RSA NETWITNESS® SUITE

# Benutzerhandbuch Reporting

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

# Reporting-Übersicht

Reporting ist eine Sammlung von Daten als Ergebnis der Überwachung des Netzwerkverkehrs, die zur weiteren Analyse verwendet werden kann. In NetWitness Suite können Sie einen Bericht für NetWitness Suite-Datenbank-Core-Services ausführen, um die Netzwerkaktivitäten zu identifizieren. Beispiel: Sie möchten die führenden Quell- und Zielländer oder die wichtigsten Bedrohungs- und Risikotrends identifizieren, mit denen alle Änderungen an den normalen Kategorien oder die Benutzer und Services überwacht werden können, die möglicherweise schädliche Aktivitäten usw. ausführen.

Das Reporting besteht in der Regel aus folgenden Komponenten: Berichte und Diagramme. Sie können Berichte für die erfassten Protokoll- und Paketdaten erstellen sowie Berichte und Diagramme anpassen, um die visuelle Darstellung zu verbessern. Sie können Echtzeitberichte über Verlaufsdaten erstellen. Sie können Diagramme und Dashlets erstellen, die auch zu Echtzeitdiagramm-Dashlets hinzugefügt werden können.

## Reporting Engine

Reporting verwendet für die Berichte, Warnmeldungen und Diagramme von der Reporting Engine bereitgestellte Daten. Daher müssen Sie die Reporting Engine als Service für NetWitness Suite konfigurieren, bevor Sie Berichte erstellen können. Außerdem müssen Sie die Datenquelle in der Reporting Engine festlegen, aus der die Daten extrahiert werden.

Die Daten, für die Sie einen Bericht oder eine Warnmeldung erstellen können, sind abhängig von der Konfiguration der Reporting Engine und den Datenquellen, die Sie als Teil der Regeldefinition festlegen.

**Hinweis:** Vergewissern Sie sich, dass Sie Zugriff auf die Komponenten im Reporting haben.

**Hinweis:** Vergewissern Sie sich, dass Sie Zugriff auf die erforderlichen Datenquellen haben. Nur Benutzer mit den nötigen Berechtigungen für den Zugriff auf vertrauliche Informationen dürfen auf bestimme Datenquellen zugreifen. Wenn Sie die Zugriffssteuerung auf Datenquellen verwalten möchten, finden Sie weitere Informationen unter „Hinzufügen einer Rolle und Zuweisen von Berechtigungen für Warehouse Analytics“ im *Leitfaden Warehouse Analytics*. Wenn die Benutzerrolle oder die Berechtigungen für die Datenquellen geändert werden, wird dies jedoch nur dann für vorhandene Berichte, Warnmeldungen und Diagramme angewendet, wenn Sie die Berechtigungen manuell aktualisieren.

**Hinweis:** Der Zugriff auf Reporting basiert auf den für den Benutzer definierten rollenbasierten Zugriffsberechtigungen.

## Bericht

Ein Bericht ist eine Kombination von Regeln und anderen Formatierungsobjekte wie Überschriften und mit HTML formatierten Hinweisen, die Daten zu einem bestimmten Bereich, der von Interesse ist, beschreiben und identifizieren. Berichte werden auf der Seite „Bericht erstellen“ definiert und gemanagt und können spontan oder anhand eines Zeitplans ausgeführt werden. Wenn ein Bericht ausgeführt wird, werden die Ergebnisse zentral gespeichert und können automatisch per E-Mail, SFTP, URL und NFS an Benutzer gesendet, über die NetWitness Suite-Weboberfläche angezeigt oder als PDF- und CSV-Dateien heruntergeladen werden.

Ein Bericht besteht aus folgenden Elementen:

| Eigenschaft | Beschreibung | Beispiel |
|---|---|---|
| Name des Berichts<br>**Hinweis:** Für das Feld **Name** wird am Ende des Spaltenfelds kein Symbol zur Erweiterung der Spaltengröße angezeigt. Sie müssen die Maus ein wenig nach links bewegen, um das Symbol zur Erweiterung der Spalte zu sehen. | Dient zur Identifizierung des Berichts, damit er für einen späteren Zeitpunkt eingeplant werden kann. | Report1 |
| Text | Vordefinierte Textfelder werden innerhalb eines Berichts verwendet, um ihn für den Benutzer leichter verständlich zu machen. | Überschrift1, Kommentar |
| Regeln | Die Regeln (Abfragen), mit denen ein Bericht erstellt wird. | select user.dst<br>where ip.src = 10.10.10.1 |

**Hinweis:** In der Reporting-Benutzeroberfläche entsprechen das Datum und die Uhrzeit immer dem vom Benutzer ausgewählten Zeitzonenprofil.

## Regel

Eine Regel ist der grundlegende, wesentliche Baustein im Reporting. Sie müssen eine Regel erstellen, die in einem Bericht, einem Diagramm oder einer Warnmeldung verwendet werden kann.

Eine Regel stellt eine eindeutige Abfrage dar, die die angeforderten Informationen in einer Sammlung von Netzwerkdaten erkennt und zusammenfasst.

Die Regelsyntax ähnelt der von Standard Query Language (SQL), in der Sie die select- und where-Klausel verwenden sowie Optionen und Einschränkungen für den Ergebnissatz sortieren und gruppieren können. Eine Regel besteht aus folgenden Elementen:

| Eigenschaft | Beschreibung | Beispiel |
|---|---|---|
| Name | Der Name der Regel | Aktivität des Windows-Systemkontos |
| Auswählen | Die Liste der Metadatentypen, die im Ergebnissatz zurückgegeben werden. Die Liste der Metadatentypen wird in der Metabibliothek bereitgestellt. Die Metabibliothek in der Regelerstellung wird fortlaufend mit der Indexkonfiguration des NetWitness Suite-Hosts synchronisiert, mit dem NetWitness Suite verbunden ist. Die Anzahl der Metadatentypen, die diese Eigenschaft darstellen kann, hängt davon ab, wie die Regel sortiert werden soll. Wenn für die Eigenschaft Sortieren nach der Wert Keine oder Nicht aggregiert angegeben ist, kann eine Regel mehrere Auswahlfelder zum Beispiel für jede Übereinstimmung enthalten, einschließlich ip.src, ip.dst, Größe und Uhrzeit im Ergebnis der Regel. Wenn für eine Regel eine Sortierung nach Sitzungsanzahl, Sitzungsgröße oder Paketgröße festgelegt wurde, darf nur ein Feld vorhanden sein, in dem die Auswahl erfolgt. | |

| Eigenschaft | Beschreibung | Beispiel |
|---|---|---|
| Dabei gilt Folgendes: | Eine Klausel, die das grundlegende Abfragekriterium für die Regel darstellt. | `alert='cleartext_ftp_passwords'` |
| Then (Regelaktionen) | Eine Reihe von Funktionen, mit denen der ursprüngliche Ergebnissatz einer Regel verändert wird, um die Ausgabe in einem Bericht aussagekräftiger zu machen oder um zusätzliche, andere Funktionen als die Abfrage und Anzeige von Daten hinzuzufügen | `lookup_and_add ('username','ip.src',10);` |
| Sortieren nach | Legt fest, wie die Daten im Ergebnissatz sortiert werden. Folgende Optionen stehen zur Verfügung:<br>• Gesamt<br>• Wert<br>• Spaltenname | Gesamt |
| Einschränkung | Bezeichnet die maximale Größe eines Ergebnissatzes für die angegebene Regel. Benutzer sollten beachten, dass bei Sortierung eines Ergebnissatzes nach Anzahl oder Größe der Grenzwert die N oberen (oder unteren) zurückzugebenden Werte darstellt. Wenn die Ergebnismenge nicht sortiert wird, werden die ersten n Werte wiedergegeben. | 20 |

**Hinweis:** Die in der Benutzeroberfläche (UI) angezeigte Uhrzeit und das angezeigte Datum hängen von der Zeitzone ab, die vom Benutzer ausgewählt wurde.

## Regeltypen

Es gibt im Reporting verschiedene Regeltypen. Regeltypen bestimmen die Datenquelle für die Berichtsregel. Es gibt folgende Regeltypen:

| Regeltyp | Beschreibung |
|---|---|
| NetWitness-Datenbank (**NetWitness-DB**) | Die NetWitness-Datenbank extrahiert die Metadaten aus einer Reporting Engine, die für die Verwendung eines Concentrator, Broker und Archiver als Datenquellen konfiguriert wurde und die Metadaten für die Regeln bereitstellt. |
| Warehouse-Datenbank (**Warehouse-DB**) | Die Warehouse-Datenbank, die auch als RSA NetWitness Warehouse bezeichnet wird, beinhaltet große Datenmengen. Das Warehouse ist darauf ausgelegt, dass Sie einfach und effizient große Datenvolumen abrufen können. Das Warehouse extrahiert außerdem Metadaten aus der Reporting Engine. |
| Antwort-Datenbank (**Antwort-DB**) | Die Antwort-Datenbank erstellt Berichte zu Warnmeldungen und Incidents. Die Antwort-Datenbank enthält Warnmeldungen und Incidents, die aus verschiedenen Services generiert wurden, und Sie können einen Bericht für diese Warnmeldungen und Incidents erstellen. |

**Hinweis:** Die in der Benutzeroberfläche (UI) angezeigte Uhrzeit und das angezeigte Datum hängen von der Zeitzone ab, die vom Benutzer ausgewählt wurde.

## Liste

Eine Liste ist eine Variable, die auf eine Serie durch Kommas getrennter Werte (Comma-Separated Values, CSV) verweist. Eine Liste können Sie in eine Regel einfügen oder als Argument für eine Regelaktion verwenden. Listen können als Platzhalter für andere Werte dienen, die Sie dann in die Liste eintragen und bei Bedarf aktualisieren können.

Sie können Listen erstellen, managen und anzeigen, die zum Definieren von Regeln für Reporting und Alerting verwendet werden können.

Listen dürfen nicht leer sein oder doppelte oder leere Werte enthalten.

**Hinweis:** Wenn Sie einen Bericht mit einer Regel definieren, die „lookup_and_add“ in der **Then**-Klausel enthält, und die Berichtsausgabe in eine Liste leiten, wird die Liste nicht mit dem Ergebnis gefüllt.
Beispiel: Wenn Sie eine Regel mit „ip.src“ in der **Select**-Klausel und „lookup_and_add“ ('ip.dst','ip.src', 10) in der **Then**-Klausel erstellen, zeigt der Bericht das Ergebnis an. Wenn Sie aber die Ausgabe in eine Liste umleiten, ist die Liste leer.

## Diagramm

Diagramm ist eine tabellarische oder rasterbasierte Darstellung von Daten. Es beinhaltet Folgendes:

| Eigenschaft | Beschreibung | Beispiel |
|---|---|---|
| Diagrammname | Identifiziert das Diagramm. | Chart1 |
| Regelbasis | Identifiziert den in der Ordnerhierarchie gewählten Regelpfad. | |

Mit jeder NetWitness Suite DB-Regel im Reporting Engine-System, die nicht nach „Keine“ sortiert ist, kann sofort ein Diagramm erstellt werden. In NetWitness Suite kann das Diagrammintervall im Bereich „Diagrammdefinition“ selbst angepasst werden. Bei jeder Ausführung eines Diagramms werden die Ergebnisdaten lokal in der Reporting Engine gespeichert, sodass sie ohne Performanceerwägungen entweder in der Dashboardansicht oder in der Diagrammansicht geprüft werden können.

**Hinweis:** In der Benutzeroberfläche „Reporting“ erfolgt die Ausgabe für das Feld, in dem Datum und Zeit angezeigt werden, immer gemäß dem vom Benutzer ausgewählten Zeitzonenprofil.

**Hinweis:** Die Reporting Engine (RE) prüft vor der Ausführung einer Regel, eines Berichts, eines Diagramms und einer Warnmeldung automatisch den verfügbaren Speicherplatz. Wenn der RE-Speicherplatz (in Prozent) kleiner ist als der Mindestschwellenwert für Speicherplatz (der Standardwert ist 5), hält die RE die aktuelle Ausführung an und es wird die Fehlermeldung angezeigt, dass der verfügbare Speicherplatz des Reporting Engine-Stammverzeichnisses niedriger als 5 % ist und dass Speicherplatz freigegeben werden muss, bevor der Vorgang fortgesetzt werden kann. Darüber hinaus können Sie den minimalen Schwellenwert für Festplattenspeicherplatz auch mithilfe des folgenden Pfads festlegen: **RE>Explore>com.rsa.soc.re>Configuration>CommonConfig>minDiskSpaceThreshold**.

## Reporting-Richtlinien

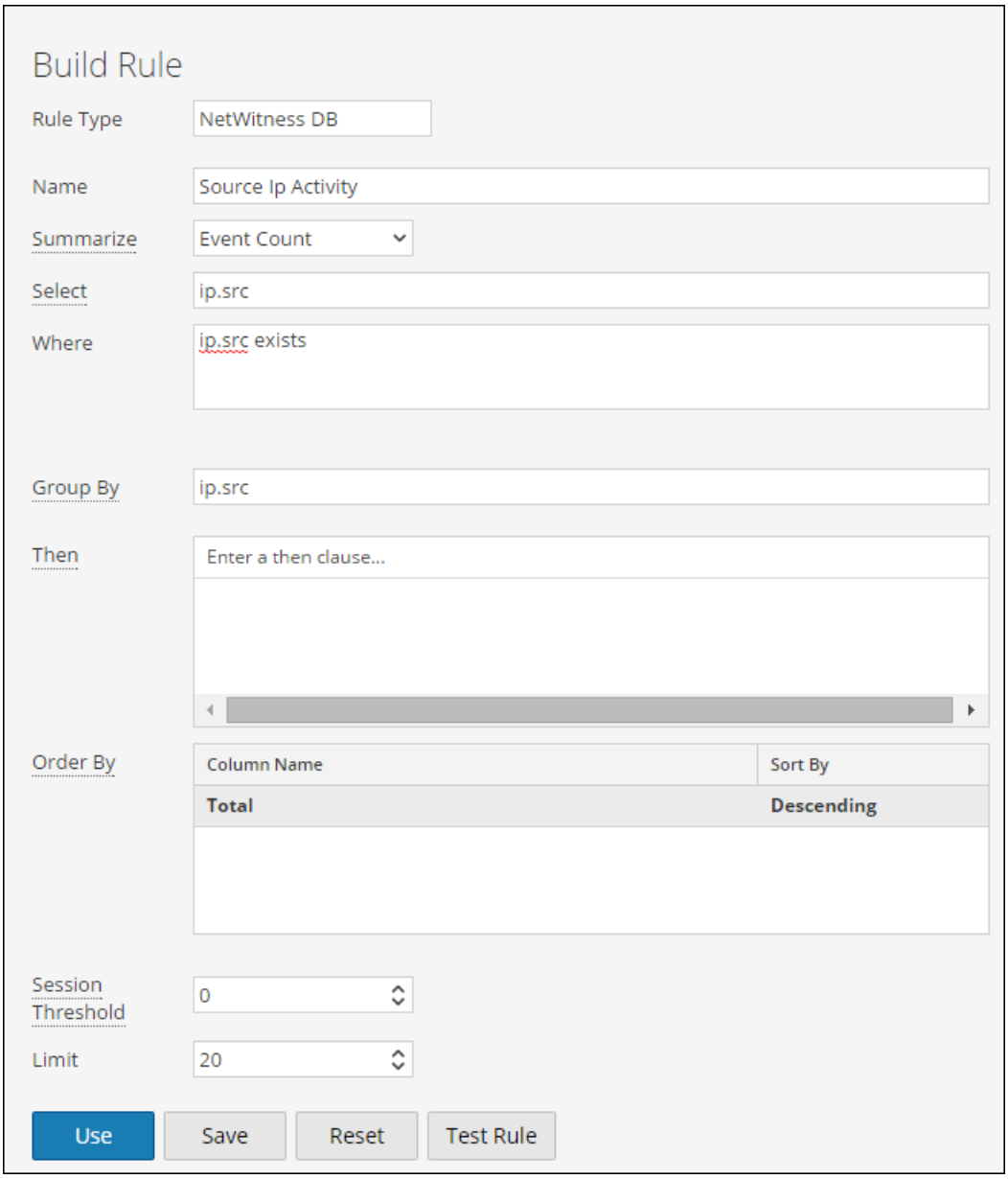
In diesem Abschnitt werden die von RSA empfohlenen Richtlinien zur Verbesserung der Ausführungszeit Ihrer Reportingentitäten erläutert, wie z. B. Regeln, Berichte, Warnmeldungen, Diagramme und Listen. Die Richtlinien gelten für Folgendes:

- NWDB-Regeln
- Timeout-Konfiguration für NWDB-Regeln
- Lookup_and_Add-Regelaktion
- Listenwertberichte

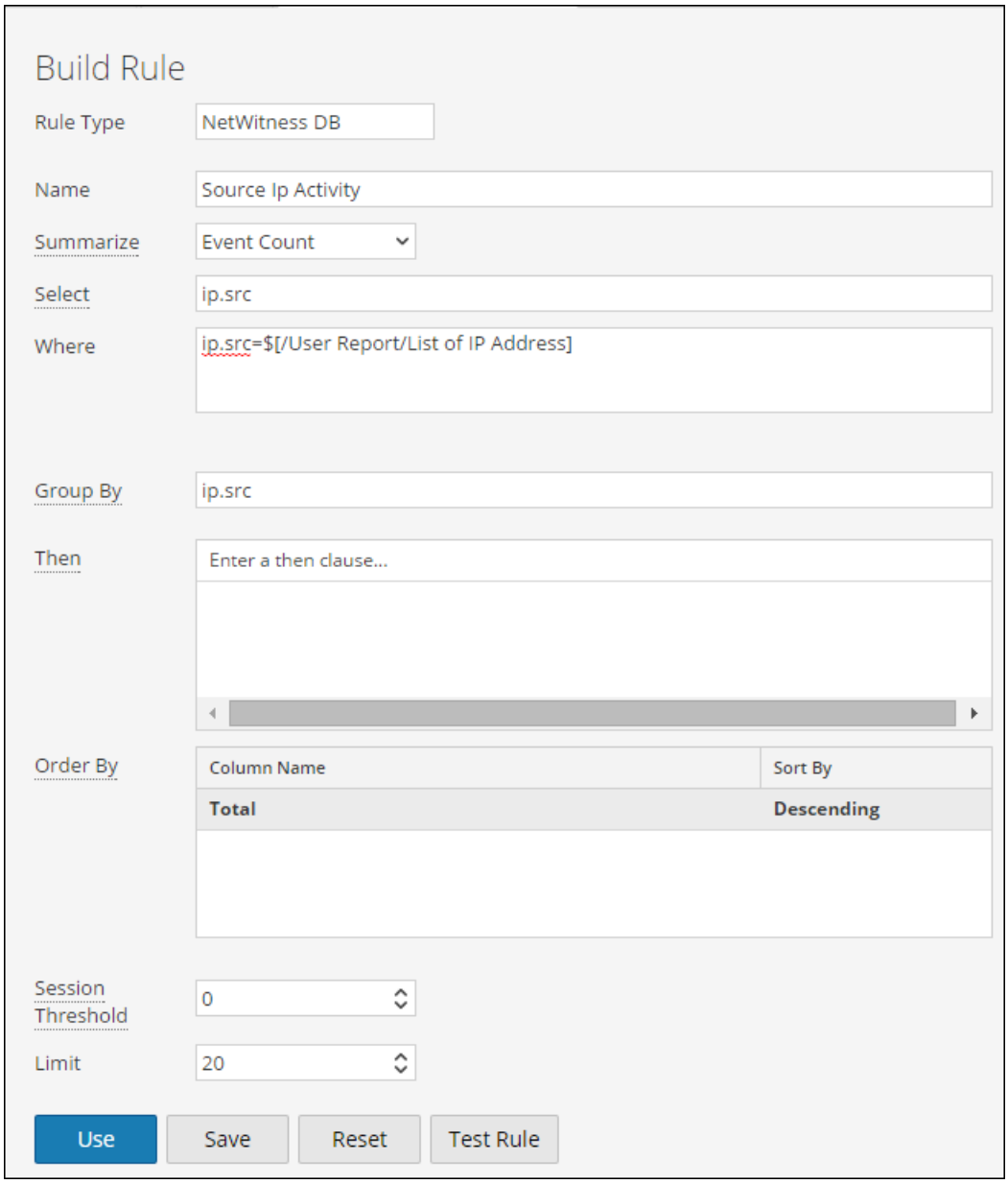
## NWDB-Regeln

Wenn die Reportingentitäten wie Berichte, Warnmeldungen oder Diagramme NWDB-Regeln enthalten (meist wenn die Abfrage „Gruppieren nach“ enthält) und die Ausführung viel Zeit in Anspruch nimmt, können Sie wie folgt vorgehen:

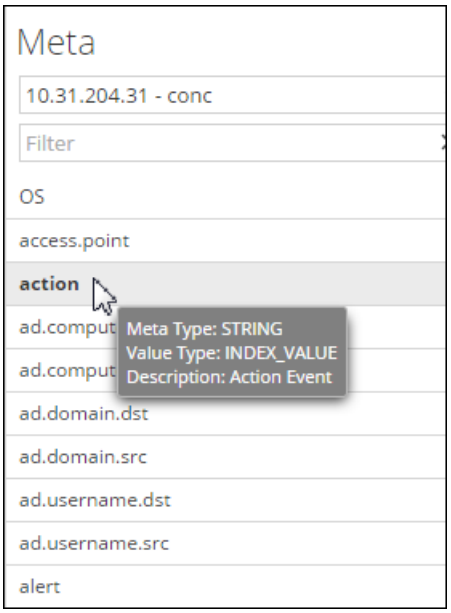
1. Anpassen der Where-Klausel:
   Sie können die Anzahl der gescannten Sitzungen einschränken, indem Sie die Where-Klausel verwenden oder anpassen (insbesondere bei Verwenden der Option „Gruppieren nach“). Betrachten Sie zum Beispiel die folgende Regel.




Wenn Sie eine Where-Klausel wie im obigen Beispiel verwenden, ist die Anzahl der aggregierten Sitzungen sehr groß. Um dies zu vermeiden, können Sie nur die erforderlichen Sitzungen filtern, indem Sie die Liste der IP-Adressen angeben oder eine Liste (Liste der IP-Adressen) erstellen, die die relevanten IP-Adressen enthält.




2. Verwenden indexierter Metaschlüssel in der Where-Klausel:
   Bewegen Sie die Maus über den Metaschlüssel, um festzustellen, ob Meta indexiert ist oder nicht. Wenn der Werttyp INDEX_VALUE lautet, ist Meta indexiert. Wenn der Werttyp INDEX_KEY oder INDEX_NONE lautet, ist Meta nicht indexiert.
   Im Folgenden ist ein Snapshot eines indexierten Metaschlüssels dargestellt.




3. Konfigurieren der Timeout-Option:
   Wenn die Ausführung der Abfrage lange dauert und aufgrund eines Timeouts fehlschlägt, können Sie das Timeout für die NWDB-Regelausführungen konfigurieren. Weitere Informationen finden Sie im folgenden Abschnitt „Timeout-Konfiguration für NWDB-Regeln“.
4. Planen der Ausführung der Abfragen zu unterschiedlichen Zeiten:
   Wenn mehrere Abfrageaggregate gleichzeitig ausgeführt werden und ein Timeout auftritt, können Sie die Abfragen so planen, dass sie ohne Überschneidungen zu unterschiedlichen Zeiten ausgeführt werden.

## Timeout-Konfiguration für NWDB-Regeln

**Hinweis:** Es wird empfohlen, die Statistiken der Reporting Engine und die NWDB-Datenquellen zu prüfen, bevor Sie Änderungen an der Konfiguration vornehmen. Weitere Informationen finden Sie im Thema „Überwachen von Servicedetails“ für die Reporting Engine und im Thema „Überwachen der Systemstatistiken“ im *Leitfaden Systemwartung*.

Wenn eine NWDB-Regelausführung aufgrund eines Timeouts fehlschlägt, werden möglicherweise folgende Fehlermeldungen auf der Seite „Bericht anzeigen“ eingeblendet:

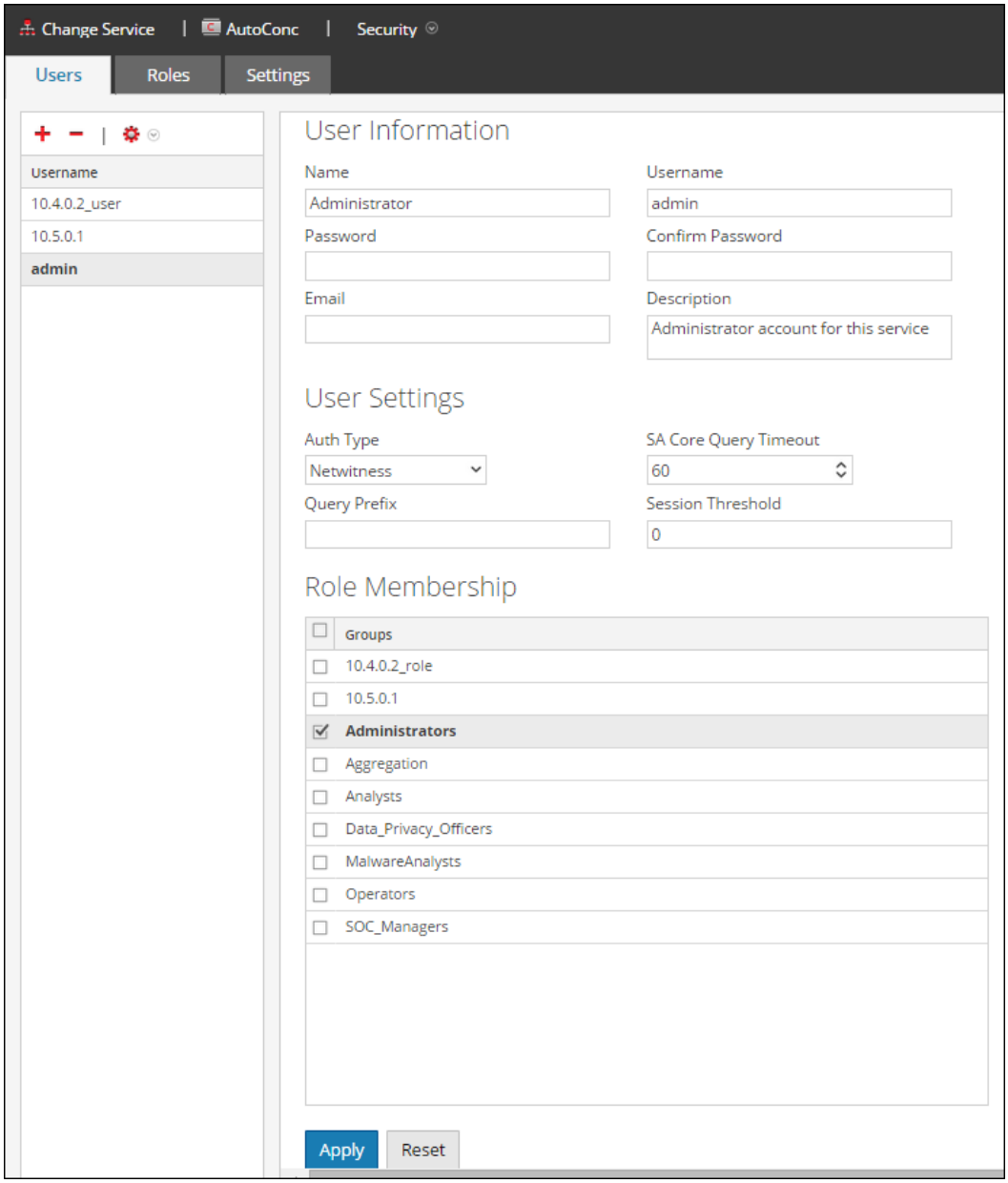
- Reporting Engine-Timeout-Fehler
  - „Datenquelle ‚`10.31.x.x Concentrator`‘ hat nicht innerhalb der konfigurierten `30` Minuten auf die Anforderung ‚`/sdk/values`‘ reagiert.“

- NWDB-Timeout-Fehler
  - „Beim Abrufen der Daten aus Quelle ‚`10.31.x.x Concentrator`‘ ist ein Fehler aufgetreten. `{Timeout message from NWDB}`“

  Gehen Sie in diesem Fall wie folgt vor:

  - Reporting Engine-Timeout
    Bei einem Reporting Engine-Timeout können Sie das Timeout auf eine längere Dauer einstellen, sodass die lang laufenden Abfragen ausgeführt werden können. Weitere Informationen zum Einrichten der `NWDB Queries Time Out`- und `NWDB Info Queries Time Out`-Option für die Reporting Engine finden Sie im Thema „Schritt 2. „Konfigurieren der Reporting-Engine-Einstellungen“ im *Konfigurationsleitfaden Reporting Engine*. RSA empfiehlt, die Option `NWDB Query Time Out` auf 0 Minuten einzustellen (dies bedeutet kein Timeout) und die Option `NWDB Info Queries Time Out` auf 60 Minuten.
  - NWDB-Timeout
    Bei einem NWDB-Timeout müssen Sie möglicherweise die Parameter `query.level.timeout` und `max.concurrent.queries` für die NWDB-Datenquelle anhand der Empfehlungen im *Tuningleitfaden für die Core-Datenbank* konfigurieren, um die Abfragen im Detail anzupassen.
    Die folgende Abbildung ist ein Beispiel für die Explorer-Ansicht, in der Sie die

Parameter für die NWDB-Datenquelle festlegen können.




- Planen von Berichten zu unterschiedlichen Zeiten
  Wenn die NWDB-Core-Geräte viel und intensiv genutzt werden, können Sie die Berichte so planen, dass sie ohne Überschneidung zu unterschiedlichen Zeiten ausgeführt werden.
- Teilen des Berichts
  Wenn viele Regeln in einem Bericht enthalten sind, können Sie ihn in mehrere Berichte

aufteilen, wobei jeder Bericht logische Regelsätze enthält. Wenn mehrere Regeln vorhanden sind, werden alle Regeln basierend auf den verfügbaren Threads zur gleichen Zeit ausgeführt. Daher können Sie die Regeln in separate Berichte logisch gruppieren.

## LookupAndAdd-Regelaktion

Wenn eine Regel, die aus einer oder mehreren `lookup_and_add`-Regelaktionen besteht, für die Ausführung des Berichts eine lange Zeit benötigt, liegt dies daran, dass jede Regelaktion mehrere Suchabfragen in der NWDB-Datenquelle auslöst, sodass sich längere Ausführungszeiten ergeben.

Um die Ausführungszeit von Berichten zu verbessern, können Sie folgende Aktionen ausführen:

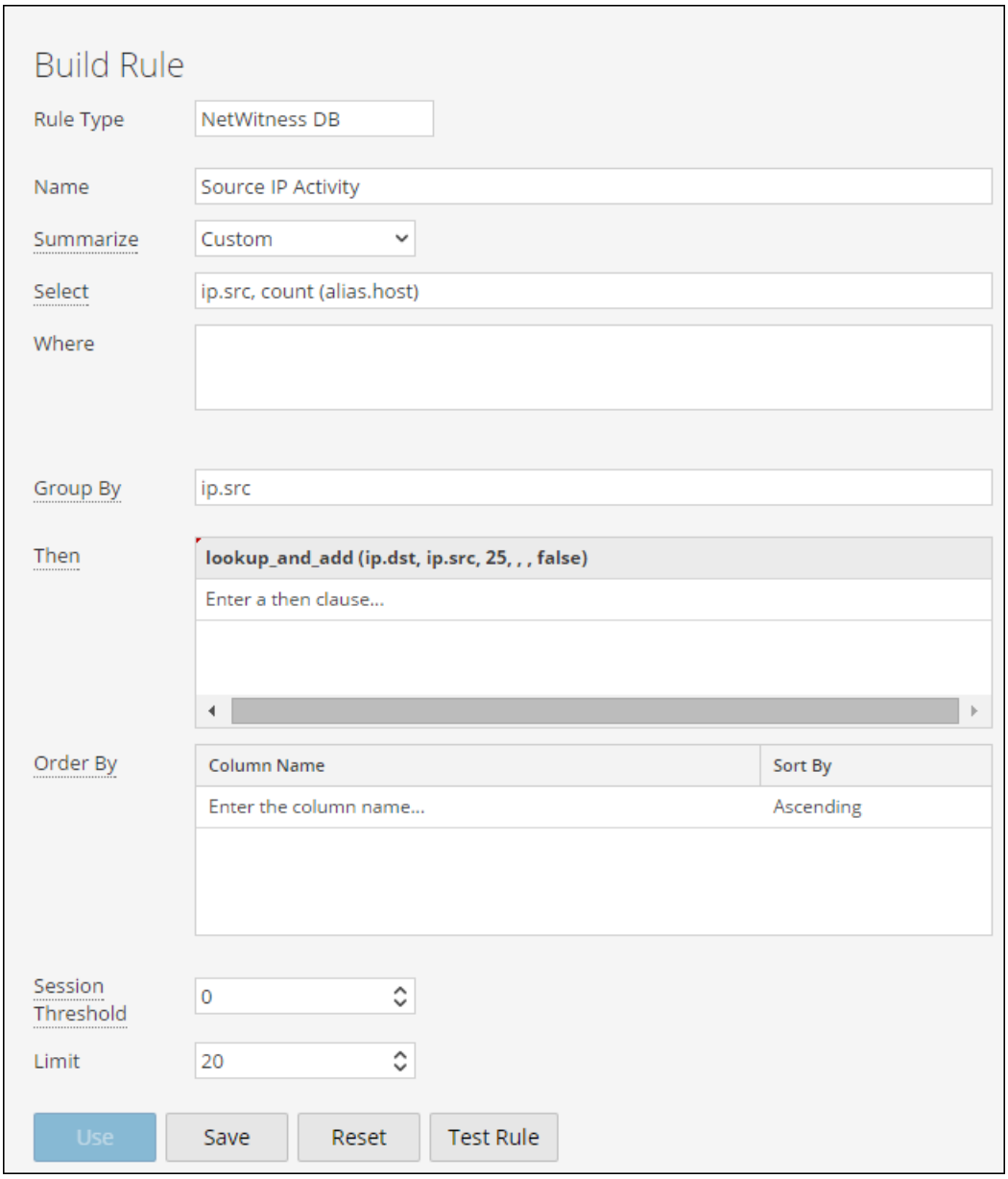
- Anpassen der Where-Klausel in den folgenden Regelaktionen:
  - Regel, die die `lookup_and_add`-Regelaktion enthält
  - `lookup_and_add`-Regelaktion:
- Festlegen von Grenzwerten

  Sie müssen die entsprechenden Grenzwerte für die Regel und Regelaktionen festlegen. Ein hoher Grenzwert führt dazu, dass viele Abfragen ausgelöst werden und daher die Ausführung des Berichts lange dauert.
- Festlegen des booleschen Aggregatparameters

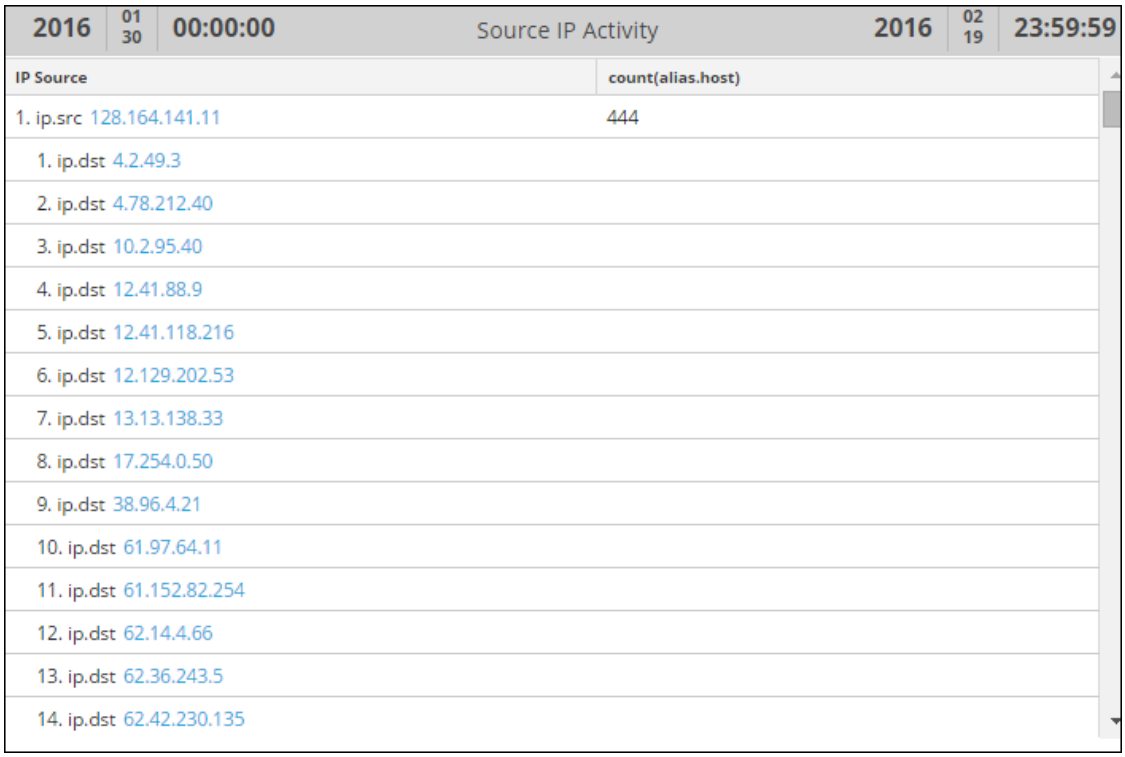
  Wenn für die Suchwerte keine Aggregatwerte wie `sum(meta), count(meta)` usw. verwendet werden sollen, legen Sie den booleschen Aggregatparameter in der `lookup_and_add`-Regelaktion auf „false“ fest. Weitere Informationen finden Sie im Abschnitt „NWDB-Regelsyntax“ unter Regelsyntax .

  ```
  lookup_and_add(string select, string field, int limit, boolean
  inherit, string extraWhere, boolean aggregate)
  ```

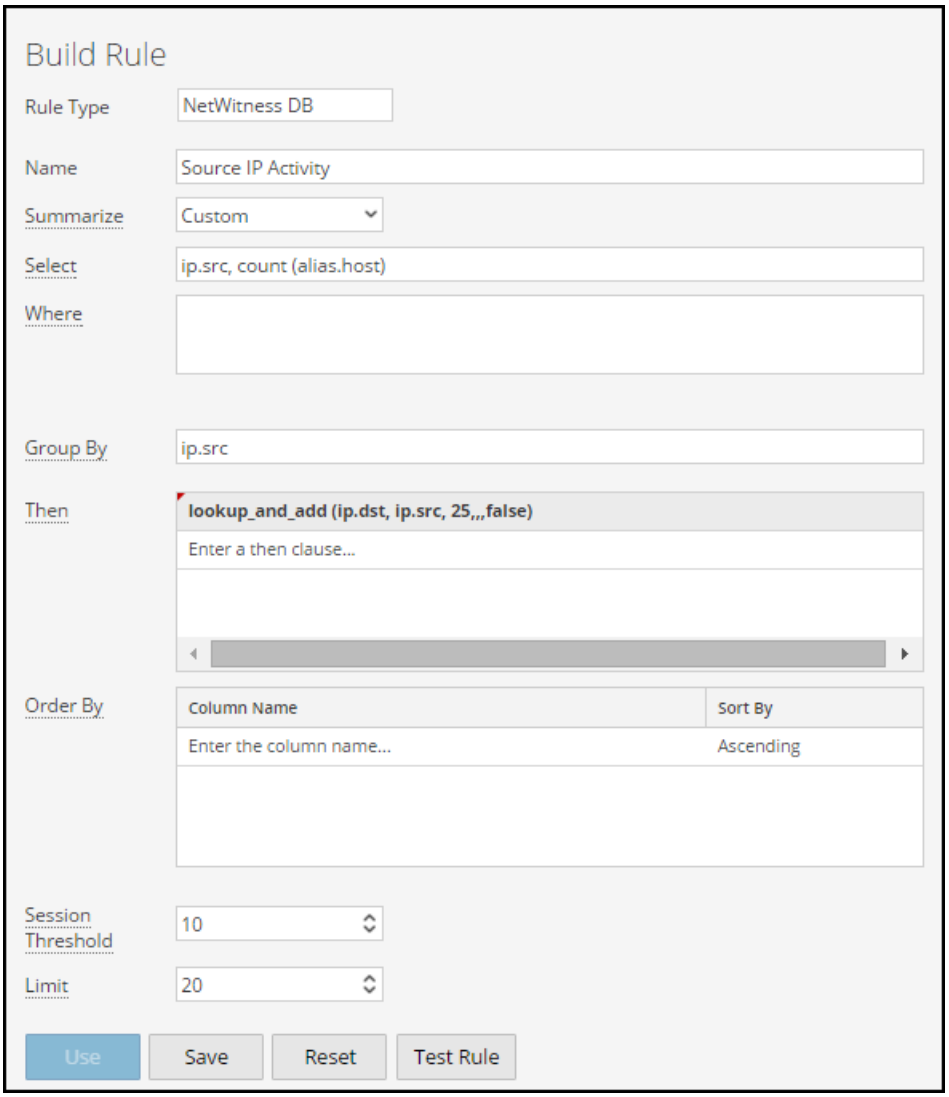
  Beachten Sie die Regel mit der lookup_and_add-Regelaktion:



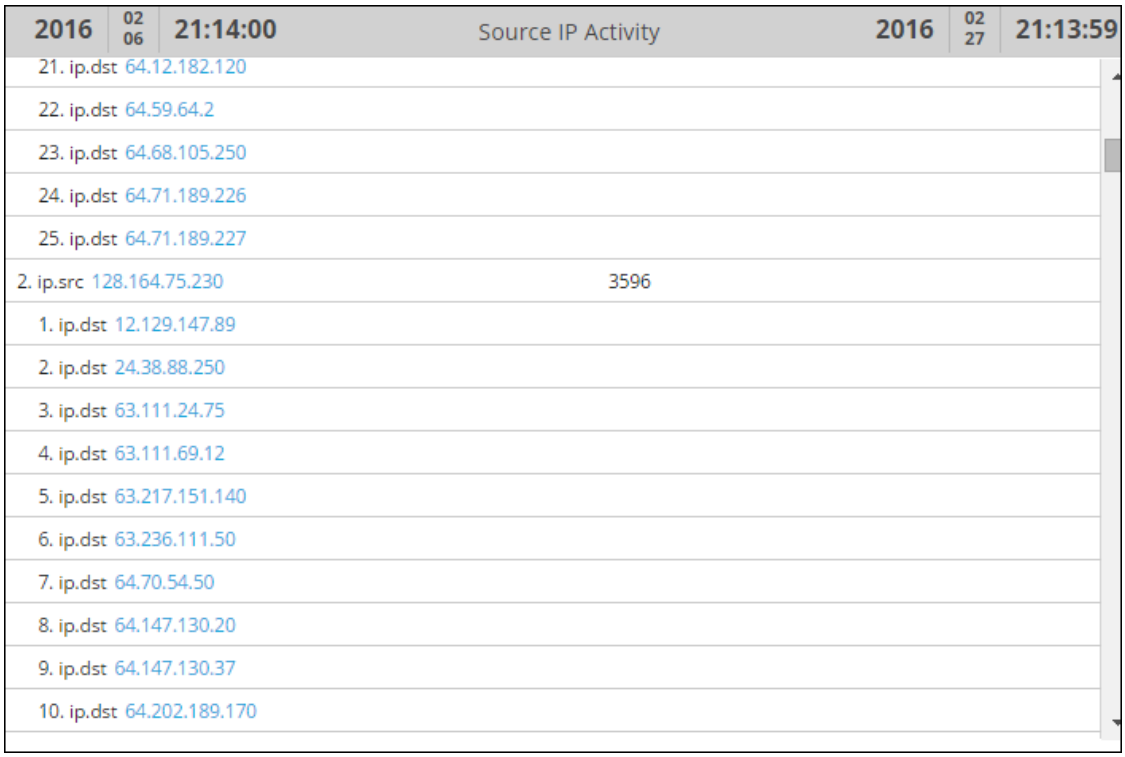

Die Ausgabe wird angezeigt:




- Jede `lookup_and_add`-Regelaktion löst standardmäßig zwei gleichzeitige Suchabfragen in der Datenquelle aus. RSA empfiehlt, dass Sie die Standardeinstellung beibehalten. Wenn Sie jedoch den Wert erhöhen möchten, vergewissern Sie sich, dass der Wert des Parameters `Max # of Concurrent LookupAndAdd Queries` in der Reporting Engine niedriger ist als der Wert `Max Concurrent Queries` in der NWDB-Datenquellenkonfiguration.
  Wenn die NWDB-Datenquelle von anderen Services gemeinsam verwendet wird, sollten Sie für den Parameter `Max # of Concurrent LookupAndAdd Queries` in der Reporting Engine einen niedrigen Wert beibehalten, da eine Erhöhung des Werts die Abfragen von anderen Services beeinflusst. Weitere Informationen finden Sie im Thema „Registerkarte Allgemein für Reporting Engine“ im *Reporting Engine-Konfigurationsleitfaden*.
- Wenn Sie nur an eindeutigen Werten und nicht an genauen Aggregatwerten interessiert sind, stellen Sie den `Session Threshold` für die NWDB-Regel auf einen Wert ungleich null ein. Weitere Informationen hierzu finden Sie im Abschnitt „Erstellen einer Regel mithilfe einer NetWitness-Datenquelle“ in Konfigurieren einer Regel. Je höher der Wert, desto länger dauert die Regelausführung. Wenn der Wert auf null eingestellt ist, dauert die Ausführung länger, ergibt jedoch genaue Aggregatwerte.
  Erwägen Sie eine Regel mit der lookup_and_add-Regelaktion und einem Sitzungsschwellenwert von 10.




Die Ausgabe wird angezeigt:




## Listenwertberichte

Verwenden einer angepassten Liste:

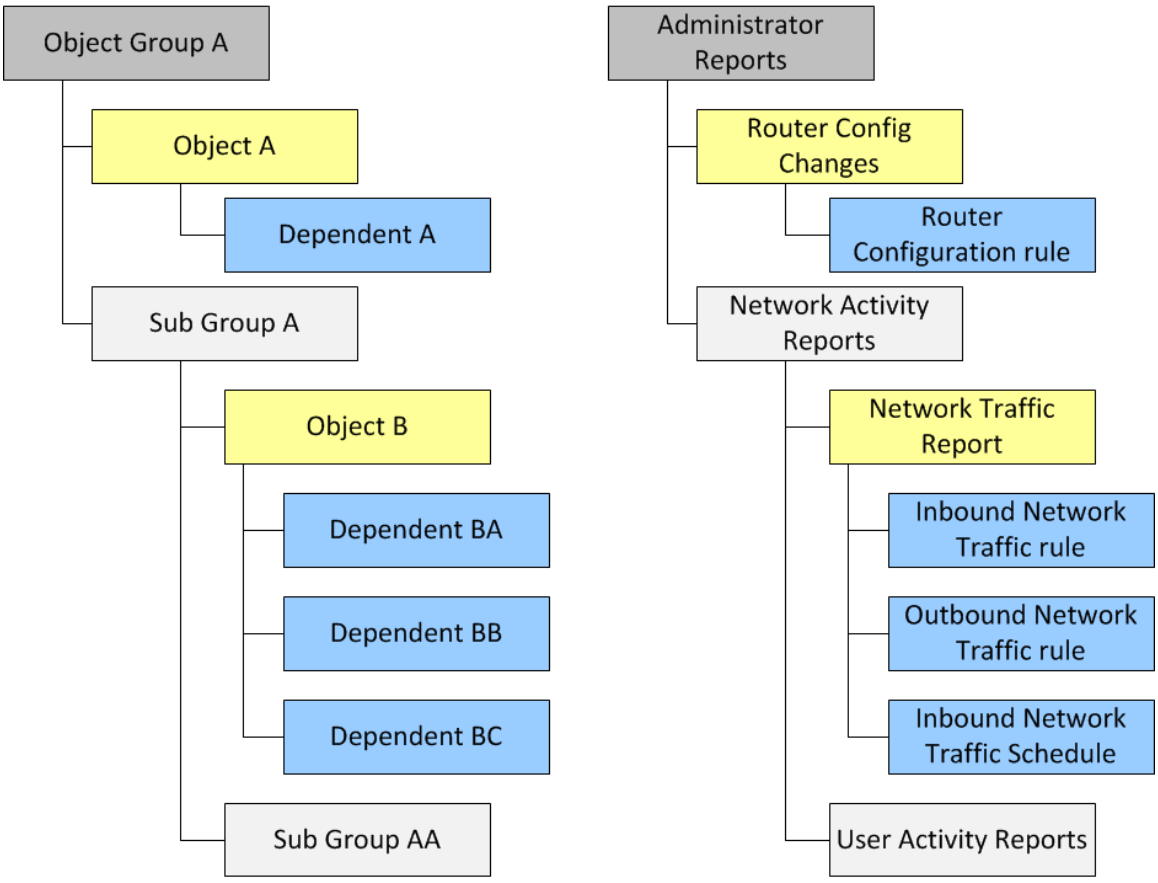
Bei Listenwertberichten (für alle Datenquellentypen) werden individuelle Berichte für jeden Wert in der Liste erzeugt. Daher gilt: Je höher die Werte in der Liste, desto länger dauert die Ausführung der Berichte. Folglich müssen Sie eine angepasste Liste zum Erzeugen solcher Berichte verwenden.

# Zugriffskontrolle für Reporting

Über das Reporting-Modul können Sie die Zugriffskontrolle für alle Komponenten im Modul einrichten. In NetWitness Suite können Sie verschiedene Rollen definieren und für jede Rolle aus dem Modul für Systemsicherheit die Zugriffskontrolle angeben. Sie können die Zugriffskontrolle so definieren, dass sie im Reporting-Modul jeder Rolle zugewiesen wird. Weitere Informationen erhalten Sie unter „Schritt 1: Überprüfen der vorkonfigurierten NetWitness-Suite-Rollen“ und „Schritt 2: (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen“ im *Handbuch Systemsicherheit und Benutzerverwaltung*.

Im Modul Reports können Sie die Rollenberechtigungen ändern oder auf folgende Reporting-Objekte zugreifen:

Hier sehen Sie ein Beispiel für die Hierarchie der Objektgruppen, Objekte und abhängigen Elemente. Diese Abbildung zeigt die Berichtsgruppen und die Berichtshierarchie.




**Berichtsgruppen und Berichtshierarchie**

## Berechtigung für Objektgruppen

- Zum Festlegen der Berechtigungen für die Objektgruppe, Objekte und abhängigen Elemente benötigen Sie die Lese- und Schreibberechtigung. Abhängige Elemente mit der Berechtigung „Kein Zugriff“ sind ausgegraut und abhängige Elemente mit der Berechtigung „Schreibgeschützt“ sind mit einem Symbol versehen.
- Beim Festlegen der Berechtigung für die Objektgruppe erhalten die Objekte und abhängigen Elemente in der Objektgruppe die Berechtigung nicht automatisch. Wenn die Objekte und abhängigen Elemente in der Objektgruppe die Berechtigung automatisch erhalten sollen, müssen Sie die Option „Diese Berechtigungen auf Untergruppen und <Objekte> in dieser Gruppe“ auswählen. Wenn Sie beispielsweise nicht möchten, dass Operatoren auf Berichte in Berichtsgruppe A zugreifen, müssen Sie die Berechtigung für Gruppe A auf „Kein Zugriff für die Rolle Operator“ festlegen und die Option „Diese Berechtigungen auf Untergruppen und <Objekte> in dieser Gruppe anwenden“ auswählen.

- Wenn Sie die Berichtigungen für die Objektgruppe festlegen und die Option „Diese Berechtigungen auf Untergruppen und Objekte in dieser Gruppe anwenden“ auswählen, erhalten abhängige Elemente wie Regeln oder Pläne der Objekte die Berechtigungen nicht automatisch. Damit die Berechtigungen auf die Regeln angewendet werden, müssen Sie die Option „Nur-Lese-Berechtigungen auf Regeln in <Objekt> anwenden“ auswählen.
- Wenn Sie die Berechtigungen für die Objekte festlegen, müssen Sie darauf achten, dass die Objekte in der Hierarchie stets über eine Berechtigung verfügen, die geringer oder gleich der darüber liegenden Berechtigung in der Hierarchie ist, damit die Berechtigung angewendet wird. Wenn beispielsweise die Berichte in einer Berichtsgruppe über die Lese- und Schreibberechtigung verfügen und Sie auf Ebene der Berichtsgruppe die Berechtigung „Schreibgeschützt“ oder „Kein Zugriff“ zuweisen und zudem die Option „Diese Berechtigungen auf Untergruppen und Berichte in dieser Gruppe anwenden“ auswählen, wird die Berechtigung der Regeln nicht geändert.
- Berechtigungen werden in der Hierarchie von oben nach unten weitergegeben, nicht umgekehrt. Wenn Sie beispielsweise einer Regel eine Berechtigung zuweisen, wird die Berechtigung des Berichts, in dem die Regel enthalten ist, nicht geändert.

## Berechtigung für Objekte oder abhängige Elemente

- Zum Festlegen der Berechtigungen für Objekte und abhängige Elemente benötigen Sie die Lese- und Schreibberechtigung.
- Anstatt jedem Objekt einzeln eine Berechtigung zuzuweisen, können Sie die Berechtigung auch mehreren Objekten gleichzeitig zuweisen.
- Beim Festlegen der Berechtigung für das Objekt erhalten die abhängigen Elemente im Objekt die Berechtigung nicht automatisch. Damit die Berechtigung auf die abhängigen Elemente angewendet wird, müssen Sie die Option „Nur-Lese-Berechtigungen auf Regeln in <Objekt> anwenden“ auswählen.

Wenn Sie die Berechtigung auf abhängige Elemente anwenden, wird die Berechtigung anhand der bestehenden Berechtigung der Rolle angewendet. Beispiel: Ein Analyst und ein Operator haben folgende Berechtigungen für die verschiedenen abhängigen Elemente. Dabei hat das Objekt Bericht A die abhängigen Elemente Regel AA, Regel AB und Regel AC.

| Objekt oder abhängiges Element | Analyst | Operator |
|---|---|---|

| | | |
|---|---|---|
| Bericht A | Lesen & Schreiben | Kein Zugriff |
| Regel AA | Lesen & Schreiben | Kein Zugriff |
| Regel AB | Lesen & Schreiben | Lesen & Schreiben |
| Regel AC | Schreibgeschützt | Kein Zugriff |

Wenn der Analyst eine Lese- und Schreibberechtigung auf die Rolle Operator anwendet und die Option „Nur-Lese-Berechtigungen auf Regeln in <Objekt> anwenden“ auswählt, werden die Berechtigungen für die verschiedenen abhängigen Elemente folgendermaßen festgelegt:

## Ändern der Berechtigungen

- **Gruppenebene:** Legen Sie die Berechtigungen auf Ebene der Objektgruppe und für alle Objekte und Einheiten in der Gruppe fest. Beispiel: Die Gruppe Administratorberichte enthält 80 Berichte und nur der Administrator darf Berichte hinzufügen oder ändern. Legen Sie dafür die Berechtigung für alle anderen Rollen auf Gruppenebene auf „Schreibgeschützt“ fest und wählen Sie die Option aus, mit der die Berichtigung auf alle Berichte und Untergruppen in der Berichtsgruppe angewendet wird.
- **Mehrere Objekte:** Wählen Sie mehrere Objekte aus und geben Sie den Zugriff für alle ausgewählten Objekte an. Beispiel: In der Untergruppe Netzwerkdatenverkehr befinden sich zehn Berichte mit vertraulichen Informationen, auf die niemand Zugriff haben soll. Wählen Sie dafür die zehn Berichte aus und legen Sie die Berechtigung für alle Rollen auf „Kein Zugriff“ fest.
- **Einzelnes Objekt:** Wählen Sie nur das Objekt aus und geben Sie die Berechtigung an. Beispiel: Wählen Sie den Bericht zum Netzwerkdatenverkehr aus und weisen Sie der Rolle „Sicherheitsanalyst“ die Lese- und Schreibberechtigung zu. Alternativ können Sie auch die Warnmeldung „Anmeldefehler“ auswählen und der Rolle „Sicherheitsanalyst“ die Lese- und Schreibberechtigung zuweisen.

| Objekt oder abhängiges Element | Operator (vor Anwenden der Berechtigung) | Operator (nach Anwenden der Berechtigung) |
|---|---|---|
| Bericht A | Kein Zugriff | Lesen & Schreiben |

| | | |
|---|---|---|
| Regel AA | Kein Zugriff | Schreibgeschützt |
| Regel AB | Lesen & Schreiben | Lesen & Schreiben |
| Regel AC | Kein Zugriff | Schreibgeschützt |

## Rollen und Berechtigungen für Reporting-Modul

Obwohl NetWitness Suite über fünf vorkonfigurierte Rollen verfügt, können Sie benutzerdefinierte Rollen hinzufügen. Beispielsweise können Sie zusätzlich zur vorkonfigurierten Rolle „Analyst“ benutzerdefinierte Rollen für „AnalystsEuropa“ und „AnalystsAsien“ hinzufügen.

| Rolle | Berechtigung |
|---|---|
| Administratoren | Voller Systemzugriff |
| Operatoren | Zugriff auf Konfigurationen, aber nicht auf Daten |
| Analysten | Zugriff auf Daten, aber nicht auf Konfigurationen |
| SOC_Managers | Gleicher Zugriff wie Analysten und eine zusätzliche Berechtigung für das Verarbeiten von Incidents |
| Malware_ Analysts | Zugriff nur auf Schadsoftware-Ereignisse |

Abhängig von der Benutzerrolle können Sie die folgenden Zugriffsberechtigungen für den Zugriff auf die Komponenten des Moduls Reporting definieren (Regeln, Berichte, Diagramme, Warnmeldungen, Listen):

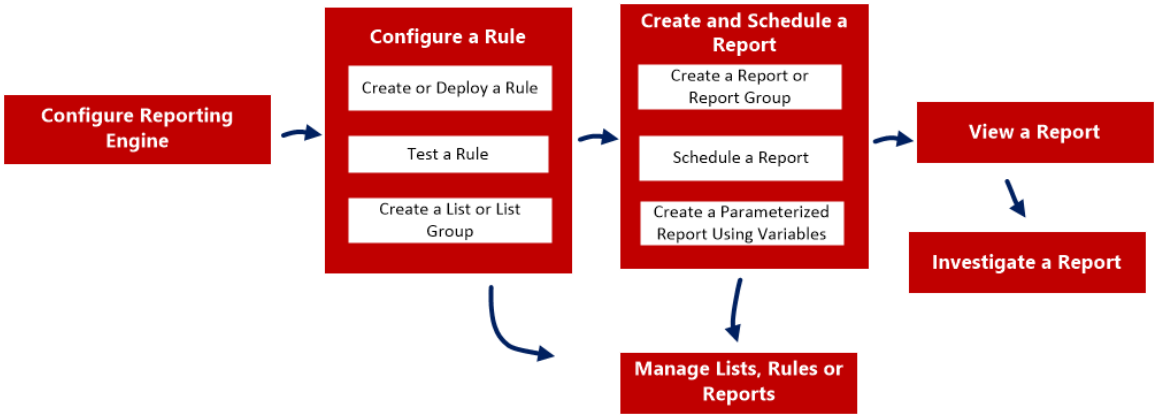
- Erstellen
- Löschen
- Exportieren
- Managen
- Anzeigen

**Hinweis:** Sie müssen alle Berechtigungen für eine Benutzerrolle aktivieren, um jedes der Reporting-Module definieren, löschen, managen und anzeigen zu können. Sie müssen die nötigen Berechtigungen haben, damit die Datenquelle aufgelistet wird, während Sie die Berichte, Diagramme oder Warnmeldungen definieren. Weitere Informationen finden Sie unter „Konfigurieren von Datenquellenberechtigungen“ im *Konfigurationsleitfaden Reporting Engine*.

Eine detaillierte Liste von Berechtigungen und Informationen zum Hinzufügen einer Rolle und Zuweisen von Berechtigungen finden Sie unter „Rollenberechtigungen“ und „Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen“ im *Handbuch Systemsicherheit und Benutzerverwaltung*.

# Konfigurieren und Erzeugen eines Berichts

Diese Abbildung stellt eine Übersicht über den gesamten Prozess zum Konfigurieren und Erzeugen eines Berichts dar.




Führen Sie zum Konfigurieren und Erzeugen eines Berichts die folgenden Aufgaben durch:

1. Konfigurieren des Reporting Engine: Sie müssen die Reporting Engine konfigurieren, bevor Sie einen Bericht konfigurieren und erzeugen können. Außerdem müssen Sie die Datenquelle in der Reporting Engine festlegen, aus der die Daten extrahiert werden. Weitere Informationen zum Konfigurieren der Reporting Engine finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting*.
2. Konfigurieren einer Regel
3. Erstellen und Planen eines Berichts
4. Anzeigen eines Berichts
5. Untersuchen eines Berichts
6. Managen von Listen, Regeln oder Berichten

# Konfigurieren einer Regel

Sie können eine neue Regel erstellen oder eine vorhandene Regel aus Live-Services bereitstellen, die in einem Bericht verwendet werden kann. Sie können unterschiedliche Bedingungen verwenden, um die Daten oder Informationen in den Datenquellen zu verfeinern:

- select-Klausel
- where-Klausel
- Gruppieren nach
- Sortieren nach usw.

Sie können beispielsweise eine Regel schreiben, um die 20 Top-Webadressen anzuzeigen, die die Benutzer täglich aufrufen.

Sie können mithilfe verschiedener Datenquellen unterschiedliche Arten von Regeln erstellen. In folgenden Themen erhalten Sie weitere Informationen zum Erstellen einer Regel für die verschiedenen Datenquellen:

- Erstellen einer Regel mithilfe einer NetWitness-Datenquelle
- Erstellen einer Regel mit einer Warehouse-Datenquelle
- Erstellen einer Regel mit einer Respond-Datenquelle

Sie können in einer Regel auch eine Liste verwenden, um ein Suchergebnis aus der Datenquelle zu verfeinern. Nach dem Erstellen einer Regel können Sie diese Regel testen, um die von der Regel zurückgegebenen Ergebnisse zu betrachten.

## Erstellen einer Regelgruppe

**Führen Sie zum Erstellen einer Regelgruppe oder -untergruppe die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Führen Sie einen der folgenden Schritte aus.
   - So definieren Sie eine Regelgruppe:
     a. Klicken Sie im Bereich „Regelgruppen“ auf + .
        Die neue Regelgruppe wird zum Bereich „Regelgruppen“ hinzugefügt.

b. Geben Sie den Namen für die Regelgruppe ein und drücken Sie die EINGABETASTE.

- So fügen Sie eine Regeluntergruppe hinzu:

a. Wählen Sie im Bereich „Regelgruppen“ die Regelgruppe aus, der Sie eine Untergruppe hinzufügen möchten.

b. Klicken Sie auf +.

Die neue Regeluntergruppe wird zur Regelgruppe hinzugefügt.

c. Geben Sie den Namen für die Regeluntergruppe ein und drücken Sie die EINGABETASTE.

## Erstellen einer Regel mithilfe einer NetWitness-Datenquelle

Sie können eine Regel erstellen, um Daten oder Ereignisse von einer NetWitness-Datenquelle abzurufen. Mit demselben Verfahren können Sie eine Regel definieren, mit der Daten oder Ereignisse von einer Archiver-Datenquelle abgerufen werden.

Die Archiver-Datenquelle kann in der Ansicht „Service-Konfiguration“ der Reporting Engine hinzugefügt werden. Weitere Informationen erhalten Sie unter „(Optional) Hinzufügen von Archiver als Datenquelle zur Reporting Engine“ im *Archiver-Konfigurationsleitfaden*.

### Voraussetzungen

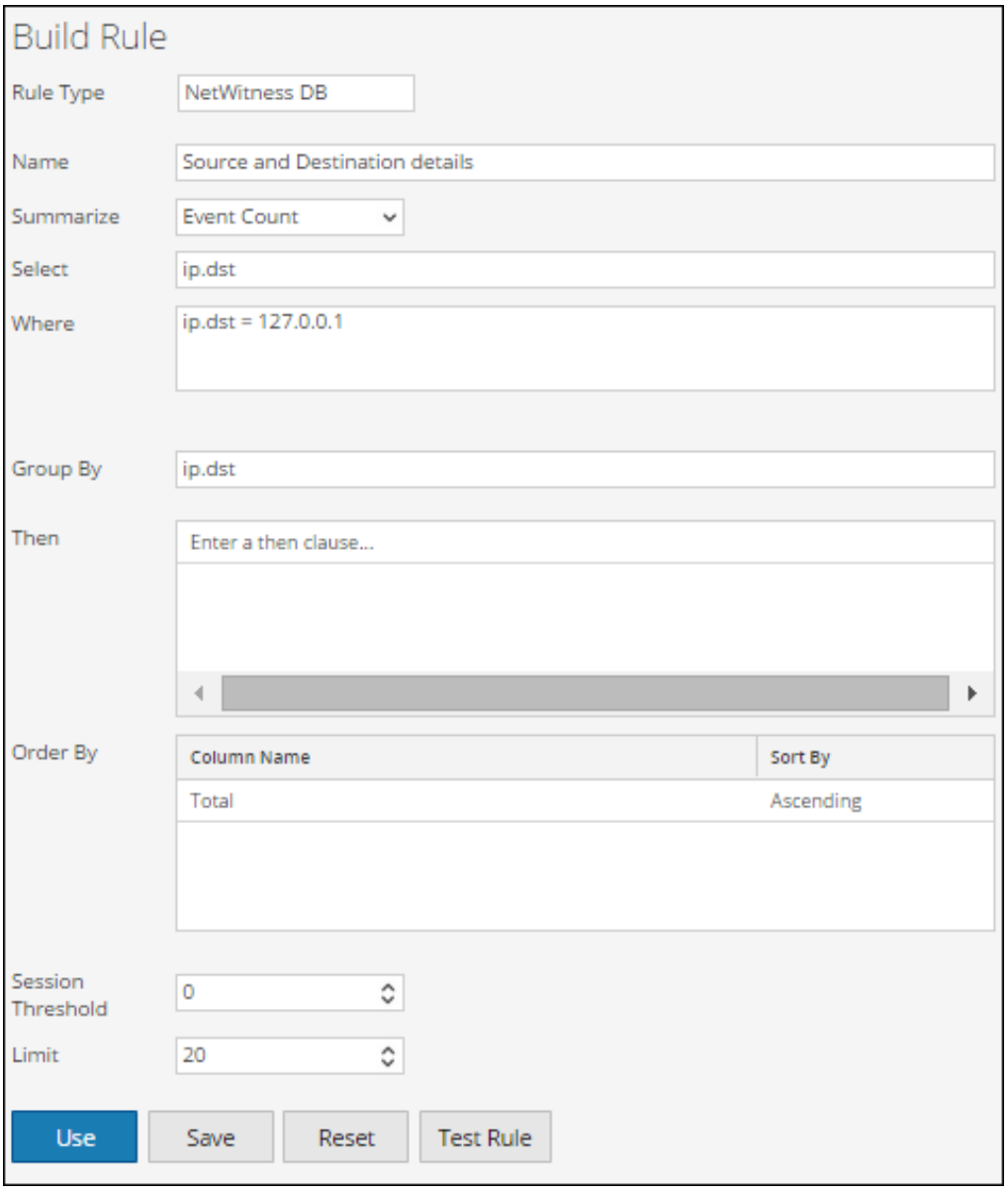
Stellen Sie sicher, dass Sie verstehen, wie benutzerdefinierte Metaschlüssel mithilfe des benutzerdefinierten Feeds erstellt werden. Weitere Informationen finden Sie unter „Erstellen benutzerdefinierter Metaschlüssel mithilfe benutzerdefinierter Feeds“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

**Um eine Regel zu erstellen, mit der Daten oder Ereignisse von einer NetWitness-Datenquelle abgerufen werden, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.

   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie in der Symbolleiste „Regeln“ auf + >**NetWitnessDB**.
   Die Registerkarte der Ansicht Regel erstellen wird angezeigt.




3. Im Feld **Regeltyp** ist standardmäßig **NetWitness-DB** ausgewählt.
4. Geben Sie in das Feld **Name** einen Namen ein, der zur Identifizierung oder Kennzeichnung der Regel in Warnmeldungen und Berichten dient.
5. Das Feld **Zusammenfassen** bestimmt den Typ der Zusammenfassung oder Aggregation für die Regel. Basierend auf dem Typ der zu definierenden Regel müssen Sie eines der Folgenden auswählen:
   - Zum Definieren einer **Nicht-Aggregatregel** ohne Gruppierung wählen Sie: **Keine**
   - Zum Definieren einer **Aggregatregel** mit spezieller Aggregation wie bei Aggregatfunktionen zu Sammlungen (Sitzungen/Ereignisse/Pakete) wählen Sie eine der

folgenden Optionen aus:

- Ereignisanzahl
- Paketanzahl
- Sitzungsgröße

- Zum Definieren einer **Aggregatregel** mit Metawerten und benutzerdefinierten Aggregatfunktionen wie sum(), count() usw. wählen Sie: **Custom**

  Durch Auswahl von Benutzerdefiniert im Feld **Zusammenfassen** können Sie in der Klausel *Auswählen* die Aggregatfunktion Ihrer Wahl im definieren. Beispiel: Wählen Sie „ip.src“, „countdistinct(ip.dst)“ und „distinct(ip.dst)“ aus. Die unterstützten Aggregatfunktionen sind:

  - sum (<meta>)
  - count(<meta>)
  - countdistinct(<meta>)
  - min(<meta>)
  - max(<meta>)
  - avg(<meta>)
  - first(<meta>)
  - last(<meta>)
  - len(<meta>)
  - distinct(<meta>)

  Detaillierte Informationen zu Aggregatregeln und Nichtaggregatregeln finden Sie im Abschnitt „NWDB-Regelsyntax in Regelsyntax .

6. Geben Sie in das Feld **Auswählen** Metadaten ein oder wählen Sie Metadaten aus der Liste verfügbarer Metadatentypen aus, die in der Metabibliothek bereitgestellt werden. Weitere Informationen finden Sie unter Bereich „Meta“ in Ansicht „Regel erstellen“. Der Metaname zum Abrufen des Rohdatenprotokolls lautet „raw“. „raw“ kann nur im Feld **Auswählen** verwendet werden. Es kann nicht in den Feldern **Wo** und **Dann** verwendet werden. Für benutzerdefinierte Aggregatregeln werden im Feld **Auswählen** mehrere Aggregatfunktionen unterstützt.

   **Hinweis:** In früheren Versionen von NetWitness Suite wurde für benutzerdefinierte Aggregatregeln in der **SELECT-Klausel** nur eine Aggregatfunktion unterstützt. Ab jetzt werden in der Klausel **Auswählen** mehrere Aggregatfunktionen unterstützt. Beispiel: Wählen Sie *ip.src, username, service, distinct(country.src), sum(payload)* aus.

7. Geben Sie im Feld **Alias** den Aliasnamen für die Spalten ein, die in der SELECT-Klausel verwendet werden.
8. Geben Sie im Feld **Wo** einen Metadatentyp ein oder wählen Sie einen aus der Liste der verfügbaren Metadatentyp aus. Erstellen Sie mithilfe der Operatoren die Where-Klausel für die zugrunde liegenden Abfragekriterien.
9. Das Feld **Gruppieren nach** ist ein schreibgeschütztes Feld, dass mit Metadaten gefüllt wird, die in der Klausel Auswählen definiert sind. Für eine Nicht-Aggregatfunktion ist dieses Feld nicht sichtbar. Im Feld **Gruppieren nach** werden maximal sechs Metadaten unterstützt.

   **Hinweis:** In früheren Versionen von NetWitness Suite wurde für benutzerdefinierte Aggregatregeln in der Klausel **Gruppieren nach** nur ein Metadatentyp unterstützt. Ab jetzt werden in der Klausel **Gruppieren nach** maximal sechs Metawerte unterstützt.
10. Geben Sie im Feld **Dann** die Regelaktionen ein, mit denen der ursprüngliche Ergebnissatz einer Regel bearbeitet wird, um die Ausgabe in einem Bericht zu konkretisieren oder um zusätzlich zum Abfragen und Anzeigen von Daten weitere Funktionen hinzuzufügen, wie etwa einen Feed aus den Ergebnissen erstellen. Eine vollständige Liste der verfügbaren Regelaktionen finden Sie unter „NWDB-Regelsyntax“ in Regelsyntax .

    **Hinweis:** Bei der Ausführung einer Regel für eine Archiver-Datenquelle wird empfohlen, keine abfragenintensiven Regelaktionen, wie lookup_and_add() und show_whats_new(), zu verwenden.
11. Führen Sie im Feld **Sortieren nach** folgende Schritte aus:
    a. Geben Sie in die Spalte **Spaltenname** den Namen der Spalten ein, nach denen Sie die Ergebnisse sortieren möchten. Standardmäßig ist der Wert leer. Der Wert wird basierend auf dem im Feld **Zusammenfassen** ausgewählten Wert ausgefüllt.
       - Wenn für Zusammenfassen der Wert Keine ausgewählt ist, wird bei Auswahl von **Sortieren nach** standardmäßig nach Sitzungs- oder Sammlungszeit sortiert.
       - Bei anderen Werten für „Zusammenfassen“ basiert die Standardsortierung auf den ersten für „Gruppieren nach“ ausgewählten Metadaten, wenn kein Wert für „Sortieren nach“ definiert ist. Die zulässigen Werte für „Ereignisanzahl“, „Paketanzahl“ und „Sitzungsgröße“ sind „Gesamt“ und „Wert“.

    b. Wählen Sie in der Spalte **Sortieren nach** eine der folgenden Möglichkeiten aus, um die Ergebnisse zu sortieren:
       - Aufsteigende Reihenfolge
       - Absteigende Reihenfolge
12. Geben Sie im Feld **Sitzungsschwellenwert** die Optimierungseinstellung ein, um das

Scannen der entsprechenden Sitzungen auf jeden möglichen eindeutigen Wert für die ausgewählten Metadaten zu stoppen. Der Schwellenwert ist eine Ganzzahl zwischen 0 (Standard) und 2147483647.

**Hinweis:** Dies gilt nur für NWDB-Aggregatregeln. Wenn der Standardwert angegeben wurde, werden alle entsprechenden Sitzungen gescannt und der korrekte Wert wird zurückgegeben. Ein höherer Sitzungsschwellenwert ermöglicht genauere Zählerangaben für einen Wert. Dies führt jedoch zu längeren Ausführungszeiten für die Regel. Beispiel: Sie möchten für ip.src den Sitzungsschwellenwert „1000“ festlegen. Wenn bei 5.000 relevanten Sitzungen ein bestimmter ip.src-Wert in mehr als 1.000 Sitzungen auftritt, wird das Scannen durch NWDB nach 1.000 Sitzungen beendet und der extrapolierte Aggregatwert zurückgegeben. Auf diese Weise wird die Abfrageausführungszeit optimiert. Wenn der Wert in weniger als 1000 Sitzungen auftritt, wird der tatsächliche Wert zurückgegeben.

13. Geben Sie im Feld **Limit** eine auf die Abfrage anzuwendende Einschränkung ein, wenn Daten aus einer Datenbank abgerufen werden. Wenn ein Ergebnissatz nach Ereignisanzahl, Paketanzahl oder Sitzungsgröße sortiert wird, repräsentiert der Grenzwert die obersten (oder untersten) wiederzugebenden n Werte. Wenn die Ergebnismenge nicht sortiert wird, werden die ersten n Werte wiedergegeben.
14. Klicken Sie auf **Speichern**.

**Hinweis:** Anders als analysierte Metadaten werden Rohdatenprotokolle von Decodern abgerufen. Wenn sowohl Rohdatenprotokolle als auch analysierte Metadaten in einer einzigen Regel abgefragt werden, können aufgrund unterschiedlicher Aufbewahrungsfristen in derselben Sitzung analysierte Metadaten verfügbar sein und Rohdatenprotokolle fehlen. Dadurch enthält das Ergebnis analysierte Metawerte und leere Rohwerte für diese Sitzungen. Beispielsweise könnten bei der Regel „Select **ip.src**, **ip.dst**, **service**, **username**, **raw**“ die analysierten Metadaten bereitgestellt werden und die **unverarbeiteten** Metadaten für einige Sitzungen leer bleiben.

## Erstellen einer Regel mit einer Warehouse-Datenquelle

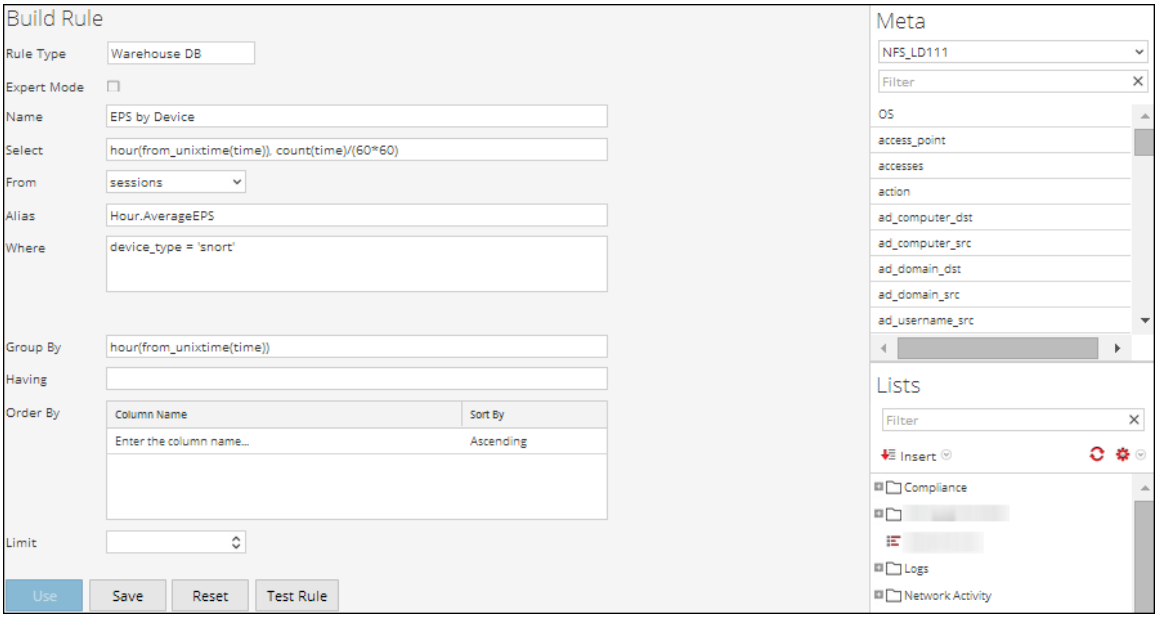
Sie können eine Regel erstellen, um Daten oder Ereignisse von einer Warehouse-Ereignisquelle abzurufen. Sie können Regeln in zwei Modi definieren:

- Standardmodus
- Expertenmodus

### Standardmodus

Im Standardmodus können Sie Regeln erstellen, die einfaches SQL enthalten, z. B. HIVE-Abfragen mit Klauseln wie Select, Where, Group By und Having. Standardmäßig können Sie Regeln erstellen, um Sitzungen oder unverarbeitete Protokolle abzufragen. Weitere Informationen zur Syntax einfacher Abfragen sowie Beispiele finden Sie unter Warehouse-DB – Einfache Regelsyntax.

In der folgenden Abbildung sehen Sie ein Beispiel der Ansicht **Regel erstellen,** die angezeigt wird, wenn Sie **Warehouse-DB** für **Regeltyp** wählen, ohne dass der Expertenmodus ausgewählt ist.

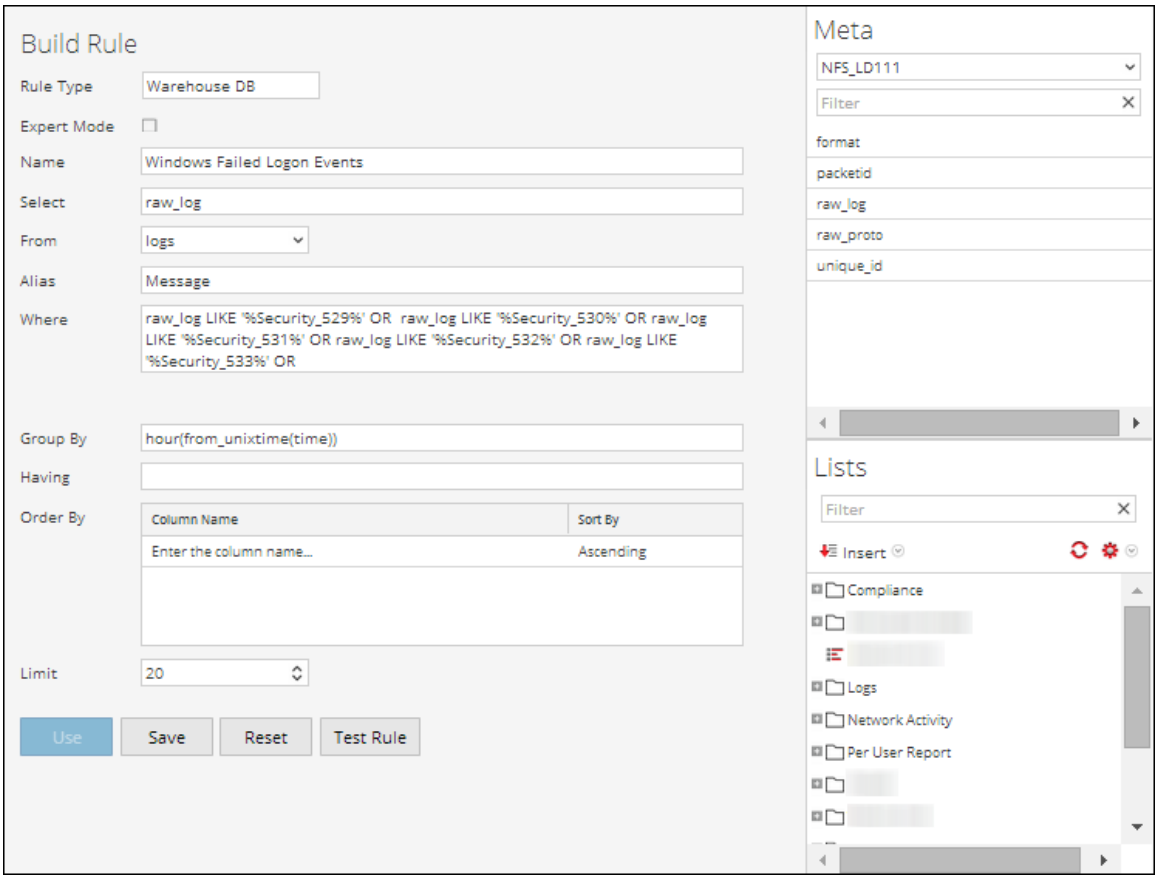



## Abfragen unverarbeiteter Protokolle

Das unverarbeitete Protokollformat wird in der Select- oder Where-Klausel verwendet, um unverarbeitete Protokolle abzufragen.

**Hinweis:** Der Zeitbereich, den Sie in Ihrer Abfrage angeben können, ist ein Tag (24 Stunden). Wenn Sie in Ihrer Abfrage einen Zeitbereich unter einem Tag angegeben haben, enthält der Ergebnissatz Daten von mindestens einem Tag (24 Stunden).

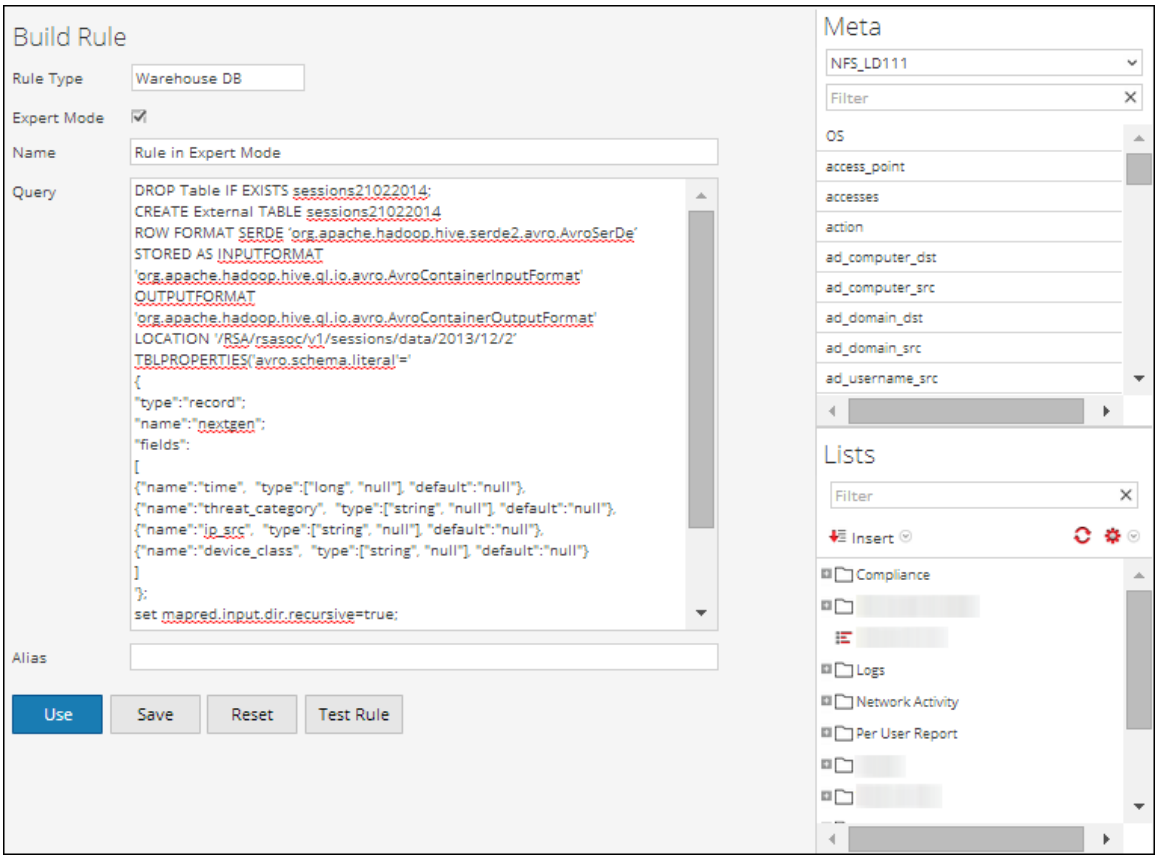
In der folgenden Abbildung sehen Sie ein Beispiel der Ansicht **Regel erstellen**, die angezeigt wird, wenn Sie **Warehouse-DB** für **Regeltyp** wählen und eine Regel zur Abfrage unverarbeiteter Protokolle erstellen.




## Expertenmodus

Erweiterte Regeln werden mithilfe von komplexen HIVE-Abfragen definiert, die durch die Klauseln DROP, CREATE usw. erstellt werden. Im Gegensatz zu einfachen Regeln setzen wir die Ergebnisse immer in eine Tabelle ein. Weitere Informationen zur erweiterten HIVE-Abfragesprache finden Sie im *HIVE-Sprachhandbuch*.

In der folgenden Abbildung sehen Sie ein Beispiel der Ansicht **Regel erstellen,** die angezeigt wird, wenn Sie **Warehouse-DB** für **Regeltyp** wählen, während der Expertenmodus ausgewählt ist.




Wenn Sie einen Bericht für einen bestimmten Zeitraum erzeugen möchten, müssen Sie den Zeitraum in der Abfrage mithilfe der folgenden zwei Variablen manuell definieren:

- ${report_starttime} - Der Startzeitpunkt des Zeitraums in Sekunden.
- ${report_endtime} - Der Endzeitpunkt des Zeitraums in Sekunden.

Beispiel: **SELECT col1, col2 FROM custom_table WHERE timecol >= ${report_starttime} AND timecol <= ${report_endtime};**

**Hinweis:** Standardmäßig behandelt Reporting Engine `${keyword}` als eine Variable. Wenn Sie HIVE-Variablen angeben möchten, müssen Sie die vollständige Syntax einer Variable angeben. Beispiel: `${hiveconf:hive.exec.scratchdir}`.

## Voraussetzungen

Stellen Sie sicher, dass Sie verstehen, wie benutzerdefinierte Metaschlüssel mithilfe des benutzerdefinierten Feeds erstellt werden. Weitere Informationen finden Sie unter „Erstellen benutzerdefinierter Metaschlüssel mithilfe benutzerdefinierter Feeds“ im *Leitfaden zur Host- und Servicekonfiguration*.

**Um eine Regel zu erstellen, mit der Daten oder Ereignisse von einer Warehouse-Datenquelle abgerufen werden, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.

   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie in der Symbolleiste „Regel“ auf + > **Warehouse-DB**.

   Die Ansicht „Regel erstellen“ wird angezeigt.

3. Im Feld **Regeltyp** ist **Warehouse-DB** standardmäßig ausgewählt.

   Wenn Sie die Regel im Standardmodus definieren, gehen Sie wie folgt vor:

   a. Geben Sie in das Feld **Name** einen Namen ein, der zur Identifizierung oder Kennzeichnung der Regel in Warnmeldungen und Berichten dient.

   b. Geben Sie in das Feld **Auswählen** einen Metadatentyp ein oder wählen Sie den Metadatentyp aus der Drop-down-Liste aus oder wählen Sie einen Metadatentyp aus der Liste verfügbarer Metadatentypen im Bereich „Meta“ aus. Weitere Informationen finden Sie unter Bereich „Meta“ in der Ansicht „Regel erstellen“.

   c. Wählen Sie im Drop-down-Menü **Von** eine der folgenden Optionen aus:

      - Sitzung
      - Protokolle

   d. Geben Sie im Feld **Alias** den Aliasnamen für die Spalten ein, die in der SELECT-Klausel verwendet werden.

   e. Geben Sie in das Feld **Where** Metadaten ein oder wählen Sie Metadaten aus der Liste verfügbarer Metadatentypen aus, die im Metadatenbereich bereitgestellt werden. Die Where-Klausel enthält die zugrunde liegenden Abfragekriterien für die Regel.

   f. Geben Sie in das Feld **Gruppieren nach** die in der Select-Klausel ausgewählten Metadaten ein, so dass die Ergebnismenge auf Basis der Metadaten gruppiert wird.

   g. Geben Sie im Feld **Enthält** die Kriterien zum Filtern des Ergebnissatzes für aggregierte Abfragen ein.

   h. Führen Sie im Feld **Sortieren nach** folgende Schritte aus:

      1. Geben Sie in die Spalte **Spaltenname** den Namen der Spalten ein, nach denen Sie die Ergebnisse gruppieren möchten.
      2. Wählen Sie in der Spalte **Sortieren nach** eine der folgenden Möglichkeiten aus, um die Ergebnisse zu sortieren:

- Aufsteigende Reihenfolge
- Absteigende Reihenfolge

i. Geben Sie im Feld **Limit** eine auf die Abfrage anzuwendende Einschränkung ein, wenn Daten aus einer Datenbank abgerufen werden. Wenn eine Ergebnismenge nach Sitzungsanzahl, Paketanzahl oder Sitzungsgröße sortiert wird, repräsentiert der Grenzwert die n obersten (oder untersten) wiederzugebenden Werte. Wenn die Ergebnismenge nicht sortiert wird, werden die ersten n Werte wiedergegeben.

j. Klicken Sie auf **Speichern**.

4. Wenn Sie die Regel im Expertenmodus definieren, aktivieren Sie das Kontrollkästchen **Expertenmodus** und gehen Sie wie folgt vor:

   a. Geben Sie in das Feld **Name** einen Namen ein, der zur Identifizierung oder Kennzeichnung der Regel in Warnmeldungen und Berichten dient.

   b. Geben Sie im Feld **Abfrage** die Hive-Abfrageanweisung zum Abfragen der Datenquelle ein.

   c. Geben Sie im Feld **Alias** den Aliasnamen für die Spalten ein, die in der SELECT-Klausel verwendet werden.

   d. Klicken Sie auf **Speichern**.

## Erstellen einer Regel mit einer Respond-Datenquelle

Sie können eine Regel zum Abrufen von Incidents oder Warnmeldungen von einer Respond-Datenquelle erstellen.

### Voraussetzungen

Stellen Sie sicher, dass Sie:

- Stellen Sie sicher, dass der Reporting Engine-Service ausgeführt wird.
- Der Incident-Management-Service ausgeführt wird. Weitere Informationen finden Sie unter „Konfigurieren einer Datenbank für den Respond Server-Service“ im *Konfigurationsleitfaden für NetWitness Respond*.
- (Optional) Stellen Sie sicher, dass der Event Stream Analysis-Service ausgeführt wird. Weitere Informationen finden Sie unter „Schritt 2. Konfigurieren erweiterter Einstellungen für einen ESA-Service“ im *ESA-Konfigurationsleitfaden*.

- (Optional) Stellen Sie sicher, dass der Malware Analysis-Service ausgeführt wird. Weitere Informationen finden Sie unter „(Optional) Konfigurieren des Auditing auf dem Malware Analysis-Host“ im *Malware-Konfigurationsleitfaden*.

**Hinweis:** Basierend auf den Anforderungen und dem Typ der Warnmeldungen oder Incidents, die Sie erzeugen möchten, müssen Sie einen der Services (Event Stream Analysis, Reporting Engine, Malware Analysis oder Endpoint) konfigurieren.

**Um eine Regel zu erstellen, mit der Daten oder Ereignisse von einer Respond-Datenquelle abgerufen werden, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.

   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie in der Symbolleiste „Regeln“ auf + > **Reagieren**.

   Die Registerkarte der Ansicht Regel erstellen wird angezeigt.

3. Im Feld **Regeltyp** ist standardmäßig „Respond“ ausgewählt.

4. Geben Sie im Feld **Name** einen Namen ein, der zur Identifizierung oder Kennzeichnung der Regel in Warnmeldungen und Incident-Berichten dient.

5. Das Feld **Zusammenfassen** bestimmt den Typ der Zusammenfassung oder Aggregation für die Regel. Basierend auf dem Typ der zu definierenden Regel müssen Sie eines der Folgenden auswählen:

   - Zum Definieren einer **Nichtaggregatregl** ohne Gruppierung wählen Sie **Ohne** aus.
   - Zum Definieren einer **Aggregatregel** mit Metawerten und benutzerdefinierten Aggregatfunktionen wählen Sie **Benutzerdefiniert** aus.

     Durch Auswahl von „Benutzerdefiniert“ im Feld **Zusammenfassen** können Sie in der *SELECT*-Klausel basierend auf dem ausgewählten Berichttyp die Aggregatfunktion Ihrer Wahl definieren.

     Detaillierte Informationen zu Aggregat- und Nichtaggregatregeln finden Sie unter Regelsyntax .

