

# RSA Security Analytics

S4 Event Stream Analysis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](http://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.

---

# S4 Event Stream Analysis構成ガイド

- S4 Event Stream Analysis構成ガイド 4
  - SA Event Stream Analysis (ESA) ハードウェアの説明 5
  - アプライアンスのマウントとネットワーク パラメータの構成 9
  - Security AnalyticsでのEvent Stream Analysis (ESA)構成の完了 15



# S4 Event Stream Analysis構成ガイド

---

## 概要

このドキュメントでは、RSA Security Analytics Event Stream Analysis ( ESA ) 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、Security Analyticsのヘルプ オプションもしくは[sadoes.emc.com/ja-jp](http://sadoes.emc.com/ja-jp)から参照可能なSecurity Analyticsオンライン ドキュメントの記載に従って、ESAアプライアンスの構成を完了してください。



# SA Event Stream Analysis (ESA) ハードウェアの説明

---

## 概要

このトピックではRSA Series 4 Event Stream Analysisアプライアンスについて紹介し、操作手順やコネクタについて概要を説明します。

---

## はじめに

RSA Series 4 Event Stream Analysisアプライアンスには、出荷時にEvent Stream Analysis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Event Stream Analysis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. Event Stream Analysisハードウェアをマウントします。
3. Event Stream Analysisをネットワークに接続して、Event Stream Analysisのネットワークパラメータを構成します。
4. Security AnalyticsでのEvent Stream Analysisの構成を完了します。

ソフトウェアパラメータの構成を開始する際に、Event Stream Analysisに物理的に接続する手段については、いくつかのオプションがあります。接続後にシステム構成を変更するには、Security Analyticsアプライアンスコンソールを使用します。各ステップの詳細は、このドキュメントに記載されています。

Security Analyticsの詳細については、オンラインドキュメントを参照してください。Security Analyticsのドキュメントを表示するには、Security Analyticsにログオンし、Security Analyticsメニューの [ ヘルプ ] オプションを選択します。

---

## パッケージの内容

Event Stream Analysis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。

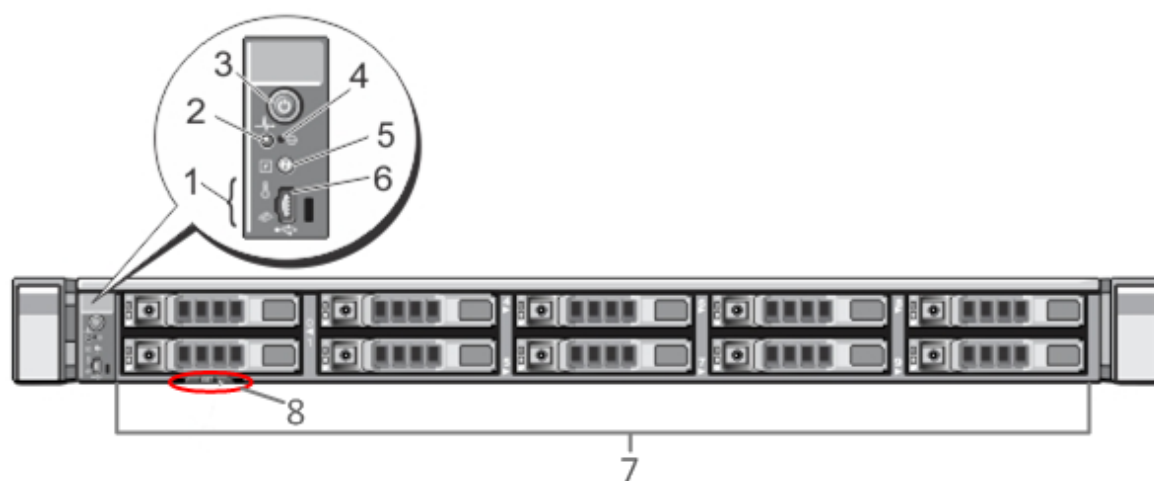
- Event Stream Analysisアプライアンス
- スライド式レール ( 2 )
- 電源コード ( 2 )

