RSA NETWITNESS® SUITE

RSA NetWitness Endpoint-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.

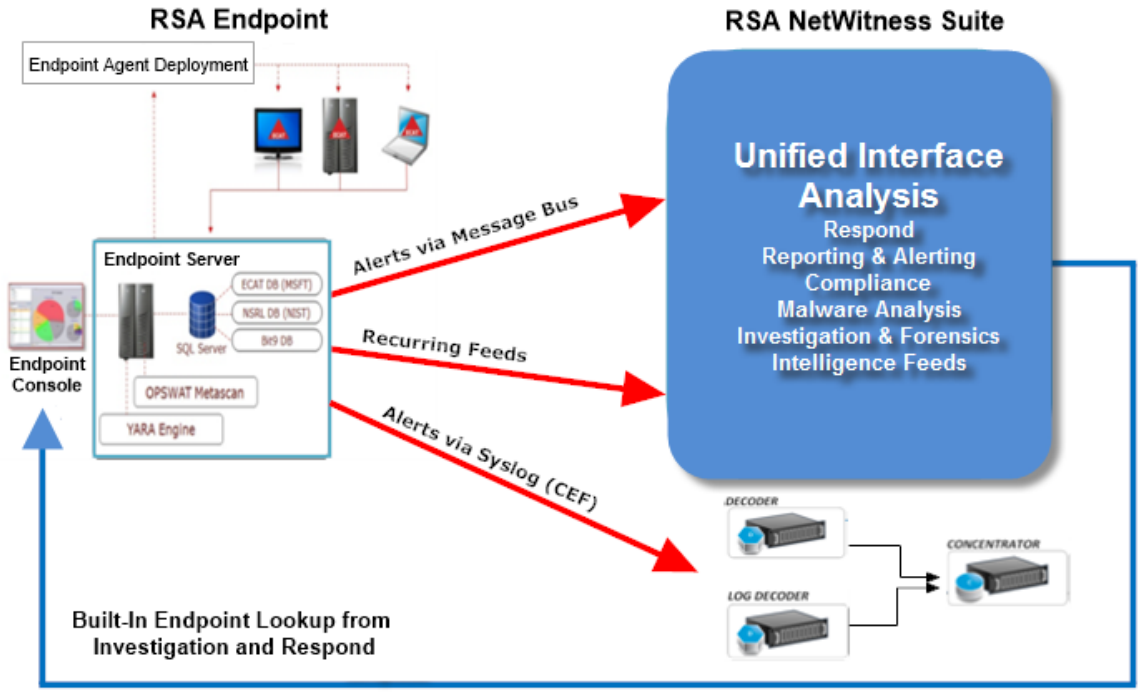
Februar 2018

Inhalt

RSA NetWitness Endpoint-Integration

RSA-Kunden, die RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5 oder 4.4 verwenden, können NetWitness Endpoint und RSA NetWitness Suite auf verschiedene Arten integrieren. Dieser Leitfaden behandelt RSA NetWitness Suite Version 11.0.

Integrationsoptionen



Integrierte NetWitness Endpoint-Suche

Wenn die RSA NetWitness Endpoint-Benutzeroberfläche auf demselben Computer installiert ist, auf dem der Analyst einen Browser für den Zugriff auf NetWitness Suite verwendet, liefert die integrierte NetWitness Endpoint-Suche von NetWitness Suite Investigation und NetWitness Suite Respond über einen Klick mit der rechten Maustaste Zugriff auf den NetWitness Endpoint-Konsolenserver für folgende Metaschlüssel: IP-Adresse (ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip), host (alias-host, domain.dst), client und file-hash. Diese sind im Thema „Starten einer externen Suche eines Metaschlüssels“ unter *Leitfaden Investigation und Malware Analysis* und im Thema „Warnmeldungen anzeigen“ unter *Leitfaden NetWitness Respond* beschrieben.

Es ist keine NetWitness Suite-Konfiguration für die Endpunktsuche erforderlich, wenn Sie einen der integrierten Parser (NetWitness Endpoint oder CEF) verwenden und die Standardmetaschlüssel, die beim Laden von Metadaten in Investigation verwendet werden, nicht angepasst haben. Weitere Informationen finden Sie im Thema „Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung“ im *Leitfaden Investigation und Malware Analysis*.

Hinweis: Eine Ausnahme liegt vor, wenn Sie NetWitness Suite anpassen, indem Sie die Anzeigeeinstellung für die Standardmetaschlüssel in Investigation bearbeiten, Metaschlüssel zur Datei „table-map-custom.xml“ hinzufügen oder NetWitness Endpoint-Feeds anpassen. Ein gewisses Maß an Konfiguration ist erforderlich, um die benutzerdefinierten Metaschlüssel dem Kontextmenü „NetWitness Endpoint-Suche“ in der Ansicht **ADMIN** > **System** hinzuzufügen, wie im Thema „Hinzufügen benutzerdefinierter Kontextmenüaktionen“ im *Systemkonfigurationsleitfaden* beschrieben.

Integrationsmethoden

Mit einem auf einem Windows-Host installierten RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5 oder 4.4 Konsolenserver und richtiger Konfiguration von NetWitness Endpoint und NetWitness Suite durch einen Administrator sind drei weitere Integrationen der NetWitness Endpoint-Analyse möglich.

Im Folgenden werden die RSA NetWitness Endpoint-Integrationsmethoden beschrieben:

- Konfigurieren von Endpoint-Warnmeldungen über Nachrichtenbus
- Konfigurieren kontextbezogener Daten von Endpoint über wiederkehrenden Feed
- Konfigurieren von Endpoint-Warnmeldungen über Syslog in einen Log Decoder

Endpoint-Warnmeldungen über Nachrichtenbus in NetWitness Respond. Diese Integration bietet die Möglichkeit für die Weiterleitung von Endpoint-Warnmeldungen an Respond über Nachrichtenbus.

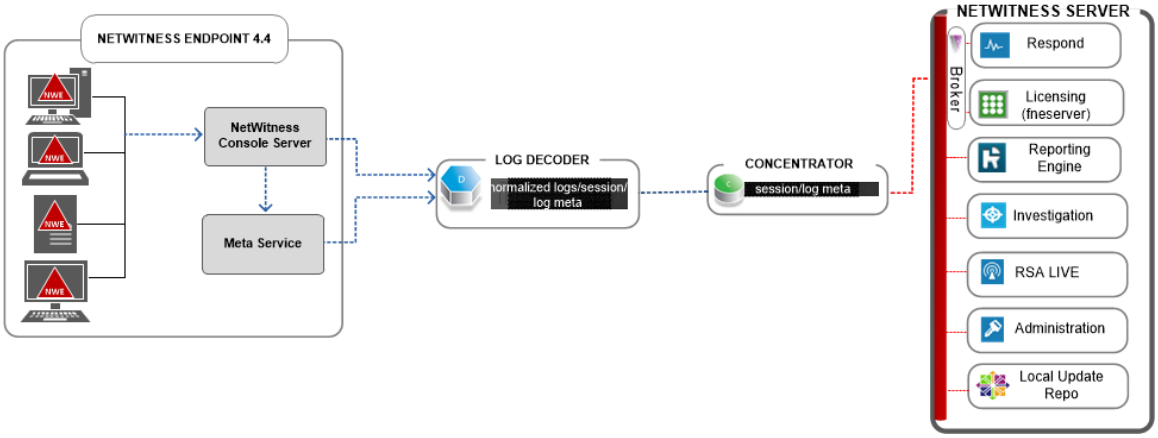
Kontextbezogene Daten von Endpoint über einen wiederkehrenden NetWitness Suite Live-Feed. Diese Integration kann die in NetWitness Suite Investigation angezeigte Sitzung mit kontextbezogenen Informationen anreichern. Einige Beispiele sind das Hostbetriebssystem, die MAC-Adresse, IIOC-Bewertung sowie andere Daten, die möglicherweise nicht in den Protokoll- oder Paketdaten enthalten sind.

NetWitness Endpoint-Warnmeldungen über Syslog (CEF) in NetWitness Suite Log Decoder. Diese Integration bietet die Möglichkeit, Endpoint-Ereignisse über Syslog weiterzuleiten und die Ereignisse mit anderen Protokoll- oder Paketmetadaten in dem NetWitness Suite-Ökosystem zu korrelieren.

NetWitness Endpoint Meta-Integration

Die NetWitness Endpoint Meta-Integration in RSA NetWitness Suite bietet Kunden, die beide Produkte besitzen, die Möglichkeit, ihre Produkte leichter auf einer einzigen Benutzeroberfläche zu nutzen. Das folgende Diagramm zeigt, wie NetWitnessEndpoint in die NetWitness Suite integriert werden kann. Die NetWitness Endpoint-Metadaten werden auf allen Computern erfasst und veröffentlicht, auf denen NetWitness Endpoint-Agents bereitgestellt wurden, und dann an den NetWitness Suite-Log Decoder gesendet.

