RSA NETWITNESS® SUITE

Handbuch Live-Services-Management

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

Live-Services-Management

RSA NetWitness Suite Live ist ein Gateway zu einer umfassenden Umgebung, die den Zugriff auf Feeds, Tools und andere Ressourcen ermöglicht.

NetWitness Suite Live

Live ist die Komponente von NetWitness Suite für das Verwalten der Kommunikation und Synchronisation zwischen NetWitness Suite-Services und einer Bibliothek von Live-Inhalten, die RSA NetWitness Suite-Kunden zur Verfügung stehen. Live bietet eine einfache Benutzeroberfläche, um Inhalte aus dem NetWitness Suite Live-Contentmanagementsystem zu durchsuchen, auszuwählen und für NetWitness Suite-Services und -Software bereitzustellen. Live managt nicht nur Feeds von der CMS-Bibliothek, sondern ermöglicht darüber hinaus Benutzern, benutzerdefinierte Feeds und Pakete bereitzustellen.

Die CMS-Bibliothek

Die CMS-Bibliothek (Contentmanagementsystem; bekannt als *Live*) ist eine nützliche Quelle für die neuesten Internetsicherheitsressourcen für NetWitness Suite-Kunden. Sie bietet einen Blick in die kollektive Intelligenz und analytischen Fähigkeiten der weltweiten Sicherheitscommunity, um sicherzustellen, dass Benutzer die neuesten Einsichten in die Angriffsvektoren zur Verfügung haben.

Live sammelt die besten fortgeschrittenen Informationen und Inhalte in der globalen Sicherheitscommunity - die Ideen, Forschungen, kontinuierlichen Erfassungen und Analysen - und bringt sie direkt in die Sicherheitszentrale des Benutzers, um Rechner definitiv klassifizieren zu können, die mit Botnets, Schadsoftware und anderen böswilligen Angriffen konfrontiert sind. Live aggregiert, konsolidiert und klärt nur die relevantesten Informationen für eine Organisation auf Echtzeitbasis.

Feedback und Data Sharing in NetWitness Suite

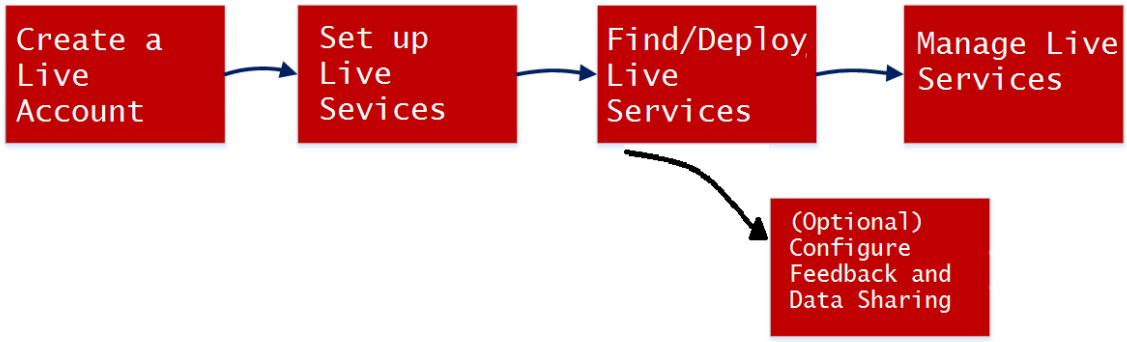
Live Feedback soll zur Verbesserung von RSA NetWitness Suite beitragen. Wenn Sie ein Live-Konto eingerichtet und konfiguriert haben, werden die Nutzungsdaten für RSA freigegeben.

Bei **RSA Live Connect** handelt es sich um einen cloudbasierten Bedrohungsinformationsservice. Der Service erfasst, analysiert und bewertet Daten zu Bedrohungen wie beispielsweise IP-Adressen, Domains und aus verschiedenen Quellen gesammelte Dateien. Er bietet die Funktion **Bedrohungseinblicke**, wodurch es Analysten möglich wird, Bedrohungsdaten aus dem Live Connect-Service abzurufen. Darüber hinaus gibt er Zugriff auf **Analystenverhalten**, einen automatisierten Datensammlungsservice, der das Ziel verfolgt, Informationen über potenzielle Bedrohungen für die Analyse freizugeben.

Weitere Informationen finden Sie in Feedback und Datenfreigabe in NetWitness Suite.

Live-Services – Obligatorische Verfahren

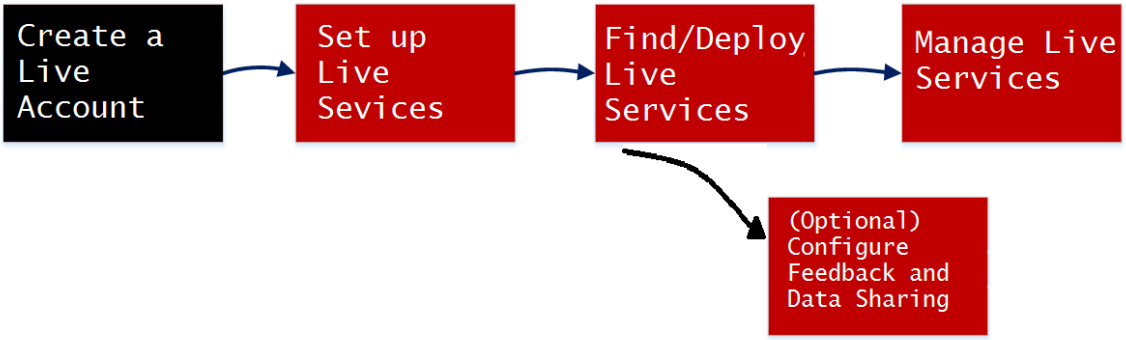
Die folgende Workflow unterteilt die grundlegende Einrichtung in vier Schritte, die Sie einzeln durchführen können. Die einfachste Methode für die Einrichtung des Decoders ist, dem durchgehenden Verfahren in diesem Abschnitt zu folgen, (Live-Services – Obligatorische Verfahren), das alle Schritte umfasst.



Konfigurationsschritt	Beschreibung
Erstellen eines Live-Kontos	Erstellen Sie im RSA Live Registration Portal unter dieser URL ein Live-Konto: https://cms.netwitness.com/registration/. Wenn Sie bereits über ein Konto verfügen, können Sie es in diesem Portal managen.
Einrichten von Live-Services in NetWitness Suite	Richten Sie Live-Services in NetWitness Suite ein, indem Sie eine Verbindung mit dem CMS-Server konfigurieren.
Suchen und Bereitstellen von Live-Ressourcen	Suchen Sie in der Ansicht „Live-Suche“ nach Ressourcen und stellen Sie die ausgewählten Ressourcen dann bereit.
Managen von Live-Ressourcen	Verfahren für Administratoren, um nach Ressourcen von Live zu suchen, diese zu abonnieren und sie bereitzustellen.
Feedback und Datenfreigabe in NetWitness Suite	Beschreibt die Funktionen für Feedback und Data Sharing in RSA NetWitness® Suite, von Live-Services. Die Teilnahme ist optional, kann jedoch dazu beitragen, dass die Community hilfreiche Bedrohungsinformationen zur Verfügung hat.

Erstellen eines Live-Kontos

Sie müssen ein Live-Konto mithilfe des RSA Live Registration Portal auf dem CMS-Server erstellen. Mit der CMS-Bibliothek können Sie an einer einzigen Stelle auf alle RSA-Inhalte zugreifen. Hier können Sie RSA-Inhalt anzeigen, suchen, bereitstellen und abonnieren. Sie müssen sich beim RSA Live-Registrierungsportal anmelden und eine Abonnementstufe auswählen.



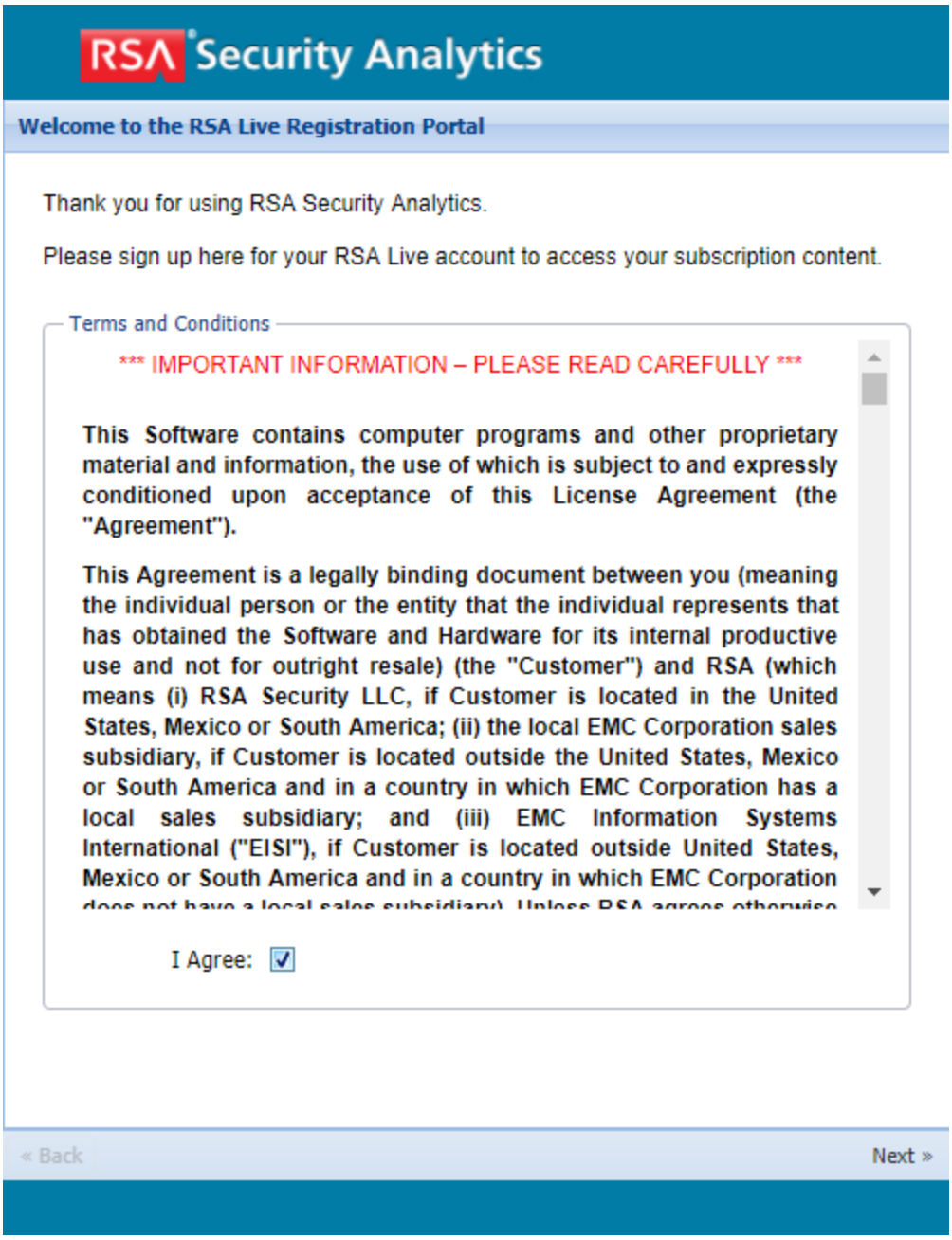
Vergewissern Sie sich, dass folgende Voraussetzungen für die Einrichtung eines RSA Live-Kontos erfüllt sind:

- Eine aktive Internetverbindung für den Zugriff auf das Portal muss vorhanden sein.
- Ein gültiger und registrierter NetWitness Suite-Lizenzserver muss auf dem Flexera-Server vorhanden sein, damit Sie sich für ein Live-Konto registrieren können. Sie können die Lizenz-ID im Bereich **ADMIN > System > Info** einsehen.

Hinweis: Wenn kein Lizenzserver eingerichtet ist, wenden Sie sich an den RSA-Kundendienst.

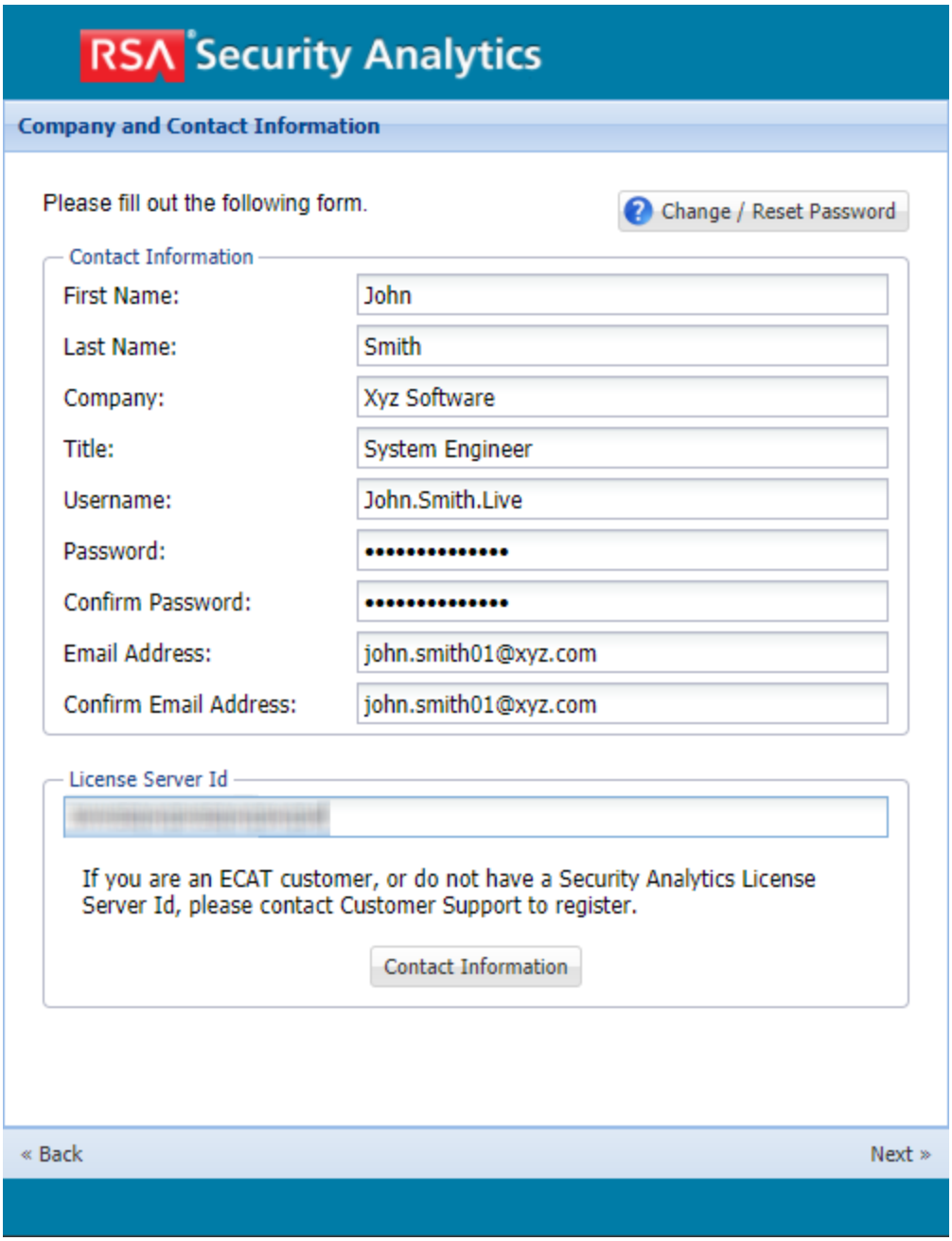
Hier können Sie ein Live-Konto erstellen:

1. Greifen Sie unter folgender URL auf das RSA Live Registration Portal zu: https://cms.netwitness.com/registration/.
   Die Begrüßungsseite wird angezeigt.
2. Lesen Sie sich die Allgemeinen Geschäftsbedingungen sorgfältig durch und aktivieren Sie das Kontrollkästchen **Akzeptieren** wie im Folgenden dargestellt:



3. Klicken Sie auf **Weiter**.
4. Füllen Sie im Abschnitt **Kontaktinformationen** alle Felder aus, wie im Folgenden dargestellt:
   - Der **Benutzername** muss aus mindestens 9 und maximal 60 Zeichen bestehen.
   - Das **Passwort** muss aus mindestens 9 und maximal 60 Zeichen bestehen und mindestens 1 Großbuchstaben, 1 Kleinbuchstaben, 1 Zahl und 1 Sonderzeichen enthalten.

- Geben Sie die **E-Mail-Adresse** ein, über die Sie Benachrichtigungen zu dem Live-Konto erhalten möchten.



5. Wählen Sie im Bereich **Abonnementstufe** eine der folgenden Abonnementstufen aus:
   - **Basic** – Dies bietet Zugriff auf Live-Inhalte, die für Gruppen wie Basic, Panorama for Log Decoder und Spectrum for Malware Analysis markiert sind.
   - **Enhanced** – Dies bietet Zugriff auf Live-Inhalte, die für Gruppen wie Enhanced, Basic, Panorama for Log Decoder und Spectrum for Malware Analysis markiert sind.

- **Premium** – Dies bietet Zugriff auf Live-Inhalte, die für Gruppen wie Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder und Spectrum for Malware Analysis markiert sind.

6. Wählen Sie im Abschnitt **Abonnementstufe bestätigen** zur Bestätigung die Abonnementstufe noch einmal aus.
7. Geben Sie die **Lizenzserver-ID** ein. Sie können die Lizenz-ID auf der Seite **ADMIN > SYSTEM > Info** einsehen.

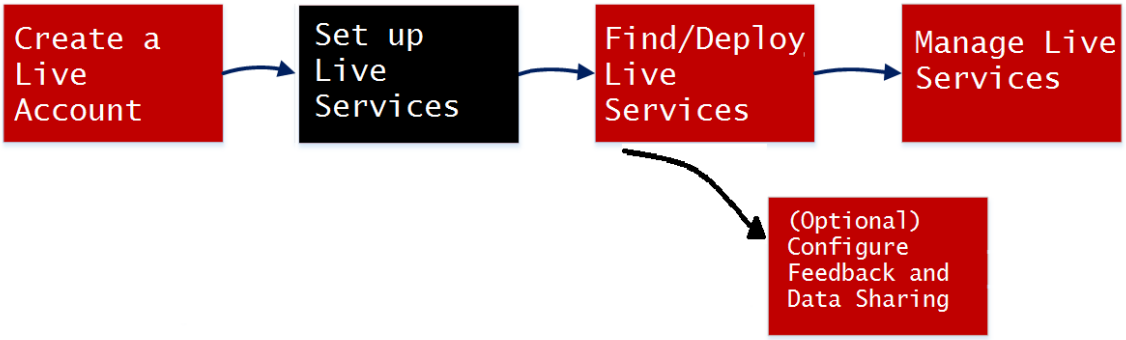
   Achtung: Überprüfen Sie, ob die Lizenzserver-ID in NetWitness Suite gültig ist und ob sie auf dem Flexera-Server registriert ist. Ist dies nicht der FalI, wenden Sie sich an den RSA Customer Service.

8. Klicken Sie auf **Weiter**.

Wenn die Registrierung erfolgreich ist, erhalten Sie eine E-Mail mit einer Bestätigung Ihres RSA Live-Kontos mit Ihrem Benutzernamen. Sie haben jetzt Zugriff auf die abonnierten Inhalte.

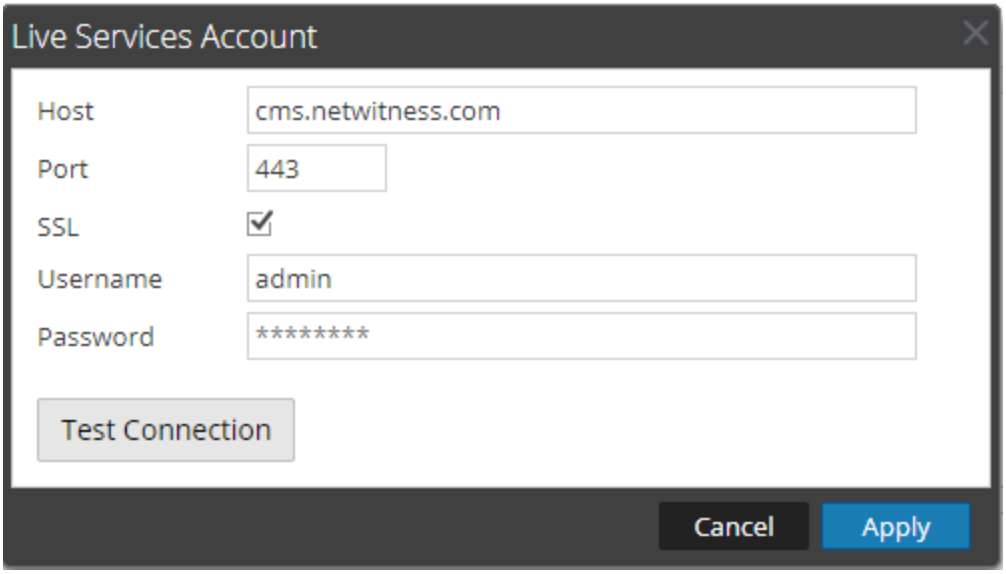
Einrichten von Live-Services in NetWitness Suite

Konfigurieren Sie die Verbindung und die Synchronisation zwischen dem CMS-Server und NetWitness Suite, um Live in NetWitness Suite einzurichten. Die zugehörige Benutzeroberfläche finden Sie unter „ADMIN“ > „System“ im Bereich „Live-Konfiguration“.



So konfigurieren Sie die Verbindung zum CMS-Server:

1. Konfigurieren Sie die Verbindung zum CMS-Server und das Live-Konto.

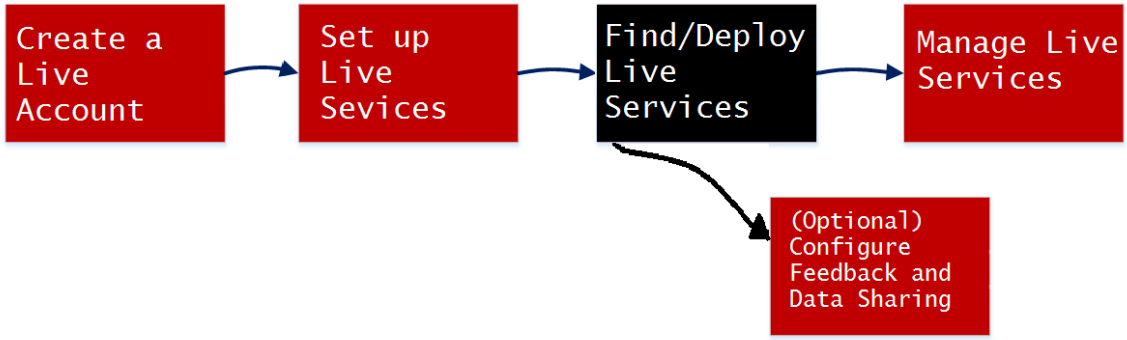


2. Konfigurieren Sie die Zeiteinstellungen für die Synchronisation von NetWitness Suite mit Aktualisierungen von Live.

Weitere Informationen finden Sie im Thema „Konfigurieren der Einstellungen von Live-Services“ im *Systemkonfigurationsleitfaden*.

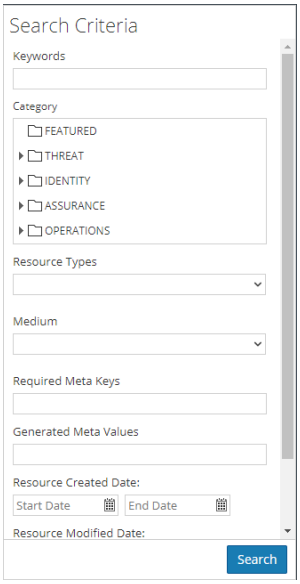
Suchen und Bereitstellen von Live-Ressourcen

Administratoren können in der Ansicht „Live-Suche“ nach Ressourcen suchen, was dem Durchsuchen des Live-CMS nach Ressourcen mithilfe des Bereichs „Suchkriterien“ in der Ansicht Live-Suche entspricht.



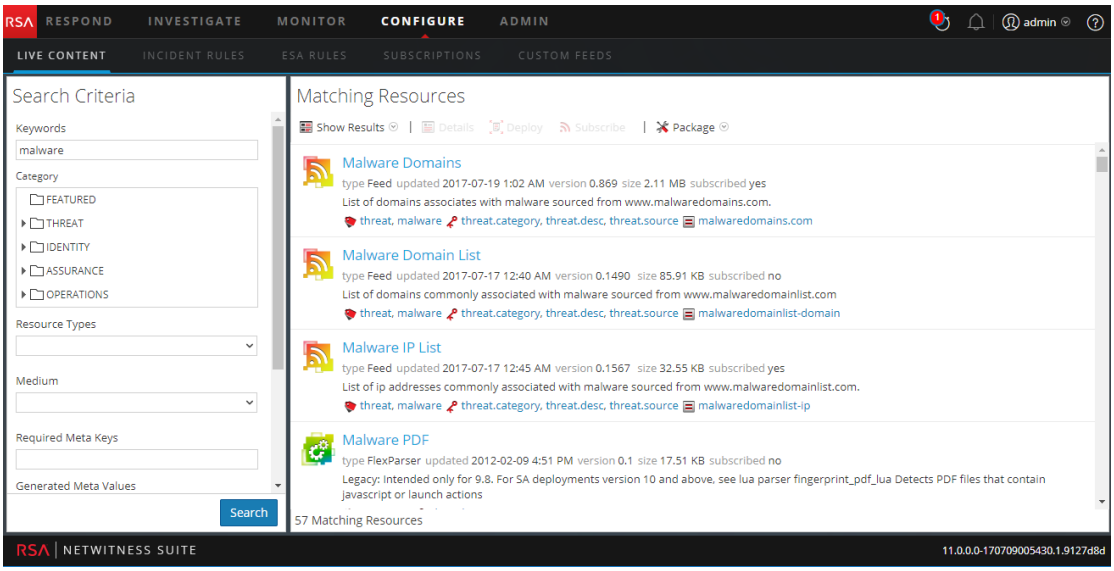
Finden von Ressourcen

1. Geben Sie im Bereich **Suchkriterien** die Suchkriterien an. Geben Sie einige oder alle der folgenden an: Schlüsselwort, Kategorie, Typ der Ressource, Mittel, Metaschlüssel, Metawerte und das Erstellungsdatum sowie das Datum der letzten Änderung der Ressource.



2. Klicken Sie auf **Suchen**.

   Detaillierte Ergebnisse werden im Bereich „Übereinstimmende Ressourcen“ angezeigt.



3. (Optional) Um die Ergebnisse im Bereich „Übereinstimmende Ressourcen“ weiter einzugrenzen, klicken Sie in einem Ergebnis auf ein Tag, einen Metaschlüssel, ein Medium oder einen Ressourcenmetawert.

Bereitstellen von Ressourcen in Live

In RSA NetWitness Suite können Sie ausgewählte Ressourcen mithilfe des Bereitstellungsassistenten manuell bereitstellen oder eine Gruppe von Ressourcen abonnieren.

- Wenn Sie beim Durchsuchen von Ressourcen in NetWitness Suite Live Ergebnisse erhalten haben, können Sie die Ressourcen für einen Service oder eine Servicegruppe manuell bereitstellen, ohne die Ressourcen abonnieren zu müssen.
- Durch die manuelle Bereitstellung von Ressourcen werden diese für die Services direkt bereitgestellt, ohne die leistungsstarken Ressourcenmanagementfunktionen von NetWitness Suite zu nutzen. Wenn Sie Benachrichtigungen und Updates zu aktualisierten Ressourcen erhalten und Ressourcen leicht aus einem Service entfernen können möchten, sollten Sie die Ressourcen jedoch in der Ansicht „Live-Suche“ abonnieren und sie in der Ansicht „Live-Konfigurieren“ bereitstellen.

Für manuelle Bereitstellungen ist dies die grundlegenden Verfahren:

1. Wählen Sie eine Ressource oder Gruppe von Ressourcen oder ein zuvor erstelltes Ressourcenpaket aus.
2. Klicken Sie auf „Breitstellen“. Der Bereitstellungsassistent wird gestartet.
3. Prüfen Sie die Liste der ausgewählten Ressourcen.

4. Wählen Sie die Services oder Servicegruppen aus, über die die ausgewählten Ressourcen bereitgestellt werden sollen.
5. Überprüfen Sie Ihre vorherige Auswahl.
6. Nehmen Sie die Bereitstellung vor.

Das folgende Verfahren beschreibt, wie Sie eine Gruppe von Ressourcen oder ein Ressourcenpaket bereitstellen:

- Sie können eine oder mehrere Ressourcen in der Live-Ressourcenansicht auswählen und sie dann für Services bereitstellen.
- Oder Sie können – wenn Sie zuvor ein Ressourcenpaket erstellt und gespeichert haben – das Paket für Services bereitstellen. Weitere Informationen dazu, wie Sie ein Paket erstellen, erhalten Sie in Assistent für die Ressourcenpaketbereitstellung.

So stellen Sie Ressourcen manuell bereit:

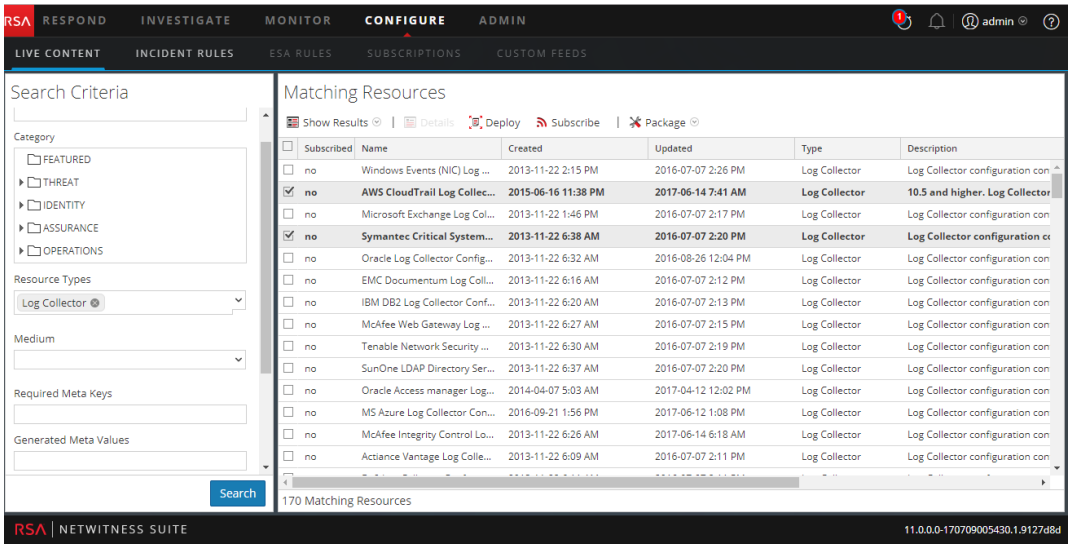
1. Navigieren Sie zu **KONFIGURIEREN > Live-Inhalte**.
2. Wählen Sie eine Gruppe von Ressourcen oder ein zuvor erstelltes Ressourcenpaket aus.

   So wählen eine Ressource oder Gruppe von Ressourcen aus:

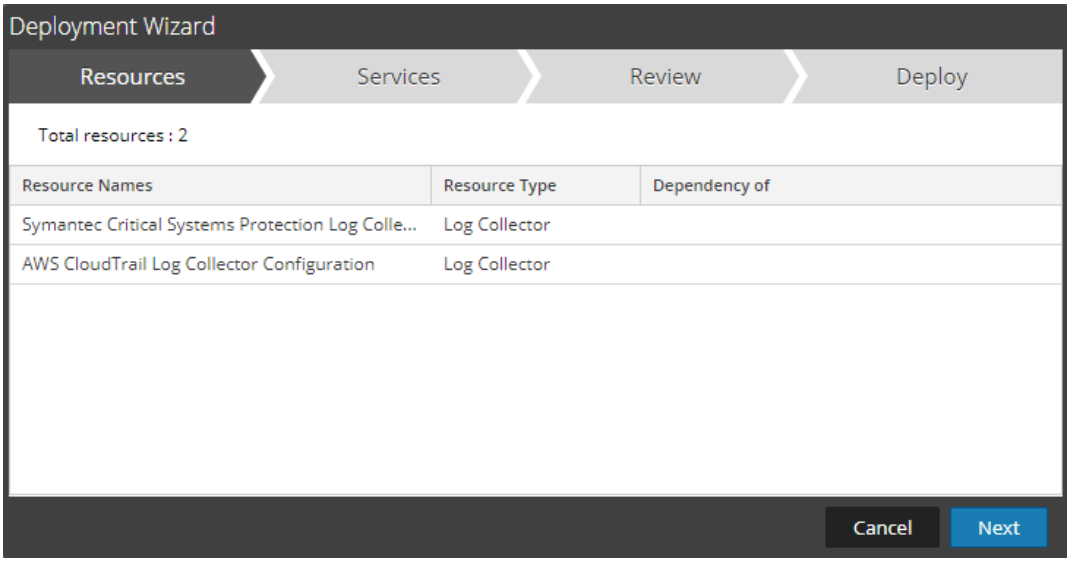
   a. Durchsuchen Sie in der **Ansicht „Live-Suche“** die Live-Ressourcen (suchen Sie z. B. nach dem Ressourcentyp **Log Collector**).

   b. Wählen Sie im Bereich **Übereinstimmende Ressourcen** die Optionen **Ergebnisse anzeigen > Raster** aus.

   c. Aktivieren Sie das Kontrollkästchen links neben den Ressourcen, die Sie bereitstellen möchten.



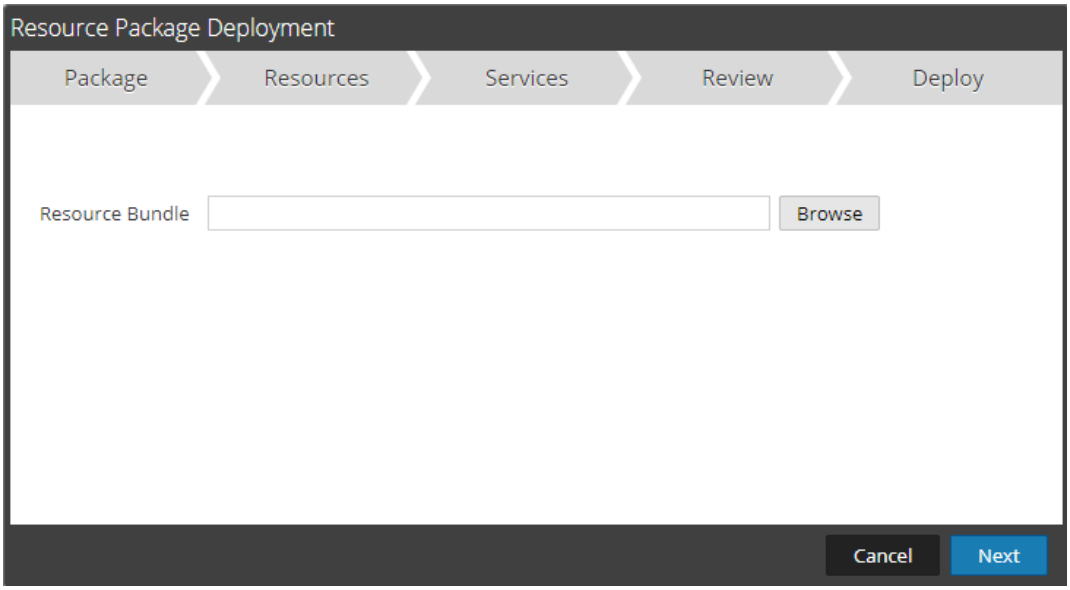
d. Klicken Sie auf der Symbolleiste „Übereinstimmende Ressourcen“ auf Deploy.



3. So wählen Sie ein Ressourcenpaket zur Bereitstellung aus:

a. Wählen Sie in der Ansicht **Live-Suche** auf der Symbolleiste **Übereinstimmende Ressourcen** die Optionen **Paket** > **Bereitstellen** aus.

Die Seite „Paket“ des Assistenten für die Ressourcenpaketbereitstellung wird angezeigt.



b. Klicken Sie auf „Durchsuchen“ und wählen Sie ein Paket in Ihrem Netzwerk aus (z. B. **resourceBundle-FeedsParsersContent.zip**).

c. Klicken Sie auf **Öffnen**.

An diesem Punkt wird unabhängig davon, ob Sie ein Paket oder eine Gruppe von Ressourcen bereitstellen, der **Bereitstellungsassisten** geöffnet und die Seite **Ressourcen** angezeigt.

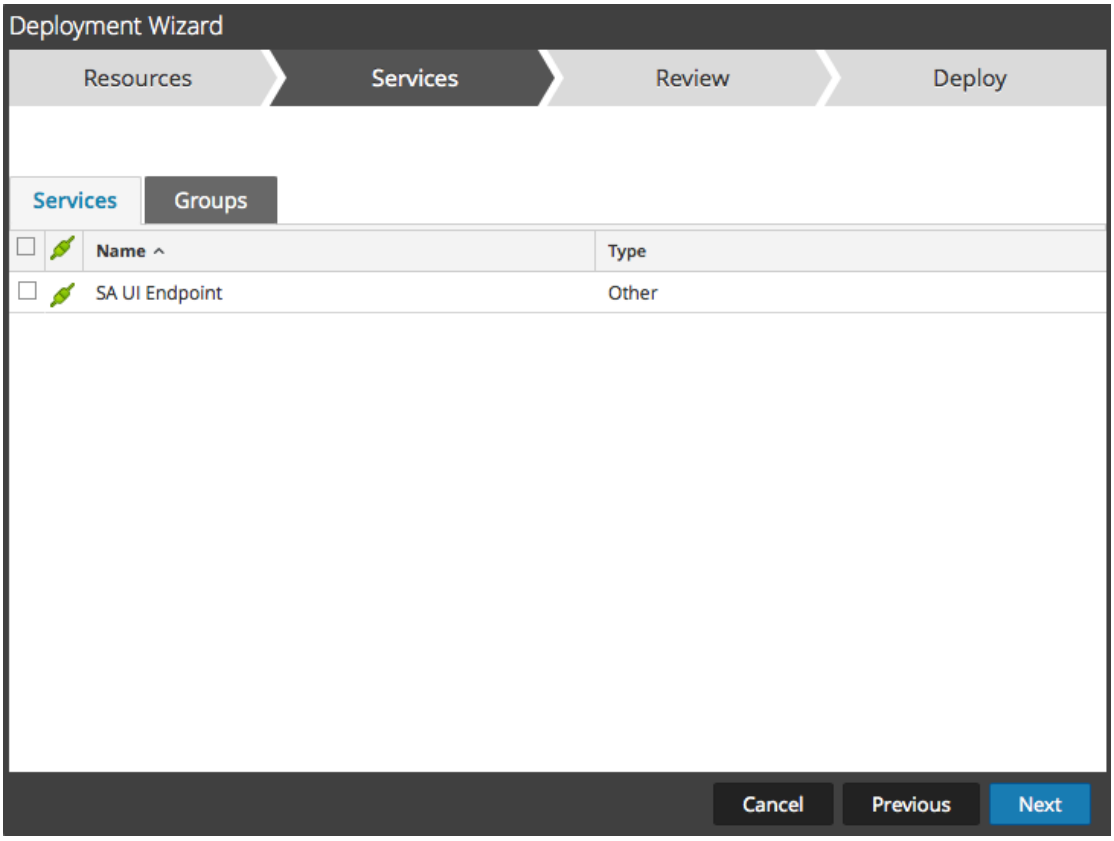
4. Klicken Sie auf **Weiter**.

   Die Seite **Services** mit zwei Registerkarten wird angezeigt: **Services** und **Gruppen**. Diese stellen eine Liste von Services und Servicegruppen bereit, die in der Ansicht „ADMIN“ > „Services“ konfiguriert werden. Die Spalten sind eine Untergruppe der Spalten, die in der Ansicht Services verfügbar sind.

   Hinweis: Die Live-Server stellt Ressourcen für Services auf intelligente Weise bereit. So stellt er Log Decodern keine Ressourcen bereit, die mittlere Pakete haben. Das bedeutet, dass nur relevante Inhaltsressourcen für Services bereitgestellt werden.

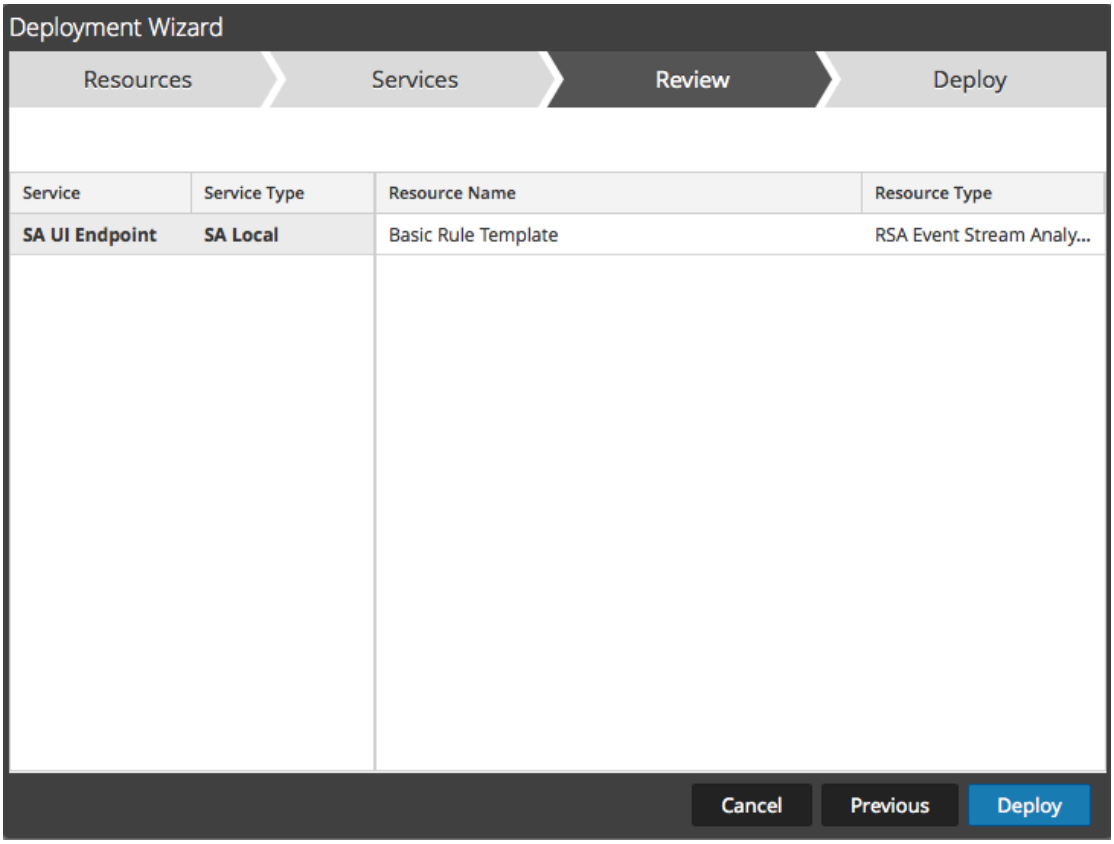
5. Wählen Sie die Services aus, für die Sie den Inhalt bereitstellen möchten. Sie können jede beliebige Kombination von Services und Servicegruppen auswählen.

