RSA Security Analytics

Guía de instalación de capacidad de conexión directa (DAC) serie 4

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.
No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Guía de instalación de capacidad de conexión directa (DAC) serie 4

- Guía de instalación de capacidad de conexión directa (DAC) serie 4 4
    - Descripción del hardware de la DAC 5
    - Instalar la DAC 7

RSA

Guía de instalación de capacidad de conexión directa (DAC) serie 4

Descripción general

En este documento se proporcionan instrucciones para instalar una DAC serie 4 de 15 unidades en los dispositivos Decoder serie 4, Concentrator serie 4, Archiver serie 4, Hybrid serie 4 y All-In-One serie 4.

Contexto

Las instrucciones de instalación del hardware que se presentan en este documento se aplican solo al hardware y no a una versión específica del software de Security Analytics.

Note: cuando consulte una guía impresa, tenga en cuenta que una versión más reciente puede estar disponible en línea en **sadocs.emc.com/es-mx**. Esta guía está disponible en la ayuda en línea de Security Analytics bajo Guías de instalación del hardware.

.

Descripción del hardware de la DAC

Descripción general

Este tema es una descripción general del dispositivo de almacenamiento de capacidad de conexión directa (DAC) serie 4 de 15 unidades de Security Analytics.

Descripción del hardware

La DAC de Security Analytics es un gabinete de arreglos de unidades con tecnología de EMC^2. La DAC se usa para ampliar el almacenamiento utilizable en un dispositivo Decoder, Concentrator, Archiver, Hybrid u All-In-One serie 4.

Introducción

El dispositivo de DAC serie 4 de RSA Security Analytics incluye el software de DAC instalado. La configuración inicial de una DAC en la red implica los siguientes pasos:

1. Revisar los requisitos del sitio y la información de seguridad.
2. Instalar la DAC.

Contenido del paquete

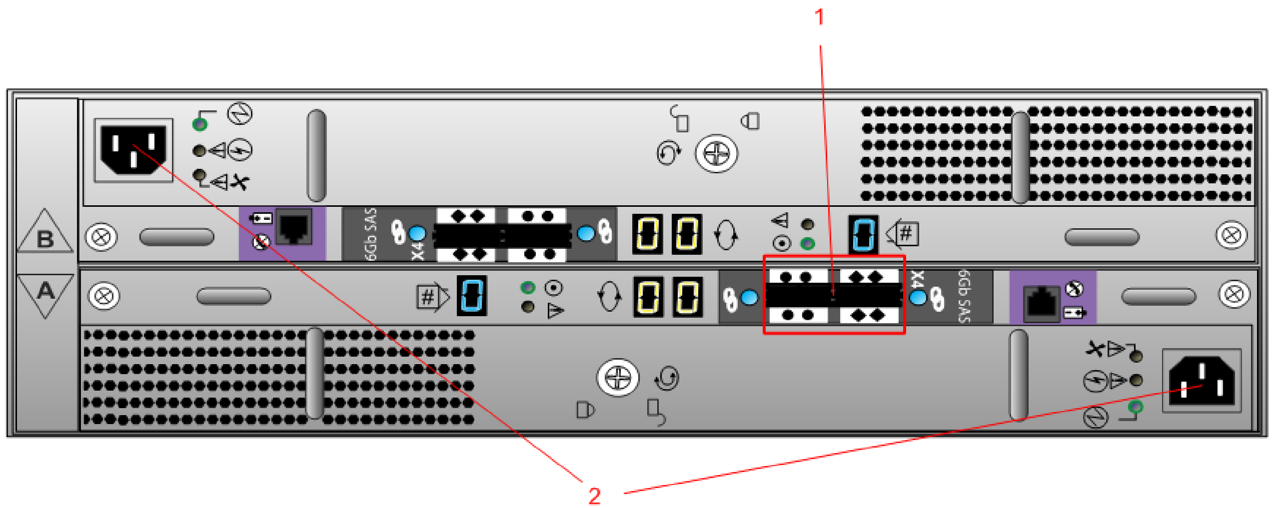
Consulte la documentación de EMC^2 que se incluye con la DAC.