6. Im Feld **Von** wählen Sie basierend auf dem anzuzeigenden Berichtsergebnis eine der folgenden Optionen aus:

   - Warnmeldung
   - Incident

7. Geben Sie in das Feld **Auswählen** Metadaten ein oder wählen Sie Metadaten aus der Liste verfügbarer Metadatentypen aus, die in der Metabibliothek bereitgestellt werden. Weitere

Informationen finden Sie unter „Metabereich“ in der Ansicht „Regel erstellen“. Er kann im Feld **Wo** nicht verwendet werden. Für benutzerdefinierte Aggregatregeln werden im Feld **Auswählen** mehrere Aggregatfunktionen unterstützt.

Unter anderem folgende Aggregatfunktionen werden für Warnmeldungen unterstützt:

- alert_host_summary
- alert.name
- alert.numEvents
- alert.severity
- alert.source
- alert.timestamp
- incidentCreated
- incidentId
- receivedTime

Unter anderem folgende Aggregatfunktionen werden für Incidents unterstützt:

- categories
- created
- priority
- riskScore
- sealed
- status

Detaillierte Informationen zu Aggregat- und Nichtaggregatregeln finden Sie unter Regelsyntax .

8. Geben Sie im Feld **Alias** den Aliasnamen für die Spalten ein, die in der SELECT-Klausel verwendet werden.
9. Geben Sie im Feld **Wo** einen Metadatentyp ein oder wählen Sie einen aus der Liste der verfügbaren Metadatentyp aus. Erstellen Sie mithilfe der Operatoren die Where-Klausel für die zugrunde liegenden Abfragekriterien.
10. Das Feld **Gruppieren nach** ist ein schreibgeschütztes Feld, das mit Metadaten gefüllt wird, die in der SELECT-Klausel definiert sind. Bei einer Nicht-Aggregatfunktion ist dieses Feld nicht sichtbar. Es werden maximal sechs Metawerte im Feld **Gruppieren nach** unterstützt.
11. Führen Sie im Feld **Sortieren nach** folgende Schritte aus:

a. Geben Sie in die Spalte **Spaltenname** den Namen der Spalten ein, nach denen Sie die Ergebnisse sortieren möchten. Standardmäßig ist der Wert leer.

b. Wählen Sie in der Spalte **Sortieren nach** eine der folgenden Möglichkeiten aus, um die Ergebnisse zu sortieren:

- Aufsteigende Reihenfolge
- Absteigende Reihenfolge

12. Geben Sie im Feld **Grenzwert** den Grenzwert ein, der für die Abfrage gelten soll, wenn Daten aus der Datenbank abgerufen werden. Wenn eine Ergebnismenge sortiert wird, repräsentiert der Grenzwert die n obersten (oder untersten) wiederzugebenden Werte. Wenn die Ergebnismenge nicht sortiert wird, werden die ersten n Werte wiedergegeben.
13. Klicken Sie auf **Speichern**.

## Bereitstellen einer Regel

In RSA NetWitness Suite können Sie die ausgewählten Regeln auf dem Service (z. B. Reporting Engine) mithilfe des Bereitstellungsassistenten bereitstellen.

### Voraussetzungen

Achten Sie auf Folgendes:

- Die Services, auf denen Sie eine Regel bereitstellen können, werden ausgeführt.
- Der Live-Services ist konfiguriert.

**Führen Sie zum Bereitstellen einer Regel die folgenden Schritte aus:**

1. Wählen Sie **KONFIGURIEREN > LIVE-INHALT** aus.
2. Suchen Sie im Bereich **Suchkriterien** nach Live-Ressourcen (z. B. nach dem Ressourcentyp **Anwendungsregel**).
3. Wählen Sie im Bereich **Übereinstimmende Ressourcen** die Optionen **Ergebnisse anzeigen > Raster** aus.
4. Aktivieren Sie das Kontrollkästchen links neben den Regeln, die Sie bereitstellen möchten.
5. Klicken Sie in der Symbolleiste **Übereinstimmende Ressourcen** auf 

.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie den Service aus, auf dem eine Regel (z. B. Reporting Engine) bereitgestellt werden soll, und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Bereitstellen**.
   Die Regel wurde erfolgreich bereitgestellt.

## Verwenden von Meta-Aliasen für Reporting

Wenn Sie in Berichten und Diagrammen Bezug auf Metadaten nehmen, werden nur Aliase für die Metanamen angezeigt. Diese Aliase sorgen dafür, dass die Metadaten für eine größere Zielgruppe verständlich sind.

Sie können nur vordefinierte Aliase für die Metadaten verwenden und können diese Werte nicht verändern.

Für Metadaten in der WHERE-Klausel können Sie keine Aliaswerte angeben, da NetWitness Suite die WHERE-Klausel verwendet, um Daten aus der Datenquelle (z. B. im Concentrator) abzurufen, und Datenquellen keine Aliase unterstützen. Das bedeutet, dass Sie für den HTTP-Port 80 nicht den Aliaswert **HTTP** angeben können.

**Hinweis:** * Sie können Aliase nur für Metadaten angeben, die noch nicht in Reporting Engine mit einem Alias versehen worden sind. Außerdem kann das Format der Aliase nicht geändert werden.
* Für Warnmeldungen und CSV-Berichte werden keine Aliase unterstützt.

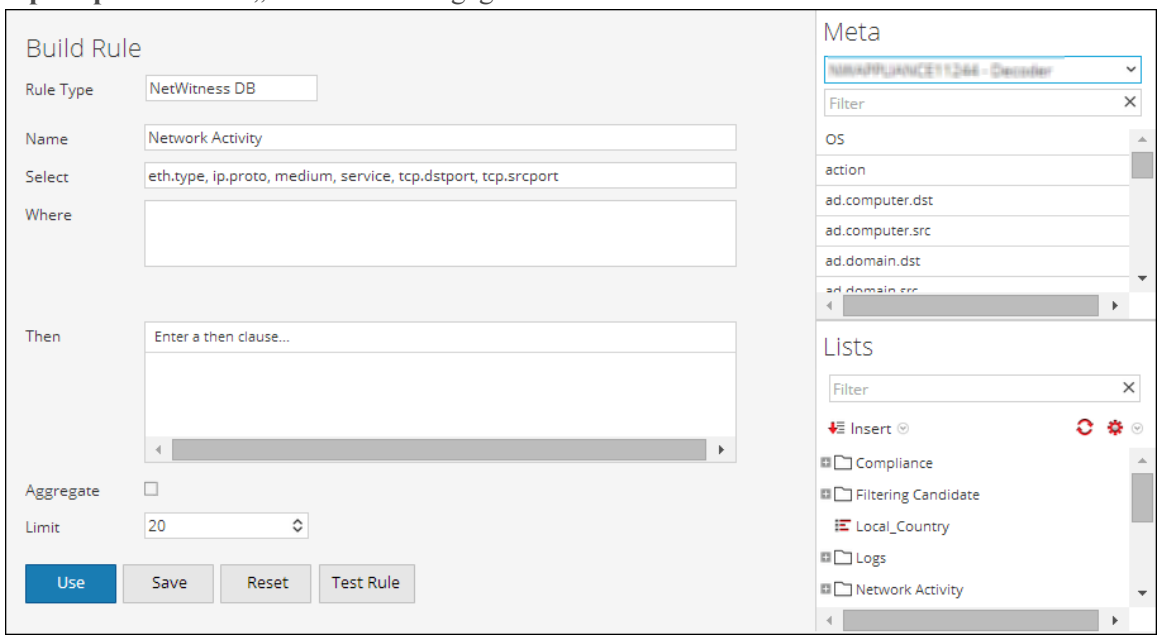
**So verwenden Sie Aliase in einer Regel:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Führen Sie im Bereich „Regelliste“ einen der folgenden Schritte aus:

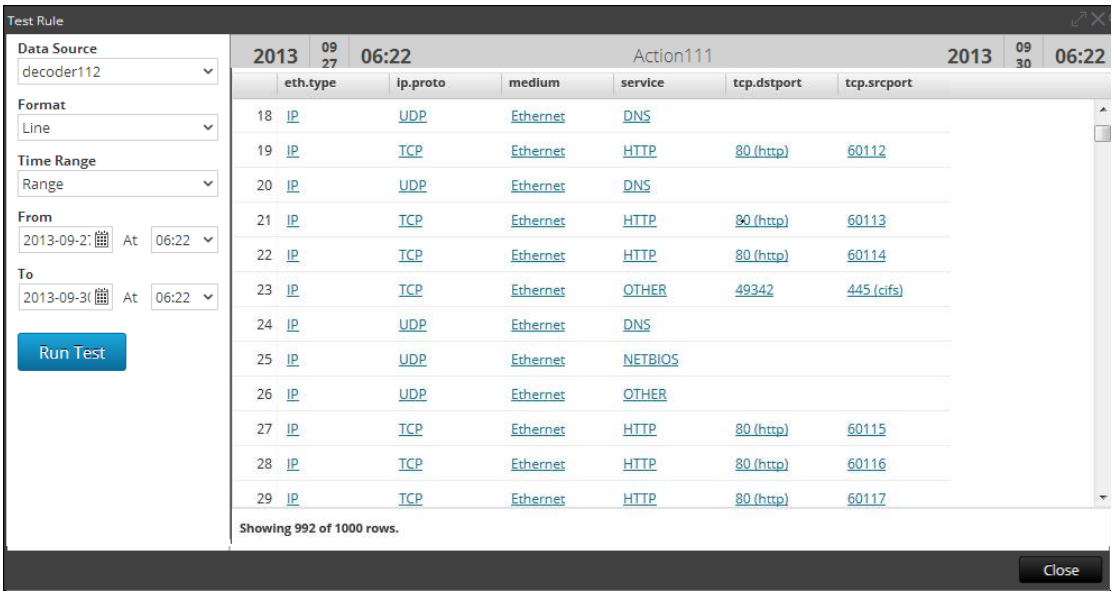
- Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste „Regeln“ auf .
- Klicken Sie auf > **Bearbeiten**.

3. Geben Sie im Feld **Auswählen** die Metadaten an, die einen Alias enthalten.

Im folgenden Beispiel sind die Metadaten **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport** und **tcp.srcport** im Feld „Auswählen“ angegeben.




4. Klicken Sie auf **Regel testen**.
   Im folgenden Beispiel werden die Ergebnisse in den Aliasspalten **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport** und **tcp.srcport** angezeigt, die im Feld **Auswählen** der Regel angegeben sind.




## Von RSA bereitgestellte Aliasdefinitionen

Die Aliasdateien in diesem Abschnitt sind nur Beispiele und basieren auf den aktuellen Aliasdefinitionen in Reporting Engine. Diese Definitionen in der Reporting Engine können je nach den Änderungen in der Concentrator-XML-Datei nicht von NetWitness Suite geändert werden. da keine der Änderungen in der XML-Datei im Contractor in der Reporting Engine widergespiegelt werden.

Die Details zu den verschiedenen Metadaten werden in den einzelnen **meta.aliases** erläutert.

**eth.type**

```
ALIAS_FORMAT=$alias
 0=802.3
 257=Experimental
 512=Xerox PUP
 513=Xerox PUP
 1024=Nixdorf
 1536=Xerox NS IDP
 1537=XNS Address Translation (3Mb only)
 2048=IP
 2049=X.75 Internet
 2050=NBS Internet
 2051=ECMA Internet
 2052=CHAOSnet
 2053=X.25 Level 3
 2054=ARP
 2055=XNS Compatibility
 2076=Symbolics Private
 2184=Xyplex
 2304=Ungermann-Bass network debugger
 2560=Xerox IEEE802.3 PUP
```

```
2561=Xerox IEEE802.3 PUP Address Translation
2989=Banyan Systems
2991=Banyon VINES Echo
4096=Berkeley Trailer negotiation
4097=Berkeley Trailer encapsulation for IP
4660=DCA - Multicast
5632=VALID system protocol
6537=Artificial Horizons
6549=Datapoint Corporation (RCL lan protocol)
15360=3Com NBP virtual circuit datagram (like XNS SPP) not registered
15361=3Com NBP System control datagram not registered
15362=3Com NBP Connect request (virtual cct) not registered
15363=3Com NBP Connect repsonse not registered
15364=3Com NBP Connect complete not registered
15365=3Com NBP Close request (virtual cct) not registered
15366=3Com NBP Close response not registered
15367=3Com NBP Datagram (like XNS IDP) not registered
15368=3Com NBP Datagram broadcast not registered
15369=3Com NBP Claim NetBIOS name not registered
15370=3Com NBP Delete Netbios name not registered
15371=3Com NBP Remote adaptor status request not registered
15372=3Com NBP Remote adaptor response not registered
15373=3Com NBP Reset not registered
16972=Information Modes Little Big LAN diagnostic
17185=THD - Diddle
19522=Information Modes Little Big LAN
21000=BBN Simnet Private
24576=DEC unassigned
24577=DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
24578=DEC Maintenance Operation Protocol (MOP) Remote Console
24579=DECNET Phase IV
24580=DEC Local Area Transport (LAT)
24581=DEC diagnostic protocol (at interface initialization?)
24582=DEC customer protocol
24583=DEC Local Area VAX Cluster (LAVC)
24584=DEC AMBER
24585=DEC MUMPS
24592=3Com Corporation
28672=Ungermann-Bass download
28673=Ungermann-Bass NIUs
28674=Ungermann-Bass diagnostic/loopback
28675=Ungermann-Bass ??? (NMC to/from UB Bridge)
28677=Ungermann-Bass Bridge Spanning Tree
28679=OS/9 Microware
28681=OS/9 Net?
28704=LRT (England) (now Sintrom)
28720=Racal-Interlan
28721=Prime NTS (Network Terminal Service)
```

```
28724=Cabletron
32771=Cronus VLN
32772=Cronus Direct
32773=HP Probe protocol
32774=Nestar
32776=AT&amp;amp;T/Stanford Univ.
32784=Excelan
32787=Silicon Graphics diagnostic
32788=Silicon Graphics network games
32789=Silicon Graphics reserved
32790=Silicon Graphics XNS NameServer
32793=Apollo DOMAIN
32814=Tymshare
32815=Tigan
32821=Reverse Address Resolution Protocol (RARP)
32822=Aeonic Systems
32823=IPX (Novell Netware?)
32824=DEC LanBridge Management
32825=DEC DSM/DDP
32826=DEC Argonaut Console
32827=DEC VAXELN
32828=DEC DNS Naming Service
32829=DEC Ethernet CSMA/CD Encryption Protocol
32830=DEC Distributed Time Service
32831=DEC LAN Traffic Monitor Protocol
32832=DEC PATHWORKS DECnet NETBIOS Emulation
32833=DEC Local Area System Transport
32834=DEC unassigned
32836=Planning Research Corp.
32838=AT&amp;amp;T
32839=AT&amp;amp;T
32840=DEC Availability Manager for Distributed Systems DECamds
32841=ExperData
32859=VMTP
32860=Stanford V Kernel
32861=Evans &amp;amp; Sutherland
32864=Little Machines
32866=Counterpoint Computers
32869=University of Mass. at Amherst
32870=University of Mass. at Amherst
32871=Veeco Integrated Automation
32872=General Dynamics
32873=AT&amp;amp;T
32874=Autophon
32876=ComDesign
32877=Compugraphic Corporation
32878=Landmark Graphics Corporation
32890=Matra
```

```
32891=Dansk Data Elektronik
32892=Merit Internodal
32893=Vitalink Communications
32896=Vitalink TransLAN III Management
32897=Counterpoint Computers
32904=Xyplex
32923=EtherTalk - AppleTalk over Ethernet
32924=Datability
32927=Spider Systems Ltd.
32931=Nixdorf Computers
32932=Siemens Gammasonics Inc.
32960=DCA Data Exchange Cluster
32966=Pacer Software
32967=Applitek Corporation
32968=Intergraph Corporation
32973=Harris Corporation
32975=Taylor Instrument
32979=Rosemount Corporation
32981=IBM SNA Services over Ethernet
32989=Varian Associates
32990=TRFS (Integrated Solutions Transparent Remote File System)
32992=Allen-Bradley
32996=Datability
33010=Retix
33011=AppleTalk Address Resolution Protocol (AARP)
33012=Kinetics
33015=Apollo Computer
33023=Wellfleet Communications
33026=Wellfleet BOFL
33027=Wellfleet Communications
33031=Symbolics Private
33067=Talaris
33072=Waterloo Microsystems Inc.
33073=VG Laboratory Systems
33079=IPX
33080=Novell Inc
33081=KTI
33087=M/MUMPS data sharing
33093=Vrije Universiteit (NL)
33094=Vrije Universiteit (NL)
33095=Vrije Universiteit (NL)
33100=SNMP
33103=Technically Elite Concepts
33169=PowerLAN
33149=XTP
33238=Artisoft Lantastic
33239=Artisoft Lantastic
33283=QNX Software Systems Ltd.
```

```
 33680=Accton Technologies (unregistered)
 34091=Talaris multicast
 34178=Kalpana
 34525=IPv6
 34617=Control Technology Inc.
 34618=Control Technology Inc.
 34619=Control Technology Inc.
 34620=Control Technology Inc.
 34848=Hitachi Cable (Optoelectronic Systems Laboratory)
 34902=Axis Communications AB
 34952=HP LanProbe test?
 36864=Loopback (Configuration Test Protocol)
 36865=3Com XNS Systems Management
 36866=3Com TCP/IP Systems Management
 36867=3Com loopback detection
 43690=DECNET
 64245=Sonix Arpeggio
 65280=BBN VITAL-LanBridge cache wakeups
 34915=PPPoe
 34916=PPPoe
 2056=Frame Relay ARP
 16962=IEEE bridge spanning protocol
 25944=Bridged Ethernet/802.3 packet
 65278=ISO CLNP/ISO ES-IS DSAP/SSAP
```

**ip.proto**

```
ALIAS_FORMAT=$alias
 0=HOPOPT
 1=ICMP
 2=IGMP
 3=GGP
 4=IP
 5=ST
 6=TCP
 7=CBT
 8=EGP
 9=IGP
 10=BBN-RCC-M
 11=NVP-II
 12=PUP
 13=ARGUS
 14=EMCON
 15=XNET
 16=CHAOS
 17=UDP
 18=MUX
 19=DCN-MEAS
 20=HMP
```

```
21=PRM
22=XNS-IDP
23=TRUNK-1
24=TRUNK-2
25=LEAF-1
26=LEAF-2
27=RDP
28=IRTP
29=ISO-TP4
30=NETBLT
31=MFE-NSP
32=MERIT-INP
33=SEP
34=3PC
35=IDPR
36=XTP
37=DDP
38=IDPR-CMTP
39=TP++
40=IL
41=IPv6
42=SDRP
43=IPv6-Rout
44=IPv6-Frag
45=IDRP
46=RSVP
47=GRE
48=MHRP
49=BNA
50=ESP
51=AH
52=I-NLSP
53=SWIPE
54=NARP
55=MOBILE
56=TLSP
57=SKIP
58=IPv6-ICMP
59=IPv6-NoNx
60=IPv6-Opts
61=AnyHost
62=CFTP
63=AnyNetwork
64=SAT-EXPAK
65=KRYPTOLAN
66=RVD
67=IPPC
68=AnyFile
```

```
69=SAT-MON
70=VISA
71=IPCV
72=CPNX
73=CPHB
74=WSN
75=PVP
76=BR-SAT-MO
77=SUN-ND
78=WB-MON
79=WB-EXPAK
80=ISO-IP
81=VMTP
82=SECURE-VM
83=VINES
84=TTP
85=NSFNET-IG
86=DGP
87=TCF
88=EIGRP
89=OSPFIGP
90=Sprite-RP
91=LARP
92=MTP
93=AX.25
94=IPIP
95=MICP
96=SCC-SP
97=ETHERIP
98=ENCAP
99=AnyPrivate
100=GMTP
101=IFMP
102=PNNI
103=PIM
104=ARIS
105=SCPS
106=QNX
107=A/N
108=IPComp
109=SNP
110=Compaq-Pe
111=IPX-in-IP
112=VRRP
113=PGM
114=AnyHop
115=L2TP
116=DDX
```

```
 117=IATP
 118=STP
 119=SRP
 120=UTI
 121=SMP
 122=SM
 123=PTP
 124=ISIS
 125=FIRE
 126=CRTP
 127=CRUDP
 128=SSCOPMCE
 129=IPLT
 130=SPS
 131=PIPE Pr
 132=SCTP St
 133=FC Fi
 134=RSVP-E2E-
 255=Reserved
```

**medium**

```
ALIAS_FORMAT=$alias
 1=Ethernet
 2=Tokenring
 3=FDDI
 4=HDLC
 5=NetWitness
 6=802.11
 7=802.11 Radio
 8=802.11 AVS
 9=802.11 PPI
 10=802.11 PRISM
 11=802.11 Management
 12=802.11 Control
 13=DLT Raw
 32=Logs
```

**service**

```
ALIAS_FORMAT=$alias
 0=OTHER
 20=FTPD
 21=FTP
 22=SSH
 23=TELNET
 25=SMTP
 53=DNS
 67=DHCP
 69=TFTP
 80=HTTP
```

```
110=POP3
111=SUNRPC
119=NNTP
123=NTP
135=RPC
137=NETBIOS
139=SMB
143=IMAP
161=SNMP
179=BGP
443=SSL
502=MODBUS
520=RIP
1024=EXCHANGE
1080=SOCKS
1122=MSN IM
1344=ICAP
1352=NOTES
1433=TDS
1521=TNS
1533=SAMETIME
1719=H.323
1720=RTP
2000=SKINNY
2040=SOULSEEK
2049=NFS
3270=TN3270
3389=RDP
3700=DB2
5050=YAHOO IM
5060=SIP
5190=AOL IM
5222=Google Talk
5900=VNC
6346=GNUTELLA
6667=IRC
6801=Net2Phone
6881=BITTORRENT
8000=QQ
8002=YCHAT
8019=WEBMAIL
8082=FIX
20000=DNP3
1000000=KERNEL
1000001=USER
1000003=SYSTEM
1000004=AUTH
1000005=LOGGER
```

```
 1000006=LPD
 1000008=UUCP
 1000009=SCHEDULE
 1000010=SECURITY
 1000013=AUDIT
 1000014=ALERT
 1000015=CLOCK
```

## tcp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
 119=nntp
 135=epmap
 137=netbios-ns
 139=netbios-ssn
 143=imap
 158=pcmail-srv
 170=print-srv
 179=bgp
 194=irc
 389=ldap
 443=https
 445=cifs
```

```
464=kpasswd
512=exec
513=login
514=cmd
515=printer
520=efs
526=tempo
530=courier
531=conference
532=netnews
540=uucp
543=klogin
544=kshell
556=remotefs
636=ldaps
749=kerberos-adm
993=imaps
995=pop3s
1109=kpop
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1524=ingreslock
1723=pptp
2053=knetd
1122=msn im
1352=notes
1521=tns
1533=sametime
1718=h323
1720=rtp
1863=msn im
2049=nfs
3389=rdp
5050=yahoo im
5060=sip
5190=aim
6346=gnuetella
6667=irc
9001=tor
9030=tor
9535=man
```

**tcp.srcport**

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
 119=nntp
 135=epmap
 137=netbios-ns
 139=netbios-ssn
 143=imap
 158=pcmail-srv
 170=print-srv
 179=bgp
 194=irc
 389=ldap
 443=https
 445=cifs
 464=kpasswd
 512=exec
 513=login
 514=cmd
 515=printer
 520=efs
 526=tempo
 530=courier
 531=conference
```

```
 532=netnews
 540=uucp
 543=klogin
 544=kshell
 556=remotefs
 636=ldaps
 749=kerberos-adm
 993=imaps
 995=pop3s
 1109=kpop
 1433=ms-sql-s
 1434=ms-sql-m
 1512=wins
 1524=ingreslock
 1723=pptp
 2053=knetd
 1122=msn im
 1352=notes
 1521=tns
 1533=sametime
 1718=h323
 1720=rtp
 1863=msn im
 2049=nfs
 3389=rdp
 5050=yahoo im
 5060=sip
 5190=aim
 6346=gnuetella
 6667=irc
 9001=tor
 9030=tor
 9535=man
```

**udp.dstport**

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 37=time
 39=rlp
 42=nameserver
 53=domain
 67=bootps
 68=bootpc
 69=tftp
```

