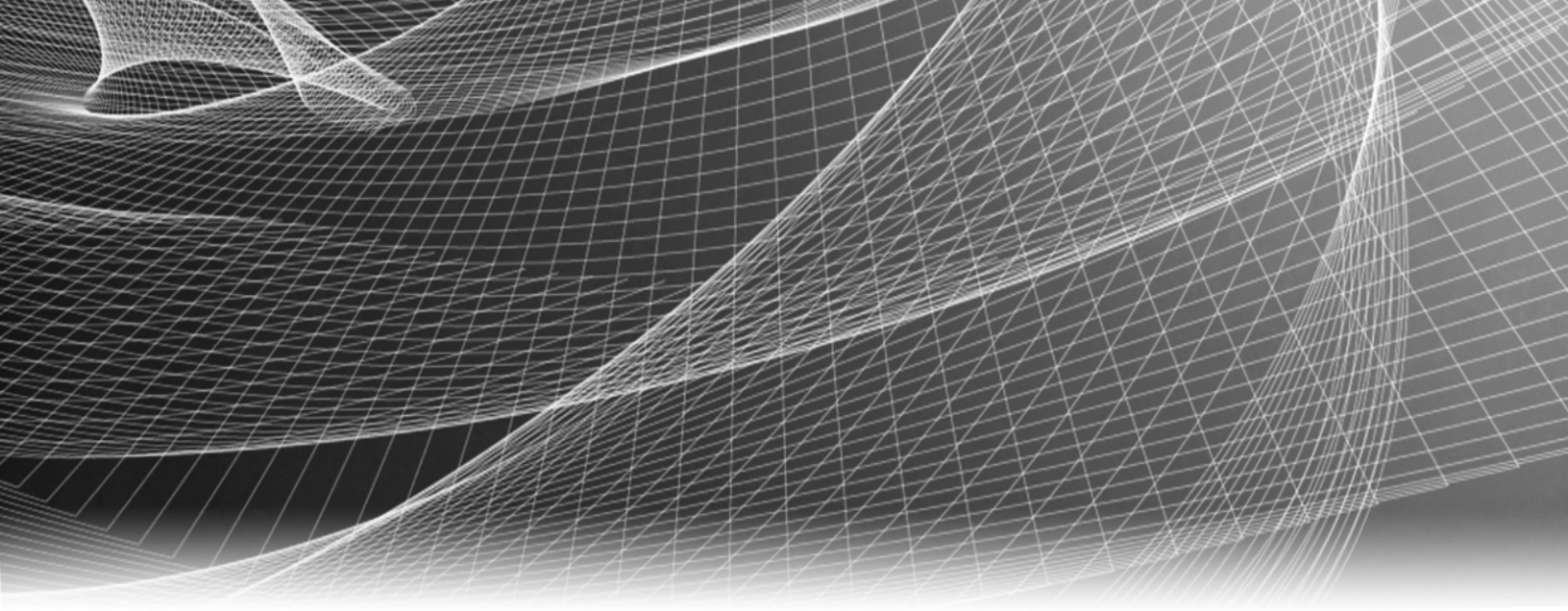


RSA Security Analytics

S4 Decoder – Konfigurationshandbuch

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 Decoder – Konfigurationshandbuch

RSA

S4 Decoder – Konfigurationshandbuch

Überblick

In diesem Dokument wird die Installation des RSA Security Analytics-Decoder und sein 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 des Decoder 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 Decoder – Hardwarebeschreibung

Überblick

In diesem Dokument wird zunächst der RSA Security Analytics Decoder vorgestellt. Danach werden die allgemeinen Verfahren zum Installieren des Decoder und zum Anschließen an das Netzwerk und die Speicherkomponenten beschrieben.

Einführung

Die RSA Security Analytics Serie 4 Decoder-Appliance wird mit installierter Decoder-Software geliefert. Die Erstkonfiguration eines Decoder in Ihrem Netzwerk umfasst die folgenden Schritte:

1. Lesen Sie die Standortanforderungen und Sicherheitsinformationen.
2. Montieren Sie die Decoder-Hardware.
3. Schließen Sie den Decoder an Ihr Netzwerk an und konfigurieren Sie die Netzwerkparameter im Decoder.
4. Schließen Sie den Decoder an das DAC(Direct-Attached Capacity)- oder SAN-Gerät an, wie im Direct-Attached Capacity (DAC) Serie 4 Konfigurationshandbuch beschrieben.
5. Stellen Sie die Decoder-Konfiguration in Security Analytics fertig.

Vor der Konfiguration der Softwareparameter kann die erstmalige physische Verbindung zum Decoder 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.

