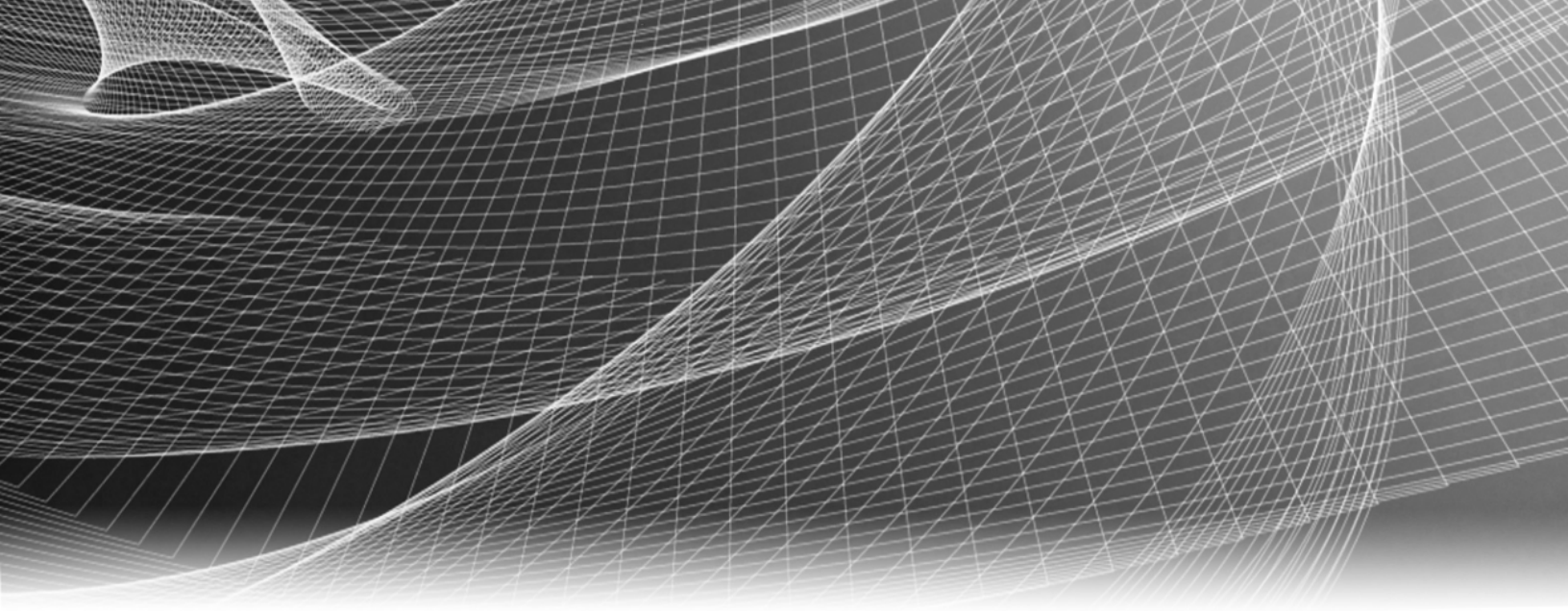


RSA Security Analytics

Guide de configuration de l'appliance Malware Analysis Appliance S4

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.

Guide de configuration de l'appliance Malware Analysis Appliance S4

RSA

Guide de configuration de l'appliance Malware Analysis Appliance S4

Présentation

Ce document est un guide étape par étape pour installer l'appliance RSA Security Analytics Malware et la connecter à votre réseau.

Contexte

Les instructions de configuration matérielle dans le présent document concernent uniquement le matériel. Elles ne s'appliquent pas à une version spécifique du logiciel Security Analytics. Une fois la configuration matérielle terminée, veuillez continuer l'installation et la configuration de l'appliance Malware Analysis, comme décrit dans la documentation en ligne Security Analytics sur le site sadocs.emc.com/fr-fr.

Last Modified: August 10 2016, 9:33AM

RSA

Description matérielle de l'appliance SA Malware Analysis Appliance

Présentation

Cette section présente l'appliance RSA Malware Analysis Appliance de la gamme 4 et fournit une description des contrôles et des connecteurs, ainsi que certaines caractéristiques.

