



# ESA-Konfigurationsleitfaden

für Version 11.0



Copyright © 1994–2017 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten.

## **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](http://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

---

<b>Event Stream Analysis – Übersicht</b> .....	<b>6</b>
<b>Konfigurieren von ESA-Korrelationsregeln</b> .....	<b>8</b>
Voraussetzungen .....	8
Verfahren .....	8
Ergebnis .....	9
Schritt 1. Hinzufügen einer Datenquelle zu einem ESA-Service .....	9
Voraussetzungen .....	9
Methoden .....	9
Schritt 2. Konfigurieren erweiterter Einstellungen für einen ESA-Service .....	11
Methoden .....	11
<b>Konfigurieren von ESA Analytics</b> .....	<b>13</b>
Konfigurieren des Whois-Abfrageservice .....	13
Voraussetzungen .....	14
Konfigurieren des Whois-Abfrageservice .....	14
Zuordnen von ESA-Datenquellen zu Analytics-Modulen .....	17
Modulbereitstellungsbeispiel: zwei ESAs .....	17
Modulbereitstellungsbeispiel: ein ESA .....	18
Voraussetzungen .....	19
Erstellen von ESA Analytics-Zuordnungen .....	20
Bereitstellen von ESA Analytics-Zuordnungen .....	25
Aktualisieren einer Zuordnung .....	25
Aufheben der Bereitstellung einer Zuordnung .....	26
Löschen einer Zuordnung .....	26
Ändern der Aufwärmphase und der Verzögerungszeit .....	27
<b>Zusätzliche Verfahren für ESA-Korrelationsregeln</b> .....	<b>29</b>
Ändern des Speicherschwellenwerts für Testregeln .....	29
Voraussetzungen .....	30
Verfahren .....	30
Konfigurieren von ESA für die Verwendung eines Speicherpools .....	30
Verfahren .....	32

Ergebnis .....	35
Konfigurieren von ESA zur Verwendung von „Ordnen nach Erfassungszeit“ .....	35
Workflow für „Ordnen nach Erfassungszeit“ .....	36
Voraussetzungen .....	37
Methoden .....	37
Troubleshooting und Tipps .....	39
Deaktivieren des Ordners nach Erfassungszeit .....	39
Deaktivieren der Positionsnachverfolgung .....	39
Starten, Beenden oder erneut Starten des ESA-Services .....	40
Starten des ESA-Services .....	40
Beenden des ESA-Services .....	40
Neustarten des ESA-Services .....	40
Auditprotokolle und Überprüfen der ESA-Komponentenversionen und -status .....	41
Regeln für Auditprotokolle .....	41
Überprüfen der ESA Server-Version .....	42
Überprüfen der MongoDB-Version .....	42
Überprüfen des MongoDB-Status .....	43
<b>Referenzen .....</b>	<b>44</b>
Ansicht „Service-Konfiguration“ – Registerkarte „Datenquellen“ .....	45
Workflow .....	45
Was möchten Sie tun? .....	46
Verwandte Themen .....	46
Überblick .....	46
Ansicht „Services-Konfiguration“ – Registerkarte „Erweitert“ .....	49
Workflow .....	49
Was möchten Sie tun? .....	50
Verwandte Themen .....	50
Überblick .....	50
Konfiguration des Whois-Abfrageservice .....	53
Was möchten Sie tun? .....	53
Verwandte Themen .....	53
Konfiguration des Whois-Abfrageservice .....	54
ESA Analytics-Zuordnungen .....	58
Workflow .....	58

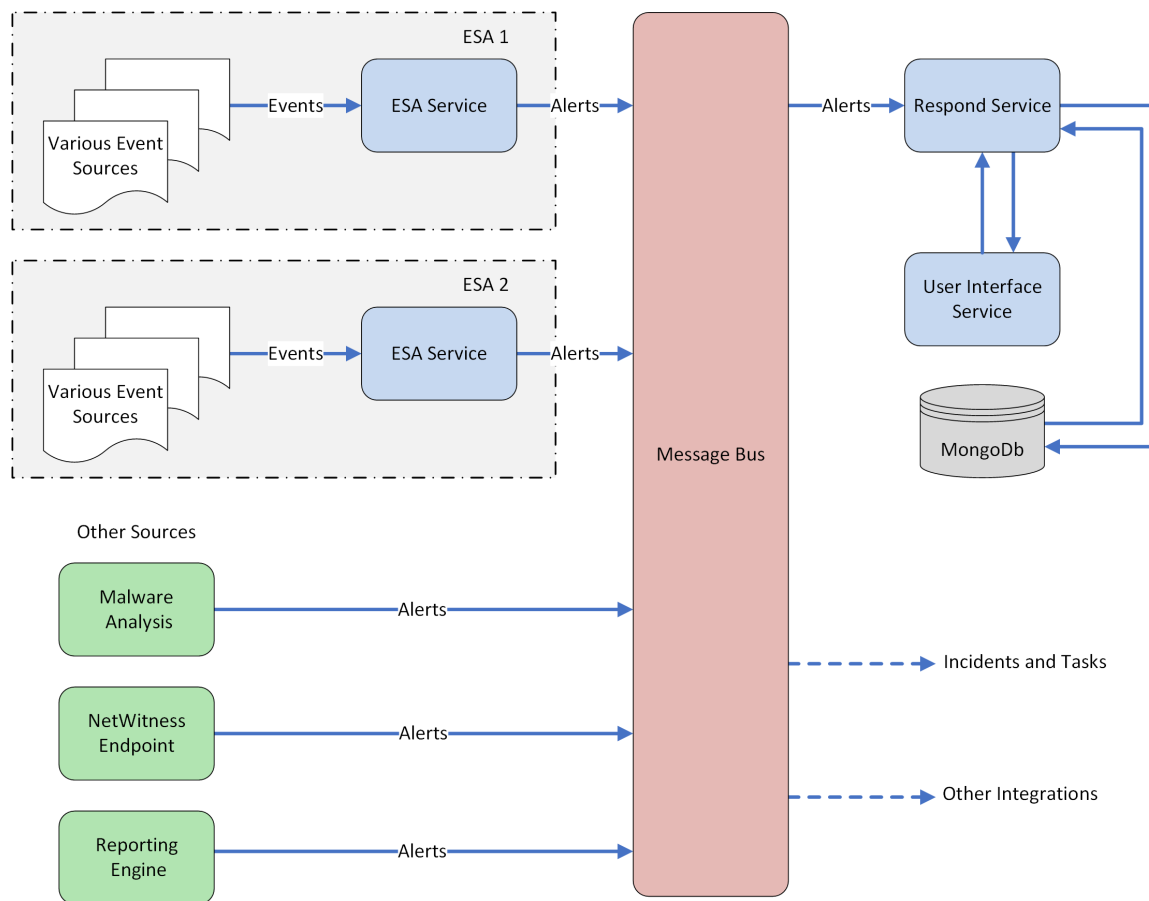
Was möchten Sie tun? .....	59
Verwandte Themen .....	59
Überblick .....	59
Moduleinstellungen .....	65
Was möchten Sie tun? .....	65
Verwandte Themen .....	65
Moduleinstellungen .....	65

## Event Stream Analysis – Übersicht

RSA NetWitness® Suite Event Stream Analysis (ESA) bietet Ereignisstreamanalysen wie Korrelation und komplexe Ereignisverarbeitung mit hohen Durchsätzen und niedriger Latenz. Er kann große Mengen unterschiedlicher Ereignisdaten aus Concentrators verarbeiten.

Die erweiterte Ereignisverarbeitungssprache von ESA ermöglicht Filterung, Aggregation, Verknüpfung, Mustererkennung und Korrelation über mehrere verteilte Ereignisstreams. Event Stream Analysis erleichtert die leistungsstarke Erkennung von Incidents und Erzeugung von Warnmeldungen.

In der folgenden Grafik ist der allgemeine Workflow dargestellt:



Es gibt zwei ESA-Services, die auf einem ESA-Host ausgeführt werden können:

- Event Stream Analysis (ESA-Korrelationsregeln)
- Event Stream Analytics Server (ESA Analytics)

Der erste Service ist der Event Stream Analysis-Service, der Warnmeldungen aus ESA-Regeln, auch bekannt als ESA-Korrelationsregeln, erstellt, die Sie manuell erstellen oder von Live herunterladen. Der zweite Service ist der ESA Analytics-Service, der für die automatisierte Bedrohungserkennung verwendet wird. Da der ESA Analytics-Service für die automatisierte Bedrohungserkennung vorkonfigurierte ESA Analytics-Module verwendet, müssen Sie keine Regeln erstellen oder herunterladen, um die automatisierte Bedrohungserkennung verwenden zu können.

Die ESA Analytics-Services verwenden abfragebasierte Aggregation (Query-Based Aggregation, QBA), um gefilterte Ereignisse für die ESA Analytics-Module von Concentrators zu erfassen. Nur die von einem Modul benötigten Daten werden zwischen dem Concentrator und dem ESA Analytics-System übertragen. Beispielsweise kann ein ESA Analytics-Service mithilfe eines ESA Analytics-Moduls „Suspicious Domains“ wie C2 für Pakete (http-packet) Ihren HTTP-Datenverkehr untersuchen, um die Wahrscheinlichkeit dafür zu ermitteln, dass böswillige Aktivitäten in Ihrer Umgebung stattfinden.

# Konfigurieren von ESA-Korrelationsregeln

In diesem Thema werden die Hauptaufgaben zur Konfiguration der Korrelationsregeln von RSA NetWitness Suite Event Stream Analysis (ESA) behandelt, die den Event Stream Analysis-Service verwenden.

## Voraussetzungen

Stellen Sie sicher, dass Sie:

- den Event Stream Analysis-Service in Ihrer Netzwerkumgebung installiert haben.
- einen oder mehrere Concentrator in Ihrer Netzwerkumgebung installiert und konfiguriert haben.

## Verfahren

**Hinweis:** Sie können ESA mit einem SSL-Port (50030) konfigurieren. Die Konfiguration eines Nicht-SSL-Port ist nicht möglich.

So konfigurieren Sie Event Stream Analysis:

Aufgaben	Referenz
1. Fügen Sie Concentrator als Datenquelle zum Event Stream Analysis-Service hinzu.	Weitere Informationen erhalten Sie unter <a href="#">Schritt 1. Hinzufügen einer Datenquelle zu einem ESA-Service</a>
2. Konfigurieren Sie Benachrichtigungen für den Event Stream Analysis-Service.	Weitere Informationen finden Sie unter „Benachrichtigungsmethoden“ im <i>Handbuch Versenden von Warnmeldungen mit ESA</i> .
3. Laden Sie Event Stream Analysis-Inhalte mithilfe von Live herunter.	Weitere Informationen finden Sie unter „Ansicht 'Live-Suche'“ im <i>Leitfaden Live-Ressourcenmanagement</i> .
4. (Optional) Erweiterte Konfiguration des Event Stream Analysis-Services	Weitere Informationen erhalten Sie unter <a href="#">Schritt 2. Konfigurieren erweiterter Einstellungen für einen ESA-Service</a>



## Ergebnis

Der Event Stream Analysis-Service ist konfiguriert und Sie können nun ESA-Regeln zur Ereignisverarbeitung und für Warnmeldungen hinzufügen. Informationen zum Hinzufügen von ESA-Regeln erhalten Sie unter „Hinzufügen von Regeln zur Regelbibliothek“ im *Handbuch zum Versenden von Warnmeldungen mit ESA*.

## Schritt 1. Hinzufügen einer Datenquelle zu einem ESA-Service

In diesem Thema wird erläutert, wie Sie dem Event Stream Analysis-Service neue oder vorhandene Datenquellen hinzufügen.

Ein ESA-Service erfasst Daten von einem Concentrator, um Incidents zu erkennen und den Benutzer in einer Warnmeldung darüber zu informieren. Damit ESA Daten analysieren kann, müssen Sie die Quellen konfigurieren, aus denen die ESA Daten liest. Verwenden Sie die Verfahren in diesem Thema, um der ESA Datenquellen hinzuzufügen.

### Voraussetzungen

In NetWitness Suite muss mindestens einer der folgenden Concentrator konfiguriert sein:



Der Event Stream Analysis-Service muss installiert sein und auf NetWitness Suite ausgeführt werden.

Sie müssen die folgenden Schritte ausführen, um eine Datenquelle hinzuzufügen:

- Hinzufügen einer verfügbaren Datenquelle
- Festlegen des Benutzernamens und Passworts für die Datenquelle

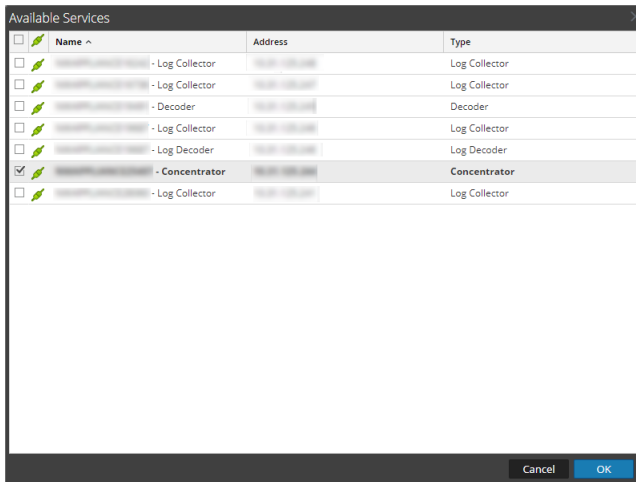
### Methoden

#### Hinzufügen vorhandener Services als Datenquelle

1. Navigieren Sie zu **ADMIN > Services**.  
Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie in der Ansicht „Services“ einen ESA-Service und dann   > **Ansicht > Konfiguration** aus.

3. Klicken Sie auf der Registerkarte **Datenquellen** auf **+**.

Die verfügbaren Services werden wie in der folgenden Abbildung dargestellt angezeigt.




4. Wählen Sie einen oder mehrere Concentrator aus und klicken Sie auf **OK**.  
Der Service wird der Liste der Services auf der Registerkarte **Datenquellen** hinzugefügt.
5. (Optional) Klicken Sie auf **Aktivieren**, um die Datenquelle zu aktivieren.
6. Klicken Sie auf **Anwenden**, um die Konfiguration zu speichern.

#### Festlegen des Benutzernamens und Passworts für die Datenquelle

**Hinweis:** Sie können einen Log Decoder als Datenquelle für ESA hinzufügen. RSA empfiehlt jedoch, Sie einen Concentrator hinzuzufügen, um die ungeteilte Aggregation zu nutzen, da auf dem Decoder möglicherweise andere Prozesse daraus aggregiert werden.

So legen Sie den Benutzernamen und das Passwort für die Datenquelle fest:

1. Navigieren Sie zu **ADMIN > Services**.  
Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie in der Ansicht **Services** einen Service aus.
3. Klicken Sie auf .
4. Legen Sie einen Benutzernamen und ein Passwort fest.
5. Klicken Sie auf **Speichern**.

## Schritt 2. Konfigurieren erweiterter Einstellungen für einen ESA-Service


In diesem Thema wird beschrieben, wie Sie erweiterte Einstellungen für einen Event Stream Analysis-Service konfigurieren.

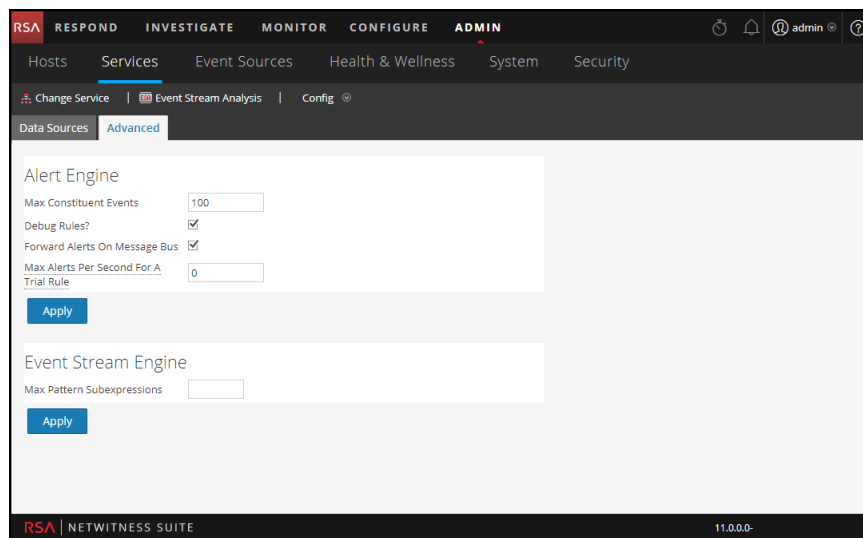
In der Ansicht „Erweitert“ können Sie erweiterte Einstellungen konfigurieren, um eine verbesserte Performance zu erzielen, die Ereignisanzahl für Regeln mit mehreren Ereignissen zu beschränken, Ereignisse im Arbeitsspeicher zu puffern und die Anzahl der in der ESA zu speichernden Ereignisse festzulegen.

### Methoden

#### Konfigurieren von erweiterten Einstellungen

So greifen Sie auf die Ansicht „Erweitert“ zu und konfigurieren erweiterte Einstellungen für einen ESA-Service:

1. Navigieren Sie zu **ADMIN > Services**.  
Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie in der Ansicht „Services“ einen ESA-Service und dann  > **Ansicht > Konfiguration** aus.
3. Wechseln Sie zur Registerkarte **Erweitert**.  
Die Ansicht „Erweitert“ wird angezeigt.



#### Konfigurieren der Warnmeldungs-Engine-Einstellungen

Im Abschnitt „Warnmeldungs-Engine“ geben Sie Werte an, um Ereignisse für Regeln zu bewahren, die mehrere Ereignisse wählen.

**Hinweis:** Nach dem Upgrade auf 10.5 wird die Option „Regeln debuggen“ deaktiviert, sofern sie zuvor aktiviert war. Sie müssen diese Option nach dem Upgrade aktivieren.

Die folgende Abbildung zeigt den Abschnitt „Warnmeldungs-Engine“.

So konfigurieren Sie die Warnmeldungs-Engine-Einstellungen:

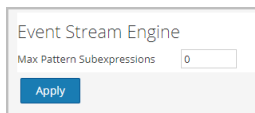
1. Geben Sie im Bereich „Warnmeldungs-Engine“ einen Wert für **Max. Bürgerereignisse** ein. Der Standardwert ist 100.
2. Wählen Sie **Regeln debuggen?** aus, um das Debugging von Regeln zu aktivieren.
3. Wenn die Warnmeldungen an den Nachrichtenbus und an Respond gesendet werden sollen, aktivieren Sie die Option **Warnmeldungen an Nachrichtenbus weiterleiten**.
4. Sie können die maximale Anzahl der an den Nachrichtenbus weiterzuleitenden Warnmeldungen für die Testregel angeben, indem Sie **Maximale Warnmeldungen pro Sekunde für eine Testregel** auswählen. Der Standardwert ist 10.
5. Klicken Sie auf **Anwenden**, um Änderungen zu speichern und sofort umzusetzen.

