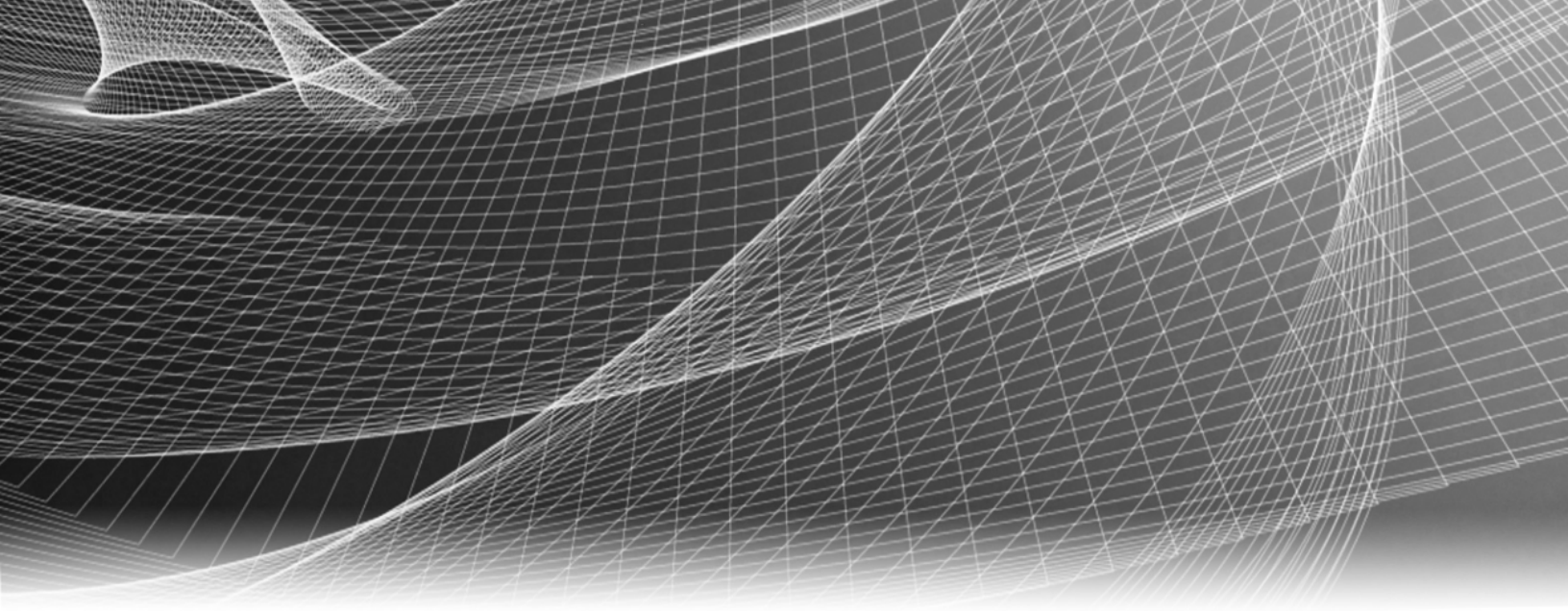


RSA Security Analytics

Security Analytics Serie 5 Appliances – 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.

Security Analytics Serie 5 Appliances – Konfigurationshandbuch

RSA

Security Analytics Serie 5 Appliances – Konfigurationshandbuch

Überblick

In diesem Dokument wird die Installation der RSA Security Analytics Serie 5 (S5) Appliances 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 dem Abschließen der Hardwarekonfiguration mit der Installation und Konfiguration der Security Analytics-Appliances fort, wie in der Security Analytics-Onlinedokumentation auf sadocs.emc.com/de-de beschrieben.

Dieses Dokument ist kein Ersatz für die Dokumentation des Herstellers. Es enthält Informationen speziell für die Security Analytics-Appliances.

Last Modified: September 14 2016, 12:09PM

RSA

S5 R630-Appliances – Hardwarebeschreibung

Einführung

Bis auf eine Ausnahme basieren alle RSA Security Analytics Serie 5 (S5) Appliances auf dem Dell PowerEdge R630-Gehäuse. Die Ausnahme bildet die Hybrid Appliance, die auf dem Dell PowerEdge R730xd-Gehäuse basiert. Die Serie 5 Appliances werden mit installierter Security Analytics 10.5-Software geliefert.

In diesem Thema werden die Serie 5 Appliances beschrieben, die auf dem Dell PowerEdge R630-Gehäuse basieren:

- Decoder und Log Decoder
- Concentrator
- Broker
- Archiver
- Security Analytics Server
- Malware Analysis
- Event Stream Analysis (ESA)

Mit Ausnahme der ESA-Appliance zeichnen sich alle auf dem Dell PowerEdge R630 basierenden Appliances durch identische Komponenten und physische Spezifikationen aus. Die ESA-Appliance verfügt über zusätzliche Laufwerke, zusätzlichen Speicher und eine andere CPU. Weitere Details finden Sie unter Security Analytics ESA-Appliance – Technische Daten.

Die Ersteinrichtung einer Serie 5 Appliance in Ihrem Netzwerk umfasst die folgenden Schritte:

1. Überprüfen Sie die Anforderungen an den Standort und Sicherheitsinformationen im *Bereitstellungshandbuch* zu Ihrer Security Analytics-Softwareversion: Security Analytics 10.5
2. Montieren oder platzieren Sie die Appliance-Hardware sicher gemäß den Anforderungen des Standort.
3. Schließen Sie die Appliance an Ihr Netzwerk an und konfigurieren Sie die Netzwerkparameter in der Appliance: Anschließen der Appliance und Konfigurieren der Netzwerkparameter
4. Schließen Sie die Appliance-Konfiguration in Security Analytics ab: Abschließen der Appliance-Konfiguration in Security Analytics

Caution: Um Schäden an den Security Analytics-Servern und -Appliances zu vermeiden, entfernen Sie diese aus dem Rack und zerlegen Sie das Rack, bevor Sie sie an einen anderen Standort transportieren. Befolgen Sie die Empfehlungen des Serverherstellers und des Rack-Hersteller bezüglich Verpackung, Transport und Installation.
RSA bietet keine Unterstützung für den erneuten Versand der in einem Rack montierten Server. Der Kunde

Last Modified: September 14 2016, 12:09PM

übernimmt alle Risiken und die Haftung für den Transport von in einem Rack montierten Security Analytics-Servern und -Appliances.

