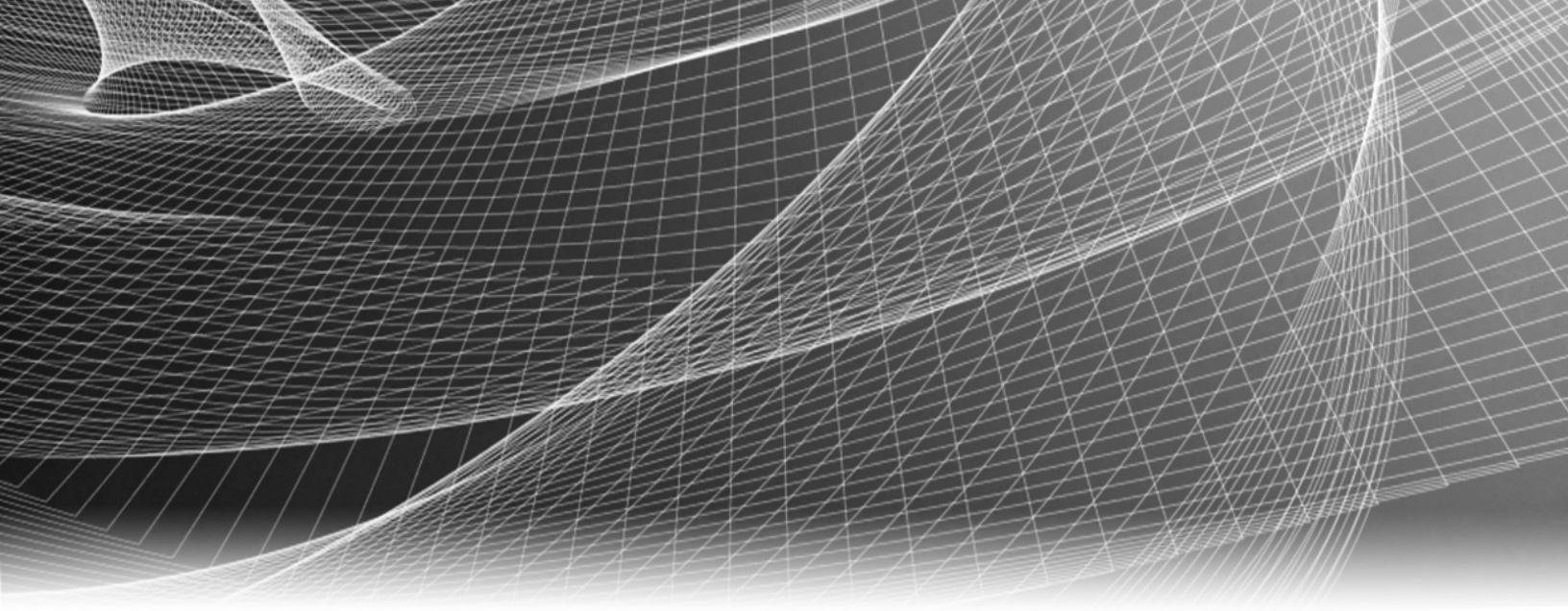


RSA Security Analytics

Guide de configuration du système Direct-Attached Capacity (DAC) de la gamme 4

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 Direct-Attached Capacity (DAC) de la gamme 4

RSA

Guide de configuration du système Direct-Attached Capacity (DAC) de la gamme 4

Présentation

Ce document fournit des instructions pour installer un DAC de 15 disques de la gamme 4 sur les appliances Series 4 Decoder, Series 4 Concentrator, Series 4 Archiver, hybrides de la gamme 4 et tout-en-un de la gamme 4.

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.

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

Description matérielle du DAC

Présentation

Cette rubrique est une description générale du périphérique de stockage Direct-Attached Capacity (DAC) de 15 disques de la gamme 4 de 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 Concentrator, un Archiver, une appliance hybride ou tout-en-un de la gamme 4.

Introduction

L'appliance DAC de RSA Security Analytics de la gamme 4 est fourni 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.

