

RSA Security Analytics

Guía de instalación de hosts virtuales para la versión 10.6





Copyright © 2016 EMC Corporation. Todos los derechos reservados.

Marcas comerciales

RSA, el logotipo de RSA y EMC son marcas registradas o marcas comerciales de EMC Corporation en los Estados Unidos y en otros países. Todas las demás marcas comerciales utilizadas en este documento pertenecen a sus respectivos propietarios. Para obtener una lista de las marcas comerciales de EMC, visite mexico.emc.com/legal/emc-corporation-trademarks.htm (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 del acuerdo de licencia que se aplica al software de otros fabricantes en este producto puede encontrarse en el archivo thirdpartylicenses.pdf.

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

El uso, la copia y la distribución de cualquier software de EMC descrito en esta publicación requieren una licencia de software correspondiente. 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.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA "TAL CUAL". EMC CORPORATION NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Contenido

Guía de instalación de hosts virtuales	5
Implementación virtual básica	6
Abreviaturas que se utilizan en la Guía de implementación virtual	6
Hosts virtuales compatibles	7
Medios de instalación	8
Recomendaciones para ambientes virtuales	8
Requisitos del sistema recomendados para un host virtual	9
Log Decoder	9
Packet Decoder	10
Concentrator para el flujo de registros	10
Concentrator para el flujo de paquetes	10
Warehouse Connector para el flujo de registros	11
Warehouse Connector para el flujo de paquetes	11
Archiver para el flujo de registros	11
Event Stream Analysis (ESA) con Context Hub	12
Servidor de Security Analytics (NW)	12
Broker	12
Log Collector (local y remoto)	12
Reglas de dimensionamiento de los recopiladores de Windows heredado	13
Instalar el host virtual de Security Analytics en un ambiente virtual .	14
Requisitos previos	14
Paso 1. Implementar el host virtual	14
Requisitos previos	14
Procedimiento	15
Paso 2. Configurar la red	17
Paso 3. Configurar las bases de datos para adaptarse a Security Analytics	17
Tarea 1. Revisar la configuración inicial del almacén de datos	17
Espacio inicial asignado a PacketDB	17
Tamaño inicial de la base de datos	18

Punto de montaje de PacketDB	18
Tarea 2. Revisar la configuración óptima del espacio del almacén de datos	19
Tasas de espacio de unidad virtual	20
Tarea 3. Agregar un volumen nuevo y extender los sistemas de archivos existentes	
Paso 4. Configurar parámetros específicos del host	
Configurar recopilación de registros en el ambiente virtual	34
Configurar una captura de paquetes en el ambiente virtual	
Uso de un Tap virtual de otros fabricantes	35

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 o	ue se	utilizan	en la	Guía de	implem	entación	virtual

Abreviaturas	Descripción
СРИ	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 sig- nifica 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 dis- cos 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
10,00- 0	8	30 GB	16	50 GB	300	50
15,00 0	12	40 GB	20	60 GB	550	100

Mb/s	vCPU de labo- ratorio	vRAM de labo- ratorio	vCPU de pro- ducción	vRAM de pro- ducción	Lec- tura IOPS	Escri- tura 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

Packet Decoder

Concentrator para el flujo de registros

EPS	vCPU de labo- ratorio	vRAM de labo- ratorio	vCPU de pro- ducción	vRAM de pro- ducción	Lec- tura IOPS	Escri- tura IOPS
10,00- 0	4	30 GB	10	50 GB	1,600	6,500
15,00 0	6	40 GB	12	60 GB	1,600	7,600

Concentrator para el flujo de paquetes

Mb/s	vCPU de labo- ratorio	vRAM de labo- ratorio	vCPU de pro- ducción	vRAM de pro- ducción	Lec- tura IOPS	Escri- tura 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

EPS	vCPU de labo- ratorio	vRAM de labo- ratorio	vCPU de pro- ducción	vRAM de pro- ducción	Lec- tura IOPS	Escri- tura IOPS
10,00- 0	6	20 GB	8	30 GB	50	50
15,00 0	6	30 GB	10	35 GB	50	50

