

# RSA® Security Analytics

## Security Analytics 10.6

### Guía de instalación de Decoder 10G

---

#### Contenido

<b>Introducción</b>	<b>2</b>
<b>Instalación de Decoder 10G</b>	<b>3</b>
REQUISITOS PREVIOS	3
INSTRUCCIONES DE INSTALACIÓN DEL BIOS	3
ACTUALIZAR DECODER 10G	3
INSTALAR DECODER 10G	4
<b>Configurar Decoder 10G</b>	<b>5</b>
<b>Consideraciones de almacenamiento</b>	<b>8</b>
USO DEL HARDWARE SERIE 4S (CON DOS O MÁS UNIDADES DE DAC)	8
USO DEL ALMACENAMIENTO SAN	8
<b>Consideración de análisis y contenido para la captura de paquetes</b>	<b>9</b>
<b>Agregación de un Decoder 10G a otros componentes de SA</b>	<b>10</b>

## Introducción

RSA Security Analytics versión 10.6 ofrece compatibilidad con la recopilación de alta velocidad de Decoder. Puede capturar datos de paquetes de redes de mayor velocidad y optimizar su Packet Decoder para capturar tráfico de red con picos de hasta 8 Gb/s continuos y 10 Gb/s, según los analizadores y los feeds que haya activado.

**Nota:** Puede dirigirse a “Configuración de Decoder 10G” si está comenzando con el nuevo hardware serie 5.

Las mejoras incorporadas para facilitar la captura en estos ambientes incluyen las siguientes:

- Utilización de la funcionalidad del controlador de **captura pf\_ring** para aprovechar la tarjeta NIC Intel 10G genérica con el fin de lograr una captura de alta velocidad.
- Introducción de la configuración de **assembler.parse.valve**. La configuración desactiva automáticamente los analizadores de aplicación cuando se superan determinados umbrales con el fin de limitar el riesgo de pérdida de paquetes. Una vez que estos analizadores se desactivan, los analizadores de la capa de red permanecen activos. Cuando las estadísticas bajan de los umbrales superados, los analizadores de aplicaciones se vuelven a activar automáticamente.
- Introducción de la configuración de **parallel.values** en Concentrator para optimizaciones de consultas.

## Instalación de Decoder 10G

Realice los siguientes pasos para instalar Decoder 10G de Security Analytics 10.6:

### Requisitos previos

- Plataformas SA-S4H-P-DEC o SMC-S4H-P-DEC basadas en la plataforma Dell R620
- NIC SMC-10GE-\* Intel 520 10G instalada (disponible en RSA)
- Packet Decoders actualizados a 10.6
- Cada Packet Decoder configurado como mínimo con dos DAC o conectividad SAN.  
**NOTA:** Consulte “Consideraciones de almacenamiento” en este documento antes de realizar la actualización, ya que puede ser necesario un recableado físico.
- Dell R620 BIOS v1.2.6 o superior. Se recomienda que los clientes actualicen al BIOS v2.2.3 más reciente, pero no es requisito para 10G si ejecutan v1.2.6 o superior.  
**NOTA:** Las revisiones de BIOS anteriores a v1.2.6 tienen problemas para identificar correctamente la ubicación de la tarjeta de captura 10G dentro del sistema. Es importante actualizar el BIOS antes de instalar paquetes, ya que estos usan información que proporciona el BIOS para inicializar el sistema.

### Instrucciones de instalación del BIOS

1. Descargue BIOS v2.2.3 en la siguiente ubicación:  
<http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=V7P04>
2. Descargue el archivo **Update Package for Red Hat Linux**.
3. Copie el archivo en el servidor de Security Analytics.
4. Inicie sesión como **raíz**.
5. Cambie los permisos en el archivo a ejecutar.
6. Ejecute el siguiente archivo:  
**./BIOS\_V7P04\_LN\_2.2.3.BIN**
7. Cuando la operación finalice, el sistema solicitará un reinicio.  
**NOTA:** El procedimiento de instalación del BIOS tarda aproximadamente 10 minutos.

### Actualizar Decoder 10G

1. Actualice el dispositivo Decoder a la versión 10.6, incluidos todos los parches del SO. **La versión mínima del parche de seguridad aplicado es RSA Security Analytics versión 10.6.** Esta versión requiere el paquete de kernel de Linux:  
  
`kernel-2.6.32-573.12.1.el6.x86_64`, que corresponde a la versión del kernel de RSA Security Analytics versión 10.6.
2. Asegúrese de que las versiones del kernel, pfring y numactl sean las siguientes:
  - `kernel-2.6.32-573.12.1.el6.x86_64`
  - `pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm`
  - `numactl-2.0.9-2.el6.x86_64.rpm`

## Instalar Decoder 10G

1. Descargue la versión más reciente del paquete **pfring** rpm desde **smcupdate**

```
pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm
```

Para obtener más información, consulte RSA SecurCare: <https://knowledge.rsasecurity.com>.

