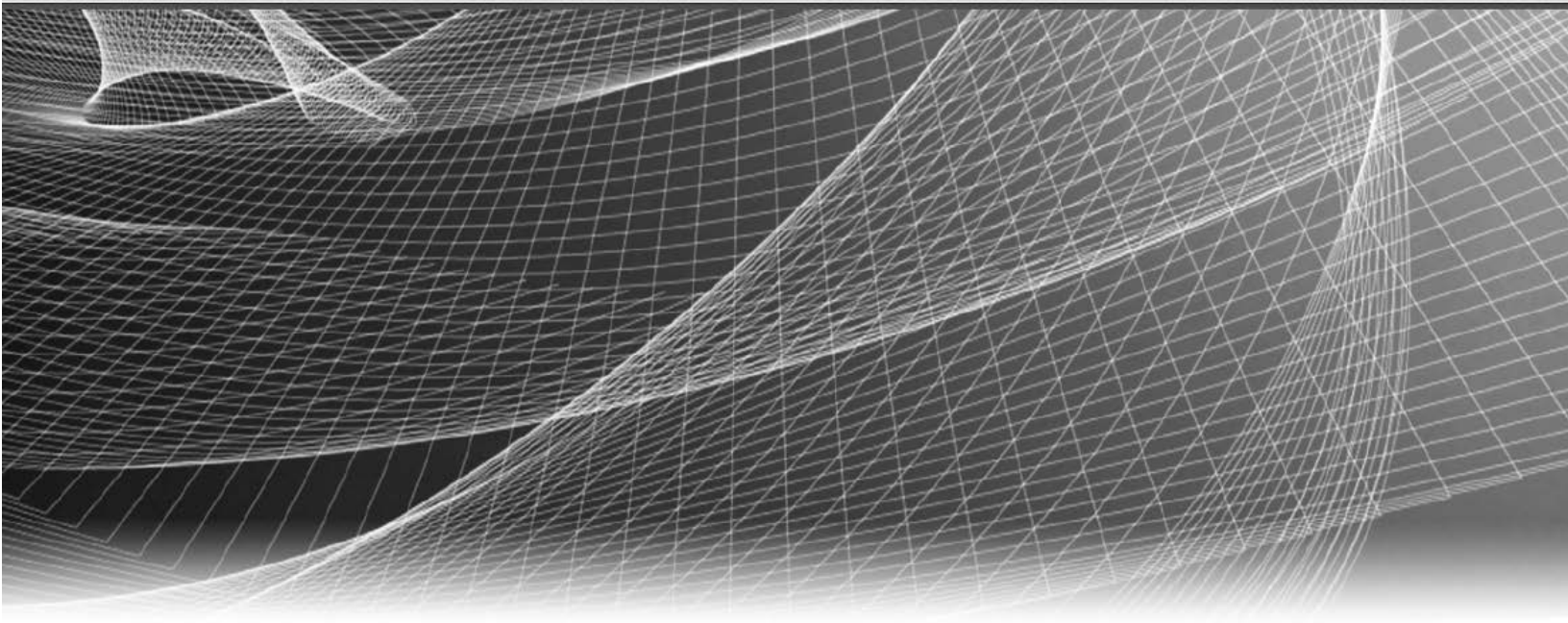


RSA Security Analytics

Konfigurationsleitfaden für Event Stream Analysis

für Version 10.6

Marken

Lizenzvereinbarung

Drittanbieterlizenzen

Hinweis zu Verschlüsselungstechnologien

Verteilung

Inhalt

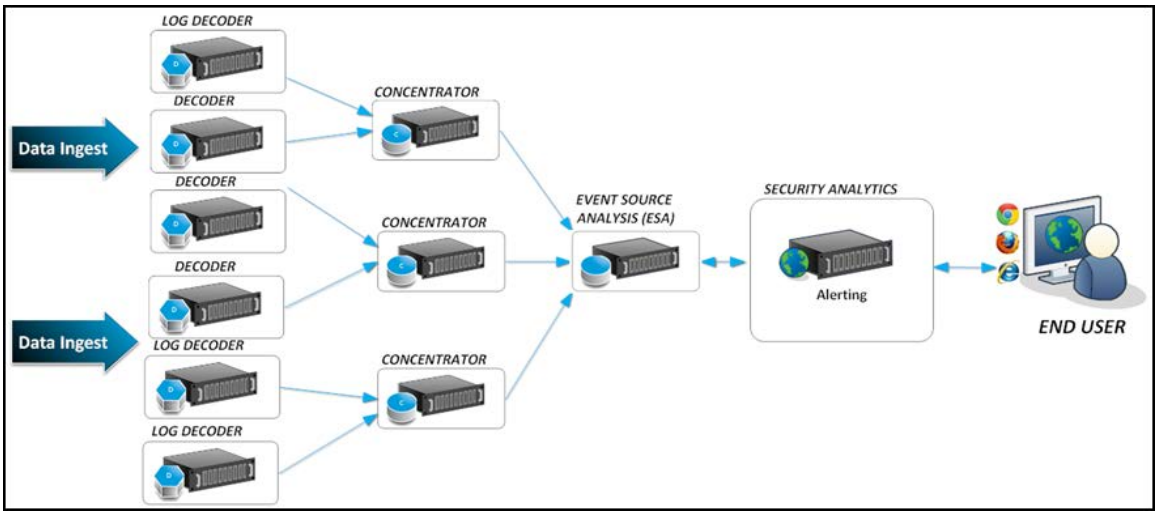
ESA-Übersicht (Event Stream Analysis)

Dieses Thema bietet eine Übersicht über das Modul Event Stream Analysis.

Der Security Analytics ESA-Service (Event Stream Analysis) 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 Workflow dargestellt:



Konfigurieren von Event Stream Analysis (ESA)

In diesem Thema werden die Hauptaufgaben zur Konfiguration von Security Analytics Event Stream Analysis beschrieben.

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. Sie können den Host ermitteln, aktualisieren oder hinzufügen, auf dem der ESA-Service installiert ist. (Optional) Wenn ESA nicht eingerichtet ist, müssen Sie Event Stream Analysis als Core-Service hinzufügen und dem Host den Event Stream Analysis-Service hinzufügen.	Weitere Informationen erhalten Sie unter „Schritt 1: „Hinzufügen oder Aktualisieren eines Hosts“ im „Leitfaden für die ersten Schritte mit Hosts und Services“. Siehe Schritt 1. Hinzufügen des Event Stream Analysis-Service.
2. Wenden Sie eine Lizenz auf den Event Stream Analysis-Service an.	Weitere Informationen finden Sie unter „Anzeigen verfügbarer Berechtigungen“ im „Lizenzierungsleitfaden“.
3. Fügen Sie den Concentrator als Datenquelle zum Event Stream Analysis-Service hinzu.	Siehe Schritt 2. Hinzufügen einer Datenquelle zu einem ESA-Service

Aufgaben	Referenz
4. Konfigurieren Sie Benachrichtigungen für den Event Stream Analysis-Service.	Weitere Informationen finden Sie unter „Benachrichtigungsmethoden“ im „Handbuch Versenden von Warnmeldungen mit ESA“.
5. Laden Sie Event Stream Analysis-Inhalte mithilfe von Live herunter.	Weitere Informationen finden Sie unter „Ansicht 'Live-Suche'“ im „Leitfaden Live-Ressourcenmanagement“.
6. (Optional) Erweiterte Konfiguration des Event Stream Analysis-Services	Siehe Schritt 3. Konfigurieren erweiterter Einstellungen für einen ESA-Service.
7. (Optional) Aktivieren Sie Context Hub.	Weitere Informationen erhalten Sie unter „Schritt 1. Hinzufügen des Context Hub-Services“ im „Context Hub-Konfigurationsleitfaden“.
8. (Optional) Konfigurieren Sie den ESA-Service für die Herstellung einer Verbindung mit dem Context Hub auf einem anderen ESA-Service.	Siehe Schritt 4. Konfigurieren eines ESA-Services zur Herstellung einer Verbindung mit dem Context Hub auf einem anderen ESA-Service.

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 des Event Stream Analysis-Service

In diesem Thema erfahren Sie, wie Sie den ESA-Service (Event Stream Analysis) auf einem Host hinzufügen.

Voraussetzungen

Stellen Sie sicher, dass Sie einen ESA-Service installiert und den Host in Security Analytics hinzugefügt haben. Weitere Informationen finden Sie unter „Schritt 1: Hinzufügen oder Aktualisieren eines Hosts“ im „Leitfaden für die ersten Schritte mit Hosts und Services“.

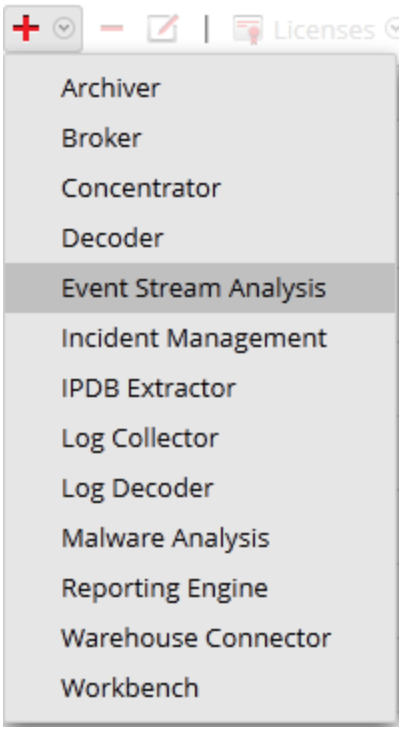
Verfahren

So fügen Sie den Event Stream Analysis-Service hinzu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.

   Die Ansicht „Services“ wird angezeigt.

2. Wählen Sie im Bereich „Services“ die Optionen + **> Event Stream Analysis** aus.



   Das Dialogfeld **Service hinzufügen** wird angezeigt.