Warehouse Connector para el flujo de registros

Warehouse Connector para el flujo de paquetes

Mb/s	vCPU de labo- ratorio	vRAM de labo- ratorio	vCPU de pro- ducción	vRAM de pro- ducción	Lec- tura IOPS	Escri- tura 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 labo- ratorio	vRAM de labo- ratorio	vCPU de pro- ducción	vRAM de pro- ducción	Lec- tura IOPS	Escri- tura IOPS
10,00- 0	8	10 GB	12	40 GB	1,300	700
15,00 0	12	20 GB	14	45 GB	1,200	900

EPS	vCPU de	vRAM de	vCPU de	vRAM de	Lec-	Escri-
	labo-	labo-	pro-	pro-	tura	tura
	ratorio	ratorio	ducción	ducción	IOPS	IOPS
90,00- 0	12	50 GB	32	94 GB	50	50

Event Stream Analysis (ESA) con Context Hub

Servidor de Security Analytics (NW)

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

Broker

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

Log Collector (local y remoto)

EPS	vCPU de labo- ratorio	vRAM de labo- ratorio	vCPU de pro- ducción	vRAM de pro- ducción	Lec- tura IOPS	Escri- tura IOPS
15,00- 0	8	8 GB	8	8 GB	50	50
30,00- 0	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.



 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.

Where do you want to sto	re the v	irtual machine fil	25?					
Source OVE Template Details	Selec	t a destination st	orage for the virtua	I machine files:				
End User License Agreement	Nar	ne	Drive Type	Capacity	Provisioned	Free	Туре	Thin Pr
Name and Location	8	datastore1	Non-SSD	144.00 GB	3.74 GB	140.26 GB	VMFS5	Suppo
Storage		datastore2	Non-SSD	18.18 TB	15.87 TB	7.84 TB	VMFS5	Suppo
Disk Format								
Network Mapping								
Ready to Complete								

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.

Network Mapping		
What networks should	the deploye	d template use?

me and Location	Source Networks	DestinationNetworks	
orage	Network 1	VM Network	
twork Mapping ady to Complete		Localization-VMNetwork VM Network Traffic Gen	
	•	III	

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.

Deploying SA_V10_Server	
Deploying SA_V10_Server	
Creating VM SA_V10_Server	
0	
Close this dialog when completed	Cancel

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.

deviceappliance	packet.dir	/var/netwitness/logdecoder/packetdb=98.74DB
	packet.compression.level	0
	packet.compression	none
	meta.write.block.size	64 KB
Storedproc	meta.integrity.flush	sync
services	meta.index.fidelity	1
III C I sdk	meta.free.space.min	267 MB
	meta.files	50
 ⊡ [^] logs	meta.file.size	3 GB
🗉 🗋 index	meta.dir.warm	
🖾 🗋 decoder	meta.dir.cold	
stats	meta.dir	/var/netwitness/logdecoder/metadb=28.48 GB
C config	meta.compression.level	0
🗏 📇 database	meta.compression	none
Connections	manifest.dir	

