RSA NETWITNESS® PLATFORM

Handbuch zur Installation physischer Hosts

für Version 11.2

Kontaktinformationen

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

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

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

Dell 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 2019

Inhalt

Einführung

Die Anweisungen in diesem Handbuch gelten nur für physische Hosts. Anweisungen zum Einrichten von virtuellen Hosts in 11.2 finden Sie im RSA *NetWitness PlatformHandbuch zur Installation virtueller Hosts*.

Unterstützte Hardware

Serie 4, Serie 4S und Serie 5.

Ausführliche Informationen zu jedem Serientyp finden Sie in den RSA *NetWitness Platform* Handbüchern zur Hardwarekonfiguration (https://community.rsa.com/community/products/netwitness/hardware-setup-guides).

Endpoint Hybrid- oder Endpoint Log Hybrid-Hardwarespezifikationen

Sie müssen den neuen Endpoint Hybrid Host oder Endpoint Log Hybrid Host auf der Hardware der Serie 5 (Dell R730) oder der Serie 6 (Dell R740) installieren. Anweisungen zum Installieren von Endpoint Hybrid und Endpoint Log Hybrid finden Sie unter „(Optional) Aufgabe 2: - Installieren von Endpoint Hybrid oder Endpoint Log Hybrid“ in den Aufgaben nach der Installation.

Hardwarespezifikation des RSA NetWitness UEBA-Hosts

Sie müssen den neuen NetWitness UEBA-Host auf der Hardware der Serie S5 (Dell R630-Appliance) installieren. Weitere Anleitungen zur Installation von NetWitness UEBA finden Sie unter „(Optional) Task 3 - Installieren von NetWitness UEBA“ in Aufgaben nach der Installation.

SPEZIFIKATIONEN DER SERIE 5 (DELL R630)

Spezifikation	Kapazität
Modell	Dell PowerEdge R630xl
Prozessortyp	Intel Xeon E5-2680v3
Prozessorgeschwindigkeit	2,5 GHz
Cache	30 MB
Anzahl Kerne	12
Anzahl der Prozessoren	2
Anzahl der Threads	24
Gesamtspeicher	256 GB
Interner Laufwerkcontroller	Dell PERC H730
Externer Laufwerkcontroller	Dell PERC H830
SAN-Konnektivität (HBA) – optional	–

Spezifikation	Kapazität
Remotemanagementkarte	iDRAC8 Enterprise
Laufwerke	Insgesamt 6 Laufwerke 2 x 2,5-Zoll-HDD mit 1 TB 4 x 2,5-Zoll-HDD mit 2 TB
Gehäuse	1 HE
Gewicht	18,4 kg
NIC-Karte*	On Board 2 x 10 Gb Kupfer 2 x 10 Gb und 2 x 1 Gb Kupfer (Weitere Optionen sind verfügbar)
Abmessungen	H: 4,28 cm B: 48,23 cm T: 75,51 cm
Stromversorgung	1.100 W redundant
BTU/h	4.100 BTU/h (max)
Amps (Spez.)	1.100 W/220 VAC = 5 A
Tatsächliche Stromaufnahme (nach dem Start)	2,1 Ampere
Ereignisse pro Sekunde	100.000 EPS
Durchsatz	–

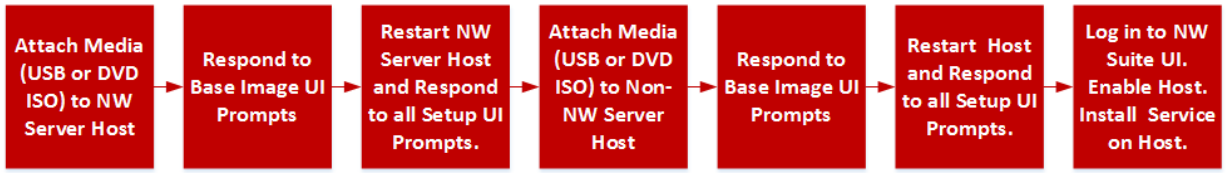
* Optionen für NIC-Karten können gegen eine Tochterkarte auf der Platine oder ein Add-on ausgetauscht werden.

Externer angeschlossener Speicher

Wenn Sie ein externes Speichergerät oder Geräte (z. B. DACs oder PowerVaults) an einen physischen Host angeschlossen haben, lesen Sie bitte die Handbücher zur Hardwarekonfiguration, um Informationen darüber zu erhalten, wie Sie diesen Speicher in RSA Link konfigurieren (https://community.rsa.com/community/products/netwitness/hardware-setup-guides).“

Workflow für die Installation physischer Hosts

Das folgende Diagramm veranschaulicht den Workflow für die Installation von RSA NetWitness® Platform 11.2 auf physischen Hosts.



Wenden Sie sich an den 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 Platform 11.2 erhalten.

Installationsvorbereitung – Öffnen von Firewallports

Im Thema „Netzwerkarchitektur und Ports“ im *RSA NetWitness® Platform Bereitstellungsleitfaden* werden alle Ports in einer Bereitstellung aufgeführt. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

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 Platform 11.2 auf physischen Hosts zu installieren.

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

Aufgabe 1: Installieren von 11.2 auf dem NetWitness-Serverhost

Aufgabe 2: Installieren von 11.2 auf den Hosts aller anderen Komponenten

Aufgabe 1: Installieren von 11.2 auf dem NetWitness-Serverhost

Für den NW-Server werden folgende Vorgänge ausgeführt:

- Erstellen eines Basis-Image
- Einrichten des 11.2 NW-Serverhosts

Führen Sie die folgenden Schritte aus, um den 11.2 NW-Serverhost zu installieren:

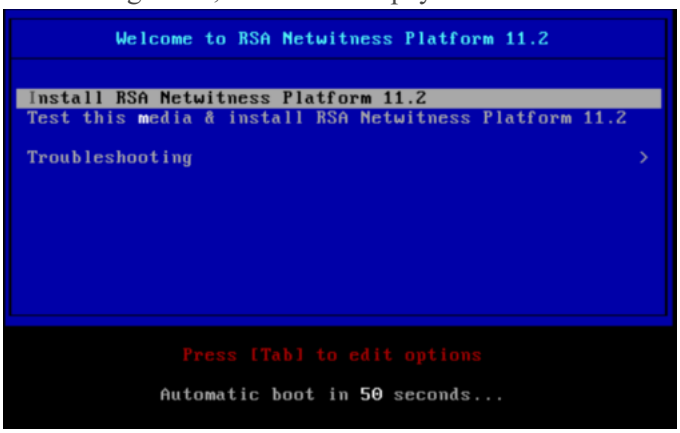
1. Erstellen Sie ein Basis-Image auf dem Host:
   a. Verbinden Sie die Medien (ISO) mit dem Host.
   Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Platform Build-Stick*.
      - Hypervisor-Installationen: Verwenden Sie das ISO-Image.
      - Physische Medien: Verwenden Sie die ISO-Datei, um startfähige Medien für Flash-Laufwerke mithilfe von Universal Netboot Installer (UNetbootin) oder einem anderen geeigneten Imaging-Tool zu erstellen. In den *RSA NetWitness® PlatformAnweisungen zum Build-Stick* finden Sie Informationen zum Erstellen eines Build-Sticks aus dem ISO-Image. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
      - iDRAC-Installationen – der Typ der virtuellen Medien lautet:
        - **Virtuelles Diskettenlaufwerk** für zugeordnete Flash-Laufwerke
        - **Virtuelle CD** für zugeordnete optische Mediengeräte oder ISO-Datei.

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

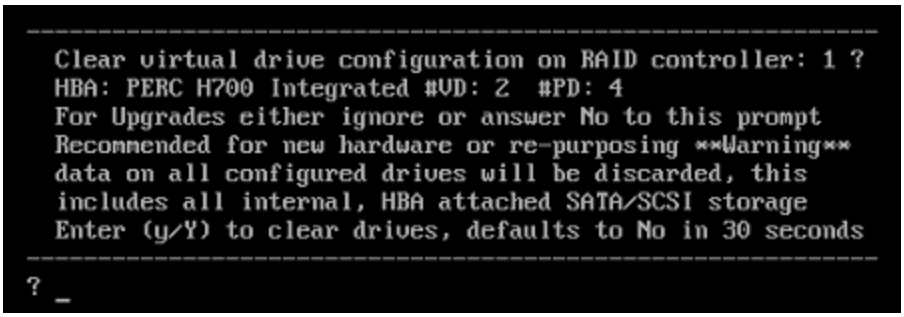
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

   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 Platform 11.2**. Die Grafiken im Menü werden

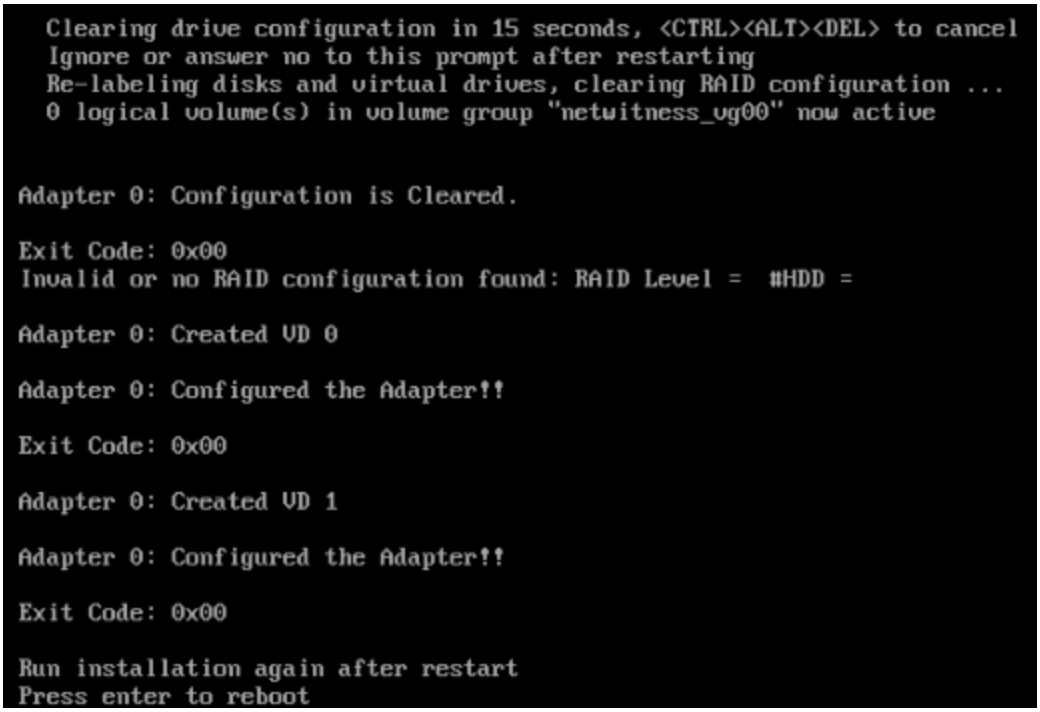
anders dargestellt, wenn Sie ein physisches USB-Flash-Medium verwenden.



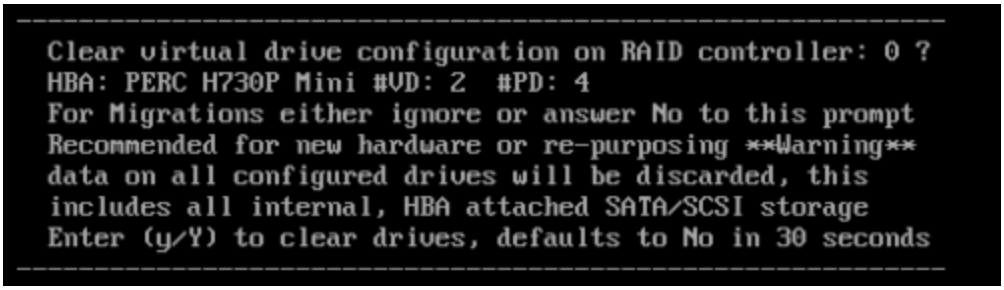
d. Wählen Sie **RSA NetWitness Platform 11.2 installieren** (Standardauswahl) aus und drücken Sie die Eingabetaste.
Das Installationsprogramm wird ausgeführt. Es wird bei der Eingabeaufforderung **j/J eingeben, um Laufwerke zu löschen** angehalten, in der Sie aufgefordert werden, die Laufwerke zu formatieren.



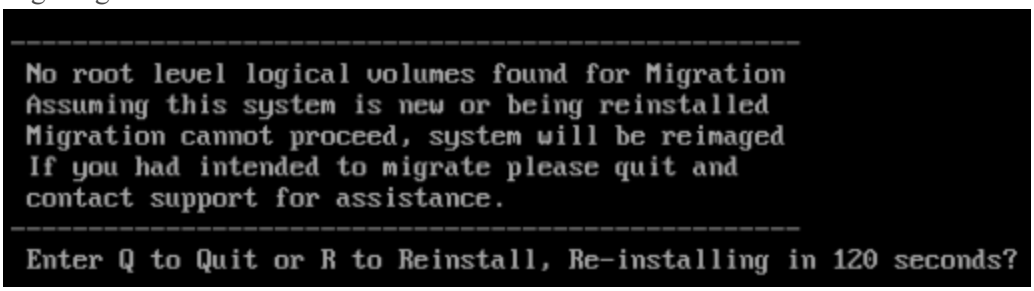
e. Geben Sie **J** ein, um fortzufahren.
Die Standardaktion ist „Nein“. Wenn Sie also die Aufforderung ignorieren, wird innerhalb von 30 Sekunden „Nein“ ausgewählt und die Laufwerke werden nicht gelöscht. Die Eingabeaufforderung **Für Neustart Eingabetaste drücken** wird angezeigt.



f. Drücken Sie die **Eingabetaste**, um den Host neu zu starten.
Das Installationsprogramm fordert Sie erneut auf, die Laufwerke zu löschen.



g. Geben Sie **N** ein, da Sie die Laufwerke bereits gelöscht haben.
Die Eingabeaufforderung **Q zum Beenden oder R für Neuinstallation eingeben)** wird angezeigt.



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.

