



# Leitfaden zur Bereitstellung

für RSA NetWitness® Platform 11.3



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

## **Kontaktinformationen**

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

## **Marken**

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

## **Lizenzvereinbarung**

Diese Software und die zugehörige Dokumentation sind Eigentum von 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 Nutzer 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 müssen 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.

Juli 2019

# Inhalt

---

<b>Die Grundlagen</b> .....	<b>5</b>
Einfache Bereitstellung .....	6
Prozess .....	6
Allgemeines Bereitstellungsdiagramm für NetWitness Platform .....	7
Detailliertes Hostbereitstellungsdiagramm für RSA NetWitness Platform .....	9
Bereitstellungsoptionen .....	10
<b>Optionale Einrichtungsverfahren für die Bereitstellung</b> .....	<b>11</b>
Gruppenaggregation .....	11
Empfehlungen zur Bereitstellung der RSA-Gruppenaggregation .....	11
Vorteile bei Verwendung der Gruppenaggregation .....	11
Konfiguration der Gruppenaggregation .....	13
Hybrid-Kategorien auf dem NW-Server .....	17
Zweiter Endpunktserver .....	18
Aktiver Stand-by-NW-Serverhost .....	19
Methoden .....	19
Geplantes Failover-Szenario .....	20
Erforderliches Failover-Szenario ohne Austausch der Hardware .....	20
Erforderliches Failover-Szenario mit Austausch der Hardware .....	20
Einrichten des sekundären NW-Servers in der Stand-by-Rolle .....	21
Führen Sie ein Failover des primären NW-Servers zu einem sekundären NW-Server durch. ....	35
Durchführen eines Failbacks des sekundären NW-Servers zum primären NW-Server .....	36
<b>Netzwerkarchitektur und Ports</b> .....	<b>37</b>
Diagramm der NetWitness Platform-Netzwerkarchitektur .....	37
Diagramm zur Netzwerkarchitektur von NetWitness Network (Packets) .....	38
Diagramm zur Netzwerkarchitektur NetWitness Logs .....	39
Umfassende Liste der Host-, Service- und iDRAC-Ports von NetWitness Platform .....	40
NW-Serverhost .....	41
Archiver-Host .....	42
Broker-Host .....	43
Concentrator-Host .....	44
Endpoint Log Hybrid .....	45
Event Stream Analysis (ESA)-Host .....	46
iDRAC Ports .....	47
Log Collector-Host .....	48
Log Decoder-Host .....	50

---

Log Hybrid-Host .....	51
Malware-Host .....	53
Network Decoder-Host .....	54
Network Hybrid-Host .....	55
UEBA-Host .....	56
NetWitness Endpoint-Architektur .....	57
NetWitness Endpoint 4.4-Integration in NetWitness Platform .....	57
So ändern Sie den UDP-Port für Endpoint Log Hybrid .....	58
Aufgabe 1: Teilen Sie allen Agents mit, dass sie einen neuen UDP-Port verwenden sollen .....	58
Aufgabe 2: Aktualisieren Sie den Port auf allen Endpoint Log Hybrid-Hosts in Ihrer Umgebung ..	58
<b>Anforderungen an den Standort und Sicherheit .....</b>	<b>60</b>
Vorgesehene Anwendung .....	60
Service .....	60
Sicherheitsinformationen .....	60
Standortauswahl .....	60
Vorgehensweise zur Handhabung des Geräts .....	60
Warnhinweise für Strom und Elektronik .....	61
Warnhinweise für Rackmontage .....	61
Kühlung und Luftstrom .....	61

## Die Grundlagen

---

In diesem Handbuch werden die grundlegenden Anforderungen einer NetWitness Platform-Bereitstellung beschrieben und optionale Szenarien zur Erfüllung der Anforderungen Ihres Unternehmens dargestellt. Selbst in kleinen Netzwerken kann durch gute Planung dafür gesorgt werden, dass alles reibungslos verläuft, wenn Sie bereit sind, die Hosts online zu schalten.

**Hinweis:** In diesem Dokument wird auf mehrere zusätzliche Dokumente Bezug genommen, die in RSA Link verfügbar sind. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Es gibt viele Faktoren, die Sie berücksichtigen müssen, bevor Sie NetWitness Platform bereitstellen. Die folgenden Elemente sind nur einige dieser Faktoren. Sie müssen bei der Berücksichtigung dieser Faktoren das Wachstum und die Speicheranforderungen abschätzen

- Größe Ihres Unternehmens (d. h. die Anzahl der Standorte und Personen, die NetWitness Platform verwenden werden)
- Menge der Netzwerkdaten und Protokolle, die Sie verarbeiten müssen
- Performance, die jede einzelne NetWitness Platform-Benutzerrolle benötigt, um ihre Jobs effektiv ausführen zu können
- Vermeidung von Ausfallzeiten (d. h. Vermeiden eines Single-Point-of-Failure).
- Die Umgebung, in der Sie NetWitness Platform ausführen möchten
  - Physische RSA-Hosts (Software, die auf von RSA bereitgestellter Hardware ausgeführt wird)  
Detaillierte Anweisungen zur Bereitstellung physischer RSA-Hosts finden Sie im *RSA NetWitness® Platform Handbuch zur Installation physischer Hosts*.
  - Nur von RSA bereitgestellte Software:
    - Lokale virtuelle Hosts  
Detaillierte Anweisungen zur Bereitstellung lokaler virtueller Hosts finden Sie im *RSA NetWitness® Platform Handbuch zur Installation virtueller Hosts*.
    - VCloud:
      - Amazon Web Services (AWS)  
Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in AWS finden Sie im *RSA NetWitness® Platform AWS-Installationshandbuch*.
      - Azure  
Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in Azure finden Sie im *RSA NetWitness® Platform Azure-Installationshandbuch*.

## Einfache Bereitstellung

Vor der Bereitstellung von NetWitness Platform müssen Sie folgende Voraussetzungen erfüllen:

- Sie haben die Anforderungen Ihres Unternehmens berücksichtigt und verstehen den Bereitstellungsprozess.
- Sie haben einen allgemeinen Überblick über die Komplexität und den Umfang einer NetWitness Platform-Bereitstellung.

## Prozess

Die Komponenten und die Topologie eines NetWitness Platform-Netzwerks können bei individuellen Installationen stark abweichen und sollten sorgfältig geplant werden, bevor der Prozess startet. Die anfängliche Planung umfasst Folgendes:

- Berücksichtigung der Standort- und Sicherheitsanforderungen
- Prüfung der Netzwerkarchitektur und Portnutzung
- Unterstützung der Gruppenaggregation auf Archivers und Concentrators und virtuellen Hosts

Wenn Sie bereit sind, mit der Bereitstellung zu beginnen, ist die allgemeine Abfolge wie folgt:

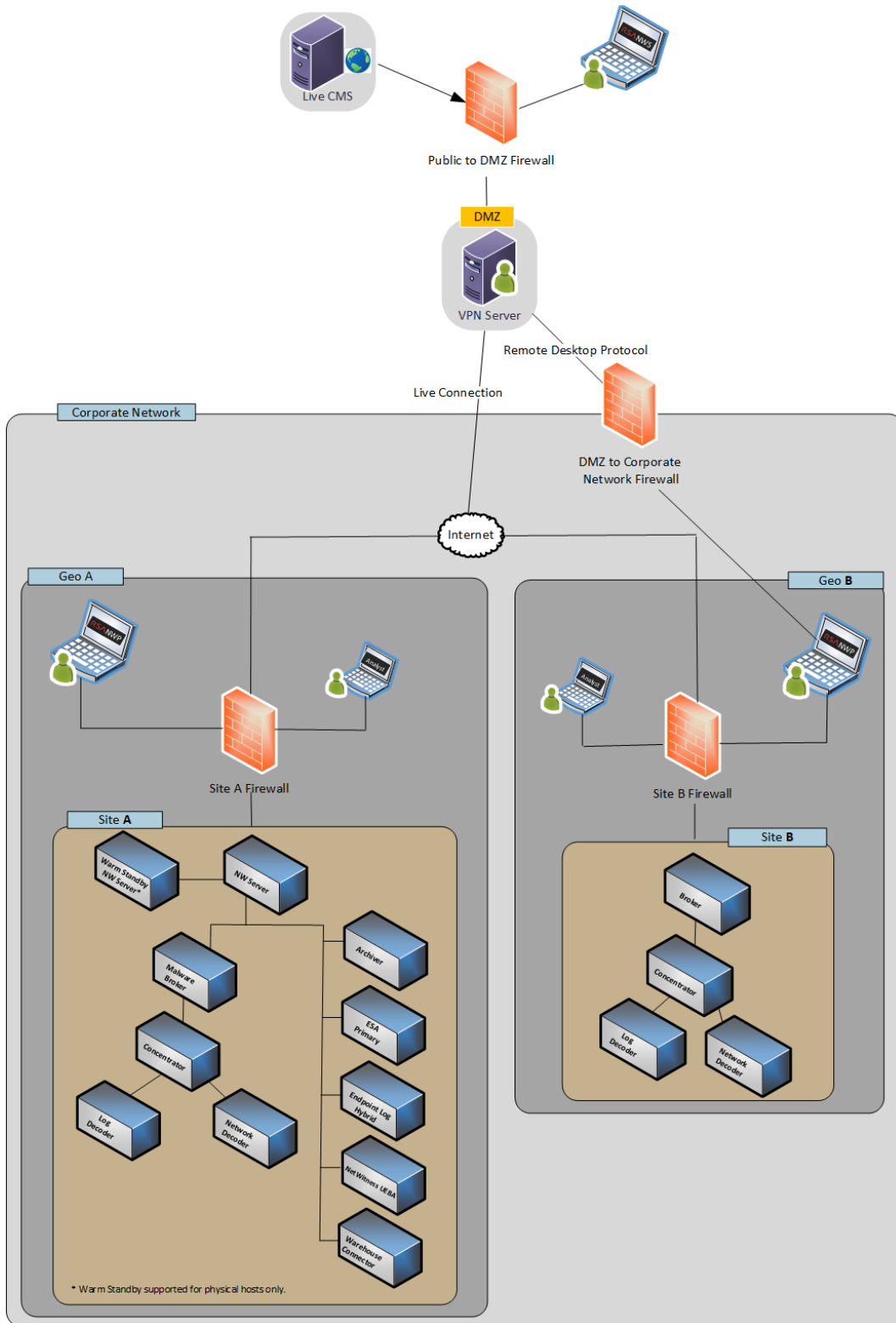
- Für physische RSA-Hosts:
  1. Installieren Sie physische Hosts und stellen Sie eine Verbindung mit dem Netzwerk her, wie im Leitfaden zur Hardwarekonfiguration von RSA NetWitness® Platform und im *RSA NetWitness® Platform Handbuch zur Installation physischer Hosts* beschrieben.
  2. Richten Sie die Lizenzierung für NetWitness Platform ein, wie im *RSA NetWitness® Platform Handbuch zur Lizenzierung* beschrieben.
  3. Konfigurieren Sie einzelne physische Hosts und Services, wie im *RSA NetWitness® Platform Leitfaden für die ersten Schritte mit Hosts und Services* beschrieben. In diesem Leitfaden finden Sie auch Verfahren zur Anwendung von Updates und zur Vorbereitung auf Versionsupgrades.
- Für lokale virtuelle Hosts befolgen Sie die Anweisungen im *RSA NetWitness® Platform Leitfaden zur Einrichtung von virtuellen Hosts*.
- Für AWS befolgen Sie die Anweisungen im *RSA NetWitness® Platform AWS-Installationshandbuch*.
- Für Azure befolgen Sie die Anweisungen im *RSA NetWitness® Platform Azure-Installationshandbuch*.

Wenn Sie Hosts und Services aktualisieren, befolgen Sie die empfohlenen Richtlinien unter dem Thema „Ausführen im gemischten Modus“ im *RSA NetWitness Platform Leitfaden für die ersten Schritte mit Hosts und Services*.

Außerdem sollten Sie sich mit Hosts, Hosttypen und Services vertraut machen, da sie im Zusammenhang mit NetWitness Platform verwendet werden. Eine Beschreibung finden Sie im *RSA NetWitness Platform Leitfaden für die ersten Schritte mit Hosts und Services*.

