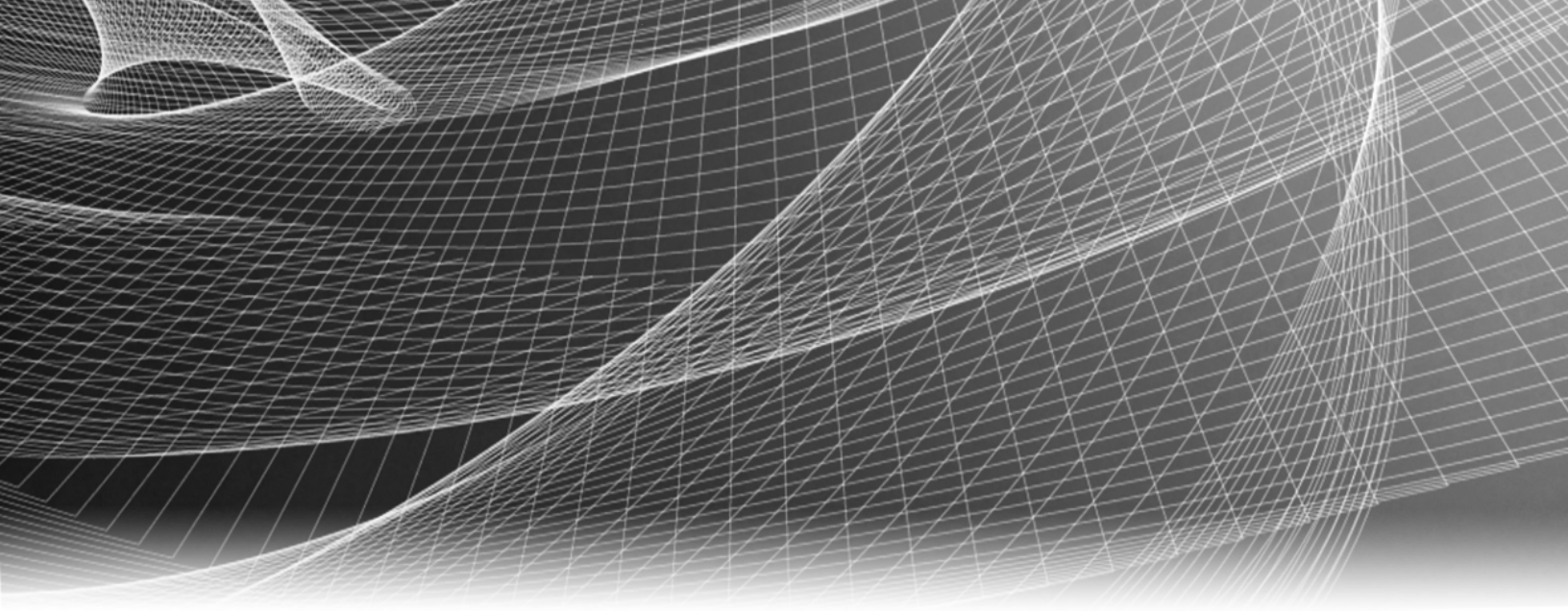


RSA Security Analytics

Guide de configuration du système DAC de 15 disques de la gamme 5

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.

Guide de configuration du système DAC de 15 disques de la gamme 5

RSA

Guide de configuration du système DAC de 15 disques de la gamme 5

Présentation

Ce document fournit des instructions pour installer un DAC de 15 disques pour les appliances de Decoder, Log Decoder, Concentrator, Archiver et les appliances hybrides de la gamme 5.

Contexte

Les instructions de configuration matérielle dans le présent document concernent uniquement le matériel. Elles ne s'appliquent pas à une version spécifique du logiciel Security Analytics. Ce document concerne uniquement le nouveau matériel. Il n'est pas destiné aux DAC avec des données préexistantes.

