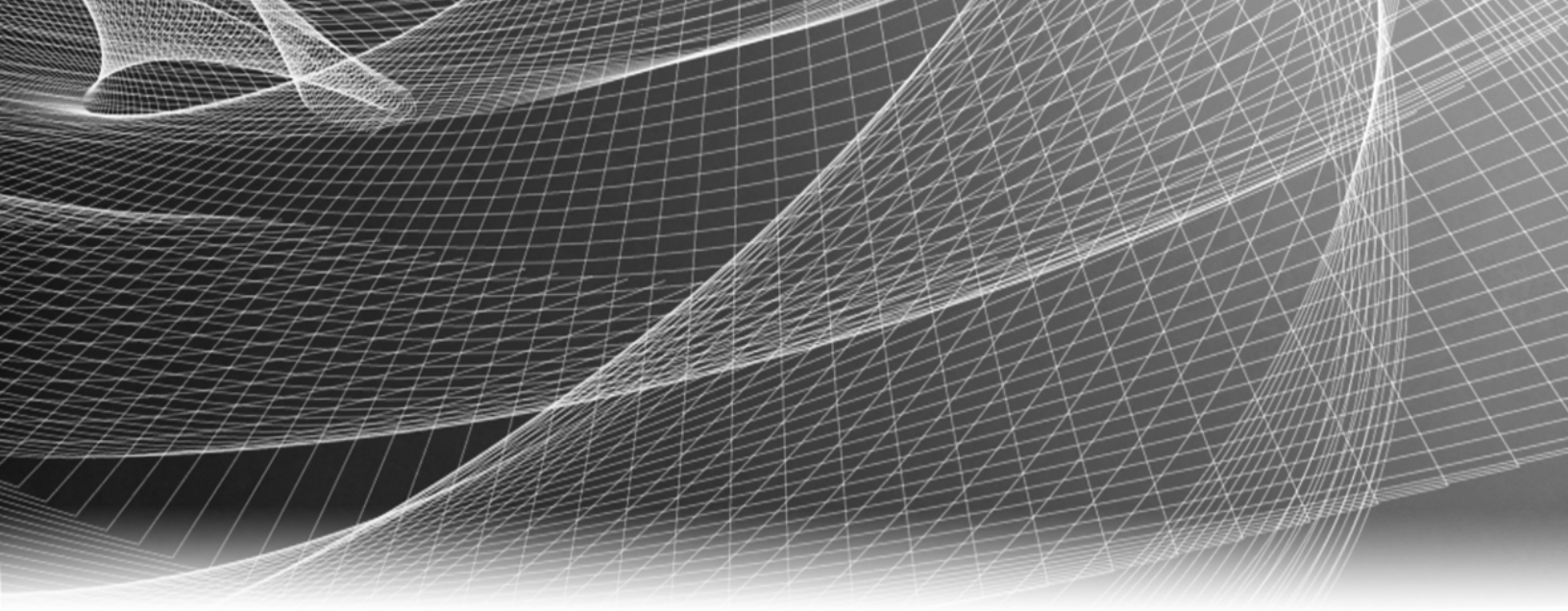


RSA Security Analytics

S4 Event Stream Analysis-Installationshandbuch

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 Event Stream Analysis-Installationshandbuch

RSA

S4 Event Stream Analysis-Installationshandbuch

Überblick

In diesem Dokument wird die Installation der RSA Security Analytics Event Stream Analysis-Appliance (ESA) und ihr Anschluss an das Netzwerk Schritt für Schritt beschrieben.

Kontext

Die Anweisungen zur Hardwarekonfiguration in diesem Dokument gelten nur für Hardware. Sie gelten nicht für eine spezifische Version der Security Analytics-Software. Fahren Sie nach Abschluss der Hardwarekonfiguration mit der Installation und Konfiguration der ESA-Appliance fort, wie in der Security Analytics-Onlinedokumentation beschrieben. Diese kann über die Security Analytics-Option **Hilfe** aufgerufen werden und steht außerdem auf sadocs.emc.com/de-de zur Verfügung.