Die Metadaten können dann im zugehörigen NetWitness Suite Concentrator und auch in NetWitness Suite Investigate angezeigt werden.



NetWitness Endpoint-Warnmeldungen und Indikatoren für eine Infizierung

Ein NetWitness Endpoint-IIOC (Indicator of Compromise, Indikator für eine Infizierung) ist eine Datenbankabfrage, die NetWitness Endpoint für gesammelte NetWitness Endpoint-Scandaten durchführt, um auf gescannten Hosts potenziell vorhandene Schadsoftware zu ermitteln. RSA NetWitness Endpoint 4.1.2 und höher enthält im Lieferumfang IOCs, die Benutzer aktivieren und als warnpflichtig markieren können. RSA NetWitness Endpoint führt regelmäßig IOC-Abfragen auf neuen Scandaten aus, die in der Datenbank gesammelt und gespeichert werden. Wenn die IOC-Abfrage positiv ist, wird ein potenzieller Indikator für eine Infizierung angezeigt und das Ereignis kann einem Benutzer gemeldet werden oder als Warnmeldung an ein externes System gesendet werden.

Mögliche Warnmeldungstypen sind:

- Warnmeldung Maschine: Diese Warnmeldung gibt an, dass die betroffene Maschine verdächtig ist.

- Warnmeldung Modul: Diese Warnmeldung gibt an, dass ein Modul, z. B. eine Datei, ein DLL oder eine ausführbare Datei, verdächtig ist. Sie enthält Details über das betroffene Modul.
- Warnmeldung Ereignis: Diese Warnmeldung stellt alle anderen verdächtigen Aktivitäten, die von NetWitness Endpoint entdeckt wurden und nicht in die oben angeführten Kategorien fallen, dar.

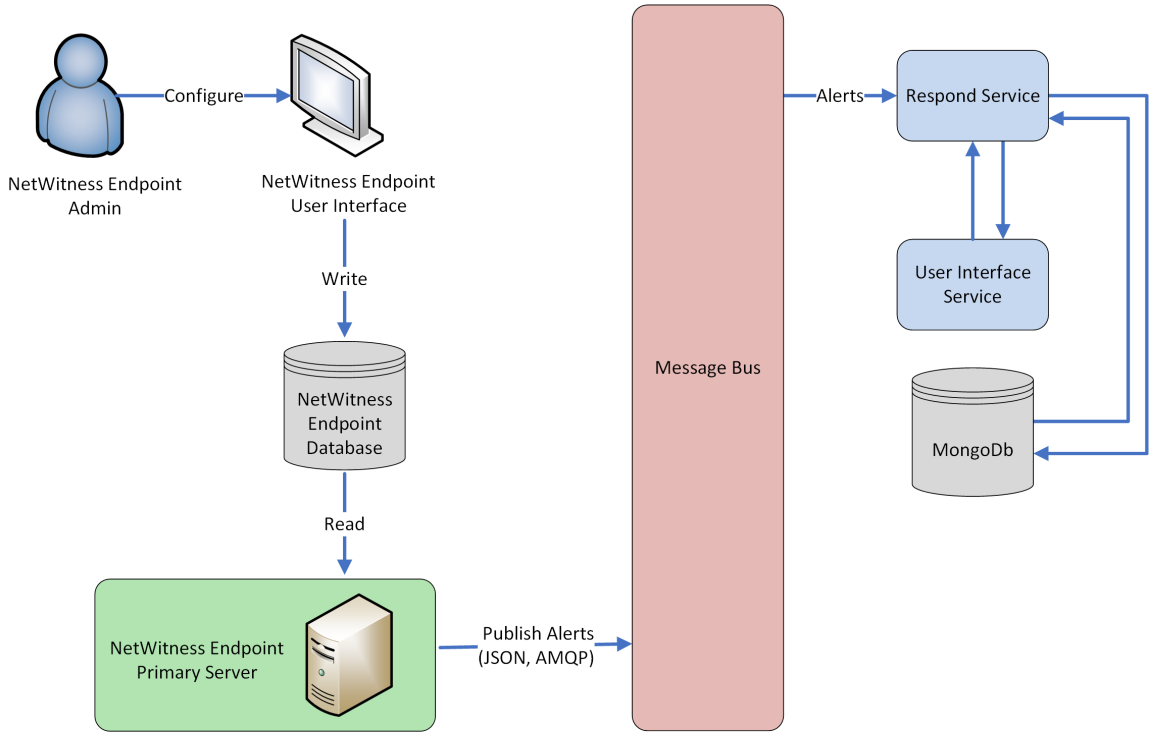
Jeder dieser Warnmeldungstypen kann an NetWitness Suite gesendet werden.

Konfigurieren von NetWitness Endpoint-Warnmeldungen über Nachrichtenbus

Dieses Verfahren ist für die Integration von NetWitness Endpoint in NetWitness Suite erforderlich, damit die NetWitness Endpoint-Warnmeldungen von der Respond-Komponente von NetWitness Suite erkannt und in der Ansicht **Reagieren > Warnmeldungen** angezeigt werden.

Hinweis: RSA unterstützt NetWitness Endpoint Versionen 4.3.0.4, 4.3.0.5 oder 4.4 für NetWitness Respond-Integration. Weitere Informationen finden Sie im Thema „RSA NetWitness Suite-Integration“ im *NetWitness Endpoint-Benutzerhandbuch*.

Das Diagramm unten stellt den Fluss von NetWitness Endpoint-Warnmeldungen zur Respond Incident-Listenansicht von NetWitness Suite und seine Anzeige in der Ansicht **Reagieren > Warnmeldungen** dar.



Voraussetzungen

Überprüfen Sie, ob die folgenden Voraussetzungen erfüllt sind:

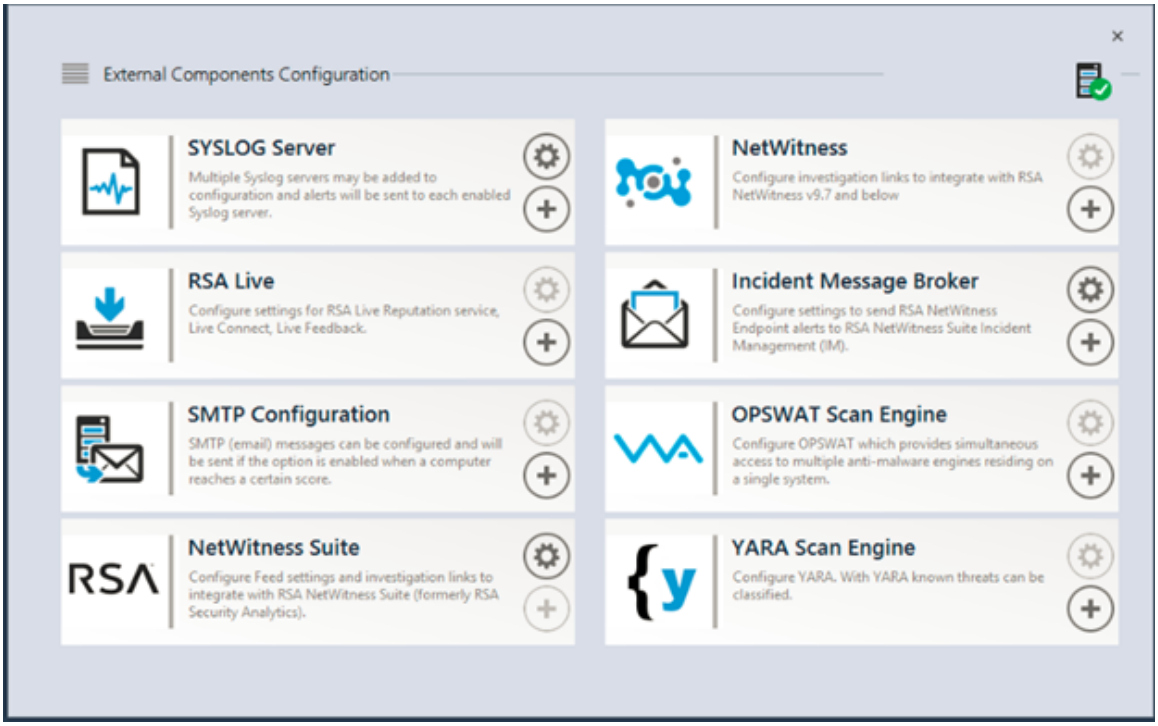
- Der Respond-Service ist auf NetWitness Suite 11.0 installiert und wird ausgeführt.
- NetWitness Endpoint 4.3.0.4, 4.3.0.5 oder 4.4 ist installiert und wird ausgeführt.