> **Note:** la DAC incluye dos cables SAS. Solo necesita un cable para conectarla al dispositivo. El segundo cable SAS es un cable de repuesto.

Materiales suministrados por el cliente

No es necesario proporcionar ningún material.

Vista posterior de la DAC



Clave	Descripción
1	Puertos SAS. Cada conjunto de puertos tiene un puerto de expansión y un puerto primario. En cada conjunto, el puerto primario está más cerca del centro del chasis.
2	Conexión de entrada de alimentación

RSA

Instalar la DAC

Descripción general

En este tema se indica cómo instalar una DAC serie 4 de 15 unidades en los dispositivos Decoder serie 4, Concentrator serie 4, Archiver serie 4, Hybrid serie 4 y All-In-One serie 4.

Introducción

En la siguiente tabla se presentan instrucciones de instalación resumidas para distintas implementaciones. Los procedimientos detallados se encuentran en subsecciones individuales. Los escenarios de implementación son:

- Múltiples DAC: en una implementación de Concentrator, Decoder, Log Decoder y Archiver.
- Una única DAC en una implementación de Hybrid.
- Una única DAC para All-In-One.

Requisitos previos

Asegúrese de contar con el siguiente software requerido:

- `arrayCfg-2.1.tgz` o más reciente, el cual necesita para configurar el almacenamiento. Este script se actualiza cada tres meses y la versión se representa de la siguiente manera: `arrayCfg-<x.y-z>.tgz`, donde `<x.y-z>` es el número de versión. Póngase en contacto con Atención al cliente de RSA para obtener la versión más reciente.
- `nwraidutil.pl`

Procedimiento general

En esta tabla se resumen los pasos para distintos escenarios de implementación.

Escenario de implementación	Tareas
Concentrator/ Archiver Decoder/ Log Decoder (Múltiples DAC)	**Caution:** asegúrese de NO haber obtenido una licencia para el dispositivo antes de ejecutar el script `NwArrayConfig.py` con la opción

<table>
<tr><th>Escenario de implementación</th><th>Tareas</th></tr>
<tr><td></td><td>--init. Cuando instale múltiples DAC en Decoder serie 4/4S, realice los pasos 1, 2 y 3 (cableado e inicialización de la primera DAC), antes de obtener licencia para los servicios e iniciarlos. Si no se siguen las instrucciones, puede haber problemas en la estructura de directorios y una posible pérdida de datos, o tal vez sea necesario volver a crear la imagen del dispositivo.

1. Conecte la primera DAC al dispositivo antes de encenderlo, como se describe en Conectar una DAC a un dispositivo.
2. Ejecute el script NwArrayConfig.py con la opción --init, como se describe en Ejecutar los scripts de instalación de la DAC en Decoder, Concentrator o Archiver en Decoder o Log Decoder.

Note: si por error obtiene una licencia para el dispositivo antes de ejecutar este script, póngase en contacto con Atención al cliente de RSA para que le ayuden a restaurar las unidades de la DAC a su estado original.

3. Reinicie el servicio como se describe en Reiniciar el servicio Decoder o Concentrator.
4. Obtenga una licencia para el dispositivo. Consulte instrucciones para obtener licencias para los dispositivos en la Guía de licencia de Security Analytics, disponible a través de la opción Ayuda de Security Analytics y en sadocs.emc.com/es-mx.
5. Conecte DAC adicionales al dispositivo antes de encender los dispositivos.
6. Ejecute scripts de instalación de la DAC con la opción --add en DAC adicionales, como se describe en Ejecutar los scripts de instalación de la DAC para agregar más arreglos de almacenamiento.
7. Reinicie el servicio como se describe en Reiniciar el servicio Decoder o Concentrator.</td></tr>
<tr><td>Hybrid/AIO</td><td>1. Conecte la DAC al dispositivo antes de encenderlo, como se describe en Conectar una DAC a un dispositivo.

