



Handbuch zur Installation virtueller Hosts

für Version 11.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell 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 Dell 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

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

Leitfaden zur Einrichtung von virtuellen Hosts	5
Grundlegende virtuelle Bereitstellungen	6
Im Leitfaden für die virtuelle Bereitstellung verwendete Abkürzungen	6
Unterstützte virtuelle Hosts	7
Installationsmedien	7
Empfehlungen zur virtuellen Umgebung	7
Empfohlene Systemanforderungen für virtuelle Hosts	8
Szenario 1	8
Szenario 2	10
Szenario 3	13
Szenario 4	15
Richtlinien zur Dimensionierung von Legacy-Windows-Collectors	15
Installieren des virtuellen NetWitness Platform-Hosts in einer virtuellen Umgebung	17
Voraussetzungen	17
Schritt 1. Bereitstellen des virtuellen Hosts zum Erstellen der VM	17
Voraussetzungen	17
Verfahren	17
Schritt 2. Konfigurieren des Netzwerks	21
Voraussetzungen	21
Verfahren	21
Überprüfen von offenen Firewallports	21
Schritt 3. Konfigurieren der Datenbanken zur Unterstützung von NetWitness Platform	21
Aufgabe 1. Überprüfen der Datenspeicher-Erstkonfiguration	22
Anfänglich der PacketDB zugewiesener Speicherplatz	22
Ursprüngliche Datenbankgröße	22
PacketDB-Mount-Punkt	23
Aufgabe 2. Überprüfen der optimalen Speicherplatzkonfiguration des Datenspeichers	24
Speicherplatzverhältnisse auf virtuellen Laufwerken	25
Aufgabe 3: Hinzufügen eines neuen Volume und Erweitern von vorhandenen Dateisystemen	26
AdminServer	29
ESAPrimary/ESASSecondary/Malware	30
LogCollector	30
LogDecoder	30
Concentrator	32

Archiver	34
Decoder	35
Installieren von RSA NetWitness Platform	37
Schritt 4. Konfigurieren von hostspezifischen Parametern	54
Konfigurieren der Protokollaufnahme in der virtuellen Umgebung	54
Konfigurieren der Paketerfassung in der virtuellen Umgebung	55
Verwenden eines Virtual Tap eines Drittanbieters	55
Schritt 5. Aufgaben nach der Installation	56
Allgemein	56
RSA NetWitness Endpoint Insights	56
FIPS-Aktivierung	58
NetWitness Analyse des Nutzer- und Entitätsverhaltens (UEBA)	59
Anhang A: Troubleshooting	65
CLI (Command Line Interface)	66
Backup (nw-backup-Skript)	67
Event Stream Analysis	69
Log Collector-Service (nwlogcollector)	70
NW-Server	72
Orchestrierung	72
Reporting Engine-Service	73
NetWitness UEBA	74
Anhang B: Erstellen eines externen Repository	75
Revisionsverlauf	77

Leitfaden zur Einrichtung von virtuellen Hosts

Dieses Dokument enthält Anweisungen für die Installation und Konfiguration von RSA NetWitness® Platform 11.2.0.0-Hosts, die in einer virtuellen Umgebung ausgeführt werden.

Grundlegende virtuelle Bereitstellungen

Dieses Thema enthält allgemeine Guidelines und Anforderungen für die Bereitstellung von RSA NetWitness Platform 11.2.0.0 in einer virtuellen Umgebung.

Im Leitfaden für die virtuelle Bereitstellung verwendete Abkürzungen

Abkürzungen	Beschreibung
CPU	Zentrale Verarbeitungseinheit (Central Processing Unit)
EPS	Ereignisse pro Sekunde
VMware ESX	Typ-1-Hypervisor der Enterprise-Klasse, unterstützte Versionen: 6.5, 6.0 und 5.5
GB	Gigabyte. 1 GB = 1.000.000.000 Byte
Gbit	Gigabit. 1 Gbit = 1.000.000.000 Bit.
Gbit/s	Gigabit pro Sekunde oder Milliarden Bit pro Sekunde. Maßeinheit für die Bandbreite eines digitalen Datenübertragungsmediums, z. B. Glasfaser.
GHz	Gigahertz. 1 GHz = 1.000.000.000 Hz
IOPS	Eingabe-/Ausgabevorgänge pro Sekunde (Input/Output Operations per Second).
Mbit/s	Megabit pro Sekunde oder Millionen Bit pro Sekunde. Maßeinheit für die Bandbreite eines digitalen Datenübertragungsmediums, z. B. Glasfaser.
NAS	Network Attached Storage
OVF	Open Virtualization Format
OVA	Open Virtual Appliance In diesem Handbuch steht OVA für Open Virtual Host.
RAM	Random Access Memory (auch als Arbeitsspeicher bezeichnet)
SAN	Storage Area Network
SSD/EFD HDD	Solid-State-Laufwerk/Enterprise-Flash-Laufwerk-Festplatte
SCSI	Small Computer System Interface
SCSI (SAS)	Serielles Punkt-zu-Punkt-Protokoll, über das Daten zu und von Computerspeichergeräten wie Festplatten und Bandlaufwerken verschoben werden.
vCPU	Virtual Central Processing Unit (auch als virtueller Prozessor bezeichnet)
vRAM	Virtual Random Access Memory (auch als virtueller Arbeitsspeicher bezeichnet)
RSA NetWitness UEBA	RSA NetWitness Analyse des Nutzer- und Entitätsverhaltens

Unterstützte virtuelle Hosts

Sie können die folgenden NetWitness Platform-Hosts in Ihrer virtuellen Umgebung als virtuelle Hosts installieren und von Ihrer virtuellen Umgebung bereitgestellte Funktionen übernehmen:

- NetWitness Server
- Event Stream Analysis – primärer und sekundärer ESA-Host
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Endpoint Hybrid
- Endpoint Log Hybrid
- Analyse des Nutzer- und Entitätsverhaltens (UEBA)

Sie sollten mit den folgenden VMware-Infrastrukturkonzepten vertraut sein:

- VMware vCenter Server
- VMware ESXi
- Virtuelle Maschine

Informationen über VMware-Konzepte können Sie der VMware-Produktdokumentation entnehmen.

Virtuelle Hosts werden als OVA-Host bereitgestellt. Sie müssen die OVA-Datei in Ihrer virtuellen Infrastruktur als virtuelle Maschine bereitstellen.

Installationsmedien

Installationsmedien stehen in Form von OVA-Paketen zur Verfügung. Diese können in Download Central (<https://download.rsasecurity.com>) zur Installation heruntergeladen werden. Im Rahmen der Erfüllung Ihrer Bestellung erhalten Sie von RSA Zugriff auf die OVA.

Empfehlungen zur virtuellen Umgebung

Die mit den OVA-Paketen installierten virtuellen Hosts haben dieselbe Funktion wie die NetWitness Platform-Hardwarehosts. Das bedeutet, dass Sie bei der Installation von virtuellen Hosts die Back-end-Hardware berücksichtigen müssen. RSA empfiehlt, die folgenden Aufgaben bei der Einrichtung Ihrer virtuellen Umgebung durchzuführen.

- Gehen Sie je nach Ressourcenanforderungen der einzelnen Komponenten bei der Nutzung des Systems gemäß bewährten Vorgehensweisen vor und weisen Sie Speicherplatz entsprechend zu.
- Vergewissern Sie sich, dass die Festplattenkonfigurationen des Back-end eine Schreibgeschwindigkeit aufweisen, die um mindestens 10 % über der erforderlichen Erfassungs- und Verarbeitungsrate für die Bereitstellung liegt.
- Erstellen Sie Concentrator-Verzeichnisse für Meta- und Indexdatenbanken auf der SSD/EFD HDD.
- Wenn die Datenbankkomponenten getrennt von den installierten Betriebssystemkomponenten sind (d. h. auf einem anderen physischen System), stellen Sie wie folgt eine direkte Verbindung her über:
 - Zwei 8-Gbit/s-Fibre-Channel-SAN-Ports pro virtuellem Host, oder
 - 6-Gbit/s-SAS-Verbindung (Serial Attached SCSI)

Hinweis: 1.) NetWitness Platform unterstützt derzeit keinen Network Attached Storage (NAS) für virtuelle Bereitstellungen.
 2.) Der Decoder ermöglicht jede Speicherkonfiguration, die die Anforderung für kontinuierlichen Durchsatz erfüllt. Der standardmäßige 8-Gbit/s-Fibre-Channel-Link zu einer SAN ist nicht ausreichend, um Paketdaten bei 10 Gbit/s zu lesen und zu schreiben. Bei der Konfiguration der Verbindung von einem **10G-Decoder** zu einem SAN müssen Sie mehrere Fibre Channels verwenden.

Empfohlene Systemanforderungen für virtuelle Hosts

Die folgenden Tabellen enthalten die empfohlenen Anforderungen bezüglich vCPUs, vRAM und Lese- und Schreib-IOPS für virtuelle Hosts basierend auf der EPS- oder Erfassungsrate für jede Komponente.

- Die Speicherzuweisung wird in Schritt 3 „Konfigurieren von Datenbanken für NetWitness Platform“ behandelt.
- Die Empfehlungen bezüglich vRAM und vCPU können je nach Erfassungsraten, Konfiguration und aktivierten Inhalten variieren.
- Die Empfehlungen wurden bei Datenaufnahmeraten von bis zu 25.000 EPS für Protokolle und 2 Gbit/s für Pakete getestet, Nicht-SSL betreffend.
- Die vCPU-Spezifikationen für alle in den folgenden Tabellen aufgeführte Komponenten sind Intel Xeon CPUs mit 2,59 GHz.
- Alle Ports sind SSL-getestet mit 15.000 EPS für Protokolle und 1,5 Gbit/s für Pakete.

Hinweis: Die oben genannten empfohlenen Werte können bei einer 11.2.0.0-Installation anders ausfallen, wenn Sie die neuen Funktionen und Verbesserungen installieren und ausprobieren.

Szenario 1

Die Anforderungen in diesen Tabellen wurden unter den folgenden Umständen berechnet:

- Alle Komponenten wurden integriert.
- Der Protokollstream umfasste einen Log Decoder, Concentrator und Archiver.
- Der Paketstream umfasste einen Netzwerk-Decoder und Concentrator.
- Die Hintergrundlast enthielt stündliche und tägliche Berichte.
- Diagramme wurden konfiguriert.

Log Decoder

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
2.500	6 oder 15,60 GHz	32 GB	50	75
5.000	8 oder 20,79 GHz	32 GB	100	100
7.500	10 oder 25,99 GHz	32 GB	150	150

Network Decoder

Mbit/s	CPU	Speicher	Lese-IOPS	Schreib-IOPS
50	4 oder 10,39 GHz	32 GB	50	150
100	4 oder 10,39 GHz	32 GB	50	250
250	4 oder 10,39 GHz	32 GB	50	350

Concentrator – Protokollstream

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
2.500	4 oder 10,39 GHz	32 GB	300	1.800
5.000	4 oder 10,39 GHz	32 GB	400	2.350
7.500	6 oder 15,59 GHz	32 GB	500	4.500

Concentrator – Paketstream

Mbit/s	CPU	Speicher	Lese-IOPS	Schreib-IOPS
50	4 oder 10,39 GHz	32 GB	50	1.350
100	4 oder 10,39 GHz	32 GB	100	1.700
250	4 oder 10,39 GHz	32 GB	150	2.100

Archiver

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
2.500	4 oder 10,39 GHz	32 GB	150	250
5.000	4 oder 10,39 GHz	32 GB	150	250
7.500	6 oder 15,59 GHz	32 GB	150	350

Szenario 2

Die Anforderungen in diesen Tabellen wurden unter den folgenden Umständen berechnet:

- Alle Komponenten wurden integriert.
- Der Protokollstream umfasste einen Log Decoder, Concentrator, Warehouse Connector und Archiver.
- Der Paketstream umfasste einen Netzwerk-Decoder, Concentrator und Warehouse Connector.
- Event Stream Analysis wurde bei 90.000 EPS von drei Hybrid Concentrators aggregiert.
- Respond erhielt Warnmeldungen von der Reporting Engine und von Event Stream Analysis.
- Die Hintergrundlast umfasste Berichte, Diagramme, Warnmeldungen, Ermittlungen und Respond.
- Warnmeldungen wurden konfiguriert.

Log Decoder

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
10.000	16 oder 41,58 GHz	50 GB	300	50
15.000	20 oder 51,98 GHz	60 GB	550	100

Network Decoder

Mbit/s	CPU	Speicher	Lese-IOPS	Schreib-IOPS
500	8 oder 20,79 GHz	40 GB	150	200
1.000	12 oder 31,18 GB	50 GB	200	400
1.500	16 oder 41,58 GHz	75 GB	200	500

Concentrator – Protokollstream

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
10.000	10 oder 25,99 GHz	50 GB	1.550+50	6.500
15.000	12 oder 31,18 GHz	60 GB	1.200+400	7.600

Concentrator – Paketstream

Mbit/s	CPU	Speicher	Lese-IOPS	Schreib-IOPS
500	12 oder 31,18 GHz	50 GB	250	4.600
1.000	16 oder 41,58 GHz	50 GB	550	5.500
1.500	24 oder 62,38 GHz	75 GB	1.050	6.500

Warehouse Connector – Protokollstream

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
10.000	8 oder 20,79 GHz	30 GB	50	50
15.000	10 oder 25,99 GHz	35 GB	50	50

Warehouse Connector – Paketstream

Mbit/s	CPU	Speicher	Lese-IOPS	Schreib-IOPS
500	6 oder 15,59 GHz	32 GB	50	50
1.000	6 oder 15,59 GHz	32 GB	50	50
1.500	8 oder 20,79 GHz	40 GB	50	50

Archiver – Protokollstream

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
10.000	12 oder 31,18 GHz	40 GB	1.300	700
15.000	14 oder 36,38 GHz	45 GB	1.200	900

Event Stream Analysis mit Context Hub

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
90.000	32 oder 83,16 GHz	94 GB	50	50

NWS1: NetWitness-Server und Komponenten am selben Standort

NetWitness Server, Jetty, Broker, Respond und Reporting Engine befinden sich im gleichen Verzeichnis.

CPU	Speicher	Lese-IOPS	Schreib-IOPS
12 oder 31,18 GHz	50 GB	100	350

Szenario 3

Die Anforderungen in diesen Tabellen wurden unter den folgenden Umständen berechnet:

- Alle Komponenten wurden integriert.
- Der Protokollstream umfasste einen Log Decoder und Concentrator.
- Der Paketstream umfasste einen Netzwerk-Decoder und den Concentrator.
- Event Stream Analysis wurde bei 90.000 EPS von drei Hybrid Concentrators aggregiert.
- Respond erhielt Warnmeldungen von der Reporting Engine und von Event Stream Analysis.
- Die Hintergrundlast enthielt stündliche und tägliche Berichte.
- Diagramme wurden konfiguriert.

Log Decoder

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
25.000	32 oder 83,16 GHz	75 GB	250	150

Network Decoder

Mbit/s	CPU	Speicher	Lese-IOPS	Schreib-IOPS
2.000	16 oder 41,58 GHz	75 GB	50	650

Concentrator – Protokollstream

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
25.000	16 oder 41,58 GHz	75 GB	650	9.200

Concentrator – Paketstream

Mbit/s	CPU	Speicher	Lese-IOPS	Schreib-IOPS
2.000	24 oder 62,38 GHz	75 GB	150	7.050

Log Collector (lokal und remote)

Der Remote Log Collector ist ein Log Collector-Service, der auf einem Remote-Host ausgeführt wird, und der Remote-Collector wird virtuell bereitgestellt.