**Hinweis:** Weitere Informationen zu den Parametern im Bereich „Warnmeldungs-Engine“ finden Sie unter „Einstellungen der Warnmeldungs-Engine“ in der erweiterten ESA-Ansicht.

### Konfigurieren der Einstellungen für die Ereignis-Stream-Engine

Im Abschnitt „Ereignis-Stream-Engine“ geben Sie Details an, um die Performance zu verbessern.

Die folgende Abbildung zeigt den Abschnitt „Ereignis-Stream-Engine“.



So konfigurieren Sie die Einstellungen für die Ereignis-Stream-Engine:

1. Geben Sie im Abschnitt „Ereignis-Stream-Engine“ einen Wert unter **Max. Muster-Teilausdrücke** ein.
2. Klicken Sie auf **Anwenden**, um Änderungen zu speichern und sofort umzusetzen.

**Hinweis:** Weitere Informationen zu den Parametern im Bereich „Ereignis-Stream-Engine“ finden Sie unter „Einstellungen der Ereignis-Stream-Engine“ in der erweiterten ESA-Ansicht.

## Konfigurieren von ESA Analytics

---

In diesem Abschnitt werden die Hauptaufgaben zur Konfiguration von ESA Analytics-Services für die automatisierte Bedrohungserkennung von RSA NetWitness® Suite beschrieben. Mit der Funktion der automatisierten Bedrohungserkennung können Sie die Daten auf einem oder mehreren Concentrators analysieren, indem Sie vorkonfigurierte ESA Analytics-Module verwenden wie z. B. „Suspicious Domains“. Beispielsweise kann ein ESA Analytics-Service mithilfe eines Moduls „Suspicious Domains“ Ihren HTTP-Datenverkehr untersuchen, um die Wahrscheinlichkeit dafür zu ermitteln, dass böswillige Aktivitäten in Ihrer Umgebung stattfinden.

Es gibt zwei ESA-Services, die auf einem ESA-Host ausgeführt werden können:

- Event Stream Analysis (ESA-Korrelationsregeln)
- Event Stream Analytics Server (ESA Analytics)

Der erste Service ist der Event Stream Analysis-Service, der Warnmeldungen aus ESA-Regeln, auch bekannt als ESA-Korrelationsregeln, erstellt, die Sie manuell erstellen oder von Live herunterladen. Der zweite Service ist der ESA Analytics-Service, der für die automatisierte Bedrohungserkennung verwendet und in diesem Abschnitt konfiguriert wird. Da der ESA Analytics-Service für die automatisierte Bedrohungserkennung vorkonfigurierte ESA Analytics-Module verwendet, müssen Sie keine Regeln erstellen oder herunterladen, um ihn verwenden zu können.

Derzeit sind zwei ESA Analytics-Module verfügbar, beide für verdächtige Domains:

- C2 für Pakete (http-packet)
- C2 für Protokolle (http-log)

## Konfigurieren des Whois-Abfrageservice

Die Funktionen zur automatisierten Bedrohungserkennung von RSA NetWitness Suite ermöglichen es Ihnen, Datenquellen automatisch zu analysieren, indem Sie vorkonfigurierte ESA Analytics-Module verwenden. Ein ESA Analytics-Modul ist eine Pipeline aus Aktivitätsobjekten, die ein Ereignis durch mathematische Berechnungen um zusätzliche Informationen ergänzen. ESA Analytics-Services verarbeiten diese Module, um Advanced Threats zu ermitteln.

Die Konfiguration des Whois-Abfrageservice ist für Suspicious Domains-Module erforderlich.

**Hinweis: (Wichtig)** RSA empfiehlt dringend die Konfiguration des Whois-Abfrageservice für mehr Genauigkeit bei der Bewertung der automatisierten Bedrohungserkennung.

## Voraussetzungen

- Zur Nutzung des Whois-Abfrageservice benötigen Sie ein RSA Live-Konto.
- Der ESA Analytics-Server-Service muss in der Ansicht „ADMIN > Services“ verfügbar sein (ein grüner Kreis wird angezeigt).


Wenn Sie ein Live-Konto im Bereich „Live-Services“ konfiguriert haben (ADMIN > System > Live-Services), wird der Whois-Abfrageservice automatisch für Sie konfiguriert. Sie müssen nur die Verbindung des Whois-Abfrageservice überprüfen.

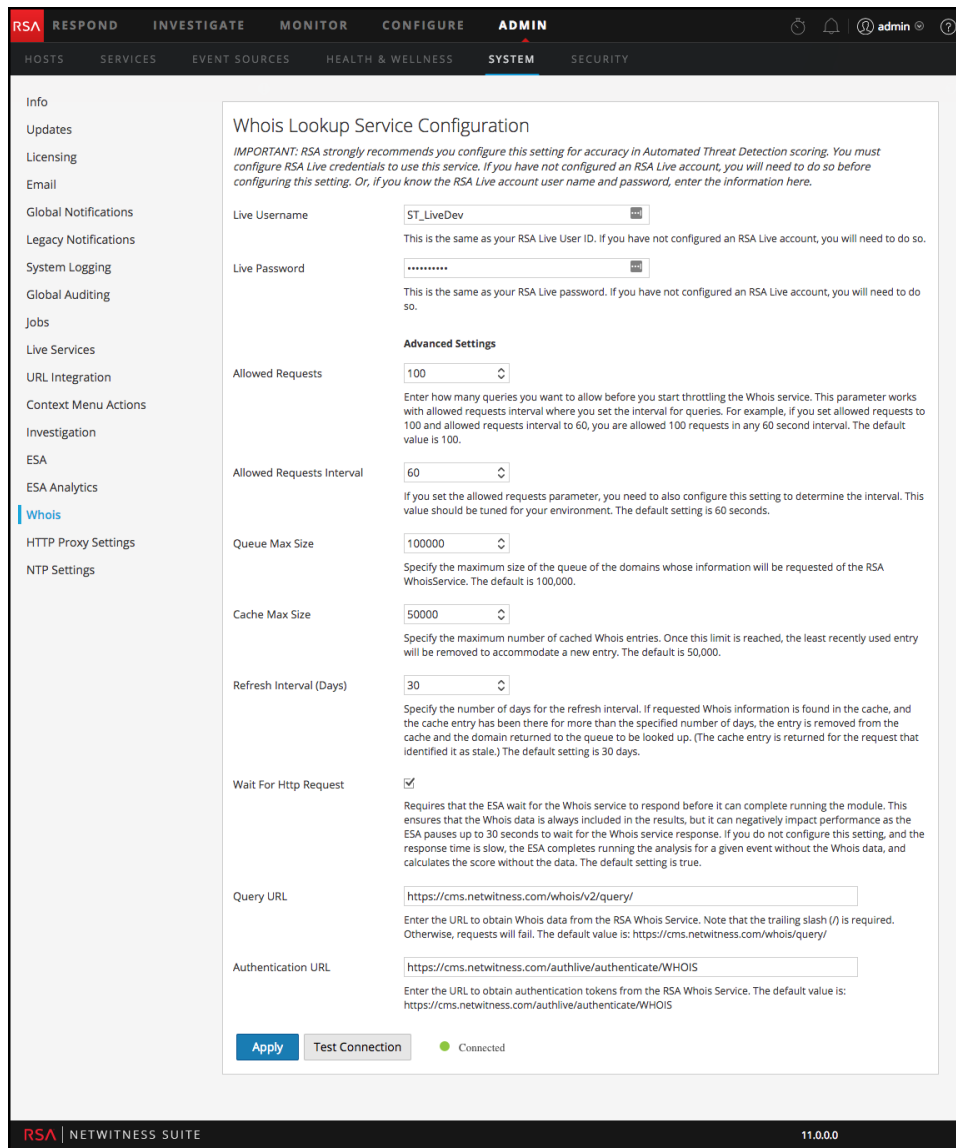
**Hinweis:** Wenn Sie kein RSA Live-Konto besitzen, können Sie eines im RSA Live-Registrierungsportal erstellen:

<https://cms.netwitness.com/registration/>

Im *Handbuch Live Services Management* finden Sie zusätzliche Informationen.

## Konfigurieren des Whois-Abfrageservice

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ **Whois** aus.
3. Überprüfen Sie im Bereich **Konfiguration des Whois-Abfrageservice**, ob der Whois-Abfrageservice verbunden ist. Am unteren Rand des Bereichs wird ein verbundener Service durch einen grünen Kreis neben **Verbunden** angezeigt:  Connected



Wenn er verbunden ist, können Sie die Konfiguration als abgeschlossen betrachten und die restlichen Schritte überspringen. Um die erweiterten Einstellungen anzupassen, fahren Sie mit Schritt 5 fort.

Wenn der Service nicht verbunden ist, fahren Sie mit Schritt 4 fort.

4. Geben Sie in den Feldern **Live-Benutzername** und **Live-Passwort** die Anmeldedaten Ihres RSA Live-Kontos ein, um auf den RSA Whois-Server zuzugreifen.
5. Falls erforderlich, können Sie die erweiterten Einstellungen anpassen. RSA empfiehlt jedoch, dass Sie die Standardwerte verwenden. Unter [Konfiguration des Whois-Abfrageservice](#) finden Sie weitere Details.
6. Klicken Sie auf **Verbindung testen**, um die Verbindung zu testen.  
Eine erfolgreiche Verbindung wird durch grünen Kreis neben **Verbunden** angezeigt: ● Connected

7. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.



## Zuordnen von ESA-Datenquellen zu Analytics-Modulen

In diesem Thema erfahren Administratoren, wie sie bestimmte ESA Analytics-Module verschiedenen Datenquellen und ESA Analytics-Services zuordnen können, um die Verarbeitung effizienter zu gestalten.

Sie können die Daten auf einem oder mehreren Concentrators mit der RSA NetWitness Suite-Funktion zur automatischen Bedrohungserkennung analysieren, indem Sie ein vorkonfiguriertes ESA Analytics-Modul auswählen. Die mit diesen Modulen analysierten Daten werden zum Identifizieren von Advanced Threats verwendet. Um Netzwerkressourcen besser nutzen zu können und unnötige Datenflüsse zu reduzieren, können Sie mehrere Datenquellen wie Concentrators mehreren ESA Analytics-Services zuordnen, um Daten effizienter zu verarbeiten und zusätzliche Kapazitäten zu nutzen.

Ein *ESA Analytics-Modul* ist eine Pipeline aus Aktivitätsobjekten, die ein Ereignis durch mathematische Berechnungen um zusätzliche Informationen ergänzen. ESA Analytics-Module befinden sich in den ESA Analytics-Services.

Bei der Bereitstellung einer Zuordnung nutzt der ausgewählte ESA Analytics-Service die abfragebasierte Aggregation, um die entsprechenden gefilterten Ereignisse für das ausgewählte Modul von den Concentrators zu erfassen. Abfragebasierte Aggregation ist eine vordefinierte Abfrage, die nur für das ausgewählte ESA Analytics-Modul Daten überträgt. Nur die vom Modul benötigten Daten werden zwischen dem Concentrator und dem ESA Analytics-System übertragen.

Derzeit sind zwei ESA Analytics-Module für verdächtige Domains verfügbar: C2 für Pakete (http-packet) und C2 für Protokolle (http-log).

### Modulbereitstellungsbeispiel: zwei ESAs

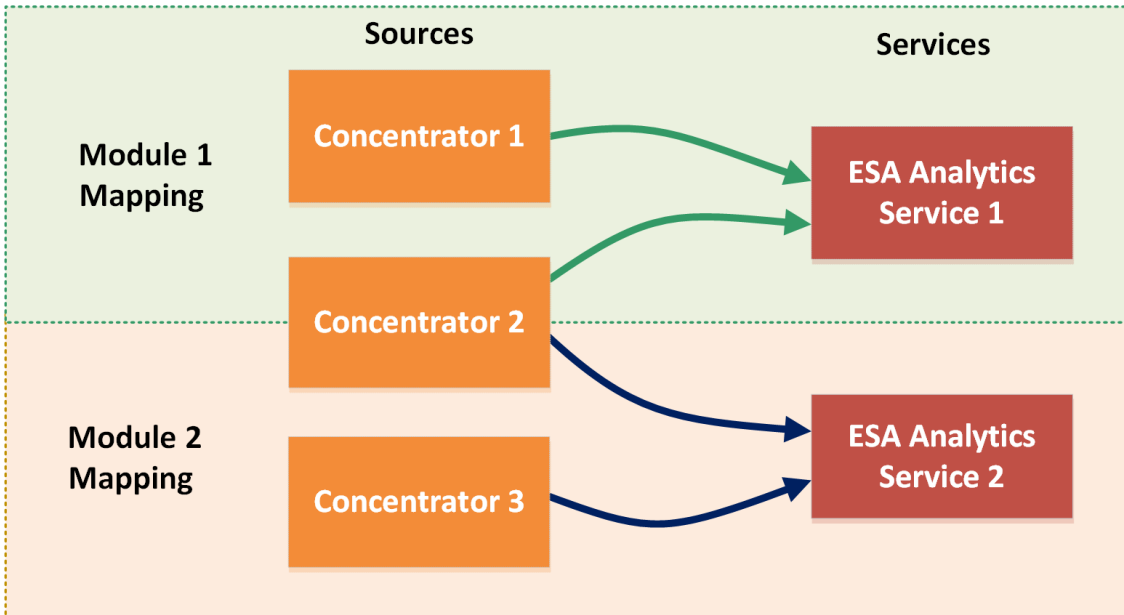
Um die zusätzliche Concentrator-Kapazität zu nutzen, können Sie ein ESA Analytics-Modul einem ESA Analytics-Service zuordnen und es zur Analyse von Daten aus verschiedenen Datenquellen zur gleichen Zeit bereitstellen.

Wenn Sie z. B. über drei Concentrators und zwei ESA Analytics-Services verfügen, können Sie die folgenden Zuordnungen erstellen und bereitstellen:

- Ordnen Sie Modul 1 den Quellen Concentrator 1 und 2 sowie dem ESA-Analytics-Service 1 zu. ESA Analytics Service 1 analysiert die von Modul 1 gefilterten Ereignisse aus den Concentrators 1 und 2.
- Ordnen Sie Modul 2 den Quellen Concentrator 2 und 3 sowie dem ESA-Analytics-Service 2 zu. ESA Analytics Service 2 analysiert die von Modul 2 gefilterten Ereignisse aus den Concentrators 2 und 3.

In diesem Beispiel steht Modul 1 für ein ESA Analytics-Modul, z. B. C2 für Pakete (http-packet), und Modul 2 steht für ein anderes ESA Analytics-Modul, z. B. C2 für Protokolle (http-logs) an einen anderen Speicherort.

### Module Deployment Example – Two ESAs



Dieses Beispiel zeigt, wie beide Services Daten aus dem gleichen Concentrator verarbeiten können. Beachten Sie, dass die beiden ESA Analytics-Services 1 und 2 Prozessdaten aus Concentrator 2 verarbeiten können. ESA Analytics-Service 1 fragt Daten für Ereignisse von Modul 1 ab und ESA Analytics-Service 2 andere Daten für Ereignisse von Modul 2.

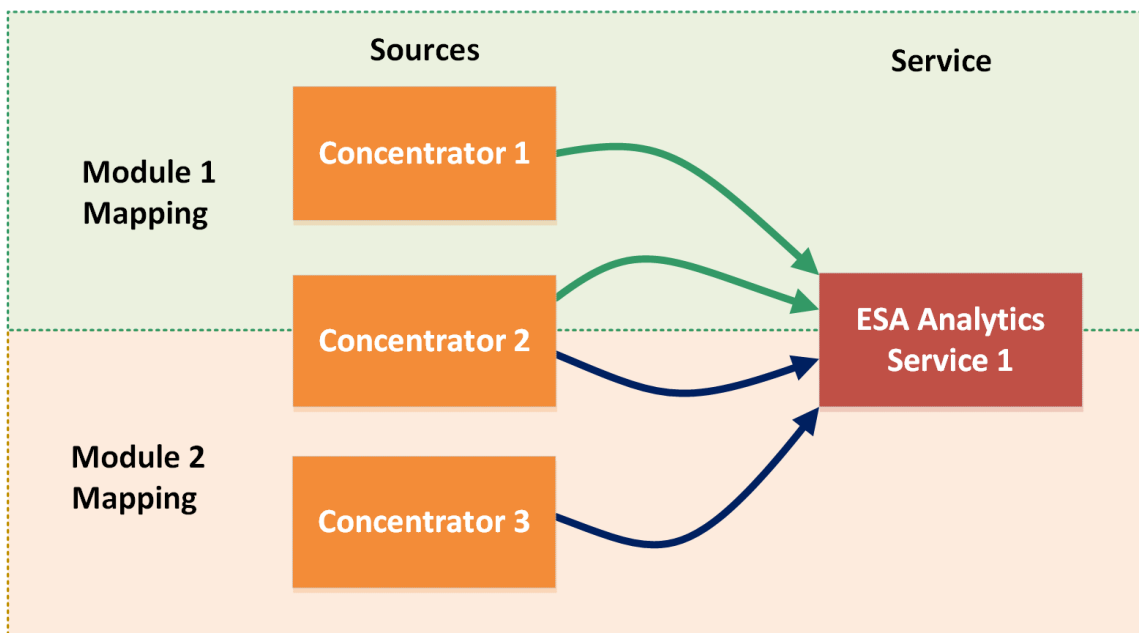
### Modulbereitstellungsbeispiel: ein ESA

Neben der Erstellung von Modulzuordnungen, die von verschiedenen ESA Analytics-Services verarbeitet werden, können Sie dem gleichen ESA Analytics-Service mehrere Module zuordnen.

Wenn Sie z. B. über drei Concentrators und einen ESA Analytics-Service verfügen, können Sie die folgenden Zuordnungen erstellen und bereitstellen:

- Ordnen Sie Modul 1 den Quellen Concentrator 1 und 2 sowie dem ESA-Analytics-Service 1 zu. ESA Analytics-Service 1 analysiert die von Modul 1 gefilterten Ereignisse aus den Concentrators 1 und 2.
- Ordnen Sie Modul 2 den Quellen Concentrator 2 und 3 sowie dem ESA-Analytics-Service 1 zu. ESA Analytics-Service 1 verarbeitet außerdem die von Modul 2 gefilterten Ereignisse aus den Concentrators 2 und 3.

## Module Deployment Example – One ESA



Dieses Beispiel zeigt, wie ein Service Daten von mehr als einem Modul verarbeiten kann. Beachten Sie, dass ESA Analytics-Service 1 Prozessdaten aus Concentrator 1 und 2 für Modul 1 verarbeiten kann. Er verarbeitet außerdem die Daten von Concentrator 2 und 3 für Modul 2. ESA Analytics-Service 1 fragt Daten für Ereignisse von Modul 1 ab und andere Daten für Ereignisse von Modul 2.

**Achtung:** Stellen Sie sicher, dass alle NetWitness Suite-Hostservices mit einer konsistenten Zeitquelle synchronisiert werden.

