



Leitfaden zur Einrichtung von virtuellen Hosts

für Version 11.0.0.0



Copyright © 1994–2017 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten.

Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Februar 2018

Inhalt

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	8
Empfehlungen zur virtuellen Umgebung	8
Empfohlene Systemanforderungen für virtuelle Hosts	9
Szenario eins	9
Szenario zwei	11
Szenario drei	13
Log Collector (Lokal und Remote)	14
Richtlinien zur Dimensionierung von Legacy-Windows-Collectors	14
Installieren des virtuellen NetWitness Suite-Hosts in einer virtuellen Umgebung	15
Voraussetzungen	15
Schritt 1. Bereitstellen des virtuellen Hosts	15
Voraussetzungen	15
Verfahren	16
Schritt 2. Konfigurieren des Netzwerks und Installieren der RSA NetWitness-Suite	19
Voraussetzungen	19
Verfahren	19
Überprüfen von offenen Firewallports	19
Installationsaufgaben	19
Schritt 3. Konfigurieren der Datenbanken zur Unterstützung von NetWitness Suite	36
Aufgabe 1. Überprüfen der Datenspeicher-Erstkonfiguration	37
Anfänglich der PacketDB zugewiesener Speicherplatz	37
Ursprüngliche Datenbankgröße	37
PacketDB-Mount-Punkt	38
Aufgabe 2. Überprüfen der optimalen Speicherplatzkonfiguration des Datenspeichers	39

Speicherplatzverhältnisse auf virtuellen Laufwerken	39
Aufgabe 3: Hinzufügen eines neuen Volume und Erweitern von vorhandenen Dateisystemen	41
Erstellen Sie ein physisches LVM-Volume auf einer neuen Partition.	48
Schritt 4. Konfigurieren von hostspezifischen Parametern	53
Konfigurieren der Protokollaufnahme in der virtuellen Umgebung	53
Konfigurieren der Paketerfassung in der virtuellen Umgebung	54
Verwenden eines Virtual Tap eines Drittanbieters	54

Leitfaden zur Einrichtung von virtuellen Hosts

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

Grundlegende virtuelle Bereitstellungen

Dieses Thema enthält allgemeine Guidelines und Anforderungen für die Bereitstellung von RSANetWitness Suite 11.0.0.0 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)

Abkürzungen	Beschreibung
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)

Unterstützte virtuelle Hosts

Sie können die folgenden NetWitness Suite-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

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 Suite-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.
- Für OVA sind 32 GB RAM pro Host-Appliance erforderlich.
- 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 Suite 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 Suite“ 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 für eine 11.0.0.0-Installation anders ausfallen, wenn Sie die neuen Funktionen und Verbesserungen installieren und ausprobieren.

Szenario eins

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 Packet 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

Packet 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 zwei

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 Packet Decoder, Concentrator und Warehouse Connector.
- Event Stream Analysis wurde bei 90.000 EPS von drei Hybrid Concentrators aggregiert.
- Incident-Management erhielt Warnmeldungen von der Reporting Engine und von Event Stream Analysis.
- Die Hintergrundlast umfasste Berichte, Diagramme, Warnmeldungen, Ermittlungen und Incident-Management.
- 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

Packet 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 GHz	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

NetWitness-Server und Komponenten am selben Standort

NetWitness-Server, Jetty, Broker, Incident-Management und Reporting Engine befinden sich im gleichen Verzeichnis.

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

Szenario drei

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 Packet Decoder und den Concentrator.
- Event Stream Analysis wurde bei 90.000 EPS von drei Hybrid Concentrators aggregiert.
- Incident-Management 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

Packet 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

Richtlinien zur Dimensionierung von Legacy-Windows-Collectors

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

Installieren des virtuellen NetWitness Suite-Hosts in einer virtuellen Umgebung

Schließen Sie die folgenden Verfahren in der nummerierten Reihenfolge ab, um RSA NetWitness® Suite 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.
- Einen installierten vSphere 4.1-Client oder vSphere 5.0-Client, um sich beim VMware-ESX-Server anzumelden.
- Administratorrechte zum Erstellen der virtuellen Maschinen im VMware-ESX-Server

Schritt 1. Bereitstellen des virtuellen Hosts

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:

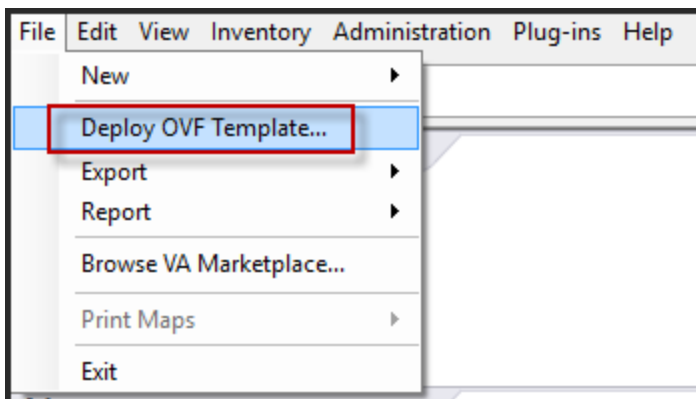
- Netzwerk-IP-Adressen, Netzmaske und Gateway-IP-Adressen für den virtuellen Host
- Netzwerknamen für alle virtuellen Hosts, wenn Sie ein Cluster erstellen
- DNS- oder Hostinformationen
- Passwort für den virtuellen Hostzugriff. Der Standardbenutzername lautet `root`, das Standardpasswort `netwitness`.
- Die Paketdatei NetWitness Suite für den virtuellen Host. (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.

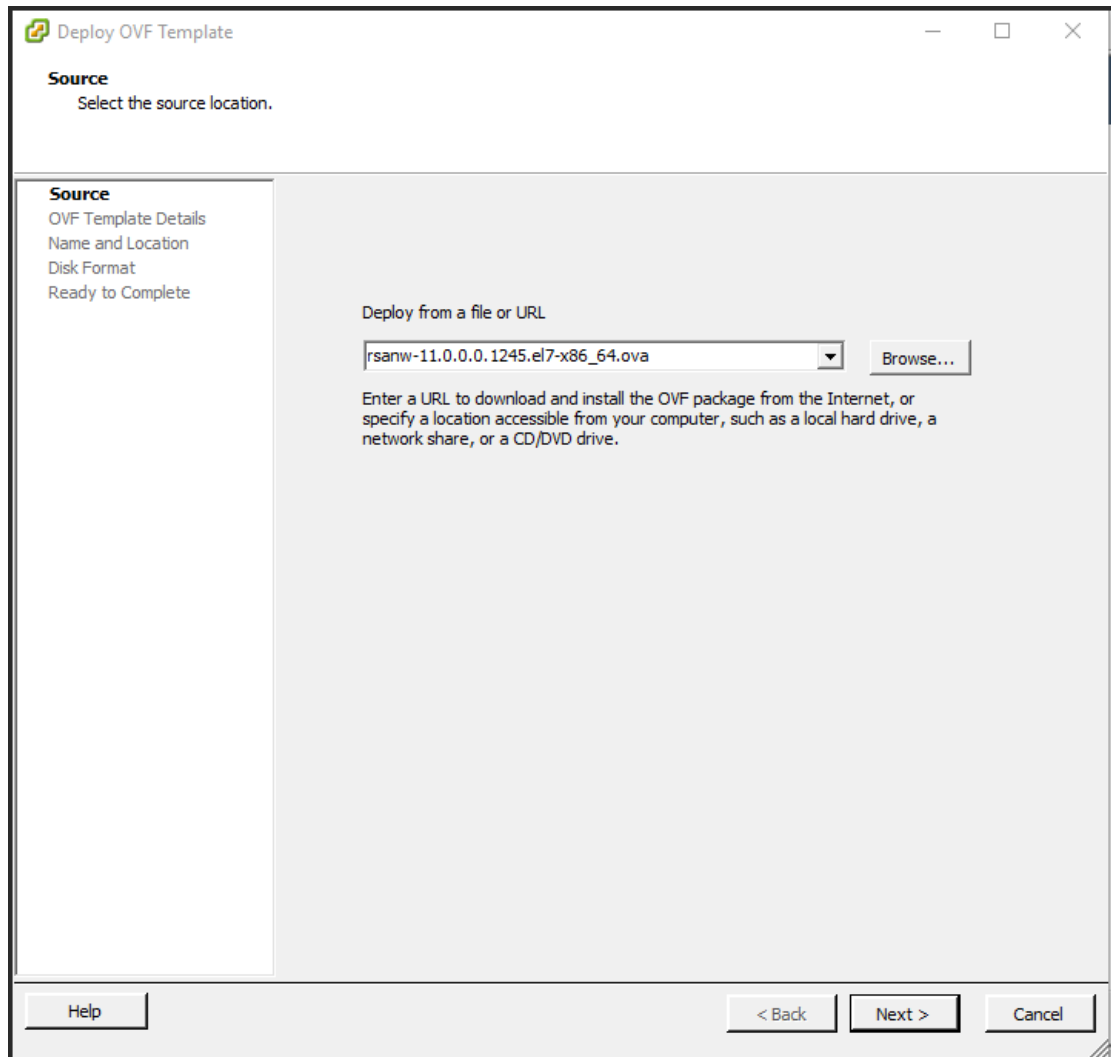
So stellen Sie den OVA-Host bereit:

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

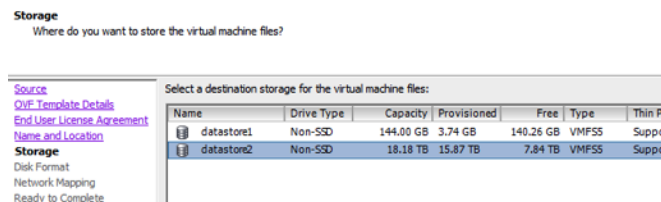


3. Das Dialogfeld „OVF-Vorlage bereitstellen“ wird geöffnet. Wählen Sie im Dialogfeld **OVF-Vorlage bereitstellen** das OVF für den Host aus, den Sie in der virtuellen Umgebung bereitstellen möchten (z. B. **V11.0 GOLD\OVFImge\v11_SA_OVF\nwreux_OVF11.ovf**),

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.