Caution: Si vous ajoutez un DAC existant à une nouvelle appliance, NE suivez PAS les instructions fournies dans ce guide. Contactez l'assistance clientèle de RSA.

Si vous disposez d'un DAC avec des données préexistantes et que vous tentez d'exécuter le script dans ces instructions, le script peut échouer ou il peut efface toutes les données existantes sur le DAC et créer tous les disques virtuels, les volumes logiques et la structure de répertoire nécessaires.

Note: Lors de l'affichage d'un guide imprimé, n'oubliez pas qu'une version plus récente peut être disponible en ligne sur le site **sadocs.emc.com/fr-fr**. Ce guide est disponible dans l'aide en ligne de Security Analytics sous Guides de configuration matérielle.

Last Modified: August 10 2016, 9:33AM

RSA

Description matérielle du DAC

Présentation

Cette rubrique est une description générale du périphérique de stockage Direct-Attached Capacity (DAC) de 15 disques Security Analytics.

Description matérielle

Le DAC de Security Analytics est un boîtier DAE optimisé par EMC^2. Le DAC est utilisé pour étendre le stockage utile sur un Decoder, un Log Decoder, un Concentrator, un Archiver ou une appliance hybride de la gamme 5.

Introduction

L'appliance DAC RSA Security Analytics est fournie avec le logiciel DAC installé. La configuration initiale d'un DAC sur votre réseau comprend ces étapes :

1. Vérifiez les exigences relatives au site et les informations de sécurité.
2. Installez le DAC.

Contenu de l'emballage

Reportez-vous à la documentation EMC^2 incluse avec le DAC.

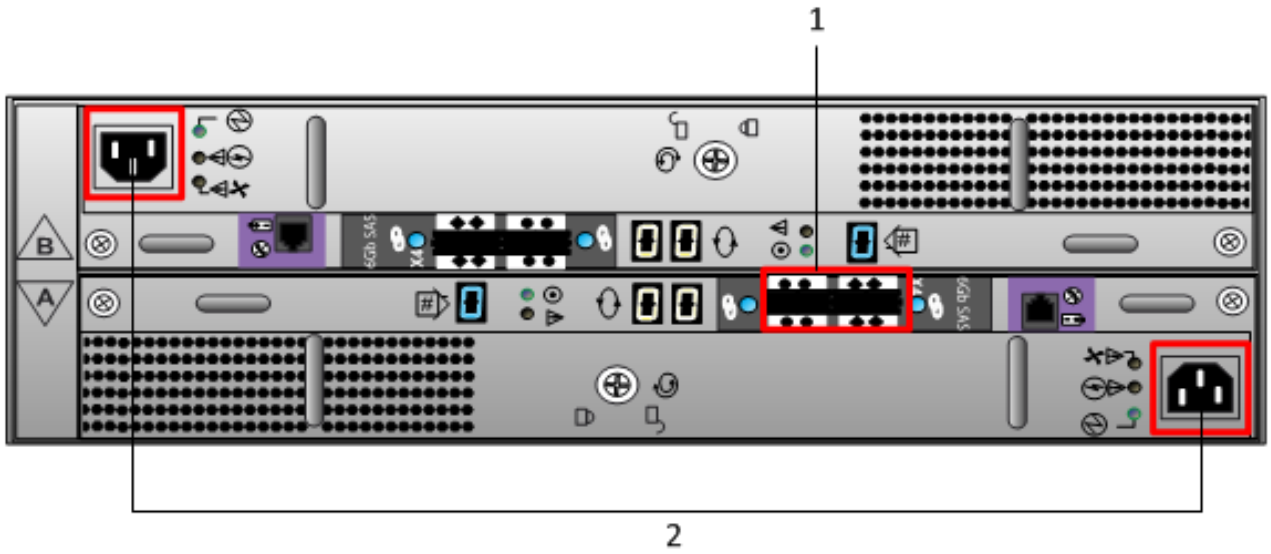
Note: Le DAC est muni de deux câbles SAS. Vous n'avez besoin que d'un câble pour connecter le DAC à l'appliance. Le second câble SAS est un câble de rechange.

