RSA NETWITNESS® SUITE

Decoder und Log Decoder Konfigurationsleitfaden

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

Decoder und Log Decoder – Schnelleinrichtung

Ein grundlegendes Netzwerk der RSA Network Suite enthält mindestens Broker, Concentrator und Decoder. Broker aggregieren Daten von Concentrators und Concentrator verbrauchen Daten von mindestens einem Packet Decoder oder Log Decoder. Das grundlegende Netzwerk kann beide Arten Decoder enthalten. Die Packet Decoder werden in der Regel als Decoder bezeichnet. Sie erfassen Netzwerkdaten als Pakete. Log Decoder erfassen Daten als Ereignisse.

Wenn **ein Decoder hinzugefügt wird**, wird er sichtbar und steht zur Benutzung mit NetWitness Suite Administration, Live-Services und Ermittlung zur Verfügung. Zum Hinzufügen eines Service in NetWitness Suite müssen Sie den Service auswählen, Verbindungsinformationen für den Service angeben und überprüfen, ob der Service erreichbar ist. Der *Leitfaden für die ersten Schritte mit Hosts und Services* enthält alle Informationen, die Sie zum Verstehen und Installieren aller NetWitness Suite-Services benötigen.

Nachdem Sie die Services hinzugefügt haben, müssen Sie sie konfigurieren. Das hier ist die bevorzugte Reihenfolge für die Konfiguration Ihres Systems:

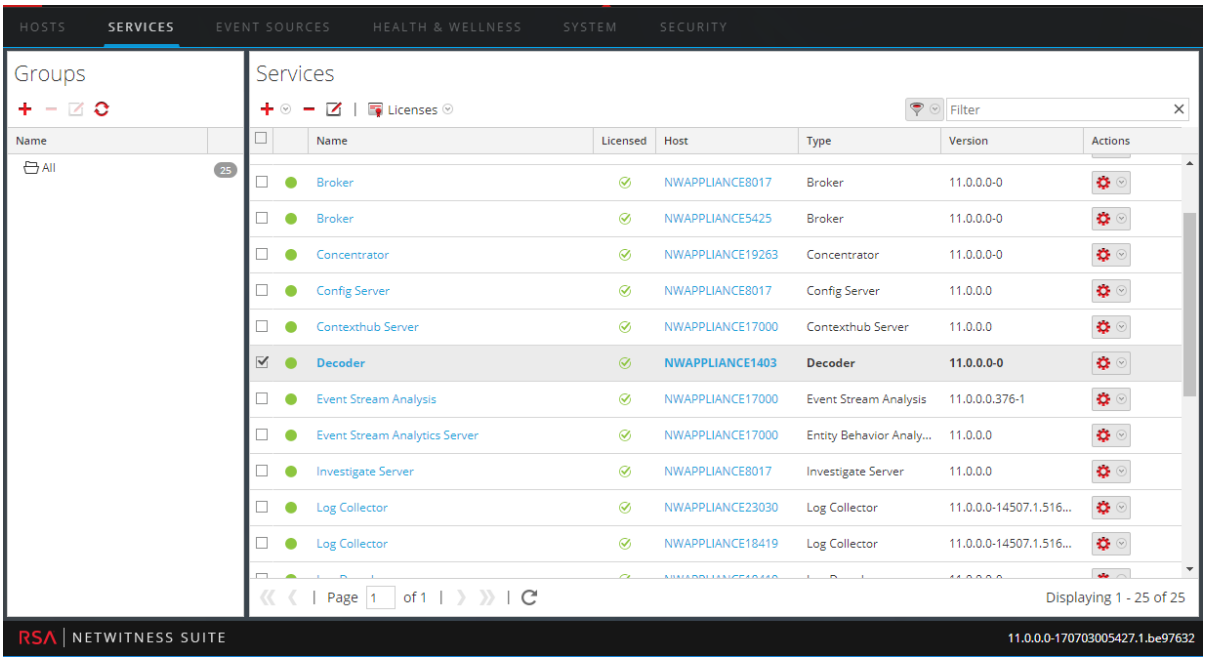
1. Decoder
2. Log Decoder
3. Concentrator (siehe *Konfigurationsleitfaden für Broker und Concentrator*)
4. Broker (siehe *Konfigurationsleitfaden für Broker und Concentrator*)

Hinweis: Ein Log Decoder ist ein spezieller Typ Decoder und wird ähnlich wie ein solcher konfiguriert und verwaltet. Ein Großteil der Informationen in diesem Abschnitt bezieht sich auf beide Arten Decoder. „Decoder“ bezieht sich auf beide Arten von Decodern. Informationen, die sich ausschließlich auf Packet Decoder oder Log Decoder beziehen, sind eindeutig gekennzeichnet.

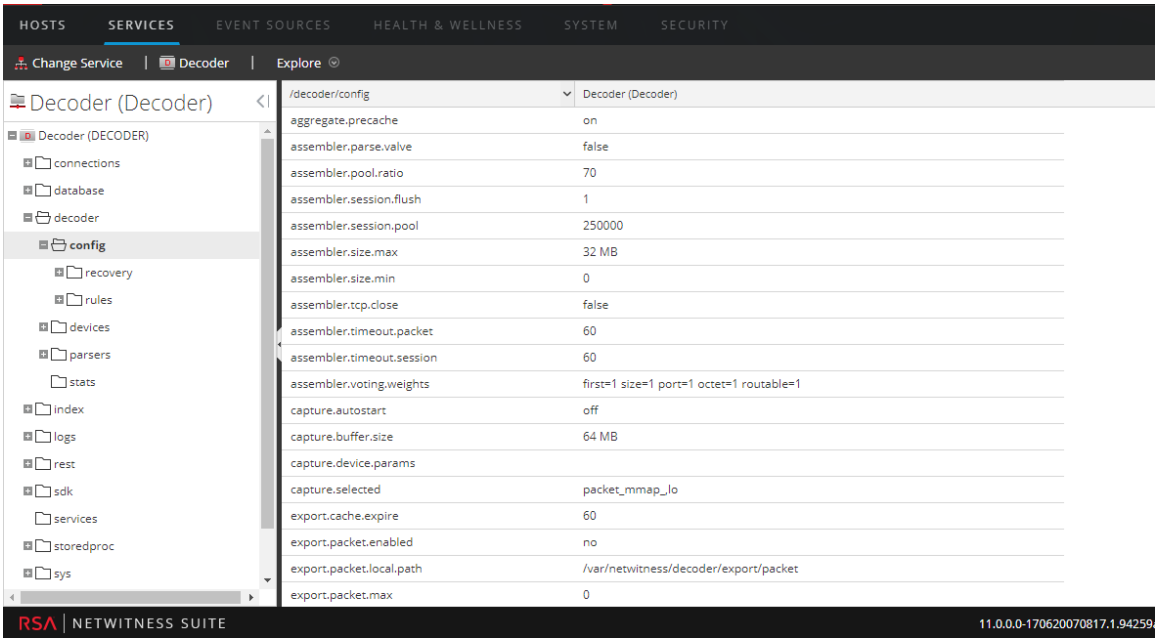
Die **grundlegende Konfiguration des Decoders** umfasst das Festlegen einer Netzwerkadapter-Schnittstelle sowie das Starten der Datenerfassung.

Zudem können Sie jeden Decoder so konfigurieren, dass er die Art des erfassten Datenverkehrs mithilfe von Regeln, Feeds und Parsern kontrolliert. Durch erweiterte Konfigurationsaufgaben können zusätzliche Funktionen aktiviert werden, die für spezielle Anwendungen relevant sind. So können zum Beispiel 10G-Decoder konfiguriert, benutzerdefinierte Metaschlüssel erstellt oder eingehende Pakete entschlüsselt werden.

Die einfachste Methode zur Konfiguration aller erforderlichen Decoder- und Log Decoder-Einstellungen ist die Verwendung der Optionen auf der NetWitness Suite-Benutzeroberfläche. Die Konfiguration erfolgt größtenteils in der Ansicht „Administration Services“ (ADMIN > Services).



Administratoren, die gerne außerhalb der Benutzeroberfläche arbeiten, können die grundlegenden Parameter sowie erweiterte Einstellungen konfigurieren, indem Sie Datenbank-Nodes in der Decoder-Node-Struktur in der Ansicht zum Durchsuchen zu einem Service bearbeiten.

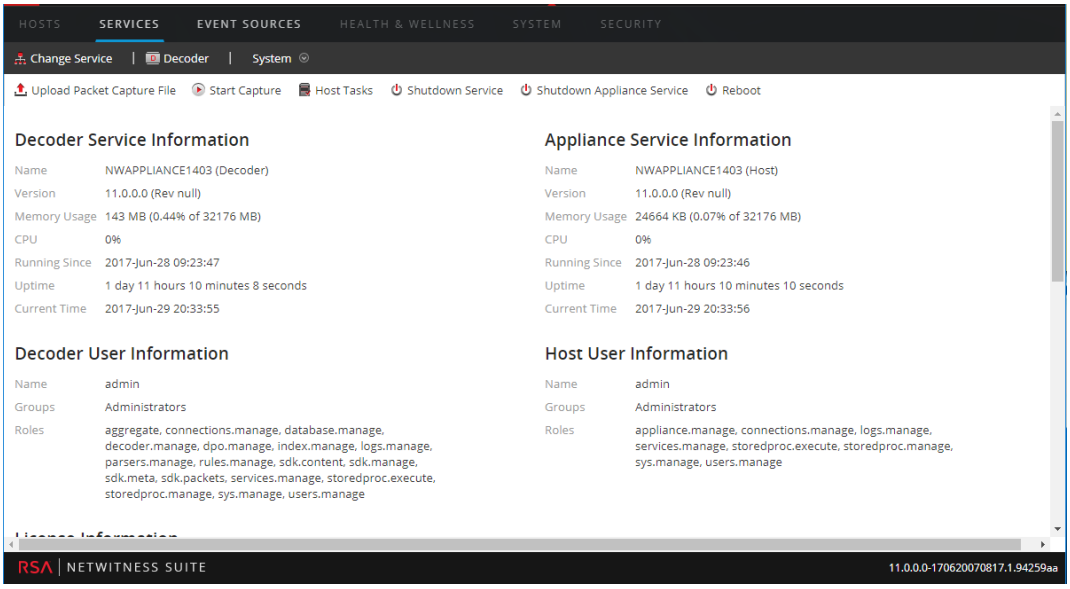


Durchführen der Ersteinrichtung

Dieses Verfahren dient zur grundlegenden Ersteinrichtung eines Decoders und zum Starten der Datenerfassung. Wenn Sie die grundlegende Einrichtung abgeschlossen ist, beginnt der Decoder mit der Erfassung von Daten, die vom Concentrator verarbeitet werden.

So konfigurieren Sie einen Decoder beginnen mit der Datenerfassung:

1. Weisen Sie eine Netzwerkschnittstelle zur Datenerfassung zu. Weitere Informationen erhalten Sie in „Auswählen eines Netzwerkadapters“ in Konfigurieren von Erfassungseinstellungen.
2. Führen Sie einen der folgenden Schritte aus:
   a. Beginnen Sie die Erfassung, indem Sie den Decoder und anschließend > **Ansicht** > **System** auswählen. Klicken Sie auf der Symbolleiste auf Start Capture.



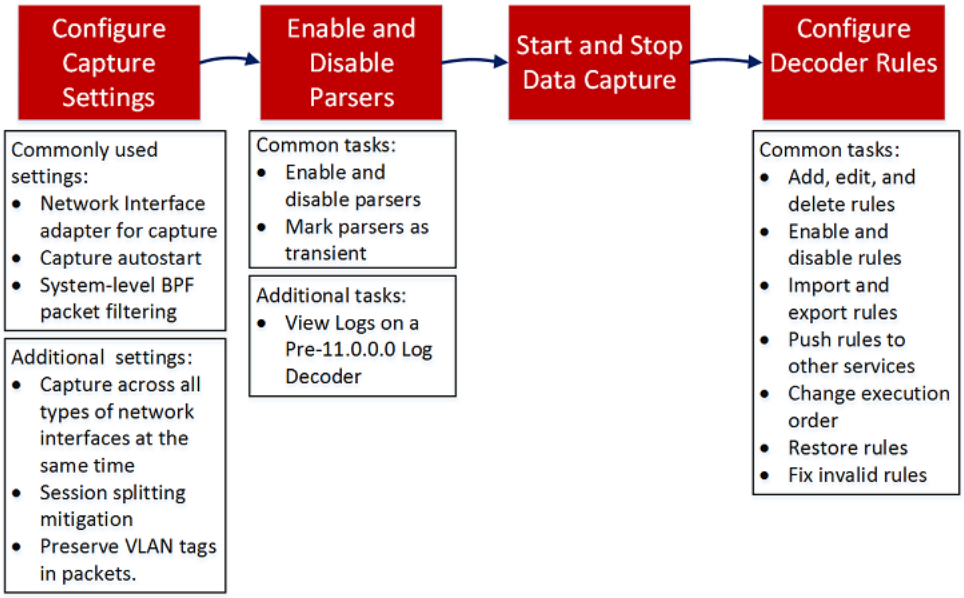
   b. Weitere Informationen zur Aktivierung von „Erfassungs-Autostart“ finden Sie in „Konfigurieren eines Decoders zum automatischen Beginn der Datenerfassung“ in Konfigurieren von Erfassungseinstellungen.
   Der Decoder beginnt mit der Erfassung von Daten zur Verarbeitung durch einen Concentrator. Zusätzliche Konfigurationsoptionen finden Sie in Konfigurieren von allgemeinen Einstellungen auf einem Decoder und Decoder und Log Decoder – zusätzliche Verfahren.

Konfigurieren von allgemeinen Einstellungen auf einem Decoder

In diesem Abschnitt werden häufig verwendete Konfigurationseinstellungen auf einem Decoder mit Verfahren und Hintergrundinformationen behandelt. Nachdem Sie Decoder und Log Decoder – Schnelleinrichtung abgeschlossen haben, können Sie Ihre Konfiguration optimieren, indem Sie Parser, Feeds und Regeln verwenden, um die erfassten Daten zu begrenzen.

Hinweis: Ein Log Decoder ist ein spezieller Typ Decoder und wird ähnlich wie ein solcher konfiguriert und verwaltet. Ein Großteil der Informationen in diesem Abschnitt bezieht sich auf beide Arten Decoder. „Decoder“ bezieht sich auf beide Arten von Decodern. Informationen, die sich ausschließlich auf Packet Decoder oder Log Decoder beziehen, sind eindeutig gekennzeichnet.

Im folgenden Workflow werden häufig verwendete Einstellungen dargestellt und der Konfigurationsprozess in vier Schritte unterteilt.

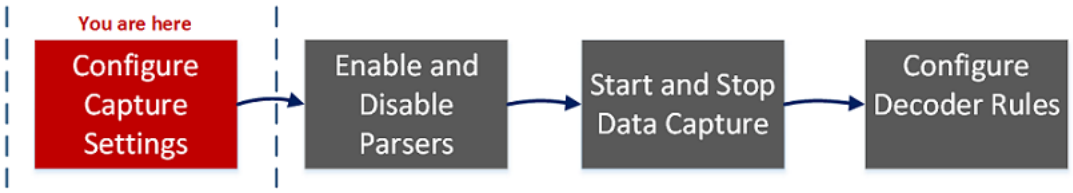


Konfigurationsschritt	Beschreibung
Konfigurieren von Erfassungseinstellungen	Beim ersten Einrichten des Decoders ist die Konfiguration der Netzwerkadapter-Schnittstelle erforderlich. Zusätzliche optionale Erfassungseinstellungen sind verfügbar. Eine häufig verwendete Einstellung ist „Erfassungs-Autostart“.

Konfigurationsschritt	Beschreibung
Aktivieren und Deaktivieren von Parsern und Protokollparsern	Lassen Sie sich anzeigen, welche Parser von Live heruntergeladen und bereitgestellt wurden, und verwalten Sie, welche aktiviert bzw. deaktiviert sind.
Starten und Beenden der Datenerfassung	Beim Starten eines Decoder werden automatisch Daten aggregiert, wenn die Funktion „Erfassungs-Autostart“ aktiviert ist. Wenn der automatische Start nicht aktiviert ist, können Sie die Datenerfassung manuell starten oder beenden.
Konfigurieren von Decoder-Regeln	Erfassungsregeln können Sitzungen oder Protokollen Warnmeldungen oder kontextbezogene Informationen hinzufügen. Sie können außerdem definieren, welche Daten von einem Decoder oder Log Decoder herausgefiltert werden. Standardmäßig sind keine Erfassungsregeln definiert, wenn Sie NetWitness Suite erstmals konfigurieren. Wenn keine Regeln festgelegt werden oder die Regeln ungültig sind, werden Pakete nicht gefiltert. Die aktuellen Regeln können Sie wie im *Handbuch zum Live-Services-Management* beschrieben von Live bereitstellen. Sie können jederzeit Erfassungsregeln definieren Regeln korrigieren, die eine ungültige Syntax haben (Korrigieren von Regeln mit ungültiger Syntax).

Konfigurieren von Erfassungseinstellungen

Beim ersten Einrichten des Decoders ist die Konfiguration der Netzwerkadapter-Schnittstelle erforderlich. Zusätzliche optionale Erfassungseinstellungen sind verfügbar. Zwei, die häufig verwendet werden, sind der Berkeley Packet Filter und der Erfassungs-Autostart.



Neben der grundlegenden Einrichtung der Netzwerkadapter-Schnittstelle können Sie eine der in (Optional) Beibehalten von VLAN-Tags bei der Nutzung der Paket-MMAP-Erfassungsschnittstelle oder (Optional) Konfigurieren eines Decoders zur Datenerfassung für alle Arten von Netzwerkschnittstellen beschriebenen speziellen Konfigurationen nutzen.

Für den Rest der Erfassungseinstellungen werden Standardwerte festgelegt, die für die meisten Fälle gut geeignet sind. Eine detaillierte Liste ist in der Ansicht Ansicht „Services-Konfiguration“ – Registerkarte „Allgemein“ zu finden. Sie können diese unter bestimmten Umständen anpassen, beispielsweise dann, wenn der Kundensupport Sie anweist, eine Änderung vorzunehmen. Sie können die Erfassungseinstellungen jederzeit ändern.

Auswählen eines Netzwerkadapters

In der Tabelle unten werden die Netzwerkadaptereinstellungen für einen Decoder beschrieben. Der Systemadministrator legt die Standardnetzwerkadapter fest, wenn der Decoder installiert wird. Wenden Sie sich für weitere Informationen an Ihren Systemadministrator.

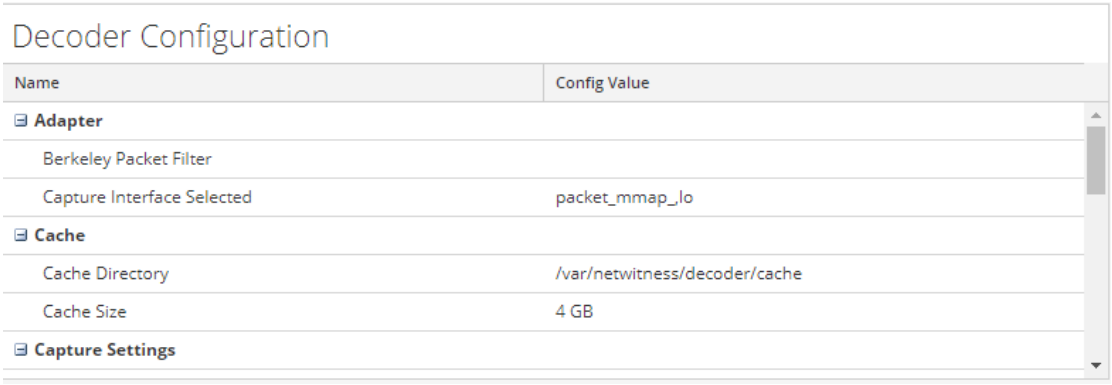
Adapter-Parameter	Beschreibung
Berkley Packet Filter	Berkeley Packet Filter (BPF) werden auf den Paketstream angewendet, bevor die Pakete auf den Decoder-Adapter zur Analyse kopiert werden. Dies ermöglicht das effiziente Verwerfen ungewollten Datenverkehrs. Allerdings werden verworfene Pakete in keiner Decoder-Statistik berücksichtigt (Erfassungsrate, Paketverluste und gefilterte Pakete und Pakete gesamt).

Adapter-Parameter	Beschreibung
Ausgewählte Erfassungsschnittstelle	Wählen Sie einen Adapter aus, durch den der Decoder Pakete erfasst. Verwenden Sie für die langsamere interne Erfassungsschnittstelle den Adapter `packet_mmap_,7,eth1`, der dem Überwachungsport auf dem Motherboard entspricht. Es gibt sechs zusätzliche Erfassungsports: • `packet_mmap_,1,lo (bpf)` • `packet_mmap_,2,eth2 (bpf)` • `packet_mmap_,3,eth3 (bpf)` • `packet_mmap_,4,eth4 (bpf)` • `packet_mmap_,5,eth5 (bpf)` • `packet_mmap_,8,ALL (bpf)` Es stehen drei drahtlose Erfassungsservices zur Verfügung: • `packet_netmon_ (Microsoft Netmon)` • `packet_mac80211_ (Linux mac80211)` • `packet_airport_ (Mac OS X AirPort)`
Für Log Decoder ausgewählte Erfassungsschnittstelle	Der folgende Erfassungsservice ist verfügbar: • `log_events,Protokollereignisse`

So konfigurieren den Netzwerkadapter auf einem Decoder:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der **Ansicht „Administration Services“** den Decoder und **> Ansicht > Konfiguration**
   aus.Die Ansicht „Service-Konfiguration“ wird angezeigt und die Registerkarte „Allgemein“

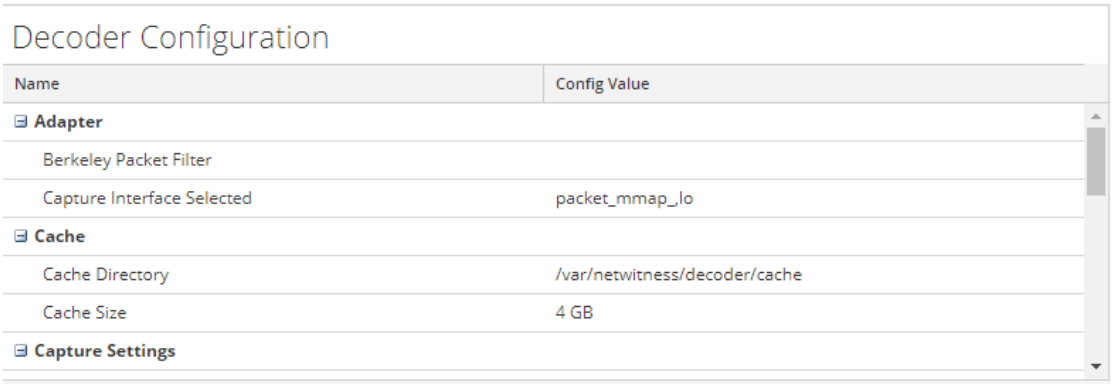
geöffnet.



3. Wählen Sie im Feld **Ausgewählte Erfassungsschnittstelle** den Netzwerkadapter aus, der sich am besten für den Decoder eignet.
4. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.
5. Sollen die Änderungen sofort übernommen werden, navigieren wieder zur **Ansicht „Administration Services“** und wählen Sie den Decoder und im Anschluss > **Neu starten** aus.

Konfigurieren eines Decoders zum automatischen Beginn der Datenerfassung

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der **Ansicht „Administration Services“** den Decoder und **> Ansicht > Konfiguration**
   aus.Die Ansicht „Service-Konfiguration“ wird angezeigt und die Registerkarte „Allgemein“ geöffnet.

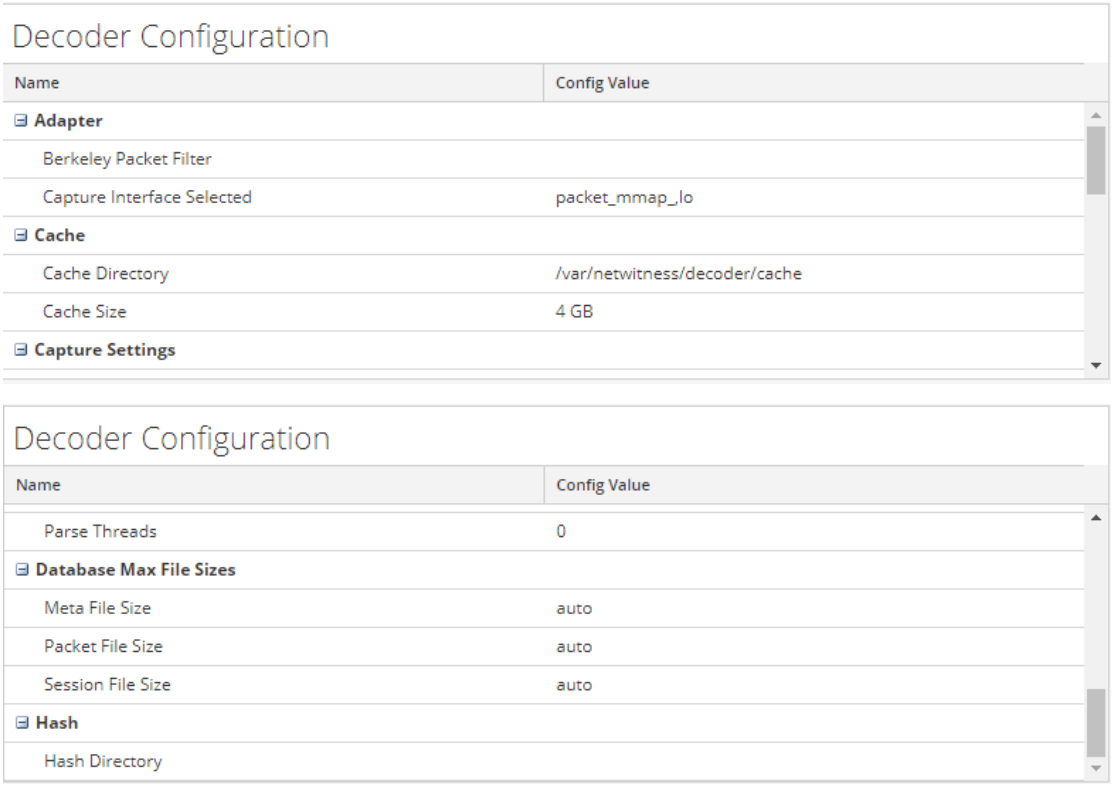


3. Wählen Sie unter **Erfassungseinstellungen** das Kontrollkästchen **Erfassungs-Autostart** aus.

4. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.
5. Sollen die Änderungen sofort übernommen werden, navigieren wieder zur **Ansicht „Administration Services“** und wählen Sie den Decoder und im Anschluss > **Neu starten** aus.

Konfigurieren von optionalen Erfassungseinstellungen

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der **Ansicht „Administration Services“** den Decoder und **> Ansicht > Konfiguration**
   aus.Die Ansicht „Service-Konfiguration“ wird angezeigt und die Registerkarte „Allgemein“ geöffnet.



3. Wenn ein Filter auf Systemebene auf den Paketstream angewendet werden soll, bevor die Pakete zur Analyse auf den Decoder-Adapter kopiert werden, konfigurieren Sie den Berkeley Packet Filter wie in (Optional) Konfigurieren der Paketfilterung auf Systemebene (BPF) beschrieben.
4. Überprüfen Sie im Abschnitt **Einstellungen erfassen** die Standardwerte. Wenn ein Service zum ersten Mal hinzugefügt wird, werden Standardwerte festgelegt, die nur unter

besonderen Umständen geändert werden dürfen, beispielsweise dann, wenn der Kundensupport Sie anweist, eine Änderung vorzunehmen. In der Ansicht „Services-Konfiguration“ – Registerkarte „Allgemein“ finden Sie eine Erläuterung dieser Einstellungen.

5. Überprüfen Sie im Abschnitt **Maximale Datenbankdateigrößen** die Standardwerte. Wenn ein Service zum ersten Mal hinzugefügt wird, werden Standardwerte festgelegt, die nur unter besonderen Umständen geändert werden dürfen, beispielsweise dann, wenn der Kundensupport Sie anweist, eine Änderung vorzunehmen. In der Ansicht „Services-Konfiguration“ – Registerkarte „Allgemein“ finden Sie eine Erläuterung dieser Einstellungen.
6. Definieren Sie im Abschnitt **Hash** ein Verzeichnis für Hash-Dateien, wenn Sie diese Funktion verwenden. In der Ansicht „Services-Konfiguration“ – Registerkarte „Allgemein“ finden Sie eine Erläuterung dieser Einstellungen.

(Optional) Konfigurieren der Paketfilterung auf Systemebene (BPF)

Sie können mit den Berkeley Packet Filters festlegen, welche Pakete und Protokolle von einem Decoder verarbeitet werden.

Berkeley Packet Filters (BPF) werden auf den Paketstream angewendet, bevor die Pakete auf den Decoder-Adapter zur Analyse kopiert werden. Dies ermöglicht das effiziente Verwerfen ungewollten Datenverkehrs. Diese verworfenen Pakete werden in keiner Decoder-Statistik berücksichtigt (Erfassungsrate, Paketverluste und gefilterte Pakete und Pakete gesamt).

Der Decoder unterstützt auch Paketfilterung auf Systemebene, die mithilfe der Syntax `tcpdump/libpcap` definiert wird. Die Angabe eines `Libpcap`-Filters kann das Paketvolumen basierend auf Attributen der Schicht 2 - Schicht 4 effizient reduzieren. Ein `Libpcap`-Filter eignet sich, wenn ein Decoder ein hohes Datenvolumen empfängt, das die physischen Ressourcen der Plattform belastet. In diesem Szenario verwirft der Decoder möglicherweise beständig Pakete und erfasst sehr viele Seiten (`/decoder/stats/capture.pagefree` ist hoch).
Hier ist ein Beispiel für einen `libpcap`-Filter, der nur Pakete behält, deren Quell- und Zieladresse nicht beide im Subnetz 10.21.0.0/16 liegen.

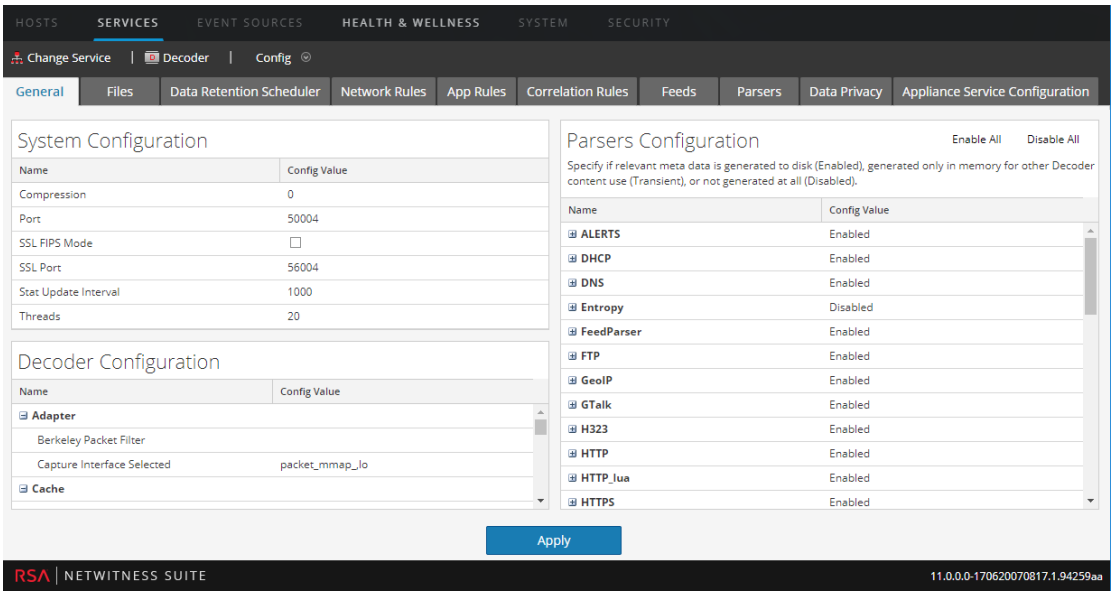
```
not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)
```

Eine vollständige Referenz der Syntax des `Libpcap`-Filters finden Sie auf den Hauptseiten für:

- tcpdump (http://www.tcpdump.org/tcpdump_man.html).
- pcap-filter (http://www.unix.com/man-page/FreeBSD/7/pcap-filter/).

So fügen Sie einen Berkeley Packet Filter auf Systemebene hinzu:

1. Navigieren Sie zu ADMIN > **Services.**
2. Wählen Sie in der Ansicht „Administration Services“ einenDecoder-Service und  > **Ansicht > Konfiguration** aus.
   Die Ansicht Ansicht „Service-Konfiguration“ wird mit geöffneter Registerkarte „Allgemein“ angezeigt.



3. Klicken Sie im Abschnitt **Decoder-Konfiguration** unter **Adapter** in das Feld neben **Berkeley Packet Filter**.
4. Geben Sie nur einen Filter in das Feld ein. Wenn Sie mehrere Elemente filtern möchten, verknüpfen Sie mehrere Ausdrücke mithilfe von `and`. Unten werden verschiedene Beispiele gezeigt.
   In der Benutzeroberfläche wird die Filterzeichenfolge validiert, während Sie sie eingeben.
5. Klicken Sie zum Speichern des Filters auf **Anwenden**.
   Ist die Syntax korrekt, wird eine Bestätigungsmeldung angezeigt.
   Wenn die Syntax falsch ist, wird die Meldung **Paketfilter ist ungültig** angezeigt, gefolgt von einer entsprechenden Protokollmeldung auf dem Decoder:
   ```
   164474800 2015-May-01 19:03:08 warning Decoder Failed to parse filter 'example_badrule': syntax error
   ```
6. Zum Aktivieren des Filters müssen Sie die Erfassung auf dem Decoder beenden und wieder starten:

a. Wechseln Sie von der Ansicht **Konfiguration** zur Ansicht **System**.

b. Klicken Sie auf **Erfassung beenden**.

c. Klicken Sie auf **Erfassung starten**.
Der aktive Filter wird in den Decoder-Protokollen angezeigt.

Beispiele

Es folgen einige Beispiele für Filter:

- Verwerfen von Paketen zu oder von Adressen im 10.21.0.0/16-Subnetz:
  `not (net 10.21.0.0/16)`
- Verwerfen von Pakten, die sowohl Quell- als auch Zieladressen im 10.21.0.0/16-Subnetz haben:
  `not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`
- Verwerfen von Paketen, die aus dem 10.21.1.2-Subnetz stammen oder an das 10.21.1.3-Subnetz gesendet werden sollen:
  `not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Kombinieren von IP und HOST:
  `not (host 192.168.1.10) and not (host api.wxbug.net)`
- Verwerfen sämtlichen Datenverkehrs auf dem TCP- und UDP-Port 53:
  `not (port 53)`
- Verwerfen des Datenverkehrs nur auf dem UDP-Port 53:
  `not (udp port 53)`
- Verwerfen sämtlichen IP-Protokoll-50-Datenverkehrs (IPSEC):
  `not (ip proto 50)`
- Verwerfen sämtlichen Datenverkehrs auf den TCP-Ports 133 bis 135:
  `not (tcp portrange 133-135`

Die folgenden Filter kombinieren einige der oben genannten Filter, um zu demonstrieren, wie mehrere Richtlinien in einem Filter vereint werden können:

- Verwerfen sämtlichen Port-53(DNS)-Datenverkehrs, der vom 10.21.1.2-Subnetz stammt oder an das 10.21.1.3-Subnetz gesendet werden soll:
  `not (port 53) and not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Verwerfen sämtlichen Datenverkehrs über IP-Protokoll 50 oder Port 53 oder Datenverkehr von net 10.21.0.0/16 zu net 10.21.0.0/16

```
not (ip proto 50 or port 53) or not (src net 10.21.0.0/16 and dst net
10.21.0.0/16)
```

Achtung: Die Verwendung von Klammern kann eine erhebliche und potenziell störende Auswirkung auf die Verwendung von Paketfiltern haben. Als Best Practice sollten „not"-Vorgänge außerhalb der Klammern platziert werden. Testen Sie Regeln stets, bevor Sie sie bereitstellen. Wenn die Regeln nicht ordnungsgemäß formatiert sind (trotz Validierung der Eingabe), kann ein Paketfilter möglicherweise SÄMTLICHEN Datenverkehr verwerfen oder auf andere Weise unerwartet reagieren. Dies ist auf die Funktionsweise der `Libpcap`-Paketfilter zurückzuführen und nicht das Ergebnis einer Logik in der NetWitness Suite-Software.

Tests

BPF-Filter können und sollten vor der Implementierung mithilfe von `tcpdump` oder `windump` getestet werden, um sicherzustellen, dass sie wie erwartet reagieren. Dieses Beispiel zeigt einen Filtertest mithilfe von „windump":

```
windump -nni 2 not (port 53 or port 443) or not (ip proto 50)
```

Konvertierungen

Wenn Sie feststellen, dass ein vorhandener Netzwerkregelfilter aus Performancegründen eher als Paketfilter auf Systemebene ausgeführt werden sollte, können Sie ihn konvertieren. Bei der Konvertierung sind einige Punkte zu berücksichtigen.

- `&&` wird zu `and`
- `ip.addr` wird zu `host`, wenn es sich um einen einzigen Host handelt, oder zu **net**, wenn es sich um ein Netzwerk handelt.
- `ip.src` wird zu `src host`, wenn es sich um einen einzigen Host handelt, oder zu `src net`, wenn es sich um ein Netzwerk handelt.
- `ip.dst` wird zu `dst host`, wenn es sich um einen einzigen Host handelt, oder zu `dst net`, wenn es sich um ein Netzwerk handelt.
- Verwenden Sie beim Auflisten eines Netzwerks die CIDR-Notation (d. h., 10.10.10.0/24).
- `||` wird zu `or`
- `!` wird zu `not`
- Mehrere Regeln müssen mit `and` verknüpft werden.

Im Handbuch für TCPDump finden Sie ebenfalls Beispiele für Filter und Zeichenfolgen, die verwendet werden können:
http://www.tcpdump.org/tcpdump_man.html

Darüber hinaus stellt die folgende Website eine hervorragende Referenz für BPF-Paketfilter dar:
http://biot.com/capstats/bpf.html

Achtung: Beim Erfassen von Paketen, die `vlan`-Tags aufweisen, funktionieren die oben genannten BPF-Standardfilter möglicherweise nicht. Wenn Sie beispielsweise `not (udp port 123)` zum Filtern des mit `vlan`-Tags versehenen NTP-Datenverkehrs auf UDP-Port 123 verwenden, funktioniert der Filter nicht. Dies liegt daran, dass der BPF-Filtermechanismus einfach ist und keine Protokolle berücksichtigt, auf die nicht in der Regel verwiesen wurde. Daher sucht das Betriebssystem, das den BPF-Filter ausführt, die `udp port`-Werte an dem Byteoffset, der in einem Standard-Ethernet/UDP-Paket gelten würde. Jedoch verschieben die optionalen, mit `vlan`-Tags versehenen Felder im Ethernet-Header diese Werte um 4 Byte, sodass die BPF-Filterregel fehlschlägt. Um dieses Problem zu beheben, müssen Sie den BPF-Filter wie folgt ändern: `not (vlan and udp port 123)`.

(Optional) Konfigurieren eines Decoders zur Datenerfassung für alle Arten von Netzwerkschnittstellen

Mit dem Adapter `packet_mmap_,ALL` können Daten über alle Arten von Netzwerkschnittstellen gleichzeitig erfasst werden. Dazu gehören beispielsweise physikalische Netzwerkschnittstellen über verschiedene Medientypen und Tunnelschnittstellen.

Das Standardverhalten des Adapters `ALL` ist es, Daten von allen Schnittstellen aus dem System zu erfassen, mit Ausnahme der hartcodierten Standards von `lo`, `eth0` und `em1`.

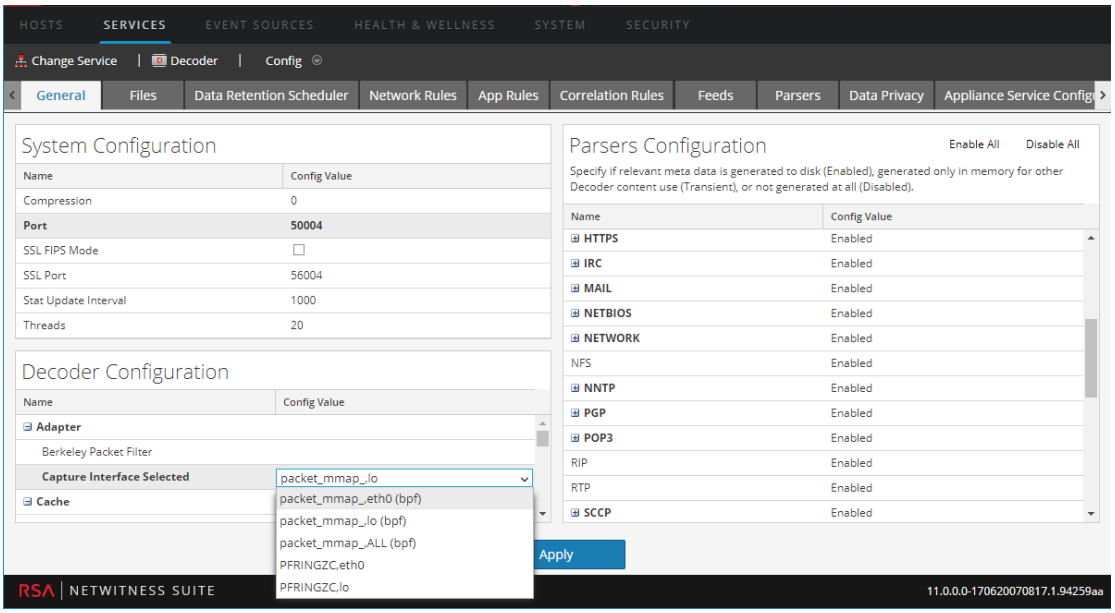
In NetWitness Suite 11.0 können Sie jede Teilmenge der Erfassungsschnittstellen auswählen, indem Sie den Decoder-Konfigurations-Node `/decoder/config/capture.device.params` so bearbeiten, dass er einen Parameter `interfaces=` einschließt. Der Parameter `interfaces` enthält eine kommagetrennte Liste von Schnittstellen, die für die Erfassung verwendet werden. Es werden nicht alle Schnittstellen für die Erfassung verwendet, sondern nur die angegebenen Schnittstellen.

Wenn Sie zum Beispiel erzwingen möchten, dass Daten auf Schnittstellen `em1`, `em2` und `em4` erfasst werden und dass `em3` ignoriert wird, können Sie den Adapter `packet_mmap_,ALL` auswählen und dann diese Zeile zu `capture.device.params` hinzufügen:`interfaces=em1,em2,em4`

Hinweis: Wenn Sie den Parameter `interfaces` verwenden, um `eth0`, `lo` oder `em1` auszuwählen, wird das Standardverhalten außer Kraft gesetzt, das darin besteht, den Datenverkehr von diesen Ports zu ignorieren.

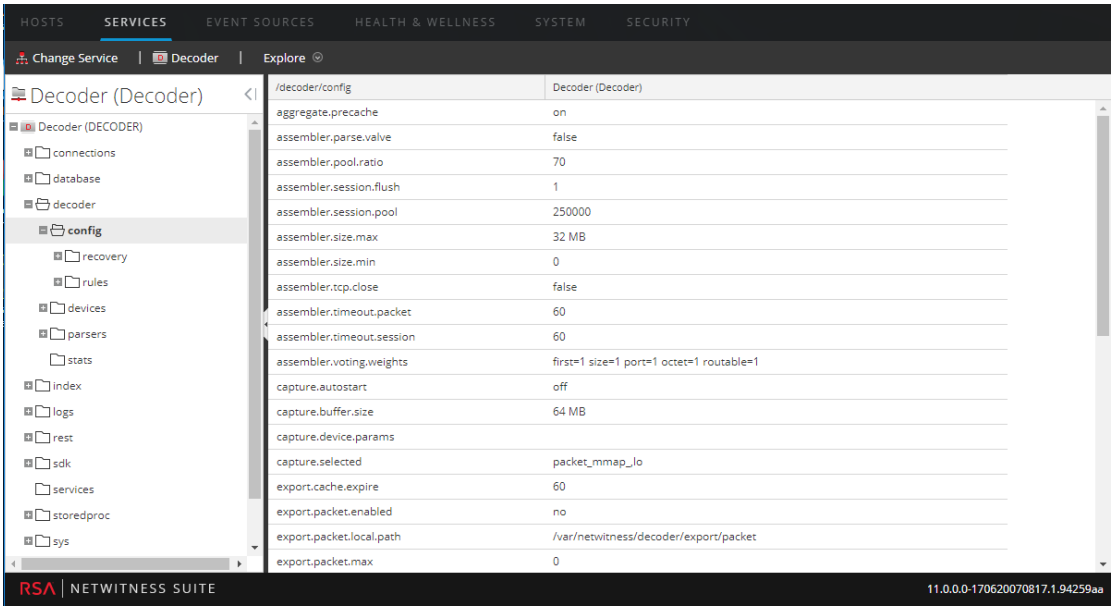
Konfigurieren des Adapters `packet_mmap_,ALL` zur Erfassung von angegebenen Schnittstellen anstatt von allen Schnittstellen:

1. Wählen Sie in der **Ansicht „Administration Services“** den Decoder-Service und  **> Ansicht > Konfiguration** aus.
2. Legen Sie in der **Ansicht „Service-Konfiguration“** die Option **Ausgewählte Erfassungsschnittstelle** auf den Adapter `packet_mmap_,ALL` fest.

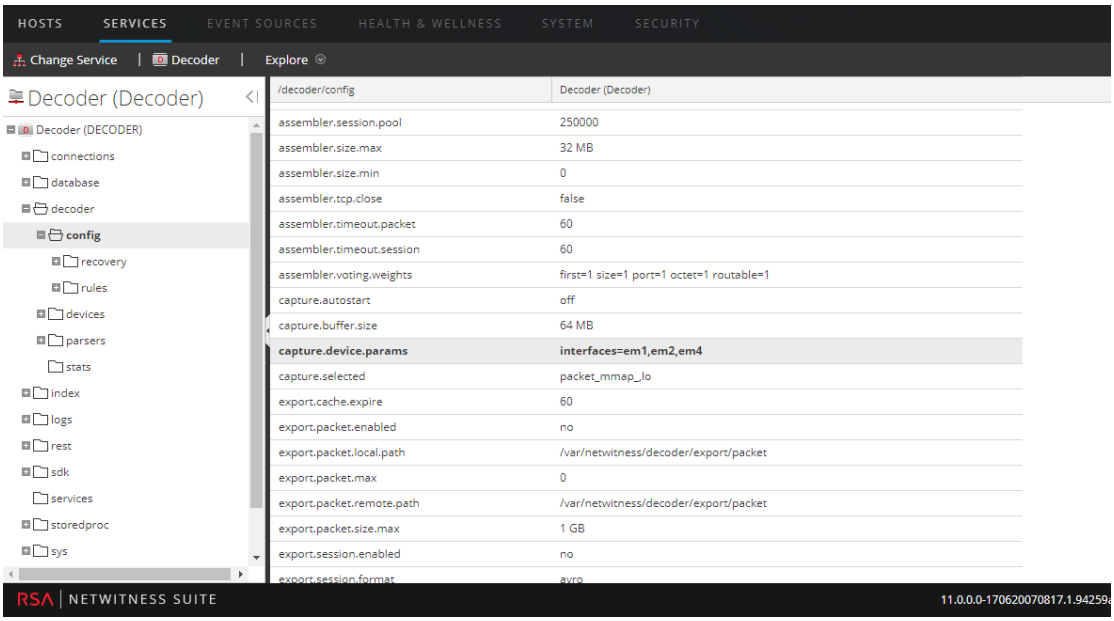


3. Wechseln Sie zur Ansicht zum Durchsuchen zu einem Service, indem Sie auf **Konfigurieren** in der Symbolleiste klicken, und wählen Sie **Durchsuchen** in der Drop-down-Liste aus.

4. Wählen Sie in der Ansicht zum Durchsuchen zu einem Service die Option **Decoder** > **Konfigurieren** aus.



5. Klicken Sie in die Spalte „Werte“ neben `capture.device.params`, geben Sie `interfaces=em1,em2,em4` ein und drücken Sie die **EINGABETASTE**.



Die Änderung tritt sofort in Kraft; nur der Datenverkehr auf den Schnittstellen `em1`, `em2` und `em4` wird erfasst.

(Optional) Beibehalten von VLAN-Tags bei der Nutzung der Paket-MMAP-Erfassungsschnittstelle

Beim Erfassen von Datenverkehr, der VLAN-Tags enthält, müssen Sie die Paket-MMAP-Erfassungsschnittstelle möglicherweise so konfigurieren, dass die VLAN-Tags in den Paketen beibehalten werden (VLAN-Korrektur). Standardmäßig entfernt die Netzwerkerfassungshardware die Tags. Mit der Durchführung dieses Verfahrens werden die Tags in den Paketen beibehalten und die Tag-Werte werden zur weiteren Analyse in VLAN-Metadaten analysiert.

Es gibt zwei Mechanismen für die Aktivierung der VLAN-Korrektur.

- Option 1: Stellen Sie `vlan-fix=true` innerhalb von `capture.device.params` ein. Diese Option führt die VLAN-Korrektur für den gesamten in den Decoder eingehenden Datenverkehr durch. Diese Option ist für die meisten Fälle geeignet, da angenommen wird, dass der gesamte Datenverkehr mit VLAN-Tags versehen ist. Dieses Verfahren funktioniert sowohl im Einzel-Schnittstellen-Modus als auch im Alle-Schnittstellen-Modus. Diese Option setzt die Einstellungen für VLAN-Korrektur auf einzelnen Schnittstellen außer Kraft. Auch bei Schnittstellen, die nicht dafür konfiguriert sind, VLAN-Korrekturen auszuführen, wird die Funktion aktiviert sein.
- Option 2: Verwenden Sie den Parameter `interfaces` in `capture.device.params` pro Gerät. Der Parameter `interfaces` akzeptiert eine kommagetrennte Liste der Namen der Schnittstellen, auf denen Pakete erfasst werden sollen. Indem Sie `:vlan` einem Schnittstellennamen hinzufügen, können Sie die VLAN-Korrektur auf einzelnen Schnittstellen aktivieren. Wenn das Suffix `:vlan` dem Schnittstellennamen nicht hinzugefügt wird, wird bei ihr die VLAN-Korrektur nicht ausgeführt.

Nach der Bearbeitung dieses Parameters müssen Sie die Erfassung auf dem Decoder erneut starten, damit die Änderungen an `capture.device.params` wirksam werden.

Dies sind `vlan`-Beispiele für beide Optionen. Wenn Sie mehrere Einstellungen für `capture.device.params` übergeben müssen, verwenden Sie die folgende Syntax. Beachten Sie, dass Anführungszeichen für Werte mit Leerzeichen erforderlich sind, siehe *Tuningleitfaden für die Core-Datenbank*.

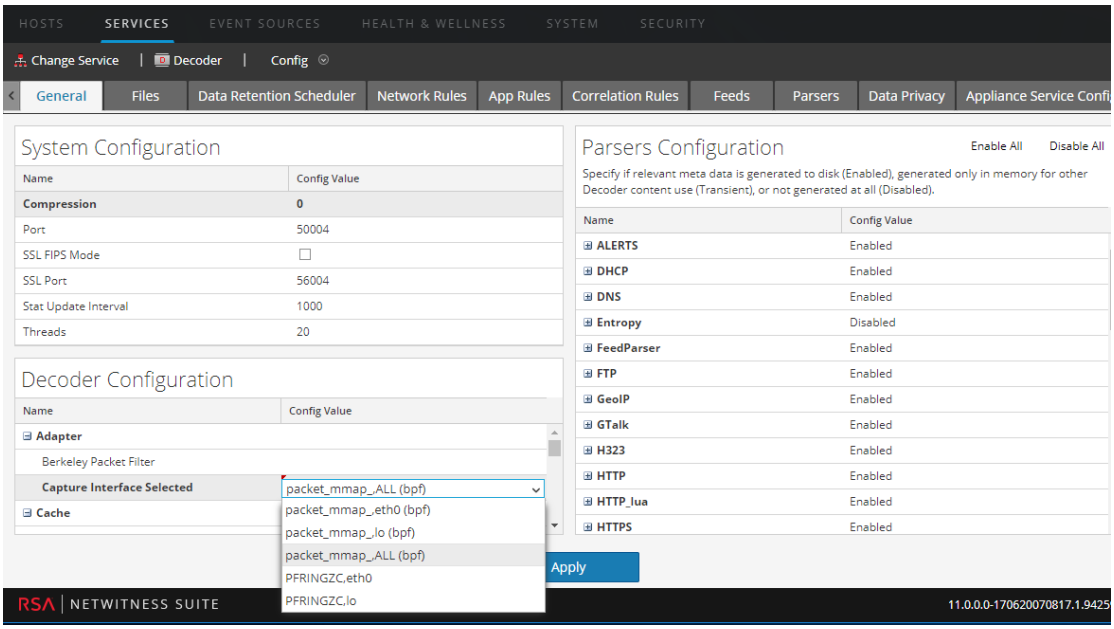
```
name1="value1" name2="value2".
```

Parameter	Wert	Wirkung
`capture.device.params`	`vlan-fix=true`	VLAN-Korrektur wird immer auf allen Schnittstellen durchgeführt. Der Standardwert ist `vlan-fix=false`.

Parameter	Wert	Wirkung
`capture.device.params`	`interfaces=eth0:vlan,eth1`	VLAN-Korrektur wird nur auf erfassten Datenverkehr auf `eth0`-Schnittstelle durchgeführt.
`capture.device.params`	`interfaces=eth0:vlan,eth1 vlan-fix=true`	VLAN-Korrektur wird immer durchgeführt, weil die Einstellung `vlan-fix` die Schnittstelleneinstellung außer Kraft setzt.

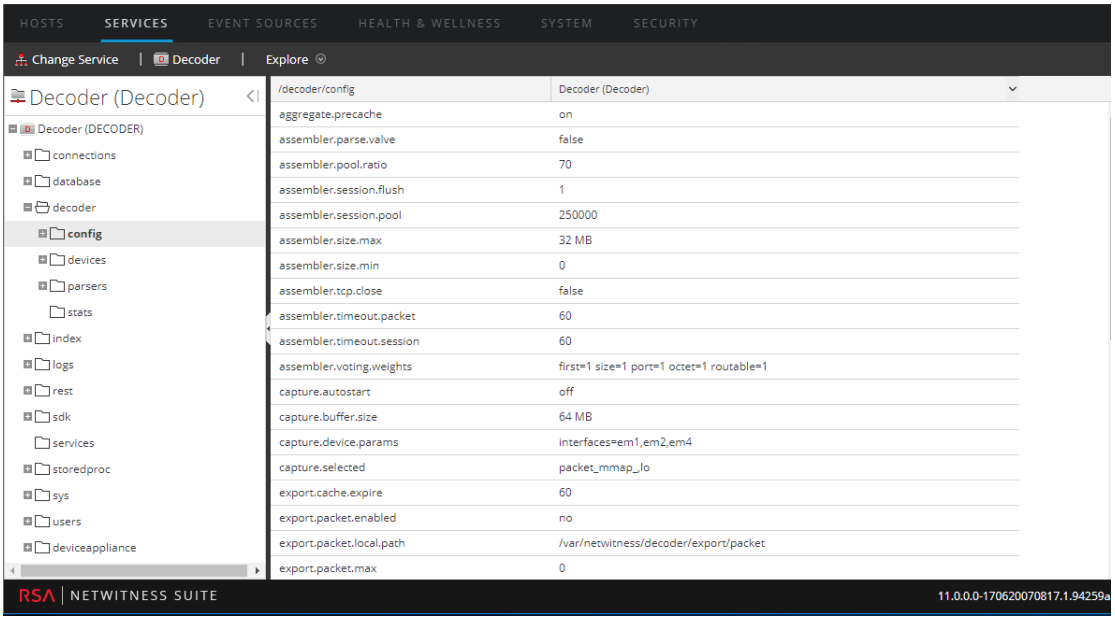
Konfigurieren des `packet_mmap_`-Adapters, um die VLAN-Tags in Paketen beizubehalten:

1. Wählen Sie in der **Ansicht „Administration Services“** den Decoder-Service und  **> Ansicht > Konfiguration** aus.
2. Legen Sie in der **Ansicht „Service-Konfiguration“** die Option **Ausgewählte Erfassungsschnittstelle** auf den Adapter `packet_mmap_,ALL` fest.



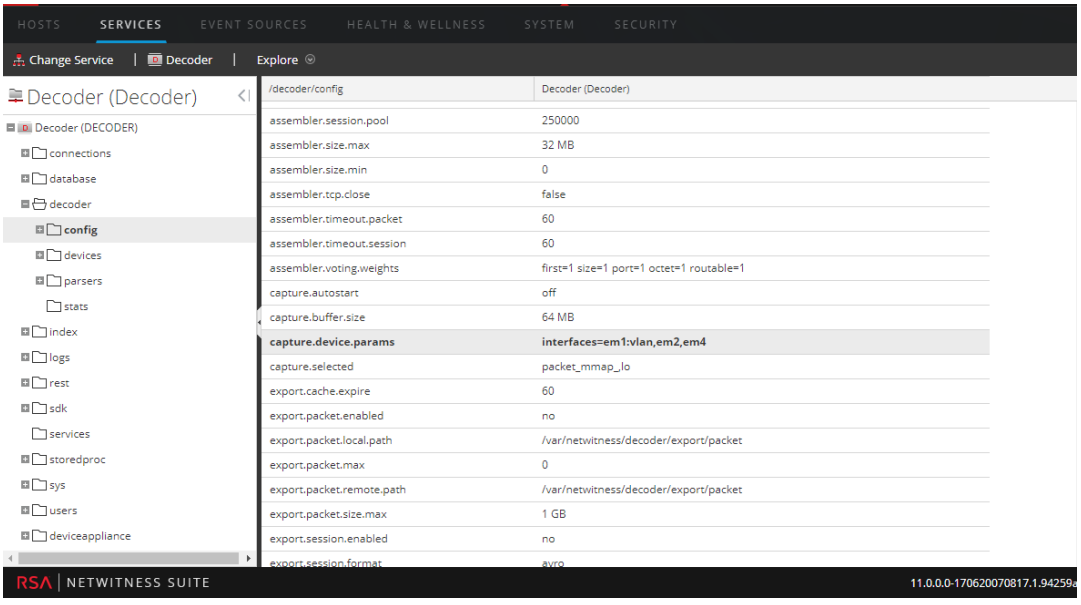
3. Wechseln Sie zur Ansicht zum Durchsuchen zu einem Service, indem Sie auf **Konfigurieren** in der Symbolleiste klicken, und wählen Sie **Durchsuchen** in der Drop-down-Liste aus.

4. Wählen Sie in der Ansicht zum Durchsuchen zu einem Service den Eintrag **Decoder** > **Konfigurieren** aus.



5. Klicken Sie in der Spalte „Werte“ neben `capture.device.params` und führen Sie einen der folgenden Schritte aus:

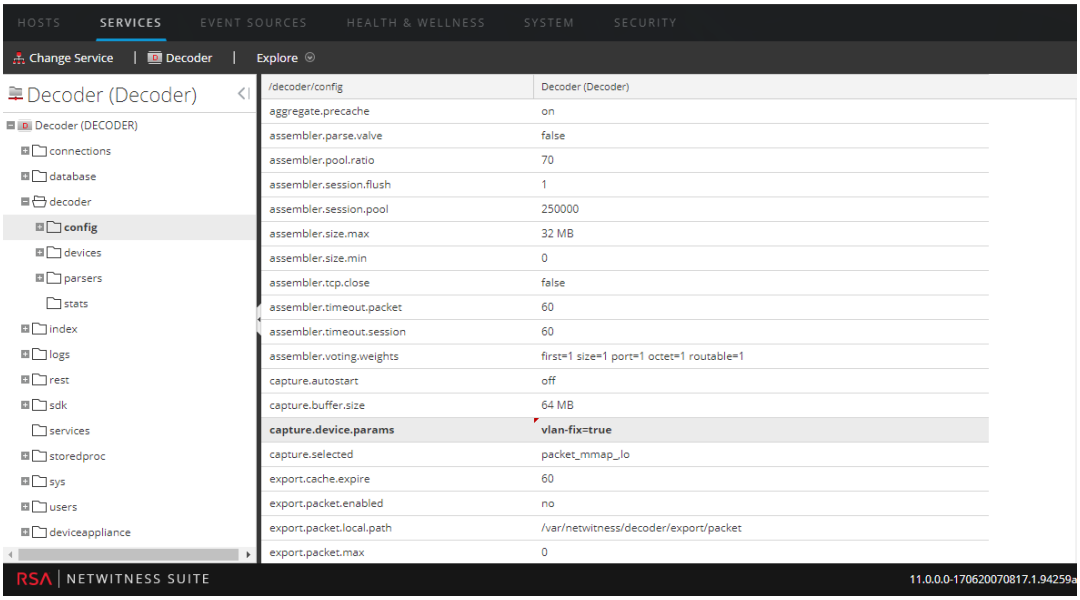
   - Zum Beibehalten von VLAN-Tags auf einer Schnittstelle in der Schnittstellenliste, fügen Sie **`:vlan`** nach dem Namen der Schnittstelle hinzu und drücken Sie die **EINGABETASTE**. Beispielsweise gibt dies an, dass VLAN-Tags auf `em1` beibehalten werden, nicht aber auf `em2` und `em4`:
     `interfaces=em1:vlan,em2,em4`



Die Änderung wird sofort wirksam. Nur für den Datenverkehr auf `em1` werden die VLAN-Tags beibehalten.

- Zum Beibehalten der VLAN-Tags auf allen Schnittstellen, geben Sie Folgendes ein und drücken Sie die **EINGABETASTE**:

  `vlan-fix=true`.

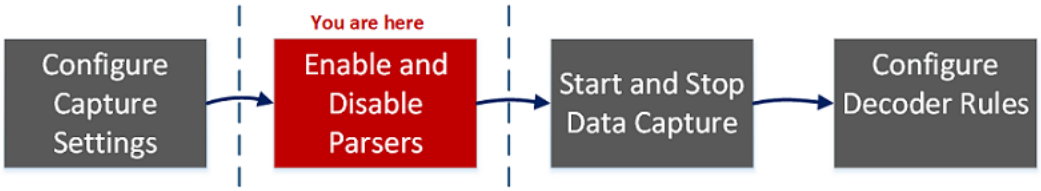


Die Änderung wird sofort wirksam. VLAN-Tags werden auf allen Erfassungsschnittstellen beibehalten.

Aktivieren und Deaktivieren von Parsern und Protokollparsern

Administratoren können sehen, welche Parser von Live heruntergeladen und auf einem Decoder oder Log Decoder bereitgestellt wurden. Sie können außerdem sehen, welche davon aktiviert wurden und Parser und Protokollparser aktivieren oder deaktivieren.

Auf der folgenden Abbildung sind häufig verwendete Einstellungen auf einem Decoder zu sehen. Eine grundlegende, schnell durchführbare Einrichtung mit den wichtigsten Schritten finden Sie in Decoder und Log Decoder – Schnelleinrichtung.



Sie sollten nur benötigte Parser herunterladen und bereitstellen, denn:

- Eine steigende Anzahl an bereitgestellten Parsern hat Auswirkungen auf die Performance.
- Je mehr Parser bereitgestellt werden, desto mehr Metadaten werden erstellt, was Auswirkungen auf die Datenaufbewahrung hat.
- Wenn keine zusätzlichen (unnötigen) Protokollparser bereitgestellt werden, reduziert dies die Wahrscheinlichkeit falsch identifizierter Meldungen.

Der Bereich „Parserkonfiguration“ bietet eine Möglichkeit zur Auswahl des auf dem Decoder zu verwendenden Parsers. Innerhalb einiger Parser können Sie auch die Metadaten, die der Parser erstellt, konfigurieren. Optionen im Bereich „Parserkonfiguration“

Option	Beschreibung
Alle aktivieren **Alle deaktivieren**	Mithilfe dieser Optionen können Sie schnell entweder alle oder keine Parser auswählen.
Name	Die Namen der für den Decoder verfügbaren Parser. Ein Pluszeichen gibt an, dass die vom Parser erzeugten Metadaten konfiguriert werden können. Durch Klicken auf das Pluszeichen werden die Metadaten angezeigt, die der Parser erstellen kann.

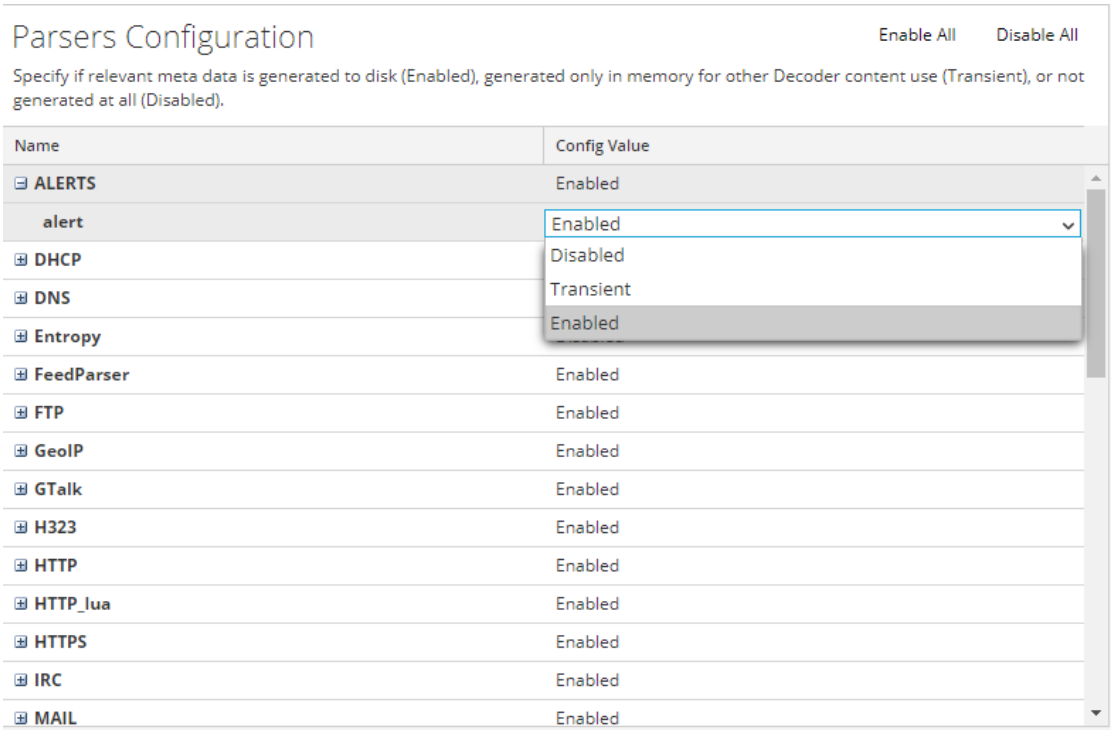
Option	Beschreibung
Konfigurationswert	In einer Drop-down-Liste werden die Einstellungen für den Parser oder die Metadaten in **Aktiviert**, **Deaktiviert** oder **Vorübergehend** geändert. • Wenn **Aktiviert** ausgewählt ist, verwendet der Decoder den Parser zum Filtern des Datenverkehrs. • Wenn **Vorübergehend** ausgewählt ist, verwendet der Decoder den Parser zum Filtern des Datenverkehrs und die erzeugten Metadaten werden nicht auf dem Datenträger gespeichert. Die vorübergehenden Metadaten sind für weitere Inhalte (d. h. Parser, Feeds und Anwendungsregeln) im Speicher auf diesem Decoder verfügbar. Damit können Administratoren bestimmte Daten schützen. Dies geschieht in der Regel im Rahmen eines Datenschutzplans (siehe den *Leitfaden zum Datenschutzmanagement*). • Wenn **Deaktiviert** ausgewählt ist, verwendet der Decoder den Parser nicht. Wenn die erzeugten Metadaten für den Parser konfigurierbar sind, werden durch Klicken auf das Pluszeichen zum Erweitern des Parsers konfigurierbare Metaschlüssel angezeigt. In derselben Drop-down-Liste werden die Metaschlüssel ausgewählt, die der Parser erstellt.

Hinweis: Für einen Log Decoder benötigen Sie vorher von Live bereitgestellte Protokollparser. Weitere Informationen finden Sie im Thema **Suchen und Bereitstellen von Live-Ressourcen** im Leitfaden zum *Live-Servicemanagement*.Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

So aktivieren oder deaktivieren Sie einen Parser oder rufen den Status für einzelne Parser auf:

1. Navigieren Sie zu **ADMIN** > **Services**.
2. Wählen Sie in der **Ansicht „Administration Services“** einen Log Decoder oder einen Decoder und anschließend  **> Ansicht** > **Konfiguration** aus.

3. Suchen Sie im Bereich **Parserkonfiguration** nach dem Decoder-Parser oder dem Log Decoder-Ereignisquellenparser.



4. In der Spalte **Konfigurationswert** finden Sie den aktuellen Status des Parsers.

   Sie können den Status der einzelnen Parser aktualisieren, indem Sie seinen **Konfigurationswert** auswählen und dann **Deaktiviert**, **Vorübergehend** oder **Aktiviert** im Drop-down-Menü auswählen. Alternativ können Sie **Alle aktivieren** oder **Alle deaktivieren** auswählen, um den Status aller Protokollparser gleichzeitig zu ändern.

5. Klicken Sie auf **Anwenden**.

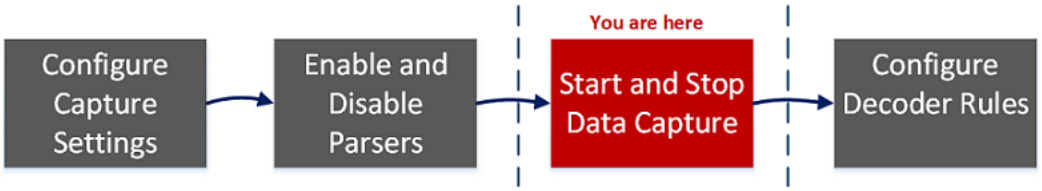
Beachten Sie, dass beim Klicken auf **Anwenden** alle Parser neu in NetWitness Suite geladen werden. Der Status für jeden Parser wird auf Grundlage Ihrer Auswahl aktualisiert.

Starten und Beenden der Datenerfassung

Beim Starten eines Decoder werden automatisch Daten aggregiert, wenn die Funktion **Automatischen Start erfassen** aktiviert ist. Wenn der automatische Start nicht aktiviert ist, können Sie die Datenerfassung manuell starten oder beenden.

Hinweis: In den Erfassungskonfigurationseinstellungen in der Ansicht „Service-Konfiguration“ für einen Decoder wird festgelegt, ob „Erfassung-Autostart“ aktiviert ist.

Auf der folgenden Abbildung sind häufig verwendete Einstellungen auf einem Decoder zu sehen. Eine grundlegende, schnell durchführbare Einrichtung mit den wichtigsten Schritten finden Sie in Decoder und Log Decoder – Schnelleinrichtung. Möglicherweise ist es sinnvoll, die Erfassung zu einem anderen Zeitpunkt zu beenden und zu starten, etwa bevor Sie den Service deaktivieren.



So starten bzw. beenden Sie die Erfassung:

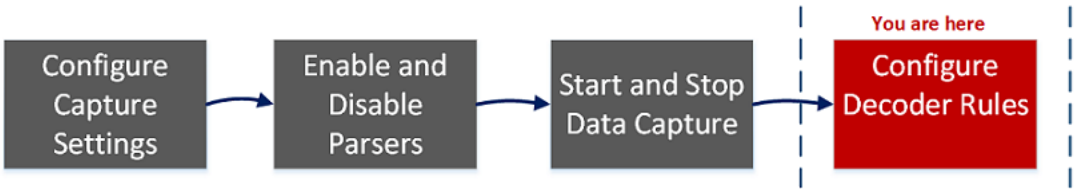
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht **Administration > Services** einen Decoder- oder Log Decoder-Service und dann > **Ansicht > System** aus.
3. Klicken Sie auf der Symbolleiste auf **Erfassung starten**.
   Wenn es sich bei dem Service um einen Decoder handelt, beginnt dieser mit der Erfassung von Paketen. Wenn es sich bei dem Service um einen Log Decoder handelt, beginnt dieser mit der Erfassung von Protokollen.
   Wenn die Paket- bzw. Protokollerfassung ausgeführt wird, ändert sich die Option in der Symbolleiste zu **Erfassung beenden** und die Option zum Hochladen einer Datei ist nicht verfügbar.
4. Wenn ein Decoder die Erfassung des Datenverkehrs beenden soll, klicken Sie auf **Erfassung beenden**.
   Die Erfassung der Pakete bzw. Protokolle wird beendet und die Option zum Hochladen einer Datei zum Service ist wieder verfügbar.

Hinweis: Wenn Sie den Log Decoder-Service beenden, während die Erfassung ausgeführt wird, werden alle Ereignisse, die sich zu diesem Zeitpunkt im Log Decoder-Arbeitsspeicher befinden, verarbeitet und persistent gemacht. Sollte ein Problem auftreten, das ein schnelles Herunterfahren des Service erforderlich macht, verwenden Sie die Ansicht „Serviceübersicht“, um die Erfassung zu beenden (**/decoder stop**). Übergeben Sie die Parameter ***flush=false***, bevor Sie den Log Decoder-Service beenden. Weitere Informationen finden Sie im Thema zur „Serviceübersicht“-Ansicht im *Leitfaden für die ersten Schritte mit Hosts und Services*.

Konfigurieren von Decoder-Regeln

In diesem Thema werden Verfahren zur Erstellung und Verwaltung von Regeln für die Erfassung von Decoder- oder Log Decoder-Datenverkehr auf der Registerkarte „Regeln“ in der Ansicht „Service-Konfiguration“ vorgestellt. Ansicht „Services-Konfiguration“ – Registerkarte „Regeln“ enthält Details zu den Optionen auf der Registerkarte „Regeln“.

Auf der folgenden Abbildung sind häufig verwendete Einstellungen auf einem Decoder zu sehen. Eine grundlegende, schnell durchführbare Einrichtung mit den wichtigsten Schritten finden Sie in Decoder und Log Decoder – Schnelleinrichtung.



Erfassungsregeln können Sitzungen oder Protokollen Warnmeldungen oder kontextbezogene Informationen hinzufügen. Sie können außerdem definieren, welche Daten von einem Decoder oder Log Decoder ausgefiltert werden. Regeln werden für bestimmte Metadatenmuster erstellt, die zu vordefinierten Aktionen führen, wenn Übereinstimmungen gefunden werden. Um zum Beispiel allen Datenverkehr beizubehalten, der bestimmten Kriterien entspricht, aber allen anderen Datenverkehr zu verwerfen, können Sie eine Regel zur Ausführung der notwendigen Aktionen definieren. Wenn sie angewendet werden, wirken sich Regeln sowohl auf das Importieren von Paketerfassungsdateien als auch auf die Live-Netzwerkerfassung aus.

In Richtlinien für Regeln und Abfragen finden Sie Richtlinien, die bei der Erstellung beliebiger Abfragen und Regelbedingungen in NetWitness Suite Core-Services befolgt werden müssen.

Standardmäßig sind keine Regeln definiert, wenn Sie NetWitness Suite erstmals installieren. Bis Regeln festgelegt werden, werden die Pakete nicht gefiltert. Sie können die neuesten Regeln von Live bereitstellen. Sie können drei Regeltypen definieren: Netzwerkregeln, Anwendungsregeln und Korrelationsregeln

- Netzwerkregeln werden auf Paketebene angewendet und bestehen aus Regeln von Ebene 2, Ebene 3 und Ebene 4. Mehrere Regeln können auf den Decoder angewendet werden. Regeln können auf mehrere Ebenen angewendet werden (zum Beispiel, wenn eine Netzwerkregel bestimmte Ports für eine bestimmte IP-Adresse herausfiltert). Netzwerkregeln sind nur auf Packet Decoders verfügbar.
- Anwendungsregeln werden auf der Sitzungsebene angewendet. Wenn die erste Regel keine Übereinstimmung ergibt, versucht der Decoder die nächste Regel auf der Liste, bis eine Übereinstimmung gefunden wurde.

- Die Korrelationsregeln werden für ein konfigurierbares gleitendes Zeitfenster angewendet. Wenn eine Übereinstimmung gefunden wird, erstellt der Service eine neue Supersitzung, die andere Sitzungen identifiziert, die mit der Regel übereinstimmen, und erstellt dann eine Sitzungsliste zur Analyse.

Die beiden häufigsten Anwendungen von Regeln sind:

- Eine Warnmeldung auslösen und damit einen angepassten Warnmeldungsmetawert erstellen, wenn bestimmte Bedingungen erfüllt sind
- Herausfiltern bestimmter Arten von Datenverkehr, die der Analyse der Daten keinen Wert hinzufügen

Gruppen von Erfassungsregeln bilden Regelsätze, die Sie importieren und exportieren können. Diese Funktion ermöglicht die Verwendung mehrerer Regelsätze für verschiedene Szenarien. Sie können den exportierten Regelsatz in Form einer .nwr-Datei in andere NetWitness Suite-Services importieren und so die Bereitstellung und Konfiguration mehrerer Services vereinfachen.

Regelverarbeitung

Diese Prinzipien bestimmen die Verarbeitung von Erfassungsregeln:

- Mehrere Regeln können auf den Decoder angewendet werden.
- Erfassungsregeln werden eine nach der anderen aufeinanderfolgend ausgeführt.
- Die Regelverarbeitung wird beendet, wenn alle Regeln verarbeitet wurden oder nachdem eine Regel verarbeitet wurde, die konfiguriert wurde, um die Regelverarbeitung zu beenden.
- Eine Standardregel kann verwendet werden, um allen Datenverkehr entweder einzuschließen oder auszuschließen, der nicht von anderen Regeln ausgewählt wird. Eine Standardregel muss, wenn sie verwendet wird, immer ans Ende einer Regelliste gestellt werden. Andernfalls wird die Regelverarbeitung beendet, sobald die Standardregel evaluiert wird, da definitionsgemäß der gesamte Datenverkehr von der Standardregel ausgewählt wird.
- Wenn die Regelverarbeitung beendet wird, wird die Sitzung unter Verwendung der konfigurierten Sitzungsoptionen und Debugoptionen gespeichert.

Regelkonfiguration

Richtlinien für Regeln und Abfragen

Alle Abfragen und Regelbedingungen in RSA NetWitness Core-Services müssen den folgenden Richtlinien entsprechen:

Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlen, MAC-Adressen oder IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden.

- `extension = 'torrent'`
- `time='2015-jan-01 00:00:00'`
- `service=80`
- `ip.src = 192.168.0.1`

Hinweis: Das Leerzeichen rechts und links neben einem Operator ist optional. Sie können eine Regel zum Beispiel als `service=80` oder `service = 80` eingeben.

Beispiele für Regeln

In der folgenden Tabelle sind Beispiele für Regelbedingungen. Sie können Regelbedingungen für Protokollaufbewahrungssammlungen in einem Archiver und für Anwendungs-, Netzwerk- und Korrelationsregeln auf einen Decoder, Log Decoder oder Concentrator verwenden. Regelbedingungen werden auch in allen `WHERE` -Klauseln in allen Core-Datenbankabfragen verwendet.

Detaillierte Informationen zur Regelsyntax in der NetWitness Suite finden Sie unter „`WHERE`-Klauseln“ im Abschnitt „Abfragen“ des *Core-Datenbank-Tuning-Leitfadens*.

