RSA NETWITNESS® SUITE

Handbuch Versenden von Warnmeldungen mit ESA

für Version 11.0

Kontaktinformationen

Der RSA-Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2018

Inhalt

Erste Schritte mit ESA

Dieses Thema enthält eine Kurzanleitung zu RSA NetWitness® Suite Event Stream Analysis (ESA), um Ihnen bei den ersten Schritten mit ESA zu helfen. Die folgenden Themen dienen zur Unterstützung bei der Arbeit mit ESA-Korrelationsregeln.

- Best Practices helfen Ihnen dabei zu verstehen, wie Sie am besten Regeln einrichten, bereitstellen und erstellen.
- Troubleshooting für ESA für ESA hilft Ihnen beim Troubleshooting verschiedener Aspekte von ESA, einschließlich dem Erstellen und der Bereitstellung von Regeln.
- Anzeigen von Speicherkennzahlen für Regeln unterstützt Sie beim Arbeiten mit Speicherkennzahlen, um den Gesamtverbrauch an Arbeitsspeicher für ESA-Services zu verstehen.

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. Dieses Benutzerhandbuch deckt das Verwenden von Warnmeldungen mit ESA Korrelationsregeln. Informationen zum Konfigurieren von ESA-Korrelationsregeln finden Sie im Abschnitt „Konfigurieren von ESA-Korrelationsregeln“ im *Konfigurationsleitfaden für ESA*.

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 ihn verwenden zu können. Informationen zum ESA Analytics-Service finden Sie im *Handbuch zur automatisierten Bedrohungserkennung* und im Abschnitt „Konfigurieren von ESA Analytics“ im *Konfigurationsleitfaden für ESA*.

Best Practices

In den Best Practices finden Sie Guidelines zum Schreiben, Verwalten und Bereitstellen von Regeln sowie zur Bewahrung der Systemintegrität für die ESA-Services.

Grundlegendes zu Event Stream Analysis-Regeltypen

Der Event Stream Analysis-Service bietet erweiterte Streamanalysen wie Korrelation und komplexe Ereignisverarbeitung mit hohen Durchsätzen und niedriger Latenz. Er ist in der Lage, große Mengen verteilter Ereignisdaten aus den Concentrators zu verarbeiten. Damit Sie effektive Regeln erstellen, sollten Sie bei der Arbeit mit Event Stream Analysis die Faktoren berücksichtigen, die sich auf den Ressourcenverbrauch auswirken.

Jedes von ESA empfangene Ereignis wird bewertet, um festzustellen, ob es möglicherweise eine Regel auslöst. Drei Typen von Regeln können bereitgestellt werden, um zu bestimmen, wie die ESA-Engine mit dem eingehenden Ereignis verfährt. Diese Regeltypen wirken sich jeweils unterschiedlich auf die Systemressourcenauslastung aus. Alle drei Regeltypen können über die Regelerstellung oder erweiterte EPL-Regeln erstellt bzw. über RSA Live heruntergeladen werden. Die Tabelle unten enthält die Regeltypen und deren mögliche Auswirkungen auf die Systemressourcen.

Regeltyp	Beschreibung
Einfache Filterregel	Diese Regel steht nicht in Beziehung zu anderen Ereignissen. Zum Zeitpunkt der Aufnahme wird diese Regel anhand einer Reihe von Bedingungen bewertet. Wenn diese Bedingungen zutreffen, wird eine Warnmeldung erzeugt. Wenn keine Bedingungen zutreffen, wird das Ereignis schnell von der Engine freigegeben, um Arbeitsspeicher zur Verfügung zu stellen. Diese Regeln beanspruchen keinen Speicher, da die Ereignisse nicht über die Erstbewertung hinaus beibehalten werden. Die Bereitstellung von weiteren einfachen Filterregeln führt nicht zu einem Anstieg der Nutzung von Arbeitsspeicherressourcen. Wenn die Filterbedingung allerdings zu allgemein ist, können zu viele Warnmeldungen erzeugt werden. Die Systemressourcen werden dann durch das Speichern und Abrufen dieser Warnmeldungen belastet. Beispiel: Sie können eine Regel schreiben, durch die eine Warnmeldung erzeugt wird, wenn HTTP-Netzwerkaktivitäten über einen Port eingehen, der kein Standard-HTTP-Port ist.

Regeltyp	Beschreibung
Ereignisfensterregel	Diese Regel bewertet eine Reihe von Ereignissen über einen Zeitraum im Hinblick auf bestimmte Bedingungen. Zum Zeitpunkt der Aufnahme wird diese Regel anhand einer Reihe von Bedingungen bewertet. Treffen diese Bedingungen zu, verbleibt das Ereignis für eine festgelegte Dauer im Speicher. Nach Ablauf der angegebenen Zeit werden die Ereignisse aus dem Zeitfenster entfernt, wenn die Anzahl der erfassten Ereignisse nicht den Schwellenwert erreicht, um eine Warnmeldung auszulösen. Der Arbeitsspeicherverbrauch solcher Regeln hängt stark von der Ereigniseingangsrate (Datenverkehr) ab, der Menge von Daten pro Ereignis und der im Ereignisfenster festgelegten Zeitdauer. Jedes zutreffende Ereignis wird im Arbeitsspeicher behalten, bis das Zeitfenster vergangen ist. Je länger das Zeitfenster dauert, desto größer ist die Menge der Daten. Beispiel: Sie können eine Regel schreiben, die eine Warnmeldung erzeugt, wenn ein Benutzer sich nicht in einem Zeitrahmen von zehn Minuten fünfmal an einem System anmeldet.
Gefolgt-von-Regel	Diese Regel bewertet eine Kette von eingehenden Ereignissen, um zu bestimmen, ob die Reihenfolge von Ereignissen einer festgelegten Bedingung entspricht. Zum Zeitpunkt der Aufnahme wird diese Regel anhand einer Reihe von Bedingungen bewertet. Treffen die Bedingungen zu, findet eine von zwei Aktionen statt: • Ist dies das erste Ereignis der Sequenz, wird ein neuer Ereignis-Thread gestartet und das Ereignis als Kopf der Sequenz beibehalten. • Gehört das Ereignis zu einem vorhandenen Ereignis-Thread, wird es dieser Sequenz hinzugefügt. In beiden Fällen verbleibt das Ereignis im Arbeitsspeicher. Der Umfang der Ressourcennutzung hängt bei diesem Regeltyp besonders von der Kundenumgebung ab. Wenn die Filterbedingung viele Ereignis-Threads erzeugt, werden für jeden neuen Thread Ressourcen verbraucht (zusätzlich zum Ereignis). Wenn zudem der Ereignis-Thread nie das Ende erreicht (also keine Warnmeldung erzeugt wird), wird das gesamte Ereignis auf unbestimmte Zeit im Arbeitsspeicher gespeichert. Beispiel: Sie könnten eine Regel schreiben, die eine Warnmeldung erzeugt, wenn die Anmeldung eines Benutzers an einem Server fehlschlägt, der Benutzer sich dann erfolgreich anmeldet und anschließend ein neues Konto erstellt.

Zusätzlich zur oben erörterten Speichernutzung verbraucht die Erzeugung von Warnmeldungen Systemressourcen. Jede erzeugte Warnmeldung muss zum Abrufen gespeichert und zudem von NetWitness Respond verarbeitet werden. Dieser Prozess verwendet Speicherplatz auf dem Datenträger zum Speichern, nutzt Datenbankspeicher und erhöht die CPU-Auslastung durch Ausführung von Abfragen.

Berücksichtigen Sie beim Schreiben und Bereitstellen von Regeln, dass jede dieser Aktionen sich zulasten der Systemressourcen auswirkt. Anhand der Anleitungen in den folgenden Abschnitten können Sie den Verbrauch auf einem ordnungsgemäßen Niveau halten und mögliche Probleme im Falle von Systemüberlastungen entdecken.

Best Practices für das Schreiben von Regeln

Hierbei handelt es sich um allgemeine Richtlinien für das Schreiben von Regeln.

- **Warnmeldungen für Ereignisse mit ausführbaren Aktionen erstellen.** Der Zweck einer Warnmeldung ist, Sie auf ein Ereignis hinzuweisen, das sofort bestimmte Aktionen erfordert. Für Ereignisse, die keine Aktion erfordern oder über die Sie nur informiert sein müssen, können Sie einen Bericht erstellen.
- **Neue Regeln als Testregeln konfigurieren, um ihre Ausführung in der Umgebung zu beobachten.** Wenn Sie neue Regeln als Testregeln bereitstellen, werden sie bei einer Überschreitung des konfigurierten Schwellenwerts für den Arbeitsspeicher deaktiviert. Im Falle der Deaktivierung einer Testregel können Sie auch mithilfe der Snapshot-Funktion für den Arbeitsspeicher sehen, wie viel Speicher verwendet wurde. Weitere Informationen finden Sie unter Verwenden von Testregeln.
- **Erstellen von Warnmeldungsbenachrichtigungen erst, nachdem die Regel getestet und optimiert wurde.** Auf diese Weise stellen Sie sicher, dass Sie nicht übermäßig viele Warnmeldungen erhalten, falls eine Regel sich anders als erwartet verhält.
- **Regeln müssen spezifisch sein, damit Sie die Ressourcennutzung beschränken können.** Beschränken Sie die Nutzung mithilfe der folgenden Guidelines:
  - Schließen Sie mit den Filtern der Regel alle bis auf die erforderlichen Ereignisse aus, um die Regel korrekt auszulösen.
  - Definieren Sie die Fenster (Zeitfenster für die Korrelation) so kurz wie möglich.
  - Begrenzen Sie die Ereignisse, die Sie dem Fenster hinzufügen. Wenn Sie zum Beispiel nur IDS-Ereignisse anzeigen möchten, fügen Sie dem Zeitfenster nur solche Ereignisse hinzu.
- **Regeln müssen für eine verwaltbare Menge von Warnmeldungen optimiert werden.** Wenn Sie übermäßig viele Warnmeldungen erhalten, geht deren Zweck und Nutzen verloren. Beispiel: Sie möchten Informationen über verschlüsselten Datenverkehr in andere Länder

erhalten. Möglicherweise können Sie aber die Liste auf die Länder eingrenzen, die ein bekanntes Risiko darstellen. Sie beschränken dadurch die Warnmeldungen auf eine Menge, die Sie verwalten können.

Best Practices zur Verwendung von RSA Live-Regeln

Hierbei handelt es sich um Richtlinien für die RSA Live-Regeln.

- **RSA Live-Regeln in kleinen Batches bereitstellen**: Nicht jede Regel ist für jede Umgebung geeignet. Stellen Sie Ihre RSA Live-Regeln in kleinen Batches bereit, damit Sie sie in Ihrer Umgebung testen können. Dies ist die beste Methode, um sicherzustellen, dass die RSA Live-Regeln erfolgreich funktionieren. Durch die Bereitstellung in kleinen Batches können Sie viel einfacher feststellen, ob eine bestimmte Regel einen Fehler aufweist.
- **Die entsprechenden Beschreibungen der RSA Live-Regeln beachten**: ESA-Regeln passen nicht allgemein. Es werden nicht alle Regeln in Ihrer Umgebung funktionieren. In den Regelbeschreibungen erfahren Sie, welche Parameter geändert werden müssen, um eine Regel in der Umgebung erfolgreich bereitzustellen.
- **Eigene Parameter festlegen**: RSA Live-Regeln haben Parameter, die geändert werden müssen. Wenn Sie die Parameter unverändert beibehalten, funktioniert die Regel vielleicht nicht oder verbraucht zu viel Speicher.
- **Neue Regeln als Testregeln bereitstellen, damit Sie ihre Auswirkung in der Umgebung beobachten können:** Wenn Sie neue Regeln als Testregeln bereitstellen, werden sie bei einer Überschreitung des konfigurierten Schwellenwerts für den Arbeitsspeicher deaktiviert. Weitere Informationen finden Sie unter Verwenden von Testregeln.

Best Practices für die Bereitstellung von Regeln

Hierbei handelt es sich um allgemeine Richtlinien für die Bereitstellung von Regeln.

- **Neue Regeln in kleinen Batches bereitstellen, damit Sie ihre Auswirkung in der Umgebung beobachten können:** Umgebungen sind unterschiedlich. Regeln müssen daher unter Berücksichtigung der Speichernutzung, der Menge an Warnmeldungen und der effektiven Erkennung von Ereignissen optimiert werden.
- **Regeln vor dem Konfigurieren von Warnmeldungsbenachrichtigungen testen**: Erstellen Sie Warnmeldungsbenachrichtigungen erst, nachdem die Regel getestet und optimiert wurde. Auf diese Weise stellen Sie sicher, dass Sie nicht übermäßig viele Warnmeldungen erhalten, falls eine Regel sich anders als erwartet verhält.

- **Systemintegrität während des Bereitstellungsprozesses überwachen**: Überwachen Sie bei der Bereitstellung von Regeln als Teil des Prozesses die Systemintegrität. Die Gesamtspeicherauslastung für ESA können Sie auf der Registerkarte „Integrität und Zustand“ prüfen. Weitere Informationen finden Sie unter „Anzeigen von Statistiken zu Integrität und Zustand“ in Troubleshooting für ESA.

Best Practices für die Systemintegrität

Hierbei handelt es sich um allgemeine Richtlinien für die Systemintegrität.

- **Neue Regeln als Testregeln definieren**: Durch neue Regeln verursachte Speicherprobleme sind weit verbreitet. Legen Sie neue Regeln als Testregeln fest, um dieses Problem zu vermeiden. Bei einer Überschreitung des konfigurierten Schwellenwerts für den Arbeitsspeicher werden alle Testregeln deaktiviert, damit das System weiter über ausreichenden Speicher verfügt. Weitere Informationen zu Testregeln finden Sie unter Verwenden von Testregeln.
- **Schwellenwerte im Modul "Integrität und Zustand" festlegen, um eine Warnmeldung bei zu hoher Speicherauslastung zu erhalten**: Das Modul „Integrität und Zustand“ enthält Metriken zur Nachverfolgung der Speicherauslastung. Sie können für die Warnmeldungen und Benachrichtigungen festlegen, dass Sie eine E-Mail erhalten, wenn die Schwellenwerte überschritten werden. Weitere Informationen zu den anzeigbaren Speicherstatistiken finden Sie unter „Anzeigen von Statistiken zu Integrität und Zustand“ in Troubleshooting für ESA.
- **Überwachen Sie für jede Regel im Modul „Integrität und Zustand“ die Speicherkennzahlen**. Sie können für jede aktive Regel im Modul „Integrität und Zustand“ den geschätzten Speicherverbrauch anzeigen lassen. Sie können diese Informationen verwenden, um sicherzustellen, dass Regeln nicht zu viel Speicher verbrauchen. Weitere Informationen zu den anzeigbaren Speicherstatistiken erhalten Sie unter „Anzeigen von Statistiken zu Integrität und Zustand“ in Troubleshooting für ESA.

Troubleshooting für ESA

In diesem Abschnitt werden häufig vorkommende Probleme beschrieben, die bei der Verwendung von ESA auftreten können, und generelle Lösungen für diese Probleme vorgeschlagen.

Troubleshooting bei ESA-Services

Problem	Mögliche Ursachen	Lösungen
Im NetWitness Suite Dashboard ist der ESA-Service rot markiert, um darauf hinzuweisen, dass er offline ist. In der Ansicht **Konfigurieren** > **ESA-Regeln** wird die folgende Meldung angezeigt: „Der Service ist entweder offline oder nicht erreichbar.“	Verschiedene	Wenn ein ESA-Service offline ist, kann dies viele Ursachen haben. Häufig liegt es jedoch daran, dass eine von Ihnen erstellte Regel zu viel Arbeitsspeicher benötigt und der ESA-Service dadurch fehlschlägt. Informationen zur Behebung des Problems finden Sie unter Schritte zur Behebung von Speicherproblemen, wenn ein ESA-Service offline ist. Andere häufige Ursachen sind die Blockierung der Verbindung zwischen ESA und NetWitness Suite durch eine Firewall oder ein Ausfall des Computers mit dem ESA-Service.
		So starten Sie ESA-Services: Klicken Sie in **ADMIN** > **Services** auf das Aktionen-Symbol  für den ESA-Service und wählen Sie **Starten** aus. Falls der ESA-Service in einer Dauerschleife angehalten und von Neuem gestartet wird, bitten Sie den Customer Service, die Services wieder zum Starten zu bringen.

Problem	Mögliche Ursachen	Lösungen
Nach einem kürzlich erfolgten Upgrade ist der ESA-Service im NetWitness Suite Dashboard rot markiert, um darauf hinzuweisen, dass er offline ist. In der Ansicht **Konfigurieren** > **ESA-Regeln** wird die folgende Meldung angezeigt: „Der Service ist entweder offline oder nicht erreichbar.“	Konfigurationsprobleme	Falls Sie Ihr System vor Kurzem aktualisiert haben, ist Ihnen vielleicht ein Konfigurationsfehler unterlaufen. Wählen Sie unter **ADMIN** > **Services** Ihren ESA-Service aus und klicken Sie auf **Service bearbeiten**. Klicken Sie im Feld „Service bearbeiten“ auf „Verbindung testen“. Wenn keine Verbindung hergestellt werden kann, liegt wahrscheinlich ein Konfigurationsfehler vor. Versuchen Sie, den Konfigurationsfehler zu beheben, und überprüfen Sie die Verbindung erneut.
Der ESA-Service wird offenbar langsam ausgeführt.	Konfigurationsprobleme	Sie können die Performance möglicherweise steigern, indem Sie den Puffer ändern (der Standardwert ist *1048576 Byte*) oder die TCP-Einstellung auf „TCPNoDelay“ festlegen, um eine Verzögerung beim Empfang von TPC Acks (Acknowledgments) zu verhindern. Sie können diese Einstellungen (*readBufferSize* und *tcpNoDelay*) in der Exploreransicht unter *Workflow/Source/nextgenAggregation* ändern.

Troubleshooting bei RSA Live-Regeln für ESA

Problem	Mögliche Ursachen	Lösungen
Ich habe eine Gruppe von Regeln aus RSA Live importiert und nun stürzt mein ESA-Service ab. Warum?	Möglicherweise haben Sie die Parameter für die RSA Live-Regeln nicht konfiguriert, um sie auf Ihre Umgebung abzustimmen.	Zu jeder Regel in RSA Live gehört eine Beschreibung, die die zu konfigurierenden Parameter sowie die umgebungsspezifischen Voraussetzungen enthält. Überprüfen Sie in dieser Beschreibung, ob die Regel für Ihre Umgebung korrekt ist. Damit gewährleistet ist, dass sichere Regeln für Ihre Umgebung bereitgestellt werden, konfigurieren Sie neue Regeln zunächst als Testregeln, um sie in Ihrer Umgebung zu testen. Testregeln sind eine Vorsichtsmaßnahme zum Testen neuer Regeln. Einzelheiten hierzu finden Sie unter Bereitstellen von Regeln als Testregeln.

Problem	Mögliche Ursachen	Lösungen

Ich habe eine Gruppe von Regeln aus RSA Live importiert. Sie wurden zwar ohne Fehler bereitgestellt, wurden aber später deaktiviert.	Nicht alle RSA Live-Regeln passen in jede Umgebung. Möglicherweise verfügen Sie nicht über die korrekten Metadaten in Ihrer ESA, um die Regel auszuführen.	Sie können überprüfen, ob eine Regel deaktiviert wurde, indem Sie zu **Konfigurieren > ESA-Regeln > Services > Statistik für bereitgestellte Regeln** wechseln. Wenn die Regel deaktiviert ist, wird das grüne Symbol neben der Regel nicht angezeigt.
		
		Wenn eine Regel korrekt bereitgestellt, jedoch deaktiviert wurde, prüfen Sie die Protokolle auf Ausnahmen in Bezug auf die Regel. Prüfen Sie insbesondere, ob die Regeln aufgrund von fehlenden Metadaten deaktiviert wurden. Gehen Sie dazu zu **ADMIN** > **Services**, wählen Sie Ihren ESA-Service und dann > **Ansicht** > **Protokolle** aus.
		
		Suchen Sie dann nach einer Meldung ähnlich der Folgenden:
		
		`"Property named '<meta_name>' is not valid in any stream"`
		
		Es könnte z. B. Folgendes angezeigt werden:
		
		`Failed to validate filter expression '(medium=1 and streams=2 or medium=3...(238 chars)': Property named 'tcp_flags_seen' is not valid in any stream`
		
		Wenn eine ähnliche Meldung angezeigt wird, müssen Sie dem Log Decoder oder Concentrator möglicherweise einen benutzerdefinierten Metaschlüssel hinzufügen. Befolgen Sie dazu die Anweisungen unter „Erstellen benutzerdefinierter Metaschlüssel mithilfe benutzerdefinierter Feeds“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

Troubleshooting für Bereitstellungen

Problem	Mögliche Ursachen	Lösungen
Ich habe die Regel erstellt und die Syntax überprüft. Die Regel sah korrekt aus. Als ich die Regel bereitstellen wollte, trat ein Fehler auf. Warum?	Möglicherweise verfügen Sie nicht über die korrekten Metadaten zur Bereitstellung der Regel.	Überprüfen Sie die Metaschlüsselverweise. Möglicherweise verfügen Sie nicht über die korrekten Metadaten zur Bereitstellung der Regel.

Troubleshooting bei Regeln

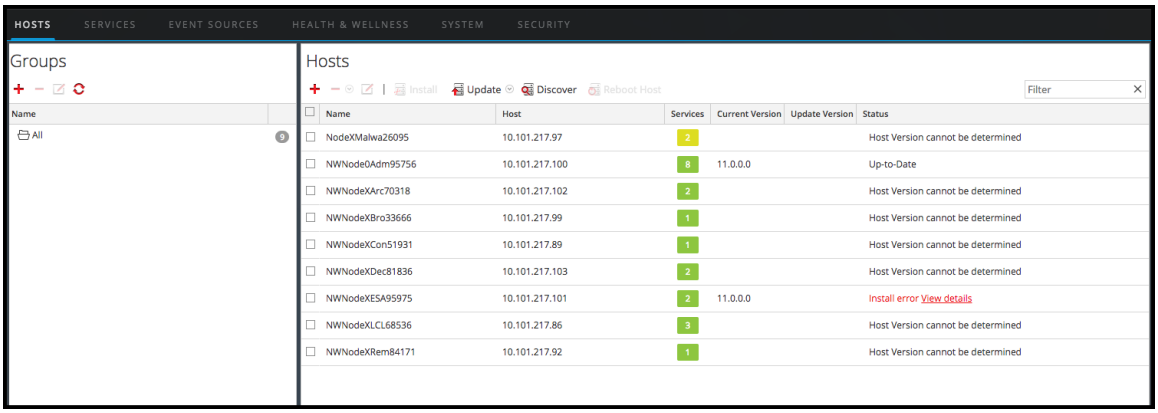
Problem	Mögliche Ursachen	Lösungen
Ich habe (über die Registerkarten Regelerstellung oder Erweiterte EPL-Regel) eine benutzerdefinierte Regel erstellt, die jedoch keine Aktion auslöst. Warum?	Möglicherweise bestehen Verbindungsprobleme.	Überprüfen Sie die Statistik „Angebotene Rate“ auf der Registerkarte **Konfigurieren** > **ESA-Regeln** > **Services**. Ist die angebotene Rate gleich null, empfängt der ESA-Service keine Daten von Concentrators. Überprüfen Sie die Verbindung des Concentrator. Gehen Sie zu **ADMIN** > **Services**, wählen Sie den ESA-Service und dann **Ansicht** > **Konfigurieren** aus. Stellen Sie sicher, dass der Concentrator aktiviert ist. Wählen Sie den Concentrator aus und klicken Sie auf **Verbindung testen**. Wenn die angebotene Rate nicht gleich null ist, stimmen wahrscheinlich der in der Regel angegebene Metaschlüsselname und -typ nicht mit dem Metaschlüssel in Ereignissen überein. Überprüfen Sie die Gültigkeit des in der Regel angegebenen Metaschlüsselnamens und -typs, indem Sie auf der Registerkarte **Konfigurieren** > **ESA-Regeln** > **Einstellungen** nach dem Namen des Metaschlüssels suchen (Metaschlüssel-Verweissuche).

Problem	Mögliche Ursachen	Lösungen
	Möglicherweise besteht ein Problem mit der Regel.	**Falls nur eine bestimmte Regel keine Aktionen auslöst**, rufen Sie **Konfigurieren** > **ESA-Regeln** > **Services** auf, um festzustellen, ob die Regel deaktiviert wurde. Bei einer deaktivierten Regel wird im Bereich **Statistik für bereitgestellte Regeln** eine durchsichtige Schaltfläche „Aktiviert“ anstelle einer grünen Schaltfläche „Aktiviert“ angezeigt. Sie können auch das Feld „Übereinstimmende Ereignisse“ überprüfen. Gehen Sie zu **Konfigurieren** > **ESA-Regeln** > **Services**. Dort wird in der Spalte **Übereinstimmende Ereignisse** die Anzahl der übereinstimmenden Ereignisse angezeigt. Wenn keine übereinstimmenden Ereignisse angezeigt werden, überprüfen Sie die Logik Ihrer Regel auf Fehler. Beispiel: Überprüfen Sie die Syntax auf Fehler bei der Groß- und Kleinschreibung und überprüfen Sie das Zeitfenster. Wenn die Regel immer noch nicht funktioniert, ziehen Sie eine Vereinfachung der Logik der Regel in Betracht, um herauszufinden ob sie in einer weniger komplexen Version funktioniert.

Schritte zur Behebung von Speicherproblemen, wenn ein ESA-Service offline ist

Schritt 1: Überprüfen, ob der Host ausgeführt wird

Vergewissern Sie sich als ersten Schritt zum Troubleshooting, dass der Host ausgeführt wird. Gehen Sie dazu zu **ADMIN**> **HOSTS**. Wenn der Host nicht verfügbar ist, werden die Systemparameter nicht angezeigt (die Aktualisierung der Hostinformationen kann jedoch manchmal etwas dauern), **Services** wird rot markiert und im Feld **Updates** wird eine Fehlermeldung angezeigt.



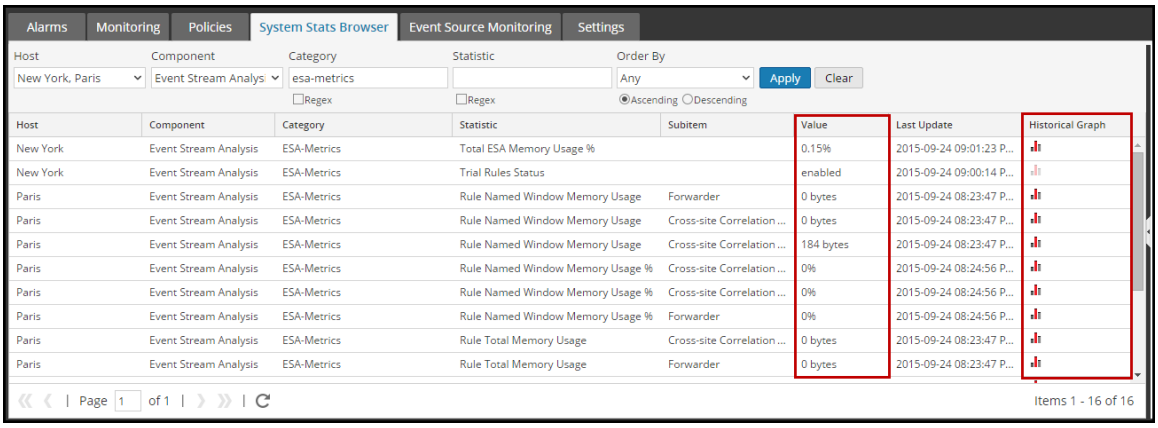
Falls der Host nicht ausgeführt wird, bitten Sie den NetWitness Suite Administrator, ihn von Neuem zu starten. Andernfalls fahren Sie mit Schritt 2 fort.

Schritt 2: Anzeigen von detaillierten Statistikdaten in „Integrität und Zustand“

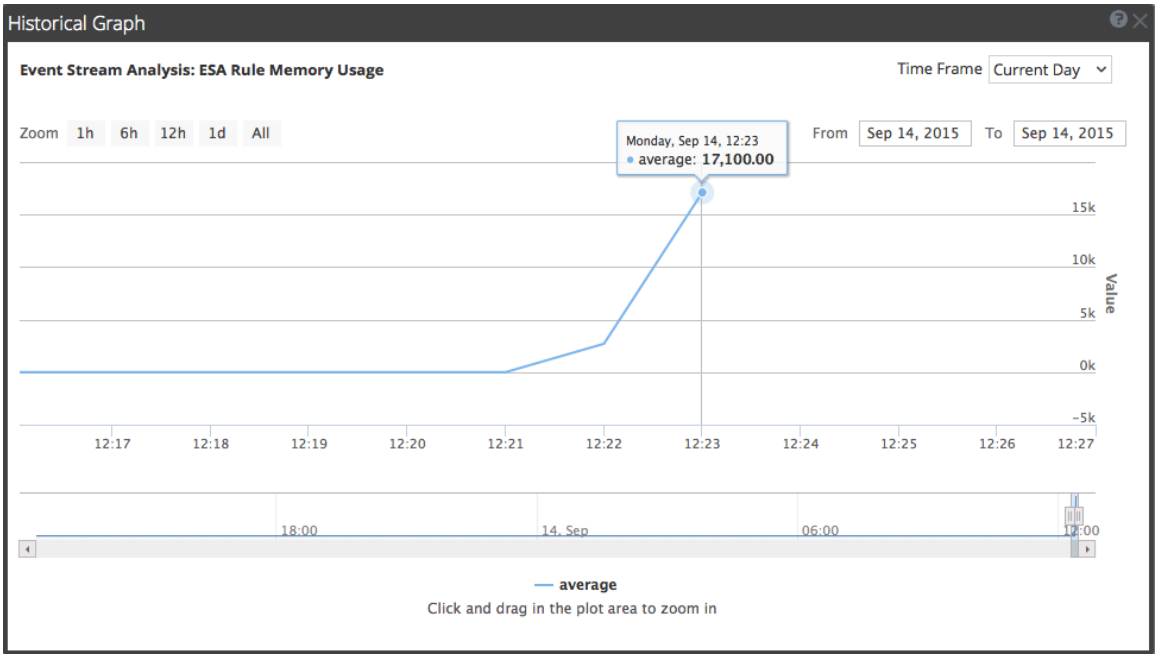
Wenn Sie sicher sind, dass der ESA-Service ausgefallen ist, können Sie „Integrität und Zustand“ aufrufen, um festzustellen, wo möglicherweise Probleme aufgetreten sind. Das häufigste Problem ist, dass der ESA-Service Arbeitsspeicher-Schwellenwerte überschreitet, was ein Stoppen oder Fehlschlagen des Services zur Folge hat.

1. Rufen Sie **ADMIN** > **Integrität und Zustand** > **Alarme** auf, um festzustellen, ob der ESA-Service Alarme ausgelöst hat. Suchen Sie nach folgenden Alarmen:
   - ESA-Gesamtspeicherauslastung > 85 %
   - ESA-Gesamtspeicherauslastung > 95 %
   - ESA-Service angehalten
2. Gehen Sie zu **ADMIN** > **Integrität und Zustand** > **Systemstatistiken Browser**, um die Speichermetriken für die Performance jeder Regel zu sehen. Um die Kennzahlen anzuzeigen, geben Sie Folgendes ein:

Host	Komponente	Kategorie
<Ihr Host>	Event Stream Analysis	ESA-Metriken



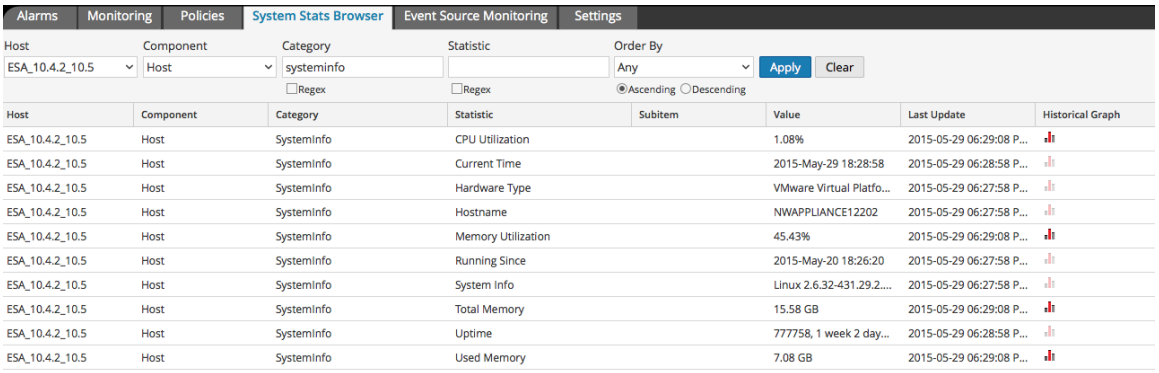
Der Arbeitsspeicher für jede Regel wird in der Spalte **Wert** angezeigt und der Wert wird in Byte angezeigt. Sie können eine Verlaufsansicht des Speicherverbrauchs in der Spalte **Verlaufsdiagramm** anzeigen.



3. Navigieren Sie zu **ADMIN** > **Integrität und Zustand** > **Systemstatistikbrowser**, um Details zur ESA-Performance anzuzeigen. Wählen Sie Ihren Host aus und verwenden Sie diese Filter zum Anzeigen der folgenden Statistikdaten:

Host	Komponente	Kategorie	Statistik	Beispiel
<Ihr Host>	Host	Systeminformationen	CPU-Auslastung	1,08 %

Host	Komponente	Kategorie	Statistik	Beispiel
<Ihr Host>	Host	Systeminformationen	Arbeitsspeicherauslastung	45,43 %
<Ihr Host>	Host	Systeminformationen	Belegter Arbeitsspeicher	7,08 GB
<Ihr Host>	Host	Systeminformationen	Gesamtspeicher	15,58 GB
<Ihr Host>	Host	Systeminformationen	Uptime	77758, 1 Woche, 2 Tage
<Ihr Host>	Event Stream Analysis	Prozessinformationen	Arbeitsspeicherauslastung	7,07 GB
<Ihr Host>	Event Stream Analysis	Prozessinformationen	CPU-Auslastung	0,2 %
<Ihr Host>	Event Stream Analysis	JVM.Memory	all	Festgelegte Heap-Arbeitsspeicherauslastung 8,0 GB
<Ihr Host>	Event Stream Analysis	ESA-Metriken	ESA-Gesamtspeichernutzung %	4,64 %



Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
ESA_10.4.2_10.5	Host	SystemInfo	CPU Utilization		1.08%	2015-05-29 06:29:08 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Current Time		2015-May-29 18:28:58	2015-05-29 06:28:58 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Hardware Type		VMware Virtual Platfo...	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Hostname		NWAPPLIANCE12202	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Memory Utilization		45.43%	2015-05-29 06:29:08 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Running Since		2015-May-20 18:26:20	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	SystemInfo	System Info		Linux 2.6.32-431.29.2....	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Total Memory		15.58 GB	2015-05-29 06:29:08 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Uptime		777758, 1 week 2 day...	2015-05-29 06:28:58 P...	
ESA_10.4.2_10.5	Host	SystemInfo	Used Memory		7.08 GB	2015-05-29 06:29:08 P...	

Falls ein Problem mit der Arbeitsspeicher- oder CPU-Auslastung besteht, fahren Sie mit Schritt 3 fort.

Schritt 3: Erneutes Starten der ESA-Services

1. Klicken Sie in **ADMIN** > **Services** auf das Aktionen-Symbol  für den ESA-Service und wählen Sie **Starten** aus.
2. Kehren Sie zum ESA-Service zurück, um festzustellen, welche Regeln Speicherprobleme verursacht haben.

Falls der ESA-Service in einer Dauerschleife angehalten und von Neuem gestartet wird, bitten Sie den Customer Service, die Services wieder zum Starten zu bringen.

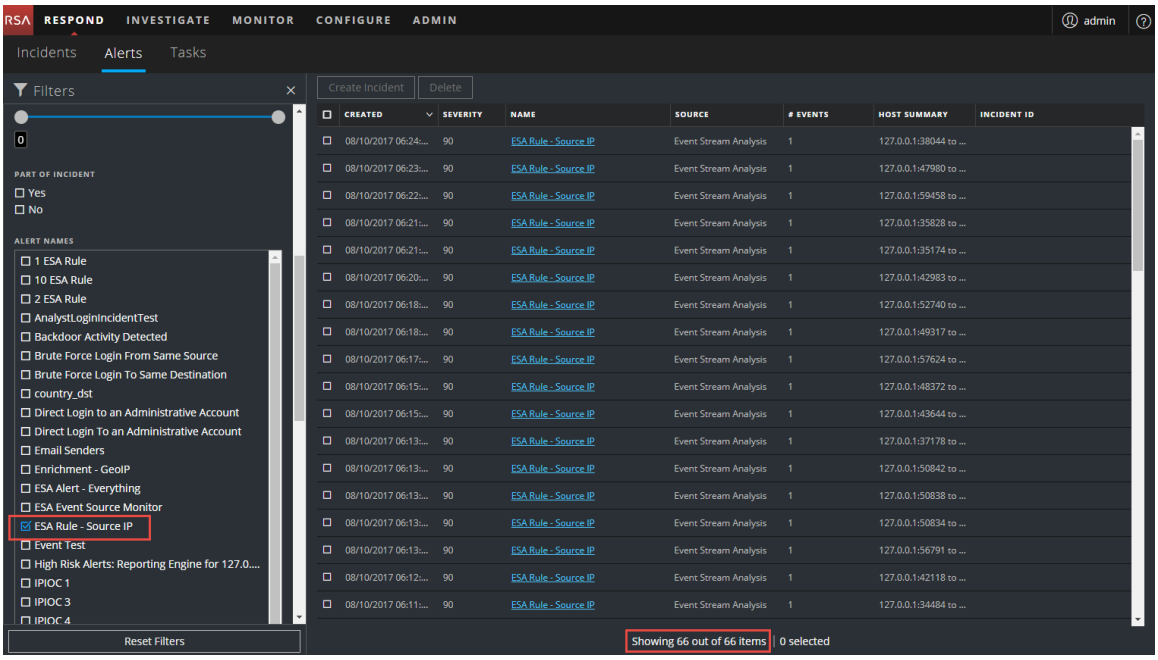
Wenn Sie den ESA-Service ohne Herunterfahren starten können, fahren Sie mit Schritt 4 fort.

Schritt 4: Überprüfen der Menge an Warnmeldungen und Ereignissen

Wenn Sie den ESA-Service erneut starten können, ohne dass er sofort wieder heruntergefahren wird, können Sie in den Regelstatistiken überprüfen, welche Regeln zu viele Ressourcen verbrauchen. Gelegentlich schlagen ESA-Services fehl, weil eine Regel zu viele Warnmeldungen erzeugt oder mit zu vielen Ereignissen übereinstimmt. Suchen Sie nach solchen Problemen, wenn Sie ermittelt haben, dass der Ausfall Ihres ESA-Services durch Speicherprobleme verursacht wird.

Anzeigen von Warnmeldungszusammenfassungen

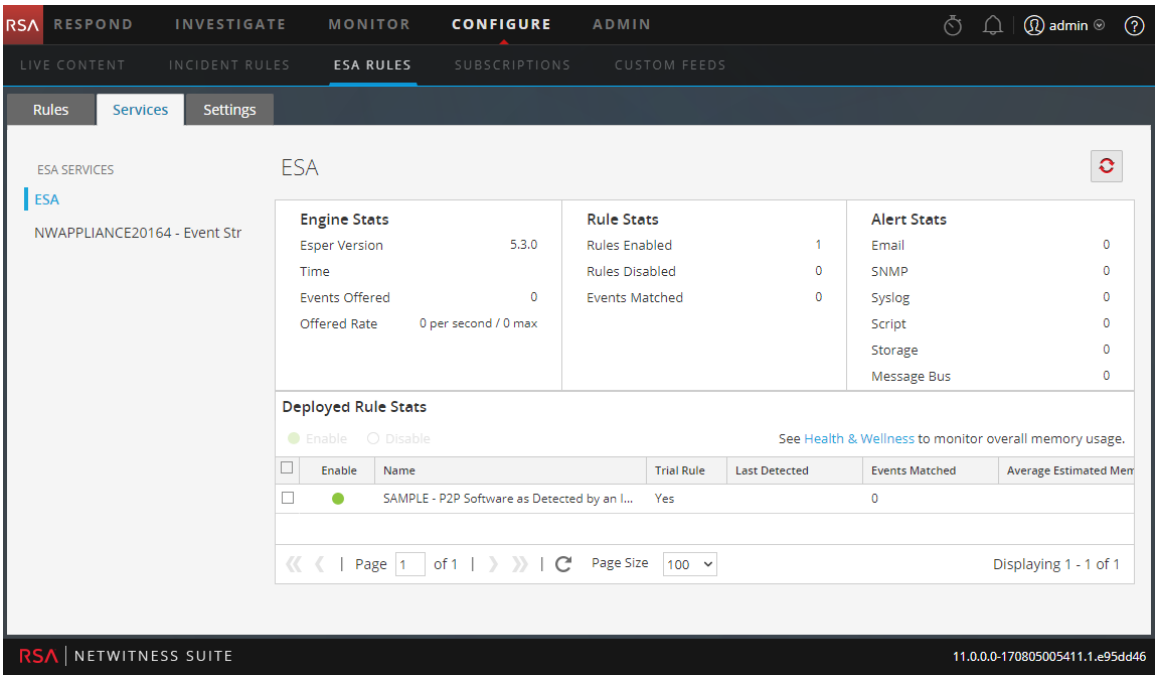
Regeln, die zu viele Warnmeldungen erzeugen, können das System überfordern und zum Ausfall oder Neustart führen. Um Zusammenfassungen von Warnmeldungen anzuzeigen, rufen Sie **Reagieren > Warnmeldungen** auf. Wählen Sie im Bereich **Filter** auf der linken Seite im Abschnitt **WARNMELDUNGSNAMEN** den Namen der Warnmeldung für die Regel aus. Die Anzahl der Warnmeldungen mit diesem Namen wird am unteren Rand der Ergebnisse der Warnmeldungsliste angezeigt. Wenn die Anzahl bei einer bestimmten Regel signifikant hoch ist, deaktivieren Sie die Regel und formulieren Sie sie so um, dass sie effizienter funktioniert.



Um den Filter zu löschen, klicken Sie auf **Filter zurücksetzen**.

Anzeigen der übereinstimmenden Ereignisse

Manchmal stimmt eine Regel mit zu vielen Ereignissen überein, wodurch übermäßig viel Speicher verbraucht wird. Dies ist typischerweise der Fall, wenn Sie ein weites Ereigniszeitfenster definieren, in dem sich eine große Anzahl von Ereignissen ansammeln kann, ohne dass eine Warnmeldung ausgelöst wird. Dies ist problematisch, da jedes Ereignis im Arbeitsspeicher gespeichert wird, während die Regel auf die Auslösung der Warnmeldung wartet. Dies können Sie unter **Konfigurieren** > **ESA-Regeln** > **Services** überprüfen. Dort wird in der Spalte **Übereinstimmende Ereignisse** die Anzahl der übereinstimmenden Ereignisse angezeigt. Wenn eine Regel eine hohe Anzahl übereinstimmender Ereignisse aufweist, sollten Sie untersuchen, ob Sie die Regel effizienter formulieren können.



Schritt 5: Deaktivieren und Reparieren der Regel, die Probleme verursacht

Nachdem Sie ermittelt haben, welche Regeln überarbeitet werden müssen, deaktivieren Sie diese undformulieren Sie sie so um, dass sie nicht mehr so viele Warnmeldungen oder Ereignisse erzeugen.Tipps zum Formulieren effizienter Regeln finden Sie unter Best Practices.

Deaktivieren von Regeln

1. Rufen Sie zum Deaktivieren von Regeln **Konfigurieren** > **ESA-Regeln** > **Services** auf und wählen Sie im Feld **Statistik für bereitgestellte Regeln** die zu deaktivierenden Regeln aus.
2. Wählen Sie **Deaktivieren** aus, um die Regeln zu deaktivieren.

Bearbeiten von Regeln

1. Wenn Sie Regeln korrigieren möchten, rufen Sie **Konfigurieren** > **ESA-Regeln** > **Regeln** > **Regelbibliothek** auf. Wählen Sie die zu bearbeitende Regel aus und klicken Sie auf das Symbol „Aktionen“  .
2. Wählen Sie **Bearbeiten** aus.
3. Formulieren Sie die Regel effizienter. Anweisungen zum Erstellen von Regeln erhalten Sie unter Hinzufügen von Regeln zur Regelbibliothek
4. Wenn Sie mit der Formulierung der Regel zufrieden sind, können Sie sie als Testregel speichern, um sicherzustellen, dass die Performance der ESA-Services nicht durch

Speicherprobleme beeinträchtigt wird. Führen Sie dazu die Schritte aus, die unter Verwenden von Testregeln aufgeführt wird.

Aktivieren von Regeln

1. Rufen Sie zum Aktivieren von Regeln Konfigurieren > **ESA-Regeln** > **Services** auf und wählen Sie im Feld **Statistik für bereitgestellte Regeln** die zu aktivierenden Regeln aus.
2. Wählen Sie **Aktivieren** aus, um die Regeln zu aktivieren.

(Optional) Überprüfen der ESA-Protokolldateien auf weitere Informationen

Wenn Sie feststellen, dass Services ausfallen, und bereits einige mögliche Ursachen für den Systemausfall untersucht haben, sollten Sie überprüfen, ob der Service in einer Dauerschleife gestoppt und von Neuem gestartet wird. Rufen Sie dazu die ESA-Protokolle auf. Wählen Sie in der Ansicht **ADMIN** > **Services** den ESA-Service und dann  > **Ansicht** > **Protokolle** aus.

Falls Sie über die NetWitness Suite-Benutzeroberfläche nicht auf die ESA-Protokolle zugreifen können, können Sie sich über SSH im System einloggen und Folgendes eingeben:`opt/rsa/esa/logs/esa.log`.

Anzeigen von Speicherkennzahlen für Regeln

In diesem Thema erfahren Autoren von ESA-Regeln, wie sie Speicherkennzahlen für Regeln anzeigen können. Sie können den geschätzten Speicherverbrauch für jede Regel, die auf einem Server ausgeführt wird, anzeigen und Sie können diese Informationen verwenden, Ihre Ihre Regelanweisungen und Bedingungen zu ändern, wenn sie zu viel Speicher verbrauchen.

Regeln können manchmal mehr Speicher verbrauchen als erwartet, wodurch Ihre ESA verlangsamt oder sogar gestoppt wird. Um annähernd zu sehen, wie viel Arbeitsspeicher eine Regel verbraucht, können Sie Speicherkennzahlen konfigurieren. Speicherkennzahlen ermöglichen es Ihnen, einen geschätzten Speicherverbrauch für jede Regel im Systemstatistikbrowser von „Integrität und Zustand“ anzuzeigen (Sie benötigen Zugriffsberechtigungen, um auf dieses Modul zuzugreifen). Sie können diese Informationen verwenden, um Ihre Regeln für mehr Effizienz zu ändern.

Allgemein müssen Sie die folgenden Schritte ausführen, um die Speicherkennzahlen für das Troubleshooting der Speichernutzung von Regeln verwenden zu können:

1. Stellen Sie sicher, dass die Funktion „Speicherkennzahlen“ aktiviert ist (über „Explorer > CEP > Kennzahlen > EnableStats“). Die Funktion „Speicherkennzahlen“ ist standardmäßig aktiviert.
2. Vergewissern Sie sich, dass Sie über die korrekten Berechtigungen zum Anzeigen des Moduls Integrität und Zustand verfügen. Informationen zu Rollen und Berechtigungen erhalten Sie unter Rollenberechtigungen.

3. Zeigen Sie die Speicherstatistik in „Integrität und Zustand“ an.
4. (Empfohlen) Konfigurieren Sie die ESA-Richtlinien für „Integrität und Zustand“ so, dass eine E-Mail gesendet wird, wenn die Speicherschwellenwerte überschritten werden. Anweisungen zum Senden von E-Mail-Benachrichtigungen erhalten Sie unter „Managen von Richtlinien“ im *Leitfaden Systemwartung*.
5. Verwenden Sie die Speicherkennzahlen, um bei Bedarf Regeln für mehr Effizienz zu ändern.

Voraussetzungen

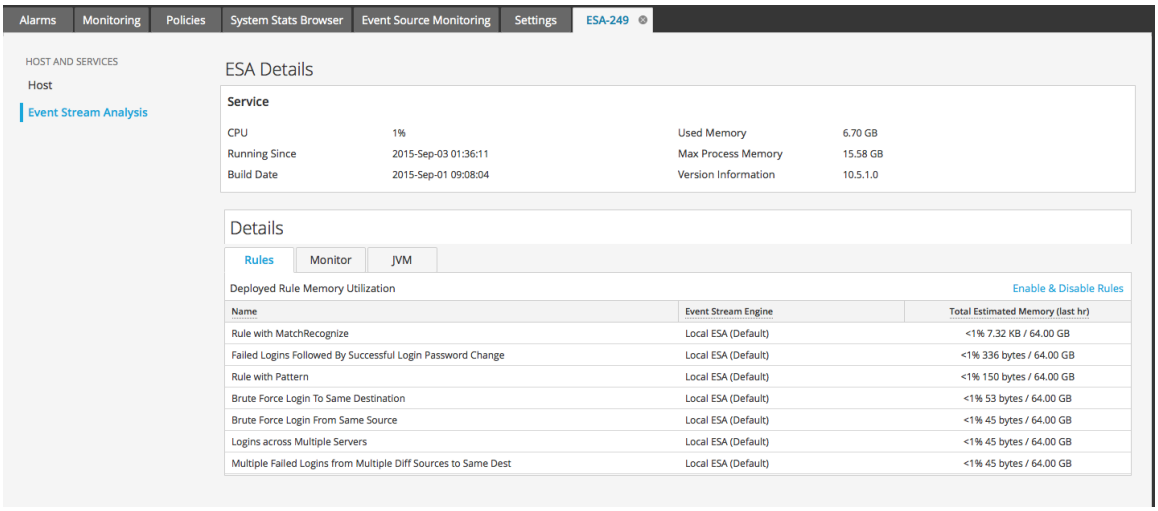
Im Folgenden sind die Anforderungen für die Verwendung von Speicherkennzahlen aufgeführt:

- Die Funktion „Speicherkennzahlen“ ist aktiviert (über **Explorer** > **CEP** > **Kennzahlen** > **EnableStats**).
- Der Benutzer muss über die entsprechenden Berechtigungen zum Anzeigen der Statistik in Integrität und Zustand verfügen.
- (Empfohlen) Konfigurieren Sie die ESA-Richtlinie für „Integrität und Zustand“ so, dass eine E-Mail gesendet wird, wenn die Speicherschwellenwerte überschritten werden.

Methoden

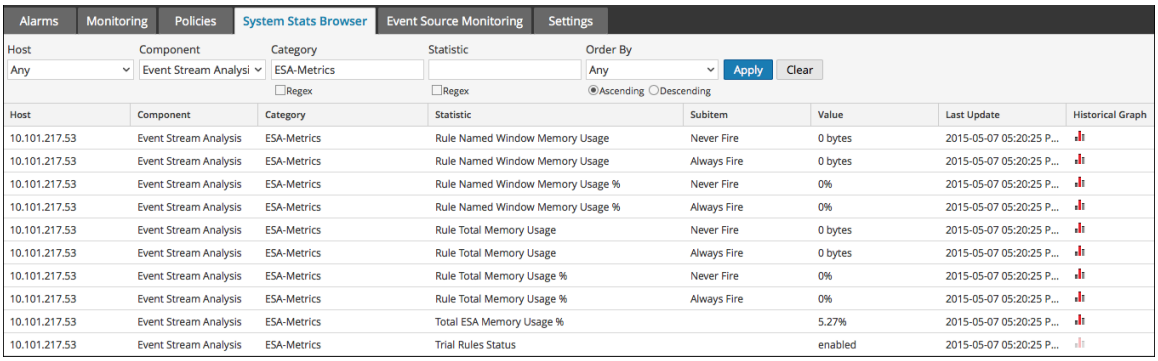
Anzeigen der Speicherkennzahlen im Systemüberwachungsmodul „Integrität und Zustand“

1. Navigieren Sie zu **ADMIN** > **Integrität und Zustand** > **Monitoring**.
2. Zeigen Sie die Details für den ESA-Service an.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Sie können die durchschnittliche Speicherauslastung für jede Regel für die vorherige Stunde anzeigen.



Anzeigen der Speicherkennzahlen im Systemstatistikbrowser „Integrität und Zustand“

1. Navigieren Sie zu **ADMIN** > **Integrität und Zustand** > **Systemstatistikbrowser**.
2. Wählen Sie als Komponente **Event Stream Analysis** aus. Geben Sie als Kategorie **ESA-Kennzahlen** ein.



