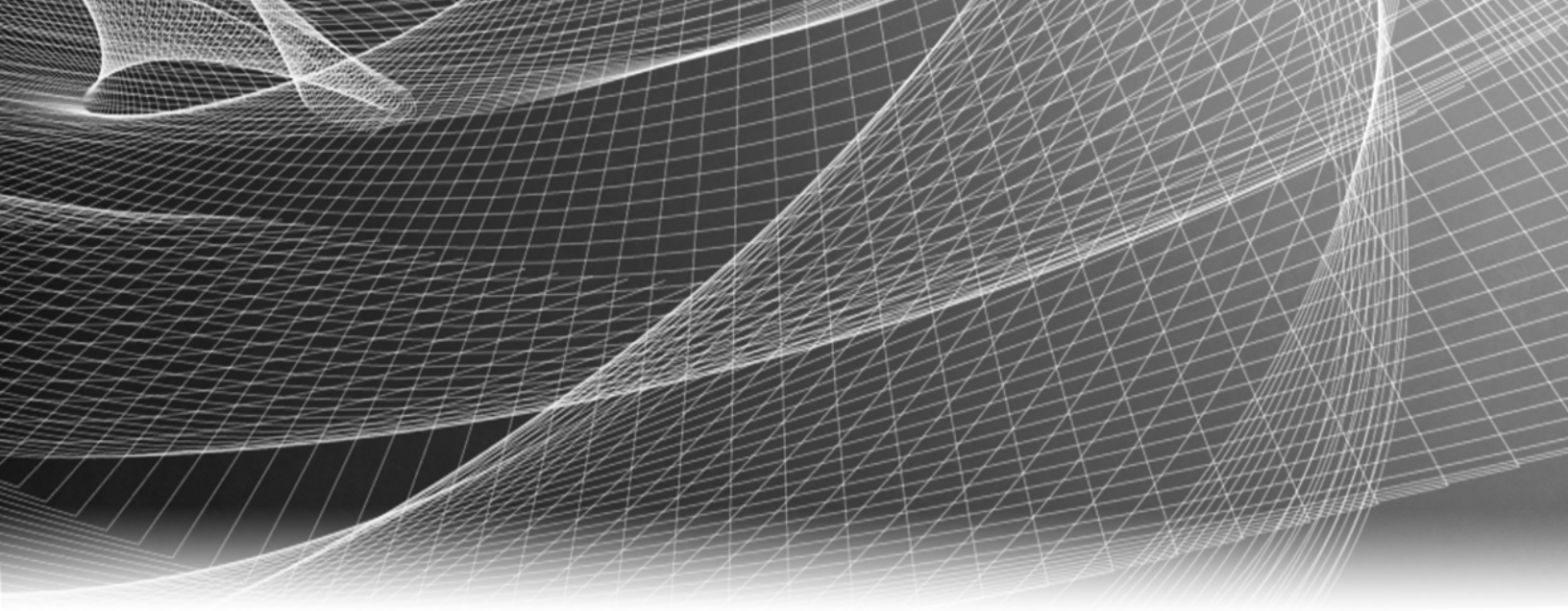


RSA Security Analytics

15-Drive DAC Series 5構成ガイド

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.

15-Drive DAC Series 5構成ガイド

RSA

15-Drive DAC Series 5構成ガイド

概要

このドキュメントでは、Series 5のDecoder、Log Decoder、Concentrator、Archiver、Hybridの各アプライアンスに15-Drive Direct-Attached Capacity（DAC）をインストールする手順について説明します。

本書について

このドキュメントは、ハードウェアの構成手順を説明する目的で記載されています。Security Analyticsソフトウェアの特定のリリースに依存するものではありません。新しいハードウェア専用です。既存のデータが存在するDACは対象外です。

⚠ **Caution:** 既存のDACを新しいアプライアンスに追加する場合は、このガイドの手順に従わないでください。詳細は、RSAにお問い合わせください。

DACに既存のデータが存在する場合、このガイドの手順でスクリプトを実行しようとすると、スクリプトが失敗するか、またはDAC上の既存のデータをすべて消去した後、必要な仮想ドライブ、論理ボリューム、ディレクトリ構造が作成される可能性があります。