Name der Regel	Bedingung
ComplianceDevices	`device.group='PCI Devices' || device.group='HIPPA Devices'`
HighValueWindows	`device.group='Windows Compliance'`
MediumValueWindows	`device.type='winevent_nic' && msg.id='security_4624_security'`
LowValueWinLogs	`device.type='winevent_nic' && msg.id='security_`

	`4648_security'`
LowValueProxyLogs	`device.class='proxy' && msg.id='antivirus_ license_expired'`
GeneralWindows	`device.type='winevent_nic'`

Ungültige Regeln

NetWitness Suite nutzt einen Regel-Parser, der die gültige Syntax für Regeln und Abfragen streng definiert. Wenn ein Core-Service auf ungültige Syntax trifft, schreibt er eine Warnmeldung in die Protokolle der NetWitness Suite und weist darin auf den Fehler hin.

Hinweis: NetWitness Suite 11.0 bietet keine Unterstützung für das Parsing von älteren Syntaxregeln (etwa von NetWitness Suite 10.6). Nach der Aktualisierung auf NetWitness Suite 11.0 werden Regeln mit ungültiger Syntax auf der Benutzeroberfläche hervorgehoben und es werden keine Regeln angewendet, bis die ungültigen Regeln korrigiert sind. Der Regel-Editor bietet zusätzliche Kurzinformationen. Nachdem Sie die Regeln repariert haben, werden die Hervorhebungen nicht mehr angezeigt. Siehe Korrigieren von Regeln mit ungültiger Syntax.

In den `/decoder/config/rules/rule.errors` - und `/concentrator/config/rules/rule.errors` -Statistiken ist die Anzahl der Regeln mit Fehlern enthalten. Wenn `rule.errors` nicht null ist, erzeugt die NetWitness Suite eine Warnmeldung zu Integrität und Zustand und weist so darauf hin, dass die Regeln korrigiert werden müssen.

Allgemeine Richtlinien zur Syntax

- Literalwerte müssen in allen Textwerten in Anführungszeichen gesetzt werden. Beispiel: `username = 'user1'`
- Anführungszeichen können einfach oder doppelt sein, sie müssen aber übereinstimmen. Das bedeutet, dass Sie nicht mit einem einfachen Anführungszeichen beginnen und am Ende ein doppeltes Anführungszeichen setzen können.
- Wenn der Literalwert ein Anführungszeichen enthält, können Sie ein Escape-Zeichen voranstellen (umgekehrter Schrägstrich) oder ein anderes öffnendes Anführungszeichen verwenden. Beide der folgenden Beispiele sind gültig: `username = "User's"` , `username = 'User\'s'`

Im Folgenden sind gültige Syntaxregeln aufgeführt:

- Um einen umgekehrten Schrägstrich in einer Literalzeichenfolge zu verwenden, stellen Sie ihm einen zusätzlichen umgekehrten Schrägstrich als Escape-Zeichen voran: \
- Für alle Zeitwerte müssen Anführungszeichen für Datumsangaben im folgenden Format verwendet werden:
  `time = 'YYYY-MM-DD HH:MM:SS'`
- Alle Zeitwerte, die der Anzahl von Sekunden seit EPOCH (1. Januar 1970) entsprechen, müssen nicht in Anführungszeichen gesetzt werden.
  Beispiel: `time = 1448034064`
- **Alles** andere wird nicht in Anführungszeichen gesetzt: IP-Adressen, MAC-Adressen, Zahlen und so weiter. Beispiel: `service = 80 && ip.src = 192.168.1.1/16`

Regelerfassungssyntax

Erfassungsregeln vergleichen Felder mit Werten oder anderen Feldern. Das hier ist ein Beispiel für einen einfachen Ausdruck mit einem Metaschlüssel auf der linken Seite des Operators und einem Wert auf der rechten Seite davon.

```
ip.dst=192.168.1.1
```

Die Syntax ermöglicht einen Metaschlüssel auf der rechten Seite des Operators in Decodern und Log Decodern für Anwendungs- und Netzwerkregeln. Der Vergleich von Metaschlüsseln ist in der `where`-Klausel von Abfragen nicht relevant. Das hier ist ein Beispiel für einen einfachen Ausdruck mit einem Metaschlüssel auf der linken Seite des Operators und einem Metaschlüssel auf der rechten Seite davon.

```
ip.src=ip.dst
```

Regeln, die einen Metaschlüsselvergleich umfassen, unterstützen umbenannte Metaschlüssel. Wenn eine Regel einen Metaschlüssel abfragt, der umbenannt wurde, wird die Regel für den umbenannten Metaschlüssel analysiert. Wenn zum Beispiel der Metaschlüssel `ip_dst` in einer Regel verwendet wird, wird er transparent dem umbenannten Metaschlüssel zugeordnet: `ip.dst`. Vorhandene Regeln, die Originalschlüssel enthalten, führen zu Warnmeldungen, die Daten für den umbenannten Metaschlüssel enthalten.

Dies ist ein Beispiel für eine Regel, die Pakete findet, die dieselbe `ip.src`- und `ip.dst`-Adresse auf einem Decoder haben, und eine Warnmeldung auf dem Concentrator erzeugt.

```
alert=alert.id name=testRule8 rule="ip.src=ip.dst" order=38
```

Diese Regel würde einen Fehler erzeugen, da es sich bei `eth.src` und `ip.src` um nicht kompatible Formate handelt.

```
rule="eth.src=ip.src" name="testRule99" alert=alert.id
```

Werte können als diskrete Werte, als Wertebereich, als obere und untere Grenzwerte oder als Kombination dieser drei Möglichkeiten ausgedrückt werden. Sie können einen Größer-als- oder Kleiner-als-Vergleich erstellen und die Gleichheit oder Ungleichheit gegenüber einem Wertebereich oder einem oberen oder unteren Grenzwert testen.

`key 0-5` (ein Wertebereich)

`key = 0-u` entspricht `key >= 0` (obere Grenze, größer als oder gleich)

In der folgende Tabelle sind die Operatoren in Metaschlüsseln zusammengefasst.

Format des linken Operanden	Operator	Format des rechten Operanden	Beschreibung
Alle	=	kompatibel mit linkem Operanden	Gleichheitsoperator. Sie können auf der rechten Seite des Gleichheitsoperators Werte oder Metaschlüssel verwenden.
Alle	!=	kompatibel mit linkem Operanden	Ungleichheitsoperator. Sie können auf der rechten Seite des Ungleichheitsoperators Werte oder Metaschlüssel verwenden.
Alle	<	kompatibel mit linkem Operanden	Kleiner-als-Operator. Sie können auf der rechten Seite dieses Operators Werte oder Metaschlüssel verwenden.
Alle	<=	kompatibel mit linkem Operanden	Kleiner-als-oder-gleich-Operator. Sie können auf der rechten Seite dieses Operators Werte oder Metaschlüssel verwenden.
Alle	>	kompatibel mit linkem Operanden	Größer-als-Operator. Sie können auf der rechten Seite dieses Operators Werte oder Metaschlüssel verwenden.
Alle	>=	kompatibel mit linkem Operanden	Größer-als-oder-gleich-Operator. Sie können auf der rechten Seite dieses Operators Werte oder Metaschlüssel verwenden.

Format des linken Operanden	Operator	Format des rechten Operanden	Beschreibung
Text	`contains`	Text	Findet Werte, die den rechten Operanden enthalten. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden.
Text	`begins`	Text	Findet Werte, die mit dem rechten Operanden beginnen. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden.
Text	`ends`	Text	Findet Werte, die mit dem rechten Operanden enden. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden.
Text	`length`	Ganze Zahl	Findet Zeichenfolgen, die eine bestimmte Länge haben. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden.
Alle	`count`	Ganze Zahl	Findet Werte mit einer bestimmten Anzahl an Vorkommen. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden.
Alle	`ucount` und `unique`	Ganze Zahl	Findet eine Anzahl nur einmal vorkommender Werte. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden. Beispiel: Wenn die Ergebnisse Instanzen eines Metaschlüssels mit 5 eindeutigen Werten enthalten und 3 davon übereinstimmen, entspricht `ucount` der Zahl 6.

Format des linken Operanden	Operator	Format des rechten Operanden	Beschreibung
–	`exists`	Alle	Findet alle Werte für den Metaschlüssel. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden.
–	`!exists`	Alle	Findet alle Sitzungen, in denen der Metaschlüssel nicht vorkommt. Sie können auf der rechten Seite dieses Operators Metaschlüssel oder Werte verwenden.
Text	`regex`	Text	Findet Werte, die mit einem regulären Ausdruck übereinstimmen. Sie können auf der rechten Seite dieses Operators Werte verwenden.

In der folgende Tabelle sind andere Syntaxelemente, die in Regeln verwendet werden, zusammengefasst.

Syntaxelement	Beschreibung
*	Standardregel Wenn Sie einen Asterisk (*) als einziges Zeichen in einer Regel verwenden, wird diese Regel den gesamten Datenverkehr auswählen.
`u`	Obergrenze für einen Zeitbereich, IP-Adressen oder numerisch Formate. Beispiel: Die Syntax zum Auswählen aller TCP-Ports über 40000 wäre: `tcp.port = 40000-u`
`l`	Untergrenze für einen Zeitbereich, IP-Adressen oder numerisch Formate. Beispiel: Die Syntax zum Auswählen aller TCP-Ports unter 40.000 wäre: `tcp.port = l-40000`

Syntaxelement	Beschreibung
- (Querstrich)	Bezeichnet einen Bereich. Dies gilt nur für Zeitwerte, IP- oder MAC-Adressen oder numerische Werte. Trennen Sie den unteren vom oberen Grenzwert des Bereichs mit einem Bindestrich (-). Die Syntax zum Auswählen von TCP-Ports zwischen 25 und 443 wäre beispielsweise: `tcp.port = 25-443`
, (Komma)	Kennzeichnet eine Liste von Bereichen oder Werten oder Metaschlüssel. Einzelne Werte können genauso verwendet werden wie jede Kombination von Bereichen und oberen und unteren Grenzwerten. Einzelne Metaschlüssel können in einer Liste verwendet werden. Metaschlüssel und Literalwerte können nicht beide auf der rechten Seite eines Operators auftreten. Beispiel: Folgendes wäre eine gültige Syntax: `tcp.port = 1-10,25,110,143-225,40000-u`
( )	Gruppierungsoperator Ein Ausdruck kann in Klammern eingeschlossen werden, um einen neuen logischen Ausdruck zu erstellen. Beispiel: Der folgende Ausdruck würde Datenverkehr auf Port 80 nach/von 192.168.1.1 ODER Datenverkehr auf Port 443 nach/von 10.10.10.1 auswählen: `(ip.addr=192.168.1.1 && tcp.port=80) || (ip.addr=10.10.10.1 && tcp.port=443)`
~	Logischer NICHT-Operator, eine Negation eines Ausdrucks.
&&	Logischer UND-Operator, eine Konjunktion zweier Ausdrücke.
||	Logischer ODER-Operator, eine Disjunktion zweier Ausdrücke.

Konfigurieren von Erfassungsregeln

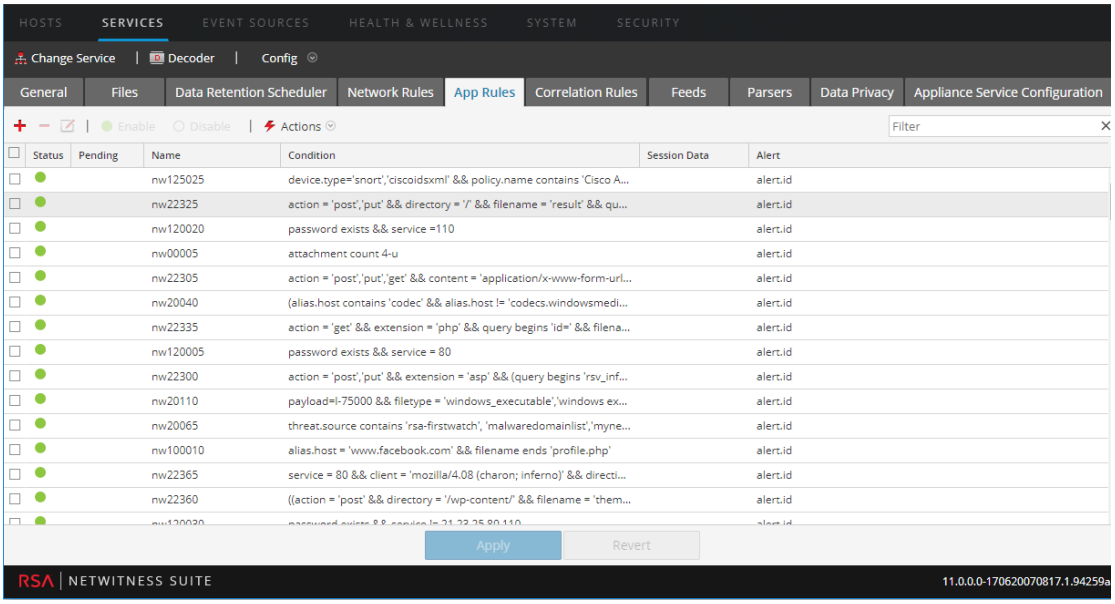
Die Decoder- und Log Decoder-Regeln können in der Ansicht „Service-Konfiguration“ bearbeitet werden. Während jeder Regeltyp (Netzwerk, Anwendung und Korrelation) seine eigene Registerkarte hat, sind die Funktionen für alle Regeltypen ähnlich. Sie können:

- Regeln hinzufügen, bearbeiten und löschen
- Regeln aktivieren und deaktivieren

- Die Ausführungsfolge von Regeln ändern
- Regeln aus einer Datei importieren
- Regeln in eine Datei exportieren
- Regeln auf einen anderen Service übertragen
- Änderungen zurücksetzen oder anwenden
- Eine der letzten zehn Regelkonfigurationen aus einem Snapshot wiederherstellen

Konfigurieren von Regeln auf den „Regeln“-Registerkarten

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht **Services** einen Decoder-Service und > **Ansicht** > **Konfigurieren** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** eine der „Regeln“-Registerkarten aus: Netzwerkregeln, App-Regeln oder Korrelationsregeln.
   Die Regelliste für den ausgewählten Regeltyp wird angezeigt.



Für jeden Regeltyp gibt es eine Liste mit etwas unterschiedlichen Spalten und unterschiedlichen Parametern. Mehrere grundlegende Richtlinien gelten für alle Regelmanagementaktivitäten:

- Die Regeln werden in der Reihenfolge ausgeführt, in der sie in der Liste angezeigt werden. Ziehen Sie die Regeln zur Änderung der Reihenfolge ihrer Ausführung per Drag-and-drop an die entsprechende Stelle in der Liste oder verwenden Sie die Kontextmenüoptionen, um die Regeln in der Liste anzuordnen.

- Klicken Sie zur Auswahl einer einzelnen Zeile auf die Zeile.
- Klicken Sie zur Auswahl einer Gruppe benachbarter Zeilen auf die erste Zeile, drücken Sie dann die Umschalttaste und klicken Sie auf die Zeile am Ende der Gruppe.
- Klicken Sie zur Auswahl mehrerer Zeilen, die nicht benachbart sind, auf die erste Zeile, halten Sie dann die Steuerungstaste gedrückt und klicken Sie auf die anderen Zeilen.
- Wenn Sie Regeln auf der Registerkarte „Regeln“ bearbeiten, müssen Sie die Änderungen an der Konfiguration anwenden, um sie zu aktivieren.
- Solange Änderungen nicht angewendet sind, können Sie Änderungen an der Liste verwerfen und zu den unbearbeiteten Regeln zurückkehren.
- Sobald Regeln angewendet sind, können Sie mithilfe der Option **Verlauf** im Menü **Aktionen** die letzten zehn Regelkonfigurationen wiederherstellen.

Führen Sie zum Hinzufügen einer Regel auf einer beliebigen „Regeln“-Registerkarte einen der folgenden Schritte aus:

- Klicken Sie auf  .
- Klicken Sie mit der rechten Maustaste auf eine Regel und wählen Sie **Oben einfügen** oder **Unten einfügen** aus dem Kontextmenü aus.
  Das Dialogfeld „Regel-Editor“ wird für diesen Regeltyp angezeigt.

So entfernen Sie eine Regel:

1. Wählen Sie auf einer der „Regeln“-Registerkarten die Regeln aus, die aus der Regelliste entfernt werden sollen.
2. Klicken Sie auf .
   Die ausgewählten Regeln werden aus der Liste entfernt, existieren jedoch noch im Service.

Bearbeiten einer Regel

1. Wählen Sie auf einer der „Regeln“-Registerkarte die Regeln aus, die Sie bearbeiten möchten.
2. Klicken Sie auf  oder klicken Sie doppelt auf die Zeile der Regel.
   Das Dialogfeld „Regel-Editor“ wird für diesen Regeltyp angezeigt.

So deaktivieren Sie eine Regel:

1. Wählen Sie auf einer der „Regeln“-Registerkarten die Regeln aus, die Sie deaktivieren möchten.

2. Klicken Sie auf Disable.

   Der Status in der Liste ändert sich zu „Deaktiviert“, aber die Regel ist im Service immer noch aktiviert.

So aktivieren Sie eine Regel:

1. Wählen Sie auf einer „Regeln“-Registerkarte die Regeln aus, die Sie aktivieren möchten.
2. Klicken Sie auf Enable.

   Der Status in der Liste ändert sich zu „Aktiviert“, aber die Regel ist im Service immer noch deaktiviert.

Importieren von Regeln aus einer Datei und Exportieren von Regeln

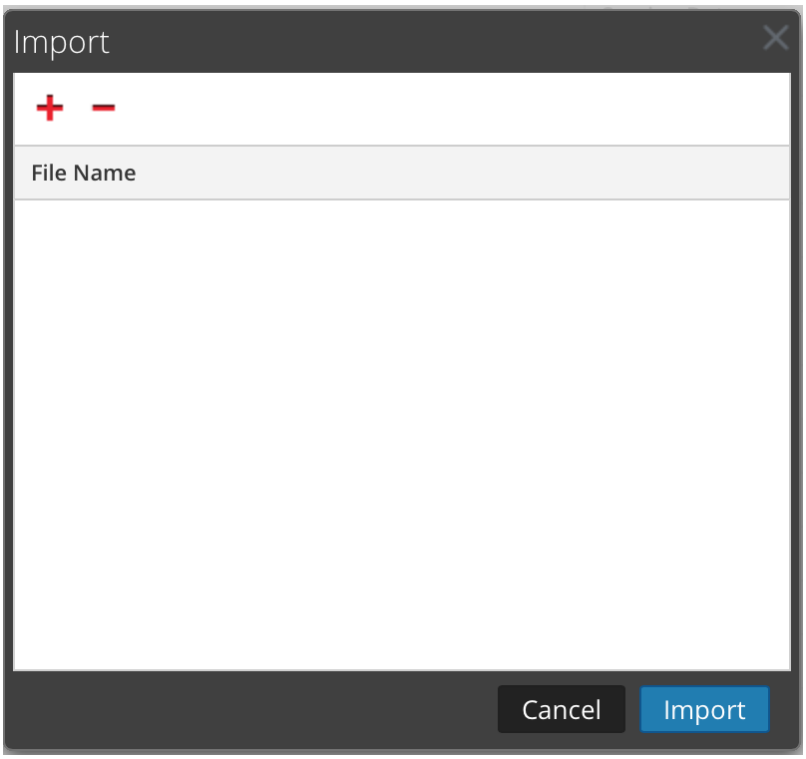
Sie können Netzwerk-, Anwendungs- und Korrelationsregeln auf einen Decoder aus einer Datei importieren, die Regeln desselben Typs enthält. Nachdem die Regeln importiert wurden, können Sie sie genauso bearbeiten und managen wie jede andere Regel.

Wenn Sie versuchen, eine Gruppe von Regeln zu importieren, prüft NetWitness Suite Administration den Typ der importierten Regeln. Wenn Sie erfolgreich sind, zeigt eine Meldung die Anzahl der importierten Regeln an. Wenn der Regeltyp vom Typ der aktiven Registerkarte abweicht, werden die Regeln nicht importiert. Sie müssen die Regeln dann unter der richtigen Registerkarte erneut importieren oder eine andere Datei zum Importieren auswählen.

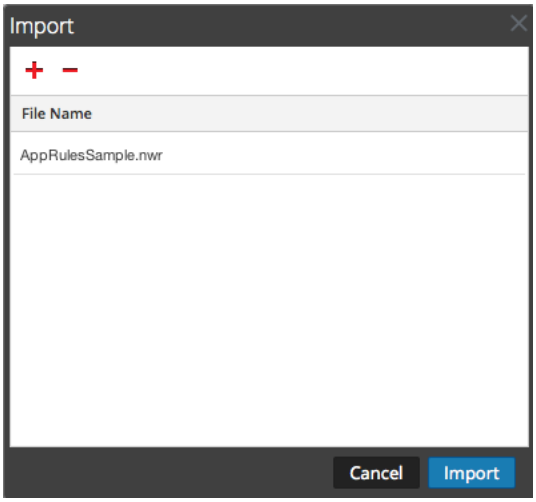
So importieren Sie Regeln in einen Service:

1. Wählen Sie auf einer „Regeln“-Registerkarte Actions > Import aus.

   Das Dialogfeld „Importieren“ wird angezeigt.



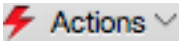
2. Klicken Sie auf + .
   Eine Ansicht der Verzeichnisstruktur wird angezeigt.
3. Wählen Sie eine oder mehrere NetWitness-Regeldateien (NWR) zum Importieren aus und klicken Sie auf **Öffnen**.
   Die Datei wird der Liste im Dialogfeld Importieren hinzugefügt.



4. Klicken Sie auf **Importieren**.
   Die Regeln werden in die Benutzeroberfläche importiert. Importierte Regeln haben eine rote Ecke in jeder bearbeiteten Spalte.

5. Bearbeiten Sie die Regeln oder verändern Sie ihre Reihenfolge nach Bedarf.
6. Klicken Sie zum Speichern der Regeln für den Service auf **Anwenden**.
   Die Regeln für den Service werden mit den Änderungen aktualisiert.

So exportieren Sie Regeln in eine Datei:

1. Zum Exportieren einer Teilmenge der Regeln wählen Sie die Regeln aus, die exportiert werden sollen.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie auf der Symbolleiste 

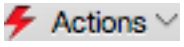
> Exportieren > Auswahl aus. Mit **Exportieren > Alle** werden alle Regeln in der Liste exportiert, auch wenn Sie eine Teilmenge für den Export ausgewählt haben.
   - Klicken Sie mit der rechten Maustaste auf die ausgewählten Regeln und wählen Sie **Exportauswahl** aus.

     Eine Eingabeaufforderung für den Dateinamen wird angezeigt.
3. Geben Sie den Dateinamen ein und klicken Sie auf **Exportieren**.
   Die .**nwr**-Datei wird heruntergeladen.

Regeln auf andere Services übertragen

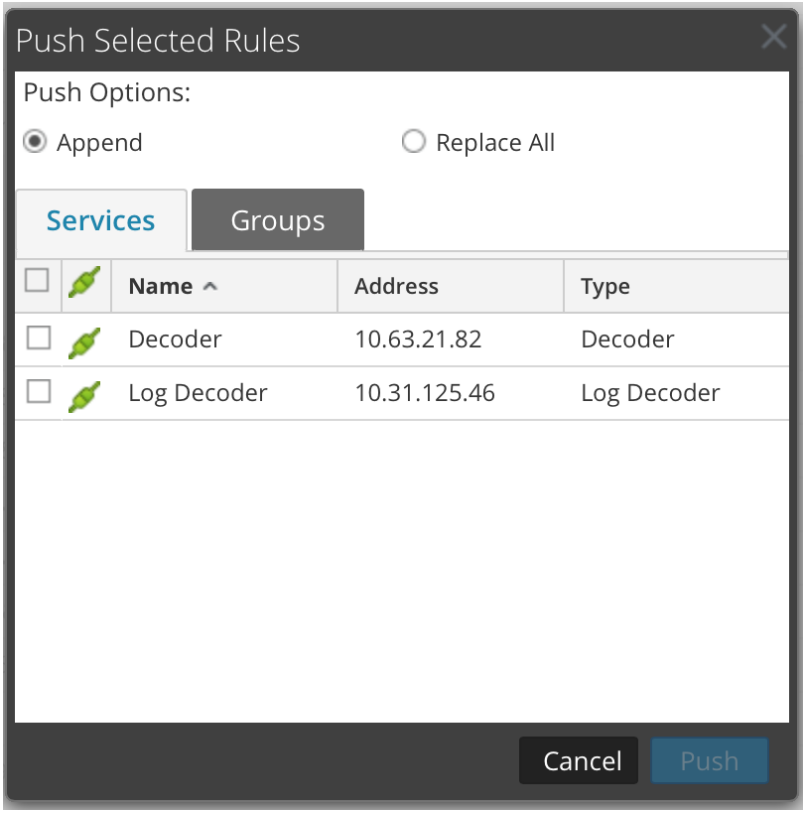
Sie können Regeln oder ausgewählte Regeln auf andere Services (Decoders oder Log Decoders) oder Servicegruppen anwenden (per Push übertragen). Wenn Sie alle Regeln per Push in andere Services übertragen, werden alle Regeln in den Zielservices entfernt und durch alle Regeln im Quellserviceersetzt.

So übertragen Sie ausgewählte Regeln von diesem Decoder auf andere Decoder:

1. Wählen Sie auf einer beliebigen „Regeln“-Registerkarte die Regeln aus, die Sie auf einen anderen Decoder übertragen möchten.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie 

> Push > Auswahl aus.
   - Klicken Sie mit der rechten Maustaste auf die ausgewählten Regeln und wählen Sie **Ausgewählte Regeln per Push übertragen** aus.

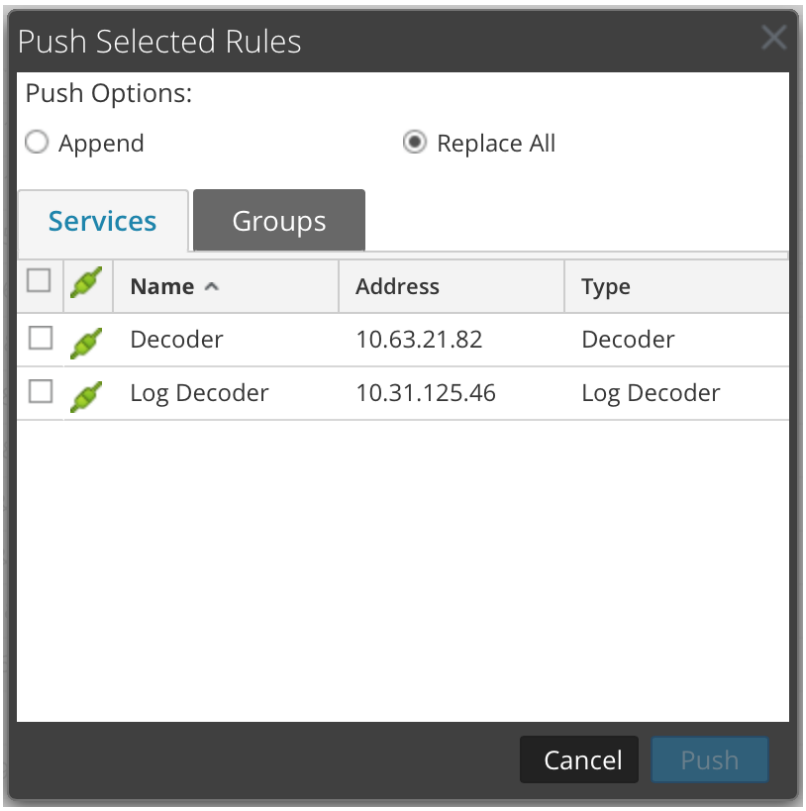
Das Dialogfeld „Ausgewählte Regeln per Push übertragen“ wird angezeigt.



3. Wählen Sie eine Push-Option aus:
   - Wählen Sie **Alle ersetzen** aus, um alle Regeln in den Zielservices zu löschen und durch die ausgewählten Regeln zu ersetzen. Dies ist die Standardoption.
   - Wählen Sie **Zusammenführen** aus, um die ausgewählten Regeln mit den vorhandenen Regeln in den Zielservices zusammenzuführten.
4. Wählen Sie auf der Registerkarte **Services** die Zielservices aus, die die per Push übertragenen Regeln empfangen sollen, oder wählen Sie die Gruppen von Services auf der Registerkarte **Gruppen** aus.
5. Klicken Sie auf **Push**.
   Die Regeln werden per Push auf die ausgewählten Services übertragen und sofort wirksam.

So übertragen Sie alle Regeln von diesem Decoder auf andere Decoder:

1. Wählen Sie auf einer „Regeln“-Registerkarte Actions > **Push** > **Alle** aus.
   Mit **Push** > **Alle** werden alle Regeln in der Liste übertragen, selbst wenn Sie eine Untergruppe für die Übertragung per Push ausgewählt haben. Das Dialogfeld „Ausgewählte Regeln per Push übertragen“ wird angezeigt.



2. Wählen Sie auf der Registerkarte **Services** die Zielservices aus, die die per Push übertragenen Regeln empfangen sollen, oder wählen Sie die Gruppen von Services auf der Registerkarte **Gruppen** aus.
3. Klicken Sie auf **Push**.
   Alle Regeln in den Zielservices werden gelöscht und durch alle Regeln aus dem Quellservice ersetzt. Die Regeln werden sofort wirksam.

Ausführungsreihenfolge von Regeln ändern

Erfassungsregeln werden in der Reihenfolge angewendet, in der sie in der Regelliste angezeigt werden. Verwenden Sie zur Neuordnung der Regeln eine der folgenden Methoden:

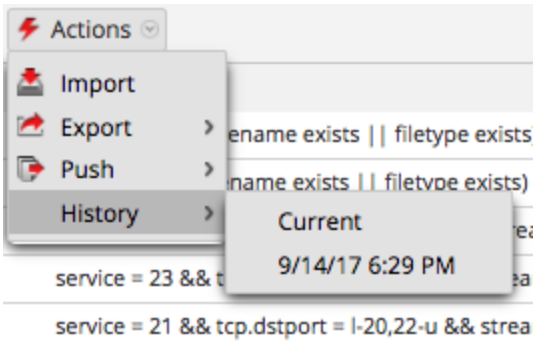
- Ziehen Sie die Regeln per Drag-and-drop an die entsprechenden Stellen in der Regelliste.
- Klicken Sie mit der rechten Maustaste auf eine Regel, um das Kontextmenü anzuzeigen, und verwenden Sie die Optionen **Ausschneiden** und **Einfügen**.

Regel-Snapshot aus dem Verlauf wiederherstellen

NetWitness Suite speichert die letzten zehn Snapshots der Regeln, die auf einen Service angewendet wurden.

So stellen Sie einen Regel-Snapshot aus dem Verlauf wieder her:

1. Wählen Sie Actions > **Verlauf** aus.
   Ein Untermenü mit Snapshots wird angezeigt.



2. Wählen Sie die Snapshot-Zeit im Untermenü aus.
   Die Regeln aus dem Snapshot werden in die Regelliste geladen und ersetzen den aktuellen Satz. Aber der aktuelle Satz wird immer noch von dem Service verwendet.
3. Klicken Sie zur Anwendung der Regeln auf den Service auf **Anwenden**.
   Die Regeln werden auf den Service angewendet.

Konfigurieren von Anwendungsregeln

Anwendungsebenenregeln werden auf der Sitzungsebene angewendet. Im Folgenden sind Beispiele für Anwendungsregeln aufgeführt.

Wenn Sie Pakete kürzen möchten, die über das SMB-Protokoll übertragen werden, erstellen Sie eine Regel wie folgt:

- Name der Regel: SMB kürzen
- Bedingung: `service=139`
- Regelaktion: Kürzen

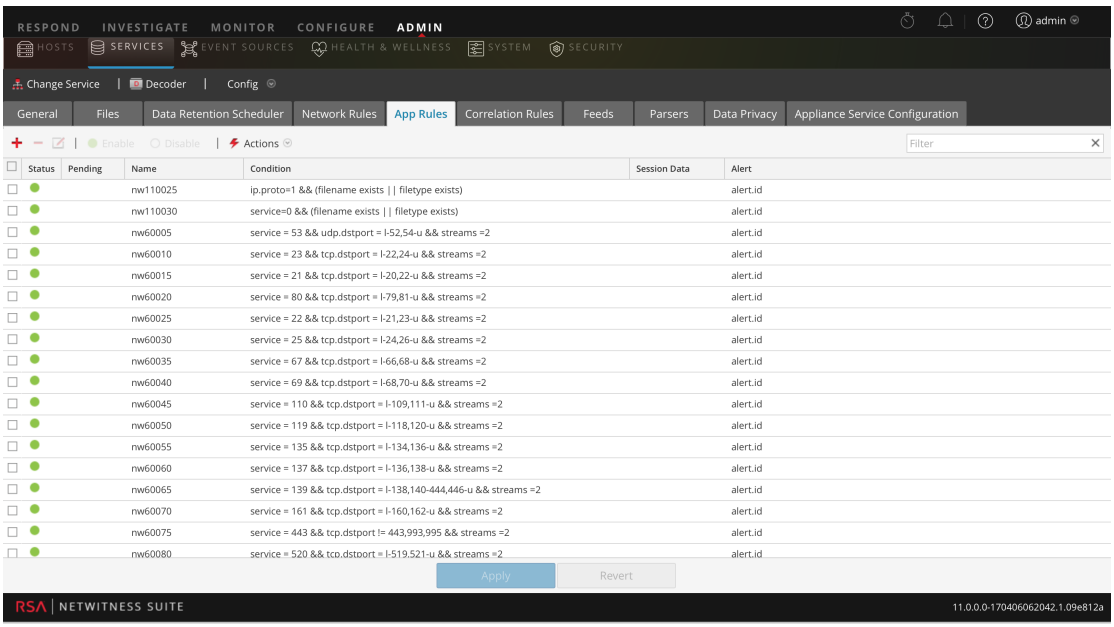
Wenn Sie E-Mails an und von einer bestimmten E-Mail-Adresse aufbewahren möchten, erstellen Sie eine Regel wie folgt:

- Name der Regel: E-Mail-Filter Tom Jones
- Bedingung: `email='Tom.Jones@TheShop.com'`
- Regelaktion: Filter

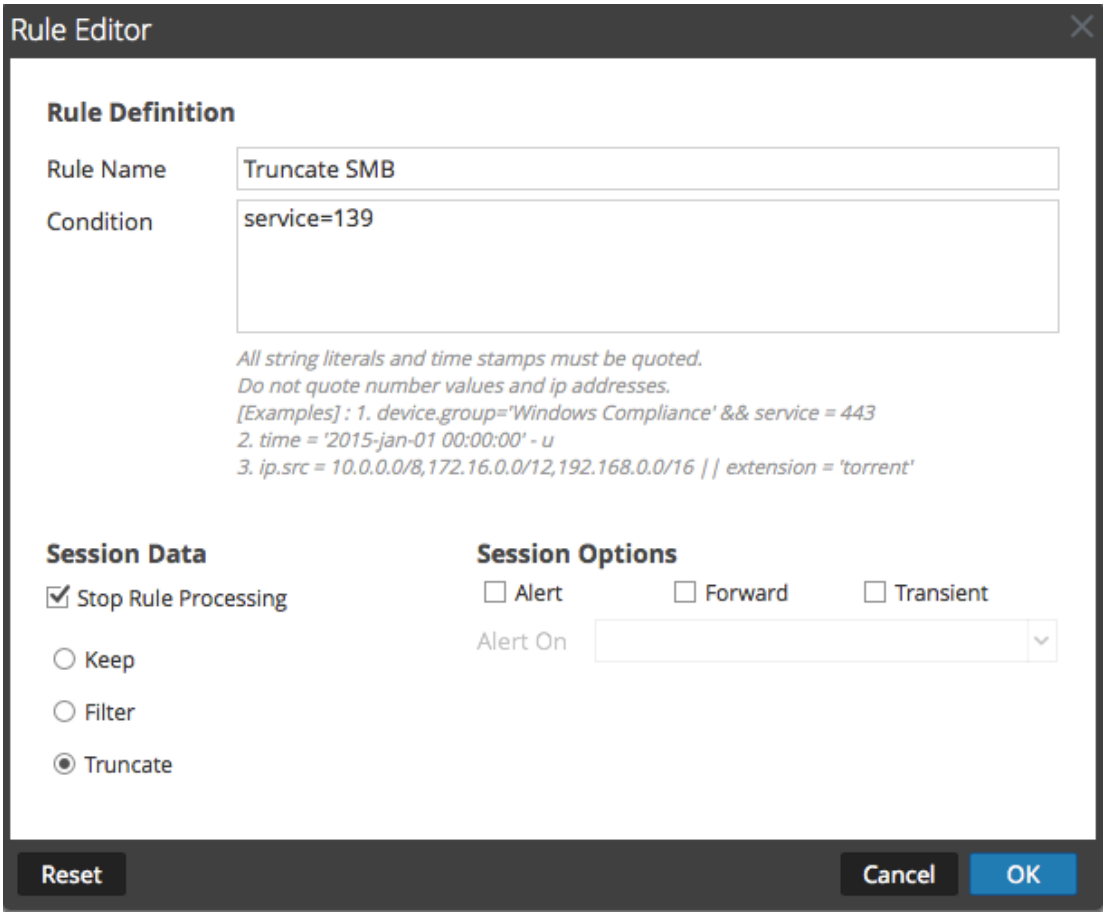
So fügen Sie eine Anwendungsregel hinzu oder bearbeiten sie:

1. Navigieren Sie zu **Administration** > **Services**.
2. Wählen Sie einen Decoder- oder Log Decoder-Service und > **Ansicht** > **Konfiguration** aus.

   Die Ansicht „Systeme-Konfiguration“ für den ausgewählten Service wird angezeigt.
3. Wählen Sie die Registerkarte **App-Regeln** aus.



4. Führen Sie einen der folgenden Schritte aus:
   Wenn Sie eine neue Regel hinzufügen möchten, klicken Sie auf + .
   Wenn Sie eine Regel bearbeiten möchten, wählen Sie die Regel aus der Regelliste aus und klicken Sie auf .
5. Das Dialogfeld Regel-Editor wird mit den Parametern der Anwendungsregel



   angezeigt.

   a. Geben Sie im Feld **Name der Regel** einen Namen für die Regel ein. Beispiel: Für eine Regel, die alle SMB kürzt, geben Sie **SMB kürzen** ein.
   b. Erstellen Sie im Feld **Bedingung** die Regelbedingung, die bei einer Übereinstimmung eine Aktion auslöst. Sie können direkt in das Feld schreiben oder die Bedingung in diesem Feld mithilfe der Metadaten aus den Fensteraktionen erstellen. Während Sie die Regeldefinition erstellen, zeigt NetWitness Suite Syntaxfehler und Warnungen an. Beispiel: Um alle SMB zu kürzen, geben Sie **service=139** ein.
      Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Unter Konfigurieren von Decoder-Regeln finden Sie zusätzliche Details.

c. Wenn die Regelauswertung mit dieser Regel enden soll, aktivieren Sie das Kontrollkästchen **Regelverarbeitung beenden**.
d. Wählen Sie im Abschnitt **Sitzungsdaten** eine der folgenden Aktionen aus, die angewendet werden soll, wenn ein passendes Paket gefunden wird:
Beibehalten: Die Paketnutzlast und die entsprechenden Metadaten werden gespeichert, wenn sie mit der Regel übereinstimmen.
Filter: Das Paket wird nicht gespeichert, wenn es mit der Regel übereinstimmt.
Kürzen: Die Paketnutzlast wird nicht gespeichert, wenn sie mit der Regel übereinstimmt, aber Paketkopfzeilen und zugehörige Metadaten werden beibehalten.
e. Führen Sie im Abschnitt **Sitzungsoptionen** einen der folgenden Schritte aus:

- **Um eine benutzerdefinierte Warnmeldung zu erzeugen**, wenn Sitzungsmetadaten der Regel entsprechen, aktivieren Sie das Flag „Warnmeldung“ und wählen Sie den Namen der Warnmeldungs-Metadaten aus der Drop-down-Liste **Warnmeldung bei** aus.
- **Um eine Syslog-Weiterleitung durchzuführen**, wenn das Protokoll der Regel entspricht, aktivieren Sie das Flag **Weiterleiten**. Achten Sie auf Folgendes:
  - Sie müssen sowohl das Flag „Warnmeldung“ als auch das Flag „Weiterleiten“ aktiviert haben, um die Syslog-Weiterleitung durchführen zu können.
  - Der Name der Regel, die im Dialogfeld „Regel-Editor“ erwähnt wird, muss dem Zielnamen für die Syslog-Weiterleitung entsprechen, der unter „Log Decoder“ > „Ansicht“ > „Durchsuchen“ im Parameter `/decoder/config/logs.forwarding.destination` angegeben ist.
- **Um zu verhindern, dass die erstellten Warnmeldungs-Metadaten auf den Datenträger geschrieben werden**, aktivieren Sie das Flag **Vorübergehend**.

6. Um die Regel zu speichern und sie dem Raster hinzuzufügen, klicken Sie auf **OK**.
Die Regel wird am Ende des Rasters oder an der von Ihnen im Kontextmenü angegebenen Stelle hinzugefügt. In der Spalte **Ausstehend** wird das Pluszeichen angezeigt.
7. Prüfen Sie, ob die Regel in der richtigen Ausführungsreihenfolge zu den anderen Regeln im Raster steht. Falls erforderlich, verschieben Sie die Regel.
8. Um den aktualisierten Regelsatz auf den Decoder oder Log Decoder anzuwenden, klicken Sie auf **Anwenden**.
NetWitness Suite speichert einen Snapshot der aktuell angewendeten Regeln und wendet dann den aktualisierten Satz auf den Decoder an und entfernt den Hinweis „Ausstehend“ von den Regeln, die noch ausstanden.

Konfigurieren von Korrelationsregeln

Grundlegende Korrelationsregeln werden auf der Sitzungsebene angewendet und weisen die Benutzer auf bestimmte Aktivitäten hin, die möglicherweise in ihrer Umgebung vorkommen. NetWitness Suite wendet Korrelationsregeln in einem konfigurierbaren gleitenden Zeitfenster an. Treffen die Bedingungen zu, werden Warnmeldungs-Metadaten für diese Aktivität erstellt, und es wird ein sichtbarer Hinweis auf die verdächtige Aktivität angezeigt.

Im Folgenden werden beispielhafte Korrelationsregeln mit zwei Anwendungsbeispielen und der entsprechenden Syntax gezeigt.

Ziel: Wenn es in Sitzungen mit tcp.dstport eine beliebige Kombination von ip.src und ip.dst gibt, bei der die Anzahl eindeutiger tcp.dstport-Instanzen innerhalb von 1 Minute größer 5 ist, wird eine Warnmeldung ausgegeben. Erstellen Sie dafür wie folgt eine Regel:

- Name der Regel: IPv6 – vertikaler TCP-Portscan 5
- Regel: `tcp.dstport exists`
- Instanzschlüssel: `ip.src,ip.dst`
- Schwellenwert: `u_count(tcp.dstport)>5`
- Zeitfenster: 1 Min.

Ziel: Wenn in Sitzungen, in denen `action==login` und `error==fail` gilt, eine beliebige Kombination von `ip.src` und `ip.dst` innerhalb von 5 Minuten in mehr als 10 Sitzungen auftritt, wird eine Warnmeldung ausgegeben. Um dieses Ziel zu erreichen, erstellen Sie eine Regel wie folgt:

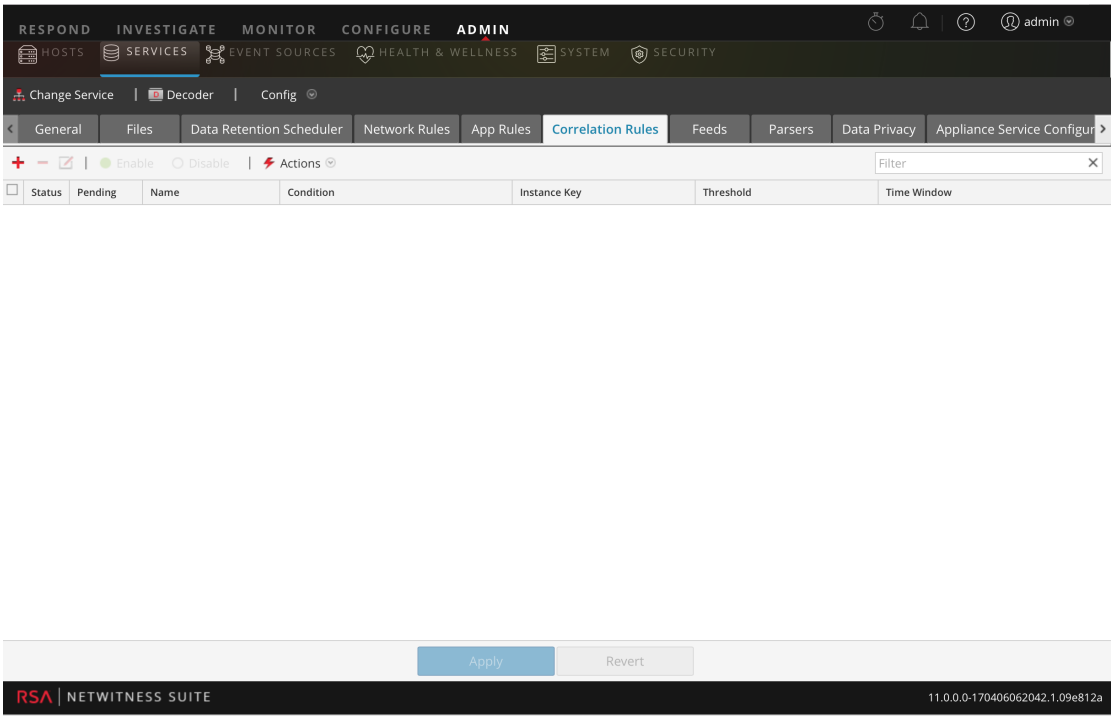
- Name der Regel: IPv4 – möglicher Brute Force 10
- Regel: action=`'login' && error='fail'`
- Instanzschlüssel: `ip.src,ip.dst`
- Schwellenwert: `count()>10`
- Zeitfenster: 5 Min.

Beide Regeln weisen denselben Instanzschlüssel auf: `ip.src` und `ip.dst`. Da wir nach eindeutigen Kombinationen von `ip.src` und `ip.dst` suchen, die der Korrelationsbedingung entsprechen, sind **`ip.src`** und **`ip.dst`** die **Primärschlüssel**.
Der Schwellenwert kann einen **zugehörigen Schlüssel** enthalten, der den Metadatentyp angibt, der gezählt wird, um die Erfüllung der Bedingung zu prüfen. Im ersten Beispiel lautet der im Schwellenwert angegebene zugehörige Schlüssel `tcp.dstport`. Wir zählen eindeutige Instanzen von `tcp.dstport` für jedes `ip.src/ip.dst`-Paar. Im zweiten Beispiel ist kein zugehöriger Schlüssel im Schwellenwert angegeben, da dieser einfach die Anzahl von Sitzungen darstellt. Stellen Sie sich dieses Szenario am einfachsten als eine Zählung von eindeutigen Sitzungs-IDs vor, bei der der zugehörige Metadatentyp implizit „session.id“ ist. Wir zählen eindeutige Instanzen von `session.id` für jedes `ip.src/ip.dst`-Paar.

Ungültiges Anwendungsbeispiel: Wenn es Sitzungen mit einer beliebigen Kombination von `ip.src` und `ip.dst` gibt (Regel), die innerhalb von (Zeitfenster) eine eindeutige Anzahl von `ipv6.dst > 5` aufweisen, wird eine Warnmeldung ausgegeben. Dieses Beispiel kann nicht funktionieren, da der zugehörige Schlüssel `ipv6.dst` ein IPv6-Metadatentyp ist. IPv4- und IPv6-Metadatentypen sind als zugehörige Schlüssel unzulässig.

So fügen Sie eine Korrelationsregel hinzu oder bearbeiten sie

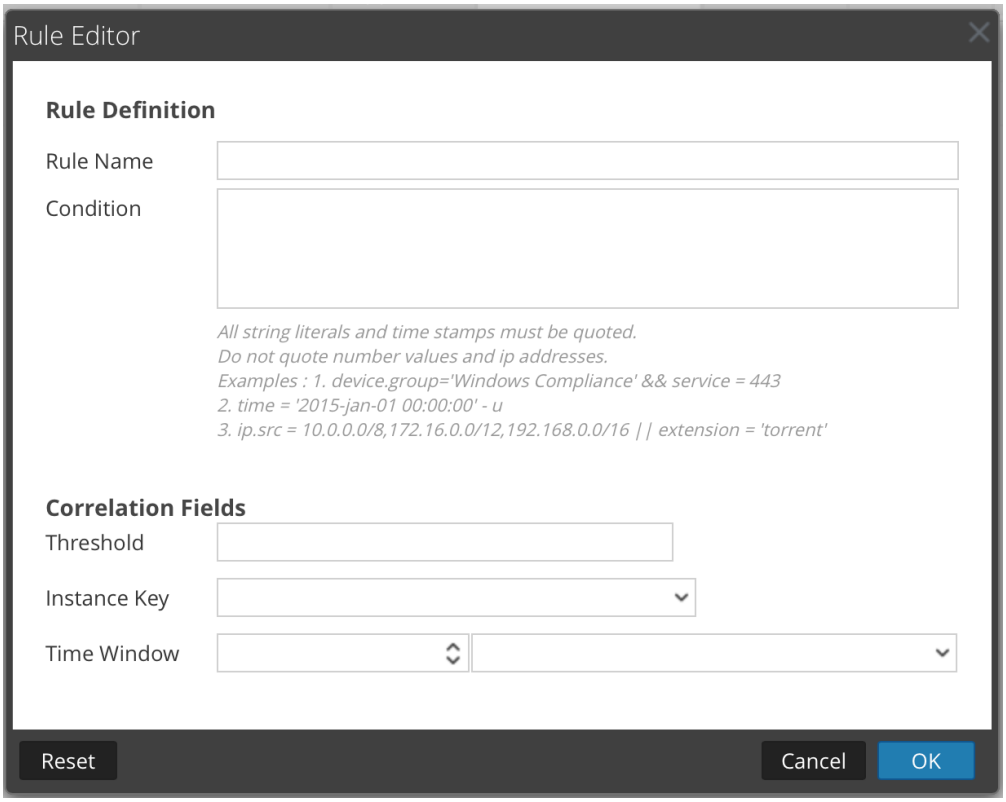
1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Service aus und dann > **Ansicht > Konfiguration**.
   Die Ansicht „Services-Konfiguration“ für den ausgewählten Service wird angezeigt.
2. Wählen Sie die Registerkarte **Korrelationsregeln** aus.



3. Führen Sie auf der Registerkarte **Korrelationsregeln** einen der folgenden Schritte aus:

- Wenn Sie eine neue Regel hinzufügen, klicken Sie auf .
- Wenn Sie eine Regel bearbeiten möchten, wählen Sie sie aus dem Regelraster aus und klicken Sie auf .

  Das Dialogfeld „Regel-Editor“ wird mit Parametern für die Korrelationsregeln angezeigt.



4. Geben Sie im Feld **Name der Regel** einen Namen für die Regel ein. Wenn Sie die Beispielregel erstellen, könnte dieser Name z. B. **IPv6 – vertikaler TCP-Portscan 5** lauten.
5. Erstellen Sie im Feld **Bedingung** die Regelbedingung, die bei einer Übereinstimmung eine Aktion auslöst. Sie können direkt in das Feld schreiben oder die Bedingung in diesem Feld mithilfe der Metadaten aus den Fensteraktionen erstellen. Während der Erstellung der Regeldefinition werden von NetWitness Suite Syntaxfehler und Warnmeldungen angezeigt. Wenn Sie die Beispielregel erstellen, können Sie z. B. **tcp.dstport exists** eingeben. Trifft die Bedingung zu, wird die Aktion für die Sitzungsdaten ausgeführt.
   Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Unter Konfigurieren von Decoder-Regeln finden Sie zusätzliche Details.
6. Verwenden Sie im Feld **Schwellenwert** einen der Schwellenwertparameter, um die Mindestanzahl von Vorkommnissen anzugeben. Diese Anzahl ist erforderlich, damit eine

Korrelationssitzung und ggf. ein zugehöriger Schlüssel erstellt wird. Der zugehörige Schlüssel darf kein IPv4- oder IPv6-Metadatentyp sein.

- u_count(associated_key) = die Anzahl eindeutiger Werte des angegebenen Schlüssels
- sum(associated_key) = die Werte des angegebenen Schlüssels
- count = number of sessions (keine Angabe des zugehörigen Schlüssels)

7. Wählen Sie im Feld **Instanzschlüssel** den Zielindikator aus, der als Basis für das Ereignis dient. Dies kann ein einziger oder ein zusammengesetzter Schlüssel sein (zwei durch ein Komma getrennte Primärschlüssel).
8. Legen Sie im Feld **Zeitfenster** die Dauer fest. Innerhalb dieser Zeit muss der Schwellenwert erreicht werden, damit eine Korrelationssitzung erstellt wird.
9. Um die Regel zu speichern und sie dem Raster hinzuzufügen, klicken Sie auf **OK**.
   Die Regel wird am Ende des Rasters oder an der von Ihnen im Kontextmenü angegebenen Stelle hinzugefügt. In der Spalte **Ausstehend** wird das Pluszeichen angezeigt.
10. Prüfen Sie, ob die Regel in der richtigen Ausführungsreihenfolge zu den anderen Regeln im Raster steht. Falls erforderlich, verschieben Sie die Regel.
11. Um den aktualisierten Regelsatz auf den Service anzuwenden, klicken Sie auf **Anwenden**.
    NetWitness Suite speichert einen Snapshot der aktuell angewendeten Regeln und wendet dann den aktualisierten Satz auf den Decoder oder Log Decoder an.

Konfigurieren von Netzwerkregeln

Netzwerkregeln werden auf Paketebene auf einem Decoder angewendet und bestehen aus Regeln von Ebene 2, Ebene 3 und Ebene 4. Sie können mehrere Regeln auf der Paketebene auf einen Decoder anwenden. Netzwerkregeln können für mehrere Netzwerkschichten gelten (z. B. wenn eine Netzwerkregel bestimmte Ports für eine bestimmte IP-Adresse herausfiltert). Netzwerkregeln gelten nicht für Log Decoder, sondern nur für Paket-Decoder.

Sie können Netzwerkregeln auf der Registerkarte „Netzwerkregeln“ der Ansicht „Services-Konfiguration“ erstellen.

Unterstützte Metaschlüssel in Netzwerkregelbedingungen

In der folgenden Tabelle werden die Metaschlüssel beschrieben, die NetWitness Suite zur Verwendung in Netzwerkregelbedingungen unterstützt.

Metaschlüssel	Beschreibung
`eth.addr`	Ethernetquelle oder Zieladresse. Allgemein bekannt als MAC-Adresse.
`eth.dst`	Ethernetzieladresse. Dies entspricht dem Feld „Ethernetadresse“, es sei denn, es werden nur Pakete ausgewählt, bei denen die Zieladresse mit den ausgewählten Werten übereinstimmt.
`eth.src`	Identisch mit Ethernetziel, außer dass der Schwerpunkt hier auf der Quelladresse liegt
`eth.type`	Ethernetframetyp
`hdlc.type`	Frametyp des HDLC-Frames
`ip.addr`	IPv4-Quell- oder -Zieladresse im Standardformat. IP-Adressen können nur in der CIDR-Notation für Subnetze eingegeben werden.
`ip.dst`	IPv4-Zieladresse im Standardformat. IP-Adressen können nur in der CIDR-Notation für Subnetze eingegeben werden.
`ip.proto`	Feld IPv4-Protokoll
`ip.src`	IPv4-Quelladresse im Standardformat. IP-Adressen können nur in der CIDR-Notation für Subnetze eingegeben werden.

Metaschlüssel	Beschreibung
ipv6.addr	IPv6-Quell- oder Zieladresse im Hexadezimalformat. In der Regel werden IPv6-Adressen in Form von acht Gruppen mit je vier hexadezimalen Ziffern geschrieben, sodass die Länge der gesamten 128-Bit-Adresse dargestellt wird. Unterstützt die Notation zur Darstellung mehrerer Blöcke aus 0000 in einer Adresse. Die CIDR-Notation wird nicht unterstützt.
ipv6.dst	IPv6-Zieladresse im Hexadezimalformat
ipv6.proto	Feld IPv6-Protokoll. Dies entspricht dem Next-Header-Feld in der IPv6-Kopfzeile und verwendet denselben Wert wie das IPv4-Protokoll-Feld.
ipv6.src	IPv6-Quelladresse im Hexadezimalformat
tcp.dstport	TCP-Zielport
tcp.port	TCP-Quell- oder Zielport
tcp.srcport	TCP-Quellport
udp.dstport	UDP-Zielport
udp.port	UDP-Quell- oder Zielport
udp.srcport	UDP-Quellport

Im Folgenden sind Beispiele für Netzwerkregeln aufgeführt.

Um alle SSL aus dem Quellport zu kürzen, erstellen Sie eine Regel wie folgt:

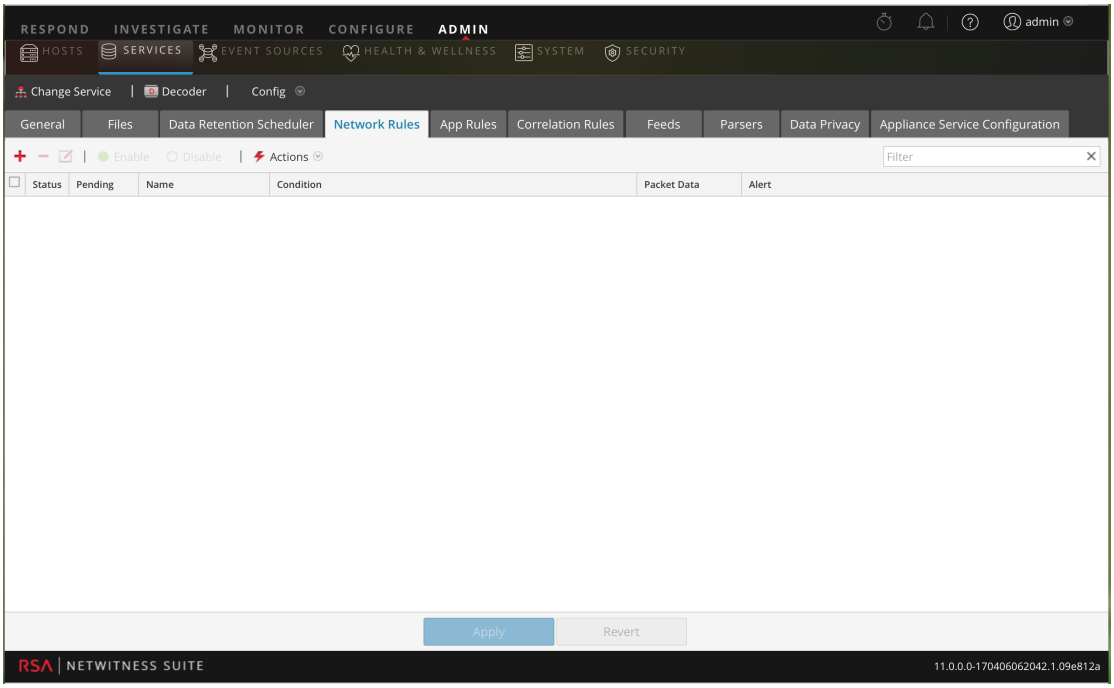
- Name der Regel: SSL kürzen
- Bedingung: `tcp.srcport=443`
- Regelaktion: Kürzen

Um den Subnetzdatenverkehr zu filtern, erstellen Sie eine Regel wie folgt:

- Name der Regel: Subnetzfilter
- Bedingung: `ip.addr=192.168.2.0/24`
- Regelaktion: Filter

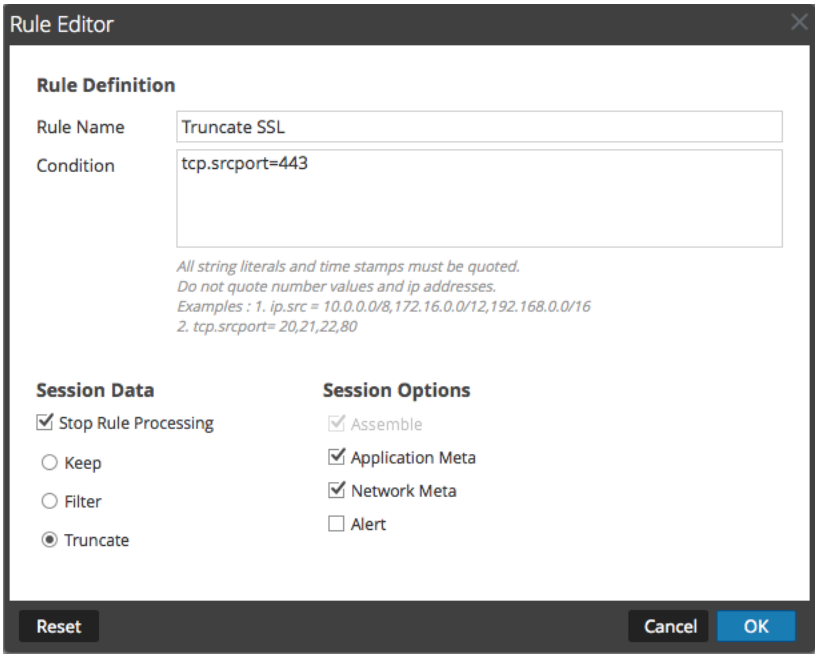
So fügen Sie eine Netzwerkregel hinzu oder bearbeiten sie:

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Decoder-Service aus und dann > **Ansicht > Konfiguration**.
   Die Ansicht „Services-Konfiguration“ für den ausgewählten Service wird angezeigt.
2. Wählen Sie die Registerkarte **Netzwerkregeln** aus.
   Die Registerkarte „Netzwerkregeln“ wird angezeigt.



3. Führen Sie auf der Registerkarte **Netzwerkregeln** einen der folgenden Schritte aus:
   - Wenn Sie eine neue Regel hinzufügen möchten, klicken Sie auf +
   - Wenn Sie eine Regel bearbeiten möchten, wählen Sie sie aus der Regelliste aus und klicken Sie auf .

Das Dialogfeld „Regel-Editor“ wird angezeigt.



4. Geben Sie im Feld **Name der Regel** einen Namen für die Regel an. Beispielsweise können Sie eine Regel, die SSL komplett aus dem Quellport kürzt, **SSL kürzen** nennen.
5. Erstellen Sie im Feld **Bedingung** die Regelbedingung, die bei einer Übereinstimmung eine Aktion auslöst. Sie können direkt in das Feld schreiben oder die Bedingung in diesem Feld mithilfe der Metadaten aus den Fensteraktionen erstellen. Während Sie die Regeldefinition erstellen, zeigt NetWitness Suite Syntaxfehler und Warnungen an. Um z. B. alle SSL vom Quellport zu kürzen, geben Sie `tcp.srcport=443` ein.
   Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Unter Konfigurieren von Decoder-Regeln finden Sie zusätzliche Details. Unter Unterstützte Metaschlüssel in Netzwerkregelbedingungen sind die Metaschlüssel beschrieben, die in NetWitness Suite in Netzwerkregelbedingungen unterstützt werden.
6. Wenn die Regelauswertung mit dieser Regel enden soll, aktivieren Sie das Kontrollkästchen **Regelverarbeitung beenden**.
7. Wählen Sie im Abschnitt **Sitzungsdaten** eine der folgenden Aktionen aus, die angewendet werden soll, wenn ein passendes Paket gefunden wird.
   - **Beibehalten**: Die Paketnutzlast und die entsprechenden Metadaten werden gespeichert, wenn sie mit der Regel übereinstimmen.
   - **Filter**: Das Paket wird nicht gespeichert, wenn es mit der Regel übereinstimmt.

- **Kürzen**: Die Paketnutzlast wird nicht gespeichert, wenn sie mit der Regel übereinstimmt, aber Paketkopfzeilen und zugehörige Metadaten werden beibehalten.

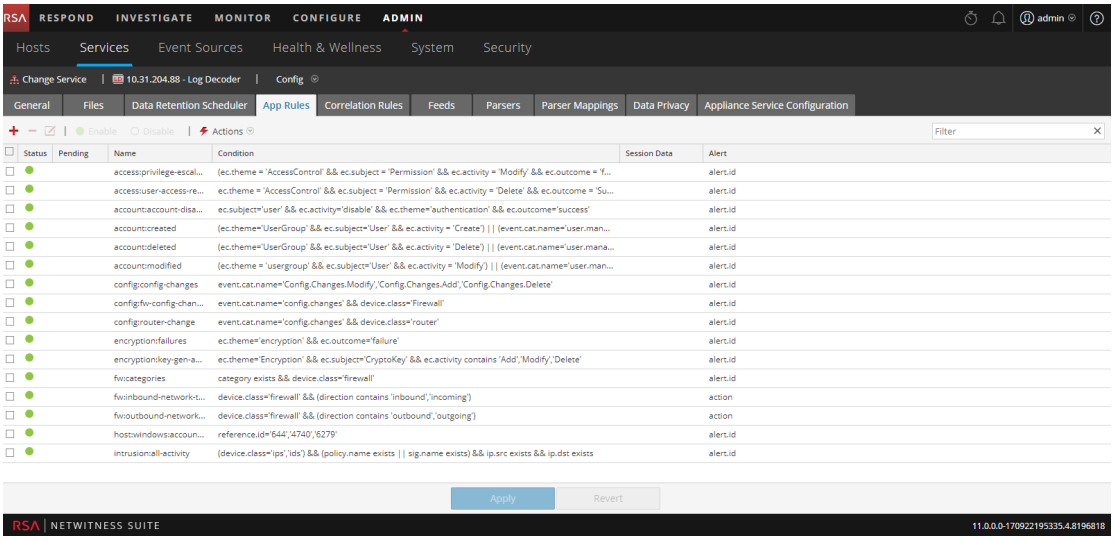
8. Wählen Sie im Abschnitt **Sitzungsoptionen** alle geltenden Optionen der folgenden vier Optionen aus.
   - **Assemblieren**: Der Assembler setzt die Paketkette zusammen, wenn sie der Regel entspricht.
   - **Netzwerkmetadaten:** Das Paket erzeugt Netzwerkmetadaten, wenn es der Regel entspricht.
   - **Anwendungsmetadaten**: Das Paket erzeugt Anwendungsmetadaten, wenn es der Regel entspricht.
   - **Warnmeldung**: Das Paket erzeugt eine angepasste Warnmeldung, wenn Metadaten der Regel entsprechen.
9. Um die Regel zu speichern und sie der Regelliste hinzuzufügen, klicken Sie auf **OK**.
   Die Regel wird am Ende der Liste oder an der von Ihnen im Kontextmenü angegebenen Stelle hinzugefügt.
10. Prüfen Sie, ob die Regel in der richtigen Ausführungsreihenfolge in der Liste enthalten ist. Falls erforderlich, verschieben Sie die Regel.
11. Um den aktualisierten Regelsatz auf den Decoder anzuwenden, klicken Sie auf **Anwenden**.
    NetWitness Suite speichert einen Snapshot der aktuell angewendeten Regeln und wendet dann den aktualisierten Satz auf den Decoder an und entfernt den Hinweis „Ausstehend“ von den Regeln, die noch ausstanden.

Korrigieren von Regeln mit ungültiger Syntax

Nach der Aktualisierung auf NetWitness Suite 11.0 werden Regeln mit ungültiger Syntax in der Benutzeroberfläche gekennzeichnet. Der Regel-Editor bietet zusätzliche Kurzinformationen. Nachdem Sie die Regeln repariert haben, werden die Hervorhebungen nicht mehr angezeigt. Unter Konfigurieren von Decoder-Regeln finden Sie Richtlinien, denen alle Abfragen und Regelbedingungen in NetWitness Suite entsprechen müssen.

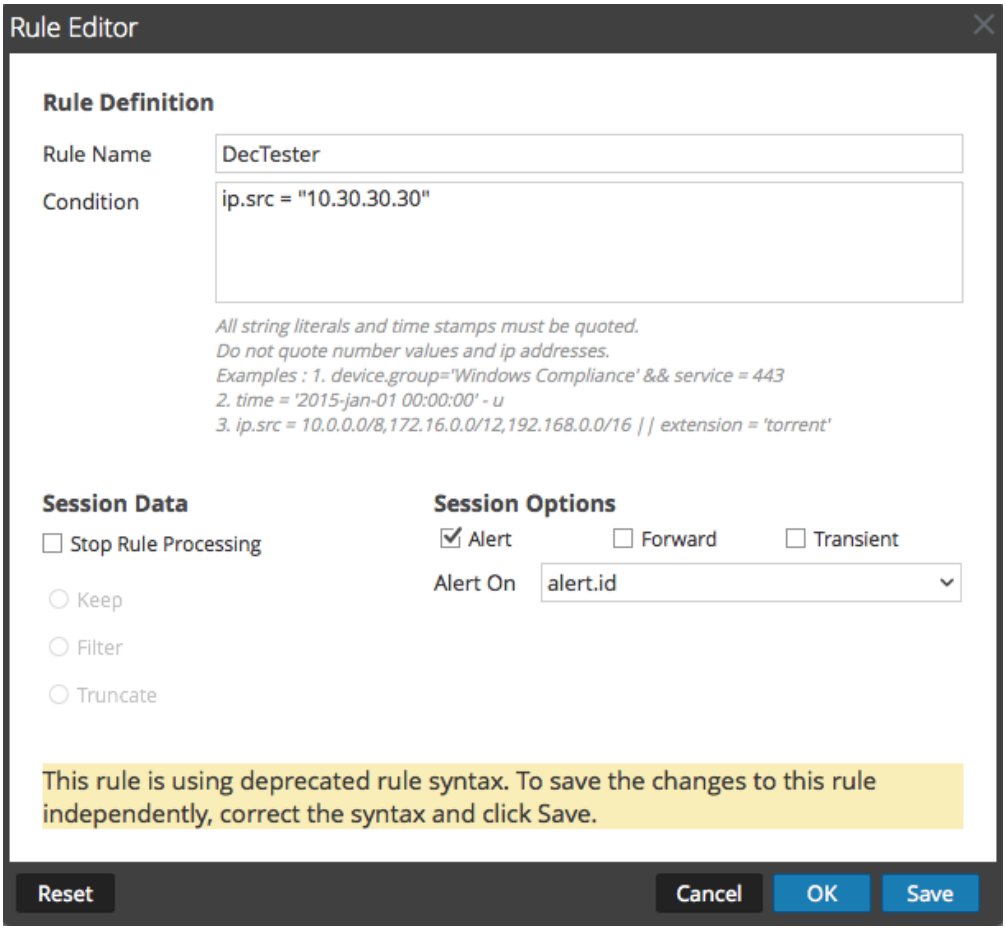
So korrigieren Sie Regeln mit ungültiger Syntax:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht **Services** einen Decoder-Service und  **> Ansicht > Konfiguration** aus.
3. Wählen Sie in der Ansicht **Services-Konfiguration** eine der Registerkarten „Regeln“ aus: Netzwerkregeln, App-Regeln oder Korrelationsregeln.
   Auf der Registerkarte „Regeln“ für den ausgewählten Regeltyp wird die Anzahl der Regeln mit ungültiger Syntax angezeigt und die ungültigen Regeln sind hervorgehoben.



4. Wählen Sie eine ungültige Regel aus und klicken Sie auf  .
   Der Regel-Editor enthält zusätzliche Informationen für die ungültige Regel und umfasst eine

zusätzliche Speicheroption.



5. Korrigieren Sie die Regelsyntax im Feld **Bedingung**.
   Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Unter Konfigurieren von Decoder-Regeln finden Sie zusätzliche Details.
   Beispiel: Wenn die ungültige Regelbedingung `ip.src="10.30.30.30"` lautet, korrigieren Sie die Syntax durch Entfernen der Anführungszeichen: `ip.src=10.30.30.30`
6. Führen Sie einen der folgenden Schritte aus:
   - Um die Regel einzeln zu korrigieren, klicken Sie auf **Speichern**.
     Die korrigierte Regel wird unabhängig auf den Decoder angewendet. Die korrigierte Regel wird auf der Registerkarte Regeln ohne Markierung angezeigt.
   - Zum Korrigieren der Regel und späteren Anwenden der Regel auf den Decoder mit anderen Regeln klicken Sie auf **OK**.
     Die korrigierte Regel wird auf der Registerkarte Regeln ohne Markierung angezeigt. Die Regel wird nicht auf den Decoder angewendet.

Decoder-Befehle für die Verwaltung von Regeln

In der NetWitness Core-Datenbank enthält die Regelstruktur die wichtigsten Funktionen für die Verwaltung von Regeln, und zwar für alle Core-Services, die über Regeln verfügen: Concentrator, Decoder, Log Decoder und Archiver. Regeln können in der NetWitness Suite-Benutzeroberfläche verwaltet werden, aber fortgeschrittene Benutzer können die Regeln eines Service auch über eine Befehlszeile hinzufügen, zusammenführen, ersetzen, löschen und validieren. Dieser Abschnitt enthält eine kurze Übersicht über die Befehle und ihre Nutzung. Dies sind die verfügbaren Befehle:

- `add`: Fügt eine Regel an der angegebenen Position ein.
- `clear`: Löscht alle vorhandenen Regeln im aktuellen Node des Service. Bei Verwendung des Befehls im Node `/decoder/config/rules/application` werden beispielsweise alle vorhandenen Anwendungsregeln im Decoder gelöscht.
- `delete`: Löscht eine oder mehrere Regeln an der angegebener Position und in der angegebenen Anzahl.
- `merge`: Führt einen übertragenen Regelsatz mit einem vorhandenen Regelsatz zusammen. Vorhandene Regeln, die mit den eingehenden Regeln übereinstimmen (und zwar entweder beim Namen oder bei der Regel selbst), werden ersetzt. Ansonsten werden die Regeln an der angegebenen Position eingefügt, wie in Befehl „merge“ beschrieben.
- `replace`: Löscht alle vorhandenen Regeln und ersetzt sie durch den eingehenden Regelsatz.
- `validate`: Validiert die Syntax einer Regel, aber nicht die Metaschlüssel.

Befehl „add“

Mit dem Befehl `add` wird dem vorhandenen Regelsatz eine Regel hinzugefügt. Die Formatierung ist wichtig, da doppelte Anführungszeichen in der API-Regelsprache und ebenso als Parameter für alle APIs von RSA NetWitness® Suite verwendet werden. Aus diesem Grund müssen Sie allen doppelten Anführungszeichen in der Regel selbst einen umgekehrten Schrägstrich (\) voranstellen. Die Syntax des Befehls lautet wie folgt:

```
add rule=<string> name=<string> alert=<string, optional> atPos=<<uint32, optional>
```

- `rule` ist die hinzuzufügende Regel. Achten Sie darauf, dass Sie alle Regeln, die Leerzeichen aufweisen, in doppelte Anführungszeichen setzen, und dass Sie allen doppelten Anführungszeichen, die Teil der Regel sind, einen umgekehrten Schrägstrich voranstellen.
- `name` ist der Name der Regel.

- `alert` ist die Warnmeldung für die Regel (falls vorhanden).
- `atPos` ist die Position, an der die Regel eingefügt werden soll (beginnend mit 1). Null ist der Anfang der Liste und bei jeder Zahl, die größer als die aktuelle Länge der Liste ist, wird die Regel am Ende angefügt.

Dies ist ein Beispiel für einen Befehl, mit dem eine Regel mithilfe von NwConsole hinzugefügt wird:

```
send /decoder/config/rules/application add rule="ip.src exists" order=1
alert=alert.id name=testrule
```

Sehen Sie sich nun diese Regel an:

```
alias.host = "myPC" && country.src="china","russian federation"
```

Um dies als Regel hinzuzufügen, müssen Sie die Parameter wie folgt übergeben:

```
rule="alias.host = \"myPC\" && country.src=\"china\",\"russian
federation\"" name=myRule filter
```

Beachten Sie, dass allen doppelten Anführungszeichen im Regelparameter ein umgekehrter Schrägstrich vorangestellt wurde. Damit dies besser lesbar ist, können Sie innerhalb der Regel auch einfache Anführungszeichen verwenden. Einfache und doppelte Anführungszeichen sind für die Regel und die Abfragesprache gleichwertig, aber nicht für API-Parameter (hier werden nur doppelte Anführungszeichen unterstützt). Mit einfachen Anführungszeichen ist die gleiche Regel besser lesbar:

```
rule="alias.host = 'myPC' && country.src='china','russian federation'"
name=myRule filter
```

Befehl „merge“

Der Befehl `merge` dient der Zusammenführung einer eingehenden Liste von Regeln mit den vorhandenen Regeln im Service. So funktioniert es:

- Vorhandene Regeln werden gefunden, die den gleichen Namen ODER die gleiche Regel aufweisen. Dann wird der vorhandene Name der Regel aktualisiert und die gleiche Position beibehalten.
- Neue Regeln werden in die Regelliste basierend auf der angegebenen ZAHL eingefügt. Wenn die Zahl Null ist, werden sie an den Anfang der Liste eingefügt.
- Die Regeln werden in der Reihenfolge ihres Empfangs verarbeitet: Wenn zwei Regeln mit Null nummeriert sind, wird die zweite Regel nach der ersten verarbeitet und an die oberste Position gesetzt. Alle vorhandenen Regeln werden zwei Stellen nach unten verschoben. Bei allen Zahlen, die höher als die vorhandenen Regelpositionen sind, werden die Regeln nach der letzten vorhandenen Regel eingefügt und entsprechend nummeriert.

- Alle nicht nummerierten Regeln werden ebenfalls nach der letzten vorhandenen Regel eingefügt und erhalten die nächste verfügbare Nummer.

Die Syntax des Befehls „merge“ lautet wie folgt:

`merge --file-data=<string> --file-format<string>`

- `file-data` ist der vollständige Pfad und Name der zusammenzuführenden Regeldatei.
- `file-format` ist das Format der Regeldatei. Gültige Werte sind `params-list`, `string`, `params`, `binary` und `params-binary`.

Methoden zum Senden einer Liste von Regeln an einen Service

Es gibt zwei Möglichkeiten, eine Liste von Regeln zu senden. Sie können sie als `.nwr` (NetWitness-Regel)-Datei oder als nummerierten Satz von Parametern senden, wobei jede Zahl die Position, an der die Regel eingefügt werden soll, sowie die codierte Regel angibt. Wenn Sie die aktuelle Liste der Regeln in einem Service anzeigen möchten, müssen Sie den Befehl `ls` für die Regelkategorie ausführen (Anwendungsregeln für einen Decoder befinden sich z. B. in `/decoder/config/rules/application`).

Dies ist ein Beispiel für Befehle, mit denen vorhandene Regeln mithilfe von NwConsole aufgelistet werden:

```
login <hostname>:50004 <username> <password>
cd /decoder/config/rules/application
ls
```

Dies ist ein weiteres Beispiel, bei dem vorhandene Regeln in NwConsole aufgelistet werden:

`send /decoder/config/rules/application ls`

Dies ist ein Beispiel des Befehls, mit dem auf Netzwerkregeln im RESTful-Port verwiesen wird, was Unterstützung für eine einfache `admin HTML`-App bietet.

`http[s]://<decoder>:50104/decoder/config/rules/network`

Senden einer NetWitness-Regeldatei

Beginnen wir mit einer beispielhaften `nwr`-Datei. Jede Regel muss sich in einer separaten Zeile befinden:

```
rule="ip.src=192.168.0.1" name=first keep
rule="ip.src=192.168.1.1" name=second alert=risk.info
rule="ip.src=192.168.2.1" name=third filter
```

Um Regeln mit NwConsole zu übertragen und zusammenzuführen, verwenden Sie die folgenden Befehle:

```
login <hostname>:50004 <username> <password>

send /decoder/config/rules/application merge --file-
data=/root/App_Rules.nwr --file-format=params-list
```

Um die vorhandenen Regeln durch die Regeln in der Datei zu ersetzen, verwenden Sie nicht den Befehl `merge`, sondern `replace`.

```
send /decoder/config/rules/application replace --file-
data=<pathname> --file-format=params-list
```

Um die Regeln in einer `nwr`-Datei mithilfe des RESTful-Ports zusammenzuführen, können Sie einen `curl`-Befehl verwenden, der die Regeln überträgt:

```
curl -u "<username>:<password>" -H "Content-Type:
application/octet-stream" --data-binary @<pathname> -X POST
"http://<hostname>:50104/decoder/config/rules/application?msg
=merge"
```

In den Beispielen werden Anwendungsregeln übertragen. Senden Sie Netzwerkregeln an `/decoder/config/rules/network`. Senden Sie Korrelationsregeln an `/decoder/config/rules/correlation`.