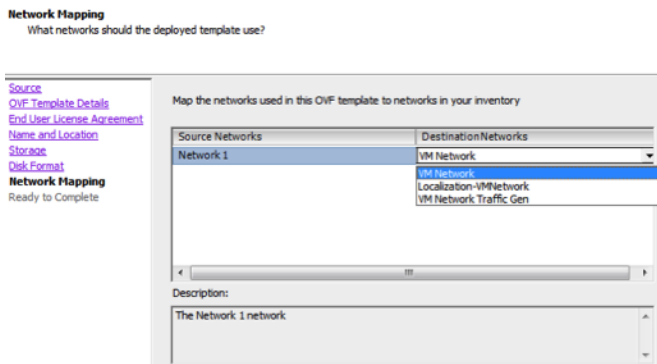


6. Geben Sie bei den Speicheroptionen den Datenspeicherort für den virtuellen Host an.

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 Suite-Datenbanken auf bestimmten Hosts benötigt wird (dies wird in den folgenden Abschnitten behandelt).

7. Klicken Sie auf **Weiter**.

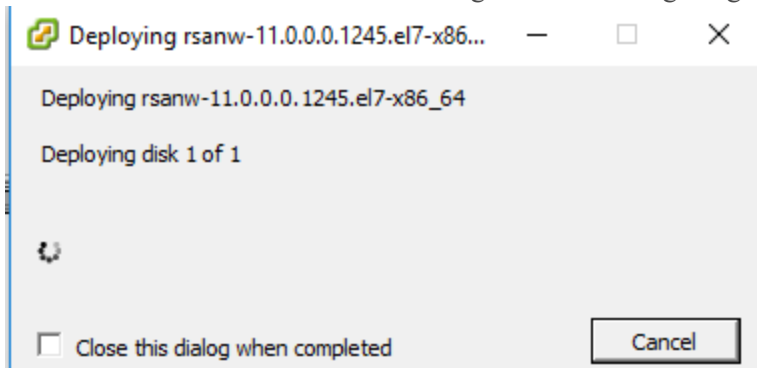
Die Optionen für Netzwerkzuordnung werden eingeblendet.



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 und Installieren der RSA NetWitness-Suite

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

Voraussetzungen

Vergewissern Sie sich, dass Sie über Folgendes verfügen:

- 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 Suite-Hilfe, um NetWitness Suite-Services und Ihre Firewalls zu konfigurieren.

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

Es gibt zwei Hauptaufgaben, die in der angegebenen Reihenfolge durchgeführt werden müssen, um NetWitness Suite 11.0.0.0 zu installieren.

Installationsaufgaben

Aufgabe 1: Installieren von 11.0.0.0 auf dem NetWitness-Server (Node 0)

Aufgabe 2: Installieren von 11.0.0.0 auf anderen NetWitness Suite-Komponenten (Node x)

Aufgabe 1: Installieren von 11.0.0.0 auf dem NetWitness-Server (Node 0)

Bei dieser Aufgabe wird auf dem Host, den Sie für den NW-Server (Node 0) bereitgestellt haben, Folgendes installiert:

- Die 11.0.0.0-Umgebungsplattform für NW-Server.
 - Die Komponenten der NW-Server (Administration, Konfiguration, Orchestrierung, Servicemanagement und Sicherheitsservices).
 - Ein Repository mit den RPM-Dateien, die für die Installation von anderen Funktionskomponenten oder Services erforderlich sind.
1. Stellen Sie die 11.0.0.0 Umgebung bereit:
 - a. Stellen Sie Hosts bereit.
 - 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 nach dem Setup DNS-Server erreichen müssen, die während des Setups nicht erreichbar waren, (z. B. zur Verlagerung eines Hosts, der über andere DNS-Server verfügt) lesen Sie [Aufgabe 1. Erneutes Konfigurieren von DNS-Servern nach 11.0.0.0](#) 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 Suite Repository aktualisieren** in Schritt 12 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repo zugreifen kann).

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

<Accept >

<Decline>

92%

3. Gehen Sie zu **Akzeptieren** und drücken Sie die EINGABETASTE.
Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.

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

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

< Yes >

< No >

4. Gehen Sie zu **Ja** und drücken Sie die EINGABETASTE.
Wählen Sie **Nein**, wenn Sie 11.0.0.0 bereits auf dem NW-Server installiert haben.

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

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

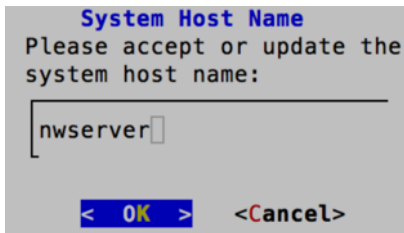
NetWitness Suite 11.0 Install or Upgrade
Specify if you are installing NetWitness for the first time or upgrading from a previous version:

1 Install (Fresh Install)
2 Upgrade (From Previous Vers.)

< OK >

< Exit >

5. Drücken Sie die EINGABETASTE (standardmäßig ist „Installation“ ausgewählt).
Die Aufforderung „Hostname“ wird angezeigt.



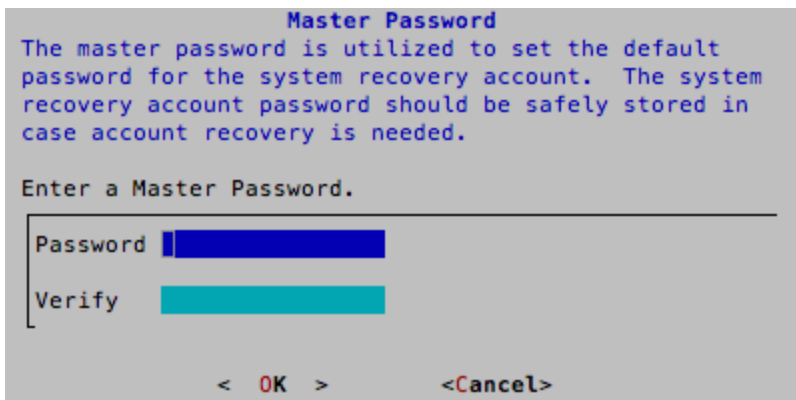
6. Drücken Sie die EINGABETASTE, wenn dieser Name beibehalten werden soll. Wenn Sie den Hostnamen bearbeiten möchten, gehen Sie zu **OK** und drücken Sie die EINGABETASTE, um ihn zu ändern.

Die Aufforderung „Masterpasswort“ wird angezeigt.

Für das Masterpasswort und das Bereitstellungspasswort werden folgende Zeichen unterstützt:

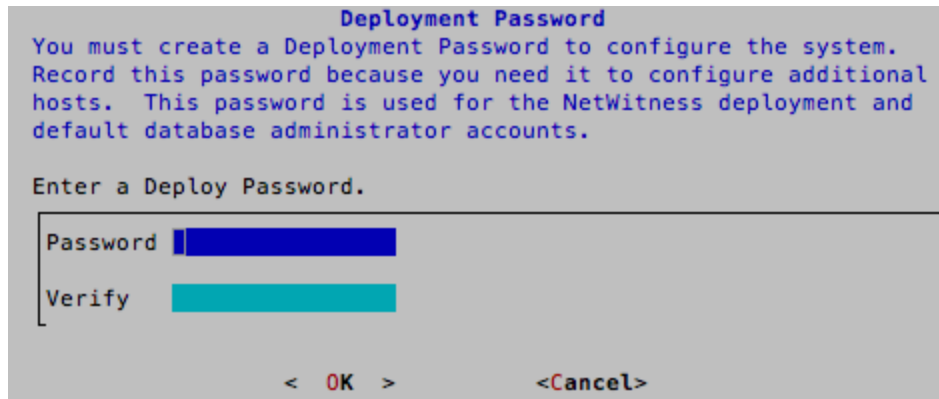
- Symbole: ! @ # % ^ +
- Zahlen: 0–9
- Kleinbuchstaben: a-z
- Großbuchstaben: A-Z

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



7. Gehen Sie mit dem Pfeil nach unten zu **Passwort** 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.

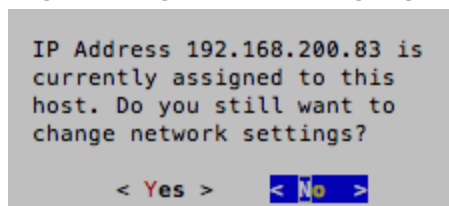
Die Aufforderung „Bereitstellungspasswort“ wird angezeigt.



