RSA NETWITNESS® SUITE

Versionshinweise

für Version 11.1.0.1

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

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Inhalt

Einführung **7**

Build-Nummern **8**

Neuheiten **9**

Endpoint Insights 9

NetWitness Investigate 9

Update-Anleitung **10**

Aufgaben bei der Aktualisierung 10

Onlinemethode (Verbindung mit Live-Services): Aktualisieren mithilfe der NetWitness-Benutzeroberfläche 10

Voraussetzungen 10

Verfahren 11

Offlinemethode (keine Verbindung mit Live-Services): Aktualisieren mithilfe der Befehlszeilenoberfläche 12

Voraussetzungen 12

Verfahren 12

Anweisungen für Aktualisierung des externen Repository über die CLI 13

Aufgaben nach der Aktualisierung 14

Aufgabe 1 (optional): Verschieben der benutzerdefinierten Zertifikate 14

Aufgabe 2 (bedingungsabhängig): Neukonfigurieren der PAM-Radius-Authentifizierung 14

Aufgabe 3: Neustart des Respond-Servers 15

Behobene Probleme **16**

Serverkorrekturen 16

Problembehebungen in Investigate 16

Korrekturen für Endpoint Insights 17

Korrekturen für Telemetrie 17

Korrekturen für Respond 17

Context Hub-Korrekturen 17

Bekannte Probleme **19**

Upgrade 19

Endpoint Insights 21

Produktdokumentation **23**

Kontaktieren des Kundendienstes **24**

Vorbereitung zum Kontaktieren des Kundendienstes 24

Revisionsverlauf **25**

Einführung

In diesem Dokument sind Verbesserungen und Korrekturen in RSA NetWitness Suite 11.1.0.1 aufgeführt. Lesen Sie dieses Dokument vor der Bereitstellung von oder der Aktualisierung auf RSA NetWitness Suite 11.1.0.1.

- Build-Nummern
- Neuheiten
- Update-Anleitung
- Behobene Probleme
- Bekannte Probleme
- Produktdokumentation
- Kontaktieren des Kundendienstes
- Revisionsverlauf

Build-Nummern

In der folgenden Tabelle sind die Build-Nummern für die verschiedenen Komponenten von RSA NetWitness Suite 11.1.0.1 aufgeführt.

Komponente	Versionsnummer
NetWitness Suite Web Server	11.1.0.1-180413052407
NetWitness Suite Decoder	11.1.0.1-9043
NetWitness Suite Concentrator	11.1.0.1-9043
NetWitness Suite Broker	11.1.0.1-9043
NetWitness Suite Log Decoder	11.1.0.1-9043
NetWitness Suite Archiver (Workbench)	11.1.0.1-9043
NetWitness Suite Event Stream Analysis Server	11.1.0.1-436
NetWitness Suite Appliance	11.1.0.1-9043
NetWitness Suite Archiver	11.1.0.1-9043
NetWitness Suite Cloud Gateway Server	11.1.0.1-180413152801
NetWitness Suite Concentrator	11.1.0.1-9043
NetWitness Suite-Konsole	11.1.0.1-9043
NetWitness Suite Endpoint Agents	11.1.0.1-1804190837
NetWitness Suite Endpoint Server	11.1.0.1-180419015718
NetWitness Suite Investigate Server	11.1.0.1-180417084126
NetWitness Suite Legacy Web Server	11.1.0.1-180413052407
NetWitness Suite Log Player	11.1.0.1-9043
NetWitness Suite Orchestration Server	11.1.0.1-180323104408
NetWitness Suite Respond Server	11.1.0.1-180322090443
NetWitness Suite SDK	11.1.0.1-9043

Neuheiten

Die RSA NetWitness Suite 11.1.0.1-Patchversion stellt Korrekturen für 11.1.0.0 bereit. In diesem Dokument werden die Verbesserungen und Korrekturen beschrieben, die in dieser Version enthalten sind.

