

RSA Security Analytics

Direct-Attached Capacity (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.

Direct-Attached Capacity (DAC) Series 4構成ガイド

• Direct-Attached Capacity (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



Direct-Attached Capacity (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 Concentrator、Series 4 Archiver、Series 4 Hybrid、Series 4 All-In-Oneの各アプライアンスに15-drive DAC Series 4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、Security Analytics 15-drive Direct-Attached Capacity (DAC) Series 4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、EMC²によって提供されるドライブ アレイ エンクロージャです DACは、Series 4の Decoder、Concentrator、Archiver、Hybrid、All-In-One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

RSASecurity Analytics Series 4 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

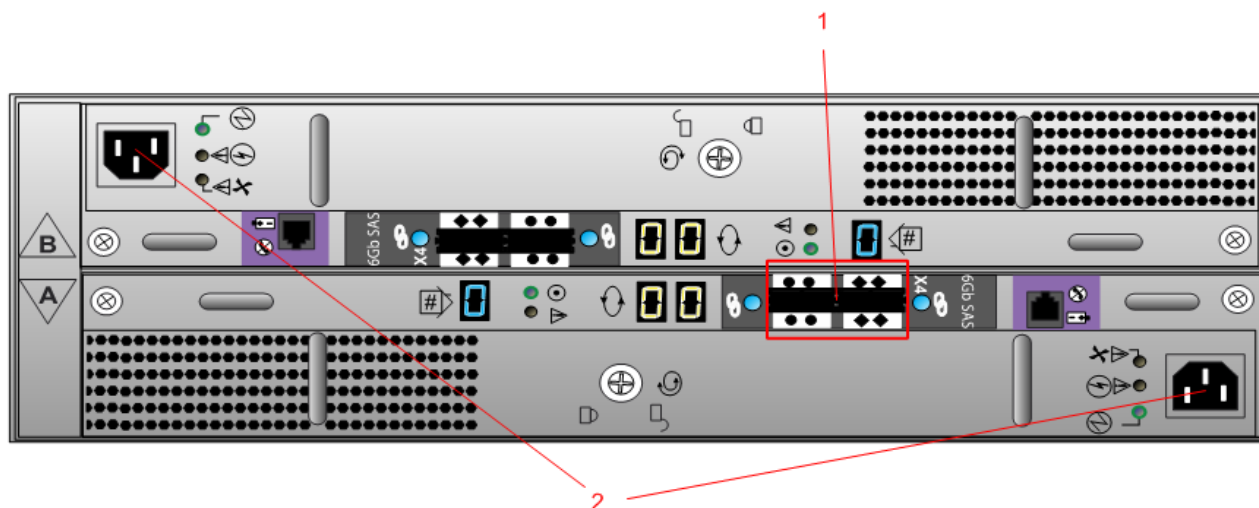
DACに付属するEMC² のドキュメントを参照してください。

 **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。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。

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、シャーシの中央近くのポートがプライマリ ポートです。
2	電源入力接続



DACのインストール

概要

このトピックでは、Series 4 Decoder、Series 4 Concentrator、Series 4 Archiver、Series 4 Hybrid、Series 4 All-In-Oneの各アプライアンスに15-drive DAC Series 4をインストールする方法について説明します。

はじめに

次の表に、さまざまな導入環境におけるインストール手順のサマリーを示します。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。導入のシナリオは、次のとおりです：

- 複数のDACをConcentrator、Decoder、Log Decoder、Archiver導入環境にインストール。
- 単一のDACをHybrid導入環境にインストール。
- 単一のDACをAll-In-One導入環境にインストール。

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。

- `arrayCfg-2.1.tgz`以降。ストレージを構成するために必要です。このスクリプトは四半期ごとに更新され、バージョンは次のように表されます。`arrayCfg-<x.y-z>.tgz`。ここで、`<x.y-z>`はバージョン番号です。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。
- `nwraidutil.pl`

手順の概要

次の表に、さまざまな導入シナリオにおける手順の概要を示します。

導入のシナリオ	タスク
Concentrator/ Archiver Decoder/ Log Decoder (複数のDAC)	⚠ Caution: <code>NwArrayConfig.py</code> スクリプトを <code>--init</code> オプション付きで実行する前に、デバイスにライセンスを付与していないことを確認しま