Lieferumfang

Überprüfen Sie den Inhalt der Verpackung, um sich zu vergewissern, dass Sie alle für die Installation und Konfiguration des RSA Decoder erforderlichen Komponenten erhalten haben.

- S4 Decoder-Appliance
- Schienenbaugruppen (2)
- Netzkabel (2)

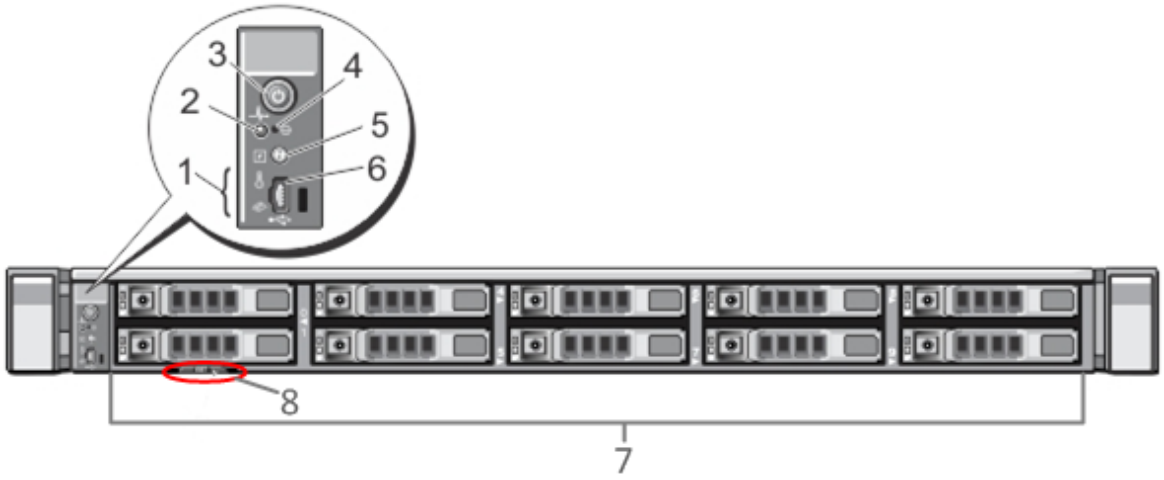
Last Modified: September 14 2016, 12:09PM

Materialien vom Kunden

Zur Durchführung des Konfigurationsverfahrens benötigen Sie Folgendes:

- Mehrere Ethernet-Netzwerkkabel (eines für das Management und jeweils eines pro Erfassungsschnittstelle)
- 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

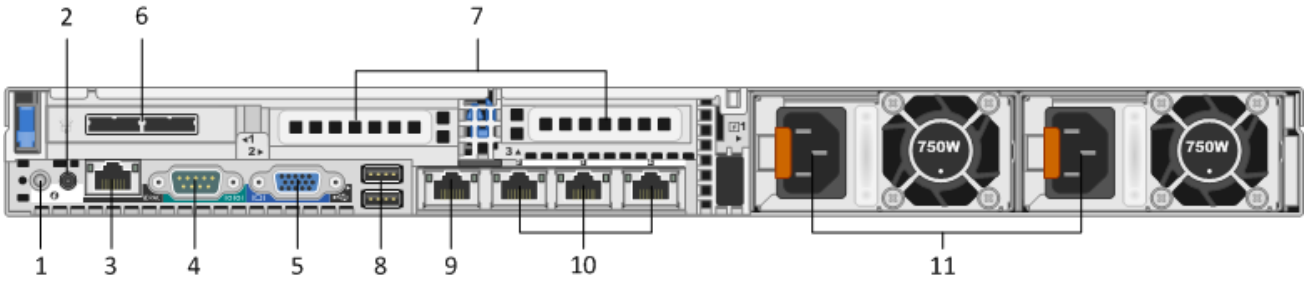
Vorderansicht des Decoder



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 Der Decoder ist mit zwei 146-GB-Laufwerken und zwei 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 des Decoder



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): em2-4 = Monitoring-Ports
11	Hot-Swap-fähiges Netzteil 1 und 2

Decoder – Technische Daten

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)
Stromversorgung	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 S4 Appliance mit Ihrem Netzwerk und zur Konfiguration der anfänglichen Managementparameter auf der Appliance.

⚠ **Caution:** Wenn Sie DAC (Direct-Attached Capacity) installieren, müssen Sie dies tun, bevor Sie die Geräte lizenzieren und die Services starten. Lesen Sie die Anweisungen zur Lizenzierung von Appliances im **Security Analytics-Lizenzierungsleitfaden**, auf den Sie über die Security Analytics-Option **Hilfe** und unter sadocs.emc.com/de-de zugreifen können.

