



# Handbuch zur Installation physischer Hosts

für Version 11.0



## **Kontaktinformationen**

Der RSA-Link unter <https://community.rsa.com> enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

## **Marken**

Eine Liste der RSA-Marken finden Sie unter [germany.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://germany.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **Lizenzvereinbarung**

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

## **Drittanbieterlizenzen**

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

## **Hinweis zu Verschlüsselungstechnologien**

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

## **Verteilung**

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2018

# Inhalt

---

<b>Einführung</b> .....	<b>4</b>
Workflow für die Installation physischer Hosts .....	4
Kundensupport .....	4
<b>Installationsvorbereitung – Öffnen von Firewallports</b> .....	<b>5</b>
<b>Installationsaufgaben</b> .....	<b>6</b>
Aufgabe 1: Installieren von 11.0 auf dem NetWitness-Serverhost .....	6
Aufgabe 2: Installieren von 11.0 auf den Hosts anderer Komponenten .....	19
<b>Aktualisieren oder Installieren der Legacy Windows Collection</b> .....	<b>33</b>
<b>Aufgaben nach der Installation</b> .....	<b>34</b>
Aufgabe 1. Beheben von Fehler bei Authentifizierung in 11.0 .....	34
(Optional) Aufgabe 2: Erneutes Konfigurieren von DNS-Servern nach 11.0.0.0 .....	34
(Bedingungsabhängig) Aufgabe 3: Für Warehouse Connector mit Log Collector-Service – Bearbeiten der Datei sshd_config .....	35
<b>Revisionsverlauf</b> .....	<b>38</b>

## Einführung

Die Anweisungen in diesem Handbuch gelten nur für physische Hosts. Anweisungen zum Upgrade Ihrer virtuellen Hosts in 11.0 finden Sie im RSA *NetWitness Suite Setup-Leitfaden für virtuelle Hosts*.

### Workflow für die Installation physischer Hosts

Das folgende Diagramm veranschaulicht den Workflow für die Installation von RSA NetWitness® Suite 11.0 auf physischen Hosts.



### Kundensupport

Auf der Website „Contact RSA Customer Support“ (<https://community.rsa.com/docs/DOC-1294>) in RSA Link finden Sie Informationen darüber, wie Sie Hilfe zu RSA NetWitness Suite 11.0 erhalten.

## Installationsvorbereitung – Öffnen von Firewallports

---

Im Thema „Netzwerkarchitektur und Ports“ im *RSA NetWitness® Suite Bereitstellungsleitfaden* werden alle Ports in einer RSA NetWitness® Suite-Bereitstellung aufgeführt. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

**Achtung:** Fahren Sie erst mit der Installation fort, wenn die Ports in Ihrer Firewall konfiguriert wurden.

## Installationsaufgaben

In diesem Thema werden die Aufgaben beschrieben, die Sie ausführen müssen, um NetWitness Suite 11.0 auf physischen Hosts zu installieren.

Es gibt zwei Hauptaufgaben, die in der angegebenen Reihenfolge durchgeführt werden müssen.

[Aufgabe 1: Installieren von 11.0 auf dem NetWitness-Serverhost](#)

[Aufgabe 2: Installieren von 11.0 auf den Hosts aller anderen Komponenten](#)

### Aufgabe 1: Installieren von 11.0 auf dem NetWitness-Serverhost

Für den NW-Server werden folgende Vorgänge ausgeführt:

- Erstellen eines Basis-Image
- Einrichten des 11.0 NW-Serverhosts

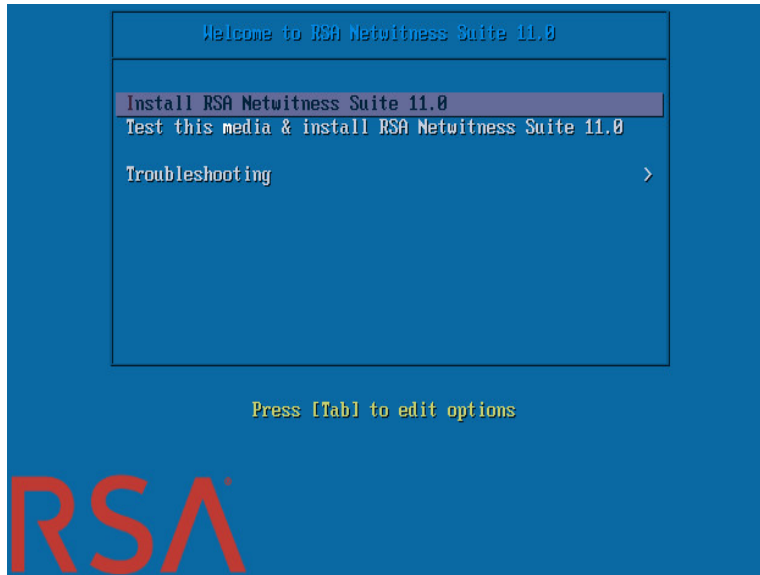
Führen Sie die folgenden Schritte aus, um den 11.0 NW-Serverhost zu installieren:

1. Erstellen Sie ein Basis-Image auf dem Host.
  - a. Verbinden Sie die Medien (d. h. Build-Stick oder DVD-ISO) mit dem Host.  
Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Suite 11.0 Build-Stick*.
    - Hypervisor-Installation: Verwenden Sie die DVD- oder USB-ISO-Images.
    - Physische Medien: Verwenden Sie die DVD-ISO, um eine startfähige optische Festplatte mit vom Benutzer bereitgestellter Imaging-Software zu erstellen, oder die USB-ISO, um startfähige Medien für Flash-Laufwerke mithilfe von Universal Netboot Installer (UNetbootin) oder einem anderen geeigneten Imaging-Tool zu erstellen. In den *Anweisungen zum RSA NetWitness® Suite Build-Stick* finden Sie Informationen zum Erstellen eines Build-Sticks von der USB-ISO. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.
    - iDRAC-Installationen – der Typ der virtuellen Medien lautet:
      - **Virtuelles Diskettenlaufwerk** für zugeordnete Flash-Laufwerke
      - **Virtuelle CD** für zugeordnete optische Mediengeräte oder ISO-Dateien
  - b. Melden Sie sich beim Host an und starten Sie ihn neu.

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

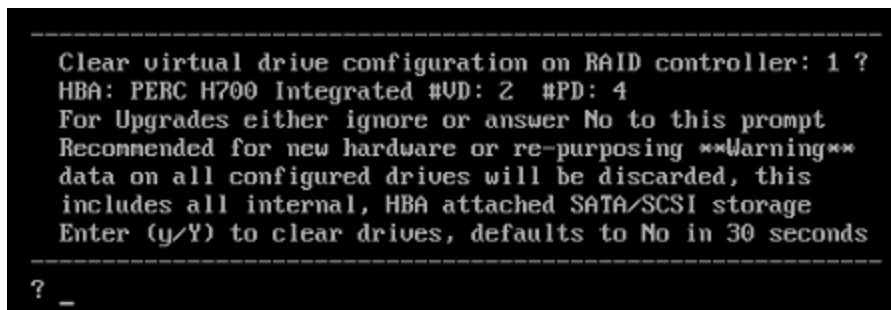
- c. Wählen Sie während des Neustarts **F11** (Startmenü) aus, um ein Startgerät auszuwählen und von den verbundenen Medien zu starten.

