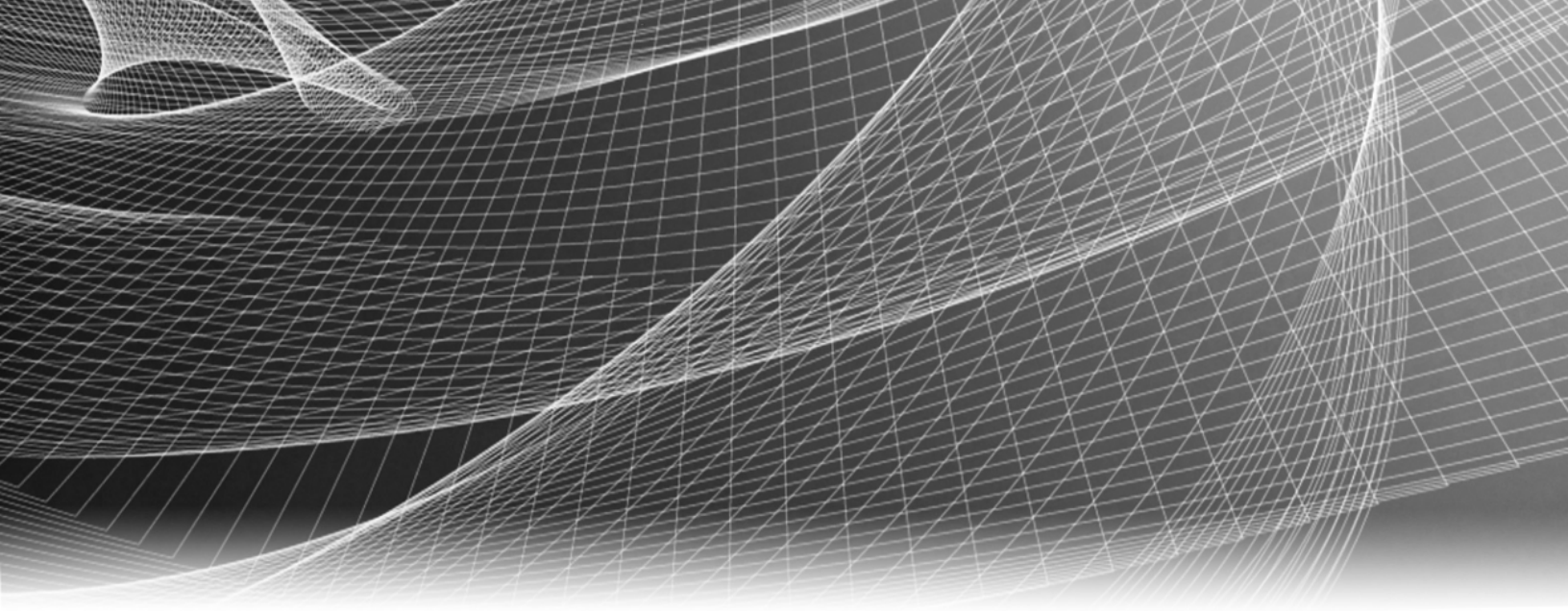


RSA Security Analytics

Series 5 Security Analyticsアプライアンス構成ガイド

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.

Series 5 Security Analyticsアプライアンス構成ガイド

RSA

Series 5 Security Analyticsアプライアンス構成ガイド

概要

このドキュメントでは、RSA Series 5 (S5) Security Analyticsアプライアンスをインストールし、ネットワークに接続するための手順を説明します。

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。ハードウェアの構成を完了した後、sadocs.emc.com/ja-jpのSecurity Analyticsオンライン ドキュメントの説明に従って、Security Analyticsアプライアンスの構成を完了してください。

このドキュメントは、ハードウェア製造メーカーのマニュアルに代わるものではありません。Security Analyticsアプライアンス専用の情報が含まれています。

Last Modified: September 14 2016, 12:10PM

RSA

S5 R630アプライアンス ハードウェアの説明

はじめに

1つの例外を除き、すべてのRSA Series 5 (S5) Security AnalyticsアプライアンスはDell PowerEdge R630シャーシをベースにしています。例外として、Hybridアプライアンスは、Dell PowerEdge R730xdシャーシをベースにしています。Series 5アプライアンスには、出荷時にSecurity Analytics 10.5ソフトウェアがインストールされています。

このトピックでは、Dell PowerEdge R630 シャーシをベースにした以下のSeries 5アプライアンスについて説明します。

- DecoderおよびLog Decoder
- Concentrator
- Broker
- Archiver
- Security Analytics Server
- Malware Analysis
- Event Stream Analysis (ESA)

ESAアプライアンスを除き、すべてのDell PowerEdge R630ベースのアプライアンスは、同一のコンポーネントと物理仕様を採用しています。ESAアプライアンスには、ハード ディスク ドライブおよびメモリが増設され、異なるCPUが搭載されています。Security Analytics ESAアプライアンスの仕様に詳細が記載されています。

ネットワーク上でSeries 5アプライアンスの初期構成を行うには、次のステップを実行します。

1. Security Analyticsソフトウェア バージョンの「*導入ガイド*」で、設置場所の要件と安全情報を確認します：Security Analytics 10.5
2. 設置場所の要件に従って、アプライアンスを安全にマウントします。
3. アプライアンスをネットワークに接続して、アプライアンスのネットワーク パラメータを構成します：アプライアンスの接続とネットワーク パラメータの構成
4. Security Analyticsでアプライアンスの構成を完了します：Security Analyticsでのアプライアンス構成の完了

⚠ **Caution:** Security Analyticsアプライアンスの損傷を防ぐため、別の場所に輸送する場合は、ラックから取り外し、ラックを解体してください。梱包、輸送、設置に関するサーバおよびラックのメーカーの推奨事項に従ってください。
RSAは、ラックに設置された状態で輸送し損傷したアプライアンスの再出荷には対応していません。お客様は、ラックに設置された状態でのSecurity Analyticsアプライアンスの輸送に関してすべてのリスクと責任を負います。

Last Modified: September 14 2016, 12:10PM

パッケージの内容

アプライアンスの設置と構成に必要なすべてのアイテムが揃っているかどうか梱包の内容を確認します。

- Series 5 Security Analyticsアプライアンス (Decoder、Concentrator、Broker、Archiver、Security Analytics Server、Malware Analysis、ESA)
- ReadyRails固定式レール (1セット)
- EMCディープ ラック用の左レール アダプタ
- RSAベゼル (1) : ベゼルに鍵が貼り付けられています。
- 電源コード (2)
- Dell製品情報ガイド ブック (1)
- RSAドキュメント フォルダ (1)
- RSA EULA (1)