Konfigurieren von NetWitness Endpoint für die Weiterleitung von NetWitness Endpoint-Warnmeldungen

Gehen Sie wie folgt vor, um NetWitness Endpoint so zu konfigurieren, dass es Warnmeldungen über den Nachrichtenbus an die NetWitness Suite-Benutzeroberfläche sendet:

1. Klicken Sie in der NetWitness Endpoint-Benutzeroberfläche auf **Konfigurieren** > **Überwachung und externe Komponenten**.

   Das Dialogfeld **Konfiguration externer Komponenten** wird angezeigt.



   a. Wählen Sie bei den aufgeführten Komponenten **Incident Message Broker** aus und klicken Sie auf +, um einen neuen IM-Broker hinzuzufügen.

2. Geben Sie Werte für die folgenden Felder ein:

   a. **Instanzenname**: Geben Sie einen eindeutigen Namen zur Identifizierung des IM-Brokers ein.

   b. **Hostname/IP-Adresse des Servers**: Geben Sie die Host-DNS- oder die IP-Adresse des IM-Brokers ein (NetWitness-Server).

   c. **Portnummer**: Der Standardport ist 5671.

3. Klicken auf Sie auf **Speichern**.

4. Navigieren Sie zur Datei **ConsoleServer.exe.config** in **C:\Programme\RSA\ECAT\Server**.
5. Ändern Sie die virtuellen Host-Konfigurationen in der Datei wie folgt:
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Hinweis: In NetWitness Suite11.0 lautet der virtuelle Host „/rsa/system“. In Version 10.6.x und niedriger lautet der virtuelle Host „/rsa/sa“.
6. Starten Sie den API-Server und Konsolenserver neu.
7. Um SSL für Respond-Warnmeldungen einzurichten, führen Sie folgende Schritte auf dem primären Konsolenserver von NetWitness Endpoint aus, um die SSL-Kommunikation einzurichten:
   a. Exportieren Sie das NetWitness Endpoint CA-Zertifikat im CER-Format (Base-64 encoded X.509) aus dem persönlichen Zertifikatspeicher des lokalen Computers (ohne den privaten Schlüssel auszuwählen).
   b. Erzeugen Sie ein Clientzertifikat für NetWitness Endpoint mithilfe des NetWitness Endpoint CA-Zertifikats. (Sie MÜSSEN den CN-Namen auf ecat einstellen).

      ```
      makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
      sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NweCA" -is MY -ir
      LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
      cy end -sy 12 client.cer
      ```

      Hinweis: Im oben genannten Codebeispiel sollten Sie „EcatCA“ durch „NweCA“ ersetzen, wenn Sie von einer früheren Version ein Upgrade auf Version 4.3 durchgeführt haben und keine neuen Zertifikate erzeugt haben.
   c. Notieren Sie sich den Thumbprint des in Schritt b generierten Clientzertifikats. Geben Sie den Thumbprint-Wert des Clientzertifikats im Abschnitt IMBrokerClientCertificateThumbprint der ConsoleServer.Exe.Config-Datei ein (siehe Abbildung).

      ```
      <add key="IMBrokerClientCertificateThumbprint"
      value="896df0efacf0c976d955d5300ba0073383c83abc"/>
      ```
8. Kopieren Sie auf dem NetWitness-Server die NetWitness Endpoint CA-Zertifikatdatei im CER-Format in den Importordner:
   `/etc/pki/nw/trust/import`
9. Geben Sie den folgenden Befehl aus, um die erforderliche Chef-Ausführung zu initiieren:
   `orchestration-cli-client --update-admin-node`
   Dadurch werden alle Zertifikate an den Truststore angehängt.
10. Starten Sie den RabbitMQ-Server neu:
    `systemctl restart rabbitmq-server`
    Das NetWitness Endpoint-Konto sollte auf RabbitMQ automatisch verfügbar sein.

11. Importieren Sie die `/etc/pki/nw/ca/nwca-cert.pem`- und `/etc/pki/nw/ca/ssca-cert.pem`-Dateien vom NetWitness-Server und fügen Sie sie den Trusted Root Certification-Speichern auf dem Endpoint-Server hinzu.

Fehlerbehebung

Dieser Abschnitt enthält Lösungsvorschläge für Probleme, die auftreten können, wenn Sie NetWitness Endpoint-Warnmeldungen über Nachrichtenbus konfigurieren.

Bekannte Probleme	Lösungen
Orchestrierung schlägt auf dem Administrations-Node fehl.	Sie müssen den Inhalt des EcatCA-Zertifikats in `/etc/rabbitmq/ssl/truststore.pem` kopieren und einfügen und den Rabbitmq-Service neu starten.

Konfigurieren kontextbezogener Daten von NetWitness Endpoint über wiederkehrenden Feed

Sie können RSA NetWitness Endpoint-Daten in RSA NetWitness Suite so konfigurieren, dass kontextbezogene Daten aus NetWitness Endpoint in Decoder- und Log Decoder-Sitzungen bereitgestellt werden. Diese Konfiguration beinhaltet das Hinzufügen kontextbezogener Metawerte zusätzlich zu den IOC-Sofortwarnmeldungen, die Korrelationen zu anderen Metadaten im NetWitness Suite-Ökosystem herstellen können.

Administratoren können NetWitness Suite so konfigurieren, dass kontextbezogene Daten aus NetWitness Endpoint, die vom System gescannt wurden, über einen wiederkehrenden Feed von NetWitness Suite Live abgerufen werden können. Diese Integration kann die Sitzung eines Decoder oder Log Decoder mit kontextbezogenen Informationen bereichern, die in NetWitness Suite Investigation angezeigt werden. Beispiele hierfür sind Hostbetriebssysteme, MAC-Adressen, die IIOC-Bewertung und andere Daten, die möglicherweise nicht im Protokoll oder in den Paketdaten von Sitzungen eines Decoder oder Log Decoder enthalten sind.

Hinweis: Obwohl diese Funktion für Kunden mit einem Paket-Decoder konzipiert ist, kann ein wiederkehrender Feed auch in Log Decoders integriert werden.

Achtung: Die Verwendung dieses wiederkehrenden Feeds in Umgebungen mit vielen NetWitness Endpoint-Hosts kann zu einer reduzierten Performance der in NetWitness Suite integrierten Geräte (Decoder und Log Decoder) führen.

Voraussetzungen

- NetWitness Endpoint-Konsolenserver Version 4.3.0.4, 4.3.0.5 oder 4.4 und NetWitness-Server-Version 10.4 und höher müssen installiert sein.
- RSA Decoder und Concentrator Version 11.0 sind mit dem NetWitness-Server im Netzwerk verbunden.

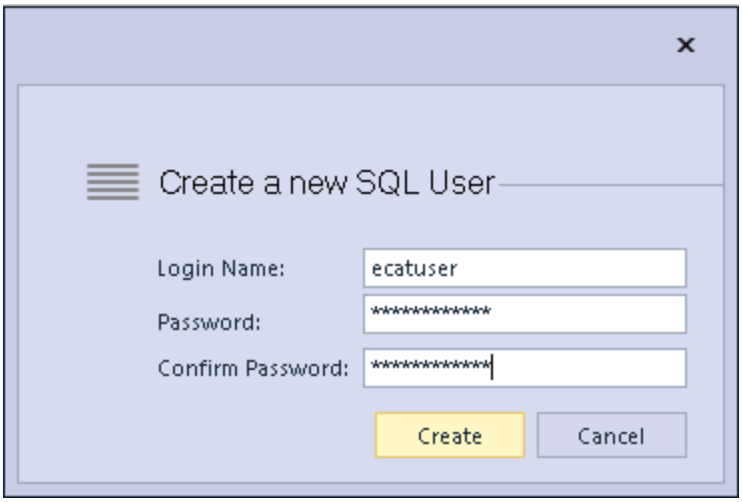
Führen Sie die folgenden Schritte aus, um kontextbezogene Daten von NetWitness Endpoint über einen wiederkehrenden Feed zu konfigurieren:

1. Aktivieren Sie den NetWitness Endpoint-Feed für NetWitness Suite in der NetWitness Endpoint-Benutzeroberfläche.
2. Exportieren Sie das NetWitness Endpoint-Zertifizierungsstellenzertifikat aus dem NetWitness Endpoint-Konsolenserver und importieren Sie es in den NetWitness Suite-Truststore.