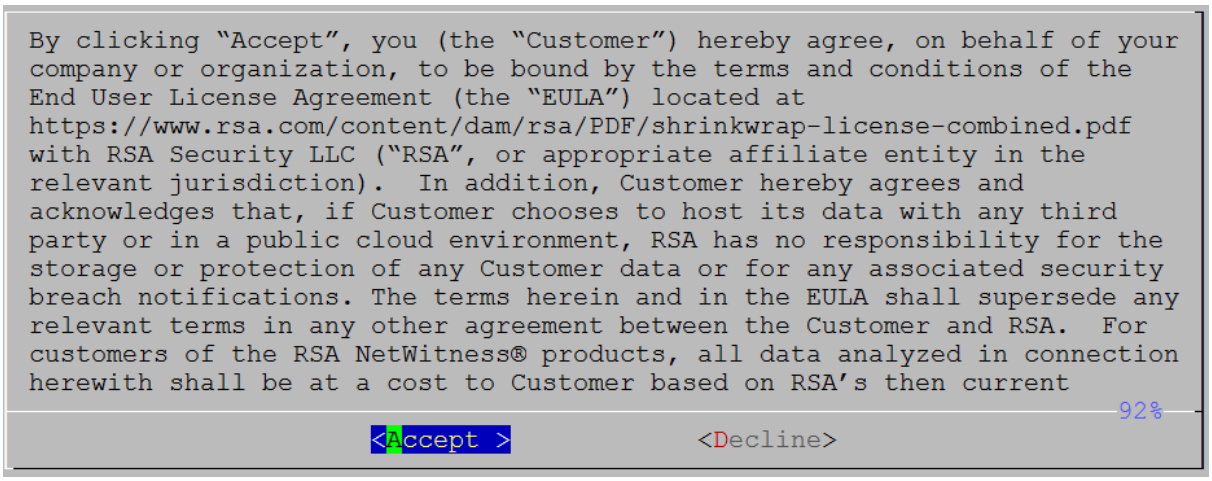
Achtung: Starten Sie die angeschlossenen Medien (Medien mit der ISO-Datei, z. B. ein Build-Stick) nicht neu.

i. Melden Sie sich mit den `root` -Anmeldedaten beim Host an.

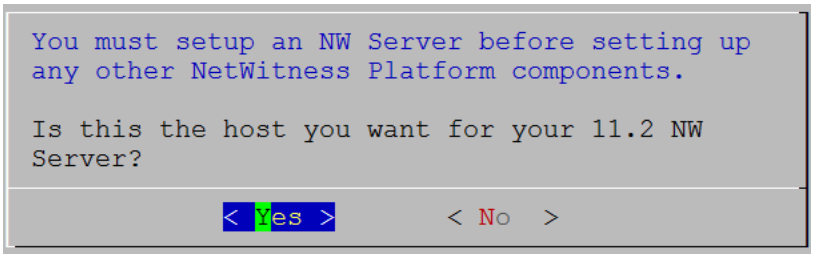
2. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.

   Dadurch wird das `nwsetup-tui` 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 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 „(Optional) Aufgabe 1: Erneutes Konfigurieren von DNS-Servern nach 11.2“ 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 Platform Update-Repository** in Schritt 12 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repository zugreifen kann).



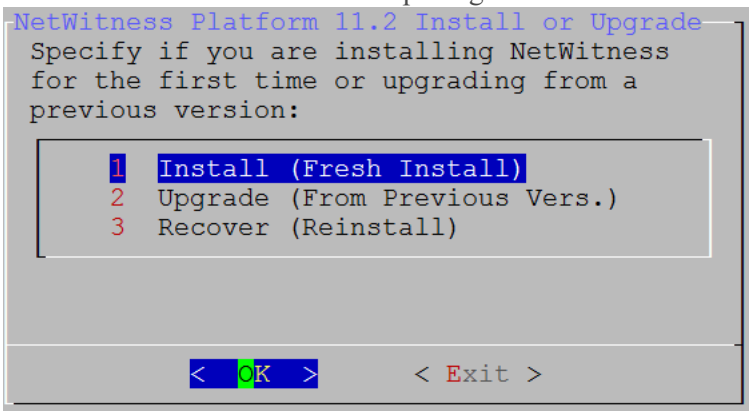
3. Navigieren Sie zu **Akzeptieren** und drücken Sie die **Eingabetaste**.
   Es wird eine Aufforderung mit der Frage angezeigt, ob dies der Host ist, den Sie für Ihren 11.2 NW-Server verwenden möchten.



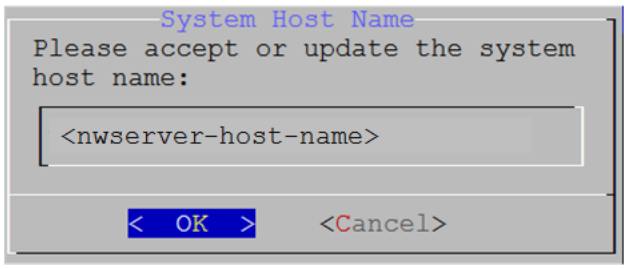
4. Navigieren Sie zu **Ja** und drücken Sie die **Eingabetaste**.
   Wählen Sie **Nein**, wenn Sie 11.2 bereits auf dem NW-Server installiert haben.

   Achtung: Wenn Sie den falschen Host für den NW-Server auswählen und das Setup abschließen, müssen Sie das Setup-Programm neu starten und die Schritte 2 bis 14 ausführen, um diesen Fehler zu korrigieren.

   Die Aufforderung für Installieren oder Upgrade durchführen wird angezeigt (**Wiederherstellen** gilt nicht für die Installation. Diese Option gilt für 11.2 Disaster Recovery.).



5. Drücken Sie die **Eingabetaste**. Die Option für Installieren (neue Installation) ist standardmäßig ausgewählt.
   Die Aufforderung **Hostname** wird angezeigt.



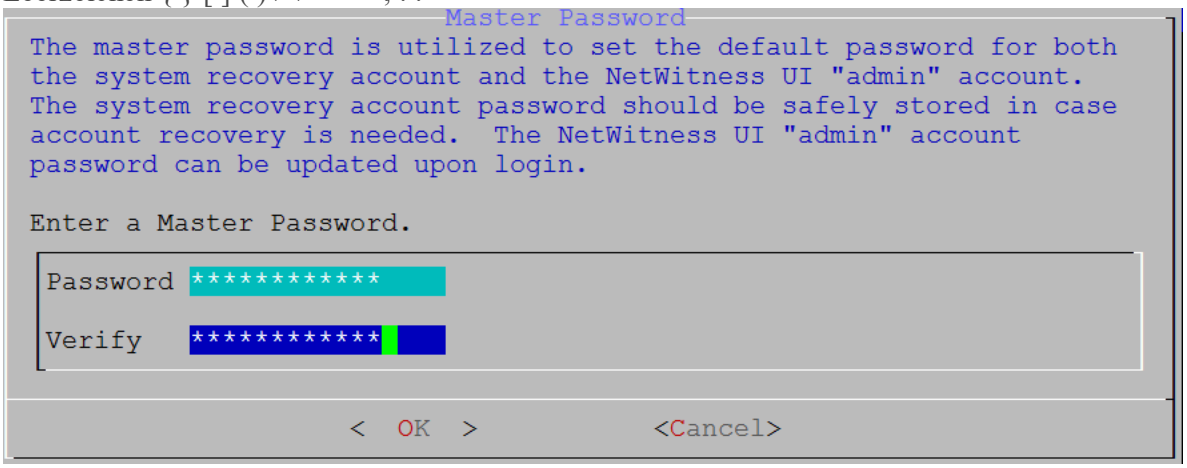
Achtung: Wenn Sie „.“ in einen Hostnamen einfügen, muss dieser auch einen gültigen Domainnamen enthalten.

Die Aufforderung **Masterpasswort** wird angezeigt.

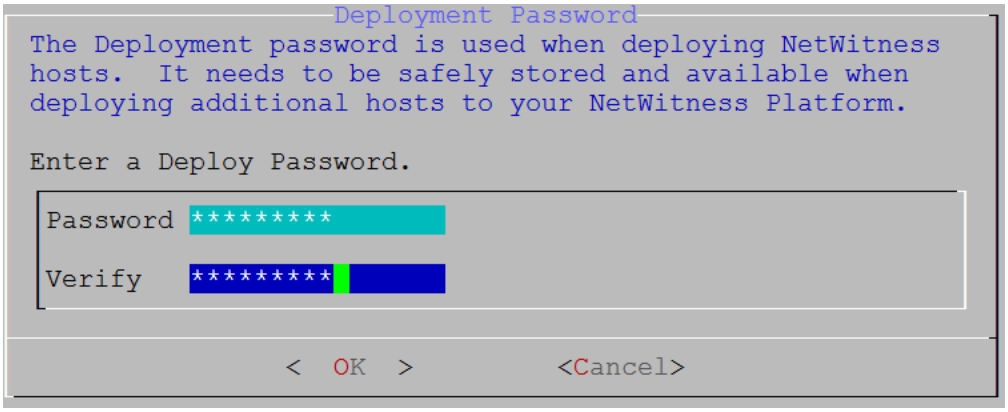
6. Drücken Sie die Eingabetaste, wenn dieser Name beibehalten werden soll. Wenn Sie den Hostnamen bearbeiten möchten, gehen Sie zu **OK** und drücken Sie die **Eingabetaste**, um ihn zu ändern.
   Für das Masterpasswort und das Bereitstellungspasswort werden folgende Zeichen unterstützt:

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

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

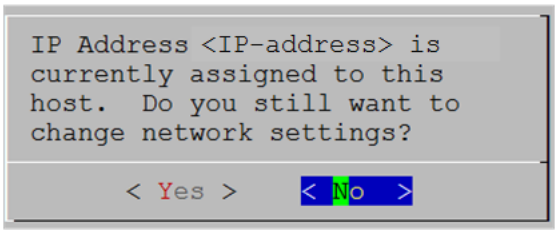


7. Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **Eingabetaste**.
   Die Aufforderung **Bereitstellungspasswort** wird angezeigt.



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**.
   Eine der folgenden bedingten Eingabeaufforderungen wird angezeigt.

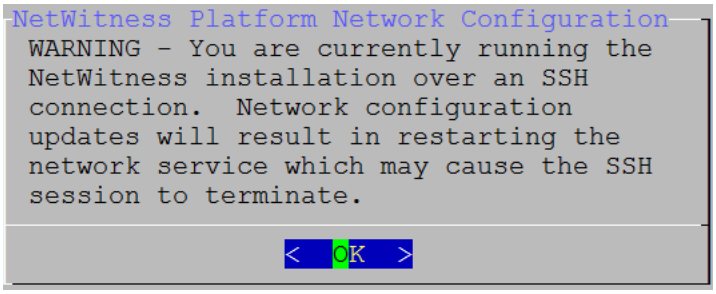
   - Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt:

     Drücken Sie die **Eingabetaste**, wenn Sie diese IP verwenden und Ihre Netzwerkeinstellungen nicht ändern möchten. Navigieren 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:

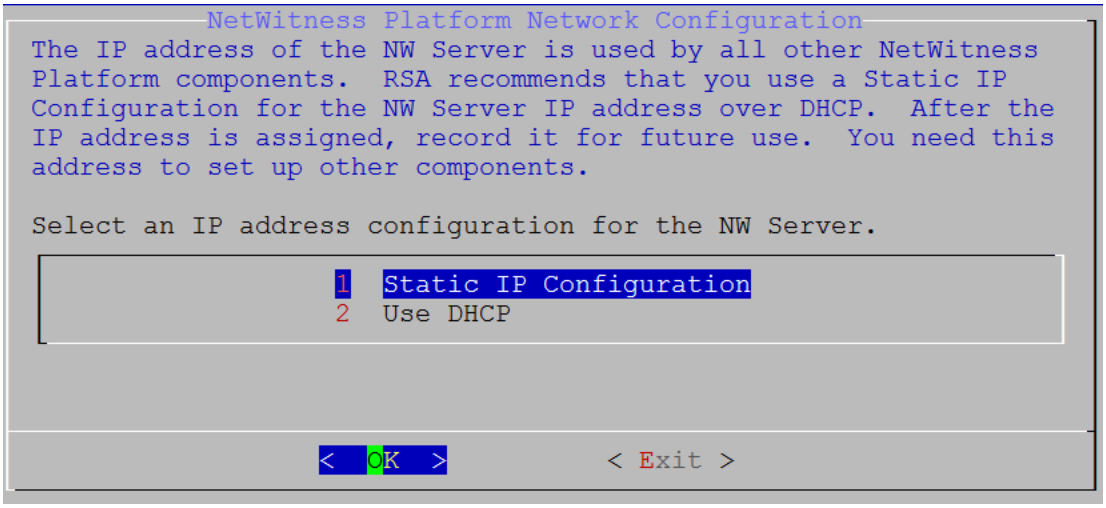
     Hinweis: Wenn die Verbindung direkt über die Hostkonsole erfolgt, wird die folgende Warnung nicht angezeigt.

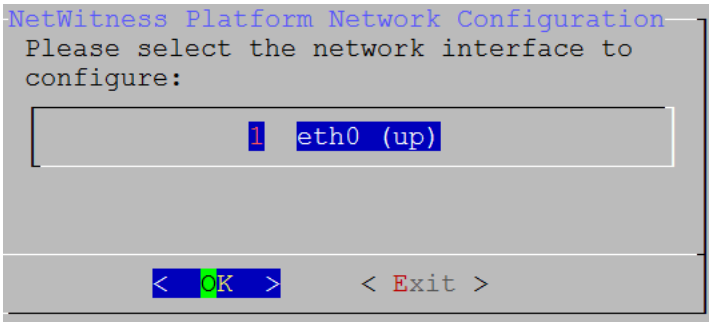
     Drücken Sie die **Eingabetaste**, um die Warnung zu schließen.

   - Wenn das Setup-Programm eine IP-Konfiguration gefunden hat und Sie sie ausgewählt haben, wird die Aufforderung **Update-Repository** angezeigt. Fahren Sie mit Schritt 12 fort und schließen Sie die Installation ab.