3. Geben Sie die folgenden Details an.

Feld	Beschreibung
Host	Wählen Sie den Host, auf dem Sie den ESA-Service installieren möchten.
Name	Geben Sie einen Namen für den Service ein.

Feld	Beschreibung
Port	Der Standardport ist 50030. **Hinweis:** ESA kann nur mithilfe des SSL-Ports 50030 konfiguriert werden. Es ist nicht möglich, einen Nicht-SSL-Port zu konfigurieren.
Service berechtigen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die gegenwärtig konfigurierten Ansprüche auf diesen Service anwenden möchten.

4. Klicken Sie auf **Verbindung testen**, um festzustellen, ob Security Analytics sich mit dem Service verbindet.

   Hinweis: Beim Hinzufügen des Services sendet Security Analytics ICMP-Pakete an den Service, um zu prüfen, ob der eingegebene Hostname und die eingegebene IP-Adresse gültig für eine erfolgreiche Testverbindung sind.

5. Wenn das Ergebnis positiv ist, klicken Sie auf **Speichern**.

   Der hinzugefügte Service wird jetzt im Bereich „Services“ angezeigt.

Hinweis: Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Serviceinformationen und versuchen Sie es erneut.

Schritt 2. 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 Security Analytics muss mindestens einer der folgenden Concentrator konfiguriert sein:

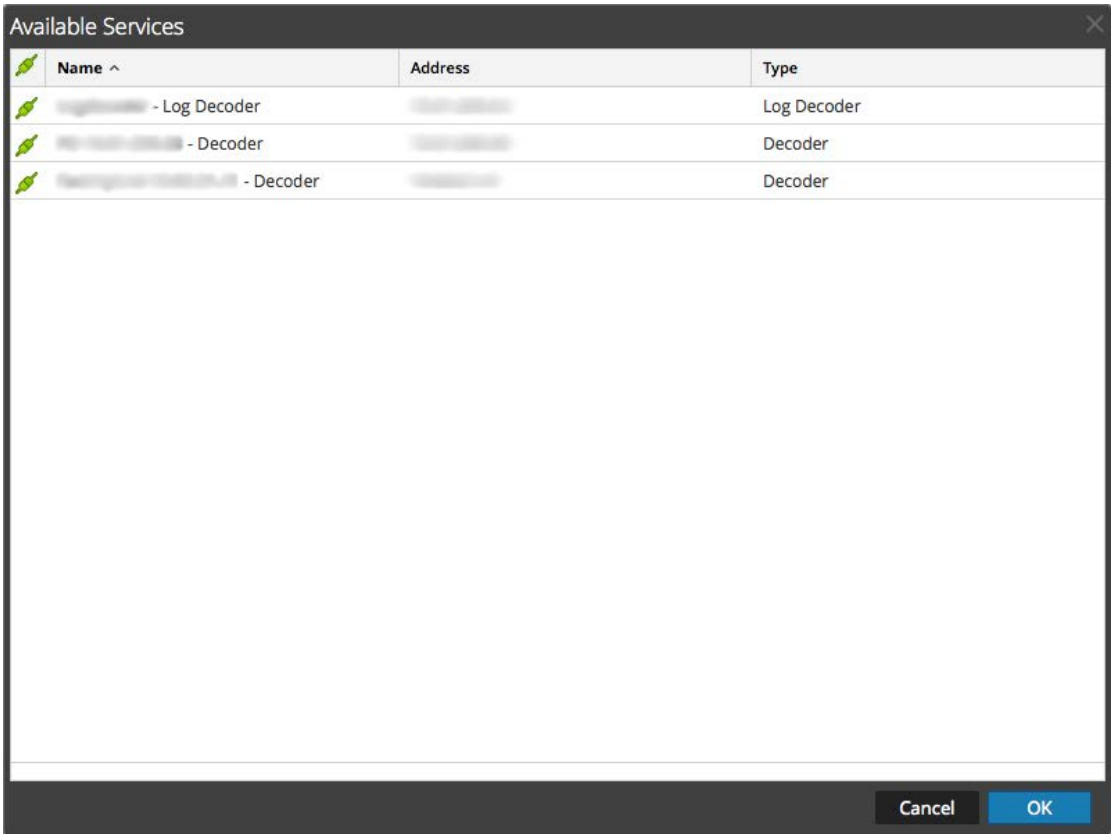
Sie müssen die folgenden Schritte ausführen, um eine Datenquelle hinzuzufügen:

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

Methoden

Hinzufügen vorhandener Services als Datenquelle

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie in der Ansicht „Services“ einen ESA-Service aus.
3. Wählen Sie in der Spalte **Aktionen** die Optionen **Ansicht > Konfiguration** aus.
4. Klicken Sie auf der Registerkarte **Datenquellen** auf +.
   Die verfügbaren Services werden wie in der folgenden Abbildung dargestellt angezeigt.



5. Wählen Sie einen oder mehrere Services aus und klicken Sie auf **OK**.
   Der Service wird der Liste der Services auf der Registerkarte **Datenquellen** hinzugefügt.
6. (Optional) Klicken Sie auf **Aktivieren**, um die Datenquelle zu aktivieren.
7. 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. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
   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 **Save**.

Schritt 3. Konfigurieren erweiterter Einstellungen für einen ESA-Service

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

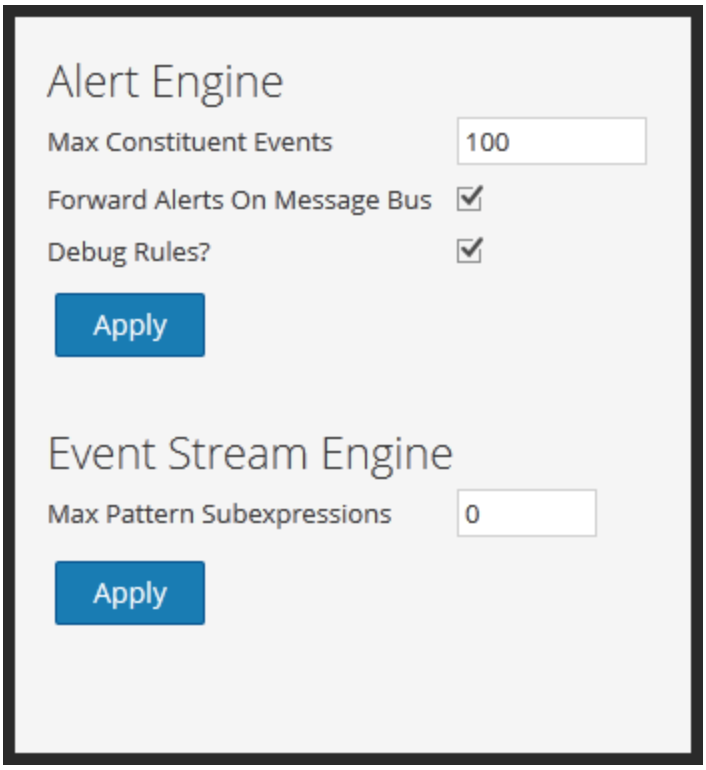
In der Ansicht „Erweitert“ können Sie erweiterte Einstellungen konfigurieren, um eine verbesserte Performance zu erzielen, die Ereignisanzahl für Regeln mit mehreren Ereignissen zu beschränken, Ereignisse im Arbeitsspeicher zu puffern und die Anzahl der in der ESA zu speichernden Ereignisse festzulegen.

Methoden

Konfigurieren von erweiterten Einstellungen

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

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie in der Ansicht „Services“ einen ESA-Service aus.
3. Wählen Sie in der Spalte **Aktionen** die Optionen **Ansicht > Konfiguration** aus.
4. Wechseln Sie zur Registerkarte **Erweitert**.
   Die Ansicht „Erweitert“ wird angezeigt.

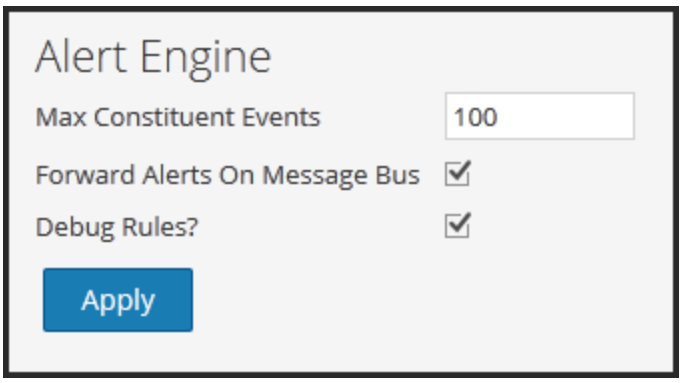


Konfigurieren der Warnmeldungs-Engine-Einstellungen

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“ an.



So konfigurieren Sie die Warnmeldungs-Engine-Einstellungen:

1. Geben Sie im Bereich „Warnmeldungs-Engine“ einen Wert für **Max. Bürgerereignisse** ein. Der Standardwert ist 100.

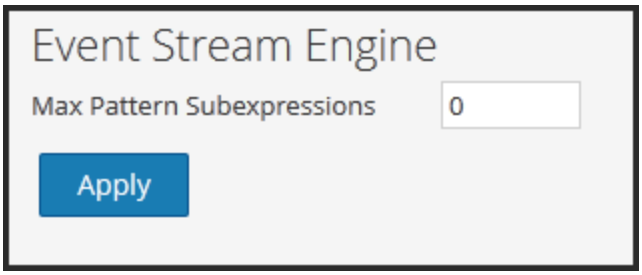
2. Wenn die Warnmeldungen an den Nachrichtenbus und an Incident Management gesendet werden sollen, aktivieren Sie die Option **Warnmeldungen an Nachrichtenbus weiterleiten**.
3. Wählen Sie **Regeln debuggen?** aus, um das Debugging von Regeln zu aktivieren.
4. Klicken Sie auf **Anwenden**, um Änderungen 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.

