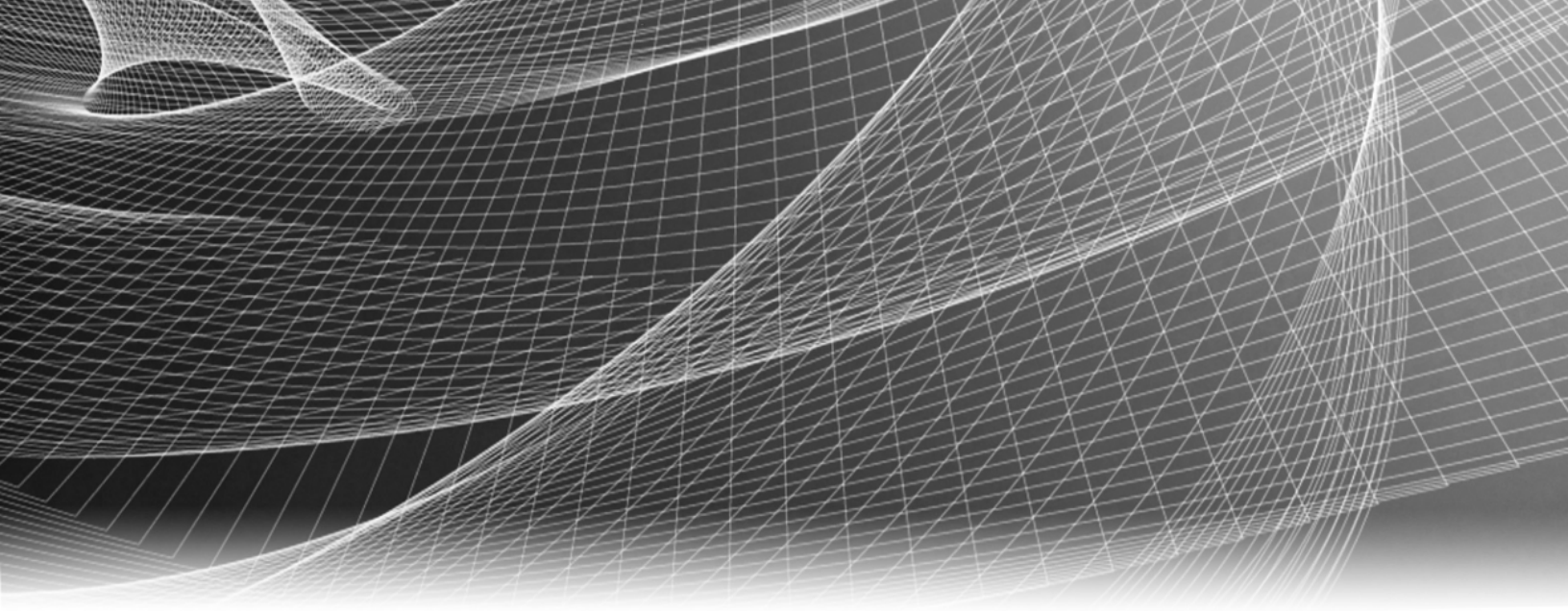


RSA Security Analytics

Guía de instalación de la DAC serie 5 de 15 unidades

RSA

EMC²

Trademarks

License Agreement

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 la DAC serie 5 de 15 unidades

RSA

Guía de instalación de la DAC serie 5 de 15 unidades

Descripción general

En este documento se proporcionan instrucciones para instalar una capacidad de conexión directa (DAC) de 15 unidades en los dispositivos Decoder, Log Decoder, Concentrator, Archiver y Hybrid serie 5.

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. Este documento es solo para el hardware nuevo. No se aplica a una DAC con datos preexistentes.

Caution: Si está agregando una DAC existente a un nuevo dispositivo, NO siga las instrucciones de esta guía. Póngase en contacto con Atención al cliente de RSA.

Si tiene una DAC con datos preexistentes e intenta ejecutar el script señalado en estas instrucciones, este podría fallar o podría eliminar los datos existentes de la DAC y crear todas las unidades virtuales, los volúmenes lógicos y la estructura de directorios necesarios.

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.

Last Modified: September 15 2016, 11:33AM

RSA

Descripción del hardware de la DAC

Descripción general

Este tema es una descripción general del dispositivo de almacenamiento de capacidad de conexión directa (DAC) 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, Log Decoder, Concentrator, Archiver o Hybrid serie 5.