NWAPPLIANCE2956-LC-LD - Log Decoder (... hash.dir

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
```

 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 alma- cenamiento de datos	Alm	acén de da	itos de c	aché
PacketDB	SessionDB	MetaDB		Index
100 % según el cál- culo de Sizing & Sco- ping Calculator	6 GB por 100 Mb/s de tráfico sostenido pro- porcionan cuatro horas de caché	60 GB por 10 de tráfico sos proporcionan horas de cach	00 Mb/s stenido cuatro né	3 GB por 100 Mb/s de tráfico sostenido proporcionan cuatro horas de caché
Concentrator				
Persistente Áreas de alma- cenamiento de datos	Áreas de aln	nacenamier	nto de da	atos en caché
MetaDB	SessionDB Index		Index	
Se calcula como el 10 % de la PacketDB requerida para una tasa de retención de 1:1	Index 30 GB por 1 TB de PacketDB para implementaciones de red mul- tiprotocolo estándar como se ven en gateways de Internet típicas.		5 % de la MetaDB calculada en Concentrator. Disco SSD o eje de alta velocidad recomendado para acceso rápido	

Áreas de alm	nacenamiento de d	atos en caché			
SessionDB	MetaDB	Index			
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 pro- porciona cuatro horas de caché			
Log Concentrator					
Áreas de alm	nacenamiento de d	atos en caché			
SessionDB	Index				
Index					
3 GB por 1,000 EPS de tráfico sostenido por día de retención	5 % de la MetaDB ca Disco SSD o ejes de mendados para acces	ilculada en Concentrator. alta velocidad reco- o rápido			
	Áreas de alm SessionDB 1 GB por 1,000 EPS de tráfico sostenido proporcionan ocho horas de caché Áreas de alm SessionDB Index 3 GB por 1,000 EPS de tráfico sostenido por día de retención	Áreas de almacenamiento de dSessionDBMetaDB1 GB por 1,000 EPS20 GB por 1,000 EPSde tráfico sostenidode tráfico sostenidoproporcionan ochoproporcionan ochohoras de cachéhoras de cachéÁreas de almacenamiento de dSessionDBIndexIndex3 GB por 1,000 EPS de5 % de la MetaDB catráfico sostenido porDisco SSD o ejes dedía de retenciónmendados para acces			

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**.

Show Al Devices Add Remove Show Al Devices Add Remove ardware Summay Memory 16384 MB CPUs 4 Video card Video card Video card Deprecated SCSI controller 0 Paravirtual SCSI controller 1 Paravirtual SCSI controller 2 Paravirtual SCSI controller 3 Paravirtual SCSI controller 4 Virtual Disk Hard disk 1 Virtual Disk Hard disk 2 Virtual Disk Hard disk 4 Virtual Disk Network adapter 1 Private	rsa_concentrator - Virtua	I Machine Properties		- L ×
Show Al Devices Add Remove ardware Summary Memory 15384 MB CPUs 4 Video card Video card Video card Deprecated SCSI controller 0 Paravirtual SCSI controller 1 Paravirtual SCSI controller 2 Paravirtual SCSI controller 3 Paravirtual SCSI controller 4 Vidual Disk Hard disk 1 Virtual Disk Hard disk 2 Virtual Disk Hard disk 4 Virtual Disk Network adapter 1 Private			- Memory Confi	Virtual Machine Version: 7 guration
iardware Summary Memory 15384 MB CPUs 4 Video card Video card VMCI device Deprecated SCSI controller 0 Paravirtual SCSI controller 1 Paravirtual SCSI controller 2 Paravirtual SCSI controller 3 Paravirtual SCSI controller 4 Vidual Disk Hard disk 1 Virtual Disk Hard disk 4 Virtual Disk Network adapter 1 Private 26 MB 16 MB 32 MB 16 MB	Show All Devices	Add Remove	255 GB	Memory Size: 16 - GB -