```
88=kerberos
111=sunrpc
123=ntp
135=epmap
137=netbios-ns
138=netbios-dgm
161=snmp
162=snmptrap
213=ipx
443=https
445=cifs
464=kpasswd
500=isakmp
512=biff
513=who
514=syslog
517=talk
518=ntalk
525=timed
533=netwall
550=new-rwho
560=rmonitor
561=monitor
749=kerberos-adm
1167=phone
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1701=l2tp
1812=radiusauth
1813=radacct
2049=nfsd
2504=nlbs
```

## Testen einer Regel

Sie können eine Regel basierend auf dem Zeitbereich und der ausgewählten Datenquelle testen.

### Führen Sie zum Testen einer Regel die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.

2. Führen Sie im Bereich „Regelliste“ einen der folgenden Schritte aus:
   - Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste „Regeln“ auf .
   - Klicken Sie auf > **Bearbeiten**.

     Die Registerkarte der Ansicht Regel erstellen wird angezeigt.
3. Klicken Sie auf **Regel testen**.

   Die Ansicht „Regel testen“ wird angezeigt.


> **Hinweis:** Wenn Sie auf **Regel testen** klicken, wird die Regel nicht gespeichert. Sie müssen in der Ansicht „Regel erstellen“ auf **Speichern** klicken, um die Regel zu speichern.

4. Wählen Sie in der Drop-down-Liste **Datenquelle** eine Datenquelle aus.

   Wählen Sie eine für die definierte Regel geeignete Datenquelle aus.
5. Wählen Sie in der Drop-down-Liste **Format** das Format aus, in dem das Ergebnis angezeigt werden soll.
6. Wählen Sie in der Drop-down-Liste **Zeitbereich** eine der folgenden Optionen aus.
   - **Vergangen**: Hier können Sie eine Anzahl von Jahren, Tagen, Wochen, Monaten, Tagen oder Stunden angeben.
   - **Bereich**: Hier können Sie einen Datumsbereich und einen Zeitraum angeben.

**Hinweis:** Die in der Benutzeroberfläche (UI) angezeigte Uhrzeit und das angezeigte Datum hängen vom Zeitzonenprofil ab, das vom Benutzer ausgewählt wurde.

7. **X-Achse** und **Y-Achse** werden zur Angabe der Metadaten verwendet, die in die Diagramme geplottet werden sollen.

   In **X-Achse** werden die Metadaten für die Regel „Gruppieren nach“ angezeigt. In **Y-Achse** werden die in der Regel verwendeten Aggregatfunktionen angezeigt.

**Hinweis:** „Sum“, „Count“, „Countdistinct“ und „Average“ sind die unterstützten Aggregatfunktionen für die Regel. Standardmäßig können Sie für benutzerdefinierte Regeln mit mehreren „Gruppieren nach“-Klauseln nur die ersten Metadaten in **X-Achse** auswählen.

8. Klicken Sie auf **Test ausführen**, um die Regel auszuführen.

   Die Regeldaten (sofern vorhanden) für den ausgewählten Zeitbereich werden angezeigt.

## Erstellen einer Liste oder Listengruppe

### Um eine Liste zu erstellen, führen Sie die folgenden Schritte aus:

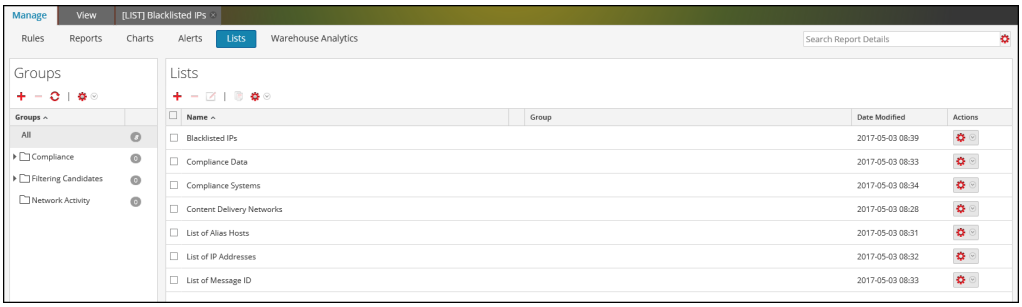
Listen können innerhalb einer Gruppe oder im Stammordner hinzugefügt werden.

1. Wählen Sie **Monitor** > **Berichte** aus.

   Die Registerkarte „Managen“ wird angezeigt.

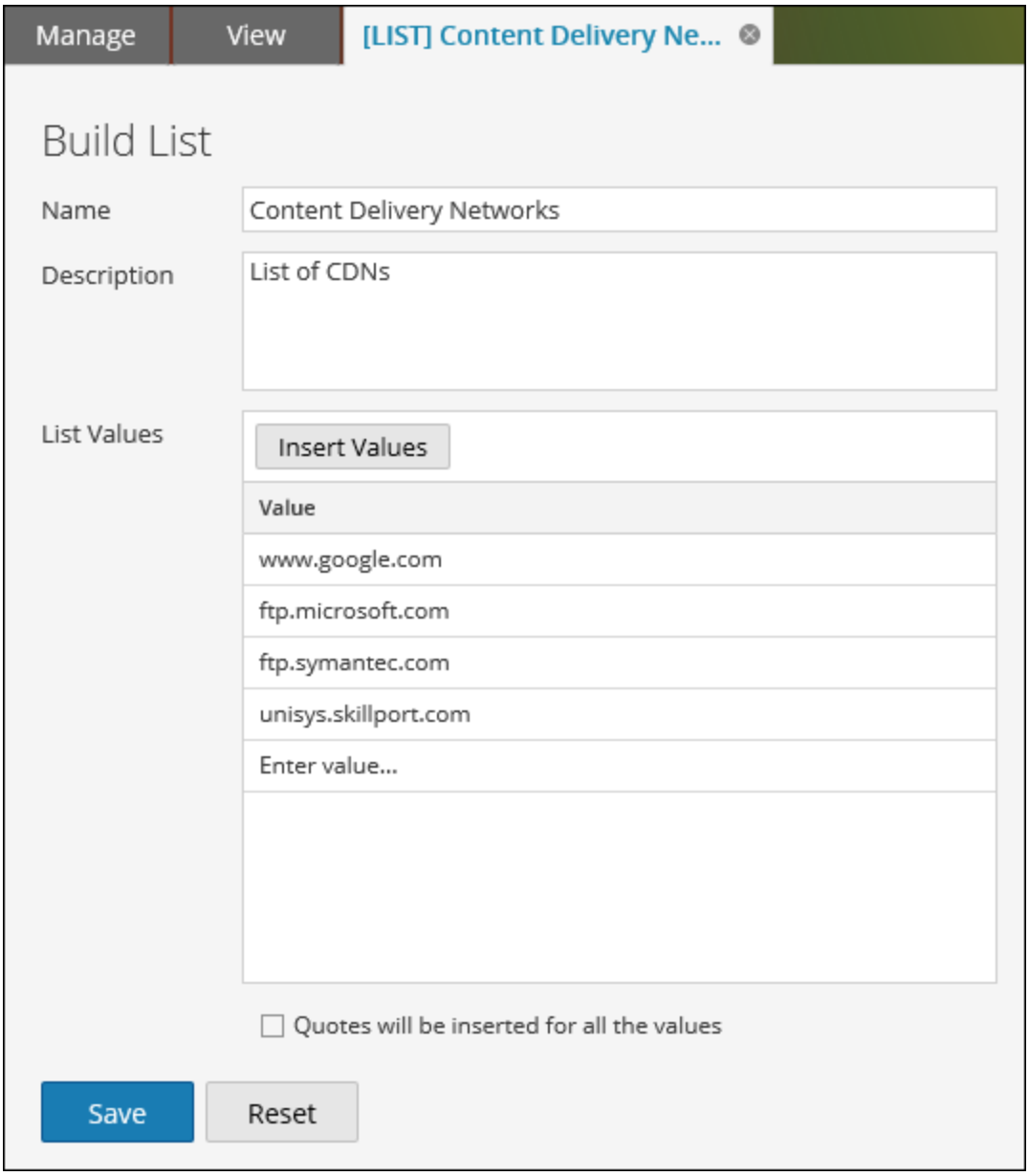
2. Klicken Sie auf **Listen**.

   Die Listenansicht wird angezeigt.




3. Klicken Sie in der Symbolleiste **Liste** auf  .

   Die Registerkarte „Ansicht „Liste aufbauen““ wird angezeigt.

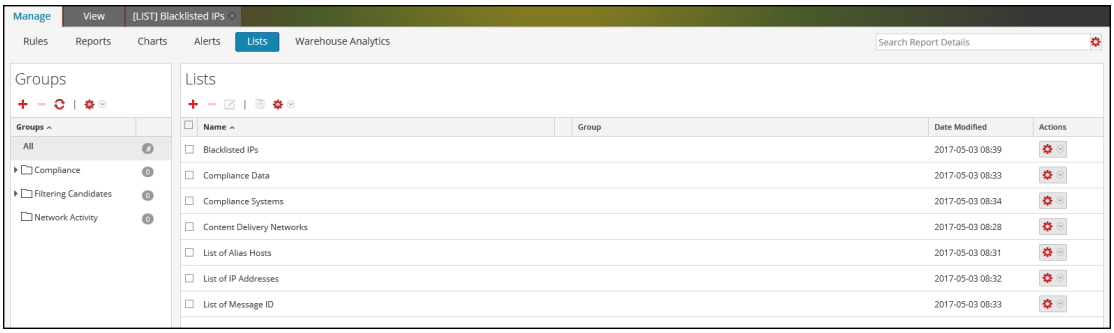



4. Geben Sie im Feld **Name** einen eindeutigen Namen für die Liste ein.
5. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Liste ein.
6. Führen Sie im Feld **Listenwerte** einen der folgenden Schritte aus:
   - Klicken Sie auf **Einfügen** und geben Sie die Werte durch Kommas getrennt ein. Sie können eine Liste von Werten aus einer Datei oder anderen Listen einfügen.
   - Geben Sie die Werte in das Feld **Wert** ein.
7. Wenn Sie möchten, dass zur Laufzeit direkt Anführungszeichen für die Werte eingefügt werden, wählen Sie **Anführungszeichen werden für alle Werte eingefügt** aus.

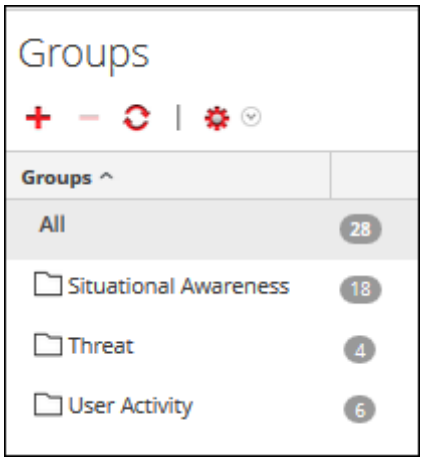
8. Klicken Sie auf **Speichern**.

### Um eine Listengruppe zu erstellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Gehen Sie folgendermaßen vor:
   - So erstellen Sie eine Listengruppe
     1. Klicken Sie im Bereich „Listengruppen“ auf +.
        Dem Bereich „Listengruppe“ wird eine neue Listengruppe hinzugefügt.




     2. Geben Sie den Namen für die Listengruppe ein und drücken Sie die EINGABETASTE.
   - So erstellen Sie eine Listenuntergruppe:
     1. Wählen Sie im Bereich „Listengruppen“ die Listengruppe aus, der Sie eine Untergruppe hinzufügen möchten.

2. Klicken Sie auf  .

   Der Listengruppe wird eine neue Listenuntergruppe hinzugefügt.

3. Geben Sie den Namen für die Listenuntergruppe ein und drücken Sie die EINGABETASTE.

# Erstellen und Planen eines Berichts

Sie können einen einfachen oder komplexen Bericht erstellen und seine Ausführungseigenschaften durch Planen eines Berichts konfigurieren. Ein Bericht kann mehrere Regeln enthalten und Sie können verschiedene Zeitbereiche planen, um den gleichen Bericht auszuführen. Je nach Ihren Anforderungen können Sie beispielsweise planen, dass ein Bericht täglich, wöchentlich oder monatlich ausgeführt wird.

Wenn Sie einen Bericht ausführen, werden die Ergebnisse in der Reporting Engine gespeichert.

Nach dem Erzeugen eines Berichts können Sie folgende Aktionen ausführen:

- Senden des Berichts per E-Mail an andere Benutzer, indem die Ausgabeaktionen konfiguriert werden. Sie können die Ausgabeaktionen auch vor dem Erzeugen eines Berichts konfigurieren.
- Herunterladen der Berichte als PDF- oder CSV-Dateien (Comma-Separated Values).

**Hinweis:** Der Abbrechen-Vorgang wird bei Antwort-Berichten nicht unterstützt.

## Erstellen eines Berichts oder einer Berichtsgruppe

**Führen Sie zum Erstellen eines Berichts zu einer Gruppe oder Untergruppe die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie in der Symbolleiste **Bericht** auf + .
   Die Registerkarte „Bericht erstellen“ wird angezeigt.
4. Geben Sie den Namen des Berichts ein.
5. Legen Sie den Text und die Regeln per Drag-and-Drop im Bericht ab.

   **Hinweis:** Der eingegebene Text ist optional und Sie brauchen diese Option möglicherweise nur, wenn Sie benutzerdefinierte Kopfzeilen oder Inhalte anzeigen möchten.

6. Klicken Sie auf **Speichern**.
   Eine Bestätigungsmeldung, dass der Bericht erfolgreich gespeichert wurde, wird angezeigt.

**Führen Sie folgende Schritte durch, um eine Gruppe zum Standardordner oder Untergruppen zu einer Berichtsgruppe hinzuzufügen:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie im Bereich **Diagrammgruppen** auf + .
   Eine Standardgruppe wird im Bereich „Diagrammgruppen“ hinzugefügt.
4. Geben Sie den Namen für die neue Gruppe ein.
5. Drücken Sie die Eingabetaste.
   Die Gruppe wird dem Bereich „Berichtsgruppen“ hinzugefügt.

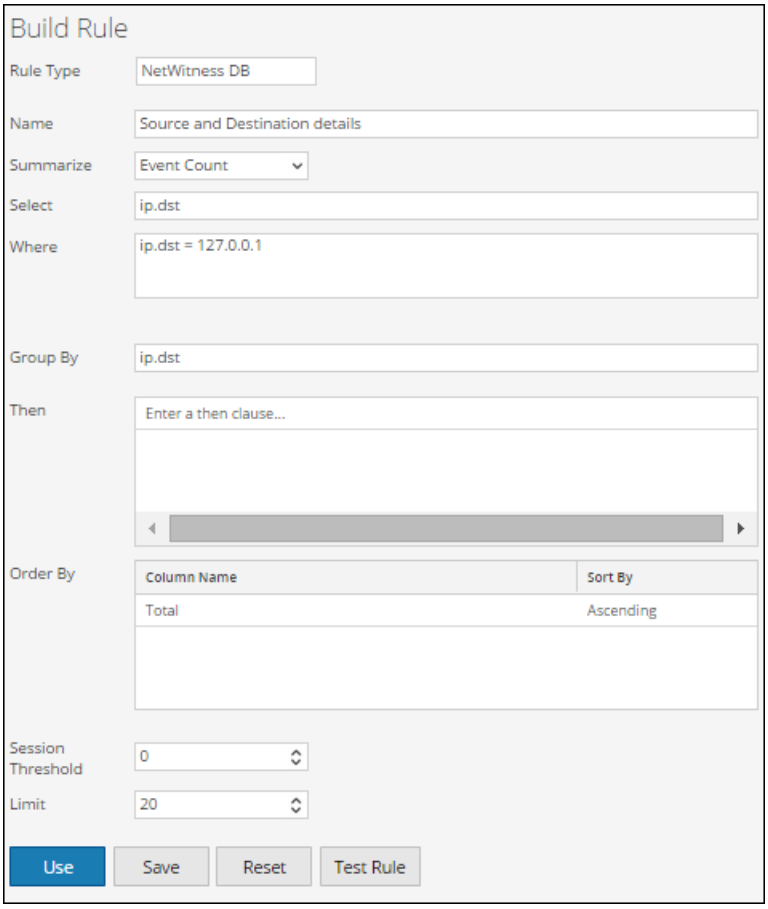
## Planen von Berichten

**Hinweis:** Wenn Sie einen Warehouse-Bericht planen, können Sie einen unterstützten Aufgabenplaner verwenden, um spezifische Ressourcen in einem Cluster für den geplanten Job zuzuweisen. Weitere Informationen zu unterstützten Aufgabenplanern finden Sie unter Aufgabenplaner für Warehouse Reporting.

**Führen Sie die folgenden Schritte aus, um einen Bericht zu planen:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie auf der Seite **Regel erstellen** auf +, um eine Regel zu erstellen.
4. Klicken Sie auf **Speichern**.

5. Klicken Sie auf **Verwenden**.




6. Wählen Sie **Neuer Bericht** oder **Vorhandener Bericht** aus.
7. Wählen Sie eine Berichtsgruppe aus und klicken Sie auf **Auswählen**.
8. Geben Sie den Namen des Berichts ein und wählen Sie die Regel aus.
9. Klicken Sie auf **Planen**.
   Die Ansicht „Bericht planen“ wird angezeigt.

> **Hinweis:** Wenn Sie einem anderen Benutzer Zugriffsberechtigungen für einen Bericht gewähren, müssen Sie auch Berechtigungen für die Berichtsgruppe, für die im Bericht verwendeten Regeln und für die Regelgruppen gewähren. Andernfalls wird eine Fehlermeldung angezeigt.

8. Aktivieren Sie für die planmäßige Ausführung der Berichte das Kontrollkästchen **Aktivieren**.

9. Geben Sie im Feld **Planname** einen Namen für die geplante Berichtsplanungskonfiguration ein.
10. Wählen Sie im Feld „Datenquelle“ die Datenquelle aus.

    **Hinweis:** Wenn die Datenquelle nicht aufgelistet ist, stellen Sie sicher, dass Sie die **Leseberechtigung** für die Datenquelle haben. Dies gilt nur für NWDB-, Respond- und Warehouse-Datenquellen. Weitere Informationen finden Sie unter „Konfigurieren von Datenquellenberechtigungen“ im *Konfigurationsleitfaden Reporting Engine*.
11. (Optional) Wählen Sie in der Drop-down-Liste **Warehouse-Ressourcenpool** die im Cluster verfügbaren Pools oder Warteschlangen aus, um den Bericht so zu planen, dass er entweder im Pool oder in der Warteschlange ausgeführt wird. Diese Drop-down-Liste steht nur zur Verfügung, wenn Sie einen Warehouse-DB-Bericht auswählen.

    **Hinweis:** Alle Warteschlangen oder Pools, die Sie auf der Seite „Durchsuchen“ für die Reporting Engine angeben, werden aufgelistet. Wenn keine Pools oder Warteschlangen auf der Seite „Durchsuchen“ konfiguriert wurden, ist diese Drop-down-Liste deaktiviert und die Jobs werden ohne Warteschlangen- oder Poolnamen an die Cluster übermittelt.

    **Hinweis:** Wenn der im Berichtsplan konfigurierte Pool bzw. die konfigurierte Warteschlange aus dem Cluster entfernt wird, bleibt der Warteschlangenname im Kapazitätsplaner undefiniert. Im Fair Scheduler wird der angegebene Poolname jedoch mithilfe der Eigenschaft „mapred.fairscheduler.allow.undeclared.pool“ erstellt.
12. Wählen Sie in der Drop-down-Liste „Zeitzone“ eine Zeitzone aus, um alle zeitbezogenen Daten in einer Berichtsausgabe im angegebenen Format anzuzeigen. Diese Einstellung kann in der Ansicht „Durchsuchen“ der Reporting Engine konfiguriert werden (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
13. Wählen Sie im Feld **Ausführen** den Typ der Ausführungsplanung aus. (Beispielsweise „Jetzt“ oder „Stündlich“.)
    Tun Sie je nach Typ der Ausführungsplanung Folgendes:
    - Wenn Sie als Ausführungsplanung **Später** oder **Monatlich** auswählen, müssen Sie im entsprechenden angegebenen Feld einen Wert für den Tag und die Uhrzeit angeben.
    - Wenn Sie als Ausführungsplanung **Stündlich** auswählen, müssen Sie die Minuten im Feld **Bei Minute** eingeben.
    - Wenn Sie als Ausführungsplanung **Täglich** auswählen, müssen Sie einen Wert im Feld **Um** eingeben.

- Wenn Sie als Ausführungsplanung **Wöchentlich** auswählen, müssen Sie einen Wert im Feld **Um** eingeben und auch die Wochentage auswählen.

**Hinweis:** Wenn Sie beim Planen eines Berichts die Option **Vergangenheit** oder **Bereich (spezifisch/generisch)** oder einen Endzeitbereich sehr nah der aktuellen Zeit auswählen, müssen Sie sicherstellen, dass die aggregierten Daten in der Datenquelle zurückgegeben werden. Wenn es in der Datenquelle zu einer Aggregationsverzögerung kommt, sollten Sie diese Verzögerung bei der Wahl der Endzeit berücksichtigen, andernfalls können in den Berichten für diese Zeitspanne nicht aggregierte Daten verloren gehen.

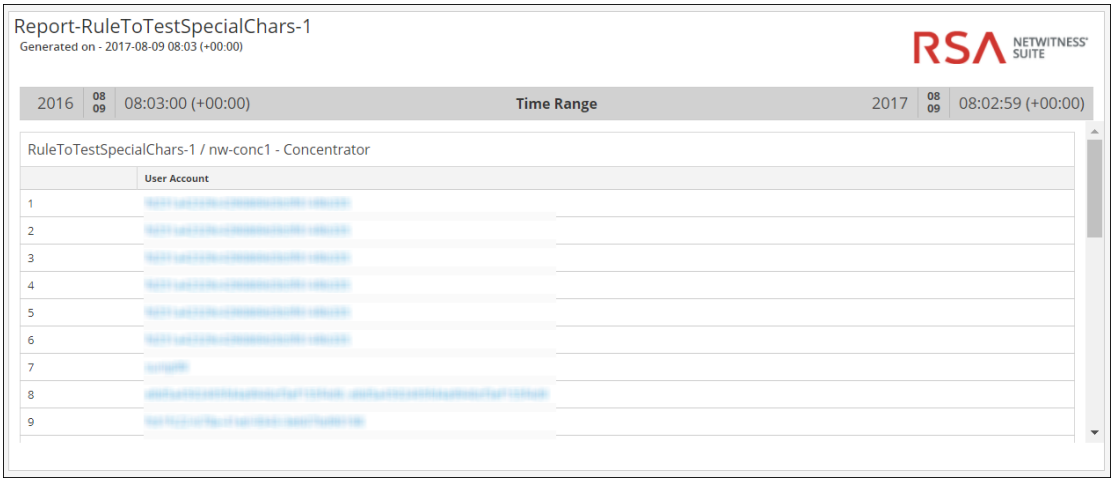
Informationen zum Erzeugen eines Berichts mit Variablen finden Sie unter Erstellen eines parametrisierten Berichts mit Variablen.

14. (Optional) Gehen Sie im Bereich **Ausgabeaktionen** wie folgt vor:
    a. Geben Sie die E-Mail-Adresse und den Betreff ein.
    b. Bearbeiten Sie den Meldungstext für den Bericht.
    c. Wählen Sie das Format des Anhangs aus.
    d. Geben Sie einen Wert für die CSV-Trennzeichen und Trennzeichen für mehrere Werte ein.
    e. (Optional) Gehen Sie im Feld „Andere Optionen“ wie folgt vor:
        i. Klicken Sie auf  und wählen Sie als Ausgabeaktion „SFTP“, „URL“ oder „Netzwerkfreigabe“ aus.
        Eine Zeile wird mit der ausgewählten Ausgabeaktion hinzugefügt.
        ii. Wählen Sie die entsprechenden Optionen aus, um den Bericht im PDF- bzw. CSV-Format oder in beiden Formaten an die mit RE konfigurierte Ausgabeaktion „SFTP“, „URL“ oder „Netzwerkfreigabe“ zu senden.
15. (Optional) Informationen zum Hinzufügen einer Liste im Bereich „Dynamische Liste“ finden Sie im Abschnitt Erzeugen einer Liste aus dem geplanten Bericht.
16. (Optional) Zum Auswählen eines Logos im Bereich „Logo“ finden Sie im Abschnitt *Managen und Auswählen von Berichtslogos* in Managen von Listen, Regeln oder Berichten nähere Informationen.

    **Hinweis:** Wenn Sie kein Logo angeben, wird das RSA-Standardlogo verwendet.

17. Klicken Sie auf **Planen**.
    Der geplante Bericht wird nach Plan ausgeführt und stellt die konfigurierten Ausgaben

bereit.




Nach dem Erstellen und Planen eines Berichts können Sie eine der folgenden Aufgaben ausführen:

1. Sie können den E-Mail-Empfänger benachrichtigen, wenn die Ausführung des Berichts abgeschlossen wurde, und Berichte im PDF- und CSV-Format als Anlagen an die E-Mail-Nachricht anfügen.
2. Sie können eine Liste anhand des geplanten Berichts erzeugen und sie im Modul **Listen** anzeigen.
3. Sie können einen geplanten Bericht im PDF- oder CSV-Format bzw. in beiden Formaten an den RE-konfigurierten SFTP-Speicherort, an die URL oder an die Netzwerkfreigabe senden.
4. Sie können das Standardlogo ändern und es im geplanten Bericht anzeigen.
5. Sie können die Konfigurationsdetails der NetWitness Suite Reporting Engine ändern, indem Sie zur Registerkarte „Allgemein“ der Reporting Engine navigieren. Weitere Informationen finden Sie im Thema „Registerkarte „Allgemein“ für Reporting Engine“ auf der *Registerkarte „Allgemein“ für Reporting Engine*.

**Beispiele**

Beim Planen von Berichten in der Ansicht „Bericht planen“ werden die Ergebnisse für die Option **Vergangen** standardmäßig basierend auf der benutzerdefinierten Zeitzone aufgeführt. Die folgenden Beispiele verdeutlichen, welche Ergebnisse bei Auswahl von **Stunden**, **Tage**, **Wochen**, **Monate** oder **Jahre** für die Option **Vergangen** basierend auf der absoluten oder relativen Dauer zu erwarten sind.

**Hinweis:** Standardmäßig ist das Kontrollkästchen für die relative Dauer deaktiviert. Dies bedeutet, dass die Ergebnisse für die Option **Vergangen** basierend auf der absoluten Dauer aufgeführt werden.

- **Basierend auf absoluter Dauer:** Die absolute Dauer ermöglicht das Planen eines Berichts zu einer absoluten Uhrzeit in Bezug auf die aktuelle Uhrzeit, wobei die Sekunden ausgeschlossen und das Zeitintervall als Ganzes berücksichtigt werden. Beispielsweise wäre 12:00 Uhr die absolute Uhrzeit der aktuellen Uhrzeit 12:45 Uhr.
  - Stunden: Angenommen, Sie haben Stunden ausgewählt und geben 1 Stunde an. Wenn die aktuelle vom Benutzer angegebene Uhrzeit 16:20 Uhr ist, wird der Bericht für den Zeitraum von 15:00 Uhr bis 16:00 Uhr erzeugt.
  - Tage: Angenommen, Sie haben Tage ausgewählt und geben 1 Tag an. Wenn das aktuelle Datum der 27. August 2014 und die aktuelle vom Benutzer angegebene Uhrzeit 10:15 Uhr ist, wird der Bericht für den folgenden Zeitraum erzeugt: 26. August 2014, 12:00 bis 27. August 2014, 12:00.
  - Wochen: Angenommen, Sie haben Wochen ausgewählt und geben 1 Woche an. Wenn das aktuelle Datum der 27. August 2014, 14:30 ist und dieser Tag auf einen Mittwoch fällt, wird der Bericht für den folgenden Zeitraum erzeugt: Samstag, 16. August 2014, 12:00 Uhr bis Samstag, 23. August 2014, 12:00 Uhr.
  - Monate: Angenommen, Sie haben Monate ausgewählt und geben 1 Monat an. Wenn das aktuelle Datum der 27. August 2014 und die aktuelle Uhrzeit 14:30 Uhr ist, wird der Bericht für den folgenden Zeitraum erzeugt:
    01.Juli 2014, 12:00 bis 31. Juli 2014, 12:00.
  - Jahre: Angenommen, Sie haben Jahre ausgewählt und geben 1 Jahr an. Wenn das aktuelle Datum der 27. August 2014 und die aktuelle Uhrzeit 14:30 Uhr ist, wird der Bericht für den folgenden Zeitraum erzeugt:
    01. Januar 2013, 12:00 Uhr bis 31. Dezember 2013, 12:00 Uhr.
- **Basierend auf relativer Dauer:** Die relative Dauer ermöglicht das Planen eines Berichts zu einer relativen Uhrzeit in Bezug auf die aktuelle Uhrzeit, die basierend auf der aktuellen Zeit variieren kann. Beispielsweise wäre 12:45 Uhr die relative Uhrzeit der aktuellen Uhrzeit 12:45 Uhr.
  - Stunden: Angenommen, Sie haben Stunden ausgewählt und geben 1 Stunde an. Wenn die aktuelle vom Benutzer angegebene Uhrzeit 16:20 Uhr ist, wird der Bericht für den Zeitraum von 15:20 Uhr bis 16:20 Uhr erzeugt.
  - Tage: Angenommen, Sie haben Tage ausgewählt und geben 1 Tag an. Wenn das aktuelle Datum der 27. August 2014 und die aktuelle vom Benutzer angegebene Uhrzeit 10:15 Uhr ist, wird der Bericht für den folgenden Zeitraum erzeugt: 26. August 2014, 10:15 bis 27. August 2014, 10:15.

- Wochen: Angenommen, Sie haben Wochen ausgewählt und geben 1 Woche an. Wenn das aktuelle Datum der 27. August 2014 und die aktuelle Uhrzeit 12:30 Uhr ist und dieser Tag auf einen Mittwoch fällt, wird der Bericht für den folgenden Zeitraum erzeugt: Donnerstag, den 21. August 2014 00:30 bis Mittwoch, den 27. August 2014 00:30.
- Monate: Angenommen, Sie haben Monate ausgewählt und geben 1 Monat an. Wenn das aktuelle Datum der 27. August 2014 und die aktuelle Uhrzeit 14:30 Uhr ist, wird der Bericht für den folgenden Zeitraum erzeugt: 27. Juli 2014, 14:30 bis 27. August 27 2014, 14:30.
- Jahre: Angenommen, Sie haben Jahre ausgewählt und geben 1 Jahr an. Wenn das aktuelle Datum der 27. August 2014 und die aktuelle Uhrzeit 14:30 Uhr ist, wird der Bericht für den folgenden Zeitraum erzeugt: 27. August 2013, 14:30 Uhr bis 27. August 2014, 14:30 Uhr.

# Zusätzliche Verfahren

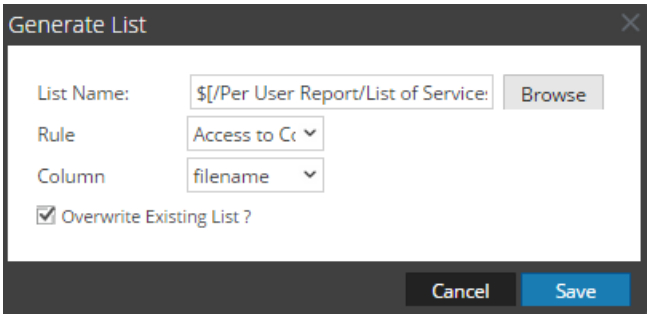
## Erzeugen einer Liste aus dem geplanten Bericht

Sie können aus der Ausgabe des geplanten Berichts eine Liste erzeugen. Stellen Sie sicher, dass Ihre Listen in NetWitness Suite erstellt werden, bevor Sie eine Liste zur Planung eines Berichts erzeugen.

**Führen Sie folgende Schritte aus, um eine Liste aus der Ansicht „Bericht erstellen“ zu erzeugen:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus und klicken Sie auf  > **Bericht planen**.
   Die Ansichtsregisterkarte Einen Bericht planen wird angezeigt.
4. Klicken Sie im Bereich **Dynamische Liste** auf  .
   Das Dialogfeld „Liste erzeugen“ wird geöffnet.
5. Klicken Sie auf **Durchsuchen**.
   Der Bereich „Listenauswahl“ wird angezeigt.
6. Wählen Sie ein Listenelement aus und klicken Sie auf **Auswählen**.
   Der Listenname wird im Feld „Listenname“ ausgefüllt.

7. Wählen Sie eine gültige Regel, um die Berichtsergebnisse auf der Grundlage der Regeldefinition weiter zu filtern.
8. Wählen Sie einen Wert für das Feld **Spalte** aus.
   Die Spalte bildet die Werte für die Liste, die erzeugt wird.
9. Wenn Sie die vorhandene Liste überschreiben möchten, aktivieren Sie das Kontrollkästchen **Vorhandene Liste überschreiben?**.
10. Klicken Sie auf **Speichern**.
    Der Listenname wird im Bereich „Liste erzeugen“ ausgefüllt.




11. (Optional) Wählen Sie eine Liste aus dem Bereich „Liste erzeugen“ aus und klicken Sie auf , um die ausgewählte Liste zu löschen.
12. (Optional) Wählen Sie eine Liste aus dem Bereich „Liste erzeugen“ aus und klicken Sie auf , um die Details der Liste zu bearbeiten.

## Erstellen eines parametrisierten Berichts mit Variablen

Sie verwenden Variablen für das Reporting im RSA NetWitness Suite Reporting Modul. Parametrisiertes Reporting ermöglicht es Ihnen, Werte dynamisch in der Laufzeit zu spezifizieren ohne die Regeldefinition zu ändern, sodass Sie die Ergebnisse basierend auf einem bestimmten Wert anzeigen können. Sie können parametrisiertes Reporting aktivieren, indem Sie in der Abfrage oder Regel Variablen verwenden. Informationen zum Hinzufügen einer Regel finden Sie unter Konfigurieren einer Regel. Sie können in der Laufzeit einen Wert für die Variable eingeben oder einen Wert aus der Liste auswählen, je nachdem, wo der Ergebnissatz angezeigt wird.

Die Syntax zur Spezifizierung der Variable ist die folgende:

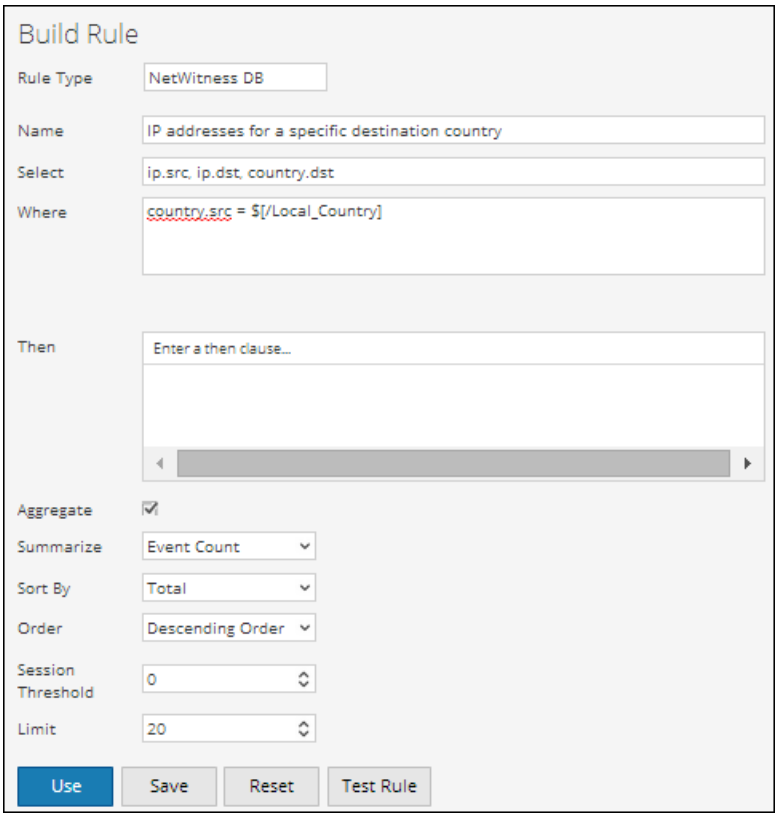
| Beschreibung | Beispiele für unterstützte Syntax |
| --- | --- |
| Geben Sie vor einer Variablen das Zeichen `$` ein.<br>Schließen Sie eine Variable in geschweiften Klammern ein. | `columnname=${<variable>}` |

Die Syntax zum Definieren einer Variablen ist für die Datenquellen NetWitness-Datenbanken, IPDB-Datenbanken und Warehouse-Datenbanken dieselbe. Wenn Sie den Wert einer Variablen in einer Laufkonfiguration zuweisen, müssen Sie den Wert in einfache Anführungszeichen setzen. `'<value>'`.

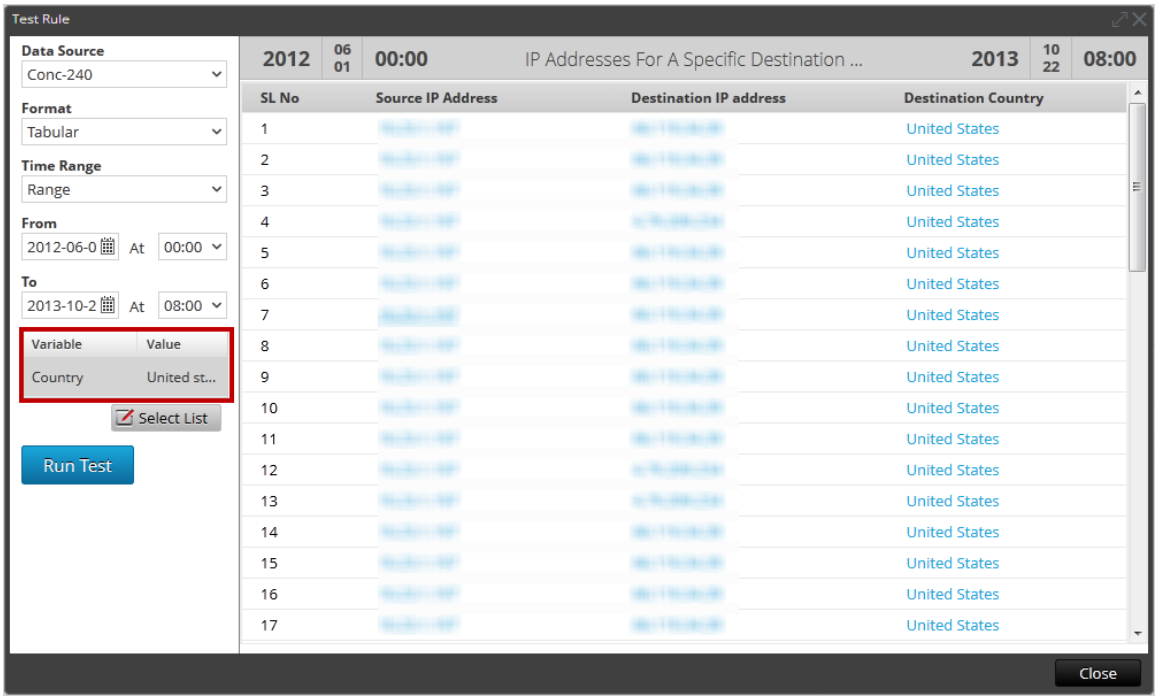
In diesem Abschnitt werden einige Beispiele, in denen Variablen verwendet werden können, angeführt.

**Anzeige der IP-Adresse der Quelle eines spezifischen Ziellandes**

Es folgt ein Beispiel einer NetWitness-DB-Regel, um die Quell- und Ziel-IP-Adresse eines spezifischen Landes anzuzeigen. Hier ist der Wert für Quellland als eine Variable `${local_country}` definiert.



In der Laufzeit werden Sie aufgefordert, den Wert der Variable einzugeben. Die Abbildung unten zeigt die Variable `local_Country`, in die Sie den Wert eingeben können. Wenn Sie den Wert **USA** eingeben, werden alle Quell- und Ziel-IP-Adressen mit dem Zielland „USA“ aufgelistet.




Sie können die oben angegebene Regel zum Planen eines Berichts verwenden. Sie können zwei Arten von Berichten planen:

- Bericht mit dynamischen Variablen
- Iterativer Bericht

## Bericht mit dynamischen Variablen

Dynamische Variablen ermöglichen dem Benutzer, die Werte für eine Variable, die in einer Regel definiert wurde, während des Planens eines Berichts festzulegen.

**Führen Sie die folgenden Schritte aus, um einen Bericht mit dynamischen Variablen zu planen:**

1. Wählen Sie **Monitor** > Berichte aus.

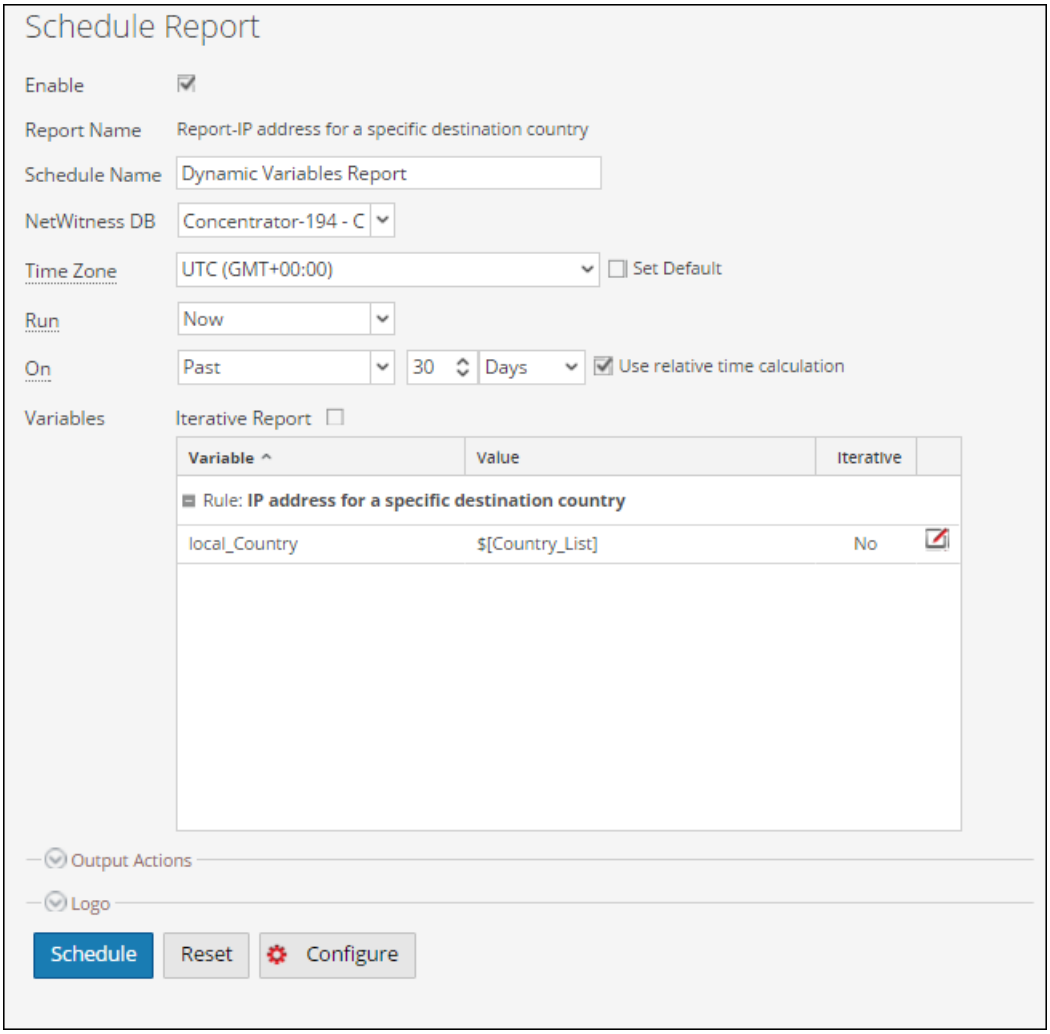
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Berichte**.

   Die Ansicht „Berichte“ wird angezeigt.

3. Klicken Sie auf der Seite **Bericht erstellen** auf + , um einen Bericht zu erstellen.

4. Fügen Sie die Regel mit der benutzerdefinierten Variable von der Registerkarte „Regeln“ hinzu.
5. Klicken Sie auf **Planen**.
   Die Registerkarte „Ansicht Bericht planen“ wird angezeigt.




6. Aktivieren Sie für die planmäßige Ausführung der Berichte das Kontrollkästchen **Aktivieren**.
7. Geben Sie im Feld **Planname** einen Namen für die geplante Berichtsplanungskonfiguration ein.
8. Wählen Sie im Feld **Datenquelle** die Datenquelle aus.

**Hinweis:** Wenn die Datenquelle nicht aufgelistet ist, stellen Sie sicher, dass Sie die **Leseberechtigung** für die Datenquelle haben. Dies gilt nur für NWDB- und Warehouse-Datenquellen. Weitere Informationen finden Sie unter „Konfigurieren von Datenquellenberechtigungen“ im *Konfigurationsleitfaden Reporting Engine*.

9. (Optional) Wählen Sie in der Drop-down-Liste **Warehouse-Ressourcenpool** die im Cluster verfügbaren Pools oder Warteschlangen aus, um den Bericht so zu planen, dass er entweder im Pool oder in der Warteschlange ausgeführt wird. Diese Drop-down-Liste steht nur zur Verfügung, wenn Sie einen Warehouse-DB-Bericht auswählen.

   **Hinweis:** Alle Warteschlangen oder Pools, die Sie auf der Seite „Durchsuchen“ für die Reporting Engine angeben, werden aufgelistet. Wenn keine Pools oder Warteschlangen auf der Seite „Durchsuchen“ konfiguriert wurden, ist diese Drop-down-Liste deaktiviert und die Jobs werden ohne Warteschlangen- oder Poolnamen an die Cluster übermittelt.

   **Hinweis:** Wenn der im Berichtsplan konfigurierte Pool bzw. die konfigurierte Warteschlange aus dem Cluster entfernt wird, bleibt der Warteschlangenname im Kapazitätsplaner undefiniert. Im Fair Scheduler wird der angegebene Poolname jedoch mithilfe der Eigenschaft `mapred.fairscheduler.allow.undeclared.pool` erstellt.

10. Wählen Sie in der Drop-down-Liste „Zeitzone“ eine Zeitzone zum Anzeigen aller zeitbezogenen Daten in einer Berichtsausgabe im angegebenen Format aus. Diese Einstellung kann über die Reporting Engine-Ansicht „Durchsuchen“ konfiguriert werden (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).

11. Wählen Sie im Feld **Ausführen** den Typ der Ausführungsplanung aus. (Beispielsweise Jetzt oder Später.) Tun Sie je nach Typ der Ausführungsplanung Folgendes:

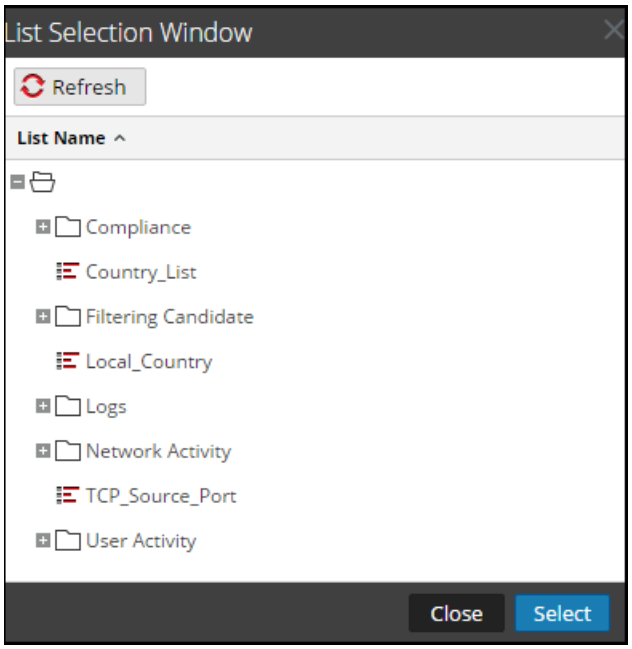
    - Wenn Sie als Ausführungsplanung **Später** oder **Monatlich** auswählen, müssen Sie im entsprechenden angegebenen Feld einen Wert für den Tag und die Uhrzeit angeben.
    - Wenn Sie als Ausführungsplanung **Stündlich** auswählen, müssen Sie die Minuten im Feld **Bei Minute** eingeben.
    - Wenn Sie als Ausführungsplanung **Täglich** auswählen, müssen Sie einen Wert für die Uhrzeit im Feld **Um** eingeben.
    - Wenn Sie als Ausführungsplanung **Wöchentlich** auswählen, müssen Sie einen Wert im Feld **Um** eingeben und auch die Wochentage auswählen.

    **Hinweis:** Wenn Sie bei der Planung eines Berichts die Option **Vergangen** oder die Option **Bereich (spezifisch/generisch)** oder einen Endzeitbereich sehr nah an der aktuellen Zeit auswählen, überprüfen Sie, ob die aggregierten Daten in der Datenquelle zurückgegeben werden. Wenn es in der Datenquelle zu einer Aggregationsverzögerung kommt, sollten Sie diese Verzögerung bei der Wahl der Endzeit berücksichtigen, andernfalls können in den Berichten für diese Zeitspanne nicht aggregierte Daten verloren gehen.

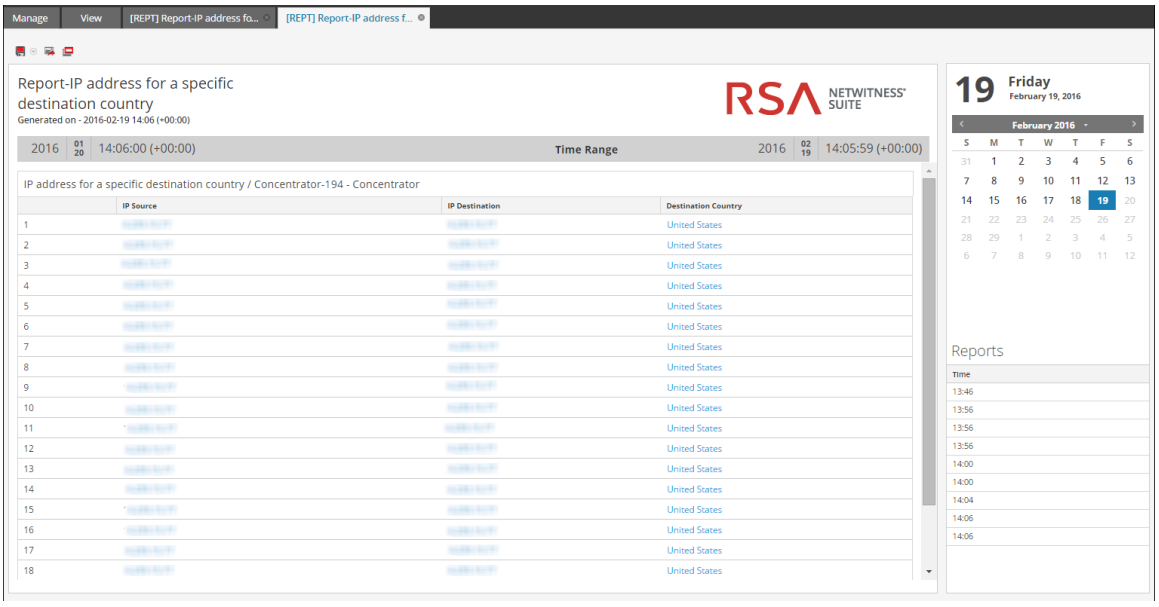
12. Klicken Sie im Feld „Variablen“ auf .

13. Führen Sie einen der folgenden Schritte aus:

- Geben Sie den Wert für die Variable ein oder
- Wählen Sie den Listenwert für die Variable aus.

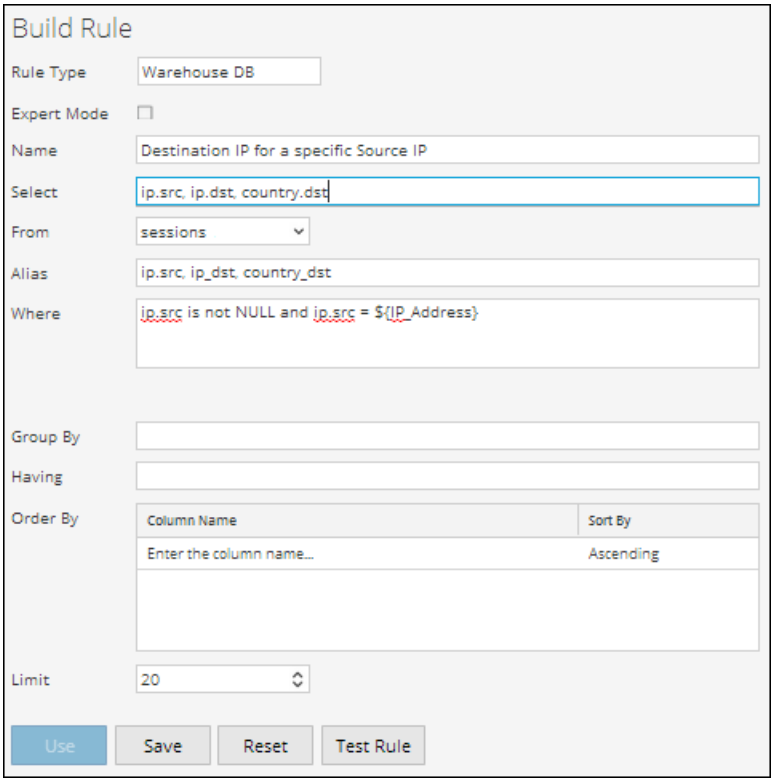



14. Klicken Sie auf **Auswählen**.
15. Klicken Sie auf **Planen**.
    Der geplante Bericht wird nach Plan ausgeführt und stellt die konfigurierten Ausgaben bereit.

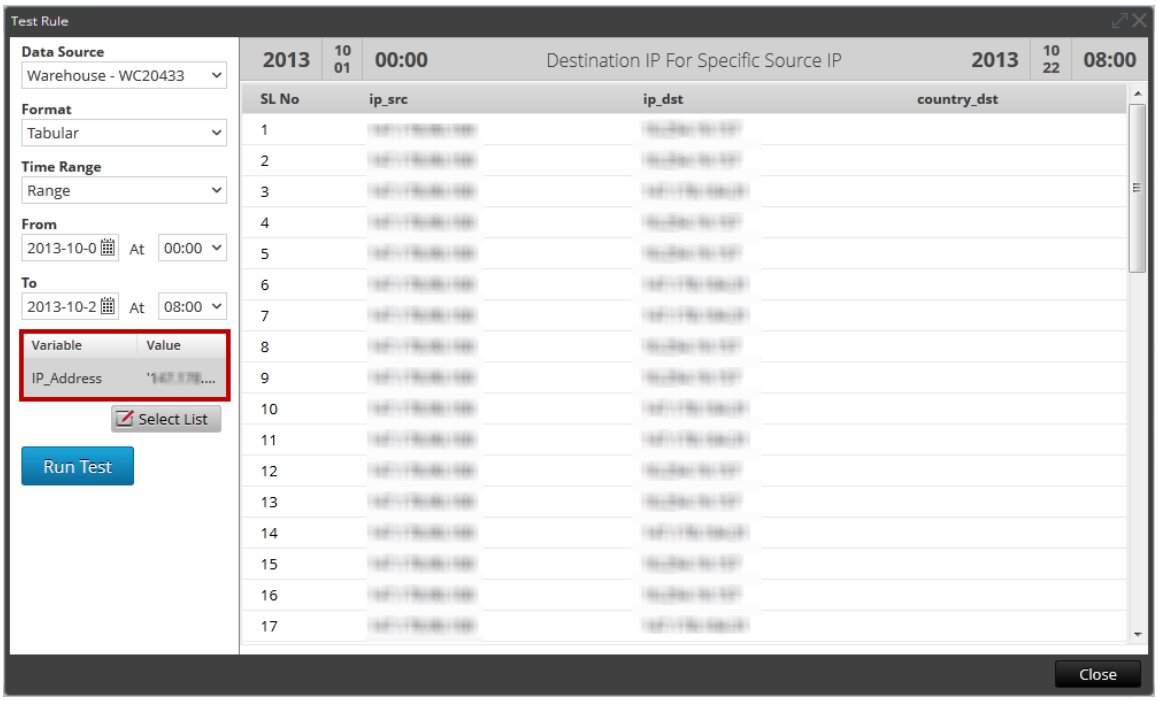



**Anzeige aller Ziel-IP-Adressen einer Quell-IP**

Es folgt ein Beispiel einer Warehouse-Regel, um alle Ziel-IP-Adressen einer bestimmten Quell-IP anzusehen. Die Quell-IP-Adresse `ip_src` ist als eine Variable `${IP_Address}` definiert.

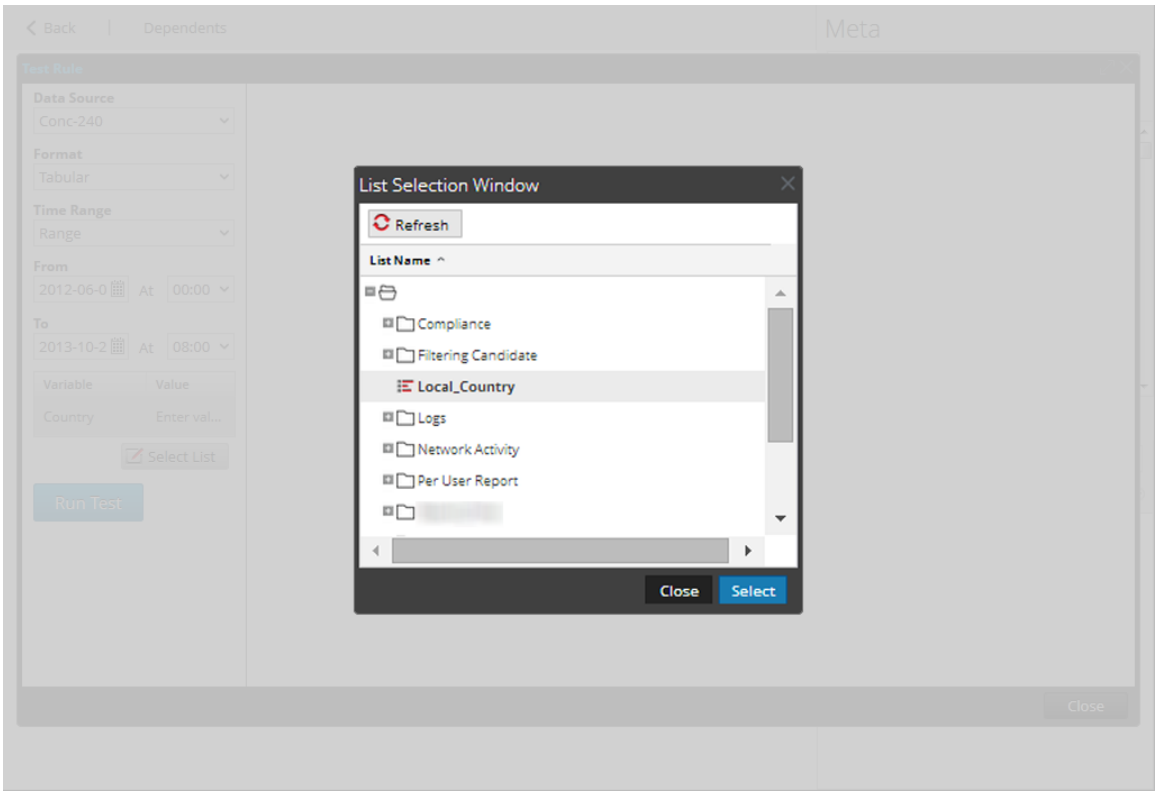



In der Laufzeit werden Sie aufgefordert, die Quell-IP-Adresse einzugeben. Die Abbildung unten zeigt die Variable `IP_Address` und Sie können eine gültige Quell-IP-Adresse eingeben. Alle Ziel-IP-Adressen mit der angegebenen Quell-IP werden aufgelistet.




### Zuordnung einer Variablen zu einer Liste von Werten

Sie können Variablen einer Liste zuordnen. Sie können zum Beispiel eine Liste mit dem Namen `Local_Country` erstellen und alle Ländernamen als Werte eingeben. Sie können die Liste `Local_Country` als Wert für die Variable `Local_Country` auswählen. Bei der Ausführungskonfiguration wird die Liste `Local_Country` ausgefüllt und Sie können das Land anhand der angezeigten Ergebnisse auswählen.




## Iterativer Bericht

Ein iterativer Bericht erzeugt einen Bericht für jeden Wert auf der Liste.

**Führen Sie die folgenden Schritte aus, um einen iterativen Bericht zu planen:**

1. Wählen Sie **Monitor** > Berichte aus.

   Die Registerkarte „Managen“ wird angezeigt.

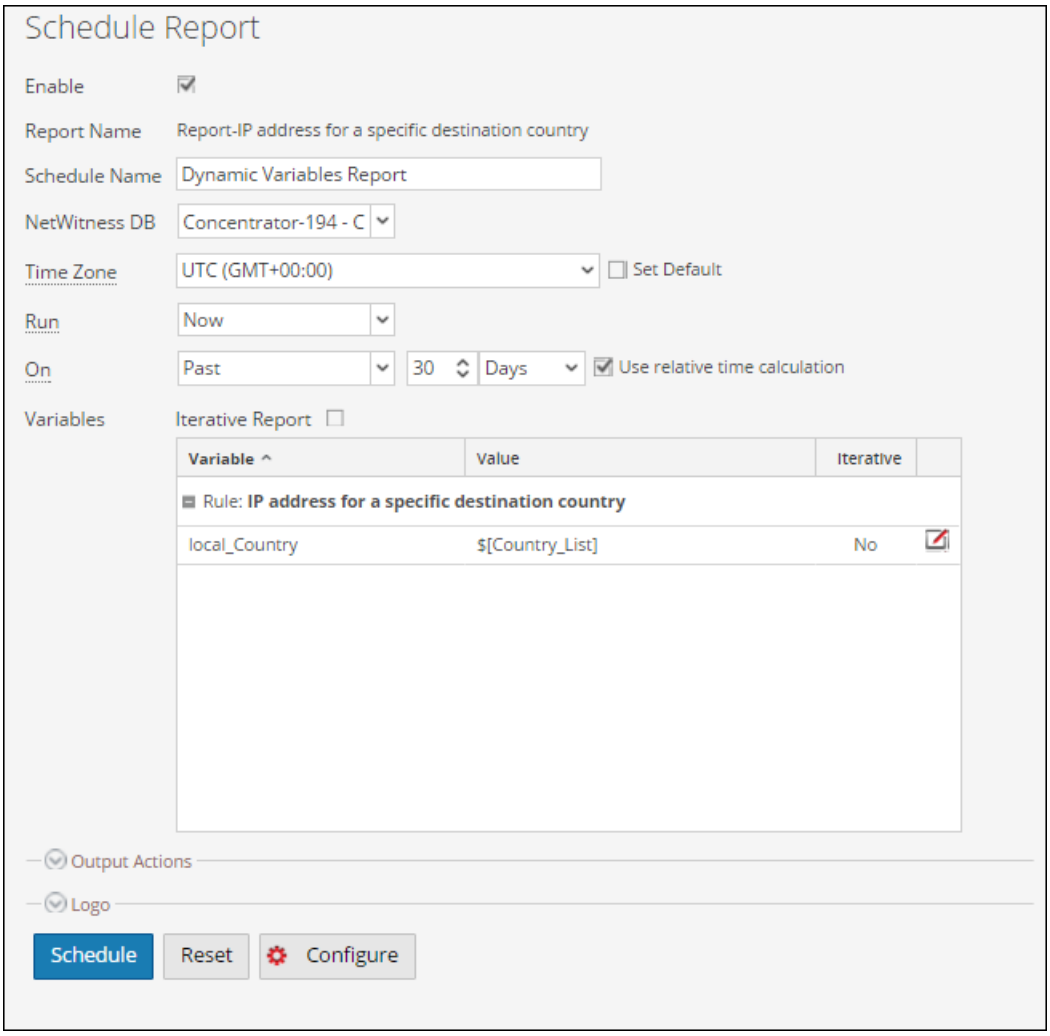
2. Klicken Sie auf **Berichte**.

   Die Ansicht „Berichte“ wird angezeigt.

3. Klicken Sie auf der Seite **Bericht erstellen** auf +, um einen Bericht zu erstellen.

4. Fügen Sie die Regel mit der benutzerdefinierten Variable von der Registerkarte „Regeln“ hinzu.

5. Klicken Sie auf **Planen**.
   Die Registerkarte „Ansicht Bericht planen“ wird angezeigt.




6. Aktivieren Sie für die planmäßige Ausführung der Berichte das Kontrollkästchen **Aktivieren**.
7. Geben Sie im Feld **Planname** einen Namen für die geplante Berichtsplanungskonfiguration ein.
8. Wählen Sie im Feld **Datenquelle** die Datenquelle aus.

   **Hinweis:** Wenn die Datenquelle nicht aufgelistet ist, stellen Sie sicher, dass Sie die **Leseberechtigung** für die Datenquelle haben. Dies gilt nur für NWDB- und Warehouse-Datenquellen. Weitere Informationen finden Sie unter „Konfigurieren von Datenquellenberechtigungen“ im *Konfigurationsleitfaden Reporting Engine*.
9. (Optional) Wählen Sie in der Drop-down-Liste **Warehouse-Ressourcenpool** die im Cluster verfügbaren Pools oder Warteschlangen aus, um den Bericht so zu planen, dass er entweder im Pool oder in der Warteschlange ausgeführt wird. Diese Drop-down-Liste steht nur zur Verfügung, wenn Sie einen Warehouse-DB-Bericht auswählen.

**Hinweis:** Alle Warteschlangen oder Pools, die Sie auf der Seite „Durchsuchen“ für die Reporting Engine angeben, werden aufgelistet. Wenn keine Pools oder Warteschlangen auf der Seite „Durchsuchen“ konfiguriert wurden, ist diese Drop-down-Liste deaktiviert und die Jobs werden ohne Warteschlangen- oder Poolnamen an die Cluster übermittelt.

**Hinweis:** Wenn der im Berichtsplan konfigurierte Pool bzw. die konfigurierte Warteschlange aus dem Cluster entfernt wird, bleibt der Warteschlangenname im Kapazitätsplaner undefiniert. Im Fair Scheduler wird der angegebene Poolname jedoch mithilfe der Eigenschaft `mapred.fairscheduler.allow.undeclared.pool` erstellt.

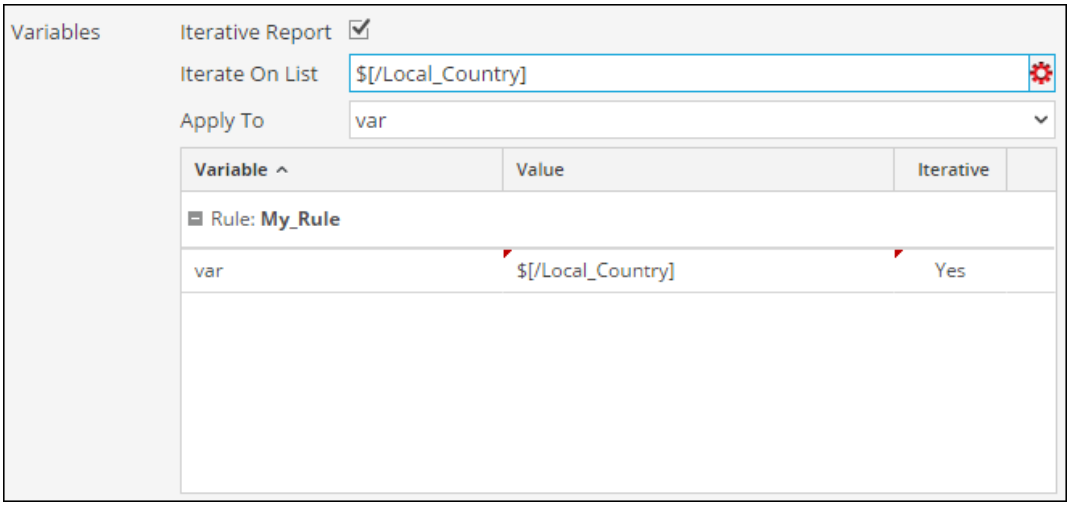
10. Wählen Sie in der Drop-down-Liste „Zeitzone“ eine Zeitzone zum Anzeigen aller zeitbezogenen Daten in einer Berichtsausgabe im angegebenen Format aus. Diese Einstellung kann über die Reporting Engine-Ansicht „Durchsuchen“ konfiguriert werden (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. Wählen Sie im Feld **Ausführen** den Typ der Ausführungsplanung aus. (Beispielsweise Jetzt oder Später.) Tun Sie je nach Typ der Ausführungsplanung Folgendes:
    - Wenn Sie als Ausführungsplanung **Später** oder **Monatlich** auswählen, müssen Sie im entsprechenden angegebenen Feld einen Wert für den Tag und die Uhrzeit angeben.
    - Wenn Sie als Ausführungsplanung **Stündlich** auswählen, müssen Sie die Minuten im Feld **Bei Minute** eingeben.
    - Wenn Sie als Ausführungsplanung **Täglich** auswählen, müssen Sie einen Wert für die Uhrzeit im Feld **Um** eingeben.
    - Wenn Sie als Ausführungsplanung **Wöchentlich** auswählen, müssen Sie einen Wert im Feld **Um** eingeben und auch die Wochentage auswählen.

    **Hinweis:** Wenn Sie bei der Planung eines Berichts die Option **Vergangen** oder die Option **Bereich (spezifisch/generisch)** oder einen Endzeitbereich sehr nah an der aktuellen Zeit auswählen, überprüfen Sie, ob die aggregierten Daten in der Datenquelle zurückgegeben werden. Wenn es in der Datenquelle zu einer Aggregationsverzögerung kommt, sollten Sie diese Verzögerung bei der Wahl der Endzeit berücksichtigen, andernfalls können in den Berichten für diese Zeitspanne nicht aggregierte Daten verloren gehen.
12. Führen Sie im Feld „Variable“ die folgenden Schritte aus:
    a. Um iterative Berichte auszuführen, aktivieren Sie das Kontrollkästchen **Iterativer Bericht**.
    b. Wenn Sie eine eine Iteration für den Listenwert durchführen möchten, klicken Sie auf  .

       Das Listenauswahlfenster wird geöffnet.
    c. Wählen Sie eine Liste aus und klicken Sie auf **Auswählen**.

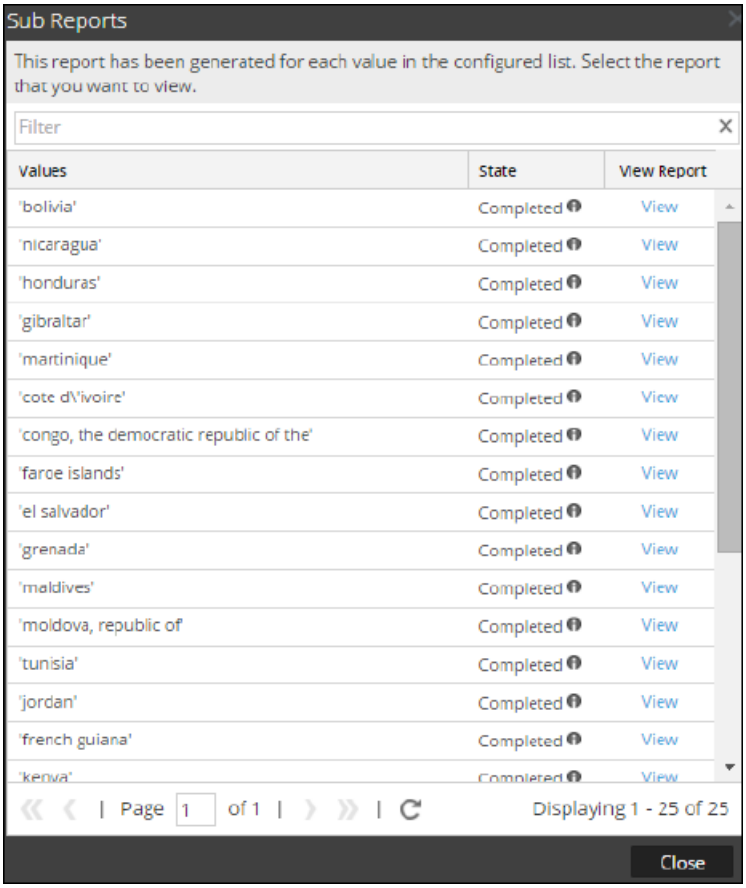
Das ausgewählte Listenelement wird zum Feld **Liste iterieren** hinzugefügt.

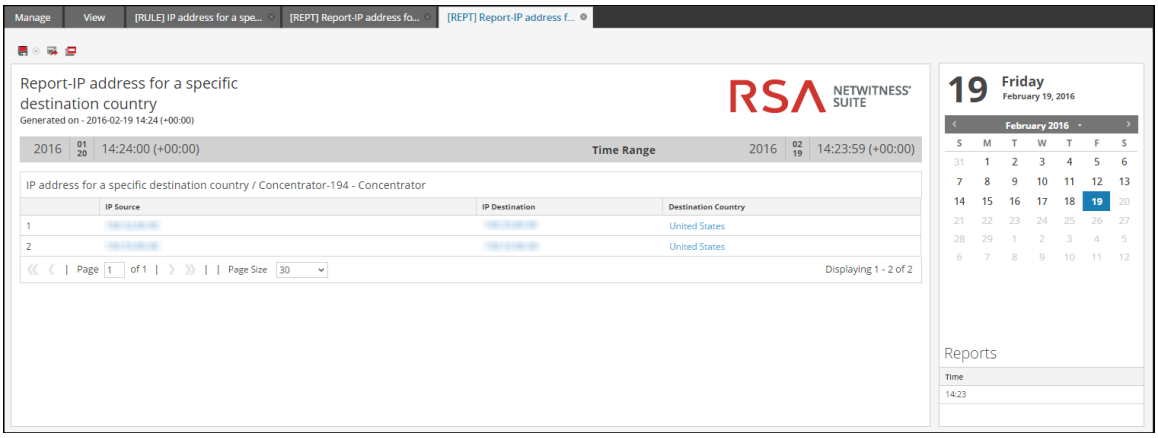
d. Wählen Sie die auf den ausgewählten Listenwert anzuwendende Variable aus.




13. Klicken Sie auf **Planen**.
Der geplante Bericht wird nach Plan ausgeführt und stellt die konfigurierten Ausgaben bereit.

Die folgende Abbildung zeigt die Ansicht „Iterative Berichte“.






## Erstellen eines Berichts mit einer Regel

Sie können einen Bericht mit einer Regel erstellen. Wenn Sie einen Bericht mithilfe einer Regel erstellen, wird ein Standardbericht mit dieser einzigen Regel erstellt. Sie können den Bericht weitergehend bearbeiten, um weitere Regeln hinzuzufügen.

### Führen Sie die folgenden Schritte aus, um einen Bericht mithilfe einer Regel zu erstellen:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - Sie können einen Bericht mithilfe einer Regel erstellefn, wenn Sie die Regel erstellen oder bearbeiten. Führen Sie folgende Schritte durch:
     a. Klicken Sie in der Ansicht **Regel erstellen** auf **Verwenden**.
        Das Dialogfeld Regel verwenden wird angezeigt.
     b. Klicken Sie auf **Bericht**.
     c. Wählen Sie **Neuer Bericht** oder **Vorhandener Bericht** anhand Ihrer Anforderungen aus.
     d. Klicken Sie auf **Auswählen**.
   - Wählen Sie im Bereich „Regelliste“ eine Regel aus und klicken Sie in der Symbolleiste „Regel“ auf  . Wählen Sie im Drop-down-Menü **Verwenden** > **Bericht** aus.
   - Klicken Sie im Bereich „Regelliste“ auf  > **Bericht erstellen**.

**Hinweis:** Zum Erstellen eines Berichts können Sie benutzerdefinierte Regeln verwenden und wenn Sie die Ansicht „Bereich“ oder „Kreis“ für die Regel ausgewählt haben, wird ein Fenster für die Eingabe der **X-Achse** und der **Y-Achse** eingeblendet. Standardmäßig können Sie nur die ersten Metadaten für die **X-Achse** auswählen.

# Anzeigen eines Berichts

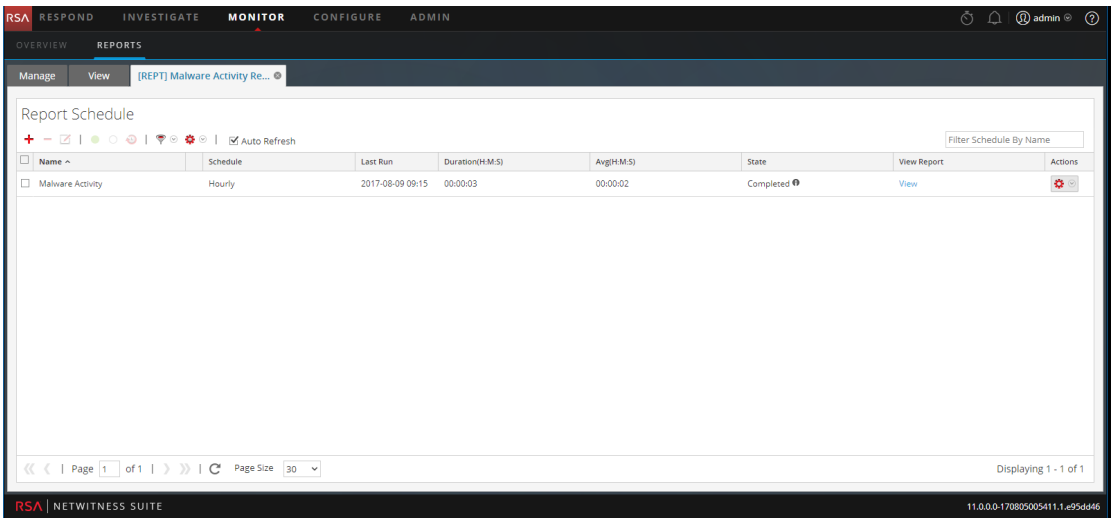
Sie können einen Bericht oder eine Liste aller Berichte anzeigen. Sie können auch die geplanten Berichte anzeigen, um deren Status zu erfahren. Wenn ein geplanter Bericht einen beendeten oder deaktivierten Status aufweist, können Sie den Bericht starten oder aktivieren.

Nach dem Anzeigen eines Berichts können Sie eine der folgenden Aufgaben ausführen:

1. Sie können Berichte ausdrucken, speichern, per E-Mail versenden und auf dem ganzen Bildschirm anzeigen.
2. Sie können außerdem im Kalender ein Datum auszuwählen, um eine Liste der erfolgreich ausgeführten Berichte für das ausgewählte Datum anzuzeigen.

### Führen Sie die folgenden Schritte aus, um einen Bericht anzuzeigen:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie im Bereich **Berichtsliste** auf  > **Geplante Berichte anzeigen**.
4. Klicken Sie auf die Spalte **#Planungen**.
   Die Registerkarte „Ansicht Geplante Berichte“ wird mit dem Status jedes geplanten Berichts angezeigt.




5. Wählen Sie einen geplanten Bericht aus und klicken Sie auf **Anzeigen**.
   Eine der folgenden Optionen wird angezeigt:

- Der ausgewählte Bericht.
- Bei geplanten Berichten, für die Iterativ ausgewählt ist, wird der Bereich Unterberichte angezeigt.

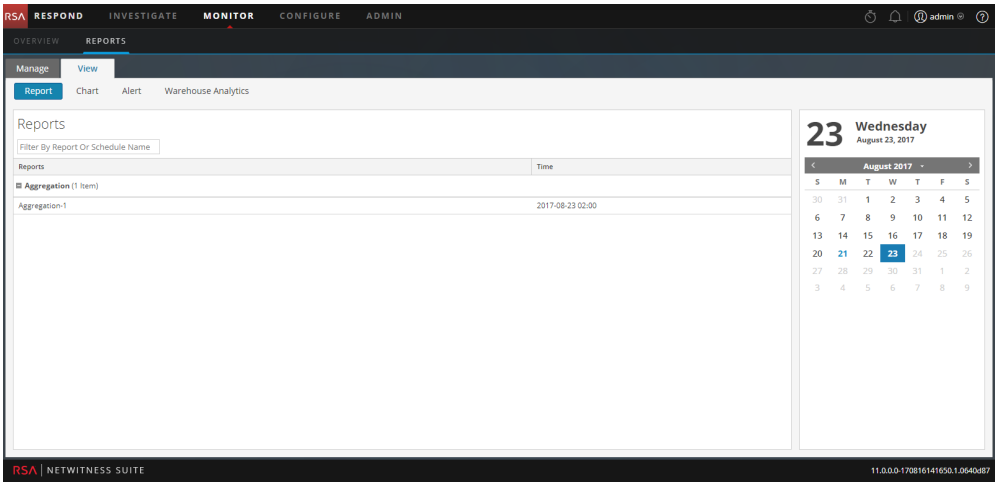
Für jeden Wert in der konfigurierten Liste wird ein Bericht angezeigt.

> **Hinweis:** Wenn der Berichtsstatus teilweise oder ganz abgeschlossen ist, werden die Felder „Zeitstempel letzte Ausführung“ und „letzte Ausführung (Sekunden)“ aktualisiert. Allerdings wird die durchschnittliche Dauer der Ausführung des Berichts nur dann aktualisiert, wenn der Berichtsstatus abgeschlossen ist, nicht wenn er nur teilweise abgeschlossen ist.

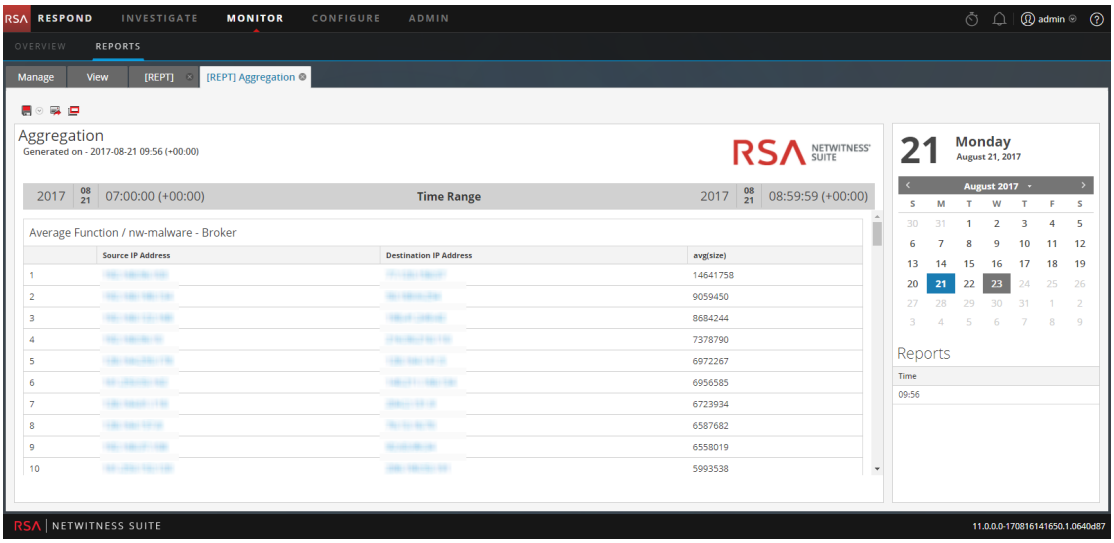
### Führen Sie die folgenden Schritte durch, um eine Liste aller Berichte anzuzeigen:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte **Managen** wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie im Bereich **Bericht** auf **Alle Berichte anzeigen**.
   Ein Liste von Berichten zusammen mit ihren Namen und ihrem Ausführungstermin wird auf der Registerkarte „Ansicht“ angezeigt.

> **Hinweis:** Wenn keine Liste angezeigt wird, wählen Sie ein Datum im Kalender aus, um eine Liste von Berichten für dieses Datum anzuzeigen.




4. Sie können einen geplanten Bericht auswählen und drucken, als PDF/CSV speichern, als E-Mail-Benachrichtigung versenden oder ihn im Vollbildmodus anzeigen.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
OVERVIEW
REPORTS
Manage
View
[REPT]
[REPT] Aggregation
Aggregation
Generated on - 2017-08-21 09:56 (+00:00)
RSA NETWITNESS SUITE
2017 08 21 07:00:00 (+00:00)
Time Range
2017 08 21 08:59:59 (+00:00)
Average Function / nw-malware - Broker
Source IP Address
Destination IP Address
avg(size)
1 14641758
2 9059450
3 8684244
4 7378790
5 6972267
6 6956585
7 6723934
8 6587682
9 6558019
10 5993538
21 Monday
August 21, 2017
August 2017
S M T W T F S
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9
Reports
Time
09:56
RSA | NETWITNESS SUITE
11.0.0.0-170816141650.1.0640d87

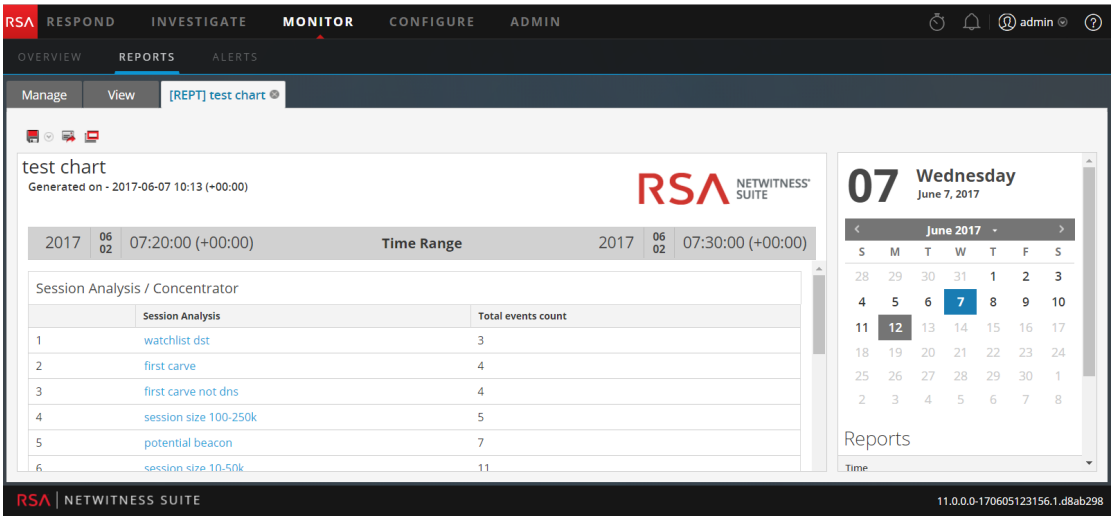
# Untersuchen eines Berichts

Sie können einen Bericht untersuchen, indem Sie im Bericht direkt zur Ansicht „Investigation“ navigieren. Mit der Option „Untersuchen eines Berichts“ können Sie jedes Ereignis untersuchen, das im Bericht erwähnt wird.

### Führen Sie die folgenden Schritte aus, um einen Bericht zu untersuchen:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie in der Symbolleiste **Bericht** auf **Alle Berichte anzeigen**.
   Die Registerkarte „Alle Berichte anzeigen“ wird angezeigt.

   **Hinweis:** Wenn auf der Registerkarte „Alle Berichte anzeigen“ keine Berichte angezeigt werden, wählen Sie ein Datum aus, für das Sie die Berichte anzeigen möchten.
4. Doppelklicken Sie auf den Namen des Berichts, um die Details anzuzeigen.
   Der Bildschirm „Berichtsdetails“ wird angezeigt.




   Klicken Sie auf die Sitzungsanalyse, um den Bericht zu untersuchen.

**Hinweis:** Wenn Sie die Ergebnisdaten manuell kopieren und für Ermittlungen nutzen möchten, stellen Sie sicher, dass Sie den Binärwerten das Präfix „hex:“ voranstellen.

# Managen von Listen, Regeln oder Berichten

Sie können Zugriffskontrollen festlegen und Listen, Regeln oder Berichte löschen, bearbeiten, importieren oder exportieren.

## Managen von Listen

### Zugriffskontrolle für Listen und Listengruppen

Sie können die Zugriffsberechtigungen für die Benutzerrollen zum Managen von Listen oder Listengruppen einrichten. Das Reporting bietet Zugriffskontrolle auf Listen- und Listengruppenlevel. Nur ein Benutzer mit den richtigen Berechtigungen kann die Aufgaben im Reporting durchführen. Die Zugriffskontrolle wird vom Administrator in der Registerkarte **ADMIN > Sicherheit > Rollen** gemanagt.

Als Administrator müssen Sie darauf achten, dass die für bestimmte Aufgaben erstellten Rollen über alle in der Rollenhierarchie höher angesiedelten Zugriffsberechtigungen verfügen.

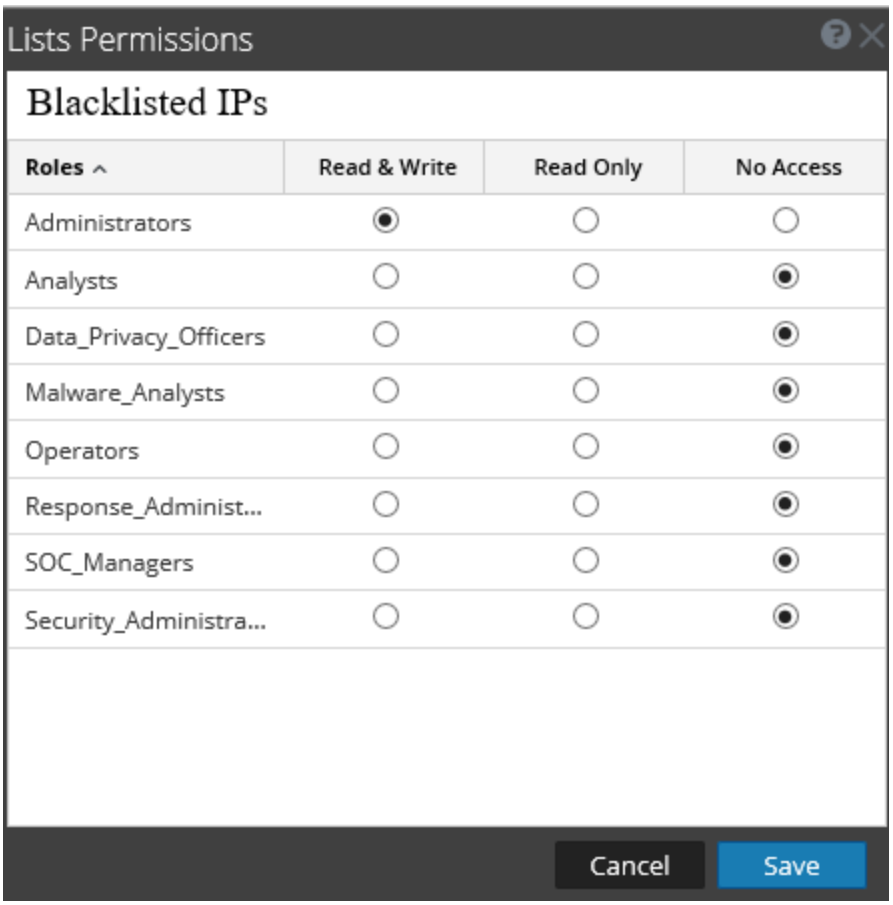
Listen oder Listengruppen können einem bestimmten Satz von Benutzerrollen zugewiesen werden. Wenn Benutzer sich bei NetWitness Suite anmelden, können sie nur auf diejenigen Listen zugreifen, zu denen sie gehören. Benutzer, die einer Benutzerrolle mit der Zugriffsberechtigung **Lesen und Schreiben** angehören, haben volle Zugriffsrechte für die Listen. Der Zugriff auf Listen kann auch eingeschränkt werden, sodass er nur mit der Berechtigung **Schreibgeschützt** möglich ist.

**Hinweis:** Sie müssen mindestens die Zugriffsberechtigung **Schreibgeschützt** für eine Liste haben, um die Listen innerhalb dieser Gruppe anzeigen zu können.

Wenn Sie beispielsweise möchten, dass die **Sicherheitsanalysten** Zugriff auf alle Listen in einer Listengruppe haben, dann können Sie die Berechtigung **Lesen und Schreiben** auf dem Listengruppenlevel einstellen. Und wenn Sie nicht möchten, dass die Rolle **Operator** Zugriff auf bestimmte Listen in einer Listengruppe hat, können Sie die Berechtigung **Kein Zugriff** auf dem Listengruppenlevel einstellen.

Auf Listen- oder Listengruppenebene können Sie folgende Zugriffsberechtigungen für die Benutzerrollen in NetWitness Suite festlegen: Weitere Informationen finden Sie unter Listenansicht.

- Lesen & Schreiben
- Schreibgeschützt
- Kein Zugriff




Die folgende Tabelle listet die verschiedenen Spalten im Bereich „Listenberechtigungen“ auf:

| Spalte | Beschreibung |
|---|---|
| Rollen | Beschreibt die Rollen der Benutzer, die bei der NetWitness Suite-Benutzeroberfläche angemeldet sind. |
| Lesen & Schreiben | Der Benutzer kann in der Listenansicht auf Listen zugreifen, sie anzeigen, bearbeiten, löschen, importieren und exportieren. Der Benutzer kann auch die Berechtigungen für die Regel ändern. |
| Schreibgeschützt | Der Benutzer kann in der Listenansicht nur auf die Liste zugreifen und sie anzeigen. |
| Kein Zugriff | Ermöglicht es Benutzern nicht, Listen aufzurufen oder anzuzeigen. |

## Zugriffskontrolle für eine Liste

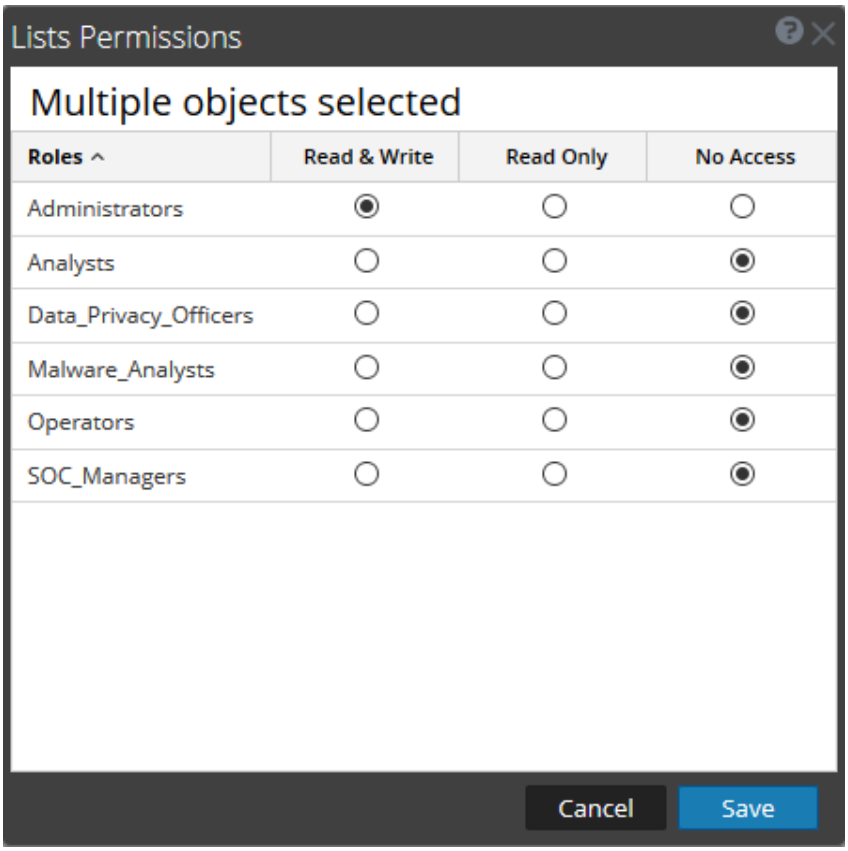
Um die Listenberechtigungen zu ändern, müssen Sie eine Liste auswählen und mithilfe des Bereichs Listenberechtigungen ihre Zugriffsberechtigungen ändern.

Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie diese auf dem Listenlevel festlegen. Bevor Jobberechtigungen festgelegt werden, lautet der festgelegte Standardberechtigungssatz für alle Benutzerrollen außer Administratoren **Kein Zugriff**.

## Festlegen von Zugriffskontrollen für mehrere Listen

Sie können mehrere Listen gleichzeitig auswählen und über den Bereich „Listenberechtigungen“ Zugriffsberechtigungen festlegen. Die Zugriffsberechtigung, die Sie auswählen, wird auf alle ausgewählten Listen angewendet.

**Hinweis: *** neben dem Rollennamen zeigt die anderen Berechtigungen an, die für diese Benutzerrolle verfügbar sind. Wenn Sie die Zugriffsberechtigung für die erforderliche Benutzerrolle ändern möchten, wählen Sie die Benutzerrolle aus und ändern Sie die Zugriffsberechtigung.



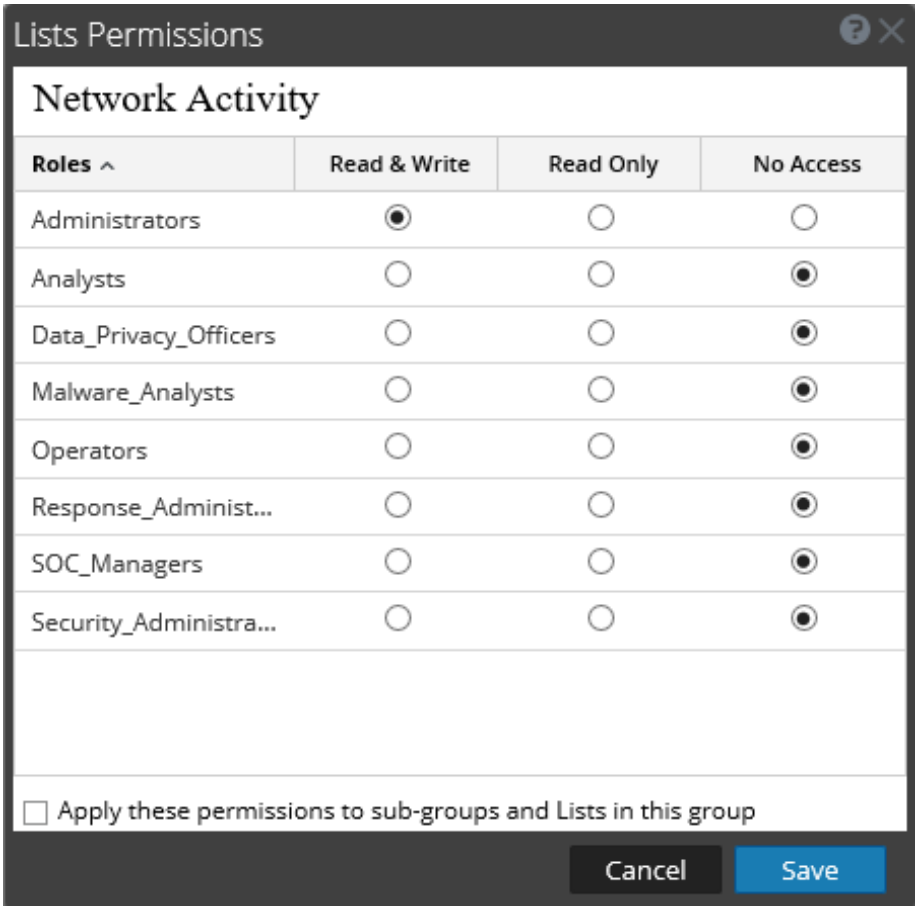

**Hinweis:** Wenn ein Benutzer (der nicht ADMIN ist) eine Liste erstellt, kann ADMIN auf diese Liste nicht zugreifen.

## Zugriffskontrolle für eine Listengruppe

Um die Berechtigungen der Listengruppe zu ändern, müssen Sie eine Listengruppe auswählen und ihre Zugriffsberechtigungen über den Bereich Listenberechtigungen einstellen.

Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie diese auf dem Listengruppenlevel festlegen. Bevor Jobberechtigungen festgelegt werden, lautet der festgelegte Standardberechtigungssatz für alle Benutzerrollen außer Administratoren **Kein Zugriff**.

Zudem können Sie Berechtigungen auf Untergruppen und Regeln einer Gruppe anwenden, indem Sie das Kontrollkästchen aktivieren.




Die folgenden Szenarien beschrieben das Definieren von Berechtigungen für Listengruppen oder -untergruppen und Listen in den Gruppen:

- Szenario 1: Berechtigungen werden basierend auf der Benutzerrolle auf eine Listengruppe bzw. -untergruppe angewendet.

  Jede Ebene erhält abhängig von der Benutzerrolle einen Berechtigungssatz. Wenn einer Listengruppe beispielswiese die Rolle eines Sicherheitsanalysten zugewiesen wird, werden die Berechtigungen für die Listengruppe auf „Lesen und Schreiben“ festgelegt.

- Szenario 2: Berechtigungen werden auf Untergruppen und Listen in der Gruppe angewendet.
  Die von Ihnen festgelegten Zugriffsberechtigungen können auf alle Untergruppen und untergeordneten Objekte dieser Gruppe angewendet werden. Die Berechtigungen auf Listengruppenlevel werden von den Untergruppen und den Listen in der Gruppe übernommen.

| Rolle (Analysten) | Berechtigungen angewendet auf eine Listengruppe bzw. -untergruppe, basierend auf der Benutzerrolle | Berechtigungen angewendet auf eine Untergruppe und Listen in der Gruppe |
|---|---|---|
| Gruppe | Lesen & Schreiben | Lesen & Schreiben |
| Untergruppe | Lesen | Lesen & Schreiben – übernommen |
| Listen | Lesen | Lesen und Schreiben – übernommen |

## Zugriffsberechtigungen für Listen oder Listengruppen

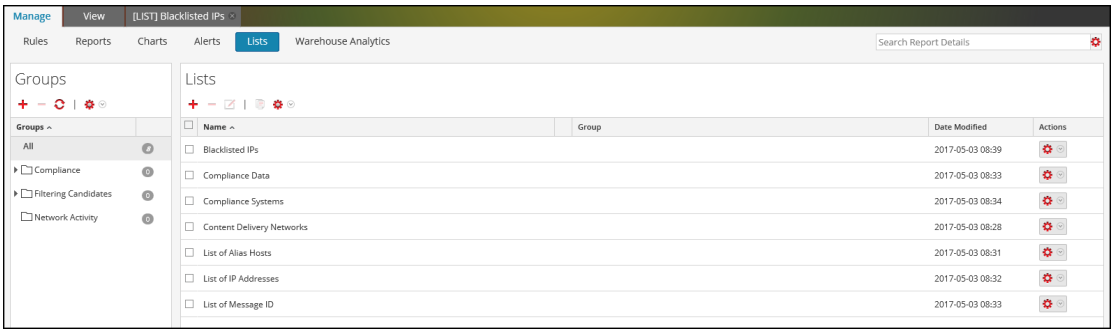
Stellen Sie sicher, dass Sie zumindest die Zugriffsberechtigung **Lesen und Schreiben** haben, sodass Sie Zugriffsberechtigungen für Listen oder Listengruppen festlegen können.

### Um Zugriffsberechtigungen für eine Liste festzulegen, führen Sie die folgenden Schritte durch:

1. Wählen Sie **Monitor** > **Berichte** aus.

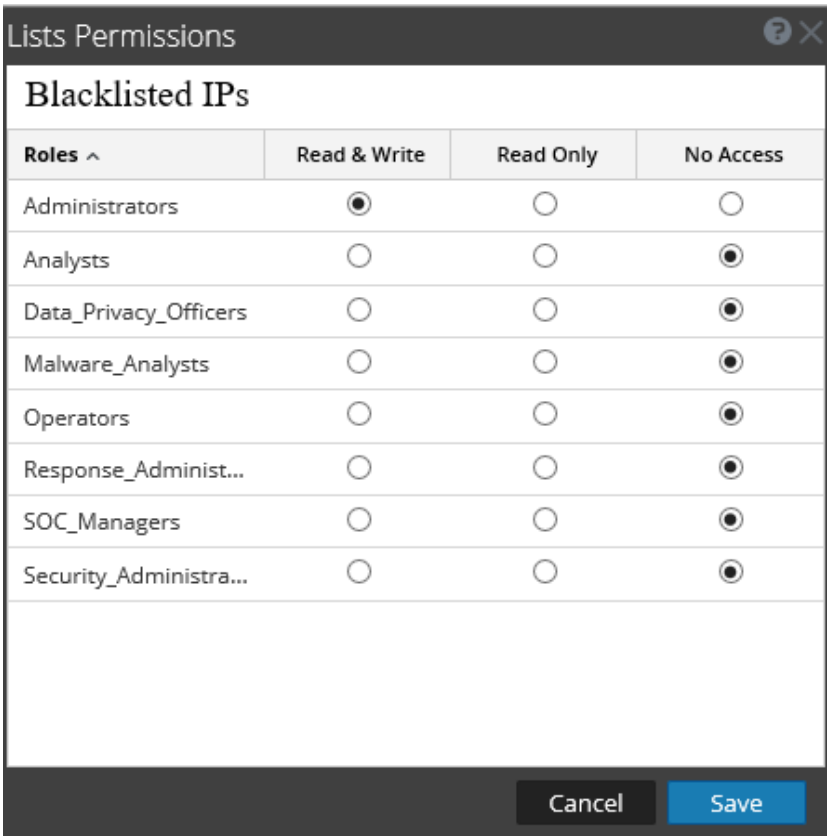
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Wählen Sie im Bereich **Listenansicht** eine Liste aus.

4. Klicken Sie in der Listensymbolleiste auf  > **Berechtigungen**.
   Das Dialogfeld „Listenberechtigungen“ wird angezeigt.




5. Wählen Sie die entsprechende Zugriffsberechtigung für jede der Benutzerrollen aus und klicken Sie auf **Speichern**.

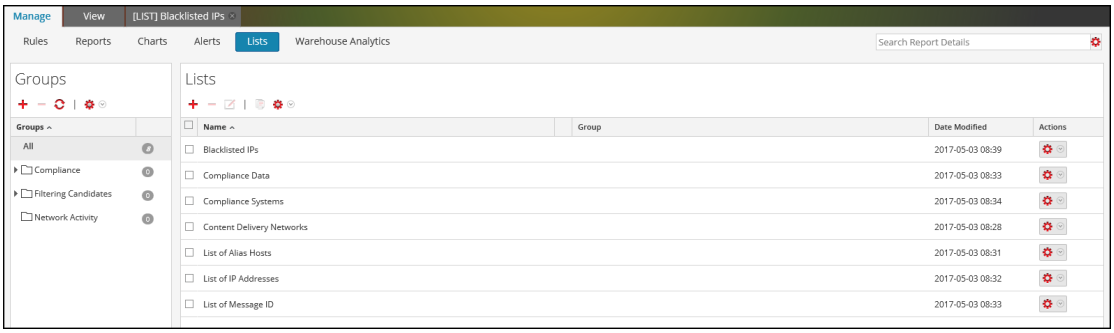
   Es wird eine Bestätigungsmeldung mit der Nachricht angezeigt, dass die Berechtigung für die ausgewählte Liste festgelegt wurde.

### Um die Zugriffskontrolle für eine Listengruppe festzulegen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.

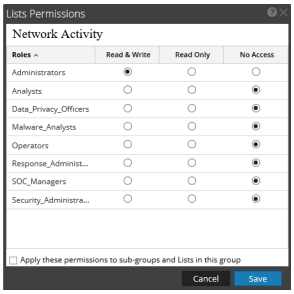
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Wählen Sie im Bereich **Listengruppen** eine Listengruppe aus.

4. Klicken Sie auf  > **Berechtigungen**.
   Das Dialogfeld „Listenberechtigungen“ wird angezeigt.




5. (Optional) Aktivieren Sie das entsprechende Kontrollkästchen, um diese Berechtigungen auf Untergruppen und untergeordnete Objekte in dieser Gruppe anzuwenden.

6. Klicken Sie auf **Speichern**.

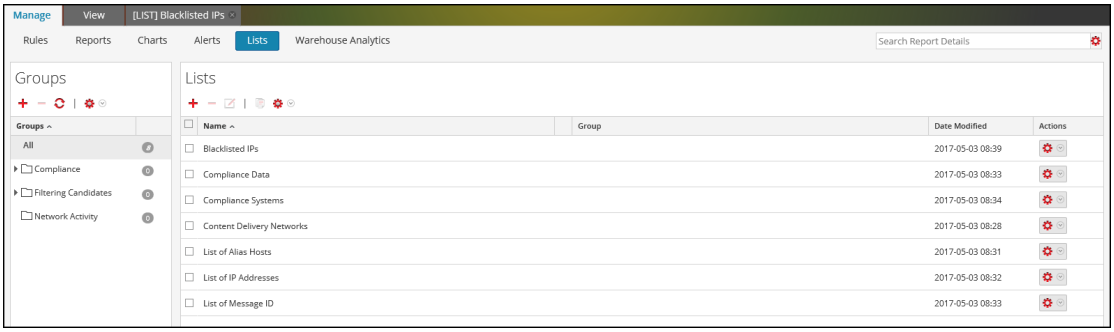
   In einer Meldung wird bestätigt, dass die Berechtigung für die ausgewählte Listengruppe erfolgreich festgelegt wurde.

## Bearbeiten einer Liste

Um eine Liste zu bearbeiten, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Wählen Sie im Bereich **Listenansicht** eine Liste aus, die Sie bearbeiten möchten, und führen Sie einen der folgenden Schritte aus.

   - Klicken Sie in der Symbolleiste der Liste auf  .
   - Klicken Sie im Bereich „Listenansicht“ auf  > **Bearbeiten**.

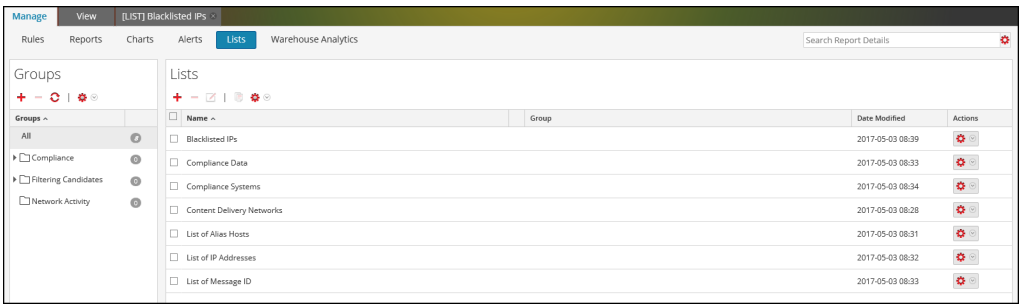
   **Hinweis:** Sie können jeweils nur eine Liste bearbeiten.

4. Bearbeiten Sie die obligatorischen Felder und fügen Sie der Liste neue Werte hinzu.
5. Klicken Sie auf **Speichern**.
   Eine Bestätigungsmeldung, dass die Liste erfolgreich gespeichert wurde, wird angezeigt.

## Löschen einer Liste oder Listengruppe

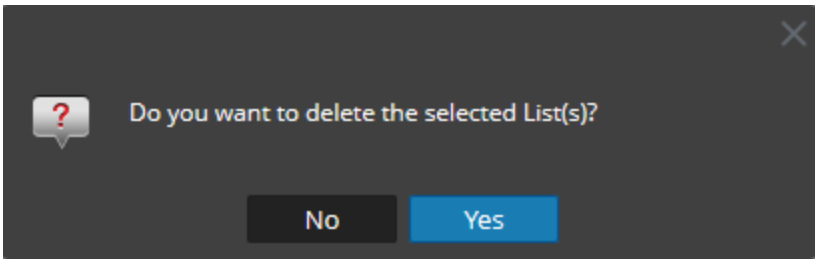
### Um eine Liste zu löschen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.



3. Führen Sie im Bereich **Listenansicht** einen der folgenden Schritte aus:

   - Wählen Sie eine oder mehrere der zu löschenden Listen aus und klicken Sie auf in der Symbolleiste der **Liste**.
   - Klicken Sie in der Spalte **Aktionen** auf > **Löschen**.
     Ein Bestätigungsdialogfeld wird angezeigt.

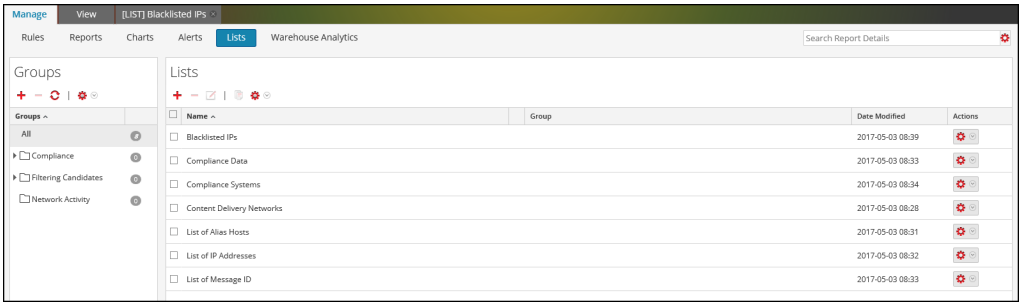



**Hinweis:** Vergewissern Sie sich vor dem Löschen einer Liste, dass diese nicht mit einer Regel verknüpft ist.

4. Klicken Sie auf **Ja**, um die Liste zu löschen.
   In einer Bestätigungsmeldung wird angezeigt, dass die Liste gelöscht wurde, und die ausgewählte Liste wird aus dem Bereich „Listenansicht“ gelöscht.

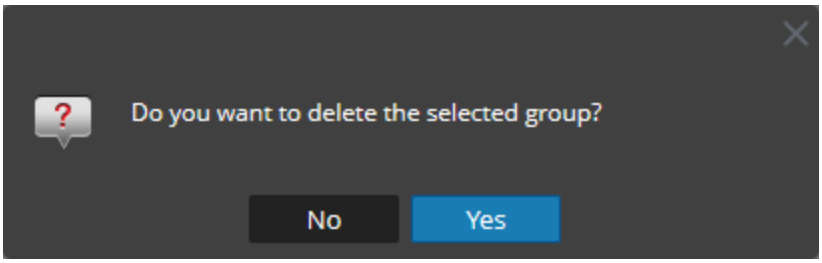
### Um eine Listengruppe zu löschen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.



3. Wählen Sie im Bereich **Listengruppen** die Gruppe aus und klicken Sie auf .

   Ein Bestätigungsdialogfeld wird angezeigt.




> **Achtung:** Wenn Sie eine Gruppe löschen, werden alle Untergruppen und Listen in dieser Gruppe gelöscht.

4. Klicken Sie auf **Ja**, um die ausgewählte Gruppe zu löschen.

> **Hinweis:** Wenn Sie versuchen, eine Listengruppe zu löschen, auf deren Listen in einer Regel oder einer Warnmeldung Bezug genommen wird, wird eine entsprechende Meldung angezeigt.

## Duplizieren einer Liste

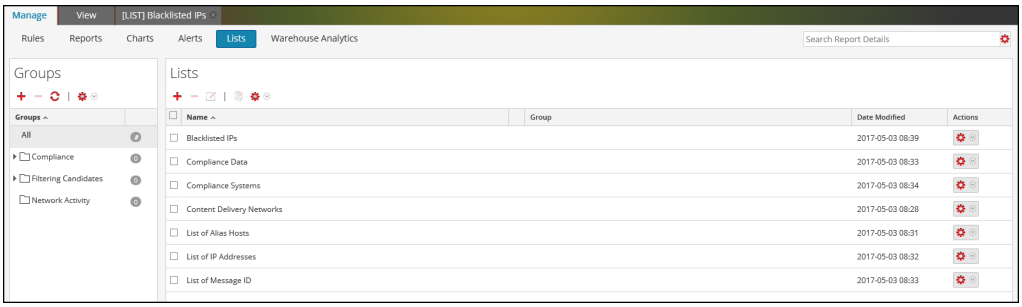
### Um eine Liste zu deduplizieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.

   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Listen**.

   Die Listenansicht wird angezeigt.




3. Wählen Sie im Bereich **Listenansicht** eine Liste aus, die Sie duplizieren möchten.

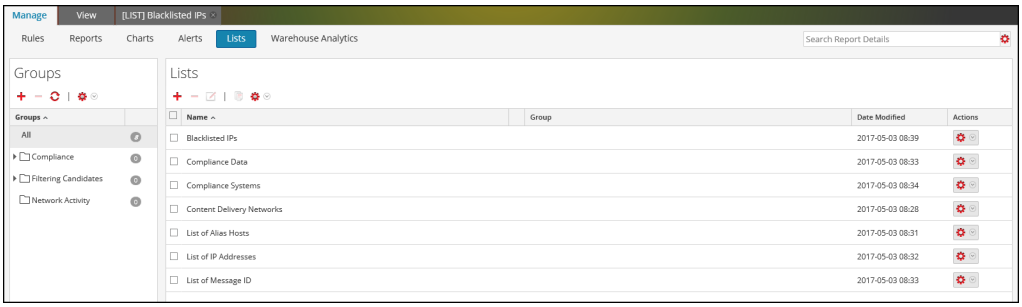
> **Hinweis:** Sie können nur jeweils eine Liste duplizieren.

4. Klicken Sie in der Symbolleiste **Liste** auf .

## Exportieren einer Liste oder Listengruppe

### Um eine Liste zu exportieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Führen Sie im Bereich **Listenansicht** einen der folgenden Schritte aus:
   - Wählen Sie eine Liste aus und klicken Sie in der Symbolleiste der Liste auf  > **Exportieren**.
   - Klicken Sie in der Spalte **Aktionen** auf  > **Exportieren**.

   Sie können mehrere Listen gleichzeitig exportieren. Um mehrere Listen auszuwählen, aktivieren Sie das Kontrollkästchen für die Listen, die exportiert werden sollen. Eventuell wird ein browserspezifisches Exportdialogfeld angezeigt, in dem Sie die Datei öffnen oder speichern können.

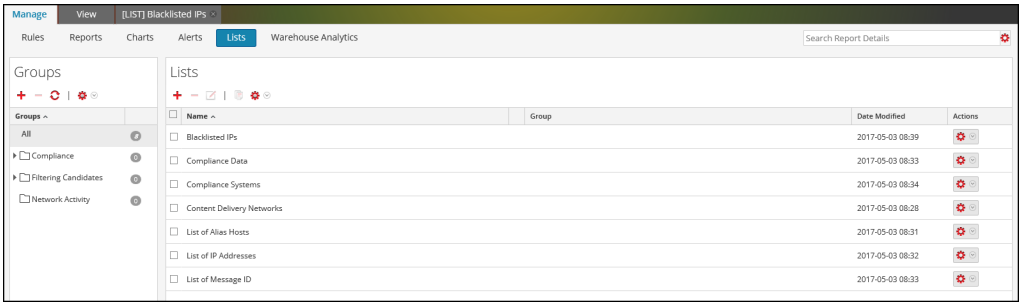
   **Hinweis:** Sie können jeweils immer nur eine Liste exportieren.

### Um eine Listengruppe zu exportieren, führen Sie die folgenden Schritte aus:

Sie können ausgewählte Listengruppen in eine externe Datei exportieren, die später in NetWitness Suite importiert werden kann. Wenn im Bereich „Listenbibliothek“ keine Liste ausgewählt wurde, dann wird die gesamte Listenstruktur exportiert. Das Ergebnis des Exports ist eine einzelne Exportdatei im Binärformat.

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Wählen Sie im Bereich **Listengruppen** die Listengruppe mit den zu exportierenden Listen aus.

4. Klicken Sie auf  > **Exportieren**.
   Sie können mehrere Listengruppen gleichzeitig exportieren. Um mehrere Listengruppen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Listengruppen aus, die exportiert werden sollen. Die exportierte Datei wird auf dem lokalen Laufwerk gespeichert.

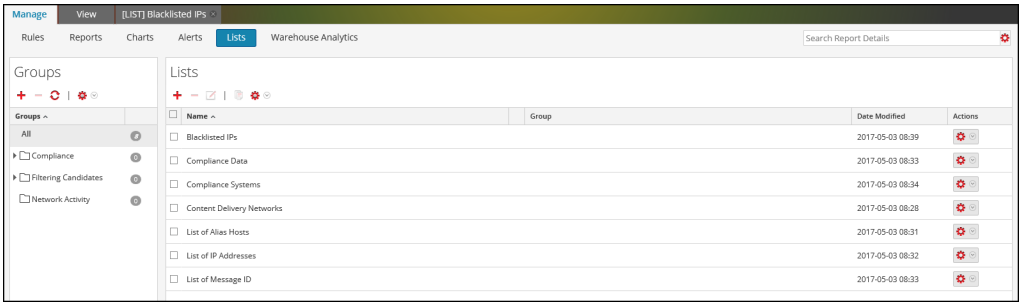
## Importieren einer Liste oder Listengruppe

### Um eine Liste zu importieren, führen Sie die folgenden Schritte aus:

Sie können Listen aus Instanzen von NetWitness Suite in die Listenstruktur im Bereich „Listenansicht“ importieren. Listen müssen in einer gültigen Binärdatei enthalten sein, die aus einer NetWitness Suite-Instanz exportiert wurde.

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.

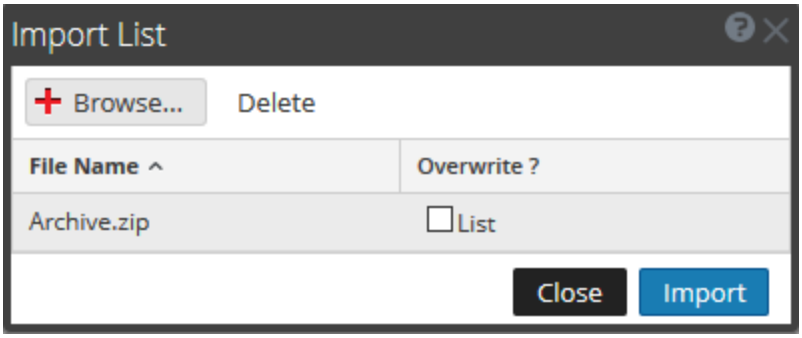
2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Klicken Sie in der Symbolleiste der **Liste** auf  > **Importieren**.
   Das Dialogfeld „Liste importieren“ wird angezeigt. Sie können mehrere Listen gleichzeitig

importieren. Um mehrere Listen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Listen aus, die importiert werden sollen.

4. Klicken Sie auf **Durchsuchen**, um die archivierte Datei, in der die Listen enthalten sind, zu suchen und auszuwählen.




5. Klicken Sie auf **Importieren**.

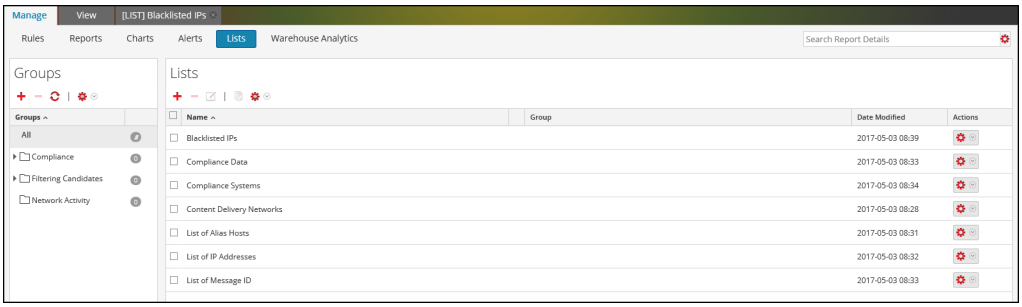
**Hinweis:** Während des Importvorgangs wird, wenn eine Duplikatliste vorhanden ist und Sie die Option zum Überschreiben nicht auswählen, die Liste importiert und keine Meldung über doppelte Listen angezeigt.

### Um eine Listengruppe zu importieren, führen Sie die folgenden Schritte aus:

Sie können Listengruppen aus Instanzen von NetWitness Suite in die Listenstruktur im Bereich „Listengruppen“ importieren. Listen müssen in einer gültigen Binärdatei enthalten sein, die aus einer NetWitness Suite-Instanz exportiert wurde.

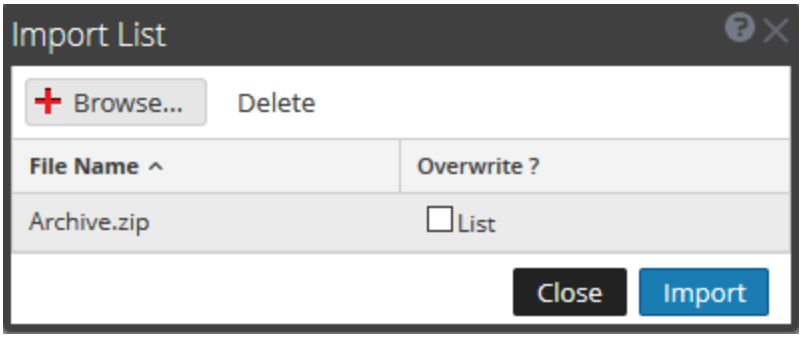
1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.




3. Klicken Sie im Bereich **Listengruppen** auf  > **Importieren**.
   Das Dialogfeld „Liste importieren“ wird angezeigt.

4. Klicken Sie auf **Durchsuchen**, um die archivierte Datei, in der die Listengruppen enthalten sind, zu suchen und auszuwählen.




   Sie können mehrere Listengruppen gleichzeitig importieren. Um mehrere Listengruppen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Listengruppen aus, die importiert werden sollen.

5. Klicken Sie auf **Importieren**.

**Hinweis:** Während des Importvorgangs wird, wenn eine doppelte Listengruppe vorhanden ist und Sie die Option zum Überschreiben nicht auswählen, die Listengruppe importiert und keine Meldung über doppelte Listengruppen angezeigt.

## Managen einer Regel

### Zugriffskontrolle für Regeln und Regelgruppen

Legen Sie die Zugriffsberechtigungen fest, über die ein Nutzer je nach Benutzerrolle zur Verwaltung einer Rolle oder Rollengruppe verfügt. Das Reporting ermöglicht eine Zugriffskontrolle auf Regel- und Regelgruppenebene. Nur ein Benutzer mit den richtigen Berechtigungen kann die Aufgaben im Reporting durchführen. Die Zugriffskontrolle wird vom Administrator in der Registerkarte **ADMIN > Sicherheit > Rollen** gemanagt.

Der Administrator muss beim Erstellen von Benutzern und Benutzerrollen darauf achten, dass die für bestimmte Aufgaben erstellten Rollen über alle in der Rollenhierarchie höher angesiedelten Zugriffsberechtigungen verfügen.

Regeln oder Regelgruppen können an bestimmte Benutzerrollen geknüpft werden. Wenn sich ein Benutzer bei NetWitness Suite anmeldet, kann dieser so nur auf die Regeln zugreifen, die für seine Benutzergruppe definiert sind. Benutzer, die einer Benutzerrolle mit Lese-und Schreibrechten angehören, verfügen über volle Zugriffsrechte für die Regel. Außerdem kann der Zugriff eingeschränkt werden, sodass nur die Benutzer mit der Berechtigung Schreibgeschützt Zugriff auf Regeln haben.

**Hinweis:** Sie müssen mindestens über Leserechte für eine Gruppe verfügen, um die Regeln innerhalb dieser Gruppe anzuzeigen.

Auf Regelebene können Sie folgende Zugriffsberechtigungen für die Benutzerrollen angeben:

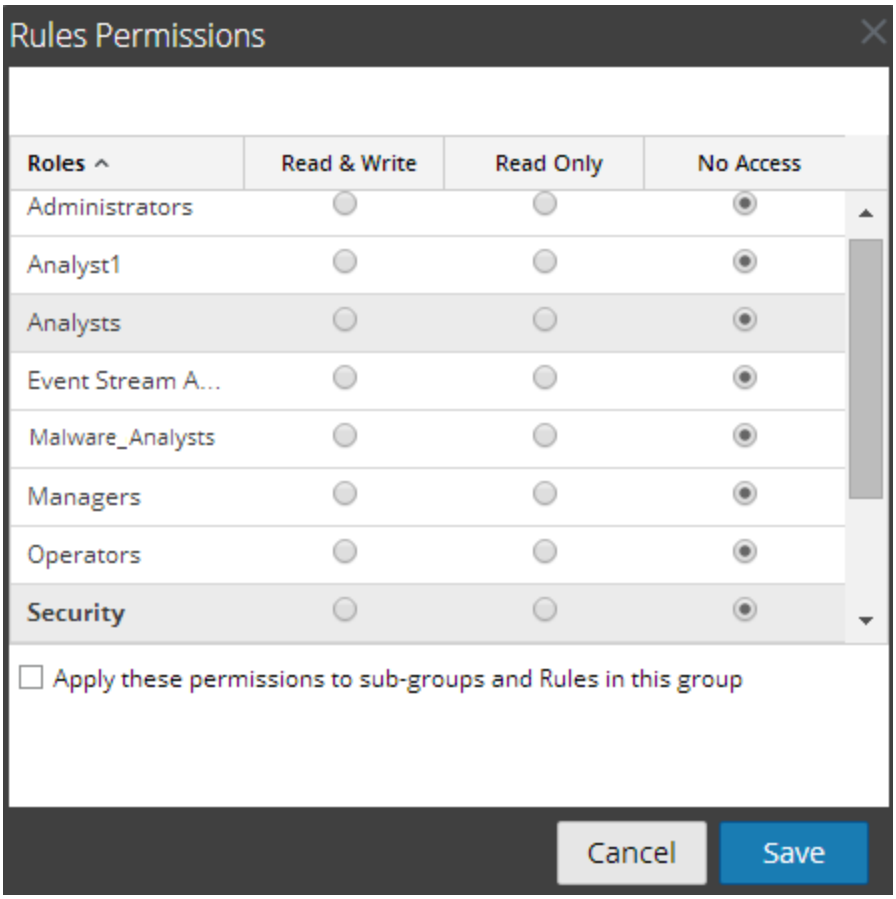
- Lesen & Schreiben
- Schreibgeschützt
- Kein Zugriff

Angenommen, **Sicherheitsanalysten** sollen Zugriff auf alle Regeln einer Regelgruppe haben, so können Sie die Berechtigung **Lesen und Schreiben** auf Regelgruppenebene festlegen. Und wenn Sie nicht möchten, dass die Rolle **Operator** Zugriff auf einen bestimmten Satz von Regeln einer Regelgruppe hat, legen Sie die Berechtigung **Kein Zugriff** auf Ebene der Regelgruppe fest. Die Berechtigung wird nur für die Regelgruppe, jedoch nicht für die Regeln oder Untergruppen in der Regelgruppe festgelegt.

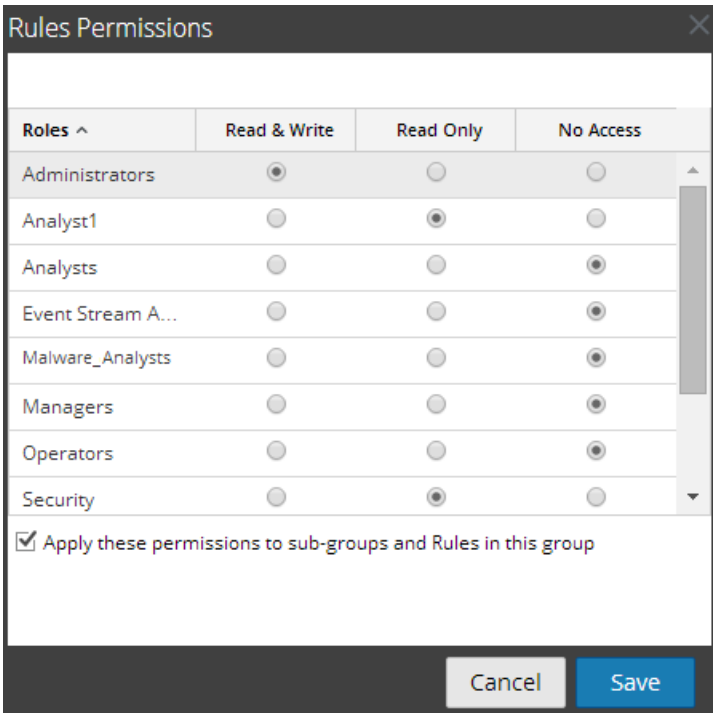
## Zugriffskontrolle für eine Regelgruppe

Möchten Sie die Regelgruppenberechtigungen ändern, müssen Sie eine Regelgruppe auswählen und Zugriffsberechtigungen über den Bereich „Regelberechtigungen“ festlegen.

Vor dem Anwenden von Regelgruppenberechtigungen lautet der standardmäßige Zugriffsstatus für alle Benutzerrollen „Kein Zugriff“ und die Kontrollkästchen sind nicht aktiviert.




Möchten Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern, müssen Sie diese, wie in der Abbildung gezeigt, auf dem Regelgruppenlevel festlegen. Angenommen, **Administratoren** soll Zugriff auf alle Regeln in einer Regelgruppe gewährt werden. In diesem Fall können Sie die Berechtigung **Lesen & Schreiben** im Bereich „Regelgruppenberechtigungen“ festlegen.




Zudem können Sie Berechtigungen auf Untergruppen und Regeln einer Gruppe anwenden, indem Sie das Kontrollkästchen aktivieren.

Die beiden Szenarien werden kurz erläutert:

- Szenario 1: Berechtigungen, die basierend auf der Benutzerrolle auf Regelgruppen/Untergruppen/Regeln angewendet werden.
- Szenario 2: Berechtigungen, die auf Untergruppen und Regeln einer Gruppe angewendet werden.

| Rolle (Analysten) | Berechtigungen werden basierend auf der Benutzerrolle auf Regelgruppen/Untergruppen/Regeln angewendet. | Berechtigungen werden auf Untergruppen und Regeln einer Gruppe angewendet. |
|---|---|---|
| **Gruppe** | **Lesen und Schreiben** | **Lesen und Schreiben** |
| **Untergruppe** | **Lesen** | **Lesen und Schreiben – übernommen** |
| **Regeln** | **Lesen** | **Lesen & Schreiben – übernommen** |

Die von Ihnen festgelegten Zugriffsberechtigungen können auf alle Untergruppen und untergeordneten Objekte dieser Gruppe angewendet werden.

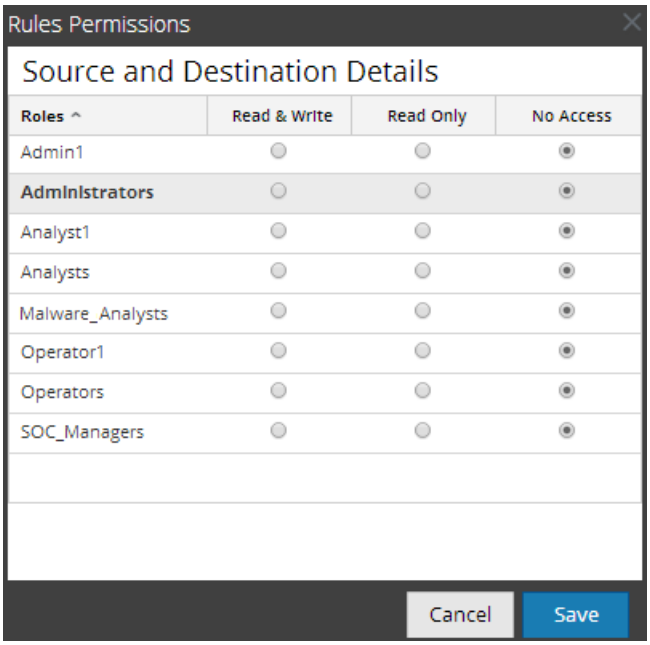
Der Regelgruppe wird die Rolle eines **Sicherheitsanalysten** zugeordnet und die Berechtigung **Lesen & Schreiben** wird für die Regelgruppe angewendet.

In Szenario 1 erhält jede Ebene abhängig von der Benutzerrolle einen Berechtigungssatz. In Szenario 2 wird die Berechtigung auf Regelgruppenebene von der Untergruppe und den Regeln der Gruppe übernommen.

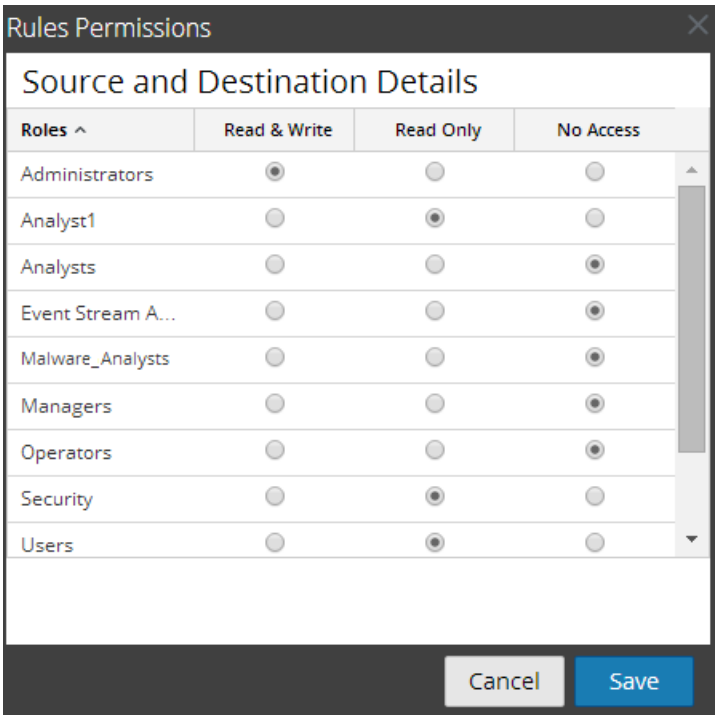
## Zugriffskontrolle für eine Regel

Möchten Sie die Regelberechtigungen ändern, müssen Sie eine Regel auswählen und deren Zugriffsberechtigung über den Bereich „Regelberechtigungen“ festlegen.

Vor dem Anwenden von Regelberechtigungen lautet der standardmäßige Zugriffsstatus für alle Benutzerrollen „Kein Zugriff“ und das Kontrollkästchen ist nicht aktiviert.



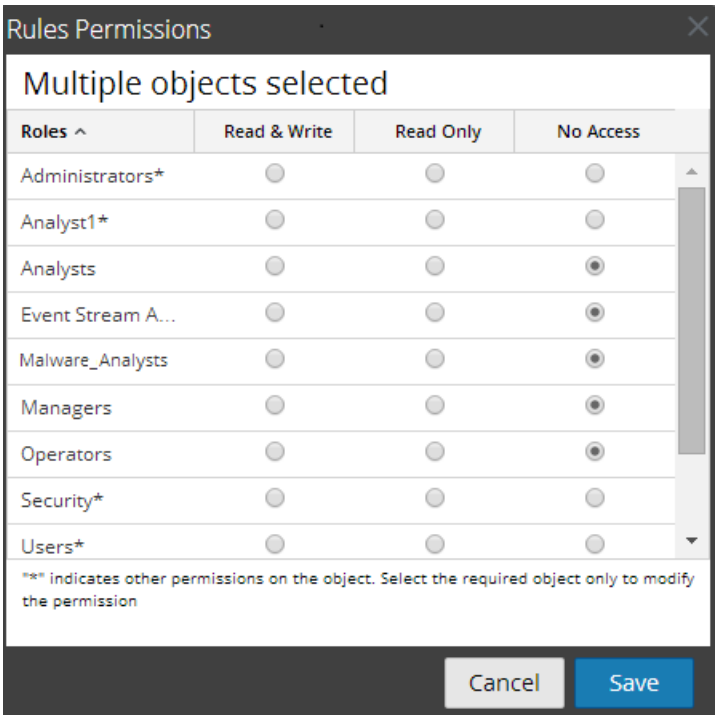

Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie diese, wie in der Abbildung gezeigt, auf Regelebene festlegen. Angenommen, **Administratoren** sollen Zugriff auf eine bestimmte Regel haben, so können Sie die Berechtigung **Lesen und Schreiben** im Bereich „Regelberechtigungen“ festlegen.




## Zugriffskontrolle für eine Regel, wenn mehrere Regeln ausgewählt sind

Möchten Sie die Berechtigungen mehrerer Regeln ändern, können Sie mehrere Regeln auf einmal auswählen und deren Zugriffsberechtigungen über den Bereich Regelberechtigungen festlegen. Die ausgewählte Zugriffsberechtigung wird auf alle ausgewählten Regeln angewendet.

**Hinweis:** „*“ neben dem Rollennamen zeigt die anderen Berechtigungen an, die für diese Benutzerrolle verfügbar sind. Wenn Sie die Zugriffsberechtigung für die erforderliche Benutzerrolle ändern möchten, wählen Sie die Benutzerrolle aus und ändern Sie die Zugriffsberechtigung.



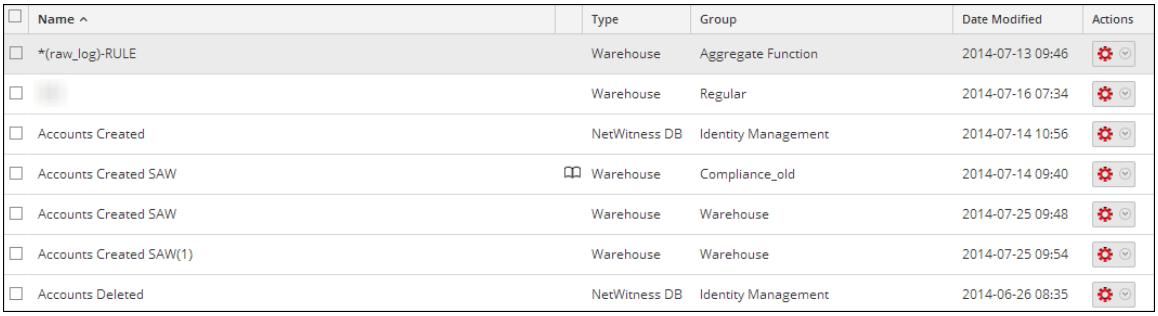

## Melden Sie sich als ein bestimmter Benutzer an und zeigen Sie die Zugriffsdetails an

Wenn Sie sich bei der NetWitness Suite-Benutzeroberfläche als Benutzer mit Leseberechtigung anmelden, werden alle Regeln mit dem Symbol (📖) gekennzeichnet. Durch Klicken auf das Symbol wird im Bereich „Regelliste“ ein Pop-up-Fenster mit der Nachricht „Schreibgeschützt“ angezeigt.

Wenn Sie sich bei der NetWitness Suite-

Benutzeroberfläche als Benutzer ohne Lese- und Schreibrechte für eine Regel anmelden, werden alle Regeln mit dem Symbol ( 👁‍🗨 ) gekennzeichnet und sind im Bereich „Regelliste“ ausgegraut.

Die folgende Abbildung zeigt den Bereich Regelliste, wenn ein Benutzer mit minimalen Lese- und Schreibrechten angemeldet ist.



**Hinweis:** Wenn ein Benutzer (der nicht Administrator ist) eine Regel erstellt, kann ADMIN nicht auf diese Regel zugreifen.

## Tabellarische Liste

Die folgende Tabelle listet die verschiedenen Spalten im Bereich „Regelberechtigungen“ auf:

| Spalte | Beschreibung |
|---|---|
| Rollen | Die Rolle des bei der NetWitness Suite-Benutzeroberfläche angemeldeten Benutzers. |
| Lesen & Schreiben | Benutzer können auf die Regeln in der Ansicht Regeln zugreifen und diese anzeigen, bearbeiten, löschen, importieren und exportieren. Der Benutzer kann die Berechtigungen für die Regel ebenfalls ändern. |
| Schreibgeschützt | Der Benutzer kann nur in der Ansicht Regeln auf die Regeln zugreifen und diese anzeigen. |
| Kein Zugriff | Der Benutzer kann mit dieser Zugriffsberechtigung nicht auf die Regel zugreifen oder diese anzeigen. |

## Einstellen der Zugriffskontrolle für eine Regel

Sie können eine Zugriffskontrolle für eine Regel einstellen. Die Reporting Engine stellt die Zugriffskontrolle auf Regelleven zur Verfügung. Nur ein Benutzer mit den entsprechenden Berechtigungen kann Aufgaben für die Regel durchführen. Der Administrator muss beim Erstellen von Benutzern und Rollen darauf achten, dass die für bestimmte Aufgaben erstellten Rollen über alle in der Rollenhierarchie höher angesiedelten Zugriffsberechtigungen verfügen.

Auf Regellevel können Sie in NetWitness Suite folgende Zugriffsberechtigungen für die Benutzerrollen angeben:

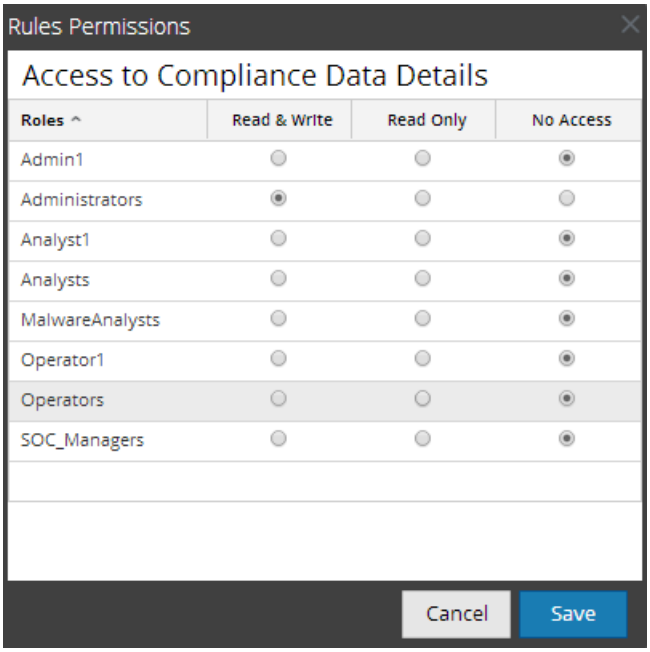
- Lesen & Schreiben – Anzeigen oder Bearbeiten der Regeln in der Regelgruppe.
- Schreibgeschützt – Nur Anzeigen der Regeln in der Regelgruppe.
- Kein Zugriff – Weder Anzeigen noch Bearbeiten der Regeln in der Regelgruppe.

## Voraussetzungen

Vergewissern Sie sich, dass Sie eine minimale „Lesen und Schreiben“-Zugriffsberechtigung haben, um Zugriffsberechtigungen für eine Regel anzugeben.

**Um die Zugriffskontrolle für eine Regel festzulegen, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Wählen Sie die Regel im Listenbereich **Regeln** aus.
3. Klicken Sie in der Symbolleiste „Regel“ auf  > **Berechtigungen**.
   Das Dialogfeld **Regelberechtigungen** wird angezeigt.




4. Wählen Sie aus den folgenden Berechtigungen die passende Zugriffsberechtigung für die Benutzerrolle aus und klicken Sie auf **Speichern**.
   - Lesen & Schreiben
   - Schreibgeschützt
   - Kein Zugriff

## Zugriffskontrolle für eine Regelgruppe einstellen

Sie können die Zugriffskontrolle auf dem regelgruppenlevel festlegen. Nur ein Benutzer mit den richtigen Berechtigungen kann die Aufgaben für die Regel durchführen. Der Administrator muss beim Erstellen von Benutzern und Rollen darauf achten, dass die für bestimmte Aufgaben erstellten Rollen über alle in der Rollenhierarchie höher angesiedelten Zugriffsberechtigungen verfügen.

Auf Regelgruppenlevel können Sie folgende Zugriffsberechtigungen für die Benutzerrollen in NetWitness Suite festlegen:

- Lesen & Schreiben – Anzeigen oder Bearbeiten der Regeln in der Regelgruppe.
- Schreibgeschützt – Nur Anzeigen der Regeln in der Regelgruppe.
- Kein Zugriff – Die Regel kann in den Regelgruppen nicht angezeigt oder bearbeitet werden.

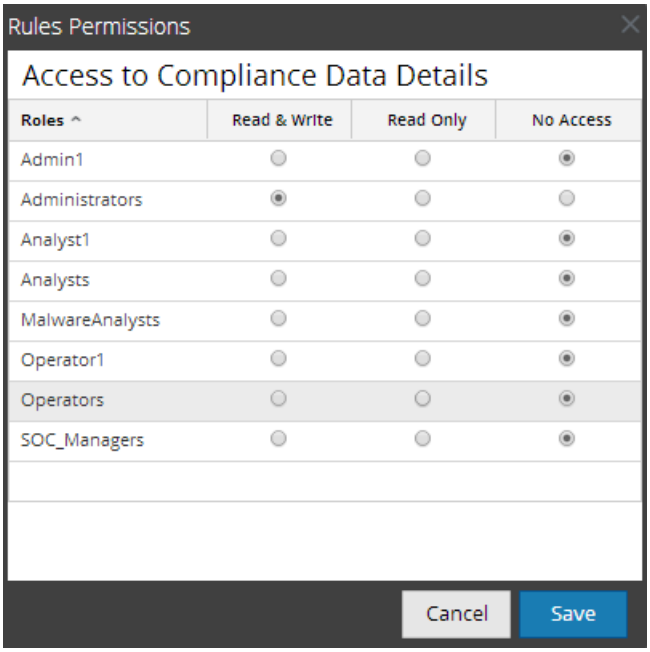
## Voraussetzungen

Vergewissern Sie sich, dass Sie eine minimale „Lesen und Schreiben“-Zugriffsberechtigung haben, um Zugriffsberechtigungen für eine Regelgruppe anzugeben.

Um die Zugriffskontrolle für eine Regelgruppe festzulegen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Wählen Sie im Bereich **Regelgruppen** die Regelgruppe aus und führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf  und wählen Sie **Berechtigungen** aus.
   - Klicken Sie mit der rechten Maustaste auf die ausgewählte Regelgruppe und wählen Sie **Berechtigungen** aus.

   Das Dialogfeld **Regelberechtigungen** wird angezeigt.



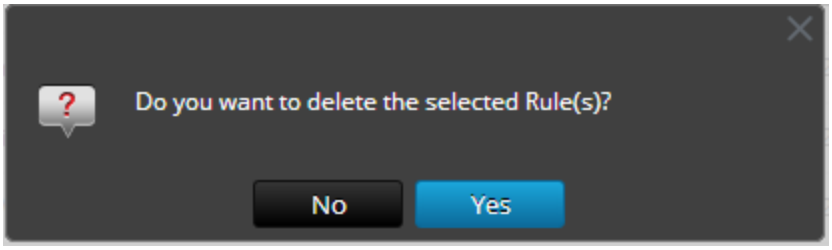

3. (Optional) Aktivieren Sie das entsprechende Kontrollkästchen, um diese Berechtigungen auf Untergruppen und untergeordnete Objekte in dieser Gruppe anzuwenden.

4. Klicken Sie auf **Speichern**.
   Eine Bestätigungsnachricht über das erfolgreiche Einrichten der Berechtigung für die ausgewählte Regelgruppe wird angezeigt.

## Löschen einer Regel oder Regelgruppe

Um eine Regel zu löschen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Führen Sie im Bereich **Regeln** einen der folgenden Schritte aus:
   - Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste „Regel“ auf .
   - Klicken Sie auf > **Löschen**.
     Ein Bestätigungsdialogfeld wird angezeigt.

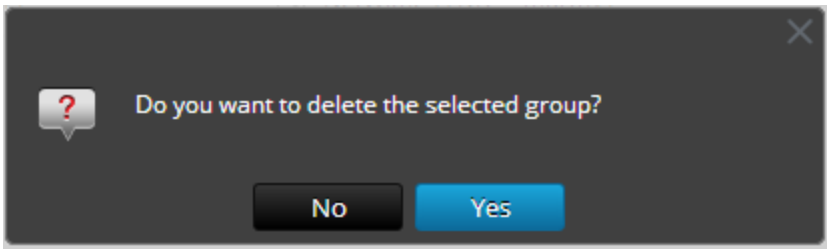



**Hinweis:** Wenn eine Regel in einem Bericht verwendet wurde, wird eine Warnung angezeigt, dass diese Regel verwendet wird und nicht gelöscht werden kann.

3. Klicken Sie auf **Ja**, um die Regel zu löschen.
   Eine Bestätigungsnachricht über das erfolgreiche Löschen der Regel wird angezeigt und die ausgewählte Regel wird aus dem Bereich Regelliste gelöscht.

Um eine Regelgruppe zu löschen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Wählen Sie im Bereich **Regelgruppen** die Regelgruppe aus, die Sie löschen möchten.
3. Klicken Sie auf .
   Ein Bestätigungsdialogfeld wird angezeigt.




**Hinweis:** Wenn eine der Regeln in der Gruppe in Berichten verwendet wird, wird eine Warnmeldung angezeigt, dass die Regel verwendet wird und nicht gelöscht werden kann.

4. Klicken Sie auf **Ja**, um die Gruppe zu löschen.

   In einer Bestätigungsmeldung wird angezeigt, dass die Gruppe erfolgreich gelöscht wurde und die ausgewählte Gruppe wurde aus dem Bereich „Regelgruppen“ entfernt.

### Duplizieren von Regeln

Um eine Regel zu deduplizieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Wählen Sie im Bereich **Regelliste** eine zu duplizierende Regel aus.
3. Klicken Sie in der Symbolleiste „Regel“ auf .

### Bearbeiten einer Regel

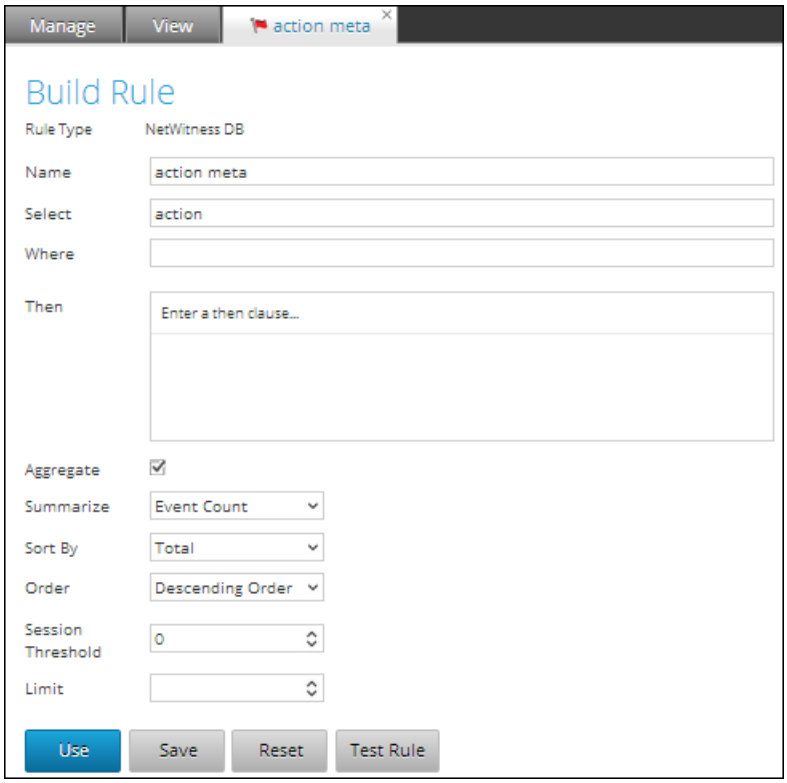
## Voraussetzungen

**Um eine Regel zu bearbeiten, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Führen Sie im Listenbereich **Regeln** einen der folgenden Schritte aus:
   - Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste „Regel“ auf .

- Klicken Sie auf  > **Bearbeiten**.

  Die Registerkarte der Ansicht Regel erstellen wird angezeigt.




**Hinweis:** Wenn eine Regel bearbeitet wurde, wird die aktualisierte Regeldefinition auf die Berichte, Diagramme und Warnmeldungen angewendet, in denen die Regel enthalten ist.

3. Ändern Sie die erforderlichen Felder.
4. Klicken Sie auf **Speichern**.

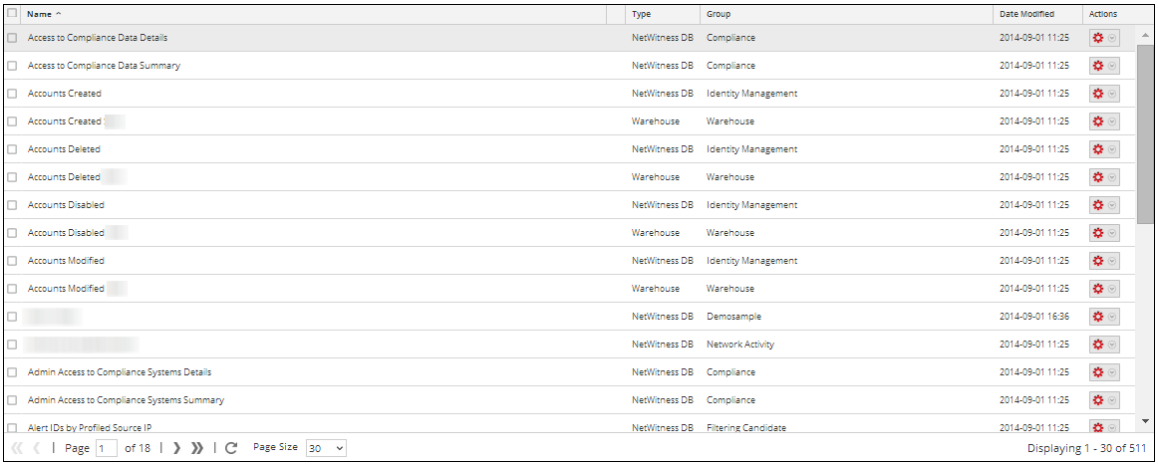
   Eine Bestätigungsmeldung, dass die Regel erfolgreich gespeichert wurde, wird angezeigt.

Stellen Sie beim Bearbeiten einer Regel sicher, dass Sie erneut die Regel auswählen, für die das Diagramm erzeugt werden soll, damit die bearbeitete Regel ausgewählt wird. Wenn Sie diese Regel nicht erneut auswählen und versuchen, die Regel zu speichern oder zu testen, wird die Regel gespeichert und eine Warnmeldung wird angezeigt.

