



# Leitfaden zur Aktualisierung

für Version 11.0.x.x oder 11.1.x.x auf 11.2



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

## **Kontaktinformationen**

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

## **Marken**

Eine Liste der RSA-Marken finden Sie unter [germany.emc.com/legal/emc-corporation-trademarks.htm#rsa](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 Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

## **Hinweis zu Verschlüsselungstechnologien**

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

## **Verteilung**

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

Februar 2019

# Inhalt

---

<b>Einführung</b> .....	<b>5</b>
Aktualisierungspfad .....	5
Ausführen im gemischten Modus .....	5
Zurücksetzen des Flags „Entropy=log2“ nach der Aktualisierung .....	5
<b>Aufgaben zur Vorbereitung der Aktualisierung</b> .....	<b>7</b>
Allgemein .....	7
Aufgabe 1: Prüfen der Core-Ports und Öffnen von Firewallports .....	7
Aufgabe 2: Sichern der Malware Analysis-Konfigurationsdatei in einem anderen Verzeichnis .....	7
Aufgabe 3: Beenden der Datenerfassung und -aggregation .....	8
Azure Hosts .....	10
Aufgabe 4: (Bedingungsabhängig) Anforderungen der Vorbereitung für die Azure Host-Aktualisierung .....	10
Endpoint Insights .....	11
Aufgabe 5: (Bedingungsabhängig) Sichern vorhandener benutzerdefinierter Metadatenzuordnungen vor dem Anwenden der Aktualisierung 11.2 auf einen Endpoint-Host .....	11
Reporting Engine .....	11
Aufgabe 6: Konfigurieren der Reporting Engine für vorkonfigurierte Diagramme .....	11
Respond .....	12
Aufgabe 7: (Bedingungsabhängig) Wiederherstellen der benutzerdefinierten Schlüssel für den Respond-Service .....	12
Aufgabe 8: Sichern der angepassten Skripte zur Normalisierung des Respond-Service .....	12
<b>Aufgaben bei der Aktualisierung</b> .....	<b>13</b>
Anwenden von Aktualisierungen über die Ansicht „Hosts“ (Webzugriff) .....	13
Aufgabe 1. Auffüllen des lokalen Repository oder Einrichten eines externen Repository .....	13
Aufgabe 2. Anwenden von Aktualisierungen über die Ansicht „Hosts“ auf einzelne Hosts .....	14
Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff) .....	18
<b>Aktualisieren oder Installieren der Legacy-Windows-Sammlung</b> .....	<b>20</b>
<b>Aufgaben nach der Aktualisierung</b> .....	<b>21</b>
Allgemeines .....	22
Aufgabe 1: Starten der Datenerfassung und -aggregation .....	22
Aufgabe 2: Einrichten von Benutzerberechtigungen für Kontextmenüaktionen .....	23
NW-Server .....	25
Aufgabe 3: (Bedingungsabhängig) Korrigieren der Auditprotokollvorlagen, die in der Logstash-Ausgabe-Konfigurationsdatei nicht aktualisiert werden .....	25
(Bedingungsabhängig) Aufgabe 4: Neukonfigurieren der PAM-Radius-Authentifizierung .....	25
Endpoint Insights .....	26

---

Aufgabe 5: Neukonfigurieren eines wiederkehrenden Feeds, der über Legacy Endpoint konfiguriert wurde, da sich die Java-Version geändert hat .....	26
Aufgabe 6: Wiederherstellen gesicherter benutzerdefinierter Endpoint-Metadatenzuordnungen ....	26
Event Stream Analysis .....	27
(Bedingungsabhängig) Aufgabe 7: Neukonfigurieren der Aggregationsregel „Verdacht auf Command-and-Control-Kommunikation von Domain“ für die automatisierte Bedrohungserkennung .....	27
Respond .....	28
Aufgabe 8: Abrufen der aktuellen Version des Schemas für Aggregationsregeln und Wiederherstellen aller benutzerdefinierten Schlüssel des Respond-Service .....	28
Aufgabe 9: Abrufen der aktuellen Version der Skripte zur Normalisierung des Respond-Service und Wiederherstellung aller benutzerdefinierten Skripte zur Normalisierung des Respond-Service ..	29
Aufgabe 10: Hinzufügen von Einstellungen für Antwort auf Benachrichtigungen .....	29
Aufgabe 11: Aktualisieren der „Gruppieren nach“-Werte der Incident-Standardregel .....	30
NetWitness UEBA .....	31
Aufgabe 12: Installieren von NetWitness UEBA .....	31
<b>Anhang A: Troubleshooting von Versionsinstallationen und -aktualisierungen .....</b>	<b>32</b>
<b>Anhang B: Auffüllen des lokalen Repository .....</b>	<b>39</b>
<b>Anhang C: Einrichten eines externen Repository .....</b>	<b>41</b>
<b>Revisionsverlauf .....</b>	<b>44</b>

## Einführung

---

RSA NetWitness® Platform 11.2.0.0 stellt Korrekturen für alle Produkte in der Plattform bereit. Die Komponenten der Plattform sind der NetWitness Server (Admin-Server, Konfigurationsserver, Integrationsserver, Investigate-Server, Orchestrierungsserver, Antwortserver, Security-Server und Quellserver), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, UEBA, Warehouse Connector und Workbench.

**Hinweis:** Die Reporting Engine ist auf dem NW-Serverhost installiert, Workbench auf dem Archiver-Host installiert, Warehouse Connector kann auf dem Decoder-Host oder dem Log Decoder-Host installiert werden.

Falls nicht anders angegeben, gelten die Anweisungen in diesem Handbuch sowohl für physische als auch für virtuelle Hosts (einschließlich AWS und Azure Public Cloud).

## Aktualisierungspfad

Die folgenden Aktualisierungspfade werden für NetWitness Platform 11.2.0.0 unterstützt:

- 11.0.x auf 11.2.0.0
- 11.1.x auf 11.2.0.0
- 10.6.6.x auf 11.2.0.0

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

Anweisungen zum Upgrade von 10.6.6.x auf 11.2 finden Sie unter *RSA NetWitness Platform 10.6.6.x auf 11.2 – Upgradehandbuch für physische Hosts* und *RSA NetWitness Platform 10.6.6.x auf 11.2.0.0 – Upgradehandbuch für virtuelle Hosts*.

## Ausführen im gemischten Modus

Der gemischte Modus ist aktiv, wenn einige Services auf die neue Version aktualisiert werden und andere in älteren Versionen beibehalten werden. Weitere Informationen finden Sie unter „Ausführen im gemischten Modus“ im *RSA NetWitness Platform – Leitfaden für die ersten Schritte mit Hosts und Services*.

## Zurücksetzen des Flags „Entropy=log2“ nach der Aktualisierung

Wenn das Flag `Entropy=log2` in 11.0.x.x auf `false` (`Entropy="log2=false"`) festgelegt ist, setzt NetWitness dieses Flag auf „true“ zurück (`Entropy="log2=true"`), nachdem Sie ein Upgrade auf 11.2 durchgeführt haben, damit alle Quellen Pakete und NetWitness Endpoint Insights enthalten. Falls gewünscht, können Sie das Flag auf „false“ setzen, um die log10-Berechnung beizubehalten: `Entropy="log2=false"`.



## Aufgaben zur Vorbereitung der Aktualisierung

---

Führen Sie die folgenden Aufgaben durch, um das Upgrade auf NetWitness Platform 11.2.0.0 vorzubereiten. Diese Aufgaben sind in die folgenden Kategorien unterteilt.

[Allgemeines](#)

[Azure Hosts](#)

[Endpoint Insights](#)

[Reporting Engine](#)

[Respond](#)

### Allgemein

#### Aufgabe 1: Prüfen der Core-Ports und Öffnen von Firewallports

In den folgenden Tabellen sind die neuen Ports in 11.2.0.0 aufgeführt.

**Achtung:** Stellen Sie vor der Aktualisierung sicher, dass die neuen Ports implementiert und getestet wurden, damit die Aktualisierung nicht aufgrund von fehlenden Ports fehlschlägt.

##### Endpoint Hybrid oder Endpoint Log Hybrid

Quellhost	Zielhost	Zielports	Anmerkungen
Endpoint Hybrid oder Endpoint Log Hybrid	NW-Server	TCP 5672	Nachrichtenbus
Endpunktserver	NW-Server	TCP 27017	MongoDB

#### Aufgabe 2: Sichern der Malware Analysis-Konfigurationsdatei in einem anderen Verzeichnis

- Erstellen Sie eine Sicherungskopie der folgenden Datei in einem anderen, sicheren Verzeichnis.  
`/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`  
Sie müssen Ihre angepassten Parameterwerte aus diesem Backup abrufen, nachdem Sie den Malware Analysis-Host auf 11.2.0.0 aktualisiert haben. Die Aktualisierung erzeugt eine neue Konfigurationsdatei, in der alle Parameter auf die Standardwerte eingestellt sind.
- Löschen Sie die folgende Datei.  
`/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`



## Aufgabe 3: Beenden der Datenerfassung und -aggregation

### Beenden der Netzwerkerfassung

1. Melden Sie sich bei NetWitness Platform 11.0.x an und wechseln Sie zu **ADMIN > Services**. Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie die einzelnen **Decoder**-Services aus.

The screenshot displays the NetWitness Platform interface. At the top, the navigation bar includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this, a secondary navigation bar shows 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Services' tab is active, and the 'S5Decoder - Decoder' service is selected. A toolbar contains actions like 'Change Service', 'Upload Packet Capture File', 'Stop Capture', 'Host Tasks', 'Shutdown Service', 'Shutdown Appliance Service', and 'Reboot'. The main content area is divided into four sections: 'Decoder Service Information', 'Appliance Service Information', 'Decoder User Information', and 'Host User Information'. Each section lists details such as Name, Version, Memory Usage, CPU, Running Since, Uptime, and Current Time.

