RSA NETWITNESS® SUITE

RSA Archer-Integrationsleitfaden

für Version 11.0

Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Februar 2018

Inhalt

Integration in RSA Archer

Administratoren können RSA NetWitness Suite in RSA NetWitness Security Operations (SecOps) Manager integrieren, um Warnmeldungen und Incidents von NetWitness Suite zu Archer für Incident Management und Korrekturen zu senden. Dieser Leitfaden enthält einen allgemeinen Workflow für das Konfigurieren dieser Integration.

In der folgenden Tabelle werden die NetWitness Suite 11.0 Optionen für die Integration in NetWitness SecOps Manager Version 1.3.1.2 aufgeführt.

NetWitness SecOps Manager Version	NetWitness Suite 11.0 Integration	Referenz
1.3.1.2	Event Stream Analysis (ESA)	Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Event Stream Analysis für die Integration in Archer SecOps“.
1.3.1.2	Reporting Engine (RE)	Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Reporting Engine für die Integration in Archer SecOps“.
1.3.1.2	Respond	Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Respond für die Integration in Archer SecOps 1.3.1.2“.
1.3.1.2	Archer-Feeds	Weitere Informationen finden Sie im Abschnitt „RSA Archer-Feeds“.

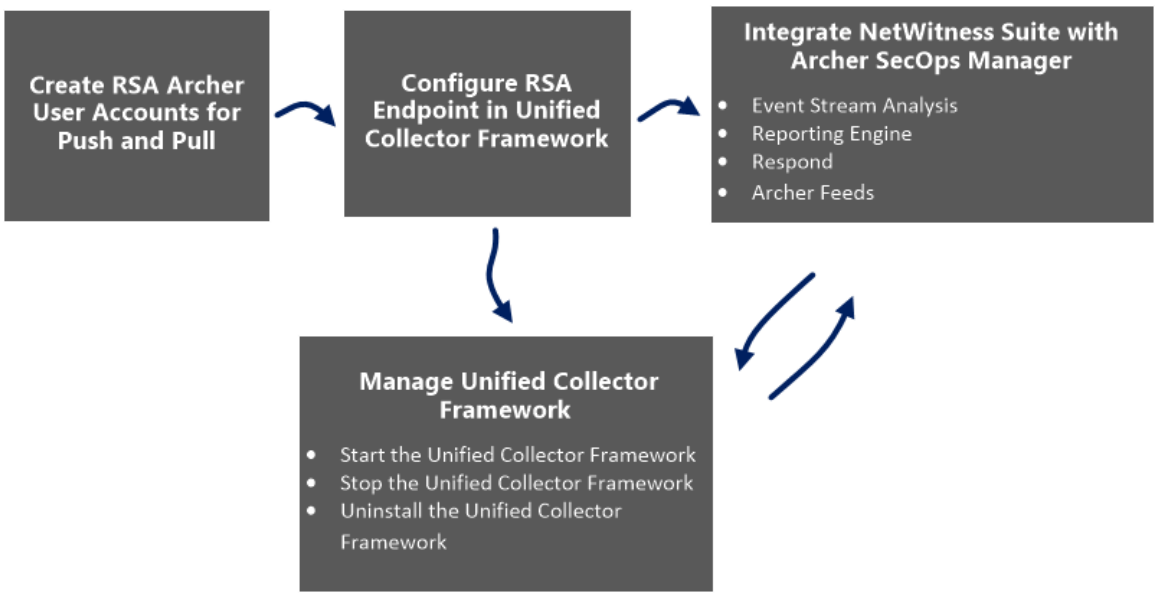
Konfigurieren von NetWitness für das Arbeiten mit Archer

Mit der RSA NetWitness SecOps Manager-Lösung können Sie alle verwertbaren Sicherheitswarnungen zusammenführen. Damit können Sie bei der Reaktion auf Incidents und dem SOC-Management effektiver, proaktiver und zielgerichteter arbeiten. Weitere Informationen zu den RSA NetWitness SecOps-Funktionen finden Sie in der RSA Archer-Dokumentation in der RSA Archer-Community oder in der RSA Archer Exchange-Community.

Die Version von RSA Archer bestimmt, wie NetWitness Suite integriert wird. Informationen zu den unterstützten Archer-Plattformen finden Sie im *SecOps-Installationshandbuch*.

Sie können NetWitness SecOps Manager 1.3.1.2 in NetWitness Suite integrieren, indem Sie das RSA UCF (Unified Collector Framework) verwenden, das den Integrationsservice Security Anlaytics Incident Management (IM) sowie den Service SecOps Watchdog umfasst.

Diese Abbildung zeigt den Ablauf der Integration von NetWitness Suite 11.0 Integration in NetWitness SecOps Manager 1.3.1.2.



Erstellen von RSA Archer-Benutzerkonten für Push- und Pull

Sie müssen ein Benutzerkonto für den Webserviceclient erstellen, um Daten an die RSA Archer GRC-Plattform zu übertragen.

Es sind zwei RSA Archer-Benutzerkonten erforderlich, um Konflikte beim Senden und Empfangen von Daten von RSA NetWitness Suite zu vermeiden.

Um ein Benutzerkonto für Push und Pull zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der RSA Archer-Benutzeroberfläche auf **Administration** > **Zugriffskontrolle** > **Benutzer** > **Neue hinzufügen**.
2. Geben Sie in den Feldern **Vorname** und **Nachname** einen Namen ein, der angibt, dass das UCF dieses Konto für den Daten-Push-Vorgang in RSA Archer GRC verwendet. Beispiel: UCF-Benutzer, Push.

   Hinweis: Geben Sie beim Konfigurieren des Pull-Kontos einen Namen ein, der angibt, dass das UCF dieses Konto für Daten-Pull-Vorgänge von RSA Archer GRC verwendet. Beispiel: UCF-Benutzer, Pull.
3. (Optional) Geben Sie einen Benutzernamen für das neue Benutzerkonto ein.

   Hinweis: Wenn Sie keinen Benutzernamen angeben, wird der Benutzername von der RSA Archer GRC-Plattform aus dem ersten und letzten Namen erstellt, die eingegeben werden, wenn Sie das neue Benutzerkonto speichern.
4. Geben Sie im Abschnitt **Kontaktinformationen** im Feld **E-Mail** eine E-Mail-Adresse ein, die dem neuen Benutzerkonto zugeordnet werden soll
5. Ändern Sie im Bereich **Lokalisierung** die Zeitzone in „Koordinierte Weltzeit (UTC)“.