Endpoint Insights

Metazuordnung für Endpunkte. Es wurden APIs eingeführt, um die Standardmetazuordnung für Endpunkte anzuzeigen oder die Metazuordnung für Endpunkte, `get-default, get-custom, set-custom`, zu ändern. Weitere Informationen zu diesen APIs finden Sie im *Endpoint Insights – Konfigurationsleitfaden*.

NetWitness Investigate

Sortierte Serviceliste in der Ansicht „Ereignisanalyse“. Services sind im Drop-down-Menü für Services in der Ansicht „Ereignisanalyse“ alphabetisch sortiert.

Operatoranzeige beim Erstellen einer Abfrage in der Ereignisanalyse. Wenn Analysten in der Ansicht „Ereignisanalyse“ Filter zu einer Abfrage hinzufügen, enthält die automatisch vervollständigte Drop-down-Liste der Operatoren eine Stoppuhranzeige, um Vorgänge zu markieren, deren Ausführung mehr Zeit in Anspruch nimmt. Weitere Informationen zu diesen Funktionen finden Sie im *NetWitness Investigate – Benutzerhandbuch*.

Update-Anleitung

Sie müssen die Informationen lesen und diese Verfahren für die Aktualisierung von RSA NetWitness Suite Version 11.1.0.1 befolgen.

Die folgenden Aktualisierungspfade werden für RSA NetWitness Suite 11.1.0.1 unterstützt:

- RSA NetWitness Suite 11.1.0.0 auf 11.1.0.1

Für 11.1.0.0 unterstützte Aktualisierungspfade finden Sie im *Leitfaden für die Aktualisierung von Version 11.0.x auf 11.1*.

Sie können den 11.1.0.1-Patch mit einer der folgenden Optionen aktualisieren:

- Wenn der NetWitness-Server über eine Internetverbindung zu Live-Services verfügt, kann die NetWitness Suite-Benutzeroberfläche verwendet werden, um den Patch anzuwenden.
- Wenn keine Internetverbindung vom NetWitness-Server zu Live-Services besteht, kann die Befehlszeilenoberfläche (CLI) verwendet werden, um den Patch anzuwenden.

Aufgaben bei der Aktualisierung

Sie können eine der folgenden Aktualisierungsmethoden basierend auf Ihrer Internetverbindung auswählen.

Onlinemethode (Verbindung mit Live-Services): Aktualisieren mithilfe der NetWitness-Benutzeroberfläche

Sie können diese Methode verwenden, wenn der NetWitness-Server mit Live-Services verbunden ist, und können das Paket abrufen.

Hinweis: Wenn der NetWitness-Server keinen Zugriff auf Live-Services hat, verwenden Sie die Offlinemethode (keine Verbindung mit Live-Services): Aktualisieren mithilfe der Befehlszeilenoberfläche .

Voraussetzungen

Achten Sie auf Folgendes:

1. Die Option „Informationen über neue Aktualisierungen täglich automatisch herunterladen“ ist aktiviert und wird in **ADMIN** > **System** > **Aktualisierungen** angewendet.
2. Navigieren Sie zu **ADMIN** > **Hosts** > **Aktualisierung** > **Nach Updates suchen**, um nach Updates zu suchen. Auf der Seite „Host“ wird der Status **Aktualisierung verfügbar** angezeigt.
3. 11.1.0.1 ist in der Spalte „Update-Version“ verfügbar.

Hinweis: Wenn Sie über benutzerdefinierte Zertifikate verfügen, verschieben Sie alle benutzerdefinierten Zertifikate aus dem Verzeichnis `/etc/pki/nw/trust/import/` in `/root/cert`. Um die Zertifikate zu verschieben, gehen Sie wie folgt vor:
1.) `mkdir /root/cert.`
2.) `mv /etc/pki/nw/trust/import/* /root/cert.`

Verfahren

1. Navigieren Sie zu **ADMIN** > **Hosts**.
2. Wählen Sie den NetWitness-Serverhost (nw-server) aus.
3. Überprüfen Sie die neuesten Aktualisierungen.