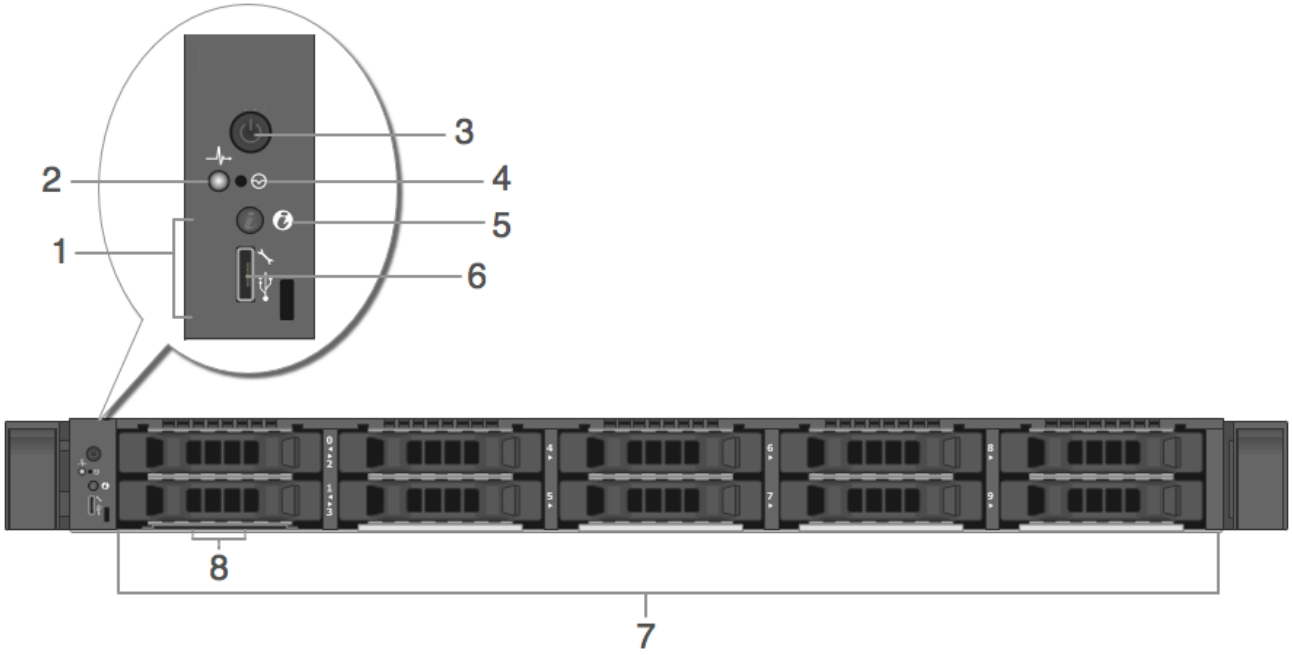
お客様側で用意が必要な機材

この構成手順を完了するには、以下の機材をご用意いただく必要があります。

- Ethernetネットワーク ケーブル1本
- モニタまたはKVMアダプタをVGAポートに接続するケーブル、およびキーボードまたはKVMアダプタをUSBポートに接続するケーブル
- 標準的なツール

Last Modified: September 14 2016, 12:10PM

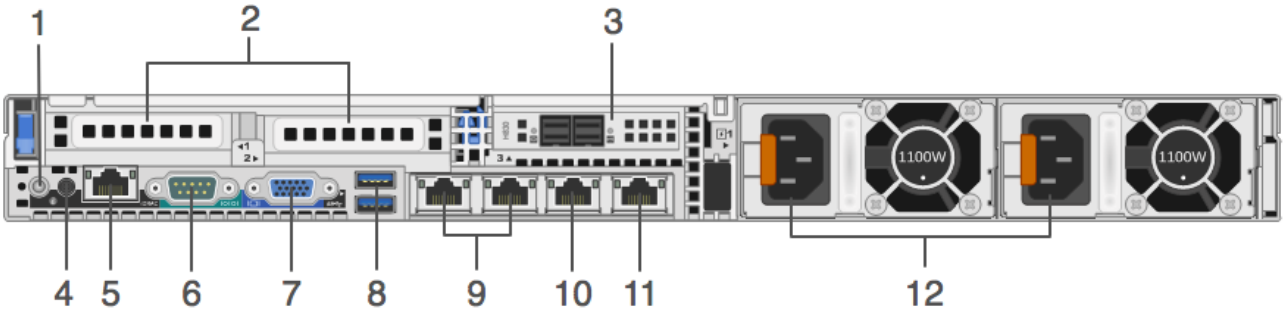
Series 5アプライアンスの前面（Hybridを除く）



番号	説明
1	診断インジケータ。エラーがある場合には、診断インジケータがこの場所にステータスを表示します。
2	システム正常性インジケータ。システム障害が検出されたときにオレンジ色に点滅します。
3	電源オン/オフ
4	埋め込み型NMIボタン
5	システム識別ボタン
6	マイクロUSBポート/iDRACダイレクト
7	2.5インチ ハード ディスク ドライブ ベイ10個（フィールド交換可能）。後述の仕様セクションで、アプライアンスに取り付けられているハード ディスク ドライブの数とタイプを記載しています。
8	情報タグ

Last Modified: September 14 2016, 12:10PM

Series 5アプライアンスの背面（Hybridを除く）



番号	説明
1	システム識別ボタン
2	LP PCIe拡張スロット1と2。10G Decoderでは、オプションのIntel X520光ネットワーク インタフェース カードを、このLP PCIeスロットに取り付けられます。
3	PERC H830 RAIDコントローラ。上記の図では、LP PCIeスロット3に取り付けられていますが、別のLP PCIeスロットに取り付けることもできます。PERC H830は、ストレージ拡張時にDACを接続するRAIDコントローラです。DACを接続するにはMini-SASポートのケーブルが必要です。
4	システム識別コネクタ
5	iDRACポート
6	RS232シリアル ポート（DB9またはシリアル サーバを経由するラップトップへのシリアル接続）
7	VGAビデオ ポート（モニタ）
8	USBポート（キーボード、マウス、USBサム ドライブなど）
9	10GBASE-T Ethernetポート：em3およびem4
10	プライマリ ネットワーク1000BASE-T管理ポート：em1
11	セカンダリ ネットワーク1000BASE-Tポート：em2
12	ホット スワップ対応電源1および2（フィールド交換可能）