## 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。

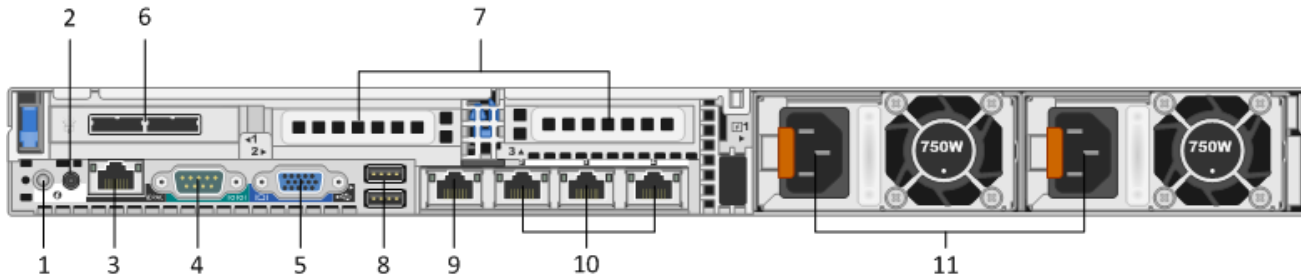
- Ethernetネットワーク ケーブル1本
- モニタまたはKVMアダプタをVGAポートに接続するケーブル、およびキーボードまたはKVMアダプタをUSBポートに接続するケーブル
- コンピュータ ハードウェアの導入および取り付けのための標準的なツール

## Event Stream Analysisアプライアンスの前面



番号	説明
1	診断LED
2	システム識別ライト
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
7	2.5インチ ハードディスク ドライブ ベイ10個。Event Stream Analysisには、10台の1 TBドライブがインストールされています。また、内蔵SD ( Secure Digital ) カード モジュールには、2枚の32 GBカードがインストールされています。ここには、デフォルトでオペレーティングシステムがインストールされています。
8	サービスタグの詳細

# Event Stream Analysisアプライアンスの背面



番号	説明
1	システム識別ボタン
2	システム識別ライト
3	iDRACポート
4	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)
5	VGAビデオポート (モニター)
6	ネットワークインターフェースカードスロット: ディスクストレージアレイ接続用のDACインターフェースポートを2個備えたSASコントローラ。
7	オプションカード用ネットワークインターフェースカード拡張スロット。以下のオプションで使用します。 <ul style="list-style-type: none"> <li>ファイバー/銅線10Gbpsネットワークキャプチャカード (RJ45)</li> <li>SANへの接続に使用するファイバチャネルホストバスアダプタ (HBA)</li> </ul>
8	USBポート (キーボード)
9	ギガビットEthernetポート1: em1 = 管理ポート。
10	ギガビットEthernetポート (2~4): em2~4
11	ホットスワップ対応電源1および2

## Event Stream Analysisアプライアンスの仕様

フォーム ファクタ	1U、全奥行
重量	39ポンド
寸法	18.99" ( w ) x 30.39" ( d ) x 1.68" ( h )
電源装置	ホット スワップ対応、冗長化750W、 100V ~ 240V オートセンシング
プロセッサ	デュアル ヘキサ コア2.66 GHz
RAM	96 GB





# アプライアンスのマウントとネットワーク 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、アプライアンスの初期管理パラメータを構成するための手順について説明します。

## はじめに

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。

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、ホスト名、DNSサーバ、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するか、またはEthernet接続によって、アプライアンス コンソールに接続します。いずれの場合でも、rootとしてアプライアンスにログオンします。アプライアンスにログオンできたら、OSのコマンド ラインを使用してアプライアンスの管理設定を変更し、DNSサーバを構成します。