Lieferumfang

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

- Serie 5 Security Analytics-Appliance (Decoder, Concentrator, Broker, Archiver, Security Analytics Server, Malware Analysis oder ESA)
- Statische ReadyRails-Schienen (1 Satz)
- Linker Schienenadapter für EMC Deep-Rack
- RSA-Blende (1) (Schlüssel mit Klebeband an Blende befestigt)
- Netzkabel (2)
- Handbuch mit Produktinformationen von Dell (1)
- Ordner mit RSA-Dokumentation (1)
- RSA-EULA (1)

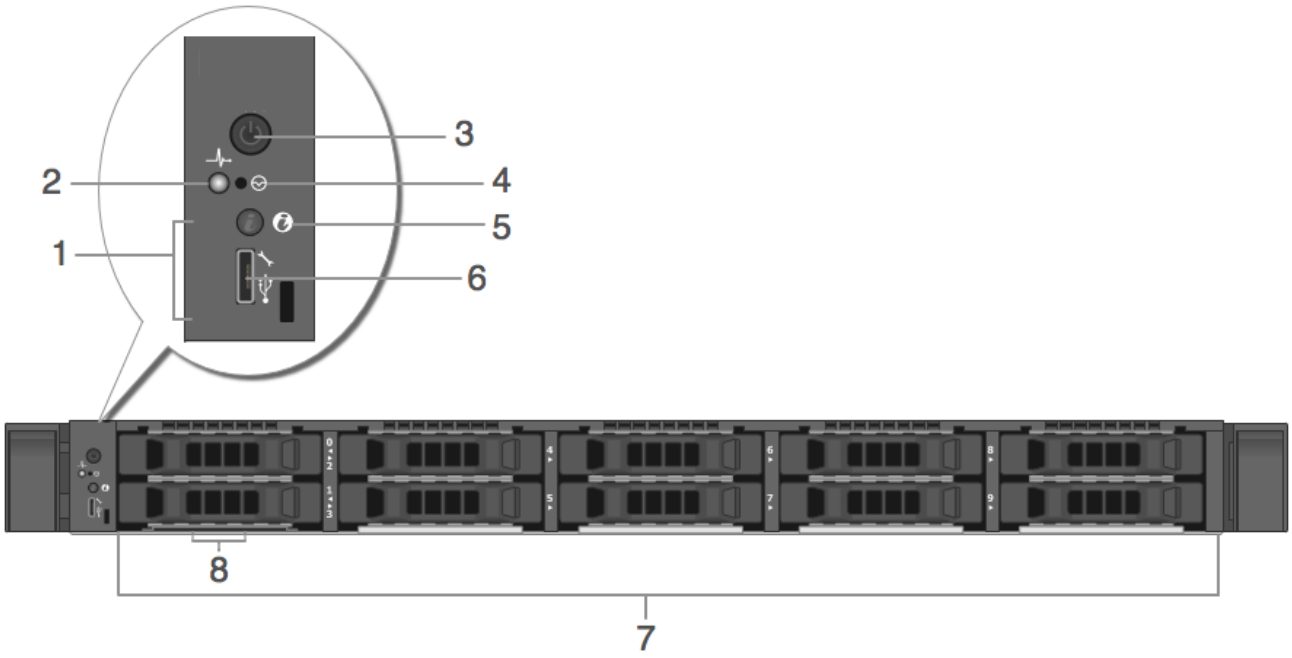
Materialien vom Kunden

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

Last Modified: September 14 2016, 12:09PM

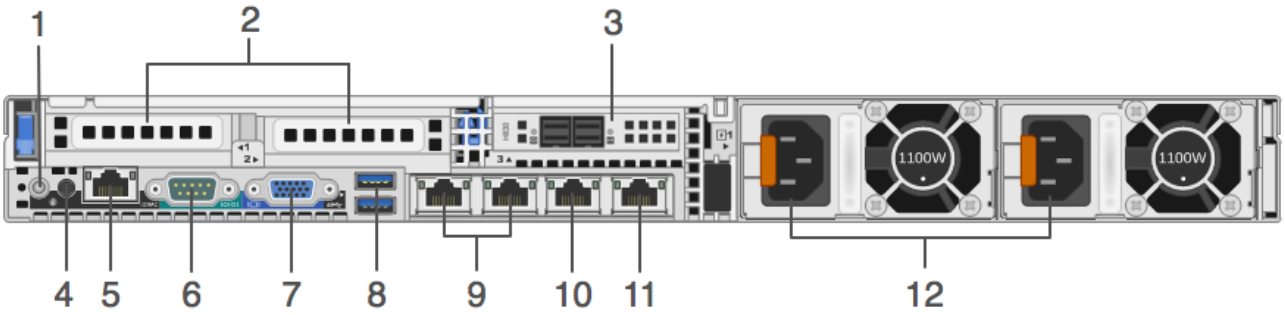
Vorderansicht der Serie 5 Appliances (außer Hybrid)



Schlüssel	Beschreibung
1	Position der Diagnoseanzeige. Bei Fehlern wird in der Diagnoseanzeige ein Status angezeigt.
2	Systemintegritätsanzeige. Blinkt gelb, wenn ein Systemfehler erkannt wird.
3	In Betrieb/Nicht in Betrieb
4	Versenkte NMI-Taste (Non-Maskable Interrupt)
5	Systemidentifizierungstaste
6	Micro-USB-Port/iDRAC Direct
7	10 2,5-Zoll-Festplatten-Bays (vor Ort austauschbar). In den unten aufgeführten technischen Daten sind Anzahl und Typen der in den Appliances installierten Festplatten angegeben.
8	Position des Informationsetiketts

Last Modified: September 14 2016, 12:09PM

Rückansicht der Serie 5 Appliances (außer Hybrid)



Schlüssel	Beschreibung
1	Systemidentifizierungstaste
2	LP-PCIe-Erweiterungssteckplätze 1 und 2. Für den 10G-Decoder kann ein LP-PCIe-Steckplatz für eine optionale optische Intel X520-Netzwerkschnittstellenkarte verwendet werden.
3	PERC H830-RAID-Controller. Dieser ist in LP-PCIe-Steckplatz 3 dargestellt, kann aber in einem anderen LP-PCIe-Steckplatz installiert werden. Der PERC H830 ist der RAID-Controller für den Speichererweiterungs-DAC. Für die Verbindung mit dem DAC ist ein Kabel mit einem Mini-SAS-Anschluss erforderlich.
4	Systemidentifizierungsanschluss
5	iDRAC-Port
6	Serieller RS232-Port (serielle Verbindung zu einem Laptop über DB9 oder einen seriellen Server)
7	VGA-Videoport (Monitor)
8	USB-Ports (Tastatur, Maus, USB-Stick usw.)
9	10G-Base-T-Ethernetports em3 und em4
10	Primärer 1000Base-T-Netzwerk-Managementport: em1
11	Sekundärer 1000Base-T-Netzwerkport: em2
12	Hot-Swap-fähige Netzteile 1 und 2 (vor Ort austauschbar)

Note: Für die Verbindung des PERC H830-RAID-Controller mit dem DAC ist ein Kabel mit einem Mini-SAS-Anschluss erforderlich.