   - Verwenden Sie die Registerkarte **Services**, um einzelne Services, Servicelisten und Servicegruppen auszuwählen, die in der Ansicht „ADMIN > Services“ konfiguriert sind.
   - Wählen Sie Gruppen von Services mithilfe der Registerkarte **Gruppen** aus.



6. Klicken Sie auf **Weiter**.

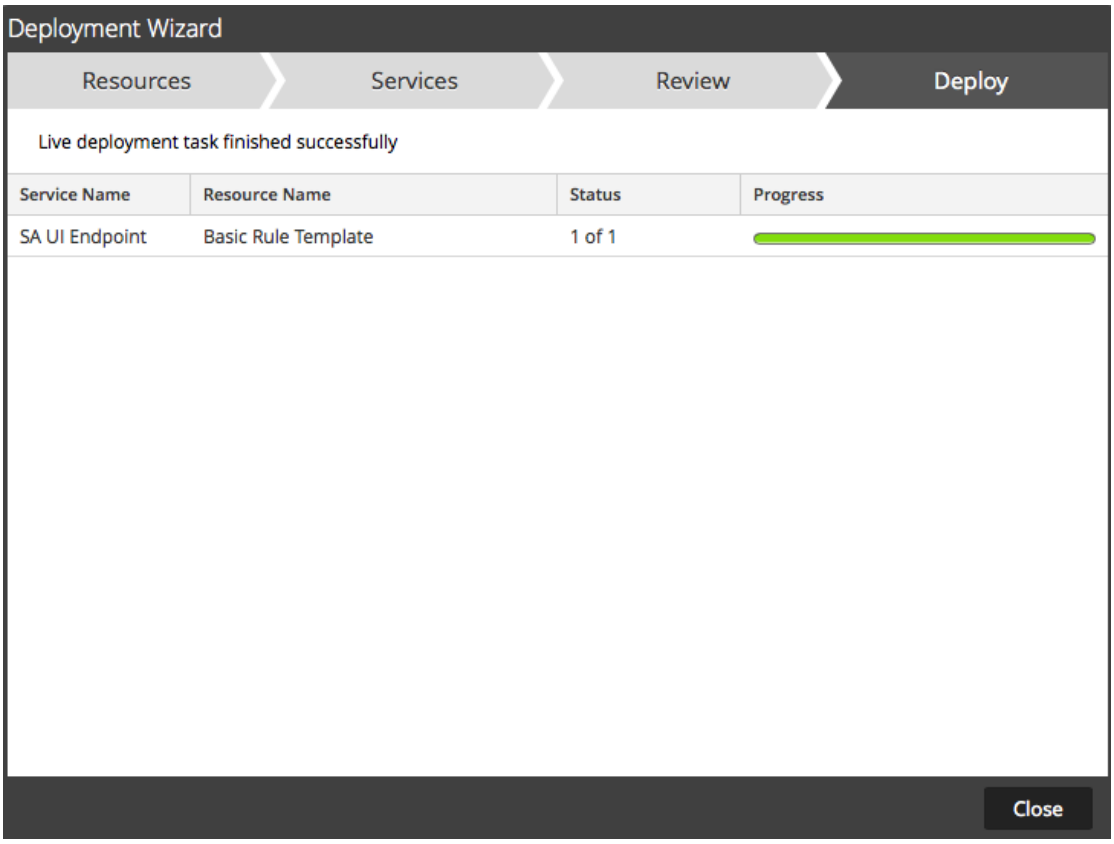
Die Seite **Überprüfung** wird angezeigt.



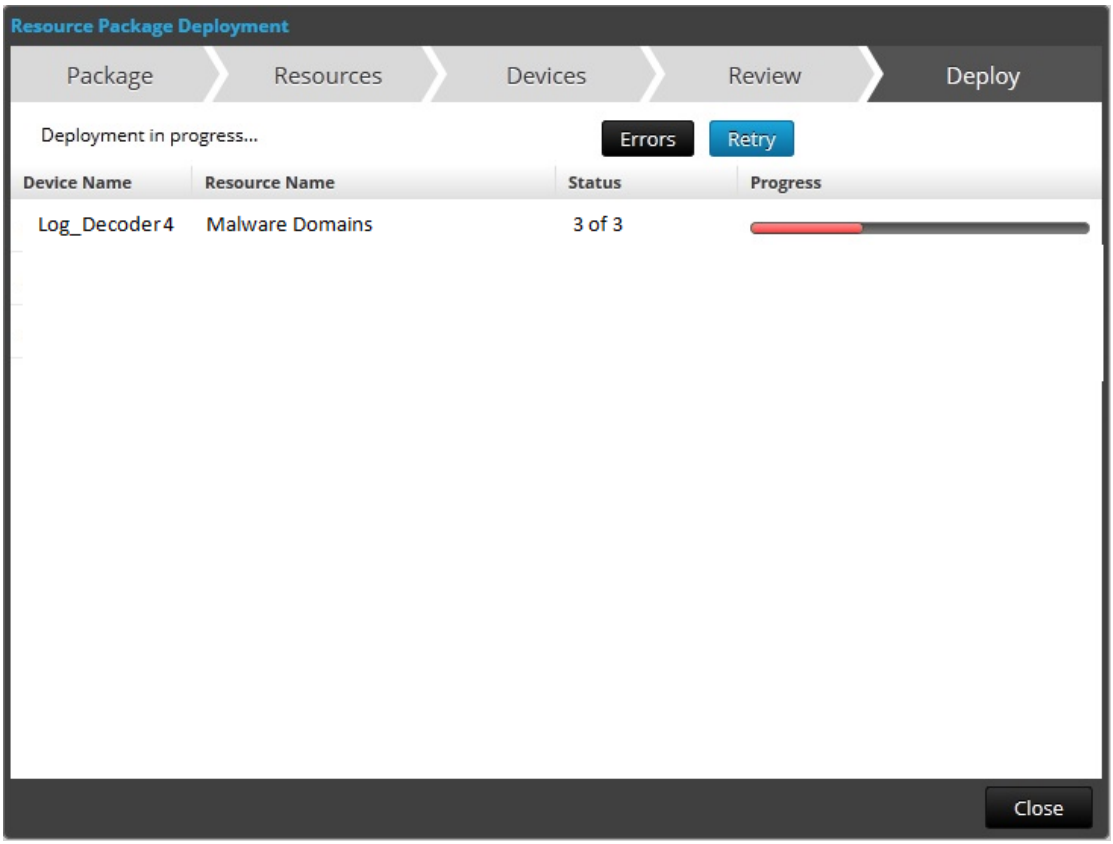
Stellen Sie sicher, dass Sie die korrekten Ressourcen und die Services ausgewählt haben, für die Sie sie bereitstellen möchten.

7. Klicken Sie auf **Bereitstellen**.

   Die Seite **Bereitstellen** wird angezeigt. Die Fortschrittsleiste wird grün, wenn die Ressourcen erfolgreich für die ausgewählten Services bereitgestellt wurden.



Wenn Sie versuchen, Ressourcen und Services bereitzustellen, die nicht kompatibel sind, werden in NetWitness Suite die Fehler und „Erneut versuchen“-Schaltflächen angezeigt. Sie können auf diese Schaltflächen klicken, um die Fehler zu überprüfen und die Bereitstellung erneut durchzuführen.



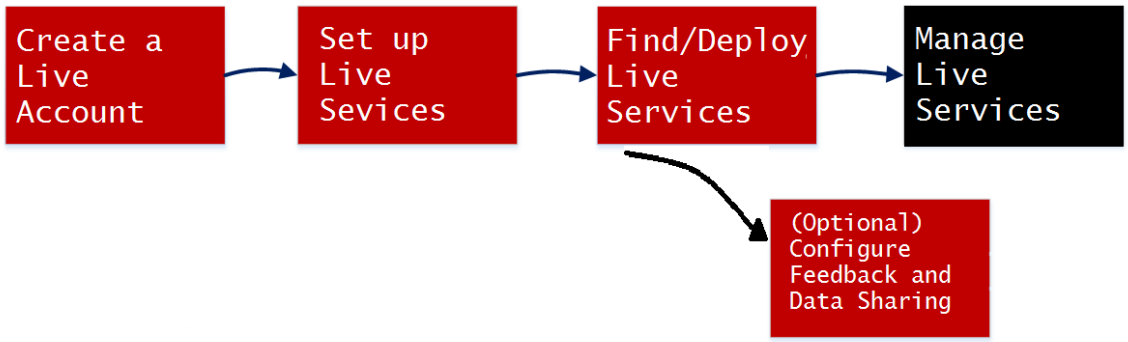
8. Klicken Sie auf **Schließen**.

Nächste Schritte

Nach der Bereitstellung von Parsern für Decoder und Log Decoder müssen Sie Parser auf den einzelnen Services aktivieren, wie in *Konfigurationsleitfaden für Decoder und Log Decoder* beschrieben.

Managen von Live-Ressourcen

Diese Verfahren sind erforderlich, wenn Administratoren Ressourcen in Live suchen, abonnieren und/oder bereitstellen möchten. Mit einer Verbindung zum CMS-Server können Sie im Rahmen Ihrer Abonnementstufe Ressourcen in Live suchen, abonnieren und bereitstellen. Wenn Sie Ressourcen gefunden haben, stellen Sie diese für Services und Servicegruppen bereit, die unter „Ansicht“ > „Services“ konfiguriert wurden.



Methoden

Es gibt mehrere mögliche Workflows für die Bereitstellung von Ressourcen für Services und das Management dieser Bereitstellungen. Dazu gehören:

- Abonnieren und Bereitstellen von Ressourcen
- Bereitstellen eines Ressourcenbündels
- Entfernen von Ressourcenbereitstellungen
- Herunterladen von Ressourcen
- Einrichten von Datenfeeds

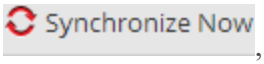
Verwalten von Abonnement und Bereitstellung

Der Abonnement- und Bereitstellungs-Workflow nutzt die in Live verfügbaren Ressourcenmanagementtools. Durch Abonnieren der Ressourcen stimmen Sie zu, aktualisierte Ressourcen entsprechend der Synchronisation zu empfangen, die im Bereich **ADMIN > Live-Konfiguration** konfiguriert wird.

Durch Hinzufügen abonnierter Ressourcen zur Bereitstellungsliste konfigurieren Sie NetWitness Suite so, dass diese Ressourcen gemäß den konfigurierten Synchronisationsintervallen automatisch per Push an die ausgewählten Services übertragen werden. Diese Methode setzt eine gewisse Planung der Servicegruppen und Services voraus, für die Ressourcen bereitgestellt werden. Ferner ist Folgendes anzumerken:

- Auf der Registerkarte Registerkarte „Bereitstellungen“ können Sie eine Ressource aus der Bereitstellungsliste entfernen.
- Auf der Registerkarte Registerkarte „Abonnements“ und in der Ansicht Live-Ressourcenansicht können Sie das Abonnement einer Ressource beenden.

So managen Sie Abonnements und Bereitstellungen:

1. Geben Sie im Bereich **ADMIN > SYSTEM > Live** ein Intervall an, in dem NetWitness Suite eine Überprüfung auf Aktualisierungen der abonnierten Ressourcen in Live durchführen soll. Geben Sie hier auch die E-Mail-Adressen der Personen an, die eine E-Mail-Nachricht über die aktualisierten, abonnierten Ressourcen empfangen sollen.
2. Suchen und abonnieren Sie Live-Ressourcen in der Ansicht **Live** > **Suche**.
3. Wählen Sie in der Ansicht **Live** > **Konfigurieren** auf der Registerkarte **Bereitstellungen** abonnierte Ressourcen aus und fügen Sie sie zur Bereitstellungsliste für Servicegruppen hinzu.
4. (Optional) Klicken Sie im Bereich **ADMIN**> **SYSTEM**> **Live** auf 

, um die auf der Registerkarte „Bereitstellungen“ aufgeführten Ressourcen sofort bereitzustellen.
5. Wählen Sie in der Ansicht **Live** > **Konfigurieren** auf der Registerkarte **Bereitstellungen** die bereitgestellten Ressourcen aus und entfernen Sie sie aus den Servicegruppen.
6. Beenden Sie die Abonnements der Ressourcen in der Ansicht **Live** > **Konfigurieren** auf der Registerkarte **Abonnements**.

Entfernen einer bereitgestellten Ressource

Sobald Live-Ressourcen für einen Service bereitgestellt wurden, verbleiben Sie im Service, bis sie entfernt werden. Es wird empfohlen, nicht verwendete Ressourcen aus den Services zu entfernen, für die sie bereitgestellt wurden.

Navigieren Sie zum Entfernen von Ressourcen zur Live-Ressourcenansicht, beenden Sie das Abonnement für eine Ressource und entfernen Sie die Ressource aus den Services, für die sie bereitgestellt wurde.

Bereitstellen eines Ressourcenbundles

Wenn Sie ein Inhaltspaket bereitstellen möchten, wählen Sie den Assistent für die Ressourcenpaketbereitstellung aus. Sie können ein Inhaltspaket, das in Live erstellt wurde, für einen oder mehrere Services bereitstellen. NetWitness Suite akzeptiert Pakete in **NWP**- oder **ZIP**-Dateien.

Herunterladen von Ressourcen

Sie können Live-Ressourcen in Ihr lokales Dateisystem herunterladen, indem Sie in der Ansicht „Live-Ressource“ auf die Schaltfläche **Herunterladen** klicken.

Einrichten von Datenfeeds

In der Ansicht **Live** > **Feeds** können Sie benutzerdefinierte Feeds und Identitätsfeeds einrichten und verwalten.

Zusätzliche Verfahren

In diesem Thema werden zusätzliche Verfahren für Administratoren beschrieben, die für die Konfiguration oder Verwendung von Live-Services nicht zwingend erforderlich sind.

Exportieren von Daten nach RSA

Ein NetWitness Suite-Administrator kann die Metriken in NetWitness Suite für Live Feedback exportieren.

Informationen über Live Feedback

Wenn das Live-Konto nicht konfiguriert ist, können Sie Nutzungsdaten manuell in RSA hochladen. Weitere Informationen finden Sie im Thema „Konfigurieren des Live-Services-Bereichs“ im *Systemkonfigurationsleitfaden*.

Der Live-Services-Konfigurationsbereich verfügt über ein Live-Feedback-Aktivitätsprotokoll, mit dem Sie die erforderlichen Nutzungsdaten für Live Feedback herunterladen können. Dies ist unabhängig von der Live-Konto-Konfiguration aktiv.

Sie können zunächst die Live Feedback-Verlaufsdaten herunterladen und danach hochladen, um sie mit RSA zu teilen

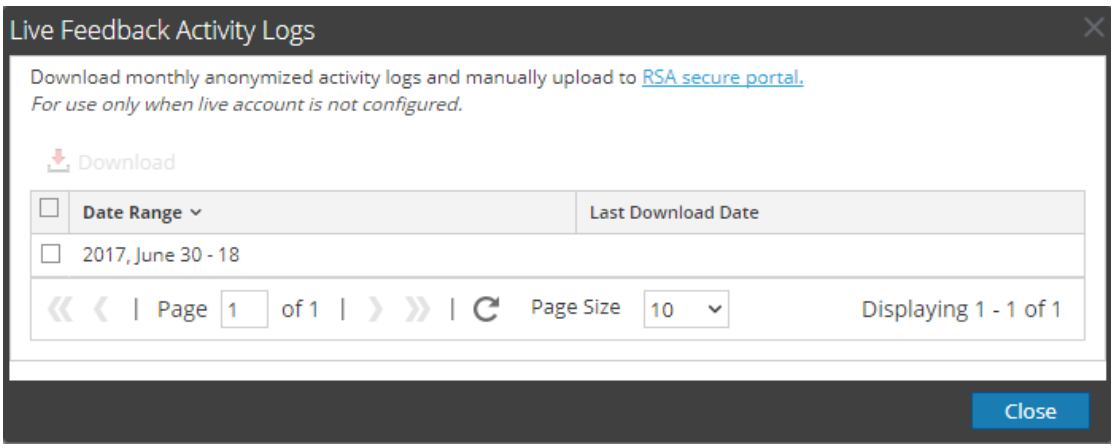
Herunterladen von Live Feedback-Verlaufsdaten

So laden Sie Live Feedback-Verlaufsdaten herunter:

1. Navigieren Sie zu **ADMIN** > **System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Live-Services** aus.

   Der Bildschirm **Live-Konto** wird angezeigt, auf dem der **RSA Live-Status** angezeigt wird und das **Live-Feedback-Aktivitätsprotokoll** heruntergeladen werden kann.
3. Klicken Sie auf **Live Feedback-Aktivitätsprotokoll herunterladen**.

   Das Fenster **Live Feedback-Aktivitätsprotokoll herunterladen** wird geöffnet, in dem Sie die erforderlichen Live Feedback-Verlaufsdaten herunterladen können.



4. Wählen Sie einen oder mehrere Einträge aus, indem Sie die Kontrollkästchen aktivieren, und

klicken Sie auf **Herunterladen**.

Hinweis: Wenn Sie mehrere Einträge in der Verlaufstabelle auswählen, besteht die heruntergeladene ZIP-Datei aus einer einzelnen JSON-Datei für jeden Monat.

Die heruntergeladenen Live Feedback-Daten haben das JSON-Format und sind in einer ZIP-Datei gepackt. Weitere Informationen finden Sie im Thema „Übersicht über Live Feedback“ im *Systemkonfigurationsleitfaden*.

Freigabe von Daten für RSA

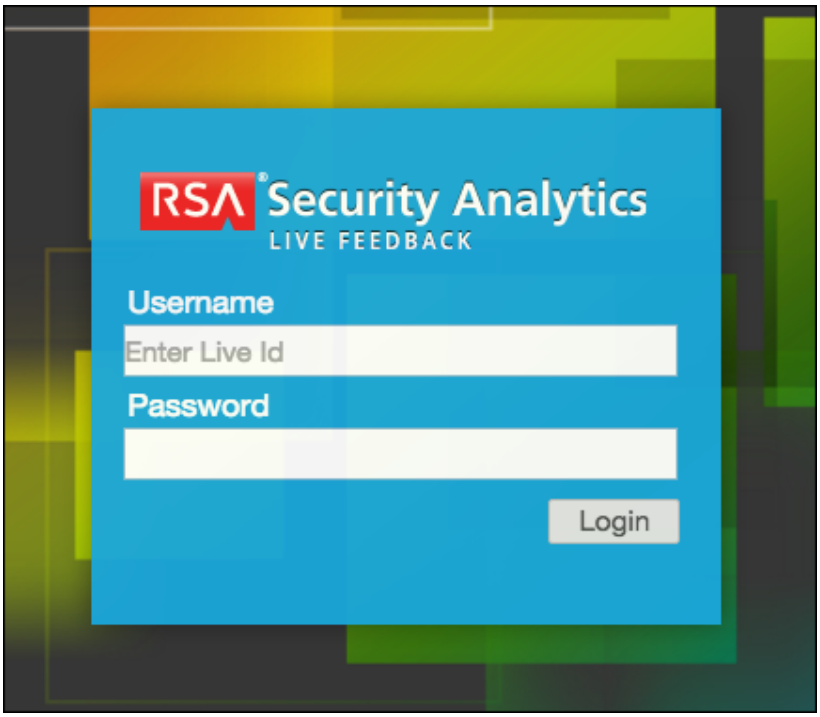
Nachdem Sie die Live Feedback-Daten heruntergeladen haben, können Sie sie mithilfe des folgenden Verfahrens hochladen.

So geben Sie die Daten für RSA frei:

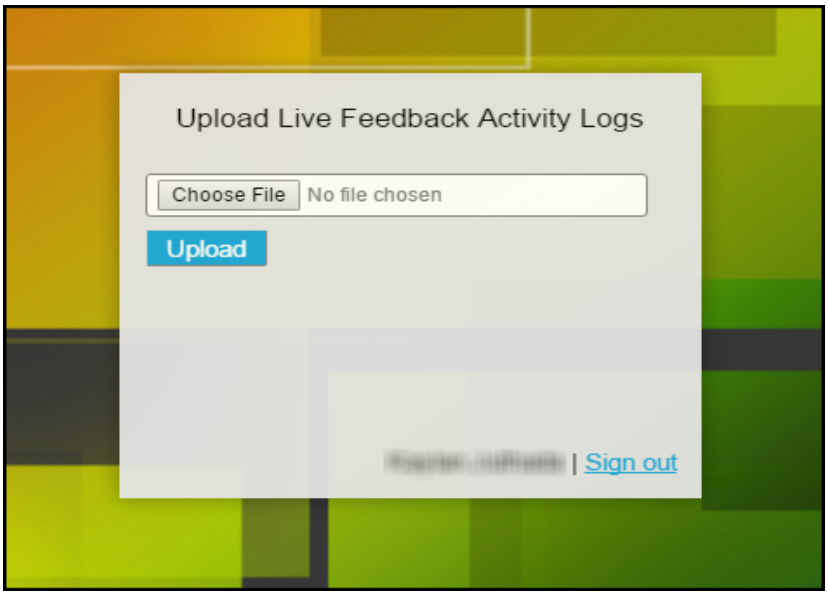
1. Klicken Sie auf das **sichere RSA-Portal**, das im Fenster **Live Feedback-Aktivitätsprotokolle** verfügbar ist.

   Der RSA NetWitness Suite Live Feedback-Anmeldebildschirm wird angezeigt.

2. Melden Sie sich beim Portal zum Hochladen der Live Feedback-Aktivitätsprotokolle mit Ihren Live-ID-Anmeldeinformationen an.



3. Klicken Sie auf **Live Feedback-Aktivitätsprotokoll herunterladen**.



4. Klicken Sie auf **Upload**.

Managen von benutzerdefinierten Feeds

Dieses Thema erläutert die Option zum Implementieren von benutzerdefinierten Feeds mithilfe des Assistenten für benutzerdefinierte Feeds in RSA NetWitness Suite um Decoder schnell mit benutzerdefinierten Feeds und Identitätsfeeds zu füllen.

Erstellung eines benutzerdefinierten Feeds

Mit dem Assistenten unter **Live** > **Feeds** > **Feed einrichten** > **Benutzerdefinierten Feed konfigurieren**können Sie schnell Decoderfeeds erstellen und anwenden. Diese Feeds basieren auf der deterministischen Logik, die speziell für die ausgewählten Decoder und Log Decoder Metaschlüssel bereitstellt. Auch wenn Sie der Assistent sowohl durch die Schritte zur Erstellung eines bedarfsorientierten Feeds als auch eines wiederkehrenden Feeds führt, sollten Sie das Format und den Inhalt einer Feeddatei bei der Erstellung eines Feeds verstehen.

Feeddateinamen in RSA NetWitness Suite haben das Format `<filename>.feed`. Um einen Feed zu erstellen, erfordert NetWitness Suite eine Feed**Datendatei** im `.csv`- oder `.xml` -Format (für STIX) und eine **Feeddefinitionsdatei** im `.xml`-Format, in der die Struktur einer Feeddatendatei beschrieben ist. Der Assistent für die Konfiguration eines benutzerdefinierten Feeds kann die Feeddefinitionsdatei basierend auf einer Feeddatendatei oder auf einer Feeddatendatei und der entsprechenden Feedkonfigurationsdatei erstellen.

Die Dateien, mit denen Sie einen bedarfsorientierten Feed erstellen, müssen in Ihrem lokalen Dateisystem gespeichert sein. Die Dateien, die zur Erstellung eines wiederkehrenden Feeds verwendet werden, müssen unter einer zugänglichen URL gespeichert werden, sodass NetWitness Suite die jeweils aktuelle Version der Datei bei jedem erneuten Aufruf abrufen kann. Nachdem ein NetWitness Suite-Feed erstellt wurde, können Sie diesen in Ihr lokales Dateisystem herunterladen, die Feeddateien bearbeiten und dann den NetWitness Suite-Feed bearbeiten, um die aktualisierten Feeddateien zu verwenden.

Beispiel für eine Feeddefinitionsdatei

Dies ist ein Beispiel für eine Feeddefinitionsdatei mit dem Namen `dynamic_dns.xml`, die NetWitness Suite auf Grundlage Ihrer Einträge in den Feedassistenten erstellt. Sie definiert die Struktur der Feeddatendatei namens `dynamic_dns.csv`.

Hinweis: Der Feeddateipfad sollte `.csv` sein, unabhängig vom Feedtyp (Standard oder STIX).

```
<?xml version="1.0" encoding="utf-8"?>
 <FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">

   <FlatFileFeed name="Dynamic DNS Domain Feed"
   path="dynamic_dns.csv"
   separator=","
   comment="#"
   version="1">

   <MetaCallback
   name="alias.host"
   valuetype="Text"
   apptype="0"
   truncdomain="true"/>

   <LanguageKeys>
            <LanguageKey name="threat.source" valuetype="Text" />
            <LanguageKey name="threat.category" valuetype="Text" />
            <LanguageKey name="threat.desc" valuetype="Text" />
   </LanguageKeys>

   <Fields>
   <Field index="1" type="index" key="alias.host" />
   <Field index="4" type="value" key="threat.desc" />
   <Field index="2" type="value" key="threat.source" />
   <Field index="3" type="value" key="threat.category" />
   </Fields>
   </FlatFileFeed>

 </FDF>
```

Feeddefinitions-Äquivalente für benutzerdefinierte Feed-Assistentenparameter

Der NetWitness Suite-Feed-Assistent verfügt über Optionen zum Definieren der Struktur der Datenfeeddatei. Diese entsprechen direkt Attributen in der Feeddefinitionsdatei (.xml).

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
Registerkarte **Feed definieren**	

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
Feedtyp	Wählen Sie Folgendes aus: **Standard** – zum Definieren eines Feeds auf Grundlage einer `.csv` -formatierten Feeddatendatei **STIX** – zum Definieren eines Feeds auf Grundlage einer STIX-formatierten `.xml` -Datei.
Typ der Feedaufgabe	Auswählen: **Ad-hoc** - zur Erstellung eines Feeds nach Bedarf. **Wiederkehrend** - zur Erstellung eines automatisch wiederkehrenden Feeds.
Name	Der benutzerdefinierte Feedname in der Feeddatendatei. Er entspricht dem Attribut **`flatfeedfile name`** in der Feeddefinitionsdatei; zum Beispiel Dynamic DNS Test Feed.
Datei/Durchsuchen	Dies ist der Name der Feeddatendatei. Er entspricht dem Attribut **`flatfeedfile path`** in der Feeddefinitionsdatei; zum Beispiel dynamic_dns.csv.
(STIX, wiederkehrend) **Allen Zertifikaten vertrauen**	Wählen Sie **Allen Zertifikaten vertrauen** aus, wenn Sie das Zertifikat des REST-Servers nicht überprüfen möchten. Diese Option ist standardmäßig aktiviert.
(STIX, wiederkehrend) **Zertifikat/Durchsuchen**	Klicken Sie für die Clientauthentifizierung mit der REST-URL im Feld **Zertifikat** auf **Durchsuchen** und wählen Sie das selbst signierte Zertifikat aus. Folgende Zertifikatformate werden unterstützt: CER, CRT mit Base64- und DER-kodierten Dateien.
Registerkarte **Feed definieren** - Erweiterte Optionen	
XML-Feeddatei	Der Name der Feeddefinitionsdatei, zum Beispiel `dynamic_dns.xml`..
Separator	Das verwendete Trennzeichen, um die Attribute in der Feeddatendatei voneinander zu trennen. Er entspricht dem **`flatfeedfile separator`** in der Feeddefinitionsdatei; zum Beispiel ein Komma.

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
Anmerkung	Das verwendete Zeichen, um einen Kommentar in der Feeddatendatei zu kennzeichnen. Er entspricht dem Attribut `flatfeedfile comment` in der Feeddefinitionsdatei, zum Beispiel #.
STIX-Daten entfernen, die älter sind als	Die Anzahl der Tage, über die die STIX-Pakete, die vom TAXII-Server heruntergeladen wurden, gespeichert werden müssen. Die STIX-Pakete, die älter als die angegebene Anzahl von Tagen sind, werden automatisch gelöscht. Der Standardwert beträgt 180 Tage, was auch dem Maximum entspricht.
Registerkarte Services auswählen	Wählen Sie die Services aus, an die Sie den Datenfeed senden möchten.
(Registerkarte Spalten definieren, Index definieren) **Typ**	Der Typ des Suchwerts in der Indexposition der Feeddatendatei. **IP** bedeutet, dass jede Zeile in der Feeddatendatei eine IP-Adresse in der Suchwertposition enthält. Der IP-Wert wird in Dezimalpunktschreibweise angegeben (Zum Beispiel 10.5.187.42). **IP-Bereich** bedeutet, dass jede Zeile in der Feeddatendatei einen IP-Adressbereich in der Suchwertposition enthält. Der IP-Bereich wird im CIDR-Format angegeben (zum Beispiel 192.168.2.0/24). **Nicht IP** bedeutet, dass jede Zeile in der Feeddatendatei einen Metadatenwert außer IP-Adressen in der Suchwertposition enthält. Die Felder Servicetyp, Domain abschneiden und Callback Keys werden für einen Nicht IP-Index aktiv.
(Registerkarte Spalten definieren, Index definieren) **CIDR**	Gibt an, dass der IP-Wert in der Suchwertposition im CIDR-Format ist. Das Attribut **CIDR** stellt das Format der IP-Adresse im Feld auf die CIDR-(Classless Inter-Domain Routing)-Notation ein.

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
(Registerkarte „Spalten definieren“, „Index definieren“) **Servicetyp**	Für einen Nicht IP-Index, der ganzzahlige Servicetyp, um Metasuchwerte zu filtern. Er entspricht dem Attribut **MetaCallback-Apptyp** in der Feeddefinitionsdatei. Ein Wert von **0** zeigt an, dass nicht nach Servicetyp gefiltert wird.
(Registerkarte „Spalten definieren“, „Index definieren“) **Domain abschneiden**	Für einen Nicht IP-Index, für Metawerte, die Domainnamen enthalten (zum Beispiel Hostnamen), kann das System das hostspezifische Element in den Daten entfernen. Domain abschneiden entspricht dem Attribut **MetaCallback truncdomain**. Wenn der Wert www.example.com ist, wird er auf example.com gekürzt. Ein Wert **Falsch** bedeutet, dass nicht gekürzt wird, **Wahr** bedeutet, dass gekürzt wird.
(Registerkarte „Spalten definieren“, „Index definieren“) **Callback-Schlüssel**	Für einen Nicht IP-Index sind die verfügbaren Metaschlüssel zur Zuordnung anstelle von ip.src/ip.dst (die Standards für den IP-Indextyp) aus der Drop-down-Liste auswählbar. Der Rückrufschlüssel entspricht dem Attribut **MetaCallbackname** und die Indexspalte der CSV-Datei muss die Daten enthalten, die zu dem ausgewählten Metaschlüssel passen. Wenn zum Beispiel der Metaschlüssel „Benutzername“ ausgewählt wurde, muss die Indexspalte der CSV-Datei dazu passende Benutzer enthalten.

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
(Registerkarte „Spalten definieren“, „Index definieren“) **Indexspalte**	Identifiziert die Spalte in der Feeddatendatei, die den Suchwert für die Zeile bereitstellt. Jede Position in jeder Zeile der Feeddatendatei wird durch ein **Feldindex**-Attribut in der Feeddefinitionsdatei identifiziert. Ein Feld mit einem Index von **1** ist der erste Eintrag in einer Zeile, das zweite Feld hat einen Index von **2**, das dritte Feld hat einen Index von **3** und so weiter. Sie können mehrere Indexspalten auswählen, wenn der **Feedtyp STIX** und der **Indextyp Nicht IP** ist. Wenn Sie mehrere Indexspalten auswählen, werden die Werte aus allen ausgewählten Spalten in der ersten Indexspalte zusammengeführt, die Sie ausgewählt haben.
(WERTE DEFINIEREN)**Schlüssel**	Der Name des **LanguageKey**, wie in der Feeddefinitionsdatei definiert, für den Metadaten von dieser Zeile der Feeddatendatei erstellt werden. Er entspricht dem Attribut **Feldschlüssel** in der Feeddefinitionsdatei. Ein Schlüssel gilt nur für ein Feld, dessen Typ auf **Wert** eingestellt ist. In der Feeddefinitionsdatei gibt es eine Liste von LanguageKeys von **index.xml** oder ein zusammenfassender Name, wenn Quellenname und Zielname verwendet werden. (Zum Beispiel ist **reputation** ein zusammenfassender Name für **reputation.src** und **reputation.dst**). Dieser Wert wird durch das Attribut Feldschlüssel referenziert.

Nächste Schritte

- Erstellen eines benutzerdefinierten Feeds
- Erstellen und Verwalten eines Identitätsfeeds
- Bearbeiten eines Feeds
- Entfernen eines Feeds

Erstellen eines benutzerdefinierten Feeds

Dieses Thema enthält Anweisungen zur Erstellung eines benutzerdefiniertes Feeds mithilfe einer CSV- oder STIX-formatierten Feeddatendatei in RSA NetWitness Suite.

Hinweis: Version 10.6.1 und neuere Versionen von NetWitness Suite unterstützen Structured Threat Information Expression (STIX). Weitere Informationen zu STIX und dem Erstellen eines benutzerdefinierten STIX-Feeds finden Sie in Erstellen eines benutzerdefinierten STIX-Feeds.

Mit dem Assistenten für benutzerdefinierte Feeds können Sie auf einfache Weise einen benutzerdefinierten Feed erstellen. Zum Abschluss dieses Verfahrens benötigen Sie eine Feeddatendatei im `.csv`- oder `.xml`-Format. Wenn Sie auch eine zugeordnete Feeddefinitionsdatei im `.xml`-Format haben, die die Struktur der Feeddatendatei beschreibt, können Sie die Feeddefinitionsdatei verwenden, um einen Feed zu erstellen. Der Assistent für benutzerdefinierte Feeds kann den Feed basierend auf einer Feeddatendatei oder basierend auf einer Feeddatendatei und der entsprechenden Feeddefinitionsdatei erstellen.

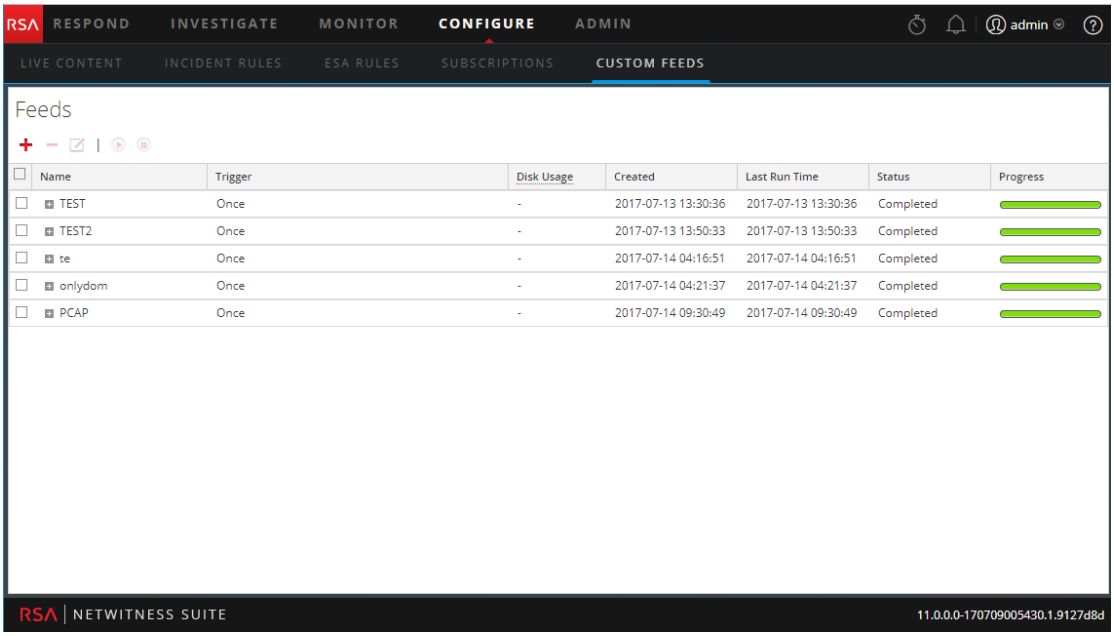
Nach Abschluss dieses Verfahrens werden Sie einen benutzerdefinierten Feed erstellt haben.

Für einen bedarfsorientierten benutzerdefinierten Feed müssen die Feeddatendatei (`.csv` oder STIX [`.xml`]) und optional die Feeddefinitionsdatei (`.xml`) auf dem lokalen Dateisystem verfügbar sein. Für einen wiederkehrenden benutzerdefinierten Feed müssen die Dateien unter einer URL verfügbar sein, auf die der NetWitness Suite-Server Zugriff hat.

So erstellen Sie einen benutzerdefinierten Feed:

1. Navigieren Sie zu **KONFIGURIEREN > BENUTZERDEFINIERTE FEEDS**.

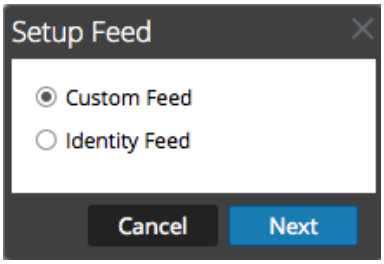
   Die Ansicht „Benutzerdefinierte Feeds“ wird angezeigt.



2. Klicken Sie auf der Symbolleiste auf

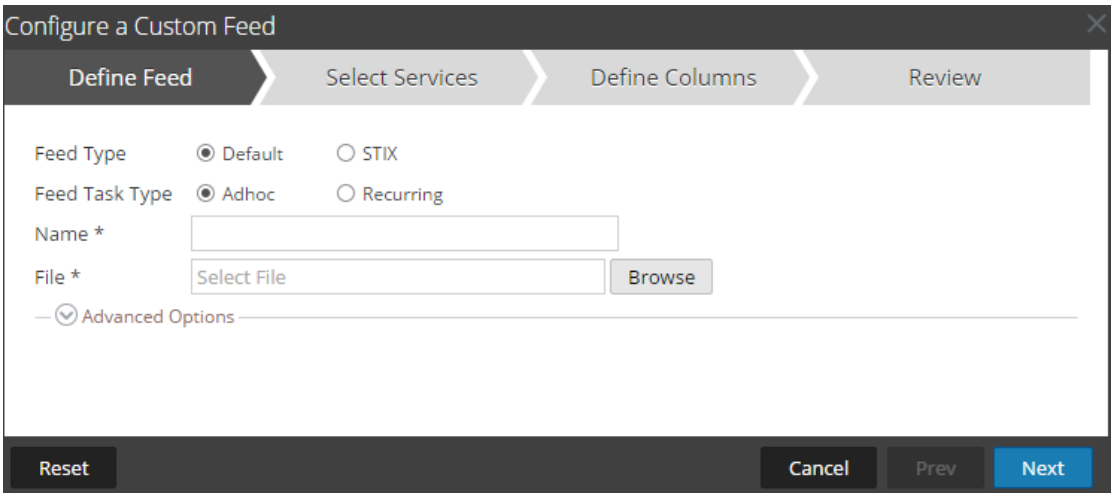
+.

Das Dialogfeld Feed einrichten wird angezeigt.



3. Um den Feedtyp auszuwählen, klicken Sie auf **Benutzerdefinierter Feed** und auf **Weiter**.

   Der Assistent Benutzerdefinierten Feed konfigurieren wird mit geöffnetem Formular Feed definieren angezeigt.

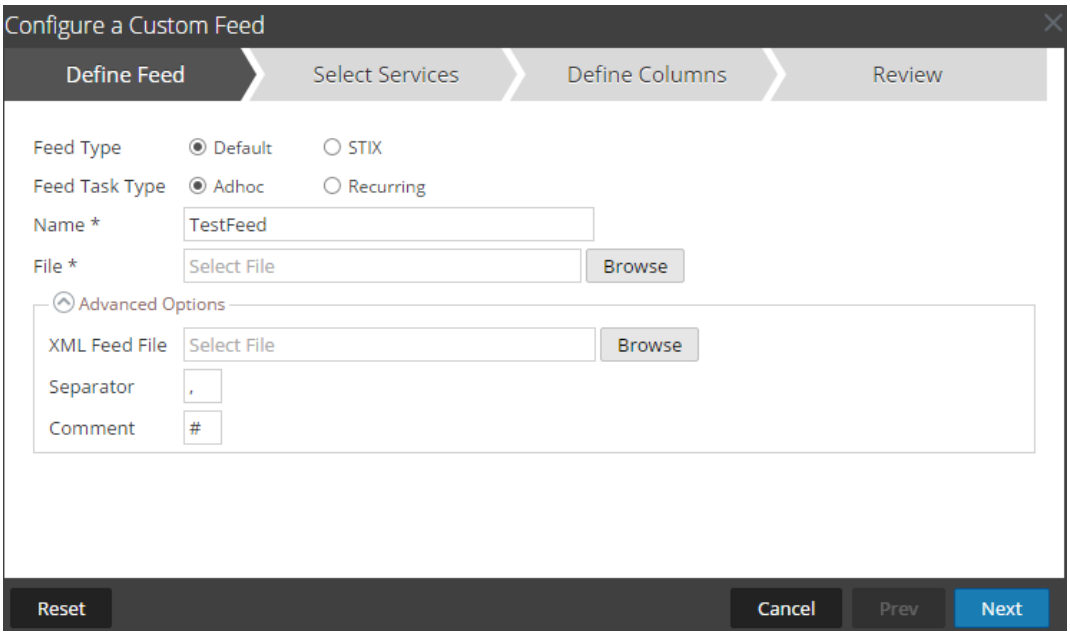


4. Definieren Sie einen Feed auf Grundlage einer `.csv`-formatierten Feeddatendatei, indem Sie im Feld **Feed-Typ** die Option **Standard** auswählen.
5. Um eine bedarfsorientierte Feedaufgabe zu definieren, die einmal ausgeführt wird, wählen Sie im Feld **Typ der Feedaufgabe** die Option **Ad-hoc** aus und fahren Sie mit einer der folgenden Aktionen fort:

   a. (Bedingungsabhängig) Um einen auf einer .csv-formatierten Datendatei basierenden Feed zu definieren, geben Sie einen **Namen** für den Feed ein, wählen Sie als **Datei** eine .csv-Inhaltsdatei im lokalen Dateisystem aus und klicken Sie auf **Weiter**.