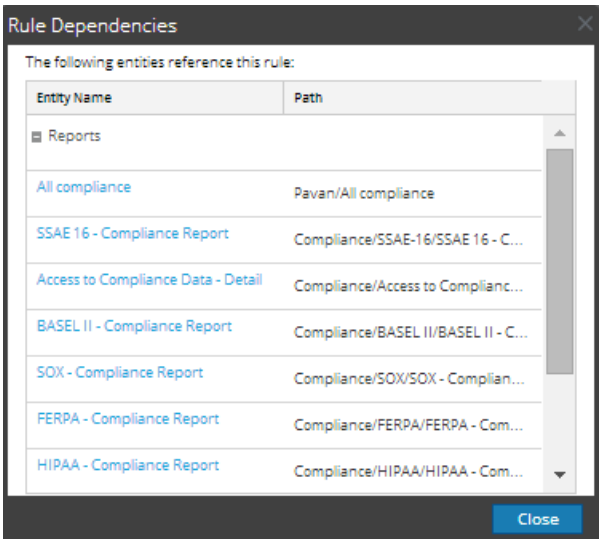
## Anzeigen der abhängigen Elemente einer Regel

Sie können die abhängigen Elemente einer Regel anzeigen. Sie müssen eine Regelliste durchsuchen und eine Regel auswählen, deren Abhängigkeit von Berichten, Diagrammen oder Warnmeldungen Sie identifizieren möchten.

In der folgenden Abbildung wird die Ansicht „Regeln“, in der Sie die Regel „Zugriff zu Details von Compliancedaten“ auswählen, dargestellt.




In der folgenden Abbildung wird die Abhängigkeit der Regel von Warnmeldungen und Berichten dargestellt.

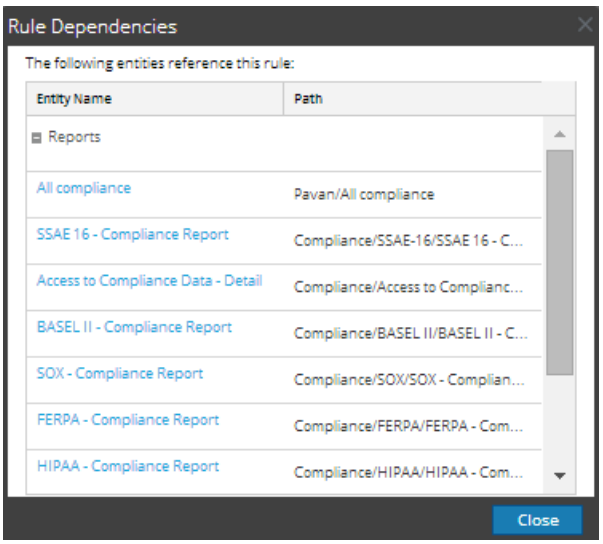



In der folgenden Tabelle sind die verschiedenen Spalten im Dialogfeld „Regelabhängigkeiten“ aufgelistet und deren Beschreibung angeführt.

| Spalte | Beschreibung |
|---|---|
| Einheitenname | Name der Einheit, der auf die Regel verweist |
| Pfad | Pfad, unter dem die Einheit in der Benutzeroberfläche zu finden ist. |

Um die abhängigen Elemente einer Regel anzuzeigen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Regeln**.
   Die Ansicht Regeln wird angezeigt.
3. Klicken Sie im Bereich **Regelliste** auf  > **Abhängige Elemente**.
   Das Dialogfeld „Regelabhängigkeiten“ wird angezeigt.




### Exportieren einer Regel oder Regelgruppe

## Voraussetzungen

Vergewissern Sie sich, dass sich in der Regelgruppe Regeln befinden.

Um eine Regel zu exportieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Führen Sie im Listenbereich **Regeln** einen der folgenden Schritte aus:
   - Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste „Regel“ auf  > **Exportieren**.
   - Klicken Sie auf  > **Exportieren**.

   Eventuell wird ein browserspezifisches Exportdialogfeld angezeigt, in dem Sie die Datei öffnen oder speichern können. Sie können mehrere Regeln gleichzeitig exportieren. Um mehrere Regeln auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Regeln aus, die exportiert werden sollen.

**Hinweis:** Wenn Sie mehrere Regeln exportieren möchten, müssen Sie eine Regelgruppe exportieren.

Um eine Regelgruppe zu exportieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Wählen Sie im Bereich **Regelgruppen** die Regelgruppe aus, die die Regel enthält, die Sie exportieren möchten.
   Sie können mehrere Regelgruppen gleichzeitig exportieren. Um mehrere Regelgruppen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Regelgruppen aus, die exportiert werden sollen.
3. Klicken Sie auf  > **Exportieren**.
   Eventuell wird ein browserspezifisches Exportdialogfeld angezeigt, in dem Sie die Datei öffnen oder speichern können.

## Managen von Berichten

### Zugriffskontrolle für Berichte oder Berichtsgruppen

In diesem Abschnitt werden die Zugriffsberechtigungen behandelt, die der Benutzer zum Management eines Berichts und einer Berichtsgruppe abhängig von der Benutzerrolle hat. Das Reporting bietet Zugriffskontrolle auf Regel- und Regelgruppenlevel. Der Benutzer, der über die geeigneten Berechtigungen verfügt, kann nur die Aufgaben im Reporting-Modul durchführen. Die Zugriffskontrolle wird vom Administrator in der Registerkarte **ADMIN > Sicherheit > Rollen** gemanagt.

Der Administrator muss beim Erstellen von Benutzern und Benutzerrollen darauf achten, dass die für bestimmte Aufgaben erstellten Rollen über alle in der Rollenhierarchie höher angesiedelten Zugriffsberechtigungen verfügen.

Berichte und Berichtgruppen können einem bestimmten Satz von Benutzerrollen zugeordnet werden, sodass die Berichte mit den Zugriffsrechten für die spezifische Benutzerrolle angezeigt werden können, wenn ein Benutzer sich bei NetWitness Suite anmeldet. Benutzer, die zu einer Benutzerrolle mit der Zugriffsberechtigung „Lesen und Schreiben“ gehören, können Berichte definieren. Außerdem kann der Zugriff eingeengt werden, sodass nur Benutzer mit Zugriff „Schreibgeschützt“ auf Berichte zugreifen können.

**Hinweis:** Sie müssen für eine Gruppe mindestens die Berechtigung „Schreibgeschützt“ haben, um die Berichte innerhalb dieser Gruppe anzuzeigen.

Auf Berichtslevel können Sie folgende Zugriffsberechtigungen für die Benutzerrollen in NetWitness Suite angeben:

- Lesen & Schreiben
- Schreibgeschützt
- Kein Zugriff

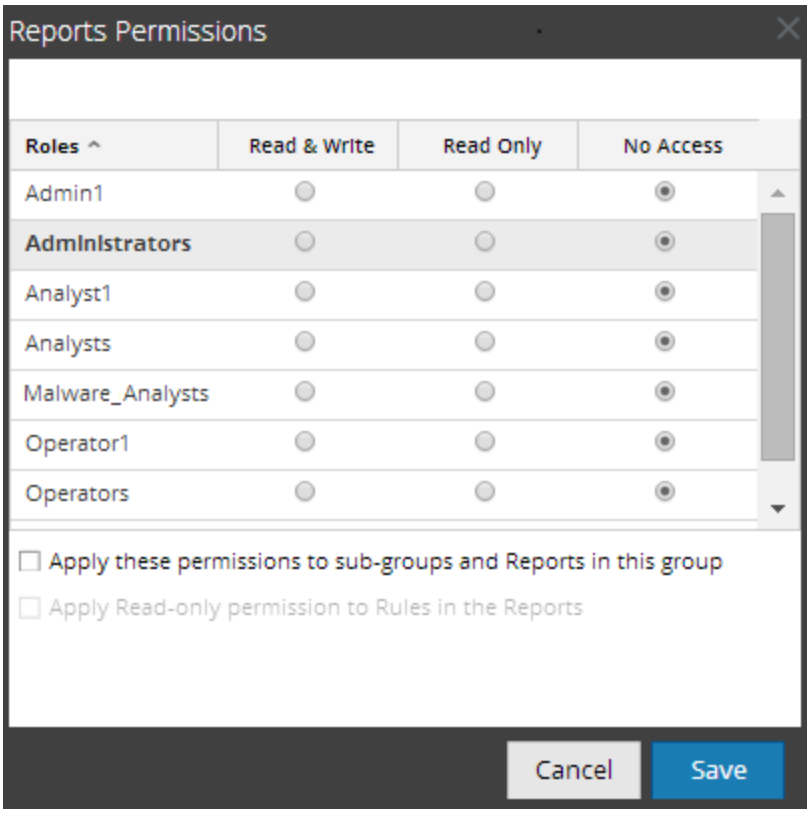
Angenommen, NetWitness Suite soll Zugriff auf alle Berichte einer Berichtsgruppe haben, so können Sie die Berechtigung **Lesen und Schreiben** auf Berichtsgruppenlevel festlegen. Und wenn Sie nicht möchten, dass die Rolle **Operator** Zugriff auf einen bestimmten Satz von Berichten in einer Berichtgruppe hat, können Sie die Berechtigung **Kein Zugriff** auf der Berichtgruppenebene festlegen.

Die Berechtigung wird nur für die Berichtsgruppe eingestellt, aber nicht für die Berichte, Regeln oder Untergruppen in der Berichtsgruppe.

## Zugriffskontrolle für eine Berichtsgruppe

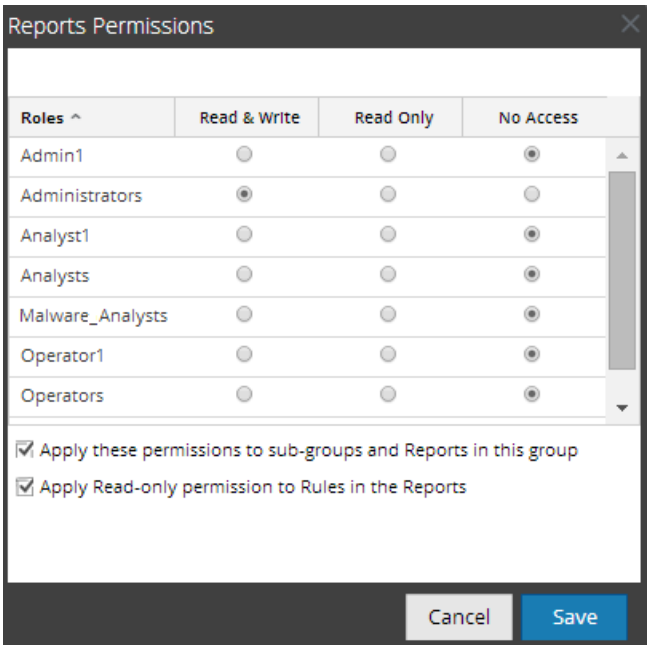
Wenn Sie die Berichtsgruppenberechtigungen ändern möchten, müssen Sie eine Berichtsgruppe auswählen und Zugriffsberechtigungen im Bereich „Berichtberechtigungen“ festlegen.

Bevor Sie Berichtsgruppenberechtigungen anwenden, ist der Standardberechtigungssatz für alle Benutzerrollen „Kein Zugriff“, außer für Administratoren, wie in der Abbildung gezeigt.



Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie diese wie in der Abbildung dargestellt auf Berichtgruppenebene festlegen. Wenn Sie beispielsweise möchten, dass die Administratoren Zugriff auf alle Berichte in einer Berichtgruppe haben, dann können Sie die Berechtigung **Lesen und Schreiben** im Bereich „Berichtgruppenberechtigungen“ festlegen.

Außerdem können Sie Berechtigungen auf Untergruppen und Berichte in der Gruppe anwenden sowie die Leseberechtigung auf Regeln in den Berichten anwenden, indem Sie wie in der Abbildung gezeigt die entsprechenden Kontrollkästchen aktivieren.




Die drei Szenarien werden kurz erläutert:

- Szenario 1: Berechtigungen werden basierend auf der Benutzerrolle auf Berichtgruppen/Untergruppen/Berichte angewendet.
- Szenario 2: Berechtigungen werden auf Untergruppen und Berichte einer Gruppe angewendet.
- Szenario 3: Leseberechtigung wird auf Regeln im Bericht angewendet.

| | Rolle (Analyst) | Berechtigungen basierend auf der Benutzerrolle auf Berichtsgruppe/Untergruppe/Bericht angewendet | Berechtigungen auf Untergruppe und Bericht in der Gruppe angewendet | Berechtigung (Schreibgeschützt) auf Regeln im Bericht angewendet |
|---|---|---|---|---|
| **Gruppe** | Lesen & Schreiben | **Lesen und Schreiben** | **Lesen und Schreiben** | Lesen & Schreiben |
| **Untergruppe** | Lesen | **Lesen** | **Lesen und Schreiben – übernommen** | Lesen & Schreiben |
| **Bericht** | Lesen | **Lesen** | **Lesen und Schreiben – übernommen** | Lesen & Schreiben |

| | | | | |
|---|---|---|---|---|
| **Regeln** | Lesen | **Lesen** | Lesen | **Lesen** |

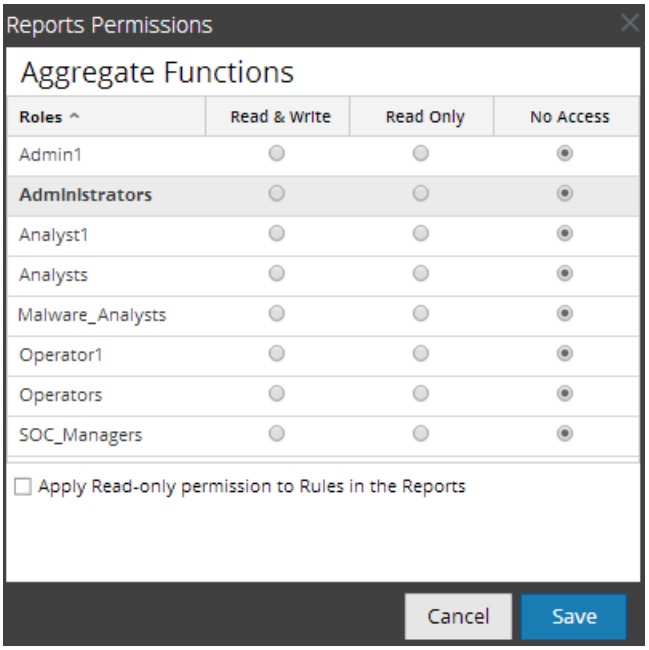
Der Berichtgruppe wird die Rolle eines **Security Analyst** zugewiesen und Berechtigungen für die Berichtgruppe werden auf **Lesen & Schreiben** eingestellt.

In Szenario 1 erhält jede Ebene abhängig von der Benutzerrolle einen Berechtigungssatz. In Szenario 2 wird die Berechtigung auf der Berichtsgruppenebene (Lesen und Schreiben) von der Untergruppe und den Berichten in der Gruppe übernommen. In Szenario 3 wird die Berechtigung "Lesen" für die Regeln festgelegt, mit der Ausnahme, dass der Berechtigungssatz für die Regeln nicht höher sein darf als der Berechtigungssatz für die Berichtsgruppe.

## Zugriffskontrolle für einen Bericht

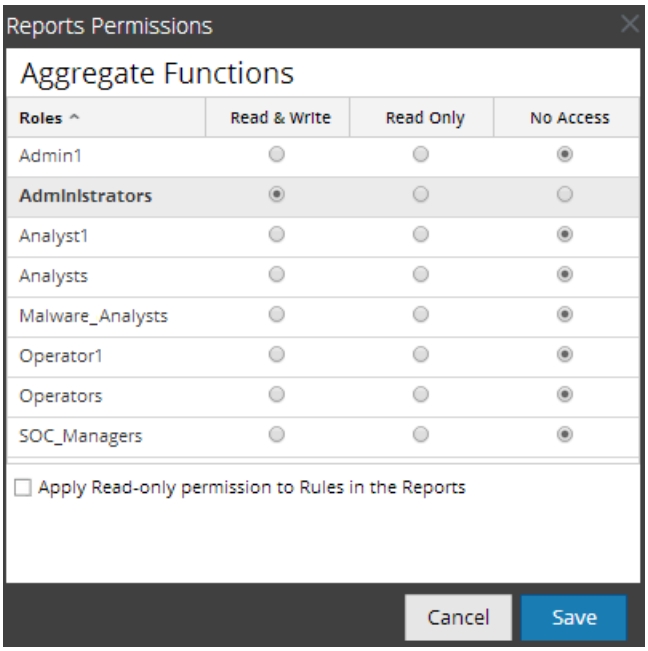
Wenn Sie die Berichtberechtigungen ändern möchten, müssen Sie einen Bericht auswählen und seine Zugriffsberechtigungen im Bereich Berichtberechtigungen festlegen.

Bevor Sie die Berichtberechtigungen anwenden, ist als Standardberechtigung für alle Benutzerrollen „Kein Zugriff“ eingestellt und das Kontrollkästchen ist wie in der Abbildung deaktiviert.




Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie diese wie abgebildet auf Berichtebene festlegen. Wenn Sie beispielsweise möchten, dass die **Administratoren** Zugriff auf einen bestimmten Bericht haben, können Sie die Berechtigung **Lesen und Schreiben** im Bereich „Berichtberechtigungen“ festlegen.

Außerdem können Sie die Leseberechtigung auf Regeln in den Berichten anwenden, indem Sie das Kontrollkästchen wie in der Abbildung gezeigt aktivieren.




Die beiden Szenarien werden kurz erläutert:

- Szenario 1: Berechtigungen auf Berichtgruppe/Untergruppe/Bericht/Regeln angewendet
- Szenario 2: Leseberechtigung wird auf Regeln im Bericht angewendet.

| | Rolle (Analysten) | Berechtigungen basierend auf der Benutzerrolle auf Berichtsgruppe/Untergruppe/Bericht/ Regeln angewendet | Berechtigung (Schreibgeschützt) auf Regeln im Bericht angewendet |
|---|---|---|---|
| **Gruppe** | Lesen & Schreiben | **Lesen und Schreiben** | Lesen & Schreiben |
| **Untergruppe** | Lesen | **Lesen** | Lesen & Schreiben |
| **Bericht** | Lesen | **Lesen** | Lesen & Schreiben |
| **Regeln** | Lesen | **Lesen** | **Lesen** |

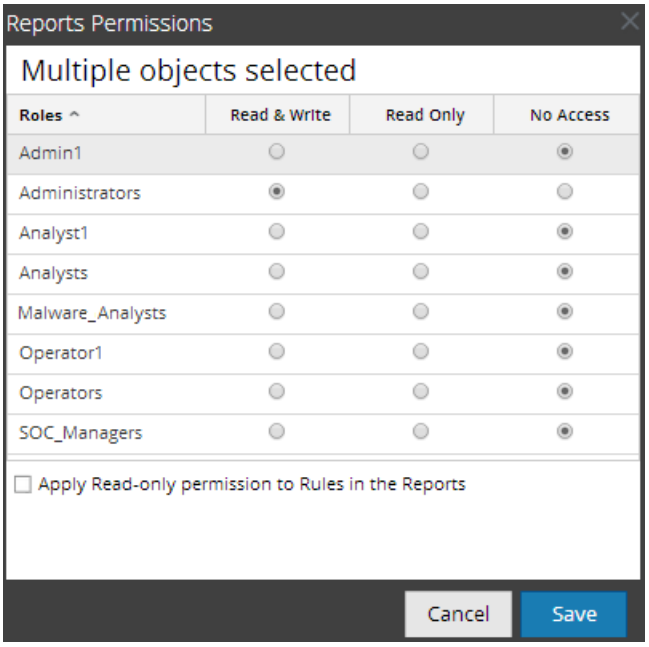
Dem Bericht wird die Rolle eines **Security Analyst** zugewiesen und Berechtigungen für die Berichte werden auf **Lesen & Schreiben** eingestellt.

In Szenario 1 verfügt jedes der Level über einen Berechtigungssatz auf Basis der Benutzerrolle. In Szenario 2 wird die Leseberechtigung für die Regeln festgelegt. Hierbei gilt, dass die für die Regeln festgelegte Berechtigung keine höhere Stufe als die für die Berichte haben kann.

**Hinweis:** Wenn die Berechtigung für die Regeln höher ist als die Berechtigung für die Berichte, wird die Berechtigung nicht angewendet. Beispiel: Wenn Sie die Berechtigungen für die Berichtsgruppe auf **Kein Zugriff** einstellen und dann die Option *Nur-Lese-Berechtigungen auf Regeln in Berichten anwenden* aktivieren, wird die Leseberechtigung für die Regeln nicht festgelegt.

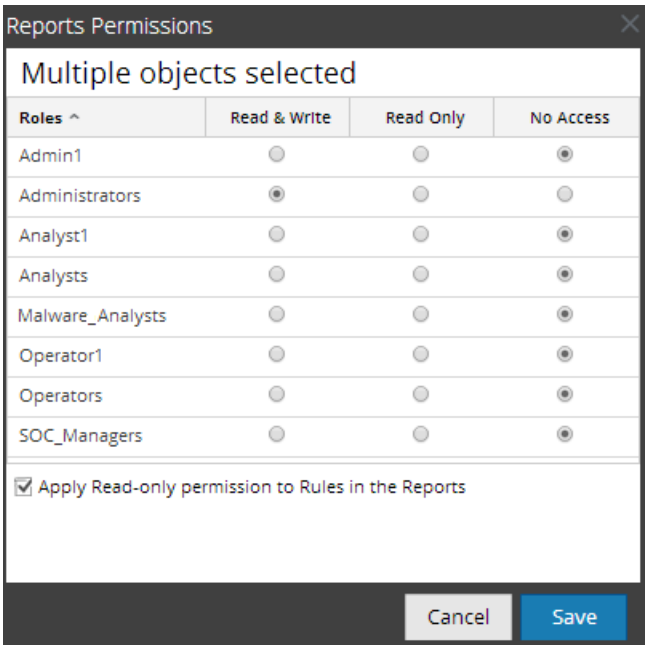
## Zugriffskontrolle für einen Bericht bei Auswahl mehrerer Berichte

Wenn Sie die Berechtigungen für mehrere Berichte ändern möchten, müssen Sie mehrere Berichte auswählen und ihre Zugriffsberechtigungen im Bereich „Berichtberechtigungen“ festlegen. Die von Ihnen ausgewählte Zugriffsberechtigung wird auf alle ausgewählten Berichte angewendet.




## Zugriffskontrolle für einen Bericht bei Auswahl mehrerer Berichte mit mehreren Regeln

Wenn Sie Berechtigungen ändern möchten, während mehrere Berichte mit mehreren Regeln ausgewählt sind, müssen Sie das Kontrollkästchen im Bereich „Berichtberechtigungen“ wie in der Abbildung gezeigt aktivieren. Die Zugriffsberechtigung für das Lesen wird auf alle Regeln in den ausgewählten Berichten angewendet, vorausgesetzt, dass die Berechtigung der Regeln niedriger ist als die Berechtigung der Berichte.

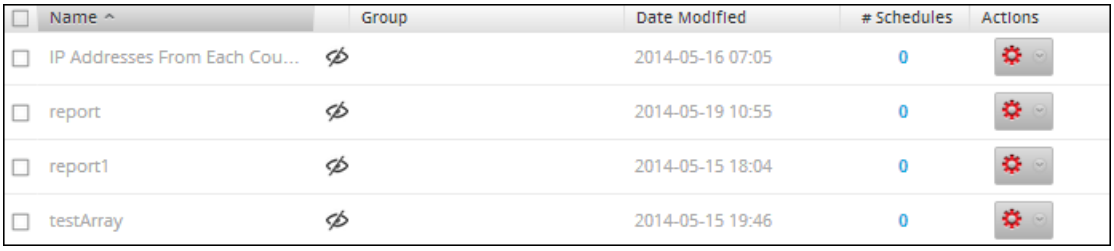



## Melden Sie sich als ein bestimmter Benutzer an und zeigen Sie die Zugriffsdetails an

Wenn Sie sich bei der NetWitness Suite-Benutzeroberfläche als Benutzer mit der Berechtigung „Lesezugriff“ anmelden, werden alle Berichte mit dem Symbol (📖) versehen. Wenn Sie auf das Symbol klicken, wird im Bereich „Berichtsliste“ „Schreibgeschützt“ angezeigt.

Wenn Sie sich bei der NetWitness Suite-Benutzeroberfläche als Benutzer ohne die Zugriffsberechtigung „Lesen und Schreiben“ für einen Bericht anmelden, werden alle Berichte mit dem Symbol ( ⊘ ) versehen und im Bereich „Berichtsliste“ grau angezeigt.

Die folgende Abbildung zeigt den Bereich Berichtliste bei Anmeldung mit minimaler Zugriffsberechtigung „Lesen & Schreiben“.




**Hinweis:** Wenn ein Benutzer (außer einem Superuser) einen Bericht erstellt, hat der Superuser keinen Zugriff auf diesen Bericht.

## Tabellarische Liste

In der folgenden Tabelle sind die verschiedenen Spalten im Bereich Berichtberechtigungen aufgeführt:

| Spalte | Beschreibung |
|---|---|
| Rollen | Die Rolle des bei der NetWitness Suite-Benutzeroberfläche angemeldeten Benutzers. |
| Lesen & Schreiben | Der Benutzer kann in der Ansicht Berichte auf den Bericht zugreifen und ihn anzeigen, bearbeiten, importieren, exportieren und löschen. Der Benutzer kann außerdem die Berechtigungen für den Bericht ändern. |
| Schreibgeschützt | Der Benutzer kann in der Ansicht Berichte lediglich auf den Bericht zugreifen und ihn anzeigen. |
| Kein Zugriff | Der Benutzer kann auf den Bericht, für den die Berechtigung festgelegt ist, nicht zugreifen und ihn nicht anzeigen. |
| Diese Berechtigungen auf Untergruppen und Berichte in dieser Gruppe anwenden | Aktivieren Sie dieses Kontrollkästchen, um die ausgewählten Berechtigungen auf die Berichtsgruppe, Untergruppen in der Gruppe und Berichte in der Gruppe anzuwenden.<br>**Hinweis:** Dieses Kontrollkästchen ist nur verfügbar, wenn Sie Zugriffsberechtigungen für eine Berichtgruppe festlegen. |
| Nur-Lese-Berechtigungen auf Regeln in Berichten anwenden | Aktivieren Sie dieses Kontrollkästchen, um Berechtigungen automatisch auf die Regeln in den Berichten anzuwenden. |

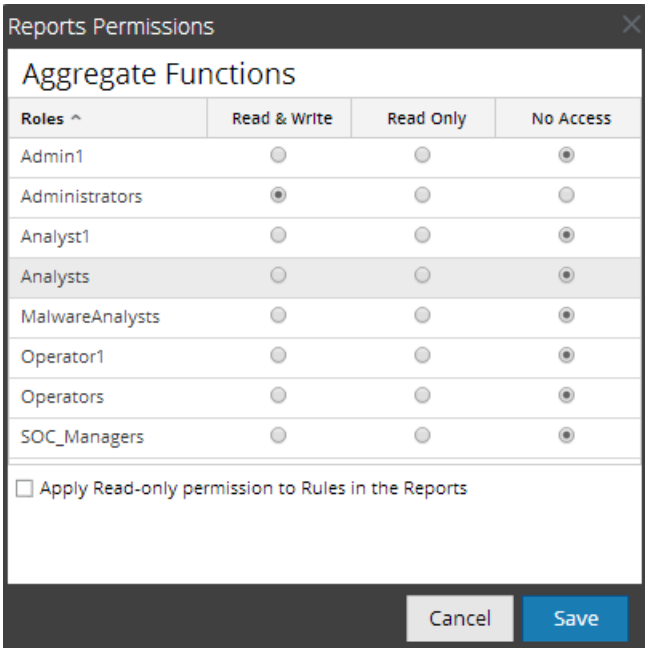
## Einstellen von Zugriffskontrollen für einen Bericht

### Voraussetzungen

Vergewissern Sie sich, dass Sie eine minimale „Lesen und Schreiben“-Zugriffsberechtigung haben, um Zugriffsberechtigungen für einen Bericht anzugeben.

Um Zugriffsberechtigungen für einen Bericht festzulegen, führen Sie die folgenden Schritte durch:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus.
4. Klicken Sie auf  > **Berechtigungen**.
   Das Dialogfeld „Berichtberechtigungen“ wird angezeigt.




5. Wählen Sie aufgrund der Benutzerrolle die entsprechenden Schaltflächen aus.
6. (Optional) Aktivieren Sie das Kontrollkästchen, wenn Sie den Regeln in den Berichten Lesezugriff zuweisen möchten.

**Hinweis:** Wenn Sie das Kontrollkästchen aktivieren, wird allen abhängigen Regeln die Zugriffsberechtigung LESEN zugewiesen, sofern die Berechtigungen für den Bericht höher als die Berechtigungen für die Regeln sind.

6. Klicken Sie auf **Speichern**.
   Eine Bestätigungsmeldung, dass die Berechtigung für den ausgewählten Bericht erfolgreich festgelegt wurde, wird angezeigt.

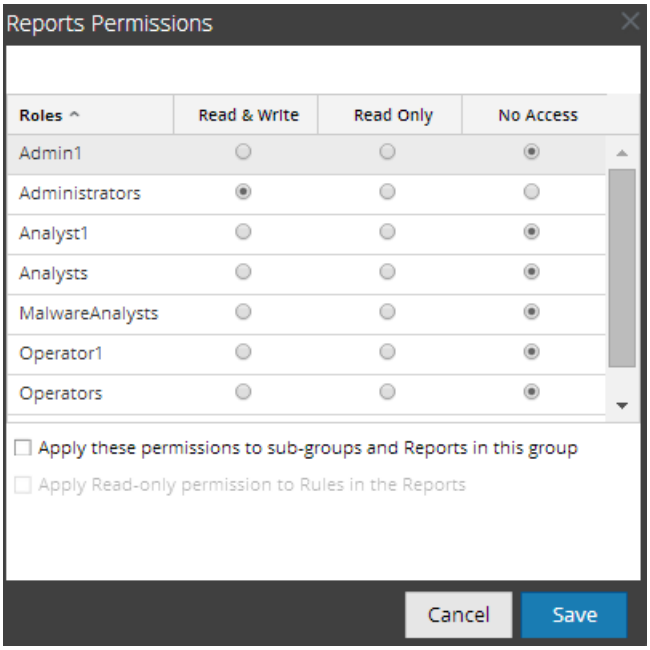
## Einstellen der Zugriffskontrolle für eine Berichtsgruppe

### Voraussetzungen

Vergewissern Sie sich, dass Sie eine minimale „Lesen und Schreiben“-Zugriffsberechtigung haben, um Zugriffsberechtigungen für eine Berichtsgruppe anzugeben.

Um Zugriffsberechtigungen für eine Berichtsgruppe festzulegen, führen Sie die folgenden Schritte durch:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsgruppen** eine Berichtsgruppe aus oder klicken Sie mit der rechten Maustaste darauf.
4. Klicken Sie auf  > **Berechtigungen**.
   Das Dialogfeld „Berichtberechtigungen“ wird angezeigt.




4. Wählen Sie aufgrund der Benutzerrolle die entsprechenden Schaltflächen aus.
5. (Optional) Aktivieren Sie das entsprechende Kontrollkästchen, um die ausgewählten Berechtigungen auf die Untergruppen und Berichte in der Gruppe anzuwenden.
6. (Optional) Aktivieren Sie das entsprechende Kontrollkästchen, um den Regeln in den Berichten die Zugriffsberechtigung „Lesen“ zu gewähren.

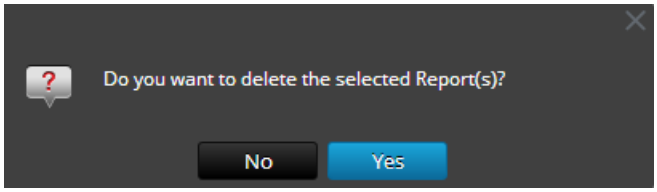
**Hinweis:** Wenn Sie das Kontrollkästchen aktivieren, wird allen abhängigen Regeln die Zugriffsberechtigung LESEN zugewiesen, sofern die Berechtigungen für den Bericht höher als die Berechtigungen für die Regeln sind.

7. Klicken Sie auf **Speichern**.
   In einer Bestätigungsmeldung wird angezeigt, dass die Berechtigung für die ausgewählte Berichtsgruppe erfolgreich festgelegt wurde.

### Löschen von Berichten oder Berichtsgruppen

So löschen Sie im Bereich „Berichtsliste“ Berichte in einer Gruppe oder Untergruppe:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Führen Sie im Bereich **Berichtsliste** einen der folgenden Schritte aus:
   - Wählen Sie die Berichte aus und klicken Sie auf .
   - Klicken Sie auf > **Löschen**.
     Ein Bestätigungsdialogfeld wird angezeigt.




4. Klicken Sie auf **Ja**, um den Bericht zu löschen.
   Eine Bestätigungsmeldung wird angezeigt, dass der Bericht erfolgreich gelöscht wurde, und der ausgewählte Bericht wird aus dem Bereich „Berichtsliste“ gelöscht.

## Löschen einer Berichtsgruppe

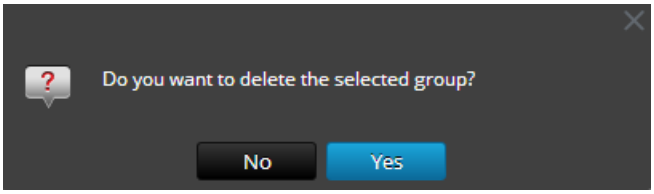
## Voraussetzungen

Der Berichtsgruppe müssen Berichte zugeordnet sein.

Um Berichtsgruppen im Standardordner oder Untergruppen unter einer Berichtsgruppe zu löschen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.

3. Wählen Sie im Bereich **Berichtsgruppe** die Berichtsgruppe aus und klicken Sie auf .
   Ein Bestätigungsdialogfeld wird angezeigt.




4. Klicken Sie auf **Ja**, um die Gruppe zu löschen.
   Eine Meldung wird angezeigt, in der bestätigt wird, dass die Gruppe gelöscht wurde. Die ausgewählte Gruppe wird aus dem Bereich „Berichtsgruppe“ gelöscht.

## Duplizieren eines Berichts

Sie können einen Bericht duplizieren, um mehrere Berichtszeitpläne oder den gleichen Bericht zu planen. Der duplizierte Bericht wird im Bereich „Berichtsliste“ mit Suffixen angezeigt. zum Beispiel „Bericht (1)“.

Im Allgemeinen wird die Option zum Duplizieren in zwei Szenarien verwendet:

- Sie möchten eine Kopie des Berichts erstellen, um den gleichen Bericht in eine andere Gruppe zu verschieben.
- Sie möchten die meisten Konfigurationseinstellungen für ein Objekt beibehalten und nur einige dieser Einstellungen ändern.
  Wenn zum Beispiel eine komplexe Abfrage in einer Regel vorhanden ist bzw. mehrere Regeln in einem Bericht vorhanden sind, ist die Option Duplizieren am besten geeignet.

Um einen vorhandenen Bericht zu duplizieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus, den Sie duplizieren möchten, und klicken Sie auf .
   Der Bericht wird erfolgreich gespeichert und zur Berichtsliste hinzugefügt.

Sie können den duplizierten Bericht in eine andere Gruppe verschieben.

## Bearbeiten eines Berichts

Um Berichte in einer Gruppe oder Untergruppe aus dem Bereich „Berichtsliste“ zu bearbeiten, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Führen Sie im Bereich **Berichtsliste** einen der folgenden Schritte aus:
   - Wählen Sie einen Bericht aus und klicken Sie auf  .
   - Klicken Sie auf  > **Bearbeiten**.

   Die Registerkarte „Bericht erstellen“ wird angezeigt.


4. Ändern Sie den Text und fügen Sie zusätzliche Regeln zum Bericht hinzu (falls erforderlich).
5. Klicken Sie auf **Speichern**.
   Eine Bestätigungsmeldung, dass der Bericht erfolgreich gespeichert wurde, wird angezeigt.

## Aktualisieren einer Berichtsgruppe oder -liste

Sie können eine Berichtsgruppe oder Berichte aktualisieren, um die Neuanordnung von Gruppen oder Berichten anzuzeigen.

Um eine Berichtsgruppe oder Berichte zu aktualisieren, führen Sie folgende Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Führen Sie die folgenden Schritte aus, um die Gruppe oder die Berichte an eine neue Position zu verschieben:

- Verschieben Sie die Gruppe im Bereich **Berichtsgruppen** per Drag-and-drop.
- Verschieben Sie die Berichte vom Bereich **Berichtsliste** per Drag-and-drop auf die gewünschte Gruppe im Bereich „Berichtsgruppen“.
  Die Berichtsgruppe bzw. die Berichte werden an die neue Position verschoben.

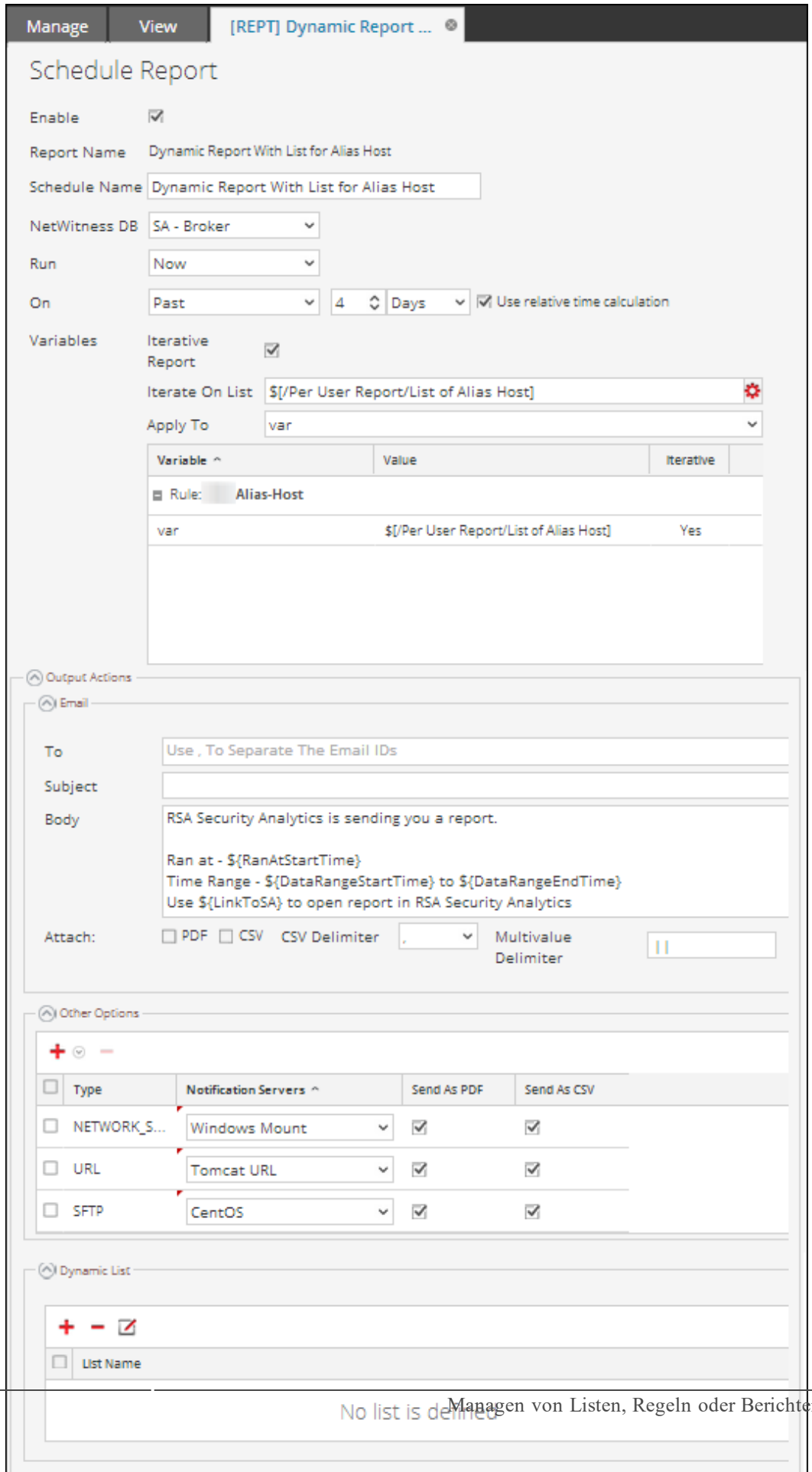
4. So aktualisieren Sie eine Berichtsgruppe oder -liste:
   - Klicken Sie im Bereich **Berichtsgruppe** auf .
     Die Berichtsgruppe wird aktualisiert.
   - Klicken Sie im Bereich **Berichtsliste** auf .
     Die Berichtsliste wird aktualisiert.

## Bearbeiten eines geplanten Berichts

Um einen geplanten Bericht aus dem Bereich „Liste geplanter Berichte“ zu bearbeiten, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus und klicken Sie auf > **Geplante Berichte anzeigen**.
   Die Registerkarte „Geplante Berichte anzeigen“ wird angezeigt.
4. Führen Sie im Bereich **Liste geplanter Berichte** einen der folgenden Schritte aus:
   - Wählen Sie einen Bericht aus und klicken Sie auf .
   - Wählen Sie einen Bericht aus und klicken Sie auf > **Plan bearbeiten**.

Die Registerkarte „Bericht planen“ wird angezeigt.


Manage
View
[REPT] Dynamic Report ...
Schedule Report
Enable
Report Name
Dynamic Report With List for Alias Host
Schedule Name
Dynamic Report With List for Alias Host
NetWitness DB
SA - Broker
Run
Now
On
Past
4
Days
Use relative time calculation
Variables
Iterative Report
Iterate On List
$[/Per User Report/List of Alias Host]
Apply To
var
Variable
Value
Iterative
Rule:
Alias-Host
var
$[/Per User Report/List of Alias Host]
Yes
Output Actions
Email
To
Use , To Separate The Email IDs
Subject
Body
RSA Security Analytics is sending you a report.
Ran at - ${RanAtStartTime}
Time Range - ${DataRangeStartTime} to ${DataRangeEndTime}
Use ${LinkToSA} to open report in RSA Security Analytics
Attach:
PDF
CSV
CSV Delimiter
Multivalue Delimiter
Other Options
Type
Notification Servers
Send As PDF
Send As CSV
NETWORK_S...
Windows Mount
URL
Tomcat URL
SFTP
CentOS
Dynamic List
List Name
No list is defined

5. Führen Sie in der Registerkarte „Bericht planen“ die folgenden Schritte aus:
   a. Ändern Sie im Feld **Planname** den Namen für die Konfiguration der Berichtsplanung.
   b. Aktivieren Sie für die planmäßige Ausführung der Berichte das Kontrollkästchen **Aktivieren**.
   c. Wählen Sie im Feld **Datenquelle** die Datenquelle aus.

   **Hinweis:** Wenn die Datenquelle nicht aufgelistet ist, stellen Sie sicher, dass Sie die **Leseberechtigung** für die Datenquelle haben. Dies gilt nur für NWDB- und Warehouse-Datenquellen. Weitere Informationen finden Sie unter „Konfigurieren von Datenquellenberechtigungen“ im *Konfigurationsleitfaden Reporting Engine*.

6. (Optional) Wählen Sie aus der Drop-down-Liste **Warehouse-Ressourcenpool** den Pool oder die Warteschlange für den Bericht aus.

   **Hinweis:** Die Drop-down-Liste **Warehouse-Ressourcenpool** wird nur angezeigt, wenn die Warehouse-Regel ausgewählt ist. Wurden für die Reporting Engine keine Pools oder Warteschlangen eingegeben, ist dieses Feld deaktiviert.

7. Wählen Sie im Feld **Ausführen** den Typ der Ausführungsplanung aus. (Beispielsweise Jetzt oder Später.)
8. Wählen Sie den Datumsbereich aus, um den Zeitpunkt der Abfrage absolut festzulegen, oder aktivieren Sie das Kontrollkästchen **Relative Zeitberechnung verwenden**, um den Zeitpunkt der Abfrage relativ festzulegen.
9. (Optional) Gehen Sie im Bereich Ausgabeaktionen wie folgt vor:
   i. Geben Sie die E-Mail-Adresse und den Betreff ein.
   ii. Bearbeiten Sie den Meldungstext für den Bericht.
   iii. Wählen Sie das Format des Anhangs aus.
   iv. Geben Sie einen Wert für die CSV-Trennzeichen und Trennzeichen für mehrere Werte ein.
10. (Optional) Gehen Sie im Feld Andere Optionen wie folgt vor:
    i. Klicken Sie auf  > **SFTP** oder **URL** oder **Netzwerkfreigabe**. Je nach ausgewählter Option wird im Feld „Andere Optionen“ eine Zeile hinzugefügt.
    ii. Wählen Sie die entsprechenden Optionen aus, um den Bericht im PDF- oder CSV-Format an die konfigurierte SFTP, URL oder Netzwerkfreigabe zu senden.

11. (Optional) Informationen zum Hinzufügen einer Liste im Bereich „Dynamische Liste“ finden Sie im Abschnitt „Erzeugen einer Liste aus dem geplanten Bericht“ in Erstellen und Planen eines Berichts.
12. (Optional) Informationen darüber, wie Sie im Bereich „Logo“ ein anderes Logo auswählen, finden Sie im Abschnitt Managen und Auswählen von Berichtslogos.

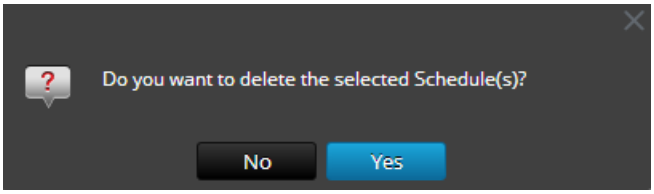
    **Hinweis:** Wenn Sie kein Logo angeben, wird das RSA-Standardlogo verwendet.

13. Klicken Sie auf **Planen**.
    Der geplante Bericht wird nach Plan ausgeführt und stellt die konfigurierten Ausgaben bereit.

## Löschen eines geplanten Berichts

Um einen geplanten Bericht aus dem Bereich „Liste geplanter Berichte“ zu löschen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie in der Symbolleiste **Bericht** auf **Alle Pläne anzeigen**.
   „Geplante Berichte anzeigen“ wird angezeigt.
4. Wählen Sie den Bericht im Bereich **Liste geplanter Berichte** aus.
5. Klicken Sie auf  > **Plan löschen**.
   Ein Bestätigungsdialogfeld wird angezeigt.




6. Klicken Sie auf **Ja**, um den geplanten Bericht zu löschen.
   Eine Bestätigungsmeldung wird angezeigt, dass der geplante Bericht erfolgreich gelöscht wurde, und der ausgewählte Plan wird aus dem Bereich „Liste geplanter Berichte“ gelöscht.

## Exportieren eines Berichts

Sie können die ausgewählten Berichte in eine externe Datei exportieren, die später in eine andere NetWitness Suite-Umgebung importiert werden kann.

## Voraussetzungen

In der Berichtsgruppe befinden sich Berichte.

Um ausgewählte Berichte im Bereich „Berichtsgruppen“ in eine externe Datei zu exportieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Führen Sie im Bereich **Berichtsliste** einen der folgenden Schritte aus:
   - Wählen Sie einen Bericht aus und klicken Sie auf  > **Exportieren**.
   - Klicken Sie auf  > **Exportieren**.

   Sie können mehrere Warnmeldungen gleichzeitig exportieren. Wenn Sie mehrere Berichte auswählen möchten, aktivieren Sie das Kontrollkästchen des Berichts, der exportiert werden soll. Die exportierte Datei wird auf dem lokalen Laufwerk in einem Archivformat gespeichert.

## Öffnen von CSV-Dateien mit Unicode-Zeichen in MS Excel

So öffnen Sie heruntergeladene CSV-Dateien, die Unicode-Zeichen enthalten, in MS Excel:

1. Laden Sie den Bericht herunter und speichern Sie die CSV-Datei.
2. Öffnen Sie Microsoft Excel und navigieren Sie zur Registerkarte **Daten**.
3. Klicken Sie auf den Menüeintrag **Aus Text**, suchen Sie die CSV-Datei, die Sie heruntergeladen haben, und klicken Sie auf **Importieren**.
   Der Textimportassistent wird angezeigt.
4. Wählen Sie als Datentyp **Getrennt** oder **Feste Breite** im Bereich **Ursprünglicher Datentyp** aus.
5. Klicken Sie auf die Drop-down-Liste **Dateiursprung**, wählen Sie **65001: Unicode (UTF-8)** aus und klicken Sie auf **Weiter**.
6. Wählen Sie das Trennzeichen, das in der importierten Datei verwendet wurde, und klicken Sie auf **Weiter**.
7. Wählen Sie das Datenformat für die einzelnen Datenspalten aus, die Sie importieren möchten, und klicken Sie auf **Fertig stellen**.
   Die korrekte Ausgabe wird in einem Arbeitsblatt in MS Excel angezeigt.

### Exportieren einer Berichtsgruppe

Sie können ausgewählte Berichtsgruppen in eine externe Datei exportieren, die später in eine andere NetWitness Suite-Umgebung importiert werden kann.

## Voraussetzungen

In der Berichtsgruppe befinden sich Berichte.

Um ausgewählte Berichtsgruppen im Bereich „Berichtsgruppen“ in eine externe Datei zu exportieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsgruppe** die Berichtsgruppe aus, klicken Sie auf  und wählen Sie eine der folgenden Optionen aus:
   - **Exportieren**: Mit dieser Auswahl wird ein Bericht in eine ZIP-Datei exportiert.
   - **Als Text exportieren**: Mit dieser Auswahl werden alle Inhalte aus der Reporting Engine in eine ZIP-Datei exportiert, welche die Daten im Textformat enthält.

   Sie können mehrere Berichtsgruppen gleichzeitig exportieren. Um mehrere Berichtsgruppen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Berichtsgruppen aus, die exportiert werden sollen. Die exportierte Datei wird auf dem lokalen Laufwerk gespeichert.

### Importieren von Berichten und Berichtsgruppen

Sie können Gruppen mit Untergruppen und Berichten aus anderen Instanzen von NetWitness Suite in den Bereich „Berichtsgruppen“ importieren. Berichte müssen als gültige Binärdatei vorliegen, die aus einer anderen NetWitness Suite-Instanz exportiert wurde.
Während des Importvorgangs wählen Sie die Binärdatei aus und geben an, ob vorhandene Berichte mit demselben Namen mit den Berichten in der binären Importdatei überschrieben werden sollen oder nicht.

- Wenn Sie sich für das Überschreiben entscheiden, werden alle doppelten Regeln, Listen und Berichte mit den Inhalten der binären Importdatei überschrieben.
- Wenn Sie sich gegen das Überschreiben entscheiden und im Zielordner ist eine doppelte Regel, Liste oder ein doppelter Bericht vorhanden, schlägt der Import fehl und es wird eine Nachricht zu den doppelten Berichten angezeigt.

Sie können keine Berichte in eine bestimmte Berichtsgruppe importieren. Die importierten Dateien werden im Stammordner **Alle** gespeichert.

## Voraussetzungen

Sie haben Berichte oder Berichtsgruppen aus einer anderen NetWitness Suite-Instanz exportiert.

Um Gruppen mit Untergruppen und Berichten aus anderen NetWitness Suite-Instanzen in den Bereich „Berichtsgruppen“ zu importieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsgruppen** einen Ordner aus, in den die Datei importiert werden soll.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie zum Importieren einer Gruppe im Bereich **Berichtsgruppen** auf  > **Importieren**.
   - Klicken Sie zum Importieren eines Berichts in der Symbolleiste **Bericht** auf  > **Importieren**.
     Das Dialogfeld „Bericht importieren“ wird angezeigt. Sie können mehrere Berichte und Berichtsgruppen gleichzeitig importieren. Um mehrere Berichte oder Berichtsgruppen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Berichte oder Berichtsgruppen aus, die importiert werden sollen.
5. Klicken Sie auf **Durchsuchen**, um nach der Binärdatei zu suchen.
   NetWitness Suite bietet eine Dateisystemansicht der Dateien.
6. Suchen Sie die Binärdatei und klicken Sie auf **Öffnen**.
   Die Datei wird der Liste „Bericht importieren“ hinzugefügt.
7. (Optional) Aktivieren Sie das Kontrollkästchen **Regel**, wenn Sie beim Import eine beliebige vorhandene Regeln in der Bibliothek mit einer identisch benannten Regel in der Binärdatei überschreiben möchten. Wenn Sie die Option Überschreiben nicht auswählen und eine identische Regel in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.
8. (Optional) Aktivieren Sie das Kontrollkästchen **Liste**, wenn Sie beim Import eine beliebige vorhandene Liste in der Bibliothek mit einer identisch benannten Liste in der Binärdatei überschreiben möchten. Wenn Sie die Option Überschreiben nicht auswählen und eine

identische Liste in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.

9. (Optional) Aktivieren Sie das Kontrollkästchen **Bericht**, wenn Sie beim Import einen beliebigen vorhandenen Bericht in der Bibliothek mit einem identisch benannten Bericht in der Binärdatei überschreiben möchten. Wenn Sie die Option Überschreiben nicht auswählen und ein identischer Bericht in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.
10. Klicken Sie auf **Importieren**, um die Binärdatei zu importieren.

## Aktivieren oder Deaktivieren eines geplanten Berichts

**Um einen geplanten Bericht aus dem Bereich „Liste geplanter Berichte“ zu aktivieren oder zu deaktivieren, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus und klicken Sie auf  > **Geplante Berichte anzeigen**.
   „Geplante Berichte anzeigen“ wird angezeigt.
4. Wählen Sie im Bereich „Liste geplanter Berichte“ einen Bericht aus.
5. Klicken Sie auf  > **Aktivieren**.
   Der Status des Berichts wird in „Wird ausgeführt“ geändert, wenn für den Bericht die sofortige Ausführung geplant ist.
6. Klicken Sie auf  > **Deaktivieren**.
   Der Status des Berichts wird in „Inaktiv“ geändert.

## Start oder Beenden eines geplanten Berichts

**Um einen geplanten Bericht zu starten oder zu beenden, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus und klicken Sie auf  > **Geplante Berichte anzeigen**.
   Die Ansicht Geplante Berichte anzeigen wird angezeigt.
4. Wählen Sie im Bereich „Liste geplanter Berichte“ einen Bericht aus.
5. Klicken Sie auf  > **Starten**.
   Der Status des Berichts wird in „Wird ausgeführt“ geändert, wenn für den Bericht die sofortige Ausführung geplant ist.
6. Klicken Sie auf  > **Beenden**.
   Der Status des Berichts wird in „Abgeschlossen“ geändert.

## Anzeigen des Ausführungsverlaufs eines geplanten Berichts

Sie können den Ausführungsverlaufs eines geplanten Berichts anzeigen. Sie können den bisherigen Verlauf eines geplanten Berichts anzeigen. Sie können den Verlauf basierend auf folgenden Kriterien anzeigen:

- Anzahl der ausgeführten Pläne
- Startdatum und Enddatum

Sie können Details anzeigen, wie z. B. die Häufigkeit der Ausführung des geplanten Berichts, die Dauer der Ausführung (in Sekunden), der Status der Ausführung. Sie könnten den erzeugten Bericht außerdem im Vollbildmodus anzeigen.

**Um den Ausführungsverlauf eines geplanten Berichts anzuzeigen, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.

3. Führen Sie im Bereich **Berichtsliste** einen der folgenden Schritte aus:
   - Klicken Sie auf  > **Geplante Berichte anzeigen**.
   - Klicken Sie auf die Spalte **#Planungen**.
     Die Registerkarte Ansicht Geplante Berichte wird mit dem Status jedes geplanten Berichts angezeigt.
4. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie einen geplanten Bericht aus und klicken Sie auf  > **Ausführungsverlauf**.
   - Wählen Sie einen geplanten Bericht aus und klicken Sie auf  .
     Die Ansicht „Ausführungsverlauf“ wird angezeigt.

   **Hinweis:** Standardmäßig können Sie 10 vergangene Ausführungsdatensätze eines geplanten Berichts anzeigen. Der angezeigte Ausführungsverlauf hängt ab von der Konfiguration der Berichtsverlaufsaufbewahrung in der Registerkarte **Allgemein** der Ansicht **ADMIN > Services > Reporting Engine-Konfiguration**.
   Wenn Sie z. B. in der Konfiguration der Berichtsverlaufsaufbewahrung 100 Tage eingestellt haben, werden die Daten im Ausführungsverlauf für die letzten 100 Tage unter Berücksichtigung des aktuellen Datums angezeigt.
5. Wählen Sie im Feld **Verlauf abrufen nach:** den abzurufenden Verlaufstyp aus. (Beispiel: Vergangen oder Bereich (spezifisch))
6. Geben Sie im Feld **Anzahl** die Anzahl der anzuzeigenden Ausführungen ein.
7. Klicken Sie auf **Verlauf einblenden**.
   Der Ausführungsverlauf des geplanten Berichts wird angezeigt.

## Managen und Auswählen von Berichtslogos

### Voraussetzungen

Vergewissern Sie sich, dass der Reporting Engine-Service vor dem Verwalten eines Logos definiert wurde.

### Managen von Berichtslogos

**Um Logos zu managen, führen Sie die folgenden Schritte aus:**

1. Wählen Sie **ADMIN** > **Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie im Bereich **Serviceliste** einen Reporting Engine-Service aus und klicken Sie auf

**Ansicht** > **Konfiguration**.

Die Ansicht „Service-Konfiguration“ wird angezeigt.

3. Wählen Sie die Registerkarte **Logos verwalten** aus.

   Alle verfügbaren Logos werden angezeigt.

## Hinzufügen eines Logos

**Um eine Logo hinzuzufügen, führen Sie die folgenden Schritte aus:**

1. Klicken Sie in der Registerkarte **Logos verwalten** auf +.

   Ein Dateibrowser wird geöffnet, in dem Sie die Datei aus dem lokalen Laufwerk auswählen können.

2. Wählen Sie das Logo aus und klicken Sie auf **Auswählen**.

   Das ausgewählte Logo wird dem Bereich „Logos verwalten“ hinzugefügt.

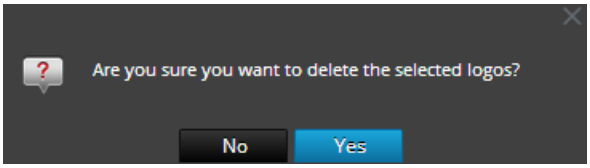
## Löschen eines Logos

**Um ein Logo zu löschen, führen Sie die folgenden Schritte aus:**

1. Führen Sie in der Registerkarte **Logos verwalten** einen der folgenden Schritte aus:

   - Wählen Sie das Logo aus und klicken Sie auf −.
   - Klicken Sie bei gedrückter STRG-Taste, um mehrere Logos auszuwählen, und klicken Sie auf −.

   Ein Bestätigungsdialogfeld wird angezeigt.




2. Wenn Sie das Logo löschen möchten, klicken Sie auf **Ja**.

   Das ausgewählte Logo wird aus dem Bereich „Logos verwalten“ gelöscht.

## Festlegen des Standardlogos

Um ein Logo als Standard festzulegen, führen Sie die folgenden Schritte aus:

Wählen Sie in der Registerkarte **Logos verwalten** ein Logo aus und klicken Sie auf Set default.

Das ausgewählte Logo wird als Standardlogo für den RE-Service festgelegt.

## Auswählen eines Logos

Um eine Logo auszuwählen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **ADMIN** > **Berichte** aus.

   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Berichte**.

   Die Ansicht „Berichte“ wird angezeigt.

3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus.

4. Klicken Sie auf  > **Geplante Berichte anzeigen**.

   Die Registerkarte „Geplante Berichte anzeigen“ wird angezeigt.

5. Wählen Sie einen geplanten Bericht aus und klicken Sie auf  > **Plan bearbeiten**.

   Die Ansichtsregisterkarte Einen Bericht planen wird angezeigt.

6. Klicken Sie im Bereich „Logo“ auf **Logo ändern**.

   Das Dialogfeld Logo ändern wird angezeigt.

7. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf **Neues Logo hochladen**, um ein weiteres Logo hochzuladen.
   - Wählen Sie ein Logo aus der Liste aus.

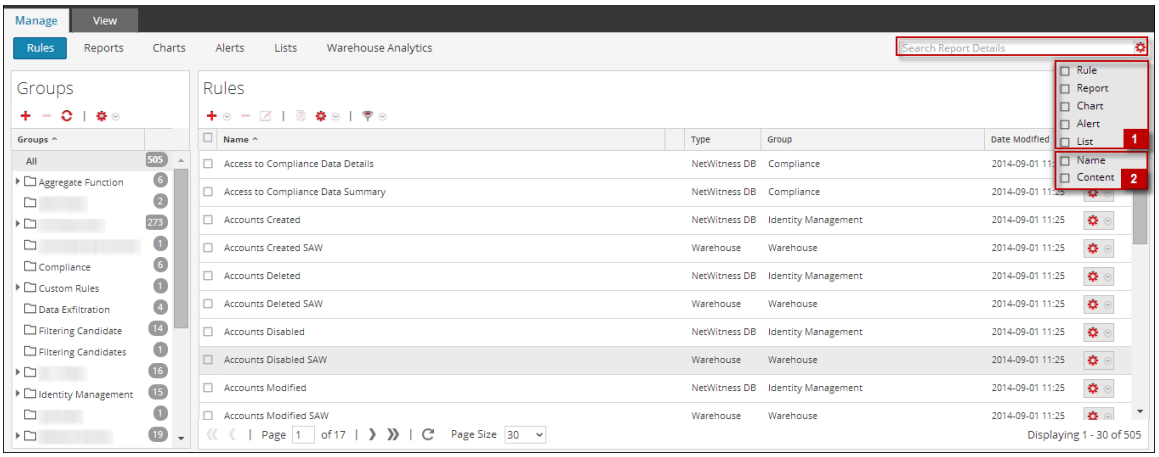
8. Klicken Sie auf **Auswählen**.
   Das ausgewählte Logo ist im Bereich „Logo“ verfügbar.

## Reporting-Details suchen

In diesem Abschnitt wird beschrieben, wie eine Schlüsselwortsuche nach Namen und Inhalten für die einzelnen Reporting-Komponenten durchgeführt wird. Sie können für jede der Reporting-Komponenten (Regel, Bericht, Diagramm, Warnmeldung, Liste) in der Reporting-Oberfläche eine Schlüsselwortsuche nach Name und Inhalt durchführen.

**Hinweis:** Sie können nicht nach einem Datum oder numerischen Werten suchen.

In der folgenden Abbildung sind die Suchparameter zu sehen, die im Reporting-Modul verfügbar sind:




Dies sind die Suchparameter, die in der Reporting-Oberfläche verfügbar sind.

1. Suche nach Entitäten (Regel, Bericht, Diagramm, Warnmeldung, Liste).
2. Suche nach Entitäten anhand von Name oder Inhalt.

**Hinweis:** Bei Suchvorgängen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Beispielsweise ergibt „Abgeschlossen“ die gleichen Suchergebnisse wie „abgeschlossen“.

## Voraussetzungen

Im Reporting-Modul können Sie eine Schlüsselwortsuche nach Name und Inhalt (Definition) durchführen. In diesem Zusammenhang bezieht sich „Inhalt“ auf die Definition der einzelnen Reporting-Komponenten. Es handelt sich also beispielsweise um den Wert, der in der Regel, dem Bericht, dem Berichtsplan, dem Diagramm oder dem Warnmeldungsbereich definiert ist. Außerdem können Sie die Priorität des Suchvorgangs ändern, indem Sie einige oder alle der folgenden Komponenten auswählen: Regel, Bericht, Diagramm, Warnmeldung oder Liste.

**Hinweis:** Die Suche nach den Listenwerten und Listenpfaden, die im Bereich mit den Plandefinitionen gespeichert sind, ist nicht möglich.

Wenn Sie beispielsweise nach dem Regelnamen (ExpertRule) suchen möchten, müssen Sie im Drop-down-Menü **Filteroptionen** die Option **Regel, Name und Inhalt** auswählen, damit alle Regelnamen entsprechend der Suche angezeigt werden. Auf die gleiche Weise können Sie nach der Definition eines Berichts, eines Diagramms, einer Warnmeldung oder einer Liste suchen.

Um von der Registerkarte „Managen“ aus nach Berichtsdetails zu suchen, führen Sie die folgenden Schritte aus:

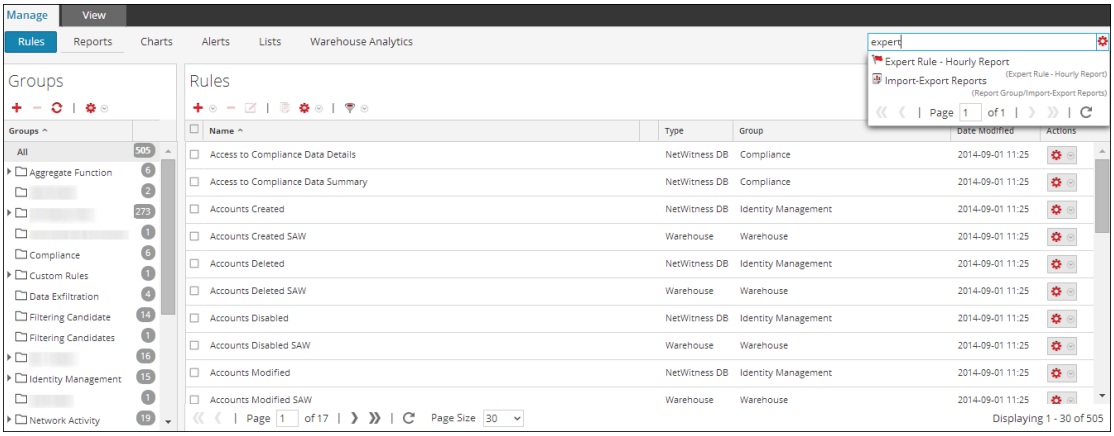
1. Wählen Sie **Monitor** > **Berichte** aus.

   Die Registerkarte **Managen** wird angezeigt.

2. Klicken Sie auf  und wählen Sie das Kriterium für die Suche aus.

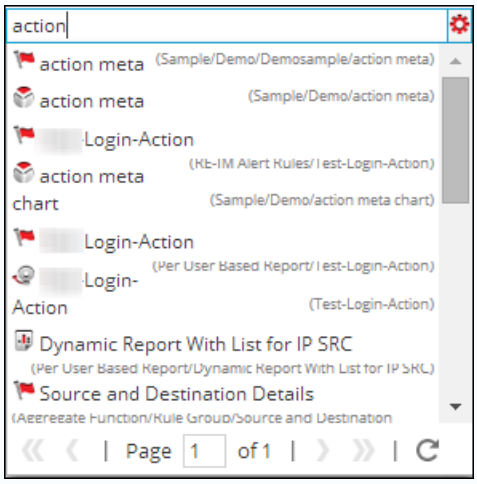
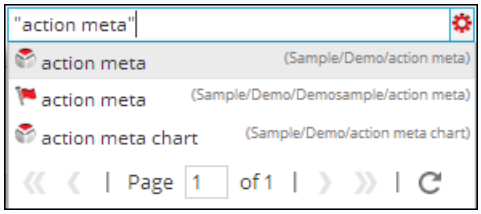
3. Geben Sie in das Feld **Suchen** den Text ein, nach dem Sie suchen möchten.

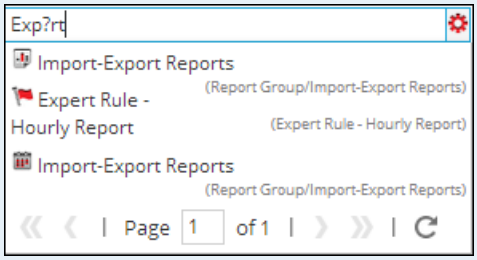
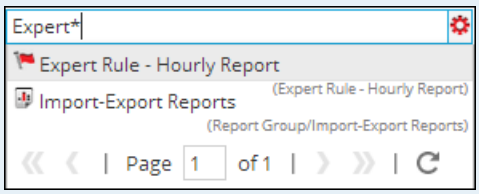
   Die Drop-down-Liste „Suchen“ wird angezeigt:

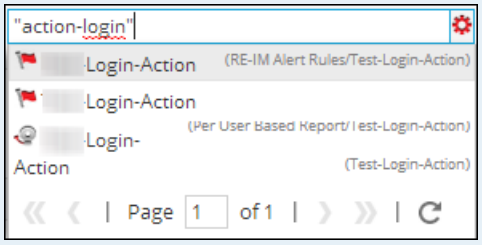


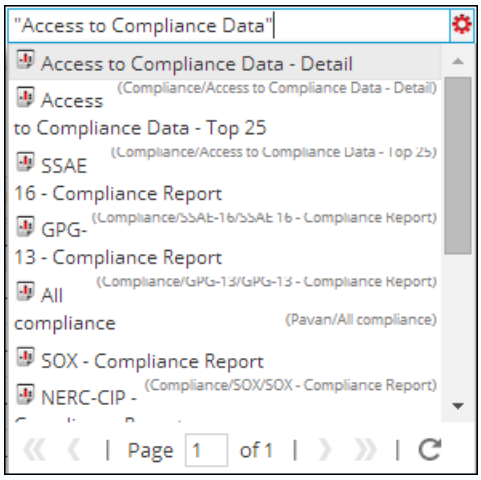
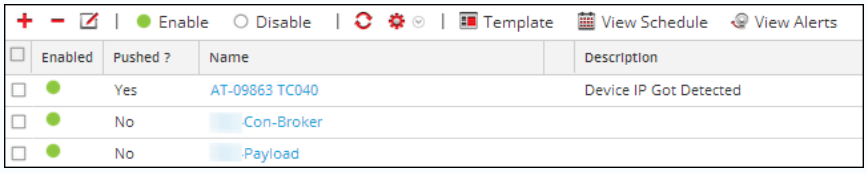

## Suchsyntax und verschiedene Suchtypen

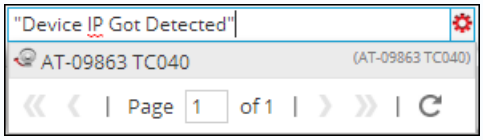
In der folgenden Tabelle werden die Suchsyntax und die möglichen Suchtypen erläutert, die in der Reporting-Oberfläche durchgeführt werden können.

| Suchtypen | Beschreibung |
| --- | --- |
| Suche nach einem Wort oder einer Wortgruppe | **Suche nach einem Wort:**<br>Wenn Sie nach einem Wort wie etwa „Aktion“ oder „Metadaten“ suchen möchten, geben Sie das Wort in das Suchfeld ein.<br>In der folgenden Abbildung sind die Suchergebnisse für das Wort **Aktion** zu sehen.<br>  <br><br>**Suche nach einer Wortgruppe:**<br>Wortgruppen wie etwa „Aktion Metadaten“ werden bei der Suche in doppelte Anführungszeichen gesetzt. Wenn Sie nach einer Wortgruppe suchen möchten, geben Sie die Wörter in das Suchfeld ein und setzen Sie an den Anfang und an das Ende der Wortgruppe doppelte Anführungszeichen.<br>In der folgenden Abbildung sind die Suchergebnisse für die Wortgruppe „Aktion Metadaten“ zu sehen.<br>  <br> |

| Suchtypen | Beschreibung |
|---|---|
| Platzhaltersuche (einzelne Zeichen / mehrere Zeichen / Sonderzeichen)<br><br>Das Fragezeichen „**?**“ ersetzt bei der Suche ein einzelnes Zeichen und das Sternchen „*“ ersetzt mehrere Zeichen. | **Suche mit Platzhalter für einzelne Zeichen:**<br><br>Bei der Suche mit Platzhalter für einzelne Zeichen wird nach Wörtern gesucht, die dem Suchwort entsprechen und anstelle des Platzhalters ein beliebiges Zeichen haben. Um beispielsweise nach „abmelden“ oder „anmelden“ zu suchen, verwenden Sie diese Suchsyntax:<br>a?melden<br><br>In der folgenden Abbildung sind die Suchergebnisse für die Platzhaltersuche **a?melden** zu sehen.<br>  <br><br>**Suche mit Platzhalter für mehrere Zeichen:**<br><br>Bei der Suche mit Platzhalter für mehrere Zeichen wird nach Wörtern gesucht, die anstelle des Platzhalters keine oder mehrere Zeichen haben. Um beispielsweise nach „Experte“ oder „Experten“ zu suchen, verwenden Sie diese Suchsyntax:<br><br>Experte*<br><br>In der folgenden Abbildung sind die Suchergebnisse für die Platzhaltersuche **Experte*** zu sehen.<br>  |

| Suchtypen | Beschreibung |
| --- | --- |
| | **Suche mit Sonderzeichen:**<br><br>Während der Suche werden bestimmte Satz- und Sonderzeichen ignoriert (@#$%^&*(){}"~=+-[]\?|!:,.). Beispielsweise wird eine Suche nach „aktion-login“ während der Suche als „aktion“ „login“ interpretiert. Wenn also Regeln mit den Namen „aktion-login“ und „aktion@login“ vorhanden sind und nach „aktion-login“ gesucht wird, werden als Suchergebnis beide Regeln ausgegeben.<br><br>  |

| Suchtypen | Beschreibung |
|---|---|
| Suche nach Name oder Inhalt | **Suche nach Name:**<br>Wenn Sie nach dem Namen eines Berichts suchen möchten, wählen Sie aus dem Drop-down-Menü mit den Filteroptionen die Felder **Bericht** und **Name** aus. Wenn Sie beispielsweise nach dem Berichtnamen „Access to Compliance Data“ mit mehreren Regeln suchen, können Sie folgende Suchsyntax verwenden:<br>„Access to Compliance Data“<br>**Hinweis:** Wenn Sie nach einem Bericht suchen, können Sie auch nach den Berichtsplänen suchen.<br>In den Suchergebnissen ist der Bericht mit dem gesuchten Namen enthalten.<br>  <br><br>**Suche nach Inhalt:**<br>Wenn Sie nach dem Inhalt einer Warnmeldung, also nach der Warnmeldungsbeschreibung, suchen möchten, wählen Sie aus dem Drop-down-Menü mit den Filteroptionen die Felder **Warnmeldung** und **Inhalt** aus. Wenn Sie beispielsweise nach der Warnmeldungsbeschreibung „Device IP Got Detected“ suchen, können Sie folgende Suchsyntax verwenden:<br>„Device IP Got Detected“<br>  <br><br>Die Suche gibt das Ergebnis zurück, in dem der spezifische Inhalt vorhanden ist. |

| Suchtypen | Beschreibung |
| --- | --- |
| |  |

# Fehlerbehebung

Dieser Abschnitt enthält Anweisungen für das Troubleshooting bei Problemen, die auftreten können, wenn Sie das Modul Reporting inNetWitness Suite verwenden.

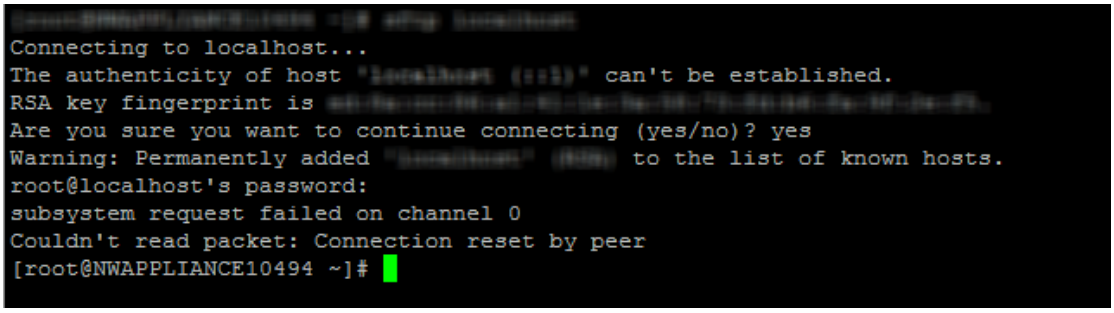
## Troubleshooting bei Problemen vor dem Konfigurieren des SFTP-Servers

### Verfahren

Führen Sie die folgenden Schritte aus, wenn Probleme mit einem konfigurierten Linux-SFTP-Server auftreten:

1. Wenn die Berichtausgabe für den konfigurierten SFTP-fehlschlägt, müssen Sie sich mit SSH mit dem FTP-Server verbinden und versuchen, eine lokale Verbindung herzustellen, um zu überprüfen, ob SFTP ordnungsgemäß funktioniert.

   Verbinden Sie sich mit dem SFTP-Server:

2. Wenn die lokale Verbindung fehlschlägt, öffnen Sie die Datei **sshd_config> vi /etc/ssh/sshd_config.**
3. Suchen Sie in der Datei nach folgendem Eintrag:

   ```
   # override default of no subsystems
   Subsystem sftp /usr/libexec/openssh/sftp-server
   ```

4. Wenn dieser Eintrag nicht vorhanden ist, fügen Sie die beiden in Schritt 3 genannten Zeilen am Ende der Datei hinzu und **Speichern** Sie sie.
5. Starten Sie den Service über **SSH > service sshd restart** neu.
6. Versuchen Sie erneut, die SFTP-Verbindung herzustellen.
7. Vergewissern Sie sich, dass der SFTP-Port nicht von der Firewall der SA-Server-Appliance blockiert wird. Aktualisieren Sie die iptables-Regeln, um den SFTP-Port freizugeben

## Definitionen:

**Strenger Parser**: Strenger Parser (nicht veraltet) erwartet, dass die Abfragesyntax korrekt eingegeben wurde.
Verwenden Sie für alle Metadaten vom Typ „Text“ Anführungszeichen, z. B. Benutzername = 'Benutzer1'.
Verwenden Sie für IP-Adressen, Ethernet-Adressen und numerische Metadatentypen keine Anführungszeichen. z. B. service = 80 &&
ip.src = 192.168.1.1.
Verwenden Sie für die Metadatentypen Datum und Uhrzeit Anführungszeichen,
wenn das Datums- und Uhrzeitformat 'YYYY-MM-DD HH:MM:SS' ist.
Wenn das Datums- und Uhrzeitformat 1448034064 (Anzahl der Epochensekunden (seit 1. Jan. 1970)) ist, verwenden Sie keine Anführungszeichen.
Die Berichtsabfragen werden mit strengem Parser analysiert, wenn der Konfigurationswert von /sdk/config/query.parse in NWDB-Core-Services **streng** ist.

**Nicht strenger Parser**: Ein nicht strenger Parser (veraltet) erwartet nicht, dass die Abfragesyntax typkorrekt ist, d. h. die Werte für die Metadaten der Typen Text und numerisch können in Anführungszeichen gesetzt werden oder nicht, unabhängig vom Metadatentyp.

Beispiel: Benutzername ist ein Metadatum vom Typ Zeichenfolge, daher können die Werte in Anführungszeichen gesetzt werden oder nicht. Also ist sowohl die Syntax Benutzername = 'Benutzer1' als auch Benutzername = Benutzer gültig.

Die Berichtsabfragen werden mit nicht strengem Parser analysiert, wenn der Konfigurationswert von /sdk/config/query.parse in NWDB-Core-Services **veraltet** ist.

**Hinweis:** Die NWDB-Regel, in der Klausel entsprechend in Anführungszeichen gesetzt wird, wenn die Syntax ein ungültiges Anführungszeichen enthält. Beispiel: Bei ungültigen Metadaten oder fehlenden Trennzeichen werden Status und Fehlermeldung entsprechend aktualisiert.

# Anhang

Dieser Abschnitt enthält detaillierte Informationen über die unterstützten Aggregatfunktionen, Regelsyntax, erweiterte Regelabfragesyntax in Reporting und Aufgabenplaner für Warehouse Reporting.

# Regelsyntax

In diesem Abschnitt wird die von der Reporting Engine unterstützte Regelsyntax beschrieben.

### NWDB-Regelsyntax

Die NWDB-Regel zählt zu der in der Reporting Engine unterstützten Regelsyntax. Informationen zur Verbesserung der Ausführungszeit Ihrer Reportingentitäten finden Sie unter „Reportingrichtlinien“ im Abschnitt Reporting-Übersicht.

Eine Regel ist eine Funktion, die den Ergebnissatz einer Regel manipuliert, um die Ausgabe in einem Bericht sinnvoller zu gestalten oder einer Regel über die Abfrage und Anzeige von Daten hinaus zusätzliche Funktionalität zu verleihen. Eine beliebige Kombination dieser Regelaktionen kann verwendet werden, um eindeutige und relevante Repräsentationen der von NetWitness Suite gesammelten Informationen zu erstellen.

Die Reporting Engine unterstützt die folgenden Kategorien der NWDB-Datenquellen-Regelsyntax:

- **select**-Klausel
  - Nichtaggregatregel
  - Aggregatregel
- **alias**
- **where**-Klausel
- **where**-Klauseloperatoren
- **Then**-Klausel
- Feld **Grenzwert**
- Regelaktionen
- Regeloperatoren

## Select-Klausel

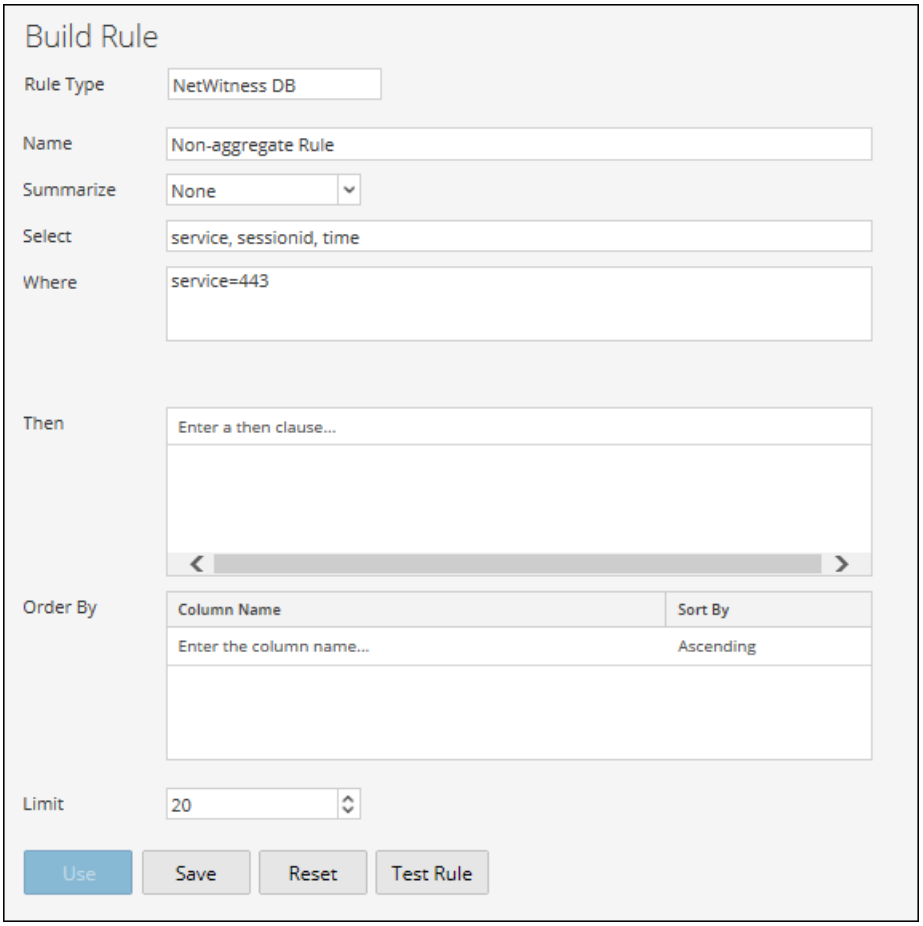
Die Select-Klausel ist eine durch Komma getrennte Liste von Werten. Beispiel: select sessionid, time, service.

Es gibt zwei Arten von select-Klauseln/Regeln für NWDB-Regeln:

- Nichtaggregatregel
- Aggregatregel

## Nichtaggregatregel

Wenn Sie eine Regel ohne eine Gruppierung definieren möchten, wählen Sie im Feld „Zusammenfassen“ die Option „Keine“ aus. In einer Nichtaggregatregel können Sie in der *Select*-Klausel eine beliebige Anzahl von Metadaten auswählen. Beispiel: select service, sessionid, time.

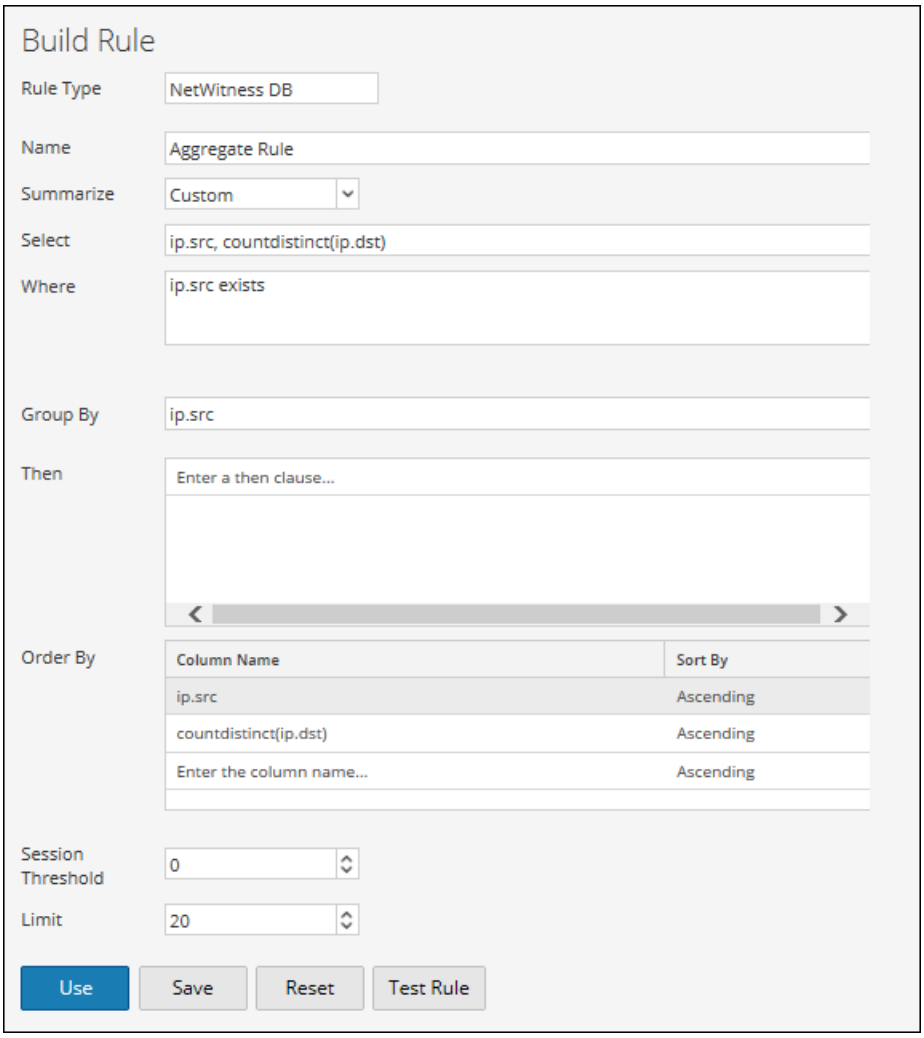



## Aggregatregel

Wenn Sie bestimmte Metadaten und den zugehörigen Aggregatwert abfragen möchten, müssen Sie die Aggregatregel verwenden. Um ein Aggregat zu erhalten, müssen Sie im Feld **Zusammenfassen** einen der drei Metadatensätze (Ereignisanzahl, Paketanzahl, Sitzungsgröße) oder „Benutzerdefiniert“ auswählen, um der *Select*-Klausel eine Aggregatfunktion hinzuzufügen. Beispiel: select ip.src, sum (ip.dst). Wenn die benutzerdefinierte Aggregatregel aktiviert ist, werden die folgenden Felder in der Benutzeroberfläche ausgefüllt:

- Gruppieren nach
- Sortieren nach
- Sitzungsschwellenwert

Die folgende Abbildung zeigt die Ansicht „Regel erstellen“ für die Aggregatregel.




Es gibt zwei Typen von Aggregatwerten, die abgefragt werden können:

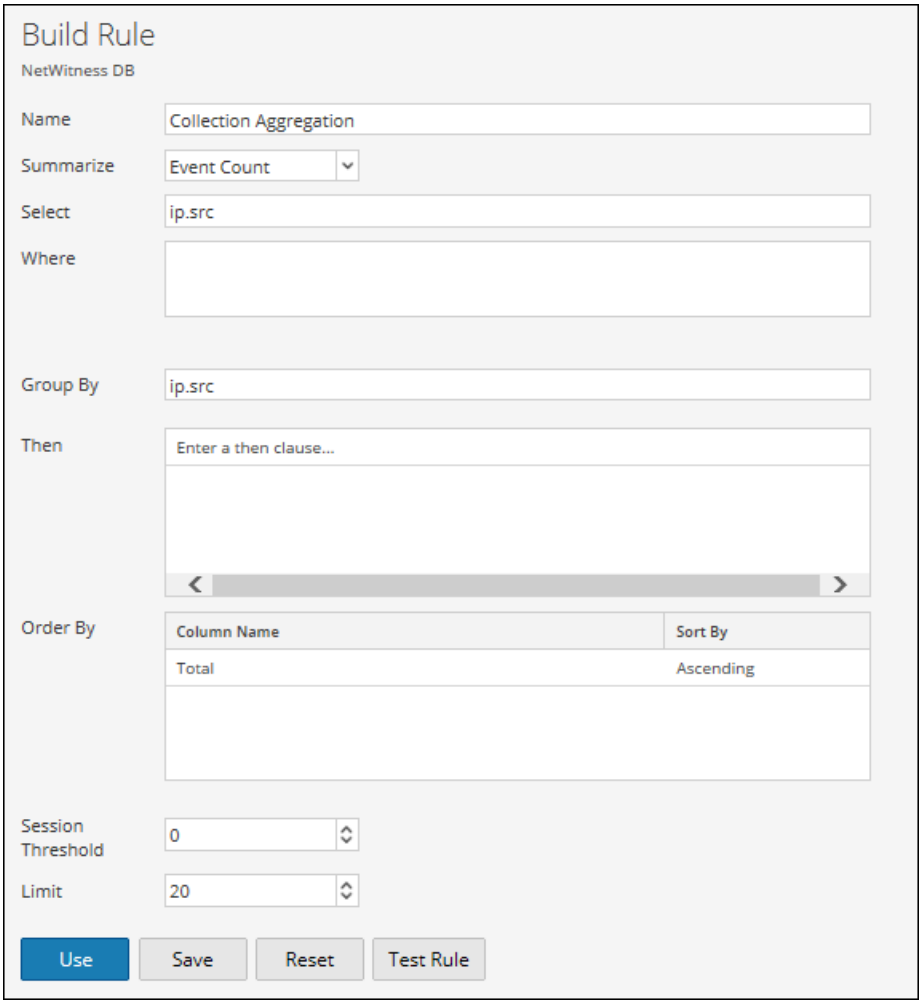
- Sammlungsaggregation
- Metaaggregation

## Sammlungsaggregation

Mit der Sammlungsaggregation können Sie Aggregate zu Ereignis, Sitzung oder Paketen abrufen. Die folgenden Werte können in einer Sammlungsaggregation abgefragt werden:

- **Ereignisanzahl:** Gesamtanzahl der Ereignisse
- **Paketanzahl**: Gesamtanzahl der Pakete
- **Sitzungsgröße:** Die gesamte Sitzungsgröße.

Diese Optionen sind im Feld „Zusammenfassen“ aufgelistet und eine beliebige Option kann in einer Regel ausgewählt werden.
Beispiel: Wählen Sie im Feld „Zusammenfassen“ ein Sammlungsaggregat (Ereignisanzahl, Paketanzahl oder Sitzungsgröße) sowie „ip.src“ aus.




## Metaaggregation

Mit der Metaaggregation können Sie Aggregate von Metawerten abrufen. Folgende Metaaggregatfunktionen werden unterstützt:

- sum(meta)
- count(meta)
- countdistinct(meta)
- min(meta)
- max(meta)

- avg(meta)
- first(meta)
- last(meta)
- len(meta)
- distinct(meta)

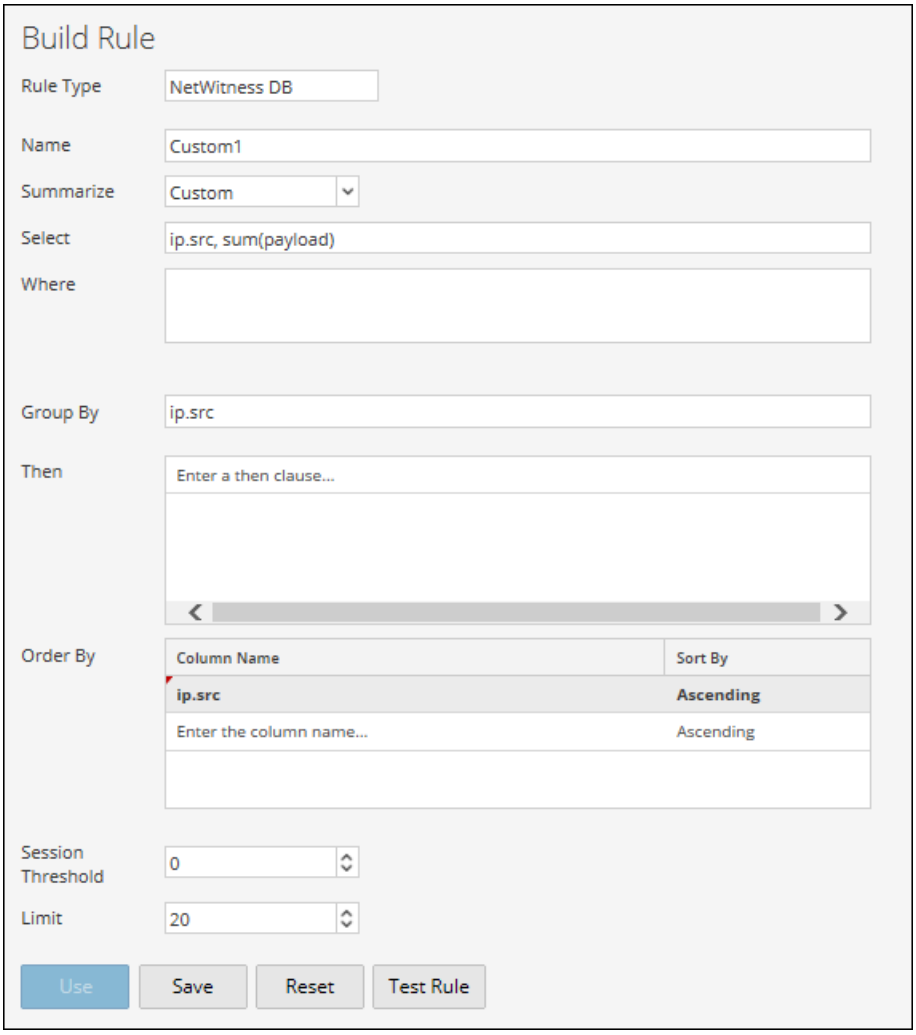
## Unterstützte Metaaggregatfunktionen

Der NWDB-Service unterstützt in dieser Version die folgenden Metaaggregatfunktionen und die folgende Syntax.

| Syntax | Funktion |
|---|---|
| sum (<meta>) | Die Summe aller Metawerte.<br>Beispiel: Wenn Sie das Feld „sum(payload)“ in der Select-Klausel angeben, wird als Ergebnissatz die Summe der Nutzdatengröße zurückgegeben.<br>**Hinweis:** Das Metafeld, das für die Aggregatfunktion sum ausgewählt wird, muss einen numerischen Datentyp haben. |
| count (<meta>) | Die Gesamtzahl der Metafelder, die zurückgegeben würden<br>Beispiel: Wenn Sie das Feld „count(ip.dst)“ in der select-Klausel angeben, gibt der Ergebnissatz die Häufigkeit an, mit der ein Wert für „ip.dst“ zurückgegeben wird. |
| countdistinct (<meta>) | Die Gesamtzahl der distinct-Metadatenfelder, die zurückgegeben werden. Beispiel: Wenn Sie das Feld „countdistinct(ip.dst)“ in der select-Klausel angeben, gibt der Ergebnissatz an, wie oft ein distinct-Wert für ip.dst zurückgegeben wird. |
| min (<meta>) | Das Minimum für alle Metawerte.<br>Beispiel: Wenn Sie das Feld „min(payload)“ in der select-Klausel angeben, wird als Ergebnissatz das Minimum der Nutzdatengröße zurückgegeben. |
| max (<meta>) | Das Maximum für alle Metawerte.<br>Beispiel: Wenn Sie das Feld „max(payload)“ in der select-Klausel angeben, wird als Ergebnissatz das Maximum der Nutzdatengröße zurückgegeben. |

| Syntax | Funktion |
|---|---|
| avg<br>(<meta>) | Der Durchschnitt aller Metawerte.<br>Beispiel: Wenn Sie das Feld „avg(payload)“ in der select-Klausel angeben, wird als Ergebnissatz der Durchschnitt der Nutzdatengröße zurückgegeben.<br>**Hinweis:** Das Metafeld, das für die Aggregatfunktion avg ausgewählt wird, muss einen numerischen Datentyp haben. |
| first<br>(<meta>) | Das erste Auftreten des Metawerts.<br>Beispiel: Wenn Sie das Feld „first(ip.src)“ in der select-Klausel angeben, ist der Ergebnissatz das erste Auftreten von „ip.src“ in dieser Gruppe. |
| last<br>(<meta>) | Das letzte Auftreten des Metawerts.<br>Beispiel: Wenn Sie das Feld „last(ip.src)“ in der select-Klausel angeben, ist der Ergebnissatz das erste Auftreten von „ip.src“ in dieser Gruppe. |
| len(<meta>) | Konvertiert alle Feldwerte in eine UInt32-Länge, statt den tatsächlichen Wert anzugeben. Diese Länge entspricht nicht der Länge der in der Metadatenbank gespeicherten Struktur, sondern der für die Speicherung des tatsächlichen Werts erforderlichen Anzahl von Byte.<br>Für den Metawert „NetWitness“ wird beispielsweise die Länge 10 zurückgegeben. Für alle IPv4-Felder, z. B. ip.src, wird stets 4 Byte zurückgegeben. |
| distinct<br>(<meta>) | Die unterschiedlichen Werte der Metadaten.<br>Beispiel: Wenn Sie das Feld „distinct(ip.src)“ in der select-Klausel angeben, umfasst der Ergebnissatz sämtliche unterschiedlichen „ip.src“in dieser Gruppe. |

Sie müssen im Feld „Zusammenfassen“ die Option „Benutzerdefiniert“ auswählen und in der select-Klausel die Metadaten und Metaaggregatfunktionen bereitstellen.




**Hinweis:** In einer WHERE-Klausel können keine Metaaggregatfunktionen verwendet werden. Zum Filtern von Aggregatfunktionen können Sie Regelaktionen wie „min_threshold/max_threshold“ nutzen. Bei Verwendung von „Gruppieren nach“ wird eine verfeinerte WHERE-Klausel empfohlen, um eine bessere Regelperformance zu erhalten.

## Aggregieren von Abfragen für mehrere Metadaten

Führen Sie die folgenden Schritte aus, um Abfragen für mehrere Metadaten zu aggregieren:

1. Wählen Sie **Monitor** > **Berichte** aus.

   Die Registerkarte „Managen“ wird hervorgehoben und die Ansicht **Rules** angezeigt.

2. Klicken Sie in der Symbolleiste „Regeln“ auf + > **NetWitnessDB**.

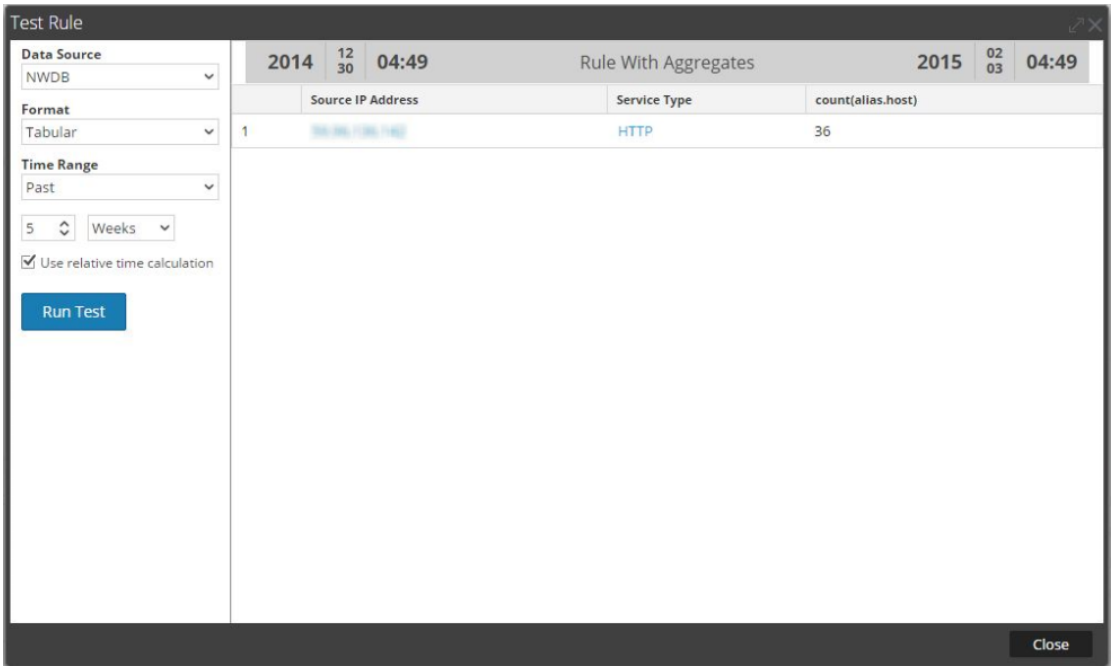
   Geben Sie beispielsweise die folgenden Metadaten in die unten hervorgehobenen Felder ein:

**SELECT**: ip.src, service, count(alias.host)
ALIAS: Quell-IP-Adresse, Servicetyp, count(alias.host)
**WHERE**: ip.src = 59.96.136.142

**Hinweis:** Im Aliasfeld können Sie einen Namen für Spalten eingeben, die in der SELECT-Klausel verwendet werden. Wenn Sie den Alias für eines der Felder in der Select-Klausel nicht angeben, wird die Standardbeschreibung verwendet. Wenn die Select-Klausel z. B. Feld1, Feld2, Feld3, Feld4 aufweist und Alias nur Feld1, Feld3, Feld4 aufweist, wird für Feld2 eine Standardbeschreibung verwendet.

3. Klicken Sie auf die Schaltfläche **Regel testen** unten auf der Seite.

   Die Seite „Regel testen“ wird angezeigt.




## Zusammenfassung

„Zusammenfassen“ bestimmt den Typ der Zusammenfassung oder Aggregation für die Regel.

| Name | Konfigurationswert |
| --- | --- |
| Zusammenfassen | Wählen Sie zum Abfragen von Metadaten ohne eine benutzerdefinierte Gruppierung folgende Option aus:<br>• **Ohne:** In diesem Fall werden die Daten nach Sitzung gruppiert.<br><br>Zum Abrufen von Aggregaten zu Sammlungen (Sitzungen/Ereignisse/Pakete) wählen Sie eine der folgenden Optionen aus:<br>• Ereignisanzahl: Gesamtanzahl der Ereignisse<br>• **Paketanzahl**: Gesamtanzahl der Pakete<br>• **Sitzungsgröße**: Gesamte Sitzungsgröße<br><br>Zum Abrufen auf Metadaten basierender Aggregate wählen Sie Folgendes aus:<br>• **Benutzerdefiniert**: Dadurch wird angegeben, dass die erwartete Metaaggregatfunktion in der select-Klausel der Regel definiert ist. |

## Sortieren nach

„Sortieren nach“ legt fest, wie der Ergebnissatz sortiert wird.

| Name | Konfigurationswert |
| --- | --- |
| Spaltenname | Der **Spaltenname** ist der Name der Spalten, nach denen Sie die Ergebnisse sortieren möchten. Standardmäßig ist der Wert leer. Wenn Sie auf eine Spalte klicken, wird der Wert auf Basis des Felds Zusammenfassen aufgefüllt.<br>• Bei „Keine“ und „Benutzerdefiniert“ wird der Wert auf Basis der Einträge aufgefüllt, die Sie im Feld Auswählen vorgenommen haben. Sie können aus dieser Liste auswählen oder einen benutzerdefinierten Namen hinzufügen.<br>• Die akzeptierten Werte für die Ereignisanzahl, Paketanzahl und Sitzungsgröße sind Gesamt und Wert.<br>• Gesamt – nach Aggregatwert sortieren<br>• Wert – nach Gruppe nach Meta sortieren |

| Name | Konfigurationswert |
| --- | --- |
| Sortieren nach | **Sortieren nach** bestimmt die Reihenfolge, in der Sie die Ergebnisse sortieren möchten. Folgende Werte sind möglich:<br>• Aufsteigende Reihenfolge<br>• Absteigende Reihenfolge |

## Sitzungsschwellenwert

Der Sitzungsschwellenwert ist die Optimierungseinstellung, mit der die Abstimmungssitzungen für jeden möglichen eindeutigen Wert für die ausgewählten Metadaten beendet werden. Der Schwellenwert ist eine ganze Zahl zwischen 0 (Standard) und 2147483647. Mit dem Schwellenwert 0 werden alle entsprechenden Sitzungen gesucht.

**Hinweis:** Wenn Sie einen Wert ungleich 0 angeben (einen Wert über 0), sind die Aggregatergebnisse ungenau. Deshalb kann dies nur verwendet werden, wenn Sie an eindeutigen Werten und nicht an Aggregatwerten interessiert sind.

## Unterstützte where-Klausel

| Syntax | Beschreibung |
| --- | --- |
| where <field1> [<field-operator>] < value1>,<value2>,<value3-value4> <logic-operator> <field2> usw. | Die where-Klausel ist eine durch Kommas getrennte Liste von Sprachfeldwerten und -bereichen, die von der Funktion NwValues verwendet wird. In der where-Klausel müssen Zeichenfolgenwerte in Apostrophe gesetzt werden. Beispiel: where username = 'admin' && service = 22. |
| where <field1> [<field-operator>] <List1> | Sie können eine Liste in der where-Klausel verwenden, wenn Sie mehrere Werte in den Bericht aufnehmen möchten. Beispiel: where ip.src exists && alias.host exists && alias.host contains $[User Reports/List of Alias Host]. Wenn Sie die Liste verwenden, muss sie im Format $[<path>/<List name>] angegeben werden. |

Stellen Sie sicher, dass in der where-Klausel die Syntax je nach Metadatentyp korrekt ist.
Beispiel:
Verwenden Sie für alle Metadaten vom Typ „Text“ Anführungszeichen, z. B.username = „user1“.
Verwenden Sie für alle IP-Adressen, Ethernetadressen und numerische Metadatentypen keine Anführungszeichen, z. B. service = 80
ip.src = 192.168.1.1. Verwenden Sie für die Metadatentypen Datum und Uhrzeit Anführungszeichen, wenn das Datums- und Uhrzeitformat 'YYYY-MM-DD HH:MM:SS' ist.
Wenn das Datums- und Uhrzeitformat 1448034064 (Anzahl der Epochensekunden (seit 1. Jan.1970)) ist, verwenden Sie keine Anführungszeichen.

**Hinweis:** Wenn die Liste in der Regel verwendet wird, stellen Sie sicher, dass die Listenwerte je nach Typ der verwendeten Metadaten in Anführungszeichen stehen oder nicht. Wenn Sie das Kontrollkästchen **Anführungszeichen werden für alle Werte eingefügt** auf der Seite „Listendefinition“ aktivieren (weitere Informationen finden Sie im Abschnitt „Erstellen von Listen oder Listengruppen“ in Konfigurieren einer Regel), werden alle Listenwerte in Anführungszeichen gesetzt.

## Unterstützte where-Klauseloperatoren

| Syntax | Beschreibung |
|---|---|
| = | Gibt Ergebnisse zurück, in denen das Feld gleich einem angegebenen Wert ist. Beispiel: tcp.dstport = 21-25,110 gibt Sitzungen mit den TCP-Zielports 21, 22, 23, 24, 25 oder 110 zurück. |
| != | Gibt Ergebnisse für Felder zurück, die den angegebenen Werten nicht entsprechen. Beispiel: eth.type !=0x0800 gibt Sitzungen außerhalb des Hex-Werts (Dezimalwert 2048) zurück, d. h. alle nicht IP-basierten Protokolle. |
| beginnt | Prüft einen Wert am Beginn eines Text- oder Binärfelds |
| enthält | Durchsucht einen Text- oder Binärwert nach einer Teilentsprechung |
| endet | Prüft einen Wert am Ende eines Text- oder Binärfelds |
| existiert | Wenn der Feldwert existiert, wird die Operation unabhängig vom Wert als „true“ ausgewertet. |
| !existiert | Wenn der Feldwert nicht existiert, wird die Operation unabhängig vom Wert als „true“ ausgewertet. |

| Syntax | Beschreibung |
|---|---|
| length | Wertet die Länge des Feldes aus. Beispiel: „username length 20-u“ gibt alle Benutzernamen zurück, die 20 oder mehr Zeichen lang sind. |
| regex | Führt eine Suche nach einem regulären Ausdruck anhand von Text- und Binärwerten durch |
| not | Der Operator NOT wird zum Negieren einer Klausel oder Bedingung verwendet. So zeigt (not(user.dst ends "$")) z. B. keine Werte für „Benutzerziel“ an. |

## Unterstützte then-Klausel

| Syntax | Beschreibung |
|---|---|
| then <rule action> | Die then-Klausel umfasst eine Regelaktion, die den ursprünglichen Ergebnissatz einer Regel manipuliert, um die Ausgabe in einem Bericht konkreter zu gestalten oder ihm über die Abfrage und Anzeige von Daten hinaus zusätzliche Funktionalität zu verleihen. Beispiel: dedup (Dateiname) |

## Feld Grenzwert

Gibt den Grenzwert an, der für die Abfrage gelten soll, wenn Daten aus der Datenbank abgerufen werden. Wenn ein Ergebnissatz nach Ereignisanzahl, Paketanzahl oder Sitzungsgröße sortiert wird, repräsentiert der Grenzwert die obersten (oder untersten) wiederzugebenden n Werte. Wenn die Ergebnismenge nicht
sortiert wird, werden die ersten n Werte wiedergegeben.

## Regelaktionen

Die NWDB-Datenquellen-Regelsyntax unterstützt die folgenden Regelaktionen:

- dedup
- filter_on
- filter_out
- lookup_and_add
- max_threshold

- min_threshold
- regex
- sum_count
- sum_values
- show_whats_new

## dedup (string field)

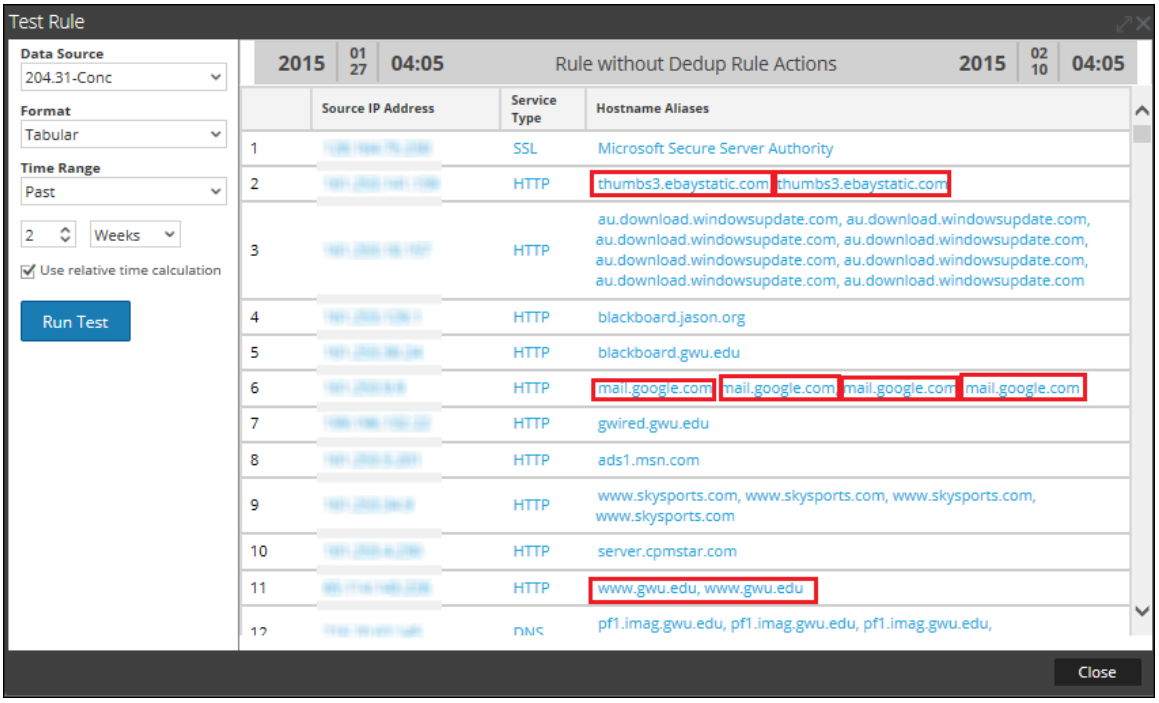
dedup entfernt Duplikateinträge in einem unsortierten Ergebnissatz und zeigt nur relevante Daten an. Die Regelaktion „dedup“ entfernt Duplikateinträge eines bestimmten Felds im Bericht, sodass nur das erste Auftreten dieses Werts im Bericht aufgeführt wird.

**Hinweis:** Die Regelaktion „dedup“ kann nicht mit einer Aggregatregel verwendet wird.

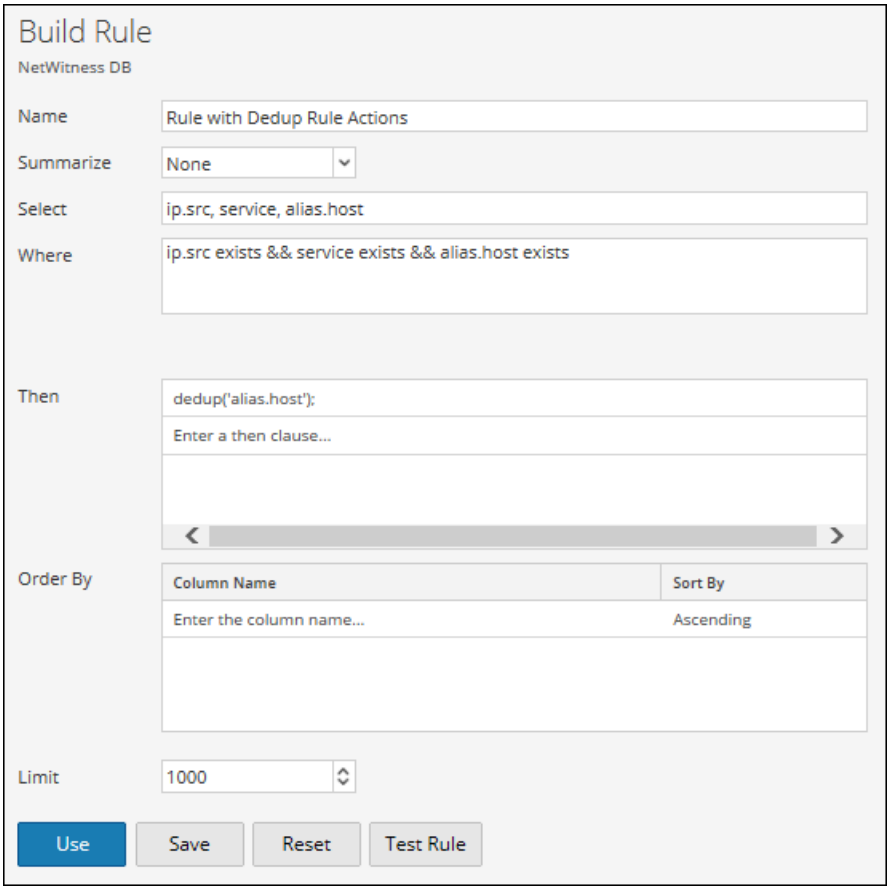
Beispielsweise sind die Metadaten, die von einer individuellen Sitzung erzeugt werden, oft repetitiv, besonders wenn Sie Sitzungen mit zahlreichen DNS-Lookups oder Websitzungen haben, bei denen für verschiedene Ressourcen (z. B. javascript und css) mehrmals auf denselben Host zugegriffen wird. Mit der Regelaktion „dedup“ können Sie Duplikateinträge des Hosts entfernen.

**Beispiel:**

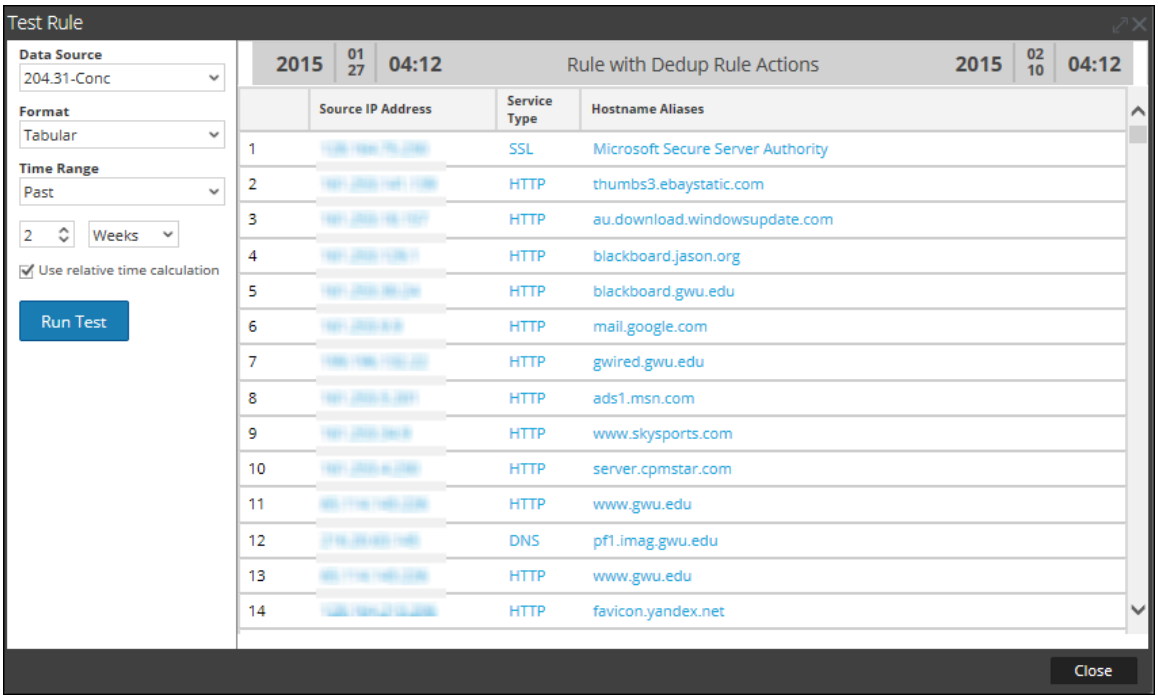
Das folgende Beispiel ist ein langer Ergebnissatz, der gekürzt werden kann, indem die Duplikatwerte in derselben Sitzung entfernt werden.



In der folgenden Abbildung sehen Sie, wie mit der Regelaktion „dedup“ Duplikateinträge aus dem Ergebnissatz entfernt werden.




Der Duplikatwert für jeden Eintrag im Regelergebnissatz wird auf einen Wert reduziert.




## filter_on (string filter, string field, bool matchExact)

`filter_on` entfernt Werte, in denen die `filter` -Kriterien nicht enthalten sind, aus dem Ergebnissatz. Wenn der Ergebnissatz mehrere Felder enthält, müssen Sie ein bestimmtes Feld auswählen, auf das der Filter angewendet wird. Wenn Sie zusätzliche Ergebnisse zu einem einzigen Ergebnissatz hinzufügen möchten, nehmen Sie eine Funktion wie „lookup_and_add“ auf.

Der Parameter matchExact bestimmt, ob die Übereinstimmung eine exakte Übereinstimmung ist oder eine Übereinstimmung enthält.

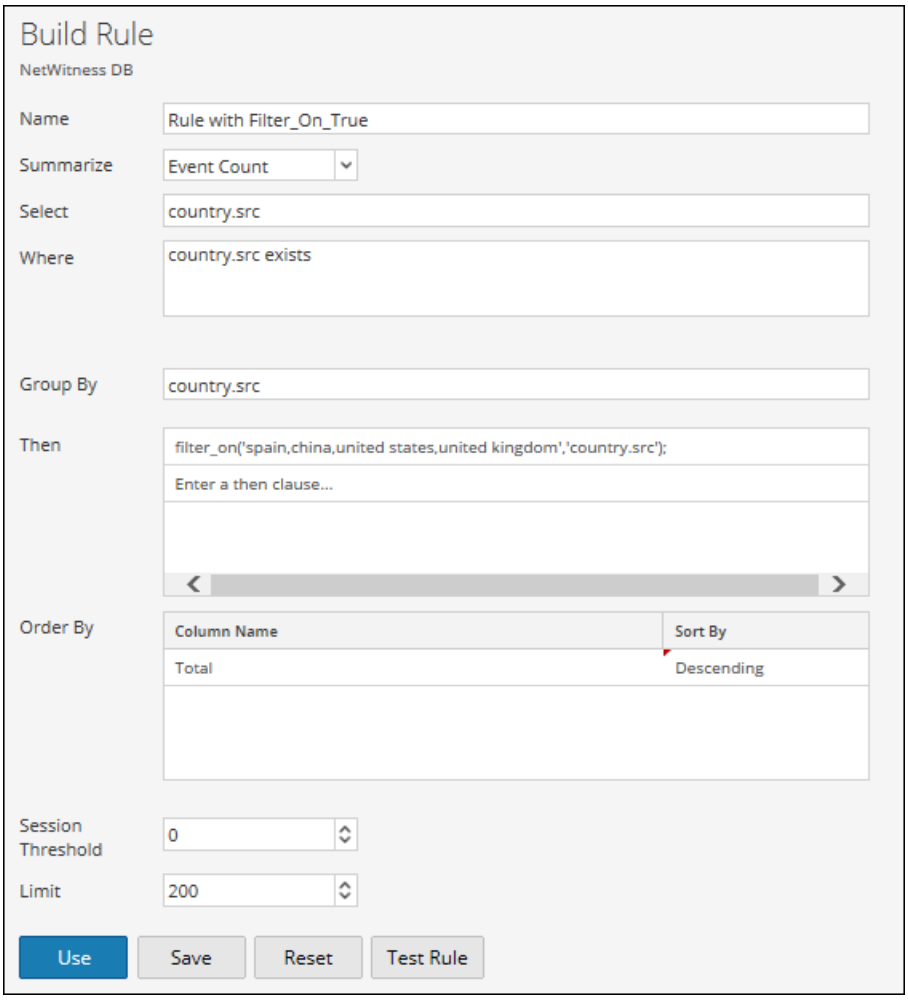
- Wenn matchExact auf `false,` eingestellt ist, wird jeder Wert, der den Filtertext enthält, als Entsprechung betrachtet.
- Wenn matchExact auf `true` eingestellt ist, werden nur Werte, die dem angegebenen Filtertext entsprechen, in den Ergebnissatz aufgenommen.

**Hinweis:** Wenn der Parameter „matchExact“ nicht angegeben wird, besteht das Standardverhalten der Regelaktion darin, dem im Filterparameter angegebenen Text genau zu entsprechen. Um anzugeben, dass Ergebnisse, die den Filtertext enthalten, im Ergebnissatz verbleiben müssen, ist es erforderlich, dass die Benutzer den Parameter „matchExact“ auf „false“ setzen.

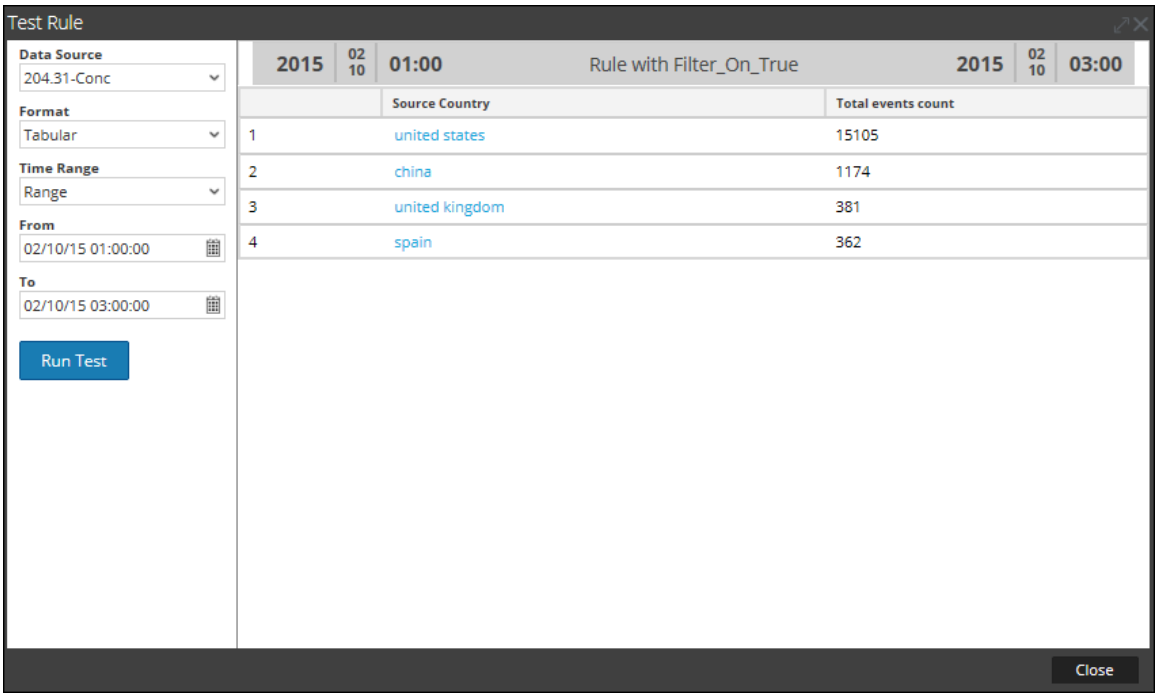
**Beispiel:**

Die folgende Abbildung zeigt die Länderliste und die Anzahl ihrer Ereignisse an.


In der folgenden Abbildung wird die Regelaktion „filter_on“ gezeigt, mit der alle Länder außer Spanien, China, den Vereinigten Staaten und dem Vereinigten Königreich aus dem Ergebnissatz herausgefiltert werden.




Die folgende Abbildung zeigt die Ausgabe mit der Regelaktion „filter_on“.




Eine weitere Möglichkeit, die Einträge aus dem Ergebnissatz herauszufiltern, besteht darin, eine Liste der Variablen zu erstellen, die Sie herausfiltern möchten. Beispielsweise können Sie eine Liste mit Großbritannien, Frankreich und Deutschland als Listenwerten erstellen. Diese Liste können Sie in der Regelaktion verwenden, um den gleichen Ergebnissatz abzurufen. Wenn Sie z. B. eine Liste namens COUNTRY_LIST erstellen, können Sie sie folgendermaßen verwenden:

