



# Konfigurationsleitfaden für NetWitness Respond

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](http://germany.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **Lizenzvereinbarung**

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

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

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

## **Drittanbieterlizenzen**

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

## **Hinweis zu Verschlüsselungstechnologien**

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

## **Verteilung**

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

Februar 2018

# Inhalt

---

<b>Über dieses Dokument</b> .....	<b>5</b>
Konfiguration von NetWitness Respond – Übersicht .....	5
<b>Konfigurieren von NetWitness Respond</b> .....	<b>7</b>
Schritt 1. Konfigurieren von Warnmeldungsquellen zur Anzeige von Warnmeldungen in der Ansicht „Reagieren“ .....	8
Voraussetzungen .....	8
Konfigurieren von Reporting Engine zur Anzeige von durch Reporting Engine ausgelösten Warnmeldungen in der Ansicht „Reagieren“ .....	8
Konfigurieren von Malware Analytics zur Anzeige von durch Malware Analytics ausgelösten Warnmeldungen in der Ansicht „Reagieren“ .....	9
Konfigurieren Sie NetWitness Endpoint zur Anzeige von durch NetWitness Endpoint ausgelöste Warnmeldungen in der Ansicht „Reagieren“ .....	9
Konfigurieren von NetWitness Endpoint zur Anzeige von NetWitness Endpoint- Warnmeldungen .....	10
Schritt 2. Zuweisen von Respond-Anzeigeberechtigungen .....	12
Respond-Server .....	13
Incidents .....	14
Schritt 3. Erstellen einer Aggregationsregel für Warnmeldungen .....	17
<b>Zusätzliche Verfahren für die Respond-Konfiguration</b> .....	<b>19</b>
Festlegen einer Aufbewahrungsfrist für Warnmeldungen und Incidents .....	19
Voraussetzungen .....	20
Verfahren .....	21
Ergebnis .....	21
Verschleiern von privaten Daten .....	22
Voraussetzungen .....	22
Verfahren .....	23
Managen von Incidents in NetWitness SecOps Manager .....	24
Voraussetzungen .....	24
Verfahren .....	24
Einstellen des Zählers für abgestimmte Warnmeldungen und Incidents .....	26

Konfigurieren einer Datenbank für den Respond Server-Service .....	28
Voraussetzungen .....	28
Verfahren .....	28
<b>Konfiguration von NetWitness Respond – Referenz .....</b>	<b>31</b>
Ansicht „Konfigurieren“ .....	31
Registerkarte „Aggregationsregeln“ .....	32
Was möchten Sie tun? .....	32
Verwandte Themen .....	32
Aggregationsregeln .....	32
Registerkarte „Neue Regel“ .....	35
Was möchten Sie tun? .....	35
Verwandte Themen .....	35
Neue Regel .....	35

## Über dieses Dokument

---

Dieser Leitfaden bietet eine Übersicht über NetWitness Respond und gibt detaillierte Anweisungen zur Konfiguration von NetWitness Respond in Ihrem Netzwerk. Außerdem enthält er Beschreibungen von zusätzlichen Verfahren, die zu anderen Zeitpunkten durchgeführt werden, sowie Referenzmaterial, das die Benutzeroberfläche für die Konfiguration von NetWitness Respond in Ihrem Netzwerk erläutert.

### Themen

- [Konfiguration von NetWitness Respond – Übersicht](#)
- [Konfigurieren von NetWitness Respond](#)
- [Zusätzliche Verfahren für die Respond-Konfiguration](#)
- [Konfiguration von NetWitness Respond – Referenz](#)

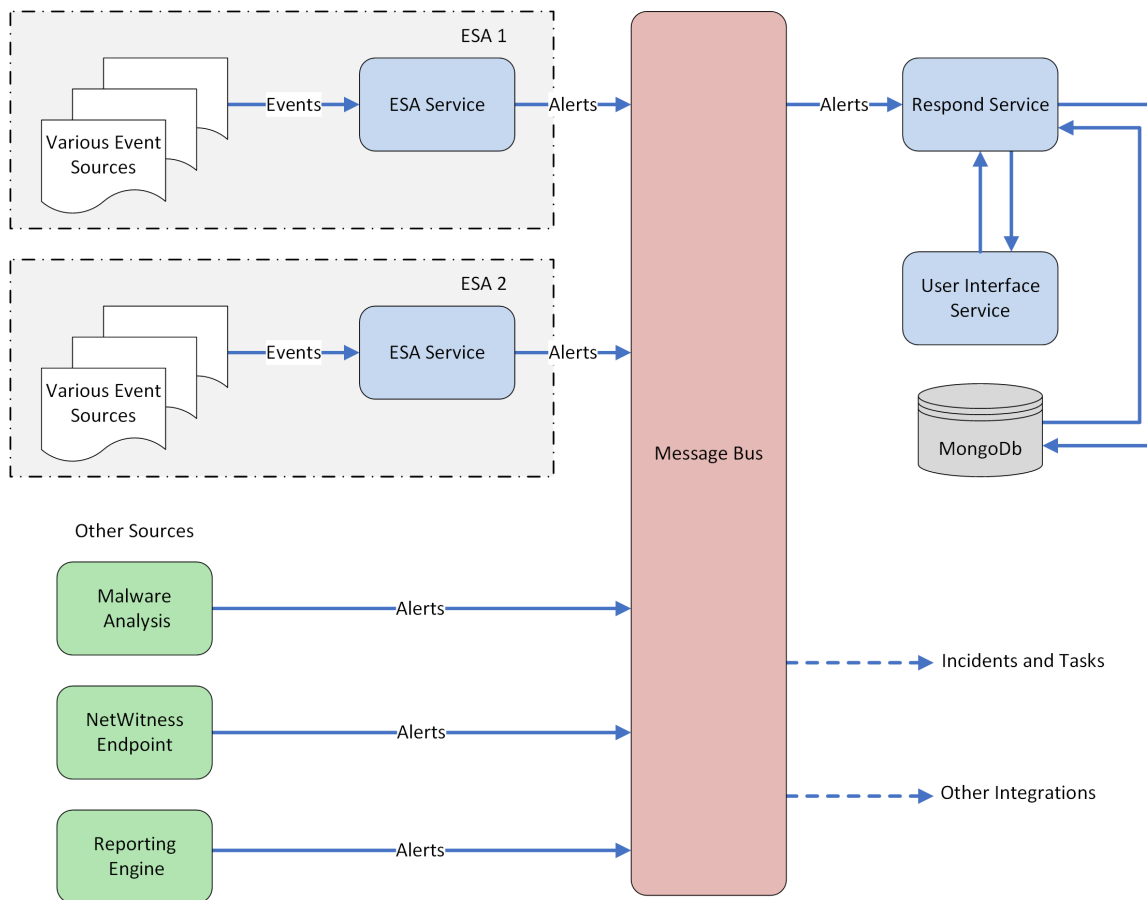
## Konfiguration von NetWitness Respond – Übersicht

RSA NetWitness® Suite NetWitness Respond verarbeitet Warnmeldungsdaten von verschiedenen Quellen über den Nachrichtenbus und zeigt diese Warnmeldungen auf der NetWitness Suite-Benutzeroberfläche an. Der Antwortserver-Dienst erlaubt Ihnen, die Warnmeldungen logisch zu gruppieren und einen NetWitness Respond-Workflow für die Reaktion auf den Incident zu starten, um die aufgetretenen Sicherheitsprobleme zu untersuchen und zu beheben.

Der Antwortserver-Dienst verarbeitet Warnmeldungen vom Nachrichtenbus und normalisiert die Daten in ein gemeinsames Format (unter Beibehaltung der Originaldaten), um eine einfachere Regelverarbeitung zu ermöglichen. Er führt regelmäßig Regeln aus, um mehrere Warnmeldungen in einem Incident zu aggregieren und einige Attribute des Incident einzustellen (zum Beispiel Schwere, Kategorie usw.). Die Incidents werden vom Antwortserver-Dienst dauerhaft in MongoDB abgelegt. Incidents werden im Nachrichtenbus auch zur Verarbeitung durch andere Systeme gepostet (zum Beispiel zur Integration in Archer).

**Hinweis:** NetWitness Respond erfordert einen primären ESA-Server, der die MongoDB enthält. Warnmeldungen, Incidents und Aufgabendatensätze werden vom Respond Server dauerhaft in der MongoDB gespeichert.

Die folgende Abbildung illustriert den allgemeinen Fluss der Warnmeldungen.



Sie müssen verschiedene Quellen konfigurieren, von denen die Warnmeldungen durch den Antwortserver-Dienst gesammelt und aggregiert werden.

## Konfigurieren von NetWitness Respond

---

Dieses Thema enthält allgemeine, zur Konfiguration von Antwortserver-Dienst erforderliche Aufgaben. Der Administrator muss die folgenden Schritte in der angegebenen Reihenfolge abschließen.