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
15.000	8 oder 20,79 GHz	8 GB	50	50
30.000	8 oder 20,79 GHz	15 GB	100	100

Szenario 4

Die Anforderungen in diesen Tabellen wurden unter den folgenden Bedingungen für Endpoint Hybrid berechnet.

- Alle Komponenten wurden integriert.
- Endpoint-Server ist installiert.
- Der Protokollstream umfasste einen Log Decoder und Concentrator.

Endpoint Hybrid

Agents	CPU	Speicher	IOPS-Werte		
			Lese-IOPS	Schreib-IOPS	
5000	16 oder 42 GHz	32 GB			
			Log Decoder	250	150
			Concentrator	150	7.050
			MongoDB	250	150

Log Collector (lokal und remote)

Der Remote Log Collector ist ein Log Collector-Service, der auf einem Remote-Host ausgeführt wird, und der Remote-Collector wird virtuell bereitgestellt.

EPS	CPU	Speicher	Lese-IOPS	Schreib-IOPS
15.000	8 oder 20,79 GHz	8 GB	50	50
30.000	8 oder 20,79 GHz	15 GB	100	100

Richtlinien zur Dimensionierung von Legacy-Windows-Collectors

Richtlinien zur Dimensionierung von Legacy-Windows-Collectors finden Sie in der Dokumentation *RSA NetWitness Platform Legacy Windows Collection – Aktualisierung und Installation*.

UEBA

CPU	Speicher	Lese-IOPS	Schreib-IOPS
16 oder 2,4 GHz	64 GB	500	500

Hinweis: RSA empfiehlt, UEBA nur dann auf einem virtuellen Host bereitzustellen, wenn Ihr Protokollsammlungsvolumen gering ist. Wenn Sie ein moderates bis hohes Protokollsammlungsvolumen haben, empfiehlt RSA, UEBA auf dem physischen Host bereitzustellen, der unter „RSA NetWitness UEBA – Hosthardwarespezifikationen“ im Handbuch zur Installation physischer Hosts beschrieben wird. Wenden Sie sich an den Kundensupport (<https://community.rsa.com/docs/DOC-1294>) für Empfehlungen dazu, welcher Host für UEBA verwendet werden soll, virtuell oder physisch.

Installieren des virtuellen NetWitness Platform-Hosts in einer virtuellen Umgebung

Schließen Sie die folgenden Verfahren in der nummerierten Reihenfolge ab, um RSA NetWitness® Platform in einer virtuellen Umgebung zu installieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Folgendes verfügen:

- Einen VMware-ESX-Server, der die im Abschnitt oben genannten Anforderungen erfüllt. Unterstützte Versionen sind 6.5, 6.0 und 5.5.
- vSphere 4.1-Client, vSphere 5.0-Client oder vSphere 6.0-Client, um sich beim VMware-ESX-Server anzumelden.
- Administratorrechte zum Erstellen der virtuellen Maschinen im VMware-ESX-Server

Schritt 1. Bereitstellen des virtuellen Hosts zum Erstellen der VM

Schließen Sie die folgenden Schritte ab, um die OVA-Datei auf dem vCenter-Server oder ESX-Server mithilfe des vSphere-Clients bereitzustellen.

Voraussetzungen

Vergewissern Sie sich, dass Sie:

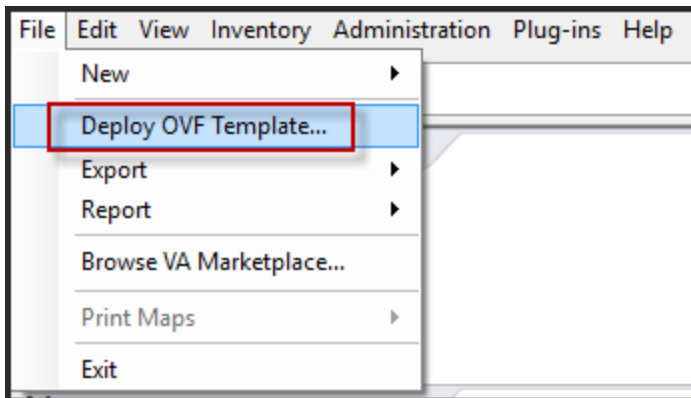
- Netzwerk-IP-Adressen, Netzmaske und Gateway-IP-Adressen für den virtuellen Host
- Netzwerknamen für alle virtuellen Hosts, wenn Sie ein Cluster erstellen
- DNS- oder Hostinformationen
- Passwort für den virtuellen Hostzugriff. Der Standardbenutzername lautet `root`, das Standardpasswort `netwitness`.
- Die Paketdatei für virtuelle Hosts für NetWitness Platform, z. B. `rsanw-11.2.0.xxxx.el7-x86_64.ova`. (Sie laden dieses Paket von Download Central unter <https://community.rsa.com> herunter.)

Verfahren

Hinweis: Die folgenden Anweisungen sind ein Beispiel für die Bereitstellung eines OVA-Hosts in der ESXi-Umgebung. Die Bildschirme, die Sie sehen, können von diesem Beispiel abweichen.

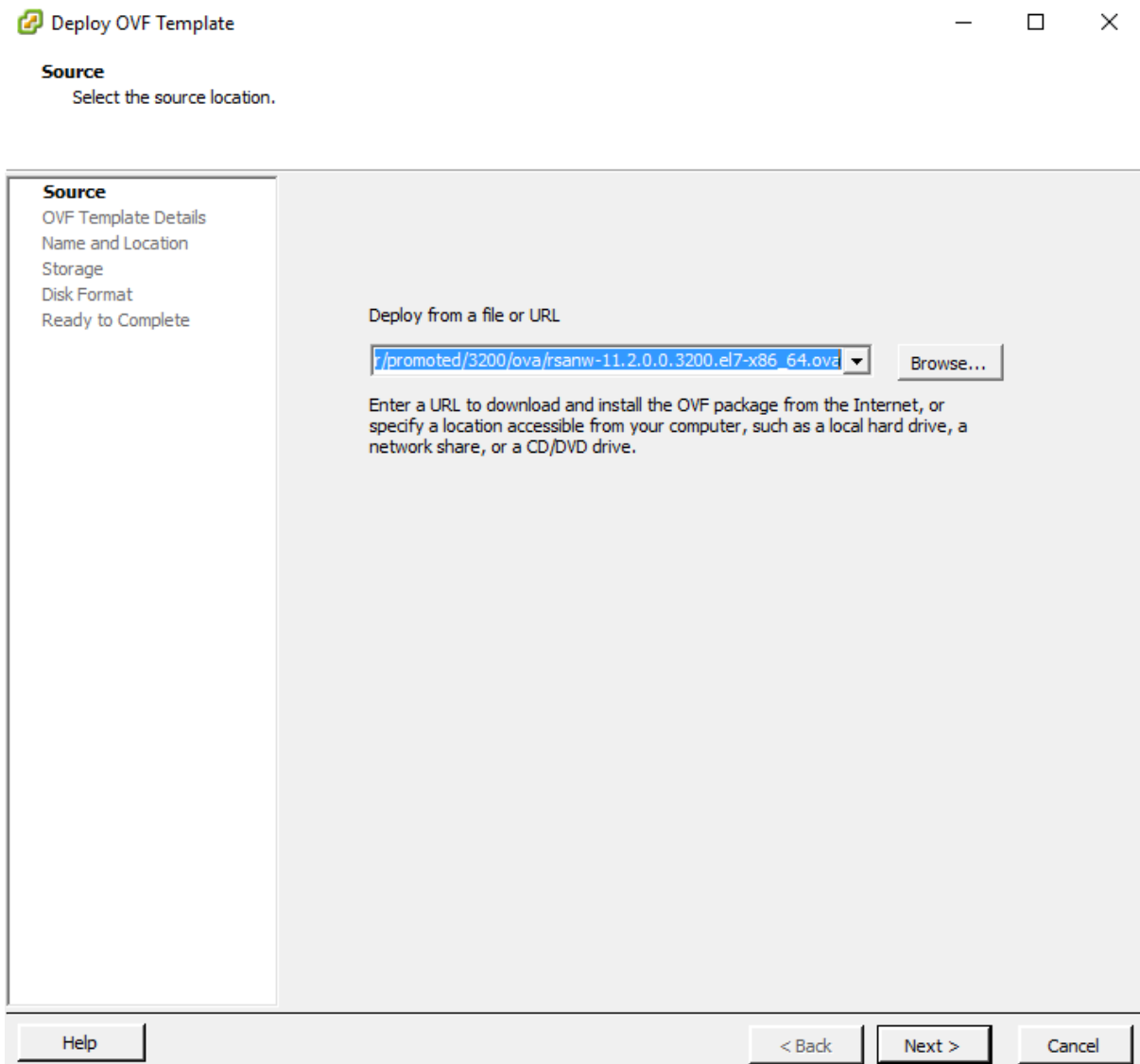
So stellen Sie den OVA-Host bereit:

1. Melden Sie sich bei der ESXi-Umgebung an.
2. Wählen Sie im Drop-down-Menü **Datei** die Option **OVF-Vorlage bereitstellen**.



3. Das Dialogfeld „OVF-Vorlage bereitstellen“ wird angezeigt. Wählen Sie im Dialogfeld **OVF-Vorlage bereitstellen** das OVF für den Host aus, den Sie in der virtuellen Umgebung bereitstellen

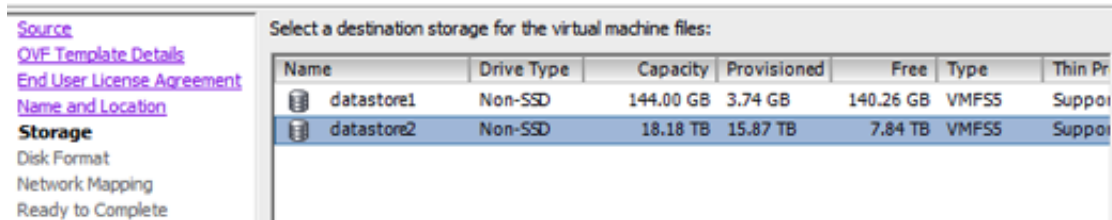
möchten (z. B. **V11.2 GOLD\rsanw-11.2.0.0.1948.el7-x86_64.ova**), und klicken Sie auf **Weiter**.



4. Das Dialogfeld „Name und Speicherort“ wird geöffnet. Der designierte Name gibt nicht den Hostnamen des Servers wieder. Der angezeigte Name ist als Bestandsreferenz innerhalb von ESXi nützlich.
5. Notieren Sie sich den Namen und klicken Sie auf **Weiter**. Die Speicheroptionen werden angezeigt.

Storage

Where do you want to store the virtual machine files?



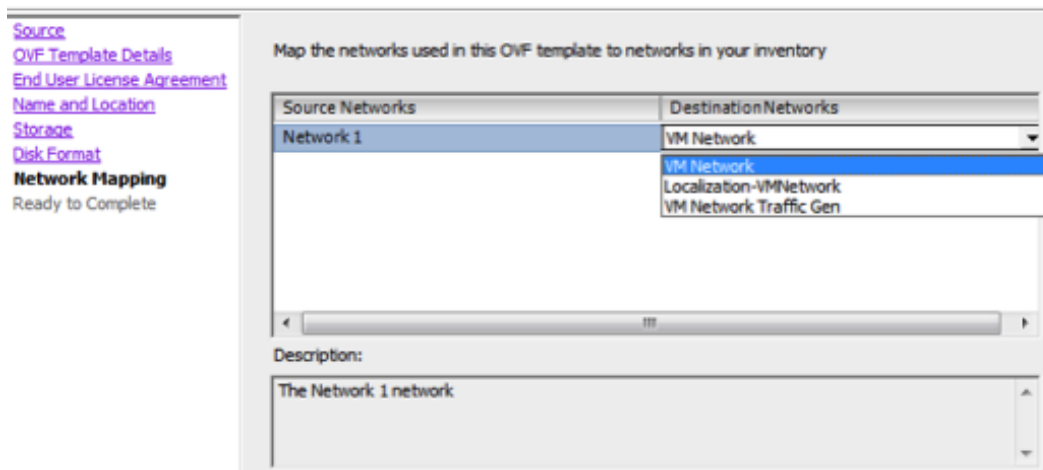
6. Geben Sie bei den Speicheroptionen den Datenspeicherort für den virtuellen Host an.

Hinweis: Dieser Speicherort gilt ausschließlich für das Hostbetriebssystem. Er muss nicht mit dem Datenspeicher identisch sein, der beim Einrichten und Konfigurieren von zusätzlichen Volumes für die NetWitness Platform-Datenbanken auf bestimmten Hosts benötigt wird (dies wird in den folgenden Abschnitten behandelt).

7. Klicken Sie auf **Weiter**.
Die Optionen für Netzwerkzuordnung werden eingeblendet.

Network Mapping

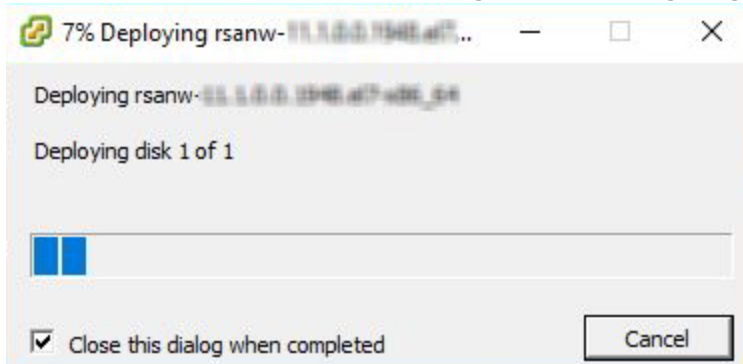
What networks should the deployed template use?



8. Behalten Sie die Standardwerte bei und klicken Sie auf **Weiter**.

Hinweis: Wenn Sie jetzt die Netzwerkzuordnung konfigurieren möchten, können Sie die Optionen auswählen. RSA empfiehlt jedoch, dass Sie die Standardwerte beibehalten und die Netzwerkzuordnung nach der Konfigurierung der OVA-Vorlage einrichten. Sie konfigurieren die OVA in [Schritt 4: Konfigurieren von hostspezifischen Parametern](#).

Ein Statusfenster mit dem Bereitstellungsstatus wird angezeigt.



Nach Abschluss des Prozesses wird die neue OVA-Datei im designierten Ressourcenpool aufgeführt, der auf ESXi innerhalb von vSphere sichtbar ist. Der virtuelle Core-Host ist dann installiert, aber noch nicht konfiguriert.

Schritt 2. Konfigurieren des Netzwerks

Schließen Sie die folgenden Schritte ab, um das Netzwerk der virtuellen Appliance zu konfigurieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie:

- Netzwerk-IP-Adressen, Netzmaske und Gateway-IP-Adressen für den virtuellen Host
- Netzwerknamen für alle virtuellen Hosts, wenn Sie ein Cluster erstellen
- DNS- oder Hostinformationen

Verfahren

Führen Sie die folgenden Schritte für alle virtuellen Hosts aus, um diese Ihrem Netzwerk hinzuzufügen.

Überprüfen von offenen Firewallports

Informieren Sie sich im Thema *Netzwerkarchitektur und Ports* im *Leitfaden zur Bereitstellung* der NetWitness Platform-Hilfe, um NetWitness Platform-Services und Ihre Firewalls zu konfigurieren. 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.