Last Modified: September 14 2016, 12:09PM

Technische Daten der Serie 5 Appliances (außer Hybrid und ESA)

Element	Beschreibung
Formfaktor	1 HE, volle Tiefe
Gewicht (ca.)	18,4 kg
Abmessungen (ca.)	Mit Frontblende: 482,43 mm x 808,59 mm x 42,80 mm (BxTxH) Ohne Blende: 482,43 mm x 776,16 mm x 42,80 mm (BxTxH)
Netzteile	Zwei Hot-Plug-fähige, redundante Netzteile (1+1), 1100 W
Prozessoren	2 x E5-2667v3
RAM	16 x 8-GB-2.133-MT/s-RDIMMs (128 GB)
Festplatten (vor Ort austauschbar)	2 x 2,5-Zoll-Hot-Plug-Festplatte, 1 TB, 7.200 U/min, NL-SAS, 6 Gbit/s 2 x 2,5-Zoll-Hot-Plug-Festplatte, 2 TB, 7.200 U/min, NL-SAS, 12 Gbit/s, 512e
RAID-Controller	Extern: PERC H830 RAID Intern: PERC H730P
Netzwerkschnittstellenkarte	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DP-Netzwerk-Tochterkarte

Technische Daten der Security Analytics ESA-Appliance

Element	Beschreibung
Formfaktor	1 HE, volle Tiefe
Gewicht (ca.)	18,4 kg
Abmessungen (ca.)	Mit Frontblende: 482,43 mm x 808,59 mm x 42,80 mm (BxTxH) Ohne Blende: 482,43 mm x 776,16 mm x 42,80 mm (BxTxH)
Netzteile	Zwei Hot-Plug-fähige, redundante Netzteile (1+1), 1100 W
Prozessoren	2 x E5-2680v3
RAM	8 x 32-GB-2.133MT/s-RDIMMs (256 GB)
Festplatten (vor Ort austauschbar)	2 x 2,5-Zoll-Hot-Plug-Festplatte, 1 TB, 7.200 U/min, NL-SAS, 6 Gbit/s 4 x 2,5-Zoll-Hot-Plug-Festplatte, 2 TB, 7.200 U/min, NL-SAS, 12 Gbit/s, 512e
RAID-Controller	Extern: PERC H830 RAID Intern: PERC H730P

Last Modified: September 14 2016, 12:09PM

Element	Beschreibung
Netzwerkschnittstellenkarte	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DP-Netzwerk-Tochterkarte

Caution: Durch das Öffnen des Appliance-Gehäuses erlischt die Gewährleistung, es sei denn, Sie wurden von RSA Cutomer CARE explizit dazu aufgefordert. Die Festplatten und Netzteile können vor Ort von einem qualifizierten Techniker ausgetauscht werden.

Last Modified: September 14 2016, 12:09PM

Installieren eines Deep-Rack-Adapters für eine R630-Appliance

Verfahren

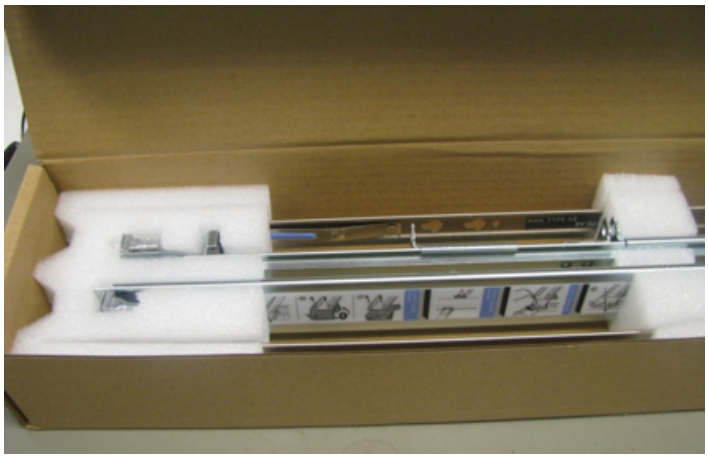
Note: Dieses Verfahren ist nur anwendbar, wenn Sie die S5 R630-Appliance im EMC Titan D Ultra Rack installieren.

Bei der Installation der S5 R630-Appliance in das EMC Titan D Ultra Rack ist ein 1U-Deep-Rack-Adapter erforderlich. Befolgen Sie dieses Verfahren, um eine neue Halterung auf den Serverschienen zu installieren.

1. Suchen Sie in der Zubehörkiste im Karton der R630-Appliance nach der alternativen Schienenhalterung.

Last Modified: September 14 2016, 12:09PM

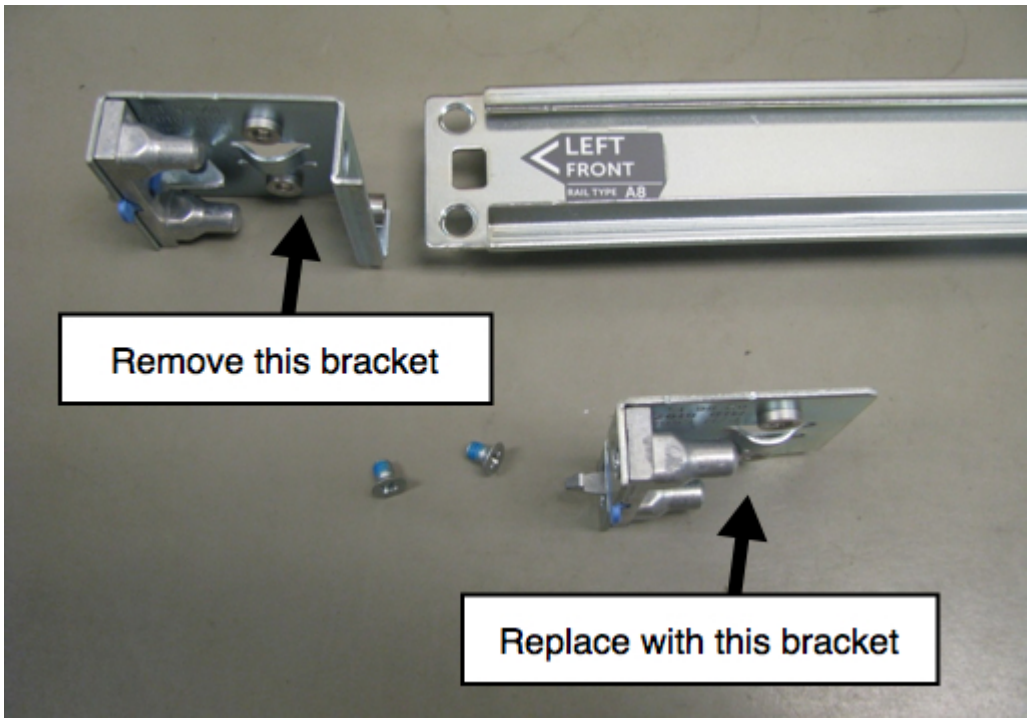
2. Entnehmen Sie die linke Schiene aus dem Schienenkarton.