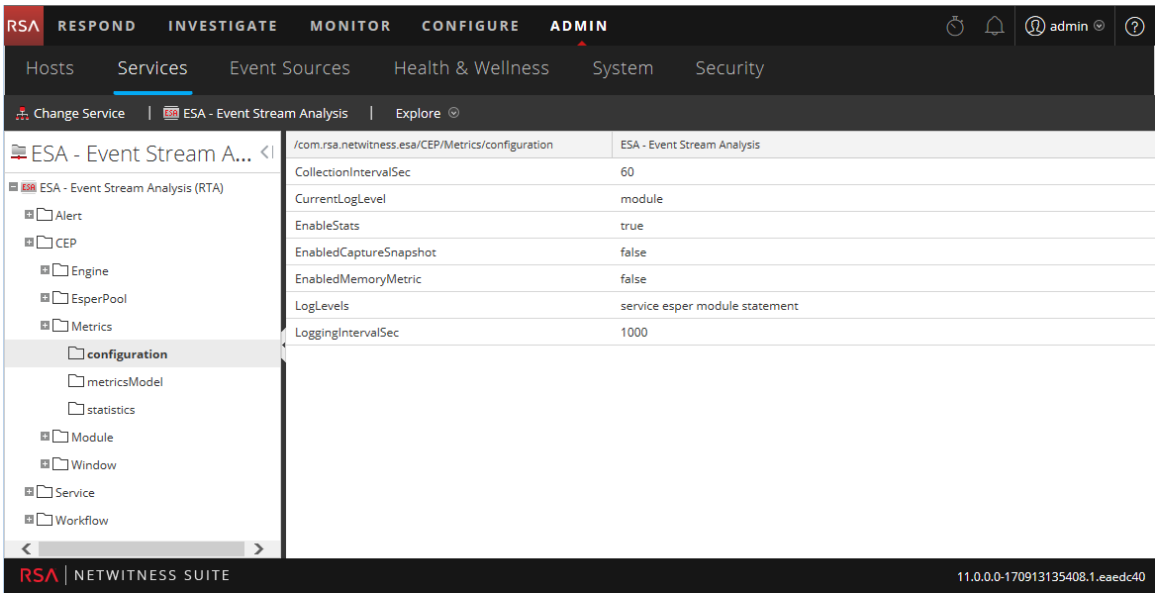
   Der Name der Regel wird im Feld **Unterelement** angezeigt, die Speichernutzung in der Spalte **Wert**.

3. Klicken Sie auf das Symbol **Verlaufsdiagramm**, um den Verlauf der Speicherauslastung für die Regel anzuzeigen.

Hinweis: Im Feld **Letzte Aktualisierung** ist angegeben, wann ESA von Integrität und Zustand abgefragt wird. Die Speicherkennzahlen werden jedoch nicht mit der Abfrage von „Integrität und Zustand“ synchronisiert. Beispiel: Wenn der Speicherschwellenwert am 10.10.15 um 12.00 Uhr überschritten wird, aber „Integrität und Zustand“ am 10.10.15 um 12:10 Uhr abfragt, zeigt das Feld **Letzte Aktualisierung** einen Zeitstempel von 10.10.15 12:10 Uhr an.

Aktivieren oder Deaktivieren der Funktion „Speicherkennzahlen“

1. Navigieren Sie zu **ADMIN** > **Services** und wählen Sie den ESA-Service aus.
2. Nachdem Sie die ESA ausgewählt haben, klicken Sie auf **Aktionen** > **Anzeigen**> **Durchsuchen** und navigieren Sie wie unten gezeigt zu **CEP > Kennzahlen** > **Konfiguration**.



3. Ändern Sie das Feld „EnabledStats“ in **wahr** oder **falsch**, je nachdem, ob Sie die Speicherkennzahlen-Funktion aktivieren oder deaktivieren möchten.

So erzeugt ESA Warnmeldungen

In diesem Thema wird kurz beschrieben, wie ein ESA (Event Stream Analysis)-Service Regeln ausführt, um Warnmeldungen zu erzeugen. Der ESA (Event Stream Analysis)-Service führt Regeln aus, die Kriterien für Problemverhalten oder bedrohliche Ereignisse in Ihrem Netzwerk bestimmen. Wenn ESA eine Bedrohung entdeckt, die Regelkriterien entspricht, wird eine Warnmeldung erzeugt.

ESA führt die folgenden Funktionen aus, um Warnmeldungen zu erzeugen:

1. Sammeln von Daten
2. Führt ESA-Regeln für die Daten aus.
3. Erfassen von Ereignissen, die die Regelkriterien erfüllen
4. Erzeugen von Warnmeldungen für diese erfassten Ereignisse

Mithilfe des Warnmeldungsmoduls können Sie Einsichten in Ihr Netzwerk gewinnen und Probleme darin erkennen.

Vertrauliche Daten

Dieses Thema erklärt, wie ESA vertrauliche Daten, wie z. B. Benutzernamen oder IP-Adressen, die von Core-Services stammen, behandelt. Die Rolle des Datenschutzbeauftragten (Data Privacy Officer, DPO) kann Metaschlüssel identifizieren, die vertrauliche Daten enthalten und verschleierte Daten anzeigen sollten. ESA zeigt vertrauliche Metadaten weder an noch speichert es sie. Folglich übergibt ESA keine vertraulichen Daten an NetWitness Respond.

Optional kann ESA eine verschleierte Version der vertraulichen Daten einem Ereignis hinzufügen. Zum Beispiel identifiziert der DPO user_dst als vertraulich. ESA kann eine verschleierte Version, wie etwa user_dst_hash, zu einem Ereignis hinzufügen. Die verschleierten Metadaten sind nicht vertraulich, sodass ESA sie auf dieselbe Weise anzeigen und speichern kann wie alle anderen nicht vertraulichen Metadaten.

Weitere Informationen über die Strategie und Vorteile der Datenverschleierung finden Sie im *Leitfaden Datenschutzmanagement*.

Dieses Thema erklärt Folgendes:

- Wie ESA sensible Daten behandelt, die von Core-Services stammen
- Wie Lecks vertraulicher Daten in einer erweiterten EPL-Regel vorzubeugen ist

Wie ESA sensible Daten behandelt, die von Core-Services stammen

Wenn ESA sensible Daten von Core-Services empfängt, gibt ESA nur die verschleierte Version der Daten weiter. ESA speichert keine vertraulichen Daten noch zeigt es sie an.

Die folgenden Funktionen sind betroffen:

- Ausgaben: ESA leitet keine vertraulichen Daten an Ausgaben weiter, dazu gehören Warnmeldungen, Benachrichtigungen und MongoDB-Speicher.
- Erweiterte EPL-Regeln: Wenn eine EPL-Aussage einen Alias für einen vertraulichen Metaschlüssel erstellt, kommt es zu einem Leck vertraulicher Daten. Dieses Thema illustriert, wie das passiert, damit Sie es verhindern können.
- Erweiterungen: Wenn ein vertraulicher Metaschlüssel in der Verknüpfungsbedingung verwendet wird, kommt es zu einem Leck vertraulicher Daten. Dieses Thema illustriert, wie das passiert, damit Sie es verhindern können.

Erweiterte EPL-Regel

Wenn eine EPL-Abfrageaussage einen vertraulichen Metaschlüssel umbenennt, sind die Daten nicht geschützt.

ESA identifiziert einen vertraulichen Metaschlüssel über den Namen:

ip_src ist der vertrauliche Metaschlüssel.
ip_src_hash ist die nicht vertrauliche, verschleierte Version.

Zur Unterstützung des Datenschutzes darf der vertrauliche Metaschlüssel in einer EPL-Abfrage nicht umbenannt werden. Wenn ein vertraulicher Metaschlüssel umbenannt wird, sind die Daten nicht mehr geschützt.

Beispiel: In einer Regel wie select ip_src as ip_alias... enthält ip_alias die vertraulichen Daten. Diese sind aber nicht geschützt, weil ESA nur ip_src kennt, nicht aber ip_alias. In diesem Fall würden die IP-Adressen nicht verschleiert. Echte Werte würden angezeigt.

Erweiterungsquelle

Wenn ein vertraulicher Metaschlüssel in einer Verknüpfungsbedingung verwendet wird, können vertrauliche Daten nicht angezeigt werden.

Die Erweiterungsdatenbank, der andere Teil der Verknüpfungsdatenbank, hat eine Spalte, die dem vertraulichen Metaschlüssel entspricht. Dieser Querverweis bezieht sich auf tatsächliche Werte, nicht verschleierte Werte. Folglich werden tatsächliche Werte angezeigt.

Im folgenden Beispiel werden beide Teile der Verknüpfungsbedingung hervorgehoben.

- ip_src enthält vertrauliche Daten.
- ipv4 wird der Warnmeldung hinzugefügt und ist als nicht vertrauliches Datenelement gefährdet

Da der ipv4-Wert derselbe ist wie der ip_src-Wert, enthält ipv4 vertrauliche Daten und zeigt sie an.

ESA-Regeltypen

In diesem Thema werden alle Typen von ESA-Regeln beschrieben, wann sie verwendet werden und über welche Berechtigungen die jeweilige Rolle verfügt. Die folgende Tabelle enthält die jeweiligen Typen und ihre Beschreibung sowie die Erläuterung, wann ein Typ verwendet wird.

Regeltyp	Beschreibung	Verwendung
Regelerstellung	Die Regelerstellung bietet eine einfache Benutzeroberfläche zum Definieren von Regelkriterien.	Verwenden Sie die Regelerstellung, um Ihre ersten Regeln zu erstellen. Sie können viele Regelbedingungen aus Listen auswählen.
Erweiterte EPL	Mit EPL (Event Processing Language) definieren Sie Regelkriterien, indem Sie eine Abfrage schreiben.	Verwenden Sie die erweiterten EPL-Regeln, um Regelkriterien in der EPL-Syntax zu definieren.
RSA Live-ESA	RSA Live bietet einen Katalog von ESA-Regeln, die Sie herunterladen und ändern können, um sie in Ihrem Netzwerk auszuführen.	Laden Sie ESA-Regeln von RSA Live herunter, um bereits erstellte Regeln zu nutzen. Ändern Sie die konfigurierbaren Parameter, um die Regeln nach Ihrem Bedarf anzupassen.

Starterpaketregeln

NetWitness Suite umfasst einige Regelerstellungsregeln, die in der Regelbibliothek angezeigt werden. Verwenden Sie die Starterpaketregeln, um sich mit der Arbeit mit Regeln vertraut zu machen, bevor Sie eigene Regeln erstellen. Sie können diese Beispielregeln sicher bearbeiten und bereitstellen.

Testregelmodus

Bei allen Typen von Regeln bietet die Auswahl der Einstellung Testregel zusätzliche Sicherheit. Testregeln werden deaktiviert, wenn sie einen vom Administrator festgelegten Schwellenwert für die Arbeitsspeicherauslastung überschreiten. Führen Sie eine Regel im Testmodus aus, um die Arbeitsspeicherauslastung zu überwachen und die Regel automatisch zu deaktivieren, wenn ihr Speicherverbrauch über dem zulässigen Schwellenwert liegt.

Rollenberechtigungen

In diesem Thema werden alle ESA-Berechtigungen aufgeführt und es wird erläutert, welche Berechtigungen den einzelnen vorkonfigurierten NetWitness Suite-Rollen zugewiesen sind. Der Benutzerzugriff wird auf der Grundlage der Rollen und der den Rollen zugewiesenen Berechtigungen eingeschränkt.

- Administratoren
- Operatoren
- Analyst
- Security Operations Center-Manager (SOC-Manager)
- Malware Analysts (MA)
- Datenschutzbeauftragter

Es gibt vier Berechtigungen für ESA:

1. Auf Alerting-Modul zugreifen: Für alle Berechtigungen erforderlich
2. Regeln anzeigen: Die Nur-Lese-Berechtigung für Regeln in der Regelbibliothek
3. Warnmeldungen anzeigen: Nur-Lese-Berechtigung für Warnmeldungen, die ESA erzeugt
4. Regeln managen: Berechtigung zum Anzeigen, Erstellen, Bearbeiten und Löschen von Regeln

In der folgenden Tabelle sind die Berechtigungen für ESA und die Rollen aufgeführt, denen sie zugewiesen sind. Anhand dieser Tabelle können Sie erkennen, wie die einzelnen Rollen mit Regeln und Warnmeldungen arbeiten können.

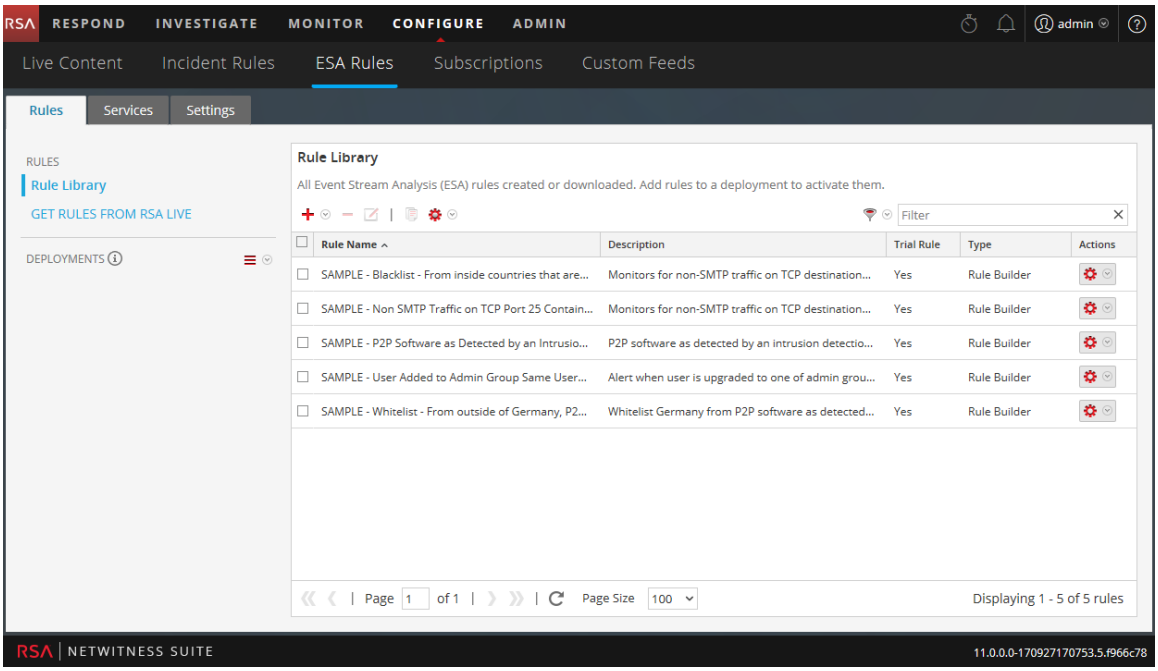
Berechtigung	Administratoren	Operatoren	Analysten	SOC-Manager	MA	DPO
Auf Alerting-Modul zugreifen	Ja	Ja	Ja	Ja		Ja
Regeln anzeigen	Ja	Ja		Ja		Ja
Warnmeldungen anzeigen	Ja		Ja	Ja		Ja
Regeln managen	Ja	Ja		Ja		Ja

Weitere Informationen über Rollen und Berechtigungen finden Sie im *Handbuch Systemsicherheit und Benutzerverwaltung*.

Üben mit Starterpaket-Regeln

NetWitness Suite enthält zwei Starterpaket-Regeln, damit Analysten sich mit dem Aussehen von Regeln vertraut machen können, bevor sie ihre eigenen Regeln erstellen. Verwenden Sie die Starterpaket-Regeln, um sich mit der Regelerstellung vertraut zu machen und das Bearbeiten und Bereitstellen von Regeln zu üben.

Die Starterpaket-Regeln sind in der Regelbibliothek installiert, die alle Regeln enthält, die Sie herunterladen oder erstellen. Die folgende Abbildung zeigt Beispielregeln in der „Regelbibliothek“.



Dies sind die verfügbaren Starterpaketregeln:

- SAMPLE: P2P Software, wie von einem Meldesystem zur Erkennung von Eindringversuchen erkannt
- SAMPLE: Nicht-SMTP-Datenverkehr auf TCP-Port 25, der eine ausführbare Datei enthält
- SAMPLE: Whitelist: von außerhalb Deutschlands, P2P-Software, wie von einem Meldesystem zur Erkennung von Eindringversuchen erkannt
- SAMPLE: Blacklist: aus Ländern außerhalb der US, Nicht-SMTP-Datenverkehr auf TCP-Port 25, der eine ausführbare Datei enthält
- SAMPLE: Benutzer derselben Administratorgruppe hinzugefügt gleicher Benutzer su Sudo

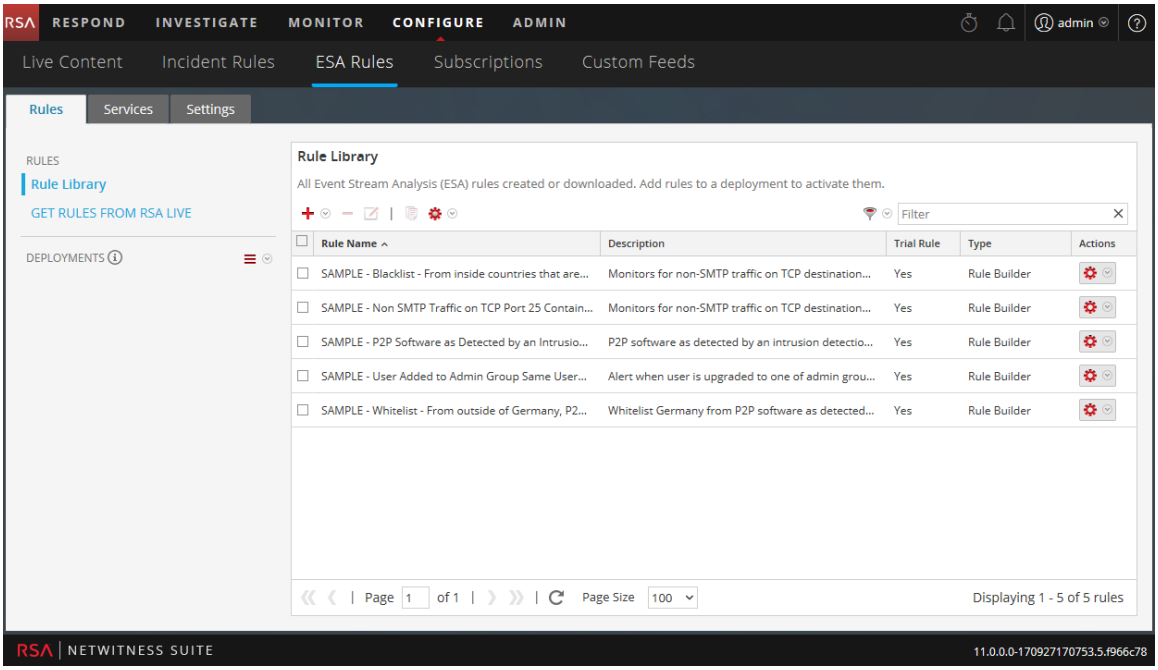
Beide Namen beginnen mit SAMPLE, um die in NetWitness Suite vorinstallierten Regeln von denen zu unterscheiden, die Sie herunterladen oder erstellen.

Regelbibliothek

Die Regelbibliothek enthält folgende Informationen zu einer Regel:

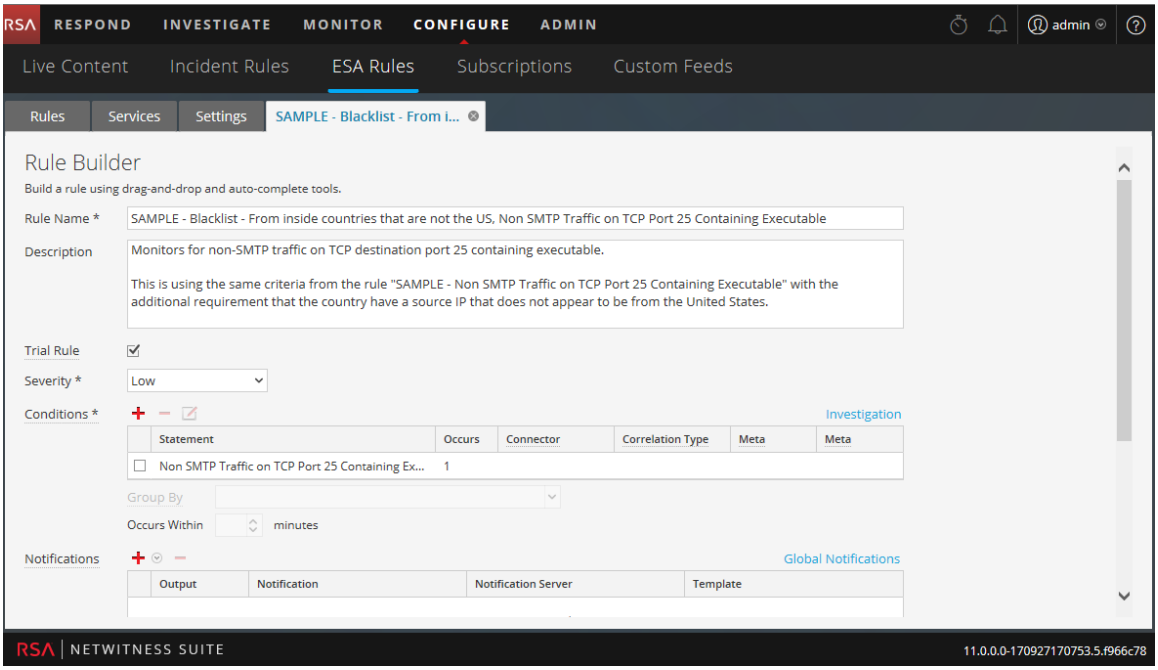
- **Name**: fasst die Daten oder Ereignisse zusammen, die die Regel sammelt.
- **Beschreibung**: erklärt die Regel detaillierter. Es wird jedoch nur der Anfang in der Regelbibliothek angezeigt.
- **Testregel**: zeigt an, ob der Testmodus für die Regel aktiviert oder deaktiviert ist.

- **Typ**: zeigt den Ursprung der Regel an (in der Regelerstellung oder erweiterten EPL erstellt oder von RSA Live heruntergeladen).



Verfahren

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Ansicht „ESA-Regeln“ wird mit geöffneter Registerkarte „Regeln“ angezeigt.
2. Wählen Sie in der **Regelbibliothek** eine Beispielregel aus und klicken Sie auf  oder doppelklicken Sie auf eine Regel.
   Die Regel wird in der Regelerstellung geöffnet.



3. Lesen Sie zum Üben mit einer Starterpaket-Regel die folgenden Themen für detaillierte Beschreibungen und Verfahren:

   - Wenn Sie sich mit der Benutzeroberfläche der Regelerstellung vertraut machen möchten, erhalten Sie auf der Registerkarte Regelerstellung eine Beschreibung aller Felder.
   - Wenn Sie lernen möchten, wie man eine Regel bearbeitet, erhalten Sie unter Hinzufügen einer Regelerstellungsregel ein schrittweises Verfahren.
   - Wenn Sie eine Starterpaket-Regel bereitstellen möchten, erhalten Sie unter Bereitstellen von Regeln für die Ausführung in ESA Anweisungen, wie die Regel einem ESA-Service zugewiesen wird.

Nachdem Sie mit den Starterpaket-Regeln geübt haben, können Sie Ihre eigenen Regeln herunterladen, erstellen und bereitstellen.

Verwenden von Testregeln

Wenn Regeln zu viel Speicher benötigen, kann Ihr ESA-Service langsam werden oder nicht mehr reagieren. Um dafür zu sorgen, dass Regeln nicht übermäßig viel Speicher benötigen, können Sie für jeden Regeltyp Testregeln aktivieren. Standardmäßig werden neue Regeln, die Sie erstellen, und RSA Live-Regeln, die Sie importieren, als Testregeln konfiguriert. RSA empfiehlt, dass Sie die Testregel-Einstellung erst nach dem Testen der neuen Regel in Ihrer Umgebung während des normalen und des höchsten Netzwerkverkehrs deaktivieren. Wenn Sie eine Testregel erstellen, stellen Sie einen globalen Schwellenwert für den Prozentsatz des Speichers ein, den Regeln verwenden können. Wenn dieser konfigurierte Speicherschwellenwert überschritten wird, werden alle Testregeln deaktiviert.

Der ESA-Service von NetWitness Suite ist in der Lage, große Mengen unterschiedlicher Ereignisdaten von Concentrators zu verarbeiten. Allerdings ist es bei der Arbeit mit Event Stream Analysis möglich, Regeln zu erstellen, die übermäßig viel Speicher verwenden. Dies kann Ihren ESA-Service verlangsamen oder sogar verursachen, dass er unerwartet herunterfährt. Um dafür zu sorgen, dass das nicht passiert, können Sie Ihre Regel als eine Testregel konfigurieren. Wenn Sie eine Testregel konfigurieren, stellen Sie auch einen globalen Schwellenwert für den Prozentsatz des Speichers ein, den Regeln verwenden können. Wenn dieser konfigurierte Speicherschwellenwert überschritten wird, werden alle Testregeln automatisch deaktiviert.

Empfehlungen zur Erstellung effizienterer Regeln finden Sie unter „Best Practices für das Schreiben von Regeln“ in Best Practices

Standardmäßig werden neue Regeln und RSA Live-Regeln als Testregeln konfiguriert. Eine Best Practice ist es, wenn Sie eine bestehende Regel bearbeiten, die Option „Testregel“ auszuwählen, die Ihnen Folgendes ermöglicht:

- Die Regel mit einer zusätzlichen Sicherung bereitzustellen
- Optional einen Snapshot der Speicherauslastung anzuzeigen, um zu erkennen, ob die Regel Speicherprobleme verursacht
- Zu wissen, ob Sie die Regelkriterien ändern müssen, um die Performance zu verbessern

Hinweis: Führen Sie eine Regel lange genug als Testregel aus, um die Performance während des normalen und des höchsten Netzwerkverkehrs zu bewerten.

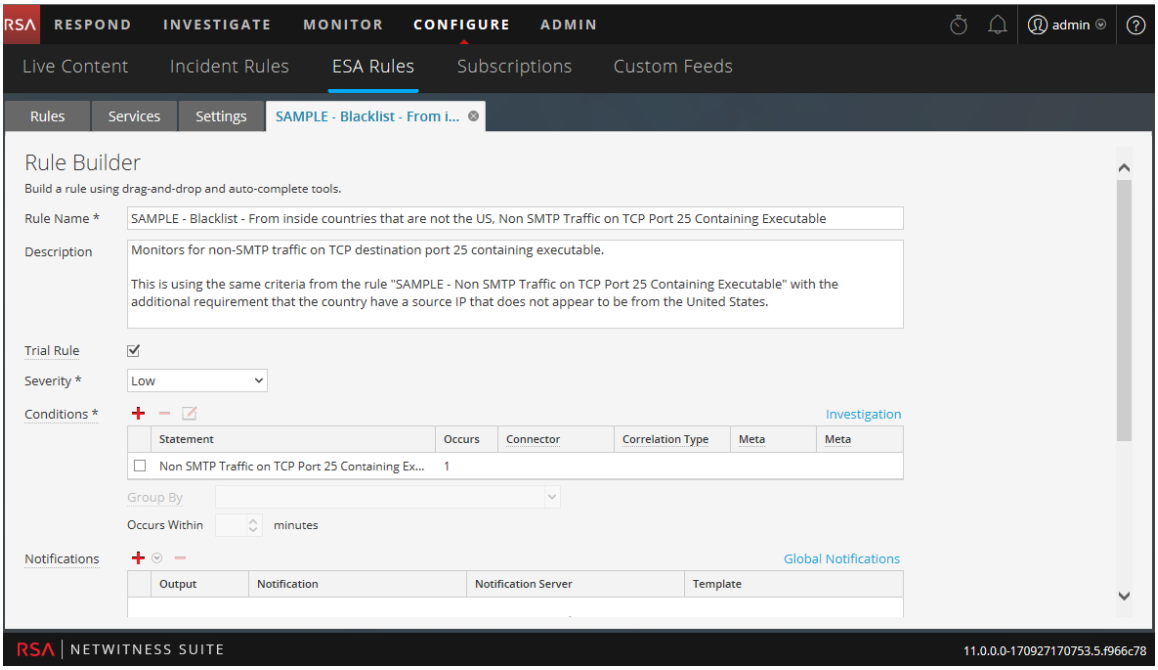
Bereitstellen von Regeln als Testregeln

In diesem Thema wird erklärt, wie Administratoren beim Erstellen neuer Regeln oder Bearbeiten von Regeln Testregeln aktivieren können. Testregeln werden automatisch deaktiviert, wenn ein festgelegter Schwellenwert für die JVM-Gesamtspeichernutzung überschritten wird.

Verfahren

So stellen Sie Regeln als Testregeln bereit:

1. Navigieren Sie zu **Konfigurieren** > **ESA-Regeln**.
   Die Ansicht „ESA-Regeln konfigurieren“ wird mit geöffneter Registerkarte „Regeln“ angezeigt.
2. Wählen Sie in der Regelbibliothek das Hinzufügen oder Bearbeiten einer Regel aus. Die Regelerstellung wird in einer neuen Registerkarte in



   angezeigt.
3. Um eine neue oder bestehende Regel zu einer Testregel zu machen, aktivieren Sie das Kontrollkästchen **Testregel**.
4. Fügen Sie bei Bedarf Regelbedingungen hinzu oder ändern Sie die Regel. Anweisungen zum Bearbeiten von Regeln erhalten Sie unter Hinzufügen von Regeln zur Regelbibliothek.
5. Klicken Sie auf **Speichern**.

6. Vergewissern Sie sich, dass die Testregeln für Ihre ESA aktiviert sind und dass die für die Testregeln konfigurierten Schwellenwerte Ihren Vorstellungen entsprechen.
   Der Speicherschwellenwert wird in der Konfigurationsdatei festgelegt. Informationen über die Konfiguration des Werts erhalten Sie unter „Ändern des Speicherschwellenwerts für Testregeln“ im *Konfigurationsleitfaden für Event Stream Analysis (ESA)*.
   Der Schwellenwert wird pro ESA konfiguriert und repräsentiert einen Prozentsatz des Java Virtual Memory.
   Der Standardwert für den Konfigurationsparameter, MemoryThresholdforTrialRules, ist 85.
7. Optional können Sie die Richtlinien in Integrität und Zustand so festlegen, dass Sie eine E-Mail-Benachrichtigung erhalten, wenn der Schwellenwert für die Gesamtnutzung des JVM-Speichers überschritten wird.

Wenn Sie die Regel das nächste Mal bereitstellen, wird Sie im Testregelmodus ausgeführt.

Hinweis: Wenn eine Testregel deaktiviert wird, müssen Sie zur Registerkarte **Konfigurieren** > **ESA-Regeln** > **Services** navigieren, um die Testregeln wieder zu aktivieren. Weitere Anweisungen zum erneuten Aktivieren von Testregeln auf einem Service finden Sie unter Anzeigen von ESA-Statistiken und -Warnmeldungen.

Anzeigen von Speicherkennzahlen für Regeln im Testmodus

In diesem Thema erfahren Autoren von ESA-Regeln, wie sie Speicherkennzahlen anzeigen können, wenn der für Testregeln konfigurierte Speicherschwellenwert überschritten wird. Wenn der Speicherschwellenwert überschritten wird, können Sie einen Snapshot der Speichernutzung von ESA-Regeln konfigurieren, der zu dem Zeitpunkt erstellt wird, wenn die Testregeln deaktiviert werden. Dies ermöglicht die Untersuchung der Speichernutzung und das Bearbeiten der Regeln für mehr Effizienz.

Wenn Sie Testregeln konfigurieren und die Funktion „Speicher-Snapshot“ aktivieren, werden bei Überschreiten des Speicherschwellenwerts alle Testregeln deaktiviert und es wird ein Snapshot der Speichernutzung für alle ESA-Regeln zum Zeitpunkt der Deaktivierung erstellt. Dies ermöglicht es Ihnen, einzusehen, wie viel Speicher verwendet wurde, damit Sie die ESA-Regeln anpassen können, um sie effizienter zu machen. Der Speicher-Snapshot kann im Systemstatistikbrowser von Integrität und Zustand angezeigt werden. Sie benötigen daher die Berechtigungen zum Zugriff auf dieses Modul. Wenn Sie die Details im Systemstatistikbrowser anzeigen, können Sie die Testregelsyntax ändern und die Testregeln wieder aktivieren.

Allgemein müssen Sie die folgenden Schritte ausführen, um den Speicher-Snapshot für das Troubleshooting der Speichernutzung von Regeln verwenden zu können:

1. Aktivieren Sie Testregeln für jede neue Regel, die Sie bereitstellen. Siehe Bereitstellen von Regeln als Testregeln.

2. Vergewissern Sie sich, dass Sie die ESA-Richtlinien in Integrität und Zustand so konfiguriert haben, dass eine E-Mail gesendet wird, wenn die Speicherschwellenwerte überschritten werden.
3. Vergewissern Sie sich, dass Sie über die korrekten Berechtigungen zum Anzeigen des Moduls Integrität und Zustand verfügen. Informationen zu Rollen und Berechtigungen erhalten Sie unter Rollenberechtigungen.
4. Vergewissern Sie sich, dass die Funktion „Speicher-Snapshot“ aktiviert ist (über den Parameter EnabledCaptureSnapshot in NetWitness Suite Explorer). Die Funktion „Speicher-Snapshot“ ist standardmäßig deaktiviert. Siehe „Aktivieren und Deaktivieren der Funktion für Speicher-Snapshots“ unten. RSA empfiehlt, die Funktion zu deaktivieren, nachdem Sie die Test neuer Regeln abgeschlossen haben.
5. Sehen Sie sich die Speicherschwellenwert-Statistiken in Integrität und Zustand an, wenn der Speicherschwellenwert für Testregeln überschritten wird.
6. Ändern Sie die Regel oder Regeln, die die Warnmeldung ausgelöst haben. Best Practices für das Erstellen von Regeln finden Sie unter Best Practices.
7. Aktivieren Sie die Testregeln wieder, die deaktiviert wurden, als der Speicherschwellenwert überschritten wurde. Anweisungen zum erneuten Aktivieren der Testregeln auf einem Service erhalten Sie unter Anzeigen von ESA-Statistiken und -Warnmeldungen.
8. Setzen Sie das Testen der Testregeln fort.

Hinweis: Wie bei jedem Debugging-Tool kann ein außergewöhnlicher Overhead mit der Verwendung der Funktion Speicher-Snapshot verbunden sein. Wenn Sie aktiv einen Snapshot erstellen, kann die Funktion Speicher-Snapshot zu Verzögerungen des ESA-Services beitragen. Der ESA-Service erzeugt keine Warnmeldungen, während ein Snapshot erstellt wird. RSA empfiehlt, die Funktion zu deaktivieren, nachdem Sie das Testen neuer Regeln abgeschlossen haben. Wenn Sie die Funktion Speicher-Snapshot deaktivieren, werden Testregeln weiterhin deaktiviert, wenn die Speichernutzung die konfigurierten Schwellenwerte überschreitet, es wird jedoch kein Speicher-Snapshot erstellt und die Statistik wird nicht im Systemstatistikbrowser von Integrität und Zustand angezeigt.

Voraussetzungen

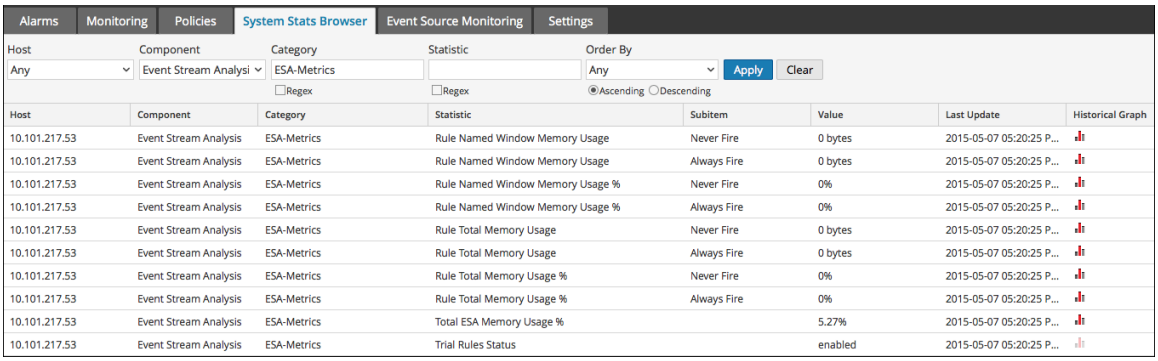
Hierbei handelt es sich um die Anforderungen für das Anzeigen von Speicherkennzahlen:

- Eine oder mehrere ESA-Regeln müssen als Testregeln konfiguriert sein.
- „Speicher-Snapshot“ muss aktiviert sein (über den Parameter EnabledCaptureSnapshot in NetWitness Suite Explorer).
- Der Benutzer muss über die entsprechenden Berechtigungen zum Anzeigen der Statistik in Integrität und Zustand verfügen.
- Der Benutzer muss die ESA-Richtlinie in Integrität und Zustand so konfiguriert haben, dass eine E-Mail gesendet wird, wenn die Speicherschwellenwerte überschritten werden.

Methoden

Anzeigen von Speicherkennzahlen

1. Navigieren Sie zu **ADMIN** > **Integrität und Zustand** > **Systemstatistikbrowser**.
2. Wählen Sie als Komponente **Event Stream Analysis** aus. Geben Sie als Kategorie **ESA-Kennzahlen** ein.

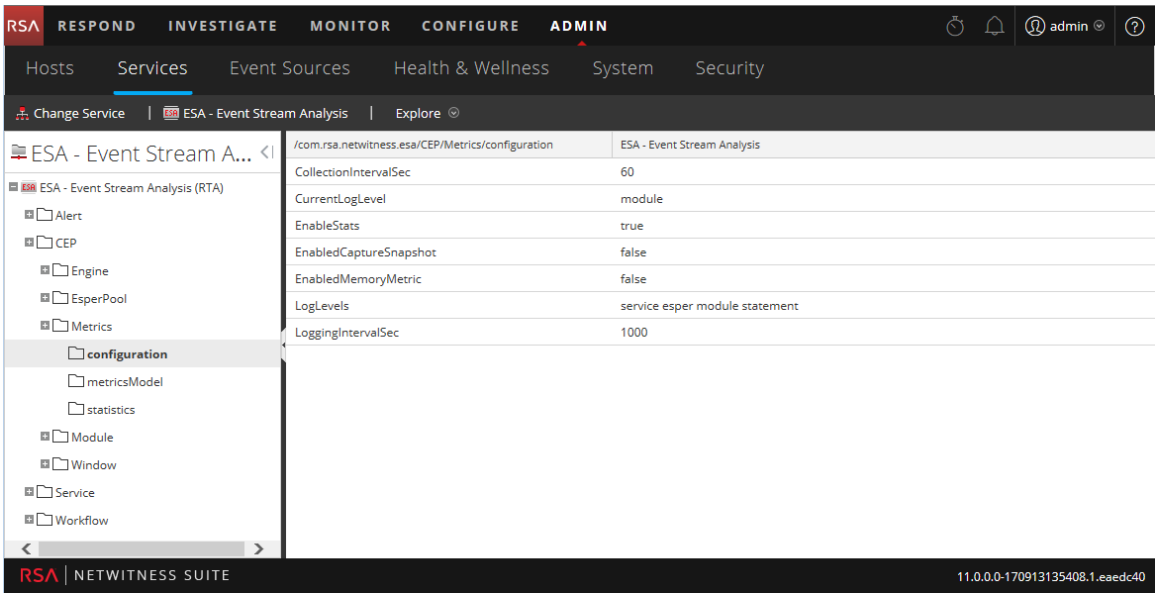


Der Name der Regel wird im Feld **Unterelement** angezeigt, die Speichernutzung in der Spalte **Wert**.

Hinweis: Im Feld **Letzte Aktualisierung** ist angegeben, wann ESA von Integrität und Zustand abgefragt wird. Der Speicher-Snapshot wird jedoch nur erstellt, wenn die Speicherschwellenwerte überschritten werden. Das Feld gibt also keine Auskunft darüber, wann der Snapshot erstellt oder aktualisiert wurde. Der Snapshot bleibt unverändert, bis der Speicherschwellenwert wieder überschritten wird. Beispiel: Wenn der Speicherschwellenwert am 10.10.15 um 12 Uhr überschritten wird, die Abfrage durch Integrität und Zustand aber am 10.10.15 um 15 Uhr erfolgt, wird im Feld **Letzte Aktualisierung** das Datum 10.10.15 15 Uhr angezeigt.

Aktivieren oder Deaktivieren der Funktion Speicher-Snapshot

1. Navigieren Sie zu **ADMIN** > **Services** und wählen Sie den ESA-Service aus.
2. Wählen Sie  > **Ansicht** > **Durchsuchen** aus und navigieren Sie zu CEP > Kennzahlen > Konfiguration, wie unten gezeigt.



3. Ändern Sie das Feld EnabledCaptureSnapshot in **wahr** oder **falsch**, je nachdem, ob Sie die Speicher-Snapshot-Funktion aktivieren oder deaktivieren möchten.

Hinzufügen von Regeln zur Regelbibliothek

In diesem Thema wird erläutert, wie der jeweilige Regeltyp zur Regelbibliothek hinzugefügt wird. Sie müssen eine Regel zur Regelbibliothek hinzufügen, um sie bereitstellen zu können. Für alle Aufgaben in diesem Abschnitt ist die Berechtigung zum Regelmanagement erforderlich. Wenn Sie Regeln hinzufügen möchten, können Sie sie von Live-ESA herunterladen, eine Regel über die Regelerstellung erstellen oder erweiterte EPL-Regeln schreiben.

Weitere Informationen über die einzelnen Verfahren finden Sie unter:

- Herunterladen von konfigurierbaren ESA-Regeln von RSA Live
- Hinzufügen einer Regelerstellungsregel
- Hinzufügen einer erweiterten EPL-Regel

Neben der Bereitstellung einer Regel können Sie sie in der Regelbibliothek auch bearbeiten, duplizieren, importieren, exportieren und entfernen. Einzelheiten zu diesen Verfahren finden Sie unter Arbeiten mit RegelnArbeiten mit Regeln

Herunterladen von konfigurierbaren ESA-Regeln von RSA Live

In diesem Thema wird erläutert, wie Sie konfigurierbare Regeln vom NetWitness Suite Live-Contentmanagementsystem herunterladen, sodass Sie sie Ihrem Bedarf anpassen können.

RSA Live enthält einen Regelkatalog. Jede Regel hat konfigurierbare Parameter, sodass Sie die Regel an Ihre Umgebung anpassen können. Wenn RSA Live eine Regel zur Erkennung von Ereignissen bietet, die Sie im Netzwerk erkennen möchten, sparen Sie Zeit, indem Sie diese Regel herunterladen. Sie können die konfigurierbaren Parameter bearbeiten und die Regel in Ihrer Regelbibliothek speichern.

Hier sehen Sie ein Beispiel dafür, wie die RSA Live-ESA-Regeln in RSA Live beschrieben werden:

Name der Regel	Beschreibung
Anmeldungen auf mehreren Servern	Erkennt Anmeldungen desselben Benutzers auf 3 oder mehr einzelnen Servern innerhalb von 5 Minuten. Das Zeitfenster und die Anzahl eindeutiger Ziele sind konfigurierbar.

Wie der Name sagt, sucht die Regel nach Anmeldungen über mehrere Server hinweg. Die Beschreibung bietet eine genauere Erklärung der Regelkriterien und gibt an, welche Parameter Sie ändern können.

Hinweis: Wenn eine Regelbeschreibung einen konfigurierbaren Parameter umfasst, wird die Standardeinstellung für diesen verwendet. In der Beispielregelbeschreibung sind 5 Minuten angegeben. Da das Zeitfenster aber konfigurierbar ist, ist 5 die Standardanzahl von Minuten.

Voraussetzungen

Dies sind die Voraussetzungen für das Herunterladen von konfigurierbaren RSA Live ESA-Regeln.

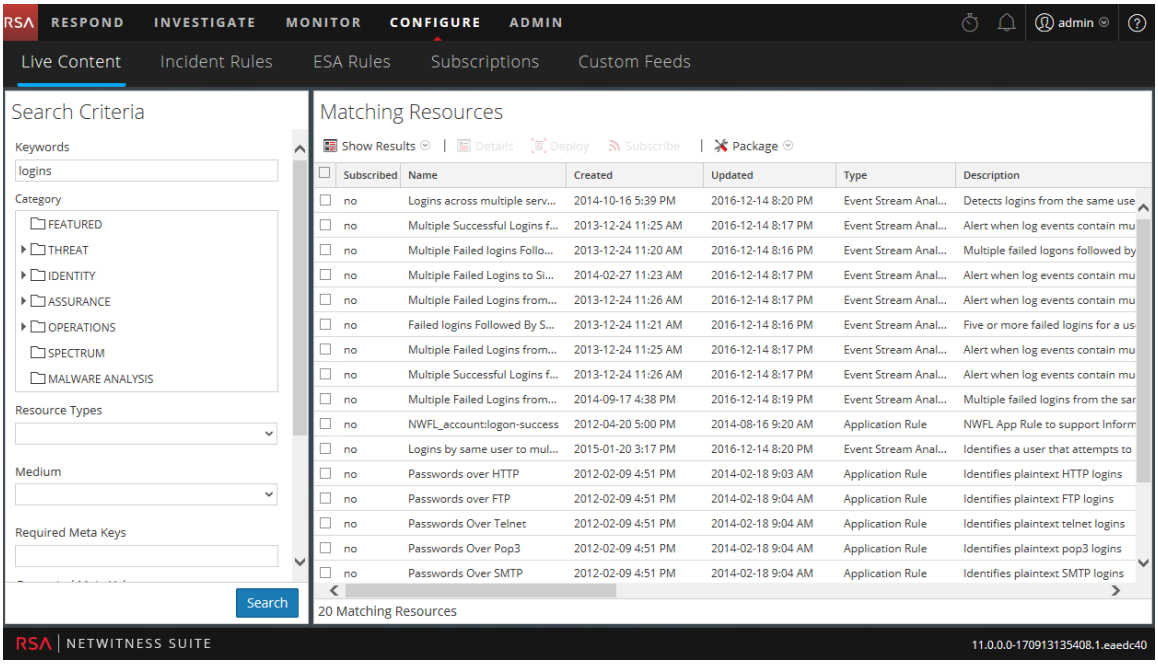
- Sie müssen zum Regelmanagement berechtigt sein.
- Erstellen eines Live-Kontos. Weitere Informationen finden Sie im *Handbuch Live-Servicemanagement*.
- Richten Sie Live auf NetWitness Suite ein. Weitere Informationen finden Sie im *Handbuch Live-Servicemanagement*.

Verfahren

So laden Sie konfigurierbare ESA-Regeln von RSA Live herunter:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte Regeln wird angezeigt.

2. Klicken Sie im Bereich „Optionen“ auf **Regeln von RSA Live abrufen**.
   Die Ansicht „Live-Inhaltssuche“ wird angezeigt.



3. Wählen Sie in den **Suchkriterien** als **Ressourcentyp** die Option **RSA Event Stream Analysis-Regel** aus.

4. Legen Sie die folgenden Kriterien nach Bedarf fest, um eine Regel zum Konfigurieren für Ihre Umgebung zu suchen.
   Genaue Beschreibungen der Suchkriterien finden Sie unter „Die Ansicht Live-Suche“ im *Handbuch Live-Servicemanagement*.

   a. Stichwörter

   b. Tags

   c. Erforderliche Metaschlüssel

   d. Erzeugte Metawerte

   e. Erstellungsdatum der Ressource

   f. Änderungsdatum der Ressource

5. Klicken Sie auf **Search**. In Übereinstimmende Ressourcen werden die Regeln angezeigt, die mit den Suchkriterien übereinstimmen.

6. Wählen Sie alle Regeln aus, die Sie herunterladen möchten, und klicken Sie auf **Bereitstellen**.
   Der Bereitstellungsassistent wird angezeigt

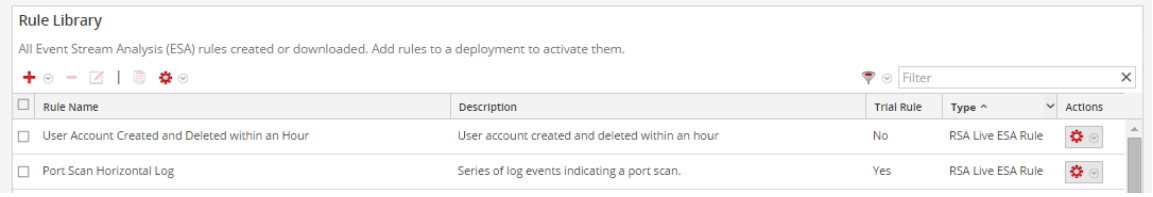
7. Befolgen Sie die Schritte im Assistenten. Wenn Sie weitere Informationen benötigen, siehe „Bereitstellen von Ressourcen in Live“ im *Handbuch Live-Servicemanagement*.

Wenn Sie die Schritte im Assistenten abgeschlossen haben, werden die ausgewählten Regeln in der Regelbibliothek angezeigt.

Anpassen von RSA Live ESA-Regeln

In diesem Thema wird erläutert, wie Parameter in einer RSA Live ESA-Regel konfiguriert werden. Wenn Sie eine RSA Live ESA-Regel konfigurieren, wird die Regel in der Regelbibliothek aufgeführt. Diese enthält folgende Spalten:

- Name
- Beschreibung
- Testregel
- Typ



Der Typ lautet „RSA Live ESA-Regel“.

Voraussetzungen

- Als Rollenberechtigungen sind erforderlich: Administrator, Operator, SOC Manager oder DPO.
- Regeln müssen in die Regelbibliothek heruntergeladen werden.

Verfahren

So passen Sie eine RSA Live ESA-Regel an:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
2. Wählen Sie in der **Regelbibliothek** eine RSA Live ESA-Regel aus und klicken Sie auf . Die Registerkarte für die RSA Live ESA-Regel wird angezeigt.
3. (Optional) Ändern Sie die folgenden Felder:
   - Name der Regel
   - Beschreibung

- Testregel (Standardmäßig aktiviert. RSA empfiehlt, eine Regel lange genug als Testregel auszuführen, um die Performance während des normalen und des höchsten Netzwerkverkehrs zu bewerten.)
- Schweregrad

4. Um die Regel für Ihre Umgebung zu konfigurieren, ersetzen Sie im Abschnitt **Parameter** den Standardwert in der Spalte **Wert**.

5. Klicken Sie auf **Speichern**.

Hinzufügen einer Regelerstellungsregel

In diesem Thema wird eine Reihe von umfassenden Verfahren zum Hinzufügen von Regeln des Typs Regelerstellung vorgestellt.

Jede ESA-Regel ist darauf ausgelegt, etwas im Netzwerk zu erkennen und eine Warnmeldung dazu zu erzeugen:

- Unerlaubte Benutzeraktivitäten, wie den Versuch, Software herunterzuladen, die nicht genehmigt wurde
- Verdächtiges Verhalten, wie Massenlöschen von Audits
- Bekannte schädliche Bedrohungen, wie Tools zur Verbreitung von Würmern oder zum von Knacken von Passwörtern

Es gibt zwei Methoden für das Entwerfen von Regeln in ESA:

- Die Regelerstellung ist eine benutzerfreundliche Oberfläche. Sie geben einen Metaschlüssel und einen Wert an und wählen dann Optionen in Listen aus, um die Kriterien zu vervollständigen.
- Erweitertes EPL ermöglicht das Schreiben von Abfragen in der Event Processing Language. Dazu müssen Sie mit der EPL-Syntax vertraut sein.

Wenn Sie mit EPL vertraut sind, können Sie beide Methoden verwenden. Wenn Sie nicht mit EPL vertraut sind, müssen Sie die Regelerstellung verwenden. Diese Themen erläutern die Regelerstellung.

Schritt 1. Benennen und Beschreiben der Rolle

Dieses Thema enthält Anweisungen zur Identifizierung einer Rolle, zur Kennzeichnung als Testregel und zum Zuweisen eines Schweregrads. Wenn Sie eine neue Regel hinzufügen, müssen Sie als erstes einen eindeutigen Namen und eine Beschreibung dessen eingeben, was die Regeln erkennt. Nach dem Speichern der Regel werden diese Informationen in der Regelbibliothek angezeigt.