Schritt 3. Konfigurieren der Datenbanken zur Unterstützung von NetWitness Platform

Wenn Sie Datenbanken von OVA bereitstellen, reicht die erste Datenbankspeicherplatzzuordnung

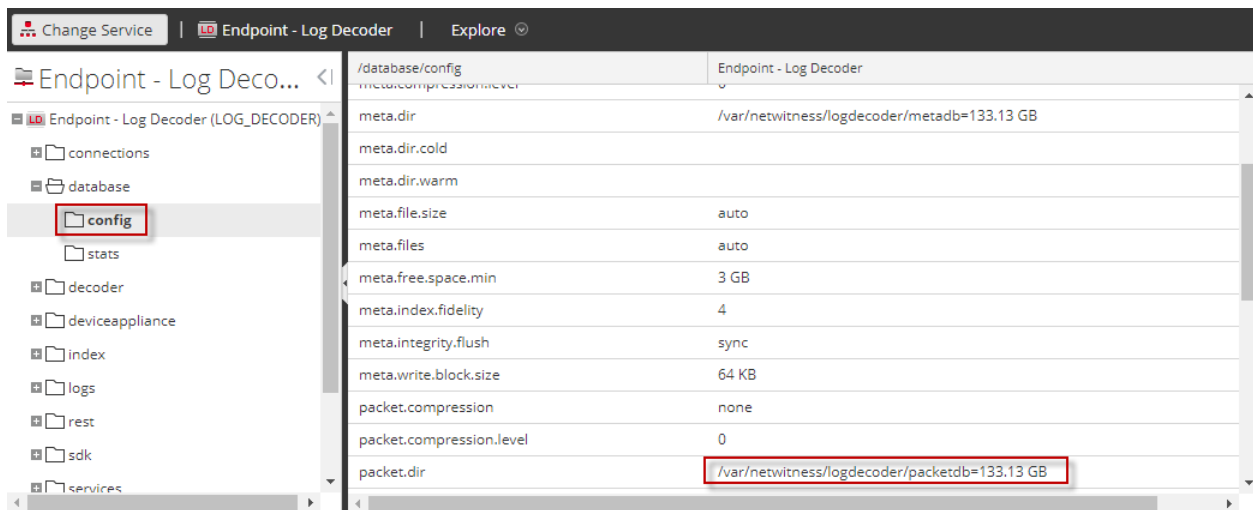
möglicherweise nicht aus, um NetWitness Server zu unterstützen. Sie müssen den Status der Datenspeicher nach der ersten Bereitstellung überprüfen und diese erweitern.

Aufgabe 1. Überprüfen der Datenspeicher-Erstkonfiguration

Überprüfen Sie die Konfiguration des Datenspeichers nach der erstmaligen Bereitstellung, um zu ermitteln, ob genügend Laufwerksspeicherplatz für die Anforderungen Ihres Unternehmens vorhanden ist. In diesem Thema wird beispielhaft die Datenspeicherkonfiguration der PacketDB auf dem Log Decoder-Host nach der ersten Bereitstellung aus einer OVA-Datei (Open Virtualization Archive) überprüft.

Anfänglich der PacketDB zugewiesener Speicherplatz

Der zugewiesene Speicherplatz für die PacketDB ist etwa 133,13 GB). Das folgende Beispiel für die NetWitness Platform-Ansicht „Durchsuchen“ zeigt die Größe der PacketDB, nachdem Sie diese anfänglich aus OVA bereitgestellt haben.



Ursprüngliche Datenbankgröße

Standardmäßig wird die Größe der Datenbank auf 95 % der Größe des Dateisystems festgelegt, auf dem sich die Datenbank befindet. Stellen Sie über SSH eine Verbindung mit dem Log Decoder her und geben Sie die Befehlszeichenfolge `df -k` ein, um das Dateisystem und seine Größe anzuzeigen. Die folgende Ausgabe ist ein Beispiel für die Informationen, die diese Befehlszeichenfolge zurückgibt.

```
[root@LogDecoder ~]# df -kh
Filesystem                Size      Used Avail Use% Mounted on
/dev/mapper/netwitness_vg00-root  30G    3.0G   27G  10% /
devtmpfs                  16G         0   16G   0% /dev
tmpfs                     16G     12K   16G   1% /dev/shm
tmpfs                     16G     25M   16G   1% /run
tmpfs                     16G         0   16G   0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome  10G    33M   10G   1% /home
/dev/mapper/netwitness_vg00-varlog   10G    42M   10G   1% /var/log
/dev/mapper/netwitness_vg00-nwhome  141G   396M  140G   1% /var/netwitness
/dev/sda1                 1014M    73M   942M   8% /boot
tmpfs                     3.2G         0   3.2G   0% /run/user/0
[root@LogDecoder ~]#
```

PacketDB-Mount-Punkt

Die Datenbank wird auf dem logischen Volume `packetdb` in Volume-Gruppe `netwitness_vg00` gemountet. `netwitness_vg00` hier beginnen Sie mit der Erweiterungsplanung für das Dateisystem.

Anfänglicher Status von `netwitness_vg00`

Führen Sie zum Überprüfen des Status von `netwitness_vg00` die folgenden Schritte aus.

1. Stellen Sie über SSH eine Verbindung zum Log Decoder-Host her.
2. Geben Sie die Befehlszeichenfolge `lvs` (logische Volumes anzeigen) ein, um festzustellen, welche logischen Volumes in `netwitness_vg00` zusammengefasst sind.

```
[root@nwappliance32431 ~]# lvs netwitness_vg00.
```

Die folgende Ausgabe ist ein Beispiel für die Informationen, die diese Befehlszeichenfolge zurückgibt.

```
[root@LogDecoder ~]# vgs
VG                #PV #LV #SN Attr   VSize   VFree
netwitness_vg00   1   5   0 wz--n- <194.31g 100.00m
```

3. Geben Sie die Befehlszeichenfolge `pvs` (physische Volumes anzeigen) ein, um zu ermitteln, welche physischen Volumes zu einer bestimmten Gruppe gehören.

```
[root@nwappliance32431 ~]# pvs
```

Die folgende Ausgabe ist ein Beispiel für die Informationen, die diese Befehlszeichenfolge zurückgibt.

```
[root@LogDecoder ~]# pvs
PV                VG                Fmt  Attr PSize   PFree
/dev/sda2         netwitness_vg00  lvm2 a--  <194.31g 100.00m
```

4. Geben Sie die Befehlszeichenfolge `vgs` (Volume-Gruppen anzeigen) ein, um die Gesamtgröße der jeweiligen Volume-Gruppe anzuzeigen.

```
[root@nwappliance32431 ~]# vgs
```

Die folgende Ausgabe ist ein Beispiel für die Informationen, die diese Befehlszeichenfolge zurückgibt.

```
[root@LogDecoder ~]# vgs
VG          #PV #LV #SN Attr   VSize   VFree
netwitness_vg00  1  5  0 wz--n- <194.31g 100.00m
```

Aufgabe 2. Überprüfen der optimalen Speicherplatzkonfiguration des Datenspeichers

Sie müssen die Optionen der Datenspeicher-Speicherplatzkonfiguration für die verschiedenen Hosts überprüfen, um eine optimale Performance Ihrer virtuellen NetWitness Platform-Bereitstellung zu erzielen. Datenspeicher sind für die virtuelle Hostkonfiguration erforderlich und die richtige Größe hängt vom Host ab.

Hinweis: (1.) Empfehlungen zur Optimierung des Datenspeicher-Speicherplatzes finden Sie im Thema **Optimierungstechniken** im [Tungleitfaden für die RSA NetWitness Platform-Core-Datenbank](#). (2.) Wenden Sie sich an die Kundenbetreuung, um Unterstützung beim Konfigurieren Ihrer virtuellen Laufwerke und Verwenden des Dimensionierungs- und Umfangsrechners zu erhalten.

Speicherplatzverhältnisse auf virtuellen Laufwerken

Die nachfolgende Tabelle enthält optimale Konfigurationen für Paket- und Protokollhosts. Weitere Partitionierungs- und Dimensionierungsbeispiele sowohl für Paketerfassungs- als auch Protokollaufnahmeumgebungen finden Sie am Ende dieses Themas.

Decoder			
Persistente Datenspeicher	Cachedatenspeicher		
PacketDB	SessionDB	MetaDB	Index
100 % wie vom Sizing & Scoping Calculator berechnet	6 GB pro 100 Mbit/s an Datenverkehr bei kontinuierlichem Durchsatz bieten 4 Stunden Cache	60 GB pro 100 Mbit/s an Datenverkehr bei kontinuierlichem Durchsatz bieten 4 Stunden Cache	3 GB pro 100 Mbit/s an Datenverkehr bei kontinuierlichem Durchsatz bieten 4 Stunden Cache

Concentrator		
Persistente Datenspeicher	Cachedatenspeicher	
MetaDB	SessionDB Index	Index
Berechnet als 10 % der PacketDB, die für ein Aufbewahrungsverhältnis von 1:1 erforderlich ist	30 GB per 1 TB der PacketDB für die Bereitstellung standardmäßiger Multiprotokollnetzwerke, wie bei typischen Internet-Gateways	5 % der berechneten MetaDB auf dem Concentrator. Bevorzugte Hochgeschwindigkeitsspindeln oder SSD für schnellen Zugriff

Log Decoder				
Persistente Datenspeicher	Cachedatenspeicher			
	PacketDB	SessionDB	MetaDB	Index
100 % wie vom Sizing & Scoping Calculator berechnet	1 GB pro 1.000 EPS an Datenverkehr bei kontinuierlichem Durchsatz bietet 8 Stunden Cache	20 GB pro 1.000 EPS an Datenverkehr bei kontinuierlichem Durchsatz bieten 8 Stunden Cache	0,5 GB pro 1000 EPS an Datenverkehr bei kontinuierlichem Durchsatz bieten 4 Stunden Cache	

Log Concentrator			
Persistente Datenspeicher	Cachedatenspeicher		
	MetaDB	SessionDB Index	Index
Berechnet als 100 % der PacketDB, die für ein Aufbewahrungsverhältnis von 1:1 erforderlich ist	3 GB pro 1.000 EPS an Datenverkehr bei kontinuierlichem Durchsatz pro Aufbewahrungstag	5 % der berechneten MetaDB auf dem Concentrator. Bevorzugte Hochgeschwindigkeitsspindeln oder SSD für schnellen Zugriff	

Aufgabe 3: Hinzufügen eines neuen Volume und Erweitern von vorhandenen Dateisystemen

Nach der Prüfung Ihrer anfänglichen Datastore-Konfiguration stellen Sie möglicherweise fest, dass Sie ein neues Volume hinzufügen müssen. In diesem Thema verwenden wir einen virtuellen Paket-/Log Decoder-Host als Beispiel.

Führen Sie die Aufgaben in der folgenden Reihenfolge aus:

1. Fügen Sie eine neue Festplatte hinzu.
2. Erstellen Sie neue Volumes auf der neuen Festplatte.
3. Erstellen Sie ein physisches LVM-Volume auf einer neuen Partition.
4. Erweitern Sie die Volume-Gruppe um physisches Volume
5. Erweitern Sie das Dateisystem.
6. Starten Sie die Services.

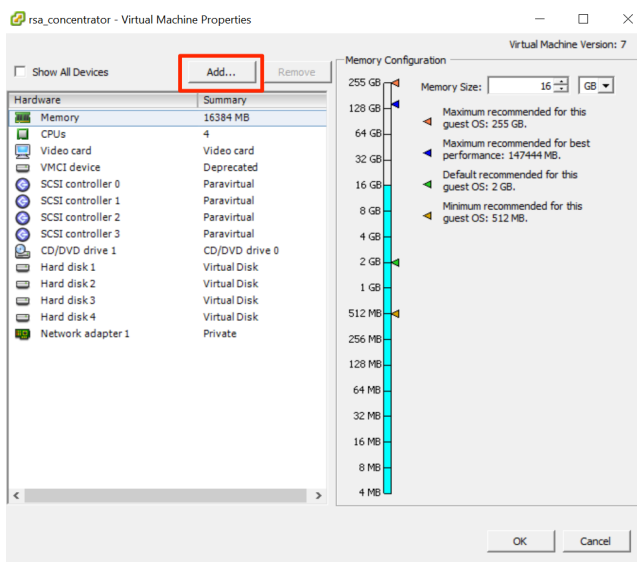
7. Stellen Sie sicher, dass die Services ausgeführt werden.
8. Konfigurieren Sie Log Decoder-Parameter neu.

Fügen Sie eine neue Festplatte hinzu.

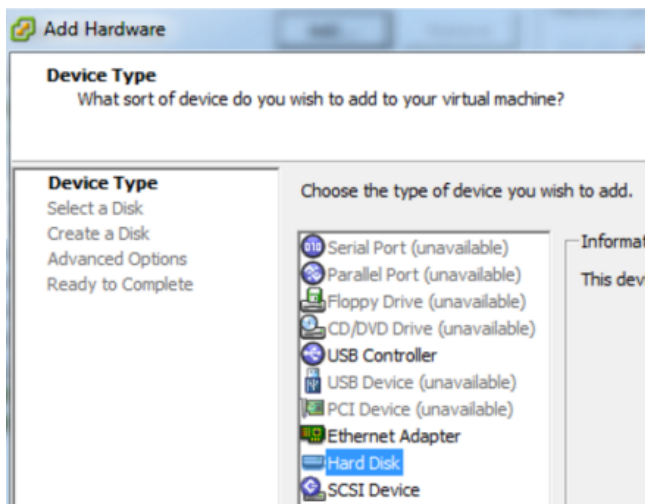
Dieses Verfahren zeigt, wie Sie ein neues 100-GB-Laufwerk auf demselben Datenspeicher hinzufügen.

Hinweis: Das Verfahren zum Hinzufügen eines Laufwerks auf einem anderen Datenspeicher ist ähnlich wie das hier gezeigte Verfahren.

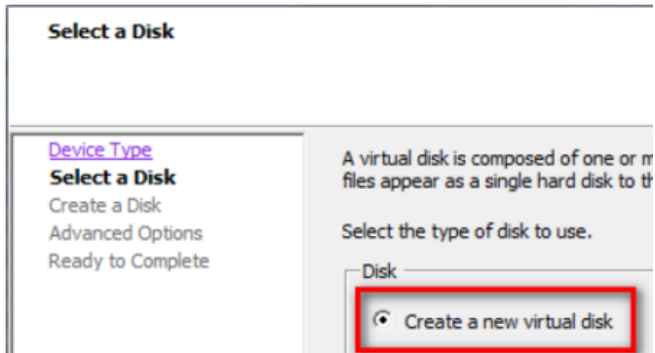
1. Fahren Sie die Maschine herunter, bearbeiten Sie die **Eigenschaften der virtuellen Maschine**, klicken Sie auf die Registerkarte **Hardware** und klicken Sie auf **Hinzufügen**.