Jede Schiene ist markiert.

3. Verwenden Sie einen Kreuzschlitz-Schraubendreher, um die beiden Befestigungsschrauben zu entfernen.

4. Entfernen Sie die Halterung und ersetzen Sie sie durch die neue Halterung.



5. Verwenden Sie die Schrauben, um die neue Halterung zu befestigen.

Die Schiene ist jetzt bereit für die Installation der R630-Appliance.

RSA

S5 R730xd-Hybrid Appliance – Hardwarebeschreibung

Einführung

Die RSA Security Analytics Serie 5 Hybrid Appliance basiert auf dem Dell PowerEdge R730xd-Gehäuse. Die RSA Security Analytics Serie 5 Hybrid Appliance wird mit installierter Security Analytics 10.5-Hybrid-Appliance-Software geliefert. Die Hybrid-Appliance-Software beinhaltet einen Concentrator und einen Decoder (entweder Log oder Packet).

Die Ersteinrichtung einer Serie 5 Appliance in Ihrem Netzwerk umfasst die folgenden Schritte:

1. Überprüfen Sie die Anforderungen an den Standort und Sicherheitsinformationen im *Bereitstellungshandbuch* zu Ihrer Security Analytics-Softwareversion: Security Analytics 10.5
2. Montieren oder platzieren Sie die Appliance-Hardware sicher gemäß den Anforderungen des Standort.
3. Schließen Sie die Appliance an Ihr Netzwerk an und konfigurieren Sie die Netzwerkparameter in der Appliance: Anschließen der Appliance und Konfigurieren der Netzwerkparameter
4. Schließen Sie die Appliance-Konfiguration in Security Analytics ab: Abschließen der Appliance-Konfiguration in Security Analytics

⚠ **Caution:** Um Schäden an den Security Analytics-Servern und -Appliances zu vermeiden, entfernen Sie diese aus dem Rack und zerlegen Sie das Rack, bevor Sie sie an einen anderen Standort transportieren. Befolgen Sie die Empfehlungen des Serverherstellers und des Rack-Hersteller bezüglich Verpackung, Transport und Installation.
RSA bietet keine Unterstützung für den erneuten Versand der in einem Rack montierten Server. Der Kunde übernimmt alle Risiken und die Haftung für den Transport von in einem Rack montierten Security Analytics-Servern und -Appliances.

Lieferumfang

Überprüfen Sie den Inhalt der Verpackung, um sich zu vergewissern, dass Sie alle für die Installation und Konfiguration der Hybrid-Appliance erforderlichen Komponenten erhalten haben.

- Serie 5 Hybrid-Appliance
- Statische ReadyRails-Schienen (1 Satz)
- 2U-Adapter für linke Schiene für EMC Deep-Rack
- 2U-RSA-Blende (1) (Schlüssel mit Klebeband an Blende befestigt)
- Netzkabel (2)
- Handbuch mit Produktinformationen von Dell (1)
- Ordner mit RSA-Dokumentation (1)

Last Modified: September 14 2016, 12:09PM

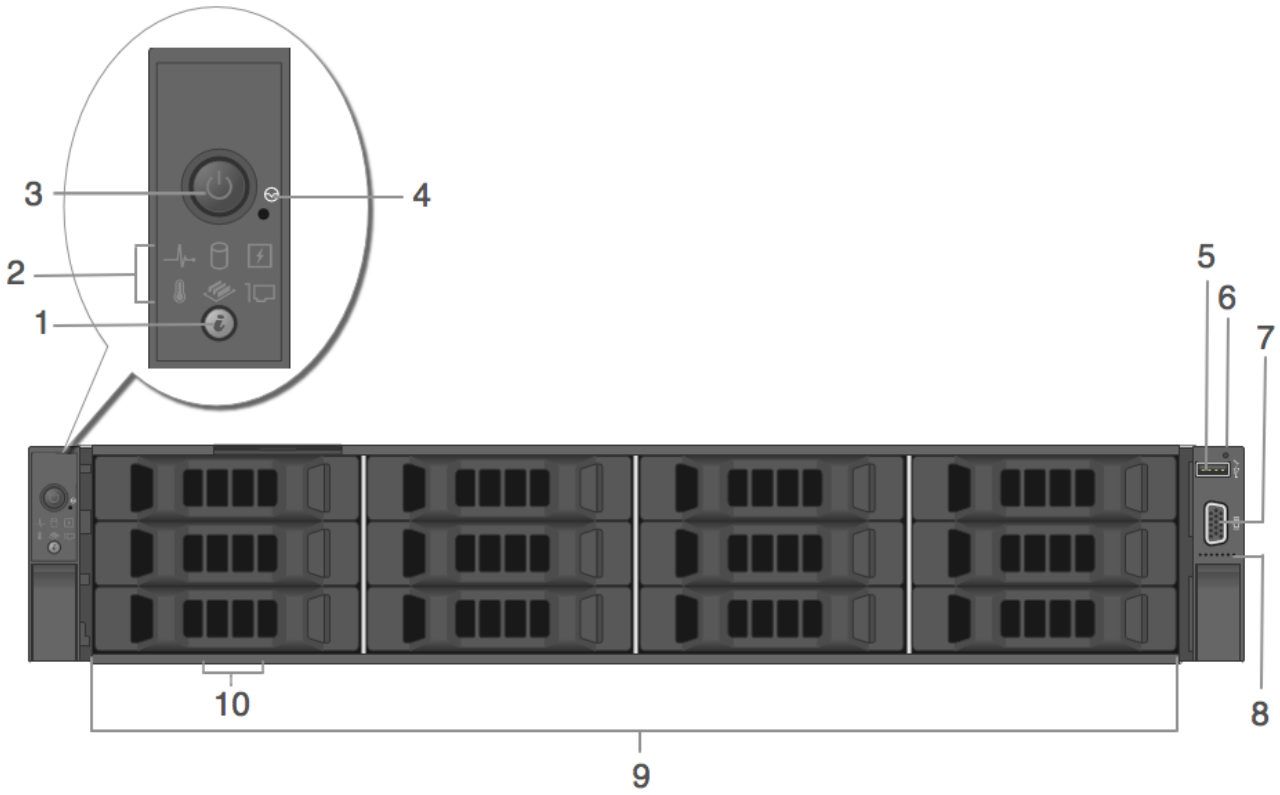
- RSA-EULA (1)