Matériel fourni par le client

Vous n'avez pas besoin de fournir de matériel.

Last Modified: August 10 2016, 9:33AM

Vue arrière du DAC



Clé	Description
1	Ports SAS. Chaque jeu de ports a un port d'extension et un port principal. Dans chaque jeu, le port principal est plus proche du centre du châssis.
2	Connexion de l'alimentation

Last Modified: August 10 2016, 9:33AM

Installation du DAC

Présentation

Cette section explique comment installer un DAC de 15 disques sur les appliances Decoder, Log Decoder, Concentrator, Archiver et les appliances hybrides de la gamme 5 (paquet).

Conditions préalables

Assurez-vous que vous disposez du logiciel requis suivant :

- `rsa-sa-tools-10.5.1.0.82-1.el6.noarch.rpm` ou une version plus récente qui contient le script nécessairepour configurer le stockage.

Ce RPM est mis à jour chaque trimestre. Veuillez contacter l'assistance clientèle de RSA pour obtenir la version la plus récente.

⚠ **Caution:** Si vous ajoutez un DAC existant à une nouvelle appliance, NE suivez PAS les instructions fournies dans ce guide. Contactez l'assistance clientèle de RSA.

Si vous disposez d'un DAC avec des données préexistantes et que vous tentez d'exécuter le script dans ces instructions, le script peut échouer ou il peut efface toutes les données existantes sur le DAC et créer tous les disques virtuels, les volumes logiques et la structure de répertoire nécessaires.

Introduction

Le tableau suivant contient les instructions d'installation résumées pour les différents déploiements et les procédures détaillées se trouvent dans les sous-sections individuelles. Les scénarios de déploiement sont les suivants :

- Plusieurs DAC : dans un déploiement d'Archiver, de Log Decoder, de Decoder (paquet) et de Concentrator.
- Un seul DAC dans un déploiement hybride.

Last Modified: August 10 2016, 9:33AM

Procédure générale

Ce tableau résume les étapes des divers scénarios de déploiement.

Scénario de déploiement	Tâches
Concentrator, Archiver, Decoder et Log Decoder (Plusieurs DAC)	1. Connectez les DAC à l'appliance avant de démarrer l'appliance, comme décrit dans Connecter des DAC à une appliance de Concentrator, d'Archiver, de Decoder ou de Log Decoder. 2. Exécutez le script `NwArrayConfig.py`, comme décrit dans Exécuter les scripts d'installation DAC sur le paquet Decoder, Log Decoder, Concentrator ou Archiver. 3. Redémarrez le service, comme décrit dans Redémarrer le service. 4. Octroyez une licence pour l'appliance (si elle n'en a pas déjà une). Reportez-vous au *Guide d'octroi de licence Security Analytics* disponible via l'option **Aide** Security Analytics et au site sadocs.emc.com/fr-fr pour obtenir des instructions sur l'octroi de licence d'appliances.
Hybride	1. Connectez le DAC à l'appliance avant de démarrer l'appliance, comme décrit dans Connexion d'un DAC à une appliance hybride. 2. Exécutez le script `NwArrayConfig.py`, comme décrit dans Exécuter les scripts d'installation DAC sur une appliance hybride. 3. Redémarrez le service, comme décrit dans Redémarrer le service.