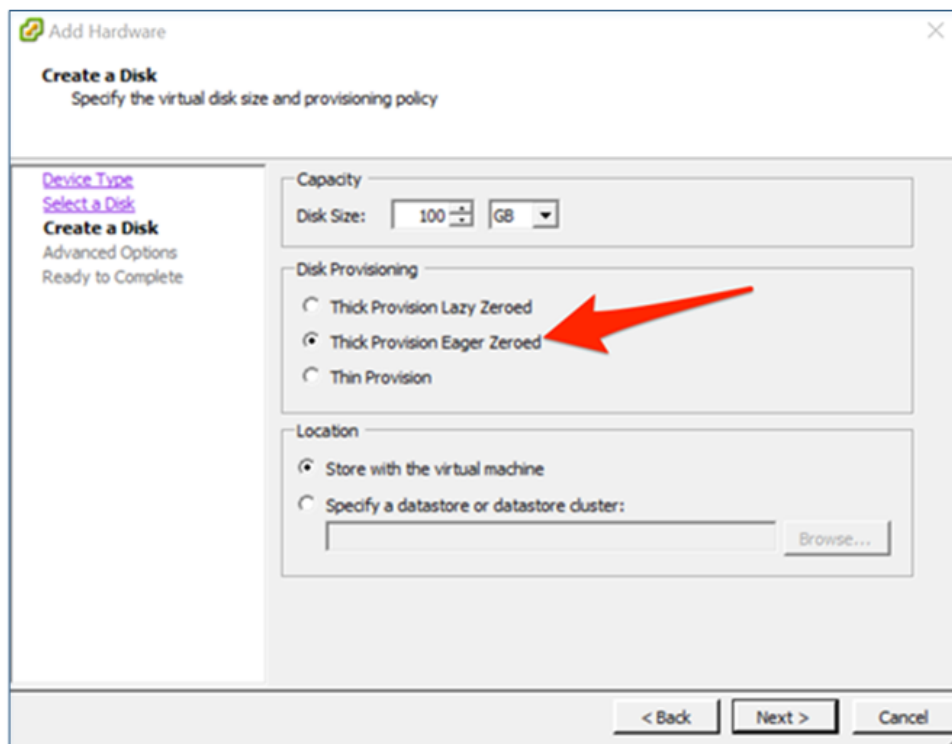
2. Wählen Sie als Gerätetyp **Festplattenlaufwerk** aus.



3. Wählen Sie **Erstellen eines neuen virtuellen Laufwerks** aus.

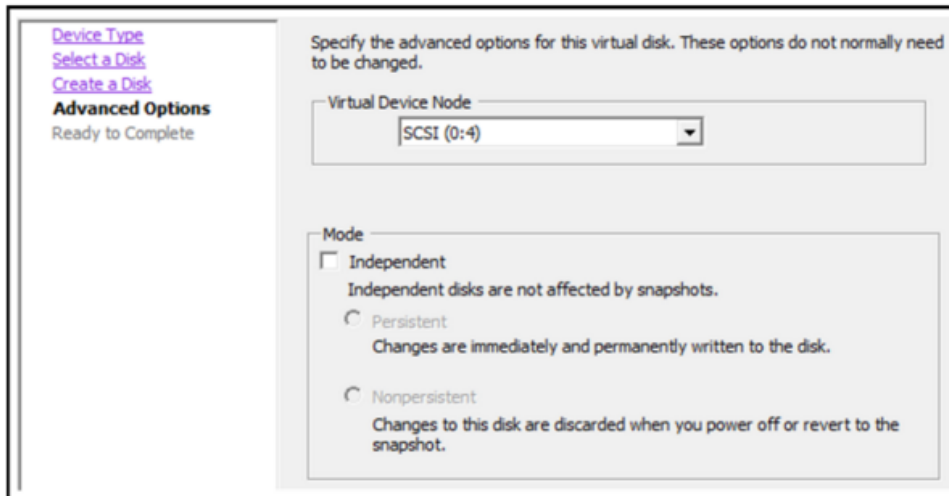


4. Wählen Sie die Größe der neuen Festplatte aus und den Speicherort, an dem es erstellt werden soll (auf demselben Datenspeicher oder auf einem anderen Datenspeicher).



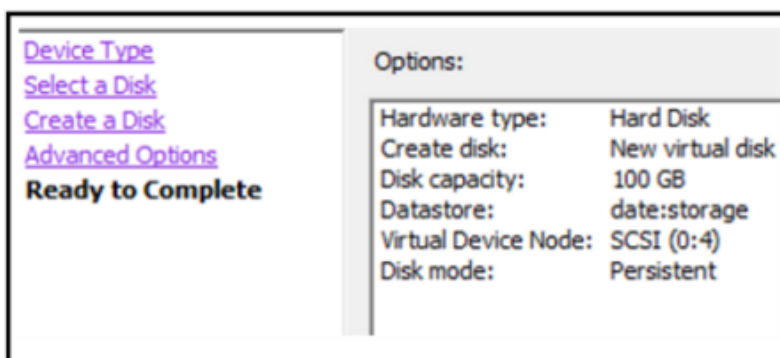
Achtung: Weisen Sie aus Gründen der Performance den gesamten Speicherplatz zu.

5. Genehmigen Sie den vorgeschlagenen virtuellen Geräte-Node.



Hinweis: Der virtuelle Geräte-Node kann unterschiedlich sein, aber er ist relevant für `/dev/sdX`-Zuordnungen.

6. Bestätigen Sie die Einstellungen.



Extending File Systems

Follow the instructions provided to extend the file systems for the various components.

AdminServer

Attach external disk for extension of `/var/netwitness/` (refer to the steps in attaching the disk) partition. Create an additional disk with suffix as `nwhome`.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk.
2. `pvcreeate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for AdminServer (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	2TB	SSD	Read/Write

ESAPrimary/ESASecondary/Malware

Attach external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
2. `pvccreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for ESAPrimary/ESASecondary (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	6TB	HDD	Read/Write

LogCollector

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

1. Execute `lsblk` and get the physical volume name, for example if you attach one 500GB disk
2. `pvccreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 600G /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for LogCollector (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	500GB	HDD	Read/Write

LogDecoder

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome, attach other external disks for Logdecoder database partition. For extending /var/netwitness partition follow these steps:

Hinweis: No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Other partitions are also required. Create the following four partitions on volume group `logdecodersmall`

Folder	LVM	Volume Group
<code>/var/netwitness/logdecoder</code>	<code>decoroot</code>	<code>logdecodersmall</code>
<code>/var/netwitness/logdecoder/index</code>	<code>index</code>	<code>logdecodersmall</code>
<code>/var/netwitness/logdecoder/metadb</code>	<code>metadb</code>	<code>logdecodersmall</code>
<code>/var/netwitness/logdecoder/sessiondb</code>	<code>sessiondb</code>	<code>logdecodersmall</code>

Follow these steps to create the partitions:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecodersmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lv_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecodersmall/<lv_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

The following four partitions should be on volume group `logdecoder` and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/logdecoder/packetdb</code>	<code>packetdb</code>	<code>logdecoder</code>

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 logdecoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb logdecoder`
5. `mkfs.xfs /dev/logdecoder/packetdb`

RSA recommends below sizing partition for LogDecoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HD D	Read/Write
/dev/logdecoderssmall/decoroot	/var/netwitness/logdecoder	10GB	HD D	Read/Write
/dev/logdecoderssmall/index	/var/netwitness/logdecoder/index	30GB	HD D	Read/Write
/dev/logdecoderssmall/metadb	/var/netwitness/logdecoder/metadb	370GB	HD D	Read/Write
/dev/logdecoderssmall/sessiondb	/var/netwitness/logdecoder/sessiondb	3TB	HD D	Read/Write
/dev/logdecoder/packetdb	/var/netwitness/logdecoder/packetdb	18TB	HD D	Read/Write

Create each directory and mount the LVM on it in a serial manner, except /var/netwitness which will be already created.

Hinweis: Create the folder /var/netwitness/logdecoder and mount on /dev/logdecoderssmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using `mount -a`.

```
/dev/logdecoderssmall/decoroot /var/netwitness/logdecoder xfs noatime,nosuid 1 2
/dev/logdecoderssmall/index /var/netwitness/logdecoder/index xfs noatime,nosuid 1 2
/dev/logdecoderssmall/metadb /var/netwitness/logdecoder/metadb xfs noatime,nosuid 1 2
/dev/logdecoderssmall/sessiondb /var/netwitness/logdecoder/sessiondb xfs noatime,nosuid 1 2
/dev/logdecoder/packetdb /var/netwitness/logdecoder/packetdb xfs noatime,nosuid 1 2
```

Concentrator

Attach external disk for extension of /var/netwitness/ partition, Create an external disk with suffix as nwhome, attach other external disks for Concentrator database partition. If there are multiple disks, create a Raid 0 array.

For extending /var/netwitness partition follow below steps:

Hinweis: No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partition are also required on volume group concentrator and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator</code>	Root	Concentrator
<code>/var/netwitness/ concentrator /sessiondb</code>	index	Concentrator
<code>/var/netwitness/ concentrator /metadb</code>	metadb	Concentrator

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 concentrator /dev/md0`
4. `lvcreate -L <disk_size> -n <lvm_name> concentrator`
5. `mkfs.xfs /dev/concentrator/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below four partitions should be on volume group index and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator/index</code>	index	index

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md1`
3. `vgcreate -s 32 index /dev/md1`
4. `lvcreate -L <disk_size> -n index index`
5. `mkfs.xfs /dev/index/index`

RSA recommends below sizing partition for Concentrator (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HD D	Read/Write
/dev/concentrator/decoroot	/var/netwitness/concentrator	10GB	HD D	Read/Write
/dev/concentrator/metadb	/var/netwitness/concentrator/metadb	370GB	HD D	Read/Write
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb	3TB	HD D	Read/Write
/dev/index/index	/var/netwitness/concentrator/index	2TB	SSD	Read/Write

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

Hinweis: Create the folder `/var/netwitness/concentrator` and mount on `/dev/concentrator/decoroot` then create the other folders and mount them.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/concentrator/root /var/netwitness/concentrator xfs noatime,nosuid 1 2
/dev/concentrator/sessiondb /var/netwitness/concentrator/sessiondb xfs
noatime,nosuid 1 2
/dev/concentrator/metadb /var/netwitness/concentrator/metadb xfs
noatime,nosuid 1 2 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
```

Archiver

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for Archiver database partition. If there are multiple disks, create a Raid 0 array.

For extending `/var/netwitness` partition follow these steps:

Hinweis: No other partition should reside on this partition, only to be used for `/var/netwitness/partition`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreeate <pv_name> . ex suppose the PV name is /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partitions are required on volume group archiver and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/archiver	Archiver	archiver

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 archiver /dev/md0`
4. `lvcreate -L <disk_size> -n archiver archiver`
5. `mkfs.xfs /dev/archiver/archiver`

RSA recommends below sizing partition for archiver (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD	Read/Write
/dev/archiver/archiver	/var/netwitness/archiver	4TB	HDD	Read/Write

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/archiver/archiver /var/netwitness/archiver xfs noatime,nosuid 1 2
```

Decoder

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for decoder database partition. For extending `/var/netwitness` partition follow these steps:

Hinweis: No other partition should reside on this partition, only to be used for `/var/netwitness/partition`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name> . ex suppose the PV name is /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Below four partition should be on volume group `decodersmall`

Folder	LVM	Volume Group
/var/netwitness/decoder	decoroot	decoderssmall
/var/netwitness/decoder/index	index	decoderssmall
/var/netwitness/decoder/metadb	metadb	decoderssmall
/var/netwitness/decoder/sessiondb	sessiondb	decoerssmall

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecoderssmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lvm_name> logdecoderssmall`
5. `mkfs.xfs /dev/logdecoderssmall/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below partition should be on volume group logdecoder and should be in single RAID 0 array

Below four partition should be on volume group logdecoder and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/logdecoder/packetdb	packetdb	decoder

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 decoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb decoder`
5. `mkfs.xfs /dev/decoder/packetdb`

RSA recommends below sizing partition for Decoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness	1TB	HDD	Read/Write
/dev/decoderssmall/decoroot	/var/netwitness/decoder	10GB	HDD	Read/Write

LVM	Folder	Size	Disk Type	Caching
/dev/decodersmall/index	/var/netwitness/decoder/index	30GB	HDD	Read/Write
/dev/decoderssmall/metadb	/var/netwitness/decoder/metadb	370GB	HDD	Read/Write
/dev/decoderssmall/sessiondb	/var/netwitness/decoder/sessiondb	3TB	HDD	Read/Write
/dev/decoder/packetdb	/var/netwitness/decoder/packetdb	18TB	HDD	Read/Write

Create each directory and mount the LVM on it in serial manner, except `/var/netwitness` which will be already created.

Hinweis: Create the folder `/var/netwitness/decoder` and mount on `/dev/decoderssmall/decoroot` then create the other folders and mount them.

After that add the below entries in `/etc/fstab` in the same order and mount them using `mount -a`.

```

/dev/decoderssmall/decoroot /var/netwitness/decoder xfs noatime,nosuid 1 2
/dev/decoderssmall/index /var/netwitness/decoder/index xfs noatime,nosuid 1 2
/dev/decoderssmall/metadb /var/netwitness/decoder/metadb xfs noatime,nosuid 1 2
/dev/decoderssmall/sessiondb /var/netwitness/decoder/sessiondb xfs
noatime,nosuid 1 2
/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2

```

Installieren von RSA NetWitness Platform

Es gibt zwei Hauptaufgaben, die in der unten angegebenen Reihenfolge durchgeführt werden müssen, um NetWitness Platform 11.2 zu installieren.

1. Aufgabe 1: Installieren von 11.2.0.0 auf dem NetWitness-Serverhost
2. Aufgabe 2: Installieren von 11.2.0.0 auf den Hosts anderer Komponenten

Aufgabe 1: Installieren von 11.2.0.0 auf dem NW-Serverhost

Bei dieser Aufgabe wird auf dem Host, den Sie für den NW-Server bereitgestellt haben, Folgendes installiert:

- Die 11.2.0.0-Umgebungsplattform für NW-Server.