導入のシナリオ	タスク
	<p>す。Series 4/4S Decoderに複数のDACをインストールする場合、サービスにライセンスを付与して開始する前に、ステップ1、2、3 (最初のDACのケーブル接続と初期化) を実行します。この手順に従わない場合、ディレクトリ構造に関する問題やデータの消失が発生する可能性があります。またアプライアンスの再イメージ化が必要になることがあります。</p> <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、アプライアンスに最初のDACを接続します。 2. 「Decoder、Concentrator、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。 <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>Note: このスクリプトを実行する前に誤ってデバイスのライセンスを付与した場合は、DACドライブを元の状態にリストアします。詳細はRSAまでお問い合わせください。</p> </div> <ol style="list-style-type: none"> 3. 「DecoderまたはConcentratorサービスの再起動」に従ってサービスを再起動します。 4. 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、Security Analyticsのヘルプ オプションもしくは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。 5. アプライアンスの電源を停止して、アプライアンスに追加のDACを接続します。 6. 「ストレージ アレイ追加時のDACインストール スクリプトの実行」に従って、追加のDACに対してDACインストール スクリプトを<code>--add</code>オプション付きで実行します。 7. 「DecoderまたはConcentratorサービスの再起動」に従ってサービスを再起動します。
Hybrid/AIO	<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。 <div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;"> <p>⚠ Caution: HybridアプライアンスまたはAll-in-One (AIO)アプライアンスに対して追加ストレージを構成する前に、HybridまたはAIOを実行するすべてのサービス (Concentrator、Decoder、Broker、Log Decoderなど) にライセンスが付与されていることを確認します。</p> </div> <ol style="list-style-type: none"> 2. サービスにライセンスを付与します。手順については、Security Analyticsのヘルプ オプションもしくは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。「HybridまたはAll-in-One (AIO)アプライアンスへのDACの追加」に従って、<code>NwArrayConfig.py</code>スクリプトを<code>--add</code>オプション付きで実行します。

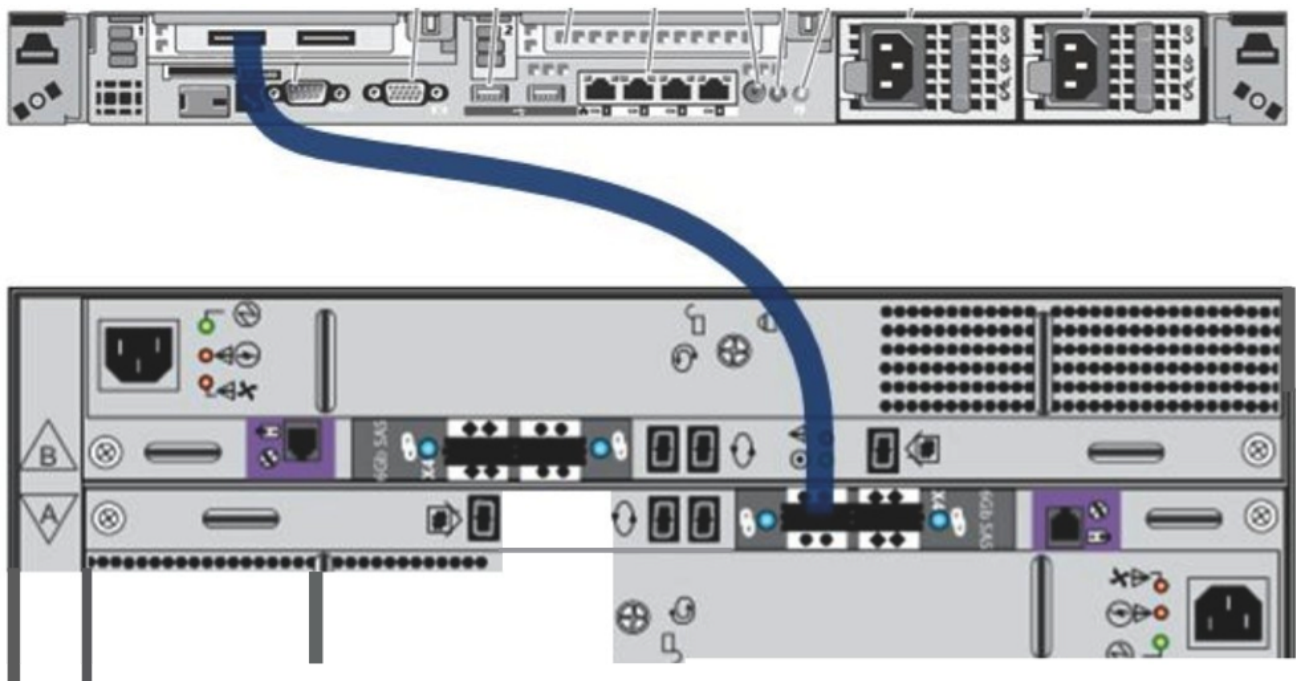
アプライアンスへのDACの接続

ここで紹介するケーブル接続手順は、次の導入タイプのすべてのアプライアンスに適用されます。Concentrator、Decoder、Log Decoder、Archiver、Hybrid、All-In-One。

