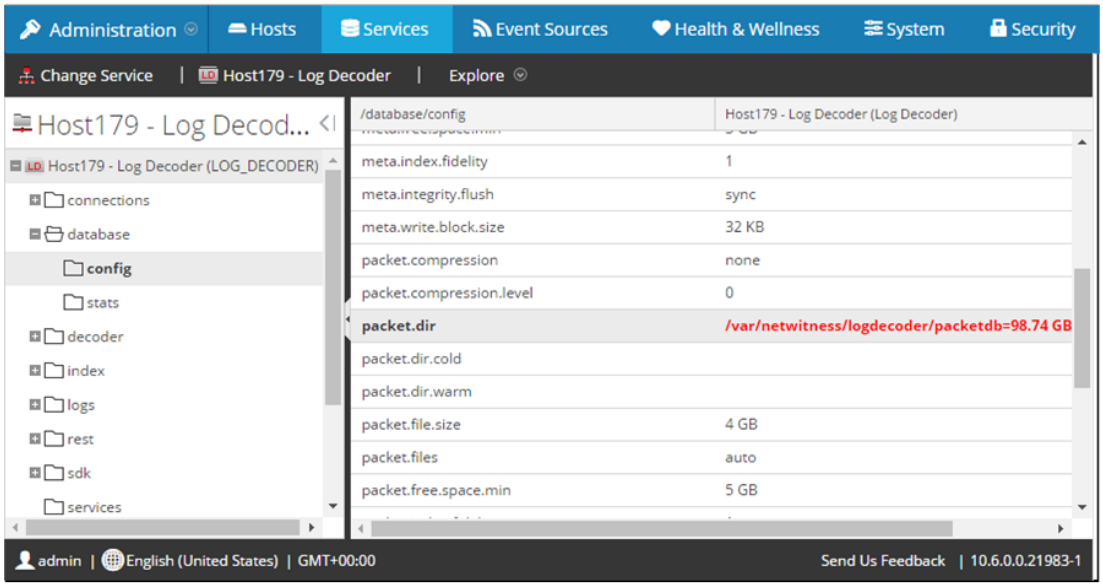
1. Inicie sesión en Security Analytics.
2. Haga clic en **Administration** > **Servicios**.

3. Asegúrese de que los servicios Log Collector y Log Decoder estén en ejecución.



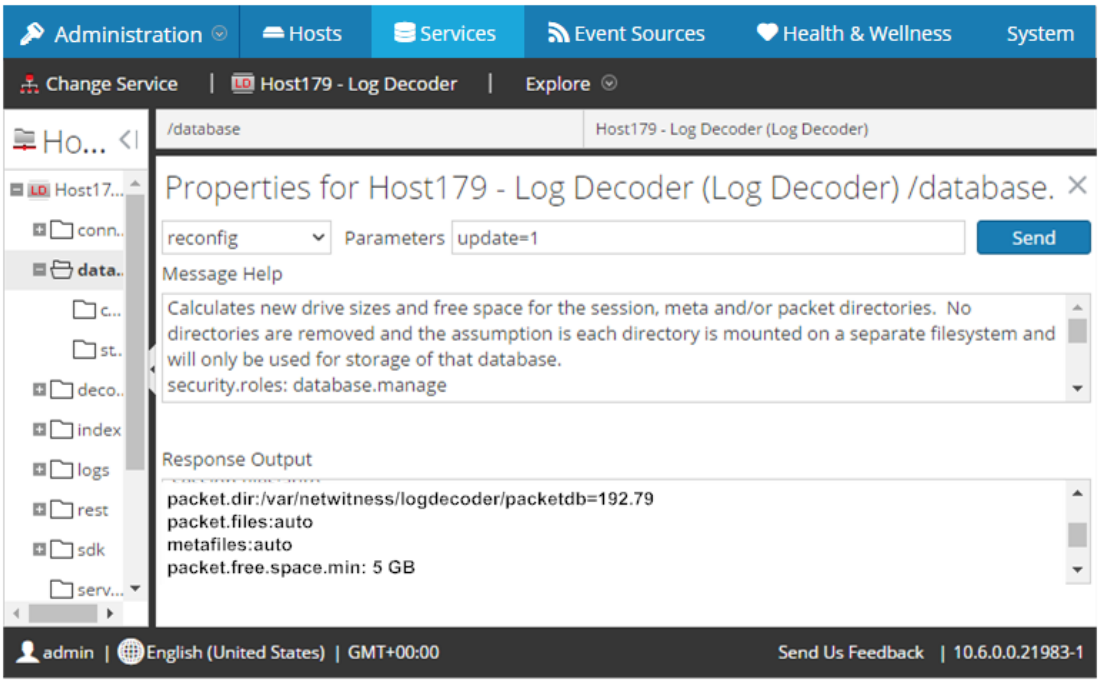
Volver a configurar los parámetros de Log Decoder

1. Inicie sesión en Security Analytics.
2. Haga clic en **Administration** > **Servicios**.
3. Seleccione el servicio Log Decoder.
4. En Acciones, seleccione Explorar.
5. Haga clic en `database > config > packet.dir`.