   Hinweis: Das UCF verwendet UTC-Zeit als Basis für alle zeitbezogenen Berechnungen.
6. Geben Sie im Abschnitt **Kontowartung** ein neues Passwort für das neue Benutzerkonto ein und bestätigen Sie es.

   Hinweis: Notieren Sie den Benutzernamen und das Passwort für das neue Benutzerkonto, das Sie soeben erstellt haben. Sie müssen diese Anmeldedaten eingeben, wenn Sie das UCF für die Kommunikation mit der RSA Archer GRC-Plattform über den Webserviceclient einrichten.
7. Deaktivieren Sie die Option **Kennwortänderung bei der nächsten Anmeldung erzwingen**.
8. Wählen Sie im Feld **Sicherheitsparameter** den Sicherheitsparameter aus, den Sie für diesen Benutzer verwenden möchten.

   Hinweis: Wenn Sie einen Standardsicherheitsparameter mit einem Passwortänderungsintervall von 90 Tagen zuweisen, müssen Sie auch das im SA IM Integration Service gespeicherte Passwort für das Benutzerkonto alle 90 Tage aktualisieren. Um dies zu vermeiden, können Sie optional einen neuen Sicherheitsparameter für das SA IM Integration Service-Benutzerkonto erstellen und das Passwortänderungsintervall auf den gemäß der Standards Ihres Unternehmens zulässigen Höchstwert festlegen.

9. Klicken Sie auf die Registerkarte **Gruppen** und führen Sie die folgenden Schritte aus:
   a. Klicken Sie im Bereich **Gruppen** auf **Abfrage**.
   b. Erweitern Sie im Fenster **Verfügbare Gruppen** den Punkt „Gruppen“.
   c. Scrollen Sie nach unten und wählen Sie „SOC: Lösungsadministrator“ und „EM: Schreibgeschützt“ aus.
   d. Klicken Sie auf **OK**.
10. Klicken Sie auf **Anwenden** und anschließend auf **Speichern**.
11. Wenn die Einstellungen für Sprache und Region des RSA Archer GRC-Systems auf einen anderen Wert als „Englisch – US“ festgelegt sind, führen Sie die folgenden Schritte aus:
   a. Öffnen Sie das soeben erstellte Benutzerkonto und wählen Sie im Bereich **Lokalisierung** im Feld „Gebietsschema“ die Option **Englisch (USA)** aus und klicken Sie auf **Speichern**.
   b. Öffnen Sie auf dem Windows-System, auf dem die RSA Archer GRC-Plattform gehostet wird, den Internetinformationsdienste-Manager (IIS).
   c. Blenden Sie den RSA Archer GRC-Standort ein, klicken Sie auf **.Net Globalisierung**, wählen Sie in den Feldern **Region** und **UI-Region** die Option **Englisch (USA)** aus und klicken Sie auf **Anwenden**.
   d. Starten Sie die RSA Archer GRC-Standort neu.
12. Wiederholen Sie die Schritte 1 bis 11, um ein zweites Benutzerkonto zu erstellen, mit dem das UCF Daten per Pull von RSA Archer GRC abrufen kann.

Konfigurieren von Endpunkten in RSA Unified Collector Framework

Endpunkte stellen die erforderlichen Verbindungsdetails bereit, damit das UCF die RSA NetWitness Suite- und RSA Archer GRC-Systeme erreichen kann.

Hinweis: Einige Endpunkte sind erforderlich, um verschiedene Integrationen verwenden zu können. Die folgende Liste enthält die obligatorischen Endpunkte.

Obligatorische Endpunkt-Integration

- Archer Push-Endpunkt
- Archer Pull-Endpunkt

- Modusauswahl: SecOps- oder Nicht-SecOps-Modus

Hinweis:
• Wenn der Modus „Nicht-SecOps“ aktiviert ist, werden Incidents in NetWitness Suite Respond anstelle von RSA Archer Security Operations Management verwaltet.
• Sie müssen den Port abhängig vom Protokoll (TCP, UDP oder sicheres TCP) konfigurieren.
• Stellen Sie sicher, dass der Name des Betreffs des Zertifikats für den RSA Archer GRC-Server dem Hostnamen entspricht.

Verfahren

1. Öffnen Sie den Verbindungsmanager auf dem UCF-System wie folgt:
   a. Öffnen Sie eine Eingabeaufforderung.
   b. `Wechseln Sie zum Verzeichnis <install_dir>\SA IM integration service\data-collector.`
   c. `Geben Sie Folgendes ein: runConnectionManager.bat`
2. Geben Sie im **Verbindungsmanager** den Wert **1** für „Endpunkt hinzuzufügen“ ein.
3. Fügen Sie wie folgt einen Endpunkt für Daten-Push-Vorgänge an RSA Archer Security Operations Management hinzu:
   a. Geben Sie die Zahl für Archer ein.

      Hinweis: SSL muss aktiviert sein, um die RSA Archer-Endpunkte hinzufügen zu können.

   b. Geben Sie als Name des Endpunkts **Push** ein.
   c. Geben Sie die URL des RSA Archer GRC-Systems ein.
   d. Geben Sie den Instanznamen des RSA Archer GRC-Systems ein.
   e. Geben Sie den Benutzernamen des Benutzerkontos ein, das Sie erstellt haben, um Daten per Push in das RSA Archer GRC-System zu übertragen.
   f. Geben Sie das Passwort für das Benutzerkonto ein, das Sie erstellt haben, um Daten per Push in das RSA Archer GRC-System zu übertragen, und bestätigen Sie das Passwort.
   g. Wenn Sie gefragt werden, ob dieses Konto für Pull-Vorgänge von Daten verwendet wird, geben Sie **False** ein.
4. Fügen Sie wie folgt einen Endpunkt für das Abrufen von Daten per Pull aus RSA Archer Security Operations Management hinzu:

a. Geben Sie die Zahl für Archer ein.