4. Aktualisierung verfügbar wird in der Spalte **Status** angezeigt, wenn für die ausgewählten Hosts im lokalen Update-Repository ein Versionsupdate vorhanden ist.
5. Wählen Sie **11.1.0.1** aus der Spalte **Update-Version** aus.
   Gehen Sie in folgenden Fällen wie folgt vor:
   - 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.
   - 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**.
7. Klicken Sie auf **Update beginnen**.
8. Klicken Sie auf **Host neu starten**.
9. Wiederholen Sie Schritte 6 bis 8 für andere Hosts.

Hinweis: Sie können erst mehrere Hosts zum gleichzeitigen Aktualisieren auswählen, nachdem Sie den NetWitness-Adminserver aktualisiert und neu gestartet haben. Alle ESA-, Endpoint Insights- und Malware-Hosts müssen auf dieselbe Version wie die des NW-Adminservers oder NetWitness-Adminservers aktualisiert werden.

Hinweis: Nicht alle Komponenten wurden für 11.1.0.1 geändert. Nachdem Sie die Aktualisierungsschritte durchgeführt haben, ist es deshalb normal, dass einige Komponenten mit verschiedenen Versionsnummern angezeigt werden. Eine Liste der Komponenten, die für diese Version aktualisiert wurden, finden Sie unter Build-Nummern.

Offlinemethode (keine Verbindung mit Live-Services): Aktualisieren mithilfe der Befehlszeilenoberfläche

Sie können diese Methode verwenden, wenn der NetWitness-Server nicht mit Live-Services verbunden ist.

Voraussetzungen

Achten Sie auf Folgendes:

- Sie haben die folgende Datei, die alle NetWitness Suite 11.1.0.1-Dateien enthält, über „RSA-Link (https://community.rsa.com/) > NetWitness Suite > RSA NetWitness Logs and Packets Downloads“ in ein lokales Verzeichnis heruntergeladen:
  `netwitness-11.1.0.1.zip`

Verfahren

Sie müssen die Schritte zur Aktualisierung für NW-Adminserver und für Komponentenserver durchführen.

Hinweis: Wenn Sie die Befehle von der PDF in das Linux SSH-Terminal kopieren und einfügen, funktionieren die Zeichen nicht. Es wird empfohlen, die Befehle einzugeben.

1. Stellen Sie 11.1.0.1 bereit, indem Sie ein Verzeichnis auf dem NetWitness-Server unter `/tmp/upgrade/11.1.0.1` erstellen und das ZIP-Paket extrahieren.
   ```
   unzip netwitness-11.1.0.1.zip -d /tmp/upgrade/11.1.0.1
   ```

   Hinweis: Wenn Sie das ZIP-Paket in das erstellte Bereitstellungsverzeichnis kopiert haben, um es zu entpacken, stellen Sie sicher, dass Sie die anfängliche ZIP-Datei, die Sie in den Bereitstellungsspeicherort kopiert haben, löschen, nachdem Sie sie extrahiert haben.