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 RSA Security Analytics S4 Appliance besteht aus dem Festlegen der Standard-IP-Adresse, der Netzwerk-Uhrzeitquelle und des Hostnamens, gefolgt von der Konfiguration des DNS-Servers. 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. Verwenden Sie, nachdem Sie sich bei der Appliance anmelden können, das Programm NwConsole, um die Managementeinstellungen für die Appliance zu ändern. Verwenden Sie die Befehlszeile des Betriebssystems, um die DNS-Server zu konfigurieren.

Methode	Benutzername	Standardpasswort
ssh/cli	root	netwitness
Appliance	admin	netwitness

Wählen Sie eine dieser Methoden für die erste Verbindung:

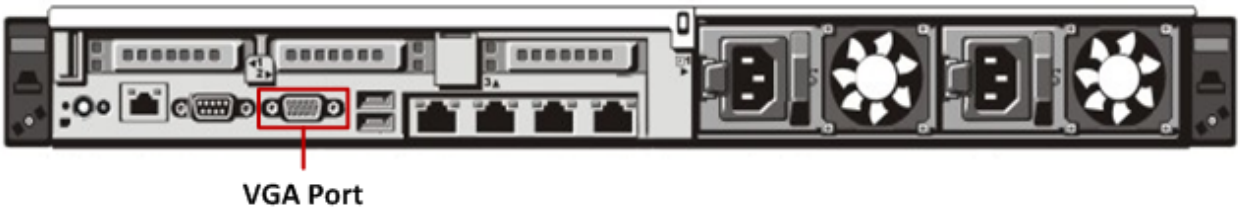
- Appliance-Konsole über VGA-Verbindung: Tastatur (USB-Port) und Monitor (VGA-Port)
- Appliance-Konsole über Netzwerkverbindung: Computer mit einem SSH-Client, der über ein Ethernetkabel zum Managementport (em1) mit der Appliance verbunden ist, die standardmäßig als 192.168.1.1 konfiguriert ist

Last Modified: September 14 2016, 12:09PM

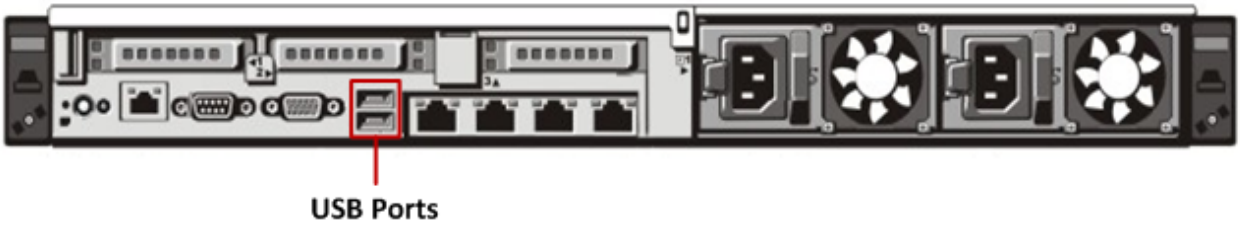
Appliance-Konsole über VGA-Verbindung

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

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.

> ⚠ **Caution:**
> 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 **Festlegen der IP-Adresse** unten fort.

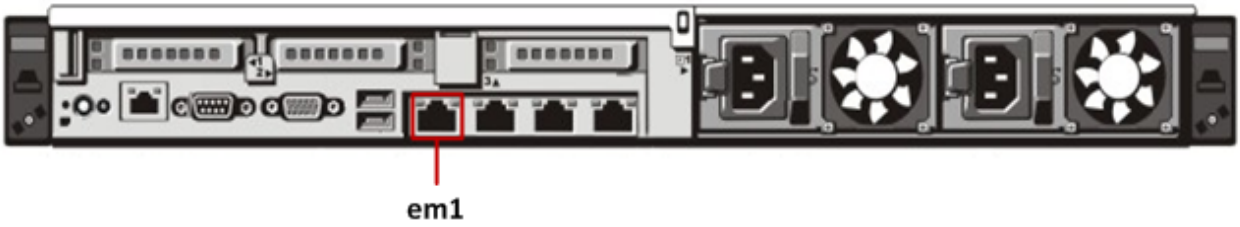
Appliance-Konsole über Netzwerkverbindung

> ⚠ **Caution:** 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 Ethernetkabel 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.
6. Fahren Sie mit dem Abschnitt **Festlegen der IP-Adresse** unten fort.