Note: DACには2本のSASケーブルがあります。アプライアンスにDACを接続するのに必要なケーブルは1本のみです。2本目のSASケーブルはスペアです。

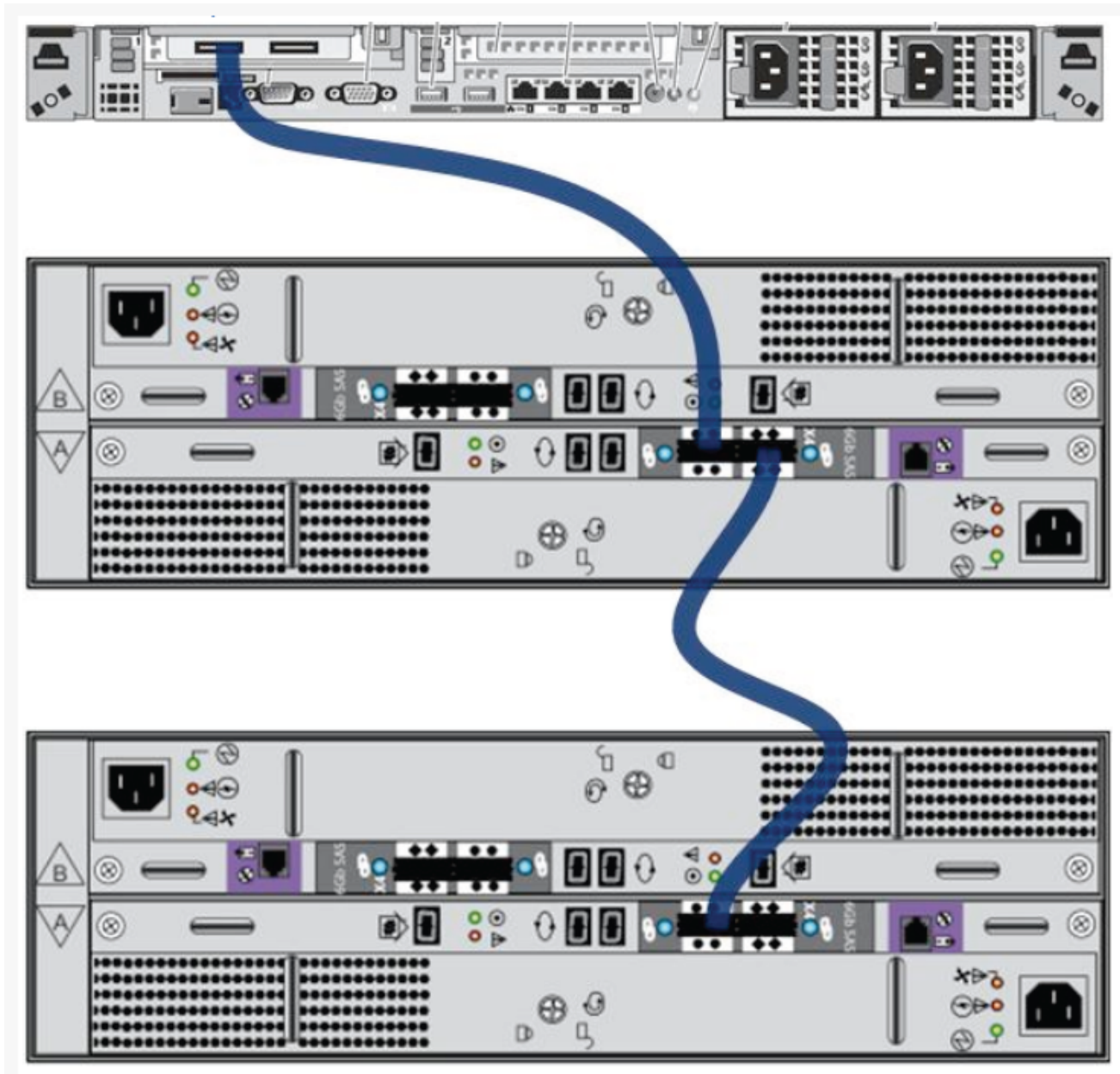
アプライアンスにDACを接続するには、次の手順を実行します。

1. Security Analytics S4アプライアンスの背面にあるRAIDコントローラの左側のポートに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. 最初のDACのプライマリ ポートにDecoderからのケーブルを挿入します。
 - b. 最初のDACのセカンダリ ポートから次のDACのプライマリ ポートにケーブルを接続します。

次の図は、複数のDACを接続する方法を示しています。



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

⚠ Caution: Decoder、Concentrator、Archiverでは、後述する`--action init`オプション付きのスクリプトを実行する前に、ライセンスを付与しないでください。