Caution: antes de configurar almacenamiento adicional en un dispositivo Hybrid u All-in-One (AIO), asegúrese de que todos los servicios que se ejecutan en Hybrid o AIO (por ejemplo, Concentrator, Decoder, Broker y Log Decoder) tengan licencia.

2. Obtenga una licencia para el dispositivo y los servicios. Consulte instrucciones en la Guía de licencia de Security Analytics, disponible a través de la opción Ayuda de Security Analytics y en sadocs.emc.com/es-mx. Ejecute el script NwArrayConfig.py con la opción --add, como se describe en Agregar una DAC en un dispositivo Hybrid o AIO.</td></tr>
</table>

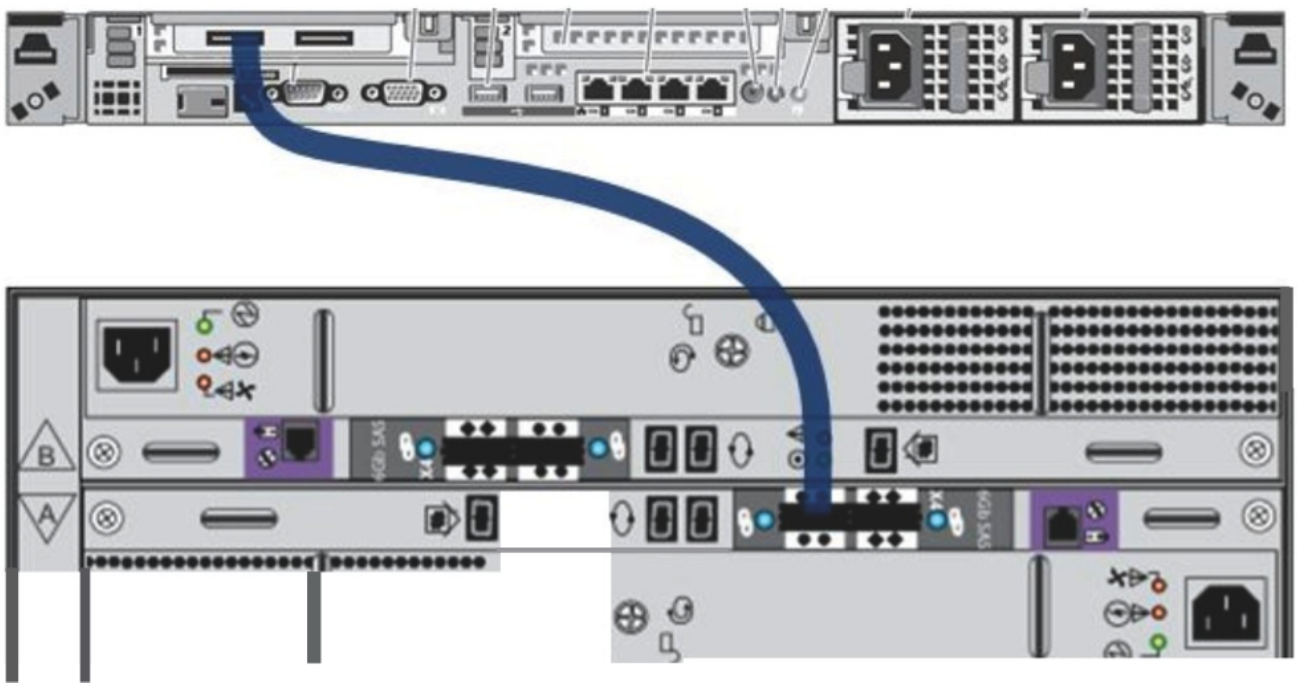
Conectar una DAC a un dispositivo

Las instrucciones de cableado se aplican a todos los dispositivos que se enumeran bajo los tipos de implementación: Concentrator, Decoder, Log Decoder, Archiver, Hybrid y All-In-One.

Note: La DAC viene con dos cables SAS. Solo necesita un cable para conectar la DAC al dispositivo. El segundo cable SAS es de repuesto.