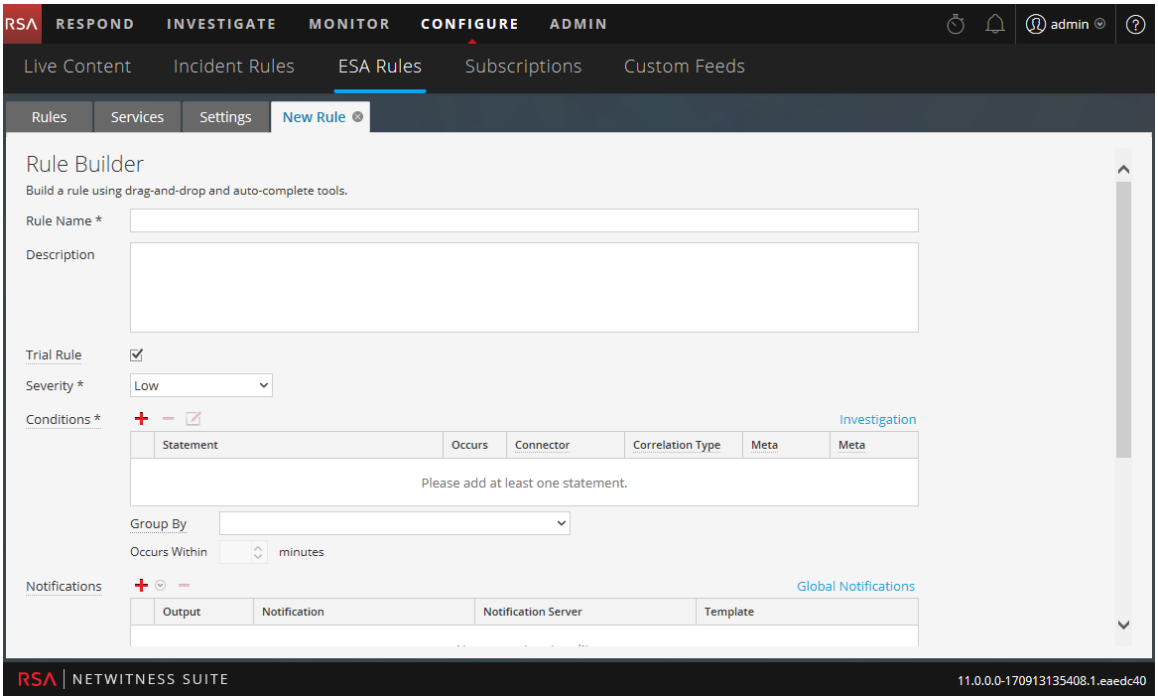
Voraussetzungen

Sie benötigen die Berechtigung zum Verwalten von Regeln. Siehe Rollenberechtigungen.

Verfahren

So benennen und beschreiben Sie eine Regel:

1. Navigieren Sie zur Registerkarte **Konfigurieren > ESA-Regeln > Regeln**.
2. Wählen Sie in der **Regelbibliothek**  **> Regelerstellung**.
   Die Registerkarte „Neue Regel“ wird angezeigt.



3. Geben Sie im Feld **Namen der Regel** einen eindeutigen, deskriptiven Namen ein.
   Dieser Name wird in der Regelbibliothek angezeigt. Wählen Sie ihn spezifisch genug, um die Regel von anderen abzugrenzen.

4. Erläutern Sie im Feld **Beschreibung**
   , welche Ereignisse von der Regel erkannt werden.Der Anfang der Beschreibung wird in der Regelbibliothek angezeigt.
5. Standardmäßig werden neue Regeln als Testregel konfiguriert. Eine Testregel deaktiviert die Regel automatisch, wenn die Summe aller Testregeln den Speicherschwellenwert überschreitet. Wenn Sie eine bestehende Regel bearbeiten, können Sie **Testregel** auswählen, um die Regeländerungen sicher zu testen.
   Verwenden Sie den Testregelmodus als Sicherheitsvorkehrung, um zu erkennen, ob eine Regel effizient ausgeführt wird,und um Ausfallzeiten aufgrund von mangelndem Speicherplatz zu vermeiden. Weitere Informationen erhalten Sie unter Verwenden von Testregeln.
6. Klassifizieren Sie den **Schweregrad** für die Regel als Niedrig, Mittel, Hoch oder Kritisch.

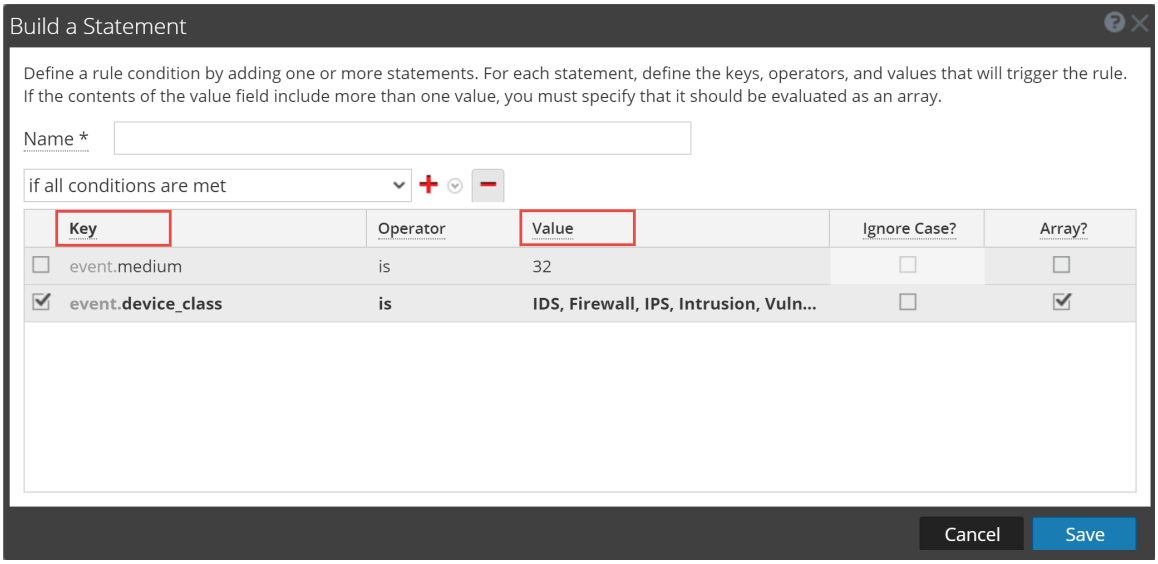
Schritt 2. Erstellen einer Regelanweisung

In diesem Thema wird erläutert, wie Sie in der Regelerstellung durch Hinzufügen von Anweisungen Regelkriterien definieren. Eine Anweisung ist eine logische Gruppierung von Regelkriterien in der Regelerstellung. Sie fügen Anweisungen hinzu, um zu definieren, was eine Regel erkennen soll.

Beispiel

Die folgende Grafik zeigt ein Beispiel für eine Anweisung in der Regelerstellung.

Jede Anweisung enthält einen Schlüssel und einen Wert. Dann erstellen Sie eine Logik um dieses Paar. Dazu wählen Sie eine Option in den anderen Feldern aus.



Voraussetzungen

Zum Erstellen einer Regelanweisung müssen Sie den Metaschlüssel und den Metawert kennen. Eine vollständige Liste der Metaschlüssel finden Sie unter **Konfigurieren > ESA-Regeln > Einstellungen > Metaschlüsselverweise**.

Verfahren

So erstellen Sie eine Regelanweisung:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.

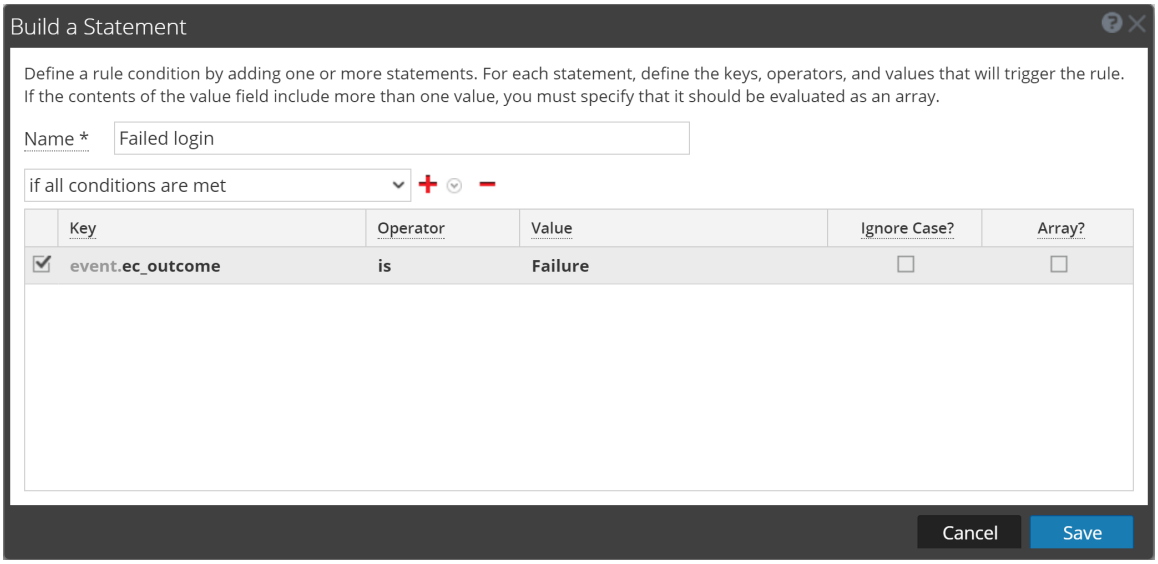
   Die Registerkarte „Regeln“ wird standardmäßig angezeigt.

2. Klicken Sie in der **Regelbibliothek** auf + **> Regelerstellung** oder bearbeiten Sie eine vorhandene Regelerstellungsregel.

   Die Ansicht „Regelerstellung“ wird angezeigt.

3. Klicken Sie im Abschnitt **Bedingungen** auf +.

   Die Ansicht „Anweisung erstellen“ wird angezeigt.



4. Geben Sie einen eindeutigen und genauen **Namen** für die Anweisung ein. Der Anweisungsname wird in der Regelerstellung angezeigt.
5. Wählen Sie in der Drop-down-Liste die Bedingungen aus, die für die Regel erforderlich sind:
   - wenn **alle Bedingungen** erfüllt sind
   - wenn **eine dieser Bedingungen** erfüllt ist
6. Geben Sie die Kriterien für die Anweisung an:

a. Geben Sie für **Schlüssel** den Namen des **Metaschlüssels** ein.

b. Geben Sie als **Operator** die Beziehung zwischen dem Metaschlüssel und dem Wert ein, den Sie für den Schlüssel angeben.
Die Optionen sind: ist, ist nicht, ist nicht null, ist größer als (>), ist größer oder gleich (>=), ist kleiner als (<), ist kleiner oder gleich (<=), enthält ,enthält nicht, beginnt mit, endet mit

c. Geben Sie den **Wert** für den Metaschlüssel ein.
Der Wert darf nicht in Anführungszeichen eingeschlossen sein. Trennen Sie mehrere Werte durch Kommata.

d. Das Kontrollkästchen **Groß-/Kleinschreibung ignorieren?** ist für die Verwendung mit Zeichenfolgewerten und Zeichenfolgearray-Werten vorgesehen. Wenn Sie das Kontrollkästchen **Groß-/Kleinschreibung ignorieren** aktivieren, behandelt die Abfrage den gesamten Zeichenfolgetext als Wert in Kleinbuchstaben. Dadurch wird sichergestellt, dass eine Regel, die nach einem Benutzer namens „Johnson“ sucht, Ereignisse auch dann findet,wenn sie „johnson“, „JOHNSON“ oder „JoHnSoN“ enthalten.

e. Das Kontrollkästchen **Array?** gibt an, ob der Inhalt des Felds „Wert“ einen oder mehrere Werte darstellt.

Aktivieren Sie das Kontrollkästchen „Array“, wenn Sie mehrere durch Komma getrennte Werte im Feld **Wert** eingegeben haben. Zum Beispiel erfordert „ec_activity is Logon, Logoff“, dass Sie das Kontrollkästchen „Array“ aktivieren.

7. Wenn Sie andere Metaschlüssel in der Anweisung verwenden möchten, klicken Sie auf +, wählen Sie **Metabedingung hinzufügen** aus und wiederholen Sie Schritt 6.

8. Klicken Sie zum Hinzufügen einer Whitelist auf + und wählen Sie **Whitelist-Bedingung hinzufügen** aus.

9. Klicken Sie auf + und wählen Sie **Blacklist-Bedingung hinzufügen** aus, um eine Blacklist hinzuzufügen.

10. Klicken Sie zum Speichern der Anweisung auf **Speichern**.

So fügen Sie eine Whitelist hinzu

Verwenden Sie eine Whitelist, um sicherzustellen, dass angegebene Ereignisse vom Auslösen der Regel ausgeschlossen sind. Whitelists können entweder auf dem geografischen Standort oder auf vom Kunden definierten CSV-Erweiterungsquellen basieren. Beispiel: Wenn Sie eine Regel erstellen möchten, die nur von IP-Adressen außerhalb der USA ausgelöst wird, können Sie eine Whitelist mit US-IP-Adressen erstellen.

1. Nachdem Sie eine Metabedingung hinzugefügt haben, klicken Sie auf + und wählen Sie **Whitelist-Bedingung hinzufügen** aus.
2. Wählen Sie im Feld **Namen für Whitelist eingeben** eine Erweiterungsquelle aus. Jede Erweiterungsquelle, die aus einer CSV-Datei oder einem benannten Fenster in Esper geladen wurde, kann als Quelle für eine Whitelist verwendet werden.
3. Wenn Sie eine GeoIP-Quelle für die Whitelist verwendet haben, wird ipv4 automatisch für die Teilbedingung eingegeben. Geben Sie den Metawert für das entsprechende Wertefeld ein. Geben Sie zum Beispiel *ipv4 is ip_src* ein, um dafür zu sorgen, dass die GeoIP-Datensätze basierend auf der ip_src ausgewählt werden, die in der GeoIP-Abfragedatenbank gefunden werden. Wenn Sie eine GeoIP-Quelle für die Whitelist verwendet haben, sollten Sie gegebenenfalls auch eine Teilbedingung hinzufügen, um die geografische Region anzugeben, die aus den Regelergebnissen ausgeschlossen werden soll. Wenn Sie beispielsweise angeben möchten, dass der Ländercode „USA“ sein muss, geben Sie *CountryCode is US* ein.

So fügen Sie eine Blacklist hinzu

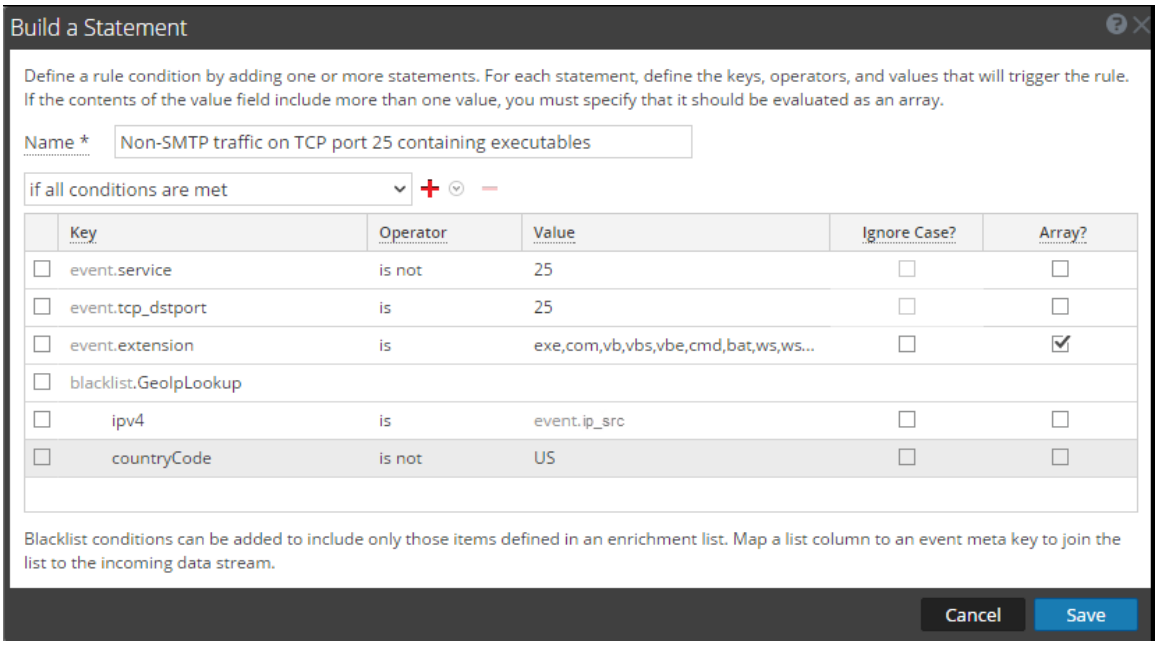
Eine Blacklist wird verwendet, um sicherzustellen, dass angegebene Ereignisse die Regel auslösen. Blacklists können entweder auf dem geografischen Standort oder auf vom Kunden definierten CSV-Erweiterungsquellen basieren. Zum Beispiel können Sie angeben, dass die Regel nur Ergebnisse aus Deutschland beinhaltet.

1. Nachdem Sie eine Metabedingung hinzugefügt haben, klicken Sie auf + und wählen Sie **Blacklist-Bedingung hinzufügen** aus.
2. Wählen Sie im Feld **Namen für Blacklist eingeben** eine Erweiterungsquelle aus. Jede Erweiterungsquelle, die aus einer CSV- oder einem benannten Fenster in Esper geladen wurde, kann als Quelle für eine Blacklist verwendet werden.
3. Wenn Sie eine GeoIP-Quelle für die Blacklist verwendet haben, wird ipv4 automatisch für die Teilbedingung eingegeben. Geben Sie den Metawert für das entsprechende Wertefeld ein. Geben Sie zum Beispiel „ipv4 is ip_src“ ein, um dafür zu sorgen, dass die GeoIP-Datensätze basierend auf der ip_src ausgewählt werden, die in der GeoIP-Abfragedatenbank

gefunden wird. Wenn Sie eine GeoIP-Quelle für die Blacklist verwendet haben, möchten Sie möglicherweise eine Teilbedingung hinzufügen, um die geografische Region anzugeben, die in die Regelergebnisse eingeschlossen werden soll. Um anzugeben, dass die Regel nur Ergebnisse für Deutschland enthält, geben Sie beispielsweise „*CountryCode is DE*“ ein.

Beispiel: Blacklist

Die folgende Anweisung zeigt eine Blacklist-Anweisung für eine Regel, die Nicht-SMTP-Datenverkehr auf TCP-Zielport 25 daraufhin überwacht, ob er ausführbare Dateien aus Ländern außerhalb der USA enthält.

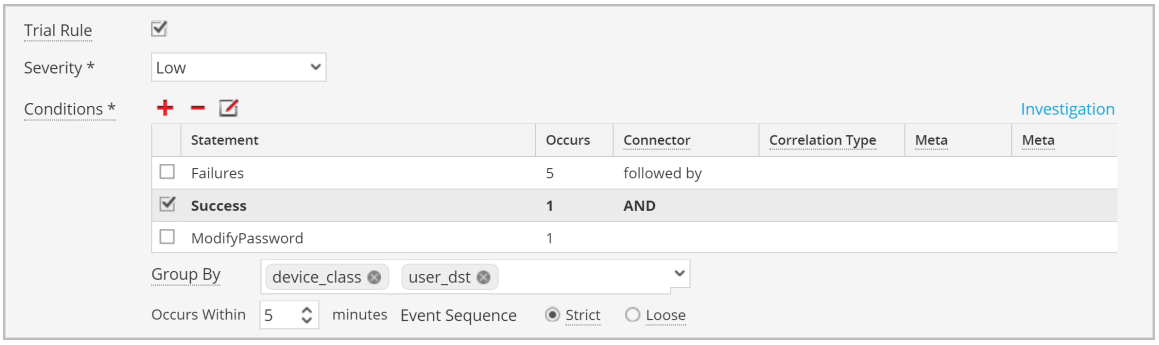


Anweisung	Beschreibung
service is not 25	Der Datenverkehr ist nicht SMTP-Datenverkehr.
tcp_dstport is 25	Der Datenverkehr wird auf TCP-Port 25 ausgeführt.
extension is exe, com,vb,vbs,vbe,cmd,bat,ws,wsf,src,sh	Die Dateierweiterung weist auf eine ausführbare Datei hin.
GeoIpLookup	Die Blacklist basiert auf einer GeoIPLookup-Quelle.
ipv4 is ip_src	Die GeoIP-Datensätze werden basierend auf der ip_src ausgewählt, die in der GeoIP-Abfragedatenbank gefunden wird.

Anweisung	Beschreibung
countryCode is not US	Bei der Abfrage der IP-Adresse „Event.ip_src“ in der GeoIP-Datenbank enthält der zurückgegebene Datensatz nicht „US“ im Feld „countryCode“.

Beispiel: Groß-/Kleinschreibung ignorieren, strenge Musterübereinstimmung und Operator *Is Not Null*

Im folgenden Beispiel wird die Groß-/Kleinschreibung ignoriert, NULL-Werte werden ausgeschlossen und es gilt eine strenge Musterübereinstimmung, um sicherzustellen, dass die erwarteten Regelergebnisse zurückgegeben werden. Die Regel besteht aus den folgenden Bedingungen:

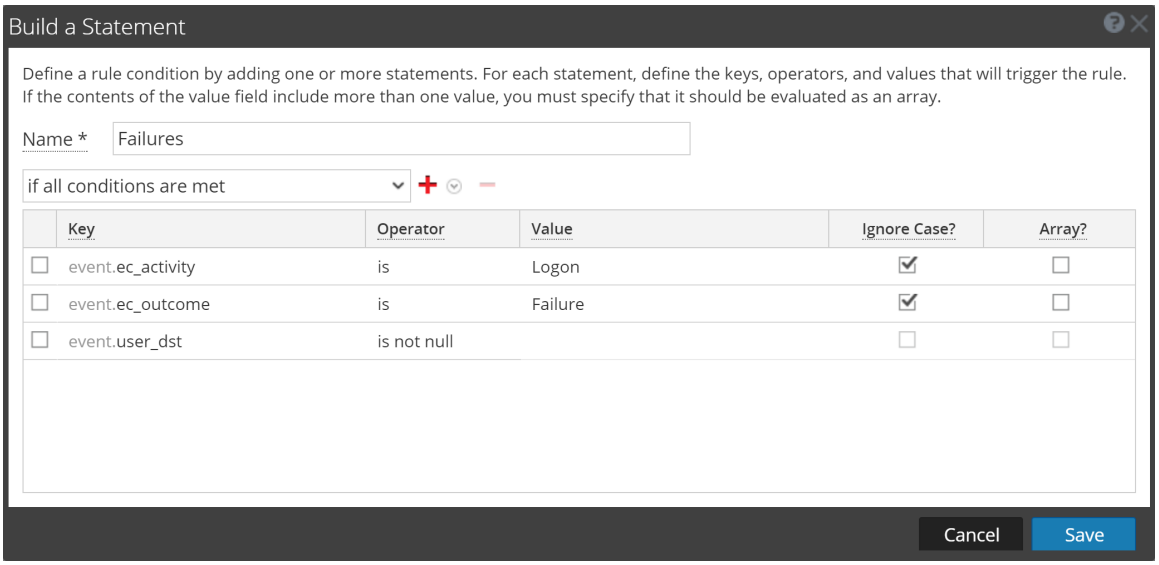


Regelbedingung	Beschreibung
Failures	Diese Bedingung sucht nach 5 fehlgeschlagenen Anmeldungen mit einem „followed by“-Connector. Das bedeutet, dass der Bedingung (Fehler) die nächste Bedingung (Erfolg) folgen muss.
Success	Diese Bedingung sucht nach einer erfolgreichen Anmeldung.
ModifyPassword	Diese Bedingung sucht nach einer Instanz, in der das Passwort geändert wird.

Regelbedingung	Beschreibung
Gruppieren nach: user_dst, Geräteklasse	Das Feld „Gruppieren nach“ sorgt dafür, dass alle vorherigen Bedingungen nach dem Metawert „user_dst“ (dem Benutzerzielkonto) und der Geräteklasse gruppiert werden. Dies ist wichtig für die Erstellung der Regel, da die Regel versucht, einen Fall zu finden, in dem ein Benutzer mehrere Male versucht hat, sich bei dem gleichen Zielkonto anzumelden, sich dann schließlich erfolgreich angemeldet und dann das Kennwort geändert hat. Durch das Gruppieren nach Geräteklasse wird sichergestellt, dass der Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht hat, sich an einem Konto anzumelden. Die Regel gibt möglicherweise unerwartete Ergebnisse zurück, wenn Sie die Ergebnisse nicht gruppieren.
Auftreten innerhalb 5 Minuten	Das Zeitfenster für das Eintreten des Ereignisses beträgt 5 Minuten. Wenn die Ereignisse außerhalb dieses Zeitfensters auftreten, wird die Regel nicht ausgelöst.
Ereignissequenz: Strikt	Die Ereignissequenz wird für eine strenge Musterübereinstimmung konfiguriert. Das bedeutet, dass das Muster genau wie angegeben übereinstimmen muss, ohne dazwischen vorkommende Ereignisse. Strenge Musterübereinstimmung erlaubt Ihnen sicherzustellen, dass die Esper-Engine nur Warnmeldungen für Regeln erzeugt, die genau dem Muster entsprechen, das Sie suchen. Beispielsweise könnte es eine allgemeine Regel sein, nach 5 fehlgeschlagenen Anmeldungen gefolgt von einer erfolgreichen Anmeldung zu suchen. Wenn Sie eine variable Musterübereinstimmung auswählen, wird diese Regel ausgelöst, wenn es eine beliebige Anzahl erfolgreicher Anmeldungen zwischen den fehlgeschlagenen Anmeldungen gibt. Da es bei der Regel darum geht, häufige *und* aufeinanderfolgende Anmeldeversuche zu finden, ist eine strenge Übereinstimmung erforderlich, um sicherzustellen, dass Sie die Ergebnisse erhalten, die Sie erwarten.

Hinweis: Jede dieser Bedingungen wird in den folgenden Abschnitten ausführlich beschrieben.

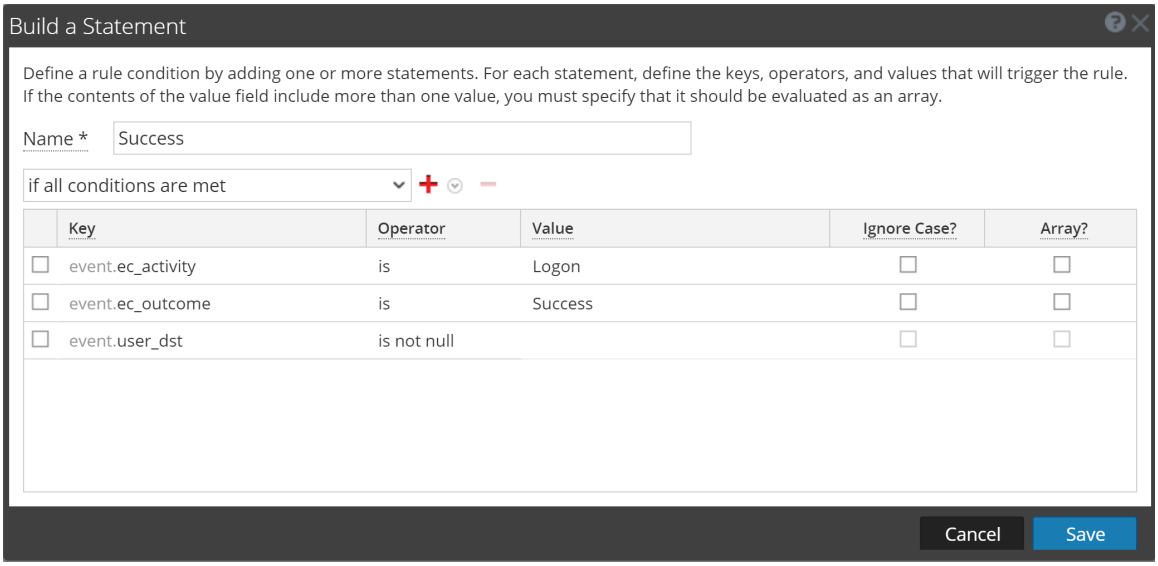
Für jede einzelne Bedingung wird eine Anweisung in der Regelerstellung erstellt. Die folgende Anweisung ergibt die Bedingung „Failures“:



Regelanweisung	Beschreibung
ec-activity is Logon (Groß-/Kleinschreibung ignorieren)	Identifiziert die Aktivität des Versuchs, sich bei einem System anzumelden Das Kontrollkästchen **Groß-/Kleinschreibung ignorieren?** ist für die Verwendung mit Zeichenfolgewerten und Zeichenfolgearray-Werten vorgesehen. Wenn Sie das Kontrollkästchen **Groß-/Kleinschreibung ignorieren** aktivieren, behandelt die Abfrage den gesamten Zeichenfolgetext als Wert in Kleinbuchstaben. Sie können dieses Kontrollkästchen verwenden, wenn Sie unsicher sind, ob ein bestimmtes Ereignis mit Groß- oder Kleinschreibung protokolliert wird. Da die Groß-/Kleinschreibung ignoriert wird, wird die Regel ausgelöst, wenn die Aktivität als „Logon“, „logon“ oder „LoGoN“ protokolliert wird.
ec_outcome is Failure (Groß-/Kleinschreibung ignorieren)	Identifiziert, dass das Ergebnis der Aktivität als „failure“ protokolliert wird. Da die Groß-/Kleinschreibung ignoriert wird, wird die Regel ausgelöst, wenn die Aktivität als „Failure“, „failure“ oder „FaiLuRe“ protokolliert wird.

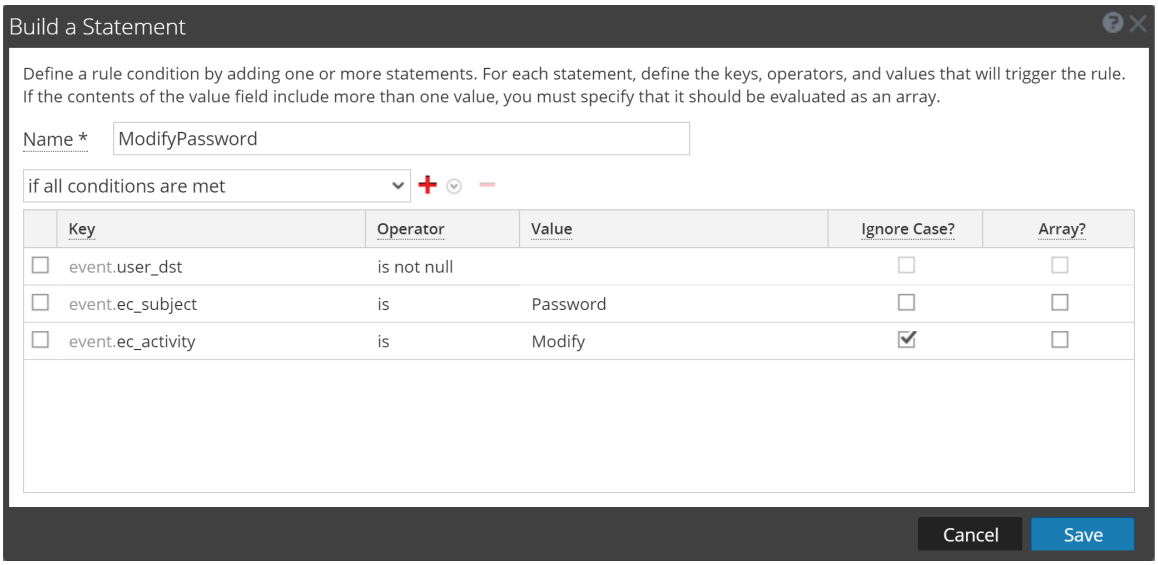
Regelanweisung	Beschreibung
user_dst is not null	Sorgt dafür, dass die Bedingung nur wahr ist, wenn user_dst einen Wert besitzt. Mit dem Operator **is not null** können Sie sicherstellen, dass ein Feld einen Wert zurückgibt. Sie können dieses Feld verwenden, wenn eine Regel davon abhängt, dass ein bestimmtes Feld einen Wert zurückgibt. Beispielsweise möchten Sie eventuell eine Regel erstellen, die denselben Benutzer identifiziert, der mehrmals versucht, sich an demselben Zielkonto anzumelden (möglicherweise also der Versuch, das Passwort zu erraten). Wenn das Feld, das das Benutzerzielkonto repräsentiert, leer ist, möchten Sie nicht, dass die Regel ausgelöst wird. Verwenden Sie den Operator **is not null**, um sicherzustellen, dass das Feld einen Wert enthält.

Die folgende Anweisung ergibt die Bedingung „Erfolg“:



Regelanweisung	Beschreibung
ec_activity is Logon	Identifiziert eine Anmeldeaktivität.
ec_outcome is Success	Identifiziert eine Anmeldung, die erfolgreich abgeschlossen wurde
user_dst is not null	Stellt sicher, dass das Feld für das Benutzerzielkonto ausgefüllt ist, damit die Bedingung wahr sein kann

Die folgende Anweisung ergibt die Bedingung „ModifyPassword“:

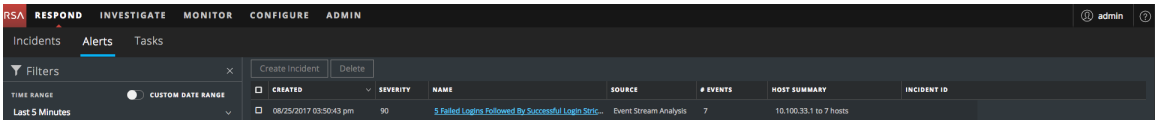


Regelanweisung	Beschreibung
user_dst is not null	Stellt sicher, dass das Feld für das Benutzerzielkonto ausgefüllt ist, damit die Bedingung wahr sein kann
ec_subject is Password	Identifiziert ein Element als Passwort.
ec_activity is Modify	Identifiziert die Aktivität, mit der das Passwort geändert wurde

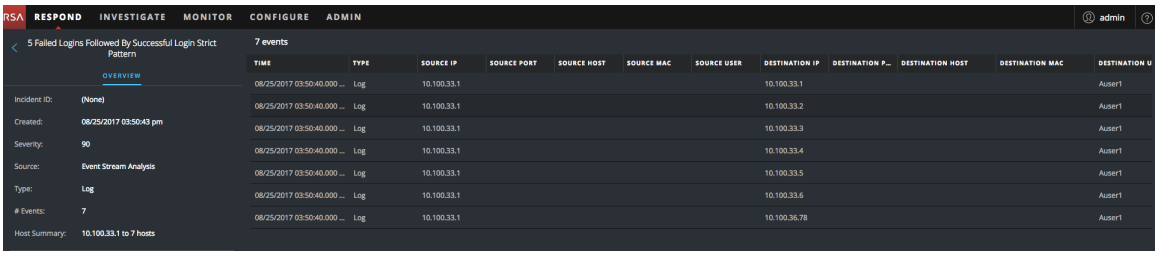
Beispielergebnisse

Wenn die Warnmeldung für die Beispielregel ausgelöst wird, sehen Sie, dass die Regel für 7 Ereignisse ausgelöst wurde und dass jedes Ereignis einen Benutzer enthält. Sie können auch sehen, dass die Ereignisse einem strengen Muster folgen: 5 fehlgeschlagene Anmeldungsereignisse, gefolgt von einem erfolgreichen Anmeldungsereignis, gefolgt von einer Änderung am Konto.

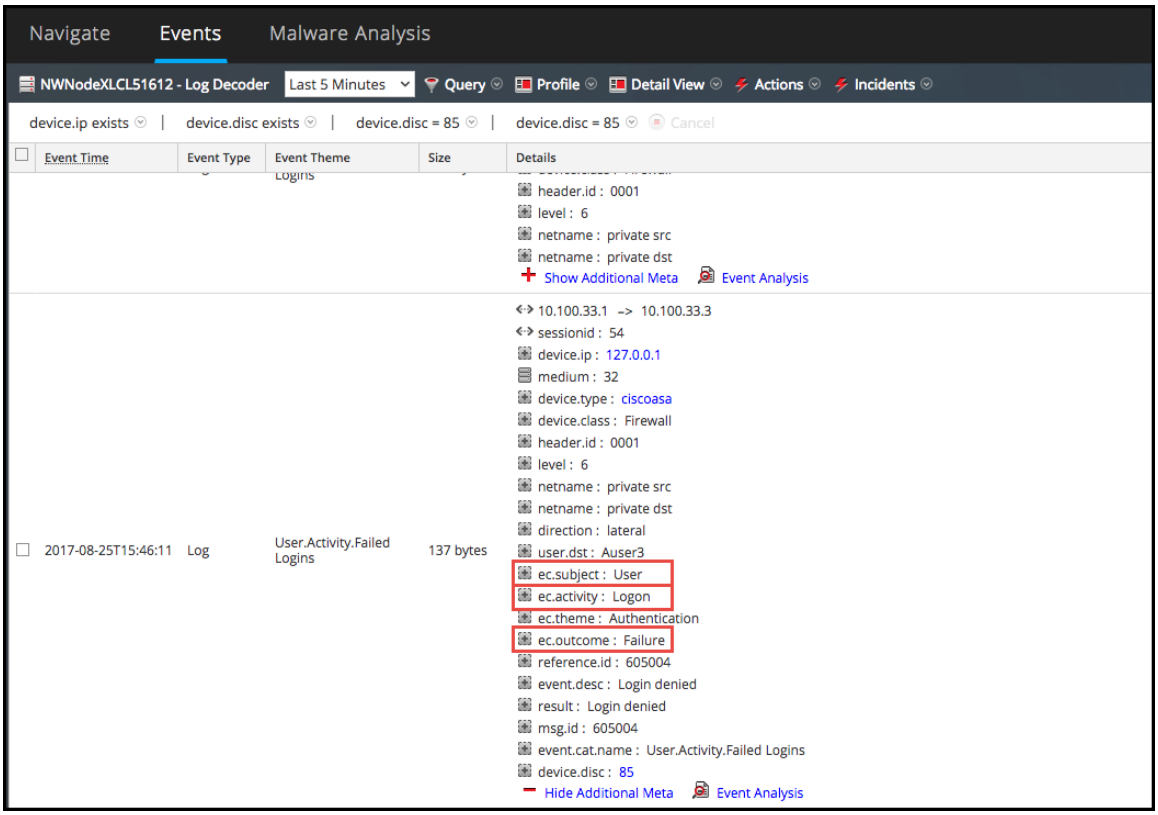
Die folgende Abbildung zeigt die Warnmeldung in der Listenansicht „Reaktionen auf Warnmeldungen“.



Die nächste Abbildung zeigt die Ereignisse in der Warnmeldung in der Ansicht „Details zu Reaktionen auf Warnmeldungen“.



Wenn Sie einen Drill-down in das Modul „Investigation“ durchführen, indem Sie auf die Quelle für eines der Ereignisse klicken, können Sie die Groß- oder Kleinschreibung bei jedem der Zeichenfolgenwerte sehen. Da Sie **Groß-/Kleinschreibung ignorieren** verwendet haben, wird die Regel ausgelöst, wenn die Zeichenfolgenwerte groß- oder kleingeschrieben wurden.

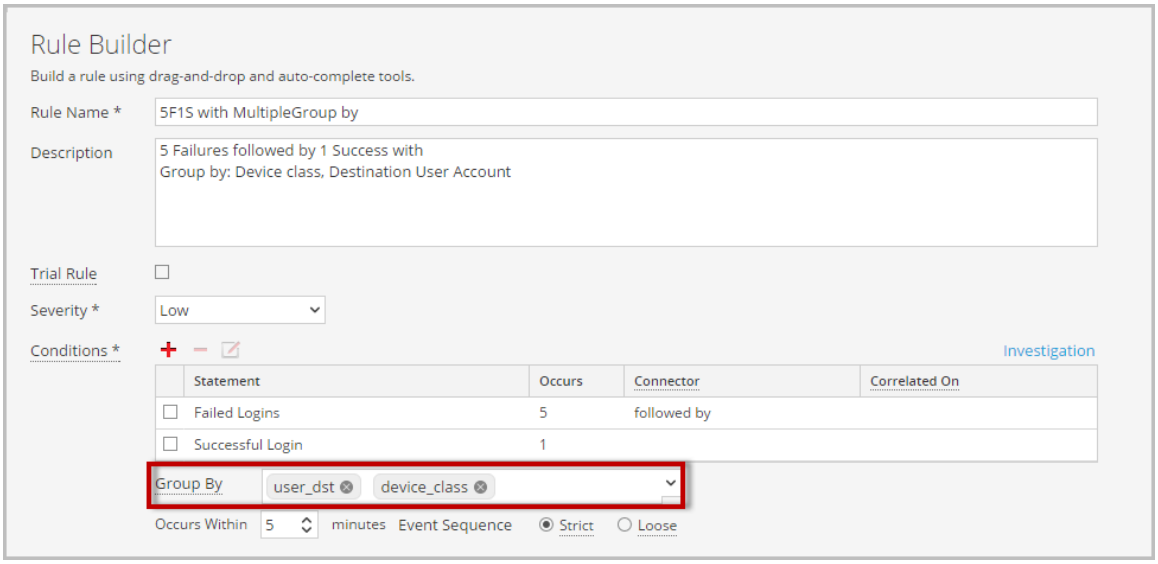


Beispiel: Gruppieren der Regelergebnisse

Das Feld **Gruppieren nach** erlaubt Ihnen, die Regelergebnisse zu gruppieren und zu filtern. Nehmen Sie zum Beispiel an, es gibt 3 Benutzerkonten – Joe, Jane und John – und Sie verwenden den Metawert **Gruppieren nach**, user_dst. Das Ergebnis zeigt Ereignisse gruppiert nach den Konten für Joe, Jane und John an.

Sie können auch nach mehreren Schlüsseln gruppieren und so die Regelergebnisse weiter filtern. Sie können zum Beispiel nach Benutzerzielkonto und Computer gruppieren, um festzustellen, ob ein Benutzer, der am selben Zielkonto von demselben Computer aus angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden. Um dies zu erreichen, können Sie nach „device_class“ und „user_dst“ gruppieren.

Das folgende Beispiel zeigt eine Regel, die nach „device_class“ und „user_dst“ gruppiert wurde.

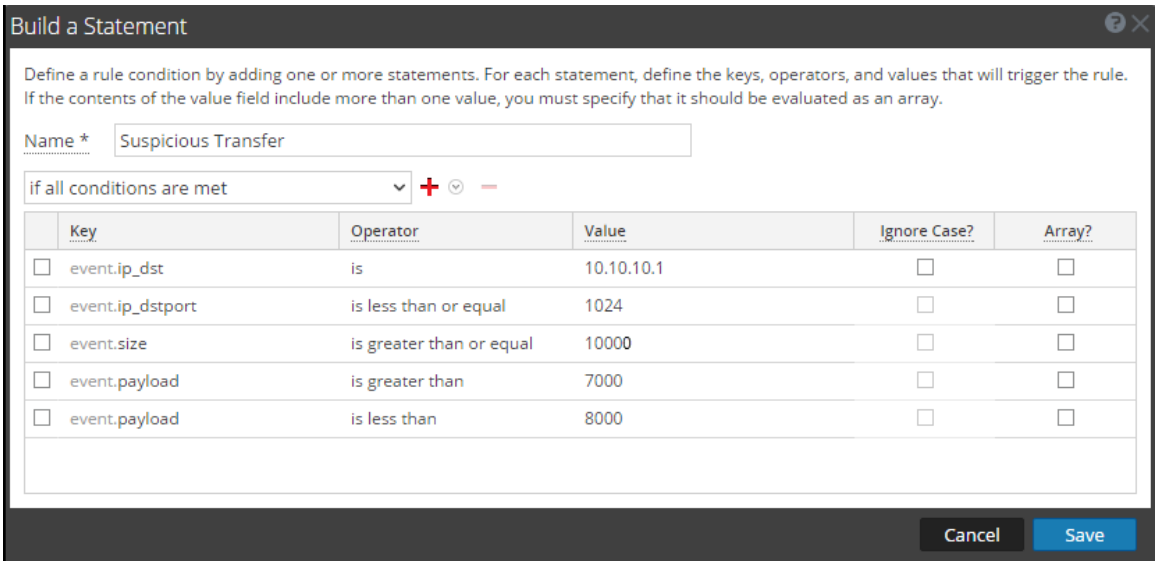


Regelbedingung	Beschreibung
Failed Logins	Identifiziert 5 fehlgeschlagene Anmeldeversuche (darauf muss die nächste Bedingung folgen; d. h. auf die 5 fehlgeschlagenen Anmeldungen muss eine erfolgreiche Anmeldung folgen).
Successful Login	Identifiziert eine erfolgreiche Anmeldung.
Gruppieren nach: user_dst und device_class	Gruppiert die Regelergebnisse nach „user_dst“ (Benutzerzielkonto) und „device_class“ (Typ des Computers, von dem aus sich der Benutzer anmeldet). Dies erlaubt der Regel, nach einem Benutzer zu suchen, der von demselben Computer aus am selben Zielkonto angemeldet ist, und führt damit zu einem weitaus gezielteren Regelergebnis.
Auftreten innerhalb von 5 Minuten mit strikter Musterübereinstimmung	Die Ereignisse müssen innerhalb von 5 Minuten auftreten und die Musterübereinstimmung ist streng, d. h., das Muster muss genau erfüllt sein, damit die Regel auslöst.

Beispiel: Arbeiten mit numerischen Operatoren

Mit numerischen Operatoren können Sie Regeln für numerische Werte schreiben, z. B. angeben, dass ein Wert größer als, kleiner als oder gleich einem bestimmten Wert ist. Dies ist insbesondere für Fälle nützlich, in denen Sie einen numerischen Schwellenwert angeben möchten, z. B. *Nutzdaten sind größer als 7000*.

Im folgenden Beispiel wird versucht, eine Datenübertragung an ein bestimmtes Ziel über gängige Ports zu identifizieren, wobei die Übertragungsgröße hoch ist und die Nutzdaten in einem verdächtigen Bereich liegen.



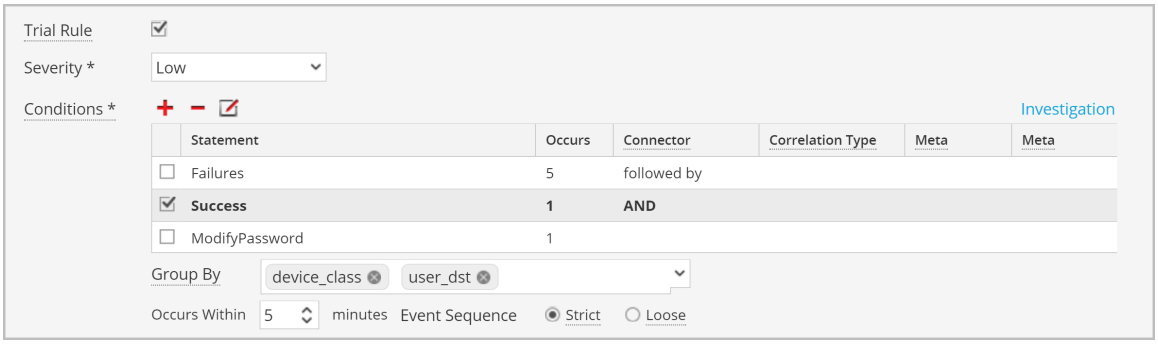
Regelanweisung	Beschreibung
ip_dst is 10.10.10.1	Der Zielport ist 10.10.10.1.
ip_dstport is greater than or equal to 1024	Der Zielport ist im Bereich häufig verwendeter Ports (1024 oder höher).
size is greater than or equal to 10000	Die Größe der Übertragung ist 10000 oder größer, was eine verdächtig große Datenübertragung ist.
payload is greater than 7000	Die Größe der Nutzdaten liegt zwischen 7000 und 8000, was verdächtig groß ist.
payload is less than 8000	Die Größe der Nutzdaten liegt zwischen 7000 und 8000, was verdächtig groß ist.

Schritt 3. Hinzufügen von Bedingungen zu einer Regelanweisung

Dieses Thema enthält Anweisungen zum Hinzufügen von Bedingungen, z. B. zum Spezifizieren eines bestimmten Zeitraums, zu einer Regelanweisung. Beim Erstellen einer Regelanweisung legen Sie fest, was eine Regel erkennt. Sie fügen Bedingungen hinzu, um weitere Festlegungen zu treffen, z. B. wie oft oder wann die Kriterien erfüllt sein müssen.

Beispiel

Die folgende Grafik enthält ein Beispiel mit den Bedingungen von Anweisungen in der Regelerstellung. In Kombination ergeben die Anweisungen und Bedingungen die Regelkriterien.



Diese Regel erkennt 5 fehlgeschlagene Anmeldeversuche gefolgt von einem erfolgreichen Versuch. Dies könnte ein Zeichen dafür sein, dass ein Benutzerkonto gehackt wurde. Die Kriterien für die Regel sind:

A. Es sind 5 fehlgeschlagene Anmeldeversuche hintereinander erforderlich.

B. Auf die Fehlschläge muss 1 erfolgreiche Anmeldung folgen.

C. Ein Kennwort wurde geändert.

D. Alle Ereignisse müssen innerhalb von 5 Minuten auftreten.

E. Gruppieren Sie Warnmeldungen nach Benutzer (user_dst), weil die Schritte A und B auf demselben Benutzerzielkonto durchgeführt werden müssen. Gruppieren Sie auch nach Computer (Device_class), um sicherzustellen, dass der Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden.

F. Die Übereinstimmung ist ein strenges Muster, was bedeutet, dass das Muster genau übereinstimmen muss, ohne dazwischenliegende Ereignisse.

Verfahren

So fügen Sie einer Regelanweisung Bedingungen hinzu:

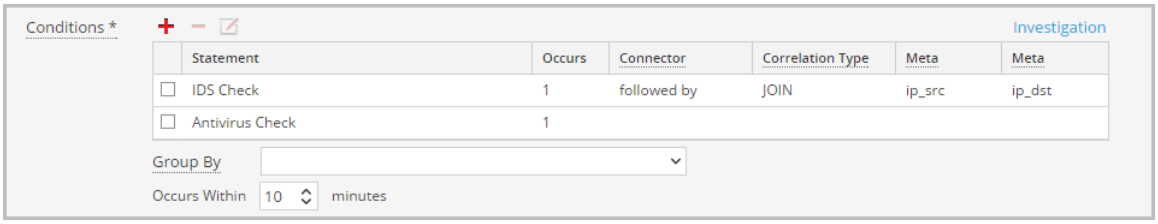
1. Wählen Sie im Bereich **Bedingungen** eine Anweisung aus und klicken Sie auf  .
2. Geben Sie für **Auftreten** einen Wert ein, um anzugeben, wie oft ein Ereignis auftreten muss, um die Regelkriterien zu erfüllen.
3. Wenn mehrere Anweisungen vorhanden sind, wählen Sie im Feld **Verbindungsoperator** einen logischen Operator aus, um die Anweisungen zusammenzufügen:
   - gefolgt von
   - nicht gefolgt von
   - UND
   - ODER
4. Der Parameter **Korrelationstyp** gilt nur für **gefolgt von** und **nicht gefolgt von**. Wenn Sie den Korrelationstyp „GLEICH“ auswählen, wählen Sie einen Metawert für die Korrelation, und wenn Sie den Korrelationstyp „VERKNÜPFEN“ auswählen, wählen Sie zwei Metawerte für die Korrelation. Sie möchten möglicherweise „VERKNÜPFEN“ verwenden, wenn Sie versuchen, Metawerte aus zwei verschiedenen Datenquellen zu korrelieren. Angenommen, Sie möchten eine AV-Warnmeldung mit einer IDS-Warnmeldung korrelieren. In den nachfolgenden Beispielen finden Sie ein Anwendungsbeispiel, in dem zwei Metawerte aus verschiedenen Quellen verknüpft werden.
5. Wenn Ereignisse innerhalb eines bestimmten Zeitraums auftreten müssen, geben Sie im Feld **Auftreten innerhalb** eine Minutenzahl ein.
6. Wählen Sie aus, ob das Muster einer **strengen** oder einer **variablen** Übereinstimmung folgen muss. Wenn Sie eine strenge Übereinstimmung angeben, bedeutet dies, dass das Muster in der genauen Reihenfolge vorkommen muss, die Sie angegeben haben, ohne dass weitere Ereignisse dazwischen vorkommen. Beispiel: Wenn als Sequenz fünf fehlgeschlagene Anmeldungen (F) gefolgt von einer erfolgreichen Anmeldung (S) angegeben ist, wird dieses Muster nur übereinstimmen, wenn der Benutzer die folgende Sequenz ausführt: F, F, F, F, F, S. Wenn Sie eine variable Übereinstimmung angeben, bedeutet dies, dass andere Ereignisse innerhalb der Sequenz auftreten dürfen, aber die Regel wird weiterhin auslösen, wenn alle angegebenen Ereignisse auch auftreten. Beispiel: Fünf fehlgeschlagene Anmeldeversuche (F), gefolgt von einer beliebigen Anzahl dazwischen liegender erfolgreicher Anmeldeversuche (S), gefolgt von einem erfolgreichen Anmeldeversuch, könnten das folgende Muster erzeugen: F, S, F, S, F, S, F, S, F, S, die die Regel trotz der dazwischenliegenden erfolgreichen Anmeldungen auslösen würden.
7. Wählen Sie die Felder, nach denen gruppiert werden soll, aus der Drop-down-Liste aus. Mit dem Feld **Gruppieren nach** können Sie die eingehenden Ereignisse gruppieren und evaluieren. Beispiel: In der Regel, die fünf fehlgeschlagene Anmeldeversuche gefolgt von

einem erfolgreichen Versuch erkennt, muss der Benutzer identisch sein. Daher lautet der unter **Gruppieren nach** aufgeführte Metaschlüssel „user_dst“. Sie können auch nach mehreren Schlüsseln gruppieren. Mithilfe des vorherigen Beispiels möchten Sie eventuell nach Benutzern und Computern gruppieren, um sicherzustellen, dass derselbe Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden. Um dies zu erreichen, können Sie nach „device_class“ und „user_dst“ gruppieren.