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

Vorderansicht der Security Analytics Hybrid Appliance

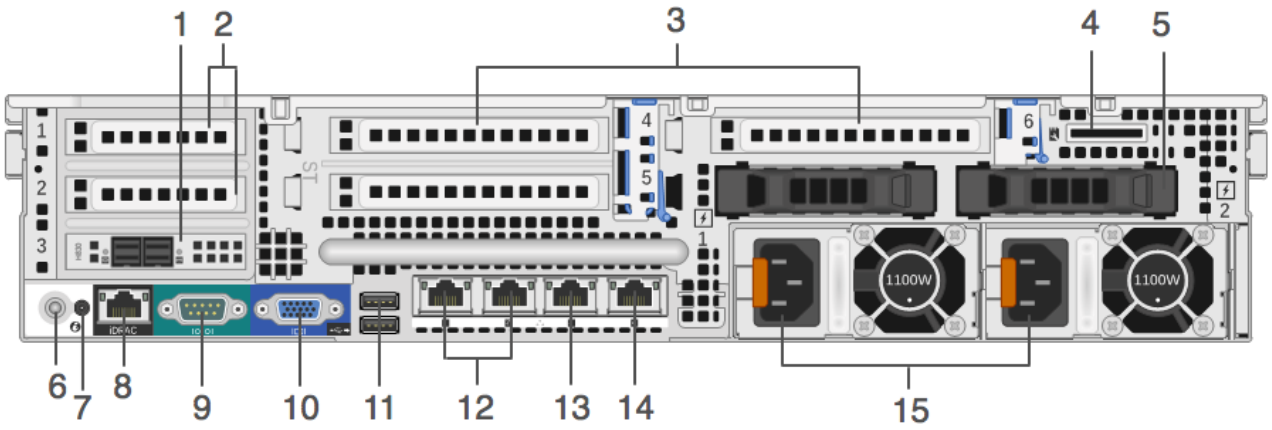


Schlüssel	Beschreibung
1	Systemidentifizierungstaste
2	Diagnoseanzeigen
3	In Betrieb/Nicht in Betrieb

Last Modified: September 14 2016, 12:09PM

Schlüssel	Beschreibung
4	Versenkte NMI-Taste (Non-Maskable Interrupt)
5	USB-Managementport/iDRAC Direct
6	iDRAC Direct-LED-Anzeige
7	Videoanschluss
8	Quick Sync (optional)
9	12 3,5-Zoll-HDDs (Festplatten) (vor Ort austauschbar). Die Security Analytics Hybrid Appliance verfügt über insgesamt 14 Festplatten. 12 HDDs an der Vorder- und 2 SSDs (Solid-State-Laufwerke) an der Rückseite. Zusätzliche Details finden Sie in den technischen Daten der Appliance.
10	Position des Informationsetiketts

Rückansicht der Security Analytics Hybrid Appliance



Schlüssel	Beschreibung
1	PERC H830-RAID-Controller. Dieser ist im halbhohen PCIe-Steckplatz 3 dargestellt, kann aber in einem anderen halbhohen PCIe-Steckplatz installiert werden. Der PERC H830 ist der RAID-Controller für den Speichererweiterungs-DAC. Für die Verbindung mit dem DAC ist ein Kabel mit einem Mini-SAS-Anschluss erforderlich.
2	PCIe-Erweiterungskarten-Steckplätze 1 und 2 mit halber Höhe
3	PCIe-Erweiterungskarten-Steckplätze (3) mit voller Höhe
4	vFlash-Medienkarten-Steckplatz
5	2 2,5-Zoll-SSDs (Hot-Swap-fähig)

Last Modified: September 14 2016, 12:09PM

Schlüssel	Beschreibung
6	Systemidentifizierungstaste
7	Systemidentifizierungsanschluss
8	iDRAC8 Enterprise-Port
9	Serieller RS232-Port (serielle Verbindung zu einem Laptop über DB9 oder einen seriellen Server)
10	VGA-Videoport (Monitor)
11	USB-Ports (Tastatur, Maus, USB-Stick usw.)
12	10G-Base-T-Gigabit-Ethernetports: em3-4
13	Primärer 1000Base-T-Netzwerk-Managementport: em1
14	Sekundärer 1000Base-T-Netzwerkport: em2
15	Hot-Swap-fähige Netzteile 1 und 2 (vor Ort austauschbar)

Note: Für die Verbindung des PERC H830-RAID-Controller mit dem DAC ist ein Kabel mit einem Mini-SAS-Anschluss erforderlich.

Security Analytics Hybrid Appliance – Technische Daten

Element	Beschreibung
Formfaktor	2U, volle Tiefe
Gewicht (ca.)	36,5 kg
Abmessungen (ca.)	H: 8,73 cm x B: 48,2 cm x D: 75,58 cm
Netzteile	Zwei Hot-Plug-fähige, redundante Netzteile (1+1), 1100 W
Prozessoren	2 x E5-2680v3
RAM	16 x 8-GB-2.133-MT/s-RDIMMs (128 GB)
Festplatten	Die Security Analytics Hybrid Appliance verfügt über insgesamt 14 Festplatten. 12 HDDs an der Vorder- und 2 SSDs (Solid-State-Laufwerke) an der Rückseite. 2 x 800-GB-SSD (Rückseite) 4 x 1 TB, 7.200 U/min, NL-SAS, 6 Gbit/s 8 x 6 TB, 7.200 U/min, NL-SAS, 6 Gbit/s
RAID-Controller	Extern: PERC H830 RAID Intern: PERC H730P

Last Modified: September 14 2016, 12:09PM

Element	Beschreibung
Netzwerkschnittstellenkarte	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DP-Netzwerk-Tochterkarte

Caution: Durch das Öffnen des Appliance-Gehäuses erlischt die Gewährleistung, es sei denn, Sie wurden von RSA Cutomer CARE explizit dazu aufgefordert. Die Festplatten und Netzteile können vor Ort von einem qualifizierten Techniker ausgetauscht werden.