```
filter_on ('$COUNTRY_LIST', 'country.src', 'false');
```

```
filter_out (string filter, string field)
```

```
filter_out (string filter, string field, bool matchExact)
```

filter_out entfernt die Werte, in denen die *filter*-Kriterien enthalten sind, aus dem Ergebnissatz. Wenn der Ergebnissatz mehrere Felder enthält, müssen Sie ein bestimmtes Feld auswählen, auf das der Filter angewendet wird (z. B. können Sie unter Verwendung von „lookup_and_add“ einem einzigen Ergebnissatz Ergebnisse hinzufügen).

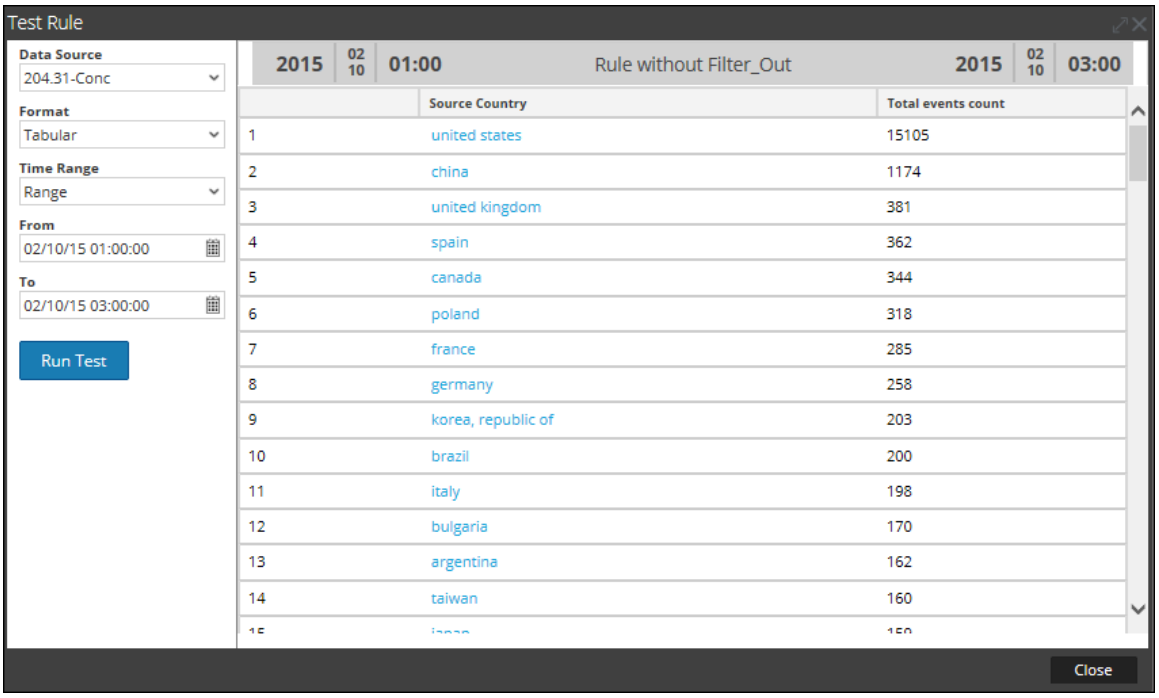
Der Parameter matchExact bestimmt, ob die Übereinstimmung eine exakte Übereinstimmung ist oder eine Übereinstimmung enthält.

- Wenn „matchExact“ auf „false“ eingestellt ist, wird jeder Wert, der den Filtertext enthält, als Entsprechung betrachtet.
- Wenn „matchExact“ auf „true“ eingestellt ist, werden nur Werte, die dem angegebenen Filtertext entsprechen, aus dem Ergebnissatz ausgeschlossen.

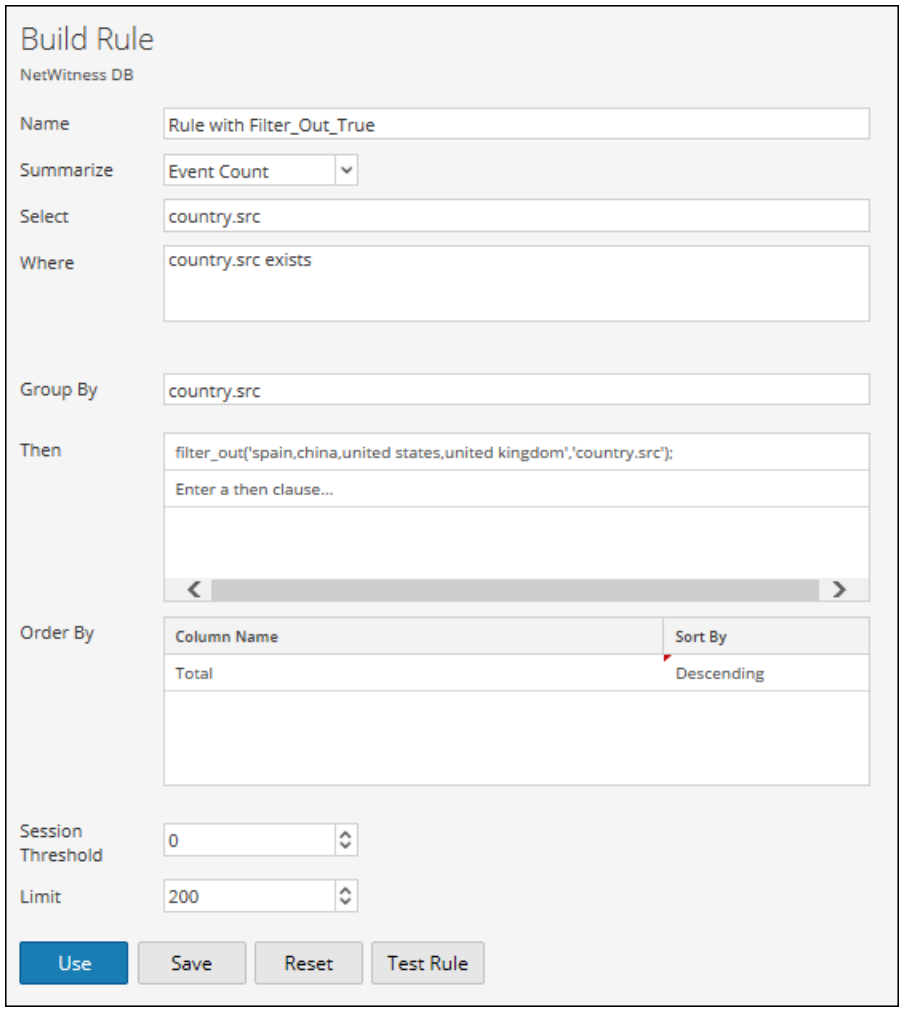
**Hinweis:** Wenn der Parameter `matchExact` nicht angegeben wird, besteht das Standardverhalten der Regelaktion darin, den im Filterparameter angegebenen Text genau abzustimmen. Um anzugeben, dass Ergebnisse, die den Filtertext enthalten, aus dem Ergebnissatz entfernt werden müssen, muss der Benutzer den Parameter `matchExact` auf „false“ setzen.

**Beispiel:**

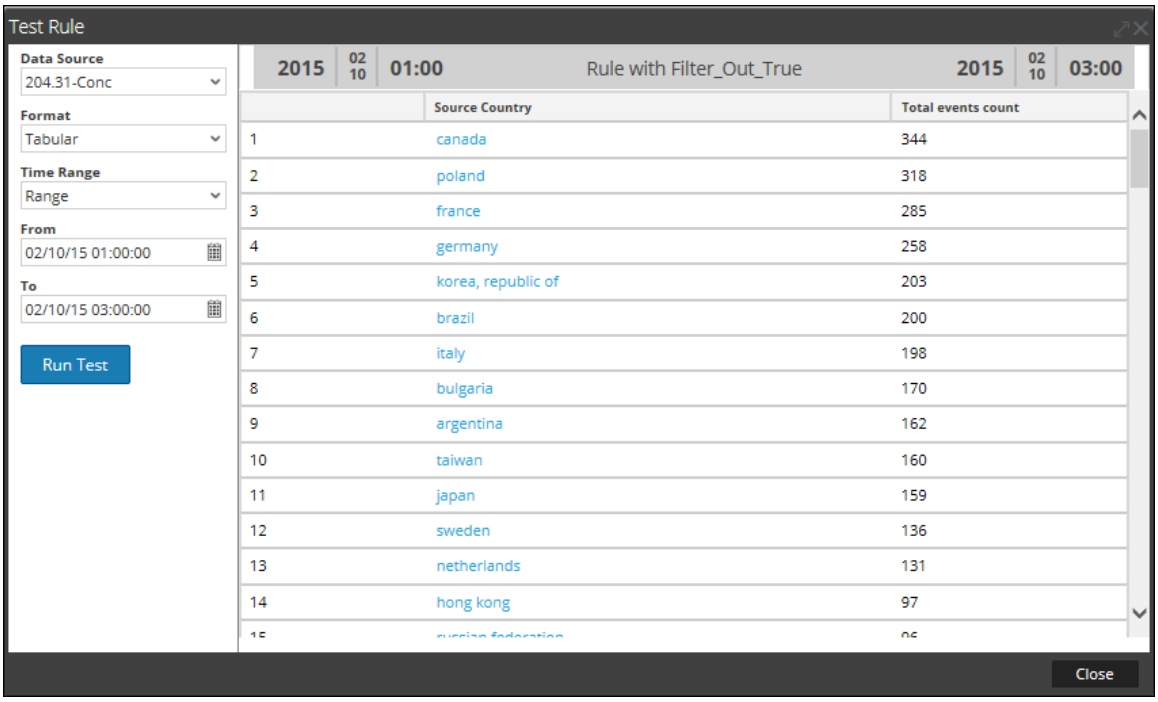
Die folgende Abbildung zeigt die Länderliste und die Anzahl ihrer Ereignisse an.




In der folgenden Abbildung sehen Sie die Regelaktion „filter_out“, mit der die Ereignisanzahl für Spanien, China, die Vereinigten Staaten und das Vereinigte Königreich aus dem Ergebnissatz entfernt wird.




Die folgende Abbildung zeigt die Ausgabe mit der Regelaktion „filter_out“.




```
lookup_and_add (string select, string field)
lookup_and_add (string select, string field, int limit)
lookup_and_add (string select, string field, int limit, boolean inherit)
lookup_and_add (string select, string field, int limit, boolean inherit,
string extraWhere)
lookup_and_add(string select, string field, int limit, boolean inherit,
string extraWhere, boolean aggregate)
```

Diese Regelaktion läuft iterativ durch eine Liste von Werten in einem Ergebnissatz und sucht zusätzliche Metadaten, mit denen die Beziehungen zwischen verschiedenen Elementen in einem Ergebnissatz näher beschrieben werden.

**Hinweis:** Die Regelaktion „lookup_and_add“ kann nicht mit einer Aggregatregel verwendet werden.

Der erste Parameter, „select“, gibt den Typ der Metadaten an, die den Elementen im Ergebnissatz hinzugefügt werden müssen. Der zweite Parameter, „field“, gibt an, wo im Ergebnissatz die Daten angehängt werden müssen. Außerdem kann ein Grenzwert angewendet werden, damit der Ergebnissatz nicht überfüllt wird.

Standardmäßig übernehmen auf das SDK folgende Abfragen die where-Klausel der übergeordneten Regel. Wenn Sie eine where-Klausel nur einmal anwenden möchten, können Sie im vierten Parameter einen Booleschen Wert als „false“ und im fünften Parameter eine andere where-Klausel angeben.

**Hinweis:** Wenn Sie in Ihrer Abfrage eine where-Klausel nur einmal verwenden, müssen Sie sicherstellen, dass Sie Argumente in Apostrophe (') und Zeichenfolgenwerte in Anführungszeichen (") einschließen.

Nachdem jetzt die Zusammenfassung **Benutzerdefiniert** und die Funktion **Gruppieren nach** hinzugefügt wurden, kann das Ergebnis sogar ohne die Regelaktion „lookup_and_add“ erzielt werden. Die neue Regelsyntax mit „groupby“ zeigt das Ergebnis in einer flachen Struktur an und ist somit eine Verbesserung gegenüber der früheren Regelsyntax ohne „groupby“. Es wird daher empfohlen, die Regeln mit der Regelaktion „lookup_and_add“ manuell zu bearbeiten bzw. zu aktualisieren und, sofern möglich, die groupby-Klausel zu verwenden.

**Hinweis:** Die Regelaktion „Lookup_And_Add“ wird nur unterstützt, wenn die SELECT-Klausel eine Metaangabe und eine Aggregatfunktion hat.

Siehe zum Beispiel die unten stehenden Szenarien: Im Beispiel **2a** wird die Regelaktion „lookup_and_add“ verwendet. Anstelle dieser Regelaktion kann dasselbe Ergebnis mithilfe der Zusammenfassung **Benutzerdefiniert** und der Funktion **Gruppieren nach** erzielt werden. Siehe Beispiel **2b** unten.

Die Regelaktion „lookup_and_add“ wird aber unter den folgenden Bedingungen weiterhin für NWDB-Regeln unterstützt:

- Alle Versionen von NWDB-Regeln, die als Zusammenfassung Ereignisanzahl, Paketanzahl oder Sitzungsgröße verwenden.
- Bei der Zusammenfassung „Benutzerdefiniert“ darf die Regel „lookup_and_add“ nur eine Metaangabe „Gruppieren nach“ mit nur einer Aggregatfunktion haben, wobei die Aggregatfunktion entweder „sum()“ oder „count()“ sein muss.

**Hinweis:** Nicht unterstützt für „Zusammenfassen-Keine“.

Die Regelaktion „lookup_and_add“ kann zum Beispiel für die folgenden Regeln verwendet werden:

- select ip.src, sum(size) group by ip.src
- select ip.src, count(filename) group by ip.src

Sie kann nicht für die diese Regeln verwendet werden:

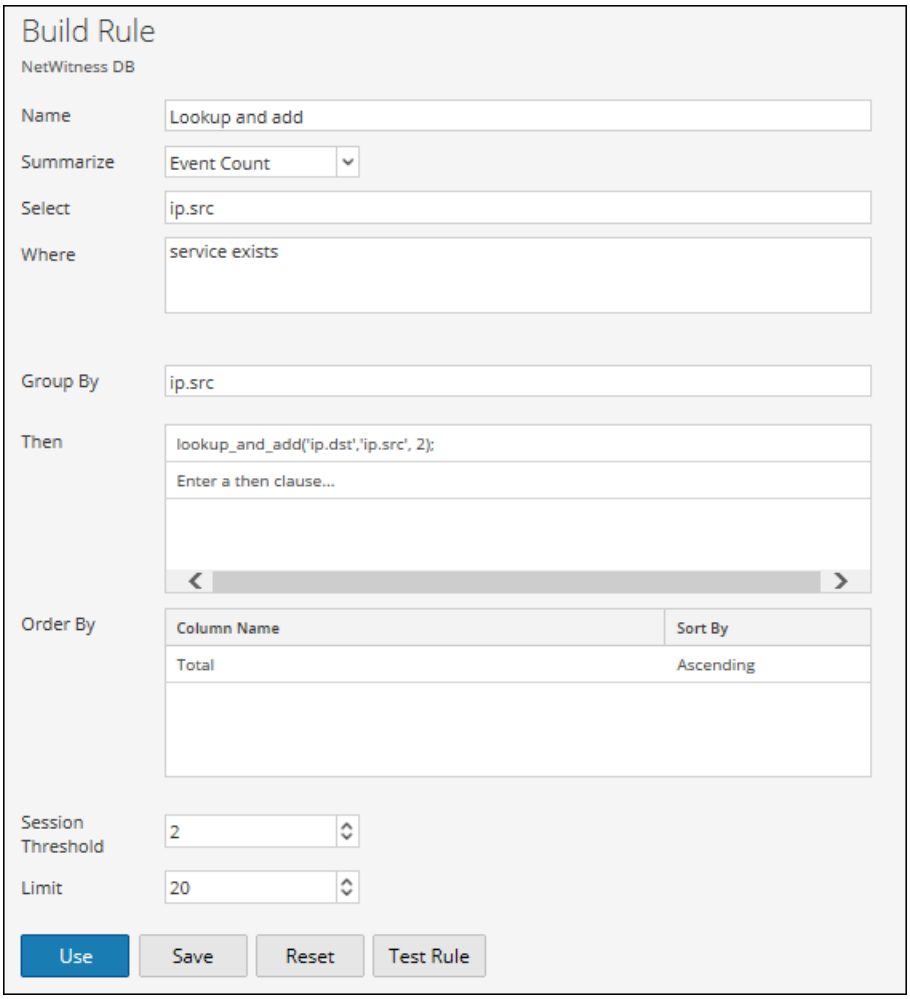
- select ip.src, sum(size),count(filename) group by ip.src
- select ip.src, sum(size),avg(size) group by ip.src
- select ip.src,ip.dst count(filename) group by ip.src,ip.dst

**Beispiele:**

**1. lookup_and_add('ip.dst','ip.src', 2);**

Diese Regelaktion würde iterativ über jede ip.src in der anfänglichen Ergebnismenge laufen und die beiden obersten Ziel-IP-Adressen mit jedem ip.src suchen.

Die folgende Abbildung zeigt die Regeldefinition an.

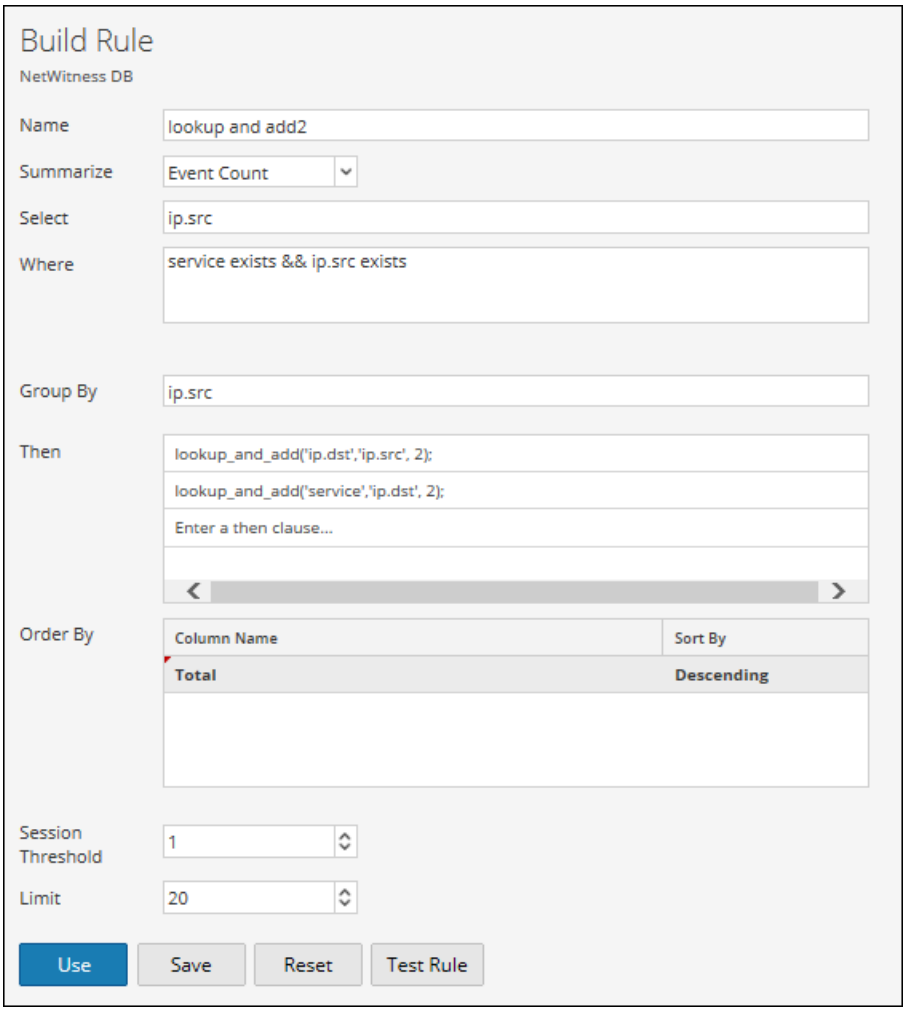



In der folgenden Abbildung wird der Ergebnissatz gezeigt, der für jedes „ip.src“ die Quell-IP-Adressen und die obersten zwei Ziel-IP-Adressen enthält.


**2a. lookup_and_add('ip.dst','ip.src', 2); lookup_and_add('service','ip.src', 3);**

Diese Regelaktion würde iterativ über jede „ip.src“ im anfänglichen Ergebnissatz laufen und für jedes „ip.src“ die beiden obersten Ziel-IP-Adressen sowie die obersten drei von jedem „ip.src“ verwendeten Ports suchen.

Die folgende Abbildung zeigt die Regeldefinition an.



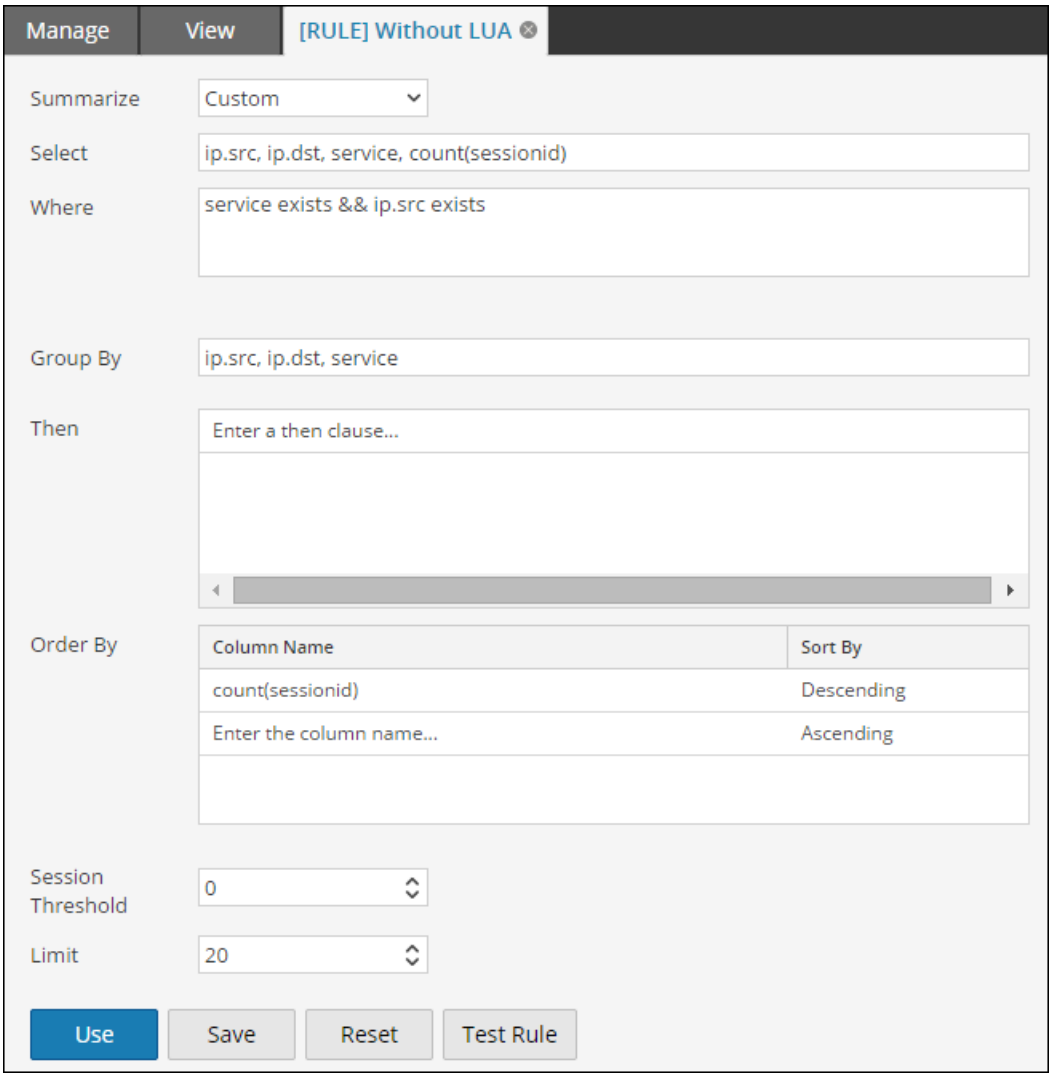

In der folgenden Abbildung wird der Ergebnissatz gezeigt, der für jedes „ip.src“ die Quell-IP-Adressen und die obersten zwei Ziel-IP-Adressen sowie die obersten drei von jedem „ip.src“ verwendeten Ports enthält.


Sie können die Abfrage beliebig komplex gestalten, indem Sie verschiedene Felder im Ergebnissatz auswählen und sie an unterschiedliche Teile anhängen. Beispiel: Angenommen, Sie möchten wissen, welche Dateien die jeweilige Quell-IP verarbeitet hat. Da die übergeordnete Regel jedoch eine WHERE-Klausel „service = '6667'“ enthält und das Standardverhalten dieser Regelaktion darin besteht, dass Daten an die ursprüngliche WHERE-Klausel angehängt werden, müssen Sie die übergeordnete WHERE-Klausel außer Kraft setzen. Dieses Konzept ist am einfachsten zu verstehen, wenn Sie sich den vorherigen Aufruf von lookup_and_add ansehen: lookup_and_add('ip.dst','ip.src',2) ansehen. Die eigentliche Abfrage, die an den Server gesendet wird, lautet: SELECT ip.dst WHERE service = 6667 ip.src = 206.42.199.194. Um zu erzwingen, dass die WHERE-Klausel diesen Teil „service = '6667'“ der WHERE-Klausel (geerbt aus der übergeordneten Regel) außer Kraft setzt, kann der Benutzer als vierten Parameter „false“ festlegen, wie in Beispiel 3 dargestellt.

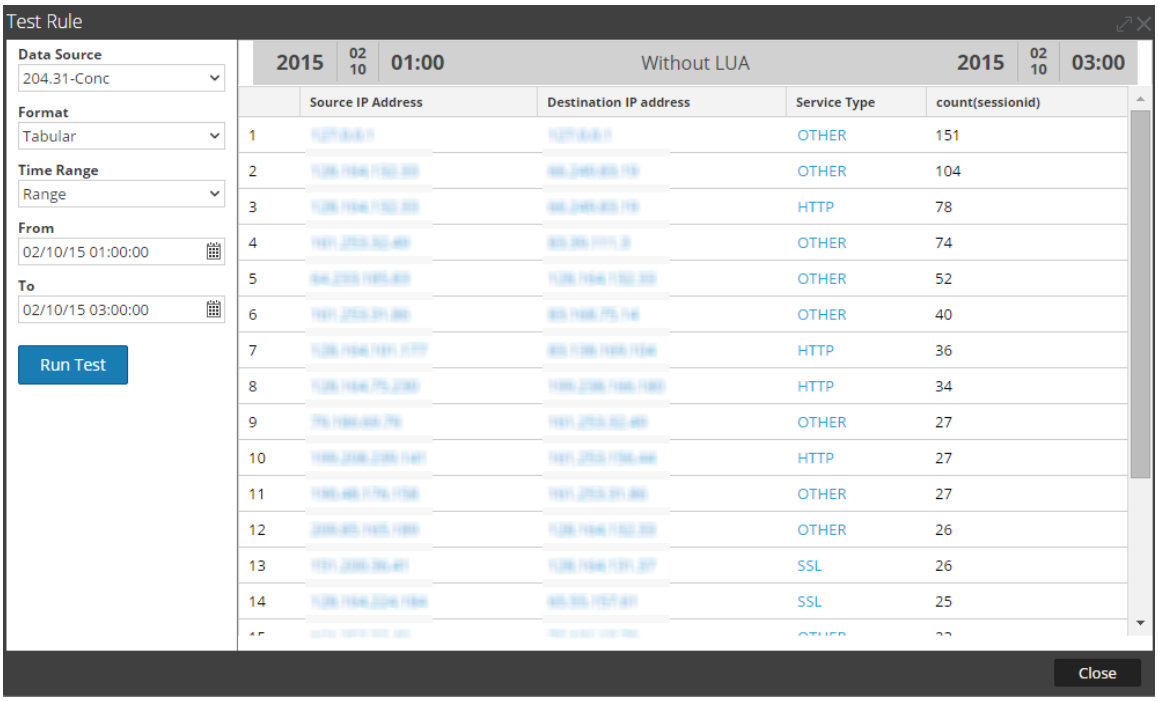
**2b. Ohne die Regel Lookup_and_add**

Diese Regel verwendet die Zusammenfassung „Benutzerdefiniert“ und die Funktion „Gruppieren nach“, um die Ergebnisse zu sortieren.

Die folgende Abbildung zeigt die Regeldefinition an.



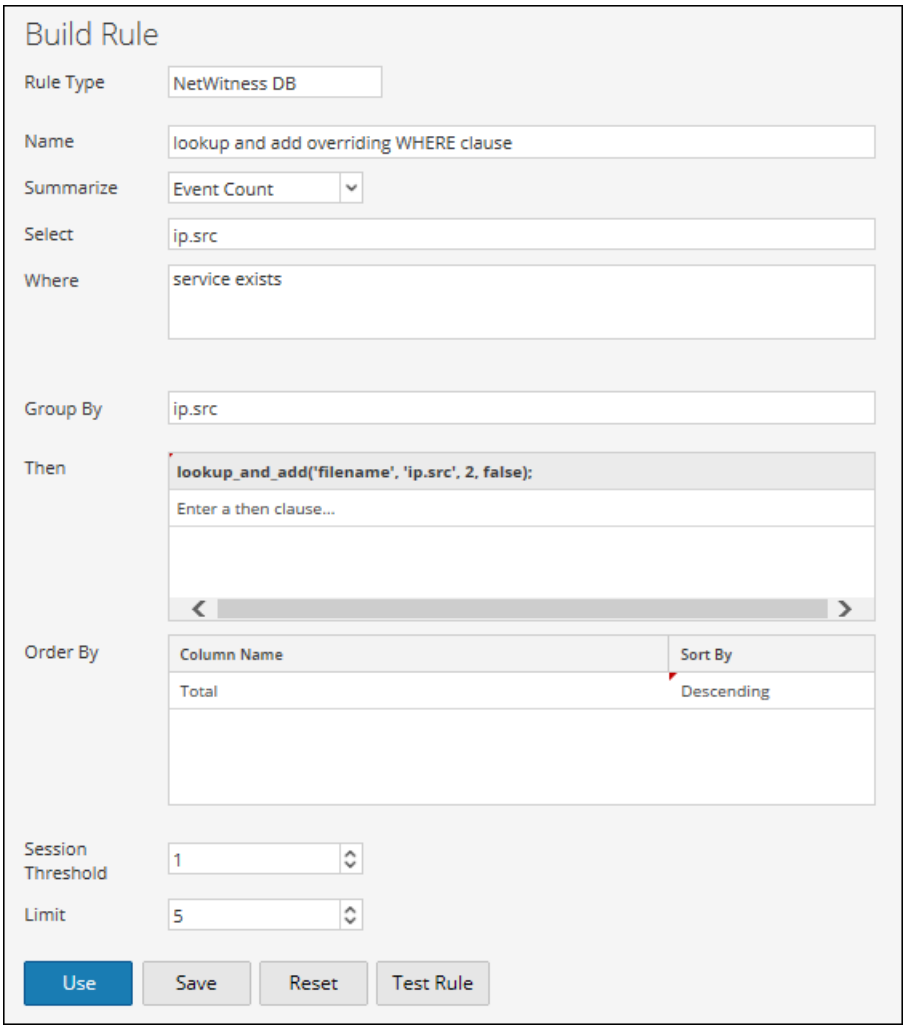

In der folgenden Abbildung wird der Ergebnissatz gezeigt, der für jedes „ip.src“ die Quell-IP-Adressen und die obersten zwei Ziel-IP-Adressen sowie die obersten drei von jedem „ip.src“ verwendeten Ports enthält.



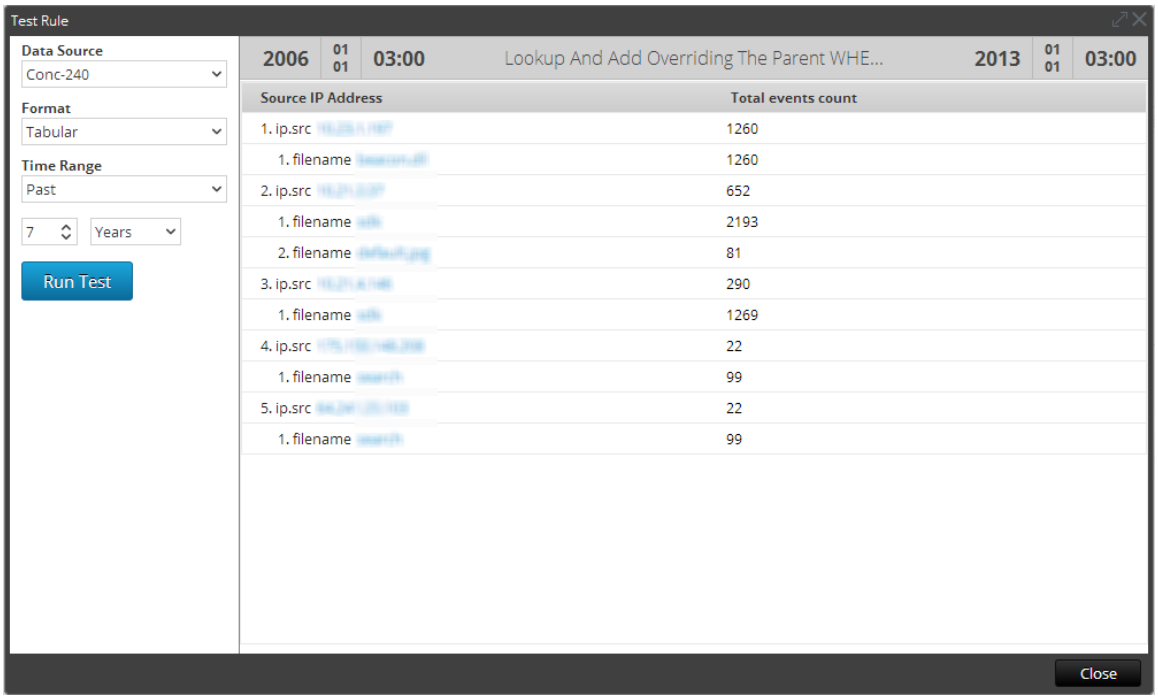

**3. lookup_and_add('filename', 'ip.src', 2, false);**

Dieser Aufruf würde eine Abfrage an den Server ausgeben, z. B. `SELECT filename WHERE ip.src = 90.0.0.142` anstelle von `SELECT filename WHERE service = 6667' && ip.src = 90.0.0.142`, da Sie angegeben haben, dass die Regelaktion die anfängliche `WHERE`-Klausel der übergeordneten Regel ignorieren soll.

Die folgende Abbildung zeigt die Regeldefinition an.




Die folgende Abbildung zeigt die Ergebnismenge an.

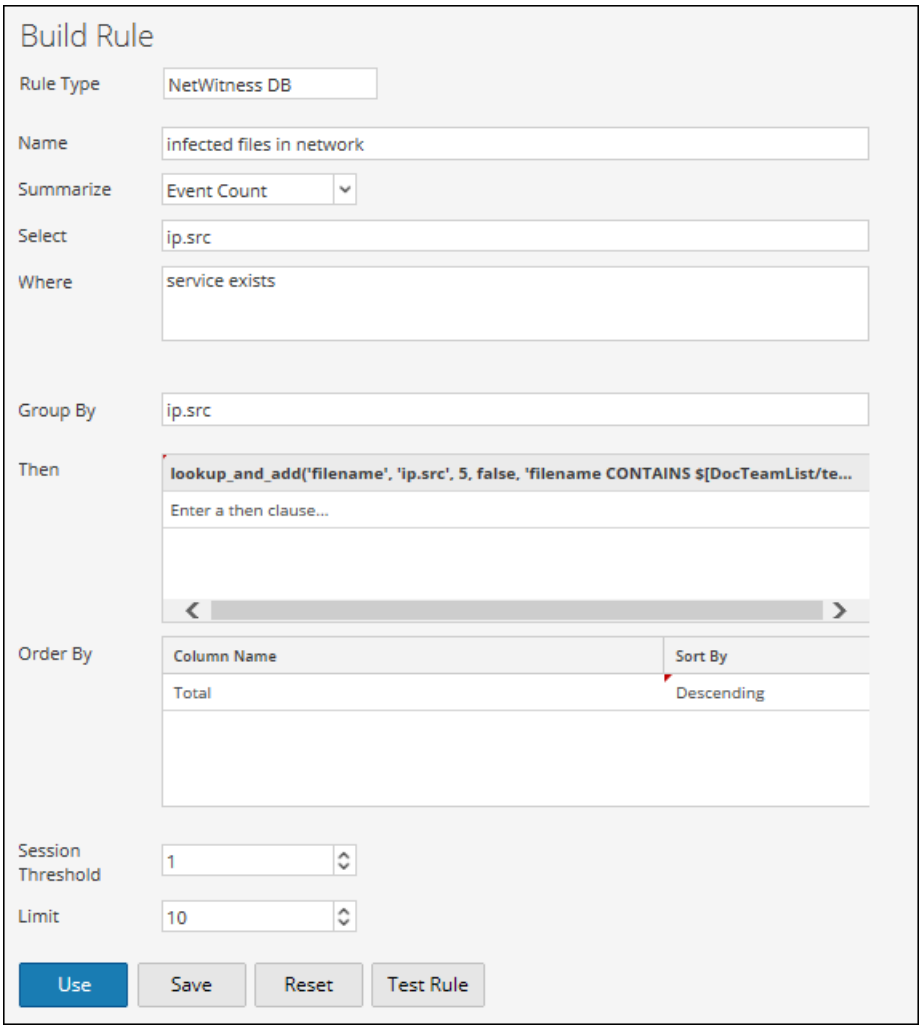



Die Liste „test“ befindet sich im Gruppennamen „netwitness“; auf diese Liste können Sie mit der folgenden Syntax zugreifen.

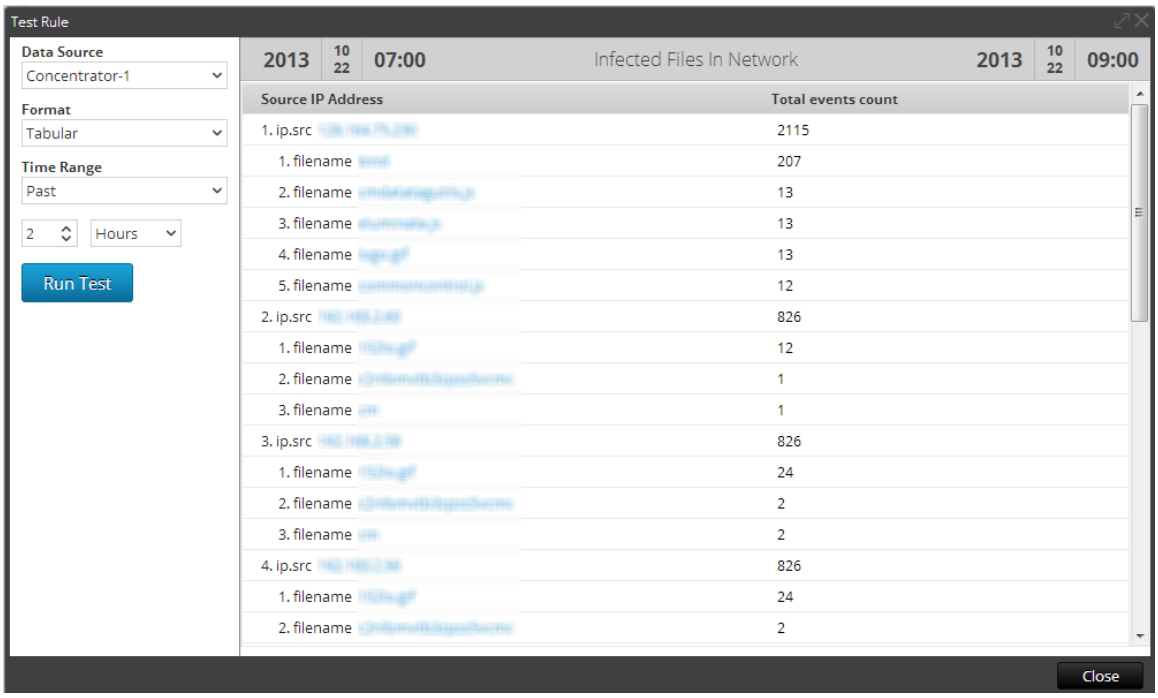
Sie können diese angehängten Ergebnisse weiter einengen, sodass nur Dateinamen mit der Erweiterung .gif aufgenommen werden, indem Sie den fünften Parameter in der Regelaktion verwenden Mit dem fünften Parameter können Sie zusätzliche Kriterien für die WHERE-Klausel angeben. Die Dateien mit der Erweiterung .gif würden in der Liste **test** innerhalb einer Gruppe namens **DocTeamList** gespeichert. Sie können mit der folgenden Syntax auf diese Liste zugreifen: threat.source = $[DocTeamList/test]
Hierauf kann im zusätzlichen where-Klauselparameter auf folgende Weise verwiesen werden:

**4. lookup_and_add('filename', 'ip.src', 5, false, 'filename CONTAINS $[DocTeamList/test]');**

Die folgende Abbildung zeigt die Regeldefinition an.




Die folgende Abbildung zeigt die Ergebnismenge an.

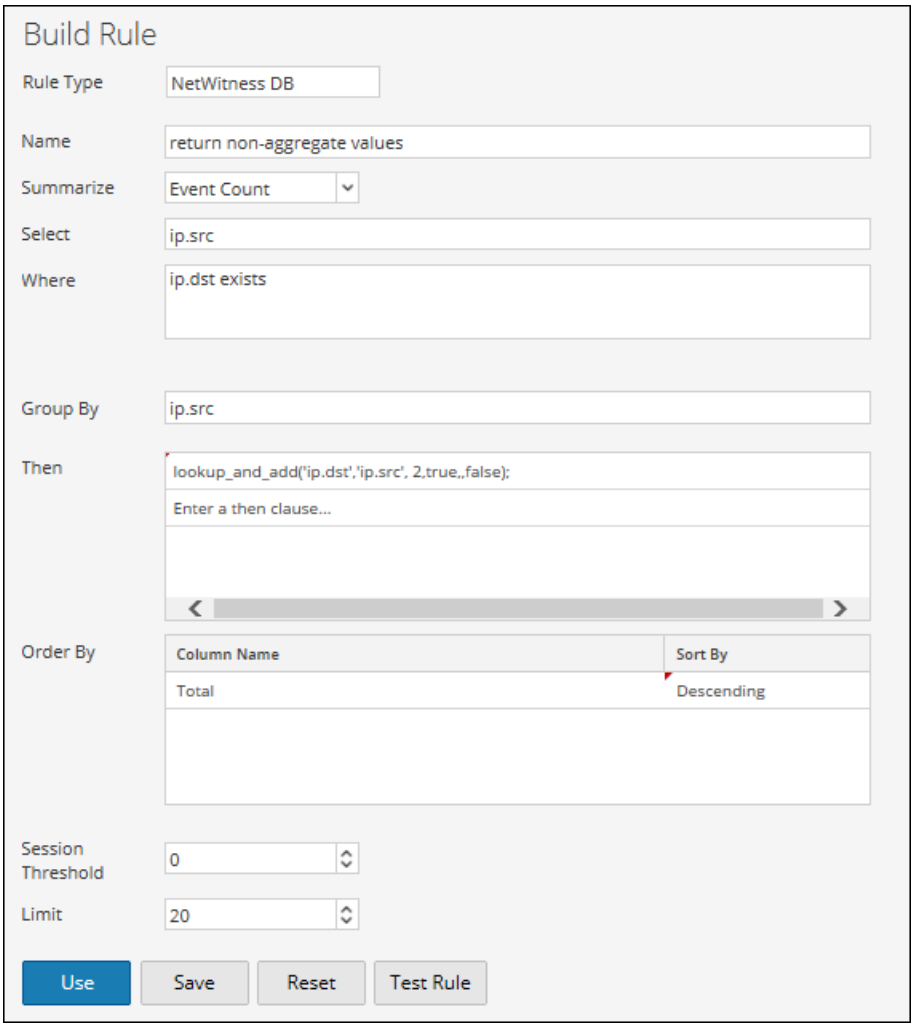



**5. lookup_and_add('ip.dst','ip.src', 2,true,,false);**

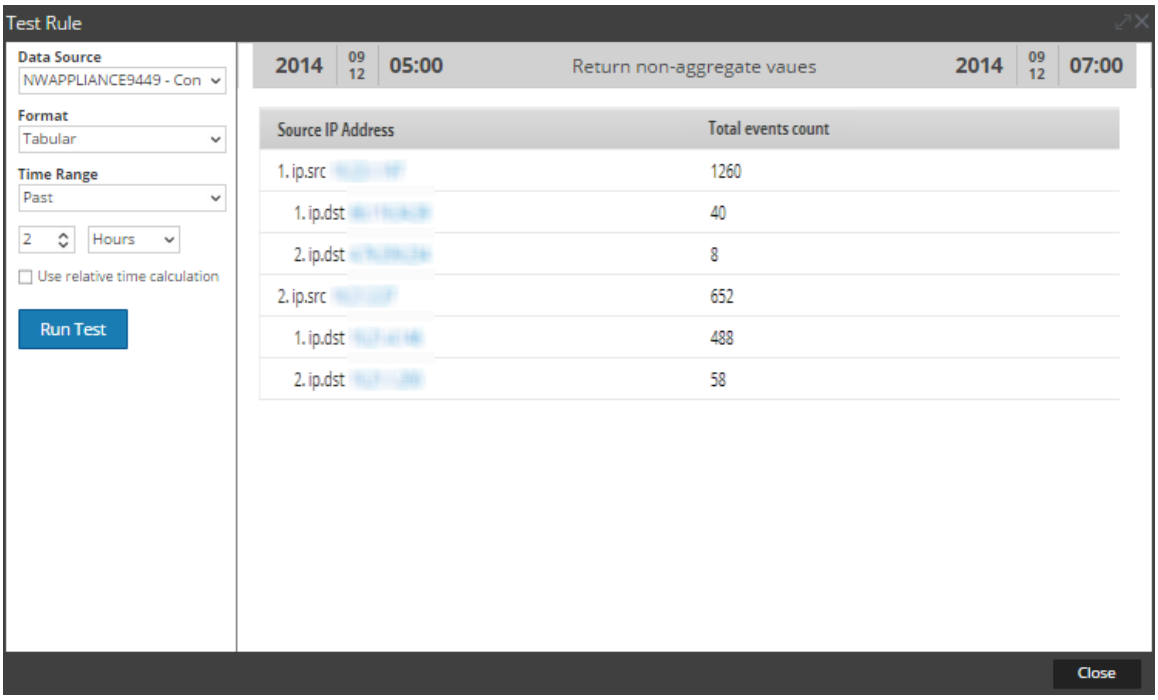
Diese Regelaktion würde iterativ über jede ip.src in der anfänglichen Ergebnismenge laufen und die beiden obersten Ziel-IP-Adressen mit jedem ip.src suchen. Der Parameter „aggregate“ ist auf „false“ gesetzt; dadurch wird impliziert, dass Aggregate für Lookup-Werte übersprungen werden und daher die Lookup-Abfrage schneller ausgeführt wird.

**Hinweis:**
Der Standardwert für „aggregate“ ist „true“. Wenn „aggregate“ auf „false“ gesetzt ist, gibt die Reporting Engine threshold=1, Sort by='value' und Order=Ascending an NWDB weiter, um die Lookup-Abfragen zu beschleunigen.
. Sie müssen „aggregate“ auf „false“ setzen, wenn die Regel Aggregatfunktionen enthält oder wenn sie für einen langen Zeitbereich ausgeführt wird. Dann wird die Regel schneller ausgeführt.

Die folgende Abbildung zeigt die Regeldefinition an.




Die folgende Abbildung zeigt die Ergebnismenge an.