- Der NW-Serverkomponenten (d. h. Admin-Server, Konfigurationsserver, Orchestrierungsserver, Integrationsserver, Broker, Investigate-Server, Reporting Engine, Respond-Server und Security Server).
 - Ein Repository mit den RPM-Dateien, die für die Installation von anderen Funktionskomponenten oder Services erforderlich sind.
1. Stellen Sie die 11.2.0.0 Umgebung bereit:
 - a. Fügen Sie eine neue VM hinzu.
 - b. Konfigurieren Sie den Speicher.
 - c. Richten Sie Firewalls ein.
 2. Führen Sie den Befehl `nwsetup-tui` aus. 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 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 Platform 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
```

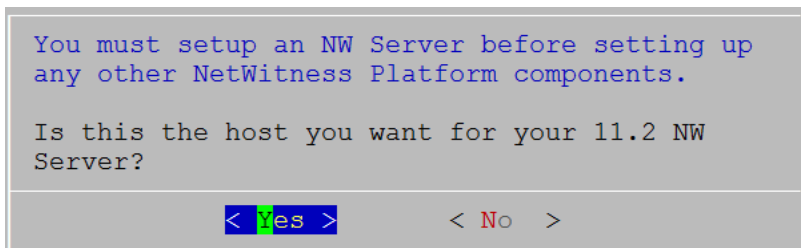
92%

<Accept >

<Decline>

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-

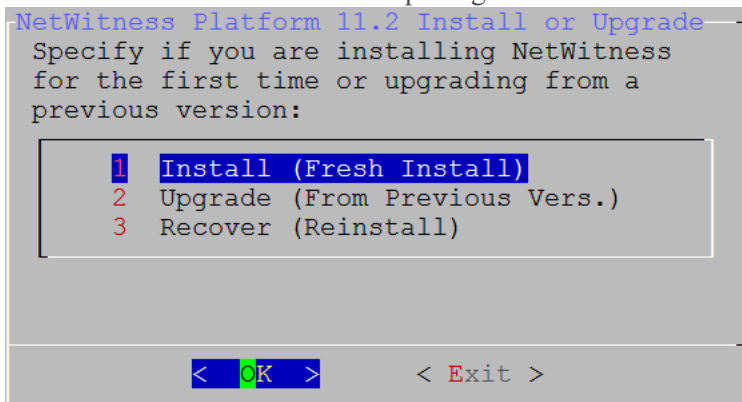
Server verwenden möchten.



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

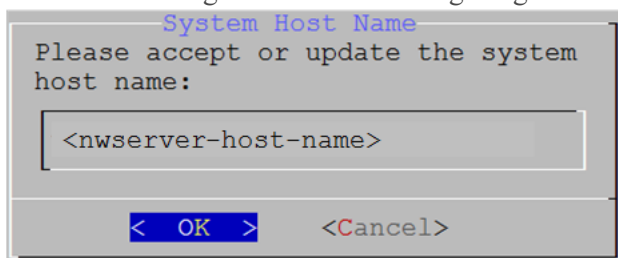
Achtung: Wenn Sie den falschen Host für den NW-Server auswählen und das Setup abschließen, müssen Sie das Setup-Programm (Schritt 3) starten und alle nachfolgenden Schritte ausführen, um diesen Fehler zu korrigieren.

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.



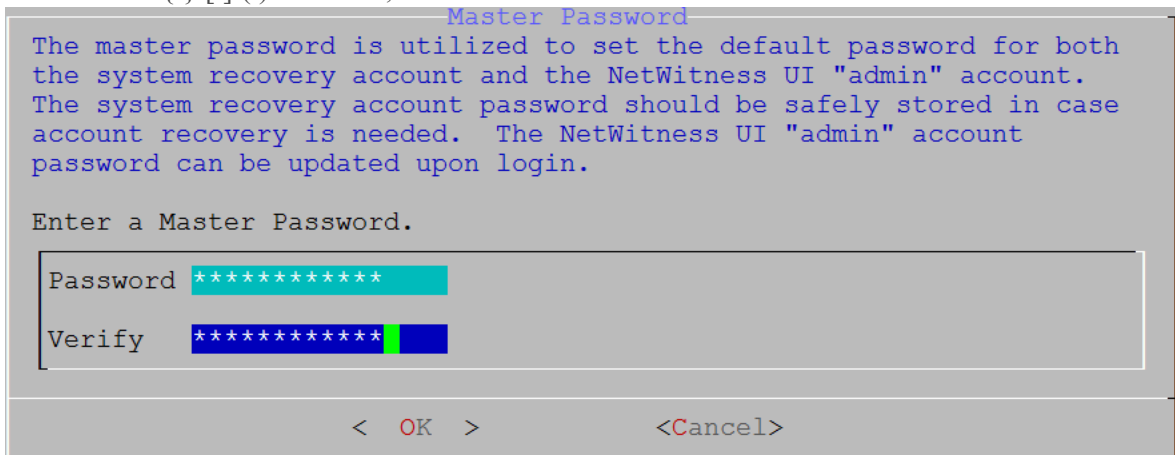
Achtung: Wenn Sie „.“ in einen Hostnamen einfügen, muss dieser auch einen gültigen Domainnamen enthalten.

6. Drücken Sie die Eingabetaste, wenn dieser Name beibehalten werden soll. Wenn Sie den Hostnamen bearbeiten möchten, gehen Sie zu **OK** und drücken Sie die EINGABETASTE, um ihn zu ändern.
7. Die Aufforderung **Masterpasswort** wird angezeigt.
Für das Masterpasswort und 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 { } [] () / \ ' " ` ~ ; : . < > -



8. Die Aufforderung **Masterpasswort** wird angezeigt.

Für das Masterpasswort und Bereitstellungspasswort werden folgende Zeichen unterstützt:

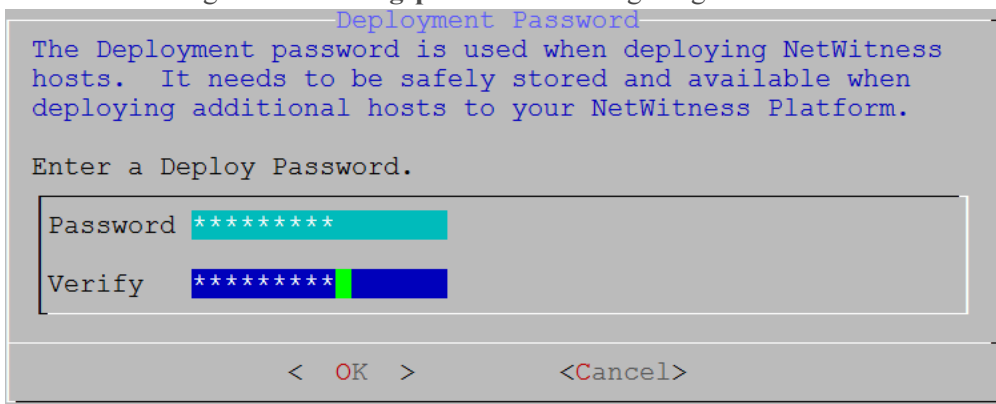
- Symbole: ! @ # % ^ +
- Zahlen: 0-9
- Kleinbuchstaben: a-z
- Großbuchstaben: A-Z

Beim Masterpasswort und Bereitstellungspasswort werden keine nicht eindeutigen Zeichen unterstützt. Beispiel:

Leerzeichen { } [] () / \ ' " ` ~ ; : . < > -

9. Gehen Sie mit dem Pfeil nach unten zu **Password** und geben Sie es ein. Gehen Sie dann mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie die EINGABETASTE.

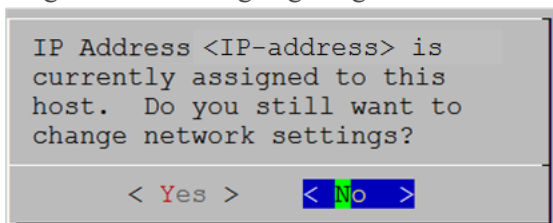
Die Aufforderung **Bereitstellungspasswort** wird angezeigt.



10. 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.

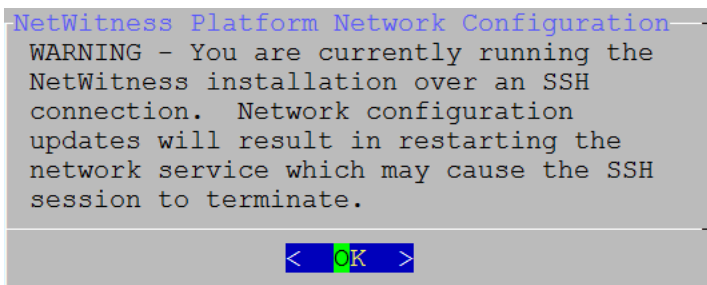
- Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt:



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

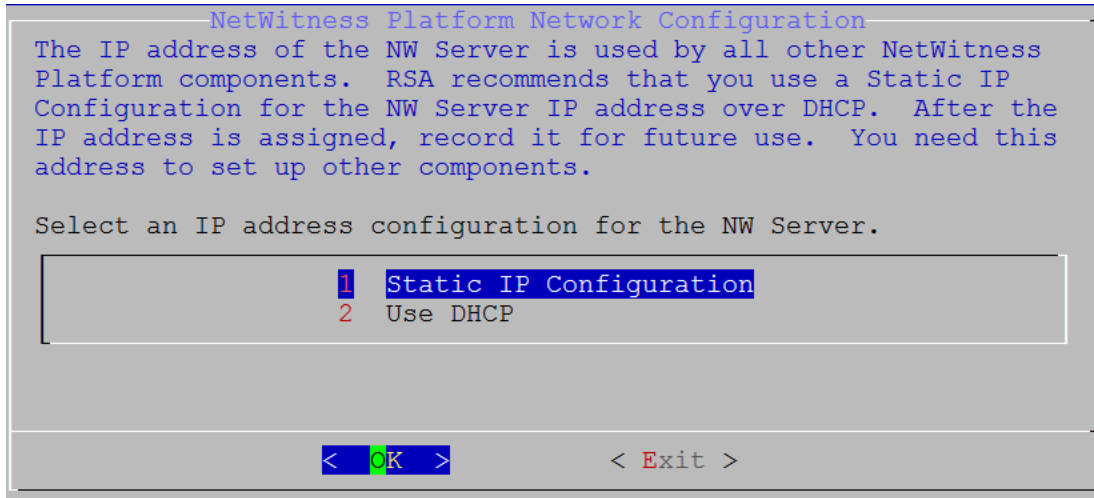
Hinweis: Wenn die Verbindung direkt über die Hostkonsole erfolgt, wird die folgende Warnung nicht angezeigt.



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

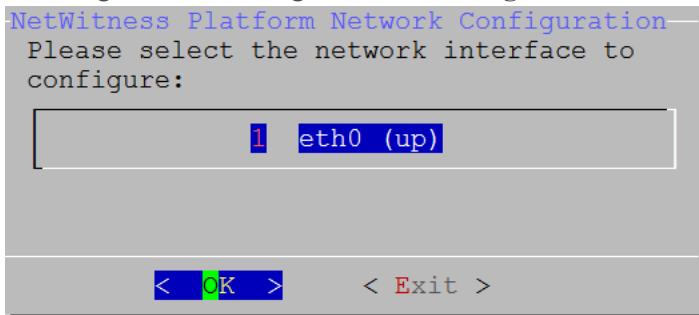
Hinweis: Wenn die Verbindung direkt über die Hostkonsole erfolgt, wird die obige Warnung nicht angezeigt.

- 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 keine IP-Konfiguration gefunden wurde oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung **Netzwerkconfiguration** angezeigt.



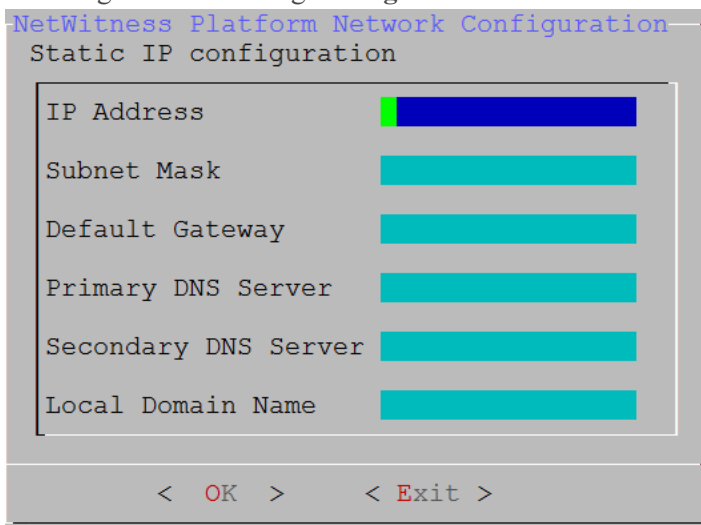
11. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um **Statische IP-Adresse** zu verwenden. Wenn Sie **DHCP** verwenden möchten, gehen Sie mit dem Pfeil nach unten zu „2 DHCP verwenden“ und drücken Sie **EINGABETASTE**.

Die Eingabeaufforderung **Netzwerkconfiguration** wird angezeigt.



12. 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.

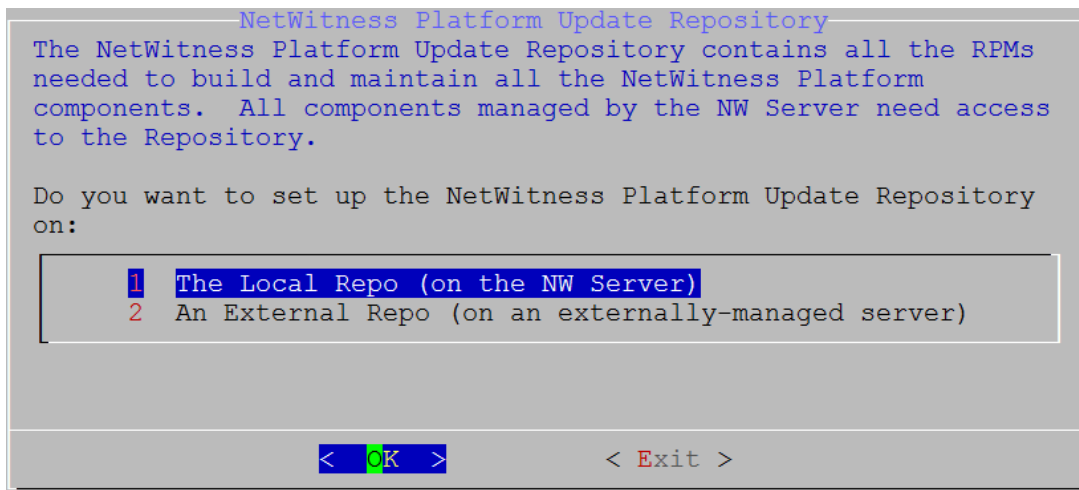


13. Geben Sie die Konfigurationswerte (indem Sie mit dem Pfeil nach unten von Feld zu Feld gehen) ein. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**. Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung `All fields are required` angezeigt (die Felder **Sekundärer DNS-Server** und **Lokaler Domainname** sind nicht erforderlich). Bei Verwendung der falschen Syntax oder Zeichenlänge für eines der Felder wird die Fehlermeldung angezeigt, dass der Feldname ungültig ist.

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.

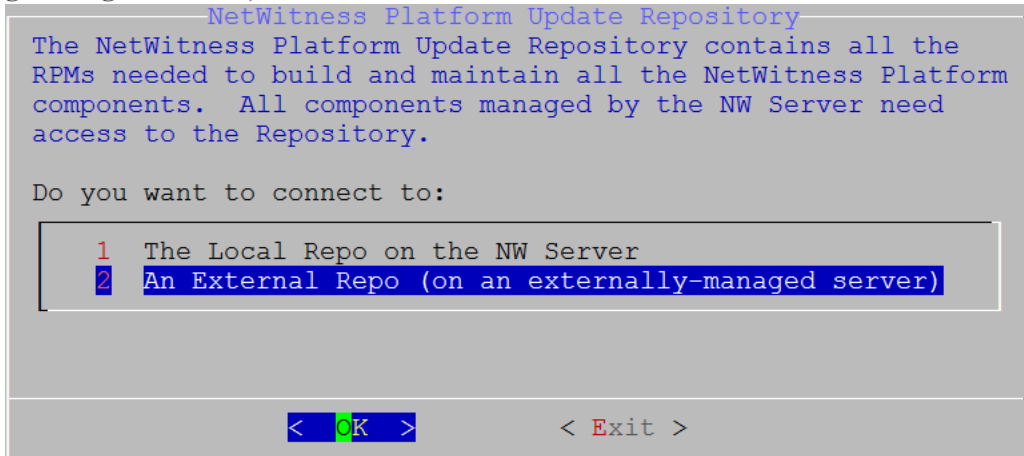
14. Wählen Sie für alle Hosts das gleiche Repository aus, das Sie bei Installation des NW-Serverhosts ausgewählt haben.



Drücken Sie die **Eingabetaste**, um **Lokales Repository** auf dem NW-Server auszuwählen. Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten

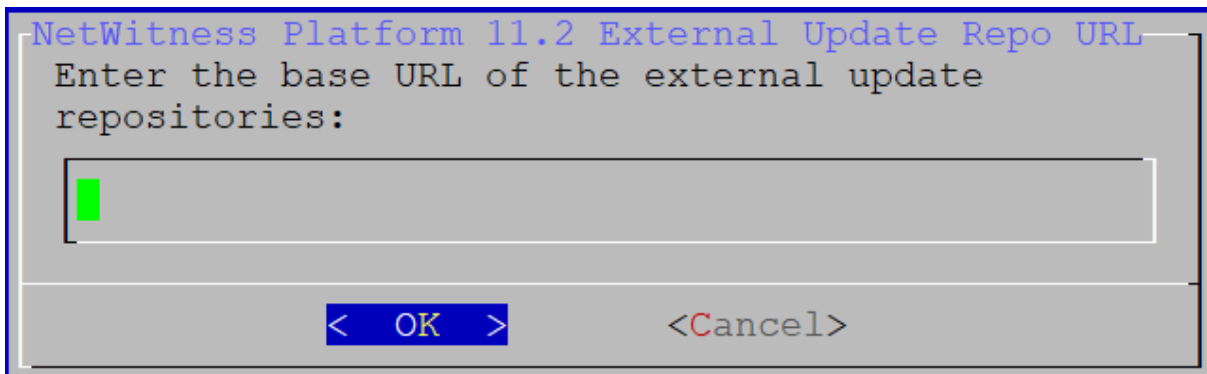
zu **Externes Repository** und dann zu **OK** und drücken Sie die **Eingabetaste**. Stellen Sie bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** im Setup-Programm sicher, dass die richtigen Medien mit dem Host verbunden sind (Medien mit der ISO-Datei, z. B. ein Build-Stick), von denen es die Installation von NetWitness Platform 11.2.0.0 abrufen kann.

15. Verwenden Sie den Pfeil nach oben oder unten, um **2 Ein externes Repository (auf einem extern gemanagten Server)** auszuwählen.



Die Eingabeaufforderung für die URL des externen Update-Repository wird angezeigt. Anweisungen zur Einrichtung eines externen Repository finden Sie in [Anhang B: Erstellen eines externen Repository](#). Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

16. Geben Sie die Basisadresse des externen Repository von NetWitness Platform aus den befolgten Anweisungen in [Anhang B: Erstellen eines externen Repository](#) (zum Beispiel **http://testserver/netwitness-repo**) und klicken Sie auf **OK**.



Die Aufforderung zur **Deaktivierung** oder Verwendung der Standardkonfiguration für **Firewalls** wird angezeigt.

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

und drücken Sie die Eingabetaste, um Standardkonfiguration für Firewalls zu deaktivieren.

