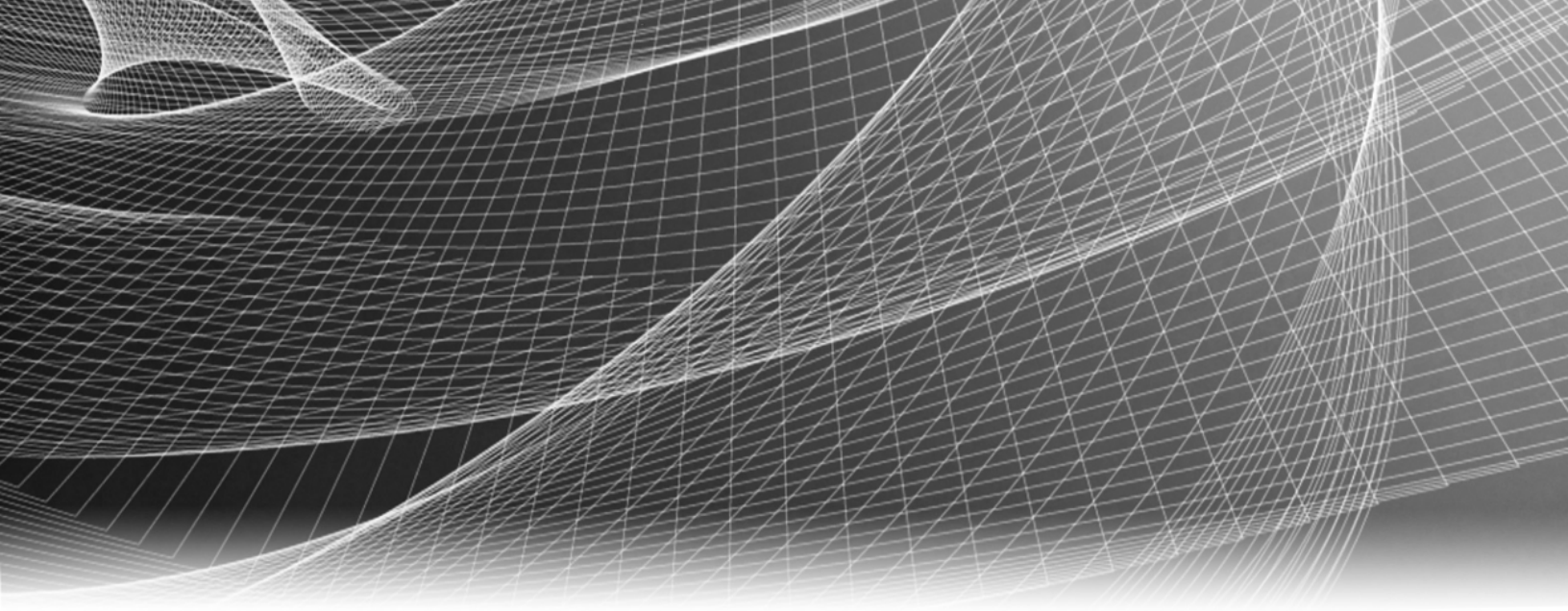


RSA Security Analytics

Guide de configuration du Decoder 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 du Decoder S4

RSA

Guide de configuration du Decoder S4

Présentation

Ce document est un guide étape par étape pour installer le RSA Security Analytics Decoder et le 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, continuez l'installation et la configuration de l'Archiver, comme décrit dans la documentation en ligne Security Analytics, qui est accessible via l'option **Aide** de Security Analytics et à l'adresse sadocs.emc.com/fr-fr.

Last Modified: August 10 2016, 9:33AM

RSA

Description matérielle du Decoder SA

Présentation

Ce document présente le RSA Security Analytics Decoder et la procédure générale pour installer le Decoder et le connecter à votre réseau et à votre stockage.