方法	ユーザー名	デフォルトのパスワード
コンソール	root	netwitness

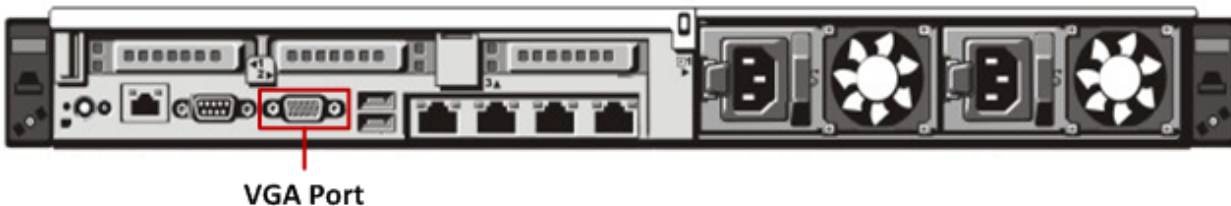
初期接続は、次のいずれかの方法で行います。

- VGA接続によるアプライアンス コンソール：キーボード（USBポート）とモニター（VGAポート）を使用してアクセスします。
- ネットワーク接続によるアプライアンス コンソール：SSHクライアントが動作するコンピュータから、Ethernetケーブルでアプライアンスの管理ポート（em1）に接続してアクセスします。このポートはデフォルトで192.168.1.1に設定されています。

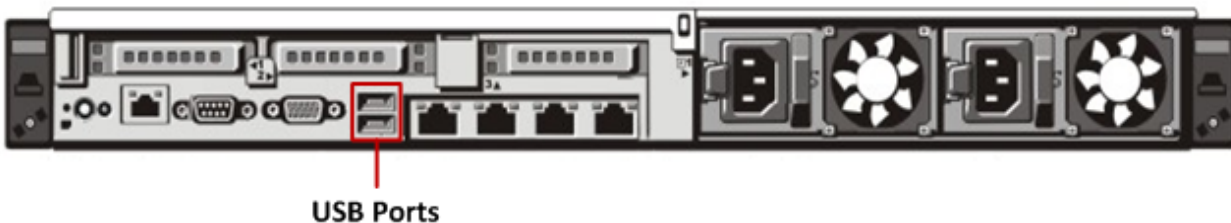
## VGA接続によるアプライアンス コンソール

VGA接続でアプライアンス コンソールを使用するには、次の手順を実行します。

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



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。



3. 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。

**Note:**

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。

4. ログインプロンプトで、デフォルトの認証情報 ( `root/netwitness` ) を使用してオペレーティングシステムにアクセスします。
5. 後述する「ネットワーク インタフェースの構成」セクションに進みます。

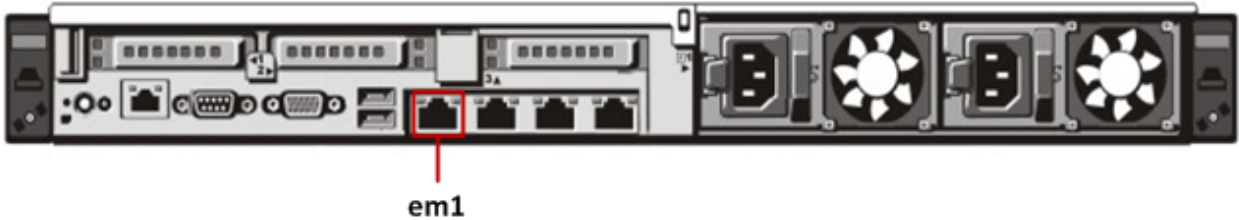
## ネットワーク接続によるアプライアンス コンソール

**Note:**

アプライアンスのデフォルトのIPアドレスは、出荷時に192.168.1.1に設定されています。192.168.1.1は、非常に一般的に使用されるIPアドレスであるため、SSHクライアントのSSH `known_hosts` ファイルにこのIPアドレスのエントリが既に登録されている可能性があります。その場合は、ファイルからこのIPアドレスに関する行を削除する必要がある場合があります。