Last Modified: September 14 2016, 12:09PM

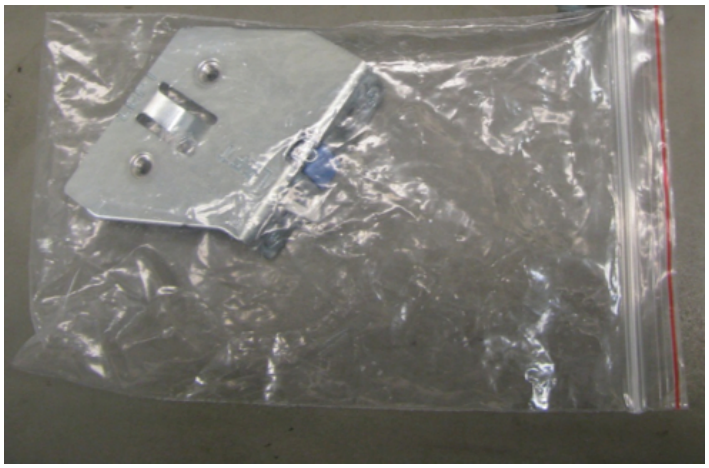
Installieren eines Deep-Rack-Adapters für eine R730xd-Hybrid Appliance

Verfahren

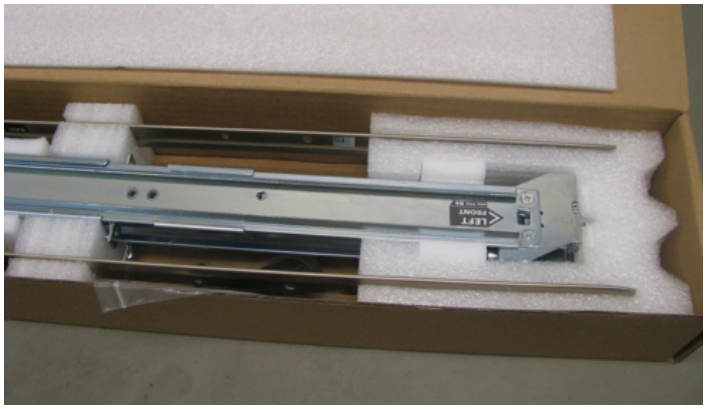
Note: Dieses Verfahren ist nur anwendbar, wenn Sie die S5 R730xd-Hybrid Appliance im EMC Titan D Ultra Rack installieren.

Bei der Installation der S5 R730xd-Hybrid Appliance in das EMC Titan D Ultra Rack ist ein 2U-Deep-Rack-Adapter erforderlich. Befolgen Sie dieses Verfahren, um eine neue Halterung auf den Serverschienen zu installieren.

1. Suchen Sie in der Zubehörkiste im Karton der R730xd-Hybrid Appliance nach der alternativen Schienenhalterung.



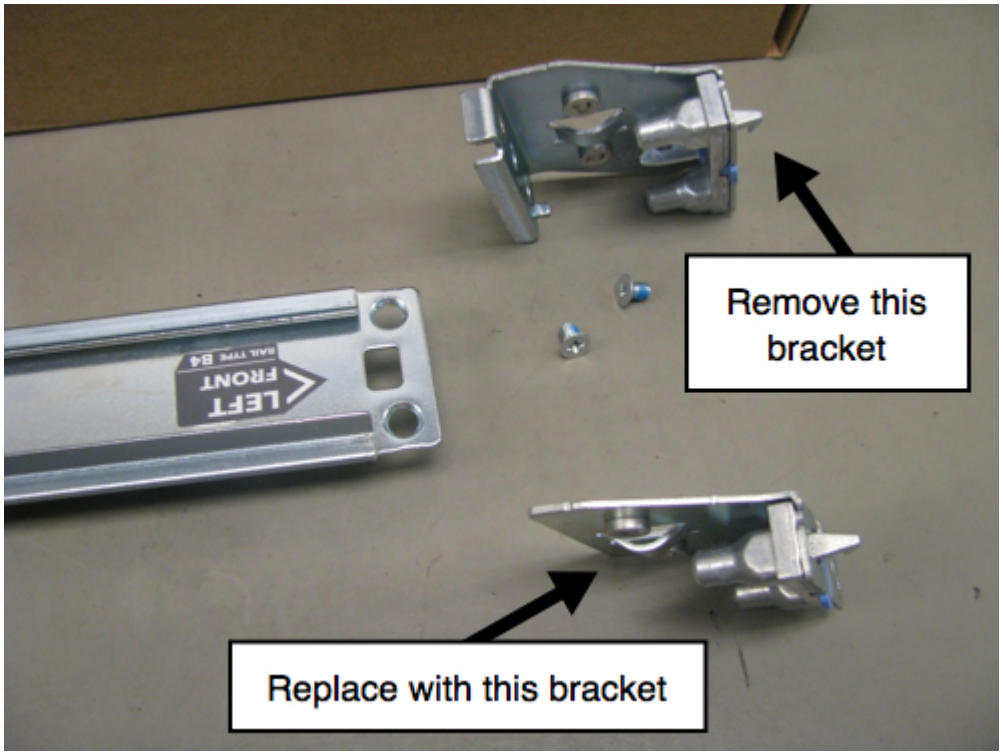
2. Entnehmen Sie die linke Schiene aus dem Schienenkarton. Jede Schiene ist markiert.



Last Modified: September 14 2016, 12:09PM

3. Verwenden Sie einen Kreuzschlitz-Schraubendreher, um die beiden Befestigungsschrauben zu entfernen.

4. Entfernen Sie die Halterung und ersetzen Sie sie durch die neue Halterung.



Last Modified: September 14 2016, 12:09PM

5. Verwenden Sie die Schrauben, um die neue Halterung zu befestigen.

Die Schiene ist jetzt bereit für die Installation der R730xd-Hybrid Appliance.

Last Modified: September 14 2016, 12:09PM

RSA

Anschließen der Appliance und Konfigurieren der Netzwerkparameter

Überblick

Dieses Thema enthält Anweisungen zum Verbinden einer Security Analytics S5 Appliance mit Ihrem Netzwerk und zur Konfiguration der Netzwerkparameter auf der Appliance.

Voraussetzungen

Sammeln Sie für jede Security Analytics Serie 5 Appliance die Informationen in der folgenden Tabelle und notieren Sie sie.

Konfiguration	Standard	Ihre Appliance
Anmeldung	root	
Passwort	netwitness	
System-IP-Adresse	192.168.1.1	
Systemnetzmaske	255.255.255.0	
Standardgateway		
Primärer DNS-Server IP-Adresse		
Sekundärer DNS-Server IP		
Lokaler Domainname (oder keiner)		
Nicht qualifizierter Hostname	NWAPPLIANCE<xxxxxx>, wobei <xxxxxx> eine generierte zufällige Zahl ist.	
IP-Adresse des Security Analytics-Servers		

Last Modified: September 14 2016, 12:09PM

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

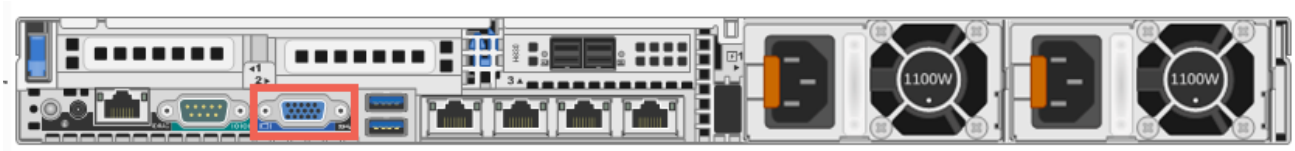
Einführung

Die Konfiguration der Netzwerkparameter für eine RSA Security Analytics S5 Appliance besteht aus dem Festlegen der Standard-IP-Adresse, des DNS-Servers, des Hostnamens und der Netzwerk-Uhrzeitquelle. Zum Festlegen dieser Parameter können Sie mit einer Tastatur und einer Maus eine Verbindung zur Appliance-Konsole herstellen.