次の手順でDecoderまたはConcentratorでDACインストール スクリプトを実行します:

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-S4Concentrator ~]# ./NwArrayConfig.py --action init --service (decoder|concentrator|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、Concentrator、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 '/(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/concentrator	30G
/var/netwitness/concentrator/index	1.1T
/var/netwitness/concentrator/sessiondb	1013G
/var/netwitness/concentrator/metadb	9.9T

ストレージ アレイ追加時のDACインストール スクリプトの実行

初期化後にストレージを追加する場合、次の手順でDecoderまたはConcentratorでDACインストール スクリプトを実行します:

1. アプライアンスにarrayCfg-2.1.tgzファイルがコピーされていない場合は、SCPなどのツールでアプライアンスの/rootにarrayCfg-2.1.tgzファイルをコピーします。
2. 次のコマンドを実行します。
`nwraidutil.pl | more`
3. 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。
4. 以下の項目を確認します:
 - a. NwArrayConfig.pyスクリプトを実行する前に、DecoderまたはConcentratorにライセンスが付与されている。
 - b. DecoderおよびApplianceサービス上でRESTが有効である。
5. 次のコマンドを実行して/root/arrayCfgディレクトリに移動します:
`cd /root/arrayCfg`
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-DecoderSM ~]# ./NwArrayConfig.py --action add --service (concentrator|decoder|archiver)`

このスクリプトは、使用可能なドライブを含む次の追加DACを検索します。対応する論理ドライブを作成し、サービス タイプに基づいて適切な構成を実行します。すべてのメッセージが./arrayCfg.logに記録されます。

7. 各DACについて、すべての構成が完了するまで、ステップ1~6を繰り返します。

8. 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、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	3.5T
/var/netwitness/decoder/sessiondb	185G
/var/netwitness/decoder/packetdb	19T
/var/netwitness/decoder/packetdb0	24T

c. 追加した各DACに対応するエントリが表示されることを確認します。作成された各DACごとに/var/netwitness/decoder/packetdb#が表示されます。/var/netwitness/decoder/packetdb#で示されたサイズが、接続した拡張ストレージ アレイから想定される値に近いことを確認します。Security Analyticsインタフェースで確認できるように、この番号をメモしておきます。

d. Security Analyticsインタフェースにログオンし、Security Analyticsメニューで [Administration] > [デバイス] を選択します。

[Administration] の [デバイス] ビューが表示されます。

e. [Decoder] または [Log Decoder] を選択し、ツールバーから [表示] > [エクスプローラー] 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>は新しいデバイスのサイズの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。

Decoder、Concentrator、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、Concentrator、Archiverの各サービスを再起動する必要があります。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。

HybridまたはAll-in-One (AIO)アプライアンスへのDACの追加

⚠ Caution: HybridアプライアンスまたはAll-in-Oneアプライアンスに対して追加ストレージを構成する前に、HybridまたはAIOを実行するすべてのサービス (Concentrator、Decoder、Broker、Log Decoderなど) にライセンスが付与されていることを確認します。手順については、Security Analyticsのヘルプ オプションもしくはsdocs.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。

HybridまたはAll-in-One (AIO)アプライアンスにDACを追加するには、次の手順を実行します:

1. 「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. 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。
3. コンテンツを展開します:

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

```
cd arrayCfg
```
5. 次のコマンドを実行して、構成済みドライブを表示します:

```
#nwraidutil.pl | more
#df -h
```
6. 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。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。

```
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/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. 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-DecoderSM ~]# ./NwArrayConfig.py --action add --service hybrid --drives <N>
```

ここで、`<N>`は、HybridのConcentrator部分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???このスクリプトは、使用可能なドライブを含む次の追加DACを検索します。Hybridの各サービスの論理ドライブを作成し、サービスタイプに基づいて適切な構成を実行します。すべてのメッセージが `./arrayCfg.log` に記録されます。
8. 各DACについて、すべての構成が完了するまで、ステップ1~7を繰り返します。
9. 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|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/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. 追加した各DACに対応するエントリが表示されることを確認します。作成された各DACごとに `/var/netwitness/decoder/packetdb#` が表示されます。 `/var/netwitness/decoder/packetdb#` で示されたサイズが、接続した拡張ストレージ アレイから想定される値に近いことを確認します。Security Analytics インタフェースで確認できるように、この番号をメモしておきます。
- d. Security Analytics インタフェースにログインし、Security Analytics メニューで [**Administration**] > [デバイス] を選択します。
[Administration] の [デバイス] ビューが表示されます。
- e. [Decoder] または [Log Decoder] を選択し、ツールバーから [表示] > [エクスプローラー] 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>は新しいデバイスのサイズの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。