RSA NETWITNESS® SUITE

Leitfaden zur Aktualisierung

für Version 11.0.x auf 11.1

Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

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.

Juli 2018

Inhalt

Einführung

RSA NetWitness® Suite11.1.0.0 stellt Korrekturen für alle Produkte in der Suite bereit. Die Komponenten der Suite sind NetWitness-Server (Admin-Server, Konfigurationsserver, Integration-Server, Investigate-Server, Orchestrierungsserver, Respond-Server und Security-Server), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, 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 Suite 11.1.0.0 unterstützt:

- 11.0.0.0 auf 11.1.0.0
- 11.0.0.1 auf 11.1.0.0
- 11.0.0.2 auf 11.1.0.0
- 10.6.5.x auf 11.1.0.0

  Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

  Anweisungen für ein Upgrade von 10.6.5.x auf 11.1 finden Sie unter *RSA NetWitness Suite 10.6.5.x auf 11.1 – Upgradehandbuch für physische Hosts* und *RSA NetWitness Suite 10.6.5.x auf 11.1 – 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 Suite – Leitfaden für die ersten Schritte mit Hosts und Services*.

Aufgaben zur Vorbereitung der Aktualisierung

Führen Sie die folgenden Aufgaben durch, um die Aktualisierung auf NetWitness Suite 11.1.0.0 vorzubereiten. Diese Aufgaben sind nach den folgenden Kategorien unterteilt.

Allgemein

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

In den folgenden Tabellen sind die neuen Ports in 11.1.0.0 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
Endpoint-Server	NW-Server	TCP 27017	MongoDB

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

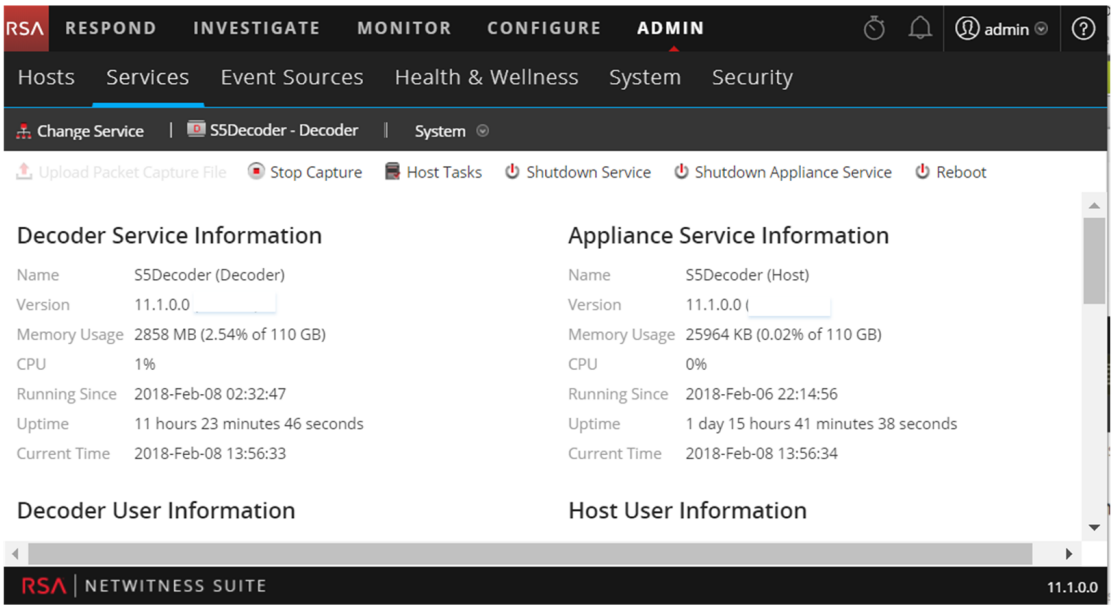
1. Erstellen Sie eine Sicherungskopie der folgenden Datei in einem anderen, sicheren Verzeichnis.
   `/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`
   Sie müssen Ihre angepassten Parameterwerte aus diesem Backup abrufen, nachdem Sie den Malware Analysis-Host auf 11.1.0.0 aktualisiert haben. Die Aktualisierung erzeugt eine neue Konfigurationsdatei, in der alle Parameter auf die Standardwerte eingestellt sind.
2. Löschen Sie die folgende Datei.
   `/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`

Aufgabe 3: Beenden der Datenerfassung und -aggregation

Beenden der Paketerfassung

So beenden Sie die Erfassung von Paketen:

1. Melden Sie sich bei NetWitness Suite 11.0.x an und wechseln Sie zu **ADMIN** > **Services**. 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 

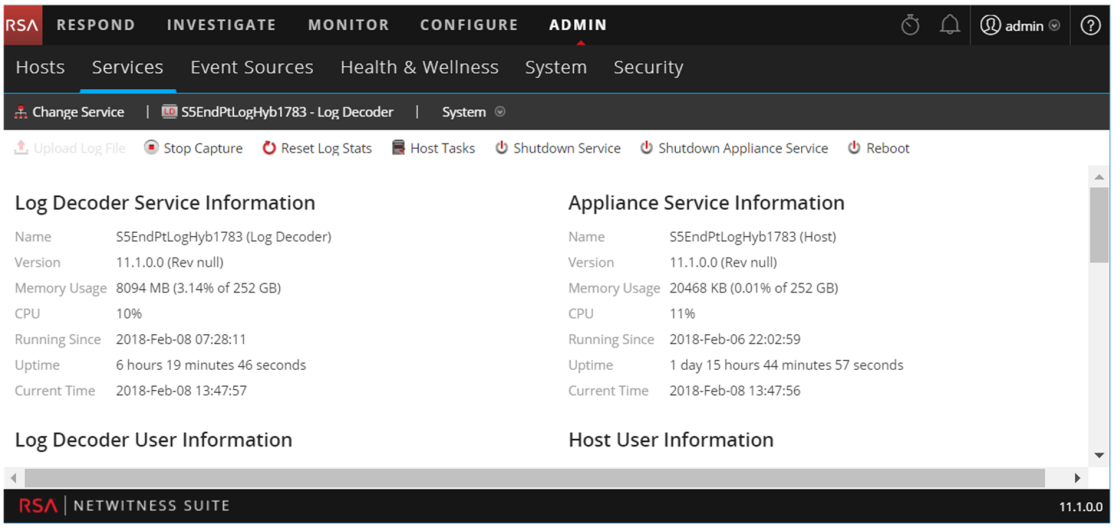
.