Schritt 4. Konfigurieren eines ESA-Services zur Herstellung einer Verbindung mit dem Context Hub auf einem anderen ESA-Service

In diesem Thema erfahren Administratoren, wie sie einen ESA-Service für die Herstellung einer Verbindung mit den Context Hub auf einem anderen ESA-Service konfigurieren. Pro Security Analytics-Installation kann jeweils nur ein Context Hub installiert werden. Wenn Sie mehrere ESA-Services haben und den Context Hub ausführen, müssen Sie den ESA-Service ohne den Context Hub aktivieren, um mit dem Context Hub auf einem anderen ESA-Service zu kommunizieren.

Voraussetzungen

Sie müssen mehrere ESAs und einen Context Hub ausführen.

Verfahren

Konfigurieren Sie den ESA-Service für die Herstellung einer Verbindung mit dem Context Hub auf einem anderen ESA-Service.

1. Notieren Sie die IP-Adresse des ESA-Services, auf dem der Context Hub-Service ausgeführt wird.
2. Wählen Sie unter „Administration“ > „Services“ den ESA-Service aus, auf dem der Context Hub-Service nicht ausgeführt wird, und wählen Sie dann  >**Ansicht** > **Durchsuchen** aus.
3. Navigieren Sie im linken Bereich zu **Service** > **Context Hub** und wählen Sie dann **contextHubTransport** aus.
4. Bearbeiten Sie das Feld **Host** so, dass es auf den Domainnamen oder die IP-Adresse des ESA-Services verweist, der den Context Hub-Service ausführt.

Ergebnis

Der ESA-Service stellt eine Verbindung mit dem Context Hub auf einem anderen ESA-Service her.

Zusätzliche Verfahren

Dieses Thema ist eine Sammlung einzelner Verfahren, die ein Administrator jederzeit durchführen kann, und es ist nicht erforderlich, dass sie die anfängliche Einrichtung von ESA abschließen. Diese Verfahren sind in alphabetischer Reihenfolge aufgeführt.

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

Ändern der Standard-Speicherpasswörter

Indiesem Thema erfahren Administratoren, wie sie Standard-Speicherpasswörter ändern für Datenbankkonten, die Warnmeldungen in ESA, Incident Management und Data Science speichern.

Security Analytics 10.5 verwendet MongoDB als Datenbank zur Speicherung von Warnmeldungen in den folgenden Modulen:

- ESA
- Incident Management
- Data Science

Die Datenbank in jedem Modul verfügt über ein Konto zur Steuerung des Zugriffs und jedes Security Analytics-Servicekonto hat ein Standardpasswort.

Um die Sicherheit zu erhöhen, empfiehlt RSA, die Standardpasswörter zu ändern. In einigen Unternehmen sind Standardpasswörter nicht zulässig. In diesen Fällen sind die Verfahren in diesem Thema obligatorisch.

Dieses Thema erklärt, wie Sie das Standardpasswort für das Datenbankkonto in jedem Modul ändern.

Vorheriges ESA-Speicherpasswort

ESA wurde in Security Analytics 10.3 eingeführt, als die Datenbank in PostgreSQL vorlag. Wenn Sie ESA in Version 10.3 verwendet haben und ein angepasstes Passwort für die PostgreSQL-Datenbank erstellt haben, hat dies keine Auswirkungen auf MongoDB. Wenn Sie Security Analytics 10.5 installieren oder ein Upgrade darauf durchführen, wird MongoDB mit dem Standardpasswort installiert.

Incident Management und Data Science wurden in Security Analytics 10.4 eingeführt. Daher wurde dort immer MongoDB verwendet.

Abhängigkeiten

MongoDB hat ein Master-Adminkonto, das Rechte über die Datenbankkonten für die Services ESA, Incident Management und Data Science hat.

Hinweis: Sie müssen zuerst das Passwort des Adminkontos ändern. Sie können Passwörter für die Services in jeder beliebigen Reihenfolge ändern.

ESA ist für Incident Management und Data Science obligatorisch. Die Konfiguration für die einzelnen Module verweist auf den Host, der den ESA-Service ausführt. Die Datenbanken für ESA, Incident Management und Data Science befinden sich auf dem Host, auf dem der ESA-Service ausgeführt wird.

Datenbankberechtigungen

Die folgende Abbildung zeigt die Berechtigungen, die jedem Konto während des Installations- oder Upgradeprozesses zugewiesen werden.

Konto	Rechte	Datenbank
admin	readWriteAnyDatabase userAdminAnyDatabase dbAdminAnyDatabase	All
Event Stream Analysis	readWrite dbAdmin clusterAdmin	ESA
Incident Management	readWrite dbAdmin clusterAdmin	IM

Konto	Rechte	Datenbank
Data Science	readWrite dbAdmin clusterAdmin	Data Science

Weitere Informationen zum Ändern jedes Passworts finden Sie unter:

- Ändern des MongoDB-Passworts für das Administratorkonto
- Ändern des ESA-Speicherpassworts
- Ändern des Incident Management-Speicherpassworts
- Ändern des Data Science-Speicherpassworts

Ändern des MongoDB-Passworts für das Administratorkonto

Dieses Thema enthält Anweisungen für Administratoren zum Ändern des Standardspeicherpassworts für das MongoDB-Administratorkonto.

In Security Analytics ist dieses Verfahren optional. Es gilt jedoch immer als Best Practice für Administratoren, jedes Standardpasswort für zusätzliche Sicherheit zu ändern. Einige Unternehmen lassen Standardpasswörter nicht zu.

Hinweis: Sie müssen zuerst das MongoDB-Passwort für das Administratorkonto ändern. Sie müssen es eingeben, bevor Sie die Passwörter für ESA, Incident Management und Data Science ändern können.

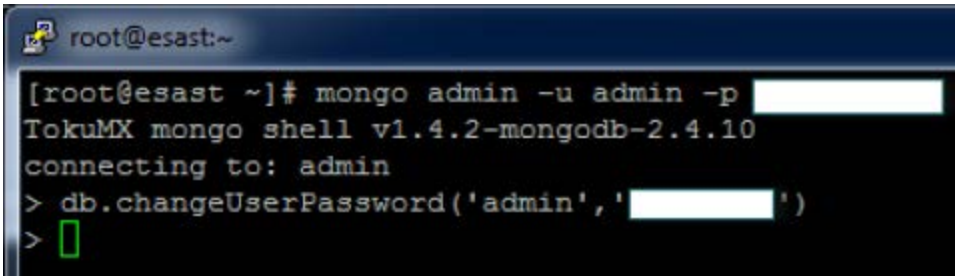
Voraussetzungen

Sie müssen über die Berechtigungen der Administratorrolle verfügen.

Verfahren

1. Melden Sie sich bei dem ESA-Host an, auf dem der ESA-Service ausgeführt wird:
   a. Greifen Sie mit SSH-Verschlüsselung auf den ESA-Host zu.
   b. Melden Sie sich als Root an.

2. Melden Sie sich bei MongoDB als admin an. Das Standardpasswort ist netwitness.
   `mongo admin -u admin -p <current_password>`



3. Geben Sie zum Ändern des Passworts für das Administratorkonto Folgendes ein:
   `db.changeUserPassword('admin','<new_password>')`

   Jetzt können Sie das Passwort für die Services ESA, Incident Management und Data Science ändern.

Ändern des ESA-Speicherpassworts

In diesem Thema erfahren Administratoren, wie sie das Standardspeicherpasswort für die ESA-Datenbank ändern können.

In Security Analytics ist dieses Verfahren optional. Es gilt jedoch immer als Best Practice für Administratoren, jedes Standardpasswort für zusätzliche Sicherheit zu ändern. Einige Unternehmen lassen Standardpasswörter nicht zu und machen dieses Verfahren obligatorisch.

Voraussetzungen

Sie müssen über die Berechtigungen der Administratorrolle verfügen.

