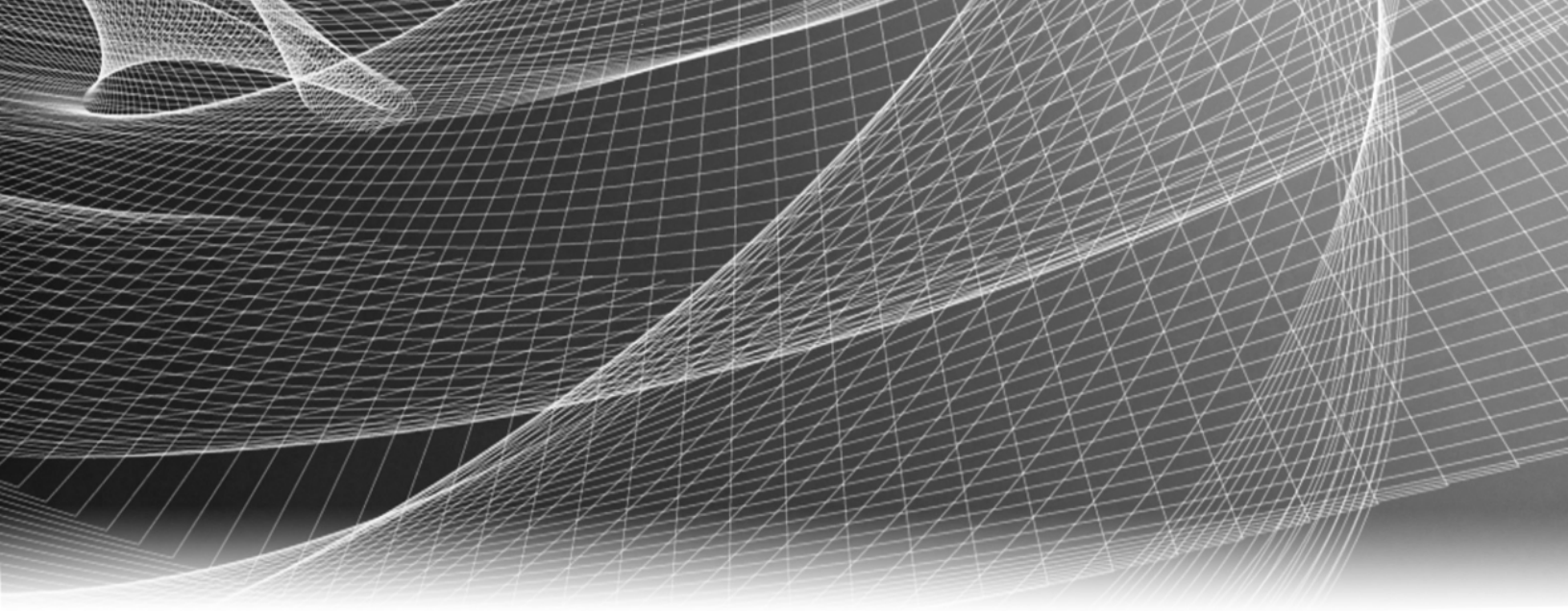


RSA Security Analytics

60-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.

60-Drive DAC Series 5構成ガイド

RSA

60-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、Archiverの各アプライアンスに60-drive 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。このドキュメントは、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、RSA 60-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

60-drive 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、Archiver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