### Voraussetzungen

- Alle NetWitness Suite-Hostservices müssen mit einer konsistenten Zeitquelle synchronisiert werden.
- Concentrator-Hosts und -Services müssen erkannt werden und in der NetWitness Suite-Benutzeroberfläche verfügbar sein.
- Alle modulspezifischen Anforderungen müssen eingehalten werden.
  - Für das Modul „Suspicious Domains“:
    - Konfigurieren Sie die Einstellungen für Protokolle („Suspicious Domains“ nur für Protokolle).
    - Erstellen Sie eine Whitelist (optional) mithilfe des Service „Context Hub“.

- [Konfigurieren des Whois-Abfrageservice](#).
- Überprüfen Sie, ob die C2-Incident Regel aktiviert ist, und überwachen Sie sie auf Aktivität.
- Überprüfen Sie, ob Incidents nach verdächtigen C&C gruppiert sind.

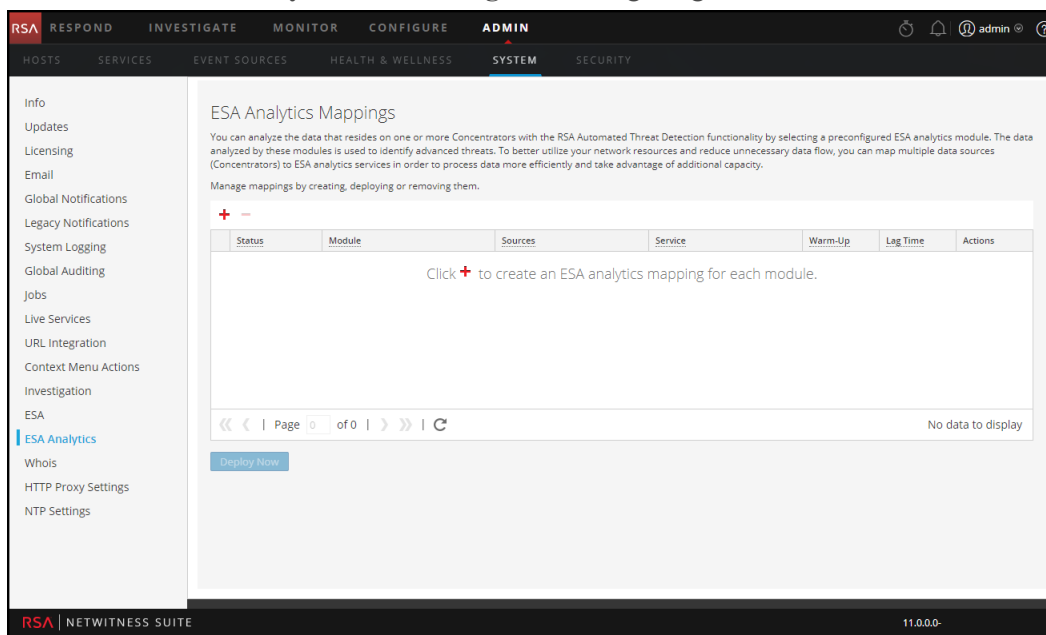
Eine schrittweise Anleitung finden Sie im Leitfaden *NetWitness Suite Automatisierte Bedrohungserkennung*.

## Erstellen von ESA Analytics-Zuordnungen

Das folgende Verfahren dient zur Zuordnung von ESA Analytics-Modulen zu Quellen und Services. Nach dem Erstellen und Überprüfen der Zuordnungen stellen Sie diese bereit, damit sie mit der Aggregation von Daten beginnen können.

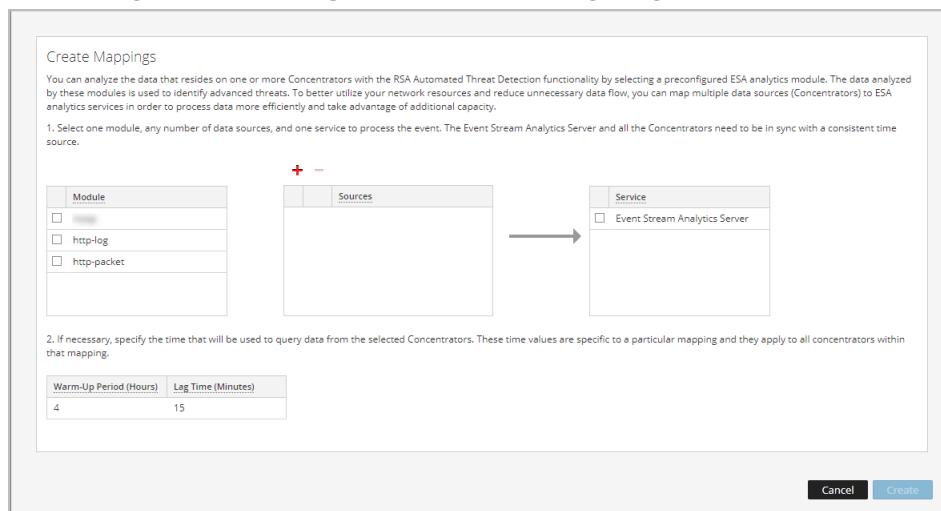
1. Navigieren Sie zu **ADMIN > SYSTEM** und wählen Sie im Bereich „Optionen“ **ESA Analytics** aus.

Der Bereich **ESA Analytics-Zuordnungen** wird angezeigt.



2. Klicken Sie auf **+**, um eine ESA Analytics-Zuordnung zu erstellen. Erstellen Sie eine separate Zuordnung für jedes Modul.

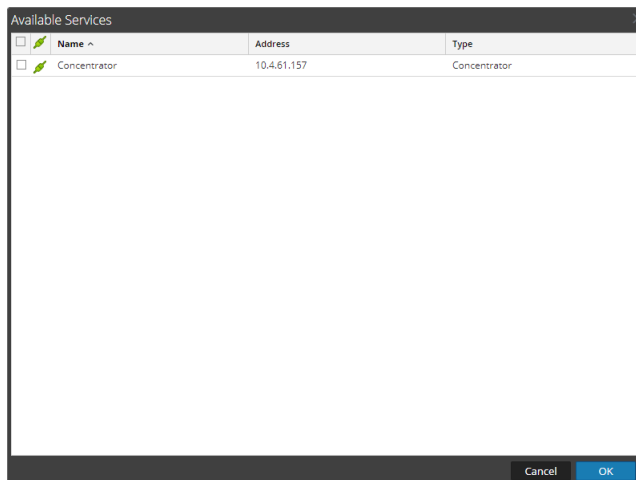
Das Dialogfeld **Zuordnungen erstellen** wird angezeigt.



3. Wählen Sie in der Auswahlliste **Modul** ein Modul aus.
4. Konfigurieren Sie eine oder mehrere Datenquellen (Concentrators) für Ihre Zuordnungen. Gehen Sie für jeden Concentrator wie folgt vor:

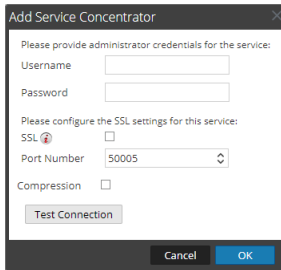
- a. Klicken Sie auf **+**.

Das Dialogfeld „Verfügbare Quellen“ zeigt die Datenquellen an, die aus der Ansicht „Admin > Services“ zur Verfügung stehen.

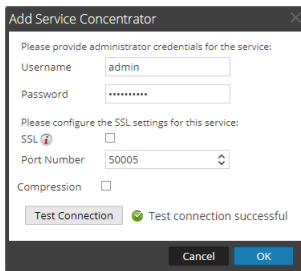


- b. Wählen Sie im Dialogfeld **Verfügbare Quellen** einen Concentrator aus und klicken Sie auf **OK**.

Das Dialogfeld „Quelle hinzufügen“ wird angezeigt.



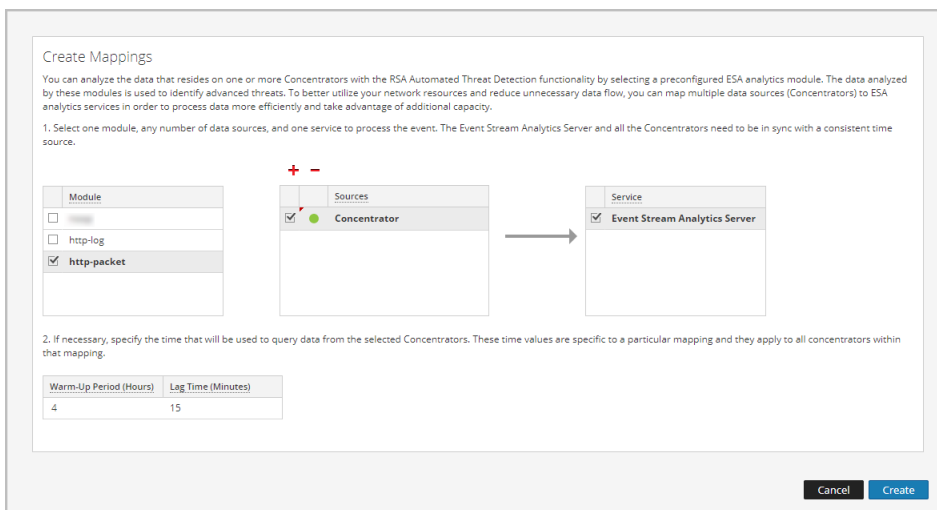
- c. Im Dialogfeld **Quelle hinzufügen** geben Sie den Benutzernamen und das Passwort für den Concentrator ein.
- d. Klicken Sie auf **Verbindungstest**, um sicherzustellen, dass die Quelle mit dem ESA Analytics-Service kommunizieren kann.



- e. Klicken Sie auf **OK**.

Nachdem Sie die Datenquellen konfiguriert haben und diese in der Liste „Quellen“ angezeigt werden, können Sie sie für weitere Zuordnungen wiederverwenden.

- 5. Wählen Sie in der Liste **Quellen** eine oder mehrere Datenquellen zum Aggregieren von Daten für das Modul aus.



Ein vollfarbiger grüner Kreis zeigt an, dass ein Service ausgeführt wird, und ein weißer Kreis zeigt einen gestoppten Service an.

6. In der Liste **Service** wählen Sie einen ESA Analytics-Service zum Verarbeiten der Daten für das Modul aus.
7. Geben Sie falls nötig die Zeit an, die zur Abfrage von Daten aus den ausgewählten Concentrators verwendet werden soll:

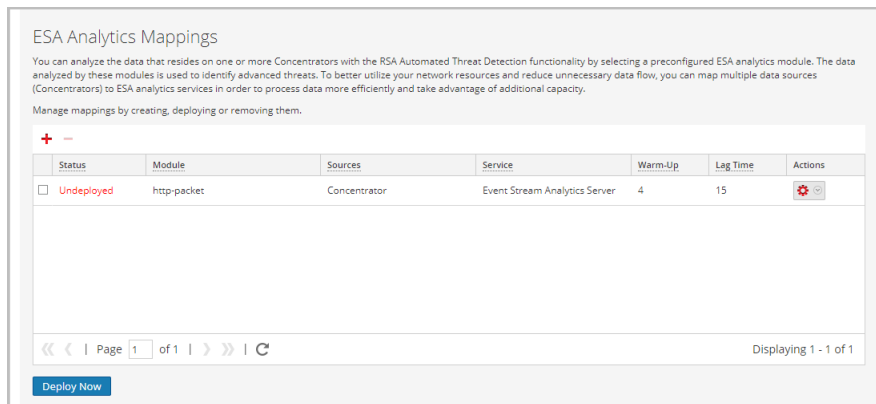
Feld	Beschreibung
Aufwärmzeit (Stunden)	<p>Gibt eine Dauer für die Aufwärmphase (in Stunden) an. Eine Aufwärmphase ist erforderlich, damit die automatisierte Bedrohungserkennung Ihren Datenverkehr „kennenlernen“ kann. Die Aufwärmphase sollte ausgeführt werden, wenn der typische Datenverkehr ausgeführt wird. Während dieser Zeit werden Warnmeldungen für die Zuordnung von Modulen unterdrückt. Die Aufwärmzeit bereitet das Modul mit Verlaufsdaten vor und sorgt dafür, dass die Datenerfassung auch wirklich die angegebene Anzahl an Stunden dauert, bevor Warnmeldungen gesendet werden.</p> <p>RSA bietet vorkonfigurierte ESA Analytics-Module. Für jeden Modultyp ist eine standardmäßige Aufwärmphase definiert, die Sie bei Bedarf an Ihre Umgebung anpassen können. Nach dieser Aufwärmphase können Warnmeldungen angezeigt werden.</p> <p>Weitere Informationen zu Aufwärmphase und Verzögerungszeit finden Sie unter <a href="#">Moduleinstellungen</a>.</p>

Feld	Beschreibung
Verzögerungszeit (Minuten)	<p>Gibt eine konstante Verzögerungszeit in Minuten an, die hinzugefügt wird, um zu vermeiden, dass Ereignisse, die in Zeiten mit hoher Aktivität von den Datenquellen verarbeitet werden, verloren gehen. Beispielsweise variiert die Concentrator-Performance in Abhängigkeit von Faktoren wie der eingehenden Last, laufenden Abfragen und Indexierung. Aufgrund von diesen Faktoren aggregiert ein Concentrator Ereignisse möglicherweise nicht in Echtzeit, was zu der Verzögerung führt.</p> <p>Der Verzögerungsparameter verschafft dem Concentrator die Möglichkeit, die Aggregation aller Daten abzuschließen.</p> <p>Nach Abschluss der Aufwärmphase wird die Datenaggregation mit der <b>aktuellen (System-)Zeit – Verzögerungszeit</b> fortgesetzt. Das ist hilfreich, wenn ein Concentrator bei der Datenaggregation langsam ist. Die Verzögerungszeit stellt sicher, dass das Modul keine Daten verarbeitet, die innerhalb des Verzögerungszeitfensters auf dem Concentrator eintreffen. Auf diese Weise ist eine ausreichende Verzögerung gegeben, damit alle Ereignisse, die im Unternehmen erzeugt werden, vom Modul verarbeitet werden können.</p> <p>Wenn beispielsweise für die Verzögerung 30 Minuten und für die aktuelle Zeit 14:00 Uhr angegeben werden, beginnt der Concentrator um 13:30 Uhr mit dem Abrufen von Datensätzen. Das Verzögerungszeitfenster, in diesem Beispiel 30 Minuten, bleibt im Zeitverlauf konstant. Wenn die aktuelle Zeit auf 14:01 Uhr vorrückt, ruft der Concentrator die nächste Minute von Daten um 13:31 Uhr ab und so weiter.</p> <p><b>Wichtig:</b> Die Verzögerungszeit definiert den Puffer zwischen der aktuellen Zeit und der Zeit, zu der das Modul die Daten aufnimmt.</p> <div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;"> <p><b>Achtung:</b> RSA empfiehlt, dass Administratoren die Verzögerungsparameter basierend auf der Performance jedes einzelnen Concentrator dynamisch anpassen, um zu vermeiden, während der Aggregation Ereignisse zu vergessen.</p> </div> <p>Weitere Informationen zu Aufwärmphase und Verzögerungszeit finden Sie unter <a href="#">Moduleinstellungen</a>.</p>

8. Klicken Sie auf **Erstellen**.

Die Zuordnungen, die Sie erstellen, werden in der Liste der vorhandenen Zuordnungen mit dem Status **Nicht bereitgestellt** angezeigt.





**Wichtig:** Um ein Modul so zu starten, dass es mit der Aggregation von Daten beginnt, müssen Sie es bereitstellen.

## Bereitstellen von ESA Analytics-Zuordnungen

Nachdem Sie Ihre Zuordnungen erstellt haben, müssen Sie sie bereitstellen, um die Aggregation von Daten für die Module starten zu können.

1. Überprüfen Sie in der Liste der Zuordnungen, ob der Status der Zuordnungen, die Sie bereitstellen möchten, **Nicht bereitgestellt** lautet.
2. Wählen Sie eine oder mehrere Zuordnungen mit dem Status „Nicht bereitgestellt“ aus und klicken Sie auf **Jetzt bereitstellen**.

Alle ausgewählten Zuordnungen mit dem Status „Nicht bereitgestellt“ beginnen mit dem Aggregieren von Daten, wie in der Zuordnung konfiguriert. Der Zuordnungsstatus ändert sich zu **Bereitgestellt**.

Sie können keine Zuordnung bereitstellen, die bereits bereitgestellt wurde.

## Aktualisieren einer Zuordnung

Pro Modul ist nur eine Zuordnung zulässig. Wenn Sie Änderungen an einer bereitgestellten Zuordnung vornehmen möchten, z. B. Concentrators hinzufügen oder entfernen oder den Service ändern, müssen Sie die Bereitstellung der vorhandenen Zuordnung aufheben und die Zuordnung löschen und dann eine neue Zuordnung für dieses Modul erstellen und bereitstellen.

Sie können die folgenden Aktualisierungen an einer bereitgestellten Zuordnung vornehmen, ohne sie zu löschen:

- Aufheben der Bereitstellung einer Zuordnung
- Ändern der Aufwärmphase und der Verzögerungszeit



Sie können auch die Aufwärmphase und die Verzögerungszeit für eine nicht bereitgestellte Modulzuordnung ändern.

## Aufheben der Bereitstellung einer Zuordnung

Wenn Sie das Aggregieren von Daten für eine Modulzuordnung beenden, die Zuordnung aber nicht löschen möchten, können Sie die Bereitstellung aufheben. Dies bietet Ihnen die Möglichkeit, sie zu einem späteren Zeitpunkt bereitzustellen. Wenn Sie die Bereitstellung einer Zuordnung aufheben, stoppt der angegebene ESA Analytics-Service das Abrufen von Daten aus den Datenquellen für dieses Modul.

**Achtung:** Das Aufheben der Bereitstellung einer Zuordnung mit dem Status „Bereitgestellt“ wirkt sich auf die Datenaggregation für dieses Modul aus.

### So heben Sie die Bereitstellung einer Zuordnung auf:

1. Wählen Sie im Bereich „ESA Analytics-Zuordnungen“ die Zuordnung aus, deren Bereitstellung Sie aufheben möchten.
2. Wählen Sie in der Spalte **Aktionen** die Option   > **Bereitstellung aufheben** aus.  
Der Status ändert sich von „Bereitgestellt“ zu „Nicht bereitgestellt“ und die Datenaggregation wird beendet.


## Löschen einer Zuordnung

Sie können eine Zuordnung mit dem Status „Nicht bereitgestellt“ zu einem beliebigen Zeitpunkt löschen. Da eine Zuordnung mit dem Status „Nicht bereitgestellt“ nicht ausgeführt wird, ergeben sich keine Auswirkungen auf die Datenaggregation.

Sie müssen die Bereitstellung einer Zuordnung mit dem Status „Bereitgestellt“ aufheben, bevor Sie sie löschen. Durch das aufheben der Bereitstellung und das Löschen einer bereitgestellten Zuordnung wird die Konfiguration auf dem ESA-Server gelöscht, die Bereitstellung für diese Zuordnung zurückgesetzt und das Abrufen von Daten aus der Datenquelle für dieses Modul gestoppt.

**Achtung:** Das Aufheben der Bereitstellung und das Löschen einer Zuordnung wirkt sich auf die Datenaggregation für dieses Modul aus.