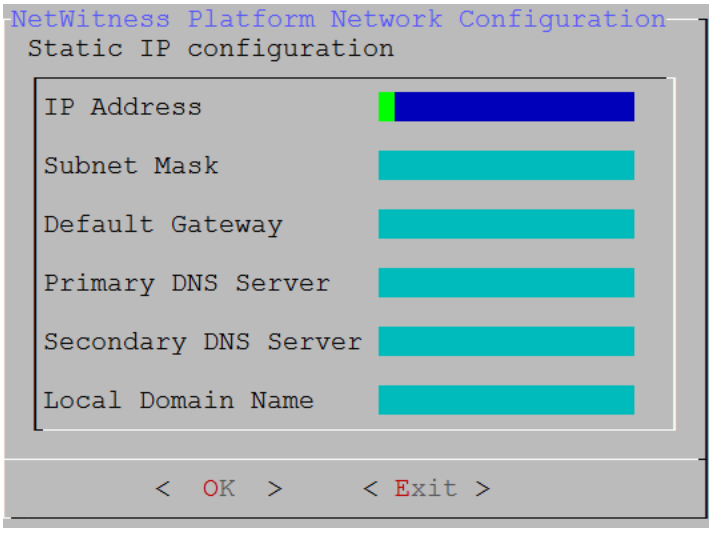
- Wenn das Setup-Programm keine IP-Konfiguration gefunden hat oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung **Netzwerkkonfiguration** angezeigt.



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.



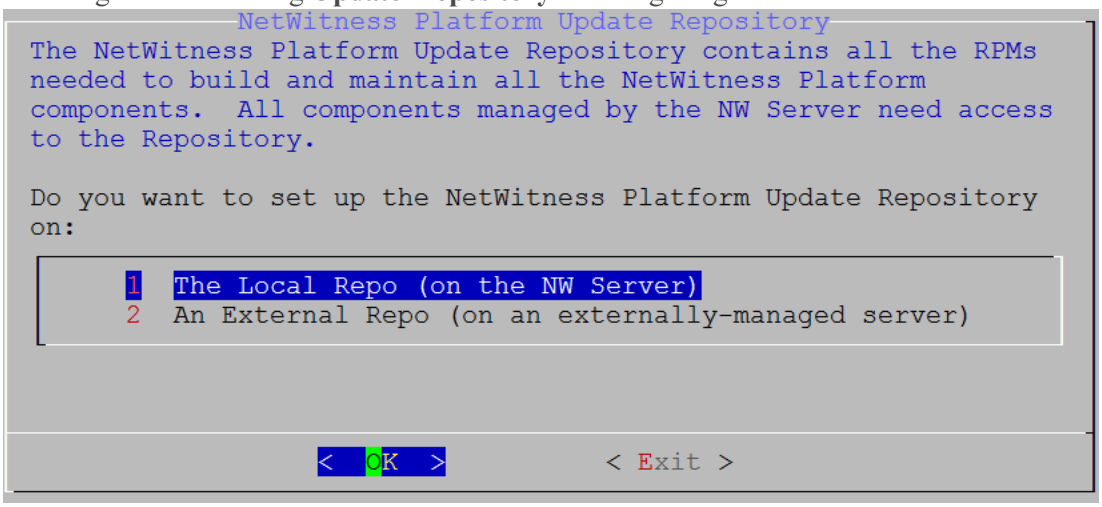
10. Gehen Sie mit dem Pfeil nach unten zur gewünschten Netzwerkschnittstelle. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**. Wenn Sie fortfahren möchten, gehen Sie zu **Beenden.**
    Die folgende Eingabeaufforderung **Konfiguration der statischen IP-Adresse** wird angezeigt.



11. Geben Sie die Konfigurationswerte (indem Sie mit dem Pfeil nach unten von Feld zu Feld gehen) ein. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**. Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung `All fields are required` angezeigt (die Felder **Sekundärer DNS-Server** und **Lokaler Domainname** sind keine Pflichtfelder). Wenn Sie für eines der Felder die falsche Syntax oder Zeichenlänge verwenden, wird die Fehlermeldung `Invalid <field-name>` angezeigt.

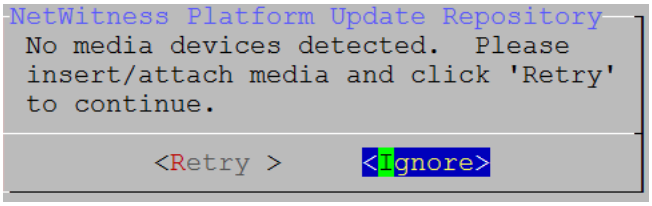
   Achtung: Wenn Sie **DNS-Server** auswählen, stellen Sie sicher, dass der DNS-Server korrekt ist und der Host darauf zugreifen kann, bevor Sie mit der Installation fortfahren.

Die Eingabeaufforderung **Update-Repository** wird angezeigt.

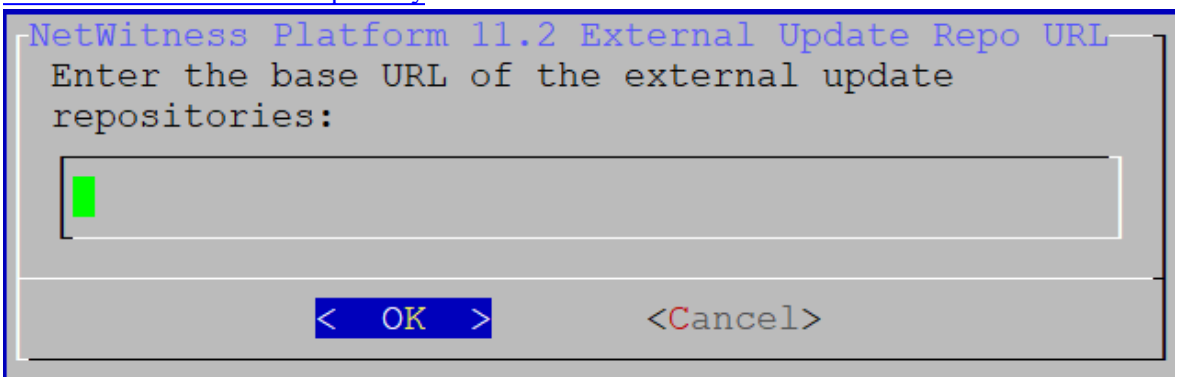


12. Drücken Sie die **Eingabetaste**, um das **lokale Repository** auf dem NW-Server auszuwählen. Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **Externes Repository** und dann zu **OK** und drücken Sie die **Eingabetaste**.

    - Stellen Sie bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** im Setup-Programm sicher, dass die richtigen Medien mit dem Host verbunden sind (Medien mit der ISO-Datei, z. B. ein Build-Stick), von denen es die Installation von NetWitness Platform 11.2.0.0 abrufen kann. Wenn das Programm die verbundenen Medien nicht finden kann, wird die folgende Aufforderung angezeigt.

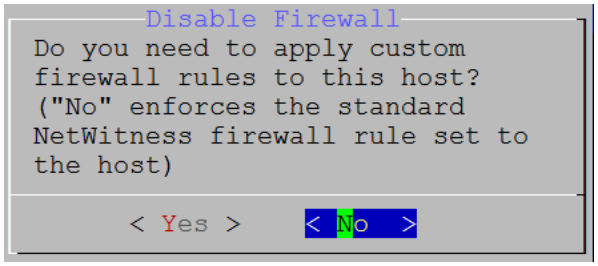


    - Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe einer URL aufgefordert. Die Repositorys bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates. Anweisungen zum Erstellen dieses Repository und der externen Repo-URL, damit Sie diese in die folgende Eingabeaufforderung eingeben können, finden Sie in Anhang B: Erstellen eines externen Repository.



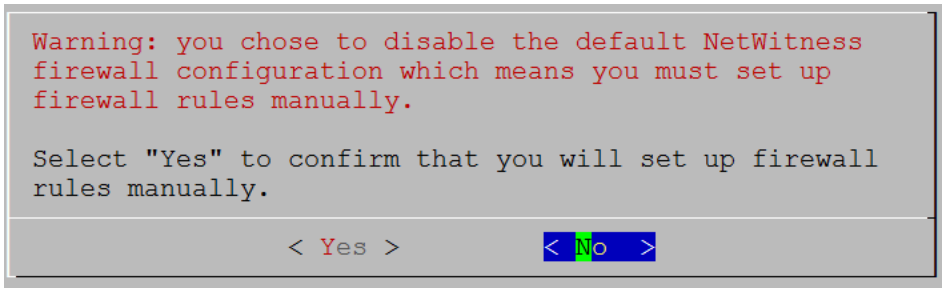
    Geben Sie den Basis-URL für das externe NetWitness Platform-Repository ein und klicken Sie

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“ im *RSA NetWitness Platform – Leitfaden für die ersten Schritte mit Hosts und Services*. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
Die Aufforderung „Firewall deaktivieren“ wird angezeigt.

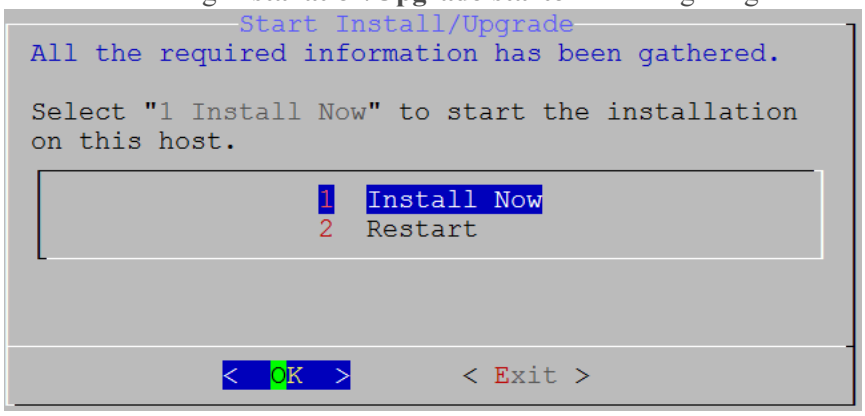


13. Um die Standardkonfiguration für Firewalls zu verwenden, gehen Sie zu **Nein** (Standardauswahl) und drücken die Eingabetaste. Um die Standardkonfiguration für Firewalls zu deaktivieren, gehen Sie zu **Ja** und drücken Sie die **Eingabetaste**.

- Bestätigen Sie Ihre Auswahl, indem Sie **Ja** auswählen, oder wählen Sie **Nein** aus, um die Standardkonfiguration für Firewalls zu verwenden.

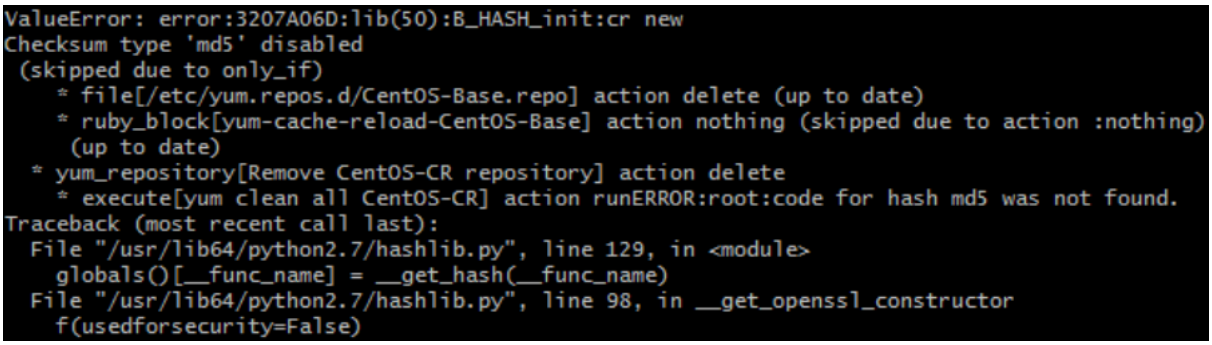


Die Aufforderung **Installation/Upgrade starten** wird angezeigt.



14. Drücken Sie die **Eingabetaste**, um 11.2 auf dem NW-Server zu installieren.
    Wenn **Installation abgeschlossen** angezeigt wird, haben Sie den 11.2 NW-Server auf diesem Host installiert.

    Hinweis: Ignorieren Sie Hashcodefehler 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.



Aufgabe 2: Installieren von 11.2 auf den Hosts anderer Komponenten

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

- Erstellen eines Basis-Image
- Einrichten des 11.2 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.

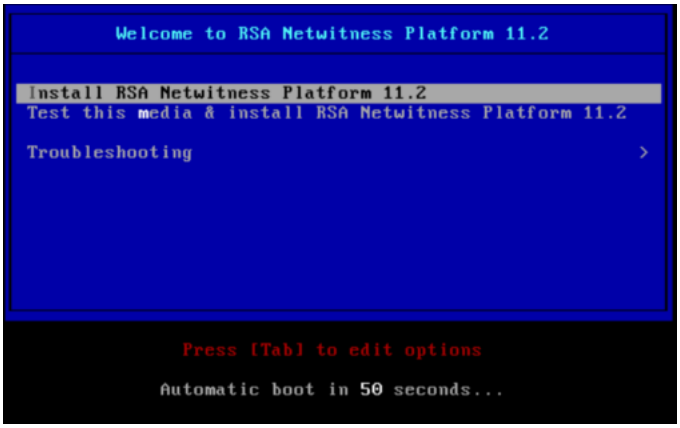
Führen Sie die folgenden Schritte aus, um NetWitness Platform 11.2 auf einem Nicht-NW-Server-Host zu installieren.

1. Erstellen Sie ein Basis-Image auf dem Host:
   a. Verbinden Sie Medien (Medien mit der ISO-Datei, z. B. ein Build-Stick) mit dem Host. Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Platform Build-Stick*.
      - Hypervisor-Installationen: Verwenden Sie das ISO-Image.
      - Physische Medien: Verwenden Sie die ISO-Datei, 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® Platform Build-Stick* finden Sie Informationen zum Erstellen eines Build-Sticks von der ISO-Datei. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
      - iDRAC-Installationen – der Typ der virtuellen Medien lautet:
        - **Virtuelles Diskettenlaufwerk** für zugeordnete Flash-Laufwerke
        - **Virtuelle CD** für zugeordnete optische Mediengeräte oder ISO-Datei.

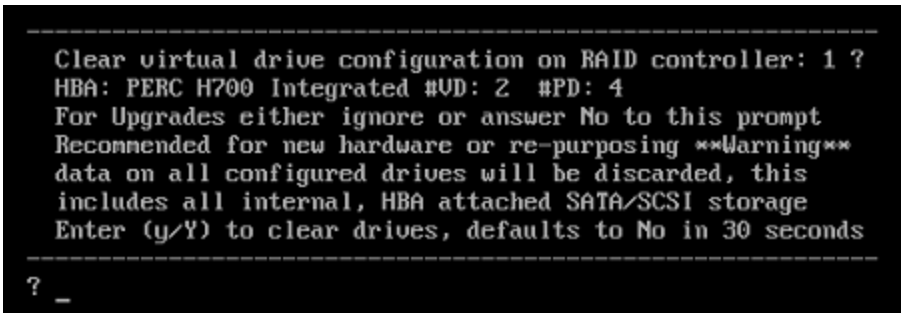
      Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Platform Build-Stick*.
   b. Melden Sie sich beim Host an und starten Sie ihn neu.