Beispiel

Die folgende Grafik zeigt ein Beispiel der Bedingungen für eine Regel, mit denen Sie die gleichen Einheiten über mehrere Geräte hinweg bewerten können, um komplexe Anwendungsbeispiele zu erreichen. Beispielsweise können Sie eine Regel erstellen, die ausgelöst wird, wenn auf eine IDS-Warnmeldung (Intrusion Detection System, Angriffserkennungssystem) eine AV-Warnmeldung (Anti-virus, Virenschutz) für die gleiche Workstation folgt. Der Workstation-Schlüssel der beiden Quellen (ISD und AV) ist nicht identisch, sodass Sie eine Verknüpfung vornehmen können, um die verschiedenen Einheiten zu bewerten.

In der IDS-Warnmeldung wird die Workstation durch die Quell-IP-Adresse aus der IDS-Warnmeldung identifiziert und würde mit der Ziel-IP-Adresse aus der AV-Warnmeldung verglichen.



Die Kriterien für die Regel sind:

A. Eine IDS-Warnmeldung erfolgt.

B. Die Ziel-IP-Adresse aus der AV-Warnmeldung und die Quell-IP-Adresse für die Workstation aus der IDS-Warnmeldung werden verknüpft, damit Sie die gleichen Einheiten über verschiedene Quellen hinweg anzeigen können.

C. Eine Virenschutz-Warnmeldung folgt auf die IDS-Warnmeldung.

Hinzufügen einer erweiterten EPL-Regel

In diesem Thema wird erläutert, wie Sie durch Schreiben einer EPL-Abfrage Regelkriterien definieren. EPL ist eine deklarative Sprache zur Bearbeitung von häufig auftretenden, zeitbasierten Ereignisdaten. Sie dient zum Ausdrücken von Filterungen, Aggregationen und Verknüpfungen über mehrere verteilte Ereignisstreams. EPL umfasst außerdem Mustersemantik zum Ausdruck komplexer zeitlicher Zusammenhänge zwischen Ereignissen.

Schreiben Sie eine erweiterte EPL-Regel, wenn die Regelkriterien komplexer sind als die Angaben in der Regelerstellung ermöglichen.

Die EPL-Syntax kann im Rahmen dieses Handbuchs nicht erläutert werden.

- Die EPL-Dokumentation finden Sie unter http://www.espertech.com/esper/documentation.php.
- Das EPL-Onlinetool finden Sie unter http://esper-epl-tryout.appspot.com/epltryout/mainform.htm.

Voraussetzungen

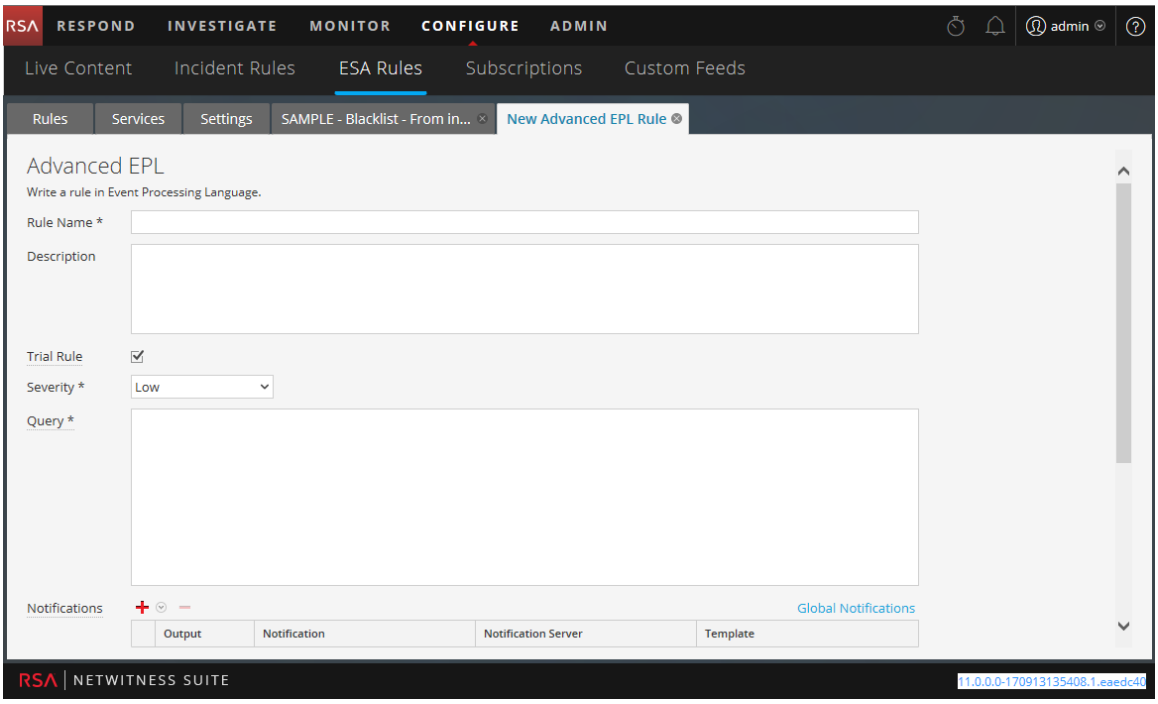
Im Folgenden finden Sie die Voraussetzungen für das Hinzufügen einer erweiterten Regel:

- Sie müssen die EPL (Event Processing Language) kennen.
- Sie müssen ESA-Anmerkungen kennen, um markieren zu können, welche EPL-Anweisungen mit erzeugten Warnmeldungen verknüpft sind.

Verfahren

So fügen Sie eine erweiterte EPL-Regel hinzu:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
2. Wählen Sie in der **Regelbibliothek** die Optionen  **> Erweiterte EPL** aus.



3. Geben Sie im Feld **Name der Regel** einen eindeutigen, deskriptiven Namen ein.

   Dieser Name wird in der Regelbibliothek angezeigt. Wählen Sie ihn spezifisch genug, um die Regel von anderen abzugrenzen.

4. Erläutern Sie im Feld **Beschreibung**, welche Ereignisse von der Regel erkannt werden..

   Der Anfang der Beschreibung wird in der Regelbibliothek angezeigt.

5. Wählen Sie **Testregel** aus, um die Regel automatisch zu deaktivieren, wenn die Summe aller Testregeln den Speicherschwellenwert überschreitet.

   Verwenden Sie den Testregelmodus als Sicherheitsvorkehrung, um zu erkennen, ob eine Regel effizient ausgeführt wird, und um Ausfallzeiten aufgrund von mangelndem Speicherplatz zu vermeiden. Weitere Informationen erhalten Sie unter Verwenden von Testregeln.

6. Klassifizieren Sie den **Schweregrad** für die Regel als Niedrig, Mittel, Hoch oder Kritisch.

7. Schreiben Sie zur Definition der Regelkriterien eine **Abfrage** in EPL.

   Hinweis: Für alle Metaschlüsselnamen müssen Sie einen Unterstrich anstelle eines Punkts verwenden. Zum Beispiel ist `ec_outcome` korrekt, aber `ec.outcome` nicht.

8. Für die Erstellung dynamischer Anweisungsnamen in ESA müssen Sie die Metaschlüssel in geschweifte Klammern setzen und diese Anmerkung in die Syntax einfügen:

   ```
   @Name("RIG {ip_src} {alias_host} {ec_activity}")
   ```

   Hierbei gilt:

- RIG ist der statische Teil des Anweisungsnamen
- {ip_src}, {alias_host}, {ec_activity} ist der dynamische Teil des Anweisungsnamen

Hinweis: Wenn Metadaten im dynamischen Teil des Anweisungsnamens einen Null-Wert aufweisen, wird dieser als statischer Text angezeigt.

Wenn eine Regel eine Warnmeldung erzeugen soll, fügen Sie diese ESA-Anmerkung in der Syntax ein:

```
@RSAAlert
```

Weitere Informationen zu ESA-Anmerkungen finden Sie unter ESA-Anmerkungen.

Event Processing Language (EPL)

In diesem Thema wird EPL (Event Processing Language, Ereignisverarbeitungssprache) beschrieben, eine deklarative Sprache zur Handhabung hochfrequenter, zeitbasierter Ereignisdaten. ESA verwendet EPL, eine deklarative Sprache zur Handhabung hochfrequenter, zeitbasierter Ereignisdaten. Sie dient zum Ausdruck von Filterung, Aggregation und Verknüpfung über mehrere verteilte Ereignisstreams. EPL umfasst außerdem Mustersemantik zum Ausdruck komplexer zeitlicher Zusammenhänge zwischen Ereignissen. Sie kann unter anderem folgende Funktionen ausführen:

- Ereignisfilterung
- Warnmeldungsunterdrückung
- Berechnung von Prozentwerten oder Verhältnissen
- Durchschnitt, Zähler, Minimum und Maximum für ein angegebenes Zeitfenster
- Korrelation von Ereignissen, die in mehreren Streams eingehen
- Korrelation von Ereignissen, die in falscher Reihenfolge eingehen
- Ein/Aus-Fenster
- Unterstützung von Gefolgt von und Nicht gefolgt von
- Unterstützung von Regex-Filtern

Datenbanken können sinnvolle Daten nur als Antwort auf explizite Abfragen zurückgeben und sind nicht zur Push-Übertragung von Daten bei Änderungen geeignet. Der Entwickler muss die zeitliche Logik und die Aggregationslogik selbst implementieren. Im Gegensatz dazu bietet die EPL-Engine eine höhere Abstraktion und Intelligenz; man kann sie sich als auf dem Kopf stehende Datenbank vorstellen. Anstatt Daten zu speichern und Abfragen an den gespeicherten Daten durchzuführen, ermöglicht EPS es Anwendungen, die Abfragen zu speichern und die Daten kontinuierlich durchlaufen zu lassen. Die Antwort der EPL-Engine wird in Echtzeit gegeben, wenn Bedingungen auftreten, die den vom Benutzer definierten Abfragen entsprechen.

Erweiterte ESA-Regeln erfordern eine korrekte Groß- und Kleinschreibung, aber in der Ansicht „Investigation“ werden alle Zeichen in Kleinbuchstaben umgewandelt. Jedoch dürfen die Metadaten trotz der Darstellung in der Ansicht „Investigation“ keine Kleinbuchstaben enthalten. Um sicherzustellen, dass Sie die korrekte Groß-/Kleinschreibung verwenden, empfiehlt RSA die Verwendung der Funktion *toLowerCase()*. Beispiel:

```
@RSAAlert(oneInSeconds=0)
SELECT * FROM Event(
/* Statement: Download PDF File */
(filetype.toLowerCase() IN ( 'pdf' ) AND medium IN ( 1 ))
OR
/* Statement: Download EXE File */
(filetype.toLowerCase() IN ( 'windows_executable' , 'x86 pe' , 'windows executable' ) AND medium IN ( 1 ))
).win:time(5 Minutes)
MATCH_RECOGNIZE (
PARTITION BY ip_src
MEASURES E1 as e1_data , E2 as e2_data
PATTERN (E1+ E2)
DEFINE
E1 as (E1.filetype.toLowerCase() IN ( 'pdf' ) AND E1.medium IN ( 1 )),
E2 as (E2.filetype.toLowerCase() IN ( 'windows_executable' , 'x86 pe' , 'windows executable' ) AND E2.medium IN ( 1 ))
```

In der Onlinehilfe wird die Einrichtung von ESA anhand von einfachen Anweisungen illustriert; wenn Sie jedoch weitere Informationen über das Verfassen von EPL-Anweisungen benötigen, erhalten Sie auf der Website http://www.espertech.com Schulungsmaterial und Beispiele.

Hinweis: ESA unterstützt Esper Version 5.3.0.

ESA-Anmerkungen

In diesem Thema werden Anmerkungen beschrieben, die NetWitness Suite zur Verwendung in erweiterten EPL-Regeln bereitstellt.

@RSAAlert-Anmerkung

Mit der @RSAAlert-Anmerkung können die EPL-Anweisungen markiert werden, die mit erzeugten Warnmeldungsbenachrichtigungen verknüpft sind. Sie ist auf die Verwendung zusammen mit der Funktion zur Unterdrückung von Warnmeldungsbenachrichtigungen in der Benutzeroberfläche der Regelerstellung ausgelegt.

Die @RSAAlert-Anmerkung kann bei der Arbeit mit Warnmeldungsbenachrichtigungen hilfreich sein, insbesondere wenn Sie Benachrichtigungen filtern möchten, z. B. das Senden einer Benachrichtigung für jeden Benutzer, der eine Warnmeldung auslöst.

Nehmen wir beispielsweise an, dass Sie Warnmeldungsbenachrichtigungen für Anmeldungsfehler erzeugen möchten. Sie können die folgende Anweisung hinzufügen:

*@RSAAlert select * from event(msg_id="login_fail")*

Ereignisnummer	Meldungs-ID	username	src_IP	Uhrzeit
1	login_fail	alice	1.2.3.4	10:00
2	login_fail	alice	1.2.3.4	10:01
3	login_fail	alice	6.7.8.9	10:01
4	login_fail	bob	1.2.3.4	10:01
5	login_fail	alice	1.2.3.4	10:03

Für die obige Anweisung werden fünf Warnmeldungen generiert.

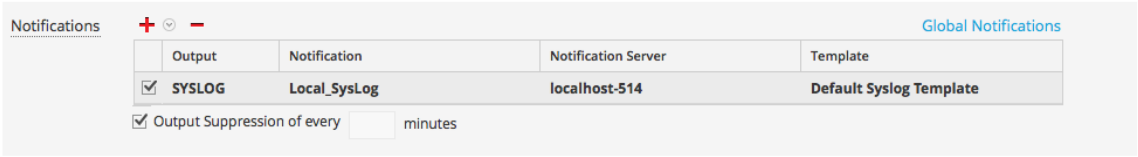
Nehmen wir jedoch an, dass Sie die Anweisung so ändern möchten, dass eine Warnmeldung für jeden separaten Benutzernamen generiert wird. Sie können das Attribut *identifier* verweden. Beispielsweise generiert die Anweisung *@RSAAlert(identifier={"username"}) SELECT* FROM Event(msg_id="login_fail")* eine Benachrichtigung für die erste Warnmeldung für „bob" und eine für die erste Warnmeldung für „alice". Nachfolgende Warnmeldungen für „bob" und „alice" werden ignoriert.

Sie können die Benutzer weiter unterscheiden, indem Sie Details über die identifier-Variable hinzufügen. Sie können beispielsweise anhand der folgenden Anweisung nach Benutzer und IP-Adresse unterscheiden: *@RSAAlert(identifier={"username", "src_ip"}) SELECT* FROM Event (msg_id="login_fail")*. Anschließend würden Sie Benachrichtigungen sehen, die nach Benutzername und IP-Adresse generiert werden (eine Warnmeldung für „alice" unter 1.2.3.4, eine weitere Warnmeldung für „alice" unter 6.7.8.9 und eine Warnmeldung für „bob" unter 1.2.3.4).

So verwenden Sie Kennungen mit Unterdrückung von Warnmeldungsbenachrichtigungen:

Die @RSAAlert-Anweisung ist auf die Verwendung zusammen mit der Funktion zur Unterdrückung von Warnmeldungsbenachrichtigungen in der Benutzeroberfläche der Regelerstellung ausgelegt. Gehen Sie hierfür folgendermaßen vor:

1. Erstellen Sie eine Regel in der Benutzeroberfläche der Regelerstellung und wählen Sie die Funktion für die Unterdrückung von Warnmeldungen aus, wenn Sie Benachrichtigungen konfigurieren.



2. Kopieren Sie den Code aus der Regelerstellungsregel in eine neue erweiterte Regel.
3. Konfigurieren Sie die erweiterte Regel für die Einbeziehung von Kennungen (wie oben beschrieben) und speichern Sie die erweiterte Regel.
4. Löschen Sie die ursprüngliche Regelerstellungsregel.

@RSAPersist-Anmerkung

Mit der @RSAPersist-Anmerkung kann ein benanntes Fenster als von ESA verwaltetes, persistentes Fenster markiert werden. Nachdem ein benanntes Fenster als von ESA verwaltetes Fenster markiert wurde, schreibt ESA die Inhalte des Fensters regelmäßig auf die Festplatte und stellt sie wieder her, wenn die Bereitstellung des Fensters aufgehoben wurde und es wiederhergestellt werden soll. Das System erfasst kurz vor dem Aufheben der Bereitstellung des Moduls und der Entfernung des Fensters einen Snapshot. In ähnlicher Weise stellt es die Fensterinhalte aus dem Snapshot sofort nach dem erneuten Bereitstellen des Moduls wieder her. Damit wird sichergestellt, dass die Inhalte des Fensters nicht verloren gehen, wenn sich der Modulstatus ändert oder der ESA-Service ausfällt.

Beispiel: Das Fenster mit der Bezeichnung `DHCPTracker` enthält eine Zuordnung von IP-Adressen zu dem zuletzt zugewiesenen Hostnamen. Sie können der Anweisung folgende @RSAPersist-Anmerkung hinzufügen:

```
@RSAPersist
 create window DHCPTracker.std:unique(ip_src) as (ip_src string, alias_
host string);
 insert into DHCPTracker select IP as ip_src, HostName as alias_
host from DHCPAssignment(ID=32);
```

Hinweis: Nicht alle Fensterdefinitionen eignen sich für die Persistenz. `@RSAPersist` - Anmerkungen müssen mit Vorsicht verwendet werden. Wenn das Fenster über Datensätze mit Zeitangaben verfügt oder wenn es von zeitbasierten Einschränkungen abhängt, ist es sehr wahrscheinlich, dass das Fenster durch den Snapshot nicht im richtigen Status wiederhergestellt wird. Außerdem machen alle Änderungen an der Fensterdefinition den Snapshot ungültig, sodass das Fenster auf einen leeren Status zurückgesetzt werden würde. Das System führt keine semantische Analyse durch, um zu ermitteln, ob die Änderungen einer Fensterdefinition Konflikte auslösen. Beachten Sie, dass Änderungen an anderen Teilen eines Moduls (d. h. anderen als dem CREATE WINDOW-Aufruf, der das Fenster definiert) die Snapshots nicht ungültig machen.

@UsesEnrichment (10.6.1.1 und höher)

@UsesEnrichment kann in erweiterten EPL-Regeln verwendet werden, um Erweiterungen zu referenzieren. Um Erweiterungen mit ESA zu synchronisieren, müssen alle Erweiterungsabhängigkeiten in EPL-Regeln mit der Anmerkung @UsesEnrichment referenziert werden.

Die Anmerkung @UsesEnrichment verwendet das folgende Format:

```
@UsesEnrichment(name= '<enrichment_name>')
```

Die folgende EPL referenziert z. B. eine Whitelist-Erweiterung:

```
@UsesEnrichment(name = 'Whitelist')

@RSAAlert

SELECT * FROM Event(ip_src NOT IN (SELECT ip_address FROM Whitelist))
```

@Name

@Name ist der Name der Anweisung, der in erweiterten ESA-Regeln definiert ist. Er wird verwendet, um Anweisungsnamen dynamisch in ESA-Warnmeldungen zu generieren. Der Anweisungsname von nur einer eine Warnmeldung auslösenden Anweisung wird angezeigt. Diese Anmerkung besitzt Metaschlüssel, die in geschweiften Klammern stehen.

Die Anmerkung @Name verwendet das folgende Format:

```
@Name("<static_part_of_statement_name> {meta_key1} {meta_
key2}…")
```

Z. B. referenziert die folgende EPL die Metaschlüssel *ip_src* und *user_name*, deren Werte dynamisch erzeugt werden.

@Name(“Login Event to {ip_src} by {user_name}”)

Hinweis: Sie können eine beliebige Anzahl von Metaschlüsseln in der Anweisung für die dynamische Erstellung von Anweisungsnamen angeben.
Die Länge der einzelnen Metaschlüssel ist auf 64 beschränkt. Danach wird der Wert gekürzt und „...“ wird angehängt.
Die Länge bei der dynamischen Generierung des Anweisungsnamens ist auf 128 beschränkt. Danach wird der Wert auf 128 gekürzt und „...“ wird angehängt. Alle übrigen Werte nach der Kürzung werden als statische Werte behandelt.

Beispiele für erweiterte EPL-Regeln

Im Folgenden sehen Sie die Beispiele für erweiterte ESA-Regeln. Jedes Beispiel bietet mehrere Möglichkeiten zur Implementierung des gleichen Anwendungsbeispiels.

Beispiel Nr. 1:

Erstellen Sie ein Benutzerkonto und löschen Sie eben dieses Benutzerkonto in 300 Sekunden. Benutzerinformationen werden in der Metadatei user_src gespeichert.

EPL Nr. 1:

Name der Regel	CreateuseraccountFollowedbyDeletionof Useraccount1
Regelbeschreibung	Erstellen Sie ein Benutzerkonto, gefolgt von einer Aktion, um eben dieses Benutzerkonto in 300 Sekunden zu löschen.

Regelcode	`SELECT * FROM Event(ec_subject='User'`
	`  AND ec_outcome='Success'`
	`  AND user_src is NOT NULL`
	`  AND ec_activity IN ('Create',`
	`'Delete')`
	`  ).win:time(300 seconds)`
	`match_recognize (partition by user_src`
	`  measures C as c, D as d`
	`  pattern (C D)`
	`  define`
	`  C as C.ec_activity='Create' ,`
	`  D as D.ec_activity='Delete');`

Hinweis	• Filtern Sie Ereignisse, die für Muster im vorgegebenen Zeitraum erforderlich sind. Aufgrund der Filterbedingungen sollten nur erforderliche Ereignisse an die Funktion match_recognize übergeben werden. In diesem Fall handelt es sich um Erstellen und Löschen

	von Benutzerkontoereignissen, d. h. Event(ec_ subject='User' AND ec_outcome='Success' AND user_ src is NOT NULL AND ec_activity IN ('Create', 'Delete'). • Partitionieren Sie durch das Erstellen von Buckets. In diesem Fall werden von Esper Buckets pro Wert von user_src erstellt. Und daher weisen beide Ereignisse den gleichen Wert von user_src auf. • Definieren Sie das gewünschte Muster. Gegenwärtig ist es auf Erstellen gefolgt von Löschen eingestellt. Sie können mehrfach Erstellen gefolgt von Löschen (C+ D) einstellen. Ein Muster ist einem regulären Ausdruck sehr ähnlich. • Dies ist das effizienteste Anwendungsbeispiel.

EPL Nr. 2:

Name der Regel	CreateuseraccountFollowedbyDeletionof Useraccount2
Regelbeschreibung	Erstellen Sie ein Benutzerkonto, gefolgt von einer Aktion, um eben dieses Benutzerkonto in 300 Sekunden zu löschen.

Regelcode	`SELECT * from pattern[every (a= Event(ec_ subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create'))`
	`->`
	`( Event(ec_subject='User' AND ec_ outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create') AND user_src = a.user_src)`
	`) )where timer:within(300 Sec) ];`

Hinweis	• Angenommen, der Benutzer wird zweimal erstellt und einmal gelöscht in dieser Reihenfolge. Dann gibt das oben genannte Muster 2 Warnmeldungen aus. • Für jede Benutzererstellung wird ein Thread erstellt.

	• Es gibt keine Möglichkeit, um Threads zu steuern. Es ist wichtig, zeitliche Begrenzungen und vorzugsweise kurze Intervalle anzugeben.

Beispiel Nr. 2:

Entdecken eines Musters, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers und der anschließenden Löschung des Benutzerkontos. Im Fall von Windows-Protokollen werden Benutzerinformationen je nach Ereignis entweder in user_dst oder user_src gespeichert.

user_src(create) = user_dst(Login) = user_src(Delete)

EPL Nr. 3:

Name der Regel	CreateUserLoginandDeleteUser
Regelbeschreibung	Entdecken Sie ein Muster, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers, gefolgt vom Löschen des Benutzerkontos.

Regelcode	`SELECT * FROM Event(ec_subject='User'`
	`  and ec_activity in`
	`('Create','Logon','Delete')`
	`  and ec_theme in ('UserGroup',`
	`'Authentication')`
	`  and ec_outcome='Success'`
	`  ).win:time(300 seconds)`
	`match_recognize (measures C as c, L as l, D as d`
	`  pattern (C L D)`
	`  define`
	`  C as C.ec_activity = 'Create',`
	`  L as L.ec_activity = 'Logon' AND L.user_dst = C.user_src,`
	`  D as D.ec_activity = 'Delete' AND D.user_src = C.user_src`
	`  );`

Hinweis	• Da user_src/user_dst nicht allen Ereignissen gemeinsam ist, kann keine Partition verwendet werden. 1 einziger Bucket führt jeweils 1 Muster aus. Beispiel: Wenn der Ereignisstream für Benutzer 1 und 2 C1C2L1D1, C1L1C2D1 lautet, wird keine Warnmeldung ausgegeben,

	da der Thread C1 von C2 zurückgesetzt wurde. Eine Warnmeldung wird nur ausgegeben, wenn C1L1D1 in dieser Reihenfolge erfolgen und kein anderes Ereignis weder von selben Benutzer noch einem anderen Benutzer dazwischen auftritt. • Eine weitere Lösung wäre die Verwendung eines benannten Fensters, das Zusammenführen von user_dst und user_src in einer einzelne Spalte und die anschließende Ausführung von match_recognize. (EPL Nr. 3). • Muster können ebenfalls verwendet werden. Möglicherweise erhalten Sie mehr Warnmeldungen als erwartet. (EPL Nr. 4).

EPL Nr. 4: Verwenden von NamedWindows und match_recognize

Name der Regel	CreateUserLoginandDeleteUser
Regelbeschreibung	Entdecken Sie ein Muster, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers, gefolgt vom Löschen des Benutzerkontos.

Regelcode	`@Name('NormalizedWindow') create window FilteredEvents.win:time(300 sec) (user String, ecactivity string, sessionid Long);`
	`@Name('UsersrcEvents') Insert into FilteredEvents select user_src as user, ec_ activity as ecactivity, sessionid from Event ( ec_subject='User' and ec_activity in ('Create','Delete') and ec_theme in ('UserGroup', 'Authentication') and ec_ outcome='Success' and user_src is not null );`
	`@Name('UsrdstEvents') Insert into FilteredEvents select user_dst as user, ec_ activity`
	`as ecactivity, sessionid from Event( ec_ subject='User' and ec_activity in (Logon') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success'`

	and user_dst is not null); @Name('Pattern') @RSAAlert(oneInSeconds=0, identifiers={"user"}) select * from FilteredEvents match_recognize (partition by user measures C as c, L as l, D as d pattern (C L+D) define C as C.ecactivity= 'Create', L as L.ecactivity= 'Logon', D as D.ecactivity='Delete');

EPL Nr. 5: Verwenden von Every @RSAAlert(oneInSeconds=0, identifiers={user_src})

SELECT a.time as time,a.ip_src as ip_src,a.user_dst as user_dst,a.ip_dst as ip_dst,a.alias_host as alias_host from pattern[every (a=Event (ec_subject='User' and ec_activity='Create' and ec_theme='UserGroup' and ec_outcome='Success') -> (Event(ec_subject='User' and ec_activity='Logon' and ec_theme='Authentication' and user_src=a.user_dst) -> b=Event (ec_subject='User' and ec_activity='Delete' and ec_theme='UserGroup' and user_dst=a.user_dst))) where timer:within(300 sec)];

Name der Regel	CreateUserLoginandDeleteUser
Regelbeschreibung	Entdecken Sie ein Muster, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers, gefolgt vom Löschen des Benutzerkontos.

Beispiel Nr. 3:

Übermäßige Anmeldungsfehler von derselben Quell-IP

EPL Nr. 6: @RSAAlert(oneInSeconds=0, identifiers={ip_src})

Name der Regel	ExcessLoginFailure
Regelbeschreibung	Derselbe Benutzer versuchte, sich von derselben Quell-IP anzumelden, und die Anmeldung ist fehlgeschlagen
Regelcode	SELECT * FROM Event(ip_src IS NOT NULL AND ec_activity='Logon'

```
AND ec_outcome = 'Failure' ).std:groupwin(ip_
src).win:time_length_batch(300 sec, 10) GROUP
BY ip_src HAVING COUNT(*) = 10;
```

Hinweis

- Erstellt Fenster gemäß ip_src
- Verwendet time_length_batch: Prüft Ereignisse in Stapeln (Rollierendes Fenster). Jedes Ereignis ist nur Teil eines Fensters. Das Fenster gibt Ereignisse frei, wenn entweder die Zeit abgelaufen oder die Anzahl erreicht ist.
- Eines der Probleme mit rollierenden Fenstern ist, dass Ereignisse, die gegen Stapelende auftreten, möglicherweise keine Warnmeldung auslösen.

Obgleich in der folgenden Reihenfolge der Ereignisse bis t=301 10 Anmeldungsfehler für dieselbe Anmeldung in den letzten 300 Sekunden auftraten, wird keine Warnmeldung ausgegeben, da der Ereignisstapel bei t=300 verworfen wurde.

Zeit t	Anmeldungsfehler für bestimmte Benutzer	Warnmeldungen	Zeitstapel
0	0	0	1
295	6	0	1
299	3	0	1
301	1	0	2
420	6	0	2
550	3	0	2
600	0	0	3
720	6	0	3
850	3	0	3
900	1	1	3 endet und 4 beginnt

- Das oben genannte Problem kann mithilfe von win:time-Fenstern (EPL Nr. 7) anstelle von win:time_length_batch-Fenstern gelöst werden.
- Mit dem äußeren Group by werden Ereignisse nach Ablauf der Zeit gesteuert. Angenommen, es liegen 9 Ereignisse nach

	60 Sekunden vor, dann werden diese 9 Ereignisse von der Esper-Engine an den Listener übertragen. Group by und Count führen zu einer Einschränkung, da die Anzahl ungleich 10 ist. • Zeit und Anzahl können nach Bedarf geändert werden.

EPL Nr. 7: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Name der Regel	ExcessLoginFailure
Regelbeschreibung	Derselbe Benutzer versuchte, sich von derselben Quell-IP anzumelden, und die Anmeldung ist fehlgeschlagen
Regelcode	`SELECT * FROM Event( ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time (300 sec) GROUP BY ip_src HAVING COUNT(*) = 10`
Hinweis	• Hierbei handelt es sich um ein Schiebefenster, d. h. nachdem eine Warnmeldung für eine Reihe von Ereignisse ausgegeben wurde, können sie für eine weitere Warnmeldung verwendet werden, bis die Zeit abgelaufen ist. • Wenn 10 Ereignisse an der Auslösung einer Warnmeldung beteiligt waren, wird nur der letzte Ereignisse angezeigt. • Wenn < oder > verwendet werden, wird möglicherweise mehr als eine Warnmeldung angezeigt. Sie sollten die Warnmeldungsunterdrückung entsprechend einsetzen.

Beispiel Nr. 4:

Mehrere fehlgeschlagene Anmeldungen von verschiedenen Benutzern von derselben Quelle an dasselbe Ziel, ein einzelner Benutzer von mehreren verschiedenen Quellen an dasselbe Ziel.

EPL Nr. 8: Verwenden von groupwin , time_length_batch und unique

Name der Regel	MultiplefailedLogins

Regelbeschreibung	Es liegen mehrere fehlgeschlagene Anmeldungen für die folgenden Fälle vor: - von mehreren Benutzern von derselben Quelle an dasselbe Ziel. - von einem einzelnen Benutzer von mehreren Quellen an dasselbe Ziel.
Regelcode	`SELECT * FROM Event( ec_activity='Logon' AND ec_outcome='Failure' AND ip_src IS NOT NULL AND ip_dst IS NOT NULL AND user_dst IS NOT NULL ).std:groupwin(ip_src,ip_dst).win:time_length_batch(300 seconds, 5}).std:unique (user_dst) group by ip_src,ip_dst having count(*) = 5;`
Hinweis	• ip.dst und ip.src sind allen Ereignissen gemeinsam. • user_dst ist für alle Ereignisse eindeutig. • Eine Warnmeldung wird abgegeben, wenn mindestens 5 verschiedene Benutzer eine Anmeldung von derselben ip.src- und ip.dst-Kombination versuchen.

Beispiel Nr. 5:

Kein Protokollverkehr von einem Gerät in einem vorgegebenen Zeitraum.

EPL Nr. 9: Verwenden von „groupwin“, „time_length“ und „unique“

Name der Regel	NoLogTraffic
Regelbeschreibung	Es wird kein Protokollverkehr von einem Gerät in einem vorgegebenen Zeitraum festgestellt.
Regelcode	`SELECT * FROM pattern [every a = Event (device_ip IN ('10.0.0.0','10.0.0.1') AND medium = 32) -> (timer:interval (3600 seconds) AND NOT Event(device_ip = a.device_ip AND device_type = a.device_type AND medium = 32))];`
Hinweis	• Von der Regel wird nur ein plötzlicher Verkehrsrückgang

	erkannt. Es wird keine Warnmeldung ausgegeben, wenn es überhaupt keinen Datenverkehr gibt. Es ist mindestens ein Ereignis erforderlich, damit aufgrund der Regel eine Warnmeldung ausgegeben wird. • Liste der Geräte-IP-Adresse oder Gerätehostnamen als Eingabe. Nur diese Systeme werden nachverfolgt. • Eine Zeiteingabe ist erforderlich. Eine Warnmeldung wird ausgegeben, wenn das Zeitintervall zwischen Ereignissen die Eingabezeit überschreitet.

Beispiel Nr. 6:

Mehrere fehlgeschlagene Anmeldungen vom selben Benutzer, auf die KEIN Sperrungsereignis folgt.

EPL Nr. 10: Verwenden von groupwin , time_length_batch und unique

Name der Regel	FailedloginswoLockout
Regelbeschreibung	Es gibt mehrere fehlgeschlagene Anmeldungen vom selben Benutzer, auf die KEIN Sperrungsereignis folgt.

Regelcode	`SELECT * FROM pattern [every-distinct (a.user_dst, a.device_ip, 1 msec) (a= Event(ec_activity='Logon' and ec_ outcome='Failure' and user_dst IS NOT NULL) -> [2]( Event( device_ip =a.device_ip and ec_activity='Logon' and ec_outcome='Failure' and user_ dst=a.user_dst)`
	`AND NOT Event( ( ec_activity='Logon' and ec_outcome='Success' and device_ip = a.device_ip and user_dst=a.user_dst) or (ec_activity='Lockout' and device_ip = a.device_ip and user_dst=a.user_dst))))`
	
	`where timer:within(60 seconds) -> (timer:interval(30 seconds) and not Event(device_ip=a.device_ip and user_ dst=a.user_dst and ec_ activity='Lockout')) ];`

Hinweis	• Mit der oben genannten Abfrage wird das Fehlen eines Sperrungsereignisses nach 2 fehlgeschlagenen Anmeldungen vom selben Benutzer erkannt. • Der Zeitpunkt des Auftretens der fehlgeschlagenen Anmeldungen wird aufgezeichnet, und es wird davon ausgegangen, dass sie in einem bestimmten Zeitraum auftreten. Außerdem wird in der Praxis davon ausgegangen, dass das Sperrungsereignis kurze Zeit nach der letzten fehlgeschlagenen Anmeldung auftritt, da der Schwellenwert für fehlgeschlagene Anmeldungen pro Benutzer in einer vorgegebenen Domain festgelegt wird. • In der aktuellen Abfrage wird durch every-distinct ein neuer Thread mit einer Kombination aus Benutzer und Gerät für 1 Millisekunde unterdrückt. • Die für 3 fehlgeschlagene Anmeldungen zulässige Zeit nach dem ersten fehlgeschlagenen Versuch beträgt 60 Sekunden. Die Wartezeit für das Auftreten des Sperrungsereignisses beträgt 30 Sekunden.

Beispiel Nr. 7:

Benutzerdefinierte Funktionen zum Durchführen von LIKE- und REGEX-Vorgängen für Arrayelemente.

EPL #11: @RSAAlert(oneInSeconds=0)

Name der Regel	MatchLikeRegex
Regelbeschreibung	Es gibt benutzerdefinierte Funktionen zum Durchführen von LIKE- und REGEX-Vergleichen für Array-Metaschlüssel.

Regelcode	`SELECT * FROM pattern[`
	`e1=Event(matchLike(alias_host, "10.0.0.%")) AND`
	`e2=Event(matchRegex(alias_host, "10\.0\.0\.1[0-9][0-9]"))`
	`where timer:within(5 Minutes)];`

Hinweis:
1. “.” in Metaschlüsseln muss durch ("_") ersetzt werden.
2. Alle Muster sollten zeitgebunden sein.
3. Verwenden von entsprechenden Tags vor den Aussagen
 a) @RSAPersist:
 b) @RSAAlert:

Weitere Informationen finden Sie im:

- EPL-Dokumentation: http://www.espertech.com/esper/documentation.php
- EPL-Onlinetool: http://esper-epl-tryout.appspot.com/epltryout/mainform.html

Arbeiten mit Regeln

In diesem Thema werden zusätzliche Verfahren erläutert, die Sie in Bezug auf Regeln durchführen können. Eventuell möchten Sie eines der folgenden Verfahren durchführen:

- Bearbeiten, Duplizieren oder Löschen einer Regel
- Filtern oder Suchen von Regeln
- Importieren oder Exportieren von Regeln

Bearbeiten, Duplizieren oder Löschen einer Regel

In diesem Thema erfahren Sie, wie Sie eine Event Stream Analysis-Regel (ESA) bearbeiten, duplizieren oder löschen. Wenn Sie eine Regel bearbeiten, wendet ESA die aktualisierten Kriterien für die zukünftige Verarbeitung an. Es werden keine Änderungen an zuvor erzeugten Warnmeldungen vorgenommen.

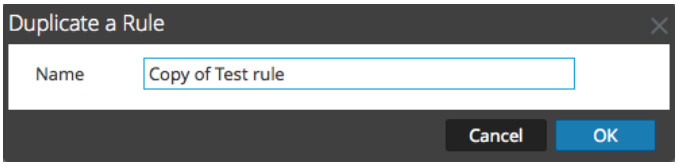
Methoden

Bearbeiten einer Regel

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
   Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie in der **Regelbibliothek** die Regel aus, die Sie bearbeiten möchten, und klicken Sie auf  .
   Je nach Regeltyp wird die entsprechende Registerkarte „Regel“ angezeigt.
3. Ändern Sie die erforderlichen Parameter.
4. Klicken Sie auf **Speichern**.

Duplizieren von Regeln

1. Wählen Sie die zu duplizierende Regel in der **Regelbibliothek** aus und klicken Sie auf .
2. Das Dialogfeld „Regel duplizieren“ wird angezeigt. Das System fügt vor dem Regelnamen **Kopie von** hinzu.

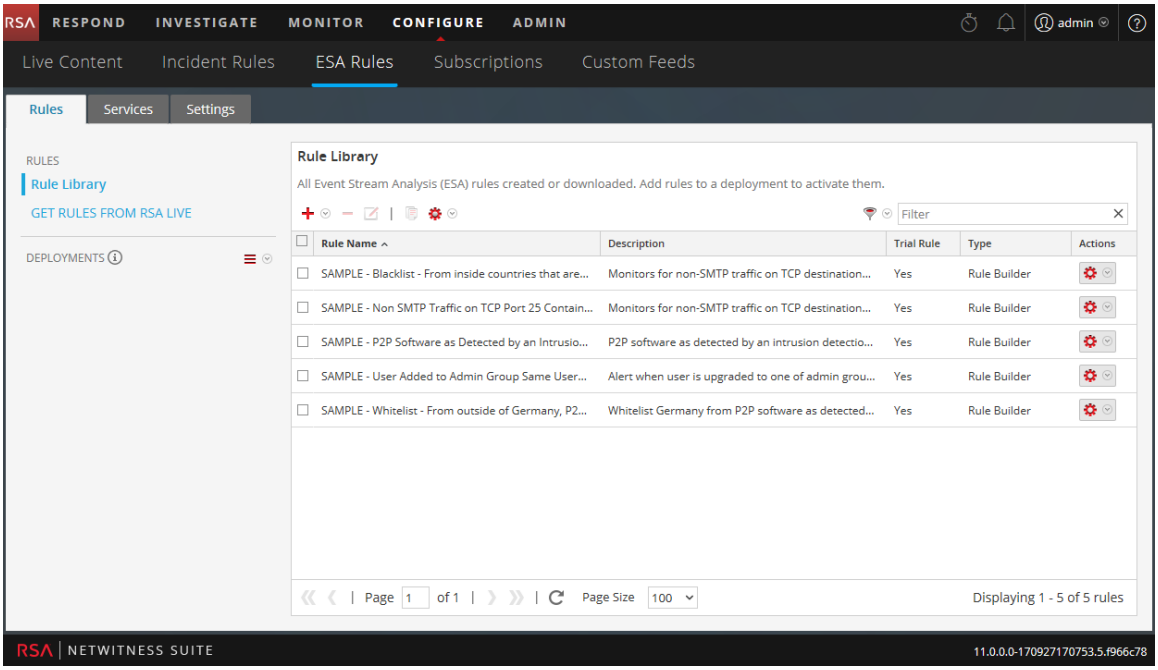


3. Geben Sie im Feld **Name** einen eindeutigen Namen für die duplizierte Regel ein und klicken Sie auf **OK**.

Dem Bereich Regelbibliothek wird eine duplizierte Regel mit dem neuen Namen hinzugefügt.

Löschen einer Regel

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
   Die Registerkarte „Regeln“ wird angezeigt.



2. Wählen Sie in der Regelbibliothek eine oder mehrere Regeln aus und klicken Sie auf .
   Ein Warnmeldungsdialogfeld wird angezeigt.
3. Klicken Sie auf **Yes**.

Es wird eine Bestätigungsmeldung angezeigt, dass die Regel erfolgreich gelöscht wurde, und die ausgewählte Regel wird aus der Regelbibliothek gelöscht.

Filtern oder Suchen von Regeln

In diesem Thema erfahren Analysten, wie sie den Typ von Regeln angeben, die in der Regelbibliothek angezeigt werden.

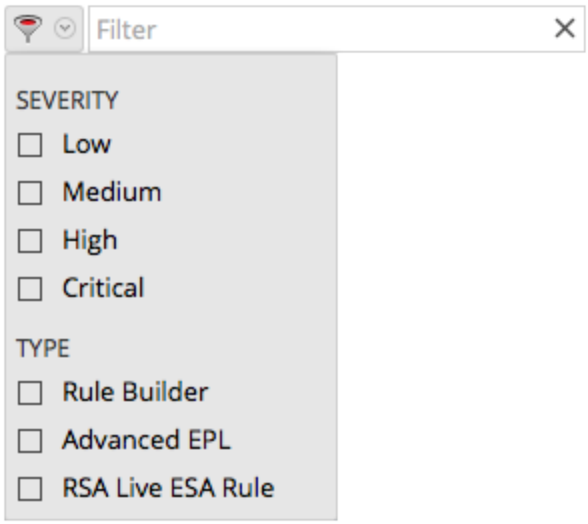
Voraussetzungen

Stellen Sie sicher, dass Sie mit den Komponenten der Ansicht „Regelbibliothek“ vertraut sind. Weitere Informationen erhalten Sie unter Bereich „Regelbibliothek“.

Methoden

Filter

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte „Regeln“ wird standardmäßig angezeigt.
2. Klicken Sie in der Symbolleiste des Bereichs **Regelbibliothek** auf  und wählen Sie den Schweregrad und die Regeltypen aus, die in der Liste der Regelbibliothek angezeigt werden sollen. Die folgende Abbildung zeigt die Drop-down-Liste „Filter“.



   Die ausgewählten Regeltypen werden in der Liste angezeigt.

Suchen

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte „Regeln“ wird standardmäßig angezeigt.

2. Geben Sie in der Symbolleiste des Bereichs **Regelbibliothek** im Feld „Filter“ einen Regelnamen ein.
   Im Bereich „Regelbibliothek“ werden die Regeln aufgelistet, die mit den ins Feld „Filter“ eingegebenen Namen übereinstimmen.

Importieren oder Exportieren von Regeln

In diesem Thema erfahren Sie, wie Sie ESA-Regeln aus einer NetWitness Suite-Instanz importieren und wie Sie ESA-Regeln auf Ihre Festplatte exportieren, damit Sie eine lokale Kopie anlegen können.

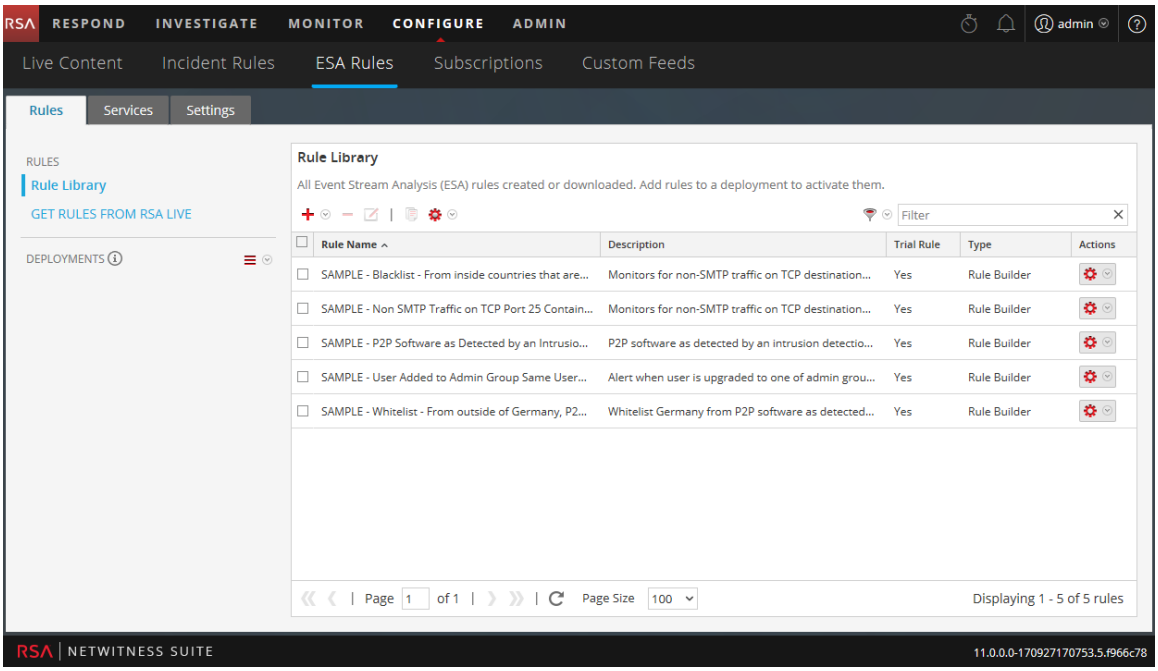
Wenn Sie eine Regel in einer früheren Version von NetWitness Suite exportiert haben, gelten beim Import der Regel in Version 10.5 oder höher die folgenden Bedingungen:

- Exportiert in Version 10.3: Die Regeln können nicht in Version 10.5 oder höher importiert werden.
- Exportiert in Version 10.4: Das Regelverhalten hängt davon ab, ob die übergreifende Korrelation deaktiviert (Standardeinstellung) oder aktiviert ist:
  - Deaktiviert: Sie können Regeln in Version 10.5 oder höher importieren.
  - Aktiviert: Sie müssen entweder NetWitness Suite neu starten oder eine kleinere Änderung an der Regel vornehmen, sie speichern, die Änderung wieder entfernen und sie erneut speichern. Mit beiden Verfahren wird die Weiterleitungsregel erstellt, die von der siteübergreifenden Korrelationsfunktion in 10.5 oder höher benötigt wird.

Methoden

Importieren von ESA-Regeln

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
   Die Registerkarte „Regeln“ wird angezeigt.



2. Klicken Sie in der Symbolleiste **Regelbibliothek** auf > **Importieren**.
   Das Dialogfeld „ESA-Regeln importieren“ wird angezeigt.

3. Klicken Sie auf **Durchsuchen**, um die Datei zu suchen und auszuwählen, die die ESA-Regeln enthält.
4. Klicken Sie auf **Importieren**.

Exportieren

1. Wählen Sie eine oder mehrere ESA-Regeln aus und klicken Sie in der Symbolleiste „Regelbibliothek“ auf > **Exportieren**.
   Ein Warnmeldungsdialogfeld wird angezeigt.
2. Klicken Sie auf **Yes**.
   Das Dialogfeld „Regeln exportieren“ wird angezeigt.
3. Geben Sie im Feld **Dateiname:** einen Dateinamen für die Datei mit den ESA-Regeln ein und klicken Sie auf **Exportieren**.
   .Die Datei wird als Binärdatei auf Ihren Rechner exportiert.

Hinweis: Die Binärdatei kann nicht bearbeitet werden.

Auswählen von Benachrichtigungsmethoden über Warnmeldungen

In diesem Thema werden die verschiedenen Benachrichtigungsmethoden beschrieben und wie Sie eine Benachrichtigungsmethode zu einer Regel hinzufügen. Für alle Aufgaben in diesem Abschnitt sind die Berechtigungen der Rollen Administrator, SOC Manager oder DPO erforderlich.

Wenn eine Regel eine Warnmeldung auslöst, kann ESA eine Benachrichtigung auf die folgenden Weisen senden:

- E-Mail
- SNMP
- Syslog
- Skript

Zur Konfiguration einer Benachrichtigung müssen Sie die folgenden Komponenten konfigurieren:

- Benachrichtigungsserver – Nachdem Sie einen Benachrichtigungsserver konfiguriert haben, können Sie ihn einer Regel hinzufügen. Wenn die Regel eine Warnmeldung auslöst, wird die Regel diesen Server verwenden, um Warnmeldungsbenachrichtigungen zu senden.
- Benachrichtigungen – Diese sind die Ausgaben, sie können in den Formaten E-Mail, Skript, SNMP und Syslog erfolgen. Wenn Sie eine Regel konzipieren, können Sie die Benachrichtigung für eine Warnmeldung angeben.
- Vorlagen – Das Format einer Warnmeldungsbenachrichtigung wird in einer Vorlage definiert.

Die Unterdrückung von Warnmeldungen und die Regulierung der Warnmeldungsrate sind zwei Funktionen von Event Stream Analysis. Die Unterdrückung von Warnmeldungen sorgt dafür, dass nicht mehrere E-Mail-Nachrichten zu derselben Warnmeldung gesendet werden. Betrachten Sie zum Beispiel eine Regel, um fehlgeschlagene Benutzeranmeldungen zu erkennen. Wenn Sie die Unterdrückung von Warnmeldungen auf drei Minuten festlegen, werden nur die für diesen Zeitrahmen erzeugten Warnmeldungen angezeigt. Das ist weniger als die Anzahl der Warnmeldungen, die Sie ohne Unterdrückung von Warnmeldungen sehen würden. Einige Warnmeldungen können Duplikate sein. Mit der Unterdrückung von Warnmeldungen werden keine E-Mails für Duplikat-Warnmeldungen gesendet. So sorgen Sie dafür, dass Ihr Posteingang nicht mit redundanten Warnmeldungsbenachrichtigungen überflutet wird.

Die Regulierung der Warnmeldungsrate ist eine vorbeugende Maßnahme, die dafür sorgt, dass Warnmeldungen von fehlgedeuteten Regeln nicht das System überschwemmen. Diese Funktion sorgt dafür, dass ESA nicht mehr als die konfigurierte maximale Anzahl von E-Mail-Nachrichten innerhalb einer Minute sendet.

Benachrichtigungsserver, Benachrichtigungen und Vorlagen werden in der Ansicht Administration > System konfiguriert. Weitere Informationen finden Sie unter „Konfigurieren von Benachrichtigungsservern“, „Konfigurieren von Benachrichtigungstypen“ und „Konfigurieren von Vorlagen für Benachrichtigungen“ im *Systemkonfigurationsleitfaden*.

Benachrichtigungsmethoden

Wenn eine Regel eine Warnmeldung auslöst, kann ESA eine Benachrichtigung auf die folgenden Weisen senden:

- E-Mail
- SNMP
- Syslog
- Skript

E-Mail-Benachrichtigungen

Event Stream Analysis kann Benachrichtigungen über verschiedene Systemereignisse per E-Mail an Benutzer senden.