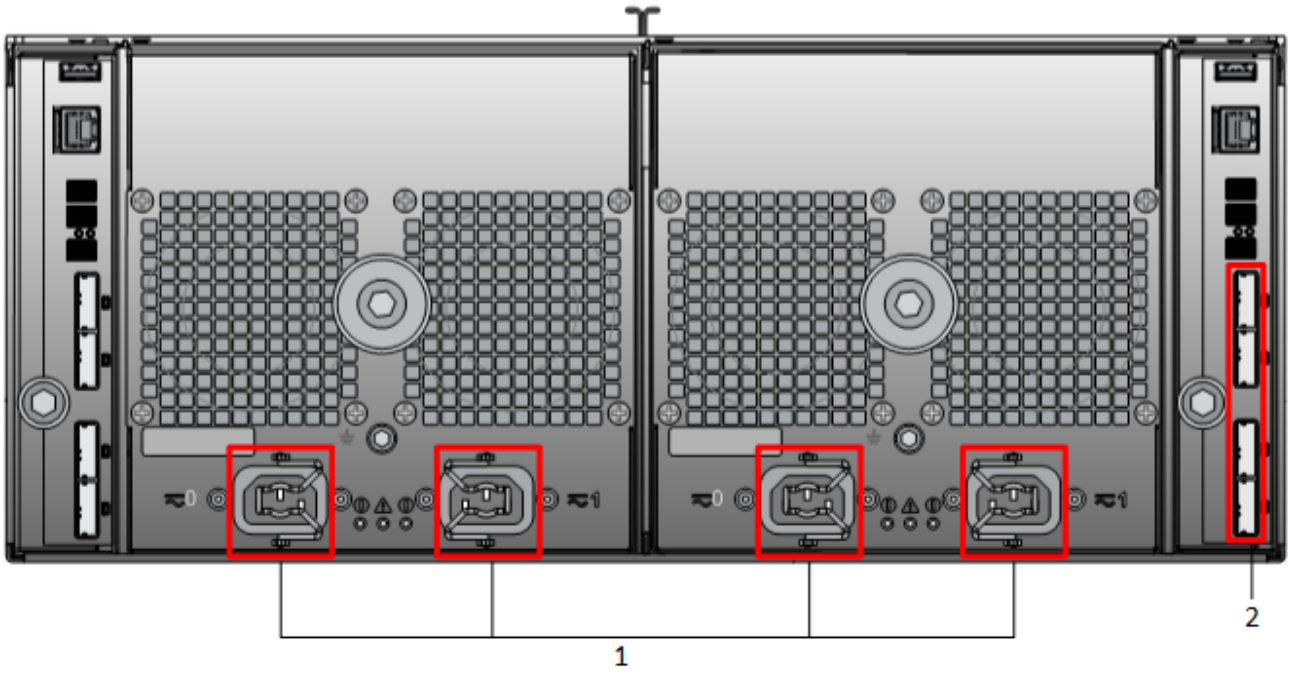
DACに付属するEMC^2 のドキュメントを参照してください。

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	電源入力接続
2	SASポート。 各ポート セットには、2個の拡張ポートと2個のプライマリ ポートがあります。各セットにおいて、シャーシの上側のポートがプライマリ ポートです。 **Note:** 60-drive DACをアプライアンスに接続する場合は、図の中でマークされた右側のSASポートのみを使用してください。

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、次のSeries 5アプライアンスに60-drive DACをインストールする方法について説明します。

- Decoder
- Log Decoder
- Archiver

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-tools-10.5.1.0.82-1.el6.noarch.rpm`以降。ストレージを構成するために必要なスクリプトが含まれます。

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。

Last Modified: September 14 2016, 12:10PM

手順の概要

次の表は、インストール手順の概要を示しています。

アプライアンス	タスク
Decoder、 Log Decoder、 Archiver	1. アプライアンスの電源を入れる前に、「アプライアンスへの60-Drive 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. 「Decoder、Log Decoder、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。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** オプションをクリックするか、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。