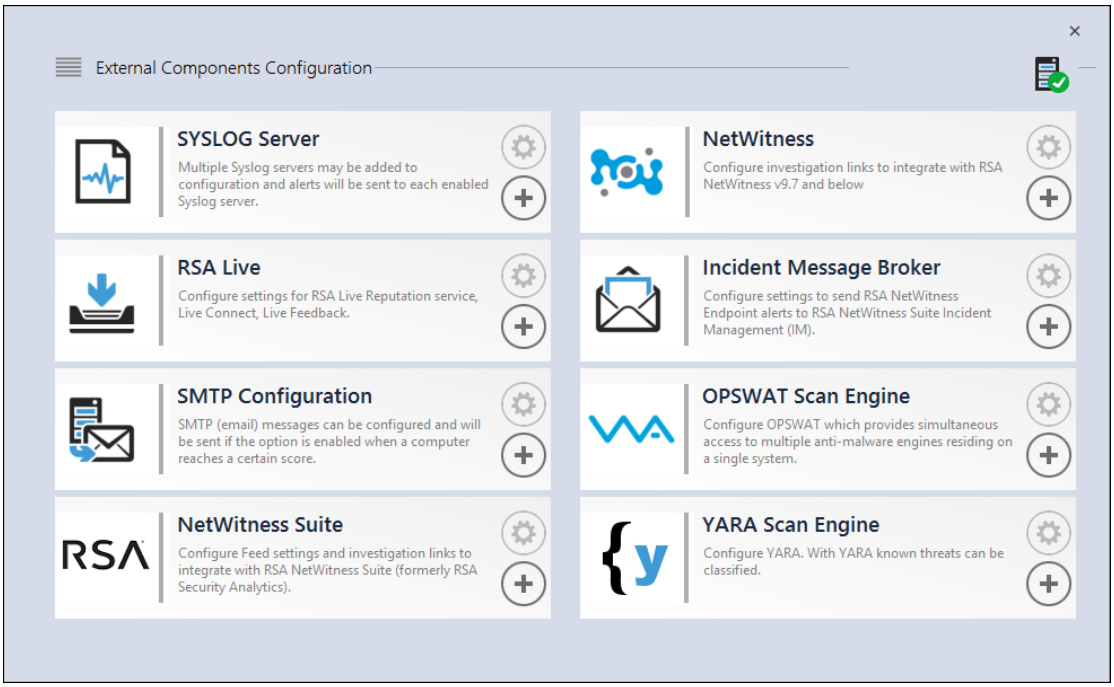
3. Konfigurieren Sie den NetWitness Suite Concentrator-Service zur Definition der indexierten Metaschlüssel.
4. Erstellen Sie einen wiederkehrenden Feed in NetWitness Suite Live.

Aktivieren des NetWitness Endpoint-Feeds für NetWitness Suite

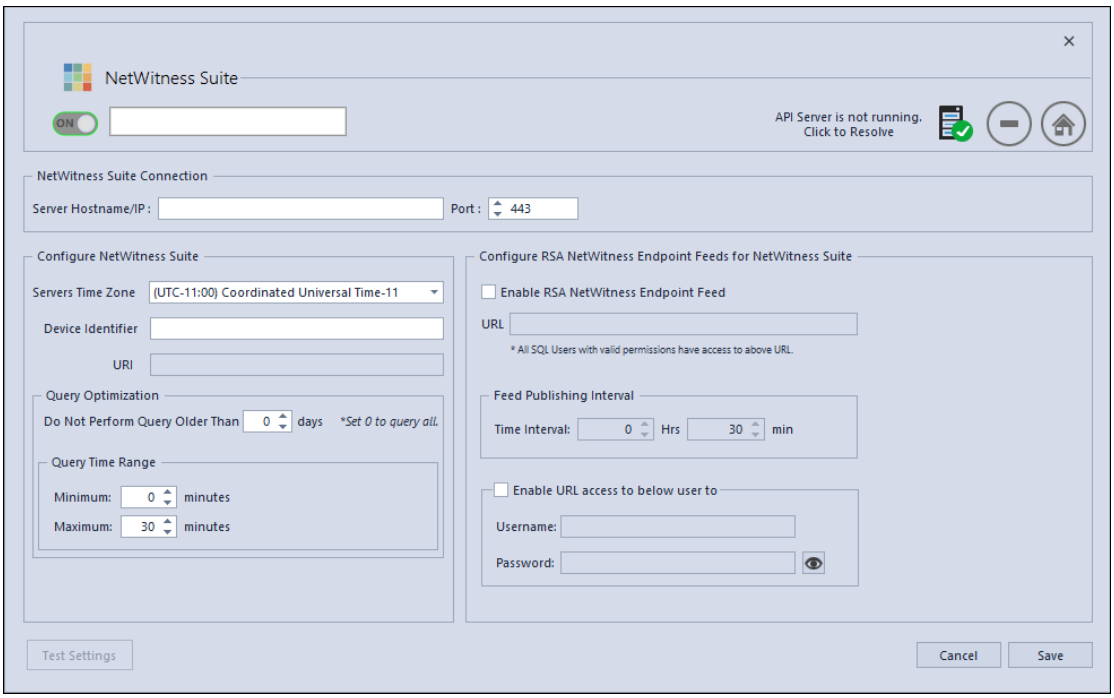
1. Erstellen Sie in der NetWitness Endpoint-Benutzeroberfläche einen SQL-Benutzer in NetWitness Endpoint:
   a. Öffnen Sie die NetWitness Endpoint-Benutzeroberfläche und melden Sie sich mit den richtigen Anmeldedaten an.
   b. Wählen Sie in der Menüleiste **Konfigurieren > Managen von Benutzern und Rollen** aus, klicken Sie mit der rechten Maustaste in den Bereich und wählen Sie **SQL-Benutzer erstellen** aus.
   Das Dialogfeld „Neuen SQL-Benutzer erstellen“ wird angezeigt.



   c. Geben Sie den **Benutzernamen** und das **Passwort** ein und klicken Sie auf **Erstellen**.
2. Wählen Sie in der Menüleiste **Konfigurieren > Überwachung und externe Komponenten** aus.
   Das Dialogfeld „Konfiguration externer Komponenten“ wird angezeigt.



3. Klicken Sie in NetWitness Suite auf +.
   Das Dialogfeld NetWitness Suite wird angezeigt.



4. Geben Sie im Bereich **NetWitness Suite** in **Ein** den Namen zur Identifizierung der NetWitness Suite-Komponente ein.

5. Führen Sie im Abschnitt **NetWitness Suite-Verbindung** die folgenden Schritte aus:
   a. Geben Sie im Feld **Hostname/IP des Servers** den Hostnamen oder die IP-Adresse des NetWitness-Server ein.
   b. Geben Sie im Feld **Port** die Portnummer ein. Die Standardportnummer ist 443.
6. Führen Sie im Bereich **NetWitness Suite konfigurieren** die folgenden Schritte aus:
   a. Wählen Sie im Feld **Serverzeitzone** die Zeitzone für die Komponente aus der Drop-down-Liste aus.
   b. Geben Sie im Feld **Geräte-ID** die NetWitness Suite Concentrator-Geräte-ID ein.

   Hinweis: Sie finden die Geräte-ID in NetWitness Suite, wenn Sie einen Concentrator oder Broker in **Investigation > Navigieren >***<Concentrator- oder Broker-Name>* suchen. Die Geräte-ID ist die Zahl in der URL nach „investigation“. Beispiel: In der URL `https://<IP address>investigation/319/navigate/values` ist die Geräte-ID **319**.

   Das Feld **URI** wird ausgefüllt, wenn Sie auf **Speichern** klicken.
7. Geben Sie im Bereich **Abfrageoptimierung** im Feld **Keine Abfrage durchführen, die älter ist als** eine Anzahl von Tagen ein, um den Abfragezeitraum zu beschränken. Geben Sie **0** ein, wenn Sie diese Funktion verwerfen möchten.
8. Führen Sie im Bereich **Zeitbereich der Abfrage** die folgenden Schritte aus:
   a. Geben Sie im Feld **Min.** die Anzahl der Minuten für den minimalen Zeitbereich der Abfrage ein. Dieser Wert wird verwendet, um den an NetWitness Suite übermittelten Zeitbereich automatisch zu erhöhen. Dadurch wird sichergestellt, dass eine Abfrage eine positive Antwort zurückgibt, wenn die vom NetWitness Endpoint-Agent berichtete Zeit geringfügig von der Zeit von NetWitness Endpoint abweicht.
   b. Geben Sie im Feld **Max.** die Anzahl der Minuten zur Beschränkung des Zeitbereichs ein. Dieser Wert wird verwendet, um den an NetWitness Suite übermittelten Zeitbereich automatisch zu beschränken, damit der NetWitness-Server von Abfragen nicht überlastet wird.
9. Führen Sie im Bereich **RSA NetWitness Endpoint-Feeds konfigurieren für NetWitness Suite** die folgenden Schritte aus:
   a. Wählen Sie **RSA NetWitness Endpoint-Feed aktivieren** aus.
   b. Geben Sie im Feld **URL Benutzername** und **Passwort** für SQL (konfiguriert in Schritt 1) für den Zugriff auf den Speicherort des Feeds ein.