Note: 印刷したガイドを参照している場合は、**sadocs.emc.com/ja-jp**に新しいバージョンが公開されている場合がありますのでご注意ください。このガイドは、Security Analyticsオンライン ヘルプのハードウェア構成ガイドからで参照可能です。

Last Modified: September 14 2016, 12:10PM

RSA

DACハードウェアの説明

概要

このトピックでは、Security Analytics 15-drive Direct-Attached Capacity（DAC）ストレージ デバイスの概要を説明します。

ハードウェアの説明

Security Analytics DACは、EMC^{2}が提供するドライブ アレイ エンクロージャです このDACは、Series 5のDecoder、Log Decoder、Concentrator、Archiver、Hybridの各アプライアンスで使用可能なストレージを拡張するために使用します。

はじめに

RSA Security Analytics DACアプライアンスには、出荷時にDACソフトウェアがインストールされています。ネットワーク上でDACの初期構成を行うには、次のステップを実行します。

1. 設置場所の要件および安全性に関する情報を確認します。
2. DACをインストールします。

パッケージの内容

DACに付属するEMC^2 のドキュメントを参照してください。

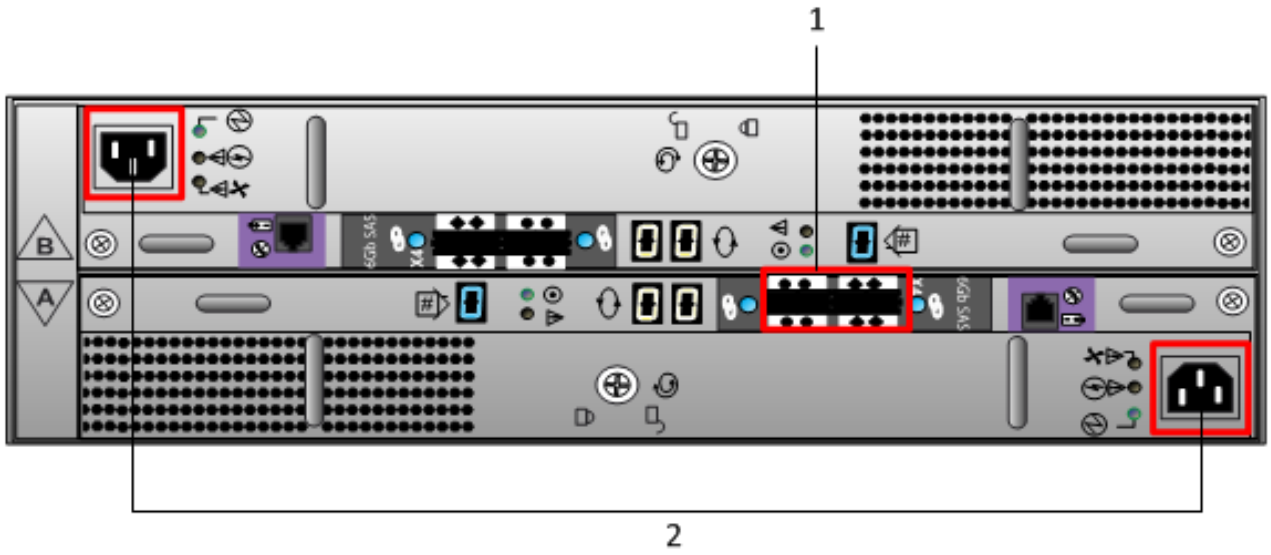
Note: DACには2本のSASケーブルが付属します。アプライアンスにDACを接続するのに必要なSASケーブルは1本のみです。2本目のSASケーブルはスペア ケーブルです。

お客様側で用意が必要な機材

お客様が機材を用意する必要はありません。

Last Modified: September 14 2016, 12:10PM

DACの背面



番号	説明
1	SASポート。各ポート セットには、拡張ポートとプライマリ ポートがあります。各セットにおいて、シャーシの中央側のポートがプライマリ ポートです。
2	電源入力接続

Last Modified: September 14 2016, 12:10PM

RSA

DACのインストール

概要

このトピックでは、Series 5のPacket Decoder、Log Decoder、Concentrator、Archiver、Hybridの各アプライアンスに15-drive DACをインストールする方法について説明します。

