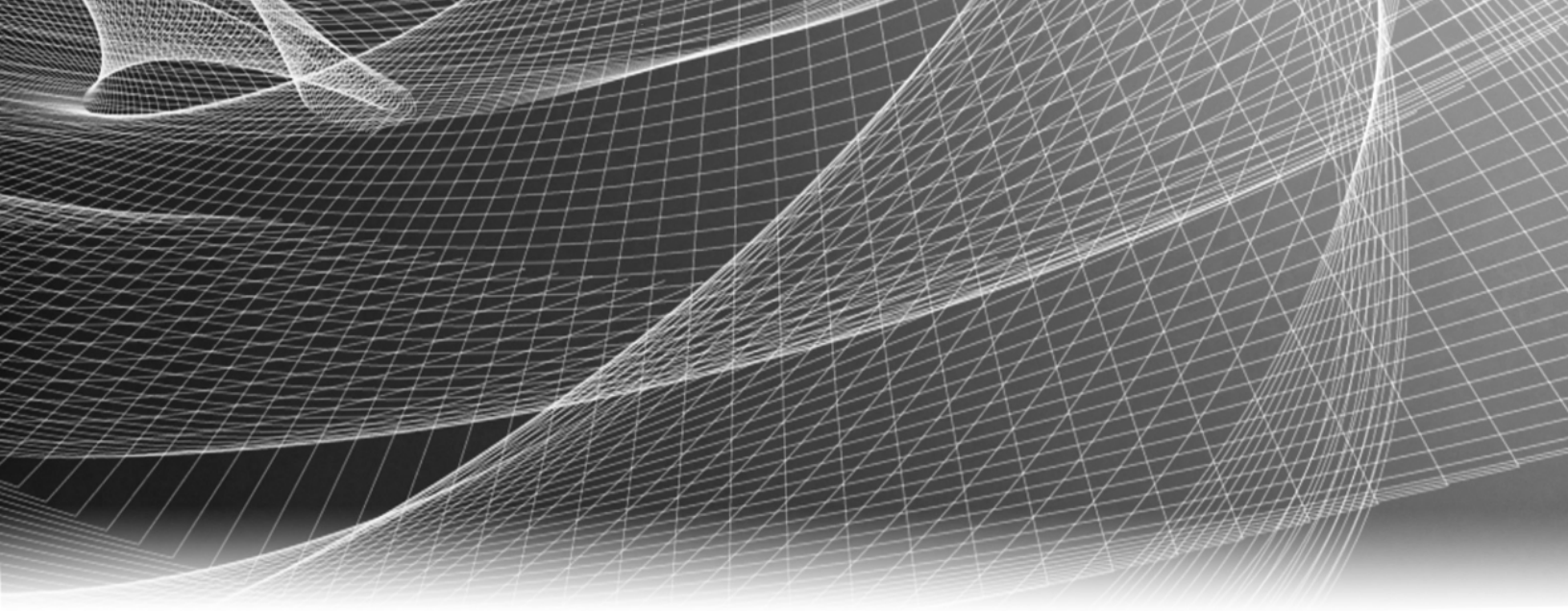


# RSA Security Analytics

## S4 RSA Analytics Warehouse（MapRベース）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.

# S4 RSA Analytics Warehouse（MapRベース）構成ガイド

RSA

# S4 RSA Analytics Warehouse（MapRベース）構成ガイド

## 概要

このドキュメントでは、RSA Analytics Warehouse (MapR)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。Warehouseは、以前にはSecurity Analytics Warehouse（SAW）と呼ばれていました。

## 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sadocs.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、Warehouseの構成を完了してください。

**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

# S4 Warehouseハードウェアの説明

## 概要

このトピックではRSA Series 4 Warehouse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 Warehouseには、出荷時にWarehouseソフトウェアがインストールされています。ネットワーク上でのWarehouse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. Warehouseハードウェアをマウントします。
3. Warehouseをネットワークに接続して、Warehouseのネットワーク パラメータを構成します。
4. Security AnalyticsでのWarehouse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、Warehouse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。

## パッケージの内容

Warehouse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 4 Warehouse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