Das Feld **URL** wird ausgefüllt, wenn Sie auf **Speichern** klicken.

c. Geben Sie das Zeitintervall für die Häufigkeit an, mit der Feeds veröffentlicht werden.

10. Wählen Sie im Bereich **Intervall Feed-Veröffentlichung** im Feld **Zeitintervall** das Zeitintervall in **Stunden** und **Minuten** für die Häufigkeit aus, mit der Feeds veröffentlicht werden.
11. Geben Sie im Bereich **Folgenden Benutzern URL-Zugriff ermöglichen auf** den **Benutzernamen** und das **Passwort** des NetWitness Endpoint-Benutzers ein.
12. Klicken Sie auf **Speichern**.
    Ein Feed wird erstellt.

Exportieren des SSL-Zertifikats von NetWitness Endpoint

Hinweis: Dieses Verfahren funktioniert nur für NetWitness Suite 10.5 und höher, da die Unterstützung für Java 8 in 10.5 hinzugekommen ist. Wenn Sie eine frühere Version von NetWitness Suite verwenden, schlagen Sie bitte in der entsprechenden Version dieses Leitfadens nach.

So exportieren Sie das NetWitness Endpoint-Zertifizierungsstellenzertifikat aus dem NetWitness Endpoint-Konsolenserver und kopieren es auf den NetWitness Suite-Host:

1. Melden Sie sich bei der NetWitness Endpoint-Konsole an.
2. Öffnen Sie**MMC**.
3. Fügen Sie ein Zertifikat-Snap-in für das **Computerkonto** hinzu.
4. Exportieren Sie das Zertifikat mit dem Namen **`EcatCA`**.
   a. Exportieren Sie es ohne privaten Schlüssel.
   b. Exportieren Sie es im DER-codierten binären X.509-Format (`.CER`).
   c. Geben Sie den Namen **`EcatCA.cer`** ein.
5. Kopieren Sie das NetWitness Endpoint-Zertifizierungsstellenzertifikat auf den NetWitness Suite-Host:
   - Bei einer Neuinstallation von NetWitness Endpoint 4.3.0.4, 4.3.0.5 oder 4.4:
     `scp NweCA.cer root@<sa-machine>:.`
   - Bei einem Upgrade von NetWitness Endpoint von der vorherigen Version auf 4.3.0.4 oder 4.3.0.5:
     `scp EcatCA.cer root@<sa-machine>:.`

6. Führen Sie die folgenden Schritte aus, um das NetWitness Endpoint-Zertifizierungsstellenzertifikat in den NetWitness Suite-Truststore zu importieren:

   a. Prüfen Sie die auf Ihrer NetWitness Suite installierte Java-Version mithilfe des folgenden Befehls:
   `java -version`
   Die openjdk-Version wird angezeigt. Beispiel: openjdk-Version „`1.8.0_71`“

   b. Navigieren Sie zum Festlegen des Parameters JDK zum Java-Verzeichnis. Geben Sie die folgenden Befehle ein:

   - `JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64/jre/`
   - Bei einer Neuinstallation von NetWitness Endpoint:

     ```
     $JDK/bin/keytool -import -v -trustcacerts -alias nweca -file ~/NweCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
     ```

   - Bei einem Upgrade von NetWitness Endpoint von der vorherigen Version:

     ```
     $JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
     ```

   Wenn Sie zur Bestätigung der Zertifikataktualisierung aufgefordert werden, geben Sie **Ja** ein.

7. Führen Sie auf dem NetWitness Suite-Host einen der folgenden Schritte aus:

   - Bei einer Neuinstallation von NetWitness Endpoint 4.3.0.4, 4.3.0.5 oder 4.4 bearbeiten Sie **`/etc/hosts`** so, dass die IP-Adresse des NetWitness Endpoint-Konsolenservers dem Namen **NweServerCertificate** zugeordnet wird, indem Sie die folgende Zeile zur Datei hinzufügen:

     ```
     <ip-address-ecat-cs> NweServerCertificate
     ```

   - Bearbeiten Sie bei einem Upgrade von NetWitness Endpoint von der vorherigen Version auf 4.3.0.4 oder 4.3.0.5 **`/etc/hosts`** so, dass die IP-Adresse des NetWitness Endpoint-Konsolenservers, für den das Upgrade durchgeführt wird, dem Namen **`ecatserverexported`** zugeordnet wird, indem Sie die folgende Zeile zur Datei hinzufügen:

     ```
     <ip-address-ecat-cs> ecatserverexported
     ```

8. Um NetWitness Suite neu zu starten, geben Sie den folgenden Befehl ein:

   ```
   service jetty restart
   ```

Konfigurieren des NetWitness Suite Concentrator-Services

1. Melden Sie sich bei NetWitness Suite an und wechseln Sie zu **ADMIN > Services**.
2. Wählen Sie einen Concentrator aus der Liste aus und wählen Sie **Ansicht > Konfiguration** aus.
3. Wählen Sie die Registerkarte **Dateien** aus und wählen Sie aus dem Drop-down-Menü **Zu bearbeitende Dateien** die Datei **index-concentrator-custom.xml** aus.
4. Fügen Sie der Datei folgende NetWitness Endpoint-Metaschlüssel hinzu und klicken Sie auf **Anwenden**. Stellen Sie sicher, dass diese Datei die XML-Abschnitte bereits enthält; wenn die Zeilen nicht enthalten sind, fügen Sie sie hinzu. Die folgenden Zeilen dienen als Beispiele. Stellen Sie sicher, dass die Werte Ihrer Konfiguration und den Spaltennamen in der Feeddefinition entsprechen. Dabei gilt Folgendes:
   description ist der Name des Metaschlüssels, den Sie in NetWitness Suite Investigation anzeigen möchten.
   level entspricht „IndexValues“
   name stimmt mit dem Spaltennamen der CSV-Datei überein, die von NetWitness Suite während der Definition des wiederkehrenden Feeds verwendet wird (siehe die unten stehende Tabelle in *Konfiguration der wiederkehrenden benutzerdefinierten Feedaufgabe in NetWitness Suite*).

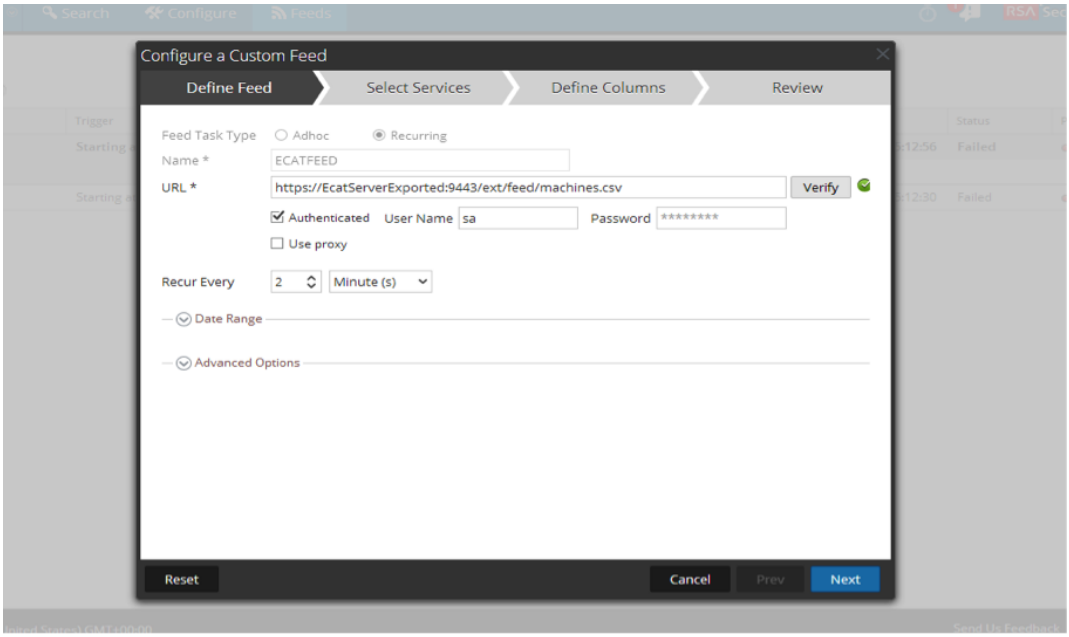
```
<key description="Gateway" format="Text" level="IndexValues"
name="gateway" valueMax="250000" defaultAction="Open"/>

<key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>

<key description="Strans Addr" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>

<key description="Domain" format="Text" level="IndexValues"
name="domain" valueMax="250000" defaultAction="Open"/>

<key description="User Account" format="Text" level="IndexValues"
name="username" valueMax="250000" defaultAction="Open"/>

<key description="Ecat Connectiontime" format="Text"
level="IndexValues" name="ecat.ctime" valueMax="250000"
defaultAction="Open"/>

<key description="Ecat Scantime" format="Text" level="IndexValues"
name="ecat.stime" valueMax="250000" defaultAction="Open"/>
```