Nach einigen Systemprüfungen während des Startvorgangs wird das folgende Installationsmenü angezeigt: **Willkommen bei RSA NetWitness Suite 11.0**. Die Grafiken im Menü werden anders dargestellt, wenn Sie ein physisches USB-Flash-Medium verwenden.



- d. Wählen Sie **RSA NetWitness-Suite 11.0 installieren** (Standardauswahl) aus und drücken Sie die **EINGABETASTE**.

Das Installationsprogramm wird ausgeführt. Es wird bei der Eingabeaufforderung **j/J eingeben, um Laufwerke zu löschen** angehalten, in der Sie aufgefordert werden, die Laufwerke zu formatieren.



- e. Geben Sie **J** ein, um fortzufahren.

Die Standardaktion ist „Nein“. Wenn Sie also die Aufforderung ignorieren, wird innerhalb von 30 Sekunden „Nein“ ausgewählt und die Laufwerke werden nicht gelöscht.

Die Eingabeaufforderung **Für Neustart Eingabetaste drücken** wird angezeigt.

```

Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
Re-labeling disks and virtual drives, clearing RAID configuration ...
0 logical volume(s) in volume group "netwitness_vg00" now active

Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level = #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot

```

- f. Drücken Sie die **EINGABETASTE**, um den Host neu zu starten.

Das Installationsprogramm fordert Sie erneut auf, die Laufwerke zu löschen.

```

-----
Clear virtual drive configuration on RAID controller: 0 ?
HBA: PERC H730P Mini #VD: 2 #PD: 4
For Migrations either ignore or answer No to this prompt
Recommended for new hardware or re-purposing **Warning**
data on all configured drives will be discarded, this
includes all internal, HBA attached SATA/SCSI storage
Enter (y/Y) to clear drives, defaults to No in 30 seconds
-----

```

- g. Geben Sie **N** ein, da Sie die Laufwerke bereits gelöscht haben.

Die Eingabeaufforderung **Q zum Beenden oder R für Neuinstallation eingeben**) wird



angezeigt.

```
-----  
No root level logical volumes found for Migration  
Assuming this system is new or being reinstalled  
Migration cannot proceed, system will be reimaged  
If you had intended to migrate please quit and  
contact support for assistance.  
-----  
Enter Q to Quit or R to Reinstall, Re-installing in 120 seconds?
```

- h. Geben Sie **R** ein, um das Basis-Image zu installieren.

Das Installationsprogramm zeigt die Komponenten an, während sie installiert werden. Dies variiert je nach Appliance. Das Programm wird neu gestartet.

**Achtung:** Starten Sie die angeschlossenen Medien (d. h. den Build-Stick oder die DVD-ISO) nicht neu.

```
CentOS Linux 7 (Core)  
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64  
  
NWAPPLIANCE9240 login: root  
Password:  
[root@NWAPPLIANCE9240 ~]#
```

- i. Melden Sie sich mit den Root-Anmeldedaten beim Host an.
2. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.

Dadurch wird das Setup-Programm gestartet und die EULA wird angezeigt.

**Hinweis:** 1.) Wenn Sie durch die Eingabeaufforderungen des Setup-Programms navigieren, verwenden Sie die Pfeile nach unten und oben, um zwischen den Feldern zu wechseln, die Tabulatortaste, um zwischen den Befehlen zu wechseln (z. B. **<Ja>**, **<Nein>**, **<OK>** und **<Abbrechen>**). Drücken Sie die **EINGABETASTE**, um Ihre Befehlsantwort zu registrieren und mit der nächsten Eingabeaufforderung fortzufahren.  
2.) Das Setup-Programm übernimmt das Farbschema des Desktops oder der Konsole, den bzw. die Sie für den Zugriff auf den Host verwenden.  
3.) Wenn Sie während des Setup-Programms (`nwsetup-tui`) die DNS-Server angeben, **MÜSSEN** diese gültig („gültig“ in diesem Zusammenhang bedeutet gültig während des

Setups) und für `nwsetup-tui` zugänglich sein, damit Sie fortfahren können. Falsch konfigurierte DNS-Server führen dazu, dass die Konfiguration fehlschlägt. Wenn Sie nach dem Setup DNS-Server erreichen müssen, die während des Setups nicht erreichbar waren, (z. B. zur Verlagerung eines Hosts, der über andere DNS-Server verfügt) lesen Sie [\(Bedingungsabhängig\) Aufgabe 1. Erneutes Konfigurieren von DNS-Servern nach 11.0](#) in den Aufgaben nach der Installation.

Wenn Sie während des Setups keinen DNS-Server angeben (`nwsetup-tui`), müssen Sie **1 Lokales Repository (auf dem NW-Server)** in der Eingabeaufforderung **NetWitness Suite Update-Repository** in Schritt 12 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repository zugreifen kann).

By clicking "Accept", you (the "Customer") hereby agree, on behalf of your company or organization, to be bound by the terms and conditions of the End User License Agreement (the "EULA") located at <https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf> with RSA Security LLC ("RSA", or appropriate affiliate entity in the relevant jurisdiction). In addition, Customer hereby agrees and acknowledges that, if Customer chooses to host its data with any third party or in a public cloud environment, RSA has no responsibility for the storage or protection of any Customer data or for any associated security breach notifications. The terms herein and in the EULA shall supersede any relevant terms in any other agreement between the Customer and RSA. For customers of the RSA NetWitness® products, all data analyzed in connection herewith shall be at a cost to Customer based on RSA's then current

<Accept >

<Decline>

92%

3. Gehen Sie zu **Akzeptieren** und drücken Sie die **EINGABETASTE**.

Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.

You must setup an NW Server before setting up any other NetWitness Suite components.

Is this the host you want for your 11.0 NW Server?

< Yes >

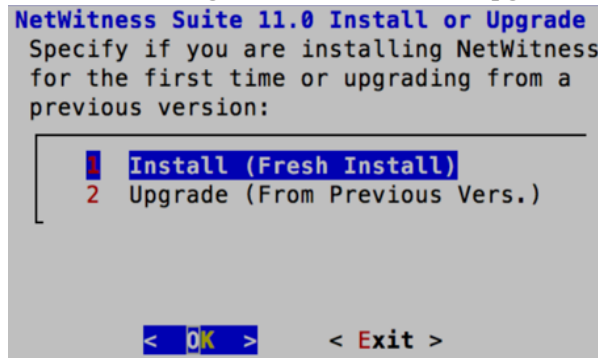
< No >

4. Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**.

Wählen Sie **Nein**, wenn Sie 11.0 bereits auf dem NW-Server installiert haben.

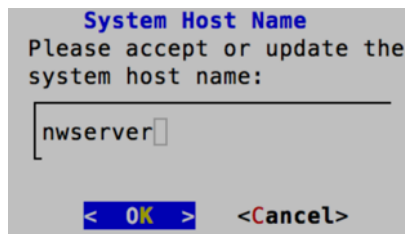
**Achtung:** Wenn Sie den falschen Host für den NW-Server auswählen und das Setup abschließen, müssen Sie das Setup-Programm (Schritt 2) neu starten und alle nachfolgenden Schritte ausführen, um diesen Fehler zu korrigieren.

Die Aufforderung „Installation“ oder „Upgrade“ wird angezeigt.



5. Drücken Sie die **EINGABETASTE** (standardmäßig ist „Installation“ ausgewählt).

Die Aufforderung „Hostname“ wird angezeigt.