Note: PERC H830 RAIDコントローラにDACを接続するにはMini-SASポートのケーブルが必要です。

Last Modified: September 14 2016, 12:10PM

Series 5アプライアンスの仕様（HybridおよびESAを除く）

項目	説明
フォーム ファクタ	1U、全奥行
重量（概算）	18.4 kg（40.5 lbs.）
寸法（概算）	ベゼルあり：482.43 mm (18.99 in) [w] x 808.59 mm (31.83 in) [d] x 42.80 mm (1.69 in) [h] ベゼルなし：482.43 mm (18.99 in) [w] x 776.16 mm (30.56 in) [d] x 42.80 mm (1.69 in) [h]
電源装置	デュアル、ホットプラグ対応、冗長化電源（1+1）、1100W
プロセッサ	2 * E5-2667v3
RAM	16 * 8GB 2133MT/s RDIMM（128GB）
ハード ディスク ドライブ（フィールド交換可能）	2 * 1TB 7.2K RPM NLSAS 6Gbps 2.5インチ ホットプラグ ハード ディスク ドライブ 2 * 2TB 7.2K RPM NLSAS 12Gbps 512e 2.5インチ ホットプラグ ハード ディスク ドライブ
RAIDコントローラ	外部：PERC H830 RAID 内蔵: PERC H730P
ネットワーク インターフェース カード	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DPネットワーク ドーターカード

Security Analytics ESAアプライアンスの仕様

項目	説明
フォーム ファクタ	1U、全奥行
重量（概算）	18.4 kg（40.5 lbs.）
寸法（概算）	ベゼルあり：482.43 mm (18.99 in) [w] x 808.59 mm (31.83 in) [d] x 42.80 mm (1.69 in) [h] ベゼルなし：482.43 mm (18.99 in) [w] x 776.16 mm (30.56 in) [d] x 42.80 mm (1.69 in) [h]
電源装置	デュアル、ホットプラグ対応、冗長化電源（1+1）、1100W
プロセッサ	2 * E5-2680v3
RAM	8 * 32GB 2133MT/s RDIMM（256GB）

Last Modified: September 14 2016, 12:10PM

項目	説明
ハード ディスク ドライブ (フィールド交換可能)	2 * 1TB 7.2K RPM NLSAS 6Gbps 2.5インチ ホットプラグ ハード ディスク ドライブ 4 * 2TB 7.2K RPM NLSAS 12Gbps 512e 2.5インチ ホットプラグ ハード ディスク ドライブ
RAIDコントローラ	外部：PERC H830 RAID 内蔵: PERC H730P
ネットワーク インターフェース カード	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DPネットワーク ドーターカード

Caution: RSAから具体的に指示された場合を除き、アプライアンス シャーシを開くと保証は無効になります。ハード ディスク ドライブと電源は、認定技術者によってフィールド交換可能です。

Last Modified: September 14 2016, 12:10PM

RSA

R630アプライアンスでのディープ ラック アダプタの取り付け

手順

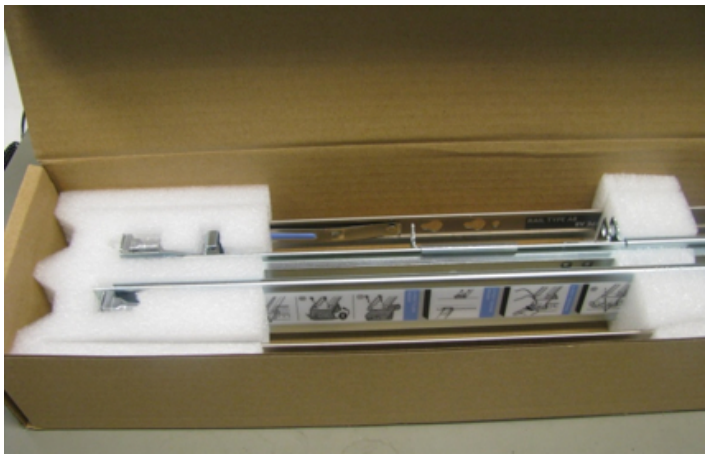
Note: この手順は、S5 R630アプライアンスをEMC Titan Dウルトラ ラックに設置する場合にのみ必要です。

S5 R630アプライアンスをEMC Titan Dウルトラ ラックに設置する場合、1U ディープ ラック アダプタが必要です。この手順に従って新しいブラケットをサーバ レールに取り付けます。

1. R630アプライアンスの付属品ボックスから、代替のレール ブラケットを取り出します。

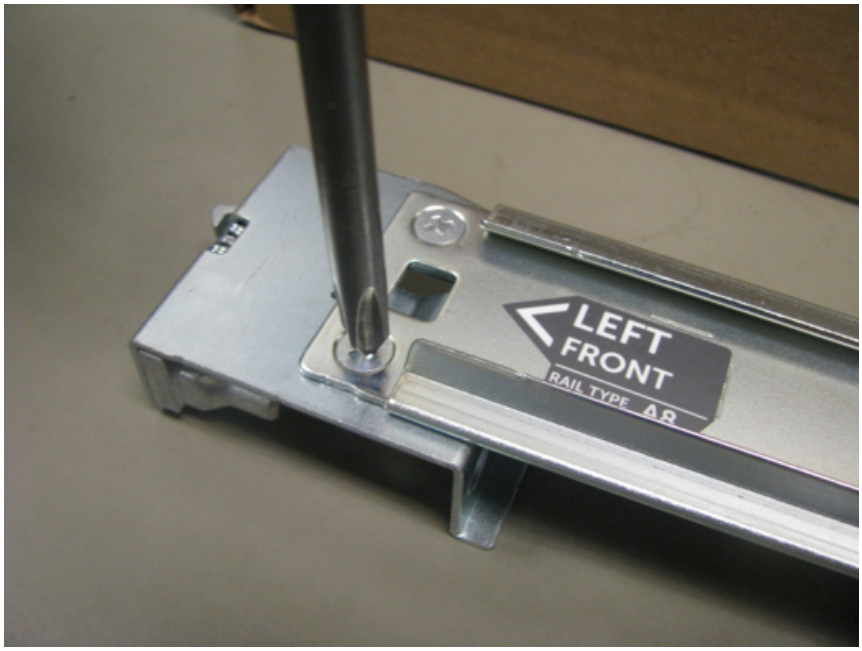
Last Modified: September 14 2016, 12:10PM