```
max_threshold (string quantity)
max_threshold (string quantity, string field)
```

„max_threshold“ entfernt alle Ergebnisse mit einer Menge, die über der maximalen Schwellenwertmenge liegt, aus einem Ergebnissatz. Die Menge kann entweder in Anzahl oder Größe angegeben werden und ist relativ zu den Sortieroptionen der übergeordneten Regel. Das bedeutet, wenn Sie eine Regel nach Größe sortieren, erwartet die Regelaktion, dass Sie die Parameter in Byte angeben (Sie können dem Parameter KB, MB, GB, TB anfügen, um die Größenkonvertierung zu vereinfachen).

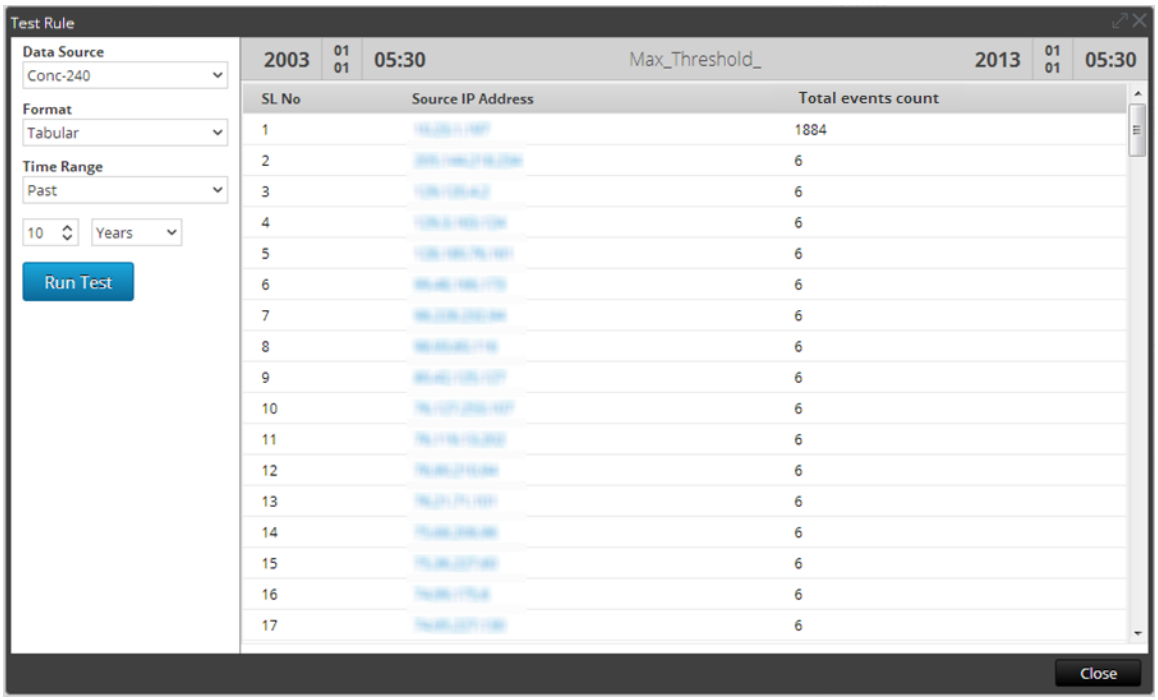
Mithilfe der Regel „max_threshold“ können auch Werte auf Basis der Aggregatfunktionswerte gefiltert werden. Verwenden Sie die Syntax auf Basis des Typs von Zusammenfassung wie in der Regel unten:

- max_threshold(String quantity): Kann zum Filtern von Ereignisanzahl, Paketanzahl und Sitzungsgröße verwendet werden.
- max_threshold(String quantity, String field): Kann zum Filtern der Werte von benutzerdefinierten Aggregaten oder beliebigen Metadaten verwendet werden.

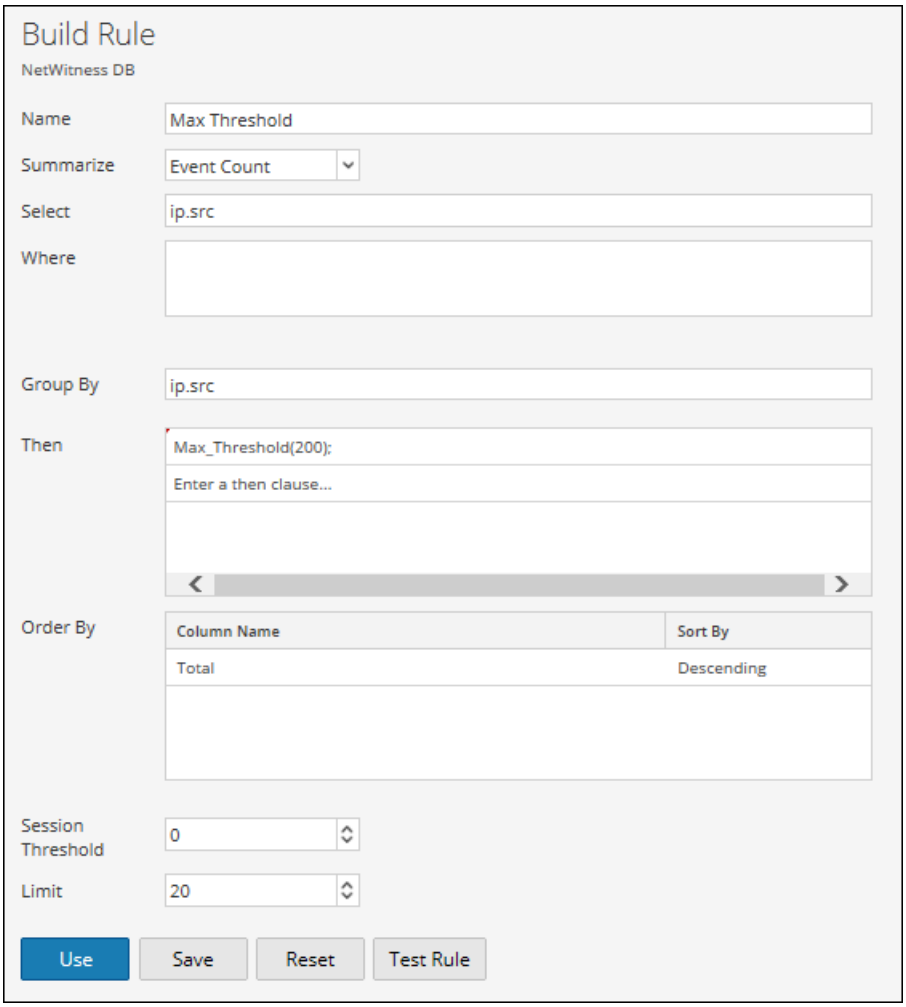
**Beispiele:**

**1. max_threshold(200);**

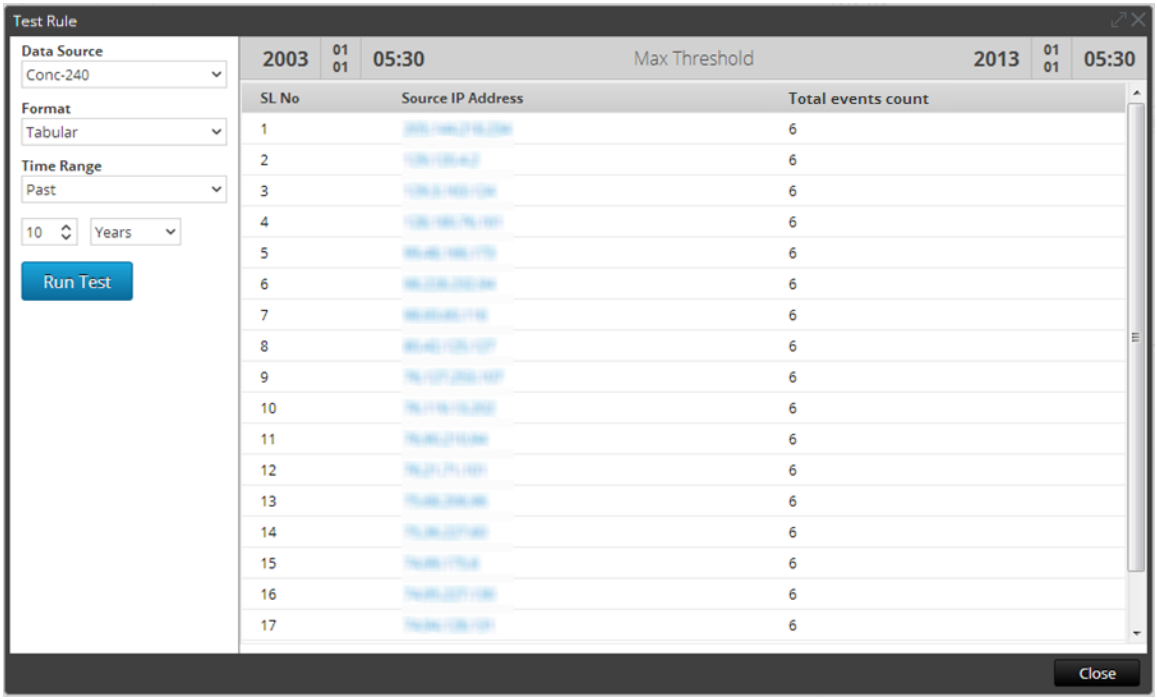
Die folgende Abbildung zeigt das Ergebnis ohne das Argument „max_threshold“. Die Ausgabeergebnisse haben Ereignisanzahlen über 200.




Die folgende Abbildung zeigt, wie die Regelaktion „max_threshold“ die Ausgabe auf 200 Byte begrenzt Alle Ausgaben, die mehr als 200 Byte an Daten umfassen, werden nicht aufgelistet.

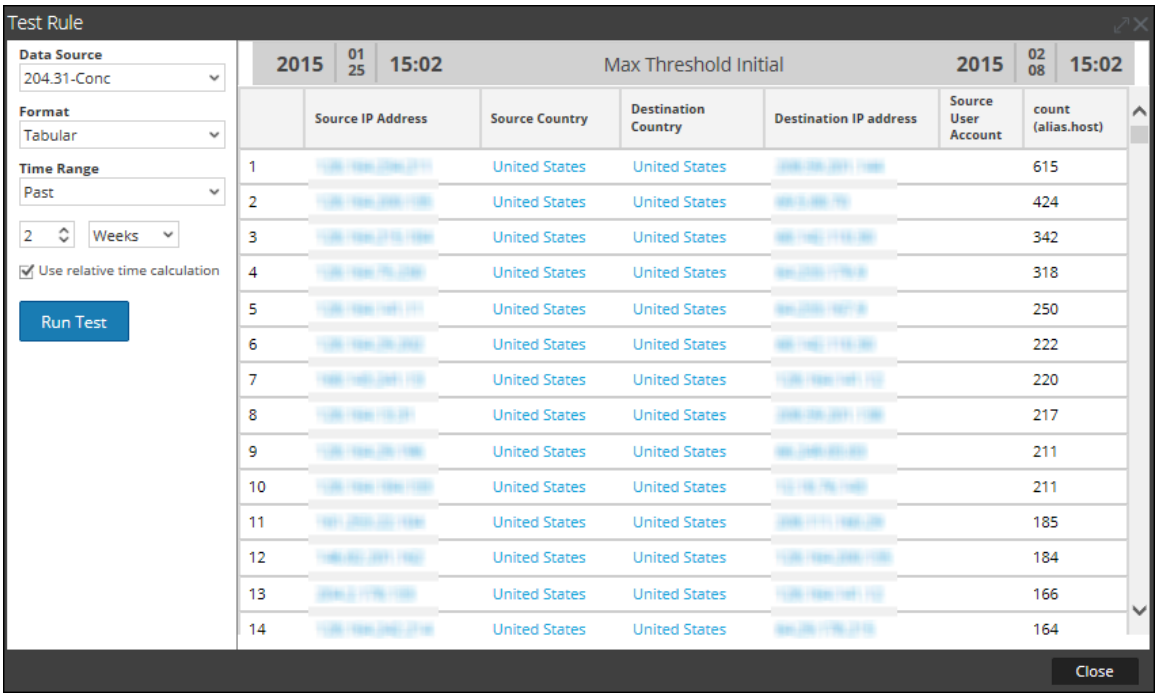



Die folgende Abbildung zeigt das Ergebnis mit angewendeter Regelaktion „max_threshold“. Das Ergebnis Nummer 1 im obigen Screenshot wurde aus dem Ergebnis entfernt.

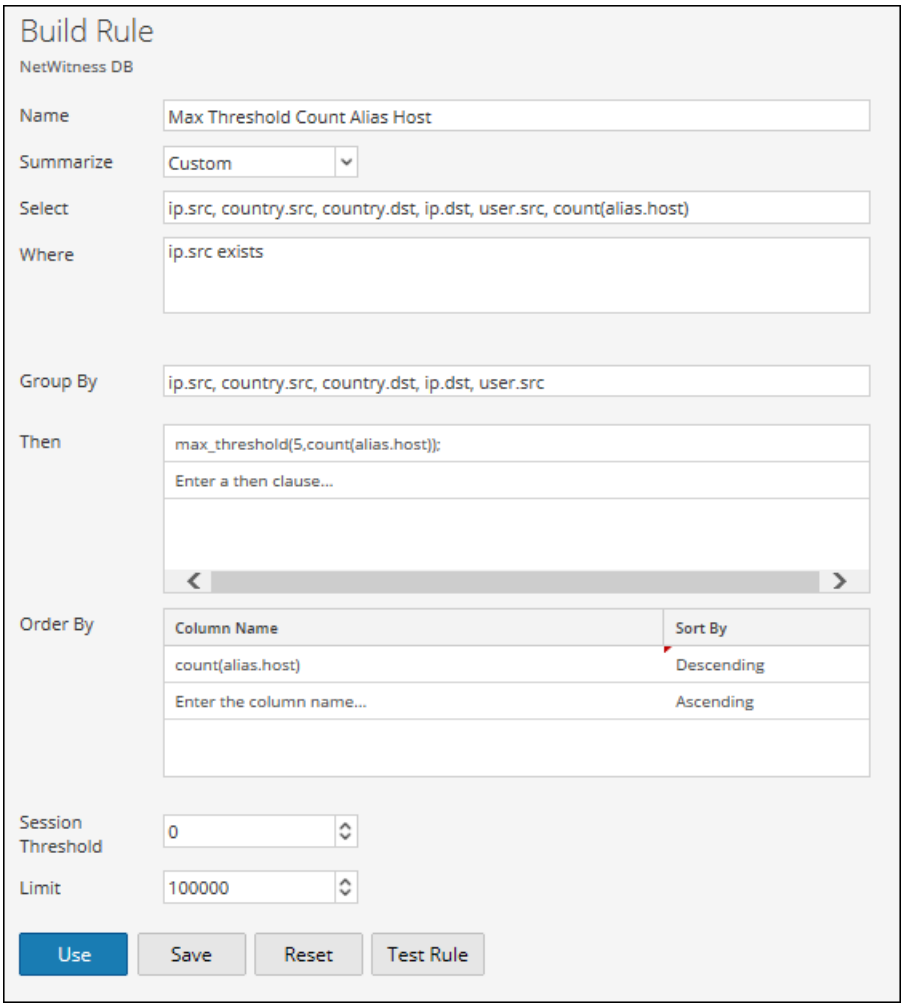



**2. max_threshold(5,count(alias.host));**

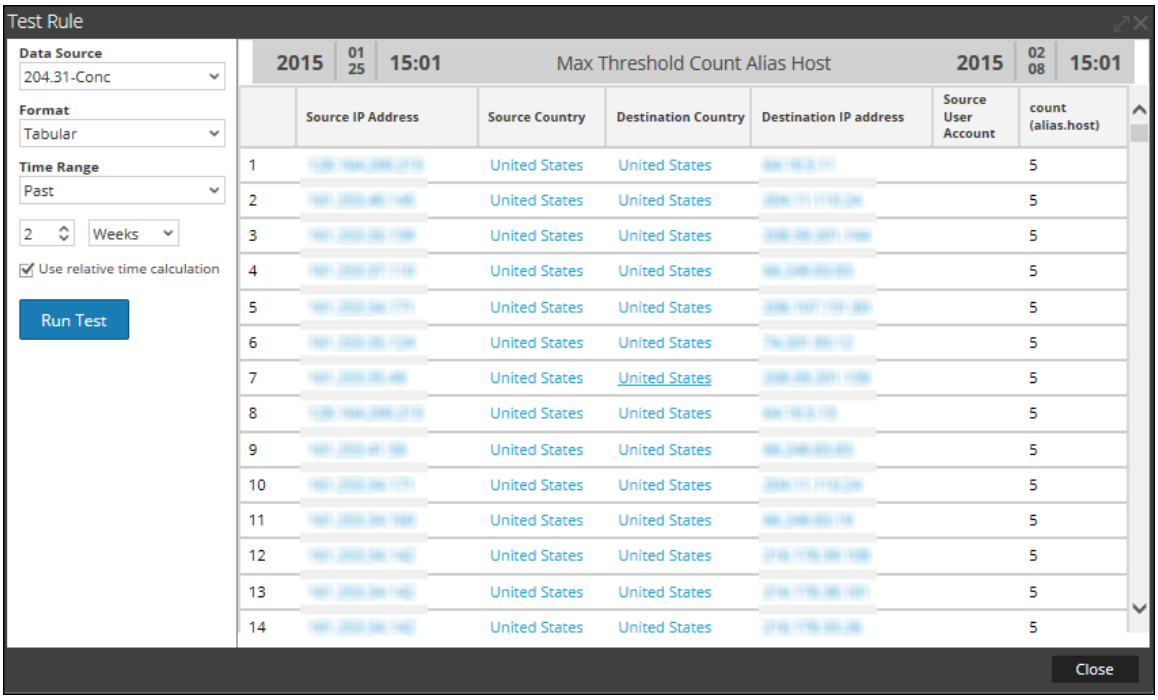
Die folgende Abbildung zeigt das Ergebnis ohne das Argument „max_threshold“. In der Ausgabe sind „alias.host“-Ergebnisse mit einer Anzahl von über 5 enthalten.




Die folgende Abbildung zeigt, wie die Regelaktion „max_threshold“ die Ausgabe auf 5 begrenzt. Ausgaben mit einem Wert über 5 werden nicht aufgelistet.




Die folgende Abbildung zeigt das Ergebnis mit angewendeter Regelaktion „max_threshold“. Alle Ausgaben mit einem Wert über 5 wurden aus dem Ergebnis entfernt.




min_threshold (string quantity)

„min_threshold“ entfernt Ergebnisse mit einer Menge, die unter der minimalen Schwellenwertmenge liegt, aus einem Ergebnissatz. Die Menge kann entweder in Anzahl oder Größe angegeben werden und ist relativ zu den Sortieroptionen der übergeordneten Regel. Das bedeutet, wenn Sie eine Regel nach Größe sortieren, erwartet die Regelaktion, dass Sie die Parameter in Byte angeben (Sie können dem Parameter KB, MB, GB, TB anfügen, um die Größenkonvertierung zu vereinfachen).

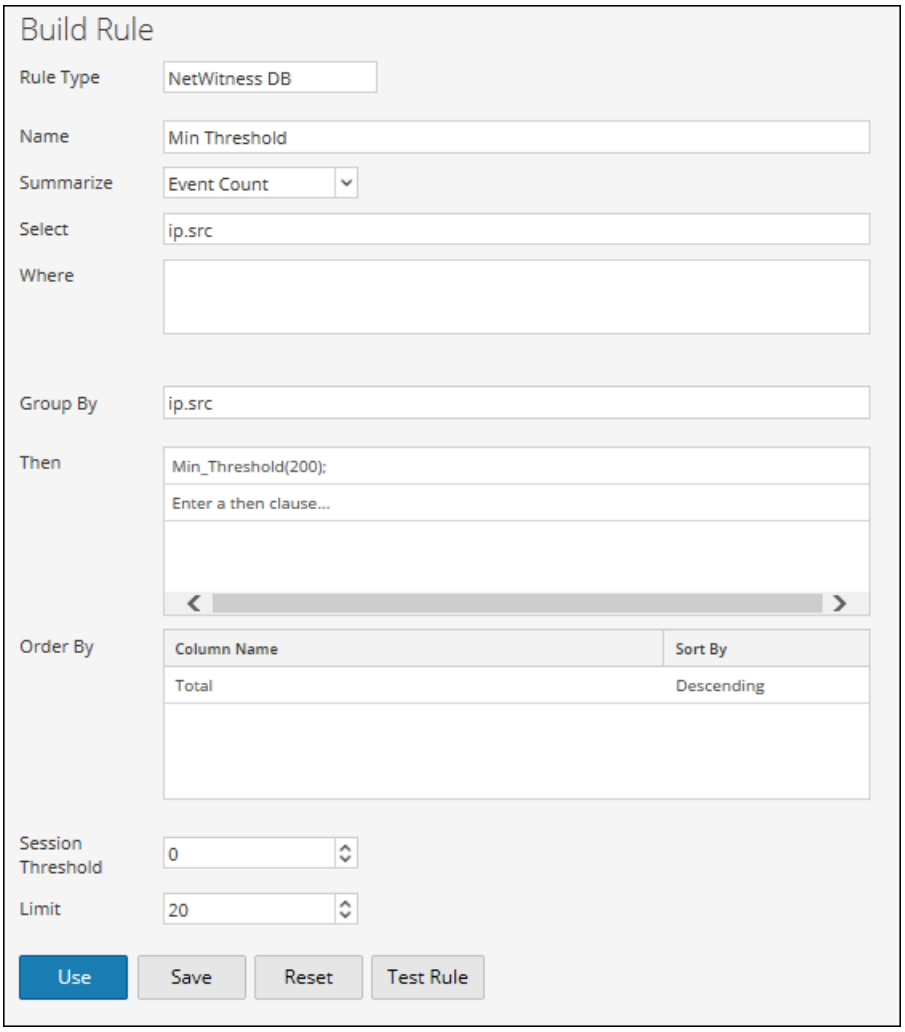
Mithilfe der Regel „min_threshold“ können Werte auch auf Basis der Aggregatfunktionswerte gefiltert werden. Verwenden Sie die Syntax auf Basis des Typs von Zusammenfassung wie in der Regel unten:

- min_threshold(String quantity): Kann zum Filtern von Ereignisanzahl, Paketanzahl und Sitzungsgröße verwendet werden.
- min_threshold(String quantity, String field): Kann zum Filtern der Werte von benutzerdefinierten Aggregaten oder beliebigen Metadaten verwendet werden.

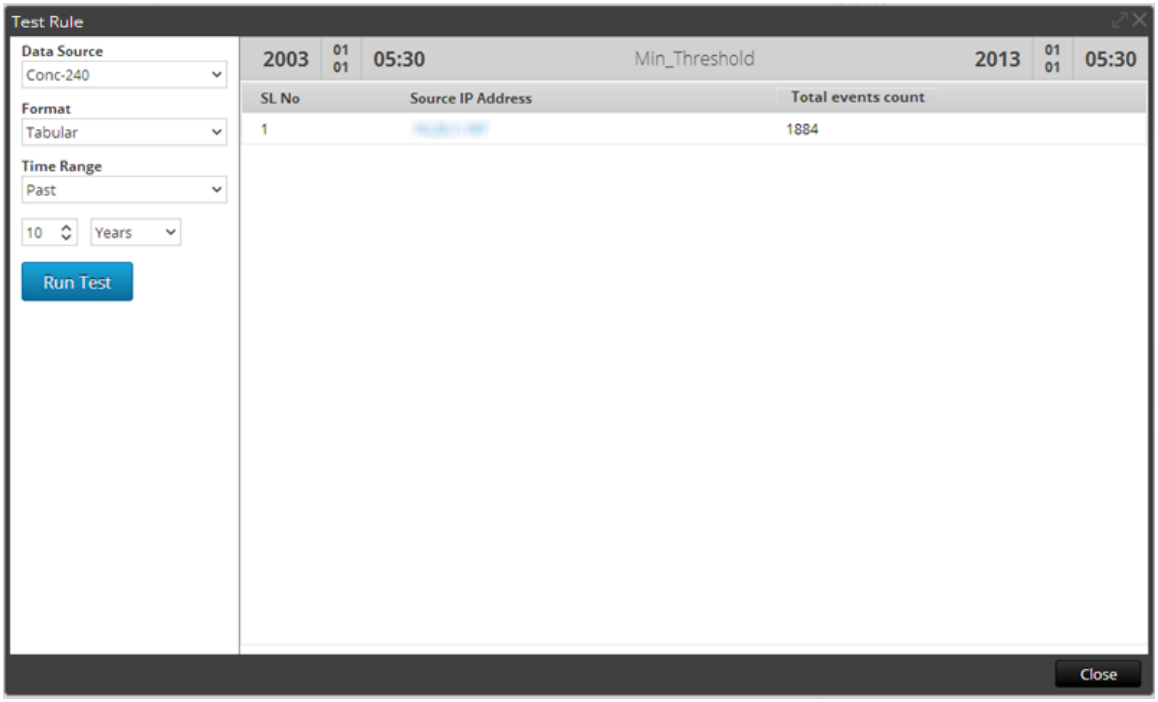
**Beispiele:**

**1. min_threshold(200);**

Die folgende Abbildung zeigt ein Beispiel für eine Abfrage mit „min_threshold“.



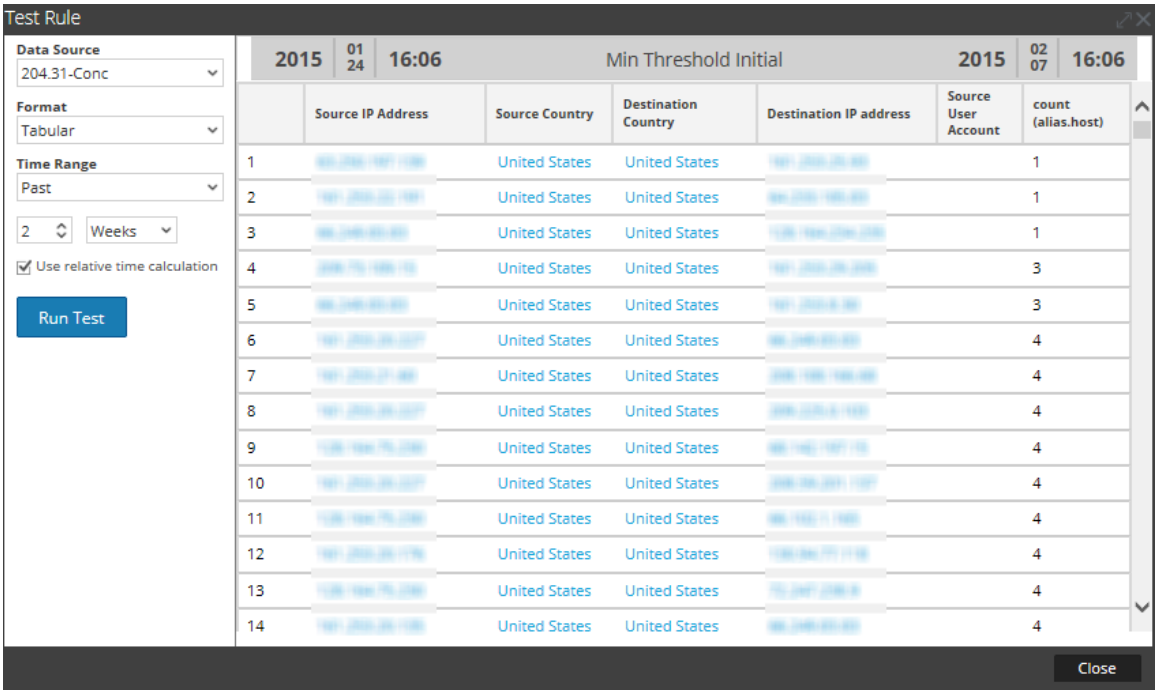

In der obigen Abbildung wird die Ausgabe auf 200 Byte begrenzt. Es wird keine Ausgabe mit weniger als 200 Byte an Daten aufgelistet. Die Ausgabe mit der Regelaktion „min_threshold“ wird angewendet.



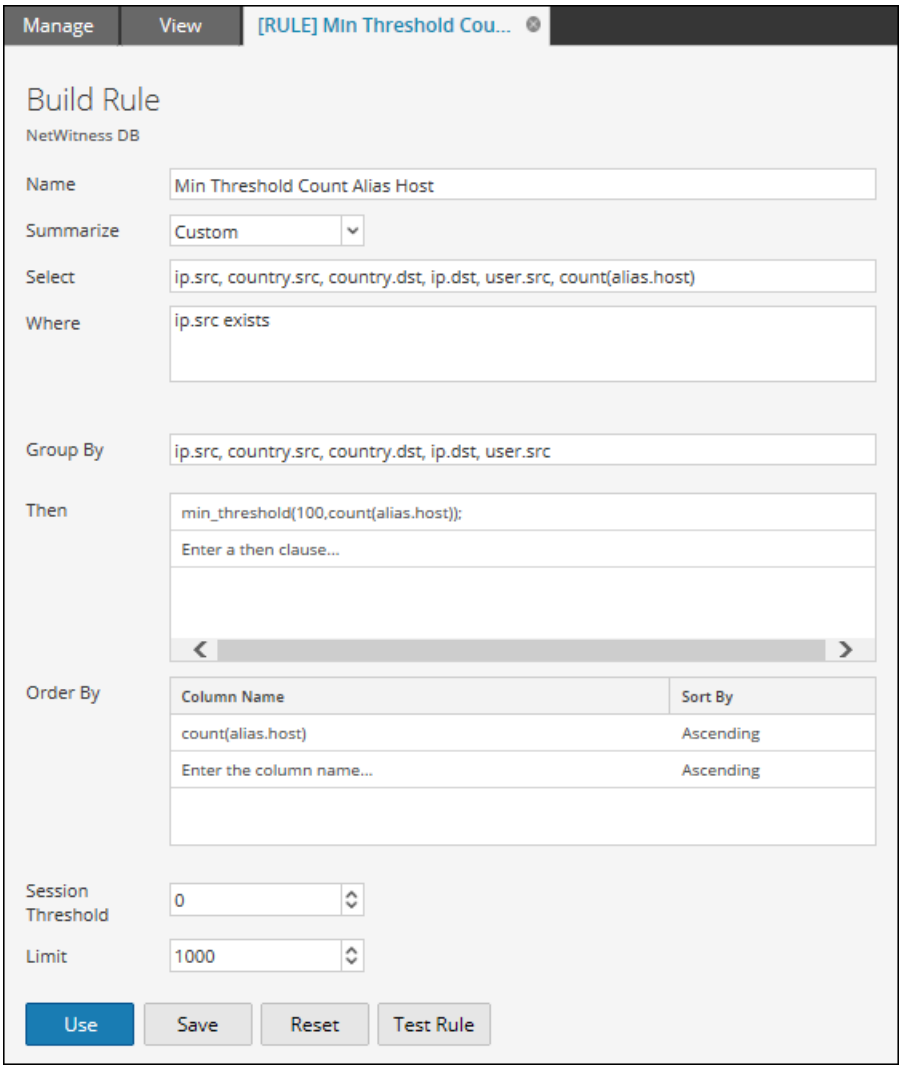

Wie aus der Abbildung hervorgeht, sind alle Werte größer als 200 Byte.

**2. min_threshold(100,count(alias.host));**

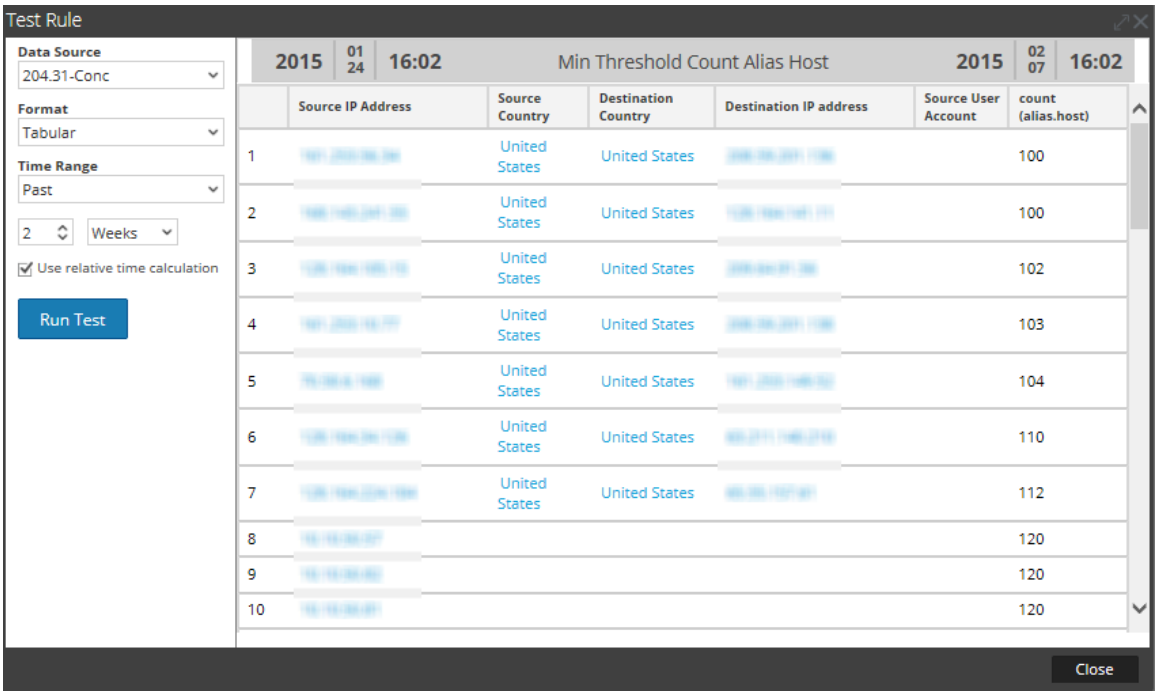
Die folgende Abbildung zeigt das Ergebnis ohne das Argument „min_threshold“. In der Ausgabe sind alias.host-Ergebnisse mit einer Anzahl von unter 100 enthalten.




Die folgende Abbildung zeigt, wie die Regelaktion „min_threshold“ die Ausgabe auf ein Minimum von 100 begrenzt. Es wird keine Ausgabe mit Daten unter 100 aufgelistet.




Die folgende Abbildung zeigt das Ergebnis mit angewendeter Regelaktion „min_threshold“. Alle Ausgaben mit Daten von weniger als 100 wurden aus dem Ergebnis entfernt.




## regex (string regex, string field)

Die Regelaktion „regex“ wendet reguläre Ausdrücke auf den Ergebnissatz an. Die Regelaktion „regex“ hat folgendes Format:

regex(regular_expression, meta_name)

Hierbei gilt:

- regular_expression: Regulärer Ausdruck zum Vergleich mit dem Metawert
- meta_name: Meta- oder Feldname, auf den regex angewendet werden soll.

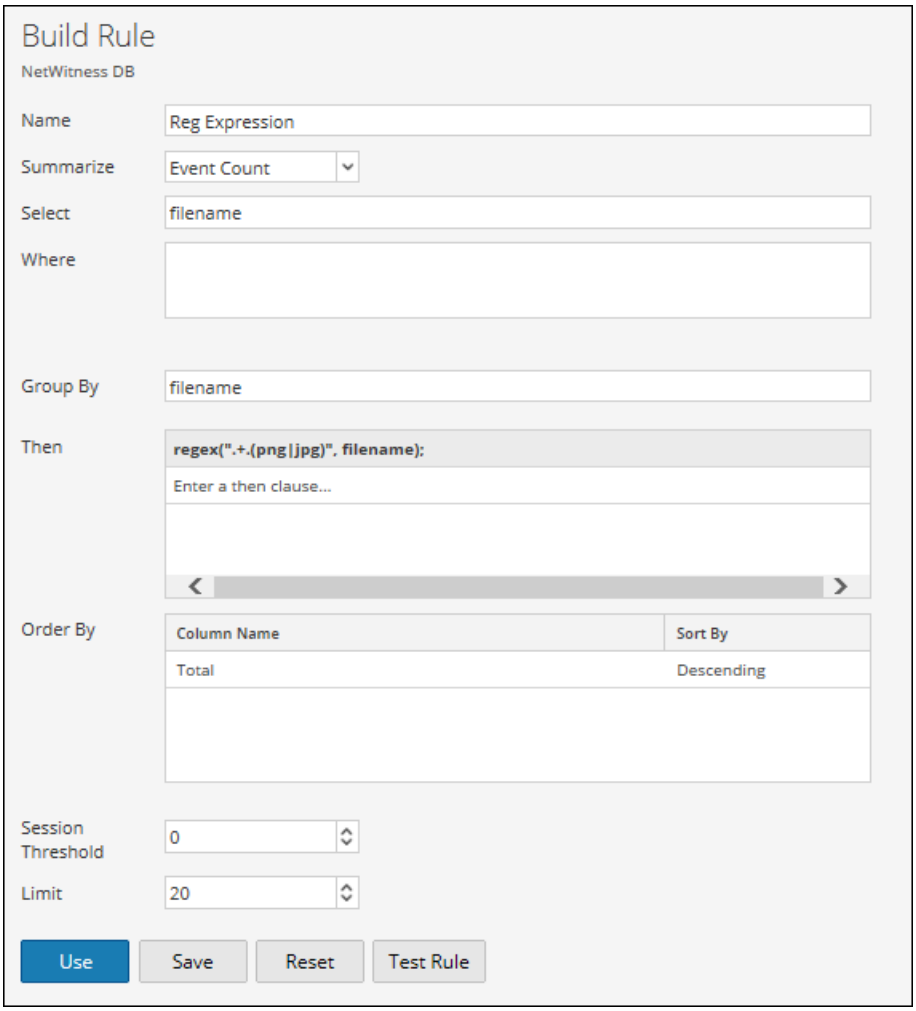
Eine umfassende Liste der unterstützten regex-Muster finden Sie unter http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.

**Beispiel für die Regelaktion „regex“:**

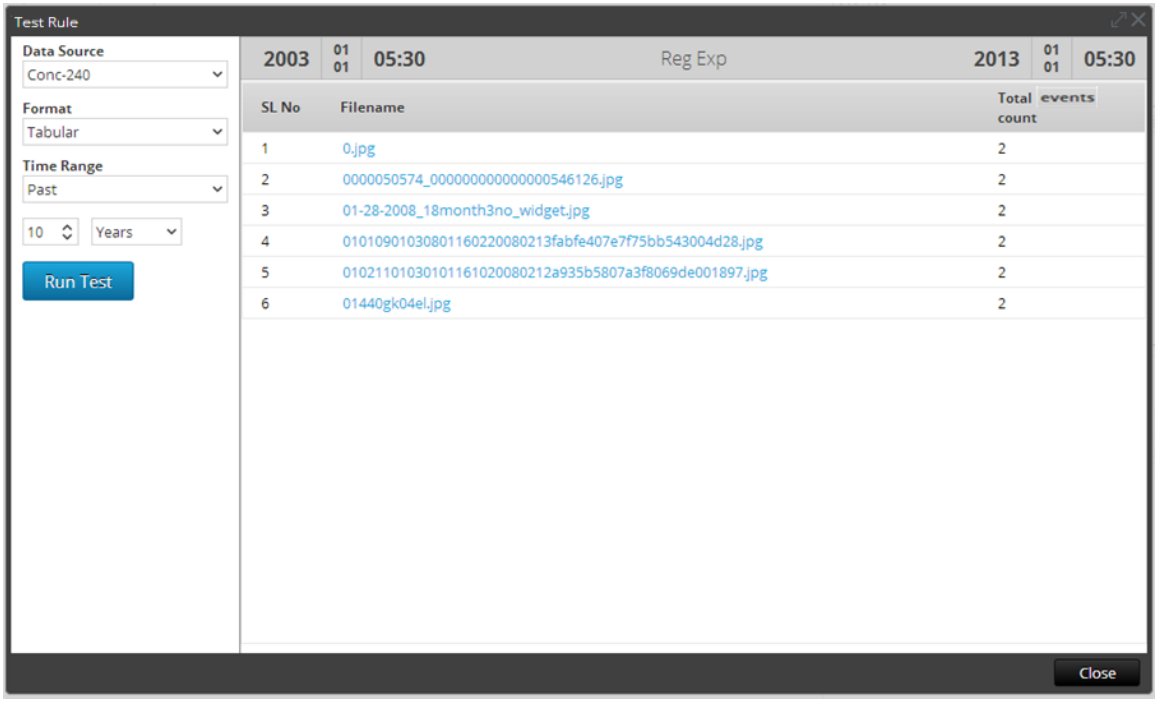
Wenn Sie die Dateinamen aller Dateien im PNG- und JPEG-Format aus verschiedenen Sitzungen auflisten möchten, können Sie eine Regel mit der folgenden Regelaktion „regex“ schreiben:

regex(".+.(png|jpg)", filename);

Die folgende Abbildung zeigt die Regel.




In der folgenden Abbildung sehen Sie die Ausgabe mit angewendeter Regelaktion „regex“.

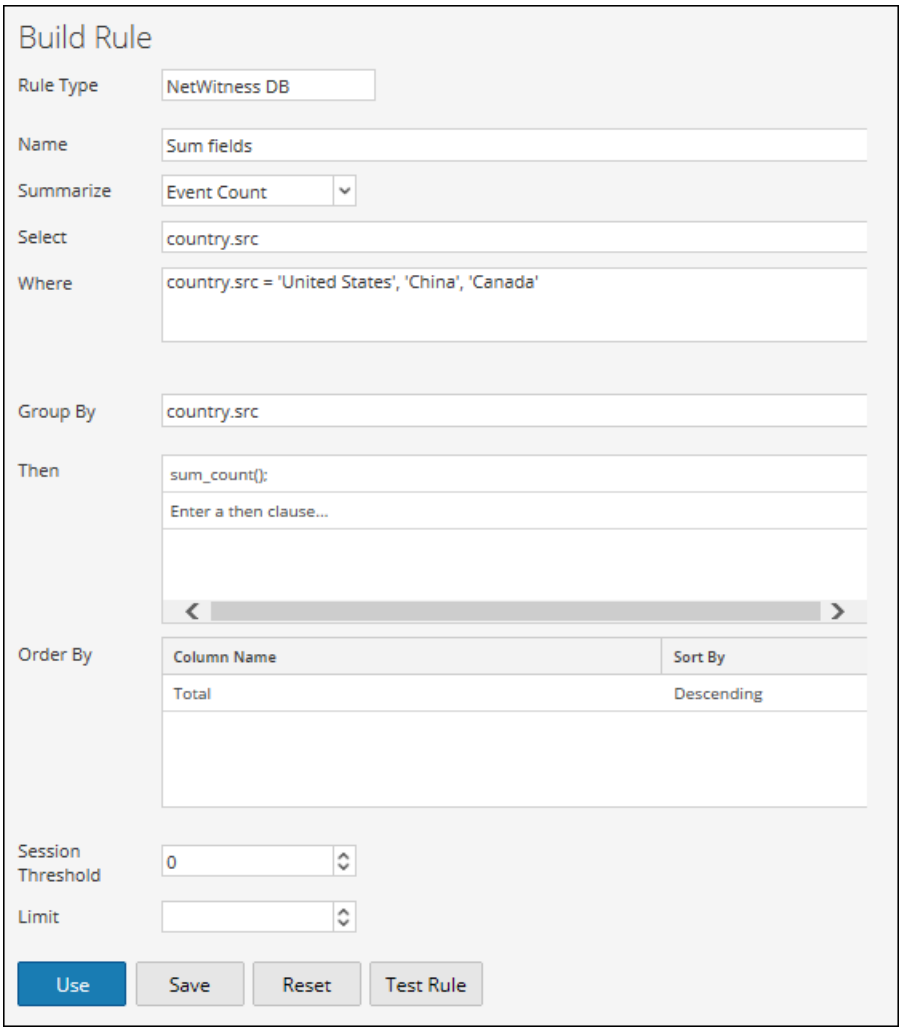



`sum_count()`

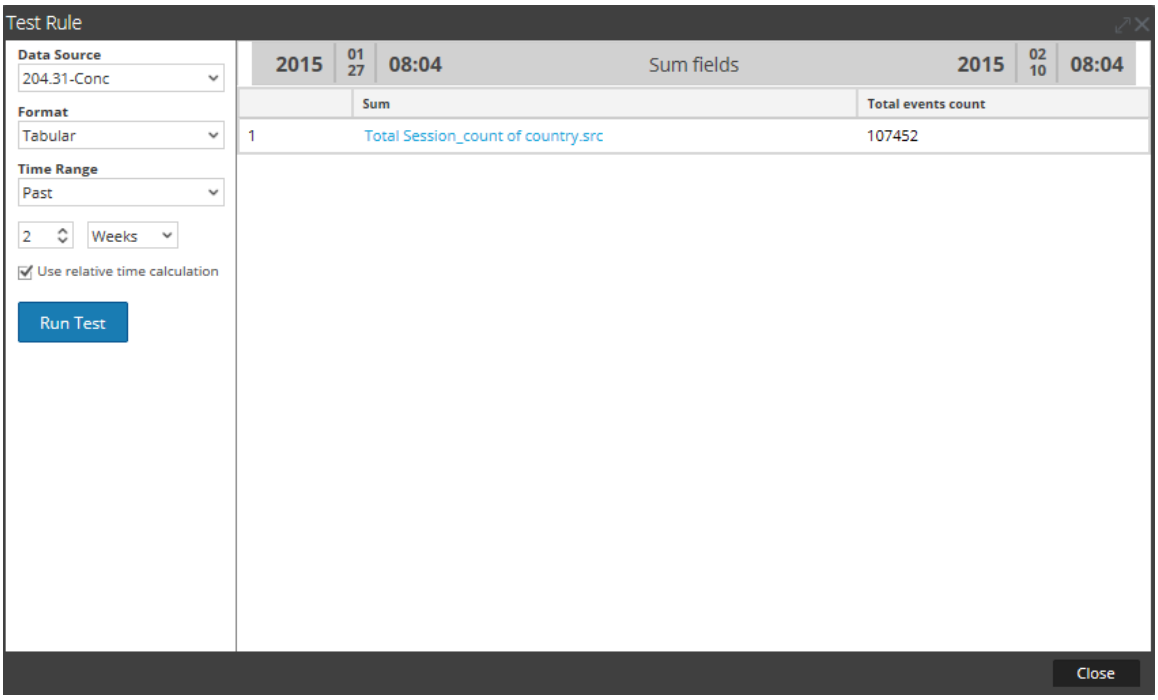
Zählt die Quantoren für einen angegebenen Ergebnissatz zusammen. Beispiel: Beim Aufruf von „sum_count()“ für eine Regel, die nach Ereignisanzahlsummen sortiert wird, werden die Größen aller Werte im Ergebnissatz zusammengezählt und der Gesamtwert anstelle des Ergebnissatzes angezeigt.

**Beispiel**:

Die folgende Abbildung zeigt die Regelaktion „sum_count()“.




Mit der Regelaktion „sum_count()“ zeigt die Ausgabe die Gesamtgröße aller Ereignisanzahlen.

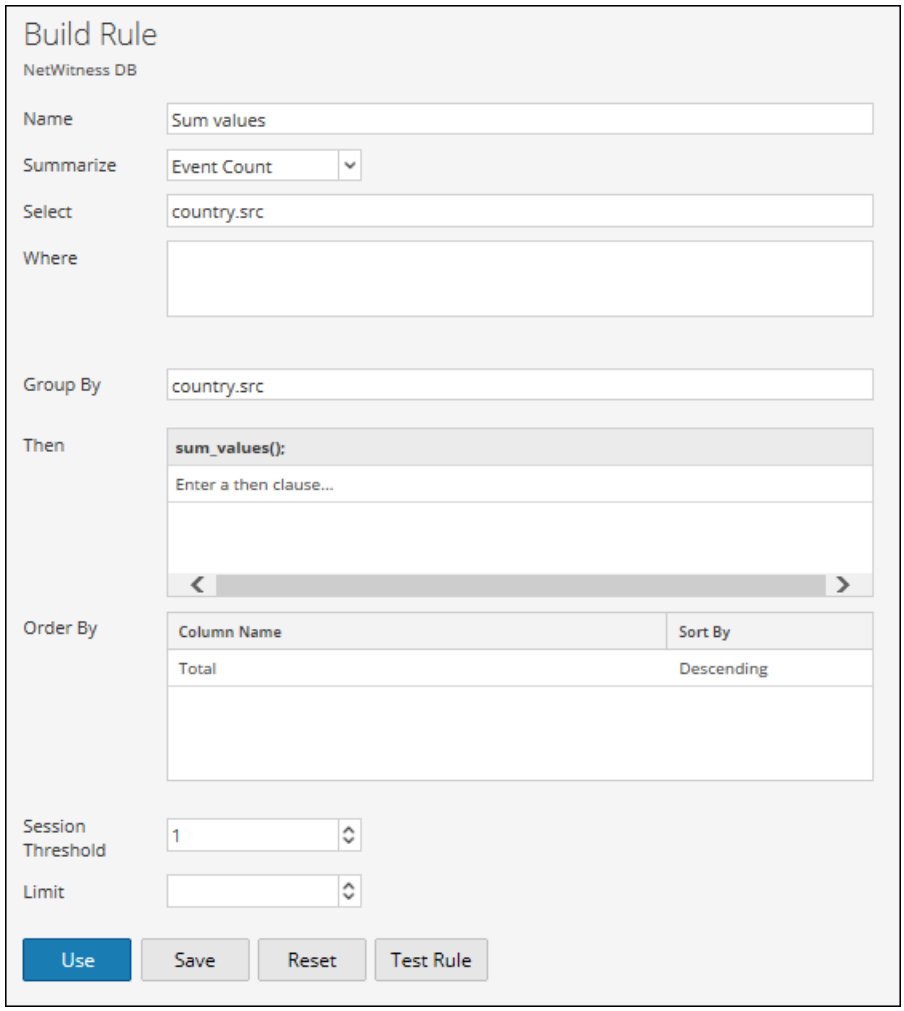



`sum_values()`

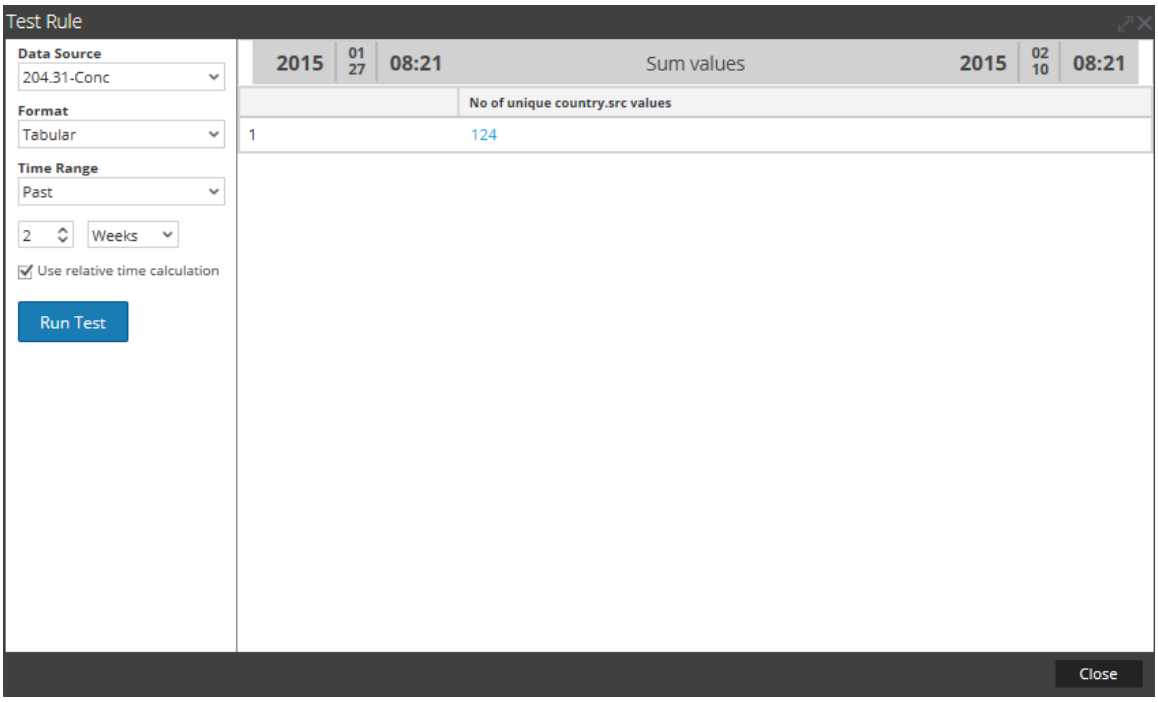
Zählt die Anzahl der Werte für einen angegebenen Ergebnissatz zusammen. Mit dieser Aktion zeigen Sie an, wie viele Entsprechungen für eine angegebene Regel existieren.

**Beispiel:**

Die folgende Abbildung zeigt die Regelaktion „sum_values()“.




Die folgende Abbildung zeigt das Ergebnis mit der Regelaktion „sum_values()“.




## show_whats_new()

Die Regelaktion „show_whats_new()“ nimmt ein beliebiges Ergebnis in einem Ergebnissatz und filtert alle Werte heraus, die bereits vor dem Zeitrahmen des derzeit ausgeführten Berichts in der NetWitness-Metadatenbank verfügbar waren. Wenn ein Bericht ausgeführt wird, bestimmt NetWitness Suite die ID der ersten Sitzung im Zeitbereich des Berichts. Wenn ein Wert in einem Ergebnissatz eine erste Sitzungs-ID hat, die größer als die erste Sitzungs-ID des Berichtzeitrahmens ist, war sie vor Ausführung des Berichts noch nicht in der NetWitness-Metadatenbank vorhanden und ist folglich im NetWitness-System relativ zum Zeitrahmen des Berichts neu.

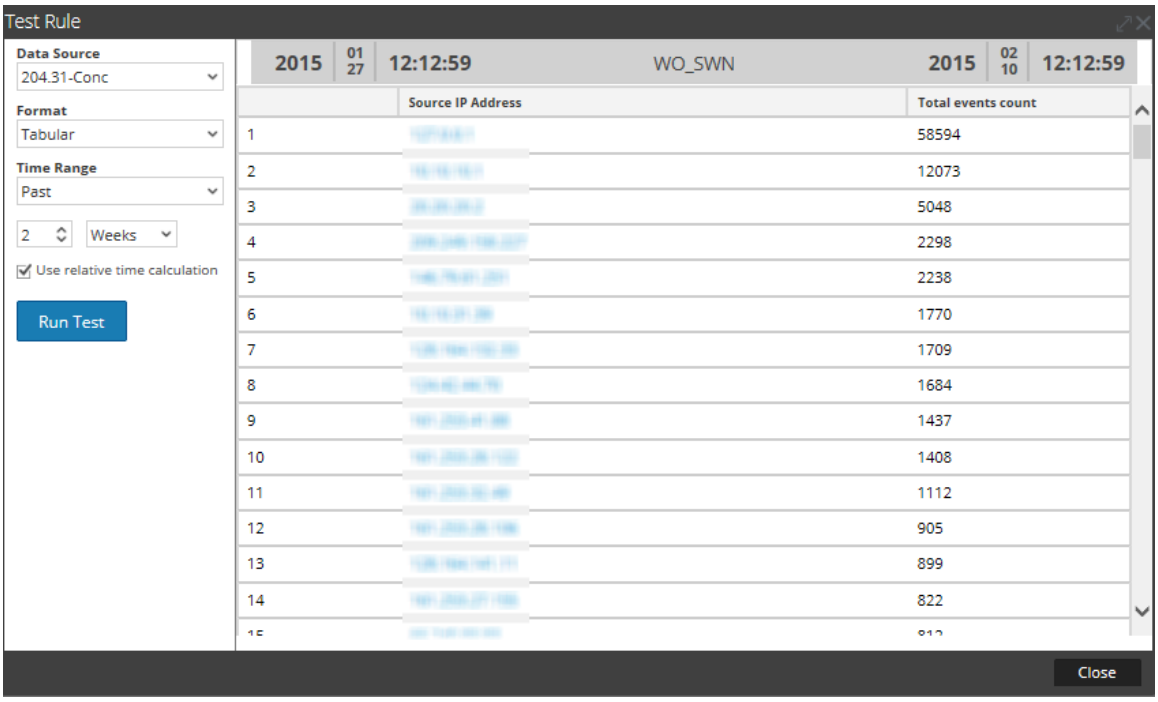
Die Regelaktion „show_whats_new()“ wird auch für die benutzerdefinierte Aggregatregel unterstützt. Werden in der benutzerdefinierten Regel mehrere Metawerte ausgewählt, wird der erste zum Herausfiltern der alten Werte herangezogen. Die Verwendung dieser Regelaktion für die benutzerdefinierte Aggregatregel wird in Beispiel 2 verdeutlicht.

**Hinweis:** Die Regelaktion „show_whats_new()“ kann nicht mit einer Aggregatregel verwendet wird.

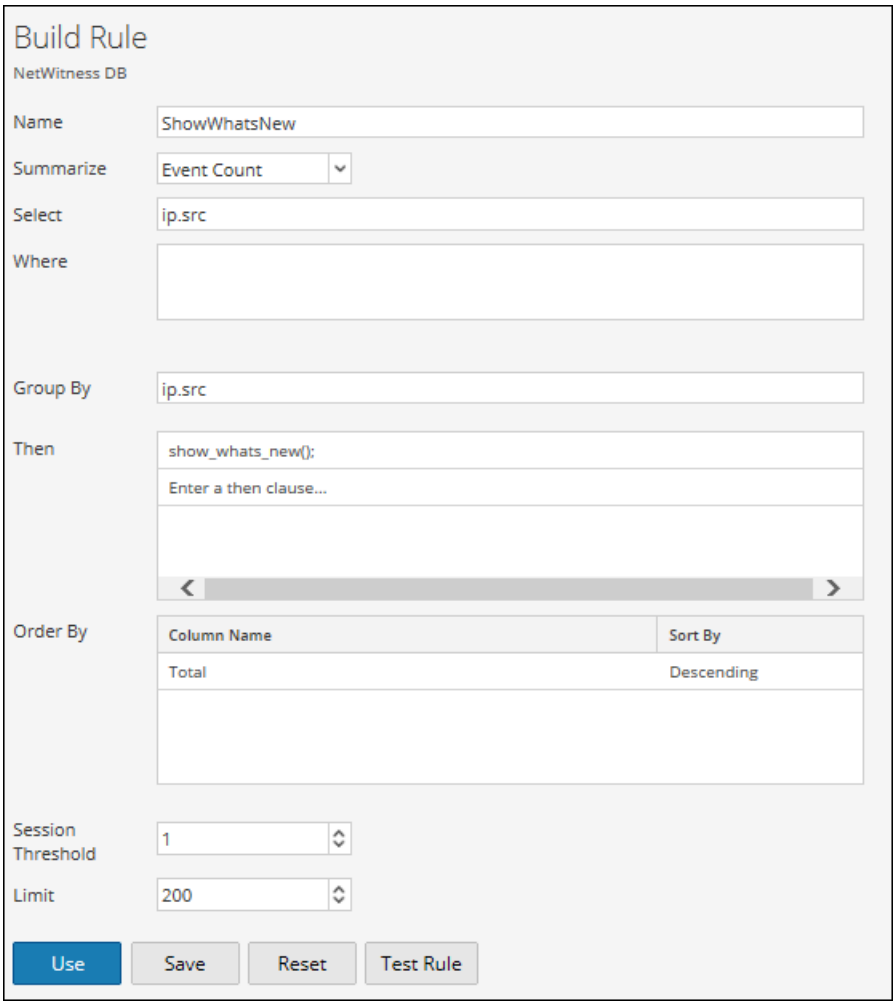
**Beispiele:**

**1. „show_whats_new()“ für eine Aggregatregel mit Ereignisanzahl**

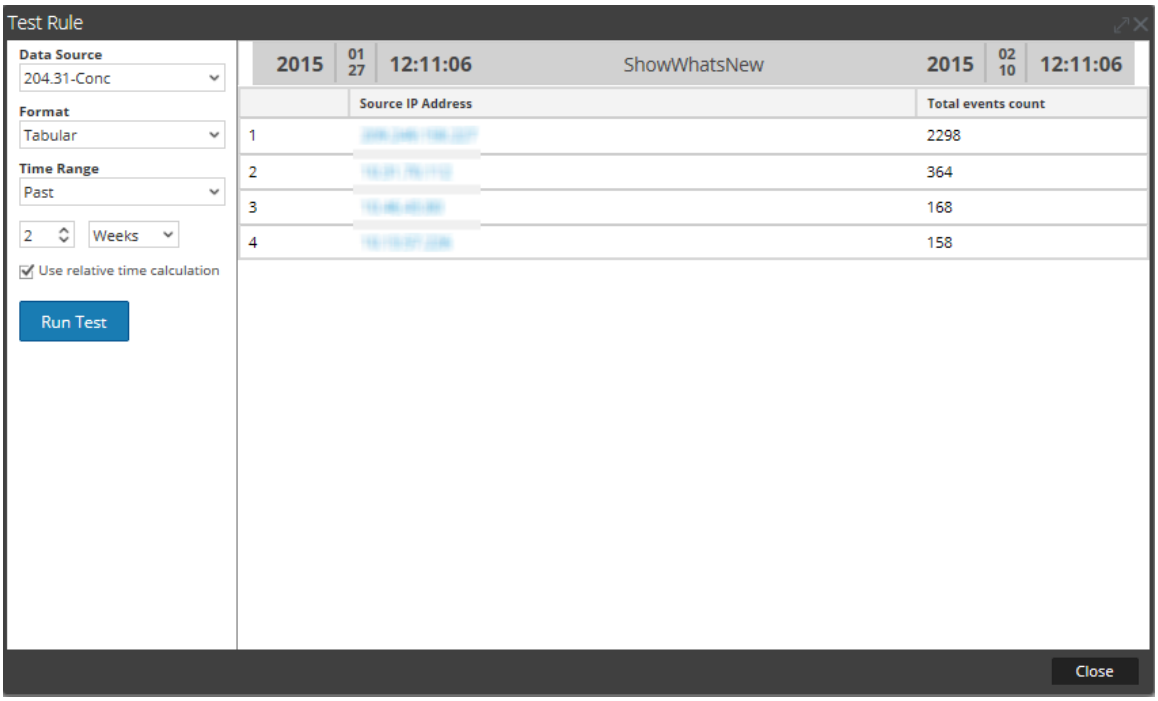
Im folgenden Beispiel werden alle verfügbaren Quell-IP-Adressen der vergangenen zwei Wochen aufgelistet.




Die folgende Abbildung zeigt, wie mit der Regelaktion „show_whats_new“ nur die neuen Einträge der letzten zwei Wochen aufgelistet werden.

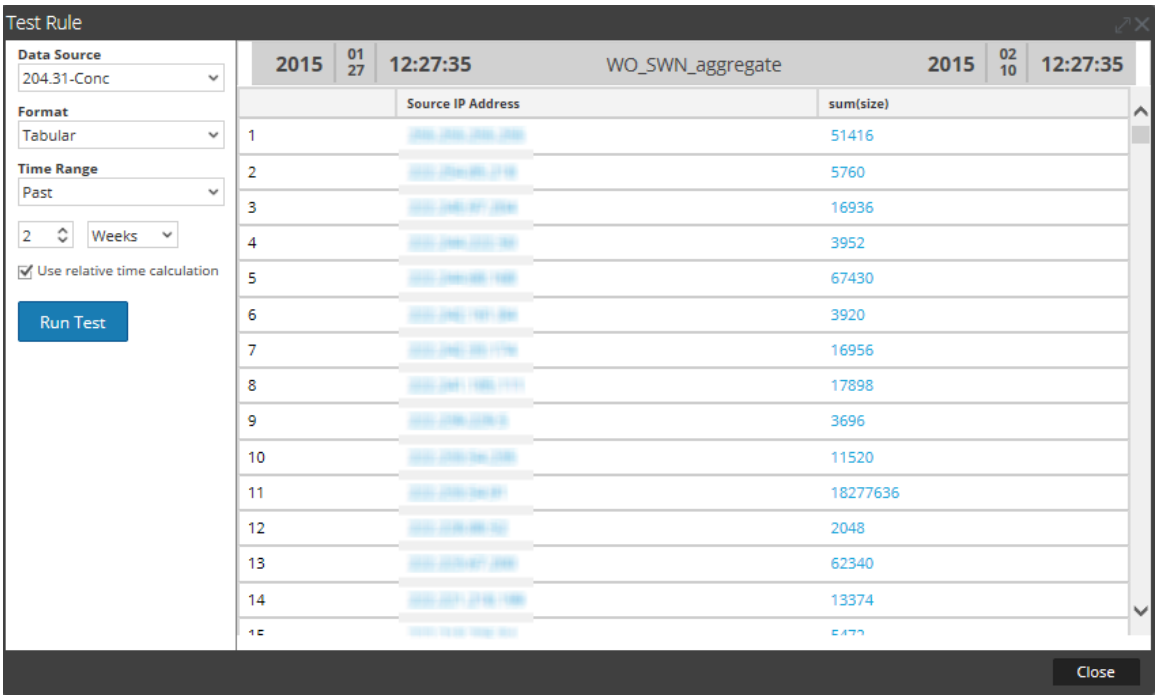



In der folgenden Abbildung werden die neuen Einträge der letzten zwei Wochen aufgelistet.

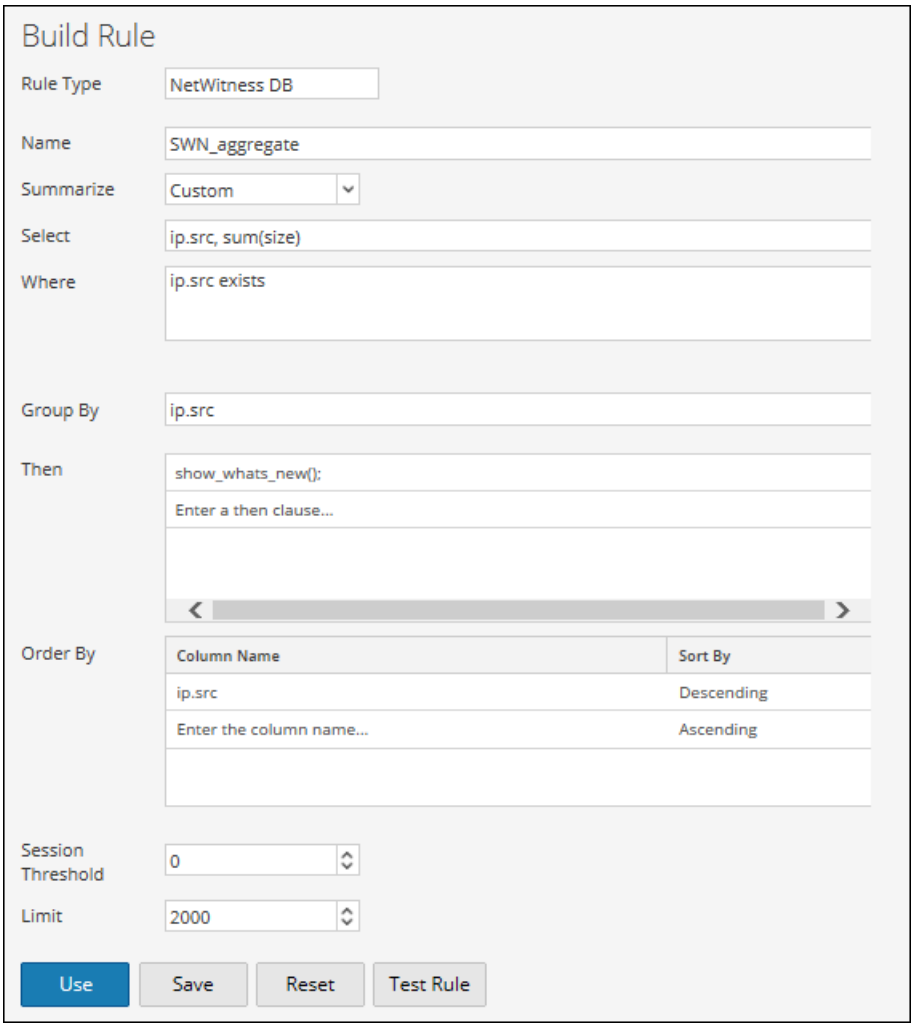



### 2. „show_whats_new()“ für eine benutzerdefinierte Aggregatregel

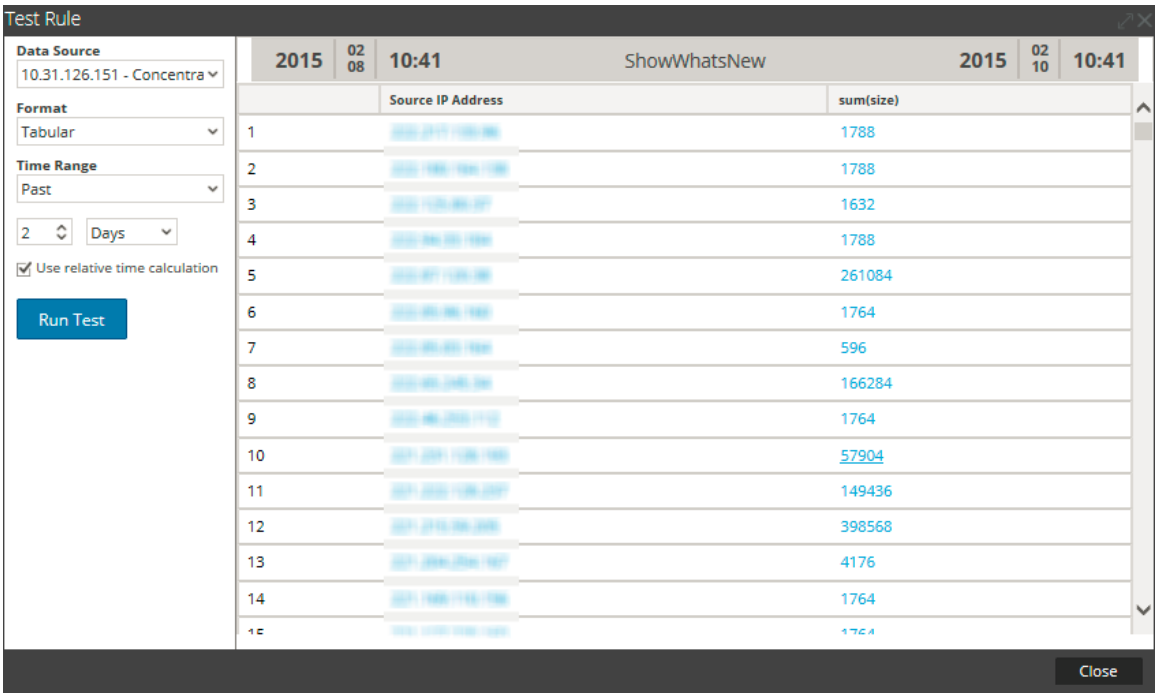
Im folgenden Beispiel werden alle verfügbaren Quell-IP-Adressen der vergangenen zwei Wochen aufgelistet.




Die folgende Abbildung zeigt, wie mit der Regelaktion „show_whats_new“ nur die neuen Einträge der letzten zwei Wochen aufgelistet werden.




In der folgenden Abbildung werden die neuen Einträge für Quell-IP-Adressen der letzten zwei Wochen aufgelistet.




Der Vorteil dieser Funktion liegt darin, dass es nicht darauf ankommt, wann der Bericht ausgeführt wird; Werte, die in NetWitness neu sind, können jederzeit identifiziert werden. Der Nachteil dieser Funktion liegt darin, dass, wenn die Daten zurückgesetzt werden, Ihre Daten verloren gehen. Es ist jedoch einfach, eine Baseline für ein System zu erstellen und Änderungen und neue Einträge zu identifizieren, ohne dass das System zu stark belastet wird (abhängig von der Größe Ihres Ergebnissatzes).

## Unterstützte Regeloperatoren

Die Datenquellen-Regelsyntax der NWDB Reporting Engine unterstützt einen Teilsatz der von NetWitness Suite unterstützten Regeloperatoren.

| Syntax | Beschreibung |
|---|---|
| * | Verwenden Sie ein Sternchen (*) als alleinigen Operator in einer Regel, um den gesamten Datenverkehr auszuwählen. |
| = | Operator gleich |
| != | Operator ungleich |
| && | Logischer Operator AND |
| \|\| | Logischer Operator OR |

| Syntax | Beschreibung |
|---|---|
| -u | Oberer Grenzwert. Beispiel: **tcp.port = 40000-u** wählt alle TCP-Ports über 40000 aus. |
| -l | Unterer Grenzwert. Beispiel: **tcp.port = l-40000** wählt alle TCP-Ports unter 40000 aus. |
| - | Der Bindestrich (-) gilt nur für numerische Werte. Trennen Sie die unteren und oberen Grenzwerte des Bereichs durch einen Bindestrich (-). Beispiel: **tcp.port = 25-443** wählt alle TCP-Ports zwischen 25 und 443 aus. |

**Beispielgestützte Abfragen**

## Regelsyntax von Respond

Die unterstützte Regelsyntax für den Reagieren-Service anhand von Beschreibungen und Beispielen für unterstützte und nicht unterstützte Syntax. Bei der Erstellung von Regeln für Berichte mithilfe des Reagieren-Service können Sie auf eine endliche Menge von Syntaxausdrücken zurückgreifen.

Die Reporting Engine unterstützt die folgenden Kategorien der Reagieren-Datenquellen-Regelsyntax:

- **select**-Klausel
  - Nichtaggregatregel
  - Aggregatregel
- **alias**
- **where**-Klausel
- **where**-Klauseloperatoren
- Gruppieren nach
- Sortieren nach
- Feld **Grenzwert**

**Hinweis:** Liste wird in Respond-Datenquellenregeln nicht unterstützt.

### Select-Klausel

Die Select-Klausel ist eine durch Kommas getrennte Liste von Werten. Beispiel: select alert.severity, alert.name, count(*).

Es gibt zwei Arten von Select-Klauseln für Reagieren-Regeln:

- Nichtaggregatregel
- Aggregatregel

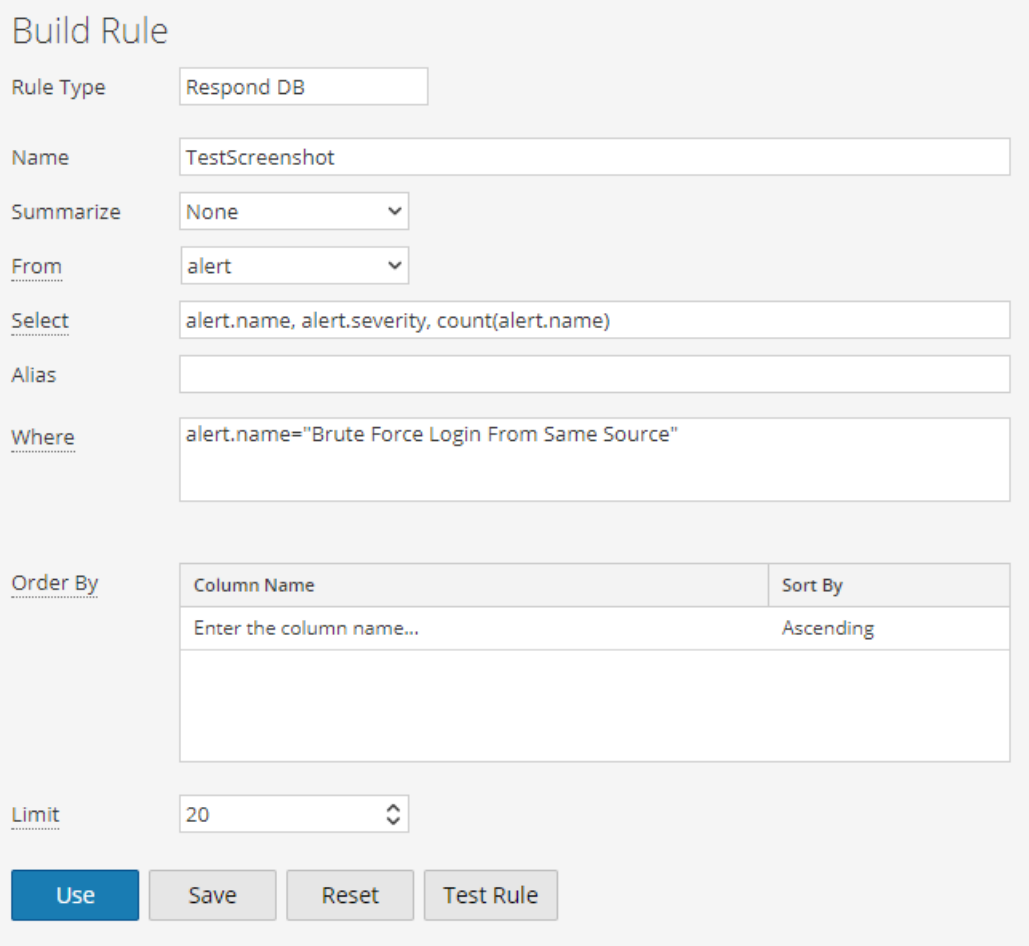
## Nichtaggregatregel

Wenn Sie eine Regel ohne eine Gruppierung definieren möchten, wählen Sie im Feld „Zusammenfassen“ die Option „Keine“ aus. In einer Nichtaggregatregel können Sie in der *Select*-Klausel eine beliebige Anzahl von Metadaten auswählen. Beispiel: select alert.severity, alert.name.

## Aggregatregel

Wenn Sie bestimmte Metadaten und den zugehörigen Aggregatwert abfragen möchten, müssen Sie die Aggregatregel verwenden. Um ein Aggregat zu erhalten, müssen Sie im Feld **Zusammenfassen** „Benutzerdefiniert“ auswählen, um der *Select*-Klausel eine Aggregatfunktion hinzuzufügen. Beispiel: select alert.severity, alert.name, count(*).

Die folgende Abbildung zeigt die Ansicht „Regel erstellen“ für die Aggregatregel.




## Unterstützte Aggregatfunktionen

Die Regeln für den Reagieren-Service unterstützen die folgenden Aggregatfunktionen und die folgende Syntax.

- count
- max
- min
- sum
- avg

**Hinweis:** Für das Aggregieren von Abfragen müssen Aggregatfunktionen am Ende einer Select-Klausel hinzugefügt werden. Beispiel: alert.name, alert.severity, sum (alert.numEvents). Standardmäßig werden Ergebnisse mit maximal 10.000 Zeilen abgerufen und dies kann mithilfe von **rsa.response.query.QueryProperties** konfiguriert werden.

**Beispiele für die select-Klausel-Syntax**

Die folgende Tabelle enthält Beispiele für die select-Klausel-Syntax.

| Beispiele | Beschreibung |
|---|---|
| select<br>*column1*<br>,<br>*column2*<br>,*column3*,...,*columnN* | Wählen Sie bestimmte Metadaten aus einer Reagieren-Datenquelle aus (trennen Sie die Spalten voneinander durch ein Komma). |

**Beispiele für unterstützte Select-Abfragen**

select alert.name, alert.numEvents, count(alert.numEvents)

select alert.severity, avg(alert.severity)

select alert.timestamp, incidentCreated where alert.timestamp >= 1475658011

## Zusammenfassung

„Zusammenfassen“ bestimmt den Typ der Zusammenfassung oder Aggregation für die Regel.

| Name | Konfigurationswert |
|---|---|
| Zusammenfassen | Wählen Sie zum Abfragen von Metadaten ohne eine benutzerdefinierte Gruppierung folgende Option aus:<br>• **Ohne**:<br>Zum Abrufen auf Metadaten basierender Aggregate wählen Sie Folgendes aus:<br>• **Benutzerdefiniert**: Dadurch wird angegeben, dass die erwartete Metaaggregatfunktion in der select-Klausel der Regel definiert ist. |

## Alias

Einige Metanamen sind möglicherweise nicht beschreibend. In diesem Fall kann die Beschreibung im Aliasfeld hinzugefügt werden, damit Spaltennamen besser lesbar sind.
Beispiel: **SELECT**: alert.severity, alert.name, count(*)
**ALIAS**: Schweregrad der Warnmeldung, Name der Warnungmeldung

Im Aliasfeld können Sie einen Namen für Spalten eingeben, die in der SELECT-Klausel verwendet werden. Wenn Sie den Alias für eines der Felder in der Select-Klausel nicht angeben, wird die Standardbeschreibung verwendet. Wenn die Select-Klausel z. B. Feld1, Feld2, Feld3, Feld4 aufweist und Alias nur Feld1, Feld3, Feld4 aufweist, wird für Feld2 eine Standardbeschreibung verwendet.

## Where-Klausel

Die where-Klausel ist ein Sprachfeldwert und -bereich, der von der Funktion Reagieren verwendet wird. In der where-Klausel müssen Zeichenfolgenwerte in Apostrophe gesetzt werden.

| Beispiele | Beschreibung |
|---|---|
| alert.host summary =' (Primary) Link status "Down" on interface INTNAME.' | Schließen Sie Zeichenfolgen oder Text, die in Daten vom Typ TEXT oder im Zeichenfolgenformat enthalten sind, in einfache Anführungszeichen ein. Sollte ein Sonderzeichen in den Daten vorhanden sein (z. B. Apostroph), müssen Sie ein zusätzliches einfaches Anführungszeichen oder doppelte Anführungszeichen verwenden. Beispiel: alert.name = 'top alerts from Cote d''Ivoire'. |
| alert.timestamp >= 1475658011 | Verwenden Sie für Datums- und Zeitangaben (Spalten mit Daten vom Typ Datum/Zeitstempel) die EPOCH-Syntax: |

## Unterstützte where-Klauseloperatoren

| Operator | Syntax |
|---|---|
| = (ist gleich) | *column1* = '*value*' |
| != (ist ungleich) | *column1* != '*value*' |
| > | *column1* > '*value*' |
| >= | *column1* >= '*value*' |
| < | *column1* < '*value*' |
| <= | *column1* <= '*value*' |

## Gruppieren nach

| Syntax | Funktion |
| --- | --- |
| Gruppieren nach: alert.severity, alert.timestamp, IncidentCreated<br><br>**Hinweis:** Das Feld „Gruppieren nach“ ist für aggregierte Abfragen aktiviert und kann nicht bearbeitet werden. | Reagieren wählt automatisch die Metadaten für das Feld „Gruppieren nach“ aus der ausgewählten Select-Klausel aus. |

## Sortieren nach

„Sortieren nach“ legt fest, wie der Ergebnissatz sortiert wird und unterscheidet nicht zwischen Groß- und Kleinschreibung.

| Name | Konfigurationswert |
| --- | --- |
| Spaltenname | Spaltenname ist der Name der Spalten, nach denen Sie die Ergebnisse sortieren möchten. Standardmäßig ist der Wert leer. Wenn Sie auf eine Spalte klicken, wird der Wert auf Basis des Felds „Zusammenfassen“ aufgefüllt.<br>• order by alert.name asc<br>• order by incidentCreated desc<br>• order by count(numEvents)<br>• order by status |
| Sortieren nach | „Sortieren nach“ bestimmt die Reihenfolge, in der Sie die Ergebnisse sortieren möchten, etwa auf- oder absteigend.<br><br>**Hinweis:** Bei allen Abfragen ist es erforderlich, das Feld „Sortieren nach“ auszuwählen. |

## Feld Grenzwert

Gibt den Grenzwert an, der für die Abfrage gelten soll, wenn Daten aus der Datenbank abgerufen werden. Wenn ein Ergebnissatz nach Ereignisanzahl, Paketanzahl oder Sitzungsgröße sortiert wird, repräsentiert der Grenzwert die obersten (oder untersten) wiederzugebenden n Werte. Wenn die Ergebnismenge nicht
sortiert wird, werden die ersten n Werte wiedergegeben.

## Warehouse-DB – Einfache Regelsyntax

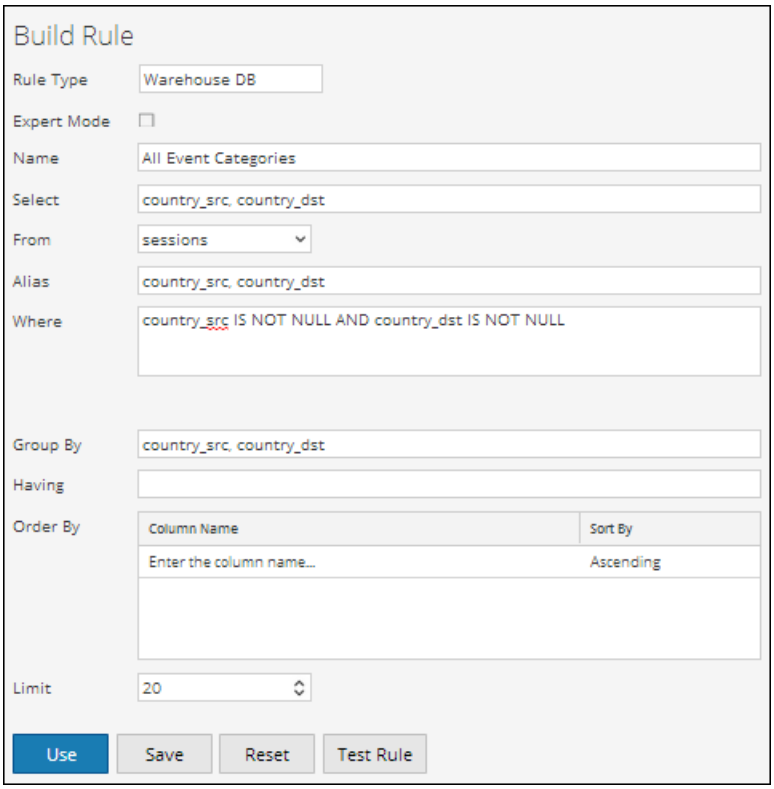
Im Abschnitt werden die einfache Regelsyntax und Beispiele erläutert.

Die folgenden Beispiele illustrieren einfache Regeln im Standardmodus:

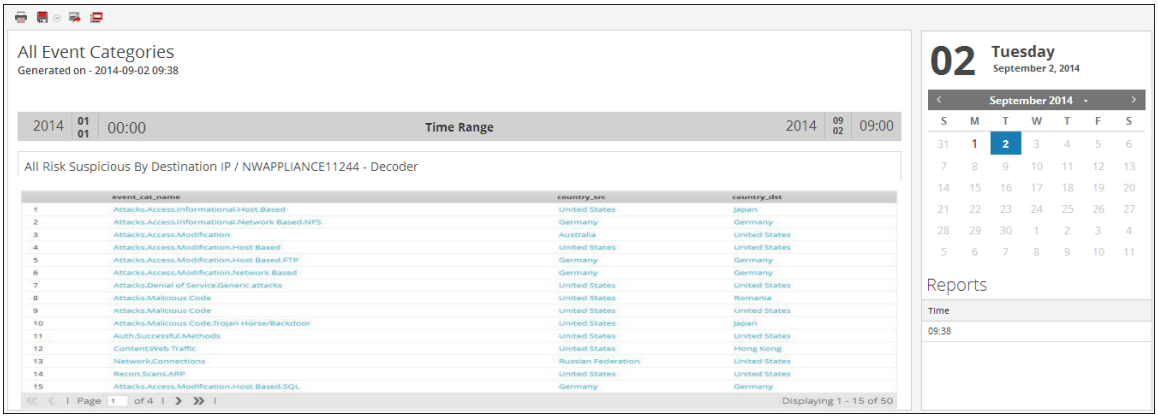
- Bericht „Alle Ereigniskategorien“
- Bericht „Angriff-Ereigniskategorien“
- Quelle: Bericht „China-Ereigniskategorien“
- Bericht „IP-Quelle- und Ziel-Ereigniskategorien“
- Bericht „Bedrohungskategorien nach Zeit“
- Bericht „Array-Site“
- Bericht „Abfragen unverarbeiteter Protokolle“

## Bericht „Alle Ereigniskategorien“

Diese Regel ruft alle Ereigniskategorien, das Quellland und das Zielland aus der Tabelle **Sitzungen** ab, indem Aliasnamen (temporäre Spaltennamen) für jedes der Felder definiert werden, die aus der Tabelle abgerufen werden sollen: **country_src** für das Quellland und **country_dst** für das Zielland.

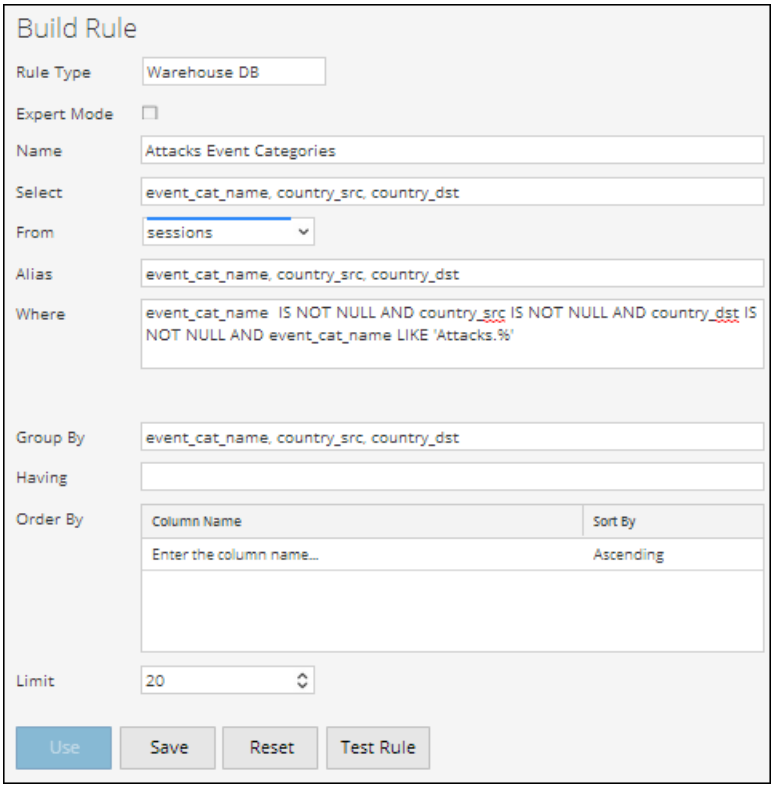


In der folgenden Abbildung sehen Sie den Ergebnissatz für die Regel „Alle Ereigniskategorien“.

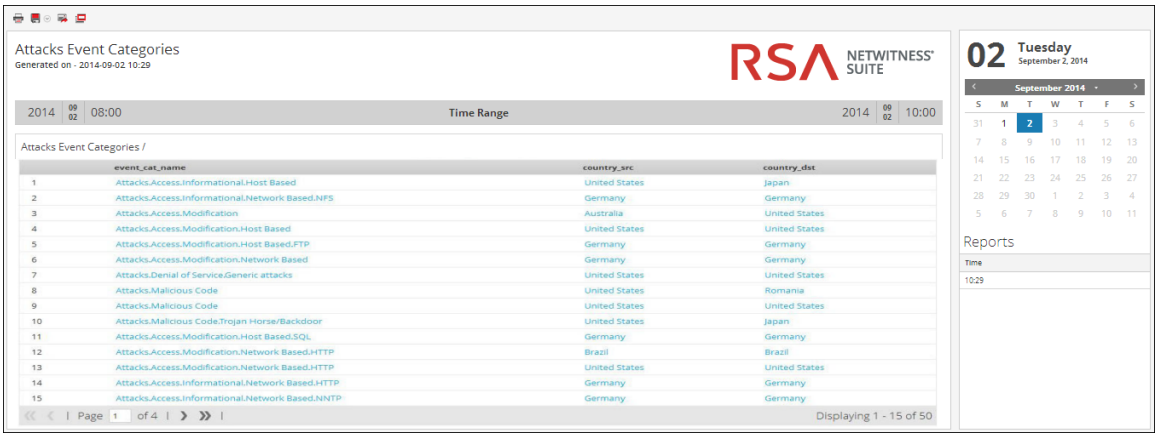



## Bericht „Angriff-Ereigniskategorien“

Diese Regel ruft alle Ereigniskategorien, das Quellland und das Zielland aus der Tabelle **Sitzungen** ab, indem Aliasnamen (temporäre Spaltennamen) für jedes der Felder definiert werden, die aus der Tabelle abgerufen werden sollen, und nur die Spalten ausgewählt werden, deren Ereigniskategorienamen „Attacks.%“ entsprechen.

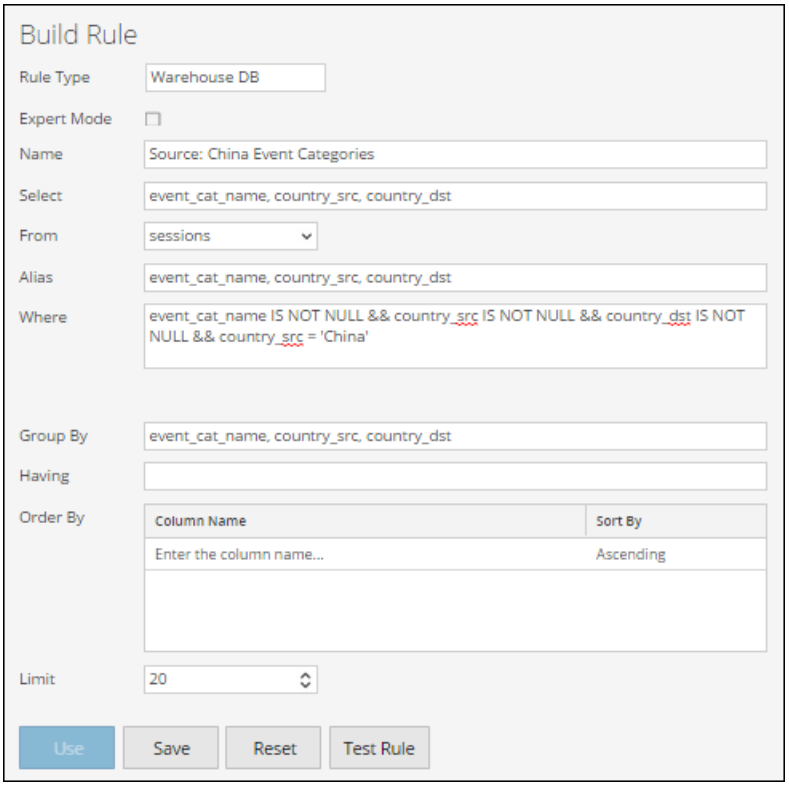



In der folgenden Abbildung sehen Sie den Ergebnissatz für die Regel „Angriff-Ereigniskategorien“.

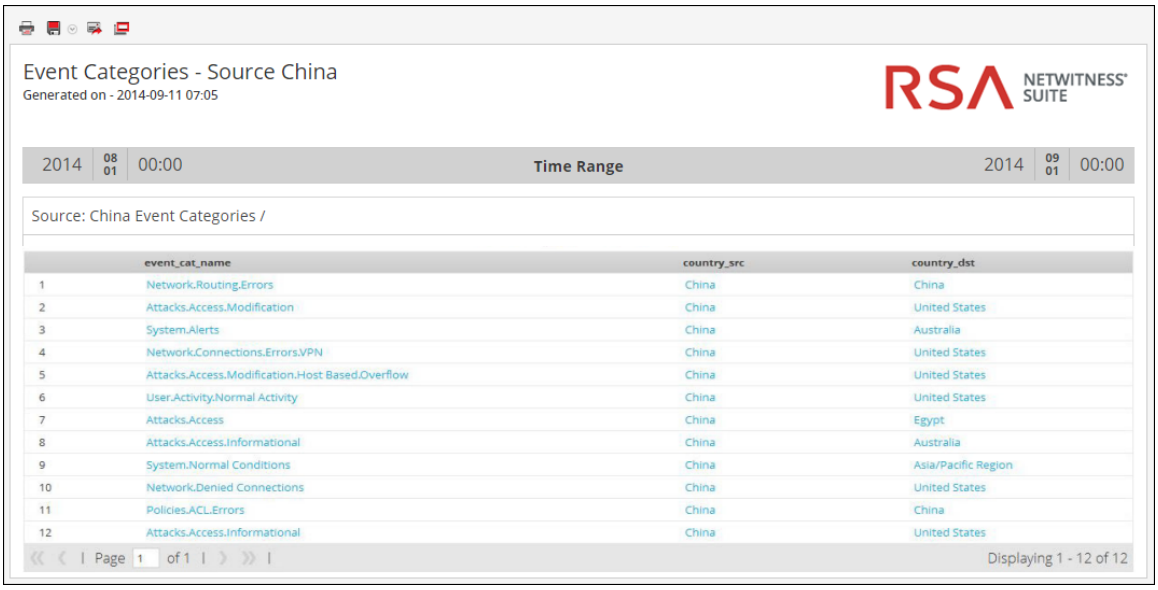



## Quelle: Bericht „China-Ereigniskategorien“

Diese Regel ruft alle Ereigniskategorien, das Quellland und das Zielland aus der Tabelle **Sitzungen** ab, indem Aliasnamen (temporäre Spaltennamen) für jedes der Felder definiert werden, die aus der Tabelle abgerufen werden sollen, und nur die Spalten ausgewählt werden, deren Quellland „China“ ist.




In der folgenden Abbildung ist der Ergebnissatz für die Regel „Quelle: China-Ereigniskategorien“ dargestellt.



Event Categories - Source China
Generated on - 2014-09-11 07:05

RSA NETWITNESS SUITE

2014 | 08 01 | 00:00 | Time Range | 2014 | 09 01 | 00:00

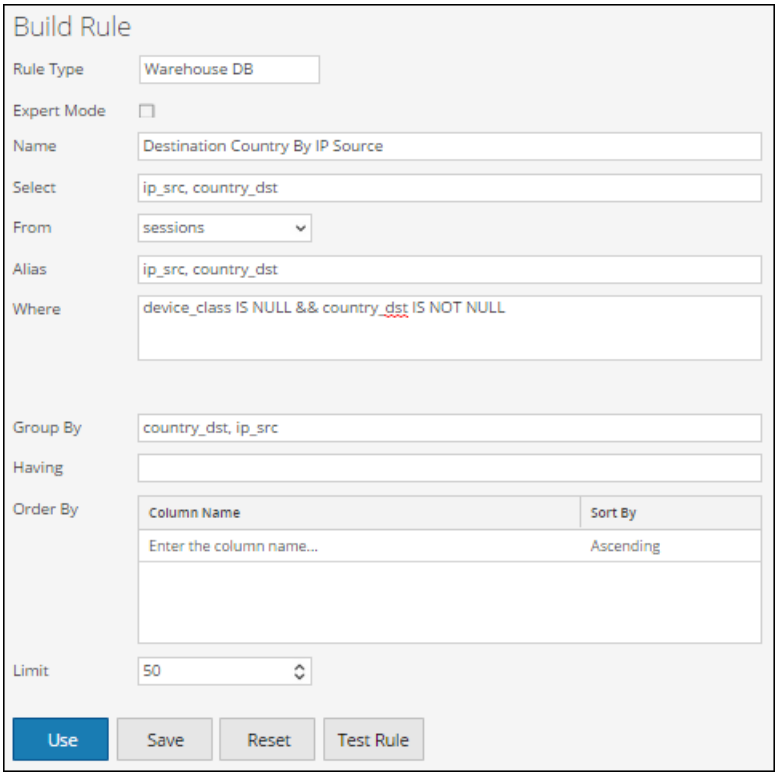
Source: China Event Categories /

| | event_cat_name | country_src | country_dst |
|---|---|---|---|
| 1 | Network.Routing.Errors | China | China |
| 2 | Attacks.Access.Modification | China | United States |
| 3 | System.Alerts | China | Australia |
| 4 | Network.Connections.Errors.VPN | China | United States |
| 5 | Attacks.Access.Modification.Host Based.Overflow | China | United States |
| 6 | User.Activity.Normal Activity | China | United States |
| 7 | Attacks.Access | China | Egypt |
| 8 | Attacks.Access.Informational | China | Australia |
| 9 | System.Normal Conditions | China | Asia/Pacific Region |
| 10 | Network.Denied Connections | China | United States |
| 11 | Policies.ACL.Errors | China | China |
| 12 | Attacks.Access.Informational | China | United States |

Page 1 of 1 | Displaying 1 - 12 of 12

## Bericht IP-Quelle- und Ziel-Ereigniskategorien

Diese Regel ruft die IP-Adresse des Quell- und Ziellandes aus der Tabelle **Sitzungen** ab, indem Aliasnamen (temporäre Spaltennamen) für jedes der Felder definiert werden, die aus der Tabelle abgerufen werden sollen, und nur die Spalten ausgewählt werden, deren Zielland NICHT NULL ist.



Build Rule

Rule Type: Warehouse DB

Expert Mode: ☐

Name: Destination Country By IP Source

Select: ip_src, country_dst

From: sessions

Alias: ip_src, country_dst

Where: device_class IS NULL && country_dst IS NOT NULL

Group By: country_dst, ip_src

Having:

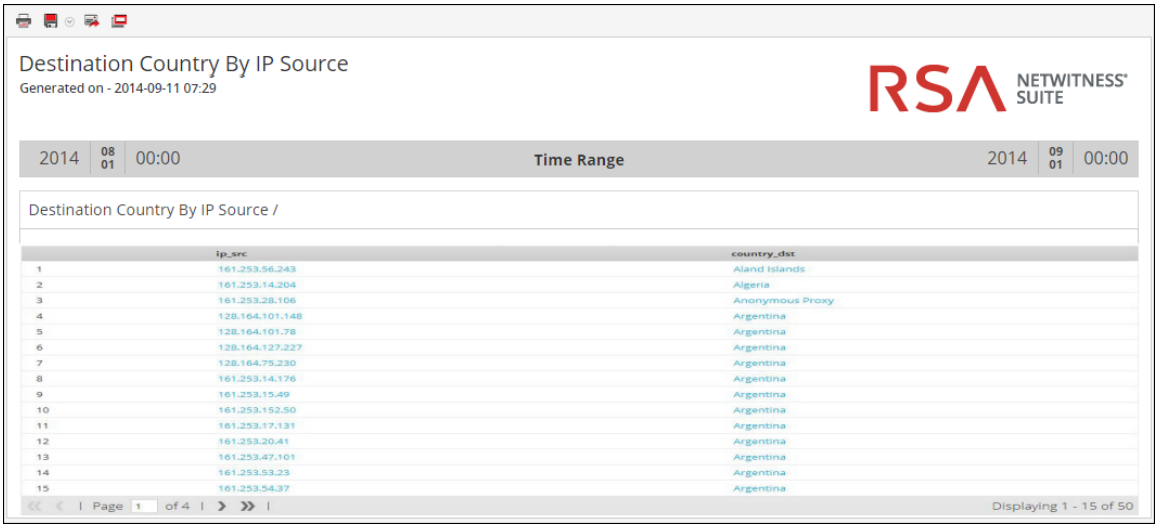
Order By:

| Column Name | Sort By |
|---|---|
| Enter the column name... | Ascending |

Limit: 50

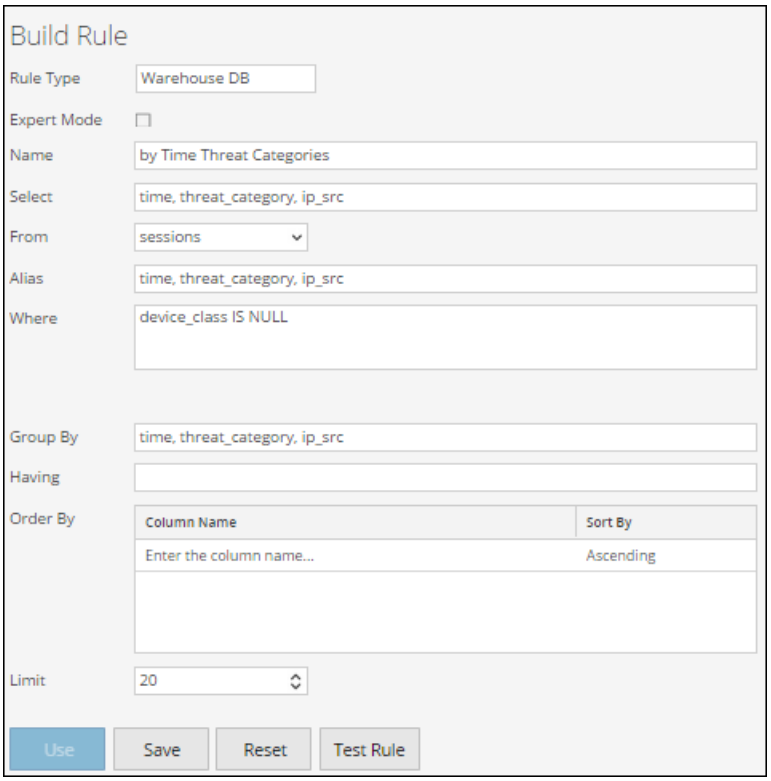
Use | Save | Reset | Test Rule

In der folgenden Abbildung sehen Sie den Ergebnissatz für die Regel „IP-Quelle-und Ziel-Ereigniskategorien“.



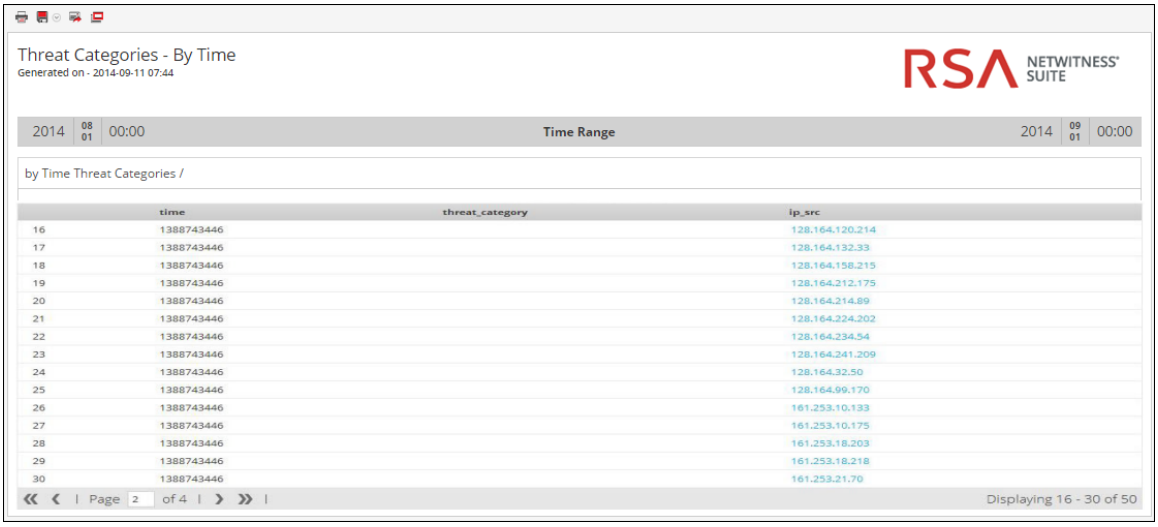

## Bericht Bedrohungskategorien nach Zeit

Diese Regel ruft die Ereignisse der Kategorie Bedrohung, die Uhrzeit, zu der das Protokoll oder das Ereignis in den Log Decoder/Decoder aufgenommen wurde, und die Quell-IP-Adressen aus der Tabelle **Sitzungen** ab, indem Aliasnamen (temporäre Spaltennamen) für jedes dieser Felder definiert werden, die aus der Tabelle abgerufen werden sollen.



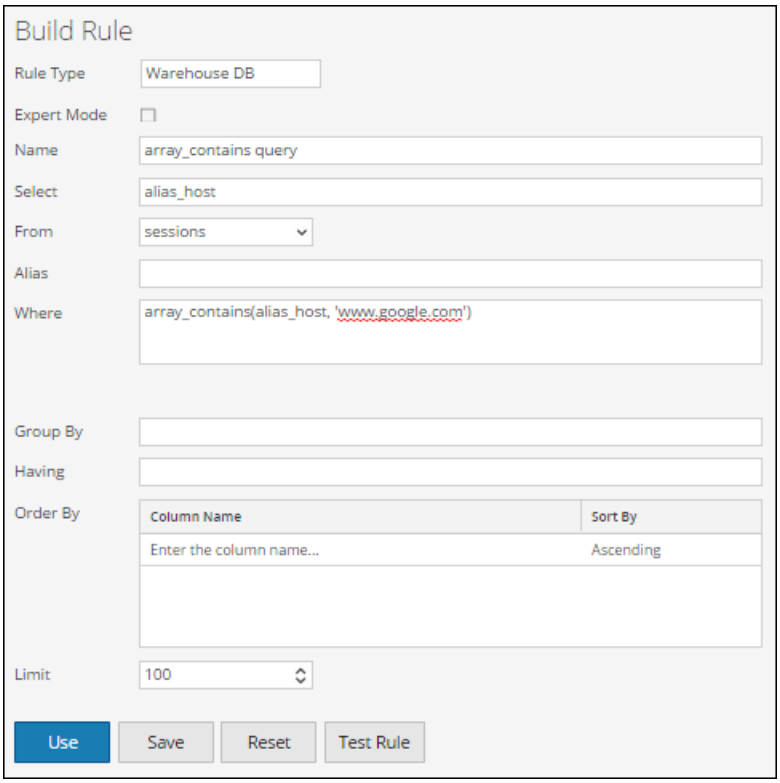
Die folgende Abbildung zeigt den Ergebnissatz für die Regel „Zeit-Bedrohungskategorien“. Die Zeit, die im Zeitfeld angezeigt wird, ist die UNIX-Zeit (z. B. 1388743446).

**Hinweis:** In der Select-Klausel wäre die Syntax „UNIX time“; im Bericht wird dies in UTC-Zeit konvertiert. Sie können UNIX-Zeit (1388743446) z. B. mit dem Zeitkonvertierungstool Epoch in UTC-Zeit (Coordinated Universal Time) umwandeln (03.01.2014 15:34:06).

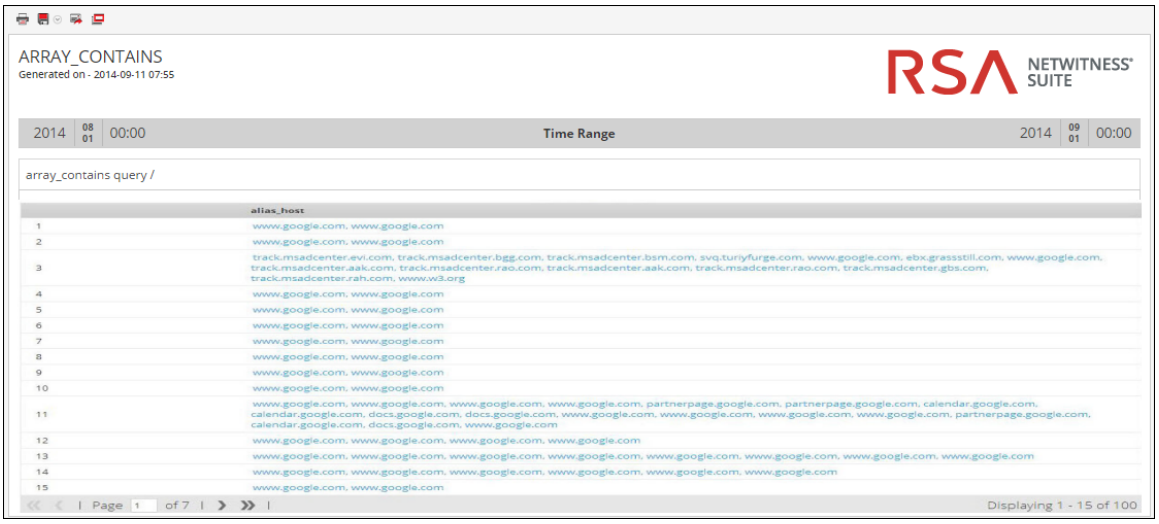



## Bericht Array-Site

Diese Regel ruft ein Array von Aliashostnamen aus der Tabelle **Sitzungen** ab, die den Wert „www.google.com“ enthalten.



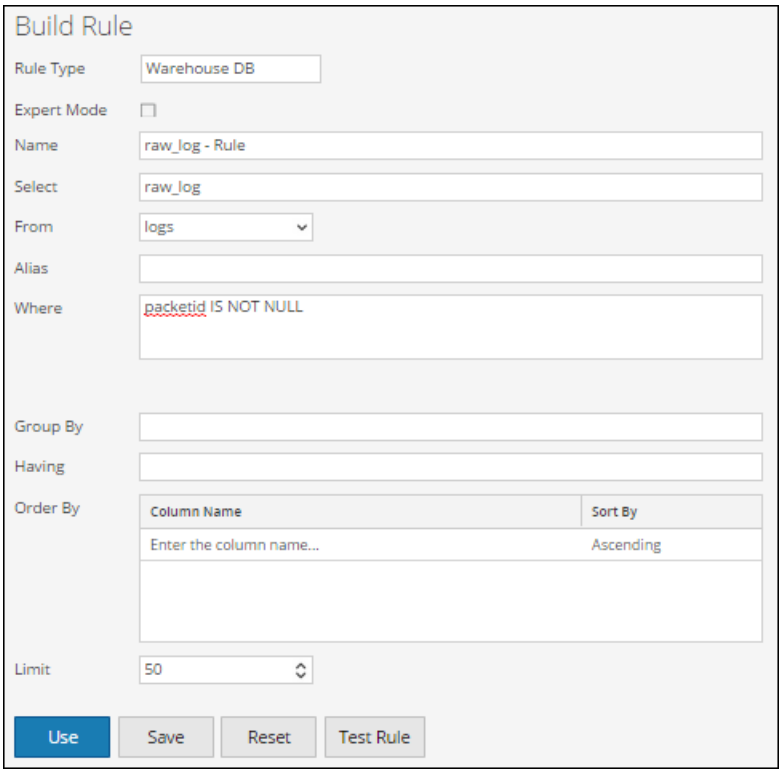

In der folgenden Abbildung sehen Sie den Ergebnissatz, der zurückgegeben wird, wenn ein Array aus Sitzungen abgefragt wird.



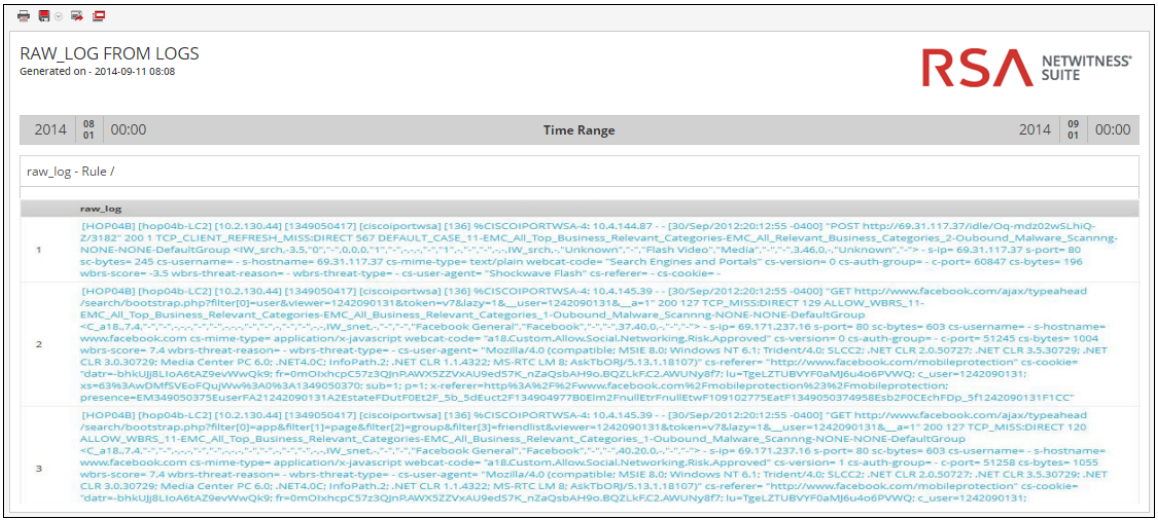

## Bericht Abfragen unverarbeiteter Protokolle

Unverarbeitete Protokolle können entweder aus der Tabelle „Protokolle“ oder „Sitzungen“ abgerufen werden.

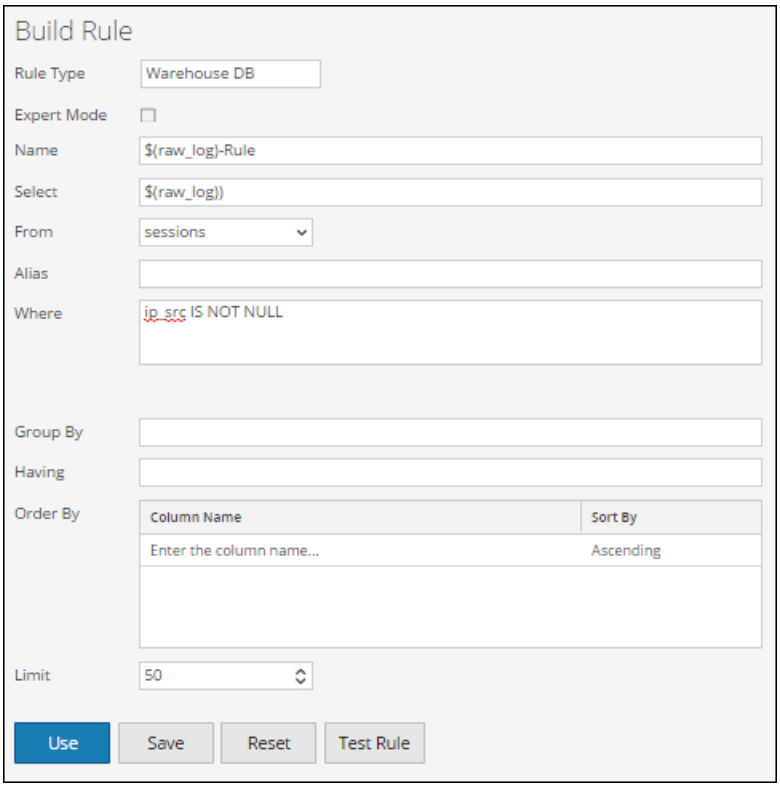
Diese Regel verwendet **raw_log** als Metadaten für die Abfrage unverarbeiteter Protokolle aus Protokollen, deren Paket-ID NICHT NULL ist.



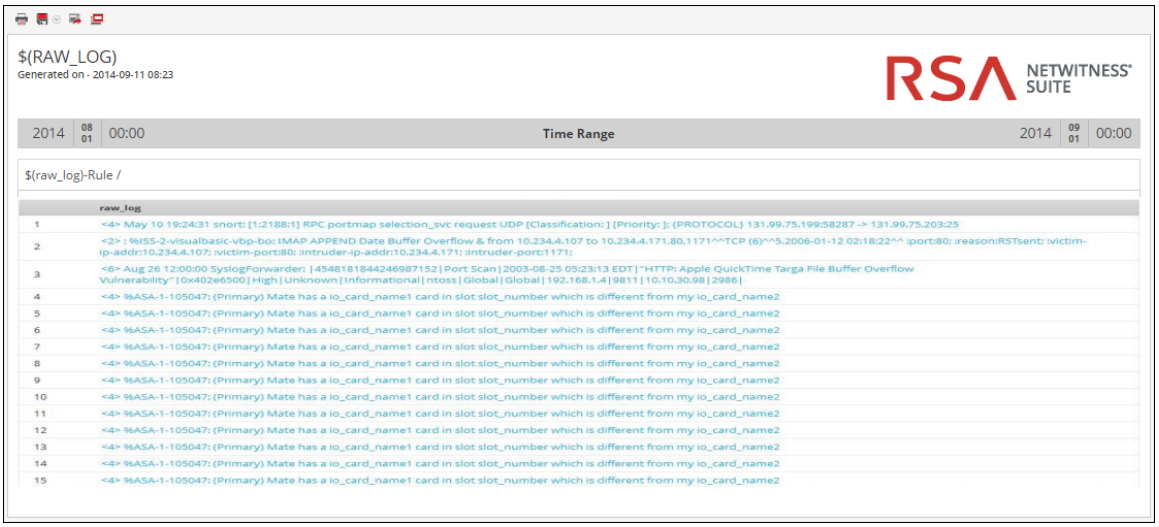

In der folgenden Abbildung sehen Sie den Ergebnissatz für die Abfrage unverarbeiteter Protokolle aus Protokollen.




Diese Regel verwendet **${raw_log}** als Metadaten für die Abfrage unverarbeiteter Protokolle aus Sitzungen, deren Quell-IP-Adresse NICHT NULL ist.




In der folgenden Abbildung sehen Sie den Ergebnissatz für die Abfrage unverarbeiteter Protokolle aus Sitzungen.

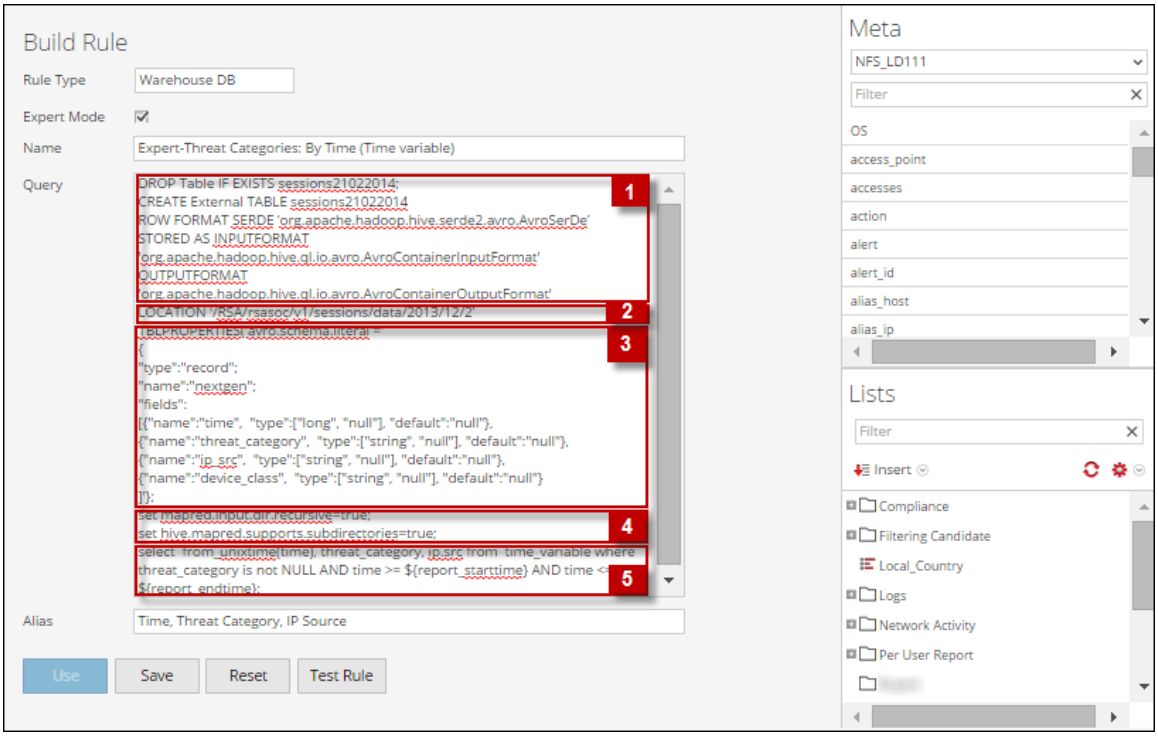


## Warehouse-DB – Erweiterte Regelsyntax

Im Abschnitt werden die erweiterte Regelabfragesyntax und Beispiele erläutert.

# Allgemeine Syntax einer erweiterten Regel

In der folgenden Abbildung sehen Sie, wie erweiterte Abfragen definiert werden.




Folgende Syntax ist ein Beispiel einer erweiterten Abfrage:

```
DROP Table IF EXISTS sessions21022014;

CREATE External TABLE sessions21022014

ROW FORMAT SERDE ‘org.apache.hadoop.hive.serde2.avro.AvroSerDe’

STORED AS INPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2’

TBLPROPERTIES('avro.schema.literal'='
 {

"type":"record";

"name":"nextgen";
```

```
"fields":
 [
 {"name":"time",  "type":["long", "null"], "default":"null"},
{"name":"threat_category",  "type":["string", "null"],
"default":"null"},
{"name":"ip_src",  "type":["string", "null"], "default":"null"},
{"name":"device_class",  "type":["string", "null"], "default":"null"}
 ]
 '};
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

select `from_unixtime(time), threat_category, ip.src` from `time_variable` where `threat_category` is not `NULL` and `time >= ${report_starttime}` and `time <= ${report_endtime};`

**Hinweis:** Reporting Engine behandelt eine Zeile, die mit <hyphen> <hyphen> beginnt, in einer Expert Warehouse-Regel als Kommentar.
Beispiel:

```
set mapred.input.dir.recursive=true;
-- This is an Expert comment
 set hive.mapred.supports.subdirectories=true;
```

Die allgemeine Syntax einer erweiterten Abfrage wird unten erklärt:

1. Eine externe Tabelle erstellen und anlegen und anschließend die Zeile formatieren:
   Zunächst legen wird die Tabelle ab, wenn die Tabelle bereits vorhanden ist, und erstellen die externe Tabelle **sessions21022014**

   ```
   DROP TABLE IF EXISTS sessions21022014
    CREATE EXTERNAL TABLE sessions21022014.
   ```

   **Hinweis:** Sie müssen nur dann eine externe Tabelle erstellen, wenn Sie gerade eine andere Tabelle benutzen. Wenn Sie zum Beispiel eine andere Tabelle außer **sessions21022014** verwenden, müssen Sie die Tabelle ablegen und eine externe Tabelle erstellen.