Last Modified: September 14 2016, 12:09PM

RSA

SA ESA (Event Stream Analysis) – Hardwarebeschreibung

Überblick

In diesem Thema wird die RSA Serie 4 Event Stream Analysis-Appliance kurz vorgestellt. Zudem werden die Steuerelemente und Anschlüsse beschrieben und einige technische Daten aufgeführt.

Einführung

Die RSA Serie 4 Event Stream Analysis-Appliance wird mit installierter Event Stream Analysis-Software geliefert. Die Ersteinrichtung von Event Stream Analysis in Ihrem Netzwerk umfasst die folgenden Schritte:

1. Lesen Sie die Standortanforderungen und Sicherheitsinformationen.
2. Montieren Sie die Event Stream Analysis-Hardware.
3. Schließen Sie die Event Stream Analysis-Appliance an Ihr Netzwerk an und konfigurieren Sie die Netzwerkparameter im Event Stream Analysis.
4. Stellen Sie die Event Stream Analysis-Konfiguration in Security Analytics fertig.

Vor der Konfiguration der Softwareparameter kann die erstmalige physische Verbindung zu Event Stream Analysis auf verschiedene Weise hergestellt werden. Nachdem eine Verbindung hergestellt wurde, wird die Konsole der Security Analytics-Appliance verwendet, um diese Konfigurationsänderungen vorzunehmen. Jeder Schritt wird detailliert in diesem Dokument beschrieben.

Weitere Informationen zu Security Analytics finden Sie in der Onlinedokumentation. Zum Anzeigen der Security Analytics-Dokumentation melden Sie sich in Security Analytics an und wählen im Security Analytics-Menü die Option **Hilfe** aus.

Lieferumfang

Überprüfen Sie den Inhalt der Verpackung, um sicherzugehen, dass Sie alle für die Installation und Konfiguration von Event Stream Analysis erforderlichen Elemente erhalten haben.

- Event Stream Analysis-Appliance
- Schienenbaugruppen (2)
- Netzkabel (2)

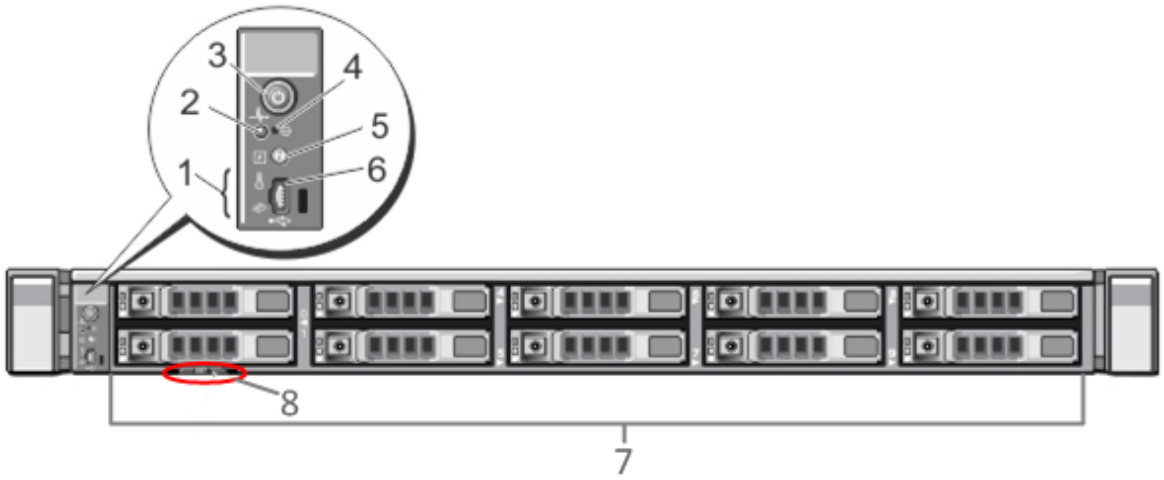
Last Modified: September 14 2016, 12:09PM

Materialien vom Kunden

Zur Durchführung des Konfigurationsverfahrens benötigen Sie Folgendes:

- Ein Ethernet-Netzwerkkabel
- Kabel für den Anschluss eines Monitors oder KVM-Adapters an den VGA-Port und einer Tastatur oder eines KVM-Adapters an den USB-Port
- Standardwerkzeuge für die Installation und das Mounten der Computerhardware

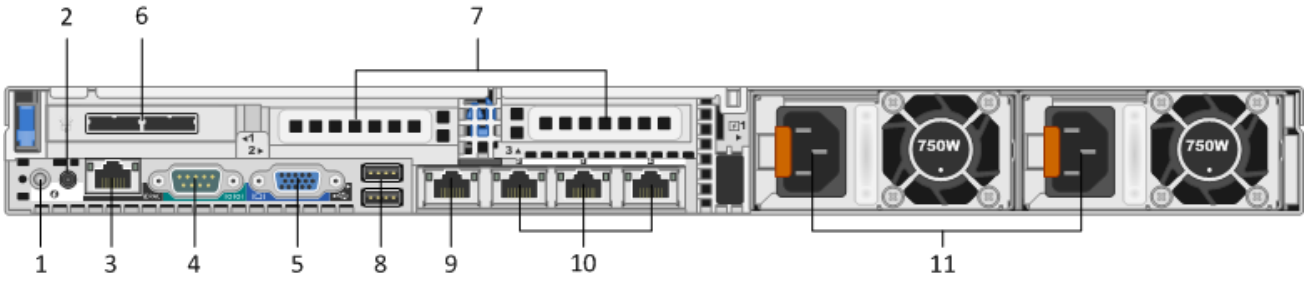
Vorderansicht der Event Stream Analysis-Appliance



Schlüssel	Beschreibung
1	Diagnose-LEDs
2	Systemidentifizierungsleuchte
3	In Betrieb/Nicht in Betrieb
4	Versenkte NMI-Taste (Non-Maskable Interrupt)
5	Systemidentifizierungstaste
6	Micro-USB-Port
7	Zehn Bays für 2,5-Zoll-Laufwerke Die Event Stream Analysis-Appliance ist mit 10 1-TB-Laufwerken ausgestattet. Es gibt außerdem ein internes SD-Kartenmodul (Secure Digital), in dem zwei 32-GB-Karten installiert sind. Darauf ist standardmäßig das Betriebssystem installiert.
8	Servicetagdetails

Last Modified: September 14 2016, 12:09PM

Rückansicht der Event Stream Analysis-Appliance



Schlüssel	Beschreibung
1	Systemidentifizierungstaste
2	Systemidentifizierungsleuchte
3	iDRAC-Port
4	Serieller RS232-Port (serielle Verbindung zu einem Laptop über DB9 oder einen seriellen Server)
5	VGA-Videoport (Monitor)
6	Steckplatz für Netzwerkschnittstellenkarten: SAS-Controller mit zwei DAC-Schnittstellenports für die Verbindung mit den Festplatten-Speicherarrays.
7	Erweiterungssteckplätze für optionale Netzwerkschnittstellenkarten Es sind folgende Optionen verfügbar: • Glasfaser-/Kupfer-10-Gbit/s-Netzwerkerfassungskarte (RJ45) • Fibre-Channel-HBA (Host Bus Adapter) zur Verbindung mit einem SAN
8	USB-Ports (Tastatur)
9	Gigabit Ethernet Port 1: em1 = Managementport
10	Gigabit Ethernet Ports (2-4): em 2-4
11	Hot-Swap-fähiges Netzteil 1 und 2

Technische Daten der Event Stream Analysis-Appliance

Formfaktor	1 HE, volle Tiefe

Last Modified: September 14 2016, 12:09PM

Gewicht	17,7 kg
Abmessungen	18,99 x 30,39 x 1,68 Zoll (B-T-H)
Netzteile	Hot-Swap-fähig, redundant, 750 W, 100 V bis 240 V, Autosensing
Prozessoren	2,66-GHz-Dual-Hex-Core
RAM	96 GB

Last Modified: September 14 2016, 12:09PM

RSA

Mounten der Appliance und Konfigurieren der Netzwerkparameter

Überblick

Dieses Thema enthält Anweisungen zum Verbinden einer Security Analytics-Appliance mit Ihrem Netzwerk und zur Konfiguration der anfänglichen Managementparameter auf der Appliance.