Introduction

L'appliance RSA Security Analytics Decoder de la gamme 4 est fournie avec le logiciel Decoder installé. La configuration initiale d'un Decoder sur votre réseau comprend ces étapes :

1. Vérifiez les exigences relatives au site et les informations de sécurité.
2. Montez le matériel du Decoder.
3. Connectez le Decoder à votre réseau et configurez les paramètres réseau sur le Decoder.
4. Connectez le Decoder au périphéroque DAC ou SAN, comme décrit dans le Guide de configuration du DAC de la gamme 4.
5. Terminez la configuration du Decoder dans Security Analytics.

Il existe plusieurs options pour la première connexion physique au Decoder 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 RSA Decoder.

- Appliance de Decoder S4
- Ensembles de glissières coulissantes (2)
- Cordon d'alimentation (2)

Matériel fourni par le client

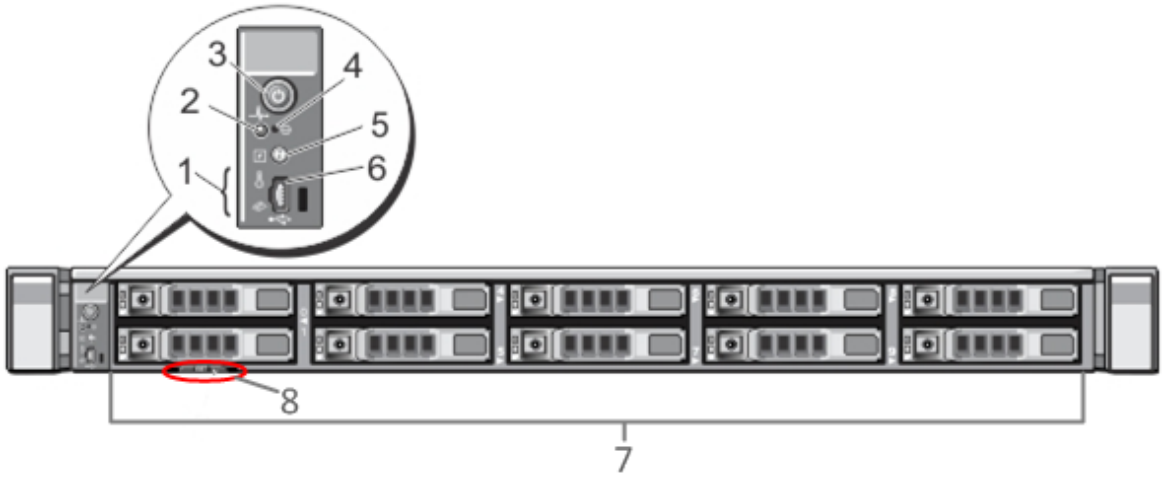
Pour terminer la procédure de configuration, vous aurez besoin des éléments suivants :

- Plusieurs câbles de réseau Ethernet (un pour la gestion et un pour chaque interface de capture)

Last Modified: August 10 2016, 9:33AM

- 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

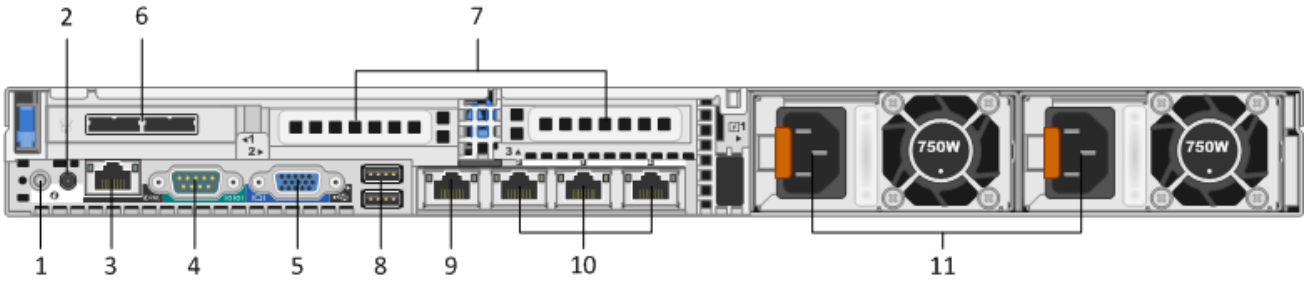
Vue avant du Decoder



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. Deux disques de 146 Go et deux disques de 1 To sont installés sur le Decoder. 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 du Decoder