Introducción

El dispositivo de DAC 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.

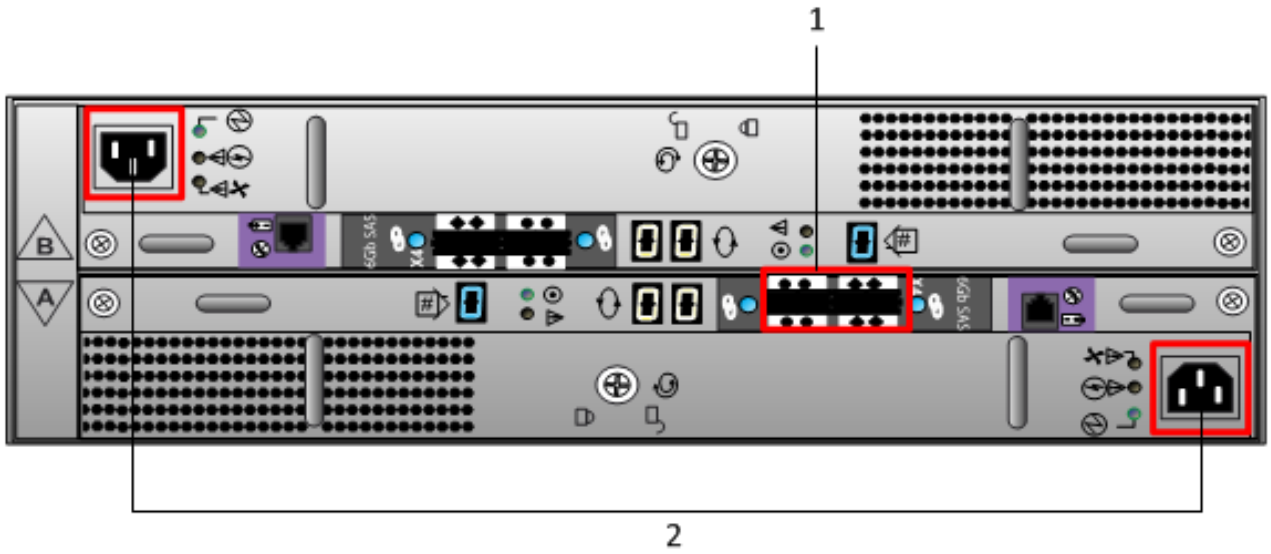
Note: La DAC viene con dos cables SAS. Solo necesita un cable para conectar la DAC al dispositivo. El segundo cable SAS es un cable de repuesto.

Materiales suministrados por el cliente

No es necesario proporcionar ningún material.

Last Modified: September 15 2016, 11:33AM

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

Last Modified: September 15 2016, 11:33AM

RSA

Instalar la DAC

Descripción general

En este tema se indica cómo instalar una DAC de 15 unidades en los dispositivos (Packet) Decoder, Log Decoder, Concentrator, Archiver y Hybrid serie 5.

Requisitos previos

Asegúrese de contar con el siguiente software requerido:

- `rsa-sa-tools-10.5.1.0.82-1.el6.noarch.rpm` o más reciente, que contiene el script necesario para configurar el almacenamiento.

Este RPM se actualiza trimestralmente. Póngase en contacto con Atención al cliente de RSA para obtener la versión más reciente.

> ⚠ **Caution:** Si está agregando una DAC existente a un nuevo dispositivo, NO siga las instrucciones de esta guía. Póngase en contacto con Atención al cliente de RSA.
>
> Si tiene una DAC con datos preexistentes e intenta ejecutar el script señalado en estas instrucciones, este podría fallar o podría eliminar los datos existentes de la DAC y crear todas las unidades virtuales, los volúmenes lógicos y la estructura de directorios necesarios.

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, (Packet) Decoder, Log Decoder y Archiver.
- Una única DAC en una implementación de Hybrid.