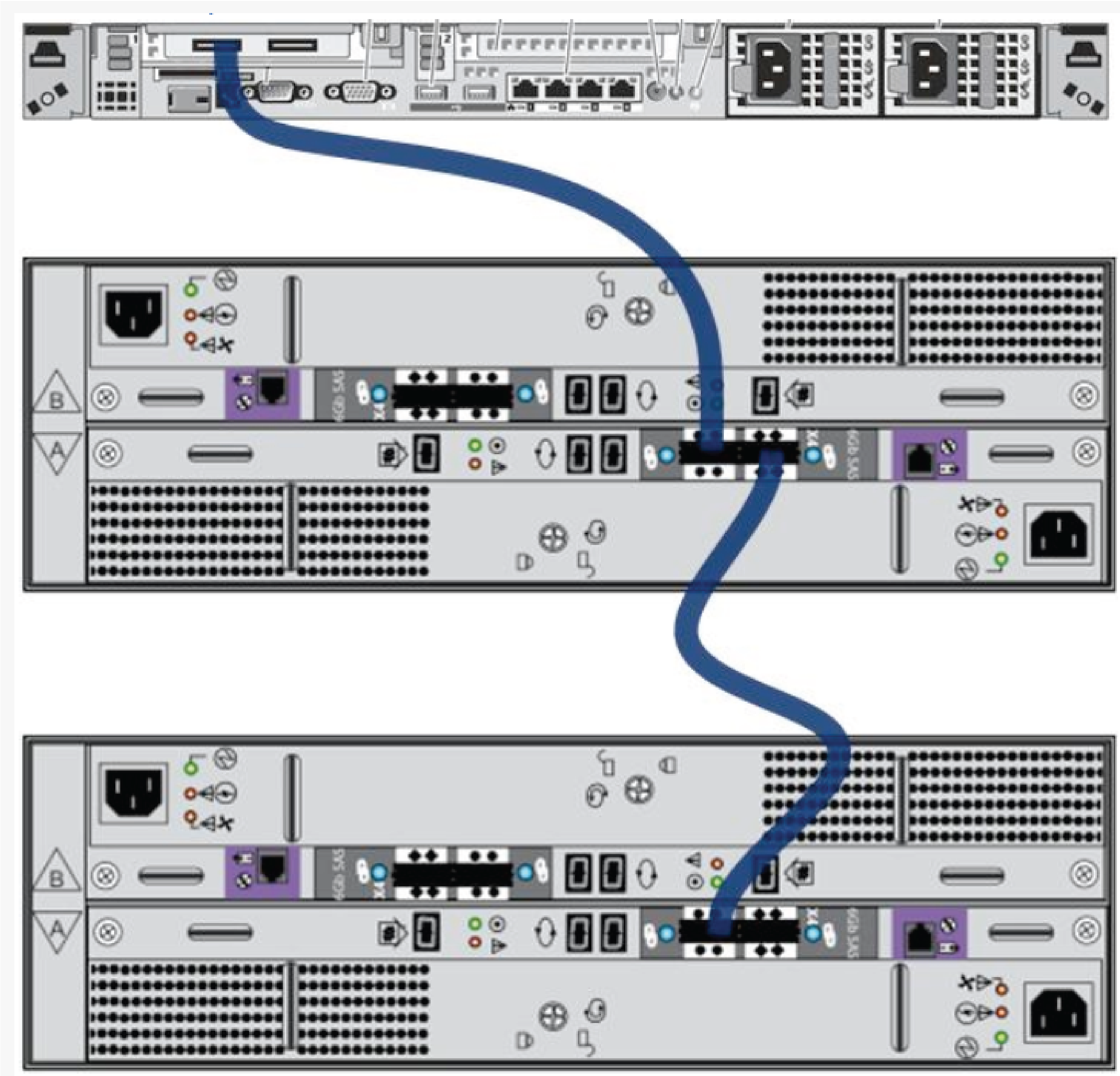
Para conectar la DAC a un dispositivo:

1. Conecte un extremo del cable SAS al puerto **izquierdo** del controlador RAID en la parte posterior del dispositivo Security Analytics serie 4.
   Si el script no detecta las unidades adicionales, puede ser necesario intentar en el otro puerto del controlador RAID.
2. Conecte el otro extremo del cable SAS a la unidad de la DAC.
   Cuando conecte la primera DAC al controlador RAID, asegúrese de insertar el cable en el **puerto SAS primario** de la DAC, como se muestra en la siguiente ilustración.