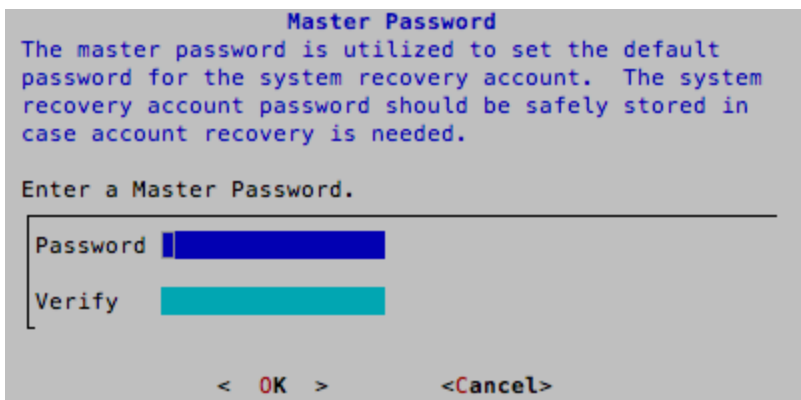
6. Drücken Sie die **EINGABETASTE**, wenn dieser Name beibehalten werden soll. Wenn Sie den Hostnamen bearbeiten möchten, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um ihn zu ändern.

Die Aufforderung „Masterpasswort“ wird angezeigt.

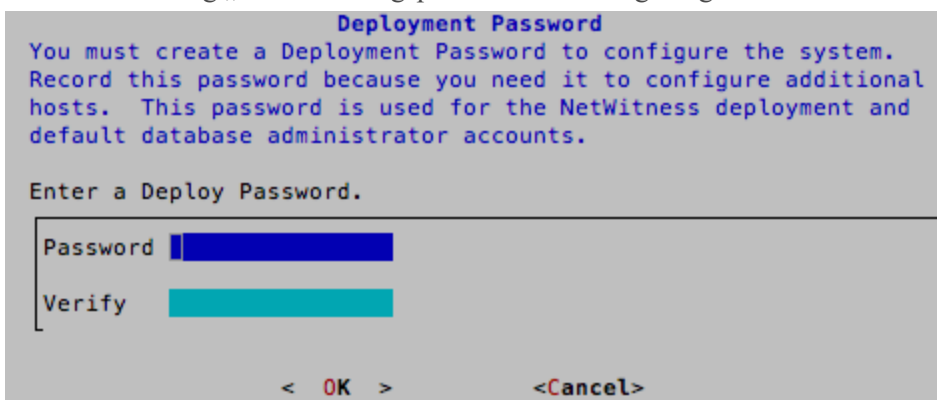
Für das Masterpasswort und Bereitstellungspasswort werden folgende Zeichen unterstützt:

- Symbole: ! @ # % ^ +
- Zahlen: 0-9
- Kleinbuchstaben: a-z
- Großbuchstaben: A-Z

Für das Masterpasswort und Bereitstellungspasswort werden keine nicht eindeutigen Zeichen unterstützt (z. B.: Leerzeichen { } [ ] ( ) / \ ' " ` ~ , ; : . < > -).

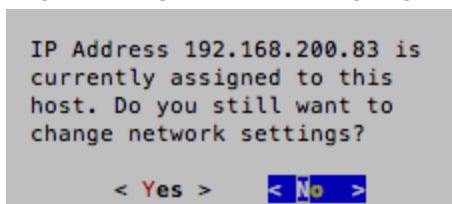


7. Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**. Die Aufforderung „Bereitstellungspasswort“ wird angezeigt.



8. Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**. Beachten Sie:

- Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt.



Drücken Sie die **EINGABETASTE**, wenn Sie diese IP verwenden und Ihre Netzwerkeinstellungen nicht ändern möchten. Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**, wenn Sie die auf dem Host gefundene IP-Konfiguration ändern möchten.

- Wenn Sie eine SSH-Verbindung verwenden, wird die folgende Warnung angezeigt.

```
NetWitness Suite Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection. Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.

< OK >
```

Drücken Sie die **EINGABETASTE**, um die Warnung zu schließen.

- Wenn das Setup-Programm eine IP-Konfiguration gefunden hat und Sie sie ausgewählt haben, wird die Aufforderung „Update-Repository“ angezeigt. Fahren Sie mit Schritt 12 fort und schließen Sie die Installation ab.
- Wenn das Setup-Programm keine IP-Konfiguration gefunden hat oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung „Netzwerkkonfiguration“ angezeigt.

```
NetWitness Suite Network Configuration
The IP address of the NW Server is used by all other NetWitness
Suite components. RSA recommends that you use a Static IP
Configuration for the NW Server IP address over DHCP. After the
IP address is assigned, record it for future use. You need this
address to set up other components.

Select an IP address configuration for the NW Server.

1 Static IP Configuration
2 Use DHCP

< OK >      < Exit >
```

9. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um **Statische IP-Adresse** zu verwenden.

Wenn Sie **DHCP** verwenden möchten, gehen Sie mit dem Pfeil nach unten zu „2 DHCP verwenden“ und drücken Sie **EINGABETASTE**.

Die Eingabeaufforderung „Netzwerkkonfiguration“ wird angezeigt.

```
NetWitness Suite Network Configuration
Please select the network interface to
configure:

1 eth0 (up)

< OK >      < Exit >
```

10. Gehen Sie mit dem Pfeil nach unten zur gewünschten Netzwerkschnittstelle. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**. Wenn Sie nicht fortfahren möchten, gehen Sie zu **Beenden**.

Die Eingabeaufforderung „Konfiguration der statischen IP-Adresse“ wird angezeigt.

```

NetWitness Suite Network Configuration
Static IP configuration

IP Address      [ ]
Subnet Mask     [ ]
Default Gateway [ ]
Primary DNS Server [ ]
Secondary DNS Server [ ]
Local Domain Name [ ]

< OK >      < Exit >

```

11. Geben Sie die Konfigurationswerte (mit dem Pfeil nach unten von Feld zu Feld gehend) ein. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung **Alle Felder sind Pflichtfelder** angezeigt (die Felder **Primärer DNS-Server**, **Sekundärer DNS-Server** und **Lokaler Domainname** sind nicht erforderlich).

Bei Verwendung der falschen Syntax oder Zeichenlänge für eines der Felder wird die Fehlermeldung **Ungültiger Feldname** angezeigt.

**Achtung:** Wenn Sie den DNS-Server auswählen, stellen Sie sicher, dass der DNS-Server korrekt ist und der Host darauf zugreifen kann, bevor Sie mit der Installation fortfahren.

Die Eingabeaufforderung „Update-Repository“ wird angezeigt.

```

NetWitness Suite Update Repository
The NetWitness Suite Update Repository contains all the RPMs
needed to build and maintain all the NetWitness Suite components.
All components managed by the NW Server need access to the
Repository.

Do you want to set up the NetWitness Suite Update Repository on:

1 The Local Repo (on the NW Server)
2 An External Repo (on an externally-managed server)

< OK >      < Exit >

```

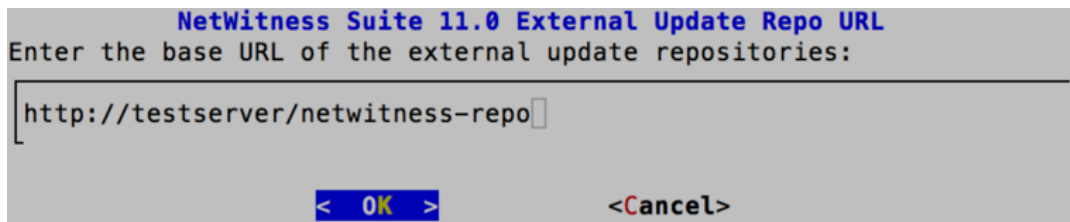
12. Drücken Sie die **EINGABETASTE**, um das **lokale Repository** auf dem NW-Server auszuwählen.

Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **Externes Repository** und dann zu **OK** und drücken Sie die EINGABETASTE.

- Bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** prüft das Setup-Programm, ob Sie die richtigen Medien mit dem Host verbunden haben (d. h. einen Build-Stick oder eine DVD), von dem/der es die Installation oder Aktualisierung der Hosts auf NetWitness Suite 11.0 abrufen kann. Wenn das Programm die verbundenen Medien nicht finden kann, wird die folgende Aufforderung angezeigt:



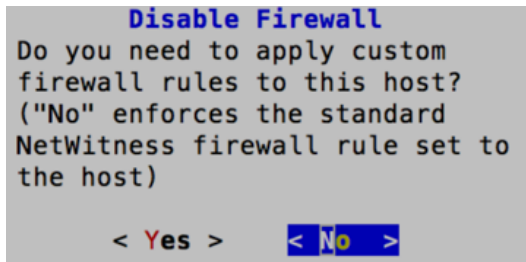
- Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe eines URL aufgefordert. Die Repositories bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates.



Geben Sie den Basis-URL für das externe NetWitness Suite-Repository ein und klicken Sie auf **OK**. Die Aufforderung „Installation starten“ wird angezeigt.

Anweisungen hierzu finden Sie unter „Einrichten eines externen Repository mit RSA und Betriebssystemupdates“ unter „Hosts und Services – Verfahren“ in der *RSA NetWitness Suite 11.0 – Leitfaden für die ersten Schritte mit Hosts und Services*. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

Die Aufforderung „Firewall deaktivieren“ wird angezeigt.





13. Gehen Sie wie folgt vor:

- Um die Standardkonfiguration für Firewalls anzuwenden, drücken Sie die **EINGABETASTE**.
- Um die Standardkonfiguration zu deaktivieren, gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**.

Die Aufforderung zur Bestätigung der Deaktivierung der Firewallkonfiguration wird angezeigt.

```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.

< Yes > < No >
```

Gehen Sie zu **Ja** und drücken Sie zur Bestätigung die **EINGABETASTE** (drücken Sie die **EINGABETASTE**, um die Standardkonfiguration für Firewalls zu verwenden).

Die Aufforderung „Installation starten“ wird angezeigt.

```
Start Install/Upgrade
All the required information has been gathered.

Select "1 Install Now" to start the installation
on this host.

1 Install Now
2 Restart

< OK > < Exit >
```

14. Drücken Sie die **EINGABETASTE**, um 11.0 auf dem NW-Server zu installieren.

Wenn „Installation abgeschlossen“ angezeigt wird, haben Sie 11.0 NW-Server auf diesem Host installiert.

**Hinweis:** Ignorieren Sie die Hashcodefehler ähnlich wie die Fehler in der folgenden Abbildung, die angezeigt werden, wenn Sie den Befehl `nwsetup-tui` initiieren. Yum verwendet kein MD5 für Sicherheitsabläufe, sodass sie sich nicht auf die Sicherheit des Systems auswirken.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove CentOS-CR repository] action delete
* execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

## Aufgabe 2: Installieren von 11.0 auf den Hosts anderer Komponenten

Für einen Nicht-NW-Server-Host führt diese Aufgabe folgende Vorgänge durch:

- Erstellen eines Basis-Image
- Einrichten des 11.0 Nicht-NW-Server-Hosts

Für ESA-Hosts:

- Installieren Sie Ihren primären ESA-Host und den Service **ESA Primary**, nachdem Sie das Setup-Programm auf der Benutzeroberfläche der Ansicht **ADMIN-Hosts** abgeschlossen haben.
- (Bedingungsabhängig) Wenn Sie über einen sekundären ESA-Host verfügen, installieren Sie diesen und installieren Sie den Service **ESA Secondary**, nachdem Sie das Setup-Programm auf der Benutzeroberfläche in der Ansicht **ADMIN-Hosts** abgeschlossen haben.

Führen Sie die folgenden Schritte aus, um NetWitness Suite 11.0 auf einem Nicht-NW-Server-Host zu installieren.

1. Erstellen Sie ein Basis-Image auf dem Host.

a. Verbinden Sie die Medien (d. h. Build-Stick oder DVD-ISO) mit dem Host.

Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Suite 11.0 Build-Stick*.

- Hypervisor-Installation: Verwenden Sie die DVD- oder USB-ISO-Images.
- Physische Medien: Verwenden Sie die DVD-ISO, um eine startfähige optische Festplatte mit vom Benutzer bereitgestellter Imaging-Software zu erstellen, oder die USB-ISO, um startfähige Medien für Flash-Laufwerke mithilfe von Universal Netboot Installer (UNetbootin) oder einem anderen geeigneten Imaging-Tool zu erstellen. In den *Anweisungen zum RSA NetWitness® Suite Build-Stick* finden Sie Informationen zum Erstellen eines Build-Sticks von der USB-ISO. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.
- iDRAC-Installationen – der Typ der virtuellen Medien lautet:
  - **Virtuelles Diskettenlaufwerk** für zugeordnete Flash-Laufwerke
  - **Virtuelle CD** für zugeordnete optische Mediengeräte oder ISO-Dateien

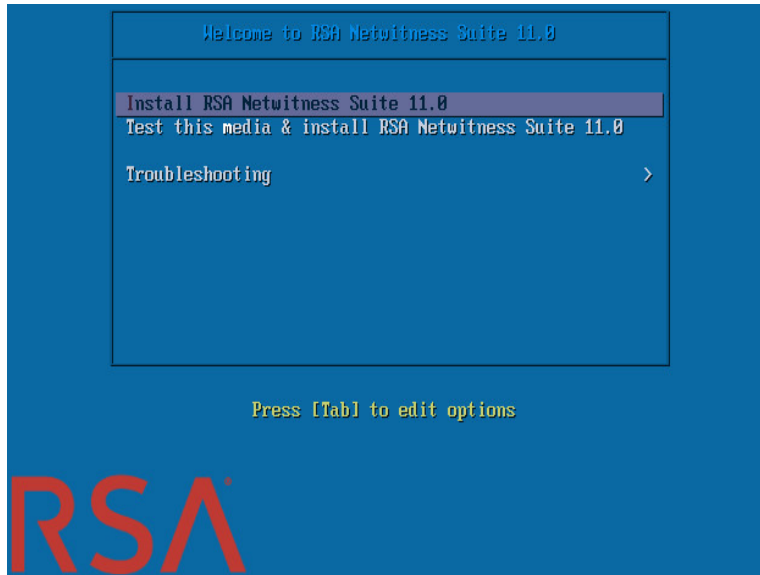
Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Suite 11.0 Build-Stick*.

- b. Melden Sie sich beim Host an und starten Sie ihn neu.