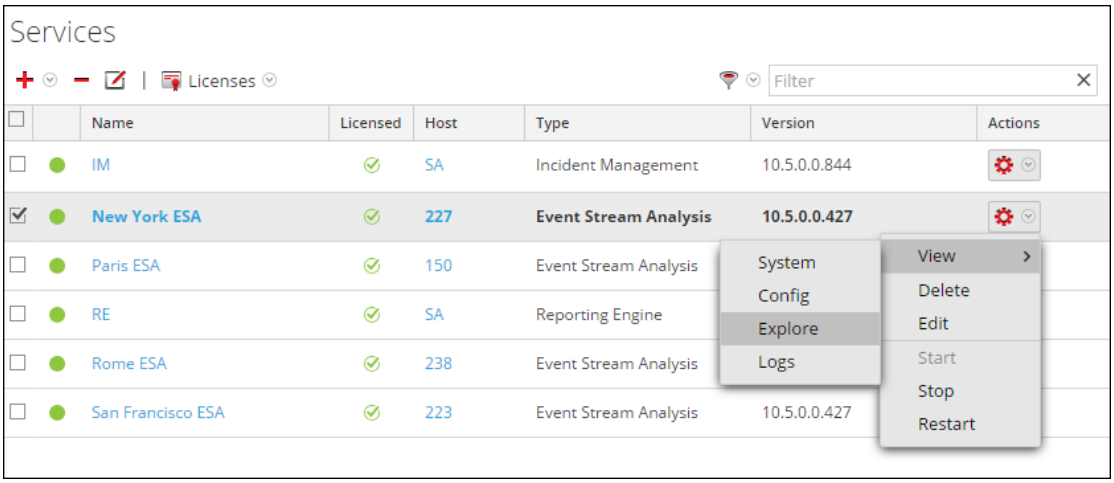
Methoden

Ändern des Passworts für das ESA-Datenbankkonto

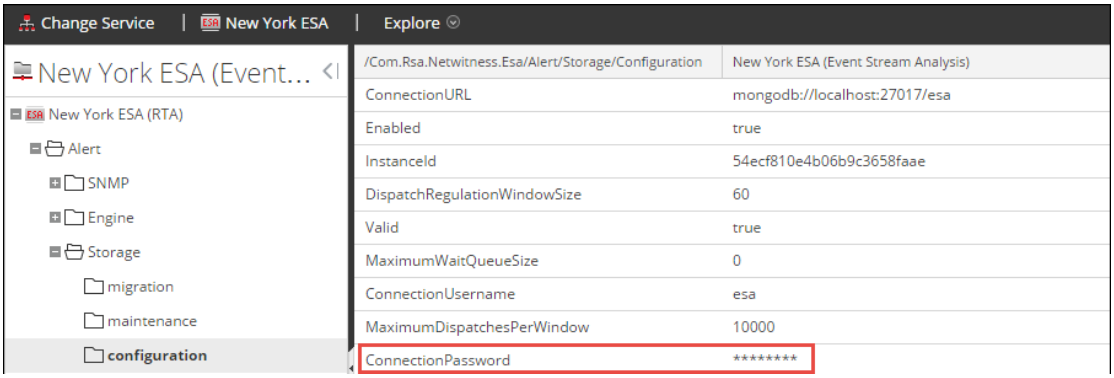
1. Melden Sie sich bei dem Host an, auf dem der ESA-Service ausgeführt wird:
   a. Greifen Sie mit SSH-Verschlüsselung auf den ESA-Host zu.
   b. Melden Sie sich als **Root** an.
2. Melden Sie sich als Administrator bei der Mongo-Datenbank an.
   `mongo esa -u admin -p <current_admin_password> --authenticationDatabase admin`
3. Geben Sie folgenden Befehl ein, um das Passwort für das ESA-Konto zu ändern. Das Standardpasswort lautet „esa“.
   `db.changeUserPassword('esa','<new_password>')`

Ändern des Passworts für den ESA-Service

1. Melden Sie sich als Administrator bei Security Analytics an.
2. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.



3. Wählen Sie den ESA-Service und anschließend  **> Ansicht > Durchsuchen** aus.
4. Wählen Sie in der Ansicht „Durchsuchen“ auf der linken Seite **Warnmeldung > Speicher > Konfiguration** aus.



5. Geben Sie im rechten Bereich im Feld **Verbindungspasswort** das Passwort für das Datenbankkonto ein.

Hinweis: Die Passwörter für die Datenbank und die Security Analytics-Servicekonfiguration müssen identisch sein.

6. Wenn Sie überprüfen möchten, ob die Passwörter für die Datenbank und Security Analytics übereinstimmen, wählen Sie im Menü „Security Analytics“ die Optionen **Warnmeldungen > Zusammenfassung** aus.

   Wenn auf der Registerkarte „Zusammenfassung“ Inhalt angezeigt wird, stimmen die Passwörter überein und wurden erfolgreich geändert.

   Wenn auf der Registerkarte „Zusammenfassung“ kein Inhalt angezeigt wird, müssen Sie

das Servicepasswort so ändern, dass es mit dem Passwort für die Mongo-Datenbank übereinstimmt.

Ändern des Incident Management-Speicherpassworts

Dieses Thema enthält Anweisungen für Administratoren zum Ändern des Standardspeicherpassworts für die Incident Management-Datenbank.

In Security Analytics ist dieses Verfahren optional. Es gilt jedoch immer als Best Practice, jedes Standardpasswort für zusätzliche Sicherheit zu ändern. In einigen Unternehmen, die Standardpasswörter nicht zulassen, ist dieses Verfahren obligatorisch.

Voraussetzungen

Sie müssen über die Berechtigungen der Administratorrolle verfügen.

Das Standardpasswort für das MongoDB-Admin-Konto muss geändert werden.

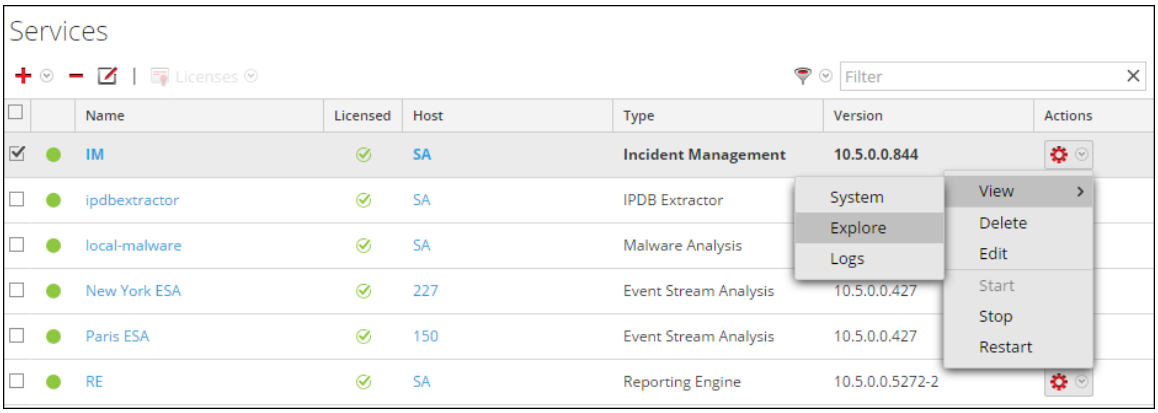
Methoden

Ändern des Passworts für das Incident Management-Datenbankkonto

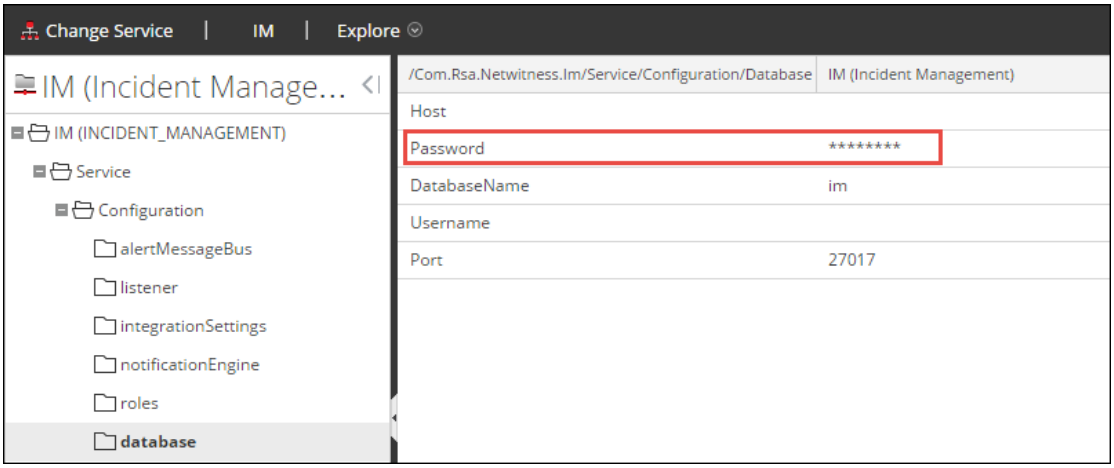
1. Melden Sie sich bei dem Host an, auf dem der ESA-Service ausgeführt wird:
   a. Greifen Sie mit SSH-Verschlüsselung auf den ESA-Host zu.
   b. Melden Sie sich als Root an.
2. Melden Sie sich bei der MongoDB als Administrator an:
   ```
   mongo im -u admin -p {current_admin_password} --
   authenticationDatabase admin
   ```
3. Geben Sie den folgenden Befehl ein, um das Passwort für das Incident Management-Konto zu ändern. Das Standardpasswort lautet **im**.
   ```
   db.changeUserPassword('im','{new_password}')
   ```

Ändern des Passworts für den Incident Management-Service

1. Melden Sie sich als Administrator bei Security Analytics an.
2. Wählen Sie im Menü **Security Analytics** die Optionen **Administration** > **Services** aus.



3. Wählen Sie den Incident Management-Service und dann > **Ansicht** > **Durchsuchen** aus.
4. Wählen Sie in der Ansicht „Durchsuchen“ auf der linken Seite **Konfiguration** > **Datenbank** aus.



5. Geben Sie im rechten Bereich im Feld **Passwort** das Passwort für das Datenbankkonto ein.

Hinweis: Die Passwörter für die Datenbank und die Security Analytics-Servicekonfiguration müssen identisch sein.

6. Starten Sie den Incident Management-Service von Neuem, um die Passwortänderung zu akzeptieren, und stellen Sie dabei sicher, dass die Sitzung mit dem neuen Passwort gestartet wird.
   a. Wählen Sie **Administration** > **Services** aus.
   b. Wählen Sie den Incident Management-Service aus und klicken Sie auf > **Neustart**.
7. Um die Übereinstimmung der neuen Passwörter zu überprüfen, wählen Sie **Incidents** > **Warnmeldungen** aus.
   Wenn auf der Registerkarte Warnmeldungen Inhalte vorhanden sind, wurden die Passwörter

erfolgreich geändert.

Falls Sie auf der Registerkarte „Warnmeldungen“ keine Inhalte sehen, ändern Sie das Servicepasswort dahingehend, das es mit dem Passwort der MongoDB übereinstimmt.

Ändern des Data Science-Speicherpassworts

In diesem Thema erfahren Administratoren, wie Sie das Standardspeicherpasswort für die Data Science-Datenbank ändern können.

In Security Analytics ist dieses Verfahren optional. Es gilt jedoch immer als Best Practice, jedes Standardpasswort für zusätzliche Sicherheit zu ändern. In einigen Unternehmen, die Standardpasswörter nicht zulassen, ist dieses Verfahren obligatorisch.

Voraussetzungen

Sie müssen über die Berechtigungen der Administratorrolle verfügen.

Das Standardpasswort für das MongoDB-Admin-Konto muss geändert werden.