Last Modified: September 14 2016, 12:10PM

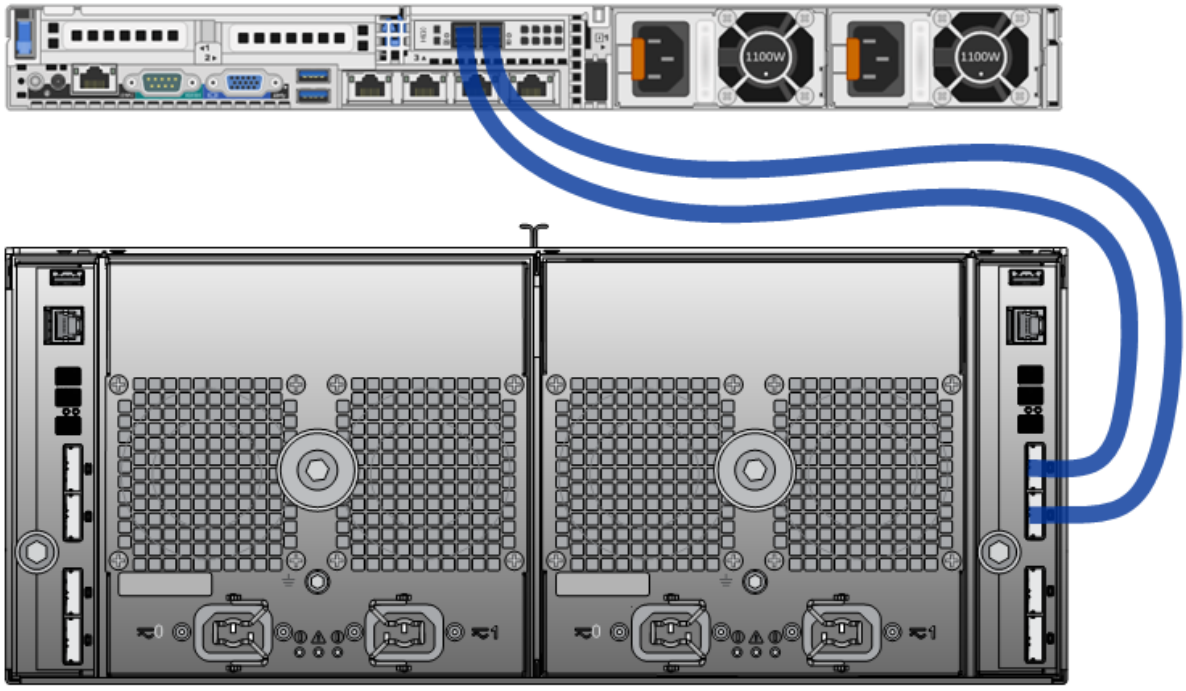
アプライアンスへの60-drive DACの接続

ここで紹介するケーブル接続手順は、Series 5 Decoder、Log Decoder、Archiverのすべてのアプライアンスに適用されます。

Note: 60-drive DACには4本のSASケーブルが付属します。このうちの2本のケーブルを使用して、次の図のように60-drive DACとアプライアンスを接続します。**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場合は、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場合に使用します。

60-drive DACをアプライアンスに接続するには、次の手順に従います。

1. Security Analytics Series 5 Archiver、Decoder、Log Decoderアプライアンスの背面にあるRAIDコントローラのポートに各SASケーブルの一端を接続します。
   スクリプト実行時に追加ドライブが検出されなかった場合、RAIDコントローラのもう一方のポートにケーブルを接続してみてください。
2. SASケーブルの他端を60-drive DACユニットに接続します。
   RAIDコントローラに60-drive DACを接続する場合、次の図に示すように、60-drive DACの**プライマリSASポート**にケーブルを接続します。



Last Modified: September 14 2016, 12:10PM

Decoder、Log Decoder、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`
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、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. 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 '/(decoder|logdecoder|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               746G
/var/netwitness/decoder/packetdb                 95T
/var/netwitness/decoder/sessiondb0              746G
/var/netwitness/decoder/metadb0                 6.6T
/var/netwitness/decoder/packetdb0                95T
```

7. スクリプトの実行を完了した後、Security Analytics Administrationを使用してアプライアンスを追加し、Decoder、Log Decoder、Archiverの各サービスにライセンスを付与します。

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、Archiverの各サービスを再起動する必要があります。

1. サービスを再起動します。
2. 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