Um diese E-Mail-Benachrichtigungen zu konfigurieren, müssen Sie Folgendes tun:

- Konfigurieren Sie den SMTP-E-Mail-Server als einen Ausgabeprovider. Weitere Anweisungen finden Sie unter „Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver“ im *Systemkonfigurationsleitfaden*.
- Richten Sie ein E-Mail-Konto für den Erhalt von Benachrichtigungen ein. Weitere Anweisungen finden Sie unter „Konfigurieren von E-Mail als Benachrichtigung“ im *Systemkonfigurationsleitfaden*.
- Konfigurieren Sie eine Vorlage für die E-Mail-Benachrichtigung. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im *Systemkonfigurationsleitfaden*.

SNMP

Event Stream Analysis kann Ereignisse als eine SNMP-Trap an einen konfigurierten SNMP-Trap-Host senden.

Hinweis:
Die MIB-Datei **NETWITNESS-MIB.txt** befindet sich auf dem ESA-RPM am folgenden Speicherort: */usr/share/snmp/mibs*. Mit der MIB-Datei können Sie die von ESA ausgelösten SNMP-Warnmeldungen identifizieren. Und der Trap-OID-Wert für ESA ist 20.

Um diese SNMP-Benachrichtigungen zu konfigurieren, müssen Sie Folgendes tun:

- Konfigurieren Sie die Einstellungen des SNMP-Trap-Host als Ausgabeprovider. Weitere Anweisungen finden Sie unter „Konfigurieren der SNMP-Einstellungen als Benachrichtigungsserver“ im *Systemkonfigurationsleitfaden*.
- Konfigurieren Sie die Einstellungen der SNMP-Trap als Ausgabeaktion. Weitere Anweisungen finden Sie unter „Konfigurieren von SNMP als eine Benachrichtigung“ im *Systemkonfigurationsleitfaden*.
- Konfigurieren Sie eine Vorlage für SNMP. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im *Systemkonfigurationsleitfaden*.

Syslog

Event Stream Analysis kann Ereignisse versenden und Protokolle im Syslog-Format auf einem Syslog-Server konsolidieren.

Um diese Syslog-Benachrichtigungen zu konfigurieren, müssen Sie Folgendes tun:

- Konfigurieren Sie die Syslog-Servereinstellungen als Ausgabeprovider. Weitere Anweisungen finden Sie unter „Konfigurieren der Syslog-Einstellungen als Benachrichtigungsserver“ im *Systemkonfigurationsleitfaden*.
- Konfigurieren Sie das Syslog-Nachrichtenformat als eine Ausgabeaktion. Weitere Anweisungen finden Sie unter „Konfigurieren von Syslog als Benachrichtigung“ im *Systemkonfigurationsleitfaden*.
- Konfigurieren Sie eine Vorlage für Syslog. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im *Systemkonfigurationsleitfaden*.

Script Alerter

Neben den Warnmeldungen ermöglicht ESA den Benutzern auch, als Reaktion auf ESA-Warnmeldungen Skripte auszuführen.

Mithilfe von Skripten können Sie eine benutzerdefinierte Integration mit Anwendungen erreichen, die in Ihrer Umgebung existieren. Beispiel: Wenn Sie ein Incident-Ticket von einer Anwendung öffnen möchten, wenn eine bestimmte Warnmeldung ausgelöst wird, können Sie mit Script Alerter ein Skript erstellen, das die Anwendungs-API aufruft. ESA kann es dann einleiten, wenn die definierte ESA-Regel ausgelöst wird. Sie können eine FreeMarker-Vorlage konfigurieren, um die von der Ausgabe der ESA-Regel zu extrahierenden Details zu definieren und als Befehlszeilenargumente an das Skript weiterzugeben.

Gehen Sie wie folgt vor, um Script Alert zu verwenden:

- Konfigurieren Sie die Benutzeridentität und weitere Details, die für die Ausführung des Skripts notwendig sind. Weitere Anweisungen finden Sie unter „Konfigurieren eines Skripts als Benachrichtigungsserver“ im *Systemkonfigurationsleitfaden*.
- Definieren Sie das Skript. Weitere Anweisungen finden Sie unter „Konfigurieren eines Skripts als eine Benachrichtigung“ im *Systemkonfigurationsleitfaden*.
- Konfigurieren Sie eine Vorlage für das Skript. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im *Systemkonfigurationsleitfaden*.

Hinzufügen einer Benachrichtigungsmethode zu einer Regel

Dieses Thema erklärt Administratoren, wie sie eine Benachrichtigung, etwa als E-Mail, zu einer Regel hinzufügen können. ESA verwendet die Benachrichtigungsmethode, wenn es eine Warnmeldung für ein Ereignis erzeugt, das die Regelkriterien erfüllt.

Fügen Sie eine Benachrichtigung zu einer Regel hinzu, kann ESA Sie informieren, wenn eine Regel eine Warnmeldung auslöst. Obwohl die Benachrichtigungsfelder nicht erforderlich sind, ist es eine bewährte Vorgehensweise, eine Benachrichtigung zu einer Regel hinzuzufügen.

Wenn Sie eine Benachrichtigungsmethode zu einer Regel hinzufügen, wählen Sie die folgenden Informationen aus:

- Ausgabe
- Benachrichtigung
- Benachrichtigungsserver
- Vorlage

Voraussetzungen

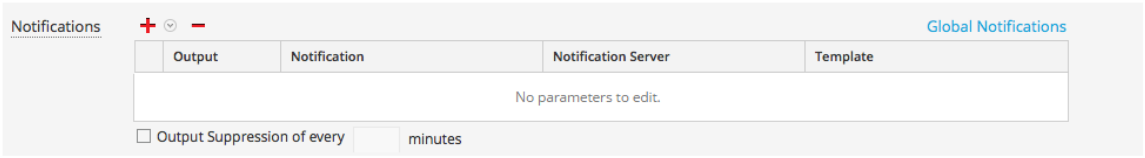
- Ihre Rolle muss die Berechtigung zum Managen von Regeln haben.
- Die Regel muss vorhanden sein.

- Die Benachrichtigungsmethode muss mit einem unterstützten Server und einer Vorlagekonfiguriert sein:
  Navigieren Sie zu **ADMIN** > **System > Globale Benachrichtigungen**.
  Detaillierte Informationen über die Verfahren finden Sie im *Systemkonfigurationsleitfaden*.

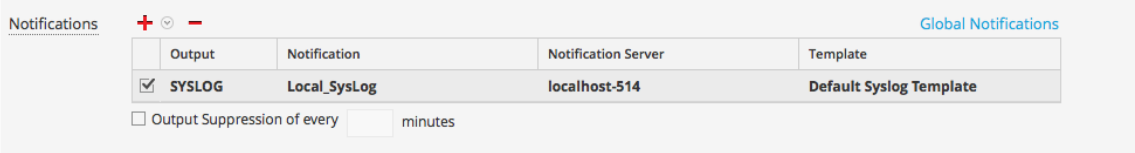
Verfahren

So fügen Sie einer Regel eine Benachrichtigungsmethode hinzu:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
2. Klicken Sie in der **Regelbibliothek** auf  , um eine neue Regel hinzufügen oder eine vorhandene Regel auszuwählen, und klicken Sie dann auf  .
   Je nach Regeltyp wird die Registerkarte „Regelerstellung“ oder „Erweiterte EPL“ angezeigt.
   Der Abschnitt „Benachrichtigungen“ ist für beide Registerkarten gleich.



3. Klicken Sie auf  und wählen Sie die **Ausgabe** für die Warnmeldung aus:
   - E-Mail
   - SNMP
   - Syslog
   - Skript
4. Doppelklicken Sie auf das Feld **Benachrichtigung** und wählen Sie den Namen einer vorher konfigurierten Ausgabe.
   Zum Beispiel könnte „Level 1 Analyst“ der Name einer E-Mail-Benachrichtigung sein, die an die Verteilergruppe „L1-Analysten“ gesendet wird.
5. Doppelklicken Sie auf das Feld **Benachrichtigungsserver** und wählen Sie den Server aus, der die Benachrichtigung versendet.
6. Doppelklicken Sie auf das Feld **Vorlage** und wählen Sie ein Format für die Warnmeldung aus.
   Die folgende Abbildung zeigt die Einstellungen für eine Syslog-Benachrichtigung:

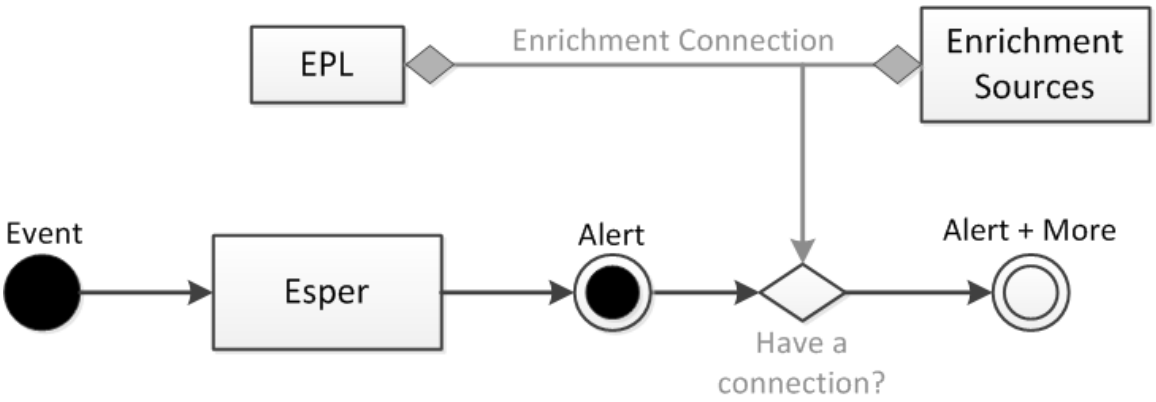


7. Wenn Sie die Frequenz angeben möchten, wählen Sie **Ausgabeunterdrückung** aus und geben Sie dann die Anzahl **Minuten** ein.
8. Wenn Sie eine weitere Benachrichtigung hinzufügen möchten, wiederholen Sie die Schritte 3 bis 7.
9. Klicken Sie auf **Speichern**.
   Wenn ESA eine Warnmeldung für ein Ereignis erzeugt, das die Regelkriterien erfüllt, werden Sie über die Warnmeldung über jede Benachrichtigungsmethode informiert, die zu der Regel hinzugefügt wurde.

Hinzufügen einer Datenerweiterungsquelle

In diesem Thema wird erläutert, wie eine zuvor konfigurierte Erweiterungsquelle zu einer Regel hinzugefügt wird. Wenn ESA eine Warnmeldung erstellt, werden die Informationen aus dieser Quelle einbezogen.

Mit Erweiterungen können Kontextinformationen in Korrelationslogiken und Warnmeldungsausgaben integriert werden. Ohne Erweiterungen stammen alle in einer ESA-Warnmeldung enthaltenen Informationen aus einem Core-Service. Mit Erweiterungen können Sie Suchvorgänge in einer Vielzahl von Quellen anfordern und die Ergebnisse in die ausgehenden Warnmeldungen integrieren. In der folgenden Abbildung ist die Erweiterungsfunktion dargestellt.



Eine Erweiterungskonfiguration besteht aus zwei logischen Einheiten:

- Erweiterungsquellen: Diese Quellen sind Datenspeicher für Kontextinformationen.
- Erweiterungsverbindungen: Diese agieren als Verbindungselemente zwischen den Warnmeldungsmetadaten und den Quellspalten.

In ESA können Sie Verbindungen zwischen EPL-Anweisungen (Event Processing Language, Ereignisverarbeitungssprache) und Erweiterungsquellen herstellen. Sobald die Verbindungen hergestellt wurden, verbindet das System die ausgewählten Felder aus der Warnmeldungsausgabe mit den Informationen der Quellen und füllt die gesendete Warnmeldung mit den übereinstimmenden Daten. ESA kann Verbindungen mit folgenden Quellen herstellen:

- Esper-Named-Windows
- Relationale Datenbanktabellen
- MaxMindGeoIP-Datenbank
- RSA Warehouse Analytics-Watchlisten

Hinweis: Die Erweiterungsquelle GeoIP kann weder erstellt noch gelöscht werden. Sie wird dem Benutzer vorkonfiguriert bereitgestellt.

Beispielregel mit Erweiterung

In der folgenden Beispielregel wird die von ESA bereitgestellte Erweiterungsfunktion illustriert:

```
@RSAAlert @Name("simple") SELECT * FROM CoreEvent(ec_theme='Login Failure')
```

Die Regel erzeugt eine Warnmeldung für jede fehlgeschlagene Anmeldung und meldet somit, ob der folgende (vereinfachte) Ereignisstream von ESA empfangen wird:

sessionid	ec_theme	username	ip_src	ip_dst	host_dst
1	Login Success	dshrute	23.xx.23x.16		
2	Login Failure	jhalpert	23.xx.23x.16	31.1x.x9.1x8	www.facebook.com

Eine Warnmeldung mit dem folgenden Bestandteil `events` wird möglicherweise als Reaktion auf die zweite Sitzung erzeugt:

```
{
     "events": [
         {
             "username": "jhalpert",
             "host_dst": "www.facebook.com",
             "ip_dst": "31.1x.x9.1x8",
             "sessionid": 2,
             "ec_theme": "Login Failure",
             "esa_time": 1406148964130,
             "ip_src": "23.xx.23x.16"
         }
     ]
 }
```

Die JSON-Ausgabe zeigt alle verfügbaren Informationen für die Integration in eine ESA-Benachrichtigung mit einer entsprechenden FreeMarker
-Vorlage an. Der Vorlagenausdruck `${events[0].username}` wird beispielsweise mit `jhalpert` erfüllt.

Mit Erweiterungen kann dasselbe Modul mit demselben Ereignisstream die unten stehende Warnmeldung erzeugen. Das System
kann mehrere Erweiterungsverbindungen herstellen und Kontextdaten abrufen, damit die Warnmeldung aussagekräftiger wird.

Zum Beispiel:
`${events[0]["RSADataScienceLookup"][0].score}` ergibt eine **Risikobewertung** der Zieldomain, die vom RSA Warehouse Analytics-Modul berechnet wird. `${events[0]["orgchart"][0].supervisor}` ergibt den Namen des Supervisors des Mitarbeiters, auf den sich die Warnmeldung bezieht (aus einer HR-Datenbank abgerufen). `${events[0]["LoginRegister"][0].username}` ergibt den Namen des Benutzers, der sich zuletzt erfolgreich mit derselben `ip_src` (mit einem Stream-basierten benannten Fenster) angemeldet hat.


```
{"events": [
     {
         "username": "jhalpert",
         "host_dst": "www.facebook.com",
         "GeoIpLookup": [
         {
             "city": "Cambridge",
             "longitude": -71,
             "countryCode": "US",
             "areaCode": 617,
             "metroCode": 506,
             "region": "MA",
             "dmaCode": 506,
             "ipv4Obj": "/23.62.236.16",
             "countryName": "United States",
             "postalCode": "02142",
             "ipv4": "23.62.236.16",
             "latitude": 42,
             "organization": "Verizon Business"
         }
     ],
     "RSADataScienceLookup": [
         {
             "model_id": "suspiciousDomains_1",
             "_id": "EXEC_BATCH_1_20140630153740_facebook.com",
             "score": 10,
             "key": "www.facebook.com"
         }
     ],
     "orgchart": [
         {
             "supervisor": "mscott",
             "name": "James Halpert",
             "extension": 3692,
             "location": "Scranton",
```

```
            "department": "Sales",
            "id": "jhalpert"
        }
    ],
    "ip_dst": "31.13.69.128",
    "sessionid": 2,
    "LoginRegister": [
        {
            "username": "dshrute",
            "ip_src": "23.62.236.16"
        }
    ],
    "ec_theme": "Login Failure",
    "esa_time": 1406155218912,
    "ip_src": "23.62.236.16"
    }
]}
```


Konfigurieren einer Datenbankverbindung

In diesem Thema wird erläutert, wie eine Verbindung zu einer externen Datenbank konfiguriert wird, in der zusätzliche Informationen für Warnmeldungen bereitgestellt werden können. Sie konfigurieren eine Datenbankverbindung, sodass Sie anschließend die Datenbank als Erweiterungsquelle konfigurieren können, um Warnmeldungen weitere Details hinzuzufügen. Dieser Prozess besteht aus drei Schritten:

1. Konfigurieren Sie eine Verbindung zu einer Datenbank.
2. Konfigurieren Sie die externe Datenbank als Erweiterungsquelle.
3. Fügen Sie die Erweiterungsquelle zu einer Regel hinzu

In diesem Thema wird Schritt 1 erläutert.

Beispiel

Dieses Beispiel veranschaulicht, wie durch Hinzufügen einer Datenbank als Erweiterungsquelle ein Wert zu Warnmeldungen hinzugefügt wird.

Eine Regel erkennt Benutzer, die versuchen, sich bei einem im Hintergrund aktiven E-Mail-Service anzumelden. Die Regelkriterien treffen auf 25 Benutzer zu. Ohne die Erweiterung enthält die Warnmeldung 25 Benutzer-IDs. Mit der Erweiterung enthält die Warnmeldung auch die folgenden Informationen zu den einzelnen Benutzer-IDs:

- Name
- Bezeichnung

- Abteilung
- Niederlassung

Abhängigkeiten

Wenn Sie eine Datenbank konfigurieren, gelten folgende Bedingungen:

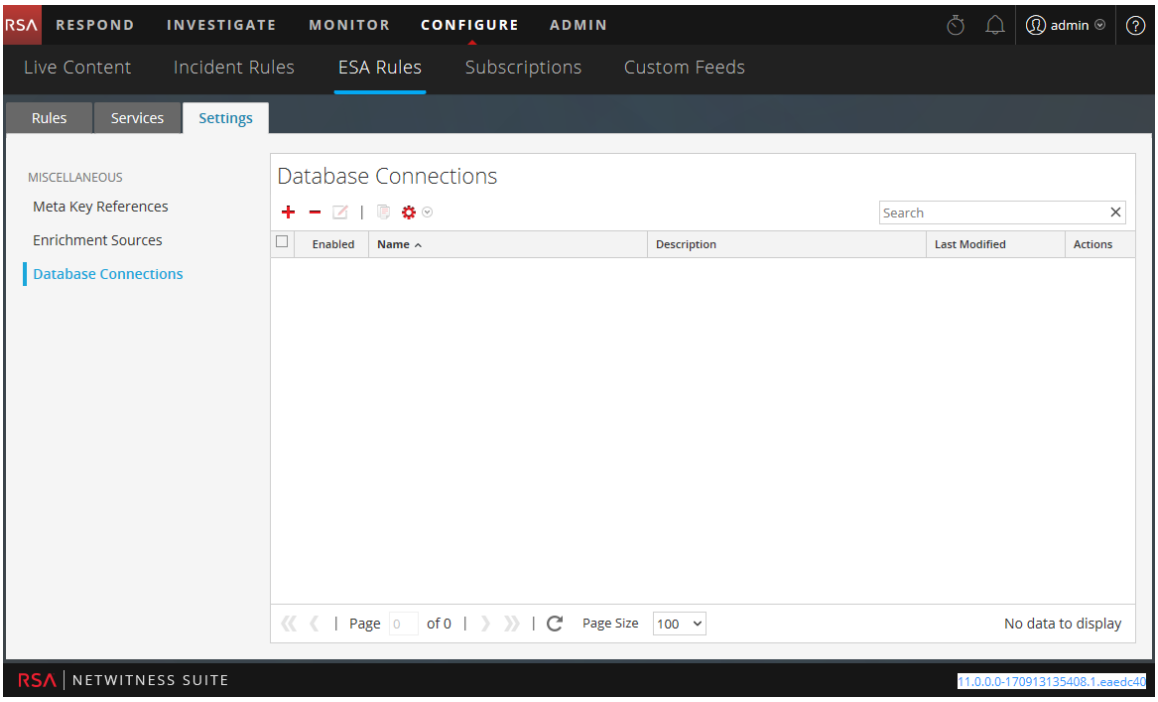
- Auf jedem ESA wird ein Verweis zu der Datenbank bereitgestellt, selbst wenn der ESA keine Regeln bereitstellt, die die Datenbank als Erweiterungsquelle verwenden.
- Wenn der Server, auf dem die Datenbank gehostet wird, ausfällt, hat dies Auswirkungen auf eine Bereitstellung.
  - Eine aktive Bereitstellung erfasst weiterhin Daten und führt Regeln aus, aber in den Warnmeldungen werden keine Erweiterungen angezeigt.
  - Eine neue Bereitstellung schlägt solange fehl, bis Sie den Host neu starten.

Verfahren

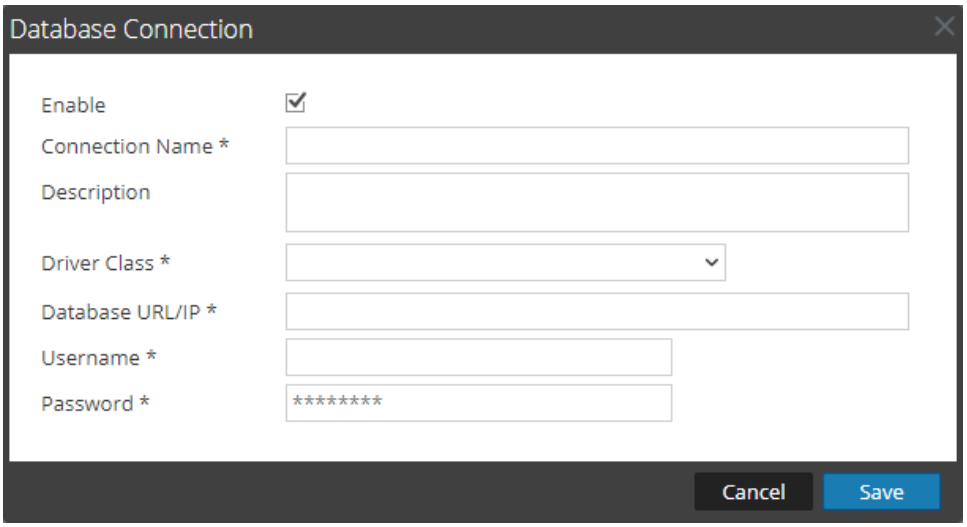
So konfigurieren Sie eine Datenbankverbindung:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie im Bereich „Optionen“ die Option **Datenbankverbindungen** aus.

   Der Bereich „Datenbankverbindungen“ wird angezeigt.



4. Klicken Sie auf +, um eine Datenbankverbindung hinzuzufügen.



5. Geben Sie im Dialogfeld **Datenbankverbindung** die folgenden Informationen an.

Feld	Beschreibung
Aktivieren	Wählen Sie Aktivieren aus, um die Warnmeldung um zusätzliche Daten zu erweitern. Standardmäßig ist „Aktiviert“ ausgewählt. Deaktivieren Sie „Aktiviert“, um zusätzliche Daten aus der Warnmeldung auszuschließen.

Feld	Beschreibung
Verbindungsname	Geben Sie einen Namen ein, um die Verbindung zu identifizieren. Wenn Sie eine Datenbank als Erweiterungsquelle hinzufügen, wird dieser Name in der Liste der Datenbankverbindungen angezeigt.
Beschreibung	(Optional) Geben Sie eine kurze Beschreibung der Datenbankverbindung ein.
Treiberklasse	Wählen Sie eine geeignete Treiberklasse für die Datenbank aus. In NetWitness Suite sind zwei Treiber enthalten: MongoDB und Postgres.
Datenbank-URL oder IP-Adresse	Geben Sie die URL oder die IP-Adresse der zu konfigurierenden Datenbank ein.
Benutzername	Geben Sie den Benutzernamen für den Zugriff auf die Datenbank ein.
Password	Geben Sie das Passwort für den Zugriff auf die Datenbank ein.

6. Klicken Sie auf **Speichern**.

Weitere Informationen erhalten Sie unter Registerkarte „Einstellungen“.

Erweiterungsquellen

In diesem Thema werden Optionen zum Hinzufügen einer externen Datenquelle für zusätzliche Informationen in Warnmeldungen erklärt. Enrichment-Quellen bieten zusätzliche Information in Warnmeldungen. Beispiel: Eine Datenbank kann Informationen zu Name, Abteilung und Bürostandort bereitstellen, wenn ein Benutzer Regelbedingungen erfüllt. Es gibt drei Typen von Enrichment-Quellen:

- Externer DB-Verweis
- In-Memory-Tabelle
- Warehouse Analytics

Konfigurieren einer Datenbank als Erweiterungsquelle

Sie können eine Datenbank als Erweiterungsquelle konfigurieren, damit Sie sie einer Regel hinzufügen können. Die Esper-Engine, die die Ereignisse analysiert, kann auf die Informationen in der Datenbank zugreifen und in der Warnmeldung zusätzliche Angaben bereitstellen.

Beispiel: Eine Regel erkennt, dass Benutzer versuchen, sich bei einem Tarnkappen-E-Mail-Service anzumelden. Die Regelkriterien treffen auf 25 Benutzer zu. Die Warnmeldung enthält 25 Benutzer-IDs. In diesem Beispiel erweitert eine externe Datenbank die Warnmeldung um die folgenden zusätzlichen Informationen für jede Benutzer-ID:

- Name
- Bezeichnung
- Abteilung
- Niederlassung
- Vorgesetzte

Sie können eine Datenbankverbindung bearbeiten, duplizieren, importieren oder exportieren.

Voraussetzungen

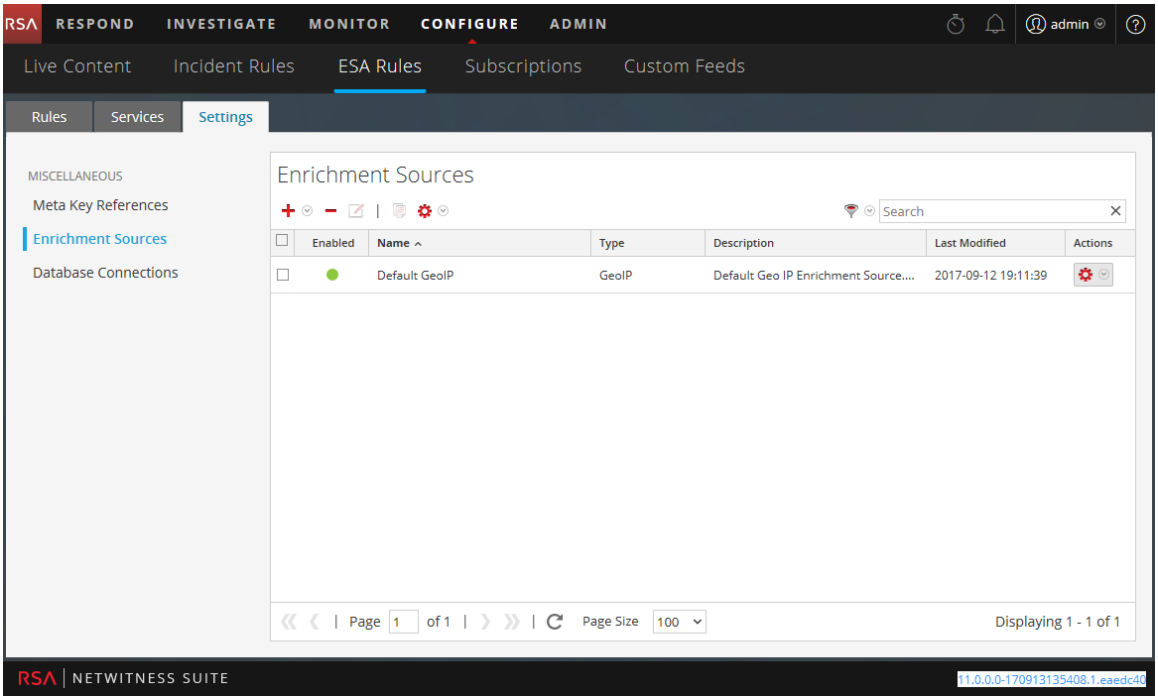
Sie müssen eine Datenbankverbindung konfigurieren. Weitere Informationen finden Sie unter Konfigurieren einer Datenbankverbindung.

Verfahren

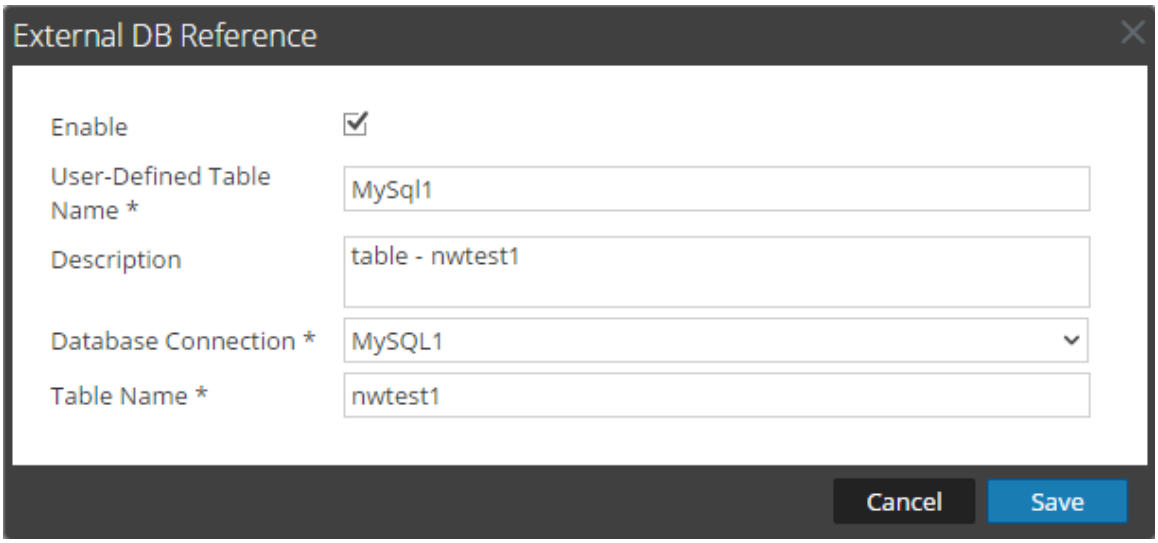
So konfigurieren Sie eine Datenbank als Erweiterungsquelle

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
   Die Registerkarte Einstellungen wird angezeigt.

3. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.
   Der Bereich „Erweiterungsquellen“ wird angezeigt.



4. Wählen Sie aus dem  -Drop-down-Menü **Externer DB-Verweis** aus. Sie müssen einen Datenbankverweis hinzufügen, damit die Datenbank aufgelistet werden kann.
   Das Dialogfeld „Externer DB-Verweis“ wird angezeigt.



5. Wählen Sie **Aktivieren** aus, um die Warnmeldung um zusätzliche Daten zu erweitern. Diese Option ist standardmäßig aktiviert. Wenn sie deaktiviert ist, wird die Warnmeldung nicht um zusätzliche Daten erweitert.

6. Geben Sie im Feld **Benutzerdefinierter Tabellenname** einen Namen ein, um die Datenbankkonfiguration zu identifizieren oder zu bezeichnen.
7. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung der Datenbankkonfiguration ein.
8. Wählen Sie im Drop-down-Menü **Datenbankverbindung** die definierten Datenbankverbindungen aus.
9. Geben Sie in das Feld **Name der Tabelle** den Tabellennamen der Datenbank ein.
10. Klicken Sie auf **Speichern**.

Weitere Informationen über Parameter und ihre Beschreibung erhalten Sie unter Registerkarte „Einstellungen“.

Konfigurieren einer In-Memory-Tabelle als Erweiterungsquelle

Dieses Thema bietet Anweisungen zum Konfigurieren einer In-Memory-Tabelle. Wenn Sie eine In-Memory-Tabelle konfigurieren, laden Sie eine CSV-Datei als Eingabe in die Tabelle hoch. Sie können diese Tabelle einer Regel als Erweiterungsquelle zuordnen. Wenn die zugeordnete Regel eine Warnmeldung erzeugt, erweitert ESA die Warnmeldung um relevante Informationen aus der In-Memory-Tabelle.

Beispiel: Eine Regel könnte dazu konfiguriert sein, zu erkennen, wenn ein Benutzer versucht, Freeware herunterzuladen, und die Person anhand der Benutzer-ID in der Warnmeldung zu identifizieren. Die Warnmeldung könnte um zusätzliche Informationen aus einer In-Memory-Tabelle erweitert werden, die Details wie vollständigen Namen, Titel, Bürostandort und Mitarbeiternummer enthält.

Eine In-Memory-Tabelle eignet sich hervorragend für den Umgang mit kleinen Datenmengen. Sie lässt sich leicht einrichten und erfordert weniger Wartungsaufwand als eine Datenbank. Beispiel: Die Firma AllTech ist ein kleines Unternehmen, daher kann der Systemadministrator die Mitarbeiterinformationen in einer .CSV-Datei verwalten. Würde sich AllTech zu einem großen Unternehmen entwickeln, müsste der Administrator eine externe Datenbankreferenz zur Erweiterung konfigurieren und die Datenbank mit einer Regel verknüpfen.

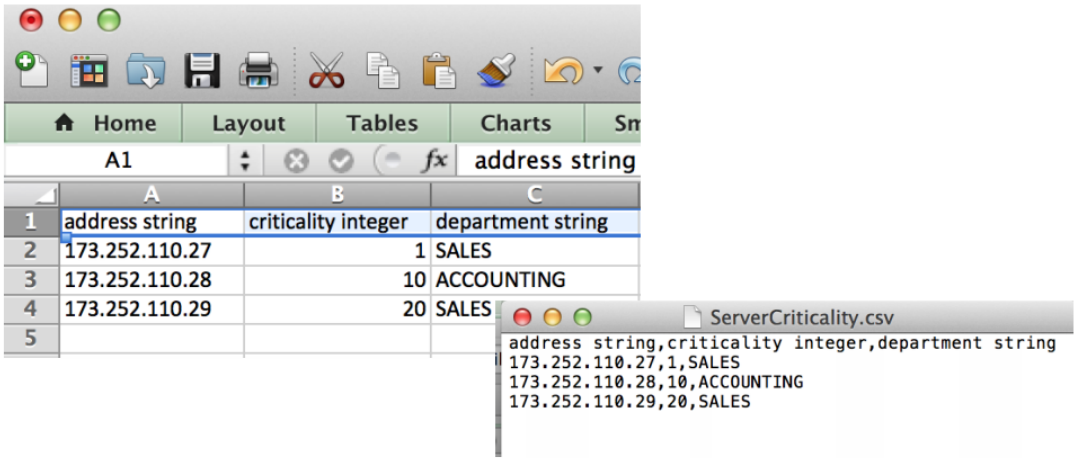
Voraussetzungen

Der Spaltenname in der CSV-Datei darf keine Leerzeichen enthalten.

Beispielsweise ist *Zeichenfolge_Adresse* korrekt und *Zeichenfolge Adresse* falsch.

Die CSV-Datei muss mit einer Kopfzeile beginnen, die Felder und Datentypen definiert. Beispielsweise würde *Adresszeichenfolge* das Kopfzeilenfeld als *Adresse* definieren und den Typ als *Zeichenfolge*.

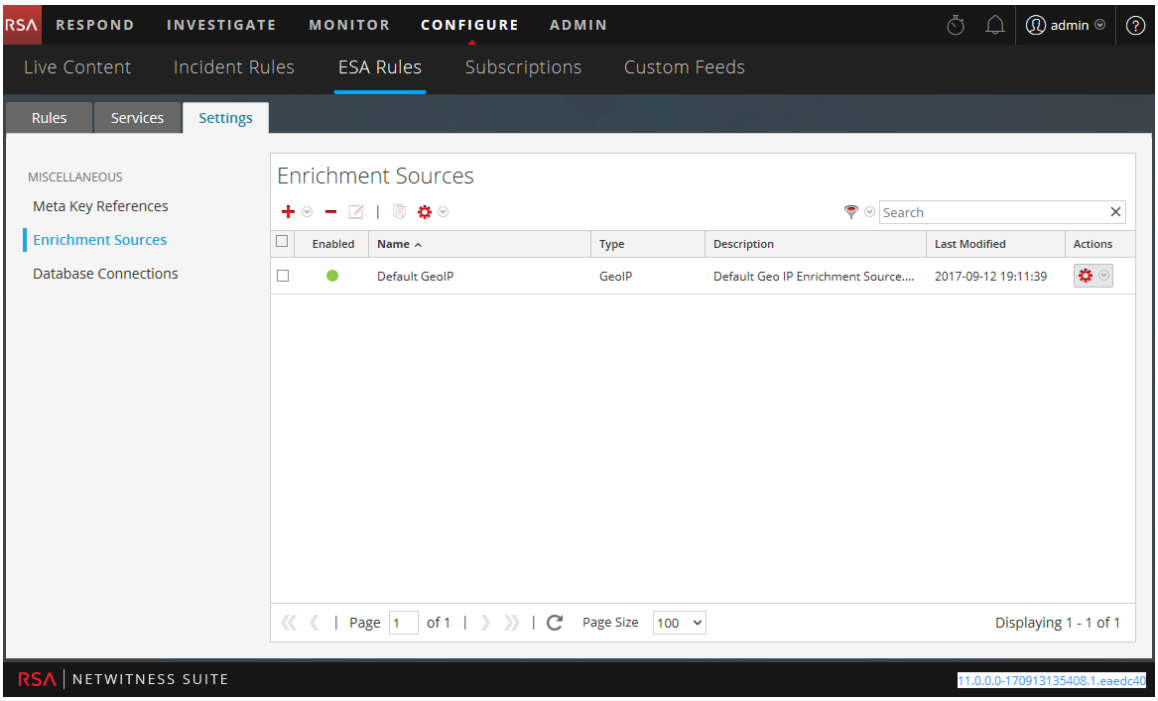
Die folgende Abbildung zeigt eine gültige CSV-Datei, die als .CSV und als Tabelle dargestellt wird.



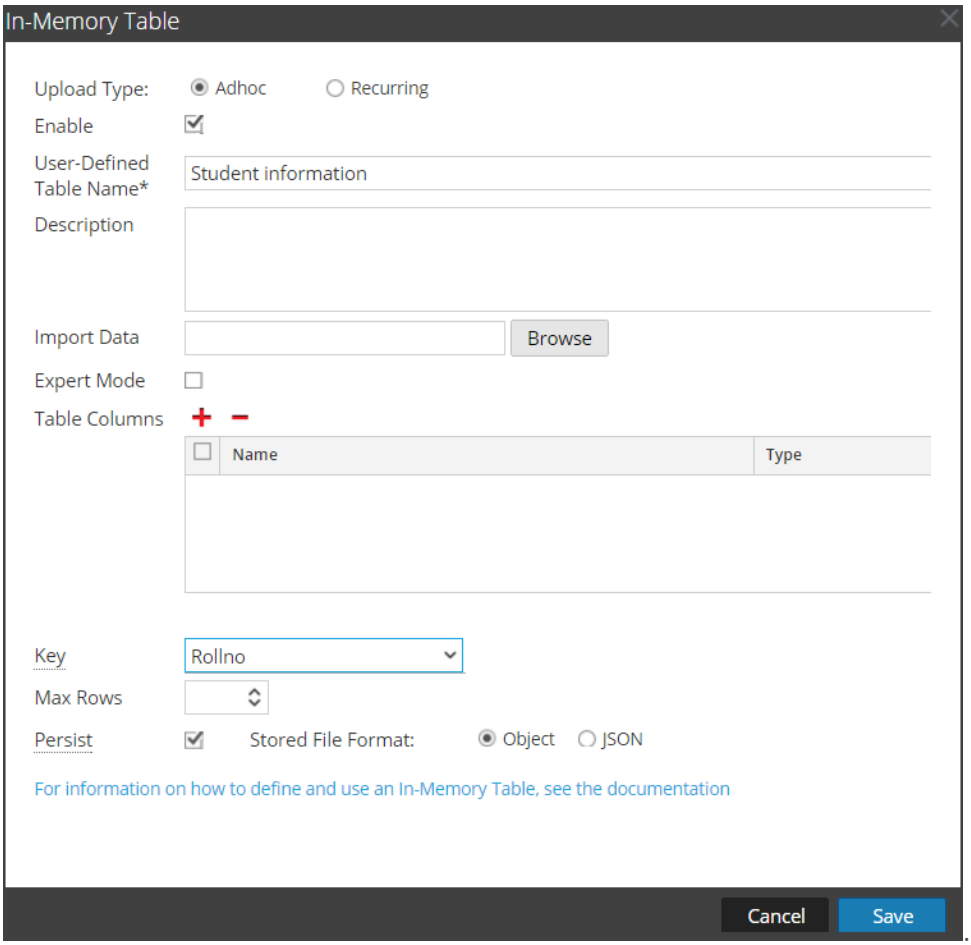
Methoden

Konfigurieren einer Ad-hoc-In-Memory-Tabelle

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Ansicht „Konfigurieren“ wird mit geöffneter Registerkarte „ESA-Regeln“ angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.



4. Klicken Sie im Abschnitt **Erweiterungsquellen** auf + > In-Memory-Tabelle



5. Beschreiben Sie die In-Memory-Tabelle:

   a. Wählen Sie **Ad-hoc**.

   b. Standardmäßig ist **Aktiviert** ausgewählt. Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, werden Warnmeldungen mit den Daten aus der Tabelle erweitert.
   Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, die Warnmeldungen aber nicht erweitert werden sollen, deaktivieren Sie das Kontrollkästchen.

   c. Geben Sie im Feld **Benutzerdefinierter Tabellenname** einen Namen für die Konfiguration der In-Memory-Tabelle ein, zum Beispiel „Studenteninformationen“.

   d. Wenn Sie erläutern möchten, welche Informationen die Erweiterung zu einer Warnmeldung hinzufügt, geben Sie eine **Beschreibung** ein, wie z. B.:
   Wenn eine Warnmeldung nach „Rollno“ gruppiert ist, fügt diese Erweiterung Studenteninformationen hinzu, z. B. Name und Markierungen.

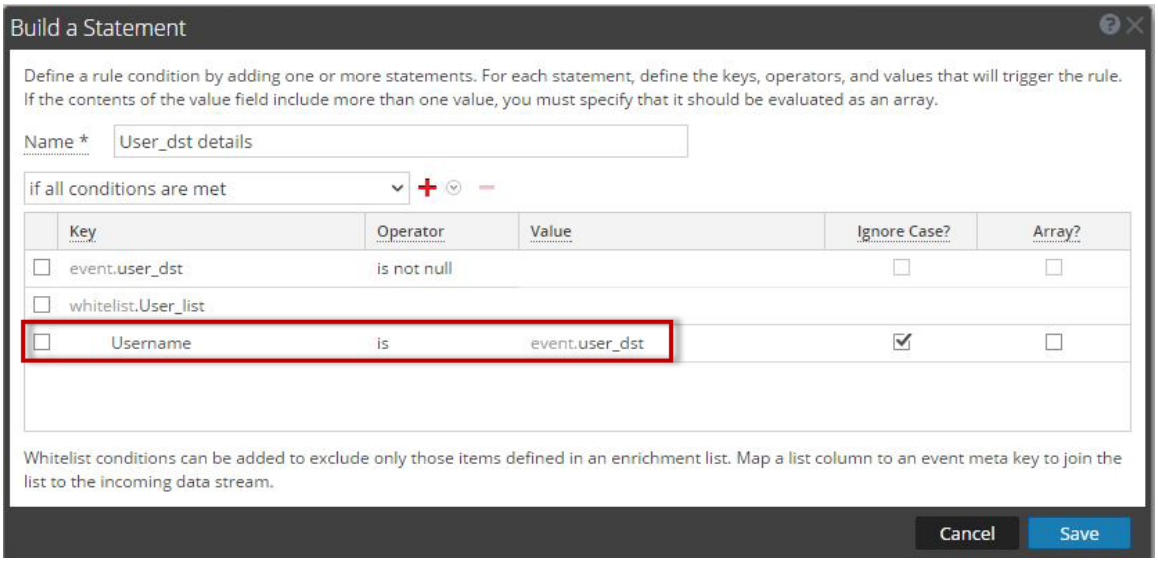
6. Wählen Sie im Feld **Daten importieren** die CSV-Datei aus, aus der Daten in die In-Memory-Tabelle übertragen werden.
7. Wenn Sie eine EPL-Abfrage schreiben möchten, um eine erweiterte Konfiguration für eine In-Memory-Tabelle zu definieren, wählen Sie **Expertenmodus** aus.
   Der Abschnitt „Tabellenspalten“ wird durch ein Feld **Abfrage** ersetzt.
8. Klicken Sie im Abschnitt **Tabellenspalten** auf  , um Spalten zur In-Memory-Tabelle hinzuzufügen.
9. Wenn Sie im Feld „Daten importieren“ eine gültige Datei ausgewählt haben, werden die Spalten automatisch ausgefüllt.

Hinweis: Wenn Sie den Expertenmodus ausgewählt haben, wird anstelle des Abschnitts „Tabellenspalten“ das Feld „Abfrage“ angezeigt.

10. Wählen Sie bei Verwendung einer CSV-basierten In-Memory-Tabelle als Erweiterung im Drop-down-Menü **Schlüssel** das Feld aus, das als Standardschlüssel verwendet werden soll, um eingehende Ereignisse mit der In-Memory-Tabelle zu verbinden. Standardmäßig ist die erste Spalte ausgewählt. Sie können den Schlüssel auch später ändern, wenn Sie die In-Memory-Tabelle in Erweiterungsquellen öffnen.
11. Wählen Sie im Drop-down-Menü **Max. Zeilen** die maximale Anzahl der Zeilen aus, die eine bestimmte Instanz der In-Memory-Tabelle enthalten kann.
12. Wählen Sie **Fortbestehen** aus, um die In-Memory-Tabelle auf dem Datenträger beizubehalten, wenn der ESA-Service angehalten wird, und um die Tabelle wieder aufzufüllen, wenn der Service wieder gestartet wird.
13. Führen Sie im Feld **Format der gespeicherten Datei** eine der folgenden Optionen aus:
    - Wählen Sie **Objekt**, wenn Sie die Datei im binären Format speichern möchten.
    - Wählen Sie **JSON**, wenn Sie die Datei im Textformat speichern möchten.
      Standardmäßig ist **Objekt** ausgewählt.
14. Klicken Sie auf **Speichern**.
    Die Ad-hoc-In-Memory-Tabelle ist konfiguriert. Sie können sie der Regel als Erweiterung oder als Teil der Regelbedingung hinzufügen. Siehe Hinzufügen einer Erweiterung zu einer Regel.

Wenn Sie eine In-Memory-Tabelle hinzufügen, können Sie sie einer Regel als Erweiterung oder als Teil der Regelbedingung hinzufügen. Zum Beispiel verwendet die folgende Regel eine In-Memory-Tabelle als Teil der Regelbedingung zur Erstellung einer Whitelist und sie verwendet ebenfalls eine In-Memory-Tabelle mit Details in der Datei „user_dst“, um die Warnmeldung, die angezeigt wird, zu erweitern.

Die Regel zeigt die In-Memory-Tabelle als eine Whitelist-Regelbedingung an:



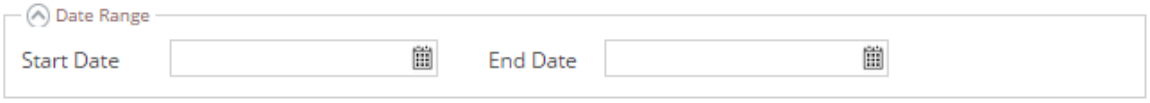
Als Nächstes wird die Warnmeldung um die In-Memory-Tabelle „User_list“ erweitert:

Aus diesem Grund wird die In-Memory-Tabelle „user_dst“ verwendet, um eine Whitelist zu erstellen, und sie wird auch verwendet, um die Daten in der Warnmeldung zu erweitern, wenn die Warnmeldung ausgelöst wird.

Hinzufügen einer wiederkehrenden In-Memory-Tabelle

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Ansicht „Konfigurieren“ wird mit geöffneter Registerkarte „ESA-Regeln“ angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.
4. Klicken Sie auf  > **In-Memory-Tabelle**.

5. Beschreiben Sie die In-Memory-Tabelle:
   a. Klicken Sie auf **Wiederkehrend**.
   b. Standardmäßig ist **Aktiviert** ausgewählt. Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, werden Warnmeldungen mit den Daten aus der Tabelle erweitert.
      Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, die Warnmeldungen aber nicht erweitert werden sollen, deaktivieren Sie das Kontrollkästchen.
   c. Geben Sie im Feld **Benutzerdefinierter Tabellenname** einen Namen für die Konfiguration der In-Memory-Tabelle ein, zum Beispiel „Studenteninformationen“.
   d. Wenn Sie erläutern möchten, welche Informationen die Erweiterung zu einer Warnmeldung hinzufügt, geben Sie eine **Beschreibung** ein, wie z. B.:
      Wenn eine Warnmeldung nach „Rollno“ gruppiert ist, fügt diese Erweiterung Studenteninformationen hinzu, zum Beispiel Name und Markierungen.
6. Geben Sie die URL der CSV-Datei ein, die die In-Memory-Tabelle mit Daten befüllt. Klicken Sie auf „Überprüfen“, um den Link zu validieren und die Spalten in der CSV-Datei zu befüllen. Sie können mithilfe der Plus- und Minus-Schaltflächen Spalten hinzufügen oder entfernen.
7. Wenn der Server hinter einem anderen Server konfiguriert ist, wählen Sie **Proxy verwenden** aus.
8. Wenn Anmeldeinformationen für den Server erforderlich sind, wählen Sie **Authentifiziert** aus.
9. Geben Sie als **Wiederholungsintervall** an, wie oft ESA die letzte CSV-Datei prüfen muss:
   a. Wählen Sie Minute(n), Stunde(n), Tag(e) oder Woche aus.
   b. Wenn Sie „Woche“ auswählen, wählen Sie einen Wochentag aus.
   c. Klicken Sie auf **Datumsbereich**, um ein **Startdatum** und ein **Enddatum** für den wiederkehrenden Plan auszuwählen.



10. Wählen Sie bei Verwendung einer CSV-basierten In-Memory-Tabelle als Erweiterung im Drop-down-Menü **Schlüssel** das Feld aus, das als Standardschlüssel verwendet werden soll, um eingehende Ereignisse mit der In-Memory-Tabelle zu verbinden. Standardmäßig ist die erste Spalte ausgewählt. Sie können den Schlüssel auch später ändern, wenn Sie die In-Memory-Tabelle in Erweiterungsquellen öffnen.

11. Wählen Sie im Drop-down-Menü **Max. Zeilen** die Anzahl der Zeilen aus, die die eine bestimmte Instanz der In-Memory-Tabelle enthalten kann.
12. Wählen Sie **Fortbestehen** aus, um die In-Memory-Tabelle auf dem Datenträger beizubehalten, wenn der ESA-Service angehalten wird, und um die Tabelle wieder aufzufüllen, wenn der Service wieder gestartet wird.
13. Führen Sie im Feld **Format der gespeicherten Datei** eine der folgenden Optionen aus:
    - Wählen Sie **Objekt**, wenn Sie die Datei im binären Format speichern möchten.
    - Wählen Sie **JSON**, wenn Sie die Datei im Textformat speichern möchten. Standardmäßig ist **Objekt** ausgewählt.
14. Klicken Sie auf **Speichern**.
    Die wiederkehrende In-Memory-Tabelle ist konfiguriert. Sie können sie der Regel als Erweiterung oder als Teil der Regelbedingung hinzufügen. Siehe Hinzufügen einer Erweiterung zu einer Regel.

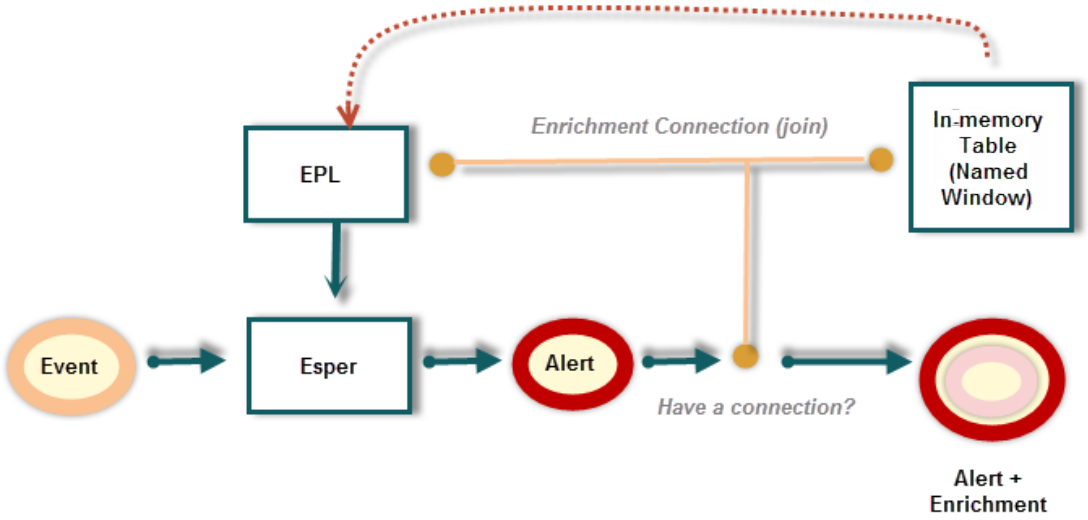
Konfigurieren eine Esper-Abfrage als Erweiterungsquelle

Bei Verwendung des „Expertenmodus“ können Sie eine Erweiterungsquelle oder ein benanntes Fenster basierend auf einer Esper-Abfrage erstellen. So haben Sie mehr Kontrolle über den Inhalt und können dynamischere Inhalte erstellen. Wenn Sie dies tun, erstellt eine EPL-Abfrage das benannte Fenster zur Erfassung eines interessanten Zustands aus dem Ereignisstream.