## **Allgemeines Bereitstellungsdiagramm für NetWitness Platform**

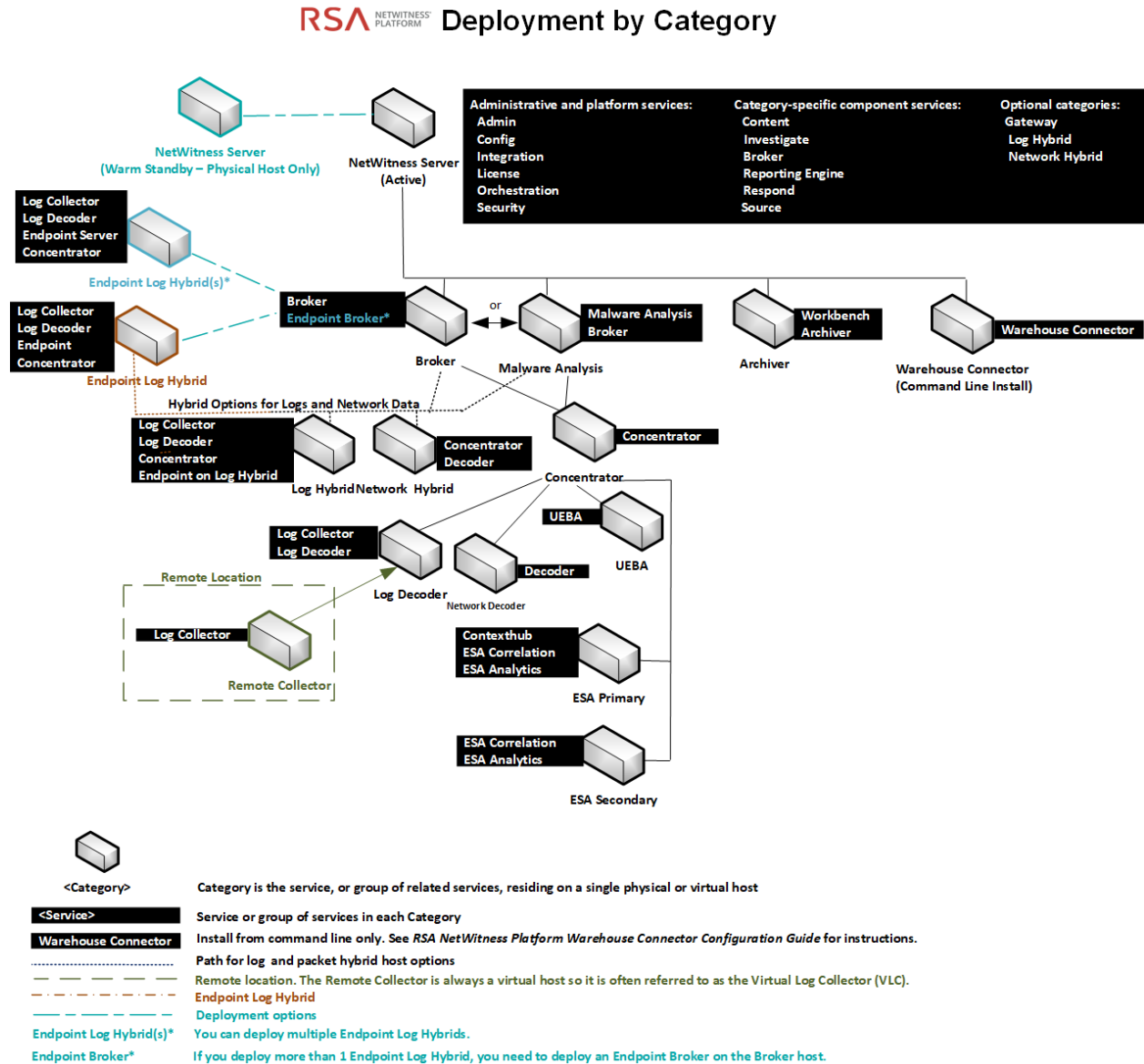
Im folgenden Diagramm ist eine einfache NetWitness Platform-Bereitstellung an mehreren Standorten dargestellt.





## Detailliertes Hostbereitstellungsdiagramm für RSA NetWitness Platform

Das folgende Diagramm zeigt ein Beispiel einer NetWitness Platform-Bereitstellung, die auf physischen oder virtuellen Rechnern gehostet wird. Anweisungen zum Installieren von NetWitness Platform finden Sie im *Handbuch zur Installation physischer Hosts*, im *Handbuch zur Installation virtueller Hosts*, im *AWS-Installationshandbuch* oder im *Azure-Installationshandbuch*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.



## Bereitstellungsoptionen

Sie stellen RSA NetWitness Platform mit den folgenden Optionen bereit.

- Gruppenaggregation
- Zweiter Endpunktserver
- Aktiver Stand-by-NW-Serverhost
- Hybrid-Kategorien auf dem NW-Server

Weitere Anweisungen finden Sie unter [Optionale Einrichtungsverfahren für die Bereitstellung](#) for instructions.

## Optionale Einrichtungsverfahren für die Bereitstellung

---

[Gruppenaggregation](#)

[Hybrid-Kategorien auf dem NW-Server](#)

[Zweiter Endpunktserver](#)

[Aktiver Stand-by-NW-Server](#)

### Gruppenaggregation

Mit der Gruppenaggregation können Sie mehrere Archiver- oder Concentrator-Services als Gruppe konfigurieren und die Aggregationsaufgaben zwischen ihnen aufteilen. Sie können mehrere Archiver-Services oder Concentrator-Services konfigurieren, um eine effiziente Aggregation aus mehreren Log Decoder-Services zu erreichen und so die Abfrageperformance der folgenden Daten zu verbessern:

- Im Archiver gespeicherte Daten
- Über den Concentrator verarbeitete Daten

### Empfehlungen zur Bereitstellung der RSA-Gruppenaggregation

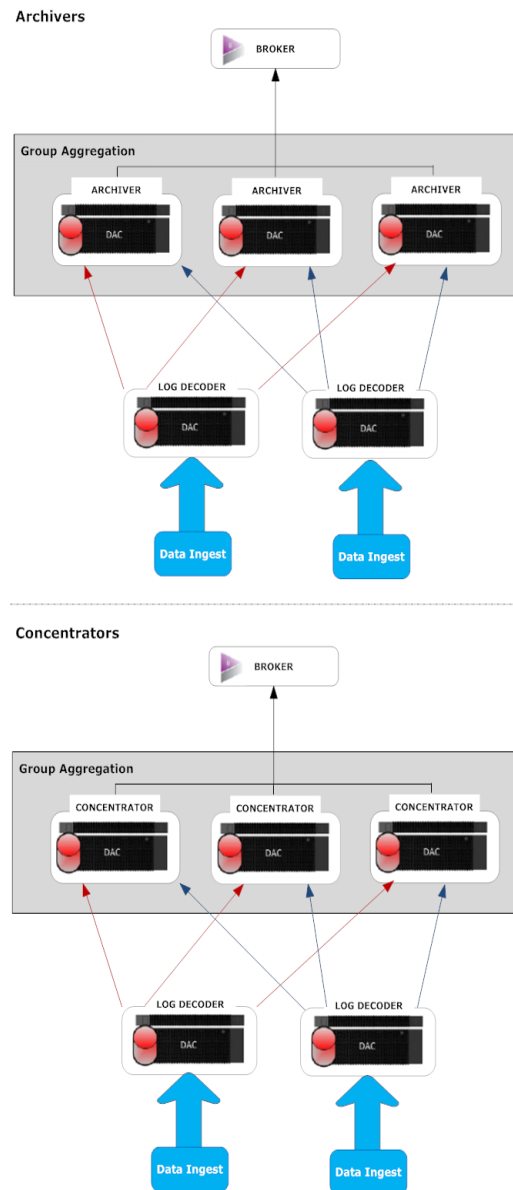
RSA empfiehlt die folgende Bereitstellung für die Gruppenaggregation:

- 1 bis 2 Log Decoder
- 3 bis 5 Archiver oder Concentrators

### Vorteile bei Verwendung der Gruppenaggregation

- Erhöht die Geschwindigkeit der RSA NetWitness® Platform-Abfragen.
- Verbessert die Performance von aggregierten Abfragen (Count und Sum) in der Umgebung
- Verbessert die Performance des Investigation-Service
- Daten können für Ermittlungszwecke für einen längeren Zeitraum gespeichert werden.

In der folgenden Abbildung wird die Gruppenaggregation dargestellt.



Sie können beliebig viele Archivers oder Concentrators gruppieren und daraus eine Aggregationsgruppe bilden. Die aggregierten Sitzungen werden auf die Archiver- oder Concentrator-Services in der Gruppe aufgeteilt, wobei die Anzahl der Sitzungen im Parameter „Max. Sitzungen für Aggregation“ festgelegt ist.

Wenn eine Aggregationsgruppe z. B. aus zwei Archiver-Services oder zwei Concentrator-Services besteht und der Parameter „Max. Sitzungen für Aggregation“ auf 10.000 festgelegt wird, werden die Sitzungen wie in der folgenden Tabelle dargestellt auf die Services aufgeteilt.

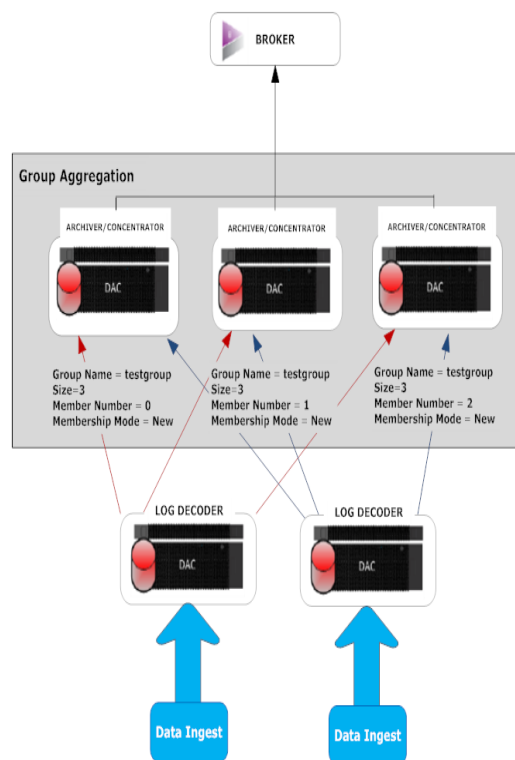
Archiver 0 oder Concentrator 0	Archiver 1 oder Concentrator 1
1 - 9.999	10.000 - 19.999
20.000 - 29.999	30.000 - 39.999
40.000 - 49.999	50.000 - 59.999

## Konfiguration der Gruppenaggregation

Schließen Sie dieses Verfahren ab, um mehrere Archiver- oder Concentrator-Services als Gruppe zu konfigurieren und die Aggregationsaufgaben zwischen ihnen aufzuteilen.

### Voraussetzungen

Planen Sie das Netzwerkdesign für die Gruppenaggregation. In der folgenden Abbildung ist ein Beispiel für eine Konfiguration einer Gruppenaggregation gezeigt.



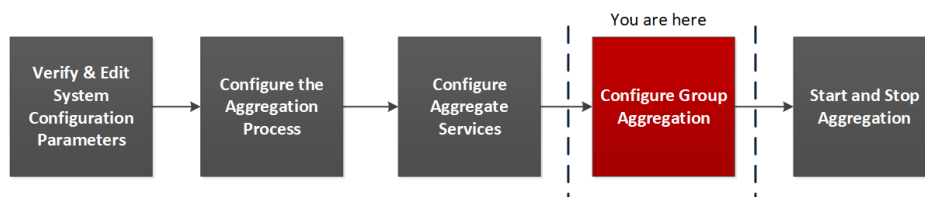
Stellen Sie sicher, dass Sie die Parameter der Gruppenaggregation in der folgenden Tabelle verstehen, und erstellen Sie einen Gruppenaggregationsplan.

Parameter	Beschreibung
Gruppenname	Bestimmt die Gruppe, zu der der Archiver oder Concentrator gehört. Sie können eine beliebige Anzahl von Gruppen hinzuzufügen, die Daten von einem Log Decoder aggregieren. Der Parameter „Gruppenname“ wird vom Log Decoder verwendet, um zu ermitteln, welche Archiver- oder Concentrator-Services zusammenarbeiten. Alle Archiver- oder Concentrator-Services in der Gruppe sollten denselben Gruppennamen haben.
Größe	Bestimmt die Anzahl der Archiver- oder Concentrator-Services in der Aggregationsgruppe.
Mitgliedsnummer	Bestimmt die Position des Archiver oder Concentrator in der Aggregationsgruppe. Für eine Gruppe der Größe N muss die Mitgliedsnummer von 0 bis N-1 auf jedem Archiver- oder Concentrator-Service in der Aggregationsgruppe definiert sein. Beispiel: Wenn die Größe der Aggregationsgruppe 2 beträgt, sollte die Mitgliedsnummer eines der Archiver- oder Concentrator-Services auf 0 und die Mitgliedsnummer des anderen Archiver oder Concentrator auf 1 festgelegt werden.
Mitgliedschaftsmodus	Es gibt zwei Mitgliedschaftsmodi: <ul style="list-style-type: none"> <li>• Neu: Hinzufügen eines neuen Archiver- oder Concentrator-Services als Mitglied zu einer bestehenden Aggregationsgruppe oder Erstellen einer neuen Aggregationsgruppe. Der Archiver- oder Concentrator-Service aggregiert keine bestehenden Sitzungen vom Service, da andere Mitglieder der Gruppe wahrscheinlich bereits alle Sitzungen auf dem Service aggregiert haben. Dieser Archiver- oder Concentrator-Service aggregiert nur neue Sitzungen, die auf dem Service angezeigt werden.</li> <li>• Ersetzen: Ersetzen eines bestehenden Mitglieds einer Aggregationsgruppe. Der Archiver oder Concentrator beginnt die Aggregation bei der ältesten verfügbaren Sitzung auf dem Service, von dem er aggregiert.</li> </ul>



**Hinweis:** Der Mitgliedschaftsmodus-Parameter hat nur Auswirkungen, wenn von dem Service noch keine Sitzungen aggregiert wurden. Nachdem eine Sitzung aggregiert wurde, hat dieser Parameter keine Auswirkungen mehr.