Beenden der Protokollerfassung

So beenden Sie die Protokollerfassung:

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

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



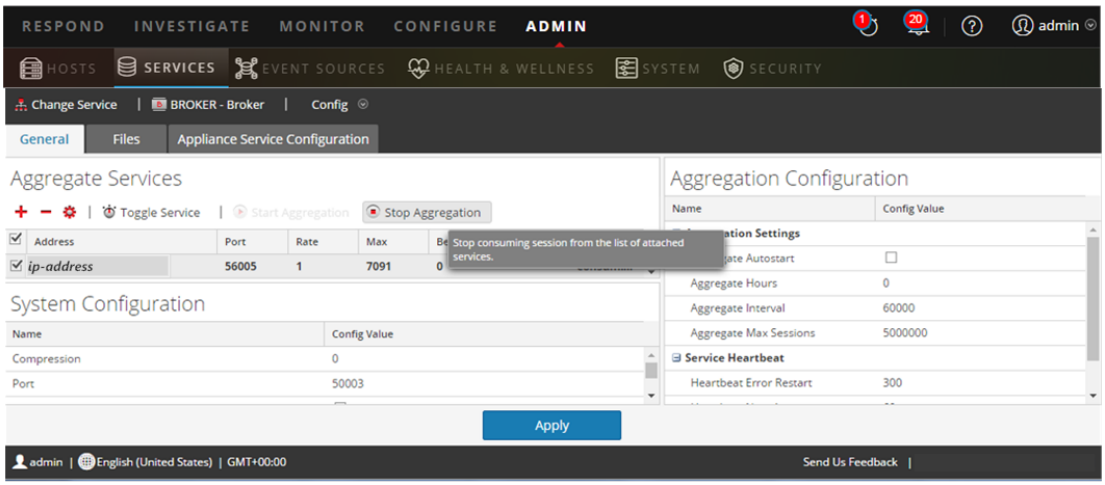
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **System** aus.

4. Klicken Sie in der Symbolleiste auf 

.

Aggregation beenden

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



5. Klicken Sie unter **Aggregierte Services** auf 

.

Aufgabe 4: Sicherstellen, dass `deploy_admin`-Benutzeranmeldedaten nach wie vor gültig (nicht abgelaufen) sind

Sie müssen über gültige (nicht abgelaufene) `deploy_admin`-Benutzeranmeldedaten verfügen, um eine Aktualisierung auf 11.1 durchführen zu können.

Teil I. Ablaufstatus von `deploy_admin`-Benutzeranmeldedaten prüfen

Führen Sie das folgende Verfahren durch, um festzustellen, ob die `deploy_admin`-Benutzeranmeldedaten abgelaufen sind.

1. Wählen Sie im NetWitness Suite-Menü **ADMIN** > **Sicherheit** > Registerkarte **Benutzer** aus.
2. Stellen Sie sicher, dass `deploy_admin` nicht abgelaufen ist.
   - Sind sie nach wie vor gültig, können Sie mit der Aktualisierung fortfahren.
   - Sind diese abgelaufen, führen Sie Teil II dieser Aufgabe aus.

(Bedingungsabhängig) Teil II. Abgelaufene `deploy_admin`-Benutzeranmeldedaten zurücksetzen

Führen Sie das folgende Verfahren zum Zurücksetzen abgelaufener `deploy_admin`-Benutzeranmeldedaten aus.

1. Wählen Sie `deploy_admin` aus und klicken Sie auf **Passwort zurücksetzen**.
2. (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**.
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 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.

Reporting Engine

Aufgabe 5: 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 Suite11.1 Reporting Engine-Konfigurationsleitfaden*Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen..

An dieser Stelle können Sie mit den Updateanweisungen fortfahren.

Respond

Aufgabe 6: (Bedinungsabhängig) 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 7: Sichern der angepassten Skripte zur Normalisierung des Respond-Service

Die von RSA umstrukturierten Skripte zur Normalisierung des Respond-Service sind in 11.1.0.0 im `/var/lib/netwitness/respond-server/scripts`-Verzeichnis gespeichert. Sie müssen diese in 11.0.x sichern, bevor Sie auf 11.1.0.0 aktualisieren, damit Sie sie in 11.1.0.0, 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 11.1.0.0 wiederherstellen können.

Aufgabe 8: (Bedingungsabhängig – für Azure Stack)

Füllen Sie das Repository mit den zusätzlichen Paketen auf.

1. Wenn Sie ein lokales Repository verwenden, extrahieren Sie die Azure-ZIP-Datei aus den folgenden Schritten auf dem Admin-Server:

a. Als Root-Benutzer ausführen: `mkdir -p /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

b. Entpacken Sie sie in das oben stehende Verzeichnis: `unzip nw-azure-11.1-extras.zip -d /var/lib/netwitness/common/repo/11.1.0.0/OS/other`

2. Gehen Sie folgendermaßen vor, wenn Sie das externe Repository verwenden:

a. Entpacken Sie nach dem Einrichten der Inhalte von 11.1.0.0 im externen Repository die Datei „nw-azure-11.1-extras.zip“ in das Verzeichnis „<Basisverzeichnis>11.1.0.0/OS/anderer Ordner“ des externen Repository.

b. Führen Sie den Befehl „createrepo“ im 11.1.0.0/OS-Verzeichnis des externen Repository aus.

Aufgaben bei der Aktualisierung

Führen Sie die folgenden Aufgaben durch, um NetWitness Suite 11.0.x.x auf 11.1.0.0 zu aktualisieren.