Senden von nummerierten Parametern

Die andere Möglichkeit, eine Regelliste zu senden, ist das Senden als nummerierte Parameter. Die Schwierigkeit bei dieser Methode ist, dass den Anführungszeichen in jeder nummerierten Regel ein Escape-Zeichen vorangestellt werden muss. Dies ist jedoch nur ein Problem, wenn Sie versuchen, es manuell durchzuführen. Um z. B. dieselben Regeln wie oben als Parameter über NwConsole zu senden, verwenden Sie den folgenden Befehl:

```
send /decoder/config/rules/application merge
1="rule=\"ip.src=192.168.0.1\" name=first keep"
2="rule=\"ip.src=192.168.1.1\" name=second alert=risk.info"
3="rule=\"ip.src=192.168.2.1\" name=third filter"
```

Dieser Befehl ist schwer zu lesen, weil den enthaltenen Anführungszeichen umgekehrte Schrägstriche (\) vorangestellt werden müssen. Ansonsten bewirken diese beiden Befehle das Gleiche: Zusammenführen oder Hinzufügen von drei Regeln an den Positionen 1, 2 und 3. Wenn Sie meinen, dass der Befehl oben schwer zu lesen ist, schauen Sie sich den äquivalenten Befehl `curl` an:

```
curl -u "<username>:<password>"
"http://<hostname>:50104/decoder/config/rules/application?msg=merge&1=r
ule%3D%22ip.src%3D192.168.0.1%22%20name%3Dfirst%20keep&2=rule%3D%22ip.s
rc%3D192.168.1.1%22%20name%3Dsecond%20alert%3Drisk.info&3=rule%3D%22ip.
src%3D192.168.2.1%22%20name%3Dthird%20filter"
```

Weitere Informationen dazu, wie doppelte Anführungszeichen in Parametern mit Escape-Zeichen versehen werden, finden Sie unter Befehl „add“.

Sortieren von Regeln während der Übertragung

Übertragene Regeln werden auf zwei verschiedene Arten sortiert. Wenn sie als Parameter übergeben werden, bestimmt die Nummer des Parameters die Reihenfolge. Hat er keine Nummer, sucht `merge` nach einem `order`-Parameter in der Regel selbst und verwendet diesen Wert, sofern vorhanden.

Hinweis: Die Verwendung von `order` ist die einzige Möglichkeit zum Festlegen der Reihenfolge in einer `.nwr`-Datei. Wenn weder eine Nummer noch ein `order` -Parameter gefunden wird, gibt es keine Garantie für die Einfügereihenfolge.

Beispiel

Bei einem Decoder sind folgende Anwendungsregeln installiert. Beachten Sie, dass die Nummerierung IMMER aufeinanderfolgend ist und bei 1 beginnt:

```
0001 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep
```

```
0002 : rule="ip.src=192.168.1.1" name=second alert=risk.info
```

```
0003 : rule="ip.src=192.168.2.1" name=third filter
```

Und Sie möchten die folgenden vier Regeln zusammenführen:

```
rule="ip.src=192.168.3.1" name=third keep
```

```
rule="ip.dst=192.168.4.1" name=NewRule filter order=0
```

```
rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append
```

```
rule="service=80,443" name=web filter order=3
```

Sie verwenden eine beliebige Methode zum Übertragen der Regeln und erhalten folgendes Ergebnis:

```
0001 : rule="ip.dst=192.168.4.1" name=NewRule filter order=1
```

```
0002 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep order=2
```

```
0003 : rule="service=80,443" name=web filter order=3
```

```
0004 : rule="ip.src=192.168.1.1" name=second alert=risk.info order=4
```

```
0005 : rule="ip.src=192.168.3.1" name=third keep order=5
```

```
0006 : rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=6
```

Gibt es hier etwas Überraschendes? Jede Regel wurde wie folgt verarbeitet:

```
1. rule="ip.src=192.168.3.1" name=third keep
```

Diese Regel hat den gleichen Namen wie eine vorhandene Regel im Decoder (die dritte). Daher wurde die vorhandene Regel `changing _filter_ to _keep_` aktualisiert.

```
2. rule="ip.dst=192.168.4.1" name=NewRule filter order=0
```

Diese Regel ist neu und enthält `order=0`, sodass sie ganz oben eingefügt wird.

```
3. rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter
order=append
```

Diese Regel hat den Nicht-Nummernwert `append` für `order` und wird deshalb an das Ende der Liste eingefügt. Sie erreichen dasselbe durch Angabe einer sehr großen Zahl wie `999999`.

```
4. rule="service=80,443" name=web filter order=3
```

Diese Regel ist die letzte, enthält aber `order=3`. Wenn sie keiner vorhandenen Regel entspricht (beim Namen oder Text der Regel selbst), wird sie an Position 3 platziert. Sie bildet also die dritte Regel in der Liste. Alle nachfolgenden Regeln wurden nach unten verschoben.

Befehl „replace“

Mit dem Befehl `replace` werden alle vorhandene Regeln entfernt und durch die eingehende Regelliste ersetzt. Unter Befehl „merge“ finden Sie ausführliche Informationen zum Formatieren der eingehenden Regelliste und zur Sortierung.

Dies ist ein Beispiel für den Befehl `replace` unter Verwendung einer NetWitness-Regeldatei:

```
send /decoder/config/rules/application replace --file-
data=/root/Decoder-AppRules.nwr --file-format=string
```

Dies ist ein Beispiel für den Befehl `replace` unter Verwendung von nummerierten Parametern:

```
send /decoder/config/rules/application replace 1="rule=\"ip.src exists\"
name=\"test rule\" order=1 alert=alert.id"
```

Befehl „clear“

Mit dem Befehl `clear` werden alle vorhandene Regeln aus dem Service entfernt. Dies ist ein Beispiel für den Befehl:

```
send /decoder/config/rules/application clear
```

Befehl „delete“

Mit dem Befehl `delete` werden eine oder mehrere Regeln vom Service gelöscht.

```
delete atPos <uint32> count <uint32, optional>
```

- `atPos` löscht die Regel an der angegebenen Position. Die Regeln sind fortlaufend nummeriert, beginnend mit 1.
- `count` löscht eine oder mehrere Regeln ab `atPos`. Dies ist ein optionaler Parameter, mit dem definiert wird, wie viele Regeln ab `atPos` gelöscht werden sollen. Der Standardwert ist 1.

Bei diesem Beispiel für den Befehl werden vier Regeln ab Position 0003 gelöscht:

```
send /decoder/config/rules/application delete atPos=0003 count=4
```

Befehl „validate“

Mit dem Befehl `validate` wird sichergestellt, dass die Regel richtig angewendet wird. Denken Sie daran, dass mit diesem Befehl nicht überprüft werden kann, ob Sprachschlüssel und Entitäten gültig sind.

```
validate rule <string>
```

`rule` ist der Name der zu validierenden Regel. Achten Sie darauf, alle Regeln, die Leerzeichen enthalten, in doppelte Anführungszeichen zu setzen.

Konfigurieren von Feeds und Parsern

Feeds und Parser sind verantwortlich für die Analyse der Pakete und Protokolle, wenn diese erfasst oder in einen Decoder oder Log Decoder importiert werden. Am häufigsten werden sie für die Extrahierung statischer Metadaten und zur Identifizierung von Services verwendet. Mit der flexiblen Definition können die definierten Core-Services um zusätzliche Servicetypenidentifizierungen und Metadatenextrahierungen erweitert werden. Dies ist aufgrund der Vielzahl an benutzerdefinierten Anwendungen in einem Netzwerk von großer Bedeutung.

Hinweis: Wenn nicht anders angegeben, gilt jede Aussage über Decoder auch für Log Decoder.

Konfigurieren von Parsern

NetWitness Suite bietet einen Satz Core-Parser, die vom System definiert sind, sowie die Möglichkeit, zusätzliche Parser hinzuzufügen. Jeder Parser kann unter Ansicht „Services-Konfiguration“ – Registerkarte „Allgemein“ konfiguriert werden. Der Bereich „Parserkonfiguration“ bietet die Möglichkeit zur Aktivierung oder Deaktivierung der auf dem Decoder zu verwendenden Parser sowie die Beschränkung der vom Parser erstellten Metadaten.

Außerdem gibt es mehrere vom Benutzer konfigurierbare Parsertypen:

- GeoIP: Dieser Parser verknüpft die IP-Adressen mit geographischen Standorten.
- Search: Dieser Parser kann vom Benutzer konfiguriert werden und generiert Metadaten durch Suchen nach vordefinierten Schlüsselwörtern und regulären Ausdrücken.
- FLEXPARSE (veraltet): Dies ist eine generische Parserdefinitionssprache zur Erweiterung der vorhandenen Anwendungsprotokollunterstützung des Decoders. Dieser Parser ist standardmäßig deaktiviert (siehe Aktivieren oder Deaktivieren der Lua- und Flex-Parsersysteme).
- Lua: Dieser Parser wird mithilfe der Lua-Skripterstellungssprache zur Erweiterung der vorhandenen Anwendungsprotokollunterstützung des Decoders definiert.
- enVision: Dieser Anwendungsparser unterstützt den Log Decoder und generiert Metadaten durch das Durchsuchen von Protokolldateien.
- SNORT®: Dieser Parser unterstützt die Nutzlast-Erkennungsfunktionen von SNORT®-IDS-Regeln.

In der Ansicht „Services-Konfiguration“ > Registerkarte „Parser“ können Sie bereitgestellte Parser in einem Decoder anzeigen, Parser hochladen und bereitgestellte Parser löschen Die Benutzeroberfläche enthält auch einen Hinweis darauf, ob der Parser von Live-Services stammt, durch NetWitness Suite installiert wurde oder manuell hochgeladen wurde. Parser können hinzugefügt und entfernt werden, während ein Decoder ausgeführt wird, ohne die Erfassung zu beeinträchtigen.

Außerdem können Sie Parser mit NetWitness Suite Live-Services herunterladen.

Konfigurieren von Feeds

NetWitness Suite verwendet Feeds zum Erstellen von Metadaten, die auf extern definierten Metadatenwerten beruhen. Ein Feed ist eine Liste von Daten, die bei der Erfassung oder Verarbeitung von Sitzungen mit diesen abgeglichen werden. Bei jedem erfolgreichen Abgleich werden zusätzliche Metadaten erstellt. Mit diesen Daten können bösartige IPs identifiziert und klassifiziert werden oder zusätzliche Unternehmensinformationen, wie Abteilung und Standort, basierend auf internen Netzwerkzuweisungen einbezogen werden. Einige Beispiele für Feeds sind Bedrohungsfeeds zur Identifizierung von BOTNets, DHCP-Zuordnungen oder auch Active Directory-Informationen wie physischer Standort oder logische Abteilung.

Sie können das Modul Live in NetWitness Suite verwenden, um Feeds aus externen Quellen zu erhalten. Eine Übersicht über das Contentmanagementtool Live finden Sie im *Handbuch Live-Services-Management* unter „Live-Inhalte in NetWitness Suite“.

In der NetWitness Suite-Benutzeroberfläche können Sie die Liste der zurzeit bereitgestellten Feeds zusammen mit einem Hinweis darauf sehen, ob ein von Live stammender Feed über NetWitness Suite installiert wurde oder manuell heruntergeladen wurde. Feeds können hinzugefügt, entfernt und aktualisiert werden, während ein Decoder ausgeführt wird, ohne die Erfassung zu beeinträchtigen.

verfügt über einen Assistenten für die schnelle Erstellung und Bereitstellung von benutzerdefinierten Decoderfeeds auf der Basis einer deterministischen Logik, die die für die ausgewählten Decoder und Log Decoder spezifischen Metaschlüssel bereitstellt. Auch wenn der Assistent Benutzer sowohl durch die Schritte zur Erstellung eines bedarfsorientierten Feeds als auch eines wiederkehrenden Feeds führt, ist es hilfreich, das Format und den Inhalt einer Feeddatei bei der Erstellung eines Feeds zu verstehen.

NetWitness Suite verfügt über einen Assistenten für benutzerdefinierte Feeds, der die Erstellung und Verwaltung benutzerdefinierter Feeds optimiert und sie an ausgewählte Decoder und Log Decoder überträgt. Darüber hinaus können Sie vorhandene Feeddateien herunterladen und die Dateien bearbeiten. Anschließend können Sie den Feed bearbeiten oder einen neuen Feed mithilfe der bearbeiteten Datei erstellen.

Definition benutzerdefinierter Feeds – Dateistruktur

Der Assistent von NetWitness Suite für benutzerdefinierte Feeds ermöglicht eine schnelle Erstellung und Bereitstellung von benutzerdefinierten Decoderfeeds auf der Basis einer deterministischen Logik, die die für die ausgewählten Decoder und Log Decoder spezifischen Metaschlüssel bereitstellt. Auch wenn der Assistent Benutzer sowohl durch die Schritte zur Erstellung eines bedarfsorientierten Feeds als auch eines wiederkehrenden Feeds führt, ist es hilfreich, das Format und den Inhalt einer Feeddatei bei der Erstellung eines Feeds zu verstehen.

Feeddateinamen in RSA NetWitness Suite haben das Format `<filename>.feed`. Um einen Feed zu erstellen, erfordert NetWitness Suite eine Feeddatendatei im `csv` - oder `.xml`-Format und eine Feeddefinitionsdatei im `.xml`-Format, in der die Struktur einer Feeddatendatei beschrieben ist. Der Assistent für benutzerdefinierte Feeds kann die Feeddefinitionsdatei basierend auf einer Feeddatendatei oder basierend auf einer Feeddatendatei und der entsprechenden Feeddefinitionsdatei 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 im Assistenten für benutzerdefinierte Feeds 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-Assistent für benutzerdefinierte Feeds bietet Optionen, mit denen Sie die Struktur der Feeddefinitionsdatei definieren können. Diese entsprechen direkt Attributen in der Feeddefinitionsdatei (.xml).

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
(Registerkarte „Feed definieren“) Feedtyp	Auswählen: **Standard** – zum Definieren eines Feeds auf Grundlage einer CSV-formatierten Feeddatendatei **STIX** – zum Definieren eines Feeds auf Grundlage einer STIX-formatierten XML-Datei
(Registerkarte „Feed definieren“) Typ der Feedaufgabe	Auswählen: **Ad-hoc** – zur Erstellung eines Feeds nach Bedarf **Wiederkehrend** – zur dauerhaften Aktualisierung der CSV- oder XML-Datei und deren Speicherung an einem Ort, der für NetWitness Suite zugänglich ist, sodass NetWitness Suite eine Datei in regelmäßigen Abständen herunterlädt und an nachgelagerte Geräte überträgt.

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
(Registerkarte Feed definieren) **Name**	Der benutzerdefinierte Feedname in der Feeddatendatei. Er entspricht dem Attribut `flatfeedfile name` in der Feeddefinitionsdatei. Zum Beispiel „Dynamic DNS Test Feed“. **Hinweis:** Sie können für den Namen des benutzerdefinierten Feeds Sonderzeichen verwenden.
(Registerkarte Feed definieren) **Datei /Durchsuchen**	Dies ist der Name der Feeddatendatei. Er entspricht dem Attribut `flatfeedfile path` in der Feeddefinitionsdatei. Zum Beispiel: `dynamic_dns.csv`
(Registerkarte Erweiterte Optionen) **XML-Feeddatei**	Der Name der Feeddefinitionsdatei. Beispiel: `dynamic_dns.xml`.
(Registerkarte Erweiterte Optionen) **Trennzeichen**	Das verwendete Trennzeichen, um die Attribute in der Feeddatendatei voneinander zu trennen. Er entspricht dem `latfeedfile separator` in der Feeddefinitionsdatei. Zum Beispiel ein Komma.
(Registerkarte Erweiterte Optionen) **Kommentar**	Das verwendete Zeichen, um einen Kommentar in der Feeddatendatei zu kennzeichnen. Er entspricht dem Attribut `flatfeedfile comment` in der Feeddefinitionsdatei. Zum Beispiel: `#`

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
(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 (z. B. 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 (z. B. 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 „Rückrufschlüssel“ 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.
(Registerkarte „Spalten definieren“, „Index definieren“) **Servicetyp**	Für einen Nicht-IP-Index, der ganzzahlige Servicetyp, um Metasuchwerte zu filtern. Er entspricht dem Attribut `MetaCallback apptype` in der Feeddefinitionsdatei. Ein Wert von 0 zeigt an, dass nicht nach Servicetyp gefiltert wird.

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
(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 `MetaCallback truncdomain`-Attribut. Wenn der Wert `www.example.com` lautet, wird er gekürzt auf `example.com`. Ein Wert **Falsch** bedeutet, dass nicht gekürzt wird, **Wahr** bedeutet, dass gekürzt wird.
(Registerkarte „Spalten definieren“, „Index definieren“) **Rückrufschlüssel**	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 `MetaCallback name` 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.
(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.

NetWitness Suite-Parameter	Feeddefinitionsdatei-Äquivalent
(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 `Field key` in der Feeddefinitionsdatei. Ein Schlüssel gilt nur für ein Feld, dessen Typ auf `value` eingestellt ist. In der Feeddefinitionsdatei gibt es eine Liste von `LanguageKeys` von `index.xml` oder einen zusammenfassenden Namen, 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.

Beispieldateien für einen MetaCallback-Feed mithilfe des CIDR-Indexbereichs für IPv4 und IPv6

Diese Beispieldateien zeigen die Verwendung der CIDR-Indexbereiche für IPv4 und IPv6 in benutzerdefinierten MetaCallback-Feeds. 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 Feeds

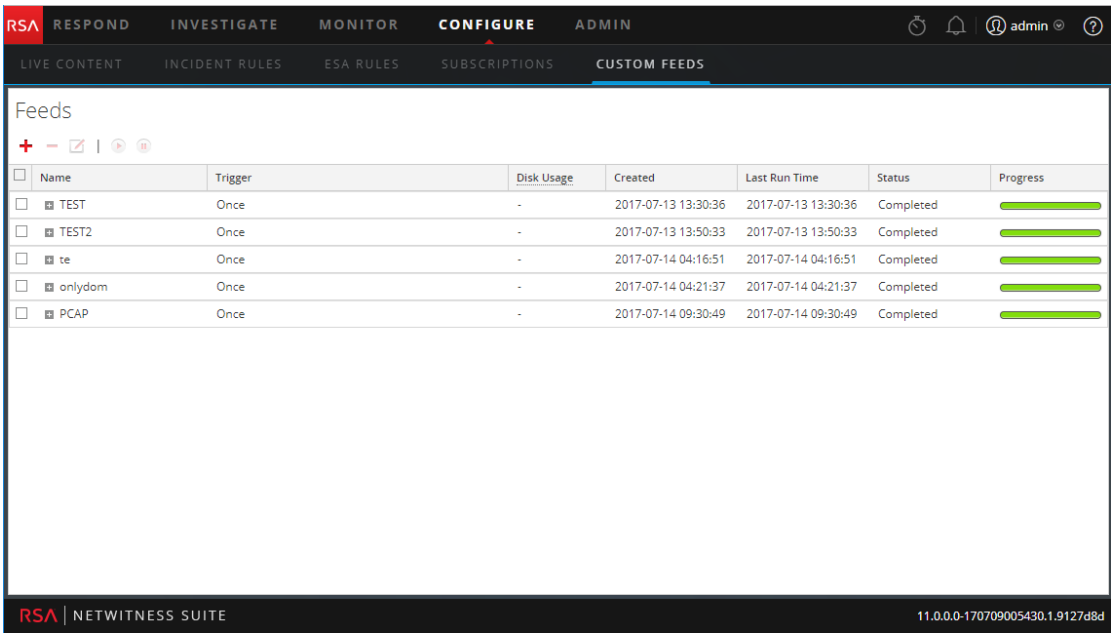
Mit dem Assistenten für benutzerdefinierte Feeds können Sie einen benutzerdefinierten Feed erstellen. Zum Abschluss dieses Verfahrens benötigen Sie eine Feeddatendatei im `.csv`- oder `.xml`-Format. Wenn Sie auch eine zugeordnete Feeddefinitionsdatei im `.xml`-Format haben, die die Struktur der Feeddatendatei 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.

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.

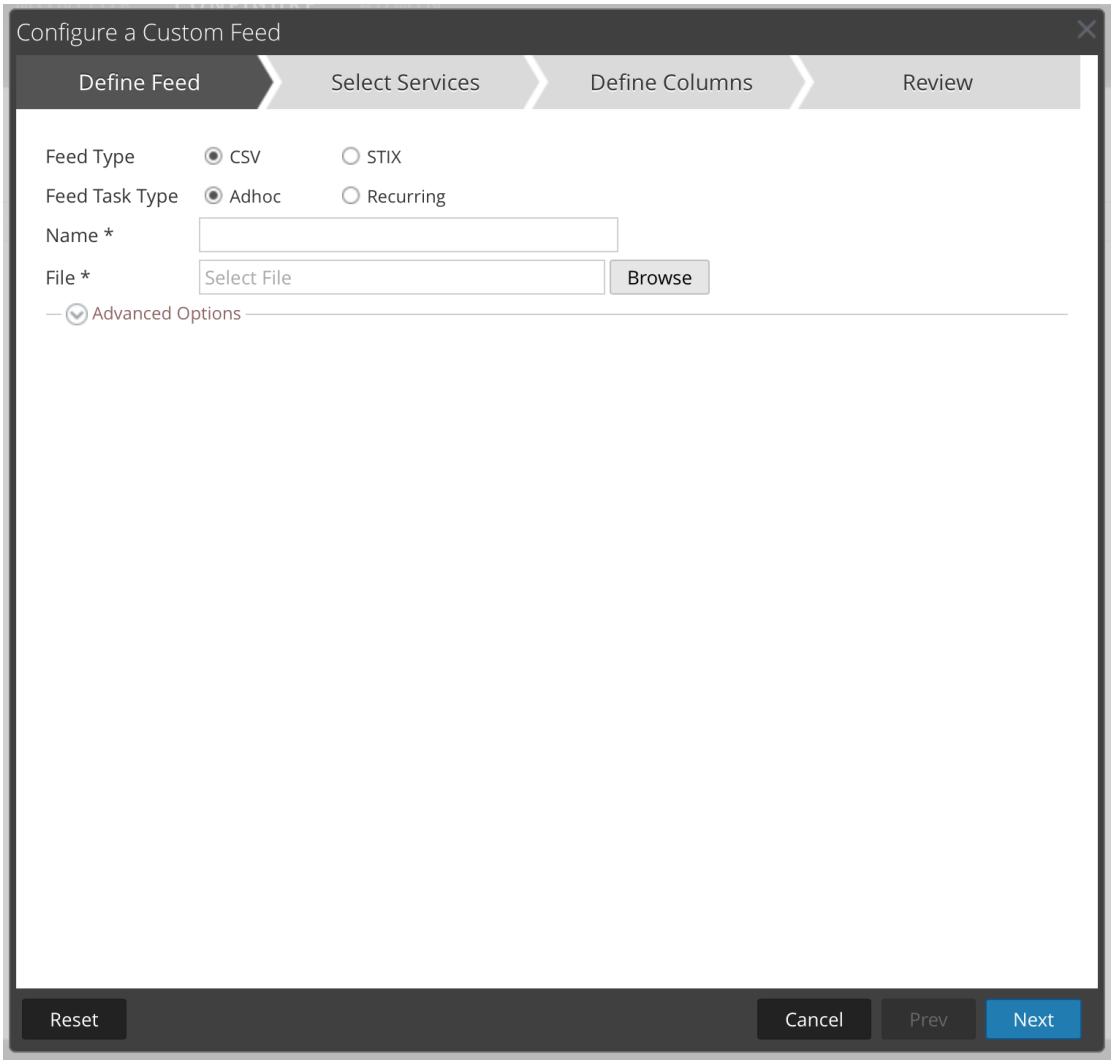
Für einen bedarfsorientierten benutzerdefinierten Feed müssen die Feeddatendatei und optional die Feeddefinitionsdatei (`.xml`) auf dem lokalen Dateisystem verfügbar sein. Für einen wiederkehrenden benutzerdefinierten Feed müssen die Dateien unter einer URL verfügbar sein, auf die der NetWitness Suite-Server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

So erstellen Sie einen benutzerdefinierten Feed:

1. Navigieren Sie zu **Konfigurieren > Benutzerdefinierte Feeds** und klicken Sie im Bereich **Feeds** auf **+**.
   Die Ansicht der benutzerdefinierte Feeds wird angezeigt..



2. Klicken Sie auf **Benutzerdefinierter Feed** und dann auf **Weiter**.
   Der Assistent „Benutzerdefinierten Feed konfigurieren“ wird mit geöffnetem Formular „Feed definieren“ angezeigt.



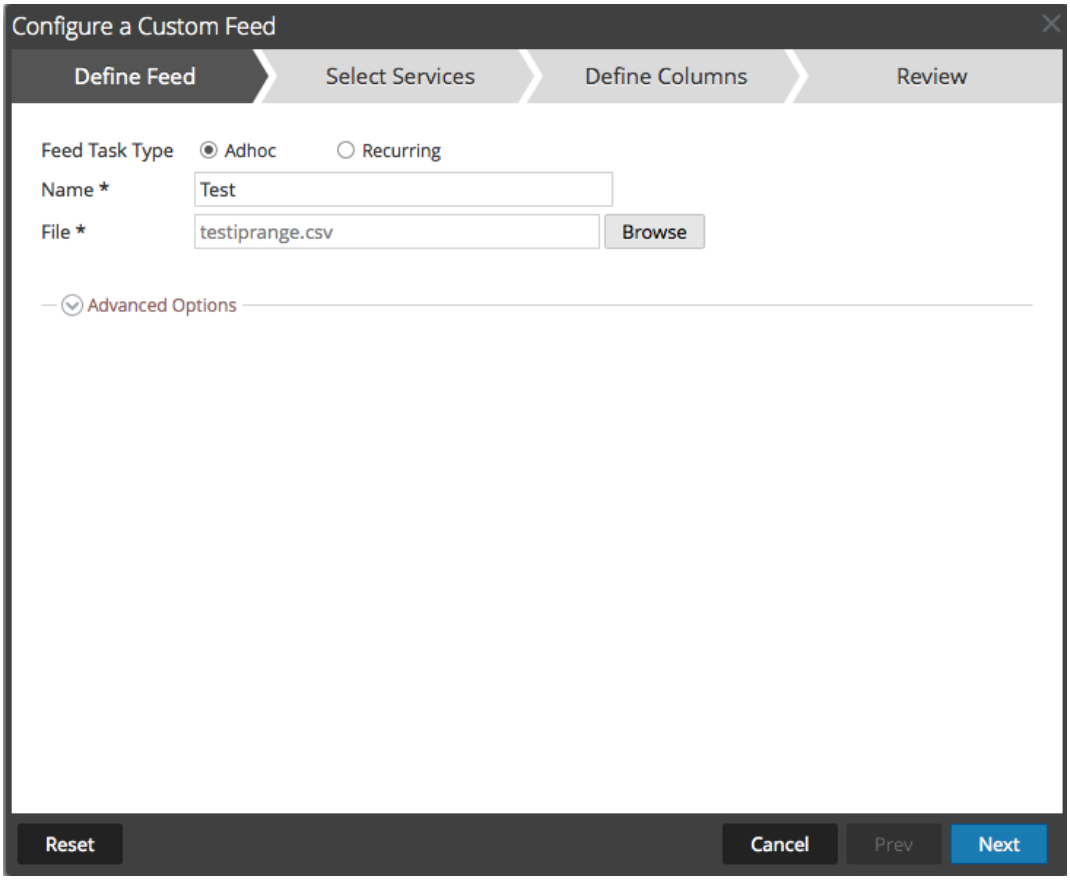
3. Wählen Sie den Feedtyp aus: **CSV** oder **STIX**.
4. Definieren Sie einen Feed auf Grundlage einer `.csv`-formatierten Feeddatendatei, indem Sie im Feld **Feed-Typ** die Option **Standard** auswählen.

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.

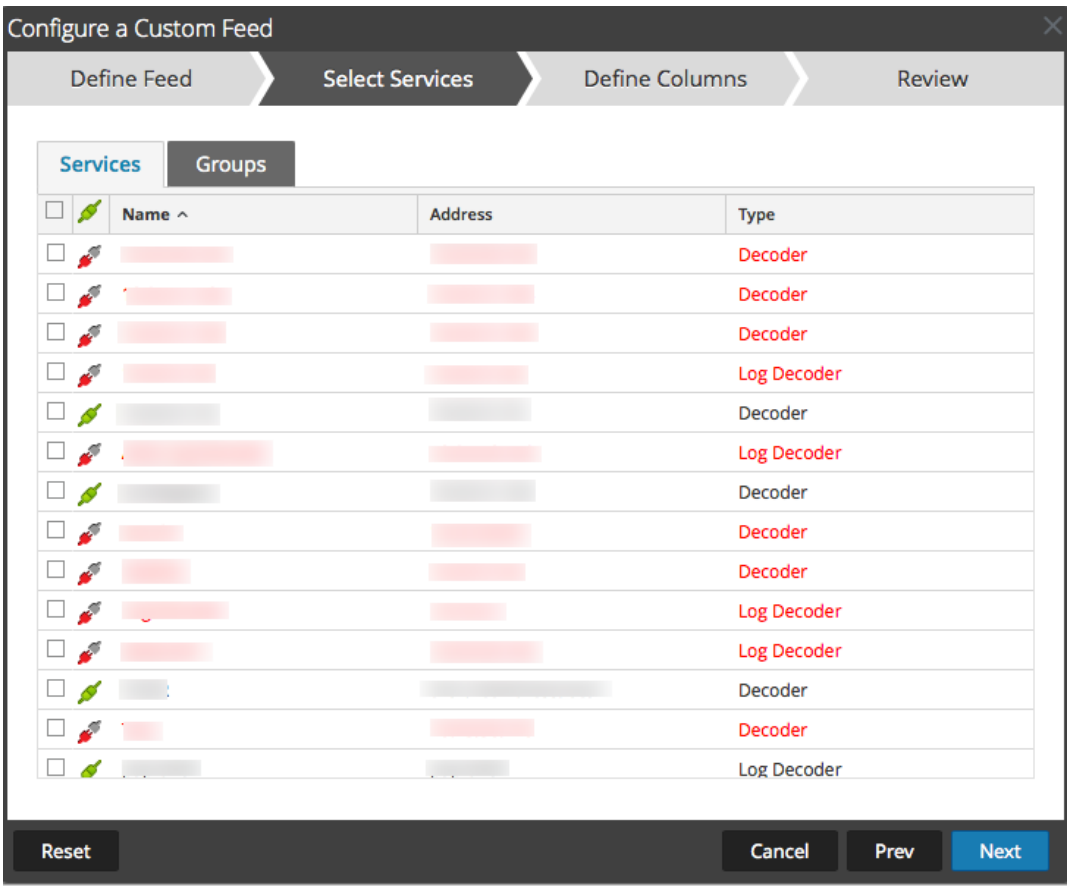
      Erweiterte Optionen werden angezeigt.



   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

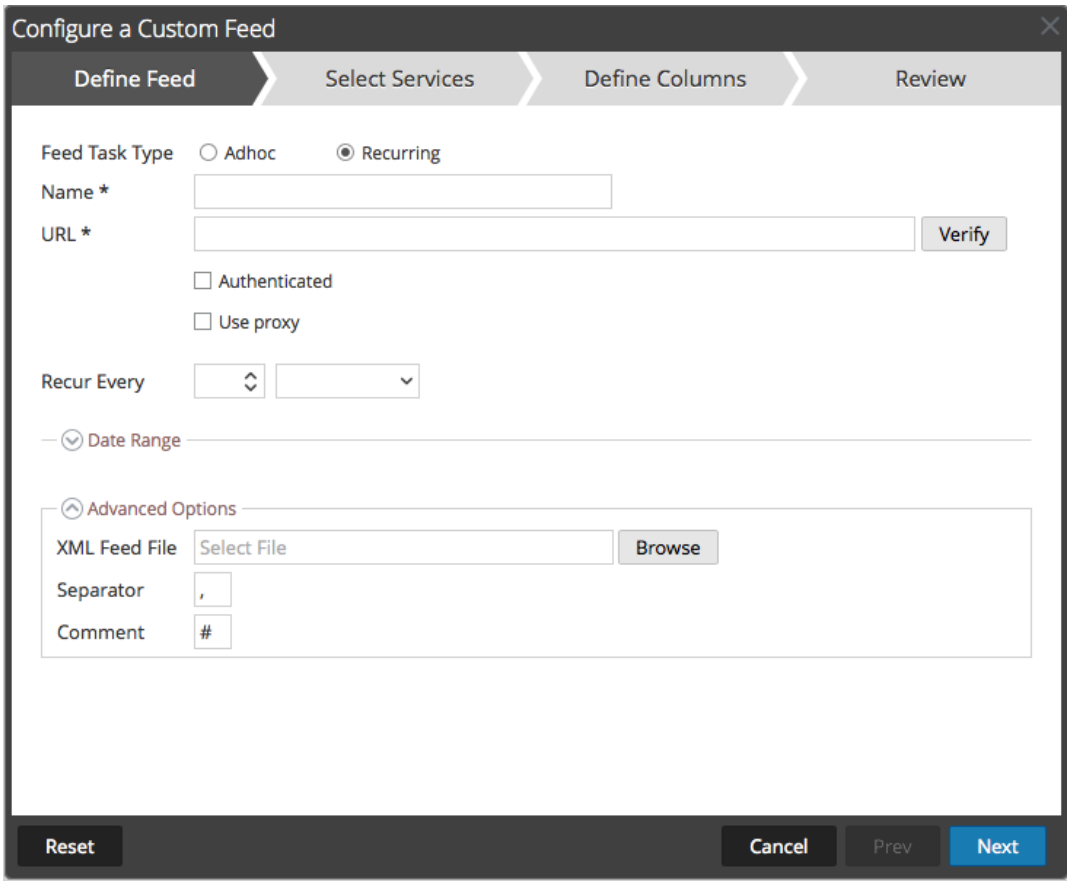
für einen Feed, der auf einer Feeddatendatei ohne Feeddefinitionsdatei basiert. Wenn Sie einen Feed definieren, der auf einer Feeddefinitionsdatei basiert, ist die Registerkarte Spalten definieren nicht erforderlich.



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 überprüft den Speicherort, an dem die Datei gespeichert ist, sodass bei jedem erneuten Aufruf automatisch nach der neuesten Datei gesucht werden kann.

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

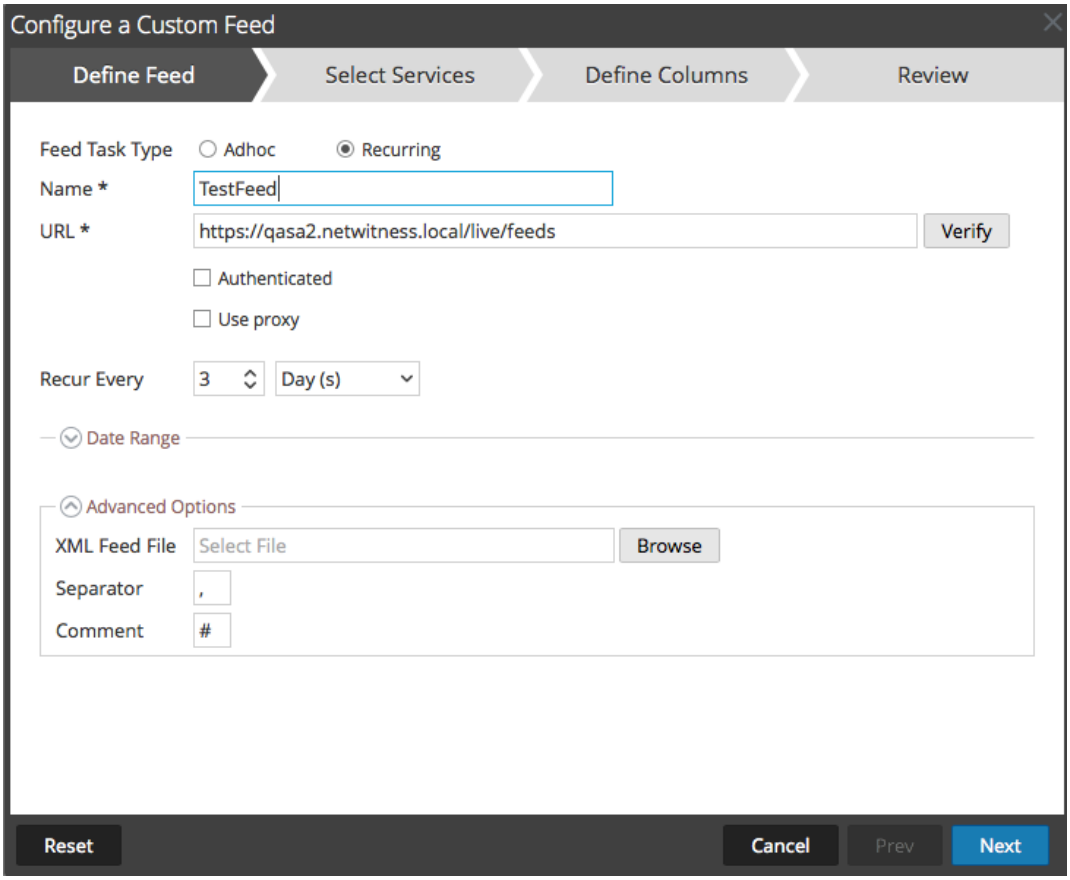
NetWitness Suite stellt Ihren Benutzernamen und Ihr Passwort zur Authentifizierung bei der URL bereit.

d. Wenn der NetWitness-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.



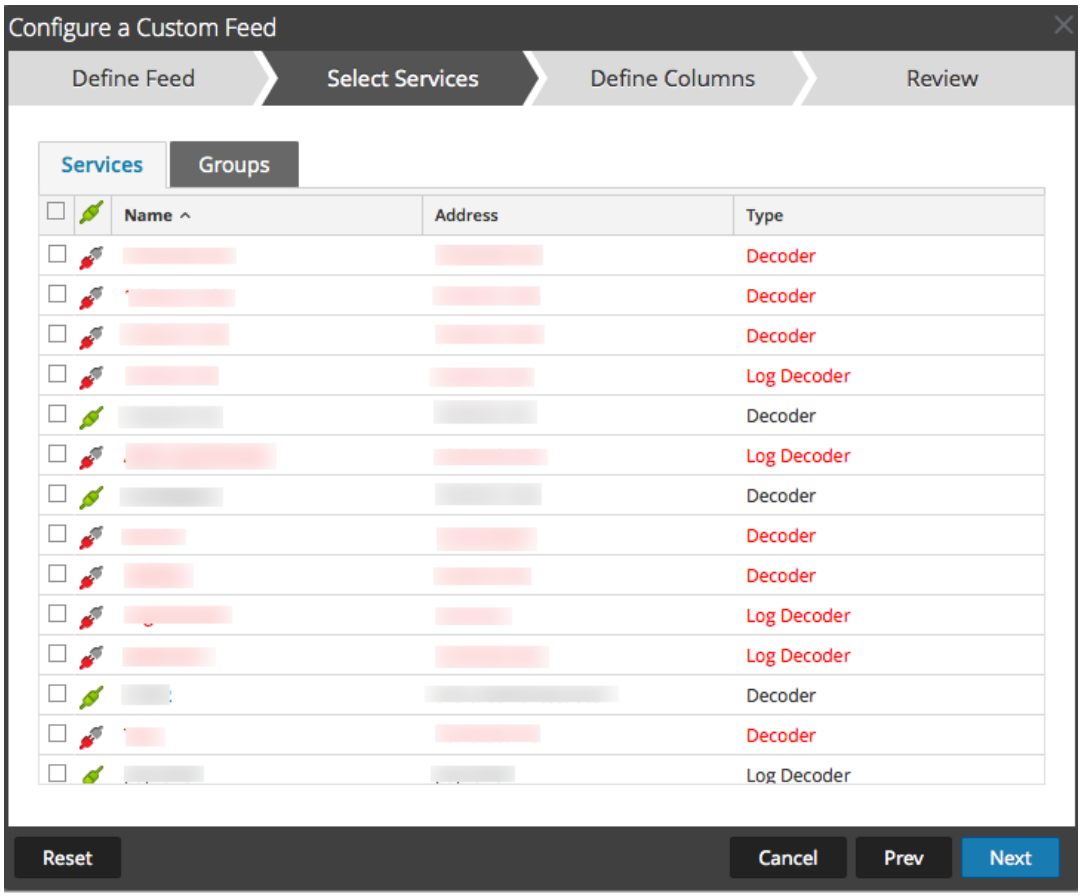
7. (Bedingungsabhängig) Wenn Sie einen Feed auf Basis einer XML-Feeddatei definieren möchten, gehen Sie wie folgt vor:

- 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**.

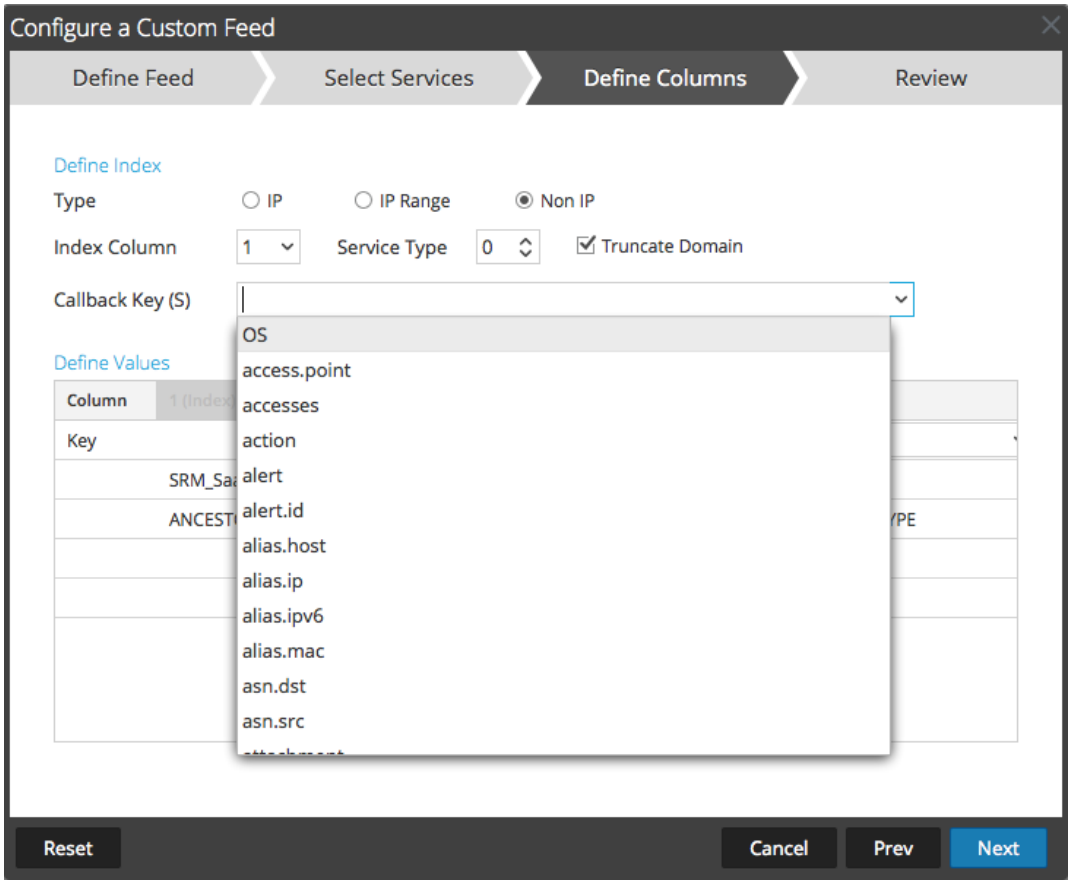
      Das Formular Spalten definieren wird angezeigt.

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

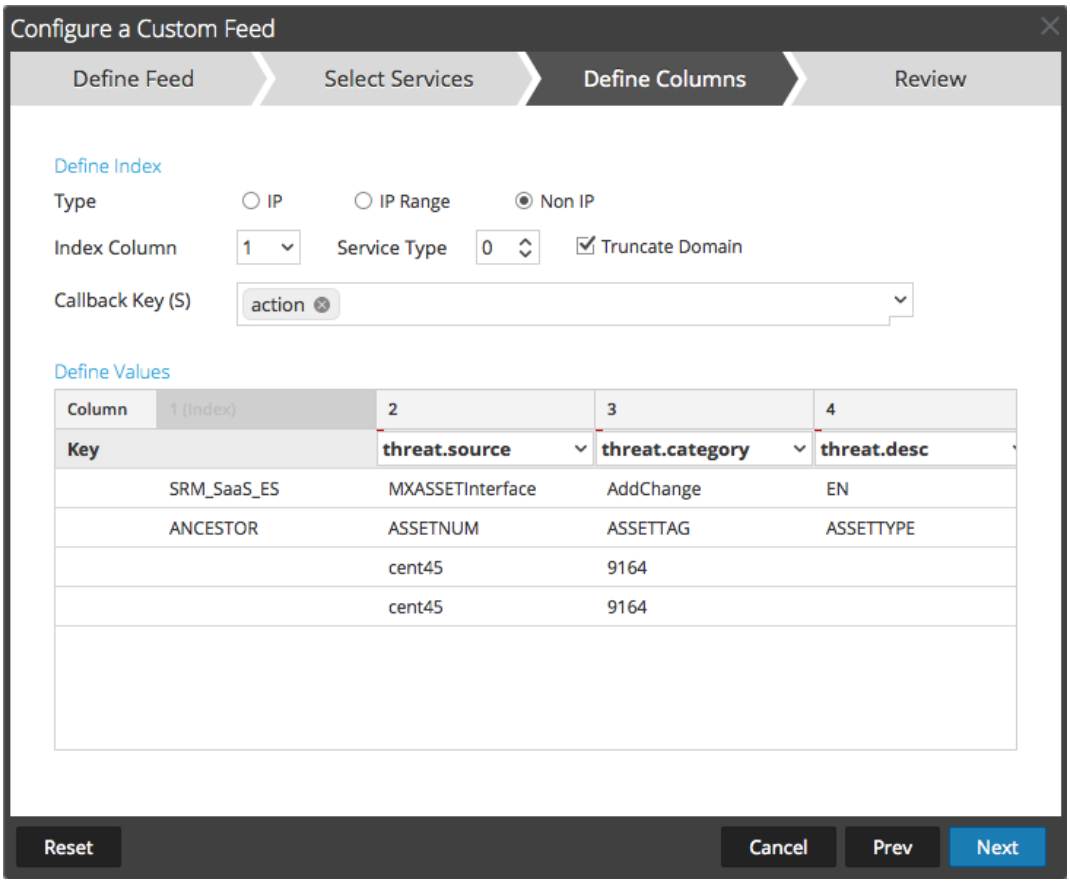
a. Definieren Sie den Indextyp: **IP**, **IP-Bereich** oder **Nicht IP** und wählen Sie die Indexspalte aus.

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.

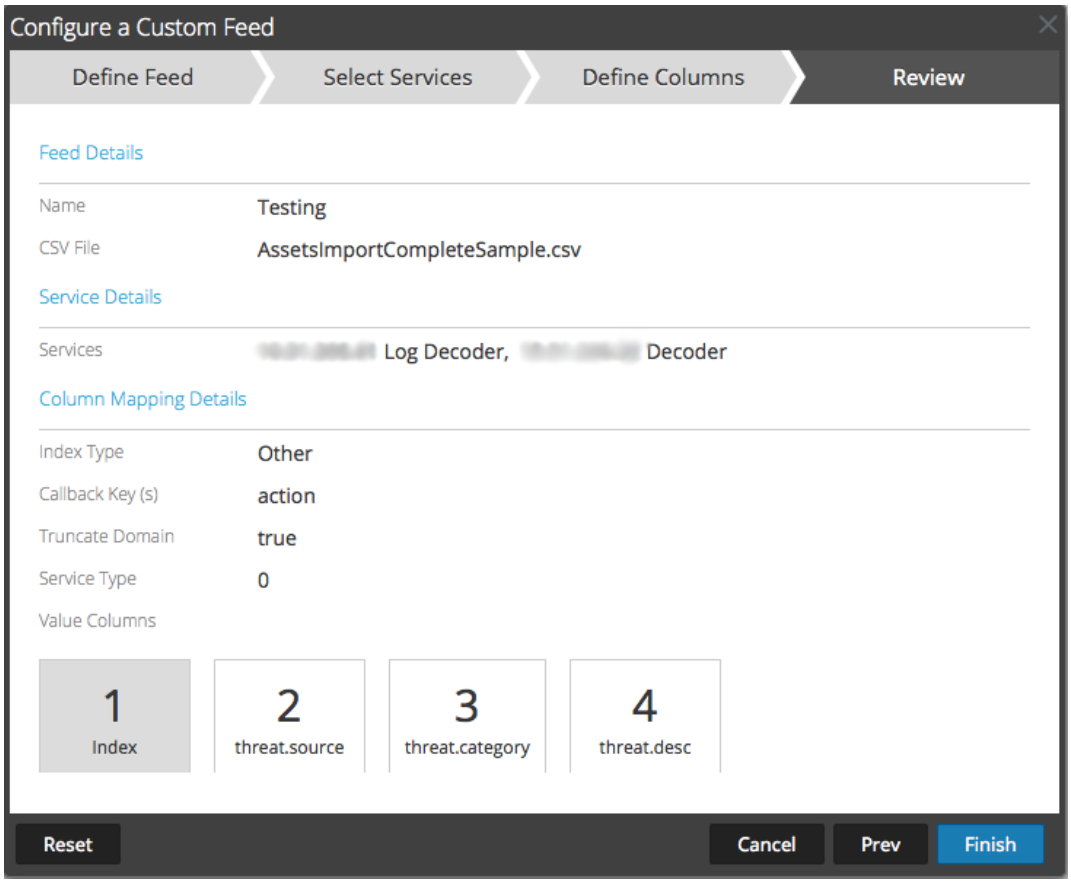


d. Wählen Sie in der Drop-down-Liste den Sprachschlüssel aus, der auf die Daten in jeder Spalte angewendet werden soll. Die in der Drop-down-Liste aufgeführten Metadaten basieren auf den für die Servicedefinitionswerte verfügbaren Metadaten. Sie können auch andere Metadaten hinzufügen, die auf erweitertem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



e. Klicken Sie auf **Weiter**.

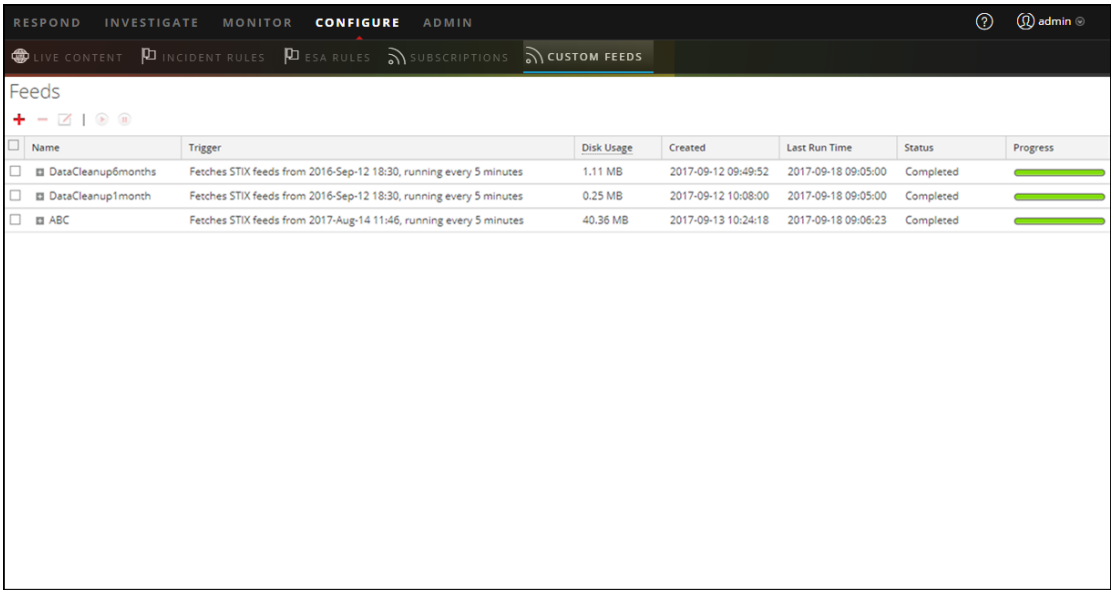
Das Formular Überprüfung wird angezeigt.



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.

    ..



Erstellen eines benutzerdefinierten STIX-Feeds

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/.

Sie können einen benutzerdefinierten Feed mithilfe einer STIX-formatierten Feeddatendatei (`.xml`) in RSA NetWitness Suite erstellen. NetWitness Suite unterstützt nur die Versionen 1.0, 1.1 und 1.2 von Structured Threat Information Expression (STIX).

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 des Typs „Indicator“ oder „Observable“ unterstützt, die Eigenschaften enthalten wie z. B. IP-Adressen, Datei-Hashes, Domain-Namen, URIs und E-Mail-Adressen. Die Eigenschaftswerte des Operators „gleich“ werden unterstützt. Attribute wie z. B. Typ und Titel werden ebenfalls von STIX gelesen. Eine STIX-Datei mit einem einzelnen STIX_Package wird unterstützt.

TAXII (Trusted Automated eXchange of Indicator Information) ist der wichtigste Transportmechanismus für Informationen zu Cyberbedrohungen, die in STIX dargestellt werden. Unternehmen können mithilfe der TAXII-Services Informationen zu Cyberbedrohungen auf sichere und automatisierte Weise freigeben.

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

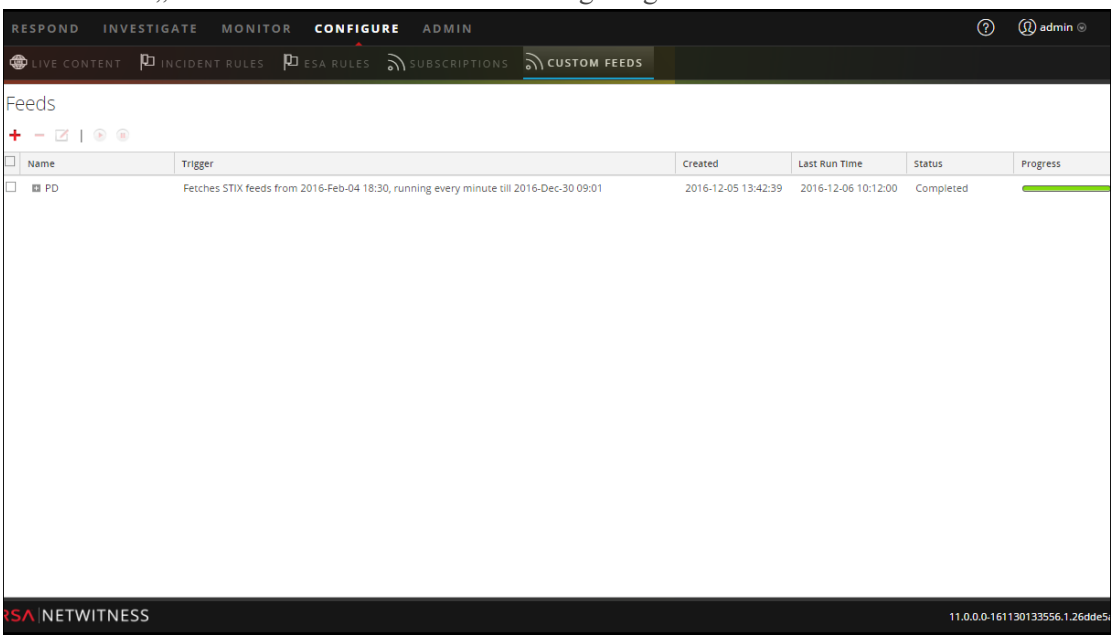
Abgesehen vom TAXII-Server können sich STIX-Daten auch auf einem REST-Server befinden. Sie können die STIX-Datei vom REST-Server durch Angabe der URL des REST-Servers abrufen. Zum Beispiel `http://stixrestserver.internal.com`.

Für einen bedarfsorientierten benutzerdefinierten Feed müssen die STIX-Feeddatendatei und optional die Feeddefinitionsdatei im `.xml`-Format 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:

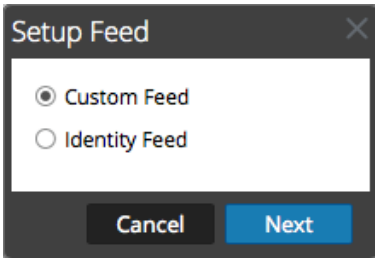
1. Navigieren Sie zu **Konfigurieren > Benutzerdefinierter Feed**.

   Die Ansicht „Benutzerdefinierter Feed“ wird angezeigt.



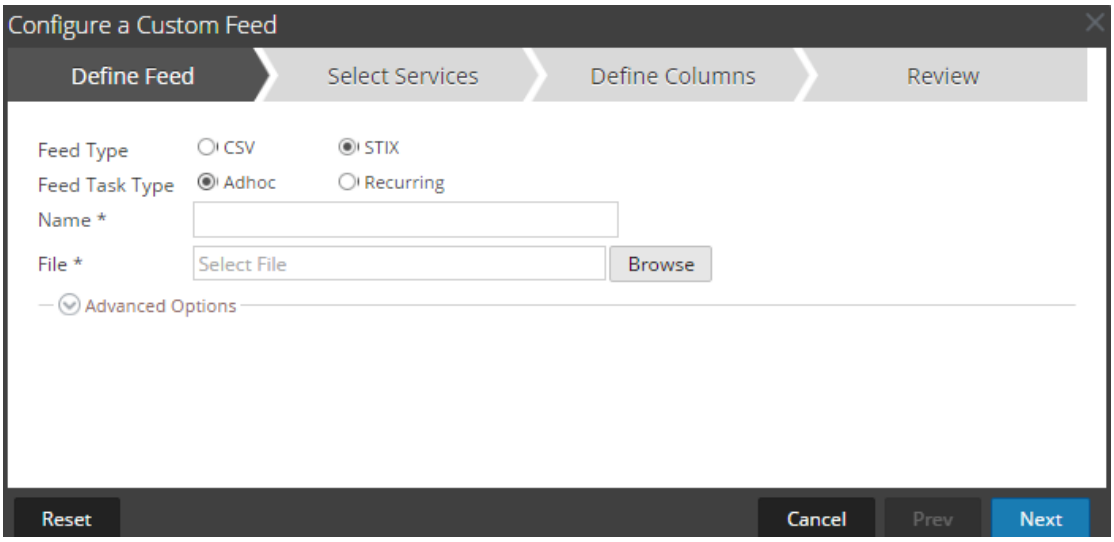
2. Klicken Sie in der Symbolleiste auf +.

   Das Dialogfeld Feed einrichten wird angezeigt.



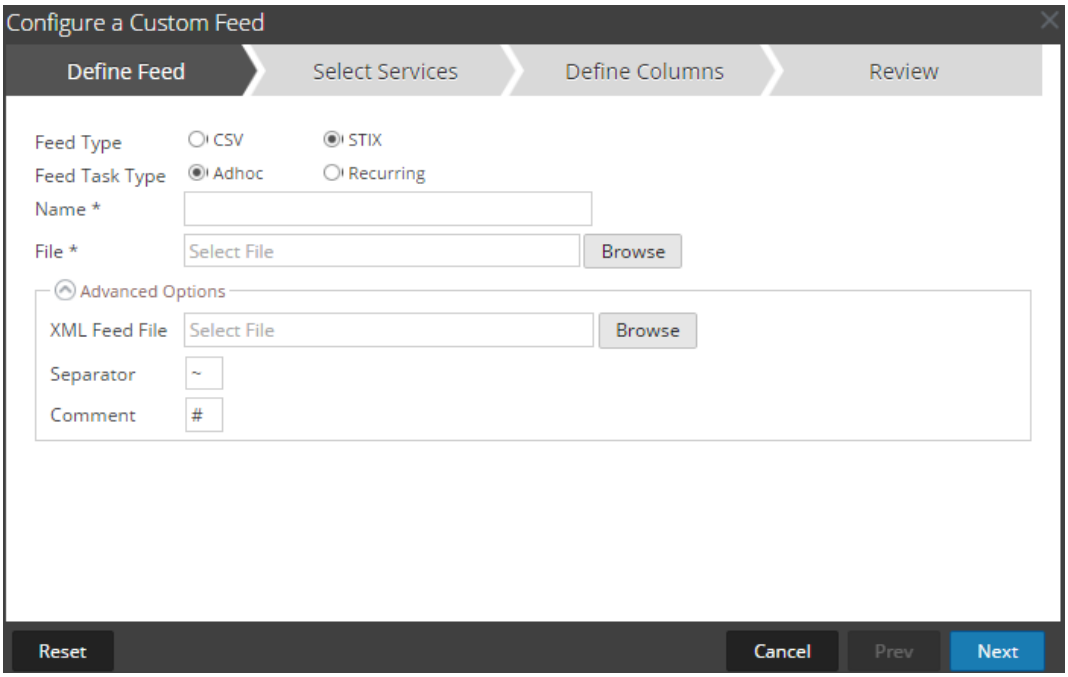
3. Um den Feedtyp auszuwählen, klicken Sie auf **Benutzerdefinierter Feed** und auf **Weiter**.

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

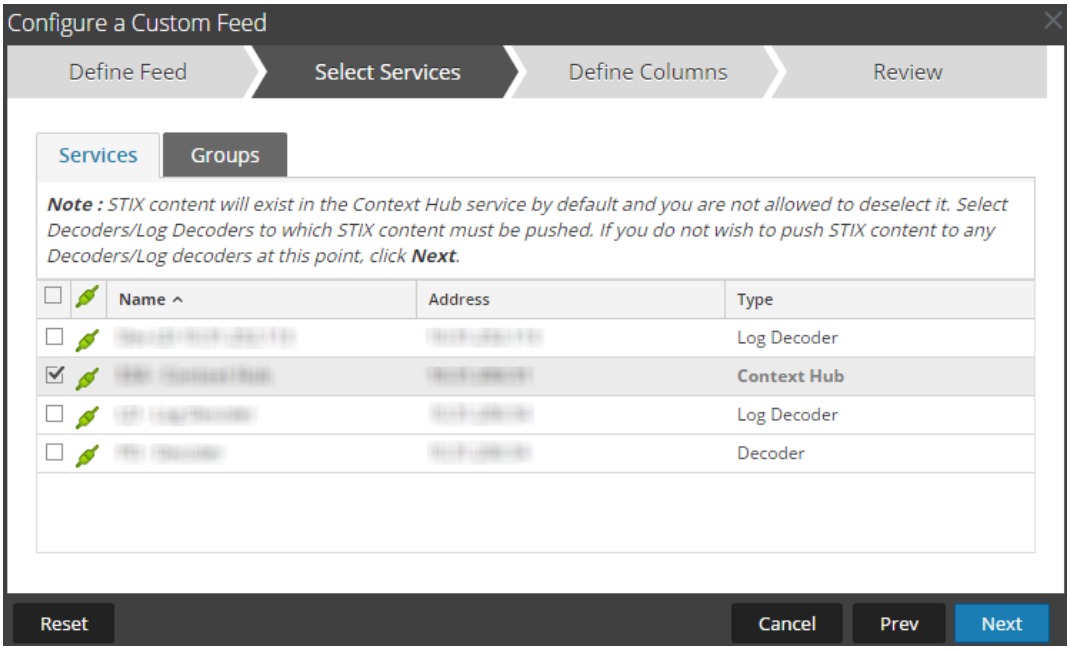


4. Definieren Sie einen Feed basierend auf einer STIX-formatierten `.xml`-Datei. Wählen Sie **STIX** im Feld **Feed-Typ** aus.
5. Um eine bedarfsorientierte Feedaufgabe zu definieren, die einmal ausgeführt wird, wählen Sie im Feld **Typ der Feedaufgabe** die Option **Ad-hoc** aus und fahren Sie mit einer 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.

      Die Erweiterten Optionen werden angezeigt.



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

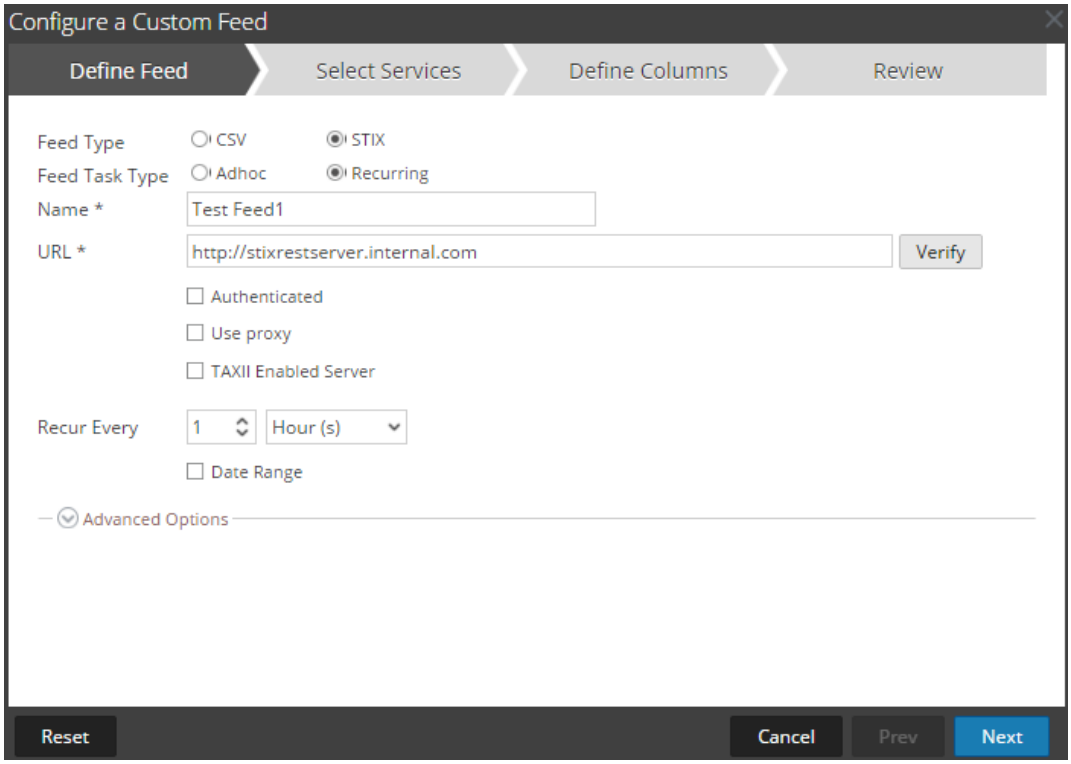


6. So definieren Sie einen wiederkehrenden Feed, der innerhalb eines bestimmten

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.



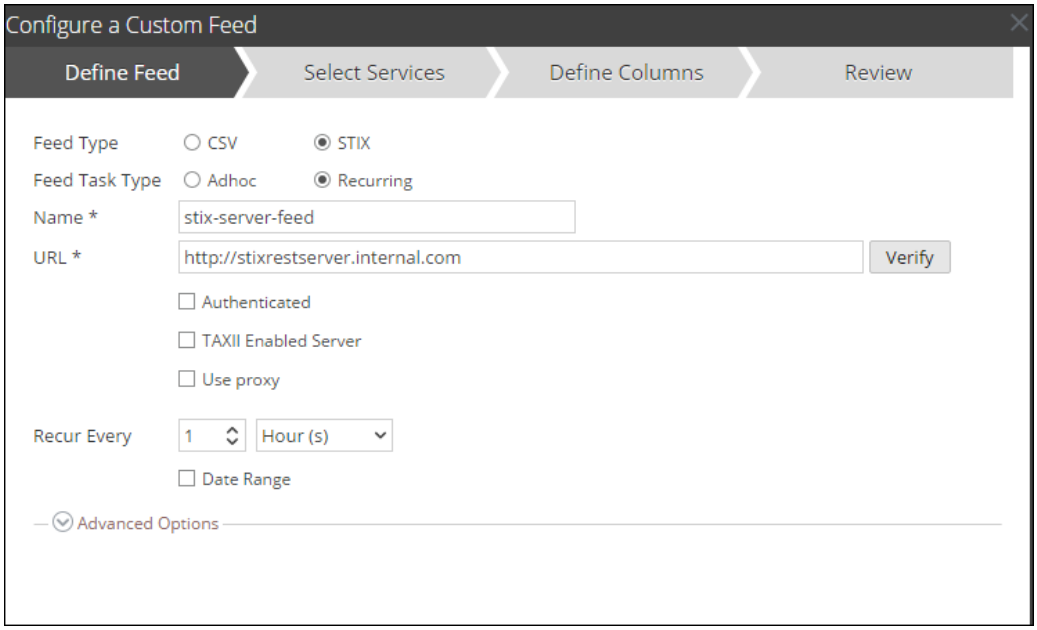
b. Gehen Sie im Feld **URL** wie folgt vor:

- Um einen wiederkehrenden Feed basierend auf STIX zu definieren, der STIX-Pakete von einem TAXII-Server abruft, geben Sie die URL des Erkennungsservices 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 basierend auf 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 neueste Datei abrufen.

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

d. Für die Clientauthentifizierung mit der REST-URL klicken Sie 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 **Für TAXII aktivierter Server**, 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, basierend auf Ihren 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, es wird aber pro TAXII-Server nur ein Konto (Benutzername und Passwort) unterstützt.

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*. (Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.) 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“, „Für TAXII aktivierter Server“ usw. konfiguriert sind, bevor Sie auf „Überprüfen“ klicken.

i. Führen Sie einen der folgenden Schritte aus, um das Intervall für Push-Vorgänge zum 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.

7. (Bedingungsabhängig) Wenn Sie einen Feed auf Basis einer XML-Feeddatei definieren möchten, gehen Sie wie folgt vor:

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

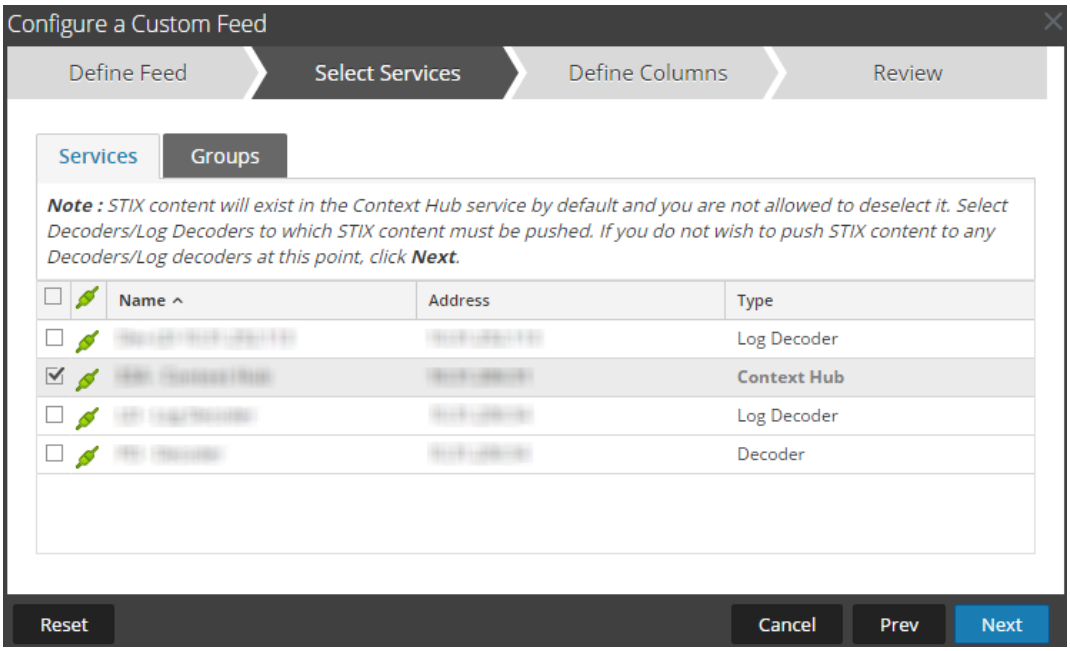
  Die Felder „Erweiterte Optionen“ werden angezeigt.
- Wählen Sie eine XML-Feeddatei aus dem lokalen Dateisystem und das **Trennzeichen** aus (Standard ist Komma), legen Sie die **Kommentarzeichen** fest, die in der Feeddatendatei verwendet werden (Standard ist #).
- Geben Sie im Feld **STIX-Daten entfernen, 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 Falle 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:
   „Das Abrufen der Beispieldaten dauert länger als erwartet. Wählen Sie eine der folgenden Optionen.“ Sie haben zwei Möglichkeiten: Sie können weiterhin warten oder eine Zuordnung ohne Beispieldaten vornehmen.

   - Wenn Sie auf **Weiter warten** klicken, wartet der Assistent für Feeds weiterhin, bis die Beispieldaten abgerufen werden oder ein Timeout (10 Minuten) erfolgt, je nachdem, was früher eintritt. Wenn ein Timeout erfolgt, werden keine Beispieldaten abgerufen.
   - Wenn Sie auf **Ohne Beispieldaten zuordnen** klicken, wird die Spalte für die Zuordnung ohne Beispieldaten angezeigt.

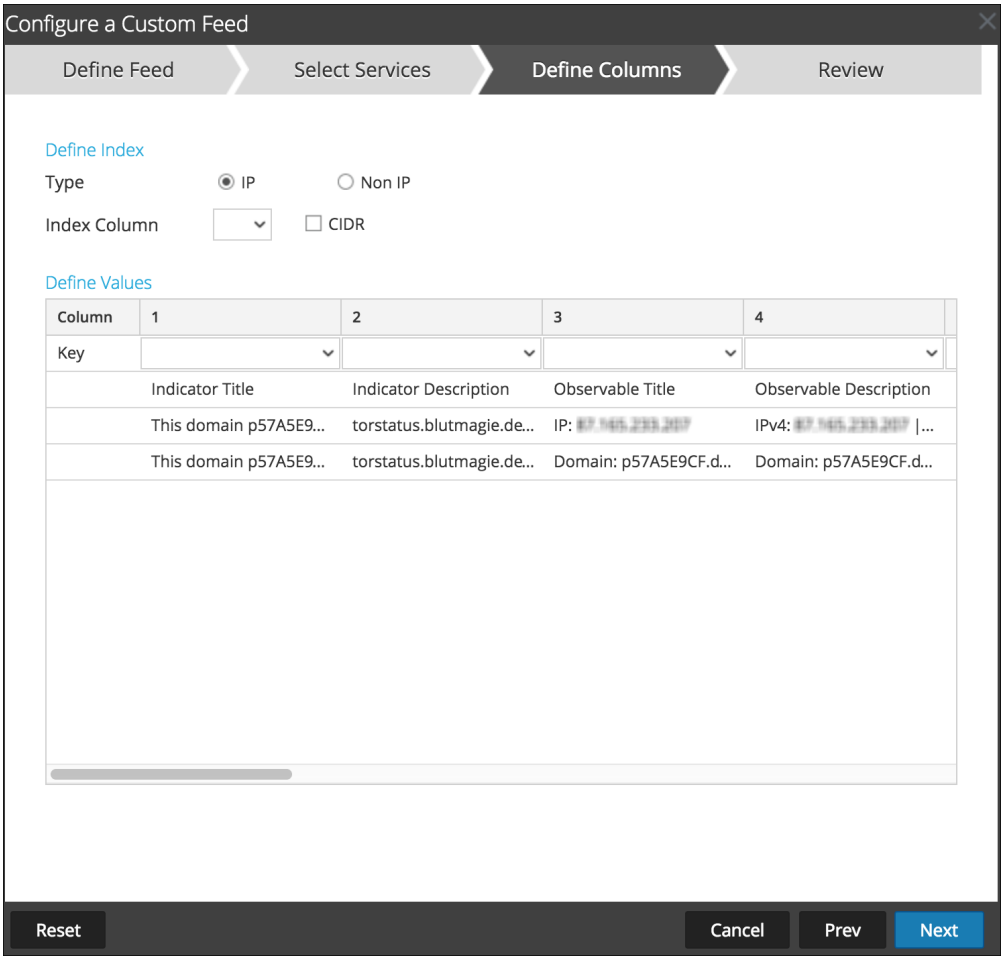
   Das Formular „Spalten definieren“ wird angezeigt.

9. So ordnen Sie 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** lautet, werden zusätzliche Einstellungen angezeigt. Wählen Sie den Servicetyp und die **Callback-Schlüssel** aus und wählen Sie optional **Domain abschneiden** aus.



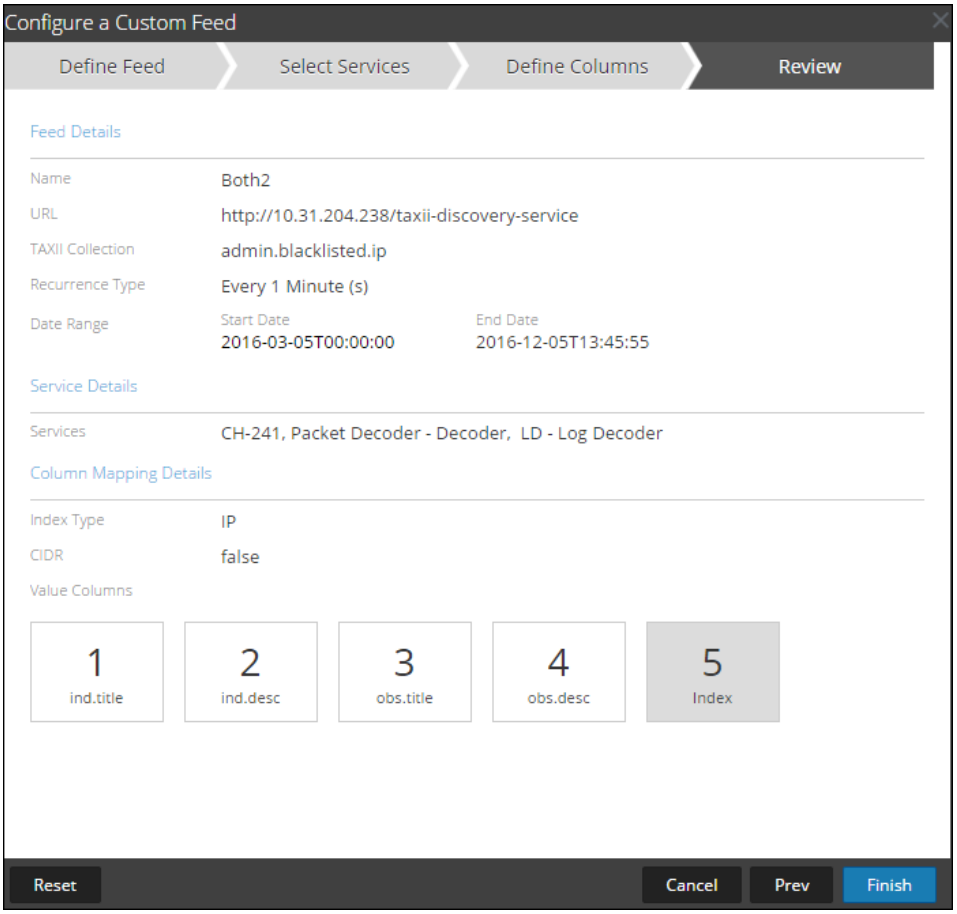
- Wenn der Indextyp „Nicht IP“ lautet, können Sie mehrere Indexspalten unter „Indexspalten“ auswählen. Die Werte aus allen ausgewählten Spalten werden in der ersten Indexspalte zusammengeführt, die Sie ausgewählt haben, und die zusammengeführten Werte werden für die Analyse an den Log Decoder übertragen. Beispiel: Wenn Sie unter „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.