2. Mediante el protocolo SSH, instale los paquetes con el siguiente comando cuando los archivos se hayan copiado con scp en Decoder:

```
rpm -ivh pfring*
```

**NOTA:** Asegúrese de realizar las siguientes comprobaciones:

- a. Compruebe el **rpm el6** mediante el siguiente comando:

```
rpm -qa |grep numactl*
```

- b. Compruebe para asegurarse de que la versión sea numactl-2.0.9-2.el6 .x86\_64.rpm

**NOTA:** Si el paso de actualización anterior se realiza antes de la actualización del BIOS, es necesario realizar los siguientes pasos:

- Desinstale los paquetes mediante el comando `rpm -e`.
- Actualice el BIOS a v2.2.3
- Ejecute comandos **rpm** para volver a instalar los paquetes necesarios.

3. Asegúrese de que las versiones del kernel, pfring y numactl sean las siguientes:

- kernel- 2.6.32-573.12.1.el6.x86\_64
- pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86\_64.rpm
- numactl-2.0.9-2.el6 .x86\_64.rpm

4. Reinicie el dispositivo Decoder (se requiere un reinicio completo del sistema para asegurarse de que los controladores `pf_ring` se carguen correctamente).

5. Cuando Decoder se reinicia, puede verificar que la instalación se haya realizado correctamente si ve interfaces **PFRINGZC** adicionales disponibles en las opciones de "Interfaz de captura seleccionada" (se muestra a continuación).

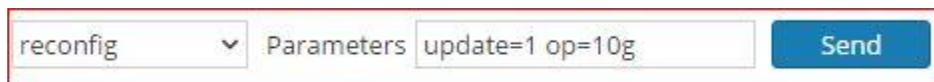
Decoder Configuration	
Name	Config Value
<b>Adapter</b>	
Berkley Packet Filter	
<b>Capture Interface Selected</b>	<b>PFRINGZC,p1p2</b>

## Configurar Decoder 10G

Después de la actualización, realice los siguientes pasos para configurar Decoder 10G:

1. En la vista Explorador de Decoder, haga clic con el botón secundario en **Decoder** y seleccione **Propiedades**.
2. En el menú desplegable Propiedades, seleccione **reconfig** e ingrese los siguientes parámetros:  
`update=1 op=10g`
3. En la vista Explorador de Decoder, haga clic con el botón secundario en **database** y seleccione **Propiedades**.
4. En el menú desplegable Propiedades, seleccione **reconfig** e ingrese los siguientes parámetros que se muestran en la siguiente captura de pantalla:

`update=1 op=10g`



The screenshot shows a configuration interface with a dropdown menu set to 'reconfig', a text input field containing 'Parameters update=1 op=10g', and a blue 'Send' button.

5. Seleccione el adaptador de puertos de captura. Las opciones incluyen:
  - a. Captura de un único puerto: **PFRINGZC,p1p1** o **PFRINGZC,p1p2**
  - b. Captura de ambos puertos:
    - i. Seleccione **PFRINGZC,P1P1**
    - ii. En la vista Explorador, configure **capture.device.params = device=zc:p1p2,zc:p1p1**
  - c. Asegúrese de que el hardware de captura seleccionado esté en el nodo NUMA correcto. Desde una sesión del protocolo SSH al dispositivo, ejecute la siguiente declaración:

```
cat /sys/class/net/<interface_name>/device/numa_node
```

donde **<interface\_name>** es la interfaz de captura seleccionada (por ejemplo, **p1p1**).

Si el resultado es **0** (cero), no se requiere ninguna configuración adicional.

Si no es así, agregue el resultado como el parámetro **core** a los parámetros de captura, como se muestra a continuación:

```
/decoder/config/capture.device.params: core=1
```

Este cambio requiere el reinicio del servicio.

**NOTA:** Según la configuración de hardware, los puertos de captura se pueden identificar con un nombre distinto de **p1p1/p1p2**, pero siempre tendrán el prefijo **PFRINGZC**. Por ejemplo, en algunos dispositivos, estos puertos se pueden identificar como **eth4 / eth5**. Para capturar desde **eth4**, seleccione **PFRINGZC,eth4**. Para capturar desde **eth5**, seleccione **PFRINGZC,eth5**.

6. Si el hilo de ejecución de escritura tiene problemas para mantener la velocidad de la captura, puede intentar lo siguiente:

Cambie **/database/config/packet.integrity.flush** a normal.

