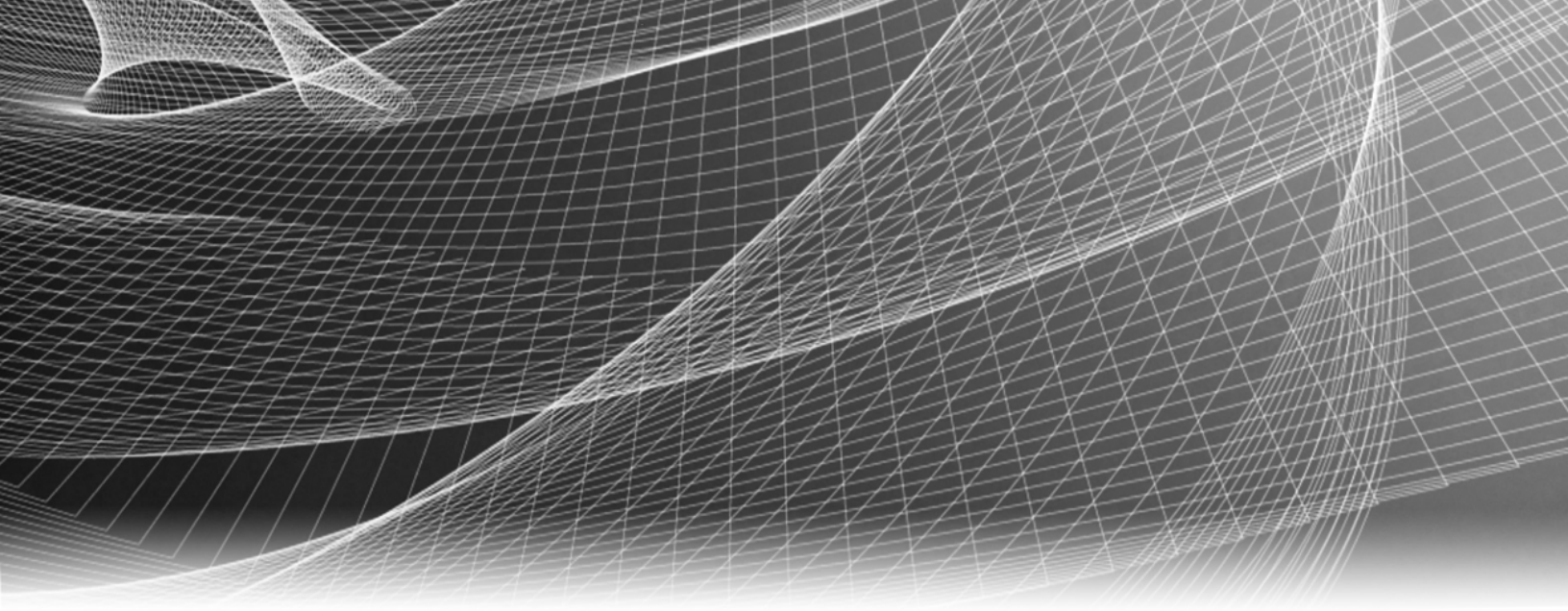


RSA Security Analytics

S4 Malware Analysis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.

S4 Malware Analysisアプライアンス構成ガイド

RSA

S4 Malware Analysis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 Security Analytics Malware Analysis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、Malware Analysisアプライアンスの構成を完了してください。

Last Modified: September 14 2016, 12:10PM

RSA

SA Malware Analysisアプライアンス ハードウェアの説明

概要

このトピックではRSA Series 4 Malware 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 Security Analytics Series 4 Malware Analysisアプライアンスには、出荷時にMalware AnalysisおよびBrokerソフトウェアがインストールされています。このBrokerは、Malware Analysis Server専用です。ネットワーク上でMalware Analysis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. 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. Malware Analysisアプライアンス ハードウェアをマウントします。
3. Malware Analysisアプライアンスをネットワークに接続して、Malware Analysis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。
4. Security AnalyticsでのMalware Analysisアプライアンス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、Malware Analysisアプライアンス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

Broker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 Malware 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