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

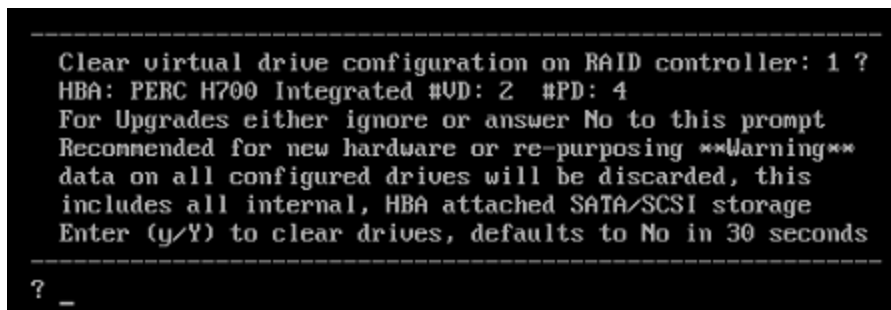
- c. Wählen Sie während des Neustarts **F11** (Startmenü) aus, um ein Startgerät auszuwählen und von den verbundenen Medien zu starten.

Nach einigen Systemprüfungen während des Startvorgangs wird das folgende Installationsmenü angezeigt: **Willkommen bei RSA NetWitness Suite 11.0**. Die Grafiken im Menü werden anders dargestellt, wenn Sie ein physisches USB-Flash-Medium verwenden.



- d. Wählen Sie **RSA NetWitness-Suite 11.0 installieren** (Standardauswahl) aus und drücken Sie die **EINGABETASTE**.

Das Installationsprogramm wird ausgeführt. Es wird bei der Eingabeaufforderung **j/J eingeben, um Laufwerke zu löschen** angehalten, in der Sie aufgefordert werden, die Laufwerke zu formatieren.



- e. Geben Sie **J** ein, um fortzufahren.

Die Standardaktion ist „Nein“. Wenn Sie also die Aufforderung ignorieren, wird innerhalb von 30 Sekunden „Nein“ ausgewählt und die Laufwerke werden nicht gelöscht.

Die Eingabeaufforderung **Für Neustart Eingabetaste drücken** wird angezeigt.

```

Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
Re-labeling disks and virtual drives, clearing RAID configuration ...
0 logical volume(s) in volume group "netwitness_vg00" now active

Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level = #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot

```

- f. Drücken Sie die **EINGABETASTE**, um den Host neu zu starten.

Das Installationsprogramm fordert Sie erneut auf, die Laufwerke zu löschen.

```

-----
Clear virtual drive configuration on RAID controller: 0 ?
HBA: PERC H730P Mini #VD: 2 #PD: 4
For Migrations either ignore or answer No to this prompt
Recommended for new hardware or re-purposing **Warning**
data on all configured drives will be discarded, this
includes all internal, HBA attached SATA/SCSI storage
Enter (y/Y) to clear drives, defaults to No in 30 seconds
-----

```

- g. Geben Sie **N** ein, da Sie die Laufwerke bereits gelöscht haben.

Die Eingabeaufforderung **Q zum Beenden oder R für Neuinstallation eingeben**) wird

angezeigt.

```
-----
No root level logical volumes found for Migration
Assuming this system is new or being reinstalled
Migration cannot proceed, system will be reimaged
If you had intended to migrate please quit and
contact support for assistance.
-----
Enter Q to Quit or R to Reinstall, Re-installing in 120 seconds?
```

- h. Geben Sie **R** ein, um das Basis-Image zu installieren.

Das Installationsprogramm zeigt die Komponenten an, während sie installiert werden. Dies variiert je nach Appliance. Das Programm wird neu gestartet.