Introduction

L'appliance Malware Analysis RSA Security Analytics de la gamme 4 est fournie avec Malware Analysis et le logiciel Broker installés. Ce Broker est pour le serveur d'analyse de malware uniquement. La configuration initiale d'une appliance Malware Analysis sur votre réseau comprend ces étapes :

1. Vérifiez les exigences relatives au site et les informations de sécurité.
2. Montez le matériel de l'appliance Malware Analysis.
3. Connectez l'appliance Malware Analysis à votre réseau et configurez les paramètres réseau sur l'appliance Malware Analysis.
4. Terminez la configuration de l'appliance Malware Analysis dans Security Analytics.

Il existe plusieurs options pour la première connexion physique à l'appliance Malware Analysis pour commencer la configuration des paramètres logiciels. Une fois connectée, la console de l'appliance Security Analytics est utilisée pour effectuer ces changements de configuration. Chaque étape est décrite en détail dans ce document.

Contenu de l'emballage

Vérifiez le contenu de la boîte d'emballage afin de vous assurer que vous avez reçu tous les éléments nécessaires pour installer et configurer votre Broker.

- Appliance Malware Analysis de la gamme 4
- Ensembles de glissières coulissantes (2)
- Cordon d'alimentation (2)

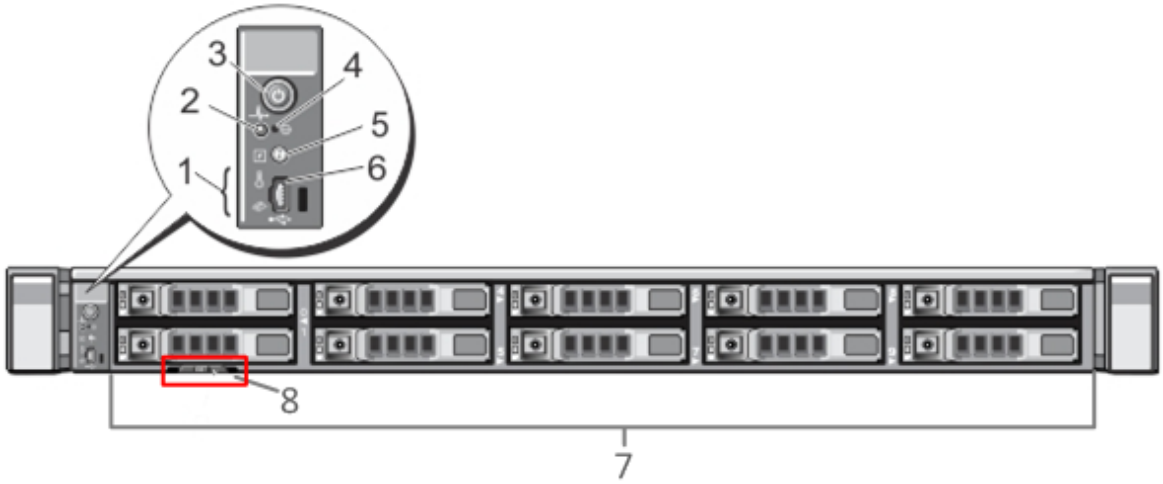
Matériel fourni par le client

Pour terminer la procédure de configuration, vous aurez besoin des éléments suivants :

Last Modified: August 10 2016, 9:33AM

- Un câble de réseau Ethernet
- Câbles pour la connexion d'un moniteur ou d'un adaptateur KVM au port VGA et d'un clavier ou d'un adaptateur KVM au port USB
- Outils standard d'installation et de montage du matériel informatique