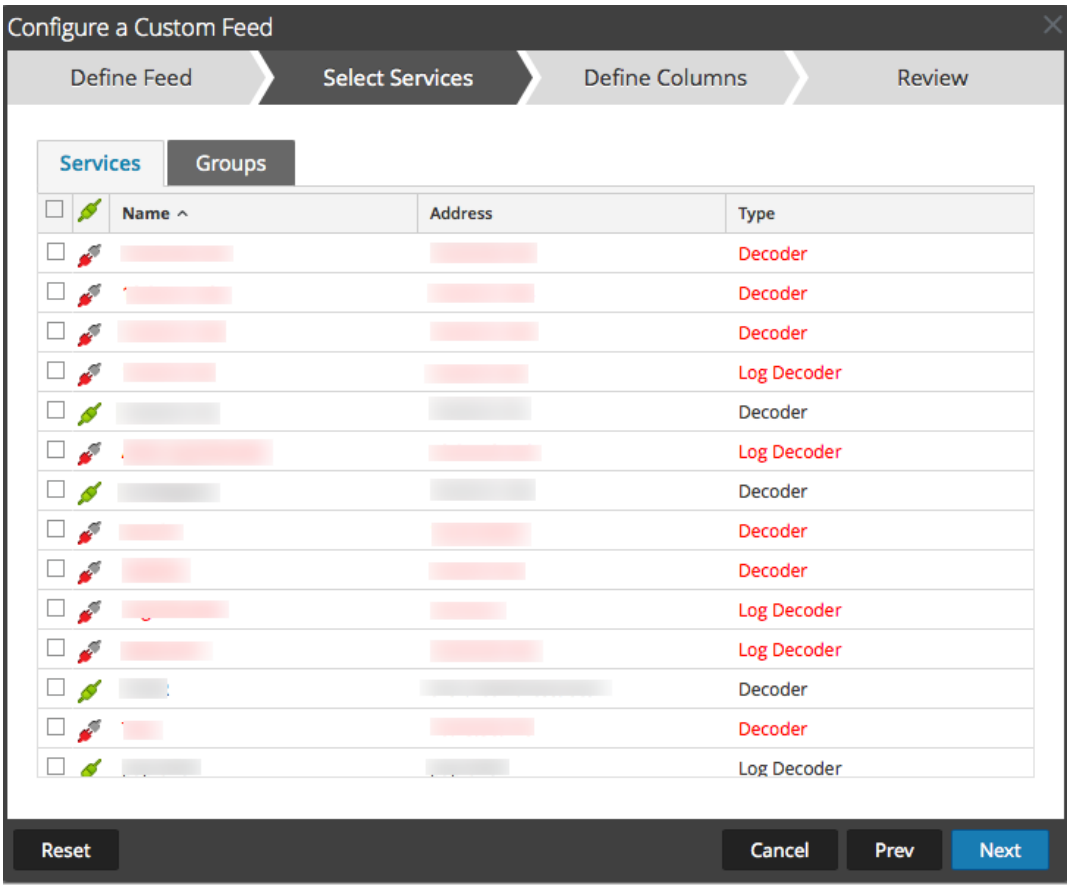
   b. (Bedingungsabhängig) Um einen auf einer XML-Feeddatei basierenden Feed zu definieren, wählen Sie **Erweiterte Optionen** aus.

      Erweiterte Optionen werden angezeigt:



c. Wählen Sie eine XML-Feeddatei aus dem lokalen Dateisystem aus. Treffen Sie eine Auswahl für das **Trennzeichen** (Standard ist Komma), legen Sie die Kommentar**zeichen** fest, die in der Feeddatendatei verwendet werden (Standard ist #), und klicken Sie auf **Weiter**.

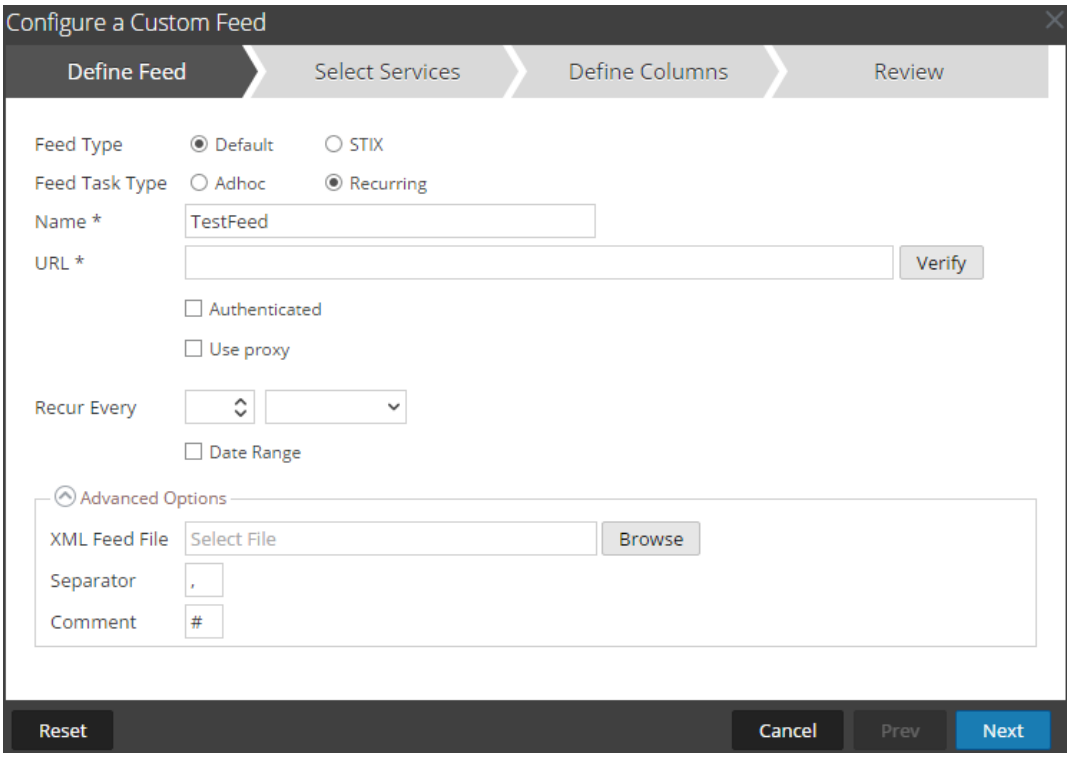
d. Das Formular Services auswählen wird angezeigt. Dies ist ein Beispiel eines Formulars für einen Feed, der auf einer Feeddatendatei ohne Feeddefinitionsdatei basiert. Wenn Sie einen Feed definieren, der auf einer Feeddefinitionsdatei basiert, ist die Registerkarte Spalten definieren nicht erforderlich.



6. So definieren Sie einen wiederkehrenden Feed, der innerhalb eines bestimmten Datumsbereichs in spezifischen Zeitabständen wiederholt ausgeführt wird:

   a. Wählen Sie im Feld **Typ der Feedaufgabe** die Option **Wiederkehrend** aus.

      Das Formular Feed definieren enthält die Felder für einen wiederkehrenden Feed.



b. Geben Sie im Feld **URL** die URL ein, unter der sich die Feeddatendatei befindet, z. B. `http://<hostname>/<feeddatafile>.csv`, und klicken Sie auf **Überprüfen**.

   NetWitness Suite verifiziert den Speicherort, an dem die Datei hinterlegt ist, sodass NetWitness Suite bei jedem erneuten Aufruf automatisch nach der aktuellen Datei suchen kann.

c. (Optional) Wenn der Zugriff auf die URL beschränkt ist und eine Authentifizierung mithilfe Ihres Benutzernamens und Passworts erfordert, wählen Sie **Authentifiziert** aus.

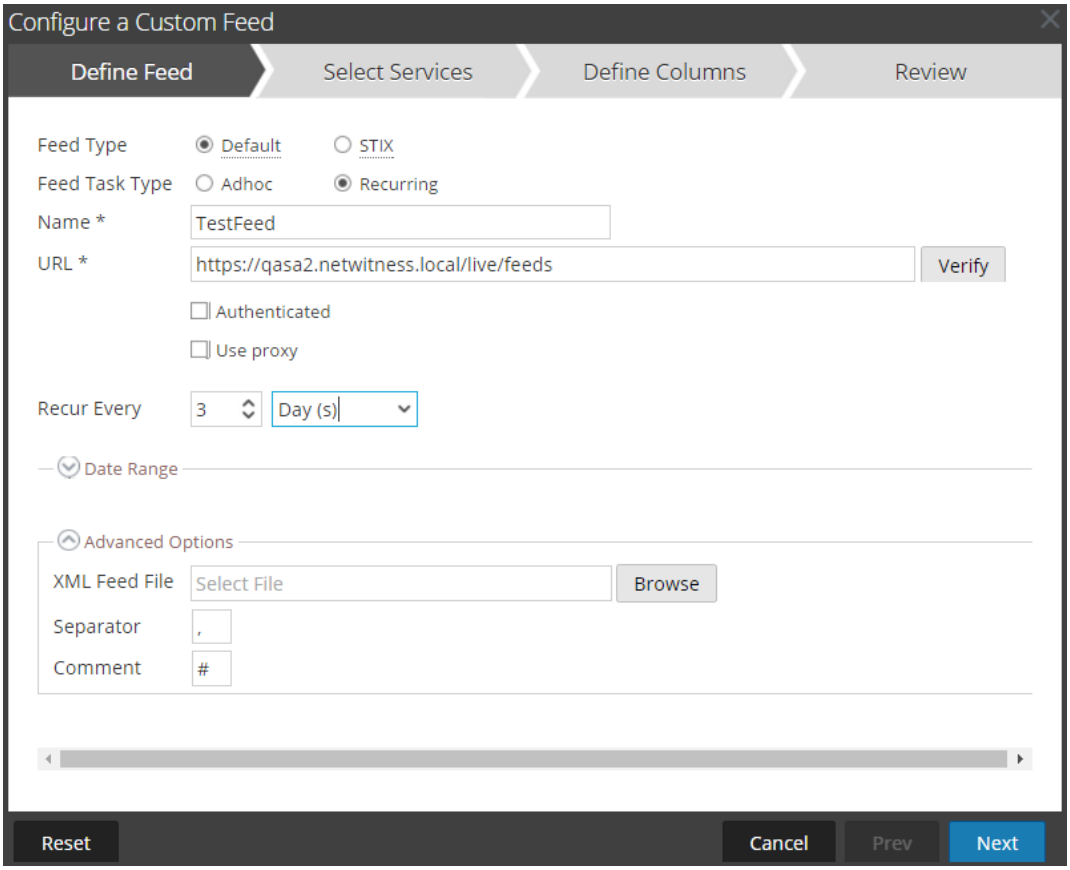
   NetWitness Suite stellt Ihren Benutzernamen und Ihr Passwort zur Authentifizierung bei der URL bereit.

d. Wenn der NetWitness Suite-Server über einen Proxy auf die Feed-URL zugreifen soll, wählen Sie **Proxy verwenden** aus. Weitere Informationen zur Konfiguration eines Proxys finden Sie im Thema **Konfigurieren des Proxys für NetWitness Suite** im *Systemkonfigurationsleitfaden*. Standardmäßig ist das Kontrollkästchen **Proxy verwenden** nicht aktiviert.

e. Führen Sie eine der folgenden Aktionen durch, um das Intervall für Wiederholungen zu definieren:

   - Legen Sie die Anzahl der Minuten, Stunden oder Tage zwischen den Wiederholungen des Feeds fest.
   - Legen Sie eine wöchentliche Wiederholung fest und wählen Sie die Wochentage aus.

f. Geben Sie zum Definieren des Datumsbereichs für die Ausführung der Feedwiederholungen das **Startdatum** und die Startzeit sowie das **Enddatum** und die Endzeit an.



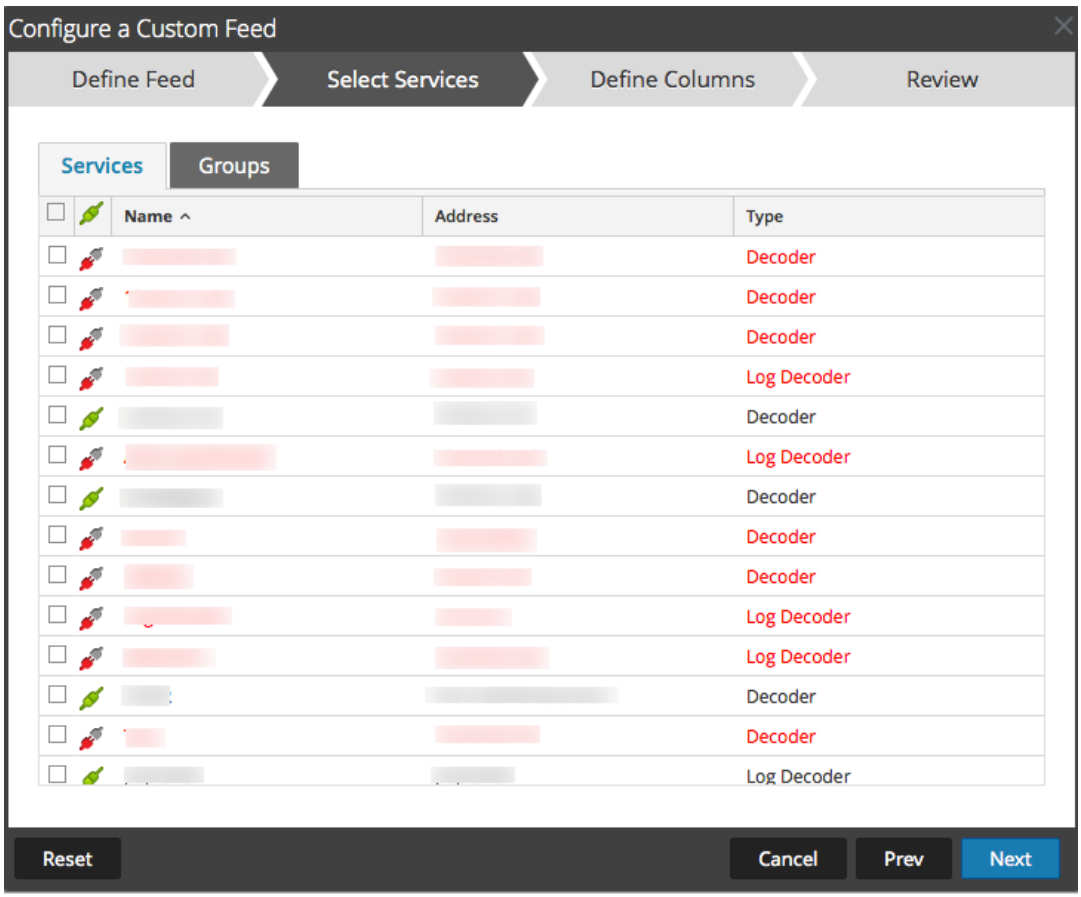
7. (Bedingungsabhängig) Gehen Sie so vor, wenn Sie einen Feed auf Grundlage einer XML-Feeddatei definieren möchten:

   - Geben Sie den **Namen** des Feeds ein und wählen Sie **Erweiterte Optionen** aus.

     Die Felder „Erweiterte Optionen“ werden angezeigt.

   - Wählen Sie eine XML-Feeddatei aus dem lokalen Dateisystem aus **Trennzeichen** (Standard ist Komma), legen Sie die **Kommentar**zeichen fest, die in der Feeddatendatei verwendet werden (Standard ist #), und klicken Sie auf **Weiter**.

Das Formular „Services auswählen“ wird angezeigt.



8. Um Services zu identifizieren, für die der Feed bereitgestellt werden soll, führen Sie eine der folgenden Aktionen aus:

   a. Wählen Sie einen oder mehrere Decoder und Log Decoder aus und klicken Sie auf **Weiter**.

   b. Klicken Sie auf die Registerkarte **Gruppen** und wählen Sie eine Gruppe aus. Klicken Sie auf **Weiter**.

      Das Formular Spalten definieren wird angezeigt.

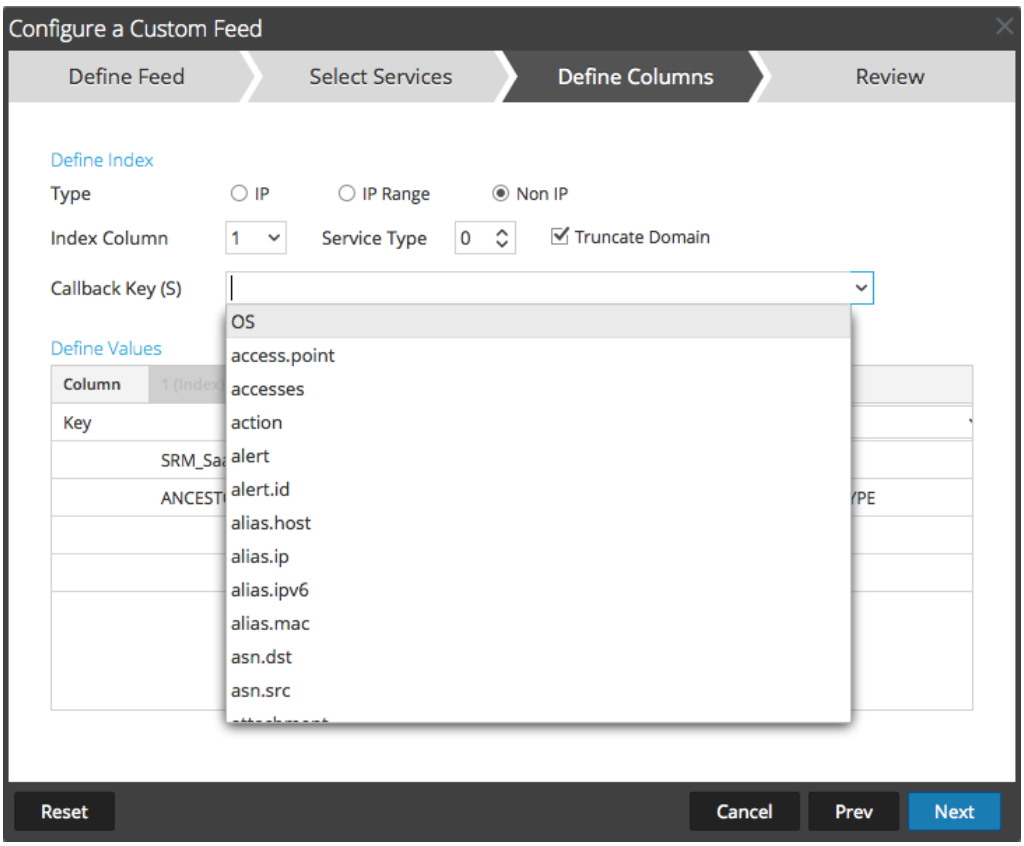
9. So ordnen Sie Spalten im Formular Spalten definieren zu:

   a. Definieren Sie den Indextyp: **IP**, **IP-Bereich** oder **Nicht IP** und wählen Sie die Indexspalte aus.

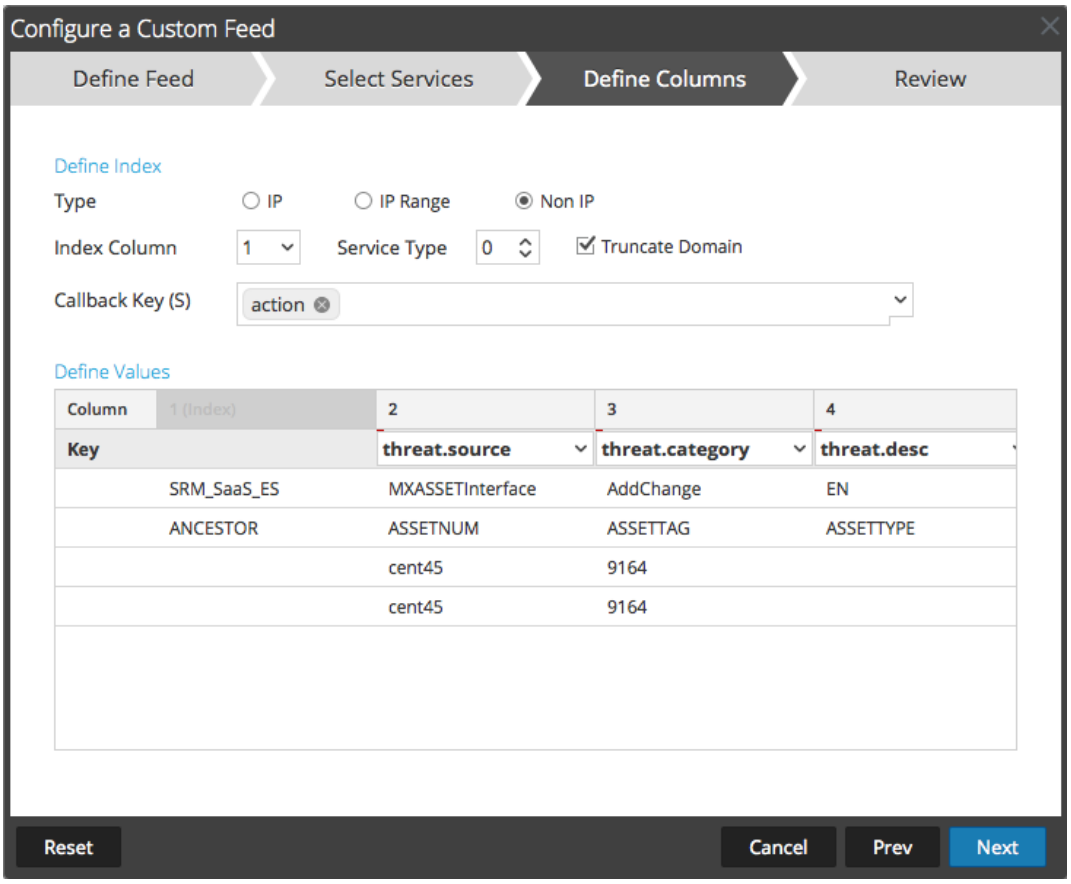
   b. (Bedingungsabhängig) Wenn der Indextyp **IP** oder **IP-Bereich** ist und die IP-Adresse in CIDR-Notation angegeben ist, wählen Sie **CIDR** aus.

   c. (Bedingungsabhängig) Wenn der Indextyp **Nicht IP** ist, werden zusätzliche Einstellungen angezeigt. Wählen Sie den Servicetyp und die **Callback-Schlüssel** aus und wählen Sie

optional **Domain abschneiden** aus.

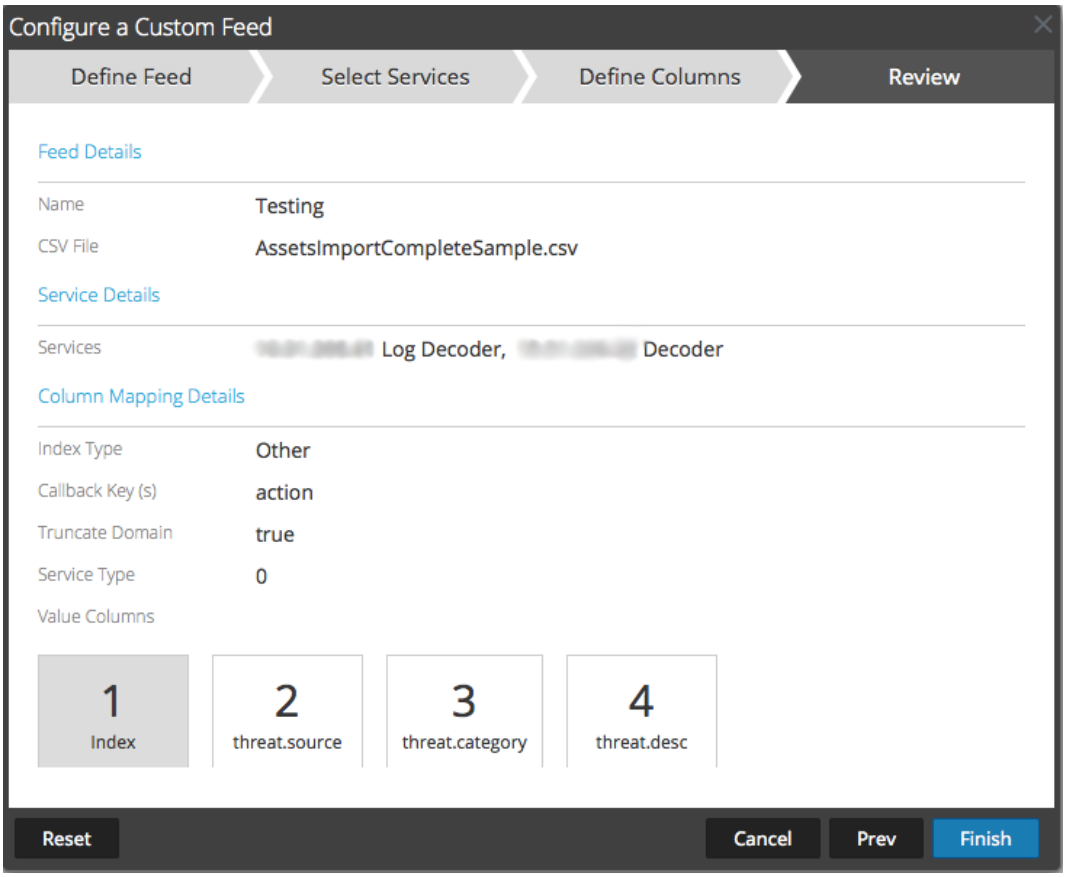


d. Wählen Sie in der Drop-down-Liste den Sprachschlüssel aus, der auf die Daten in jeder Spalte angewendet werden soll. Die in der Drop-down-Liste aufgeführten Metadaten basieren auf den für die Servicedefinitionswerte verfügbaren Metadaten. Sie können auch andere Metadaten hinzufügen, die auf erweitertem Know-how basieren.



e. Klicken Sie auf **Weiter**.

   Das Formular Überprüfung wird angezeigt.



10. Bevor Sie auf **Fertigstellen** klicken, können Sie jederzeit Folgendes tun:
    - Auf **Abbrechen** klicken, um den Assistenten zu schließen, ohne die Feeddefinition zu speichern
    - Auf **Zurücksetzen** klicken, um die Daten im Assistenten zu löschen
    - Auf **Weiter** klicken, um das nächste Formular anzuzeigen (wenn nicht das letzte Formular angezeigt wird)
    - Auf **Vorheriges** klicken, um das vorherige Formular anzuzeigen (wenn nicht das erste Formular angezeigt wird)

11. Überprüfen Sie die Feedinformationen und klicken Sie auf **Fertigstellen**, wenn diese korrekt sind.
12. Nach der erfolgreichen Erstellung der Feeddefinitionsdatei wird der Assistent für das Erstellen von Feeds geschlossen. Der Feed und die zugehörige Tokendatei werden im Feedraster aufgeführt und die Fertigstellung wird in einem Fortschrittsbalken nachverfolgt.

Sie können den Eintrag ein- oder ausblenden, um festzustellen, wie viele Services enthalten sind und welche erfolgreich waren.

MetaCallback-Feeds unter Verwendung des CIDR-Indexbereichs für IPv4 und IPv6

In diesem Abschnitt wird beschrieben, wie Sie CIDR-Indexbereiche für IPv4 und IPv6 in benutzerdefinierten MetaCallback-Feeds verwenden. Wie bei anderen benutzerdefinierten Feeds müssen Sie eine Feeddatendatei im CSV-Format und eine Feeddefinitionsdatei im XML-Format erstellen.

Hinweis: Die Verwendung von MetaCallback-Feeds mit CIDR-Indexbereichen wird nur über den Assistenten „Erweiterte Konfiguration“ oder die REST-Schnittstelle unterstützt.

Das folgende Beispiel zeigt den Inhalt einer CSV-Datei und einer XML-Datei für einen MetaCallback-Feed unter Verwendung der CIDR-Indexbereiche für IPv4 oder IPv6.

.csv file:

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator=","
comment="#">
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0"
truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

Hinweis: Um einen CIDR-Indexbereich für Feeds mit einzelnen oder mehreren MetaCallbacks des Werttyps IPv4 oder IPv6 zu konfigurieren, MUSS das Feld des Typs „Index“ ein Bereichsattribut mit range="cidr" enthalten. Darüber hinaus wird die Konfiguration von „cidr“-Indexbereichen für Feeds mit MetaCallbacks mehrerer verschiedener Werttypen nicht unterstützt.

Erstellen eines benutzerdefinierten STIX-Feeds

Sie können mithilfe einer CSV- oder STIX-formatierten Feeddatendatei einen benutzerdefinierten Feed in RSA NetWitness Suite erstellen.

Hinweis: NetWitness Suite unterstützt nur die STIX-Versionen (Structured Threat Information Expression) 1.0, 1.1 und 1.2.

Hinweis: Version 10.6.1 und neuere Versionen von Security Analytics unterstützen Structured Threat Information Expression (STIX).

Structured Threat Information Expression (STIX™) ist eine strukturierte Sprache zur Beschreibung von Cyber-Threat-Informationen, um diese durchgängig gemeinsam nutzen, speichern und analysieren zu können. Weitere Informationen zu STIX finden Sie unter https://stixproject.github.io/.

Achtung: Wenn ein wiederkehrender STIX-Feed konfiguriert ist und Sie Security Analytics von 10.6.x auf NetWitness Suite 11.0 aktualisieren, müssen Sie den wiederkehrenden STIX-Feed erneut konfigurieren.

In NetWitness Suite werden STIX-Feeds (`.xml`) des Typs „Indicator“ oder „Observable“ unterstützt, die Eigenschaften enthalten wie z. B. IP-Adressen, Datei-Hashes, Domain-Namen, URIs und E-Mail-Adressen. Nur die Eigenschaftswerte des Operators „gleich“ werden unterstützt. Und Attribute wie z. B. Typ und Titel werden ebenfalls von STIX (`.xml`) gelesen. STIX (`.xml`) wird nur mit einem einzigen STIX_Package unterstützt.

TAXII (Trusted Automated eXchange of Indicator Information) ist der wichtigste Transportmechanismus für Informationen zu Cyberbedrohungen, die in STIX dargestellt werden. Organisationen können mithilfe der TAXII-Services Informationen zu Cyberbedrohungen sicher und automatisiert freigeben.

Die STIX- und TAXII-Communitys arbeiten eng zusammen, um sicherzustellen, dass das Paket, das sie für die Weitergabe von Informationen über Bedrohungen anbieten, auch weiterhin vollständig ist.

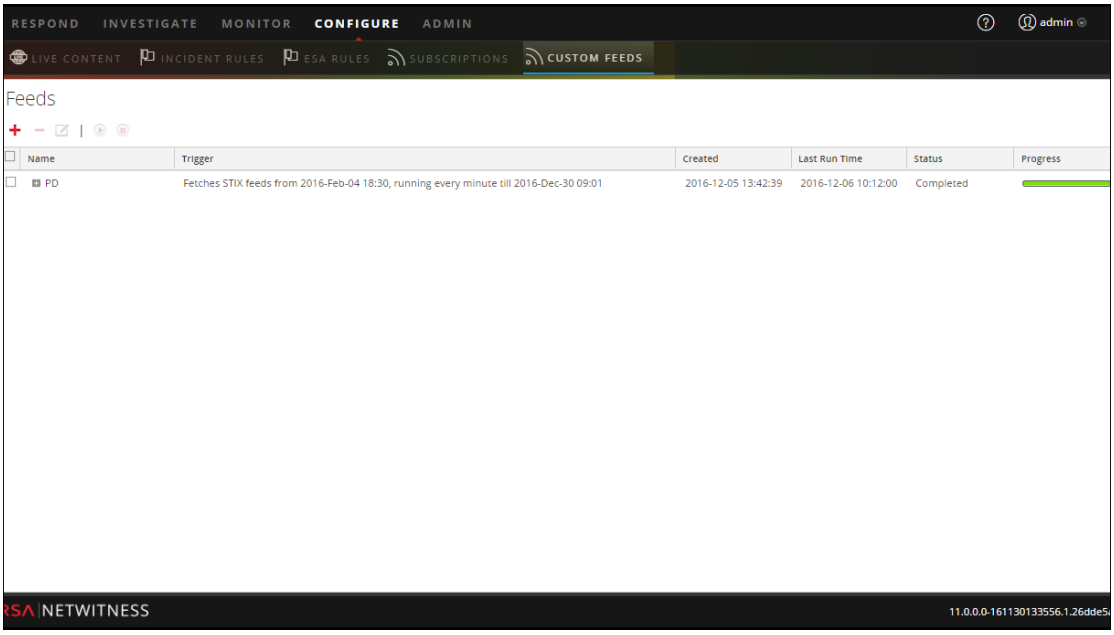
Abgesehen vom TAXII-Server können sich STIX-Daten auch auf einem REST-Server befinden. Sie können die STIX-Datei vom REST-Server durch Angabe der URL des REST-Servers abrufen. Beispiel: http://stixrestserver.internal.com.

Für einen bedarfsorientierten benutzerdefinierten Feed müssen die Feeddatendatei (`.csv` oder STIX [`.xml`]) und optional die Feeddefinitionsdatei (`.xml`) auf dem lokalen Dateisystem verfügbar sein. Für einen wiederkehrenden benutzerdefinierten Feed müssen die Dateien unter einer URL verfügbar sein, auf die der NetWitness Suite-Server Zugriff hat.

So erstellen Sie einen benutzerdefinierten STIX-Feed:

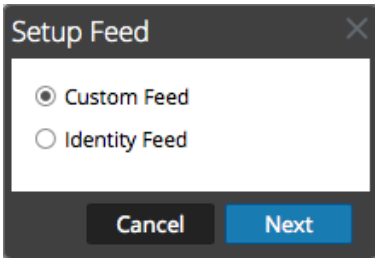
1. Navigieren Sie zu **Konfigurieren > Benutzerdefinierte Feeds**.

   Die Ansicht „Feeds“ wird angezeigt.



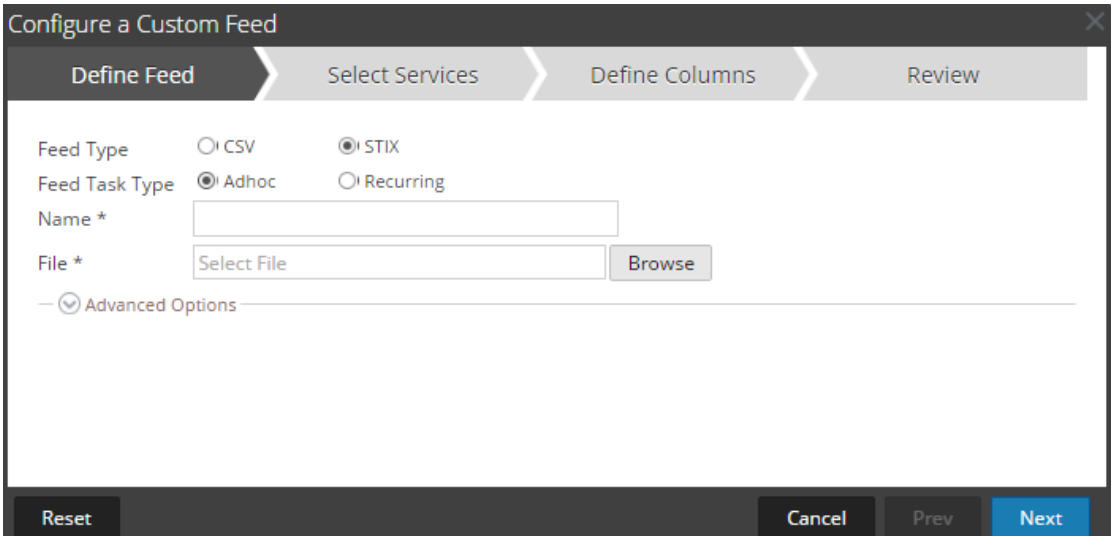
2. Klicken Sie auf der Symbolleiste auf +.

   Das Dialogfeld „Feed einrichten“ wird angezeigt.



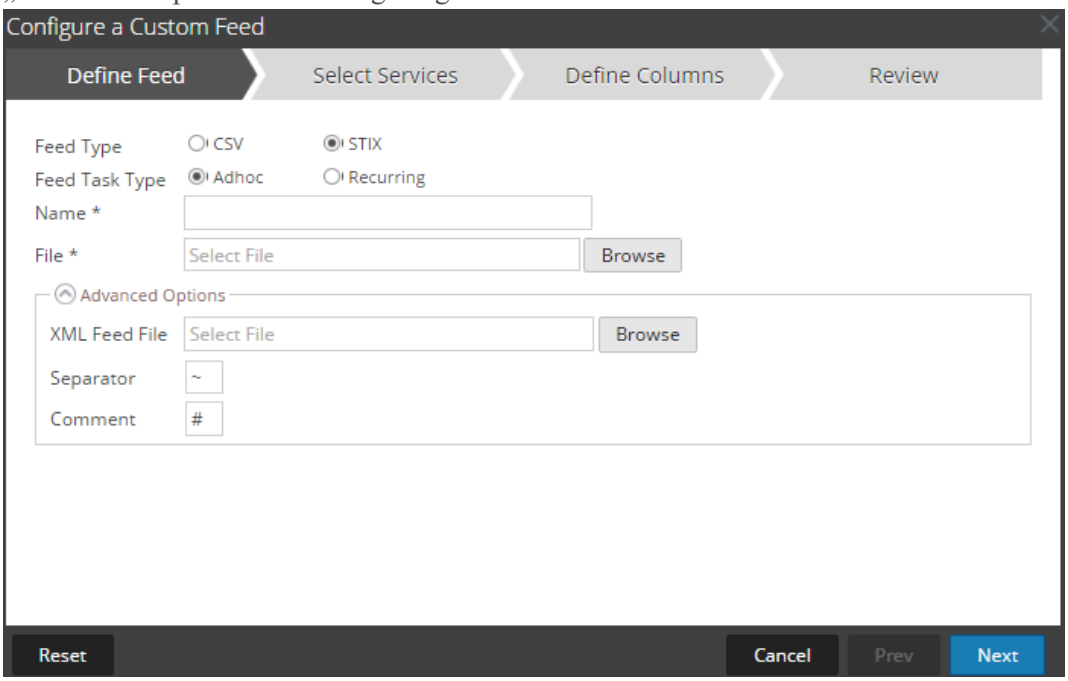
3. Um den Feedtyp auszuwählen, klicken Sie auf **Benutzerdefinierter Feed** und auf **Weiter**.

Der Assistent „Benutzerdefinierten Feed konfigurieren“ wird angezeigt und das Formular „Feed definieren“ geöffnet.



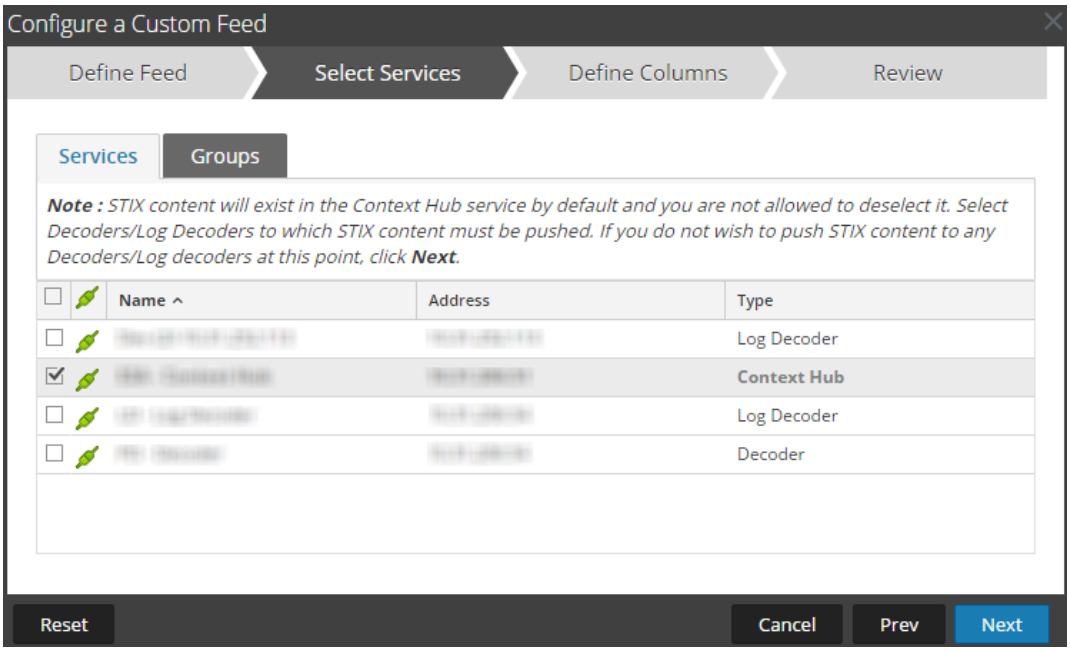
4. Definieren Sie einen Feed auf Grundlage einer STIX-formatierten `.xml`-Datei. Wählen Sie **STIX** im Feld **Feed-Typ** aus.
5. Um eine bedarfsorientierte Feedaufgabe zu definieren, die einmal ausgeführt wird, wählen Sie im Feld **Typ der Feedaufgabe** die Option **Ad-hoc** aus und fahren Sie mit einer der folgenden Aktionen fort:
   a. (Bedingungsabhängig) Um einen auf einer STIX-formatierten `.xml`-Datei basierenden Feed zu definieren, geben Sie einen **Namen** für den Feed ein, wählen Sie eine STIX-formatierte `.xml`-Inhaltsdatei unter **Datei** im lokalen Dateisystem aus und klicken Sie auf **Weiter**.
   b. (Bedingungsabhängig) Um einen auf einer XML-Feeddatei basierenden Feed zu definieren, wählen Sie **Erweiterte Optionen** aus.

„Erweiterte Optionen“ wird angezeigt:



c. Wählen Sie eine XML-Feeddatei aus dem lokalen Dateisystem aus. Treffen Sie eine Auswahl für das **Trennzeichen** (Standard ist Komma), legen Sie die Kommentar**zeichen** fest, die in der Feeddatendatei verwendet werden (Standard ist #), und klicken Sie auf **Weiter**.

