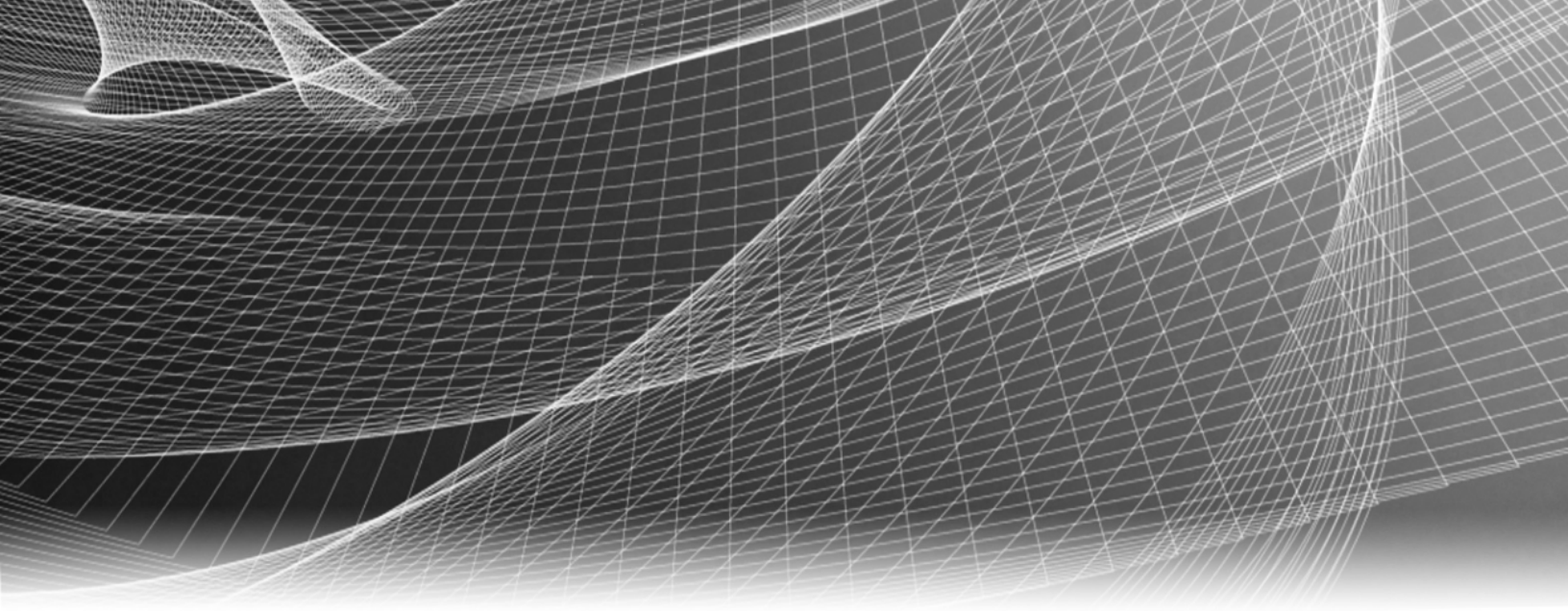


RSA Security Analytics

Guide de configuration d'Event Stream Analysis 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 d'Event Stream Analysis S4

RSA

Guide de configuration d'Event Stream Analysis S4

Présentation

Ce document est un guide étape par étape pour installer l'appliance RSA Security Analytics Event Stream Analysis 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, continuez l'installation et la configuration de l'appliance ESA, 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 de SA Event Stream Analysis (ESA)

Présentation

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

Introduction

L'appliance RSA Event Stream Analysis de la gamme 4 est livré avec le logiciel Event Stream Analysis installé. La configuration initiale du Event Stream Analysis sur votre réseau implique les étapes suivantes :

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

Il existe plusieurs options pour la première connexion physique au Event Stream 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.

Vous pouvez en savoir plus sur Security Analytics dans la documentation en ligne. Pour afficher la documentation Security Analytics, connectez-vous à Security Analytics et sélectionnez l'option **Aide** dans le menu Security Analytics.

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 Event Stream Analysis.