## Einrichten der Gruppenaggregation

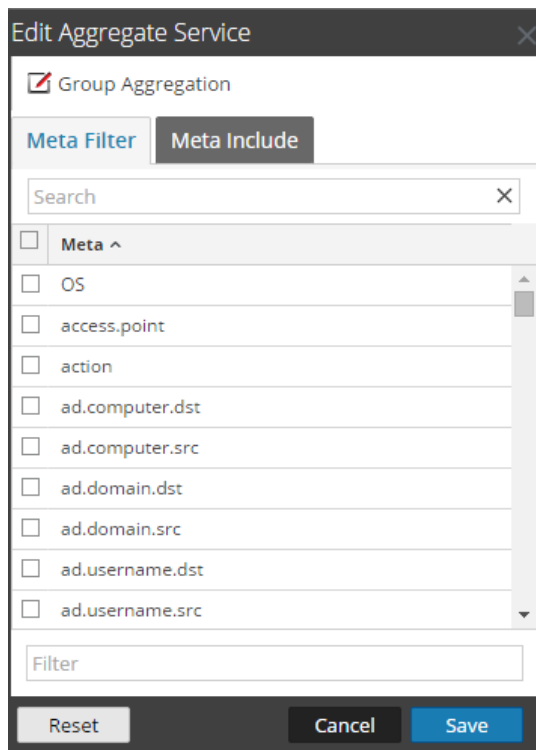
Dieser Workflow zeigt die Schritte, die Sie zur Konfiguration der Gruppenaggregation abschließen müssen.



Schließen Sie die folgende Schritte ab, um die Gruppenaggregation einzurichten.

1. Konfigurieren Sie mehrere Archiver- oder Concentrator-Services in Ihrer Umgebung. Vergewissern Sie sich, dass Sie den gleichen Log Decoder als Datenquelle zu allen Services hinzufügen.
2. Führen Sie die folgenden Schritte für alle Archiver- oder Concentrator-Services aus, die zur Aggregationsgruppe gehören sollen:
  - a. Navigieren Sie zu **ADMIN > Services**.
  - b. Wählen Sie den Archiver- oder Concentrator-Service aus und wählen Sie dann in der Spalte **Aktionen** die Optionen **Ansicht > Konfiguration** aus.  
Die Ansicht „Servicekonfiguration“ von Archiver oder Concentrator wird angezeigt.
  - c. Wählen Sie im Abschnitt **Services aggregieren** die Option **Log Decoder** aus.
  - d. Klicken Sie auf  **Toggle Service** , um den Status des Log Decoder in „offline“ zu ändern, sofern er „online“ lautet.
  - e. Klicken Sie auf .

Das Dialogfeld **Aggregierten Service bearbeiten** wird angezeigt.



- f. Klicken Sie auf  **Group Aggregation** .  
Das Dialogfeld **Gruppenaggregation bearbeiten** wird angezeigt.

- g. Aktivieren Sie das Kontrollkästchen **Aktiviert** und legen Sie die folgenden Parameter fest:
- Geben Sie im Feld **Gruppenname** den Namen der Gruppe ein.
  - Wählen Sie im Feld **Größe** die Anzahl der Archiver- oder Concentrator-Services in der Aggregationsgruppe aus.
  - Wählen Sie im Feld **Mitgliedsnummer** die Position des Archiver oder Concentrator in der Aggregationsgruppe aus.
  - Wählen Sie den Modus im Drop-down-Menü **Mitgliedschaftsmodus** aus.
- h. Klicken Sie auf **Speichern**.
- i. Klicken Sie in der Ansicht „Servicekonfiguration“ auf **Anwenden**.
- j. Führen Sie **Schritt b** bis **Schritt i** für alle anderen Archiver- oder Concentrator-Services aus, die Teil der Gruppenaggregation sein sollen.
3. Legen Sie im Abschnitt **Aggregationskonfiguration** den Parameter für **Max. Sitzungen für Aggregation** auf **10.000** fest.

Name	Config Value
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
<b>Aggregate Max Sessions</b>	<b>10000</b>
<b>Service Heartbeat</b>	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	<input checked="" type="checkbox"/>
SSL Port	56005
Start Update Interval	1000
Threads	20



## Hybrid-Kategorien auf dem NW-Server

Sie können Hybrid-Kategorien wie Log Hybrid- und Network (Packet) Hybrid-Servicekategorien auf einem physischen Host (R640) der Serie 6 installieren. So haben Sie die Möglichkeit, mehrere externe PowerVault-Speichergeräte an den physischen Host der Serie 6 (R640) anzuhängen.

## Zweiter Endpunktserver

Führen Sie das folgende Verfahren aus, um einen zweiten Endpunktserver bereitzustellen.

1. Richten Sie einen neuen Host in NetWitness Platform ein.
  - Führen Sie für einen physischen Host die Schritte 1 bis 14 im Abschnitt „Aufgabe 2: Installieren von 11.3 auf anderen Komponentenhosts“ unter „Installationsaufgaben“ des *Handbuchs zur Installation virtueller Hosts* aus. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
  - Befolgen Sie für einen virtuellen Host die Anweisungen im *Handbuch zur Installation virtueller Hosts* in „Aufgabe 2: Installieren von 11.3 auf anderen Komponentenhosts“ unter „Schritt 4. Installation von RSA NetWitness Platform“.

2. Greifen Sie mit SSH-Verschlüsselung auf den Host zu, den Sie in Schritt 1 eingerichtet haben.
3. Senden Sie die folgende Befehlszeichenfolge:

```
mkdir -p /etc/pki/nw/nwe-ca
```

**Hinweis:** Sie müssen keine Berechtigungen ändern.

4. Kopieren Sie die folgenden zwei Dateien vom zuvor bereitgestellten Endpunktserver auf den neuen/zweiten Endpunktserver:

```
/etc/pki/nw/nwe-ca/nwrootca-cert.pem
```

```
/etc/pki/nw/nwe-ca/nwrootca-key.pem
```

5. Installieren Sie den Endpunkt auf dem Host.

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

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

- b. Wählen Sie im Dialogfeld **Neue Hosts** den neuen 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. Endpunkt) in der Ansicht „Hosts“ aus und klicken Sie auf



Das Dialogfeld **Services installieren** wird angezeigt.

- d. Wählen Sie **Endpunkt** unter **Hosttyp** aus und klicken Sie auf **Installieren**.

## Aktiver Stand-by-NW-Serverhost

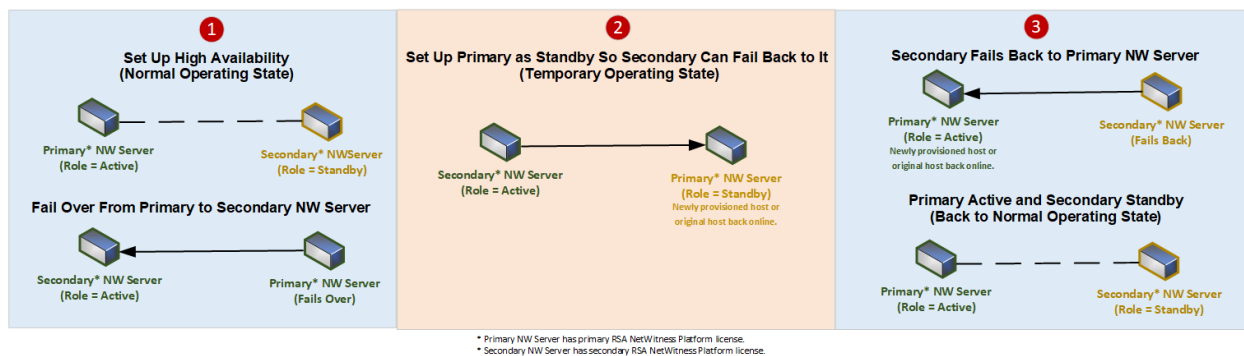
Der aktive Stand-by-NW-Server dupliziert die kritischen Komponenten und Konfigurationen des aktiven NW-Serverhosts, um die Zuverlässigkeit zu erhöhen.

Ein sekundärer NW-Server verbleibt in der Stand-by-Rolle und empfängt bei entsprechender Konfiguration in regelmäßigen Abständen Backups des primären NW-Servers in der aktiven Rolle. Wenn der primäre NW-Server ausfällt (offline geht), muss das Failover-Verfahren ausgeführt werden, sodass der sekundäre NW-Server die aktive Rolle übernehmen kann.

Wenn Sie einen sekundären NW-Server als aktiven Stand-by-NW-Server einrichten, wird ein Ausfall oder ein geplanter Wechsel vom primären NW-Server zum sekundären NW-Server als Failover bezeichnet. Sie führen ein Failback durch, um zum normalen Betriebszustand (d. h. zum primären NW-Server in der aktiven Rolle und zum sekundären NW-Server in der Stand-by-Rolle) zurückzukehren.

Das folgende Diagramm zeigt den Failover- und den Failback-Prozess.

- 1** Richten Sie den sekundären NW-Server als Stand-by-Server (Erstkonfiguration) ein. Dies ist der normale Betriebsstatus.
- 2** Der primäre NW-Server führt ein Failover zum sekundären NW-Server durch. Schalten Sie den primären NW-Server nach dem Failover wieder online und richten Sie ihn in der Stand-by-Rolle ein. Hierbei handelt es sich um einen temporären Betriebsstatus.
- 3** Führen Sie einen Failback des sekundären NW-Servers zum primären Server durch. Der primäre NW-Server ist wieder auf die aktive Rolle und der sekundäre auf die Stand-by-Rolle gesetzt. Dies ist der normale Betriebsstatus.



**WICHTIG:** Während eines Failovers müssen Sie dem sekundären NW-Server die gleiche IP-Adresse wie dem primären NW-Server zuweisen, damit er die aktive Rolle übernehmen kann.

## Methoden

Führen Sie die folgende Aufgabe aus, um einen sekundären NW-Server in der Stand-by-Rolle für Failover einzurichten:

- Richten Sie einen sekundären NW-Server in der Stand-by-Rolle ein.

Führen Sie bei Bedarf die folgenden Aufgaben aus, um eine hohe Verfügbarkeit aufrechtzuerhalten.

- Führen Sie ein Failover des primären NW-Servers zu einem sekundären NW-Server durch.
- Führen Sie ein Failback des sekundären NW-Servers zum primären NW-Server durch.

## Geplantes Failover-Szenario

Dieses Szenario tritt auf, wenn Sie ein Failover planen (siehe **Geplantes Failover** unter Schritt 3 im Verfahren [Durchführen eines Failovers des primären NW-Servers zum sekundären NW-Server](#)). Nach Abschluss des Failovers sollten Sie keine Aktionen durchführen.

## Erforderliches Failover-Szenario ohne Austausch der Hardware

Dieses Szenario tritt auf, wenn der primäre NW-Server ausfällt (siehe *Erforderliches Failover* unter Schritt 3 im Thema [Durchführen eines Failovers des primären NW-Servers zum sekundären NW-Server](#)), Sie können es jedoch einfach ohne erneutes Imaging wiederherstellen (wenn der aktive NW-Server einen beschädigten oder unzureichenden RAM aufweist). Im folgenden Fall müssen Sie weder den `nwsetup-tui` ausführen noch den Customer Service (<https://Community.RSA.com/docs/doc-1294>) kontaktieren, um die korrekte Lizenzierung wiederherzustellen:

1. Der aktive (primäre NW-Server) führt ein Failover zum Stand-by-Server durch (sekundärer NW-Server) und dieser sekundäre Host übernimmt vorübergehend die Rolle des aktiven NW-Servers.
2. Beheben Sie das Problem mit dem primären NW-Server (installieren Sie beispielsweise einen neuen RAM) und führen Sie ein Failback vom sekundären Host zu ihm durch.

## Erforderliches Failover-Szenario mit Austausch der Hardware

Dieses Szenario tritt auf, wenn der aktive NW-Server vollständig ausfällt und die Hardware ausgetauscht werden muss, wenn Sie beispielsweise eine Rücksendeautorisierung (Return Merchandise Authorization, RMA) erhalten. Sie müssen den Host mit dem `nwsetup-tui` neu konfigurieren und sich an den Customer Support (<https://community.rsa.com/docs/DOC-1294>) wenden, um die Lizenzierung wiederherzustellen. Wenn Sie den Ersatzhost als temporären Stand-by-Host neu erstellen (z. B. bis zum geplanten Failback), müssen Sie die `nw-setup-tui`-Eingabeaufforderung **Stand-by-Host-Recovery-Modus** mit „Ja“ bestätigen, wenn Sie diesen temporären Stand-by-Host für das Failback konfigurieren (siehe Schritt 4 im Verfahren [Einrichten eines sekundären NW-Servers in der Stand-by-Rolle](#) für den Kontext dieser Aufforderung).