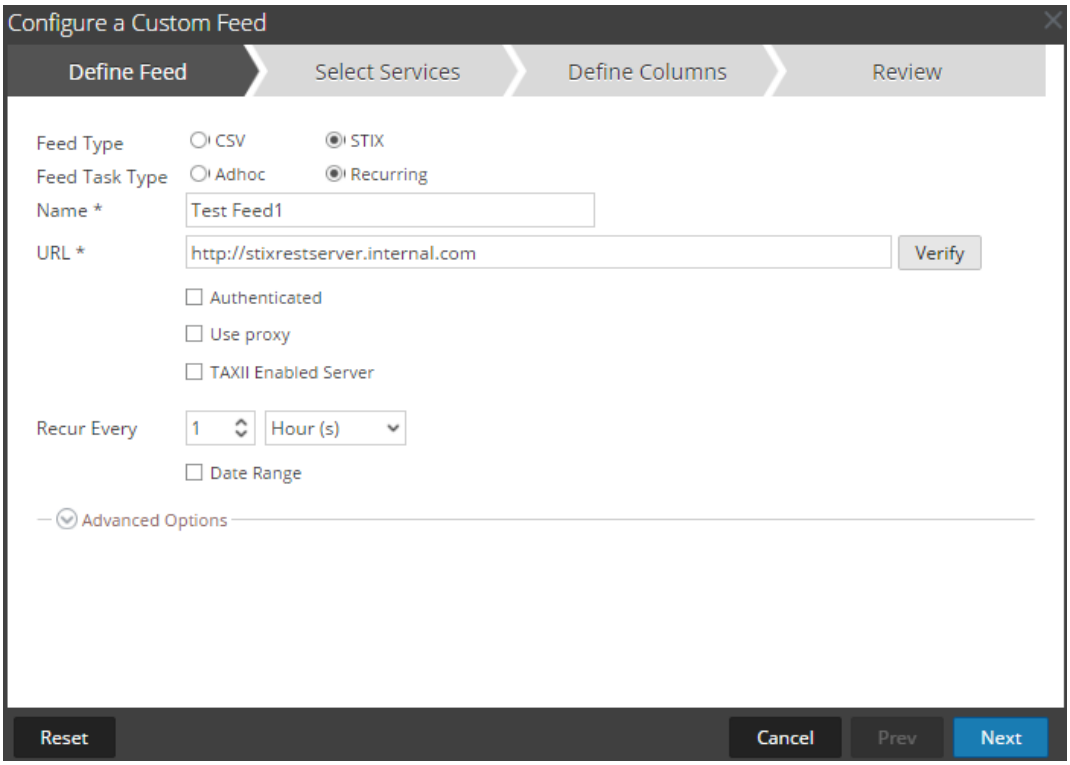
d. Das Formular Services auswählen wird angezeigt. Dies ist ein Beispiel eines Formulars für einen Feed, der auf einer Feeddatendatei ohne Feeddefinitionsdatei basiert. Wenn Sie einen Feed definieren, der auf einer Feeddefinitionsdatei basiert, ist die Registerkarte Spalten definieren nicht erforderlich.



6. So definieren Sie einen wiederkehrenden Feed, der innerhalb eines bestimmten Datumsbereichs in spezifischen Zeitabständen wiederholt ausgeführt wird:

   a. Wählen Sie im Feld **Typ der Feedaufgabe** die Option **Wiederkehrend** aus.

   Das Formular „Feed definieren“ enthält die Felder für einen wiederkehrenden Feed.

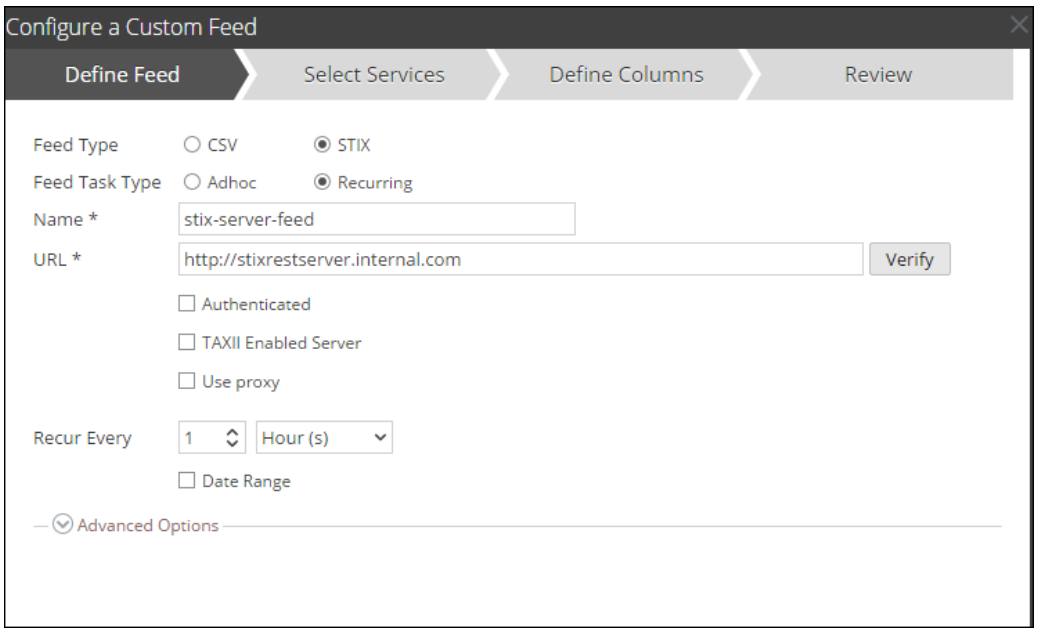


b. Geben Sie im Feld **URL** eine der folgenden URLs ein:

- Um einen wiederkehrenden Feed basierend auf STIX zu definieren, der STIX-Pakete von einem TAXII-Server abruft, geben Sie die URL des Erkennungsservice des TAXII-Servers ein, z. B. http://hailataxii.com/taxii-discovery-service.

  Hinweis: Ein Context Hub-Service, der auf dem Event Stream Analysis-Host installiert ist, muss für den angegebenen TAXII-Server erreichbar sein.

- Um einen wiederkehrenden Feed auf Grundlage einer STIX-formatierten XML-Datei unter Verwendung des REST-Servers zu definieren, geben Sie die URL des REST-Servers ein, unter der sich die STIX-Datendatei befindet, z. B. http://stixrestserver.internal.com.



NetWitness Suite überprüft die Verbindung zum Server. So kann NetWitness Suite vor jedem erneuten Aufruf automatisch die aktuelle Datei abrufen.

c. Wenn Sie nicht möchten, dass NetWitness Suite das SSL-Zertifikat des REST-Servers überprüft, wählen Sie **Allen Zertifikaten vertrauen** aus. Diese Option ist standardmäßig aktiviert.

d. Klicken Sie für die Clientauthentifizierung mit der REST-URL im Feld **Zertifikat** auf **Durchsuchen** und wählen Sie das selbst signierte Zertifikat aus. Folgende Zertifikatformate werden unterstützt: CER, CRT mit Base64- und DER-kodierten Dateien.

e. (Optional) Wenn der Zugriff auf die URL beschränkt ist und eine Authentifizierung

mithilfe Ihres Benutzernamens und Passworts erfordert, wählen Sie **Authentifiziert** aus.

NetWitness Suite stellt Ihren Benutzernamen und Ihr Passwort zur Authentifizierung bei der URL bereit.

f. Wählen Sie **TAXII-fähiger Server** aus, wenn Sie eine TAXII-Sammlung aus der Liste auswählen möchten.
Für eine gültige URL werden eine oder mehrere TAXII-Sammlungen, die die STIX-Datendatei enthalten, auf Grundlage Ihrer Anmeldedaten angezeigt. Wählen Sie die erforderliche TAXII-Sammlung aus der Liste aus. Von einem TAXII-Server kann nur eine Sammlung für einen Feed hinzugefügt werden.

Hinweis: Es werden zwar mehrere Feeds von mehreren TAXII-Servern unterstützt, pro TAXII-Server aber nur ein Konto (Benutzername und Passwort).

g. Wenn der NetWitness Suite-Server über einen Proxy auf die Feed-URL zugreifen soll, wählen Sie **Proxy verwenden** aus. Weitere Informationen zur Konfiguration eines Proxys finden Sie im Thema **Konfigurieren des Proxys für NetWitness Suite** im *Systemkonfigurationsleitfaden*. Standardmäßig ist das Kontrollkästchen **Proxy verwenden** nicht aktiviert.

h. (Optional) Klicken Sie auf **Überprüfen**, um die Einstellungen zu testen.

Hinweis: Vergewissern Sie sich, dass alle erforderlichen Verbindungsparameter wie z. B. „Authentifizierung“, „Proxy“, „Zertifikatvertrauen“, „TAXII-fähiger Server“ usw. konfiguriert sind, bevor Sie auf **Überprüfen** klicken.

i. Führen Sie eine der folgenden Aktionen durch, um das Wiederholungsintervall für die Weitergabe an Decoder oder Log Decoder zu definieren:

- Legen Sie die Anzahl der Minuten, Stunden oder Tage zwischen den Wiederholungen des Feeds fest.
- Legen Sie eine wöchentliche Wiederholung fest und wählen Sie die Wochentage aus.

j. Geben Sie zum Definieren des Datumsbereichs für die Ausführung der Feedwiederholungen das **Startdatum** und die Startzeit sowie das **Enddatum** und die Endzeit an. Das Startdatum sollte als das Datum definiert werden, ab dem die Daten abgerufen werden sollen. Stellen Sie sicher, dass sich das **Startdatum** nicht innerhalb der nächsten 180 Tage befindet.

7. (Bedingungsabhängig) Gehen Sie folgendermaßen vor, wenn Sie einen Feed auf Grundlage einer XML-Feeddatei definieren möchten:

- Geben Sie den **Namen** des Feeds ein und wählen Sie **Erweiterte Optionen** aus.

  Die Felder „Erweiterte Optionen“ werden angezeigt.

- Wählen Sie eine XML-Feeddatei aus dem lokalen Dateisystem und das **Trennzeichen**

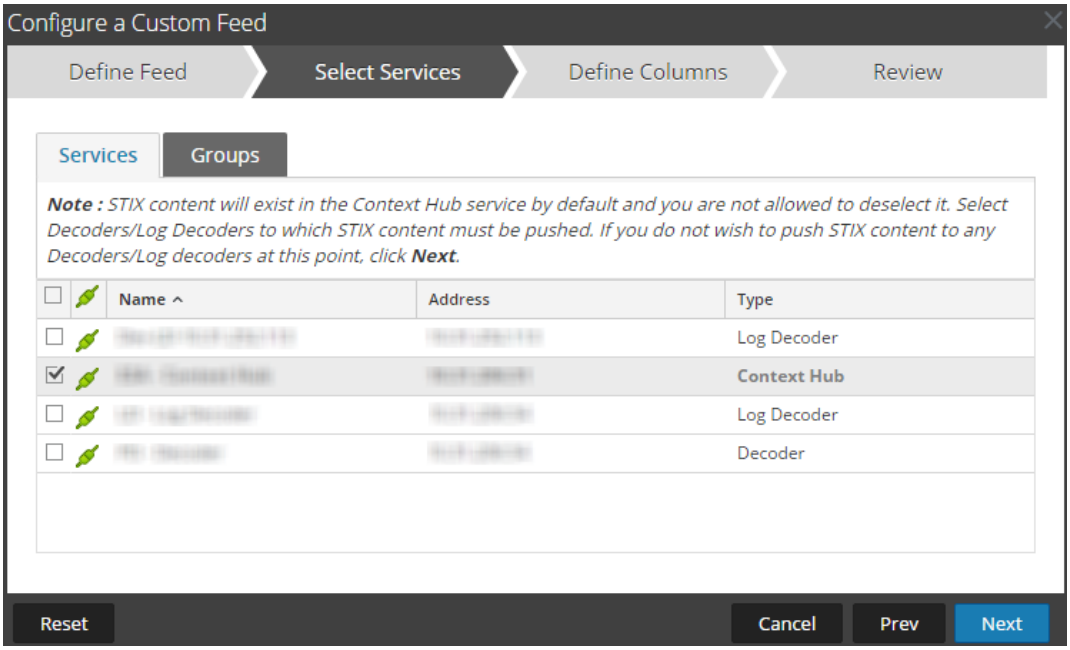
aus (Standard ist Komma), legen Sie die **Kommentarzeichen** fest, die in der Feeddatendatei verwendet werden (Standard ist #).

- Geben Sie im Feld **STIX-Daten entfernen, die älter sind als** die Anzahl der Tage an, für die vom TAXII-Server abgerufene STIX-Pakete gespeichert werden sollen. Die STIX-Pakete, die älter als die angegebene Anzahl von Tagen sind, werden automatisch gelöscht.
- Klicken Sie auf **Weiter**.
  Das Formular „Services auswählen“ wird angezeigt.

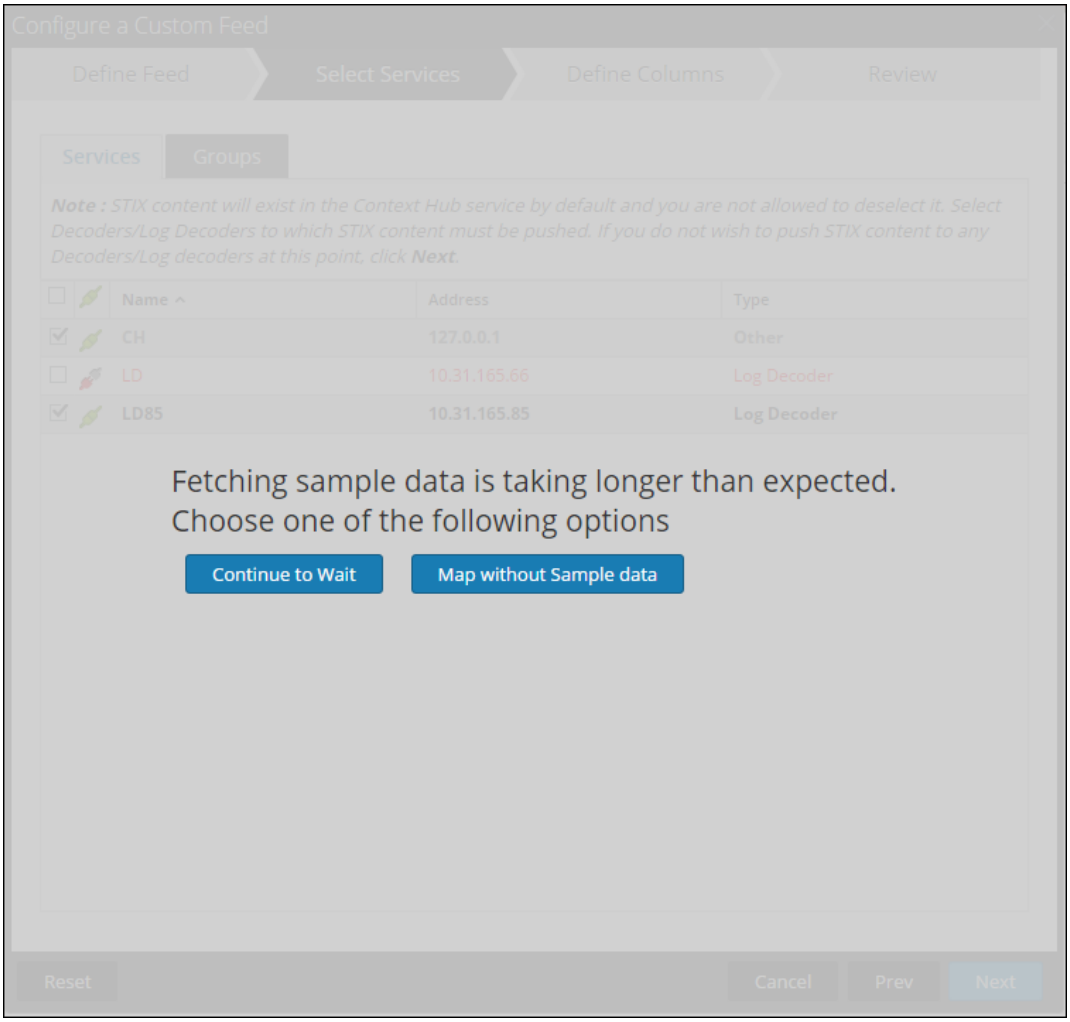
8. Um Services zu identifizieren, für die der Feed bereitgestellt werden soll, führen Sie eine der folgenden Aktionen aus:

   a. Wählen Sie einen oder mehrere Decoder und Log Decoder aus und klicken Sie auf **Weiter**.

   b. Im Fall eines STIX-Feeds ist standardmäßig „Context Hub“ ausgewählt. Sie dürfen diese Auswahl nicht aufheben. Außerdem können Sie einen oder mehrere Decoder und Log Decoder auswählen und auf **Weiter** oder auf die Registerkarte **Gruppen** klicken und eine Gruppe auswählen. Klicken Sie auf **Weiter**.



Wenn die Daten vom STIX-Server sehr umfangreich sind, wird die folgende Meldung angezeigt:



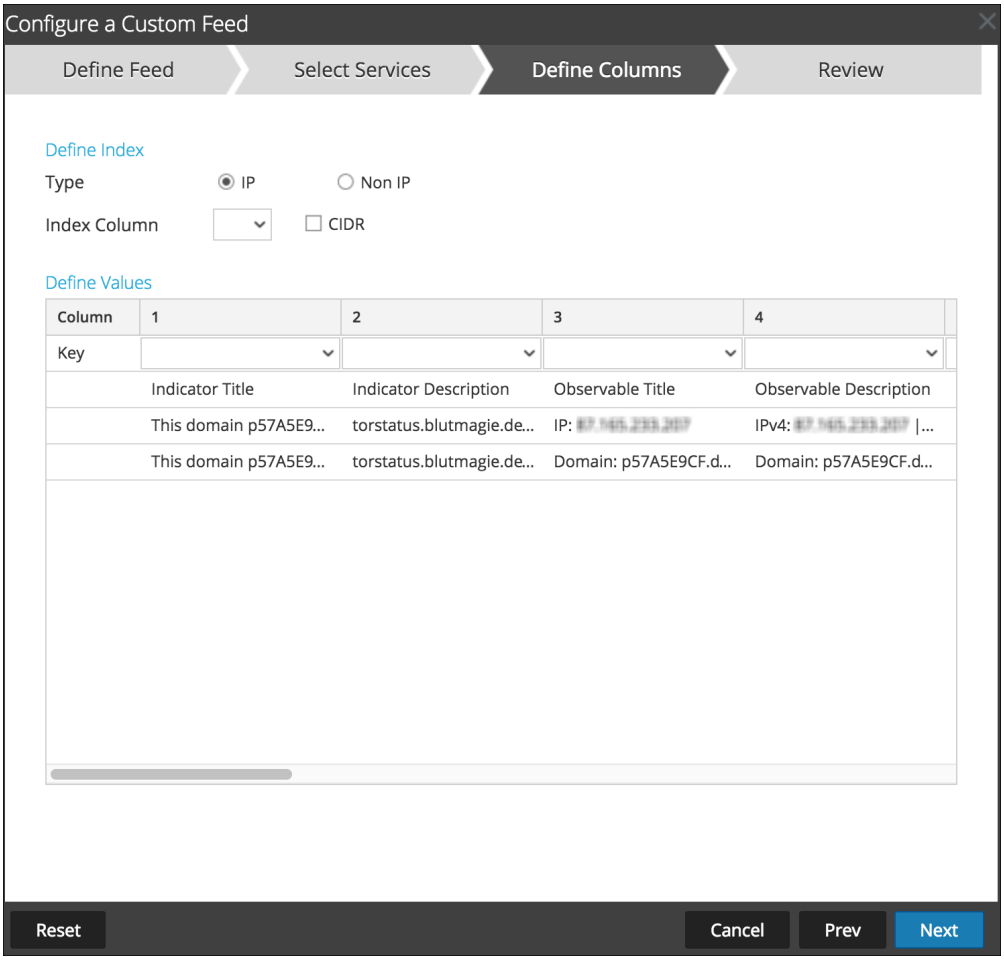
- Wenn Sie auf **Weiter warten** klicken, wartet er weiter, bis die Beispieldaten abgerufen werden oder ein Timeout (10 Minuten) erfolgt, je nachdem, was früher eintritt. Bei einem Timeout werden auch nach 10 Minuten keine Beispieldaten abgerufen.
- Wenn Sie auf **Ohne Beispieldaten zuordnen** klicken, wird die Spalte für die Zuordnung ohne Beispieldaten angezeigt.

Das Formular „Spalten definieren“ wird angezeigt.

9. So ordnen Sie im Formular „Spalten definieren“ Spalten zu:
   a. Definieren Sie den Indextyp: **IP**, **IP-Bereich** oder **Nicht IP** und wählen Sie die Indexspalte aus.

b. (Bedingungsabhängig) Wenn der Indextyp **IP** oder **IP-Bereich** ist und die IP-Adresse in CIDR-Notation angegeben ist, wählen Sie **CIDR** aus.

c. (Bedingungsabhängig) Wenn der Indextyp **Nicht IP** ist, werden zusätzliche Einstellungen angezeigt. Wählen Sie den Servicetyp und die **Callback-Schlüssel** aus und wählen Sie optional **Domain abschneiden** aus.

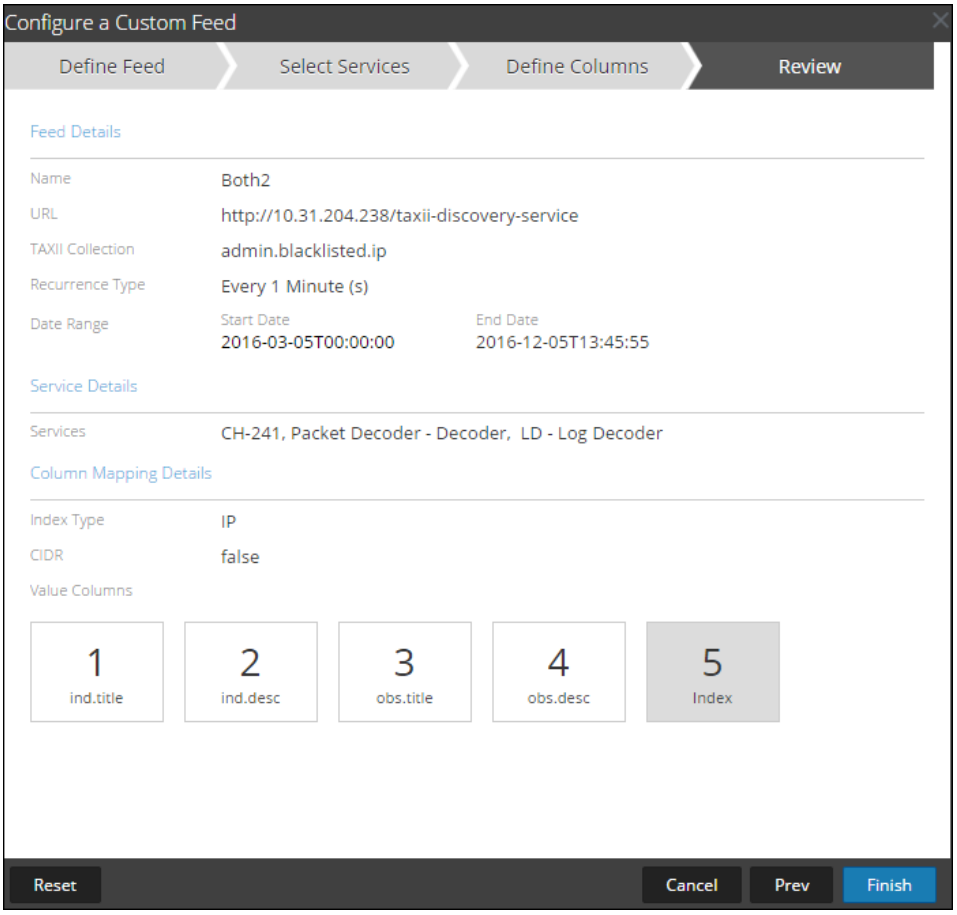


Hinweis:
- Wenn der **Indextyp** „Nicht IP“ lautet, können Sie mehrere Indexspalten in den **Indexspalten** auswählen. Die Werte aus allen ausgewählten Spalten werden in der ersten Indexspalte zusammengeführt, die Sie ausgewählt haben, und die zusammengeführten Werte werden für die Analyse an den Log Decoder übertragen. Beispiel: Wenn Sie in den **Indexspalten** 2, 4, 7 als Indexspalten auswählen, werden die Werte aus den Spalten 2, 4 und 7 in der Spalte 2 zusammengeführt und die Werte für die Analyse an Log Decoder übertragen.
- Für Spalten wie „Indicator Title“, „Indicator Description“, „Observable Title“ oder „Observable Description“ kann keine Indexierung erfolgen, da keine Suche für diese Spalten durchgeführt werden kann.

d. Wählen Sie in der Drop-down-Liste den Sprachschlüssel aus, der auf die Daten in jeder Spalte angewendet werden soll. Die in der Drop-down-Liste aufgeführten Metadaten basieren auf den für die Servicedefinitionswerte verfügbaren Metadaten. Sie können auch andere Metadaten hinzufügen, die auf erweitertem Know-how basieren.

e. Klicken Sie auf **Weiter**.

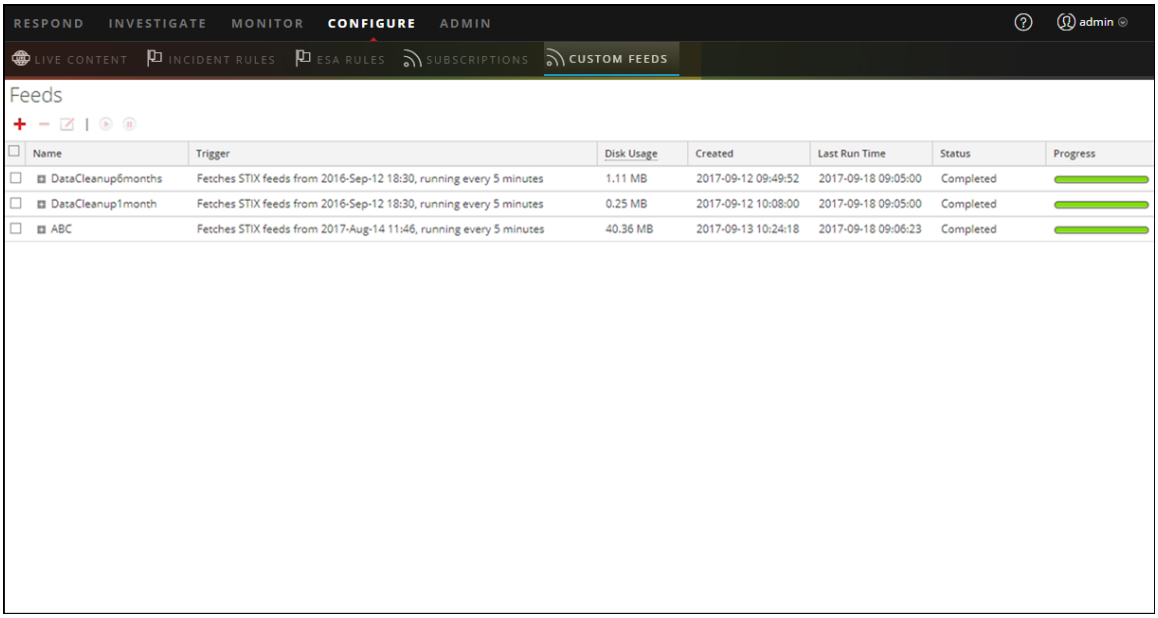
Das Formular Überprüfung wird angezeigt.



10. Bevor Sie auf **Fertigstellen** klicken, können Sie jederzeit Folgendes tun:

- Auf **Abbrechen** klicken, um den Assistenten zu schließen, ohne die Feeddefinition zu speichern
- Auf **Zurücksetzen** klicken, um die Daten im Assistenten zu löschen
- Auf **Weiter** klicken, um das nächste Formular anzuzeigen (wenn nicht das letzte Formular angezeigt wird)
- Auf **Vorheriges** klicken, um das vorherige Formular anzuzeigen (wenn nicht das erste Formular angezeigt wird)

11. Überprüfen Sie die Feedinformationen und klicken Sie auf **Fertigstellen**, wenn diese korrekt sind.
12. Nach der erfolgreichen Erstellung der Feeddefinitionsdatei wird der Assistent für das Erstellen von Feeds geschlossen. Der Feed und die zugehörige Tokendatei werden im Feedraster aufgeführt und die Fertigstellung wird in einem Fortschrittsbalken nachverfolgt. Sie können den Eintrag ein- oder ausblenden, um festzustellen, wie viele Services enthalten sind und welche erfolgreich waren.



Hinweis: Integrität und Zustand gibt Warnmeldungen aus, falls der verfügbare Heap-Speicher des Context Hub-Servers sehr niedrig ist. Wenn der Status des Context Hub-Servers aufgrund von Speichermangel fehlerhaft ist. Weitere Informationen zum Troubleshooting bei einem `OutOfMemoryError` auf einem `Contexthub`-Server finden Sie unter „Troubleshooting“ im *Handbuch Live-Services-Management*.

MetaCallback-Feeds unter Verwendung des CIDR-Indexbereichs für IPv4 und IPv6

In diesem Abschnitt wird beschrieben, wie Sie CIDR-Indexbereiche für IPv4 und IPv6 in benutzerdefinierten MetaCallback-Feeds verwenden. Wie bei anderen benutzerdefinierten Feeds müssen Sie eine Feeddatendatei im CSV-Format und eine Feeddefinitionsdatei im XML-Format erstellen.

Hinweis: Die Verwendung von MetaCallback-Feeds mit CIDR-Indexbereichen wird nur über den Assistenten „Erweiterte Konfiguration“ oder die REST-Schnittstelle unterstützt.

Das folgende Beispiel zeigt den Inhalt einer CSV-Datei und einer XML-Datei für einen MetaCallback-Feed unter Verwendung der CIDR-Indexbereiche für IPv4 oder IPv6.

`.csv file:`

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator=","
comment="#">
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0"
truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

Hinweis: Um einen CIDR-Indexbereich für Feeds mit einzelnen oder mehreren MetaCallbacks des Werttyps IPv4 oder IPv6 zu konfigurieren, MUSS das Feld des Typs „Index“ ein Bereichsattribut mit range="cidr" enthalten. Darüber hinaus wird die Konfiguration von „cidr“-Indexbereichen für Feeds mit MetaCallbacks mehrerer verschiedener Werttypen nicht unterstützt.

Erstellen und Verwalten eines Identitätsfeeds

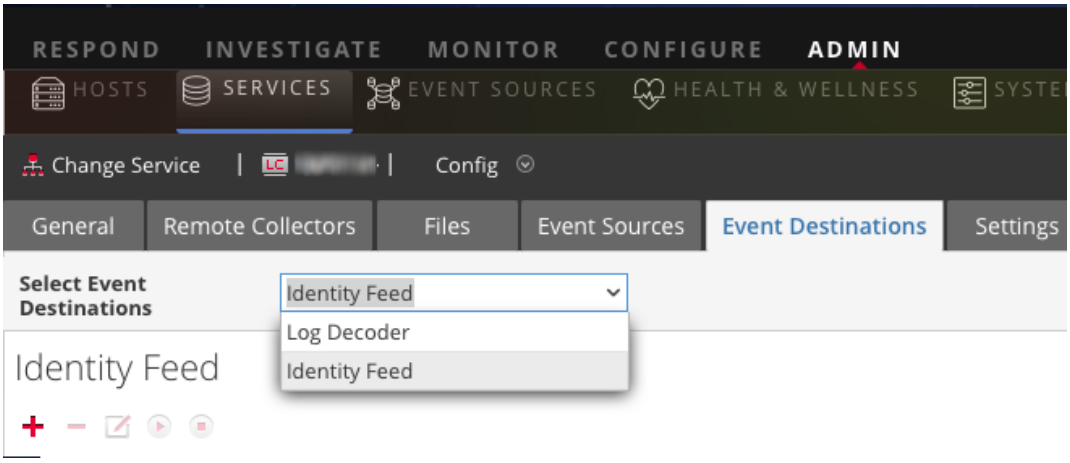
Sie können einen Identitätsfeed einfach erstellen und ihn in ausgewählten Decoders und Log Decoders auffüllen. Nach Abschluss dieses Verfahrens werden Sie einen Identitätsfeed erstellt haben.

So erstellen Sie einen Identitätsfeed:

1. Fügen Sie ein Ziel für den Feed hinzu.
   a. Navigieren Sie zu **ADMIN > Services** und wählen Sie aus der Liste **Services** einen **Log Collector**-Service und dann **Anzeigen > Konfig** aus.

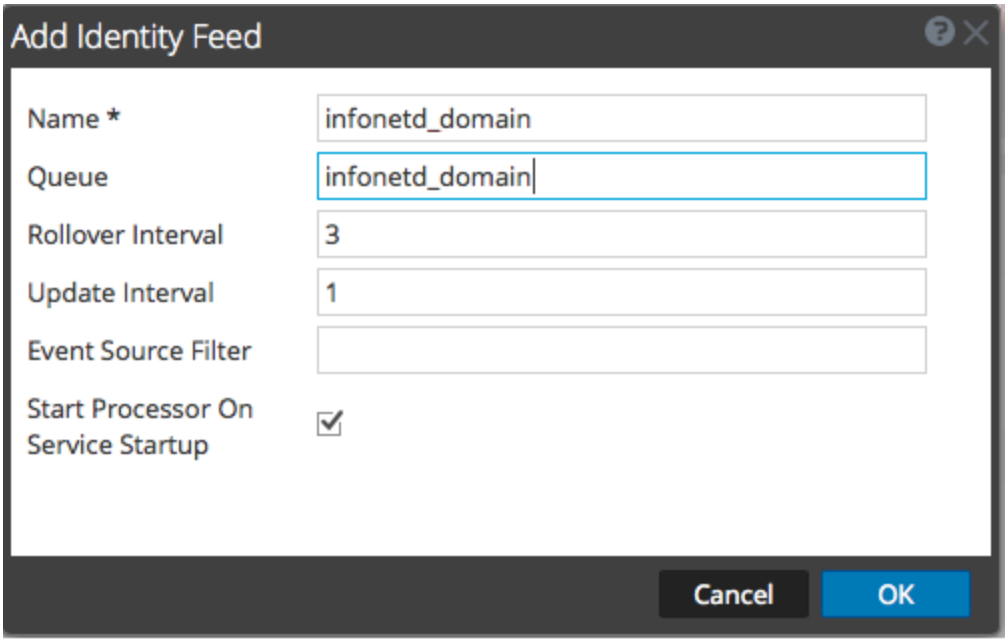
b. Wählen Sie die Registerkarte **Ereignisziele** aus.

c. Wählen Sie im Feld **Ereignisziele auswählen** die Option **Identitätsfeed**.



d. Klicken Sie auf + und geben Sie einen eindeutigen Namen für den Feed ein.

Der Name der Warteschlange identifiziert den Feed im Log Collector. Verwenden Sie den Namen des Feeds für die Warteschlange.



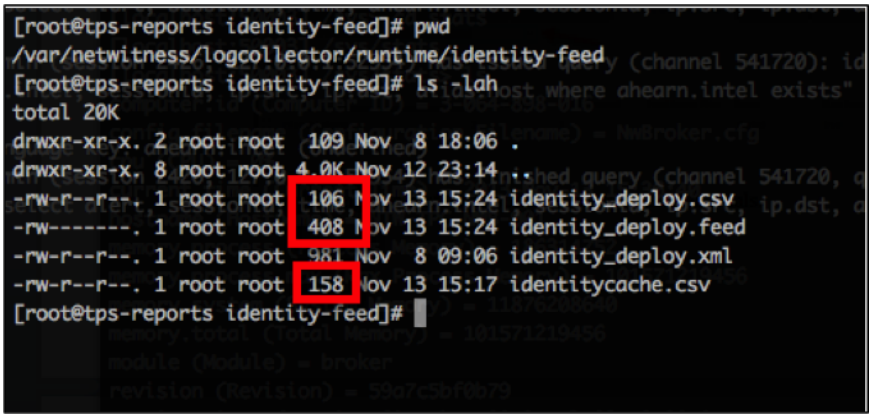
e. Klicken Sie auf **OK**.

2. Testen Sie das Generieren von Meldungen.

a. Benutzer sollten sich in Windows-Feldern in der Domain anmelden, um die entsprechenden Protokollmeldungen auf den Domain-Controllern zum Testen zu

erzeugen.

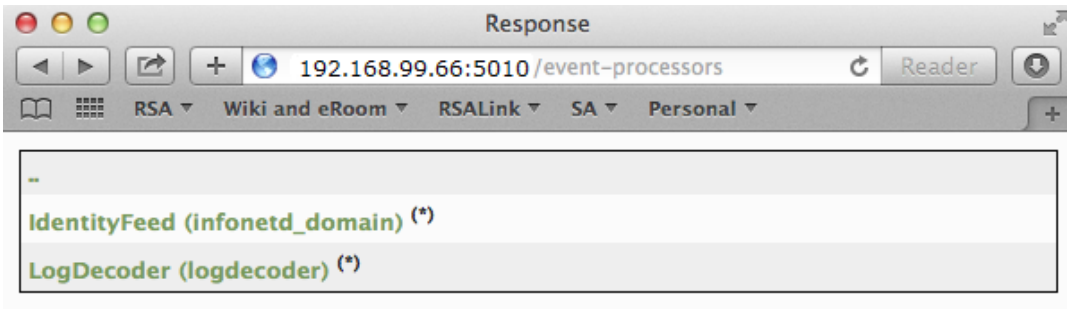
b. Stellen Sie sicher, dass die Daten in die Feeddateien geschrieben werden. Stellen Sie über SSH eine Verbindung mit dem Log Decoder/Collector oder Virtual Log Collector her, der konfiguriert wird. Navigieren Sie zu `/var/netwitness/logcollector/runtime/identity-feed` und überprüfen Sie, ob die `Identity_deploy`-Dateien mit Daten gefüllt werden.



c. Öffnen Sie einen Webbrowser (Internet Explorer nicht empfohlen) und melden Sie sich bei der REST-Schnittstelle des Log Collector an. Verwenden Sie für die Anmeldung Administrator-Anmeldedaten. Wenn die IP-Adresse Ihres Log Collector beispielsweise 192.168.99.66 ist, würde die URL wie folgt lauten:

- SSL nicht aktiviert: **http://192.168.99.66:50101/event-processors**
- SSL aktiviert: **http://192.168.99.66:50101/event-processors**

Die Browseranzeige sollte wie folgt aussehen:

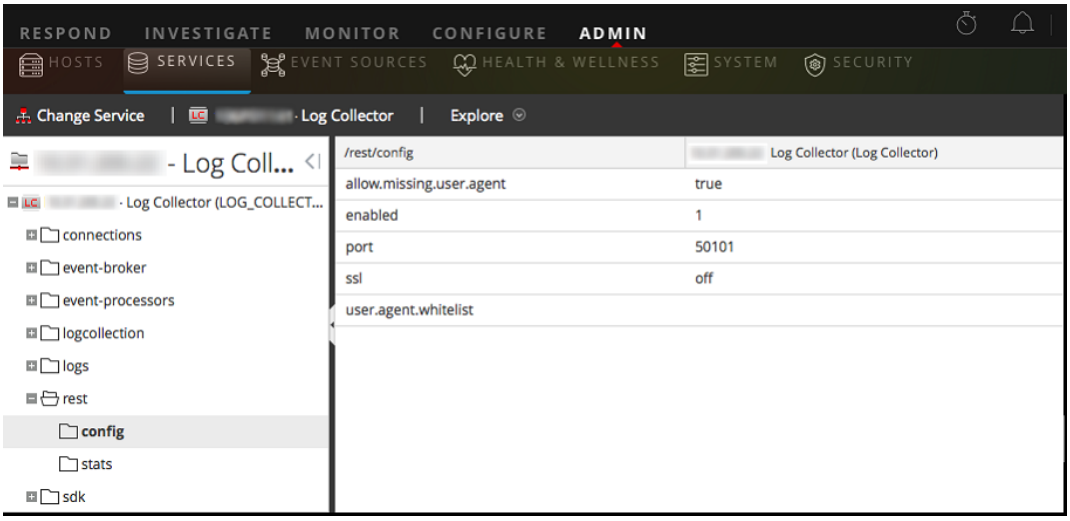


Sie sehen, dass der Bildschirm den Namen des Identitätsfeeds enthält, den Sie zuvor erstellt haben (in diesem Beispiel `infonetd_domain`).

Damit der Identitätsfeed ordnungsgemäß funktioniert, muss Port 50101 auf dem Log Collector aktiv sein und Sie müssen bestimmen, ob die SSL-Verschlüsselung aktiv ist.

d. Navigieren Sie zu **ADMIN > Services > *<einzurichtender Log Collector>***  **> Ansicht > Durchsuchen**.

e. Erweitern Sie im linken Bereich **REST > Konfig**.



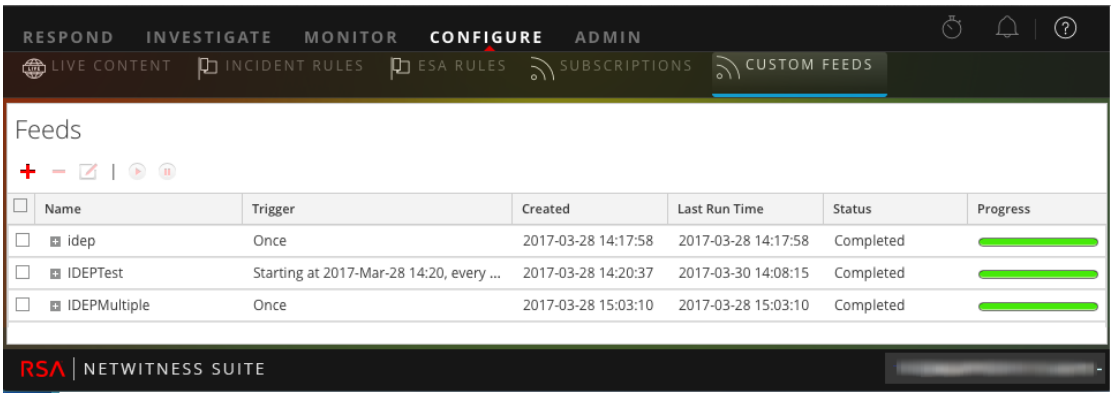
Damit REST aktiv ist, muss **aktiviert** auf **1** festgelegt sein.

f. Notieren Sie sich den Wert für **SSL**. Wenn SSL für Ihre Umgebung aktiviert werden soll, muss diese Option auf **Ein** festgelegt sein.

> **Hinweis:** Wenn Sie die Einstellung für die Option **aktiviert** oder **SSL** geändert haben, müssen Sie den Log Collector-Service neu starten, bevor Sie fortfahren.

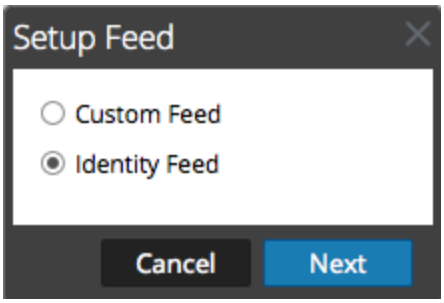
3. Navigieren Sie zu **Konfigurieren > Live Content > Benutzerdefinierte Feeds**.

Das Feedraster wird angezeigt.



4. Klicken Sie in der Symbolleiste auf +.

Das Dialogfeld Feed einrichten wird angezeigt.