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

Hinweis: Wenn Sie vorhaben, ein Update-Repository (Repo) für NetWitness-Suite 11.1.0.0 zu verwenden, das sich von dem Repository unterscheidet, das Sie jetzt für 11.0.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 11.1.0.0 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.

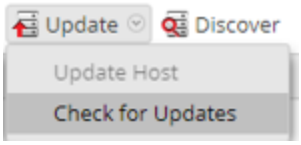
Wenn Sie ein externes Repository ausgewählt haben, müssen Sie es einrichten. Anweisungen zum Einrichten eines externen Repository finden Sie unter Anhang C: Einrichten eines externen Repository.

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

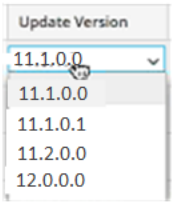
In der Ansicht „Hosts“ werden die in Ihrem lokalen Update-Repository verfügbaren Softwareversionsaktualisierungen angezeigt und Sie wählen die gewünschten Aktualisierungen über die Ansicht „Hosts“ aus und wenden diese an.

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

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



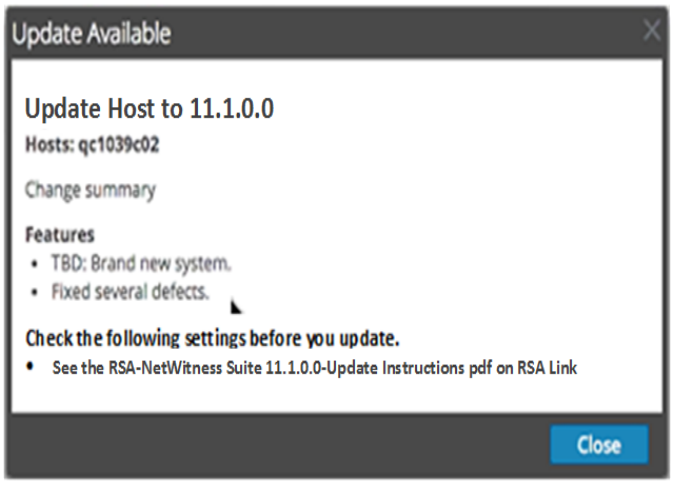
4. Wählen Sie einen Host oder Hosts aus.
   Sie müssen zunächst die NW-Server auf die neueste Version aktualisieren. Sie können die anderen Hosts in beliebiger Reihenfolge aktualisieren, aber RSA empfiehlt, dass Sie die Richtlinien unter „Ausführen im gemischten Modus“ im *RSA NetWitness Suite – Leitfaden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

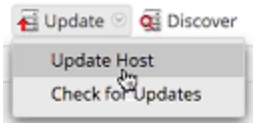
   - Wenn Sie mehr als einen Host auf diese Version aktualisieren möchten, dann aktivieren Sie nach der Aktualisierung des NW-Serverhosts das Kontrollkästchen links neben den Hosts. Es sind nur Versionen von Aktualisierungen aufgelistet, die derzeit unterstützt werden.
   - Wenn Sie ein Dialogfeld mit den 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.

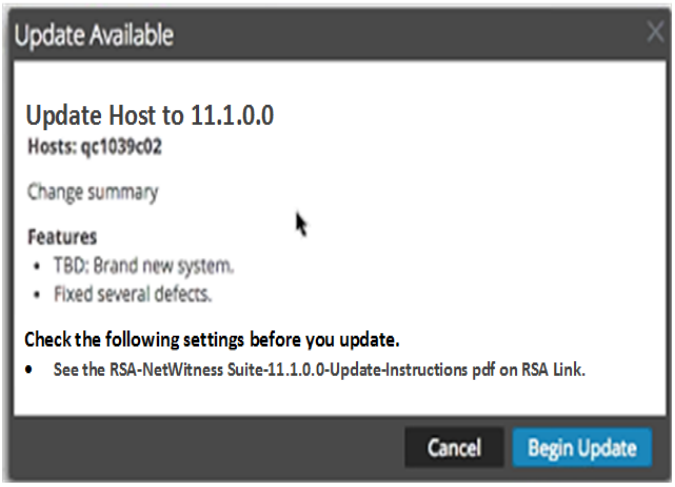


- Wenn Sie die gewünschte Version nicht finden können, wählen Sie **Aktualisieren > Nach Updates suchen** aus, um das Repository auf alle verfügbaren Aktualisierungen zu prüfen. Wenn eine Aktualisierung verfügbar ist, wird die Meldung „Es sind neue Hostaktualisierungen verfügbar“ angezeigt und die Spalte **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 wird 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 Suite die Aufforderung **Host neu starten** an.
8. Klicken Sie in der Symbolleiste auf **Host neu starten**.
   NetWitness Suite 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: 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.

Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff)