前提条件

次の必要なソフトウェアが利用可能であることを確認します。

- `rsa-sa ? ??? ? 10.5.1.0.82-1.el6.noarch.rpm`または、新しいストレージを構成する必要があるスクリプトを含みます。

このRPMは4か月ごとに更新されます。最新バージョンの入手については、RSAまでお問い合わせください。

> ⚠ **Caution:** 既存のDACを新しいアプライアンスに追加する場合は、このガイドの手順に従わないでください。詳細は、RSAにお問い合わせください。
>
> DACに既存のデータが存在する場合、このガイドの手順でスクリプトを実行しようとすると、スクリプトが失敗するか、またはDAC上の既存のデータをすべて消去した後、必要な仮想ドライブ、論理ボリューム、ディレクトリ構造が作成される可能性があります。

はじめに

次の表に、導入シナリオに応じたインストール手順の概要を示します。詳細な手順については、個別のサブセクションを参照してください。次の導入シナリオがあります。

- 複数のDACをConcentrator、Packet Decoder、Log Decoder、Archiverにインストール。
- 単一のDACをHybridにインストール。

Last Modified: September 14 2016, 12:10PM

手順の概要

次の表に、各導入シナリオの手順の概要を示します。

導入シナリオ	タスク
Concentrator、Archiver、Decoder、Log Decoder（複数のDAC）	1. アプライアンスの電源を入れる前に、「Concentrator、Archiver、Decoder、Log Decoderアプライアンスへの DACの接続」の手順に従って、アプライアンスにDACを接続します。 2. 「Packet Decoder、Log Decoder、Concentrator、Archiver上でのDACインストール スクリプトの実行」の手順に従って、`NwArrayConfig.py`スクリプトを実行します。 3. 「サービスの再起動」の手順に従ってサービスを再起動します。 4. アプライアンスにライセンスを付与します（まだライセンスを付与していない場合）。アプライアンスへのライセンス付与の手順については、Security Analyticsの**ヘルプ** オプションもしくはsadocs.emc.com/ja-jpにアクセスし、*Security Analytics ライセンス ガイド*を参照してください。
Hybrid	1. アプライアンスの電源を入れる前に、「Hybridアプライアンスへの DACの接続」の手順に従って、アプライアンスにDACを接続します。 2. 「Hybridアプライアンス上でのDACインストール スクリプトの実行」の手順に従って、`NwArrayConfig.py`スクリプトを実行します。 3. 「サービスの再起動」の手順に従ってサービスを再起動します。

Last Modified: September 14 2016, 12:10PM

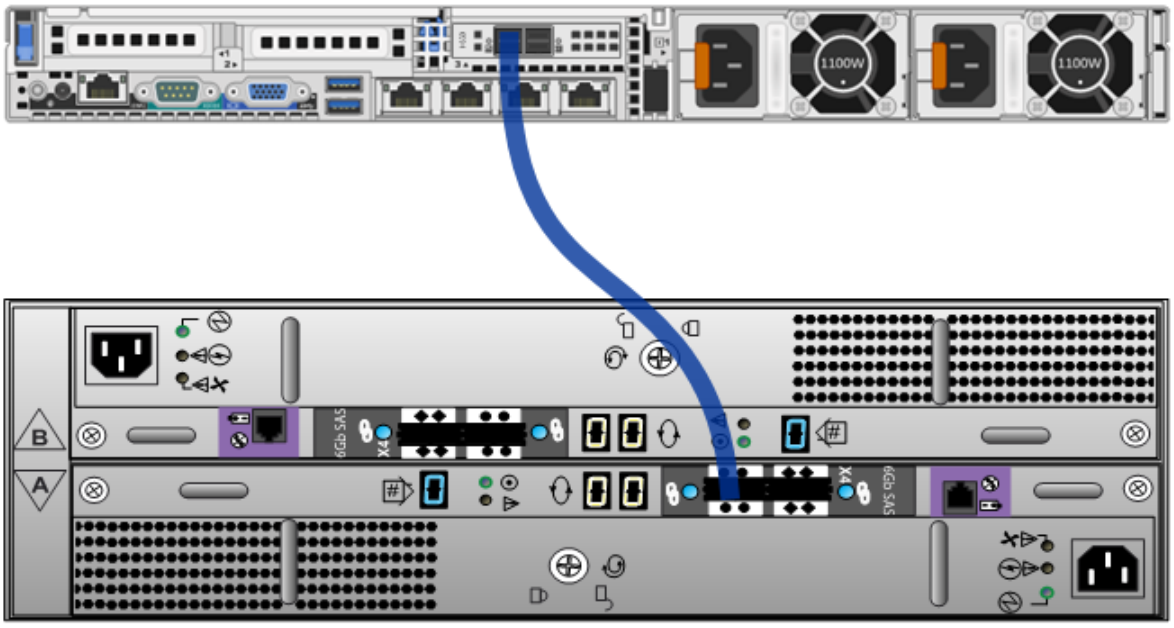
Concentrator、Archiver、Decoder、Log Decoderアプライアンスへの DACの接続