Decoder Service Information		Appliance Service Information	
Name	S5Decoder (Decoder)	Name	S5Decoder (Host)
Version	11.1.0.0	Version	11.1.0.0 (
Memory Usage	2858 MB (2.54% of 110 GB)	Memory Usage	25964 KB (0.02% of 110 GB)
CPU	1%	CPU	0%
Running Since	2018-Feb-08 02:32:47	Running Since	2018-Feb-06 22:14:56
Uptime	11 hours 23 minutes 46 seconds	Uptime	1 day 15 hours 41 minutes 38 seconds
Current Time	2018-Feb-08 13:56:33	Current Time	2018-Feb-08 13:56:34

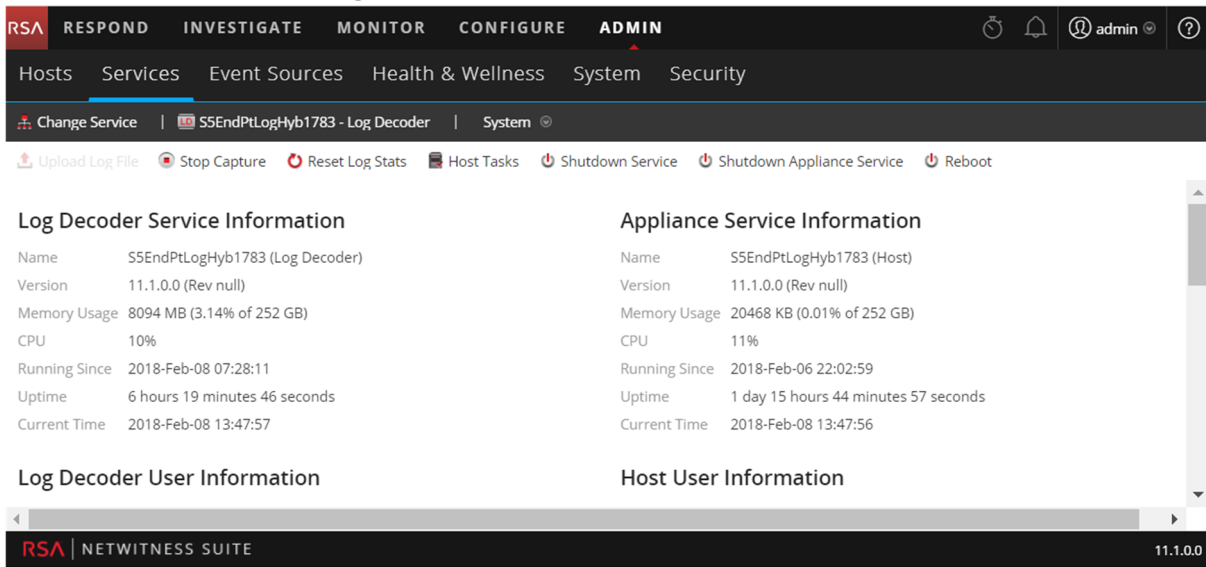
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht > System** aus.
4. Klicken Sie in der Symbolleiste auf  **Stop Capture**.

### Beenden der Protokollerfassung

1. Melden Sie sich bei NetWitness Platform 11.0.x an und wechseln Sie zu **ADMIN > Services**. Die Ansicht „Services“ wird angezeigt.




- Wählen Sie die einzelnen **Log Decoder**-Services aus.

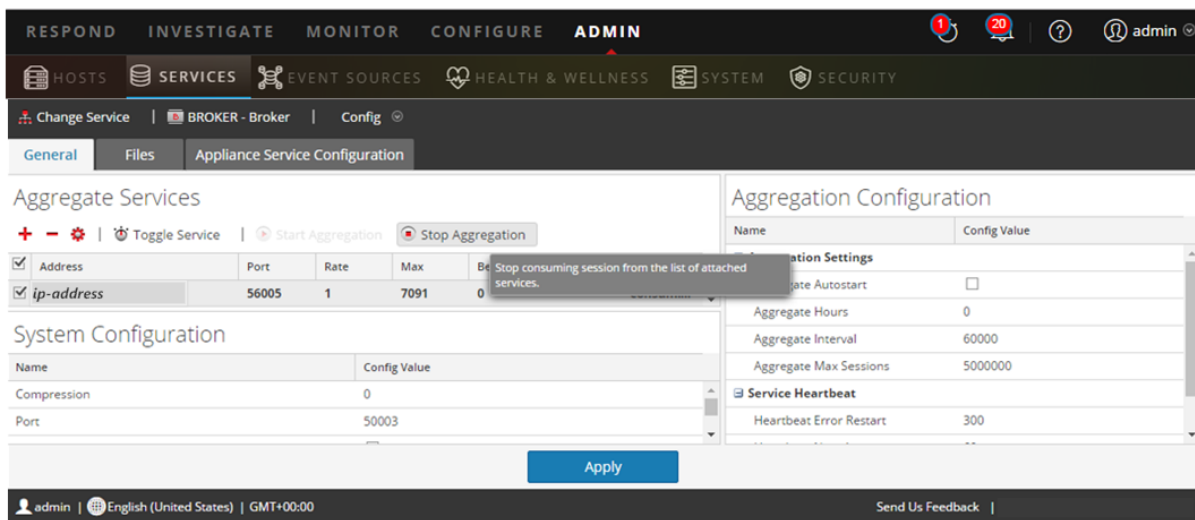


- Wählen Sie unter  (Aktionen) die Optionen **Ansicht > System** aus.

- Klicken Sie in der Symbolleiste auf  **Stop Capture**.

### Aggregation beenden

- Melden Sie sich bei NetWitness Platform 11.0.x an und wechseln Sie zu **ADMIN > Services**.
- Wählen Sie den **Broker**-Service aus.
- Wählen Sie unter  (Aktionen) die Optionen **Ansicht > Konfiguration** aus.
- Die Registerkarte **Allgemein** wird angezeigt.



- Klicken Sie unter **Aggregierte Services** auf  **Stop Aggregation**.

## Azure Hosts

### Aufgabe 4: (Bedingungsabhängig) Anforderungen der Vorbereitung für die Azure Host-Aktualisierung

Überprüfen Sie Ihre Azure-Hostbereitstellung für die folgenden drei Bedingungen und führen Sie ggf. die Aufgaben unter diesen Bedingungen durch.

- Wenn sich auf dem Host ein 11.0.0.0 Azure-Basis-Image befindet (auch wenn Sie den Host auf 11.1.0.x aktualisiert haben), erstellen Sie ein CentOS-Base-Repo.

**Achtung:** Führen Sie die folgenden Schritte nicht aus, wenn kein `libgudev1-219-30.e17_3.9.x86_64-RPM` vorhanden ist.

1. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
  2. Führen Sie den folgenden Befehl aus NW-Serverhost-root -Verzeichnis aus.  

```
yum remove libgudev1-219-30.e17_3.9.x86_64
```
  3. Erstellen Sie ein Centos-Base-Repo, wie in Schritt 6 des **CentOS 7.0+**-Verfahrens (<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/create-upload-centos#centos-70>), beschrieben.
  4. Führen Sie die folgenden Befehlszeichenfolgen aus dem NW-Server-Host-root -Verzeichnis aus.  

```
yum clean all
yum install WALinuxAgent
sudo systemctl enable waagent
```
  5. Löschen Sie das CentOS-Basis-Repo.
- Füllen Sie beim Update-Pfad von 11.0.0.x auf 11.2 das Repository mit zusätzlichen Paketen. Wenden Sie sich an den Kundensupport (<https://community.rsa.com/docs/DOC-1294>) für die `nw-azure-11.1-extras.zip`-Datei).
    1. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
    2. Navigieren Sie zum `root` -Verzeichnis des NW Server-Hosts.
    3. Führen Sie die folgenden Befehlszeichenfolgen aus, um die Azure-Zip-Datei zu extrahieren.  

```
mkdir -p /var/lib/netwitness/common/repo/11.2.0.0/OS/other+
unzip nw-azure-11.1-extras.zip -d
/var/lib/netwitness/common/repo/11.2.0.0/OS/other
```
    4. Verwenden Sie ein externes Repository.
  - Wenn Sie ein externes Repository verwenden, um Aktualisierungen anzuwenden, aktualisieren Sie es mit den zusätzlichen Paketen.
    1. Nachdem Sie die den 11.2.0.0-Inhalt für das externe Repository eingerichtet haben, navigieren Sie zum Verzeichnis `<base-directory>11.2.0.0/OS/other` des externen Repositories.

2. Führen Sie die folgende Befehlszeichenfolge aus, um die Azure-Zip-Datei aus dem externen Repository-Verzeichnis 11.2.0.0/OS zu extrahieren.  
`unzip nw-azure-11.1-extras.zip -d /<base-directory/11.2.0.0/OS/other`
3. Führen Sie den folgenden Befehl aus dem 11.2.0.0/OS-Verzeichnis des externen Repositories aus:  
`createrepo`

## Endpoint Insights

### Aufgabe 5: (Bedingungsabhängig) Sichern vorhandener benutzerdefinierter Metadatenzuordnungen vor dem Anwenden der Aktualisierung 11.2 auf einen Endpoint-Host

In 11.2 hat RSA die Endpoint-Metadatenzuordnungen erweitert, um sie an die aktuellen Änderungen des Unified Data Modells (UDM) anzupassen. Wenn Sie das die Aktualisierung 11.2 Ihres Endpoint Insights-Hosts anwenden, wird die bestehende benutzerdefinierte Zuordnung gelöscht, um zu vermeiden, dass die neu hinzugefügten Standard-Metadatenzuordnungen überschrieben werden. Wenn Sie die vorhandenen benutzerdefinierten Metadatenzuordnungen verwenden möchten, empfiehlt RSA, die vorhandenen benutzerdefinierten Zuordnungen zu sichern, bevor Sie den Endpoint Insights-Host auf 11.2 aktualisieren. So führen Sie das Backup durch:

1. Führen Sie die `get-custom-API` über `nw-shell` aus. Die Liste der benutzerdefinierten Zuordnungen wird angezeigt.
2. Kopieren Sie die benutzerdefinierten Zuordnungen manuell in ein sicheres Verzeichnis.

Weitere Informationen finden Sie im *Endpoint Insights-Konfigurationsleitfaden*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

## Reporting Engine

### Aufgabe 6: Konfigurieren der Reporting Engine für vorkonfigurierte Diagramme

Für nach der Aktualisierung auszuführende vorkonfigurierte Diagramme müssen Sie die Standarddatenquelle auf der Reporting Engine-Konfigurationsseite konfigurieren, bevor Sie die Aktualisierung durchführen. Wenn Sie diese Aufgabe nicht ausführen, müssen Sie manuell nach der Aktualisierung die Datenquelle einrichten. Weitere Informationen zu Reporting Engine-Datenquellen finden Sie im *NetWitness Platform 11.2 Reporting Engine-Konfigurationsleitfaden*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können..

## Respond

### Aufgabe 7: (Bedingungsabhängig) Wiederherstellen der benutzerdefinierten Schlüssel für den Respond-Service

Wenn Sie in `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` benutzerdefinierte Schlüssel zur Verwendung in der GroupBy-Klausel in 11.0 hinzugefügt haben, kopieren und speichern Sie die benutzerdefinierten Schlüssel in einer Datei.

### Aufgabe 8: Sichern der angepassten Skripte zur Normalisierung des Respond-Service

Die von RSA umstrukturierten Skripte zur Normalisierung des Respond-Service sind in 11.2.0.0 im `/var/lib/netwitness/respond-server/scripts`-Verzeichnis gespeichert. Sie müssen diese in 11.0.x sichern, bevor Sie auf 11.2.0.0 aktualisieren, damit Sie sie in 11.2.0.0, wie in den Aufgaben nach der Aktualisierung für [Respond](#) beschrieben, wiederherstellen können.

1. Navigieren Sie zum Verzeichnis `/var/lib/netwitness/respond-server/scripts`.
2. Sichern Sie die folgenden Dateien:  
data\_privacy\_map.js  
normalize\_alerts.js  
normalize\_core\_alerts.js  
normalize\_ecat\_alerts.js  
normalize\_ma\_alerts.js  
normalize\_wtd\_alerts.js  
utils.js
3. (Bedingungsabhängig) Wenn Sie in 11.0.x oder einer vorherigen Version benutzerdefinierte Logik hinzugefügt haben, kopieren und speichern Sie diese Logik aus den gesicherten Skripten, damit Sie sie in 11.2.0.0 wiederherstellen können.