ネットワーク接続でアプライアンス コンソールを使用するには、次の手順を実行します。

1. コンピュータと、アプライアンスの背面にあるEthernet管理ポートをクロス ケーブルで接続します。



2. アプライアンスの電源コネクタと電源コンセントに電源コードを接続します。
3. アプライアンスのデフォルトのIPアドレスは、出荷時に192.168.1.1に設定されます。したがって、クライアント システムには同じサブネット内のIPアドレスを設定します。たとえば、ラップトップのIPアドレスを192.168.1.15、デフォルト ゲートウェイを192.168.1.1に設定し、SSH ( Secure Shell ) クライアントからアプライアンスに接続します。

#### Note:

SSHでの接続中にネットワーク パラメータを変更すると、SSHセッションが切断されます。その場合には、新しいアドレスでアプライアンスに再接続します。

4. SSHキーを受け入れます。
5. ログイン プロンプトで、デフォルトの認証情報を使用してオペレーティング システムにアクセスします。

後述する「ネットワーク インタフェースの構成」セクションに進みます。

## ネットワーク インタフェースの構成

次の手順に従って、アプライアンスの管理IPアドレスを設定します。

#### Note:

アプライアンスに設定する内部用IPアドレスは、ネットワーク環境のプライベートIP範囲内で一意である必要があります。

ネットワークを構成するには、次の手順を実行します。

1. rootユーザーとしてアプライアンスにログオンします。
2. em1ネットワーク インタフェースを構成するには、`/etc/sysconfig/network-scripts/ifcfg-em1` ファイルを編集します。次のコマンドを実行します。

```
vi /etc/sysconfig/network-scripts/ifcfg-em1
```

ファイル内の次のパラメータに適切な値を指定します。

パラメータ	値
DEVICE	ネットワーク インタフェースのタイプ。たとえば、em1。
BOOTPROTO	static
IPADDR	ネットワーク インタフェースのIPアドレス

パラメータ	値
NETMASK	サブネット マスク
GATEWAY	デフォルト ゲートウェイ アドレス
HWADDR	アプライアンスのMacアドレス
ONBOOT	yes
TYPE	ネットワークのタイプ

3. 次のコマンド実行して、ネットワーク サービスを再起動します。

```
service network restart
```

## ホスト名の設定

システムのホスト名の設定は比較的簡単なタスクですが、一般的に発生しやすい問題を回避するよう考慮することが推奨されます。ホスト名の選択についてガイダンスが必要な場合は、RFC 1178を参照してください。Security Analyticsでは、アプライアンス上のデータベースはホスト名に関連づけられます。収集または集計を開始すると、ホスト名に関連づけられたデータベースが作成されます。その後、ホスト名が変更されると、別のデータベースが作成されます（この動作を避けるため、収集または集計の開始がデフォルトでオンになっていません）。ホスト名は、通信上の問題を避けるために、（#、\_、@、-などの特殊文字ではなく）英数字のみで構成するようにしてください。

**Note:** IPv4またはv6のループバック アドレスの詳細は変更しないでください。

ホスト名を設定するには、次の手順を実行します。

1. rootユーザーとしてアプライアンスにログオンします。
2. アプライアンスのホスト名を設定するには、`/etc/sysconfig/network` ファイルを編集します。次のコマンドを実行します。  
`vi /etc/sysconfig/network`
3. 次のように構成を追加/変更します。  
`NETWORKING=yes`  
`HOSTNAME=myserver.example.com`
4. 変更内容を保存して、viエディタを終了します。次のコマンドを実行します。  
`:wq`
5. ネットワークを再起動するため、次のコマンドを実行します。  
`service network restart`
6. ホスト名が正しく設定されていることを確認します。次のコマンドを実行します。  
`hostname`  
設定したホスト名が表示されます。

## DNSサーバの構成

DNSサーバを構成するには、次の手順を実行します。

1. rootユーザーとしてアプライアンスにログインします。
2. 次のコマンドを実行します。  
`vi /etc/resolv.conf`
3. 以下のように、ファイルに各DNSサーバの行を追加します。  
`nameserver <DNS_server_ip_address>`  
`search <domain_name>`  
ここで、<DNS\_server\_ip\_address>はDNSサーバのIPアドレスで、<domain\_name>はドメイン名です  
次に例を示します。  
`nameserver 192.168.0.1`  
`search acmecorp.com`
4. 変更内容を保存して、viエディタを終了します。次のコマンドを実行します。  
`:wq`