### So löschen Sie eine Zuordnung:

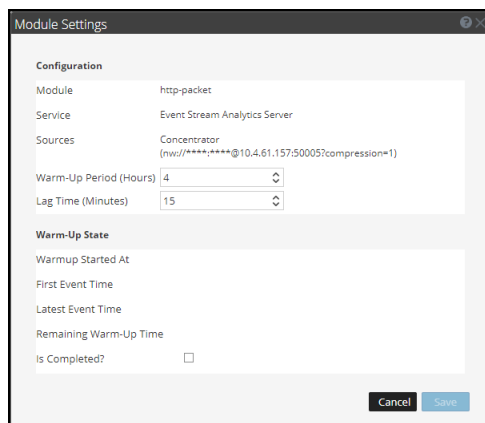
1. Wählen Sie im Bereich „ESA Analytics-Zuordnungen“ die Zuordnung aus, die Sie löschen möchten. Sie können jeweils immer nur eine Zuordnung löschen.
2. Klicken Sie auf  .

## Ändern der Aufwärmphase und der Verzögerungszeit

Eventuell möchten Sie die Aufwärmphase für eine spezifische Modulzuordnung anpassen. Zum Beispiel können Sie, nachdem die Aufwärmphase abgeschlossen ist, die Einstellung für die Aufwärmphase erhöhen, um zusätzliche Aufwärmzeit zu ermöglichen. Sie können die Aufwärmphase sogar dann verlängern, wenn die Modulzuordnung aktiv aufgewärmt wird.





Falls erforderlich, können Sie die Verzögerungszeit für das Modul ändern. Die Verzögerungszeit definiert den Puffer zwischen der aktuellen Zeit (Systemzeit) und der Zeit, zu der das Modul die Daten aufnimmt.

1. Wählen Sie im Bereich „ESA Analytics-Zuordnungen“ die Zuordnung aus, die Sie ändern möchten, und wählen Sie in der Spalte **Aktionen** die Option   > **Modul bearbeiten**. Das Dialogfeld „Moduleinstellungen“ zeigt das ausgewählte Modul, den ESA Analytics-Service und die Datenquellen für die Zuordnung an. Die Datenquellen zeigen die für die Kommunikation mit ESA verwendeten URLs an.



2. Überprüfen Sie den Abschnitt **Aufwärmzustand**, um den aktuellen Aufwärmzustand zu bestimmen:
  - **Aufwärmen gestartet um** – Die Zeit, zu der das erste Event vom ESA Analytics-Modul aus der Datenquelle verarbeitet wurde.
  - **Zeit des ersten Ereignisses** – Die Uhrzeit des ersten Ereignisses. Die Aufwärmphase basiert auf dieser Uhrzeit.
  - **Zeit des letzten Ereignisses** – Die Uhrzeit des letzten Ereignisses.
  - **Verbleibende Aufwärmzeit** – Die Anzahl der in der Aufwärmphase verbleibenden Stunden.
  - **Abgeschlossen?** – Gibt an, ob die Aufwärmphase abgeschlossen ist. Bei „true“ ist die Aufwärmphase abgeschlossen. Bei „false“ wird das Modul weiterhin aufgewärmt und Sie

können die Anzahl der verbleibenden Stunden im Feld „Verbleibende Aufwärmzeit“ anzeigen.

3. Im Abschnitt **Konfiguration** können Sie abhängig davon, ob die Aufwärmphase abgeschlossen ist, die **Aufwärmzeit (Stunden)** aktualisieren.
  - **Während der Aufwärmphase** – Sie können der Aufwärmphase Stunden hinzuzufügen oder verbleibende Aufwärmzeit abziehen.
  - **Abschluss der Aufwärmphase** – Sie können der Aufwärmphase Stunden hinzufügen, indem Sie die Differenz zwischen der aktuellen Zeit und der Zeit des ersten Ereignisses zu den Stunden hinzufügen, die Sie hinzufügen möchten.  
 Zum Beispiel ist eine Aufwärmphase 10 Stunden abgeschlossen und die Zeit des ersten Ereignisses lautet 12:00:00. Die aktuelle Zeit lautet 16:00:00 (4 Stunden später) und Sie möchten der Aufwärmphase 5 weitere Stunden hinzufügen. Um dies zu erreichen, müssen Sie der Aufwärmphase von 10 Stunden 9 Stunden hinzufügen ( $4+5 = 9$ ), sodass die neue Aufwärmphase auf 19 Stunden festgelegt wird.  
 Sie können die Aufwärmphase nicht reduzieren, wenn sie abgeschlossen ist, sofern Sie nicht die Zuordnung löschen und eine neue erstellen.
4. Falls erforderlich, ändern Sie die **Verzögerungszeit (Minuten)**, um den Concentrators in der Zuordnung zusätzliche Zeit zum Fertigstellen der Aggregation aller Daten zu bieten.
5. Klicken Sie auf **Speichern**.  
 Die Änderungen treten nicht sofort in Kraft. Damit die Einstellungen wirksam werden, müssen Sie die Bereitstellung aufheben und die Zuordnung erneut bereitstellen.
6. Um die Bereitstellung einer Zuordnung aufzuheben, wählen Sie im Bereich „ESA Analytics-Zuordnungen“ die entsprechende Zuordnung aus und klicken dann auf   >  
**Bereitstellung aufheben.**  
 Die Datenaggregation wird für die ausgewählte Zuordnung beendet.
7. Wenn Sie die Zuordnung erneut bereitstellen möchten, wählen Sie sie aus und klicken auf   > **Bereitstellen.**  
 Die ausgewählte Zuordnung wird bereitgestellt und beginnt mit dem Aggregieren von Daten, wie in der Zuordnung konfiguriert.

## Zusätzliche Verfahren für ESA-Korrelationsregeln

---

Dieses Thema ist eine Sammlung einzelner Verfahren, die ein Administrator jederzeit durchführen kann, und es ist nicht erforderlich, dass sie die anfängliche Einrichtung der ESA-Korrelationsregeln abschließen.

Verwenden Sie diesen Abschnitt, wenn Sie nach Anweisungen suchen, um eine bestimmte Aufgabe nach der anfänglichen Einrichtung von ESA durchzuführen.

- [Ändern des Speicherschwellenwerts für Testregeln](#)
- [Konfigurieren von ESA für die Verwendung eines Speicherpools](#)
- [Konfigurieren von ESA zur Verwendung von „Ordnen nach Erfassungszeit“](#)
- [Starten, Beenden oder erneut Starten des ESA-Services](#)
- [Auditprotokolle und Überprüfen der ESA-Komponentenversionen und -status](#)

### Ändern des Speicherschwellenwerts für Testregeln

Dieses Verfahren ist optional und gilt nur für ESA-Korrelationsregeln.

Administratoren können den Speicherschwellenwert für Testregeln anheben oder senken. Schwellenwert bezieht sich auf die Arbeitsspeichernutzung von ESA, die den ESA-Basisarbeitsspeicher, Testregeln und andere Regeln umfasst. Wenn der Schwellenwert überschritten wird, werden alle bereitgestellten Testregeln auf einem ESA-Service deaktiviert.

Sie können Testregeln verwenden, um zu überprüfen, ob eine Regel effizient ausgeführt wird und nicht übermäßig Speicher belegt, was negative Auswirkungen auf die Performance haben oder ein Beenden des Services erzwingen kann.

Standardmäßig ist der Speicherschwellenwert 85. Dies steht für den Prozentsatz des JVM (Java Virtual Memory).



- Der Speicherschwellenwert gilt pro ESA nicht pro Regel.
- Wenn der Speicherschwellenwert überschritten wird, werden alle auf dem ESA-Service ausgeführten Testregeln automatisch deaktiviert.
- Die ESA-Konfiguration verfügt über 2 Parameter für Testregeln:
  - MemoryThresholdforTrialRules
  - MemoryCheckPeriod mit einem Standardwert von 300 Sekunden

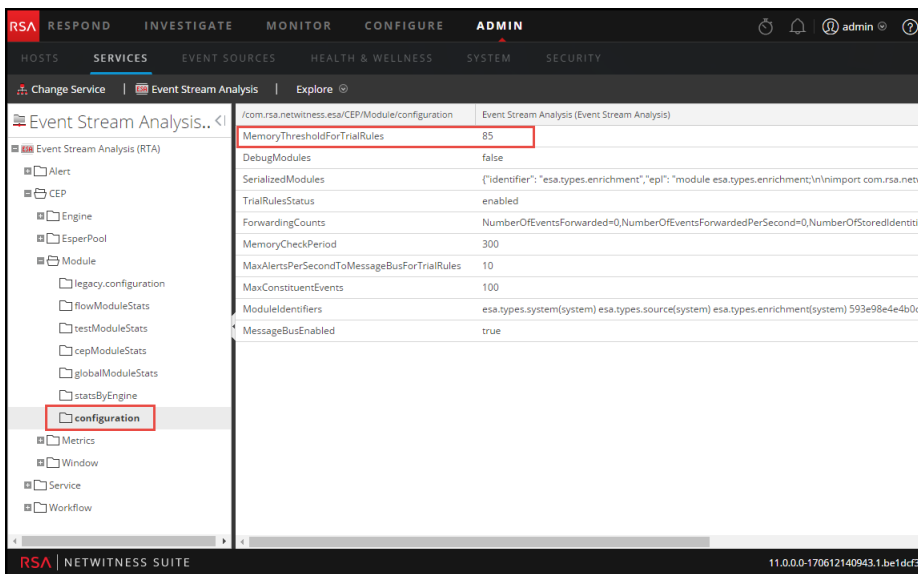
Weitere Informationen finden Sie unter „Arbeiten mit Testregeln“ im „Handbuch zum Versenden von Warnmeldungen mit ESA“.

## Voraussetzungen

Ihnen muss eine Rolle mit Administratorrechten zugewiesen sein.

## Verfahren

1. Melden Sie sich bei NetWitness Suite als Administrator an.
2. Navigieren Sie zu **ADMIN > Services**.
3. Wählen Sie den ESA-Service aus und wählen Sie   > **Ansicht > Durchsuchen** .
4. Wählen Sie auf der linken Seite **CEP > Modul > Konfiguration** aus.



5. Geben Sie im rechten Bereich unter **MemoryThresholdForTrialRules** den Prozentsatz des JVM ein, den Testregeln auf dem ESA nicht überschreiten dürfen.  
Der neue Speicherschwelldwert wird sofort wirksam.

## Konfigurieren von ESA für die Verwendung eines Speicherpools

Dieses Verfahren gilt nur für ESA-Korrelationsregeln.

Administratoren können ESA für die Verwendung eines Speicherpools konfigurieren. Ein Speicherpool ist eine kundenspezifische Implementierung des virtuellen Speichers für Ereignisse, die nach Regeln in ESA stattfinden. Dadurch kann die Fähigkeit von Regeln um ein Vielfaches erweitert werden. Wenn Sie Regeln erstellen möchten, die einen großen Zeitraum abdecken oder die sehr komplex sind, sollten Sie möglicherweise einen Speicherpool verwenden, um Speicher effizienter zu verarbeiten. Wenn Sie einen Arbeitsspeicherpool verwenden, können Ereignisse auf Festplatte geschrieben werden und müssen nicht im Arbeitsspeicher behalten werden. Das ist hilfreich, denn wenn eine Regel vorhanden ist, die komplex ist oder einen langen Zeitraum abdeckt, muss eine große Anzahl von Ereignissen im Arbeitsspeicher gespeichert werden.

Sie können die Ausführung von Speicherpools im Non-Batch-Modus oder im Batch-Modus konfigurieren:

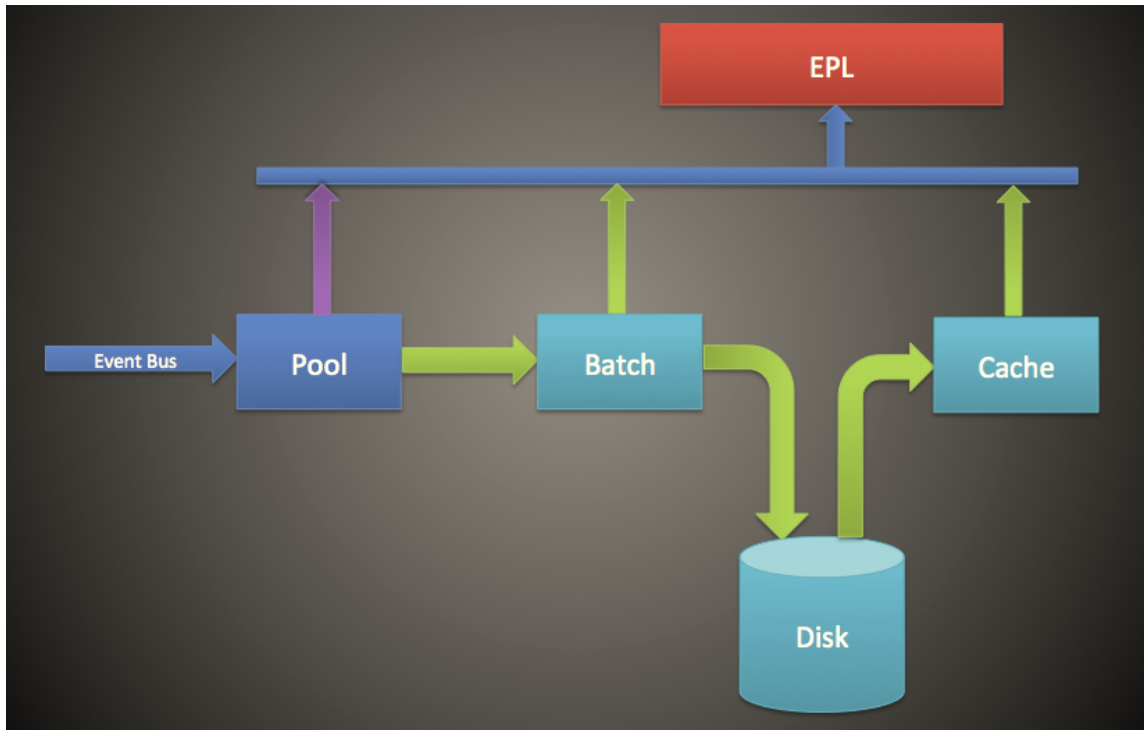
- **Non-Batch-Modus.** Im Non-Batch-Modus werden Ereignisse auf die Festplatte geschrieben, wenn sie im Speicherpool eingehen. Legen Sie zum Konfigurieren des Non-Batch-Modus das Attribut **MapPoolBatchWriteSize** auf den Wert 1 fest. Der Non-Batch-Modus bietet eine stabilere Lösung, da jedes Ereignis separat abgelegt und abgerufen wird, ohne Arbeitsspeicherspitzen zu verursachen.
- **Batch-Modus.** Im Batch-Modus werden Ereignisse in Batches gruppiert und dann auf die Festplatte geschrieben. Legen Sie zum Konfigurieren des Batch-Modus das Attribut **MapPoolBatchWriteSize** auf einen größeren Wert als 1 fest. Der Batch-Modus bietet eine bessere Performance, da die Festplattenaktivität für auf der Festplatte abgelegte Ereignisse optimiert ist.

**Hinweis:** Für alle Änderungen an diesen Einstellungen ist ein Neustart des ESA-Services erforderlich. Wenn beim Neustart von ESA aktuell Ereignisse im Speicherpool gespeichert sind, werden diese nach dem Neustart verworfen.

**Achtung:** Diese Funktion kann zwar sehr hilfreich beim Managen von Speicher sein, kann sich aber auf die Ereignisverarbeitungsgeschwindigkeit des ESA-Services auswirken. Die Performance kann zwischen 10 und 30 Prozent beeinträchtigt sein, je nach Regeln und Konfigurationseinstellungen.

### Workflow



Das folgende Diagramm zeigt den Datenfluss bei Verwendung des Speicherpools für den Batch-Modus:



1. Ereignisse werden dem Speicherpool hinzugefügt und Verweise auf die Ereignisse werden im Speicherpool gespeichert.
2. Die Ereignisse werden dann in Batches gruppiert, die auf die Festplatte gesendet werden (im Non-Batch-Modus wird dieser Schritt übersprungen).
3. Sobald der Batch den Schwellenwert erreicht hat, werden die Ereignisse auf die Festplatte geschrieben (im Non-Batch-Modus ist kein Schwellenwert erforderlich).
4. Wenn die EPL ein Ereignis erfordert, das auf die Festplatte geschrieben wurde, wird das Ereignis in den Cache übertragen und in der EPL-Regel verwendet.

## Verfahren

Führen Sie zum Konfigurieren eines ESA-Speicherpools die folgenden Schritte aus.

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie den ESA-Service aus und wählen Sie dann   > **Ansicht > Durchsuchen**.
2. Wählen Sie **CEP > EsperPool > Konfiguration**.
3. Geben Sie Werte für die folgenden Felder ein:

Attribut	Beschreibung	Konfiguration
----------	--------------	---------------



<p>MapPoolPersistenceURI</p>	<p>Speicherort zum Speichern der Speicherpooldatei.</p>	<p>Der Standardwert ist <b>/opt/rsa/esa/pool/esperPool</b>. RSA empfiehlt, den Standardwert nicht zu ändern.</p> <p>Wenn Sie diese Einstellung ändern, um eine andere Partition zu verwenden, stellen Sie sicher, dass die Partition mindestens zehnmals mehr Speicherplatz als der für ESA zugewiesene Speicher enthält.</p> <div style="border: 1px solid yellow; padding: 5px;"> <p><b>Achtung:</b> Wenn der Speicherpool in Verwendung ist, während dieser Pfad geändert wird, ist ein ESA-Neustart erforderlich. In diesem Fall verwirft ESA die gespeicherten Ereignisse nicht, was bedeutet, dass Sie diese manuell löschen müssen.</p> </div>
<p>MapPoolEnable</p>	<p>Aktivieren oder deaktivieren Sie den Speicherpool.</p>	<p>Der Standardwert ist <b>false</b>. Legen Sie den Wert auf <b>true</b> fest, um den Speicherpool zu aktivieren. Wenn Sie den Speicherpool aktivieren oder deaktivieren, ist ein Neustart erforderlich.</p>
<p>MapPoolFlushIntervalSecs</p>	<p>Zeitintervall zum Leeren von Ereignissen an die Festplatte. Beispielsweise wird jedes Ereignis, das länger als 15 Minuten in Esper verbleibt, auf die Festplatte geleert.</p>	<p>Der Standardwert ist <b>15 Minuten</b>. Ein kleinerer Wert sorgt dafür, dass der ESA-Service stabiler ist, wenn EPLs eine große Anzahl von Ereignissen im Arbeitsspeicher speichern. Ein größerer Wert (mehr als 30 Minuten) sorgt dafür, dass nur relevante Ereignisse, die über einen längeren Zeitraum erforderlich sind, auf die Festplatte geleert werden.</p> <div style="border: 1px solid green; padding: 5px;"> <p><b>Hinweis:</b> Aufgrund des Designs des Java-Speichermanagements kann es vorkommen, dass Ereignisse, die nicht von EPL verwendet werden, auf die Festplatte übertragen werden. Um dies zu verhindern, können Sie einen höheren Wert für MapPoolFlushIntervalSecs festlegen.</p> </div>

<p>MapPoolBatchWriteSize</p>	<p>Geben Sie die Batch-Größe (und ob der Batch-Modus verwendet wird) an. Die Ereignisse werden in Gruppen zusammengefasst und dann auf die Festplatte geleert.</p> <p>Zur Verwendung des Non-Batch-Modus legen Sie diesen Wert auf 1 fest.</p> <p>Zur Verwendung des Batch-Modus legen Sie diesen Wert auf einen höheren Wert als 1 fest.</p>	<p>Die Standard-Batchgröße beträgt <b>100.000</b> Ereignisse. Wenn am Ende des Leerungsintervalls die Batchkapazität nicht erreicht ist, läuft der Batch nach 30 Sekunden ab und alle Batch-Inhalte werden als Speicherpooldateien auf die Festplatte geschrieben.</p> <p>Ein kleinerer Wert für die Batchgröße (z. B. 10.000 Ereignisse) sorgt dafür, dass bei Ereignissen, die von der Festplatte abgerufen werden, kein Risiko besteht, dass sie den Speicher aufblähen, was für eine höhere Stabilität sorgt. Dagegen minimiert eine größere Batchgröße (100.000 Ereignisse) die Eingabe-/Ausgabeaktivität beim Schreiben von Ereignissen auf die Festplatte, wodurch sich die Performance verbessert.</p>
<p>MapPoolMinSize</p>	<p>Mindestgröße des Speicherpools.</p> <p>Dieser Wert wird für die Initialisierung verwendet, erfordert in der Regel also keine Bearbeitung.</p>	<p>Der Standardwert ist <b>10.000</b> Ereignisse. Ein höherer Wert kann die Performance steigern.</p> <p>Ein niedrigerer Wert sorgt dafür, dass das System stabiler ist.</p>
<p>MapPool Persist Type</p>	<p>Dies ist ein schreibgeschützter Parameter, der den Typ der verwendeten Optimierung angezeigt.</p>	<p>Der Standardwert ist <b>RMSerialize</b>.</p>

**Hinweis:** Die Wirksamkeit dieser Funktion hängt von Ihrer Umgebung ab. Wenn Sie Regeln erstellen, die einen häufigen Zugriff von Ereignissen über einen Zeitraum erfordern, kann diese Funktion die Performance verschlechtern und bietet keine oder minimale Verbesserung der Skalierbarkeit.