- Appliance Event Stream Analysis
- Ensembles de glissières coulissantes (2)
- Cordon d'alimentation (2)

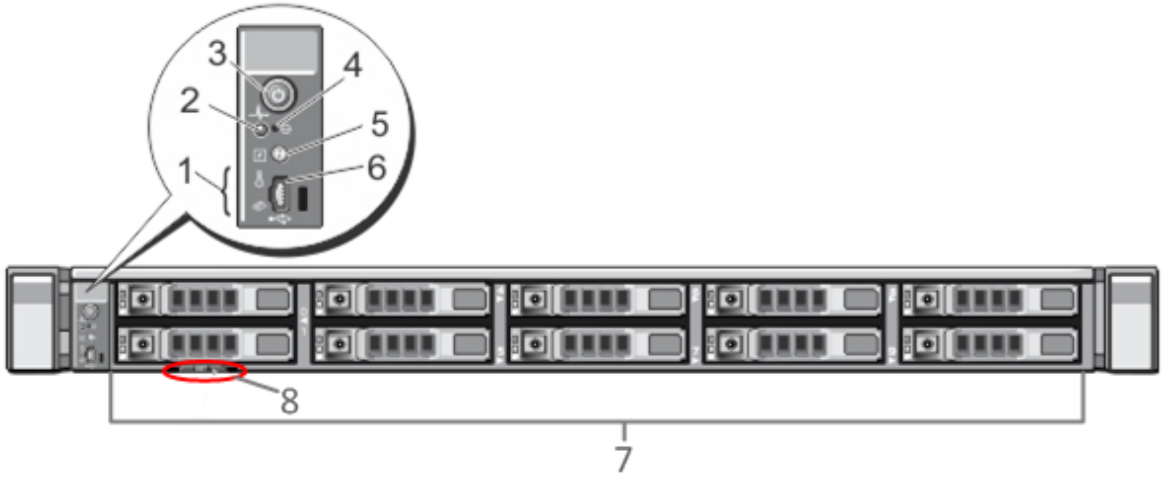
Last Modified: August 10 2016, 9:33AM

Matériel fourni par le client

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

- 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

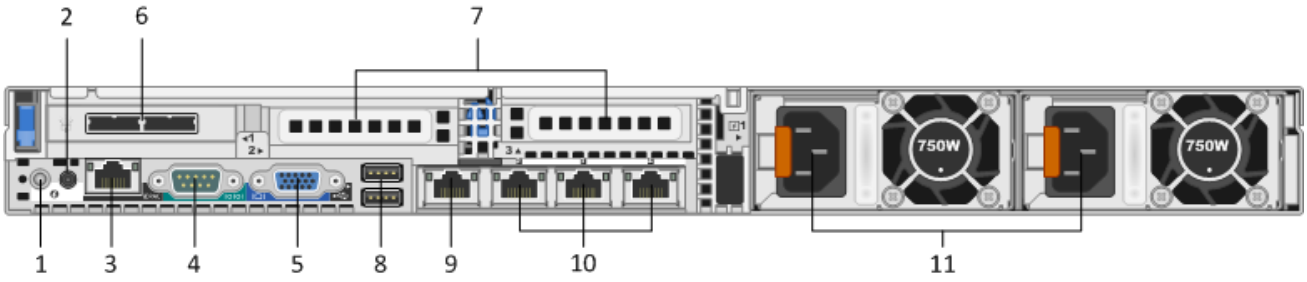
Vue avant de l'appliance Event Stream Analysis



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 le Event Stream Analysis. 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 Event Stream Analysis



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) : em 2-4
11	Alimentation remplaçable à chaud 1 et 2

Last Modified: August 10 2016, 9:33AM

Caractéristiques techniques de l'appliance Event Stream Analysis

Encombrement	1U, profondeur complète
Poids	17,69 kg
Dimensions	48,23 cm (l) x 77,19 cm (p) x 4,26 cm (h)
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

Montage de l'appliance et configuration des paramètres réseau

Présentation

Cette section fournit des instructions pour connecter une appliance Security Analytics 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 inclut la définition de l'adresse IP par défaut et le nom d'hôte, la configuration de vos serveurs DNS, puis la source de l'horloge réseau. 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 que vous pouvez vous connecter à l'appliance, utilisez la ligne de commande du système d'exploitation pour modifier les paramètres de gestion de l'appliance et configurer les serveurs DNS.