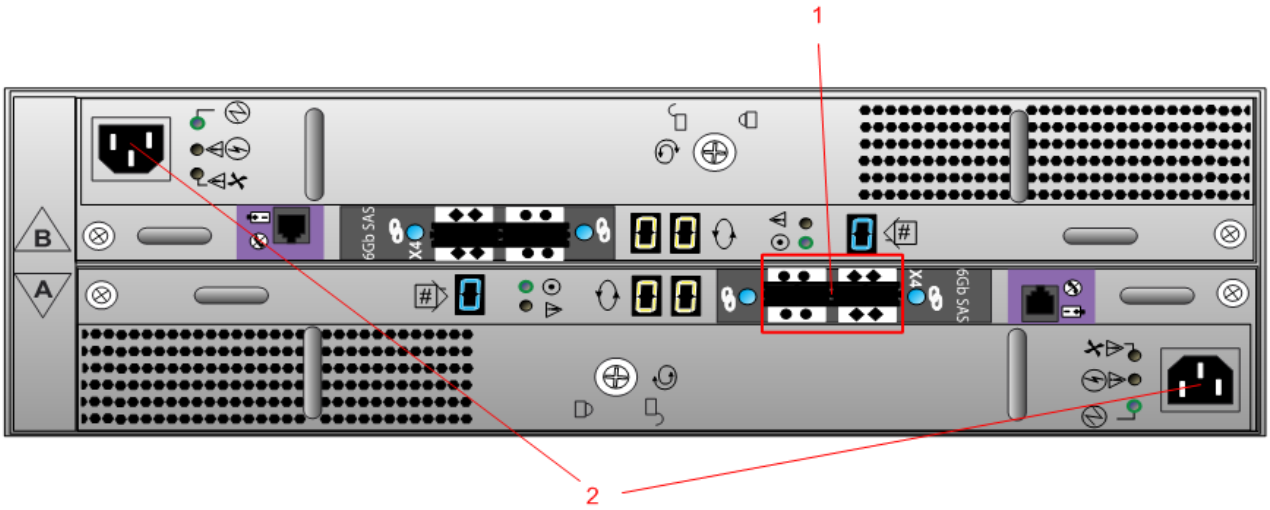
Note: Deux câbles SAS sont fournis avec le DAC. Vous n'avez besoin que d'un câble pour connecter le DAC à l'appliance. Le second câble SAS est un câble de rechange.

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

RSA

Installation du DAC

Présentation

Cette section explique comment installer le DAC de 15 disques de la gamme 4 sur le Decoder de la gamme 4, le Concentrator de la gamme 4, l'Archiver de la gamme 4, les appliances hybrides de la gamme 4 et celles tout-en-un de la gamme 4.

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 et de Concentrator.
- Un seul DAC dans le déploiement hybride.
- Un seul DAC pour le tout-en-un.

Conditions préalables

Assurez-vous que vous disposez du logiciel requis suivant :

- `arrayCfg-2.1.tgz` ou une version plus récente, nécessaire pour configurer le stockage. Ce script est mis à jour chaque trimestre et la version est représentée comme suit : `arrayCfg-<x.y-z>.tgz`, où `<x.y-z>` est le numéro de version. Veuillez contacter l'assistance clientèle de RSA pour obtenir la version la plus récente.
- `nwraidutil.pl`

Procédure générale

Ce tableau résume les étapes des divers scénarios de déploiement.

Scénario de déploiement	Tâches
Concentrator/ Archiver Decoder/ Log Decoder (Plusieurs DAC)	⚠ **Caution:** Assurez-vous que vous ne disposez PAS d'une licence pour le périphérique avant d'exécuter le script `NwArrayConfig.py` avec

Last Modified: August 10 2016, 9:33AM

<table>
<tr><th>Scénario de déploiement</th><th>Tâches</th></tr>
<tr><td></td><td>
l'option <code>--init</code>. Lorsque vous installez plusieurs DAC sur le Decoder de la gamme 4/4S, effectuez les étapes 1, 2 et 3 (câblage et initialisation du premier DAC), avant l'octroi de licence et le démarrage des services. Le fait de ne pas suivre les instructions peut entraîner des problèmes avec la structure des répertoires et une possible perte de données, ou vous devrez peut-être créer une nouvelle image de l'appliance.