1つ以上のDACをSeries 5の Concentrator、Archiver、Decoder、Log Decoderアプライアンスに接続できます。1つのPERC H830 RAIDコントローラには、各ポートに最大4つ、合計8つのDACを追加できます。

Note: DACには2本のSASケーブルが付属します。アプライアンスにDACを接続するために必要なケーブルは1本のみです。**Series 4とSeries 5のアプライアンスでは必要なケーブルが異なります。**Series 5アプライアンスに接続するには、Mini-SASポートのケーブルを使用します。もう一方のケーブルは、Series 4アプライアンスに接続する時に使用します。

1. Security Analytics S5 Concentrator、Archiver、Decoder、Log Decoderアプライアンスの背面にあるRAIDコントローラの**左側**のポートにSASケーブルの一端を接続します。

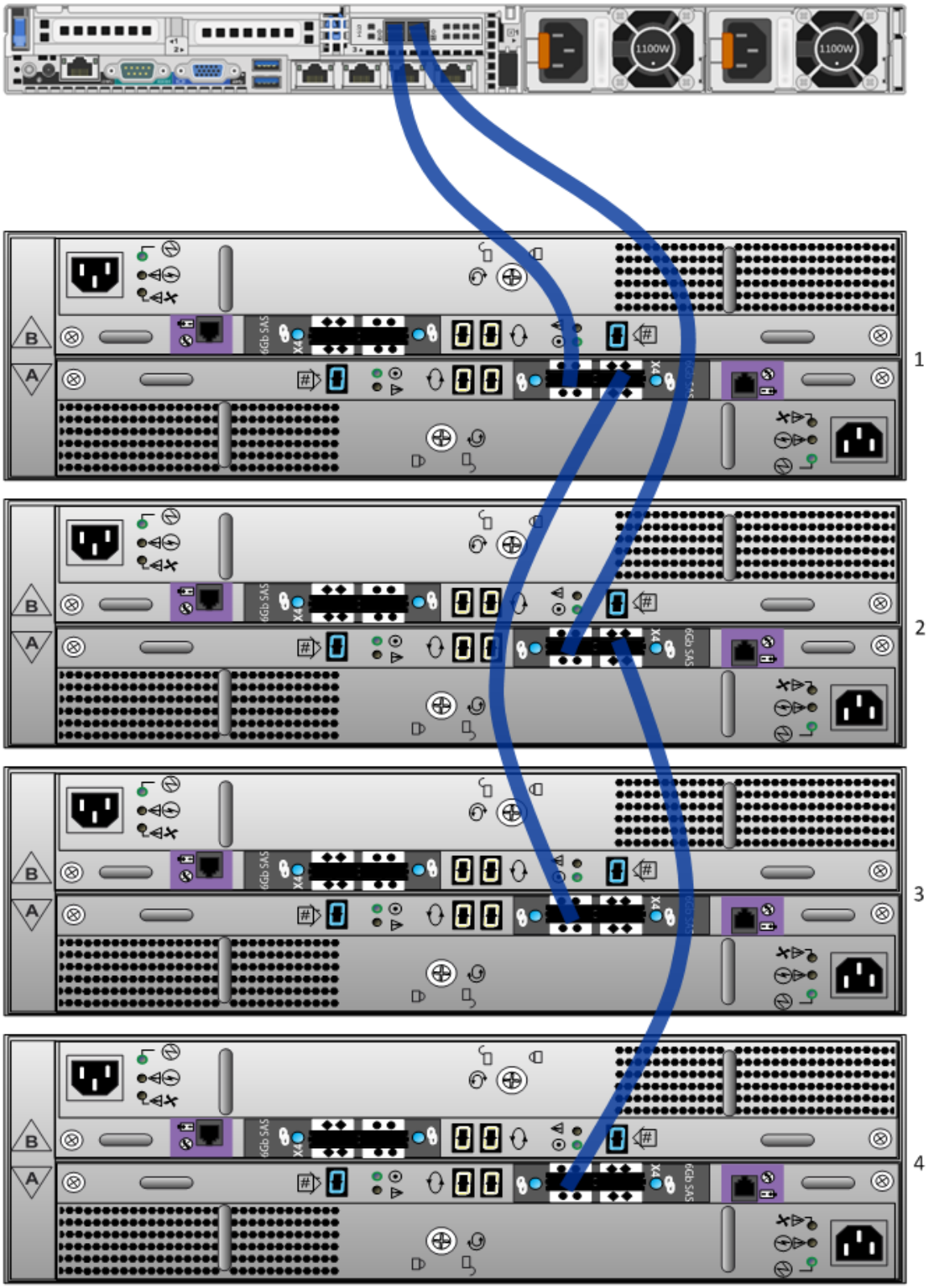
2. SASケーブルの他端をDACユニットに接続します。
   RAIDコントローラに最初のDACを接続する場合、次の図に示すように、DACの**プライマリSASポート**にケーブルを挿入します。