## Aufgaben bei der Aktualisierung

---

Führen Sie die folgenden Aufgaben durch, um NetWitness Platform 11.0.x.x oder 11.1.x.x auf 11.2.0.0 zu aktualisieren.

Es gibt zwei Methoden, um Versionsaktualisierungen auf einen Host anzuwenden.

**Hinweis:** Wenn Sie vorhaben, ein Update-Repository (Repo) für NetWitness Platform 11.2.0.0 zu verwenden, das sich von dem Repository unterscheidet, das Sie jetzt für 11.0.x.x oder 11.1.x.x eingerichtet haben, finden Sie unter [Anhang C: Einrichten eines externen Repository](#) entsprechende Anweisungen.

- [Anwenden von Aktualisierungen über die Ansicht „Hosts“ \(Webzugriff\)](#)
- [Anwenden von Aktualisierungen über die Befehlszeile \(Kein Webzugriff\)](#)

### Anwenden von Aktualisierungen über die Ansicht „Hosts“ (Webzugriff)

Es gibt zwei Aufgaben, die Sie zum Anwenden von Aktualisierungen über die Ansicht „Hosts“ ausführen müssen:

- Aufgabe 1. Füllen Sie das lokale Repository auf oder richten Sie ein externes Repository ein. Stellen Sie sicher, dass Sie die neuesten Versionsaktualisierungen verwenden.
- Aufgabe 2. Wenden Sie auf jeden Host über die Ansicht „Hosts“ Aktualisierungen an.

#### Aufgabe 1. Auffüllen des lokalen Repository oder Einrichten eines externen Repository

Wenn Sie Ihren NW-Server in 11.2.0.0 einrichten, wählen Sie das lokale Repository oder ein externes Repository aus. Die Ansicht „Hosts“ ruft Versionsaktualisierungen aus dem ausgewählten Repository ab.

Wenn Sie das lokale Repository ausgewählt haben, müssen Sie dieses nicht einrichten, aber Sie müssen sicherstellen, dass es die neuesten Aktualisierungen enthält. Anweisungen zum Auffüllen des Repository mit Versionsaktualisierungen finden Sie unter [Anhang B: Auffüllen des lokalen Repository](#).

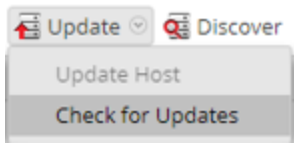
Wenn Sie ein externes Repository ausgewählt haben, müssen Sie es einrichten. Anweisungen zum Einrichten eines externen Repository finden Sie unter [Anhang C: Einrichten eines externen Repository](#).

## Aufgabe 2. Anwenden von Aktualisierungen über die Ansicht „Hosts“ auf einzelne Hosts

In der Ansicht „Hosts“ werden die in Ihrem lokalen Update-Repository verfügbaren Softwareversionsaktualisierungen angezeigt und Sie wählen die gewünschten Aktualisierungen über die Ansicht „Hosts“ aus und wenden diese an.

In diesem Verfahren erfahren Sie, wie Sie einen Host auf eine neue Version von NetWitness Platform aktualisieren.

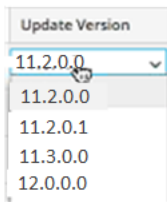
1. Melden Sie sich bei NetWitness Platform an.
2. Navigieren Sie zu **ADMIN > Hosts**.
3. (Bedingungsabhängig) Überprüfen Sie die neuesten Aktualisierungen.




4. Wählen Sie einen Host oder Hosts aus.  
Sie müssen zunächst die NW-Server auf die neueste Version aktualisieren. Sie können die anderen Hosts in beliebiger Reihenfolge aktualisieren, aber RSA empfiehlt, dass Sie die Richtlinien unter „Ausführen im gemischten Modus“ im *RSA NetWitness Platform – Leitfaden für die ersten Schritte mit Hosts und Services* befolgen.

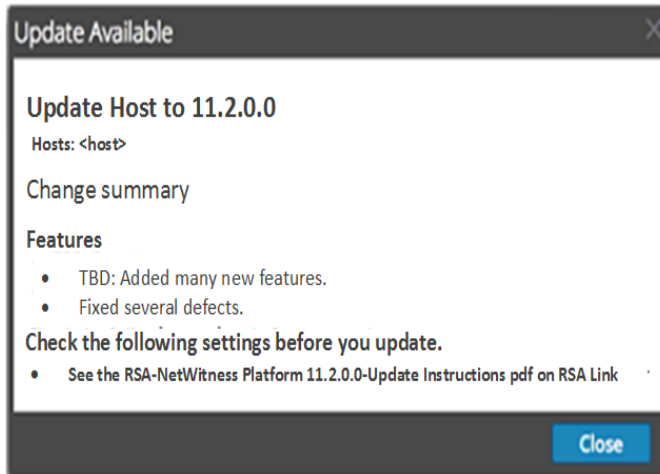
**Aktualisierung verfügbar** wird in der Spalte **Status** angezeigt, wenn für die ausgewählten Hosts im lokalen Update-Repository eine Versionsaktualisierung vorhanden ist.

5. Wählen Sie die Version, die Sie anwenden möchten, aus der Spalte **Update-Version** aus.



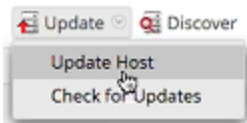
Gehen Sie in folgenden Fällen wie folgt vor:

- Wenn Sie mehr als einen Host auf diese Version aktualisieren möchten, dann aktivieren Sie nach der Aktualisierung des NW-Serverhosts das Kontrollkästchen links neben den Hosts. Es sind nur Versionen von Aktualisierungen aufgelistet, die derzeit unterstützt werden.
- Wenn Sie ein Dialogfeld mit den wichtigsten Funktionen der Aktualisierung sowie Informationen über die Aktualisierungen anzeigen möchten, klicken Sie auf das Informationssymbol (  ) rechts neben der Versionsnummer der Aktualisierung. Nachfolgend finden Sie ein Beispiel für das Dialogfeld.

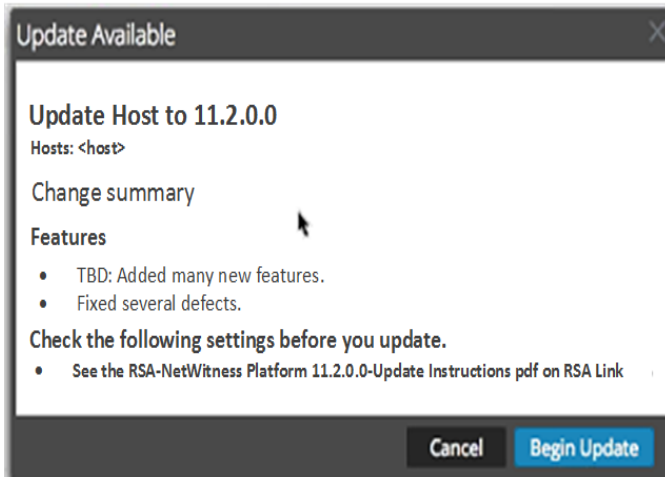


- Wenn Sie die gewünschte Version nicht finden können, wählen Sie **Aktualisieren > Nach Updates suchen** aus, um das Repository auf alle verfügbaren Aktualisierungen zu prüfen. Wenn eine Aktualisierung verfügbar ist, wird die Meldung „Es sind neue Hostaktualisierungen verfügbar“ angezeigt und die Spalte **Status** wird automatisch aktualisiert und zeigt **Aktualisierung verfügbar** an. Standardmäßig werden nur die unterstützten Aktualisierungen für den ausgewählten Host angezeigt.

6. Klicken Sie in der Symbolleiste auf **Aktualisieren > Host aktualisieren**.



Ein Dialogfeld wird mit Informationen über die ausgewählte Aktualisierung angezeigt. Klicken Sie auf **Update beginnen**.



Die Spalte **Status** informiert Sie darüber, was in jeder der folgenden Phasen der Aktualisierung geschieht:

- Phase 1: **Aktualisierungspakete werden heruntergeladen** – lädt die Repository-Artefakte auf den NW-Server für die Services auf dem ausgewählten Host herunter.
  - Phase 2: **Aktualisierungspakete werden konfiguriert** – konfiguriert die Aktualisierungsdateien im richtigen Format.
  - Phase 3: **Aktualisierung wird durchgeführt** – aktualisiert den Host auf die neue Version.
7. Wenn **Aktualisierung wird durchgeführt** angezeigt wird, aktualisieren Sie das Browserfenster. Eventuell wird dadurch der Anmeldebildschirm von NetWitness angezeigt. Melden Sie sich in diesem Fall an und navigieren Sie erneut zur Ansicht „Host“.
- Nachdem der Host aktualisiert wurde, zeigt NetWitness Platform die Aufforderung **Host neu starten an**.
8. (Bedingungsabhängig – Nur für Host mit Unity-Speicher) Wenn der Unity-Speicher des Hosts (z. B. der Network Decoder-Host) mit PowerPath unter 11.1.x.x konfiguriert wurde) und EMCPower.LINUX.6.3.0.b049 als Powerpath-Version installiert ist, stellen Sie über SSH eine Verbindung mit dem Host her und senden Sie die folgenden Befehle zum Installieren der neuen PowerPath-Version (d. h. DellEMCPower.LINUX.6.4.0.b095).
- ```
systemctl stop nwdecoder
umount -R /var/netwitness/decoder
yum update DellEMCPower.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm
```
9. Klicken Sie in der Symbolleiste auf **Host neu starten**.
- NetWitness Platform zeigt den Status als **Neustart an**, bis der Host wieder online ist. Nachdem der



Host wieder online ist, wird unter **Status** der Status **Auf dem neuesten Stand** angezeigt. Wenden Sie sich an die Kundenbetreuung, wenn der Host nicht wieder online geschaltet wird.

**Hinweis:** 1.) Wenn DISA STIG aktiviert ist, kann das Öffnen der Core-Services ca. 5 bis 10 Minuten dauern. Grund für diese Verzögerung ist das Erstellen neuer Zertifikate. 2.) Wenn Sie über einen Unity-Speicher verfügen, überprüfen Sie den PowerPath-Status und ob das Unity-Gerät erkannt wird.

## Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff)

Wenn Ihre Bereitstellung von RSA NetWitness Platform keinen Webzugriff hat, führen Sie das folgende Verfahren aus, um eine Versionsaktualisierung anzuwenden.