Workflow

Nachfolgenden sehen Sie den Workflow für die Erstellung einer Abfrage unter Verwendung eines benannten Fensters:

1. Das Ereignis wird an die Esper-Engine gesendet.
2. Eine EPL-Abfrage wird erzeugt.
3. Eine Warnmeldung wird ausgelöst.
4. Die Abfrage überprüft, ob eine Verbindung zwischen dem Ereignis und das benannten Fenster vorhanden ist.
5. Wenn eine Verbindung vorhanden ist, wird die Abfrage, die das benannte Fenster füllt, ausgeführt und ausgefüllt.
6. Der Inhalt des benannten Fensters wird dem Inhalt der Warnmeldung hinzugefügt und gesendet oder angezeigt (je nach Ihren Einstellungen).



Voraussetzungen

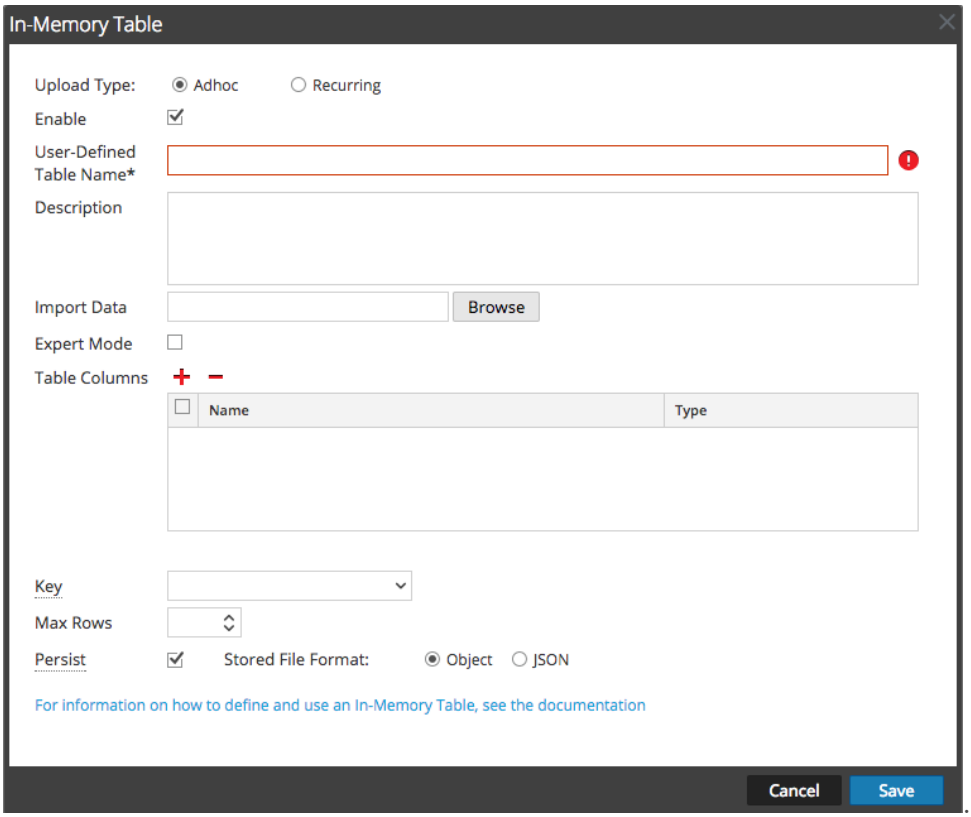
- Die in der EPL-Anweisung verwendeten Metadaten müssen in den Daten vorhanden sein.
- Sie müssen wohlgeformte EPL-Anweisungen erstellen.

Verfahren

Konfigurieren einer In-Memory-Tabelle mit einer EPL-Abfrage

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Ansicht „Konfigurieren“ wird mit geöffneter Registerkarte „Regeln“ angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.

4. Klicken Sie im Abschnitt **Erweiterungsquellen** auf > In-Memory-Tabelle



5. Wählen Sie **Ad-hoc** aus.
   Standardmäßig ist Aktiviert ausgewählt. Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, werden Warnmeldungen mit den Daten aus der Tabelle erweitert.

6. Geben Sie im Feld **Benutzerdefinierter Tabellenname** einen beschreibenden Namen ein, um die In-Memory-Tabelle zu beschreiben.

7. Wenn Sie erklären möchten, was die Erweiterung einer Warnmeldung hinzufügt, geben Sie Informationen in das Feld **Beschreibung** ein.
   Diese Beschreibung wird angezeigt, wenn Sie die Liste der Erweiterungen aus der Ansicht „Erweiterungsquellen“ anzeigen. Daher ist es empfehlenswert, als Best Practice eine detaillierte Beschreibung einzugeben. Dadurch können andere Benutzer den Inhalt der Erweiterung verstehen, ohne sie zu öffnen, um den Inhalt zu untersuchen.

8. Wählen Sie den **Expertenmodus**, um eine erweiterte Konfiguration für eine In-Memory-Tabelle zu definieren, indem Sie eine EPL-Abfrage schreiben.
   Der Abschnitt „Tabellenspalten“ wird durch ein Feld **Abfrage** ersetzt.

9. Wählen Sie **Fortbestehen** aus, um die In-Memory-Tabelle auf dem Datenträger beizubehalten, wenn der ESA-Service angehalten wird, und um die Tabelle wieder aufzufüllen, wenn der Service wieder gestartet wird.
10. Geben Sie die EPL-Abfrage in das Feld **Abfrage** ein. Die Abfrage sollte wohlgeformt sein und getestet werden, bevor sie in das Feld eingegeben wird.
11. Klicken Sie auf **Speichern**.

Beispiel

Beispielsweise können Sie eine Regel erstellen, die nach fünf fehlgeschlagenen Anmeldungen gefolgt von einer erfolgreichen Anmeldung sucht. Wenn diese Regel ausgelöst wird, kann die Benachrichtigung Informationen über den Benutzer enthalten, der zuletzt am System angemeldet war, als diese erfolgreiche Anmeldung erfolgt ist. Um diese Erweiterung der Benachrichtigung hinzuzufügen, können Sie eine Stream-basierte In-Memory-Lookup-Tabelle erstellen, die von eingehenden Ereignissen ausgefüllt wird, um eine Zuordnung von IP-Adressen zu dem letzten über diese Adresse angemeldeten Benutzer beizubehalten. Um dies zu erreichen, erstellen Sie eine Erweiterung mithilfe einer Abfrage als Quelle.

Schritt 1: Erstellen der Regel

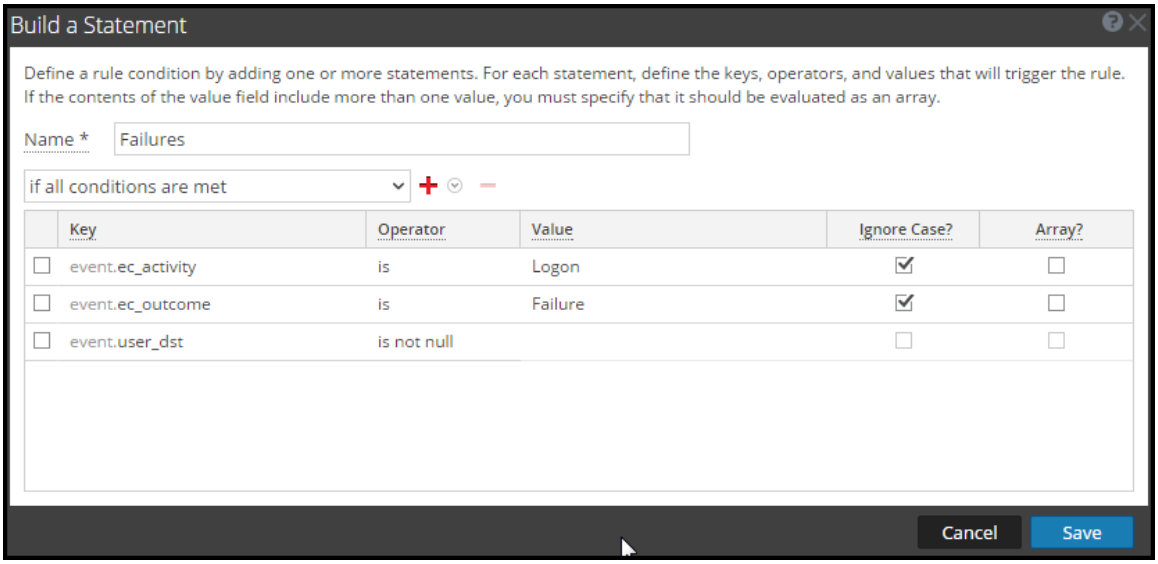
Zunächst müssen Sie Ihre Korrelationsregel erstellen. In diesem Fall erstellen Sie Regelbedingungen für Fehler und Erfolg und gruppieren nach „ip_src“.

Regelbedingung	Beschreibung
Failures	Diese Bedingung sucht nach 5 fehlgeschlagenen Anmeldungen mit einem „followed by“-Connector. Das bedeutet, dass der Bedingung (Failure) die nächste Bedingung (Success) folgen muss.
Success	Diese Bedingung sucht nach einer erfolgreichen Anmeldung.

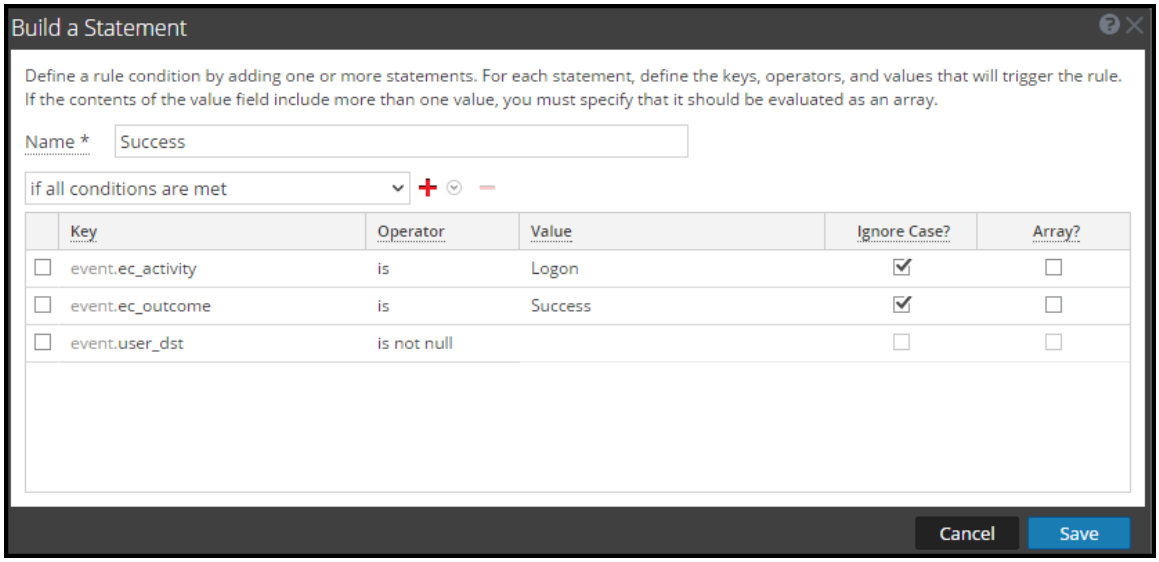
Regelbedingung	Beschreibung
GroupBy: ip_src, Geräteklasse	Das Feld „GroupBy“ sorgt dafür, dass alle vorherigen Bedingungen nach Geräteklasse „ip_srcand“ gruppiert werden. Dies ist wichtig für die Erstellung der Regel, da die Regel versucht, einen Fall zu finden, in dem ein Benutzer mehrere Male versucht hat, sich bei dem gleichen Zielkonto anzumelden und sich dann schließlich erfolgreich angemeldet hat. Durch das Gruppieren nach Geräteklasse wird sichergestellt, dass der Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht hat, sich an einem Konto anzumelden. Die Regel gibt möglicherweise unerwartete Ergebnisse zurück, wenn Sie die Ergebnisse nicht gruppieren.
Auftreten innerhalb 5 Minuten	Das Zeitfenster für das Eintreten des Ereignisses beträgt 5 Minuten. Wenn die Ereignisse außerhalb dieses Zeitfensters auftreten, wird die Regel nicht ausgelöst.
Ereignissequenz: Strikt	Die Ereignissequenz wird für eine strenge Musterübereinstimmung konfiguriert. Das bedeutet, dass das Muster genau wie angegeben übereinstimmen muss, ohne dazwischen vorkommende Ereignisse.

Für die Regelbedingungen erstellen Sie die folgenden Anweisungen:

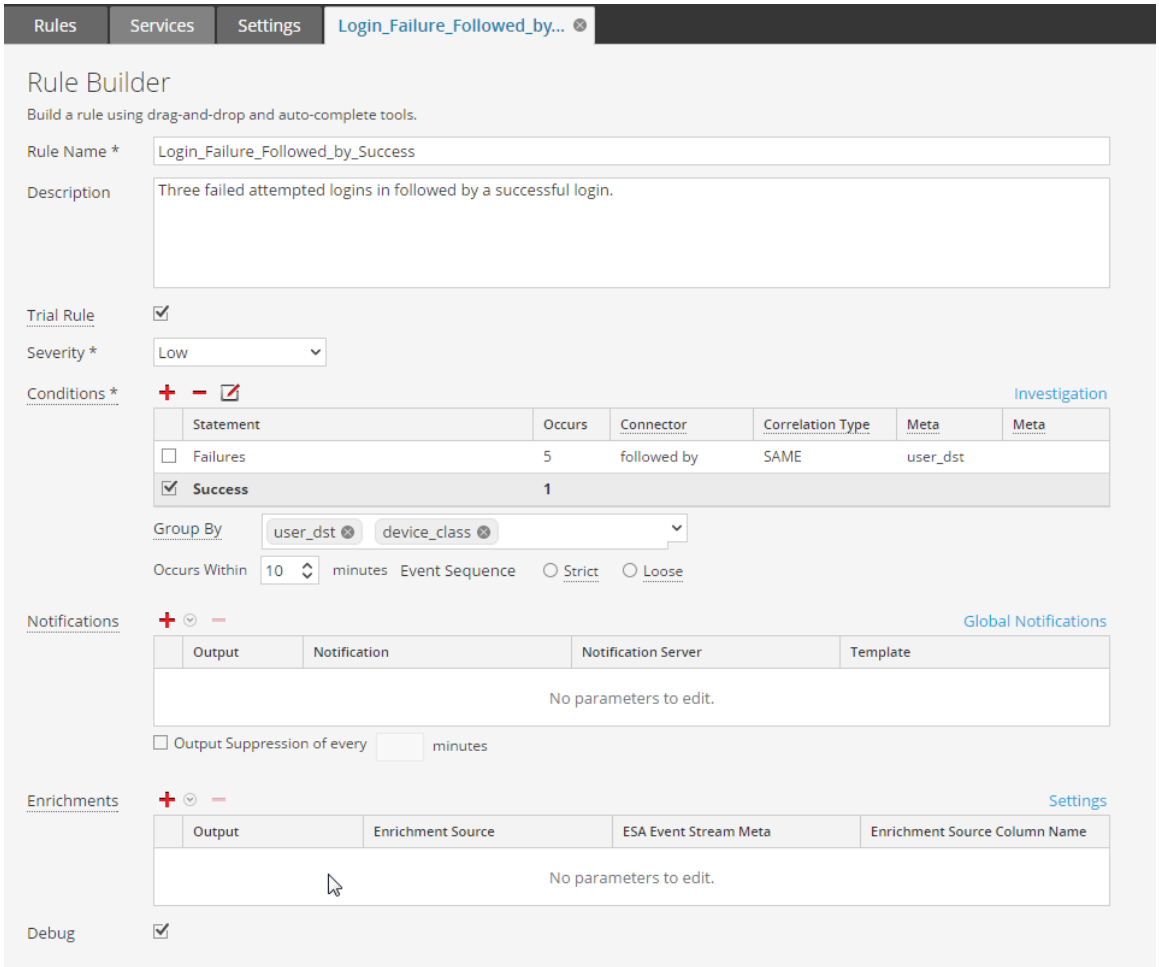
- Die Anweisung „Fehler“ sucht nach fehlgeschlagenen Anmeldeversuchen:



- Die Anweisung „Erfolg“ sucht nach einer erfolgreichen Anmeldung:



- Kombiniert haben Sie die folgende Korrelationsregel:



Schritt 2: Erstellen der Erweiterung

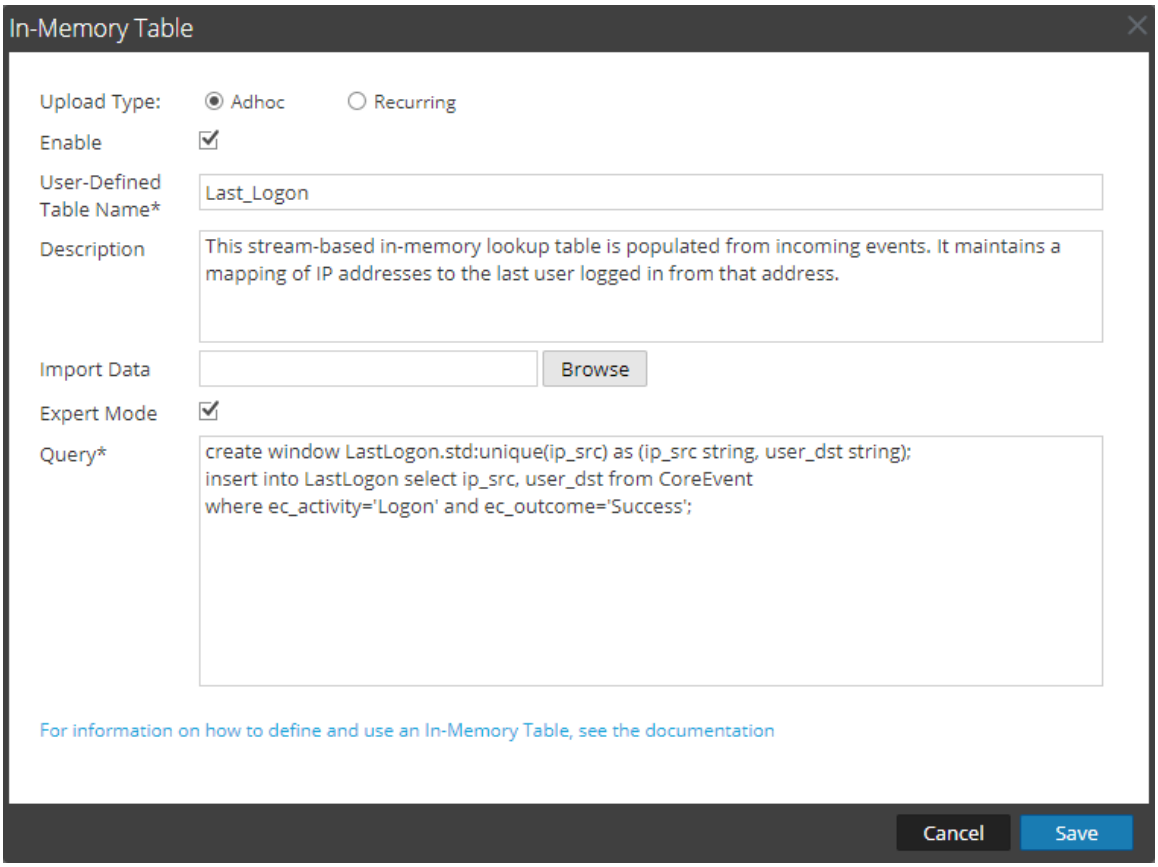
Nun, da Sie Ihre Regel erstellt haben, müssen Sie die Erweiterung erstellen, die der Benachrichtigungsausgabe hinzugefügt werden soll. Befolgen Sie die obigen Schritte, um die Erweiterung zu erstellen, nennen Sie sie *Last_Logon* und fügen Sie die folgende Abfrage hinzu:

```
create window LastLogon.std:unique(ip_src) as (ip_src string, user_dst string);

insert into LastLogon select ip_src, user_dst from CoreEvent

where ec_activity='Logon' and ec_outcome='Success';
```

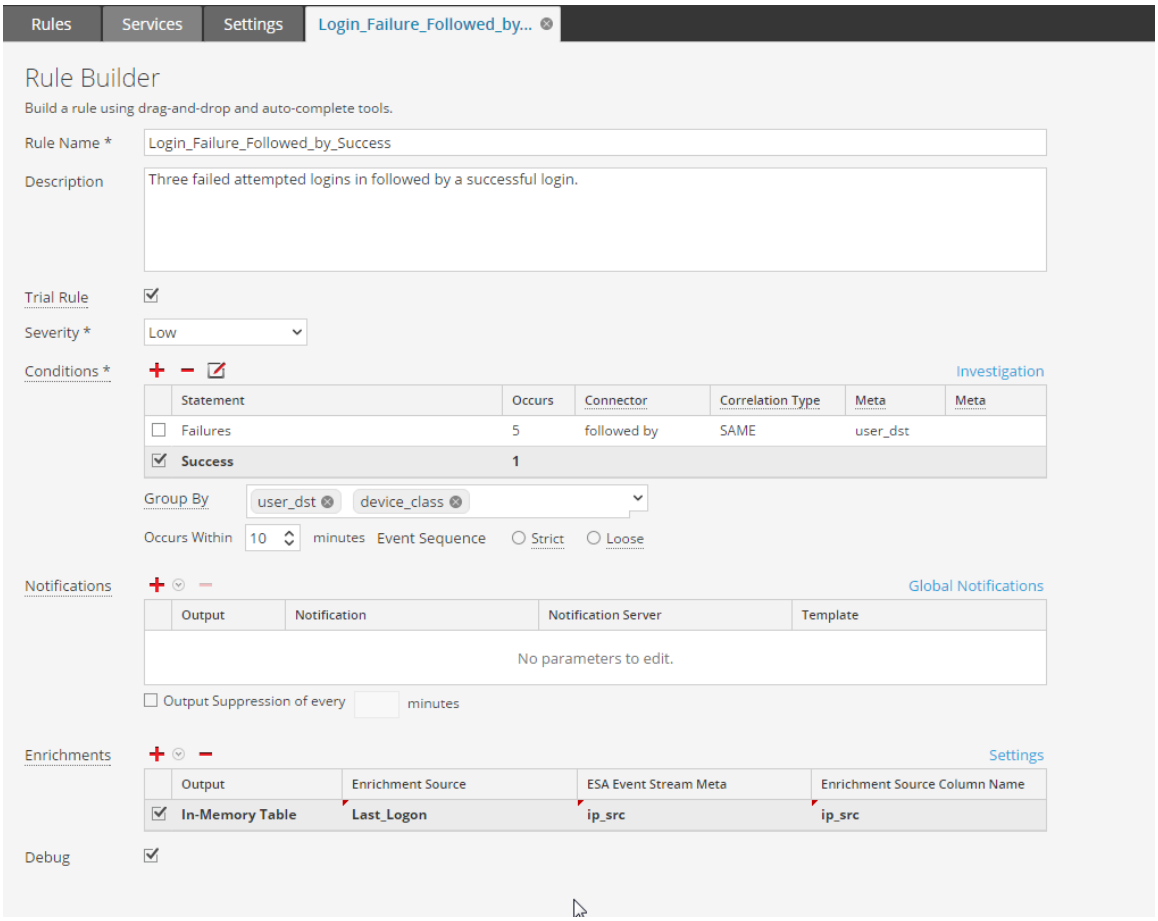
Die Erweiterung sollte wie folgt aussehen:



Schritt 3: Hinzufügen der Erweiterung zur Regel

Nun, da Sie Ihre grundlegende Regel und Ihre Erweiterung erstellt haben, müssen Sie die Erweiterung der Regel hinzufügen und die Erweiterung mit den Metadaten in der Regel verknüpfen (oder verbinden).

Öffnen Sie die Regel „Login_Failure_Followed_by_Success“ zur Bearbeitung.



Feld	Eingabe	Beschreibung
Ausgabe	In-Memory-Tabelle	Mit der Option „In-Memory-Tabelle“ erstellen Sie ein benanntes Fenster, das mit den Daten der EPL-Abfrage ausgefüllt werden kann.
Erweiterungsquelle	Last_Logon (die oben erstellte Erweiterung).	Dies ist die Stream-basierte In-Memory-Lookup-Tabelle, die von eingehenden Ereignissen ausgefüllt wird, um eine Zuordnung von IP-Adressen zu dem letzten über diese Adresse angemeldeten Benutzer beizubehalten.
ESA Ereignis-Stream-Metadaten	ip_src	Hierbei handelt es sich um Ereignis-Stream-Metadaten, die Sie den Erweiterungsdaten hinzufügen können, die Sie eingeben. Im Grunde ist „ip_src“ die Verknüpfungsbedingung.

Feld	Eingabe	Beschreibung
Spaltenname „Erweiterungsquelle“	ip_src	Hierbei handelt es sich um die Metadaten aus der Erweiterung, die Sie den Ereignis-Stream-Daten hinzufügen können. Es müssen die gleichen wie die Verknüpfungsbedingung aus dem Feld „Ereignis-Stream-Metadaten“ sein.

Nachdem Sie die Erweiterung hinzugefügt haben, können Sie die Regel speichern.

Wenn die Regel ausgelöst wird, führt der ESA-Service die Abfrage in der Erweiterung aus und füllt das benannte Fenster mit den Daten. Wenn die Daten im benannten Fenster mit der Verknüpfungsbedingung übereinstimmen, werden die Daten der Ausgabe hinzugefügt, die Sie als E-Mail, SNMP, Syslog oder Skript anzeigen können, je nachdem, wie Sie Benachrichtigungen konfiguriert haben.

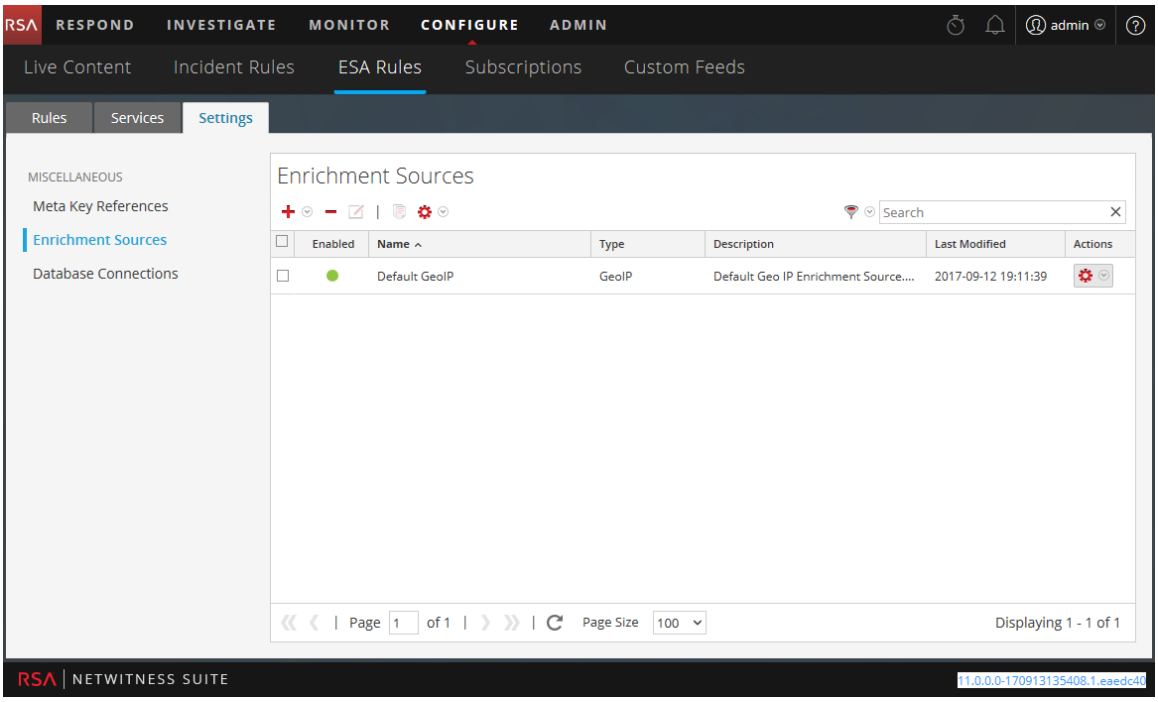
Konfigurieren von Warehouse Analytics als Erweiterungsquelle

In diesem Thema werden Anweisungen zur Konfiguration von RSA Warehouse Analytics als Erweiterungsquelle für ESA bereitgestellt. Datenanalysten nutzen Warehouse Analytics-Daten, um Sitzungs- und Protokolldaten zu analysieren.

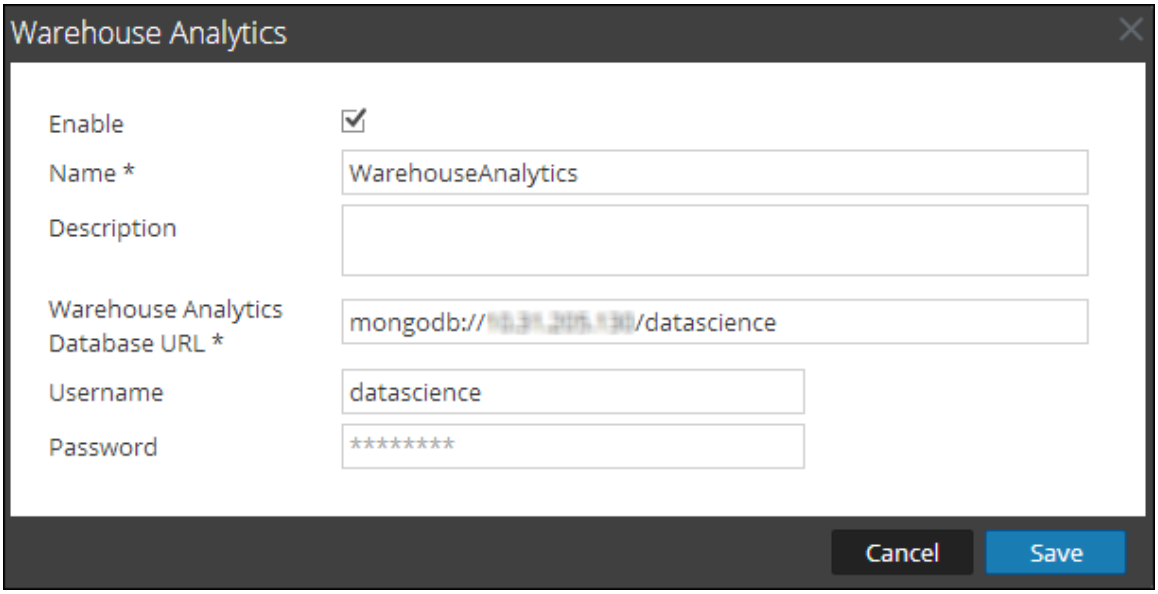
So konfigurieren Sie Warehouse Analytics als Erweiterungsquelle:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Einstellungen**.
2. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.

   Der Bereich Erweiterungsquellen wird angezeigt.



3. Wählen Sie aus dem  -Drop-down-Menü **Warehouse Analytics** aus.



4. Wählen Sie **Aktivieren** aus, um Warnmeldungen um zusätzliche Daten zu erweitern. Diese Option ist standardmäßig aktiviert. Wenn sie deaktiviert ist, werden die Warnmeldungen nicht um zusätzliche Daten erweitert.
5. Geben Sie in das Feld **Name** einen Namen ein, um die Warehouse Analytics-Konfiguration zu identifizieren oder zu bezeichnen.

6. Geben Sie in das Feld **Beschreibung** eine kurze Beschreibung der Warehouse Analytics-Konfiguration ein.
7. Geben Sie in das Feld **Warehouse Analytics-Datenbank-URL** die MongoDb-URL für die Warehouse Analytics-Datenbank ein.
8. Geben Sie in das Feld **Benutzername** den Benutzername ein, um auf die MongoDB zugreifen zu können.
9. Geben Sie in das Feld **Passwort** das Passwort ein, um auf die MongoDB zugreifen zu können.
10. Klicken Sie auf **Speichern**.

Weitere Informationen finden Sie unter Registerkarte „Einstellungen“.

Hinzufügen einer Erweiterung zu einer Regel

In diesem Thema wird erläutert, wie eine zuvor konfigurierte Erweiterungsquelle zu einer Regel hinzugefügt wird. Wenn ESA eine Warnmeldung erstellt, werden die Informationen aus dieser Quelle einbezogen.

Durch Hinzufügen einer Erweiterungsquelle können Sie eine Suche in einer Vielzahl von Quellen anfordern und die Ergebnisse in die ausgehenden Warnmeldungen integrieren, um deren Inhalt detaillierter zu gestalten. Für dieses Verfahren sind die Rollenberechtigungen Administrator, DPO und SOC Manager erforderlich.

Verfahren

So fügen Sie einer Regel eine Erweiterung hinzu:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
2. Führen Sie in der Ansicht **Regelbibliothek** einen der folgenden Schritte aus:
   - Doppelklicken Sie auf eine Regel.
   - Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste der **Regelbibliothek** auf  .

   Der Bereich „Regelerstellung“ wird in einer neuen NetWitness Suite-Registerkarte angezeigt.
3. Klicken Sie im Bereich **Erweiterungen** auf  und wählen Sie einen der folgenden Erweiterungstypen aus:

- In-Memory-Tabelle
- Externer DB-Verweis
- Warehouse Analytics
- GeoIP

> **Hinweis:** Wenn Sie eine GeoIP-Quelle verwenden, wird ipv4 automatisch ausgefüllt und kann nicht bearbeitet werden.

Die von Ihnen ausgewählten Erweiterungstypen werden in der Tabelle angezeigt.

4. Gehen Sie für den hinzugefügten Erweiterungstyp wie folgt vor:
   - Wählen Sie in der Spalte **Ausgabe** den Typ aus, den Sie konfiguriert haben.
   - Wählen Sie in Drop-down-Liste **Erweiterungsquelle** die definierte Erweiterungsquelle aus.
   - Geben Sie im Feld **ESA Ereignis-Stream-Metadaten** den Metaschlüssel des Ereignis-Streams ein, dessen Wert als ein Operand der Verknüpfungsbedingung verwendet wird.

   - Geben Sie im Feld **Spaltenname „Erweiterungsquelle“** den Spaltennamen der Erweiterungsquelle ein, dessen Wert als weiterer Operand der Verknüpfungsbedingung verwendet wird.
5. Wählen Sie **Debuggen** aus. Hierdurch wird eine @Audit(‚Stream‘)-Anmerkung zur Regel hinzugefügt. Das ist für das Debuggen der Esper-Regeln von Vorteil.
6. Klicken Sie auf **Syntax anzeigen**, um zu testen, ob die definierte ESA-Regel gültig ist.
7. Klicken Sie auf **Speichern**.

Nähere Einzelheiten zu Parametern und deren Beschreibung finden Sie auf der Registerkarte Registerkarte Regelerstellung.

Bereitstellen von Regeln für die Ausführung in ESA

In diesem Thema wird erläutert, wie ein ESA-Service und die darauf anzuwendenden Regeln ausgewählt werden. Für alle Aufgaben in diesem Abschnitt sind die Berechtigungen der Rollen Administrator, SOC Manager oder DPO erforderlich.

Für die Erstellung einer Bereitstellung müssen Sie die Schritte ausführen, die beschrieben sind unter Bereitstellungsschritte.

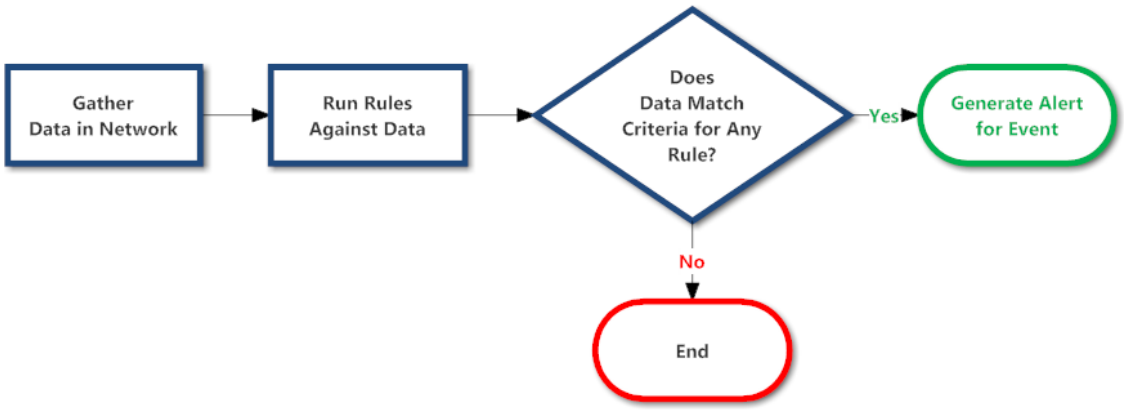
Funktionsweise der Bereitstellung

Eine Bereitstellung besteht aus einem ESA-Service und einem Satz von ESA-Regeln. Wenn Sie Regeln bereitstellen, führt der ESA-Service diese aus, um verdächtige oder unerwünschte Aktivitäten in Ihrem Netzwerk zu erkennen. Jede ESA-Regel erkennt ein unterschiedliches Ereignis, zum Beispiel den Fall, dass ein Benutzerkonto erstellt und innerhalb einer Stunde gelöscht wird.

Der ESA-Service führt die folgenden Funktionen aus:

1. Sammelt **Daten** im Netzwerk.
2. Führt ESA-**Regeln** für die Daten aus.
3. Wendet **Regelkriterien** auf Daten an.
4. Erzeugt eine **Warnmeldung**für das erfasste Ereignis.

In der folgenden Grafik wird dieser Workflow dargestellt:



Darüber hinaus möchten Sie möglicherweise weitere Schritte für die Bereitstellung durchführen, beispielsweise einen ESA-Service in der Bereitstellung löschen, eine Regel aus der Bereitstellung bearbeiten oder löschen, eine Bereitstellung bearbeiten oder löschen oder Updates für eine Bereitstellung anzeigen. Beschreibungen dieser Verfahren finden Sie unter Zusätzliche Bereitstellungsverfahren

Bereitstellungsschritte

In diesem Thema wird das Hinzufügen einer Bereitstellung erläutert, die einen ESA-Service und einen Satz ESA-Regeln enthält. Sie können eine Bereitstellung zum Organisieren und Managen von ESA-Services und -Regeln hinzufügen. Stellen Sie sich die Bereitstellung als Container für beide Komponenten vor:

1. Einen ESA-Service
2. Einen Satz ESA-Regeln

Wenn Sie beispielsweise die Bereitstellung für Spamaktivität hinzufügen, kann sie ESA London und einen Satz ESA-Regeln zur Erkennung von verdächtiger E-Mail-Aktivität enthalten.

Zum Hinzufügen einer Bereitstellung müssen Sie die folgenden Verfahren durchführen:

- Schritt 1. Hinzufügen einer Bereitstellung
- Schritt 2. Hinzufügen eines ESA-Services
- Schritt 3. Hinzufügen und Bereitstellen von Regeln

Schritt 1. Hinzufügen einer Bereitstellung

Voraussetzungen

Folgendes ist erforderlich, um eine Bereitstellung hinzuzufügen:

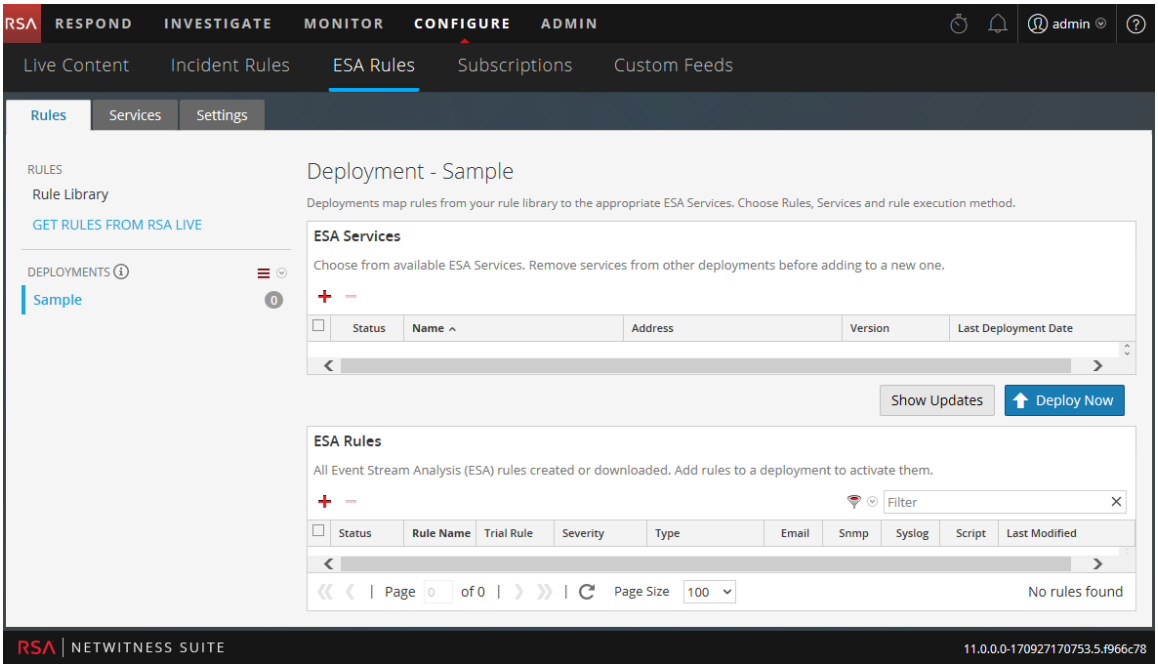
- Der ESA-Service muss auf dem Host konfiguriert werden. Siehe „Konfigurieren von ESA-Services“ im *Konfigurationsleitfaden für Event Stream Analysis (ESA)*.
- Regeln müssen in der Regelbibliothek festgelegt werden. Siehe Hinzufügen von Regeln zur Regelbibliothek.

Verfahren

So fügen Sie eine Bereitstellung hinzu:

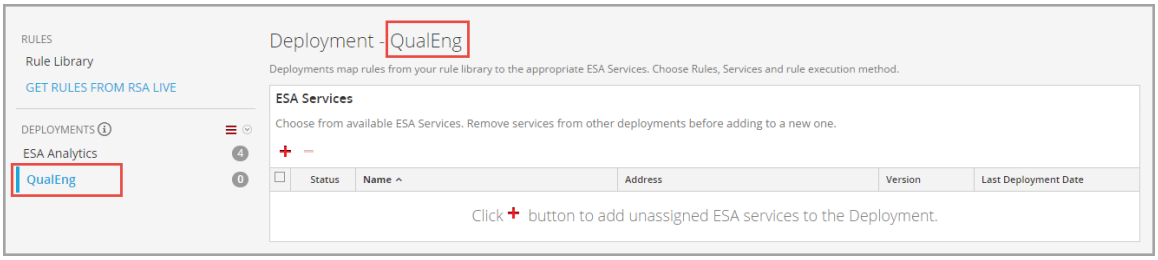
1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte Regeln wird angezeigt.

2. Wählen Sie im Bereich „Optionen“ neben den Bereitstellungen die Optionen  > **Hinzufügen** aus.
   Die Ansicht „Bereitstellung“ wird rechts angezeigt.



3. Geben Sie im Optionsbereich einen **Namen** für die Bereitstellung ein. Sie können die Benennungskonvention beliebig festlegen.
   Sie kann beispielsweise den Verwendungszweck angeben oder einen Eigentümer identifizieren.

4. Drücken Sie die **Eingabetaste**.
   Die Bereitstellung wird hinzugefügt.



Schritt 2. Hinzufügen eines ESA-Services

Der ESA-Service in einer Bereitstellung sammelt Daten im Netzwerk und führt ESA-Regeln an den Daten aus. Dies dient dazu, Ereignisse zu erfassen, die den Regelkriterien entsprechen, und dann eine Warnmeldung zu dem erfassten Ereignis zu erzeugen.

Der gleiche ESA-Service kann zu mehreren Bereitstellungen hinzugefügt werden. Beispielsweise kann ESA London gleichzeitig in folgenden Bereitstellungen vorhanden sein:

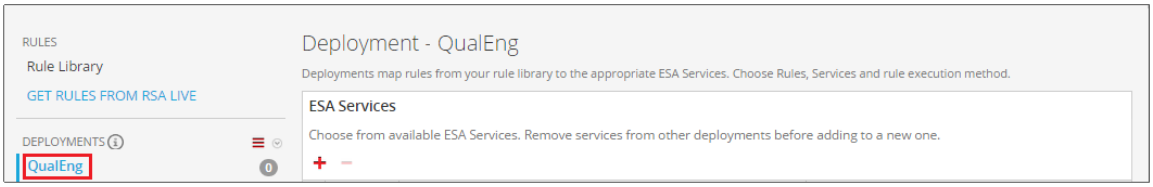
- Bereitstellung EUR, die einen Satz von ESA-Regeln enthält
- Bereitstellung CORP, die einen anderen Satz von ESA-Regeln enthält

Wenn Sie einen ESA-Service aus einer Bereitstellung entfernen, werden die Regeln ebenfalls aus dem ESA-Service entfernt. Beispielsweise kann die Bereitstellung EUR ESA London sowie 25 Regeln enthalten. Wenn Sie ESA London aus der Bereitstellung EUR entfernen, werden die 25 Regeln ebenfalls aus ESA London entfernt. Folglich enthält ein ESA-Service keine Regeln, wenn er nicht Bestandteil einer Bereitstellung ist.

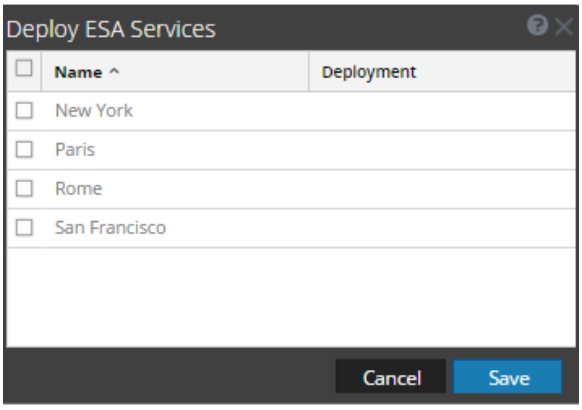
Verfahren

So fügen Sie einen ESA-Service hinzu:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich „Optionen“ eine **Bereitstellung** aus:



3. Klicken Sie in der Ansicht **Bereitstellung** unter **ESA-Services** auf + .
   Im Dialogfeld „ESA-Services bereitstellen“ werden alle konfigurierten ESA-Services aufgelistet.



4. Wählen Sie eine ESA aus und klicken Sie auf **Speichern**.
   Die Ansicht „Bereitstellung“ wird angezeigt. Der ESA-Service wird im Bereich **ESA-Services** mit dem Status „Hinzugefügt“ aufgeführt.

Schritt 3. Hinzufügen und Bereitstellen von Regeln

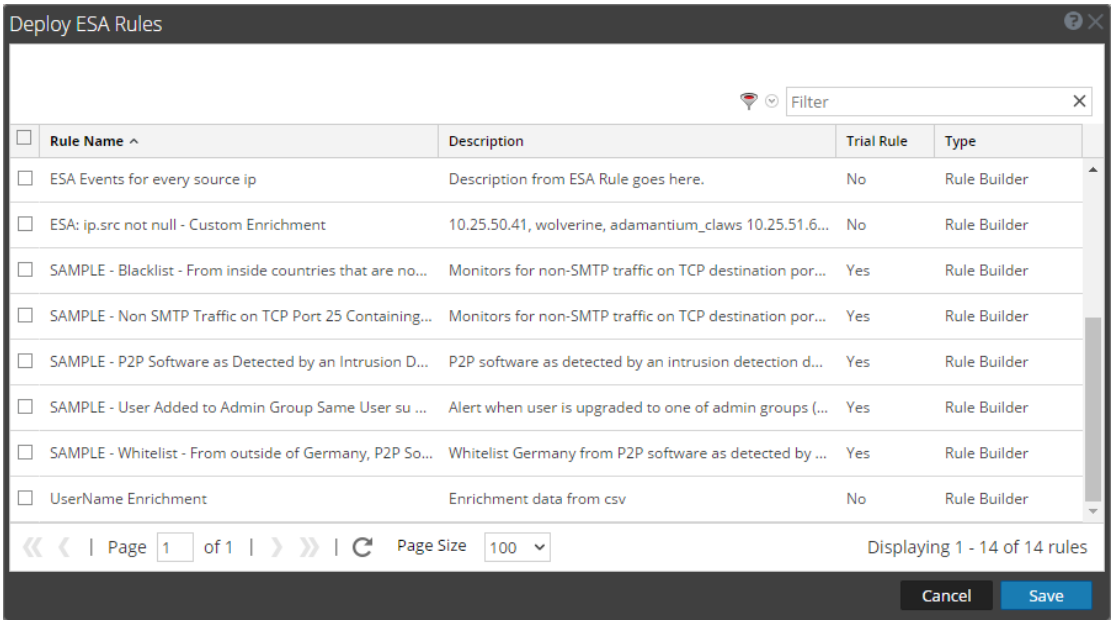
In diesem Thema wird erläutert, wie Sie einer Bereitstellung ESA-Regeln hinzufügen und die Regeln dann in ESA bereitstellen. Jede ESA-Regel hat eindeutige Kriterien. Die ESA-Regeln in einer Bereitstellung legen fest,welche Ereignisse von ESA erfasst werden. Damit werden wiederum die Warnmeldungen festgelegt, die Sie erhalten.

Zum Beispiel enthält Bereitstellung A ESA Paris und unter anderem eine Regel, mit der Dateitransfer über einen nicht standardmäßigen Port erfasst wird. Wenn ESA Paris einen Dateitransfer erkennt, der den Regelkriterien entspricht, wird das Ereignis erfasst und eine entsprechende Warnmeldung erzeugt. Wenn Sie diese Regel aus der Bereitstellung A entfernen, erzeugt ESA keine Warnmeldung mehr für ein solches Ereignis.

Verfahren

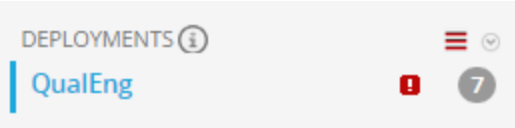
So fügen Sie Regeln hinzu und stellen sie bereit:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich Optionen eine Bereitstellung aus.
3. Klicken Sie in der Ansicht **Bereitstellung** auf + in **ESA-Regeln**.
   Das Dialogfeld „ESA-Regeln bereitstellen“ wird angezeigt. Es enthält die einzelnen Regeln in Ihrer Regelbibliothek:



4. Wählen Sie Regeln aus und klicken Sie auf **Speichern**.
   .Die Ansicht „Bereitstellung“ wird angezeigt.
5. Die Regeln werden im Abschnitt „ESA-Regeln“ aufgelistet.

- In der Spalte „Status“ wird **Hinzugefügt** neben jeder neuen Regel angezeigt.
- Im Abschnitt „Bereitstellung“ zeigt an, dass Updates für die Bereitstellung vorhanden sind.
- Die Gesamtzahl der Regeln in der Bereitstellung wird auf der rechten Seite angezeigt.



6. Klicken Sie auf **Jetzt bereitstellen**.
   Der ESA-Service führt den Regelsatz aus.

Zusätzliche Bereitstellungsverfahren

Neben der Bereitstellung eines ESA-Services und -Regeln möchten Sie möglicherweise weitere Schritte für die Bereitstellung durchführen, beispielsweise einen ESA-Service in der Bereitstellung löschen, eine Regel aus der Bereitstellung bearbeiten oder löschen, eine Bereitstellung bearbeiten oder löschen oder Updates für eine Bereitstellung anzeigen.

Um diese Verfahren durchführen zu können, gehen Sie zu:

- Löschen eines ESA-Services in einer Bereitstellung
- Bearbeiten oder Löschen einer Regel in einer Bereitstellung
- Bearbeiten oder Löschen einer Bereitstellung
- Anzeigen der Aktualisierungen an einer Bereitstellung

Löschen eines ESA-Services in einer Bereitstellung

Dieses Thema bietet Anweisungen zum Löschen eines ESA-Services in einer Bereitstellung. In einer Bereitstellung mit einem Service können Sie die auf den Service angewendeten Regeln bearbeiten und den Service aus der Bereitstellung löschen.

Jedes der folgenden Verfahren beginnt auf der Registerkarte „Regeln“.

Verfahren

So löschen Sie einen ESA-Service:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
   Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.

