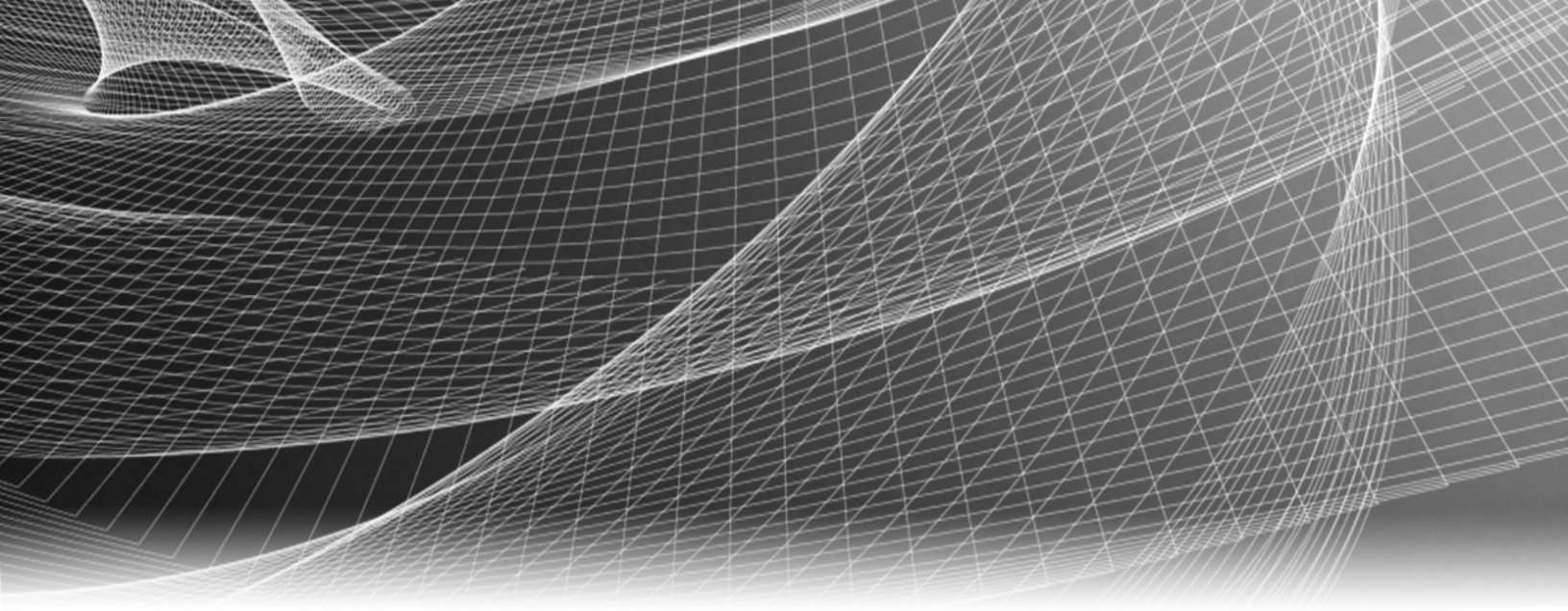


RSA Security Analytics

S4 RSA Analytics Warehouse (MapR-basiert) – 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 RSA Analytics Warehouse (MapR-basiert) – Konfigurationshandbuch

RSA

S4 RSA Analytics Warehouse (MapR-basiert) – Konfigurationshandbuch

Überblick

In diesem Dokument wird die Installation des RSA Analytics Warehouse (MapR) und sein Anschluss an das Netzwerk Schritt für Schritt beschrieben. Dieses Warehouse wurde bisher als Security Analytics Warehouse (SAW) bezeichnet.

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 Warehouse 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.

Note: Beachten Sie beim Lesen eines gedruckten Handbuchs, dass eventuell online unter **sadocs.emc.com/de-de** eine neuere Version erhältlich ist. Dieses Handbuch ist in der Security Analytics-Onlinehilfe unter "Hardware-Installationshandbücher" verfügbar.

Last Modified: September 14 2016, 12:09PM

RSA

S4 Warehouse – Hardwarebeschreibung

Überblick

In diesem Thema wird das RSA Serie 4 Warehouse kurz vorgestellt. Zudem werden die Steuerelemente und Anschlüsse beschrieben und einige technische Daten aufgeführt.

Einführung

Das RSA Serie 4 Warehouse wird mit installierter Warehouse-Software geliefert. Die Ersteinrichtung des Warehouse in Ihrem Netzwerk umfasst die folgenden Schritte:

1. Lesen Sie die Standortanforderungen und Sicherheitsinformationen.
2. Montieren Sie die Warehouse-Hardware.
3. Schließen Sie das Warehouse an Ihr Netzwerk an und konfigurieren Sie die Netzwerkparameter im Warehouse.
4. Stellen Sie die Konfiguration des Warehouse in Security Analytics fertig.