Network adapter 1 Private 256 MB - 128 MB - 64 MB - 32 MB - 16 MB - 8 MB - 8 MB - 4 MB -	Hardware Memory CPUs VMCI device SCSI controller 0 SCSI controller 2 SCSI controller 3 COJVD drive 1 Hard disk 1 Hard disk 2 Hard disk 4	Summary 16384 MB 4 Video card Deprecated Paravirtual Paravirtual Paravirtual CD/DVD drive 0 Virtual Disk Virtual Disk Virtual Disk	128 GB - G4 GB - 32 GB - 16 GB - 4 GB - 2 GB - 1 GB - 1 GB - 512 MB -	Maximum recommended for this guest OS: 255 GB. Maximum recommended for best performance: 147444 MB. Default recommended for this guest OS: 26 B. Minimum recommended for this guest OS: 512 MB.
	Network adapter 1	Private	256 MB - 128 MB - 64 MB - 32 MB - 16 MB - 8 MB - 4 MB -	

2. Seleccione Disco duro como el tipo de dispositivo.

Device Type What sort of device do	you wish to add to your virtual machine?
Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	Choose the type of device you wish to add Serial Port (unavailable) Parallel Port (unavailable) Floppy Drive (unavailable) CD/DVD Drive (unavailable) USB Controller USB Device (unavailable) PCI Device (unavailable) Ethernet Adapter Hard Diss

3. Seleccione Crear un nuevo disco virtual.

Select a Disk	
Device Type	
Select a Disk	A virtual disk is composed of one or m files appear as a single hard disk to th
Advanced Options Ready to Complete	Select the type of disk to use.
	Create a new virtual disk

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

Device Type Select a Disk	Capacity Disk Size: 100 + G8 V
Advanced Options	Disk Provisioning
ceacy to Complete	C Thick Provision Lazy Zeroed
	Thick Provision Eager Zeroed
	C Thin Provision
	Location
	Store with the virtual machine
	C Specify a datastore or datastore duster:
	Browse

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

5. Apruebe el nodo del dispositivo virtual propuesto.

Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	Specify the advanced options for this virtual disk. These options do not normally need to be changed. Virtual Device Node SCSI (0:4)
	Mode Independent Independent disks are not affected by snapshots. C Persistent Changes are immediately and permanently written to the disk.
	C Nonpersistent Changes to this disk are discarded when you power off or revert to the snapshot.

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

6. Confirme los ajustes.

Device Type Select a Disk	Options:	
Create a Disk Advanced Options Ready to Complete	Hardware type: Create disk: Disk capacity: Datastore: Virtual Device Node: Disk mode:	Hard Disk New virtual disk 100 GB date:storage SCSI (0:4) Persistent

- 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.

34	2.012.0	· [360]	Caone data unavairusle
sd	2:0:2:0	: [sdc]	Assuming drive cache: write through
30	ic:		
sd	2:0:4:0	: [sde]	209715200 512-byte logical blocks: (107 GB/100 GiB)
sd	2:0:4:0	: [sde]	Write Protect is off
sd	2:0:4:0	: [sde]	Mode Sense: 03 00 00 00
sd	2:0:4:0	: [sde]	Cache data unavailable
sd	2:0:4:0	: [sde]	Assuming drive cache: write through
sd	2:0:4:0	: [sde]	Cache data unavailable
sd	2:0:4:0	: [sde]	Assuming drive cache: write through
30	ie: unkn	lown part	tition table)
зd	2:0:4:0	: [sde]	Cache data unavailable
sd	2:0:4:0	: [sde]	Assuming drive cache: write through
sd	2:0:4:0	: [sde]	Attached SCSI disk
30	ib1		
sd	2:0:1:0	: [sdb]	Cache data unavailable
şġ,	2:0:1:0	: [sdb]	Assuming drive cache: write through

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
```