3. Cuando conecte dos o más DAC al controlador RAID, asegúrese de:
   a. Insertar el cable del Decoder en el puerto **primario** de la primera DAC.
   b. Conectar la DAC siguiente y las posteriores desde el puerto **secundario** de la primera al puerto **primario** de la siguiente.

   En la siguiente ilustración se muestra cómo conectar múltiples DAC.



Ejecutar los scripts de instalación de la DAC en Decoder, Concentrator o Archiver

> ⚠ **Caution:** Los servicios Decoder, Concentrator o Archiver no deben haberse habilitado con licencia antes de la ejecución del script con la opción `--action init`.

Para ejecutar los scripts de instalación de la DAC en Decoder o Concentrator:

1. Copie el archivo `arrayCfg-2.1.tgz` al dispositivo en `/root` a través de SCP.

2. Escriba el siguiente comando para extraer el contenido:
   `tar -zxf arrayCfg-2.1.tgz`
3. Cambie al directorio `arrayCfg` que acaba de crear:
   `cd arrayCfg`
4. Ejecute el siguiente comando:
   `#nwraidutil.pl | more`
5. Compruebe los resultados para asegurarse de que no haya configuraciones que no correspondan ni unidades con estado `Unconfigured(bad)` en las unidades de la DAC. Si estas condiciones están presentes, resuélvalas antes de ejecutar el script.
6. Ejecute el script `NwArrayConfig.py` mediante el uso de la siguiente cadena de comandos:
   ```
   [root@CSO-S4Concentrator  ~]# ./NwArrayConfig.py --action init --service
   (decoder|concentrator/archiver)
   ```
   El script crea todas las unidades virtuales, los volúmenes lógicos y la estructura de directorios necesarios, y escribe los mensajes de depuración en `arrayCfg.log.`
7. Cuando se haya completado la ejecución del script, agregue el dispositivo mediante Security Analytics Administration y obtenga licencia para los servicios Decoder, Concentrator y Archiver.
8. Verifique los resultados:
   a. Asegúrese de que el script no haya producido ningún error. Para esto, consulte el archivo `arrayCfg.log`.
   b. Ejecute el siguiente comando para verificar los nuevos tamaños de las bases de datos:
      `df -Ph|awk '/(concentrator|decoder|archiver|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'`
      El siguiente es un ejemplo de los resultados que se muestran:
      ```
      Mounted                                         Size
      /var/netwitness/concentrator                    30G
      /var/netwitness/concentrator/index              1.1T
      /var/netwitness/concentrator/sessiondb          1013G
      /var/netwitness/concentrator/metadb             9.9T
      ```

Ejecutar los scripts de instalación de la DAC para agregar más arreglos de almacenamiento

Para ejecutar los scripts de instalación de la DAC en Decoder o Concentrator con el fin de agregar más almacenamiento después de la inicialización:

1. Si el archivo `arrayCfg-2.1.tgz` no se copió en el dispositivo, copie el archivo `arrayCfg-2.1.tgz` al dispositivo en `/root` a través de SCP.
2. Ejecute el siguiente comando:
   `nwraidutil.pl | more.`
3. Compruebe los resultados para asegurarse de que no haya configuraciones que no correspondan ni unidades con estado `Unconfigured(bad)` en las unidades de la DAC. Si estas condiciones están presentes, resuélvalas antes de ejecutar el script.
4. Asegúrese de que:
   a. Decoder o Concentrator tengan licencia antes de ejecutar el script `NwArrayConfig.py`.
   b. REST esté habilitado en Decoder y en el servicio del dispositivo.
5. Ingrese la siguiente cadena de comandos para cambiar de directorio a `/root/arrayCfg`:
   `cd /root/arrayCfg`
6. Ingrese la siguiente cadena de comandos para ejecutar el script `NwArrayConfig.py`:
   ```
   [root@CSO-DecoderSM ~]# ./NwArrayConfig.py --action add --service
   (concentrator|decoder|archiver)
   ```