2. レールの箱から左レールを取り出します。



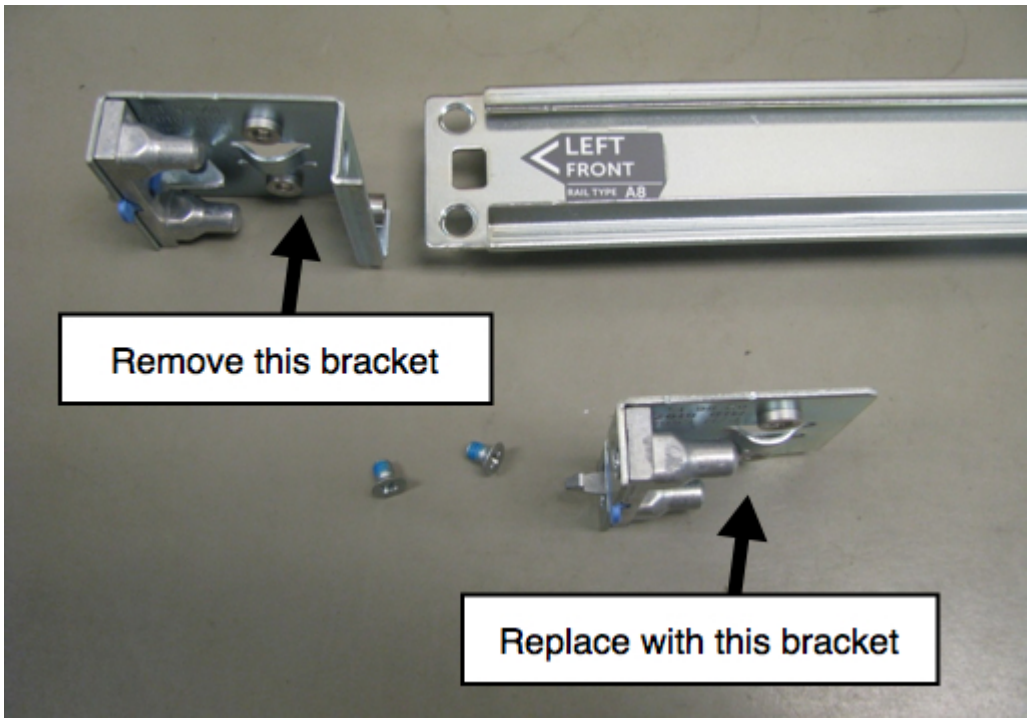
各レールにはマークがついています。

3. プラス ドライバを使用して、2つのネジを取り外します。



Last Modified: September 14 2016, 12:10PM

4. ブラケットを取り外し、新しいブラケットに交換します。



5. ネジで、新しいブラケットを固定します。

R630アプライアンスにレールを取り付ける準備ができました。

Last Modified: September 14 2016, 12:10PM

RSA

S5 R730xd Hybridアプライアンス ハードウェアの説明

はじめに

RSA Security Analytics Series 5 HybridアプライアンスはDell PowerEdge R730xdシャーシをベースにしています。RSA Security Analytics Series 5 Hybridアプライアンスには、出荷時にSecurity Analytics 10.5 Hybridアプライアンス ソフトウェアがインストールされています。Hybridアプライアンス ソフトウェアには、ConcentratorとDecoder（ログまたはパケットのいずれか）が含まれています。

ネットワーク上でSeries 5アプライアンスの初期構成を行うには、次のステップを実行します。

1. Security Analyticsソフトウェア バージョンの「*導入ガイド*」で、設置場所の要件と安全情報を確認してください：Security Analytics 10.5
2. 設置場所の要件に従って、アプライアンスを安全にマウントします。
3. アプライアンスをネットワークに接続して、アプライアンスのネットワーク パラメータを構成します：アプライアンスの接続とネットワーク パラメータの構成
4. Security Analyticsでアプライアンスの構成を完了します：Security Analyticsでのアプライアンス構成の完了

⚠ **Caution:** Security Analyticsアプライアンスの損傷を防ぐため、別の場所に輸送する場合は、ラックから取り外し、ラックを解体してください。梱包、輸送、設置に関するサーバおよびラックのメーカーの推奨事項に従ってください。
RSAでは、ラックに設置された状態で輸送し損傷したアプライアンスの再出荷には対応していません。お客様は、ラックに設定された状態でのSecurity Analyticsアプライアンスの輸送に関してすべてのリスクと責任を負います。

パッケージの内容

Hybridアプライアンスのインストールと構成に必要なすべてのアイテムが揃っているかどうか梱包の内容を確認します。

- Series 5 Hybridアプライアンス
- ReadyRails固定式レール（1セット）
- EMCディープ ラック用の左レール2Uアダプタ
- 2U RSAベゼル（1）：ベゼルに鍵が貼り付けられています。
- 電源コード（2）
- Dell製品情報ガイド ブック（1）