3. Wählen Sie im Bereich **ESA-Services** einen Service aus und klicken Sie in der Symbolleiste auf .
   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Yes**.
   Der Service wird gelöscht.

Bearbeiten oder Löschen einer Regel in einer Bereitstellung

In einer Bereitstellung mit Regeln können Sie die Regeln bearbeiten oder löschen, um die Bereitstellung anzupassen. Jedes der folgenden Verfahren beginnt auf der Registerkarte „Regeln“.

Methoden

Bearbeiten einer Regel

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
   Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich „Optionen“ unter „Bereitstellungen“ eine Bereitstellung aus.
3. Doppelklicken Sie im Bereich **ESA-Regeln** auf eine Regel, um diese in einer neuen Registerkarte zu öffnen.
4. Ändern Sie die Regel und klicken sie anschließend auf **Anwenden**.
   Die Regel wird gespeichert.

Löschen einer Regel

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Regeln**.
   Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.
3. Wählen Sie im Bereich **ESA-Regeln** eine Regel aus und klicken Sie in der Symbolleiste auf .
   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Yes**.
   Die Regel wird gelöscht.

Bearbeiten oder Löschen einer Bereitstellung

In diesem Thema wird erläutert, wie NetWitness Suite eine Korrelationsregel an alle ESA-Services in einer Korrelationsgruppe weiterleitet. In einer Korrelationsgruppe muss jeder ESA-Service denselben Satz von Regeln ausführen. Wenn Sie einer Korrelationsgruppe eine Regel hinzufügen, leitet NetWitness Suite die Regel an jeden ESA-Service in der Gruppe weiter.

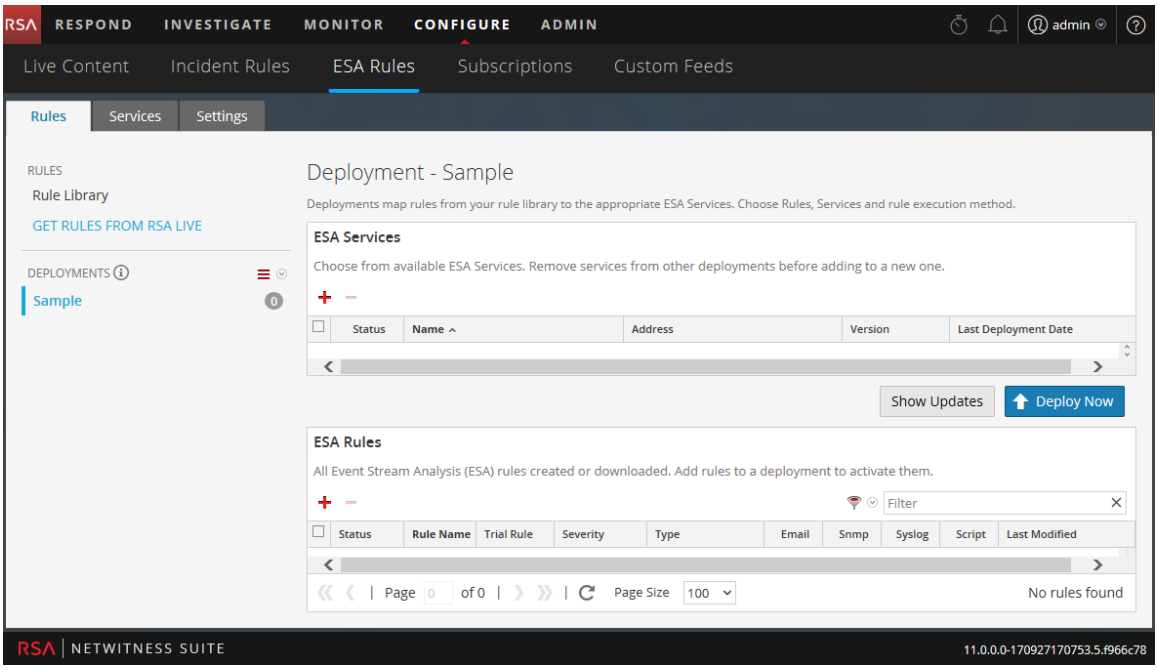
So greifen Sie auf die Bereitstellungen zu

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.

   Die Ansicht „Konfigurieren“ wird mit geöffneter Registerkarte „Regeln“ angezeigt.

2. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.

   Die Ansicht „Bereitstellung“ wird angezeigt.



Bearbeiten einer Bereitstellung

1. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.

   Die Ansicht „Bereitstellung“ wird angezeigt.

2. Wählen Sie  **> Bearbeiten** aus.

   Der Bereitstellungsname kann jetzt bearbeitet werden.

Löschen einer Bereitstellung

1. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.

   Die Ansicht „Bereitstellung“ wird angezeigt.

2. Wählen Sie > **Löschen** aus.

   Ein Bestätigungsdialogfeld wird angezeigt.

3. Klicken Sie auf **Yes**.

   Die Bereitstellung wird gelöscht.

Anzeigen der Aktualisierungen an einer Bereitstellung

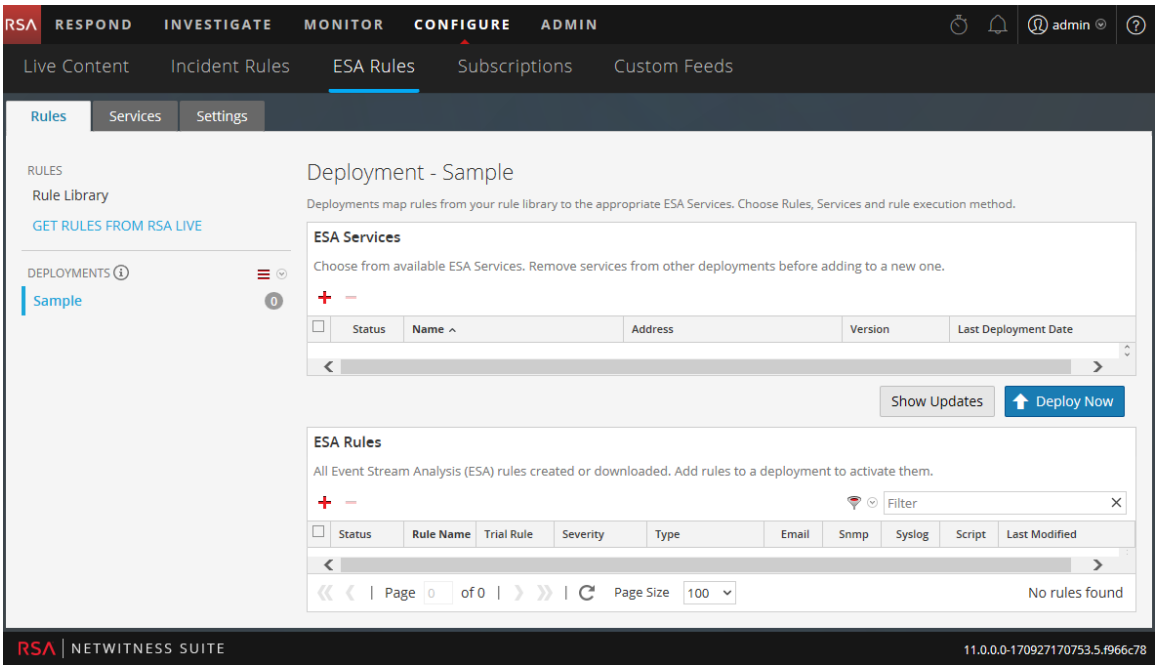
In diesem Thema wird erläutert, wie Aktualisierungen an einer Bereitstellung, beispielsweise das Hinzufügen und Löschen von Regeln, angezeigt werden. Wenn Sie eine Änderung an einer Bereitstellung vornehmen, wird das Aktualisierungssymbol ( ) neben dem Namen der Bereitstellung angezeigt.

Verfahren

So zeigen Sie die Updates zu einer Bereitstellung:

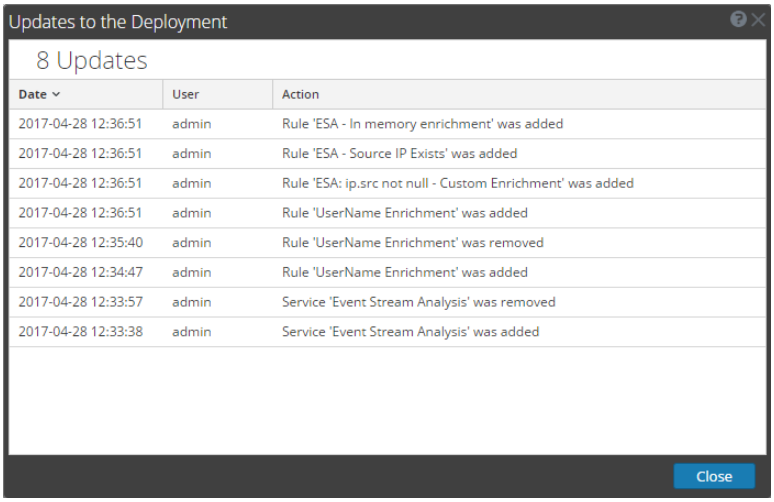
1. Navigieren Sie zu **Konfigurieren > ESA-Regeln.**
   Die Registerkarte Regeln wird angezeigt.

2. Klicken Sie im Bereich „Optionen“ unter **Bereitstellungen** ganz rechts auf **Updates anzeigen**.



   Das Dialogfeld „Aktualisierungen an der Bereitstellung“ wird geöffnet und zeigt die

Änderungen an der Bereitstellung.



3. Klicken Sie auf **Schließen**.

Anzeigen von ESA-Statistiken und -Warnmeldungen

Wenn der ESA-Service Warnmeldungen erzeugt, können Sie Informationen dazu anzeigen, wie die Regeln ausgeführt wurden, wie etwa Statistiken zur Engine, Regel und Warnmeldung, und Sie können auch Informationen dazu anzeigen, welche Regeln aktiviert oder deaktiviert sind. Anweisungen zur Anzeige von ESA-Statistiken finden Sie unter Anzeigen der Statistiken zu einem ESA-Service.

Wenn Ihr ESA-Service Warnmeldungen erzeugt, können Sie die Ergebnisse auf der Seite „Zusammenfassung der Warnmeldungen“ anzeigen. So können Sie Trends sehen und sowohl die Menge als auch die Häufigkeit von Warnmeldungen erkennen. Anweisungen zur Anzeige von Warnmeldungen finden Sie unter Anzeigen einer Zusammenfassung der Warnmeldungen.

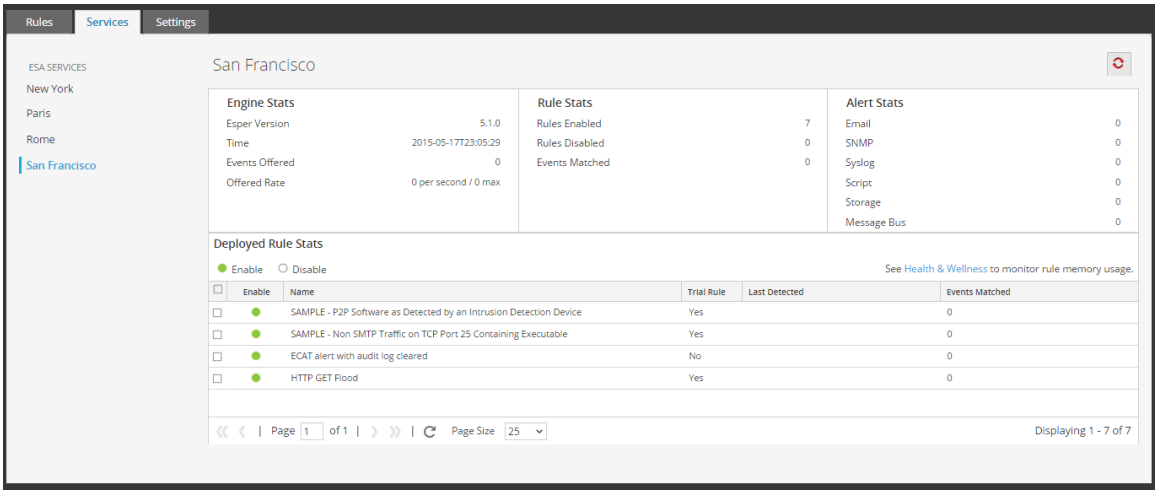
Anzeigen der Statistiken zu einem ESA-Service

In diesem Thema wird beschrieben, wie die Bereitstellungsstatistiken für einen ESA-Service angezeigt werden können. Dieses Verfahren ist nützlich bei dem Versuch, die Effektivität einer Regel oder des Troubleshooting einer Bereitstellung zu ermitteln.

Methoden

Anzeigen der ESA-Statistiken

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln > Services**.
2. Wählen Sie aus der Liste **ESA-Services** auf der linken Seite einen Service aus.
   Die Bereitstellungsstatistiken für den ausgewählten Service werden angezeigt.



3. Lesen Sie die folgenden Abschnitte mit ESA-Statistiken.
   Eine vollständige Beschreibung jeder Statistik in den Abschnitten finden Sie unter Registerkarte Services.
   - **Engine-Statistiken**
   - **Regelstatistiken**
   - **Warnmeldungsstatistiken**
4. Lesen Sie die detaillierten Informationen zu den auf dem ESA bereitgestellten Regeln unter „Statistik für bereitgestellte Regeln“ nach.
   Eine vollständige Beschreibung jeder Spalte in den Abschnitten finden Sie unter Registerkarte Services.
   - Ob die Regel aktiviert oder deaktiviert ist
   - Der Name der Regel
   - Ob die Regel im Testregelmodus ausgeführt wird
   - Zuletzt erkannt
   - Übereinstimmende Ereignisse
5. Klicken Sie zum Erstellen eines Snapshot des Regelspeichers auf **Integrität und Zustand**.

Aktivieren und Deaktivieren von Regeln

1. Wählen Sie im Bereich **Statistik für bereitgestellte Regeln** eine Regel aus dem Raster aus.
2. Klicken Sie auf Enable, um die Regel zu aktivieren, oder klicken Sie auf Disable, um die Regel zu deaktivieren.
   Die Registerkarte „Services“ wird mit den Änderungen aktualisiert, die sofort wirksam sind.

Aktualisieren der Statistiken

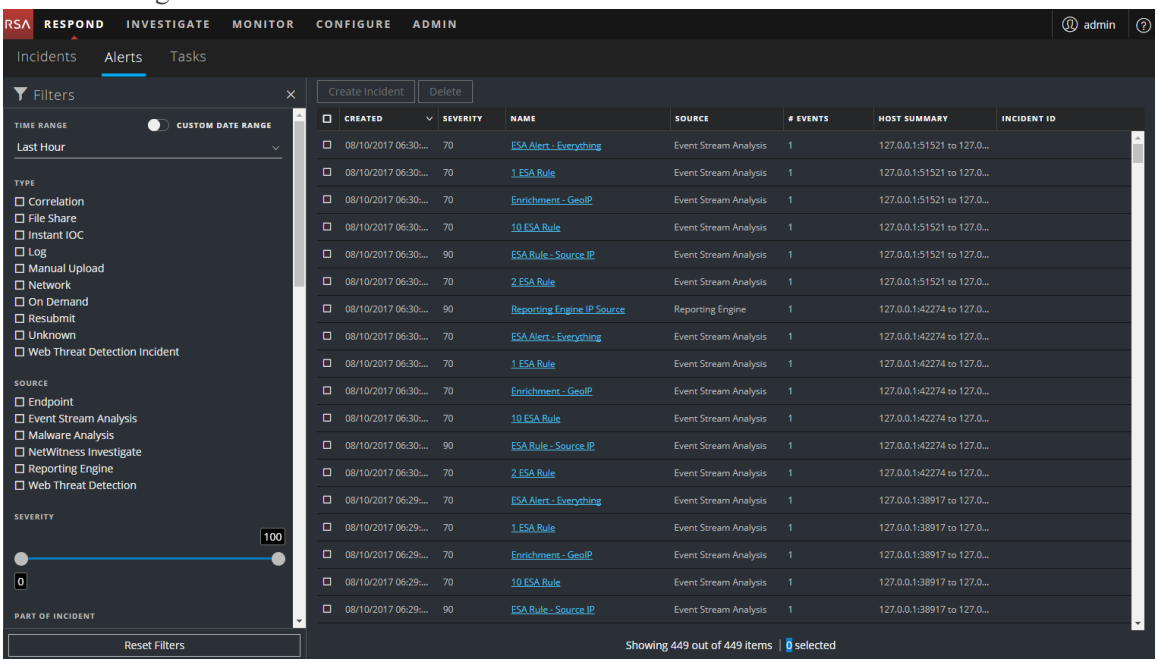
Die Registerkarte Services aktualisiert Statistiken nicht automatisch, es sei denn, Sie aktivieren oder deaktivieren eine Regel. So sorgen Sie dafür, dass die aktuellen Statistiken angezeigt werden:

1. Klicken Sie in der oberen rechten Ecke auf  , um die Informationen zu aktualisieren.
2. Zeigen Sie die aktualisierten Kundeninformationen an.

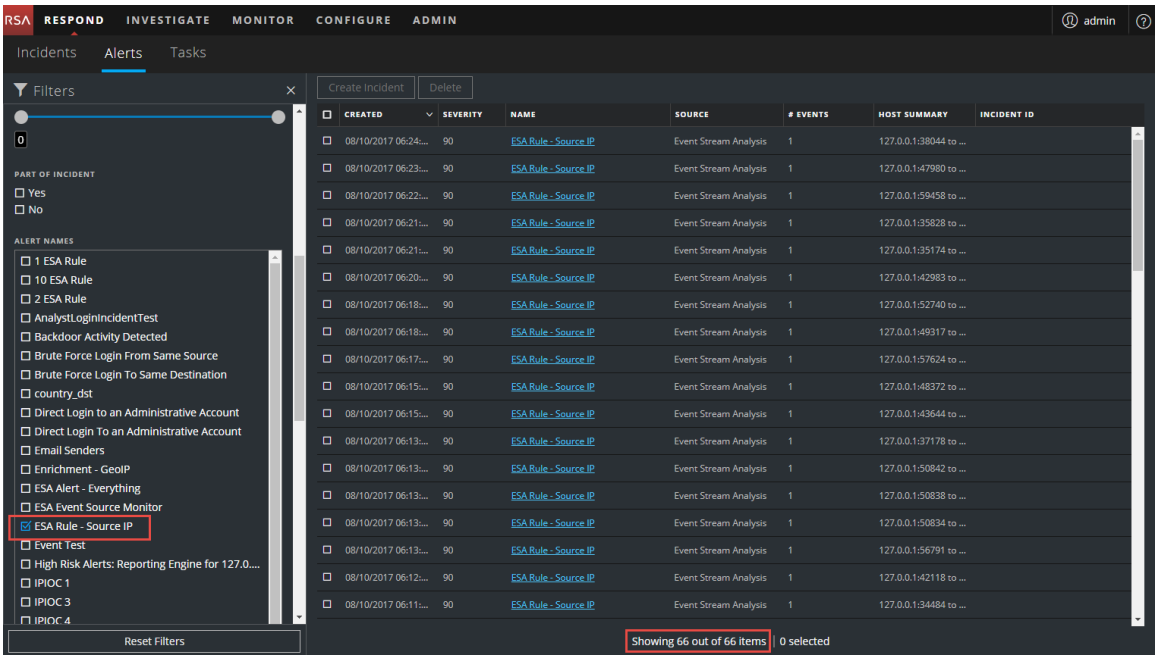
Anzeigen einer Zusammenfassung der Warnmeldungen

In der Ansicht Reagieren anzeigen können Sie verschiedene Warnmeldungen aus mehreren Quellen durchsuchen. Sie können die Liste der Warnmeldungen filtern, um nur Warnmeldungen von Interesse anzuzeigen, z. B. nach Name der Warnmeldung, Warnmeldungsquelle und bestimmtem Zeitraum.

1. Navigieren Sie zu **Reagieren > Warnmeldungen**.
   Die Listenansicht „Reaktionen auf Warnmeldungen“ zeigt eine Liste aller NetWitness Suite-Warnmeldungen.



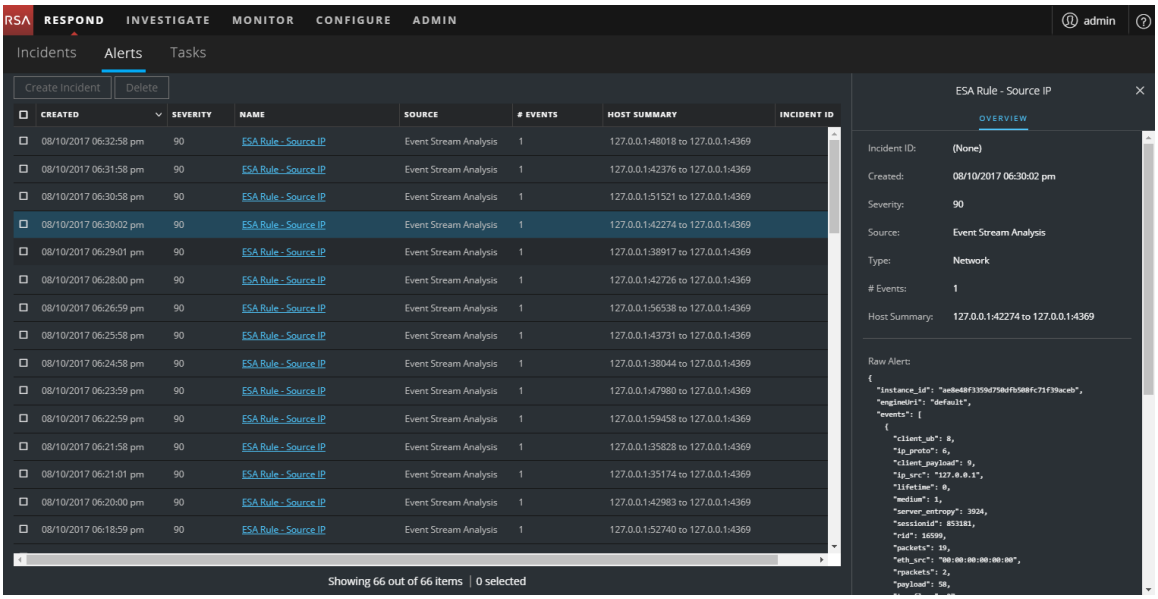
2. Im Bereich **Filter** auf der linken Seite können Sie die Liste „Warnmeldungen“ filtern, um bestimmte Warnmeldungen für einen bestimmten Zeitraum anzuzeigen. Beispielsweise können Sie im Bereich „WARNMELDUNGSNAMEN“ eine Warnmeldung für eine ESA-Regel auswählen, z. B. ESA-Regel – Quell-IP, und für den ZEITRAHMEN „Letzte Stunde“ beibehalten.
   Die Liste „Warnmeldungen“ auf der rechten Seite zeigt eine Liste der Warnmeldungen, die Ihrer Filterauswahl entsprechen, zusammen mit der Anzahl der Warnmeldungen am unteren Rand der Liste der Warnmeldungen.



Die Liste „Warnmeldungen“ zeigt Informationen über die einzelnen Warnmeldungen.

- **Erstellt**: Zeigt das Datum und die Uhrzeit der Erstellung der Warnmeldung im Quellsystem an.
- **Schweregrad**: Zeigt den Schweregrad der Warnmeldung an. Mögliche Werte sind 1 bis 100.
- **Name**: Zeigt eine grundlegende Beschreibung der Warnmeldung an.
- **Quelle:** Zeigt die ursprüngliche Quelle der Warnmeldung an.
- **Anzahl an Ereignissen**: Zeigt die Anzahl an Ereignissen, die in einer Warnmeldung enthalten sind.
- **Hostzusammenfassung**: Zeigt Details des Hosts an, wie zum Beispiel den Hostnamen, von dem die Warnmeldung ausgelöst wurde.
- **Incident-ID**: Zeigt die Incident-ID der Warnmeldung an. Gibt es keine Incident-ID, gehört die Warnmeldung nicht zu einem Incident.

3. Klicken Sie auf eine Warnmeldung in der Liste, um einen **Übersichtsbereich** auf der rechten Seite zu öffnen, in dem Sie die Rohversion von Warnmeldungs-Metadaten anzeigen können.



Weitere Informationen zum Filtern von Warnmeldungen und Anzeigen von Details zu Warnmeldungen finden Sie im *NetWitness Respond-Benutzerhandbuch*.

ESA-Warnmeldungsreferenzen

Das Modul „Warnmeldungen“ dient zur Konfiguration und Bereitstellung von ESA-Regeln, die Sie über potenzielle Netzwerkbedrohungen informieren.

In diesen Themen wird die Benutzeroberfläche des Moduls „Warnmeldungen“ erläutert.

Registerkarte „Neue erweiterte EPL-Regel“

Auf der Registerkarte „Erweiterte EPL-Regel“ können Sie Regelkriterien mit einer EPL-Abfrage (Event Processing Language) definieren.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Eine erweiterte EPL-Regel definieren	Hinzufügen einer erweiterten EPL-Regel
Contentexperte	Sehen Sie sich Beispiele für eine erweiterte EPL-Regel an.	Beispiele für erweiterte EPL-Regeln

Verwandte Themen

- Hinzufügen einer Regelerstellungsregel
- Erweiterungsquellen

Erweiterte EPL-Regel

So greifen Sie auf die Registerkarte „Erweiterte EPL-Regel“ zu:

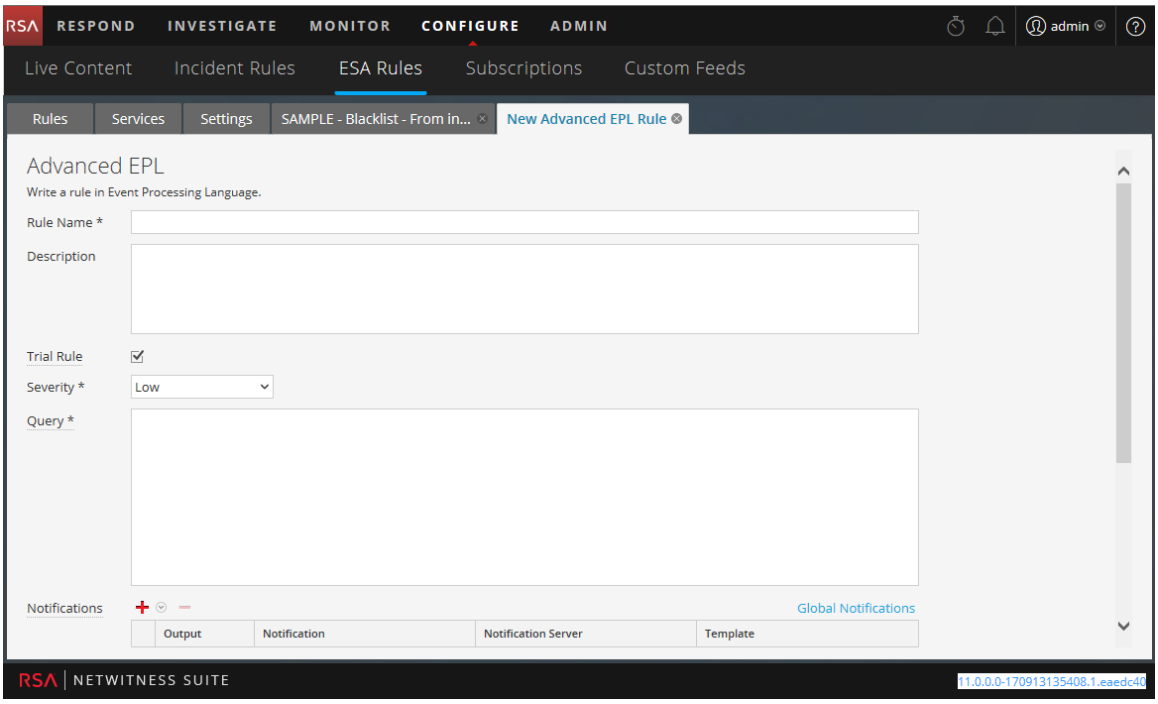
1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.

   Die Ansicht Konfigurieren wird standardmäßig mit geöffneter Registerkarte Regeln angezeigt.

2. Wählen Sie in der Symbolleiste **Regelbibliothek** die Option  **>Erweiterte EPL** aus.

   Die Registerkarte Erweiterte EPL-Regel wird angezeigt.

Unten sehen Sie einen Screenshot der Registerkarte Erweiterte EPL-Regel.



In der folgenden Tabelle sind die Parameter der Registerkarte Erweiterte EPL-Regel aufgeführt.

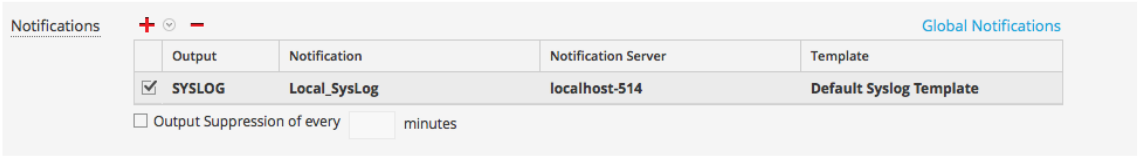
Parameter	Beschreibung
Name der Regel	Zweck der ESA-Regel
Beschreibung	Zusammenfassung dessen, was die ESA-Regel erkennt
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung
Abfrage	EPL-Abfrage, die die Regelkriterien definiert

Benachrichtigungen

Im Abschnitt „Benachrichtigungen“ können Sie auswählen, wie Sie benachrichtigt werden, wenn ESA eine Warnmeldung für die Regel erzeugt.

Weitere Informationen zu Warnmeldungsbenachrichtigungen erhalten Sie unter Hinzufügen einer Benachrichtigungsmethode zu einer Regel.

Die folgende Abbildung zeigt den Abschnitt Benachrichtigungen.



Parameter	Beschreibung
+	So fügen Sie einen Warnmeldungsbenachrichtigungstyp hinzu.
−	So löschen Sie den ausgewählten Warnmeldungsbenachrichtigungstyp.
Ausgabe	Typ der Warnmeldungsbenachrichtigung Optionen: • E-Mail • SNMP • Syslog • Skript
Benachrichtigung	Name der zuvor konfigurierten Ausgabe, beispielsweise ein E-Mail-Verteiler
Benachrichtigungsserver	Name des die Ausgabe sendenden Servers
Vorlage	Name der Vorlage für die Warnmeldungsbenachrichtigung
Ausgabeunterdrückung alle	Option zur Spezifizierung der Warnmeldungshäufigkeit
Minuten	Warnmeldungshäufigkeit in Minuten

Erweiterung

Im Abschnitt „Erweiterung“ können Sie einer Regel eine Datenerweiterungsquelle hinzufügen.

Weitere Informationen zu Erweiterungen erhalten Sie unter Hinzufügen einer Erweiterung zu einer Regel.
In der folgenden Abbildung wird der Abschnitt „Erweiterungen“ dargestellt.

Parameter	Beschreibung
+	So fügen Sie eine Erweiterung hinzu.
−	So löschen Sie eine ausgewählte Erweiterung.
Ausgabe	Erweiterungsquellentyp Optionen: • In-Memory-Tabelle • Externer DB-Verweis • Warehouse Analytics • GeoIP
Erweiterungsquelle	Name der zuvor konfigurierten Erweiterungsquelle, z. B. ein .CSV-Dateiname einer In-Memory-Tabelle
ESA Ereignis-Stream-Metadaten	ESA-Metaschlüssel, der als ein Operand der Verknüpfungsbedingung verwendet wird
Spaltenname „Erweiterungsquelle“	Erweiterungsquellen-Spaltenname, dessen Wert als ein weiterer Operand der Verknüpfungsbedingung verwendet wird

Dialogfeld „Anweisung erstellen“

Das Dialogfeld „Anweisung erstellen“ ermöglicht das Zusammenstellen einer Bedingungsanweisung, wenn eine neue Regelerstellungsregel erstellt wird.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Eine Regelanweisung konfigurieren.	Hinzufügen einer erweiterten EPL-Regel
Contentexperte	Bedingungen zu der Regel hinzufügen.	Schritt 3. Hinzufügen von Bedingungen zu einer Regelanweisung

Verwandte Themen

- Hinzufügen einer Regelerstellungsregel

Dialogfeld „Anweisung erstellen“

So greifen Sie auf das Dialogfeld „Anweisung erstellen“ zu:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.

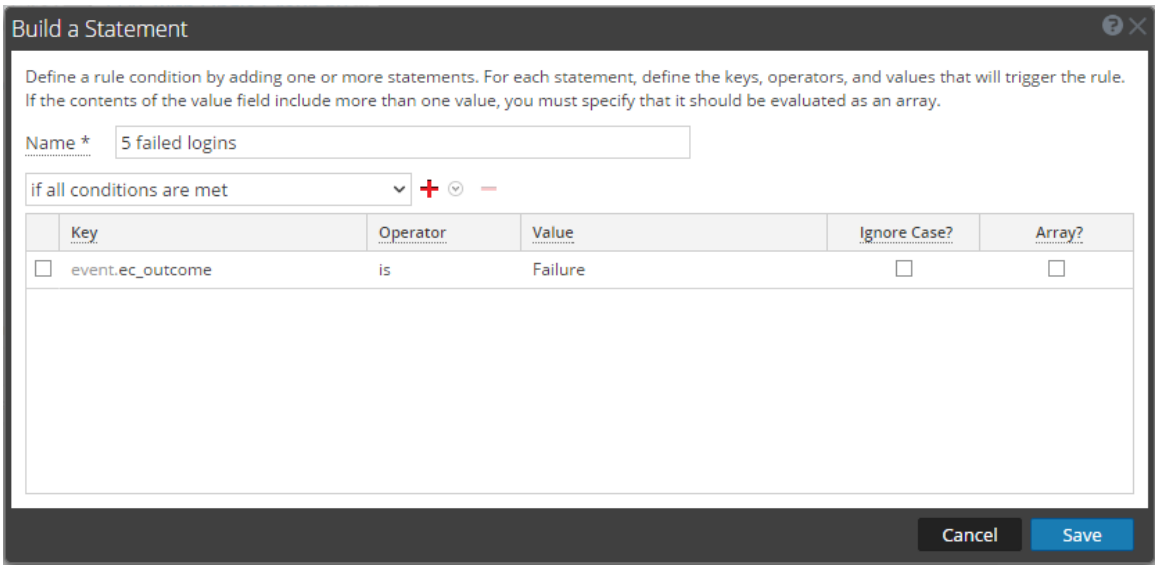
   Die Ansicht „ESA-Regeln konfigurieren“ wird mit geöffneter Registerkarte „Regeln“ angezeigt.

2. Wählen Sie in der Symbolleiste **Regelbibliothek** die Optionen  **> Regelerstellung** aus.

   Die Registerkarte „Neue Regel“ wird angezeigt.

3. Klicken Sie im Abschnitt **Bedingungen** auf  .

   Das Dialogfeld „Anweisung erstellen“ wird angezeigt.



In der folgenden Tabelle werden die Parameter im Dialogfeld „Anweisung erstellen“ beschrieben.

Parameter	Beschreibung
Name	Zweck der Anweisung
Auswählen	Bedingungen, die die Regel erfordert Es gibt zwei Optionen: • Alle Bedingungen sind erfüllt • Keine der Bedingungen ist erfüllt
Schlüssel	Schlüssel, den ESA in der Regelanweisung überprüfen soll

Parameter	Beschreibung
Evaluierungstyp	Beziehung zwischen dem Metaschlüssel und dem Wert für den Schlüssel: • is • ist nicht • ist nicht null • größer als (>) • ist größer als oder gleich (>=) • ist kleiner als (<) • ist kleiner als oder gleich (<=) • enthält • enthält nicht • beginnt mit • endet in
Wert	Wert, nach dem ESA in dem Schlüssel sucht
Groß-/Kleinschreibung ignorieren?	Dieses Feld wurde für die Verwendung mit Zeichenfolgen- und Array-von-Zeichenfolgenwerten entworfen. Indem Sie das Feld **Groß-/Kleinschreibung ignorieren** auswählen, wird die Abfrage den ganzen Text der Zeichenfolge als Wert in Kleinbuchstaben behandeln. Dadurch wird sichergestellt, dass eine Regel, die nach einem Benutzer namens „Johnson“ sucht, Ereignisse auch dann findet,wenn sie „johnson“, „JOHNSON“ oder „JoHnSoN“ enthalten.
Array?	Auswahl zur Angabe, ob die Inhalte des Felds Wert für einen oder mehrere Werte stehen: • Aktivieren Sie das Kontrollkästchen, wenn mehrere Werte angegeben werden. • Deaktivieren Sie das Kontrollkästchen, wenn nur ein Wert angegeben wird.
+	Fügt eine Anweisung hinzu Sie können ein Metabedingung, eine Whitelist-Bedingung oder eine Blacklist-Bedingung hinzufügen.
−	Löscht die ausgewählte Anweisung

Parameter	Beschreibung
Speichern	Fügt eine Anweisung zum Abschnitt Bedingungen der Registerkarte Regelerstellung hinzu.

Die folgende Tabelle zeigt die Operatoren, die Sie bei der Regelerstellung verwenden können:

Operator	Erforderlicher Wert	Verwendung	Beispiel	Bedeutung
is	Einzelne-Zeichenfolge-Wert	Der Metaschlüssel entspricht dem Feld *Wert*.	***user_dst*** ist „John Doe“.	***user_dst*** ist gleich der Zeichenfolge *„John Doe“*.
is	Array-Zeichenfolge-Wert	Der Metaschlüssel ist gleich einem der Elemente des Felds *Wert*.	*user_dst* ist „John Doe“, „Smith“.	*user_dst* ist entweder gleich der Zeichenfolge *„John“* oder der Zeichenfolge *„Doe“* oder der Zeichenfolge *„Smith*“ (beachten Sie, dass die Leerzeichen entfernt werden).
ist nicht	Einzelne-Zeichenfolge-Wert	Der Metaschlüssel entspricht nicht dem Feld *Wert*.	***Größe*** ist nicht 200.	***Größe*** ist nicht gleich der Anzahl 200 („Größe“ ist ein numerischer Wert).
ist nicht	Array-Zeichenfolge-Wert	Der Metaschlüssel ist nicht gleich einem der Elemente des Felds *Wert*.	***Größe*** ist nicht 200, 300, 400.	***Größe*** ist weder gleich *200* noch gleich *300* noch gleich *400*.
ist nicht null	– (sucht nach jedem Wert)	Der Metaschlüsselwert ist nicht null.	***user_dst*** ist nicht null.	***user_dst*** ist ein Metadatum, das einen Wert enthält.
größer als (>)	Anzahl	Der numerische Wert des Metaschlüssels ist größer als die Anzahl im Feld *Wert*.	***payload*** ist größer als 7000.	***payload*** ist ein numerischer Wert, der größer als 7000 ist.
ist größer als oder gleich (>=)	Anzahl	Der numerische Wert des Metaschlüssels ist größer als oder gleich der Anzahl im Feld *Wert*.	***payload*** ist größer als oder gleich 7000.	***payload*** ist ein numerischer Wert, der größer als oder gleich 7000 ist.
ist kleiner als (<)	Anzahl	Der numerische Wert des Metaschlüssels ist kleiner als die Anzahl im Feld *Wert*.	***ip_dstport*** ist kleiner als 1024.	***ip_dstport*** ist ein numerischer Wert, der kleiner ist als der numerische Wert 1024.

Operator	Erforderlicher Wert	Verwendung	Beispiel	Bedeutung
ist kleiner als oder gleich (<=)	Anzahl	Der numerische Wert des Metaschlüssels ist kleiner als oder gleich der Anzahl im Feld *Wert*.	***ip_dstport*** ist kleiner als oder gleich 1024.	***ip_dstport*** ist ein numerischer Wert, der kleiner als oder gleich dem numerischen Wert 1024 ist.
enthält	Zeichenfolge	Das Feld *Wert* ist eine Teilzeichenfolge des Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	***ec_outcome*** enthält „failure“.	***ec_outcome*** ist eine Zeichenfolge, die die Teilzeichenfolge *„failure“ enthält.*
enthält nicht	Zeichenfolge	Das Feld *Wert* ist nicht eine Teilzeichenfolge des Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	***ec_outcome*** enthält nicht „failure“.	***ec_outcome*** ist eine Zeichenfolge, die nicht die Teilzeichenfolge *„failure“ enthält.*
beginnt mit	Zeichenfolge	Das Feld *Wert* ist der Anfang eines Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	***ip_dst*** beginnt mit 127.0.	***ip_dst*** ist eine Zeichenfolge, die mit *„127.0“ beginnt.*
endet in	Zeichenfolge	Das Feld *Wert* ist das Ende eines Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	***user_dst*** endet auf „son“.	***user_dst*** ist eine Zeichenfolge, die auf *„son“ endet.*

Hinweis: Ausdrücke in ***fett kursiv*** sind Metadaten, die möglicherweise nicht in allen Kundenumgebungen vorhanden sind.

Dialogfeld „ESA-Regeln bereitstellen“

Im Dialogfeld ESA-Regeln bereitstellen können Sie Regeln für die Bereitstellung eines ESA-Services filtern und auswählen.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Eine Bereitstellung konfigurieren	Schritt 1. Hinzufügen einer Bereitstellung
Contentexperte	Regel bereitstellen	Schritt 3. Hinzufügen und Bereitstellen von Regeln

Verwandte Themen

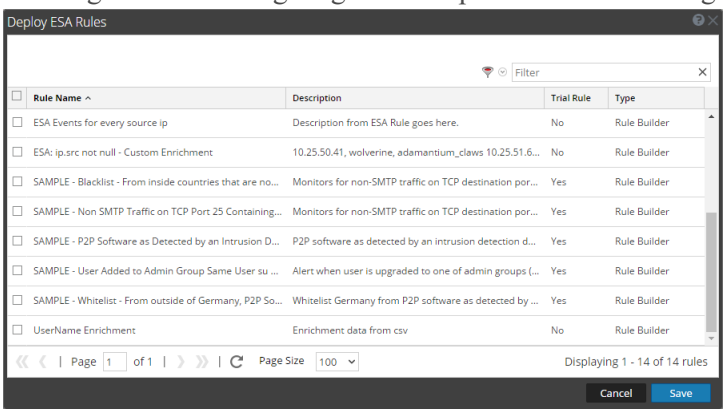
- Zusätzliche Bereitstellungsverfahren

Dialogfeld „ESA-Regeln bereitstellen“

So rufen Sie dieses Dialogfeld auf:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte „Regeln“ wird standardmäßig geöffnet.
2. Wählen Sie im Bereich „Optionen“ im Abschnitt **Bereitstellung** eine Bereitstellung aus.
   Alternativ können Sie durch Klicken auf  **> Hinzufügen** eine neue Bereitstellung hinzufügen.
3. Wenn Sie eine neue Bereitstellung hinzufügen: Geben Sie den Namen der Bereitstellung in das entsprechende Feld im Bereich „Optionen“ ein.
4. Klicken Sie im Bereich **ESA-Regeln** auf  .
   Das Dialogfeld „ESA-Regeln bereitstellen“ wird angezeigt.

Die folgende Abbildung zeigt ein Beispiel für dieses Dialogfeld.



In der folgenden Tabelle werden die Parameter im Dialogfeld „ESA-Regeln bereitstellen“ beschrieben.

Parameter	Beschreibung
	Filtert die Regelliste nach Schweregrad und Typ. Das Textfeld neben diesem Symbol filtert nach Regelname.
Name der Regel	Zeigt den Namen einer Regel an.
Beschreibung	Beschreibt die Regel.
Testregel	Gibt an, ob die Regel eine Testregel ist.
Typ	Zeigt den Typ der Regel an: RSA Live ESA-Regel, Erweiterte EPL-Regel oder Regelerstellungsregel.

Dialogfeld „ESA-Services bereitstellen“

Im Dialogfeld „ESA-Services bereitstellen“ werden alle verfügbaren ESA-Services angezeigt, die einer Bereitstellung hinzugefügt werden können.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Eine Bereitstellung konfigurieren	Schritt 1. Hinzufügen einer Bereitstellung
Contentexperte	Einen Service bereitstellen	Schritt 2. Hinzufügen eines ESA-Services

Verwandte Themen

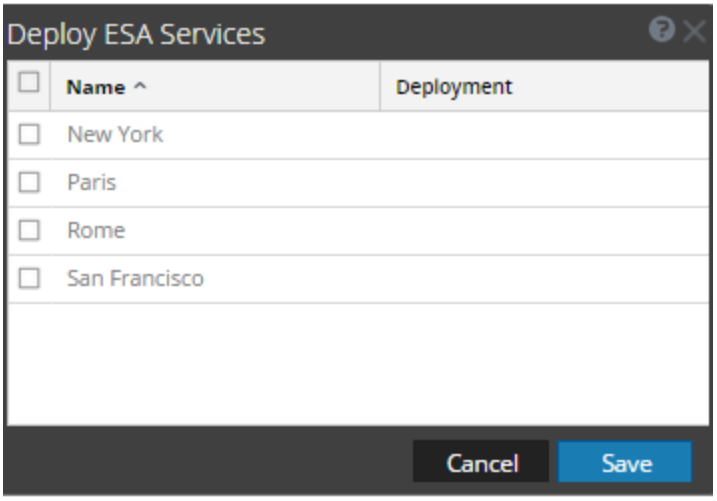
- Zusätzliche Bereitstellungsverfahren
- Anzeigen der Statistiken zu einem ESA-Service

Dialogfeld „ESA-Services bereitstellen“

So rufen Sie dieses Dialogfeld auf:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte „Regeln“ wird standardmäßig geöffnet.
2. Wählen Sie im Bereich „Optionen“ im Abschnitt **Bereitstellungen** eine Bereitstellung aus oder fügen Sie eine hinzu.
3. Klicken Sie im Bereich **ESA-Services** auf  .
   Das Dialogfeld „ESA-Services bereitstellen“ wird angezeigt.

Die folgende Abbildung zeigt ein Beispiel für dieses Dialogfeld.



In der folgenden Tabelle werden die Parameter im Dialogfeld „ESA-Services bereitstellen“ beschrieben.

Parameter	Beschreibung
Name	Zeigt die Namen von konfigurierten ESA-Services an.
Bereitstellung	Zeigt die Bereitstellungen an, für die der Service schon hinzugefügt wurde.

Registerkarte Regelerstellung

Auf der Registerkarte „Regelerstellung“ können Sie eine Regelerstellungsregel definieren.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Regelerstellungsregel definieren	Hinzufügen einer Regelerstellungsregel
Contentexperte	Regelkriterien definieren	Schritt 2. Erstellen einer Regelanweisung
Contentexperte	Bedingungen zu einer Regel hinzufügen	Schritt 3. Hinzufügen von Bedingungen zu einer Regelanweisung

Verwandte Themen

- Hinzufügen einer erweiterten EPL-Regel

Regelerstellung

So greifen Sie auf die Registerkarte Regelerstellung zu:

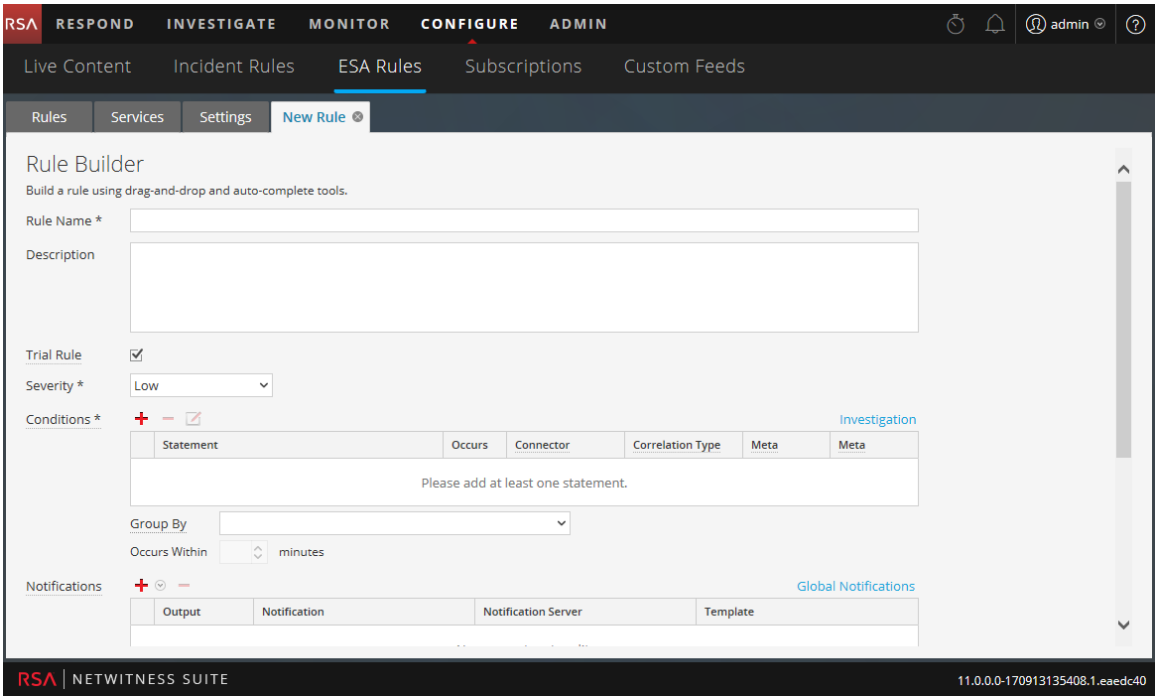
1. Navigieren Sie zu **Konfigurieren** > **ESA-Regeln**.

   Die Registerkarte „Regeln“ wird standardmäßig geöffnet.

2. Wählen Sie in der Symbolleiste **Regelbibliothek** die Optionen  > **Regelerstellung** aus.

   Die Registerkarte „Regelerstellung“ wird angezeigt.

Die folgende Abbildung zeigt die Registerkarte „Regelerstellung“.



In der folgenden Tabelle sind die Parameter auf der Registerkarte „Regelerstellung“ beschrieben.

Parameter	Beschreibung
Name der Regel	Zweck der ESA-Regel
Beschreibung	Zusammenfassung dessen, was die ESA-Regel erkennt

Parameter	Beschreibung
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung

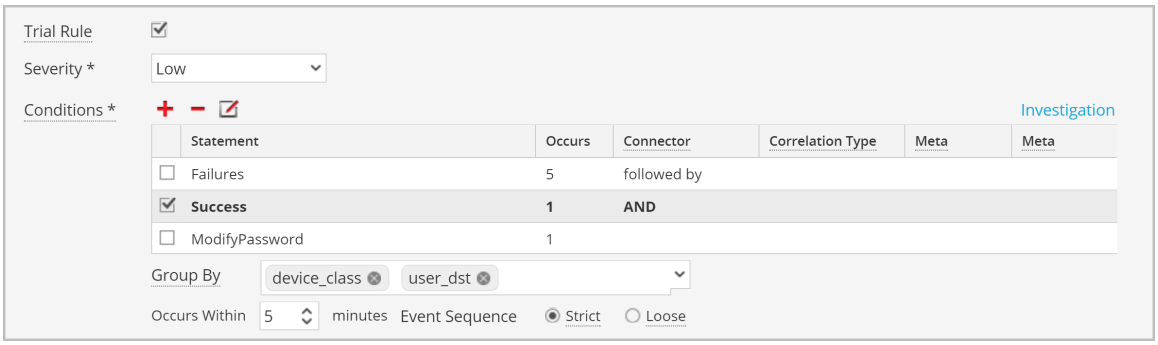
Die „Regelerstellung“ umfasst die folgenden Komponenten:

- Abschnitt Bedingungen
- Abschnitt Meldungen
- Abschnitt Erweiterungen

Abschnitt Bedingungen

Im Abschnitt „Bedingungen“ der Registerkarte „Regelerstellung“ definieren Sie, was die Regel erkennt.

Die folgende Abbildung zeigt den Abschnitt „Bedingungen“.



In der folgenden Tabelle sind die Parameter im Abschnitt „Bedingungen“ aufgelistet.

Parameter	Beschreibung
+	Fügt eine Anweisung hinzu
−	Ausgewählte Anweisung löschen.
✎	Ausgewählte Anweisung bearbeiten.
Anweisung	Logische Gruppe von Bedingungen für eine Operation.