> **Hinweis:** SSL muss aktiviert sein, um die RSA Archer-Endpunkte hinzufügen zu können.

b. Geben Sie als Name des Endpunkts **Pull** ein.

c. Geben Sie die URL des RSA Archer GRC-Systems ein.

d. Geben Sie den Instanznamen des RSA Archer GRC-Systems ein.

e. Geben Sie den Benutzernamen des Benutzerkontos ein, das Sie erstellt haben, um Daten per Pull von dem RSA Archer GRC-System abzurufen.

f. Geben Sie das Passwort für das Benutzerkonto ein, das Sie erstellt haben, um Daten per Pull von dem RSA Archer-System abzurufen, und bestätigen Sie das Passwort.

g. Wenn Sie gefragt werden, ob dieses Konto für Pull-Vorgänge von Daten verwendet wird, geben Sie **True** ein.

5. Hinzufügen eines Endpunkts für RSA NetWitness Suite

- Für Reagieren

a. Geben Sie die Zahl für Security Analytics IM ein.

b. Geben Sie einen Namen für den Endpunkt ein.

c. Geben Sie die IP-Adresse des SA-Hosts ein.

d. Geben Sie als SA Messaging Port **5671** ein.

e. Geben Sie die Zielwarteschlange für Korrekturaufgaben ein. Wählen Sie dabei alle Prozesse aus, sowohl „Integration in RSA Archer“ als auch „IT-Helpdesk (Vorgänge)“.

f. So fügen Sie automatisch Zertifikate zum NetWitness Suite-Truststore hinzu:

i. Geben Sie **Ja** ein.

ii. Geben Sie den Benutzernamen und das Passwort für den NetWitness Suite-Host ein.

> **Hinweis:** Wenn ein Fehler angezeigt wird, dass der Zertifizierungsstellen-Truststore nicht festgelegt werden konnte, lesen Sie die Informationen unter Troubleshooting einer RSA Archer-Integration.

g. Wählen Sie im UCF-Verbindungsmanager wie folgt den Modus:

i. Geben Sie die Zahl für „Modusauswahl“ ein.

ii. Wählen Sie eine der folgenden Optionen:

- Incident-Workflow in RSA NetWitness Suite managen.
- Incident-Workflow ausschließlich in RSA Archer Security Operations Management managen

- Für Reporting Engine und Event Stream Analysis

a. Fügen Sie zum Verwenden von Integrationen von Drittanbietern den Syslog-Serverendpunkt wie folgt hinzu:

i. Geben Sie die Zahl für „Syslog-Serverendpunkt“ ein.

ii. Geben Sie Folgendes ein:

- Benutzerdefinierter Name
- Für SSL konfigurierte TCP-Portnummer

  Hinweis: Der Standardwert ist 1515. Wenn Sie den Syslog-Server in diesem Modus nicht hosten möchten, geben Sie **0** ein.

- TCP-Portnummer: Geben Sie den TCP-Port ein, wenn der Syslog-Client die Syslog-Meldung im TCP-Modus sendet.

  Hinweis: Der Standardwert ist 1514. Wenn Sie den Syslog-Server in diesem Modus nicht hosten möchten, geben Sie **0** ein.

- UDP-Portnummer: Geben Sie den UDP-Port ein, wenn der Syslog-Client die Syslog-Meldung im UDP-Modus sendet.

  Hinweis: Der Standardwert ist 514. Wenn Sie den Syslog-Server in diesem Modus nicht hosten möchten, geben Sie **0** ein.

Standardmäßig wird der Syslog-Server in den oben genannten drei Modi ausgeführt, es sei denn, er wird durch Eingabe von **0** deaktiviert.

b. Geben Sie zum Testen des Syslog-Clients die Zahl für „Syslog-Client testen“ ein. Verwenden Sie den Syslog-Testclient mit den Dateien aus `<install_dir>\SA IM integration service\config\mapping\test-files\`.

6. Geben Sie im Verbindungsmanager **5** ein, um jeden Endpunkt zu testen.

Integrieren von NetWitness Suite in Archer SecOps Manager

Sie müssen die Systemintegrationseinstellungen konfigurieren, um den Incident-Workflow in RSA NetWitness SecOps Manager zu managen.

Informationen zur Konfiguration von Systemintegrationseinstellungen für das Management von Incident-Workflows in RSA Archer Security Operations finden Sie im Thema „Konfigurieren von Integrationseinstellungen zur Verwaltung von Incidents in RSA Archer Security Operations“ im *NetWitness Respond – Benutzerhandbuch*.

RSA Unified Collector Framework

Sie können RSA NetWitness Suite in RSA Archer SecOps Manager 1.3.1.2 integrieren, indem Sie das RSA Unified Collector Framework (UCF) verwenden. Das RSA Unified Collector Framework (UCF) kann in alle unterstützten SIEM-Tools und die RSA NetWitness SecOps Manager-Lösung integriert werden. Wenn Sie RSA NetWitness Suite Respond integrieren, können Sie den Incident-Workflow in NetWitness Suite Respond managen und es Analysten ermöglichen, Korrekturaufgaben und offene Datenschutzverletzungen zur Verwaltung und Korrektur in die RSA Archer Security Operations Management-Lösung zu eskalieren. Und das Unified Collector Framework übermittelt Korrekturaufgaben (erstellt als Befunde) und/oder Datenschutzverletzungen.

Hinweis:
• Sie müssen in RSA NetWitness Suite und dem Unified Collector Framework dieselbe Option konfigurieren.
• Die Integration des RSA NetWitness Respond-Moduls in Reporting Engine oder in Event Stream Analysis kann zu in RSA Archer SecOps Manager erstellten duplizierten Ereignissen und Incidents führen.

UCF unterstützt mehrere Verbindungen von SIEM-Tools gleichzeitig, z. B. Unterstützung von NetWitness Suite Reporting Engine, HP ArcSight und NetWitness Suite Respond. Verschiedene Instanzen desselben SIEM-Tools werden jedoch nicht unterstützt, z. B. die gleichzeitige Verbindung von zwei NetWitness Suite-Servern mit dem gleichen UCF.

Voraussetzungen

- Installieren Sie das Paket „RSA_Archer_Security_Operations_Management“ auf Archer. Siehe RSA Archer-Dokumentation in der RSA Archer-Community oder in der Registerkarte „Content“ unter https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.
- Installieren Sie NetWitness SecOps Manager.
- Stellen Sie sicher, dass Sie NetWitness Suite 11.0 verwenden, da diese Version mit

NetWitness SecOps Manager 1.3.1.2 kompatibel ist.

- Stellen Sie sicher, dass Respond in RSA NetWitness Suite konfiguriert ist.