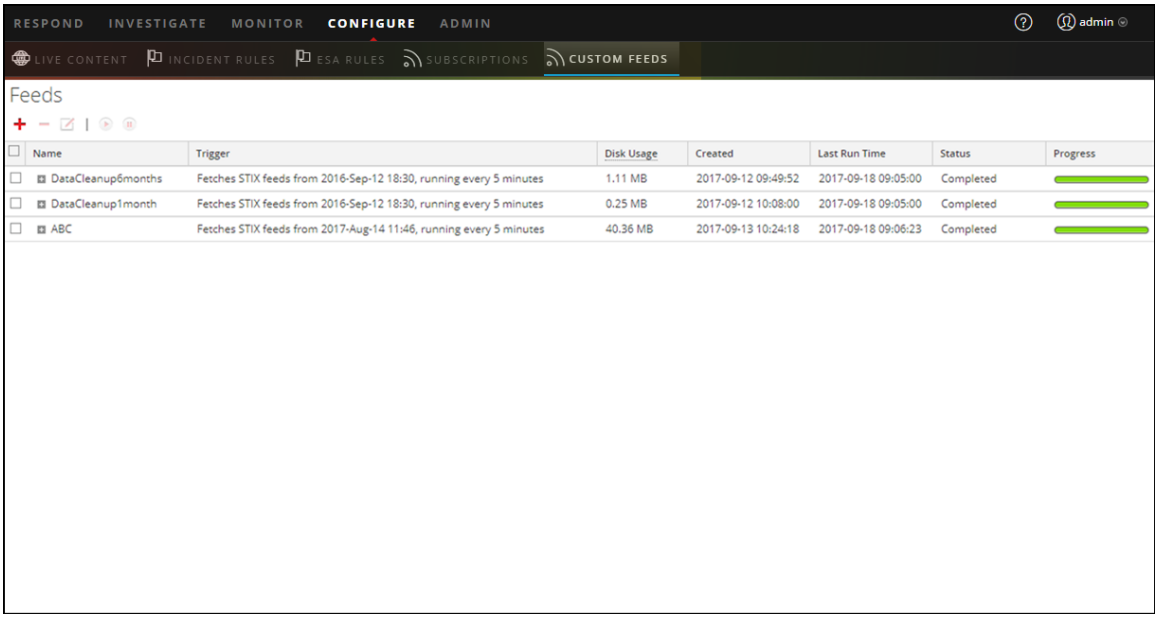


10. Bevor Sie auf **Fertigstellen** klicken, können Sie jederzeit Folgendes tun:

- 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*.

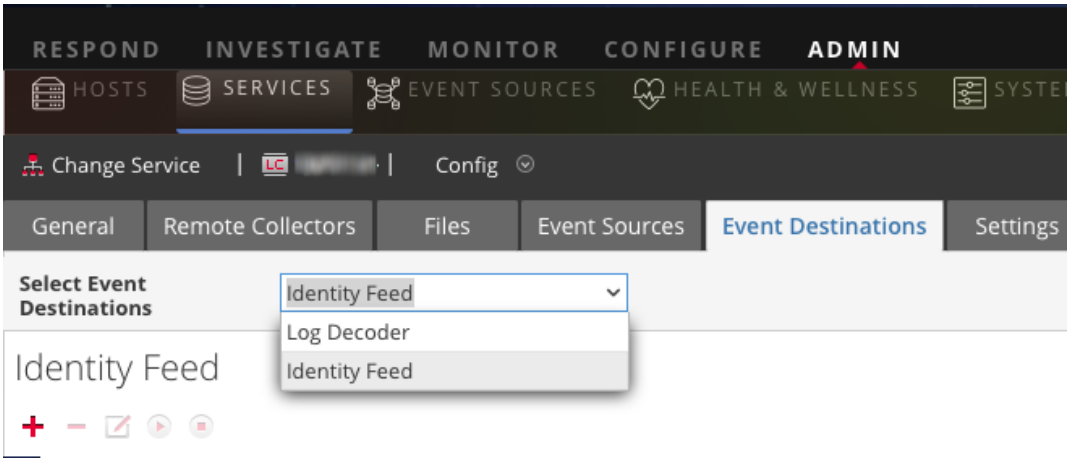
Erstellen von Identitätsfeeds

Sie können einen Identitätsfeed erstellen und ihn in ausgewählten Decodern und Log Decodern verwenden. Zum Erstellen eines Identitätsfeeds benötigen Sie Folgendes:

- einen Log Collector-Service mit einem Identitätsfeed-Ereignisprozessor haben
- einen Log Collector-Service mit konfigurierter und aktivierter Windows-Sammlung

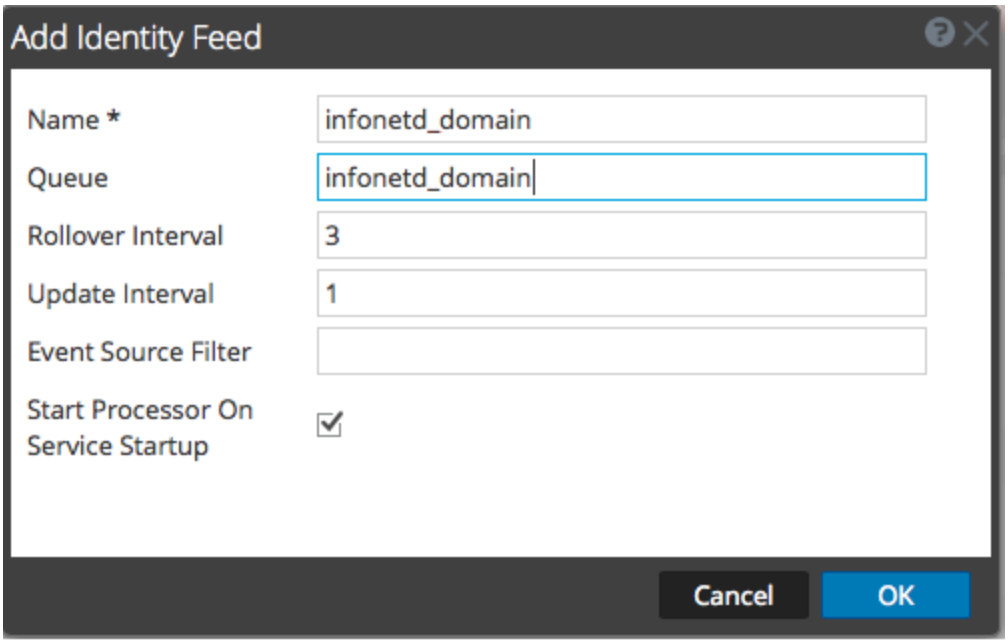
So erstellen Sie einen Identitätsfeed:

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.

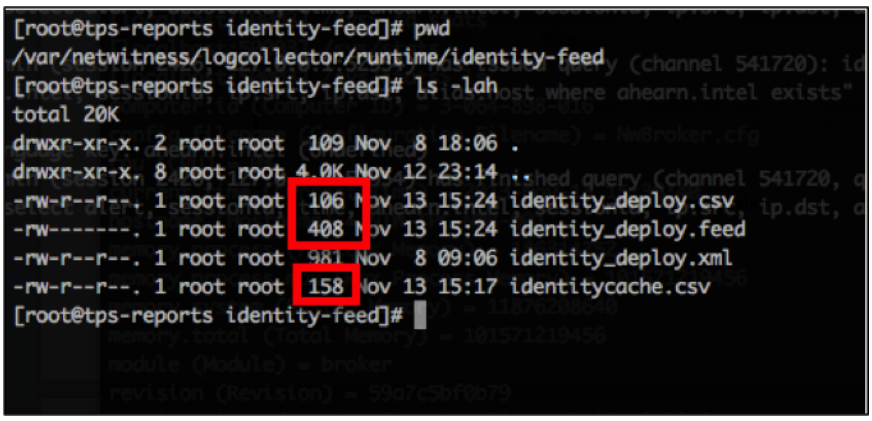


e. Klicken Sie auf **OK**.

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.

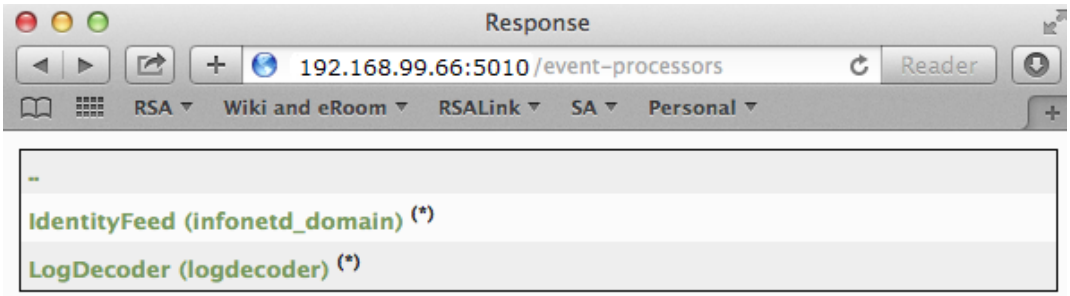


   c. Öffnen Sie einen Webbrowser (Internet Explorer nicht empfohlen) und melden Sie sich bei der REST-Schnittstelle des Log Collector an. Verwenden Sie für die Anmeldung Administrator-Anmeldedaten. Wenn die IP-Adresse Ihres Log Collector beispielsweise

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:

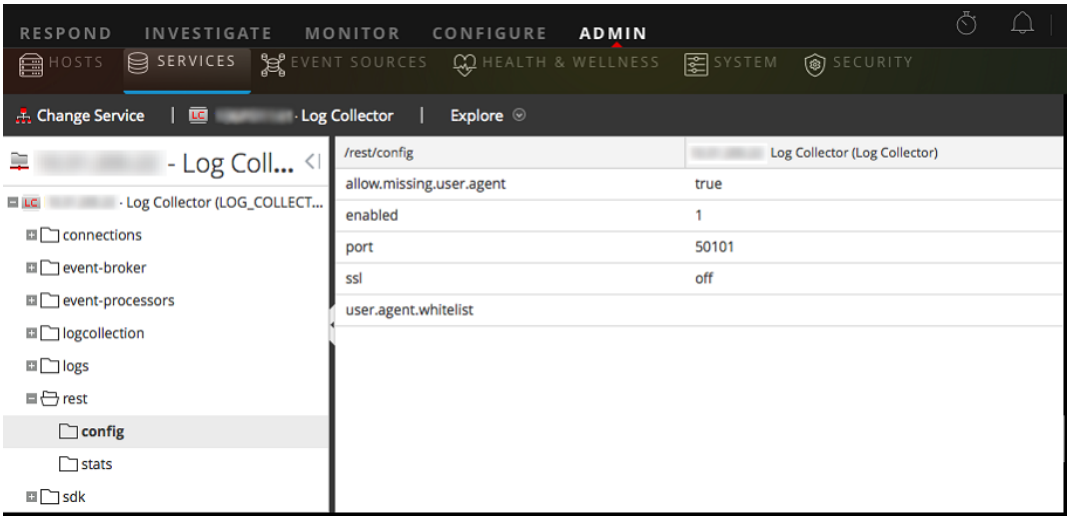


Sie sehen, dass der Bildschirm den Namen des Identitätsfeeds enthält, den Sie zuvor erstellt haben (in diesem Beispiel `infonetd_domain`).

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**.



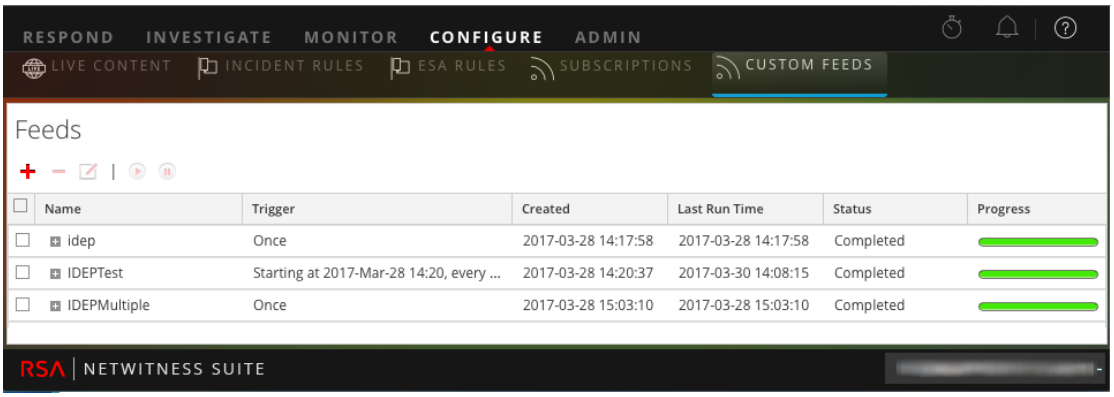
Damit REST aktiv ist, muss **aktiviert** auf **1** festgelegt sein.

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.

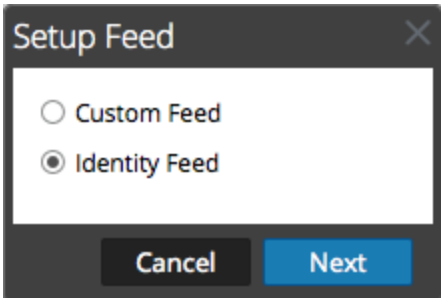
3. Navigieren Sie zu **Konfigurieren > Live Content > Benutzerdefinierte Feeds**.

   Das Feedraster wird angezeigt.



4. Klicken Sie in der Symbolleiste auf +.

   Das Dialogfeld Feed einrichten wird angezeigt.



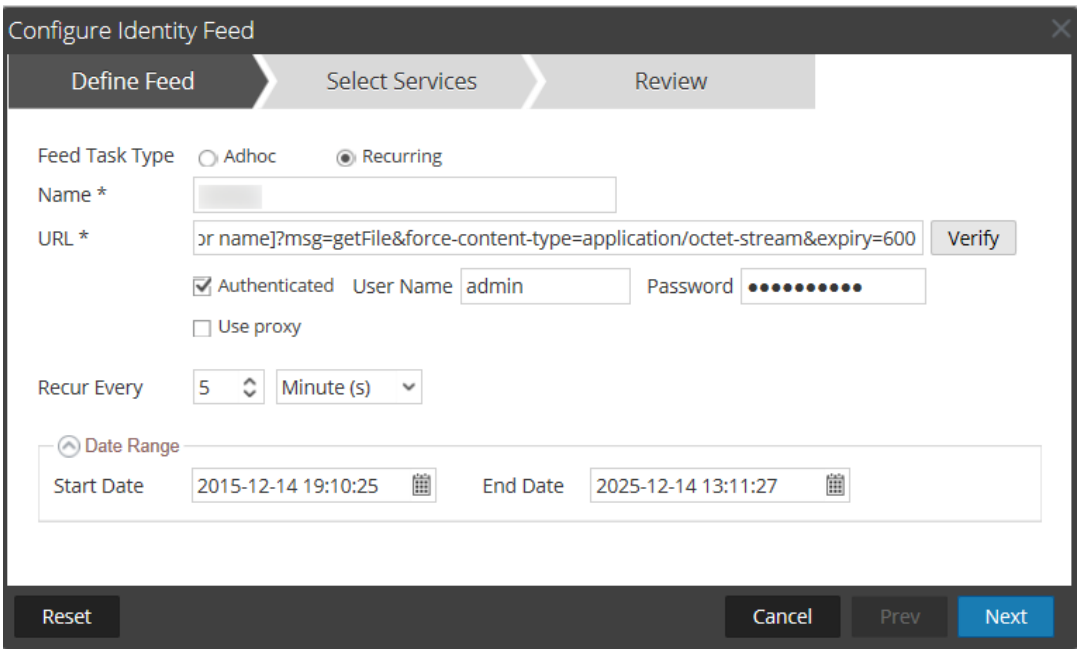
5. Vergewissern Sie sich, dass **Identitätsfeed** ausgewählt ist, und klicken Sie auf **Weiter**.

   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.

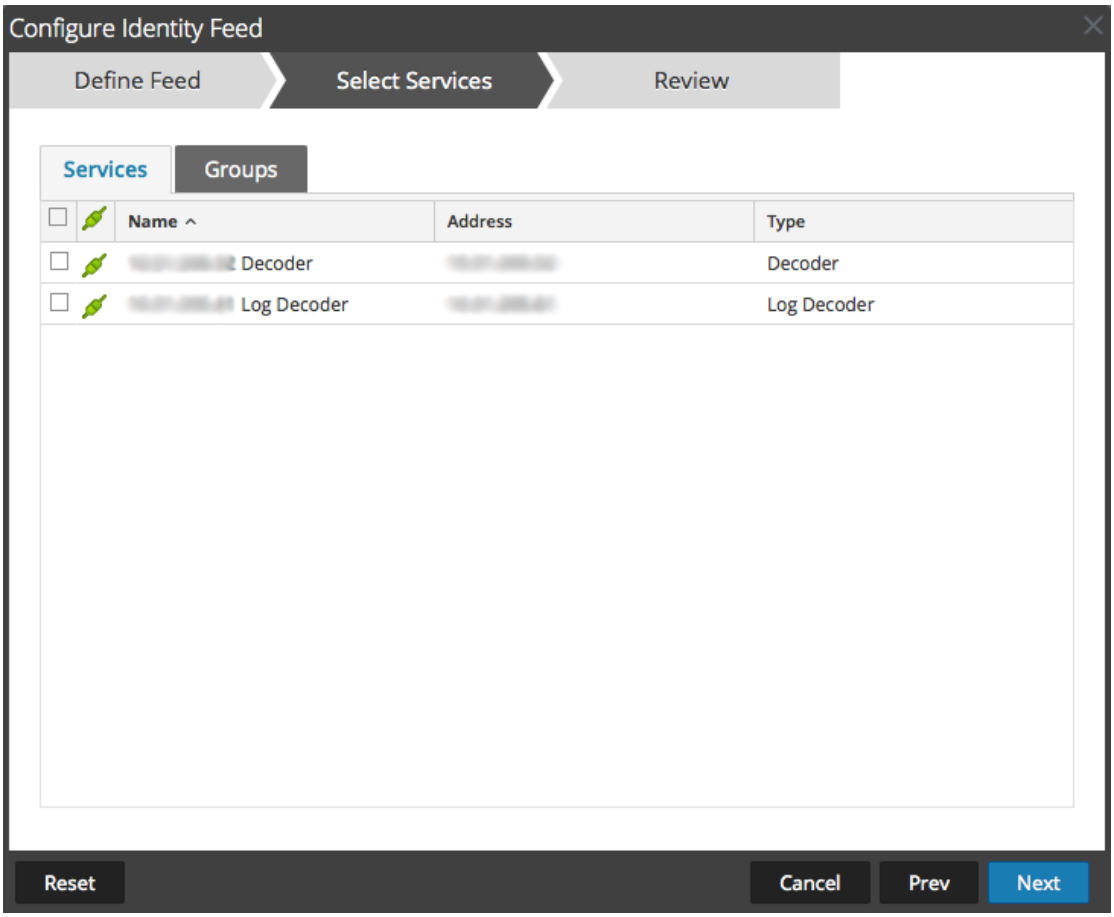
10. Wenn Sie SSL-Verschlüsselung verwenden, müssen Sie das REST-API-SSL-Zertifikat für

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.

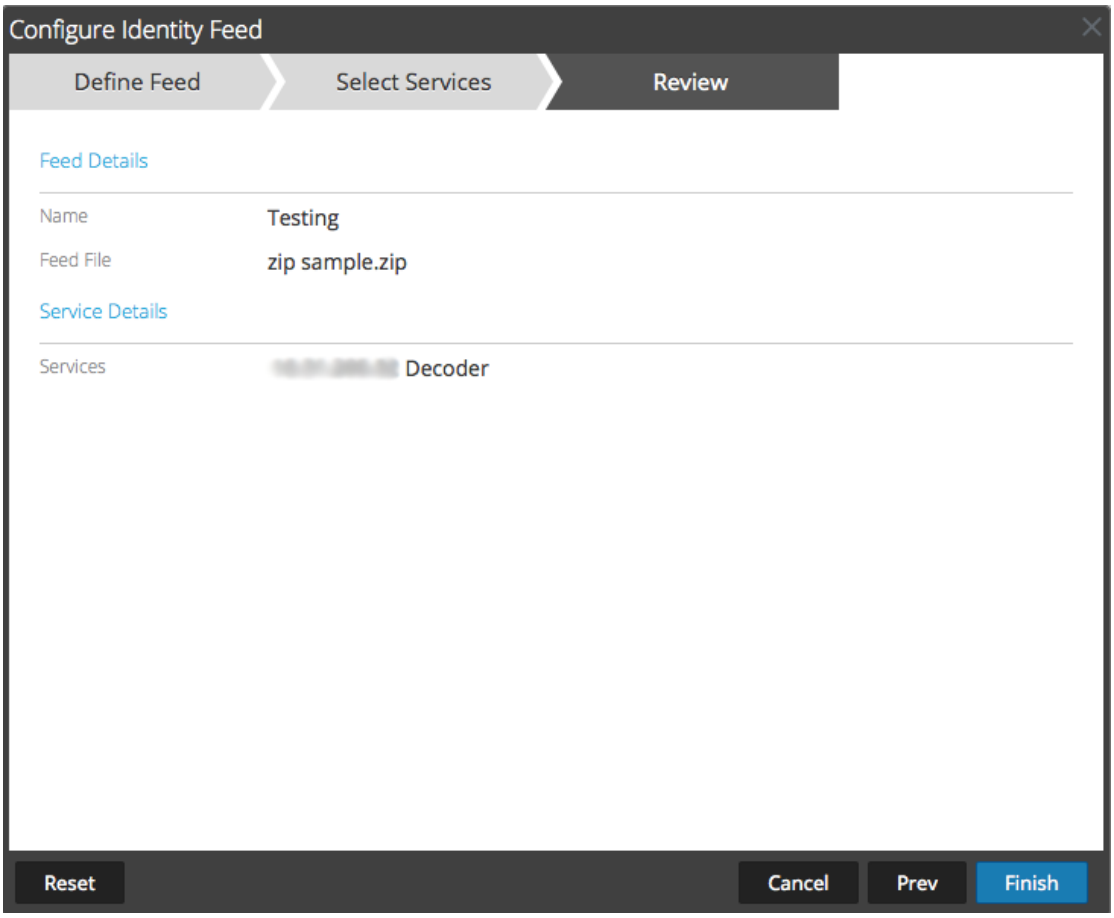
11. Klicken Sie auf **Verifizieren**, um die Konfiguration Ihres Identitätsfeeds zu überprüfen, bevor Sie das Formular „Services auswählen“ öffnen.
12. Klicken Sie auf **Weiter**.

    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**

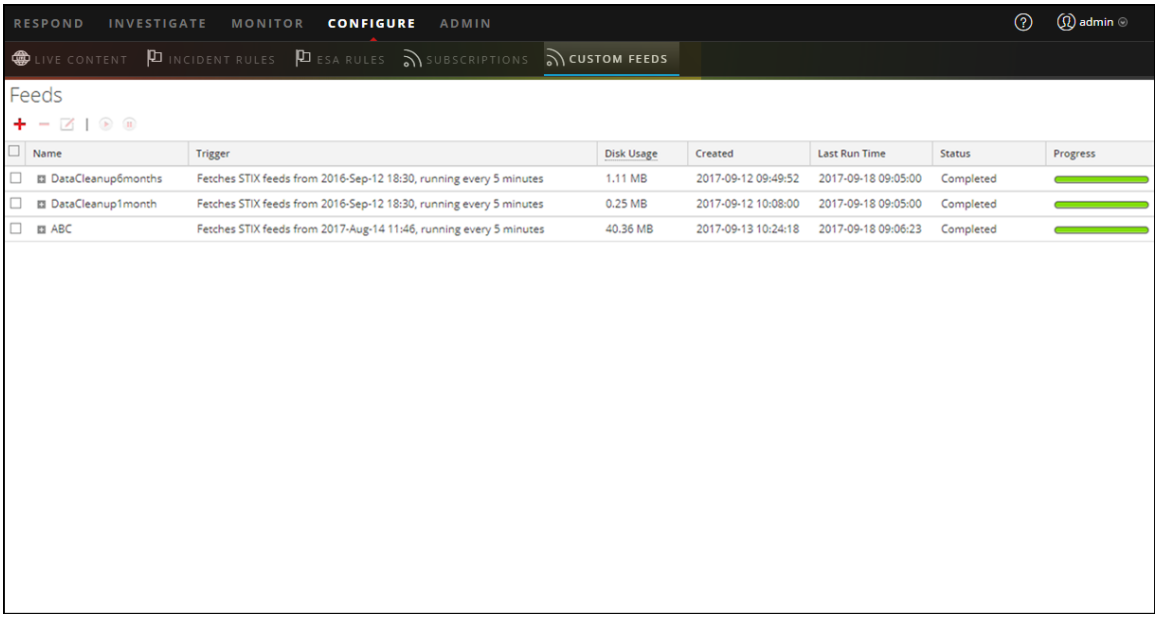
    Das Formular Überprüfung wird angezeigt.



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.

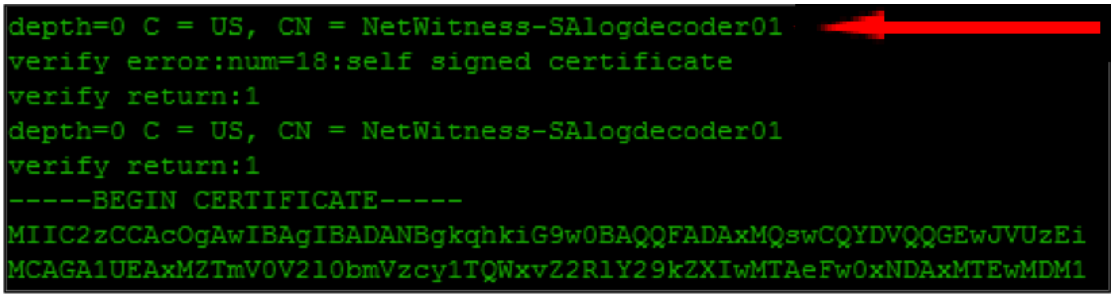
1. Stellen Sie über SSH eine Verbindung mit dem Security Analytics-UI-Server her.
2. Führen Sie den folgenden Befehl aus, um den CN-Namen des SSL-Zertifikats auszugeben:

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

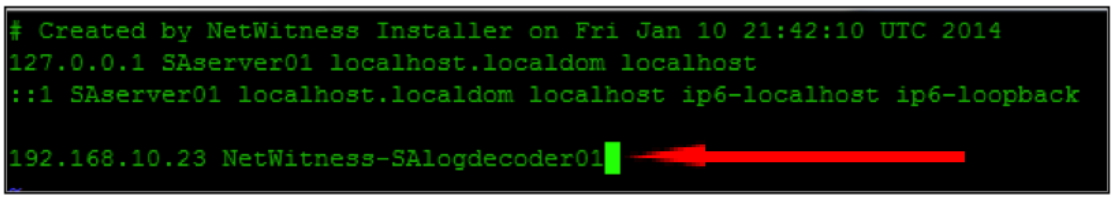
Beispiel:

```
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.

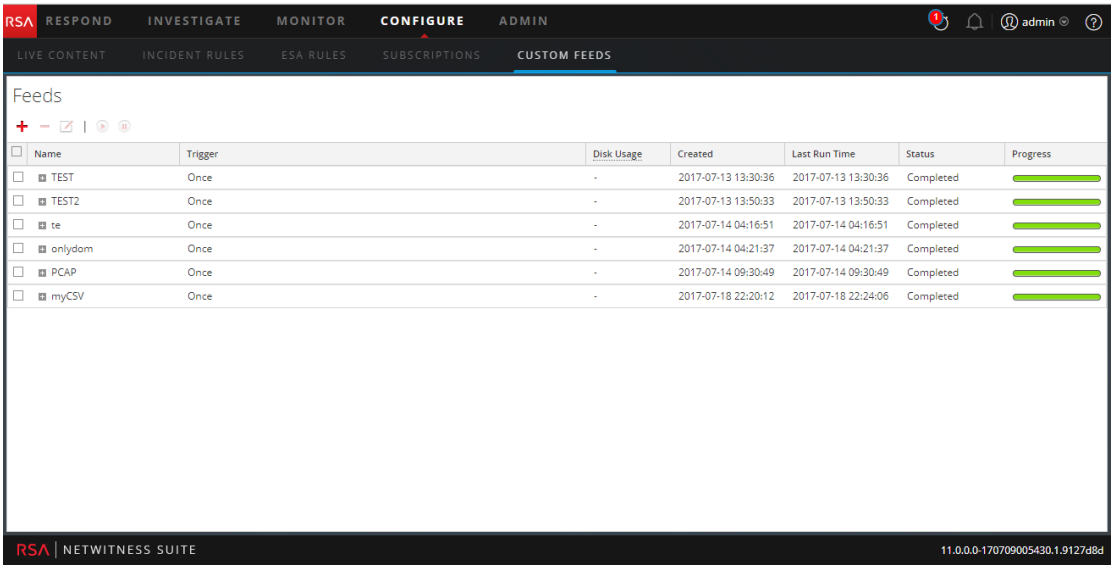
Hochladen, Bearbeiten oder Entfernen eines Feeds

Sie können einen Feed hochladen, einen vorhandenen Feed bearbeiten oder einen Feed entfernen.

So bearbeiten Sie einen vorhandenen Feed:

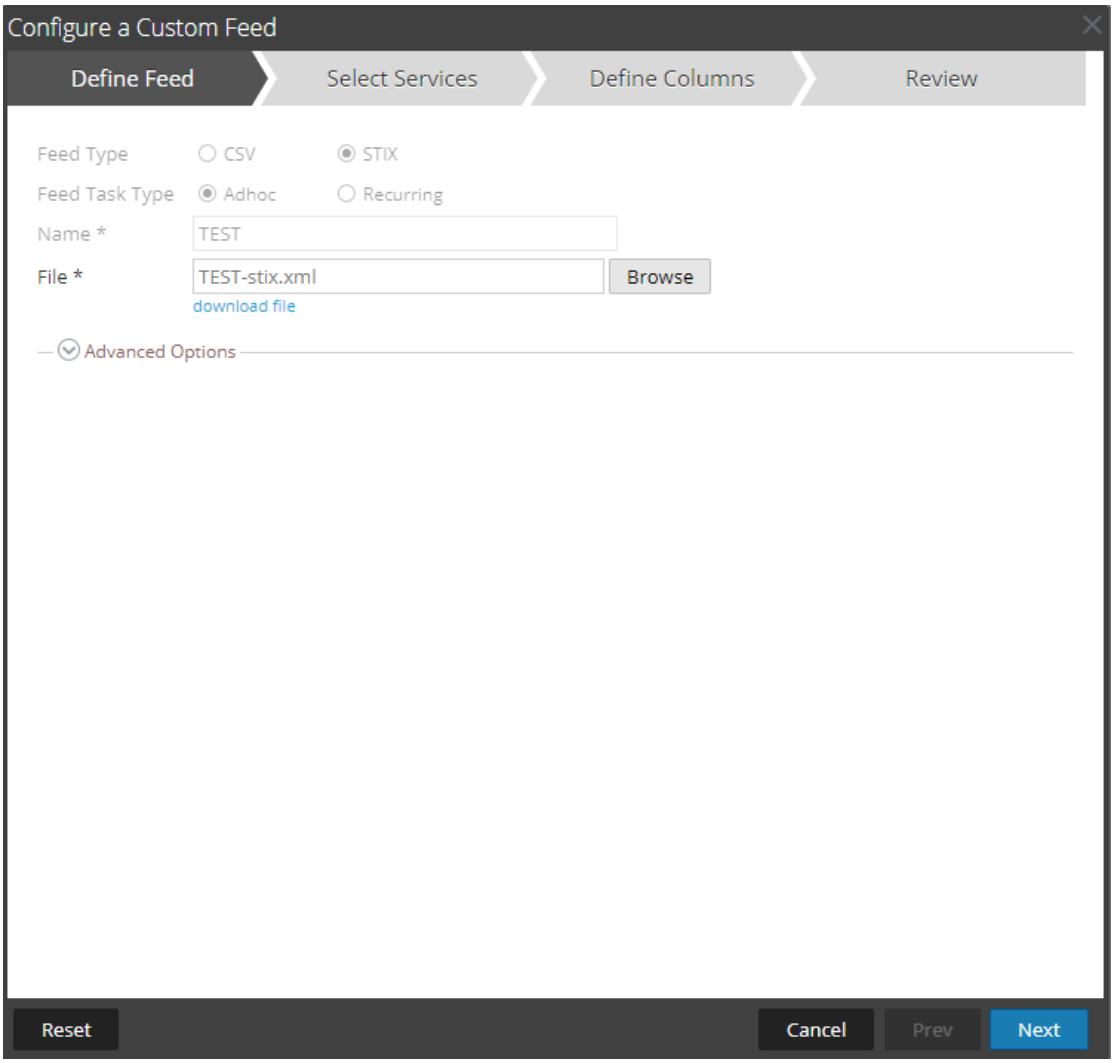
1. Navigieren Sie zu **Konfigurieren > Benutzerdefinierte Feeds**.

   Die Ansicht Feeds wird angezeigt.



2. Wählen Sie in 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. Bei einem STIX-Feed wird die .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)

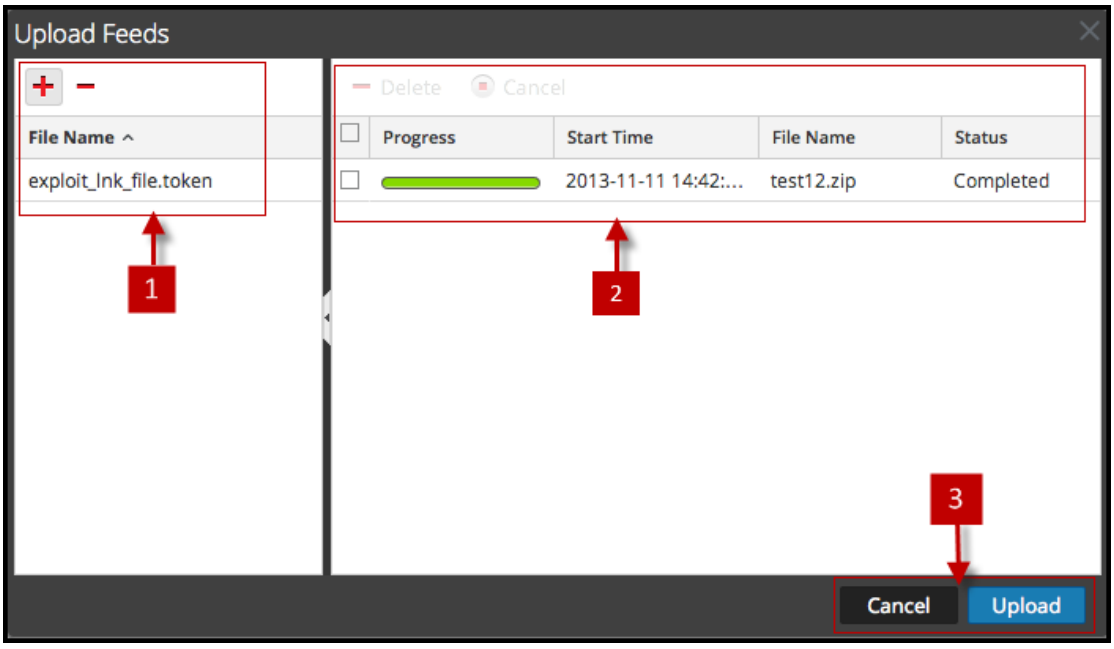
6. Überprüfen Sie die Feedinformationen in der Registerkarte **Überprüfen** und klicken Sie auf **Fertigstellen**, wenn diese korrekt sind.

Der Feed wird mit der aktualisierten Datei und neuen Feedspezifikationen erneut erstellt. 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 werden 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.

So laden Sie einen Feed auf einen Decoder oder Log Decoder hoch:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Service aus und klicken Sie auf  **> Ansicht > Konfiguration**.
   Die Ansicht „Services-Konfiguration“ wird mit geöffneter Registerkarte „Allgemein“ angezeigt.
3. Wählen Sie die Registerkarte **Feeds** aus.

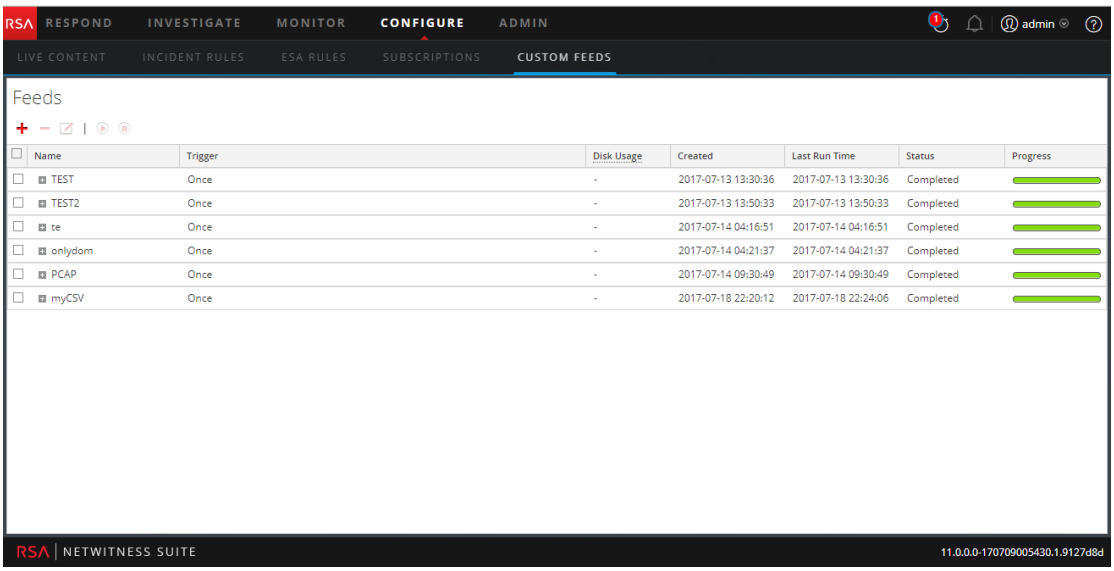
4. Klicken Sie in der Symbolleiste der Registerkarte „Feeds“ auf Upload.
   Das Dialogfeld „Feeds hochladen“ wird angezeigt.



5. Klicken Sie im Raster **Datei** auf + und wählen Sie eine Feeddatei aus. Unterstützte Dateiformate sind: *.feed, *.token und *.filter
6. Wählen Sie die Feeddatei aus der Liste **Datei** aus und klicken Sie auf **Hochladen**.
   Der Liste „Job hochladen“ wird aktualisiert und zeigt den Fortschritt und Status des hochgeladenen Feeds an.

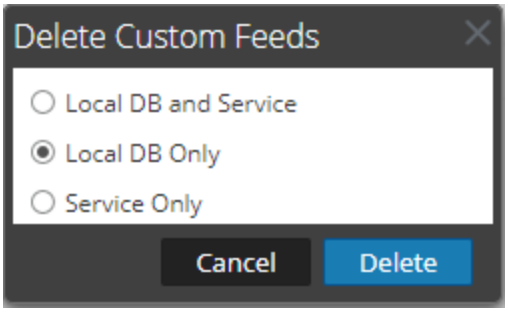
So entfernen Sie einen Feed:

1. Navigieren Sie zu **Konfigurieren > Benutzerdefinierte Feeds**.
   Die Ansicht „Benutzerdefinierte Feeds“ wird angezeigt.



2. Wählen Sie in 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:

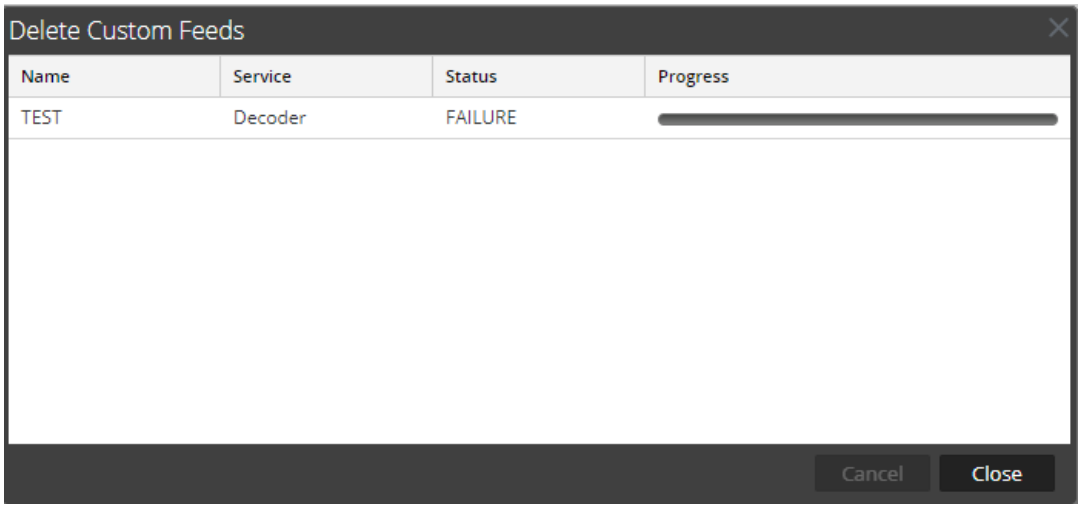
   - Wenn Sie zum Löschen des Feeds die Option **Lokale DB und lokaler Service** wählen, wird der Feed sowohl vom Service als auch aus dem lokalen NetWitness Suite-Posteingang gelöscht. Der gelöschte Feed wird nicht mehr auf der NetWitness Suite-Benutzeroberfläche angezeigt.
   - Wenn Sie zum Löschen des Feeds die Option **Nur lokale DB** wählen, wird der Feed aus dem lokalen NetWitness Suite-Posteingang gelöscht. Der gelöschte Feed wird nicht mehr in 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 in 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.



Erstellen benutzerdefinierter Metaschlüssel mithilfe benutzerdefinierter Feeds

In diesem Thema erfahren Sie, wie Sie benutzerdefinierte Metaschlüssel mithilfe eines benutzerdefinierten Feeds im Log Decoder hinzufügen.

Sie können benutzerdefinierte Metaschlüssel zum Abrufen von Daten und zur Untersuchung und Analyse der Protokolle und Pakete erstellen. Benutzerdefinierte Metaschlüssel ermöglichen Ihnen, den Protokoll- und Paketdaten einen Erweiterungskontext hinzuzufügen. In diesem Dokument werden die Änderungen an der Konfiguration hervorgehoben, die benutzerdefinierte Metaschlüssel im Concentrator, ESA,Archiver, Warehouse Connector und dem Reporting Engine-Schema reflektieren.

Hier ist ein Beispiel für die Erstellung des benutzerdefinierten Metaschlüssels im Log Decoder. In diesem Szenario möchte ein Unternehmen den Speicherort einer Ressource wie einen Drucker verfolgen. Deshalb wird der benutzerdefinierte Metaschlüssel **Quellstandort** eingeführt, der den Standort der Ressource angibt, z. B. Drucker1, der sich im „fünften Stock in Gebäuteteil A“ befindet.

Hinweis: Benutzerdefinierte Metaschlüssel können auch im Decoder erstellt werden. Wählen Sie die Datei `index-decoder-custom.xml` aus, wenn Sie einen benutzerdefinierten Metaschlüssel im Decoder erstellen möchten.

Hinzufügen eines benutzerdefinierten Metaschlüssels im Log Decoder

So fügen Sie benutzerdefinierte Metaschlüssel mithilfe von benutzerdefinierten Feeds hinzu:

1. Navigieren Sie zu **Administration** > **Services** > **Log Decoder.**
2. Wählen Sie einen Service aus und klicken Sie auf > **Ansicht** > **Konfiguration** > > **Registerkarte „Dateien“** > **index-logdecoder-custom.xml**.

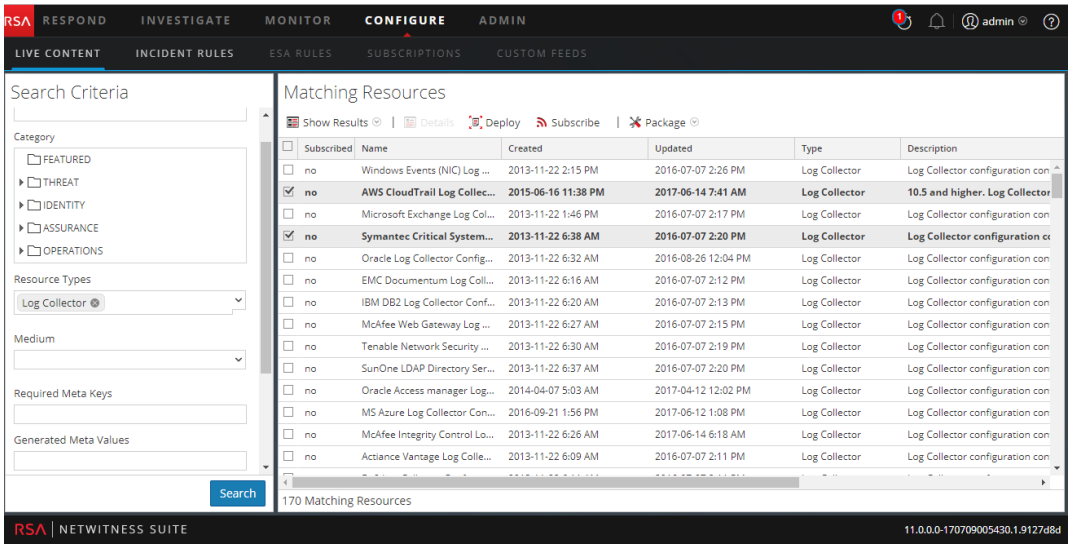
```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexNone"
name="location.src" format="Text"/>
 </Language>
```

3. Starten Sie den Log Decoder-Service neu. Klicken Sie in der Ansicht „Services“ auf > **Neu starten**.

Bereitstellen eines Log Decoder-Feeds in Live

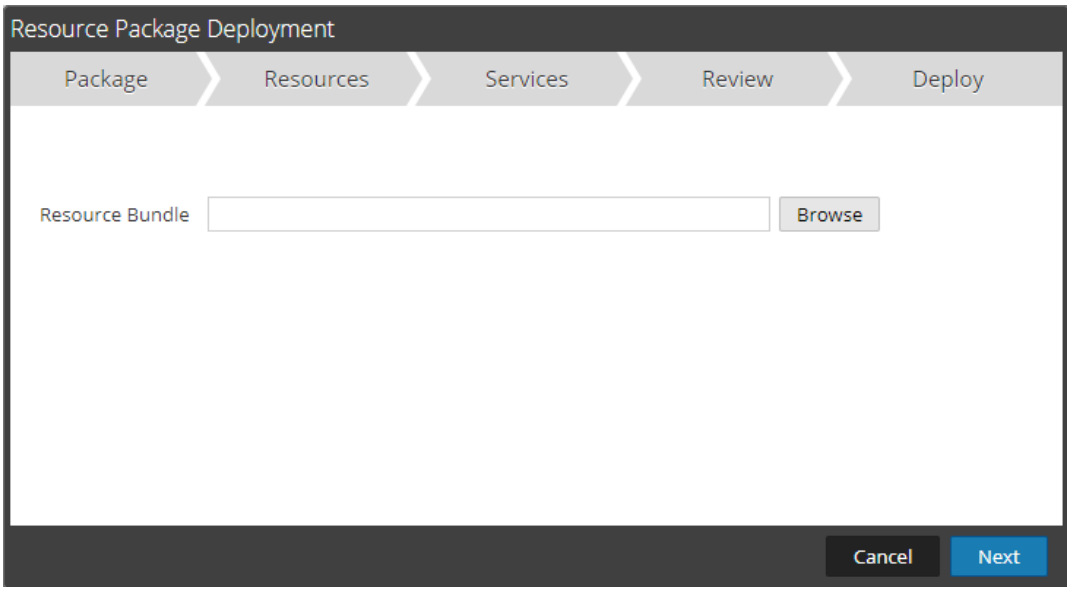
So stellen Sie den Feed in der Live-Umgebung bereit:

1. Navigieren Sie zu **Konfigurieren > Live-Inhalte.**
2. Wählen Sie eine Gruppe von Ressourcen oder ein zuvor erstelltes Ressourcenpaket aus. So wählen Sie 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**.
   c. Aktivieren Sie das Kontrollkästchen links neben den Ressourcen, die Sie bereitstellen möchten.

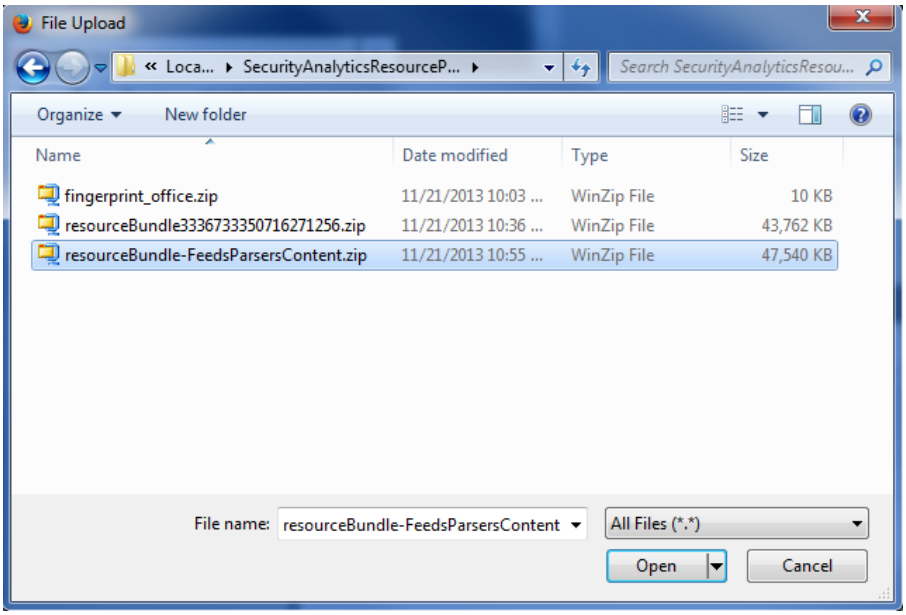


   d. Klicken Sie in der Symbolleiste „Übereinstimmende Ressourcen“ auf 

   .
3. So wählen Sie ein Ressourcenpaket zur Bereitstellung aus:
   a. Wählen Sie in der Symbolleiste **Übereinstimmende Ressourcen** der Ansicht **Live-Suche** 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**).



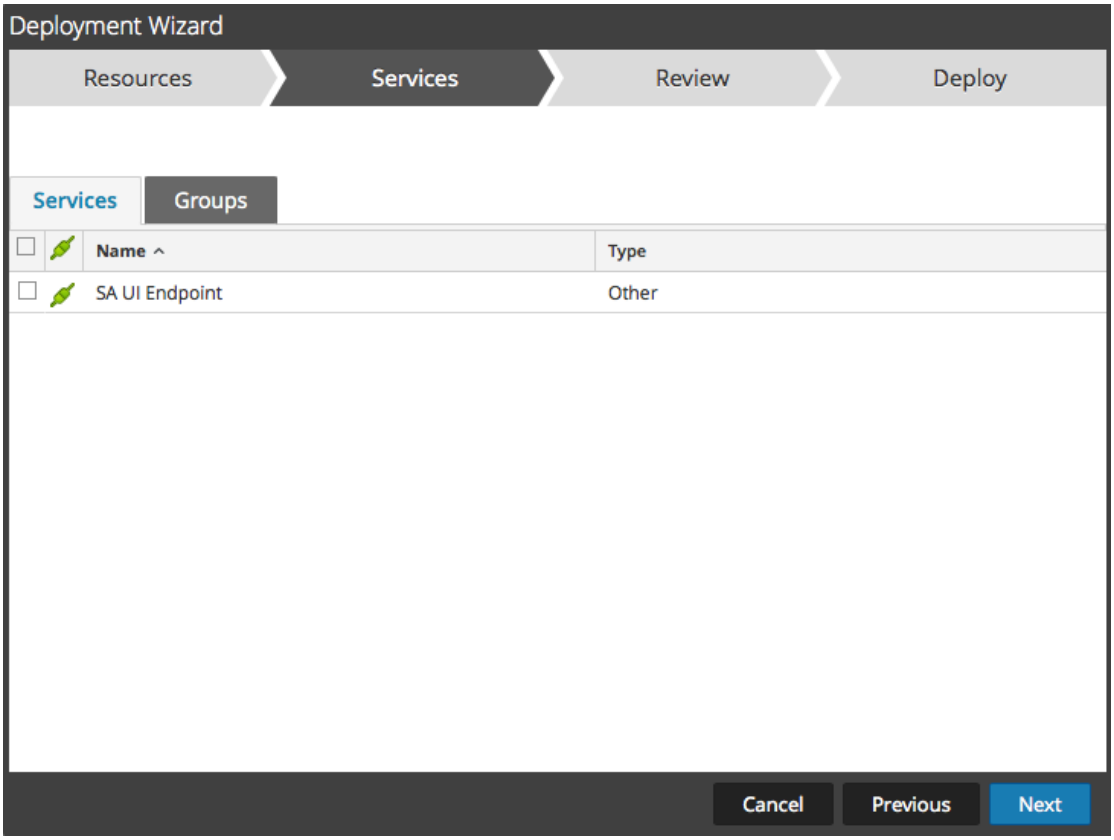
c. Klicken Sie auf **Öffnen.**
An diesem Punkt wird unabhängig davon, ob Sie ein Paket oder eine Gruppe von Ressourcen bereitstellen, der Bereitstellungsassistent geöffnet und die Seite „Ressourcen“ angezeigt.

3. Klicken Sie auf **Weiter**.
Die Seite **Services** wird angezeigt. Sie verfügt über zwei Registerkarten: **Services** und **Gruppen**. Diese stellen eine Liste von Services und Servicegruppen bereit, die in der

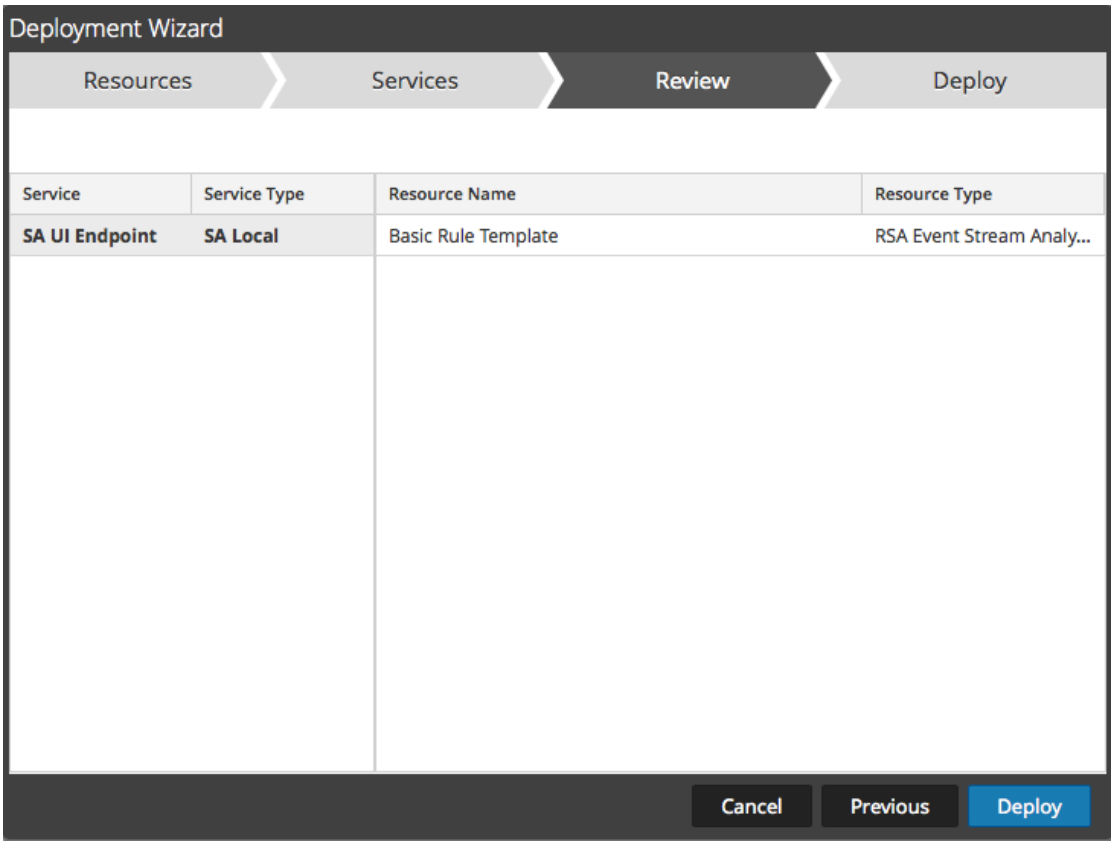
Ansicht „Administration > Services“ konfiguriert werden können. Die Spalten sind eine Untergruppe der Spalten, die in der Ansicht Services verfügbar sind.

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.

4. 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 „Administration“ > „Services“ konfiguriert sind.
   Wählen Sie Gruppen von Services mithilfe der Registerkarte **Gruppen** aus.

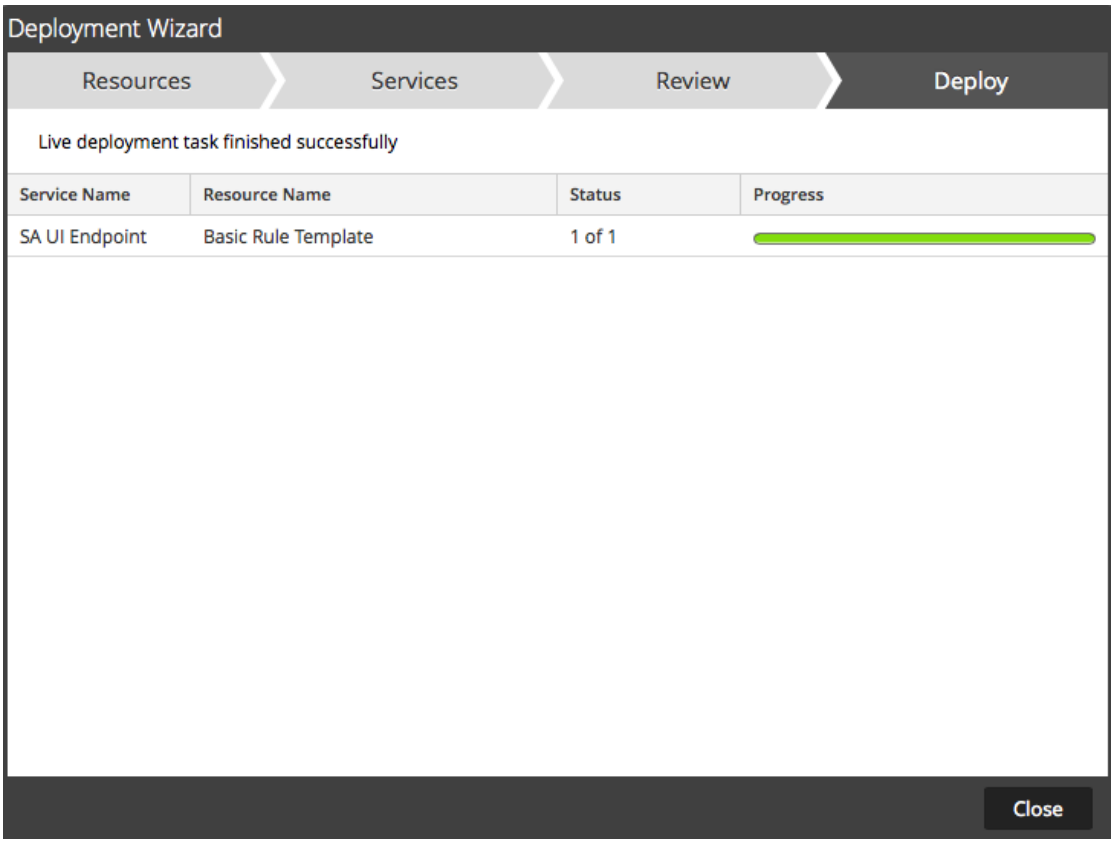


5. Klicken Sie auf **Weiter**.
   Die Seite **Überprüfung** wird angezeigt.

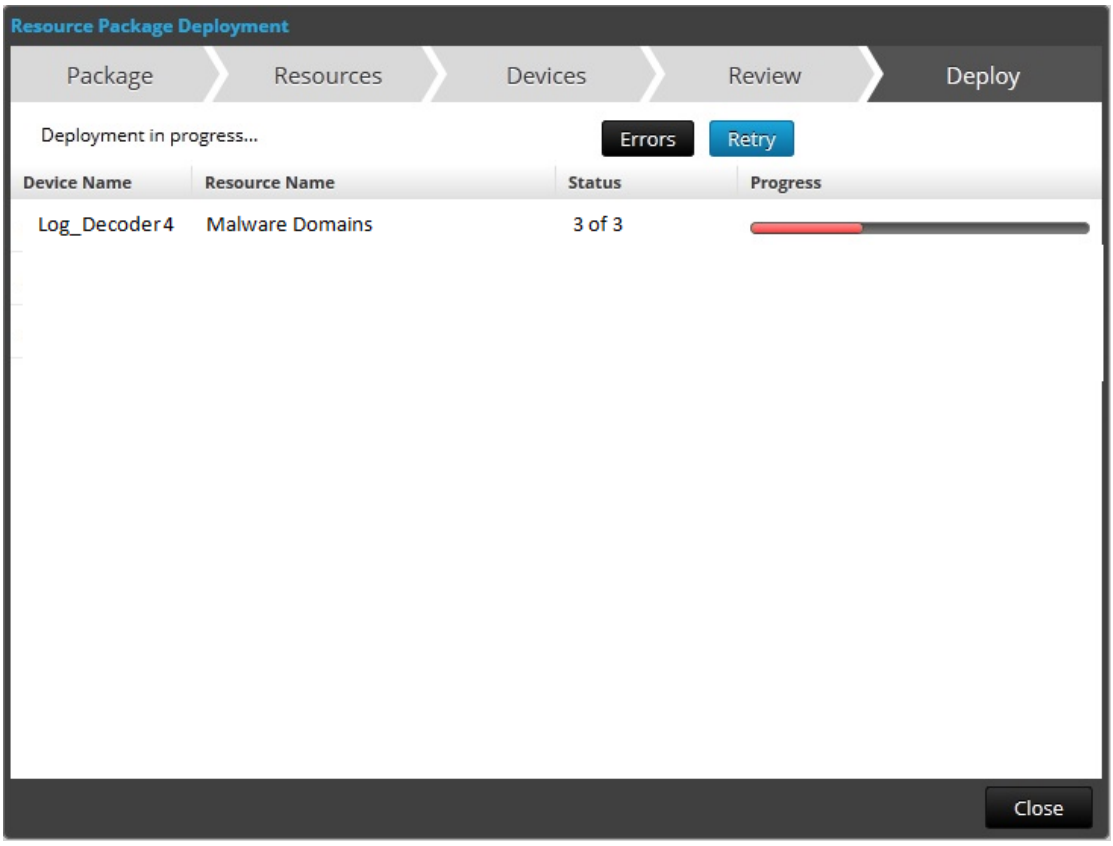


Stellen Sie sicher, dass Sie die korrekten Ressourcen und die Services ausgewählt haben, für die Sie sie bereitstellen möchten.

6. 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.



7. Klicken Sie auf **Schließen**.

Hinweis: Die Quell-IP sollte indexiert werden, indem der Typ als „IP“ ausgewählt wird, da ip.src und ip.dst das IPv4-Format aufweisen.

In diesem Szenario wird der benutzerdefinierte Metaschlüssel location.src (Quellstandort) durch Indexierung des Hostnamens (alias.host) hinzugefügt. In diesem Beispiel wird der Hostname des Druckers im Metaschlüssel alias.host ausgefüllt. Wählen Sie also „alias.host“ als Callback-Schlüssel und den Indextyp „Nicht IP“ im Assistenten für Feeds aus, wie nachfolgend dargestellt. Wählen Sie im Abschnitt „Werte definieren“ den benutzerdefinierten Metaschlüssel aus dem Drop-down-Menü aus.

Hinzufügen des benutzerdefinierten Metaschlüsseleintrags zur benutzerdefinierten Concentrator-Indexdatei

So fügen Sie den benutzerdefinierten Metaschlüsseleintrag der benutzerdefinierten Concentrator-Indexdatei hinzu:

1. Navigieren Sie zu **Administration** > **Services** > **Concentrator**.
2. Klicken Sie auf > **Ansicht** > **Konfiguration** > **Registerkarte „Dateien“** > **index-concentrator-custom.xml**.
3. Fügen Sie den benutzerdefinierten Metaschlüsseleintrag zur Concentrator-Indexdatei hinzu.

```
<Language>
 <?xml version="1.0" encoding="utf-8"?>
 <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location"  level="IndexValues"
name="location.src" format="Text"  valueMax="10000"
defaultAction="Open"/>
 </Language>
```

4. Um den Concentrator-Service neu zu starten, klicken Sie in der Ansicht „Services“ auf > **Neu starten**.

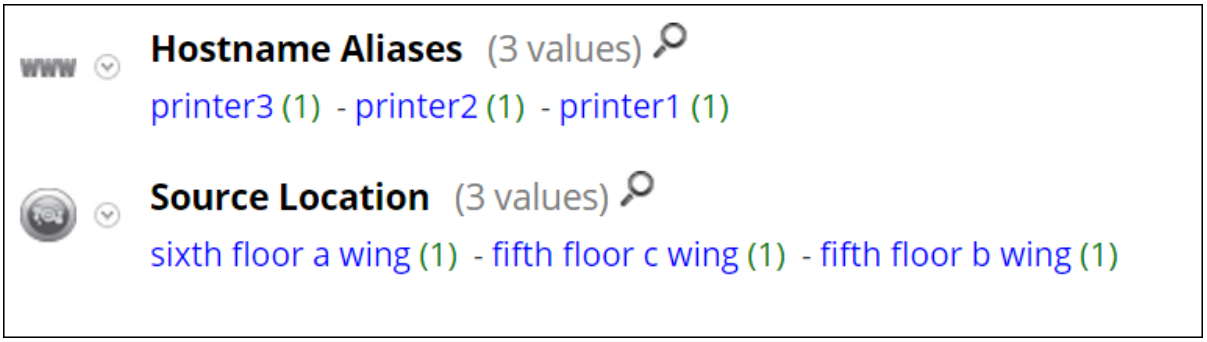
Hinweis: Bei einem Broker wird der Index vom Concentrator abgeleitet, von dem er aggregiert wird. Deshalb müssen Sie keinen benutzerdefinierten Metaschlüssel im Broker erstellen. Wenn Sie den Metaschlüssel nicht im Concentrator indexiert haben, wird der Broker nicht in der Ansicht „Investigation“ angezeigt.

Untersuchen des benutzerdefinierten Metaschlüssels

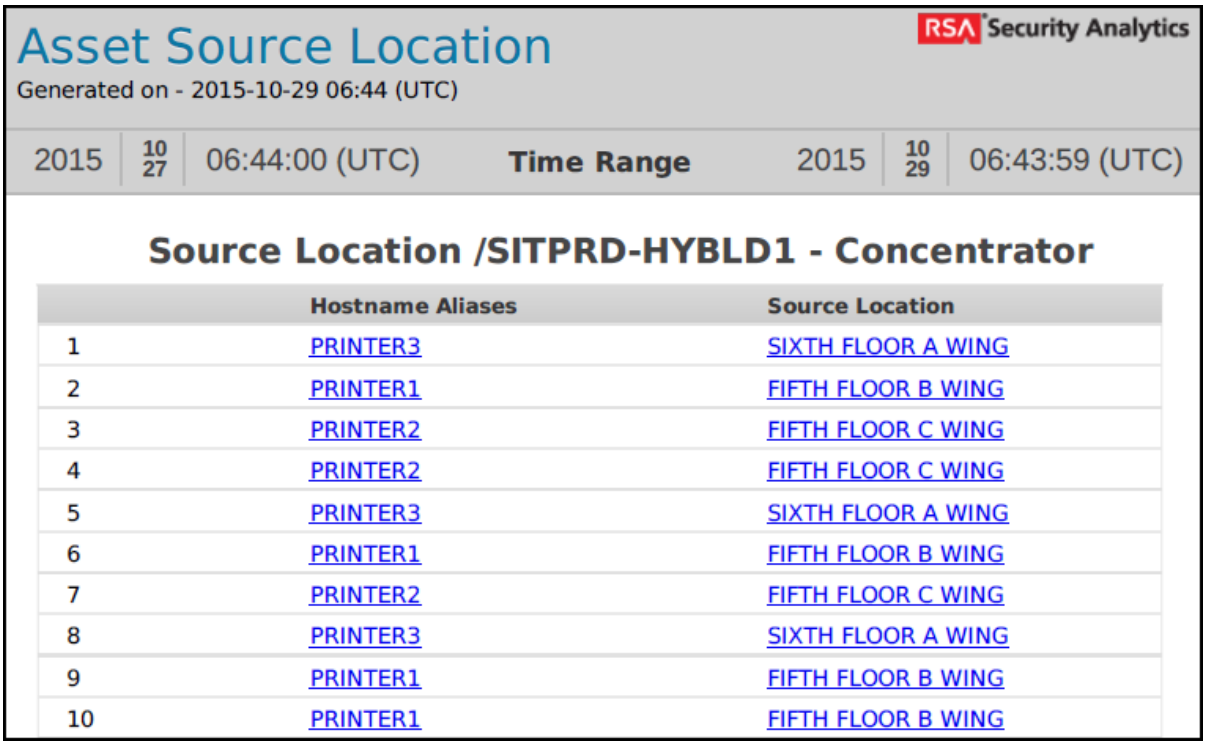
Hinweis: Sie müssen sich von der NetWitness Suite-Benutzeroberfläche abmelden und wieder anmelden, um den benutzerdefinierten Metaschlüssel in Investigation anzuzeigen.

So zeigen Sie den benutzerdefinierten Metaschlüsselin der Ansicht Investigation an:

1. Gehen Sie zu **Ermittlung** > **Navigieren**.
2. Wählen Sie einen Concentrator-Service aus und klicken Sie auf **Navigieren**.



Hier ist ein Beispiel für einen Bericht, der auf dem Concentrator ausgeführt wird.



Asset Source Location

RSA Security Analytics

Generated on - 2015-10-29 06:44 (UTC)

2015 | 10 27 | 06:44:00 (UTC) | **Time Range** | 2015 | 10 29 | 06:43:59 (UTC)

Source Location /SITPRD-HYBLD1 - Concentrator

	Hostname Aliases	Source Location
1	PRINTER3	SIXTH FLOOR A WING
2	PRINTER1	FIFTH FLOOR B WING
3	PRINTER2	FIFTH FLOOR C WING
4	PRINTER2	FIFTH FLOOR C WING
5	PRINTER3	SIXTH FLOOR A WING
6	PRINTER1	FIFTH FLOOR B WING
7	PRINTER2	FIFTH FLOOR C WING
8	PRINTER3	SIXTH FLOOR A WING
9	PRINTER1	FIFTH FLOOR B WING
10	PRINTER1	FIFTH FLOOR B WING

Zusätzliche Verfahren

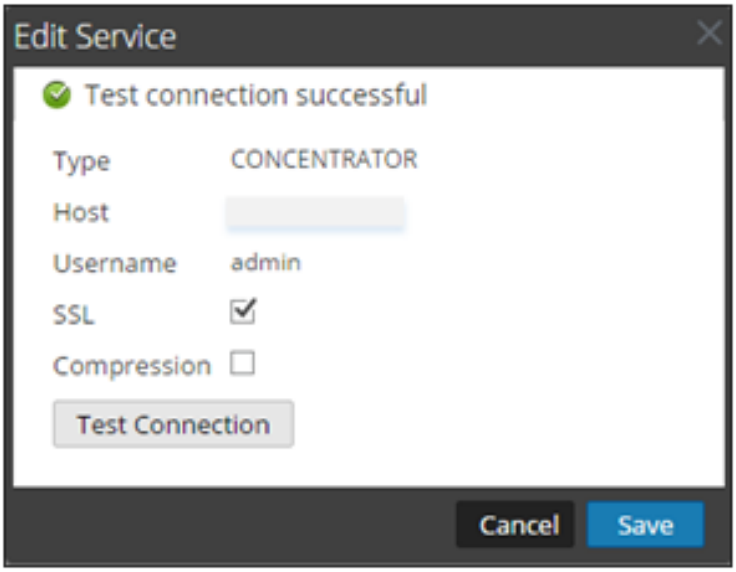
Die folgenden Verfahren müssen ausgeführt werden, wenn Sie Warehouse Connector, Archiver, Reporting Engine und ESA konfiguriert haben.

Aktualisieren des Schemas in ESA

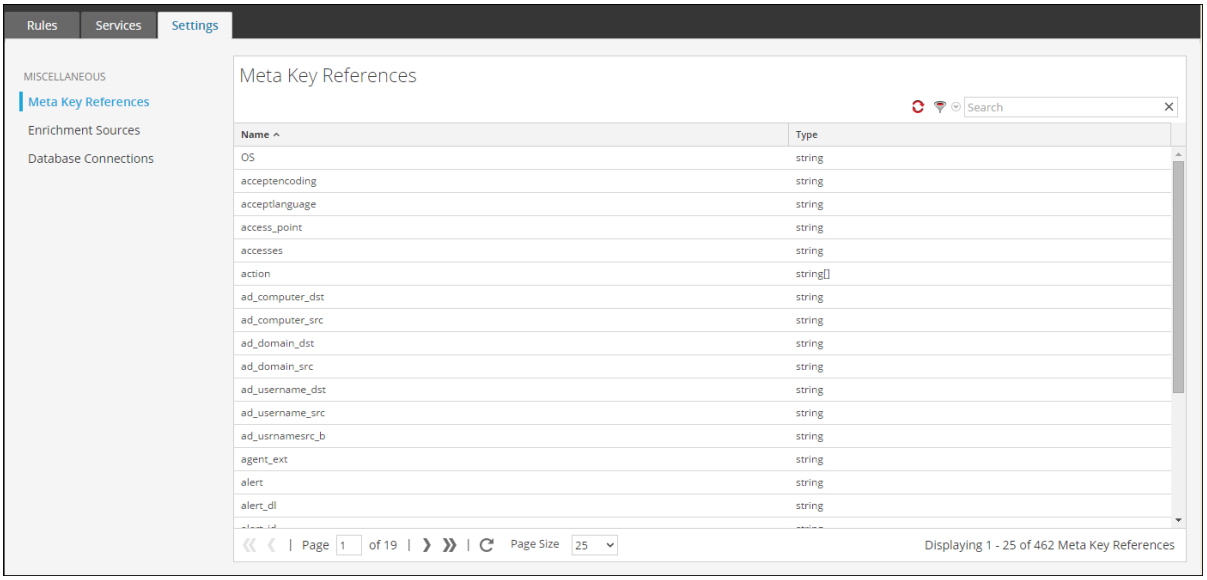
Bevor Sie das Schema in ESA aktualisieren, sollte der benutzerdefinierte Metaschlüssel im Concentrator indexiert werden.

So aktualisieren Sie die Schema-ESA-Regeln, um die neuen benutzerdefinierten Metaschlüssel verwenden zu können:

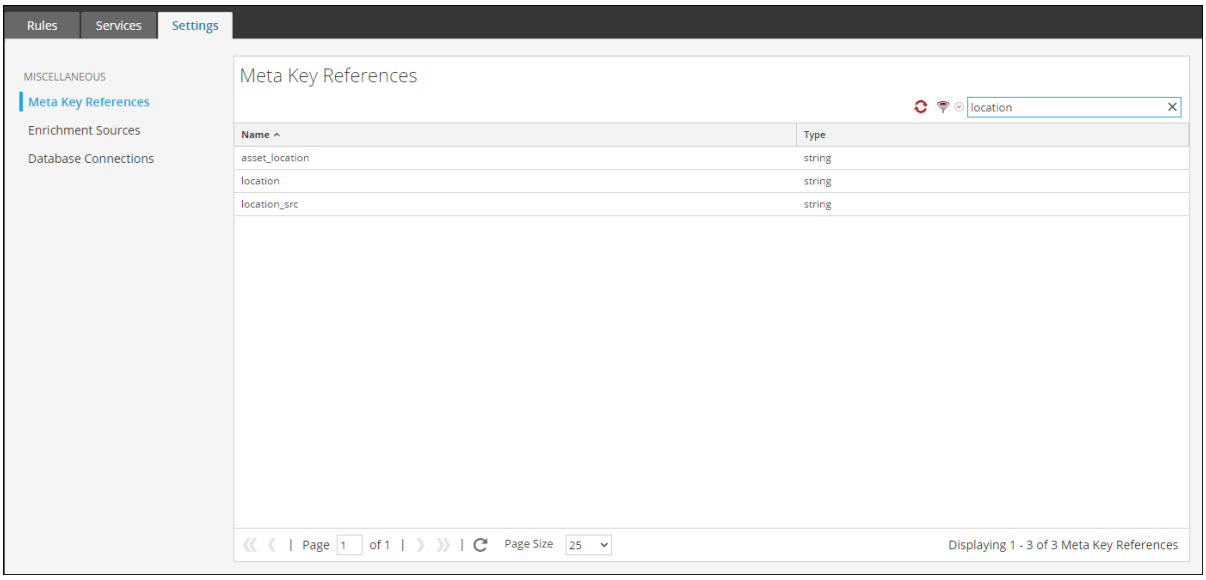
1. Navigieren Sie zu **Administration** > **Services** > **ESA – Event Stream Analysis** > **Ansicht** > **Konfiguration**.
2. Bearbeiten Sie die Concentrator-Datenquelle.
3. Klicken Sie auf **Verbindung testen**.



4. Klicken Sie auf **Speichern**, nachdem die Verbindung erfolgreich hergestellt wurde.
5. Klicken Sie auf **Anwenden**.
6. Navigieren Sie zu **Warnmeldungen** > **Konfigurieren** > **Einstellungen**.



7. Klicken Sie auf die Registerkarte **Suche** und suchen Sie nach dem Namen des benutzerdefinierten Metaschlüssels.
   Der Name und der Typ des benutzerdefinierten Metaschlüssels werden angezeigt.



Aktualisieren des Schemas im Archiver

Wenn Sie den Archiver mithilfe der neuen benutzerdefinierten Metaschlüssel konfigurieren möchten, müssen Sie das Archiver-Schema in der Reporting Engine aktualisieren. So aktualisieren Sie das Archiver-Schema in der Reporting Engine:

1. Navigieren Sie zu **Administration** > **Services** > **Archiver**.
2. Klicken Sie auf > **Ansicht** > **Konfiguration** > **Dateien** > **index-archiver-custom.xml**.
3. Fügen Sie den benutzerdefinierten Metaschlüsseleintrag zur Archiver-Indexdatei hinzu.

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexValues"
name="location.src" format="Text"
  valueMax="10000" defaultAction="Open"/>
 </Language>
```

4. Um den Archiver-Service neu zu starten, klicken Sie auf > **Neu starten.**

   Das Archiver-Schema wird mit dem benutzerdefinierten Metaschlüssel aktualisiert.

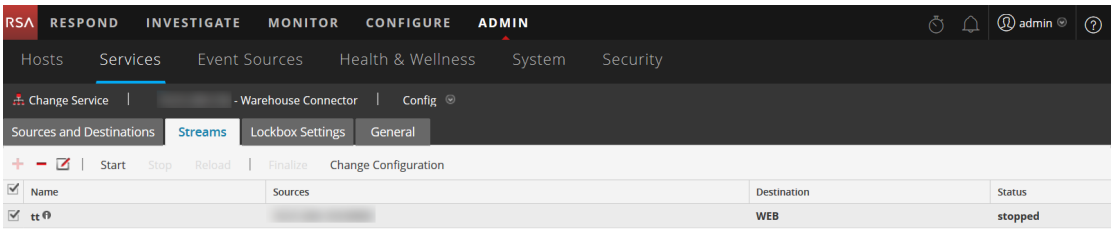
Aktualisieren des Schemas im Warehouse Connector

Wenn Sie das Warehouse mit einem benutzerdefinierten Metaschlüssel konfigurieren und diesen in Warehouse-Berichten verwenden möchten, müssen Sie das Warehouse-Schema in der Reporting Engine aktualisieren.