Last Modified: September 15 2016, 11:33AM

Procedimiento general

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

Escenario de implementación	Tareas
Concentrator, Archiver, Decoder y Log Decoder (Múltiples DAC)	1. Conecte la DAC al dispositivo antes de encenderlo, como se describe en Conectar una DAC a un dispositivo Concentrator, Archiver, Decoder o Log Decoder. 2. Ejecute el script `NwArrayConfig.py` como se describe en Ejecutar los scripts de instalación de la DAC en Packet Decoder, Log Decoder, Concentrator o Archiver. 3. Reinicie el servicio como se describe en Reiniciar el servicio. 4. Obtenga una licencia para el dispositivo (si aún lo la tiene). 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.
Hybrid	1. Conecte la DAC al dispositivo antes de encenderlo, como se describe en Conectar una DAC a un dispositivo Hybrid. 2. Ejecute el script `NwArrayConfig.py` como se describe en Ejecutar los scripts de instalación de la DAC en un dispositivo Hybrid. 3. Reinicie el servicio como se describe en Reiniciar el servicio.

Last Modified: September 15 2016, 11:33AM

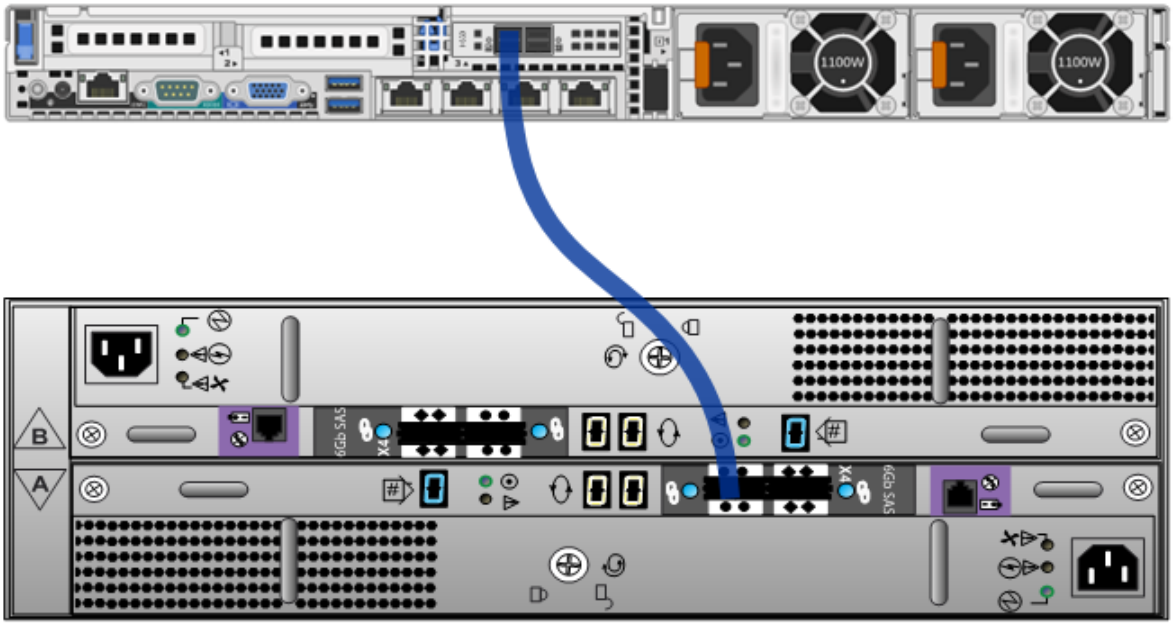
Conectar las DAC a un dispositivo Concentrator, Archiver, Decoder o Log Decoder

Puede conectar una o más DAC a un dispositivo Concentrator, Archiver, Decoder o Log Decoder serie 5. Solo puede agregar cuatro DAC por puerto para un total de ocho DAC por controlador RAID PERC H830.

Note: la DAC incluye dos cables SAS. Solo necesita un cable para conectarla al dispositivo. **Los dispositivos serie 4 y serie 5 requieren cables distintos.** Use el cable con el puerto mini-SAS para la conexión a un dispositivo serie 5. El otro cable permite la conexión a un dispositivo serie 4.

1. Conecte un extremo del cable SAS al puerto **izquierdo** del controlador RAID en la parte posterior del dispositivo Security Analytics Concentrator, Archiver, Decoder o Log Decoder serie 5.