### Themen

- [Schritt 1. Konfigurieren von Warmmeldungsquellen zur Anzeige von Warmmeldungen in der Ansicht „Reagieren“](#)
- [Schritt 2. Zuweisen von Respond-Anzeigeberechtigungen](#)
- [Schritt 3. Erstellen einer Aggregationsregel für Warmmeldungen](#)

## Schritt 1. Konfigurieren von Warnmeldungsquellen zur Anzeige von Warnmeldungen in der Ansicht „Reagieren“

Dieses Verfahren ist erforderlich, damit Warnmeldungen von den Warnmeldungsquellen in NetWitness Respond angezeigt werden. Sie haben die Möglichkeit, die Warnmeldungen in der Ansicht „Reagieren“ anzuzeigen, zu aktivieren oder zu deaktivieren. Standardmäßig ist diese Option in Reporting Engine, Malware Analytics und NetWitness Endpoint deaktiviert und nur in Event Stream Analysis aktiviert. Wenn Sie also den Antwortserver-Dienst installieren, müssen Sie diese Option in Reporting Engine, Malware Analytics und NetWitness Endpoint aktivieren, damit die entsprechenden Warnmeldungen in der Ansicht „Reagieren“ angezeigt werden.


### Voraussetzungen

Stellen Sie Folgendes sicher:

- Antwortserver-Dienst ist installiert und wird auf NetWitness Suite ausgeführt.
- Eine Datenbank ist für Antwortserver-Dienst konfiguriert.
- NetWitness Endpoint ist installiert und wird ausgeführt.

### Konfigurieren von Reporting Engine zur Anzeige von durch Reporting Engine ausgelösten Warnmeldungen in der Ansicht „Reagieren“

Die Anzeige der Reporting Engine-Warnmeldungen ist in der Ansicht „Reagieren“ standardmäßig deaktiviert. Um die Reporting Engine-Warnmeldungen anzuzeigen, müssen Sie die NetWitness Respond-Warnmeldungen auf der Registerkarte „Allgemein“ in der Ansicht „Services-Konfiguration“, Registerkarte „Allgemein“, für die Reporting Engine aktivieren.

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie einen Reporting Engine-Service aus und wählen Sie  > **Ansicht > Konfiguration**.

Die Servicekonfigurationsansicht wird mit geöffneter Registerkarte Reporting Engine Allgemein angezeigt.

2. Wählen Sie **Systemkonfiguration** aus.
3. Aktivieren Sie das Kontrollkästchen für **Warnmeldungen weiterleiten an Antwort**.  
Die Reporting Engine leitet nun die Warnmeldungen an NetWitness Respond weiter.

Informationen zu Parametern auf der Registerkarte „Allgemein“ finden Sie im Thema „Reporting Engine – Registerkarte Allgemein“ im *Reporting Engine-Konfigurationsleitfaden*.



## Konfigurieren von Malware Analytics zur Anzeige von durch Malware Analytics ausgelösten Warnmeldungen in der Ansicht „Reagieren“

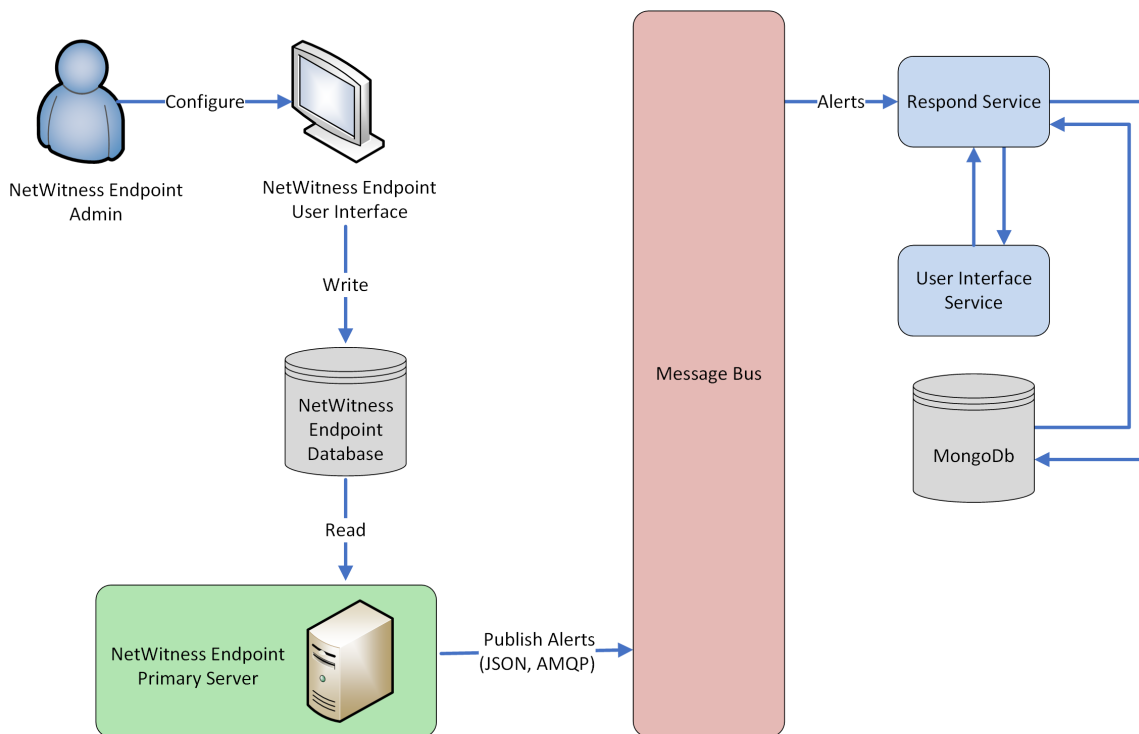
Die Anzeige von NetWitness Respond-Warnmeldungen ist eine Auditing-Funktion in Malware Analysis. Eine Beschreibung des Verfahrens zum Aktivieren von NetWitness Respond-Warnmeldungen aus Incident Management finden Sie im Thema „(Optional) Konfigurieren des Auditing auf dem Malware Analysis-Host“ im *Malware Analysis-Konfigurationsleitfaden*.

## Konfigurieren Sie NetWitness Endpoint zur Anzeige von durch NetWitness Endpoint ausgelöste Warnmeldungen in der Ansicht „Reagieren“

Dieses Verfahren ist für die Integration von NetWitness Endpoint in NetWitness Suite erforderlich, damit die NetWitness Endpoint-Warnmeldungen von der NetWitness Respond-Komponente von NetWitness Suite erkannt und in der Ansicht **Reagieren > Warnmeldungen** angezeigt werden.

**Hinweis:** RSA unterstützt NetWitness Endpoint Versionen 4.3.0.4, 4.3.0.5 oder höher für NetWitness Respond-Integration. Weitere Informationen finden Sie im Thema „RSA NetWitness Suite-Integration“ im *NetWitness Endpoint-Benutzerhandbuch*.

Das Diagramm unten stellt den Fluss von NetWitness Endpoint-Warnmeldungen zur NetWitness Suite Antwortserver-Dienst und dessen Anzeige in der Ansicht **Reagieren > Warnmeldungen** dar.

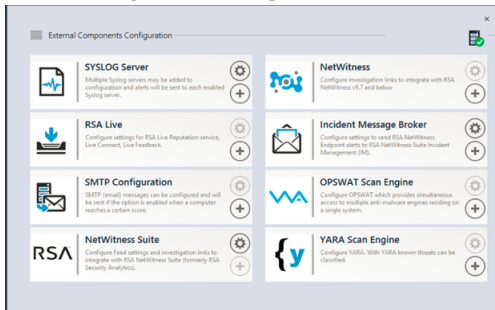


## Konfigurieren von NetWitness Endpoint zur Anzeige von NetWitness Endpoint-Warmmeldungen

So konfigurieren Sie NetWitness Endpoint so, dass NetWitness Endpoint-Warmmeldungen in der NetWitness Suite-Benutzeroberfläche angezeigt werden:

1. Klicken Sie in der NetWitness Endpoint-Benutzeroberfläche auf **Konfigurieren > Überwachung und externe Komponenten**.

Das Dialogfeld **Konfiguration externer Komponenten** wird angezeigt.



2. Wählen Sie bei den aufgeführten Komponenten **Incident Message Broker** aus und klicken Sie auf +, um einen neuen IM-Broker hinzuzufügen.
3. Geben Sie Werte für die folgenden Felder ein:
  - a. **Instanzname:** Geben Sie einen eindeutigen Namen zur Identifizierung des IM-Brokers ein.
  - b. **Hostname/IP-Adresse des Servers:** Geben Sie die Host-DNS- oder die IP-Adresse des IM-Brokers ein (NetWitness-Server).
  - c. **Portnummer** Der Standardport ist 5671.
4. Klicken Sie auf **Speichern**.
5. Navigieren Sie zur Datei **ConsoleServer.exe.Config** in **C:\Programme\RSA\ECAT\Server**.
6. Ändern Sie die virtuellen Host-Konfigurationen in der Datei wie folgt:
 

```
<add key="IMVirtualHost" value="/rsa/system" />
```

**Hinweis:** In NetWitness Suite 11.0 lautet der virtuelle Host „/rsa/system“. In Version 10.6.x und niedriger lautet der virtuelle Host „/rsa/sa“.