   Spezifizieren Sie dann das Zeilenformat als Avro.SerDe-Schnittstelle, um HIVE über die Verarbeitung eines Berichts anzuweisen. Mithilfe von Avro.SerDe können Sie Avro-Daten als HIVE-Tabellen lesen und speichern und sie als Eingabe- und Ausgabeformat speichern.

   ```
   ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.Avro.SerDe'
    STORED AS INPUTFORMAT
   'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
    OUTPUTFORMAT
   'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'
   ```

2. HDFS-Verzeichnis angeben:
   Im nächsten Schritt müssen Sie das HDFS-Verzeichnis '/RSA/rsasoc/v1/sessions/data/2013/12/2' angeben, aus dem die Daten vor der Ausführung der HIVE-Anweisungen abgefragt werden. Der Speicherortparameter spezifiziert die Daten, die abhängig von ihrem Eingabedatum abgerufen werden müssen. Dies ist ein Variablenparameter. Folglich können Sie Werte nach dem festgelegten Eingabedatum abrufen.
3. Tabellenschema definieren:
   Im dritten Schritt definieren Sie das Tabellenschema, indem Sie Spalten mit einem spezifischen Datentyp und Standardwert als „Null“ definieren.

```
TBLPROPERTIES('avro.schema.literal'='
 {"type":"record";
 "name":"nextgen";
 "fields":
 [
 {"name":"ip_src",  "type":["string", "null"], "default":"null"}
 ]
 '};
```

4. Daten von dem Verzeichnis, das Unterverzeichnisse enthält, importieren:
   Anschließend müssen Sie HIVE aktivieren, damit alle Unterverzeichnisse rekursiv gescannt und alle Daten aus allen Unterverzeichnissen abgerufen werden.

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

5. Daten aus der HIVE-Tabelle abrufen:
   Sobald Sie alle oben angeführten Anweisungen ausgeführt haben, können Sie die Datenbank mit der HIVE-Abfrageklausel **Auswählen** abfragen, um die Daten aus der HIVE-Tabelle abzurufen.

Folgende Beispiele beschreiben erweiterte Regeln im Expertenmodus:

- Stündlicher, täglicher, wöchentlicher und monatlicher Bericht
- Tabellenpartition auf Basis eines Standortberichts
- Verbinden von Protokollen und Sitzungen auf Grundlage eines unique_id-Berichts
- Listenbericht
- Parametrisierter Bericht

- Partitionsbasierte Tabelle mit mehreren Speicherorten
- Automatisierte Partitionierung mithilfe der benutzerdefinierten Funktion(ab Version 10.5.1)

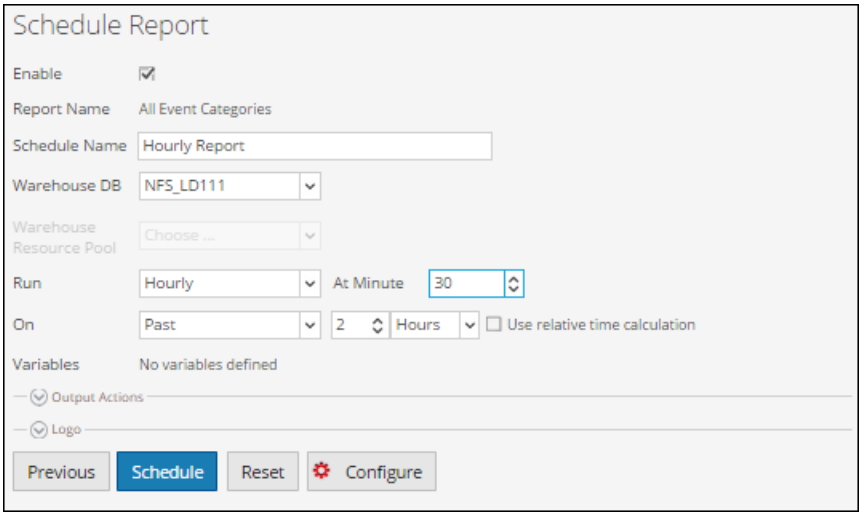
## Stündlicher, täglicher, wöchentlicher und monatlicher Bericht

In diesen Beispielregeln können Sie verschiedene Berichte für den 2. Dezember 2013 erstellen (siehe Abbildung unten). Die Variable „Datum“ in der Anweisung LOCATION kann verändert werden, je nachdem, in welcher Sie einen stündlichen, täglichen, wöchentlichen und monatlichen Bericht erstellen können.

## Stündlicher Bericht

In dieser Beispielregel können Sie einen stündlichen Bericht für den 2. Dezember 2013 erstellen. Die Anweisung LOCATION kann verändert werden, um einen stündlichen Bericht zu erzeugen.

**LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2'** - Die Datumsangabe (2013/12/2) steht für Jahr/Monat/Tag. Die gesamten Daten für den 2. Dezember 2013 werden mithilfe der Anweisung LOCATION abgerufen.

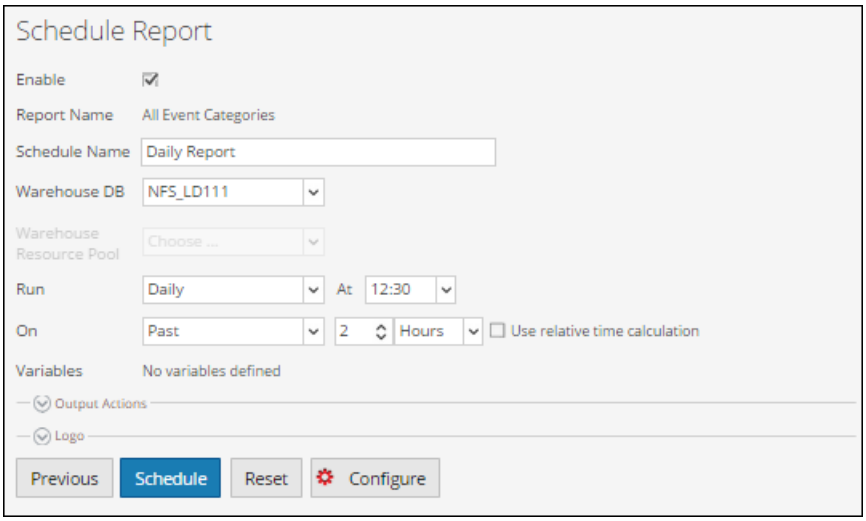



Der Ergebnissatz dieser Abfrage wäre ein stündlicher Bericht.

## Täglicher Bericht

In dieser Beispielregel können Sie einen täglichen Bericht für Dezember 2013 erstellen. Die Anweisung LOCATION kann verändert werden, um einen täglichen Bericht zu erzeugen.

**LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12'** – Die Datumsangabe (2013/12) steht für Jahr/Monat. Die gesamten Daten für Dezember 2013 werden mithilfe dieser Location-Anweisung abgerufen.

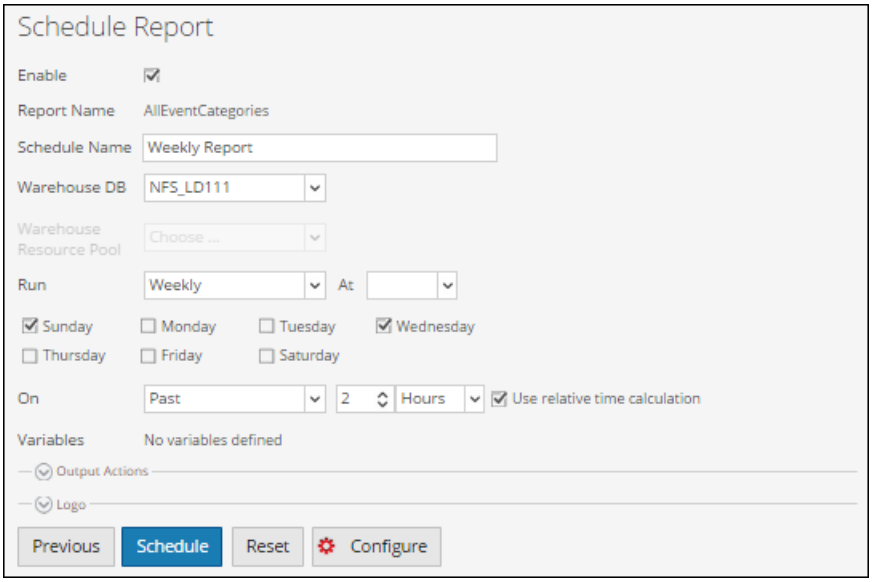



Das ResultSet dieser Abfrage wäre ein täglicher Bericht.

## Wöchentlicher Report

In dieser Beispielregel können Sie einen wöchentlichen Bericht für Dezember 2013 erstellen. Die Anweisung LOCATION kann verändert werden, um einen wöchentlichen Bericht zu erzeugen.

**LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12'** – Die Datumsangabe (2013/12) steht für Jahr/Monat. Die gesamten Daten für Dezember 2013 werden mithilfe dieser Location-Anweisung abgerufen.

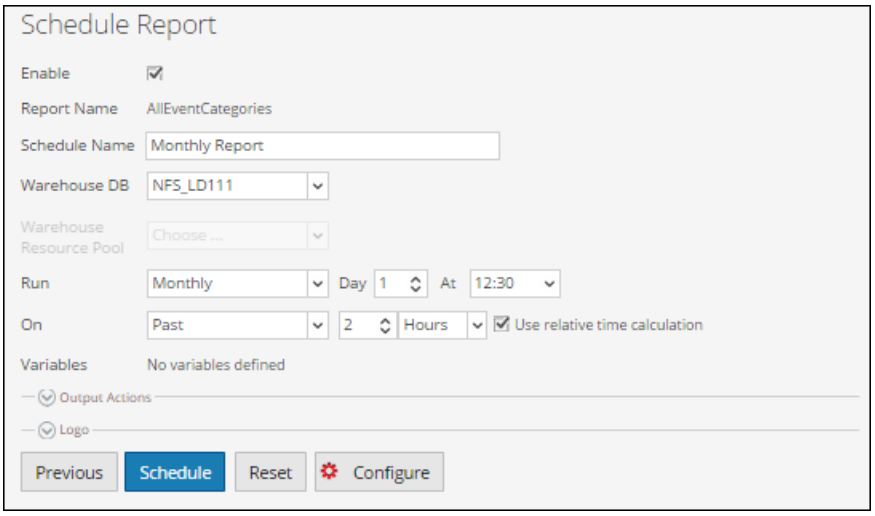



Der Ergebnissatz dieser Abfrage wäre ein wöchentlicher Bericht.

## Monatlicher Bericht

In dieser Beispielregel können Sie einen monatlichen Bericht für das Jahr 2013 erstellen. Die Anweisung LOCATION kann verändert werden, um einen monatlichen Bericht zu erzeugen.

**LOCATION '/RSA/rsasoc/v1/sessions/data/2013'** – Die Datumsangabe (2013) steht für Jahr. Die gesamten Daten für das Jahr 2013 werden mithilfe dieser Location-Anweisung abgerufen.



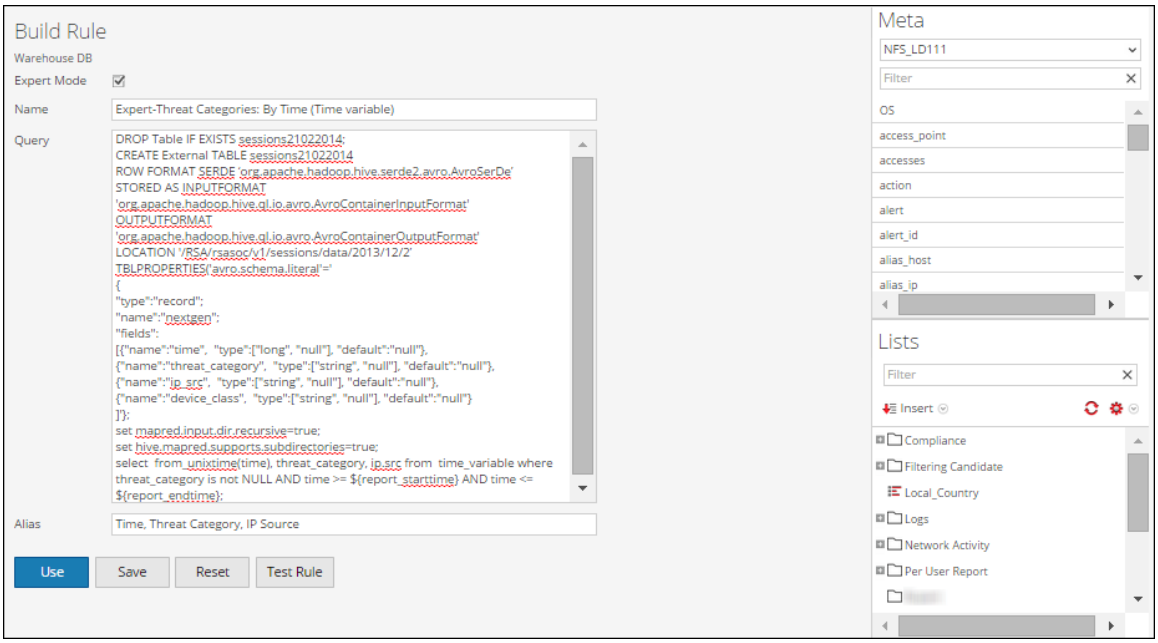

Der Ergebnissatz dieser Abfrage wäre ein monatlicher Bericht.

Weitere Informationen zur LOCATION-Definition erhalten Sie unter **HDFS-Standort spezifizieren** in dem Abschnitt **Allgemeine Syntax einer erweiterten Regel**.

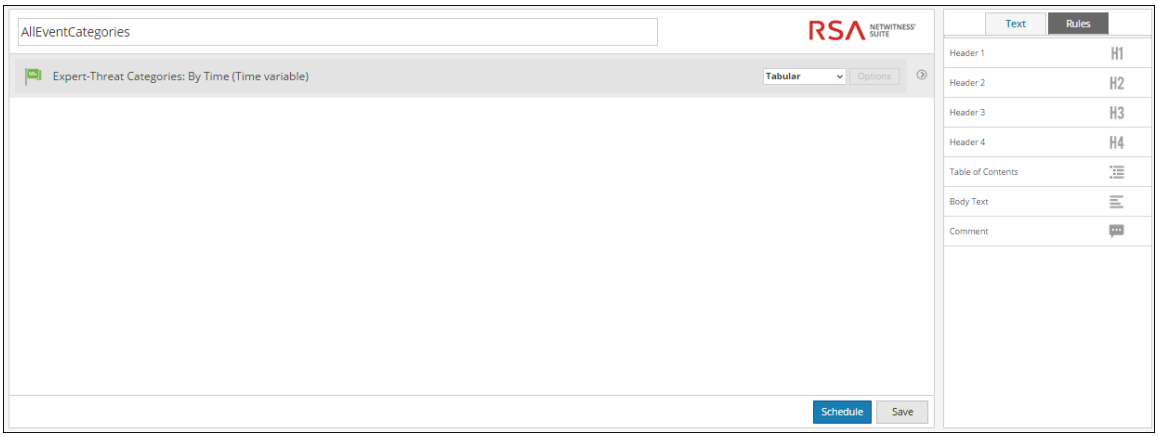
Führen Sie folgende Schritte nacheinander aus, um das ResultSet einer erweiterten Regel anzusehen.

1. Definieren einer erweiterten Regel
2. Hinzufügen einer erweiterten Regel zu einem Bericht
3. Planen von Berichten
4. Anzeigen von geplanten Berichten

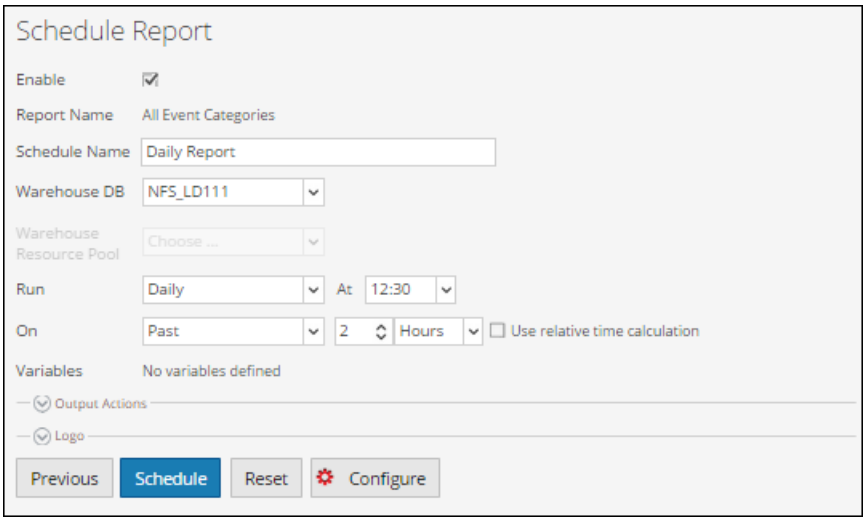
Die folgende Abbildung zeigt, wie Sie eine erweiterte Regel definieren können.




Die folgende Abbildung zeigt, wie Sie einem Bericht eine erweiterte Regel hinzufügen (Zum Beispiel **AllEventCategories**).




Die folgende Abbildung zeigt, wie Sie einen täglichen Bericht planen.

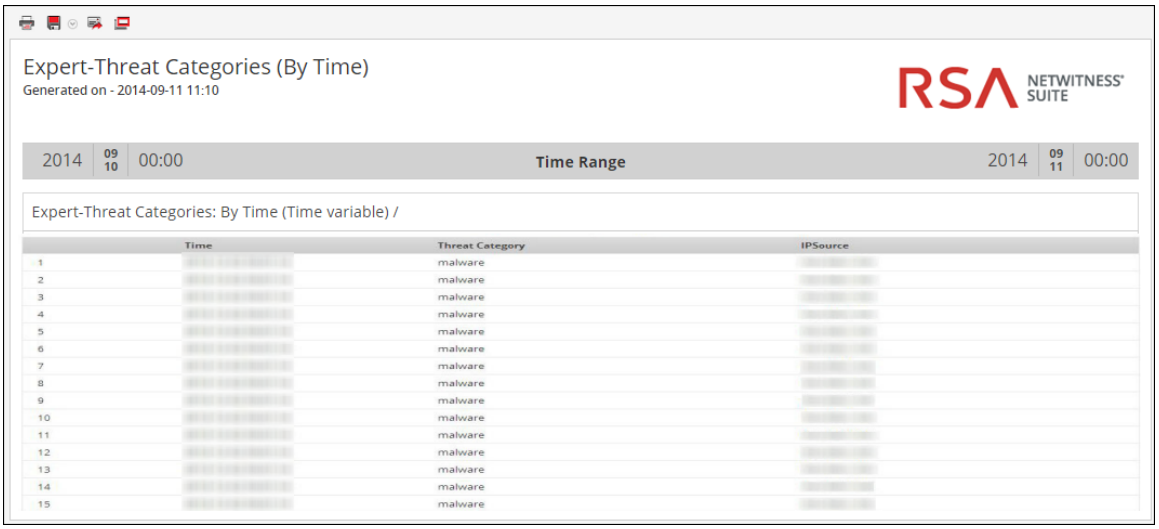



Wenn Sie einen Bericht für einen bestimmten Zeitraum erzeugen möchten, müssen Sie den Zeitraum in der Abfrage mithilfe der folgenden zwei Variablen manuell definieren:

`${report_starttime} - The starting time of the range in seconds.`
`${report_endtime} - The ending time of the range in seconds.`

Beispiel: `SELECT from_unixtime(time), threat_category, ip.src FROM time_variable WHERE threat_category is not NULL AND time >= ${report_starttime} AND time <= ${report_endtime};`

Die folgende Abbildung zeigt den Ergebnissatz der Planung eines täglichen Berichts.

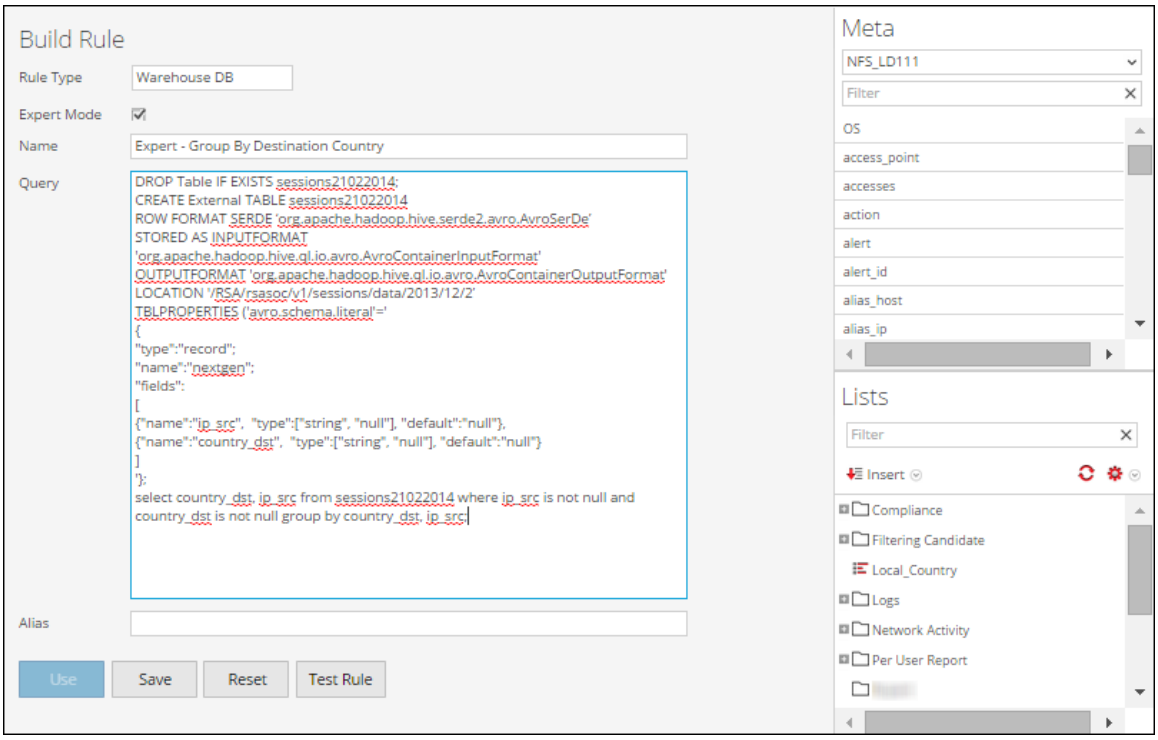



## Tabellenpartition auf Basis eines Standortberichts

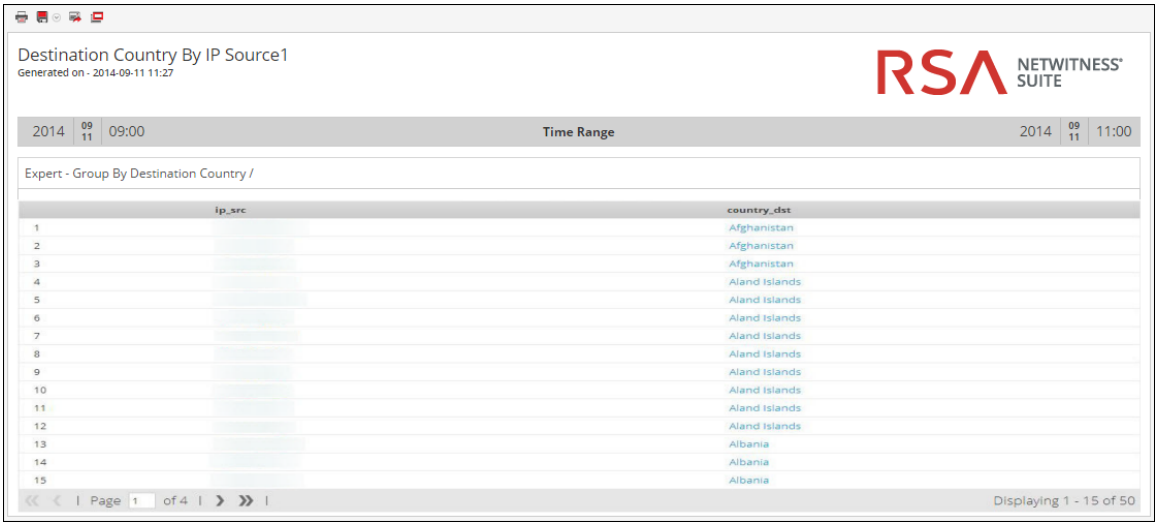
In dieser Beispielregel können Sie eine standortbasierte Tabellenpartition erstellen. Jede Tabelle kann einen oder mehrere Partitionsschlüssel haben, die festlegen, welche Daten gespeichert werden. Zum Beispiel: Ein country_dst des Typs STRING und ein ip_src des Typs STRING. Jeder einzelne Wert der Partitionsschlüssel definiert eine Partition der Tabelle.

In dem angeführten Beispiel wird eine HIVE-Abfrage ausgeführt, um das Zielland und die IP-Adresse der Quelle aus der Tabelle sessions05032014 abzurufen und den Ergebnissatz zu gruppieren, die in diesen Feldern eingestellt sind.

Diese Regel bietet Informationen zur erstellten Tabelle, zur formatierten Zeile, zum Speicherort (Verzeichnispfad) für Avro-Datendateien in Warehouse und gibt einen Ergebnissatz anhand der HIVE-Abfrage zurück, um anzuzeigen, dass die Abfrage einen Ergebnissatz zurückgegeben hat. Weitere Informationen zu diesen Anweisungen finden Sie im Abschnitt Allgemeine Syntax einer erweiterten Regel.




Die folgende Abbildung zeigt den Ergebnissatz der Erstellung einer Tabellenpartition gestützt auf einen Standortbericht.

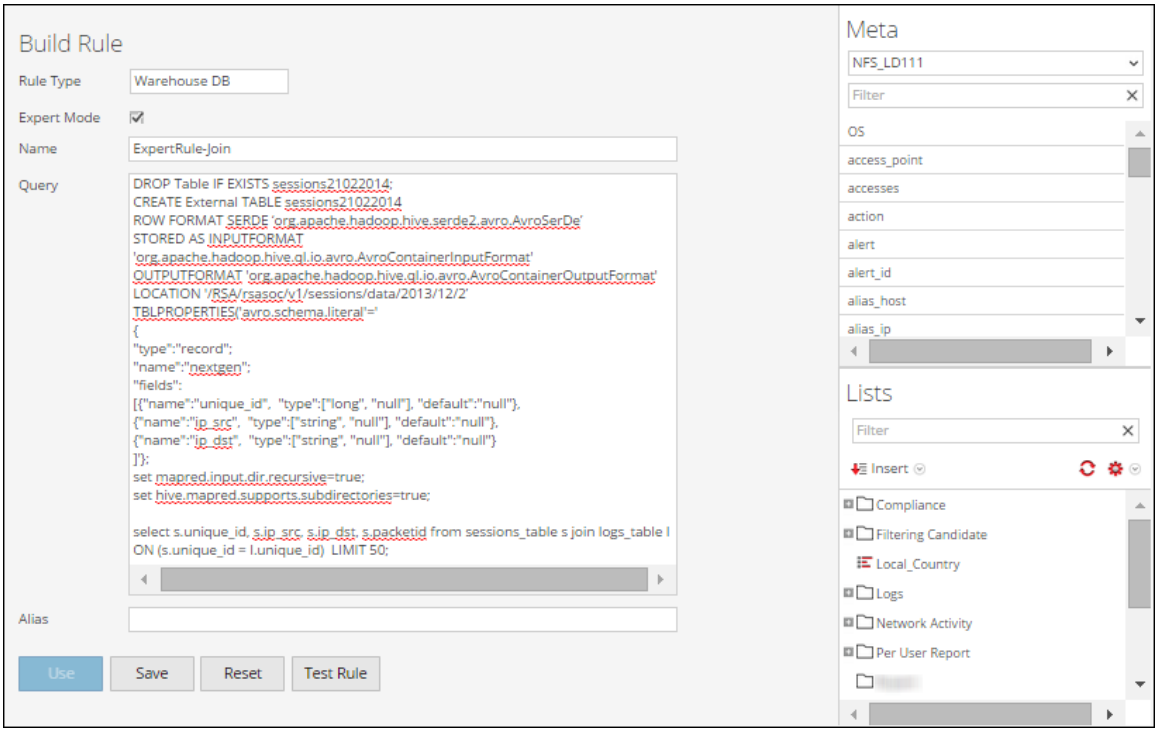


## Verbinden von Protokollen und Sitzungen auf Grundlage eines unique_id-Berichts

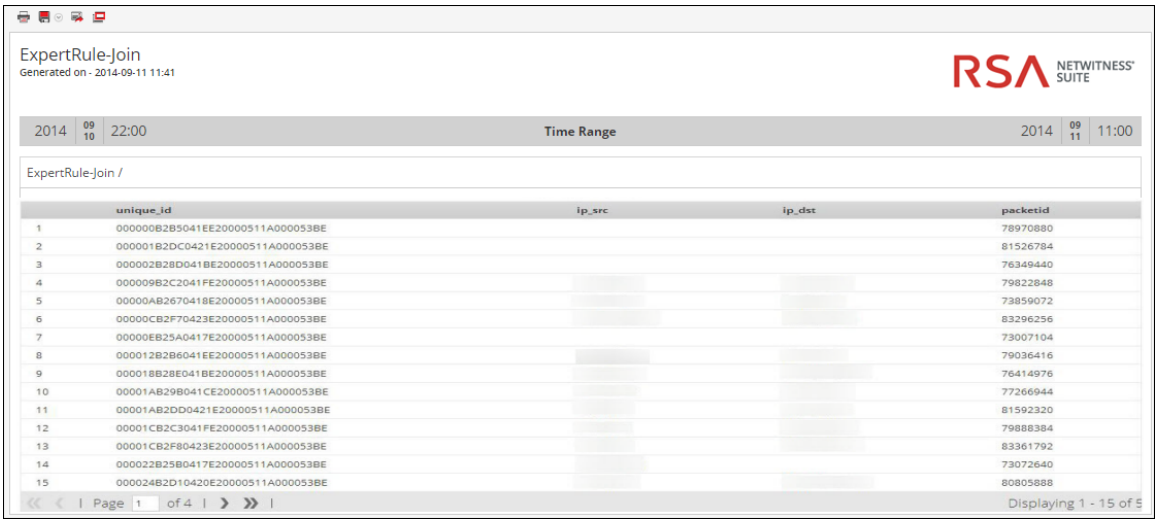
In dieser Beispielregel können Sie eine Regel zur Verbindung der Protokoll- und Sitzungstabelle erstellen, um die unique_id, die IP-Adresse der Quelle und des Ziels und das ID-Paket, basierend auf unique_id, abzurufen.

Im angeführten Beispiel kann eine HIVE-Abfrage ausgeführt werden, um bestimmte Felder sowohl aus der sessions_table als auch der logs_table abzurufen, indem eine Verbindung auf Basis des Feldes „unique_id“ ausgeführt wird.

Diese Regel bietet Informationen zur erstellten Tabelle, zur formatierten Zeile, zum Speicherort (Verzeichnispfad) für Avro-Datendateien in Warehouse und gibt einen Ergebnissatz anhand der HIVE-Abfrage zurück, um anzuzeigen, dass die Abfrage einen Ergebnissatz zurückgegeben hat. Weitere Informationen zu diesen Anweisungen finden Sie im Abschnitt **Allgemeine Syntax einer erweiterten Regel**.



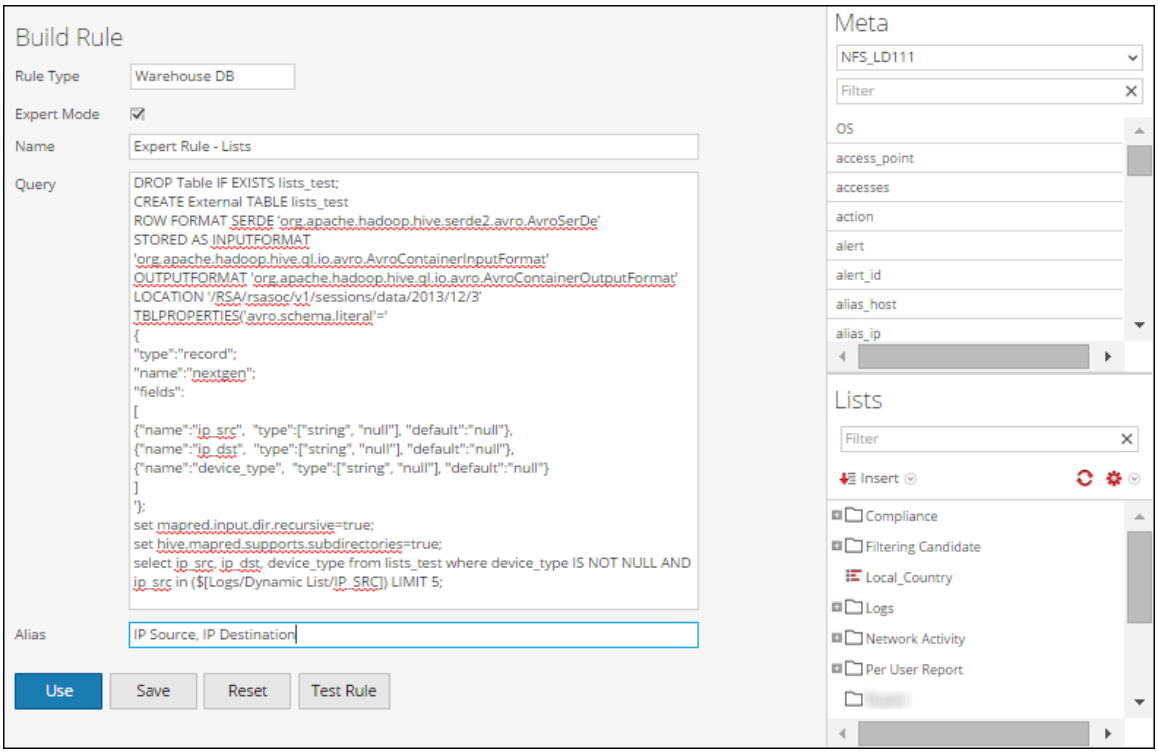

Die folgende Abbildung zeigt den Ergebnissatz der Verbindung der Protokoll- und Sitzungsstabelle auf Basis der unique_id.



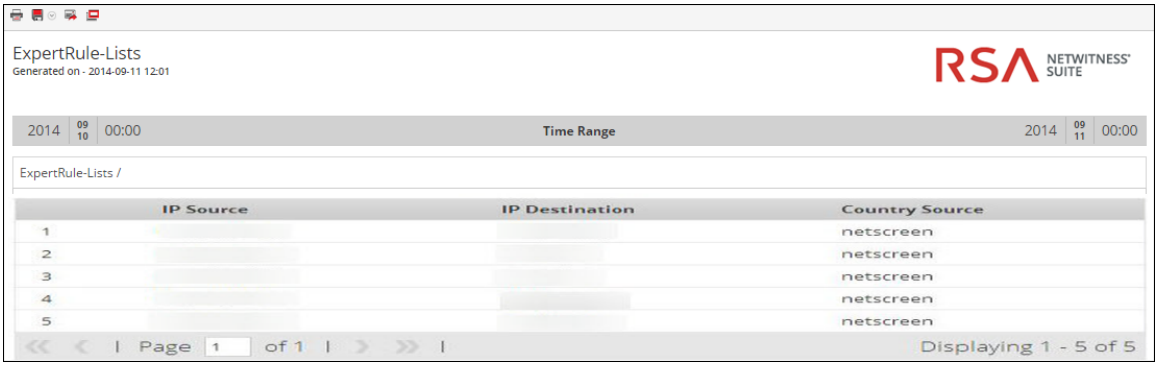

## Listenbericht

In diesem Beispiel können Sie eine Berichtliste erstellen, um die IP-Adresse der Quelle und des Ziels ebenso wie den Gerätetyp aus der Tabelle **lists_test**, in welcher der Gerätetyp nicht Null ist und die IP-Adresse von der richtigen Ereignisliste abgerufen wird.

Diese Regel bietet Informationen zur erstellten Tabelle, zur formatierten Zeile, zum Speicherort (Verzeichnispfad) für Avro-Datendateien in Warehouse und gibt einen Ergebnissatz anhand der HIVE-Abfrage zurück, um anzuzeigen, dass die Abfrage einen Ergebnissatz zurückgegeben hat. Weitere Informationen zu diesen Anweisungen finden Sie im Abschnitt **Allgemeine Syntax einer erweiterten Regel**.



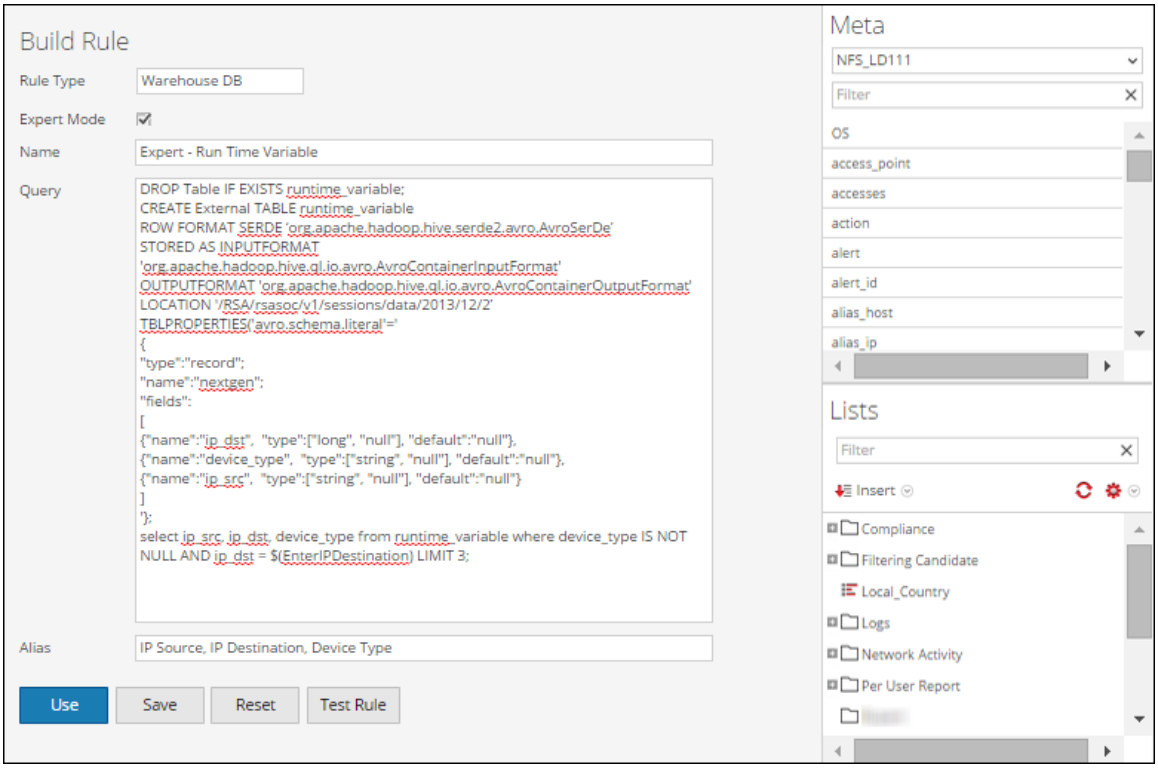
Folgende Abbildung zeigt den Ergebnissatz der Ausführung einer Berichtliste an.



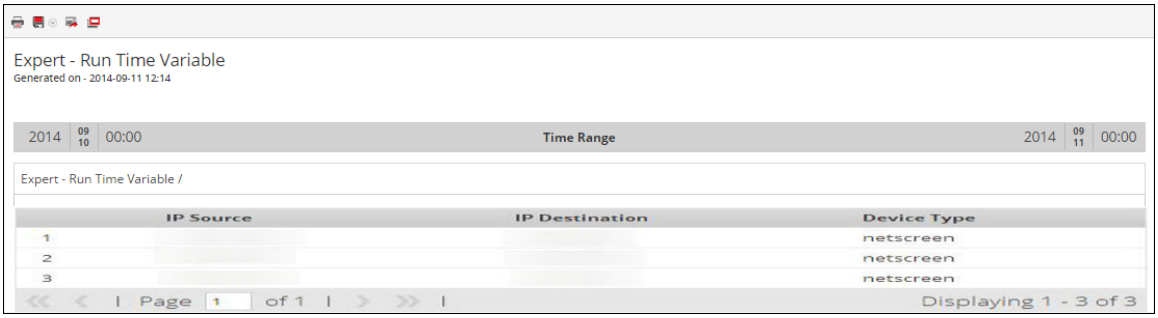

## Parametrisierter Bericht

In dieser Beispielregel können Sie eine Regel erstellen, um die IP-Adressen der Quelle und des Ziels ebenso wie den Gerätetyp aus der Tabelle **runtime_variable** auf Basis der angegebenen Laufzeitvariable `${EnterIPDestination}` abzurufen. Bei der Laufzeit werden Sie aufgefordert, einen Wert für die IP-Adresse des Ziels ip_dst einzugeben. Basierend auf dem eingegebenen Wert wird der Ergebnissatz angezeigt.

Diese Regel bietet Informationen zur erstellten Tabelle, zur formatierten Zeile, zum Speicherort (Verzeichnispfad) für Avro-Datendateien in Warehouse und gibt einen Ergebnissatz anhand der HIVE-Abfrage zurück, um anzuzeigen, dass die Abfrage einen Ergebnissatz zurückgegeben hat. Weitere Informationen zu diesen Anweisungen finden Sie im Abschnitt **Allgemeine Syntax einer erweiterten Regel**.



Die folgende Abbildung zeigt den Ergebnissatz der Ausführung eines parametrisierten Berichts.




## Partitionsbasierte Tabelle mit mehreren Speicherorten

Im Folgenden finden Sie ein Beispiel für eine partitionsbasierte Tabelle mit mehreren Speicherorten:

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;
 CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
 "name": "my_record", "type": "record",
 "fields": [
 {"name":"sessionid", "type":["null", "long"], "default" :
null},
 {"name":"time", "type":["null", "long"], "default" : null}
 ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1) LOCATION
```

```
'/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/12/';
 SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >=
${report_starttime} AND time
 <= ${report_endtime};
```

Die partitionsbasierte Tabelle mit mehreren Speicherorten wird im Folgenden erläutert:

1. Aktivieren Sie HIVE, um alle Unterverzeichnisse rekursiv zu scannen und alle Daten aus den Unterverzeichnissen abzurufen.

   ```
   set mapred.input.dir.recursive=true;
    set hive.mapred.supports.subdirectories=true;
   ```

2. Sie müssen eine externe Tabelle erstellen und anlegen und anschließend die Zeile formatieren:

   ```
    DROP TABLE IF EXISTS AVRO_COUNT;
    CREATE EXTERNAL TABLE AVRO_COUNT
    PARTITIONED BY (partition_id int)
    ROW FORMAT SERDE
   'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
    WITH SERDEPROPERTIES (
    'avro.schema.literal'='{
    "name": "my_record", "type": "record",
    "fields": [
    {"name":"sessionid", "type":["null", "long"], "default" :
   null},
    {"name":"time", "type":["null", "long"], "default" : null}
    ]}'
    )
    STORED AS
    INPUTFORMAT
    'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
    OUTPUTFORMAT
   ```

```
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputForma
t';
```

**Hinweis:** Sie müssen nur dann eine externe Tabelle erstellen, wenn Sie eine andere Tabelle benutzen. Wenn Sie zum Beispiel eine andere Tabelle außer **AVRO_COUNT** verwenden, müssen Sie die Tabelle ablegen und eine externe Tabelle erstellen.

**Hinweis:** Wichtige Punkte, die Sie beim Erstellen einer Tabelle beachten müssen:
- Wenn Sie eine „nicht externe“ Tabelle ablegen, werden die Daten gelöscht.
- Die Tabelle wird auf einer einzigen Spalte mit dem Namen „partition_id“ partitioniert. Dies ist die Standardspalte für Reporting Engine.
- Der Standardwert einer beliebigen Spalte ist Null, da die AVRO-Datei die angegebene Spalte nicht enthalten darf.
- Die Spaltennamen müssen in Kleinschreibung angegeben sein, da in HIVE nicht zwischen Groß- und Kleinschreibung unterschieden wird, in AVRO jedoch wird unterschieden.
- Sie müssen **avro.schema.literal** in *SERDEPROPERTIES* angeben.

Weitere Informationen zur Regelsyntax finden unter *Apache HIVE*.

3. Partitionen hinzufügen:
   Nachdem Sie eine Tabelle definiert haben, müssen Sie die HDFS-Speicherorte angeben, von denen die Daten abgefragt werden müssen, bevor Sie die HIVE-Anweisungen ausführen. Der Speicherortparameter gibt die Daten an, die je nach dem angegebenen Datum abgerufen werden sollen. Die Daten sind auf mehrere Speicherorte oder Verzeichnisse in HDFS verteilt. Für jeden Speicherort müssen Sie eine Partition mit zugewiesenen eindeutigen Werten in der Partitionsspalte hinzufügen. Die Speicherorte können jedes Verzeichnis in HDFS sein

```
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/12/';
```

**Hinweis:** HIVE liest alle Dateien an diesen Speicherorten als AVRO. Falls an einem dieser Speicherorte eine Nicht-AVRO-Datei vorliegt, kann die Abfrage fehlschlagen.

4. Abfrage ausführen

```
SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >=
${report_starttime} AND time
 <= ${report_endtime};
```

Wenn eine Tabelle erstellt wird, können Sie bestimmte Abfragen ausführen, um die Daten zu filtern. Beispiel: Nach der Erstellung der Tabelle können Sie die Daten wie in den folgenden Beispielen gezeigt filtern:

**Sitzungen mit einer bestimmten Quell-IP-Adresse:**

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime}
AND time <= ${report_endtime}  AND ip_src = '127.0.0.1';
```

**Gruppieren nach Benutzerziel:**

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime}
AND time <= ${report_endtime}  GROUP BY usr_dst;
```

## Automatisierte Partition mit benutzerdefinierter Funktion

In 10.5.1 können Sie im Expertenmodus die benutzerdefinierte Funktion zur Automatisierung des Hinzufügens von Partitionierungen in einer vom Benutzer definierten Tabelle verwenden.

## Allgemeine Syntax

```
RE WH CUSTOM ADDPARTITIONS(table, namespace, rollup, [starttime,
endtime])
```

Die folgende Tabelle beschreibt die Syntax der benutzerdefinierten Funktion:

| S.No | Name | Beschreibung |
|---|---|---|
| 1 | Tabelle | Der Tabellenname, für den die Partitionierung hinzugefügt werden muss. |
| 2 | namespace | Der Namespace kann Sitzungen oder Protokolle umfassen. |
| 3 | rollup | Dieser Wert bestimmt die Ebene des Verzeichnispfads, der in Partitionierungen einbezogen werden soll. Der Wert kann „STUNDE“, „TAG“ oder „MINUTE“ sein. Wenn Warehouse Connector für den Rollup „TAG“ konfiguriert ist, ergibt das Festlegen dieses Wertes auf „STUNDE“ KEINE Ergebnisse. Die Anzahl und der Speicherort jeder Partitionierung basiert auf dem Zeitbereich für das Ausführen der Regel und dem Rollup-Wert. |

| S.No | Name | Beschreibung |
|---|---|---|
| 4 | (Optional) starttime, endtime | Um Partitionen für einen bestimmten Zeitbereich zu erzeugen, der nicht dem in der Regel genannten entspricht, müssen Sie „starttime“ und „endtime“ in **Epochensekunden** angeben.<br><br>**Hinweis:** Ausdrücke werden für „starttime“ und „endtime“ nicht unterstützt. |

Die benutzerdefinierte Funktion wird aufgerufen, wenn Reporting Engine die Regel entweder während eines Regeltests oder eines geplanten Berichts ausführt. Während der Ausführung einer Expertenregel extrahiert Reporting Engine jedes Mal, wenn die Funktionsdeklaration erkannt wird, die erforderlichen
Argumente, fügt *n* Anweisungen vom Typ „ADD PARTITION HiveQL“ hinzu und führt sie auf dem Hive-Server aus.

Der Speicherort und die Verzeichnisstruktur werden durch das in der Regel übergebene Argument und die Hive-Datenquellenkonfiguration
in Reporting Engine bestimmt. Die Anzahl der Partitionen ist abhängig vom angegebenen Rollup und dem bei der Ausführung der Regel verwendeten Zeitraum. Beispiel: Der Rollup „STUNDE“ und der Zeitbereich als „LETZTE 2 Tage“ führen zu 48 Partitionierungen für 48 Stunden während
Reporting Engine mit dem Rollup „TAG“ 2 Partitionierungen erstellt, eine für jeden Tag.

Die Partitionierungsabfrage wird durch die im Attribut AlterTableTemplate der Hive-Konfiguration der Reporting Engine festgelegte Syntax-Vorlage erzeugt.

**Hinweis:** Standardmäßig beginnt diese Funktion das Hinzufügen von Partitionierungen in einer Tabelle mit den Partitions-IDs von 0 bis N-1. Daher muss die Tabelle nach einer nach einer einzelnen Ganzzahl benannten Partitionierungs-ID partitioniert werden.

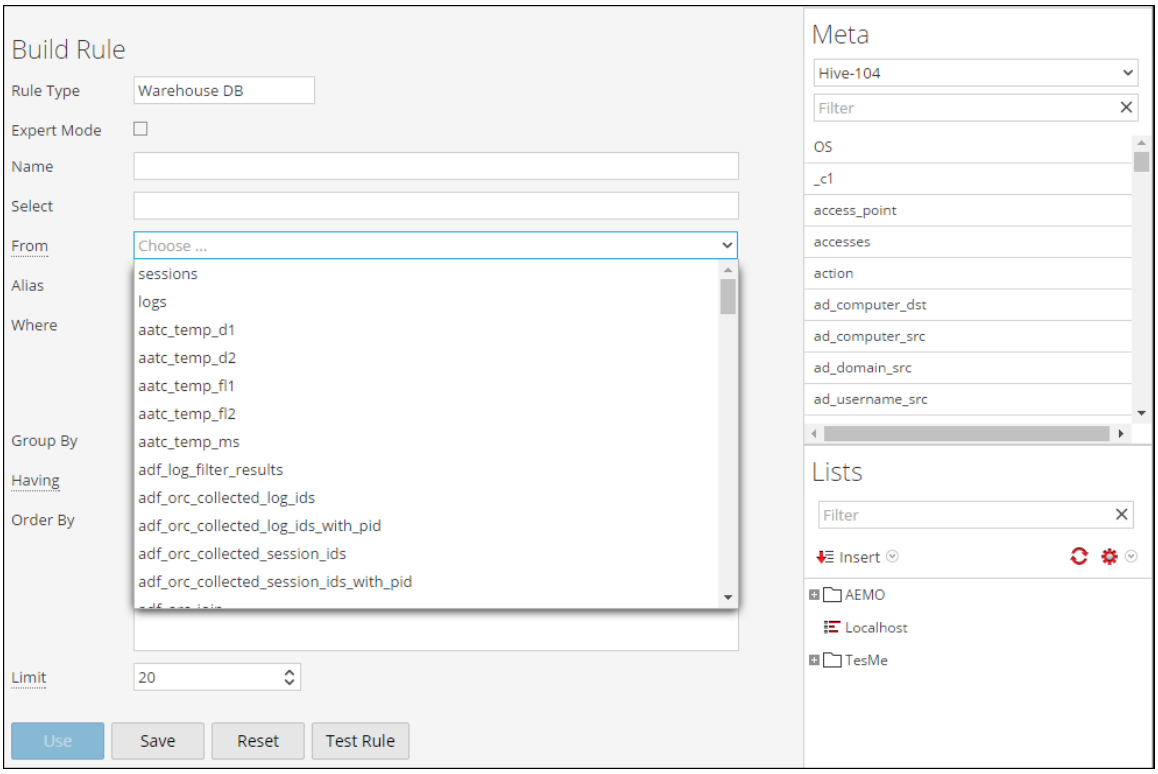
Im Folgenden ist ein Beispiel für eine automatisierte Partitionierung mithilfe der benutzerdefinierten Funktion dargestellt:

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;
```

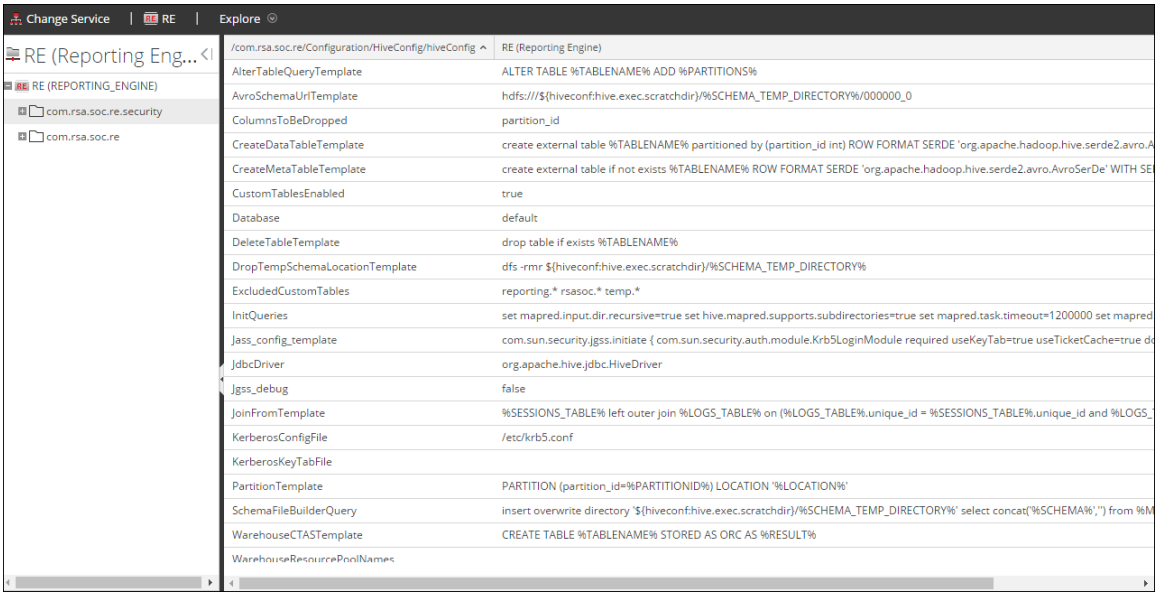
```
CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
  "name": "my_record", "type": "record",
  "fields": [
  {"name":"sessionid", "type":["null", "long"], "default" :
null}
  ,{"name":"time", "type":[ "null" , "long"], "default" : null}
  ,{"name":"unique_id", "type":["null", "string"], "default" :
null}
  ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';
RE_WH_CUSTOM_ADDPARTITIONS(AVRO_COUNT, 'sessions', 'DAY');
 SELECT COUNT(*) as TotalSessions FROM AVRO_COUNT
 WHERE time >= ${report_starttime} AND time <= ${report_
endtime};
```

## Erstellen eines benutzerdefinierten Tabellenberichts

In 10.6.1 können Sie benutzerdefinierte Tabellen auf dem Hive-Server verwenden und erstellen. Reporting Engine unterstützt die Ausführung von Abfragen für benutzerdefinierte Tabellen und die Möglichkeit, aus einer einzigen Regelausgabe eine neue Tabelle zu erstellen. Wenn diese Funktion in der Benutzeroberfläche der Warehouse-Regelerstellung aktiviert ist, wird Benutzern eine Liste mit benutzerdefinierten Tabellen angezeigt, die im Hive-Server verfügbar sind.




Legen Sie zur Aktivierung dieser Funktion **CustomTablesEnabled** auf **TRUE** fest, indem Sie zu **Reporting Engine -> Durchsuchen ->Hive-Konfiguration** navigieren.



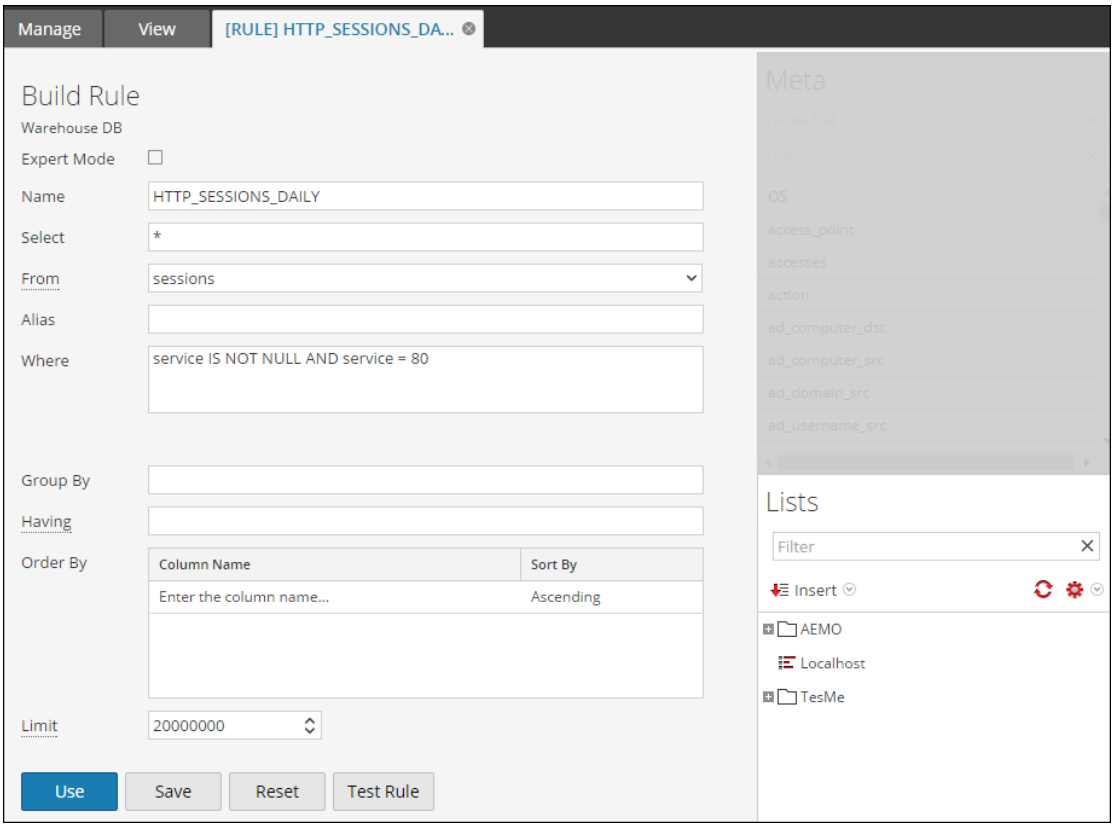

## Erstellen einer benutzerdefinierten Tabelle aus regulären Regeln

Um einen Bericht planen, der eine einzelne SAW-Regel enthält, wird eine neue Texteingabe mit einem **Warehouse CTAS Name** hinzugefügt. Der Benutzer kann jetzt einen Namen für die benutzerdefinierte Tabelle angeben, die aus der Ausgabe der Regel im Bericht erstellt wird.

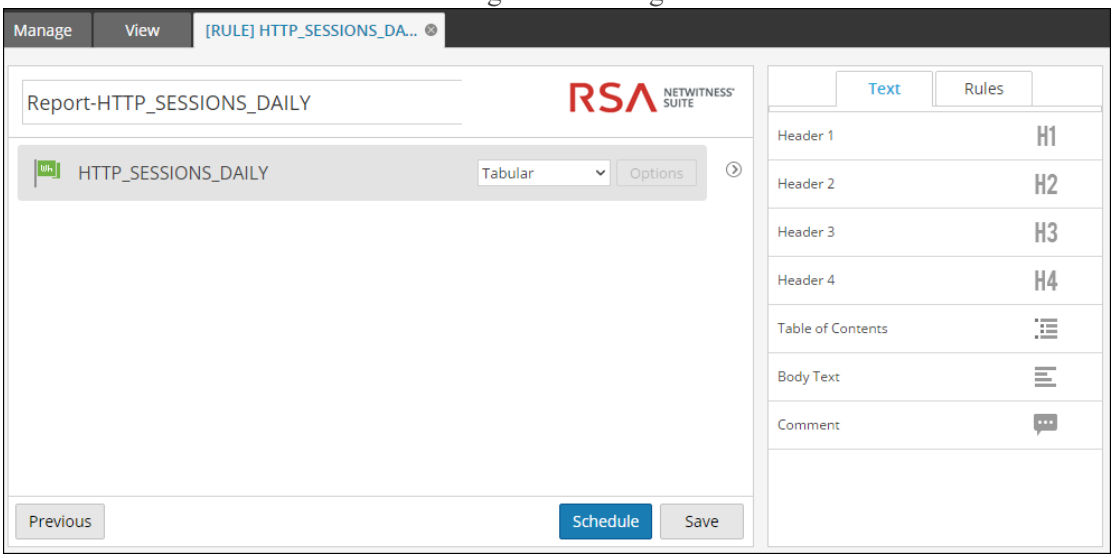
**Hinweis:** Diese Funktion ist nur verfügbar, wenn der Bericht eine einzelne SAW-Regel auf der Seite „Planung“ enthält. Ansonsten ist diese Option ausgeblendet.

Der Prozess zur Verwendung der Funktion wird unten erklärt:

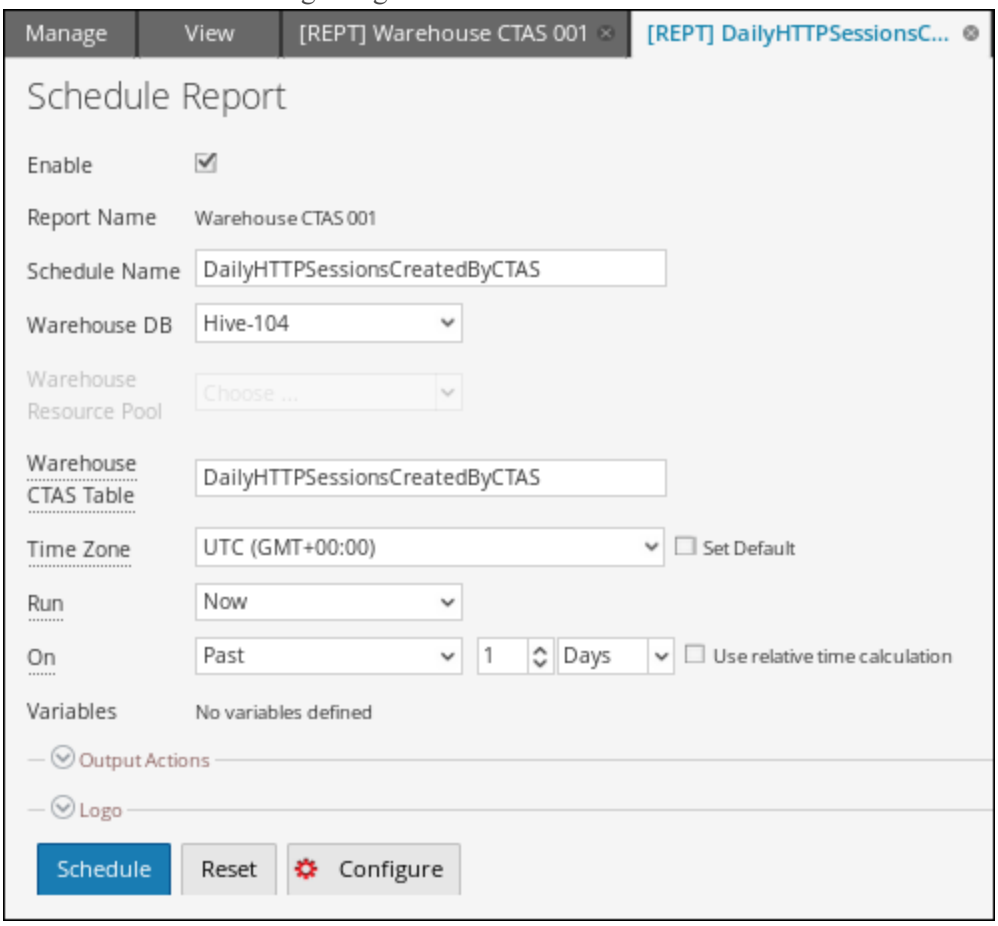
1. Erstellen Sie eine Regel zum Filtern mit Daten in SAW.



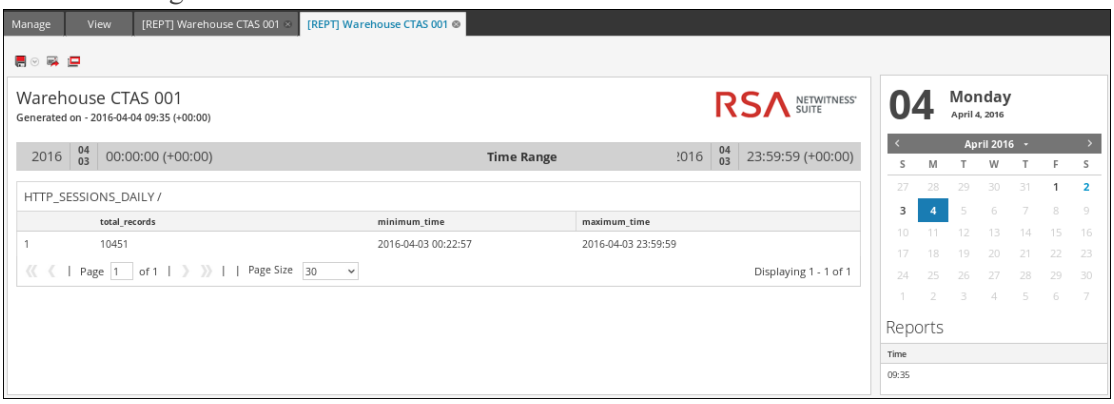

2. Erstellen Sie einen Bericht mit der oben genannten Regel.



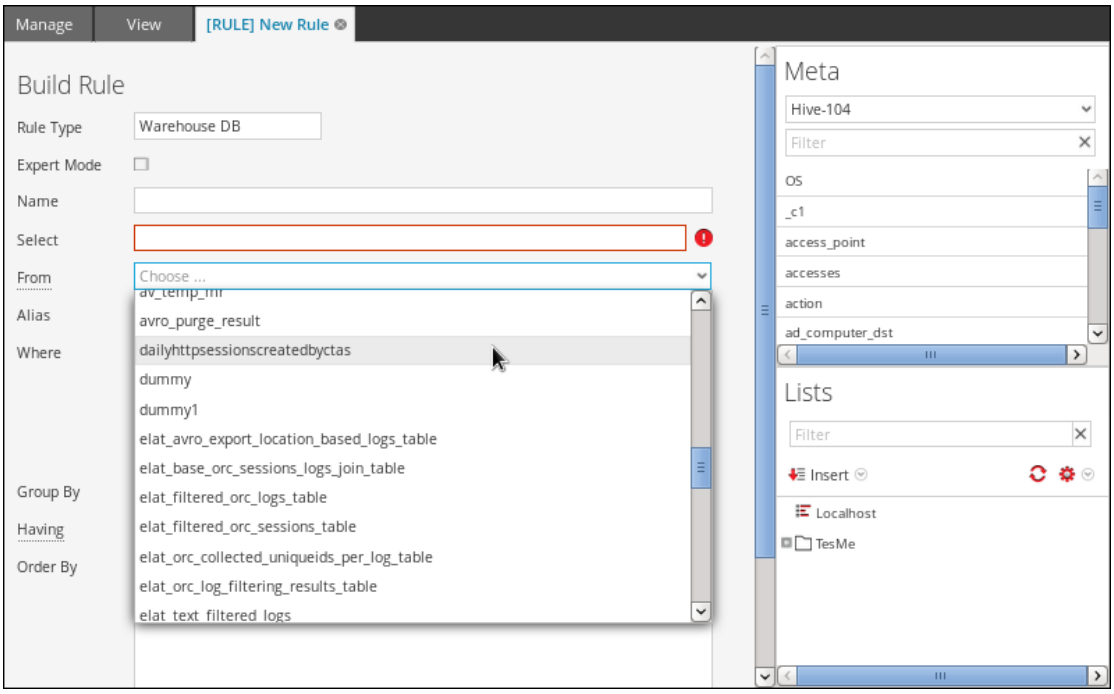
3. Erstellen Sie eine Planung und geben Sie den CTAS-Tabellennamen ein.




4. Führen Sie den Bericht aus und Reporting Engine erstellt die nachstehende Ergebnisübersicht für die Planung.




5. Im nächsten Schema aktualisieren Sie Reporting Engine oder starten Reporting Engine neu, die CTAS-Tabelle wird aufgeführt.


Manage
View
[RULE] New Rule
Build Rule
Rule Type
Warehouse DB
Expert Mode
Name
Select
From
Choose ...
Alias
Where
Group By
Having
Order By
avro_purge_result
dailyhttpsessionscreatedbyctas
dummy
dummy1
elat_avro_export_location_based_logs_table
elat_base_orc_sessions_logs_join_table
elat_filtered_orc_logs_table
elat_filtered_orc_sessions_table
elat_orc_collected_uniqueids_per_log_table
elat_orc_log_filtering_results_table
elat_text_filtered_logs
Meta
Hive-104
Filter
OS
_c1
access_point
accesses
action
ad_computer_dst
Lists
Filter
Insert
Localhost
TesMe

## Aufgabenplaner für Warehouse Reporting

Ein Aufgabenplaner in einem Hadoop-Cluster plant die aus Aufgaben bestehenden Jobs und weist jedem Job, der in einem Cluster ausgeführt wird, spezifische Ressourcen zu. Standardmäßig weist der Aufgabenplaner allen Jobs gleich viele Ressourcen zu. Wenn z. B. 10 Jobs ausgeführt werden, so werden die Ressourcen des Clusters gleichmäßig aufgeteilt. Sie können den Aufgabenplaner jedoch so konfigurieren, dass er einen Job schneller als die anderen ausführen lässt, indem diesem Job mehr Ressourcen (Pools oder Warteschlangen) zugewiesen werden. Dadurch können Sie einige Berichte bevorzugt vor allen anderen ausführen lassen.

# Funktionen

NetWitness Suite unterstützt zwei Aufgabenplaner:

- Fair-Planer (`org.apache.hadoop.mapred.FairScheduler`)
- Kapazitätsplaner (`org.apache.hadoop.mapred.CapacityTaskScheduler`)

# Fair-Planer

Dieser Planer teilt die Gesamtkapazität des Clusters in logische Pools auf. Sie können einen Job an einen beliebigen dieser Pools senden. Alle an einen Pool gesendeten Jobs teilen sich nur die Ressourcen, die dem Pool zugewiesen sind. Wenn ein Pool Ressourcen frei hat, werden die freien Ressourcen anderen Pools zur Verfügung gestellt, in denen Jobs ausgeführt werden. Beispiel: Ein Fair Scheduler hat 100 % Ressourcen in zwei Pools namens Pool A und Pool B zur Verfügung, wobei auf Pool A 40 % und auf Pool B 60 % der Ressourcen entfallen. Wenn in Pool A vier Jobs ausgeführt werden, so werden dort jedem Job 10 % der Ressourcen zugewiesen. Wenn die vier Jobs abgeschlossen sind, werden die freien Ressourcen Pool B zugewiesen.

**Hinweis:** Sie können einen Pool so konfigurieren, dass er mehrere Jobs parallel ausführt.

# Kapazitätsplaner

Dieser Planer teilt die Gesamtkapazität des Clusters in Warteschlangen auf. Jeder Warteschlange wird ein vorkonfigurierter Anteil der Gesamtkapazität zugewiesen. Ein Job kann an eine beliebige dieser Warteschlangen gesendet werden. Wenn mehrere Jobs an dieselbe Warteschlange gesendet werden, so werden die Jobs nacheinander ausgeführt. Beispiel: Ein Capacity Scheduler hat 100 % Ressourcen in drei Warteschlangen namens „Standard“, „Niedrig“ und „Hoch“ zur Verfügung, auf die jeweils 20 %, 30 % bzw. 50 % der Ressourcen entfallen. Wenn auf „Standard“ zwei Jobs namens S1 und S2 ausgeführt werden, auf „Niedrig“ drei Jobs namens N1, N2 und N3 und auf „Hoch“ vier Jobs namens H1, H2, H3 und H4, werden diese Jobs nacheinander in ihren jeweiligen Warteschlangen ausgeführt. Wenn die Jobs in einer Warteschlange abgeschlossen sind, werden die freien Ressourcen nicht an die anderen Warteschlangen verteilt.

## Abfrageaggregate

In diesem Abschnitt werden die unterstützten Aggregatfunktionen erläutert.

# Unterstützte Aggregatfunktionen

In der folgenden Tabelle sind die unterstützten Aggregatfunktionen aufgelistet.

| Aggregatfunktion | Beschreibung | Eingabedatentypen | Ausgabedatentypen |
|---|---|---|---|
| count | Gibt die Anzahl der Metawerte zurück, dazu gehören auch doppelte Werte. | Numerisch | Numerisch |
| countdistinct | Gibt die Gesamtanzahl unterschiedlicher oder einzigartiger Werte zurück. | Numerisch | Numerisch |
| distinct | Gibt alle einzigartigen Werte zurück. | Alle | Alle |
| first | Gibt das erste Auftreten des Metawerts zurück. | Alle | Gleich wie Eingabe |
| last | Gibt das letzte Auftreten des Metawerts zurück. | Alle | Gleich wie Eingabe |

| Aggregatfunktion | Beschreibung | Eingabedatentypen | Ausgabedatentypen |
|---|---|---|---|
| sum | Gibt eine Summe aller Werte ungleich Null des Metaschlüssels in einer Gruppe zurück. | Numerisch | Numerisch |
| avg (Durchschnitt) | Gibt den Durchschnittswert aller Werte ungleich Null des Metaschlüssels innerhalb einer Gruppe zurück. | Numerisch | Numerisch |
| min (Minimum) | Gibt den Mindestwert für alle Werte des Metaschlüssels in jeder Gruppe zurück. Dieser Wert basiert auf dem Feld Sortieren nach. | Alle | Alle |

| Aggregatfunktion | Beschreibung | Eingabedatentypen | Ausgabedatentypen |
|---|---|---|---|
| max (Maximum) | Gibt den Höchstwert für alle Werte des Metaschlüssels in jeder Gruppe zurück. Der Höchstwert ist der Wert, der basierend auf dem Feld Sortieren nach zurückgegeben wird. | Alle | Alle |
| length | Gibt die Länge der Werte des Metaschlüssels zurück. Dies wird in SQL „skalare Funktion“ genannt. | Alle | Numerisch |

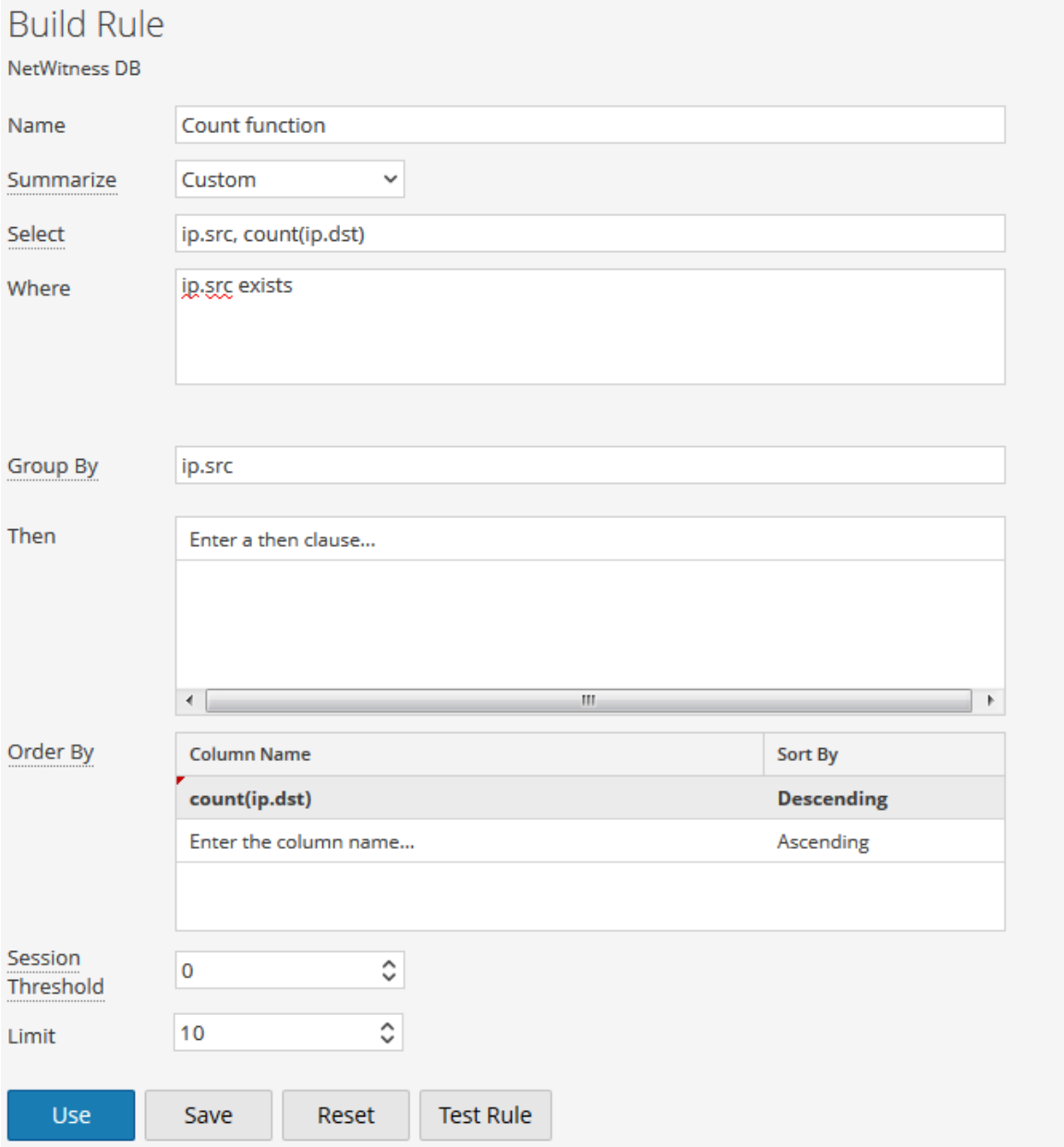
## Beispiele für Abfragen und Ergebnisse pro Funktion

### Count

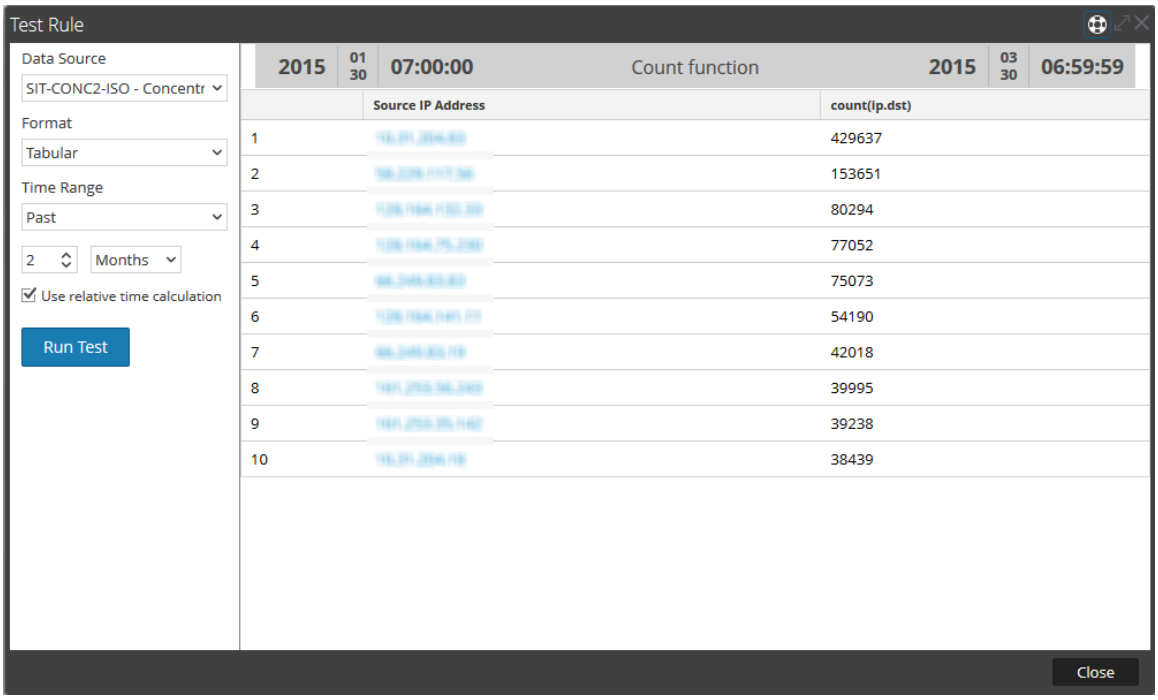
Diese Funktion gibt die Anzahl der Werte für einen bestimmten Metaschlüssel zurück, wobei Nullwerte ausgeschlossen, Duplikatwerte aber eingeschlossen sind.

**Beispiel**

Die folgende Abbildung zeigt eine Musterabfrage für die Funktion „count“, die für die Ziel-IP und die entsprechende Quell-IP verwendet wird.




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.




Hier gibt die Seite für jede eindeutige ip.src (Quell-IP) die Gesamtanzahl der ip.dst (Ziel-IP)-Werte zurück, wobei auch die Duplikatwerte mit eingeschlossen sind.

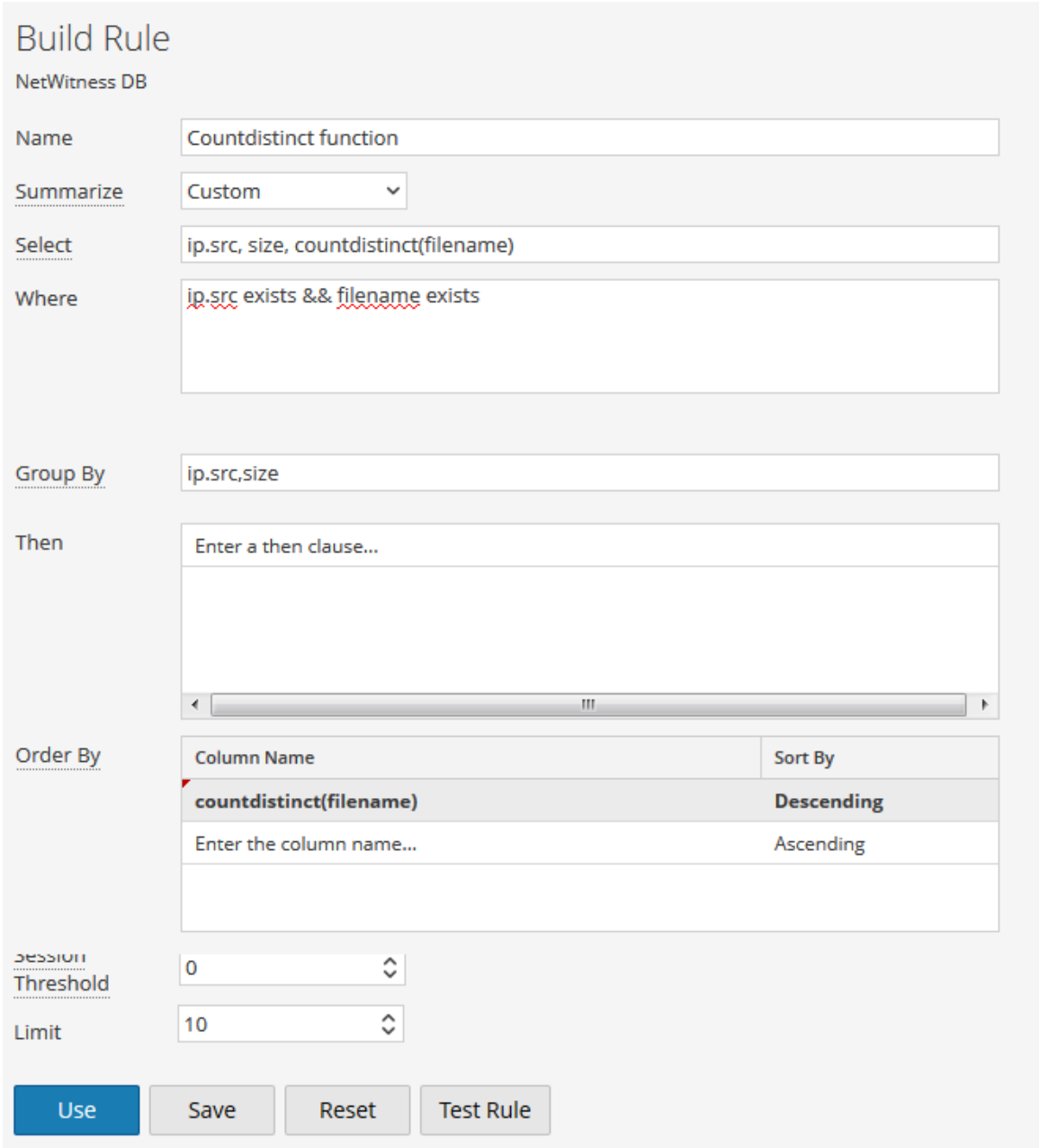
**Hinweis:** Wenn Sie RSA NetWitness Suite aktuell in der Version 10.5 oder neuer verwenden und eines Ihrer NetWitness Suite Core-Geräte noch in der Version 10.3 oder 10.4 vorliegt, können einige der Aggregatfunktionen eventuell unerwartete Fehler anzeigen. Allerdings werden Aggregatfunktionen wie sum() und count() in Version 10.4 unterstützt.