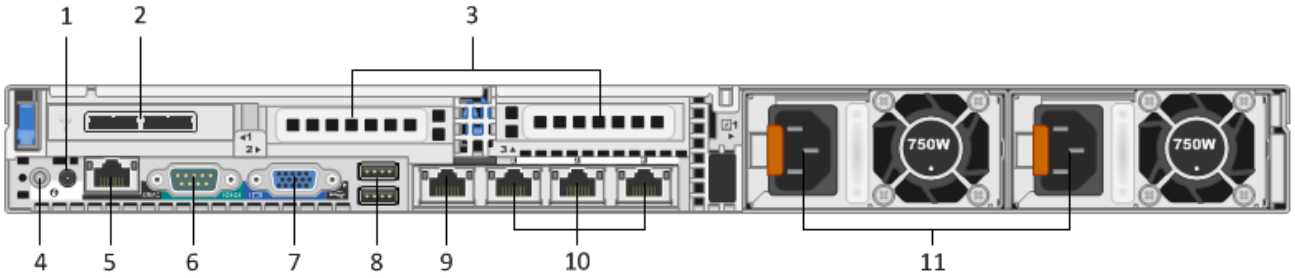
Vue avant de l'appliance d'analyse de malware



Clé	Description
1	Voyants de diagnostic
2	Voyant d'identification du système
3	Marche/Arrêt
4	Bouton d'interruption non masquable encastré
5	Bouton d'identification du système
6	Micro port USB
7	Dix baies de disque dur 2,5 pouces. Dix disques de 1 To sont installés sur l'appliance d'analyse de malware. Un module de carte SD interne est également présent, où sont installées deux cartes de 32 Go et où le système d'exploitation est installé par défaut.
8	Détails du libellé du service

Last Modified: August 10 2016, 9:33AM

Vue arrière de l'appliance Malware Analysis Appliance



Clé	Description
1	Voyant d'identification du système
2	Contrôleur SAS installé avec deux ports d'interface DAC pour la connexion aux baies de stockage de disque
3	Slots d'extension pour les cartes en option
4	Bouton d'identification du système
5	Port iDRAC
6	Port série RS232 (connexion série pour les ordinateurs portables via DB9 ou serveur série)
7	Port vidéo VGA (moniteur)
8	Ports USB (clavier)
9	Port Gigabit Ethernet 1 : em1 = port de gestion.
10	Ports Gigabit Ethernet (2-4) : em 2-4
11	Alimentation remplaçable à chaud 1 et 2

Spécifications de l'appliance Malware Analysis Appliance

Encombrement	1U, profondeur complète
Poids	20 kg
Dimensions (approximatives)	Avec panneau : 434 mm (l) x 787,1 mm (p) x 42,8 mm (h) Sans panneau : 434 mm (l) x 752,1 mm (p) x 42,8 mm (h)

Last Modified: August 10 2016, 9:33AM

Les alimentations	Remplaçables à chaud, redondant 750 W Autodétecteurs 100 à 240 V
Processeurs	Double six cœurs 2,66 GHz
RAM	96 Go

Last Modified: August 10 2016, 9:33AM

RSA

Montage de l'appliance et configuration des paramètres réseau

Présentation

Cette section fournit des instructions pour connecter une appliance Security Analytics S4 à votre réseau et configurer les paramètres de gestion initiaux sur l'appliance.

Introduction

Avant de commencer la configuration réseau, montez ou placez l'appliance en toute sécurité, conformément aux exigences du site.

La configuration des paramètres réseau pour une appliance RSA Security Analytics S4 inclut la définition de l'adresse IP par défaut, de la source d'horloge réseau et du nom d'hôte, puis la configuration de vos serveurs DNS. Pour définir ces paramètres, vous pouvez vous connecter à la console de l'appliance à l'aide d'un clavier et d'une souris ou de la connexion Ethernet. Dans les deux cas, connectez-vous à l'appliance en tant qu'utilisateur racine. Une fois en mesure de vous connecter à l'appliance, utilisez le programme NwConsole pour modifier les paramètres de gestion de l'appliance. Utilisez la ligne de commande du système d'exploitation pour configurer les serveurs DNS.