Einführung

Bevor Sie mit der Netzwerkkonfiguration beginnen, mounten oder platzieren Sie die Appliance sicher gemäß den Anforderungen des Standorts.

Die Konfiguration der Netzwerkparameter für eine Appliance umfasst das Festlegen der Standard-IP-Adresse und des Hostnames sowie die Konfiguration des DNS-Servers gefolgt von der Netzwerk-Uhrzeitquelle. Zum Festlegen dieser Parameter können Sie mit einer Tastatur und einer Maus oder über eine Ethernetverbindung eine Verbindung zur Appliance-Konsole herstellen. Melden Sie sich in beiden Fällen als Root bei der Appliance an. Wenn Sie sich bei der Appliance anmelden können, verwenden Sie die Befehlszeile des Betriebssystems, um die Managementeinstellungen für die Appliance zu ändern und DNS-Server zu konfigurieren.

Methode	Benutzername	Standardpasswort
Konsole	root	netwitness

Wählen Sie eine dieser Methoden für die erste Verbindung:

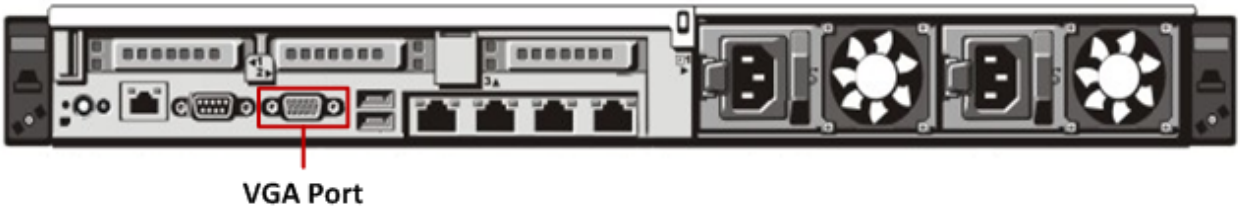
- Appliance-Konsole über VGA-Verbindung: Tastatur (USB-Port) und Monitor (VGA-Port)
- Appliance-Konsole über Netzwerkverbindung: Computer mit einem SSH-Client, der über ein Ethernetkabel zum Managementport (em1) mit der Appliance verbunden ist, die standardmäßig als 192.168.1.1 konfiguriert ist

Appliance-Konsole über VGA-Verbindung

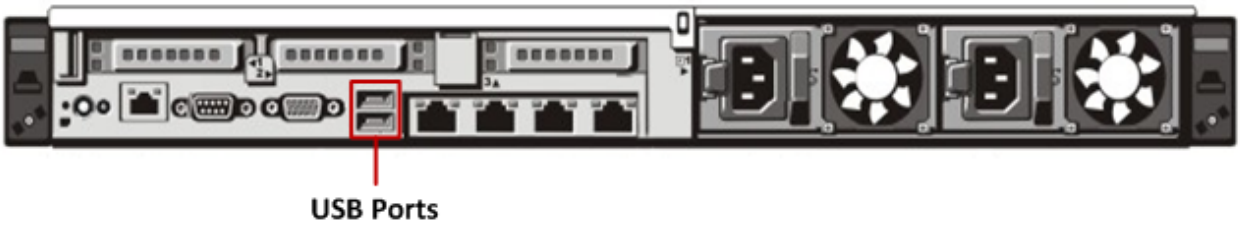
So verwenden Sie die Appliance-Konsole über die VGA-Verbindung:

Last Modified: September 14 2016, 12:09PM

1. Schließen Sie einen Monitor oder einen KVM-Adapter an den VGA-Port auf der Rückseite der Appliance an.



2. Schließen Sie eine Tastatur oder einen KVM-Adapter an einen der USB-Ports auf der Rückseite der Appliance an.



3. Schließen Sie ein Netzkabel an jedes der beiden Netzteile auf der Rückseite der Appliance an. Schließen Sie die Netzkabel an die Stromquelle an. Schließen Sie für eine robustere Konfiguration jedes Netzteil an einen anderen Stromkreis an.