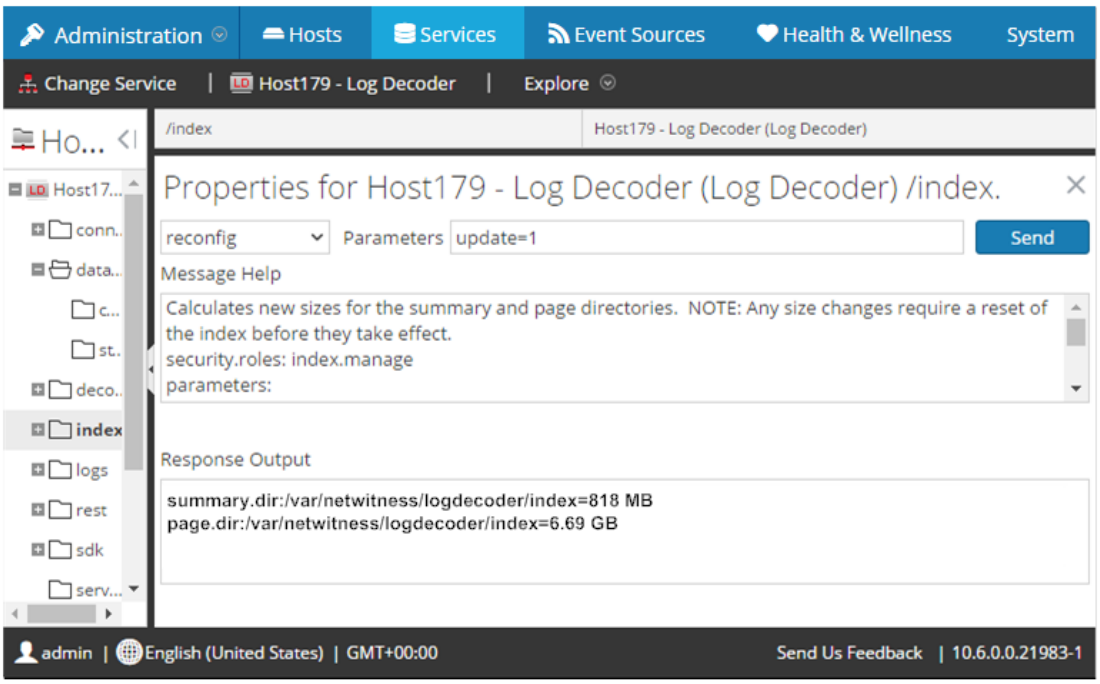


6. Haga clic con el botón secundario en `database`, haga clic en **Propiedades**, seleccione el comando **reconfig**, especifique **update=1** en **Parámetros** y haga clic en **Enviar**.

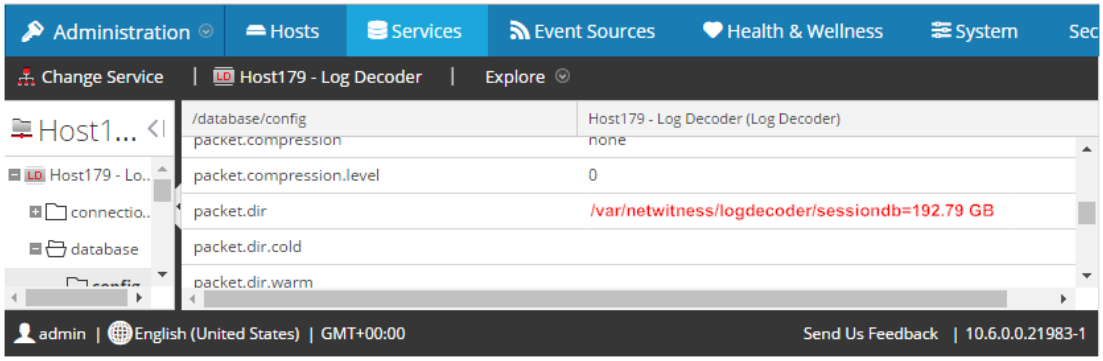
El valor del parámetro `packetdb` cambió de 98.74 GB a 192.79 GB.



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



8. Cierre el cuadro de diálogo Propiedades para volver a la vista Explorar. El valor del parámetro `packet.dir` ahora es 192.79 GB (un 95 % de 203 GB).



Paso 4. Configurar parámetros específicos del host

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

Configurar recopilación de registros en el ambiente virtual

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

Configurar una captura de paquetes en el ambiente virtual

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

Configurar un vSwitch en modo promiscuo

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

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

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

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

Uso de un Tap virtual de otros fabricantes

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

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

- Se requiere un host externo para terminar el túnel y el host externo dirige el tráfico a la interfaz de Decoder.
- El túnel envía el tráfico directamente a la interfaz de Decoder, donde Security Analytics maneja su desencapsulado.