Méthode	Username	Default Password
console	racine	netwitness

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

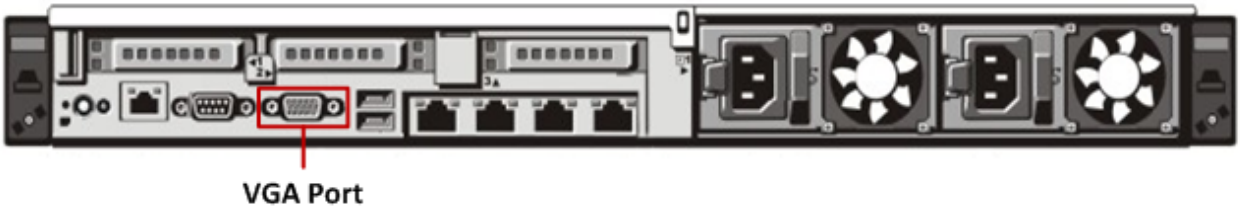
- Console de l'appliance via une connexion VGA : Clavier (port USB) et moniteur (port VGA).
- Console de l'appliance via une connexion réseau : ordinateur utilisant un client SSH connecté à l'appliance via un câble Ethernet pour le port de gestion (em1), qui est configuré sur 192.168.1.1 par défaut.

Console de l'appliance via une connexion VGA

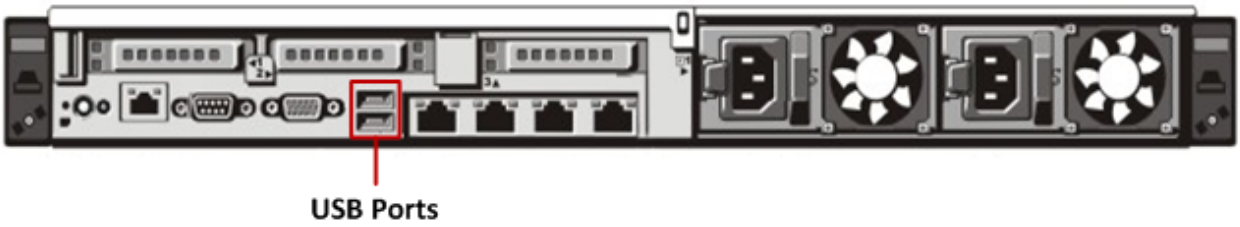
Pour utiliser la console de l'appliance via une connexion VGA :

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.

> **Note:**
> 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. Passer à la section **Configurer l'interface réseau** ci-dessous.

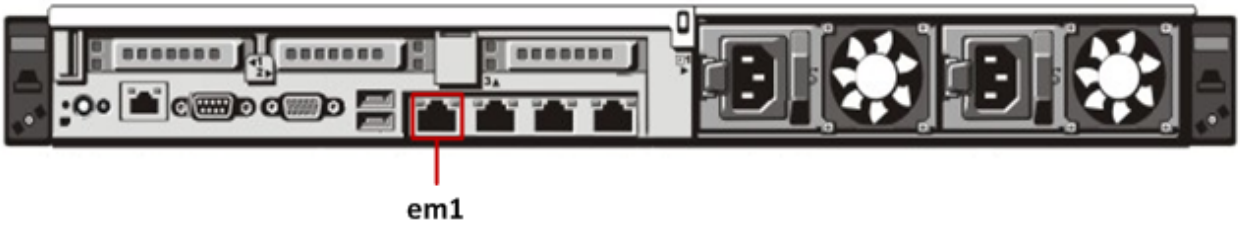
Console de l'appliance via une connexion réseau

> **Note:**
> 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.

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

Last Modified: August 10 2016, 9:33AM

1. Connectez un câble croisé 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.

Passez à la section *Configurer l'interface réseau* ci-dessous.

Configurer l'interface réseau

Utilisez la procédure ci-dessous pour définir l'adresse IP de gestion sur l'appliance.

> **Note:**
> L'adresse IP que vous définissez pour l'appliance doit être unique au sein de la plage d' IP privée dans votre environnement de réseau.

Pour configurer le réseau :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Pour configurer l'interface de réseau em1, modifiez le fichier /etc/sysconfig/network-scripts/ifcfg-em1. saisissez la commande suivante :
   `vi /etc/sysconfig/network-scripts/ifcfg-em1`
   Définissez les valeurs appropriées pour les paramètres suivants dans le fichier :

Paramètre	Valeur
DEVICE	Type d'interface réseau. Par exemple, em1.
BOOTPROTO	static
IPADDR	Adresse IP de l'interface réseau

Last Modified: August 10 2016, 9:33AM

Paramètre	Valeur
NETMASK	Adresse du masque de sous-réseau
GATEWAY	Adresse de passerelle par défaut
HWADDR	Adresse Mac de l'appliance
ONBOOT	yes
TYPE	Type de réseau

3. Pour redémarrer le service réseau, entrez la commande suivante :
   `service network restart`

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.