Méthode	Username	Default Password
SSH/cli	racine	netwitness
appliance	admin	netwitness

Choisissez l'une des méthodes suivantes pour la connexion initiale :

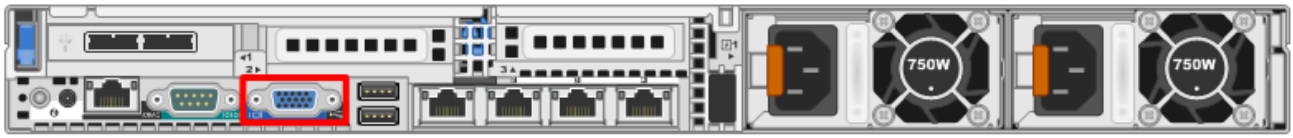
- Console de l'appliance via une connexion VGA : Clavier (port USB) et moniteur (port VGA).
- Console de l'appliance via une connexion réseau : ordinateur utilisant un client SSH connecté à l'appliance via un câble Ethernet pour le port de gestion (em1), qui est configuré sur 192.168.1.1 par défaut.

Console de l'appliance via une connexion VGA

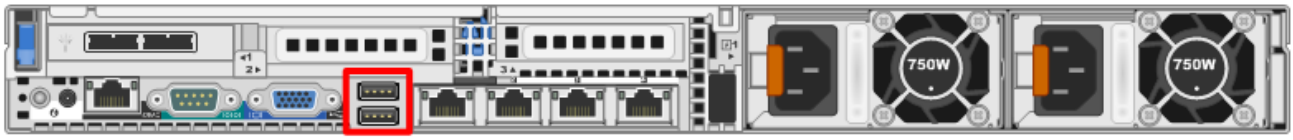
Pour utiliser la console de l'appliance via une connexion VGA :

Last Modified: August 10 2016, 9:33AM

1. Connectez un moniteur ou un adaptateur KVM au port VGA à l'arrière de l'appliance.



2. Connectez un clavier ou un adaptateur KVM à l'un des ports USB à l'arrière de l'appliance.



3. Connectez un câble d'alimentation à chacune des deux alimentations à l'arrière de l'appliance. Connectez les câbles d'alimentation à une source d'alimentation. Pour fournir une configuration plus robuste, connectez chaque alimentation à un circuit différent.

> ⚠ **Caution:** Une alimentation auxiliaire de 5 V est active chaque fois que le système est branché. Pour couper l'alimentation du système, vous devez débrancher les deux câbles d'alimentation CA de la source d'alimentation

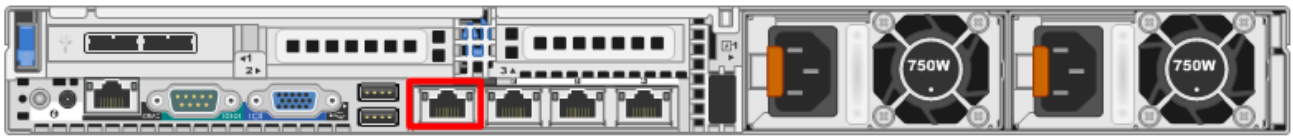
4. À l'invite de connexion, utilisez les informations d'identification par défaut pour accéder au système d'exploitation (`root/netwitness`).
5. Passez à la section **Configurer les paramètres réseau (appliances 10.3.x et versions antérieures)** ou à la section **Configurer les paramètres réseau (appliances 10.4.x et version ultérieure)**, en fonction de la version de votre logiciel Security Analytics.

Console de l'appliance via une connexion réseau

> ⚠ **Caution:** L'adresse IP par défaut de l'appliance est définie en usine sur 192.168.1.1. L'utilisation de 192.168.1.1 est assez courante et l'adresse IP est peut-être déjà dans le fichier SSH known_hosts de votre système. Il est possible que la ligne spécifique pour cette adresse doive être supprimée.

Pour utiliser la console de l'appliance via une connexion réseau :

1. Connectez un câble Ethernet entre un ordinateur et le port de gestion Ethernet (em1) à l'arrière de l'appliance.



2. Connectez les cordons d'alimentation aux connecteurs d'alimentation de l'appliance et du réceptacle d'alimentation.
3. L'adresse IP par défaut de l'appliance est définie en usine sur 192.168.1.1. Par conséquent, définissez l'adresse IP du système client sur le même sous-réseau. Par exemple, définissez votre ordinateur portable sur 192.168.1.15 avec la passerelle par défaut de 192.168.1.1, puis à l'aide d'un client secure shell (SSH) connectez-vous à l'appliance.