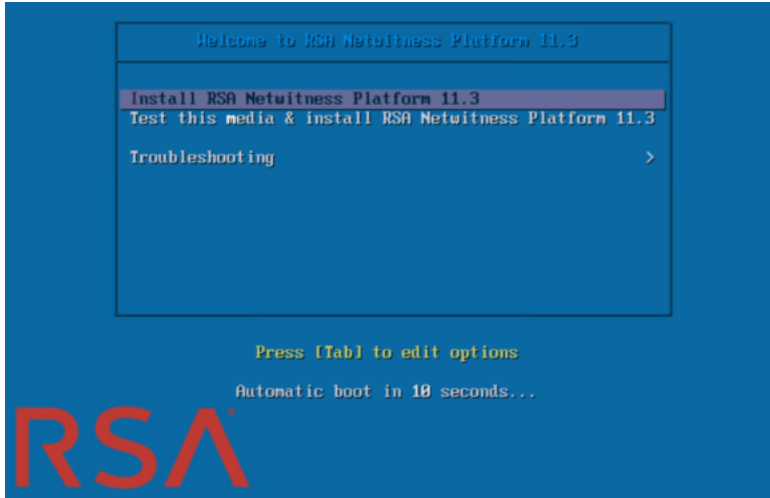
## Einrichten des sekundären NW-Servers in der Stand-by-Rolle

1. Bevor Sie einen sekundären NW-Serverhost für die Stand-by-Rolle installieren, stellen Sie Folgendes sicher:
  - a. Auf dem primären NW-Server wird 11.3 ausgeführt.
  - b. Auf allen Komponentenhosts wird 11.3 ausgeführt.  
Beachten Sie Folgendes:
    - Befolgen Sie zum Installieren von NetWitness Platform 11.3 die Anweisungen im *RSA NetWitness Platform 11.3 Installationshandbuch für physische Hosts* oder im *RSA NetWitness Platform 11.3 Installationshandbuch für virtuelle Hosts*.
    - Befolgen Sie zum Durchführen eines Upgrades von 10.6.x auf 11.3 die Anweisungen im *RSA NetWitness Platform 10.6.6.x auf 11.3 – Upgradehandbuch für physische Hosts* oder das *RSA NetWitness Platform 11.3 Installationshandbuch für physische Hosts*.
    - Befolgen Sie zum Aktualisieren von 11.x auf 11.3 die Anweisungen im *RSA NetWitness Platform Leitfaden zur Aktualisierung von Version 11.x auf 11.3*.  
Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.
2. Erstellen Sie ein Basis-Image auf dem sekundären NW-Server:
  - a. Verbinden Sie die Medien (ISO) mit dem Host.  
Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Platform Build-Stick*.
    - Hypervisor-Installationen: Verwenden Sie das ISO-Image.
    - Physische Medien: Verwenden Sie die ISO-Datei, um startfähige Flash-Laufwerksmedien mit dem Tool **Etcher**® oder einem anderen geeigneten Imaging-Tool zu erstellen und ein Image des Linux-Dateisystems auf das USB-Laufwerk zu bringen. In den *RSA NetWitness® Platform Anweisungen zum Build-Stick* finden Sie Informationen zum Erstellen eines Build-Sticks aus dem ISO-Image. Etcher ist unter <https://etcher.io> verfügbar.
    - iDRAC-Installationen – der Typ der virtuellen Medien lautet:
      - **Virtuelles Diskettenlaufwerk** für zugeordnete Flash-Laufwerke
      - **Virtuelle CD** für zugeordnete optische Mediengeräte oder ISO-Datei.
  - b. Melden Sie sich beim Host an und starten Sie ihn neu.

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

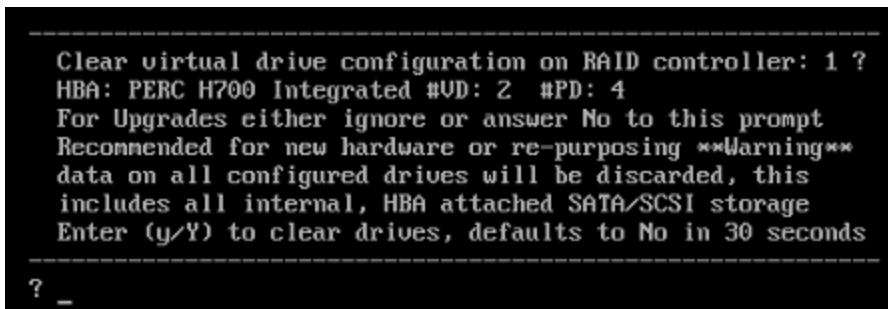
- c. Wählen Sie während des Neustarts **F11** (Startmenü), um ein Startgerät auszuwählen und von den verbundenen Medien zu starten.

Nach einigen Systemprüfungen während des Startvorgangs wird das folgende Installationsmenü angezeigt: **Willkommen bei RSA NetWitness Platform 11.3**. Die Grafiken im Menü werden anders dargestellt, wenn Sie ein physisches USB-Flash-Medium verwenden.



- d. Wählen Sie **RSA NetWitness Platform 11.3 installieren** (Standardauswahl) aus und drücken Sie die **Eingabetaste**.

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



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

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

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

Adapter 0: Configuration is Cleared.

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

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot
```

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

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

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

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

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

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

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

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

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

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

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

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

2. Führen Sie den Befehl `nwsetup-tui` aus.

**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 nach der Netzwerkkonfiguration des Hosts gefragt werden, stellen Sie sicher, dass Sie exakt die gleiche Netzwerkkonfiguration angeben, die für die ursprüngliche Installation von 11.x auf diesem Host verwendet wurde.

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

```
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
```

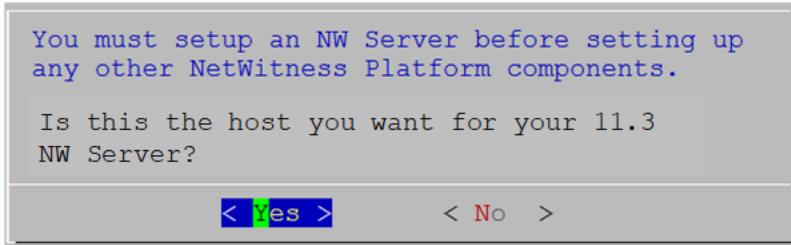
92%

`<Accept >`

`<Decline>`

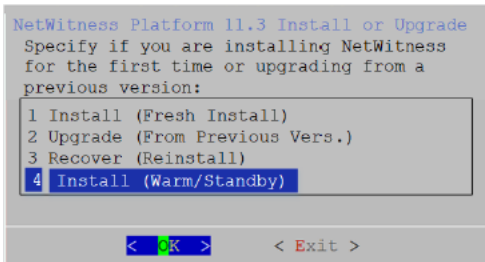


3. Gehen Sie zu **Akzeptieren** und drücken Sie die **Eingabetaste**.  
Es wird eine Aufforderung mit der Frage angezeigt, ob dies der Host ist, den Sie für Ihren 11.3 NW-Server verwenden möchten.

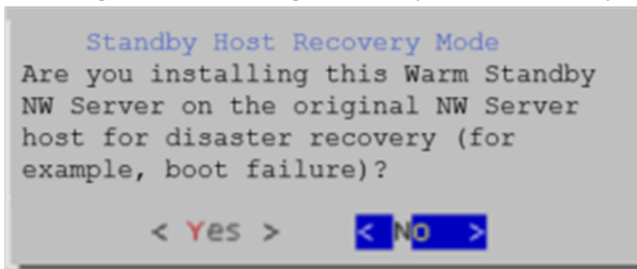


Die Antwort auf diese Eingabeaufforderung identifiziert einen Host während einer Neuinstallation entweder als primär oder als sekundär (und die ausgewählte Antwort bleibt unabhängig von der aktuellen oder zukünftigen Rolle des Hosts, d. h. aktiv oder Stand-by, konstant).

4. Gehen Sie zu **Ja** und drücken Sie die **Eingabetaste**.  
Die Aufforderung **Installation oder Upgrade** wird angezeigt.



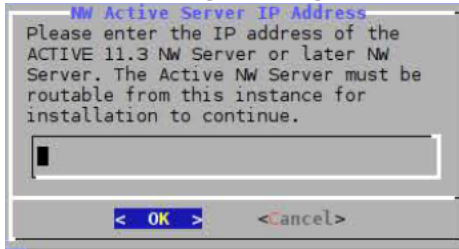
5. Gehen Sie zu **4 Installieren (aktiver Stand-by)** und drücken Sie die **Eingabetaste**.  
Die Eingabeaufforderung „Stand-by-Host-Recovery-Modus“ wird angezeigt.



6. Gehen Sie zu:

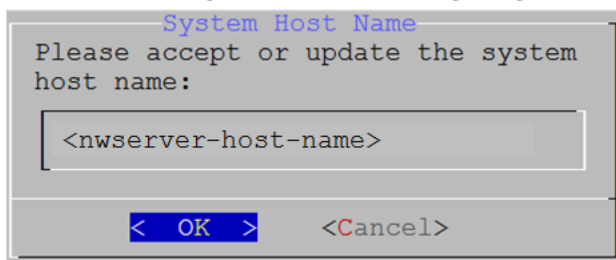
- **Nein** und drücken Sie die **Eingabetaste**, um einen sekundären NW-Server mit der Stand-by-Rolle (Häufigstes Szenario) einzurichten.
- **Ja** und drücken Sie die **Eingabetaste**, um einen Host einzurichten, der zuvor als primärer NW-Server mit der Stand-by-Rolle verwendet wurde, damit Sie ein Failover und ein Failback durchführen können. Gehen Sie zu Ja und drücken Sie die Eingabetaste (seltenes Szenario).

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



7. Geben Sie die IP-Adresse des NW-Servers in der aktiven Rolle ein, gehen Sie zu **OK** und drücken Sie die **Eingabetaste**.

Die Aufforderung **Hostname** wird angezeigt



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

- 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.

**Hinweis:** Sie müssen für den aktiven Standby-NW-Serverhost die gleichen Master- und Bereitstellungsanmeldedaten verwenden, die Sie für den aktiven NW-Server Host verwendet haben.

Für das Masterpasswort und Bereitstellungspasswort werden folgende Zeichen unterstützt:

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

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

**Master Password**

The master password is utilized to set the default password for both the system recovery account and the NetWitness UI "admin" account. The system recovery account password should be safely stored in case account recovery is needed. The NetWitness UI "admin" account password can be updated upon login.

Enter a Master Password.

Password \*\*\*\*\*

Verify \*\*\*\*\*

< OK >      <Cancel>

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

**Deployment Password**

The Deployment password is used when deploying NetWitness hosts. It needs to be safely stored and available when deploying additional hosts to your NetWitness Platform.

Enter a Deploy Password.

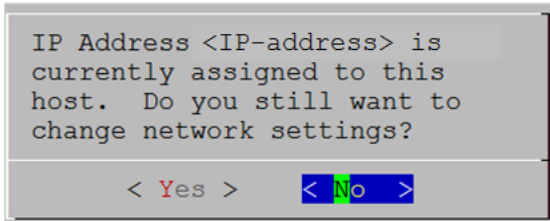
Password \*\*\*\*\*

Verify \*\*\*\*\*

< OK >      <Cancel>

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.

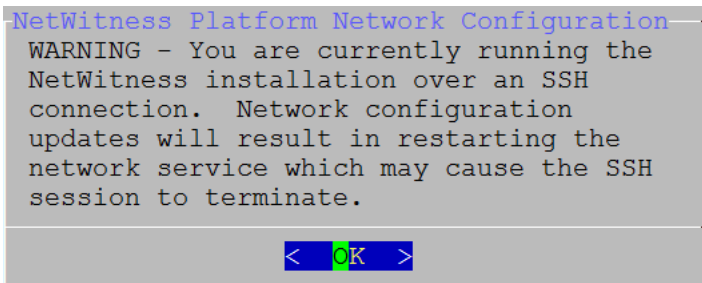
- Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt:



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:

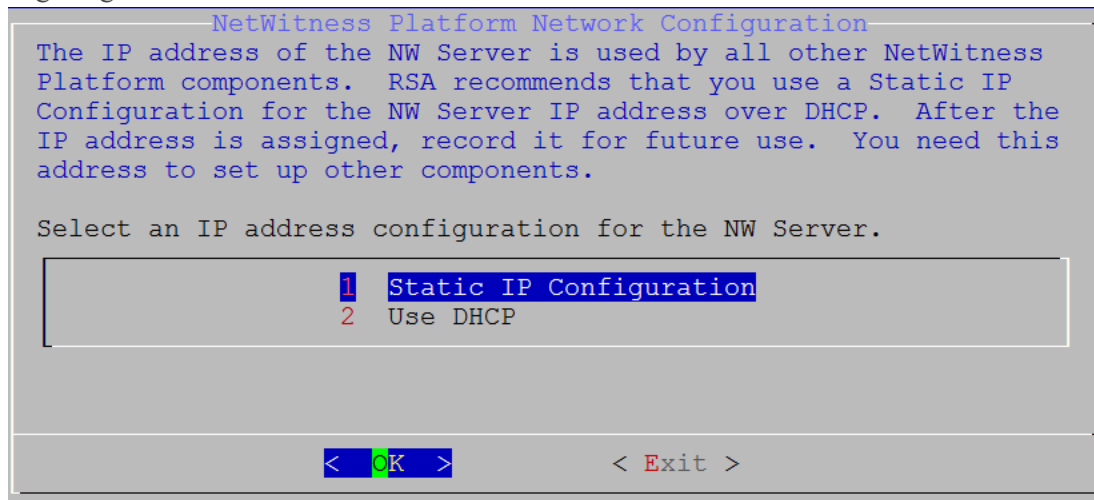
**Hinweis:** Wenn die Verbindung direkt über die Hostkonsole erfolgt, wird die folgende Warnung nicht angezeigt.



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

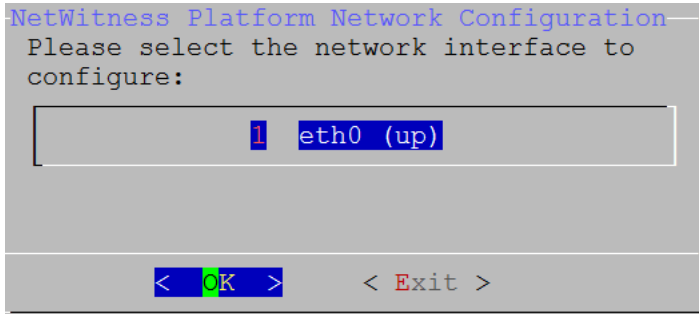
- Wenn das Setup-Programm eine IP-Konfiguration gefunden hat und Sie sie ausgewählt haben, wird die Aufforderung **Update-Repository** angezeigt. Fahren Sie mit Schritt 12 fort und schließen Sie die Installation ab.
- Wenn das Setup-Programm keine IP-Konfiguration gefunden hat oder Sie beschlossen haben,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

angezeigt.

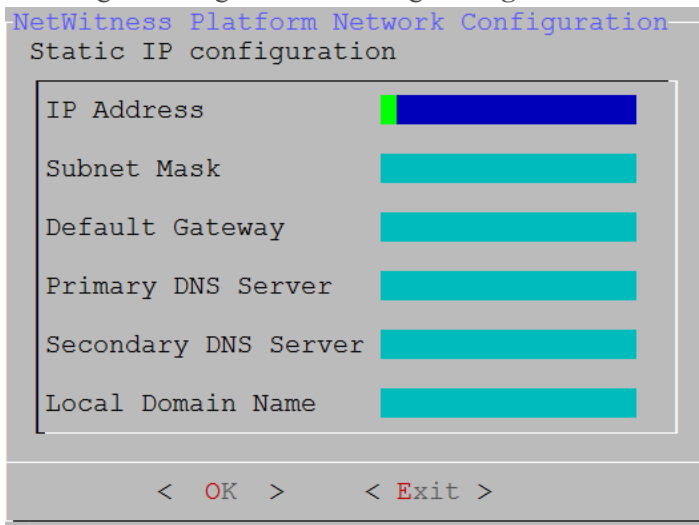


11. Gehen Sie zu **OK** und drücken Sie die **Eingabetaste**, um **Statische IP-Adresse** zu verwenden. Wenn Sie **DHCP** verwenden möchten, gehen Sie mit dem Pfeil nach unten zu 2 DHCP verwenden und drücken Sie **Eingabetaste**.

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 fortfahren möchten, gehen Sie zu **Beenden**. Die folgende 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 keine Pflichtfelder). Wenn Sie für eines der Felder die falsche Syntax oder Zeichenlänge verwenden, wird die Fehlermeldung `Invalid <field-name>` angezeigt.

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

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

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

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

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

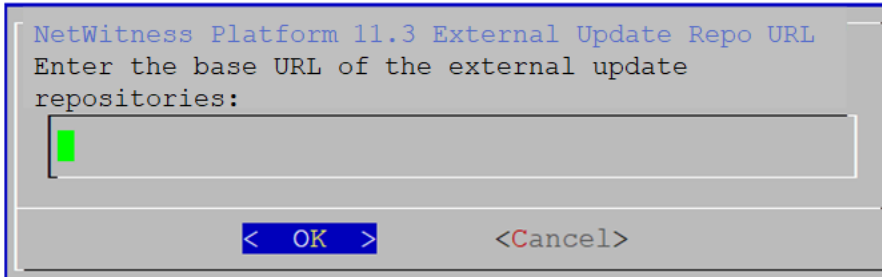
< OK >          < Exit >
```