Speicherpooldateien werden gelöscht, wenn alle in der Pooldatei enthaltenen Ereignisse nicht mehr von einer EPL referenziert werden.

## Ergebnis

Für eine einfache EPL-Regel verbessert ESA den Speicher in der Regel um das 8- bis 9-Fache.

## Konfigurieren von ESA zur Verwendung von „Ordnen nach Erfassungszeit“

Dieses Verfahren gilt nur für ESA-Korrelationsregeln.

Administratoren können ESA für das Ordnen nach Erfassungszeit konfigurieren, wenn sie zwei oder mehr Concentrators als Quelle verwenden.

Standardmäßig verwendet ESA den ESA-Zeitstempel (Zeitpunkt, zu dem Ereignisse von ESA empfangen werden), um Ereignisse zu korrelieren. ESA unterstützt aber auch das Ordnen von Sitzungen basierend auf der Erfassungszeit (Zeitpunkt, zu dem das Paket oder Protokollereignis die Decoders erreicht hat). Diese Funktion ist nützlich, wenn Sie Ereignisse von zwei oder mehr Concentrators korrelieren möchten. Bei zwei oder mehreren Concentrators als Quellen kann mit dem Ordnen nach Zeit sichergestellt werden, dass die zugehörigen Sitzungen entsprechend der Erfassungszeit zusammen korreliert werden. Dadurch wird sichergestellt, dass Sitzungen, die gleichzeitig erfasst werden, miteinander korreliert sind und Warnmeldungen mit Benutzererwartungen konsistent sind, selbst bei Übertragungsverzögerungen. Wenn Quellen offline gehen oder zu langsam sind, um Sitzungen zu senden, hält ESA an, um sicherzustellen, dass Sitzungen mit den gleichen Erfassungszeitstempeln miteinander korreliert werden.

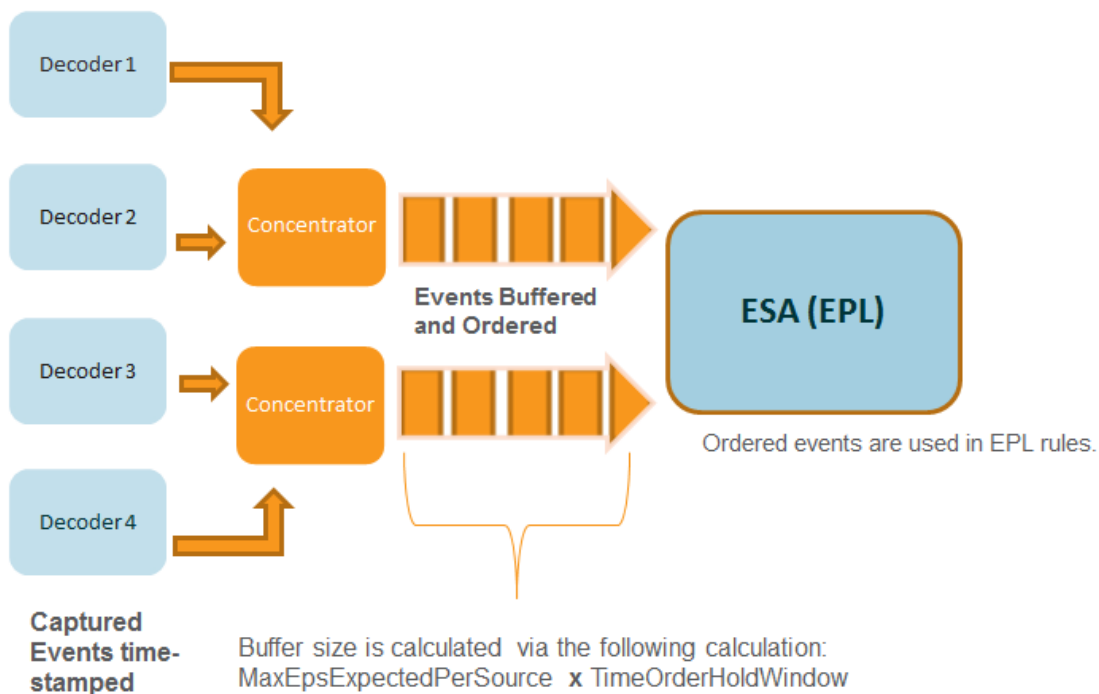
Angenommen, Sie verfügen über zwei Quellen mit Ereignissen, die um 10:00 Uhr stattfinden. Mithilfe von „Ordnen nach Erfassungszeit“ werden diese Ereignisse so lange im Puffer behalten, bis ESA erkennt, dass alle um 10:00 Uhr stattfindenden Ereignisse dem Puffer hinzugefügt wurden. Sobald alle Ereignisse eingetroffen sind, werden sie dann anhand der EPL-Regeln verarbeitet. Dadurch wird sichergestellt, dass eine Regel alle Ereignisse mit dem gleichen Zeitstempel aus verschiedenen Quellen findet und korrekte Ergebnisse erzielt werden. Wenn beispielsweise ein Concentrator hinter einem anderen zurückliegt, wird ESA angehalten, bis es über alle Ereignisse mit dem Zeitstempel 10:00 Uhr aus beiden Quellen verfügt. Erst dann werden die EPL-Regeln auf die Ereignisse angewendet.

**Achtung:** Diese Funktion erhöht zwar die Genauigkeit, beeinträchtigt aber die Performance. In der Standardkonfiguration von ESA ist vorgesehen, dass die Daten konstant gestreamt werden, da aber „Ordnen nach Erfassungszeit“ einen Puffer verwendet, dauert das Verarbeiten der Ereignisse länger. Dies gilt insbesondere, wenn ESA vorübergehend warten muss, bis sich der Puffer füllt. Es gibt verschiedene Parameter, die Sie für diese Situation konfigurieren können; trotzdem kann die Performance nach wie vor beeinträchtigt sein.

Diese Funktion ist standardmäßig deaktiviert.

### Workflow für „Ordnen nach Erfassungszeit“

Das folgende Diagramm zeigt den Workflow bei aktivierter Funktion „Ordnen nach Erfassungszeit“.



1. Ereignisse werden bei Erfassung durch den Decoder mit einem Zeitstempel versehen.
2. Nach der Concentrator-Verarbeitung werden die Ereignisse gepuffert und geordnet. Die Größe des Puffers wird wie folgt berechnet: Parameter „MaxEPSExpectedPerSource“ (der maximale Umfang des Datenverkehrs (EPS), der erwartungsgemäß **pro Quelle** von ESA empfangen wird) multipliziert mit „TimeOrderHoldWindow“ (wie lange gewartet wird, bis Ereignisse aus allen Quellen eingetroffen sind).
3. Die geordneten Ereignisse werden dann anhand von EPL-Regeln korreliert.

## Voraussetzungen

Mindestens zwei Concentrators müssen als Datenquelle in ESA konfiguriert sein.



Wenn der Parameter **StreamEnabled** auf „true“ festgelegt ist, ist es wichtig, dass bei allen Computern, auf denen Core-Services ausgeführt werden, die NTP-Synchronisierung gewährleistet ist.

## Methoden

In den folgenden Verfahren wird beschrieben, wie Sie das Ordnen nach Erfassungszeit aktivieren und konfigurieren.

### Aktivieren von Pufferung und Ordnen nach Erfassungszeit

**Hinweis:** Nach einem Upgrade oder in einer Umgebung mit hoher Ereignislast müssen Sie Datenquellen erneut hinzufügen, damit die Vorteile sichtbar werden. Alternativ müssen Sie warten, bis die Sitzungen auf dem neuesten Stand sind, bevor Sie das Ordnen nach Erfassungszeit aktivieren.

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie den ESA-Service aus und wählen Sie dann   > **Ansicht > Durchsuchen**.
2. Navigieren Sie zu **Workflow > Quelle > nextgenAggregationSource**.
3. Legen Sie das Attribut **StreamEnabled** auf **true** fest. Mithilfe von „StreamEnabled“ kann ESA Ereignisse puffern, die von Concentrators empfangen werden.
4. Legen Sie das Attribut **TimeOrdered** auf **true** fest. Dies ermöglicht, dass die gepufferten Ereignisse anhand des Zeitstempels vom Concentrator geordnet werden.

### Konfigurieren des Ordners nach Erfassungszeit

Für das Ordnen nach Erfassungszeit benötigen Sie noch verschiedene andere Parameter, um eine gute Performance zu gewährleisten. In der folgenden Tabelle sind die Parameter und ihre Funktionen aufgelistet. Das Konfigurieren dieser Parameter erfordert Kenntnisse über das Volumen und die Rate Ihres Netzwerkverkehrs.



**Hinweis:** Wenn Sie das Volumen oder die Latenz Ihres Netzwerkverkehrs nicht kennen, wenden Sie sich vor der Konfiguration dieser Funktion an Ihren Professional Services-Ansprechpartner.

<p>MaxEPSExpectedPerSource</p>	<p>Geben Sie das maximale Datenverkehrsvolumen (EPS oder Ereignisse pro Sekunde) an, das pro Quelle beim ESA-Service eintreffen wird (wenn z. B. eine Quelle 20.000 EPS empfängt und eine andere 25.000 EPS empfängt, geben Sie den höheren Wert, also 25.000 EPS, an).</p> <p>Wenn Sie diese Rate zu niedrig einstellen, wirkt sich dies kurzzeitig auf die Performance aus. Allerdings erhöht ESA den Wert für <code>MaxEPSExpectedPerSource</code> nach Bedarf automatisch, damit das Ordnen nach Erfassungszeit erfolgreich ist.</p> <p>Der Standardwert ist 20K.</p>
<p>TimeOrderHoldWindow</p>	<p>Geben Sie in Sekunden (Ganzzahl) an, wie lange gewartet werden soll, bis Ereignisse aus allen Quellen eingetroffen sind.</p> <p>Konfigurieren Sie diesen Wert basierend auf der Latenz zwischen den Quellen.</p> <p>Der Standardwert ist 2 Sekunden. Ein geringerer Wert kann das Risiko von übersprungenen Ereignissen erhöhen. Ein höherer Wert kann die Performance verschlechtern, da mehr Arbeitsspeicher verbraucht wird.</p>
<p>IdleSourceAdvanceAfterSeconds</p>	<p>Geben Sie den Zeitraum (in Sekunden) an, nach dessen Ablauf ESA eine inaktive Quelle ignoriert, damit das Ordnen nach Erfassungszeit weiterhin funktioniert. Eine inaktive Quelle bedeutet, dass keine Ereignisse von dieser Quelle empfangen werden, obwohl die Quelle nicht offline ist. Der Standardwert ist 0, was bedeutet, dass der ESA-Service auf unbestimmte Zeit wartet, bis Ereignisse eintreffen.</p>
<p>OfflineSourceAdvanceAfterSeconds</p>	<p>Geben Sie den Zeitraum (in Sekunden) an, nach dessen Ablauf ESA eine Offlinequelle ignoriert, damit das Ordnen nach Erfassungszeit weiterhin funktioniert. Der Standardwert ist 0, was bedeutet, dass der ESA-Service auf unbestimmte Zeit wartet. Dieser Parameter wirkt sich nicht auf erneute Verbindungsversuche aus; diese werden in jedem Fall durchgeführt.</p>

## Troubleshooting und Tipps

Bei dieser Funktion kann es vorkommen, dass ein Rückstand bei Ereignissen auftritt. Um dieses Problem zu beheben, können Sie eine der folgenden Optionen durchführen.



### Deaktivieren des Ordners nach Erfassungszeit

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie den ESA-Service aus und wählen Sie dann   > **Ansicht > Durchsuchen**.
2. Navigieren Sie zu **Workflow > Quelle > nextgenAggregationSource**.
3. Legen Sie das Attribut „StreamEnabled“ auf „false“ fest.
4. Legen Sie das Attribut „TimeOrdered“ auf „false“ fest.

Wenn Sie das Ordnen nach Erfassungszeit deaktivieren, verlieren Sie diese Daten im Rückstand und Ereignisse werden nicht mehr nach Erfassungszeit geordnet.

### Deaktivieren der Positionsnachverfolgung

Durch die Positionsnachverfolgung kann ESA nachvollziehen, wo das Verarbeiten der Ereignisse unterbrochen wurde, wenn ESA anhält oder heruntergefahren wird. Die Positionsnachverfolgung ist beim Ordnen nach Erfassungszeit standardmäßig aktiviert. Wenn Sie die Positionsnachverfolgung deaktivieren, kann ESA die Ereignisse im Rückstand überspringen. Beispiel: Wenn ESA um 7:00 Uhr ausfällt und Sie es um 11:00 Uhr mit deaktivierter Positionsnachverfolgung neu starten, beginnt ESA mit der Verarbeitung von Ereignissen ab 10:55 Uhr. Bei aktivierter Positionsnachverfolgung startet ESA das Verarbeiten von Ereignissen genau an dem Punkt, an dem die Verarbeitung unterbrochen wurde.

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie den ESA-Service aus und wählen Sie dann   > **Ansicht > Durchsuchen**.
2. Navigieren Sie zu **Workflow > Quelle > nextgenAggregationSource**.
3. Legen Sie das Attribut **PositionTrackingEnabled** auf „false“ fest.

Wenn Sie die Positionsnachverfolgung deaktivieren, gehen die Daten im Rückstand verloren, aber Ereignisse werden zukünftig nach Erfassungszeit geordnet.

## Starten, Beenden oder erneut Starten des ESA-Services

In diesem Thema wird das Starten, Beenden oder Neustarten eines Event Stream Analysis-Services beschrieben. Das Verfahren gilt für ESA-Korrelationsregeln.

### Starten des ESA-Services

Bevor Sie beginnen:

- Stellen Sie sicher, dass MongoDB ausgeführt wird.
- Wenn der MongoDB-Service nicht ausgeführt wird, verwenden Sie folgenden Befehl zum Starten des MongoDB-Services:  

```
systemctl start mongod
```

So starten Sie einen ESA-Service:

1. Verbinden Sie sich über ssh mit dem ESA-Service und melden Sie sich als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:  

```
systemctl start rsa-nw-esa-server
```

### Beenden des ESA-Services

So beenden Sie einen ESA-Service:

1. Verbinden Sie sich über ssh mit dem ESA-Service und melden Sie sich als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:  

```
systemctl stop rsa-nw-esa-server
```

### Neustarten des ESA-Services

So starten Sie einen ESA-Service neu:

1. Verbinden Sie sich über ssh mit dem ESA-Service und melden Sie sich als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:  

```
systemctl restart rsa-nw-esa-server
```



## Auditprotokolle und Überprüfen der ESA-Komponentenversionen und -status

Dieses Thema enthält Details zur Auditprotokollierung und Anweisungen zur Überprüfung der Versionen der installierten Event Stream Analysis-Komponenten. Diese Verfahren gelten für ESA-Korrelationsregeln.

### Regeln für Auditprotokolle

Auditprotokollierung ermöglicht es, Details zu den Regeln anzuzeigen, die in NetWitness Suite erstellt und bearbeitet werden.

Informationen zum Zugriff auf Ihre Auditprotokolle finden Sie unter „Lokale Speicherorte für Auditprotokolle“ im *Systemkonfigurationsleitfaden*.

Das folgende Beispiel zeigt ein Erstellen-, Aktualisieren- und Löschmodell für eine bestimmte Regel.

- **Beispiel für ein Erstellen-Protokoll:** 2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT\_STREAM\_ANALYSIS" category: SYSTEM operation: "**CREATE RULE**" parameters: "Epl Module Identifier: 56elf2adbee8290008241296, Esper Instance: default, Rule Enabled: true, Trial Rule: false " key: "Epl Rule: @RSAAalert select \* from Event;" identity: "admin" userRole: "ROLE\_ESA\_ADMINISTRATOR"
- **Beispiel für ein Aktualisieren-Protokoll:** 2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT\_STREAM\_ANALYSIS" category: SYSTEM operation: "**UPDATE RULE**" parameters: "Epl Module Identifier: 56elf2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAalert select \* from Event;" identity: "admin" userRole: "ROLE\_ESA\_ADMINISTRATOR"
- **Beispiel für ein Löschmodell:** 2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT\_STREAM\_ANALYSIS" category: SYSTEM operation: "**DELETE RULE**" parameters: "Epl Module Identifier: 56elf2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAalert select \* from Event;" identity: "admin" userRole: "ROLE\_ESA\_ADMINISTRATOR "

Jedes Protokoll enthält die folgenden Parameter:

- Zeitstempel: Zeit, zu der die Regel geändert wurde. Beispiel: 2016-03-10 14:19:37,951
- DeviceVersion: Version des ESA-Geräts. Beispiel: „10.6.1.0-SNAPSHOT“
- DeviceService: Beispiel: EVENT\_STREAM\_ANALYSIS
- Kategorie: Beispiel: SYSTEM
- Operation: Beispiel: REGEL LÖSCHEN/ERSTELLEN/AKTUALISIEREN
- Parameter: Platzhalter für die folgenden Schlüssel:
- EPL-Modul-ID: eindeutige Kennung für die Regel. Beispiel: 56e1f2adbee8290008241296
- Esper-Instanz: Esper-Instanz, auf der die Regel bereitgestellt wurde. Beispiel: Standard
- Aktivierte Regel: Zeigt an, ob die Regel aktiviert ist oder nicht. Beispiel: Aktivierte Regel: true
- Testregel: Zeigt an, ob die Regel als Testregel konfiguriert ist oder nicht. Beispiel: Testregel: false
- EPL-Regel: Zeigt die Regelsyntax an. Beispiel:

```
@RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR+ROLE_ESA_ADMINISTRATOR+ROLE_ESA_ADMIN"
```
- Identity: Beispiel: „admin“
- userRole: Beispiel: „ROLE\_ESA\_ADMINISTRATOR“

**Hinweis:** Wenn eine Regel deaktiviert ist, werden für dieselbe Regel zwei Protokolle erzeugt. Erst wird ein Auditprotokoll „Regel löschen“ [Attribut „Aktivierte Regel“ = True] erstellt, gefolgt von einem Auditprotokoll „Regel erstellen“ [Attribut „Aktivierte Regel“ = False].