Wenn Ihre Bereitstellung von RSA NetWitness Suite 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-11.1.0.0.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/11.1.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.1.0.0
   ```
4. Entpacken Sie das Paket in das Staging-Verzeichnis, das Sie erstellt haben (z. B. `tmp/upgrade/11.1.0.0`).
   ```
   cd /tmp/upgrade/11.1.0.0
   unzip /tmp/upgrade/11.1.0.0/netwitness-11.1.0.0.zip
   ```
5. Initialisieren Sie die Aktualisierung auf dem NW-Server.
   ```
   upgrade-cli-client --init --version 11.1.0.0 --stage-dir
   /tmp/upgrade/
   ```
6. Wenden Sie die Aktualisierung auf den NW-Server an.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version
   11.1.0.0
   ```
7. Melden Sie sich bei NetWitness Suite an und starten Sie den NW-Serverhost in der Ansicht „Host“.
8. Wenden Sie die Aktualisierung auf jeden Nicht-NW-Serverhost an.
   ```
   upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> -
   -version 11.1.0.0
   ```
   Die Aktualisierung ist abgeschlossen, wenn der Abruf abgeschlossen ist.
9. Melden Sie sich bei NetWitness Suite 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
   ```

Aktualisieren oder Installieren der Legacy-Windows-Sammlung

Siehe *Leitfaden RSA NetWitness Legacy Windows Collection*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

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 die Aktualisierung auf NetWitness Suite 11.1.0.0 durchgeführt haben.

Allgemein

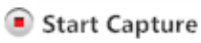
Diese Aufgaben gelten für alle Kunden von NetWitness Suite 11.1.0.0.

Aufgabe 1: Starten der Datenerfassung und -aggregation

Starten Sie Paket- und Protokollerfassung sowie Paket- und Protokollaggregation nach der Aktualisierung auf 11.1.0.0 neu.

Starten der Paketerfassung

So starten Sie die Paketerfassung:

1. Wählen Sie im Menü **NetWitness Suite** 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

So starten Sie die Protokollerfassung:

1. Wählen Sie im Menü **NetWitness Suite** die Optionen **ADMIN** > **Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie die einzelnen **Log Decoder**-Services aus.

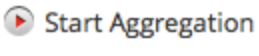
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **System** aus.

4. Klicken Sie in der Symbolleiste auf 

.

Aggregation starten

So starten Sie die Aggregation:

1. Wählen Sie im Menü **NetWitness Suite** 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 

.

NW-Server

Aufgabe 2: (Bedingungsabhängig) Korrigieren der Auditprotokollvorlagen, die in der Logstash-Ausgabe-Konfigurationsdatei nicht aktualisiert werden

Problem: Wenn ein Benutzer von 11.0.0.0 auf 11.1.0.0 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 Suite 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 klicken Sie auf **Speichern**.

(Bedingungsabhängig) Aufgabe 3: 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 11.1.0.0 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® Suite 11.1 – Handbuch Systemsicherheit und Benutzerverwaltung*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

RSA NetWitness® Endpoint

Aufgabe 4: 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.

- Importieren Sie das NetWitness Endpoint CA-Zertifikat in den vertrauenswürdigen NetWitness Suite-Speicher, wie in „Exportieren des SSL-Zertifikats von NetWitness Endpoint“ unter dem Thema „Konfigurieren kontextbezogener Daten von Endpoint über wiederkehrenden Feed“ im *RSA NetWitness 11.1 Endpoint-Integrationsleitfaden* beschrieben. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