Last Modified: August 10 2016, 9:33AM

> **Note:** Gardez à l'esprit que si vous modifiez les paramètres réseau tout en étant connecté via SSH, votre session SSH sera abandonnée et vous devrez vous reconnecter à la nouvelle adresse de l'appliance.

4. Acceptez la clé SSH.
5. À l'invite de connexion, connectez-vous en tant qu'utilisateur racine pour pouvoir accéder au système d'exploitation. Si vous recevez une invite pour saisir l'adresse IP pour le serveur Security Analytics, appuyez sur **CTRL+C** pour quitter l'invite.
6. Passez à la section **Configurer les paramètres réseau (appliances 10.3.x et versions antérieures)** ou à la section **Configurer les paramètres réseau (appliances 10.4.x et version ultérieure)**, en fonction de la version de votre logiciel Security Analytics.

Configurer les paramètres réseau (appliances 10.3.x et versions antérieures)

Suivez les procédures décrites dans cette section pour configurer les paramètres réseau pour les appliances 10.3.x et versions antérieures.

Définir l'adresse IP (10.3.x et versions antérieures)

Utilisez l'une des procédures ci-dessous pour définir l'adresse IP de gestion sur l'appliance.

Définir une adresse IP statique (10.3.x et versions antérieures)

Pour définir une adresse IP statique :

1. À l'invite racine : `[root@NwAppliance~]#`
   saisissez la commande suivante :
   `NwConsole`
   NwConsole démarre et le message suivant s'affiche :
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  Tous droits réservés.
   ```
2. Dans NwConsole, saisissez la commande suivante :
   `login localhost:50006 <adminusername> <password>`
   Par exemple : `login localhost:50006 admin netwitness`
   Vous êtes connecté à l'appliance et le message suivant s'affiche :
   `Est connecté avec succès en tant que session <session #>`
3. À l'invite de l'hôte local : `[localhost:50006] />`
   saisissez la commande suivante :
   `appliance setNet mode=static address=<desired IP address> netmask=<desired netmask> gateway=<desired network gateway>`
   Par exemple : Pour définir l'adresse IP de l'interface em1 de l'appliance sur 10.1.2.35 pour un réseau de classe C avec la passerelle 10.1.2.1, exécutez la commande suivante :
   `appliance setNet mode=static address=10.1.2.35 netmask=255.255.255.0 gateway=10.1.2.1`
   Les services réseau redémarrent automatiquement sur l'appliance et les nouveaux paramètres sont appliqués.
4. Si l'appliance est connectée via une connexion réseau, vous devrez vous reconnecter à l'appliance à l'aide de la nouvelle adresse IP pour continuer. Si vous avez déplacé l'appliance vers un nouveau sous-réseau, les modifications apportées au client de mise en réseau peuvent également être requises.
5. Pour se déconnecter et quitter NwConsole, saisissez **`exit`**.

Last Modified: August 10 2016, 9:33AM

Définir une adresse IP dynamique (10.3.x et versions antérieures)

Pour définir une adresse IP dynamique :

1. À l'invite racine : `[root@NwAppliance~]#`
   saisissez la commande suivante :
   `NwConsole`
   NwConsole démarre et le message suivant s'affiche :
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  Tous droits réservés.
   ```
2. Dans NwConsole, saisissez la commande suivante :
   `login localhost:50006 <username> <password>`
   Vous êtes connecté à l'appliance et le message suivant s'affiche :
   ```
   Est connecté avec succès en tant que session <session #>
   ```
3. À l'invite de l'hôte local : `[localhost:50006] />`
   saisissez la commande suivante :
   `appliance setNet mode=dhcp`
4. Les services réseau redémarrent automatiquement sur l'appliance et les nouveaux paramètres sont appliqués. Si l'appliance est connectée via une connexion réseau, vous devrez vous reconnecter à l'appliance à l'aide de la nouvelle adresse IP pour continuer. Si vous avez déplacé l'appliance vers un nouveau sous-réseau, les modifications apportées au client de mise en réseau peuvent également être requises.