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

Blocks

Id

System

Device Boot Start End

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

En el indicador Command m for help:, escribat.
 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	lvm2	a	104.00g	0
/dev/sdd1	VolGroup01	lvm2	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.
- 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.

Administration		s 😑 Services	S Ev	vent Sourc	es 🔍	Health & W	/ellness	Syste
Groups	Services	S						
+ - 🛛 O	+ 🛛 – 1	🗹 📔 🛐 Licenses	\odot	♥ ⊙	Filter			×
Name	□ Na	ame	Licensed	Host	Туре	Version	Actions	
🗄 All 🛛 🚺	🗆 🔴 Но	ost179 - Log Collec	ø	Host179	Log Col	10.6.0.0	✿ ⊙	-
🗄 Log Collect 🕚	🗆 🌒 Но	ost179 - Log Deco	\bigotimes	Host179	Log Dec	10.6.0.0	♦ ⊙	-
	« (1	Page 1 of 1	$\rangle \rangle \rangle$	C		Displa	aying 1 - 17	of 17

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.

🔎 Administration 🛛	🖴 Hosts	Services	Event Sources	Health & Wellness	😂 System	🖥 Security			
🚠 Change Service 🔟 Host179 - Log Decoder Explore 🐵									
≡Host179 - Log	Decod ·	/database/cor	fig	Host179 - Log De	coder (Log Decoder)				
🖬 ഥ Host179 - Log Decoder (L	LOG_DECODER)	 meta.index.f 	idelity	1	1				
connections		meta.integri	ty.flush	sync					
🗏 🗁 database		meta.write.b	lock.size	32 KB	32 KB				
C config		packet.comp	packet.compression		none				
stats		packet.comp	pression.level	0					
decoder		packet.dir	packet.dir /		/var/netwitness/logdecoder/packetdb=98.74 GB				
II 🗋 index		packet.dir.co	old						
		packet.dir.w	arm						
		packet.file.si	packet.file.size		4 GB				
		packet.files	packet.files		auto				
		packet.free.s	pace.min	5 GB					
services	•	•	• • • •						
2 admin English (United States) GMT+00:00 Send Us Feedback 10.6.0.0.21983-1									

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**.

🔎 Administr	ation 🗟 🧯	Hosts	Services	Svent Sources	🗢 Health & Wellness	System			
🚓 Change Service 🛛 🧰 Host179 - Log Decoder 🔰 Explore 💿									
⊫Ho <i< th=""><th colspan="8">/database Host179 - Log Decoder (Log Decoder)</th></i<>	/database Host179 - Log Decoder (Log Decoder)								
🖬 💵 Host17 ^	Properties for Host179 - Log Decoder (Log Decoder) /database. ×								
Conn	reconfig Parameters update=1 Send								
🗏 🕀 data.	Message Help								
□ c □ st. □ deco	Calculates new drive sizes and free space for the session, meta and/or packet directories. No directories are removed and the assumption is each directory is mounted on a separate filesystem and will only be used for storage of that database. security.roles: database.manage								
I _ index	Response O	utput							
Crest	packet.dir:/var/netwitness/logdecoder/packetdb=192.79 packet.files:auto metafiles:auto								
Serv ▼	packet.free.	.space.min:	5 GB			•			
Ladmin Indexes GMT+00:00 Send Us Feedback 10.6.0.0.21983-1									

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**.

🔎 Administr	ration 💿 🗕 Hosts 😂 Services 🔊 Event Sources 🗢 Health & Wellness System								
🕂 Change Serv	rice 🔟 Host179 - Log Decoder Explore 🐵								
≡Ho <i< th=""><th colspan="8">/index Host179 - Log Decoder (Log Decoder)</th></i<>	/index Host179 - Log Decoder (Log Decoder)								
🖬 💶 Host17 ^	Properties for Host179 - Log Decoder (Log Decoder) /index. 🛛 🗡								
Conn	reconfig Parameters update=1 Send								
🗏 🔂 data	Message Help								
□ c □ st. □ deco	Calculates new sizes for the summary and page directories. NOTE: Any size changes require a reset of the index before they take effect. security.roles: index.manage parameters:								
🗆 🗋 index									
🖬 🗋 logs 📕	Response Output summary.dir:/var/netwitness/logdecoder/index=818 MB page.dir:/var/netwitness/logdecoder/index=6.69 GB								
🖬 🗋 rest									
🖬 🗋 sdk									
Serv ▼		_							
Ladmin Brglish (United States) GMT+00:00 Send Us Feedback 10.6.0.0.21983-1									

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).

🔎 Administration 😔		🖴 Hosts	Services	ervices 🔊 Event S		Health & Wellness	🞏 System	Sec
🚠 Change Service		🗕 Host179 - Log	g Decoder 🛛 🗍	Explore 💿				
⊫Host1 <	/data раск	abase/config (et.compression			Host179 - Log none	g Decoder (Log Decoder)		
🖬 💷 Host179 - Lo 📤	packet.compression.level				0			
🗈 🗋 connectio	packet.dir				/var/netwitness/logdecoder/sessiondb=192.79 GB			
🗖 🔂 database	pack	ket.dir.cold						
< □ config ↓ ↓	oack	ket.dir.warm						+
admin Itref English (United States) GMT+00:00 Send Us Feedback							dback 10.6.0.0.2	1983-1

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.