## Überprüfen der ESA Server-Version

So überprüfen Sie die ESA Server-Version:

1. Verbinden Sie sich über ssh mit dem ESA-Service und melden Sie sich als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:

```
rpm -qa | grep rsa-nw-esa-server
```

Die ESA-Serverversion wird angezeigt.

## Überprüfen der MongoDB-Version

So überprüfen Sie die MongoDB-Version:

1. Verbinden Sie sich über ssh mit dem ESA-Service und melden Sie sich als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:  
`mongo --version`  
Die MongoDB-Version wird angezeigt.

## **Überprüfen des MongoDB-Status**

So überprüfen Sie den MongoDB-Status:

1. Verbinden Sie sich über ssh mit dem ESA-Service und melden Sie sich als Root-Benutzer an.
2. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:  
`systemctl status mongod`
3. Führen Sie den folgenden Befehl aus, wenn MongoDB nicht ausgeführt wird:  
`systemctl start mongod`

## Referenzen

---

Dieser Abschnitt ist eine Sammlung der Referenzinformationen, in denen die Benutzeroberfläche zur ESA-Konfiguration in NetWitness Suite beschrieben werden.

Weitere Details finden Sie in den folgenden Themen:

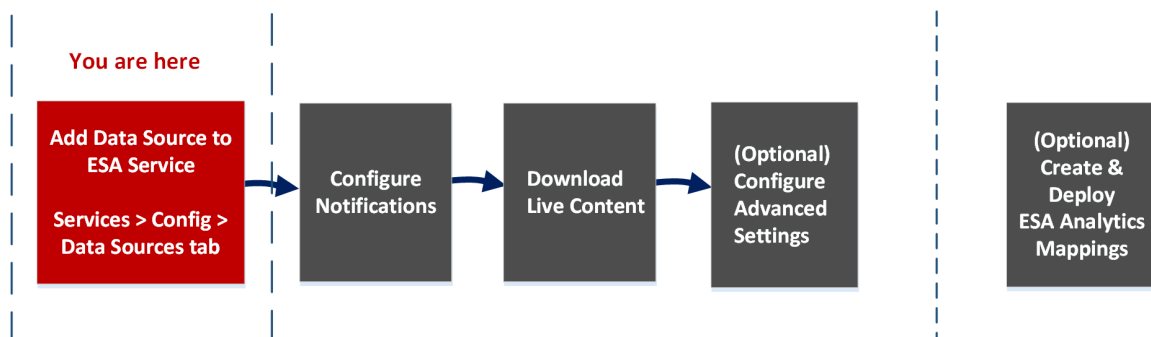
- [Ansicht „Services-Konfiguration“ – Registerkarte „Erweitert“](#)
- [Ansicht „Service-Konfiguration“ – Registerkarte „Datenquellen“](#)
- [ESA Analytics-Zuordnungen](#)
- [Moduleinstellungen](#)
- [Konfiguration des Whois-Abfrageservice](#)

## Ansicht „Service-Konfiguration“ – Registerkarte „Datenquellen“

Unter Ansicht „Services-Konfiguration“ > Registerkarte „Datenquellen“ eines ESA-Service können Sie die Quellen konfigurieren, die ESA zum Analysieren von Daten verwendet. Ein ESA-Service erfasst Daten von einem Concentrator, um Incidents zu erkennen und Analysten über mögliche Bedrohungen zu informieren.

### Workflow

Dieser Workflow zeigt den allgemeinen Prozess für die Konfiguration von ESA. Er zeigt auch, wo im Prozess sich die Konfiguration von Datenquellen befindet.



ESA bietet zwei Services, den Event Stream Analysis-Service (ESA-Korrelationsregeln) und den Event Stream Analytics-Server-Service (ESA Analytics). Die ersten vier gezeigten Verfahren beziehen sich auf das Konfigurieren des Event Stream Analysis-Service:

- **Hinzufügen einer Datenquelle zu einem ESA-Service**
- Benachrichtigungen konfigurieren
- Live-Inhalt herunterladen
- (Optional) Konfigurieren von erweiterten Einstellungen

Das letzte Verfahren ist getrennt von den anderen und bezieht sich auf das Erstellen von Zuordnungen für die ESA Analytics-Services, um die automatische Ermittlung von Advanced Threats zu starten:

- (Optional) Erstellen und Bereitstellen von ESA Analytics-Zuordnungen

## Was möchten Sie tun?


Rolle	Ziel	Details anzeigen
Administrator	Einen Concentrator als Datenquelle zum Event Stream Analysis-Service hinzufügen*	Siehe <a href="#">Konfigurieren von ESA-Korrelationsregeln</a> und <a href="#">Schritt 1. Hinzufügen einer Datenquelle zu einem ESA-Service</a>
Administrator	Benachrichtigungen konfigurieren	Siehe „Benachrichtigungsmethoden“ im <i>Handbuch Versenden von Warnmeldungen mit ESA</i> .
Administrator	Live-Inhalt herunterladen	Siehe „Ansicht 'Live-Suche“ im <i>Leitfaden Live-Ressourcenmanagement</i> .
Administrator	Konfigurieren von erweiterten Einstellungen	<a href="#">Schritt 2. Konfigurieren erweiterter Einstellungen für einen ESA-Service</a>

\*Sie können diese Aufgaben hier (auf der Registerkarte „Datenquellen“ der Ansicht „Services-Konfiguration“) durchführen.

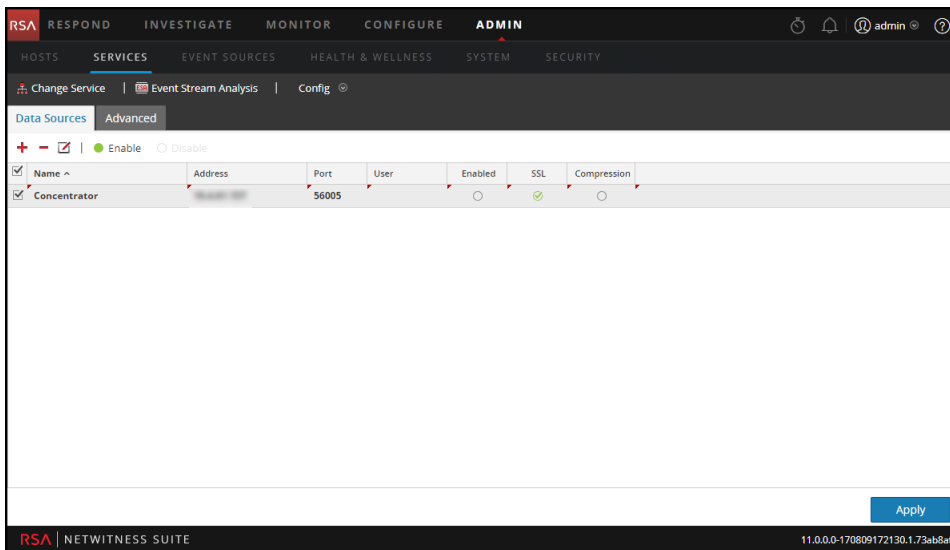
## Verwandte Themen

- Siehe „Hinzufügen oder Aktualisieren eines Hosts“ im *Leitfaden für die ersten Schritte mit Hosts und Services*.

## Überblick

Um auf die Registerkarte „Datenquellen“ zuzugreifen, gehen Sie zu **ADMIN > Services >** (wählen Sie einen ESA-Service) >  > **Ansicht > Konfiguration** aus.

Die folgende Abbildung zeigt die Registerkarte „Erweitert“ der Ansicht „Services-Konfiguration“ für einen ESA-Service.



### Symbolleiste

In der nachstehenden Tabelle werden die Optionen in der Symbolleiste beschrieben.

Option	Beschreibung
	Fügt eine neue Datenquelle zum ESA-Service hinzu.
	Löscht eine Datenquelle aus dem ESA-Service.
	Bearbeitet eine Datenquelle. Sie müssen einen Benutzernamen und ein Passwort für den Service angeben, um Änderungen vornehmen zu können.
<input checked="" type="checkbox"/> Enable	Aktiviert die ausgewählte Datenquelle.
<input type="checkbox"/> Disable	Deaktiviert die ausgewählte Datenquelle.

### Datenquellen

Die Liste „Datenquellen“ zeigt alle Datenquellen, die dem ESA-Service hinzugefügt wurden. In der folgenden Tabelle werden die Spalten der Liste „Datenquellen“ beschrieben.

Spalte	Beschreibung
Name	Der Name des Datenquellenservices

Spalte	Beschreibung
Adresse	Die Adresse des Datenquellenservices
Port	Der von der Datenquelle verwendete Port
Benutzer	Der mit der Datenquelle verbundene Benutzer
Aktiviert	Gibt an, ob die Datenquelle aktiviert ist
SSL	Gibt an, ob die SSL-Kommunikation aktiviert ist
Komprimierung	Gibt an, ob die Komprimierung aktiviert ist

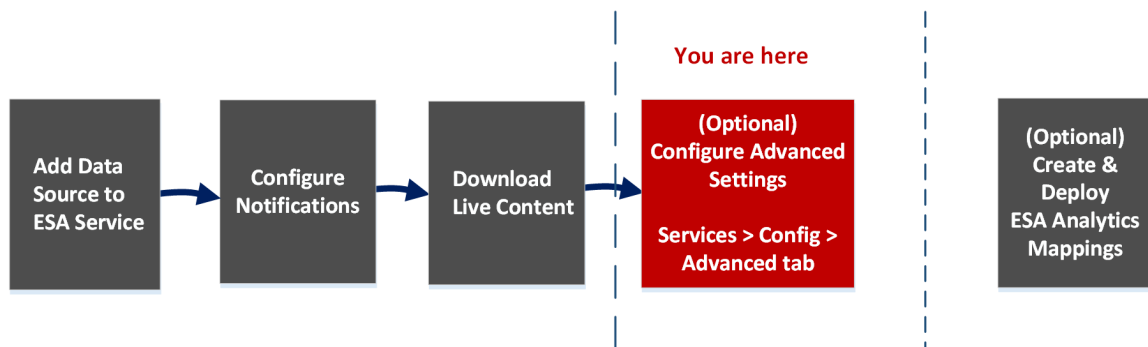


## Ansicht „Services-Konfiguration“ – Registerkarte „Erweitert“

Die Ansicht „Services-Konfiguration“ > Registerkarte „Erweitert“ eines ESA-Service ermöglicht Ihnen die Konfiguration erweiterter Einstellungen. In der Ansicht „Erweitert“ können Sie erweiterte Einstellungen konfigurieren, um eine verbesserte Performance zu erzielen, die Ereignisanzahl für Regeln mit mehreren Ereignissen zu beschränken, Ereignisse im Arbeitsspeicher zu puffern und die Anzahl der in der ESA zu speichernden Ereignisse festzulegen.

### Workflow

Dieser Workflow zeigt den allgemeinen Prozess für die Konfiguration von ESA. Er zeigt auch, wo im Prozess sich die erweiterten Einstellungen befinden.



ESA bietet zwei Services, den Event Stream Analysis-Service (ESA-Korrelationsregeln) und den Event Stream Analytics-Server-Service (ESA Analytics). Die ersten vier gezeigten Verfahren beziehen sich auf das Konfigurieren des Event Stream Analysis-Service:

- Hinzufügen einer Datenquelle zu einem ESA-Service
- Benachrichtigungen konfigurieren
- Live-Inhalt herunterladen
- **(Optional) Konfigurieren von erweiterten Einstellungen**

Das letzte Verfahren ist getrennt von den anderen und bezieht sich auf das Erstellen von Zuordnungen für die ESA Analytics-Services, um die automatische Ermittlung von Advanced Threats zu starten:

- (Optional) Erstellen und Bereitstellen von ESA Analytics-Zuordnungen

## Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Einen Concentrator als Datenquelle zum Event Stream Analysis-Service hinzufügen	Siehe <a href="#">Konfigurieren von ESA-Korrelationsregeln</a> und <a href="#">Schritt 1. Hinzufügen einer Datenquelle zu einem ESA-Service</a>
Administrator	Benachrichtigungen konfigurieren	Siehe „Benachrichtigungsmethoden“ im <i>Handbuch Versenden von Warnmeldungen mit ESA</i> .
Administrator	Live-Inhalt herunterladen	Siehe „Ansicht 'Live-Suche“ im <i>Leitfaden Live-Ressourcenmanagement</i> .
Administrator	Erweiterte Einstellungen konfigurieren*	<a href="#">Schritt 2. Konfigurieren erweiterter Einstellungen für einen ESA-Service</a>

\*Sie können diese Aufgaben hier (auf der Registerkarte „Erweitert“ der Ansicht „Services-Konfiguration“) durchführen.

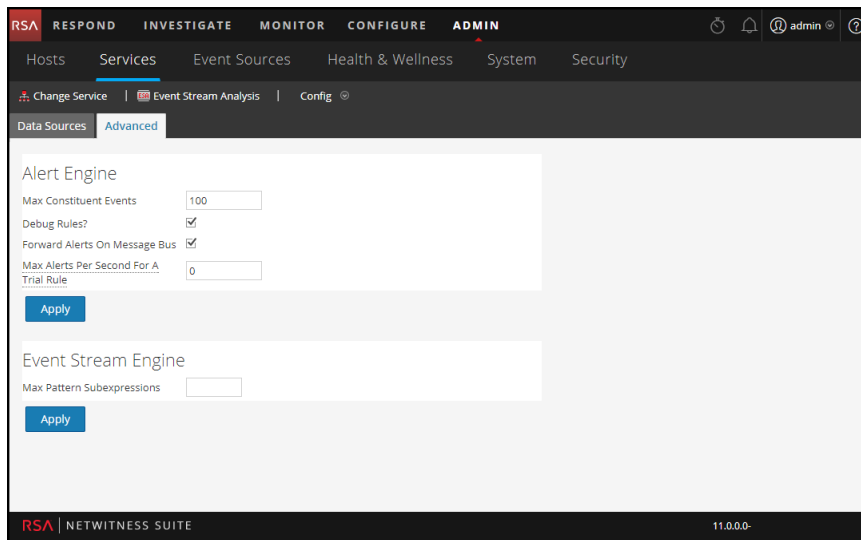
## Verwandte Themen

- Siehe „Hinzufügen oder Aktualisieren eines Hosts“ im *Leitfaden für die ersten Schritte mit Hosts und Services*.

## Überblick

Um auf die Registerkarte „Erweitert“ zuzugreifen, gehen Sie zu **ADMIN > Services >** (wählen Sie einen ESA-Service) >  > **Ansicht > Konfiguration** aus.

Die folgende Abbildung zeigt die Registerkarte „Erweitert“ der Ansicht „Services-Konfiguration“ für einen ESA-Service.



### Einstellungen der Warnmeldungs-Engine

Im Abschnitt Warnmeldungs-Engine geben Sie Werte an, um Ereignisse für Regeln zu bewahren, die mehrere Ereignisse wählen. Die folgende Abbildung zeigt den Abschnitt „Warnmeldungs-Engine“ an.

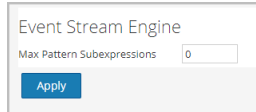
In der folgenden Tabelle werden die Parameter im Abschnitt „Warnmeldungs-Engine“ mit einer Beschreibung aufgelistet.

Parameter	Beschreibung
Max. Bürgerereignisse	Für Regeln, die mehrere Ereignisse auswählen, legt dieser Konfigurationswert fest, wie viele der zugehörigen Ereignisse erhalten bleiben. Wenn eine Regel z. B. eine Warnmeldung mit 200 zugehörigen Ereignissen auslöst und dieser Parameter auf 100 eingestellt ist, werden nur die ersten 100 von ESA gespeichert; der Rest wird gelöscht. Der Standardwert ist <b>100</b> .
Regeln debuggen?	Aktivieren Sie dieses Kontrollkästchen, um das Debugging von Regeln zu aktivieren.

Parameter	Beschreibung
Warnmeldungen an Nachrichtenbus weiterleiten	Wenn Sie ESA-Warnmeldungen für NetWitness Respond weiterleiten möchten, müssen Sie diese Option auswählen. Die erzeugten ESA-Warnmeldungen werden an den Nachrichtenbus und dann an Respond gesendet. Diese Option ist standardmäßig ausgewählt. Stellen Sie sicher, dass der Antwortserver-Service ausgeführt wird.
Max. Warnmeldungen pro Sekunde für eine Testregel	Sie können die maximale Anzahl der an den Nachrichtenbus weiterzuleitenden Warnmeldungen für die Testregel angeben. Wenn der Wert beispielsweise auf <b>50</b> festgelegt ist, werden nur 50 Warnmeldungen für die Testregel an den Nachrichtenbus weitergeleitet. Wenn der Wert auf <b>0</b> festgelegt ist, werden die durch die Testregel erzeugten Warnmeldungen nicht an den Nachrichtenbus weitergeleitet. Der Standardwert ist <b>10</b> .

### Einstellungen der Ereignis-Stream-Engine

Im Abschnitt Ereignis-Stream-Engine geben Sie Details an, um die Performance zu verbessern. Die folgende Abbildung zeigt den Abschnitt „Ereignis-Stream-Engine“.



In der folgenden Tabelle werden die Parameter im Abschnitt „Ereignis-Stream-Engine“ mit einer Beschreibung aufgelistet.

Parameter	Beschreibung
Max. Muster-Teilausdrücke	Für bestimmte Regeln muss ESPER Teilausdrücke im Speicher behalten, bevor entschieden wird, ob sie ausgelöst werden. Diese Teilausdrücke belegen Platz im Arbeitsspeicher und können ohne Kontrolle den Arbeitsspeicher überlasten und einen Servicefehler verursachen. Dieser Parameter ist eine Sicherheitsmaßnahme, damit nicht zu viel Arbeitsspeicher belegt wird. Wenn eine Regel die angegebene Anzahl von Teilausdrücken überschreitet, wird die Verarbeitung verzögert. Der Standardwert ist <b>0</b> ; hiermit ist die Einstellung deaktiviert. Sie müssen einen Wert festlegen, wenn Probleme mit der Stabilität des Services auftreten.