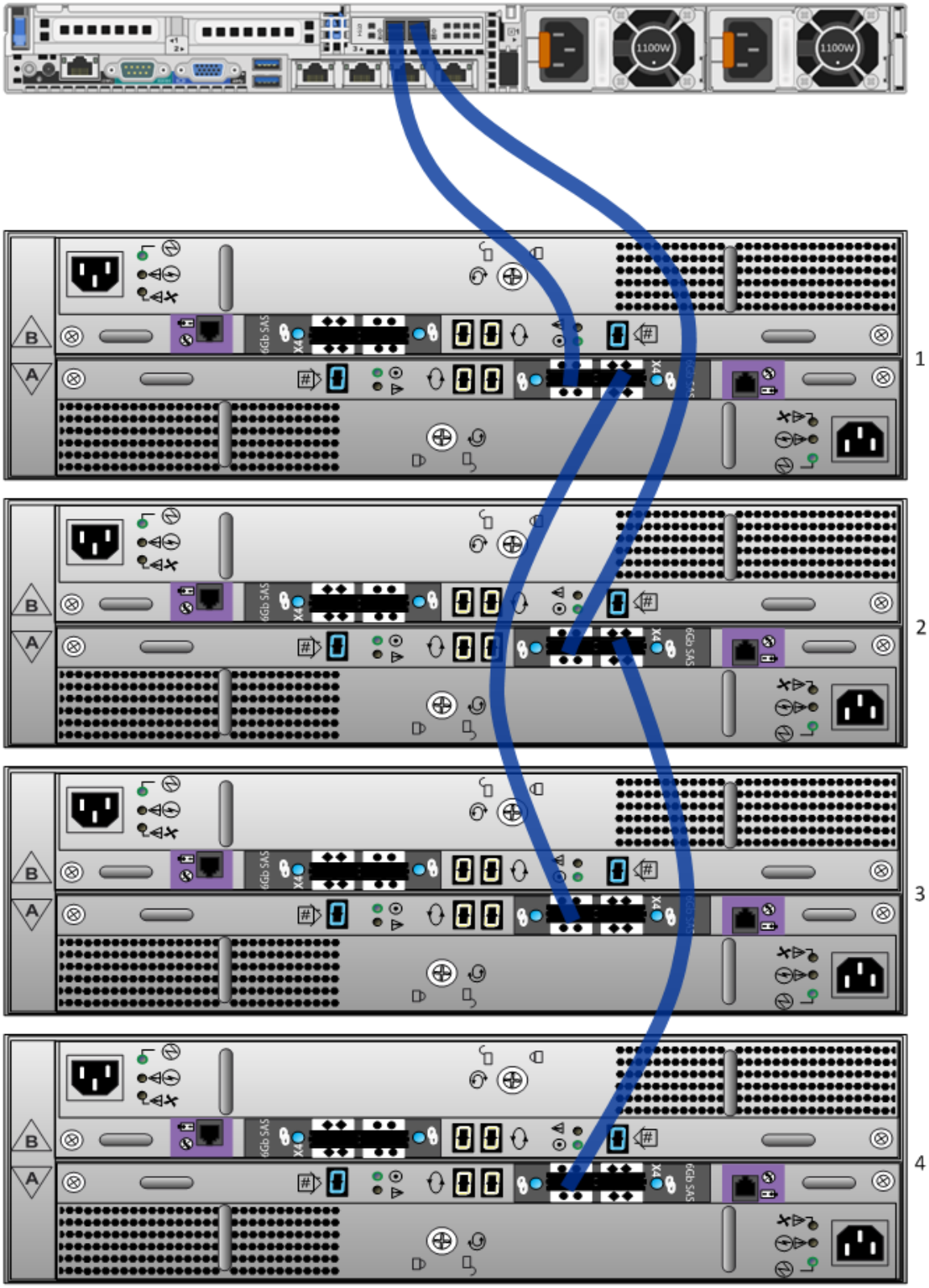
2. Conecte el otro extremo del cable SAS a la unidad de la DAC.
   Cuando conecte la primera DAC al controlador RAID, asegúrese de insertar el cable en el **puerto SAS primario** de la DAC, como se muestra en la siguiente figura.



3. Cuando conecte dos o más DAC al controlador RAID, asegúrese de:
   a. Conecte el puerto **primario** de la primera DAC al puerto izquierdo del controlador RAID de Decoder.
   b. Conecte el puerto **primario** de la segunda DAC al puerto derecho del controlador RAID de Decoder.
   c. Conecte el puerto **primario** de la tercera DAC al puerto **secundario** de la primera DAC.
   d. Conecte el puerto **primario** de la cuarta DAC al puerto **secundario** de la segunda DAC.
   e. Continúe con este patrón hasta un total de ocho DAC por controlador RAID PERC H830.

Last Modified: September 15 2016, 11:33AM

En la siguiente figura se muestra cómo conectar múltiples DAC.