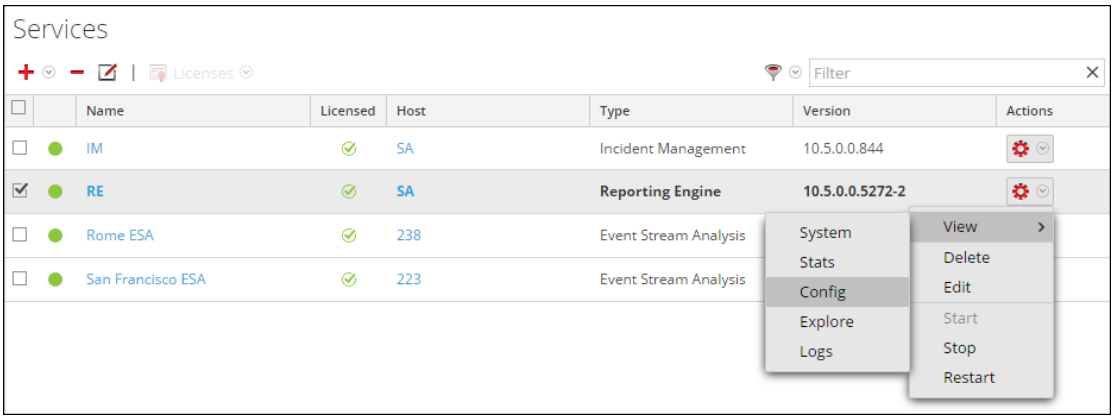
Methoden

Ändern des Data Science-Passworts für Datenbankkonten

1. Melden Sie sich bei dem Host an, auf dem der ESA-Service ausgeführt wird.
   a. Greifen Sie mit SSH-Verschlüsselung auf den ESA-Host zu.
   b. Melden Sie sich als Root an.
2. Melden Sie sich bei MongoDB als admin an.
   ```
   mongo ds -u admin -p {current_admin_password} --
   authenticationDatabase admin
   ```
3. Geben Sie zum Ändern des Data Science-Passwords folgendes ein:
   ```
   db.changeUserPassword('ds','{new_password}')
   ```

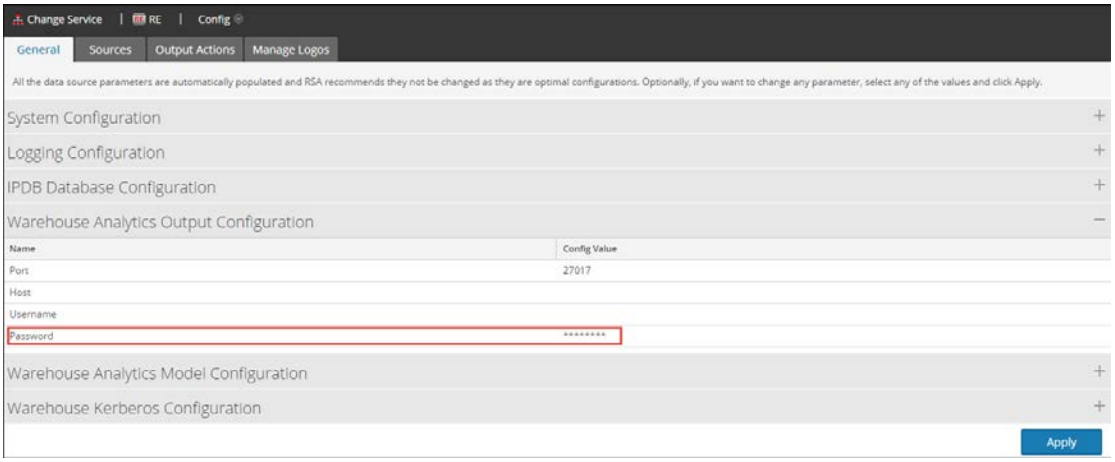
Ändern des Data Science-Passworts für Security Analytics

1. Melden Sie sich als Administrator bei Security Analytics an.
2. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.



3. Wählen Sie den Reporting Engine-Service und anschließend die Optionen  **> Ansicht > Konfiguration** aus.

   Die Ansicht „Konfiguration“ wird mit geöffneter Registerkarte „Allgemein“ angezeigt.



4. Wählen Sie **Warehouse Analytics – Ausgabekonfiguration** aus.
5. Geben Sie das Passwort für das Datenbankkonto im Feld **Passwort** ein.

Hinweis: Die Passwörter für die Datenbank und die Security Analytics-Servicekonfiguration müssen identisch sein.

6. Führen Sie zur Validierung der Übereinstimmung der neuen Passwörter einen Bericht in der Reporting Engine aus, die Warehouse Analytics verwendet.

Ändern des Speicherschwellenwerts für Testregeln

In diesem Thema erfahren Administratoren, wie Sie einen Schwellenwert für die Speichernutzung von Testregeln festlegen. Wenn der Schwellenwert überschritten wird, werden alle bereitgestellten Testregeln deaktiviert.

Dieses Verfahren ist optional. 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

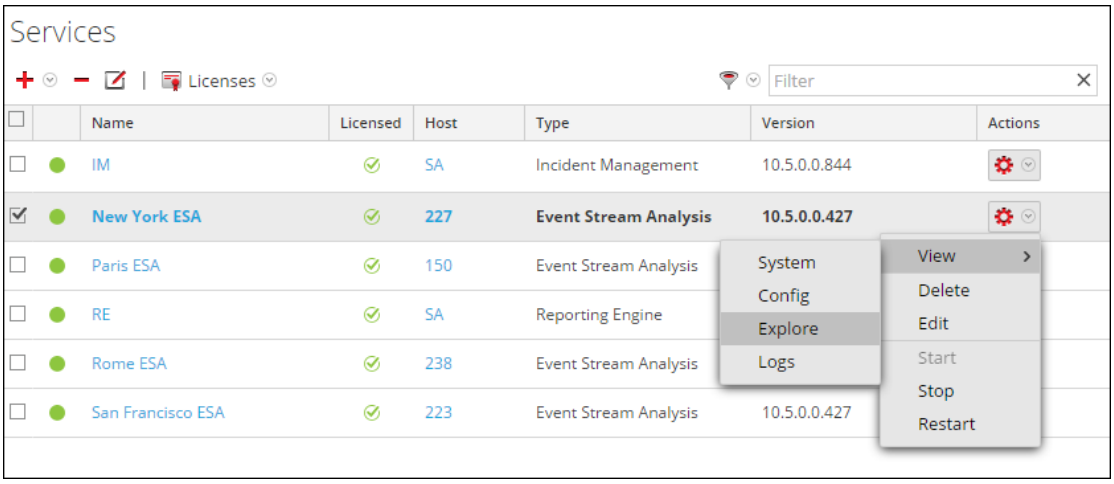
Weitere Informationen finden Sie unter „Arbeiten mit Testregeln“ im „Handbuch zum Versenden von Warnmeldungen mit ESA“.

Voraussetzungen

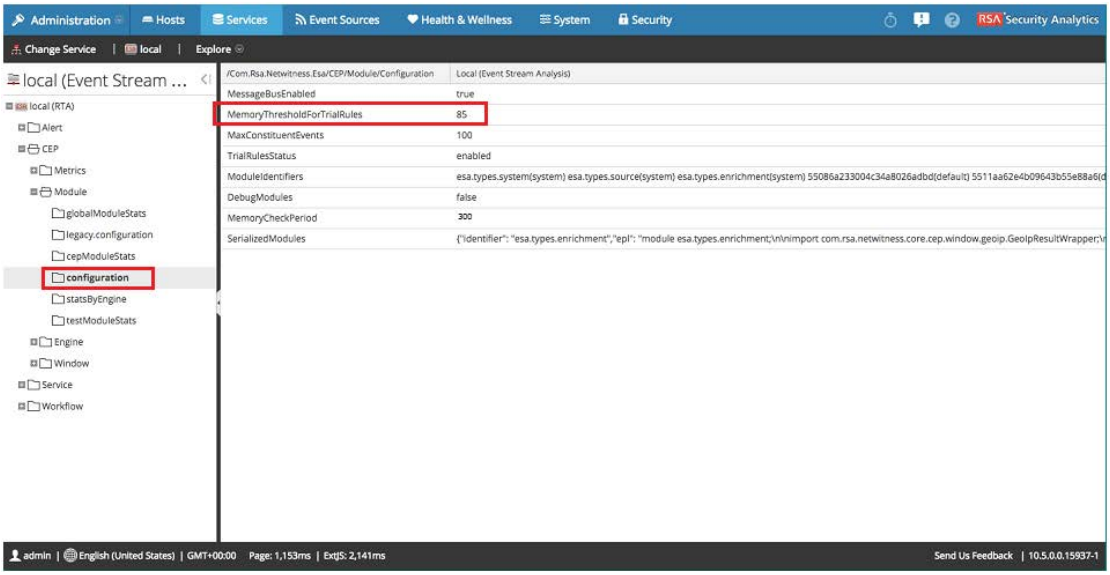
Ihnen muss eine Rolle mit Administratorrechten zugewiesen sein.

Verfahren

1. Melden Sie sich als Administrator bei Security Analytics an.
2. Wählen Sie im Menü **Security Analytics** die Optionen **Administration** > **Services** aus.



3. Wählen Sie den ESA-Service und anschließend >**Ansicht** > **Durchsuchen** aus.
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 Speicherschwellenwert wird sofort wirksam.

Konfigurieren des ESA-Speichers

In diesem Thema wird die Konfiguration der ESA-Datenbank zur Aufrechterhaltung eine angemessenen Menge an Warnmeldung erklärt.

Dieses Verfahren ist optional. Administratoren können eine Aufbewahrungsfrist für Warnmeldungen angeben. Das Löschen alter Warnmeldungen ist eine Best Practice zur Wartung der Warnmeldungsdatenbank. Andernfalls würde die Datenbank stetig wachsen, was schließlich negative Auswirkungen auf die Performance hätte.