2. Initialisieren Sie die Aktualisierung mit dem folgenden Befehl:
   ```
   upgrade-cli-client --init --version 11.1.0.1 --stage-dir /tmp/upgrade
   ```
3. Aktualisieren Sie den NetWitness-Server mit dem folgenden Befehl:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.1.0.1
   ```
4. Wenn die Aktualisierung des Komponentenhosts erfolgreich ist, starten Sie den Host von der NetWitness-Benutzeroberfläche neu.

5. Wiederholen Sie die Schritte 3 und 4 für jeden Komponentenhost und ändern Sie dabei die IP-Adresse auf die des Komponentenhosts, der aktualisiert wird.

Hinweis: Sie können die Versionen aller Hosts mit dem Befehl `upgrade-cli-client --list` auf dem NetWitness-Server überprüfen. Wenn Sie den Hilfeinhalt von `upgrade-cli-client` anzeigen möchten, verwenden Sie den Befehl `upgrade-cli-client --help`.

Hinweis: Wenn während des Aktualisierungsprozesses der folgende Fehler angezeigt wird:
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
, wird der Patch ordnungsgemäß installiert. Es ist keine Aktion erforderlich. Wenn beim Aktualisieren eines Hosts auf eine neue Version weitere Fehler auftreten, wenden Sie sich an den Kundensupport (Kontaktieren des Kundendienstes).

Anweisungen für Aktualisierung des externen Repository über die CLI

Hinweis: Das einzurichtende externe Repository sollte ein 11.1.0.1-Repository sein, das unter demselben Verzeichnis wie in 11.1.0.0 festgelegt ist.

1. Stellen Sie 11.1.0.1 bereit, indem Sie ein Verzeichnis auf dem NetWitness-Server unter `/tmp/upgrade/11.1.0.1` erstellen und das ZIP-Paket extrahieren.
   ```
   unzip netwitness-11.1.0.1.zip -d /tmp/upgrade/11.1.0.1
   ```

   Hinweis: Wenn Sie das ZIP-Paket in das erstellte Bereitstellungsverzeichnis kopiert haben, um es zu entpacken, stellen Sie sicher, dass Sie die anfängliche ZIP-Datei, die Sie in den Bereitstellungsspeicherort kopiert haben, löschen, nachdem Sie sie extrahiert haben.

2. Initialisieren Sie die Aktualisierung mit dem folgenden Befehl:
   ```
   upgrade-cli-client --init --version 11.1.0.1 --stage-dir /tmp/upgrade
   ```
3. Aktualisieren Sie den NetWitness-Server mit dem folgenden Befehl:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version
   11.1.0.1
   ```
4. Wenn die Aktualisierung des Komponentenhosts erfolgreich ist, starten Sie den Host von der NetWitness-Benutzeroberfläche neu.
5. Wiederholen Sie die Schritte 3 und 4 für jeden Komponentenhost und ändern Sie dabei die IP-Adresse auf die des Komponentenhosts, der aktualisiert wird.

Hinweis: Sie können die Versionen aller Hosts mit dem Befehl `upgrade-cli-client --list` auf dem NetWitness-Server überprüfen. Wenn Sie den Hilfeinhalt von `upgrade-cli-client` anzeigen möchten, verwenden Sie den Befehl `upgrade-cli-client --help`.

Hinweis: Wenn während des Aktualisierungsprozesses der folgende Fehler angezeigt wird:
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
, wird der Patch ordnungsgemäß installiert. Es ist keine Aktion erforderlich. Wenn beim Aktualisieren eines Hosts auf eine neue Version weitere Fehler auftreten, wenden Sie sich an den Kundensupport (Kontaktieren des Kundendienstes).

Aufgaben nach der Aktualisierung

Aufgabe 1 (optional): Verschieben der benutzerdefinierten Zertifikate

Verschieben Sie die benutzerdefinierten Zertifikate aus dem externen Verzeichnis in das Verzeichnis `/etc/pki/nw/trust/import`.

Aufgabe 2 (bedingungsabhängig): Neukonfigurieren der PAM-Radius-Authentifizierung

Wenn Sie die PAM-Radius-Authentifizierung in 11.1.x.x mit dem `pam_radius`-Paket konfiguriert haben, müssen Sie sie in 11.1.0.1 mit dem `pam_radius_auth`-Paket neu konfigurieren.

Sie müssen die unten stehenden Befehle auf dem NW-Server ausführen, auf dem sich der Admin-Server befindet.

Hinweis: Wenn Sie `pam_radius` in 11.x.x.x konfiguriert haben, führen Sie die unten stehenden Schritte aus, um die vorhandene Version zu deinstallieren, oder fahren Sie mit Schritt 2 fort.