Last Modified: September 15 2016, 11:33AM

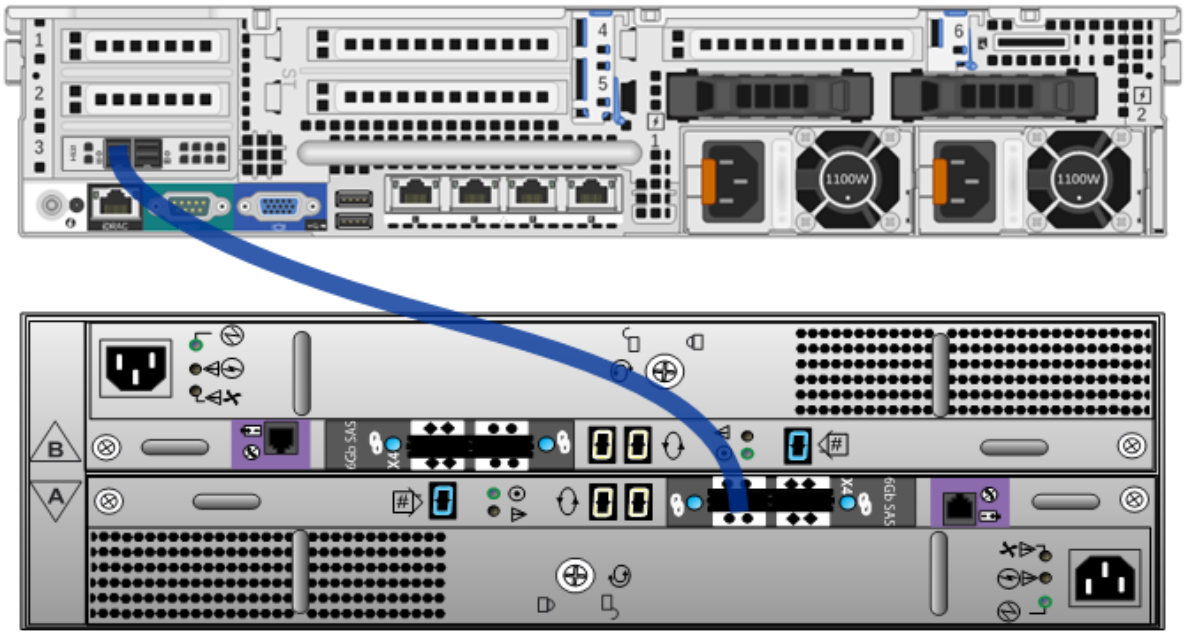
Conectar una DAC a un dispositivo Hybrid

Puede conectar solo una DAC a un dispositivo Hybrid serie 5.

Note: la DAC incluye dos cables SAS. Solo necesita un cable para conectarla al dispositivo. **Los dispositivos serie 4 y serie 5 requieren cables distintos.** Use el cable con el puerto mini-SAS para la conexión a un dispositivo serie 5. El otro cable permite la conexión a un dispositivo serie 4.

1. Conecte un extremo del cable SAS al puerto **izquierdo** del controlador RAID en la parte posterior del dispositivo Security Analytics Hybrid serie 5.

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 figura.



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

1. Inicie sesión como `raíz` y verifique que el paquete **rsa-sa-tools** esté instalado mediante la ejecución del siguiente comando:
`rpm -qa | grep sa-tools`
Si el paquete no está instalado, póngase en contacto con el soporte de RSA para obtener una copia del RPM e instalarlo.
2. Cambie de directorio al directorio base de RPM de rsa-sa-tools:
`cd /opt/rsa/saTools`
3. Ejecute el siguiente comando:
`nwraidutil.pl | more`