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

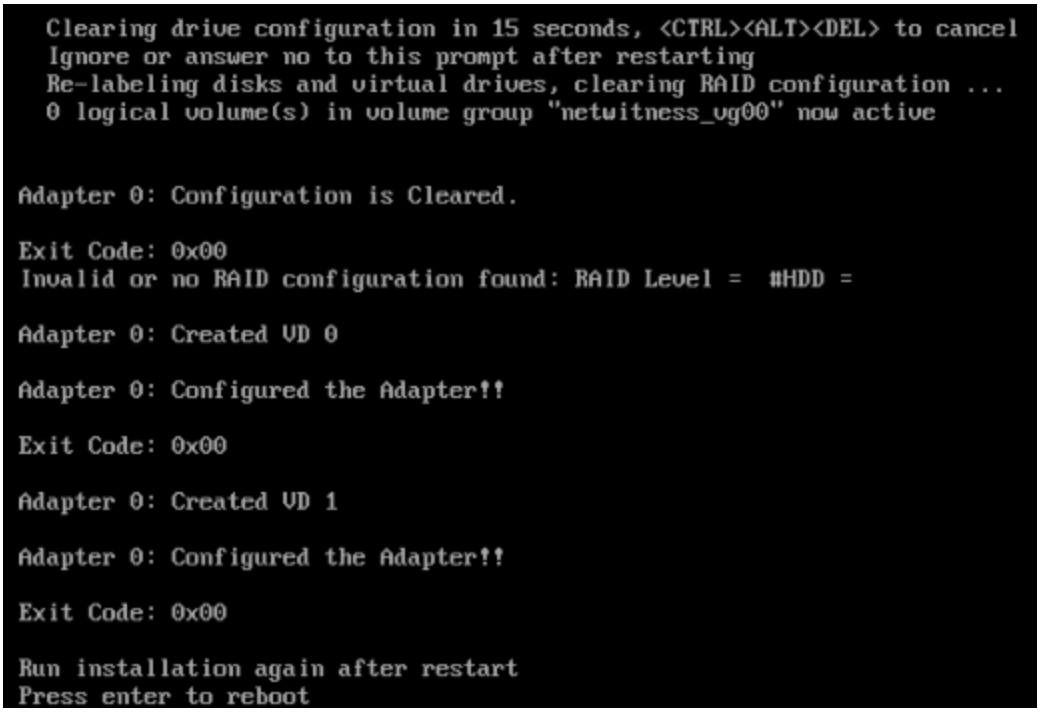
c. Wählen Sie während des Neustarts **F11** (Startmenü) aus, um ein Startgerät auszuwählen und von den verbundenen Medien zu starten.
Nach einigen Systemprüfungen während des Startvorgangs wird das folgende Installationsmenü angezeigt: **Willkommen bei RSA NetWitness Platform 11.2**. Die Grafiken im Menü werden anders dargestellt, wenn Sie ein physisches USB-Flash-Medium verwenden.



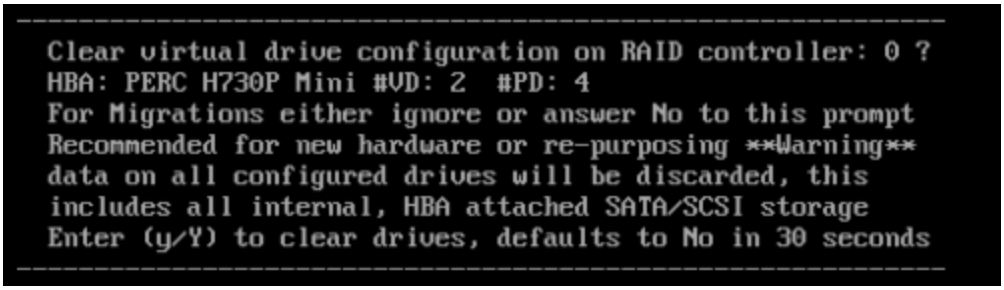
d. Wählen Sie **RSA NetWitness Platform 11.2 installieren** (Standardauswahl) aus und drücken Sie die **Eingabetaste**.
Das Installationsprogramm wird ausgeführt. Es wird bei der Eingabeaufforderung **j/J eingeben, um Laufwerke zu löschen** angehalten, in der Sie aufgefordert werden, die Laufwerke zu 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.

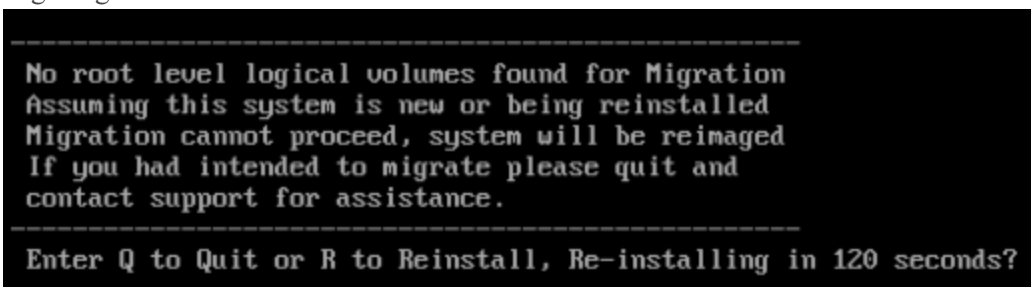


f. Drücken Sie die **Eingabetaste**, um den Host neu zu starten.
Das Installationsprogramm fordert Sie erneut auf, die Laufwerke zu löschen.



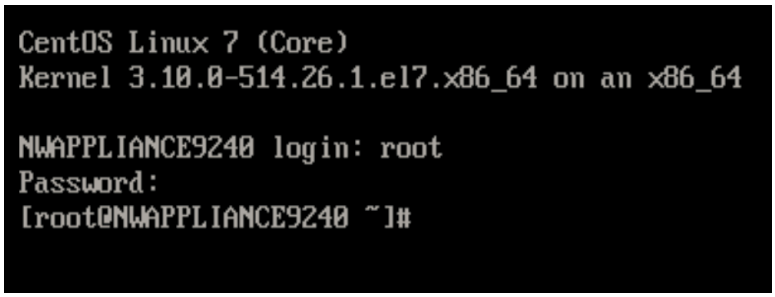
g. Geben Sie **N** ein, da Sie die Laufwerke bereits gelöscht haben.
Die Eingabeaufforderung **Q zum Beenden oder R für Neuinstallation eingeben)** wird

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.

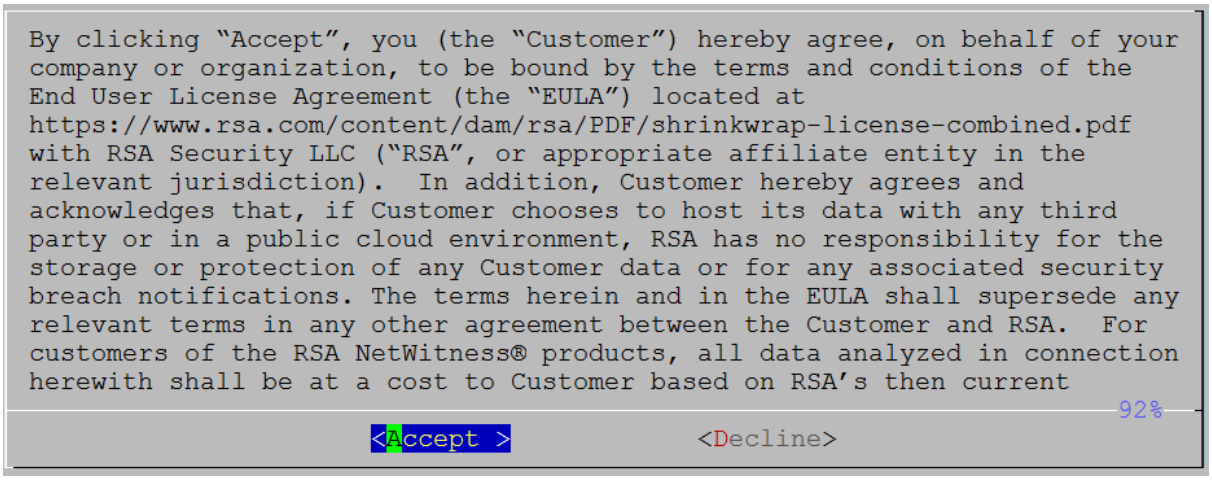
Achtung: Starten Sie die angeschlossenen Medien (Medien mit der ISO-Datei, z. B. ein Build-Stick) nicht neu.



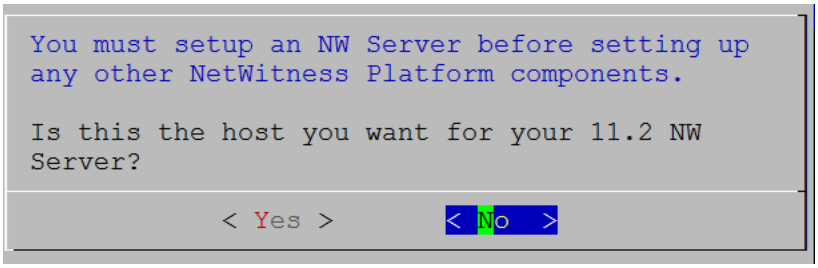
i. Melden Sie sich mit den `root` -Anmeldedaten beim Host an.

2. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.
Dadurch wird das `nwsetup-tui` 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 „(Optional) Aufgabe 1: Erneutes Konfigurieren von DNS-Servern nach 11.2“ in den Aufgaben nach der Installation.
Wenn Sie keinen DNS-Server während `nwsetup-tui` angeben, müssen Sie **1 Lokales Repository (auf dem NW-Server)** in der Eingabeaufforderung **NetWitness PlatformRepository aktualisieren** in Schritt 11 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repository zugreifen kann).

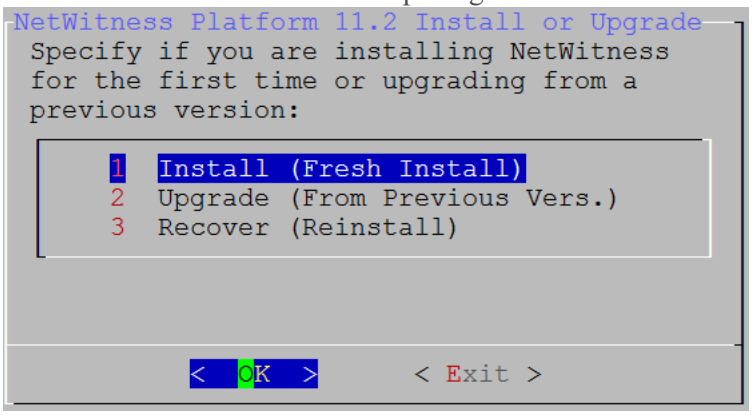


3. Gehen Sie zu **Akzeptieren** und drücken Sie die **Eingabetaste**.
   Es wird eine Aufforderung mit der Frage angezeigt, ob dies der Host ist, den Sie für Ihren 11.2 NW-Server verwenden möchten.

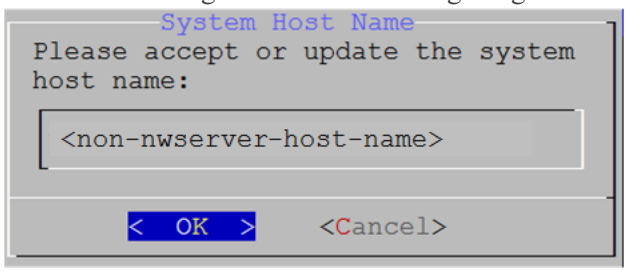


Achtung: Wenn Sie den falschen Host für den NW-Server auswählen und die Installation abschließen, müssen Sie das Setup-Programm neu starten und Aufgabe 1: Installieren von 11.2 auf dem NetWitness-Server-Host (Schritt 2 bis 14) ausführen, um diesen Fehler zu korrigieren.

4. Drücken Sie die **Eingabetaste** (Nein).
   Die Aufforderung **Installieren** oder **Upgrade durchführen** wird angezeigt (**Wiederherstellen** gilt nicht für die Installation. Diese Option gilt für 11.2 Disaster Recovery.).



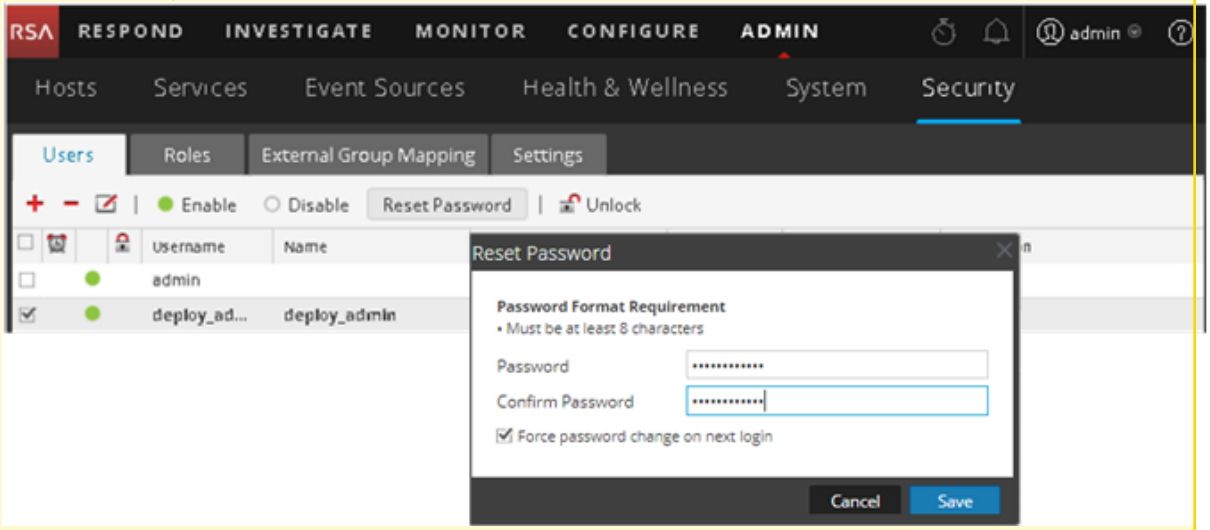
5. Drücken Sie die **Eingabetaste**. Die Option für Installieren (neue Installation) ist standardmäßig ausgewählt.
   Die Aufforderung **Hostname** wird angezeigt.