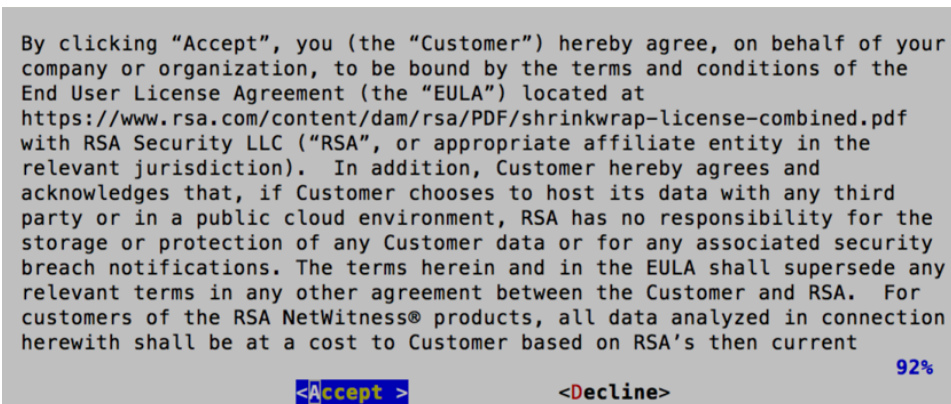
**Achtung:** Starten Sie die angeschlossenen Medien (d. h. den Build-Stick oder die DVD-ISO) nicht neu.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#
```

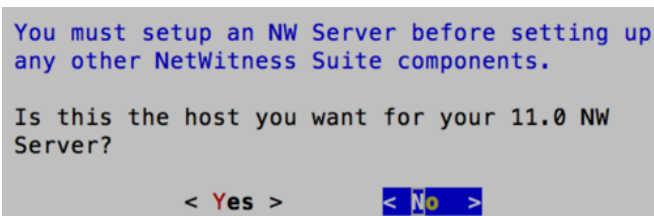
- i. Melden Sie sich mit den Root-Anmeldedaten beim Host an.
2. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten. Dadurch wird das Setup-Programm gestartet und die EULA wird angezeigt.

**Hinweis:** Wenn Sie während des Setup-Programms (`nwsetup-tui`) die DNS-Server angeben, MÜSSEN diese gültig („gültig“ in diesem Zusammenhang bedeutet gültig während des Setups) und für `nwsetup-tui` zugänglich sein, damit Sie fortfahren können. Falsch konfigurierte DNS-Server führen dazu, dass die Konfiguration fehlschlägt. Wenn Sie den DNS-Server beim Setup erreichen müssen, dieser aber während des Setups nicht erreichbar ist (z. B. um einen Host nach dem Setup zu verlagern, der über andere DNS-Server verfügt) lesen Sie [Erneutes Konfigurieren von DNS-Servern nach 11.0](#). Wenn Sie keinen DNS-Server während `nwsetup-tui` angeben, müssen Sie **1 Lokales Repository (auf dem NW-Server)** in der Eingabeaufforderung **NetWitness Suite Update-Repository** in Schritt 11 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repo zugreifen kann).



3. Gehen Sie zu **Akzeptieren** und drücken Sie die **EINGABETASTE**.

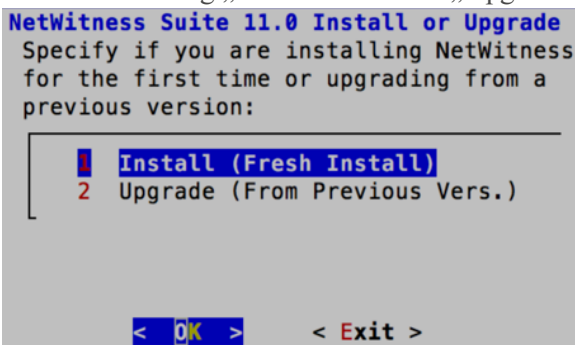
Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.



**Achtung:** Wenn Sie den falschen Host für den NW-Server auswählen und die Installation abschließen, müssen Sie das Setup-Programm neu starten und alle Schritte unter [Aufgabe 1 – Installieren von 11.0 auf dem NetWitness-Server-Host](#) (Schritt 2 bis 14) ausführen, um diesen Fehler zu korrigieren.

4. Drücken Sie die **EINGABETASTE** (Nein).

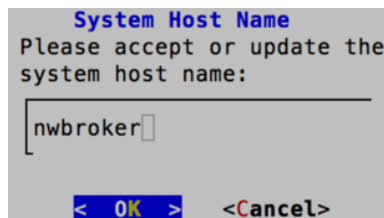
Die Aufforderung „Installation“ oder „Upgrade“ wird angezeigt.





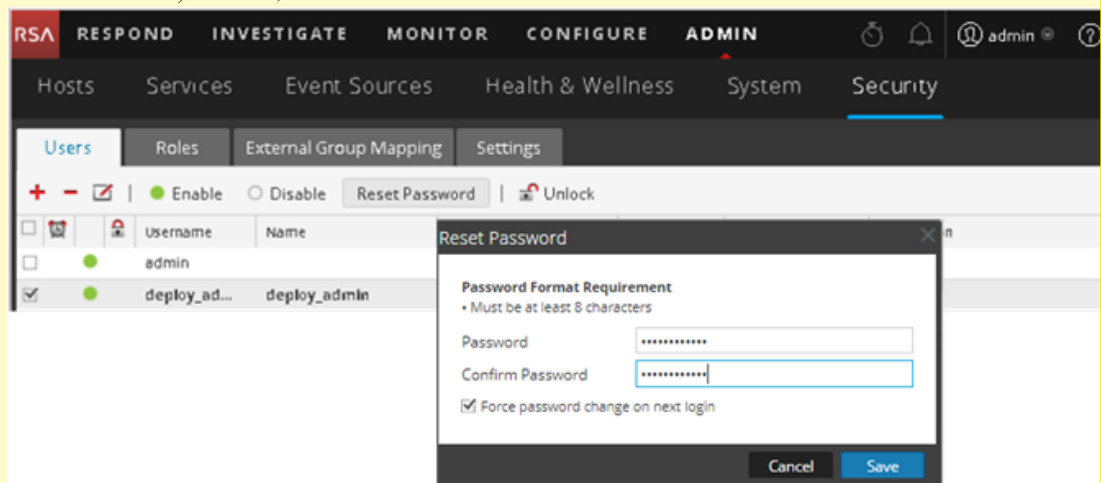
5. Drücken Sie die **EINGABETASTE** (standardmäßig ist „Installation“ ausgewählt).

Die Aufforderung „Hostname“ wird angezeigt.



6. Drücken Sie die **EINGABETASTE**, wenn dieser Name beibehalten werden soll. Wenn Sie diesen Namen ändern möchten, bearbeiten Sie ihn, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

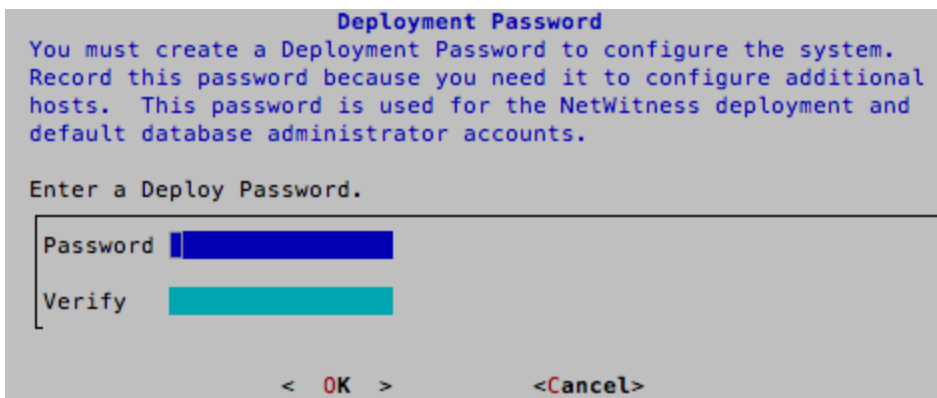
**Achtung:** Wenn Sie das Benutzerpasswort **deploy\_admin** auf der NetWitness Suite-Benutzeroberfläche (**ADMIN > Sicherheit > deploy\_admin** auswählen – **Passwort zurücksetzen**) ändern,



müssen Sie Folgendes tun:

1. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
2. Führen Sie das Skript `/opt/rsa/saTools/bin/set-deploy-admin-password` aus.
3. Verwenden Sie das neue Passwort, wenn Sie neue Nicht-NW-Serverhosts installieren.
4. Führen Sie das `/opt/rsa/saTools/bin/set-deploy-admin-password`-Skript auf allen Nicht-NW-Serverhosts in Ihrer Bereitstellung aus.
5. Notieren Sie sich das Passwort, da Sie es möglicherweise zu einem späteren Zeitpunkt bei der Installation benötigen.

Die Aufforderung „Bereitstellungspasswort“ wird angezeigt.

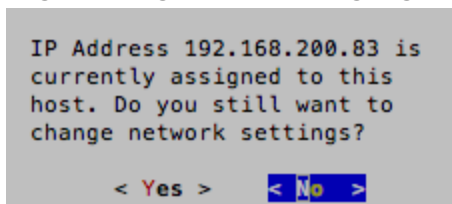


**Hinweis:** Sie müssen das gleiche Bereitstellungspasswort verwenden, das Sie bei der Installation des NW-Servers verwendet haben.

7. Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**.

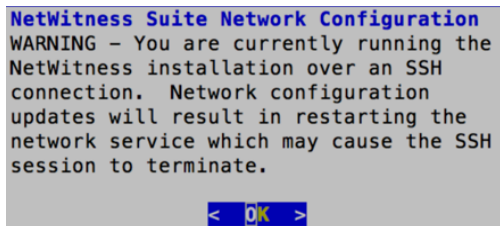
Beachten Sie:

- Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt.



Drücken Sie die **EINGABETASTE**, wenn Sie diese IP verwenden und Ihre Netzwerkeinstellungen nicht ändern möchten. Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**, wenn Sie die auf dem Host gefundene IP-Konfiguration ändern möchten.