RSA NetWitness® Endpoint Insights

(Optional) Aufgabe 5: Installieren von Endpoint Hybrid oder Endpoint Log Hybrid

Siehe:

RSA NetWitness Suite 11.1 Installationshandbuch für physische Hosts für Anweisungen zur Installation auf einem physischen Host

RSA NetWitness Suite 11.1 Installationshandbuch für virtuelle Hosts für Anweisungen für die Installation auf einem virtuellen Host

Event Stream Analysis

Diese Aufgaben gelten für Kunden von NetWitness Suite 11.1.0.0, die Event Stream Analysis verwenden.

(Bedingungsabhängig) Aufgabe 6: 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 11.1.0.0 einwandfrei und sollte als die „Gruppieren nach“-Bedingung für die Aggregationsregel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ (in 11.1.0.0 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 11.1.0.0 wieder in „Domain für verdächtige C&C“ ändern.

1. Melden Sie sich bei NetWitness Suite 11.1.0.0 an.
2. Navigieren Sie zu **KONFIGURIEREN** > **Incident-Regeln**.
3. 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.
4. 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 Suite – Automatisierte Bedrohungserkennung“ und im Abschnitt

„Konfigurieren von ESA Analytics“ im NetWitness Suite ESA-Konfigurationsleitfaden. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Respond

Aufgabe 7: (Bedingungsabhängig) 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 11.1.0.0 wurden neue „Gruppieren nach“-Felder zu Respond hinzugefügt. Die neuen „Gruppieren nach“-Felder sind in der NetWitness Suite-Benutzeroberfläche nicht sichtbar, wenn Sie nicht die aktuelle Version der Datei vom Server abrufen.

Aufgabe 8: Abrufen der aktuellen Version der Skripte zur Normalisierung des Respond-Service und Wiederherstellung aller benutzerdefinierten Skripte zur Normalisierung des Respond-Service

RSA hat in 11.1.0.0 die Skripte zur Normalisierung des Respond-Service im `/var/lib/netwitness/respond-server/scripts`-Verzeichnis umstrukturiert. Sie müssen die alten Versionen ersetzen.

Vor der Aktualisierung auf 11.1.0.0 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 11.1.0.0 geändert:
`normalize_alerts.js`
`normalize_core_alerts.js`
`normalize_ma_alerts.js`

Aufgabe 9: Hinzufügen von Einstellungen für Antwort auf Benachrichtigungen

Berechtigungen für Einstellungen für Antwort auf Benachrichtigungen erlauben Respond-Administratoren, Datenschutzbeauftragten und SoC-Managern, auf Einstellungen für Antwort auf Benachrichtigungen 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 Suite-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 für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 10: Aktualisieren der „Gruppieren nach“-Werte der Incident-Standardregel

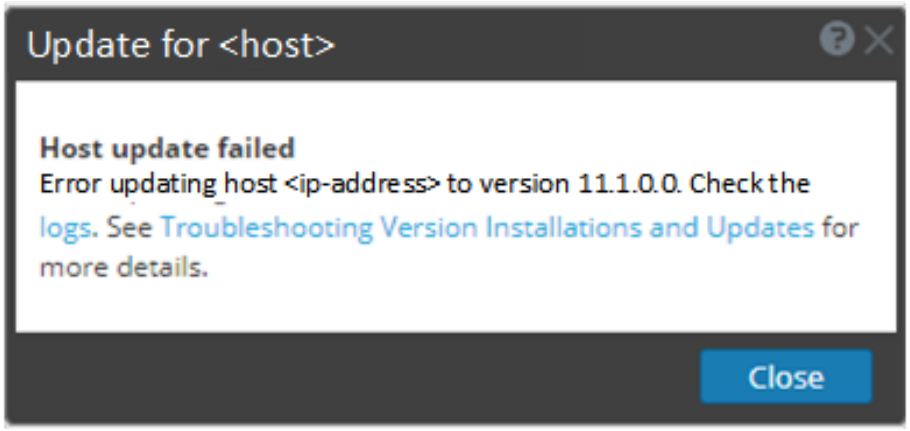
Vier der Incident-Standardregeln verwenden als „Gruppieren nach“-Wert jetzt „Quell-IP-Adresse“. Um die Standardregeln zu aktualisieren, ändern Sie den „Gruppieren nach“-Wert der folgenden Standardregeln in „Quell-IP-Adresse“:

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

1. Navigieren Sie zu **KONFIGURIEREN** > **Incident-Regeln** und klicken Sie bei der Regel, die Sie aktualisieren möchten, auf den Link in der Spalte **Name**. Die Detailansicht der Incident-Regel wird angezeigt.
2. Wählen Sie im Feld **Gruppieren nach** den neuen „Gruppieren nach“-Wert aus.
3. Klicken Sie auf **Speichern**, um die Regel zu aktualisieren.

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	