Schritt 1: Überprüfen der vorhandenen Seite und Deinstallieren der vorhandenen `pam_radius`

```
rpm -qi |grep pam_radius
yum erase pam_radius
```

Schritt 2: Führen Sie für die Installation des `pam_radius_auth` -Pakets den folgenden Befehl aus:

```
yum install pam_radius_auth
```

Schritt 3: Bearbeiten Sie die RADIUS-Konfigurationsdatei `/etc/raddb/server` wie folgt und fügen Sie die Konfigurationen für dem Radius-Server hinzu:

```
# server[:port] shared_secret timeout (s)
```

```
server secret 3
```

Beispiel: 111.222.33.44 secret 1

Schritt 4: Bearbeiten Sie die NetWitness-Server-PAM-Konfigurationsdatei `/etc/pam.d/securityanalytics`, um die folgende Zeile hinzuzufügen. Wenn die Datei nicht vorhanden ist, erstellen Sie sie und fügen Sie die folgende Zeile hinzu:

```
auth sufficient pam_radius_auth.so
```

Schritt 5: Stellen Sie die Schreibberechtigung für `/etc/raddb/server`-Dateien mit dem folgenden Befehl bereit.

```
chown netwitness:netwitness /etc/raddb/server
```

Schritt 6: Führen Sie zum Kopieren der `pam_radius_auth`-Bibliothek den folgenden Befehl aus:

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```

Schritt 7: Führen den folgenden Befehl aus, um den Jetty-Server nach Vornehmen von Änderungen an `pam_radius_auth`-Konfigurationen neu zu starten.

```
systemctl restart jetty
```

Aufgabe 3: Neustart des Respond-Servers

Starten Sie den Respond-Server neu:

```
systemctl restart rsa-nw-respond-server
```

Behobene Probleme

In diesem Abschnitt werden die Probleme aufgeführt, die seit der letzten -Hauptversion behoben wurden.

Serverkorrekturen

Rückverfolgungsnummer	Beschreibung
ASOC-50835	Nach der Aktualisierung fehlt der Integrationsserverservice in der Benutzeroberfläche.

Problembehebungen in Investigate

Rückverfolgungsnummer	Beschreibung
ASOC-50771	Wenn Sie über die Ansicht „Ereignisse“ zur Ereignisanalyse wechseln, entweder durch Klicken auf den Link „Ereignisanalyse“ oder durch Klicken mit der rechten Maustaste auf eines der Ereignisse, funktionieren die Optionen im Kontextmenü für Metawerte nicht.
ASOC-49854	Der Service wird unendlich geladen.
ASOC-51011	Die Spaltengruppen und Metagruppen RSA Endpoint Analysis, RSA Outbound SSL/TLS und RSA Outbound HTTP werden nach einem Upgrade von 10.6.5 auf 11.x nicht erstellt.
ASOC-48710	Die Meldung „Unerwarteter Fehler ist aufgetreten“ wird beim Zugriff auf entfernte oder gelöschte Sitzungen angezeigt.
ASOC-50924	Die direkte Navigation zu Ereignisanalyse von Endpoint wird nur für IPv4 unterstützt.
ASOC-50712	Metaentitäten können bei deaktivierter Option „Optimieren des Ladens der Seite ‚Investigation‘“ nicht zu einer benutzerdefinierten Spaltengruppe hinzugefügt werden.