> ⚠ **Caution:** Si vous sélectionnez DHCP, il peut n'y avoir aucun moyen de déterminer la nouvelle adresse. Vous devez vous connecter à la console d'appliance directement afin de déterminer la nouvelle adresse.

Définir le nom d'hôte (10.3.x et versions antérieures)

La création du nom d'hôte du système est une tâche relativement simple, mais il peut être profitable de la prendre en considération pour limiter les problèmes courants. Si vous recherchez des conseils pour choisir un nom d'hôte, reportez-vous à la RFC 1178. En termes de Security Analytics les bases de données sur les appliances sont associées au nom d'hôte. Si la collecte ou l'agrégation a commencé (c'est pour cette raison qu'elle n'est pas activée par défaut), alors la base de données est créée et si vous modifiez le nom d'hôte après que cela se produit correctement, cela crée une deuxième base de données. Le nom d'hôte doit uniquement comporter des caractères alphanumériques (pas de caractères spéciaux tels que #, _, @, -) afin d'éliminer les problèmes de communication.

1. Si toujours connecté à NwConsole, alors ignorez les étapes 2 et 3.
2. À l'invite racine : `[root@NwAppliance~]#`
   saisissez la commande suivante :
   `NwConsole`
   NwConsole démarre et le message suivant s'affiche :
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  Tous droits réservés.
   ```
3. Dans NwConsole, saisissez la commande suivante :
   `login localhost:50006 <username> <password>`
   Vous êtes connecté à l'appliance et le message suivant s'affiche :
   ```
   Est connecté avec succès en tant que session <session #>
   ```


Last Modified: August 10 2016, 9:33AM

4. À l'invite de l'hôte local : `[localhost:50006] />`
   saisissez la commande suivante :
   `appliance hostname name=<desired_name_for_appliance>`
   Par exemple : **`appliance hostname name=myserver`**
5. Lorsque le résultat est `Success`, saisissez **`exit`** pour vous déconnecter, puis quittez le programme NwConsole.
6. Redémarrer le serveur à l'aide de la commande suivante : **`reboot`**

> **Note:** Il est recommandé de redémarrer le système après avoir modifié le nom d'hôte.

Spécifier la source d'horloge réseau (10.3.x et versions antérieures)

> **Note:** Si le serveur NTP n'est pas configuré ou accessible à ce stade, la configuration de la source d'horloge réseau échouera, mais elle peut être effectuée à partir de l'interface SA ultérieurement.

Il est recommandé que tous les systèmes de la suite Security Analytics soient synchronisés à l'aide d'une source d'heure réseau afin que tous les services et toutes les appliances indiquent avec précision la même heure. Si cela n'est pas fait, alors l'heure sur les appliances peut ne pas être synchronisée, entraînant des requêtes pour une heure spécifique qui ne renvoient pas les résultats attendus.

> **Note:** Les commandes dans ces instructions sont sensibles à la casse.

Pour définir la source d'horloge réseau :

1. Si toujours connecté à NwConsole, alors ignorez les étapes 2 et 3.
2. À l'invite racine : `[root@NwAppliance~]#`
   saisissez la commande suivante :
   `NwConsole`
   NwConsole démarre et le message suivant s'affiche :
   `RSA Security Analytics Console 10.2`
   `Copyright 2001-2012, RSA Security Inc.  Tous droits réservés.`