Connectez le premier DAC à l'appliance avant de la mettre sous tension, comme décrit dans Connexion d'un DAC à une appliance.
Exécutez le script <code>NwArrayConfig.py</code> avec l'option <code>--init</code>, comme décrit dans Exécution des scripts d'installation du DAC sur le Decoder, Concentrator ou l'Archiver sur le Decoder ou Log Decoder.
Note: Si vous octroyez une licence au périphérique par inadvertance avant d'exécuter ce script, contactez l'assistance clientèle de RSA pour savoir comment restaurer les disques DAC à leur état d'origine.
Redémarrez le service, comme décrit dans Redémarrage du service Decoderou Concentrator.
Octroyez une licence à l'appliance. 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.
Avant de démarrer les appliances, connectez les DAC supplémentaires à l'appliance.
Exécutez les scripts d'installation du DAC avec l'option <code>--add</code> sur les DAC supplémentaires comme décrit à la section Exécution des scripts d'installation du DAC pour ajouter plusieurs baies de stockage.
Redémarrez le service, comme décrit dans Redémarrage du service Decoderou Concentrator.

</td></tr>
<tr><td>Hybride/AIO</td><td>

Connectez le DAC à l'appliance avant de démarrer l'appliance, comme décrit dans Connecter un DAC à une appliance.

Caution: Avant de configurer le stockage supplémentaire à une appliance hybride ou tout-en-un, assurez-vous que tous les services s'exécutant sur l'appliance hybride ou tout-en-un (par exemple, Concentrator, Decoder, Broker et Log Decoder) disposent d'une licence.
<ol start="2">
Octroyez une licence à l'appliance et aux services. 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. Exécutez le script <code>NwArrayConfig.py</code> avec l'option <code>--add</code>, comme décrit dans Ajouter un DAC à une appliance hybride ou tout-en-un.

</td></tr>
</table>

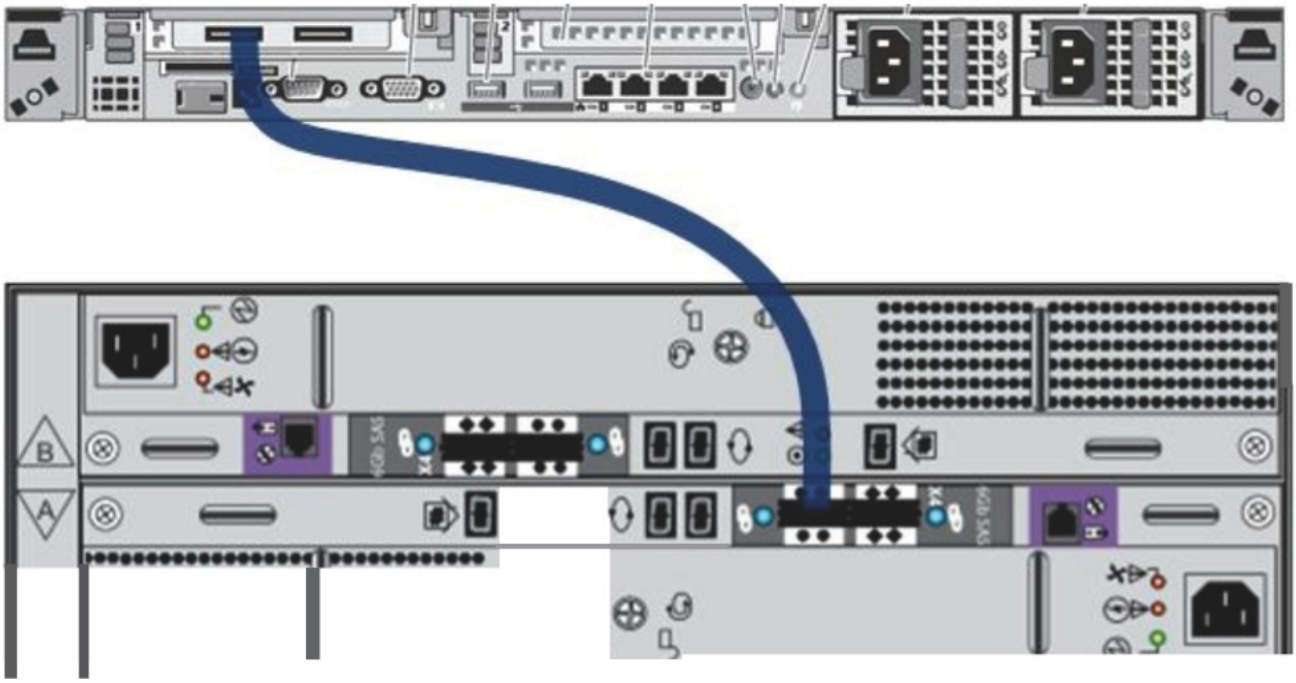
Connexion d'un DAC à une appliance

Les instructions de câblage s'appliquent à toutes les appliances répertoriées sous les types de déploiement : Concentrator, Decoder, Log Decoder, Archiver, hybride et tout-en-un.