14. Drücken Sie die **Eingabetaste**, um das **lokale Repository** auf dem NW-Server auszuwählen. Wenn Sie ein externes Repository verwenden möchten, gehen Sie mit dem Pfeil nach unten zu **Externes Repository** und dann zu **OK** und drücken Sie die **Eingabetaste**.
- Stellen Sie bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** im Setup-Programm sicher, dass die richtigen Medien mit dem Host verbunden sind (Medien mit der ISO-Datei, z. B. ein Build-Stick), von denen es die Installation von NetWitness Platform 11.2.0.0 abrufen kann. Wenn das Programm die verbundenen Medien nicht finden kann, wird die folgende Aufforderung angezeigt.

```
NetWitness Platform Update Repository
No media devices detected. Please
insert/attach media and click 'Retry'
to continue.

<Retry >      <Ignore>
```

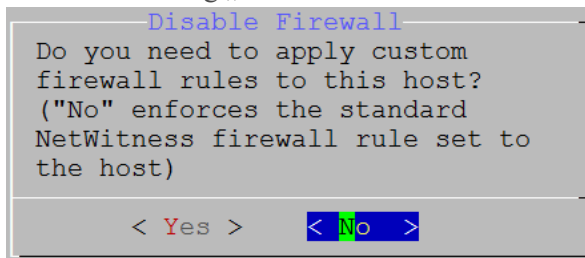
- Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe einer URL aufgefordert. Die Repositories bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates. Anweisungen zum Erstellen dieses Repository und der externen Repo-URL, damit Sie diese in die folgende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



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

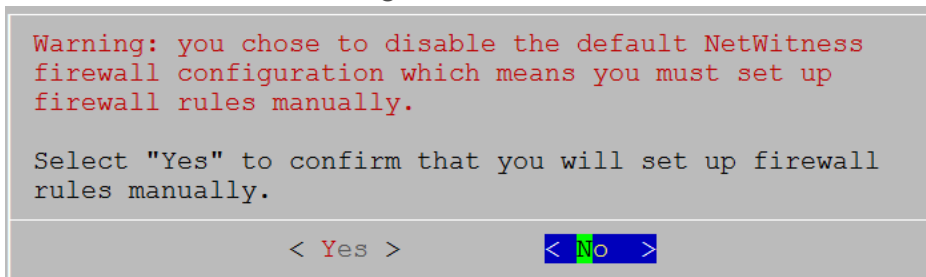
Anweisungen hierzu finden Sie unter „Einrichten eines externen Repository mit RSA und Betriebssystemupdates“ unter „Hosts und Services – Verfahren“ im *RSA NetWitness Platform – Leitfaden für die ersten Schritte mit Hosts und Services*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Die Aufforderung „Firewall deaktivieren“ wird angezeigt.



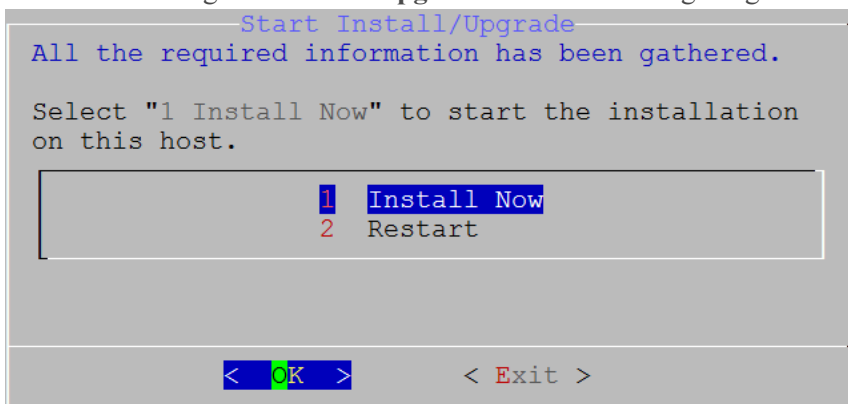
15. Um die Standardkonfiguration für Firewalls zu verwenden, gehen Sie zu **Nein** (Standardauswahl) und drücken die Eingabetaste. Um die Standardkonfiguration für Firewalls zu deaktivieren, gehen Sie zu **Ja** und drücken Sie die **Eingabetaste**.

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





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



16. Drücken Sie die **Eingabetaste**, um 11.3 auf dem NW-Server zu installieren. Wenn **Installation abgeschlossen** angezeigt wird, haben Sie den 11.3 NW-Server auf diesem Host installiert.

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

```
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)
```

17. Lizenzieren Sie den sekundären NW-Server.
- Melden Sie sich bei der sekundären NW-Server-Benutzeroberfläche an, klicken Sie auf **ADMIN > System > Info** und notieren Sie sich die **Lizenzserver-ID** unter **Versionsinformationen**.
  - Stellen Sie über SSH eine Verbindung mit dem primären NW-Server her.
  - Bearbeiten Sie die `/opt/netwitness/flexnetls/local-configuration.yaml` Datei und fügen Sie `back up hostid` (d. h. die **Lizenzserver-ID**) hinzu.  
Dies ist ein Beispiel für den Abschnitt der `local-configuration.yaml` Datei, bevor Sie die **Lizenz Server-ID** hinzufügen.  

```
# Hostid of the backup server, if in fail over configuration.
#backup-hostid:
```

Dies ist ein Beispiel für den Abschnitt der Datei `local-configuration.yaml`, nachdem Sie die MAC-Adresse (z. B. `000c2918c80d`) des aktiven Stand-by-NW-Serverhosts hinzugefügt haben.

```
# Hostid of the backup server, if in fail over configuration.
backup-hostid: "000c2918c80d"
```

- d. Starten Sie den Service „fneserver“ neu.
 

```
systemctl restart flexnetls-RSALM
```
- e. (Bedingungsabhängig) Wenn die Bereitstellung von RSA NetWitness Platform keinen Zugriff auf das Internet hat (Air GAP), müssen Sie folgendermaßen vorgehen:
  - i. Laden Sie die Funktionsanforderung über die NetWitness Platform-Benutzeroberfläche herunter.
  - ii. Laden Sie die Anforderung in FNO hoch.
  - iii. Laden Sie die Antwort von FNO in die NetWitness Platform-Benutzeroberfläche hoch.

18. Planen Sie das Backup des primären NW-Servers und das Kopieren dieser gesicherten Daten auf den sekundären NW-Server.

- a. Stellen Sie über SSH eine Verbindung mit dem primären NW-Server her.

- b. Senden Sie die folgenden Befehle.

```
/opt/rsa/saTools/bin/schedule-standby-admin-data-sync -di <warm-standby-admin-server-ip>
```

Dadurch werden die Daten des primären NW-Servers gesichert und die Backup-Archivdatei wird für die zukünftige Failover-Verwendung täglich auf den sekundären NW-Server kopiert.

Außerdem werden das Backup und die Kopie für die tägliche Ausführung geplant. Sie können die Hilfe für das `schedule-standby-admin-data-sync`-Skript mit der folgenden Befehlszeichenfolge anzeigen.

```
/opt/rsa/saTools/bin/schedule-standby-admin-data-sync --help
```

Dies gibt die folgende Hilfe zurück, in der Sie weitere Informationen zum Anpassen des Backups der Hostdaten (z. B. die Backup-Häufigkeit) finden.

```
Schedule Data Synch between AdminServer and Standby AdminServer
Script also executes a synchronization each time.
```

Usage:

```
schedule-standby-admin-data-sync command [options]
```

Commands:

```
-h, --help           Display Help
-d, --daily          Schedule daily data synchronization
-w, --weekly         Schedule weekly data synchronization
-c, --custom <crontab formatted> Schedule custom data synchronization
                    i.e. to schedule for midnight on 1st
                    and 10th of the month: '0 0 1,10 * *'
                    -
-i, --standby-ip <ip address> IP address of standby Admin Server
-v, --verbose        Enable verbose output
```

## Führen Sie ein Failover des primären NW-Servers zu einem sekundären NW-Server durch.

Der primäre NW-Server führt zunächst ein Failover zum sekundären NW-Server durch. Ein nachfolgendes Failover, d. h. ein Failover vom sekundären NW-Server zum primären NW-Server wird als Failback bezeichnet. Führen Sie das folgende Verfahren durch, um ein Failover vom primären NW-Server zum sekundären NW-Server durchzuführen.

1. Stellen Sie über SSH eine Verbindung mit dem sekundären NW-Server her.
2. Führen Sie das Skript `nw-failover` mit den entsprechenden Argumenten aus. Beispiel:  
`nw-failover --make-active --ip-address <active-nw-server-host-ip> --name <primary-nw-server-hostname>`  
Nachdem das Skript abgeschlossen wurde, wird die folgende Meldung angezeigt:  
`*** Please update network ip and reboot host to complete the fail over process ***`
3. Aktualisieren Sie die CentOS-Netzwerkkonfiguration, um IP-Adressen auszutauschen.
  - **Geplantes Failover** – primärer NW-Server ist nicht fehlgeschlagen:
    - a. Stellen Sie über SSH eine Verbindung mit dem primären NW-Server her.
    - b. Weisen Sie dem primären NW-Server eine nicht verwendete IP-Adresse zu.
    - c. Führen Sie das Failover-Skript mit den entsprechenden Argumenten aus, um die Stand-by-Rolle dem primären NW-Server zuzuweisen. Beispiel:  
`nw-failover --make-standby --ip-address <unused-ip-or-previous-standby-ip> --name <previous-standby-nw-server-hostname>`
    - d. Fahren Sie den primären NW-Server herunter.
    - e. Stellen Sie über SSH eine Verbindung mit dem sekundären NW-Server her.
    - f. Weisen Sie die IP-Adresse des primären NW-Servers zu, den Sie auf dem sekundären NW-Server aufgezeichnet haben.
  - **Erforderliches Failover** – primärer NW-Server ist fehlgeschlagen:
    - a. Stellen Sie über SSH eine Verbindung mit dem sekundären NW-Server her.
    - b. Weisen Sie dem sekundären NW-Server die IP-Adresse des primären NW-Servers zu.
4. Starten Sie den Host neu.