El script busca la siguiente DAC adicional con unidades disponibles. Crea una unidad lógica para esta y la configura según corresponda de acuerdo con el tipo de servicio. Todos los mensajes se registran en `./arrayCfg.log.`

7. Repita los pasos del 1 al 6 para cada DAC hasta que estén todas configuradas.
8. Verifique los resultados:
   a. Asegúrese de que el script no haya producido ningún error.
   b. Ejecute la siguiente cadena de comandos para verificar los nuevos tamaños de las bases de datos:
   `df -Ph|awk '/(concentrator|decoder|archiver|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'`
   El siguiente es un ejemplo de los resultados que se muestran:
   ```
   Mounted                                                Size
   /var/netwitness/decoder                                10G
   /var/netwitness/decoder/index                          30G
   /var/netwitness/decoder/metadb                         3.5T
   /var/netwitness/decoder/sessiondb                      185G
   /var/netwitness/decoder/packetdb                       19T
   /var/netwitness/decoder/packetdb0                      24T
   ```
   c. Asegúrese de que haya una entrada para cada DAC que se agregó. Habrá una `/var/netwitness/decoder/packetdb#` para cada una que se crea. Verifique que el tamaño que se indica para `/var/netwitness/decoder/packetdb#` sea aproximadamente el previsto con los arreglos de almacenamiento ampliados conectados. Anote este número de modo que pueda verificarlo en la interfaz de Security Analytics.
   d. Inicie sesión en la interfaz de Security Analytics y, en el menú de Security Analytics, seleccione **Administration** > **Dispositivos**.
   Se muestra la vista Dispositivos de Administration.
   e. Seleccione el Decoder o el Log Decoder y elija **Ver > Explorar** en la barra de herramientas.
   f. Expanda la carpeta **database** y seleccione la carpeta **config**.
   g. Observe el nodo **packet.dir** y expándalo por completo. Asegúrese de que haya una entrada para cada DAC que se agregó y que el tamaño de `packetdb` para cada una de ellas sea el siguiente:
   `/var/netwitness/decoder/packetdb#/packetdb==<n>`
   donde `<n>` es igual a un 95 % del tamaño del nuevo dispositivo en TB. Esto debe corresponder al 95 % del resultado que devolvió el comando `df -Ph` ejecutado anteriormente para `/var/netwitness/decoder/packetdb#`

Reiniciar los servicios Decoder, Concentrator o Archiver

Debe reiniciar los servicios Decoder, Concentrator o Archiver de modo que puedan reconocer el nuevo espacio. Reinicie los servicios Decoder, Concentrator o Archiver y asegúrese de que vuelvan a estar en línea y que inicien la captura.

Agregar una DAC a un dispositivo Hybrid u All-in-One (AIO)

> **Caution:** antes de agregar almacenamiento adicional en un dispositivo Hybrid u All-in-One, asegúrese de que todos los servicios que se ejecutan en Hybrid o AIO (por ejemplo, Concentrator, Decoder, Broker y Log Decoder) tengan licencia. Consulte instrucciones en la **Guía de licencia de Security Analytics**, disponible a través de la opción **Ayuda** de Security Analytics y en sadocs.emc.com/es-mx.

Para agregar una DAC a un dispositivo Hybrid u All-in-One (AIO):