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.

Pour connecter des DAC à une appliance :

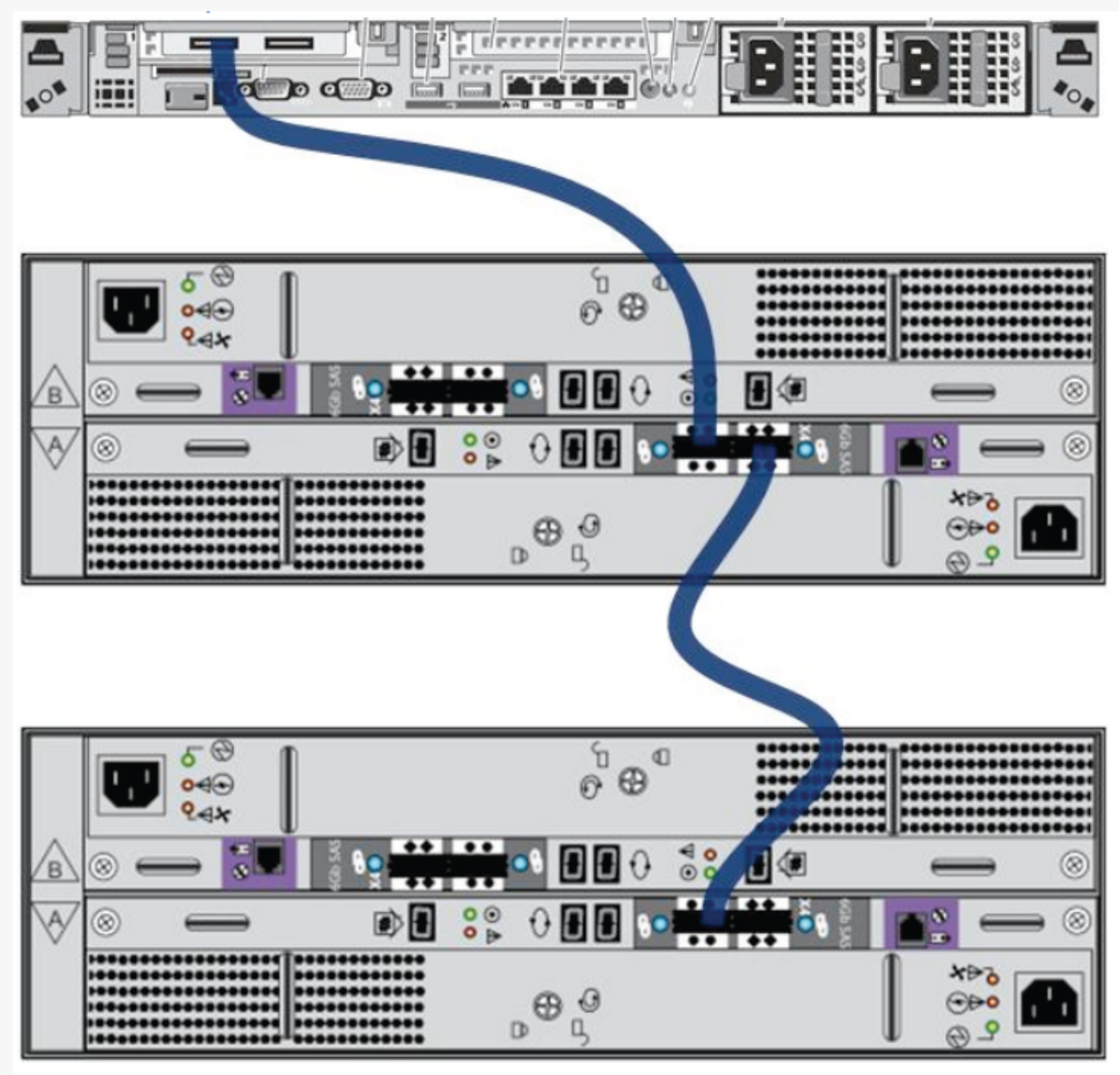
1. Connectez une extrémité du câble SAS au port **gauche** du contrôleur RAID à l'arrière de l'appliance Security Analytics S4. Si le script ne détecte pas les disques supplémentaires, vous devrez peut-être essayer l'autre port sur le contrôleur RAID.
2. Connectez l'autre extrémité du câble SAS au DAC.
   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 l'illustration suivante.