8. Gehen Sie mit dem Pfeil nach unten zu **Passwort** 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.

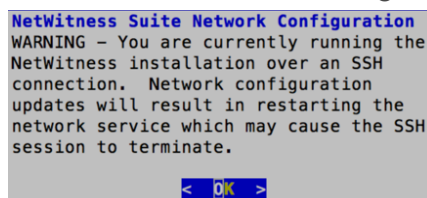
Bedingte Eingabeaufforderungen:

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



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

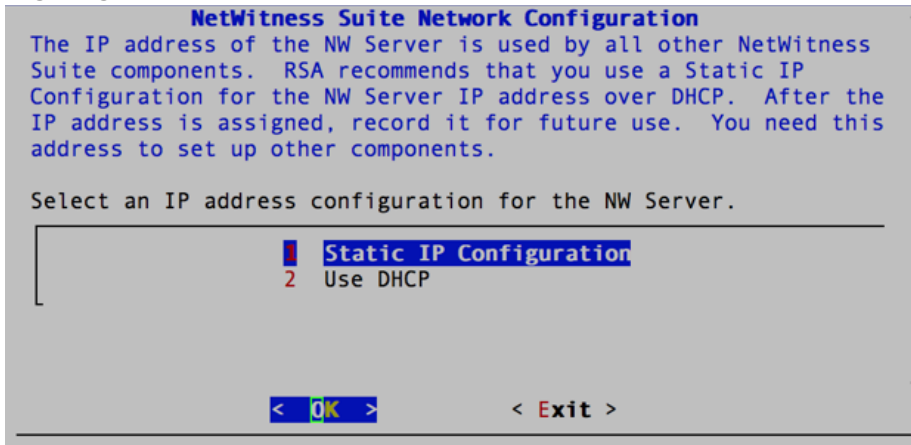
- Wenn Sie eine SSH-Verbindung verwenden, wird die folgende Warnung angezeigt:



Drücken Sie die EINGABETASTE, um die Warnung zu schließen.

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

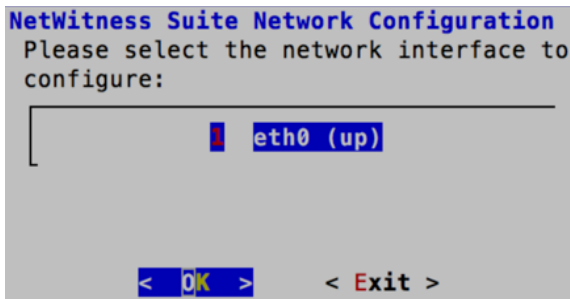
Wenn keine IP-Konfiguration gefunden wurde oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung „Netzwerkkonfiguration“ angezeigt.



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

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

Die Eingabeaufforderung „Netzwerkkonfiguration“ wird angezeigt.



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

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

```
NetWitness Suite Network Configuration
Static IP configuration

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

< OK >      < Exit >
```

11. Geben Sie die Konfigurationswerte (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 **Alle Felder sind Pflichtfelder** angezeigt (die Felder **Primärer DNS-Server**, **Sekundärer DNS-Server** und **Lokaler Domainname** sind nicht erforderlich).

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

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

Die Eingabeaufforderung „Repository für Aktualisierungen“ wird angezeigt.

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

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

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

< OK >      < Exit >
```

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

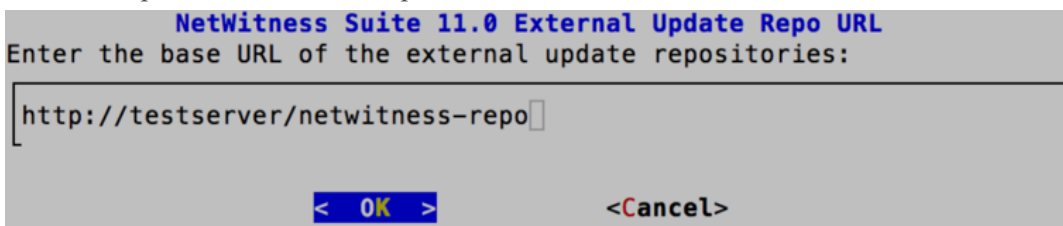
Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten

zu **Externes Repository** und dann zu **OK** und drücken Sie die EINGABETASTE.

- Bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** stellt das Setup-Programm sicher, dass Sie die richtigen Medien mit dem Host verbunden haben (d. h. einen Build-Stick oder eine DVD), von denen aus die Installation oder Aktualisierung der Hosts auf NetWitness Suite 11.0.0.0 abgerufen werden kann. Wenn das Programm die verbundenen Medien nicht finden kann, wird die folgende Aufforderung angezeigt:

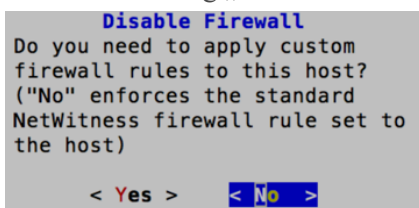


- Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe einer URL aufgefordert. Die Repositories bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates.



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

Die Aufforderung „Firewall deaktivieren“ wird angezeigt.



13. Aufgabe

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

Die Aufforderung zur Bestätigung der Deaktivierung der Firewallkonfiguration wird angezeigt.

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

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

< Yes > < No >
```

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

Die Aufforderung „Installation starten“ wird angezeigt.