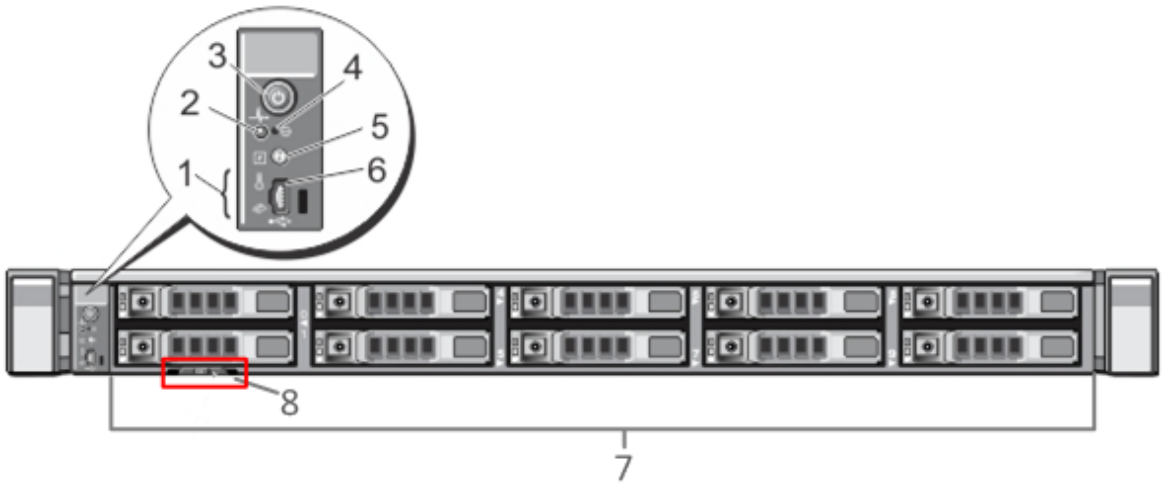
この構成手順を完了するには、以下の機材をご用意いただく必要があります。

- Ethernetネットワーク ケーブル1本

Last Modified: September 14 2016, 12:10PM

- 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

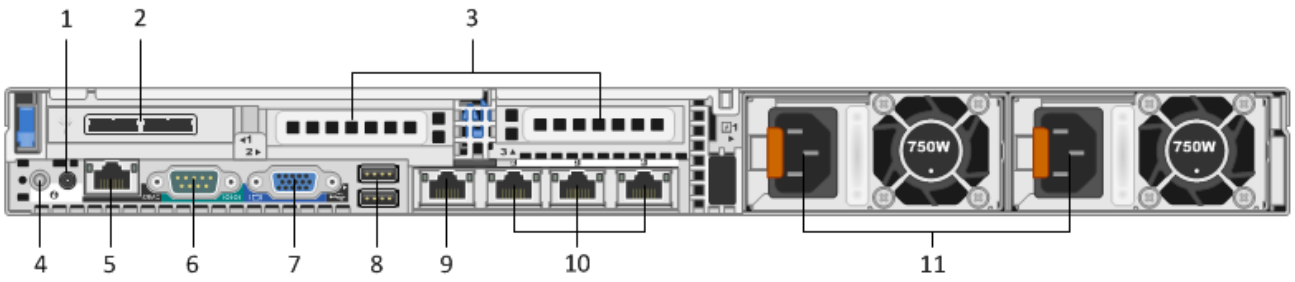
Malware Analysisアプライアンスの前面



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。Malware Analysisアプライアンスには、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

Malware Analysisアプライアンスの背面



番号	説明
1	システム識別ライト
2	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
3	オプション カード用拡張スロット
4	システム識別ボタン
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）
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

Malware 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	43.56ポンド
寸法（概算）	ベゼルあり：434.0mm（w）x 787.1mm（d）x 42.8mm（h） ベゼルなし：434.0mm（w）x 752.1mm（d）x 42.8mm（h）

Last Modified: September 14 2016, 12:10PM

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

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、Security Analytics 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 Security Analytics 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、ネットワーク クロック ソース、ホスト名、DNSサーバを設定します。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、NwConsoleプログラムを使用して、アプライアンスの管理設定を変更します。DNSサーバの構成では、OSのコマンド ラインを使用します。

方法	ユーザー名	デフォルトのパスワード
ssh/cli	root	netwitness
アプライアンス	admin	netwitness

初期接続は、次のいずれかの方法で行います。

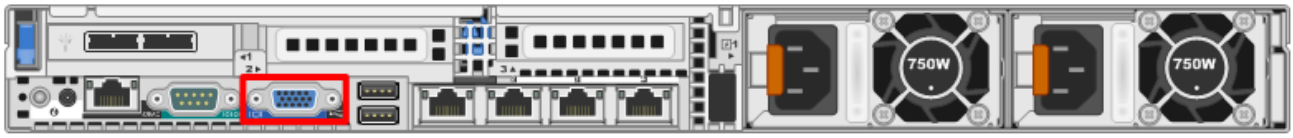
- VGA接続によるアプライアンス コンソール：キーボード（USBポート）とモニタ（VGAポート）を使用してアクセスします。
- ネットワーク接続によるアプライアンス コンソール：SSHクライアントが動作するコンピュータから、Ethernetケーブルでアプライアンスの管理ポート（em1）に接続してアクセスします。このポートはデフォルトで192.168.1.1に設定されています。