7. Starten Sie den API-Server und Konsolenserver neu.
8. Um SSL für Respond-Warmmeldungen einzurichten, führen Sie folgende Schritte auf dem

primären Konsolenserver von NetWitness Endpoint aus, um die SSL-Kommunikation einzurichten:

- a. Exportieren Sie das NetWitness Endpoint CA-Zertifikat im CER-Format (Base-64 encoded X.509) aus dem persönlichen Zertifikatspeicher des lokalen Computers (ohne den privaten Schlüssel auszuwählen).
- b. Erzeugen Sie ein Clientzertifikat für NetWitness Endpoint mithilfe des NetWitness Endpoint CA-Zertifikats. (Sie MÜSSEN den CN-Namen auf ecat einstellen).

```
makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a  
sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NWECA" -is MY -ir  
LocalMachine -sp "Microsoft RSA Schannel Cryptographic Provider" -  
cy end -sy 12 client.cer
```

**Hinweis:** Im oben genannten Codebeispiel sollten Sie „EcatCA“ durch „NWECA“ ersetzen, wenn Sie von einer früheren Version ein Upgrade auf Version 4.3 durchgeführt haben und keine neuen Zertifikate erzeugt haben.

- c. Notieren Sie sich den Thumbprint des in Schritt b generierten Clientzertifikats. Geben Sie den Thumbprint-Wert des Clientzertifikats im Abschnitt `IMBrokerClientCertificateThumbprint` der `ConsoleServer.Exe.Config-Datei` ein (siehe Abbildung).  

```
<add key="IMBrokerClientCertificateThumbprint"  
value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```
9. Kopieren Sie auf dem NetWitness-Server die NetWitness Endpoint CA-Zertifikatdatei im CER-Format in den Importordner:  
`/etc/pki/nw/trust/import`
10. Geben Sie den folgenden Befehl aus, um die erforderliche Chef-Ausführung zu initiieren:  
`orchestration-cli-client --update-admin-node`  
Dadurch werden alle Zertifikate an den Truststore angehängt.
11. Starten Sie den RabbitMQ-Server neu:  
`systemctl restart rabbitmq-server`  
Das NetWitness Endpoint-Konto sollte auf RabbitMQ automatisch verfügbar sein.
12. Importieren Sie die Dateien `/etc/pki/nw/ca/nwca-cert.pem` und `/etc/pki/nw/ca/ssca-cert.pem` aus der NetWitness-Server und fügen Sie sie den Trusted Root Certification-Speichern auf dem Endpoint-Server hinzu.

## Schritt 2. Zuweisen von Respond-Anzeigeberechtigungen

Fügen Sie Benutzer mit den erforderlichen Berechtigungen zum Untersuchen der zugewiesenen Incidents und Warnmeldungen in NetWitness Respond hinzu. Benutzer mit Zugriff auf die Ansicht „Reagieren“ benötigen Berechtigungen für Incidents und den Respond-Server-.

Die folgenden vorkonfigurierten Rollen haben Berechtigungen in der Ansicht „Reagieren“:

- **Analysten:** SOC-Analysten (Security Operation Center) haben Zugriff auf Warnmeldungen, NetWitness Respond, Ermittlungen und Reporting, aber nicht auf Systemkonfigurationen.
- **Malware-Analysten:** Malware-Analysten haben Zugriff auf Ermittlungen und Schadsoftwareereignisse.
- **Operatoren:** Operatoren haben Zugriff auf Konfigurationen, jedoch nicht auf Ermittlungen, ESA, Warnmeldungen, Reporting und NetWitness Respond.
- **SOC-Manager:** SOC-Manager haben den gleichen Zugriff wie Analysten sowie zusätzliche Berechtigung für das Verarbeiten von Incidents und die Konfigutaion von NetWitness Respond.
- **Data Privacy Officers:** Die Rolle des DPO (Data Privacy Officer, Datenschutzbeauftragter) ist ähnlich der des Administrators, mit zusätzlichem Fokus auf Konfigurationsoptionen, die Verschleierung und die Anzeige sensibler Daten innerhalb des Systems managen. Unter *Datenschutzmanagement* finden Sie weitere Informationen.
- **Respond-Administrator:** Der Respond-Administrator hat vollen Zugriff auf NetWitness Respond.
- **Administratoren:** Ein Administrator hat kompletten Systemzugriff auf NetWitness Suite und verfügt standardmäßig über alle Berechtigungen.

Die NetWitness Respond-Standardberechtigungen werden in den folgenden Tabellen angezeigt. Sie müssen beide Benutzerberechtigungen auf den Registerkarten **Incidents** und **Respond-Server** zuweisen, die den Registerkartennamen der Berechtigungen in der Ansicht „ADMIN > Sicherheit“ im Dialogfeld „Rollen hinzufügen“ oder „Rollen bearbeiten“ entsprechen. Sie möchten eventuell weitere Benutzerberechtigungen für Warnmeldungen, Context Hub, Investigate, Investigate-Server und Berichte hinzufügen.

**Respond-Server**

Berechtigungen	Analyste n	SOC- Manage r	DP O	Respon d- Admin	Operatore n	M A
respond-server.alert.delete			Ja*	Ja*		
respond-server.alert.manage	Ja	Ja	Ja*	Ja*		Ja
respond-server.alert.read	Ja	Ja	Ja*	Ja*		Ja
respond-server.alertrule.manage		Ja	Ja*	Ja*		
respond-server.alertrule.read		Ja	Ja*	Ja*		
respond-server.configuration.manage			Ja*	Ja*		
respond-server.health.read			Ja*	Ja*		
respond-server.incident.delete			Ja*	Ja*		
respond-server.incident.manage	Ja	Ja	Ja*	Ja*		Ja
respond-server.incident.read	Ja	Ja	Ja*	Ja*		Ja
respond-server.journal.manage	Ja	Ja	Ja*	Ja*		Ja
respond-server.journal.read	Ja	Ja	Ja*	Ja*		Ja

Berechtigungen	Analyste n	SOC- Manag er	DP O	Respon d- Admin	Operatore n	M A
respond- server.logs.manage			Ja*	Ja*		
respond- server.metrics.read			Ja*	Ja*		
respond- server.process.manage			Ja*	Ja*		
respond- server.remediation.manage	Ja	Ja	Ja*	Ja*		Ja
respond- server.remediation.read	Ja	Ja	Ja*	Ja*		Ja
respond- server.security.manage			Ja*	Ja*		
respond- server.security.read			Ja*	Ja*		

\* Data Privacy Officer und Respond-Administratoren haben die Berechtigung **respond-server.\***, die alle Berechtigungen für Respond-Server enthält.

## Incidents

Berechtigungen	Analyste n	SOC- Manag er	DP O	Respon d- Admin	Operatore n	M A
Auf Incident-Modul zugreifen	Ja	Ja	Ja	Ja		Ja
Konfigurieren der Incident- Managementintegration		Ja	Ja	Ja		

Berechtigungen	Analysten	SOC-Manager	DP O	Respond-Admin	Operatoren	MA
Löschen von Warnmeldungen und Incidents			Ja	Ja		
Managen der Regeln für die Warnmeldungsverarbeitung		Ja	Ja	Ja		
Anzeigen und Managen von Incidents	Ja	Ja	Ja	Ja		Ja

Der Respond-Administrator hat alle Berechtigungen für Respond-Server und Incidents.

**Achtung:** Es ist sehr wichtig, dass Sie entsprechenden Benutzerberechtigungen über **BEIDE** Registerkarten, für den Respond-Server und die Incidents, zuweisen.

Die folgende Abbildung zeigt Respond-Serverberechtigungen für die Standardrolle Respond-Administrator. Die Rolle des Respond-Administrators enthält alle Berechtigungen für NetWitness Respond.

**Edit Role**

**Role Info**

Name: Respond\_Administrator

Description:

**Attributes**

Core Query Timeout: 5

Core Session Threshold: 100000

Core Query Prefix:

**Permissions**

Malware | Orchestration-server | Reports | Respond-server | Security-server

Assigned: Respond-server

Assigned	Description
<input checked="" type="checkbox"/>	respond-server.*
<input type="checkbox"/>	respond-server.alert.delete
<input type="checkbox"/>	respond-server.alert.manage
<input type="checkbox"/>	respond-server.alert.read
<input type="checkbox"/>	respond-server.alertrule.manage
<input type="checkbox"/>	respond-server.alertrule.read

Cancel Save

Die folgende Abbildung zeigt die Incidents-Berechtigungen für die Standardrolle des Analysten:

**Edit Role**

**Role Info**

Name: Analysts

Description: The SOC Analysts persona is centered around Investigation, ESA Alerting, Reporting, and Incident Management, but not system configuration.

**Attributes**

Core Query Timeout: 5

Core Session Threshold: 100000

Core Query Prefix: ip.src =

**Permissions**

Server | Contexthub-server | Dashboard | Esa-analytics-server | Incidents | Investigate

Assigned: Incidents

Assigned	Description
<input checked="" type="checkbox"/>	Access Incident Module
<input type="checkbox"/>	Configure Incident Management integration
<input type="checkbox"/>	Delete Alerts and incidents
<input type="checkbox"/>	Manage Alert Handling Rules
<input checked="" type="checkbox"/>	View and Manage Incidents

Cancel Save

Weitere Informationen finden Sie in den Abschnitten „Rollenberechtigungen“ und „Managen von Benutzern mit Rollen und Berechtigungen“ im Handbuch *Systemsicherheit und Benutzerverwaltung*.