Mit dem RSA UCF (Unified Collector Framework) können Sie Ihr RSA Archer Security Operations Manager-System in die folgenden Anwendungen integrieren:

- NetWitness Suite Respond
- NetWitness Suite Reporting Engine
- NetWitness Suite Event Stream Analysis
- Archer-Feeds

Konfigurieren von Respond für die Integration in Archer SecOps

Um Respond für Archer SecOps zu konfigurieren, führen Sie in NetWitness Suite die folgenden Schritte aus:

Schritt 1: Auswählen des Modus für NetWitness Suite Respond

1. Wählen Sie **ADMIN > Services > Respond > Erkunden** aus.
2. Navigieren Sie zu `Respond/Aggregation/export`.
3. Legen Sie für das Feld `archer-secops-integration-enabled` die Option **True** fest.
4. Starten Sie den Respond-Service neu.

Schritt 2: Konfigurieren von NetWitness Suite Respond zum Weiterleiten von Warnmeldungen an das UCF

1. Navigieren Sie zu `C:\Program Files\RSA\SA IM integration service\cert-tool\certs` in der Secops Middleware-Box.
2. Kopieren Sie sowohl `keystore.cert.pem` als auch `rootcastore.cert.pem` aus dem Zertifikatordner (in den Importordner auf dem NW-Server).
   ```
   cp rootcastore.crt.pem /etc/pki/nw/trust/import

   cp keystore.crt.pem /etc/pki/nw/trust/import
   ```
3. SSH zu NW-Serverbox
   a. Führen Sie den Befehl „update-admin-node“ aus.
      ```
      orchestration-cli-client --update-admin-node
      ```
   b. Starten Sie den RabbitMQ-Service neu.
      ```
      service rabbitmq-server restart
      ```
   c. Erstellen Sie den Archer-Benutzer und legen Sie die Berechtigungen für den virtuellen

Host „/rsa/system“ fest.

```
rabbitmqctl add_user archer archer

rabbitmqctl clear_password archer

rabbitmqctl set_permissions -p /rsa/system archer ".*" ".*" ".*"
```

Schritt 3: Weiterleiten von Warnmeldung an NetWitness Suite Respond

- **Um NetWitness Suite Event Stream Analysis-Warnmeldungen an NetWitness Respond weiterzuleiten, führen Sie folgende Schritte aus:**
  a. Wählen Sie **ADMIN > Services > ESA** aus.
  b. Wählen Sie einen Event Stream Analysis-Service aus und klicken Sie auf > **Ansicht** > **Konfiguration**.
  c. Klicken Sie auf die Registerkarte **Erweitert**.
  d. Vergewissern Sie sich, dass das Kontrollkästchen **Warnmeldungen an Nachrichtenbus weiterleiten** standardmäßig ausgewählt ist. Falls nicht, aktivieren Sie das Kontrollkästchen **Warnmeldungen an Nachrichtenbus weiterleiten** und klicken Sie auf **Anwenden**.

- **Um NetWitness Suite Report Engine-Warnmeldungen an NetWitness Respond weiterzuleiten, führen Sie folgende Schritte aus:**
  a. Wählen Sie **ADMIN > Services > Reporting Engine** aus.
  b. Klicken Sie für den Reporting Engine-Service auf > **Ansicht** > **Konfiguration**.
  c. Klicken Sie auf die Registerkarte **Allgemein**.
  d. Aktivieren Sie im Abschnitt **Systemkonfiguration** das Kontrollkästchen **Warnmeldungen weiterleiten an Antwort** und klicken Sie auf **Anwenden**.

- **Um NetWitness Suite Malware Analysis-Warnmeldungen an NetWitness Respond weiterzuleiten, führen Sie folgende Schritte aus:**
  a. Wählen Sie **ADMIN >Services > Malware Analysis** aus.
  b. Klicken Sie für den Malware Analysis-Service auf > **Ansicht** > **Konfiguration**.
  c. Klicken Sie auf die Registerkarte **Auditing**.

d. Überprüfen Sie im Abschnitt **Auf Warnmeldung antworten**, ob das Kontrollkästchen **Aktivierter Konfigurationswert** aktiviert ist. Wenn das Kontrollkästchen nicht aktiviert ist, aktivieren Sie es und klicken Sie auf **Anwenden**.

Schritt 4: Weiterleiten von Endpoint-Warnmeldung an NetWitness Suite Respond

RSA Endpoint-Warnmeldungen können über NetWitness Respond an RSA Archer GRC gesendet werden. Weitere Informationen zum Konfigurieren von NetWitness Endpoint-Warnmeldungen über den Nachrichtenbus finden Sie im Thema *Konfigurieren von NetWitness Endpoint-Warnmeldungen über den Nachrichtenbus“ im NetWitness Endpoint-Integrationsleitfaden*.

Schritt 5: Aggregieren von Warnmeldungen zu Incidents

In NetWitness Respond eingehende Warnmeldungen können automatisch zu Incidents aggregiert und an RSA Archer Security Operations Management weitergeleitet werden. Aggregationsregeln werden automatisch jede Minute ausgeführt und aggregieren die Warnmeldungen basierend auf den ausgewählten Übereinstimmungsbedingungen und Gruppierungsoptionen zu Incidents. Weitere Informationen zur Aggregation von Warnmeldungen finden Sie im Thema „Konfigurieren von Warnmeldungsquellen zur Anzeige von Warnmeldungen in Respond“ im *Konfigurationsleitfaden für NetWitness Respond*.