Standardmäßig ist die Funktion zur automatischen Löschung von Warnmeldungen nicht aktiviert, da jedes Unternehmen eigene Richtlinien hat. In diesem Thema erfahren Sie, wie Sie die folgenden Aufgaben durchführen:

- Aktivieren der automatischen Löschung von Alarmen
- Festlegen der Kriterien für die Löschung von Alarmen
  - Nach Datenbankgröße
  - Nach Alter der Warnmeldung
  - Nach Datenbankgröße und Alter der Warnmeldung

Konfigurationsparameter

Die folgende Konfigurationsparameter sind verfügbar:

Parameter	Beschreibung
Aktiviert	Aktiviert die Funktion für die Warnmeldungsaufbewahrung
NextMaintenanceScheduledAt	(Schreibgeschützt) Der Zeitpunkt, zu dem die Ausführung der nächste Wartung geplant ist.
HaveAlertForDays	(Schreibgeschützt) Aktuelle Anzahl an Tagen, die Warnmeldungen in der Datenbank gespeichert sind. Beispiel: Wenn diese Zahl am 4. Juni überprüft wird und ab dem 1. Juni täglich Warnmeldungen erzeugt wurden, wäre der Wert 4.
DatabaseDiskUsage	(Schreibgeschützt) Aktuelle Datenbankgröße.

Parameter	Beschreibung
Schedule	Planung für das Ausführen der Warnmeldungswartung. Die Planung verwendet die UNIX-Crontab und muss im korrekten Crontab-Format angegeben werden. Der Standardwert ist im Verfahren unten dargestellt. Weitere Informationen zur Cron-Planung erhalten Sie unter http://www.cronmaker.com.
DatabaseDiskUsageLimtInMB	Schwellenwert für die Datenbankgröße. Wird dieser überschritten, werden Warnmeldungen gelöscht.
Gültig	Schreibgeschützter Parameter, der anzeigt, ob die aktuelle Konfiguration gültig ist.
DaysToDeleteWhenLimitExceeded	Anzahl der zu entfernenden Tage, wenn DatabaseDiskUsageLmitInMB überschritten wird.
KeepAlertsForDays	Anzahl der Tage, die Warnmeldungen vor dem Löschen in der Datenbank aufbewahrt werden.

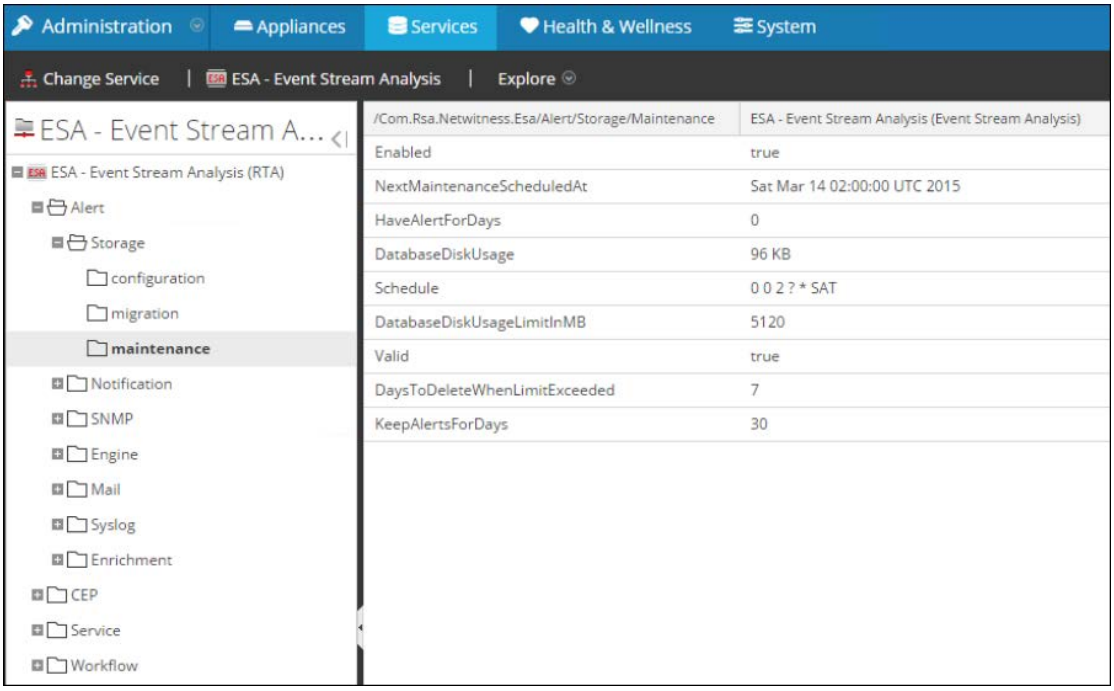
Voraussetzungen

Sie benötigen Administratorberechtigungen.

Verfahren

1. Melden Sie sich als Administrator bei Security Analytics an.
2. Wählen Sie im Security Analytics-Menü die Optionen **Administration > Services** aus.
3. Wählen Sie den ESA-Service und anschließend **Ansicht > Durchsuchen** aus.

4. Wählen Sie auf der linken Seite **Warnmeldung > Speicher > Wartung** aus.



5. Wählen Sie im Feld **Aktiviert** die Option wahr aus, um die Funktion für die Warnmeldungsaufbewahrung zu aktivieren.
6. Konfigurieren Sie, wie alte Warnmeldungen entfernt werden sollen:
   - Nach Datenbankgröße: Geben Sie in **DatabaseDiskUsageLimitInMB** die maximale Datenbankgröße ein. Geben Sie dann in **DaysToDeleteWhenLimitExceeded** ein, wie viele Tage mit den ältesten Warnmeldungen gelöscht werden sollen. Beispiel: Wenn die Festplattenauslastung 5.120 MB erreicht, sollen 7 Tage mit den ältesten Warnmeldungen gelöscht werden.
   - Nach Alter der Warnmeldung: Es werden alle Warnmeldungen gelöscht, die älter als **KeepAlertsForDays** sind.

     Hinweis: In Security Analytics 10.4.1 und darunter müssen Sie KeepAlertsForDays verwenden. DatabaseDiskUsageLimitInMB kann nicht verwendet werden.

   - Nach Datenbankgröße und Alter der Warnmeldung: Wenn Sie beide Parameter konfigurieren, wird die Regel verwendet, durch die die höhere Anzahl an Warnmeldungen gelöscht wird.
7. **Schedule**

   Verwenden Sie den Planungsparameter, um ESA mitzuteilen, wie oft der Job für die

Warnmeldungswartung ausgeführt werden soll (d. h. wie häufig die Datenbank überprüft und die Löschungsregeln angewandt werden). Verwenden Sie die Syntax für einen Cron-Planungsjob. Weitere Informationen über die Cron-Planung finden Sie unter http://www.cronmaker.com.

8. **Aktualisieren** Sie das Browserfenster.
   - Das Datum und die Zeit der nächsten Wartung werden im Feld **NextMaintenanceScheduledAt** angezeigt.
   - Im Feld **Gültig** wird „wahr“ angezeigt. Dies bedeutet, dass die Konfiguration gültig ist. Wenn falsch angezeigt wird, korrigieren Sie die Einstellungen für die Festplattengröße oder das Warnmeldungsalter.
9. (Optional) Der Wartungsstatus kann auch in der Datei /opt/rsa/esa/logs/esa.log auf dem ESA-Host überwacht werden, der Meldungen ähnlich dem Beispiel unten anzeigt.

Beispiel

Der Wartungsstatus kann auch in der Datei /opt/rsa/esa/logs/esa.log auf dem ESA-Service überwacht werden, der Meldungen ähnlich dem Beispiel unten anzeigt.

```
2015-03-12 09:46:48,197 [Carlos@65dd6c04-56] INFO
com.rsa.netwitness.carlos.config.ConfigurationMXBean -
 MongoStorageMaintenance changed by admin
 2015-03-12 09:46:51,121 [scheduler_Worker-1] INFO
  com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
Starting the scheduled database maintenance
 job with policy {keepAlertForDays=30, maxDiskUsageInMb=5120}
 2015-03-12 09:46:51,122 [Carlos@3801f0b3-58] INFO
  com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
Scheduled a database maintenance job with
 policy {keepAlertForDays=30, maxDiskUsageInMb=5120} to run at 2/28/15
2:00 AM
 2015-03-12 09:46:51,129 [Carlos@3801f0b3-58] INFO
com.rsa.netwitness.carlos.config.ConfigurationMXBean -
 MongoStorageMaintenance changed by admin
 2015-03-12 09:46:51,133 [scheduler_Worker-1] INFO
  com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
Finished the database maintenance job,
 deleted 0 partitions, next run scheduled at 3/14/15 2:00 AM
```

Konfigurieren von ESA für die Verwendung eines Speicherpools

In diesem Thema erfahren Administratoren, wie sie den ESA-Service 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 Speicherpool verwenden, statt alle Ereignisse im Arbeitsspeicher aufzubewahren, können die Ereignisse auf die Festplatte geschrieben 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.