> **Note:**
> Wenn das System mit einer Stromquelle verbunden ist, fließen 5 V Stand-by-Strom. Um dem System den Strom zu entziehen, müssen Sie beide Netzkabel von der Stromquelle abziehen.

4. Verwenden Sie in der Anmeldeaufforderung die Standardanmeldedaten, um Zugriff auf das Betriebssystem (`root/netwitness`) zu erhalten.
5. Fahren Sie mit dem Abschnitt **Konfigurieren der Netzwerkschnittstelle** unten fort.

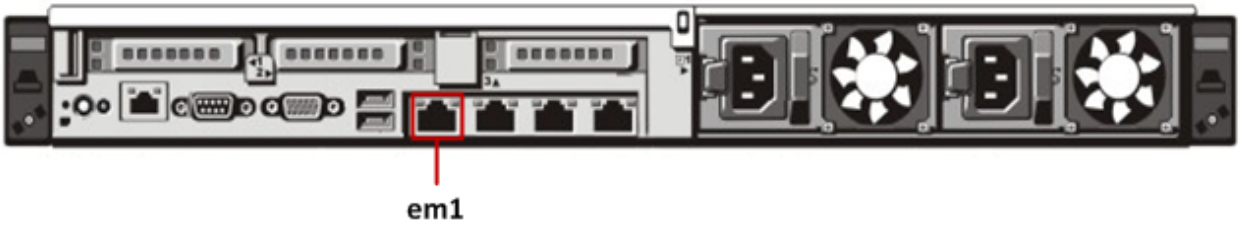
Appliance-Konsole über Netzwerkverbindung

> **Note:**
> Die Standard-IP-Adresse der Appliance ist ab Werk auf 192.168.1.1 festgelegt. 192.168.1.1 wird relativ häufig verwendet und die IP-Adresse ist in der Datei SSH known_hosts Ihres Systems möglicherweise bereits vorhanden. Die Zeile für diese IP-Adresse muss evtl. entfernt werden.

So verwenden Sie die Appliance-Konsole über eine Netzwerkverbindung:

Last Modified: September 14 2016, 12:09PM

1. Stellen Sie mit einem Crossover-Kabel eine Verbindung zwischen einem Computer und dem Ethernetmanagementport auf der Rückseite der Appliance her.



2. Verbinden Sie die Netzkabel mit den Netzanschlüssen der Appliance und einer Steckdose.
3. Die Standard-IP-Adresse der Appliance ist ab Werk auf 192.168.1.1 festgelegt. Legen Sie die IP-Adresse des Clientsystems daher im selben Subnetz fest. Legen Sie beispielsweise für Ihren Laptop 192.168.1.15 mit dem Standardgateway 192.168.1.1 fest und verwenden Sie einen SSH-Client (Secure Shell) für die Verbindung mit der Appliance.

> **Note:**
> Beachten Sie, dass Änderungen an den Netzwerkparametern während der Verbindung über SSH zum Abbruch der SSH-Sitzung führen. In diesem Fall müssen Sie erneut eine Verbindung zu der Appliance an der neuen Adresse herstellen.

4. Akzeptieren Sie den SSH-Schlüssel.
5. Verwenden Sie in der Anmeldeaufforderung die Standardanmeldedaten, um Zugriff auf das Betriebssystem zu erhalten.

Fahren Sie mit dem Abschnitt *Konfigurieren der Netzwerkschnittstelle* unten fort.

Konfigurieren der Netzwerkschnittstelle

Befolgen Sie das untenstehende Verfahren, um die Management-IP-Adresse auf der Appliance festzulegen.

> **Note:**
> Die für die Appliance festgelegte IP-Adresse muss innerhalb des privaten IP-Bereichs in der Netzwerkumgebung eindeutig sein.