VGA接続によるアプライアンス コンソール

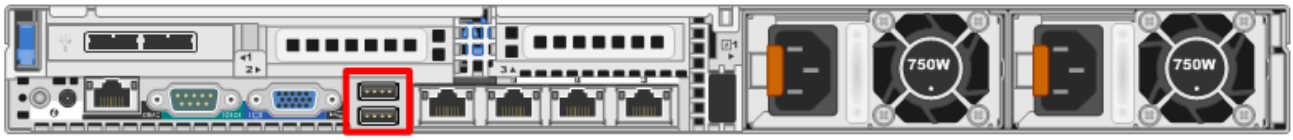
VGA接続でアプライアンス コンソールを使用するには、次の手順を実行します。

Last Modified: January 27 2017, 9:14AM

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。



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。

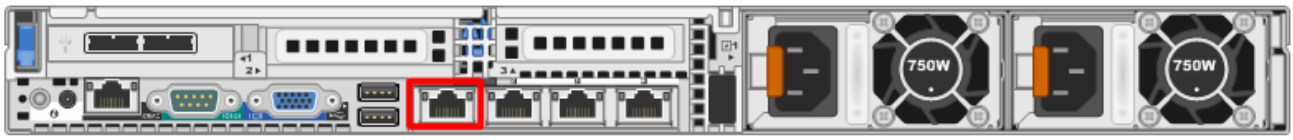
4. ログイン プロンプトで、デフォルトの認証情報（`root/netwitness`）を使用してオペレーティング システムにアクセスします。
5. 使用しているSecurity Analyticsソフトウェアのバージョンに応じて、「**ネットワーク パラメータの構成（10.3.x以前のアプライアンス）**」または「**ネットワーク パラメータの構成（10.4.x以降のアプライアンス）**」セクションに進みます。

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（em1）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。

Last Modified: September 14 2016, 12:10PM

> **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、rootとしてログオンし、オペレーティング システムにアクセスします。Security AnalyticsサーバのIPアドレスの入力を求めるプロンプトが表示されたら、**CTRL+C**キーを押して、プロンプトを終了します。
6. 使用しているSecurity Analyticsソフトウェアのバージョンに応じて、「**ネットワーク パラメータの構成 (10.3.x以前のアプライアンス)**」または「**ネットワーク パラメータの構成 (10.4.x以降のアプライアンス)**」セクションに進みます。

ネットワーク パラメータの構成 (10.3.x以前のアプライアンス)

10.3.x以前のアプライアンスについては、このセクションの手順に従って、ネットワーク パラメータを構成します。

IPアドレスの設定 (10.3.x以前)

次のいずれかの手順に従って、アプライアンスの管理IPアドレスを設定します。

固定IPの設定 (10.3.x以前)

固定IPアドレスを設定するには、次の手順を実行します。

1. rootプロンプト: `[root@NwAppliance~]#`
   で、次のコマンドを実行します。
   `NwConsole`
   NwConsoleが開始し、次のメッセージが表示されます。
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  All rights reserved.
   ```
2. NwConsoleで、次のコマンドを実行します。
   `login localhost:50006 <adminusername> <password>`
   例 : `login localhost:50006 admin netwitness`
   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、次のコマンドを実行します。
   `appliance setNet mode=static address=<desired IP address> netmask=<desired netmask> gateway=<desired network gateway>`
   例 : アプライアンスのem1インタフェースのIPアドレスをクラスCネットワークで10.1.2.35に設定し、ゲートウェイを10.1.2.1に設定するには、次のコマンドを実行します。
   `appliance setNet mode=static address=10.1.2.35 netmask=255.255.255.0 gateway=10.1.2.1`
   アプライアンスでネットワーク サービスが自動的に再開し、新しい設定が適用されます。
4. アプライアンスにネットワーク経由で接続している場合、構成手順を続行するには新しいIPアドレスを使用してアプライアンスに再接続する必要があります。新しいサブネットにアプライアンスを移動した場合は、クライアント ネットワークの変更も必要になることがあります。
5. NwConsoleからログアウトして終了するには、「**`exit`**」と入力します。

Last Modified: September 14 2016, 12:10PM

動的IPの設定 (10.3.x以前)

動的IPアドレスを設定するには、次の手順を実行します。

1. rootプロンプト : `[root@NwAppliance~]#`
   で、次のコマンドを実行します。
   `NwConsole`
   NwConsoleが開始し、次のメッセージが表示されます。
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  All rights reserved.
   ```
2. NwConsoleで、次のコマンドを実行します。
   `login localhost:50006 <username> <password>`
   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、次のコマンドを実行します。
   `appliance setNet mode=dhcp`
4. アプライアンスでネットワーク サービスが自動的に再開し、新しい設定が適用されます。アプライアンスにネットワーク経由で接続している場合、構成手順を続行するには新しいIPアドレスを使用してアプライアンスに再接続する必要があります。新しいサブネットにアプライアンスを移動した場合は、クライアント ネットワークの変更も必要になることがあります。