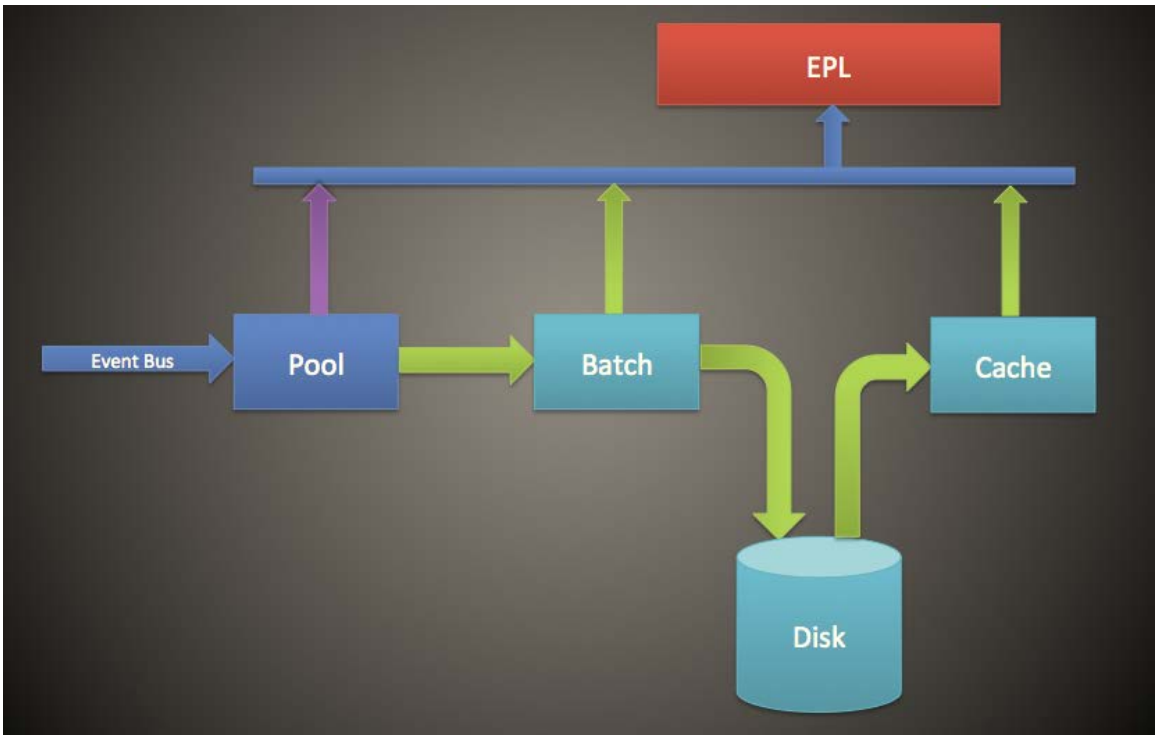
- **Batch-Modus.** Im Batch-Modus werden Ereignisse in Batches gruppiert und dann auf die Festplatte geschrieben. Legen Sie zum Konfigurieren des Batch-Modus das Attribut **MapPoolBatchWriteSize** auf einen größeren Wert als 1 fest. Der Batch-Modus bietet eine bessere Performance, da die Festplattenaktivität 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. Wählen Sie unter **Administration** > **Services** den ESA-Service und dann > **Ansicht** > **Durchsuchen** aus.
2. Wählen Sie **CEP** > **EsperPool** > **Konfiguration** aus.
3. Geben Sie Werte für die folgenden Felder ein:

Attribut	Beschreibung	Konfiguration

MapPoolPersistenceURI	Speicherort zum Speichern der Speicherpooldatei.	Der Standardwert ist **/opt/rsa/esa/pool/esperPool**. RSA empfiehlt, den Standardwert nicht zu ändern. Wenn Sie diese Einstellung ändern, um eine andere Partition zu verwenden, stellen Sie sicher, dass die Partition mindestens zehnmal mehr Speicherplatz als der für ESA zugewiesene Speicher enthält. **Achtung:** 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.
MapPoolEnable	Aktivieren oder deaktivieren Sie den Speicherpool.	Der Standardwert ist **false**. Legen Sie den Wert auf **true** fest, um den Speicherpool zu aktivieren. Wenn Sie den Speicherpool aktivieren oder deaktivieren, ist ein Neustart erforderlich.
MapPoolFlushIntervalSecs	Zeitintervall zum Leeren von Ereignissen an die Festplatte. Beispielsweise wird jedes Ereignis, das länger als 15 Minuten in Esper verbleibt, auf die Festplatte geleert.	Der Standardwert ist **15 Minuten**. 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. **Hinweis:** 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.

MapPoolBatchWriteSize	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. Zur Verwendung des Non-Batch-Modus legen Sie diesen Wert auf 1 fest. Zur Verwendung des Batch-Modus legen Sie diesen Wert auf einen höheren Wert als 1 fest.	Die Standard-Batchgröße beträgt **100.000** 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. 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.
MapPoolMinSize	Mindestgröße des Speicherpools. Dieser Wert wird für die Initialisierung verwendet, erfordert in der Regel also keine Bearbeitung.	Der Standardwert ist **10.000** Ereignisse. Ein höherer Wert kann die Performance steigern. Ein niedrigerer Wert sorgt dafür, dass das System stabiler ist.
MapPool Persist Type	Dies ist ein schreibgeschützter Parameter, der den Typ der verwendeten Optimierung angezeigt.	Der Standardwert ist **RMSerialize**.

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.

Hinweis: 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“

In diesem Thema erfahren Administratoren, wie sie 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. Gleichzeitig erfasste Sitzungen werden auf diese Weise miteinander korreliert und Warnmeldungen entsprechen selbst bei Übertragungsverzögerungen den Benutzererwartungen. 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.

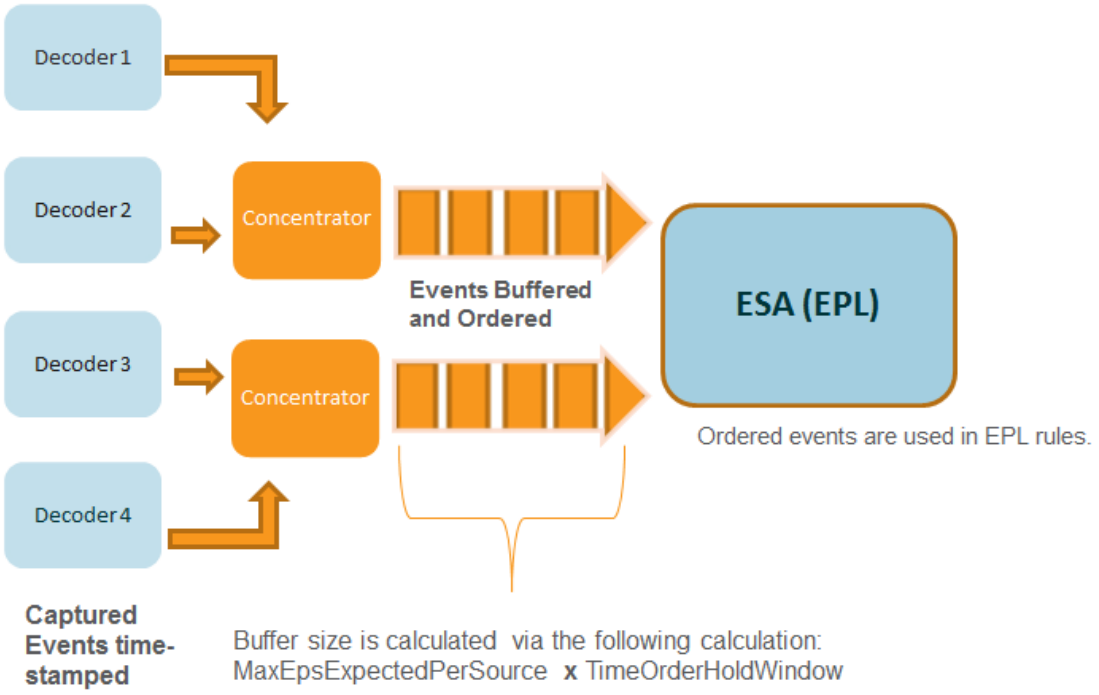
Angenommen, Sie verfügen über zwei Quellen mit Ereignissen, die um 10:00 Uhr stattfinden. Mithilfe von „Ordnen nach Erfassungszeit“ werden diese Ereignisse so lange im Puffer behalten, bis ESA erkennt, dass alle um 10:00 Uhr stattfindenden Ereignisse dem Puffer hinzugefügt wurden. Sobald alle Ereignisse 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. Wählen Sie im Menü „Security Analytics“ die Optionen **Administration** > **Services** aus. Wählen Sie den ESA-Service und anschließend >Ansicht >Durchsuchen **aus.**
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 Ordnens 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.

MaxEPSExpectedPerSource	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). Wenn Sie diese Rate zu niedrig einstellen, wirkt sich dies kurzzeitig auf die Performance aus. Allerdings erhöht ESA den Wert für `MaxEPSExpectedPerSource` nach Bedarf automatisch, damit das Ordnen nach Erfassungszeit erfolgreich ist. Der Standardwert ist 20K.
TimeOrderHoldWindow	Geben Sie in Sekunden (Ganzzahl) an, wie lange gewartet werden soll, bis Ereignisse aus allen Quellen eingetroffen sind. Konfigurieren Sie diesen Wert basierend auf der Latenz zwischen den Quellen. 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.
IdleSourceAdvanceAfterSeconds	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.
OfflineSourceAdvanceAfterSeconds	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.

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 Ordnens nach Erfassungszeit

1. Wählen Sie im Menü „Security Analytics“ die Optionen **Administration** > **Services** aus. Wählen Sie den ESA-Service und anschließend  > „Ansicht“ > „Durchsuchen“ aus.
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. Wählen Sie im Menü „Security Analytics“ die Optionen **Administration** > **Services** aus. Wählen Sie den ESA-Service und anschließend  > **Ansicht** > **Durchsuchen** aus.
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.

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:
  ```
  service tokumx start
  ```

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:
   ```
   service  rsa-esa start
   ```

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:
   ```
   service rsa-esa stop
   ```

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:
   ```
   service rsa-esa restart
   ```

Überprüfen der ESA-Komponentenversionen und Status

Dieses Thema erläutert die Überprüfung der Versionen der installierten Event Stream Analysis-Komponenten.

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-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:
   `service tokumx status`
3. Führen Sie den folgenden Befehl aus, wenn MongoDB nicht ausgeführt wird.
   `service tokumx start`

Referenzen

Dieses Thema ist eine Referenzsammlung zur Benutzeroberfläche für ESA in Security Analytics. Diese Themen sind in alphabetischer Reihenfolge aufgeführt.