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

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

1 Install Now
2 Restart

< OK > < Exit >
```

14. Drücken Sie die EINGABETASTE, um 11.0.0.0 auf dem NW-Server zu installieren.
Wenn „Installation abgeschlossen“ angezeigt wird, haben Sie den 11.0.0.0 NW-Server auf diesem Host installiert.

Aufgabe 2: Installieren von 11.0 auf anderen NetWitness Suite-Komponenten (Node x)

Für einen funktionalen Servicehost (Node x) wird durch diese Aufgabe Folgendes ausgeführt:

- Installation der 11.0.0.0-Umgebungsplattform.
 - Anwendung der 1-RPM-Dateien aus dem Repository für NW-Serveraktualisierungen auf den Service.
1. Stecken Sie den Build-Stick am Host ein.
In „RSA NetWitness® Suite Build-Stick“ finden Sie Informationen zum Erstellen eines Build-Sticks.
 2. Installieren Sie die CentOS7 als Hostbetriebssystem.
Anweisungen hierzu finden Sie unter [Anhang A: Installieren von CentOS7 auf dem Host](#).
 3. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.
Dadurch wird das Setup-Programm gestartet und die EULA wird angezeigt.

Hinweis: Wenn Sie während des Setup-Programms (`nwsetup-tui`) die DNS-Server angeben, MÜSSEN diese gültig („gültig“ in diesem Zusammenhang bedeutet gültig während des Setups) und für `nwsetup-tui` zugänglich sein, damit Sie fortfahren können. Falsch konfigurierte DNS-Server führen dazu, dass die Konfiguration fehlschlägt. Wenn Sie den DNS-Server beim Setup erreichen müssen, dieser aber während des Setups nicht erreichbar ist (z. B. um einen Host nach dem Setup zu verlagern, der über andere DNS-Server verfügt) lesen Sie [Erneutes Konfigurieren von DNS-Servern nach 11.0.0.0](#). Wenn Sie keinen DNS-Server während `nwsetup-tui` angeben, müssen Sie **1 Lokales Repository (auf dem NW-Server)** in der Eingabeaufforderung **NetWitness Suite Repository aktualisieren** in Schritt 12 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repo 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>

4. Gehen Sie zu **Akzeptieren** und drücken Sie die EINGABETASTE. Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.

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

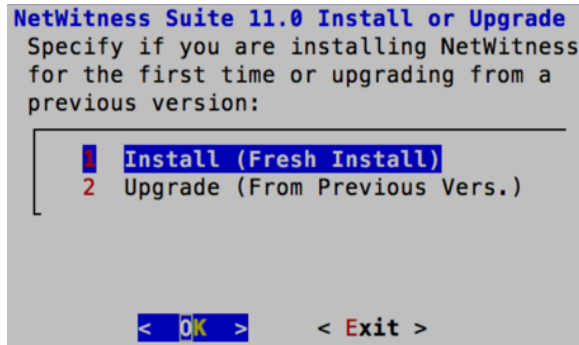
Is this the host you want for your 11.0 NW Server?

< Yes >

< No >

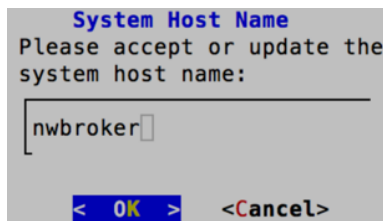
5. Drücken Sie die EINGABETASTE (Nein).

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



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

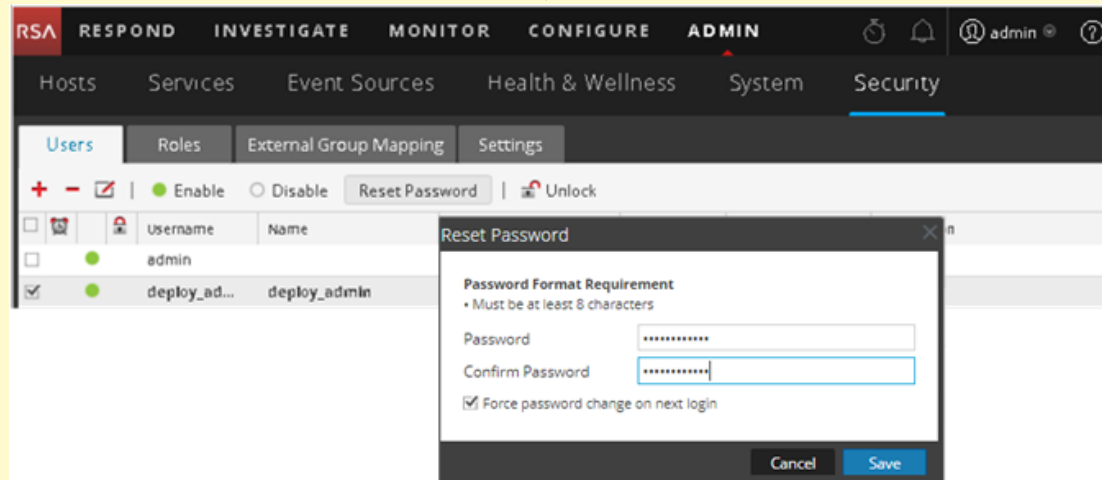
Die Aufforderung „Hostname“ wird angezeigt.



7. 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.

Achtung:**Szenario 1**

Wenn Sie nach dem Upgrade des NW-Servers auf 11.0.0.0 das Benutzerpasswort **deploy_admin** in der NetWitness Suite-Benutzeroberfläche (**ADMIN > Sicherheit > deploy_admin** auswählen – **Passwort zurücksetzen**) ändern,



müssen Sie folgende Schritte ausführen:

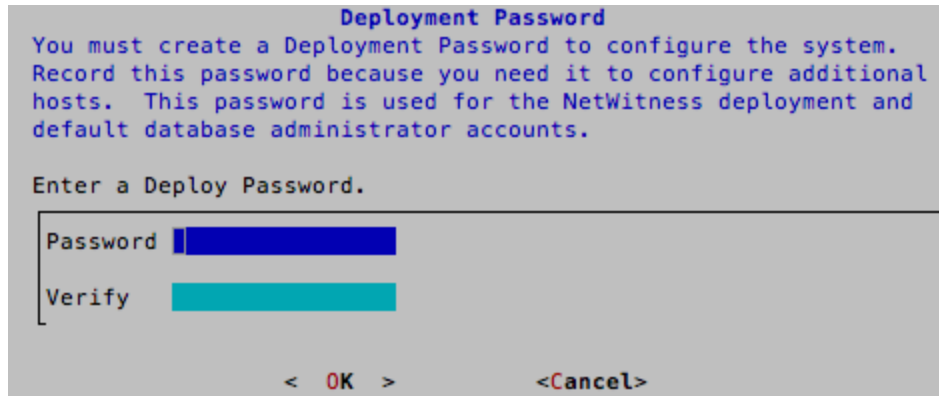
1. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
2. Führen Sie das (`/opt/rsa/saTools/bin/set-deploy-admin-password`-Skript aus.
3. Verwenden Sie das neue Passwort, wenn Sie Upgrades für neue Nicht-NW-Serverhosts durchführen.

Szenario 2

Wenn Sie nach dem Upgrade des NW-Servers und einer beliebigen Anzahl von Nicht-NW-Serverhosts auf 11.0.0.0 das Benutzerpasswort **deploy_admin** in der NetWitness Suite-Benutzeroberfläche ändern, müssen Sie folgende Schritte ausführen:

1. Führen Sie das (`/opt/rsa/saTools/bin/set-deploy-admin-password`-Skript auf allen Nicht-NW-Serverhosts in Ihrer Bereitstellung aus.
2. Notieren Sie sich das Passwort, da Sie es möglicherweise zu einem späteren Zeitpunkt bei der Installation benötigen.

Die Aufforderung „Bereitstellungspasswort“ wird angezeigt.

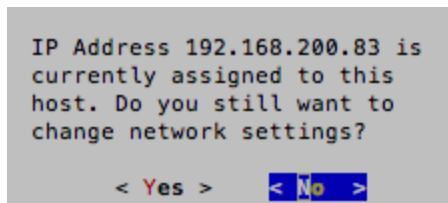


Hinweis: Sie müssen das gleiche Bereitstellungspasswort verwenden, das Sie beim Upgrade des NW-Servers verwendet haben.

8. Gehen Sie mit dem Pfeil nach unten zu **Passwort** 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.

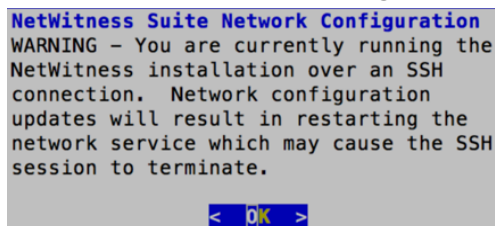
Bedingte Eingabeaufforderungen:

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



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

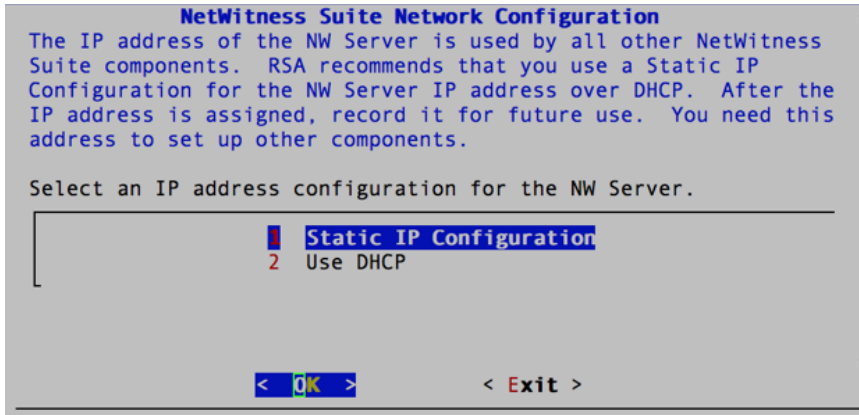
- Wenn Sie eine SSH-Verbindung verwenden, wird die folgende Warnung angezeigt:



Drücken Sie die EINGABETASTE, um die Warnung zu schließen.

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

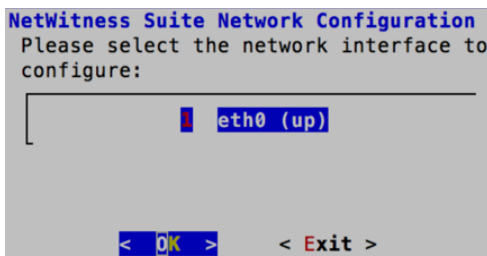
Wenn keine IP-Konfiguration gefunden wurde oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung „Netzwerkconfiguration“ angezeigt.



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

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

Die Eingabeaufforderung „Netzwerkconfiguration“ wird angezeigt.



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

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

```

NetWitness Suite Network Configuration
Static IP configuration

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

< OK >        < Exit >
    
```

11. Geben Sie die Konfigurationswerte (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 **Alle Felder sind Pflichtfelder** angezeigt (die Felder „Primärer DNS-Server“, „Sekundärer DNS-Server“ und „Lokaler Domainname“ sind nicht erforderlich).
 Bei Verwendung der falschen Syntax oder Zeichenlänge für eines der Felder wird die Fehlermeldung **Ungültiger Feldname** angezeigt.

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

Die Eingabeaufforderung „Repository für Aktualisierungen“ wird angezeigt.
 Wählen Sie für alle Hosts das gleiche Repository aus, das Sie beim Upgrade des NW-Serverhosts ausgewählt haben.

```

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

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

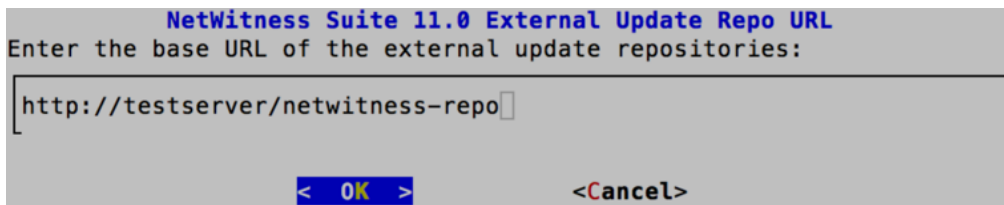
1 The Local Repo (on the NW Server)
2 An External Repo (on an externally-managed server)