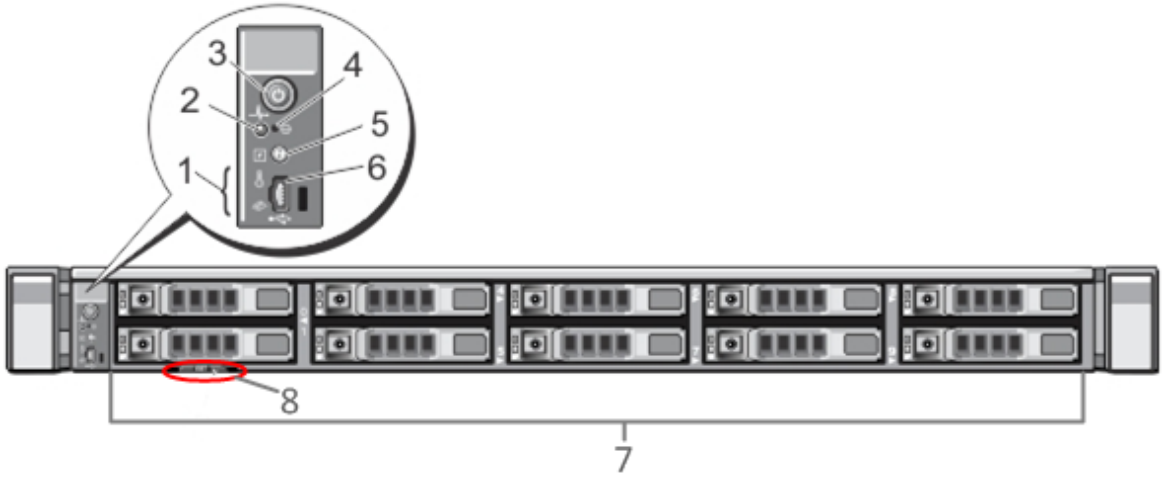
この構成手順を完了するには、以下の機材をご用意いただく必要があります。

- Ethernetネットワーク ケーブル2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


Last Modified: September 14 2016, 12:10PM

- 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

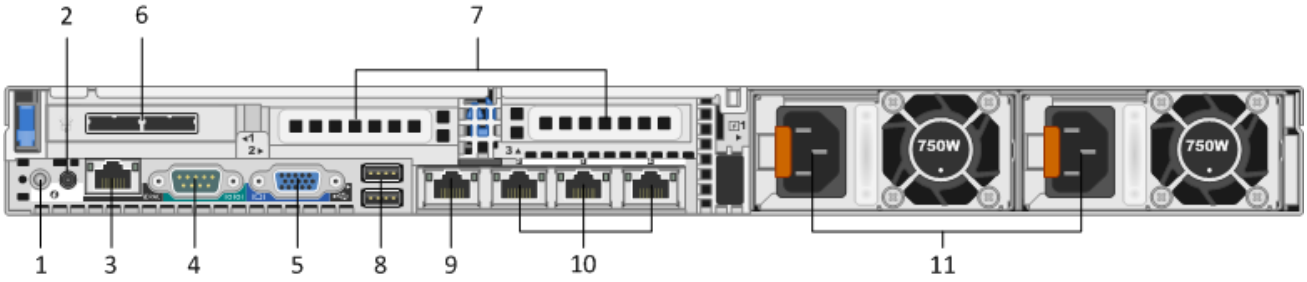
# Warehouseの前面




| 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。Warehouse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 |


Last Modified: September 14 2016, 12:10PM

# Warehouse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） |
| 6 | ネットワーク インタフェース 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。<br>• ファイバ/銅線10Gbpsネットワーク キャプチャ カード（RJ45）<br>• 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） |
| 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）：em 2～4 |
| 11 | ホット スワップ対応電源1および2 |


Last Modified: September 14 2016, 12:10PM

# Warehouse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、<br>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 |


Last Modified: September 14 2016, 12:10PM

RSA

# 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、RSA S4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。

RSA S4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アドレスとホスト名の設定、DNSサーバと**/etc/hosts**ファイルの構成を行い、ネットワーク クロック ソースを指定します。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。