Wenn der Log Decoder oder Decoder, dem der benutzerdefinierte Metaschlüssel hinzugefügt wurde, eine der Quellen im Warehouse Connector-Stream ist, müssen Sie das Schema im Warehouse Connector aktualisieren.

So aktualisieren Sie das Warehouse-Schema in der Reporting Engine:

1. Navigieren Sie zu **Administration** > **Services** > **Warehouse Connector**.
2. Klicken Sie auf > **Ansicht** > **Konfiguration** > Registerkarte **Dateien** > **index-logdecoder-custom.xml**.
3. Wählen Sie den Stream aus und klicken Sie auf **Neu laden**.
   Der Warehouse Connector ruft das Schema von den Downstreamgeräten (Log Decoder/Decoder) ab.



Weitere Informationen über Streams finden Sie unter „Konfigurieren von Streams“ im *Warehouse Connector-Konfigurationsleitfaden*.

Aktualisieren des Schemas in Reporting Engine

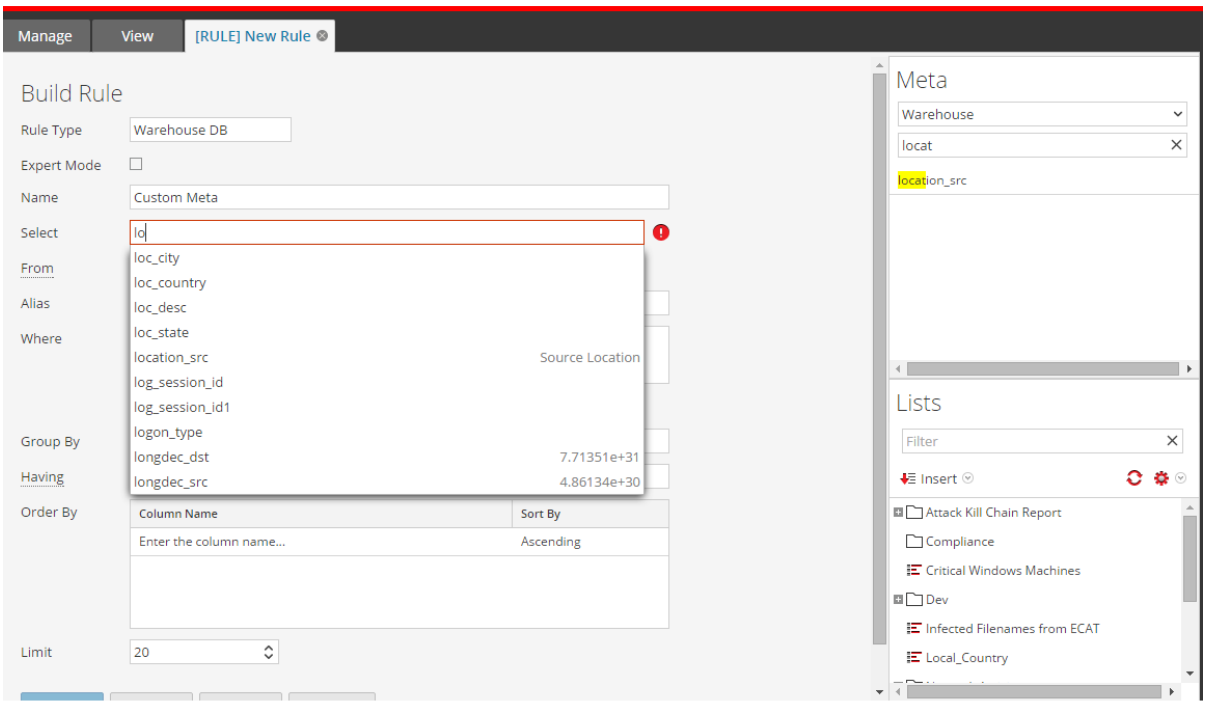
So aktualisieren Sie das Schema in Reporting Engine:

1. Navigieren Sie zu **Administration** > **Services** > **Reporting Engine.**
2. Klicken Sie auf > **Neu starten**.

Hinweis: Starten Sie die Reporting Engine neu oder warten Sie 30 Minuten lang, bis das Schema aktualisiert wurde.

So zeigen Sie den benutzerdefinierten Metaschlüssel an:

1. Navigieren Sie zu **Berichte**> **Regeln**.
2. Klicken Sie in der Symbolleiste auf .
3. Wählen Sie **Warehouse-DB** aus.
4. Suchen Sie auf der Registerkarten „Regel erstellen“ im rechten Bereich nach dem benutzerdefinierten Metaschlüssel.
   Der benutzerdefinierte Metaschlüssel wird angezeigt.



Hochladen und Löschen benutzerdefinierter Parser

In RSA NetWitness Suite können Sie Parser von Ihrem lokalen System hochladen und diese Parser löschen.

Hochladen von Parsern zu einem Decoder oder Log Decoder

Mit der Option „Upload“ in der Ansicht „Services-Konfiguration“ > Registerkarte „Parser“ wird das Dialogfeld „Parser hochladen“ angezeigt, in dem Sie den Upload von Parsern in einen Decoder oder Log Decoder managen können. In der Dateiliste können Sie eine Liste von hochzuladenden Parsern vorbereiten. Sie können Dateien aus einer Verzeichnisstruktur hinzufügen und Dateien aus der Liste löschen, wenn Sie eine bestimmte Datei nicht hochladen möchten. Wenn die Liste bereit ist, wird durch Klicken auf Hochladen der Hochladeprozess gestartet.

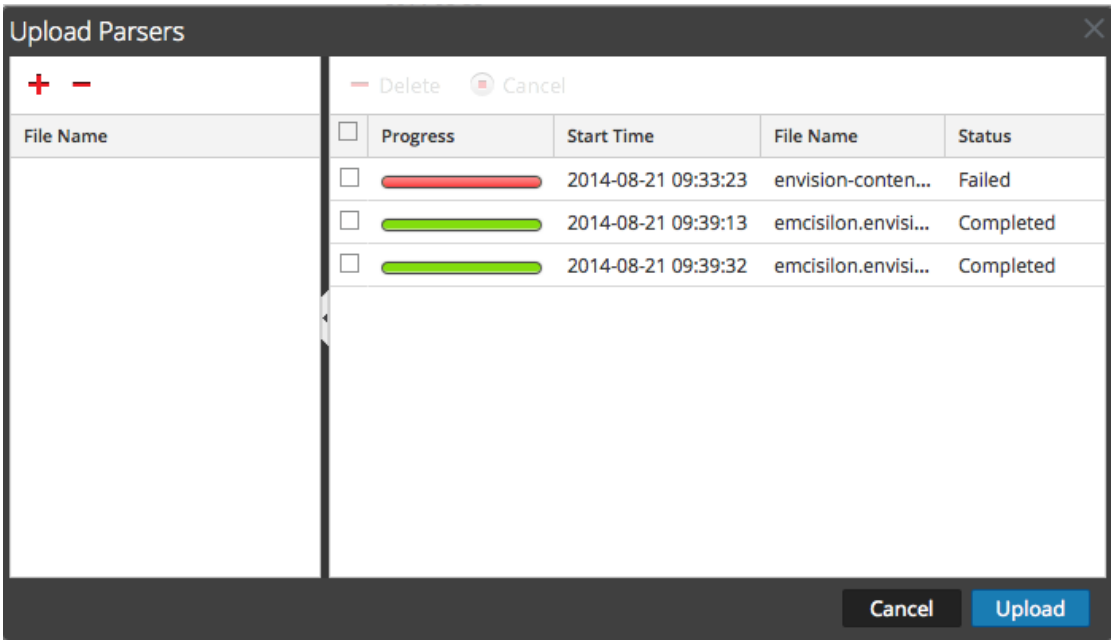
1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Service aus und dann > **Ansicht > Konfiguration**.

   Die Ansicht „Konfiguration“ für den ausgewählten Service wird angezeigt.

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

3. Klicken Sie auf Upload.

   Das Dialogfeld „Parser hochladen“ wird angezeigt.

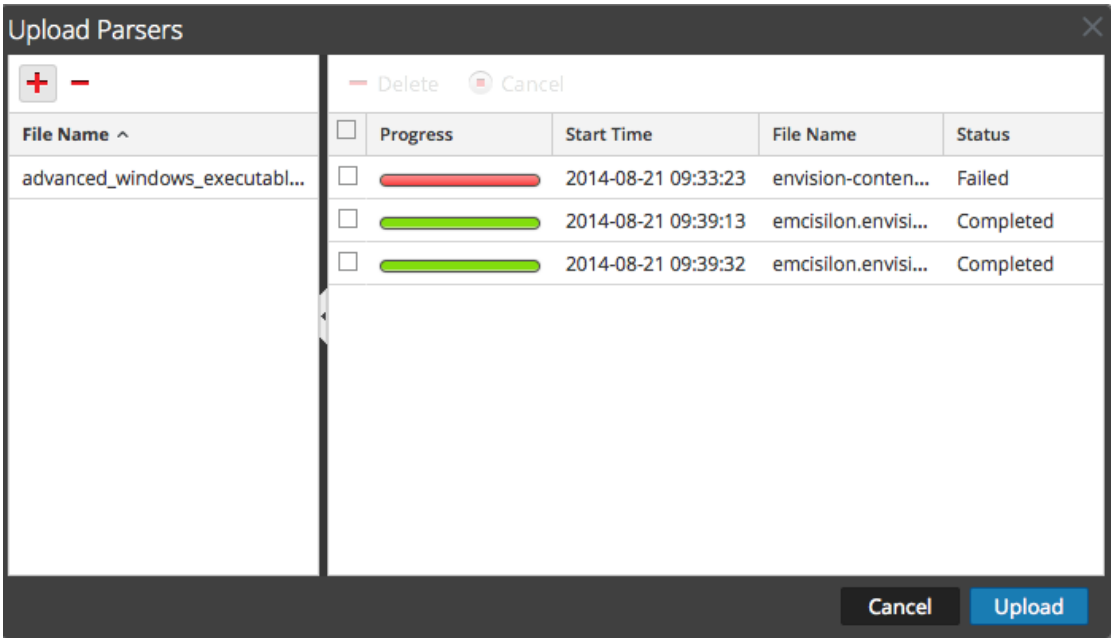


4. Klicken Sie auf + .

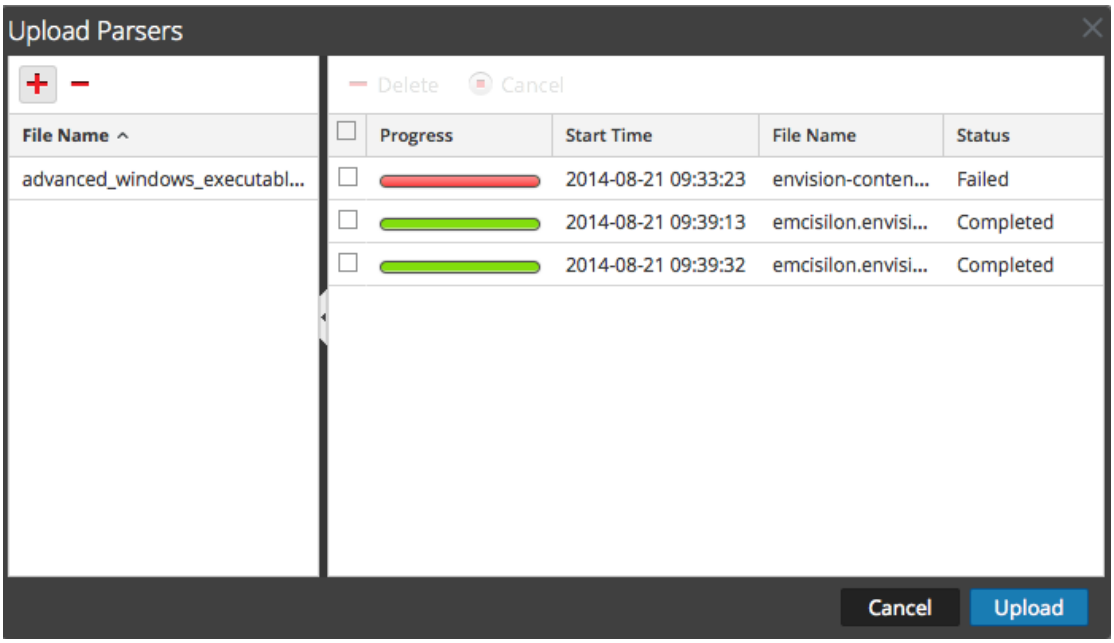
   Ein Dialogfeld zur Dateiauswahl wird angezeigt.

5. Wählen Sie die **.flex**-, **.parser**- und **.lua**-Dateien aus, die aktualisiert werden sollen, und klicken Sie auf **Öffnen**.

   Das Dialogfeld wird geschlossen und die ausgewählten Dateien werden in der Dateiliste angezeigt.



6. Klicken Sie auf **Hochladen**.
   Das Raster „Job hochladen“ zeigt den Uploadfortschritt an; hierbei steht jeder Job für eine hochgeladene Datei.



7. Mit den Tools im Raster können Sie den Upload der ausgewählten Jobs managen: Sie können Jobs anhalten und wiederaufnehmen, abbrechen und löschen.
   Wenn ein Job abgeschlossen ist, wird der Parser im Decoder bereitgestellt und auf der Registerkarte „Parser“ bei den bereitgestellten Parsern aufgeführt.

Managen von Uploadjobs

Mit den Uploadrastertools können Sie den Upload der ausgewählten Jobs managen: Sie können Jobs anhalten und wiederaufnehmen, abbrechen und löschen.

- Wenn Sie den Upload einer Gruppe von Parsern abbrechen möchten, während sich der Upload in der Warteschlange befindet oder bereits läuft, klicken Sie auf Cancel.
- Wenn Sie den Upload einer Gruppe von Parsern anhalten möchten, klicken Sie, bevor der Upload abgeschlossen ist, auf Pause.
- Wenn Sie den angehaltenen Upload einer Gruppe von Parsern fortsetzen möchten, klicken Sie auf Resume.
- Wenn Sie einen Uploadjob löschen möchten, klicken Sie auf .

Löschen von bereitgestellten Parsern

Mit der Option Löschen in der Ansicht „Services-Konfiguration“ > Registerkarte „Parser“ können Sie bereitgestellte Parser aus einem Decoder oder Log Decoder löschen. Parser können hinzugefügt und entfernt werden, während ein Decoder ausgeführt wird, ohne die Erfassung zu beeinträchtigen.

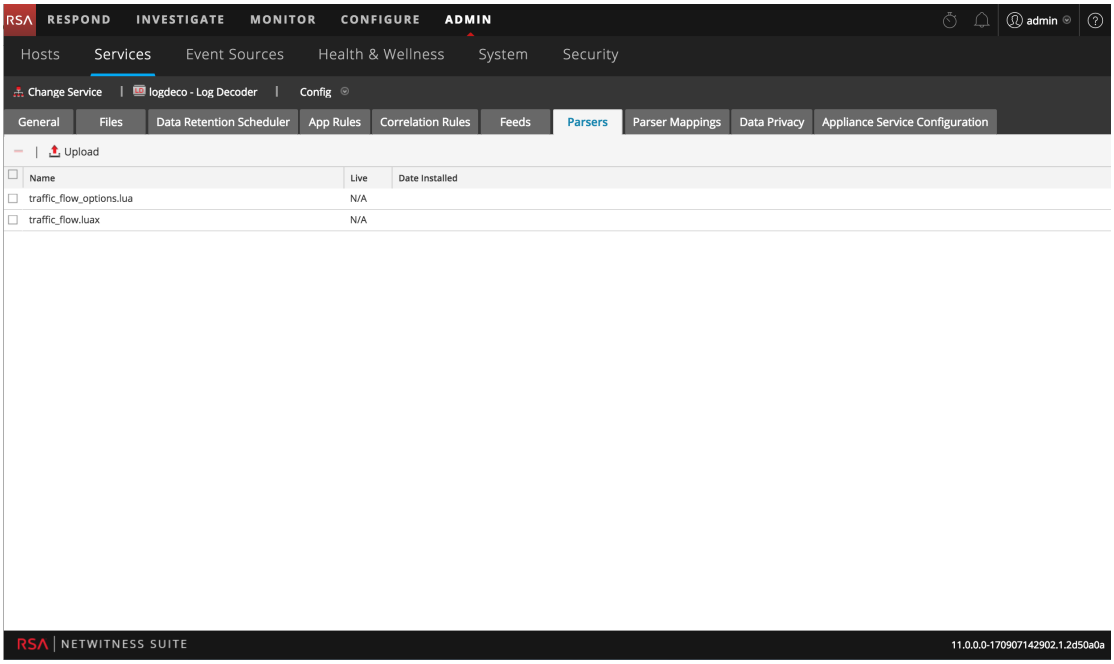
Hinweis: Wenn nicht anders angegeben, gilt jede Aussage über Decoder auch für Log Decoder.

So löschen Sie einen Parser aus einem Decoder:

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Service aus und dann > **Ansicht > Konfiguration**.

   Die Ansicht „Services-Konfiguration“ für den ausgewählten Service wird angezeigt.

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



3. Wählen Sie auf der Registerkarte **Parser** einen oder mehrere Parser zum Löschen aus.
4. Klicken Sie auf .

   In einem Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Parser löschen möchten.

5. Wenn Sie die Parser löschen möchten, klicken Sie auf **Ja**.

   Die Parser werden sofort aus dem Decoder entfernt.

Aktivieren und Konfigurieren des Entropy Parser

Ab NetWitness Suite 11.0 kann der Administrator einen nativen NetWitness-Parser, den Entropy Parser, für einen Decoder konfigurieren. Wenn der Entropy Parser aktiviert ist, können Analysten Kanäle sehen, die sich versuchen in anderen Verkehr einzufügen, aber kein normales Protokollverhalten aufweisen. Dadurch können Kanäle identifiziert werden, die nicht dem normalen Umgebungsverkehr entsprechen und daher möglicherweise einer Untersuchung bedürfen.

Der Parser erstellt Metaschlüssel basierend auf vom nativen NetWitness Suite-Parser erfassten Statistiken, mit denen das Verhalten von Kanälen, die sehr viel Netzwerkverkehr aufweisen, identifiziert werden kann. Bei der ersten Aktivierung des Parsers müssen die Analysten sich zunächst mit dem allgemeinen Verhalten der verschiedenen Kanäle in der erfassten Sitzung vertraut machen, um die Bytefrequenz und die normale Client-und Servernutzlast zu verstehen. Wenn die Analysten das normale Verhalten kennen, können sie mithilfe der Metaschlüssel auffälliges Verhalten finden, das nicht dem erwarteten Verhalten entspricht.

Standardmäßig erzeugt der Entropy Parser 10 zusätzliche Metaschlüssel, die die Last an einem Decoder nicht wesentlich erhöhen und für diesen speziellen Fall sehr nützlich sind. Der Parser ist standardmäßig deaktiviert.

Aktivieren Sie die Indexierung, wenn Sie interessante Sitzungen basierend auf einer Nutzlastbyte-Analyse der Pakete untersuchen möchten. Standardmäßig wird der normale `Float32`-Wert für `entropy.req` und `entropy.res` mit 10.000 multipliziert und in `UInt16` gespeichert (und ergibt eine Ganzzahl mit maximal 5 Stellen: 0 bis 10.000), um die Indexierung zu vereinfachen.

Wenn Sie jedoch die `entropy.*`-Felder in der Decoder-Sprache als `Float32` definieren, speichert der Decoder ihn als Gleitkommazahl mit einem Bereich von 0,0 bis 1,0. Achten Sie darauf, überall die Sprache zu ändern, wenn Sie ihn als `Float32` beibehalten möchten.

RSA empfiehlt die Indexierung als `Float32` nicht, da dabei eine sehr hohe Anzahl eindeutiger Werte aufgrund von kleinsten Änderungen in der Genauigkeit entsteht.

Dies sind die 10 neuen Metaschlüssel, die vom Entropy Parser standardmäßig erzeugt werden:

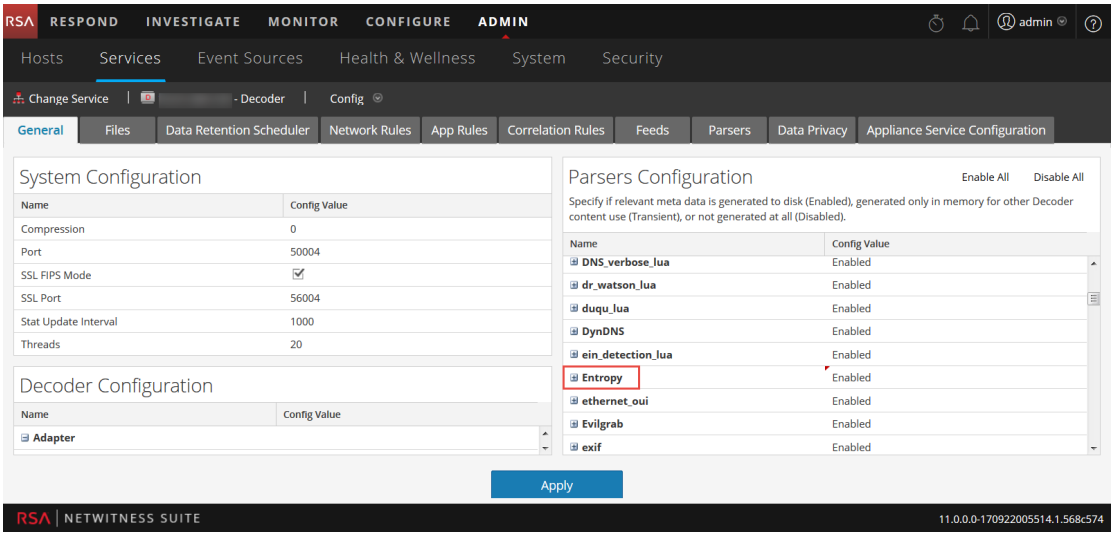
- `entropy.req` und `entropy.res`: Diese Metaschlüssel erfassen die Entropie mithilfe der Entropiegleichung nach Shannon, die einen Gleitkommawert als Ergebnis hat. Der Gleitkommawert von 0 bis 1,000 wird mit 10.000 multipliziert und in die NetWitness Suite als `UInt 16` geschrieben: als vorzeichenlose Ganzzahl von 0 bis 10.000.
- `mcb.req` und `mcb.res`: Das häufigste Byte ist ganz einfach das Byte, das für jede Seite (0 bis 255) am häufigsten gesehen wurde.
- `mcbc.req` und `mcbc.res`: Die Anzahl des häufigsten Bytes ist die Häufigkeit, mit der das häufigste Byte (siehe oben) in den Sitzungsstreams gesehen wurde.
- `ubc.req` und `ubc.res`: Die Anzahl der eindeutigen Bytes ist die Zahl der eindeutigen Bytes,

die in jedem Stream gesehen wurden. 256 bedeutet z. B., dass alle Bytewerte von 0 bis 255 mindestens einmal gesehen wurden.

- `payload.req` und `payload.res`: Die Nutzlastgrößen-Kennzahlen sind die Nutzlastgrößen jeder Sitzungsseite zum Zeitpunkt des Parsings. Um hohe Anzahlen eindeutiger Werte (schlecht für die Performance) in der Indexierung zu vermeiden, werden die folgenden zwei Nutzlastgrößen-Metadaten auf die genannte Weise berechnet:
  - Weniger als 1.000: Die genaue Anzahl der Nutzlastbytes wird zurückgegeben.
  - 1.000 oder mehr: wird auf den nächsten 1.000er abgerundet. Eine Größe von 5.826 würde also als 5.000 gespeichert werden.

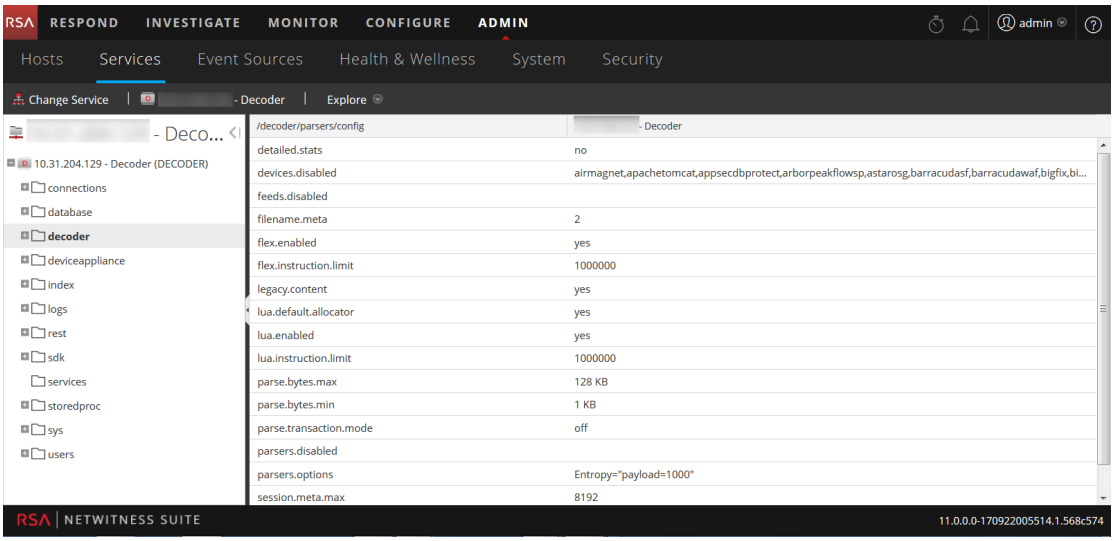
Aktivieren und Konfigurieren des Entropy Parsers in einem Decoder

1. Melden Sie sich bei RSA NetWitness an und wählen Sie im Menü NetWitness Suite die Optionen **Administration > Services** aus.
2. Wählen Sie in der Ansicht „Services“ den Decoder, den Sie konfigurieren möchten, und dann **Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ für den ausgewählten Decoder wird angezeigt.
3. Der Entropy Parser ist standardmäßig deaktiviert. Klicken Sie auf die Drop-down-Liste unter **Konfigurationswert** und wählen Sie **Aktiviert**. Wenn Sie einige der Metaschlüssel deaktivieren möchten, klicken Sie auf die Drop-down-Liste und wählen Sie neben dem jeweiligen Metaschlüssel **Deaktivieren** aus.



4. Klicken Sie auf **Anwenden**.
   Der Entropy Parser ist aktiviert und beginnt mit der Erstellung der neuen Metaschlüssel, die in der benutzerdefinierten Concentrator-Indexdatei konfiguriert sind.

5. Navigieren Sie zur **Ansicht „Durchsuchen“** für den Decoder und wählen Sie den Node **decoder > parsers > config** aus. In `parsers.options` können Sie Nutzlast des Entropy Parsers festlegen. Der im Screenshot gezeigte Standardwert ist `Entropy = payload = 1000`. Wenn Sie den Wert definieren, lautet die Syntax `Entropy = payload = "1000"`. Die Anführungszeichen sind erforderlich, wenn der Wert Leerzeichen aufweist, und es wird empfohlen, diese prinzipiell immer zu verwenden, damit keine Probleme aufgrund von Leerzeichen auftreten können. Wenn Sie die genaue Nutzlast sehen möchten, legen Sie diesen Parameter auf „1“ fest.



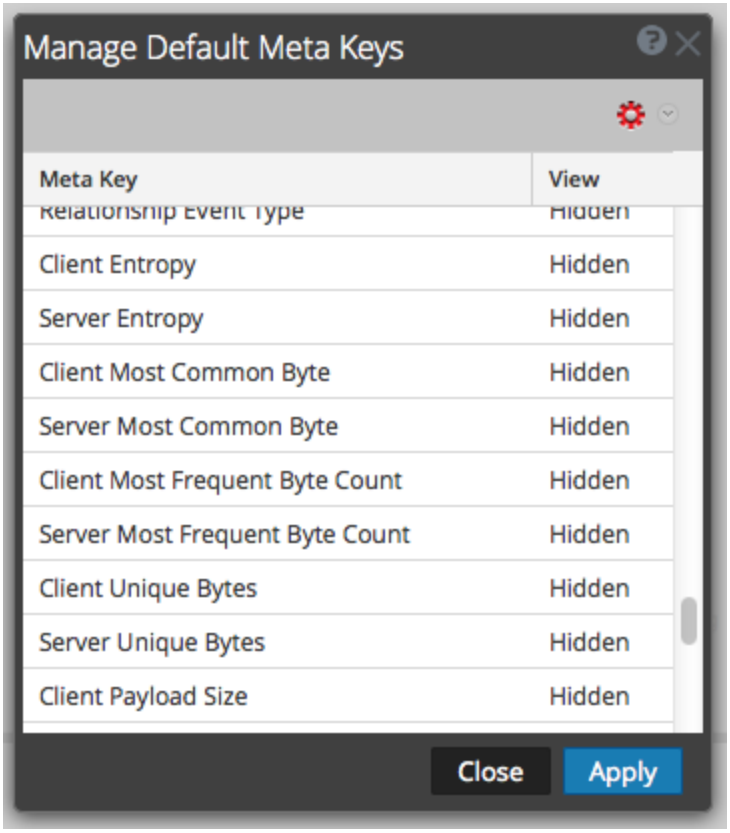
Die standardmäßige Entropy-Nutzlast ist 1.000, d. h.: Wenn die Nutzlast kleiner als 1.000 ist, wird der genaue Wert bereitgestellt. Wenn die Nutzlast größer als 1.000 ist, wird der Wert auf die nächsten 1.000er abgerundet. Beispielsweise wird ein Wert von 3.798 auf 3.000 abgerundet.

6. Wenn Sie den standardmäßigen Rundungsfaktor für die Entropy-Nutzlast ändern möchten, können Sie den Wert bearbeiten. Diese Änderung wird wirksam, wenn der Parser neu geladen wird.

7. Wählen Sie in der Ansicht „Services-Konfiguration“ den Concentrator aus, der den Datenverkehr von diesem Decoder aggregiert. Wählen Sie **Anzeigen > Dateien** und öffnen Sie die benutzerdefinierte Indexdatei für den Concentrator. Suchen Sie nach den Metaschlüsseln des Entropy Parsers, um festzustellen, ob sie enthalten und nicht auskommentiert sind.
   Standardmäßig sind die Schlüssel auskommentiert und daher nicht aktiviert. Um diesen Teil der Sprache zu aktivieren, muss der Administrator diesen Teil der Indexdatei in `index-concentrator-custom.xml` kopieren und die Zeile `key description` für jeden

Metaschlüssel auskommentieren. Unten finden Sie ein Beispiel der benutzerdefinierten Indexdatei mit den Schlüsseln des Entropy Parsers und Anweisungen.

8. Sind die Entropy-Metaschlüssel aktiviert, sind sie für Analysten in Investigate verfügbar, aber standardmäßig ausgeblendet. Um die Metaschlüssel in der Ansicht „Werte untersuchen“ sichtbar zu machen, bearbeiten Sie die Standardmetaschlüssel im Dialogfeld „Standardmetaschlüssel“ so, dass sie offen sichtbar und nicht ausgeblendet sind. Sie können diese Metaschlüssel genau wie andere Metaschlüssel managen.



Konfiguration des Entropy Parsers in der benutzerdefinierten Concentrator-Indexdatei

Im Folgenden ist ein Auszug der Concentrator-Indexdateizeilen zu sehen, die der Administrator in die benutzerdefinierte Indexdatei kopieren muss. Die Kommentare enthalten Anleitungen zur Konfiguration des Parsers.

```
<!-- This section is commented out because it's only used by the Entropy
parser which is disabled by default. To enable this part of the
language, copy to index-concentrator-custom.xml and uncomment the keys.
HOWEVER, take note that depending on how the Entropy parser is
configured, the entropy.req and entropy.res format might be a Float32
instead of a UInt16. So make sure to change to the correct type if
necessary.-->

<!-- Entropy parser meta - enable indexing if you have interest in
exploring this for interesting sessions based on payload byte analysis
of the packets. By default, to make indexing easier, the normal Float32
value for entropy.res and entropy.req is multiplied by 10k and stored in
a UInt16 (thus giving 4 digits of precision, 0 to 10,000). However, if
you define the *.entropy fields in the Decoder language to be Float32,
it will store it as a float with a range of 0.0 to 1.0. Take care to
change the language everywhere if you decide to keep it as a Float32. We
also don't recommend indexing as a Float32.-->

<!--

<key description="Client Entropy" format="UInt16" level="IndexNone"
name="entropy.req" valueMax="10001"/>

<key description="Server Entropy" format="UInt16" level="IndexNone"
name="entropy.res" valueMax="10001"/>

-->

<!-- The most common byte is simply which byte for each side (0 thru
255) was seen the most -->

<!--

<key description="Client Most Common Byte" format="UInt8"
level="IndexNone" name="mcb.req"/>

<key description="Server Most Common Byte" format="UInt8"
level="IndexNone" name="mcb.res"/>

-->

<!-- The most frequest byte count is the number of times the most common
byte was seen in the session streams -->

<!--

<key description="Client Most Frequent Byte Count" format="UInt32"
level="IndexNone" name="mcbc.req" valueMax="500000"/>

<key description="Server Most Frequent Byte Count" format="UInt32"
level="IndexNone" name="mcbc.res" valueMax="500000"/>

-->
```

```
<!-- Unique byte count is the number of unique bytes seen in each
stream. 256 would mean all byte values of 0 thru 255 were seen at least
once -->

<!--

<key description="Client Unique Bytes" format="UInt16" level="IndexNone"
name="ubc.req"/>

<key description="Server Unique Bytes" format="UInt16" level="IndexNone"
name="ubc.res"/>

-->

<!-- The payload size metrics are the payload sizes of each session side
at the time of parsing. However, in order to keep

indexing from having high unique counts (bad for performance), the two
payload size meta values below are calculated like so:

Less than 1000 is the exact number of payload bytes

1000 or greater is bucketed in increments of 1000. So a size of 5826
would be stored as 5000. -->

<!--

<key description="Client Payload Size" format="UInt32" level="IndexNone"
name="payload.req" valueMax="500000"/>

<key description="Server Payload Size" format="UInt32" level="IndexNone"
name="payload.res" valueMax="500000"/>

-->
```

Decoder und Log Decoder – zusätzliche Verfahren

In diesem Thema werden zusätzliche Verfahren für Administratoren beschrieben, die für die Konfiguration des Decoder oder Log Decoder nicht zwingend erforderlich sind.

Themen

Konfigurieren der 10G-Funktion

In diesem Thema erfahren Administratoren, wie ein Paket-Decoder speziell für die Hochgeschwindigkeits-Paketerfassung mit NetWitness Suite 11.0 optimiert werden kann. Dies gilt für die Erfassung von Paketen über die 10G-Schnittstellenkarte. Für die Hochgeschwindigkeits-Paketerfassung ist eine sorgfältige Konfiguration erforderlich, da diese die Decoder-Hardware stark belastet. Lesen Sie daher das gesamte Thema, wenn Sie eine 10G-Erfassungslösung implementieren möchten.

RSA NetWitness Suite bietet Unterstützung für die Hochgeschwindigkeitserfassung auf dem Decoder. Sie können Netzwerkdatenpakete von schnelleren Netzwerken erfassen und Ihren Packet Decoder so optimieren, dass Netzwerkdatenverkehr bis zu 8 Gbit/s bei kontinuierlichem Durchsatz und bis zu 10 Gbit/s bei Belastungsspitzen erfasst werden kann, je nachdem, welche Parser und Feeds aktiviert sind.

Zu den Verbesserungen bei der Erfassung in diesen Umgebungen gehören folgende:

- Verwendung der Treibererfassungsfunktion `pf_ring`, um die handelsübliche 10G-Netzwerkschnittstellenkarte von Intel für die Hochgeschwindigkeitserfassung nutzen zu können.
- Einführung der `assembler.parse.valve`-Konfiguration, durch die die Anwendungsparser bei Überschreitung bestimmter Schwellenwerte automatisch deaktiviert werden, um die Gefahr eines Datenpaketverlusts einzudämmen. Wenn die Anwendungsparser deaktiviert sind, sind Parser der Netzwerkschicht weiterhin aktiv. Wenn die Statistikwerte wieder unter den Schwellenwert sinken, werden die Anwendungsparser automatisch erneut aktiviert.

Hardwarevoraussetzungen

- Ein Decoder der Serie 4S oder 5
- Eine Intel 82599-basierte Ethernetkarte, z. B. Intel x520. Alle von RSA bereitgestellten 10G-Karten erfüllen diese Anforderung. Zwei Beispiele:
  - Alle von RSA zur Verfügung gestellten SMC-10GE-Karten
  - Eine Dell Network Daughter Card mit einem Intel-Controller, die 10G-Netzwerkschnittstellen zur Verfügung stellt. Dies ist in jeglicher Hardware der Serie 5 enthalten.
- Nur bei der Serie 4S/Dell R620: 96 GB DD3-1600-Arbeitsspeicher in **Dual-Rank**-DIMMs. Single-Rank-DIMMs können die Performance um bis zu 10 % verringern. Führen Sie zur Ermittlung der Geschwindigkeit und des Rank-Typs der installierten DIMMs folgenden

Befehl aus:

```
dmidecode -t 17.
```

- Ausreichend großer und schneller Speicher zur Erfüllung der Erfassungsanforderungen. Überlegungen zum Speicher werden später in diesem Thema behandelt.
- Jeder Packet Decoder wurde mit mindestens zwei DACs oder SAN-Verbindung konfiguriert.

Softwarevoraussetzungen

- Bei Dell R620-basierten Systemen, z. B. der Serie 4S, muss das BIOS auf v1.2.6 oder höher aktualisiert werden.
- Die 10G-Decoder-Funktion wird nur in von RSA bereitgestellten Decoder-Installations-Images unterstützt. Jegliche erforderliche Software wird standardmäßig installiert.
- Wenn Sie ein Upgrade einer früheren Version durchführen, sollten Sie dies abgeschlossen haben, bevor Sie mit der Konfiguration fortfahren.

Installieren des 10G-Decoders

Hinweis: Wenn Sie über neue Hardware der Serie 5 verfügen, können Sie direkt mit „Konfigurieren des 10G-Decoders“ fortfahren.

Führen Sie die folgenden Schritte aus, um den NetWitness 10G-Decoder zu installieren:

Herunterladen und Aktualisieren des BIOS

Hinweis: Bei früheren BIOS-Versionen vor v1.2.6 treten Probleme bei der eindeutigen Identifizierung des Orts der 10G-Erfassungskarte innerhalb des Systems auf. Es wird empfohlen, dass Kunden eine Aktualisierung auf das aktuelle BIOS v2.2.3 durchführen, aber es ist nicht erforderlich für 10G, wenn Sie v1.2.6 oder höher ausführen.

1. Laden Sie BIOS v2.2.3 von folgendem Speicherort herunter:

   http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=V7P04
2. Laden Sie das Updatepaket für Red Hat Linux herunter.
3. Kopieren Sie die Datei auf den NetWitness-Server.
4. Melden Sie sich als `root` an.
5. Ändern Sie die Berechtigungen für die Datei auf execute.
6. Führen Sie die folgende Datei aus:

   ```
   ./BIOS_V7P04_LN_2.2.3.BIN
   ```

7. Starten Sie das System neu, wenn die Ausführung abgeschlossen und ein Neustart erforderlich ist.

Hinweis: Das BIOS-Installationsverfahren dauert ungefähr 10 Minuten.

Suchen nach den Decoder 10G-Paketen

Die zum Konfigurieren des 10G-Decoders erforderlichen Pakete sollten sich bereits im Decoder-Installations-Image befinden. Sie sollten keine zusätzlichen Pakete installieren müssen. Die Pakete, die die 10G-Treiberfunktion bieten, sind folgende:

- `pfring-dkms-6.5.0-6.rpm`
- `ixgbe-zc-4.1.5.6-dkms.noarch.rpm`

Überprüfen, ob 10G-Decoder-Pakete installiert sind

Die Installation der 10G-Decoder-Pakete wird automatisch durchgeführt. Daher sollten keine Maßnahmen zur Aktivierung der 10G-Funktion erforderlich sein.

- Wenn Sie für die Kernel-Pakete ein Upgrade durchgeführt haben, ist ein Neustart erforderlich. Das Betriebssystem wird neu kompiliert und Treiber für den aktualisierten Kernel werden installiert.
- Wenn Sie bei Auswahl des Erfassungsportadapters (im Folgenden beschrieben) zusätzliche `PFRINGZC`-Schnittstellen sehen, war die Installation erfolgreich.

Konfigurieren des 10G-Decoders

Führen Sie die folgenden Schritte aus, um den 10G-Decoder zu konfigurieren:

1. Klicken Sie in der **Decoder Explorer**-Ansicht mit der rechten Maustaste auf **Decoder** und wählen Sie **Eigenschaften** aus.
2. Wählen Sie im Drop-down-Menü „Eigenschaften“ die Option **reconfig** aus und geben Sie die folgenden Parameter ein:
   `update=1 op=10g`
   Dadurch wird die Pipeline der Decoder-Paketverarbeitung für einen höheren Durchsatz von Rohdaten, aber weniger Parsingmöglichkeiten angepasst.
3. Klicken Sie in der Ansicht **Decoder Explorer** mit der rechten Maustaste auf **Datenbank** und wählen **Eigenschaften** aus.
4. Wählen Sie im Drop-down-Menü **Eigenschaften** die Option **reconfig** aus und geben Sie die folgenden Parameter ein:
   `update=1 op=10g`

Dadurch wird die Paketdatenbank an die Verwendung von sehr großen Dateien und direktes I/O angepasst.

5. Wählen Sie den Erfassungsportadapter aus. Hierzu gehören die folgenden Optionen:
   - Erfassung von einem Port: **PFRINGZC,p1p1** oder **PFRINGZC,p1p2**
   - Erfassung von beiden Ports: Wählen Sie **PFRINGZC,P1P1** aus und legen Sie in der **Explorer**-Ansicht `capture.device.params = device=zc:p1p2,zc:p1p1` fest.
6. Wenn der Schreib-Thread Schwierigkeiten hat, die Geschwindigkeit der Erfassung zu unterstützen, können Sie Folgendes versuchen:

   Ändern Sie `/datebase/config/packet.integrity.flush` zu `normal`.

   Hinweis: Sie können versuchen, `packet.file.size` auf einen höheren Wert einzustellen, aber halten Sie die Dateigröße unter 10 GB, da die gesamte Datei im Arbeitsspeicher gepuffert wird.
7. (Optional) Das Parsen von Anwendungen ist äußerst CPU-intensiv und kann dazu führen, dass der Decoder Pakete verliert. Um Paketverluste durch das Anwendungsparsing zu vermeiden, können Sie `/decoder/config/assembler.parse.valve` auf `true` festlegen. Dies sind die Ergebnisse:
   - Wenn das Sitzungsparsing zum Engpass wird, werden die Anwendungsparser (HTTP, SMTP, FTP usw.) vorübergehend deaktiviert.
   - Sitzungen gehen nicht verloren, wenn die Anwendungsparser deaktiviert werden, nur die Genauigkeit des auf diesen Sitzungen durchgeführten Parsings nimmt ab.
   - Sitzungen, die geparst werden, wenn die Anwendungsparser deaktiviert sind, haben immer noch zugehörige Netzwerkmetadaten (vom Netzwerkparser).
   - Die Statistik `/decoder/parsers/stats/blowoff.count` zeigt die Anzahl aller Sitzungen an, die Anwendungsparser umgangen haben (Netzwerkparsing wird immer noch durchgeführt).
   - Wenn Sitzungsparsing nicht länger ein potentieller Engpass ist, werden die Anwendungsparser automatisch wieder aktiviert.
   - Der Assembler-Sitzungspool sollte groß genug sein, um Sitzungen nicht zu erzwingen.
   - Sie können über die Statistik `/decoder/stats/assembler.sessions.forced` ermitteln, ob Sitzungen erzwungen werden (die Werte würden ansteigen). Außerdem würde sich `/decoder/stats/assembler.sessions` innerhalb mehrerer hundert von `/decoder/config/assembler.session.pool` befinden.
8. (Optional) Wenn Sie die MTU für die Erfassung anpassen möchten, fügen Sie den Parameter

`snaplen` zu `capture.device.params` hinzu. Im Gegensatz zu früheren Versionen muss `snaplen` nicht auf eine bestimmte Grenze aufgerundet werden. Der Decoder passt die MTU an den Erfassungsschnittstellen automatisch an.

9. Die folgenden Konfigurationsparameter sind veraltet und nicht mehr erforderlich:
   - Der `core= parameter` in `capture.device.params`
   - Alle Konfigurationsdateien im Verzeichnis `/etc/pf_ring`

   Hinweis: Ein nach dem Erstellen eines neuen Image installiertes Ethernetgerät benötigt keine Konfiguration zur Verwendung als Erfassungsgerät. Eine Konfiguration ist nur dann erforderlich, wenn es als Netzwerkschnittstelle verwendet wird oder wenn Systemprogramme ohne manuelle Konfiguration darauf zugreifen.

Typische Konfigurationsparameter

Typische Konfigurationsparameter sind unten aufgeführt. Die tatsächlichen Parameter variieren je nach Arbeitsspeichermenge und CPU-Ressourcen, die zur Verfügung stehen.

1. Einstellungen für Sitzungs- und Paketpool (unter `/decoder/config`):
   - `pool.packet.pages` = 1000000
   - `pool.session.pages` = 300000
2. Blockgröße des Paketschreibvorgangs unter (`/database/config/packet.write.block` Größe) festgelegt auf `filesize`

   Hinweis: Dies konfiguriert den Decoder, die Datei mit sehr langen Seiten zu puffern und für maximale Performance mithilfe von direktem I/O zu schreiben.
3. Parse-Thread-Anzahl (unter `/decoder/config`)

   `parse.threads =12`

Überlegungen zum Speicher

Bei der Erfassung mit 10G-Leitungsgeschwindigkeit muss das Speichersystem, auf dem die Paket- und Metadatenbank liegt, in der Lage sein, einen Schreibdurchsatz von 1.400 MB/s aufrechtzuerhalten.

Verwenden der Hardware der Serie 4S (mit zwei oder mehreren DAC-Einheiten)

Die Serie 4S ist mit einem Hardware-RAID-SAS-Controller ausgerüstet, der einen aggregierten I/O-Durchsatz von 48 Gbit/s unterstützt. Er verfügt über acht externe 6-Gbit-Ports, die in zwei SAS-Kabeln mit je 4 Bahnen zusammengefasst sind. Die empfohlene Konfiguration für 10G sieht mindestens zwei ausgeglichen aufgeteilte DAC-Einheiten für diese zwei externen Verbindungen vor. Beispiel: Schließen Sie einen DAC an einen Port auf der SAS-Karte und dann den zweiten DAC an den anderen Port auf der SAS-Karte an.

Für Umgebungen mit mehr als zwei DACs verbinden Sie sie von jedem Port in ausgewogener Weise. Dafür ist unter Umständen eine erneute Verkabelung der DACs in der bestehenden Bereitstellung erforderlich. Dies sollte sich jedoch nicht auf die Daten auswirken, die bereits auf dem Decoder erfasst wurden.

Wenn Sie neue Speicherkapazität hinzufügen, verwenden Sie das derzeit verfügbare Skript `NwMakeArray`, um die DAC-Einheiten bereitzustellen. Das Skript fügt automatisch einen DAC pro Ausführung hinzu (d. h. wenn drei DACs hinzugefügt werden sollen, muss das Skript dreimal ausgeführt werden). Die DACs werden der `NwDecoder10G`-Konfiguration als separate Mount-Punkte hinzugefügt. Die unabhängigen Mount-Punkte sind wichtig, da sie `NwDecoder10G` ermöglichen, I/O-Schreibvorgänge der Erfassung von I/O-Lesevorgängen zu trennen, die zum Erfüllen der Paketinhaltsanforderungen erforderlich sind.

Verwenden von SAN und anderen Speicherkonfigurationen

Der Decoder ermöglicht jede Speicherkonfiguration, die die Anforderung für kontinuierlichen Durchsatz erfüllt. Der standardmäßige 8-Gbit-FC-Link zu einem SAN ist nicht ausreichend, um Paketdaten bei 10G zu speichern. Um ein SAN verwenden zu können, muss daher ggf. eine Linkzusammenfassung mithilfe eines Software-RAID-Schemas auf mehreren Zielen durchgeführt werden. Somit sind Umgebungen mit SAN erforderlich, um die Verbindung zum SAN mit mehreren FCs zu konfigurieren.

Überlegungen zum Parsing und Inhalt

Das Parsen von Rohdatenpaketen bei hohen Geschwindigkeiten bringt einzigartige Herausforderungen mit sich. Angesichts der höheren Sitzungs- und Paketraten kommt der Parsingeffizienz die höchste Bedeutung zu. Ein einziger ineffizienter Parser (der zu lange für die Paketuntersuchung braucht) kann das gesamte System bis zu einem Punkt verlangsamen, an dem Pakete an der Karte abgewiesen werden.

Beginnen Sie anfängliche 10G-Tests nur mit nativen Parsern (außer SMB/WebMail). Verwenden Sie native Parser, um eine Baseline-Performance ohne oder mit nur sehr wenigen Paketverlusten zu ermitteln. Laden Sie keine Live-Inhalte herunter, bis dies erfolgt ist und das System die Erfassung bei hohen Geschwindigkeiten nachweislich ohne Probleme durchführt.

Nachdem das System betriebsbereit ist und reibungslos funktioniert, sollten Live-Inhalte (insbesondere Parser) sehr langsam hinzugefügt werden.

Best Practices

Unabhängig davon, ob Sie ein derzeit bereitgestelltes System aktualisieren oder ein neues System bereitstellen, wird empfohlen, dass Sie die folgenden Best Practices anwenden, um die Gefahr eines Datenpaketverlusts weitestgehend zu vermeiden. Ein Vorbehalt besteht dabei, wenn Sie eine aktuelle 10G-Bereitstellung aktualisieren, jedoch keinen zusätzlichen Datenverkehr hinzufügen. Beispielsweise sollte bei einem aktuellen Decoder, der die Erfassung von einer 10G-Karte mit einem kontinuierlichen 2G-Durchsatz durchführt, keine Performanceabweichung auftreten, es sei denn, die Aktualisierung bedingt auch das Hinzufügen von zusätzlichem Datenverkehr für die Erfassung.

- Integrieren Sie Baseline-Parser (außer SMB/Webmail, die in der Regel eine hohe CPU-Auslastung haben) und überwachen Sie sie, um sicherzustellen, dass nur wenige oder gar keine Datenpakete verloren gehen.
- Beim Hinzufügen zusätzlicher Parser dürfen Sie nur jeweils einen oder zwei Parser gleichzeitig hinzufügen.
- Messen Sie die Auswirkung des neu hinzugefügten Inhalts auf die Performance, vor allem in Spitzenzeiten mit hohem Datenverkehrsaufkommen.
- Wenn nun im Gegensatz zu vorher Paketverluste auftreten, deaktivieren Sie alle neu hinzugefügten Parser, aktivieren Sie sie einzeln nacheinander und messen Sie die Auswirkung. Hierdurch kann leichter ermittelt werden, welche Parser sich negativ auf die Performance auswirken. Es besteht die Möglichkeit, die Parser umzugestalten, um eine bessere Performance zu erzielen, oder den Funktionsumfang nur auf die für das Fallbeispiel des Kunden erforderlichen Funktionen zu reduzieren.
- Obwohl Feeds sich nur geringfügig auf die Performance auswirken, sollten sie auch überprüft und schrittweise hinzugefügt werden, um die Messung der Performanceauswirkungen zu erleichtern.
- Bei Anwendungsregeln lassen sich auch eher nur geringfügige Auswirkungen feststellen, obwohl es sich dennoch empfiehlt, nicht zu viele Regeln gleichzeitig hinzuzufügen, ohne die Auswirkung auf die Performance zu messen.

Darüber hinaus können durch die empfohlenen Konfigurationsänderungen, die im Abschnitt „Konfiguration“ erläutert werden, potenzielle Probleme minimiert werden.

Getestete Live-Inhalte

Die folgenden Parser können für unser Test-Dataset alle (nicht jeder einzelne) bei 10G ausgeführt werden:

- MA-Inhalte (7 Lua-Parser,1 Feed, 1 Anwendungsregel)
- 4 Feeds (alert ids info, nwmalwaredomains, warning und suspicious)
- 41 Anwendungsregeln
- DNS_verbose_lua (DNS deaktivieren)
- fingerprint_javascript_lua
- fingerprint_pdf_lua
- fingerprint_rar_lua

- fingerprint_rtf_lua
- MAIL_lua (MAIL deaktivieren)
- SNMP_lua (SNMP deaktivieren)
- spectrum_lua
- SSH_lua (SSH deaktivieren)
- TLS_lua
- windows_command_shell
- windows_executable

NICHT GETESTET:

- SMB_lua, natives SMB standardmäßig deaktiviert
- html_threat

ANDERE:

- HTTP_lua, reduziert die Erfassungsrate von >9G auf <7G. Bei knapp unter 5G kann dieser Parser statt des nativen Parsers ohne Verluste (zusätzlich zur Liste oben) verwendet werden.
- „xor_executable“ lastet die Parser-CPU zu 100 % aus und beim System können aufgrund des Parsebackups Verluste auftreten.

Aggregationsanpassungen basierend auf getesteten Live-Inhalten

Ein 10G-Decoder kann bei Ausführung bei einer Geschwindigkeit von 10G die Aggregation für einen einzigen Concentrator übernehmen. Bereitstellungen, die Malware Analysis, Event Stream Analysis, Warehouse Connector und Reporting Engine verwenden, beeinträchtigen voraussichtlich die Performance und können zu Paketverlusten führen.

Beim getesteten Szenario aggregiert der Concentrator 45–70.000 Sitzungen/Sek. Der 10G-Decoder erfasst 40–50.000 Sitzungen/Sek. Bei den oben genannten Inhalten entspricht dies ca. 1,5 bis 2 Millionen Meta/Sek. Aufgrund der großen Anzahl von Sitzungen werden die folgenden Konfigurationsänderungen empfohlen:

- Mit der „nice“-Aggregation auf dem Concentrator kann die Performanceauswirkung auf dem 10G-Decoder begrenzt werden. Mit dem folgenden Befehl wird die „nice“-Aggregation aktiviert.
  ```
  /concentrator/config/aggregate.nice = true
  ```
- Aufgrund der großen Anzahl von Sitzungen auf dem Concentrator sollten Sie erwägen, den Modus „parallel values“ auf dem Concentrator zu aktivieren, indem Sie den Wert

`/sdk/config/parallel.values` auf `16` festlegen. Hierdurch wird die Investigation-Performance verbessert, wenn die Anzahl der Sitzungen pro Sekunde über 30.000 liegt.

- Wenn mehrere Aggregationsstreams erforderlich sind, hat das Aggregieren vom Concentrator geringere Auswirkungen auf den Decoder.
- Weitere Prüfungen auf Inhalte und Parsing sind für Bereitstellungen erforderlich, bei denen andere NetWitness Suite-Komponenten verwendet werden sollen (z. B. Warehouse, Malware Analysis, ESA und Reporting Engine).

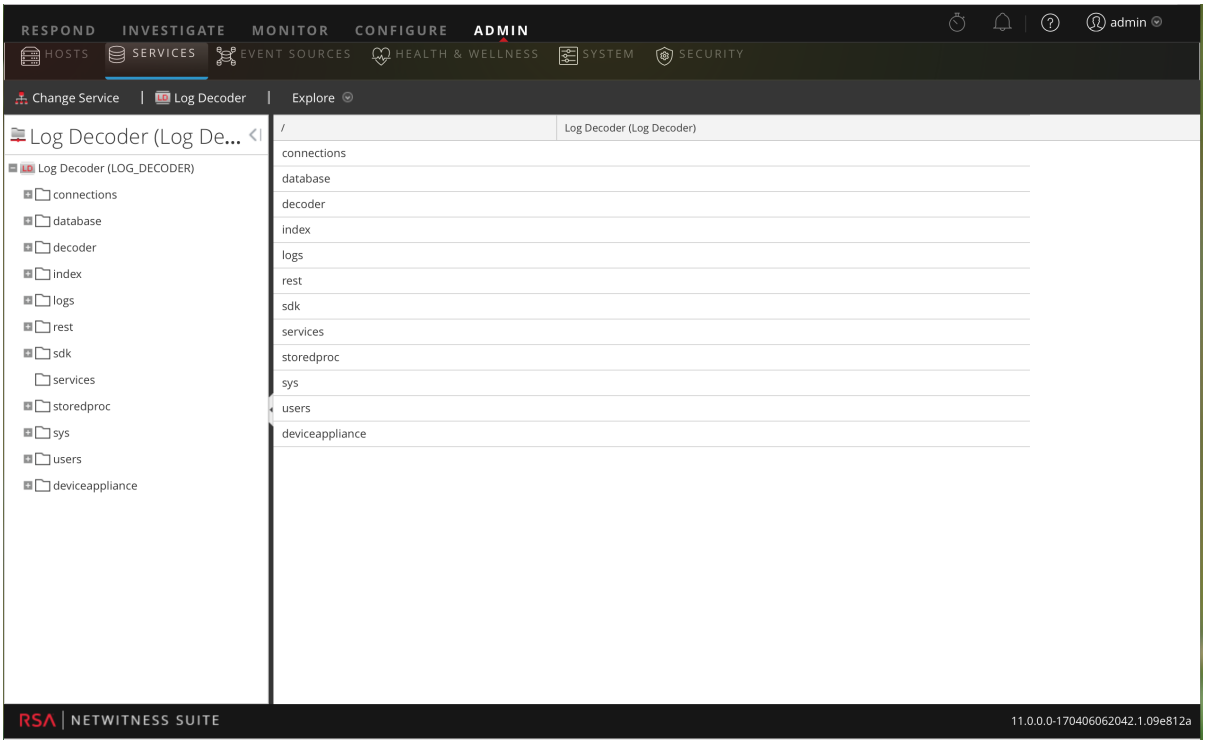
Konfigurieren eines Log Decoder für das Akzeptieren von Protobuf

Es gibt Situationen, in denen Sie Protokolldateien im Protobuf-Format (Protocol Buffer) analysieren müssen. Sie können einen Log Decoder konfigurieren, der Protokolle im protobuf-Format (Protocol Buffer) akzeptiert.

So importieren Sie eine Protokolldatei in einen Log Decoder:

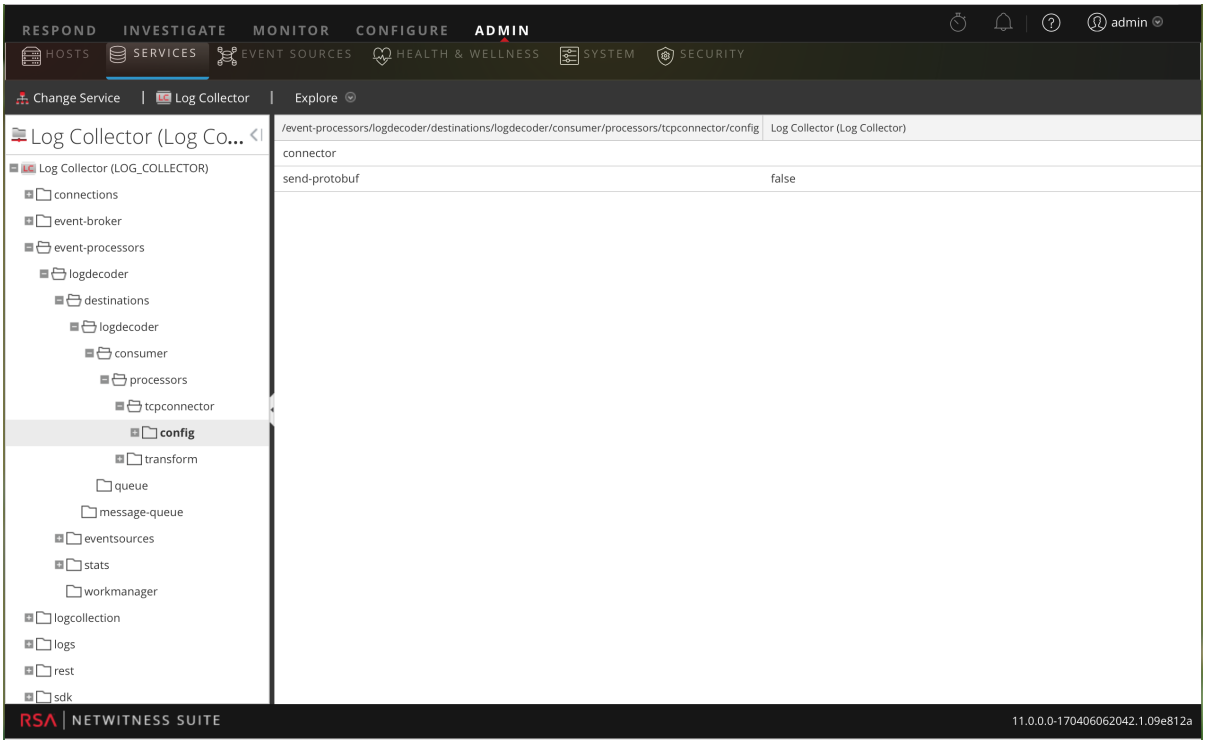
1. Navigieren Sie zu **Administration** > **Services**.
2. Wählen Sie in der Liste **Service** einen Log Decoder und dann > **Ansicht** > **Durchsuchen** aus.

   Die Ansicht „Durchsuchen“ für den Log Decoder wird angezeigt.



3. Navigieren Sie zu `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config`

.Der Bildschirm sollte ähnlich wie der folgende aussehen.



4. Wählen Sie für das Feld **send-protobuf** die Option **false** aus und ändern Sie den Wert auf **true**.
5. Navigieren Sie zu `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/channel/tcp` und ändern Sie den **port**-Wert in **50202**.
6. Navigieren Sie zu `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/event` und ändern Sie die folgenden Parameter:
   - Löschen Sie das Feld **Trennzeichen**.
   - Ändern Sie **Format** zu **%text%**

Konfigurieren von Timeouts für die Sitzungsteilung

Das Standardverhalten des Decoder besteht darin, Sitzungen automatisch zu beenden, die eine konfigurierte Größe überschreiten oder über einen bestimmten Zeitraum inaktiv waren. Wenn die Sitzung aufgrund eines Timeouts beendet wird, werden alle nachfolgenden, in dieser Sitzung empfangenen Pakete in einer neuen Sitzung gespeichert. Sie können die Auswirkungen der Sitzungsteilung aufgrund langer Inaktivität zwischen Paketen mit folgender Vorgehensweise abmildern.

Wenn eine Decoder-Sitzung eine konfigurierte Größe überschreitet (standardmäßig 32 MB, `/decoder/config/assembler.max.size`) oder über einen bestimmten Zeitraum inaktiv war, wird die Sitzung geteilt. Die NetWitness Suite verfügt über das vorherige Paket und das nächste Paket und kann den Sitzungsstatus vom ersten Sitzungsfragment an das nachfolgende Sitzungsfragment weitergeben.

Jedes Sitzungsfragment ist so gekennzeichnet (mit den Metadaten `session.split`), dass es identifiziert und mit anderen Fragmenten der tatsächlichen Netzwerksitzung verknüpft werden kann. Durch die in der ersten Sitzung ermittelte Richtung wird die Häufigkeit von Fragmenten mit umgekehrter Richtung reduziert.

Wenn zwischen Paketen eine so große Pause auftritt, dass keine Pakete für die Sitzung mehr im Arbeitsspeicher vorhanden sind, wird die Sitzung aus dem Decoder entfernt. Wenn anschließend ein nachfolgendes Paket eingeht, wird eine neue Sitzung erstellt, die keinen Kontext der vorherigen Sitzung enthält. Das Problem ist die fehlende Möglichkeit, eine Sitzung fortzuführen, wenn die Lücke zwischen den Paketen einer Sitzung größer ist als die Pakete, die gepuffert werden können (basierend auf verfügbarem Arbeitsspeicher und Timeoutkonfigurationen). Nachdem das letzte Paket einer Sitzung aus dem Arbeitsspeicher entfernt wurde, wird auch die Sitzung entfernt und mit ihr der notwendige Kontext für eine konsistente Richtung.

Es gibt zwei Timeouteinstellungen in einem Packet Decoder: `/decoder/config/assember.timeout.session` und `assembler.timeout.packet`. Standardmäßig gilt für beide 60 Sekunden. Die Einstellung `assembler.timeout.session` steuert, wie lange sich eine Sitzung im Assembler befinden kann, ohne ein weiteres Paket zu empfangen. Die Einstellung `assembler.timeout.packet` steuert, wie lange eine Sitzung in der Warteschlange bleiben kann, bevor sie analysiert wird. Wenn die Sitzung vor diesem Timout aus dem Assembler entfernt wird, wird sie automatisch analysiert.

Das Sitzungstimeout ist die Anzahl der Sekunden, seitdem dieser Sitzung das letzte Paket hinzugefügt wurde. Daher wird dieses Timeout jedes Mal zurückgesetzt, wenn der Sitzung ein Paket hinzugefügt wird. Das Pakettimeout ist die Anzahl der Sekunden, seitdem das erste Paket für diese Sitzung hinzugefügt wurde (das ist das Paket, das die Sitzung erstellt hat). Dies wird niemals zurückgesetzt und sobald das Timeout abläuft, wird die Sitzung analysiert.

Der wichtige Punkt ist hier, dass eine Sitzung analysiert werden kann und dennoch im Assembler verbleiben kann. Einer Sitzung im Assembler können noch Pakete hinzugefügt werden, selbst wenn sie bereits analysiert wurde. Pakete, die hinzugefügt werden, nachdem die Sitzung analysiert wurde, werden nie von Parsern verarbeitet, aber an die Sitzung angehängt. Sie können durch einen nachfolgenden Aufruf von `/sdk content` oder `/sdk packets` angezeigt werden.

Nachdem eine Sitzung analysiert wurde, werden die Sitzung UND seine Metadaten auf die Festplatte geschrieben. An diesem Punkt können sie aggregiert und und von `sdk`-Befehlen „gesehen“ werden. Pakete werden in der Reihenfolge der Erfassung geschrieben und nicht entsprechend der Sitzung, zu der sie gehören, neu sortiert. Außerdem werden sie auch nicht unbedingt geschrieben, wenn die Sitzung und die Metadaten geschrieben werden.

Sie können beide Timeout-Nodes (`/decoder/config/assembler.timeout.session` und `assembler.timeout.packet`) deaktivieren, indem Sie sie im Ansicht zum Durchsuchen zu einem Service auf Null setzen.

Wenn beide Timeouts deaktiviert sind, werden die Sitzungen nach wie vor aufgrund von Dauer oder Größe geteilt. Dennoch überwacht der Decoder den Netzwerkstream, solange er über ausreichend Arbeitsspeicher verfügt. Wenn in einem Netzwerkstream mehr Pakete eingehen, fügt der Decoder den nachfolgenden Sitzungen `split`-Metaelemente hinzu. Durch eine Kombination aus den `split` Metadaten und dem Streamschlüssel, ist es möglich, den Netzwerkstream aus mehreren Sitzungen rekonstruieren.

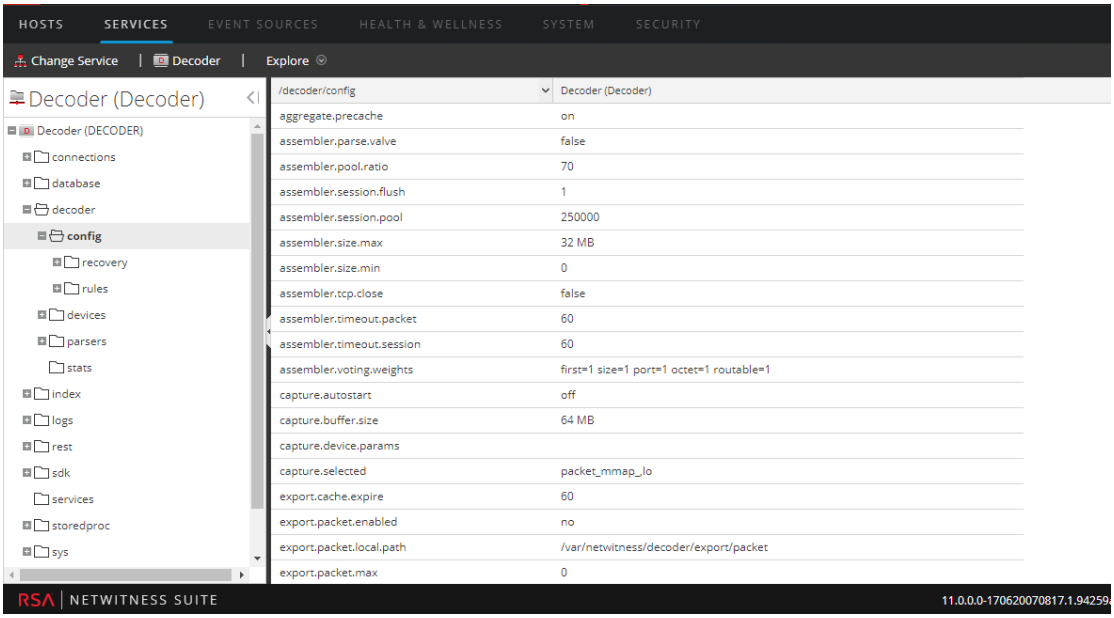
Die Zeitdauer, für die Sitzungen überwacht werden können, wird durch die Anzahl der auf dem Decoder verfügbaren Sitzungspooleinträge beschränkt, und daher variiert das tatsächliche Zeitfenster entsprechend der Geschwindigkeit, mit der neue Sitzungen hinzugefügt werden. Wenn neue Sitzungen mit hoher Geschwindigkeit hinzugefügt werden, verringert sich die Größe des Zeitfensters. Die Größe des Pools wird mit dem Konfigurationseintrag `/decoder/config/assembler.session.pool` festgelegt. Hierdurch wird die maximale Anzahl der Sitzungen definiert, die jeweils gleichzeitig überwacht werden können.

In der Statistik `/decoder/stats/assembler.timespan` können Sie sehen, wenn der Decoder keine Sitzungsteilungen mehr überwacht, da die Aufnahmerate zu hoch ist und der Decoder nicht mehr über genügend Arbeitsspeicher verfügt. Diese Statistik zeigt die Anzahl der überwachten Sekunden in der Sitzungstabelle. Dies ist das effektive Zeitfenster, in dem der Decoder Sitzungen verknüpfen kann. Im normalen Betrieb entspricht diese Statistik dem Wert von `/decoder/config/assembler.timeout.session`, aber bei der Ausführung im Modus „Zeitaufteilung“ wächst oder schrumpft die Statistik `/decoder/stats/assembler.timespan` abhängig von der Aufnahmerate.

Um den Modus „Zeitaufteilung“ zu konfigurieren, legen Sie die folgenden Konfigurationsparameter fest und starten Sie den Decoder neu:

1. Wählen Sie in der Ansicht „Administration“ > „Services“ den Decoder-Service und  **> Ansicht > Durchsuchen** aus.

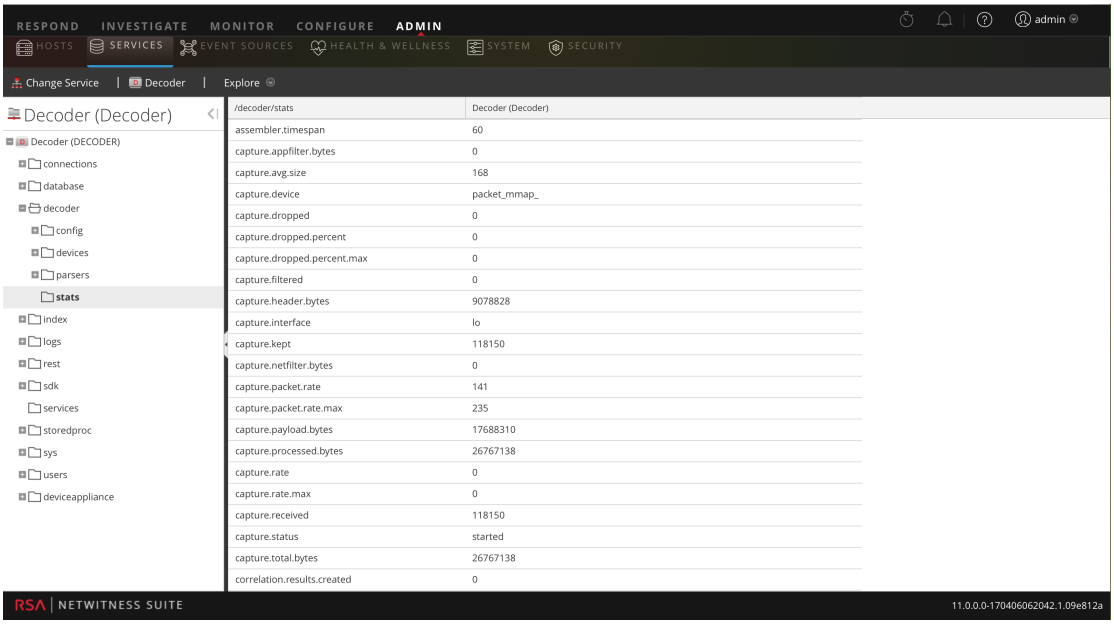
2. Wählen Sie in der Ansicht zum Durchsuchen zu einem Service-Ansicht den Eintrag **decoder** > **config**.



3. Klicken Sie neben dem Parameter in die Spalte **Wert** und legen Sie diese beiden Parameter fest:
   `/decoder/config/assembler.session.flush = 0`
   `/decoder/config/assembler.timeout.session = 0`

4. Um zu prüfen, ob der Decoder eventuell keine Sitzungsteilungen mehr überwacht, da die Aufnahmerate zu hoch ist und der Decoder nicht mehr über genügend Arbeitsspeicher verfügt, schauen Sie sich die Statistik `/decoder/stats/assembler.timespan` an:

Wählen Sie in der Ansicht zum Durchsuchen zu einem Service **decoder** > **stats** aus.



Konfigurieren der Syslog-Weiterleitung zum Ziel

Zusätzlich zur Sammlung von Syslog-Nachrichten können Sie den Log Decoder so konfigurieren, dass er Syslog-Nachrichten an einen anderen Syslog-Empfänger weiterleitet.NetWitness Suite leitet Syslog-Nachrichten nach der Analyse und vor der Erstellung der Nachricht für den Log Decoder weiter.

Hinweis: Sie müssen die Syslog-Weiterleitung mithilfe der in diesem Abschnitt beschriebenen Schritte unter **Verfahren** in der Ansicht **Durchsuchen** konfigurieren.

Der Log Decoder muss den **Gestartet**-Status aufweisen, damit Sie die Syslog-Weiterleitung konfigurieren können. So konfigurieren Sie die Syslog-Weiterleitung:

1. Konfigurieren Sie die Anwendungsebenenregeln (Anwendungsregeln) des Log Decoders, sodass Syslog-Nachrichten mit Metadaten markiert werden und NetWitness Suite den Befehl zur Nachrichtenweiterleitung erhält:

   a. Wählen Sie in der Ansicht **Services** einen Log Decoder und in der Spalte „Aktionen“ > **Ansicht** > **Durchsuchen** aus.

   b. Gehen Sie zu dem Node **/decoder/config/rules/application**, klicken Sie mit der rechten Maustaste auf **Anwendung** und klicken Sie auf **Eigenschaften**.

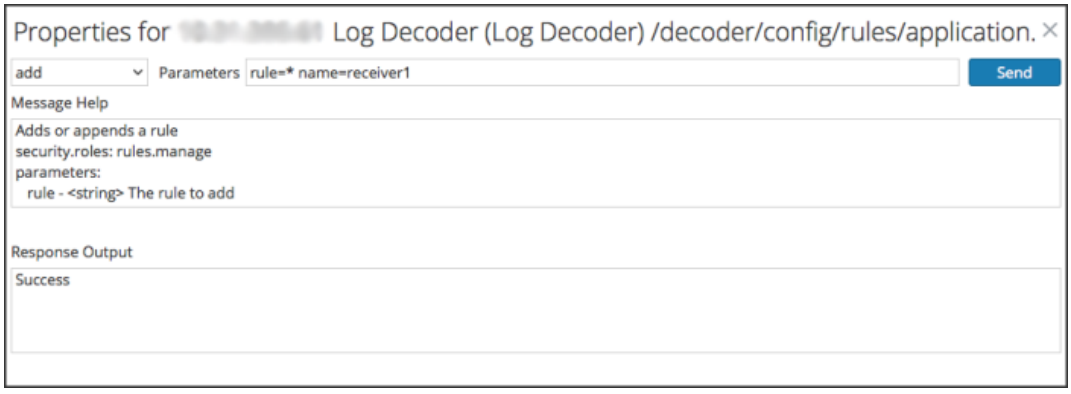
   c. Legen Sie in der Ansicht **Eigenschaften** den Befehl **add** mit den folgenden Parametern fest:

   `rule=<query> name=<name>`

   Beispiel 1: `rule=*name=receiver1`

   Beispiel 2: `rule="device.type='winevent_nic'" name=receiver`)

   d. Klicken Sie auf **Senden**.



NetWitness Suite erstellt die Regel `name=receiver1 rule=* order=<n>`. NetWitness Suite fügt die Position (z. B. `order=49`) entsprechend des

Zeitpunkts ein, an dem Sie die Regel erstellt haben.

0049	rule=* name=receiver1 order=49

e. Navigieren Sie zum Node `/decoder/config/rules/application` und klicken Sie auf die Regel `name=receiver1 rule=* order=49`.

f. Fügen Sie den Regelparametern **alert forward**-Parameter hinzu.

```
rule=* name=receiver1 order=49 alert forward
```

Alle anderen Regelparameter haben die gleiche Bedeutung wie in anderen Anwendungsregeln.

Das folgende Beispiel einer Anwendungsregel wählt alle Protokolle mithilfe der `*`-Regel aus. Sie erstellt ein Warnmeldungsmetadatum mit dem Wert **`receiver1`** und kennzeichnet das gesamte Protokoll zur Weiterleitung an das Syslog-Weiterleitungsziel. Sie können beliebig viele verschiedene Weiterleitungsregeln mit demselben oder mit eindeutigen Namen definieren.

2. Definieren von Syslog-Weiterleitungszielen und Aktivieren der Weiterleitung

a. Wählen Sie in der Ansicht **Services** einen Log Decoder und dann ⚙ > **Ansicht** > **Durchsuchen** aus.

b. Syslog-Weiterleitungsziele sind im Konfigurations-Node definiert `/decoder/config/logs.forwarding.destination`.
Dieser Konfigurations-Node enthält ein oder mehrere Name/Wert-Paare. Der Name entspricht dem Namensparameter in der Anwendungsregel, die Sie zum Markieren von Protokollen mit Weiterleitungs-Metadaten verwenden. Der Wert enthält das Transportprotokoll, den Host und den Port (getrennt durch Doppelpunkte) und danach optional einen Formatierungsparameter.
`name=(udp|tcp|tls):host:port[:(retainsource|rfc3164)]`
Der erste Parameter gibt das Transportprotokoll an und muss „udp“, „tcp“ oder „tls“ lauten. Bei Angabe von „udp“ werden Protokolldateien über das UDP-Syslog-Protokoll gemäß RFC 3164 / RFC 5426 weitergeleitet. Bei Angabe von „tcp“ werden Protokolle über eine TCP-Verbindung mit Framing gemäß RFC 6587 weitergeleitet. Bei Angabe von „tls“ werden Protokolle gemäß RFC 5425 weitergeleitet.

Der Host ist eine IPv4-Adresse, eine IPv6-Adresse oder der Hostname.

Der Port ist der Port, an den die Protokolle gesendet werden. Dies ist in der Regel der Port 514 für UDP-Syslog und 6514 für TLS-Verbindungen. Es gibt keine Standardportzuweisung für Syslog über TCP.