< OK >        < Exit >
    
```

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

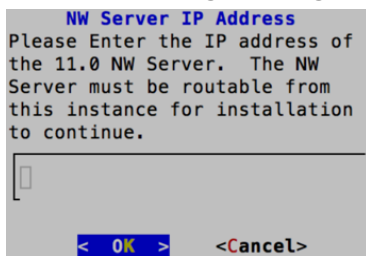
Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **Externes Repository** und dann zu **OK** und drücken Sie die EINGABETASTE.

- Bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** stellt das Setup-Programm sicher, dass Sie die richtigen Medien mit dem Host verbunden haben (d. h. einen Build-Stick oder eine DVD), von denen aus die Installation oder Aktualisierung der Hosts auf NetWitness Suite 11.0.0.0 abgerufen werden kann.
- Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe einer URL aufgefordert. Die Repositories bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates.



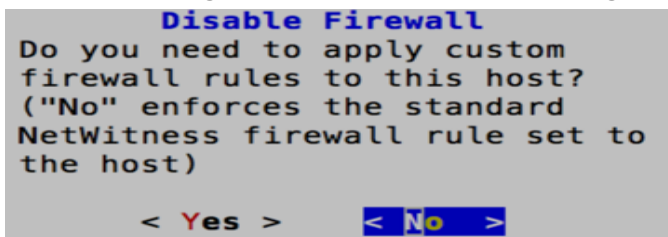
Geben Sie die Basis-URL für das externe NetWitness Suite-Repository ein und klicken Sie auf **OK**.

Die Aufforderung zur Eingabe der 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.

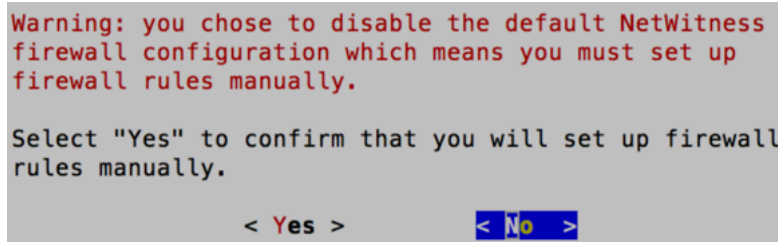
Die Aufforderung „Firewall deaktivieren“ wird angezeigt.



14. Aufgabe

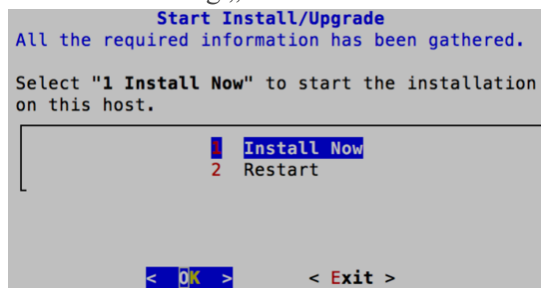
- Um die Standardkonfiguration für Firewalls anzuwenden, drücken Sie die EINGABETASTE.
- Um die Standardkonfiguration zu deaktivieren, gehen Sie zu **Ja** und drücken Sie die EINGABETASTE.

Die Aufforderung zur Bestätigung der Deaktivierung der Firewallkonfiguration wird angezeigt.



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

Die Aufforderung „Installation starten“ wird angezeigt.





15. Drücken Sie die EINGABETASTE, um 11.0.0.0 auf dem NW-Server zu installieren. Wenn „Installation abgeschlossen“ angezeigt wird, verfügen Sie über einen generischen Host (Node x) mit einem Betriebssystem, das mit NetWitness Suite 11.0.0.0 kompatibel ist.
16. Installieren Sie einen Komponentendienst auf dem Host (Node x).

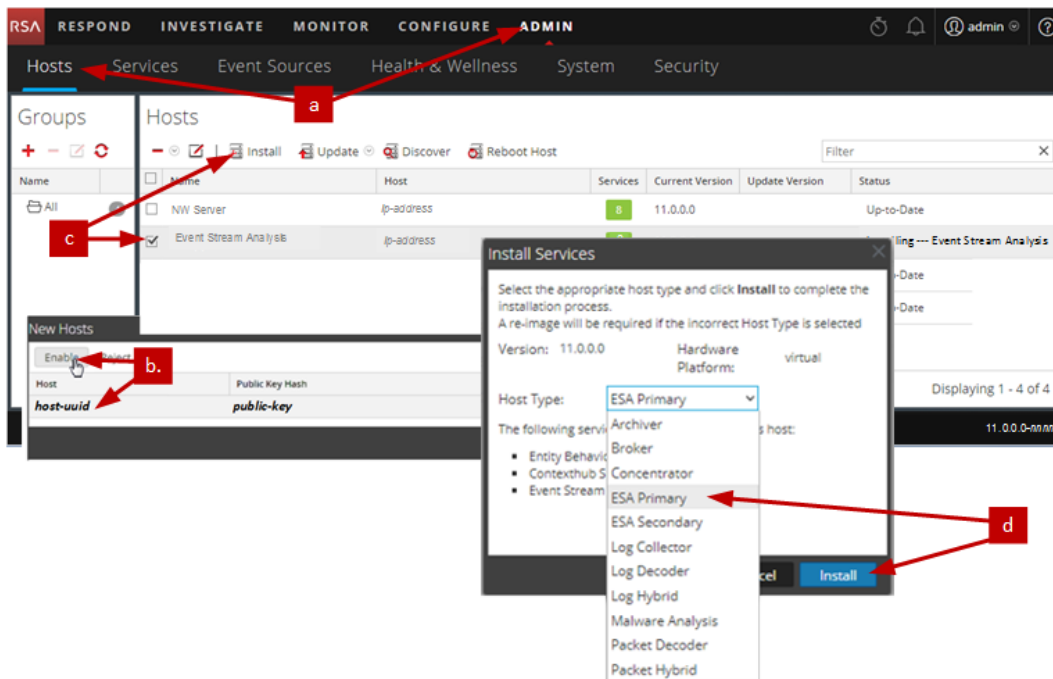
- a. Klicken Sie auf **ADMIN > Hosts**.

Das Dialogfeld **Neue Hosts** wird angezeigt. Die Ansicht **Hosts** ist im Hintergrund abgeblendet.

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

- b. Wählen Sie einen Nicht-NW-Serverhost aus der Ansicht **Hosts** aus.

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



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

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

Schritt 3. Konfigurieren der Datenbanken zur Unterstützung von NetWitness Suite

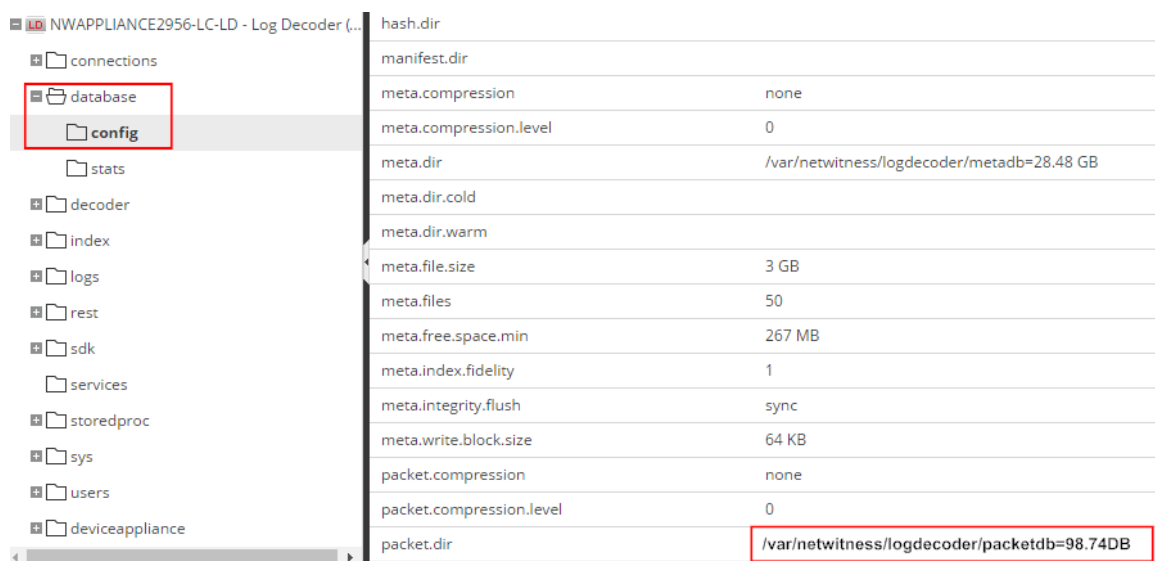
Wenn Sie Datenbanken von OVA bereitstellen, reicht die erste Datenbankspeicherplatzzuordnung möglicherweise nicht aus, um NetWitness-Server zu unterstützen. Sie müssen den Status der Datenspeicher nach der ersten Bereitstellung überprüfen und diese erweitern.

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 sehr klein (ca. 98 GB). Das folgende Beispiel für die NetWitness Suite-Ansicht „Durchsuchen“ zeigt die Größe der PacketDB, nachdem Sie diese anfänglich aus OVA bereitgestellt haben.



Parameter	Value
hash.dir	
manifest.dir	
meta.compression	none
meta.compression.level	0
meta.dir	/var/netwitness/logdecoder/metadb=28.48 GB
meta.dir.cold	
meta.dir.warm	
meta.file.size	3 GB
meta.files	50
meta.free.space.min	267 MB
meta.index.fidelity	1
meta.integrity.flush	sync
meta.write.block.size	64 KB
packet.compression	none
packet.compression.level	0
packet.dir	/var/netwitness/logdecoder/packetdb=98.74DB

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@nwappliance32431 ~]# df -k
Filesystem            1K-blocks    Used Available Use% Mounted on
/dev/mapper/netwitness_vg00-root 31441920 3148972 28292948 11% /
devtmpfs              16462812     0 16462812  0% /dev
tmpfs                 16474132     12 16474120  1% /dev/shm
tmpfs                 16474132  41492 16432640  1% /run
tmpfs                 16474132     0 16474132  0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome 10475520  32984 10442536  1% /home
/dev/mapper/netwitness_vg00-varlog  10475520  72868 10402652  1% /var/log
/dev/mapper/netwitness_vg00-nwhome 146950036 399908 146550128  1% /var/netwitness
/dev/sda1             1038336  88448  949888  9% /boot
tmpfs                  3294828     0  3294828  0% /run/user/0
```