So konfigurieren Sie die Aggregation von Warnmeldungen:

1. Wählen Sie **Konfigurieren > Incident-Regeln** aus.
2. Um die bereitgestellten einsatzbereiten Regeln zu aktivieren, führen Sie die folgenden Schritte aus:
   a. Doppelklicken Sie auf die Regel.
   b. Wählen Sie **Aktiviert** aus.
   c. Klicken Sie auf **Speichern**.
   d. Wiederholen Sie die Schritte a bis c für jede Regel.
3. Gehen Sie wie folgt vor, um eine neue Regel hinzuzufügen:
   a. Klicken Sie auf ✚.
   b. Wählen Sie **Aktiviert** aus.
   c. Füllen Sie die folgenden Felder aus:
      - Regelname
      - Aktion

- Bedingungen abstimmen
- Gruppierungsoptionen
- Incident-Optionen
- Priorität
- Benachrichtigungen

4. Klicken Sie auf **Speichern**.

Konfigurieren von Reporting Engine für die Integration in NetWitness SecOps Manager

Um Syslog-Ausgabeaktionen für Reporting Engine zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie den Reporting Engine-Service aus und klicken Sie auf **Ansicht** > **Konfiguration**.
3. Klicken Sie auf die Registerkarte **Ausgabeaktionen**.
4. Geben Sie im Bereich **NetWitness Suite-Konfiguration** in das Feld **Hostname** den Hostnamen oder die IP-Adresse des Reporting Engine-Servers ein.
5. Fügen Sie im Abschnitt **Syslog-Konfiguration** die Syslog-Konfiguration wie folgt hinzu:
   a. Geben Sie im Feld **Servername** den Hostnamen des UCF ein.
   b. Geben Sie im Feld **Serverport** den Port ein, den Sie in der UCF-Syslog-Konfiguration ausgewählt haben.
   c. Wählen Sie im Feld **Protokoll** das Transportprotokoll aus.

   Hinweis: Wenn Sie „Sicheres TCP“ auswählen, muss SSL konfiguriert werden.
6. Klicken Sie auf **Speichern**.

So konfigurieren Sie die NetWitness Suite Reporting Engine-SSL für den sicheren Syslog-Server:

Konfigurieren Sie SSL, wenn der Syslog-Server mit „Sicheres TCP“ konfiguriert ist.

1. Kopieren Sie das Zertifikat `keystore.crt.der` vom UCF-Rechner in die NetWitness Suite-Serverbox unter `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3.x86_64/jre/lib/security`.

2. Führen Sie den folgenden Befehl aus:

```
keytool -import -file keystore.crt.der -alias ucf-syslog -keystore
/etc/pki/nw/trust/truststore.jks -storepass changeit
```

Hinweis: Verwenden Sie nicht Kopieren und Einfügen, um den obigen Befehl einzugeben. Geben Sie ihn zur Vermeidung von Fehlern manuell ein.

3. Legen Sie **ServerCertificateValidationEnabled** auf **true** fest.
   - Navigieren Sie zu **ADMIN** > **Service**.
   - Klicken Sie auf > **Ansicht > Erkunden** des Reporting Engine-Service.
   - Erweitern Sie **com.rsa.soc.re** > **Konfiguration** > **SSLContextConfiguration**.
   - Erweitern Sie **sslContextConfiguration** und legen Sie für **ServerCertificateValidationEnabled** die Option **true** fest.
4. Starten Sie den Reporting Engine-Service neu.

So konfigurieren Sie Regeln in NetWitness Suite:

1. Klicken Sie auf **Monitor >Berichte > Managen**
   .Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie im Bereich **Regelgruppen** auf +.
3. Geben Sie für die neue Gruppe einen Namen ein.
4. Wählen Sie die erstellte Gruppe aus und klicken Sie in der Symbolleiste „Regel“ auf +.
5. Wählen Sie im Feld **Regeltyp** die Option „NetWitness-DB“ aus.
6. Geben Sie einen Namen für die Regel ein.
7. Geben Sie in den Feldern **Auswählen** und **Dabei gilt Folgendes** der zu erstellenden Regel entsprechende Werte ein.

Hinweis: Fügen Sie die Syslog-Konfiguration mit dem oben festgelegten Syslog-Namen hinzu.

8. Klicken Sie auf **Speichern**.

Hinweis: Um zu erreichen, dass in Reporting Engine und RSA Archer GRC dieselbe Anzahl von Warnmeldungen angezeigt wird, vergewissern Sie sich, dass Sie auf den Registerkarten „Syslog“ und „Datensatz“ für die Ausführung jeweils „Einmal“ ausgewählt haben.

So fügen Sie Warnmeldungsvorlagen für Reporting Engine in NetWitness Suite hinzu:

Im Lieferumfang der UCF-Syslog-Konfiguration sind einsatzbereite Warnmeldungsvorlagen enthalten, die Sie beim Erstellen einer Warnmeldung mit einer Syslog-Ausgabeaktion verwenden können. In diesen Vorlagen werden die Kriterien definiert, die in der RSA Archer GRC-Plattform zur Aggregation von Warnmeldungen zu Incidents verwendet werden.

Die Beispielvorlagen befinden sich an folgender Stelle auf dem UCF-System:

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates`

1. Klicken Sie auf **Monitor > Berichte > Managen > Warnmeldungen**.
2. Klicken Sie auf die Registerkarte **Vorlage**.
3. Klicken Sie auf ✚.
4. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
5. Geben Sie im Feld **Meldung** die Warnmeldung ein.
6. Klicken Sie auf **Create**.
7. Wiederholen Sie die Schritte 3 bis 6 für jede Warnmeldungsvorlage, die Sie hinzufügen möchten.

So konfigurieren Sie Warnmeldungen in NetWitness Suite:

In RSA NetWitness Suite Reporting Engine ist eine Warnmeldung eine Regel, für die Sie eine kontinuierliche Ausführung planen können und deren Befunde in mehreren verschiedenen Warnmeldungsausgaben protokolliert werden können.

1. Klicken Sie auf **Monitor > Berichte > Managen > Warnmeldungen**.
2. Klicken Sie auf ✚.
3. Wählen Sie **Aktivieren** aus.
4. Wählen Sie die Regel aus, die Sie erstellt haben.
5. Wählen Sie **Per Push an die Decoder übertragen** aus.

   Hinweis: Wenn Sie in diesem Feld keinen Wert eingeben, funktioniert die Verbindung zu RSA NetWitness Suite in der RSA Archer Security Alerts-Anwendung nicht.
6. Wählen Sie in der Liste „Datenquellen“ eine Datenquelle aus.
7. Wählen Sie im Bereich **Benachrichtigung** die Option **Syslog** aus.
8. Klicken Sie auf ✚.
9. Füllen Sie die Felder für die Syslog-Konfiguration aus.

10. Wählen Sie im Feld **Textkörpervorlage** die Vorlage aus, die Sie für diese Syslog-Benachrichtigung verwenden möchten.
11. Klicken Sie auf **Speichern**.