3. RAIDコントローラに複数のDACを接続する場合は、次の項目を確認します。
   a. 1つ目のDACの**プライマリ** ポートをDecoder RAIDコントローラの左側のポートに接続します。
   b. 2つ目のDACの**プライマリ** ポートをDecoder RAIDコントローラの右側のポートに接続します。
   c. 3つ目のDACの**プライマリ** ポートを1つ目のDACの**セカンダリ** ポートに接続します。
   d. 4つ目のDACの**プライマリ** ポートを2つ目のDACの**セカンダリ** ポートに接続します。
   e. このパターンを繰り返し、PERC H830 RAIDコントローラあたり最大8つのDACを接続できます。

Last Modified: September 14 2016, 12:10PM

次の図は、複数のDACを接続する方法を示しています。



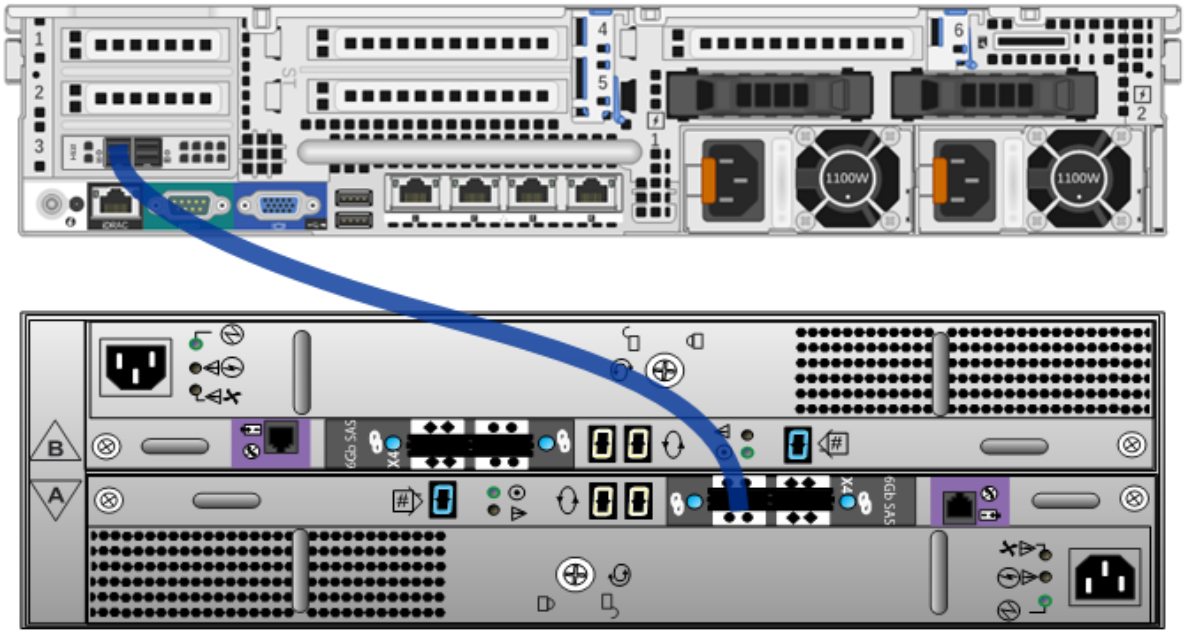
HybridアプライアンスへのDACの接続

Series 5 Hybridアプライアンスには、1つのDACしか接続できません。

Note: DACには2本のSASケーブルが付属します。アプライアンスにDACを接続するために必要なケーブルは1本のみです。**Series 4とSeries 5のアプライアンスでは必要なケーブルが異なります。**Series 5アプライアンスに接続するには、Mini-SASポートのケーブルを使用します。もう一方のケーブルは、Series 4アプライアンスに接続する時に使用します。

1. Security Analytics Series 5 Hybridアプライアンスの背面にあるRAIDコントローラの左側のポートにSASケーブルの一端を接続します。

2. SASケーブルの他端をDACユニットに接続します。
RAIDコントローラに最初のDACを接続する場合、次の図に示すように、DACの**プライマリSASポート**にケーブルを挿入します。



Decoder、Log Decoder、Concentrator、Archiver上でのDACインストール スクリプトの実行

1. `root`としてログインし、次のコマンドを実行して**rsa-sa-tools**パッケージがインストールされていることを確認します。
```
rpm -qa | grep sa-tools
```
パッケージがインストールされていない場合は、RSAサポートに連絡し、RPMを取得してインストールします。
2. rsa-sa-tools RPMのベース ディレクトリに移動します。
```
cd /opt/rsa/saTools
```