Last Modified: August 10 2016, 9:33AM

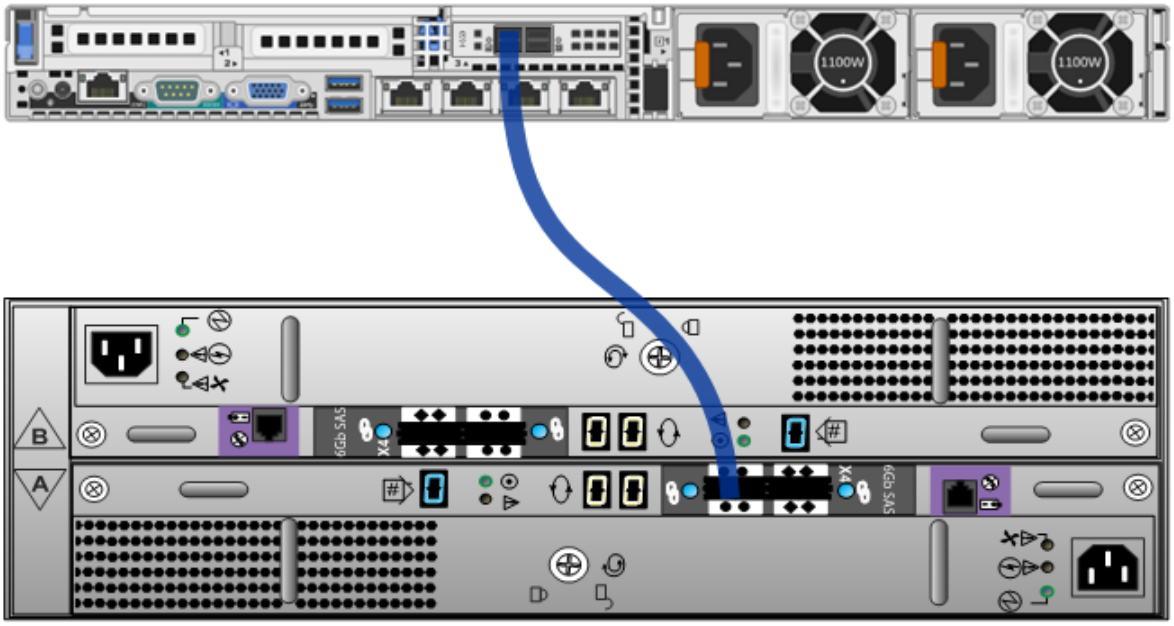
Connecter les DAC à une appliance de Concentrator, d'Archiver, de Decoder ou de Log Decoder

Vous pouvez connecter un ou plusieurs DAC à une appliance de Concentrator, d'Archiver, de Decoder ou de Log Decoder de la gamme 5. Vous pouvez uniquement ajouter quatre DAC par port pour un total de huit DAC par contrôleur RADI PERC H830.

Note: Deux câbles SAS sont fournis avec le DAC. Vous n'avez besoin que d'un câble pour connecter le DAC à l'appliance. **Les appliances de la gamme 4 et de la gamme 5 nécessitent différents câbles.** Utilisez le câble avec le port mini-SAS pour une connexion à une appliance de la gamme 5. L'autre câble vous permet de vous connecter à une appliance de la gamme 4.

1. Connectez une extrémité du câble SAS au port **gauche** du contrôleur RAID à l'arrière de l'appliance Security Analytics Concentrator, Archiver, Decoder ou Log Decoder de la gamme 5.