Parameter	Beschreibung
Tritt auf	Warnmeldungshäufigkeit bei erfüllter Bedingung. Dies gibt an, dass eine bestimmte Mindestanzahl von Ereignissen vorhanden sein muss, damit die Kriterien zum Auslösen einer Warnmeldung erfüllt sind. Das Minutenzeitfenster bindet den Tritt auf-Zähler.
Connector	Optionen zur Spezifizierung der Beziehung zwischen Anweisungen: • gefolgt von • nicht gefolgt von • UND • ODER Der Connector verbindet zwei Anweisungen mit „UND“, „ODER“, „gefolgt von“ oder „nicht gefolgt von“. Wenn gefolgt von verwendet wird, wird angegeben, dass es eine Sequenz dieser Ereignisse gibt. UND und ODER erstellen ein großes Kriterium. Die Option „gefolgt von“ erstellt verschiedene Kriterien, die in einer bestimmten Reihenfolge auftreten.
Korrelationstyp	Der Parameter **Korrelationstyp** gilt nur für **gefolgt von** und **nicht gefolgt von**. Wenn Sie den Korrelationstyp „GLEICH“ auswählen, wählen Sie einen Metawert für die Korrelation, und wenn Sie den Korrelationstyp „VERKNÜPFEN“ auswählen, wählen Sie zwei Metawerte für die Korrelation. Sie möchten möglicherweise „VERKNÜPFEN“ verwenden, wenn Sie versuchen, Metawerte aus zwei verschiedenen Datenquellen zu korrelieren. Angenommen, Sie möchten eine AV-Warnmeldung mit einer IDS-Warnmeldung korrelieren.
Meta	Die Metabedingung muss angegeben werden, wenn Sie den Korrelationstyp „GLEICH“ oder „VERKNÜPFEN“ auswählen (siehe oben).
Meta	Die zweite Metabedingung muss angegeben werden, wenn Sie den Korrelationstyp „VERKNÜPFEN“ ausgewählt haben (siehe oben). Beispiel: Die Ziel-IP-Adresse aus der AV-Warnmeldung und die Quell-IP-Adresse der Workstation aus der IDS-Warnmeldung werden verknüpft, damit Sie dieselben Einheiten quellübergreifend anzeigen können.

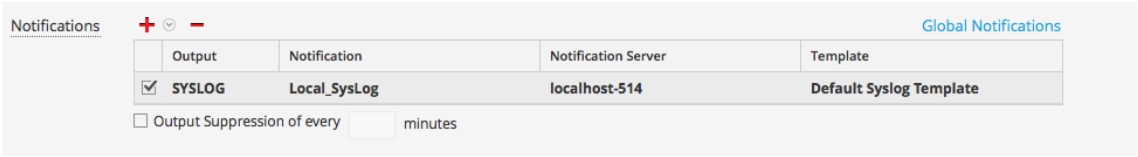
Parameter	Beschreibung
tritt innerhalb von Minuten auf	Zeitfenster, innerhalb dessen die Bedingungen auftreten müssen.
Ereignissequenz	Wählen Sie aus, ob das Muster einer *strengen* oder einer *variablen* Übereinstimmung folgen muss. Wenn Sie eine strenge Übereinstimmung angeben, bedeutet dies, dass das Muster in der *genauen* Reihenfolge vorkommen muss, die Sie angegeben haben, ohne dass weitere Ereignisse dazwischen vorkommen. Beispiel: Wenn als Sequenz fünf fehlgeschlagene Anmeldungen (F) gefolgt von einer erfolgreichen Anmeldung (S) angegeben ist, wird dieses Muster nur übereinstimmen, wenn der Benutzer die folgende Sequenz ausführt: F, F, F, F, F, S. Wenn Sie eine variable Übereinstimmung angeben, bedeutet dies, dass andere Ereignisse innerhalb der Sequenz auftreten dürfen, aber die Regel wird weiterhin auslösen, wenn alle angegebenen Ereignisse auch auftreten. Beispiel: Fünf fehlgeschlagene Anmeldeversuche (F), gefolgt von einer beliebigen Anzahl dazwischen liegender erfolgreicher Anmeldeversuche (S), gefolgt von einem erfolgreichen Anmeldeversuch, könnten das folgende Muster erzeugen: F, S, F, S, F, S, F, S, F, S, die die Regel trotz der dazwischenliegenden erfolgreichen Anmeldungen auslösen würden.
Gruppieren nach	Wählen Sie den Metaschlüssel aus, nach dem die Ergebnisse aus der Drop-down-Liste gruppiert werden sollen. Nehmen Sie zum Beispiel an, es gibt die drei Benutzer Joe, Jane und John und Sie verwenden das Metadatum „Gruppieren nach“, **user_dst** („user_dst“ ist das Metadatenfeld für das Benutzerzielkonto). Das Ergebnis zeigt Ereignisse gruppiert nach den Benutzerzielkonten, Joe, Jane und John, an. Sie können auch nach mehreren Schlüsseln gruppieren. Beispielsweise möchten Sie eventuell nach Benutzern und Computern gruppieren, um zu sehen, ob ein Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden. Um dies zu erreichen, können Sie nach „device_class“ und „user_dst“ gruppieren.

Benachrichtigungen

Im Abschnitt „Benachrichtigungen“ können Sie auswählen, wie Sie benachrichtigt werden, wenn ESA eine Warnmeldung für die Regel erzeugt.

Weitere Informationen zu Warnmeldungsbenachrichtigungen erhalten Sie unter Hinzufügen einer Benachrichtigungsmethode zu einer Regel.

Die folgende Abbildung zeigt den Abschnitt „Benachrichtigungen“.



Parameter	Beschreibung
	So fügen Sie einen Warnmeldungsbenachrichtigungstyp hinzu.
	So löschen Sie die ausgewählte Warnbenachrichtigung.
Ausgabe	Typ der Warnmeldungsbenachrichtigung Optionen: • E-Mail • SNMP • Syslog • Skript
Benachrichtigung	Name der zuvor konfigurierten Ausgabe, beispielsweise ein E-Mail-Verteiler
Benachrichtigungsserver	Name des die Ausgabe sendenden Servers
Vorlage	Name der Vorlage für die Warnmeldungsbenachrichtigung
Ausgabeunterdrückung alle	Option zur Spezifizierung der Warnmeldungshäufigkeit
Minuten	Warnmeldungshäufigkeit in Minuten

Erweiterung

Im Abschnitt Erweiterung können Sie einer Regel eine Datenerweiterungsquelle hinzufügen.

Weitere Informationen zu Erweiterungen erhalten Sie unter Hinzufügen einer Erweiterung zu einer Regel.

In der folgenden Abbildung wird der Abschnitt Erweiterungen dargestellt.

Parameter	Beschreibung
+	So fügen Sie eine Erweiterung hinzu.
−	So löschen Sie eine ausgewählte Erweiterung.
Ausgabe	Erweiterungsquellentyp Optionen: • In-Memory-Tabelle • Externer DB-Verweis • Warehouse Analytics • GeoIP
Erweiterungsquelle	Name der zuvor konfigurierten Erweiterungsquelle, z. B. ein .CSV-Dateiname einer In-Memory-Tabelle
ESA Ereignis-Stream-Metadaten	ESA-Metaschlüssel, der als ein Operand der Verknüpfungsbedingung verwendet wird
Spaltenname „Erweiterungsquelle“	Erweiterungsquellen-Spaltenname, dessen Wert als ein weiterer Operand der Verknüpfungsbedingung verwendet wird Für eine In-Memory-Tabelle gilt, wenn Sie beim Erstellen einer CSV-basierten Erweiterung einen Schlüssel konfiguriert haben, wird diese Spalte mit dem ausgewählten Schlüssel automatisch ausgefüllt. Allerdings können Sie es nach Wunsch ändern. Für eine GeoIP-Erweiterungsquelle wird ipv4 automatisch ausgewählt.

Registerkarte Regeln

Auf der Registerkarte „Regeln“ können Sie ESA-Regeln und -Bereitstellungen managen.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Regeltypen anzeigen	ESA-Regeltypen
Contentexperte	Testregeln bereitstellen	Verwenden von Testregeln
Contentexperte	Regel erstellen	Hinzufügen von Regeln zur Regelbibliothek
Contentexperte	Regel bereitstellen	Bereitstellen von Regeln für die Ausführung in ESA

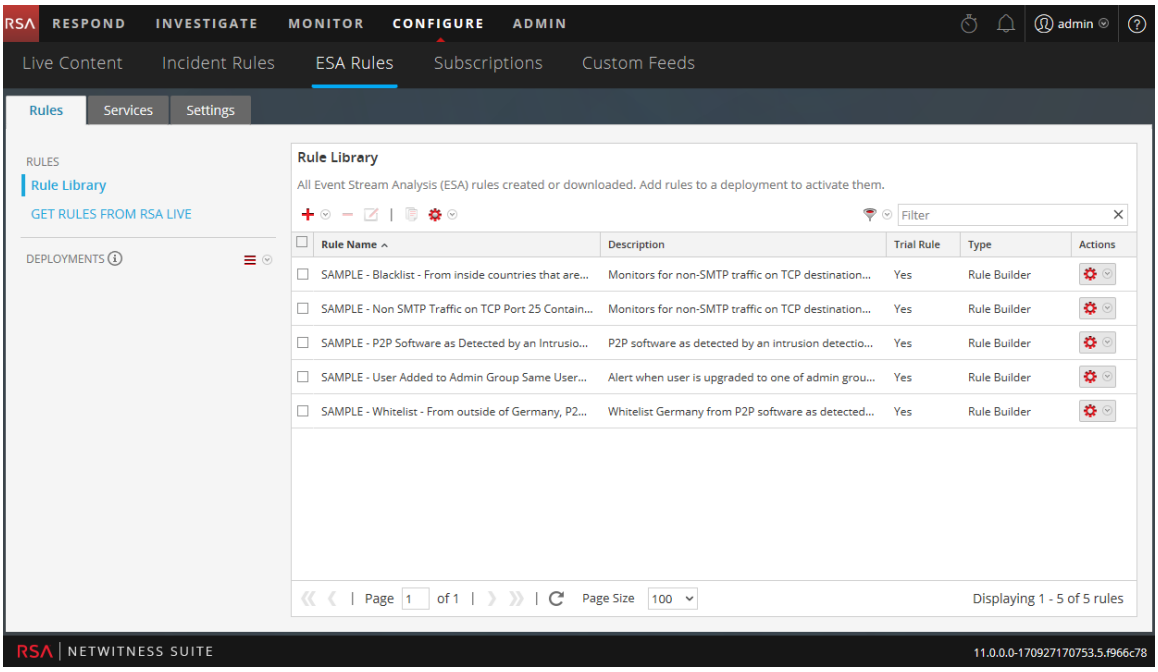
Verwandte Themen

- Erste Schritte mit ESA

Regelerstellung

Die Registerkarte „Regeln“ wird angezeigt, wenn Sie auf **Konfigurieren > ESA-Regeln** klicken.

Die folgende Abbildung zeigt die Registerkarte „Regeln“.



Die Registerkarte „Regeln“ ist in drei Bereiche unterteilt:

- Bereich „Optionen“ der Registerkarte „Regeln“
- Bereich „Regelbibliothek“
- Bereich „Bereitstellung“

Bereich „Optionen“ der Registerkarte „Regeln“

Im Bereich „Optionen“ der Registerkarte **Regeln** auf der linken Seite können Sie ESA-Regeln in der Regelbibliothek anzeigen und Bereitstellungen erstellen.

Was möchten Sie tun?

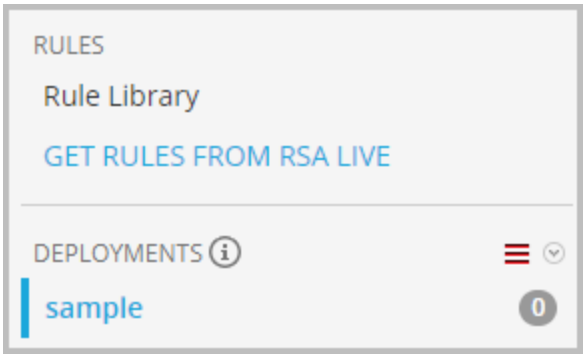
Rolle	Ziel	Details anzeigen
Contentexperte	Eine ESA-Regel anzeigen.	Hinzufügen von Regeln zur Regelbibliothek
Contentexperte	Eine Bereitstellung erstellen	Bereitstellungsschritte

Verwandte Themen

- Arbeiten mit Regeln

Bereich „Optionen“

In der folgenden Abbildung ist der Bereich „Optionen“ der Registerkarte **Regeln** dargestellt.



Der Bereich Optionen enthält zwei Abschnitte: Regeln und Bereitstellungen.

Abschnitt Regeln

Der Abschnitt „Regeln“ enthält zwei Optionen. Die Option **Regelbibliothek** ist standardmäßig aktiviert und wenn sie ausgewählt ist, wird die Ansicht „Regelbibliothek“ auf der Registerkarte angezeigt. Mit der Option **Regeln aus RSA Live abrufen** können Sie zur Ansicht „Live-Suche“ navigieren, in der Sie nach Regeln suchen können.

Abschnitt Bereitstellungen

Im Abschnitt Bereitstellungen werden Bereitstellungen aufgeführt und hierfür verfügbare Aktualisierungen angezeigt. In diesem Abschnitt können Bereitstellungen hinzugefügt, gelöscht, bearbeitet und aktualisiert werden. Durch Auswahl einer Bereitstellung aus der Liste wird der Bereich Bereitstellung auf der Registerkarte angezeigt. In der folgenden Tabelle werden die Funktionen dieses Abschnitts beschrieben.

Funktion	Beschreibung
	Öffnet ein Drop-down-Menü, mit dem Sie eine Bereitstellung hinzufügen, bearbeiten oder löschen können. Sie können auch die Liste der Bereitstellungen aktualisieren, um festzustellen, ob neue Aktualisierungen für die Liste vorhanden sind.
	Gibt an, ob neue Aktualisierungen für die Bereitstellung vorhanden sind.
	Gibt die Anzahl der Regeln in der Bereitstellung an.

Bereich „Regelbibliothek“

Im Bereich „Regelbibliothek“ können Sie Regeln managen.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Eine ESA-Regel hinzufügen.	Hinzufügen einer Regelerstellungsregel
Contentexperte	Eine Regel bearbeiten, duplizieren oder löschen.	Bearbeiten, Duplizieren oder Löschen einer Regel
Contentexperte	ESA-Regeln importieren oder exportieren.	Importieren oder Exportieren von Regeln
Contentexperte	Die ESA-Regelliste filtern.	Filtern oder Suchen von Regeln

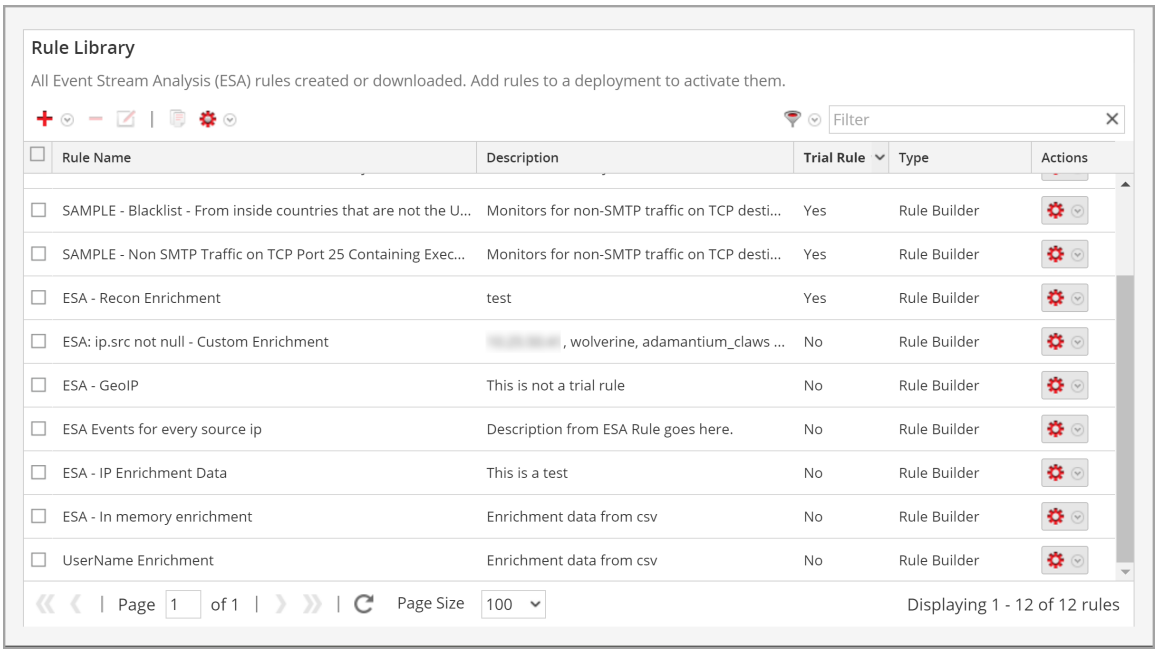
Verwandte Themen

- Hinzufügen einer erweiterten EPL-Regel

Bereich „Regelbibliothek“

Um auf diese Ansicht zuzugreifen, gehen Sie zu **Konfigurieren > ESA-Regeln**. Die Registerkarte „Regeln“ wird angezeigt und die Ansicht „Regelbibliothek“ befindet sich auf der rechten Seite.

Die folgende Abbildung zeigt die Liste „Regelbibliothek“.



Die Ansicht „Regelbibliothek“ enthält folgende Komponenten:

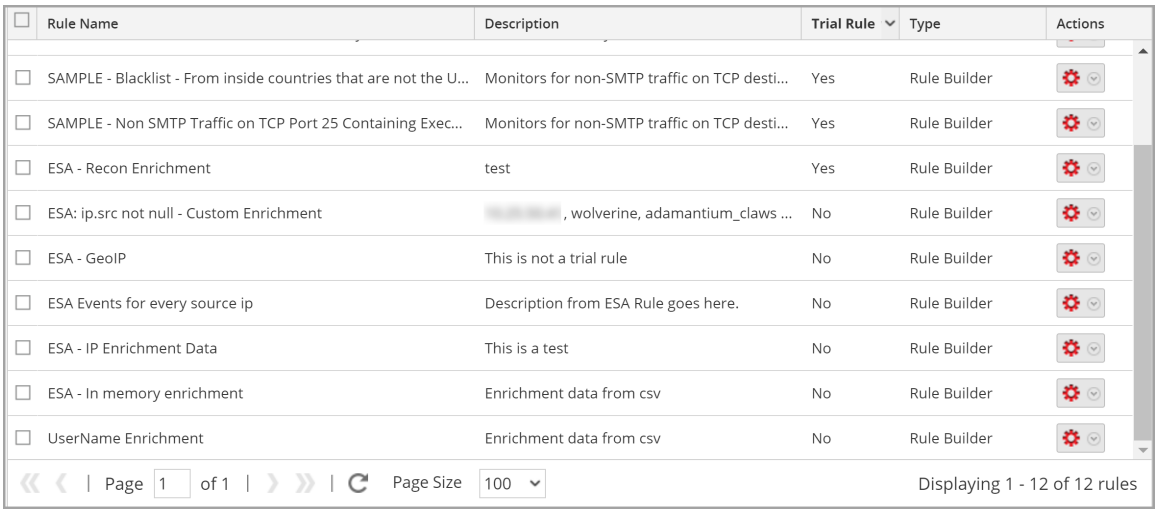
- Symbolleiste Regelbibliothek
- Regelbibliotheksliste

Symbolleiste Regelbibliothek

Über die Symbolleiste „Regelbibliothek“ können Sie ESA-Regeln hinzufügen, löschen, bearbeiten, duplizieren, filtern, exportieren und importieren.

Regelbibliotheksliste

Die folgende Abbildung zeigt die Liste „Regelbibliothek“.

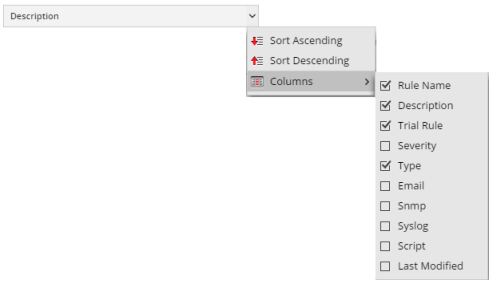


Die Liste „Regelbibliothek“ enthält alle ESA-Regeln, die von RSA Live heruntergeladen oder in den Registerkarten „Erweiterte EPL“ und „Regelerstellung“ erstellt wurden. In der folgenden Tabelle sind die verschiedenen Spalten der Liste „Regelbibliothek“ mit Beschreibung aufgelistet.

Spalte	Beschreibung
Name der Regel	Zweck der ESA-Regel
Beschreibung	Zusammenfassung dessen, was die ESA-Regel erkennt
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Typ	Der Typ der Regel
Aktionen (⚙)	Menü für das Löschen, Bearbeiten, Duplizieren oder Exportieren der ausgewählten Regel
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung
E-Mail	Gibt an, ob eine Warnbenachrichtigung für die Regel per E-Mail gesendet werden soll. Diese Spalte wird standardmäßig nicht angezeigt.
SNMP	Gibt an, ob eine Warnbenachrichtigung für die Regel über SNMP gesendet werden soll. Diese Spalte wird standardmäßig nicht angezeigt.

Spalte	Beschreibung
Syslog	Gibt an, ob eine Warnbenachrichtigung für die Regel über Syslog gesendet werden soll. Diese Spalte wird standardmäßig nicht angezeigt.
Skript	Gibt an, ob eine Warnbenachrichtigung für die Regel ein Skript ausführt. Diese Spalte wird standardmäßig nicht angezeigt.
Zuletzt geändert	Datum und Uhrzeit der letzten Änderung der ESA-Regel Diese Spalte wird standardmäßig nicht angezeigt.

Bewegen Sie die Maus über den Titel einer Spalte und klicken Sie rechts auf das **v**, um Spalten anzuzeigen, die nicht standardmäßig sichtbar sind. Dadurch wird ein Drop-down-Menü geöffnet, in dem Sie die Inhalte der Spalte sortieren oder wählen können, welche Spalten Sie in der Regelbibliotheksliste sehen möchten.



Bereich „Bereitstellung“

Dieses Thema bietet eine Übersicht über den Bereich „Bereitstellung“. In dem Bereich „Bereitstellung“ können Sie die Bereitstellungen erstellen und konfigurieren. Der Bereich „Bereitstellung“ umfasst folgende Abschnitte:

- ESA-Services
- ESA-Regeln

Was möchten Sie tun?

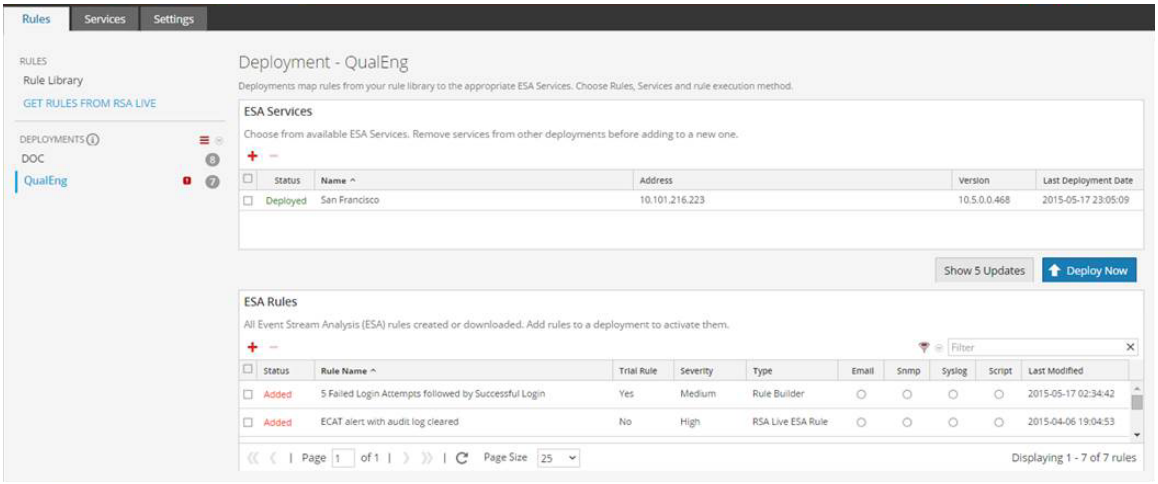
Rolle	Ziel	Details anzeigen
Contentexperte	Eine Bereitstellung hinzufügen.	Bereitstellungsschritte
Contentexperte	Bereitstellungen verwalten.	Zusätzliche Bereitstellungsverfahren

Verwandte Themen

- Anzeigen der Statistiken zu einem ESA-Service

Bereich „Bereitstellung“

Die folgende Abbildung zeigt den Bereich „Bereitstellung“.



ESA-Services

Im Abschnitt „ESA-Services“ können Sie die ESA-Services in der Bereitstellung managen.

Im Abschnitt ESA-Services können Sie die folgenden Aufgaben ausführen:

Aufgabe	Beschreibung
+	Mit diesem Symbol fügen Sie der Bereitstellung einen ESA-Service hinzu.
−	Der ausgewählte ESA-Service wird aus der Bereitstellung entfernt.
Updates anzeigen	Das Dialogfeld „Aktualisierungen an der Bereitstellung“ wird geöffnet.
Jetzt bereitstellen	Stellen Sie die aktuellen Regelsätze bereit.

In der folgenden Tabelle sind die Parameter im Abschnitt „ESA-Services“ aufgelistet.

Parameter	Beschreibung
Status	Zeigt an, ob der Bereitstellungsstatus **Hinzugefügt**, **Bereitgestellt**, **Aktualisiert** oder **Fehlgeschlagen** ist.
Name	Der Name des ESA-Service.
Adresse	Die IP-Adresse des Hosts, auf dem der ESA-Service installiert ist.
Version	Die Version des ESA-Service.
Datum der letzten Bereitstellung	Datum und Uhrzeit der letzten Bereitstellung des ESA-Services.

ESA-Regeln

Im Abschnitt ESA-Regeln managen Sie die Regeln in der Bereitstellung. In diesem Abschnitt sind alle Regel aufgeführt, die derzeit in der Bereitstellung vorhanden sind.

Im Abschnitt **ESA-Regeln** können Sie die folgenden Aufgaben ausführen.

Aufgabe	Beschreibung
+	Öffnet das Dialogfeld „ESA-Regeln bereitstellen“, in dem Sie eine Regel auswählen können.
−	Mit diesem Symbol werden die ausgewählten ESA-Regeln aus der Bereitstellung entfernt.

Aufgabe	Beschreibung
	Mit diesem Symbol filtern Sie die Regelliste.
	In diesem Feld können Sie nach einer Regel suchen.

In der folgenden Tabelle sind die Parameter des Abschnitts „ESA-Regeln“ aufgeführt.

Parameter	Beschreibung
Status	Gibt den Regelstatus an: • Bereitgestellt: Die Regel wurde bereitgestellt. • Aktualisiert: Die Regel wurde seit der letzten Bereitstellung aktualisiert. • Hinzugefügt: Die Regel wurde seit der letzten Bereitstellung hinzugefügt. • „Fehlgeschlagen“: Die Bereitstellung ist fehlgeschlagen.
Name der Regel	Zweck der ESA-Regel
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung
Ausgabe	Der Typ der ESA-Regel.
E-Mail, SNMP, Syslog, Skript	Gibt an, welche Benachrichtigungstypen für durch die Regeln erzeugte Warnmeldungen verwendet werden
Zuletzt geändert	Datum und Uhrzeit der letzten Änderung der ESA-Regel

Dialogfeld Regelsyntax

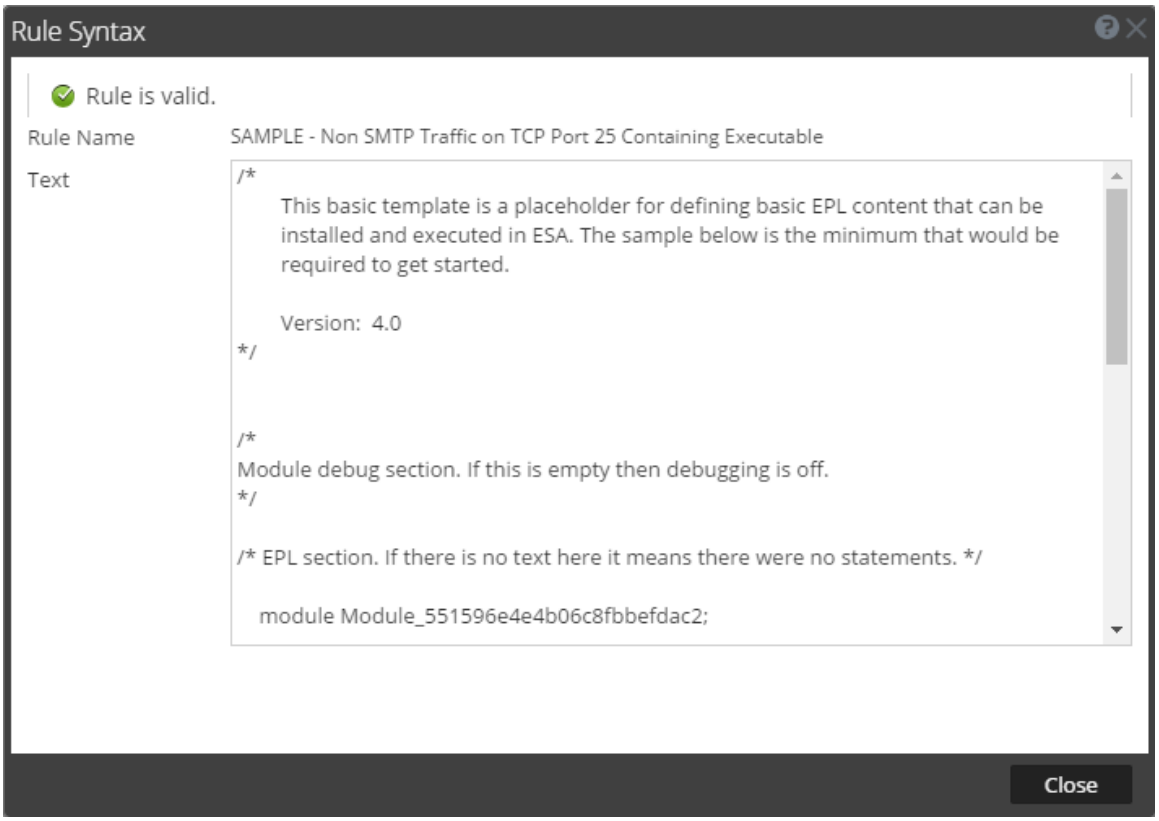
In diesem Thema werden die Funktionen des Dialogfelds Regelsyntax beschrieben. Im Dialogfeld „Regelsyntax“ wird die EPL-Syntax von Bedingungen, Anweisungen und Debugging-Parametern angezeigt. Wenn die Syntax ungültig ist, erscheint eine Warnmeldung.

Dialogfeld „Regelsyntax“

So rufen Sie dieses Dialogfeld auf:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
2. Führen Sie in der Ansicht **Regelbibliothek** eine der folgenden Aktionen durch:
   a) Klicken Sie auf  und wählen Sie **Erweiterte EPL** oder **Regelerstellung** aus.
   b) Doppelklicken Sie auf eine vorhandene Regel.
   c) Wählen Sie eine vorhandene Regel aus und klicken Sie in der Symbolleiste der **Regelbibliothek** auf  .
   Klicken Sie in der Zeile einer vorhandenen Regel auf  **> Bearbeiten**.
   Die neue oder vorhandene Regel wird in einer neuen Registerkarte angezeigt und kann bearbeitet werden.
3. Klicken Sie unten auf der Registerkarte auf **Syntax anzeigen**.

Die folgende Abbildung zeigt ein Beispiel für das Dialogfeld „Regelsyntax“.



In der folgenden Tabelle sind die Eigenschaften der Parameter des Dialogfelds Regelsyntax beschrieben:

Parameter	Beschreibung
Regel ist gültig oder **Validierungsfehler in Regel**	Zeigt an, ob die Regelsyntax gültig ist oder geändert werden muss.
Name der Regel	Zeigt den Namen einer Regel an.
Text	Zeigt die EPL-Syntax von Bedingungen, Anweisungen und Debugging-Parametern an, wenn die Regel gültig ist.

Registerkarte Services

In diesem Thema finden Sie eine Übersicht über die Registerkarte **Konfigurieren > ESA-Regeln > Services**. Auf der Registerkarte „Services“ finden Sie Details zu den ESA-Services, die Sie NetWitness Suite hinzugefügt haben.

Was möchten Sie tun?

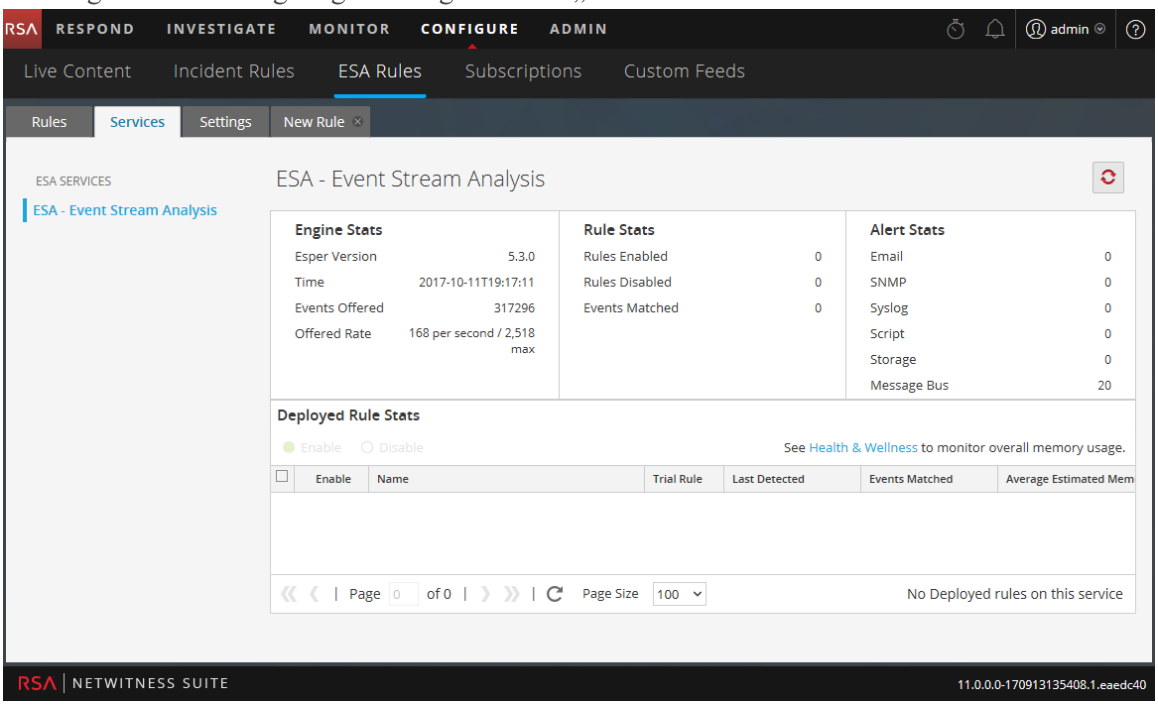
Rolle	Ziel	Details anzeigen
Contentexperte	Troubleshooting auf der Registerkarte „Services“	Troubleshooting für ESA
Contentexperte	Bereitstellungsstatistiken für einen ESA-Service anzeigen	Anzeigen der Statistiken zu einem ESA-Service

Verwandte Themen

- Anzeigen einer Zusammenfassung der Warnmeldungen

Services

Die folgende Abbildung zeigt die Registerkarte „Services“:



Die Registerkarte „Services“ umfasst die folgenden Abschnitte:

- Bereich „ESA-Services“
- Bereich „Allgemeine Statistik“
- Bereich „Statistik für bereitgestellte Regeln“

Bereich „ESA-Services“

Im Bereich „ESA-Services“ sind die Namen aller ESA-Services aufgelistet, die zu NetWitness Suite hinzugefügt wurden.

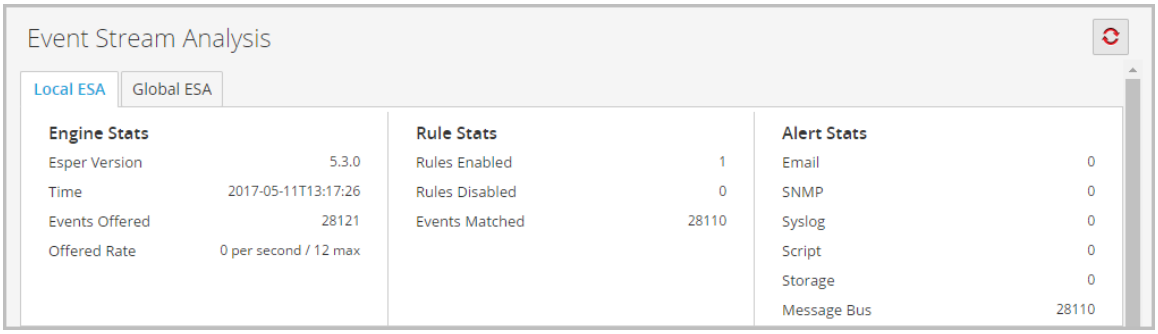
Bereich „Allgemeine Statistik“

Der Bereich „Allgemeine Statistik“ enthält Informationen über die Esper-Engine, Regeln und Warnmeldungen.

Der Bereich Allgemeine Statistik ist in die folgenden Abschnitte unterteilt:

- Engine-Statistiken
- Regelstatistiken
- Warnmeldungsstatistiken

Die Abbildung unten zeigt den Bereich „Allgemeine Statistik“.



In der folgenden Tabelle sind die Parameter im jeweiligen Abschnitt beschrieben.

Abschnitte	Parameter	Beschreibung
Engine-Statistiken	Esper-Version	Esper-Version, die im ESA-Service ausgeführt wird
	Zeit	Zeitpunkt, an dem das letzte Ereignis an die Esper-Engine gesendet wurde
	Angebotene Ereignisse	Anzahl an Ereignissen, die vom ESA-Service seit dem letzten Servicestart analysiert wurde
	Angebotene Rate	Aktuelle Rate angebotener Ereignisse im ESA-Service
Regelstatistiken	Regeln aktiviert	Anzahl aktivierter Regeln
	Regeln deaktiviert	Anzahl deaktivierter Regeln
	Übereinstimmende Ereignisse	Gesamtanzahl der Ereignisse, die mit allen Regeln im ESA-Service übereinstimmen
Warnmeldungsstatistiken	E-Mail	Anzahl von E-Mail-Benachrichtigungen, die vom ESA-Service gesendet wurden
	SNMP	Anzahl von SNMP-Benachrichtigungen, die vom ESA-Service gesendet wurden
	Syslog	Anzahl von Syslog-Benachrichtigungen, die vom ESA-Service gesendet wurden
	Skript	Anzahl von Skript-Benachrichtigungen, die vom ESA-Service gesendet wurden
	Speicher	Gesamtanzahl der in der Datenbank gespeicherten Warnmeldungen
	Nachrichtenbus	Gesamtanzahl von Warnmeldungen, die an den Nachrichtenbus gesendet wurden

Bereich „Statistik für bereitgestellte Regeln“

Der Bereich „Statistik für bereitgestellte Regeln“ liefert Details zu den im ESA-Service bereitgestellten Regeln.

In der folgenden Abbildung wird der Bereich „Statistik für bereitgestellte Regeln“ dargestellt.

In der Tabelle werden die verschiedenen Parameter und deren Beschreibung aufgelistet.

Parameter	Beschreibung
●	Gibt an, dass die Regel aktiviert ist. Aktiviert eine Regel, die deaktiviert war.
○ Disable	Gibt an, dass die Regel deaktiviert ist. Deaktiviert eine Regel, die aktiviert war.
Integrität und Zustand	Zeigt eine Momentaufnahme des Speichernutzung an, wenn Testregeln deaktiviert werden.
Aktivieren	Zeigt an, ob die Regel aktiviert oder deaktiviert ist Das grüne Symbol gibt an, dass die Regel aktiviert ist. Das weiße Symbol gibt an, dass die Regel deaktiviert ist.
Name	Name der ESA-Regel
Testregel	Zeigt an, ob die Regel im Testregelmodus ausgeführt wird.
Zuletzt erkannt	Zeitpunkt, an dem das letzte Mal eine Warnmeldung für diese Regel ausgelöst wurde
Übereinstimmende Ereignisse	Gesamtanzahl von Ereignissen, die mit der Regel übereinstimmten

Registerkarte „Einstellungen“

In diesem Thema werden die Komponenten der Registerkarte **Konfigurieren > ESA-Regeln > Einstellungen** beschrieben. In der Registerkarte Einstellungen können Sie folgende Aufgaben durchführen:

- Eine Liste der Metaschlüssel anzeigen
- Eine Datenerweiterungsquelle konfigurieren
- Eine Verbindung zu einer externen Datenbank hinzufügen

Was möchten Sie tun?

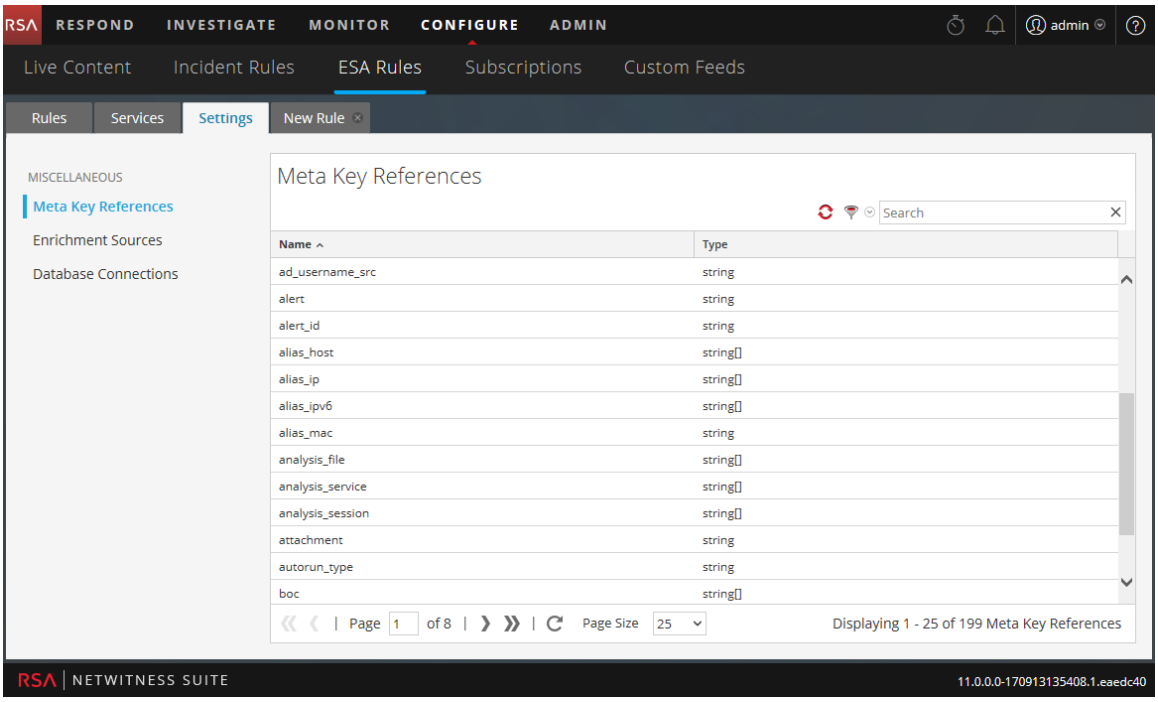
Rolle	Ziel	Details anzeigen
Contentexperte	Verbindung zu einer externen Datenbank konfigurieren	Konfigurieren einer Datenbankverbindung
Contentexperte	Datenbank als Erweiterungsquelle konfigurieren	Erweiterungsquellen

Verwandte Themen

- Hinzufügen einer Datenerweiterungsquelle

Einstellungen

Die folgende Abbildung zeigt den Abschnitt Metaschlüsselverweise der Registerkarte Einstellungen.



Metaschlüsselverweise

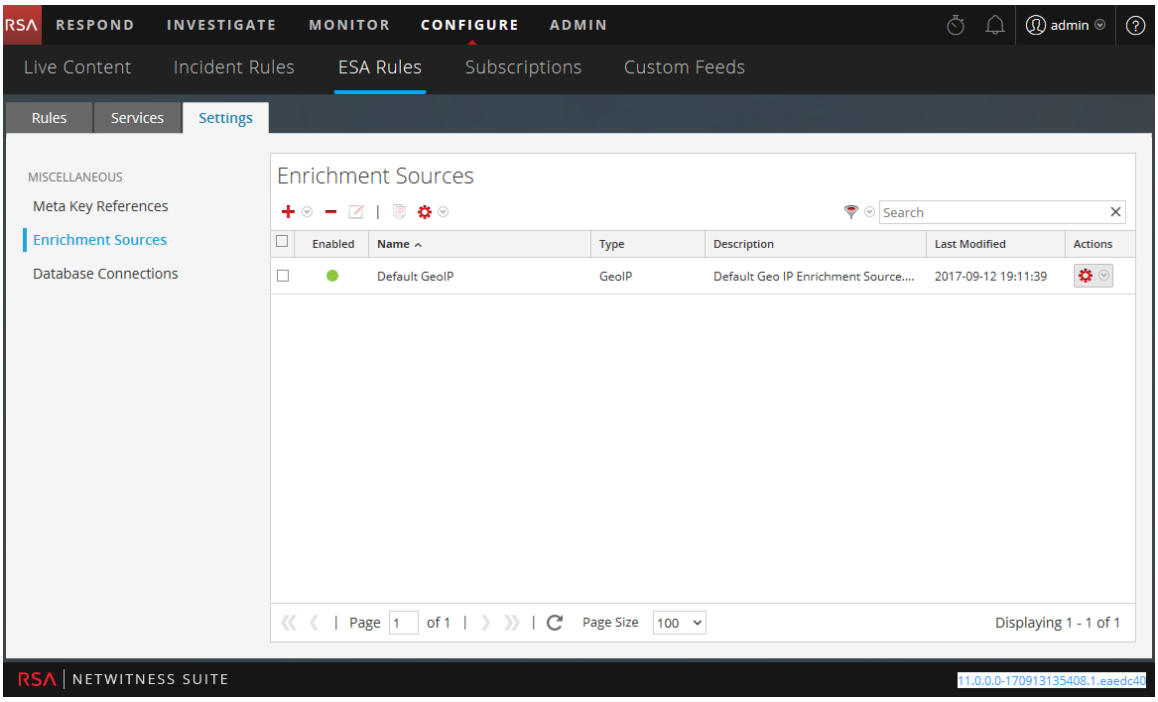
Im Bereich „Metaschlüsselverweise“ werden die einzelnen Metaschlüssel und die Art des Werts, die für einen Schlüssel erforderlich ist, aufgelistet.

Erweiterungsquellen

Im Bereich Erweiterungsquellen können Sie die folgenden externen Datenquellen konfigurieren:

- GeoIP
- Externe Datenbankreferenz
- In-Memory-Tabelle
- Warehouse Analytics

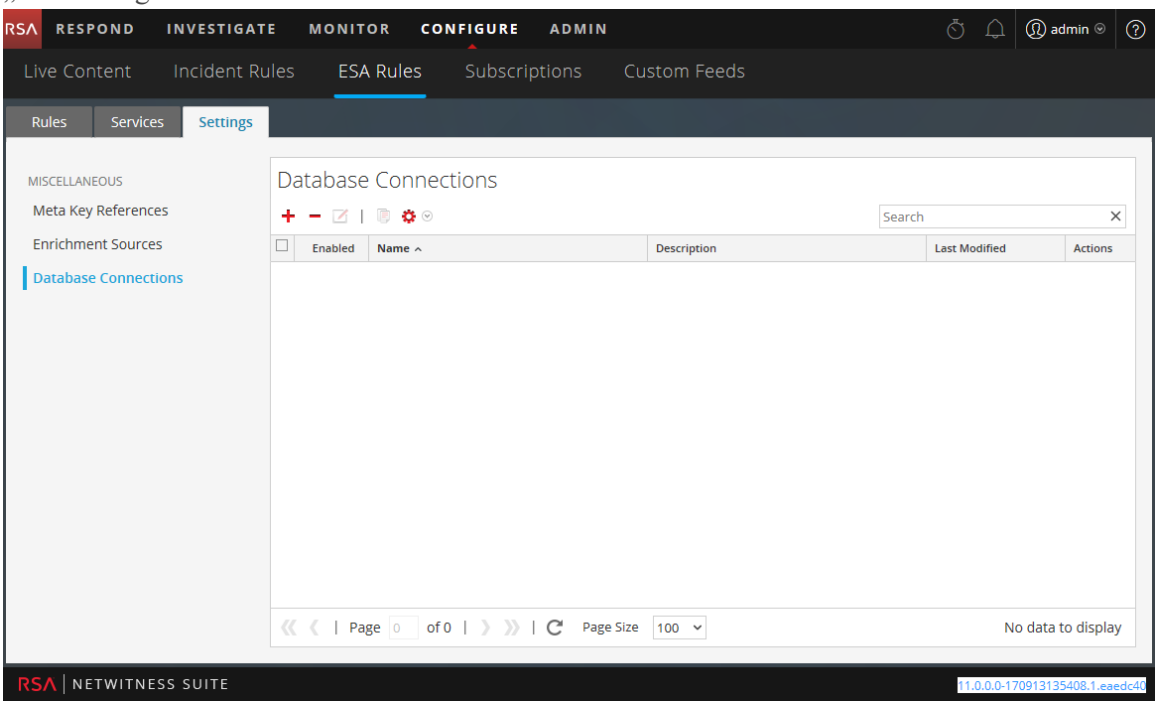
Die folgende Abbildung zeigt den Abschnitt Erweiterungsquellen der Registerkarte Einstellungen.



Datenbankverbindungen

Im Abschnitt „Datenbankverbindungen“ können Sie eine Verbindung zu einer externen Datenbank konfigurieren, damit ESA auf die dort gespeicherten Daten zugreifen kann.

Die folgende Abbildung zeigt den Abschnitt „Datenbankverbindungen“ auf der Registerkarte „Einstellungen“.



Im Abschnitt Datenbankverbindungen können Sie folgende Vorgänge ausführen:

- Hinzufügen einer Datenbankverbindung
- Löschen von Datenbankverbindungen
- Bearbeiten von Datenbankverbindungen
- Duplizieren von Datenbankverbindungen
- Importieren von Datenbankverbindungen
- Exportieren von Datenbankverbindungen

Dialogfeld „Aktualisierungen an der Bereitstellung“

Im Dialogfeld „Aktualisierungen an der Bereitstellung“ werden Änderungen an der Bereitstellung angezeigt, wie etwa die Hinzufügung einer Regel oder eines Services. Aktualisierungen an der Bereitstellung werden durch das Aktualisierungssymbol () neben dem Namen der Bereitstellung im Bereich „Optionen“ auf der Registerkarte „Regeln“ angezeigt.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Contentexperte	Regeln zur Ausführung in ESA bereitstellen	Bereitstellungsschritte
Contentexperte	Eine Bereitstellung bearbeiten oder löschen	Bearbeiten oder Löschen einer Bereitstellung
Contentexperte	Aktualisierungen an einer Bereitstellung anzeigen	Anzeigen der Aktualisierungen an einer Bereitstellung

Verwandte Themen

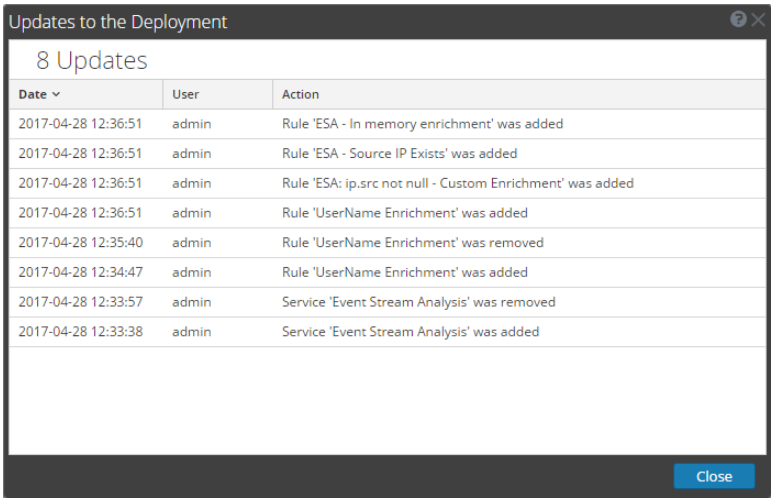
- Löschen eines ESA-Services in einer Bereitstellung
- Bearbeiten oder Löschen einer Regel in einer Bereitstellung

Dialogfeld „Bereitstellung“

So rufen Sie dieses Dialogfeld auf:

1. Navigieren Sie zu **Konfigurieren > ESA-Regeln**.
   Die Registerkarte „Regeln“ wird standardmäßig geöffnet.
2. Wählen Sie im Bereich „Optionen“ unter dem Abschnitt **Bereitstellungen** eine Bereitstellung aus oder fügen Sie eine hinzu.
3. Klicken Sie im Bereich **Bereitstellung** auf **Updates anzeigen**.
   Das Dialogfeld „Aktualisierungen an der Bereitstellung“ wird angezeigt.

Die folgende Abbildung zeigt ein Beispiel für dieses Dialogfeld.



Im Dialogfeld „Aktualisierungen an der Bereitstellung“ wird die Anzahl der Aktualisierungen oben im Dialog angezeigt. In der folgende Tabelle werden die Parameter dieses Dialogs beschrieben.

Parameter	Beschreibung
Datum	Zeigt den Tag und die Uhrzeit der Aktualisierung an.
Benutzer	Zeigt den Benutzer an, der die Aktualisierung vorgenommen hat.
Aktion	Beschreibt die Aktualisierung.