Vor der Konfiguration der Softwareparameter kann die erstmalige physische Verbindung zum Warehouse 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 Warehouse erforderlichen Komponenten erhalten haben.

- Serie 4 Warehouse-Appliance
- Schienenbaugruppen (2)
- Netzkabel (2)

Materialien vom Kunden

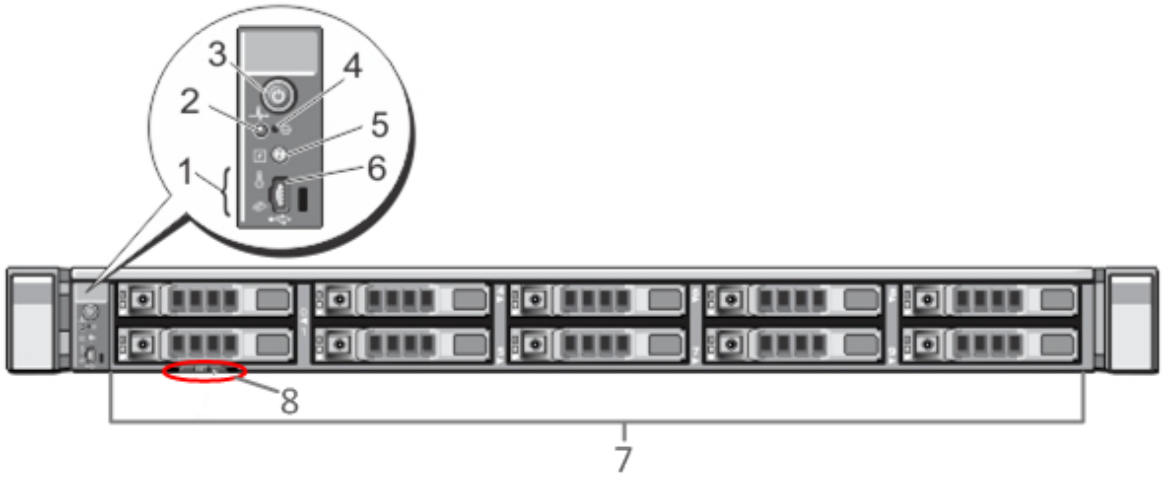
Zur Durchführung des Konfigurationsverfahrens benötigen Sie Folgendes:

- Zwei Ethernet-Netzwerkkabel

Last Modified: September 14 2016, 12:09PM

- 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

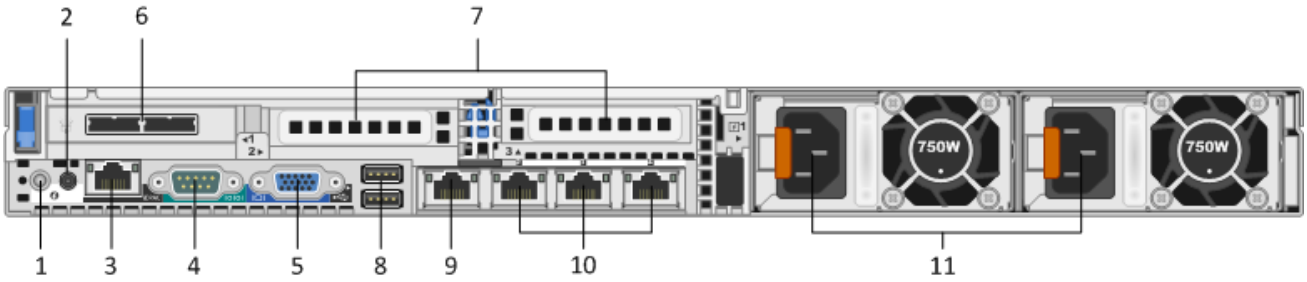
Vorderansicht des Warehouse



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 Das Warehouse ist mit zehn 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 Warehouse



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-10Gbit/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 des Warehouse

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 RSA S4 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 RSA S4 Appliance umfasst das Festlegen der Standard-IP-Adresse und des Hostnamens, die Konfiguration der DNS-Server und der Datei **/etc/hosts** sowie das Festlegen 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 Befehlszeilenschnittstelle 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:

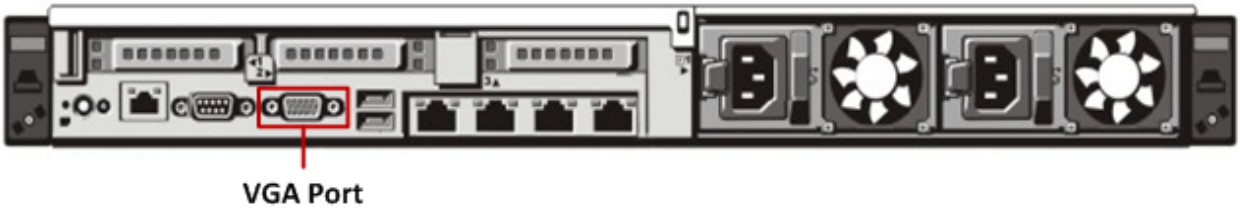
- Appliance-Konsole über VGA-Verbindung: Tastatur (USB-Port) und Monitor (VGA-Port)
- Appliance-Konsole über Netzwerkverbindung: Computer mit einem SSH-Client, der über ein Ethernetkabel zum Managementport (em1) mit der Appliance verbunden ist, die standardmäßig als 192.168.1.1 konfiguriert ist

Appliance-Konsole über VGA-Verbindung

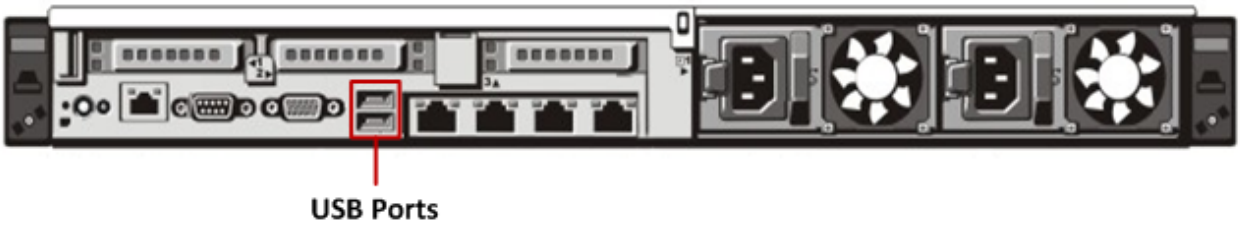
So verwenden Sie die Appliance-Konsole über die VGA-Verbindung:

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.

> ⚠ **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 (`root/netwitness`), um Zugriff auf das Betriebssystem zu erhalten.
5. Fahren Sie mit dem Abschnitt **Festlegen der IP-Adresse** unten fort.

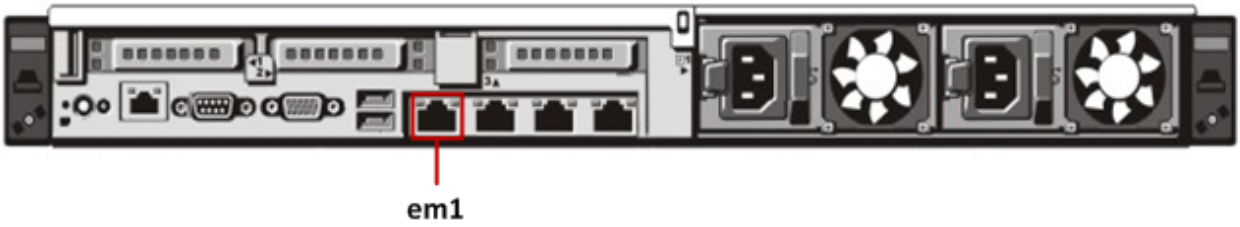
Appliance-Konsole über Netzwerkverbindung

> ⚠ **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. Verwenden Sie in der Anmeldeaufforderung die Standardanmeldedaten (`root`/`netwitness`), um Zugriff auf das Betriebssystem zu erhalten.
5. Fahren Sie mit dem Abschnitt **Festlegen der IP-Adresse** unten fort.

Festlegen der IP-Adresse

In der Warehouse-Appliance muss das Netzwerk manuell konfiguriert werden. Wenn Sie Cluster der Warehouse-Appliances haben möchten, stellen Sie sicher, dass Sie die folgenden Aufgaben auf allen Appliances im Cluster durchführen. Für jede Appliance im Cluster muss die IP-Adresse entweder über die Appliance-Konsole oder über die Dell Remote Access Console (iDRAC) konfiguriert werden. Weitere Informationen zur iDRAC finden Sie in der Dell Dokumentation.

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

Abhängig von Ihren jeweiligen Anforderungen müssen folgende Netzwerkschnittstellen konfiguriert werden:

Schnittstellen	Zweck
em1	Öffentlich, Verbindung mit dem Kunden-Switch
em2	Privat, Verbindung mit dem dedizierten Warehouse-Switch
em3	Offen, Verbindung mit einem beliebigen Switch oder Netzwerk
em4	Offen, Verbindung mit einem beliebigen Switch oder Netzwerk

Last Modified: September 14 2016, 12:09PM

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: eth0
BOOTPROTO	static
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`
4. (Optional) Konfigurieren Sie die Netzwerkschnittstelle em2, wenn die interne Schnittstelle, die von der jeweiligen Warehouse-Appliance zur Kommunikation mit anderen Warehouse-Appliances im Cluster verwendet wird, mit einem Switch verbunden ist. Die zugehörige Konfigurationsdatei hat den Namen **/etc/sysconfig/network-scripts/ifcfg-em2**.