1. Laden Sie das Aktualisierungspaket `.zip` für die gewünschte Version (z. B. `netwitness-11.2.0.0.zip`) von RSA Link in ein lokales Verzeichnis herunter.
2. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
3. Erstellen Sie ein Bereitstellungsverzeichnis `/tmp/upgrade/<version>` für die gewünschte Version (z. B. `/tmp/upgrade/11.2.0.0`).  
`mkdir -p /tmp/upgrade/11.2.0.0`
4. Kopieren Sie das `.zip`-Updatepaket in ein anderes Verzeichnis als das Staging-Verzeichnis auf dem NW-Server (z. B. das `/tmp`-Verzeichnis).
5. Entpacken Sie das Paket in das Staging-Verzeichnis, das Sie erstellt haben (z. B. `/tmp/upgrade/11.2.0.0`).  
`unzip /<download-location>/netwitness-11.2.0.0.zip -d /tmp/upgrade/11.2.0.0`
6. Initialisieren Sie die Aktualisierung auf dem NW-Server.  
`upgrade-cli-client --init --version 11.2.0.0 --stage-dir /tmp/upgrade/`
7. Wenden Sie die Aktualisierung auf den NW-Server an.  
`upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.2.0.0`
8. Melden Sie sich bei NetWitness Platform an und starten Sie den NW-Serverhost in der Ansicht „Host“.
9. Wenden Sie die Aktualisierung auf jeden Nicht-NW-Serverhost an.  
`upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> --version 11.2.0.0`  
 Die Aktualisierung ist abgeschlossen, wenn der Abruf abgeschlossen ist.
10. (Bedingungsabhängig) Wenn der Unity-Speicher des Hosts (z. B. der Network Decoder-Host) mit PowerPath unter 11.1.xx konfiguriert wurde) und EMCPower.LINUX.6.3.0.b049 als Powerpath-Version installiert ist, stellen Sie über SSH eine Verbindung mit dem Host her und senden Sie die folgenden Befehle zum Installieren der neuen PowerPath-Version (d. h. DelleMCPower.LINUX.6.4.0.b095).  
`systemctl stop nwdecoder`  
`umount -R /var/netwitness/decoder`  
`yum update DelleMCPower.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm`
11. Melden Sie sich bei NetWitness Platform an und starten Sie den Host in der Ansicht „Host“. Sie können mit dem folgenden Befehl überprüfen, welche Version auf den Host angewendet wurde:  
`upgrade-cli-client --list`

**Hinweis:** 1.) Wenn DISA STIG aktiviert ist, kann das Öffnen der Core-Services ca. 5 bis 10 Minuten dauern. Grund für diese Verzögerung ist das Erstellen neuer Zertifikate. 2.) Wenn Sie über einen Unity-Speicher verfügen, überprüfen Sie den PowerPath-Status und ob das Unity-Gerät erkannt wird.



## Aktualisieren oder Installieren der Legacy-Windows-Sammlung

---

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

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

## Aufgaben nach der Aktualisierung

---

Führen Sie die folgenden Aufgaben durch, nachdem Sie das Upgrade auf NetWitness Platform 11.2.0.0 durchgeführt haben.

- [Allgemeines](#)
- [NW-Server](#)
- [Endpoint Insights](#)
- [Event Stream Analysis](#)
- [Respond](#)
- [NetWitness UEBA](#)



## Allgemeines

Diese Aufgaben gelten für alle Kunden von NetWitness Platform 11.2.0.0.

### Aufgabe 1: Starten der Datenerfassung und -aggregation

Starten Sie Netzwerk- und Protokollerfassung sowie Paket- und Protokollaggregation nach dem Upgrade auf 11.2.0.0 neu.


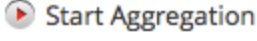
#### Starten der Netzwerkerfassung

1. Wählen Sie im Menü **NetWitness Platform** die Optionen **ADMIN > Services** aus.  
Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie die einzelnen **Decoder**-Services aus.
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht > System** aus.
4. Klicken Sie in der Symbolleiste auf .

#### Starten der Protokollerfassung


1. Wählen Sie im Menü **NetWitness Platform** die Optionen **ADMIN > Services** aus.  
Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie die einzelnen **Log Decoder**-Services aus.
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht > System** aus.
4. Klicken Sie in der Symbolleiste auf .

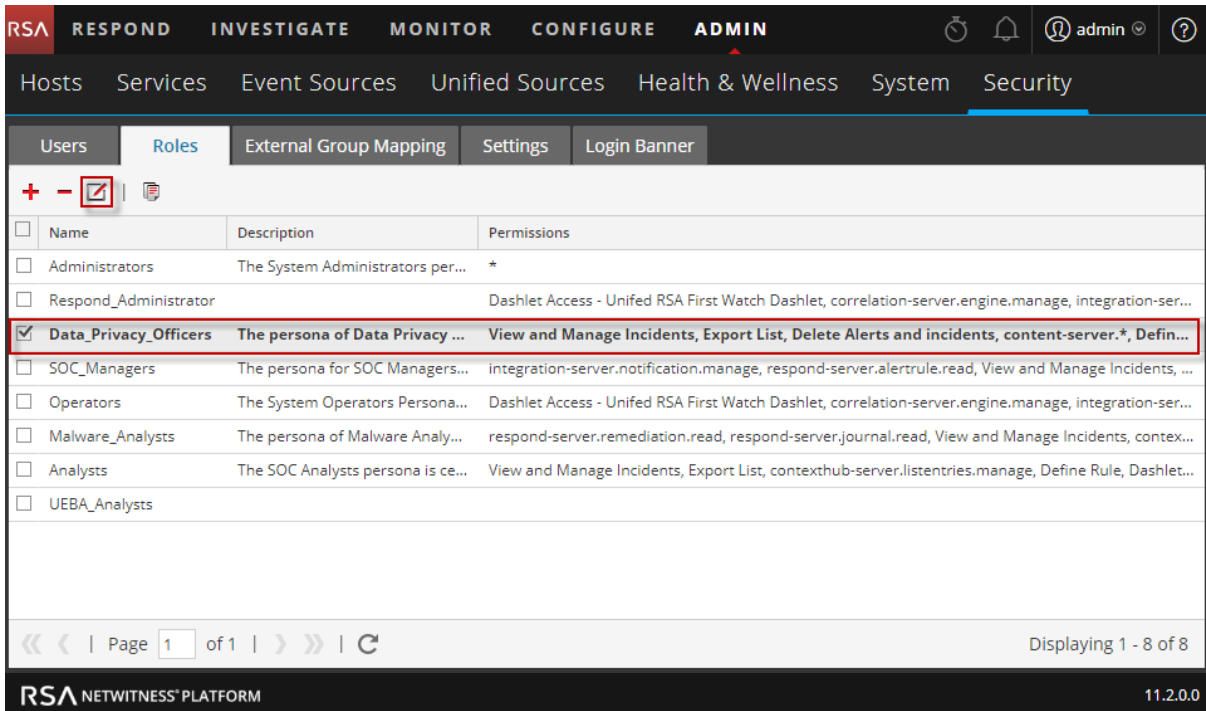
#### Aggregation starten

1. Wählen Sie im Menü **NetWitness Platform** die Optionen **ADMIN > Services** aus.  
Die Ansicht „Services“ wird angezeigt.
2. Für jeden Concentrator- und Broker-Service.
  - a. Wählen Sie den Service aus.
  - b. Wählen Sie unter  (Aktionen) die Optionen **Ansicht > Konfiguration** aus.
  - c. Klicken Sie in der Symbolleiste auf .

## Aufgabe 2: Einrichten von Benutzerberechtigungen für Kontextmenüaktionen

Führen Sie die folgenden Schritte für die Rollen **Analysten**, **SOC-Manager**, **Datenschutzbeauftragte** aus, um deren Kontextmenüaktionen einzurichten. Sie müssen diese Schritte für die Rollen **Analysten**, **SOC-Manager** und **Datenschutzbeauftragte** ausführen.

1. Wählen Sie im Menü **NetWitness Platform** die Optionen **ADMIN > Sicherheit > Rollen**.
2. Doppelklicken Sie auf die Benutzerrolle (z. B. **Datenschutzbeauftragte**), oder klicken Sie auf den Nutzer und dann auf  (Bearbeiten).



The screenshot shows the RSA NetWitness Platform Admin console. The top navigation bar includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' menu is expanded to show 'Hosts', 'Services', 'Event Sources', 'Unified Sources', 'Health & Wellness', 'System', and 'Security'. The 'Security' menu is further expanded to show 'Users', 'Roles', 'External Group Mapping', 'Settings', and 'Login Banner'. The 'Roles' tab is active, displaying a table of roles. The 'Data\_Privacy\_Officers' role is selected and highlighted with a red box. The table has columns for 'Name', 'Description', and 'Permissions'.

| Name                                                      | Description                       | Permissions                                                                                           |
|-----------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Administrators                   | The System Administrators per...  | *                                                                                                     |
| <input type="checkbox"/> Respond_Administrator            |                                   | Dashlet Access - Unifed RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input checked="" type="checkbox"/> Data_Privacy_Officers | The persona of Data Privacy ...   | View and Manage Incidents, Export List, Delete Alerts and incidents, content-server.*, Defini...      |
| <input type="checkbox"/> SOC_Managers                     | The persona for SOC Managers...   | integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, ... |
| <input type="checkbox"/> Operators                        | The System Operators Persona...   | Dashlet Access - Unifed RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input type="checkbox"/> Malware_Analysts                 | The persona of Malware Analy...   | respond-server.remediation.read, respond-server.journal.read, View and Manage Incidents, contex...    |
| <input type="checkbox"/> Analysts                         | The SOC Analysts persona is ce... | View and Manage Incidents, Export List, contexthub-server.listentries.manage, Define Rule, Dashlet... |
| <input type="checkbox"/> UEBA_Analysts                    |                                   |                                                                                                       |

At the bottom of the page, there is a pagination control showing 'Page 1 of 1' and 'Displaying 1 - 8 of 8'. The footer includes the RSA logo and 'NETWITNESS PLATFORM' on the left, and the version number '11.2.0.0' on the right.

3. Aktivieren Sie in der Ansicht **Rolle bearbeiten** unter **Berechtigungen** die Kontrollkästchen **Protokolle managen**, **Plug-ins managen** und **Systemeinstellungen managen** und klicken Sie auf **Speichern**.

The screenshot shows the 'Edit Role' window with the following details:

- Attributes:**
  - Core Query Timeout: 5
  - Core Session Threshold: 100000
  - Core Query Prefix: (empty)
- Permissions:**
  - Navigation: Admin-server, **Administration** (highlighted), Alerting, Config-server, Content-serv
  - Table with columns: Assigned, Description ^

| Assigned                            | Description ^          |
|-------------------------------------|------------------------|
| <input checked="" type="checkbox"/> | Manage Logs            |
| <input type="checkbox"/>            | Manage Notifications   |
| <input checked="" type="checkbox"/> | Manage Plugins         |
| <input type="checkbox"/>            | Manage Predicates      |
| <input type="checkbox"/>            | Manage Reconstruction  |
| <input checked="" type="checkbox"/> | Manage Security        |
| <input checked="" type="checkbox"/> | Manage Services        |
| <input checked="" type="checkbox"/> | Manage System Settings |
| <input type="checkbox"/>            | Modify ESA Settings    |
| <input type="checkbox"/>            | Modify Event Sources   |
| <input type="checkbox"/>            | Modify Hosts           |

4. Führen Sie die Schritte 1 bis 3 für die Rollen **Analysten**, **SOC-Manager** und **Datenschutzbeauftragte** aus.




## NW-Server

### **Aufgabe 3: (Bedingungsabhängig) Korrigieren der Auditprotokollvorlagen, die in der Logstash-Ausgabe-Konfigurationsdatei nicht aktualisiert werden**

**Problem:** Wenn ein Nutzer von 11.0.0.0 auf 11.2.0.0 aktualisiert, werden Auditprotokollvorlagen in der Logstash-Ausgabe-Konfigurationsdatei nicht aktualisiert, wenn globales Auditing eingerichtet ist.