Achtung: Wenn Sie „.“ in einen Hostnamen einfügen, muss dieser auch einen gültigen Domainnamen enthalten.

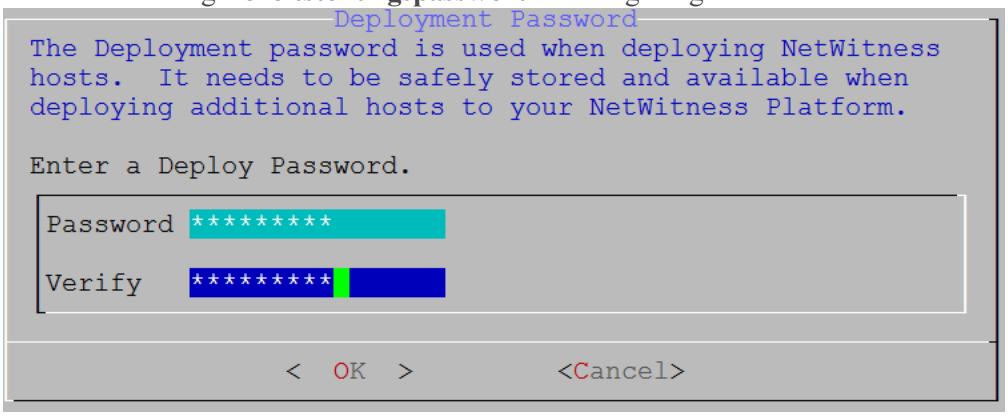
6. Drücken Sie die **Eingabetaste**, wenn dieser Name beibehalten werden soll. Wenn Sie diesen Namen ändern möchten, bearbeiten Sie ihn, gehen Sie zu **OK** und drücken Sie die **Eingabetaste**.
   Die Aufforderung **Masterpasswort** wird angezeigt.

Achtung: Wenn Sie das Nutzerpasswort **deploy_admin** auf der NetWitness Platform-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.

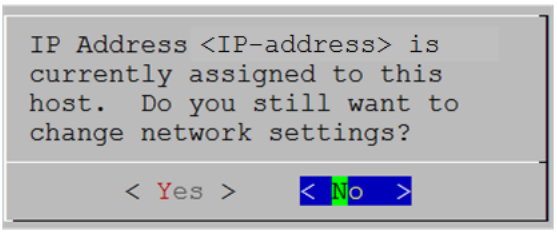
Die Aufforderung **Bereitstellungspasswort** wird angezeigt.



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**.

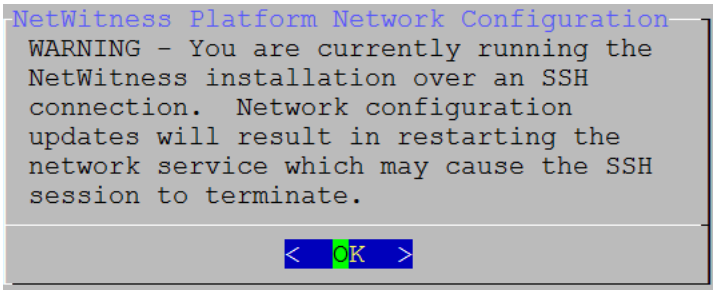
   - Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt:

     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:

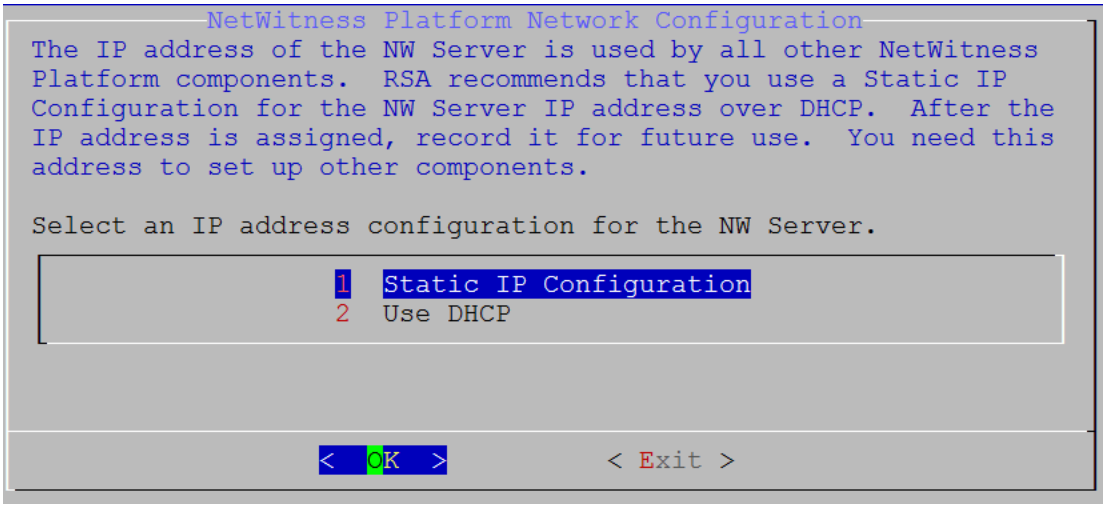
     Hinweis: Wenn die Verbindung direkt über die Hostkonsole erfolgt, wird die folgende Warnung nicht angezeigt.

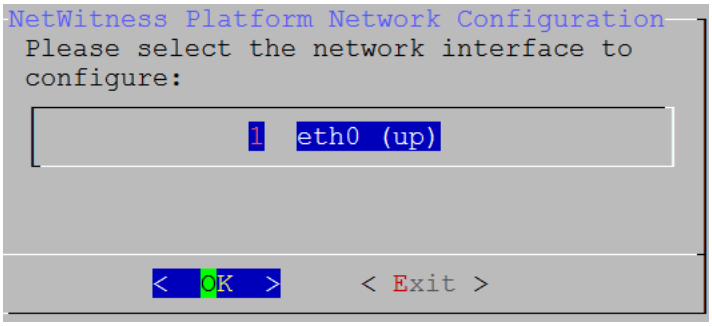
     Drücken Sie die **Eingabetaste**, um die Warnung zu schließen.

   - 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.

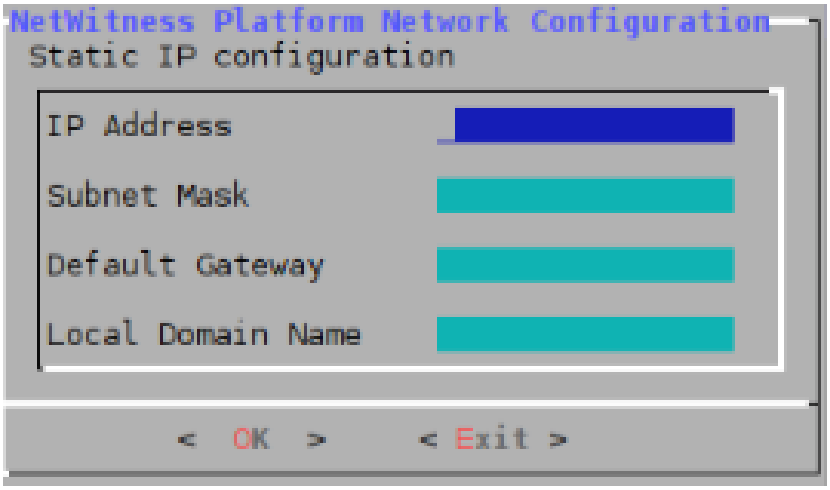
- Wenn das Setup-Programm keine IP-Konfiguration gefunden hat oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung **Netzwerkkonfiguration** angezeigt.



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 **Eingabetaste**.
   Die Eingabeaufforderung **Netzwerkkonfiguration** wird angezeigt.



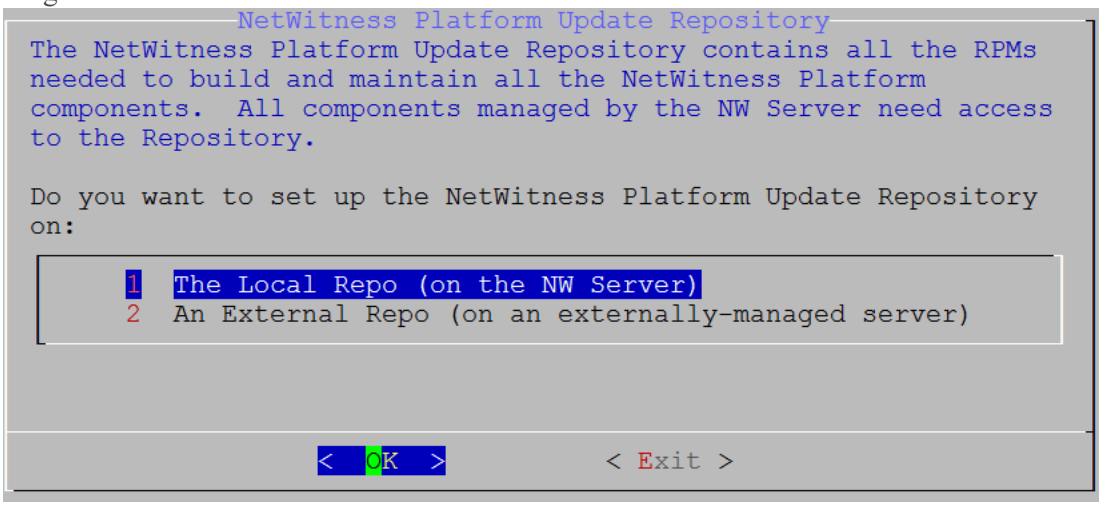
9. Gehen Sie mit dem Pfeil nach unten zur gewünschten Netzwerkschnittstelle. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**. Wenn Sie fortfahren möchten, gehen Sie zu **Beenden**.
   Die folgende Eingabeaufforderung **Konfiguration der statischen IP-Adresse** wird angezeigt.



10. Geben Sie die Konfigurationswerte (indem Sie mit dem Pfeil nach unten von Feld zu Feld gehen) ein. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**.
    Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung `All fields are required` angezeigt (die Felder **Sekundärer DNS-Server** und **Lokaler Domainname** sind keine Pflichtfelder).
    Wenn Sie für eines der Felder die falsche Syntax oder Zeichenlänge verwenden, wird die Fehlermeldung `Invalid <field-name>` angezeigt.

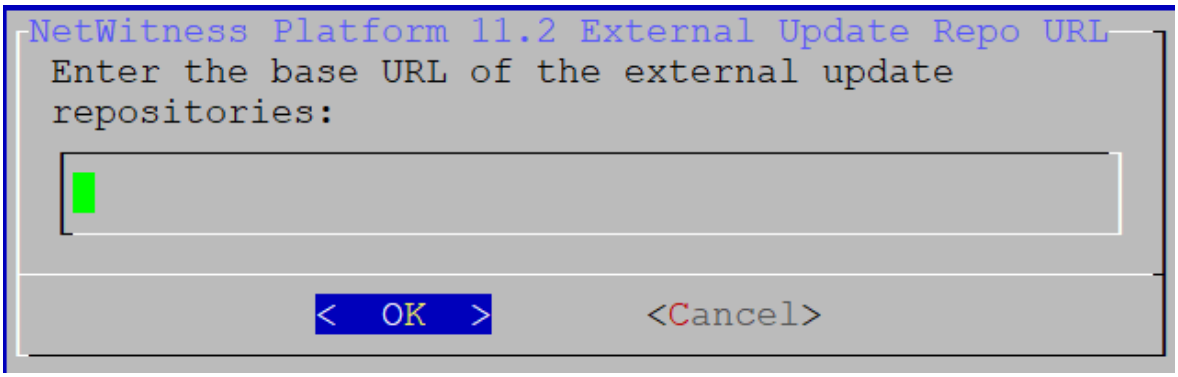
    Achtung: Wenn Sie **DNS-Server** auswählen, stellen Sie sicher, dass der DNS-Server korrekt ist und der Host darauf zugreifen kann, bevor Sie mit der Installation fortfahren.

    Die Eingabeaufforderung **Update-Repository** wird angezeigt.
    Wählen Sie für alle Hosts das gleiche Repository aus, das Sie bei Installation des NW-Serverhosts ausgewählt haben.

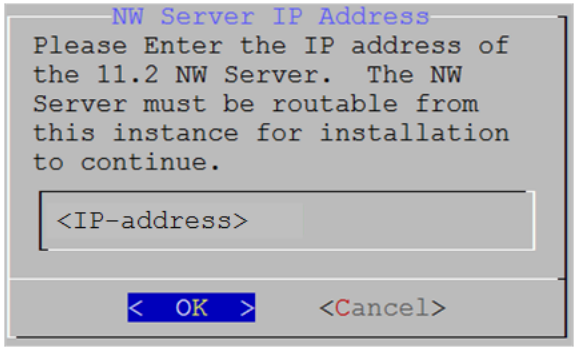


11. Drücken Sie die **Eingabetaste**, um das **lokale Repository** auf dem NW-Server auszuwählen.
    Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **Externes Repository** und dann zu **OK** und drücken Sie die **Eingabetaste**.

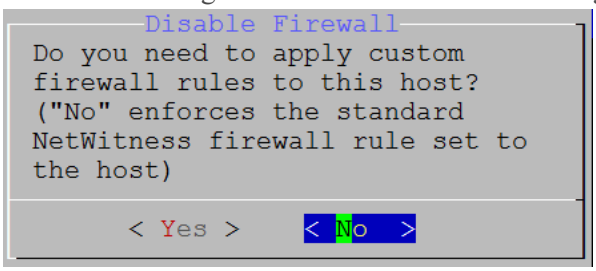
    - Stellen Sie bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** im Setup-Programm sicher, dass die richtigen Medien mit dem Host verbunden sind (Medien mit der ISO-Datei, z. B. ein Build-Stick), von denen es die Installation von NetWitness Platform 11.2.0.0 abrufen kann.
    - Bei Auswahl von **2 Ein externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe einer URL aufgefordert. Die Repositorys bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates. Anweisungen zum Erstellen dieses Repository und der externen Repo-URL, damit Sie diese in die folgende Eingabeaufforderung eingeben können, finden Sie in Anhang B: Erstellen eines externen Repository.