So konfigurieren Sie das Netzwerk:

1. Melden Sie sich bei der Appliance als Root-Benutzer an.
2. Bearbeiten Sie zum Konfigurieren der Netzwerkschnittstelle em1 die Datei **/etc/sysconfig/network-scripts/ifcfg-em1**. Geben Sie den folgenden Befehl ein:
   `vi /etc/sysconfig/network-scripts/ifcfg-em1`
   Geben Sie die entsprechenden Werte für die folgenden Parameter in der Datei an:

Parameter	Wert
DEVICE	Typ der Netzwerkschnittstelle, Beispiel: em1.
BOOTPROTO	static

Last Modified: September 14 2016, 12:09PM

Parameter	Wert
IPADDR	IP-Adresse der Netzwerkschnittstelle
NETMASK	Adresse der Subnetzmaske
GATEWAY	Standardgateway-Adresse
HWADDR	MAC-Adresse der Appliance
ONBOOT	ja
TYP	Typ des Netzwerks

3. Geben Sie zum Neustarten des Netzwerkservices den folgenden Befehl ein:
   `service network restart`

Festlegen des Hostnamens

Das Erstellen eines Hostnamens für das System ist eine relativ einfache Aufgabe, einige Überlegungen können allerdings dazu beitragen, häufige Probleme zu vermeiden. Hilfestellung bei der Auswahl eines Hostnamens finden Sie in RFC 1178. Was Security Analytics angeht, sind die Datenbanken auf der Appliance dem Hostnamen zugeordnet. Wenn die Sammlung oder Aggregation begonnen hat (und das ist der Grund, warum dies nicht standardmäßig aktiviert ist), wird die Datenbank erstellt und durch eine Änderung des Hostnames nach diesem Vorgang wird effektiv eine zweite Datenbank erstellt. Der Hostname darf nur alphanumerische Zeichen enthalten (keine Sonderzeichen wie #, _, @, -), um Probleme bei der Kommunikation zu verhindern.

Note: Achten Sie darauf, die IPv4- oder v6-Loopback-Details nicht zu verändern.

So legen Sie den Hostnamen fest:

1. Melden Sie sich bei der Appliance als Root-Benutzer an.
2. Bearbeiten Sie zum Festlegen des Hostnamens der Appliance die Datei **/etc/sysconfig/network**. Geben Sie den folgenden Befehl ein:
   `vi /etc/sysconfig/network`
3. Ergänzen/ändern Sie die Konfiguration wie folgt:
   ```
   NETWORKING=yes
   HOSTNAME=myserver.example.com
   ```
4. Speichern Sie die Änderungen und schließen Sie den vi-Editor. Geben Sie den folgenden Befehl ein:
   `:wq`
5. Geben Sie zum Neustarten des Netzwerks den folgenden Befehl ein:
   `service network restart`
6. Überprüfen Sie, ob der Hostname erfolgreich festgelegt wurde. Geben Sie den folgenden Befehl ein:
   `Hostname`
   Der von Ihnen festgelegte Hostname wird angezeigt.

Konfigurieren von DNS-Servern

So konfigurieren Sie DNS-Server:

1. Melden Sie sich bei der Appliance als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein:
   `vi /etc/resolv.conf`
3. Fügen Sie der Datei für jeden DNS-Server die folgenden Zeilen hinzu:
   `nameserver <DNS_server_ip_address>`
   `search <domain_name>`
   wobei `<DNS_server_ip_address>` die IP-Adresse des DNS-Servers und `<domain_name>` der Name der Domain sind.
   Beispiel:
   ```
   nameserver 192.168.0.1
   search acmecorp.com
   ```
4. Speichern Sie die Änderungen und schließen Sie den vi-Editor. Geben Sie den folgenden Befehl ein:
   `:wq`

Konfigurieren der Datei /etc/hosts

Bearbeiten Sie die Hostdatei der Appliance und fügen Sie die IP-Adresse und den Hostnamen der ESA-Box hinzu.

> ⚠ **Caution:** Der Hostname der ESA-Box darf jedoch nicht als Bestandteil der Loopback-Adressenkonfiguration angezeigt werden.