**Hinweis:** Wenn ein schwerwiegender Fehler vorliegt, müssen Sie möglicherweise einen neuen Host bereitstellen oder ein neues Image des primären NW-Servers erstellen und das Verfahren zum [Einrichten des sekundären NW-Servers in der Stand-by-Rolle](#) abschließen, sodass dieser Host einen neuen primären NW-Server erstellt und Sie ein Failback durchführen können.

5. Vergewissern Sie sich, dass das Failover ordnungsgemäß eingerichtet ist.
  - a. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
  - b. Stellen Sie sicher, dass der aktive NW-Server die folgenden Voraussetzungen erfüllt:
    - i. Er kann seine UUID (universelle eindeutige Kennung) auflösen.

```
source /usr/lib/netwitness/bootstrap/resources/nwcommon 2>/dev/null >
/dev/null
nslookup $(getNodeID)
nslookup sollte die aktuelle aktive NW-Server-IP-Adresse zurückgeben.
```
    - ii. Seine IP-Adresse stimmt mit der überein, die im vorherigen Schritt aufgelöst wurde.

## Durchführen eines Failbacks des sekundären NW-Servers zum primären NW-Server

Nach einem Failover vom primären NW-Server zum sekundären NW-Server müssen Sie ein Failback zur ursprünglichen Einrichtung des primären NW-Servers in der aktiven Rolle und zum sekundären NW-Server in der Stand-by-Rolle durchführen.

Im Grunde befolgen Sie dieselben Schritte, die unter [Durchführen eines Failovers des primären NW-Servers zum sekundären NW-Server](#) beschrieben sind, um ein Failback zur ursprünglichen Konfiguration durchzuführen (d. h. primärer NW-Server, aktiv, und sekundärer NW-Server, Stand-by). Der Unterschied besteht darin, dass Sie jetzt ein Failover vom sekundären NW-Server zum primären NW-Server durchführen müssen.

# Netzwerkarchitektur und Ports

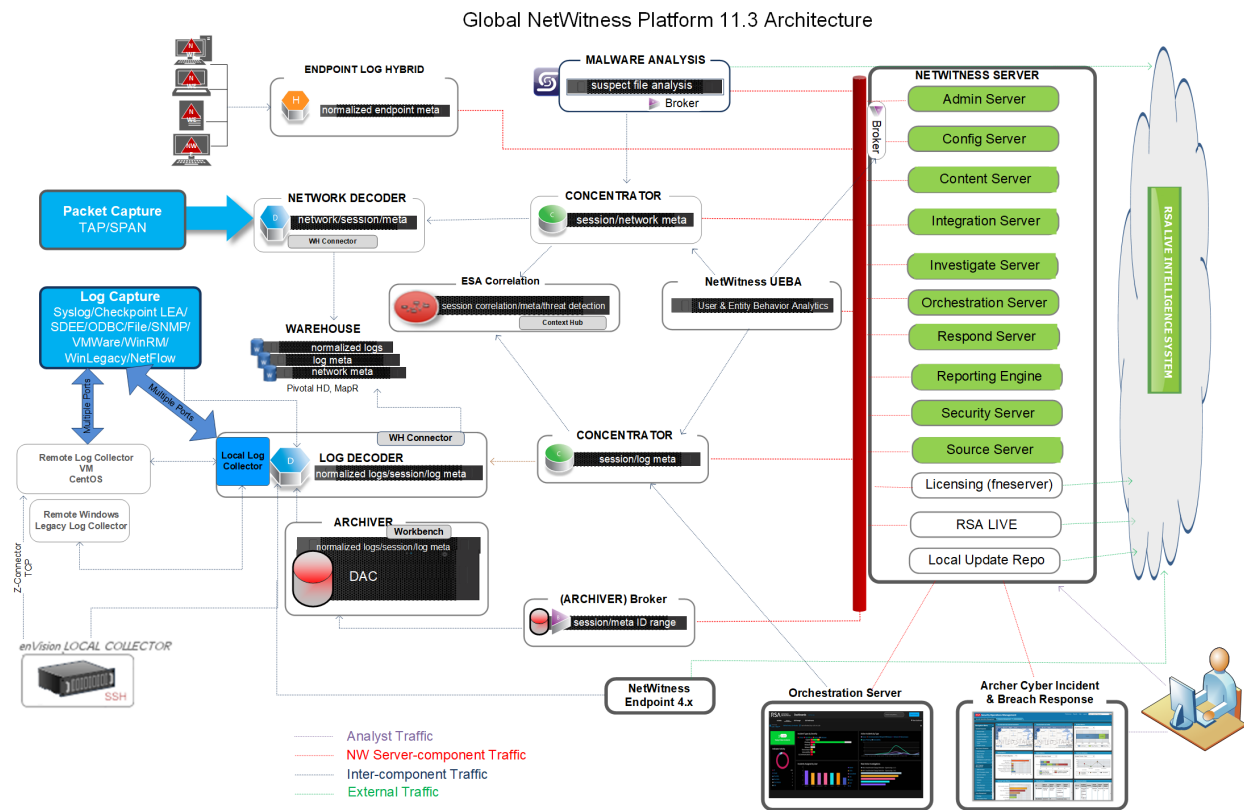
Mit den Informationen im folgenden Diagramm und in der Porttabelle können Sie sicherstellen, dass alle relevanten Ports für Komponenten in Ihrer NetWitness Platform-Bereitstellung geöffnet sind und miteinander kommunizieren können.

Einzelne Endpunkt-Architekturdiagramme finden Sie unter [NetWitness Endpoint-Architektur](#) am Ende dieses Themas.

## Diagramm der NetWitness Platform-Netzwerkarchitektur

Das folgende Diagramm veranschaulicht die Netzwerkarchitektur von NetWitness Platform mit allen zugehörigen Produktkomponenten.

**Hinweis:** NetWitness Platform-Core-Hosts müssen mit dem NetWitness-Server (dem primären Server in einer Bereitstellung mit mehreren Servern) über UDP-Port 123 kommunizieren können, um eine NTP-Synchronisation (Network Time Protocol) durchzuführen.



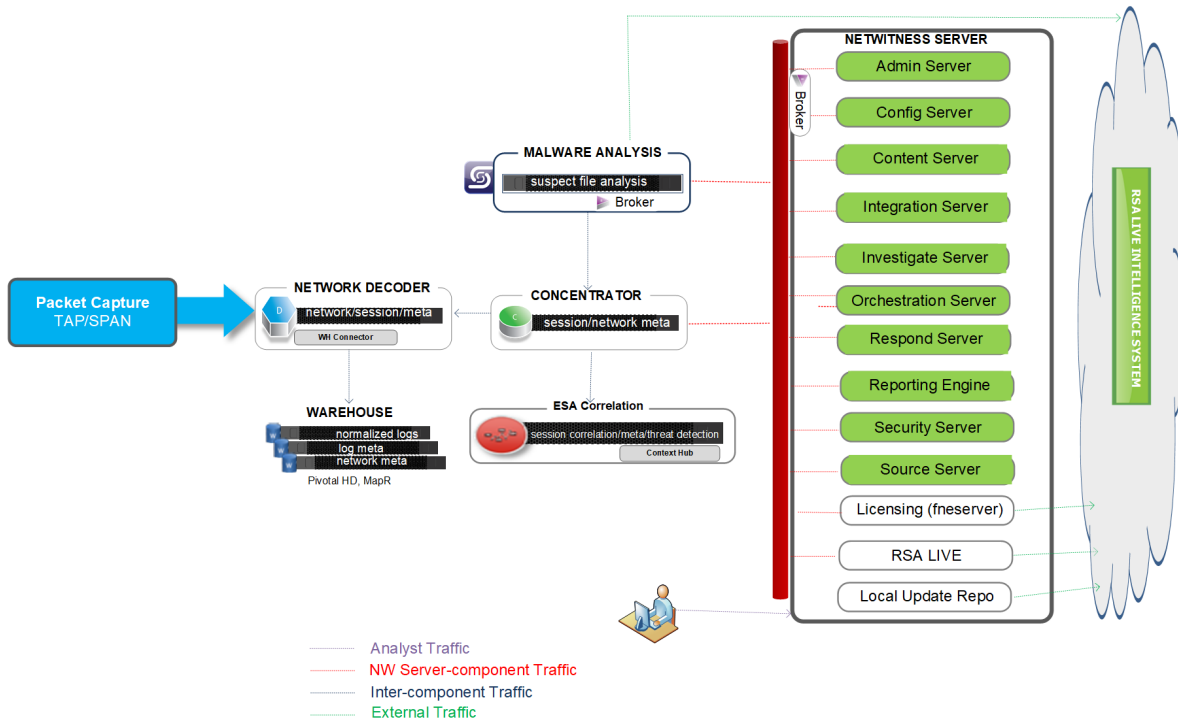
**Note:**  
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).  
 NW Endpoint needs to access <https://cms.netwitness.com> to download Live Feeds.  
 RSA recommends that you use the Broker at the top of your deployment hierarchy for UEBA data source.  
 See *RSA NetWitness Platform Cloud Behavioral Analytics Gateway Configuration Guide* for information on the Cloud Gateway service.



## Diagramm zur Netzwerkarchitektur von NetWitness Network (Packets)

Das folgende Diagramm zeigt die Netzwerkarchitektur von NetWitness Network (Packets).

NetWitness Network 11.3 Architecture



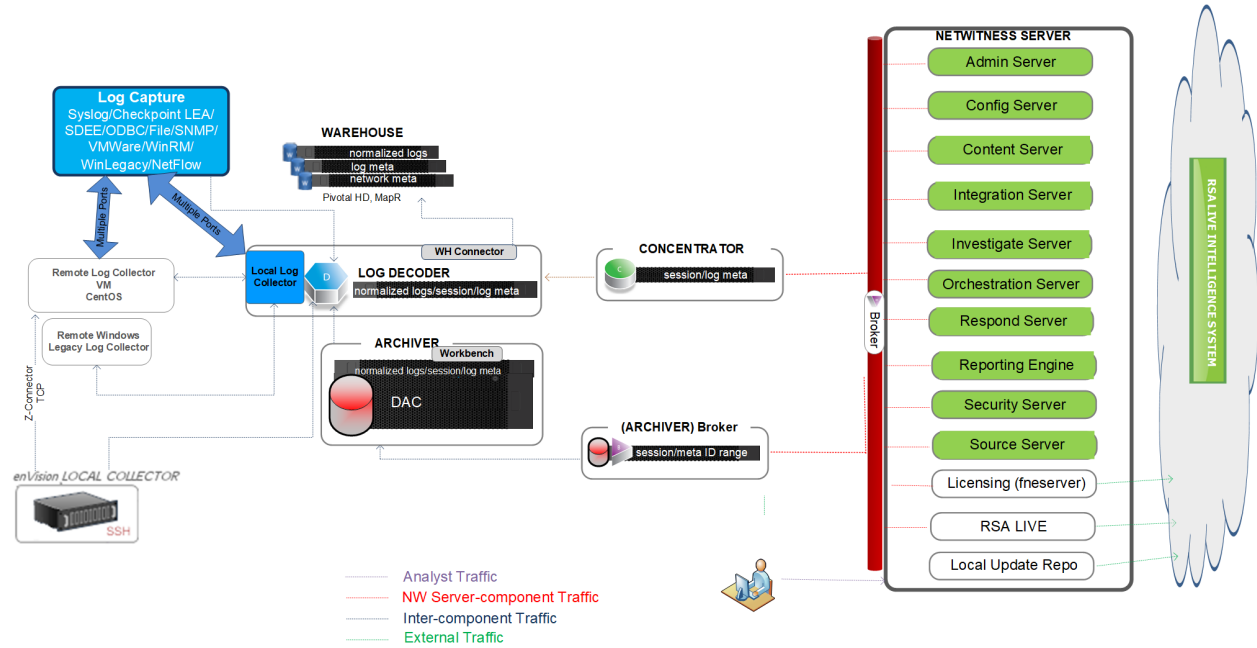
**Notes:**

Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

## Diagramm zur Netzwerkarchitektur NetWitness Logs

Das folgende Diagramm zeigt die Netzwerkarchitektur von NetWitness Logs.

NetWitness Logs 11.3 Architecture



**Note:** Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

## Umfassende Liste der Host-, Service- und iDRAC-Ports von NetWitness Platform

**Hinweis:** Informationen zu Ports, die in der Ereignissammlung über die RSA NetWitness Logs verwendet werden, finden Sie unter „Grundlagen“ im *RSA NetWitness Suite Leitfaden zur Bereitstellung der Protokollsammlung*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Dieser Abschnitt enthält die Portspezifikationen für die folgenden Hosts.