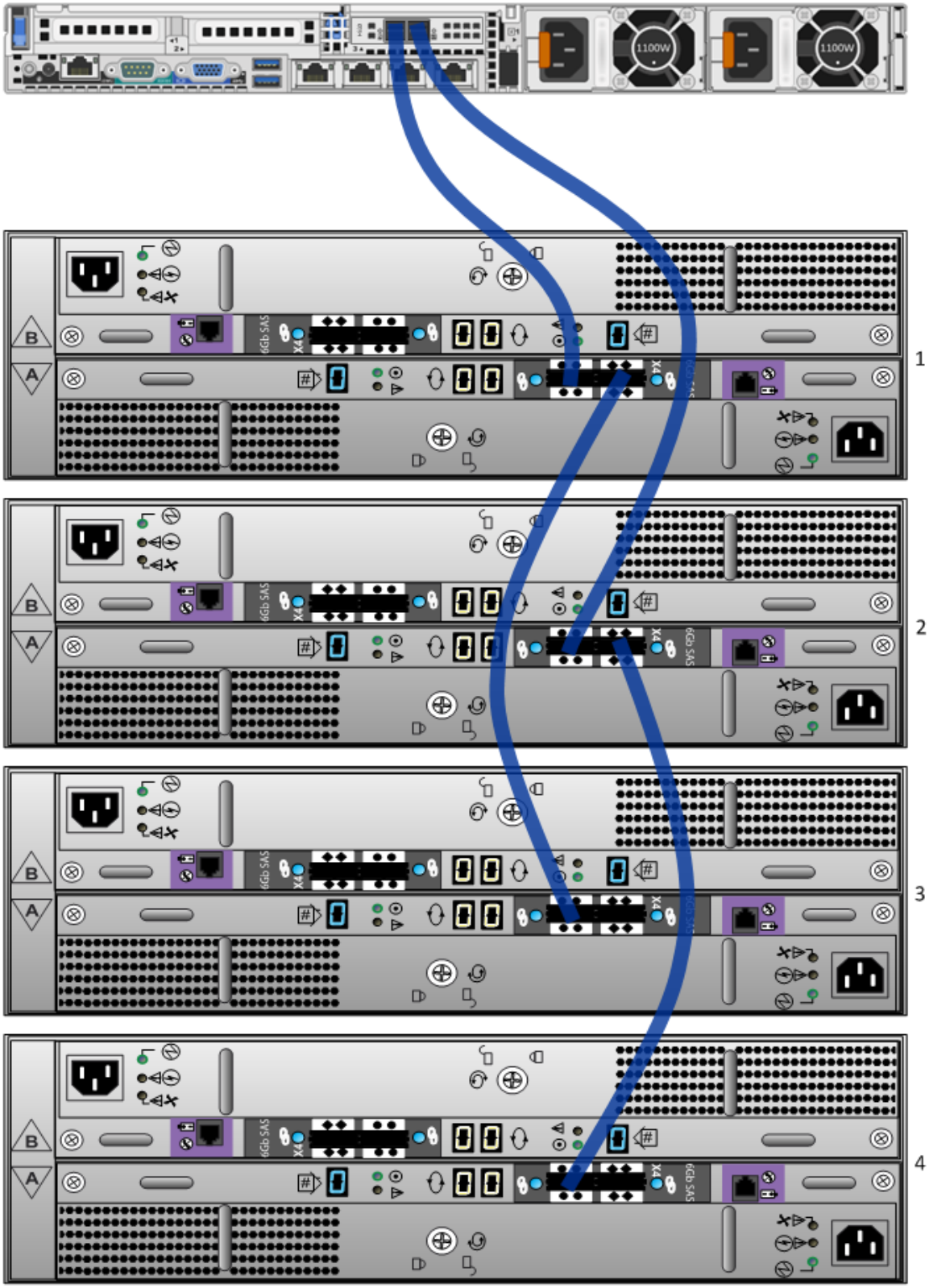
2. Connectez l'autre extrémité du câble SAS au DAC.
   Lorsque vous connectez le premier DAC au contrôleur RAID, assurez-vous d'insérer le câble dans le **port SAS principal** sur le DAC comme indiqué dans la figure suivante.



3. Lorsque vous connectez au moins deux DAC au contrôleur RAID, assurez-vous de ce qui suit :
   a. Connectez le port **principal** du premier DAC au port gauche du contrôleur RAID du Decoder.
   b. Connectez le port **principal** du deuxième DAC au port droit du contrôleur RAID du Decoder.
   c. Connectez le port **principal** au troisième DAC du port **secondaire**du premier DAC.
   d. Connectez le port **principal** au quatrième DAC au port **secondaire** du deuxième DAC.
   e. Continuez avec ce modèle jusqu'à un total de huit DAC par contrôleur RAID PERC H830.