```
Disable Firewall
Do you need to apply custom
firewall rules to this host?
("No" enforces the standard
NetWitness firewall rule set to
the host)
< Yes > < No >
```

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

```
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 >
```

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

18. Drücken Sie die Eingabetaste, um 11.2.0.0 auf dem Nicht-NW-Server zu installieren (**Jetzt installieren** ist der Standardwert).

```
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 >
```

Wenn **Installation abgeschlossen** angezeigt wird, haben Sie den 10.6.6 NW-Server auf den 11.2 NW-Server aktualisiert.

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.

```
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 11.2 auf den Hosts anderer Komponenten

Führen Sie für einen funktionsfähigen Service die folgenden Aufgaben auf einem Nicht-NW-Serverhost aus.

- Installieren Sie die 11.2.0.0-Umgebungsplattform.
 - Wenden Sie die 11.2.0.0 RPM-Dateien aus dem Repository für NW-Serveraktualisierungen auf den Service an.
1. Stellen Sie 11.2.0.0 OVA bereit.
 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 [\(Optional\) 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 Platform 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
```

92%

<Accept >

<Decline>

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 11.2.0.0 auf dem NW-Serverhost](#) (Schritte 2 bis 14) ausführen, um diesen Fehler zu korrigieren.

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

```
Is this the host you want for your 11.2 NW
Server?
```

```
< Yes >
```

```
< No >
```

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.).

```
NetWitness Platform 11.2 Install or Upgrade
```

```
Specify if you are installing NetWitness
for the first time or upgrading from a
previous version:
```

- ```
1 Install (Fresh Install)
2 Upgrade (From Previous Vers.)
3 Recover (Reinstall)
```

```
< OK >
```

```
< Exit >
```

5. Drücken Sie die Eingabetaste. Die Option für Installieren (neue Installation) ist standardmäßig ausgewählt.

Die Aufforderung **Hostname** wird angezeigt.