Last Modified: September 15 2016, 11:33AM

4. 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.
5. Ejecute el script **NwArrayConfig.py** mediante el uso de la siguiente cadena de comandos:
   `./NwArrayConfig.py`
   Este script descubre todas las DAC disponibles; crea todas las unidades virtuales, los volúmenes lógicos y la estructura de directorios necesarios, y escribe los mensajes de depuración en **arrayCfg.log**.
6. Cuando se haya completado la ejecución del script, agregue, si aún no lo ha hecho, el dispositivo mediante Security Analytics Administration y obtenga licencia para los servicios Decoder, Log Decoder, Concentrator y Archiver.
7. Verifique los resultados:
   a. Asegúrese de que el script no haya producido ningún error. Para esto, consulte el archivo **arrayCfg.log**.
   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                                   6.6T
      /var/netwitness/decoder/sessiondb                                701G
      /var/netwitness/decoder/packetdb                                  41T
      /var/netwitness/decoder/sessiondb0                               746G
      /var/netwitness/decoder/metadb0                                  6.6T
      /var/netwitness/decoder/packetdb0                                 41T
      ```
   c. Asegúrese de que haya una entrada para cada DAC que se agregó. Se crean `packetdb#`, `metadb#` y `sessiondb#` individuales para cada DAC, donde `#` es el número asociado con la DAC en el orden en que se agregó. Para la primera DAC que agregó, `#` aparece en blanco sin un número añadido. A la segunda DAC que agregó se le agrega un `0`. Por ejemplo, las entradas de la primera DAC son `metadb`, `sessiondb` y `packetdb`. Las entradas de la segunda DAC son `metadb0`, `sessiondb0` y `packetdb0`.
      Verifique que el tamaño enumerado para `/var/netwitness/decoder/packetdb#` sea el previsto con los arreglos de almacenamiento ampliados conectados. **Anote este valor** de modo que pueda verificarlo en la interfaz de Security Analytics.
   d. Inicie sesión en Security Analytics y, en el menú de Security Analytics, seleccione **Administration > Servicios**.
      Se muestra la vista Servicios de Administration.
   e. Seleccione el Decoder o el Log Decoder y elija  **> Ver > Explorar**.
   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 almacenamiento en TB. Esto debe corresponder al 95 % del resultado que devolvió el comando `df -Ph` ejecutado anteriormente para `/var/netwitness/decoder/packetdb#`
   h. Siga los pasos 7 e al g y verifique el nodo **meta.dir** en Concentrator y el nodo **database.dir** en Archiver.

Last Modified: September 15 2016, 11:33AM

Ejecutar los scripts de instalación de la DAC en un dispositivo Hybrid

1. Inicie sesión como `raíz` y verifique que el paquete **rsa-sa-tools** esté instalado mediante la ejecución del siguiente comando:
   `rpm -qa | grep sa-tools`
   Si el paquete no está instalado, póngase en contacto con el soporte de RSA para obtener una copia del RPM e instalarlo.
2. Cambie de directorio al directorio base de RPM de rsa-sa-tools:
   `cd /opt/rsa/saTools`
3. Ejecute el siguiente comando:
   `nwraidutil.pl | more`
4. 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.
5. 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|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
   ```
6. Para ejecutar el script `NwArrayConfig.py`, escriba el siguiente comando:
   `./NwArrayConfig.py --drives <N>`
   donde `<N>` es la cantidad de unidades que se asignarán al servicio Concentrator. De manera predeterminada `<N>` es `3`. Si se trata de un Hybrid Log, RSA recomienda usar el valor `7` para asignar el almacenamiento entre los dos servicios de manera más eficiente. Todos los mensajes se registran en `./arrayCfg.log`.
7. 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|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
      ```


Last Modified: September 15 2016, 11:33AM

```
/var/netwitness/concentrator/sessiondb0              373G
/var/netwitness/concentrator/metadb0                 3.3T
/var/netwitness/logdecoder/packetdb0                 19T
```

c. Asegúrese de que haya una entrada para la DAC que se agregó. Se crean `packetdb0`, `metadb0` y `sessiondb0` individuales para la DAC que se agregó. Verifique que el tamaño que se indica para `/var/netwitness/decoder/packetdb0` sea el previsto con los arreglos de almacenamiento ampliados conectados. **Anote este valor** de modo que pueda verificarlo en la interfaz de Security Analytics.

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

e. Seleccione el Decoder o el Log Decoder y elija  **> Ver** > **Explorar**.

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 la DAC que se agregó y que el tamaño de packetdb sea el siguiente:
`/var/netwitness/decoder/packetdb0/packetdb==<n>`
donde `<n>` es igual a un 95 % del tamaño del nuevo almacenamiento en TB. Esto debe corresponder al 95 % del resultado que devolvió el comando `df -Ph` ejecutado anteriormente para `/var/netwitness/decoder/pcketdb0`

h. Siga los pasos 7 e al g y verifique el nodo **meta.dir** en el Concentrator.

Reiniciar el servicio

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

Last Modified: September 15 2016, 11:33AM