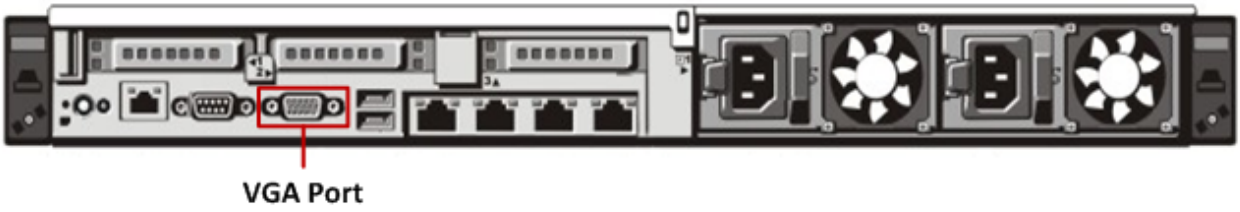
- VGA接続によるアプライアンス コンソール：キーボード（USBポート）とモニタ（VGAポート）を使用してアクセスします。
- ネットワーク接続によるアプライアンス コンソール：SSHクライアントが動作するコンピュータから、Ethernetケーブルでアプライアンスの管理ポート（em1）に接続してアクセスします。このポートはデフォルトで192.168.1.1に設定されています。

## VGA接続によるアプライアンス コンソール

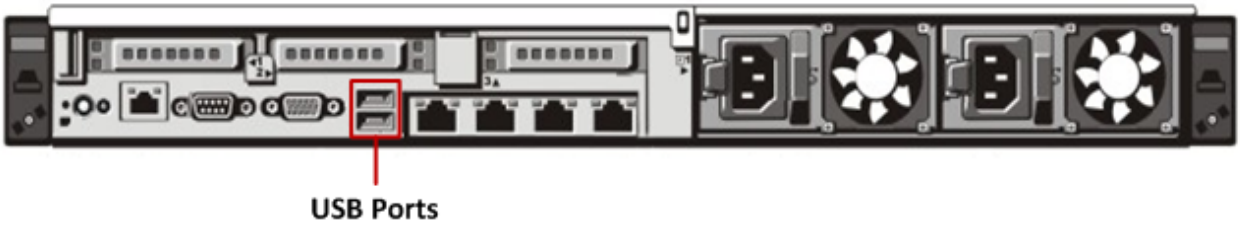
VGA接続でアプライアンス コンソールを使用するには、次の手順を実行します。


Last Modified: September 14 2016, 12:10PM

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。

> ⚠ **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。

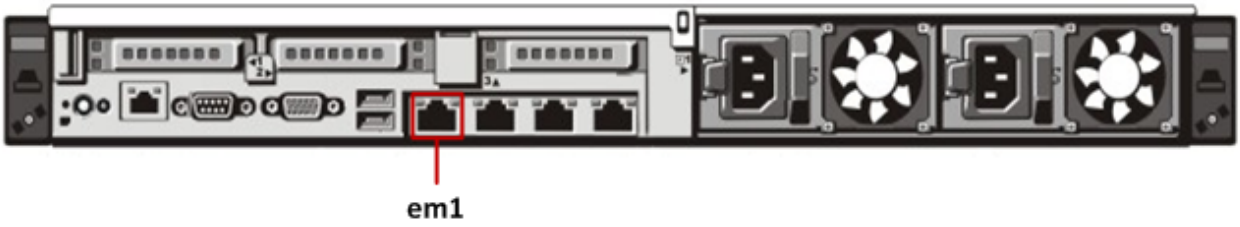
4. ログイン プロンプトで、デフォルトの認証情報 ( `root/netwitness` ) を使用してオペレーティング システムにアクセスします。
5. 後述の「**IPアドレスの設定**」セクションに進みます。

# ネットワーク接続によるアプライアンス コンソール

> ⚠ **Caution:** 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Ethernet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. 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. 後述の「**IPアドレスの設定**」セクションに進みます。

# IPアドレスの設定

Warehouseアプライアンスのネットワークは手動で構成する必要があります。Warehouseアプライアンスをクラスタ構成で設定する場合は、クラスタ内のすべてのアプライアンスで次のタスクを実行します。クラスタ内の各アプライアンスでは、アプライアンスのコンソールまたはDell Remote Access Console（iDRAC）のいずれかを使用してIPアドレスを構成する必要があります。iDRACについては、Dellのドキュメントを参照してください。