5. Starten Sie den Concentrator neu, um die Aktualisierungen für benutzerdefinierte Schlüssel zu aktivieren.

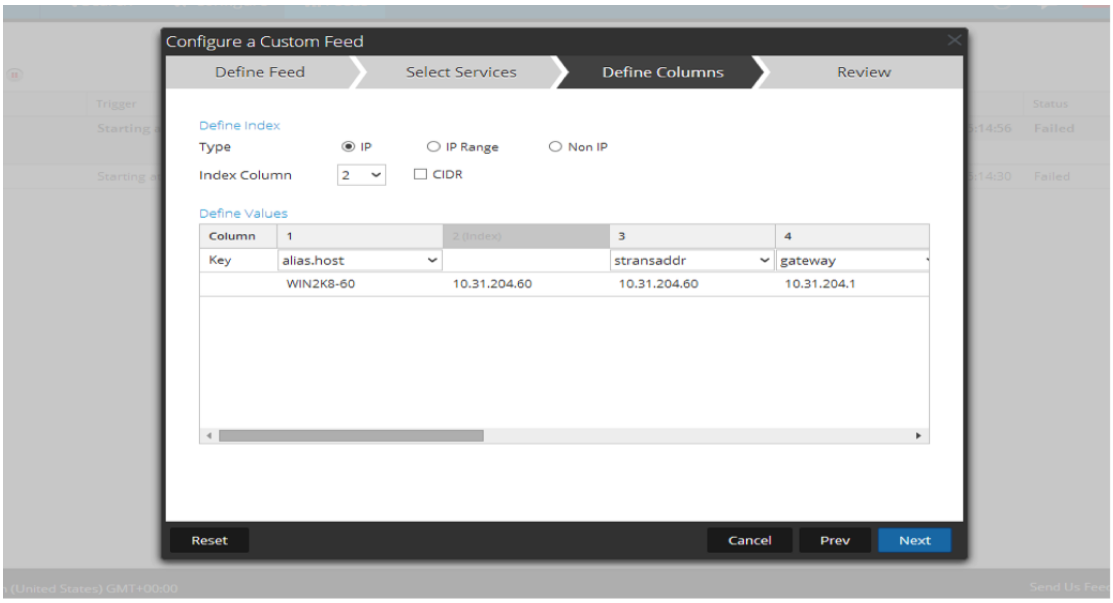
Konfigurieren der wiederkehrenden benutzerdefinierten Feedaufgabe in NetWitness Suite

1. Melden Sie sich bei NetWitness Suite an und wechseln Sie zu **Konfigurieren** > **Benutzerdefinierte Feeds**.
   Die Ansicht Feeds wird angezeigt.
2. Klicken Sie in der Symbolleiste auf  .
   Das Dialogfeld „Feed einrichten“ wird angezeigt.
3. Wählen Sie im Dialogfeld „Feed einrichten“ die Option **Benutzerdefinierter Feed** aus und klicken Sie auf **Weiter**.
   Der Assistent „Benutzerdefinierten Feed konfigurieren“ wird mit geöffnetem Formular „Feed definieren“ angezeigt.
4. Führen Sie im Feld **Feed definieren** folgende Schritte aus:
   a. Wählen Sie im Feld **Typ der Feedaufgabe** die Option **Wiederkehrend** aus.
   b. Geben Sie im Feld **Name** den Namen des Feeds ein, z. B. EndpointFeed.
   c. Geben Sie im Feld **URL** die URL mit dem Hostnamen des Windows-Servers ein, auf dem NetWitness Endpoint installiert ist:
      - Verwenden Sie bei einer Neuinstallation von NetWitness Endpoint 4.3.0.4, 4.3.0.5 oder 4.4 die URL
        `https://NweServerCertificate:9443/api/v2/feed/machines.csv.`.
      - Verwenden Sie bei einem Upgrade von NetWitness Endpoint von der vorherigen Version auf 4.3.0.4 oder 4.3.0.5 die URL
        `https://ecatserverexported:9443/api/v2/feed/machines.csv.`.
   d. Aktivieren Sie das Kontrollkästchen **Authentifiziert** und geben Sie den Benutzernamen und das Passwort ein, dass Sie beim *Aktivieren des ECAT-Feeds* notiert haben.
   e. Klicken Sie auf **Überprüfen**, um zu prüfen, ob NetWitness Suite die Webressource erreichen kann.

f. Legen Sie den Zeitplan fest und klicken Sie auf **Weiter**.



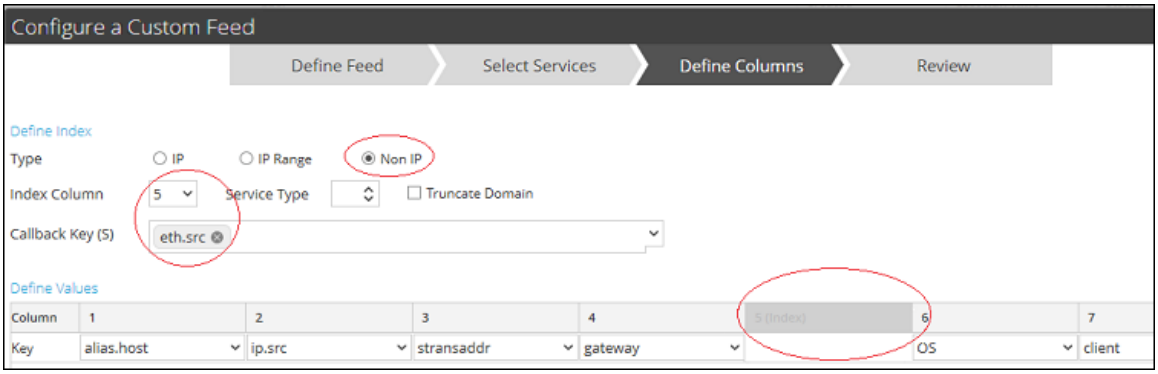
5. Wählen Sie in der Registerkarte **Services auswählen** den Decoder oder die Gruppen aus, die den Feed abrufen. Klicken Sie auf **Weiter**.
6. Geben Sie in der Registerkarte **Spalten definieren** die Spaltennamen ein (wie in der unten stehenden Tabelle gezeigt) und speichern Sie den Feed.



Die folgende Tabelle zeigt die Spalten in der CSV-Datei für den NetWitness Endpoint-Feed.

Spalte	Name	Beschreibung	Spaltenname in NetWitness Suite (Metaschlüsselname)
1	MachineName	Hostname des Windows-Agent	alias.host
2	LocalIp	IPv4-Adresse	IP-Typ (indexierte Spalte)
3	RemoteIp	Entfernte IP, wie sie vom Router gesehen wird	stransaddr
4	GatewayIp	IP-Adresse des Gateways	gateway
5	MacAddress	MAC-Adresse	eth.src
6	OperatingSystem	Vom Windows-Agent verwendetes Betriebssystem	Betriebssystem
7	AgentID	Agent-ID des Hosts (eindeutige dem Agent zugewiesene ID)	Client
8	ConnectionUTCTime	Letzter Zeitpunkt, zu dem sich der Agent mit dem NetWitness Endpoint-Server verbunden hat	ecat.ctime
9	Quelldomain	Domain	domain.src
10	ScanUTC-Zeit	Zeitpunkt der letzten Überprüfung des Agent	ecat.stime
11	UserName	Benutzername des Clientcomputers	username
12	Maschinenbewertung	Wert, der das Verdachtslevel des Agent anzeigt	risk.num

Hinweis: In der Tabelle ist die empfohlene Indexeinstellung „LocalIp“. Wenn die LocalIp für den NetWitness Endpoint-Agent-PC von einem DHCP-Server zugewiesen wurde, die DHCP-Zuweisung abgelaufen ist und die IP-Adresse auf einem anderen PC erneut zugewiesen wird, sind die vom Feed erstellten Metadaten nicht korrekt. Verwenden Sie zur Vermeidung dieses Risikos den Computernamen oder die MAC-Adresse anstelle der localIP-Adresse als Feedindex. Wenn Sie beispielsweise eine MAC-Adresse verwenden, können Sie die Werte wie in der folgenden Abbildung gezeigt eingeben.