**Workaround:** Wenn globales Auditing konfiguriert ist, müssen Sie einen der Syslog-Einträge auf den Servern für globale Benachrichtigungen bearbeiten und auf „Speichern“ klicken, um die aktuelle Auditprotokollkonfiguration anzuwenden.

Wenn Sie globales Auditing in 11.0.x konfiguriert hatten, müssen Sie das folgende Verfahren durchführen, um die aktuelle globale Auditingkonfiguration anzuwenden.

1. Wählen Sie im Menü **NetWitness Platform ADMIN > System > Globale Benachrichtigungen** aus.  
Die Ansicht **Globale Benachrichtigungen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Server** und wählen Sie einen Syslog-Server aus.
3. Klicken Sie auf  (Symbol „Bearbeiten“) und dann auf **Speichern**.

### **(Bedingungsabhängig) Aufgabe 4: Neukonfigurieren der PAM-Radius-Authentifizierung**

Wenn Sie PAM-Radius-Authentifizierung in 11.0.x.x unter Verwendung des `pam_radius`-Pakets konfiguriert haben, müssen Sie sie in 11.2.0.0 unter Verwendung des `pam_radius_auth` package neu konfigurieren, um eine bessere Leistung zu erzielen. Anweisungen hierzu finden Sie unter „Konfigurieren der PAM-Anmeldefunktion“ im *RSA NetWitness® Platform 11.2 – Handbuch Systemsicherheit und Benutzerverwaltung*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

## Endpoint Insights

### **Aufgabe 5: Neukonfigurieren eines wiederkehrenden Feeds, der über Legacy Endpoint konfiguriert wurde, da sich die Java-Version geändert hat**

Sie müssen den wiederkehrenden Legacy Endpoint-Feed aufgrund der Änderung der Java-Version neu konfigurieren. Führen Sie den folgenden Schritt zur Behebung des Problems aus.

1. Importieren Sie das NetWitness Endpoint CA-Zertifikat in den vertrauenswürdigen NetWitness Platform-Speicher, wie in „Exportieren des SSL-Zertifikats von NetWitness Endpoint“ unter dem Thema „Konfigurieren kontextbezogener Daten von Endpoint über wiederkehrenden Feed“ im *RSA NetWitness Endpoint-Integrationsleitfaden* beschrieben.  
Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

### **Aufgabe 6: Wiederherstellen gesicherter benutzerdefinierter Endpoint-Metadatenzuordnungen**

RSA empfiehlt, 11.2 Standardzuordnungen nicht zu überschreiben, es sei denn, es ist erforderlich. Wenn Sie benutzerdefinierte Zuordnungen von 11.1.x.x vor dem Aktualisieren auf 11.2 gesichert haben, überprüfen Sie die Liste der benutzerdefinierten Zuordnungen und stellen Sie nur diejenigen wieder her, die nicht bereits auf die Standardeinstellung festgelegt sind, indem Sie `set-custom API` über die `nw-Shell` verwenden.

Weitere Informationen zum Ändern von Zuordnungen finden Sie unter *Endpoint Insights – Konfigurationsleitfaden*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

## Event Stream Analysis

Diese Aufgaben gelten für Kunden von NetWitness Platform 11.2.0.0, die Event Stream Analysis verwenden.

### **(Bedingungsabhängig) Aufgabe 7: Neukonfigurieren der Aggregationsregel „Verdacht auf Command-and-Control-Kommunikation von Domain“ für die automatisierte Bedrohungserkennung**

In 11.0 hat die „Gruppieren nach“-Bedingung „Domain für verdächtige C&C“ der Aggregationsregel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ nicht wie erwartet funktioniert und musste in „Domain“ geändert werden, um Warnmeldungen zu aggregieren und das Erstellen von Incidents für „Verdächtige C&C“ zu ermöglichen. Die Bedingung „Domain für verdächtige C&C“ funktioniert in 11.2.0.0 einwandfrei und sollte als die „Gruppieren nach“-Bedingung für die Aggregationsregel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ (in 11.2.0.0 als Incident-Regel bezeichnet) verwendet werden.

Wenn Sie die „Gruppieren nach“-Bedingung der Aggregationsregel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ für 11.0 in „Domain“ geändert haben, müssen Sie sie für 11.2.0.0 wieder in „Domain für verdächtige C&C“ ändern.

1. Wählen Sie im Menü **NetWitness Platform Konfigurieren > Incident-Regeln** aus.
2. Suchen Sie in der Liste „Incident-Regeln“ nach der Regel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ und klicken Sie auf den Link im Feld NAME, um ihn zu öffnen.
3. Legen Sie in der Ansicht mit den Details der Incident-Regel im Abschnitt „Gruppierungsoptionen“ das Feld „Gruppieren nach“ auf „Domain für verdächtige C&C“ fest und klicken Sie auf „Speichern“.

Weitere Informationen finden Sie im „Handbuch NetWitness Platform – Automatisierte Bedrohungserkennung“ und im Abschnitt

„Konfigurieren von ESA Analytics“ im NetWitness Platform ESA-Konfigurationsleitfaden. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

## Respond

### Aufgabe 8: Abrufen der aktuellen Version des Schemas für Aggregationsregeln und Wiederherstellen aller benutzerdefinierten Schlüssel des Respond-Service

Führen Sie das folgende Verfahren durch, um die aktuelle Version des Schemas für Aggregationsregeln abzurufen und alle benutzerdefinierten Schlüssel des Respond-Service wiederherzustellen.

1. Löschen Sie die `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`-Datei.
2. Starten Sie den Respond-Server neu, um die aktuelle Version der `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` -Datei abzurufen.  

```
systemctl restart rsa-nw-respond-server
```
3. Wenn Sie in der `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`-Datei benutzerdefinierte Schlüssel zur Verwendung in der GroupBy-Klausel in 11.0 hinzugefügt haben, ändern Sie die `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`-Datei und fügen Sie die benutzerdefinierten Schlüssel hinzu, die Sie zuvor als eine Aufgabe zur Vorbereitung der Aktualisierung gespeichert haben.

**Hinweis:** In 11.2.0.0 wurden neue „Gruppieren nach“-Felder zu Respond hinzugefügt. Die neuen „Gruppieren nach“-Felder sind in der NetWitness Platform-Benutzeroberfläche nicht sichtbar, wenn Sie nicht die aktuelle Version der Datei vom Server abrufen.

## Aufgabe 9: Abrufen der aktuellen Version der Skripte zur Normalisierung des Respond-Service und Wiederherstellung aller benutzerdefinierten Skripte zur Normalisierung des Respond-Service

RSA hat in 11.2.0.0/`/var/lib/netwitness/respond-server/scripts` die Skripte zur Normalisierung des Respond-Service im -Verzeichnis umstrukturiert. Sie müssen die alten Versionen ersetzen.

Vor dem Upgrade auf 11.2.0.0 haben Sie die folgenden Dateien aus dem `/var/lib/netwitness/respond-server/scripts` -Verzeichnis gesichert.

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_wtd_alerts.js
utils.js
```

Führen Sie das folgende Verfahren aus, um die aktuelle Version der Normalisierungsskripte abzurufen.

1. Löschen Sie nach dem Sichern der oben aufgeführten Dateien das `/var/lib/netwitness/respond-server/scripts`-Verzeichnis und seine Inhalte.
2. Starten Sie den Respond-Server neu.  
`systemctl restart rsa-nw-respond-server`
3. (Bedingungsabhängig) Bearbeiten Sie die neuen Dateien so, dass benutzerdefinierte Logik aus den gesicherten 11.0-Skripten eingeschlossen wird.

**Hinweis:** Die folgenden Dateien wurden mit der Version 11.2.0.0 geändert:

```
normalize_alerts.js
aggregation_rule_schema.json
```

## Aufgabe 10: Hinzufügen von Einstellungen für Antwort auf Benachrichtigungen

**Hinweis:** Wenn Sie diese Berechtigungen bereits in 11.1 konfiguriert haben, können Sie diese Aufgabe überspringen.

Berechtigungen für Einstellungen für Antwort auf Benachrichtigung erlauben Respond-Administratoren, Datenschutzbeauftragten und SOC-Managern, auf Einstellungen für Antwort auf Benachrichtigung zuzugreifen (**KONFIGURIEREN > Auf Benachrichtigungen antworten**). So können sie E-Mail-Benachrichtigungen senden, wenn Incidents erstellt oder aktualisiert werden.

Um diese Einstellungen aufzurufen, müssen Sie Ihren vorhandenen integrierten NetWitness Plattform-Benutzerrollen weitere Berechtigungen hinzufügen. Sie müssen auch Ihren benutzerdefinierten Rollen Berechtigungen hinzufügen. Weitere Informationen finden Sie im Thema „Berechtigungen für Einstellungen für Antwort auf Benachrichtigungen“ im *Konfigurationsleitfaden für NetWitness Respond*. Ausführliche Informationen zu Benutzerberechtigungen finden Sie im *Handbuch Systemsicherheit und Benutzerverwaltung*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Plattform Logs & Network 11.x aufgerufen werden können.

## Aufgabe 11: Aktualisieren der „Gruppieren nach“-Werte der Incident-Standardregel

Vier der Incident-Standardregeln verwenden als „Gruppieren nach“-Wert jetzt „Quell-IP-Adresse“:

- Warnmeldungen mit hohem Risiko: Reporting Engine
- Warnmeldungen mit hohem Risiko: Malware Analysis
- Warnmeldungen mit hohem Risiko: NetWitness Endpoint
- Warnmeldungen mit hohem Risiko: ESA

Um die Standardregeln zu aktualisieren, ändern Sie den „Gruppieren nach“-Wert der oben aufgeführten Standardregeln in „Quell-IP-Adresse“:

**Hinweis:** Wenn Sie bereits die „Gruppieren nach“-Werte für die oben aufgeführten Standardregeln in 11.1 aktualisiert haben, müssen Sie diesen Schritt nicht erneut ausführen.

1. Wählen Sie im **NetWitness Platform**-Menü **Konfigurieren** > **Incident-Regeln** aus und klicken Sie in der Spalte **Name** auf die Regel, die Sie aktualisieren möchten. Die Detailansicht der **Incident-Regel** wird angezeigt.
2. Wählen Sie im Feld **Gruppieren nach** den neuen „Gruppieren nach“-Wert aus der Drop-down-Liste aus.
3. Klicken Sie auf **Speichern**, um die Regel zu aktualisieren.

Um NetWitness Endpoint-Alarme auf der Grundlage der Detektor-IP-Adresse zu aggregieren, führen Sie die folgenden Schritte aus, um die Standard-NetWitness-Endpoint-Incident-Regel zu klonen und die als „Gruppieren-nach“-Wert verwendete IP-Adresse zu ändern.

1. Wählen Sie im Menü **NetWitness Platform** die Optionen **Konfigurieren** > **Incident-Regeln** aus. Die Ansicht **Incident-Regelliste** wird angezeigt.
2. Wählen Sie die Standard-Incident-Regel **Warnmeldungen mit hohem Risiko: NetWitness Endpoint** aus und klicken Sie auf **Klonen**. Sie erhalten eine Meldung, dass Sie die ausgewählte Regel erfolgreich geklont wurde.
3. Ändern Sie den Namen der Regel in einen entsprechenden Namen, z. B. „Warnmeldungen mit hohem Risiko: NetWitness Endpunkt Detektor-IP“.
4. Entfernen Sie im Feld **Gruppieren nach Quell-IP-Adresse** und fügen Sie **Detektor-IP-Adresse** hinzu. Es ist wichtig, dass die Detektor-IP-Adresse der einzige aufgeführte „Gruppieren nach“-Wert ist.
5. Klicken Sie auf **Speichern**, um die Regel zu erstellen.

Weitere Informationen finden Sie im *Konfigurationsleitfaden für NetWitness Respond*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

## NetWitness UEBA

### Aufgabe 12: Installieren von NetWitness UEBA

NetWitness UEBA ist eine neue Funktion ab NetWitness® Platform 11.2.

Siehe

*RSA NetWitness Platform 11.2 Installationshandbuch für physische Hosts* für Anweisungen zur Installation auf einem physischen Host.

*RSA NetWitness Platform 11.2 Installationshandbuch für virtuelle Hosts* für Anweisungen zur Installation auf einem virtuellen Host.

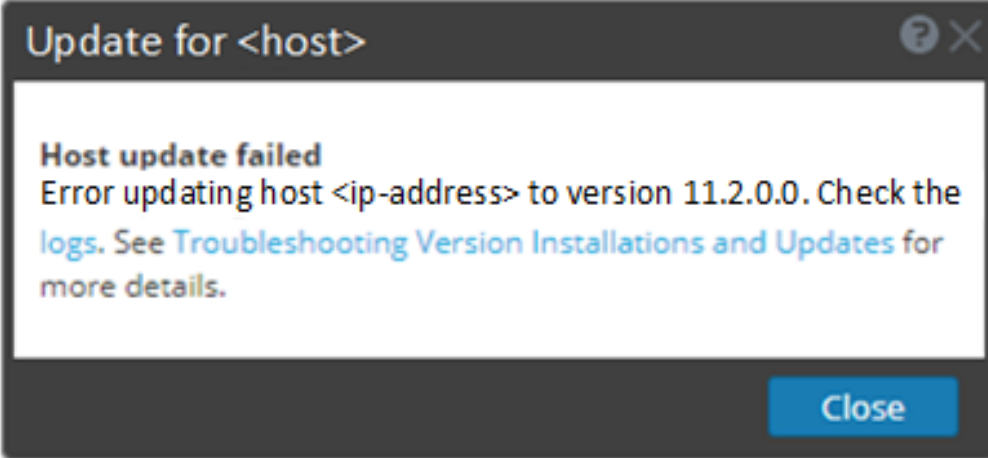
*RSA NetWitness UEBA – Benutzerhandbuch* für Informationen zu UEBA.

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

6. Wählen Sie **Systemeinstellungen managen und Plug-ins managen** aus.

## Anhang A: Troubleshooting von Versionsinstallationen und -aktualisierungen

In diesem Abschnitt werden die Fehlermeldungen beschrieben, die in der Ansicht **Hosts** angezeigt werden, wenn beim Aktualisieren von Hostversionen und der Installation von Services auf Hosts in der Ansicht **Hosts** Probleme auftreten. Wenn Sie Probleme bei der Aktualisierung oder Installation mithilfe der folgenden Troubleshooting-Lösungen nicht beheben können, wenden Sie sich an den Kundensupport (<https://community.rsa.com/docs/DOC-1294>).

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fehlermeldung | <p><b>Hostaktualisierung fehlgeschlagen</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Problem       | <p>Wenn Sie eine Aktualisierungsversion auswählen und auf <b>Aktualisieren &gt;Host aktualisieren</b> klicken, ist zwar der Download erfolgreich, aber die Aktualisierung schlägt fehl.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Lösung        | <ol style="list-style-type: none"> <li>1. Versuchen Sie, die Versionsaktualisierung erneut auf den Host anzuwenden. Häufig ist das alles, was Sie tun müssen.</li> <li>2. Gehen Sie folgendermaßen vor, wenn Sie die neue Aktualisierungsversion weiterhin nicht anwenden können:       <ol style="list-style-type: none"> <li>a. Überwachen Sie während der Verarbeitung die folgenden Protokolle auf dem NW-Server (senden Sie beispielsweise die Befehlszeichenfolge über die Befehlszeile):           <pre data-bbox="509 1541 1382 1780">/var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log /var/log/netwitness/deployment-upgrade/chef-solo.log /var/log/netwitness/config-management/chef-solo.log /var/lib/netwitness/config-management/cache/chef-stacktrace.out</pre>           Der Fehler wird in einem oder mehreren dieser Protokolle angezeigt.         </li> <li>b. Versuchen Sie, das Problem zu lösen, und wenden Sie die</li> </ol> </li> </ol> |



Versionsaktualisierung erneut an.

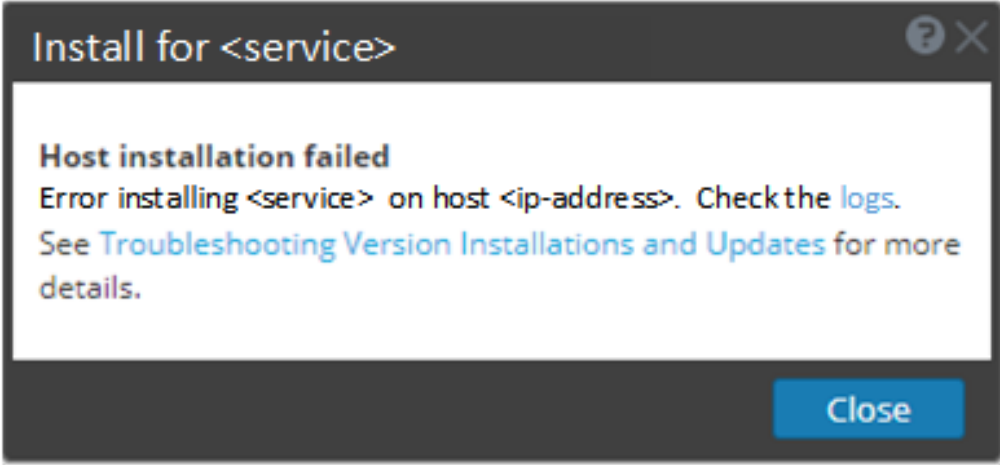
- Ursache 1: Das `deploy_admin`-Passwort ist abgelaufen.  
Lösung: Setzen Sie das `deploy_admin`-Passwort zurück.  
Führen Sie zur Behebung von Ursache 1 die folgenden Schritte aus.
    1. Wählen Sie im NetWitness Suite-Menü **ADMIN > Sicherheit > Registerkarte Benutzer** aus.
    2. Wählen Sie `deploy_admin` aus und klicken Sie auf **Passwort zurücksetzen**.
    3. (Bedingungsabhängig) Wenn NetWitness Suite Ihnen nicht erlaubt, das abgelaufene `deploy_admin`-Passwort im Dialogfeld **Passwort zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus.
      - a. Setzen Sie `deploy_admin` zurück, um ein neues Passwort zu verwenden.
      - b. Führen Sie auf allen Nicht-NW-Serverhosts auf 11.x den folgenden Befehl mit dem übereinstimmenden `deploy_admin`-Passwort vom NW-Serverhost aus.

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```
  - Ursache 2: Das `deploy_admin`-Passwort wurde auf dem NW-Serverhost geändert, nicht aber auf den Nicht-NW-Serverhosts.  
Führen Sie zur Behebung von Ursache 2 die folgenden Schritte aus.
    - Führen Sie auf allen Nicht-NW-Serverhosts auf 11.x den folgenden Befehl mit dem übereinstimmenden `deploy_admin`-Passwort vom NW-Serverhost aus.

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```
3. Wenn Sie die Aktualisierung weiterhin nicht anwenden können, wenden Sie sich mit den Protokollen aus Schritt 2 an den Kundensupport (<https://community.rsa.com/docs/DOC-1294>).

Fehlermeldung

Installation des Host fehlgeschlagen

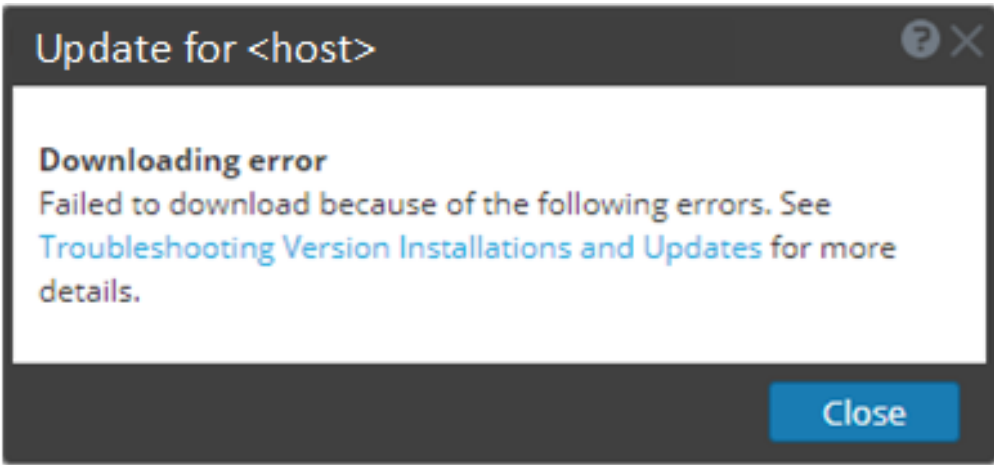
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p><b>Problem</b></p> | <p>Wenn Sie einen Host auswählen und auf <b>Installieren</b> klicken, schlägt der Service für den Installationsprozess fehl.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p><b>Lösung</b></p>  | <ol style="list-style-type: none"> <li>1. Versuchen Sie, den Service erneut zu installieren.<br/>Häufig ist das alles, was Sie tun müssen.</li> <li>2. Gehen Sie folgendermaßen vor, falls Sie den Service immer noch nicht installieren können:       <ol style="list-style-type: none"> <li>a. Überwachen Sie während der Verarbeitung die folgenden Protokolle auf dem NW-Server (senden Sie beispielsweise die Befehlszeichenfolge über die Befehlszeile):           <pre> /var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log /var/log/netwitness/deployment-upgrade/chef-solo.log /var/log/netwitness/config-management/chef-solo.log /var/lib/netwitness/config-management/cache/chef-stacktrace.out </pre>           Der Fehler wird in einem oder mehreren dieser Protokolle angezeigt.         </li> <li>b. Versuchen Sie, das Problem zu lösen, und installieren Sie den Service neu.           <ul style="list-style-type: none"> <li>• Ursache 1: Für nwsetup-tui wurde das falsche <code>deploy_admin</code>-Passwort eingegeben.<br/>Lösung: Rufen Sie Ihr <code>deploy_admin</code> -Passwort ab.<br/>Führen Sie zur Behebung von Ursache 1 die folgenden Schritte aus.               <ol style="list-style-type: none"> <li>1. Wählen Sie im NetWitness Suite-Menü <b>ADMIN &gt; Sicherheit &gt; Registerkarte Benutzer</b> aus.</li> <li>2. Wählen Sie <code>deploy_admin</code> aus und klicken Sie auf <b>Passwort zurücksetzen</b>.</li> <li>3. (Bedingungsabhängig) Wenn NetWitness Suite Ihnen nicht erlaubt, das abgelaufene <code>deploy_admin</code>-Passwort im Dialogfeld <b>Passwort</b></li> </ol> </li> </ul> </li> </ol> </li> </ol> |

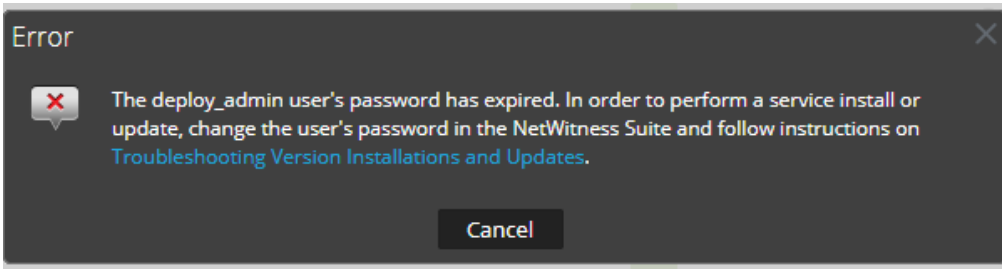
**zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus.

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