### Schritt 3. Erstellen einer Aggregationsregel für Warnmeldungen

Sie können Aggregationsregel mit unterschiedlichen Kriterien erstellen, um den Prozess der Incident-Erzeugung zu automatisieren. Warnmeldungen, die die Regelkriterien erfüllen, werden gruppiert und bilden einen Incident. Dies ist hilfreich, wenn Sie eine Reihe an Warnmeldungen kennen, die in einem Incident gruppiert werden können. Sie können eine Aggregationsregel einrichten, die die Gruppierung der Warnmeldungen übernimmt, und müssen nicht Zeit vergeuden, um einen Incident manuell zu erstellen und diesem die einzelnen Warnmeldungen hinzuzufügen. Zum automatischen Erstellen von Incidents müssen Sie eine Aggregationsregel erstellen.

So erstellen Sie eine Aggregationsregel:

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

Die Registerkarte **Aggregationsregeln** wird angezeigt.

Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
1	●	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication wi...		0	0
2	●	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA ...		0	0
3	●	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA ...		0	0
4	●	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA ...	2017-08-11 18:2...	2510	62
5	●	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ...	2017-08-12 20:0...	105464	1236
6	●	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addre...		0	0
7	●	User Watch List: Activity Detected	This incident rule captures alerts generated by network ...		0	0
8	●	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of w...		0	0
9	●	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common l...		0	0
10	●	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert desig...		0	0
11	●	Web Threat Detection	This incident rule captures alerts generated by the RSA ...		0	0

Eine Liste mit 11 vordefinierten Regeln wird angezeigt. Sie können einen der folgenden Schritte durchführen:

- Neue Regel hinzufügen
  - Vorhandene Regeln bearbeiten
  - Regel klonen
2. Klicken Sie auf **+**, um einen neuen Benutzer hinzuzufügen.

Die Registerkarte **Neue Regel** wird angezeigt.

Im folgenden Beispiel wird dargestellt, wie Warnmeldungen aufgrund der Risikobewertung in einem Incident gruppiert werden.

The screenshot shows the configuration page for a new aggregation rule in NetWitness Respond. The rule is named "Risk based" and is currently enabled. The description is "Alerts grouped by risk score". The match conditions are set to "Query Builder" mode with a single condition: "Risk Score is greater than 40". The action is set to "Group into an Incident". The grouping options are "Alert Type" with a time window of "1 Hours". The incident options include a title template "\${ruleName} for \${groupByValue1}", a summary field, and a category of "Hacking: Abuse of functionality". The priority is set to "Average of Risk Score across all of the Alerts". A priority scale is visible on the right, ranging from 1 (Low) to 90 (Critical).

### 3. Klicken Sie auf **Speichern**.

Die Regel wird auf der Registerkarte **Aggregationsregeln** angezeigt. Die Regel wird aktiviert und beginnt mit der Erstellung von Incidents gemäß den eingehenden Warnmeldungen, die mit dem ausgewählten Kriterium übereinstimmen.

#### Siehe auch:

- Einzelheiten zu den verschiedenen Parametern, die für die Kriterien einer Aggregationsregel verwendet werden können, finden Sie unter [Registerkarte „Neue Regel“](#).
- Einzelheiten zu den Beschreibungen der Parameter und Felder auf der Registerkarte „Aggregationsregeln“ finden Sie unter [Registerkarte „Aggregationsregeln“](#).

## Zusätzliche Verfahren für die Respond-Konfiguration

---

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

- [Festlegen einer Aufbewahrungsfrist für Warnmeldungen und Incidents](#)
- [Verschleiern von privaten Daten](#)
- [Managen von Incidents in NetWitness SecOps Manager](#)
- [Einstellen des Zählers für abgestimmte Warnmeldungen und Incidents](#)
- [Konfigurieren einer Datenbank für den Respond Server-Service](#)

### Festlegen einer Aufbewahrungsfrist für Warnmeldungen und Incidents

Manchmal möchten Datenschutzbeauftragte Daten für eine bestimmte Dauer aufbewahren und sie dann löschen. Eine kürzere Aufbewahrungsfrist macht den Speicherplatz früher wieder frei. In manchen Fällen muss die Aufbewahrungsfrist kurz sein. Zum Beispiel legen Gesetze in Europa fest, dass vertrauliche Daten nicht länger als 30 Tage aufbewahrt werden dürfen. Nach 30 Tagen müssen die Daten verschleiert oder gelöscht werden.

Die Einstellung einer Aufbewahrungsfrist für Daten ist ein optionales Verfahren. Der Zeitpunkt, zu dem NetWitness Respond Warnmeldungen empfängt und einen Incident erstellt, bestimmt, wann die Aufbewahrung beginnt. Aufbewahrungsfristen können von 30 bis zu 365 Tagen dauern. Wenn Sie eine Aufbewahrungsfrist einstellen, werden die Daten einen Tag, nachdem die Frist endet, dauerhaft gelöscht.

Aufbewahrung basiert auf dem Zeitpunkt, zu dem NetWitness Respond die Warnmeldungen empfängt und zu dem der Incident erstellt wird.

**Achtung:** Daten, die nach der Aufbewahrungsfrist gelöscht werden, können nicht wiederhergestellt werden.

Wenn die Aufbewahrungsfrist abläuft, werden die folgenden Daten **dauerhaft gelöscht**:

- Warnmeldungen
- Incidents
- Aufgaben
- Journaleinträge

Protokolle verfolgen Aufbewahrung und manuelles Löschen, sodass Sie sehen können, was gelöscht wurde. Sie können Antwortserver-Protokolle an folgenden Speicherorten anzeigen:



- **Antwortserver-Serviceprotokoll:** /var/log/netwitness/respond-server/respond-server.log
- **Antwortserver-Auditprotokoll:** /var/log/netwitness/respond-server/respond-server.audit.log

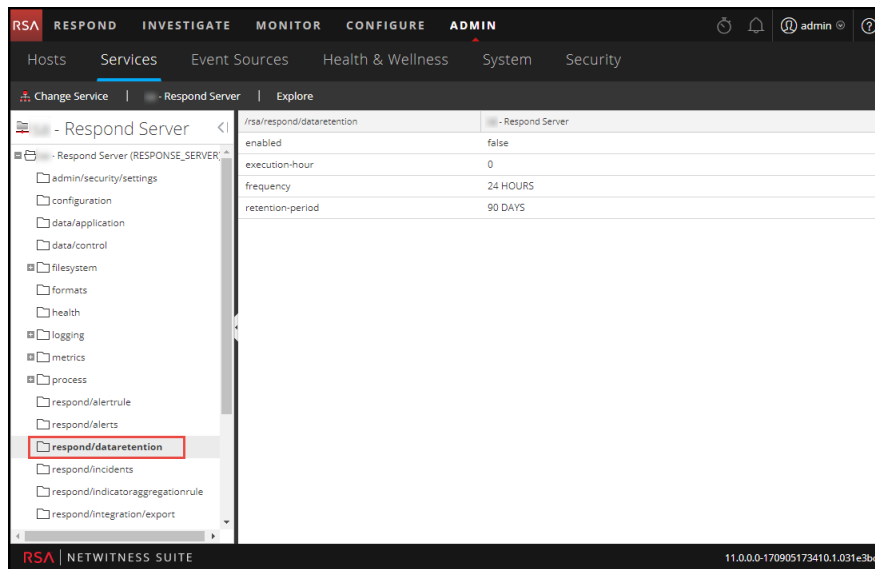
Die Datenaufbewahrungsfrist, die Sie hier festlegen, ist nicht anwendbar auf Archer oder andere SOC-Tools von Drittanbietern. Warnmeldungen und Incidents von anderen Systemen müssen getrennt gelöscht werden.

## **Voraussetzungen**

Ihnen muss die Administratorrolle zugewiesen sein.

## Verfahren

1. Navigieren Sie zu **ADMIN** > ServicesAntwortserver-Dienst, wählen Sie den aus und wählen Sie dann   > **Ansicht** > **Durchsuchen**.
2. Wählen Sie in der Ansicht „Durchsuchen“ der Node-Liste **respond/dataretention** aus.



3. Wählen Sie im Feld **enabled** die Option **true** aus, um Incidents und Warnmeldungen zu löschen, die älter sind als die Aufbewahrungsfrist.  
Der Planer wird alle 24 Stunden um 23:00 Uhr ausgeführt.  
Eine Meldung wird angezeigt, dass die Konfiguration erfolgreich aktualisiert wurde.
4. Geben Sie im Feld **retention-period** die Anzahl der Tage ein, für die Incidents und Warnmeldungen aufbewahrt werden. Geben Sie z. B. 30 DAYS, 60 DAYS, 90 DAYS, 120 DAYS, 365 DAYS oder eine beliebige Anzahl von Tagen ein.  
Eine Meldung wird angezeigt, dass die Konfiguration erfolgreich aktualisiert wurde.

## Ergebnis

Innerhalb von 24 Stunden nach Ende der Aufbewahrungsfrist löscht der Planer alle Warnmeldungen und Incidents, die älter als die spezifizierte Frist sind, aus NetWitness Respond. Journaleinträge und Aufgaben, die zu den gelöschten Incidents gehören, werden ebenfalls gelöscht.

## Verschleiern von privaten Daten

Die Rolle des Datenschutzbeauftragten (Data Privacy Officer, DPO) kann Metaschlüssel identifizieren, die vertrauliche Daten enthalten und verschleierte Daten anzeigen sollten. In diesem Thema wird erläutert, wie der Administrator diesen Metaschlüsseln einen gehashten Wert anstelle des tatsächlichen Werts zuordnen kann.

Bei gehashten Metawerten sind folgende Punkte zu beachten:

- NetWitness Suite unterstützt zwei Speichermethoden für Hash-Metawerte: HEX (Standard) und Zeichenfolge.
- Wenn ein Metaschlüssel zum Anzeigen eines Hash-Werts ist, sehen alle Sicherheitsrollen im Modul Incidents nur den gehashten Wert.
- Gehashte Werte werden genauso wie die tatsächlichen Werte verwendet. Wenn Sie beispielsweise in Regelkriterien einen gehashten Wert verwenden, sind die Ergebnisse die gleichen wie bei Verwendung des tatsächlichen Werts.

In diesem Thema wird erläutert, wie private Daten in NetWitness Respond verschleiert werden. Zusätzliche Informationen zum Datenschutz finden Sie im Thema **Übersicht zum Datenschutzmanagement** im Leitfaden *Datenschutzmanagement*.

### Zuordnungsdatei für die Verschleierung von Metaschlüsseln

Im NetWitness Respond trägt die Zuordnungsdatei für die Datenverschleierung den Namen „data\_privacy\_map.js“. Darin geben Sie den Namen für einen verschleierten Metaschlüssel ein und ordnen diesen dem Namen des tatsächlichen Metaschlüssels zu.

Das folgende Beispiel zeigt die Zuordnungen für die Verschleierung der Daten von zwei Metaschlüsseln, ip.src und user.dst:

```
'ip.src.hash' : 'ip.src',  
'user.dst.hash' : 'user.dst'
```

Sie bestimmen die Benennungskonvention für Namen von verschleierten Metaschlüsseln. Beispielsweise könnte ip.src.hash auch ip.src.private sein oder ip.src.bin heißen. Die festgelegte Benennungskonvention muss jedoch konsistent auf allen Hosts verwendet werden.

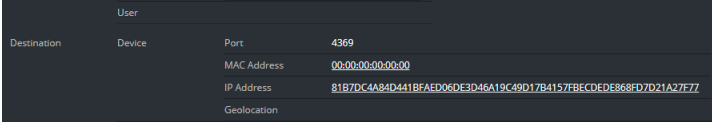
### Voraussetzungen

- Von der DPO-Rolle wird festgelegt, für welche Metaschlüssel eine Datenverschleierung erforderlich ist.
- Die Administratorrolle ordnet anschließend die Metaschlüssel für die Datenverschleierung zu.

## Verfahren

1. Öffnen Sie die Datenschutz-Zuordnungsdatei:  
`/var/lib/netwitness/respond-server/scripts/data_privacy_map.js`
2. Geben Sie in der Variablen `obfuscated_attribute_map` den Namen des Metaschlüssels ein, der verschleierte Daten enthalten soll. Ordnen Sie diesen dann dem Metaschlüssel zu, der die nicht verschleierte Originaldaten enthält. Verwenden Sie dazu folgendes Format:  
`'ip.src.hash' : 'ip.src'`
3. Wiederholen Sie Schritt 2 für jeden Metaschlüssel, der einen gehashten Wert anzeigen soll.
4. Folgen Sie derselben Benennungskonvention wie in Schritt 2 und verwenden Sie diese konsistent auf allen Hosts.
5. Speichern Sie die Datei  
.Alle zugeordneten Metaschlüssel zeigen nun gehashte Werte statt der tatsächlichen Werte an.

In der folgenden Abbildung wird ein Hash-Wert für die Ziel-IP-Adresse in den Ereignisdetails angezeigt:



User	
Destination	Device
Port	4369
MAC Address	00:00:00:00:00:00
IP Address	81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBECEDE868FD7D21A27E77
Geolocation	

In neuen Warnmeldungen werden verschleierte Daten angezeigt.

**Hinweis:** Vorhandene Warnmeldungen können weiterhin sensible Daten enthalten. Das Verfahren funktioniert nicht rückwirkend.

## Managen von Incidents in NetWitness SecOps Manager

Wenn Sie Incidents in RSA NetWitness® SecOps Manager anstelle von NetWitness Respond managen möchten, müssen Sie Systemintegrationseinstellungen in der Ansicht „Durchsuchen“ von Antwortserver-Dienst konfigurieren. Nach der Konfiguration der Systemintegrationseinstellungen werden alle Incidents in NetWitness SecOps Manager gemanagt. Vor der Integration erstellte Incidents werden nicht in NetWitness SecOps Manager gemanagt.



**Achtung:** Wenn Sie Incidents in NetWitness SecOps Manager anstelle von NetWitness Respond managen, verwenden Sie Folgendes in der Ansicht „Reagieren“ nicht: Ansicht „Incidents-Liste“, Ansicht „Incident-Details“ und Ansicht „Aufgabenliste“. Erstellen Sie Incidents nicht aus der Listenansicht der Respond-Warmmeldungen.

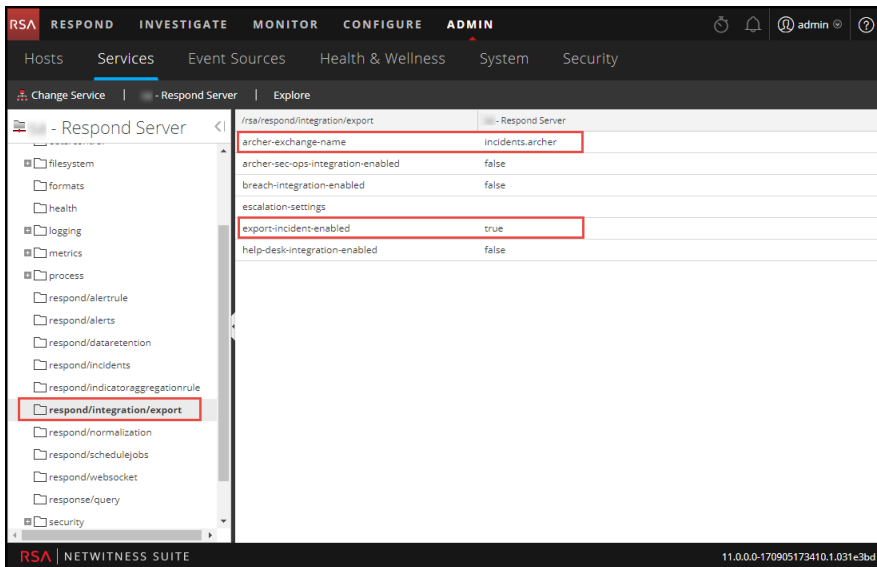
### Voraussetzungen

- NetWitness SecOps Manager 1.3.1.2 (NetWitness Suite 11.0 funktioniert nur mit NetWitness SecOps Manager 1.3.1.2.)

### Verfahren

Befolgen Sie dieses Verfahren zum Konfigurieren von Respond Server-Serviceeinstellungen zum Management von Incidents in NetWitness SecOps Manager.

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie den Antwortserver-Dienst aus und wählen Sie dann   > **Konfiguration > Durchsuchen**.
2. Wählen Sie in der Node-Liste der Ansicht „Durchsuchen“ **respond/integration/export** aus.





3. Geben Sie im Feld **archer-exchange-name** den Exchange-Namen von NetWitness SecOps Manager ein.  
Eine Meldung wird angezeigt, dass die Konfiguration erfolgreich aktualisiert wurde.
4. Wählen Sie im Feld **archer-sec-ops-integration-enabled** die Option **true** aus.  
Eine Meldung wird angezeigt, dass die Konfiguration erfolgreich aktualisiert wurde.  
Incidents werden ausschließlich in NetWitness SecOps Manager verwaltet.

## Einstellen des Zählers für abgestimmte Warnmeldungen und Incidents

Dieses Verfahren ist optional. Administratoren können damit ändern, wann der Zähler für abgestimmte Warnmeldungen auf 0 zurückgesetzt wird. Auf der Registerkarte „Aggregationsregeln“ werden diese Zähler in Spalten auf der rechten Seite angezeigt.

Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
1	●	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication wi...		0	0
2	●	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA ...		0	0
3	●	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA ...		0	0
4	●	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA ...	2017-08-11 18:2...	2510	62
5	●	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ...	2017-08-12 20:0...	105464	1236
6	●	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addre...		0	0
7	●	User Watch List: Activity Detected	This incident rule captures alerts generated by network ...		0	0
8	●	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of w...		0	0
9	●	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common l...		0	0
10	●	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert desig...		0	0
11	●	Web Threat Detection	This incident rule captures alerts generated by the RSA ...		0	0