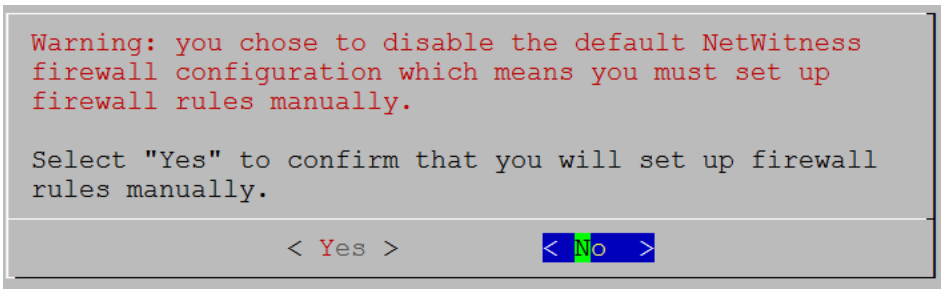
Geben Sie den Basis-URL des externen NetWitness Platform-Repository an, gehen Sie zu **OK** und drücken Sie die **Eingabetaste**.
Die Aufforderung zur Eingabe der **IP-Adresse des NW-Servers** wird angezeigt.



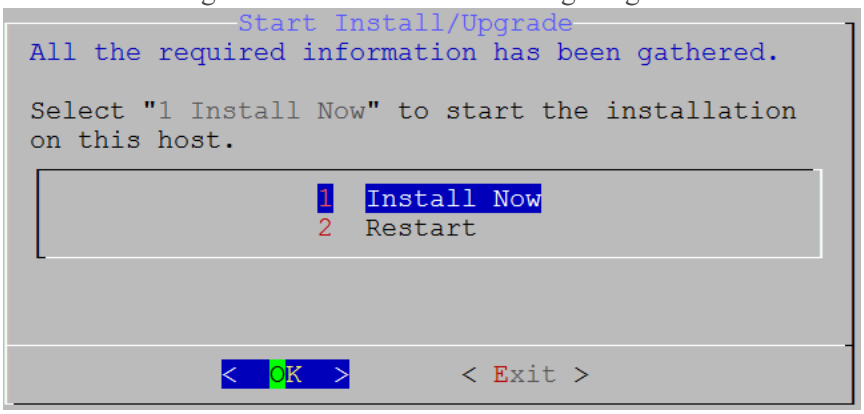
12. Geben Sie die IP-Adresse des NW-Servers ein. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**.
    Die Aufforderung **Firewall deaktivieren** wird angezeigt.



13. Um die Standardkonfiguration für Firewalls zu verwenden, gehen Sie zu **Nein** (Standardauswahl) und drücken die Eingabetaste. Um die Standardkonfiguration für Firewalls zu deaktivieren, gehen Sie zu **Ja** und drücken die **Eingabetaste**.
    - Bestätigen Sie Ihre Auswahl, indem Sie **Ja** auswählen, oder wählen Sie **Nein** aus, um die Standardkonfiguration für Firewalls zu verwenden.



Die Aufforderung **Installation starten** wird angezeigt.

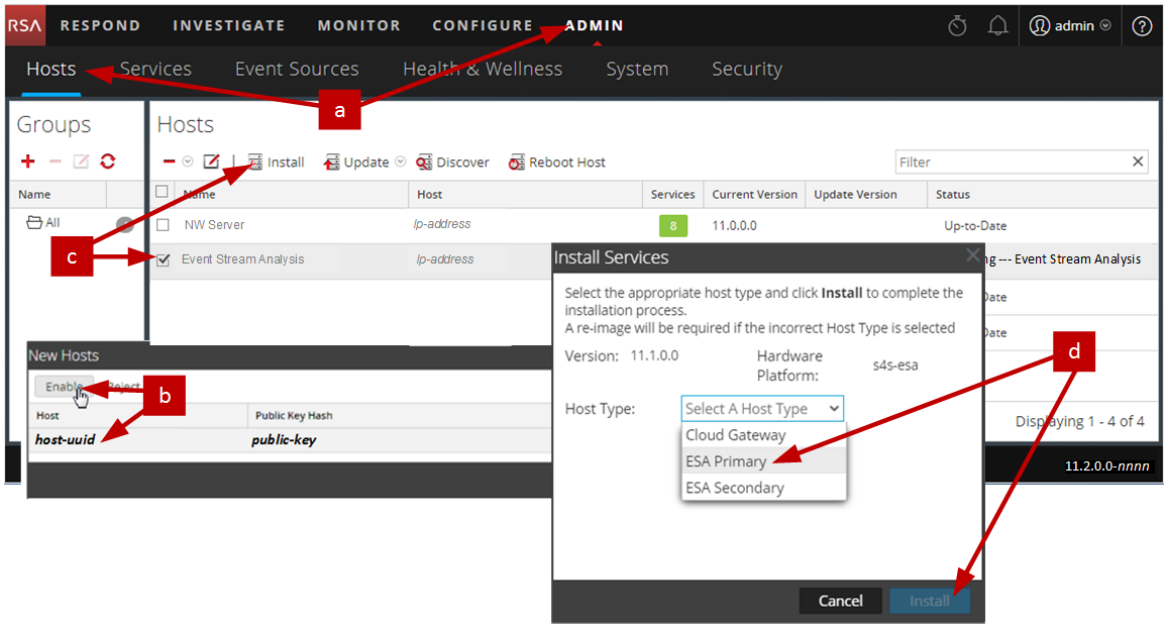


14. Drücken Sie die Eingabetaste, um 11.2 auf dem NW-Server zu installieren.
    Wenn **Installation abgeschlossen** angezeigt wird, verfügen Sie über einen generischen Nicht-NW-Serverhost mit einem Betriebssystem, das mit NetWitness Platform 11.2 kompatibel ist.
15. Installieren Sie einen Komponentendienst auf dem Host.
    a. Melden Sie sich bei NetWitness Platform an und gehen Sie zu **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**.

    b. Wählen Sie im Dialogfeld **Neue Hosts** den Host aus und klicken Sie auf **Aktivieren**.
    Das Dialogfeld **Neue Hosts** wird geschlossen und der Host wird in der Ansicht **Hosts** angezeigt.
    c. Wählen Sie diesen Host (z. B. **Event Stream Analysis**) in der Ansicht **Hosts** aus und klicken Sie auf Install.
    Das Dialogfeld **Services installieren** wird angezeigt.

d. Wählen Sie den entsprechenden Hosttyp (z. B. **ESA Primary**) in **Hosttyp** aus und klicken Sie auf **Installieren**.



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

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

17. Füllen Sie die Lizenzierungsanforderungen für installierte Dienste aus.
Weitere Informationen finden Sie im *Leitfaden zum Lizenzierungsmanagement für RSA NetWitness Platform 11.2*.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Aktualisieren oder Installieren der Legacy-Windows-Sammlung

Siehe *Leitfaden RSA NetWitness Legacy Windows Collection*. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

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 11.2 ausführen.

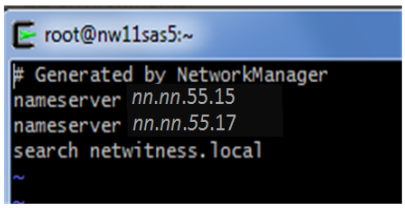
- Allgemeines
- RSA NetWitness® Endpoint Insights
- Aktivierung von FIPS
- RSA NetWitness® UEBA

Allgemein

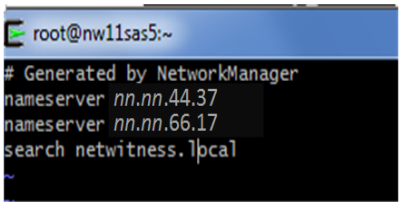
(Optional) Aufgabe 1: Erneutes Konfigurieren von DNS-Servern nach 11.2

Führen Sie auf dem NetWitness Server folgende Schritte aus, um die DNS-Server in NetWitness Platform 11.2 neu zu konfigurieren.

1. Melden Sie sich beim Serverhost mit Ihren `root` -Anmeldedaten an.
2. Bearbeiten Sie die Datei `/etc/netwitness/platform/resolv.dnsmasq`:
   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 dargestellt.



   Das folgende Beispiel zeigt die neuen DNS-Werte.



   b. Speichern Sie die Datei `/etc/netwitness/platform/resolv.dnsmasq`.
   c. Starten Sie den internen DNS neu, indem Sie folgenden Befehl ausführen:
   `systemctl restart dnsmasq`

RSA NetWitness Endpoint Insights

(Optional) Aufgabe 2: Installieren von Endpoint Hybrid oder Endpoint Log Hybrid

Sie müssen einen der folgenden Services zur Installation von NetWitness Platform Endpoint Insights in Ihrer Bereitstellung installieren:

- Endpoint Hybrid
- Endpoint Log Hybrid

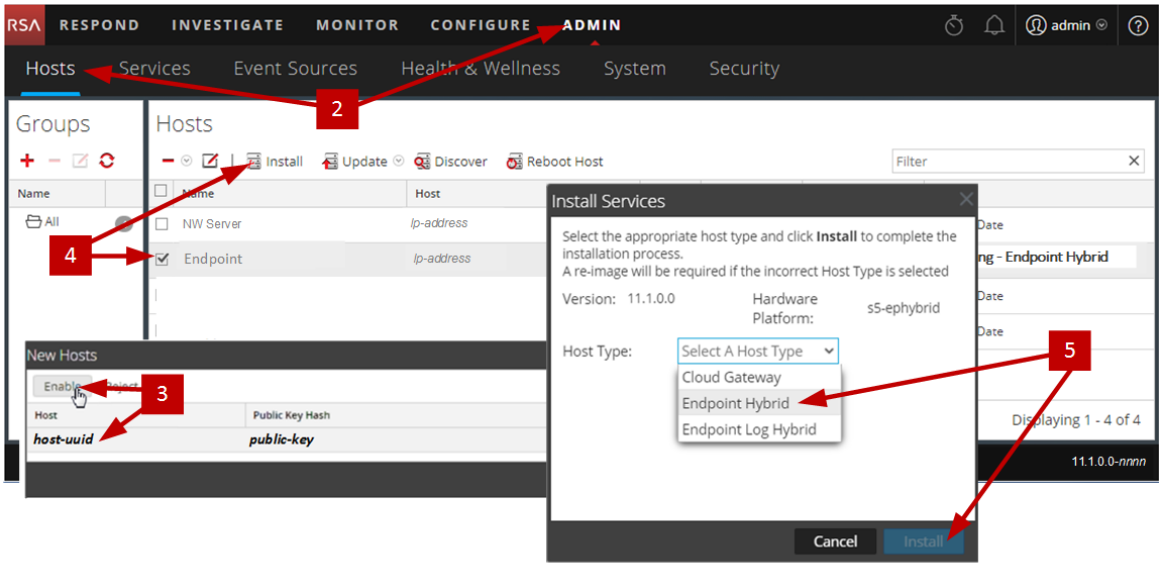
Achtung: Sie können nur eine Instanz der oben genannten Services in Ihrer Bereitstellung installieren.

Hinweis: Sie müssen den Endpoint Hybrid oder Endpoint Log Hybrid auf der S5- oder Dell R730-Appliance installieren.

1. Führen Sie für physische Hosts die Schritte 1 bis 14 bzw. für virtuelle Hosts die Schritte 1 bis 15 unter „Aufgabe 2: Installieren von 11.2 auf den Hosts anderer Komponenten“ in „Installationsaufgaben“ des *Installationshandbuchs für physische Hosts für Version 11.2 der NetWitness-Platform* aus. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
2. Melden Sie sich bei NetWitness Platform an und gehen Sie zu **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**.
3. Wählen Sie im Dialogfeld **Neue Hosts** den Host aus und klicken Sie auf **Aktivieren**.
   Das Dialogfeld „Neue Hosts“ wird geschlossen und der Host wird in der Ansicht „Hosts“ angezeigt.
4. Wählen Sie diesen Host (z. B. **Endpoint**) in der Ansicht **Hosts** aus und klicken Sie auf Install.
   Das Dialogfeld „Services installieren“ wird angezeigt.

5. Wählen Sie den entsprechenden Service aus, entweder **Endpoint Hybrid** oder **Endpoint Log Hybrid**, und klicken Sie auf **Installieren**.
   Endpoint Hybrid wird im folgenden Screenshot als Beispiel verwendet.



6. Stellen Sie sicher, dass alle Endpoint Hybrid- oder Endpoint Log Hybrid-Services ausgeführt werden.
7. Konfigurieren Sie die Weiterleitung von Endpunktmetadaten.
   Anweisungen zum Konfigurieren der Weiterleitung von Endpunktmetadaten finden Sie im *Konfigurationsleitfaden zu Endpoint Insights*.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
8. Installieren Sie den Endpoint Insights Agent.
   Detaillierte Anweisungen zum Installieren des Agenten finden Sie im *Endpoint Insights Agent-Installationshandbuch*.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

FIPS-Aktivierung

(Optional) Aufgabe 3: FIPS-Modus aktivieren

Federal Information Processing Standard (FIPS) ist für alle Services aktiviert, mit Ausnahme von Log Collector, Log Decoder und Decoder. FIPS kann für keinen Service deaktiviert werden, mit Ausnahme von Log Collector, Log Decoder und Decoder. Weitere Informationen darüber, wie FIPS für diese Services aktiviert werden kann, finden Sie im Thema „Aktivieren oder Deaktivieren von FIPS“ im *Leitfaden für die Systemwartung in RSA NetWitness Platform*.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

RSA NetWitness® UEBA

(Optional) Aufgabe 4: Installieren von NetWitness UEBA

Um NetWitness UEBA in NetWitness Platform 11.2 einzurichten, müssen Sie den NetWitness UEBA-Service installieren und konfigurieren.

Die folgenden Schritte zeigen, wie Sie den NetWitness UEBA-Service auf einem NetWitness UEBA-Hosttyp installieren und den Service konfigurieren.

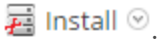
1. Führen Sie für physische Hosts die Schritte 1 bis 14 bzw. für virtuelle Hosts die Schritte 1 bis 15 unter „Aufgabe 2: Installieren von 11.2 auf den Hosts anderer Komponenten“ in „Installationsaufgaben“ des *Installationshandbuchs für physische Hosts für Version 11.2 der NetWitness-Platform* aus. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

   Hinweis: Das Passwort der Benutzeroberfläche von Kibana und dem Airflow-Webserver ist das gleiche wie das „deploy_admin“-Passwort. Vergewissern Sie sich, dass Sie dieses Passwort notieren und an einem sicheren Ort aufbewahren.