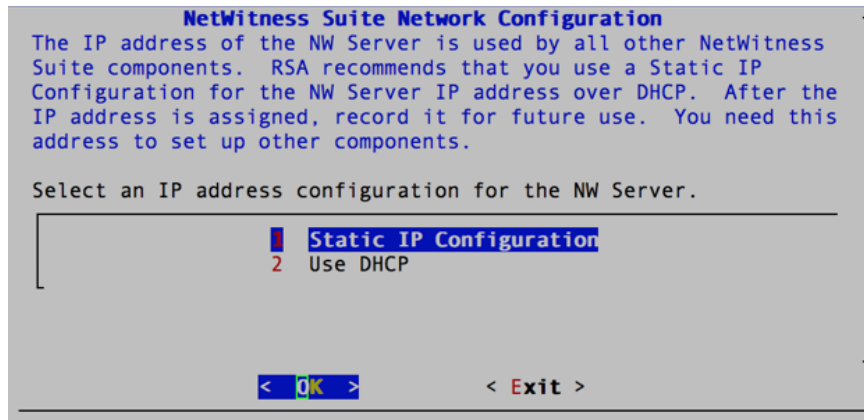
- Wenn Sie eine SSH-Verbindung verwenden, wird die folgende Warnung angezeigt.



Drücken Sie die **EINGABETASTE**, um die Warnung zu schließen.

- Wenn das Setup-Programm eine IP-Konfiguration gefunden hat und Sie sie ausgewählt haben, wird die Aufforderung „Update-Repository“ angezeigt. Fahren Sie mit Schritt 11 fort und schließen Sie die Installation ab.

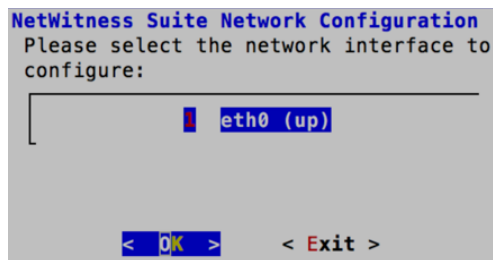
- Wenn das Setup-Programm keine IP-Konfiguration gefunden hat oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung „Netzwerkconfiguration“ angezeigt.



8. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um eine **statische IP-Adresse** zu verwenden.

Wenn Sie **DHCP** verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **2 DHCP verwenden** und drücken Sie die **EINGABETASTE**.

Die Eingabeaufforderung „Netzwerkconfiguration“ wird angezeigt.



9. Gehen Sie mit dem Pfeil nach unten zur gewünschten Netzwerkschnittstelle. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**. Wenn Sie fortfahren möchten, gehen Sie zu **Beenden**.

Die Eingabeaufforderung „Konfiguration der statischen IP-Adresse“ wird angezeigt.

10. Geben Sie die Konfigurationswerte (mit dem Pfeil nach unten von Feld zu Feld gehend) ein. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung **Alle Felder sind Pflichtfelder** angezeigt (die Felder **Primärer DNS-Server**, **Sekundärer DNS-Server** und **Lokaler Domainname** sind nicht erforderlich).

Bei Verwendung der falschen Syntax oder Zeichenlänge für eines der Felder wird die Fehlermeldung **Ungültiger Feldname** angezeigt.

**Achtung:** Wenn Sie den DNS-Server auswählen, stellen Sie sicher, dass der DNS-Server korrekt ist und der Host darauf zugreifen kann, bevor Sie mit der Installation fortfahren.

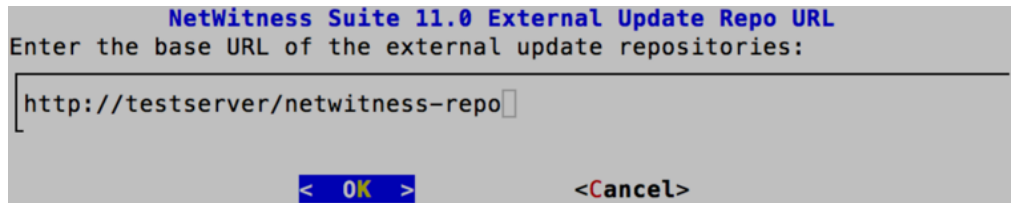
Die Eingabeaufforderung „Update-Repository“ wird angezeigt.

Wählen Sie für alle Hosts das gleiche Repository aus, das Sie bei Installation des NW-Serverhosts ausgewählt haben.

11. Drücken Sie die **EINGABETASTE**, um das **lokale Repository** auf dem NW-Server auszuwählen.

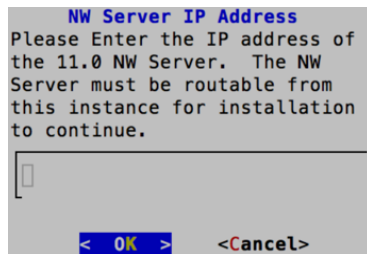
Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **Externes Repository** und dann zu **OK** und drücken Sie die **EINGABETASTE**.

- Bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** prüft das Setup-Programm, ob Sie die richtigen Medien mit dem Host verbunden haben (d. h. einen Build-Stick oder eine DVD), von dem/der es die Installation oder Aktualisierung der Hosts auf NetWitness Suite 11.0 abrufen kann.
- Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe eines URL aufgefordert. Die Repositories bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates.



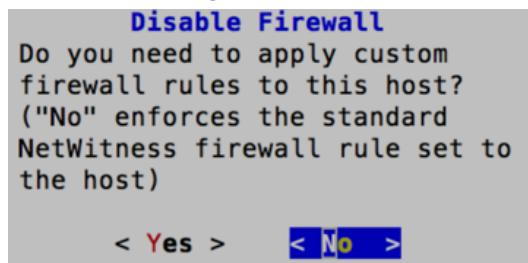
Geben Sie den Basis-URL des externen NetWitness Suite-Repository an, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

Die Aufforderung zur Eingabe der IP-Adresse des NW-Servers wird angezeigt.



12. Geben Sie die IP-Adresse des NW-Servers ein. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

Die Aufforderung „Firewall deaktivieren“ wird angezeigt.



13. Gehen Sie wie folgt vor:

- Um die Standardkonfiguration für Firewalls anzuwenden, drücken Sie die **EINGABETASTE**.
- Um die Standardkonfiguration zu deaktivieren, gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**.

Die Aufforderung zur Bestätigung der Deaktivierung der Firewallkonfiguration wird angezeigt.