3. Dans NwConsole, saisissez la commande suivante :
   `login localhost:50006 <username> <password>`
   Vous êtes connecté à l'appliance et le message suivant s'affiche :
   `Est connecté avec succès en tant que session <session #>`
4. À l'invite de l'hôte local : `[localhost:50006] />`
   saisissez la commande suivante :
   `appliance setNTP source=<NTP_server_hostname or IP_address>`
   Par exemple : **`appliance setNTP source=0.pool.ntp.org`**
   Ou, si vous souhaitez utiliser l'horloge de l'appliance comme source d'horloge, saisissez : **`appliance setNTP source=local`**
5. Lorsque le résultat de la commande est `Success`, saisissez **`exit`** pour vous déconnecter, puis quittez le programme NwConsole.

> **Note:** Si vous avez spécifié une source d'horloge NTP locale, l'horloge de l'appliance constitue la source de l'horloge et l'heure est configurée à l'aide de Définir l'horloge intégrée de l'appliance, comme décrit dans l'aide en ligne Security Analytics.

Last Modified: August 10 2016, 9:33AM

Configurer les serveurs DNS (10.3.x et versions antérieures)

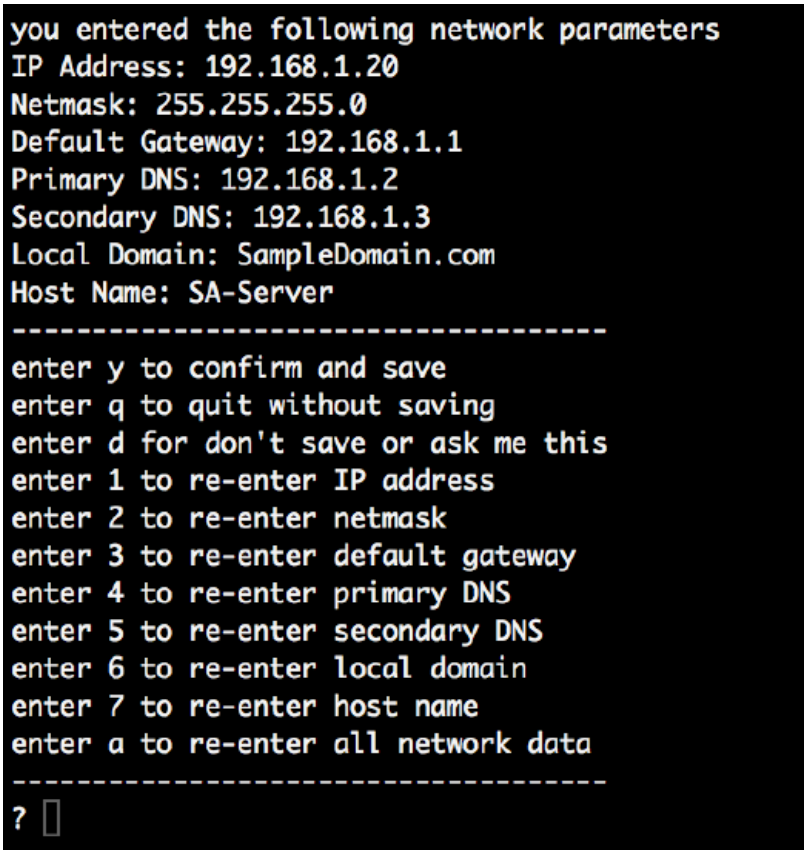
Pour définir l'adresse IP du serveur DNS :

1. À l'invite racine : `[root@NwAppliance~]#`
   saisissez la commande suivante :
   `vi /etc/resolv.conf`
2. Ajoutez les lignes suivantes au fichier pour chaque serveur DNS :
   `nameserver <DNS_server_ip_address>`
   `search <domain_name>`
   où `<DNS_server_ip_address>` est l'adresse IP de votre serveur DNS, et `<domain_name>` est le nom du domaine.
   Par exemple :
   ```
   nameserver 192.168.0.1
   search acmecorp.com
   ```
3. Enregistrez les modifications et quittez l'éditeur vi.

Configurer les paramètres réseau (appliances 10.4.x et version ultérieure)

Lors du démarrage et de la connexion au système pour la première fois, vous êtes invité à exécuter **netconfig.sh** afin de rationaliser la configuration des deux configurations réseau statique ou dynamique. Si vous ne recevez pas d'invite, vous pouvez exécuter `#netconfig.sh` à partir de la ligne de commande pour vous inviter à saisir les options de configuration. Au terme de la configuration initiale, vous devez voir une invite à enregistrer, comme illustré sur la figure suivante.

Last Modified: August 10 2016, 9:33AM



Spécifier la source d'horloge réseau (10.4.x et versions ultérieures)

Si le serveur NTP n'est pas configuré ou accessible à ce stade, la configuration de la source d'horloge réseau échouera, mais elle peut être effectuée à partir de l'interface Security Analytics ultérieurement.

> ⚠ **Caution:** La configuration de la synchronisation horaire entre les appliances et les services est obligatoire. Il est vivement recommandé d'utiliser une source d'heure NTP pour la synchronisation. Non seulement l'heure est essentielle pour les communications sous-jacentes entre les services, mais si les appliances ne sont pas synchronisées, cela peut entraîner une non-concordance des heures indiquées lors de l'analyse des données.

Les commandes dans les instructions suivantes sont sensibles à la casse.

Pour définir la source d'horloge réseau :

1. Si toujours connecté à NwConsole, alors ignorez les étapes 2 et 3.
2. À l'invite racine : `[root@NwAppliance~]#`