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@nwappliance32431 ~]# lvs netwitness_vg00
LV      VG          Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao--- 140.21g
root    netwitness_vg00 -wi-ao--- 30.00g
swap    netwitness_vg00 -wi-ao--- 4.00g
usrhome netwitness_vg00 -wi-ao--- 10.00g
varlog  netwitness_vg00 -wi-ao--- 10.00g
```

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@nwappliance32431 ~]# 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@nwappliance32431 ~]# 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 Suite-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 [Tuningleitfaden für die RSA NetWitness Suite-Core-Datenbank](#). (2.) Wenden Sie sich an die Kundenbetreuung, um Unterstützung beim Konfigurieren Ihrer virtuellen Laufwerke und Verwenden des Dimensionierungs- und Umfangsrechners.

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

Concentrator		
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:

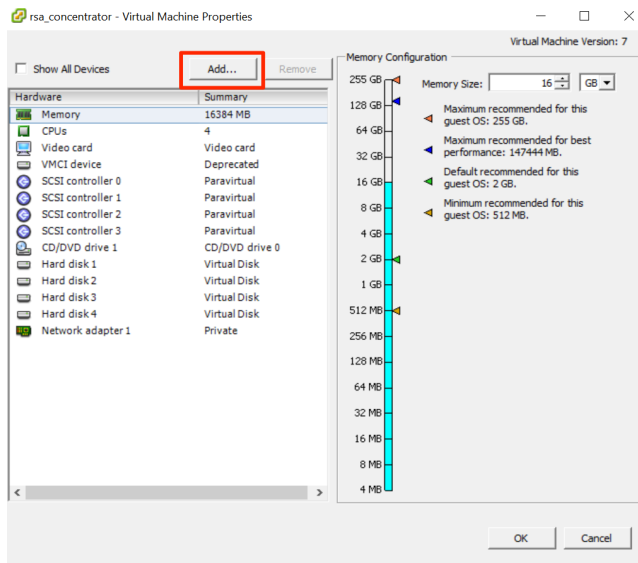
1. Fügen Sie eine neue Festplatte hinzu.
2. Erstellen Sie neue Volumes auf der neuen Festplatte.
3. Erstellen Sie ein physisches LVM-Volume auf einer neuen Partition.
4. Erweitern Sie die Volume-Gruppe um physisches Volume
5. Erweitern Sie das Dateisystem.
6. Starten Sie die Services.
7. Stellen Sie sicher, dass die Services ausgeführt werden.
8. Konfigurieren Sie Log Decoder-Parameter neu.

Fügen Sie eine neue Festplatte hinzu.

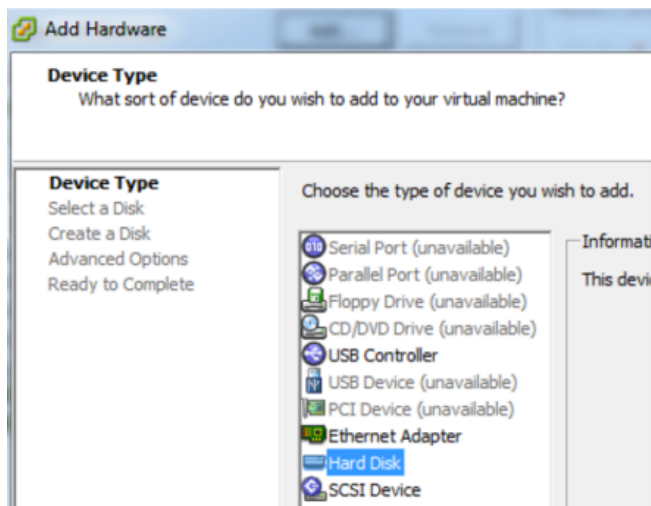
Dieses Verfahren zeigt, wie Sie ein neues 100-GB-Laufwerk auf demselben Datenspeicher hinzufügen.

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

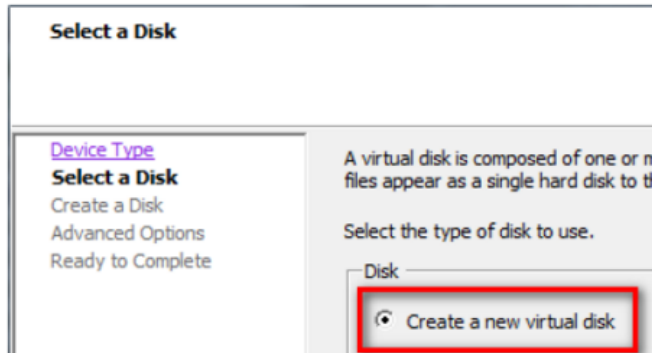
1. Fahren Sie die Maschine herunter, bearbeiten Sie die **Eigenschaften der virtuellen Maschine**, klicken Sie auf die Registerkarte **Hardware** und klicken Sie auf **Hinzufügen**.



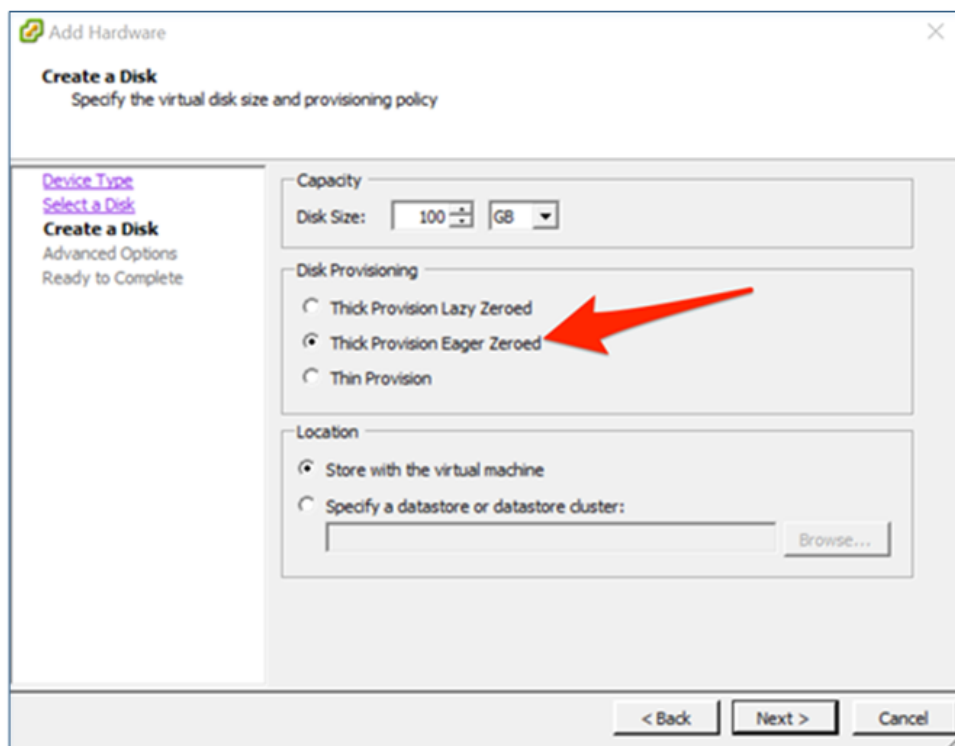
2. Wählen Sie als Gerätetyp **Festplattenlaufwerk** aus.



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.

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node:

Mode:

- Independent
Independent disks are not affected by snapshots.
- Persistent
Changes are immediately and permanently written to the disk.
- Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.

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

6. Bestätigen Sie die Einstellungen.

Options:

Hardware type:	Hard Disk
Create disk:	New virtual disk
Disk capacity:	100 GB
Datastore:	date:storage
Virtual Device Node:	SCSI (0:4)
Disk mode:	Persistent

7. Virtuelle Maschine > Status
8. Verbinden Sie sich per SSH mit der Maschine.
9. Starten Sie die Maschine neu und geben Sie den folgenden Befehl ein.

```
lsblk
```

Die folgende Ausgabe wird mit der neuen Festplatte angezeigt.

```

[root@NWAPPLIANCE2599 database]# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
fd0                                  2:0      1    4K  0 disk
sda                                  8:0      0 195.3G  0 disk
├─sda1                               8:1      0     1G  0 part /boot
└─sda2                               8:2      0 194.3G  0 part
   ├─netwitness_vg00-nwhome          253:15   0 140.2G  0 lvm  /var/netwitness
   ├─netwitness_vg00-varlog          253:16   0    10G  0 lvm  /var/log
   ├─netwitness_vg00-usrhome         253:17   0    10G  0 lvm  /home
   ├─netwitness_vg00-root            253:18   0   30G  0 lvm  /
   └─netwitness_vg00-swap            253:19   0     4G  0 lvm  [SWAP]
sdb                                  8:16     0   48G  0 disk
├─sdb1                              8:17     0   48G  0 part
│   ├─VolGroup00-usr                253:6    0     4G  0 lvm
│   ├─VolGroup00-usrhome            253:7    0     2G  0 lvm
│   ├─VolGroup00-var                 253:8    0     4G  0 lvm
│   ├─VolGroup00-log                 253:9    0     4G  0 lvm
│   ├─VolGroup00-tmp                 253:10   0     6G  0 lvm
│   ├─VolGroup00-vartmp              253:11   0     2G  0 lvm
│   ├─VolGroup00-opt                 253:12   0     4G  0 lvm
│   ├─VolGroup00-rabmq               253:13   0    10G  0 lvm
│   └─VolGroup00-nwhome              253:14   0    12G  0 lvm
└─sdc                               8:32     0  104G  0 disk
   ├─sdc1                           8:33     0  104G  0 part
   │   ├─VolGroup01-decoroot          253:0    0     20G  0 lvm  /var/netwitness/logdecoder
   │   ├─VolGroup01-index            253:1    0     10G  0 lvm  /var/netwitness/logdecoder/index
   │   ├─VolGroup01-sessiondb        253:2    0     30G  0 lvm  /var/netwitness/logdecoder/sessiondb
   │   └─VolGroup01-metadb           253:3    0     44G  0 lvm  /var/netwitness/logdecoder/metadb
   └─sdd                             8:48     0  168G  0 disk
      ├─sdd1                         8:49     0  168G  0 part
      │   ├─VolGroup01-logcoll        253:4    0     64G  0 lvm  /var/netwitness/logcollector
      │   └─VolGroup01-packetdb       253:5    0    104G  0 lvm  /var/netwitness/logdecoder/packetdb
      └─sde                           8:64     0    10G  0 disk
sr0                                  11:0     1  1024M  0 rom
[root@NWAPPLIANCE2599 database]#

```

Hinweis: 1.) Sie erhalten die Fehlermeldung **Unbekannte Partitionstabelle**, da das neue Laufwerk nicht initialisiert wurde. 2.) Die **sd 2:0:4:0** gehört zu dem virtuellen Geräte-Node **SCSI:0:4**, der angezeigt wurde, als Sie das neue Gerät hinzugefügt haben. 3.) Das neue Festplattengerät ist **sde** (oder `/dev/sde`).

10. Geben Sie die folgende Befehlszeichenfolge ein, um den Service zu beenden.