Korrekturen für Endpoint Insights

Rückverfolgungsnummer	Beschreibung
ASOC-49846	Es ist keine Option zum Deaktivieren der Protokollsammlung in Windows-Agent vorhanden.
ASOC-49957	Eine Warnmeldung wurde in Protokolle (/var/log/messages) geschrieben. Diese Meldung wurde jetzt entfernt.
ASOC-50782	In 11.1.0.1 wurden die Paketnamen für das Linux-Installationsprogramm geändert von: • nwe-agent.rpm to nwe-agent.i686.rpm für Linux 32-Bit. • nwe-agent(64-bit).rpm to nwe-agent.x86_64.rpm für Linux 64-Bit.
ASOC-50162	Die Endpoint-Metadatenintegration wurde aktualisiert, sodass die Zuordnungen für die Metaschlüssel besser an Metadaten ausgerichtet ist, die aus Protokollen und Paketen erzeugt werden Metadaten.

Korrekturen für Telemetrie

Rückverfolgungsnummer	Beschreibung
ASOC-50740	Die Telemetrie-JSON-Datei wurde mit Kontozuordnungsdetails auf Servicelevеln wie Decoder, Log Decoder und Malware aktualisiert.

Korrekturen für Respond

Rückverfolgungsnummer	Beschreibung
ASOC-51133	Respond verarbeitet eine benachrichtigungsbezogene Last nicht ordnungsgemäß und stürzt ab.

Context Hub-Korrekturen

Rückverfolgungsnummer	Beschreibung

ASOC-51110	Eine ESA-Regel mit einer CH-Liste wurde beim Neustart des Systems deaktiviert.
ASOC-51069	Eine ESA-Regel, die einer großen Context Hub-Liste zugeordnet ist, kann nicht bereitgestellt werden.

Bekannte Probleme

In diesem Abschnitt werden Probleme beschrieben, die in dieser Version fortbestehen. Sofern ein Workaround oder eine Problembehebung verfügbar ist, werden ausführliche Anmerkungen bzw. Verweise eingefügt.

Hinweis: Die bekannten Probleme der früheren Versionen von 11.1.0.0 sind möglicherweise in den Service Packs behoben. Weitere Informationen finden Sie im entsprechenden Service Pack oder den Patchversionshinweisen, die auf RSA Link verfügbar sind: https://community.rsa.com/.

Upgrade

Die folgenden bekannten Probleme treten während eines Upgrades von Version 11.1.0.x auf:

Endpunkt-Incidents werden nicht erstellt.

Rückverfolgungsnummer: ASOC-51480

Problem: Endpunktereignisse mit einer Quell-IP funktionieren ordnungsgemäß, aber Endpunktereignisse mit einer Detektor-IP werden nicht von der Endpunkt-Incident-Regel aggregiert und erstellen keine Incidents. In NetWitness Suite 11.1 wurde das „Gruppieren nach“-Feld der Incident-Regel „Warnmeldungen mit hohem Risiko: NetWitness Endpoint“ von „Risikowert“ in „Quell-IP-Adresse“ geändert.

Workaround: Für Upgrades von 10.6.x to 11.1:

1. Navigieren Sie zu **KONFIGURIEREN** > **Incident-Regeln**. Die Ansicht „Incident-Regelliste“ wird angezeigt.
2. Klicken Sie auf den Link im Feld **Name** der Incident-Regel **Warnmeldungen mit hohem Risiko: NetWitness Endpoint**, um sie zu bearbeiten.
3. Ändern Sie den Wert für das Feld **Gruppieren nach** in **Risikowert**.

Bei Neuinstallationen:

1. Navigieren Sie zu **KONFIGURIEREN** > **Incident-Regeln**. Die Ansicht „Incident-Regelliste“ wird angezeigt.
2. Klicken Sie auf den Link im Feld **Name** der Incident-Regel **Warnmeldungen mit hohem Risiko: NetWitness Endpoint**, um sie zu bearbeiten.
3. Ändern Sie den Wert des Felds **Gruppieren nach** in **Risikowert** oder einen beliebigen anderen „Gruppieren nach“-Feldwert.

Doppelte Warnmeldungen in Respond

Rückverfolgungsnummer: ASOC-50994

Problem: Doppelte Warnmeldungen in Respond werden aus bestimmten Quellen wie der Reporting Engine beobachtet.