1. Conecte la DAC al dispositivo (como se describe en **Conectar una DAC a un dispositivo**).
2. Copie el archivo `arrayCfg-2.1.tgz` al dispositivo en `/root` a través de SCP.
3. Extraiga el contenido:
   ```
   tar -zxf arrayCfg-2.1.tgz
   ```
4. Cambie al directorio `arrayCfg` que acaba de crear:
   ```
   cd arrayCfg
   ```
5. Escriba los siguientes comandos para ver las unidades configuradas:
   ```
   #nwraidutil.pl | more
   #df -h
   ```
6. Revise los volúmenes antes de ejecutar el script. Para asegurarse de que no haya configuraciones que no correspondan ni unidades con estado `Unconfigured(bad)` en las unidades de la DAC, escriba el siguiente comando:
   ```
   df -Ph|awk '/(concentrator|decoder|archiver|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'
   ```
   El siguiente es un ejemplo de los resultados que se muestran:
   ```
   Mounted                                    Size
   /var/netwitness/concentrator               30G
   /var/netwitness/concentrator/index         300G
   /var/netwitness/concentrator/metadb        2.2T
   /var/netwitness/concentrator/sessiondb     300G
   /var/netwitness/logdecoder                 30G
   /var/netwitness/logdecoder/index           10G
   /var/netwitness/logdecoder/packetdb        2.7T
   /var/netwitness/logdecoder/metadb          300G
   /var/netwitness/logdecoder/sessiondb       30G
   ```
7. Para ejecutar el script `NwArrayConfig.py`, escriba el siguiente comando:
   ```
   [root@CSO-DecoderSM ~]# ./NwArrayConfig.py --action add --service hybrid --drives <N>
   ```
   donde `<N>` es la cantidad de unidades que se asignarán a la parte de Concentrator del dispositivo Hybrid. De manera predeterminada `<N>` es `3.` El script busca la siguiente DAC adicional con unidades disponibles. Crea unidades lógicas para cada servicio Hybrid y las configura según corresponda de acuerdo con el tipo de servicio. Todos los mensajes se registran en `./arrayCfg.log.`
8. Repita los pasos del 1 al 7 para cada DAC hasta que estén todas configuradas.
9. Verifique los resultados:
   a. Asegúrese de que el script no haya producido ningún error.
   b. Escriba el siguiente comando para verificar los nuevos tamaños de las bases de datos:
      ```
      df -Ph|awk '/(concentrator|decoder|archiver|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'
      ```
      El siguiente es un ejemplo de los resultados que se muestran:
      ```
      Mounted                                    Size
      /var/netwitness/concentrator               30G
      /var/netwitness/concentrator/index         300G
      /var/netwitness/concentrator/metadb        2.2T
      /var/netwitness/concentrator/sessiondb     300G
      /var/netwitness/logdecoder                 30G
      /var/netwitness/logdecoder/index           10G
      /var/netwitness/logdecoder/packetdb        2.7T
      /var/netwitness/logdecoder/metadb          300G
      /var/netwitness/logdecoder/sessiondb       30G
      /var/netwitness/concentrator/sessiondb0    373G
      /var/netwitness/concentrator/metadb0       3.3T
      /var/netwitness/logdecoder/packetdb0       19T
      /var/netwitness/concentrator/sessiondb1    373G
      /var/netwitness/concentrator/metadb1       3.3T
      /var/netwitness/logdecoder/packetdb1       19T
      ```

c. Asegúrese de que haya una entrada para cada DAC que se agregó. Habrá una `/var/netwitness/decoder/packetdb#` para cada una que se crea. Verifique que el tamaño que se indica para `/var/netwitness/decoder/packetdb#` sea aproximadamente el previsto con los arreglos de almacenamiento ampliados conectados. Anote este número de modo que pueda verificarlo en la interfaz de Security Analytics.

d. Inicie sesión en la interfaz de Security Analytics y, en el menú de Security Analytics, seleccione **Administration** > **Dispositivos**.
Se muestra la vista Dispositivos de Administration.

e. Seleccione el Decoder o el Log Decoder y elija **Ver** > **Explorar** en la barra de herramientas.

f. Expanda la carpeta **database** y seleccione la carpeta **config**.

g. Observe el nodo **packet.dir** y expándalo por completo. Asegúrese de que haya una entrada para cada DAC que se agregó y que el tamaño de packetdb para cada una de ellas sea el siguiente:
`/var/netwitness/decoder/packetdb#/packetdb==<n>`
donde `<n>` es igual a un 95 % del tamaño del nuevo dispositivo en TB. Esto debe corresponder al 95 % del resultado que devolvió el comando `df -Ph` ejecutado anteriormente para `/var/netwitness/decoder/packetdb#`