2. Melden Sie sich bei NetWitness Platform an und gehen Sie zu **ADMIN** > **Hosts**.
   Das Dialogfeld „Neue Hosts“ wird angezeigt; die Ansicht „Hosts“ ist im Hintergrund abgeblendet.

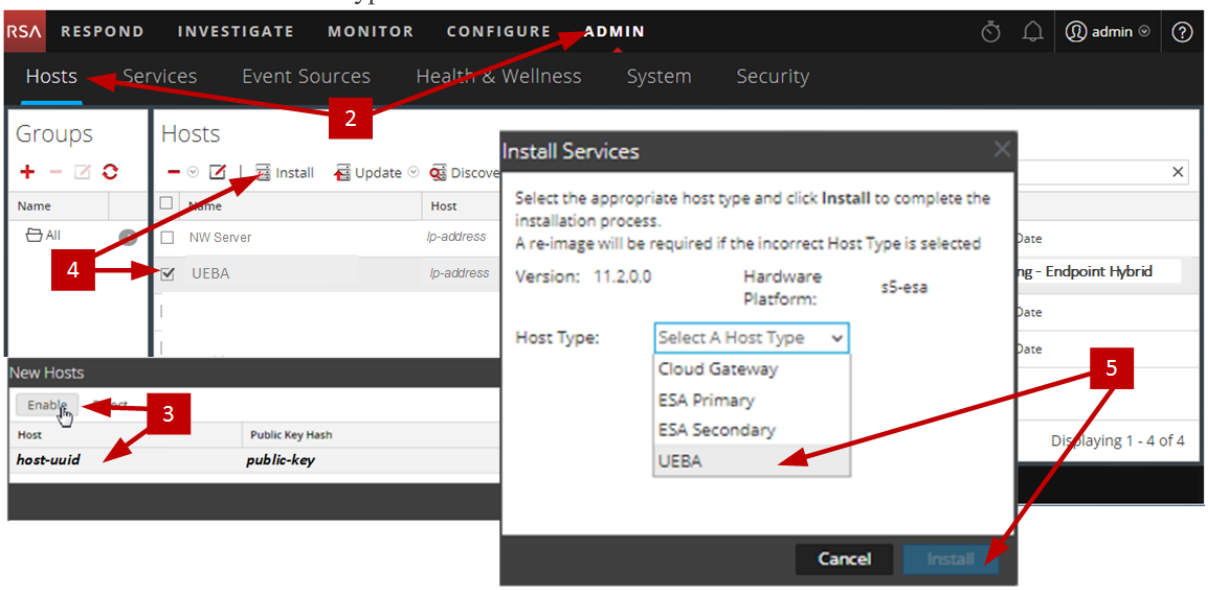
   Hinweis: Wenn das Dialogfeld **Neue Hosts** nicht angezeigt wird, klicken Sie in der Symbolleiste der Ansicht „Hosts“ auf **Erkennen**.

3. Wählen Sie im Dialogfeld **Neue Hosts** den Host aus und klicken Sie auf **Aktivieren**.
   Das Dialogfeld „Neue Hosts“ wird geschlossen und der Host wird in der Ansicht „Hosts“ angezeigt.

4. Wählen Sie diesen Host (z. B. **UEBA**) in der Ansicht **Hosts** aus und klicken Sie auf 

.
   Das Dialogfeld „Services installieren“ wird angezeigt.

5. Wählen Sie den **UEBA**-Hosttyp aus und klicken Sie auf **Installieren**.



6. Überprüfen Sie, ob der UEBA-Service ausgeführt wird.

7. Sorgen Sie dafür, dass alle Lizenzierungsvoraussetzungen für NetWitness UEBA erfüllt sind. Weitere Informationen finden Sie im *Leitfaden zum Lizenzierungsmanagement für RSA NetWitness Platform 11.2*. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

   Hinweis: NetWitness Platform unterstützt die UEBA-Lizenz (Analyse des Nutzer- und Entitätsverhaltens). Diese Lizenz richtet sich nach der Anzahl der Nutzer. Die vorkonfigurierte Testlizenz gilt für 90 Tage. Im Falle von UEBA-Lizenzen beginnt die 90-tägige Testzeit ab dem Zeitpunkt, ab dem der UEBA-Service auf NetWitness Platform bereitgestellt ist.

8. Konfigurieren Sie NetWitness UEBA.
   Sie müssen eine Datenquelle (Broker oder Concentrator), ein Startdatum für die Erfassung historischer Daten und Datenschemata konfigurieren.

   WICHTIG: Wenn Ihre Bereitstellung über mehrere Concentrators verfügt, empfiehlt RSA, dass Sie den Broker als Datenquelle von NetWitness UEBA an die Spitze der Bereitstellungshierarchie platzieren.

   a. Bestimmen Sie das früheste Datum in der NWDB des Datenschemas, das Sie auswählen möchten (`AUTHENTICATION`, `FILE`, `ACTIVE_DIRECTORY` oder eine Kombination dieser Schemata), um dies in `startTime` in Schritt c anzugeben. Wenn Sie mehrere Schemata angeben möchten, verwenden Sie das früheste Datum aus diesen Schemata. Wenn Sie sich nicht sicher sind, welches Datenschema Sie auswählen sollten, können Sie alle drei Datenschemata angeben (das heißt `AUTHENTICATION`, `FILE` und `ACTIVE_DIRECTORY`), damit UEBA die unterstützten Modelle auf Grundlage der verfügbaren Windows-Protokolle anpassen kann. Mit einer der folgenden Methoden können Sie das Datum der Datenquelle ermitteln.

- Verwenden Sie das Datum der Datenaufbewahrung (das heißt, wenn die Dauer der Datenaufbewahrung 48 Stunden beträgt, `startTime` = <aktueller Zeitpunkt minus 48 Stunden>).
- Suchen Sie in der NWDB nach dem frühesten Datum.

b. Erstellen Sie ein Nutzerkonto für die Datenquelle (Broker oder Concentrator), um sich bei der Datenquelle zu authentifizieren.

i. Melden Sie sich bei NetWitness Platform an.

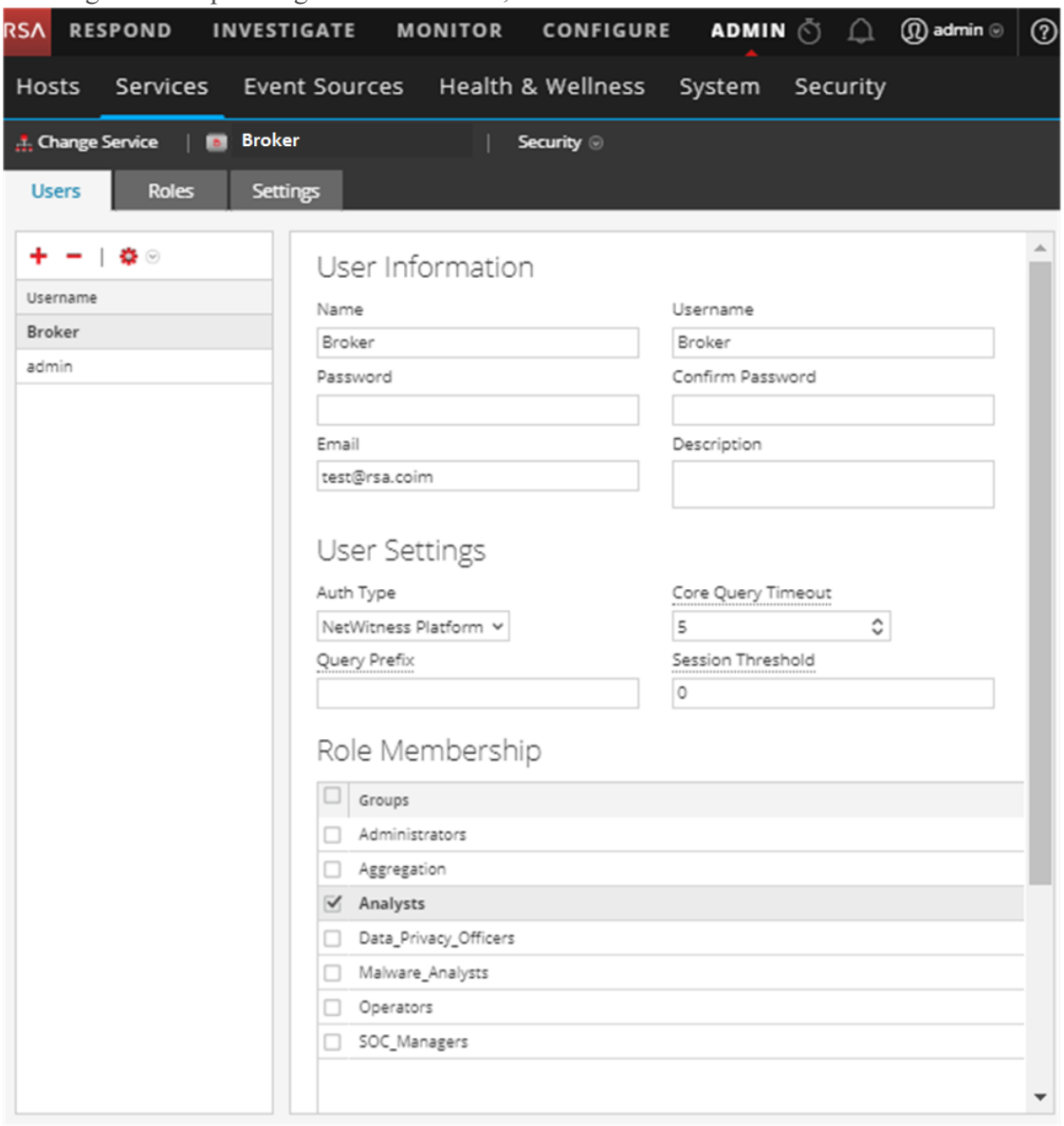
ii. Navigieren Sie zu **Administration** > **Services**.

iii. Suchen Sie den Datenquellenservice (Broker oder Concentrator).

Wählen Sie einen Service und anschließend  (Aktionen) > **Ansicht** > **Sicherheit** aus.

iv. Erstellen Sie einen neuen Nutzer und weisen Sie ihm die „Analysten“-Rolle zu.

Das folgende Beispiel zeigt ein Nutzerkonto, das für einen Broker erstellt wurde.



c. Stellen Sie über SSH eine Verbindung mit dem NetWitness UEBA-Serverhost her.

d. Senden Sie die folgenden Befehle.

```
/opt/rsa/saTools/ueba-server-config -u <user> -p <password> -h <host> -o
<type> -t <startTime> -s <schemas> -v
```

Dabei gilt Folgendes:

Argument	Variable	Beschreibung
`-u`	`<user>`	Nutzername für die Broker oder Concentrator-Instanz, die Sie als Datenquelle verwenden.
`-p`	`<password>`	Passwort für die Broker oder Concentrator-Instanz, die Sie als Datenquelle verwenden. Folgende Sonderzeichen werden in einem Passwort unterstützt. `!"#$%&()*+,-:;<=>?@[\]^_`\{\|}` Wenn Sie Sonderzeichen verwenden möchten, müssen Sie das Passwort in gerade Anführungszeichen setzen, zum Beispiel: `sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '!"UHfz?@ExMn#$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_ DIRECTORY' -o broker -v`
`-h`	`<host>`	IP-Adresse des Broker oder Concentrator, der als Datenquelle verwendet wird. Derzeit wird nur eine Datenquelle unterstützt.
`-o`	`<type>`	Datenquellen-Hosttyp (`broker` oder `concentrator`).
`-t`	`<startTime>`	Historische Startzeit, ab der Daten aus der Datenquelle im Format YYYY-MM-DDTHH-MM-SSZ erfasst werden (zum Beispiel `2018-08-15T00:00:00Z`). **Hinweis:** Das Skript interpretiert die eingegebene Zeit als UTC (Coordinated Universal Time) und passt die Zeit nicht an Ihre Zeitzone an.

Argument	Variable	Beschreibung
`-s`	`<schemas>`	Array von Datenschemata. Wenn Sie mehrere Schemata angeben möchten, verwenden Sie ein Leerzeichen zwischen den Schemata (zum Beispiel `'AUTHENTICATION FILE ACTIVE_DIRECTORY'`). **Hinweis:** Wenn Sie alle drei Datenschemata angeben (das heißt `AUTHENTICATION`, `FILE` und `ACTIVE_DIRECTORY`), passt UEBA die unterstützten Modelle auf Grundlage der verfügbaren Windows-Protokolle an.
`-v`		Ausführlicher Modus.

9. Führen Sie die NetWitness UEBA-Konfiguration entsprechend den Anforderungen Ihres Unternehmens durch.
   Weitere Informationen finden Sie im *RSA NetWitness UEBA – Benutzerhandbuch*. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Anhang A: Troubleshooting

Dieser Abschnitt beschreibt Lösungen für Probleme, die während Installationen oder Upgrades auftreten können. In den meisten Fällen erstellt NetWitness Platform Protokollmeldungen, wenn Probleme auftreten.

Hinweis: Wenn Sie Probleme beim Upgrade mithilfe der folgenden Troubleshooting-Lösungen nicht beheben können, wenden Sie sich an den Kundensupport (https://community.rsa.com/docs/DOC-1294).

Dieser Abschnitt enthält Troubleshooting-Dokumentation für die folgenden Services, Funktionen und Prozesse:

- CLI (Command Line Interface)
- Backupskript
- Event Stream Analysis
- Log Collector-Service (`nwlogcollector`)
- Orchestrierung
- NW-Server
- Reporting Engine
- NetWitness UEBA

CLI (Command Line Interface)

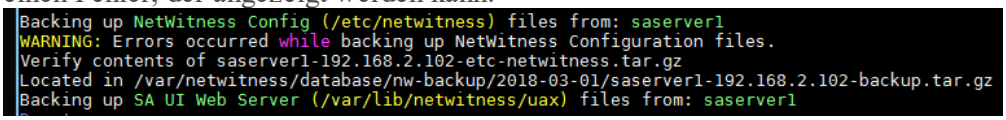
Fehlermeldung	CLI (Command Line Interface) wird angezeigt: „Orchestrierung ist fehlgeschlagen.“ `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Ursache	Es wurde das falsche Passwort für `deploy_admin` in `nwsetup-tui` eingegeben.
Lösung	Rufen Sie Ihr Passwort für `deploy_admin` ab. 1. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` Stellen Sie über SSH eine Verbindung mit dem fehlgeschlagenen Host her. 2. Führen Sie `nwsetup-tui` erneut mit dem korrekten Passwort für `deploy_admin` aus.