So konfigurieren Sie die Datei **/etc/hosts**:

1. Melden Sie sich bei der Appliance als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein:
   `vi/etc/hosts`
3. Fügen Sie die folgenden Zeilen in die Datei ein:
   `<node_private_ip_address> <node_fqdn> <node_hostname>`
   Dabei gilt Folgendes:
   - `<node_private_ip_address>` ist die private Schnittstelle der ESA-Box.
   - <`node_fqdn`> ist der vollständig qualifizierte Domainname der ESA-Box.
   - `<node_hostname>` ist der Hostname der ESA-Box.

Beispiel für die Datei **/etc/hosts** mit den Daten der ESA-Box:

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

4. `Speichern Sie die Änderungen und schließen Sie den vi-Editor. Geben Sie folgenden Befehl ein:`
   :wq

Last Modified: September 14 2016, 12:09PM

Angeben der Netzwerkzeitquelle

Es wird empfohlen, alle Systeme in der Security Analytics-Suite mithilfe einer Netzwerk-Uhrzeitquelle zu synchronisieren, sodass alle Geräte präzise die gleiche Zeit anzeigen. Wird dies nicht umgesetzt, kann die Zeit auf den Geräten abweichen und Abfragen zu einem bestimmten Zeitpunkt geben nicht die erwarteten Ergebnisse zurück.

Sie müssen die NTP-Einstellungen (Network Time Protocol), die in der Datei **/etc/ntp.conf** in der SAW-Appliance bereitgestellt sind, manuell aktualisieren.

So aktualisieren Sie die NTP-Einstellungen:

1. Melden Sie sich bei der Appliance als Root-Benutzer an.
2. Geben Sie zum Bearbeiten der Datei **/etc/ntp.conf** den folgenden Befehl ein:
   ```
   vi /etc/ntp.conf
   ```
3. Blättern Sie zu den Serverzeilen mit den NTP-Standorten und aktualisieren Sie die aufgeführten Server mit den entsprechenden NTP-Standorten.
   Beispiel:
   Serverdetails als vollständig qualifizierter Domainname angegeben:
   ```
   server 0.centos.pool.ntp.org
   ```
   Die oben genannten Serverdetails können auch wie folgt mithilfe der IP-Adresse angegeben werden:
   ```
   server 91.121.92.90
   ```
4. Speichern Sie die Änderungen und schließen Sie den vi-Editor. Geben Sie den folgenden Befehl ein:
   ```
   :wq
   ```
5. Geben Sie zum Neustarten des ntpd-Service den folgenden Befehl ein:
   ```
   service ntpd restart
   ```


Last Modified: September 14 2016, 12:09PM

RSA

Abschließen der ESA-Konfiguration (Event Stream Analysis) in Security Analytics

Überblick

Dieses Thema enthält Anweisungen zum Abschließen der Event Stream Analysis-Konfiguration und Starten der Aggregation in Security Analytics.

Einführung

Die abschließenden Schritte zur Konfiguration der Event Stream Analysis-Appliance werden in Security Analytics vorgenommen. und zwar:

1. Fügen Sie die Event Stream Analysis in der Ansicht "Geräte" zu Security Analytics hinzu.
2. Wenden Sie eine Gerätelizenz (oder Berechtigung) auf die Event Stream Analysis an.
3. Fügen Sie der Event Stream Analysis-Appliance einen oder mehrere Concentrator als Aggregatgeräte hinzu.
4. Konfigurieren und starten Sie die Aggregation.

Mehrere dieser Schritte können nur dann abgeschlossen werden, wenn andere Bestandteile des Security Analytics-Netzwerks eingerichtet sind:

- Mindestens ein Concentrator-Service muss installiert, lizenziert und konfiguriert sein und Daten erfassen, um Metawerte zu erzeugen, die die Event Stream Analysis-Appliance abrufen kann.
- Die Security Analytics-Gerätelizenzen (oder Berechtigungen) müssen zur Aktivierung der Geräte verfügbar sein.

Melden Sie sich bei Security Analytics an und befolgen Sie die Anweisungen in der Onlinehilfe, um die Event Stream Analysis-Konfiguration als Bestandteil der Security Analytics-Suite abzuschließen.

Last Modified: September 14 2016, 12:09PM