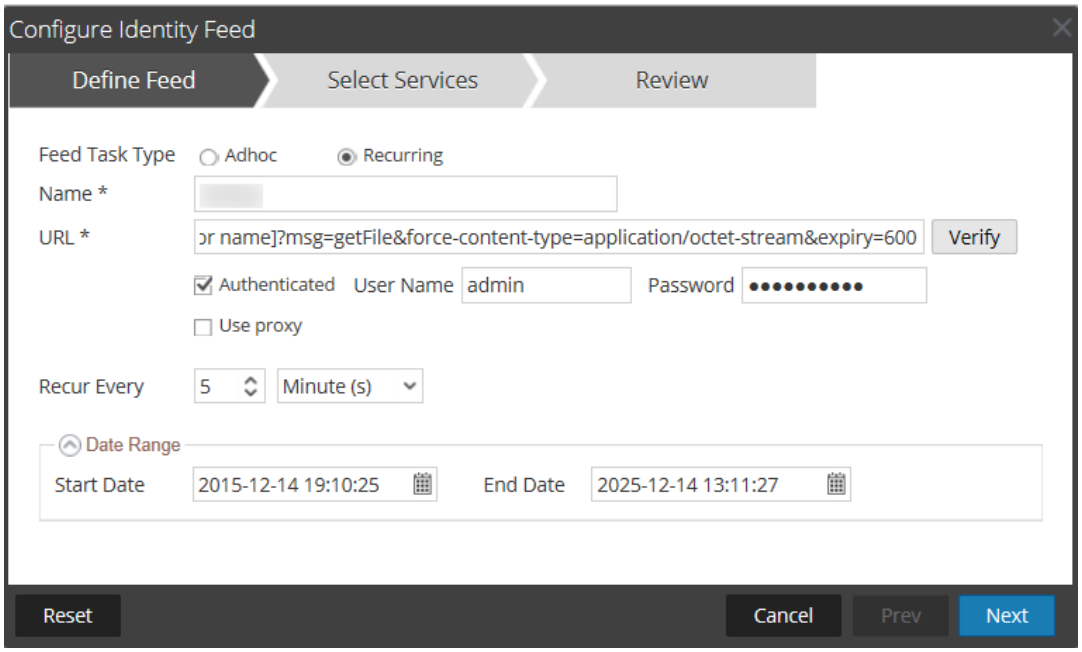
5. Vergewissern Sie sich, dass **Identitätsfeed** ausgewählt ist, und klicken Sie auf **Weiter**.

   Der Bereich „Identitätsfeed konfigurieren“ wird mit geöffneter Registerkarte **Feed definieren** angezeigt.

6. (Bedingungsabhängig) Sie können einen bedarfsorientierten oder einen wiederkehrenden Feed erstellen.

   - Um eine Identitätsfeedaufgabe nach Bedarf zu definieren, die einmal ausgeführt wird, wählen Sie **Ad hoc** im Feld **Typ der Feedaufgabe** aus, geben Sie den **Namen** des Feeds ein, suchen Sie nach dem Feed und öffnen Sie ihn.
   - Zum Definieren einer wiederkehrenden Identitätsfeedaufgabe, die wiederholt ausgeführt wird, wählen Sie im Feld **Typ der Feedaufgabe** die Option **Wiederholt** aus.

     Das Formular **Feed definieren** enthält die Felder für einen wiederkehrenden Feed.



Hinweis: RSA NetWitness Suite überprüft den Speicherort, an dem die Datei gespeichert ist, sodass Security Analytics bei jedem erneuten Aufruf automatisch nach der neuesten Datei suchen kann.

7. Geben Sie Werte in das URL-Feld ein und überprüfen Sie dieses.

   a. Geben Sie im Feld **URL** die URL ein, unter der sich die Feeddatendatei befindet. Dies ist die REST-API-Schnittstelle, die zuvor eingerichtet wurde. Sie benötigen die folgenden Informationen, um die URL zu bestimmen:

      - Die IP-Adresse des Log Collector, die verwendet wird, um die Identitätsfeeddatei zu erstellen.
      - Der Name der Identitätswarteschlange, wie in Schritt 2c festgelegt.
      - Gibt an, ob SSL auf dem REST-Port des Log Collector aktiviert ist, wie in Schritt 2f festgelegt.

      Dieser Wert wird wie folgt erstellt:

      - SSL aktiviert: `https://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`
      - SSL nicht aktiviert: `http://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

      Wenn wir also unser Beispiel von weiter oben verwenden, würden Sie in dieses Feld den folgenden vollständigen Wert eingeben:

      ```
      http://192.168.99.66:50101/event-processors/infonetd_domain?msg=getFile&force-content-type=application/octet-stream&expiry=600?msg=getFile&force-content-type=application/octet-stream&expiry=600
      ```

   b. Damit die URL-Überprüfung ordnungsgemäß ausgeführt werden kann, ist es wichtig, dass der Security Analytics-UI-Server auf den REST-API-Port (50101) des Log Collector zugreifen kann. Dies kann getestet werden, indem über SSH eine Verbindung mit dem Security Analytics-UI-Server hergestellt wird. Führen Sie dort den folgenden Befehl aus:

      - SSL aktiviert: `curl -vk https://<ip of log collector>:50101`
      - SSL nicht aktiviert: `curl -v http://<ip of log collector>:50101`

      Wenn der Befehl `curl` keine Verbindung herstellt, liegt möglicherweise ein Problem mit der Netzwerkfirewall oder mit der Weiterleitung zwischen dem Security Analytics-UI-Server und Log Collector vor.

      Beispiel für eine schlechte Verbindung:

      ```
      * About to connect() to 192.168.99.66 port 50105 (#0)
      * Trying 192.168.99.66... No route to host
      ```

```
* couldn't connect to host

* Closing connection #0

curl: (7) couldn't connect to host

Example of Good connection:

* About to connect() to 192.168.99.66 port 50105 (#0)

* Trying 192.168.99.66... connected

* Connected to 192.168.99.66 (192.168.99.66) port 50105
(#0)

> GET / HTTP/1.1

> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu)
libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18
libssh2/1.4.2

> Host: 192.168.99.66:50105

> Accept: */*

>

< HTTP/1.1 401 Unauthorized

< Content-Length: 71

< Connection: Keep-Alive

< Pragma: no-cache

< Expires: -1

< Cache-Control: no-cache, no-store, must-revalidate

< WWW-Authenticate: Basic realm="NetWitness"

< Content-Type: text/xml; charset=utf-8

<

<?xml version="1.0" encoding="utf-8"?>

<error>401 Unauthorized</error>

* Connection #0 to host 192.168.99.66 left intact

* Closing connection #0
```

8. Die REST-API erfordert einen Benutzernamen und ein Passwort, wenn sie versucht, die `identity_deploy.csv`-Datei vom Log Collector abzurufen. Dies kann ein beliebiger Benutzername bzw. ein beliebiges Passwort sein, der bzw. das auf dem Service selbst verfügbar ist. Informationen finden Sie im Thema „Ansicht Services-Sicherheit“ im

Leitfaden für Hosts und Services.

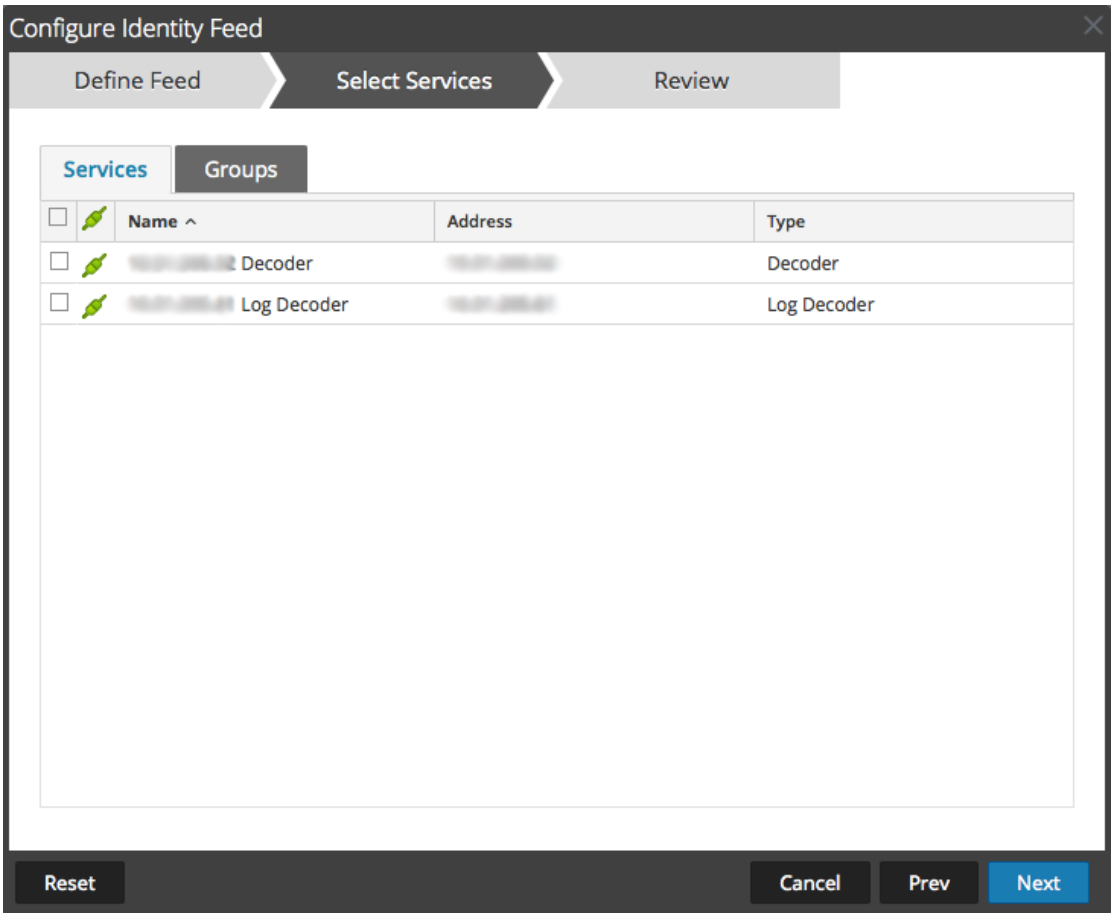
Um festzustellen, welche Konten zur Verfügung stehen, navigieren Sie zu **ADMIN > Services > <einzurichtender Log Collector> > Aktionen > Ansicht > Sicherheit**.

In der Tabelle „Benutzer“ sehen Sie alle Benutzer, die in diesem Schritt verwendet werden können. Es wird empfohlen, ein separates Benutzerkonto speziell für dieses Setup zu erstellen, das an keiner anderen Stelle in der Umgebung verwendet wird, um die Sicherheit zu erhöhen. Details finden Sie unter „Hinzufügen eines Benutzers und einer Rolle“ im *Handbuch Systemsicherheit und Benutzerverwaltung*. (Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.)

9. Führen Sie eine der folgenden Aktionen durch, um das Intervall für Wiederholungen zu definieren:
   - Legen Sie die Anzahl der Minuten, Stunden oder Tage zwischen den Wiederholungen des Feeds fest.
   - Geben Sie zum Definieren des Datumsbereichs für die Ausführung der Feedwiederholungen das **Startdatum** und die Startzeit sowie das **Enddatum** und die Endzeit an.
10. Wenn Sie SSL-Verschlüsselung verwenden, müssen Sie das REST-API-SSL-Zertifikat für den Log Collector auf dem Security Analytics-UI-Server installieren. Weitere Informationen finden Sie unter Importieren des SSL-Zertifikats.

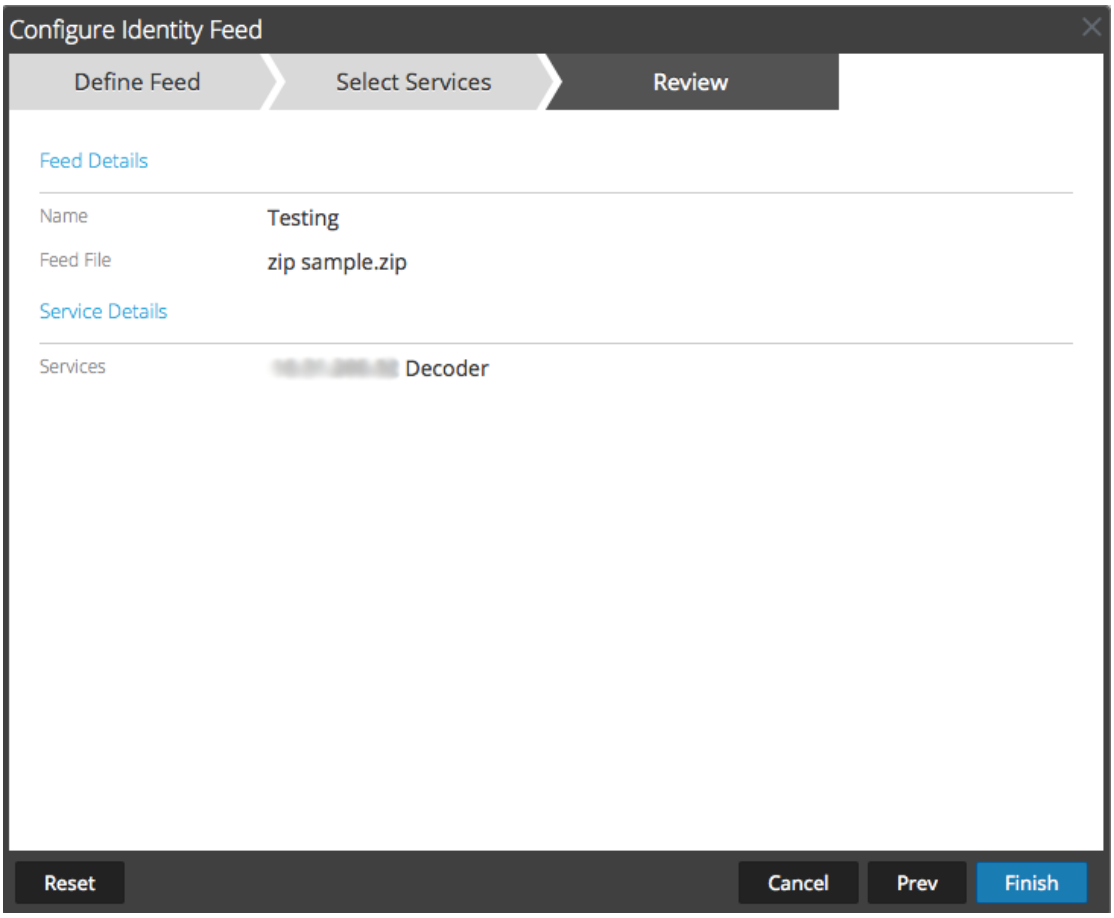
    Wenn nach dem Importieren des SSL-Zertifikats die Überprüfung der URL weiterhin fehlschlägt, lesen Sie URL des Identitätsfeeds kann nicht überprüft werden.
11. Klicken Sie auf **Verifizieren**, um die Konfiguration Ihres Identitätsfeeds zu überprüfen, bevor Sie das Formular „Services auswählen“ öffnen.
12. Klicken Sie auf **Weiter**.

    Das Formular „Services auswählen“ wird angezeigt.



13. Um Services zu identifizieren, in denen der Feed bereitgestellt werden soll, wählen Sie einen oder mehrere Decoders und Log Decoders aus und klicken Sie auf **Weiter**.
14. Klicken Sie auf die Registerkarte **Gruppen**, wählen Sie eine Gruppe aus und klicken Sie auf **Weiter**

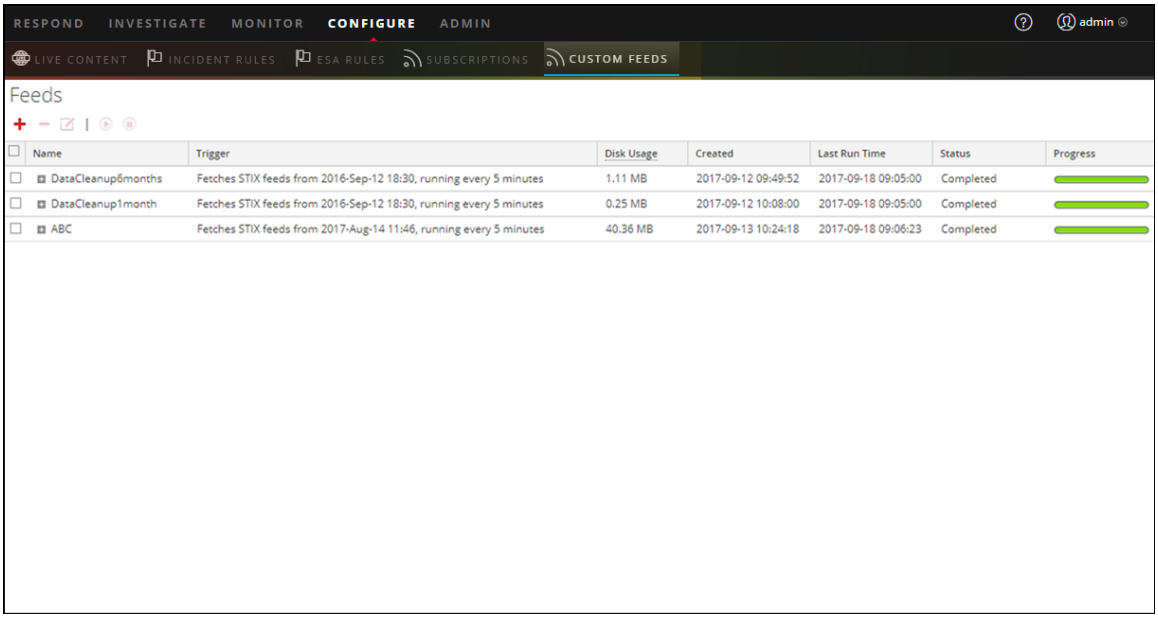
    Das Formular Überprüfung wird angezeigt.



Hinweis: Wenn eine Gruppe von Geräten mit Decoder und Log Decoder zum Erstellen von wiederkehrenden oder benutzerdefinierten Feeds verwendet wird und diese Gruppe gelöscht wird, können Sie den Feed bearbeiten und eine neue Gruppe zum Feed hinzufügen.

15. Bevor Sie auf **Fertigstellen** klicken, können Sie jederzeit Folgendes tun:
    - Auf **Abbrechen** klicken, um den Assistenten zu schließen, ohne die Feeddefinition zu speichern
    - Auf **Zurücksetzen** klicken, um die Daten im Assistenten zu löschen
    - Auf **Weiter** klicken, um das nächste Formular anzuzeigen (wenn nicht das letzte Formular angezeigt wird)
    - Auf **Vorheriges** klicken, um das vorherige Formular anzuzeigen (wenn nicht das erste Formular angezeigt wird)
16. Überprüfen Sie die Feedinformationen und klicken Sie auf **Fertigstellen**, wenn diese korrekt sind.

Nach der erfolgreichen Erstellung der Feeddefinitionsdatei wird der Assistent für das Erstellen von Feeds geschlossen. Der Feed und die zugehörige Tokendatei werden im Feedraster aufgeführt und die Fertigstellung wird in einem Fortschrittsbalken nachverfolgt. Sie können den Eintrag ein- oder ausblenden, um festzustellen, wie viele Services enthalten sind und welche erfolgreich waren.



Importieren des SSL-Zertifikats

Wenn für den Log Collector des Identitätsfeeds SSL konfiguriert ist, führen Sie diese Schritte aus, um das SSL-Zertifikat des Log Collector in den Keystore des Security Analytics-UI-Servers zu importieren. Wenn dieses Zertifikat nicht importiert wird, ist der Security Analytics-UI-Server nicht in der Lage, die Identitätsfeeddatei vom Log Collector abzurufen.

1. Um das SSL-Zertifikat vom Log Collector abzurufen, stellen Sie über SSH eine Verbindung mit dem Security Analytics-UI-Server her und führen Sie den folgenden Befehl aus:

   ```
   echo -n | openssl s_client -connect <HOST>:<PORT> | sed -ne
   '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/<SERVERNAME>.cert
   ```

   Mit diesem Befehl wird das SSL-Zertifikat in `/tmp/<SERVERNAME>.cert` gespeichert.

   Beispiel:

   ```
   echo -n | openssl s_client -connect 192.168.99.66:50101 | sed
   -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/logcollector.cert
   ```

2. Um das SSL-Zertifikat in den Security Analytics-UI-Server zu importieren, stellen Sie über SSH eine Verbindung mit dem UI-Server her und führen Sie den folgenden Befehl aus:

```
keytool -importcert -alias <name an alias for the cert> -file
<the cert file pathname> -keystore /etc/pki/java/cacerts
```

Beispiel:

```
keytool -importcert -alias logcollector01 -file
/tmp/logcollector.cert -keystore /etc/pki/java/cacerts
```

3. Das System fordert ein Passwort an. Geben Sie das Passwort für den Keystore auf dem Security Analytics-UI-Server ein, nicht für den Jetty-Keystore. Das Standardpasswort lautet **changeit**.
4. Starten Sie **jettysrv** neu, um es Jetty zu erlauben, das neue Zertifikat im Speicher zu lesen.

URL des Identitätsfeeds kann nicht überprüft werden

Wenn die URL des Identitätsfeeds nicht überprüft werden kann und Sie SSL verwenden, vergewissern Sie sich, dass Sie die Schritte unter Importieren des SSL-Zertifikats ordnungsgemäß durchgeführt haben.

Wenn weiterhin Probleme auftreten, ist es möglich, dass der interne Name des Zertifikats nicht mit dem Hostnamen des Log Collector übereinstimmt. Durch das folgende Verfahren wird dies überprüft.

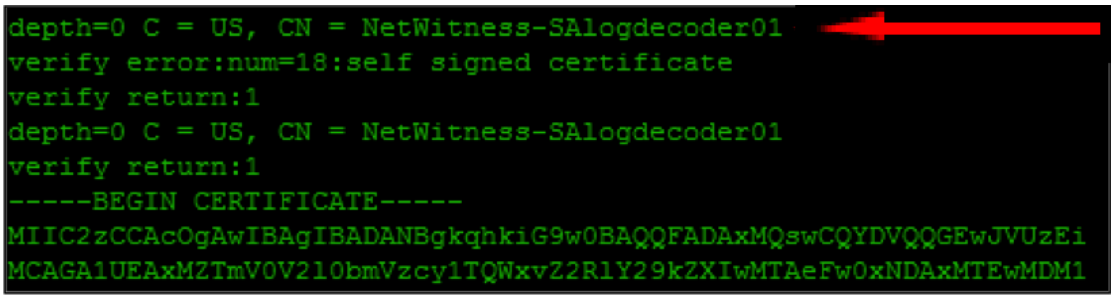
1. Stellen Sie über SSH eine Verbindung mit dem Security Analytics-UI-Server her.
2. Führen Sie den folgenden Befehl aus, um den CN-Namen des SSL-Zertifikats auszugeben:

```
echo -n | openssl s_client -connect <log decoder>:50101 | sed
-ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
```

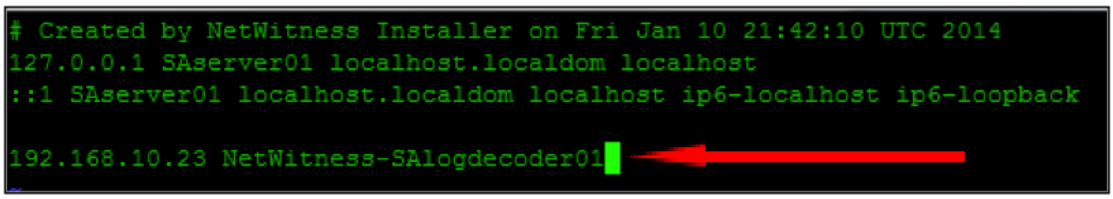
Beispiel:

```
echo -n | openssl s_client -connect salogdecoder01:50101 |
sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
```

3. Rufen Sie den CN-Namen des SSL-Zertifikats ab.



4. Bearbeiten Sie die `/etc/hosts`-Datei und fügen Sie die IP-Adresse und den CN-Namen zur Datei hinzu.



5. Starten Sie die Netzwerkservice auf der Appliance neu.
6. Vergewissern Sie sich, dass der Name in der Datei **/etc/hosts** anstelle des vollständig qualifizierten Domainnamens oder der IP-Adresse in der URL des Identitätsfeeds verwendet wird.
7. Überprüfen Sie die URL des Identitätsfeeds erneut.

Untersuchen eines Identitätsfeeds

Ein Identitätsfeed dient zum Nachverfolgen von interaktiven Anmeldeereignissen des Windows-Betriebssystems. Interaktive Abmeldeereignisse werden nicht von Identitätsfeeds nachverfolgt.

Damit ein Identitätsfeed Ereignisse verarbeiten und kennzeichnen kann, müssen diese mithilfe eines Windows-Protokollsammlungsmoduls erfasst werden, auf dem ein aktiver Domain-Controller/Nicht-Domain-Controller konfiguriert ist. Beachten Sie, dass Identitätsfeeds nur über einen Identitätsfeed-Ereignisprozessor verarbeitet werden können.

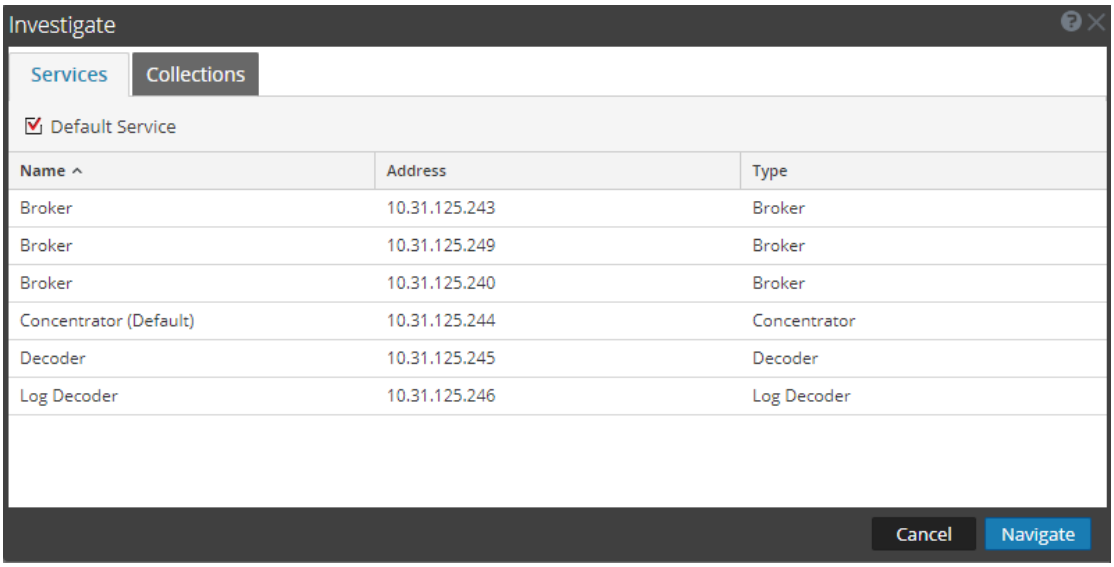
Hinweis: Ein Identitätsfeed kann Anmeldeereignisse nur jeweils nacheinander nachverfolgen. Wenn zwei Benutzer sich gleichzeitig bei einem System anmelden, überschreibt der zweite Benutzer die Daten des ersten Benutzers im Identitätsfeed.

Nach dem Erstellen eines Identitätsfeeds können Sie die Ergebnisse aufrufen, indem Sie den Feed näher untersuchen.

So untersuchen Sie einen konfigurierten Identitätsfeed:

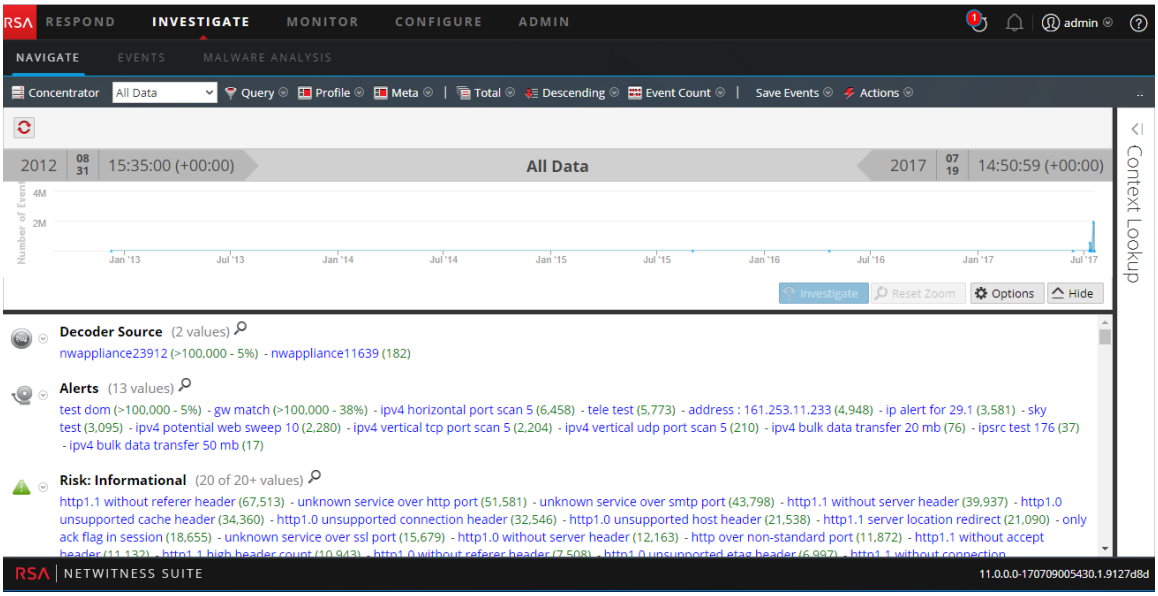
1. Navigieren Sie zu **UNTERSUCHEN > Navigieren**.

   Wenn kein Standardservice ausgewählt ist, wird das Dialogfeld „Untersuchen“ angezeigt.



2. Wählen Sie einen Service aus, in der Regel einen Concentrator, und klicken Sie auf **Navigieren**.
3. Wählen Sie **Werte laden** aus, um Metadaten abzurufen.

Führen Sie im Bereich „Werte“ einen Bildlauf nach unten aus, um die in der folgenden Abbildung dargestellten Metaschlüssel zu suchen.



Der Identitätsfeed liefert Informationen an die ausgewählte Decoder und Log Decoder. Er ordnet die Host-IP-Adresse des Windows-Betriebssystems dem Benutzer zu, der sich bei diesem Host anmeldet, um alle mit dieser IP-Adresse verbundenen Protokolle zu kennzeichnen und zu untersuchen.

Bearbeiten eines Feeds

Dieses Thema enthält Anweisungen zur Bearbeitung eines benutzerdefinierten Feeds mithilfe des Assistenten für benutzerdefinierte Feeds.

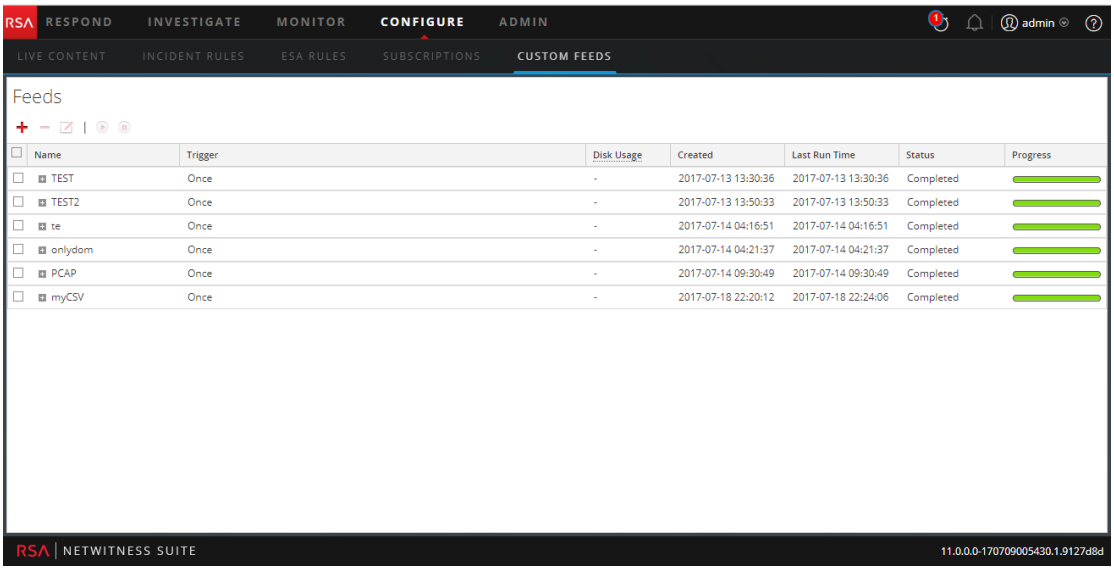
Nach Abschluss dieses Verfahrens haben Sie:

- einen bestehenden benutzerdefinierten Feed geöffnet.
- den Feed (**.zip**-Format) oder die Datei, die zur Erstellung des Feeds verwendet wird (**.csv** oder **.xml**), heruntergeladen und bearbeitet.
- den Feed mit der aktualisierten Datei und neuen Feedspezifikationen erneut erstellt.

So bearbeiten Sie einen vorhandenen Feed:

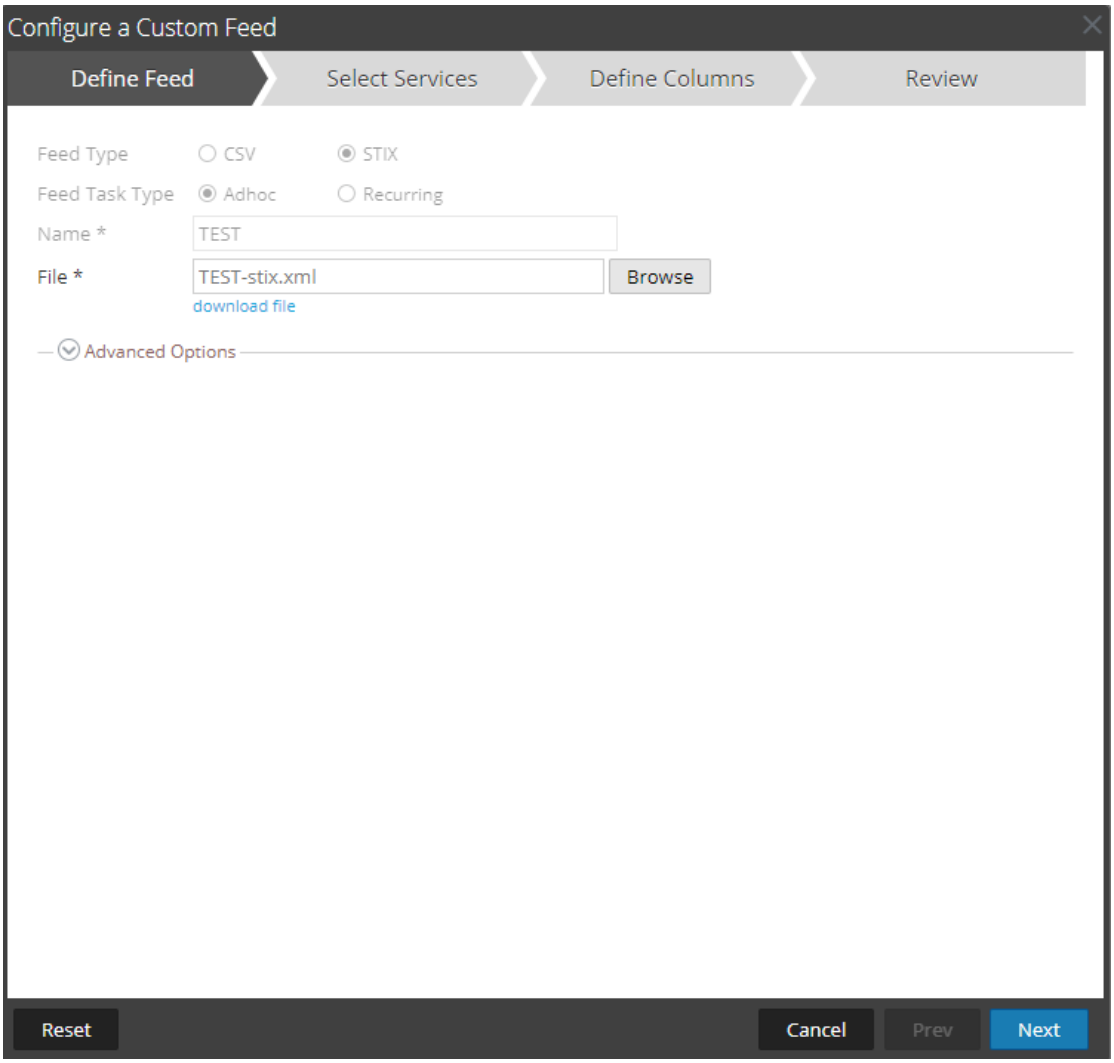
1. Navigieren Sie zu **KONFIGURIEREN > BENUTZERDEFINIERTE FEEDS**.

   Die Ansicht „Benutzerdefinierte Feeds“ wird angezeigt.



2. Wählen Sie auf der Symbolleiste einen Feed aus und klicken Sie auf .

   Der Bereich Benutzerdefinierten Feed konfigurieren oder Identitätsfeed konfigurieren wird im Assistenten für benutzerdefinierte Feeds geöffnet.



3. Wenn Sie die Feeddatei bearbeiten möchten:
   a. Klicken Sie auf **Datei herunterladen**.

      Bei Identitätsfeeds wird die .zip-Datei heruntergeladen. Bei benutzerdefinierten Feeds wird die .csv- oder .xml-Datei auf das lokale Dateisystem heruntergeladen.

   b. Bearbeiten und speichern Sie die Datei.

   c. Suchen Sie in der Registerkarte **Feed definieren** nach der bearbeiteten Datei und öffnen Sie sie.

4. Bearbeiten Sie alle anderen Parameter auf den Registerkarten **Feed definieren**, **Services auswählen** und **Spalten definieren**, die für den Feedtyp gelten.
5. Bevor Sie auf **Fertigstellen** klicken, können Sie jederzeit Folgendes tun:

- Auf **Abbrechen** klicken, um den Assistenten zu schließen, ohne die Änderungen zu speichern
- Auf **Zurücksetzen** klicken, um die Daten im Assistenten zu löschen
- Auf **Weiter** klicken, um das nächste Formular anzuzeigen (wenn nicht das letzte Formular angezeigt wird)
- Auf **Vorheriges** klicken, um das vorherige Formular anzuzeigen (wenn nicht das erste Formular angezeigt wird)

6. Überprüfen Sie die Feedinformationen in der Registerkarte **Überprüfen** und klicken Sie auf **Fertigstellen**, wenn diese korrekt sind.

Der Feed wird zur Feedliste hinzugefügt und in einem Fortschrittsbalken wird der Abschluss nachverfolgt. Nach der erfolgreichen Erstellung der Feeddefinitionsdatei wird der Assistent für das Erstellen von Feeds geschlossen und der Feed und die zugehörige Tokendatei in der Liste „Feeds“ aufgeführt. Sie können den Eintrag ein- oder ausblenden, um zu sehen, wie viele Services enthalten sind und welche Services erfolgreich sind.

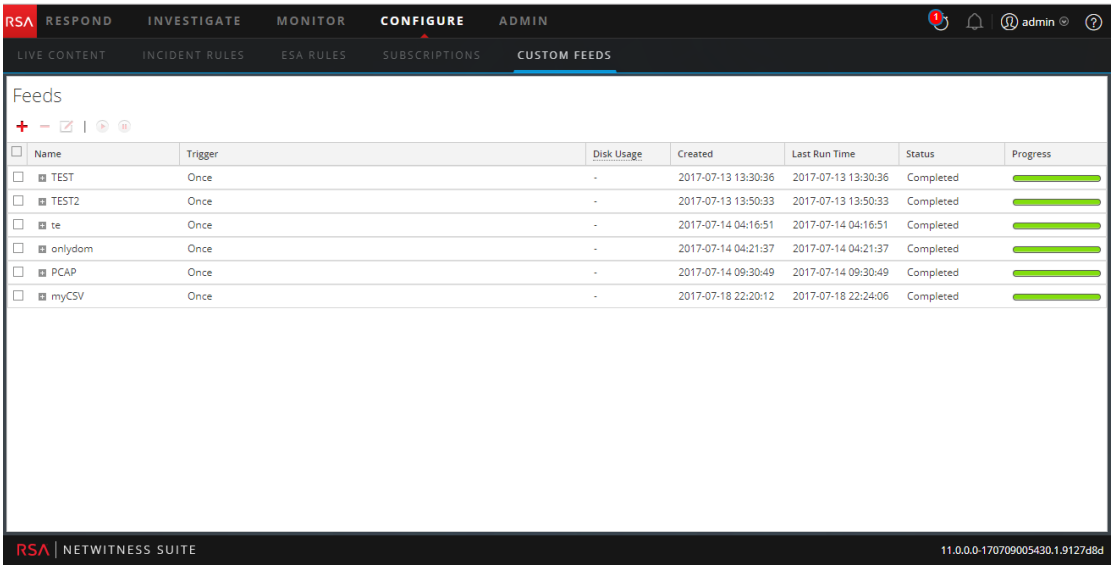
Entfernen eines Feeds

Dieses Thema enthält Anweisungen zum Entfernen eines Feeds.

So entfernen Sie einen Feed:

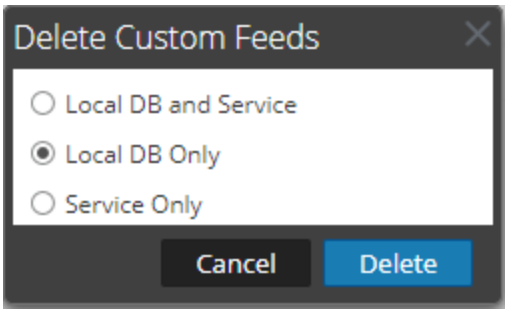
1. Navigieren Sie zu **KONFIGURIEREN > BENUTZERDEFINIERTE FEEDS**.

   Die Ansicht „Benutzerdefinierte Feeds“ wird angezeigt.



2. Wählen Sie auf der Symbolleiste einen Feed aus und klicken Sie auf .

   Das Dialogfeld „Benutzerdefinierte Feeds löschen“ wird angezeigt.