**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。

次に、構成する必要のあるネットワーク インタフェースを示します。

| インタフェース | 目的 |
|---|---|
| em1 | パブリック、組織内LANアクセス用スイッチへの接続 |
| em2 | プライベート、Warehouse専用スイッチへの接続 |
| em3 | オープン、いずれかのスイッチまたはネットワークに接続します |
| em4 | オープン、いずれかのスイッチまたはネットワークに接続します |

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。


Last Modified: September 14 2016, 12:10PM

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`
   ファイル内で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。例：eth0。 |
| BOOTPROTO | static |
| IPADDR | ネットワーク インタフェースのIPアドレス |
| 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`
4. （オプション）クラスタ内の他のWarehouseアプライアンスとの通信に専用の内部スイッチを経由する場合は、em2ネットワーク インタフェースを構成します。対応する構成ファイルは、**/etc/sysconfig/network-scripts/ifcfg-em2**です。

# 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。

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または変更します。
   `NETWORKING=[yes|no]`
   `HOSTNAME=<sawnode_hostname>`
   ここで、`<sawnode_hostname>`はWarehouseアプライアンスのホスト名です。
   `DOMAINNAME = <value>`


Last Modified: September 14 2016, 12:10PM

> **Note:** 構成するWarehouseノードのホスト名にドメイン名が必要な場合、DOMAINNAMEの値を設定します。 ドメイン名を使用しない場合は、この値は空白のままにします。

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. 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`
6. ホスト名が正しく設定されているかどうかを確認するために、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オンします。
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、クラスタ内の各WarehouseノードのIPアドレスとホスト名を追加します。

> **Caution:** Warehouseノードのホスト名に対して、ループバック アドレスを指定することはできません。

**/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オンします。
2. 次のコマンドを実行します。
   `vi /etc/hosts`
3. 各Warehouseノードについて次の行をファイルに追加します。
   `<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、Warehouseクラスタ内のノードのプライベート インタフェースに設定したIPアドレスです。
   <node_fqdn>は、Warehouseクラスタ内のノードの完全修飾ドメイン名です。


Last Modified: September 14 2016, 12:10PM

`<node_hostname>`は、Warehouseクラスタ内のノードのホスト名です。

**/etc/hosts**ファイルに、Warehouseクラスタ内のすべてのノードを記述します。

Warehouseクラスタ内のすべてのノードを記述した**/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 sawnode1.domainname.com sawnode1
192.168.1.11 sawnode2.domainname.com sawnode2
192.168.1.12 sawnode3.domainname.com sawnode3
```

4. 変更内容を保存して、viエディターを終了します。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、すべてのデバイ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、デバイ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。Warehouseアプライアンスの/etc/ntp.confを編集し、NTP（Network Time Protocol）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」で始ま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. サービスを再起動するため、次のコマンドを実行します。
   ```
   service ntpd restart
   ```

RSA

# Security AnalyticsでのWarehouse構成の完了

## 概要

このトピックでは、RSA Analytics Warehouse (MapR)の構成を完了するための手順について説明します。

## はじめに

Warehouseを構成するための最後のステップは次の手順で実行します。

1. アプライアンスのUUIDを生成してデフォルトのUUIDを更新します。
2. アプライアンスのHive Serverのバージョンを更新します。
3. Warehouseアプライアンスで構成テンプレート ファイルを更新します。
4. Warehouseライセンス ファイルをインストールします。
5. Warehouseアプライアンスの仮想IPアドレスを生成します。
6. Warehouse Connectorを構成し、Warehouseに対するデータの書き込みを開始します。
7. Reporting EngineにWarehouseデータ ソースを追加します。

詳細については、「*RSA Analytics Warehouse (MapR)構成ガイド*」（Security Analytics 10.4）または「*Security Analytics Warehouse構成ガイド*」（Security Analytics 10.3以前）」をオンライン ヘルプ（sadocs.emc.com/ja-jp）で参照してください。


Last Modified: September 14 2016, 12:10PM