Problem	Wenn Sie eine Aktualisierungsversion auswählen und auf **Aktualisieren >Host aktualisieren** klicken, ist zwar der Download erfolgreich, aber die Aktualisierung schlägt fehl.

Lösung	1. **Versuchen Sie, die Versionsaktualisierung erneut auf den Host anzuwenden**.
	Häufig ist das alles, was Sie tun müssen.
	2. Gehen Sie folgendermaßen vor, wenn Sie die neue Aktualisierungsversion weiterhin nicht anwenden können:
	a. Überwachen Sie während der Aktualisierung die folgenden Protokolle auf dem NW-Server (Senden Sie hierfür über die Befehlszeile z. B. die Befehlszeichenfolge `tail -f`.):
	`/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`
Der Fehler wird in einem oder mehreren dieser Protokolle angezeigt.

b. Versuchen Sie, das Problem zu lösen, und wenden Sie die 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.

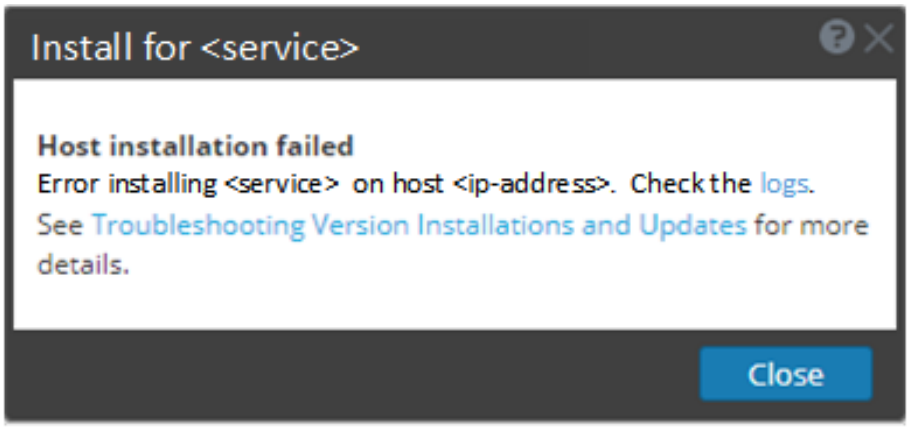
     a. Setzen Sie `deploy_admin` zurück, um ein neues Passwort zu verwenden.

     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	
Problem	Wenn Sie einen Host auswählen und auf **Installieren** klicken, schlägt der Service für den Installationsprozess fehl.

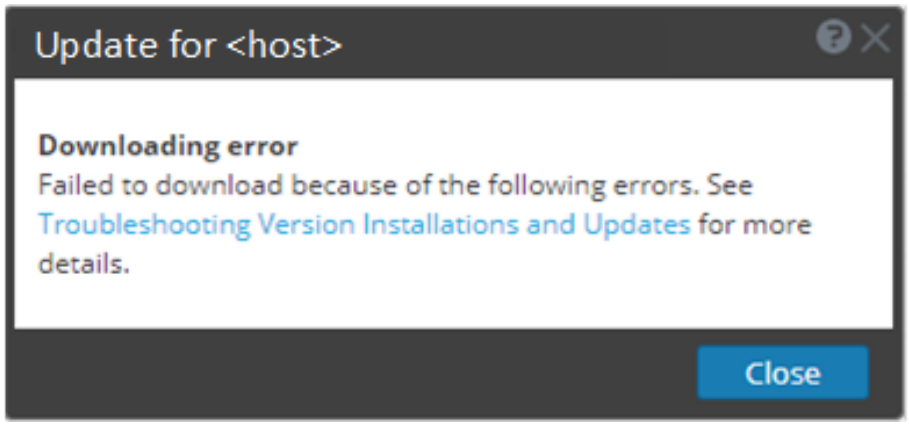
Lösung	1. **Versuchen Sie, den Service erneut zu installieren**.
	Häufig ist das alles, was Sie tun müssen.
	2. Gehen Sie folgendermaßen vor, falls Sie den Service immer noch nicht installieren können:
	a. Überwachen Sie während der Aktualisierung die folgenden Protokolle auf dem NW-Server (Senden Sie hierfür über die Befehlszeile z. B. die Befehlszeichenfolge `tail -f`.):
	`/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`
	Der Fehler wird in einem oder mehreren dieser Protokolle angezeigt.
	b. Versuchen Sie, das Problem zu lösen, und installieren Sie den Service neu.
	• Ursache 1: In den Befehl nwsetup-tui wurde das falsche`deploy_admin` Passwort eingegeben.
	Lösung: Rufen Sie Ihr `deploy_admin` -Passwort ab.

Führen Sie zur Behebung von Ursache 1 die folgenden Schritte aus.

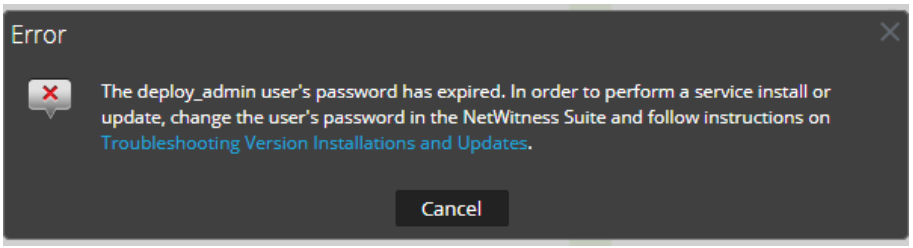
1. Wählen Sie im NetWitness Suite-Menü **ADMIN** > **Sicherheit** > Registerkarte **Benutzer** aus.
2. Wählen Sie `deploy_admin` aus und klicken Sie auf **Passwort zurücksetzen**.
3. (Bedingungsabhängig) Wenn NetWitness Suite Ihnen nicht erlaubt, das abgelaufene `deploy_admin`-Passwort im Dialogfeld **Passwort zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus.
   a. 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, dessen 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	
Problem	Wenn Sie eine Aktualisierungsversion auswählen und auf **Aktualisieren** > **Host aktualisieren** klicken, wird der Download zwar gestartet, kann aber nicht abgeschlossen werden.
Ursache	Die Downloaddateien der Version können groß sein und das Herunterladen

	kann daher lange dauern. Wenn beim Download Kommunikationsprobleme auftreten, schlägt er fehl.
Lösung	1. Versuchen Sie erneut, die Dateien herunterzuladen. 2. Wenn der Download weiterhin fehlschlägt, versuchen Sie, die Dateien außerhalb von NetWitness Suite herunterzuladen. Eine entsprechende Beschreibung finden Sie in Anwenden von Aktualisierungen über die Befehlszeile (Kein Webzugriff). 3. Wenn Sie die Aktualisierungsdatei weiterhin nicht herunterladen können, wenden Sie sich an den Kundensupport (https://community.rsa.com/docs/DOC-1294).

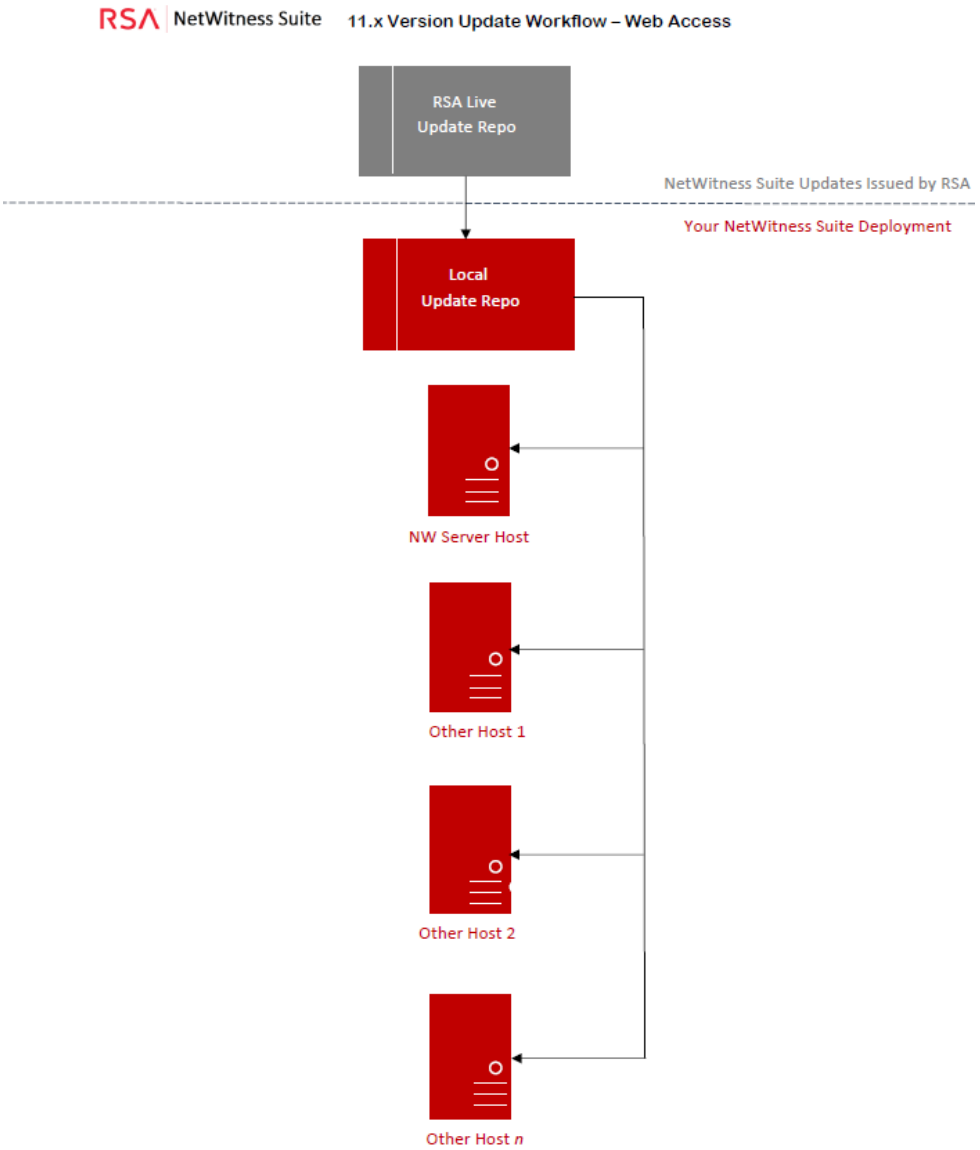
Fehlermeldung	
Ursache	Das `deploy_admin`-Benutzerpasswort ist abgelaufen.