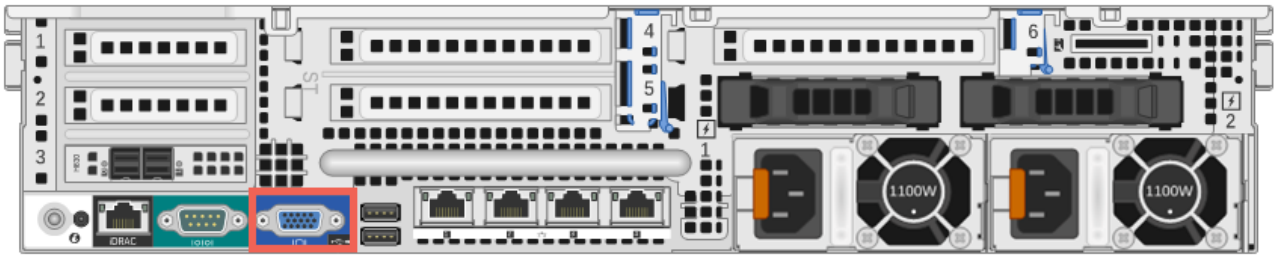
Die bevorzugte Vorgehensweise besteht darin, das Provisioning von Security Analytics Server vor der Konfiguration der anderen Security Analytics-Appliances vorzunehmen.

Verbinden mit der Appliance-Konsole

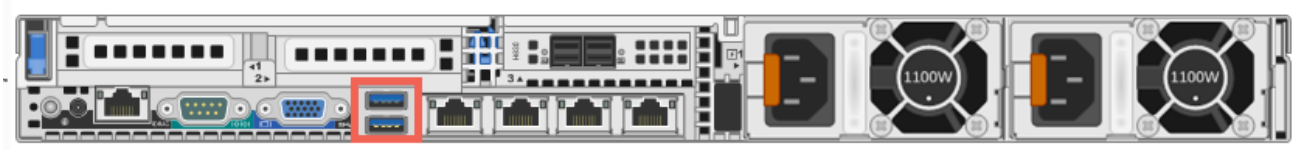
1. Schließen Sie einen Monitor oder einen KVM-Adapter an den VGA-Port auf der Rückseite der Appliance an.



Die folgende Abbildung zeigt die Position des VGA-Ports der Hybrid Appliance.

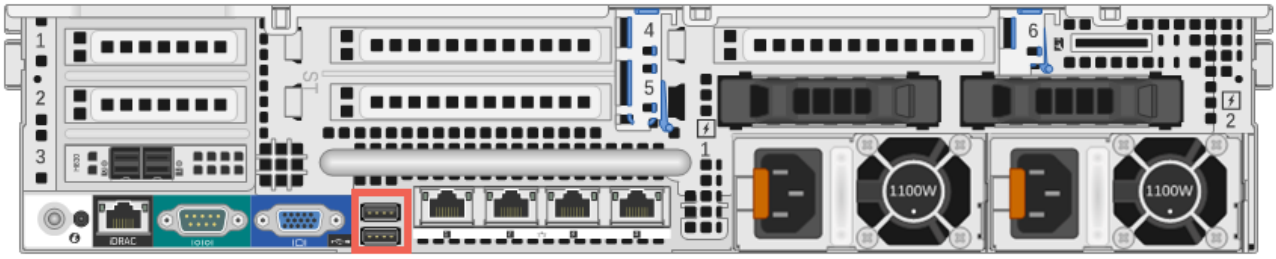


2. Schließen Sie eine Tastatur oder einen KVM-Adapter an einen der USB-Ports auf der Rückseite der Appliance an.

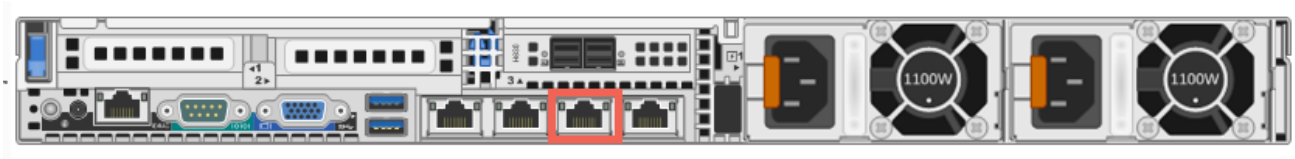


Last Modified: September 14 2016, 12:09PM

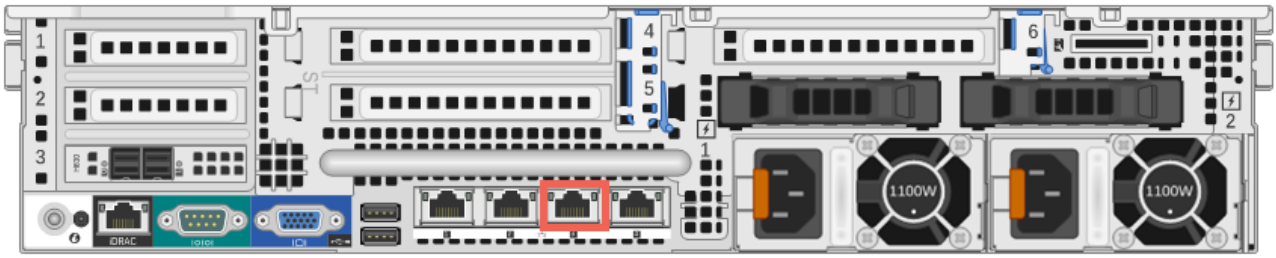
Die folgende Abbildung zeigt die Position des USB-Ports der Hybrid Appliance.



3. Schließen Sie ein Ethernet-Kabel aus dem Netzwerk an den em1-Port auf der Rückseite der Appliance an.



Die folgende Abbildung zeigt die Position des em1-Ports der Hybrid Appliance.



4. 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.

5. Schalten Sie die Appliance ein und fahren Sie mit dem Abschnitt Konfigurieren der Netzwerkparameter fort.

Konfigurieren der Netzwerkparameter

1. Geben Sie in der Anmeldeaufforderung die Standardanmeldedaten ein, um Zugriff auf das Betriebssystem zu erhalten:

```
NWAPPLIANCE<xxxxxx> login: root
Password: netwitness
```

> **Note:** Wenn die Aufforderung zum Konfigurieren der Netzwerkparameter nicht angezeigt wird, können Sie `#netconfig.sh` über die Befehlszeile ausführen, um die Aufforderung zur Eingabe der Konfigurationsoptionen einzublenden.