Festlegen der IP-Adresse

Verwenden Sie eines der untenstehenden Verfahren, um die Management-IP-Adresse auf der Appliance festzulegen.

Festlegen einer statischen IP

So legen Sie eine statische IP-Adresse fest:

1. Geben Sie in der Root-Eingabeaufforderung `[root@NwAppliance~]#`
   den folgenden Befehl ein:
   `NwConsole`
   Die NwConsole wird gestartet und die folgende Meldung wird angezeigt:
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  Alle Rechte vorbehalten.
   ```
2. Geben Sie in der NwConsole den folgenden Befehl ein:
   `login localhost:50006 <adminusername> <password>`
   Beispiel: `login localhost:50006 admin netwitness`
   Sie werden bei der Appliance angemeldet und die folgende Meldung wird angezeigt:
   `Successfully logged in as session <session #>`
3. Geben Sie in der localhost-Eingabeaufforderung `[localhost:50006] />`
   den folgenden Befehl ein:
   `appliance setNet mode=static address=<desired IP address> netmask=<desired netmask> gateway=<desired network gateway>`

Last Modified: September 14 2016, 12:09PM

- Beispiel: Führen Sie den folgenden Befehl aus, um die IP-Adresse der em1-Schnittstelle auf 10.1.2.35 für ein Klasse-C-Netzwerk mit Gateway 10.1.2.1 festzulegen:
  `appliance setNet mode=static address=10.1.2.35 netmask=255.255.255.0 gateway=10.1.2.1`
  Die Netzwerkservices auf der Appliance werden automatisch neu gestartet und die neuen Einstellungen werden angewendet.

4. Wenn die Appliance über eine Netzwerkverbindung verbunden ist, müssen Sie die Appliance mithilfe der neuen IP-Adresse erneut verbinden, um fortzufahren. Wenn Sie die Appliance in ein neues Subnetz verschoben haben, können ebenfalls Änderungen an den Client-Netzwerkeinstellungen erforderlich sein.
5. Um sich abzumelden und NwConsole zu beenden, geben Sie **`exit`** ein.

Festlegen einer dynamischen IP

So legen Sie eine dynamische IP-Adresse fest:

1. Geben Sie in der Root-Eingabeaufforderung `[root@NwAppliance~]#`
   den folgenden Befehl ein:
   `NwConsole`
   Die NwConsole wird gestartet und die folgende Meldung wird angezeigt:
   `RSA Security Analytics Console 10.2`
   `Copyright 2001-2012, RSA Security Inc.  Alle Rechte vorbehalten.`
2. Geben Sie in der NwConsole den folgenden Befehl ein:
   `login localhost:50006 <username> <password>`
   Sie werden bei der Appliance angemeldet und die folgende Meldung wird angezeigt:
   `Successfully logged in as session <session #>`
3. Geben Sie in der localhost-Eingabeaufforderung `[localhost:50006] />`
   den folgenden Befehl ein:
   `appliance setNet mode=dhcp`
4. Die Netzwerkservices auf dem Gerät werden automatisch neu gestartet und die neuen Einstellungen werden angewendet. Wenn die Appliance über eine Netzwerkverbindung verbunden ist, müssen Sie die Appliance mithilfe der neuen IP-Adresse erneut verbinden, um fortzufahren. Wenn Sie die Appliance in ein neues Subnetz verschoben haben, können ebenfalls Änderungen an den Client-Netzwerkeinstellungen erforderlich sein.

> ⚠ **Caution:** Wenn es sich beim Modus um DHCP handelt, ist es möglicherweise nicht möglich, die neue Adresse zu bestimmen. Sie müssen direkt mit der Appliance-Konsole verbunden sein, um die neue Adresse ermitteln zu können.

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.

Last Modified: September 14 2016, 12:09PM

1. Wenn Sie noch bei NwConsole angemeldet sind, überspringen Sie die Schritte 2 und 3.
2. Geben Sie in der Root-Eingabeaufforderung `[root@NwAppliance~]#` den folgenden Befehl ein:
   `NwConsole`
   Die NwConsole wird gestartet und die folgende Meldung wird angezeigt:
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  Alle Rechte vorbehalten.
   ```
3. Geben Sie in der NwConsole den folgenden Befehl ein:
   `login localhost:50006 <username> <password>`
   Sie werden bei der Appliance angemeldet und die folgende Meldung wird angezeigt:
   ```
   Successfully logged in as session <session #>
   ```
4. Geben Sie in der localhost-Eingabeaufforderung `[localhost:50006] />` den folgenden Befehl ein:
   `appliance hostname name=<desired_name_for_appliance>`
   Beispiel: **`appliance hostname name=myserver`**
5. Wenn Sie die Ausgabe `Success` sehen, geben Sie **`exit`** ein, um sich abzumelden und das Programm NwConsole zu beenden.
6. Starten Sie den Server mithilfe des folgenden Befehls neu: **`reboot`**

> **Note:** Es wird empfohlen, das System nach der Änderung des Hostnamens neu zu starten.