Lösung	Setzen Sie das `deploy_admin`-Passwort zurück. 1. Wählen Sie im NetWitness Suite-Menü **ADMIN** > **Sicherheit** > Registerkarte **Benutzer** aus. 2. Wählen Sie **deploy_admin** aus und klicken Sie auf **Passwort zurücksetzen**. • 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**. • Wenn NetWitness Suite Ihnen nicht erlaubt, das abgelaufene `deploy_admin`-Passwort im Dialogfeld **Passwort zurücksetzen** einzugeben, führen Sie die folgenden Schritte aus. a. Führen Sie auf dem NW-Server-Host 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` b. Führen Sie auf dem Host mit dem Installations-/Orchestrierungsfehler den Befehl nwsetup-tui aus und verwenden Sie das neue `deploy_admin`-Passwort.

Fehlermeldung	Das `/var/log/netwitness/orchestration-server/orchestration-server.log` enthält einen ähnlichen Fehler wie den folgenden: `API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgument Exception::Version '11.0.0.n' is not supported`
Problem	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.
Lösung	Sie haben zwei Möglichkeiten: • Aktualisieren Sie die Nicht-NW-Serverhosts auf Version 11.1, oder • Aktualisieren Sie den Nicht-NW-Serverhost nicht (behalten sie die aktuelle Version).

Anhang B: Auffüllen des lokalen Repository

NetWitness-Suite 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 Suite-Bereitstellung über Webzugriff verfügt.



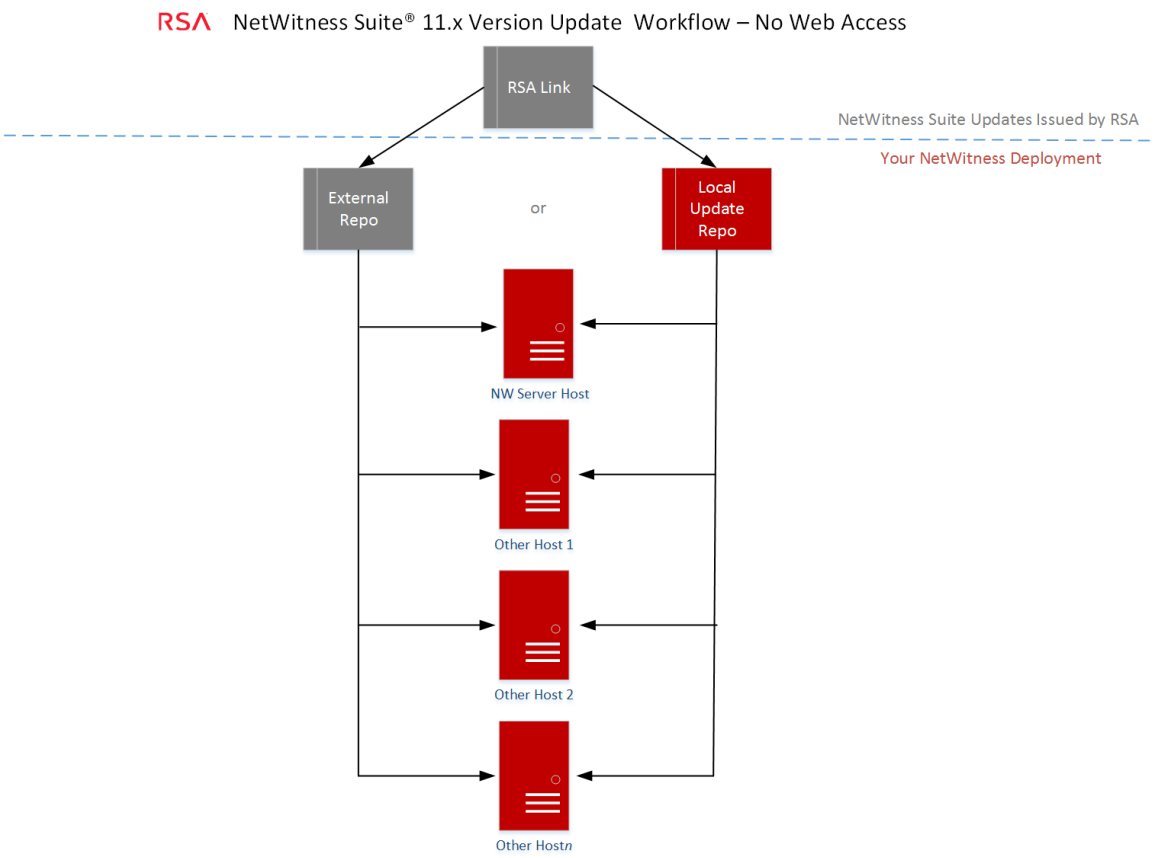
Hinweis: Wenn Sie erstmalig eine Verbindung mit dem Live-Update-Repository herstellen, können Sie auf alle CentOS 7-Systempakete und die RSA-Produktionspakete zugreifen. Je nach Internetverbindung Ihres NW-Servers und Datenverkehr des RSA-Repository kann der Download dieser Daten von mehr als 2,5 GB eine unbestimmte Dauer 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“.

Zur Verbindung mit dem Live-Update-Repository navigieren Sie zu der Ansicht **ADMIN > SYSTEM**, wählen Sie im Optionsbereich **Live** aus und vergewissern Sie sich, dass die Anmeldedaten konfiguriert sind (Licht für **Verbindung** sollte grün 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 Suite“ im *Systemkonfigurationsleitfaden für NetWitness Suite 1.1*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Wenn Ihre NetWitness Suite-Bereitstellung keinen Webzugriff hat, siehe „Anwenden von Aktualisierungen über die Befehlszeile“.

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


RSA NetWitness Suite® 11.x Version Update Workflow – No Web Access
RSA Link
NetWitness Suite Updates Issued by RSA
Your NetWitness Deployment
External Repo
or
Local Update Repo
NW Server Host
Other Host 1
Other Host 2
Other Hostn

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/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-cli-client` aus.
        Anweisungen finden Sie unter
        .
   - 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/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-cli-client` aus.
        Die Anweisungen finden Sie unter „Anwenden von Aktualisierungen über die Befehlszeile“.

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-11.1.0.0.zip`) zu hosten, z. B. `ziprepo` unter `web-root` des Webservers. Beispiel: /var/netwitness ist der Webstamm, senden Sie die folgende Befehlszeichenfolge:
   `mkdir -p /var/netwitness/<your-zip-file-repo>`

   c. Erstellen Sie das Verzeichnis 11.1.0.0 unter `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`

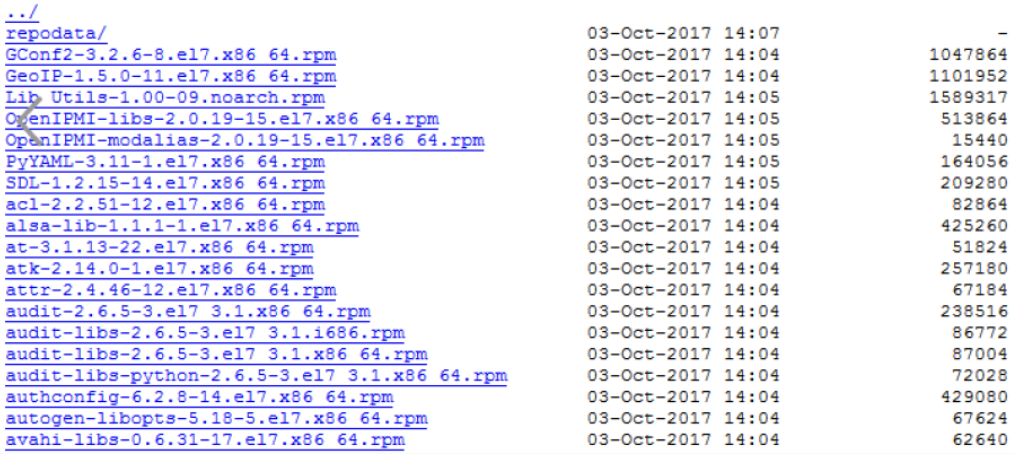
   d. Erstellen Sie die Verzeichnisse `OS` und `RSA` unter `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
   ```