Last Modified: August 10 2016, 9:33AM

La figure suivante indique comment connecter plusieurs DAC.



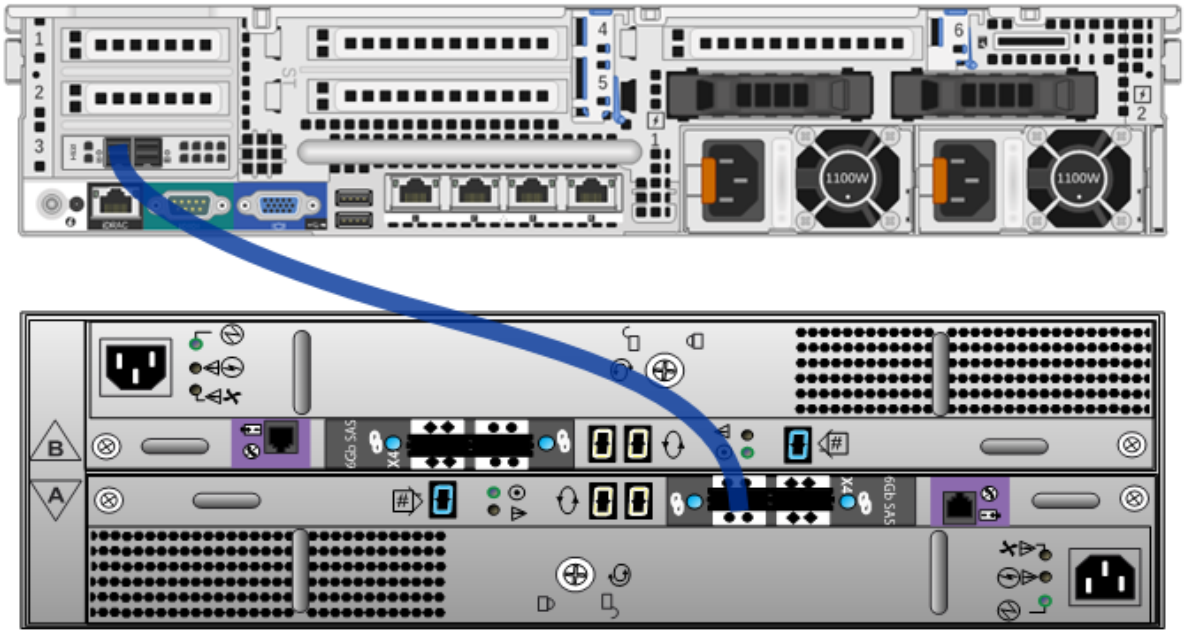
Connecter un DAC à une appliance hybride

Vous pouvez uniquement connecter un DAC à une appliance hybride de la gamme 5.

Note: Deux câbles SAS sont fournis avec le DAC. Vous n'avez besoin que d'un câble pour connecter le DAC à l'appliance. **Les appliances de la gamme 4 et de la gamme 5 nécessitent différents câbles.** Utilisez le câble avec le port mini-SAS pour une connexion à une appliance de la gamme 5. L'autre câble vous permet de vous connecter à une appliance de la gamme 4.

1. Connectez une extrémité du câble SAS au port **gauche** du contrôleur RAID à l'arrière de l'appliance hybride Security Analytics de la gamme 5.

2. Connectez l'autre extrémité du câble SAS au DAC.
   Lorsque vous connectez le premier DAC au contrôleur RAID, assurez-vous d'insérer le câble dans le **port SAS principal** sur le DAC comme indiqué dans la figure suivante.