<a href="#">NW-Serverhost</a>	<a href="#">Log Collector-Host</a>
<a href="#">Archiver-Host</a>	<a href="#">Log Decoder-Host</a>
<a href="#">Broker-Host</a>	<a href="#">Log Hybrid-Host</a>
<a href="#">Concentrator-Host</a>	<a href="#">Malware-Host</a>
<a href="#">Endpoint Log Hybrid-Host</a>	<a href="#">Network Decoder-Host</a>
<a href="#">Event Stream Analysis-Host</a>	<a href="#">Network Hybrid-Host</a>
<a href="#">iDRAC-Ports</a>	<a href="#">UEBA-Host</a>



## NW-Serverhost

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	NW-Server	TCP 443, 80	NGINX – NetWitness-Benutzeroberfläche
Admin-Workstation	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Admin-Workstation	NW-Server	TCP 22	SSH
NW-Hosts	NW-Server	TCP 53 UDP 53	DNS
NW-Hosts	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
NW-Hosts	NW-Server	TCP 4505, 4506	Salt Master-Ports
NW-Hosts	NW-Server	TCP 443	RSA Update-Repository
NW-Hosts	NW-Server	TCP 5671	RabbitMQ-amqp
NW-Hosts	NW-Server	UDP 123	NTP
NW-Hosts	NW-Server	TCP 27017	MongoDB
NW-Server	cloud.netwitness.com	TCP 443	Live
NW-Server	cms.netwitness.com	TCP 443	Live
NW-Server	smcupdate.emc.com	TCP 443	Live
NW-Server	NFS-Server	TCP 111, 2049, UDP 111, 2049	iDRAC-Installationen
NW-Server	NW-Hosts	UDP 123	NTP
NW-Server	NW Endpoint	TCP 443, 9443	Für NW-Endpoint 4.x-Integrationen

## Archiver-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Archiver	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Archiver	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Archiver	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Archiver	TCP 22	SSH
NW-Server	Archiver	TCP 56008 (SSL), 50108 (REST)	Archiver-Anwendungsports
NW-Server	Archiver	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Archiver	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
NW-Server	Archiver	TCP 514, 6514, 56007 (SSL), 50107 (REST), UDP 514	Workbench-Anwendungsports
Archiver	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

## Broker-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Broker	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Broker	Concentrator	TCP 56005	Concentrator-Anwendungsport
Broker	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Broker	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Broker	TCP 22	SSH
NW-Server	Broker	TCP 56003 (SSL), 50103 (REST)	Broker-Anwendungsports
NW-Server	Broker	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Broker	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Broker	NW-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen
Endpoint Broker	NW-Server	TCP 443	RSA Update-Repository

## Concentrator-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Concentrator	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Concentrator	Log Decoder	TCP 56002	Concentrator-Anwendungsport
Concentrator	Network Decoder	TCP 56004	Concentrator-Anwendungsport
Concentrator	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Concentrator	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Concentrator	TCP 22	SSH
NW-Server	Concentrator	TCP 56005 (SSL), 50105 (REST)	Concentrator-Anwendungsports
Malware	Concentrator	TCP 56005 (SSL)	Malware
NW-Server	Concentrator	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Concentrator	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Concentrator	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

## Endpoint Log Hybrid

Quellhost	Zielhost	Zielports	Anmerkungen
Endpoint-Agent	Endpoint Log Hybrid	TCP 443 UDP 444	NGINX HTTPS NGINX UDP. Wenn UDP Port 444 in Ihrer Umgebung nicht akzeptabel ist, finden Sie weitere Informationen unter <a href="#">Ändern des UDP-Ports für Endpoint Log Hybrid</a> .
Endpoint-Agent	Log Decoder oder Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows-Protokollsammlung
Endpoint Log Hybrid	Log Decoder (extern)	TCP 50102 (REST) 56202 (Protobuf SSL) 50202 (Protobuf)	Um Metadaten an einen externen Log Decoder weiterzuleiten
Endpoint Log Hybrid	NW-Server	TCP 443	RSA Update-Repository
NW-Server	Endpoint Log Hybrid	TCP 7050	Webdatenverkehr über die Benutzeroberfläche
Endpoint Log Hybrid	NW-Server	TCP 5671	Nachrichtenbus
Endpoint Log Hybrid	NW-Server	TCP 27017	MongoDB
NW-Server	Endpoint Log Hybrid	TCP 7054	Webdatenverkehr über die Benutzeroberfläche
NW-Server	NFS-Server	TCP 111, 2049 UDP 111, 2049	iDRAC-Installationen

## Event Stream Analysis (ESA)-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	ESA	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
ESA Primary und Secondary	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
ESA Primary und Secondary	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	ESA	TCP 22	SSH
NW-Server, ESA Secondary	ESA Primary	TCP 27017	MongoDB
NW-Server	ESA Primary	TCP 7005	Context Hub Launch-Port – (ESA Primary)
NW-Server	ESA	TCP 50030 (SSL)	ESA-Anwendungsport
NW-Server	ESA	TCP 50035 (SSL)	ESA-Anwendungsport
NW-Server	ESA	TCP 50036 (SSL)	ESA-Anwendungsport
NW-Server	ESA	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
ESA Primary und Secondary	cms.netwitness.com	TCP 443	Live
ESA Primary und Secondary	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen
ESA Primary und Secondary	Active Directory	636 (SSL)/389 (Nicht-SSL)	
NW-Server	ESA	80 (HTTP)/443 (HTTPS)(REST)	
ESA Primary	Archer	443 (SSL)/80 (Nicht-SSL)	
ESA Primary	ESA Primary	TCP 7007	Start-Port

## iDRAC Ports

Port	Funktion	Anmerkungen
22*	SSH	Standardmäßiger, konfigurierbarer Port, über den iDRAC auf Verbindungen lauscht
443*	HTTP	Standardmäßiger, konfigurierbarer Port, über den iDRAC auf Verbindungen lauscht
5900*	Virtuelle Konsolentastatur- und -mausumleitung, virtuelle Medien, virtuelle Ordner und Remotedateifreigabe	Standardmäßiger, konfigurierbarer Port, über den iDRAC auf Verbindungen lauscht
111, 2049	TCP	NetWitness Platform-Hosts zu NFS-Server
111, 2049	UDP	NetWitness Platform-Hosts zu NFS-Server

## Log Collector-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Collector	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Collector	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Collector	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Log Collector	TCP 22	SSH
Log Collector	Protokollereignisquellen	Siehe <i>Protokollsammlung-Konfigurationsleitfaden</i> . Navigieren Sie zu <a href="#">Masterinhaltsverzeichnis</a> , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.	
Protokollereignisquellen	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Protokollsammelungsports
Protokollereignisquellen	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Protokollsammelungs-FTP/S-Ports
NW-Server	Log Collector	TCP 56001 (SSL), 50101 (REST)	Log Collector-Anwendungsports
NW-Server	Log Collector	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Log Collector	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Log Collector	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen
Log Collector	Virtual Log Collector	TCP 5671	Im Pull-Modus



Quellhost	Zielhost	Zielports	Anmerkungen
Virtual Log Collector	Log Collector	TCP 5671	Im Push-Modus

## Log Decoder-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Decoder	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Decoder	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Protokollereignisquellen	Siehe <i>Protokollsammlung-Konfigurationsleitfaden</i> . Navigieren Sie zu <a href="#">Masterinhaltsverzeichnis</a> , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.	
Protokollereignisquellen	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Protokollsammlungsports
Protokollereignisquellen	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Protokollsammlungs-FTP/S-Ports
NW-Server	Log Decoder	TCP 56001 (SSL), 50101 (REST)	Log Collector-Anwendungsports
NW-Server	Log Decoder	TCP 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder-Anwendungsports
NW-Server	Log Decoder	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

## Log Hybrid-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Log Hybrid	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Hybrid	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Log Hybrid	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Protokollereignisquellen	Siehe <i>Protokollsammlung-Konfigurationsleitfaden</i> . Navigieren Sie zu <a href="#">Masterinhaltsverzeichnis</a> , worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.	
Protokollereignisquellen	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Protokollsammelungsports
Protokollereignisquellen	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Protokollsammelungs-FTP/S-Ports
NW-Server	Log Hybrid	TCP 56001 (SSL), 50101 (REST)	Log Collector-Anwendungsports
NW-Server	Log Hybrid	TCP 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Log Decoder-Anwendungsports
NW-Server	Log Hybrid	TCP 56005 (SSL), 50105 (REST)	Concentrator-Anwendungsports
NW-Server	Log Hybrid	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports

---

Quellhost	Zielhost	Zielports	Anmerkungen
NW-Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS)- Nachrichtenbus für alle NW- Hosts
Log Hybrid	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

## Malware-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Malware	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Malware	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Malware	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Malware	TCP 22	SSH
NW-Server	Malware	TCP 60007	Malware-Anwendungsports
NW-Server	Malware	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Malware	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
NW-Server	Malware	TCP 5432	PostgreSQL
NW-Server	Malware	TCP 56003 (SSL), 50103 (REST)	Broker-Anwendungsports
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community-Bewertung/Opwat
Malware	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

## Network Decoder-Host

Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Network Decoder	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Decoder	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Decoder	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Network Decoder	TCP 22	SSH
NW-Server	Network Decoder	TCP 56004 (SSL), 50104 (REST)	Network Decoder-Anwendungsports
NW-Server	Network Decoder	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Network Decoder	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Network Decoder	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

## Network Hybrid-Host

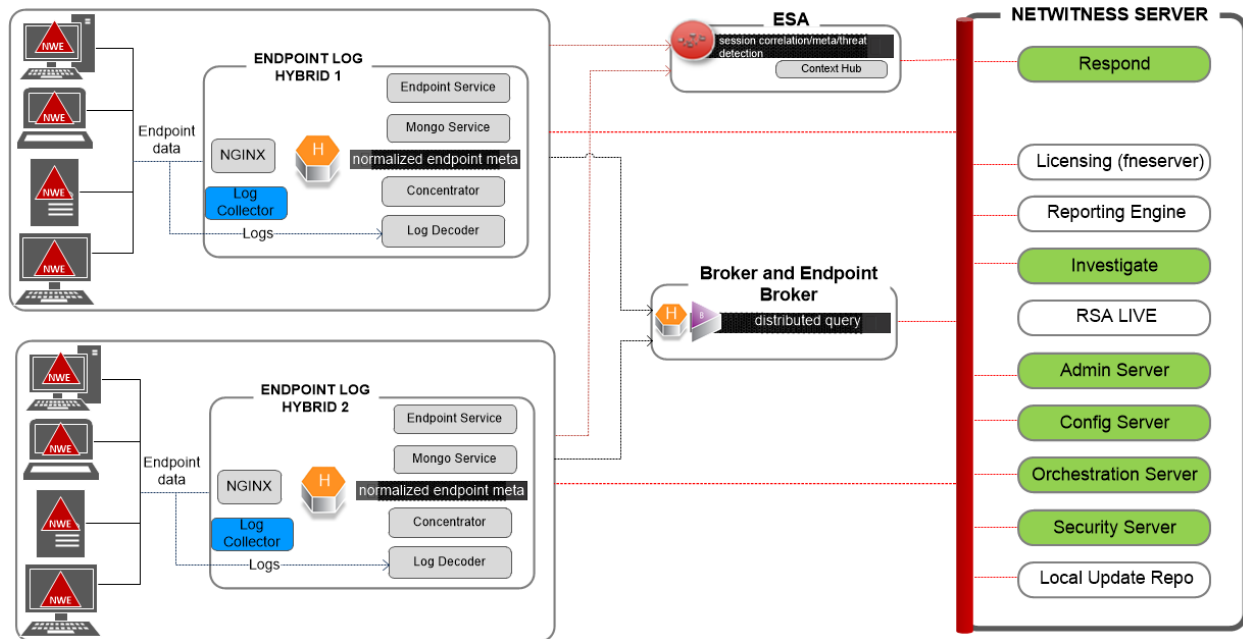
Quellhost	Zielhost	Zielports	Anmerkungen
Admin-Workstation	Network Hybrid	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Hybrid	NW-Server	TCP 15671	RabbitMQ-Managementbenutzeroberfläche
Network Hybrid	NW-Server	TCP 443	RSA Update-Repository
Admin-Workstation	Network Hybrid	TCP 22	SSH
NW-Server	Network Hybrid	TCP 56004 (SSL), 50104 (REST)	Network Decoder-Anwendungsports
NW-Server	Network Hybrid	TCP 56005 (SSL), 50105 (REST)	Concentrator-Anwendungsports
NW-Server	Network Hybrid	TCP 56006 (SSL), 50106 (REST)	NetWitness-Appliance-Ports
NW-Server	Network Hybrid	TCP 5671	RabbitMQ (AMQPS)-Nachrichtenbus für alle NW-Hosts
Network Hybrid	NFS-Server	TCP 111 2049 UDP 111 2049	iDRAC-Installationen