Clé	Description
1	Bouton d'identification du système
2	Voyant d'identification du système
3	Port iDRAC
4	Port série RS232 (connexion série pour les ordinateurs portables via DB9 ou serveur série)
5	Port vidéo VGA (moniteur)
6	Slot des cartes d'interface réseau : Contrôleur SAS installé avec deux ports d'interface DAC pour la connexion aux baies de stockage de disque.
7	Slots d'extension de la carte d'interface réseau pour les cartes supplémentaires. Les options possibles sont les suivantes : • Carte de capture réseau 10 Gbit/s fibre/cuivre (RJ45) • Adaptateur de bus hôte Fibre channel (HBA) utilisé pour se connecter à un réseau SAN
8	Ports USB (clavier)
9	Port Gigabit Ethernet 1 : em1 = port de gestion
10	Ports Gigabit Ethernet (2-4) : em2-4 = surveillance des ports
11	Alimentation remplaçable à chaud 1 et 2

Caractéristiques techniques de Decoder

Encombrement	1U, profondeur complète

Last Modified: August 10 2016, 9:33AM

Poids	17,69 kg
Dimensions	48,23 cm (l) x 77,19 cm (p) x 4,26 cm (h)
Alimentation	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.

⚠ **Caution:** Si vous installez un système DAC, vous devez installer le DAC avant d'octroyer une licence au périphérique et de démarrer les services. Reportez-vous au **Guide d'octroi de licence Security Analytics** disponible via l'option **Aide** Security Analytics et au site sadocs.emc.com/fr-fr pour obtenir des instructions sur l'octroi de licence d'appliances.

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 :

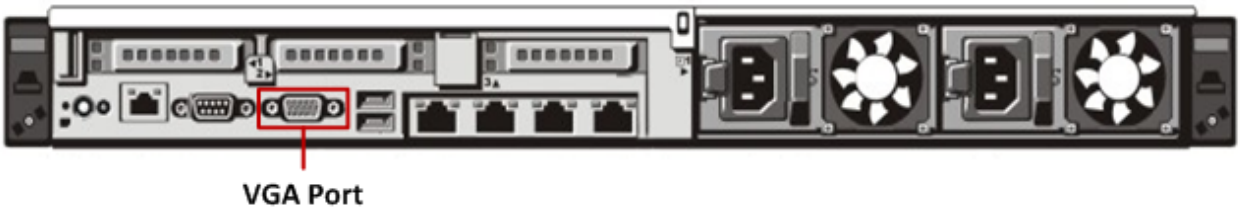
- Console de l'appliance via une connexion VGA : Clavier (Port USB) et moniteur (Port VGA).
- Console de l'appliance via une connexion réseau : ordinateur utilisant un client SSH connecté à l'appliance via un câble Ethernet pour le port de gestion (em1), qui est configuré sur 192.168.1.1 par défaut.

Last Modified: August 10 2016, 9:33AM

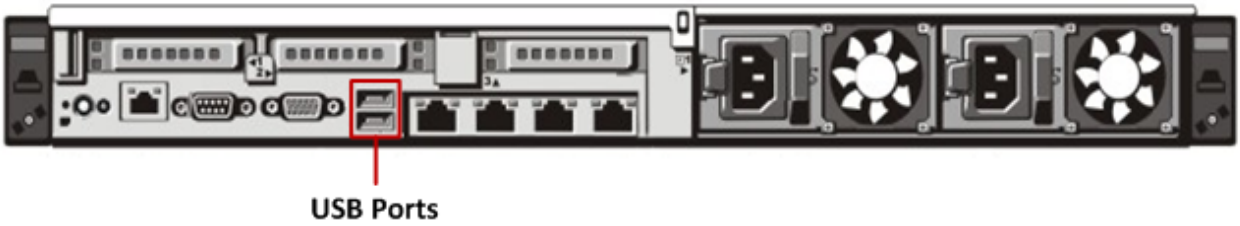
Console de l'appliance via une connexion VGA

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

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 **Définir l'adresse IP** ci-dessous.

