

RSA Security Analytics

60-Drive DAC Series 4構成ガイド

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

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 4構成ガイド

• 60-Drive DAC Series 4構成ガイド	4
◦ DACハードウェアの説明	5
◦ DACのインストール	7



60-Drive DAC Series 4構成ガイド

概要

このドキュメントでは、Series 4 Decoder、Series 4 Log Decoder、Series 4 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。

Note: 印刷したガイドを参照している場合は、sadoes.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。



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、EMC²が提供するドライブ アレイ エンクロージャです。DACは、Series 4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。
-

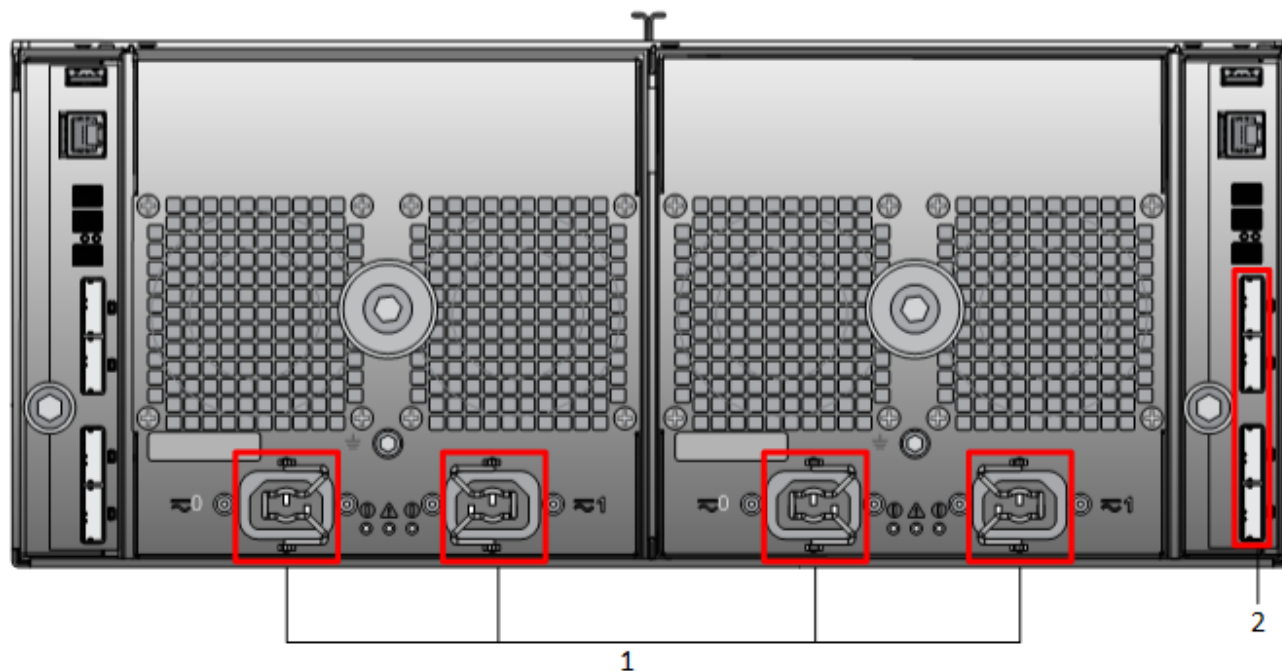
パッケージの内容

DACに付属するEMC²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。

DACの背面



番号	説明
1	電源入力接続
2	<p>SASポート。</p> <p>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、シャーシの上部に近いポートがプライマリ ポートです。</p> <p>Note: 60-drive DACをアプライアンスに接続する場合は、図の右側のマークされたSASポートのみを使用してください。</p>



DACのインストール

概要

このトピックでは、次のSeries 4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

はじめに

下の表に、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。

前提条件

ストレージを構成するために、`arrayCfg-2.1.tgz` (バージョン2.1以降) が必要です。このスクリプトは四半期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。

手順の概要

次の表に、導入手順の概要を示します。

アプライアンス	タスク
Decoder Log Decoder Archiver	<ol style="list-style-type: none"> 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DACの接続」に従って、アプライアンスにDACを接続します。 2. 「DecoderまたはArchiver上でのDACインストール スクリプトの実行」に従って、<code>NwArrayConfig.py</code>スクリプトを<code>--init</code>オプション付きで実行します。 4. 「Decoderサービスの再起動」に従ってサービスを再起動します。 5. アプライアンスの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、sadoes.emc.com/ja-jpから参照可能な「Security Analyticsライセンスガイド」を参照してください。