Last Modified: September 14 2016, 12:10PM

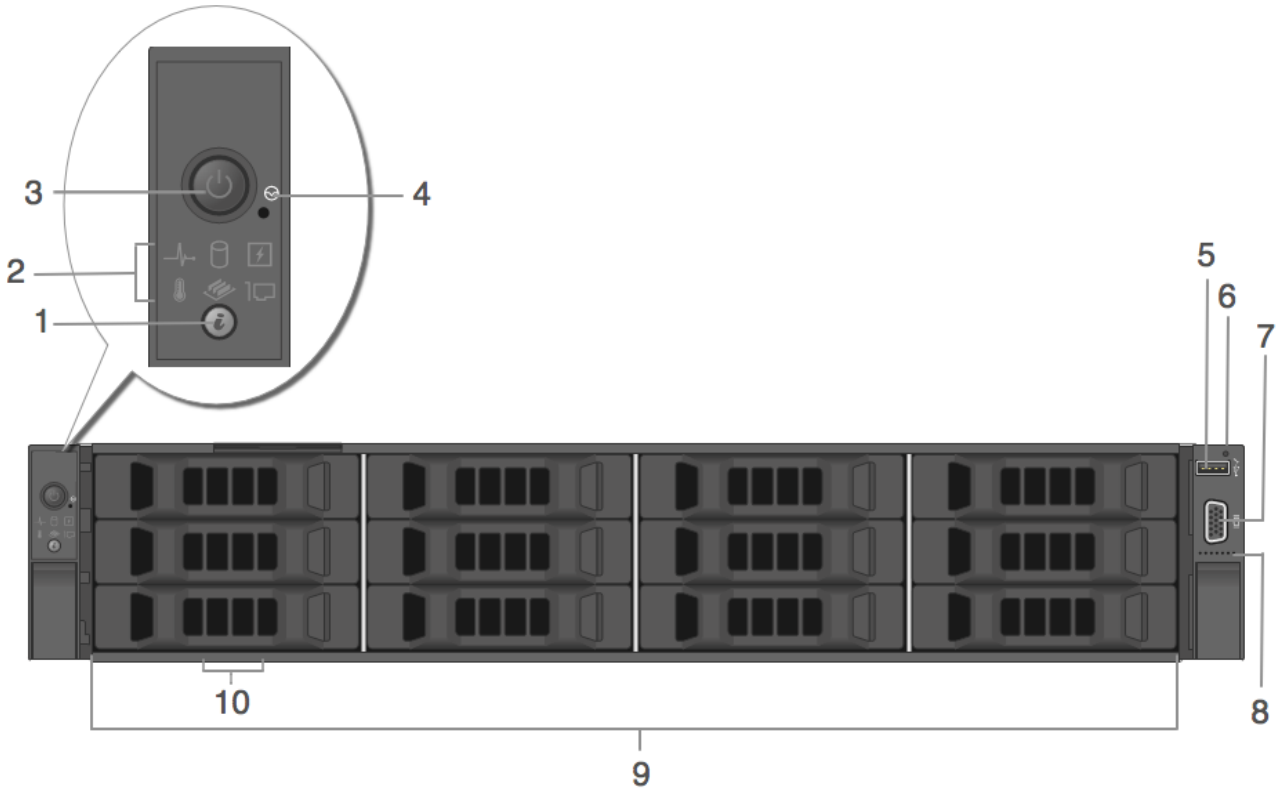
- RSAドキュメント フォルダ（1）
- RSA EULA（1）

お客様側で用意が必要な機材

この構成手順を完了するには、以下の機材をご用意いただく必要があります。

- Ethernetネットワーク ケーブル1本
- モニタまたはKVMアダプタをVGAポートに接続するケーブル、およびキーボードまたはKVMアダプタをUSBポートに接続するケーブル
- 標準的なツール

Security Analytics Hybridアプライアンスの前面

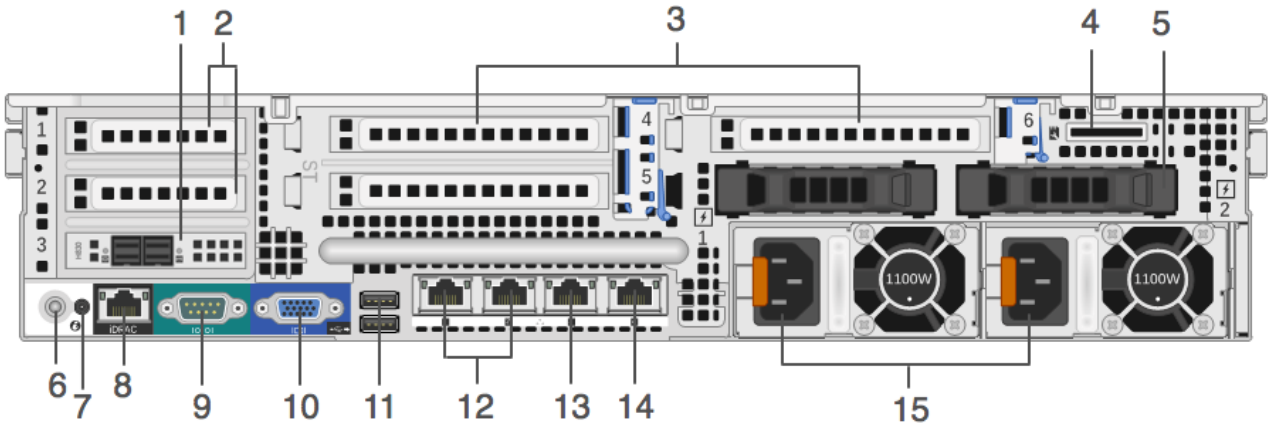


番号	説明
1	システム識別ボタン
2	診断インジケータ

Last Modified: September 14 2016, 12:10PM

番号	説明
3	電源オン/オフ
4	埋め込み型NMIボタン
5	USB管理ポート/iDRACダイレクト
6	iDRACダイレクトLEDインジケータ
7	ビデオ コネクタ
8	Quick Sync（オプション）
9	3.5インチ ハード ディスク ドライブ（HDD）12個（フィールド交換可能） Security Analytics Hybridアプライアンスには、合計14個のディスク ドライブがあります。前面に12個のHDDと背面に2個のSSD（ソリッド ステート ディスク）があります。詳細については、後述のアプライアンスの仕様を参照してください。
10	情報タグ

Security Analytics Hybridアプライアンスの背面



番号	説明
1	PERC H830 RAIDコントローラ。上記の図では、ハーフハイトPCIeカード スロット3に取り付けられていますが、別のハーフハイトPCIeスロットに取り付けることもできます。PERC H830は、ストレージ拡張時にDACを接続するRAIDコントローラです。DACを接続するにはMini-SASポートのケーブルが必要です。
2	ハーフハイトPCIe拡張カード スロット1および2
3	フルハイトPCIe拡張カード スロット（3）
4	vFlashメディア カード スロット

Last Modified: September 14 2016, 12:10PM

番号	説明
5	2.5インチSSD（ホット スワップ対応）2個
6	システム識別ボタン
7	システム識別コネクタ
8	iDRAC8 Enterpriseポート
9	RS232シリアル ポート（DB9またはシリアル サーバを経由するラップトップへのシリアル接続）
10	VGAビデオ ポート（モニタ）
11	USBポート（キーボード、マウス、USBサム ドライブなど）
12	10GBASE-TギガビットEthernetポート：em3およびem4
13	プライマリ ネットワーク1000BASE-T管理ポート：em1
14	セカンダリ ネットワーク1000BASE-Tポート：em2
15	ホット スワップ対応電源1および2（フィールド交換可能）

Note: PERC H830 RAIDコントローラにDACを接続するにはMini-SASポートのケーブルが必要です。

Security Analytics Hybridアプライアンスの仕様

項目	説明
フォーム ファクタ	2U、全奥行
重量（概算）	36.5 kg（80.47ポンド）
寸法（概算）	H: 8.73 cm（3.44インチ） x W: 48.2 cm（18.98インチ） x D: 75.58 cm（29.75インチ）
電源装置	デュアル、ホットプラグ対応、冗長化電源（1+1）、1100W
プロセッサ	2 * E5-2680v3
RAM	16 * 8GB 2133MT/s RDIMM（128GB）
ハード ディスク ドライブ	Security Analytics Hybridアプライアンスには、合計14個のディスクがあります。前面に12個のHDDと背面に2個のSSD（ソリッド ステート ディスク）があります。 2 * 800 GB SSD（背面） 4 x 1TB 7.2K RPM NLSAS 6Gbps 8 x 6TB 7.2K RPM NLSAS 6Gbps

Last Modified: September 14 2016, 12:10PM

項目	説明
RAIDコントローラ	外部：PERC H830 RAID 内蔵: PERC H730P
ネットワーク インターフェース カード	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DPネットワーク ドーターカード

Caution: RSAから具体的に指示された場合を除き、アプライアンス シャーシを開くと保証は無効になります。ハード ディスク ドライブと電源は、認定技術者によってフィールド交換可能です。