```
security-cli-client --get-config-prop --prop-hierarchy
nw.security-client --prop-name
platform.deployment.password -quiet
```
  - b. Stellen Sie über SSH eine Verbindung mit dem Host her, auf dem die Installation/Orchestrierung fehlgeschlagen ist.
  - c. Führen Sie den Befehl `nwsetup-tui` erneut mit dem korrekten `deploy_admin`-Passwort aus.
- Ursache 2: Das `deploy_admin`-Passwort ist abgelaufen. Führen Sie zur Behebung von Ursache 2 die folgenden Schritte aus.
    1. Wählen Sie im NetWitness Suite-Menü **ADMIN > Sicherheit > Registerkarte Benutzer** aus.
    2. Wählen Sie `deploy_admin` aus und klicken Sie auf **Passwort zurücksetzen**.
    3. (Bedingungsabhängig) Wenn NetWitness Suite Ihnen erlaubt, das abgelaufene `deploy_admin`-Passwort im Dialogfeld **Passwort zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus.
      - a. Geben Sie das abgelaufene `deploy_admin`-Passwort ein.
      - b. Deaktivieren Sie das Kontrollkästchen „Passwortänderung bei nächster Anmeldung erzwingen“.
      - c. Klicken Sie auf **Speichern**.
    4. (Bedingungsabhängig) Wenn NetWitness Suite Ihnen nicht erlaubt, das abgelaufene `deploy_admin`-Passwort im Dialogfeld „Passwort zurücksetzen“ einzugeben, führen Sie die folgenden Schritte aus.
      - a. Setzen Sie `deploy_admin` zurück, um ein neues Passwort zu verwenden.
      - b. Führen Sie auf allen NW-Server-Hosts und allen anderen Hosts auf 11.x den folgenden Befehl mit dem neuen `deploy_admin`-Passwort aus.
 

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```
      - c. Führen Sie auf dem Host mit dem Installations-/Orchestrierungsfehler den Befehl `nwsetup-tui` aus und verwenden Sie das neue `deploy_admin`-Passwort.
3. Wenn Sie die Aktualisierung weiterhin nicht anwenden können, wenden Sie sich mit den Protokollen aus Schritt 2 an den Kundensupport (<https://community.rsa.com/docs/DOC-1294>).

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fehlermeldung | <p><b>Downloadfehler</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Problem       | <p>Wenn Sie eine Aktualisierungsversion auswählen und auf <b>Aktualisieren &gt; Host aktualisieren</b> klicken, wird der Download zwar gestartet, kann aber nicht abgeschlossen werden.</p>                                                                                                                                                                                                                                                                                                                                                                                                            |
| Ursache       | <p>Die Downloaddateien der Version können groß sein und das Herunterladen kann daher lange dauern. Wenn beim Download Kommunikationsprobleme auftreten, schlägt er fehl.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Lösung        | <ol style="list-style-type: none"> <li>1. Versuchen Sie erneut, die Dateien herunterzuladen.</li> <li>2. Wenn der Download weiterhin fehlschlägt, versuchen Sie, die Dateien außerhalb von NetWitness Suite herunterzuladen. Eine entsprechende Beschreibung finden Sie in <a href="#">Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff)</a>.</li> <li>3. Wenn Sie die Aktualisierungsdatei weiterhin nicht herunterladen können, wenden Sie sich an den Kundensupport (<a href="https://community.rsa.com/docs/DOC-1294">https://community.rsa.com/docs/DOC-1294</a>).</li> </ol> |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fehlermeldung</b> | <p><b>deploy_admin Das Passwort des Nutzers ist abgelaufen</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Ursache</b>       | <p>Das <code>deploy_admin</code>-Benutzerpasswort ist abgelaufen.</p> <p>Setzen Sie das <code>deploy_admin</code>-Passwort zurück.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Lösung</b>        | <ol style="list-style-type: none"><li>1. Wählen Sie im NetWitness Suite-Menü <b>ADMIN &gt; Sicherheit &gt; Registerkarte Benutzer</b> aus.</li><li>2. Wählen Sie <b>deploy_admin</b> aus und klicken Sie auf <b>Passwort zurücksetzen</b>.<ul style="list-style-type: none"><li>• Wenn NetWitness Suite Ihnen erlaubt, das abgelaufene <code>deploy_admin</code>-Passwort im Dialogfeld <b>Passwort zurücksetzen</b> einzugeben, führen Sie die folgenden Schritte aus.<ol style="list-style-type: none"><li>a. Geben Sie das abgelaufene <code>deploy_admin</code>-Passwort ein.</li><li>b. Deaktivieren Sie das Kontrollkästchen <b>Passwortänderung bei nächster Anmeldung erzwingen</b>.</li><li>c. Klicken Sie auf <b>Speichern</b>.</li></ol></li><li>• Wenn NetWitness Suite Ihnen nicht erlaubt, das abgelaufene <code>deploy_admin</code>-Passwort im Dialogfeld <b>Passwort zurücksetzen</b> einzugeben, führen Sie die folgenden Schritte aus.<ol style="list-style-type: none"><li>a. Führen Sie auf dem NW-Server-Host und allen anderen Hosts auf 11.x den folgenden Befehl mit dem neuen <code>deploy_admin</code>-Passwort aus.<br/><code>/opt/rsa/saTools/bin/set-deploy-admin-password</code></li><li>b. Führen Sie auf dem Host mit dem Installations-/Orchestrierungsfehler den Befehl <code>nwsetup-tui</code> aus und verwenden Sie das neue <code>deploy_admin</code>-Passwort.</li></ol></li></ul></li></ol> |

|                      |                                                                                                                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fehlermeldung</b> | Das <code>/var/log/netwitness/orchestration-server/orchestration-server.log</code> enthält einen ähnlichen Fehler wie den folgenden:<br><pre>API Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException Exception::Version '11.0.0.n' is not supported</pre> |
| <b>Problem</b>       | Nach der Aktualisierung des NW-Serverhosts auf 11.1 ist der einzige Aktualisierungspfad für die Nicht-NW-Serverhosts 11.1. Wenn Sie versuchen, einen Nicht-NW-Serverhost zu einem Patch 11.0.0.n zu aktualisieren (z. B. von 11.0.0.0 auf 11.0.0.3), erhalten Sie diesen Fehler.                           |
| <b>Lösung</b>        | Sie haben zwei Möglichkeiten: <ul style="list-style-type: none"> <li>• Aktualisieren Sie die Nicht-NW-Serverhosts auf Version 11.1, oder</li> <li>• Aktualisieren Sie den Nicht-NW-Serverhost nicht (behalten sie die aktuelle Version).</li> </ul>                                                        |

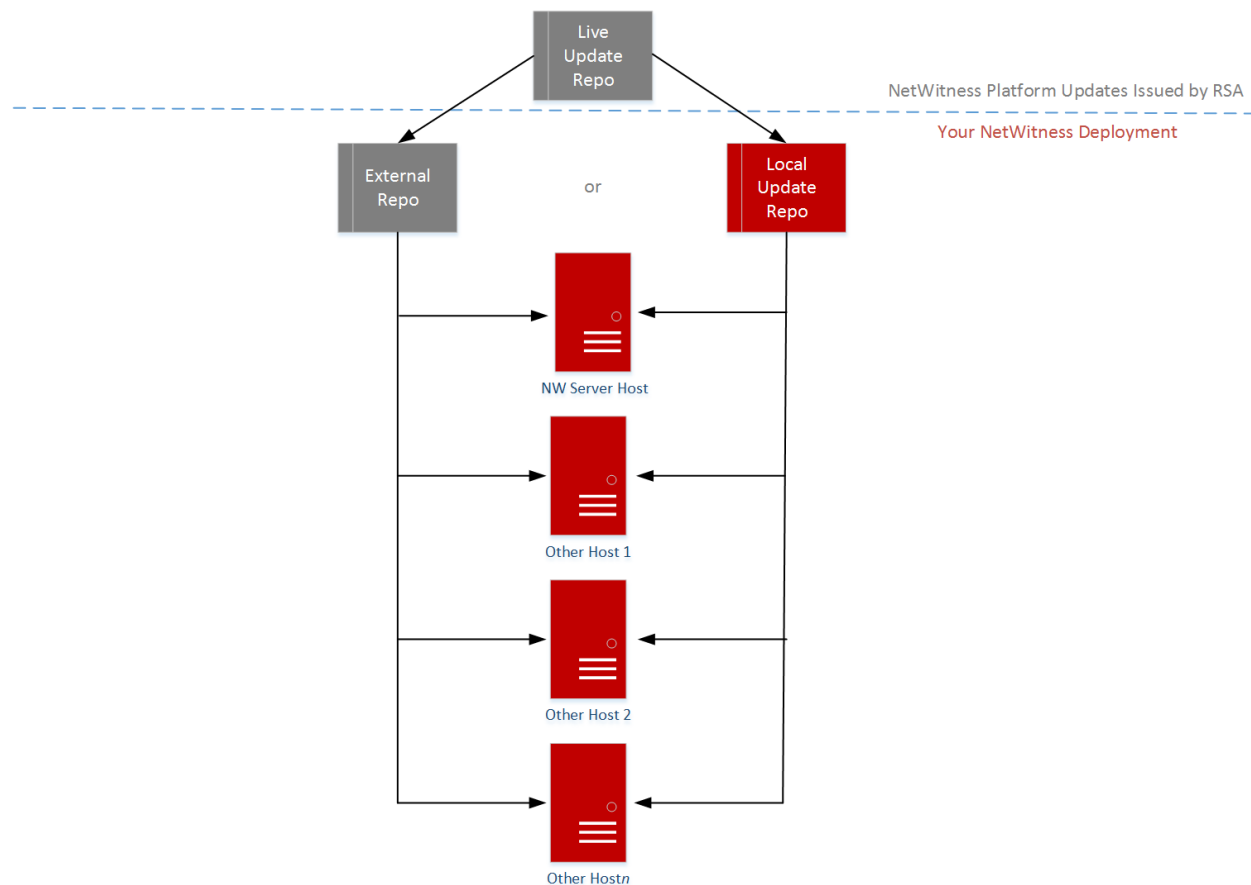
|                      |                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------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