Exécuter les scripts d'installation du DAC sur le Decoder, Log Decoder, Concentrator ou Archiver

1. Connectez-vous en tant qu'utilisateur `racine` et vérifiez que le package **rsa-sa-tools** est installé en exécutant la commande suivante :
   `rpm -qa | grep sa-tools`
   Si le package n'est pas installé, contactez l'assistance RSA pour obtenir une copie du RPM et l'installer.
2. Changez le répertoire pour le répertoire de base RPM rsa-sa-tools :
   `cd /opt/rsa/saTools`

Last Modified: August 10 2016, 9:33AM

3. Exécutez la commande suivante :
   `nwraidutil.pl | more`
4. Vérifiez les résultats pour vous assurer qu'il n'y a aucune configuration externe et aucun disque avec l'état `Unconfigured(Bad)` sur les disques du DAC. Si l'une des conditions est vraie, résolvez-la avant d'exécuter le script.
5. Exécutez le script NwArrayConfig.py à l'aide de la chaîne de commande suivante :
   `./NwArrayConfig.py`
   Ce script permet de découvrir tous les DAC disponibles ; crée tous les disques virtuels, les volumes logiques et la structure de répertoires nécessaires et écrit les messages de débogage dans **arrayCfg.log**.
6. Une fois l'exécution du script terminée, si vous ne le n'avez pas déjà fait, ajoutez l'appliance à l'aide de Security Analytics Administration et octroyez une licence aux services Decoder, Log Decoder, Concentrator et Archiver.
7. Vérifiez les résultats :
   a. Assurez-vous que le script n'a pas généré d'erreurs en consultant le fichier **arrayCfg.log**.
   b. Exécutez la chaîne de commande suivante pour vérifier les nouvelles tailles des bases de données :
      `df -Ph|awk '/(concentrator|decoder|archiver|Filesystem)/ {printf("%-64s %4s\n",$6,$2)}'`
      Voici un exemple des résultats qui s'affichent :

      ```
      Monté                                                          Taille
      /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. Assurez-vous qu'il existe une entrée pour chaque DAC ajouté. Un seul `packetdb#`, `metadb#` et `sessiondb#` est créé pour chaque DAC, où `#` est le nombre associé au DAC dans l'ordre dans lequel il a été ajouté. Pour la premier DAC que vous ajoutez, `#` est vide et aucun nombre n'est ajouté. `0` est ajouté au deuxième DAC que vous ajoutez. Par exemple, les entrées du premier DAC sont `metadb`, `sessiondb` et`packetdb`. Les entrées du deuxième DAC sont `metadb0`, `sessiondb0` et`packetdb0`.
      Vérifiez que la taille répertoriée pour `/var/netwitness/decoder/packetdb#` est ce que vous attendez avec les baies de stockage étendues rattachées. **Notez cette valeur** pour pouvoir la vérifier dans l'interface de Security Analytics.
   d. Connectez-vous à Security Analytics et dans le menu Security Analytics sélectionnez **Administration > Services**.
      La vue Services Administration s'affiche.
   e. Sélectionnez le Decoder ou Log Decoder et sélectionnez  **> Vue > Découvrir**.
   f. Développez le dossier de la **base de données** et sélectionnez le dossier **config**.
   g. Examinez le noeud **packet.dir** et étendez-le entièrement. Veillez à ce qu'il existe une entrée pour chaque DAC ajouté et que la taille du `packetdb` pour chaque est comme suit :
      `/var/netwitness/decoder/packetdb#/packetdb==<n>`
      où `<n>` est égal à 95 % de la taille du nouveau stockage en téraoctets. Cela doit correspondre à 95 % du résultat renvoyé par la commande `df -Ph` exécutée précédemment pour `/var/netwitness decoder/packetdb#`
   h. Suivez les étapes 7 e-g et vérifiez le nœud **meta.dir** sur le Concentrator, ainsi que le nœud **database.dir** sur l'Archiver. .