Last Modified: September 14 2016, 12:10PM

3. 次のコマンドを実行します。
   `nwraidutil.pl | more`
4. コマンドの実行結果をチェックし、DACドライブ上にForeignおよび`Unconfigured(Bad)`状態のドライブがないことを確認します。いずれかの状態が見つかった場合は、スクリプトを実行する前にそれらの問題を解消します。
5. 次のコマンドを使用して**NwArrayConfig.py**スクリプトを実行します。
   `./NwArrayConfig.py`
   スクリプトは、利用可能なすべてのDACを検出し、必要な仮想ドライブ、論理ボリューム、ディレクトリ構造を作成し、デバッグ メッセージを**arrayCfg.log**に書き込みます
6. スクリプトの実行を完了した後、まだ行っていない場合は、Security Analytics Administrationを使用してアプライアンスを追加し、Decoder、Log Decoder、Concentrator、Archiverの各サービスにライセンスを付与します。
7. 結果を確認します。
   a. **arrayCfg.log**ファイルを確認し、スクリプトによりエラーが発生しなかったことを確認します。
   b. 次のコマンドを実行し、データベースの新しいサイズを確認します。
      `df -Ph|awk '/(concentrator|decoder|archiver|Filesystem)/ {printf("%-64s %4s\n",$6,$2)}'`
      表示される結果の例を次に示します。

```
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. 追加した各DACのエントリが表示されることを確認します。各DACに個別の`packetdb#`、`metadb#`、`sessiondb#`が作成されます。ここで、`#`は追加した順に割り当てられるDACの番号です。最初に追加したDACでは、`#`は空白で番号は付加されません。2つ目に追加したDACでは`0`が付加されます。たとえば、最初に追加したDACのエントリは、`metadb`、`sessiondb`、`packetdb`となります。2つ目のDACのエントリは、`metadb0`、`sessiondb0`、`packetdb0`となります。`/var/netwitness/decoder/packetdb#`のサイズが、接続した拡張ストレージ アレイから想定されるサイズであることを確認します。**この値を書き留めて**、Security Analyticsインタフェースで確認します。
   d. Security Analyticsにログオンして、Security Analyticsメニューで、 **[Administration] > [サービス]** を選択します。
      [Administration] の [サービス] ビューが表示されます。
   e. [Decoder] または [Log Decoder] を選択し、  **> [表示] > [エクスプローラ]** を選択します。
   f. **database**フォルダを展開し、**config**フォルダを選択します。
   g. **packet.dir**ノードを見つけ、完全に展開します。追加した各DACに対応するエントリが存在し、それぞれの`packetdb`のサイズが以下のように表示されていることを確認します。
      `/var/netwitness/decoder/packetdb#/packetdb==<n>`
      ここで、`<n>`は新しいストレージのサイズの95%（TB単位）と等しくなります。この値は、前の手順で実行した`df -Ph`コマンドから返された`/var/netwitness/decoder/packetdb#`の結果値の95%である必要があります。
   h. ステップ7 e-gを実行し、Concentratorの**meta.dir**ノードとArchiverの**database.dir**ノードを確認します?

Hybridアプライアンス上でのDACインストール スクリプトの実行

1. rootとしてログインし、次のコマンドを実行して**rsa-sa-tools**パッケージがインストールされていることを確認します。
   ```
   rpm -qa | grep sa-tools
   ```
   パッケージがインストールされていない場合は、RSAサポートに連絡し、RPMを取得してインストールします。
2. rsa-sa-tools RPMのベース ディレクトリに移動します。
   ```
   cd /opt/rsa/saTools
   ```