Note: Veillez à ne pas modifier les détails de loopback IPv4 ou v6.

Pour définir le nom d'hôte :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Pour définir le nom d'hôte de l'appliance, modifiez le fichier **/etc/sysconfig/network**. Saisissez la commande suivante :
   `vi /etc/sysconfig/network`
3. Ajoutez/modifiez la configuration comme suit :
   ```
   NETWORKING=yes
   HOSTNAME=myserver.example.com
   ```
4. Enregistrez les modifications et quittez l'éditeur vi. Saisissez la commande suivante :
   `:wq`
5. Redémarrez le réseau et entrez la commande suivante :
   `service network restart`
6. Vérifiez si le nom d'hôte est défini correctement. Saisissez la commande suivante :
   `hostname`
   Le nom d'hôte que vous avez défini s'affiche.

Configurer les serveurs DNS

Pour configurer les serveurs DNS :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Saisissez la commande suivante :
   vi /etc/resolv.conf
3. 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
4. Enregistrez les modifications et quittez l'éditeur vi. Saisissez la commande suivante :
   :wq

Configurer le fichier /etc/hosts

Modifiez le fichier des hôtes de l'appliance et incluez l'adresse IP et le nom d'hôte du boîtier ESA.

> ⚠ **Caution:** Le nom d'hôte du boîtier ESA ne doit pas s'afficher dans le cadre de la configuration de l'adresse loopback.

Pour configurer le fichier **/etc/hosts** :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Saisissez la commande suivante :
   vi/etc/hosts
3. Ajoutez les lignes suivantes au fichier :
   <node_private_ip_address> <node_fqdn> <node_hostname>
   Où :
   - <node_private_ip_address> est l'interface privée du boîtier ESA.
   - <node_fqdn> est le nom de domaine complet du boîtier ESA.
   - <node_hostname> est le nom d'hôte du boîtier ESA.

Voici un exemple du fichier **/etc/hosts** avec plus d'informations sur le boîtier ESA :

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

4. Enregistrez les modifications et quittez l'éditeur vi. Saisissez la commande suivante :
   :wq

Spécifier la source de l'horloge réseau

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.

Vous devez mettre à jour manuellement les paramètres du protocole NTP (Network Time Protocol) fournis dans /etc/ntp.conf de l'appliance SAW.

Pour mettre à jour les paramètres NTP :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Pour modifier le fichier **/etc/ntp.conf**, entrez la commande suivante :
   `vi /etc/ntp.conf`
3. Faites défiler les lignes de serveur contenant les sites NTP et mettez à jour les serveurs répertoriés pour refléter les sites NTP appropriés.
   Exemple :
   Détails du serveur fournis en tant que nom de domaine complet :
   `server 0.centos.pool.ntp.org`
   Les détails du serveur ci-dessus peuvent également être fournis à l'aide de l'adresse IP, comme suit :
   `server 91.121.92.90`
4. Enregistrez les modifications et quittez l'éditeur vi. Saisissez la commande suivante :
   `:wq`
5. Redémarrez le service ntpd et entrez la commande suivante :
   `service ntpd restart`

Last Modified: August 10 2016, 9:33AM

RSA

Fin de la configuration d'Event Stream Analysis (ESA) dans Security Analytics

Présentation

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

Introduction

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

1. Ajoutez le Event Stream Analysis à Security Analytics dans la vue Périphériques.
2. Appliquez une licence de périphérique (ou des habilitations) au Event Stream Analysis.
3. Ajoutez un ou plusieurs concentrateurs à l'Event Stream Analysis en tant que périphériques agrégés.
4. Configurez et démarrez l'agrégation.

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

- Au moins un service Concentrator doit être installé, sous licence, configuré et capturant les données afin de générer des métadonnées que l'Event Stream Analysis peut récupérer.
- Les licences de périphérique Security Analytics (ou les habilitations) doivent être disponibles pour activer les périphériques.

Connectez-vous à Security Analytics et suivez les instructions dans l'aide en ligne pour terminer la configuration de l'Event Stream Analysis dans le cadre de la suite Security Analytics.

Last Modified: August 10 2016, 9:33AM