Konfigurieren von Event Stream Analysis für die Integration in Archer SecOps

So konfigurieren Sie Event Stream Analysis-Syslog-Benachrichtigungseinstellungen in NetWitness Suite:

1. Klicken Sie auf **ADMIN** > **System** > **Globale Benachrichtigungen**.
2. Klicken Sie auf die Registerkarte **Ausgabe**.
3. Definieren und aktivieren Sie eine Event Stream Analysis-Syslog-Benachrichtigung.
4. Klicken Sie auf die Registerkarte **Server**.
5. Definieren und aktivieren Sie einen Syslog-Benachrichtigungsserver.
6. Geben Sie im Bereich „Syslog-Serverkonfiguration“ Folgendes ein:

   Feldbeschreibung:

   - Name: Geben Sie den benutzerdefinierten Namen an
   - Server-IP (Hostname): Geben Sie den Hostnamen oder die IP-Adresse des Systems an, auf dem Sie das UCF installiert haben.
   - Port: Geben Sie die Portnummer an, die das UCF für die Erfassung verwenden soll.
   - Facility: Geben Sie die Syslog-Facility an.
   - Protokoll: Wählen Sie das Protokoll aus.
7. Klicken Sie auf **Speichern**.

So konfigurieren Sie die NetWitness Suite Event Stream Analysis-SSL für den sicheren Syslog-Server:

Konfigurieren Sie SSL, wenn der Syslog-Server mit „Sicheres TCP“ konfiguriert ist.

1. Wählen Sie **ADMIN > Services** aus.
2. Wählen Sie den Event Stream Analysis-Service aus. Navigieren Sie zu **Durchsuchen > Konfiguration > SSL**.
3. Legen Sie für **ServerCertificateValidationEnabled** die Option **true** fest.

4. Kopieren Sie `rootcastore.cert.pem` vom UCF-Rechner auf den Event Stream Analysis-Server in das Verzeichnis `/etc/pki/ca-trust/source/anchors`.
5. Führen Sie den folgenden Befehl aus:

   ```
   update-ca-trust
   ```

6. Starten Sie den Event Stream Analysis-Server neu.

So fügen Sie Event Stream Analysis-Warnmeldungsvorlagen hinzu:

Im Lieferumfang der UCF-Syslog-Konfiguration sind einsatzbereite Warnmeldungsvorlagen enthalten, die Sie beim Erstellen einer Warnmeldung mit einer Syslog-Ausgabeaktion verwenden können. In diesen Vorlagen werden die Kriterien definiert, die in der RSA Archer GRC-Plattform zur Aggregation von Warnmeldungen zu Incidents verwendet werden.

Die Beispielvorlagen befinden sich an folgender Stelle auf dem UCF-System:

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_`

`Templates\SecOps_SA_ESA_templates.txt`

1. Wählen Sie **ADMIN > System > Globale Benachrichtigungen** aus.
2. Klicken Sie auf die Registerkarte **Vorlagen**.
3. Klicken Sie auf ✚.
4. Wählen Sie im Feld **Vorlagentyp** die Option „Event Stream Analysis“ aus.
5. Geben Sie im Feld **Name** den Namen für die Vorlage ein.
6. (Optional) Geben Sie im Feld **Beschreibung** eine kurze Beschreibung der Vorlage ein.
7. Geben Sie im Feld **Vorlage** die Warnmeldung ein.
8. Klicken Sie auf **Speichern**.
9. Wiederholen Sie die Schritte 3 bis 8 für jede Warnmeldungsvorlage, die Sie hinzufügen möchten.

So erstellen Sie Event Stream Analysis-Regeln:

1. Klicken Sie auf **Konfigurieren** > **ESA-Regeln**.
2. Klicken Sie in der **Regelbibliothek** auf ✚.
3. Wählen Sie **Regelerstellung** aus.
4. Geben Sie im Feld **Name der Regel** einen Namen für die Regel ein.
5. Geben Sie in das Feld **Beschreibung** eine Beschreibung für die Regel ein.
6. Wählen Sie den **Schweregrad** aus.
7. Führen Sie im Abschnitt **Bedingung** die folgenden Schritte aus:

a. Klicken Sie auf +, um eine Anweisung zu erstellen.

b. Geben Sie einen Namen ein und fügen Sie Metadaten/Wertepaare für die Anweisung hinzu.

c. Klicken Sie auf **Speichern**.

d. Wiederholen Sie die Schritte a bis c, bis Sie alle Ihre Anweisungen für die Regel erstellt haben.

8. Wählen Sie im Bereich **Benachrichtigungen** die Option **Syslog** aus.
9. Wählen Sie die Benachrichtigung, den Syslog-Server und die Vorlage aus, die Sie zuvor erstellt haben.
10. Klicken Sie auf **Speichern** und **Schließen**.
11. Klicken Sie auf **Konfigurieren** > **Bereitstellungen**.
12. Klicken Sie für den Event Stream Analysis-Servicesabschnitt auf +.
13. Wählen Sie den Event Stream Analysis-Service aus.
14. Klicken Sie auf **Jetzt bereitstellen**.
15. Klicken Sie im Abschnitt **Event Stream Analysis-Regeln** auf +, um die erstellte Event Stream Analysis-Regel auszuwählen, und klicken Sie dann auf **Jetzt bereitstellen**.

RSA Archer-Feed

Standardmäßig werden nur die Felder „IP-Adresse“ und „Wichtigkeitsrating“ in der Anwendung RSA Archer Devices durch den SA IM Integration Service in RSA NetWitness Suite eingespeist. Sie können das Enterprise-Management-Plug-in so anpassen, dass die Felder „Geschäftsbereich“ und „Facility“, auf die verwiesen wird, in der Anwendung Devices in den Feed einbezogen werden. Weitere Informationen finden Sie in der Archer-Dokumentation unter https://community.emc.com/community/connect/grc_ecosystem/rsa archer oder https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.

Hinweis: Wenn Sie vorhaben, die Informationen in „Geschäftsbereich“ und „Facility“ aus der RSA Archer GRC-Plattform per Feed in Live zu übertragen, müssen Sie in der Datei index-concentrator-custom.xml Schlüssel für diese Felder hinzufügen.