Optional kann `retainsource` oder `rfc3164` am Ende der destination-Zeichenfolge eingefügt werden, um darauf hinzuweisen, dass zusätzliche Formatierung und Informationen in jedem weitergeleiteten Protokoll enthalten sein müssen. Durch die Angabe von `retainsource` werden Z-Connector-Header an den Anfang des Protokolls eingefügt und mit den Metadaten `time`, `device.(ip|ipv6|host)` und `lc.cid` ausgefüllt. Diese Option ist am besten für das Weiterleiten an andere Log Decoder geeignet. Mit der Option `rfc3164` wird allen weitergeleiteten Ereignissen, die die Metadaten `syslog.pri`, `time` und `device.(ip|ipv6|host)` enthalten, ein gültiger RFC3164-Header vorangestellt. In beiden Fällen bleibt der ursprüngliche Protokolltext unverändert.

Beispiel für ein Weiterleitungsziel:

```
gears=tls:gears.netwitness.local:6514
```

Beispiel für die Weiterleitung über tcp zu blackout an Port 514 mit Z-Connector-Headers:

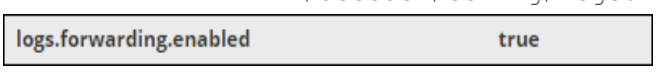
```
fwdrule=tcp:blackout.netwitness.local:514:retainsour
```

Geben Sie im Parameter `/decoder/config/logs.forwarding.destination` das Ziel an. Beispiel:
TLS-Verbindungen: `receiver1=tls:receiver1.netwitness.local:6514`
UDP-Verbindungen: `receiver1=udp:receiver1.netwitness.local:514`
TCP-Verbindungen: ***`receiver1=tcp:receiver1.netwitness.local:514`***

Hinweis:
Sie können Folgendes konfigurieren:
- Mehrere Regeln zum Weiterleiten von Protokollen an ein Ziel
- Mehrere Regeln zum Weiterleiten von Protokollen an mehrere Ziele

Im Falle von TLS-Verbindungen muss das Zertifikat des Weiterleitungsziels validiert werden. Die Zertifizierungsstelle, die das Zertifikat des Ziels signiert hat, muss im CA-Truststore des Log Decoders präsent sein und das Zertifikat muss sich im Ziel oder auf dem Syslog-Empfänger befinden. Weitere Informationen zur Bearbeitung des CA-Truststore für den Log Decoder finden Sie im Thema „Konfigurieren von Zertifikaten“ im *Protokollsammlung-Konfigurationsleitfaden*. (Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.)

c. Geben Sie im Parameter `/decoder/config/logs.forwarding.enabled` **true** an.



Konfigurieren der Transaktionsbehandlung auf einem Decoder

Ab Version 11.0 können Administratoren einen Decoder konfigurieren, um eingehende Sitzungen in kleinere Transaktionssitzungen zu unterteilen, wenn LUA-Parser zum Erstellen von Transaktionen verwendet werden. Die Funktion ermöglicht Analysten die Durchführung von Analysen der geteilten Sitzungen in Downstreamservices wie Ermittlung.

Transaktionsbehandlung

Der Konfigurations-Node des Decoder-Service verfügt über einen neuen Parameter für die Konfiguration der Transaktionsbehandlung: `/decoder/parsers/config/parser.transaction.mode`. Dieser Node steuert das Verhalten des Decoders, wenn ein Parser eine Transaktion innerhalb einer Netzwerksitzung definiert.

Die Werte für `parser.transaction.mode` entsprechen folgenden Betriebsmodi:

- `{{off}}` (Transaktionen deaktiviert)
- `{{meta}}` (Transaktionen werden als Metaelemente dargestellt)
- `{{split}}` (Teilen von Sitzungen)

Transaktionen deaktiviert

Wenn der Transaktionsmodus deaktiviert ist, werden vom Parser erstellte Transaktionen auf Anwendungsebene ignoriert, und in der Sammlung, die die Transaktion wiedergibt, wird nichts gespeichert.

Transaktionen werden als Metaelemente dargestellt

Wenn ein Parser eine Transaktion auf Anwendungsebene erzeugt, wird in diesem Betriebsmodus derjenigen Sitzung ein neues Metaelement des Typs `{{trans}}` hinzugefügt, in der die Transaktion stattgefunden hat. Das Metaelement `{{trans}}` enthält eine Liste anderer Metaelemente, die die Transaktion bilden.

Teilen von Sitzungen

Wenn ein Parser eine Transaktion auf Anwendungsebene erzeugt, wird die Sitzung in diesem Betriebsmodus geteilt. Die Sitzungsteilung wird wie folgt durchgeführt:

1. Es wird ein neues Sitzungselement erstellt.
2. Netzwerk-Metaelemente werden aus der analysierten Sitzung in die neue Sitzung kopiert.
3. In der Transaktion markierte Metaelemente werden aus der ursprünglichen Sitzung in die neue Sitzung verschoben.

Die folgenden Metaelemente werden aus der analysierten Sitzung in die geteilte Sitzung dupliziert:

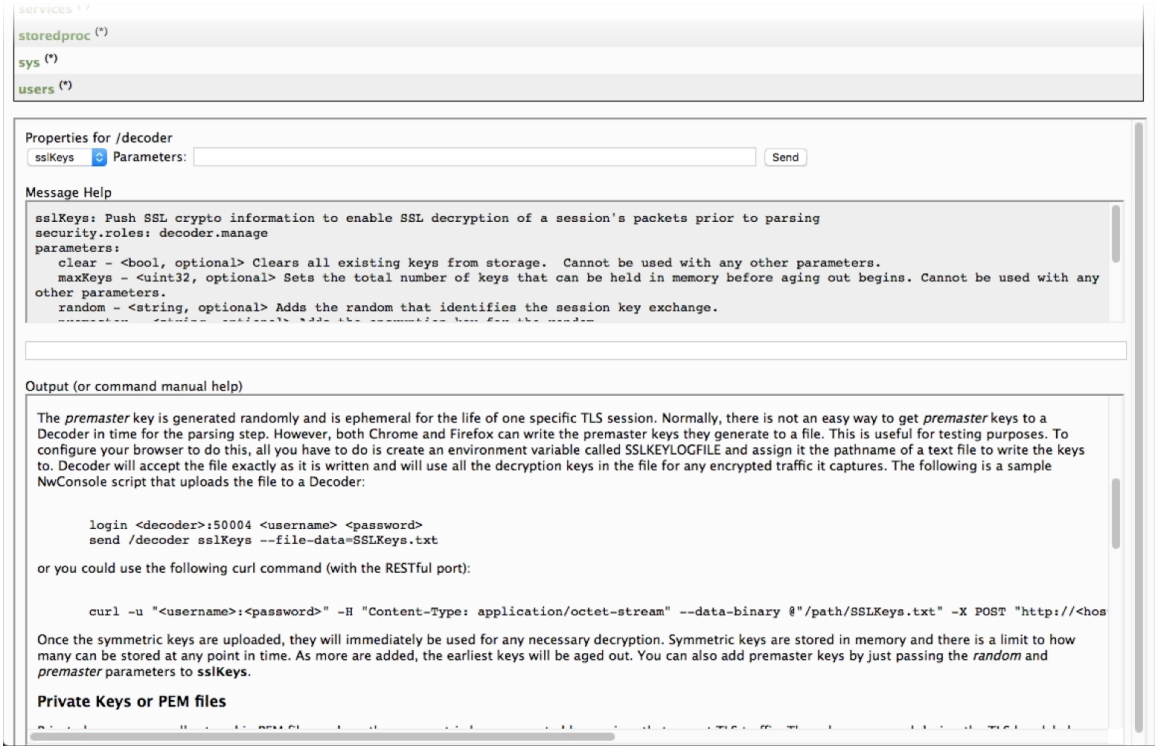
- time
- medium
- eth.src
- eth.dst
- eth.type
- ip.proto
- ip.src
- ip.dst
- ipv6.src
- ipv6.dst
- ipv6.proto
- tcp.srcport
- tcp.dstport
- tcp.flags
- udp.srcport
- udp.dstport
- service
- udp.srcport
- udp.srcport
- tls.premaster

Entschlüsseln eingehender Pakete

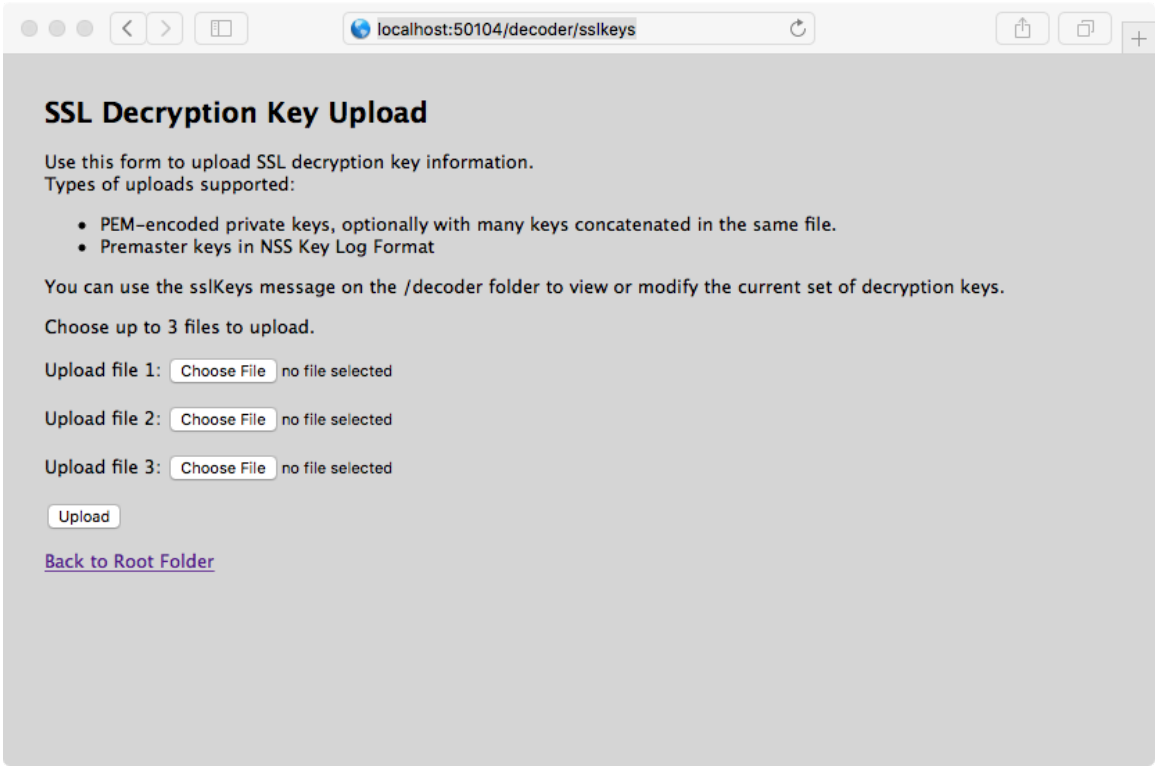
Ab NetWitness Suite 11.0 können Administratoren einen Packet Decoder so konfigurieren, dass eingehende Pakete mithilfe des Befehls `sslKeys` entschlüsselt werden können. Für die aktivierten Parser ist dann die unverschlüsselte Paketnutzlast sichtbar und die Metadaten können entsprechend erstellt werden. Wenn der Decoder nicht so konfiguriert ist, dass eingehende Pakete entschlüsselt werden, sind für die meisten aktivierten Parser nur verschlüsselte, unleserliche Daten sichtbar, und es können keine aussagekräftigen Metadaten erstellt werden.

Hinweis: Wenn FIPS aktiviert ist, können nur von FIPS zugelassene Verschlüsselungsverfahren verwendet werden.

Mit `sslKeys` können Pre-Master-Schlüssel oder private Schlüssel in den Decoder hochgeladen werden, sodass erfasste verschlüsselte Pakete, die mit diesen Schlüsseln übereinstimmen, vor dem Analysieren entschlüsselt werden können. Administratoren konfigurieren den Decoder durch Eingabe des Befehls `sslKeys` in der NwConsole-Befehlszeilenoberfläche oder in der RESTful-Schnittstelle des Decoders.



Das Formular der RESTful-Schnittstelle am Pfad: `/decoder/sslkeys` ermöglicht das Hochladen eines einzelnen PEM-kodierten privaten Schlüssels, einer einzelnen Datei mit mehreren, verketteten privaten Schlüsseln oder einer einzelnen Datei mit mehreren Pre-Master-Schlüsseln.



Die Pakete werden zwar in der Analysephase entschlüsselt, aber nur die verschlüsselten Pakete werden auf die Festplatte geschrieben. Der passende Pre-Master-Schlüssel für die Entschlüsselung wird in den Metaschlüssel `tls.premaster` geschrieben, den Analysten anschließend zum Anzeigen unverschlüsselter Pakete nach Bedarf nutzen können.

Weitere Informationen für Administratoren zum Konfigurieren der Entschlüsselung der eingehenden Pakete und für Analysten zum Anzeigen unverschlüsselter Pakete nach Bedarf werden unten genannt.

Überlegungen zur Performance

Das Entschlüsseln der Pakete in Echtzeit verursacht zusätzliche Last in der Analysephase. Planen Sie die Implementierung dieser Funktion sorgfältig, damit die eingehende Datenverkehrsbandbreite nicht über die verfügbare Rechenleistung hinausgeht. Möglicherweise benötigen Sie mehr Decoder zum Entschlüsseln von Datenverkehr, als Sie ohne die Entschlüsselung benötigen würden.

Auf einem Decoder erfasste Pakete haben in der Regel ein Timeout von ca. 60 Sekunden in der Zusammenstellungsphase, bevor sie an den Analyseschritt gesendet werden. Wenn beim Decoder der Arbeitsspeicher aufgrund der sehr hohen Bandbreite knapp wird, kann sich die Lebensdauer der Pakete im Assembler verkürzen. Um diese Situation zu vermeiden, können Sie einen längeren Timeoutwert konfigurieren und die Menge des Arbeitsspeichers erhöhen, der für die Pakete in der Zusammenstellungsphase zur Verfügung steht. Darüber hinaus muss der Decoder den Dechiffrierschlüssel vor der Analysephase erhalten, um die Entschlüsselung der Pakete durchführen zu können.

Hinweis: Derzeit können nur TLS-Protokolle der Version 1.2 und früher entschlüsselt werden.

Ohne geladene Feeds, mit folgenden aktivierten Parsern und bei einem Anteil von 50 % von zu entschlüsselnden Sitzungen, kann ein Decoder Datenverkehr mit 3 Gbit/s verarbeiten.

Name des Parsers	Beschreibung
SYSTEM	Details zu Sitzung
NETWORK	Netzwerkschicht
ALERTS	Warnmeldungen
GeoIP	Geografische Daten basierend auf ip.src und ip.dst
HTTP	Hyper Text Transport Protocol (HTTP)
HTTP_Lua	Hyper Text Transport Protocol (HTTP) Lua
FTP	File Transfer Protocol (FTP)
TELNET	TELNET-Protokoll
SMTP	Simple Mail Transport Protocol (SMTP)
POP3	Post Office Protocol (POP3)
NNTP	Network News Transport Protocol (NNTP)
DNS	Domain Name Service (DNS)
HTTPS	Secure Socket Layer (SSL) Protocol
MAIL	E-Mail-Standardformat (RFC822)
VCARD	Extrahiert den vollständigen Namen und E-Mail-Informationen für VCARD.
PGP	Identifiziert PGP-Blöcke innerhalb des Netzwerkverkehrs.
SMIME	Identifiziert SMIME-Blöcke innerhalb des Netzwerkverkehrs.
SSH	Secure Shell (SSH)

Name des Parsers	Beschreibung
TFTP	TFTP (Trivial File Transfer Protocol)
DHCP	Dynamic Host Configuration Protocol (DHCP und BOOTP)
NETBIOS	Extrahiert NETBIOS-Computernameninformationen.
SNMP	SNMP (Simple Network Management Protocol)
NFS	Network File System (NFS)-Protokoll
RIP	Routing Information Protocol (RIP)
TDS	MSSQL- und Sybase-Datenbankprotokoll (TDS)
TNS	Oracle-Datenbankprotokoll (TNS)
IRC	Internet Relay Chat (IRC)-Protokoll
RTP	Real Time Protocol (RTP) für Audio/Video
SIP	Session Initiation Protocol (SIP)
H323	H.323-Telekonferenzprotokoll
SCCP	Cisco Skinny Client Control Protocol
GTalk	Google Talk (GTalk)
VlanGre	VLAN-ID und GRE/EtherIP-Tunneladressen
BITTORRENT	BitTorrent-Dateifreigabeprotokoll
FIX	Financial Information eXchange Protocol
GNUTELLA	Gnutella-Dateifreigabeprotokoll
IMAP	Internet Message Access Protocol
MSRPC	Microsoft Remote Procedure Call-Protokoll
RDP	Remote Desktop Protocol
SHELL	Command Shell Identification

Name des Parsers	Beschreibung
TLSv1	TLSv1
SearchEngines	Ein Parser, der Suchbegriffe extrahiert.
FeedParser	Externer Feedparser

Chiffrierschlüssel

Mit dem Befehl `sslKeys` können zwei Arten von Chiffrierschlüsseln verwendet werden:

- Pre-Master-Schlüssel: der symmetrische Schlüssel, der im TLS-Nutzlaststream für die Verschlüsselung und Entschlüsselung verwendet wird.
- Privater Schlüssel: der asymmetrische private Schlüssel, der den Pre-Master während des TLS-Handshake verschlüsselt.

Pre-Master-Schlüssel

Der Pre-Master-Schlüssel wird per Zufallsprinzip generiert und gilt nur für die Lebensdauer einer bestimmten TLS-Sitzung. Es gibt in der Regel keine gute Möglichkeit, den Pre-Master-Schlüssel rechtzeitig für den Analyseschritt zu einem Decoder zu bringen. Jedoch können Chrome und Firefox die Pre-Master-Schlüssel, die sie generieren, in eine Datei schreiben. Dies ist nützlich für Testzwecke. Um Ihren Browser dafür zu konfigurieren, erstellen Sie eine Umgebungsvariable namens SSLKEYLOGFILE und weisen Sie ihr den Pfadnamen der Datei zu, in die die Schlüssel geschrieben werden sollen. Der Decoder akzeptiert die Datei und verwendet alle Dechiffrierschlüssel in der Datei für jeglichen verschlüsselten Datenverkehr, den er erfasst.

Dies ist ein Beispiel für ein NwConsole-Skript, mit dem die Datei in einen Decoder hochgeladen wird:

```
login <decoder>:50004 <username> <password>

send /decoder sslKeys --file-data=SSLKeys.txt
```

Dies ist ein Beispiel für einen curl-Befehl (mit dem RESTful-Port), mit dem die Datei in einen Decoder hochgeladen wird:

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-
stream" --data-binary @"/path/SSLKeys.txt" -X POST
"http://<hostname>:50104/decoder?msg=sslKeys"
```

Nachdem die symmetrischen Schlüssel hochgeladen wurden, werden sie sofort für alle erforderlichen Entschlüsselungsvorgänge verwendet. Symmetrische Schlüssel werden im Arbeitsspeicher gespeichert und es gibt eine Begrenzung, wie viele jeweils gleichzeitig gespeichert werden können. Wenn viele Schlüssel hinzugefügt werden, werden die jeweils ältesten Schlüssel gelöscht. Sie können auch Pre-Master-Schlüssel hinzufügen, indem Sie einfach die Parameter `random` und `premaster` an `sslKeys` übergeben.

Private Schlüssel oder PEM-Dateien

Private Schlüssel werden in der Regel in PEM-Dateien gespeichert und sind die asymmetrischen Schlüssel, die von den Diensten generiert werden, die TLS-Datenverkehr entgegennehmen. Diese Schlüssel werden während des TLS-Handshake verwendet, um den symmetrischen Pre-Master-Schlüssel zu verschlüsseln, der für den Rest der Nutzlastverschlüsselung verwendet wird.

Wenn Sie z. B. einen Webserver haben und dessen Datenverkehr prüfen möchten, müssen Sie den privaten Schlüssel hochladen, den er zum Verschlüsseln des Datenverkehrs verwendet. Sie müssen dies nur einmal durchführen, da er dauerhaft gespeichert wird (bzw. solange, bis er durch einen Löschbefehl entfernt wird). Private Schlüssel werden vor der Speicherung automatisch verschlüsselt, um sie zu schützen. Nach dem Upload müssen Sie einen Befehl zum Neuladen des Parsers ausgeben, damit der neu installierte Schlüssel für den HTTPS-Parser sichtbar wird. Jetzt können alle TLS-Handshakes, die den privaten Schlüssel verwenden, vom Decoder entschlüsselt werden.

Hinweis: Nicht alle Verschlüsselungssuites verwenden „bekannte“ private Schlüssel (z. B. den kurzlebigen Diffie Hellman). Mit solchen Verschlüsselungsverfahren verschlüsselter Datenverkehr kann nur entschlüsselt werden, wenn der Pre-Master-Schlüssel auf den Decoder hochgeladen wurde, bevor die Sitzung analysiert wird.

Im Folgenden sind Beispielbefehle aufgeführt, mit denen eine PEM-Datei für die Entschlüsselung hochgeladen wird.

Mit NwConsole:

```
send /decoder sslKeys pemFilename=MyKey.pem --file-data=/path/MyKey.pem
```

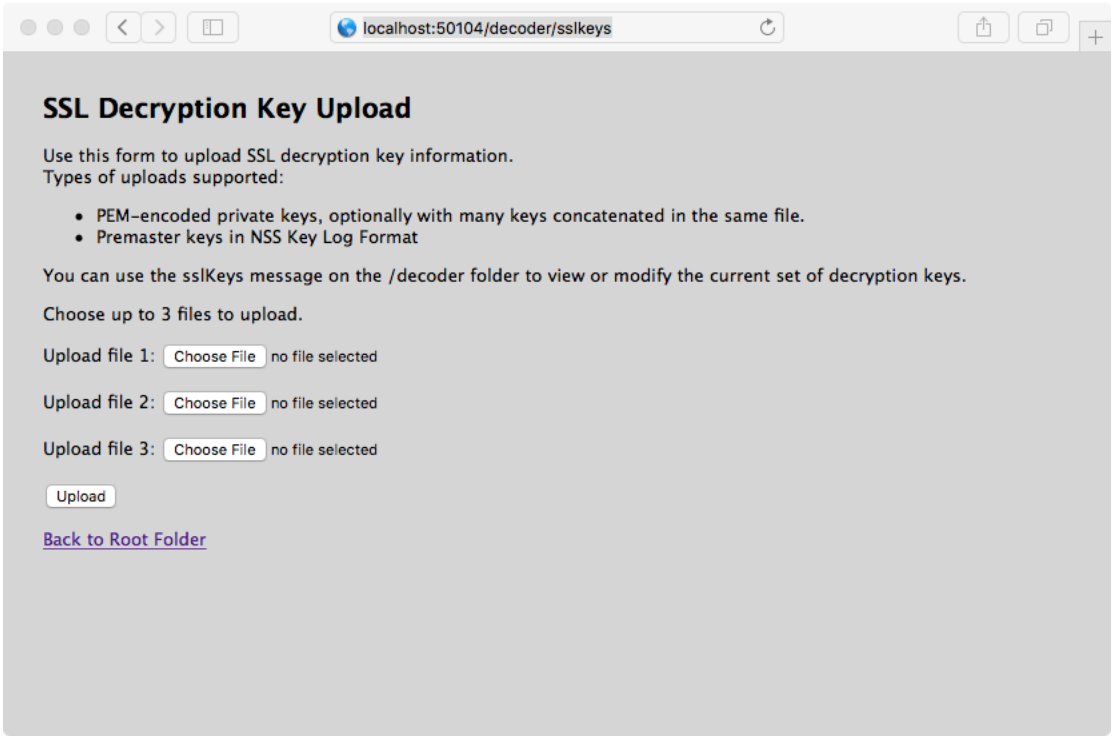
Über die RESTful-Schnittstelle (der Parameter `pemFilename` muss in der URL enthalten sein):

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-
stream" --data-binary @"/path/MyKey.pem" -X POST
"http://<hostname>:50104/decoder?msg=sslKeys&pemFilename=MyKey.pem"
```

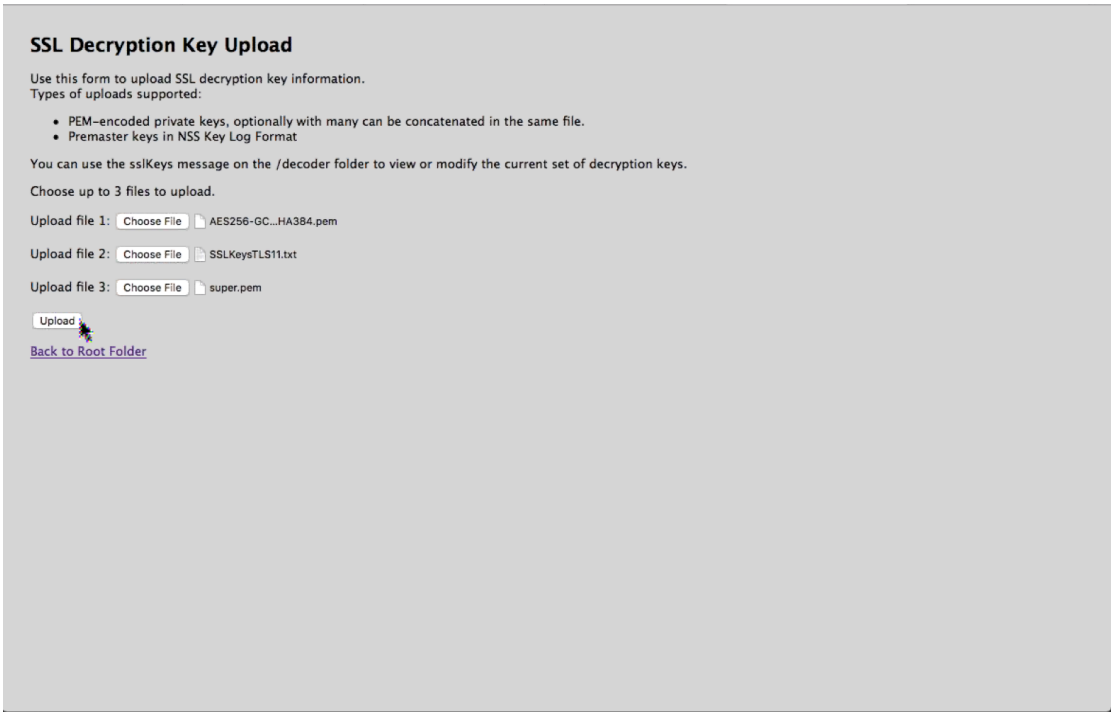
Hochladen mehrerer Pre-Master- und privater Schlüssel

Über das Formular der RESTful-Schnittstelle können Sie mehrere Schlüssel, Pre-Master und privat, gleichzeitig hochladen.

1. Öffnen Sie die RESTful-API in Ihrem Browser und navigieren Sie zu diesem Pfad im Decoder, den Sie konfigurieren möchten: `/decoder/sslkeys`.

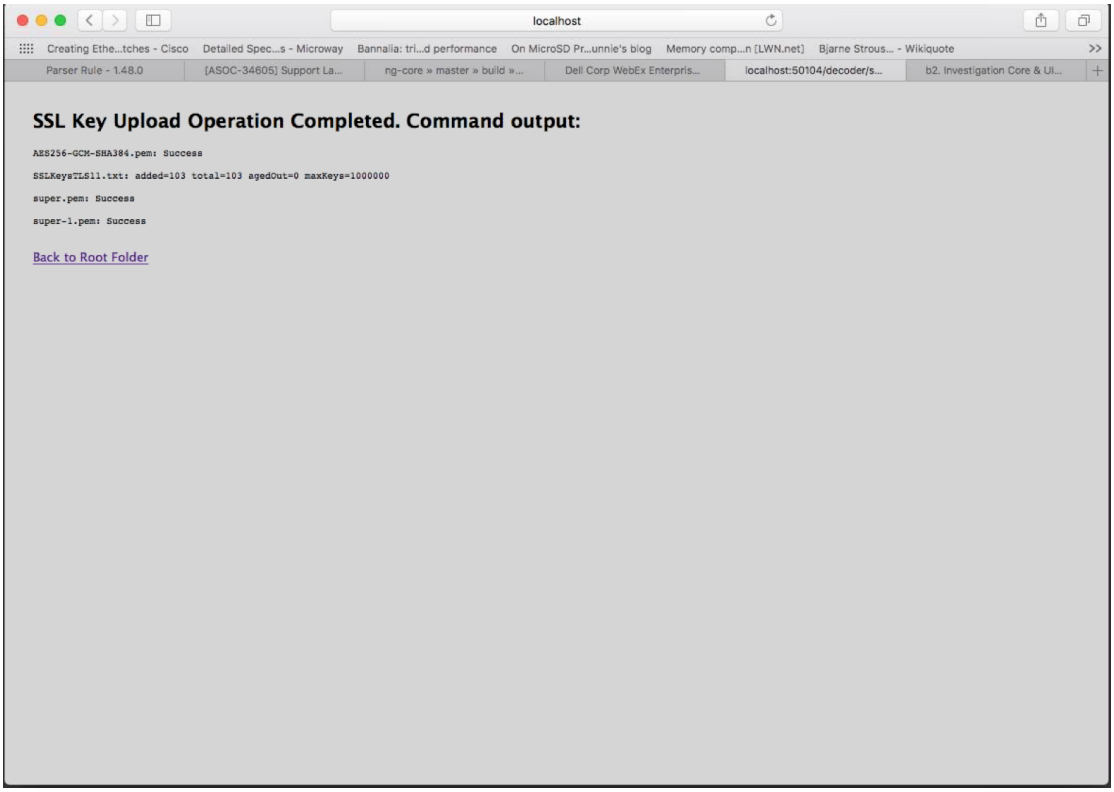


2. Klicken Sie neben **Datei 1 hochladen** auf **Datei auswählen** und suchen Sie die Pre-Master-Schlüsseldatei oder PEM-Datei, die Sie in das lokale Dateisystem hochladen möchten.
3. (Optional) Wiederholen Sie dies für **Datei 2 hochladen** und **Datei 3 hochladen**.



4. Klicken Sie auf **Hochladen**.
   Die Dateien werden in den Decoder hochgeladen und die Ergebnisse werden im Formular

angezeigt.



Parameter für das Verwalten von Schlüsseln

Der Befehl `sslKeys` hat verschiedene Parameter für das Verwalten von Pre-Master- und privaten Schlüsseln. Dies ist die vollständige Liste der Parameter:

Parameter	Beschreibung
`clear`	Entfernt alle Pre-Master-Schlüssel aus dem Arbeitsspeicher. Löscht keine PEM-Dateien, die im System installiert sind.
`maxKeys`	Ändert die maximale Anzahl der Pre-Master-Schlüssel, die im Arbeitsspeicher gespeichert sind.
`listPems`	Gibt eine Liste aller installierten PEM-Dateien mit privaten Schlüsseln zurück.

Parameter	Beschreibung
`deletePem`	Löscht die benannte PEM-Datei aus dem Dateisystem. Sie können diesen Parameter mehr als einmal übergeben, um mehrere Dateien zu entfernen.
`random`	Der zufällige Hash-Wert zum Identifizieren des Pre-Master-Schlüssels.
`premaster`	Der Pre-Master-Schlüssel, der für den vorherigen Parameter `random` installiert wird. Sie müssen paarweise auftreten und `random` muss der erste sein.

Rückgabewerte

Die meisten `sslKeys`-Befehle geben statistische Name/Wert-Paare zu den Pre-Master-Schlüsseln im Arbeitsspeicher zurück. Die zurückgegebenen Statistiken sind in der folgenden Tabelle aufgeführt.

Name	Beschreibung
`added`	Die Anzahl der gerade während dieses Befehls hinzugefügten Pre-Master-Schlüssel.
`total`	Die Gesamtzahl der im Arbeitsspeicher geladenen Pre-Master-Schlüssel.
`agedOut`	Die Gesamtzahl der Pre-Master-Schlüssel, die während dieses Befehls entfernt wurden; dies ist keine Lebensdauerstatistik.
`maxKeys`	Die aktuelle maximal zulässige Anzahl an Pre-Master-Schlüsseln.

Anzeigen von unverschlüsseltem Datenverkehr

Wenn Pakete während der Analysephase entschlüsselt werden, werden die verschlüsselten Pakete auf die Festplatte geschrieben und der passende Pre-Master-Schlüssel für die Entschlüsselung wird in den Metaschlüssel `tls.premaster` geschrieben. Analysten können die unverschlüsselten Pakete dann mit dem Metaschlüssel `tls.premaster` anzeigen.

Eine Decoder-API, mit der Sie unverschlüsselte Pakete anzeigen können, ist der RESTful-Service /sdk/content. Sie müssen die Sitzungs-ID der verschlüsselten Pakete und den Parameter `flags`, der auf den Wert 128 (oder 0x80 im Hexidezimalformat) maskiert ist, kennen. Gehen Sie in Ihrem Browser zur RESTful-Schnittstelle des Decoders und geben Sie folgenden Befehl ein, wobei Sie die tatsächliche Sitzungs-ID statt <id> verwenden:

```
http://<decoder>:50104/sdk/content&session=<id>&flags=128&render=text
```

Der Decoder gibt eine einfache Webseite zurück und zeigt die Pakete an, nachdem sie entschlüsselt wurden.

Wenn Sie wissen möchten, wie die Pakete verschlüsselt aussehen, geben Sie einen der folgenden Befehle ein, wobei Sie statt <id> die Sitzungs-ID verwenden:

```
http://<decoder>:50104/sdk/content&session=<id>&render=text
```

```
http://<decoder>:50104/sdk/content&session=<id>&flags&render=text
```

Weitere Informationen zum Service /sdk/content service finden Sie auf der Anleitungsseite für /sdk content.

Bearbeiten der Decoder-Systemkonfiguration

Wenn ein Service zum ersten Mal zu NetWitness Suite hinzugefügt wird, sind Standardwerte für die Systemkonfigurationsparameter wirksam. In den meisten Fällen sind die Standardwerte für Komprimierung, Statistikaktualisierungsintervall und Anzahl der Threads im Threadpool auf einen geeigneten Wert für eine optimale Systemperformance festgelegt. Sie müssen diese Einstellungen nicht bearbeiten, es sei denn, ein Techniker des RSA Customer Service empfiehlt Ihnen, sie zu ändern.

System Configuration

Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	☐
SSL Port	56004
Stat Update Interval	1000
Threads	20

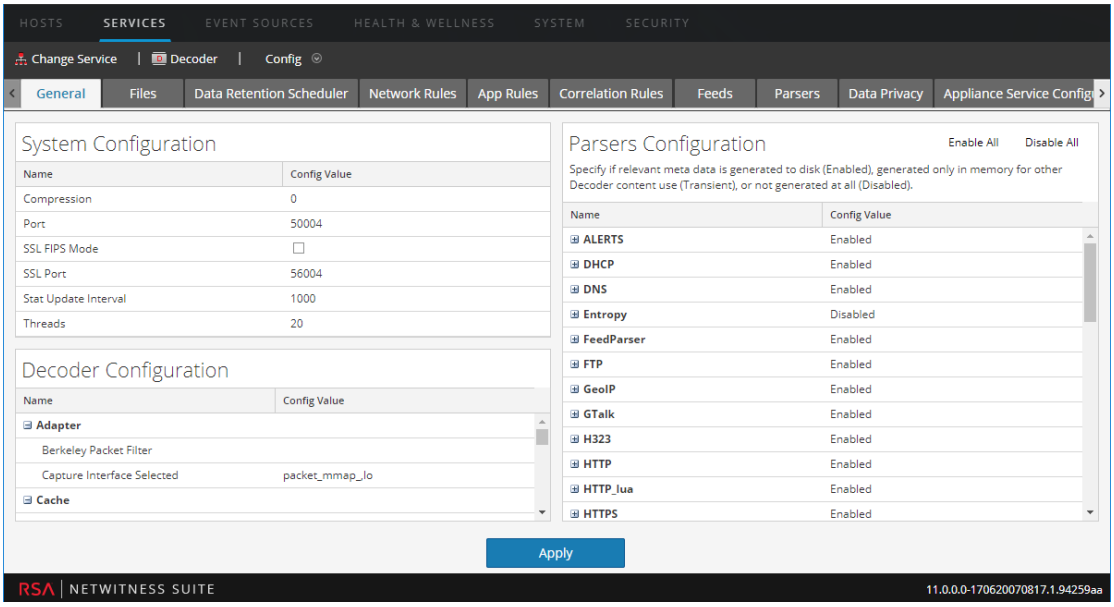
Ein Parameter, den Sie für Ihre Umgebung ändern sollten, ist die SSL-Einstellung, die standardmäßig nicht aktiviert ist. Sofern aktiviert, wird die Sicherheit der Datenübertragung durch Verschlüsselung der Informationen und Authentifizierung mit SSL-Zertifikaten organisiert.

So bearbeiten Sie Systemkonfigurationsparameter für einen Decoder oder Log Decoder:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Administration > Services“ einen Decoder- oder Log Decoder-Service und wählen Sie  **> Ansicht > Konfigurieren** aus.

   Die Ansicht „Service-Konfiguration“ für den Service wird mit geöffneter Registerkarte

„Allgemein“ angezeigt.



3. Klicken Sie unter **Systemkonfiguration** in ein zu bearbeitendes Feld **(Komprimierung**, **Port**, **SSL FIPS-Modus**, **SSL-Port**, **Statistikaktualisierungsintervalle** oder **Threads**). Geben Sie einen neuen Wert ein.
4. Klicken Sie nach dem Bearbeiten auf **Anwenden** .Die Einstellungen werden sofort wirksam.

Aktivieren von CPU-Auslastungsstatistiken für installierte Inhalte

Ab NetWitness Suite 11.0 bietet der Decoder CPU-Auslastungsstatistiken für alle installierten Inhalte, die Sie verwenden können, um zu prüfen, wie viel CPU-Zeit von Parsern, Feeds, Anwendungsregeln und lexikalischen Überprüfungen belegt wird. Die Statistiken werden als Stat-Nodes in der Servicestruktur der Ansicht „Explorer“ angezeigt, wenn **/decoder/parsers/config/detailed.stats** aktiviert ist und der Decoder Statistiken erfasst.

Jedes Inhaltselement wird als einzelner Prozentwert (0-100) berücksichtigt, unabhängig von der Anzahl der ausgeführten Parse-Threads. Der Prozentsatz spiegelt die durchschnittliche CPU-Auslastung für den Inhalt über alle Threads hinweg wider.

So aktivieren Sie die Auslastungsstatistiken:

1. Navigieren Sie zur Explorer-Ansicht des Decoders und wählen Sie den Parameter `/decoder/parsers/config/detailed.stats` aus.
2. Ändern Sie den Wert in **Aktiviert**. Wenn der Decoder keine Daten erfasst, starten Sie die Erfassung.
   Wenn Sie den Stat-Node des Decoders in der Ansicht „Explorer“ öffnen, wird die neue Statistik angezeigt.

Parser-Zuordnungen aktivieren

In diesem Thema erfahren Administratoren, wie sie die Ereignisquellenzuordnung auf einem Log Decoder aktivieren.

Der Log Collector erkennt den Ereignisquelltyp auf Meldungsbasis. Wenn für die Ereignisquelle nicht der richtige Parser erkannt wird, kann ein geringer Prozentsatz der Protokolle falsch klassifiziert werden. Die falsch klassifizierten Nachrichten füllen Ereignisquellregeln und Warnmeldungen nicht auf und die Berichte enthalten nicht die richtigen Daten. Wenn mehrere Ereignisquelltypen mit einer IP-Adresse verknüpft sind, können die Parser möglicherweise nur schwer identifizieren, aus welcher Ereignisquelle die Protokolle erzeugt werden.

Wenn Sie eine IP-Adresse zu ihrem Ereignisquelltyp zuordnen, kann der Log Decoder die Ereignisquelle ermitteln, aus der das Protokoll erzeugt wird. Wenn Nachrichten aus einer zugeordneten Ereignisquelle für den Log Decoder bereitgestellt werden, werden nur die zugewiesenen Parser abgefragt, um Ereignisentsprechungen zu finden.

Sie können Ereignisquelltypen zu IPv4-, IPv6- oder Hostnamenwerten der Ereignisquelle zuweisen. Sie können auch mehrere Ereignisquellentypen zu einer einzigen IP-Adresse zuweisen. Sie können auch die Log Collector-ID verwenden, wenn verschiedene Ereignisquelltypen mit derselben IP-Adresse an verschiedene Log Collectors gesendet werden.

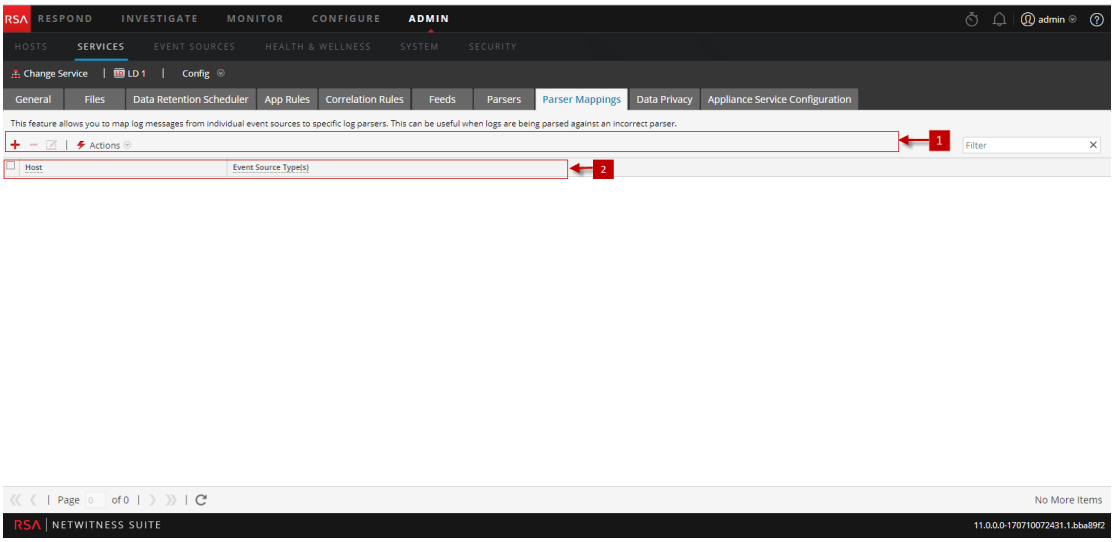
Hinweis: Sie können auch Parser-Zuordnungsfunktionen aktivieren, indem Sie zu **ADMIN > Ereignisquellen > Erkennung** navigieren.

Aktivieren der Zuordnung der IP-Adresse zur Ereignisquelle

So aktivieren Sie die Zuordnung der IP-Adresse zur Ereignisquelle:

1. Navigieren Sie zu **ADMIN > System > Protokoll-Parser-Zuordnungen**.
2. Wählen Sie **Decoder** und  **> Ansicht > Konfiguration** aus.
3. Wählen Sie auf der Seite „Konfiguration“ die Registerkarte **Parser-Zuordnungen**.
   In der Ansicht „Services-Konfiguration“ wird die Registerkarte „Parser-Zuordnungen“

angezeigt.

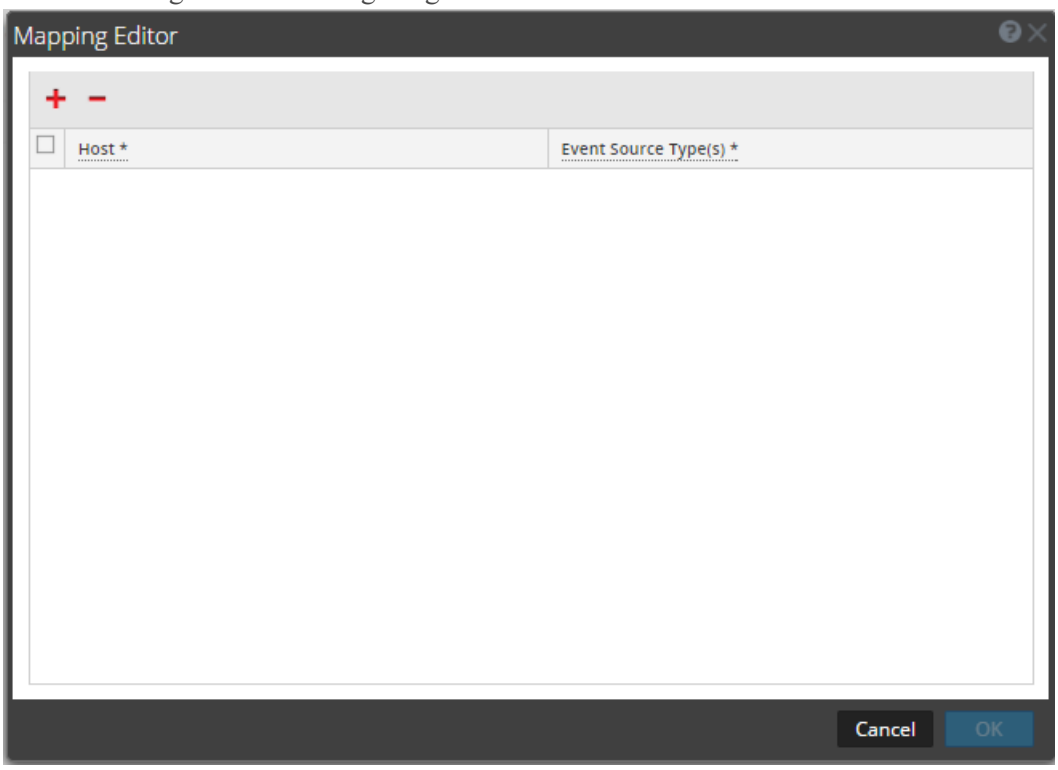


Aktualisieren der Zuordnung der IP-Adresse zur Ereignisquelle

So aktualisieren Sie die Zuordnung der IP-Adresse zur Ereignisquelle:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen **Log Decoder** und in der Spalte **Aktionen** die Optionen > **Ansicht** > **Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnung** aus.
4. Klicken Sie auf + .

Der Zuordnungseditor wird angezeigt.



5. Eine der folgenden Zuordnungen kann definiert werden:

Ein Host und ein Ereignisquellentyp
: Geben Sie im Feld **Host** den Hostnamen ein.
Beispiel:`10.0.0.1`
- Geben Sie in das Feld **Ereignisquelle(n)** den Ereignisquellentyp ein.
Beispiel:`apache`

Ein Host und ein oder mehrere Ereignisquellentypen
: Geben Sie im Feld **Host** den Hostnamen ein.
Beispiel: `10.0.0.1`
- Geben Sie in das Feld **Ereignisquelle(n)** den Ereignisquellentyp ein.
Beispiel: `apache,sap,aix`

Ein Host, ein Log Collector und ein Ereignisquellentyp
: - Geben Sie im Feld **Host** den Hostnamen und die Log Collector-ID ein.
Beispiel: `10.0.0.1,LC-1`.
- Geben Sie in das Feld **Ereignisquelle(n)** den Ereignisquellentyp ein.
Beispiel: `apache`

Ein Host, eine Log Collector-ID und ein oder mehrere Ereignisquellentypen
- Geben Sie im Feld **Host** den Hostnamen und die Log Collector-ID ein.
Beispiel: `10.0.0.1,LC-1`
- Geben Sie im Feld **Ereignisquelle(n)** den Ereignisquellentyp ein.
Beispiel: `apache,sap,aix`

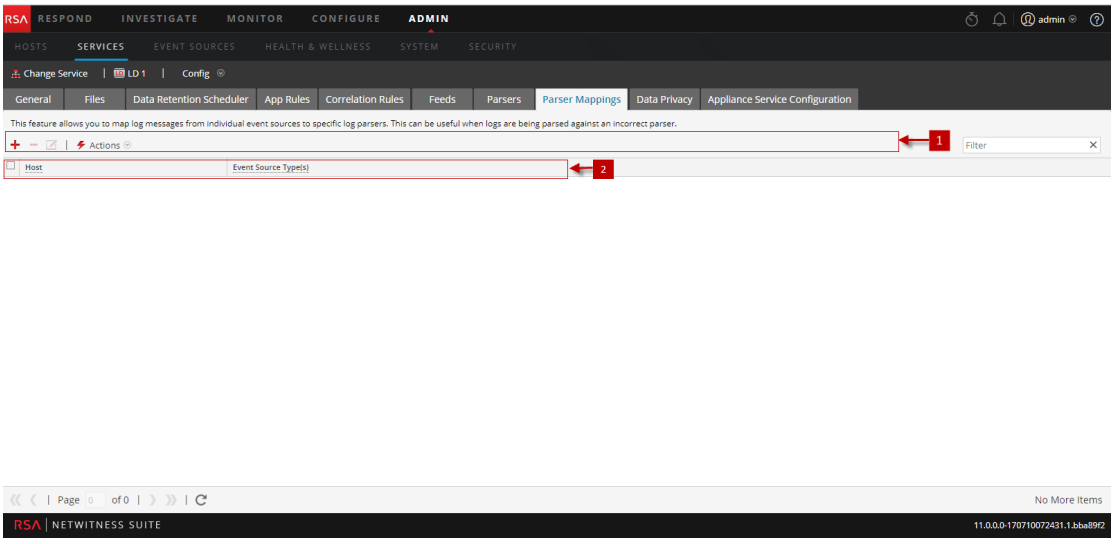
Hinweis: Die Ereignisquellentyp werden in der Reihenfolge verarbeitet, in der Sie die Parser eingeben, und wenn ein oder mehrere Parser einem Protokoll entsprechen, wird der erste Parser in der Liste abgefragt. „Host/IP“ kann eine IPv4-Adresse, eine IPv6-Adresse oder ein Hostname sein.

6. Klicken Sie auf **OK**.
   Die Parser-Zuordnung wird hinzugefügt.
7. Um die Auswahl der Parser-Zuordnungen abzubrechen, klicken Sie auf **Abbrechen**.

Lesen der Zuordnungen der IP-Adresse zum Ereignisquelltyp

So lesen Sie die Zuordnungen der IP-Adresse zum Ereignisquelltyp:

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Log Decoder-Service aus.
2. Wählen Sie in der Spalte Aktionen die Optionen > **Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.
   Die Zuordnungen werden angezeigt.



Bearbeiten einer Zuordnung der IP-Adresse zum Ereignisquelltyp

So bearbeiten Sie eine Zuordnung der IP-Adresse zum Ereignisquelltyp

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Log Decoder-Service aus.
2. Wählen Sie in der Spalte „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.

3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.
4. Wählen Sie die Zuordnung aus, die Sie bearbeiten möchten.
   Hinweis: Sie können jeweils immer nur eine Zuordnung bearbeiten.
5. Klicken Sie auf  .
6. Ändern Sie im Feld **Ereignisquelle(n)** die Ereignisquelle(n).
   Hinweis: Der Host kann nicht bearbeitet werden und das Feld ist deaktiviert.
7. Klicken Sie auf **OK**, um die bearbeitete Ereignisquelle zu übernehmen.
8. Um die Änderungen zu widerrufen, klicken Sie auf **Abbrechen**.

Löschen einer Zuordnung der IP-Adresse zum Ereignisquelltyp

So löschen Sie eine Zuordnung der IP-Adresse zum Ereignisquelltyp

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Log Decoder-Service aus.
2. Wählen Sie in der Spalte „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.
4. Wählen Sie die Zuordnung aus, die Sie löschen möchten.
5. Klicken Sie auf .
   Die Zuordnung wird gelöscht und das Raster wird aktualisiert.
6. Um die Änderungen zu widerrufen, klicken Sie auf **Abbrechen**.

Sortieren des Hostnamens oder Ereignisquelltyps

So sortieren Sie den Hostnamen oder Ereignisquelltyp:

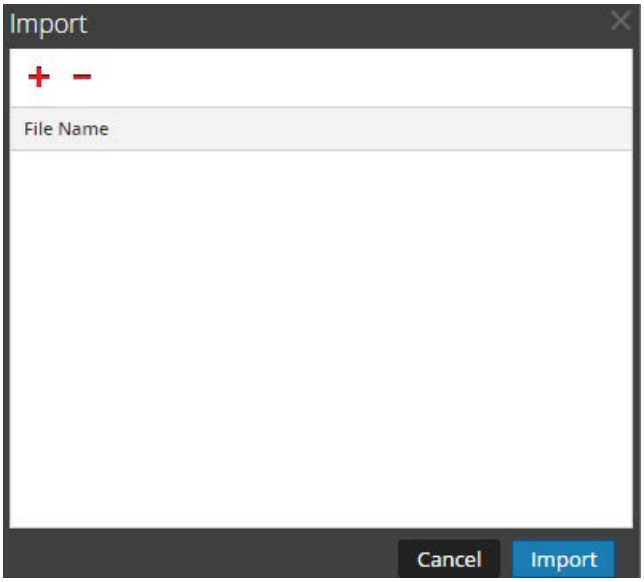
1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Log Decoder-Service aus.
2. Wählen Sie in der Spalte „Aktionen“ die Optionen  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.

4. Klicken Sie zum Sortieren einer Spalte in der Kopfzeile der Spalte auf .Die Quellereignistypen werden auf die ausgewählte IP-Adresse angewendet. Die Protokolle werden in der Reihenfolge analysiert, in der sie aufgeführt sind.

Importieren von Einträgen für die Zuordnung der IP-Adresse zur Ereignisquelle

So importieren Sie Einträge für die Zuordnung der IP-Adresse zur Ereignisquelle

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Log Decoder-Service aus.
2. Wählen Sie in der Spalte „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus. Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.
4. Wählen Sie **Aktionen > Importieren** aus.
   Das Dialogfeld „Importieren“ wird angezeigt.



5. Klicken Sie auf .
6. Wählen Sie die Datei aus, die Sie importieren möchten, und klicken Sie auf **OK**.
7. Klicken Sie zum Laden des Parsers auf **Importieren**.

Hinweis: Sie können jeweils nur eine CSV-Datei importieren.

Exportieren von Einträgen für die Zuordnung der IP-Adresse zur Ereignisquelle

So exportieren Sie Einträge für die Zuordnung der IP-Adresse zur Ereignisquelle

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Log Decoder-Service aus.
2. Wählen Sie in der Spalte „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.
4. Wählen Sie die Zuordnungen aus, die Sie exportieren möchten.
5. Wählen Sie **Aktionen > Exportieren > Auswahl** aus.
   Das Dialogfeld „Exportauswahl“ wird angezeigt.

6. Geben Sie den Dateinamen ein und klicken Sie auf **Exportieren**.

Suchen nach Einträgen für die Zuordnung der IP-Adresse zur Ereignisquelle

So suchen Sie nach Einträgen für die Zuordnung der IP-Adresse zur Ereignisquelle

1. Wechseln Sie zu **Administration > Services** und wählen Sie einen Log Decoder-Service aus.
2. Wählen Sie in der Spalte „Aktionen“ die Optionen > **Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.
4. Geben Sie in der Symbolleiste Parser Zuordnungen den Host oder eine Ereignisquelle in das Feld **Filter** ein.
5. Klicken Sie auf **Eingabe**.
   Die Hosts oder Ereignisquellen, die den eingegebenen Namen entsprechen, werden im Feld **Filter** angezeigt.

Aktivieren oder Deaktivieren der Lua- und Flex-Parsersysteme

In diesem Thema erfahren Administratoren, wie sie Lua- und Flex-Parsingsysteme auf einem Decoder oder Log Decoder aktivieren oder deaktivieren. Flex-Parser sind veraltet und standardmäßig deaktiviert.

Die Einstellungen zum Aktivieren oder Deaktivieren von Lua- und Flex-Parsersystemen sind standardmäßig korrekt konfiguriert und müssen in der Regel nicht geändert werden. Allerdings müssen Sie diese Einstellungen möglicherweise auf Anfrage der RSA-Kundenbetreuung oder aus Troubleshooting-Gründen anpassen.

Neben dem Konfigurieren einzelner Parser können Sie alle LUA- sowie alle Flex-Parser in der Ansicht „Services > Durchsuchen“ aktivieren und deaktivieren. Sie aktivieren und deaktivieren Einstellungen der Lua- und Flex-Parsersysteme zwar separat, sie funktionieren jedoch auf dieselbe Weise.

- Wenn Sie das Lua-/Flex-Parsersystem **deaktivieren**, wird das entsprechende Parsersystem deaktiviert und es werden keine Parser geladen.
- Wenn Sie das Lua-/Flex-Parsersystem **aktivieren**, wird das entsprechende Parsersystem aktiviert und einzelne Parser werden gemäß der aktuellen individuellen Konfigurationen aktiviert und deaktiviert.

So aktivieren oder deaktivieren Sie Lua- und Flex-Parsersysteme auf einem Decoder oder Log Decoder:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie einen Decoder oder Log Decoder und > **Ansicht > Durchsuchen** aus.
   Die Ansicht „Services-Konfiguration“ für den ausgewählten Service wird angezeigt.
3. Navigieren Sie in der Liste „Node“ zu **/decoder/parsers/config** und wählen Sie diese Option aus.
4. Gehen Sie im Überwachungsbereich wie folgt vor:
   - Um das Lua-Parsersystem zu aktivieren, geben Sie im Wertefeld für `lua.enabled` den Wert **yes** ein.
   - Um das Lua-Parsersystem zu deaktivieren, geben Sie im Wertefeld für `lua.enabled` den Wert **no** ein.
   - Um das Flex-Parsersystem zu aktivieren, geben Sie im Wertefeld für `flex.enabled` den Wert **yes** ein.

- Um das Flex-Parsersystem zu deaktivieren, geben Sie im Wertefeld für `flex.enabled` den Wert **no** ein.

Zuordnen von IP-Adressen zu einem Servicetyp für die Protokollanalyse

In diesem Thema wird das Verfahren zur Zuordnung einer IP-Adresse zu einem Servicetyp für die Protokollanalyse beschrieben.

Der Log Collector erkennt den Ereignisquellentyp auf Meldungsbasis. Wenn für die spezifische Ereignisquelle nicht der richtige Parser verwendet wird, werden die Meldungen, die mehreren Ereignisquelltypen gemeinsam sind, falsch klassifiziert. Die falsch identifizierten Meldungen werden nicht richtig in Serviceregeln und Warnmeldungen eingetragen und die Berichte enthalten nicht die richtigen Informationen. Außerdem können, wenn mehrere Services mit einer IP-Adresse verknüpft sind, die Parser möglicherweise nur schwer identifizieren, aus welchem Service genau das Protokoll erzeugt wird.

Wenn Sie eine IP-Adresse ihren Services zuordnen, kann der Log Decoder den Service identifizieren, aus dem das Protokoll erzeugt wird. Wenn Meldungen aus einem zugeordneten Service in das Protokoll kommen, werden die zugewiesenen Parser geladen, um Ereignisentsprechungen zu finden.

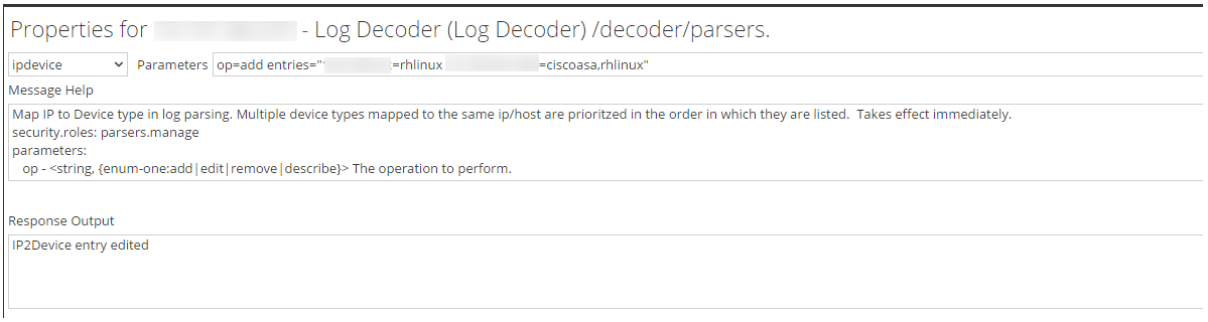
Sie können Servicetypen zu IPv4-, IPv6- oder Hostnamenwerten der Ereignisquelle zuweisen. Sie können auch mehrere Servicetypen zu einer einzelnen IP-Adresse zuweisen. Sie können außerdem die CollectorID verwenden, wenn verschiedene Servicetypen mit derselben IP-Adresse an verschiedene Collectors gesendet werden.

Zuordnen von IP-Adressen zu einem Servicetyp

Zur Zuordnung einer IP-Adresse zu einem Servicetyp führen Sie folgende Schritte aus:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht **Services** einen Log Decoder aus und wählen Sie in der Spalte **Aktionen** > **Ansicht > Durchsuchen**.
3. Wechseln Sie zum Node **/decoder/parsers**, klicken Sie mit der rechten Maustaste auf **parsers** und wählen Sie **Eigenschaften** aus.
4. Geben Sie in der Ansicht **Eigenschaften** den Befehl **ipdevice** mit den folgenden Parametern an:
   `op=add/remove entries="ipaddress=service"` (z. B. `op=add entries="10.100.201.300=ciscoasa"`)

5. Klicken Sie auf **Senden**.



Befehl „IPdevice“

Beim Befehl `ipdevice` sind drei Vorgänge möglich:

- `add`: Hiermit werden die Einträge in der ipdevice-Zuordnung hinzugefügt oder aktualisiert. Mehrere durch Leerzeichen getrennte Adress-/Typ-Paare können angegeben werden.
  `op=add entries="<address>=<service type>"`
- `remove`: Hiermit werden Einträge aus der ipdevice-Zuordnung entfernt. Mehrere durch Leerzeichen getrennte Adress-/Typ-Paare können angegeben werden.
  `op=remove entries="<address>"`
- `describe`: Hiermit werden die Werte zurückgegeben, die derzeit in der ipdevice-Zuordnung enthalten sind.

Zuordnen einer IP-Adresse zu einer Zeitzone

Oft enthalten Protokolle keine vollständigen Zeitstempel und keine Zeitzoneninformationen. Um solche Zeitstempel korrekt in UTC anzeigen zu lassen, bietet der Log Decoder die Möglichkeit, Geräte mit einer bestimmten Adresse (IPv4 oder IPv6) oder einem bestimmten Hostnamen einer festen Zeitzone oder Zeitverschiebung zuzuordnen.

Drei Zeitzonenformate werden derzeit akzeptiert und werden in den folgenden Beispielen gezeigt:

- Olson-Format: America/Anguilla
- POSIX-Format: AST2:45ADT0:45,M4.1.6/1:45,M10.5.6/2:45
- Format für die Zeitverschiebung in Stunden: = -500

NetWitness Suite ordnet die Geräteadresse (IPv4 oder IPv6) oder den Hostnamen einer spezifischen Zeitzone oder Zeitverschiebung zu. Ereigniszeit-Metadaten, die aus einem Protokoll analysiert werden, das von einer zugeordneten Adresse stammt und keine Verschiebung oder Zeitzone als Teil der Zeitstempels beinhaltet, werden entsprechend der Zuordnung in UTC umgewandelt.

Zur Zuordnung einer IP-Adresse zu einer Zeitzone führen Sie folgende Schritte aus:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht **Services** einen Log Decoder aus und wählen Sie in der Spalte **Aktionen** > **Ansicht > Durchsuchen** aus.
3. Wechseln Sie zum Node **/decoder/parsers**, klicken Sie mit der rechten Maustaste auf **Parsers** und wählen Sie **Eigenschaften** aus.
4. Geben Sie in der Ansicht **Eigenschaften** den Befehl `iptmzone` mit folgenden Parametern an:
   `op=add entries="IP-Adresse=Zeitzone" (z. B. op=add entries="10.10.10.10=Africa/Addis Ababa")`
5. Klicken Sie auf **Senden**.

Befehl „iptmzone“

Beim Befehl `iptmzone` sind drei Vorgänge möglich:

- `add`: Hiermit werden Einträge in der iptmzone-Zuordnung hinzugefügt oder aktualisiert. Mehrere durch Leerzeichen getrennte Adress-/Typ-Paare können angegeben werden.
  `op=add entries="<Adresse>=<Zeitzone>"`
- `remove`: Hiermit werden Einträge aus der iptmzone-Zuordnung entfernt. Mehrere durch Leerzeichen getrennte Adress-/Typ-Paare können angegeben werden.
  `op=remove entries="<Adresse>“`
- `describe`: Hiermit werden die Werte zurückgegeben, die derzeit in der iptmzone-Zuordnung enthalten sind.

Beispiele

Im Folgenden werden Beispiele für die Zuordnung von IP-Adressen zu Zeitzonen genannt:

- Wenn Sie zwei verschiedene Einträge mit unterschiedlichen IPV4-Werten und Zeitzonen zuordnen möchten, verwenden Sie folgenden Parameter im Befehl **iptmzone** und klicken Sie auf **Senden**
  `"op=add entries=”10.10.10.10=America/Anguilla 10.10.10.11=Pacific/Rarotonga"`
- Wenn Sie einen Eintrag für einen IPv4-Wert und eine Zeitzone entfernen möchten, verwenden Sie folgenden Parameter im Befehl **iptmzone** und klicken Sie auf **Senden**.

`"op=remove entries=10.5.245.9"`

- Wenn Sie einen Eintrag für einen IPv6-Wert und eine Zeitzone erstellen möchten, verwenden Sie folgenden Parameter im Befehl **iptmzone** und klicken Sie auf **Senden**.

```
op=add entries="2001:DB8:85A3::8A2E:370:7334=America/Anguilla"
```

- Wenn Sie einen Eintrag für die Zuordnung zwischen einer IPv4-Adresse, IPv6-Adresse oder einem Hostnamen und dem Zeitverschiebungsformat, Olson-Format oder POSIX-Format erstellen möchten, verwenden Sie den folgenden Parameter im Befehl **iptmzone** und klicken Sie auf **Senden**.

```
 op=add entries="10.168.0.2=America/Anguilla
2001:DB8:85A3::8A2E:370:7334=0500nwappliance21=EST5EDT,M3.2.0/2
,M11.1.0"
```

Abrufen von Protokolldateien von Log Decoder-Versionen vor 11.0

In NetWitness 11.0. besteht nun die Möglichkeit, eine kleine Auswahl der letzten Protokolle für bestimmte Geräte auf den jeweiligen Detail-Registerkarten der Ansicht „Erkennung“ anzuzeigen. Standardmäßig besitzen Log Decoder vor Version 11.0 nicht die erforderliche Konfiguration zum Aktivieren dieser Funktion. Dies ist jedoch durch Vornehmen einiger geringfügiger Änderungen möglich.

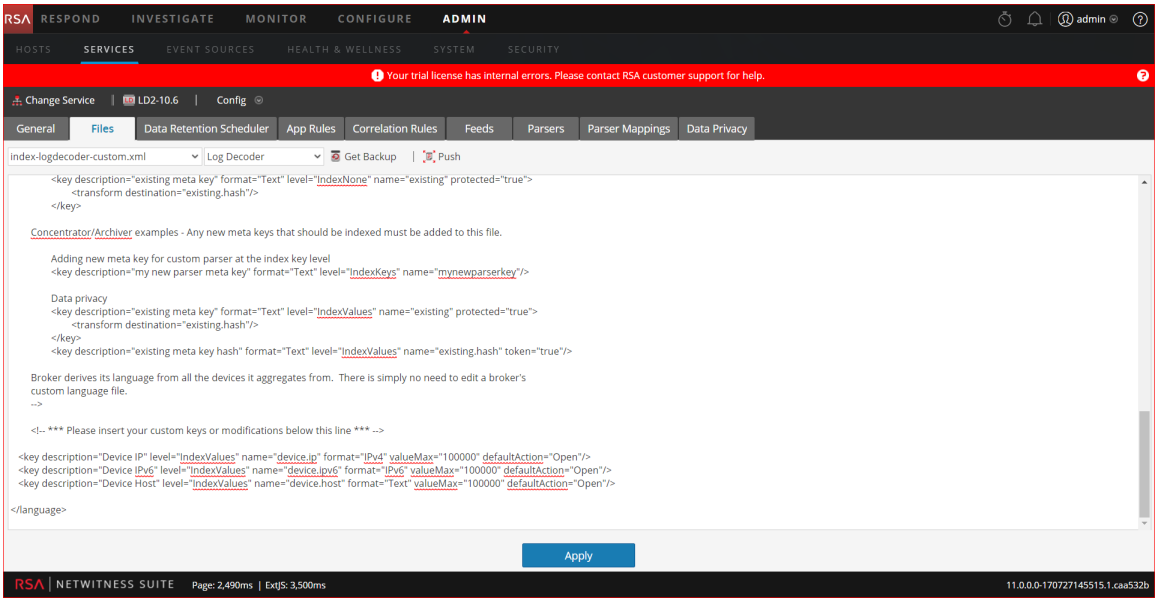
Um die Protokollvorschau für eine Log Decoder-Version vor 11.0 zu aktivieren, führen Sie auf dem Log Decoder die folgenden Schritte aus:

1. Gehen Sie zu **ADMIN > Services >**, wählen Sie einen **Log Decoder** aus und wählen Sie dann  **> Ansicht > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Dateien** und wählen Sie aus dem Drop-down-Menü **index-logdecoder-custom.xml** aus.
3. Fügen Sie die folgenden drei Zeilen am Ende der Datei ein (vor dem schließenden language-Tag):

```
<key description="Device IP" level="IndexValues" name="device.ip" format="IPv4"
valueMax="100000" defaultAction="Open"/>
<key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
valueMax="100000" defaultAction="Open"/>
<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```

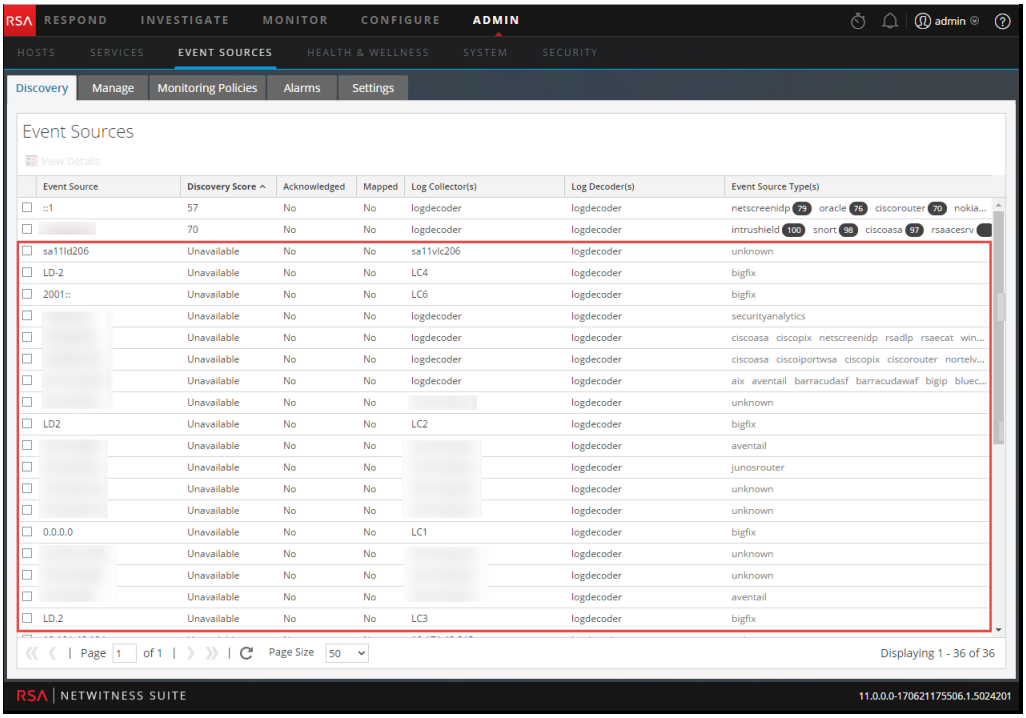
4. Klicken Sie auf **Anwenden**.
5. Starten Sie den Log Decoder folgendermaßen neu.
   Wählen Sie den Log Decoder-Service **> Durchsuchen > Decoder > Eigenschaften > zurücksetzen**
   .

Dies ist ein Beispiel der Datei **index-logdecoder-custom.xml**.



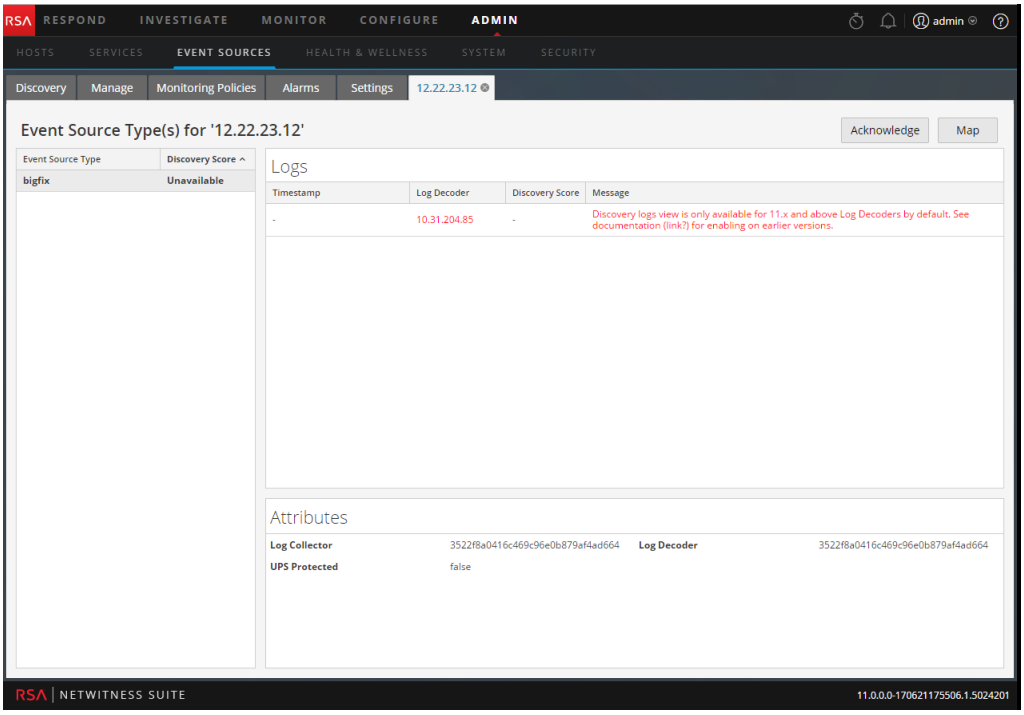
Hinweis: Discovery Scores sind nur für Log Decoder der Version 11.x und höher verfügbar. Discovery Scores für Log Decoder einer Version vor 11.x werden als nicht verfügbar angezeigt.

Im folgenden Beispiel wird der Discovery Score für einen Log Decoder einer Version vor 11.0 in der Ansicht **Details** als **nicht verfügbar** angezeigt.



Hinweis: Geräteprotokolle sind nur für Log Decoder der Version 11.x und höher verfügbar.

Das folgende Beispiel enthält die Meldung, die im Protokollbereich für einen Log Decoder einer Version vor 11.0 angezeigt wird.



Hochladen einer Protokolldatei zu einem Log Decoder

In diesem Thema wird die Methode zum Importieren einer Protokolldatei in einen Log Decoder beschrieben.

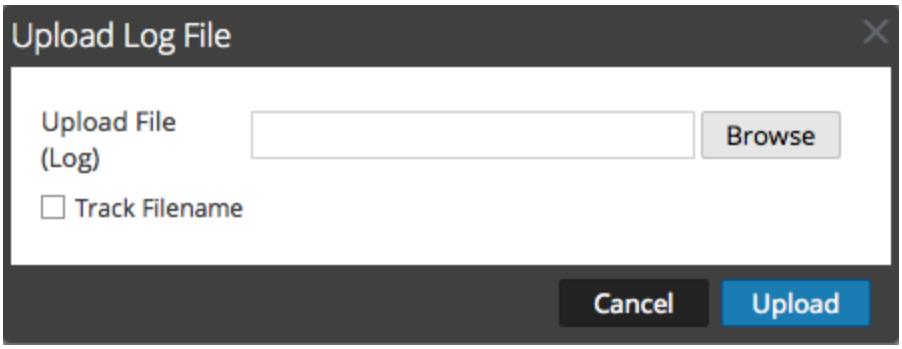
Es kann vorkommen, dass Sie eine Protokolldatei analysieren möchten, die in dem von Ihnen verwendeten Dienst nicht verfügbar ist. Sie können eine Protokolldatei, die in einem anderen Service erfasst wurde, in NetWitness Suite hochladen. Protokolldateinamen haben die Erweiterung **.log**.

Wenn eine Protokolldatei in einen Log Decoder hochgeladen wird, führt der Log Decoder eine Analyse der Datei aus und erzeugt Metadaten für jedes enthaltene Protokoll. Diese Protokolle werden zu den bereits dekodierten Protokollen auf dem Log Decoder hinzugefügt und stehen für die Analyse zur Verfügung. NetWitness Suite enthält eine Option zum Nachverfolgen von Dateinamen, die die Suche nach einem bestimmten Satz von Protokollen erleichtert. Wenn die Protokolldatei mit Dateinachverfolgung hochgeladen wird, fügt der Log Decoder anhand des Namens der hochgeladenen Datei Metadaten zu den Protokollen hinzu. Sie können dann mithilfe dieser Metadaten Sitzungen zur Analyse filtern.

Die Option zum Hochladen einer Protokolldatei ist abgeblendet, wenn andere Log Decoder-Verfahren das Hochladen verhindern, beispielsweise wenn der Log Decoder Protokolle erfasst.

So importieren Sie eine Protokolldatei in einen Log Decoder:

1. Navigieren Sie zu **Administration** > **Services**.
2. Wählen Sie im Raster **Service** einen Log Decoder aus und wählen Sie > **Ansicht** > **System** aus.
   Die Ansicht „Services-System“ für den Log Decoder wird angezeigt.
3. Klicken Sie in der Symbolleiste auf **Protokolldatei hochladen**.



4. Klicken Sie auf **Durchsuchen**, um eine Protokolldatei auszuwählen.
   Eine Verzeichnisansicht wird angezeigt.
5. Wählen Sie die Protokolldatei aus, die Sie hochladen möchten.
   Der Dateiname wird im Feld **Datei hochladen** angezeigt.

6. Wenn der Log Decoder den Protokollen Metadaten auf Basis des hochgeladenen Dateinamens hinzufügen soll, aktivieren Sie das Kontrollkästchen neben **Dateiname nachverfolgen**.
7. Um die Datei hochzuladen, klicken Sie auf **Hochladen**.
   Die ausgewählte Datei wird hochgeladen und eine Statusmeldung gibt an, dass die Datei hochgeladen wurde. Die Protokolldatei ist für Analysen verfügbar.

Hochladen einer Paketerfassungsdatei

Unter Umständen möchten Sie eine Paketerfassungsdatei analysieren, die mit dem verwendeten Service nicht verfügbar ist. Sie können eine Datei, die bei einem anderen Service erfasst wurde, auf NetWitness Suite hochladen. Als Typen von Paketerfassungsdateien werden `pcap` und `pcap.gz` unterstützt.

Wenn eine Paketerfassungsdatei auf einen Decoder hochgeladen wird, erstellt er Sitzungen aus den Paketen der Paketerfassungsdatei. Diese Sitzungen werden zu den bereits dekodierten Sitzungen auf dem Decoder hinzugefügt und stehen für die Analyse zur Verfügung. NetWitness Suite enthält eine Option zum Nachverfolgen von Dateinamen, die die Suche nach einem bestimmten Satz von Sitzungen erleichtert. Wenn die Paketerfassungsdatei mit Dateinachverfolgung hochgeladen wird, fügt der Decoder anhand des Namens der hochgeladenen Datei Metadaten zu den Sitzungen hinzu. Sie können dann mithilfe dieser Metadaten Sitzungen zur Analyse filtern.

Die Option zum Hochladen einer Paketerfassungsdatei ist abgeblendet, wenn andere Decoder-Vorgänge einen Upload verhindern, z. B. wenn der Decoder Pakete erfasst.

So wählen Sie eine Paketerfassungsdatei aus und laden sie hoch:

1. Navigieren Sie zu **Administration** > **Services**.

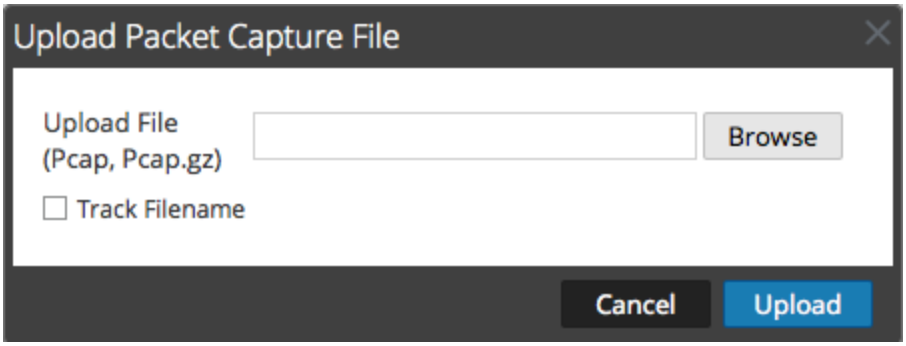
   Die Ansicht „Administration“ > „Services“ wird angezeigt.

2. Wählen Sie den Decoder-Namen und dann die Optionen > **Ansicht** > **System** aus.

   Die Ansicht „Services-System“ für den Decoder wird angezeigt.

3. Klicken Sie in der Symbolleiste auf **Paketerfassungsdatei hochladen**.

   Das Dialogfeld **Paketerfassungsdatei hochladen** wird geöffnet.



4. Um eine Erfassungsdatei auszuwählen, klicken Sie auf **Auswählen**.

   Eine Verzeichnisansicht wird angezeigt.

5. Durchsuchen Sie das Verzeichnis und wählen Sie die Paketerfassungsdatei aus, die Sie hochladen möchten.

Der Dateiname wird im Feld **Datei hochladen (pcap,pcap.gz)** angezeigt.

6. Wenn der Decoder anhand des Dateinamens Metadaten zu den Sitzungen hinzufügen soll, aktivieren Sie das Kontrollkästchen neben **Dateiname nachverfolgen**.
7. Um die Datei hochzuladen, klicken Sie auf **Hochladen**.

   Eine Statusleiste zeigt den Fortschritt des Uploads an.

   Die Uploaddauer hängt von der Dateigröße ab. Wenn der Dateiupload abgeschlossen wurde, wird eine Statusmeldung eingeblendet. Die Datei steht nun zur Untersuchung zur Verfügung.

Feed- und Parser-Referenzen

In diesem Thema finden Sie weitere Informationen zu Feeds und Parsern, die vom Decoder verwendet werden.

- Feeddefinitionsdatei
- Flex-Parser
- Geo IP-Parser
- Lua-Parser
- Suchparser
- Wireless-LAN-Konfiguration

Feeddefinitionsdatei

In diesem Thema wird die Feeddefinitionsdatei beschrieben, die auf der Registerkarte „Dateien“ der Ansicht „Services-Konfiguration“ zur Bearbeitung verfügbar ist.

Eine der Dateien, die in der Ansicht „Services-Konfiguration“ auf der Registerkarte „Dateien“ bearbeitet werden können, ist **`feed-definitions.xml`**, die Feeddefinitionsdatei.

feed-definitions.xml

Sie können Feeds in der Datei `feed-definitions.xml` definieren. Der Decoder verwendet ein XML-Schema, um Feedmeldungen zu definieren, wenn er eine .feed-Binärdatei aus den hier definierten Feeds erstellt.

Details zur Feeddefinitionssprache finden Sie im NextGen-Systemadministratorhandbuch.

Flex-Parser

Eine der Dateien, die in der Ansicht „Services-Konfiguration“ auf der Registerkarte „Dateien“ bearbeitet werden können, ist **NwFlex.xml** (der Flex-Parser).

NwFlex.xml

Es gibt zwei Arten von Flex-Parsern:

- **Serviceidentifizierung auf reiner Portbasis:** Bei diesen Parsern werden zur Identifizierung des Sitzungsanwendungstyps (Service) nur die Quell- oder Zielports verwendet. Diese Parser bieten grundlegende Funktionen und sind einfach zu definieren.
- **Serviceidentifizierung auf Basis gefundener Token:** Bei diesen Parsern wird der Servicetyp anhand von Token identifiziert. Mit ihnen lässt sich einfach erweitern, welche Servicetypen identifiziert werden können. Diese Parser spielen beim Identifizieren von Standardanwendungen ohne Internet eine wichtige Rolle. Für diese Parser muss das Protokoll über ein definierbares Token verfügen, mit dem der Servicetyp eindeutig identifiziert werden kann.

Fünf häufige Parseroperationen sind:

- Port abstimmen und sofort identifizieren
- Port abstimmen und Identifizierung verzögern
- Token abstimmen und sofort identifizieren
- Mehrere Tokens abstimmen
- Token abstimmen und Metadaten erstellen

In diesem Thema werden detaillierte Sprachinformationen und Beispiele gegeben. Das XML-Schema wird beschrieben, mit dem eine FlexParse-Datei definiert wird. Der SML-Knoten, das Attribut und die Werte, auf die in der Beschreibung Bezug genommen wird, sind **fett** hervorgehoben. In jeder Datei muss der Stammknoten der Knoten **parsers** sein. Unter diesem Knoten ist eine beliebige Anzahl des Knotens parser möglich. Über jeden Knoten parser wird ein einzelner Parser definiert. Ein Knoten parser kann optional einen Knoten **declaration** und eine beliebige Anzahl Knoten **match** aufweisen.

Themen

- Arithmetische Funktionen
- Häufige Parservorgänge
- Allgemeine Funktionen
- Protokollierungsfunktionen
- Nodes
- Nutzlastfunktionen
- Regex
- Zeichenfolgefunktionen

Arithmetische Funktionen

In diesem Thema wird die Sprache für die arithmetischen Funktionen des Flex-Parsers definiert.

In diesem Thema wird die Sprache für die arithmetischen Funktionen des Flex-Parsers definiert. Die Zahlen sind nicht signierte 64 Bit-Werte und unterliegen je nach Vorgang dem Überlauf oder dem Unterlauf.

Sprachdefinition

In der folgenden Tabelle werden Sprachdefinitionen beschrieben.

Node-Name	Attributname	Beschreibung
`and`		Verfährt bitweise UND zwischen zwei Zahlen
	`name`	Variable für UND Ergebnis in
	`value`	Zahl für UND in Ergebnis.
`or`		Verfährt bitweise ODER zwischen zwei Zahlen
	`name`	Variable für ODER Ergebnis in
	`value`	Zahl für ODER in Ergebnis
`increment`		ADDITION zweier Zahlen
	`name`	Variable, die den Anfangswert enthält UND ADDITIONS-Ergebnisse erhält
	`value`	Zahl, die zum Anfangswert ADDIERT wird
`decrement`		SUBSTRAKTION zweier Zahlen
	`name`	Variable, die den Anfangswert enthält UND SUBSTRAKTIONS-Ergebnisse erhält.
	`value`	Zahl, die vom Anfangswert SUBTRAHIERT wird.
`divide`		DIVISION zweier Zahlen

Node-Name	Attributname	Beschreibung
	name	Variable, die den Anfangswert enthält UND DIVISIONS-Ergebnisse erhält
	value	Eine Zahl, durch die der Anfangswert geteilt werden soll. Eine Division durch null erzeugt einen Fehler und beendet die weitere Verarbeitung der aktuellen Sitzung durch diesen Parser.
modulo		MODULO zweier Zahlen
	name	Variable, die den Anfangswert enthält UND MODULO-Ergebnisse erhält
	value	Eine Zahl, durch die der Anfangswert geteilt werden soll. Eine Division durch null erzeugt einen Fehler und beendet die weitere Verarbeitung der aktuellen Sitzung durch diesen Parser.
multiply		MULTIPLIKATION zweier Zahlen.
	name	Variable, die den Anfangswert enthält UND MULTIPLIKATIONS-Ergebnisse erhält
	value	Zahl, mit der der Anfangswert MULTIPLIZIERT werden muss
shiftleft		Binäre Umverteilung nach links
	name	Variable, die den Anfangswert enthält UND Umverteilungsergebnisse erhält
	value	Anzahl der Bits, um die verschoben werden soll.
shiftright		Binäre Umverteilung nach rechts

Node-Name	Attributname	Beschreibung
	name	Variable, die den Anfangswert enthält UND Umverteilungsergebnisse erhält.
	value	Anzahl der Bits, um die verschoben werden soll.

Häufige Parservorgänge

In diesem Thema finden Sie einige Beispiele für häufige Parservorgänge.

Dieses Thema enthält fünf häufige Parservorgänge.

Port abstimmen und sofort identifizieren

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
          <parser name="CustApp" desc="Acme Custom App" service="45324">
               <declaration>
                    <port name="port" value="45324" />
               <declaration>
               </match name="port">
                    <identify />
               </match>
          </parser>
</parsers>
```

Port abstimmen und Identifizierung verzögern

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MSRPC" desc="Microsoft RPC protocol" service=135">
          <declaration>
               <port name="port" value="135" />
               <number name="state" scope="session" />
               <session name="end" value="end" />
          </declaration>
          <match name="port">
               <assign name="state" value="1" />
          </match>
          <match name="end">
```

```
            <if name="state" equal="1" />
                 <identify />
            </if>
        </match>
    </parser>
</parsers>
```

Token abstimmen und sofort identifizieren

```
<?xml version="1.0" encoding="utf-8?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="RDP" desc="Remote Desktop Protocol" service="3389">
          <declaration>
               <token name="signature" value="Cookie: mstshash=" />
          </declaration>
          <match name="signature">
               <identify />
          </match>
     </parser>
</parsers>
```

Mehrere Tokens abstimmen

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MyServiceMultiToken" desc="Multiple Tokens"
     service="333">
          <declaration>
               <number name="state" scope="stream" />
               <token name="user" value="USER " />
               <token name="pass" value="PASS " />
               <session name="session" value="end" />
          </declaration>
```

```
          <match name="user">
               <or name="state" value="1" />
          </match>
          <match name="pass">
               <or name="state" value="2" />
          </match>
          <match name="session">
               <if name="state" equal="3">
                    <identify />
               </if>
          </match>
     </parser>
</parsers>
```

Token abstimmen und Metadaten erstellen

```
<?xml version="1.0" encoding="utf-8"?>
<parsers xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="SHELL" desc="Command Shell Identification">
          <declaration>
               <token name="cmd.exe" value=" (C) Copyright 1985-2001
               Microsoft Corp" options="linestart" />
               <meta name="client" key="client" format="Text" />
          </declaration>
          <match name="cmd.exe"
               <register  name="client" value="MS Command Shell" />
          </match>
     </parser>
</parsers>
```

Allgemeine Funktionen

In diesem Thema wird die Sprache für die allgemeinen Funktionen des Flex-Parsers definiert.