Sie können eine der folgenden Optionen wählen, um den Feed zu löschen:

- Wenn Sie zum Löschen des Feeds die Option **Lokale DB und lokaler Service** wählen, wird der Feed sowohl vom Service als auch aus dem NetWitness Suite-Posteingang gelöscht. Der gelöschte Feed wird nicht mehr auf der NetWitness Suite-Benutzeroberfläche angezeigt.
- Wenn Sie zum Löschen des Feeds die Option **Nur lokale DB** wählen, wird der Feed aus dem lokalen NetWitness Suite-Posteingang gelöscht. Der gelöschte Feed wird nicht mehr auf der NetWitness Suite-Benutzeroberfläche angezeigt, die zuletzt bereitgestellte Version der Feeds ist jedoch im Service vorhanden. Die nicht bereitgestellten Feeds werden permanent gelöscht.
- Wenn Sie zum Löschen des Feeds die Option **Nur Service** wählen, wird der Feed aus dem Service gelöscht. Der gelöschte Feed wird auf der NetWitness Suite-Benutzeroberfläche angezeigt und kann erneut bereitgestellt werden.

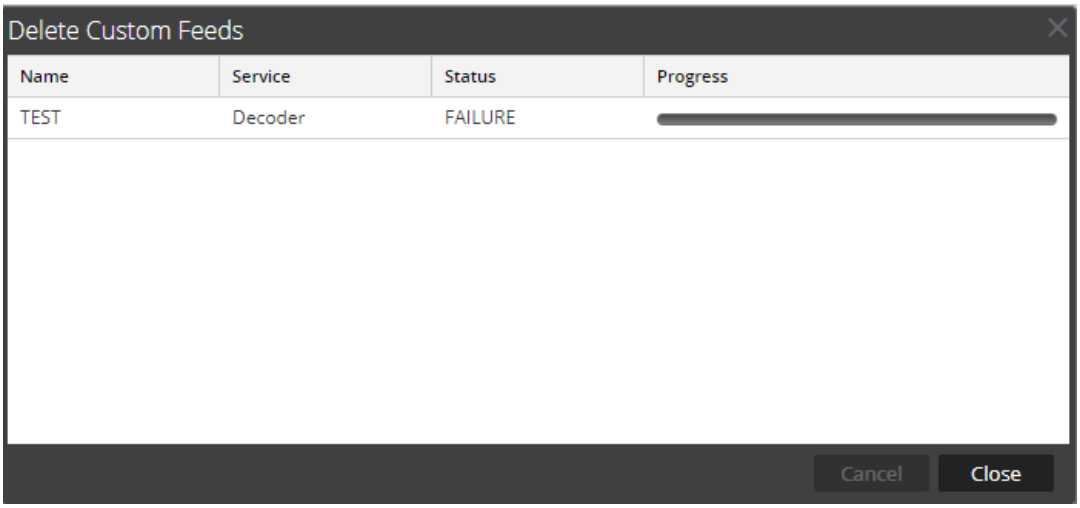
3. Geben Sie an, wo Sie den Feed löschen möchten, und klicken Sie auf **Löschen**.

   Ein Warnmeldungsdialogfeld wird angezeigt.

4. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie den Feed aus den ausgewählten Bereichen löschen möchten.

   - Wenn Sie als Option **Nur lokale DB** auswählen, wird der Feed gelöscht.
   - Wenn Sie zum Löschen des Feeds die Option **Lokale DB und lokaler Service** oder **Nur Service** auswählen, wird die Ansicht „Benutzerdefinierte Feeds löschen“ angezeigt, in

der Sie den Fortschritt des Löschvorgangs des Services verfolgen können.



Verschiedene Live-Services-Verfahren

Dieser Abschnitt behandelt die folgenden Verfahren:

- Hinzufügen abonnierter Ressourcen für die Bereitstellung zu Services
- Erstellen eines Ressourcenpakets
- Löschen eines Abonnements
- Anzeigen von Ressourcendetails in der Live-Ressourcenansicht
- Herunterladen einer Ressource
- Suchen einer bereitgestellten Ressourcen und Entfernen aus Services
- Löschen abonnierter Ressourcen aus dem Bereitstellungsabonnementraster
- Aufrufen von Ergebnissen als Liste oder detailliert
- Abonnieren und Deabonnieren einer Ressource
- Ressourcendetails anzeigen
- Anzeigen der abonnierten Ressourcen, die für Services bereitgestellt werden sollen

Hinzufügen abonnierter Ressourcen für die Bereitstellung zu Services

1. Navigieren Sie zur Registerkarte **KONFIGURIEREN > ABONNEMENTS > Bereitstellungen**.
2. Wählen Sie im Bereich **Gruppen** eine Gruppe aus.
   Abonnierte Ressourcen werden, falls vorhanden, im Bereich „Abonnements“ der Registerkarte „Bereitstellungen“ aufgeführt.
3. Klicken Sie im Bereich **Abonnements** auf  .
   Das Dialogfeld „Abonnement hinzufügen“ wird angezeigt, in dem die zur Bereitstellung verfügbaren Abonnements aufgelistet sind.
4. Wählen Sie die abonnierten Ressourcen aus, die Sie für die Servicegruppe bereitstellen möchten.
5. Klicken Sie auf **Speichern**.
   Das Dialogfeld wird geschlossen und die Abonnements werden der Liste auf der Registerkarte „Bereitstellungen“ im Bereich „Abonnements“ hinzugefügt. Dadurch werden die Ressourcen zur Bereitstellung bei der nächsten Synchronisation verfügbar gemacht.

Erstellen eines Ressourcenpakets

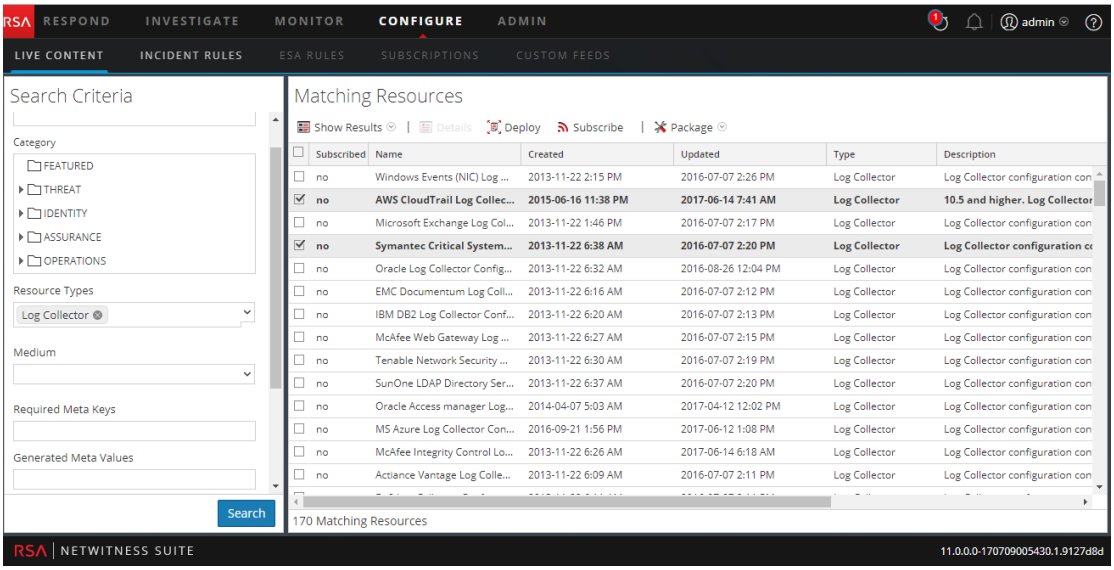
Sie können ein Ressourcenpaket erstellen, das Sie in einer .zip-Datei speichern und für andere freigeben können.

Voraussetzungen

Eine Vorbedingung für die Erstellung von Ressourcenpaketen ist die Konfiguration der Verbindung und Synchronisation zwischen dem CMS-Server und NetWitness Suite und die Möglichkeit, in der Benutzeroberfläche nach Ressourcen suchen zu können.

So erstellen Sie ein Ressourcenpaket:

1. Wählen Sie im Raster „Übereinstimmende Ressourcen“ die Ressourcen aus, die das Paket enthalten soll.



2. Wählen Sie **Paket** > **Erstellen** aus:

   NetWitness Suite erstellt eine **.zip**-Datei, die die ausgewählten Ressourcen enthält, und zeigt das folgende Dialogfeld an, in dem Sie die .zip-Datei öffnen oder auf einem Netzlaufwerk speichern können, sodass Sie die Ressourcen im Paket freigeben oder zu einem späteren Zeitpunkt bereitstellen können.

   NetWitness Suite benennt das Paket mit einem generischen Namen. Sie sollten es beim Speichern umbenennen, damit Sie die im Paket enthaltenen Ressourcen erkennen.

Löschen eines Abonnements

Wenn Sie ein Abonnement einer Ressource löschen, werden bereitgestellte Instanzen der Ressource nicht gelöscht. Die bereitgestellte Ressource bleibt auf den Services, bis sie explizit gelöscht wird, aber die Ressource wird nicht länger mit der Ressource in NetWitness Suite Live synchronisiert.

So löschen Sie ein Abonnement:

1. Wählen Sie auf der Registerkarte **Abonnements** die Abonnements aus, die Sie löschen möchten.
2. Klicken Sie auf .

   Ein Dialogfeld fordert Sie auf, zu bestätigen, dass Sie das Abonnement löschen möchten.
3. Klicken Sie zur Bestätigung auf **Ja**.

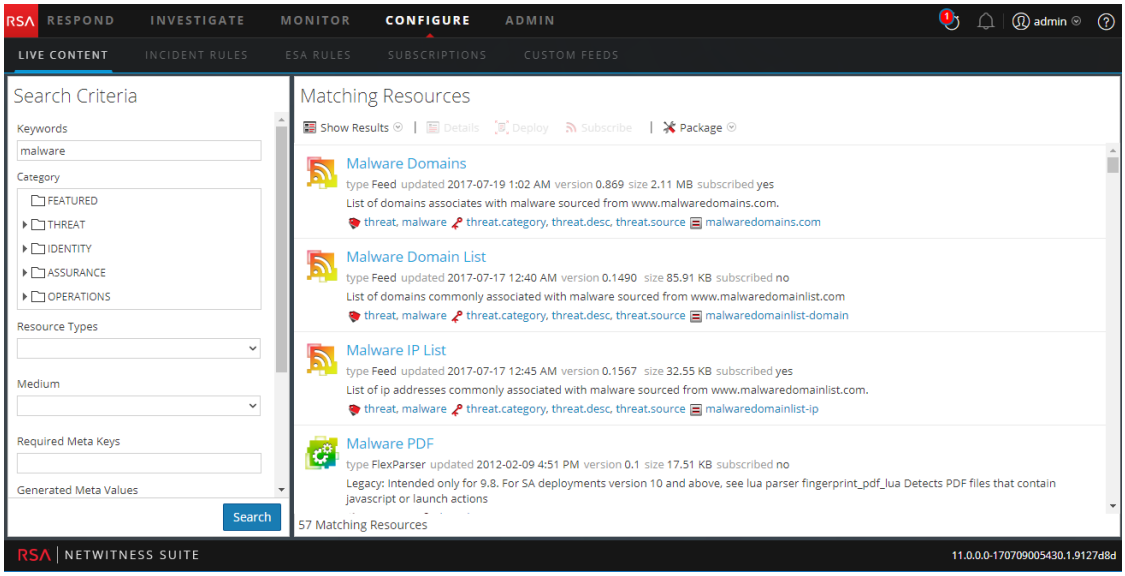
   Das Abonnement wird von der Abonnementliste gelöscht, aber alle bereitgestellten Instanzen der abonnierten Ressource bleiben auf den Services.

Anzeigen von Ressourcendetails in der Live-Ressourcenansicht

Nachdem Sie eine Ressource (in der Ansicht „Live-Ressource“) ausgewählt haben, können Sie ausführliche Informationen aufrufen.

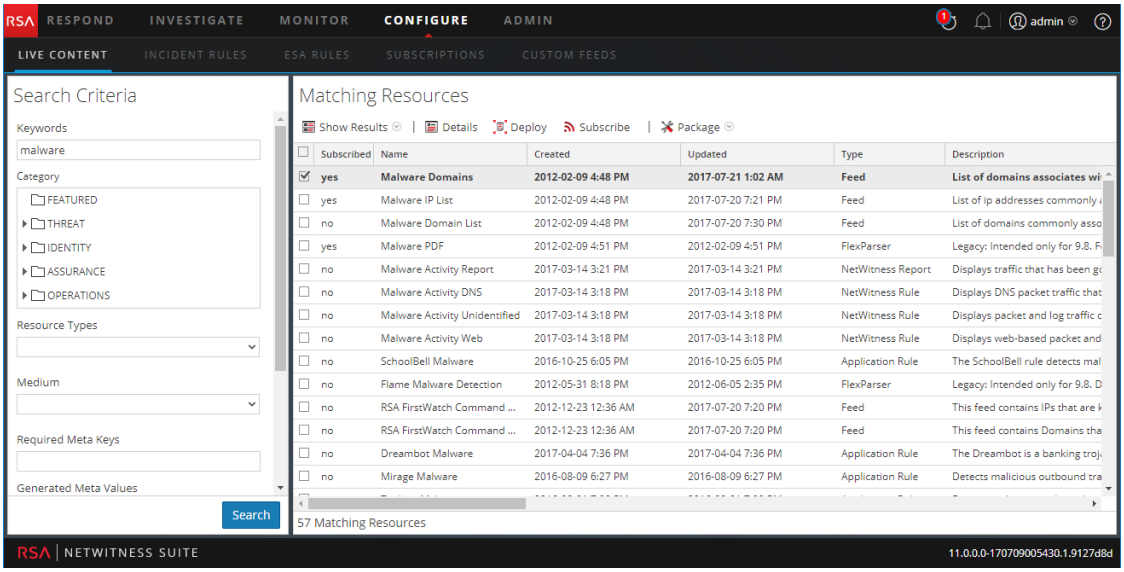
Um eine separate Registerkarte in der Live-Ressourcenansicht mit den Details einer ausgewählten Ressource anzuzeigen, führen Sie einen der folgenden Schritte aus:

- Wenn Sie **Detaillierte Ergebnisse** anzeigen, klicken Sie auf das Symbol des Ressourcentyps oder auf den Ressourcennamen.



- Wenn Sie sich die Listenansicht der Ergebnisse anzeigen lassen, doppelklicken Sie auf eine

Ressource oder wählen Sie eine Ressource aus und klicken Sie auf **Details**.



Herunterladen einer Ressource

Sie können in der Live-Ressourcenansicht eine einzelne Ressource herunterladen.

So laden Sie eine Ressource herunter:

1. Navigieren Sie zu **KONFIGURIEREN > Live-Inhalte**.
2. Geben Sie im Bereich **Suchkriterien** die Kriterien ein, die die Ressourcen zurückgeben, die Sie herunterladen möchten.
3. Wählen Sie eine einzelne Ressource aus und klicken Sie auf Details.
4. Klicken Sie auf Download.

Die Ressource wird als ZIP-Archiv in Ihrem lokalen Ordner für Downloads gespeichert.

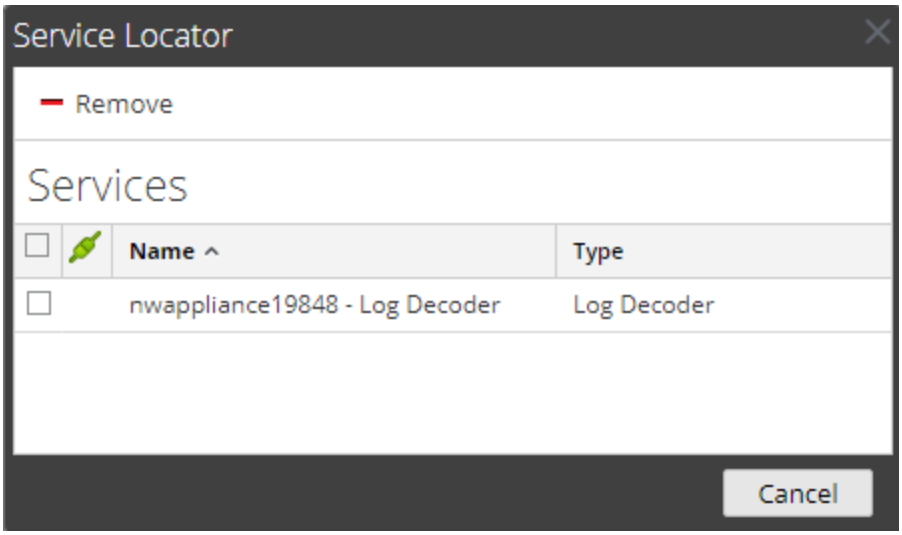
Suchen einer bereitgestellten Ressourcen und Entfernen aus Services

Sie können eine bereitgestellte Ressource von Services in der Ansicht Live-Ressourcenansicht finden und löschen.

So zeigen Sie eine Liste mit Services an, auf denen eine Ressource bereitgestellt ist:

1. Wenn eine Ressource in der Ansicht **Ressource** angezeigt wird, klicken Sie auf Service Locator.

   Das Dialogfeld „Servicesuche“ wird angezeigt.



2. Wählen Sie in der Liste **Services** einen oder mehrere Services aus.
3. Klicken Sie auf .

   Die Ressource wird vom ausgewählten Service gelöscht.

Löschen abonnierter Ressourcen aus dem Bereitstellungsabonnementraster

Abonnements, die für eine Bereitstellung in einer Servicegruppe ausgewählt wurden, werden während der Synchronisation bereitgestellt. Sie können Abonnements in der Live-Ansicht „Konfigurieren“ auf der Registerkarte „Bereitstellungen“ im Bereich „Abonnements“ entfernen, dabei bleiben jedoch alle Abonnements bereitgestellt, die schon in Services bereitgestellt wurden.

So entfernen Sie Ressourcen von der Registerkarte „Bereitstellungen“ im Bereich „Abonnements“:

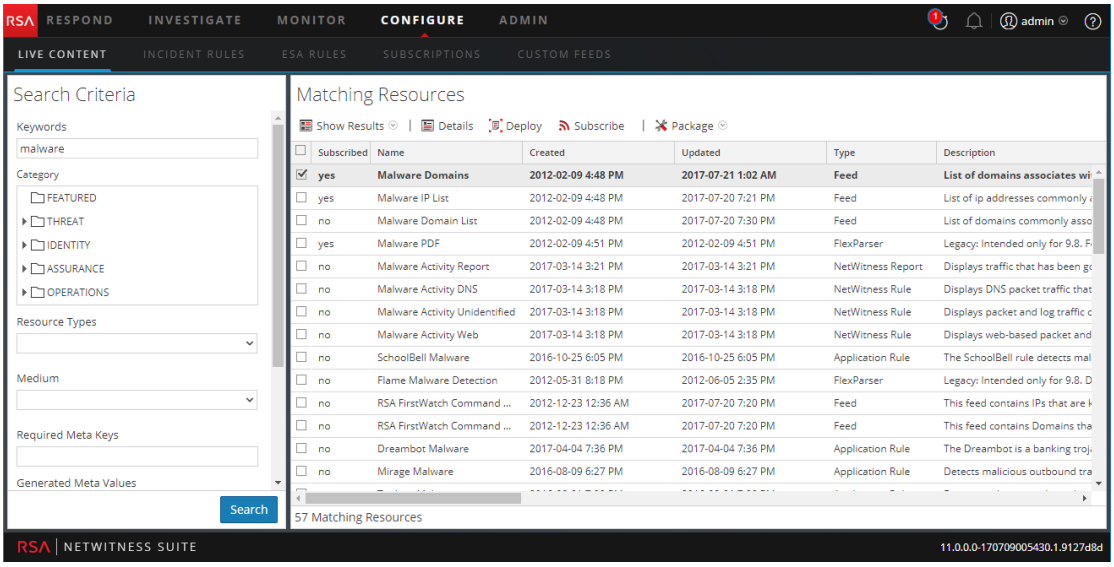
1. Wählen Sie im Bereich **Gruppen** eine Gruppe aus.

   Abonnierte Ressourcen, sofern vorhanden, werden im Bereich „Abonnements“ aufgeführt.
2. Klicken Sie im Bereich „Abonnements“ auf .

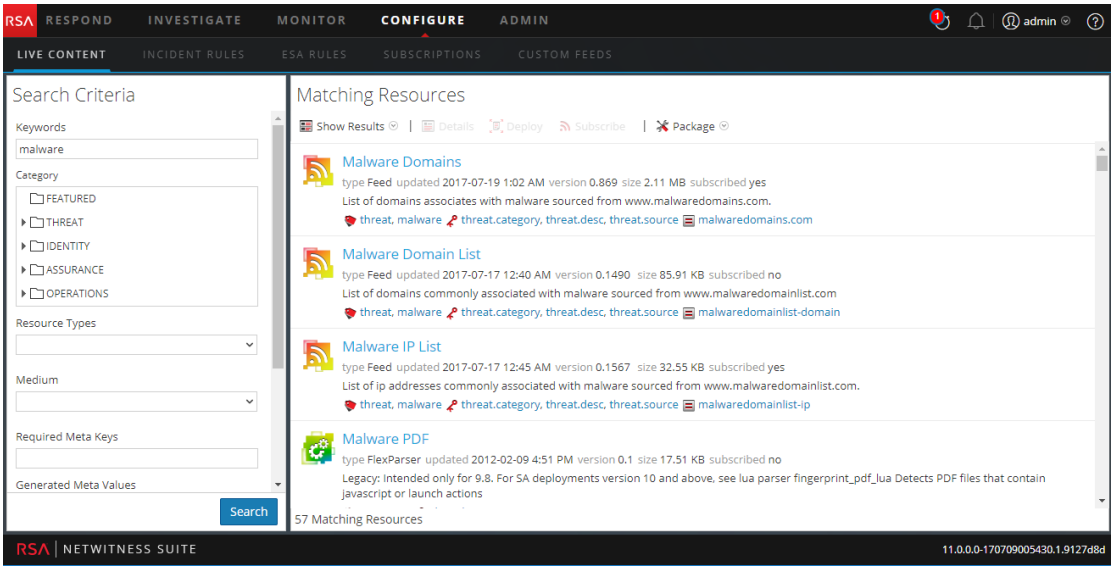
   In einem Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Ressource aus der Servicegruppe löschen möchten. Die Ressource wird von der Registerkarte „Bereitstellungen“ im Bereich „Abonnements“ entfernt, aber nicht aus den Services, für die sie bereitgestellt wurde.

Aufrufen von Ergebnissen als Liste oder detailliert

1. Um von der detaillierten Ansicht zur Rasteransicht zu wechseln, wählen Sie **Ergebnisse anzeigen > Raster** aus.



2. Um zur detaillierten Ansicht zu wechseln, wenn die Rasteransicht aktiviert ist, wählen Sie **Ergebnisse anzeigen > Raster** aus.



Abonnieren und Deabonnieren einer Ressource

Abonnieren

Wenn Sie Ressourcen abonnieren, erhalten Sie Benachrichtigungen, wenn neue Versionen der Ressourcen verfügbar sind.

So abonnieren Sie eine Ressource:

1. Navigieren Sie zu „Live“ > Ansicht „Suche“.
2. Geben Sie im Bereich **Suchkriterien** die Suchkriterien ein und klicken Sie auf **Suchen**.
3. Wählen Sie eine oder mehrere Ressourcen aus und klicken Sie auf Subscribe.

   Ein Bestätigungsdialogfeld wird angezeigt: **Durch das Abonnement dieser Ressourcen geben Sie an, dass Sie benachrichtigt werden möchten, wenn neue Versionen verfügbar sind.**
4. Zur Bestätigung, dass Sie die Ressource abonnieren möchten, klicken Sie auf **OK**.

   Die Ressource wird den Abonnements hinzugefügt, die auf der Registerkarte Abonnements gemanagt werden, und steht auf der Registerkarte Bereitstellungen zur Bereitstellung zur Verfügung.

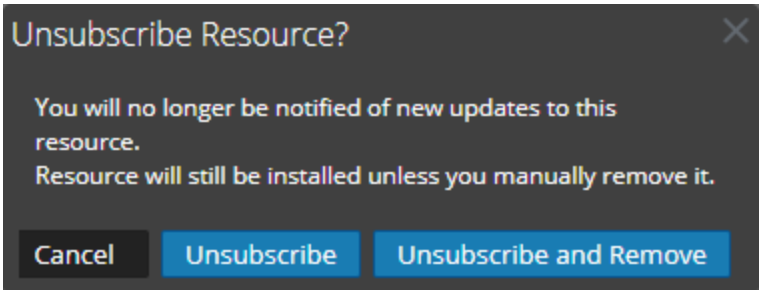
Abonnement beenden

Wenn Sie ein Ressourcenabonnement beenden, haben Sie die Wahl, ob Sie die Ressourcen auf den Services, auf denen sie bereitgestellt wurde, bestehen lassen oder aus den Services entfernen möchten.

So beenden Sie ein Ressourcenabonnement:

1. Eine Ressource wirdunter **ABONNEMENTS** angezeigt. Klicken Sie auf Unsubscribe.

   Ein Bestätigungsdialogfeld wird angezeigt.



2. Führen Sie einen der folgenden Schritte aus:
   - Zur Bestätigung, dass Sie das Abonnement der Ressource beenden möchten und sie auf den Services, auf denen sie bereitgestellt wurde, belassen möchten, klicken Sie auf **Abonnement beenden**.
   - Zur Bestätigung, dass Sie das Abonnement der Ressource beenden möchten und sie aus den Services, auf denen sie bereitgestellt wurde, entfernen möchten, klicken Sie auf **Abonnement beenden und aus Services entfernen**.

- Wenn Sie das Dialogfeld schließen möchten, ohne das Abonnement zu beenden, klicken Sie auf **Abbrechen**.

Die ausgewählte Aktion wird angewendet.

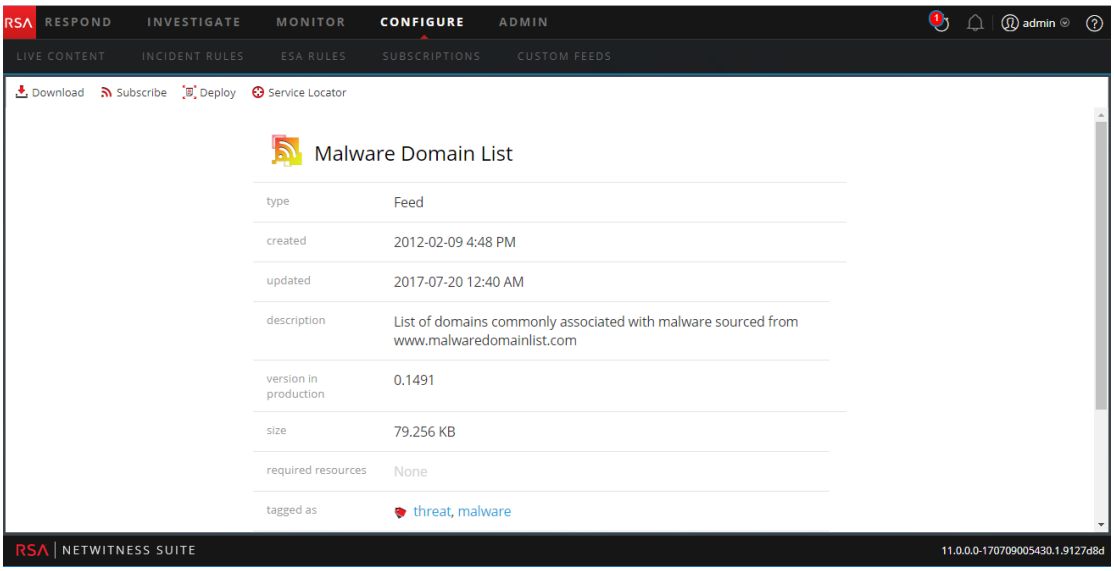
Ressourcendetails anzeigen

Sie können ausführliche Informationen über eine abonnierte Ressource in der Ansicht Ressourcen anzeigen.

So zeigen Sie Details an:

1. Wählen Sie in der **Registerkarte Abonnements** ein einziges Abonnement aus.
2. Klicken Sie auf Details .

   Die Details der Ressource werden in der Ansicht „Ressource“ angezeigt.



Anzeigen der abonnierten Ressourcen, die für Services bereitgestellt werden sollen

In der Ansicht „Live-Konfiguration“ > Registerkarte „Bereitstellungen“ können Sie die abonnierten Ressourcen anzeigen, die für die Bereitstellung in Services ausgewählt wurden.

So zeigen Sie abonnierte Ressourcen an, die für die Bereitstellung in Services ausgewählt wurden:

Wählen Sie im Bereich **Gruppen** eine Gruppe aus und erweitern Sie diese, um die Services in der Gruppe aufzurufen.

Die für die Bereitstellung ausgewählten Ressourcenabonnements werden im Bereich „Abonnements“ auf der Registerkarte „Bereitstellungen“ angezeigt.

Troubleshooting

Dieser Abschnitt enthält Anweisungen für das Troubleshooting bei Problemen, die auftreten können, wenn Sie das Live-Services-Modul inNetWitness Suite verwenden.

Troubleshooting bei „OutOfMemoryError“ auf Context Hub-Server

In diesem Abschnitt finden Sie Troubleshooting-Anweisungen, wenn ein „OutOfMemoryError“ auf Context Hub-Server auftritt und der Service nicht mehr reagiert.

Wenn TAXII-Feeds konfiguriert sind, gibt Integrität und Zustand Warnmeldungen aus, falls der verfügbare Heap-Speicher des Context Hub-Servers sehr niedrig ist. Wenn der Status des Context Hub-Servers aufgrund von Speichermangel fehlerhaft ist, gehen Sie so vor:

1. Stellen Sie sicher, dass das **Startdatum** des Feeds innerhalb der nächsten 180 Tage liegt.
2. Prüfen Sie, ob ein TAXII-Feed zu viel Speicherplatz in Anspruch nimmt. Ein TAXII-Feed darf maximal 300 MB verbrauchen. Wenn er mehr Speicherplatz belegt, müssen Sie den Wert im Feld **STIX-Daten entfernen, die älter sind als** unter **Erweiterte Optionen** im **Erstellungsassistenten für benutzerdefinierte Feeds** reduzieren, während Sie den TAXII-Feed bearbeiten.

Hinweis: Wenn das Problem weiterhin besteht, müssen Sie Schritt 3 ausführen.

3. Verringern Sie die Anzahl der parallelen Threads, die für die Verarbeitung von STIX verfügbar sind. Gehen Sie dazu so vor:
    a. Navigieren Sie zu **ADMIN** > **Services** > **Context Hub-Service** > **Ansicht** > **Durchsuchen**.
    b. Navigieren Sie im Strukturbereich zu **enrichment/stix/config**.
    c. Legen Sie im Bereich rechts den Feldwert **stix-query-scheduler-pool-size** auf 2 fest. Der Standardwert ist 5. Mit dieser Einstellung legen Sie fest, wie viele Threads zur Verarbeitung von Abfragen für STIX-Daten gleichzeitig zulässig sind.
    d. Legen Sie den Feldwert **taxii-poll-scheduler-pool-size** auf 2 fest. Der Standardwert ist 5. Mit dieser Einstellung legen Sie fest, wie viele Threads für Abfragen von TAXII-Servern gleichzeitig zulässig sind.
    e. Starten Sie den Context Hub-Server neu.

Referenzen

Dieses Thema umfasst eine Sammlung an Referenzen, die die Benutzeroberfläche beschreiben und detailliertere Informationen zur Funktionsweise von Live in der NetWitness Suite enthalten. Diese Themen sind in alphabetischer Reihenfolge aufgeführt.

- Registerkarte „Bereitstellungen“
- Registerkarte „Eingestellte Ressourcen“
- Ansicht „Live-Konfigurieren“
- Ansicht Live-Feeds
- Live-Ressourcenansicht
- Ansicht Live-Suche
- Feedback und Datenfreigabe in NetWitness Suite
- Assistent für die Ressourcenpaketbereitstellung
- RSA Live-Registrierungsportal
- Registerkarte „Abonnements“

Ansicht „Live-Konfigurieren“

In der Ansicht „Live-Konfiguration“ stellt NetWitness Suite integrierte Tools zum Managen von Live-Ressourcen bereit. Sie können Ressourcenabonnements, Servicebereitstellungen und eingestellte Ressourcen verwalten. Die erforderliche Rolle für den Zugriff auf diese Ansicht ist **Live-Ressourcen konfigurieren**. Eine allgemeine Beschreibung zur Verwendung der verschiedenen Ansichten in NetWitness Suite Live finden Sie unter Live-Services-Management.

Um auf diese Ansicht zuzugreifen, navigieren Sie zu **KONFIGURIEREN > Abonnements**. Diese Ansicht umfasst folgende Registerkarten:

- Registerkarte „Bereitstellungen“
- Registerkarte „Abonnements“
- Registerkarte „Eingestellte Ressourcen“

Registerkarte „Bereitstellungen“

Auf der Registerkarte „Bereitstellungen“ in der Ansicht „Live-Konfiguration“ können folgende Aktionen durchgeführt werden:

- Anzeigen von abonnierten Ressourcen, die für die Bereitstellung bei Services in einer Servicegruppe ausgewählt wurden.
- Auswählen von abonnierten Ressourcen, um sie bei Services in einer Servicegruppe bereitzustellen.
- Entfernen von Ressourcen, die für die Bereitstellung bei Services in einer Servicegruppe ausgewählt sind.

Die hier genannten Ressourcen werden nicht unmittelbar nach dem Hinzufügen zu einer Servicegruppe bereitgestellt. Stattdessen werden die abonnierten Ressourcen an die Services übergeben, wenn NetWitness Suite mit RSA NetWitness Suite Live synchronisiert wird. Der Synchronisationsplan wird im Bereich „Live-Konfiguration“ konfiguriert. Wenn Sie nicht auf die geplante Synchronisation warten möchten, können Sie die Synchronisation von NetWitness Suite auch jederzeit im Bereich „Live-Konfiguration“ starten.

Ebenso werden Ressourcen, die aus dem Bereich „Bereitstellungen“ gelöscht wurden, nicht aus dem Service gelöscht, in dem sie bereitgestellt wurden. Sie können Ressourcen aus Services über die Ansicht Live-Ressource löschen.

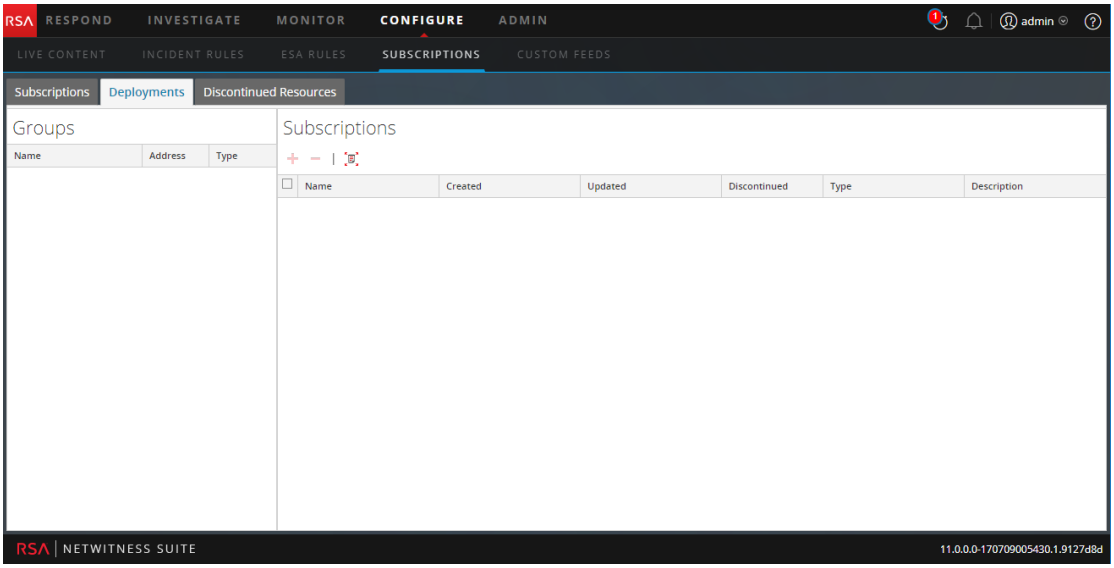
Die erforderliche Berechtigung, um auf diese Ansicht zugreifen zu können, ist **Live-Ressourcen managen**.

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **KONFIGURIEREN > Abonnements**.

   Die Registerkarte **Abonnements** ist standardmäßig geöffnet.

2. Klicken Sie auf die Registerkarte **Bereitstellungen**.



Die Registerkarte „Bereitstellungen“ verfügt über zwei Bereiche: **Gruppen** und **Abonnements**.

Bereich „Gruppen“

Beim Gruppenbereich handelt es sich um eine statische Ansicht der konfigurierten Servicegruppen, die in der Ansicht Administrationsservices erstellt wurden. Wenn Sie im Gruppenbereich eine Gruppe auswählen, wird der Abonnementbereich mit einer Liste der Abonnements befüllt, die zur Bereitstellung bei den Services in der Servicegruppe ausgewählt sind.

Funktion	Beschreibung
Name	Dies ist der Name der Servicegruppe. Wenn Sie auf das Plussymbol klicken, wird eine verschachtelte Liste der Services in dieser Gruppe eingeblendet.
Adresse	Dies ist die IP-Adresse der einzelnen Services in der Gruppe.
Typ	Dies ist der Servicetyp.

Abonnementbereich

In der folgenden Tabelle werden die Komponenten im Bereich „Abonnements“ beschrieben.

Funktion	Beschreibung
	Klicken Sie auf , um ein Dialogfeld mit den Abonnements zu öffnen, die in der Ansicht „Live-Suche“ oder in der Ansicht „Live-Ressource“ hinzugefügt wurden und die für die Bereitstellung verfügbar sind.
	Klicken Sie auf  , um die ausgewählten Abonnements aus der Bereitstellungsliste für Servicegruppen zu löschen.
	Klicken Sie auf  , um Ihre Ressourcen mit der aktuellsten Version, die bei Live verfügbar ist, zu synchronisieren.
Name	Dies ist der Name der Ressource.
Erstellt	Dies ist das Datum und die Uhrzeit der Ressourcenerstellung.
Updated	Dies ist das Datum und die Uhrzeit der letzten Ressourcenaktualisierung.
Typ	Dies ist der Typ der Ressource.
Beschreibung	Dies ist die Beschreibung der Ressource.

Registerkarte „Abonnements“

Abonnements sind Live-Ressourcen in NetWitness Suite, die Sie in der Ansicht „Live-Suche“ oder „Live-Ressource“ abonniert haben. Wenn Sie eine Ressource abonnieren, geben Sie an, dass Sie regelmäßig Aktualisierungen von RSA NetWitness Suite Live erhalten möchten. Die im Bereich Live-Konfiguration gewählten Optionen legen fest, wie oft die Synchronisation durchgeführt wird und ob Sie per E-Mail über Updates benachrichtigt werden. Außerdem können Sie, wenn Sie nicht auf das nächste Update warten möchten, eine sofortige Synchronisation erzwingen.

Auf der Registerkarte „Abonnements“ können Sie Abonnements managen. Jede Ressource, die in NetWitness Suite abonniert ist, wird auf dieser Registerkarte aufgelistet.

Auf der Registerkarte „Abonnements“ können Sie:

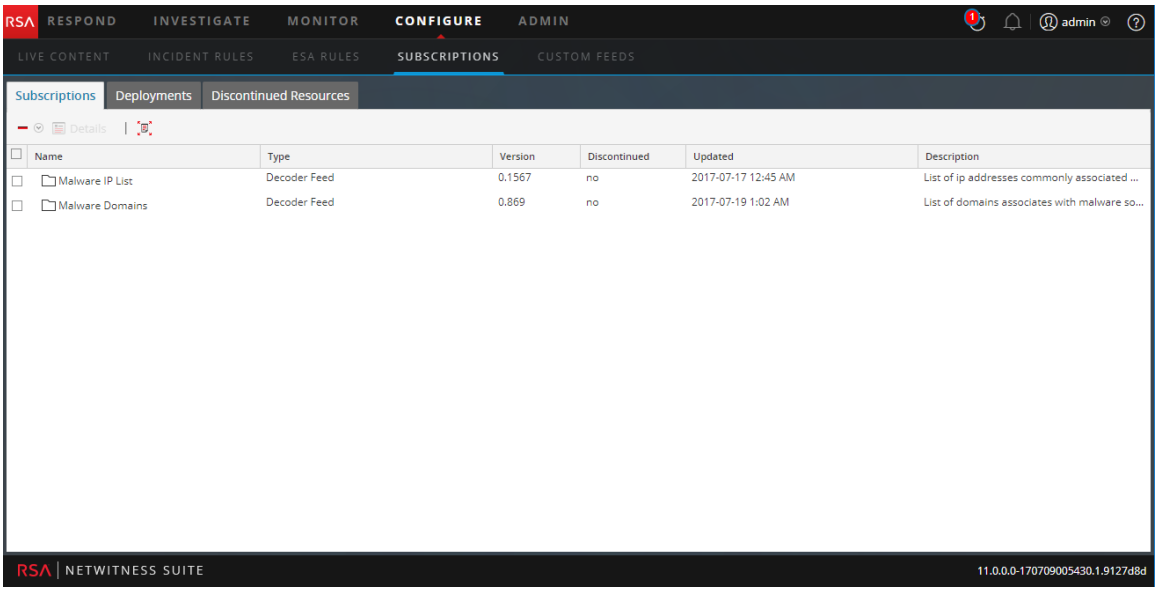
- Alle Ressourcen anzeigen, die in dieser Instanz von NetWitness Suite abonniert sind
- Eine detaillierte Ansicht eines Abonnements in der Live-Ansicht Ressource anzeigen
- Löschen eines Abonnements

Hinweis: Wenn Sie eine Ressource abonnieren, wird sie dadurch noch nicht auf einem Service bereitgestellt. Wenn Sie eine oder mehrere abonnierte Ressourcen bereitstellen möchten, wechseln Sie zur Registerkarte „Bereitstellungen“. Wenn Sie eine einzige Ressource manuell bereitstellen möchten, wählen Sie die Option „Bereitstellen“ in der Ansicht „Ressource“.

Die erforderliche Berechtigung, um auf diese Ansicht zugreifen zu können, ist **Live-Ressourcen managen**.

Um auf diese Ansicht zuzugreifen, wählen Sie in Hauptmenü **KONFIGURIEREN > Abonnements** aus.

Die Registerkarte „Abonnements“ ist standardmäßig geöffnet.



Die Registerkarte **Abonnements** verfügt über eine Symbolleiste und ein Raster.

Symbolleiste

In dieser Tabelle werden die in der Symbolleiste verfügbaren Optionen beschrieben.

Funktion	Beschreibung
	Löscht die ausgewählten Abonnements.
	Zeigt die Details einer abonnierten Ressource in der Ansicht „Ressource“ an.
	Überprüft den Live-Server auf neu eingestellte Ressourcen.

Raster

Spalte	Beschreibung
	Wählt die abonnierten Ressourcen aus, damit sie detailliert angezeigt oder gelöscht werden können. Sie können Details für eine einzige Ressource anzeigen. Sie können eine oder mehrere Ressourcen aus den abonnierten Ressourcen löschen, wodurch das Abonnement beendet wird.
Name	Dies ist der Name der abonnierten Ressource.
Typ	Dies ist der Typ der abonnierten Ressource.