## Anhang B: Auffüllen des lokalen Repository

NetWitness Platform sendet Versionsaktualisierungen aus dem Live-Update-Repository in das lokale Update-Repository. Für den Zugriff auf das Live-Update-Repository ist die Eingabe der Anmeldedaten des Live-Kontos erforderlich, die unter **ADMIN > SYSTEM > Live** konfiguriert werden. Darüber hinaus müssen Sie das Kontrollkästchen `Automatically download information about new updates every day` unter **ADMIN > SYSTEM > Aktualisierungen** aktivieren, um das lokale Repository täglich aufzufüllen.

Das folgende Diagramm zeigt, wie Sie Versionsaktualisierungen erhalten, wenn Ihre NetWitness Platform-Bereitstellung über Webzugriff verfügt.

**RSA** NetWitness Platform® 11.x.x.x Version Update Workflow – Web Access



**Hinweis:** Wenn Sie erstmalig eine Verbindung mit dem Live-Update-Repository herstellen, können Sie auf alle CentOS 7-Systempakete und die RSA-Produktionspakete zugreifen. Je nach Internetverbindung Ihres NW-Servers und Datenverkehr des RSA-Repository kann der Download dieser Daten von mehr als 2,5 GB längere Zeit in Anspruch nehmen. Es ist nicht obligatorisch, das Live-Update-Repository zu verwenden. Alternativ können Sie ein externes Repository verwenden, wie beschrieben unter [Einrichten eines externen Repository mit RSA und Betriebssystemupdates](#).

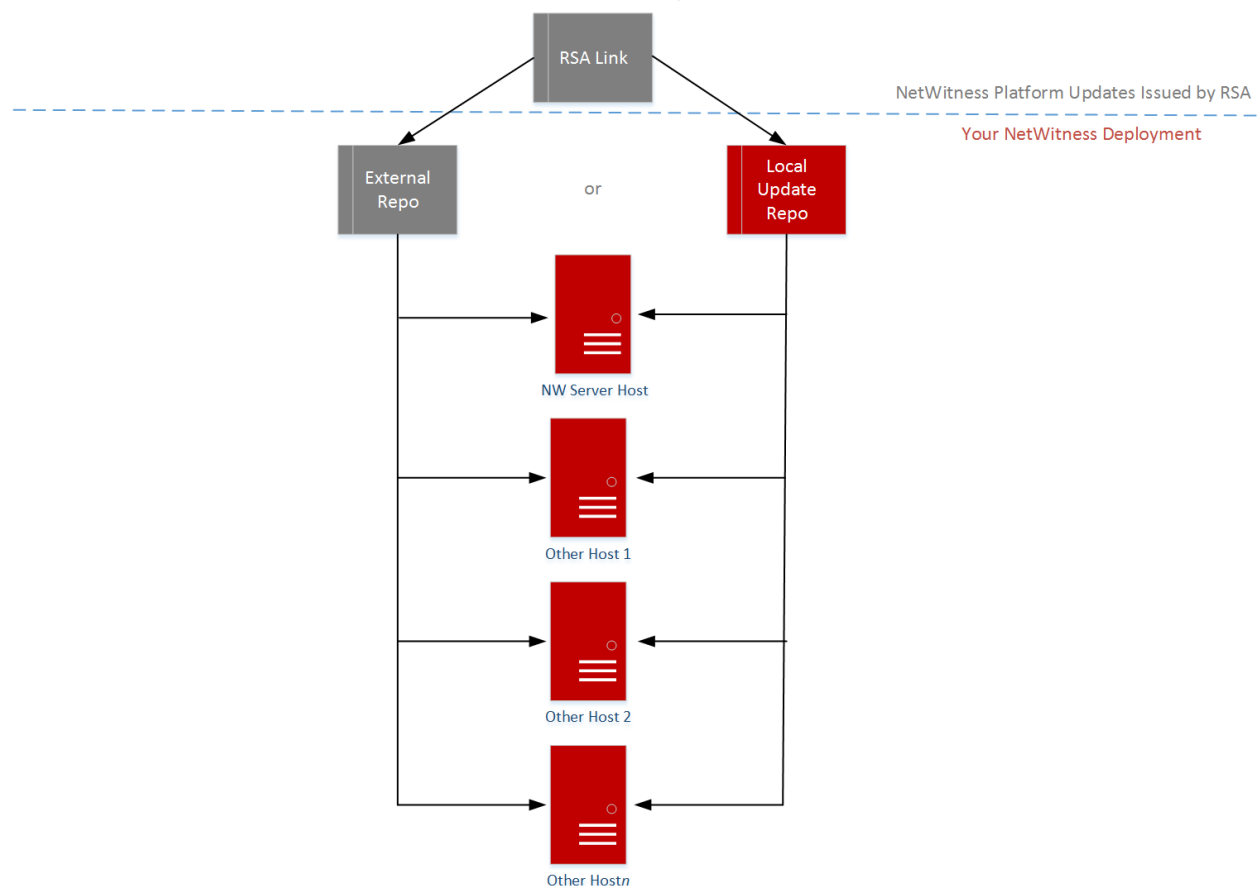
Zur Verbindung mit dem Live-Update-Repository navigieren Sie zu der Ansicht „ADMIN“ > „System“, wählen Sie im Optionsbereich **Live-Services** aus und vergewissern Sie sich, dass die Anmeldedaten konfiguriert sind (**Verbindung** sollte grün markiert sein). Wenn es nicht grün ist, klicken Sie auf **Anmelden** und stellen Sie eine Verbindung her.

**Hinweis:** Wenn Sie Proxys zum Kommunizieren mit dem Live-Update-Repository benötigen, können Sie den Proxy-Host, den Proxybenutzernamen und das Proxypasswort konfigurieren. Weitere Informationen finden Sie unter „Konfigurieren des Proxy für NetWitness Platform“ im *Systemkonfigurationsleitfaden für NetWitness Platform 1.1*.

Wenn Ihre NetWitness Platform-Bereitstellung keinen Webzugriff hat, siehe [Anwenden von Aktualisierungen über die Befehlszeile \(Kein Webzugriff\)](#).

Das folgende Diagramm zeigt, wie Sie Versionsaktualisierungen erhalten, wenn Ihre NetWitness Platform-Bereitstellung nicht über Webzugriff verfügt.

RSA NetWitness Platform® 11.x.x.x Version Update Workflow – No Web Access





## Anhang C: Einrichten eines externen Repository

---

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

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

1. (Bedingungsabhängig) Führen Sie diesen Schritt durch, wenn Sie ein externes Repository haben und Sie dieses außer Kraft setzen möchten.
  - 1. Fall: Sie haben den Host von einem externen Repository aus per Bootstrap neu gestartet und Sie möchten ein Upgrade durchführen mithilfe eines lokalen Repository auf dem Adminserver.
    - a. Erstellen Sie die Datei `/etc/netwitness/platform/repobase`.  
`vi /etc/netwitness/platform/netwitness/repobase`
    - b. Bearbeiten Sie die Datei `repobase`, sodass die einzige Information in der Datei die folgende URL ist.  
`https://nw-node-zero/nwrpmrepo`
    - c. Führen Sie die Anweisungen zum Ausführen des Upgrade mithilfe des Tools `upgrade-client` aus.
  - 2. Fall: Sie haben den Host von eines lokalen Repository auf dem Adminserver (NW-Serverhost) per Bootstrap neu gestartet und Sie möchten ein externes Repository für das Upgrade verwenden.
    - a. Erstellen Sie die Datei `/etc/netwitness/platform/repobase`.  
`vi /etc/netwitness/platform/netwitness/repobase`
    - b. Bearbeiten Sie die Datei `repobase`, sodass die einzige Information in der Datei die folgende URL ist.  
`https://<webserver-ip>/<alias-for-repo>`
    - c. Führen Sie die Anweisungen zum Ausführen des Upgrade mithilfe des Tools `upgrade-client` aus.  
Die Anweisungen finden Sie unter [Anwenden von Aktualisierungen über die Befehlszeile \(Kein Webzugriff\)](#).
2. Richten Sie das externe Repository ein.
  - a. Melden Sie sich bei dem Webserverhost an.
  - b. Erstellen Sie ein Verzeichnis, um das NW-Repository (`netwitness-11.2.0.0.zip`) zu hosten, z. B. `ziprepo` unter `web-root` des Webservers. Beispiel: Wenn `/var/netwitness` das „web-root“-Verzeichnis ist, senden Sie die folgende Befehlszeichenfolge.  
`mkdir -p /var/netwitness/<your-zip-file-repo>`
  - c. Erstellen Sie das Verzeichnis `11.2.0.0` unter `/var/netwitness/<your-zip-file-repo>`.  
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0`

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

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```

- e. Entpacken Sie die Datei `netwitness-11.2.0.0.zip` in das Verzeichnis

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

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

Durch das Entpacken von `netwitness-11.2.0.0.zip` entstehen zwei Zip-Dateien (`OS-11.2.0.0.zip` und `RSA-11.2.0.0.zip`) und einige andere Dateien.

- f. Entpacken Sie die Datei:

- i. `OS-11.2.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`.

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

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

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

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

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

Das folgende Beispiel zeigt, wie die Dateistruktur der RSA Versionsaktualisierung aussieht,

nachdem Sie die Datei entpackt haben.

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

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

- g. (Bedingungsabhängig – für Azure) Befolgen Sie diese Schritte, um Azure zu aktualisieren.
  - i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
  - ii. `unzip nw-azure-11.2-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
  - iii. `cd /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
  - iv. `createrepo .`
- h. Verwenden Sie die `http://<web server IP address>/<your-zip-file-repo>` als Antwort auf die Eingabeaufforderung **Geben Sie den Basis-URL des externen Update-Repository ein** des NW 11.2.0.0 Setup-Programms (`nwsetup-tui`).

## Revisionsverlauf

| Version | Datum           | Beschreibung                                                                                                            | Verfasser |
|---------|-----------------|-------------------------------------------------------------------------------------------------------------------------|-----------|
| 1.0     | 15. August 2018 | Betriebsfreigabe                                                                                                        | IDD       |
| 1.1     | 4. Sept. 2018   | Post-RTO-Updates.                                                                                                       | IDD       |
| 1.2     | 9-Okt-18        | Die Syntax wurde in den Anweisungen „Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff)“ korrigiert. |           |