Ergebnis

Bei der Anzeige von Feeddaten in NetWitness Suite werden Metadaten in die Benutzeroberflächen „Investigation“, „Reporting“ und „Alerting“ übermittelt, wenn der Indexwert (ip.scr) übereinstimmt.

Konfigurieren von Endpoint-Warnmeldungen über Syslog in einen Log Decoder

Sie können die Verwendung von RSA NetWitness Endpoint-Daten in RSA NetWitness Suite konfigurieren, um NetWitness Endpoint-Warnmeldungen über Syslog in Log Decoder-Sitzungen bereitzustellen. Dadurch werden Metadaten erzeugt, die von NetWitness Suite Investigation, von Warnmeldungen und der Reporting Engine verwendet werden.

In NetWitness Suite-Netzwerken, die Protokolle nutzen, werden mithilfe dieser Integration von NetWitness Endpoint in NetWitness Suite NetWitness Endpoint-Ereignisse an den Log Decoder gesendet. Dies geschieht unter Verwendung von Syslog-Meldungen im CEF-Format (Common Event Format) und es werden Metadaten erzeugt, die von NetWitness Suite Investigation, von Warnmeldungen und der Reporting Engine verwendet werden. Anwendungsbeispiel für diese Integration ist die SIEM-Integration, um zentralisiertes Ereignismanagement, Korrelation von NetWitness Endpoint-Ereignissen mit anderen Log Decoder-Daten, NetWitness Suite-Reporting für NetWitness Endpoint-Ereignisse sowie NetWitness Suite-Warnmeldungen für NetWitness Endpoint-Ereignisse zu ermöglichen.

Voraussetzungen

Folgendes ist für diese Integration erforderlich:

- NetWitness Endpoint-Benutzeroberfläche der Version 4.3.0.4, 4.3.0.5 oder 4.4.
- NetWitness-Server 11.0 Version ist installiert.
- RSA Log Decoder und Concentrator Version 10.4 oder höher, die mit dem NetWitness-Server im Netzwerk verbunden sind.
- Offener Port UDP- 514 oder TCP - 1514 vom NetWitness Endpoint-Server zum Log Decoder in der Firewall.

Verfahren

1. Stellen Sie den erforderlichen Parser (CEF oder rsaecat) auf dem Log Decoder bereit, wie im Thema „Managen von Live-Ressourcen“ in *Life-Services-Management* beschrieben. Nachdem Sie den Parser bereitgestellt haben, stellen Sie sicher, dass der Parser aktiviert ist. Weitere Informationen finden Sie unter Ansicht „Services-Konfiguration“ – Registerkarte „Allgemein“.

Hinweis: Verwenden Sie nur einen dieser Parser. Wenn der CEF-Parser bereitgestellt wird, hat dieser Vorrang vor dem NetWitness Endpoint-Parser und alle CEF-Meldungen in NetWitness Suite werden vom CEF-Parser verarbeitet. Im Hinblick auf die Performance stellt die Aktivierung beider Parser eine unnötige Belastung dar.

2. Konfigurieren Sie NetWitness Endpoint für das Senden von Syslog-Ausgaben an NetWitness Suite und Erzeugen von NetWitness Endpoint-Warnmeldungen für den Log Decoder.
3. (Optional) Bearbeiten Sie die Tabellenzuordnung in `table-map-custom.xml` und `index-concentrator-custom.xml`, um Felder hinzuzufügen, die auf Benutzereinstellungen für Metadaten basieren, die NetWitness Suite zugeordnet werden sollen.

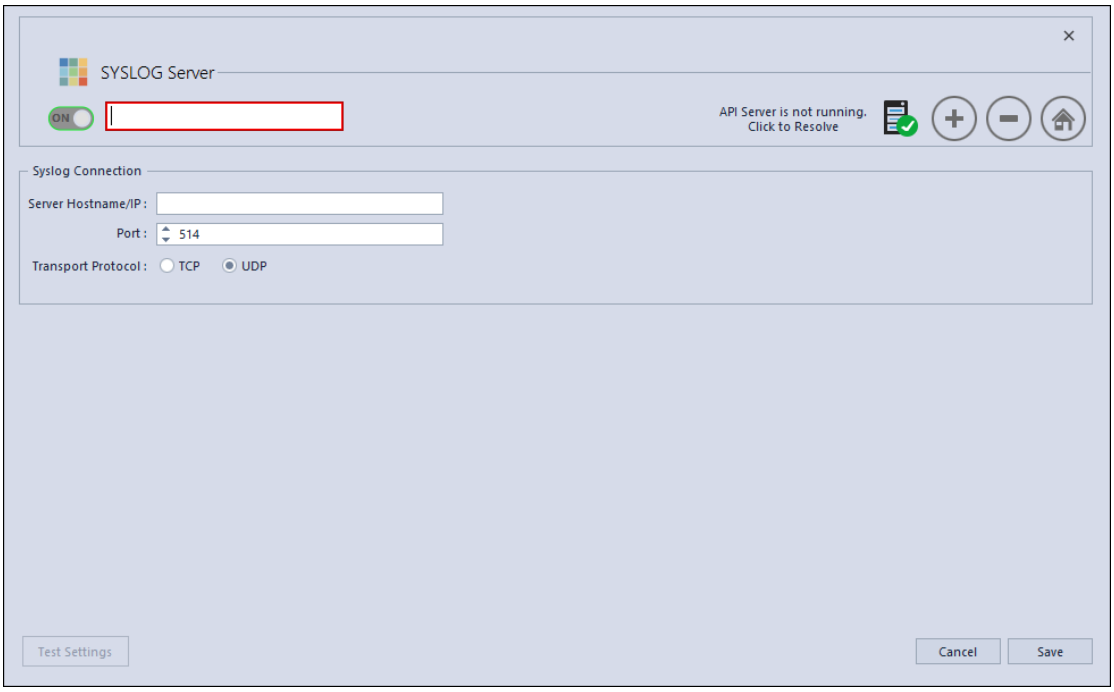
Konfigurieren von NetWitness Endpoint zum Senden von Syslog-Ausgaben an NetWitness Suite

So fügen Sie den Log Decoder als externe Syslog-Komponente hinzu und erzeugen NetWitness Endpoint-Warnmeldungen für den Log Decoder:

1. Öffnen Sie die NetWitness Endpoint-Benutzeroberfläche und melden Sie sich mit den richtigen Anmeldedaten an.
2. Wählen Sie in der Menüleiste **Konfigurieren > Überwachung und externe Komponenten** aus.

   Das Dialogfeld „Konfiguration externer Komponenten“ wird angezeigt.
3. Klicken Sie in **SYSLOG-Server** auf  .

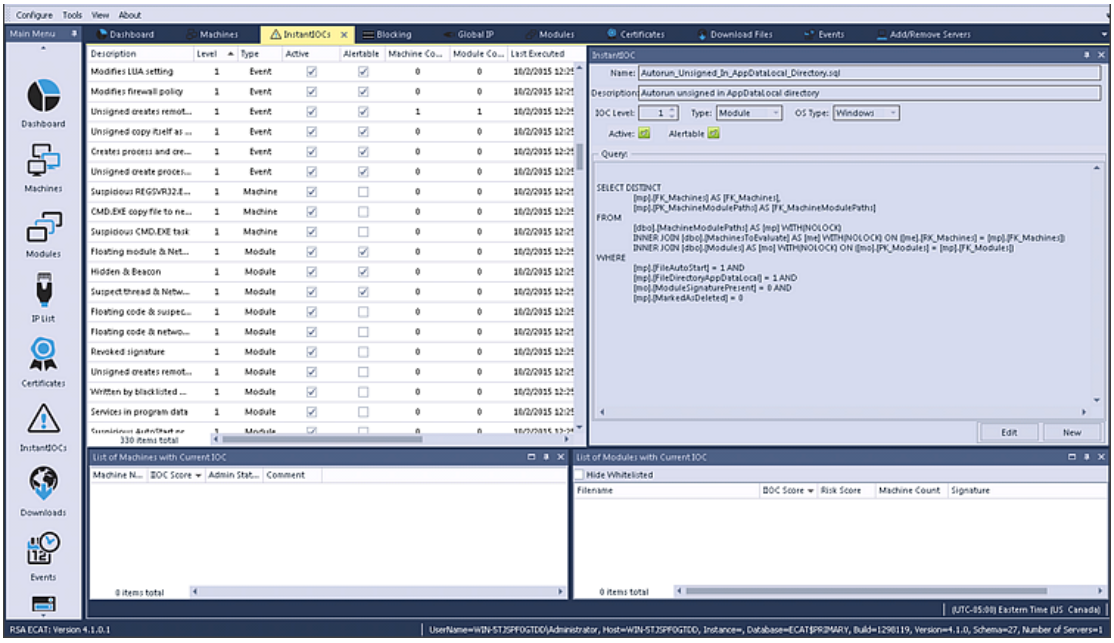
   Das Dialogfeld „SYSLOG-Server“ wird angezeigt.