**NOTA:** Puede intentar ajustar **packet.file.size** a un valor mayor, pero debe mantener el tamaño del archivo en menos de 10 GB, ya que el archivo completo se coloca en el buffer en la memoria a estas velocidades.

7. (Opcional) El análisis de aplicaciones consume mucho CPU y puede hacer que Decoder pierda paquetes. Para moderar las pérdidas inducidas por el análisis de aplicaciones, el ajuste **/decoder/config/assembler.parse.valve** se puede configurar en **true**. Esto dará lugar a lo siguiente:
  - Cuando el análisis de sesiones se transforme en un cuello de botella, los analizadores de aplicación (HTTP, SMTP, FTP, etc.) se inhabilitarán temporalmente.
  - Las sesiones no se pierden cuando se inhabilitan los analizadores de aplicación, solo la fidelidad del análisis ejecutado en ellas.
  - Las sesiones analizadas con los analizadores de aplicación desactivados tendrán metadatos de red asociados (analizador de RED).
  - La estadística **/decoder/parsers/stats/blowoff.count** muestra el conteo de todas las sesiones que no se sometieron a los analizadores de aplicaciones (el análisis de red se ejecuta de todos modos).
  - Cuando el análisis de sesiones deja de ser un posible cuello de botella, los analizadores de aplicación se reactivan automáticamente.
  
8. El pool de sesiones del ensamblador debe ser lo suficientemente grande de modo que las sesiones no se fuercen.
  - Se puede determinar si las sesiones se están forzando con la estadística **/decoder/stats/assembler.sessions.forced** (que irá en aumento) y **/decoder/stats/assembler.sessions**, que estará dentro de varios cientos de **/decoder/config/assembler.session.pool**.
  - El sitio de pruebas de RSA Security usó la siguiente configuración a un poco menos de 10G: **/decoder/config/assembler.session.pool** se configuró en 1,000,000 y **/decoder/stats/assembler.sessions** promediara 630,000.

Se puede usar un método alternativo a los pasos del 1 al 4 enumerados anteriormente para configurar Decoder 10G mediante la ejecución de los pasos 1, 2, 3 y 4 que se explican a continuación. Si se usa este método, los pasos del 5 al 8 enumerados anteriormente son obligatorios.

1. Actualice la configuración de pools de sesiones y paquetes a los siguientes valores (bajo **/decoder/config**):
  - a. **pool.packet.pages** = 1000000
  - b. **pool.session.pages** = 300000
2. Actualice el tamaño del bloque de escritura de paquetes al siguiente valor (bajo **/database/config**):
  - a. **Packet.write.block.size** = filesize  
**Nota:** Esto configura el Decoder para que coloque en el búfer el archivo con páginas gigantes y escriba mediante I/O directos para lograr el máximo rendimiento.
3. Actualice la configuración de los hilos de ejecución de análisis a los siguientes valores (bajo **/decoder/config**):
  - a. **parse.threads** =12
4. Seleccione el adaptador de puertos de captura. Las opciones incluyen:
  - a. Captura de un único puerto: **PFRINGZC,p1p1** o **PFRINGZC,p1p2**
  - b. Captura de ambos puertos:
    - i. Seleccione **PFRINGZC,P1P1**
    - ii. En la vista Explorador, configure **capture.device.params** = **capture=zc:p1p2,zc:p1p1**

**NOTA:** Según la configuración de hardware, los puertos de captura se pueden identificar con un nombre distinto de **p1p1/p1p2**, pero siempre tendrán el prefijo **PFRINGZC**. Por ejemplo, en algunos dispositivos, estos puertos se pueden identificar como **eth4 / eth5**. Para capturar desde **eth4**, seleccione **PFRINGZC,eth4**. Para capturar desde **eth5**, seleccione **PFRINGZC,eth5**.

## Consideraciones de almacenamiento

Cuando se captura a mayores velocidades, el sistema de almacenamiento que contiene las bases de datos de paquetes y metadatos debe ser capaz de entregar el rendimiento necesario para las lecturas y las escrituras en el disco. A continuación, se describen las opciones compatibles para configuraciones de DAC y SAN.

### Uso del hardware serie 4S (con dos o más unidades de DAC)

La unidad principal de Decoder está equipada con una tarjeta controladora SAS de RAID por hardware que proporciona conectividad a la DAC. En la configuración de la mayoría de las implementaciones, las DAC están conectadas en serie a un único puerto de la tarjeta SAS. Para lograr compatibilidad con ambientes de mayor velocidad, se requiere un mínimo de dos DAC por Decoder y cada una debe estar conectada directamente a la tarjeta SAS. Para ajustar dos DAC, conecte la primera a un puerto de la tarjeta SAS y, a continuación, conecte otra al otro puerto de la tarjeta SAS. Para los ambientes con más de dos DAC, conéctelas a cada puerto de manera balanceada. Esto puede requerir el recableado de las DAC en una implementación existente, pero no debería afectar a los datos que ya se capturaron en Decoder.