Workaround: Gehen Sie folgendermaßen vor, um veraltete Verbundaustauschvorgänge zu löschen, die zu doppelten Warnmeldungen in Respond führen können:

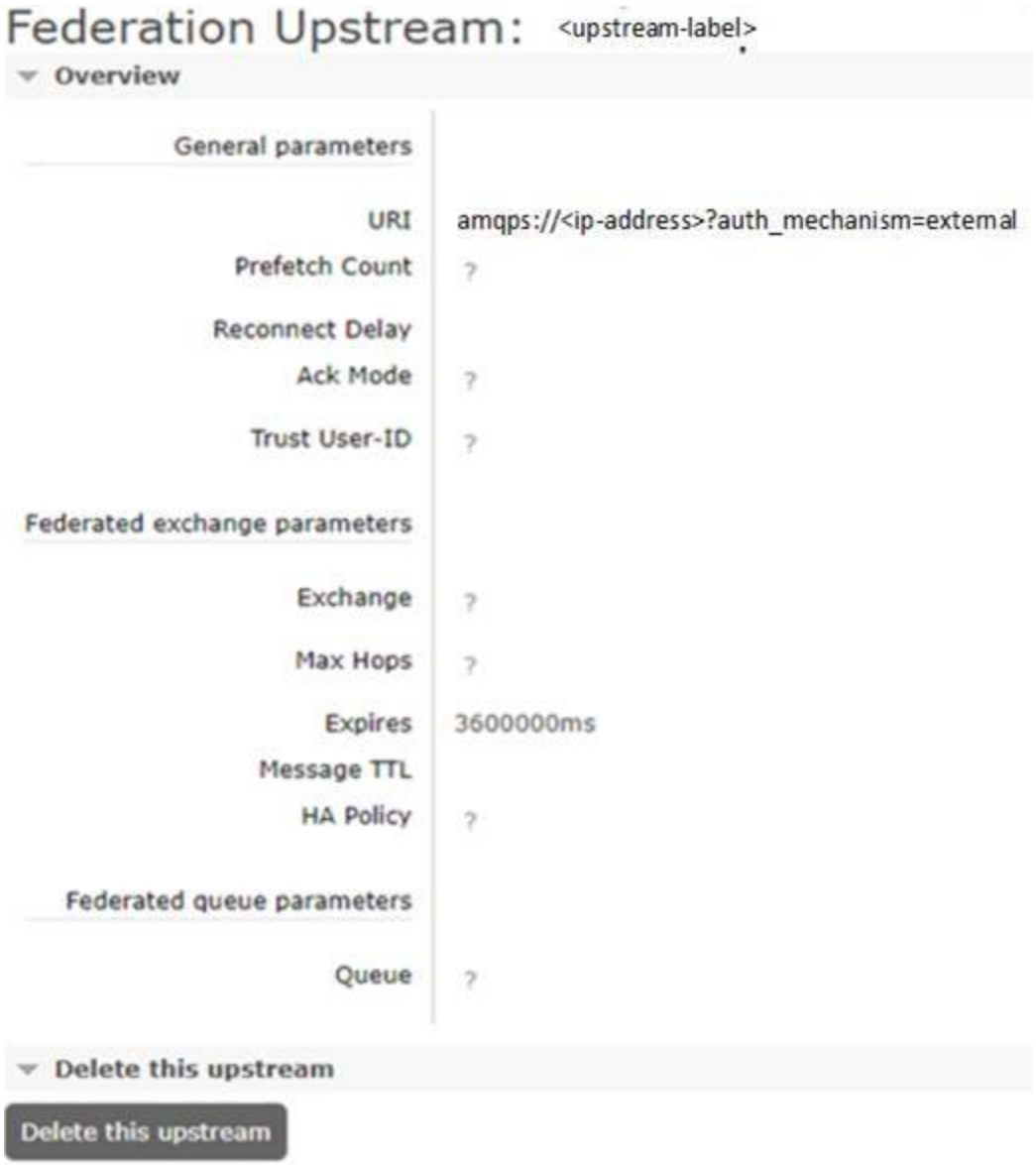
1. Melden Sie sich unter https://<adminServerIP>:15671/RabbitMQ-Cluster mit den folgenden Anmeldedaten an.

```
username: deploy_admin
password: <deployment-password-used-during-NW-Server-host-11.x-setup>
```