3. 次のコマンドを実行します。
   ```
   nwraidutil.pl | more
   ```
4. コマンドの実行結果をチェックし、DACドライブ上にForeignおよびUnconfigured(Bad)状態のドライブがないことを確認します。いずれかの状態が見つかった場合は、スクリプトを実行する前にそれらの問題を解消します。
5. スクリプトを実行する前に、ボリュームをレビューします。次のコマンドを実行し、現在のデータベースの情報を確認します。
   ```
   df -Ph|awk '/(concentrator|decoder|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'
   ```
   表示される結果の例を次に示します。
   ```
   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. 次のコマンドを使用して、NwArrayConfig.pyスクリプトを実行します。
   ```
   ./NwArrayConfig.py --drives <N>
   ```
   ここで、<N>は、Concentratorサービスに割り当てられるドライブの数です。デフォルトでは、<N>は3です。Hybrid Logの場合、2つのサービスにストレージをより効率的に割り当てるため、7が推奨値です。すべてのメッセージが./arrayCfg.logに記録されます。
7. 結果を確認します。
   a. スクリプトでエラーが生成されなかったことを確認します。
   b. 次のコマンドを実行して、データベースの新しいサイズを確認します。
      ```
      df -Ph|awk '/(concentrator|decoder|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'
      ```
      表示される結果の例を次に示します。
      ```
      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
      ```


Last Modified: September 14 2016, 12:10PM

```
/var/netwitness/concentrator/metadb0                3.3T
/var/netwitness/logdecoder/packetdb0                19T
```

c. 追加したDACのエントリが表示されることを確認します。追加したDACの`packetdb0`、`metadb0`、`sessiondb0`が作成されます。`/var/netwitness/decoder/packetdb0`のサイズが、接続した拡張ストレージ アレイから想定されるサイズであることを確認します。Security Analyticsインタフェースでの確認のため、**この値をメモ**しておきます。

d. Security Analyticsにログインし、Security Analyticsメニューで [**Administration**] > [**サービス**] を選択します。
[Administration] の [サービス] ビューが表示されます。

e. [Decoder] または [Log Decoder] を選択し、  > [**表示**] > [**エクスプローラ**] を選択します。

f. **database**フォルダを展開し、**config**フォルダを選択します。

g. **packet.dir**ノードを見つけ、完全に展開します。追加したDACのエントリが存在し、packetdbのサイズが次のように表示されていることを確認します。
`/var/netwitness/decoder/packetdb0/packetdb==<n>`
ここで、`<n>`は新しいストレージのサイズの95% (TB単位) と等しくなります。この値は、前の手順で実行した`df -Ph`コマンドから返された`/var/netwitness/decoder/packetdb0`の結果値の95%である必要があります。

h. ステップ7 e-gを実行し、Concentratorの**meta.dir**ノードを確認します。

サービスの再起動

サービスが新しい領域を認識できるように、Decoder、Log Decoder、Concentrator、Archiverの各サービスを再起動する必要があります。Decoder、Log Decoder、Concentrator、Archiverの各サービスを再起動し、サービスがオンラインに戻り、収集を開始したことを確認します。

Last Modified: September 14 2016, 12:10PM