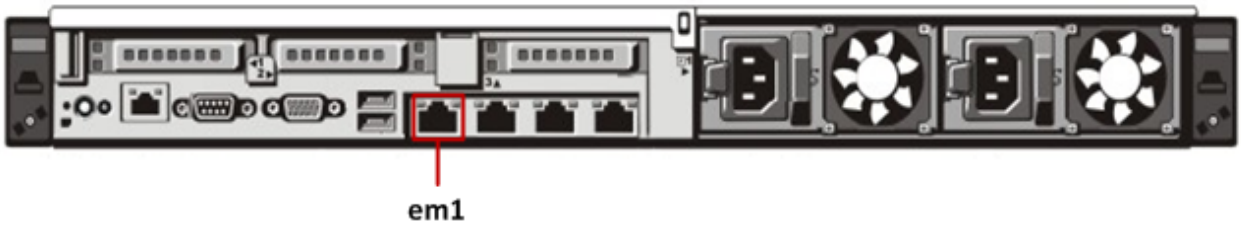
Console de l'appliance via une connexion réseau

> ⚠ **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 de votre système SSH known_hosts. Il est possible que la ligne spécifique pour cette adresse doive être supprimée.

Last Modified: August 10 2016, 9:33AM

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 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.

> **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, utilisez les informations d'identification par défaut pour accéder au système d'exploitation.
6. Passez à la section **Définir l'adresse IP** ci-dessous.

Définir l'adresse IP

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

Définir une adresse IP statique

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>`

Last Modified: August 10 2016, 9:33AM

- 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`**.

Définir une adresse IP dynamique

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 le périphérique 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

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.

Last Modified: August 10 2016, 9:33AM

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 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 de l'horloge réseau

> **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 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>`

Last Modified: August 10 2016, 9:33AM

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

Pour définir une adresse IP statique :

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.

RSA

Fin de la configuration du Decoder dans Security Analytics

Présentation

Cette section fournit des instructions pour terminer la configuration de Decoder et pour commencer l'agrégation dans Security Analytics.

Introduction

Caution: Avant de commencer la configuration finale dans Security Analytics, vous devez exécuter le script d'initialisation du DAC pour configurer la première baie de stockage, comme décrit dans le Guide de configuration du DAC de la gamme 4.

Les dernières étapes de configuration du Decoder sont effectuées à partir du serveur Security Analytics. Elles sont les suivantes :

1. Ajoutez le Decoder à Security Analytics dans la vue Périphériques.
2. Appliquez une licence de périphérique (ou des habilitations) au Decoder.
3. Configurez les sources et les analyseurs.
4. Configurez et démarrez la capture.
5. Ajoutez un ou plusieurs Decoder à un Concentrator en tant que périphériques agrégés.

Plusieurs de ces étapes peuvent être effectuées uniquement lorsque les autres parties du réseau Security Analytics sont en place :

- À l'étape 2, les licences de périphérique Security Analytics (ou les habilitations) doivent être disponibles pour activer les périphériques.
- À l'étape 5, au moins un service Concentrator doit être installé, sous licence, configuré et capturant des données afin de générer des métadonnées que le Decoder peut agréger.

Connectez-vous à Security Analytics et suivez les instructions dans l'aide en ligne pour terminer la configuration du Decoder.

Last Modified: August 10 2016, 9:33AM