Last Modified: September 14 2016, 12:10PM

RSA

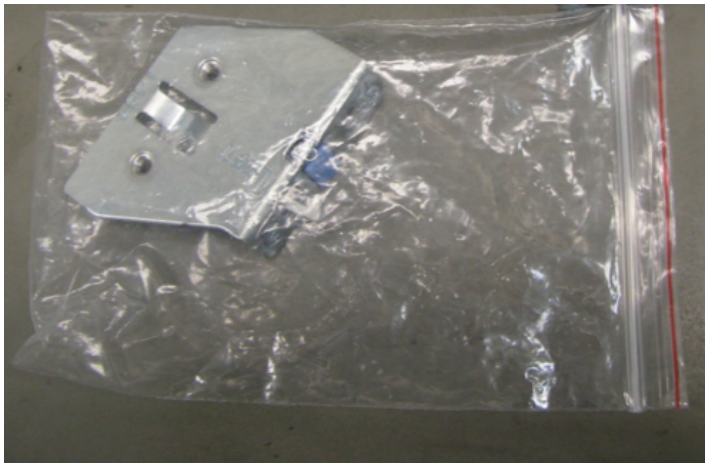
R730xd Hybridでのディープ ラック アダプタの設置

手順

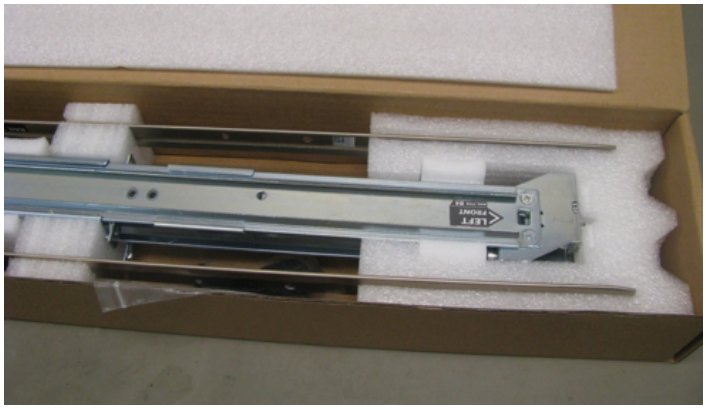
Note: この手順は、S5 R730xd HybridアプライアンスをEMC Titan D Ultraラックに取り付ける場合にのみ必要です。

S5 R730xd HybridアプライアンスをEMC Titan Dウルトラ ラックに設置する場合、2Uディープ ラック アダプタが必要です。この手順に従って新しいブラケットをサーバ レールに取り付けます。

1. R730xd Hybridアプライアンスの付属品ボックスから、代替のレール ブラケットを取り出します。



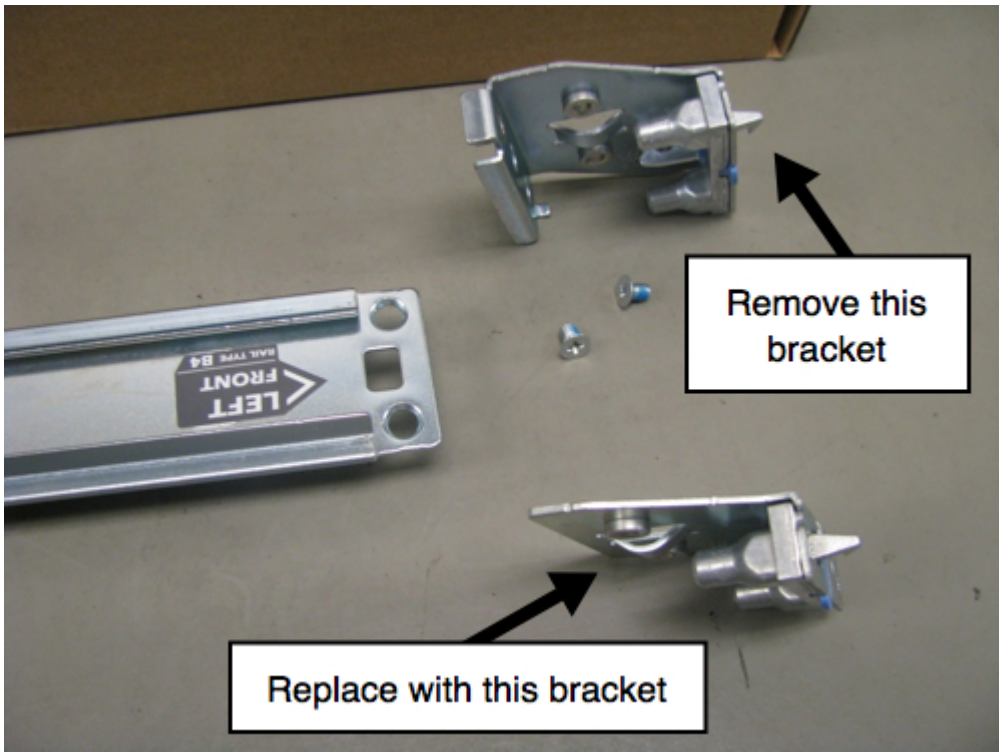
2. レールの箱から左レールを取り出します。各レールにはマークがついています。



Last Modified: September 14 2016, 12:10PM

3. プラス ドライバを使用して、2つのネジを取り外します。

4. ブラケットを取り外し、新しいブラケットに交換します。



Last Modified: September 14 2016, 12:10PM

5. ネジで、新しいブラケットを固定します。

R730xd Hybridアプライアンスにレールを取り付ける準備ができました。

Last Modified: September 14 2016, 12:10PM

RSA

アプライアンスの接続とネットワーク パラメータの構成

概要

このトピックでは、Security Analytics S5アプライアンスをネットワークに接続し、アプライアンスのネットワーク パラメータを構成する手順について説明します。

前提条件

各Security Analytics Series 5アプライアンスの情報を次の表に書き込みます。

項目	デフォルト値	アプライアンスの設定値
ログイン	root	
パスワード	netwitness	
システムのIPアドレス	192.168.1.1	
システムのネットマスク	255.255.255.0	
デフォルト ゲートウェイ		
プライマリDNSサーバ IPアドレス		
セカンダリDNSサーバ IP		
ローカル ドメイン名 （オプション）		
非修飾ホスト名	NWAPPLIANCE<xxxxxx> <xxxxxx>はランダムに生成された数です。	
Security Analytics ServerのIP アドレス		