Aktualisieren von Concentrator- und Decoder-Services

Der SA IM Integration Service in NetWitness SecOps Manager managt die Dateien für einen benutzerdefinierten Feed und legt diese Dateien in einem lokalen Ordner ab, den Sie bei der Enterprise-Management-Endpunkts angeben. Das Modul Live von RSA NetWitness Suite ruft die Feeddateien aus diesem Ordner ab. Live überträgt den Datenfeed dann per Push an die Decoder, die basierend auf dem erfassten Netzwerkdatenverkehr und der Feeddefinition mit der Erstellung von Metadaten beginnen. Damit jeder Concentrator die neuen Metadaten erkennt, die von den Decodern erstellt wurden, bearbeiten Sie die Dateien `index-concentrator-custom.xml`, `index-logdecoder-custom.xml` und `index-decoder-custom.xml` files.

1. Wählen Sie **ADMINISTRATION > Services** aus.
2. Wählen Sie den Concentrator und dann  > **Ansicht > Konfiguration** aus.
3. Klicken Sie auf die Registerkarte **Dateien**.
4. Wählen Sie in der Drop-down-Liste die Datei index-concentrator-custom.xml aus. Führen Sie einen der folgenden Schritte aus:
   - Wenn in der Datei bereits Inhalte vorhanden sind, fügen Sie wie folgt einen Schlüssel für das neue Metadatenelement hinzu:

     ```
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     ```

     Hinweis: Verwenden Sie nicht Kopieren und Einfügen, um den obigen Befehl einzugeben. Geben Sie ihn zur Vermeidung von Fehlern manuell ein.
   - Wenn die Datei leer ist, fügen Sie den folgenden Inhalt hinzu:

     ```
     <?xml version="1.0" encoding="utf-8"?>
     <language level="IndexNone" defaultAction="Auto">
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     </language>
     ```
5. Klicken Sie auf **Anwenden**.
6. Gehen Sie wie folgt vor, um mehrere Geräte hinzuzufügen:
   a. Klicken Sie auf **Push**.
   b. Wählen Sie die Geräte aus, zu denen Sie diese Datei per Push übertragen möchten.
   c. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 1 bis 7 für die Log Decoder und Index-Decoder mit den Dateien index-logdecoder-custom.xml und index-decoder-custom.xml.
8. Starten Sie die Concentrator- und Decoder-Services neu.

Hinzufügen des RSA Archer Enterprise Management-Endpunkts im UCF

1. Wählen Sie im UCF-Verbindungsmanager wie folgt den Modus aus:
   a. Geben Sie die Zahl für „Modusauswahl“ ein.
   b. Wählen Sie eine der folgenden Optionen:
      - Incident-Workflow in RSA NetWitness Suite managen.
      - Incident-Workflow ausschließlich in RSA Archer Security Operations Management managen
2. Fügen Sie den RSA Archer Enterprise Management-Endpunkt wie folgt hinzu:
   a. Geben Sie die Zahl für Enterprise Management ein.
   b. Füllen Sie die Felder in der Tabelle unten aus.

Feld	Beschreibung
Endpunktname	Optionaler Name des Endpunkts
Webserver-Port	Der Standardwert ist 9090. Kann für das Hosten der Webserver-URL konfiguriert werden. Die URL mit der Portnummer sollte als die URL im NetWitness Suite Live-Feed bereitgestellt werden: http://hostname:port/archer/sa/feed
Bedeutung	Wichtigkeit der Ressourcen, die von RSA Archer GRC abgerufen werden sollen. Bei **false** werden Ressourcen mit beliebigem Wichtigkeitsrating abgerufen. Bei **true** werden nur Ressourcen mit hohem Wichtigkeitsrating abgerufen. Bearbeiten Sie zum manuellen Konfigurieren die Eigenschaft „em.criticality“ in der Eigenschaftendatei collector-properties, um eine durch Kommas getrennte Liste von Wichtigkeitsratings bereitzustellen: NIEDRIG, MITTEL, HOCH.
Feedverzeichnis	Verzeichnis, in dem die Ressourcen-CSV-Datei von RSA Archer GRC gespeichert ist. **Hinweis:** Der angegebene Verzeichnispfad muss vorhanden sein.

Feld	Beschreibung
Webserver-Benutzername	Benutzername für die Authentifizierung auf dem EM-Webserver. **Hinweis:** Dieser wird bei der Konfiguration des NetWitness Suite Live-Feeds angegeben.
Webserverpasswort	Passwort für die Authentifizierung auf dem EM-Webserver. **Hinweis:** Dieser wird bei der Konfiguration des NetWitness Suite Live-Feeds angegeben.
SSL-Modus	Der Standardwert ist „Nein“. Bei **Nein** verwendet die URL `http mode: http://hostname:port/archer/sa/feed` Wenn Sie die Hostdatei nicht aktualisiert haben, lesen Sie den Abschnitt „Aktualisieren der RSA NetWitness Suite Hostdatei“. **Hinweis:** NetWitness Suite unterstützt derzeit im SSL-Modus keine wiederkehrenden Archer-Feeds.

Aktualisieren Sie die RSA NetWitness Suite-Hostdatei.

1. Bearbeiten Sie die Hostdatei auf dem NetWitness Suite-Server am folgenden Speicherort:
   vi/etc/hosts
2. Geben Sie Folgendes als UCF-Host-IP-Adresse ein:
   `<ucf-host-ip> <ucf-host-name>`
3. Starten Sie den NetWitness Suite-Server durch Ausführen des folgenden Befehls neu:
   `service jetty restart`
4. Geben Sie bei der Konfiguration des NetWitness Suite Live-Feeds den Hostnamen für die URL statt der in Enterprise Management im UCF konfigurierten IP-Adresse und Portnummer ein:
   `http: //<ucf-host-name> : <EM_Port>/archer/sa/feed.`
5. Überprüfen Sie, ob die Verbindung funktioniert.

Erstellen einer wiederkehrenden Feedaufgabe

Damit RSA NetWitness Suite Feeddateien aus dem NetWitness Respond Integration Service herunterladen und per Push auf Decoder übertragen kann, müssen Sie eine wiederkehrende Feedaufgabe erstellen und die Datenfeedeinstellungen definieren.

Hinweis: Für RSA Archer SecOps 1.2: Damit RSA NetWitness Suite Feeddateien vom RCF-Rechner herunterladen und per Push auf Decoder übertragen kann, müssen Sie eine wiederkehrende Feedaufgabe erstellen und die Datenfeedeinstellungen definieren. Das Verfahren ist mit wenigen Ausnahmen dasselbe wie für RSA Archer SecOps 1.3. Weitere Informationen erhalten Sie in der Dokumentation in der RSA Archer Exchange-Community.