   saisissez la commande suivante :
   `NwConsole`
   NwConsole démarre et le message suivant s'affiche :
   `RSA Security Analytics Console 10.2`
   `Copyright 2001-2012, RSA Security Inc.  Tous droits réservés.`

Last Modified: August 10 2016, 9:33AM

3. Dans NwConsole, saisissez la commande suivante :
   login localhost:50006 <username> <password>
   Vous êtes connecté à l'appliance et le message suivant s'affiche :
   Est connecté avec succès en tant que session <session #>
4. À l'invite de l'hôte local : [localhost:50006] />
   saisissez la commande suivante :
   appliance setNTP source=<NTP_server_hostname or IP_address>
   Par exemple : **appliance setNTP source=0.pool.ntp.org**
   Ou, si vous souhaitez utiliser l'horloge de l'appliance comme source d'horloge, saisissez : **appliance setNTP source=local**
5. Lorsque le résultat de la commande est Success, saisissez **exit** pour vous déconnecter, puis quittez le programme NwConsole.

> **Note:** Si vous avez spécifié une source d'horloge NTP locale, l'horloge de l'appliance constitue la source de l'horloge et l'heure est configurée à l'aide de Définir l'horloge intégrée de l'appliance, comme décrit dans l'aide en ligne Security Analytics.

Configurer les serveurs DNS (10.4.x et versions ultérieures)

Pour définir l'adresse IP du serveur DNS :

1. À l'invite racine : [root@NwAppliance~]#
   saisissez la commande suivante :
   vi /etc/resolv.conf
2. Ajoutez les lignes suivantes au fichier pour chaque serveur DNS :
   nameserver <DNS_server_ip_address>
   search <domain_name>
   où <DNS_server_ip_address> est l'adresse IP de votre serveur DNS, et <domain_name> est le nom du domaine.
   Par exemple :
   nameserver 192.168.0.1
   search acmecorp.com
3. Enregistrez les modifications et quittez l'éditeur vi.

Définir l'adresse IP du serveur du serveur Security Analytics (10.4.x et versions ultérieures)

Pour définir l'adresse IP du serveur Security Analytics :

1. Après avoir terminé la configuration initiale, redémarrez l'appliance.
2. Connectez-vous à l'appliance en tant qu'utilisateur racine.
3. À l'invite, entrez l'adresse IP du serveur Security Analytics.

Last Modified: August 10 2016, 9:33AM

RSA

Fin de la configuration de l'appliance Malware Analysis Appliance dans Security Analytics

Présentation

Cette section fournit des instructions pour terminer la configuration de l'appliance Malware Analysis dans Security Analytics.

Introduction

Les dernières étapes de configuration de l'appliance Malware Analysis sont effectuées à l'aide de Security Analytics. Elles sont les suivantes :

1. Ajoutez l'appliance Malware Analysis (et service) et le service Broker intégré à Security Analytics.
2. Appliquez une licence (ou habilitation) au service Malware Analysis.
3. Configurez l'analyse de malware.
4. (Facultatif) Réglez Malware Analysis Service et implémentez la personnalisation avancée. Par exemple, activez le contenu YARA personnalisé.

Pour obtenir des instructions détaillées, consultez le *Guide de Configuration de l'analyse de malware* et le *Guide d'octroi de licence*de votre version de Security Analytics dans l'aide en ligne à l'adresse sadocs.emc.com/fr-fr.

Last Modified: August 10 2016, 9:33AM