Spalte	Beschreibung
Version	Dies ist die Version der abonnierten Ressource.
Eingestellt	Gibt den Status der eingestellten Ressourcen für die abonnierte Ressource an. **Ja** – Ressource ist eingestellt. **Nein** – Ressource ist nicht eingestellt. **--** – Der Live-Server ist nicht für die eingestellten Ressourcen aktiviert.
Updated	Dies sind das Datum und die Uhrzeit, zu der die abonnierte Ressource zuletzt aktualisiert wurde.
Beschreibung	Dies ist eine Beschreibung der abonnierten Ressource.

Registerkarte „Eingestellte Ressourcen“

In diesem Thema werden die Funktionen der **Ansicht „Live-Konfiguration“ > Registerkarte „Eingestellte Ressourcen“** beschrieben.

Auf der Registerkarte „Eingestellte Ressourcen“ in der Ansicht „Live-Konfiguration“ können folgende Aktionen durchgeführt werden:

- Scannen der Services für die eingestellten Ressourcen.
- Entfernen der eingestellten Ressourcen von jedem Service oder jeder Servicegruppe.

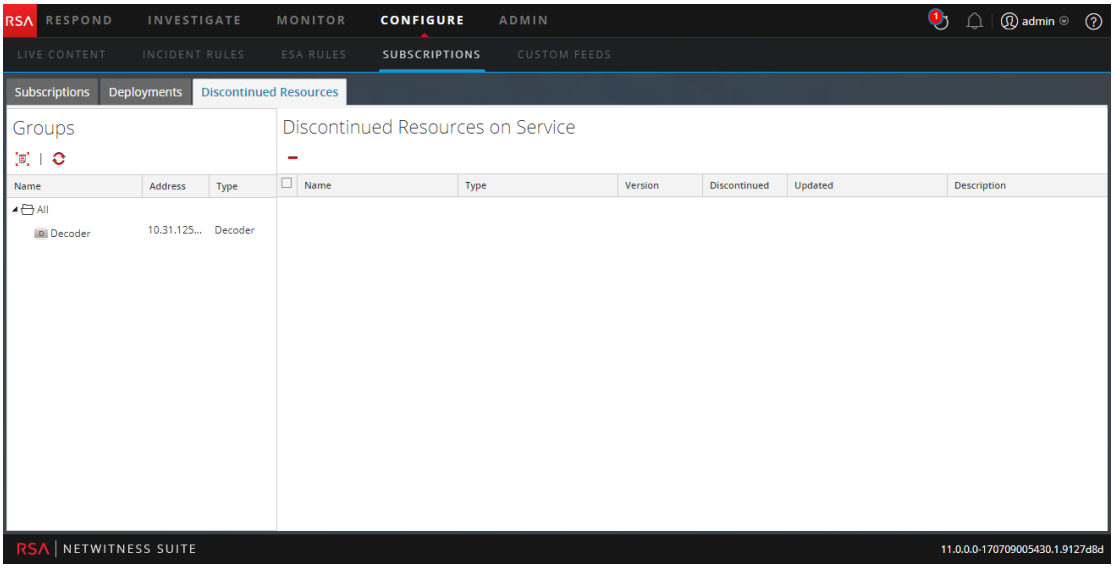
Die erforderliche Berechtigung, um auf diese Ansicht zugreifen zu können, ist **Live-Ressourcen managen**.

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **KONFIGURIEREN > Abonnements**.

   Die Registerkarte **Abonnements** ist standardmäßig geöffnet.
2. Klicken Sie auf die Registerkarte **Eingestellte Ressourcen**.

Dies ist ein Beispiel für die Registerkarte „Eingestellte Ressourcen“.



Die Registerkarte „Eingestellte Ressourcen“ umfasst zwei Bereiche: „Gruppen“ und „Service mit eingestellten Ressourcen“

Bereich „Gruppen“

Beim Gruppenbereich handelt es sich um eine statische Ansicht der konfigurierten Servicegruppen, die in der Ansicht „Admin-Services“ erstellt wurden. Durch Auswählen einer Gruppe im Bereich „Gruppen“ wird der Bereich „Eingestellte Ressourcen“ mit einer Liste eingestellter Ressourcen gefüllt, die die Bereitstellung für den ausgewählten Service oder die Servicegruppe darstellen.

Funktion	Beschreibung
	Klicken Sie auf  , um die Services nach einer eingestellten Ressource zu scannen.
	Zeigt den aktuellen Status der eingestellten Ressourcen für einen Service an. **Hinweis:** Der Status des Services kann sich ändern, während die Services gescannt werden.
Name	Dies ist der Name der Servicegruppe. Wenn Sie auf das Plussymbol klicken, wird eine verschachtelte Liste der Services in dieser Gruppe eingeblendet.
Adresse	Dies ist die IP-Adresse der einzelnen Services in der Gruppe.
Typ	Dies ist der Servicetyp.

Bereich „Service mit eingestellten Ressourcen“

In der folgenden Tabelle sind die Funktionen im Bereich „Service mit eingestellten Ressourcen“ beschrieben.

Funktion	Beschreibung
	Klicken Sie auf , um die ausgewählten Ressourcen aus dem Service oder der Servicegruppe zu löschen.
Name	Dies ist der Name der Ressource.
Typ	Dies ist der Typ der Ressource.
Version	Version der eingestellten Ressource.
Eingestellt	Gibt den Status der eingestellten Ressourcen für die abonnierte Ressource an. **Ja** – Ressource ist eingestellt. **Nein** – Ressource ist nicht eingestellt. **--** – Der Live-Server ist nicht für die eingestellten Ressourcen aktiviert.
Updated	Dies ist das Datum und die Uhrzeit der letzten Ressourcenaktualisierung.
Beschreibung	Dies ist die Beschreibung der Ressource.

Ansicht Live-Feeds

In der Ansicht Live-Feeds können Sie Folgendes erledigen:

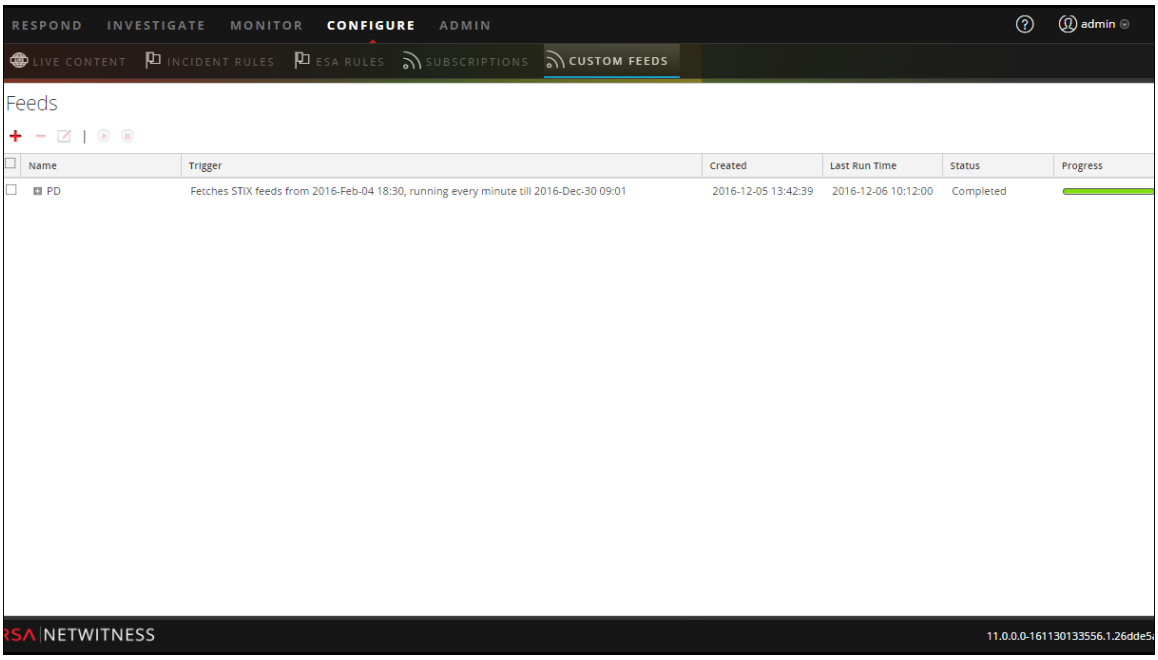
- Benutzerdefinierte Feeds erstellen
- Identitätsfeeds erstellen
- Feeds bearbeiten

Die erforderliche Rolle für den Zugriff auf diese Ansicht ist **Geräte managen**.

Um auf diese Ansicht zuzugreifen, führen Sie einen der folgenden Schritte aus:

- Wählen Sie in Hauptmenü die Option **Live > Feeds** aus.
- Wählen Sie in einer beliebigen Ansicht im Live-Modul die Option **Feeds** in Hauptmenü aus.

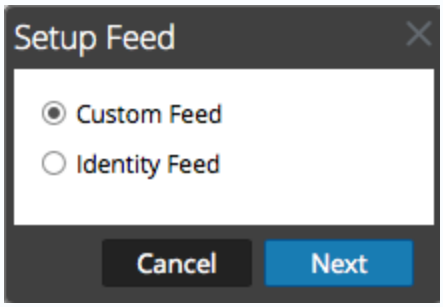
Dies ist ein Beispiel für die Ansicht Feeds.



Die Registerkarte **Feeds** besteht aus einer Symbolleiste und einem Raster.

Symbolleiste

In dieser Tabelle werden die Optionen in der Symbolleiste beschrieben.

Funktion	Beschreibung
+	Initiiert die Erstellung eines benutzerdefinierten Feeds oder Identitätsfeeds, indem das Dialogfeld **Feed einrichten** angezeigt wird.  • Mit der Option „Benutzerdefinierter Feed“ wird der Assistent **Benutzerdefinierten Feed konfigurieren** geöffnet. • Mit der Option „Identitätsfeed“ wird der Assistent **Identitätsfeeds konfigurieren** geöffnet.
−	Löscht den ausgewählten Feed.

Funktion	Beschreibung
	Öffnet für den ausgewählten Feed den Assistenten „Benutzerdefinierten Feed konfigurieren“ oder „Identitätsfeed konfigurieren“ (weitere Informationen hierzu finden Sie unter Bearbeiten eines Feeds).
	Hiermit wird der Datenfeed gestartet oder fortgesetzt.
	Hiermit wird der Datenfeed beendet oder angehalten.

Feedraster

In der folgenden Tabelle sind die Spalten im Raster beschrieben.

Spalte	Beschreibung
	Wählt einen Feed aus.
Name	Gibt den Namen des Feeds an. **Hinweis:** Sie können jetzt Sonderzeichen verwenden, um den Namen des benutzerdefinierten Feeds zu definieren.
Auslöser	Zeigt an, wie oft der Feed ausgeführt wird. Dies wird bestimmt durch den bei der Feederstellung definierten **Typ der Feedaufgabe**.
Erstellt	Gibt das Datum und die Uhrzeit der Feederstellung an.
Festplattenauslastung	Zeigt die Größe des MongoDB-Speichers an, der vom TAXII-Feed verwendet wird.
Letzte Ausführungszeit	Datum und Uhrzeit der letzten Ausführung des Feeds
Status	Der Status des Feeds
Progress	Fortschrittsleiste

Live-Ressourcenansicht

Die Ansicht Live-Ressource zeigt eine detaillierte Ansicht einer ausgewählten Ressource und bietet folgende Optionen:

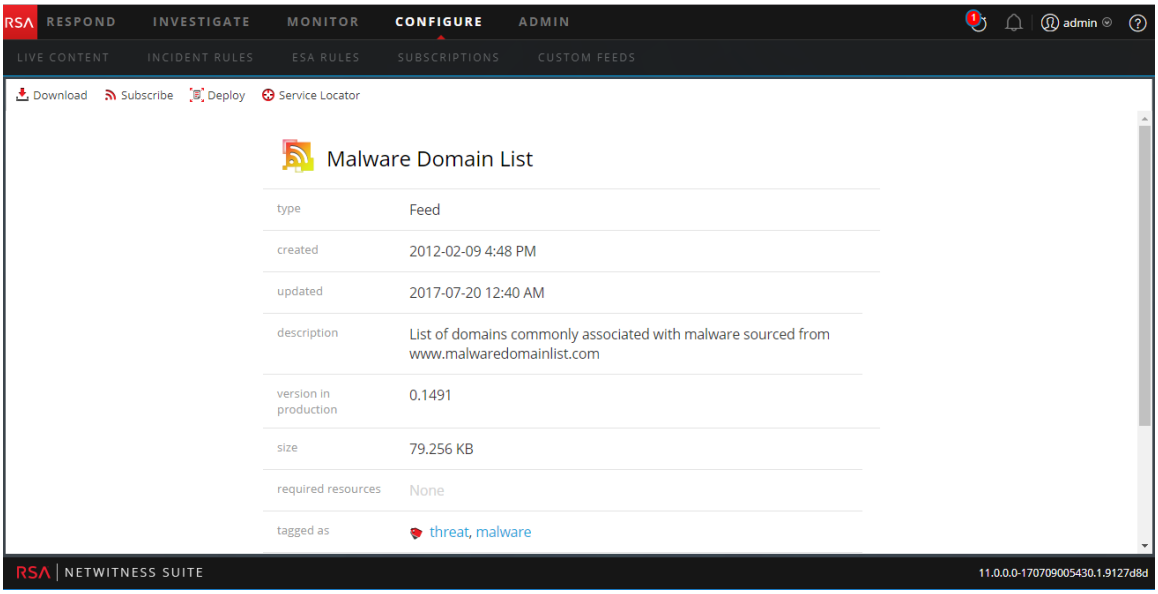
- Herunterladen der Ressource
- Abonnieren oder deabonnieren der Ressource
- Bereitstellen der Ressource für Services
- Suchen von Services, für die die Ressource bereitgestellt wurde, und Entfernen der Ressource aus Services

Für den Zugriff auf diese Ansicht ist die Berechtigung Live-Ressourcendetails anzeigen erforderlich.

Um auf diese Ansicht zuzugreifen, führen Sie einen der folgenden Schritte aus:

1. Wählen Sie in Hauptmenü die Option **KONFIGURIEREN > LIVE-INHALTE > Suchkriterien** aus.
2. Klicken Sie in der Ansicht „Live-Suche“ unter **Detaillierte Ergebnisse** auf das Symbol für den Ressourcentyp oder auf den Ressourcennamen.
3. Doppelklicken Sie in der Ansicht „Live-Suche“ unter **Rasteransicht der Ergebnisse** auf eine Ressource oder wählen Sie eine Ressource aus und klicken Sie auf **Details**.

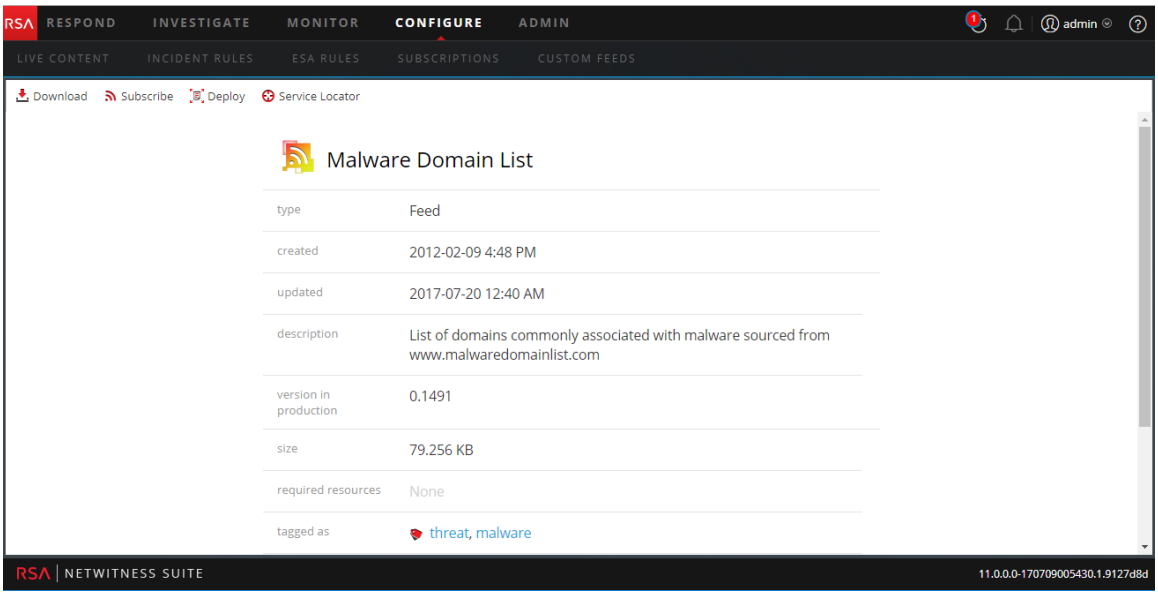
Dies ist ein Beispiel für die Ansicht Ressourcen.



Die Ansicht Live-Ressource bietet eine detaillierte Ansicht einer einzigen Ressource und eine Symbolleiste.

Ressourcendetails

Dies ist ein Beispiel für die Ressourcendetails, die in der Ansicht „Ressourcen“ angezeigt werden.



In der folgenden Tabelle sind die Felder im Abschnitt „Ressourcendetails“ beschrieben.

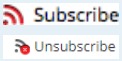
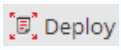
Funktion	Beschreibung
Ressourcentyp-Symbol	Eine grafische Darstellung des Ressourcentyps, zum Beispiel  .
Name	Der Ressourcenname, zum Beispiel **fingerprint_office_lua**.
Typ	Der Ressourcentyp, zum Beispiel **RSA Lua Parser**.
Erstellt	Das Erstellungsdatum der Ressource, zum Beispiel **2013-09-15 02:16 PM**.
Updated	Datum der letzten Aktualisierung der Ressource, zum Beispiel **2013-09-15 02:16 PM**.
Beschreibung	Die Beschreibung der Ressource, zum Beispiel: **Identifiziert Dokumente für Microsoft Office 95, 2007 Word, Excel und PowerPoint**.
Version in Produktion	Die Version der Ressource, beispielsweise **0.1**.
Größe	Die Größe der Ressource, zum Beispiel **9.079 KB**.

Funktion	Beschreibung
Erforderliche Ressourcen	Eine Liste der Ressourcen, von denen diese Ressource abhängig ist, zum Beispiel **NetWitness Lua Library**. Wenn Sie auf eine Ressource klicken, werden die aktuell angezeigten Details durch die Details derjenigen Ressource ersetzt, auf die Sie geklickt haben.
Markiert als	Die Tags für diese Ressource. In diesem Beispiel gelten die Tags **featured, informational**. Wenn Sie auf einen Tag klicken, wird die Ansicht Live-Suche geöffnet. Die Suche ist dabei auf die Ressourcen mit diesem Tag eingeschränkt.
Erforderliche Metaschlüssel	Die Metaschlüssel für diese Ressource. In diesem Beispiel gibt es keine erforderlichen Metaschlüssel. Wenn Sie auf einen Metaschlüssel klicken, wird die Ansicht Live-Suche geöffnet. Die Suche ist dabei auf die Ressourcen mit diesem Metaschlüssel beschränkt.
Erzeugt Metawerte	Die von der Ressource erzeugten Metawerte . In diesem Beispiel liegen keine erzeugten Metawerte vor. Wenn Sie auf einen Metawert klicken, wird die Ansicht „Live-Suche“ geöffnet. Die Suche ist dabei auf die Ressourcen mit diesem Metawert beschränkt.
Berechtigungen	Die für die Ressource erforderlichen Berechtigungen.

Symbolleiste Ansicht Ressource

In dieser Tabelle sind die Optionen der Ansicht „Live-Ressource“ beschrieben.

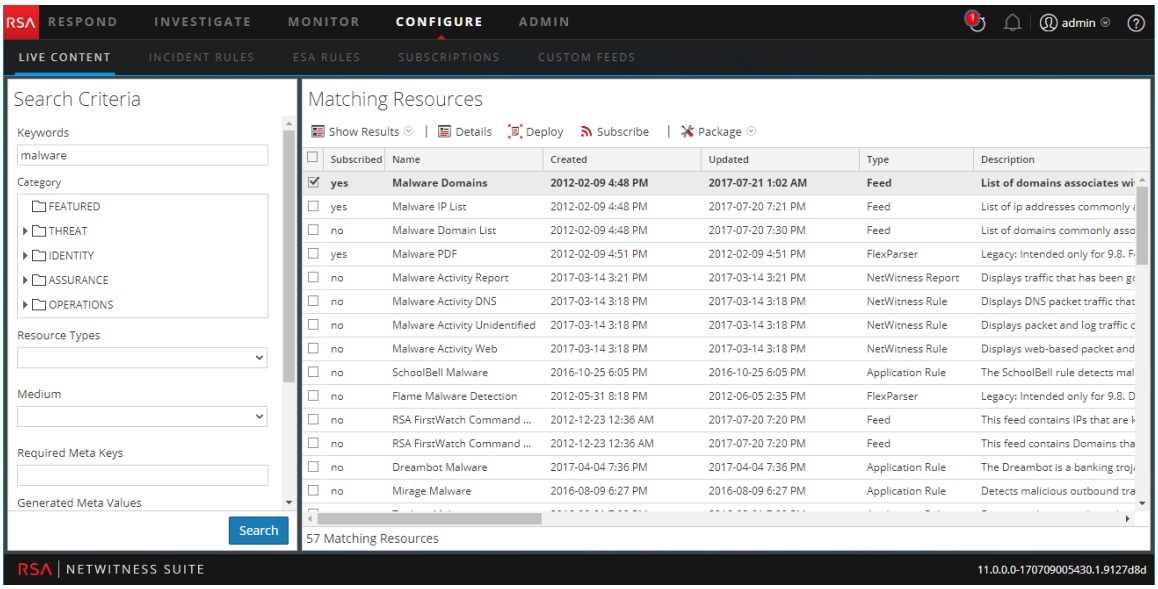
Funktion	Symbol	Beschreibung
Download	Download	Diese Option lädt die Ressource herunter, die aktuell in der Ansicht Ressource angezeigt wird.

Funktion	Symbol	Beschreibung
Abonnieren oder Abonnement beenden		Diese Option abonniert oder deabonniert die Ressource, die aktuell in der Ansicht Ressource angezeigt wird. • Wenn Sie auf **Abonnieren** klicken, wird ein Benachrichtigungs-Dialogfeld geöffnet, in dem Sie dem Erhalt von Benachrichtigungen bei der Aktualisierung der ausgewählten Ressourcen zustimmen. Sie können den Vorgang abbrechen oder auf **OK** klicken. • Wenn Sie auf **Abonnement beenden** klicken, müssen Sie bestätigen, dass Sie keine Benachrichtigungen mehr erhalten möchten, wenn die ausgewählten Ressourcen aktualisiert werden. Sie können dann wahlweise den Vorgang abbrechen oder auf **Abonnement beenden** bzw. **Abonnement beenden und entfernen** klicken, wodurch die Ressource auch aus den Services entfernt wird, für die sie bereitgestellt wird.
Bereitstellen		Diese Option bietet einen Weg, die Ressource bereitzustellen, die aktuell in der Ansicht Ressource angezeigt wird. Wenn Sie auf **Bereitstellen** klicken, wird das Dialogfeld „Manuelle Ressourcenbereitstellung“ geöffnet.
Servicesuche		Diese Option zeigt eine Liste von Services an, für die die derzeit angezeigte Ressource bereitgestellt wird. Sie können die Ressource aus allen oder aus ausgewählten Services entfernen.

Ansicht Live-Suche

Die Ansicht Live-Suche bietet die Möglichkeit, die konfigurierten Live-CMS nach Ressourcen zu durchsuchen. Wenn entsprechende Ressourcen gefunden werden, können Sie Details anzeigen, Ressourcen abonnieren und Ressourcen für Services und Servicegruppen bereitstellen.

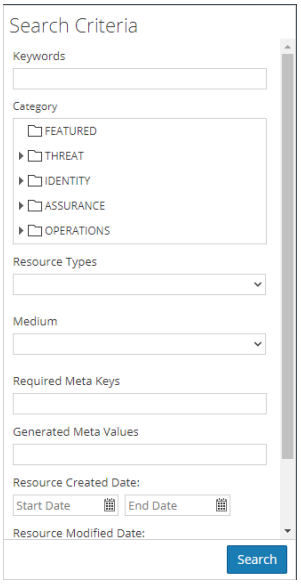
Dies ist ein Beispiel für die Suchansicht.



Die Ansicht Live-Suche hat einen Bereich, in dem Sie Suchkriterien angeben können, und einen Bereich, in dem übereinstimmende Ressourcen angezeigt werden. Der Bereich „Suchkriterien“ kann ausgeblendet werden, damit für die Ansicht des Bereichs „Übereinstimmende Ressourcen“ mehr Platz zur Verfügung steht.

Bereich „Suchkriterien“

Dies ist ein Beispiel für den Bereich „Suchkriterien“.



In der folgenden Tabelle werden die Funktionen des Bereichs „Suchkriterien“ aufgeführt.

Funktion	Beschreibung
Schlüsselwort (Schlüsselwörter)	Geben Sie ein oder mehrere Schlüsselwörter ein, um nach Ressourcen zu suchen, bei denen das Schlüsselwort im Namen oder in der Ressourcenbeschreibung vorkommt. Sie können Platzhalter verwenden, wenn Sie ein Schlüsselwort eingeben.
Kategorie	Die Kategorien spiegeln das hierarchische Ermittlungsmodell wider, das RSA für die Organisation von Ressourcen verwendet. Der Zweck des Ermittlungsmodells besteht darin, einen genauen Pfad zur Reaktion auf Informationssicherheitsvorfälle bereitzustellen. Weitere Informationen finden Sie im Thema Ermittlungsmodell.
Ressourcentypen	Wählen Sie Ressourcentypen aus der Drop-down-Liste aus, um Ressourcen nach Ressourcentyp zu filtern. Die möglichen Werte sind: • Erweiterte Analyse (Warehouse) • Anwendungsregel • Bundle • Korrelationsregel • Event Stream Analysis-Regel • Feed • FlexParser • Log Collector • Protokollgerät • Lua-Parser • Malwareregeln • NetWitness-Liste • NetWitness-Bericht • NetWitness-Regel

Funktion	Beschreibung
Mittel	Wählen Sie ein oder mehrere Medien aus der Drop-down-Liste aus, um nach Inhalten basierend auf der Metadatenquelle zu suchen. Verfügbare Werte für Medium sind: • **log**: auf Inhalte angewendet, die aus Protokolldaten abgeleitete Metadaten verwenden • **packet**: auf Inhalte angewendet, die aus Netzwerkpaketen abgeleitete Metadaten verwenden • **log and packet**: auf Inhalte angewendet, die aus Protokoll-und Paketdaten abgeleitete Metadaten korrelieren
Tags	Wählen Sie Metatags aus der Drop-down-Liste zum Durchsuchen aus, basierend darauf, wie die Metadaten getaggt sind. Wenn Sie z. B. nach Ressourcen für einen Log Decoder suchen, wählen Sie das Tag **netwitness für Protokolle** aus. Alternativ können Sie einen Tag im Bereich Übereinstimmende Ressourcen anklicken, um diesen Tag in dieses Feld einzufügen.
Erforderliche(r) Metaschlüssel	Geben Sie einen bestimmte Metaschlüssel ein; z. B. **threat.source**. Alternativ können Sie einen Metaschlüssel im Bereich Übereinstimmende Ressourcen anklicken, um diesen Tag in dieses Feld einzufügen.
Erzeugte(r) Metawert(e)	Geben Sie einen erzeugten Metawert ein, z. B. **netwitness**. Alternativ können Sie einen erzeugten Metaschlüssel im Bereich Übereinstimmende Ressourcen anklicken, um diesen Tag in dieses Feld einzufügen.
Nach Erstellungsdatum suchen	Geben Sie einen Datumsbereich an, in dem die Ressourcen erstellt wurden. Um zum Beispiel nach Ressourcen zu suchen, die zwischen dem 1. und dem 4. Januar erstellt wurden, wählen Sie den 1. Januar als Startdatum und den 4. Januar als Enddatum. Sie müssen Datumsangaben im Format MM/TT/JJJJ eingeben oder auf  klicken und das Datum aus einem Kalender auswählen.

Funktion	Beschreibung
Nach Änderungsdatum suchen	Geben Sie einen Datumsbereich an, in dem die Ressourcen geändert wurden. Um zum Beispiel nach Ressourcen zu suchen, die zwischen dem 1. und dem 4. Januar geändert wurden, wählen Sie den 1. Januar als Startdatum und den 4. Januar als Enddatum. Sie müssen Datumsangaben im Format MM/TT/JJJJ eingeben oder auf klicken und das Datum aus einem Kalender auswählen.
Suchen	Klicken Sie auf **Suchen**, um die Suchanfrage an den Live-Server zu senden. Je spezifischer die Suchkriterien sind, desto schneller werden übereinstimmende Ressourcen zurückgegeben.
Abbrechen	Klicken Sie auf **Abbrechen**, um die laufende Suche abzubrechen.
Eingestellte Ressourcen einschließen	Aktivieren Sie **Eingestellte Ressourcen einschließen**, um die eingestellten Ressourcen in die Suchergebnisse einzuschließen. Eine aktuelle Liste der Ressourcen, die eingestellt wurden, finden Sie im Thema Eingestellter Content.

Bereich „Übereinstimmende Ressourcen“

Der Bereich „Übereinstimmende Ressourcen“ präsentiert Suchergebnisse basierend auf der Auswahl, die im Bereich „Suchkriterien“ vorgenommen wurde. Die Ergebnisse werden anfänglich in einem Raster angezeigt, aber Sie können zwischen zwei Optionen der Ergebnisanzeige wechseln: Detailliert oder Raster.

Detaillierte Ergebnisse

In den detaillierten Ergebnissen können Sie auf ein Tag, einen Metaschlüssel oder einen Ressourcenmetawert klicken, um den Bereich „Suchkriterien“ automatisch auszufüllen und ein Pivot in den Suchergebnissen auszuführen.

In der folgenden Tabelle werden die Elemente der detaillierten Ergebnisse beschrieben.

Funktion	Beschreibung
Ressourcentyp-Symbol	Eine grafische Repräsentation des Ressourcentyps. Beispiel:

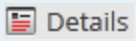
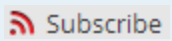
Funktion	Beschreibung
Name	Der Name der Ressource, z. B. **Gruppenmanagement**. **Hinweis:** (Eingestellt) wird neben dem Ressourcennamen angezeigt, wenn eine Ressource eingestellt ist.
Typ	Der Typ der Ressource, z. B. **Regel**.
Updated	Das Datum, an dem die Ressource zuletzt aktualisiert wurde, zum Beispiel **2015-09-15 4:27 PM**.
Version	Die Version der Ressource, beispielsweise **0.1**.
Größe	Die Größe der Ressource, zum Beispiel **153 B**.
Subscribed	Abonnementstatus: • **yes**: Diese NetWitness Suite-Instanz hat diese Contentressource abonniert. • **no**: Diese NetWitness Suite-Instanz hat diese Contentressource nicht abonniert.
Beschreibung	Die Beschreibung der Ressource, z. B. **Complianceregel-Gruppenmanagement**.
Tags	Die Tags für diese Ressource. Wenn Sie auf ein Tag klicken, wird die Suche auf Ressourcen mit diesem Tag beschränkt. Beispiel:  .
Metaschlüssel	Die Metaschlüssel für diese Ressource. Wenn Sie auf einen Metaschlüssel klicken, wird die Suche auf Ressourcen mit diesem Metaschlüssel beschränkt. Beispiel:  .
Ressourcenmetawerte	Die von der Ressource erzeugten Metawerte. Wenn Sie auf einen Metawert klicken, wird die Suche auf Ressourcen beschränkt, die den Metawert erzeugt haben. Beispiel:  .

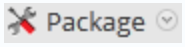
Rasteransicht der Ergebnisse

In der Rasteransicht können Sie eine oder mehrere Ressourcen auswählen und mithilfe zusätzlicher Optionen in der Symbolleiste die Details einer einzelnen Ressource anzeigen, Ressourcen abonnieren und bereitstellen.

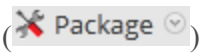
In der folgenden Tabelle werden die Elemente im Ergebnisraster beschrieben.

Funktion	Beschreibung
Abonniert	Abonnementstatus: • **yes**: Diese NetWitness Suite-Instanz hat diese Contentressource abonniert. • **no**: Diese NetWitness Suite-Instanz hat diese Contentressource nicht abonniert.
Name	Der Name der Ressource, z. B. **Gruppenmanagement**. **Hinweis:** Der Ressourcenname wird rot angezeigt, wenn die Ressource eingestellt ist.
Erstellt	Das Erstellungsdatum der Ressource, zum Beispiel **2015-08-12 3:11 PM**.
Updated	Das Datum, an dem die Ressource zuletzt aktualisiert wurde, zum Beispiel **2015-09-15 4:27 PM**.
Typ	Der Typ der Ressource, z. B. **Regel**.
Eingestellt	Der Status der eingestellten Ressourcen: **yes**: Die den Suchkriterien entsprechende Ressource ist eingestellt. **no**: Die Ressource ist nicht eingestellt. **--**: Der Live-Server ist nicht für die eingestellten Ressourcen aktiviert.
Beschreibung	Die Beschreibung der Ressource, z. B. **Complianceregel-Gruppenmanagement**.
Symbolleiste	

Funktion	Beschreibung
	Dieses Menü bietet zwei Möglichkeiten, die Suchergebnisse anzuzeigen: **Detailliert** und **Raster**.
	Diese Option ist auf eine einzige ausgewählte Ressource anwendbar. Wenn Sie auf **Details** klicken, wird die ausgewählte Ressource in der Ansicht „Live-Ressource“ geöffnet.
	Diese Option ist auf eine oder mehrere ausgewählte Ressourcen anwendbar.
	Diese Option ist auf eine oder mehrere ausgewählte Ressourcen anwendbar. Wenn Sie auf **Abonnieren** klicken, wird ein Dialogfeld geöffnet, in dem Sie bestätigen müssen, dass Sie benachrichtigt werden möchten, wenn die ausgewählten Ressourcen aktualisiert werden.

	Dieses Menü bietet zwei Paketfunktionen für die ausgewählten Ressourcen:
	• **Erstellen**: Erstellt eine **resourceBundle.zip**-Datei mit allen ausgewählten Ressourcen und öffnet ein Dialogfeld, in dem Sie folgende Aktionen ausführen können:
	  • Öffnen der Datei, oder
	  • Speichern der Datei für nachfolgende Bereitstellung.
	• **Bereitstellen**: Öffnet den Bereitstellungsassistenten, in dem Sie eine Datei namens **resourceBundle.zip** auswählen und bereitstellen können.

Siehe auch

- Einzelheiten zur Bereitstellung () finden Sie unter Suchen und Bereitstellen von Live-Ressourcen.
- Weitere Informationen zum Bereitstellen eines Pakets () finden Sie unter Assistent für die Ressourcenpaketbereitstellung.

Assistent für die Ressourcenpaketbereitstellung

Wenn Sie ein Ressourcenpaket erstellt und auf einem Netzlaufwerk gespeichert haben, können Sie den Assistenten für die Ressourcenpaketbereitstellung verwenden, um die Ressourcen manuell für einen Service oder eine Servicegruppe bereitzustellen, ohne die Ressourcen zu abonnieren. NetWitness Suite akzeptiert Pakete in **.nwp**-Dateien oder **.zip**-Dateien.

Durch die manuelle Bereitstellung von Ressourcen werden diese den Services direkt bereitgestellt, ohne die leistungsstarken Ressourcenmanagement-Funktionen von NetWitness Suite zu nutzen.

Wenn Sie zu aktualisierten Ressourcen Benachrichtigungen oder Aktualisierungen erhalten und Ressourcen einfach aus einem Service löschen möchten, müssen Sie Ressourcen in der Ansicht „Live-Suche“ abonnieren und dann in der Ansicht **Live konfigurieren** bereitstellen.

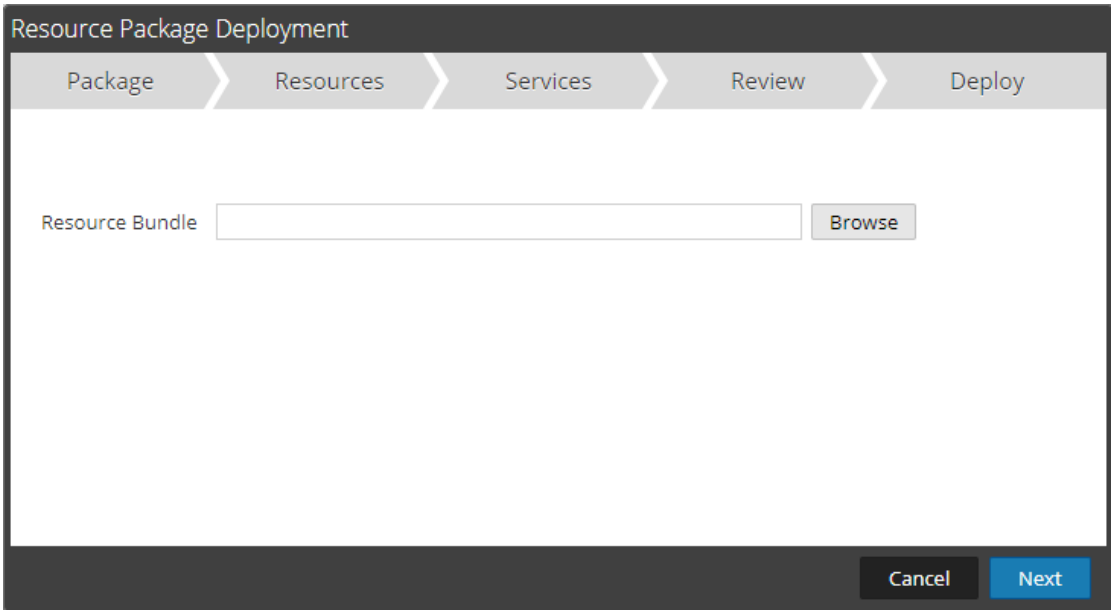
Hinweis: Verwenden Sie NetWitness Suite Live, um Ressourcenbündel zu erstellen. Dies ist eine andere Anwendung, die nicht Bestandteil von NetWitness Suite ist. Wenn Sie in der Symbolleiste **Live-Suche – Übereinstimmende Ressourcen** die Option **Paket** > **Erstellen** auswählen, wird das Fenster „Inhaltspakettool“ angezeigt. Sie können Ressourcen auswählen, die in einem Paket enthalten sein sollen, und das Paket als NetWitness Suite-Paketdatei speichern.

Die erforderliche Berechtigung für den Zugriff auf diese Ansicht ist **Live-Ressourcen bereitstellen**.

So greifen Sie auf diese Ansicht zu:

1. Wählen Sie in Hauptmenü die Option **KONFIGURIEREN > LIVE-INHALT** aus.
2. Wählen Sie in der Symbolleiste **Live-Suche - Übereinstimmende Ressourcen** die Optionen **Paket > Bereitstellen** aus.

Der Assistent für die Ressourcenpaketbereitstellung wird angezeigt.



Funktionen

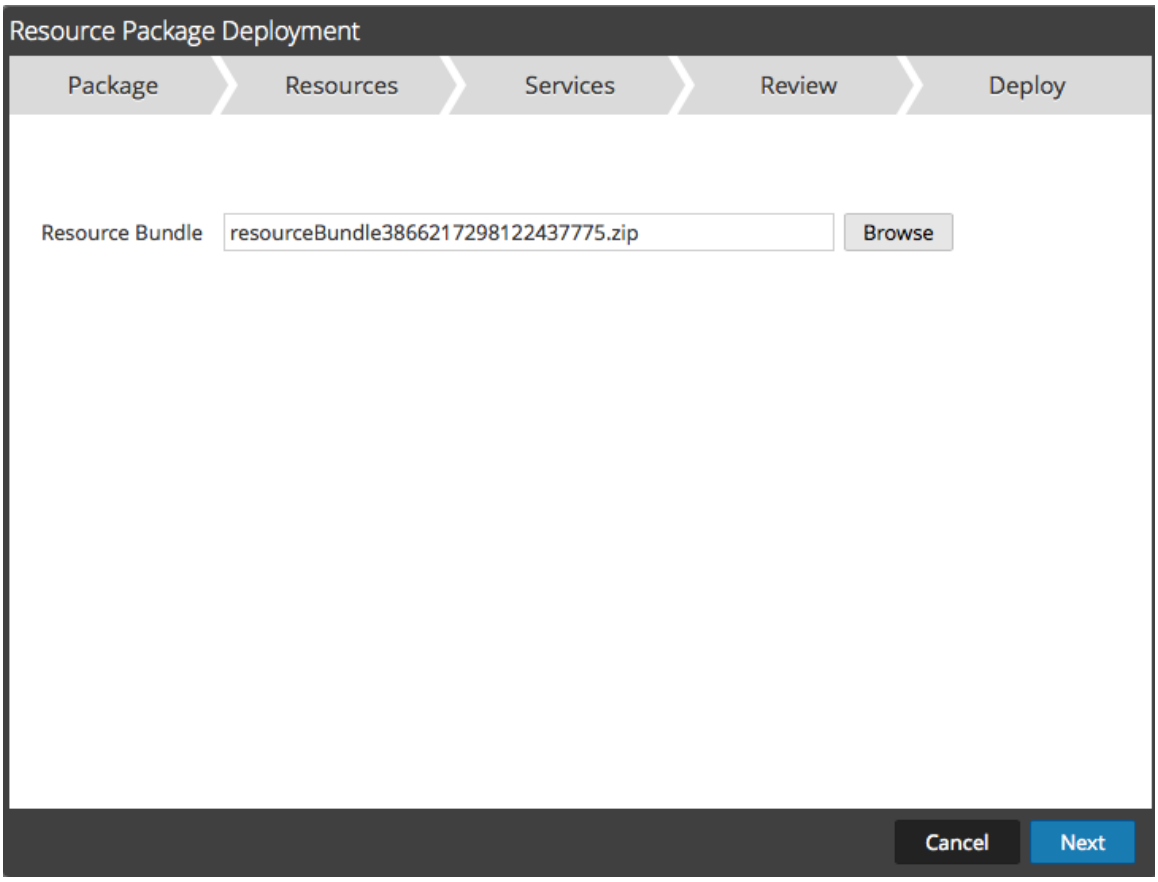
Der „Bereitstellungsassistent“ hat fünf Registerkarten: **Paket**, **Ressourcen**, **Services**, **Überprüfen** und **Bereitstellen**.
Verwenden Sie **Schließen**, um zu beenden, bevor Sie den Assistenten abschließen.

Wenn Sie den Assistenten abschließen, kehrt NetWitness Suite zur Ansicht „Live-Ressourcen“ zurück.