Si agrega nueva capacidad, use el script `NwMakeArray` actualmente disponible para provisionar las unidades de DAC. El script agrega automáticamente una DAC por ejecución (es decir, si se agregan tres DAC, el script se debe ejecutar tres veces) y las agrega a la configuración de `NwDecoder10G` como puntos de montaje por separado. Los puntos de montaje independientes son importantes, ya que permiten a `NwDecoder10G` segregarse los I/O de escritura de captura de los I/O de lectura necesarios para cumplir con solicitudes de contenido de paquetes.

### Uso del almacenamiento SAN

Decoder permitirá cualquier configuración de almacenamiento que pueda cumplir con el requisito de rendimiento continuo. Tenga en cuenta que el vínculo FC de 8 Gbit estándar a una SAN no es suficiente para leer y escribir datos de paquetes a 10G, razón por la cual es necesario que los ambientes que utilizan una SAN configuren la conectividad a esta mediante el uso de varios vínculos FC.

## Consideración de análisis y contenido para la captura de paquetes

La captura y la ejecución de enriquecimiento contra paquetes crudos pueden presentar retos únicos a cualquier velocidad de captura. A mayores velocidades de sesiones y paquetes en 10G, la eficiencia del análisis es primordial. Un único analizador puede tener un efecto perjudicial en el sistema y generar finalmente pérdidas de paquetes. Las pruebas realizadas para la captura 10G incluyeron analizadores de base y combinaciones de feeds, reglas y otro contenido accesibles mediante RSA Live. Tanto para un cliente que actualiza un sistema actualmente implementado como para uno que implementa un sistema nuevo, la recomendación es usar las siguientes mejores prácticas para minimizar el riesgo de pérdida de paquetes. Preste atención si actualiza una implementación actual de 10G, pero no agrega tráfico adicional. Por ejemplo, un Decoder actual que captura de una tarjeta 10G a 2G constantes no debería percibir una diferencia en el rendimiento, a menos que parte de la actualización también implique agregar tráfico adicional para la captura.

Mejores prácticas:

1. Incorpore analizadores de base (excepto SMB/Webmail, los cuales generalmente tienen una alta utilización del CPU) y compruebe que la pérdida de paquetes sea escasa o nula.
2. Cuando agregue analizadores adicionales, agregue solo uno o dos por vez.
3. Mida el impacto en el rendimiento del contenido recientemente agregado, en especial durante periodos de máximo tráfico.
  - Si se comienzan a producir pérdidas en circunstancias en que antes no se producían, inhabilite todos los analizadores recientemente agregados, habilite solo uno por vez y mida el impacto. Esto ayuda a detectar analizadores individuales que tienen efectos perjudiciales en el rendimiento. Tal vez sea posible reestructurarlos para que tengan un mejor funcionamiento o reducir su conjunto de funciones solo a aquellas que son necesarias para el caso de uso del cliente.
  - Aunque tienen impactos menores en el rendimiento, los feeds también se deben revisar y agregar en etapas con el fin de medir su impacto.
  - Las reglas de aplicaciones también tienden a tener un impacto mínimo observable, pero, nuevamente, es mejor no agregar una gran cantidad de ellas de una sola vez sin medir su impacto en el rendimiento.

Finalmente, la aplicación de los cambios recomendados en la configuración, los cuales se describen en la sección Configuración, ayudará a minimizar los posibles problemas.

## Agregación de un Decoder 10G a otros componentes de SA

La versión inicial ofrece compatibilidad con la agregación desde Packet Decoder a Concentrator. Se espera que las implementaciones que usan Malware Analytics, Event Stream Analysis, Warehouse Connector y Reporting Engine afecten el rendimiento y puedan causar una pérdida de paquetes. Debido al alto volumen de tasas de sesiones, se recomienda aplicar los siguientes cambios en la configuración:

- Una agregación de tipo nice en Concentrator limitó el impacto en el rendimiento en Decoder 10G  
`/concentrator/config/aggregate.nice = true`
- Debido al alto volumen de sesiones en Concentrator, puede considerar la activación del modo “valores paralelos” en Concentrator con la configuración de `/sdk/config/parallel.values` en `true`. Esto mejorará el rendimiento de las investigaciones cuando la cantidad de sesiones por segundo sea mayor que 30,000.
- Se requerirá una revisión adicional del contenido y el análisis en aquellas implementaciones en las cuales se desee el uso de otros componentes de SA (es decir, Warehouse, Malware Analysis, ESA y Reporting Engine).