Allgemeine Funktionen Sprachdefinition

Node-Name	Attributname	Beschreibung
apptype		Ruft den aktuell definierten Servicetyp für die aktuelle Sitzung ab.
	name	Eine Zahlenvariable, um den aktuellen Servicetyp zu erhalten
identify		Markiert die Sitzung mit dem Servicetyp des Parsers, wenn der Servicetyp noch nicht identifiziert wurde.
assign		Weist der Variablen einen Wert zu.
	name	Die eindeutige Kennung, die dem Element im Abschnitt „declaration“ zugewiesen wird.
	value	Optional. Falls angegeben, wird die in der Übereinstimmung definierte Aktion nur angewendet, wenn die Deklaration mit dem gegebenen Wert übereinstimmt.
getmeta		Ruft den Wert von Metadaten ab, die einen Rückruf erzeugt haben. Diese Funktion wird zu leeren Ergebnissen führen (0, leere Zeichenfolge), wenn sie aufgerufen wird und es gar keinen Metarückruf gab.
	name	Die Variable, die den Wert der Metadaten empfängt, die den Rückruf erzeugt haben.
gettoken		Gibt das aktuell übereinstimmende Token zurück.
	name	Eine Zeichenfolgenvariable, die das aktuell übereinstimmende Token empfängt. Wenn es kein aktuelles Token gibt, wird der Variablen eine leere Zeichenfolge zugewiesen.

Node-Name	Attributname	Beschreibung
end		Dies beendet die Ausführung des aktuellen Abschnitts **Übereinstimmung**.
if		Vergleicht zwei Werte. Führt eventuelle Unteraktionen aus, wenn der Vergleich wahr ist. Vergleiche können vom Typ **Zahl** oder **Zeichenfolge** sein, solange beide Werte den gleichen Typ haben.
	name	Die eindeutige Variablenkennung, die dem Element im Abschnitt **Deklaration** zugewiesen wurde.
	equal notequal less lessequal greater greaterequal and or	Der zu vergleichende Vorgangswert. Wenn wahr, werden eventuelle Unteraktionen ausgeführt.
register		Fügt der Sitzung Metadaten hinzu.
	name	Die eindeutige Kennung einer zu erstellenden Metavariablen, wie im Abschnitt **Deklaration** definiert.
	value	Der Wert der zu erstellenden Metadaten.
while		Vergleicht zwei Werte und führt eventuelle Unteraktionen aus, wenn der Vergleich wahr ist. Vergleiche können vom Typ **Zahl** oder **Zeichenfolge** sein, solange beide Werte den gleichen Typ haben.

Node-Name	Attributname	Beschreibung
	name	Die eindeutige Variablenkennung, die dem Element im Abschnitt „declaration“ zugewiesen wird.
	equal notequal less lessequal greater greaterequal and or	Gibt den zu vergleichenden Vorgangswert an. Wenn wahr, werden eventuelle Unteraktionen ausgeführt. Die Attribute **and** und **or** bedeuten bitweise Vorgänge und können nur auf **Zahlen**variablen angewendet werden.
call		Führt das angegebene **übereinstimmende** Element aus. Dies kann jedes übereinstimmende Element sein, das im gleichen Flex-Parser definiert wurde, unabhängig davon, wie es deklariert wurde.
	value	Der Name des übereinstimmenden Elements oder eine Zeichenfolgenvariable, die den Namen eines übereinstimmenden Elements enthält. • Wenn das übereinstimmende Element angegeben wurde, wird der Parser nicht laden, wenn das benannte übereinstimmende Element nicht existiert. • Wenn eine Zeichenfolgenvariable angegeben wird, wird das Element **call** alle eventuell vorhandenen untergeordneten Elemente ausführen, wenn sich der Wert der Zeichenfolge nach Ausführung des benannten übereinstimmenden Elements in ein übereinstimmendes Element auflöst. • Wenn kein **übereinstimmendes** Element gefunden werden kann, das mit dem Zeichenfolgenwert übereinstimmt, erfolgt keine Aktion.

Protokollierungsfunktionen

In diesem Thema wird die Sprache für die Protokollierungsfunktionen des Flex-Parsers definiert.

Die Protokollierungsfunktionen bieten eine Methode für den Flex-Parser zum Schreiben in das Systemprotokoll. Protokollierungsfunktionen können beim Erstellen eines neuen Flex-Parsers sehr nützlich sein, sollten jedoch auf ein absolutes Minimum beschränkt werden, wenn ein Flex-Parser für ein Produktionssystem bereitgestellt wird.

Sprachdefinition

Node-Name	Attributname	Beschreibung
`failure`		Protokolliert eine Meldung im Systemprotokoll mit dem Level **Fehler**.
	`value`	Eine Zeichenfolge, die als Protokollmeldung verwendet werden soll.
`warning`		Protokolliert eine Meldung im Systemprotokoll mit dem Level **Warnung**.
	`value`	Eine Zeichenfolge, die als Protokollmeldung verwendet werden soll.
`info`		Protokolliert eine Meldung im Systemprotokoll mit dem Level **Info**.
	`value`	Eine Zeichenfolge, die als Protokollmeldung verwendet werden soll.
`debug`		Protokolliert eine Meldung im Systemprotokoll mit dem Level **Debug**.
	`value`	Eine Zeichenfolge, die als Protokollmeldung verwendet werden soll.

Nodes

In diesem Thema wird die Sprache für die Flex-Parser-Nodes definiert.

Definition Node-Sprache

Node-Name	Attributname	Beschreibung
parsers		Stammknoten in jeder einzelnen Definitionsdatei
	xmins:xsi	Definiert den Namespace zur Verwendung in der Schema-Aufnahme. Dieses Attribut ist nicht erforderlich; eine Sprachdefinition ist jedoch ohne das Attribut nicht möglich. Dieser Node muss folgenden Wert haben: http://www.w3.org/2001/XMLSchema-instance
	xsi:noNamespaceSchemaLocation	Definiert die XSD-Schema-Validierungsdatei, die zur Validierung der Sprachdefinition verwendet wird. Dieses Attribut ist nicht erforderlich; eine Sprachdefinition ist jedoch ohne das Attribut nicht möglich. Dieser Node muss folgenden Wert haben: parsers.xsd

Node-Name	Attributname	Beschreibung
parser		Node, der eine einzelne Parserdefinition definiert Dieser Node muss sich direkt unterhalb des Node parsers befinden. Es kann mehr als einen pro Datei geben.
	name	Name, der den Parser eindeutig identifiziert Dieser Name sollte kurz und prägnant sein. Er wird vom System verwendet, um eine Aktivierung und Deaktivierung zu ermöglichen. Er sollte ausschließlich die Buchstaben [a-z] und [A-Z] beinhalten.
	desc	Dieser Node bietet eine Tätigkeitsbeschreibung des Parsers.
	service	Dies ist die eindeutige Kennnummer, die der Sitzung nach der Identifizierung zugewiesen wird.
declaration		Node, der die Definition beschreibt Jede dieser Definitionen kann über einen zugeordneten match-Eintrag verfügen.

Node-Name	Attributname	Beschreibung
token		Gibt eine Definition zur Identifizierung eines Tokens innerhalb des Sitzungsprotokolls an Hiermit wird ein match-Rückruf definiert, wenn die festgelegten Token in einer Sitzungsnutzlast gefunden werden. Die read-Position wird auf das Byte gesetzt, das unmittelbar nach dem übereinstimmenden Token folgt.
	name	Dies ist eine eindeutige Kennung für die Deklaration.
	value	Dies ist der exakte, zu identifizierende Tokenwert.
	options	Die Optionen geben an, dass das Token in einer neuen Zeile oder am Ende einer Zeile beginnen soll (linestart oder linestop).
meta-callback		Erfasst einen Rückruf für den Flex-Parser, wenn Metadaten eines bestimmten Formats erstellt werden. Dies kann zusätzlich so qualifiziert werden, dass nur Rückrufe von Sitzungen generiert werden, die als spezifischer Anwendungstyp (z. B. 80 für http) identifiziert wurden.

Node-Name	Attributname	Beschreibung
	name	Name des übereinstimmenden Elements, das nach einem Rückruf ausgeführt wird (Zeichenfolge)
	key	Name des Metaschlüssels, der Rückrufe generiert (Zeichenfolge)
	format	Datentyp des Metaschlüssels, der Metadaten generiert
	apptype	Der Metarückruf wird nur dann generiert, wenn die analysierte Sitzung mithilfe des festgelegten Anwendungstyps identifiziert wurde. (Ganzzahl ohne Vorzeichen, optional)
number		Definiert eine numerische Variable, die an anderer Stelle innerhalb der Parserdefinition referenziert werden kann. Alle numerischen Werte sind nicht signierte 64-Bit-Werte.
	name	Dies ist eine eindeutige Kennung für die Deklaration.
	scope (optional)	Gibt an, wann die Variable zurückgesetzt werden soll. Dies kann entweder für beide Seiten einer zweiseitigen Sitzung oder erst nach Erkennung einer neuen Sitzung erfolgen. Die möglichen Werte sind **global**, **constant**, **stream** und session (Standard).

Node-Name	Attributname	Beschreibung
`string`		Definiert eine numerische Variable, die an anderer Stelle innerhalb der Parserdefinition referenziert werden kann.
	`name`	Dies ist eine eindeutige Kennung für die Deklaration.
	`scope` (optional)	Gibt an, wann die Variable zurückgesetzt werden soll. Dies kann entweder für beide Seiten einer zweiseitigen Sitzung oder erst nach Erkennung einer neuen Sitzung erfolgen. Die möglichen Werte sind **`global`**, **`constant`**, **`stream`** und `session` (Standard).
port		Definiert einen **übereinstimmenden** Rückruf, wenn eine Sitzung festgestellt wird, die diesen bestimmten Port verwendet Die **Lese**position wird auf das erste Byte des ersten Datenstreams (Clients) in der Sitzung gelegt.
	`name`	Dies ist eine eindeutige Kennung für die Deklaration.
	`value`	Dies ist die zu identifizierende Portnummer.

Node-Name	Attributname	Beschreibung
session		Definiert einen match -Rückruf für Anfangs-/Endereignisse einer Sitzung Diese Ereignisse treten nur auf, wenn in der Sitzung ein Token für den Parser vorhanden ist.
	name	Dies ist eine eindeutige Kennung für die Deklaration.
	value	Gibt an, ob die Verarbeitung zu Beginn einer neuen Sitzung oder am Ende einer Sitzung ausgeführt wird (begin oder end).
stream		Definiert einen match-Rückruf für Anfangs-/Endereignisse eines Datenstreams. Diese Ereignisse kommen nur vor, wenn ein Token für den Parser im Datenstream vorhanden ist.
	name	Dies ist eine eindeutige Kennung für die Deklaration.
	value	Legt fest, dass die Verarbeitung zu Beginn oder am Ende eines Datenstreams ausgeführt wird (begin oder end).

Node-Name	Attributname	Beschreibung
function		Definiert einen match-Abschnitt, der als generische Funktion verwendet werden kann Es stehen keine Rückrufe mit dieser Deklaration im Zusammenhang.
	name	Dies ist eine eindeutige Kennung für die Deklaration.
meta		Definiert den Datentyp, den der Parser erstellt
	key	Legt den Schlüsselnamen fest Der Schlüssel muss eine Größe von 1-16 Bytes haben.
	format	Gibt den Variantentyp an (z. B. **Text**, **IPv4**, **UInt32**). Um eine vollständige Liste zu erhalten, siehe die SDK-Dokumentation.
pattern		Definiert eine Variable für einen regulären Ausdruck zur Verwendung durch die regex-Funktion.
	name	Dies ist eine eindeutige Kennung für die Deklaration.

Node-Name	Attributname	Beschreibung
	`scope` (optional)	Gibt an, wann die Variable zurückgesetzt werden soll. Dies kann entweder für beide Seiten einer zweiseitigen Sitzung oder erst nach Erkennung einer neuen Sitzung erfolgen. Die möglichen Werte sind **`global`**, **`constant`**, **`stream`** und `session` (Standard).
	`value` (optional)	Legt einen regulären Ausdruck fest, welcher der Mustervariable zugeordnet wird Dieses Attribut ist nur gültig, wenn das Attribut **`scope attribute`** auf `constant` gesetzt ist.

Node-Name	Attributname	Beschreibung
match		Die möglichen Einträge für Maßnahmen, die nach Finden eines Übereinstimmungskriteriums für eine Deklaration ausgeführt werden. Diese Nodes können zudem verschachtelt werden, um eine tiefere Logik bereitzustellen. Es gibt verschiedene Kategorien für Ausführungselemente (Funktionen), die einem übereinstimmenden Element untergeordnet werden können: • Allgemein • Arithmetisch • Zeichenfolge • Nutzlast

Nutzlastfunktionen

In diesem Thema wird die Sprache für die Nutzlastfunktionen des Flex-Parsers definiert.

Diese Funktionen werden auf eine `read`-Position angewendet, die am Beginn eines `match` -Elements festgelegt wird.

Sprachdefinition

Node-Name	Attributname	Beschreibung
`find`		Durchsucht die Streamnutzlast ab der Leseposition nach einem angegebenen Zeichenfolgenwert. Wenn der Wert gefunden wird, so wird der Offset von der Leseposition zurückgegeben. Dann werden alle untergeordneten Elemente ausgeführt. Wenn der Wert nicht gefunden wird, werden die untergeordneten Elemente nicht ausgeführt.
	`name`	Eine `number`-Variable, um Abweichungen von der `read`-Position abzurufen, an der die Übereinstimmung beginnt.
	`value`	Eine zu suchende Zeichenfolge
	`length` (optional)	Eine Beschränkung der Länge der zu durchsuchenden Nutzlast. Wenn kein Limit angegeben wird, wird der Rest der Nutzlast durchsucht. Es wird empfohlen, hier immer den kleinstmöglichen Wert zu verwenden, um die Auswirkungen auf die Performance zu reduzieren.

Node-Name	Attributname	Beschreibung
`install-decoder`		Ermöglicht Token die Abstimmung mit Nutzlastdaten, auch wenn diese fragmentiert oder anderweitig codiert sind. Ein Scandecoder kann installiert werden, um einen Abschnitt der Nutzlast vorzubereiten, bevor er auf Token gescannt wird. Ein Beispiel wäre eine HTTP-Antwort, bei der die segmentierte Übertragungscodierung mit gzip-Inhaltscodierung verwendet wird. Durch Analyse des HTTP-Headers können die benötigten Parameter für Typ, Offset und Länge alle eingestellt werden, und danach scheint die HTTP-Antwortnutzlast gegenüber dem scannenden Token so, als ob keine Codierung angewendet worden wäre. Dabei ergeben sich jedoch bedeutende Overheads.
	`type`	Der Typ des zu installierenden Decoders. Gültige Optionen sind: gzip, deflate, chunked, chunked-gzip, chunked-deflate.
	`offset`	Offset von der aktuellen Leseposition für den Beginn der Decodierung.
	`length`	Die maximale zu decodierende Nutzlastlänge.
`isdecoding`		Testet, ob ein installierter Decoder derzeit aktiv ist. Wenn dies der Fall ist, werden alle untergeordneten Elemente dieser Funktion ausgeführt. Diese Funktion hat keine Parameter.

Node-Name	Attributname	Beschreibung
`move`		Verschiebt die `read`-Position im aktuellen Stream um die angegebene Byteanzahl nach vorn. Wenn im Stream genügend Daten enthalten sind, wird die `read`-Position aktualisiert. Dann werden alle untergeordneten Elemente ausgeführt. Wird nichts gefunden, bleibt die `read`-Position unverändert und untergeordnete Elemente werden nicht ausgeführt.
	`value`	Gibt an, um wie viele Byte die `read`-Position verschoben werden soll.
	`direction` (optional)	Die Richtung, in der die aktuelle Leseposition verschoben wird. Kann `forward` (Standard) oder **`reverse`** sein.
`packetid`		Gibt die ID des Pakets für die aktuelle Leseposition zurück. Das Ergebnis kann 0 sein, wodurch angegeben wird, dass die Paket-ID nicht festgestellt werden konnte.
	`name`	Eine Zahlenvariable zum Empfang der aktuellen Paket-ID.
`payload-position`		Gibt die aktuelle Leseposition zurück. Dies ist ein null-basierter Index in die Streamnutzlast.
	`name`	Eine Zahlenvariable zum Empfang der aktuellen Leseposition.
`read`		Liest eine angegebene Anzahl von Byte ab der `read`-Position in eine Variable. Wenn im Stream genügend Daten enthalten sind, wird die `read`-Position aktualisiert, der Datenlesevorgang wird zugewiesen und alle untergeordneten Elemente werden dann ausgeführt. Wird nichts gefunden, bleibt die `read`-Position unverändert und untergeordnete Elemente werden nicht ausgeführt.

Node-Name	Attributname	Beschreibung
	`name`	Der Name einer `string`- oder `number`-Variablen zum Empfang der Streamdaten. Wenn eine `number`-Variable angegeben wird, werden die gelesenen Byte als ein vorzeichenloser numerischer Wert interpretiert.
	`length`	Die Anzahl der Byte, die aus einem Stream gelesen werden sollen.
	`endianess` (optional)	Die Byte-Reihenfolge, die beim Lesen in eine Zahlenvariable verwendet werden soll. Kann `big` (Standardwert) oder `little` sein. Das Attribut ist beim Lesen in eine `string`-Variable ungültig.

Regex

In diesem Thema wird die Sprache für den Regex-Node des Flex-Parsers definiert.

Regex sucht in der Streamnutzlast ausgehend von der `read`-Position nach Treffern für einen bestimmten regulären Ausdruck. Werden Treffer gefunden, werden die Abweichung von der `read`-Position und optional auch die gefundene Zeichenfolge zurückgegeben. Untergeordnete Elemente werden ausgeführt. Werden keine Treffer gefunden, werden untergeordnete Elemente nicht ausgeführt.

Sprachdefinition

Attributname	Beschreibung
`name`	Eine `number`-Variable, um Abweichungen von der `read`-Position abzurufen, an der die Übereinstimmung beginnt
`value`	Ein regulärer Ausdruck, der gefunden werden soll.
`length` (optional)	Eine Beschränkung der Länge der zu durchsuchenden Nutzlast. Wenn kein Limit angegeben wird, wird der Rest der Nutzlast durchsucht. Es wird empfohlen, hier immer den kleinstmöglichen Wert zu verwenden, um die Auswirkungen auf die Performance zu reduzieren.
`found` (optional)	Der Name einer `string`-Variablen, die eine gefundene Zeichenfolge erhalten soll.

Zeichenfolgefunktionen

Dieses Thema enthält Sprachdefinitionen für die Zeichenfolgenfunktionen des Flex-Parsers.

Sprachdefinitionen der Zeichenfolgenfunktionen

Node-Name	Attributname	Beschreibung
`append`		Fügt am Ende einer `string`-Variablen eine Zahl oder eine Zeichenfolge hinzu.
	`name`	Die eindeutige Kennung einer Zeichenfolgenvariablen, der der angegebene Wert hinzugefügt werden soll.
	`value`	Eine hinzuzufügende Zahl oder Zeichenfolge.
`find`		Durchsucht eine Zeichenfolge nach dem angegebenen Zeichenfolgenwert. Wenn dieser gefunden wurde, wird die Position zurückgegeben und alle untergeordneten Elemente werden ausgeführt. Andernfalls werden die untergeordneten Elemente nicht ausgeführt.
	`name`	Eine `number`-Variable, die die nullbasierte Position erhalten soll, an der die angegebene Wertzeichenfolge in der **in**-Zeichenfolge gefunden wurde.
	`value`	Eine zu suchende Zeichenfolge
	`in`	Eine zu suchende Zeichenfolge.
	`length` (optional)	Eine Beschränkung der Länge der zu durchsuchenden **in**-Zeichenfolge. Wenn keine Beschränkung angegeben wird, wird die gesamte **in**-Zeichenfolge durchsucht.

Node-Name	Attributname	Beschreibung
`length`		Weist einer `number`-Variablen die Länge einer Zeichenfolge zu.
	`name`	Eine `number`-Variable, die die Länge der angegebenen Zeichenfolge erhalten soll.
	`value`	Ein Zeichenfolgenwert, dessen Länge bestimmt werden soll.
`regex`		Durchsucht eine Zeichenfolge nach Übereinstimmungen in Bezug auf den angegebenen regulären Ausdruck. Wird eine Übereinstimmung gefunden, werden die Position und wahlweise auch die übereinstimmende Zeichenfolge zurückgegeben. Dann werden alle untergeordneten Elemente ausgeführt. Wenn der Wert nicht gefunden wird, werden die untergeordneten Elemente nicht ausgeführt. Vorgänge unter Verwendung regulärer Ausdrücke können sich negativ auf die Systemperformance auswirken.
	`name`	Eine Zahlenvariable, die die nullbasierte Position erhalten soll, an der eine Übereinstimmung mit dem angegebenen regulären Ausdruck in der „in“-Zeichenfolge gefunden wurde.
	`value`	Ein regulärer Ausdruck, nach dem gesucht wird.
	`in`	Eine zu suchende Zeichenfolge.

Node-Name	Attributname	Beschreibung
	`length` (optional)	Eine Beschränkung der Länge der zu durchsuchenden `in`-Zeichenfolge. Wenn keine Beschränkung angegeben wird, wird die gesamte **in**-Zeichenfolge durchsucht.
	`found` (optional)	Der Name einer Zeichenfolgenvariablen, die die übereinstimmende Zeichenfolge erhalten soll.
`substring`		Es muss mindestens eins der optionalen Attribute `from` und `length` angegeben werden.
	`name`	Die eindeutige Kennung einer Zeichenfolgenvariablen, die den extrahierten Wert erhalten soll.
	`value`	Ein Zeichenfolgenwert, aus dem eine untergeordnete Zeichenfolge extrahiert werden soll.
	`from` (optional)	Die nullbasierte Position, ab der die untergeordnete Zeichenfolge beginnt. Wird dieser Wert nicht angegeben, wird standardmäßig null verwendet.
	`length` (optional)	Die Anzahl der zu extrahierenden Zeichen. Wird dieser Wert nicht angegeben, wird standardmäßig die verbleibende Länge der Zeichenfolge verwendet.
`tolower`		Wandelt eine Zeichenfolge komplett in Kleinbuchstaben um.

Node-Name	Attributname	Beschreibung
	`name`	Der Name einer zu verarbeitenden `string` -Variablen.
`toupper`		Wandelt eine Zeichenfolge komplett in Großbuchstaben um.
	`name`	Der Name einer zu verarbeitenden `string`-Variablen.
`urldecode`		Dekodiert eine Zeichenfolge, die URl-kodierte Zeichen enthält.
	`name`	Eine Zeichenfolgenvariable, um die dekodierte Zeichenfolge zu erhalten.
	`value`	Eine URL-kodierte zu dekodierende Zeichenfolge.
`base64decode`		Dekodiert eine Zeichenfolge mit Base-64-Kodierung.
	`name`	Eine Zeichenfolgenvariable, um die dekodierte Zeichenfolge zu erhalten.
	`value`	Eine URL-kodierte zu dekodierende Zeichenfolge.
uudecode		Dekodiert eine Zeichenfolge mit UU-Kodierung.
	`name`	Eine Zeichenfolgenvariable, um die dekodierte Zeichenfolge zu erhalten.
	`value`	Eine Zeichenfolge mit UU-Kodierung. Der Header und die nachstehenden Zeilen sollten nicht enthalten sein.

Node-Name	Attributname	Beschreibung
quotedprintabledecode		Dekodiert eine Zeichenfolge mit Quoted-Printable-Kodierung.
	name	Eine Zeichenfolgenvariable, um die dekodierte Zeichenfolge zu erhalten.
	value	Eine Zeichenfolge mit Quoted-Printable-Kodierung.
convert-ebcdic		Konvertiert eine EBCDIC-Zeichenfolge in das entsprechende ASCII-Format.
	name	Eine Zeichenfolgenvariable, um die dekodierte Zeichenfolge zu erhalten.
	value	Eine URL-kodierte zu dekodierende Zeichenfolge.

Geo IP-Parser

In diesem Thema wird der Geo IP-Parser für Decoder eingeführt.

Eine der Dateien, die in der Ansicht „Services-Konfiguration“ auf der Registerkarte „Dateien“ bearbeitet werden können, ist **`GeoPrivate.ipl`** (der Geo IP-Parser).

GeoPrivate.ipl

Der Geo IP-Parser ist ein fester Parser, der IP-Adressen in geografische Standorte konvertiert. Die Standorte werden über die Google Earth-Anzeige angezeigt.

Die Geostandort-Metadaten in `GeoPrivate.ipl` werden für **`ip.src`** und `ip.dst` hinzugefügt. Der Parser verwendet die externen Datendateien **`GeoCity.dat`** und `GeoCountry.dat`, die beide im Anwendungsverzeichnis gespeichert sind. Für jede IP-Adresse gibt es bis zu acht Metadaten, die in der Tabelle unten aufgeführt sind.

Metadaten	Beschreibung
`city.dst`	Zielstadt
`city.src`	Quellstadt
`country.dst`	Zielland
`country.src`	Quellland
`latdec.dst`	Dezimaler Breitengrad des Ziels
`latdec.src`	Dezimaler Breitengrad der Quelle
`longdec.dst`	Dezimaler Längengrad des Ziels
`longdec.src`	Dezimaler Längengrad der Quelle

Lua-Parser

Eine der Dateien, die in der Ansicht „Services-Konfiguration“ auf der Registerkarte „Dateien“ bearbeitet werden können, ist **`NwLua.xml`** (der Lua-Parser).

Liste der Lua-Parser

Es gibt eine Reihe von Lua-Parsern, die in Live zur Verfügung stehen. In RSA Content finden Sie Folgendes:

- eine vollständige Liste dieser Parser
- ihre Abhängigkeiten voneinander
- die Flex-Parser, die von den Lua-Parsern zusammengefasst werden

Fünf häufige Parseroperationen sind:

- Port abstimmen und sofort identifizieren
- Port abstimmen und Identifizierung verzögern
- Token abstimmen und sofort identifizieren
- Mehrere Tokens abstimmen
- Token abstimmen und Metadaten erstellen

Suchparser

In diesem Thema wird erläutert, wie Sie einen benutzerdefinierten Parser auf einem Decoder konfigurieren, damit er Metadaten generiert. Der Parser durchsucht zum Generieren der Metadaten die Ansicht „Services-Konfiguration“ > Registerkarte „Dateien“ nach vordefinierten Schlüsselwörtern und regulären Ausdrücken.

Eine der in der Ansicht „Services-Konfiguration“ > Registerkarte „Dateien“ zur Bearbeitung verfügbaren Dateien ist **search.ini** (der Suchparser).

search.ini

Der Such-Parser ist ein benutzerdefinierter Parser, der Metadaten generiert, indem er nach vordefinierten Schlüsselwörtern und regulären Ausdrücken sucht. Der Parser durchsucht die Nutzlast einer rekonstruierten Sitzung nach passenden Zeichenfolgen und kann eine Suche nach einem regulären Ausdruck durchführen. Sie können den Parser konfigurieren, indem Sie die Datei search.ini bearbeiten.

Achtung: Der Suchparser kann wesentliche Auswirkungen auf die Systemperformance haben. Es ist wichtig, dass sowohl der Suchmechanismus als auch die Daten, auf die er angewendet wird, vor der Erstellung neuer Suchdefinitionen und der Aktivierung des Suchparsers gründlich verstanden wurden.

Die Suchdefinition wird über alle Protokolle verwendet. Es gibt drei grundlegende Suchmethoden:

- Schlüsselwort: Einen Stream nach bestimmten Wörtern durchsuchen
- Pattern: Einen Stream nach Übereinstimmungen mit einem regulären Ausdruck durchsuchen
- Schlüsselwort + Muster: Einen Stream nach einem regulären Ausdruck durchsuchen, wenn er einen angegebenen Satz von Schlüsselwörtern enthält.

Eine detaillierte Erläuterung finden Sie unter Such-Parser in der Syntax der Suchzeichenfolge für search.ini.

Syntax der Suchzeichenfolge für search.ini

In diesem Thema werden Suchmethoden und die Syntax zur Verwendung im Suchparser vorgestellt.

Der Suchparser verwendet drei grundlegende Suchmethoden:

- Schlüsselwort: Durchsuchen eines Streams nach bestimmten Wörtern
- Pattern: Durchsuchen eines Streams nach Übereinstimmungen mit einem regulären Ausdruck
- Schlüsselwort+Muster: Durchsuchen eines Streams nach einem regulären Ausdruck, wenn er einen angegebenen Satz von Schlüsselwörtern enthält

Syntax

```
Maxrecon=<max_size>Maxsearch=<max_ssearch_length>MatchLimit=<max_
matches_per_stream
Search Name
Services=<service_id_list>Keywords=<keyword_
list>|Pattern=<expression>Case=0|1
Proximity=<number_of_bytes>Recon=0|1
Raw=0|1
```

Parameter

In diesem Befehl verwendete Parameter:

Parameter	Beschreibung
`autocheck`	Behebt automatisch alle Probleme ohne Eingabeaufforderung
`header Only`	Prüft den Header jeder Datei und zeigt ihn an
`chatty`	Zeigt einen Hex-Speicherauszug von jedem Objekt in der Datei (riesige Datenmenge)
`dump#-#`	Gibt ein nullbasiertes Objekt oder einen nullbasierten Objektbereich an, der in hex an die Konsole ausgegeben werden soll

Beispiel

Im Folgenden wird ein Beispiel für den Befehl gezeigt:

Prüft alle NetWitness-Datenbankdateien in der Sammlung „Default“. Wenn Probleme gefunden werden, werden diese beschrieben und Sie gefragt, ob Sie sie beheben möchten.

```
dbcheck C:\Documents and Settings\User\My Documents\NetWitness\
Investigations\Default\*.nw*
```

Wireless-LAN-Konfiguration

In diesem Thema wird die Wireless-LAN-Konfigurationsdatei für Decoder erläutert, die Sie in der Ansicht „Services-Konfiguration“ > Registerkarte „Dateien“ finden.

wlan-config.xml

Eine der Dateien, die in der Ansicht „Services-Konfiguration“ **Registerkarte „Dateien“ bearbeitet werden kann, ist** `wlan-config.xml` (die Wireless-LAN-Konfigurationsdatei).

Sie steuert die 802.11-Parser. Ihr Hauptzweck besteht darin, die Entschlüsselung unverarbeiteter 802.11-Frames zu steuern, die vom Decoder erfasst werden. Diese Datei ist optional. Wenn die Entschlüsselung des 802.11-Datenverkehrs nicht gewünscht wird, braucht die Datei nicht erstellt zu werden.

Es gibt fünf Parser auf Linkebene, die mit der Wireless-LAN-Paketerfassung verknüpft sind:

- IEEE 802.11-Parser (nur Datenframes und Beacons)
- Radiotap mit 802.11-Header
- AVS (Absolute Value Systems) mit 802.11-Header
- Prism II mit 802.11-Header
- CACE's „Per Packet Information“ (PPI) mit 802.11-Header

Die 802.11-Wireless-Parser, die in 9.8 eingeführt wurden, verwenden alle dieselbe Konfigurationsdatei. Diese Datei, wlan-config.xml, dient zur Definition aller Wireless-Zugriffspunkte, über die der Benutzer im Netzwerk verfügt, und ihr Hauptzweck besteht in der Steuerung der Entschlüsselung. Die BSSID des Zugriffspunkts und die SSID, für die sie als Autorität gilt, werden der Datei hinzugefügt, ebenso wie alle aktiven Standardschlüssel, die vom Zugriffspunkt verwendet werden.

Decoder- und Log Decoder-Referenzen

Dies ist eine Sammlung von Referenzen, in denen Sie Informationen zur Benutzeroberfläche für Decoder und Log Decoder in NetWitness Suite finden, mit Verweisen auf Verfahren, die beschreiben, was Sie im jeweiligen Teil der Benutzeroberfläche tun können. Diese Themen sind in alphabetischer Reihenfolge aufgeführt.

Themen

Ansicht „Services-Konfiguration“ – Registerkarte „Datenschutz“

Auf der Registerkarte „Datenschutz“ (**ADMIN > Services > Wählen Sie einen Decoder oder Log Decoder >**  **> Konfiguration > Registerkarte Datenschutz)** können Administratoren Datenschutzparameter für bestimmte Core-Services konfigurieren. Für den Decoder und Log Decoder können Sie den Standard-Hashalgorithmus und das Salt einstellen.

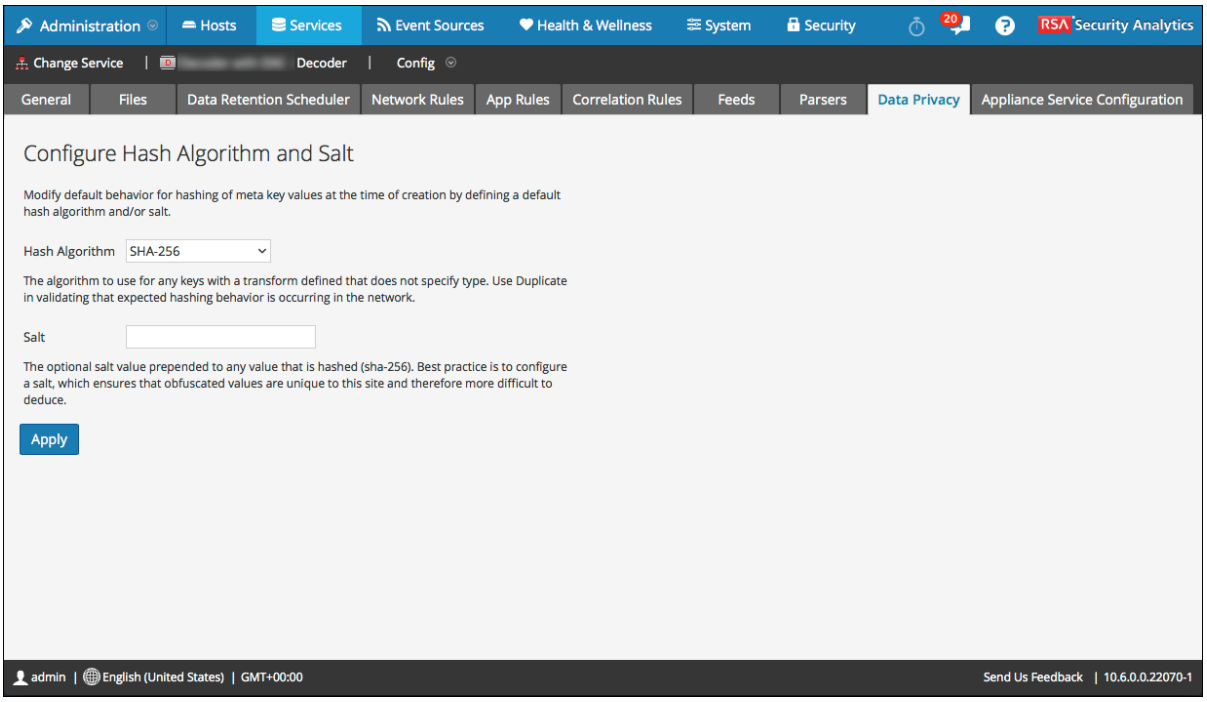
Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Administrator	Hashalgorithmus und Salt konfigurieren	„Konfigurieren von Hashalgorithmus und Salt“ im *Leitfaden Datenschutzmanagement.* (Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.)

Verwandte Themen

- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder

Überblick



Die Registerkarte „Datenschutz“ verfügt über die Konfigurationseinstellungen für den Hashalgorithmus und Salt. In der folgenden Tabelle werden die Parameter auf dieser Registerkarte beschrieben.

Parameter	Beschreibung
Hashalgorithmus	Zeigt eine Drop-down-Liste von Hashalgorithmen an, die für alle Schlüssel mit einer Umwandlung, in der kein Algorithmustyp angegeben wird, zu verwenden ist. Die möglichen Werte liegen zwischen SHA-256 und Duplicate. „Duplicate“ ist ein besonderer für Administratoren verfügbarer Algorithmus, mit dem sie überprüfen können, ob erwartetes Hashingverhalten im Netzwerk erfolgt. In Versionen von NetWitness Suite vor 10.5 war SHA-1 als Hash-Algorithmus verfügbar, aber RSA rät von der Verwendung von SHA-1 ab.

Parameter	Beschreibung
Salt	Gibt den optionalen Salt-Wert an, der gehashten Werten vorangestellt wird. Bewährte Vorgehensweisen für Sicherheitszwecke geben einen Salt-Wert vor, der nicht kleiner als 100 Bits oder 16 Zeichen lang ist. Die Konfiguration eines Wertes stellt sicher, dass verborgene Werte für diese Site eindeutig sind und sich somit schwerer herleiten lassen. Weitere Informationen über dieses Feld finden Sie unter „Konfigurieren der Datenverschleierung“ im *Leitfaden Datenschutzmanagement*.
Anwenden	Übernimmt alle Änderungen.

Ansicht „Services-Konfiguration“ – Datenaufbewahrungsplaner

Auf der Registerkarte „Datenaufbewahrungsplaner“ der Ansicht „Services-Konfiguration“ können Sie die Rollover-Kriterien für das Entfernen von Datenbankdatensätzen aus dem primären Speicher über einen altersbasierten Schwellenwert festlegen. Sie können auch festlegen, wann geprüft werden soll, ob der Schwellenwert erreicht wurde.

Um auf die Registerkarte „Datenaufbewahrungsplaner“ zuzugreifen, gehen Sie zu ADMIN > „Services“ > Wählen Sie einen Decoder- oder Log Decoder-Service und klicken Sie auf > „Ansicht“ > „Konfiguration“ > Registerkarte „Datenaufbewahrung“.

Was möchten Sie tun?

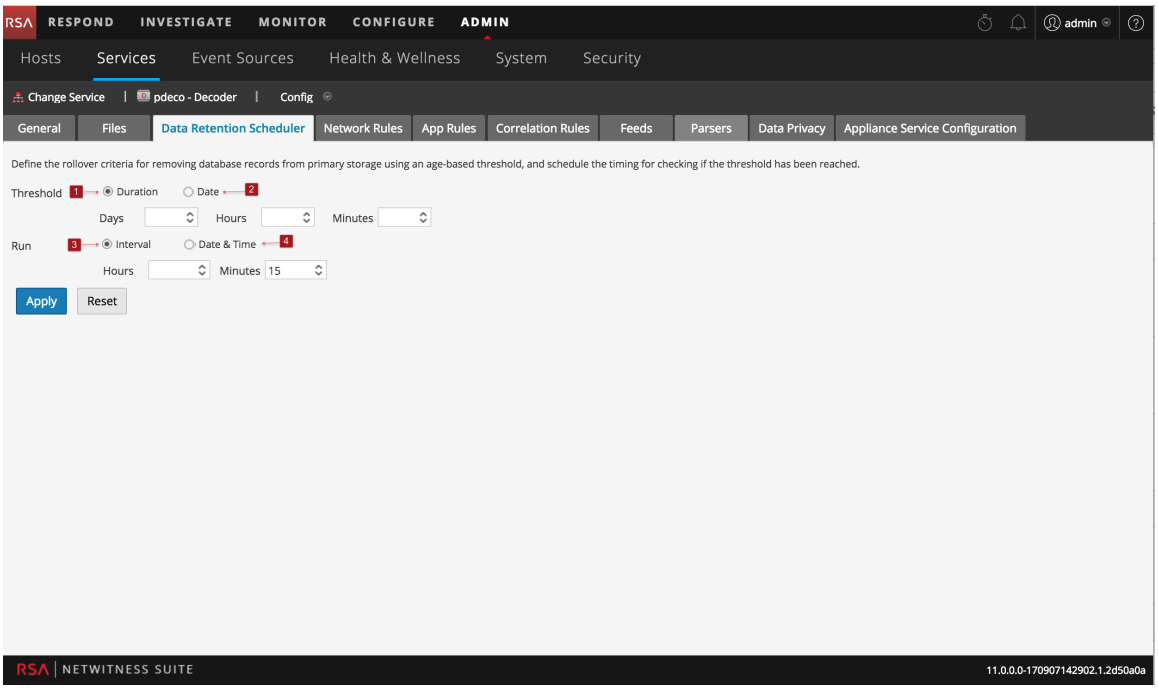
Benutzerrolle	Ziel	Dokumentation
Administrator	Planen, wann geprüft werden soll, ob der Schwellenwert erreicht wurde.	Konfigurieren der Transaktionsbehandlung auf einem Decoder

Verwandte Themen

- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Decoder und Log Decoder – Schnelleinrichtung

Überblick

Dies ist ein Beispiel für die Registerkarte „Datenaufbewahrungsplaner“.



1	**Schwellenwert-Dauer**: Entfernt Datenbankdateien, die älter sind als die ausgewählte Anzahl an Tagen, Minuten oder Stunden.
2	**Schwellenwert-Datum**: Entfernt Datenbankdateien, die älter als das angegebene UTC-Datum (JJJJ-MM-TT HH:MM:SS) und nicht kompatibel mit den Parametern für Minuten, Stunden oder Tage sind.
3	**Ausführungsintervall:** Gibt die Anzahl von Stunden zwischen den Ausführungen an.
4	**Datum und Uhrzeit der Ausführung**: Definiert, an welchen Wochentagen der Scheduler ausgeführt werden soll sowie die Zeit der Ausführung im Format HH:MM:SS für die lokale Uhrzeit des Services.

Ansicht „Services-Konfiguration“ – Registerkarte „Feeds“

Feeds und Parser sind Lua-Programme, die geladen und kompiliert werden, wenn entweder erfasste Daten in Ermittlungen verarbeitet oder Daten mit Decodern erfasst werden. Am häufigsten werden sie für die Extrahierung statischer Metadaten und zur Identifizierung von Services verwendet.

Hinweis: NetWitness-Versionen vor 11.0 verwendeten zusätzlich zu Lua-Programmen FLEXPARSE-Programme. Flexparsers sind in NetWitness Suite 11.0 veraltet. Wenn nicht anders angegeben, gilt jede Aussage über Decoder auch für Log Decoder.

NetWitness Suite verwendet Feeds, um Metadaten basierend auf extern definierten Metawerten zu erstellen. Ein Feed ist eine Liste von Daten, die bei der Erfassung oder Verarbeitung von Sitzungen mit diesen abgeglichen werden. Für jeden Treffer werden zusätzliche Metadaten erstellt. Diese Daten können schadhafte IPs erkennen und klassifizieren oder zusätzliche Informationen mit einbeziehen, wie etwa Abteilung und Standort, basierend auf internen Netzwerkzuordnungen. Einige Beispiele für Feeds sind Bedrohungsfeeds zur Identifizierung von BOTNets, DHCP-Zuordnungen oder auch Active Directory-Informationen wie physischer Standort oder logische Abteilung.

Feeds können hinzugefügt, entfernt und aktualisiert werden, während ein Decoder ausgeführt wird, ohne die Erfassung zu beeinträchtigen. Die Registerkarte „Feeds“ (**ADMIN > Services >** wählen Sie einen Service aus und klicken Sie auf  **> Ansicht > Konfiguration > Feeds**) stellt eine Benutzeroberfläche für das Managen von Feeds auf Decodern bereit.

Was möchten Sie tun?

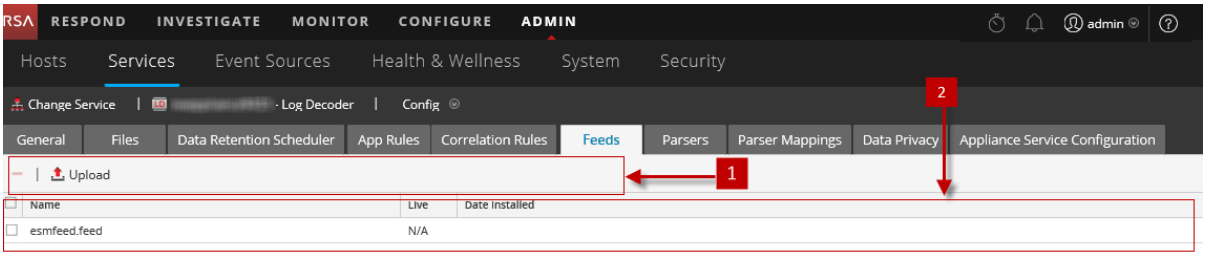
Benutzerrolle	Ziel	Dokumentation
Administrator	Konfigurieren von Feeds	Konfigurieren von Feeds und Parsern
Administrator	Protokollparser aktivieren und deaktivieren	Aktivieren und Deaktivieren von Parsern und Protokollparsern

Verwandte Themen

- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Decoder und Log Decoder – Schnelleinrichtung
- Dialogfeld Feeds hochladen
- Feed- und Parser-Referenzen

Überblick

Dies ist ein Beispiel für die Registerkarte Feeds.



1 Symbolleiste der Registerkarte „Feeds“ – bietet Optionen zur Arbeit mit Feeds im Raster

2 Feedraster – Listet alle Feeds auf, die gegenwärtig auf dem Decoder bereitgestellt sind

Symbolleiste der Registerkarte „Feeds“

Funktion	Beschreibung
Upload	Zeigt das Dialogfeld „Feeds hochladen“ an.
−	Löscht die ausgewählten Feeds.

Liste der Feeds

Die Liste der Feeds bietet eine Auflistung aller gegenwärtig bereitgestellten Feeds für den Decoder.

Spalte	Beschreibung
Name	Der Name des Feeds oder der Feeddatei.

Spalte	Beschreibung
Live	Zeigt an, ob der Feed von Live stammt. Mögliche Werte sind **Ja**, **Nein** oder **N/A**. • **Ja** = Installiert über Live • **Nein** = Installiert über NetWitness Suite • **N/A** = Der Feed hat keine von NetWitness Suite erstellte Attributdatei, um das Installationsdatum nachzuverfolgen. Der Feed wurde möglicherweise manuell installiert, nicht über NetWitness Suite oder Live-Services. Manuell installierte Feeds arbeiten weiterhin korrekt.
Installationsdatum	Das Datum des Feeds wurde per Push auf den Service übertragen.

Dialogfeld Feeds hochladen

Dieses Thema beschreibt die Funktionen des Dialogfelds „Feeds hochladen“ in der Ansicht „Services-Konfiguration“ > Registerkarte „Feeds“.

Mit der Option **Hochladen** auf der Registerkarte „Feeds“ der Ansicht „Services-Konfiguration“ wird das Dialogfeld „Feeds hochladen“ angezeigt, in dem Sie das Hochladen von Feeds auf einen Decoder oder Log Decoder managen können.

Was möchten Sie tun?

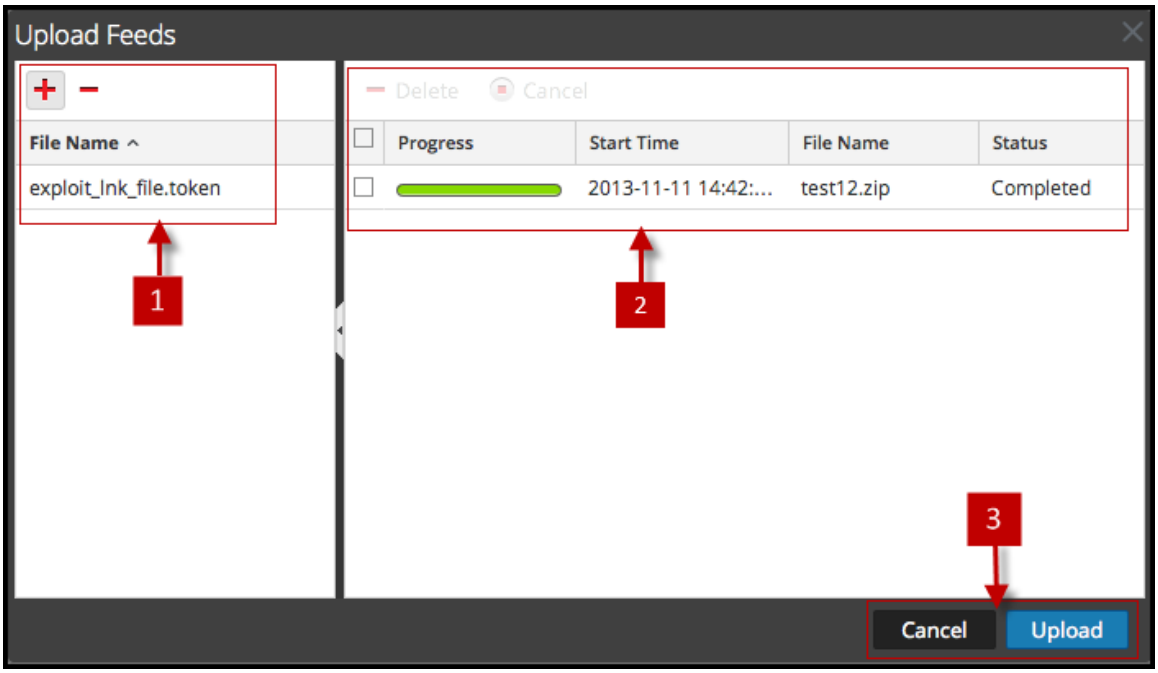
Benutzerrolle	Ziel	Dokumentation
Administrator	Eine Liste von Feeds für das Hochladen vorbereiten	Hochladen, Bearbeiten oder Entfernen eines Feeds
Administrator	Hochladejobs anzeigen und löschen	Hochladen, Bearbeiten oder Entfernen eines Feeds

Verwandte Themen

- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Feed- und Parser-Referenzen

Überblick

Dies ist ein Beispiel für das Dialogfeld „Feeds hochladen“.



1 Liste „Datei“ – ermöglicht das Erstellen einer Liste von Feeds für das Hochladen

2 Liste „Hochladejobs“ – bietet eine Ansicht der Hochladejobs

3 Schaltflächen des Dialogfelds „Feeds hochladen“

Dateiliste

In der Liste „Datei“ kann eine Liste der Feeds für das Hochladen erstellt werden. Sie können Dateien aus einer Verzeichnisstruktur hinzufügen und Dateien aus dem Raster löschen, wenn Sie entscheiden, dass Sie eine spezifische Datei nicht hochladen möchten. Wenn die Liste bereit ist, wird durch Klicken auf **Hochladen** der Hochladeprozess gestartet.

Funktion	Beschreibung
+	Öffnet eine Ansicht der Verzeichnisstruktur, aus der Sie Dateien für das Hinzufügen zur Liste „Datei“ auswählen können.
−	Löscht die ausgewählten Dateien aus der Liste „Datei“.
Dateiname	Listet die Feed-Dateien auf, die Sie von einem Dateisystem, das gerade zum Hochladen vorbereitet wird, zu einem Decoder hinzugefügt haben. Wenn Sie auf **Hochladen** klicken, werden die hier aufgelisteten Dateien hochgeladen.

Liste „Hochladejob“

Die Liste „Hochladejob“ bietet eine Ansicht der Hochladejobs, die durch das Anklicken von **Hochladen** gestartet werden.

Funktion/Spalte	Beschreibung
	Löscht einen Hochladejob.
Fortschritt	Zeigt den Fortschritt eines Hochladejobs an
Startzeit	Zeigt die Startzeit eines Hochladejobs an
Dateiname	Listet den Dateinamen des Feeds auf, der gerade hochgeladen wird
Status	Zeigt den Status eines Hochladejobs an

Schaltflächen des Dialogfelds „Feeds hochladen“

Funktion	Beschreibung
Abbrechen	Schließt das Dialogfeld „Feeds hochladen“.
Hochladen	Startet das Hochladen der in der Liste „Datei“ aufgeführten Feeddateien. Jeder Feed ist in einer separaten Zeile in der Liste „Hochladeprozess“ aufgelistet.

Ansicht „Services-Konfiguration“ – Registerkarte „Dateien“

Die Decoder- und Log Decoder-Konfigurationsdateien können in der Ansicht „Services-Konfiguration“ > Registerkarte „Dateien“ angezeigt und bearbeitet werden. Unter „Bearbeiten von Core-Service-Konfigurationsdateien“ im *Leitfaden für die ersten Schritte mit Hosts und Services* finden Sie allgemeine Anweisungen zum Bearbeiten von Dateien. (Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.)

Wie andere Core-Services verfügen auch Decoder und Log Decoder über eine Indexdatei. Außerdem kann es eine Crashreporter-, Netwitness- und Scheduler-Datei geben. Die Decoder- und Log Decoder-Indexdateien heißen **`index-decoder-custom.xml`** und **`index-logdecoder-custom.xml`**.

Hinweis: Dieser Dateityp ist nur für Log Decoder mit installiertem Envision-Inhalt verfügbar. `Table-map.xml` und `table-map-custom.xml` werden jetzt angezeigt, aber nur, wenn `table-map.xml` auf dem Dateisystem gefunden wurde (z. B. kann es sich um einen Log Decoder mit installiertem Envision-Inhalt handeln).

Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Administrator	Protokolldateien von Log Decoder-Versionen vor 11.0 abrufen	Abrufen von Protokolldateien von Log Decoder-Versionen vor 11.0
Administrator	Dateien und Parser bearbeiten	Feed- und Parser-Referenzen

Verwandte Themen

- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Decoder und Log Decoder – Schnelleinrichtung
- Erstellen benutzerdefinierter Metaschlüssel mithilfe benutzerdefinierter Feeds

Überblick

Dateiname	Beschreibung
`GeoPrivate.ipl`	Dieser feste Parser konvertiert die IP-Adressen in geografische Standorte. Die Standorte werden über die Google Earth-Anzeige angezeigt.
`feed-definitions.xml`	Erstellt benutzerdefinierte Feeds. Dies ist das vom Decoder bei der Erstellung einer **.feed**-Datei zur Definition einer **Feednachricht** verwendete XML-Schema.
`traffic_flow_options.lua`	Verwendet, um Richtungsinformationen bereitzustellen. Aktualisieren Sie diese Datei mit umgebungsspezifischen internen und externen Subnetzen, damit der Lua-Parser die korrekte Richtung in den Metadaten erstellen kann. Der Parser wird unter RSA Content für die RSA NetWitness Suite beschrieben.
`search.ini`	Dies ist die Konfigurationsdatei des Such-Parsers. Der Such-Parser ist ein benutzerdefinierter Parser, der Metadaten generiert, indem er nach vordefinierten Schlüsselwörtern und regulären Ausdrücken sucht.
`wlan-config.xml`	Dies ist die WLAN-Konfigurationsdatei (9.9.2009). Diese Datei steuert die 802.11-Parser. Ihr Hauptzweck besteht darin, die Entschlüsselung unverarbeiteter 802.11-Frames zu steuern, die vom Decoder erfasst werden.

Ansicht „Services-Konfiguration“ – Registerkarte „Allgemein“

Die Registerkarte „Allgemein“ für einen Decoder in der Ansicht „Services-Konfiguration“ bietet eine Möglichkeit, die grundlegende Servicekonfiguration zu managen, die Datenerfassung zu konfigurieren und die Parser auszuwählen, die auf die erfassten Daten angewendet werden. Um auf die Registerkarte „Allgemein“ zuzugreifen, gehen Sie zu **ADMIN > Services >** wählen Sie einen Decoder oder Log Decoder aus und klicken Sie auf  **> Ansicht > Konfiguration > Registerkarte „Allgemein“**.

Workflow

Die folgende Abbildung zeigt allgemeine Decoder-Konfigurationsaufgaben. Die Schritte, die in dieser Ansicht durchgeführt werden können, sind hervorgehoben.

Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Administrator	Konfigurieren von Erfassungseinstellungen*	Konfigurieren von Erfassungseinstellungen
Administrator	Managen von Parsern und Protokollparsern*	Aktivieren und Deaktivieren von Parsern und Protokollparsern
Administrator	Datenerfassung starten und beenden	Starten und Beenden der Datenerfassung
Administrator	Konfigurieren von Regeln	Konfigurieren von Decoder-Regeln

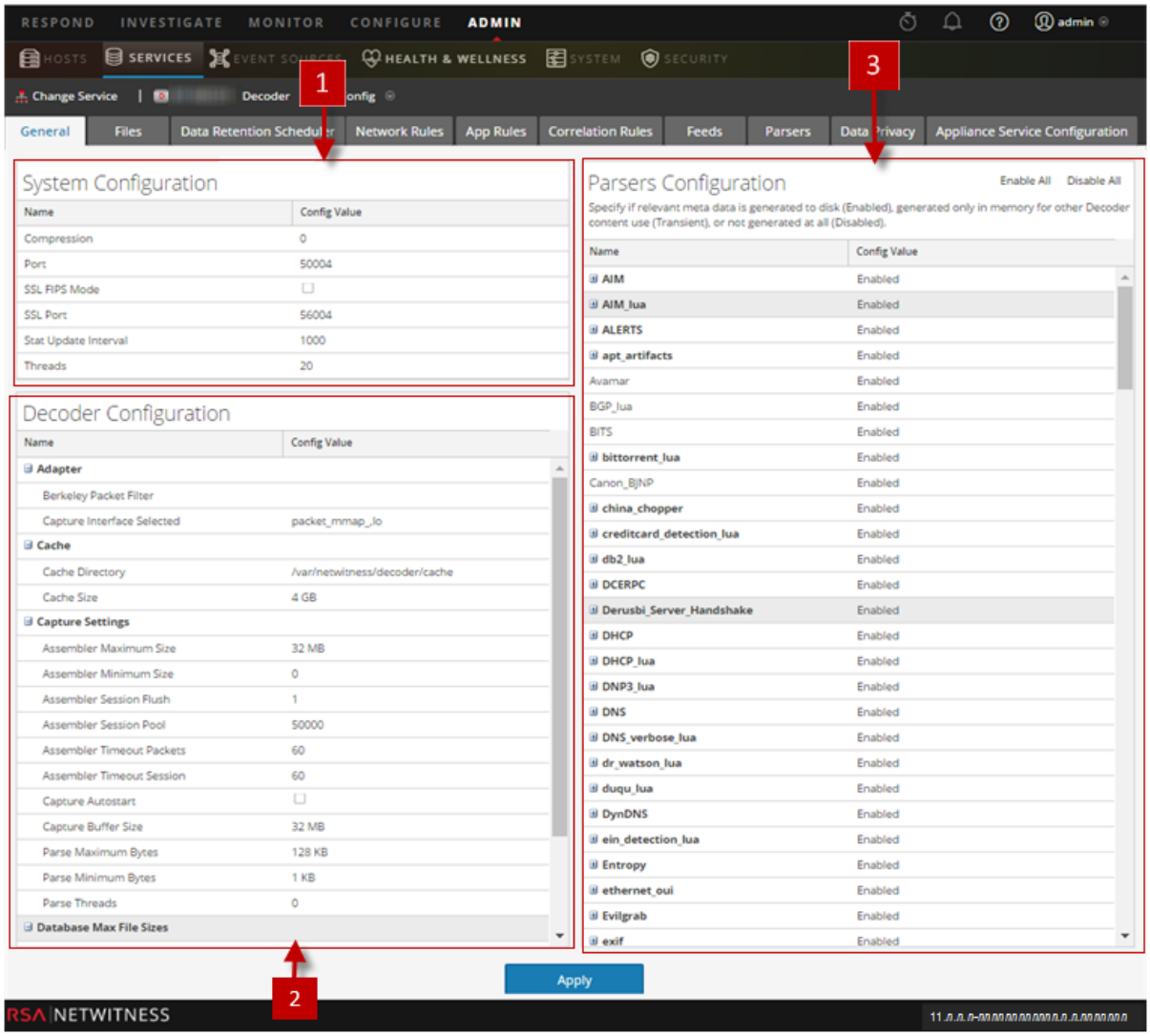
*Sie können diese Aufgaben hier durchführen.

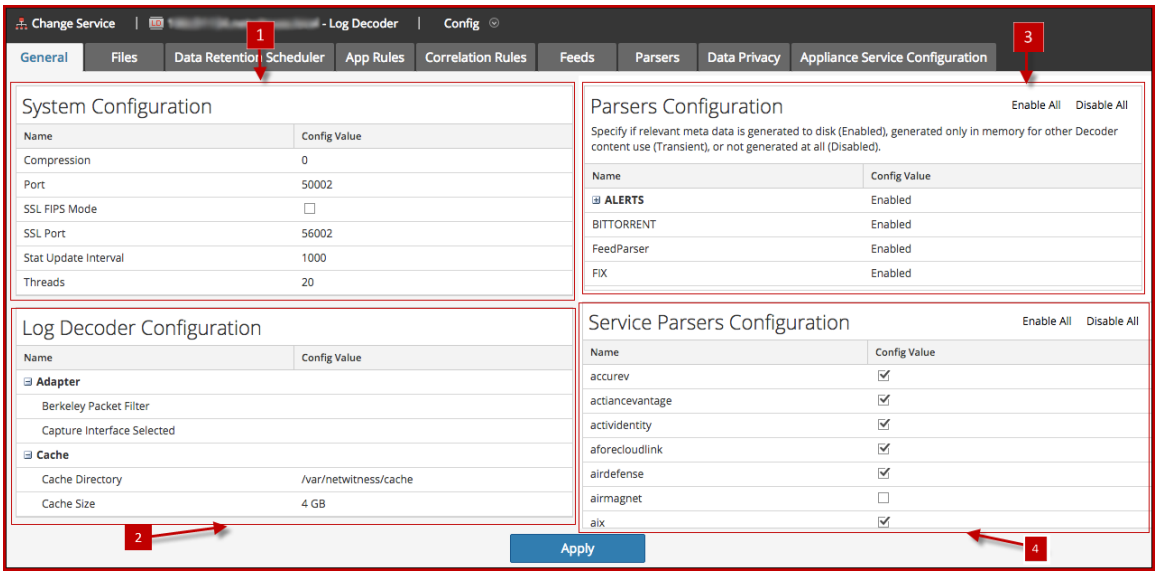
Verwandte Themen

- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Konfigurieren von Feeds und Parsern

Überblick

Die erste Abbildung ist ein Beispiel für die Registerkarte „Allgemein“ für einen Decoder. Die zweite ist die Registerkarte „Allgemein“ für einen Log Decoder.

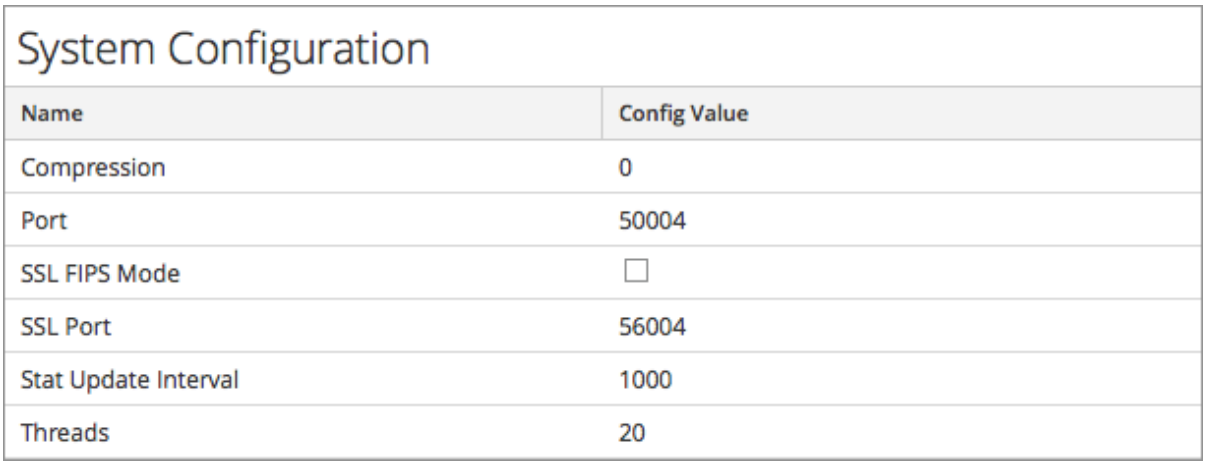




1	Systemkonfiguration – Managt die Servicekonfiguration für einen Decoder.
2	Konfiguration für Decoder oder Konfiguration für Log Decoder – Ermöglicht Ihnen das Anzeigen und Bearbeiten von Servicekonfigurationsparametern für einen Decoder oder Log Decoder.
3	Parserkonfiguration – Ermöglicht Ihnen die Auswahl von auf dem Decoder zu verwendenden Parsern.
4	Serviceparserkonfiguration (nur Log Decoders) – Ermöglicht Ihnen die Auswahl von auf dem Log Decoder zu verwendenden Serviceparsern.

Abschnitt Systemkonfiguration

Der Abschnitt „Systemkonfiguration“ managt die Servicekonfiguration für einen Decoder. Wenn ein Service zum ersten Mal hinzugefügt wird, werden Standardwerte festgelegt, die nur unter besonderen Umständen geändert werden dürfen, beispielsweise dann, wenn der Kundensupport Sie anweist, eine Änderung vorzunehmen.



System Configuration

Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	☐
SSL Port	56004
Stat Update Interval	1000
Threads	20

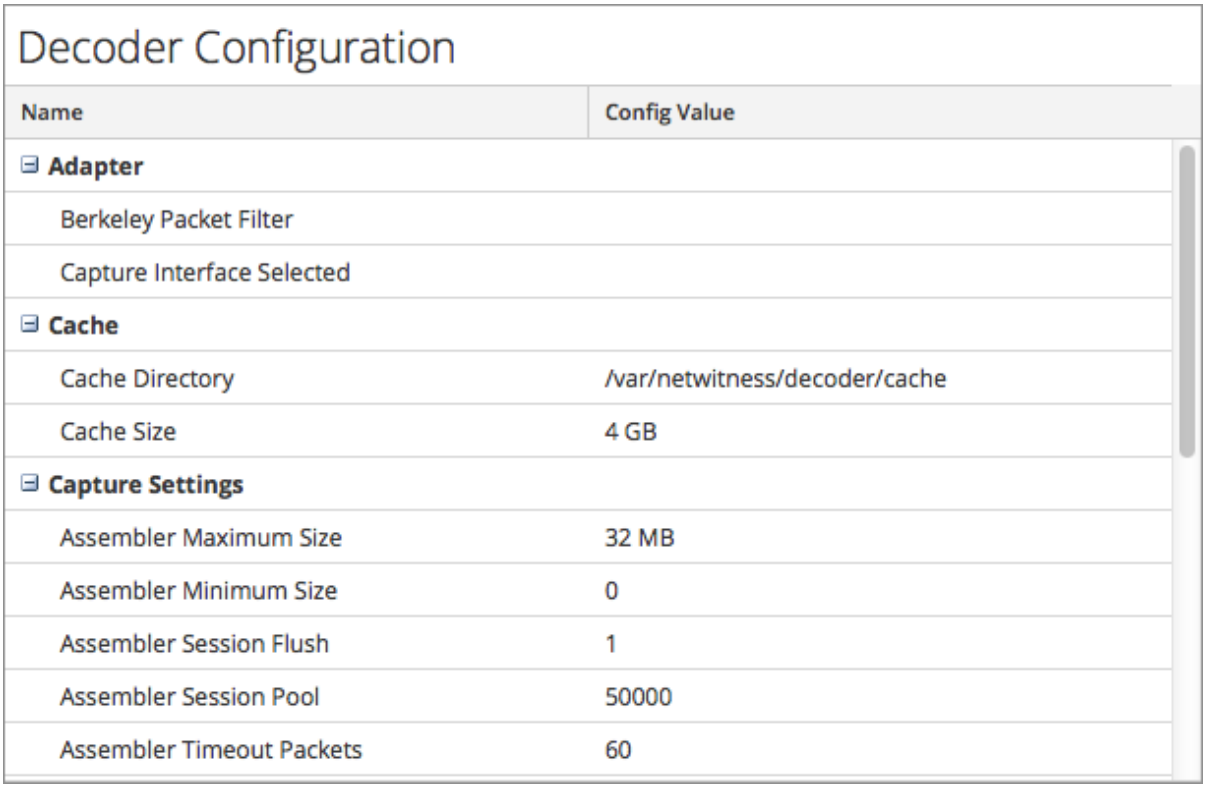
Der Abschnitt Systemkonfiguration enthält diese Parameter.

Parameter	Beschreibung
Komprimierung	Die Mindestanzahl Byte, die pro Antwort vor der Komprimierung übertragen werden muss. Die Einstellung 0 deaktiviert die Komprimierung. Der Standardwert ist **0**. Eine Veränderung des Werts ist sofort für alle nachfolgenden Verbindungen wirksam.
Port	Bestimmt den Port, den der Service verwendet. **Hinweis:** Wenn Sie die Portnummer ändern, müssen Sie den Service neu starten.
SSL FIPS-Modus	Wenn diese Option aktiviert ist, werden alle Daten, die in das Netzwerk übertragen werden, mithilfe von SSL verschlüsselt.
SSL-Port	Gibt den Port an, der zur Verschlüsselung mithilfe von SSL verwendet wird.