Registerkarte Paket

Verwenden Sie diese Registerkarte, um auf dieser Seite ein Ressourcenbündel im Netzwerk auswählen.

Dies ist ein Beispiel für die Registerkarte „Paket“ mit einem ausgewählten Ressourcenbündel.



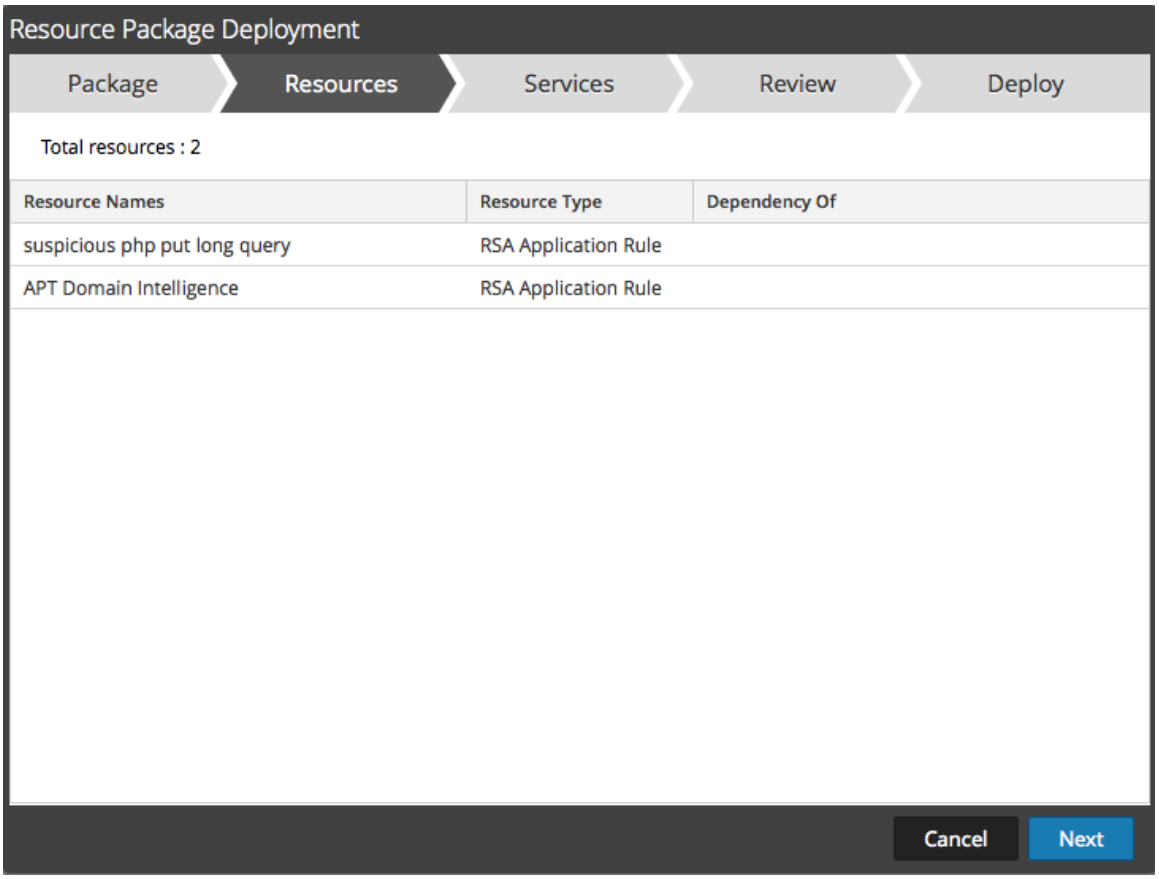
In der folgenden Tabelle werden die Elemente auf der Registerkarte „Paket“ beschrieben.

Spalte	Beschreibung
Ressourcenbündel	Das Eingabefeld zur Angabe eines Ressourcenbündels. Sie können einen Pfad in dieses Feld eingeben oder mithilfe der Schaltfläche Browse suchen.
Befehlsschaltflächen	
Browse	Diese Schaltfläche öffnet ein Dialogfeld Datei hochladen, in dem Sie das lokale Dateisystem durchsuchen und ein Bündel auswählen können.
Abbrechen	Bricht die Bereitstellung ab und schließt den Assistenten
Weiter	Zeigt die nächste Registerkarte des Assistenten an.

Registerkarte Ressourcen

Auf dieser Registerkarte sind die im Bündel enthaltenen Ressourcen aufgelistet.

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Ressourcen.



In der folgenden Tabelle sind die Elemente der Registerkarte „Ressourcen“ beschrieben.

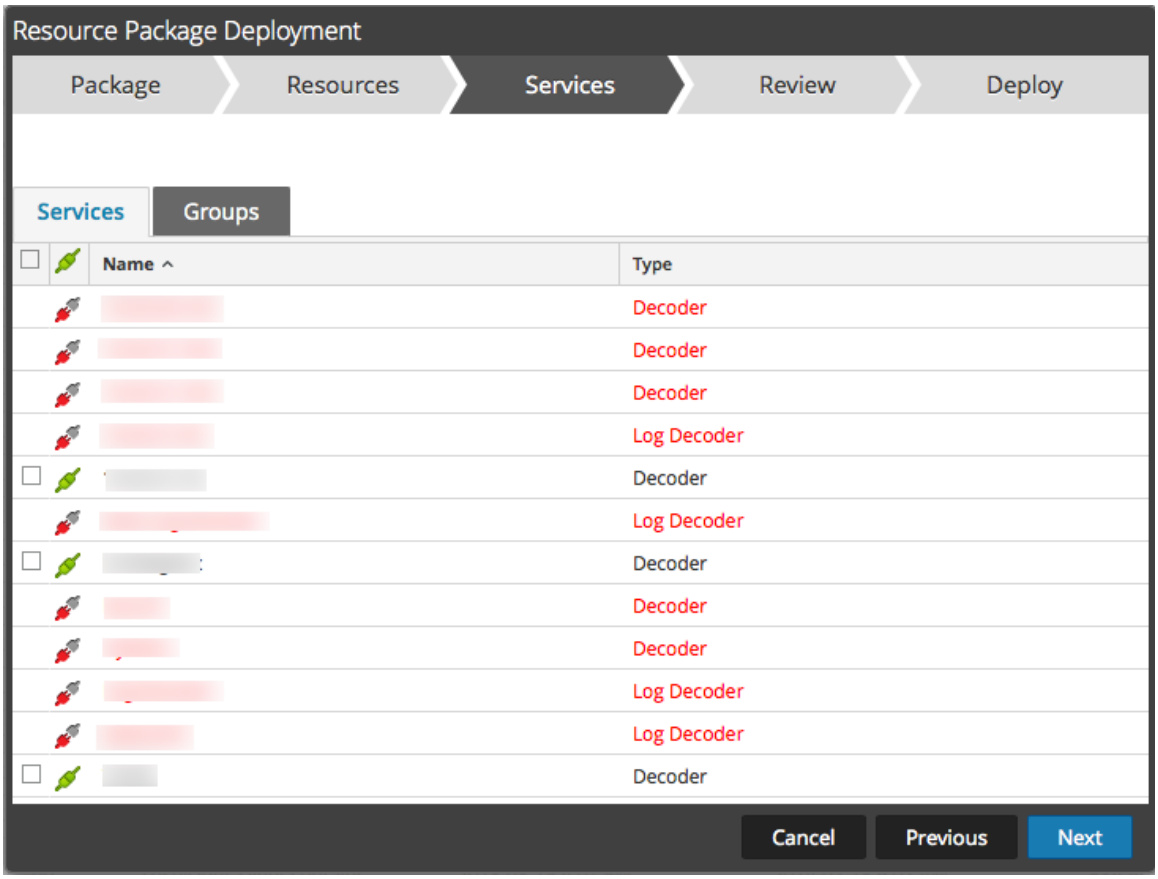
Spalte	Beschreibung
Ressourcenname	Zeigt den Namen der Ressourcen in dem Bundle an (z. B. **NetWitness Lua Library**).
Ressourcentyp	Zeigt die Ressourcentypen der Ressourcen in dem Bundle an (z. B. **RSA Lua Parser**).
Abhängigkeit von	Zeigt Ressourcen an, von denen die ausgewählte Ressource abhängt (z. B. **AIM lua**)

Registerkarte Services

Sie wählen den Service aus, für den Sie die Ressourcen im Bündel bereitstellen möchten.

Die Registerkarte „Services“ umfasst zwei Registerkarten, **Services** und **Gruppen**. Diese enthalten eine Liste von Services und Servicegruppen, die in der Ansicht „ADMIN“ > „Services“ konfiguriert sind. Die Spalten sind eine Untergruppe der Spalten, die in der Ansicht Services verfügbar sind. Sie können die Services oder die Servicegruppen auswählen, für die Sie die Ressourcen im Bündel bereitstellen möchten.

Dies ist ein Beispiel für die Registerkarte Services.



In der folgenden Tabelle werden die Elemente auf der Registerkarte „Services“ beschrieben.

Spalte	Beschreibung
Services	
☐	Wählt Services aus, auf denen der Inhalt bereitgestellt werden soll Sie können jede beliebige Kombination von Services und Servicegruppen auswählen.
Name	Zeigt die Services in Ihrer Umgebung an, auf denen Sie den Inhalt bereitstellen können
Host	Zeigt den Namen des Hosts der Ressource an.

Spalte	Beschreibung
Typ	Zeigt den Typ des NetWitness Suite-Services an.
Gruppen	
☐	Wählt Servicegruppen aus (wenn Sie in Ihrer Umgebung Gerätegruppen definiert haben)
Name	Zeigt die Namen der Servicegruppen an

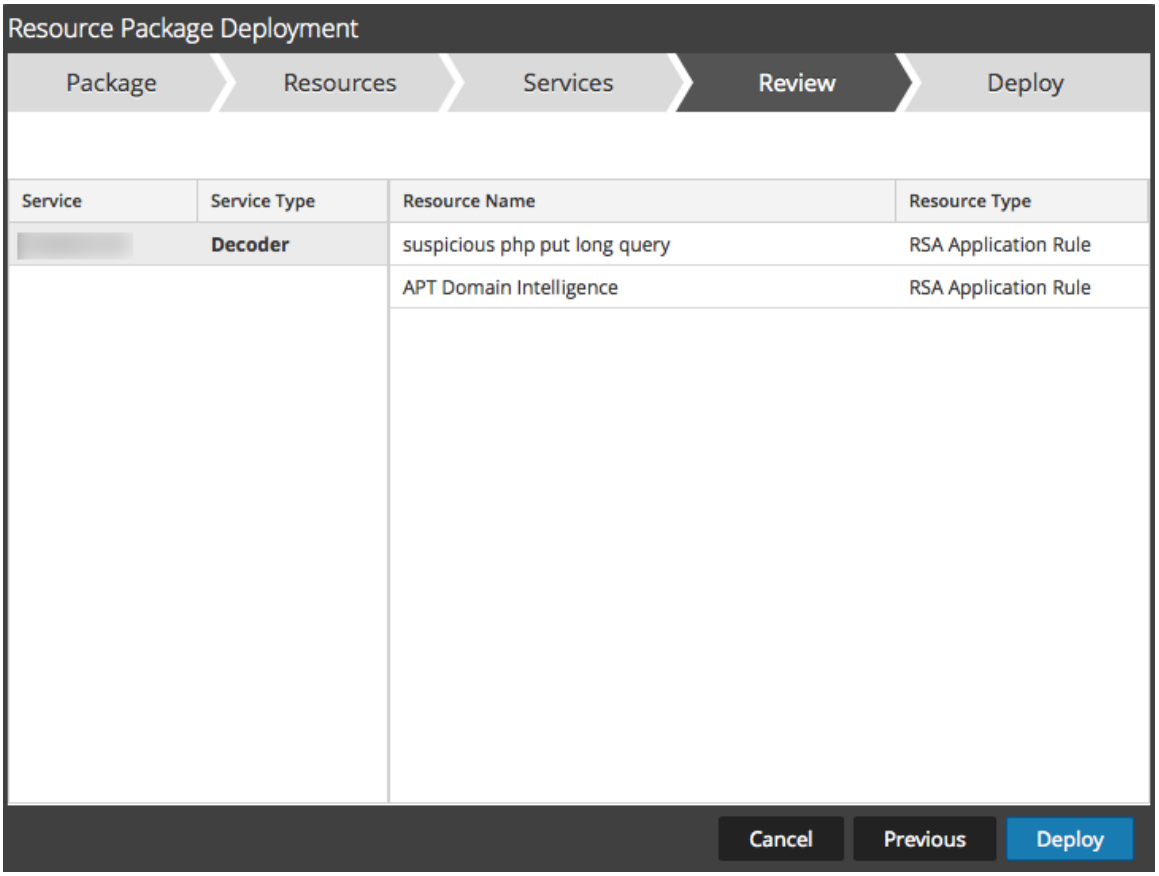
Registerkarte Überprüfen

Zeigt die Ressourcen und Services an, auf denen die Ressourcen bereitgestellt werden

In dieser Registerkarte können Sie folgende Aktionen ausführen:

- Überprüfen der Inhalte und Services vor der Bereitstellung
- Initiieren der Bereitstellung der Ressourcen

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Überprüfung.



In der folgenden Tabelle werden die Elemente auf der Registerkarte „Überprüfung“ beschrieben.

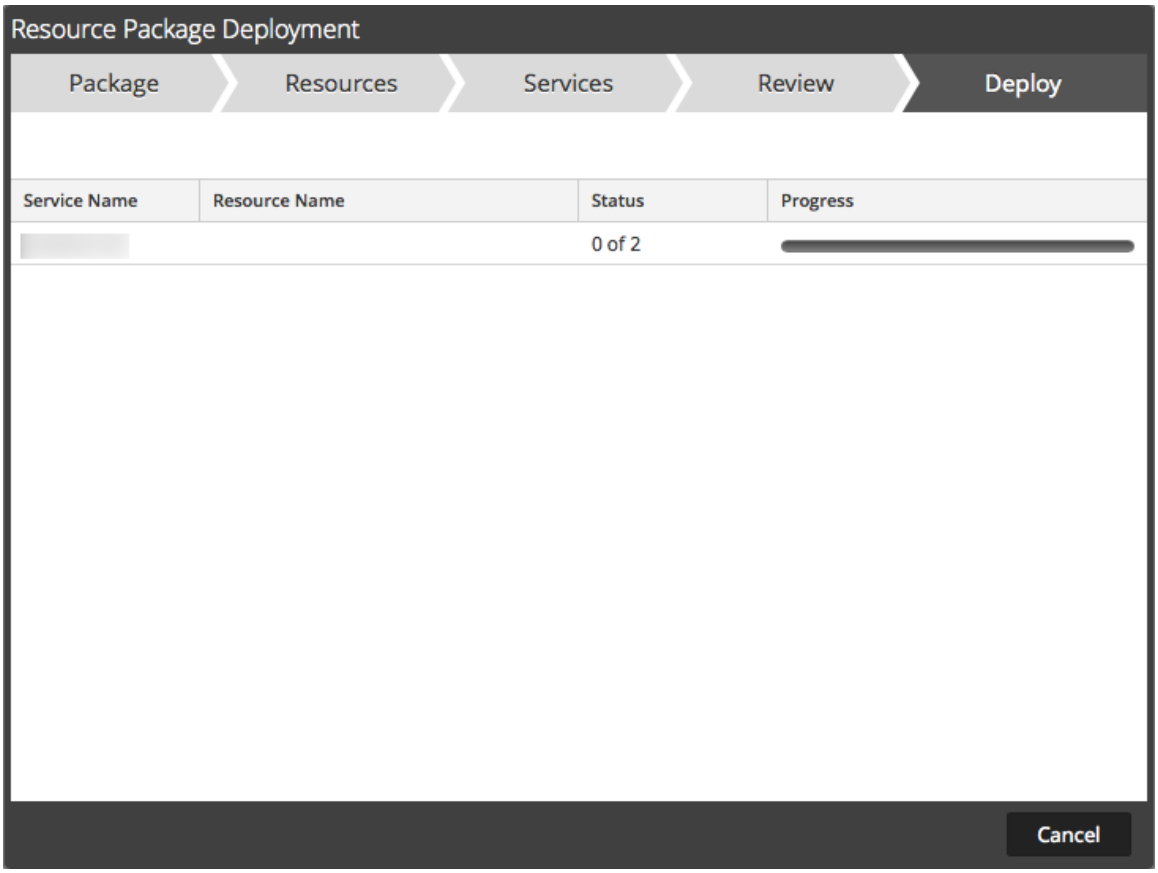
Spalte	Beschreibung
Serviceinformationen	
Service	Zeigt die Services in Ihrer Umgebung an, auf denen Sie den Inhalt bereitstellen können
Servicetyp	Zeigt den Typ des jeweiligen NetWitness Suite-Services an (Typ des Hosts/Services).
Informationen zur Ressource	
Ressourcenname	Zeigt den Namen der Ressourcen an, die Sie ausgewählt haben (z. B. **NetWitness Lua Library**).
Ressourcentyp	Zeigt die Ressourcentypen der Ressourcen an, die Sie ausgewählt haben (z. B. **RSA Lua Parser**).
Bereitstellen	Initiiert die Bereitstellung der Ressourcen und zeigt die Seite **Bereitstellen** an (letzte Seite des Assistenten)

Registerkarte Bereitstellen

Auf dieser Registerkarte können Sie Folgendes tun:

- Fortschritt des Jobs anzeigen
- Job abbrechen

Dies ist ein Beispiel für die Registerkarte Bereitstellen.



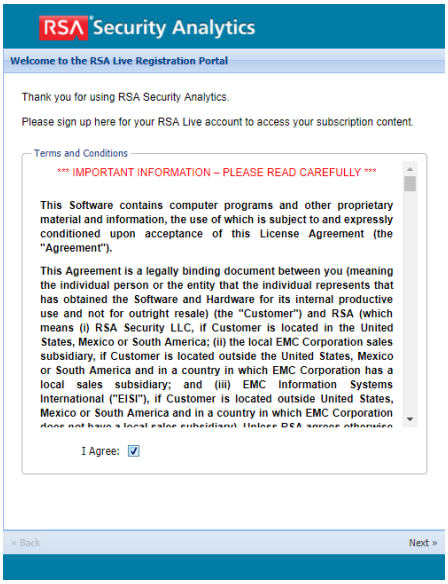
In der folgenden Tabelle werden die Elemente auf der Registerkarte „Bereitstellen“ beschrieben.

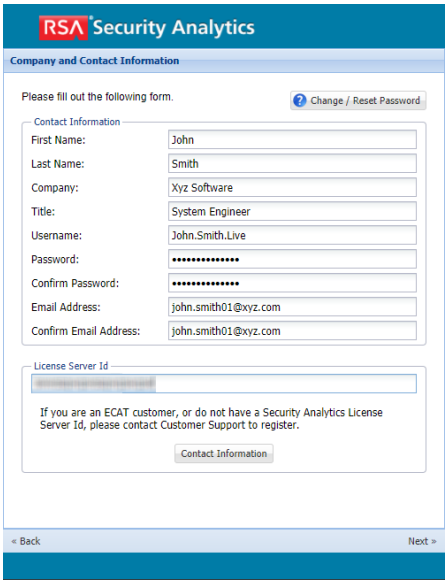
Funktion	Beschreibung
Servicename	Name des Services, auf dem die Ressourcen bereitgestellt werden
Ressourcenname	Name der Ressourcen
Status	Status der manuellen Bereitstellung
Progress	Fortschritt der manuellen Bereitstellung in einem Fortschrittsbalken Wenn der Vorgang abgeschlossen ist, ist dieser Balken durchgehend grün.
Befehlsschaltflächen	
Schließen	Schließt den Assistenten
Errors	Wird nur angezeigt, wenn in NetWitness Suite ein Fehler aufgetreten ist. Klicken Sie hierauf, um die Fehler anzuzeigen.

Funktion	Beschreibung
Erneut versuchen	Wird nur angezeigt, wenn in NetWitness Suite ein Fehler aufgetreten ist. Klicken Sie auf diese Schaltfläche, um die Ressourcen erneut mithilfe des Assistenten bereitzustellen.

RSA Live-Registrierungsportal

Das RSA Live-Registrierungsportal ist ein Selfservice-Assistent, in dem Kunden ein Live-Konto einrichten und das Passwort ändern oder zurücksetzen können. Ein Live-Konto wird für den Zugriff auf die Feeds, Parser, Regeln und andere Inhalte in der RSA Live-Bibliothek benötigt. Rufen Sie für den Zugriff auf das Portal die folgende URL auf: https://cms.netwitness.com/registration/.





Nachdem Sie den „Allgemeinen Geschäftsbedingungen“ zugestimmt und auf **Weiter** geklickt haben, werden die Felder zum Einrichten eines Kontos angezeigt. Dazu zählen die Abschnitte „Kontaktinformationen“, „Abonnementstufe“ und „Lizenzserver-ID“.

In der folgenden Tabelle sind die Felder des Abschnitts „Kontaktinformationen“ mit einer Beschreibung aufgeführt:

Parameter	Beschreibung
Passwort ändern/zurücksetzen	Über diese Option können die Benutzer ihr RSA Live-Passwort ändern oder zurücksetzen.

Parameter	Beschreibung
Vorname	Ihr Vorname
Nachname	Ihr Nachname
Unternehmen	Der Name des Unternehmens
Titel	Der Titel Ihrer Tätigkeit oder Funktion im Unternehmen
Benutzername	Der Benutzername, den Sie für die Anmeldung im RSA Live-Konto verwenden. Der Benutzername muss aus mindestens 9 und maximal 60 Zeichen bestehen.
Password	Das Passwort für das RSA Live-Konto Das Passwort muss aus mindestens 9 und maximal 60 Zeichen bestehen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.
Passwort bestätigen	Die Bestätigung Ihres Passworts
E-Mail-Adresse	Die E-Mail-Adresse, über die Sie Benachrichtigungen zu dem Live-Konto erhalten möchten.
E-Mail-Adresse bestätigen	Die Bestätigung der E Mail Adresse

Parameter	Beschreibung
Abonnementstufe/Abonnementstufe bestätigen	• **Basic**: Dies bietet Zugriff auf Live-Inhalte, die für Gruppen wie „Basic“, „Panorama for Log Decoder“ und „Spectrum for Malware Analysis“ markiert sind. • **Enhanced**: Dies bietet Zugriff auf Live-Inhalte, die für Gruppen wie „Enhanced“, „Basic“, „Panorama for Log Decoder“ und „Spectrum for Malware Analysis“ markiert sind. • **Premium**: Dies bietet Zugriff auf Live-Inhalte, die für Gruppen wie „Premium“, „Verisign Premium“, „Enhanced“, „Basic“, „Panorama for Log Decoder“ und „Spectrum for Malware Analysis“ markiert sind.
Lizenzserver-ID	Die Lizenzserver-ID, die sich auf der Seite **ADMIN > SYSTEM > Info** befindet. **Achtung:** Die Lizenzserver-ID in NetWitness Suite muss gültig und auf dem Flexera Server registriert sein. Ist dies nicht der Fall, wenden Sie sich an den RSA Customer Service.

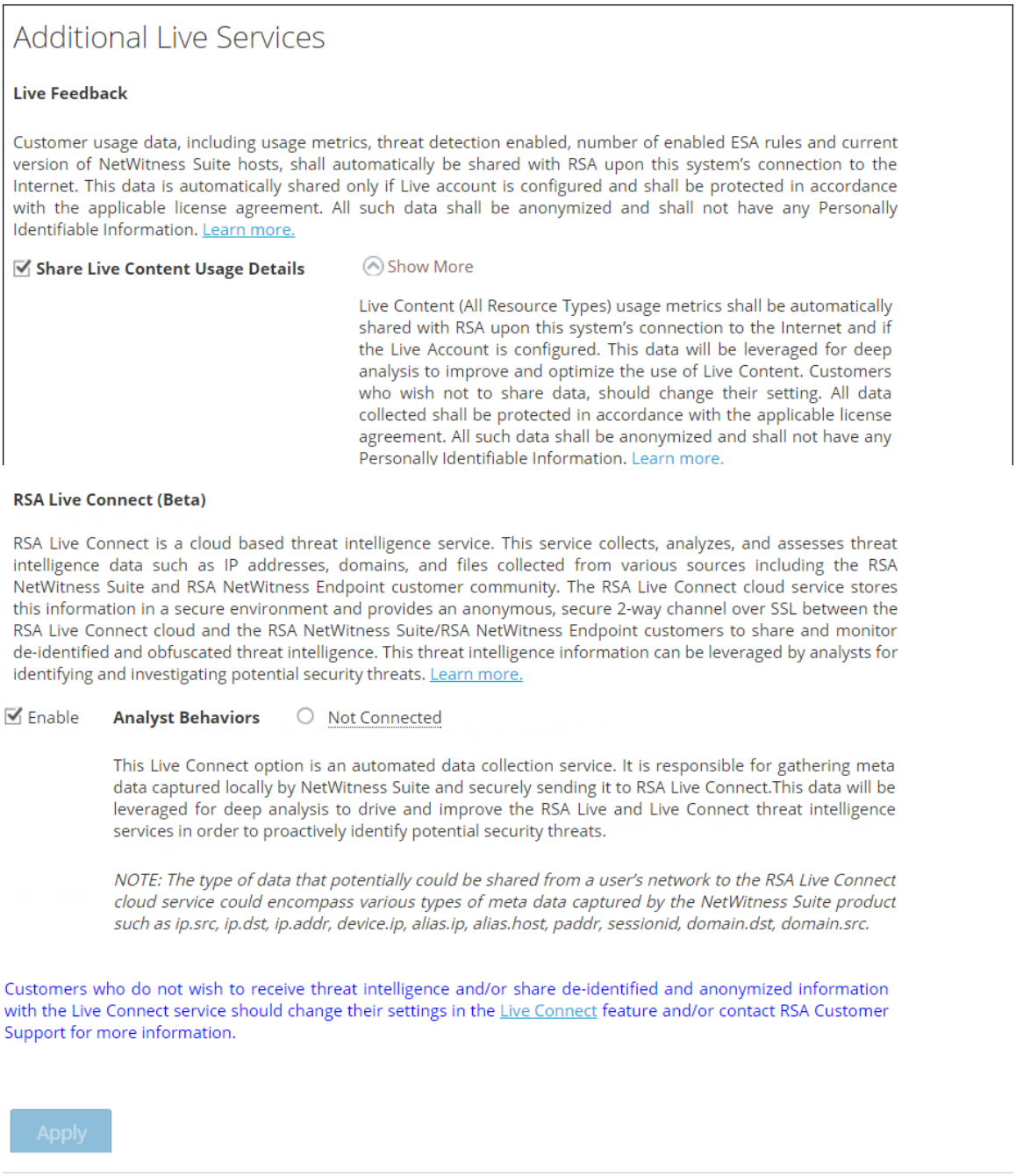
Feedback und Datenfreigabe in NetWitness Suite

In diesem Thema werden die Feedback- und Datenfreigabefunktionen von NetWitness Suite erläutert.

Die Einstellungen für diese Funktionen sind in der Ansicht **ADMIN** > **SYSTEM** > **Live-Services** im Bereich „Weitere Live-Services“ verfügbar.

Weitere Live-Services

Die Teilnahme an den weiteren Live-Services wird in der Ansicht **ADMIN > SYSTEM > Live-Services** konfiguriert.



Live Feedback

Live Feedback soll zur Verbesserung von RSA NetWitness Suite beitragen.

Wenn Sie ein Live-Konto eingerichtet und konfiguriert haben, werden die Nutzungsdaten für RSA freigegeben. Die Daten sind entsprechend den Bestimmungen des geltenden Lizenzvertrags geschützt. Sobald eine Internetverbindung mit dem System hergestellt wurde, können Nutzungsdaten von Kunden, z. B. Auslastungskennzahlen und die verwendete Version der NetWitness Suite-Hosts, automatisch an RSA übermittelt werden.

Bevor Daten an RSA gesendet werden, werden sämtliche personenbezogenen Informationen entfernt. Daher werden nur anonyme Nutzungsdaten an RSA übertragen.

Weitere Informationen finden Sie im Thema **Übersicht über Live Feedback** im *Systemkonfigurationsleitfaden*.

RSA Live Connect

Bei RSA Live Connect handelt es sich um einen cloudbasierten Bedrohungsinformationsservice. Dieser Service erfasst, analysiert und bewertet Daten zu Bedrohungen, wie beispielsweise IP-Adressen, Domains und Dateien, die aus verschiedenen Quellen erfasst wurden, unter anderem aus der Kunden-Community von RSA NetWitness Suite und RSA ECAT. RSA Live Connect bietet die folgenden Funktionen:

- Bedrohungseinblicke
- Analystenverhalten

Bedrohungseinblicke

„Bedrohungseinblicke“ ermöglicht Analysten das Abrufen von Daten zu Bedrohungen (z. B. IP-bezogene Informationen) vom Live Connect-Service, um sie bei Untersuchungen zu nutzen.

Bedrohungseinblicke ist im Abschnitt **Weitere Live-Services** standardmäßig aktiviert. Wenn der Context Hub-Service konfiguriert wurde, wird Live Connect automatisch als Datenquelle für Context Hub hinzugefügt. Weitere Informationen finden Sie im Thema **Konfigurieren von Live Connect-Datenquellen für Context Hub** im *Context Hub-Konfigurationsleitfaden*.

Mit Live Connect als Datenquelle für Context Hub können Sie die Option „Kontextabfrage“ in der Ansicht „Untersuchung > Navigieren“ oder der Ansicht „Untersuchung > Ereignisse“ verwenden, um kontextbezogene Informationen abzurufen. Anweisungen dazu finden Sie unter „Anzeigen von zusätzlichem Kontext für einen Datenpunkt“.

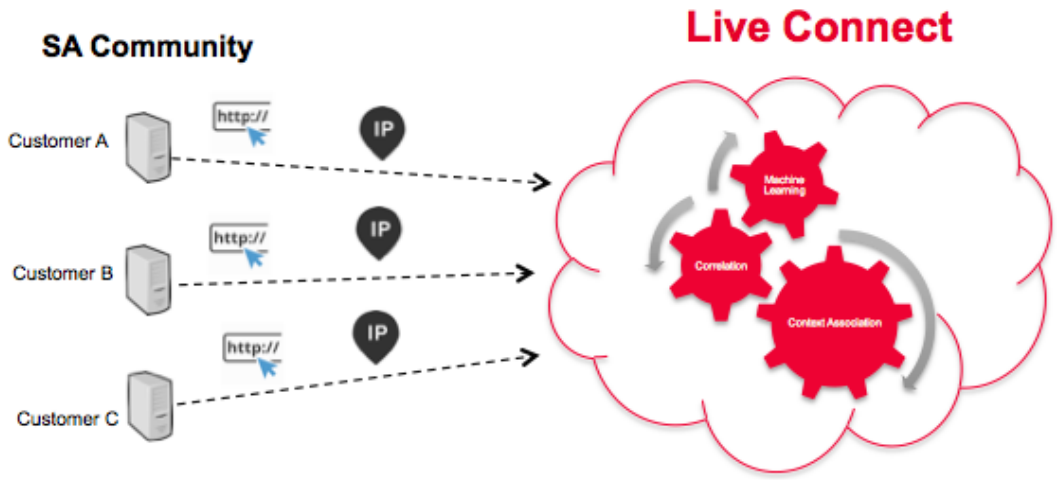
Analystenverhalten

„Analystenverhalten“ ist eine Funktion, bei der Analysten Daten mit der RSA-Community teilen. Dies ist ein automatisierter Datensammlungsservice. Ihr Ziel ist es, Informationen über potenzielle Bedrohungen im RSA Live Connect-Cloudservice für Analysezwecke zu teilen. Bei den Daten, die möglicherweise aus Ihren Netzwerk mit RSA Live Connect geteilt werden, kann es sich um verschiedene von NetWitness Suite erfasste Metadatentypen wie ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst oder domain.src handeln.

Hinweis: Alle lokal erfassten Daten werden anonymisiert und verschleiert und anschließend sicher und anonym an den RSA Live Connect-Cloudservice gesendet, wo sie in einer sicheren Umgebung gespeichert werden.

Beschreibung

Live Connect Threat Data Sharing wurde als Plattform für den communitybasierten Austausch von Bedrohungsinformationen entwickelt.



Die Funktion weist die folgenden Merkmale und Ziele auf:

- Crowdsourcing: Die RSA Community trägt zur gesamten Sammlung von Informationen bei
- Zentrales Erfassen und Analysieren von Daten aus der RSA-Community
- Reduzieren der Informationszykluszeit von Tagen auf Minuten

Einige zu berücksichtigende Details:

- Es werden die Untersuchungsaktivitäten von Analysten genutzt.
- Es werden Metadaten erfasst, z. B. IP-Adressen und Domainnamen.
- Es erfolgt eine umfassende Analyse der Daten: Trends, Korrelationen, Erkennung von Anomalien
- Diese Funktion befindet sich derzeit in der Betaphase.

Teilnahme

Die Mitwirkung unserer Kunden ist optional. Bei der Erstinstallation von oder dem Upgrade auf NetWitness Suite 11.0 wird ein Bestätigungsbildschirm angezeigt. Standardmäßig werden Sie in das Programm eingeschlossen, Sie können Ihre Teilnahme aber jederzeit beenden.

Cloudauthentifizierung

Die Authentifizierung für das Programm erfolgt auf der NetWitness Suite-Benutzeroberfläche, auf dem Sie das Live-Konto im Abschnitt „Live-Services“ konfigurieren.

Konfiguration

Wählen Sie zum Anzeigen oder Ändern der Einstellungen für Live Connect Threat Data Sharing im Menü „Hauptmenü“ die Optionen **ADMIN > SYSTEM > Live-Services** aus. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktivieren**, um teilzunehmen oder die Teilnahme am Programm zu beenden.

Datenerfassung

Daten werden wie folgt erfasst:

- Datenzuordnung: Anonym
- Datenquelle: Teile der Metaschlüssel und Metawerte der Seitenaufrufe von Analysten in NetWitness Suite aus den NetWitness Suite Core-Abfrageprotokollen
- Verfahren der Abfrageprotokollsammlung:
  - Zeit: Alle 24 Stunden im Batchmodus (4–6 Uhr UTC)
  - Protokollsammlung: Der NetWitness Suite-Server erfasst Protokolleinträge für NetWitness Suite Core-Geräte der letzten 24 Stunden
  - Protokolleinträge: Es werde nur SDK-Werte und SDK-Abfrage-API-Aufrufe erfasst, die eine Where-Klausel enthalten.
  - Protokollattribut-Parsing: Jeder Eintrag muss einen der folgenden Metaschlüsselindikatoren enthalten: **ip.src**, **ip.dst**, **ip.addr**, **device.ip**, **alias.ip**, **alias.host**, **paddr**, **sessionid**, **domain.dst** oder **domain.src**. Wenn dies der Fall ist, werden Metaschlüssel und Metawerte aus dem Eintrag erfasst.

Hinweis: Sobald die oben genannten Kriterien erfüllt sind, sendet NetWitness Suite alle Metaschlüssel und -werte aus der Abfrage in die Cloud – nicht nur die Metadaten wichtiger Indikatoren.

Der Protokollbericht wird im JSON-Format über SSL gesendet. Er enthält Folgendes:

- Zeitstempel
- Live-CMS-Benutzername (SHA-256)
- NetWitness Suite-Lizenzserver-ID (SHA-256)

- Liste der SA-Endpunkt-IDs (SHA-256)
- Erfasste Metawerte (MD5- und SHA-256-Hash)

Beispiel

In diesem Abschnitt werden die Einträge aus einem Protokoll und dann die entsprechenden Abschnitte der extrapolierten Daten aufgelistet.

Ausschnitt aus einer Protokolldatei:

```
User admin (session 204298, 10.4.50.60:57454) has issued values (channel 205237)
(thread 2332): fieldName=filter id1=1 id2=23138902 threshold=100000 size=20
flags=sessions,sort-total,order-descending,ignore-cache where="(alias.host =
'mail.google.com') && (ip.src = 161.253.31.130) && time=\"2015-12-07 18:08:00\"-
\"2015-12-07 21:07:59\""
```

Durch Hashing extrapolierte Daten:


```
-
{
    timestamp: 1452282588000,
    session: 204298,
    id1: 1,
    id2: 23138902,
    userName: "8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918",
    loggerName: "SDK-Values",
    timeRange: "\"2015-12-07 18:08:00\"-\"2015-12-07 21:07:59\"",
  - metaList: [
      - {
            metaKey: "alias.host",
          - properties: {
                domain_hint: "mai*********.com",
                domain_tld: "com",
                md5_value: "be5cab0695415d9363d18ad1345c73eb",
                sha256_value: "3f2728499a4b29460f3e3150df508e06b19edf0f58efd051fac777844d28e452"
            }
        },
      - {
            metaKey: "ip.src",
          - properties: {
                md5_value: "03b81ffdff109a05a3dac88dbec10c59",
                sha256_value: "1d88c6893797c896070bd5470d0026e11b515d5dee97c6173771a43719fa7e78"
            }
        }
    ]
},
```


Troubleshooting

Dieser Abschnitt enthält einige Informationen zum Troubleshooting von Live Connect Threat Data Sharing.

Beispiel für den Abfrageprotokollabruf

Um einen Auszug der an Live Connect gesendeten Bedrohungsinformationsdaten abzurufen, erstellen Sie eine URL, indem Sie die folgenden Parameter festlegen:

- **sendReport**: Wert ist **true** oder **false**: Legen Sie „true“ fest, um diesen Bericht an den Live Connect-Server zu senden. Legen Sie „false“ fest, um den Bericht nur für die Anzeige zu erstellen. Der Standardwert ist „false“.
- **hashValues**: Wert ist **true** oder **false**: Legen Sie „true“ fest, um die Werte in MD5/SHA-256-Hash-Werte umzuwandeln. Legen Sie „False“ fest, um die Werte als Klartext anzuzeigen. Dies sollte nur für die manuelle Anzeige verwendet werden. Der Standardwert ist „false“.
- **startDate/endDate**: Datumsangaben für Zeitbeschränkungen für Protokolleinträge. Format: JJJJ-MM-TT HH:mm:ss

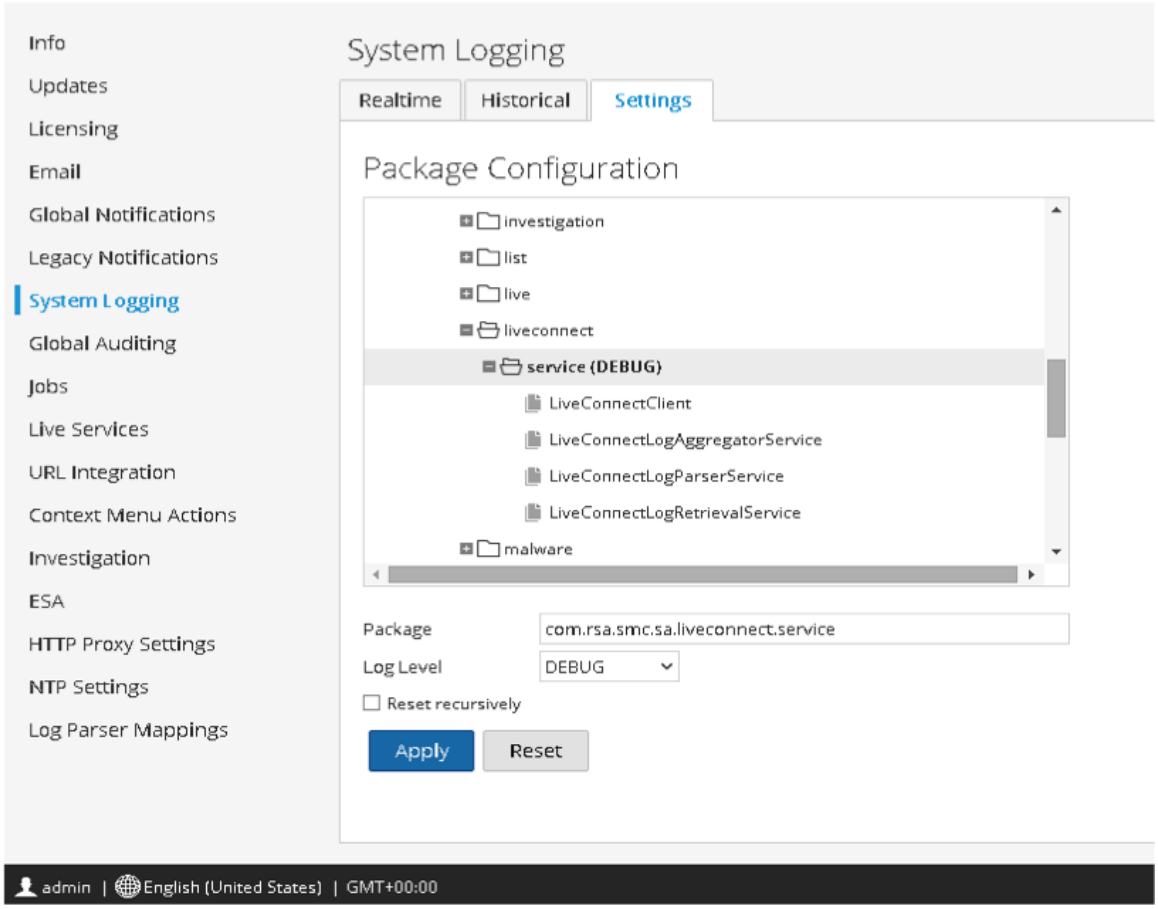
Es folgt ein Beispiel für die URL zum Abrufen der Abfrageprotokolle:

`https://<server>/admin/liveconnect/force_aggregation?`**`startDate=2016-01-18%2000:00:00&endDate=2016-01-19%2010:10:00&sendReport=false&hashValues=true`**

Systemprotokollierung: Debuggen

Sie können einige Debuginformationen wie folgt aufrufen.

1. Wählen Sie **ADMIN > SYSTEM > Systemprotokollierung** aus.
2. Wählen Sie die Registerkarte **Einstellungen** aus.
3. Wählen Sie im Bereich „Paketkonfiguration“ den Pfad **com > netwitness > platform > server > liveconnect > service (DEBUG)** aus.


Info
Updates
Licensing
Email
Global Notifications
Legacy Notifications
System Logging
Global Auditing
Jobs
Live Services
URL Integration
Context Menu Actions
Investigation
ESA
HTTP Proxy Settings
NTP Settings
Log Parser Mappings
System Logging
Realtime
Historical
Settings
Package Configuration
investigation
list
live
liveconnect
service (DEBUG)
LiveConnectClient
LiveConnectLogAggregatorService
LiveConnectLogParserService
LiveConnectLogRetrievalService
malware
Package
com.rsa.smc.sa.liveconnect.service
Log Level
DEBUG
Reset recursively
Apply
Reset
admin | English (United States) | GMT+00:00