Last Modified: September 14 2016, 12:10PM

Note: ネットワークの構成を開始する前に、設置場所の要件に従ってアプライアンスを安全にマウントします。

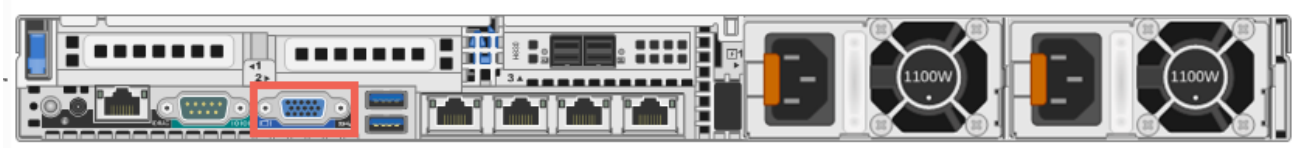
はじめに

RSA Security Analytics S5アプライアンスのネットワーク パラメータの構成では、デフォルトのIPアドレス、DNSサーバ、ホスト名、ネットワーク クロック ソースを設定します。これらのパラメータを設定するには、キーボードとマウスを使用して、アプライアンス コンソールに接続します。

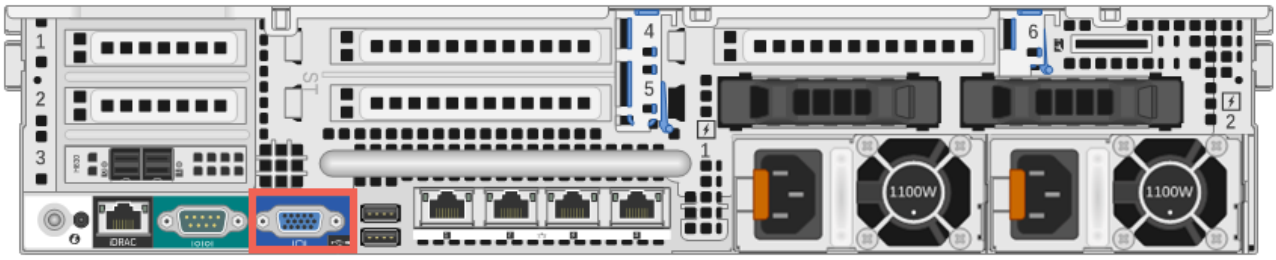
他のSecurity Analyticsアプライアンスを構成する前に、Security Analytics Serverの構成を完了することを推奨します。

アプライアンス コンソールへの接続

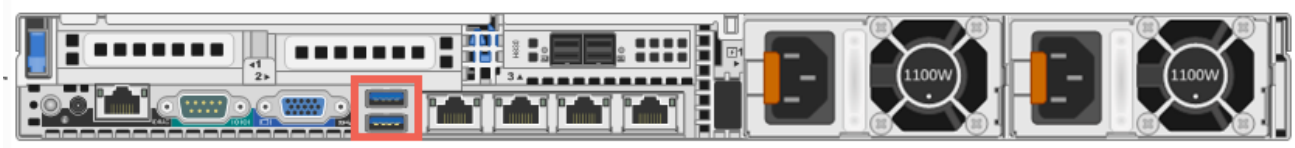
1. アプライアンスの背面にあるVGAポートにモニタまたはKVMアダプタを接続します。



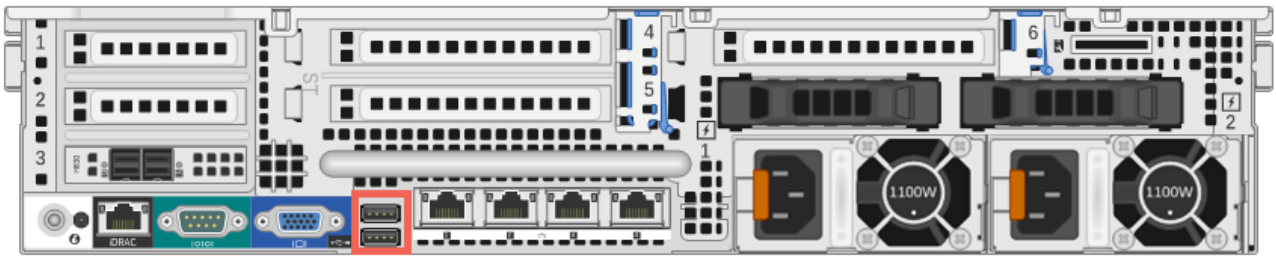
次の図は、HybridアプライアンスのVGAポートの位置を示しています。



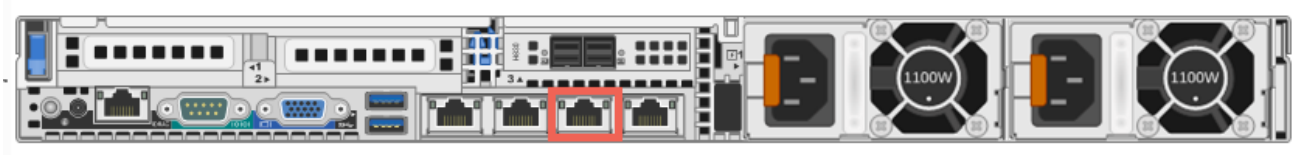
2. アプライアンスの背面にあるいずれかのUSBポートにキーボードまたはKVMアダプタを接続します。



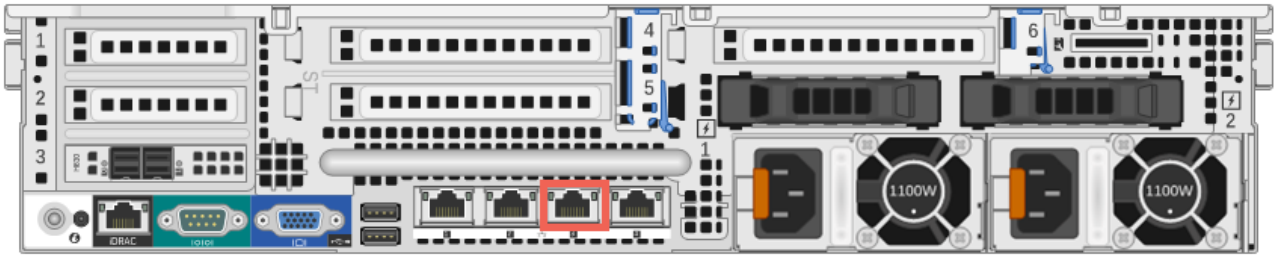
次の図は、HybridアプライアンスのUSBポートの位置を示しています。



3. アプライアンスの背面のem1ポートを、Ethernetケーブルでネットワークに接続します。



次の図は、Hybridアプライアンスのem1ポートの位置を示しています。



4. アプライアンスの背面にある2基の電源装置に電源コードを接続します。電源コードを電源に接続します。より堅牢な構成にするには、各電源装置を別の回路に接続します。