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.

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** mithilfe des folgenden Befehls:
   `vi /etc/sysconfig/network`
3. Ergänzen oder ändern Sie die Konfiguration wie folgt:
   `NETWORKING=[yes|no]`

`HOSTNAME=<sawnode_hostname>`
wobei `<sawnode_hostname>` der Hostname der Warehouse-Appliance ist.
`DOMAINNAME = <Wert>`

> **Note:** Sie können einen Wert für `DOMAINNAME` eingeben, wenn in Ihrem Unternehmen ein Domainname für die Warehouse Node-Hostnamen benötigt wird. Wenn Sie keinen Domainnamen verwenden möchten, lassen Sie den Wert leer.

4. Geben Sie zum Speichern der Änderungen und Beenden des vi-Editors 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, indem Sie folgenden Befehl eingeben:
   `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 Domainname ist.
   Beispiel:
   `nameserver 192.168.0.1`
   `search acmecorp.com`
4. Geben Sie zum Speichern der Änderungen und Beenden des vi-Editors den folgenden Befehl ein:
   `:wq`

Konfigurieren der Datei /etc/hosts

Fügen Sie in die Datei **hosts** der Appliance die IP-Adresse und den Hostnamen aller Warehouse-Nodes im Cluster ein.

> **Caution:** Der Hostname der Warehouse-Nodes 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 für jeden der Warehouse-Nodes die folgende Zeile in die Datei ein:
   `<node_private_ip_address> <node_fqdn> <node_hostname>`

Last Modified: September 14 2016, 12:09PM

Dabei gilt Folgendes:
`<node_private_ip_address>` ist die private Schnittstelle des Node im Warehouse-Cluster.
`<node_fqdn>` ist der vollständig qualifizierte Domainname des Node im Warehouse-Cluster.
`<node_hostname>` ist der Hostname des Node im Warehouse-Cluster.

Fügen Sie die Daten aller Nodes im Warehouse-Cluster in separaten Zeilen in die Datei **/etc/hosts** ein.

Beispiel für die Datei **/etc/hosts** mit den Daten aller Nodes im Warehouse-Cluster:

```
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
192.168.1.10 sawnode1.domainname.com sawnode1
192.168.1.11 sawnode2.domainname.com sawnode2
192.168.1.12 sawnode3.domainname.com sawnode3
```

4. Geben Sie zum Speichern der Änderungen und Beenden des vi-Editors den folgenden Befehl ein:
   `:wq`

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. Die NTP-Einstellungen (Network Time Protocol) in der Datei /etc/ntp.conf auf der Warehouse-Appliance müssen manuell aktualisiert werden.

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 Serverliste mit den betreffenden 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. Geben Sie zum Speichern der Änderungen und Beenden des vi-Editors den folgenden Befehl ein:
   `:wq`
5. Geben Sie zum Neustarten des Services den folgenden Befehl ein:
   `service ntpd restart`

Last Modified: September 14 2016, 12:09PM

RSA

Abschließen der Warehouse-Konfiguration in Security Analytics

Überblick

Dieses Thema enthält Anweisungen zum Abschließen der RSA Analytics Warehouse (MapR)-Konfiguration.

Einführung

Zum Fertigstellen der Konfiguration des Warehouse sind folgende abschließende Schritte erforderlich:

1. Erzeugen und Aktualisieren der Standard-UUID in den Appliances
2. Aktualisieren der Hive Server-Version in der Appliance
3. Aktualisieren der Konfigurationsvorlagendatei in der Warehouse-Appliance
4. Installieren der Warehouse-Lizenzdatei
5. Erzeugen der virtuellen IP-Adresse für die Warehouse-Appliance
6. Konfigurieren von Warehouse-Connector zum Schreiben in Warehouse
7. Hinzufügen von Warehouse-Datenquellen zur Reporting Engine

Detaillierte Anweisungen hierzu erhalten Sie im *RSA Analytics Warehouse (MapR)-Konfigurationsleitfaden* (Security Analytics 10.4) oder im *Security Analytics Warehouse-Konfigurationsleitfaden* (Security Analytics 10.3 und früher) in der Onlinehilfe auf sadocs.emc.com/de-de.

Last Modified: September 14 2016, 12:09PM