```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.

      < Yes >          < No >
```

Gehen Sie zu **Ja** und drücken Sie zur Bestätigung die **EINGABETASTE** (drücken Sie die **EINGABETASTE**, um die Standardkonfiguration für Firewalls zu verwenden).

Die Aufforderung „Installation starten“ wird angezeigt.

```
Start Install/Upgrade
All the required information has been gathered.

Select "1 Install Now" to start the installation
on this host.

      1 Install Now
      2 Restart

      < b/k >          < Exit >
```

14. Drücken Sie die **EINGABETASTE**, um 11.0 auf dem NW-Server zu installieren.

Wenn „Installation abgeschlossen“ angezeigt wird, verfügen Sie über einen generischen Nicht-NW-Serverhost mit einem Betriebssystem, das mit NetWitness Suite 11.0 kompatibel ist.

15. Installieren Sie einen Komponentendienst auf dem Host.



a. Melden Sie sich bei NetWitness Suite an.

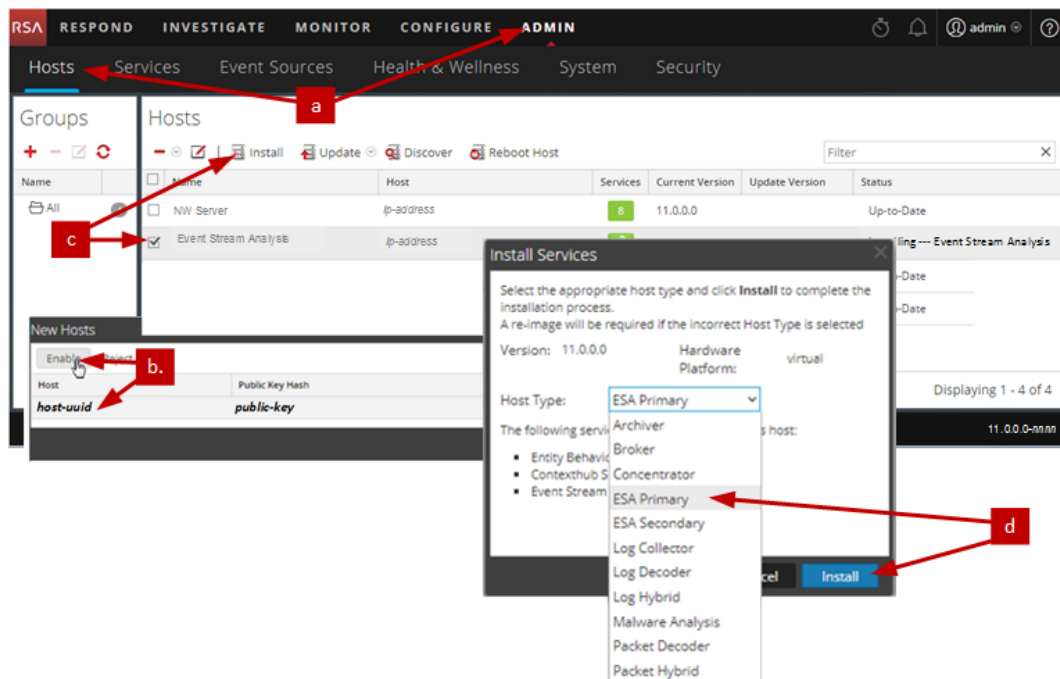
Geben Sie `https://<NW-Server-IP-Address>/login` in Ihrem Browser ein, um zum NetWitness Suite-Anmeldebildschirm zu gelangen.

b. Klicken Sie auf **ADMIN > Hosts**.

Das Dialogfeld „Neue Hosts“ wird angezeigt; die Ansicht „Hosts“ ist im Hintergrund abgeblendet.

**Hinweis:** Wenn das Dialogfeld **Neue Hosts** nicht angezeigt wird, klicken Sie in der Symbolleiste der Ansicht „Hosts“ auf **Erkennen**.

- c. Wählen Sie einen Nicht-NW-Serverhost aus der Ansicht **Hosts** aus.
- d. Klicken Sie im Dialogfeld **Neue Hosts** auf den Host und klicken Sie dann auf **Aktivieren**.  
Das Dialogfeld **Neue Hosts** wird geschlossen und der Host wird in der Ansicht **Hosts** angezeigt.
- e. Wählen Sie diesen Host (z. B. **Event Stream Analysis**) aus und klicken Sie auf  **Install** .
- f. Wählen Sie den entsprechenden Service (z. B. **ESA Primary**) aus und klicken Sie auf **Installieren**.



Sie haben die Installation des Nicht-NW-Serverhosts in NetWitness Suite abgeschlossen.

16. Führen Sie für den Rest der Nicht-NW-Serverkomponenten von NetWitness Suite die Schritte 1 bis 15 aus.





## Aktualisieren oder Installieren der Legacy Windows Collection

---

Detaillierte Anweisungen zur Installation oder zum Update der Legacy Windows Collection finden Sie im *Leitfaden RSA NetWitness 11.0 Legacy Windows Collection* auf RSA Link (<https://community.rsa.com/docs/DOC-75593>).

**Hinweis:** Starten Sie nach dem Aktualisieren oder Installieren der Legacy Windows Collection das System neu, um sicherzustellen, dass Log Collection korrekt funktioniert.

## Aufgaben nach der Installation

---

Dieses Thema enthält die Aufgaben, die Sie nach der Installation von 11.0 ausführen.

- [Aufgabe 1: Beheben von Fehler bei Authentifizierung in 11.0](#)
- (Optional) [Aufgabe 2: Erneutes Konfigurieren von DNS-Servern nach 11.0.0.0](#)
- (Bedingungsabhängig) [Aufgabe 3: Für Warehouse Connector mit Log Collector-Service – Bearbeiten der Datei `sshd\_config`](#)

### Aufgabe 1. Beheben von Fehler bei Authentifizierung in 11.0

Benutzer können sich nicht an der NetWitness Suite-Benutzeroberfläche anmelden, nachdem Sie ein Upgrade auf 11.0 durchgeführt haben, da die Benutzeroberfläche Benutzerkontoinformationen von MongoDB nicht abrufen kann.

- Wenden Sie sofort nach der Aktualisierung auf 11.0 den Patch 11.0.0.1 an, um dieses Problem zu beheben.

### (Optional) Aufgabe 2: Erneutes Konfigurieren von DNS-Servern nach 11.0.0.0

Führen Sie folgende Schritte aus, um die DNS-Server in NW 11.0 neu zu konfigurieren:

1. Melden Sie sich beim Serverhost mit Ihren `root` -Anmeldedaten an.
2. Bearbeiten Sie die Datei `/etc/resolv.conf`:
  - a. Ersetzen die IP-Adresse entsprechend dem `nameserver`.  
Wenn Sie beide DNS-Server ersetzen müssen, ersetzen Sie die IP-Einträge für die beiden Hosts durch gültige Adressen.  
Im folgenden Beispiel werden die beiden DNS-Einträge als geändert dargestellt.

```

root@nw11sas5:~
# Generated by NetworkManager
nameserver nn.nn.55.15
nameserver nn.nn.55.17
search netwitness.local
~

```

Das folgende Beispiel zeigt die neuen DNS-Werte.

```

root@nw11sas5:~
# Generated by NetworkManager
nameserver nn.nn.44.37
nameserver nn.nn.66.17
search netwitness.local
~

```

- b. Speichern Sie die Datei `/etc/resolv.conf`.

### **(Bedingungsabhängig) Aufgabe 3: Für Warehouse Connector mit Log Collector-Service – Bearbeiten der Datei `sshd_config`**

Wenn Sie einen Warehouse Connector-Service mit einem Log Collector installiert haben, führen Sie die folgenden Schritte aus, um sicherzustellen, dass beide Services ordnungsgemäß funktionieren:

1. Kommentieren Sie in der Datei `/etc/ssh/sshd_config` die folgende Zeile:  
`#Subsystem sftp /usr/libexec/openssh/sftp-server`
2. Fügen Sie die folgenden Abschnitte zur Datei hinzu:

```

# SFTP server settings added for NwLogCollector
StrictModes no

Subsystem sftp internal-sftp

Match User sftp
    AllowTCPForwarding no
    PasswordAuthentication no
    X11Forwarding no
    ForceCommand internal-sftp

```

```
ChrootDirectory /var/lib/logcollector
```

```
Match Group uploads
```

```
ChrootDirectory /var/lib/logcollector/upload_  
chroot  
X11Forwarding no  
AllowTcpForwarding no  
PasswordAuthentication no
```

### 3. Stellen Sie sicher, dass die Inhalte der Datei `sshd` dem folgenden Beispiel ähneln:

```
# Accept locale-related environment variables  
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY  
LC_MESSAGES  
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT  
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE  
AcceptEnv XMODIFIERS  
  
# override default of no subsystems  
#Subsystem sftp /usr/libexec/openssh/sftp-server  
  
# Example of overriding settings on a per-user basis  
#Match User anoncvs  
#    X11Forwarding no  
#    AllowTcpForwarding no  
#    PermitTTY no  
#    ForceCommand cvs server  
  
#disabled CBC mode cipher encryption and MD5 or 96-bit MAC  
algorithms  
Ciphers aes128-ctr,aes192-ctr,aes256-ctr  
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512  
  
# SFTP server settings added for NwLogCollector  
StrictModes no  
  
Subsystem sftp internal-sftp  
  
Match User sftp  
    AllowTCPForwarding no  
    PasswordAuthentication no  
    X11Forwarding no  
    ForceCommand internal-sftp  
    ChrootDirectory /var/lib/logcollector  
  
Match Group uploads  
    ChrootDirectory /var/lib/logcollector/upload_chroot  
    X11Forwarding no  
    AllowTcpForwarding no  
    PasswordAuthentication no
```

4. Speichern Sie die Datei und starten Sie den sshd-Service erneut mit dem folgenden Befehl:  
`systemctl restart sshd`

## Revisionsverlauf

---

Version	Datum	Beschreibung	Verfasser
1,0	16-Okt-17	Betriebsfreigabe	IDD
1.1	25-Okt-17	Aufgabe nach der Installation zur Behebung des Fehlers bei der Authentifizierung in 11.0	IDD