## /etc/hostsファイルの構成

アプライアンスのhostsファイルを編集して、ESAアプライアンスのIPアドレスとホスト名を追加します。

**⚠ Caution:** ESAアプライアンスのホスト名を、ループバックアドレスの構成に追加しないでください。

/etc/hostsファイルを構成するには、次の手順を実行します。

1. rootユーザーとしてアプライアンスにログインします。
2. 次のコマンドを実行します。  
`vi /etc/hosts`
3. このファイルに次の行を追加します。  
`<node_private_ip_address> <node_fqdn> <node_hostname>`  
各項目の意味は以下のとおりです。
  - <node\_private\_ip\_address>はESAアプライアンスのプライベート インタフェースに設定したIPアドレスです。
  - <node\_fqdn>は、ESAアプライアンスの完全修飾ドメイン名です。
  - <node\_hostname>はESAアプライアンスのホスト名です。

次に、ESAアプライアンスの詳細を記述した/etc/hostsファイルの例を示します。

```
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
192.168.1.10 esabox.domainname.com esabox
```

4. 変更内容を保存して、viエディタを終了します。次のコマンドを実行します。  
`:wq`

---

# ネットワーク クロック ソースの指定

Security Analyticsのすべてのシステムでネットワーク クロック ソースを使用して時刻を同期し、すべてのアプライアンスで正確に同じ時刻を示すように設定することを推奨します。これを行わない場合、アプライアンスの時刻が同期されず、特定の時間に対するクエリーで期待される結果が返されないことがあります。

ESAアプライアンスでは、`/etc/ntp.conf`のNTP ( ネットワーク タイム プロトコル ) 設定を手動で更新する必要があります。

NTP設定を更新するには、次の手順を実行します。

1. rootユーザーとしてアプライアンスにログオンします。
2. `/etc/ntp.conf`ファイルを編集するには、次のコマンドを実行します。  
`vi /etc/ntp.conf`
3. 「server」で開始する行までスクロールし、使用するNTPサイトを反映するようにserverのリストを更新します。  
例：  
NTPサイトの完全修飾ドメイン名を指定します。  
`server 0.centos.pool.ntp.org`  
また、次のようにIPアドレスを使用することもできます。  
`server 91.121.92.90`
4. 変更内容を保存して、viエディタを終了します。次のコマンドを実行します。  
`:wq`
5. ntpdサービスを再開するため、次のコマンドを実行します。  
`service ntpd restart`



# Security AnalyticsでのEvent Stream Analysis (ESA)構成の完了

---

## 概要

このトピックでは、Event Stream Analysisの構成を完了し、Security Analyticsで集計を開始するための手順について説明します。

---

## はじめに

Event Stream Analysisアプライアンスを構成するための最後のステップは、Security Analyticsサーバから行います。以下のとおりです。

1. Event Stream Analysisの [ ホスト ] ビューでSecurity Analyticsを追加します。
2. Event Stream Analysisにライセンス ( エンタイトルメント ) を適用します。
3. Event Stream Analysisに集計対象デバイスとして1つ以上のConcentratorを追加します。
4. 集計を構成し、開始します。

これらのうちいくつかのステップを実行するには、Security Analyticsネットワークの他のサービスの準備が完了している必要があります。

- 少なくとも1つのConcentratorサービスをインストールして、ライセンスの付与と構成を完了し、データ収集を開始し、Event Stream Analysisが取得するメタを生成している必要があります。
- デバイスをアクティブ化するには、Security Analyticsデバイスライセンス ( エンタイトルメント ) が必要です。

Security Analyticsにログオンし、オンライン ヘルプの手順に従ってSecurity Analyticsシステムの一部としてEvent Stream Analysisの構成を完了します。