```
root@LogDecoderGM ~] # service nwlogcollector stop; service
nwlogdecoder stop.
```

Dieses Verfahren verwendet den Log Decoder als Beispiel.

Wenn Sie Services auf einem Concentrator beenden möchten, geben Sie Folgendes ein:

```
service nwconcentrator stop
```

Wenn Sie Services auf einem Packet Decoder beenden möchten, geben Sie Folgendes ein:

```
service nwdecoder stop
```

Erstellen von Volumes auf der neuen Festplatte

1. Stellen Sie über SSH eine Verbindung zum Log Decoder-Host her.
2. Erstellen Sie eine Partition auf der neuen Festplatte und ändern Sie dessen Typ zu Linux

LVM.

```
[root@NWAPPLIANCE2599 ~]# fdisk /dev/sde
```

Die folgenden Informationen und die folgende Aufforderung werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x7cab96b5.

Command (m for help): _
```

3. Geben Sie `p` ein.

Die folgenden Informationen werden angezeigt:

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
Command (m for help):
```

Der Standardtyp für die Partition ist **Linux (83)**. Sie müssen ihn zu **Linux LVM (8e)** ändern.

4. Geben Sie `n` ein.

Die folgende Aufforderung wird angezeigt:

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set

Command (m for help): _
```

Partition 1 vom Typ Linux mit 10 GB Größe ist eingestellt

1. Geben Sie an der Command m for help:-Befehlsaufforderung t ein.

Die folgenden Informationen und die folgende Aufforderung werden angezeigt:

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help):
```

2. Geben Sie 8e ein.

Die folgenden Informationen und die folgende Aufforderung werden angezeigt:

Changed system type of partition 1 to 8e (Linux LVM).

Command (m for help):

3. Geben Sie p ein.

Die folgenden Informationen werden angezeigt:

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1          2048     20971519     10484736   8e  Linux LVM

Command (m for help):
```

4. Geben Sie an der Command (m for help):-Befehlsaufforderung w ein.

Die neue Partitionstabelle wird auf die Festplatte geschrieben und fdisk wird zur Root-Shell beendet.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
[ 9838.504920] sde: sde1
Syncing disks.
[root@NWAPPLIANCE2599 database1]# _
```

Die neue /dev/sde1-Partition wird auf der neuen Festplatte erstellt.

5. Führen Sie einen der folgenden Schritte aus, um sicherzustellen, dass die neue Partition vorhanden ist.

- Geben Sie `dmesg | tail` ein

Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# dmesg | tail
[ 773.090059] XFS (dm-2): Mounting U4 Filesystem
[ 773.214176] XFS (dm-2): Ending clean mount
[ 785.595678] XFS (dm-3): Mounting U4 Filesystem
[ 785.750078] XFS (dm-3): Ending clean mount
[ 802.874171] XFS (dm-4): Mounting U4 Filesystem
[ 803.020083] XFS (dm-4): Starting recovery (logdev: internal)
[ 803.041709] XFS (dm-4): Ending recovery (logdev: internal)
[ 813.249001] XFS (dm-5): Mounting U4 Filesystem
[ 813.439422] XFS (dm-5): Ending clean mount
[ 9838.504920] sde: sde1
[root@NWAPPLIANCE2599 database]#
```

- Geben Sie `fdisk /dev/sde` ein.
- Geben Sie `p` ein.

Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks    Id System
  /dev/sde1                2048     20971519     10484736    8e  Linux LVM

Command (m for help): _
```

Erstellen Sie ein physisches LVM-Volume auf einer neuen Partition.

1. Stellen Sie über SSH eine Verbindung zum Log Decoder-Host her.
2. Geben Sie die folgende Befehlszeichenfolge ein, um einen physischen Logical Volume Manager (LVM) auf der neuen Partition zu erstellen.

```
[root@LogDecoderGM ~]# pvcreate /dev/sde1
```


- Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# pvcreate /dev/sde1
Physical volume "/dev/sde1" successfully created.
[root@NWAPPLIANCE2599 database]#
```

Erweitern der Volume-Gruppe um ein physisches Volume

- Stellen Sie über SSH eine Verbindung zum Log Decoder-Host her.
- Geben Sie die folgende Befehlszeichenfolge ein, um einen physischen Logical Volume Manager (LVM) auf der neuen Partition zu erstellen.

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

Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# pvs
  PU          VG          Fmt Attr PSize  PFree
  /dev/sda2  netwitness_vg00 lvm2 a-- 194.31g 100.00m
  /dev/sdb1  VolGroup00      lvm2 a--  48.00g   0
  /dev/sdc1  VolGroup01      lvm2 a-- 104.00g   0
  /dev/sdd1  VolGroup01      lvm2 a-- 168.00g   0
  /dev/sde1          lvm2 ---  10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

netwitness_vg00 besteht aus /dev/sdc1 und /dev/sdd1 physischen Volumes (PV) und einem LVM-System. Beachten Sie, dass das neue /dev/sde1 Volume über 10 GB an freiem Speicherplatz verfügt.

- So fügen Sie das physische Volume netwitness_vg00 hinzu.
 - Geben Sie `vgextend netwitness_vg00 /dev/sde1` ein.

Die folgenden Informationen werden angezeigt:

```
Volume group "netwitness_vg00" successfully extended
```

- Geben Sie „pvs“ ein.

Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# vgextend netwitness_vg00 /dev/sde1
Volume group "netwitness_vg00" successfully extended
[root@NWAPPLIANCE2599 database]# pvs
  PU          VG          Fmt Attr PSize  PFree
  /dev/sda2  netwitness_vg00 lvm2 a-- 194.31g 100.00m
  /dev/sdb1  VolGroup00      lvm2 a--  48.00g   0
  /dev/sdc1  VolGroup01      lvm2 a-- 104.00g   0
  /dev/sdd1  VolGroup01      lvm2 a-- 168.00g   0
  /dev/sde1  netwitness_vg00 lvm2 a--  10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

Das Volume wurde zu netwitness_vg00 hinzugefügt, aber es wurde noch nicht erweitert (es sind immer noch 10 GB Speicherplatz frei). Es gibt mehrere logische Volumes in netwitness_vg00, in diesem Beispiel geht es um die PacketDB.

4. So erweitern Sie das logische Volume PacketDB, sodass es alle 10 GB an freiem Speicherplatz verwendet.
- Geben Sie `lvs netwitness_vg00` ein.
Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# lvs
LV      VG      Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao---- 140.21g
root    netwitness_vg00 -wi-ao---- 30.00g
swap    netwitness_vg00 -wi-ao---- 4.00g
usrhome netwitness_vg00 -wi-ao---- 10.00g
varlog  netwitness_vg00 -wi-ao---- 10.00g
[root@LogDecoder ~]#
```

- Geben Sie `lvextend -L+9.5G /dev/netwitness_vg00/nwhome` ein.
Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# lvextend -L+9.5G /dev/netwitness_vg00/nwhome
Size of logical volume netwitness_vg00/nwhome changed from 140.21 GiB (35894 extents) to 149.71 GiB (38326 extents).
Logical volume netwitness_vg00/nwhome successfully resized.
[root@NWAPPLIANCE2599 database]#
```

- Geben Sie `lvs netwitness_vg00` ein.
Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database]# lvs netwitness_vg00
LU      VG      Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao---- 149.71g
root    netwitness_vg00 -wi-ao---- 30.00g
swap    netwitness_vg00 -wi-ao---- 4.00g
usrhome netwitness_vg00 -wi-ao---- 10.00g
varlog  netwitness_vg00 -wi-ao---- 10.00g
[root@NWAPPLIANCE2599 database]#
```

Das logische packetdb-Volumen wurde auf 149.71 GB erweitert, aber das /var/netwitness-Dateisystem hat immer noch 140.21 GB.

Erweitern des Dateisystems

- Stellen Sie über SSH eine Verbindung zum Log Decoder-Host her.
- Geben Sie die folgende Befehlszeichenfolge ein, um einen physischen Logical Volume Manager (LVM) auf der neuen Partition zu erstellen.