3. Lorsque vous connectez au moins deux DAC au contrôleur RAID, assurez-vous de ce qui suit :
   a. Insérez le câble du Decoder dans le port **principal** sur le premier DAC.
   b. Connectez le DAC suivant et ceux qui suivent à partir du port **secondaire** du premier DAC au port **principal** du DAC suivant.

   L'illustration suivante montre comment connecter plusieurs DAC.

Last Modified: August 10 2016, 9:33AM



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

Caution: Le Decoder, Concentrator ou l'Archiver ne doivent pas disposer d'une licence avant d'exécuter le script avec l'option `--action init`.

Pour exécuter les scripts d'installation DAC sur le Decoder ou Concentrator :

1. Copiez le fichier `arrayCfg-2.1.tgz` sur l'appliance dans `/root` via SCP.

Last Modified: August 10 2016, 9:33AM

2. Saisissez la commande suivante pour extraire le contenu :
   `tar -zxf arrayCfg-2.1.tgz`
3. Changez de répertoire pour le répertoire nouvellement créé `arrayCfg` :
   `cd arrayCfg`
4. Exécutez la commande suivante :
   `#nwraidutil.pl | more`
5. 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.
6. Exécutez le script `NwArrayConfig.py` à l'aide de la chaîne de commande suivante :
   `[root@CSO-S4Concentrator  ~]# ./NwArrayConfig.py --action init --service (decoder|concentrator/archiver)`
   Le script crée tous les disques virtuels, les volumes logiques et la structure de répertoires nécessaires et écrit les messages de débogage dans `arrayCfg.log.`
7. Une fois l'exécution du script terminée, ajoutez le périphérique à l'aide d'Administration Security Analytics et octroyez une licence au service Decoder, Concentrator et Archiver.
8. Vérifiez les résultats :
   a. Assurez-vous que le script n'a pas généré d'erreurs en consultant le fichier `arrayCfg.log`.
   b. Exécutez la 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/concentrator                           30G
/var/netwitness/concentrator/index                     1,1T
/var/netwitness/concentrator/sessiondb                 1013G
/var/netwitness/concentrator/metadb                    9,9T
```

Exécuter les scripts d'installation du DAC pour ajouter plus de baies de stockage

Pour exécuter les scripts d'installation du DAC sur le Decoder ou Concentrator pour ajouter davantage de stockage après l'initialisation :

1. Si le fichier `arrayCfg-2.1.tgz` n'a pas été copié sur l'appliance, copiez le fichier `arrayCfg-2.1.tgz` sur l'appliance dans `/root` via SCP.
2. Exécutez la commande suivante :
   `nwraidutil.pl | more.`
3. 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.
4. Vérifiez que :
   a. Decoder ou Concentrator dispose d'une licence avant d'exécuter le script `NwArrayConfig.py`.
   b. REST est activé sur le décodeur et sur le service de l'appliance.
5. Saisissez la chaîne de commande suivante pour passer au répertoire `/root/arrayCfg` :
   `cd /root/arrayCfg`
6. Saisissez la chaîne de commande suivante pour exécuter le script `NwArrayConfig.py` :
   `[root@CSO-DecoderSM ~]# ./NwArrayConfig.py --action add --service (concentrator|decoder|archiver)`
   Le script détecte le DAC supplémentaire suivant avec des disques disponibles. Il crée un disque logique pour le DAC et le configure de manière appropriée en fonction du type de service. Tous les messages sont consignés dans `./arrayCfg.log.`

Last Modified: August 10 2016, 9:33AM

7. Répétez les étapes 1 à 6 pour chaque DAC jusqu'à ce qu'ils soient tous configurés.
8. Vérifiez les résultats :
   a. Assurez-vous que le script n'a pas entraîné d'erreurs.
   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                   3,5T
   /var/netwitness/decoder/sessiondb                185G
   /var/netwitness/decoder/packetdb                 19T
   /var/netwitness/decoder/packetdb0                24T
   ```
   c. Assurez-vous qu'il existe une entrée pour chaque DAC ajouté. Il y aura un `/var/netwitness/decoder/packetdb#` pour chaque DAC créé. Vérifiez que la taille répertoriée pour `/var/netwitness/decoder/packetdb#` correspond à peu près à ce que vous attendez avec les baies de stockage étendues attachées. Notez ce numéro afin de pouvoir le vérifier dans l'interface Security Analytics.
   d. Connectez-vous à l'interface Security Analytics et dans le menu Security Analytics, sélectionnez **Administration** > **Périphériques**.
   La vue Périphériques d'administration s'affiche.
   e. Sélectionnez le Decoder ou Log Decoder et sélectionnez **Vue > Explorer** dans la barre d'outils.
   f. Développez le dossier de la **base de données** et sélectionnez le dossier **config**.
   g. Examinez le nœud **packet.dir** et développez-le complètement. Veillez à ce qu'il existe une entrée pour chaque DAC ajouté et que la taille de la `packetdb` pour chacun d'eux est la suivante :
   `/var/netwitness/decoder/packetdb#/packetdb==<n>`
   où `<n>` est égal à 95 % de la taille du nouveau périphérique en téraoctets. Cela doit correspondre à 95 % du résultat renvoyé par la commande `df -Ph` exécutée précédemment pour `/var/netwitness/decoder/packetdb#`