2. Navigieren Sie zu **Admin** > **Federation Upstream**.
3. Wählen Sie den URI mit der **NW-Server-Host-IP-Adresse** aus. Die Ansicht **Federation Upstream** wird angezeigt.
4. Stellen Sie sicher, dass der URI dem folgenden Wert ähnelt.

```
amqps : // <adminServerIP>?auth_mechanism=external
```

5. Klicken Sie auf **Upstream löschen**, um den URI zu löschen.



Endpoint Insights

Nach der Agent-Aktualisierung wird die Agent-Version nicht in der Benutzeroberfläche angezeigt.

Rückverfolgungsnummer: ASOC-52761

Problem: Wenn Sie die Agent-Version von 11.1 auf 11.1.0.1 aktualisieren, wird in der Ansicht „Hosts“ 11.1 als Agent-Version angezeigt.

Workaround: Wählen Sie in der Ansicht **Untersuchen** > **Hosts** den Host aus, auf dem Sie die neueste Version des Agent installiert haben, und klicken Sie auf **Scan starten**. Der Agent-Version wird auf 11.1.0.1 aktualisiert.

Protokolle können nicht auf 6514 weitergeleitet werden, wenn nur TLS 1.2 im Log Decoder aktiviert ist.

Rückverfolgungsnummer: ASOC-52761

Problem: Wenn im Log Decoder `/sys/config/ssl.context.options` auf `SSL_OP_NO_SSLv2,SSL_OP_NO_SSLv3,SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1` festgelegt ist und nur TLS 1.2 Protokolle akzeptieren darf, funktioniert die Protokollweiterleitung nicht, wenn die Weiterleitung an 6514 von Agents erfolgt, die in Windows 7 SP1 und Windows 2008 bereitgestellt werden.

Workaround: Informationen zum Aktivieren von TLS 1.2 finden Sie im folgenden Artikel: https://support.microsoft.com/de-de/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows.

Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

Dokument	Speicherort
RSA NetWitness Suite 11.1.0.0 – Onlinedokumentation	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 – Upgradeanweisungen	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 – Upgradecheckliste	https://community.rsa.com/community/products/netwitness/111
Leitfaden zur Hardwarekonfiguration von RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA-Inhalte für RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

Kontaktieren des Kundendienstes

Verwenden Sie die folgenden Kontaktinformationen, wenn Sie Fragen haben oder Unterstützung benötigen.

RSA SecurCare	https://knowledge.rsasecurity.com
Tel.	1-800-995-5095, Option 3
Internationale Kontakte	http://germany.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/docs/DOC-1294
Basis-Support	Der technische Support für Ihre technischen Probleme ist von montags bis freitags von 08:00 bis 17:00 Uhr Ortszeit erreichbar.
Enhanced Support	Der technische Support ist nur für Fehler des Schweregrads 1 und 2 telefonisch an 365 Tagen im Jahr rund um die Uhr verfügbar.

Vorbereitung zum Kontaktieren des Kundendienstes

Wenn Sie sich mit dem Kundendienst in Verbindung setzen, sollten Sie sich an Ihrem Computer befinden. Halten Sie die folgenden Informationen bereit:

- Die Versionsnummer des verwendeten RSA NetWitness Suite-Produkts oder der Appliance
- Typ der verwendeten Hardware

Revisionsverlauf

Version	Datum	Beschreibung
0,1	17. April	RTO-Entwurf