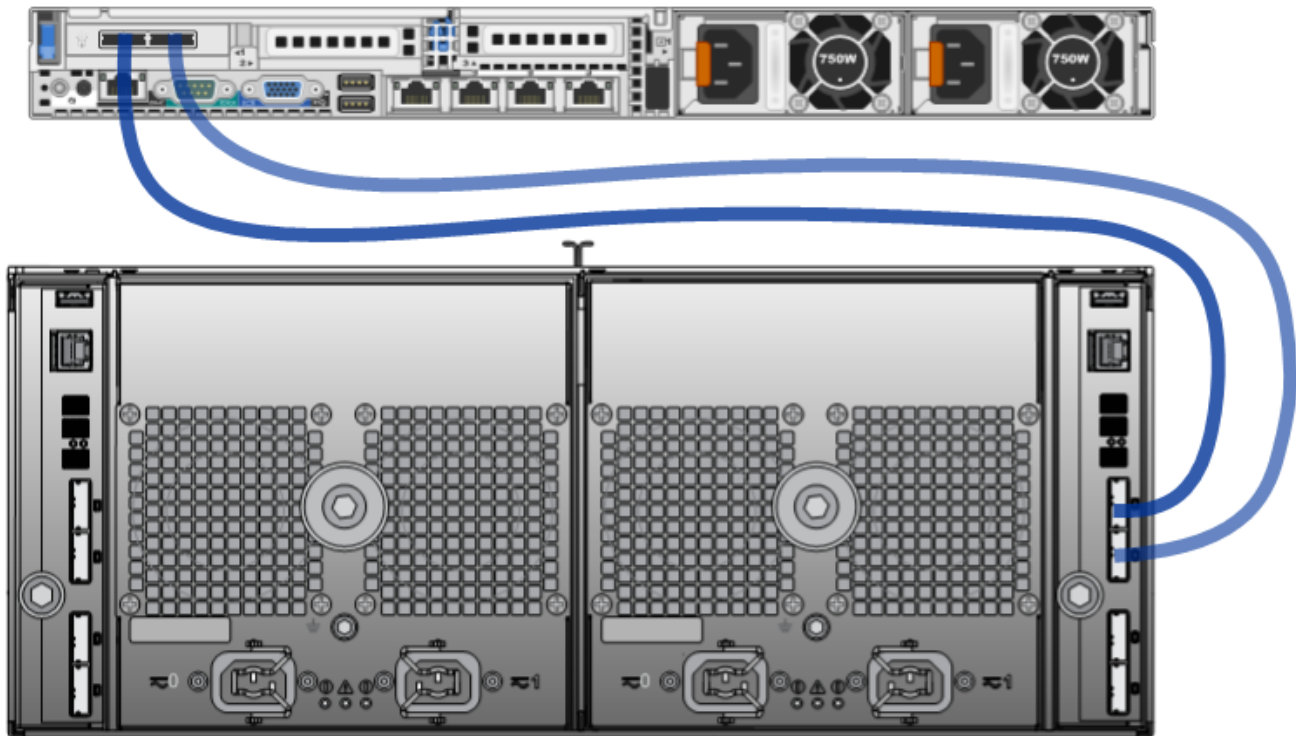
アプライアンスへの60-drive DACの接続

ここで紹介するケーブル接続手順は、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2本のSASケーブルが付属します。この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。

アプライアンスに60-drive DACを接続するには、次の手順を実行します。

1. Security Analytics S4アプライアンスの背面にあるRAIDコントローラーのポートに各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コントローラー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コントローラーに最初の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。



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

Decoder、Log Decoder、Archiver上でDACインストール スクリプトを実行するには、次の手順に従います。

1. SCPを使用して、`arrayCfg-2.1.tgz` ファイルをアプライアンス上の `/root` にコピーします。
2. 次のコマンドを実行してコンテンツを展開します:

```
tar -zxvf arrayCfg-2.1.tgz
```
3. 新しく作成された `arrayCfg` ディレクトリに移動します:

```
cd arrayCfg
```
4. 次のコマンドを実行します。

```
#nwraidutil.pl | more
```
5. 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。
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。

```
[root@CSO-S4Decoder ~]# ./NwArrayConfig.py --action init --service (decoder/logdecoder/archiver)
```

スクリプトは、必要なすべての仮想ドライブ、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
7. スクリプトの実行を完了した後、Security Analytics Administrationを使用してデバイスを追加し、Decoder、Log Decoder、Archiverの各サービスにライセンスを付与します。
8. 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
<code>/var/netwitness/decoder</code>	30G
<code>/var/netwitness/decoder/index</code>	30G
<code>/var/netwitness/decoder/sessiondb</code>	1013G
<code>/var/netwitness/decoder/metadb</code>	9.9T

Decoder、Log Decoder、Archiver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。