```
System Host Name
```

```
Please accept or update the system
host name:
```

```
<non-nwserver-host-name>
```

```
< OK >
```

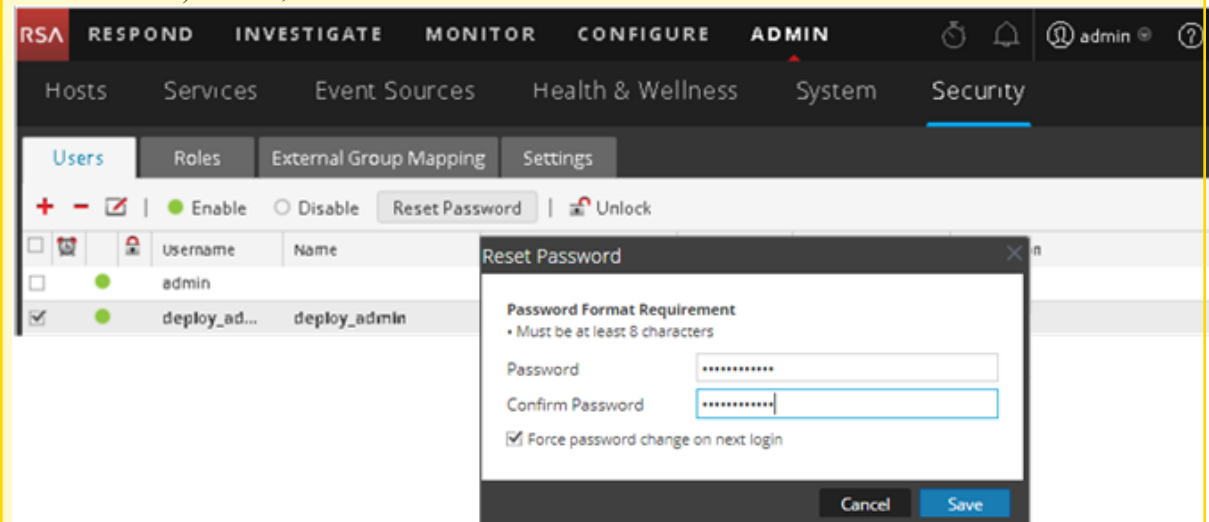
```
<Cancel>
```

**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.



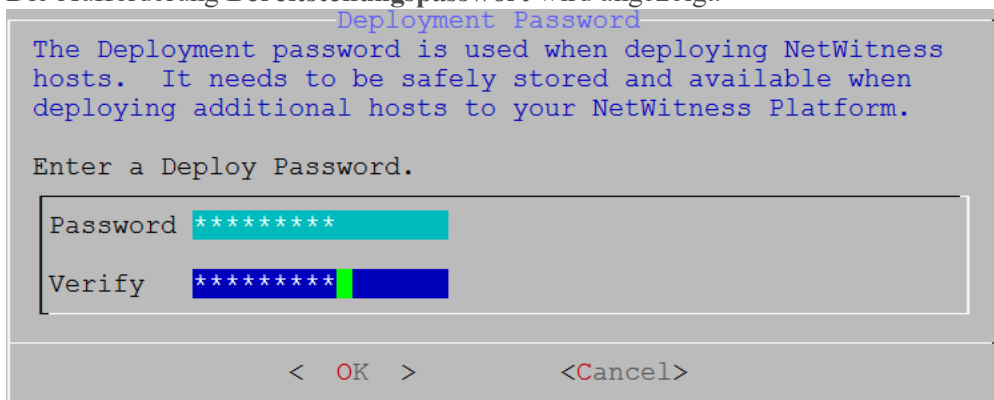
**Achtung:** Wenn Sie das Nutzerpasswort **deploy\_admin** auf der NetWitness Platform-Benutzeroberfläche (**ADMIN > Sicherheit > deploy\_admin** auswählen – **Passwort zurücksetzen**) ändern,



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.

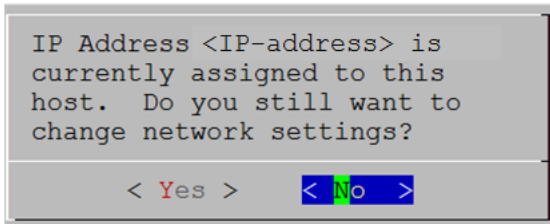


**Hinweis:** Sie müssen das gleiche Bereitstellungspasswort verwenden, das Sie bei der Installation des NW-Servers verwendet haben.

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**.

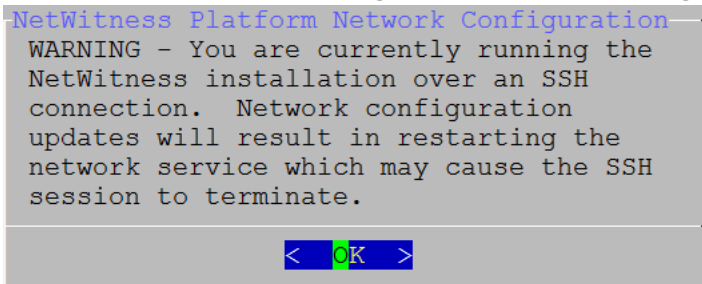
Eine der folgenden bedingten Eingabeaufforderungen wird angezeigt.

- 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. Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**, wenn Sie die auf dem Host gefundene IP-Konfiguration ändern möchten.

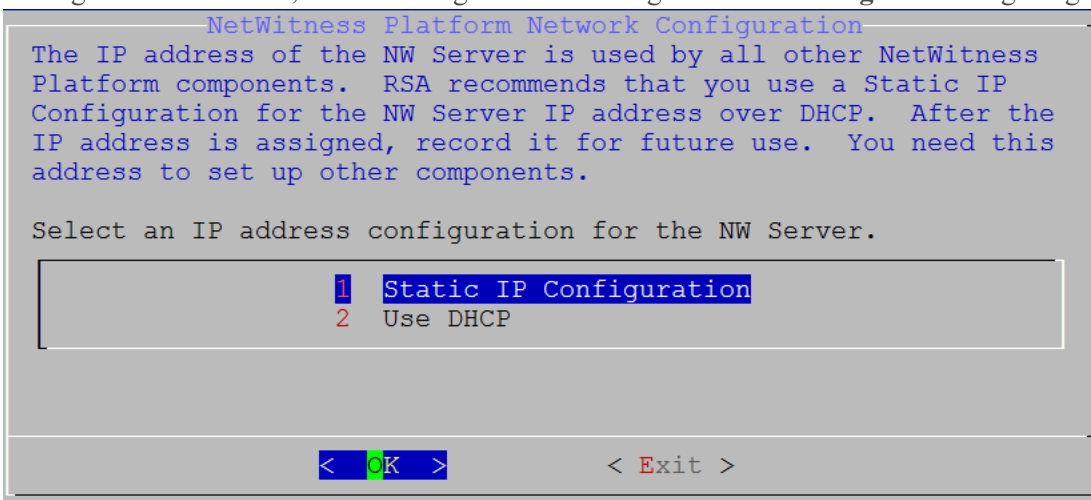
- Wenn Sie eine SSH-Verbindung verwenden, wird die folgende Warnung angezeigt:



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

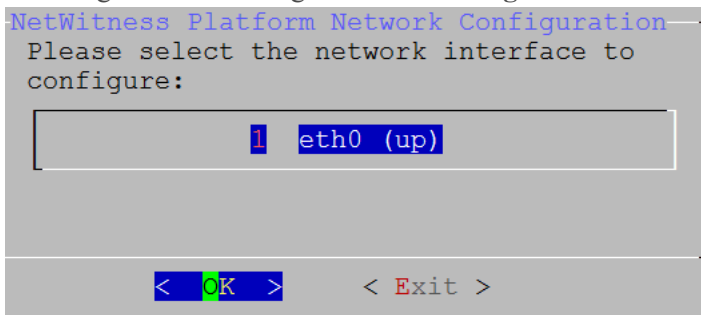
**Hinweis:** Wenn die Verbindung direkt über die Hostkonsole erfolgt, wird die obige Warnung nicht angezeigt.

- 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 keine IP-Konfiguration gefunden wurde oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung **Netzwerkkonfiguration** angezeigt.

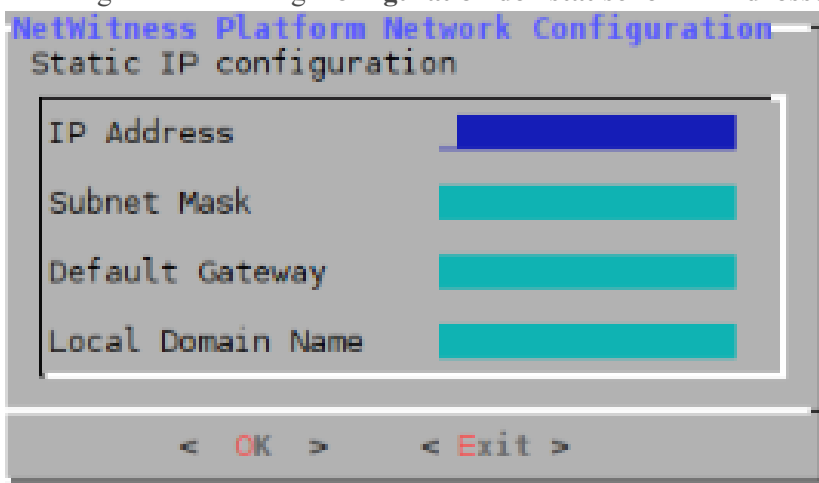


- Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um **Statische IP-Adresse** zu verwenden. Wenn Sie **DHCP** verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **2 DHCP verwenden** und drücken Sie die Eingabetaste.

Die Eingabeaufforderung **Netzwerkconfiguration** wird angezeigt.



- 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.

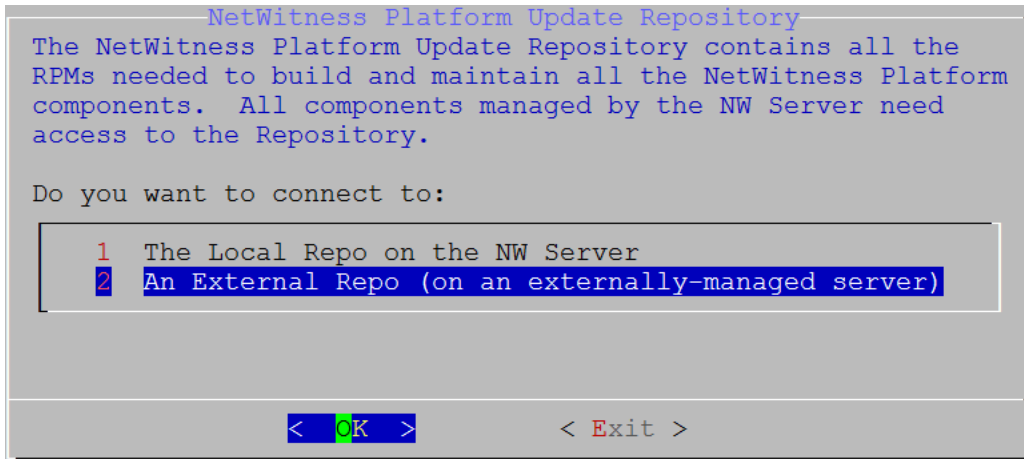


- Geben Sie die Konfigurationswerte (indem Sie mit dem Pfeil nach unten von Feld zu Feld gehen) ein. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**. Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung `All fields are required` angezeigt (die Felder **Sekundärer DNS-Server**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

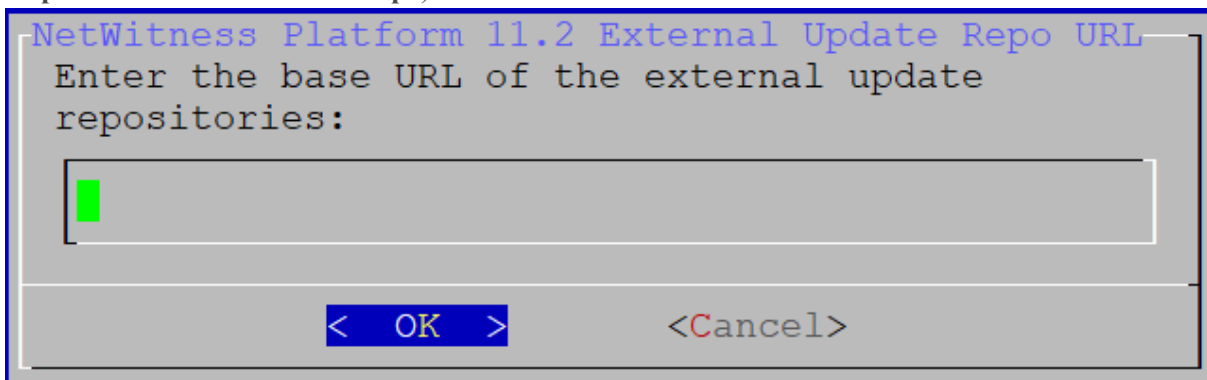
Die Eingabeaufforderung **Update-Repository** wird angezeigt.

- Verwenden Sie den Pfeil nach oben oder unten, um **2 Ein externes Repository (auf einem extern gemanagten Server)** auszuwählen, gehen Sie zu **OK** und drücken Sie die Eingabetaste.



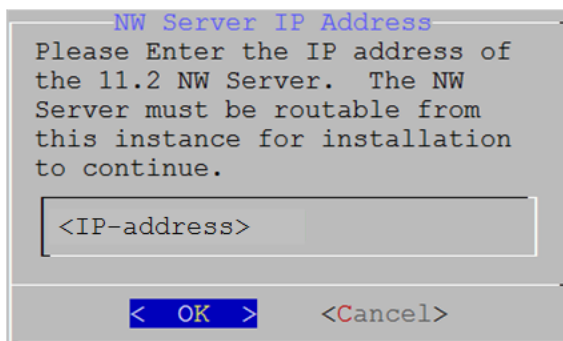
Die Eingabeaufforderung für die URL des externen Update-Repository wird angezeigt. Die Repositories bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates.

12. Geben Sie den Basis-URL für das externe Repository für NetWitness Platform ein, das zum Einrichten des NW-Servers im vorherigen Schritt verwendet wurde (z. B. <http://testserver/netwitness-repo>) und klicken Sie auf **OK**.



Die IP-Adresse des NW-Servers wird angezeigt.

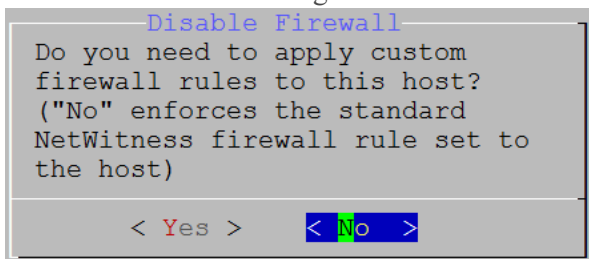
13. Geben Sie die IP-Adresse des NW-Servers ein, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.



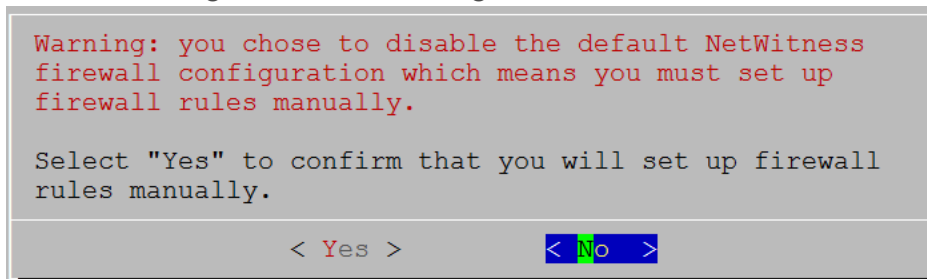
Die Aufforderung zur Deaktivierung oder Verwendung der Standardkonfiguration für Firewalls wird angezeigt.

14. 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.

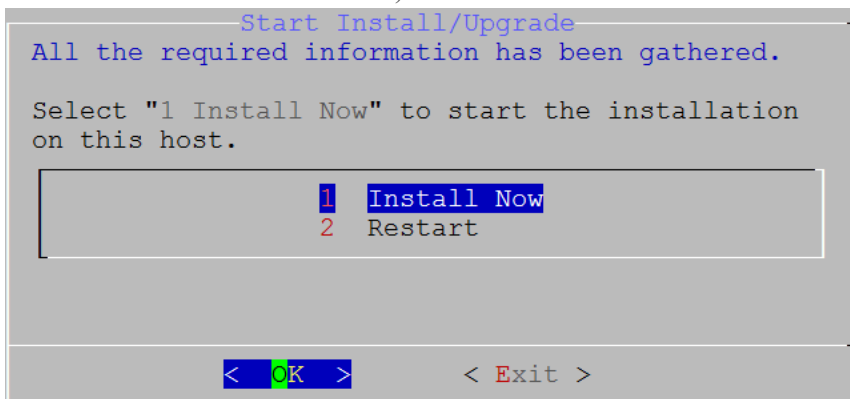


- Wenn Sie **Ja** ausgewählt haben, bestätigen Sie Ihre Auswahl.



- Wenn Sie **Nein** ausgewählt haben, wird die Standardkonfiguration für Firewalls angewendet. Die Aufforderung **Installation starten** wird angezeigt.



15. Drücken Sie die Eingabetaste, um 11.2.0.0 auf dem Nicht-NW-Server zu installieren (**Jetzt installieren** ist der Standardwert).

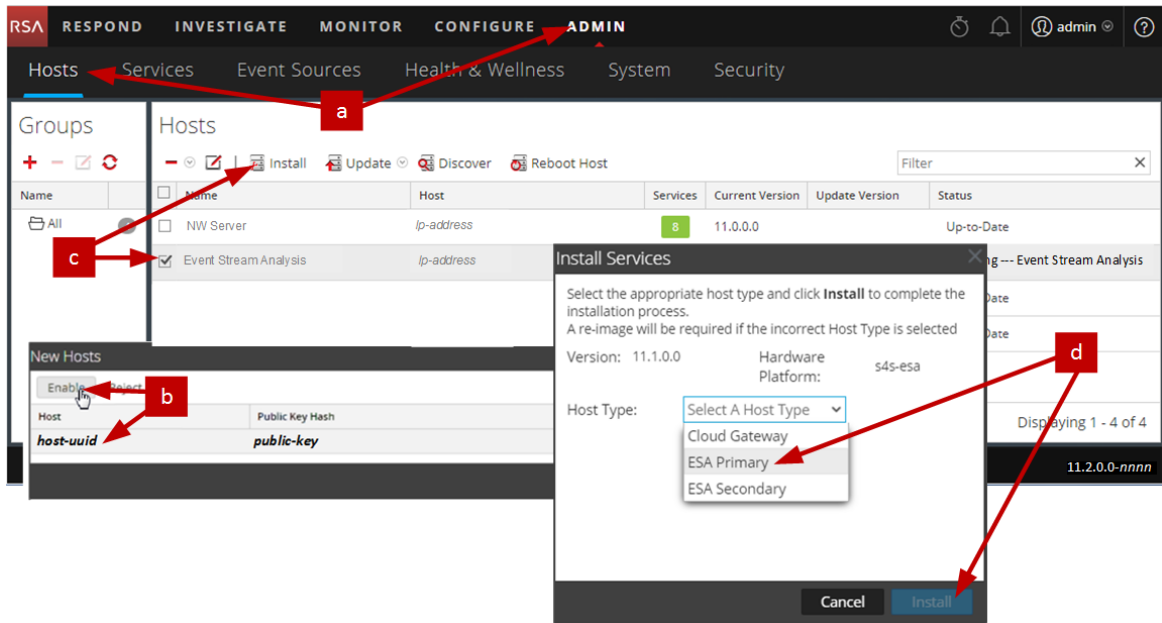


Wenn **Installation abgeschlossen** angezeigt wird, verfügen Sie über einen generischen Host mit einem Betriebssystem, das mit NetWitness Platform 11.2.0.0 kompatibel ist.

16. Installieren Sie einen Komponentendienst auf dem Nicht-NW-Serverhost.
  - 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**) 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.

17. Komplette Lizenzanforderungen für installierte Services.  
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.
18. Führen Sie für den Rest der Nicht-NW-Serverkomponenten von NetWitness Platform die Schritte 1 bis 16 aus.

## Schritt 4. Konfigurieren von hostspezifischen Parametern

Bestimmte anwendungsspezifische Parameter sind erforderlich, um die Protokollaufnahme und die Paketerfassung in der virtuellen Umgebung zu konfigurieren.

### Konfigurieren der Protokollaufnahme in der virtuellen Umgebung

Die Protokollaufnahme ist leicht zu bewerkstelligen, indem die Protokolle an die IP-Adresse gesendet werden, die Sie für den Decoder angegeben haben. In der Managementoberfläche des Decoder können Sie dann die richtige Schnittstelle zum Überwachen des Datenverkehrs auswählen, falls die automatische Standardauswahl nicht korrekt ist.

## Konfigurieren der Paketerfassung in der virtuellen Umgebung

Es gibt zwei Optionen für die Erfassung von Paketen in einer VMware-Umgebung. Die erste besteht darin, Ihren vSwitch in den Empfangsmodus zu versetzen, die zweite ist die Verwendung eines Virtual Tap eines Drittanbieters.

### Einstellen eines vSwitch auf den Empfangsmodus

Beim Einstellen eines Switches (virtuell oder physisch) auf den Empfangsmodus, auch als SPAN-Port (Cisco-Services) und Portspiegelung bezeichnet, sind bestimmte Einschränkungen zu berücksichtigen. Bei virtuellen wie physischen Switchen kann die Paketerfassung je nach Menge und Art des kopierten Datenverkehrs leicht zu einer Überlastung des Ports führen, was mit Paketverlusten gleichzusetzen ist. Taps, die ebenfalls physisch oder virtuell sein können, sind auf verlustfreie, 100%ige Erfassung des anvisierten Datenverkehrs ausgelegt.

Der Empfangsmodus ist standardmäßig deaktiviert und sollte nur eingeschaltet werden, wenn es im spezifischen Fall erforderlich ist. Software, die innerhalb einer Virtual Machine ausgeführt wird, kann in der Lage sein, den gesamten Datenverkehr über einen vSwitch zu überwachen, wenn sie den Empfangsmodus aktivieren und Paketverluste aufgrund einer Überbelastung des Ports verursachen darf.

So konfigurieren Sie eine Portgruppe oder einen virtuellen Switch so, dass der Empfangsmodus erlaubt ist:

1. Melden Sie sich beim ESXi/ESX-Host oder beim vCenter-Server mit dem vSphere-Client an.
2. Wählen Sie den ESXi/ESX-Host im Bestand aus.
3. Wählen Sie die Registerkarte **Konfiguration** aus.
4. Klicken Sie im Abschnitt **Hardware** auf **Netzwerk**.
5. Wählen Sie die **Eigenschaften** des virtuellen Switch aus, für den Sie den Empfangsmodus aktivieren möchten.
6. Wählen Sie den virtuellen Switch oder die Portgruppe aus, den bzw. die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
7. Klicken Sie auf die Registerkarte **Sicherheit**. Wählen Sie aus dem Drop-down-Menü **Empfangsmodus** die Option **Akzeptieren** aus.

### Verwenden eines Virtual Tap eines Drittanbieters

Die Installationsmethoden für ein Virtual Tap variieren je nach Anbieter. Anweisungen zur Installation finden Sie in der Dokumentation Ihres Anbieters. Virtual Taps sind normalerweise leicht zu integrieren und die Benutzeroberfläche des Tap vereinfacht die Auswahl und die Art des zu kopierenden Datenverkehrs.

Virtual Taps kapseln den erfassten Datenverkehr in einem GRE-Tunnel ein. Je nach gewähltem Typ gilt eines der folgenden Szenarios:

- Am Ende des Tunnels wird ein externer Host benötigt, der den Datenverkehr zur Decoder-Schnittstelle leitet.
- Der Tunnel sendet den Datenverkehr direkt an die Decoder-Schnittstelle, wo NetWitness Platform den Datenverkehr aus der Kapsel entnimmt.

## Schritt 5. Aufgaben nach der Installation

Dieses Thema enthält die Aufgabe, die Sie nach der Installation von 11.2 ausführen.

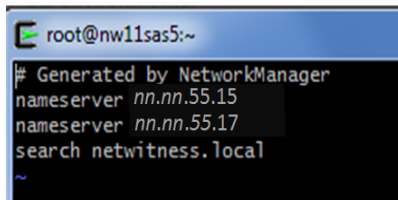
- Allgemein
- RSA NetWitness® Endpoint Insights
- FIPS-Aktivierung
- RSA NetWitness Analyse des Nutzer- und Entitätsverhaltens (UEBA)

### 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.

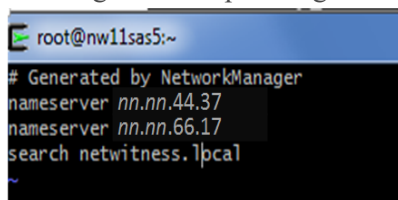


```

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/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.

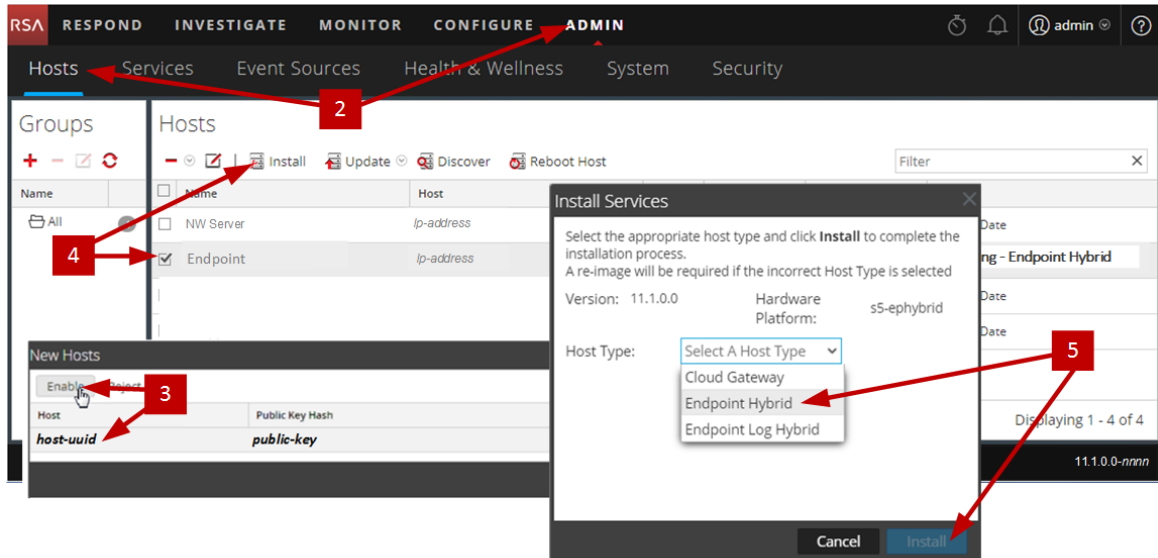
1. Führen Sie für physische Hosts die Schritte 1 bis 14 bzw. für virtuelle Hosts die Schritte 1 bis 15 unter „Aufgabe 2: Installieren von 11.2 auf den Hosts anderer Komponenten“ in „Installationsaufgaben“ des *Installationshandbuchs für physische Hosts für Version 11.2 der NetWitness-Plattform* aus. 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.