Redémarrez le service Decoder, Concentrator ou Archiver

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

Ajout d'un DAC à une appliance hybride ou tout-en-un

> ⚠ **Caution:** Avant d'ajouter plus de stockage à une appliance hybride ou tout-en-un, assurez-vous que tous les services s'exécutant sur l'appliance hybride ou tout-en-un (par exemple, Concentrator, Decoder, Broket et Log Decoder) disposent de licences. Reportez-vous au **Guide d'octoi de licence Security Analytics** disponible dans l'option **Aide** Security Analytics et au site sadocs.emc.com/fr-fr pour obtenir des instructions.

Pour ajouter un DAC à une appliance hybride ou tout-en-un :

1. Connectez le DAC à l'appliance (comme décrit sous **Connexion d'un DAC à une appliance**).
2. Copiez le fichier `arrayCfg-2.1.tgz` sur l'appliance dans `/root` via SCP.

Last Modified: August 10 2016, 9:33AM

3. Extrayez le contenu :
   `tar -zxf arrayCfg-2.1.tgz`
4. Changez de répertoire pour le répertoire nouvellement créé `arrayCfg` :
   `cd arrayCfg`
5. Saisissez les commandes suivantes pour afficher les disques configurés :
   ```
   #nwraidutil.pl | more
   #df -h
   ```
6. 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|archiver|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
   ```
7. Pour exécuter le script `NwArrayConfig.py`, saisissez la commande suivante :
   `[root@CSO-DecoderSM ~]# ./NwArrayConfig.py --action add --service hybrid --drives <N>`
   où `<N>` est le nombre de disques à attribuer à la partie concentrateur de l'appliance hybride. Par défaut `<N>` est `3`. Le script détecte le DAC supplémentaire suivant avec des disques disponibles. Il crée un disque logique pour chaque service hybride et les configure correctement, en fonction du type de service. Tous les messages sont consignés dans `./arrayCfg.log`.
8. Répétez les étapes 1 à 7 pour chaque DAC jusqu'à ce qu'ils soient tous configurés.
9. 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|archiver|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
      /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. Assurez-vous qu'il existe une entrée pour chaque DAC ajouté. Il y aura un seul `/var/netwitness/decoder/packetdb#` pour chaque DAC créé. Vérifiez que la taille répertoriée pour `/var/netwitness/decoder/packetdb#` est à peu près ce que vous attendiez avec les baies de stockage étendues rattachées. Notez ce numéro afin de pouvoir le vérifier dans l'interface Security Analytics.

d. Connectez-vous à l'interface Security Analytics et dans le menu Security Analytics, sélectionnez **Administration** > **Périphériques**.
La vue Périphériques d'administration s'affiche.

e. Sélectionnez le Decoder ou Log Decoder et sélectionnez **Vue** > **Explorer** dans la barre d'outils.

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 chaque DAC ajouté et que la taille de la packetdb pour chacun d'eux est comme suit :
`/var/netwitness/decoder/packetdb#/packetdb==<n>`
où `<n>` est égal à 95 % de la taille du nouveau périphérique en téraoctets. Cela doit correspondre à 95 % du résultat renvoyé par la commande `df -Ph` exécutée précédemment pour `/var/netwitness/decoder/packetdb#`

Last Modified: August 10 2016, 9:33AM