Angeben der Netzwerkzeitquelle

> **Note:** Wenn der NTP-Server zu diesem Zeitpunkt nicht konfiguriert oder nicht erreichbar ist, schlägt die Konfiguration der Netzwerk-Uhrzeitquelle fehl. Sie kann aber später über die SA-Schnittstelle nachgeholt werden.

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.

> **Note:** Bei den Befehlen in diesen Anweisungen ist die Groß-/Kleinschreibung wichtig.

So legen Sie die Netzwerk-Uhrzeitquelle fest:

1. Wenn Sie noch bei NwConsole angemeldet sind, überspringen Sie die Schritte 2 und 3.
2. Geben Sie in der Root-Eingabeaufforderung `[root@NwAppliance~]#` den folgenden Befehl ein:
   `NwConsole`
   Die NwConsole wird gestartet und die folgende Meldung wird angezeigt:
   ```
   RSA Security Analytics Console 10.2
   Copyright 2001-2012, RSA Security Inc.  Alle Rechte vorbehalten.
   ```
3. Geben Sie in der NwConsole den folgenden Befehl ein:
   `login localhost:50006 <username> <password>`
   Sie werden bei der Appliance angemeldet und die folgende Meldung wird angezeigt:
   ```
   Successfully logged in as session <session #>
   ```
4. Geben Sie in der localhost-Eingabeaufforderung `[localhost:50006] />` den folgenden Befehl ein:

Last Modified: September 14 2016, 12:09PM

appliance setNTP source=<NTP_server_hostname or IP_address>
Beispiel: **appliance setNTP source=0.pool.ntp.org**
Wenn Sie die Uhr der Appliance als Uhrzeitquelle verwenden möchten, geben Sie Folgendes ein: **appliance setNTP source=local**

5. Wenn durch den Befehl die Ausgabe `Success` angezeigt wird, geben Sie **exit** ein, um sich abzumelden und das Programm NwConsole zu beenden.

> **Note:** Wenn Sie eine lokale NTP-Uhrzeitquelle angegeben haben, dient die Appliance-Zeit als Uhrzeitquelle und die Zeit wird unter "Integrierte Appliance-Uhr einstellen" konfiguriert, wie in der Security Analytics-Onlinehilfe beschrieben.

Konfigurieren von DNS-Servern

So legen Sie eine statische IP-Adresse fest:

1. Geben Sie in der Root-Eingabeaufforderung `[root@NwAppliance~]#`
den folgenden Befehl ein:
vi /etc/resolv.conf

2. 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
```
3. Speichern Sie die Änderungen und schließen Sie den vi-Editor.

RSA

Abschließen der Decoder-Konfiguration in Security Analytics

Überblick

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

Einführung

> ⚠ **Caution:** Bevor Sie mit der abschließenden Konfiguration in Security Analytics beginnen, müssen Sie das DAC-Initialisierungsskript ausführen, um das erste Speicherarray zu konfigurieren. Entsprechende Anweisungen finden Sie im Direct-Attached Capacity (DAC) Serie 4 Konfigurationshandbuch.

Die abschließenden Schritte zur Konfiguration des Decoder werden vom Security Analytics-Server aus vorgenommen. und zwar:

1. Fügen Sie den Decoder in der Ansicht "Geräte" zu Security Analytics hinzu.
2. Wenden Sie eine Gerätelizenz (oder Berechtigung) auf den Decoder an.
3. Konfigurieren Sie Feeds und Parser.
4. Konfigurieren und starten Sie die Erfassung.
5. Fügen Sie einem Concentrator einen oder mehrere Decoder als Aggregatgeräte hinzu.

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

- Für Schritt 2 sind die Security Analytics-Gerätelizenzen (oder Berechtigungen) erforderlich, um die Geräte aktivieren zu können.
- Für Schritt 5 muss mindestens ein Concentrator-Service installiert, lizenziert, konfiguriert und zum Aggregieren von Daten vom Decoder bereit sein.

Melden Sie sich bei Security Analytics an und befolgen Sie die Anweisungen in der Onlinehilfe, um die Konfiguration des Decoder abzuschließen.

Last Modified: September 14 2016, 12:09PM