Fehlermeldung	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Ursache	NetWitness Platform erkennt den Servicemanagement-Service (SMS) nach einem erfolgreichen Upgrade als „down“, obwohl der Service ausgeführt wird.
Lösung	Starten Sie den SMS-Service neu. `systemctl restart rsa-sms`

Fehlermeldung	Sie erhalten die Aufforderung, den Host nach dem Update offline neu zu starten. 
Ursache	Sie können nicht die CLI zum Neustarten des Hosts verwenden. Sie müssen die Benutzeroberfläche verwenden.
Lösung	Starten Sie den Host in der Hostansicht der Benutzeroberfläche neu.

Backup (`nw-backup`-Skript)

Fehlermeldung	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Ursache	Das ESA Mongo-Admin-Passwort enthält Sonderzeichen (z. B. "! @# $% ^ qwertz').
Lösung	Ändern Sie das ESA Mongo-Admin-Passwort zurück auf den ursprünglichen Standardwert „netwitness“, bevor Sie das Backup ausführen.

Fehler	Backupfehler aufgrund der Einstellung des Attributs `immutable`. Hier ist ein Beispiel für einen Fehler, der angezeigt werden kann: 
Ursache	Wenn Sie Dateien haben, bei denen das Flag „unveränderlich“ eingestellt ist (um zu verhindern, dass der Puppet-Prozess eine angepasste Datei überschreibt), wird die Datei nicht in den Backupprozess einbezogen und es wird ein Fehler generiert.
Lösung	Führen Sie auf dem Host, der die Dateien mit gesetztem Flag „unveränderlich“ enthält, folgenden Befehl aus, um die Einstellung „unveränderlich“ aus den Dateien zu entfernen: `chattr -i <filename>`

Fehler	Fehler beim Erstellen der Datei mit Netzwerkkonfigurationsinformationen aufgrund von doppelten oder ungültigen Einträgen in primärer Netzwerkkonfigurationsdatei: `/etc/sysconfig/network-scripts/ifcfg-em1` Überprüfen Sie den Inhalt von `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Ursache	Es gibt falsche oder doppelte Einträge für jedes der folgenden Felder: DEVICE, BOOTPROTO, IPADDR, NETMASK oder GATEWAY, die beim Lesen der primären Ethernet-Schnittstellenkonfigurationsdatei des zu sichernden Host gefunden wurden.

Lösung	Erstellen Sie manuell eine Datei am Backupspeicherort auf dem externen Backupserver sowie am lokalen Backupspeicherort des Rechners, auf dem andere Backups bereitgestellt wurden. Der Dateiname muss das Format `<hostname>-<hostip>-network.info.txt` haben und die folgenden Einträge enthalten:
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problem	Der ESA-Service stürzt nach dem Upgrade auf 11.2.0.0 aus einem Setup mit FIPS-Aktivierung ab.
Ursache	Der ESA-Service verweist auf einen ungültigen Keystore.

Lösung	1. Stellen Sie über SSH eine Verbindung mit dem ESA Primary-Host her und melden Sie sich an.
	2. Ersetzen Sie in Datei `/opt/rsa/esa/conf/wrapper.conf` die folgende Zeile:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	durch:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Geben Sie den folgenden Befehl ein, um ESA neu zu starten:
	`systemctl restart rsa-nw-esa-server`
	Hinweis: Wenn Sie über mehrere ESA-Hosts verfügen, auf denen dasselbe Problem auftritt, wiederholen Sie die Schritte 1 bis 3 inklusive auf jedem sekundären ESA-Host.

Log Collector-Service (`nwlogcollector`)

Log Collector-Protokolle werden an `/var/log/install/nwlogcollector_install.log` auf dem Host, auf dem der `nwlogcollector` -Service ausgeführt wird, gesendet.

Fehlermeldung	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Ursache	Die Log Collector Lockbox konnte nach der Aktualisierung nicht geöffnet werden.
Lösung	Melden Sie sich bei NetWitness Platform an und setzen Sie den Systemfingerabdruck zurück, indem Sie das Passwort für den Systemstabilitätswert der Lockbox zurücksetzen, wie im Thema „Zurücksetzen des Systemstabilitätswerts“ unter „Konfigurieren von Lockbox-Sicherheitseinstellungen“ im *Protokollsammlung-Konfigurationsleitfaden* beschrieben. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Fehlermeldung	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Ursache	Die Log Collector Lockbox wird nach der Aktualisierung nicht konfiguriert.
Lösung	Wenn Sie eine Log Collector Lockbox verwenden, melden Sie sich bei NetWitness Platform an und konfigurieren die Lockbox wie im Thema „Konfigurieren von Lockbox-Sicherheitseinstellungen“ im *Protokollsammlung-Konfigurationsleitfaden* beschrieben. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Fehlermeldung	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Ursache	Sie müssen das Feld für den Schwellenwert des Stabilitätswerts für die Log Collector Lockbox zurücksetzen.
Lösung	Melden Sie sich bei NetWitness Platform an und setzen Sie das Passwort für den Systemstabilitätswert der Lockbox zurück, wie im Thema „Zurücksetzen des Systemstabilitätswerts“ unter „Konfigurieren von Lockbox-Sicherheitseinstellungen“ im *Protokollsammlung-Konfigurationsleitfaden* beschrieben. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Problem	Sie haben einen Log Collector für das Upgrade vorbereitet und möchten kein Upgrade mehr durchführen.
Ursache	Verzögerungen beim Upgrade.
Lösung	Verwenden Sie die folgende Befehlszeichenfolge, um einen Log Collector, der für ein Upgrade vorbereitet wurde, in den normalen Betrieb zurückzusetzen. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW-Server

Diese Protokolle werden an `/var/netwitness/uax/logs/sa.log` auf dem NW-Serverhost gesendet.

Problem	Nach dem Upgrade bemerken Sie, dass Auditprotokolle nicht zur konfigurierten globalen Audit-Einrichtung weitergeleitet werden oder Die folgende Meldung, angezeigt in `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Ursache	Die globale Audit-Einrichtung des NW-Servers konnte nicht von Version 10.6.6.x auf 11.2.0.0 migriert werden.
Lösung	1. Stellen Sie über SSH eine Verbindung mit dem NW-Server her. 2. Senden Sie den folgenden Befehl: `orchestration-cli-client --update-admin-node`

Orchestrierung

Die Protokolle des Orchestrierungsservers werden an `/var/log/netwitness/orchestration-server/orchestration-server.log` auf dem NW-Serverhost gesendet.

Problem	1. Es wurde erfolglos versucht, ein Upgrade für einen Nicht-NW-Serverhost durchzuführen. 2. Das Upgrade für diesen Host wurde erneut gestartet und war wieder erfolglos. Die folgende Meldung wird im `orchestration-server.log` angezeigt. `"'file' _virtual_ returned False: cannot import name HASHES""`
Ursache	Es wurde eventuell ein Upgrade für Salt Minion durchgeführt und Salt Minion wurde auf dem fehlerhaften Nicht-NW-Serverhost nicht neu gestartet.

Lösung	1. Stellen Sie über SSH eine Verbindung zu dem Nicht-NW-Serverhost her, bei dem das Upgrade fehlgeschlagen ist.
	2. Senden Sie die folgenden Befehle.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Versuchen Sie das Upgrade des Nicht-NW-Serverhosts erneut.

Reporting Engine-Service

Reporting Engine-Aktualisierungsprotokolle werden an die Datei `/var/log/re_install.log` auf dem Host übermittelt, auf dem der Reporting Engine-Service ausgeführt wird.

Fehlermeldung	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Ursache	Die Aktualisierung der Reporting Engine ist fehlgeschlagen, da Sie nicht über ausreichend Speicherplatzverfügen.
Lösung	Geben Sie Festplattenspeicherplatz frei, um den in der Protokollmeldung angezeigten erforderlichen Speicherplatz bereitzustellen. Anweisungen zum Freigeben von Festplattenspeicherplatz finden Sie unter „Hinzufügen von zusätzlichem Speicherplatz für große Berichte“ im *Reporting Engine-Konfigurationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

NetWitness UEBA

Problem	Die Benutzeroberfläche lässt sich nicht aufrufen.
Ursache	Es ist mehr als ein NetWitness UEBA-Service in Ihrer NetWitness-Bereitstellung vorhanden, es ist aber nur ein NetWitness UEBA-Service zulässig.

Lösung	Füllen Sie die folgenden Schritte aus, um den überflüssigen NetWitness UEBA-Service zu entfernen.
	1. Stellen Sie über SSH eine Verbindung zum NW-Server her und führen Sie die folgenden Befehle aus, um die Liste der installierten NetWitness UEBA-Services abzufragen.
	`# orchestration-cli-client --list-services|grep presidio-airflow`
	`... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`
	`... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`
	2. Ermitteln Sie in der Liste der Services, welche Instanz des `presidio-airflow`-Services entfernt werden soll (mithilfe der Hostadressen).
	3. Führen Sie den folgenden Befehl aus, um den überflüssigen Service aus der Orchestrierung zu entfernen (verwenden Sie dazu die zugehörige Service-ID aus der Liste der Services):
	`# orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output>`
	4. Führen Sie den folgenden Befehl aus, um den Node 0 zu aktualisieren, um NGINX wiederherzustellen:
	`# orchestration-cli-client --update-admin-node`
	5. Melden Sie sich bei NetWitness Platform an, gehen Sie zu **ADMIN** > **Hosts** und entfernen Sie den überflüssigen NetWitness UEBA-Host.

Anhang B: Erstellen eines externen Repository

Führen Sie das folgende Verfahren aus, um ein externes Repository (Repo) einzurichten.

1. Melden Sie sich bei dem Webserverhost an.
2. Erstellen Sie das Verzeichnis `ziprepo`, um das NW-Repository (`netwitness-11.2.0.0.zip`) unter `web-root` des Webservers zu hosten. Wenn `/var/netwitness` beispielsweise der Webstamm ist, senden Sie die folgende Befehlszeichenfolge.
   `mkdir /var/netwitness/ziprepo`
3. Erstellen Sie das Verzeichnis 11.2.0.0 unter `/var/netwitness/ziprepo`.
   `mkdir /var/netwitness/ziprepo/11.2.0.0`
4. Erstellen Sie die Verzeichnisse `OS` und `RSA` unter `/var/netwitness/ziprepo/11.2.0.0`.
   `mkdir /var/netwitness/ziprepo/11.2.0.0/OS`
   `mkdir /var/netwitness/ziprepo/11.2.0.0/RSA`
5. Entpacken Sie die Datei `netwitness-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/ziprepo/11.2.0.0`.
   `unzip netwitness-11.2.0.0.zip -d /var/netwitness/ziprepo/11.2.0.0`
   Durch das Entpacken von `netwitness-11.2.0.0.zip` entstehen zwei Zip-Dateien (`OS-11.2.0.0.zip` und `RSA-11.2.0.0.zip`) und einige andere Dateien.
6. Entpacken Sie die Datei:
   a. `OS-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/ziprepo/11.2.0.0/OS`.
      `unzip /var/netwitness/ziprepo/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/ziprepo/11.2.0.0/OS`

Parent Directory		-
GeoIP-1.5.0-11.el7.x86_64.rpm	20-Nov-2016 12:49	1.1M
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 10:07	4.6M
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 10:05	1.5M
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	502K
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	15K
PyYAML-3.11-1.el7.x86_64.rpm	19-Dec-2017 12:30	160K
SDL-1.2.15-14.el7.x86_64.rpm	25-Nov-2015 10:39	204K
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 10:04	81K
adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm	13-Feb-2018 05:10	706K
alsa-lib-1.1.3-3.el7.x86_64.rpm	10-Aug-2017 10:52	421K
at-3.1.13-22.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	51K
atk-2.22.0-3.el7.x86_64.rpm	10-Aug-2017 10:53	258K
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 10:04	66K

   b. `RSA-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/ziprepo/11.2.0.0/RSA`.
      `unzip /var/netwitness/ziprepo/11.2.0.0/RSA-11.2.0.0.zip -d`

```
/var/netwitness/ziprepo/11.2.0.0/RSA
```

Parent Directory	-
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07 1.2M
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07 173K
bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03 203K
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07 52K
cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14 85K
device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56 134K
dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36 277K
elasticsearch-5.6.9.rpm	17-Apr-2018 09:37 32M
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07 17K
fneserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11 1.3M
htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23 102K
i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08 399K
ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41 441K
iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20 51K
ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08 374K

Der externe URL für das Repository ist `http://<web server IP address>/ziprepo`.

7. Verwenden Sie die `http://<web server IP address>/ziprepo` als Antwort auf die Eingabeaufforderung **Geben Sie den Basis-URL des externen Update-Repository ein** des NW 11.2 Setup-Programms (nwsetup-tui).

Revisionsverlauf

Version	Datum	Beschreibung	Verfasser
1,0	15. August 2018	Betriebsfreigabe	IDD

1.1	24. Sept. 2018	Aktualisierte UEBA-Konfigurationsskript-Befehlszeichenfolge in den Aufgaben nach der Installation, um Verwirrung zu vermeiden und die `.sh` Erweiterung aus dem Skript zu entfernen.
		Falsche Befehlszeichenfolge:
		`./ueba-server-config.sh -u <user> -p <password> -h <host> -o <type> -t <startTime> -s <schemas> -v`
		Überarbeitete Befehlszeichenfolge:
		`/opt/rsa/saTools/ueba-server-config -u <user> -p <password> -h <host> -o <type> -t <startTime> -s <schemas> -v`
			IDD

1.2	10-Okt-18	Es wurden verschiedene Änderungen an "Aufgabe 4: Installieren von NetWitness UEBA" unter den Aufgaben nach der Installation vorgenommen (sieheSADOCS-1592).	IDD
1.3	11-Okt-18	Das Thema zur Konfiguration von externem angeschlossenen Speicher für SADOCS-1597 wurde hinzugefügt.	IDD
1.4	29. November 2018	Es wurde ein Hinweis zur UEBA-Trail-Lizenzierung hinzugefügt.	IDD