1. Wählen Sie **Konfigurieren >Benutzerdefinierte Feeds** aus.
2. Klicken Sie in der Ansicht „Feeds“ auf ✚.
3. Wählen Sie **Benutzerdefinierter Feed** aus und klicken Sie dann auf **Weiter**.
4. Wählen Sie **Wiederkehrend** aus.
5. Geben Sie einen Namen für den Feed ein.
6. Geben Sie im Feld „URL“ Folgendes ein:

   `http://ucf_hostname/archer/sa/feed`

   Dabei gilt Folgendes: *`http :ucf_hostname_or_ip:port`* ist die Adresse des NetWitness Respond Integration Service-Systems. Beispiel: `http://10.10.10.10:9090`.

   Hinweis: Wenn Respond im SSL-Modus ausgeführt wird, muss der Hostname in der URL verwendet werden.
7. Wählen Sie **Authentifiziert**.
8. Geben Sie in die Felder **Benutzername** und **Passwort** die Anmeldedaten des Benutzerkontos ein, das Sie für RSA NetWitness Suite für den Zugriff auf Dateien auf dem NetWitness Respond Integration Service-System erstellt haben.
9. Definieren Sie das Wiederholungsintervall für den Feed.
10. Definieren Sie im Abschnitt **Datumsbereich** ein Start- und Enddatum für den Feed und klicken Sie auf **Weiter**.
11. Wählen Sie alle Decoder aus, auf die dieser Feed per Push übertragen werden soll, und klicken Sie auf **Weiter**.
12. Stellen Sie sicher, dass im Feld **Typ** die Option „IP“ ausgewählt ist.
13. Wählen Sie im Feld **Indexspalte** den Wert „1“ aus.
14. Legen Sie in der zweiten Spalte für den Wert „Schlüssel“ das Wirksamkeitsrating fest und klicken Sie auf **Weiter**.
15. Überprüfen Sie die Details der Feedkonfiguration und klicken Sie auf **Fertigstellen**.

Managen des Unified Collector Framework

Dieser Abschnitt bietet zusätzliche Aufgaben für Konfiguration und Management der Integration von RSA UCF (Unified Collector Framework) für Archer SecOps 1.3.1.2.

Starten des RSA Unified Collector Framework

1. Klicken Sie auf **Systemsteuerung > Verwaltungstools > Services**.
2. Wählen Sie „RSA Unified Collector Framework“ aus.
3. Klicken Sie auf **Start**.

Beenden des RSA Unified Collector Framework

1. Klicken Sie auf **Systemsteuerung > Verwaltungstools > Services**.
2. Beenden Sie den RSA SecOps-Watchdog-Service.

   Hinweis: Wenn Sie den Watchdog-Service nicht beenden, startet der Watchdog-Service den NetWitness-Respond-Service frühzeitig.
3. Wählen Sie „RSA Unified Collector Framework“ aus.
4. Klicken Sie auf **Stop**.

Hinweis: Wenn das Herunterfahren des Services zu lange dauert, verwenden Sie den Task-Manager, um den Prozess RSASAIMDCService zu beenden.

Deinstallieren des RSA Unified Collector Framework

1. Klicken Sie auf **Systemsteuerung**> **Programme und Funktionen**.
2. Wählen Sie **RSA Unified Collector Framework** aus.
3. Klicken Sie auf **Deinstallieren**.

Troubleshooting einer RSA Archer-Integration

Dieser Abschnitt enthält Lösungen für häufige Probleme, die bei der Konfiguration von Archer SecOps 1.3.1.2 mit NetWitness Suite Respond auftreten können.

Festlegen des Zertifizierungsstellen-Truststore

Problem: Nach dem Hinzufügen des Endpunkts für NetWitness Suite Respond kann der Zertifizierungsstellen-Truststore nicht festgelegt werden.

Lösung:

1. Stellen Sie sicher, dass die SSH-Anmeldedaten für den NetWitness Suite-Host gültig sind.
2. Wenn die Anmeldedaten korrekt sind, der Fehler aber weiterhin auftritt, kopieren Sie die Zertifikate manuell.

Korrekturaufgaben in RSA Archer Security Operations Manager

Problem: Korrekturaufgaben werden per Push über den UCF in die Vorgangswarteschlange übertragen und nicht als Befunde in RSA Archer Security Operations Management angezeigt.

Lösung:

1. Öffnen Sie den Verbindungsmanager:
   - Öffnen Sie eine Eingabeaufforderung
   - `Wechseln Sie zum Verzeichnis <install_dir>\SA IM integration service\data-collector.`
   - `Geben Sie Folgendes ein: runConnectionManager.bat`
2. Geben Sie „2“ ein, um den Endpunkt zu bearbeiten.
3. Geben Sie in NetWitness Suite Respond „3“ ein.
4. Vergewissern Sie sich, dass die Zielwarteschlange auf „Alle“ oder „Vorgänge“ festgelegt ist.

Fehler zwischen RSA NetWitness Suite und dem RSA Unified Collector Framework

Problem: Im Verzeichnis `<install_dir>\SA IM integration service\logs\collector.log` liegen Fehler zwischen RSA NetWitness Suite und dem RSA Unified Collector Framework vor.

Lösung:

1. Vergewissern Sie sich, dass die SSL-Zertifikate gültig sind.

   Hinweis: Zertifikate für NetWitness Suite Respond sind zwei Jahre gültig.

2. Wenn die Zertifikate abgelaufen sind, erzeugen Sie die abgelaufenen Zertifikate erneut und kopieren Sie diese.

Gehen Sie wie folgt vor, um die Zertifikate neu zu erzeugen und zu kopieren:

1. Navigieren Sie über die Befehlszeile zum Verzeichnis `<install_dir>\SA IM integration service\data-collector`.
2. Geben Sie `runConnectionManager.bat` ein.
3. Geben Sie die Zahl für „SA IM Integration Service-Zertifikat neu generieren“ ein
4. Geben Sie im NetWitness Suite Respond-Endpunkt die Zahl für „Endpunkt bearbeiten“ ein.
5. Geben Sie „Ja“ ein, um die Zertifikate automatisch in den NetWitness Suite-Truststore zu kopieren.

Hinweis: Wenn die Zertifikate nicht kopiert werden, kopieren Sie diese manuell.