## Konfiguration des Whois-Abfrageservice

Im Bereich „Whois-Abfragekonfiguration“ (ADMIN > System > Whois) konfigurieren Sie eine Verbindung zum Whois-Abfrageservice für Ihre vorkonfigurierten ESA Analytics-Module, die bei der automatisierten Bedrohungserkennung von RSA verwendet werden. Mit dem Service „Whois“ können Sie präzise Daten über Domains erhalten, mit denen Sie sich verbinden. Um eine effektive Bewertung zu ermöglichen, ist es wichtig, dass Sie die Whois-Serviceeinstellungen konfigurieren.

Zur Nutzung dieses Service benötigen Sie ein RSA Live-Konto.

Wenn Sie ein Live-Konto im Bereich „Live-Services“ konfiguriert haben (ADMIN > System > Live-Services), wird der Whois-Abfrageservice automatisch für Sie konfiguriert. Sie müssen nur die Verbindung des Whois-Abfrageservice überprüfen.

**Hinweis:** Wenn Sie kein RSA Live-Konto besitzen, können Sie eines im RSA Live-Registrierungsportal erstellen:

<https://cms.netwitness.com/registration/>

Im *Handbuch Live Services Management* finden Sie zusätzliche Informationen.

### Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Den Whois-Abfrageservice konfigurieren.	<a href="#">Konfigurieren des Whois-Abfrageservice</a>
Administrator	Die Verbindung des Whois-Abfrageservice überprüfen.	<a href="#">Konfigurieren des Whois-Abfrageservice</a>

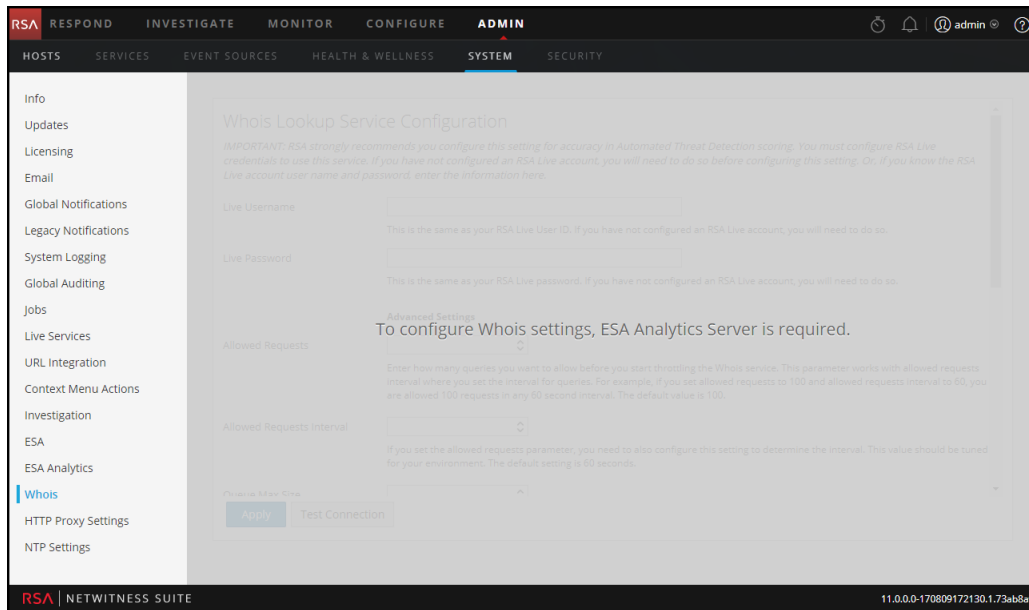
### Verwandte Themen

- [ESA Analytics-Zuordnungen](#)

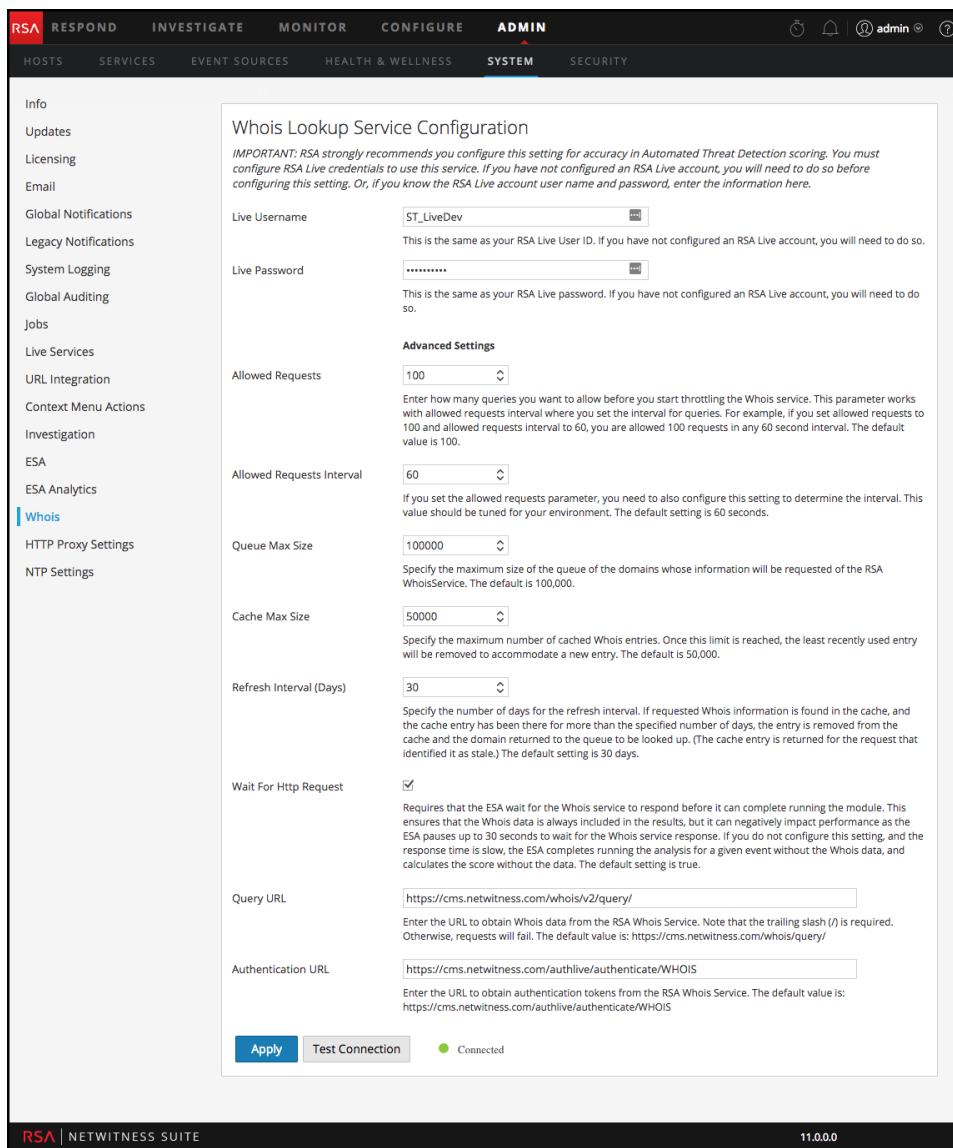
## Konfiguration des Whois-Abfrageservice

Um auf die Konfiguration des Whois-Abfrageservice zuzugreifen, gehen Sie zu „ADMIN > System“ und wählen Sie im Bereich „Optionen“ die Option „Whois“.

Der ESA Analytics-Server-Service muss in der Ansicht „ADMIN > Services“ verfügbar sein (ein grüner Kreis wird angezeigt). Wenn kein ESA Analytics-Server-Service verfügbar ist, wird der folgende Bereich angezeigt.



Wenn ein ESA Analytics-Server-Service verfügbar ist, wird der folgende Bereich angezeigt.



In der folgenden Tabelle werden die aufgeführten Whois-Abfrageservice-Konfigurationseinstellungen beschrieben.

Parameter	Beschreibung
Live-Benutzername	<p><b>Nur erforderlich, wenn Sie nicht bereits den Whois-Abfrageservice konfiguriert haben.</b> Geben Sie die Anmeldeinformationen für die Authentifizierung für den RSA Whois-Server ein. Diese sind identisch mit Ihrer RSA Live-Benutzer-ID. Wenn Sie noch kein RSA Live-Konto konfiguriert haben, müssen Sie dies jetzt tun.</p> <p>Der Standardwert ist „whois“.</p>

Parameter	Beschreibung
Live-Passwort	<p><b>Nur erforderlich, wenn Sie bereits den Whois-Abfrageservice konfiguriert haben.</b> Geben Sie die Anmeldeinformationen für die Authentifizierung für den RSA Whois-Server ein. Diese sind identisch mit Ihrem RSA Live-Passwort. Wenn Sie noch kein RSA Live-Konto konfiguriert haben, müssen Sie dies jetzt tun.</p> <p>Der Standardwert ist null.</p>
Zulässige Anforderungen	<p>(Optional) Geben Sie die Anzahl der zulässigen Anfragen ein, bevor Sie damit beginnen, den Whois-Service zu drosseln. Dieser Parameter funktioniert mit <b>Intervall für zulässige Anforderungen</b> (in Sekunden), wo Sie das Intervall für Abfragen festlegen können. Beispiel: Wenn Sie <b>Zulässige Anforderungen</b> auf 100 und <b>Intervall für zulässige Anforderungen</b> auf 60 festlegen, können Sie 100 Anforderungen in jedem 60-Sekunden-Intervall starten.</p> <p>Der Standardwert ist 100.</p>
Intervall für zulässige Anforderungen	<p>(Optional) Wenn Sie den Parameter <b>Zulässige Anforderungen</b> festlegen, müssen Sie auch diese Einstellung konfigurieren, um das Intervall festzulegen. Dieser Wert sollte für Ihre Umgebung optimiert werden.</p> <p>Die Standardeinstellung beträgt 60 Sekunden.</p>
Max. Größe Warteschlange	<p>(Optional) Geben Sie die maximale Größe der Warteschlange der Domains an, deren Informationen von dem RSA Whois-Service angefordert werden.</p> <p>Die Standardeinstellung ist 100.000.</p>
Max. Cachegröße	<p>(Optional) Geben Sie die maximale Anzahl der zwischengespeicherten Whois-Einträge an. Sobald diese Grenze erreicht ist, wird der am längsten nicht verwendete Eintrag entfernt, um Platz für einen neuen Eintrag freizugeben.</p> <p>Die Standardeinstellung ist 50.000.</p>



Parameter	Beschreibung
Aktualisierungsintervall in Tagen	<p>(Optional) Geben Sie die Anzahl der Tage für das Aktualisierungsintervall an. Wenn die angeforderte Whois-Information im Cache gefunden wird und der Cacheeintrag älter ist als die angegebene Anzahl Sekunden, wird der Eintrag aus dem Cache entfernt und die Domain an die Warteschlange zurückgegeben, um abgefragt zu werden. (Der Cache-Eintrag wird für die Anforderung zurückgegeben, die ihn als veraltet gekennzeichnet hat.)</p> <p>Die Standardeinstellung beträgt 30 Tage.</p>
Warten auf HTTP-Anforderung	<p>(Optional) Erfordert, dass der ESA-Service wartet, bis der Whois-Service antwortet, bevor die Ausführung des Moduls abgeschlossen werden kann. Dadurch wird sichergestellt, dass die Whois-Daten immer in den Suchergebnissen enthalten sind, aber die Performance kann beeinträchtigt werden, da ESA bis zu 30 Sekunden auf die Antwort des Whois-Service wartet.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren und die Antwortzeit langsam ist, schließt ESA die Analyse für ein gegebenes Ereignis ohne die Whois-Daten ab und berechnet die Bewertung ohne die Daten.</p> <p>Die Standardeinstellung ist <b>true</b>.</p>
Abfrage-URL	<p>(Optional) Geben Sie die URL ein, um Whois-Daten von dem RSA Whois-Service zu erhalten. Der nachgestellte Schrägstrich („/“) ist erforderlich. Andernfalls werden Anfragen fehlschlagen.</p> <p>Der Standardwert ist: <b>https://cms.netwitness.com/whois/v2/query/</b></p>
Authentifizierungs-URL	<p>(Optional) Geben Sie die URL ein, um Authentifizierungstoken von dem RSA Whois-Service zu erhalten.</p> <p>Der Standardwert ist: <b>https://cms.netwitness.com/authlive/authenticate/WHOIS</b></p>

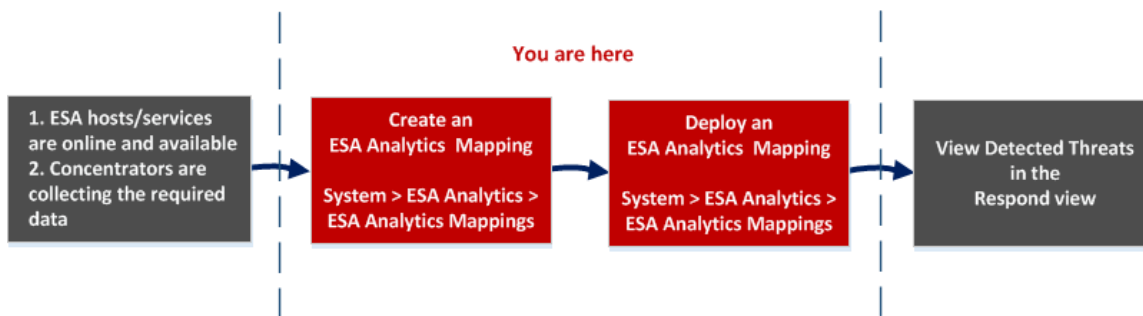
## ESA Analytics-Zuordnungen

Im Bereich „ESA Analytics-Zuordnungen“ (ADMIN > System > ESA Analytics) definieren Sie, wie die RSA-Funktion zur automatischen Bedrohungserkennung automatisch Advanced Threats erkennen soll. Sie können die Daten auf einem oder mehreren Concentrators analysieren, indem Sie ein vorkonfiguriertes ESA Analytics-Modul auswählen.

Um Netzwerkressourcen besser nutzen zu können und unnötige Datenflüsse zu reduzieren, können Sie mehrere Datenquellen wie Concentrators verfügbaren ESA Analytics-Services zuordnen, um Daten effizienter zu verarbeiten und zusätzliche Kapazitäten zu nutzen.

### Workflow

Dieser Workflow zeigt den Prozess zum Erstellen und Aktivieren einer ESA Analytics-Zuordnung, um die automatische Ermittlung von Advanced Threats zu starten.



Bevor Sie eine ESA Analytics-Zuordnung erstellen, stellen Sie sicher, dass die ESA-Hosts und -Services, die Sie für Ihre Zuordnungen verwenden möchten, online und verfügbar sind. Alle Services müssen mit einer konsistenten Zeitquelle synchronisiert sein. Stellen Sie außerdem sicher, dass die Concentrators die erforderlichen Daten erfassen. Wenn Sie eine ESA Analytics-Zuordnung erstellen, wählen Sie ein ESA Analytics-Modul für die Zuordnung aus, z. B. „Verdächtige Domains“. Dann wählen Sie die Datenquellen, z. B. Concentrators, die für dieses Modul zusammen mit einem Analytics ESA-Service für die Verarbeitung der Daten verwendet werden sollen. Wenn Sie zum Starten der Aggregation von Daten bereit sind, stellen Sie die Zuordnung bereit. Analysten können erkannte Bedrohungen für dieses Modul in der Ansicht „Reagieren“ anzeigen.

## Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Sicherstellen, dass die ESA-Hosts und -Services online und verfügbar sind.	ADMIN > HOSTS und ADMIN > SERVICES Siehe <i>Leitfaden für die ersten Schritte mit Hosts und Services</i> .
Administrator	Sicherstellen, dass die Concentrators die erforderlichen Daten erfassen.	Siehe <i>Konfigurationsleitfaden für Broker und Concentrator</i>
Administrator	ESA Analytics-Zuordnungen erstellen*	<a href="#">Zuordnen von ESA-Datenquellen zu Analytics-Modulen</a>
Administrator	ESA Analytics-Zuordnungen bereitstellen*	<a href="#">Zuordnen von ESA-Datenquellen zu Analytics-Modulen</a>
Administrator, Analyst	Erkannte Bedrohungen anzeigen	Siehe <i>NetWitness Respond – Benutzerhandbuch</i> .

\* Sie können diese Aufgaben hier (im Bereich „ESA Analytics-Zuordnungen“) durchführen.

## Verwandte Themen

- [Konfigurieren von ESA Analytics](#)
- [Aktualisieren einer Zuordnung](#)
- [Aufheben der Bereitstellung einer Zuordnung](#)
- [Löschen einer Zuordnung](#)
- [Ändern der Aufwärmphase und der Verzögerungszeit](#)
- [Moduleinstellungen](#)

## Überblick

Das folgende Beispiel zeigt eine ESA Analytics-Zuordnung. Die Konfiguration definiert die Datenquellen für das ausgewählte Modul und den ESA Analytics-Service, der die Ereignisse aus diesen Datenquellen verarbeiten wird.

The screenshot displays the 'ESA Analytics Mappings' configuration interface. At the top, there are navigation tabs: HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The left sidebar contains a navigation menu with 'ESA Analytics' highlighted. The main content area shows a table of mappings with columns for Status, Module, Sources, Service, Warm-Up, Lag Time, and Actions. A 'Deploy Now' button is located below the table. An inset window titled 'Create Mappings' shows the process of selecting a module ('http-packet'), sources ('Concentrator'), and service ('Event Stream Analytics Server'), along with configuring 'Warm-Up Period (Hours)' and 'Lag Time (Minutes)'. Red callouts 1 through 8 are placed over the interface to identify key components.

- 1 Zeigt den Bereich „ESA Analytics-Zuordnungen“ an.
- 2 Zeigt den Status der ESA Analytics-Zuordnung.
- 3 Der Name des Moduls, das zugeordnet wird.
- 4 Datenquellen wie Concentrators, die der Zuordnung zugewiesen sind.
- 5 ESA Analytics-Service, der die Daten für die Zuordnung verarbeitet.
- 6 Konfiguration der Aufwärmphase (in Stunden) auf den Datenquellen für die Zuordnung.
- 7 Konfiguration der Verzögerung (in Minuten) auf den Datenquellen für die Zuordnung.
- 8 Aktionen für die Änderung von Moduleinstellungen, Bereitstellung von Modulzuordnungen und Aufhebung der Bereitstellung von Modulzuordnungen.

## Symbolleiste


In der folgenden Tabelle werden die Aktionen der Symbolleiste beschrieben.