> ⚠ **Caution:** システムを電源に接続しているときは、常時5Vの予備電源がアクティブになっています。システムへの電源を切断するには、両方のAC電源ケーブルを電源から抜く必要があります。

5. アプライアンスの電源をオンにし、「ネットワーク パラメータの構成」セクションに進みます。

ネットワーク パラメータの構成

1. ログイン プロンプトで、デフォルトの認証情報を入力してオペレーティング システムにアクセスします。

```
NWAPPLIANCE<xxxxxx> login: root
Password: netwitness
```

> **Note:** ネットワーク パラメータを構成するためのプロンプトが表示されない場合は、コマンド ラインから`#netconfig.sh`を実行すると、構成オプションの入力プロンプトが表示されます。

2. プロンプトが表示されたら、次の情報を入力します。
   a. システムのIPアドレス (DHCPの場合は、**d**を入力)
   b. システムのネットマスク
   c. デフォルト ゲートウェイ

Last Modified: September 14 2016, 12:10PM

d. プライマリDNSサーバのIPアドレス
e. セカンダリDNSサーバのIPアドレス (設定しない場合は**Enter**キーを押します)
f. ローカル ドメイン名 (設定しない場合は**Enter**キーを押します)
g. 非修飾ホスト名

初期構成の入力が完了すると、構成を保存する前に内容を確認するため、次の図のようなプロンプトが表示されます。

3. 入力した情報を確認し、yを入力して構成を保存します。
   これでネットワーク情報が設定され、ネットワーク サービスが再起動されます。
4. 構成中のアプライアンスがSecurity Analytics Server以外の場合、**プロンプトが表示されるまで約15秒間待ち**、Security Analytics ServerのIPアドレスを入力します。
5. DNSサーバにpingを実行してネットワーク接続を確認します。
6. 「ネットワーク クロック ソースの指定」セクションに進みます。

ネットワーク クロック ソースの指定

各サービスやアプライアンス間で時刻同期を構成しておく必要があります。時刻同期にはNTP時刻ソースを使用することを強く推奨します。時刻設定は、基盤となるサービス間の通信にとってきわめて重要です。また、各アプライアンスの時刻が同期されていないと、データの分析において時間のずれが生じ、正常な結果が得られなくなります。この時点でNTPサーバが構成されていないか、接続できない場合、ネットワーク クロック ソースの構成は失敗しますが、後でSecurity Analyticsインタフェースから構成することができます。

ベスト プラクティス

次のベスト プラクティスを推奨します。

データの完全性を確実にするため、 Security Analytics Serverを他のすべてのアプライアンスのクロック ソースとして設定します。ESA (Event Stream Analysis) を含むすべてのアプライアンスは、Security Analytics Serverから時刻を取得します。Security Analytics Serverにのみ、外部のNTPサーバを設定します。

Security Analytics Serverアプライアンスでは、NwConsoleユーティリティを使用してNTPサーバを設定します。

Security Analytics10.5.1以降の場合、Security Analytics Serverアプライアンスにアタッチされたすべてのアプライアンスのクロック ソースは、自動的にSecurity Analytics Serverに設定されます。Security Analytics10.5.1より前のアプライアンスの場合、手動でSecurity Analytics Serverをクロック ソースとして設定します。

NwConsoleユーティリティを使用したSecurity Analytics Serverの時刻の設定

NwConsoleユーティリティを使用してSecurity Analytics Serverの時刻を設定するには、次の手順に従います。

1. rootプロンプト：`[root@NwAppliance~]#`で、次のコマンドを実行します。
   `NwConsole`
   NwConsoleが起動し、バージョンと日付を含む起動メッセージが表示されます。
   `RSA Security Analytics Console`
2. NwConsoleで、次のコマンドを実行します。
   `login localhost:50006 <username> <password>`
   Security Analyticsのシステム管理者アカウントのユーザー名は**admin**で、デフォルトのパスワードは**netwitness**です。
   アプライアンスにログオンすると、次のメッセージが表示されます。
   `Successfully logged in as session <session #>`
3. localhostプロンプト`[localhost:50006] />`で、次のいずれかを行います。
   a. ネットワーク クロック ソースを使用する場合は、次のコマンドを実行します。
      `appliance setNTP source=<NTP_server_hostname or IP_address>`
      例：**`appliance setNTP source=0.pool.ntp.org`**
   b. クロック ソースとしてアプライアンスのクロックを使用する場合は、次のように実行します：**`appliance setNTP source=local`**
4. コマンドからの`Success`の出力を確認したら、「**`exit`**」と入力し、NwConsoleプログラムをログアウトして終了します。

> **Note:** NTPクロック ソースとしてlocalを指定した場合、アプライアンスのクロックが使用されます。アプライアンスの時刻は、Security Analyticsオンライン ヘルプの [Set Host Built-In Clock(ホスト内蔵クロックの設定)] に記載されている手順で構成することができます。

RSA

Security Analyticsでのアプライアンス構成の完了

はじめに

Series 5アプライアンスの構成を完了するには、Security Analyticsにログオンして、Security AnalyticsのAdministrationモジュールの構成オプションを実行する必要があります。アプライアンスのタイプによって構成手順は若干異なります。このセクションでは、基本的な情報と構成プロセスについて説明したオンライン ヘルプへのリンクを提供します。

Security Analyticsへのログオン

RSA Security Analyticsは、ブラウザからアクセス可能なWebベースのアプリケーションです。WebSockets、LocalStorage、HTML5 History APIをサポートするブラウザが互換性のあるブラウザです。これには、Google Chrome、Apple Safari、Mozilla Firefox、Internet Explorer 10以降が含まれます。

1. Webブラウザに次のように入力します。
   `https://<hostname or IP address>/login`
   `<hostname or IP address>`はSecurity Analyticsサーバのホスト名またはIPアドレスです。
   Security Analyticsのログイン画面が表示されます。

Last Modified: September 14 2016, 12:10PM

2. ユーザー名とパスワードを入力し、 [**ログイン**] をクリックします。
   Security Analyticsのシステム管理者アカウントのユーザー名は**admin**で、デフォルトのパスワードは**netwitness**です。

オンライン ヘルプを開く

アプライアンスの構成手順は、アプライアンスにインストールされているソフトウェアのバージョンごとに提供されます。

Security Analytics 10.5の場合は、ホストおよびサービスの構成ガイドおよびライセンス ガイドを参照してください。構成を開始する前に全般的な構成プロセスを理解するには、「*ホストおよびサービス スタート ガイド*」が良い出発点となります。

Last Modified: September 14 2016, 12:10PM