> ⚠ **Caution:** DHCPを選択した場合、新しいアドレスを確認できません。新しいアドレスを確認するには、アプライアンス コンソールに直接ログインして確認する必要があります。

ホスト名の設定 (10.3.x以前)

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。

1. まだNwConsoleにログインしている場合は、ステップ2および3はスキップします。
2. rootプロンプト: `[root@NwAppliance~]#`
   で、次のコマンドを実行します。
   `NwConsole`
   NwConsoleが開始し、次のメッセージが表示されます。
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  All rights reserved.
   ```
3. NwConsoleで、次のコマンドを実行します。
   `login localhost:50006 <username> <password>`
   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 #>
   ```
4. localhostプロンプト: `[localhost:50006] />`
   で、次のコマンドを実行します。

appliance hostname name=<desired_name_for_appliance>
例： **appliance hostname name=myserver**

5. 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。
6. 次のコマンドを使用してサーバを再起動します：**reboot**

> **Note:** ホスト名を変更した後、システムを再起動することを推奨します。

ネットワーク クロック ソースの指定 (10.3.x以前)

> **Note:** 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SAインタフェースから構成することができます。

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、すべてのサービスと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。

> **Note:** この手順のコマンドでは、大文字と小文字が区別されます。

ネットワーク クロック ソースを設定するには、次の手順を実行します。

1. まだNwConsoleにログインしている場合は、ステップ2および3はスキップします。
2. rootプロンプト：[root@NwAppliance~]#
で、次のコマンドを実行します。
NwConsole
NwConsoleが開始し、次のメッセージが表示されます。
```
RSA Security Analytics Console 10.2
Copyright 2001-2012, RSA Security Inc.  All rights reserved.
```
3. NwConsoleで、次のコマンドを実行します。
login localhost:50006 <username> <password>
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 #>
```
4. localhostプロンプト：[localhost:50006] />
で、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**
また、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**
5. 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。

DNSサーバの構成（10.3.x以前）

DNSサーバのアドレスを設定するには、次の手順を実行します。

1. rootプロンプト: `[root@NwAppliance~]#`
   で、次のコマンドを実行します。
   `vi /etc/resolv.conf`
2. 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`
3. 変更内容を保存して、vi工ディタを終了します。

ネットワーク パラメータの構成（10.4.x以降のアプライアンス）

初めてシステムを起動し、ログインすると、**netconfig.sh**を実行して、固定または動的なネットワーク構成を行うためのプロンプトが表示されます。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。初期構成の入力が完了すると、保存する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。

ネットワーク クロック ソースの指定 (10.4.x以降)

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。

> ⚠ **Caution:** 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。

次の手順のコマンドでは、大文字と小文字が区別されます。

ネットワーク クロック ソースを設定するには、次の手順を実行します。

1. まだNwConsoleにログインしている場合は、ステップ2および3はスキップします。
2. rootプロンプト：`[root@NwAppliance~]#`
   で、次のコマンドを実行します。
   `NwConsole`
   NwConsoleが開始し、次のメッセージが表示されます。
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  All rights reserved.
   ```


Last Modified: September 14 2016, 12:10PM

3. NwConsoleで、次のコマンドを実行します。
   login localhost:50006 <username> <password>
   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 #>
4. localhostプロンプト：[localhost:50006] />
   で、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**
   また、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**
5. 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。

DNSサーバの構成 (10.4.x以降)

DNSサーバのアドレスを設定するには、次の手順を実行します。

1. rootプロンプト: [root@NwAppliance~]#
   で、次のコマンドを実行します。
   vi /etc/resolv.conf
2. 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
3. 変更内容を保存して、viエディタを終了します。

Security AnalyticsサーバのIPアドレスの設定 (10.4.x以降)

Security AnalyticsサーバのIPアドレスを設定するには、次の手順を実行します。

1. 初期構成を完了した後、アプライアンスを再起動します。
2. rootとしてアプライアンスにログオンします。
3. プロンプトが表示されたら、Security AnalyticsサーバのIPアドレスを入力します。

Last Modified: September 14 2016, 12:10PM

RSA

Security AnalyticsでのMalware Analysisアプライアンス構成の完了

概要

このトピックでは、Security AnalyticsでのMalware Analysisアプライアンス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

Malware 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。以下の手順を実行します。

1. Security AnalyticsにMalware Analysisアプライアンス（およびサービス）とオンボードBrokerサービスを追加します。
2. Malware Analysisサービスにライセンス（エンタイトルメント）を適用します。
3. Malware Analysisを構成します。
4. （オプション）Malware Analysisサービスを調整して詳細なカスタマイズを行います。例として、カスタムYARAコンテンツの有効化があります。

詳細については、使用しているSecurity Analyticsバージョンの「*Malware Analysis構成ガイド*」および「*ライセンス ガイド*」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