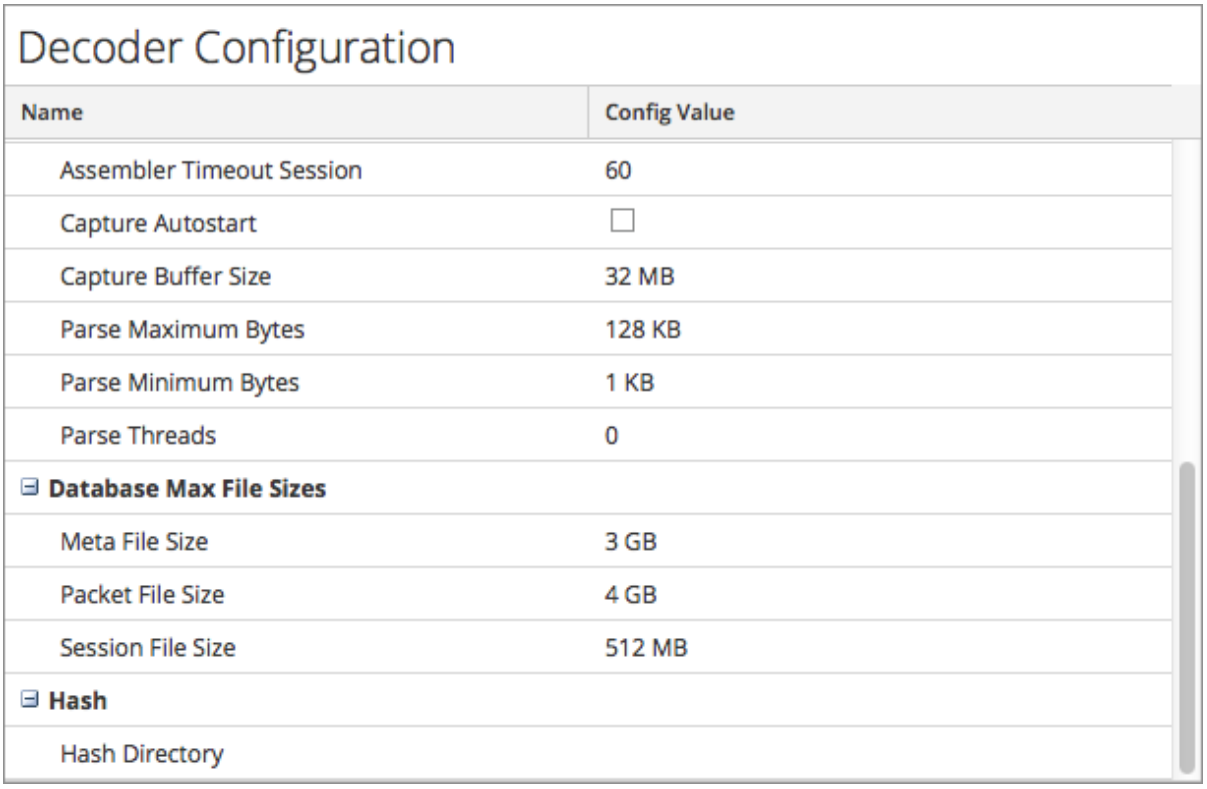
Parameter	Beschreibung
Statistikaktualisierungsintervall	Die Anzahl der Millisekunden zwischen Statistikaktualisierungen auf dem System. Niedrigere Zahlen führen zu häufigeren Aktualisierungen und können andere Prozesse verlangsamen. Der Standardwert ist **1000**. Eine Änderung des Werts ist sofort wirksam.
Threads	Die Anzahl der Threads im Threadpool für die Verarbeitung eingehender Anforderungen. Bei der Einstellung **0** wird es vom System entschieden. Die Änderung wirkt sich beim Serviceneustart aus.

Abschnitt Decoderkonfiguration

Im Abschnitt Decoder-Konfiguration können die Servicekonfigurationsparameter für einen Decoder oder Log Decoder angezeigt und bearbeitet werden. Wenn ein Service zum ersten Mal hinzugefügt wird, sind Standardwerte wirksam. Sie können diese Werte bearbeiten, um die Erfassung des Datenverkehrs zu managen.



Wenn Sie ans Ende dieses Abschnitts scrollen, sehen Sie diese zusätzlichen Decoderkonfigurationsparameter.



Abschnitt „Adapter“

Adapter-Parameter konfigurieren die Netzwerkschnittstelle für die Erfassung wie unter Konfigurieren von Erfassungseinstellungen beschrieben.

Abschnitt „Cache“

Cacheparameter konfigurieren das Cacheverzeichnis und die Größe für Sitzungs-Cachedateien. In der folgenden Tabelle sind die Cacheeinstellungen beschrieben. Wenn ein Service zum ersten Mal hinzugefügt wird, werden Standardwerte festgelegt, die nur unter besonderen Umständen geändert werden dürfen, beispielsweise dann, wenn der Kundensupport Sie anweist, eine Änderung vorzunehmen.

Cacheparameter	Beschreibung
Cacheverzeichnis	Das Verzeichnis, in dem Cachedateien der Sitzung gespeichert werden. Der Standardwert ist `/var/netwitness/decoder/cache`. Die Änderung wird sofort wirksam.

Cacheparameter	Beschreibung
Cachegröße	Die maximale Größe, in Megabyte (MB), die alle Dateien im Cacheverzeichnis erreichen können, bevor die ältesten Dateien gelöscht werden. Sobald der Schwellenwert erreicht ist, wird die Cachegröße um 10 % reduziert. Der Standardwert ist **4 GB**. Die Änderung wird sofort wirksam.

Abschnitt „Einstellungen erfassen“

Im Abschnitt „Einstellungen erfassen“ können Sie die Einstellungen für den Erfassungsvorgang konfigurieren. Wenn ein Service zum ersten Mal hinzugefügt wird, werden Standardwerte festgelegt, die nur unter besonderen Umständen geändert werden dürfen, beispielsweise dann, wenn der Kundensupport Sie anweist, eine Änderung vorzunehmen.

Erfassungseinstellungsparameter	Beschreibung
Maximale Größe des Assemblers	Gibt die maximale Größe in Byte an, die die Paketdaten einer Sitzung erreichen können. Der Standardwert ist **32 MB**. Die Änderung wird sofort wirksam.
Minimale Größe des Assemblers	Gibt die minimale Größe in Byte an, die eine Sitzung haben muss, um Metadaten erzeugen zu können. Ein Wert von **0** bedeutet, dass jede Sitzung Metadaten erzeugt hat. Der Standardwert ist **0**. Die Änderung wird sofort wirksam.

Erfassungseinstellungsparameter	Beschreibung
Leeren der Assembler-Sitzung	Gibt an, ob eine Sitzung vom Assembler entfernt wird, wenn die letzte Kette der Sitzung vom Assembler entfernt wurde. Der Standardwert ist **1**. • **2** = wenn das erste Paket einer Sitzung im Assembler abläuft, wird die Sitzung vom Assembler entfernt, nachdem das Parsen abgeschlossen wurde. Alle nachfolgenden Pakete für diese Sitzung erstellen eine neue Sitzung im Assembler. • **1** = Wenn die letzte Kette einer Sitzung im Assembler abläuft, wird die Sitzung aus dem Assembler entfernt. Alle nachfolgenden Pakete für diese Sitzung erstellen eine neue Sitzung im Assembler. • **0** = wenn die letzte Kette einer Sitzung im Assembler abläuft, bleibt die Sitzung im Assembler, bis sie abläuft. Alle nachfolgenden Pakete für diese Sitzung werden gefiltert. Die Änderung wirkt sich beim Serviceneustart aus.
Assembler-Sitzungspool	Gibt die Anzahl der Einträge im Sitzungspool an. Der Standardwert ist **350000**. Die Änderung wirkt sich beim Serviceneustart aus.
Assembler-Timeout-Pakete	Gibt die Anzahl der Sekunden an, bevor ein Paket oder eine Kette abläuft. Der Standardwert ist **60**. Die Änderung wird sofort wirksam.

Erfassungseinstellungsparameter	Beschreibung
Assembler-Timeout-Sitzung	Gibt die Anzahl der Sekunden an, bevor eine Sitzung abläuft. Der Standardwert ist **60**. Die Änderung wird sofort wirksam.
Erfassung-Autostart	Gibt an, ob die Erfassung jedes Mal automatisch beginnt, wenn Decoder gestartet wird. Wenn die Option aktiviert ist, ist der Wert = Ja. Wenn sie nicht aktiviert ist, ist der Wert = Nein. Der Standardwert ist **Nein**. Die Änderung wird sofort wirksam.
Erfassungspuffergröße	Die Pufferzuweisung des Erfassungsspeichers in Megabyte. Der Standardwert ist **64 MB**. Die Änderung wirkt sich beim Serviceneustart aus.
Maximale Anzahl Byte parsen	Die maximale Anzahl zu scannender Byte eines Streams für zusätzliche Token. Wenn der erste Token gefunden wird, wird der Stream bis zu der eingestellten Anzahl Byte gescannt, aber nicht weiter. Bei einer Einstellung von **0** wird die frühzeitige Beendigung entfernt und der gesamte Stream wird unabhängig von seiner Größe gescannt. Der Standardwert ist **128 KB**. Die Änderung wird sofort wirksam.

Erfassungseinstellungsparameter	Beschreibung
Minimale Anzahl Byte parsen	Die minimale Anzahl zu scannender Byte eines Streams für das erste Token. Wenn innerhalb der eingestellten Anzahl von Byte kein Token gefunden wird, wird das Scannen beendet. Bei einer Einstellung von **0** wird die frühzeitige Beendigung entfernt und der gesamte Stream wird unabhängig von seiner Größe gescannt. Der Standardwert ist **1 KB**. Die Änderung wird sofort wirksam.
Parse-Threads	Die Anzahl der für das Sitzungs-Parsing verwendeten Parser-Threads Ein Wert **0** bedeutet, dass der Server entscheidet. Der Standardwert ist **0**. Die Änderung wirkt sich beim Serviceneustart aus.

Abschnitt „Maximale Datenbankdateigrößen“

Der Abschnitt „Maximale Datenbankdateigrößen“ legt die maximale Dateigröße verschiedener Datenbanken fest. Wenn ein Service zum ersten Mal hinzugefügt wird, werden Standardwerte festgelegt, die nur unter besonderen Umständen geändert werden dürfen, beispielsweise dann, wenn der Kundensupport Sie anweist, eine Änderung vorzunehmen.

Dateigrößenparameter	Beschreibung
Metadatendateigröße	Die maximale Größe der Metadatenbankdateien in Megabyte Der Standardwert ist **10 MB**. Die Änderung wirkt sich beim Serviceneustart aus.
Paketdateigröße	Die maximale Größe der Paketdatenbankdateien in Megabyte Der Standardwert ist **10 MB**. Die Änderung wirkt sich beim Serviceneustart aus.
Sitzungsdateigröße	Die maximale Größe der Sitzungsdatenbankdateien in Megabyte Der Standardwert ist **100 MB**. Die Änderung wirkt sich beim Serviceneustart aus.

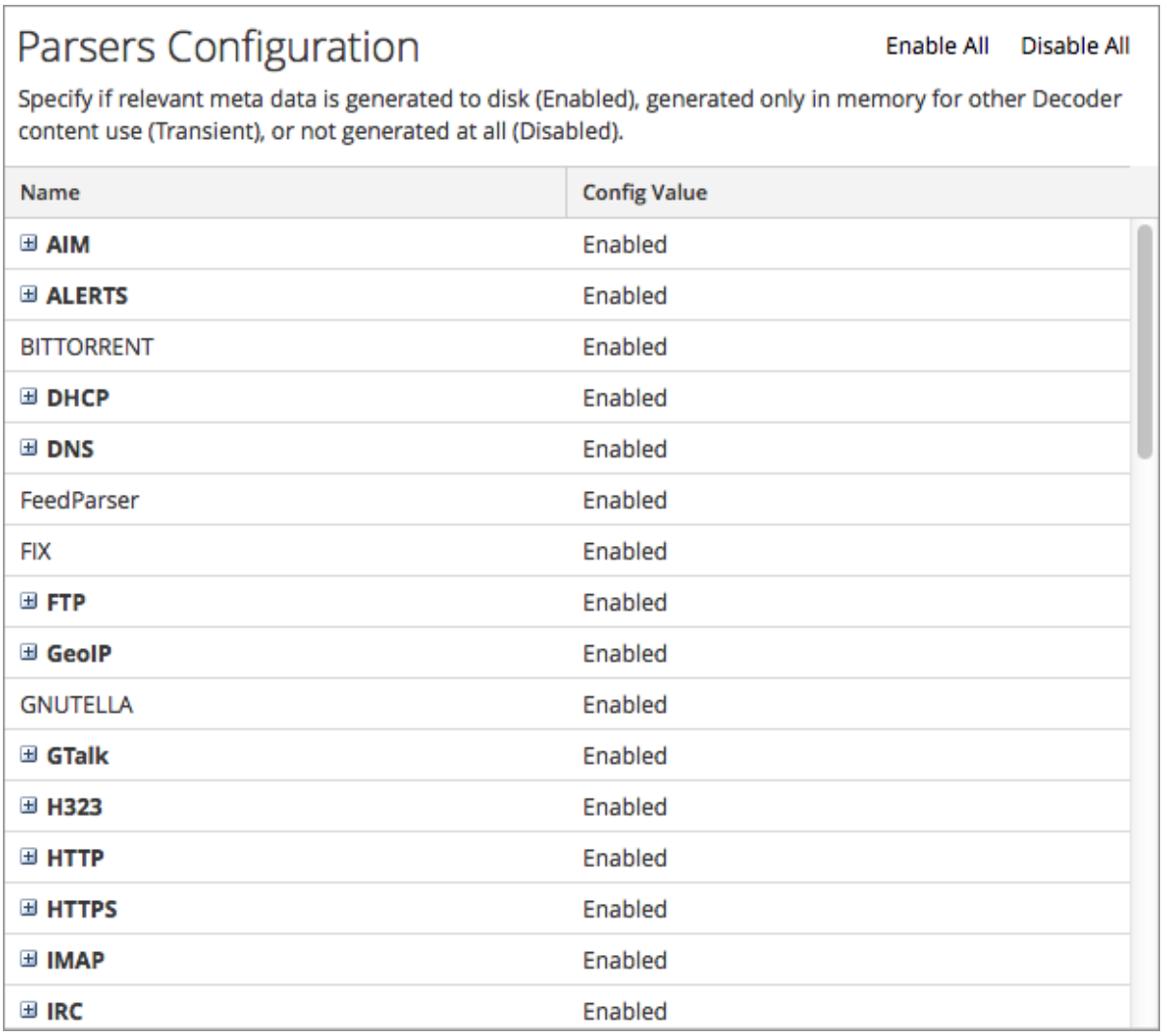
Abschnitt „Hash“

Die Einstellungen für den Abschnitt „Hash“ steuern Hashing-Optionen für Datenbankdateien. Beim Hashing tritt eine geringe Performanceverschlechterung auf.

Hash-Parameter	Beschreibung
Hash-Verzeichnis	Das Serververzeichnis, in das alle Hash-Dateien geschrieben werden Wenn es leer ist, wird jede Hash-Datei in dasselbe Verzeichnis geschrieben wie die gehashte Datei. Der Standardwert ist leer. Die Änderung wirkt sich beim Serviceneustart aus.

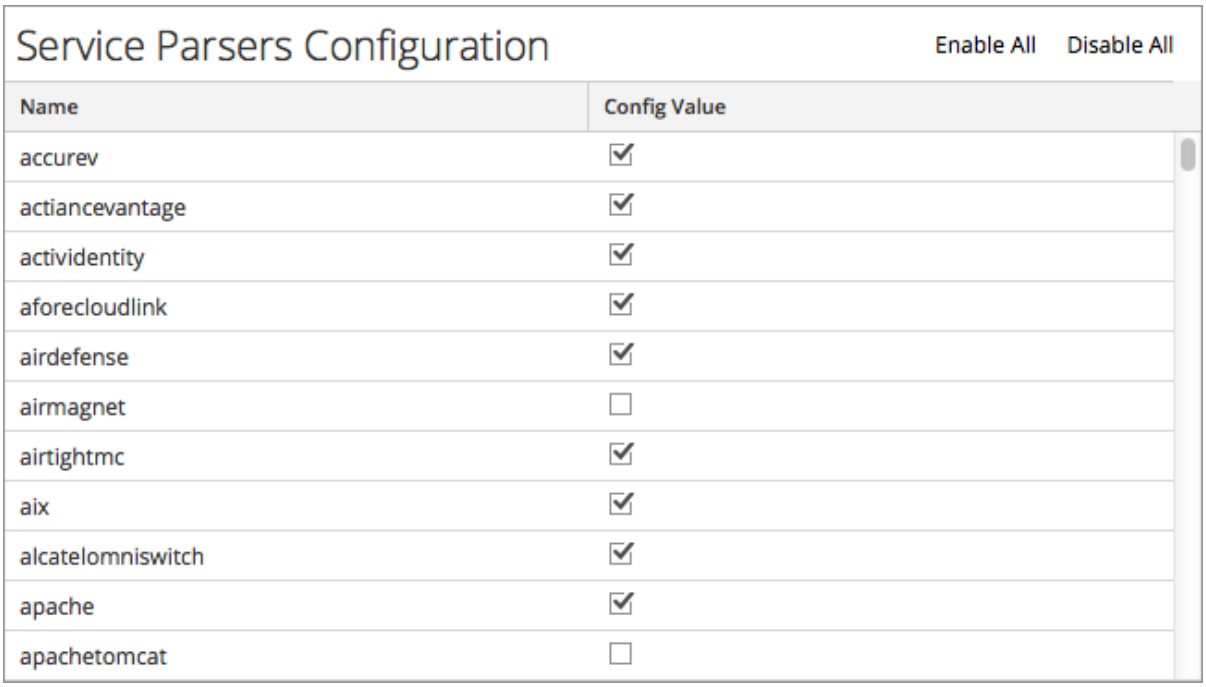
Bereich „Parserkonfiguration“

Der Bereich „Parserkonfiguration“ bietet eine Möglichkeit zur Auswahl des auf dem Decoder zu verwendenden Parsers. Innerhalb einiger Parser können Sie auch die Metadaten konfigurieren, die der Parser erstellt. Detaillierte Informationen und Verfahren finden Sie unter Aktivieren und Deaktivieren von Parsern und Protokollparsern.



Abschnitt „Serviceparserkonfiguration“ für Log Decoder

Im Abschnitt „Serviceparserkonfiguration“ können Sie Serviceparser zur Verwendung auf dem Log Decoder auswählen.



Ansicht „Services-Konfiguration“ – Registerkarte „Parser“

In der Ansicht „Services-Konfiguration“ > Registerkarte „Parser“ können Sie bereitgestellte Parser in einem Decoder oder Log Decoder anzeigen, Parser hochladen und bereitgestellte Parser löschen. Parser können hinzugefügt und entfernt werden, während ein Decoder oder Log Decoder ausgeführt wird, ohne die Erfassung zu beeinträchtigen.

Um auf die Registerkarte „Parser“ zuzugreifen, gehen Sie zu ADMIN > Services > wählen Sie einen Decoder- oder Log Decoder-Service aus und klicken Sie auf > Ansicht > Konfiguration > Registerkarte „Parser“.

Was möchten Sie tun?

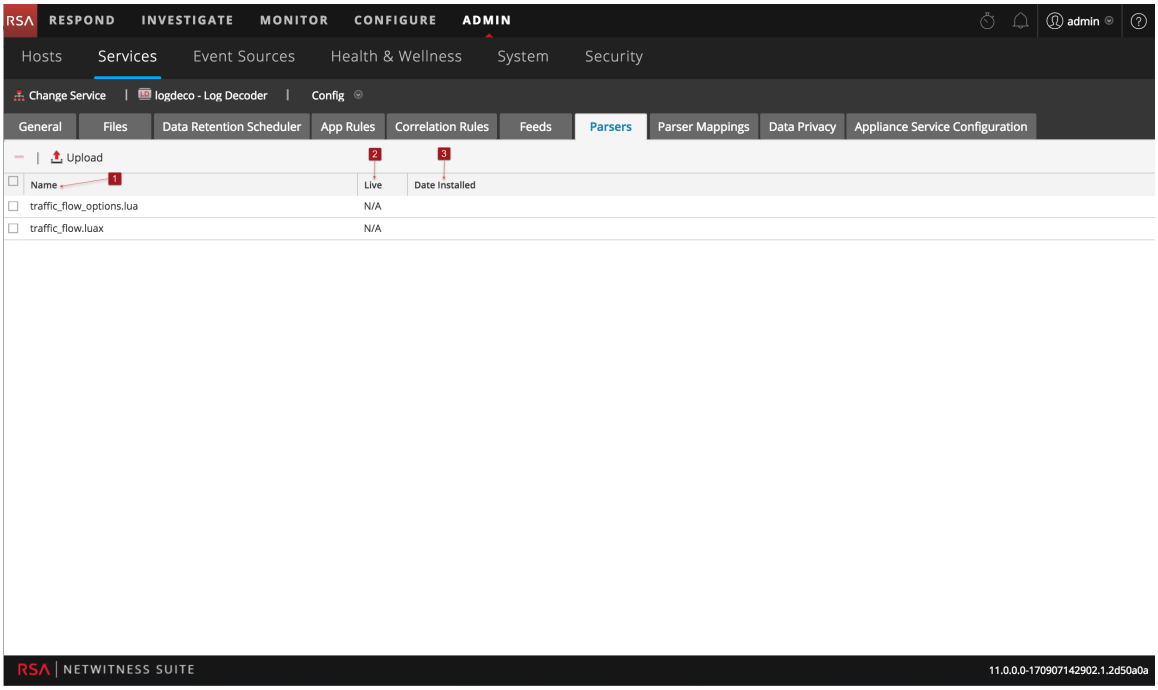
Benutzerrolle	Ziel	Dokumentation
Administrator	Bereitgestellte Parser anzeigen.	Aktivieren und Deaktivieren von Parsern und Protokollparsern
Administrator	Parser zu einem Decoder oder Log Decoder hochladen.	Aktivieren und Deaktivieren von Parsern und Protokollparsern

Verwandte Themen

- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Hochladen und Löschen benutzerdefinierter Parser

Überblick

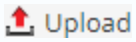
Dies ist ein Beispiel für die Registerkarte „Parser“. Im Raster „Parser“ werden alle Parser aufgeführt, die aktuell auf dem Decoder bereitgestellt sind.



1	**Name**: Der Name des Parsers oder der Parserdatei.
2	**Live**: Gibt an, ob der Parser von Live stammt. Mögliche Werte sind **Ja**, **Nein** oder **N/A**. • **Ja** = Installiert über Live-Services. • **Nein** = Installiert über NetWitness. • **N/A** = Der Parser hat keine von NetWitness erstellte Attributdatei, um das Installationsdatum nachzuverfolgen. Der Parser wurde möglicherweise manuell installiert, nicht über NetWitness oder Live-Services.
3	**Installationsdatum**: Das Datum, an dem der Parser an den Service übergeben wurde.

Symbolleiste auf der Registerkarte „Parser“

Die Symbolleiste auf der Registerkarte „Parser“ enthält Optionen für die Arbeit mit Parsern im Raster.

Funktion	Beschreibung
	Ermöglich das Hochladen von Parsern zu einem Decoder oder Log Decoder.
	Fordert Ihre Bestätigung an, dass die ausgewählten Parser gelöscht werden sollen. Wenn Sie **Nein** auswählen, wird der Löschvorgang abgebrochen. Klicken Sie auf **Ja**, um die ausgewählten Parser zu löschen.

Ansicht „Service-Konfiguration“ – Registerkarte „Parser-Zuordnungen“

In diesem Thema werden die konfigurierbaren Optionen für einen Log Decoder auf der Registerkarte „Parser-Zuordnungen“ beschrieben.

Auf der Registerkarte „Parser-Zuordnungen“ können Administratoren Protokollparserzuordnungen für Log Decoder-Services konfigurieren. Um auf die Registerkarte „Parser-Zuordnungen“ zuzugreifen, gehen Sie zu ADMIN > „Services“ > wählen Sie einen Service aus und klicken Sie auf  > Ansicht > Konfiguration > Registerkarte „Parser-Zuordnungen“.

Hinweis: Sie können auch Protokoll-Parser-Zuordnungen für Log Decoder-Services konfigurieren, indem Sie zu **ADMIN > Services > Ereignisquellen > Discovery** navigieren.

Mit dieser Funktion wird ein Teil der Ereignisquellen nachverfolgt, die mit dem falschen Parser analysiert werden.

Was möchten Sie tun?

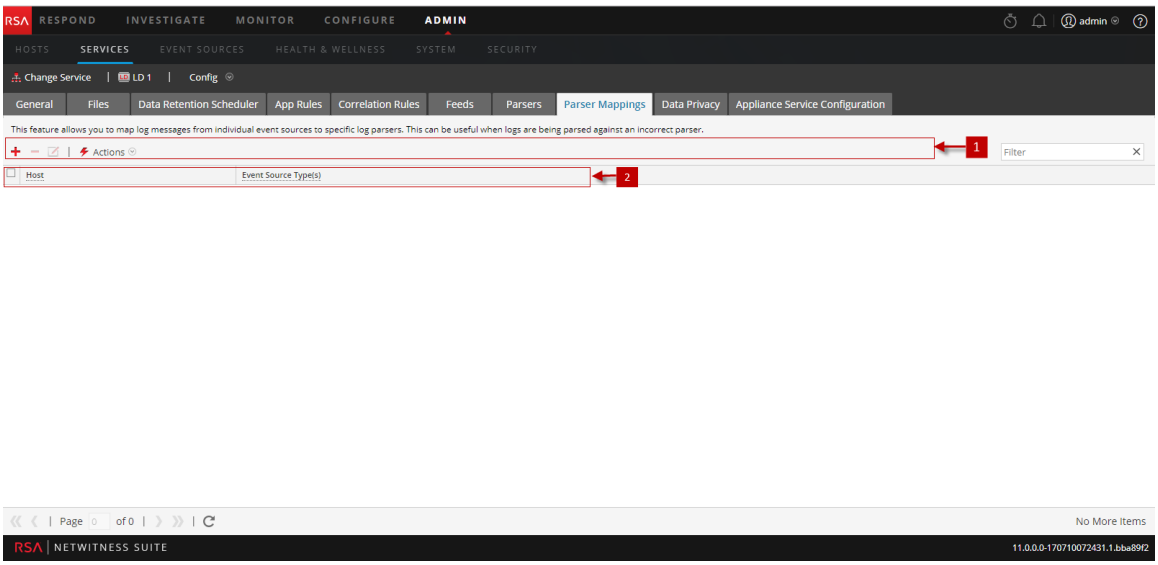
Benutzerrolle	Ziel	Dokumentation
Administrator	IPs für Ereignisquellenzuordnung verwalten	Parser-Zuordnungen aktivieren

Verwandte Themen

- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder

Überblick

Dies ist ein Beispiel für die Registerkarte.



1	Symbolleiste für Parser-Zuordnungen – Enthält Optionen für die Arbeit mit Parser-Zuordnungen im Raster.
2	Im Raster „Parser-Zuordnungen“ werden alle Parser aufgeführt, die aktuell auf dem Log Decoder zugeordnet sind.

Symbolleiste für Parser-Zuordnungen

Die Symbolleiste für Parser-Zuordnungen enthält Optionen für die Arbeit mit Parser-Zuordnungen im Raster.

Funktion	Beschreibung
	Hinzufügen einer Parserzuordnung
	Löschen der ausgewählten Parserzuordnung
	Bearbeiten einer Parserzuordnung
	Aktualisieren der Liste der Parserzuordnungen
	Anzeigen des Menüs „Aktionen“ • **Importieren**: Importieren einer Parserzuordnung in eine Datei • **Exportieren**: Speichern einer Parserzuordnung in einer Datei

Liste „Parser-Zuordnungen“

In der Liste „Parser-Zuordnungen“ werden alle Parser angezeigt, die aktuell auf dem Log Decoder zugeordnet sind.

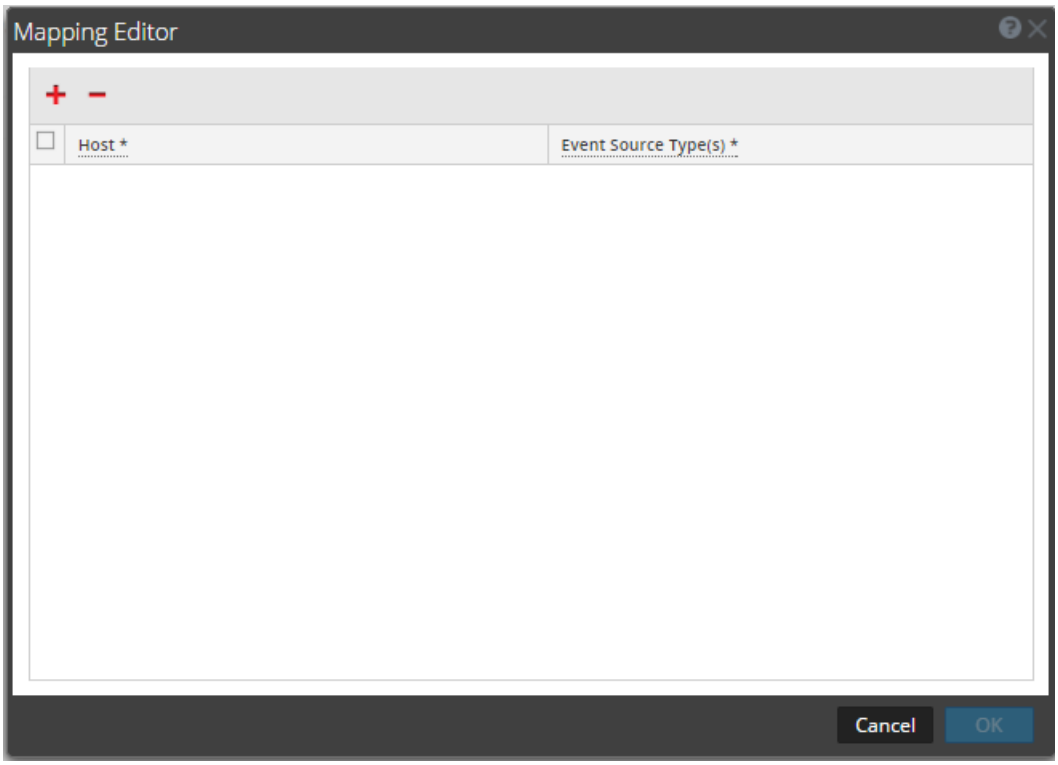
Parameter	Beschreibung
Host	Zeigt die IP-Adresse des Hosts an.
Ereignisquelle	Zeigt die Ereignisquellen an, die nicht korrekt analysiert werden.

Dialogfeld „Parser-Zuordnungseditor“

Im Dialogfeld „Parser-Zuordnungseditor“ können Sie eine IP für die Ereignisquellenzuordnung aktualisieren.

Um das Dialogfeld „Parser-Zuordnungseditor“ aufzurufen, gehen Sie folgendermaßen vor:

1. Wählen Sie im Menü NetWitness Suite die Optionen **ADMIN > Services**.
2. Wählen Sie einen **Log Decoder** und in der Spalte **Aktionen** die Optionen  **> Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie die Registerkarte **Parser-Zuordnungen** aus.
4. Klicken Sie auf  .
   Das Dialogfeld „Zuordnungseditor“ wird angezeigt.



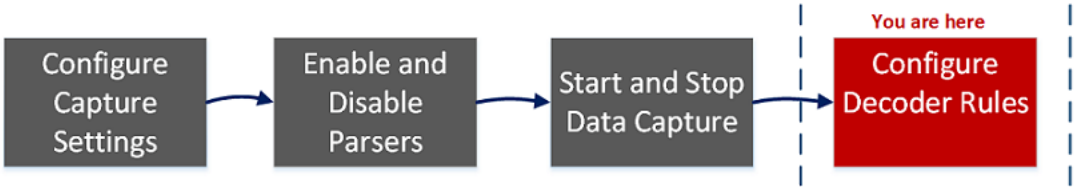
Weitere Informationen zum Dialogfeld „Parser-Zuordnungseditor“ finden Sie unter Parser-Zuordnungen aktivieren.

Ansicht „Services-Konfiguration“ – Registerkarte „Regeln“

Über die Registerkarte „Regeln“ in der Ansicht „Services-Konfiguration“ (**ADMIN > Services** > wählen Sie einen Service aus und klicken Sie auf > **Ansicht > Konfiguration**) können Sie Erfassungsregeln definieren und verwalten. Jeder Regeltyp weist ein Raster mit leicht unterschiedlichen Spalten und Parametern im Dialogfeld „Regel-Editor“ auf. Anwendungs- und Korrelationsregeln gelten für Decoder und Log Decoder. Netzwerkregeln gelten nur für Packet Decoders.

Workflow

Die folgende Abbildung zeigt den Workflow für allgemeine Decoder-Konfigurationsaufgaben. Die Schritte, die in dieser Ansicht durchgeführt werden können, sind hervorgehoben.



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Administrator	Erfassungseinstellungen konfigurieren	Konfigurieren von Erfassungseinstellungen
Administrator	Parser und Protokollparser verwalten	Aktivieren und Deaktivieren von Parsern und Protokollparsern
Administrator	Datenerfassung starten und beenden	Starten und Beenden der Datenerfassung
Administrator	Regeln konfigurieren*	Konfigurieren von Decoder-Regeln
Administrator	Eine Regel importieren, exportieren oder per Push übertragen*	Konfigurieren von Decoder-Regeln
Administrator	Eine Regel aktivieren oder deaktivieren	Konfigurieren von Decoder-Regeln

Benutzerrolle	Ziel	Dokumentation
Administrator	Eine Regel hinzufügen, bearbeiten oder löschen*	Konfigurieren von Decoder-Regeln

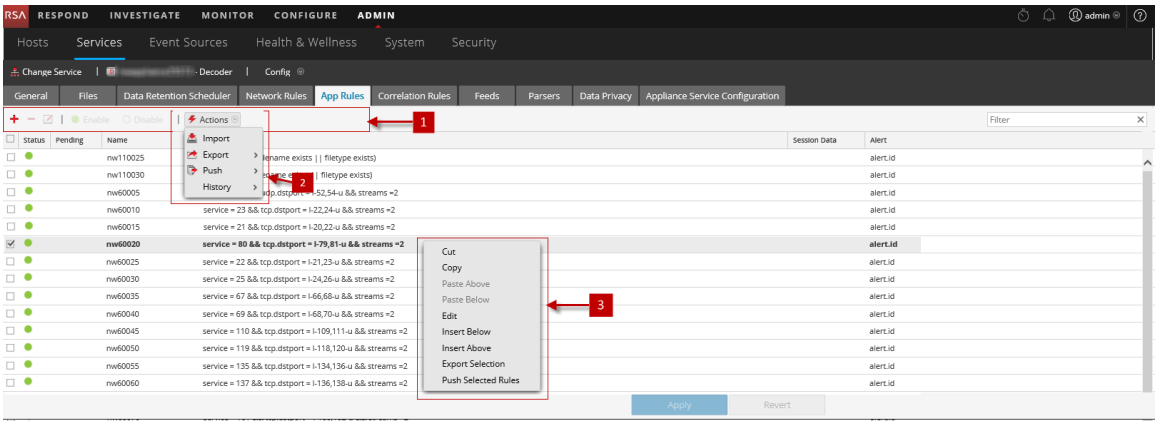
*Sie können diese Aufgaben hier durchführen.

Verwandte Themen

- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Decoder und Log Decoder – Schnelleinrichtung
- Registerkarte „App-Regeln“
- Registerkarte „Korrelationsregeln“
- Registerkarte „Netzwerkregeln“

Überblick

Dies dient als Beispiel der Registerkarte „App-Regeln“.



1	Symbolleiste der Registerkarte „Regeln“ – bietet Optionen zur Arbeit mit Regeln im Raster
2	Menü „Regelaktionen“ – bietet Optionen zum Verwalten von Gruppen von Regeln
3	Kontextaktionen Liste „Regeln“ – zeigt das Kontextmenü der Liste „Regeln“ an

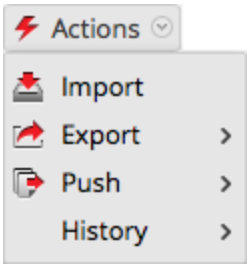
Symbolleiste der Registerkarte Regeln

Die Symbolleiste ist bei allen Registerkarten „Regeln“ unter der Ansicht „Konfiguration“ identisch.

Funktion	Beschreibung
Actions	Zeigt das Menü **Aktionen** an.
+	Fügt dem Service eine neue Regel hinzu
−	Löscht eine Regel aus dem Service
	Ermöglicht die Bearbeitung einer Regel
Disable	Deaktiviert eine Regel (Regel wird nicht gelöscht)
Enable	Aktiviert (Reaktiviert) eine Regel
Filter	Das Eingabefeld für eine zu suchende Zeichenfolge.NetWitness Suite filtert die Regeln dynamisch, während Sie eine Suchzeichenfolge eingeben. Der Text im Eingabefeld wird durch Klicken auf **x** gelöscht und die ungefilterte Ansicht wird so wiederhergestellt.
Anwenden	Speichert die Regeländerungen und wendet die konfigurierten Regeln in einem Service an Bevor Sie die Änderungen übernehmen, besteht die Möglichkeit, die ursprüngliche unbearbeitete Regel wiederherzustellen.
Zurücksetzen	Verwirft ungespeicherte Änderungen an dem Raster und stellt die unbearbeiteten Regeln wieder her.

Menü Regelaktionen

Das Menü „Aktionen“ verfügt über Optionen, die Ihnen dabei helfen, Regeln zu verwalten.



Option	Beschreibung
Importieren	Importiert Regeln in die Benutzeroberfläche, sodass diese in einem Service angewendet werden können Sie können die Regeln vor der Anwendung bearbeiten.
Exportieren	Speichert ausgewählte Regeln oder alle Regeln in einer .nwr-Datei auf dem Clientcomputer.

Push	Ermöglicht die Anwendung von Regeln auf andere Services (Decoders oder Log Decoders) oder Decoders, die einer Servicegruppe angehören. Während der Übertragung können Regeln entweder zusammengefügt (bestehende aktualisiert und neue hinzugefügt) oder ersetzt werden.
	• **Push > Alle.** Überträgt alle Regeln per Push in andere Services. Alle Regeln in den Zielservices werden entfernt und durch alle Regeln im Quellservice ersetzt.
	• **Push > Auswahl.** Überträgt ausgewählte Regeln per Push an andere Services. Sie haben zwei Optionen:
	  • **Ersetzen.** Löscht alle Regeln in den Zielservices und ersetzt sie durch die ausgewählten Regeln aus dem Quellservice.
	  • **Zusammenführen.** Führt die ausgewählten Regeln mit den vorhandenen Regeln in den Zielservices zusammen

Verlauf	Zeigt die letzten zehn Snapshots der durch NetWitness Suite angewendeten Regeln an. Sie können einen Snapshot jederzeit auswählen und auf dem Decoder anwenden (wiederherstellen).

Kontextaktionen Liste „Regeln“

Wenn Sie innerhalb des Regelrasters mit der rechten Maustaste auf eine Zeile klicken, wird das Kontextmenü des Regelrasters angezeigt.

Option	Beschreibung
Ausschneiden	Löscht die aktuelle Regel
Kopieren	Kopiert die aktuelle Regel

Option	Beschreibung
Oben einfügen	Fügt die kopierte Regel aus der Zwischenablage oberhalb der aktuellen Regel ein
Unten einfügen	Fügt die kopierte Regel aus der Zwischenablage unterhalb der aktuellen Regel ein
Edit	Bearbeitet die aktuelle Regel
Unten einfügen	Fügt die importierte Regel unterhalb der aktuellen Regel ein
Oben einfügen	Fügt die importierte Regel oberhalb der aktuellen Regel ein
Exportauswahl	Exportiert die ausgewählten Regeln
Ausgewählte Regeln per Push übertragen	Überträgt die ausgewählten Regeln auf andere Services

Registerkarte „App-Regeln“

Über die Registerkarte „App-Regeln“ (**ADMIN > Services >** wählen Sie einen Decoder oder Log Decoder aus und klicken Sie auf > **Ansicht > Konfiguration > Registerkarte „App-Regeln“**) können Sie Anwendungsregeln managen. NetWitness Suite wendet Anwendungsregeln auf der Sitzungsebene an.

Was möchten Sie tun?

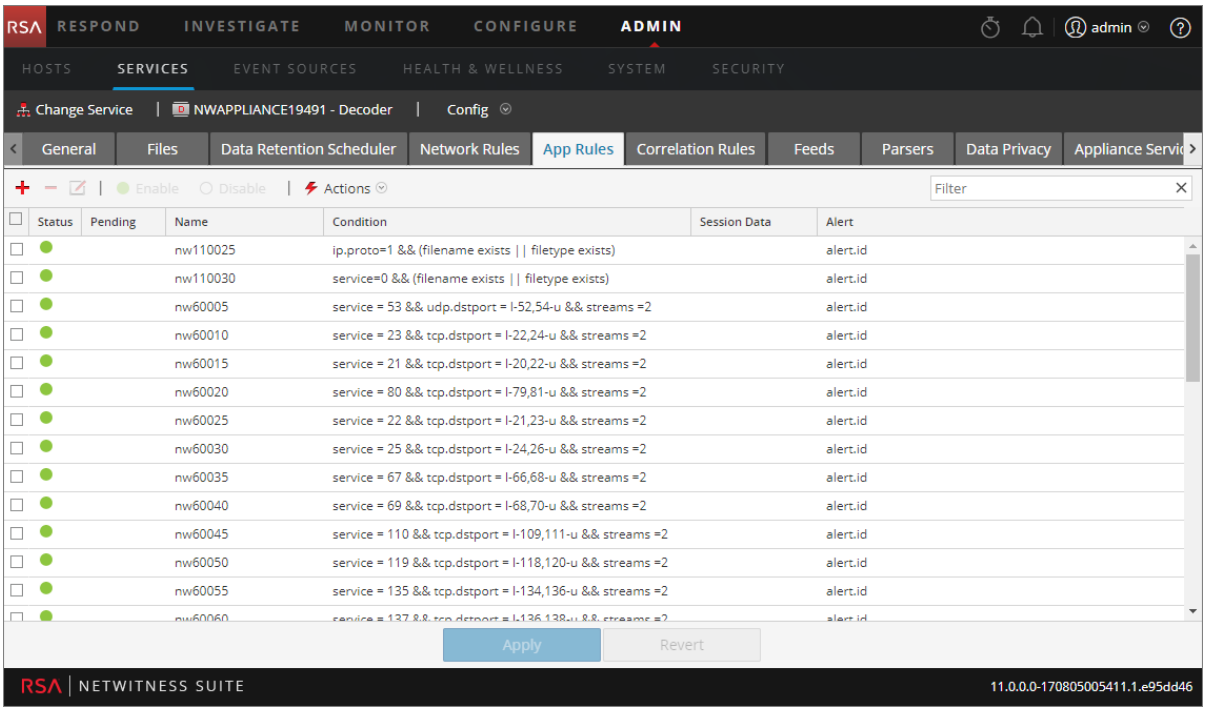
Benutzerrolle	Ziel	Dokumentation
Administrator	Anwendungsregeln hinzufügen oder bearbeiten	Konfigurieren von Anwendungsregeln

Verwandte Themen

- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Konfigurieren von Decoder-Regeln
- Ansicht „Services-Konfiguration“ – Registerkarte „Regeln“

Überblick

Die folgende Abbildung zeigt die Registerkarte „App-Regeln“ und die Tabelle beschreibt die Spalten.

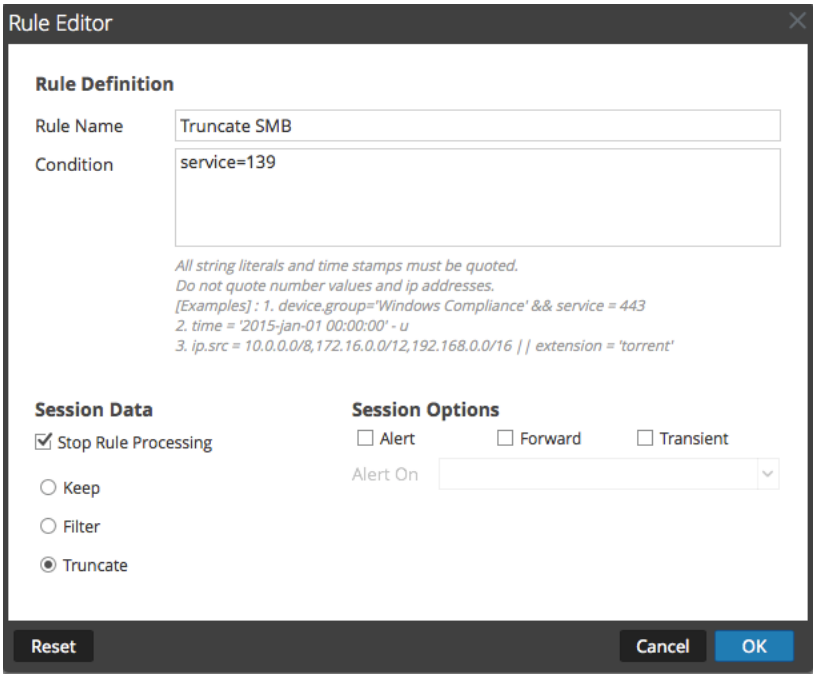


Spalte	Beschreibung
Ausstehend	In dieser Spalte wird angezeigt, ob für eine Regel Änderungen ausstehen. Zu Regeln, die derzeit auf dem Decoder aktiv sind, wird dies nicht angezeigt. Wenn die Regel neu ist oder geändert wurde, enthält die Spalte . Sobald die Regeln angewendet werden, wird das Anzeigeelement gelöscht.
Name	Dies ist der Name der Regel, eine beschreibende Kennung für die Regel.
Bedingung	Dies ist die Definition der Bedingung, die eine Aktion auslöst, wenn sie erfüllt wird.
Sitzungsdaten	In dieser Spalte wird angegeben, welche Aktion für die Sitzungsdaten ausgeführt wird, wenn ein Paket mit der Regel übereinstimmt. Mögliche Werte sind **Filtern**, **Beibehalten** oder **Kürzen**.
Warnmeldung	In dieser Spalte wird der Name der benutzerdefinierten Warnmeldung angegeben, die der Decoder erzeugt, wenn Metadaten mit der Regel übereinstimmen.

Spalte	Beschreibung
Status	In dieser Spalte wird mit einem Kreissymbol angezeigt, ob die Regel aktiviert oder deaktiviert ist. Wenn der Kreis grün gefüllt ist, ist die Regel aktiviert. Wenn der Kreis leer ist, ist die Regel deaktiviert.

Dialogfeld Regel-Editor

In der folgenden Abbildung ist das Dialogfeld Regel-Editor für eine Anwendungsregel gezeigt.



Das **Dialogfeld Regel-Editor** enthält Felder und Optionen, die zur Definition einer Anwendungsregel erforderlich sind.

Feld	Beschreibung
Name der Regel	Ein beschreibender Name, der die Regel identifiziert.

Feld	Beschreibung
Bedingung	Die Definition der Bedingung, die eine Aktion auslöst, wenn sie zutrifft. Sie können Ihre Eingabe direkt im Feld tätigen oder die Bedingung in diesem Feld mit Metadaten aus den Intellisense-Fensteraktionen erstellen. Während der Regeldefinition zeigt Intellisense Syntaxfehler und Warnungen an. Alle Zeichenfolgenliterale und Zeitstempel müssen in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Unter Konfigurieren von Decoder-Regeln finden Sie zusätzliche Details.

In der folgenden Tabelle werden die Aktionen und Optionen für Sitzungsdaten beschrieben.

Aktion	Beschreibung
Regelverarbeitung beenden	Bei erfolgter Überprüfung, wird keine weitere Regelevaluierung durchgeführt, wenn die Regel übereinstimmt, und die Sitzung wird entsprechend der Sitzungsaktion gespeichert. Ist dies nicht aktiviert, wird die Regelauswertung so lange ausgeführt, bis alle Regeln ausgewertet wurden.
Beibehalten	Die Paketnutzlast und die entsprechenden Metadaten werden gespeichert, wenn sie mit der Regel übereinstimmen.
Filter	Das Paket wird nicht gespeichert, wenn es mit der Regel übereinstimmt.
Kürzen	Die Paketnutzlast wird nicht gespeichert, wenn sie mit der Regel übereinstimmt, Paketkopfzeilen und zugehörige Metadaten werden jedoch beibehalten.
Warnmeldung und **Warnmeldung aktiviert**	Bei der Überprüfung von **Warnmeldungen** erzeugt das Paket eine benutzerdefinierte Warnmeldung, wenn Metadaten mit der Regel übereinstimmen. Im Feld **Warnmeldung aktiviert** können Sie den Namen der Warnmeldung auswählen.

Aktion	Beschreibung
Weiterleiten	Aktiviert die Ausführung der Syslog-Weiterleitung, wenn das Protokoll mit der Regel übereinstimmt.
Vorübergehend	Verhindert, dass die erstellten Warnmeldungs-Metadaten auf den Datenträger geschrieben werden.

In der folgenden Tabelle werden die Aktionen des Dialogfelds Regel-Editor beschrieben.

Aktion	Beschreibung
Zurücksetzen	Setzt die Inhalte des Dialogfelds auf die Werte vor der Bearbeitung zurück; Änderungen werden verworfen.
Abbrechen	Bricht alle Bearbeitungen ab und schließt das Dialogfeld „Regel-Editor“.
OK	Speichert die neue oder bearbeitete Regel und fügt diese dem Regelraster hinzu Das Dialogfeld „Regel-Editor“ wird geschlossen.
Speichern	(Nur für Regeln mit veralteter Syntax) Wendet eine korrigierte Regel einzeln auf den Decoder-Service an. Siehe Korrigieren von Regeln mit ungültiger Syntax.

Registerkarte „Korrelationsregeln“

Über die Registerkarte „Korrelationsregeln“ (**ADMIN > Services >** wählen Sie einen Service aus und klicken Sie auf > **Ansicht > Konfiguration > Registerkarte „Korrelationsregeln“**) können Sie Korrelationsregeln managen. Grundlegende Korrelationsregeln werden auf der Sitzungsebene angewendet und weisen die Benutzer auf bestimmte Aktivitäten hin, die möglicherweise in ihrer Umgebung vorkommen. NetWitness Suite wendet Korrelationsregeln über ein konfigurierbares gleitendes Zeitfenster an.

Was möchten Sie tun?

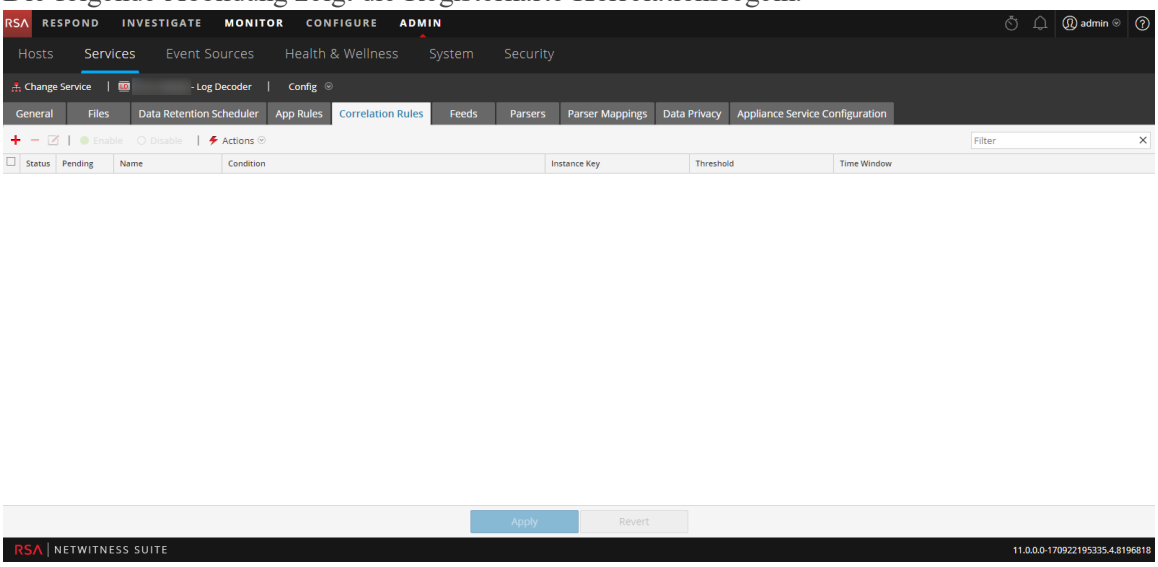
Benutzerrolle	Ziel	Dokumentation
Administrator	Eine Korrelationsregel hinzufügen oder bearbeiten	Konfigurieren von Korrelationsregeln

Verwandte Themen

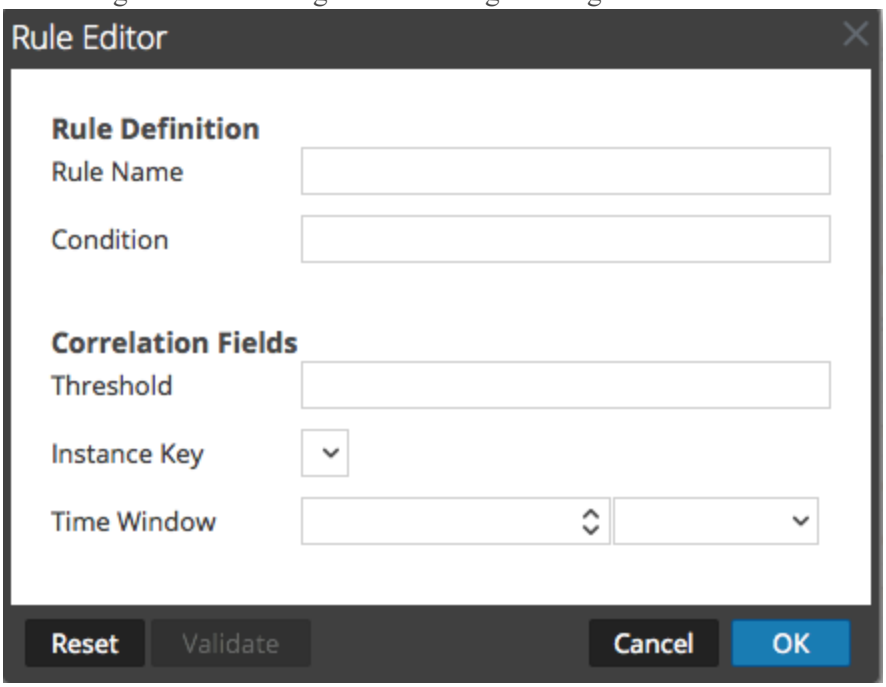
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von Decoder-Regeln
- Ansicht „Services-Konfiguration“ – Registerkarte „Regeln“

Überblick

Die folgende Abbildung zeigt die Registerkarte Korrelationsregeln.



In der folgenden Abbildung ist das Dialogfeld Regel-Editor für eine Korrelationsregel gezeigt.



In der folgenden Tabelle sind die Spalten der Registerkarte Korrelationsregeln beschrieben.

Spalte	Beschreibung
Ausstehend	In dieser Spalte wird angezeigt, ob für eine Regel Änderungen ausstehen. Zu Regeln, die derzeit auf dem Decoder aktiv sind, wird dies nicht angezeigt. Wenn die Regel neu ist oder geändert wurde, enthält die Spalte . Sobald die Regeln angewendet werden, wird das Anzeigeelement gelöscht.
Name	Dies ist ein beschreibender Name für die Regel.
Bedingung	Dies ist die Definition der Bedingung, die eine Aktion auslöst, wenn sie erfüllt wird. In Bedingungen müssen alle Zeichenfolgenliterale und Zeitstempel in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Unter Konfigurieren von Decoder-Regeln finden Sie zusätzliche Details.

Spalte	Beschreibung
Instanzschlüssel	Dies ist der Zielindikator, auf dem das Ereignis basiert. Er kann ein einziger Primärschlüssel sein, wie etwa ip.src, oder ein zusammengesetzter Primärschlüssel, wie etwa ip.src,ip.dst.
Schwellenwert	Dies ist die Mindestanzahl von Vorkommnissen, die erforderlich sind, um eine Korrelationssitzung auszulösen. Dazu kann ein Schlüssel angegeben werden, der den Metadatentyp identifiziert, anhand dessen wir feststellen können, ob die Bedingung erfüllt ist. Die Korrelations-Engine kann IPv4 oder IPv6 nicht als zugehörigen Metadatentyp verwenden. Verwenden Sie eines dieser drei Argumente: • u_count(associated_key) = die Anzahl eindeutiger Werte des angegebenen Schlüssels. Ein Schlüssel ist erforderlich. • sum(associated_key) = die Werte des angegebenen Schlüssels, ein Schlüssel ist erforderlich. • count() = Anzahl der Sitzungen, kein zugehöriger Schlüssel verwendet. Wenn enthalten, wird er ignoriert.
Zeitfenster	Dies ist die Dauer in Stunden, Minuten oder Sekunden, innerhalb der der Schwellenwert erreicht werden muss, um eine Korrelationssitzung auszulösen.
Status	In dieser Spalte wird mit einem Kreissymbol angezeigt, ob die Regel aktiviert oder deaktiviert ist. Wenn der Kreis grün gefüllt ist, ist die Regel aktiviert. Wenn der Kreis leer ist, ist die Regel deaktiviert.

Das Dialogfeld **Regel-Editor** enthält die Felder und Optionen, die zur Definition einer Netzwerkregel erforderlich sind. Die Felder entsprechen genau den Rasterspalten.

Aktion	Beschreibung
Zurücksetzen	Setzt die Inhalte des Dialogfelds auf die Werte vor der Bearbeitung zurück; Änderungen werden verworfen.
Abbrechen	Bricht alle Bearbeitungen ab und schließt das Regel-Editor-Dialogfeld.

Aktion	Beschreibung
OK	Speichert die neue oder bearbeitete Regel und fügt diese dem Regelraster hinzu Das Regel-Editor-Dialogfeld wird geschlossen.
Speichern	(Nur für Regeln mit veralteter Syntax) Wendet eine korrigierte Regel einzeln auf den Decoder-Service an. Siehe Korrigieren von Regeln mit ungültiger Syntax.

Registerkarte „Netzwerkregeln“

Über die Registerkarte „Netzwerkregeln“ (**ADMIN > Services >** wählen Sie einen Decoder aus und klicken Sie auf > **„Ansicht“ > „Konfiguration“ > Registerkarte „Netzwerkregeln“**) können Sie Netzwerkregeln managen. NetWitness Suite wendet Netzwerkregeln auf Paketebene an. Netzwerkregeln bestehen aus Regelsätzen aus Layer 2, Layer 3 und Layer 4. Mehrere Regeln können auf den Decoder angewendet werden. Regeln können auf mehrere Ebenen angewendet werden (zum Beispiel, wenn eine Netzwerkregel bestimmte Ports für eine bestimmte IP-Adresse herausfiltert). Netzwerkregeln gelten nur für Packet Decoder.

Was möchten Sie tun?

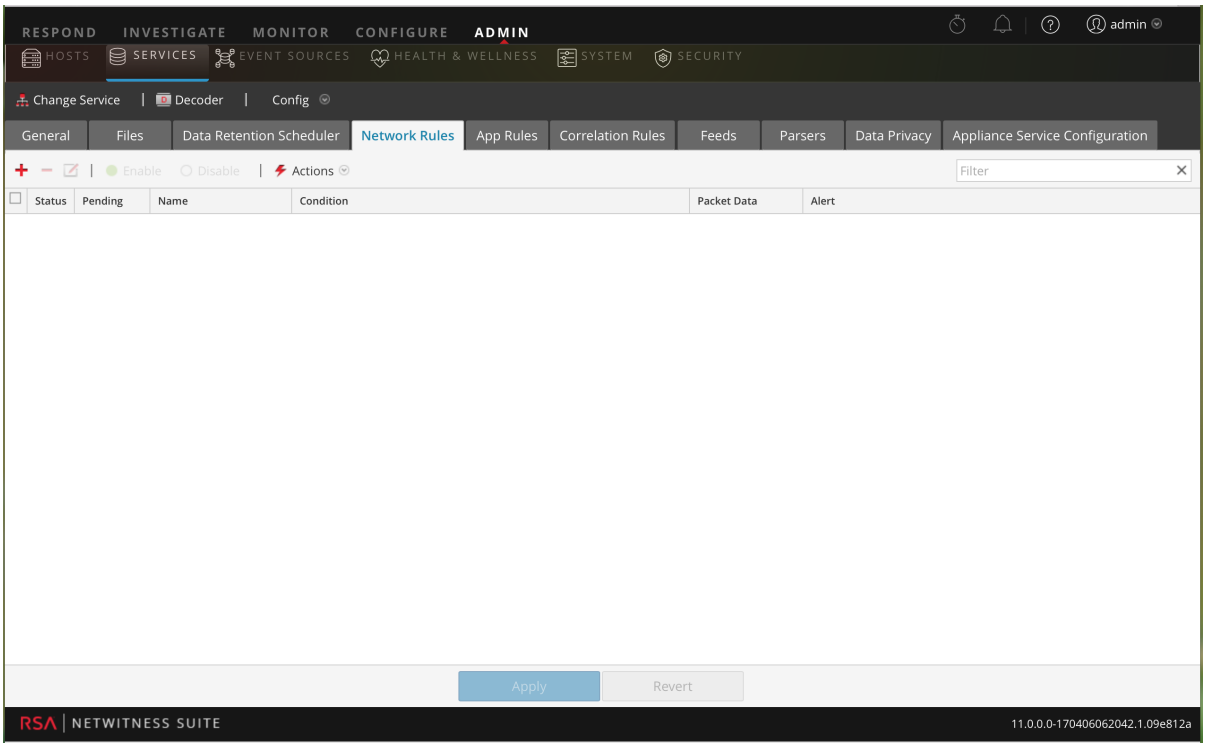
Benutzerrolle	Ziel	Dokumentation
Administrator	Netzwerkregeln hinzufügen, bearbeiten oder korrigieren	Konfigurieren von Netzwerkregeln

Verwandte Themen

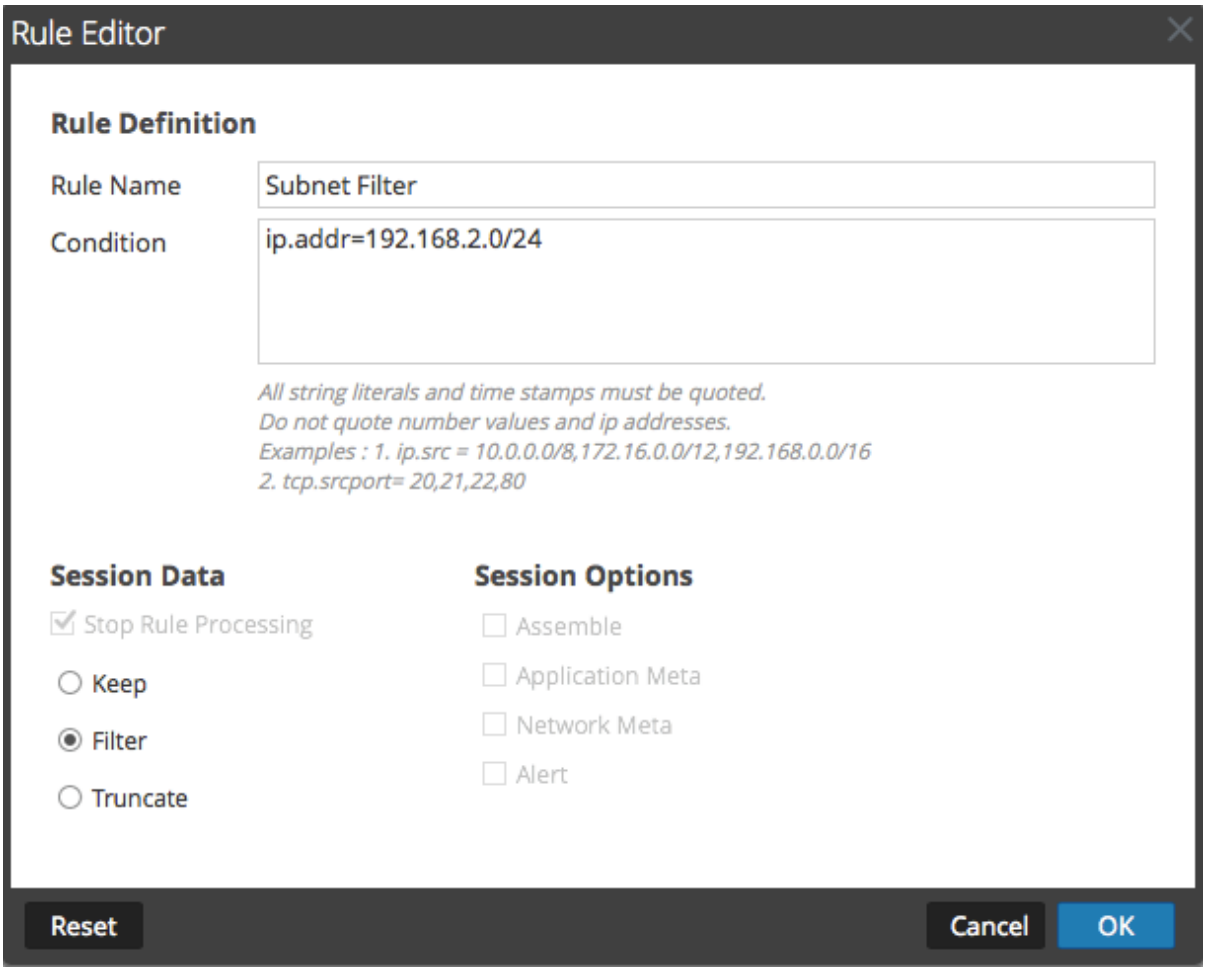
- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- Konfigurieren von Decoder-Regeln
- Ansicht „Services-Konfiguration“ – Registerkarte „Regeln“

Überblick

Die folgende Abbildung zeigt die Registerkarte Netzwerkregeln.



In der folgenden Abbildung ist das Dialogfeld Regel-Editor für eine Netzwerkregel gezeigt.



In der folgenden Tabelle werden die Spalten im Raster „Netzwerkregeln“ beschrieben.

Spalte	Beschreibung
Ausstehend	In dieser Spalte wird angezeigt, ob für eine Regel Änderungen ausstehen. Zu Regeln, die derzeit auf dem Decoder aktiv sind, wird dies nicht angezeigt. Wenn die Regel neu ist oder geändert wurde, enthält die Spalte . Sobald die Regeln angewendet wurden, wird der Indikator „Ausstehend“ entfernt.
Name	Dies ist der Name der Regel, eine beschreibende Kennung für die Regel.
Bedingung	Dies ist die Definition der Bedingung, die eine Aktion auslöst, wenn sie erfüllt wird.

Spalte	Beschreibung
Paketdaten	In dieser Spalte wird angegeben, welche Aktion für die Sitzungsdaten ausgeführt wird, wenn ein Paket mit der Regel übereinstimmt. Mögliche Werte sind **Filtern**, **Beibehalten** oder **Kürzen**.
Warnmeldung	In dieser Spalte wird angegeben, ob der Decoder eine benutzerdefinierte Warnmeldung generiert, wenn Metadaten mit der Regel übereinstimmen. Mögliche Werte sind **Aktiviert** oder **Deaktiviert**.
Status	In dieser Spalte wird mit einem Kreissymbol angezeigt, ob die Regel aktiviert oder deaktiviert ist. Wenn der Kreis grün gefüllt ist, ist die Regel aktiviert. Wenn der Kreis leer ist, ist die Regel deaktiviert.

Das Dialogfeld **Regel-Editor** enthält die Felder und Optionen, die zur Definition einer Netzwerkregel erforderlich sind.

Die folgende Tabelle beschreibt die Regeldefinitionsfelder.

Feld	Beschreibung
Name der Regel	Ein beschreibender Name, der die Regel identifiziert.
Bedingung	Die Definition der Bedingung, die bei einer Übereinstimmung eine Aktion auslöst. Sie können direkt in das Feld schreiben oder die Bedingung in diesem Feld mithilfe der Metadaten aus den Intellisense-Fensteraktionen erstellen. Während der Regeldefinition zeigt Intellisense Syntaxfehler und Warnungen an. In Bedingungen müssen alle Zeichenfolgenliterale und Zeitstempel in Anführungszeichen gesetzt werden. Zahlenwerte und IP-Adressen dürfen nicht in Anführungszeichen gesetzt werden. Unter Konfigurieren von Decoder-Regeln finden Sie zusätzliche Details. In diesem Abschnitt werden auch die Metaschlüssel beschrieben, die NetWitness Suite zur Verwendung in Netzwerkregelbedingungen unterstützt.

In der folgenden Tabelle werden die Aktionen für Sitzungsdaten beschrieben.

Aktion	Beschreibung
Regelverarbeitung beenden	Ist dies aktiviert, wird die Regelauswertung beendet, wenn eine Übereinstimmung mit der Regel gefunden wird, und die Sitzung wird wie angegeben gespeichert. Ist dies nicht aktiviert, wird die Regelauswertung so lange ausgeführt, bis alle Regeln ausgewertet wurden.
Beibehalten	Die Paketnutzlast und die entsprechenden Metadaten werden gespeichert, wenn sie mit der Regel übereinstimmen.
Filter	Das Paket wird nicht gespeichert, wenn es mit der Regel übereinstimmt.
Kürzen	Die Paketnutzlast wird nicht gespeichert, wenn sie mit der Regel übereinstimmt, aber Paketkopfzeilen und zugehörige Metadaten werden beibehalten.

In der folgenden Tabelle werden die Sitzungsoptionen beschrieben.

Aktion	Beschreibung
Assemblieren	Ist dies aktiviert, setzt der Assembler die Paketkette zusammen, wenn sie mit der Regel übereinstimmt.
Netzwerkmetadaten	Das Paket erzeugt Netzwerkmetadaten, wenn es der Regel entspricht.
Anwendungsmetadaten	Das Paket erzeugt Anwendungsmetadaten, wenn es der Regel entspricht.
Warnmeldung	Das Paket erzeugt eine angepasste Warnmeldung, wenn Metadaten der Regel entsprechen.

In der folgenden Tabelle werden die Aktionen des Dialogfelds Regel-Editor beschrieben.

Aktion	Beschreibung
Zurücksetzen	Setzt die Inhalte des Dialogfelds auf die Werte vor der Bearbeitung zurück; Änderungen werden verworfen.
Abbrechen	Bricht alle Bearbeitungen ab und schließt das Dialogfeld „Regel-Editor“.
OK	Speichert die neue oder bearbeitete Regel und fügt diese dem Regelraster hinzu Das Dialogfeld „Regel-Editor“ wird geschlossen.
Speichern	(Nur für Regeln mit veralteter Syntax) Wendet eine korrigierte Regel einzeln auf den Decoder-Service an. Siehe Korrigieren von Regeln mit ungültiger Syntax.

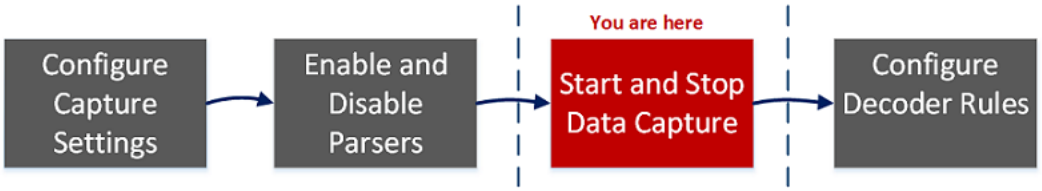
Ansicht „Services-System“ – Decoder

Ein Log Decoder ist ein spezieller Typ Decoder und wird ähnlich wie ein solcher konfiguriert und gemanagt. Daher bezieht sich ein Großteil der Informationen in diesem Abschnitt auf beide Arten Decoder. Auf Unterschiede für Log Decoders wird hingewiesen.

Um die Ansicht „Services-System“ aufzurufen, gehen Sie zu **ADMIN > Services >** wählen Sie einen Decoder oder Log Decoder > > **Ansicht** > **System**.

Workflow

Die folgende Abbildung zeigt den Workflow für allgemeine Decoder-Konfigurationsaufgaben. Die Schritte, die in dieser Ansicht durchgeführt werden können, sind hervorgehoben.



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Administrator	Erfassungseinstellungen konfigurieren	Konfigurieren von Erfassungseinstellungen
Administrator	Parser und Protokollparser verwalten	Aktivieren und Deaktivieren von Parsern und Protokollparsern
Administrator	Datenerfassung starten und beenden*	Starten und Beenden der Datenerfassung
Administrator	Paketerfassungs- und Protokolldateien hochladen*	Hochladen einer Protokolldatei zu einem Log Decoder Hochladen einer Paketerfassungsdatei

Benutzerrolle	Ziel	Dokumentation
Administrator	Protokollstatistiken zurücksetzen, Hostaufgaben ausführen, den Service herunterfahren, den Appliance-Service herunterfahren und den Host neu starten*	*Leitfaden für die ersten Schritte mit Hosts und Services*
Administrator	Regeln konfigurieren	Konfigurieren von Decoder-Regeln

*Sie können diese Aufgaben hier durchführen.

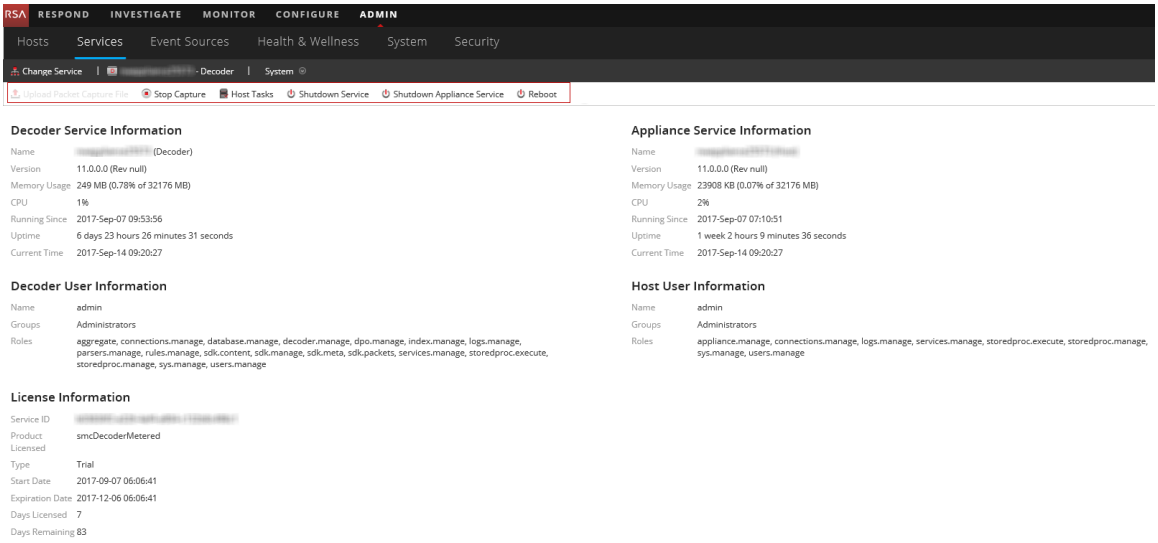
Verwandte Themen

Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

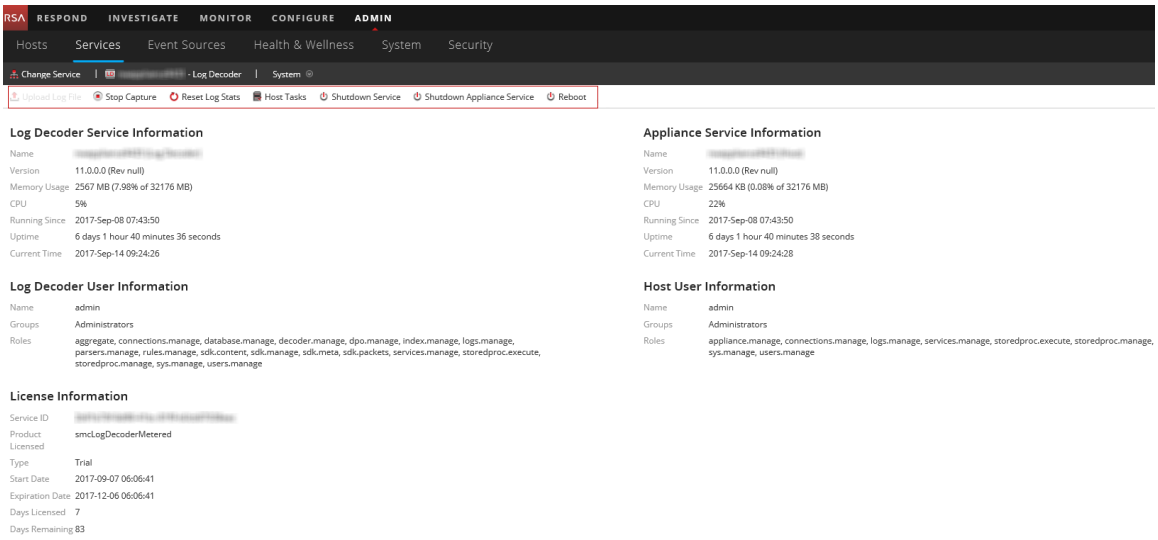
- Decoder und Log Decoder – Schnelleinrichtung
- Konfigurieren von allgemeinen Einstellungen auf einem Decoder
- „Ansicht Services > System“ im *Leitfaden für die ersten Schritte mit Hosts und Services*

Überblick

Hier sehen Sie ein Beispiel der Ansicht „Services > System“ für einen Decoder.

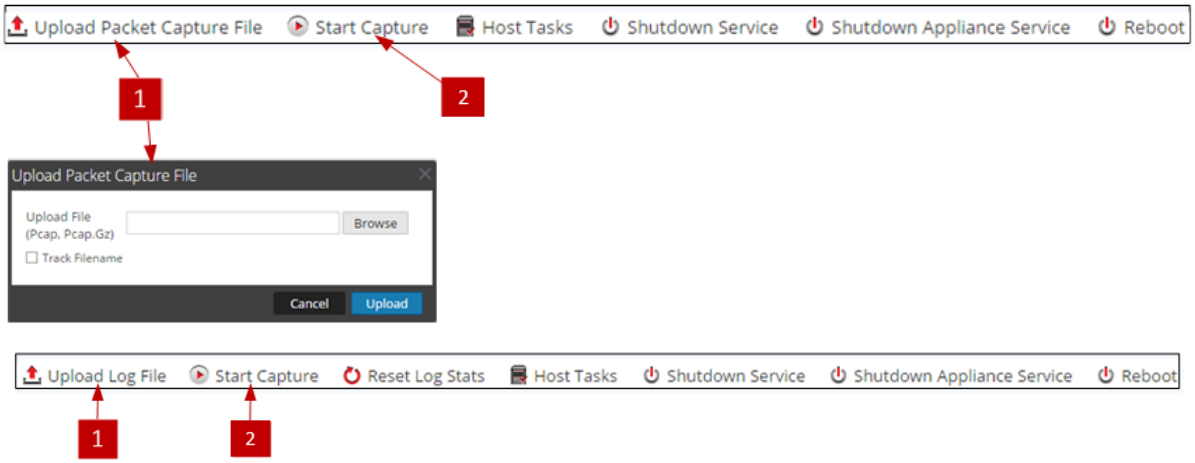


Hier sehen Sie ein Beispiel der Ansicht Services > System für einen Log Decoder.



Symbolleiste „Serviceinformationen“

Diese zwei Symbolleisten illustrieren die spezifischen Optionen für Decoder und Log Decoder.



Zusätzlich zu den gemeinsamen Optionen in der Symbolleiste der Ansicht Services > System können Sie die Erfassung von Paketen oder Protokollen starten und beenden. Die Uploaddateioptionen für den Standard-Decoder (Paketerfassungsdatei) und den Log Decoder (Protokolldatei) sind unterschiedlich.

Aktion	Beschreibung
Hochladen einer Paketerfassungsdatei	Es wird ein Dialogfeld angezeigt, in dem eine Paketerfassungsdatei (.pcap) für das Hochladen zu dem ausgewählten Decoder ausgewählt werden kann. Weitere Informationen finden Sie unter Hochladen einer Paketerfassungsdatei. **Hinweis:** Diese Option gilt nicht für Log Decoders.
Hochladen einer Protokolldatei	Es wird ein Dialogfeld angezeigt, in dem eine Protokolldatei (.log) für das Hochladen zu dem gewählten Decoder ausgewählt werden kann. Weitere Informationen finden Sie unter Hochladen einer Protokolldatei zu einem Log Decoder.
Starten/Beenden der Erfassung	Startet die Paketerfassung auf dem ausgewählten Decoder. Wenn die Paketerfassung ausgeführt wird, ändert sich die Option in der Symbolleiste zu Erfassung beenden und die Option zum Hochladen einer Datei ist nicht verfügbar.