Diese Spalten bieten die folgenden Informationen für eine Regel:

- Die Spalte **Zuletzt abgestimmt** zeigt die Uhrzeit an, zu der die Regel zuletzt Warnmeldungen abgestimmt hat.
- Die Spalte **Abgestimmte Warnmeldungen** zeigt die Anzahl der abgestimmten Warnmeldungen für die Regel an.
- Die Spalte **Incidents** zeigt die Anzahl der von der Regel erstellten Incidents an.

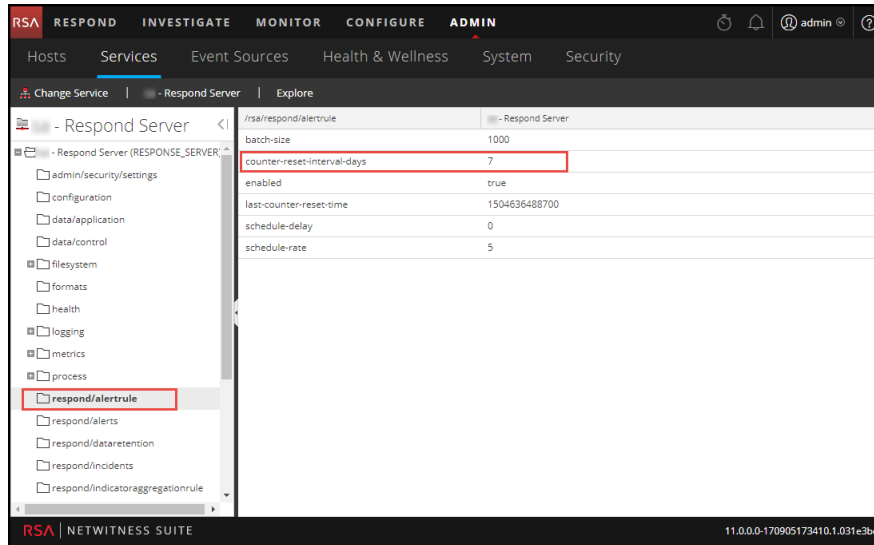
Standardmäßig werden diese Werte alle 7 Tage auf Null zurückgesetzt. Je nachdem, wie lange die Zählungen fortgesetzt werden sollen, können Sie die Standardanzahl der Tage ändern.


**Hinweis:** Wenn der Zähler auf Null zurückgesetzt wird, wechseln nur die Zahlen in den drei Spalten auf Null. Es werden keine Warnmeldungen oder Incidents gelöscht.

### So stellen Sie einen Zähler für abgestimmte Warnmeldungen und Incidents ein:

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie den Antwortserver-Dienst aus und wählen Sie dann  > **Ansicht > Durchsuchen**.

2. Wählen Sie in der Ansicht „Durchsuchen“ der Node-Liste **respond/alertrule** aus.



3. Geben Sie im rechten Bereich die Anzahl der Tage in das Feld **counter-reset-interval-days** ein.
4. Starten Sie Antwortserver-Dienst neu, damit die Änderungen wirksam werden. Navigieren Sie hierzu zu **ADMIN > Services**, wählen Sie Antwortserver-Dienst aus und anschließend  > **Neu starten**.

## Konfigurieren einer Datenbank für den Respond Server-Service


Dieses Verfahren ist nur dann erforderlich, wenn Sie die Datenbankkonfiguration für den Respond Server nach der Bereitstellung der NetWitness- oder ESA Primary-Hosts und ihrer entsprechenden Services ändern müssen. Sie müssen den ESA Primary-Server als Datenbankhost für NetWitness Respond-Anwendungsdaten festlegen, wie z. B. Warnmeldungen, Incidents und Aufgaben. Außerdem müssen Sie den NetWitness Server als Datenbankhost für NetWitness Respond-Kontrolldaten festlegen, wie z. B. Aggregationsregeln und Kategorien.

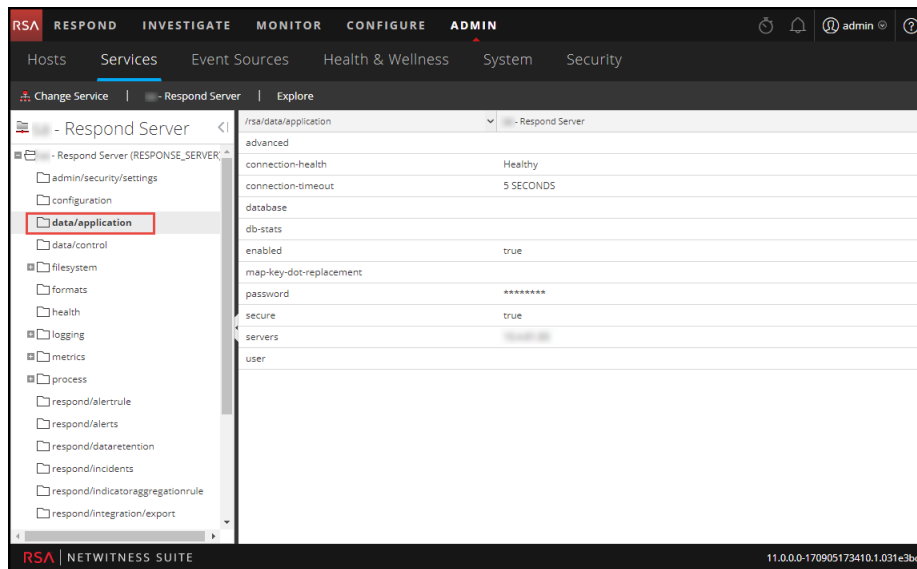
### Voraussetzungen

Stellen Sie Folgendes sicher:

- Sie haben einen Host installiert, auf dem Sie den Antwortserver-Dienst ausführen möchten. Siehe „Schritt 1: Bereitstellen eines Hosts“ im *Leitfaden für die ersten Schritte mit Hosts und Services* zum Verfahren für das Hinzufügen eines Hosts.
- Antwortserver-Dienst ist installiert und wird auf NetWitness Suite ausgeführt.
- Ein ESA-Host ist installiert und konfiguriert.

### Verfahren

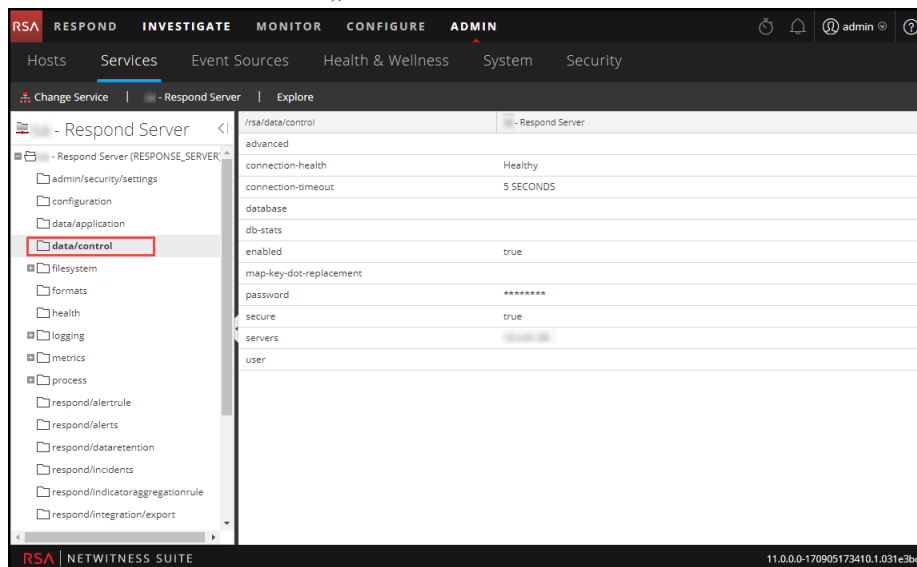
1. Navigieren Sie zu **ADMIN > Services**.  
Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie im Bereich „Services“ den **Antwortserver-Service** und dann  > **Ansicht > Durchsuchen** aus.
3. Wählen Sie in der Ansicht „Durchsuchen“ der Node-Liste **data/application** aus.





#### 4. Stellen Sie folgende Informationen bereit:

- **database:** Der Name der Datenbank. Standardwert ist „respond-server“.
- **password:** Das Passwort für die Bereitstellung des ESA Primary-Servers (Passwort für Benutzer „deploy\_admin“).
- **servers:** Der Hostname oder die IP-Adresse des **ESA Primary-Servers**, der als Datenbankhost für NetWitness Respond-Anwendungsdaten fungiert, wie z. B. Warnmeldungen, Incidents und Aufgaben.
- **user:** Geben Sie **deploy\_admin** ein.

#### 5. Wählen Sie in der Ansicht „Durchsuchen“ der Node-Liste **data/control** aus.



#### 6. Stellen Sie folgende Informationen bereit:

- **database:** Der Name der Datenbank. Standardwert ist „respond-server“.
  - **password:** Das Passwort für die Bereitstellung von NetWitness-Server (Passwort für Benutzer „deploy\_admin“).
  - **servers:** Der Hostname oder die IP-Adresse von **NetWitness-Server**, der als Datenbankhost für NetWitness Respond-Kontrolldaten dient, wie z. B. Aggregationsregeln und Kategorien.
  - **user:** Geben Sie **deploy\_admin** ein.
7. Starten Sie Antwortserver-Dienst neu. Navigieren Sie hierzu zu **ADMIN > Services**, wählen Sie Antwortserver-Dienst aus und anschließend   > **Neu starten**.

**Hinweis:** Der Neustart von Antwortserver-Dienst ist wichtig, damit die Datenbankkonfiguration abgeschlossen werden kann.

## Konfiguration von NetWitness Respond – Referenz

---

Dieser Abschnitt enthält Referenzinformationen für die Konfiguration von NetWitness Respond.

### **Ansicht „Konfigurieren“**

In der Ansicht „Konfigurieren“ können Sie die Funktionen von NetWitness Respond konfigurieren.

Sie haben die Möglichkeit, Aggregationsregeln zu konfigurieren, die den Respond-Workflow automatisieren. Incidents werden dann automatisch erstellt.

## Registerkarte „Aggregationsregeln“

Auf der Registerkarte „Aggregationsregeln“ können Sie Aggregationsregeln zur Automatisierung der Incident-Erstellung erstellen und verwalten. NetWitness Suite stellt 11 vorkonfigurierte Regeln bereit. Sie können diese Regeln ergänzen und an Ihre eigene Umgebung anpassen.