- 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.



- Stellen Sie sicher, dass alle Endpoint Hybrid- oder Endpoint Log Hybrid-Services ausgeführt werden.
- Konfigurieren Sie die Weiterleitung von Endpunktmeldungen. Anweisungen zum Konfigurieren der Weiterleitung von Endpunktmeldungen finden Sie im *Konfigurationsleitfaden zu Endpoint Insights*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
- 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.

## NetWitness Analyse des Nutzer- und Entitätsverhaltens (UEBA)

### (Optional) Aufgabe 3: Installieren von NetWitness UEBA

#### Voraussetzung: Erhöhen des Speichers für virtuelle Bereitstellung

Virtuelle Maschinen werden standardmäßig mit etwa 104 GB im Speichermount eingesetzt. Zur Installation von NetWitness UEBA müssen Sie den Speicherplatz in Ihrer virtuellen Umgebung auf mindestens 800 GB erhöhen.

#### 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-Plattform* aus. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

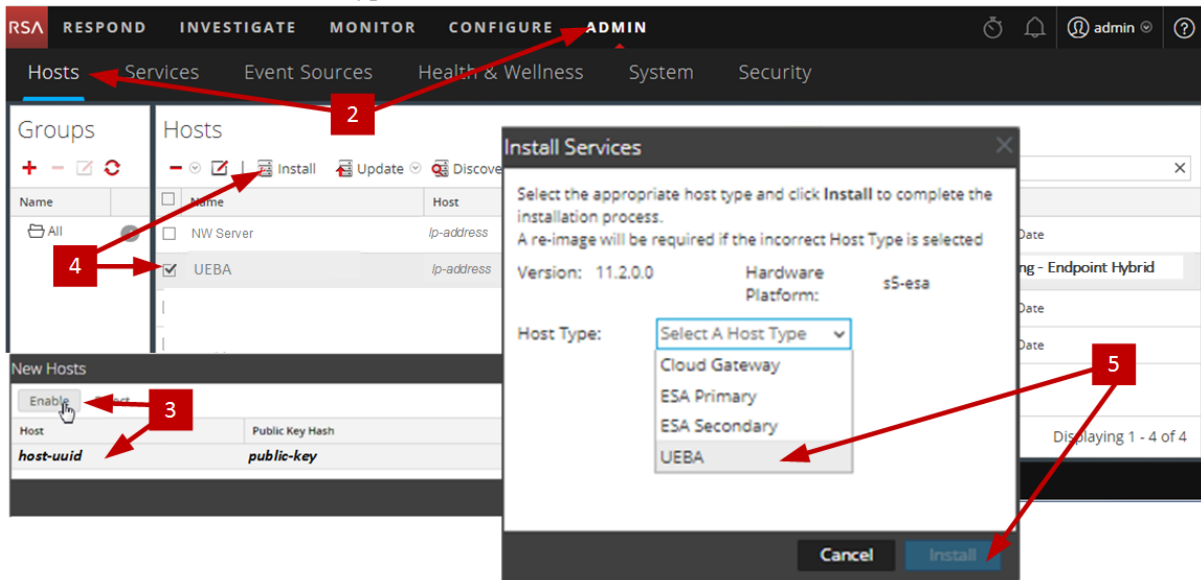
**Hinweis:** Das Passwort der Benutzeroberfläche von Kibana und dem Airflow-Webserver ist das gleiche wie das „deploy\_admin“-Passwort. Vergewissern Sie sich, dass Sie dieses Passwort notieren und an einem sicheren Ort aufbewahren.

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  **Install** . 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.

The screenshot displays the RSA NetWitness Platform Admin console. The top navigation bar includes tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The current view is 'Security' > 'Broker' > 'Users'. A sidebar on the left shows a list of users: 'Broker' and 'admin'. The main content area is titled 'User Information' and contains the following fields:

- Name: Broker
- Username: Broker
- Password: (empty)
- Confirm Password: (empty)
- Email: test@rsa.coim
- Description: (empty)

Below this is the 'User Settings' section:

- Auth Type: NetWitness Platform
- Core Query Timeout: 5
- Query Prefix: (empty)
- Session Threshold: 0

The 'Role Membership' section shows a list of roles with checkboxes:

- Groups
- Administrators
- Aggregation
- Analysts
- Data\_Privacy\_Officers
- Malware\_Analysts
- Operators
- SOC\_Managers

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>	<p>Passwort für die Broker oder Concentrator-Instanz, die Sie als Datenquelle verwenden. Folgende Sonderzeichen werden in einem Passwort unterstützt.</p> <pre>!"#\$%&amp;()*+,-.;&lt;=&gt;?@[\\]^_`{ }</pre> <p>Wenn Sie Sonderzeichen verwenden möchten, müssen Sie das Passwort in gerade Anführungszeichen setzen, zum Beispiel:</p> <pre>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</pre>
-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>	<p>Array von Datenschemata. Wenn Sie mehrere Schemata angeben möchten, verwenden Sie ein Leerzeichen zwischen den Schemata (zum Beispiel 'AUTHENTICATION FILE ACTIVE_DIRECTORY').</p> <div style="border: 1px solid green; padding: 5px;"> <p><b>Hinweis:</b> 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.</p> </div>
-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)

<b>Fehlermeldung</b>	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
<b>Ursache</b>	Es wurde das falsche Passwort für <code>deploy_admin</code> in <code>nwsetup-tui</code> eingegeben.
<b>Lösung</b>	Rufen Sie Ihr Passwort für <code>deploy_admin</code> ab.  <ol style="list-style-type: none"> <li>Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.  <pre>security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password</pre> Stellen Sie über SSH eine Verbindung mit dem fehlgeschlagenen Host her.</li> <li>Führen Sie <code>nwsetup-tui</code> erneut mit dem korrekten Passwort für <code>deploy_admin</code> aus.</li> </ol>

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

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

## Backup (`nw-backup`-Skript)

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

<b>Fehler</b>	<p>Backupfehler aufgrund der Einstellung des Attributs <code>immutable</code>. Hier ist ein Beispiel für einen Fehler, der angezeigt werden kann:</p> <pre>Backing up NetWitness Config (/etc/netwitness) files from: saserver1 WARNING: Errors occurred while backing up NetWitness Configuration files. Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1</pre>
<b>Ursache</b>	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.
<b>Lösung</b>	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: <code>chattr -i &lt;filename&gt;</code>

<b>Fehler</b>	<p>Fehler beim Erstellen der Datei mit Netzwerkkonfigurationsinformationen aufgrund von doppelten oder ungültigen Einträgen in primärer Netzwerkkonfigurationsdatei: /etc/sysconfig/network-scripts/ifcfg-em1</p> <p>Überprüfen Sie den Inhalt von /var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt</p>
<b>Ursache</b>	<p>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.</p>
<b>Lösung</b>	<p>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 &lt;hostname&gt;-&lt;hostip&gt;-network.info.txt haben und die folgenden Einträge enthalten:</p> <pre>DEVICE=&lt;devicename&gt; ; # from the host's primary ethernet interface config file BOOTPROTO=&lt;bootprotocol&gt; ; # from the host's primary ethernet interface config file IPADDR=&lt;value&gt; ; # from the host's primary ethernet interface config file NETMASK=&lt;value&gt; ; # from the host's primary ethernet interface config file GATEWAY=&lt;value&gt; ; # from the host's primary ethernet interface config file search &lt;value&gt; ; # from the host's /etc/resolv.conf file nameserver &lt;value&gt; ; # from the host's /etc/resolv.conf file</pre>

## Event Stream Analysis

<b>Problem</b>	Der ESA-Service stürzt nach dem Upgrade auf 11.2.0.0 aus einem Setup mit FIPS-Aktivierung ab.
<b>Ursache</b>	Der ESA-Service verweist auf einen ungültigen Keystore.
<b>Lösung</b>	<ol style="list-style-type: none"><li>1. Stellen Sie über SSH eine Verbindung mit dem ESA Primary-Host her und melden Sie sich an.</li><li>2. Ersetzen Sie in Datei <code>/opt/rsa/esa/conf/wrapper.conf</code> die folgende Zeile: <code>wrapper.java.additional.5=- Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore</code> durch: <code>wrapper.java.additional.5=- Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore</code></li><li>3. Geben Sie den folgenden Befehl ein, um ESA neu zu starten: <code>systemctl restart rsa-nw-esa-server</code></li></ol> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"><b>Hinweis:</b> 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.</div>

## 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.

<b>Fehlermeldung</b>	<code>&lt;timestamp&gt;.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.</code>
<b>Ursache</b>	Die Log Collector Lockbox konnte nach der Aktualisierung nicht geöffnet werden.
<b>Lösung</b>	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 <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben. Navigieren Sie zu <a href="#">Masterinhaltsverzeichnis</a> , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

<b>Fehlermeldung</b>	<code>&lt;timestamp&gt; NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
<b>Ursache</b>	Die Log Collector Lockbox wird nach der Aktualisierung nicht konfiguriert.
<b>Lösung</b>	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 <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben. Navigieren Sie zu <a href="#">Masterinhaltsverzeichnis</a> , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

<b>Fehlermeldung</b>	<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.
<b>Ursache</b>	Sie müssen das Feld für den Schwellenwert des Stabilitätswerts für die Log Collector Lockbox zurücksetzen.
<b>Lösung</b>	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 <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben. Navigieren Sie zu <a href="#">Masterinhaltsverzeichnis</a> , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

<b>Problem</b>	Sie haben einen Log Collector für das Upgrade vorbereitet und möchten kein Upgrade mehr durchführen.
<b>Ursache</b>	Verzögerungen beim Upgrade.
<b>Lösung</b>	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.

<b>Problem</b>	Nach dem Upgrade bemerken Sie, dass Auditprotokolle nicht zur konfigurierten globalen Audit-Einrichtung weitergeleitet werden oder Die folgende Meldung, angezeigt in <code>sa.log</code> . <code>Syslog Configuration migration failed. Restart jetty service to fix this issue</code>
<b>Ursache</b>	Die globale Audit-Einrichtung des NW-Servers konnte nicht von Version 10.6.6.x auf 11.2.0.0 migriert werden.
<b>Lösung</b>	<ol style="list-style-type: none"> <li>1. Stellen Sie über SSH eine Verbindung mit dem NW-Server her.</li> <li>2. Senden Sie den folgenden Befehl: <code>orchestration-cli-client --update-admin-node</code></li> </ol>

## Orchestrierung

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

<b>Problem</b>	<ol style="list-style-type: none"> <li>1. Es wurde erfolglos versucht, ein Upgrade für einen Nicht-NW-Serverhost durchzuführen.</li> <li>2. Das Upgrade für diesen Host wurde erneut gestartet und war wieder erfolglos.</li> </ol>
<b>Ursache</b>	<p>Die folgende Meldung wird im <code>orchestration-server.log</code> angezeigt. <code>''file' _virtual_ returned False: cannot import name HASHES''</code></p> <p>Es wurde eventuell ein Upgrade für Salt Minion durchgeführt und Salt Minion wurde auf dem fehlerhaften Nicht-NW-Serverhost nicht neu gestartet.</p>
<b>Lösung</b>	<ol style="list-style-type: none"> <li>1. Stellen Sie über SSH eine Verbindung zu dem Nicht-NW-Serverhost her, bei dem das Upgrade fehlgeschlagen ist.</li> <li>2. Senden Sie die folgenden Befehle. <code>systemctl unmask salt-minion</code> <code>systemctl restart salt-minion</code></li> <li>3. Versuchen Sie das Upgrade des Nicht-NW-Serverhosts erneut.</li> </ol>



## 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.

<b>Fehlermeldung</b>	<code>&lt;timestamp&gt; : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ &gt;&lt;existing-GB ] is less than the required space [ &lt;required-GB&gt; ]</code>
<b>Ursache</b>	Die Aktualisierung der Reporting Engine ist fehlgeschlagen, da Sie nicht über ausreichend Speicherplatz verfügen.
<b>Lösung</b>	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 <i>Reporting Engine-Konfigurationsleitfaden</i> . Navigieren Sie zu <a href="#">Masterinhaltsverzeichnis</a> , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

## NetWitness UEBA

<b>Problem</b>	Die Benutzeroberfläche lässt sich nicht aufrufen.
<b>Ursache</b>	Es ist mehr als ein NetWitness UEBA-Service in Ihrer NetWitness-Bereitstellung vorhanden, es ist aber nur ein NetWitness UEBA-Service zulässig.
<b>Lösung</b>	<p>Füllen Sie die folgenden Schritte aus, um den überflüssigen NetWitness UEBA-Service zu entfernen.</p> <ol style="list-style-type: none"> <li>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. <pre># 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</pre> </li> <li>Ermitteln Sie in der Liste der Services, welche Instanz des presidio-airflow-Services entfernt werden soll (mithilfe der Hostadressen).</li> <li>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): <pre># orchestration-cli-client --remove-service --id &lt;ID-for-presidio-airflow-form-previous-output&gt;</pre> </li> <li>Führen Sie den folgenden Befehl aus, um den Node 0 zu aktualisieren, um NGINX wiederherzustellen: <pre># orchestration-cli-client --update-admin-node</pre> </li> <li>Melden Sie sich bei NetWitness Platform an, gehen Sie zu <b>ADMIN &gt; Hosts</b> und entfernen Sie den überflüssigen NetWitness UEBA-Host.</li> </ol>

## Anhang B: Erstellen eines externen Repository

---

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

**Hinweis:** 1.) Auf dem Host muss ein Dienstprogramm zum Entpacken installiert sein, damit Sie dieses Verfahren abschließen können. 2.) Sie müssen wissen, wie Sie einen Webserver erstellen, bevor Sie das folgende Verfahren durchführen.

1. Melden Sie sich bei dem Webserverhost an.
2. Erstellen Sie ein Verzeichnis, um das NW-Repository (`netwitness-11.2.0.0.zip`) zu hosten, z. B. `ziprepo` unter `web-root` des Webserver. Beispiel: Wenn `/var/netwitness` das `web-root`-Verzeichnis ist, senden Sie die folgende Befehlszeichenfolge.  

```
mkdir -p /var/netwitness/<your-zip-file-repo>
```
3. Erstellen Sie das Verzeichnis `11.2.0.0` unter `/var/netwitness/<your-zip-file-repo>`.  

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0
```
4. Erstellen Sie die Verzeichnisse `OS` und `RSA` unter `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.  

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```
5. Entpacken Sie die Datei `netwitness-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.  

```
unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/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/<your-zip-file-repo>/11.2.0.0/OS`.  

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
```

Das folgende Beispiel zeigt, wie die Dateistruktur des Betriebssystems (OS) angezeigt wird, nachdem Sie die Datei entpackt haben.

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

- b. RSA-11.2.0.0.zip in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`.  
`unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`

Das folgende Beispiel zeigt, wie die Dateistruktur der RSA Versionsaktualisierung angezeigt wird, nachdem Sie die Datei entpackt haben.

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

Die externe URL für das Repository ist `http://<web server IP address>/<your-zip-file-repo>`.

7. Verwenden Sie die `http://<web server IP address>/<your-zip-file-repo>` als Antwort auf die Eingabeaufforderung **Geben Sie den Basis-URL des externen Update-Repository ein** des NW 11.2.0.0 Setup-Programms (`nwsetup-tui`).

## Revisionsverlauf

---

Version	Datum	Beschreibung	Verfasser
1,0	17. August 2018	Betriebsfreigabe	IDD
1.1	29. November 2018	Es wurde ein Hinweis auf die Lizenzierung des UEBA-Pfads hinzugefügt.	IDD