Verwenden Sie diesen Abschnitt, wenn Sie eine Beschreibung der Berechtigungsbenutzeroberfläche und Definitionen der Funktionen der Benutzeroberfläche suchen.

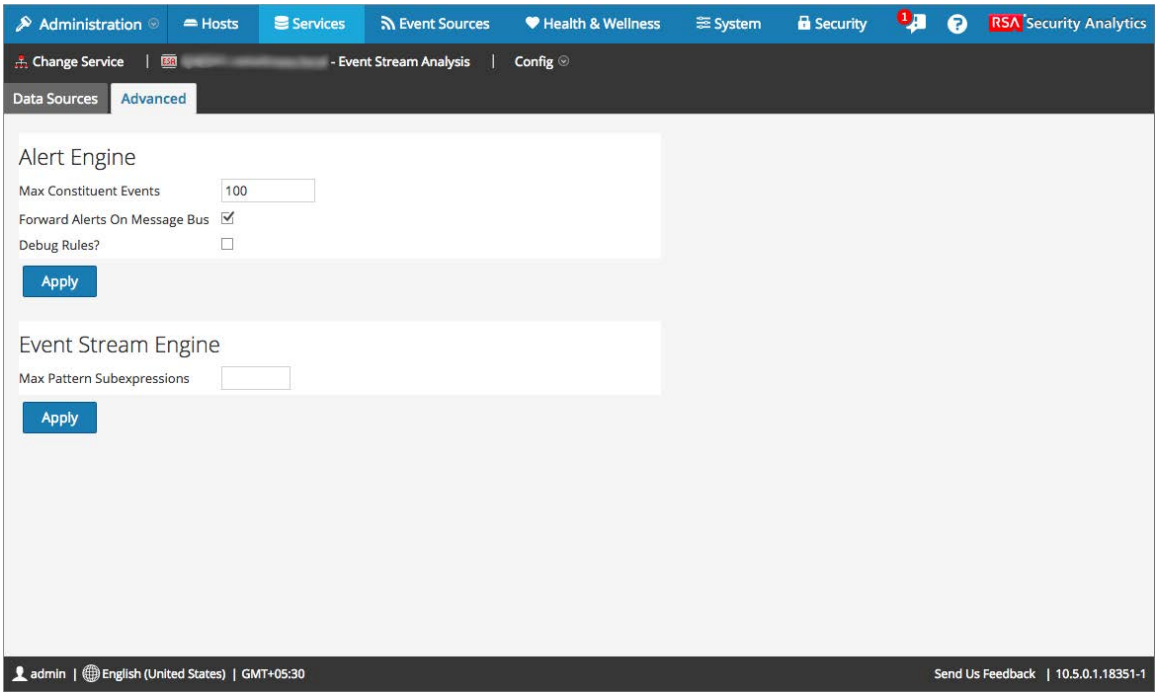
Details finden Sie in einem den folgenden Abschnitten:

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

Ansicht „Service-Konfiguration“ – Registerkarte „Erweitert“

In diesem Thema werden die Komponenten in der Ansicht „Service-Konfiguration“ auf der Registerkarte „Erweitert“ für ESA beschrieben.

Wenn Sie erweiterte Einstellungen für einen ESA-Service konfigurieren möchten, können Sie dies auf der Registerkarte **Erweitert** der Ansicht „Service-Konfiguration“ der ESA tun.



Funktionen

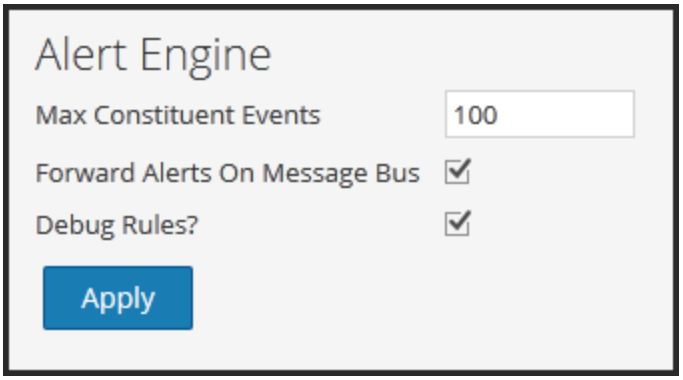
Die Erweiterte Ansicht enthält folgende Abschnitte:

- Warnmeldungs-Engine
- Ereignis-Stream-Engine

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.



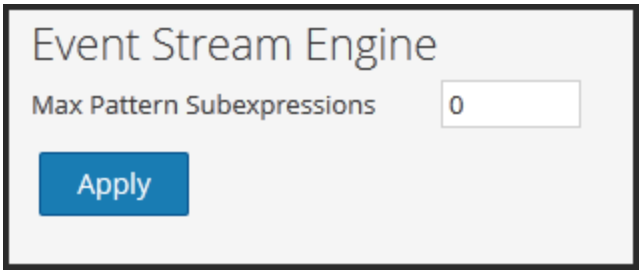
In der folgenden Tabelle werden die Parameter im Abschnitt Warnmeldungs-Engine mit einer Beschreibung aufgelistet.

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 **100**.
Warnmeldungen an Nachrichtenbus weiterleiten	Wählen Sie diese Option, wenn Sie ESA-Warnmeldungen für Incident Management weiterleiten möchten. Die erzeugten ESA-Warnmeldungen werden an den Nachrichtenbus und dann an Incident Management gesendet. Diese Option ist standardmäßig ausgewählt. Stellen Sie sicher, dass der Incident Management-Service ausgeführt wird.
Regeln debuggen?	Aktivieren Sie dieses Kontrollkästchen, um das Debugging von Regeln zu aktivieren.

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“.



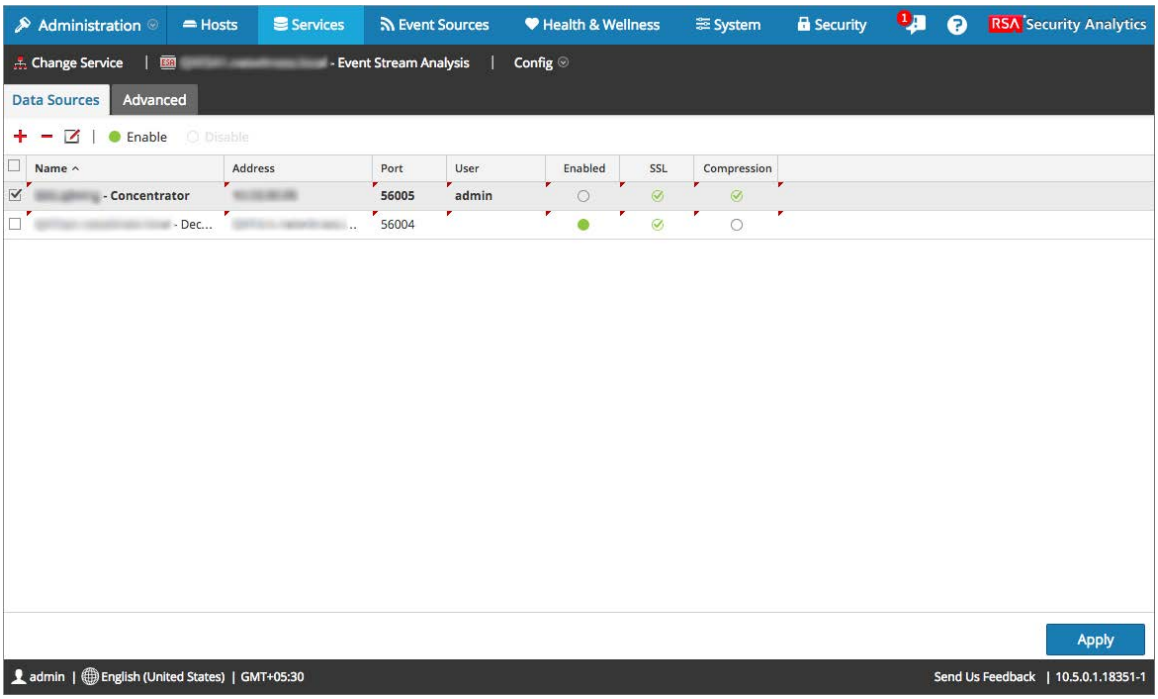
In der folgenden Tabelle werden die Parameter im Abschnitt Ereignis-Stream-Engine mit einer Beschreibung aufgelistet.

Parameter	Beschreibung
Max. Muster-Teilausdrücke	Für bestimmte Regeln muss ESPER Teilausdrücke im Speicher behalten, bevor entscheiden 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 **0**; hiermit ist die Einstellung deaktiviert. Sie müssen einen Wert festlegen, wenn Probleme mit der Stabilität des Services auftreten.

Ansicht „Service-Konfiguration“ – Registerkarte „Datenquellen“

In diesem Thema werden die Komponenten der Registerkarte „Datenquellen“ der Ansicht „Service-Konfiguration“ für ESA beschrieben.

Die Ansicht **Service-Konfiguration > Registerkarte „Datenquellen“** der ESA dient der Konfiguration der Datenquellen für ESA.



Funktionen

Die Registerkarte Datenquellen enthält folgende Abschnitte:

- Symbolleiste
- Raster Datenquellen

Symbolleiste

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

Parameter	Beschreibung
+	Fügt neue Datenquellen zu ESA hinzu.
−	Löscht eine Datenquelle aus ESA.
	Bearbeitet eine Datenquelle. Sie müssen einen Benutzernamen und ein Passwort für den Service angeben, um Änderungen vornehmen zu können.
Enable	Aktiviert die ausgewählte Datenquelle.
Disable	Deaktiviert die ausgewählte Datenquelle.

Raster Datenquellen

Im Raster „Datenquellen“ werden alle Datenquellen angezeigt, die dem ESA-Service hinzugefügt wurden. Die folgende Tabelle beschreibt die Parameter im Raster „Datenquelle“.

Parameter	Beschreibung
Name	Der Name des Datenquellenservices
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