### Was möchten Sie tun?

Rolle	Ich möchte...	Anleitung
Analyst, Contentexperte, SOC-Manager	eine Aggregationsregel erstellen.	<a href="#">Schritt 3. Erstellen einer Aggregationsregel für Warnmeldungen</a>
Incident-Experten, Analysten, Contentexperten, SOC-Manager	die Ergebnisse einer Aggregationsregel anzeigen („Erkannte Bedrohungen anzeigen“).	Siehe „Reagieren auf Incidents“ im <i>NetWitness Respond-Benutzerhandbuch</i>

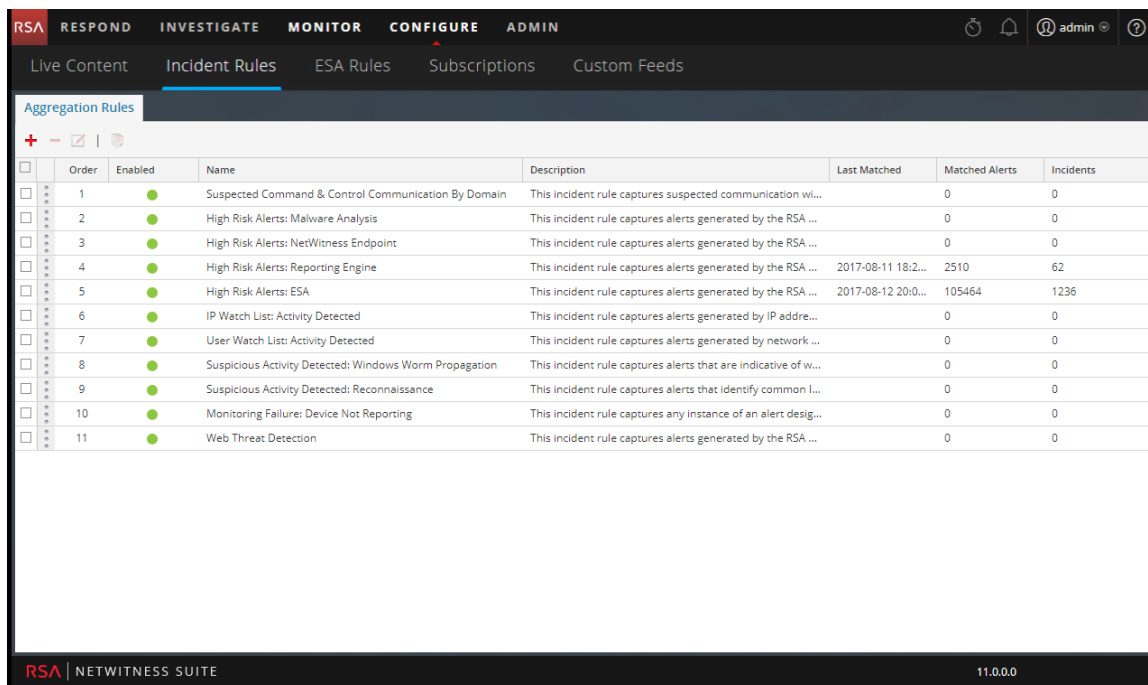
### Verwandte Themen

- [Registerkarte „Neue Regel“](#)

### Aggregationsregeln

Klicken Sie zum Öffnen der Registerkarte „Aggregationsregeln“ auf **Konfigurieren > Incident-Regeln > Aggregationsregeln**.





Die Registerkarte „Aggregationsregeln“ besteht aus einer Liste und einer Symbolleiste.

## Liste „Aggregationsregeln“





In der folgenden Tabelle werden die Spalten in der Liste „Aggregationsregeln“ beschrieben.

Spalte	Beschreibung
Auswählen	Ermöglicht, eine Regel auszuwählen, um eine Aktion dafür durchzuführen, etwa sie zu klonen oder zu löschen.
Reihenfolge	Zeigt die Position der Regel in der Regelreihenfolge an. Die Reihenfolge der Regeln legt fest, welche Regel aktiv wird, wenn die Kriterien mehrerer Regeln mit derselben Warnmeldung übereinstimmen. Wenn zwei Regeln mit einer Warnmeldung übereinstimmen, wird nur die Regel mit der höchsten Priorität ausgewertet.
Name	Zeigt den Namen einer Regel an.
Aktiviert	Zeigt an, ob die Regel aktiviert ist. ● gibt an, dass die Regel aktiviert ist.
Beschreibung	Zeigt die Beschreibung einer Regel an.

Spalte	Beschreibung
Zuletzt abgestimmt	Zeigt an, wann zuletzt eine Warnmeldung mit der Regel übereingestimmt hat. Dieser Wert wird einmal pro Woche zurückgesetzt.
Abgestimmte Warnmeldungen	Zeigt die Anzahl der Warnmeldungen an, die mit der Regel übereingestimmt haben. Dieser Wert wird einmal pro Woche zurückgesetzt. Informationen zum Ändern dieser Einstellungen erhalten Sie unter <a href="#">Einstellen des Zählers für abgestimmte Warnmeldungen und Incidents</a> .
Incidents	Zeigt die Anzahl der von der Regel erstellten Incidents an. Dieser Wert wird einmal pro Woche zurückgesetzt. Informationen zum Ändern dieser Einstellungen finden Sie unter <a href="#">Einstellen des Zählers für abgestimmte Warnmeldungen und Incidents</a> .

### Symbolleiste auf der Registerkarte „Aggregationsregeln“

In der folgenden Tabelle sind die Vorgänge aufgelistet, die Sie auf der Registerkarte „Aggregationsregeln“ durchführen können.

Option	Beschreibung
	Ermöglicht es Ihnen, eine neue Regel hinzuzufügen.
	Ermöglicht es Ihnen, eine Regel zu bearbeiten.
	Ermöglicht es Ihnen, eine Regel zu löschen.
	Ermöglicht es Ihnen, eine Regel zu duplizieren.

## Registerkarte „Neue Regel“

Auf der Registerkarte „Neue Regel“ können Sie benutzerdefinierte Aggregationsregeln erstellen, um die Incident-Erstellung zu automatisieren. In diesem Thema wird beschrieben, welche Informationen bei der Erstellung einer neuen Regel benötigt werden.

### Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Analyst, Contentexperte, SOC-Manager	Aggregationsregel erstellen	<a href="#">Schritt 3. Erstellen einer Aggregationsregel für Warmmeldungen</a>
Incident-Experten, Analysten, Contentexperten, SOC-Manager	Ergebnisse einer Aggregationsregel anzeigen („Erkannte Bedrohungen anzeigen“)	Siehe „Reagieren auf Incidents“ im <i>NetWitness Respond-Benutzerhandbuch</i> .

### Verwandte Themen

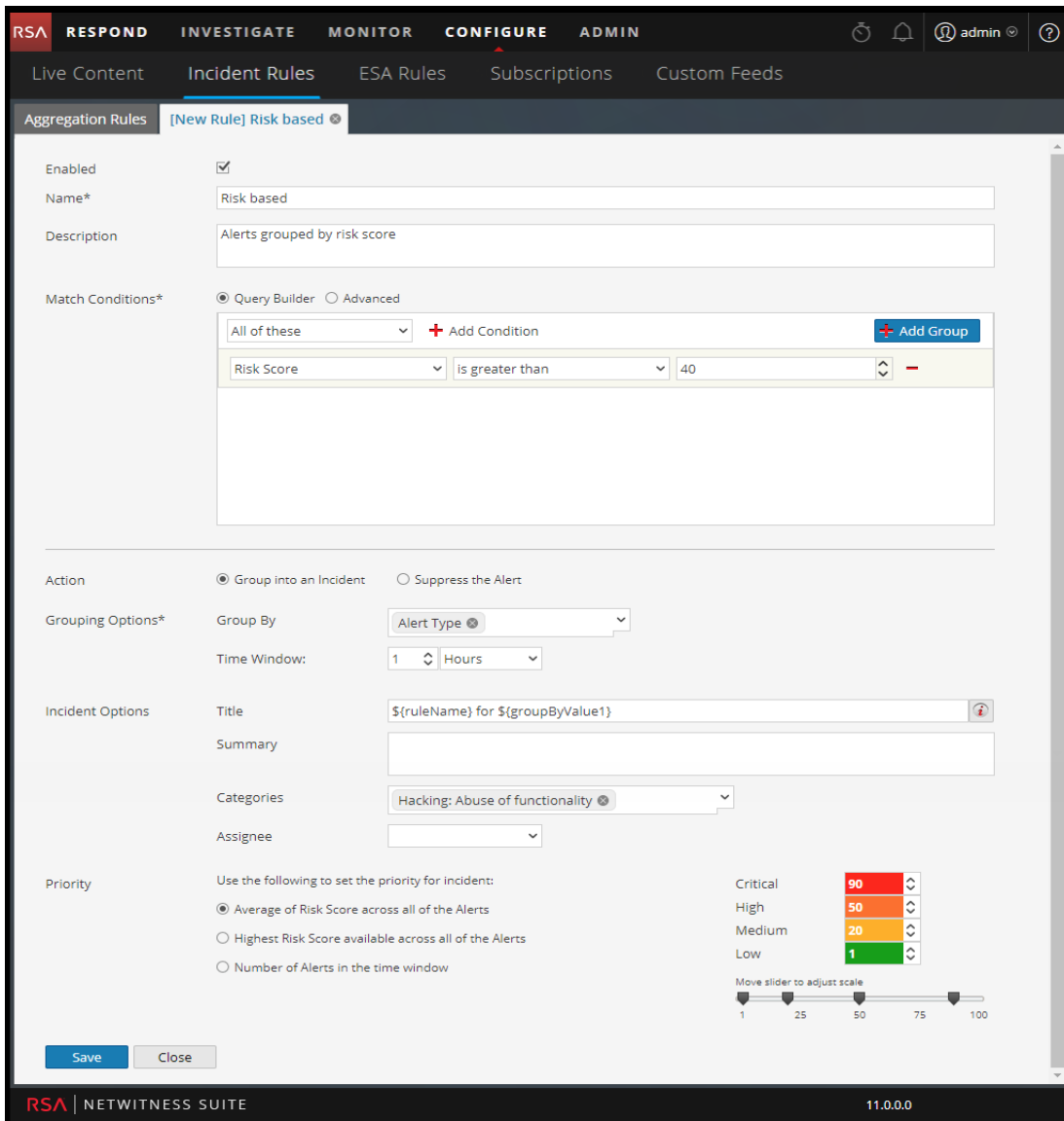
- [Registerkarte „Aggregationsregeln“](#)

### Neue Regel

So greifen Sie auf die Registerkartenansicht Neue Regel zu:

1. Navigieren Sie zu **Konfigurieren > Incident-Regeln > Aggregationsregeln**.
2. Klicken Sie auf **+**.

Die Registerkarte **Neue Regel** wird angezeigt.



In der folgenden Tabelle sind die Optionen beschrieben, die bei der Erstellung benutzerdefinierter Aggregationsregeln zur Verfügung stehen.

Feld	Beschreibung
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, um die Regel zu aktivieren.
Name*	Name der Regel. Dies ist ein Pflichtfeld.
Beschreibung	Eine Beschreibung der Regel, um knapp zu erläutern, welche Warnmeldungen kumuliert werden.

Feld	Beschreibung
Bedingungen abstimmen*	<p><b>Abfrageerstellung</b> – Markieren Sie diese Option, wenn Sie eine Abfrage mit verschiedenen Bedingungen erstellen möchten, die gruppiert werden können. Auch verschachtelte Gruppen von Bedingungen sind möglich.</p> <p>Bedingungen abstimmen - Sie können die folgenden Werte zum Abstimmen der Bedingungen auswählen: <b>Alle diese, Beliebige von diesen</b> oder <b>Nichts davon</b>. Abhängig von Ihrer Auswahl werden die in den Bedingungen und den Gruppen von Bedingungen angegebenen Kriterientypen abgestimmt, um die Warnmeldungen zu gruppieren.</p> <p><b>Beispiel:</b> Wenn Sie die Abstimmungsbedingung „Alle diese“ festlegen, werden die Warnmeldungen, die den in den Bedingungen und Gruppen von Bedingungen aufgeführten Kriterien entsprechen, in einem Incident gruppiert.