**UEBA-Host**

Quellhost	Zielhost	Zielports	Anmerkungen
UEBA-Server	NW-Server	TCP 443	RSA Update-Repository
UEBA-Server	Broker	TCP 56003 (SSL), 50103 (REST)	Broker-Anwendungsports
UEBA-Server	Concentrator	TCP 56005 (SSL), 50105 (REST)	Concentrator-Anwendungsports
Admin-Workstation	UEBA-Server	443	UEBA-Monitoring
Admin-Workstation	UEBA-Server	22	SSH
UEBA-Server	NW-Server	15671	UEBA-Warnmeldungen werden an Respond weitergeleitet
NW-Server	NFS-Server	TCP 111, 2049 UDP 111, 2049	iDRAC-Installationen

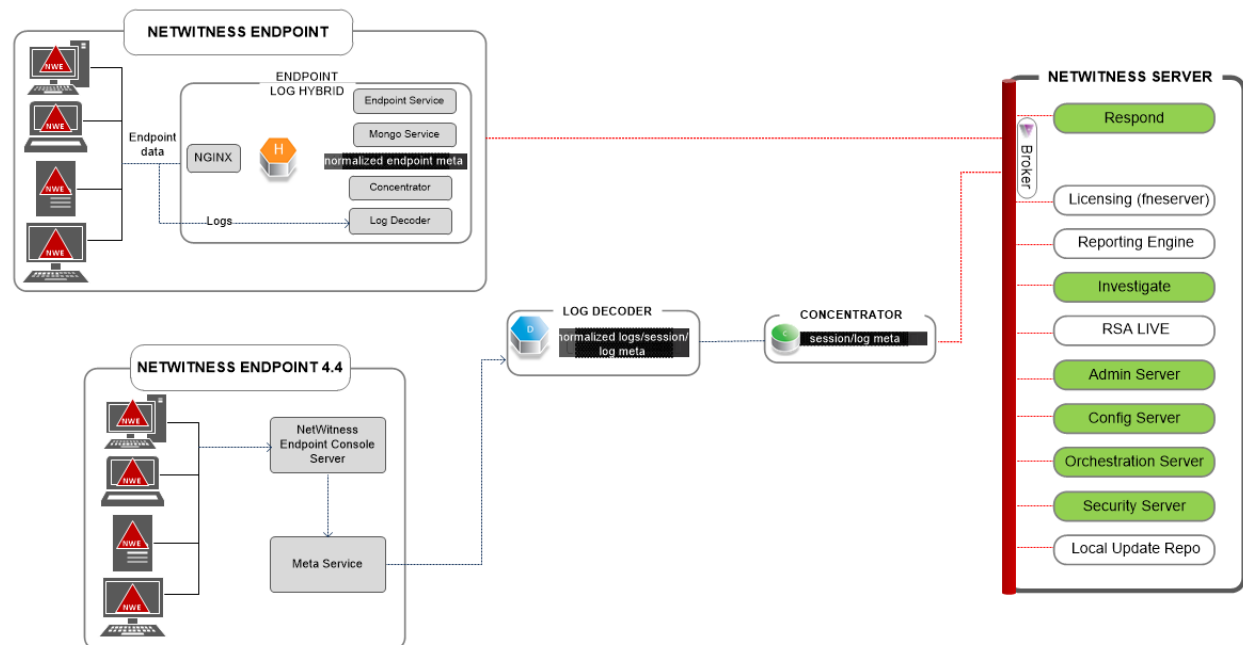


## NetWitness Endpoint-Architektur



**Note:** Log Collector collects Windows logs from event sources.

## NetWitness Endpoint 4.4-Integration in NetWitness Platform



Weitere Informationen zu Services, die auf Endpoint Log Hybrid ausgeführt werden, finden Sie unter *Konfigurationsleitfaden für RSA NetWitness Endpoint*.

## So ändern Sie den UDP-Port für Endpoint Log Hybrid

In den folgenden Schritten erfahren Sie, wie Sie den standardmäßigen UDP-Port 444 des Endpoint Log Hybrid ändern können, wenn er in Ihrer Umgebung nicht akzeptabel ist. 555 ist das Beispiel, das dieses Verfahren als Ersatz für den 444 UDP-Port verwendet.

Es gibt zwei Aufgaben, die Sie ausführen müssen, um den Endpoint Log Hybrid-Standard-UDP-Port 444 zu ändern:

**Aufgabe 1:** Teilen Sie allen Agents mit, dass sie einen neuen UDP-Port verwenden sollen

**Aufgabe 2:** Aktualisieren Sie den Port auf allen Endpoint Log Hybrid-Hosts in Ihrer Umgebung

**Hinweis:** Wenn Sie bei der Ausführung von `nwsetup-tui` die Option für benutzerdefinierte Firewall-Regeln nicht ausgewählt haben, überschreibt NetWitness Platform die Firewall-Regeln nach einiger Zeit. Lesen Sie in diesem Fall den folgenden Wissensdatenbankartikel 00036446 (<https://community.rsa.com/docs/DOC-93651>).

### Aufgabe 1: Teilen Sie allen Agents mit, dass sie einen neuen UDP-Port verwenden sollen

Führen Sie die folgenden Schritte aus, um den UDP-Port in der Standard-EDR-Policy (Enterprise Data Replication) und allen anderen Policies, die Sie haben, zu aktualisieren, um allen Agenten mitzuteilen, einen neuen UDP-Port zu verwenden.

1. Wählen Sie im Menü **NetWitness Platform** die Option **ADMIN > Endpoint-Quellen > Policies** aus.  
Die Ansicht **Policies** wird angezeigt.
2. Wählen Sie die **Standard-EDR-Policy** aus und klicken Sie in der Symbolleiste auf **Bearbeiten**.
3. Blättern Sie nach unten, um den **UDP-Port** zu suchen und ändern Sie den Wert (z. B. von **444** auf **555**).
4. Klicken Sie am unteren Rand der Ansicht auf **Policy veröffentlichen**.

### Aufgabe 2: Aktualisieren Sie den Port auf allen Endpoint Log Hybrid-Hosts in Ihrer Umgebung

Stellen Sie über SSH eine Verbindung her zu jedem Endpoint Log Hybrid-Host in Ihrer Umgebung mit `admin` Anmeldeinformationen und führen Sie die folgenden Updates durch.

1. Aktualisieren Sie die `iptables` Regeln, um 555 anstelle von 444 zu ermöglichen.
  - a. Ersetzen Sie in der folgenden Datei 444 durch 555 .  
`vi /etc/sysconfig/iptables`
  - b. Starten Sie `iptables` mit der folgenden Befehlszeichenfolge neu.  
`systemctl restart iptables`
  - c. Überprüfen Sie die Änderung mit der folgenden Befehlszeichenfolge.  
`iptables -L -n`  
Nachfolgend ein Beispiel dafür, was für eine korrekte Änderung angezeigt wird.

```
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp multiport dports 555 /*  
EndpointNginxPort */ ctstate NEW
```

2. Aktualisieren Sie die SELinux-Policy. 555 ist ein privilegierter Port, daher müssen Sie die SELinux-Policy aktualisieren, um diesen Port zuzulassen.

- a. Führen Sie die folgende Befehlszeichenfolge aus.

```
semanage port -a -t http_port_t -p udp 555
```

Wenn Sie Python-Fehler oder Warnungen erhalten, ignorieren Sie diese.

- b. Überprüfen Sie die Änderung mit der folgenden Befehlszeichenfolge.

```
semanage port -l | grep http_port_t
```

Nachfolgend ein Beispiel dafür, was für eine korrekte Änderung angezeigt wird.

```
http_port_t udp 555, 444
```

- c. (Optional) Entfernen Sie 444.

3. Aktualisieren Sie nginx config.

- a. Bearbeiten Sie die folgende Datei.

```
vi /etc/nginx/nginx.conf
```

- b. Suchen Sie die folgende Zeichenfolge.

```
listen 444 udp;
```

- c. Ersetzen Sie 444 durch:555

- d. Starten Sie nginx mit der folgenden Befehlszeichenfolge neu.

```
systemctl restart nginx
```

4. Überprüfen Sie, ob die Agents über den neuen Port kommunizieren.

- a. Führen Sie die folgende Befehlszeichenfolge aus.

```
tcpdump -i eth0 port 555
```

- b. Warten Sie 30 Sekunden, da der Port alle 30 Sekunden ein Beacon sendet. Wenn alles ordnungsgemäß funktioniert, werden Informationen ähnlich der folgenden angezeigt.

```
09:20:12.571316 IP 10.40.15.103.60807 >
```

```
NiranjanEPS1.rsa.lab.emc.com.dsf: UDP, length 20
```

```
09:20:12.572433 IP NiranjanEPS1.rsa.lab.emc.com.dsf >
```

```
10.40.15.103.60807: UDP, length 1
```

Beide Zeilen müssen zurückgegeben werden. Eine ist die Größenanforderung (20 Byte) und die andere die Antwortgröße (1 Byte).

## Anforderungen an den Standort und Sicherheit

---

Lesen Sie dieses Thema unbedingt sorgfältig durch und beachten Sie alle Warnhinweise und Vorsichtsmaßnahmen vor der Installation oder Wartung Ihrer RSA-Geräte.

### Vorgesehene Anwendung

Dieses Produkt ist ein Informationstechnologie-Gerät, das in Büros, Schulen, Computerräumen und ähnlichen gewerblich genutzten Innenräumen installiert werden kann. Das Gerät ist nicht zur Verbindung mit einem Außenkabel geeignet.

### Service

Dieses Gerät enthält keine Komponenten, die vom Nutzer gewartet werden können. Im Falle einer Funktionsstörung kontaktieren Sie bitte den Customer Service. Im Falle einer Störung können sich innerhalb des Geräts hohe Temperaturen entwickeln, was ein Alarmsignal auslöst. Ertönt ein solches Alarmsignal, sollten Sie das Gerät umgehend von der Stromquelle trennen und den Customer Service kontaktieren. Eine weitere Verwendung des Geräts würde ein Sicherheitsrisiko darstellen und könnte zu Verletzungen und Sachschäden führen.

### Sicherheitsinformationen

#### Standortauswahl

Das System ist für eine typische Büroumgebung konzipiert. Wählen Sie einen Standort nach den folgenden Kriterien aus:

- Sauber, trocken und ohne Partikel in der Luft (abgesehen von dem normalen Hausstaub).
- Gut belüftet und nicht in der Nähe von Hitzequellen, wie direktes Sonnenlicht oder Heizungen.
- Nicht in der Nähe von Vibrations- oder Erschütterungsquellen.
- Isoliert von starken elektromagnetischen Feldern, die durch elektronische Geräte erzeugt werden.
- In Regionen, die anfällig für Gewitterstürme sind, empfehlen wir, das System an einen Überspannungsschutz anzuschließen.
- Ausgestattet mit ordnungsgemäß geerdeten Wandsteckdosen.
- Ausreichend Platz, um auf Netzkabel zugreifen zu können, da diese die Hauptstromquelle darstellen.

#### Vorgehensweise zur Handhabung des Geräts

Reduzieren Sie das Risiko von Personen- oder Sachschäden, indem Sie Folgendes beachten:

- Halten Sie die lokalen Vorschriften zu Sicherheit und Gesundheitsschutz am Arbeitsplatz ein, wenn Sie das Gerät anheben oder bewegen.
- Verwenden Sie mechanische oder andere geeignete Hilfsmittel, wenn Sie das Gerät anheben oder bewegen.
- Verringern Sie das Gewicht des Geräts für eine leichtere Handhabung, indem Sie alle leicht lösbaren Komponenten entfernen.

### Warnhinweise für Strom und Elektronik

**Achtung:** Der Hauptschalter, gekennzeichnet durch die Stand-by-Stromversorgungsanzeige, schaltet die Wechselstromversorgung des Systems NICHT komplett aus. Ein Stand-by-Stromverbrauch von 5 V ist immer zu verzeichnen, wenn das System angeschlossen ist. Um die Stromversorgung des Systems zu unterbrechen, müssen Sie die Wechselstromkabel aus der Steckdose ziehen.

- Verwenden und bearbeiten Sie kein Wechselstromkabel, das nicht exakt dem erforderlichen Typ entspricht. Für jede Systemversorgung wird ein separates Netzkabel benötigt.
- Dieses Produkt enthält keine Komponenten, die vom Nutzer gewartet werden können. Öffnen Sie das System nicht.
- Beim Austauschen von Hot-Plug-Netzteilen ziehen Sie das Stromkabel von dem auszutauschenden Netzteil ab, bevor Sie es von dem Server entfernen.

### Warnhinweise für Rackmontage

- Befestigen Sie das Rack des Geräts an einem nicht beweglichen Gebäudeteil, um ein Umfallen zu verhindern, wenn ein Server oder Teil des Geräts erweitert wird. Das Rack muss gemäß den Herstelleranweisungen für die Rackmontage installiert werden.
- Die Montage des Geräts in einer Rackhalterung sollte so vorgenommen werden, dass keine gefährliche Situation aufgrund einer ungleichmäßigen mechanischen Belastung entstehen kann.
- Erweitern Sie die Anlage jeweils nur mit einem Teil vom Rack aus.
- Um das Risiko eines möglichen Stromschlags zu vermeiden, muss eine ordnungsgemäße Sicherheitserdung für das Rack und alle darin installierten Anlagenteile eingerichtet sein.

### Kühlung und Luftstrom

Die Installation des Geräts sollte so erfolgen, dass die für den sicheren Betrieb der Geräte erforderliche Luftstrommenge nicht beeinträchtigt wird.