Exécuter les scripts d'installation du DAC sur une appliance hybride

1. Connectez-vous en tant qu'utilisateur `racine` et vérifiez que le package **rsa-sa-tools** est installé en exécutant la commande suivante :
   `rpm -qa | grep sa-tools`
   Si le package n'est pas installé, contactez l'assistance RSA pour obtenir une copie du RPM et l'installer.
2. Changez le répertoire pour le répertoire de base RPM rsa-sa-tools :
   `cd /opt/rsa/saTools`
3. Exécutez la commande suivante :
   `nwraidutil.pl | more`
4. Vérifiez les résultats pour vous assurer qu'il n'y a aucune configuration externe et aucun disque avec l'état `Unconfigured(Bad)` sur les disques du DAC. Si l'une des conditions est vraie, résolvez-la avant d'exécuter le script.
5. Vérifiez les volumes avant d'exécuter le script. Pour vous assurer qu'il n'y a aucune configuration externe ou aucun disque avec l'état `Unconfigured(bad)` sur les disques du DAC, entrez la commande suivante :
   `df -Ph|awk '/(concentrator|decoder|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'`
   Voici un exemple des résultats qui s'affichent :

   ```
   Monté                                              Taille
   /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. Pour exécuter le script `NwArrayConfig.py`, saisissez la commande suivante :
   `./NwArrayConfig.py --drives <N>`
   où `<N>` est le nombre de disques à attribuer au service Concentrator. Par défaut `<N>` est `3`. S'il s'agit d'un Log hybride, RSA recommande l'utilisation de la valeur `7` pour allouer plus efficacement le stockage entre les deux services. Tous les messages sont consignés dans `./arrayCfg.log`.
7. Vérifiez les résultats :
   a. Assurez-vous que le script n'a pas entraîné d'erreurs.
   b. Saisissez la commande suivante pour vérifier les nouvelles tailles des bases de données :
      `df -Ph|awk '/(concentrator|decoder|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'`
      Voici un exemple des résultats qui s'affichent :

      ```
      Monté                                              Taille
      /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: August 10 2016, 9:33AM

```
/var/netwitness/concentrator/sessiondb0              373G
/var/netwitness/concentrator/metadb0                 3,3T
/var/netwitness/logdecoder/packetdb0                 19T
```

c. Assurez-vous qu'il existe une entrée pour le DAC ajouté. Un seul `packetdb0`,`metadb0` et `sessiondb0` est créé pour le DAC ajouté. Vérifiez que la taille répertoriée pour `/var/netwitness/decoder/packetdb0` correspond à peu près à ce que vous attendez avec les baies de stockage étendues attachées. **Notez cette valeur** afin de pouvoir la vérifier dans l'interface Security Analytics.

d. Connectez-vous à Security Analytics et dans le menu Security Analytics sélectionnez **Administration** > **Services**.
La vue Services Administration s'affiche.

e. Sélectionnez le Decoder ou Log Decoder et sélectionnez  **> Vue** > **Découvrir**.

f. Développez le dossier de la base de données et sélectionnez le dossier config.

g. Examinez le nœud **packet.dir** et développez-le complètement. Vérifiez qu'il existe une entrée pour le DAC ajouté et que la taille de packetdb est comme suit :
`/var/netwitness/decoder/packetdb0/packetdb==<n>`
où `<n>` est égal à 95 % de la taille du nouveau stockage en To. Cela doit correspondre à 95 % du résultat renvoyé par la commande `df -Ph` exécutée précédemment pour `/var/netwitness/decoder/packetdb0`

h. Suivez les étapes 7 e-g et vérifiez le noeud **meta.dir** sur le Concentrator.

Redémarrer le service

Vous devez redémarrer le service Decoder, Log Decoder, Concentrator ou Archiver afin que le service puisse reconnaître le nouvel espace. Redémarrez le service Decoder, Log Decoder, Concentrator ou Archiver et assurez-vous qu'il est de nouveau ligne et commence la capture.

Last Modified: August 10 2016, 9:33AM