Symbol/Schaltfläche	Beschreibung
	<p>Öffnet das Dialogfeld „Zuordnungen erstellen“, in dem Sie eine ESA Analytics-Zuordnung erstellen können. Erstellen Sie eine separate Zuordnung für jedes Modul.</p> <p>Nach dem Erstellen und Überprüfen der Zuordnungen stellen Sie diese bereit.</p>
	<p>Löscht eine ESA Analytics-Zuordnung.</p> <ul style="list-style-type: none"> <li>• Sie können eine Zuordnung mit dem Status „Nicht bereitgestellt“ zu einem beliebigen Zeitpunkt löschen. Da eine Zuordnung mit dem Status „Nicht bereitgestellt“ nicht bereitgestellt ist und nicht ausgeführt wird, ergeben sich keine Auswirkungen auf die Datenaggregation.</li> <li>• Durch das Löschen einer bereitgestellten Zuordnung wird die Konfiguration auf dem ESA-Server gelöscht, die Bereitstellung für diese Zuordnung zurückgesetzt und das Abrufen von Daten aus der Datenquelle für dieses Modul gestoppt. Sie müssen die Bereitstellung einer Zuordnung mit dem Status „Bereitgestellt“ aufheben, bevor Sie sie löschen.</li> </ul>
Jetzt bereitstellen	<p>Nachdem Sie Ihre Zuordnungen erstellt haben, müssen Sie sie bereitstellen, um die Aggregation von Daten für die Module starten zu können. Sie können eine oder mehrere Zuordnungen mit dem Status „Nicht bereitgestellt“ für die Bereitstellung auswählen.</p>

**Hinweis:** Wenn Sie Änderungen an einer bereitgestellten Zuordnung vornehmen möchten, z. B. Concentrators hinzufügen oder entfernen oder den Service ändern, müssen Sie die Bereitstellung der vorhandenen Zuordnung aufheben und die Zuordnung löschen und dann eine neue Zuordnung für dieses Modul erstellen und bereitstellen.


## ESA Analytics-Zuordnungen

In der folgenden Tabelle werden die aufgeführten ESA Analytics-Zuordnungen beschrieben.

Bezeichnung	Beschreibung
	<p>Um eine einzelne Zuordnung auszuwählen, aktivieren Sie das Kontrollkästchen neben der Zuordnung.</p>

Bezeichnung	Beschreibung
Status	<p>Zeigt den Status der Zuordnung. Es gibt zwei Status:</p> <p><b>Nicht bereitgestellt</b> – Eine nicht bereitgestellte Zuordnung ordnet ein ESA Analytics-Modul Quellen und einem ESA Analytics-Service zu. Das Aggregieren von Daten für das Modul wird erst gestartet, wenn Sie die Zuordnung bereitstellen.</p> <p><b>Bereitgestellt</b> – Eine bereitgestellte Zuordnung ist bereitgestellt und wird ausgeführt. In einer bereitgestellten Zuordnung nutzt der ausgewählte ESA Analytics-Service die abfragebasierte Aggregation, um die entsprechenden gefilterten Ereignisse für das ausgewählte Modul von den Concentrators zu erfassen.</p>
Modul	<p>Gibt das ausgewählten ESA Analytics-Modul an. Ein ESA Analytics-Modul ist eine Pipeline aus Aktivitätsobjekten, die ein Ereignis durch mathematische Berechnungen um zusätzliche Informationen ergänzen. Das Modul befindet sich im ESA Analytics-Service.</p>
Quellen	<p>Quellen sind die Datenquellen, wie Concentrators, von denen ESA die Daten für das angegebene Modul aggregiert.</p>
Service	<p>Gibt den ESA Analytics-Service an, von dem die Daten für das angegebene Modul verarbeitet werden. Der ausgewählte Service muss mit einer konsistenten Zeitquelle synchronisiert sein.</p>
Aufwärmzeit (Stunden)	<p>Gibt eine Dauer für die Aufwärmphase (in Stunden) an. Eine Aufwärmphase ist erforderlich, damit die automatisierte Bedrohungserkennung Ihren Datenverkehr „kennen lernen“ kann. Die Aufwärmphase sollte ausgeführt werden, wenn der typische Datenverkehr ausgeführt wird. Während dieser Zeit werden Warnmeldungen für die Zuordnung von Modulen unterdrückt. Die Aufwärmzeit bereitet das Modul mit Verlaufsdaten vor und sorgt dafür, dass die Datenerfassung auch wirklich die angegebene Anzahl an Stunden dauert, bevor Warnmeldungen gesendet werden.</p> <p>RSA bietet vorkonfigurierte ESA Analytics-Module. Für jeden Modultyp ist eine standardmäßige Aufwärmphase definiert, die Sie bei Bedarf an Ihre Umgebung anpassen können. Nach dieser Aufwärmphase können Warnmeldungen angezeigt werden.</p> <p>Weitere Informationen zu Aufwärmphase und Verzögerungszeit finden Sie unter <a href="#">Moduleinstellungen</a>.</p>

Bezeichnung	Beschreibung
Verzögerungszeit (Minuten)	<p>Gibt eine konstante Verzögerungszeit in Minuten an, die hinzugefügt wird, um zu vermeiden, dass Ereignisse, die in Zeiten mit hoher Aktivität von den Datenquellen verarbeitet werden, verloren gehen. Beispielsweise variiert die Concentrator-Performance in Abhängigkeit von Faktoren wie der eingehenden Last, laufenden Abfragen und Indexierung. Aufgrund von diesen Faktoren aggregiert ein Concentrator Ereignisse möglicherweise nicht in Echtzeit, was zu der Verzögerung führt.</p> <p>Der Verzögerungsparameter verschafft dem Concentrator die Möglichkeit, die Aggregation aller Daten abzuschließen.</p> <p>Nach Abschluss der Aufwärmphase wird die Datenaggregation mit der <b>aktuellen (System-)Zeit – Verzögerungszeit</b> fortgesetzt. Das ist hilfreich, wenn ein Concentrator bei der Datenaggregation langsam ist. Die Verzögerungszeit stellt sicher, dass das Modul keine Daten verarbeitet, die innerhalb des Verzögerungszeitfensters auf dem Concentrator eintreffen. Auf diese Weise ist eine ausreichende Verzögerung gegeben, damit alle Ereignisse, die im Unternehmen erzeugt werden, vom Modul verarbeitet werden können.</p> <p>Wenn beispielsweise für die Verzögerung 30 Minuten und für die aktuelle Zeit 14 Uhr angegeben werden, beginnt der Concentrator um 13:30 mit dem Abrufen von Datensätzen. Das Verzögerungszeitfenster, in diesem Beispiel 30 Minuten, bleibt im Zeitverlauf konstant. Wenn die aktuelle Zeit auf 14:01 vorrückt, ruft der Concentrator die nächste Minute von Daten um 13:31 Uhr ab und so weiter.</p> <p><b>Wichtig:</b> Die Verzögerungszeit definiert den Puffer zwischen der aktuellen Zeit und der Zeit, zu der das Modul die Daten aufnimmt.</p> <div data-bbox="532 1297 1421 1470" style="border: 1px solid yellow; padding: 5px;"><p><b>Achtung:</b> RSA empfiehlt, dass Administratoren die Verzögerungsparameter basierend auf der Performance jedes einzelnen Concentrator dynamisch anpassen, um zu vermeiden, während der Aggregation Ereignisse zu vergessen.</p></div> <p>Weitere Informationen zu Aufwärmphase und Verzögerungszeit finden Sie unter <a href="#">Moduleinstellungen</a>.</p>

Bezeichnung	Beschreibung
	<p>Ermöglicht Ihnen die Auswahl zusätzlicher Aktionen für die ausgewählte Modulzuordnung:</p> <ul style="list-style-type: none"><li>• <b>Modul bearbeiten</b> – Ermöglicht Ihnen die Konfiguration der Aufwärmphase und der Verzögerungszeit für die ausgewählte Modulzuordnung.</li><li>• <b>Bereitstellen</b> – Stellt die ausgewählte Modulzuordnung bereit. Der angegebene ESA Analytics-Service beginnt mit dem Abrufen von Daten aus den Datenquellen für dieses Modul.</li><li>• <b>Bereitstellung aufheben</b> – Hebt die Bereitstellung der ausgewählten Modulzuordnung auf. Der angegebene ESA Analytics-Service stoppt das Abrufen von Daten aus den Datenquellen für dieses Modul.</li></ul> <p><b>Achtung:</b> Das Aufheben der Bereitstellung einer Zuordnung mit dem Status „Bereitgestellt“ wirkt sich auf die Datenaggregation für dieses Modul aus.</p>



## Moduleinstellungen

Nach dem Erstellen oder Bereitstellen einer Modulzuordnung im Bereich „ESA Analytics-Zuordnungen“ (ADMIN > System > ESA Analytics) haben Sie die Möglichkeit, einige Modulkonfigurationen für diese Zuordnung zu ändern.



### Was möchten Sie tun?

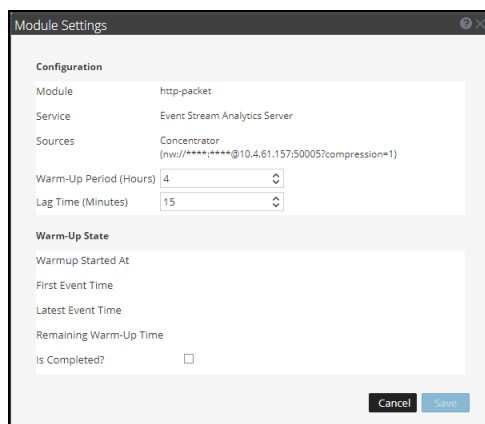
Rolle	Ziel	Details anzeigen
Administrator	Die Aufwärmphase für eine nicht bereitgestellte Modulzuordnung ändern.	<a href="#">Ändern der Aufwärmphase und der Verzögerungszeit</a>
Administrator	Die Aufwärmphase für eine Modulzuordnung während der Aufwärmphase ändern.	<a href="#">Ändern der Aufwärmphase und der Verzögerungszeit</a>
Administrator	Die Aufwärmphase für eine Modulzuordnung nach Abschluss der Aufwärmphase ändern.	<a href="#">Ändern der Aufwärmphase und der Verzögerungszeit</a>

### Verwandte Themen

- [Zuordnen von ESA-Datenquellen zu Analytics-Modulen](#)
- [ESA Analytics-Zuordnungen](#)

## Moduleinstellungen

Um auf die Moduleinstellungen zuzugreifen, wählen Sie im Bereich „ESA Analytics-Zuordnungen“ die Zuordnung, die Sie ändern möchten, und wählen Sie in der Spalte **Aktionen**   > **Modul bearbeiten**. Das Dialogfeld „Moduleinstellungen“ verfügt über die Abschnitte „Konfigurationen“ und „Aufwärmzustand“.



## Konfigurationen

Im Abschnitt „Konfigurationen“ können Sie die Konfigurationen für Aufwärmphase und Verzögerungszeit ändern.

In der folgenden Tabelle werden die Einstellungen beschrieben, die für eine ESA Analytics-Modulzuordnung zur Verfügung stehen.

Feld	Beschreibung
Modul	Zeigt den Namen des zugeordneten Moduls.
Service	Zeigt den ESA Analytics-Service, der die Daten für die Zuordnung verarbeitet.
Quellen	Zeigt die zugeordneten Datenquellen und die für die Kommunikation mit ESA verwendeten URLs.

Feld	Beschreibung
<p>Aufwärmzeit (Stunden)</p>	<p>Gibt eine Dauer für die Aufwärmphase in Stunden an. Eine Aufwärmphase ist erforderlich, damit die automatisierte Bedrohungserkennung Ihren Datenverkehr „kennen lernen“ kann. Die Aufwärmphase sollte ausgeführt werden, wenn der typische Datenverkehr ausgeführt wird. Während dieser Zeit werden Warnmeldungen für die Zuordnung von Modulen unterdrückt. Die Aufwärmzeit bereitet das Modul mit Verlaufsdaten vor und sorgt dafür, dass die Datenerfassung auch wirklich die angegebene Anzahl an Stunden dauert, bevor Warnmeldungen gesendet werden.</p> <p>RSA bietet vorkonfigurierte ESA Analytics-Module. Für jeden Modultyp ist eine standardmäßige Aufwärmphase definiert, die Sie bei Bedarf an Ihre Umgebung anpassen können. Nach dieser Aufwärmphase können Warnmeldungen angezeigt werden.</p> <p>Sie können die Aufwärmphase einer bereitgestellten Modulzuordnung abhängig davon aktualisieren, ob die Aufwärmphase abgeschlossen ist:</p> <ul style="list-style-type: none"> <li>• <b>Während der Aufwärmphase</b> – Sie können der Aufwärmphase Stunden hinzuzufügen oder verbleibende Aufwärmzeit abziehen.</li> <li>• <b>Abschluss der Aufwärmphase</b> – Sie können der Aufwärmphase Stunden hinzufügen, indem Sie die Differenz zwischen der aktuellen Zeit und der Zeit des ersten Ereignisses zu den Stunden hinzufügen, die Sie hinzufügen möchten.</li> </ul> <p>Beispiel: Eine Aufwärmphase von 10 Stunden ist abgeschlossen und die Zeit des ersten Ereignisses zeigt 12:00:00. Die aktuelle (System-)Zeit lautet 16:00:00 (4 Stunden später) und Sie möchten der Aufwärmphase 5 weitere Stunden hinzufügen möchten. Um dies zu erreichen, müssen Sie der Aufwärmphase von 10 Stunden 9 Stunden hinzufügen (<math>4+5 = 9</math>), sodass die neue Aufwärmphase auf 19 Stunden festgelegt wird.</p> <p>Sie können die Aufwärmphase nicht reduzieren, wenn sie abgeschlossen ist, sofern Sie nicht die Zuordnung löschen und eine neue erstellen.</p> <p>Der Wert der Aufwärmphase ist spezifisch für eine bestimmte Zuordnung und gilt nach der Bereitstellung für alle Concentrators innerhalb dieser Zuordnung. Wenn ein Concentrator zwischen zwei Modulen mit verschiedenen Aufwärmphasen gemeinsam verwendet wird, verwendet der Concentrator separate Aufwärmphasenwerte für jede Modulzuordnung.</p>

Feld	Beschreibung
Verzögerungszeit (Minuten)	<p>Gibt eine konstante Verzögerungszeit in Minuten an, die hinzugefügt wird, um zu vermeiden, dass Ereignisse, die in Zeiten mit hoher Aktivität von den Datenquellen verarbeitet werden, verloren gehen. Beispielsweise variiert die Concentrator-Performance in Abhängigkeit von Faktoren wie der eingehenden Last, laufenden Abfragen und Indexierung. Aufgrund von diesen Faktoren aggregiert ein Concentrator Ereignisse möglicherweise nicht in Echtzeit, was zu der Verzögerung führt.</p> <p>Der Verzögerungsparameter verschafft dem Concentrator die Möglichkeit, die Aggregation aller Daten abzuschließen. Bei der Angabe einer Verzögerungszeit beginnt die Datenaggregation bei der ersten Bereitstellung des Moduls unter <b>Aktuelle (System-)Zeit - Verzögerungszeit - Aufwärmzeit</b>. Lautet die aktuelle Uhrzeit beispielsweise 14:00 Uhr, beträgt die Verzögerungszeit 30 Minuten und die Aufwärmphase 4 Stunden, startet die Datenerfassung bei der ersten Bereitstellung des Moduls um 9:30 Uhr (14:00 Uhr – 0,5 Stunden – 4 Stunden).</p> <p>Nach Abschluss der Aufwärmphase wird die Datenaggregation mit der <b>aktuellen (System-)Zeit - Verzögerungszeit</b> fortgesetzt. Das ist hilfreich, wenn ein Concentrator bei der Datenaggregation langsam ist. Die Verzögerungszeit stellt sicher, dass das Modul keine Daten verarbeitet, die innerhalb des Verzögerungszeitfensters auf dem Concentrator eintreffen. Auf diese Weise ist eine ausreichende Verzögerung gegeben, damit alle Ereignisse, die im Unternehmen erzeugt werden, vom Modul verarbeitet werden können.</p> <p>Wenn beispielsweise für die Verzögerung 30 Minuten und für die aktuelle Zeit 14 Uhr angegeben werden, beginnt der Concentrator um 13:30 mit dem Abrufen von Datensätzen. Das Verzögerungszeitfenster, in diesem Beispiel 30 Minuten, bleibt im Zeitverlauf konstant. Wenn die aktuelle Zeit auf 14:01 vorrückt, ruft der Concentrator die nächste Minute von Daten um 13:31 Uhr ab und so weiter.</p> <p><b>Wichtig:</b> Die Verzögerungszeit definiert den Puffer zwischen der aktuellen Zeit und der Zeit, zu der das Modul die Daten aufnimmt.</p> <p>Der Wert der Verzögerungszeit ist spezifisch für eine bestimmte Zuordnung und gilt nach der Bereitstellung für alle Concentrators innerhalb dieser Zuordnung. Wenn ein Concentrator zwischen zwei Modulen mit verschiedenen Verzögerungszeiten gemeinsam verwendet wird, verwendet der Concentrator separate Verzögerungswerte für jede Modulzuordnung.</p> <div style="border: 1px solid yellow; padding: 5px; margin-top: 10px;"> <p><b>Achtung:</b> RSA empfiehlt, dass Administratoren die Verzögerungsparameter basierend auf der Performance jedes einzelnen</p> </div>

Feld	Beschreibung
	<p style="border: 1px solid yellow; padding: 5px;">Concentrator dynamisch anpassen, um zu vermeiden, während der Aggregation Ereignisse zu vergessen.</p> <p>Um die richtige Verzögerungszeit zu bestimmen, addieren Sie Folgendes, um eine ökologische Verzögerungszeit zu erhalten:</p> <ol style="list-style-type: none"> <li>1. <b>Protokoll- oder Paketlatenz</b> – Dies ist die erforderliche Zeit, die der Log Decoder benötigt, um die Protokolle zu erhalten, oder der (Packet-)Decoder, um Pakete zu empfangen. Beispielsweise kann der Log Decoder alle 20 Minuten Protokolle erhalten. In diesem Fall sollten Sie die Verzögerungszeit auf mindestens 20 Minuten, vorzugsweise 25 Minuten festlegen, damit Ihnen kein Ereignis entgeht.</li> <li>2. <b>Aggregationslatenz</b> – Dies ist die Zeit, die benötigt wird, um die Daten aus dem Log Decoder zum Concentrator zu übertragen.</li> <li>3. <b>Andere Puffer</b> – Fügen Sie eine für Ihre Umgebung spezifische Zeit ein.</li> </ol>

### Aufwärmzustand

Der Abschnitt „Aufwärmzustand“ bietet Informationen über den Aufwärmstatus, den Sie verwenden können, um die entsprechenden Anpassungen für die Aufwärmphase zu bestimmen.

Feld	Beschreibung
Aufwärmen gestartet um	Die Zeit, zu dem das erste Ereignis vom ESA Analytics-Modul aus der Datenquelle verarbeitet wurde.
Zeit des ersten Ereignisses	Die Uhrzeit des ersten Ereignisses. Die Aufwärmphase basiert auf dieser Uhrzeit.
Zeit des letzten Ereignisses	Die Uhrzeit des letzten Ereignisses.
Verbleibende Aufwärmzeit	Die Anzahl der in der Aufwärmphase verbleibenden Stunden.
Abgeschlossen?	Gibt an, ob die Aufwärmphase abgeschlossen ist. Bei „true“ ist die Aufwärmphase abgeschlossen. Bei „false“ wird das Modul weiterhin aufgewärmt und Sie können die Anzahl der verbleibenden Stunden im Feld „Verbleibende Aufwärmzeit“ anzeigen.