   e. Entpacken Sie die Datei `netwitness-11.1.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   Durch das Entpacken von `netwitness-11.1.0.0.zip` entstehen zwei Zip-Dateien (`OS-11.1.0.0.zip` und `RSA-11.1.0.0.zip`) und einige andere Dateien.

   f. Entpacken Sie die Datei:

      1. `OS-11.1.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`.
      `unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
      Das folgende Beispiel zeigt, wie die Dateistruktur des Betriebssystems (OS)

angezeigt wird, nachdem Sie die Datei entpackt haben.

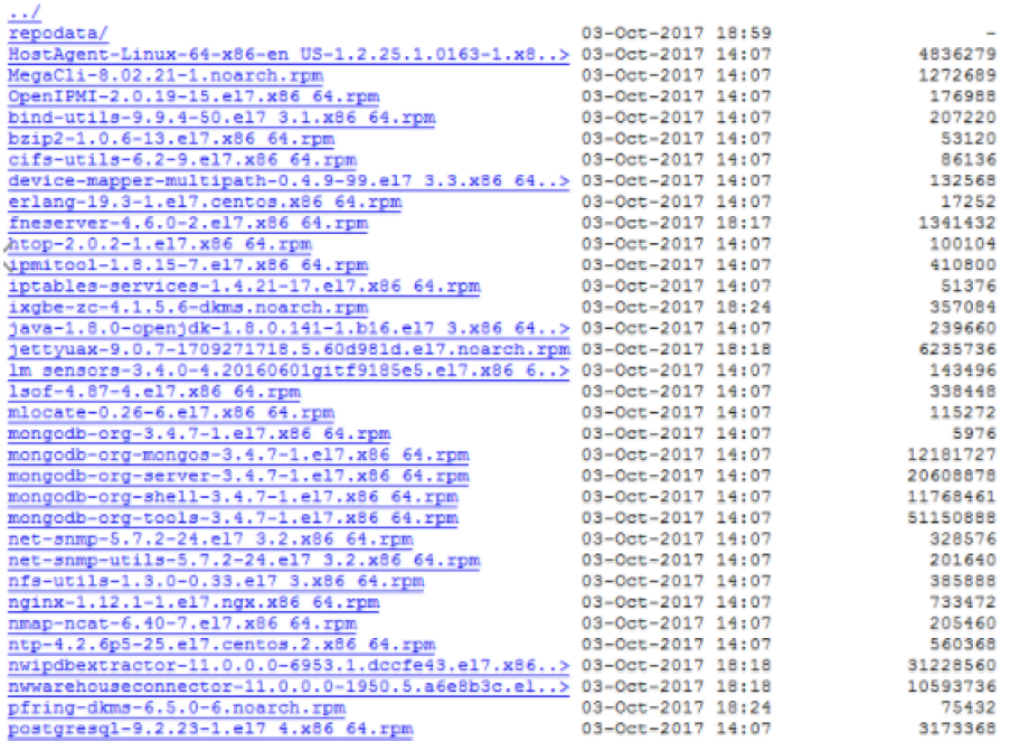


../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

2. `RSA-11.1.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`.

   ```
   unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
   ```

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



../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

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>/11.1.0.0/OS/other`

ii. `unzip nw-azure-11.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.1.0.0/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 11.1.0.0 Setup-Programms (`nwsetup-tui`).

Revisionsverlauf

Version	Datum	Beschreibung	Verfasser
1,0	08. März 2018	Betriebsfreigabe (Release to Operations, RTO)	IDD
1.1	12. März 2017	Änderung, die zu Beginn der Aktualisierungsaufgaben bei einem externen Repository beachtet werden soll.	IDD
1.2	12. April 2018	„Aufgabe 4: Sicherstellen, dass `deploy_admin`-Benutzeranmeldedaten nach wie vor gültig (nicht abgelaufen) sind“ wurde zu den Aufgaben zur Vorbereitung der Aktualisierung hinzugefügt.	IDD