2. Geben Sie die folgenden Informationen ein, wenn Sie dazu aufgefordert werden:
   a. System-IP-Adresse (oder **d** für DHCP)
   b. Systemnetzmaske
   c. Standardgateway

Last Modified: September 14 2016, 12:09PM

d. Primäre IP-Adresse des DNS-Servers
e. Sekundäre IP des DNS-Servers (oder drücken Sie die **Eingabetaste** für keine)
f. Lokaler Domainname (oder drücken Sie die **Eingabetaste**für keinen)
g. Nicht qualifizierter Hostname

Nach Abschluss der Erstkonfiguration sollte wie in der folgenden Abbildung dargestellt eine Aufforderung zum Speichern der Konfiguration angezeigt werden.

3. Überprüfen Sie die eingegebenen Informationen und geben Sie `y` ein, um die Konfiguration zu speichern. Dadurch werden die Netzwerkinformationen festgelegt und die Netzwerkservices werden neu gestartet.
4. Wenn die Appliance kein Security Analytics-Server ist,**warten Sie ca. 15 Sekunden auf eine Eingabeaufforderung** und geben Sie anschließend die IP-Adresse des Security Analytics-Servers in der Eingabeaufforderung ein.
5. Überprüfen Sie die Netzwerkverbindung mithilfe eines Ping-Tests Ihres DNS-Servers.
6. Fahren Sie mit dem Abschnitt Angeben der Netzwerk-Uhrzeitquelle fort.

Angeben der Netzwerkzeitquelle

Die Zeitsynchronisation zwischen den Services und Appliances muss konfiguriert werden. Es wird dringend empfohlen, für die Synchronisation eine NTP-Zeitquelle zu verwenden. Die Zeit ist nicht nur wichtig für die zugrunde liegende Kommunikation zwischen den Services, nicht synchronisierte Appliances können auch zu falschen Zeitangaben während der Datenanalyse führen. 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 Security Analytics-Schnittstelle nachgeholt werden.

Last Modified: September 14 2016, 12:09PM

Best Practices

RSA empfiehlt die folgenden Best Practices:

Konfigurieren Sie für eine bessere Datenintegrität den Security Analytics-Server als Uhrzeitquelle für alle anderen Appliances. Alle Appliances, einschließlich ESA (Event Stream Analysis), beziehen die Zeit vom Security Analytics-Server. Nur für den Security Analytics-Server ist eine externe NTP-Zeitquelle konfiguriert.

Verwenden Sie für die Security Analytics Server Appliance das Dienstprogramm NwConsole zur Verbindung mit der NTP-Zeitquelle.

Wenn die anderen Appliances Security Analytics 10.5.1 oder höher verwenden, wird die Zeit auf allen mit der Security Analytics Server-Appliance verbundenen Appliances automatisch festgelegt. Wenn die anderen Appliances nicht über Security Analytics 10.5.1 oder höher verfügen, legen Sie als Zeitquelle manuell den Security Analytics-Server fest.

Festlegen der Zeit auf dem Security Analytics-Server mit dem Dienstprogramm NwConsole

So legen Sie die Netzwerk-Uhrzeitquelle auf dem Security Analytics-Server mithilfe des Dienstprogramms NwConsole fest:

1. Geben Sie in der Root-Eingabeaufforderung `[root@NwAppliance~]#` den folgenden Befehl ein:
   `NwConsole`
   NwConsole wird gestartet und die Startmeldung mit einer Version und dem Datum wird angezeigt:
   `RSA Security Analytics Console`
2. Geben Sie in der NwConsole den folgenden Befehl ein:
   `login localhost:50006 <username> <password>`
   Der Benutzername des Systemadministratorkontos für Security Analytics ist **admin** und das Standardpasswort lautet**netwitness**.
   Sie werden bei der Appliance angemeldet und die folgende Meldung wird angezeigt:
   `Successfully logged in as session <session #>`
3. Führen Sie in der localhost-Eingabeaufforderung `[localhost:50006] />` eine der folgenden Aktionen aus:
   a. Wenn Sie die Netzwerk-Uhrzeitquelle verwenden möchten, geben Sie den folgenden Befehl ein:
      `appliance setNTP source=<NTP_server_hostname or IP_address>`
      Beispiel: **`appliance setNTP source=0.pool.ntp.org`**
   b. Wenn Sie die Uhr der Appliance als Uhrzeitquelle verwenden möchten, geben Sie Folgendes ein: **`appliance setNTP source=local`**
4. 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.

Last Modified: September 14 2016, 12:09PM

RSA

Abschließen der Appliance-Konfiguration in Security Analytics

Einführung

Um die Konfiguration einer Serie 5 Appliance abzuschließen, müssen Sie sich bei Security Analytics anmelden und die im Modul Security Analytics Administration verfügbaren Konfigurationsoptionen verwenden. Die Konfigurationsschritte für jeden Appliance-Typ unterscheiden sich leicht. Dieser Abschnitt enthält grundlegende Informationen und Links zu Onlinehilfe-Dokumenten, die Sie durch den Prozess führen.

Melden Sie sich bei Security Analytics an.

RSA Security Analytics ist eine webbasierte Anwendung, die Sie in einem Browserfenster starten. Kompatible Browser umfassen alle Browser, die WebSockets, LocalStorage und die HTML5 History API unterstützen: Google Chrome, Apple Safari, Mozilla Firefox und Internet Explorer 10 und höher.

1. Geben Sie in Ihrem Webbrowser Folgendes ein:
   `https://<hostname or IP address>/login`
   wobei `<hostname or IP address>` der Hostname oder die IP-Adresse des Security Analytics-Servers ist.

Last Modified: September 14 2016, 12:09PM

Der Security Analytics-Anmeldebildschirm wird angezeigt.

2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf **Anmelden**.
   Der Benutzername des Systemadministratorkontos für Security Analytics ist **admin** und das Standardpasswort lautet **netwitness**.

Öffnen der Onlinehilfe

Anweisungen zur Konfiguration der einzelnen Appliances werden abhängig von der auf der Appliance installierten Softwareversion bereitgestellt.

Lesen Sie zu Security Analytics 10.5 diese Dokumente: Host- und Services-Konfigurationsleitfäden und Lizenzierungsleitfaden.Ein guter Ausgangspunkt für das Verständnis des allgemeinen Konfigurationsprozesses und für den Beginn der Konfiguration ist der *Host and Service Getting Started Guide*.

Last Modified: September 14 2016, 12:09PM