</p> <ul style="list-style-type: none"> <li>• Klicken Sie zum Hinzufügen einer Abstimmungsbedingung auf <b>+</b> <b>Bedingung hinzufügen</b>.</li> <li>• Klicken Sie zum Hinzufügen einer Gruppe von Bedingungen zunächst auf <b>+</b> <b>Gruppe hinzufügen</b> und fügen Sie anschließend durch Klicken auf <b>+</b> <b>Bedingung hinzufügen</b> Bedingungen hinzu.</li> </ul> <p>Sie können mehrere Bedingungen und Gruppen von Bedingungen hinzufügen, die gemäß Kriteriensatz abgestimmt werden. Die eingehenden Warnmeldungen können Sie in Incidents gruppieren.</p> <p><b>Erweitert</b> – Markieren Sie diese Option, wenn Sie eine erweiterte Abfrageerstellung hinzufügen möchten. Sie können eine bestimmte Bedingung hinzufügen, die gemäß der ausgewählten Abstimmungsoption zutreffen muss.</p> <p><b>Beispiel:</b> Geben Sie das Kriterienerstellungsformat <code>{"\$and": [{"alert.severity": {"\$gt": 4}}]}</code> ein, um Warnmeldungen zu gruppieren, deren Schweregrad 4 übersteigt.</p> <p>Informationen zur erweiterten Syntax erhalten Sie unter <a href="http://docs.mongodb.org/manual/reference/operator/query/">http://docs.mongodb.org/manual/reference/operator/query/</a> oder <a href="http://docs.mongodb.org/manual/reference/method/db.collection.find/">http://docs.mongodb.org/manual/reference/method/db.collection.find/</a></p>

Feld	Beschreibung
Aktion	<p><b>In einen Incident eingruppiern</b> – Wenn diese Option aktiviert ist, werden die Warnmeldungen, die den festgelegten Kriterien entsprechen, in einer Warnmeldung gruppiert.</p> <p><b>Warnmeldung unterdrücken</b> – Wenn diese Option aktiviert ist, werden die den Kriterien entsprechenden Warnmeldungen unterdrückt.</p>
Gruppierungsoptionen*	<p><b>Gruppieren nach:</b> Hier finden Sie die verfügbaren Kriterien zur Gruppierung der Warnmeldungen ausgehend von der angegebenen Kategorie. Sie können Warnmeldungen anhand von maximal 2 Attributen gruppieren. Die Warnmeldungen können wahlweise anhand von 1 oder 2 Attributen gruppiert werden. Eine Gruppierung von Warnmeldungen anhand von Attributen ohne Wert (leere Attribute) ist nicht mehr möglich.</p> <p>Die Gruppierung anhand eines Attributs hat zur Folge, dass alle übereinstimmenden Warnmeldungen, die denselben Wert für dieses Attribut aufweisen, gemeinsam im selben Incident gruppiert werden.</p> <p><b>Zeitfenster:</b> Der festgelegte Zeitbereich für die Gruppierung der Warnmeldungen.</p> <p>Wenn Sie als Zeitfenster beispielsweise 1 Stunde angeben, werden alle Warnmeldungen in einem Incident gruppiert, die den im Feld „Gruppieren nach“ festgelegten Kriterien entsprechen und innerhalb einer Stunde aufeinanderfolgen.</p>

Feld	Beschreibung
Incident-Optionen	<p><b>Titel:</b> (Optional) Titel des Incident. Sie können Platzhalter auf Basis der gruppierten Attribute angeben. Die Platzhalter sind optional. Wenn Sie keine Platzhalter verwenden, erhalten alle durch die Regel erstellten Incidents denselben Titel.</p> <p>Wenn Sie beispielsweise eine Gruppierung anhand der Quelle konfiguriert haben, können Sie den resultierenden Incident „Warnmeldungen für <b>\${groupByValue1}</b>“ nennen. Dann würden die Incidents aller Warnmeldungen von NetWitness Endpoint zukünftig den Namen <b>Warnmeldungen für NetWitness Endpoint</b> erhalten.</p> <p><b>Zusammenfassung</b> (optional) – Zusammenfassung des Incident.</p> <p><b>Kategorie</b> (optional) – Kategorie des erstellten Incident. Ein Incident kann unter Verwendung von mehr als einer Kategorie klassifiziert werden.</p> <p><b>Zuweisungsempfänger</b> (optional) – Name des Empfängers, dem der Incident zugewiesen wird.</p>

Feld	Beschreibung
Priorität	<p><b>Durchschn. Risikobewertung für alle Warnmeldungen</b> – Verwendet den Durchschnitt der Risikobewertungen von allen Warnmeldungen, um die Priorität des erstellten Incident festzulegen.</p> <p><b>Höchste verfügbare Risikobewertung für alle Warnmeldungen</b> – Verwendet die höchste verfügbare Risikobewertung von allen Warnmeldungen, um die Priorität des erstellten Incident festzulegen.</p> <p><b>Anzahl der Warnmeldungen im Zeitfenster</b> – Verwendet die Anzahl von Warnmeldungen in dem ausgewählten Zeitfenster, um die Priorität des erstellten Incident festzulegen.</p> <p><b>„Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“</b> – Hier können Sie den Prioritätsschwellenwert festlegen, dem die Incidents entsprechen sollen. Die Standardwerte sind:</p> <ul style="list-style-type: none"> <li>• Kritisch: 90</li> <li>• Hoch: 50</li> <li>• Mittel: 20</li> <li>• Low: 1</li> </ul> <p>Beispiel: Wenn Sie für die Priorität „Kritisch“ den Wert „90“ festlegen, wird diese Regel Incidents mit einer Risikobewertung ab 90 die Priorität „Kritisch“ zuweisen.</p> <p>Zum Ändern dieser Standardeinstellungen können Sie die Prioritäten manuell anpassen oder den Schieberegler unter <b>Skala mit Schieberegler anpassen</b> entsprechend versetzen.</p>