```
[root@LogDecoderGM ~]# xfs_growfs /var/netwitness/
```

Die folgenden Informationen werden angezeigt:

```
[root@NWAPPLIANCE2599 database1]# xfs_growfs /var/netwitness/
meta-data=/dev/mapper/netwitness_vg00-nwhome isize=256   agcount=4, agsize=9188864 blks
        =                               sectsz=512   attr=2, projid32bit=1
        =                               crc=0        finobt=0 spinodes=0
data      =                               bsize=4096   blocks=36755456, imaxpct=25
        =                               sunit=0      swidth=0 blks
naming    =version 2                       bsize=4096   ascii-ci=0 ftype=0
log       =internal                       bsize=4096   blocks=17947, version=2
        =                               sectsz=512   sunit=0 blks, lazy-count=1
realtime  =none                             extsz=4096   blocks=0, rtextents=0
data blocks changed from 36755456 to 39245824
[root@NWAPPLIANCE2599 database1]# _
```

Starten von Services

Geben Sie die folgende Befehlszeichenfolge ein, um die Services auf dem Log Decoder-Host zu starten.

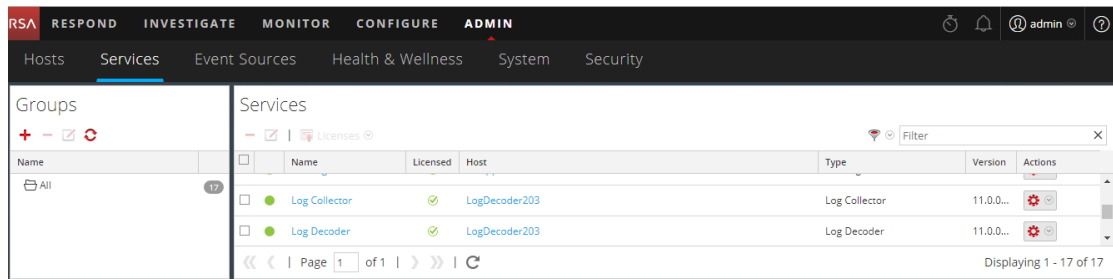
```
[root@LogDecoderGM ~]# service nwlogcollector start; service
nwlogdecoder start
```

Die folgenden Informationen werden angezeigt:

```
nwlogcollector start/running, process 4069
nwlogdecoder start/running, process 4069
```

Sicherstellen, dass die Services ausgeführt werden

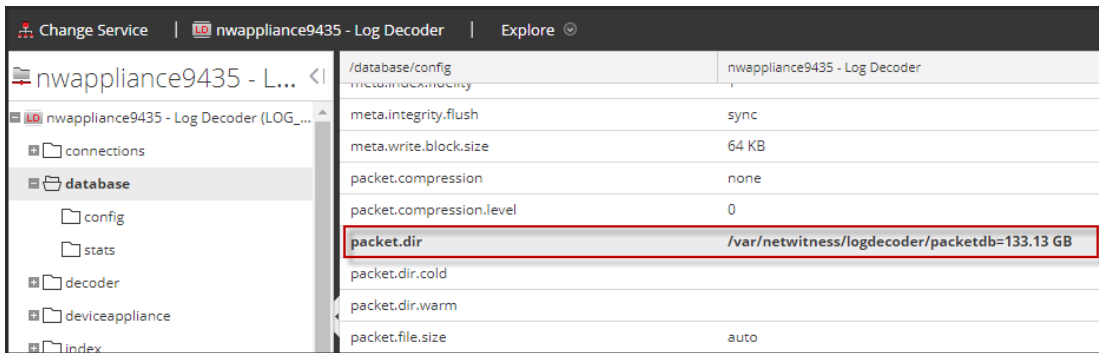
1. Melden Sie sich bei NetWitness Suite an.
2. Klicken Sie auf **Administration > Services**.
3. Stellen Sie sicher, dass der Log Collector- und Log Decoder-Service ausgeführt wird.



Neukonfigurieren der Log Decoder-Parameter

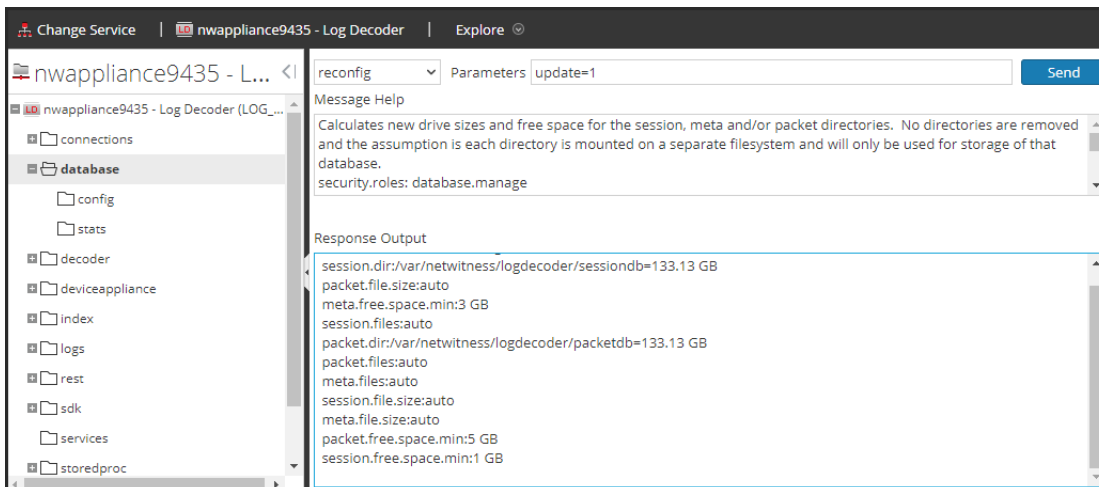
1. Melden Sie sich bei NetWitness Suite an.
2. Klicken Sie auf **Administration > Services**.
3. Wählen Sie den Log Decoder-Service aus.
4. Wählen Sie unter „Aktionen“ die Option „Ansicht > Durchsuchen“ aus.

5. Klicken Sie auf `database > config > packet.dir`.



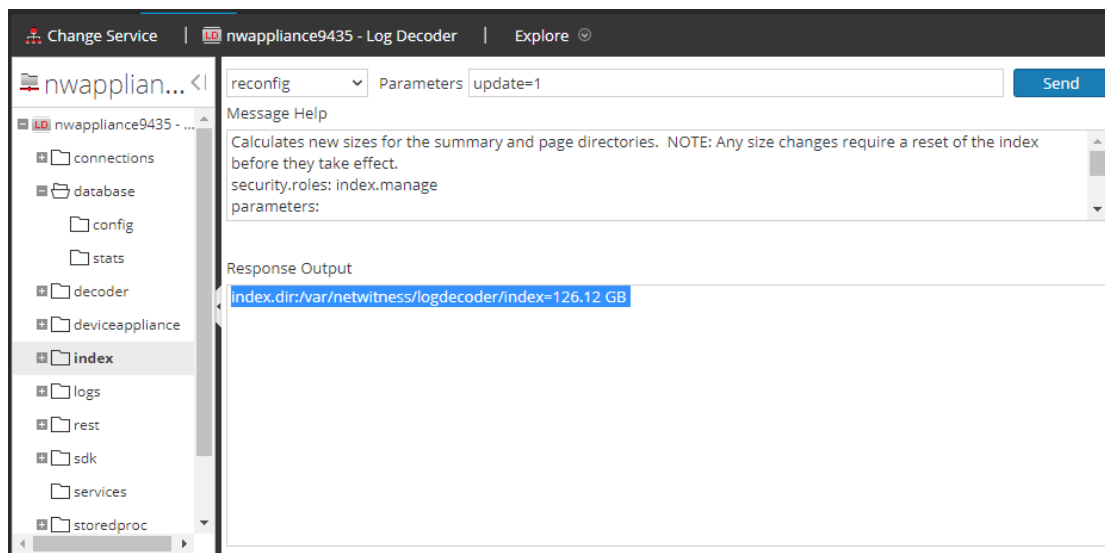
6. Klicken Sie mit der rechten Maustaste auf `database`, klicken Sie auf **Eigenschaften**, wählen Sie den Befehl **reconfig** aus, geben Sie **update=1** in **Parameter** an und klicken Sie auf **Senden**.

Der `packetdb`-Parameterwert wurde von 98,74 GB auf 133,13 GB geändert.

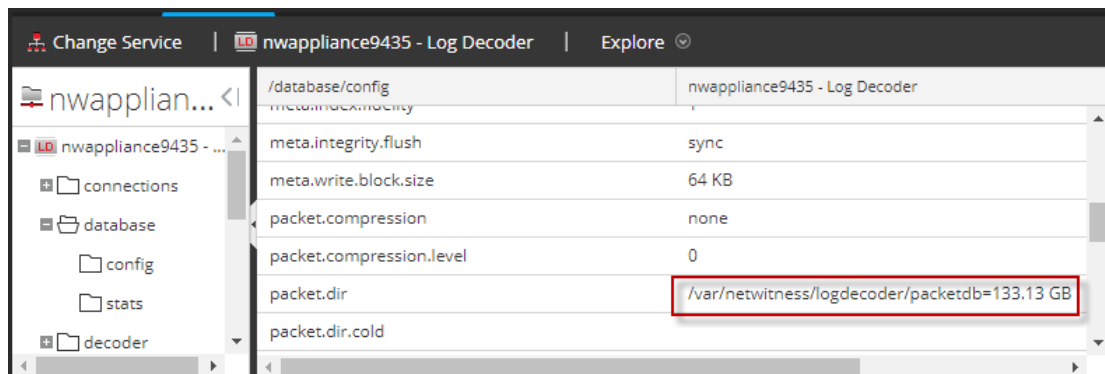


7. Klicken Sie mit der rechten Maustaste auf `index`, klicken Sie auf **Eigenschaften**, wählen Sie den Befehl **reconfig** aus, geben Sie **update=1** in **Parameter** an und klicken Sie auf

Senden.



- Schließen Sie das Dialogfeld „Eigenschaften“, um zur Ansicht „Durchsuchen“ zurückzukehren. Der `packet.dir`-Parameterwert beträgt nun 133,13 GB (95 % von 203 GB).



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

Die Option zur Einstellung eines Switches (virtuell oder physisch) auf den Empfangsmodus, auch als SPAN-Port (Cisco-Services) und Portspiegelung bezeichnet, ist nicht ohne Einschränkungen. Bei virtuellen wie physischen Switches kann die Paketerfassung je nach Menge und Art des kopierten Datenverkehrs leicht zu einer Überbelastung 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 die 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 Suite den Datenverkehr aus der Kapsel entnimmt.