4. Geben Sie im Bereich **NetWitness Suite** in **Ein** den beschreibenden Namen für den Log Decoder ein.
5. Führen Sie im Bereich **Syslog-Verbindung** die folgenden Schritte aus, um Syslog-Meldungen zu aktivieren:

   Hostname/IP des Servers = Hostnamens-DNS oder IP-Adresse des RSA Log Decoder
   Port = 514
   Transportprotokoll = Wählen Sie beim Transportprotokoll ihrem Syslog-Server entsprechend **UDP** oder **TCP** aus.
6. Klicken Sie auf **Speichern**.
7. Öffnen Sie das Fenster **InstantIOCs** in der NetWitness Endpoint-Benutzeroberfläche und klicken Sie in die Spalte **Warnpflichtig**, um jeden IIOC zu aktivieren, für den

Warnmeldungen an den Log Decoder gesendet werden sollen.



Bei Auslösung der Instant-IOCs werden Syslog-Warnmeldungen vom NetWitness Endpoint-Server an den Log Decoder gesendet. Die Log Decoder-Warnmeldungen werden dann für den Concentrator aggregiert. Diese Ereignisse werden als Metadaten in den Concentrator eingefügt.

Bearbeiten der Tabellenzuordnung in table-map-custom.xml

In der in RSA bereitgestellten standardmäßigen XML-Zuordnungstabelle table-map.xml ist für die Metaschlüssel in der Datei `table-map.xml` der Wert `Transient` festgelegt. Um die Metaschlüssel in Investigation anzuzeigen, muss `None` festgelegt werden. Um die Zuordnung zu ändern, müssen Sie die Einträge der `table-map-custom.xml` auf dem Log Decoder hinzufügen.

Im Folgenden finden Sie eine Liste der Metaschlüssel in `table-map.xml`.

NetWitness Endpoint-Felder	NetWitness Suite-Zuordnung	Vorübergehend in NetWitness Suite
agentid	Client	Nein
CEF-Header für Hostnamensfeld	alias.host	Nein

NetWitness Endpoint-Felder	NetWitness Suite-Zuordnung	Vorübergehend in NetWitness Suite
CEF-Header für Produktversion	version	Ja
CEF-Header für Produktname	Produkt	Ja
CEF-Header für Schweregrad	severity	Ja
CEF-Header für Signatur-ID	event.type	Nein
CEF-Header – Signaturname	event.desc	Nein
destinationDnsDomain	ddomain	Ja
deviceDnsDomain	domain	Ja
dhost	host.dst	Nein
dst	ip.dst	Nein
Ende	endtime	Ja
fileHash	Prüfsumme	Ja
fname	filename	Nein
fsize	filename.size	Ja
gatewayip	gateway	Ja
instantIOCLevel	threat.desc	Nein
instantIOCName	threat.category	Nein
machineOU	dn	Ja

NetWitness Endpoint-Felder	NetWitness Suite-Zuordnung	Vorübergehend in NetWitness Suite
machineScore	risk.num	Nein
md5sum	Prüfsumme	Ja
BS	Betriebssystem	Ja
port	ip.dstport	Nein
protocol	protocol	Ja
Nicht formatierte Meldung	msg	Ja
remoteip	stransaddr	Ja
rt	alias.host	Nein
sha256sum	Prüfsumme	Ja
shost	host.src	Nein
smac	eth.src	Ja
src	ip.src	Nein
start	starttime	Ja
suser	user.dst	Nein
timezone	timezone	Ja
totalreceived	rbytes	Ja
totalsent	bytes.src	Nein
useragent	user.agent	Nein
userOU	org	Ja

Die folgenden sieben Schlüssel befinden sich nicht in `table-map.xml`. Um diese Schlüssel in NetWitness Suite zu verwenden, müssen Sie sie zu `table-map-custom.xml` hinzufügen und die Flags auf `None` festlegen.

NetWitness Endpoint-Felder	NetWitness Suite-Zuordnung	Vorübergehend in NetWitness Suite
moduleScore	cs.modulescore	Ja
moduleSignature	cs.modulesign	Ja
Zielmodul	cs.targetmodule	Ja
YARA-Ergebnis	cs.yararesult	Ja
Quellmodul	cs.sourcemodule	Ja
OPSWATResult	cs.opswatresult	Ja
ReputationResult	cs.represult	Ja

Im Folgenden finden Sie die Einträge, die gegebenenfalls in `table-map-custom.xml` hinzuzufügen sind.

```
<mapping envisionName="cs_represult" nwName="cs.represult" flags="None"
envisionDisplayName="ReputationResult"/>
 <mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
 <mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
 <mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
 <mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
 <mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
 <mapping envisionName="cs_yararesult" nwName="cs.yararesult" flags="None"
envisionDisplayName="YaraResult"/>
```

Hinweis: Starten Sie den Log Decoder neu oder laden Sie die Protokollparser neu, damit die Änderungen wirksam werden.

Konfigurieren des NetWitness Suite Concentrator-Services

1. Melden Sie sich bei NetWitness Suite an und wechseln Sie zu **ADMIN** > **Services**.
    1. Wählen Sie einen Concentrator aus der Liste aus und wählen Sie **Ansicht** > **Konfiguration** aus.
2. Wählen Sie die Registerkarte **Dateien** aus und wählen Sie aus der Drop-down-Liste **Zu bearbeitende Dateien** die Datei **index-concentrator-custom.xml** aus.

3. Fügen Sie die NetWitness Endpoint-Metaschlüssel der Datei hinzu und klicken Sie auf **Anwenden**. Stellen Sie sicher, dass diese Datei die XML-Abschnitte bereits enthält; wenn die Zeilen nicht enthalten sind, fügen Sie sie hinzu.
4. Starten Sie den Concentrator.
5. Um den Concentrator als Datenquelle in der Reporting Engine hinzuzufügen, wählen Sie in der Ansicht **ADMIN** > **Services** die Reporting Engine aus und wählen Sie **Ansicht> Konfiguration > Quellen aus.**
   NetWitness Endpoint-Metadaten werden in Reporting Engine geladen und Sie können durch Auswahl der entsprechenden Metaschlüssel Berichte ausführen.

Beispiel

Hinweis: Die folgenden Zeilen sind Beispiele. Stellen Sie sicher, dass die Werte Ihrer Konfiguration und den Spaltennamen entsprechen, die Sie der Feeddefinition hinzugefügt haben, wobei gilt:
Beschreibung ist der Name des Metaschlüssels, der in NetWitness Suite Investigation angezeigt werden soll.
level entspricht „IndexValues“
name ist der NetWitness Endpoint-Metaschlüsselname aus der Tabelle unten

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
 <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
 <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
 <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
 <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
 <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
 <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
 <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
 <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
 <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.represult" valueMax="250000" defaultAction="Open"/>
 <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
 <key description="Module Sign" format="Text" level="IndexValues"
```

```
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
 <key description="opswat result" format="Text" level="IndexValues"
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
 <key description="source module" format="Text" level="IndexValues"
name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
 <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
 <key description="yara result" format="Text" level="IndexValues"
name="cs.yararesult" valueMax="250000" defaultAction="Open"/>
 <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
 <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
 <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
 <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
 <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
 <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
 <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
 <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
 <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
 </language>
```

Ergebnis

Analysten können:

- NetWitness Suite-Warnmeldungen auf Basis von NetWitness Endpoint-Ereignissen erstellen, indem sie NetWitness Endpoint-Ereignisse als Erweiterungsquelle auswählen.
- ESA-Regeln erstellen, indem sie NetWitness Endpoint-Metadaten wie im Thema „Hinzufügen von Regeln zur Regelbibliothek“ in *Handbuch Versenden von Warnmeldungen mit ESA* beschrieben, verwenden.
- Berichte zu NetWitness Endpoint-Ereignissen mithilfe von NetWitness Endpoint-Metadaten erstellen, wie im Thema „Konfigurieren einer Regel“ im *Reporting – Benutzerhandbuch* beschrieben.
- NetWitness Endpoint-Warnmeldungen in NetWitness Respond anzeigen, wie im Thema „Warnmeldungen anzeigen“ im *NetWitness Respond – Benutzerhandbuch* beschrieben.

- NetWitness Endpoint-Metaschlüssel zusammen mit standardmäßigen NetWitness Suite Core-Metaschlüsseln in Investigation anzeigen, wie im Thema „Durchführen einer Ermittlung“ in *Leitfaden Investigation und Malware Analysis* beschrieben.