## Countdistinct

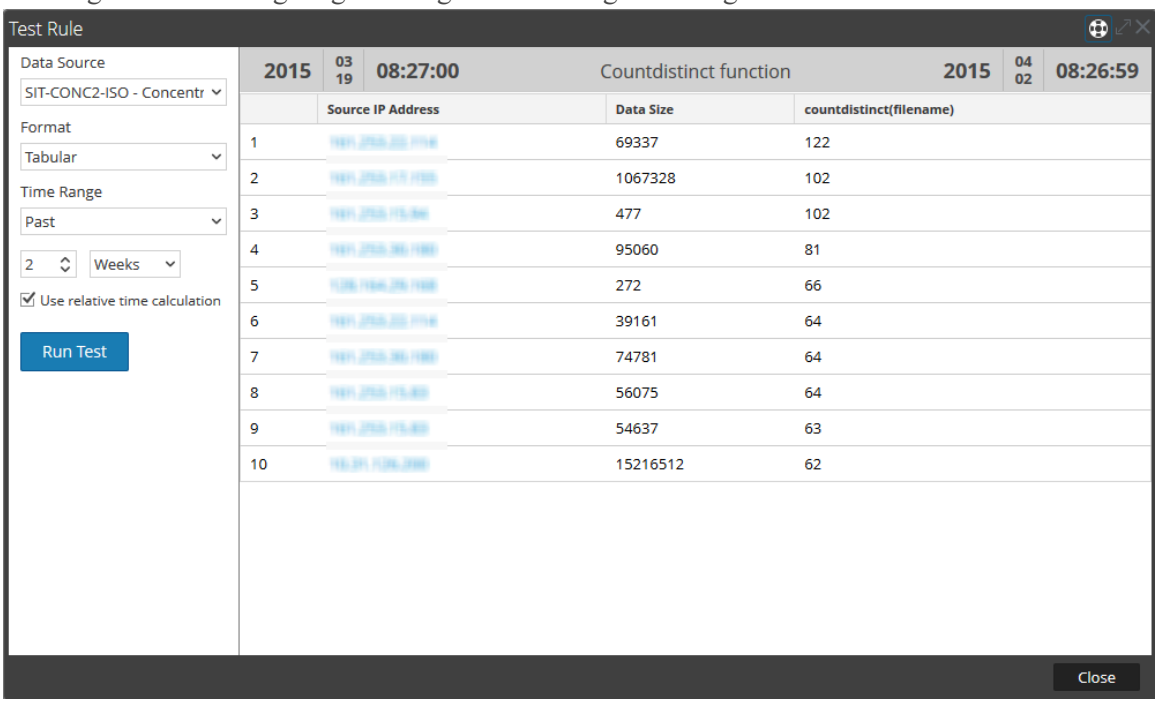
Die Funktion countdistinct gibt die Anzahl eindeutiger oder unterschiedlicher Werte für den Metaschlüssel zurück. Mit anderen Worten, mithilfe der Funktion countdistinct kann eine Anzahl unterschiedlicher Werte für den angegebenen Metaschlüssel abgerufen werden.

Die folgende Abbildung zeigt eine Musterabfrage, in der die Funktion countdistinct zusammen mit IP-Quelle (ip.src) und Datengröße (size) verwendet wird.

**Beispiel**


Build Rule
NetWitness DB
Name
Countdistinct function
Summarize
Custom
Select
ip.src, size, countdistinct(filename)
Where
ip.src exists && filename exists
Group By
ip.src,size
Then
Enter a then clause...
Order By
Column Name
Sort By
countdistinct(filename)
Descending
Enter the column name...
Ascending
Threshold
0
Limit
10
Use
Save
Reset
Test Rule

Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.



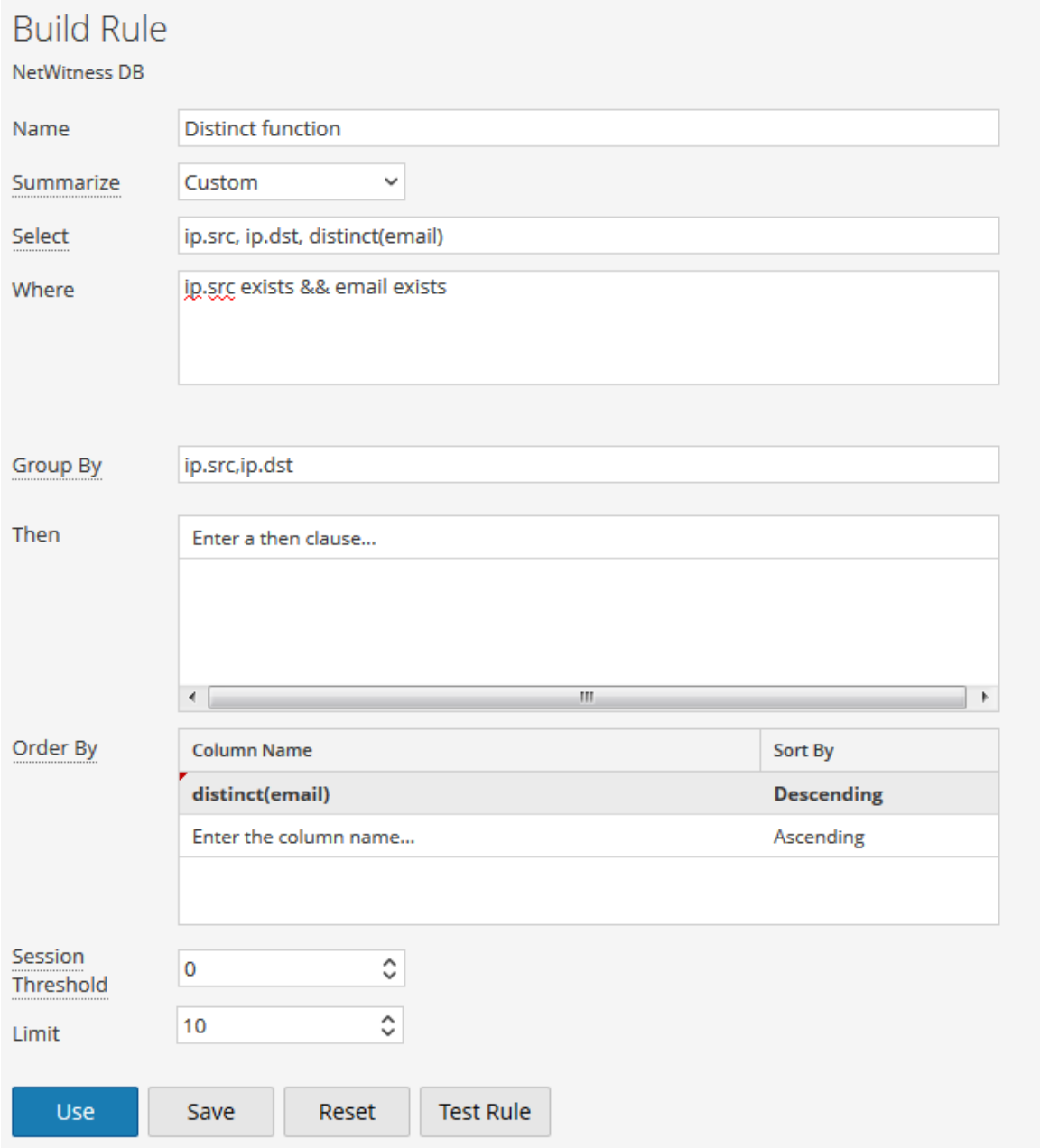

Hier zeigt die Seite die Datengröße zusammen mit der Gesamtanzahl unterschiedlicher Dateinamen von der entsprechenden IP-Quelle an. Anders als die Funktion count schließt countdistinct die Duplikatwerte aus dem Ergebnis aus.

## Distinct

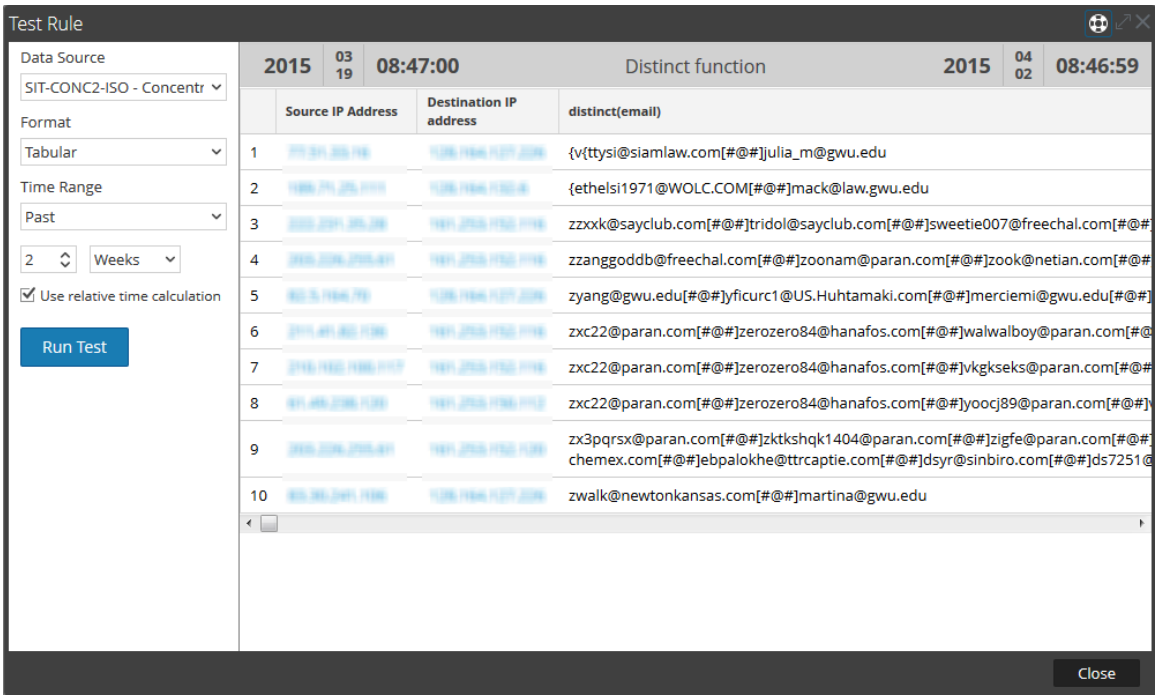
Diese Funktion gibt alle eindeutigen oder unterschiedlichen Werte des Metaschlüssels zurück.

**Beispiel**

Die folgende Abbildung zeigt eine Musterabfrage für die Funktion distinct zum Abrufen von E-Mails zwischen verschiedenen Quell- und Ziel-IPs (ip.dst).




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.



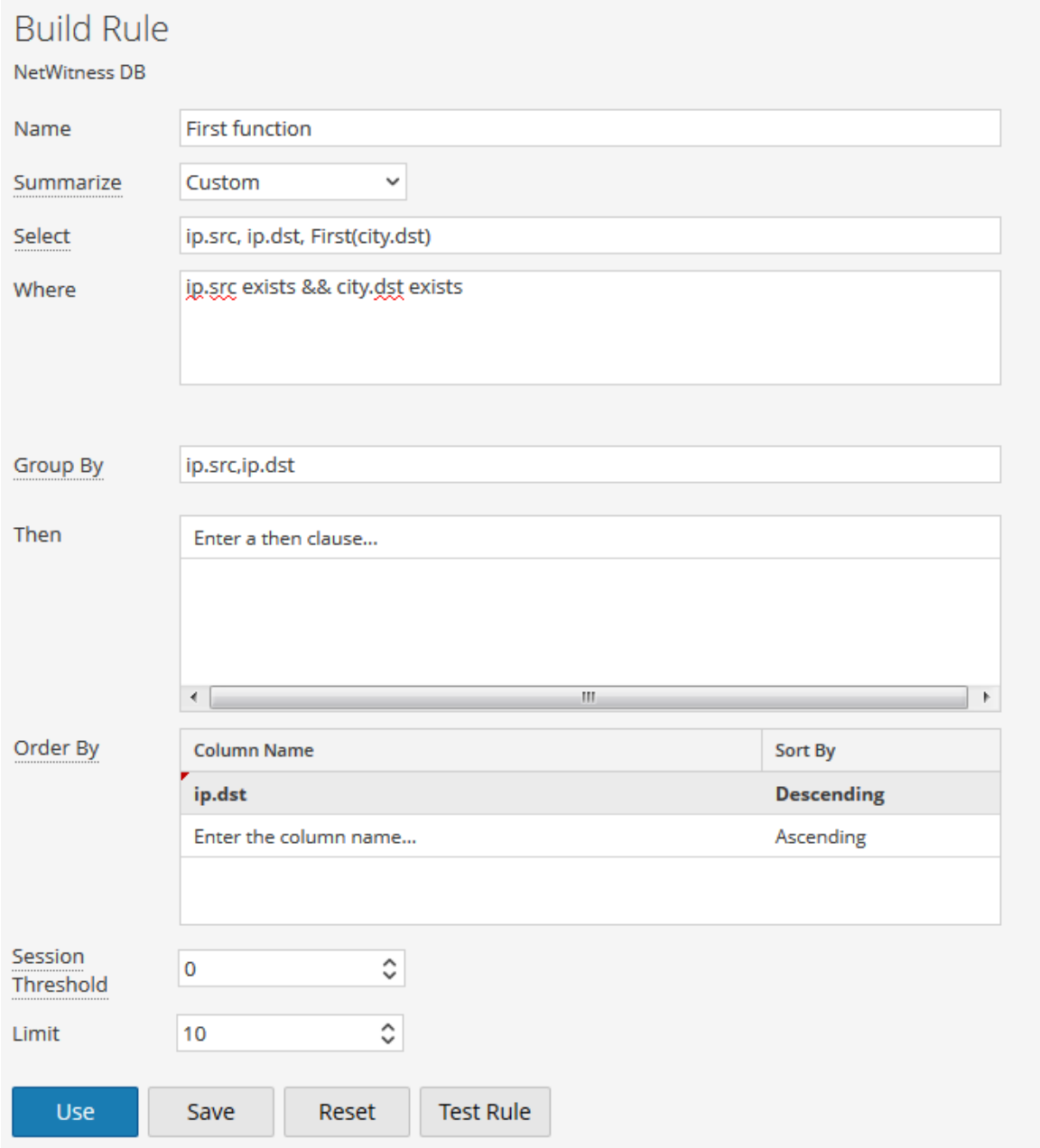

Hier zeigt die Seite die Liste eindeutiger E-Mails an, die zwischen den entsprechenden Quell- und Ziel-IPs ausgetauscht wurden.

## First

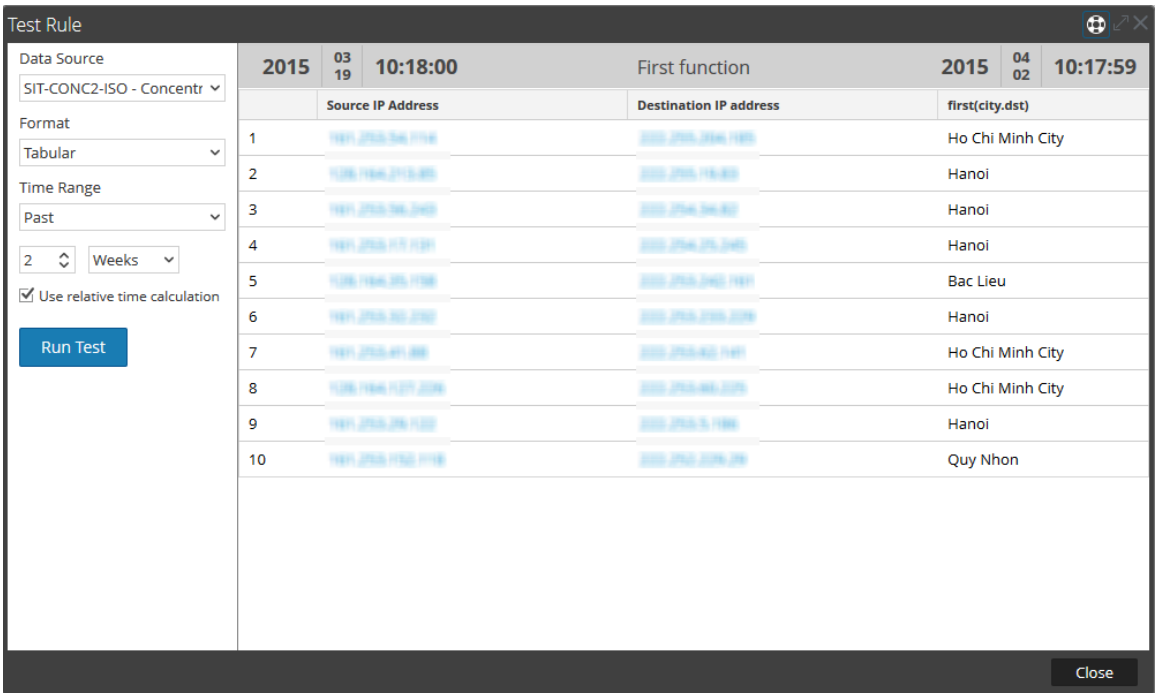
Diese Funktion wird verwendet, um den ersten Wert aus einer sortierten Folge von Werten für einen angegebenen Metaschlüssel abzurufen.

**Beispiel**

Die folgende Abbildung zeigt eine Musterabfrage für die Funktion first, die verwendet wird, um den Namen der ersten Zielstadt abzurufen.




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.



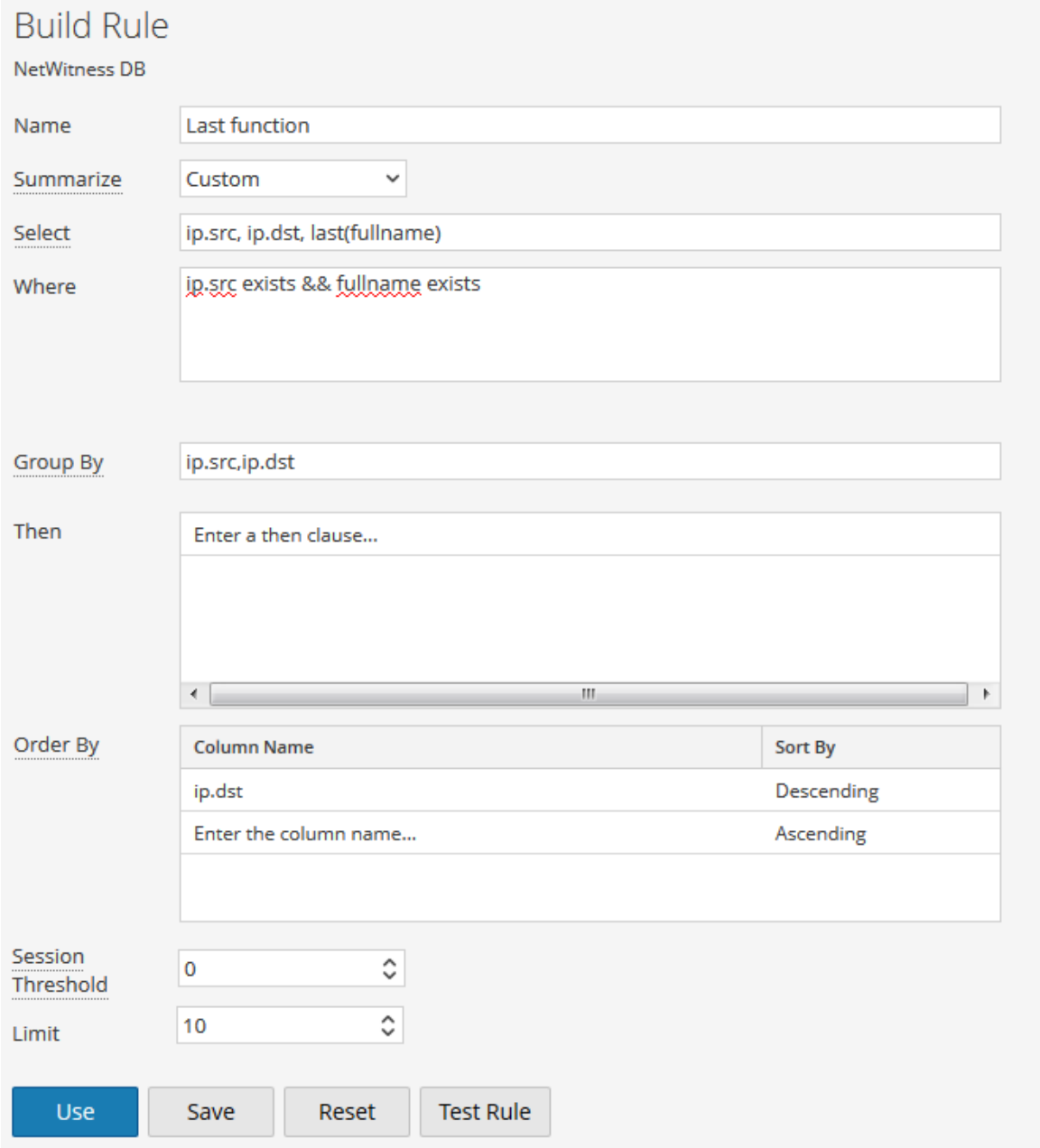

Hier zeigt die Seite die erste Zielstadt für die entsprechende Quell- und Ziel-IP an. Sie können die first-Funktion verwenden, um einen bestimmten Wert aus einem Suchergebnis zu isolieren.

## Letzter

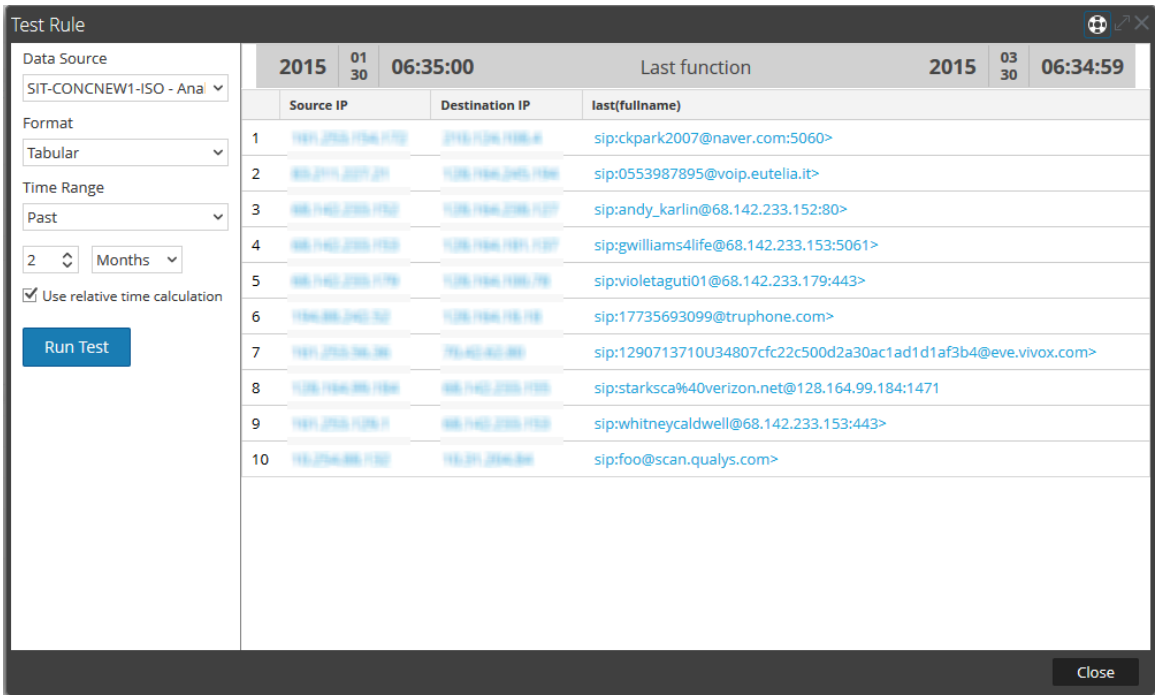
Diese Funktion wird verwendet, um den letzten Wert aus einer sortierten Folge von Werten für einen angegebenen Metaschlüssel abzurufen.

**Beispiel**

Die folgende Abbildung zeigt eine Musterabfrage für die Funktion last, die verwendet wird, um den Namen des neuesten Benutzers abzurufen.




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.



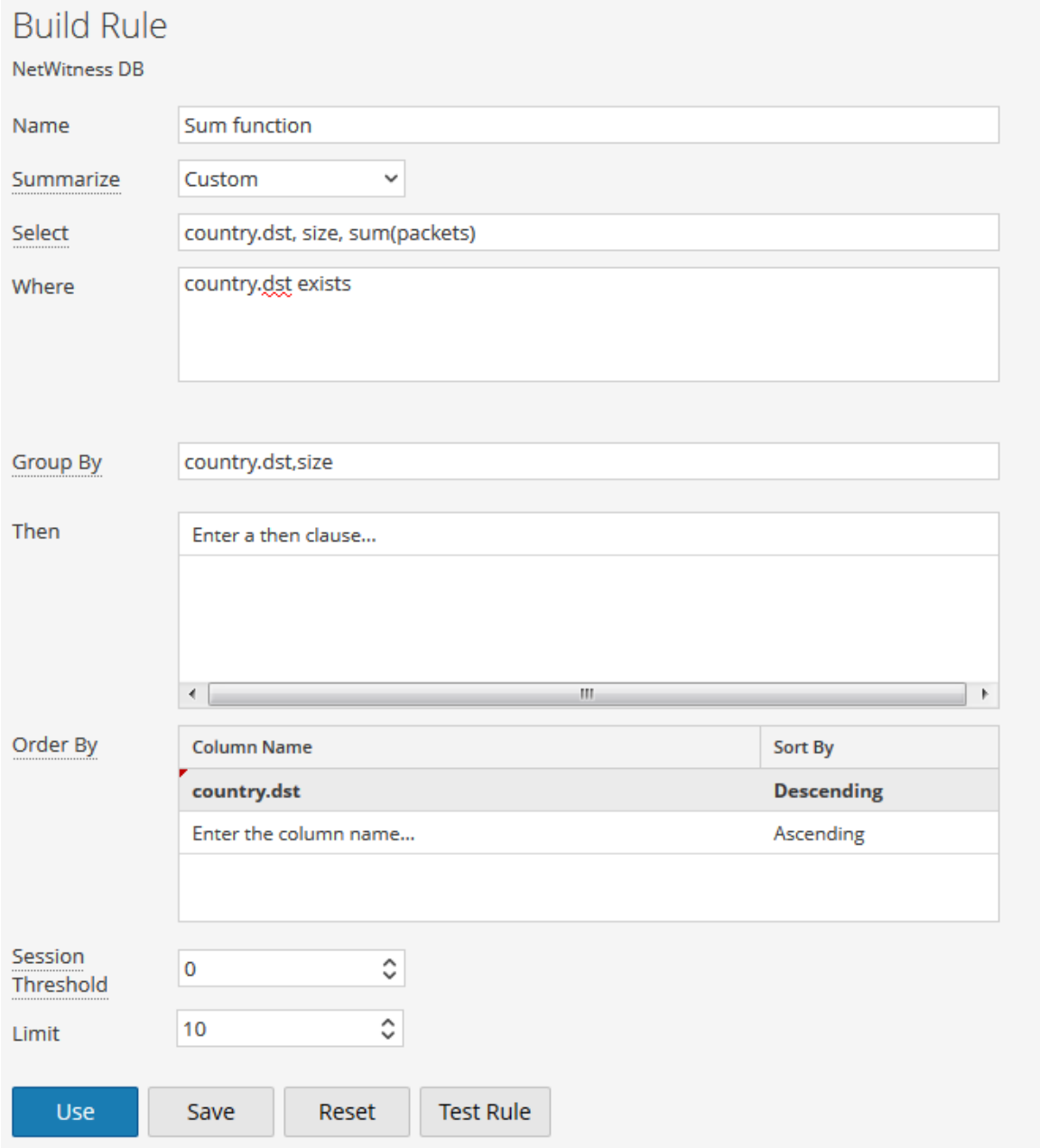

Hier zeigt die Seite die Liste der neuesten oder letzten Benutzernamen vollständig an, die zwischen Quell- und Ziel-IP ausgetauscht wurden.

## Summe

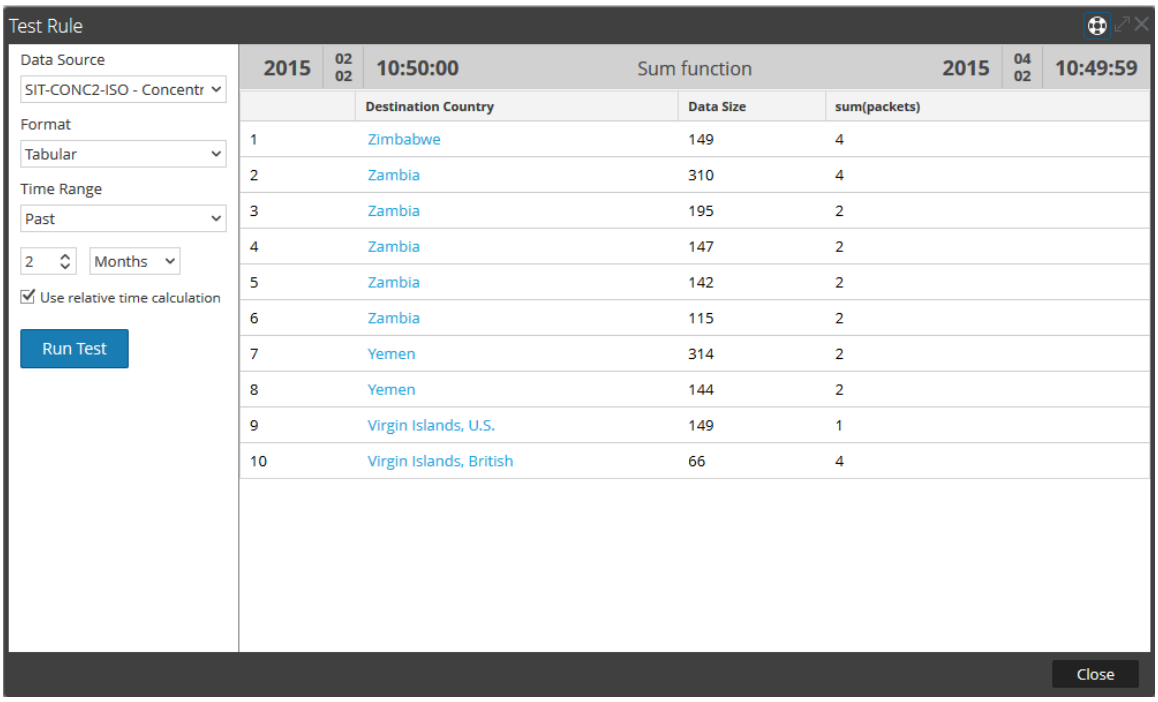
Diese Funktion gibt die Gesamtzahl der Werte ungleich Null des Metaschlüssels innerhalb einer Gruppe zurück.

**Beispiel**

Die folgende Abbildung zeigt die Abfrage für die Funktion Sum, die für Pakete verwendet wird.




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.



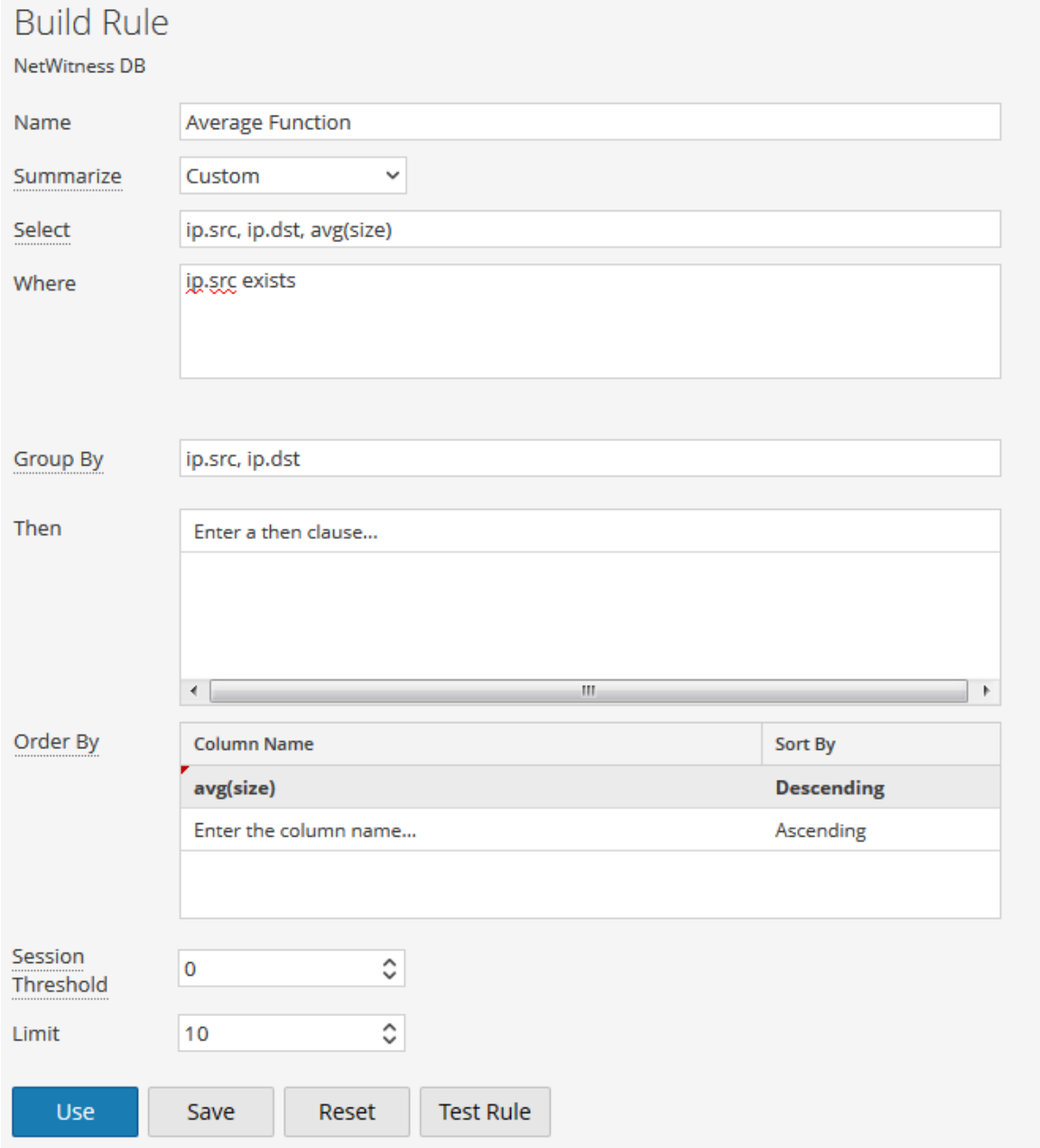

Hier zeigt die Seite die Gesamtanzahl oder Summe der Pakete zusammen mit der Größe der Daten für das entsprechende Zielland an.

## Avg

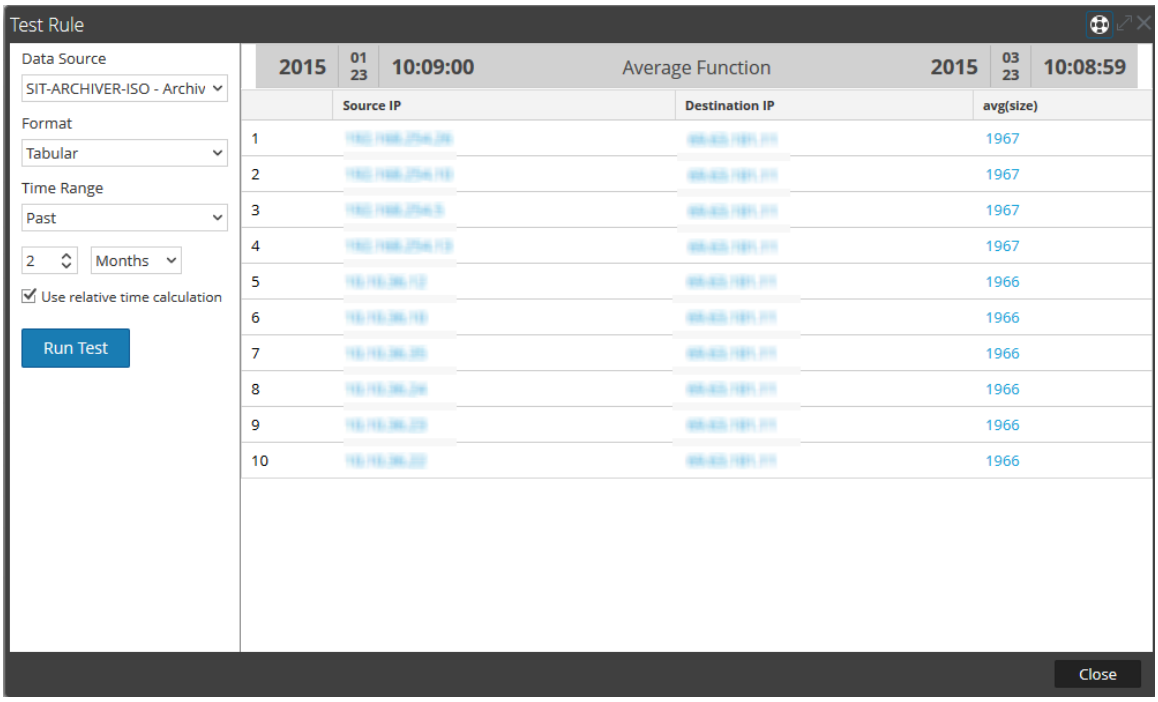
Die average-Funktion gibt die durchschnittliche Anzahl der Werte ungleich Null des Metaschlüssels innerhalb einer Gruppe zurück.

**Beispiel**

Die folgende Abbildung zeigt eine Musterabfrage für die durchschnittliche Datengröße an, die zwischen einer Quell- und einer Ziel-IP übertragen wurde.




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.



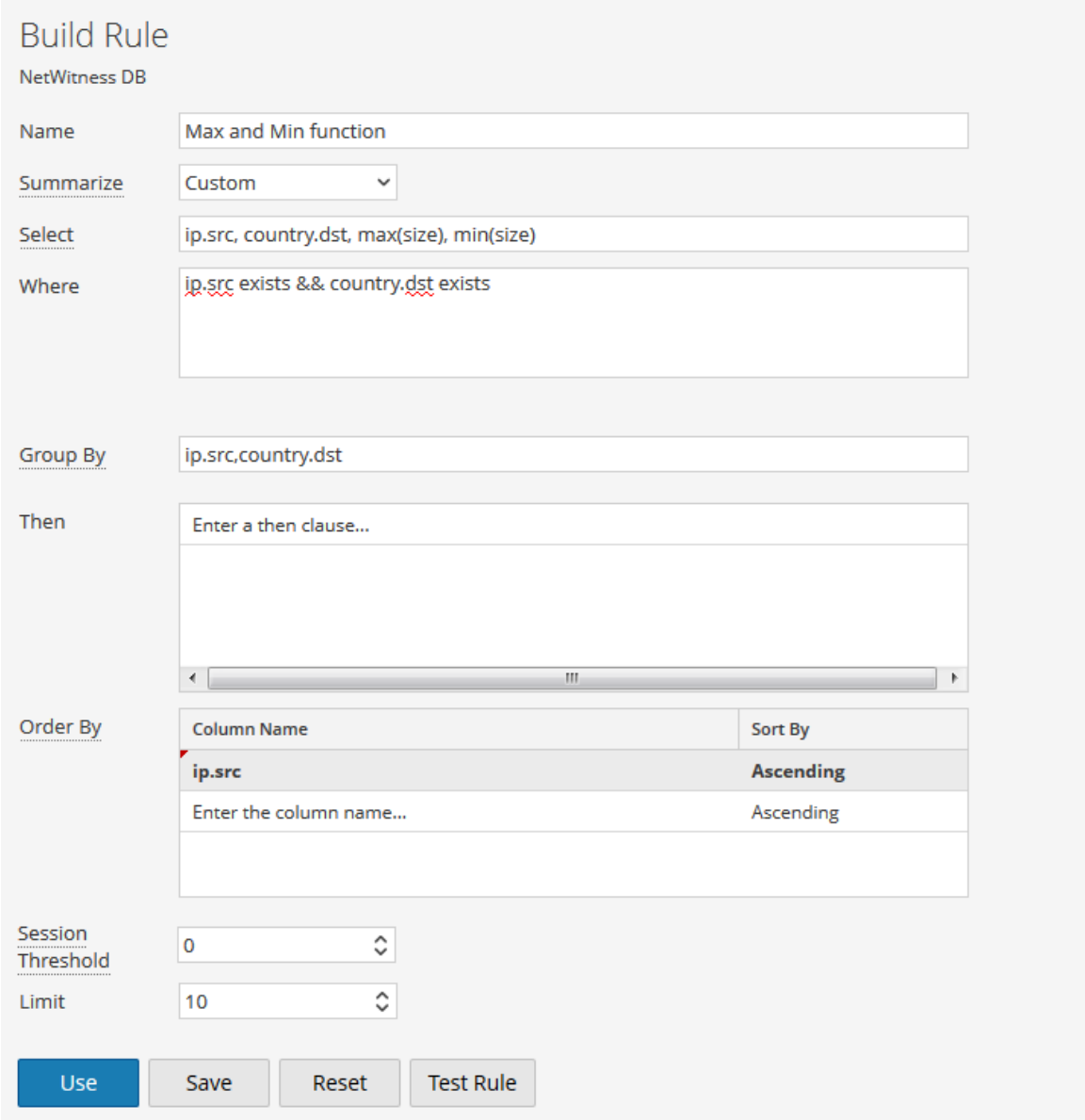

Hier zeigt die Seite die durchschnittliche Größe der zwischen Quell- und Ziel-IP ausgetauschten Daten an:

## Max und Min

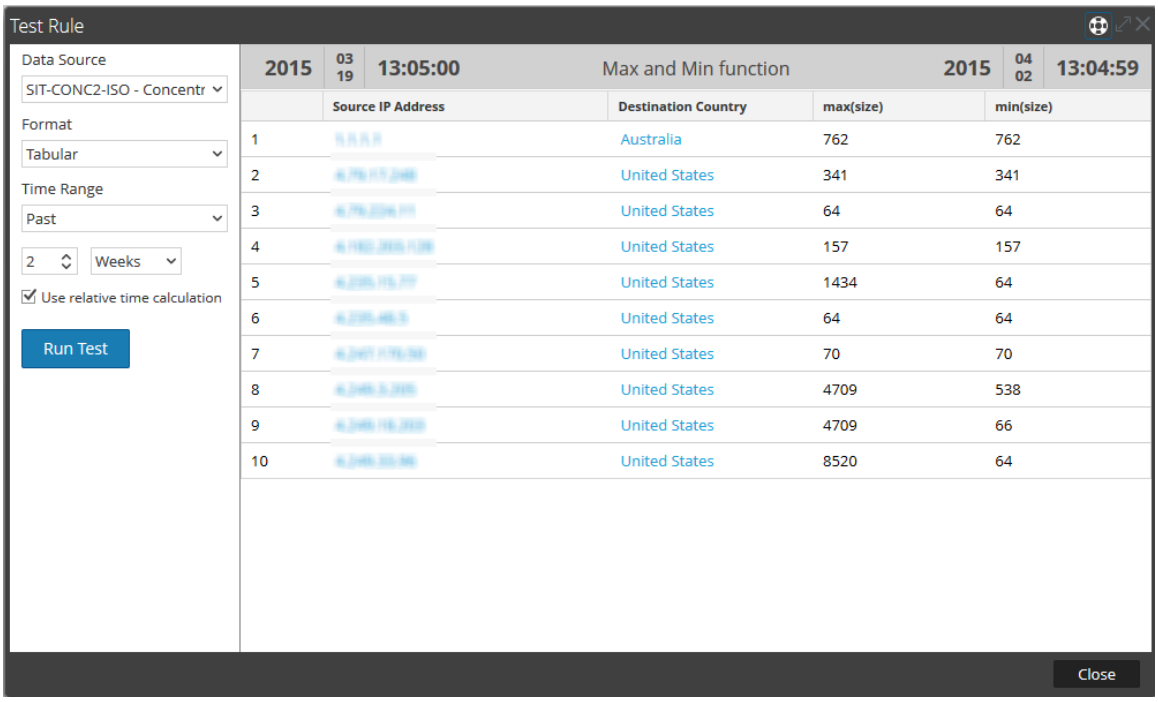
Die Funktionen Max und Min geben das Maximum bzw. das Minimum für gegebene Werte eines Metaschlüssels zurück.

Die folgende Abbildung zeigt eine Musterabfrage für die Funktionen max und min für verschiedene Datengrößen, für Quell-IP und Zielland.

**Beispiel**




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.



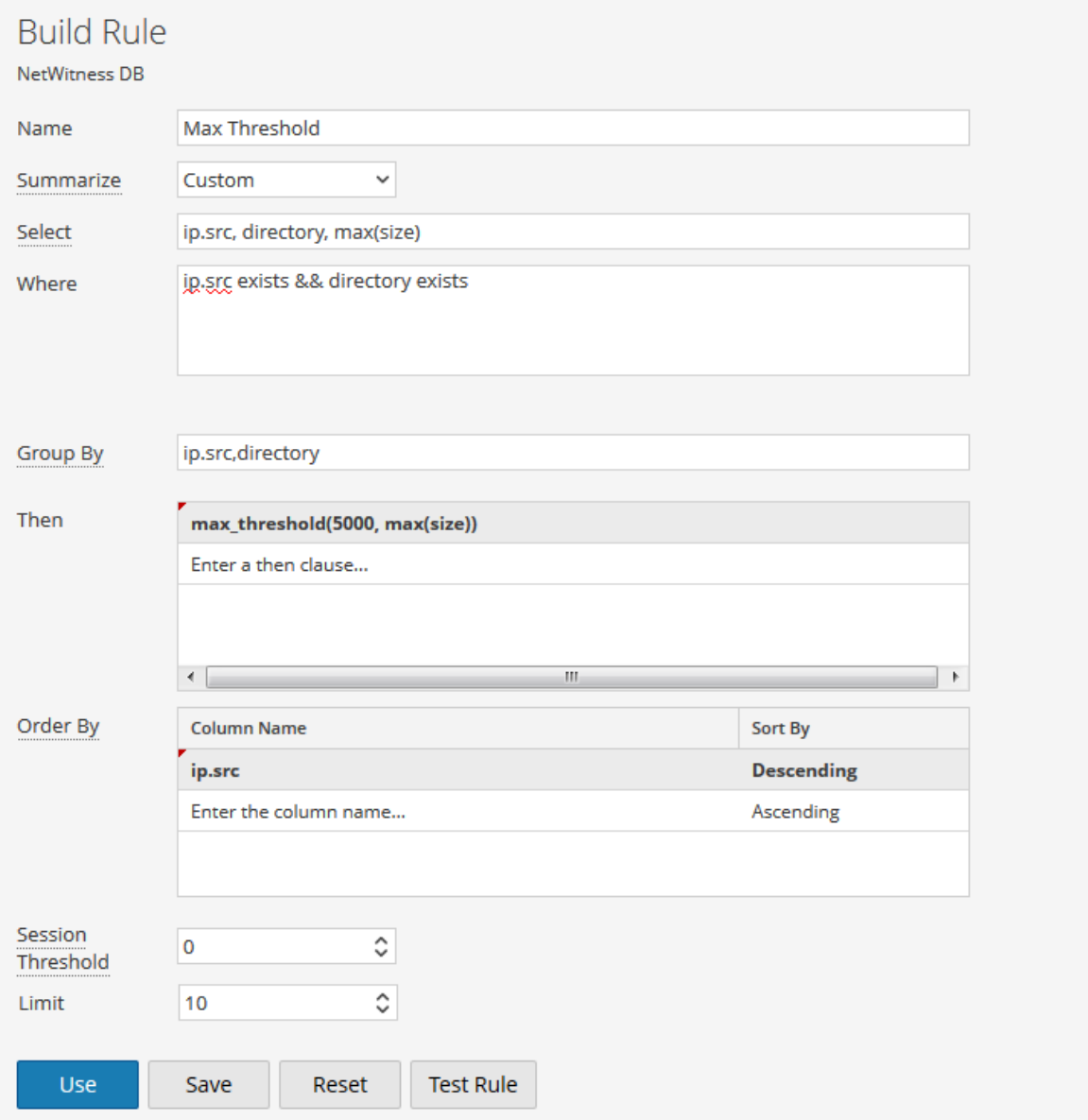

Hier zeigt die Seite die Spalten max(size) und min(size) an, zusammen mit der Liste von Quell-IP und Zielland. Die Spalte max(size) listet die maximalen ausgetauschten Datengrößen und die Spalte min(size) die minimalen ausgetauschten Datengrößen auflistet.

## Filtern aggregierter Metaergebnisse mit „max_threshold“

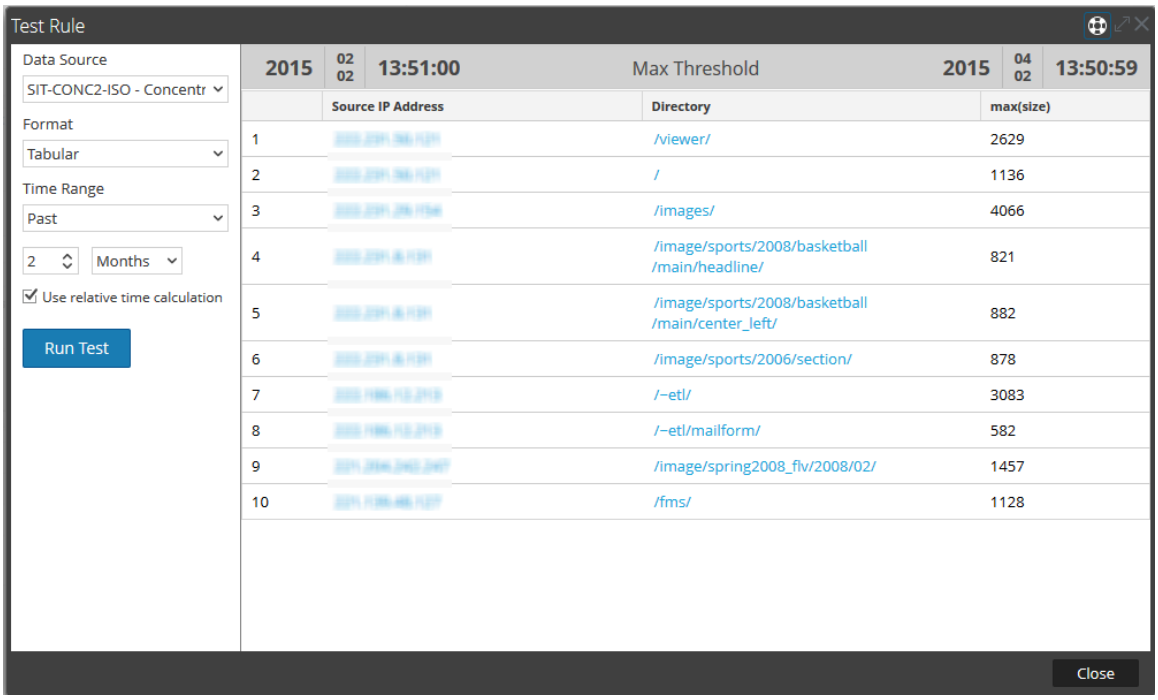
Sie können die Ergebnisse jeder Funktion mithilfe der Schwellenwertregelaktion weiter filtern.

**Beispiel**
Es folgt eine Musterabfrage für „max_threshold“ zusammen mit der Max-Funktion im Feld **Dann**:
**max_threshold(5000,max(size))**

Die folgende Abbildung zeigt den Bildschirm „Regel erstellen“ für die obige Abfrage.




Hier wird der Schwellenwert max_threshold für Datengrößen mit einem oberen Grenzwert von 5000 angewandt. Die folgende Abbildung zeigt das Ergebnis.




Hier zeigt die Ergebnisseite die Spalte max(size) an, in der die Datengrößen kleiner als 5000 angezeigt werden, da dies der obere Grenzwert in der Abfrage ist, zusammen mit der entsprechenden IP-Quelle und dem entsprechenden Verzeichnis.

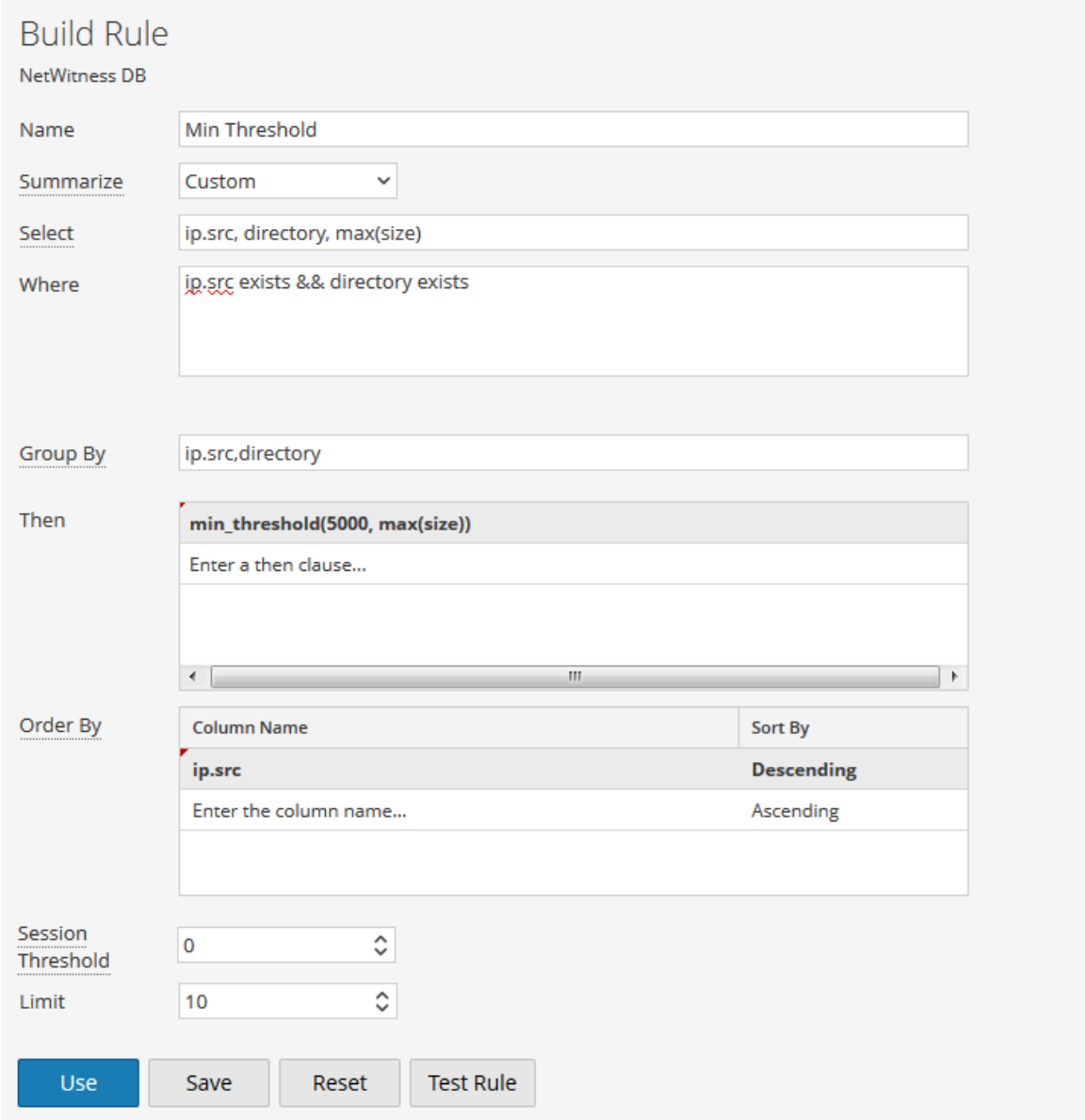
## Filtern aggregierter Metaergebnisse mitMin_threshold

Auf ähnliche Weise werden mithilfe von min_threshold die Ergebnisse für jede beliebige Funktion gefiltert. Betrachten wir ein ähnliches Szenario wie für max_threshold, um dies zu erklären.

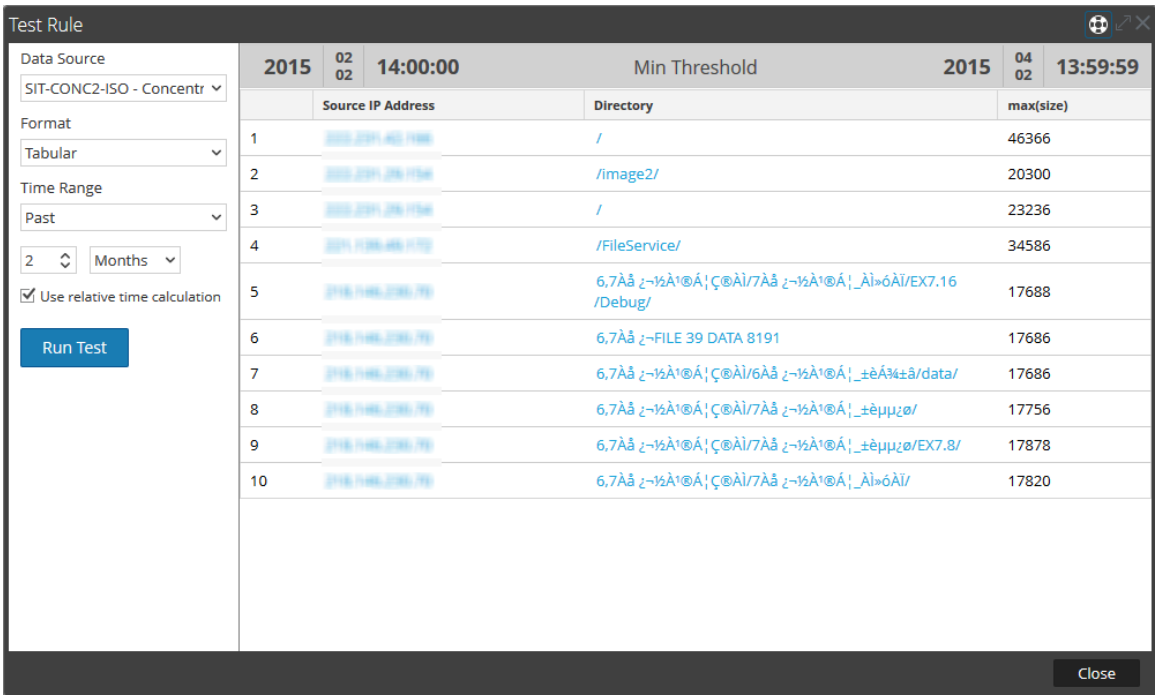
**Beispiel**

Abfrage für „min_threshold“ zusammen mit der Max-Funktion im Feld **Dann**:
**max_threshold(5000,max(size))**

Die folgende Abbildung zeigt den Bildschirm „Regel erstellen“ für die obige Abfrage.




Hier wird der Schwellenwert min_threshold für Datengrößen mit einem unteren Grenzwert von 5000 angewandt. Die folgende Abbildung zeigt das Ergebnis.




Hier zeigt die Ergebnisseite die Spalte max(size) an, in der die Datengrößen größer als 5000 angezeigt werden, da dies der untere Grenzwert in der Abfrage ist, zusammen mit der entsprechenden IP-Quelle und dem entsprechenden Verzeichnis.

**Hinweis:** Die Regelaktionen Max_threshold und Min_threshold haben alle Funktionen gemeinsam und sie können zusammen mit den anderen Abfragen im Feld **Dann** verwendet werden, um die entsprechende Ausgabe abzurufen.

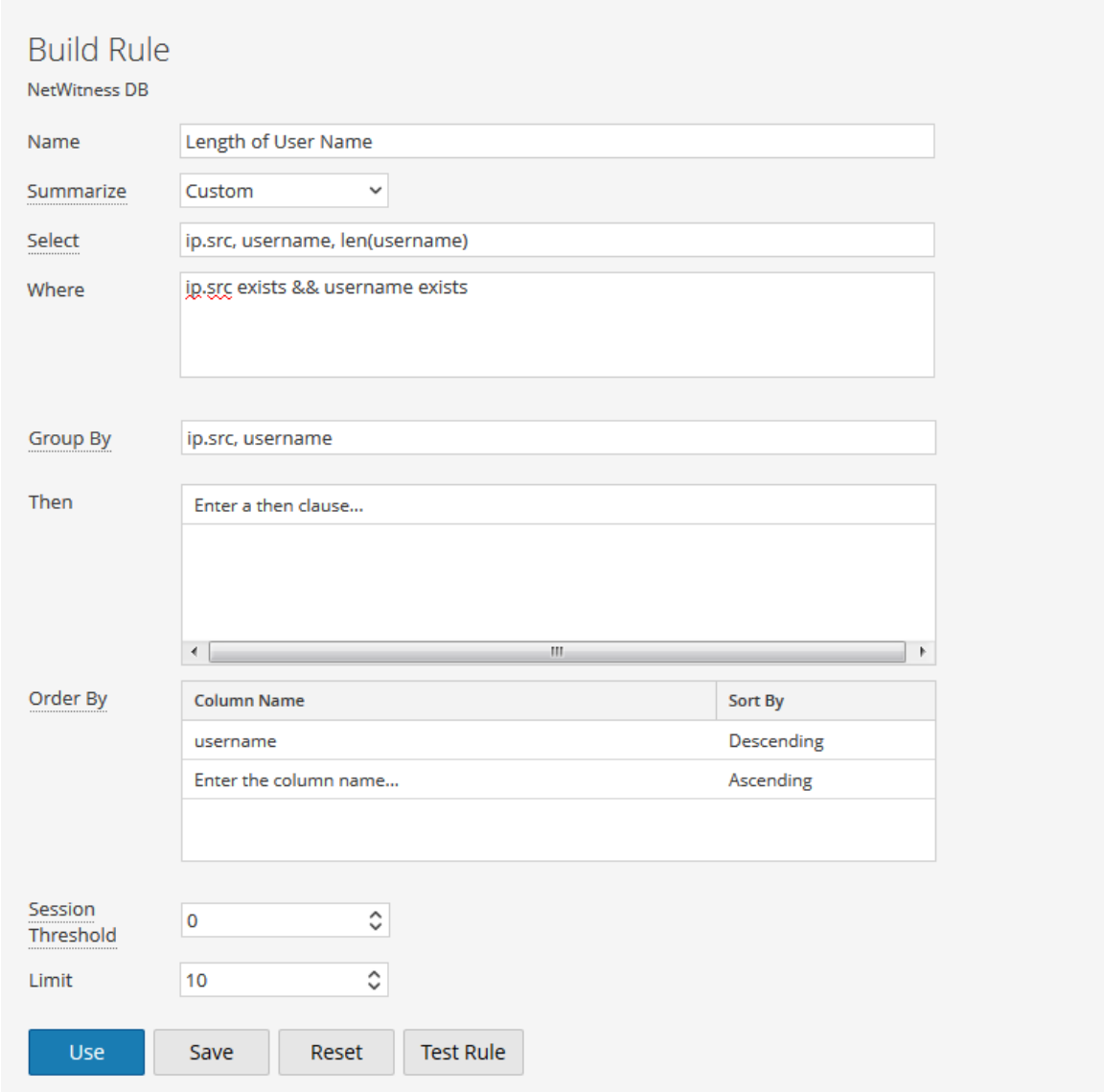
## Länge

Diese Funktion gibt die Länge eines Metawerts zurück. Mit anderen Worten, die Length-Funktion gibt die Anzahl der Byte zurück, die für das Speichern des tatsächlichen Werts verwendet werden.

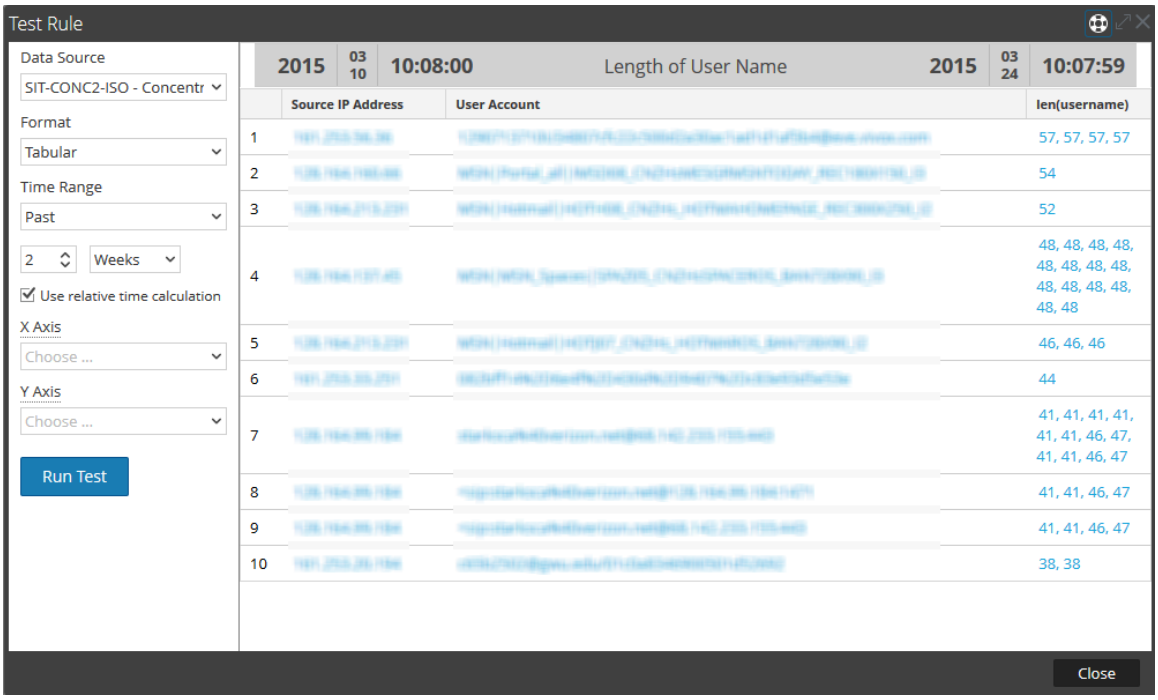
So gibt sie z. B. für den Wert „Analytics“ die Länge 9 zurück. Auf ähnliche Weise gibt sie für ein „IPv4 ip.src“ 4 (für 4 Bytes) zurück.

**Beispiel**

Die folgende Abbildung zeigt eine Musterabfrage für die Funktion length, die für Benutzernamen verwendet wird.




Die folgende Abbildung zeigt das Ergebnis der obigen Abfrage.




Hier zeigt die Seite die Länge der Benutzernamen an, die mit dem Benutzerkonto und ihrer entsprechenden Quell-IP assoziiert sind.

## Weitere Informationen

Wenn Sie mit **Group By** auf einem Metadatum, das mehrere Werte in einer Sitzung hat, nach Aggregaten fragen (z. B. sum(size)), dann wird die Sitzung mit mehreren Werten für aggregierte Berechnung für jeden Wert dieses Metadatums berücksichtigt.

**Beispiel**

Wenn Sie nach der Count-Aggregatfunktion mit „Group By“ auf Alias.host fragen und wenn die Spalte mehrere Werte in einer Sitzung hat, dann wird die Sitzung für jedes Vorkommnis gezählt, einschließlich der Duplikatwerte.

Betrachten Sie die folgende Tabelle.

| SessionID | Alias.host | Ip.src | Größe |
|---|---|---|---|
| 1 | host-a, host-b, host-a | a | 10 |
| 2 | host-b, host-c, host-a, host-c | c | 20 |
| 3 | host-b, host-c, host-d | b | 30 |
| 4 | host-c, host-a | a | 40 |

In der Tabelle oben hat alias.host für **host-a** und **host-c** für eine einzige Sitzung aufgelistete Duplikatwerte. Betrachten wir die folgende Abfrage:

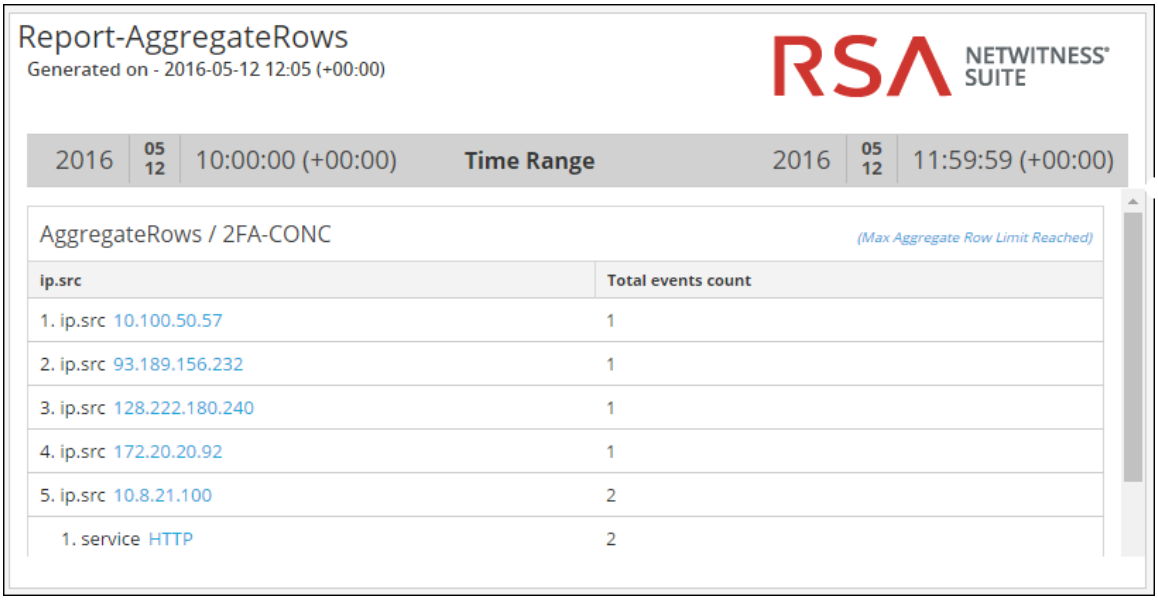
**Auswählen:** alias.host, count(ip.src), sum(size)
**Gruppieren nach**: alias.host

Hier sind **host-a** und **host-c** in 3 Sitzungen vorhanden und sie sind für zwei verschiedene Sitzungen dupliziert. Die Ausgabe wird allerdings wie unten gezeigt.

| Alias.host | count(Ip.src) | Sum (size) |
|---|---|---|
| host-a | 4 | 80 |
| host-b | 3 | 60 |
| host-c | 4 | 110 |
| host-d | 1 | 30 |

Die Ausgabetabelle zeigt, dass die Anzahl für **host-a** und **host-c** 4 ist. Der Grund ist, dass für jeden alias.host-Wert die gesamte Sitzung in Betracht gezogen wird. Auf ähnliche Weise werden zur Berechnung von „sum (size)“ dieselben Sitzungen für jeden alias.host-Wert in Betracht gezogen.

Wenn die Anzahl der Zeilen **NWDB - max. Aggregationszeilen**, wie in der RE-Konfiguration definiert, erreicht hat, wird in der Berichtsausgabe die Meldung **Max. Anzahl aggregierter Zeilen erreicht** angezeigt, um darauf hinzuweisen, dass weitere Informationen zur Anzeige vorhanden sind. Das Standardlimit beträgt 1000 und Sie können diesen Wert entsprechend Ihren Anforderungen auf der Reporting Engine-Konfigurationsseite ändern.



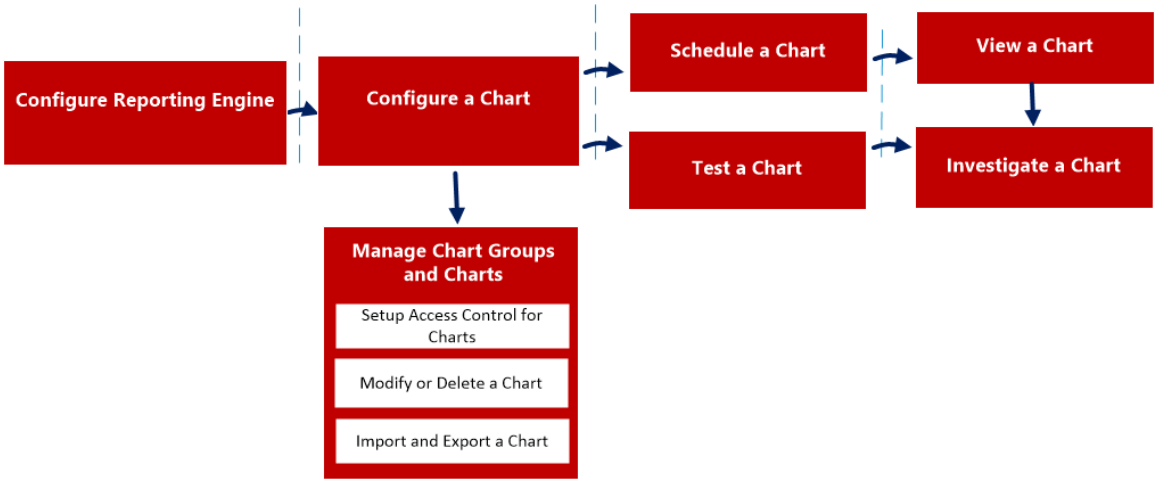
# Konfigurieren und Erzeugen eines Berichts

Ein Diagramm ist eine grafische Darstellung der Daten. Sie können verschiedene Arten von Diagrammen anzeigen, zu denen mehrere Typen von Kurven-, Linien-, Balken- und Flächendiagrammen zählen.

Mit jeder NWDB-Regel im Reporting Engine-System, die nicht nach „Keine“ sortiert ist, kann sofort ein Diagramm erstellt werden. Weitere Informationen zum Erstellen einer NWDB-Regel finden Sie unter Konfigurieren einer Regel.

Das Diagrammintervall kann im Bereich „Diagrammdefinition“ selbst angepasst werden. Bei jeder Ausführung eines Diagramms werden die Ergebnisdaten lokal in der Reporting Engine gespeichert, sodass sie ohne Performanceerwägungen entweder in der Dashboardansicht oder in der Diagrammansicht geprüft werden können.

Die folgende Abbildung stellt eine Übersicht über den gesamten Prozess zum Konfigurieren und Erzeugen eines Diagramms dar.




Führen Sie zum Konfigurieren und Erzeugen eines Diagramms die folgenden Aufgaben durch:

1. Konfigurieren der Reporting Engine
2. Konfigurieren einer NWDB-Regel
3. Konfigurieren eines Diagramms
4. Planen eines Diagramms
5. Anzeigen eines Diagramms
6. Testen eines Diagramms
7. Untersuchen eines Diagramms
8. Managen einer Diagrammgruppe und eines Diagramms

## Konfigurieren Sie Reporting Engine

Sie müssen die Reporting Engine konfigurieren, bevor Sie ein Diagramm konfigurieren und erzeugen können. Außerdem müssen Sie die Datenquelle in der Reporting Engine festlegen, aus der die Daten extrahiert werden. Weitere Informationen zum Konfigurieren der Reporting Engine finden Sie unter **Konfigurieren der Reporting Engine** im *Konfigurationsleitfaden Reporting Engine*.

## Konfigurieren einer NWDB-Regel

Die NetWitness-Regel, die nicht nach „Keine“ sortiert ist, wird zum Erstellen eines Diagramms verwendet. Die NetWitness-Datenbank extrahiert die Metadaten aus der Reporting Engine und stellt die Metadaten für die Regeln bereit. Diese Regeln sind ein wichtiger Baustein im Management eines Diagramms.

**Hinweis:** Wenn die Regel die Regelaktionen „lookup_and_add“, „sum_count“ oder „sum_values“ enthält, enthält das zugehörige Diagramm keine Daten.

## Konfigurieren eines Diagramms

Sie können ein Diagramm mithilfe der NWDB-Regeln konfigurieren.

## Planen eines Diagramms

Nachdem ein Diagramm mit den erforderlichen Komponenten definiert wurde, können Sie seine Ausführungseigenschaften konfigurieren, indem Sie ein Diagramm planen. Hier können Sie die Planungsdetails für ein Diagramm schnell anzeigen, hinzufügen und bearbeiten.

## Anzeigen eines Diagramms

Sie können die geplanten Diagramme in der Ansicht „Diagramm“ anzeigen.

## Testen eines Diagramms

Sie können den Test für ein Diagramm ausführen und alle Diagrammdetails basierend auf dem ausgewählten Zeitbereich anzeigen.

## Zugriffskontrolle für ein Diagramm

Das Modul Reporting stellt die Zugriffskontrolle auf dem Level des Diagramms bereit. Nur ein Benutzer mit den richtigen Berechtigungen kann die Aufgaben im Reporting-Modul durchführen. Die Zugriffskontrolle wird vom Administrator auf der Registerkarte **Administration > Sicherheit > Rollen** gemanagt.

Wenn Sie Benutzer und Benutzerrollen erstellen, stellen Sie sicher, dass die von Ihnen für bestimmte Aufgaben erstellten Rollen Zugriff auf alle erforderlichen Berechtigungen haben. Dies könnte Berechtigungen auf verschiedenen Levels der Rollenhierarchie erfordern.

Diagramme können einem bestimmten Satz von Benutzerrollen zugeordnet werden, sodass die Diagramme mit den Zugriffsrechten für die spezifische Benutzerrolle angezeigt werden können, wenn ein Benutzer sich bei NetWitness anmeldet. Benutzer, die zu einer Benutzerrolle mit der Zugriffsberechtigung „Lesen & Schreiben“ gehören, können Berichte definieren. Darüber hinaus kann der Zugriff so eingeschränkt werden, dass nur die Benutzer mit der Berechtigung „Schreibgeschützt“ auf Diagramme zugreifen können.

Auf dem Level der Diagramme können Sie die folgenden Zugriffsberechtigungen für die Benutzerrollen in NetWitness angeben:

- Lesen & Schreiben
- Schreibgeschützt
- Kein Zugriff

Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie diese auf dem Level der Diagramme festlegen. Damit z. B. **Administratoren** Zugriff auf ein bestimmtes Diagramm haben, könnten Sie die Berechtigung „Lesen & Schreiben“ im Dialogfeld „Diagrammberechtigungen“ festlegen.

Sie können die Leseberechtigung auf die Regeln in den Diagrammen anwenden, indem Sie das Kontrollkästchen aktivieren.

Im Folgenden werden zwei Szenarien erklärt, die beschreiben, wie Sie die Zugriffskontrolle festlegen:

- Szenario 1: Berechtigungen werden basierend auf der Benutzerrolle auf Diagrammgruppe/Untergruppe/Diagramm/Regeln angewendet.
- Szenario 2: Leseberechtigung wird auf Regeln im Diagramm angewendet.

| | Rolle (Analyst) | Berechtigungen werden basierend auf der Benutzerrolle auf Diagrammgruppe/Untergruppe/Diagramm oder Regeln angewendet | Berechtigungen (Schreibgeschützt) werden auf Regeln im Diagramm angewendet |
|---|---|---|---|
| **Gruppe** | Lesen & Schreiben | Lesen & Schreiben | Lesen & Schreiben |
| **Untergruppe** | Lesen | Lesen | Lesen & Schreiben |

| | Rolle (Analyst) | Berechtigungen werden basierend auf der Benutzerrolle auf Diagrammgruppe/Untergruppe/Diagramm oder Regeln angewendet | Berechtigungen (Schreibgeschützt) werden auf Regeln im Diagramm angewendet |
|---|---|---|---|
| **Diagramm** | Lesen | Lesen | Lesen & Schreiben |
| **Regeln** | Lesen | Lesen | Lesen |

Dem Diagramm wird die Rolle eines **Sicherheitsanalysten** zugewiesen und die Berechtigungen für Diagramme werden auf Lesen und Schreiben festgelegt.

In Szenario 1 verfügt jedes der Level über einen Berechtigungssatz auf Basis der Benutzerrolle. In Szenario 2 wird die Leseberechtigung für die Regeln festgelegt. Hierbei gilt, dass die für die Regeln festgelegte Berechtigung nicht höher sein darf als die für die Diagramme.

**Hinweis:** Wenn die Berechtigung für die Regeln eine höhere Stufe als die für das Diagramm hat, wird sie nicht angewendet. Wenn Sie beispielsweise die Berechtigungen für die Berichtsgruppe auf **Kein Zugriff** festlegen und die Option *Nur-Lese-Berechtigungen auf Regeln in Berichten anwenden* aktivieren, wird die Leseberechtigung für die Regeln nicht festgelegt.

## Zugriffskontrolle für ein Diagramm bei Auswahl von mehreren Diagrammen

Wenn Sie Berechtigungen für mehrere Diagramme ändern möchten, müssen Sie mehrere Diagramme auswählen und ihre Zugriffsberechtigungen im Bereich „Diagrammberechtigungen“ festlegen. Die von Ihnen ausgewählte Zugriffsberechtigung wird auf alle ausgewählten Diagramme angewendet.

## Zugriffskontrolle für ein Diagramm bei Auswahl von mehreren Diagrammen mit verschiedenen Regeln

Wenn Sie Zugriffsberechtigungen bei Auswahl mehrerer Diagramme mit verschiedenen Regeln ändern möchten, aktivieren Sie das Kontrollkästchen im Bereich „Diagrammberechtigungen“.

Die Lesezugriffsberechtigung wird auf alle Regeln der ausgewählten Diagramme angewendet, sofern die Berechtigung für die Regeln eine niedrigere Stufe als die für Diagramme hat.

**Hinweis:** Wenn ein Benutzer (ein anderer als der Superuser) ein Diagramm erstellt, hat der Superuser keinen Zugriff auf dieses Diagramm.

# Zugriffskontrolle für eine Diagrammgruppe

Wenn Sie Berechtigungen für eine Diagrammgruppe ändern möchten, wählen Sie diese aus und legen Sie ihre Zugriffsberechtigungen im Bereich „Diagrammberechtigungen“ fest. Bevor Diagrammgruppenberechtigungen angewendet werden, lautet der Standardberechtigungssatz für alle Benutzerrollen „Kein Zugriff“.

Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie die Berechtigung auf dem Level der Diagrammgruppen festlegen. Damit z. B. Administratoren Zugriff auf alle Diagramme in einer Diagrammgruppe haben, legen Sie die Berechtigung „Lesen & Schreiben“ im Bereich „Diagrammgruppenberechtigungen“ fest.

Sie können Berechtigungen auch auf Untergruppen und Diagramme in der Gruppe sowie Leseberechtigungen auf Regeln in den Diagrammen anwenden, indem Sie die entsprechenden Kontrollkästchen aktivieren.

Im Folgenden werden drei Szenarien erklärt, die beschreiben, wie Sie die Zugriffskontrolle festlegen:

- Szenario 1: Berechtigungen werden basierend auf der Benutzerrolle auf Diagrammgruppen, Untergruppen oder Diagramme angewendet.
- Szenario 2: Berechtigungen werden auf Untergruppen und Diagramme in der Gruppe angewendet.
- Szenario 3: Leseberechtigung wird auf Regeln im Diagramm angewendet.

| | Rolle (Analyst) | Berechtigungen werden basierend auf Benutzerrollen auf Diagrammgruppen, Untergruppen oder Diagramme angewendet. | Berechtigungen werden auf Untergruppen und Diagramme in der Gruppe angewendet | Berechtigungen (Schreibgeschützt) werden auf Regeln im Diagramm angewendet |
|---|---|---|---|---|
| **Gruppe** | Lesen & Schreiben | Lesen & Schreiben | Lesen & Schreiben | Lesen & Schreiben |
| **Untergruppe** | Lesen | Lesen | Lesen & Schreiben – übernommen | Lesen & Schreiben |

| | Rolle (Analyst) | Berechtigungen werden basierend auf Benutzerrollen auf Diagrammgruppen, Untergruppen oder Diagramme angewendet. | Berechtigungen werden auf Untergruppen und Diagramme in der Gruppe angewendet | Berechtigungen (Schreibgeschützt) werden auf Regeln im Diagramm angewendet |
|---|---|---|---|---|
| **Diagramm** | Lesen | Lesen | Lesen & Schreiben – übernommen | Lesen & Schreiben |
| **Regeln** | Lesen | Lesen | Lesen | **Lesen** |

Der Diagrammgruppe wird die Rolle eines **Sicherheitsanalysten** zugewiesen und Berechtigungen werden auf „Lesen & Schreiben“ festgelegt.

In Szenario 1 erhält jede Ebene abhängig von der Benutzerrolle einen Berechtigungssatz.

In Szenario 2 wird die Berechtigung auf der Diagrammgruppenebene von der Untergruppe und von Diagrammen in der Gruppe übernommen.

In Szenario 3 wird die Leseberechtigung für die Regeln festgelegt. Der Berechtigungssatz für die Regeln darf jedoch nicht höher sein als der Berechtigungssatz für die Diagrammgruppe.

In der folgenden Tabelle werden die Spalten im Bereich „Diagrammberechtigungen“ aufgelistet.

| Spalte | Beschreibung |
|---|---|
| Rollen | Die Rolle des an der NetWitness-Benutzeroberfläche angemeldeten Benutzers. |
| Lesen & Schreiben | Der Benutzer kann das Diagramm in der Ansicht „Diagramme“ aufrufen, anzeigen, bearbeiten, importieren, exportieren und löschen. Der Benutzer kann auch die Berechtigung für das Diagramm ändern. |

| Spalte | Beschreibung |
| --- | --- |
| Schreibgeschützt | Der Benutzer kann in der Ansicht „Diagramme“ nur auf das Diagramm zugreifen und dieses anzeigen. |
| Kein Zugriff | Der Benutzer kann Diagramme, für die diese Berechtigung festgelegt wurde, weder anzeigen noch darauf zugreifen. |
| ☐ Diese Berechtigungen auf Untergruppen und Diagramme in dieser Gruppe anwenden | Aktivieren Sie das Kontrollkästchen, um die ausgewählten Berechtigungen auf die Diagrammgruppe, Untergruppen in der Gruppe und Diagramme in der Gruppe anzuwenden.<br>**Hinweis:** Das Kontrollkästchen wird nur gefüllt, wenn Zugriffsberechtigungen für eine Diagrammgruppe festgelegt werden. |
| ☐ Nur-Lese-Berechtigungen auf Regeln in Diagrammen anwenden | Aktivieren Sie das Kontrollkästchen, um die Berechtigungen automatisch auf die Regeln in den Diagrammen anzuwenden. |

# Konfigurieren eines Diagramms

Nachdem ein Diagramm mit den NetWitness-Regeln mit NWDB als Datenquelle definiert wurde, können Sie seine Ausführungseigenschaften konfigurieren.

## Löschen einer Diagrammgruppe

Führen Sie folgende Schritte durch, um Gruppen zum Standardordner oder Untergruppen unter einer Diagrammgruppe hinzuzufügen:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Klicken Sie im Bereich **Diagrammgruppen** auf +.
   Eine Standardgruppe wird im Bereich „Diagrammgruppen“ hinzugefügt.
4. Geben Sie den Namen für die neue Gruppe ein.
5. Drücken Sie die Eingabetaste.
   Die Gruppe wird im Bereich „Diagrammgruppen“ hinzugefügt.

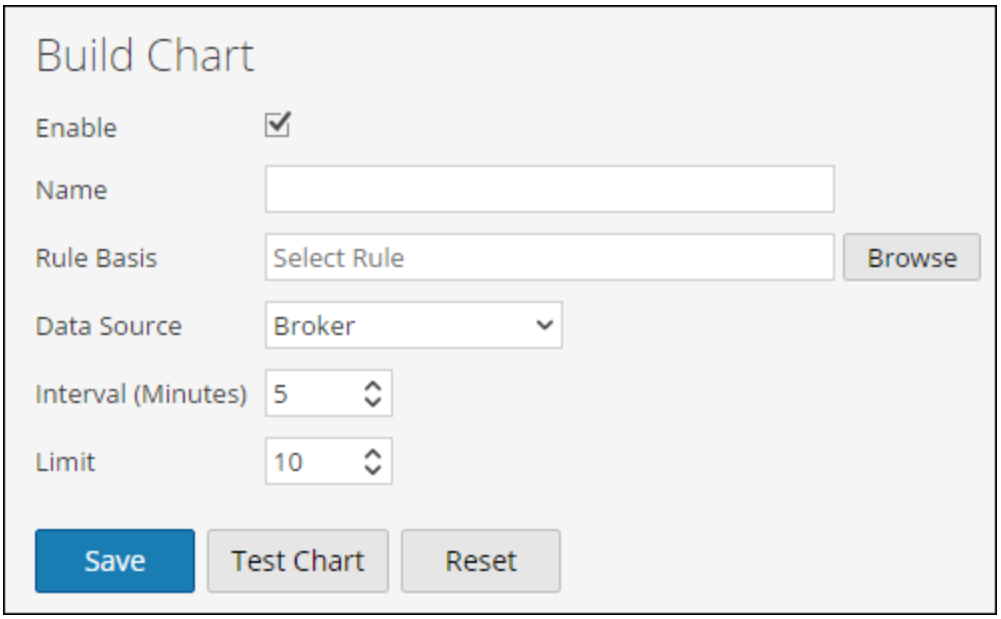
## Erstellen von Diagrammen

Sie fügen Sie einer Gruppe oder Untergruppe Diagramme hinzu:

1. Navigieren Sie zu **Monitor** > **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**, um die Diagrammansicht anzuzeigen.

3. Klicken Sie in der Symbolleiste **Diagramm** auf +.

   Die Registerkarte „Diagramm erstellen“ wird angezeigt.




4. Geben Sie den Namen für das Diagramm ein.
5. Um der Reporting Engine das Sammeln von Daten und Erzeugen von Diagrammergebnissen zu ermöglichen, aktivieren Sie das Kontrollkästchen **Aktivieren**.
6. Gehen Sie im Feld Regelbasis wie folgt vor:
   a. Klicken Sie auf **Durchsuchen**. Das Dialogfeld Regel hinzufügen wird angezeigt.
   b. Navigieren Sie in der Regelstruktur und wählen Sie eine Regel aus.
   c. Klicken Sie auf **Auswählen**.
7. Die Regel wird im Feld Regelbasis angezeigt.
8. Wählen Sie die Datenquelle aus der Drop-down-Liste **Datenquelle** aus.

   **Hinweis:** Wenn die Standarddatenquelle in der Reporting Engine konfiguriert ist, wird die Datenquelle standardmäßig auf der Seite „Diagramm erstellen“ angezeigt. Wenn die Datenquelle nicht aufgelistet wird, stellen Sie sicher, dass Sie die Berechtigung „Lesen“ für die Datenquelle festgelegt haben. Dies gilt für NWDB- und Warehouse-Datenquellen. Weitere Informationen finden Sie im Thema **Konfigurieren von Datenquellenberechtigungen** im *Leitfaden zur Host- und Servicekonfiguration.*

9. (Optional) Um den Intervallwert zu ändern, klicken Sie auf den Pfeil nach oben oder nach unten.

   Der Intervallwert gibt an, in welchen Intervallen in Minuten die Regel, auf der das

Diagramm basiert, zur Datensammlung ausgeführt wird.

10. Wählen Sie den Grenzwert aus, um die Anzahl der anzuzeigenden Datensätze zu begrenzen.
11. **X-Achse** und **Y-Achse** werden zur Angabe der Metadaten verwendet, die in die Diagramme geplottet werden sollen.
    In der **X-Achse** werden die Metadaten für die Regel „Gruppieren nach“ angezeigt. In der **Y-Achse** werden die in der Regel verwendeten Aggregatfunktionen angezeigt.

    **Hinweis:** Die unterstützten Aggregatfunktionen für Diagramme sind „Sum“, „Count“, „Countdistinct“ und „Average“. Standardmäßig können Sie für benutzerdefinierte Regeln mit mehreren „Gruppieren nach“-Klauseln nur die ersten Metadaten in **X-Achse** auswählen.
12. Klicken Sie auf **Speichern**.
    In einer Meldung wird bestätigt, dass das Diagramm erfolgreich gespeichert wurde.

# Planen eines Diagramms

Sie müssen ein Diagramm planen, um die Diagrammdetails näher zu untersuchen.

Wenn Sie ein Diagramm aktivieren, wird es wie geplant ausgeführt und stellt die konfigurierte Ausgabe zur Verfügung; der Status des Diagramms wechselt auf „Geplant“.

So planen Sie ein Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammliste** ein Diagramm oder mehrere Diagramme aus, die in der Spalte **Aktiviert** mit ○ gekennzeichnet sind.
4. Klicken Sie auf ●.
   In einer Meldung wird bestätigt, dass der Diagrammstatus erfolgreich geändert wurde.

# Anzeigen eines Diagramms

Nach dem Anzeigen eines Diagramms können Sie die folgenden Aufgaben ausführen:

1. Sie können Diagramme ausdrucken, speichern, per E-Mail versenden und auf dem ganzen Bildschirm anzeigen.
2. Sie können außerdem im Kalender ein Datum auswählen, um eine Liste der erfolgreich ausgeführten Diagramme für das ausgewählte Datum anzuzeigen.

So zeigen Sie ein Diagramm an:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Führen Sie im Bereich **Diagrammliste** einen der folgenden Schritte aus:
   - Wählen Sie ein Diagramm aus und klicken Sie auf  > **Anzeigen**.
   - Wählen Sie ein Diagramm aus und klicken Sie in der Spalte „Diagramm anzeigen“ auf **Anzeigen**.
     Die Registerkarte der Ansicht Diagramm anzeigen wird angezeigt.
4. Führen Sie in **Diagrammoptionen** die folgenden Schritte aus:
   a. Legen Sie den **Zeitbereich** fest.

   **Hinweis:** Wenn Sie die Option „Zeitbereich“ auswählen, können Sie einen vordefinierten Zeitbereich auswählen, z. B. die letzte Stunde, die letzten 3 Stunden und die letzten n Tage usw., oder Sie können die Auswahl durch Verwenden von „Letzte N Tage“ oder „Benutzerdefiniert“ anpassen. Wenn Sie die Option „Letzte N Tage“ auswählen, können Sie die Verlaufsdaten für maximal 15 Tage anzeigen. Wenn Sie die Option „Benutzerdefiniert“ auswählen, können Sie ein Startdatum und Enddatum zum Anzeigen der Daten für den ausgewählten Datumsbereich festlegen.

   b. Wählen Sie die **Serie** aus, entweder **Diagramm mit Werten im Zeitverlauf zeichnen** oder **Diagramm mit Summen zeichnen**.
   Wenn Sie **Diagramm mit Werten im Zeitverlauf zeichnen** auswählen, zeigt das Diagramm die Änderung der Werte im ausgewählten Zeitraum an. Wenn Sie **Diagramm mit Summen zeichnen** auswählen, zeigt das Diagramm eine Summe für jeden Aggregatwert für den ausgewählten Zeitraum an.

c. Wählen Sie **Zu zeichnende Elemente** aus, um die Anzahl der Ereignisse zu definieren, die im Diagramm angezeigt werden sollen.

d. Wählen Sie aus der Drop-down-Liste **Diagrammtyp** den Diagrammtyp aus.

e. Klicken Sie auf **Neu laden**, um das ausgewählte Diagramm neu zu laden.
Wenn beim Abrufen der Verlaufsdaten für den ausgewählten Zeitraum eine Verzögerung auftritt, wird eine Meldung angezeigt.

Nachdem das Diagramm erzeugt wurde, wird im Benachrichtigungsbereich in der NetWitness-Symbolleiste eine Benachrichtigung angezeigt. Weitere Informationen zur NetWitness-Symbolleiste finden Sie im Thema **Browserfenster** im *Leitfaden für die ersten Schritte mit NetWitness*.

## Anzeigen der Liste aller Diagramme

So zeigen Sie eine Liste aller Diagramme an:

1. Wählen Sie **Monitor** > **Berichte** aus.
Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
Die Ansicht „Diagramm“ wird angezeigt.
3. Klicken Sie in der Symbolleiste **Diagramm** auf **Alle Diagramme anzeigen**.
Alle ausgeführten Diagramme für die ausgewählten Daten werden in einer neuen Registerkarte angezeigt.

**Hinweis:**
* Wenn keine Liste angezeigt wird, können Sie ein Datum im Kalender auswählen, um eine Liste von Diagrammen anzuzeigen.
* Wenn Sie ein bestimmtes Diagramm anzeigen möchten, geben Sie den Diagrammnamen im Feld Suchkriterien ein.

4. Klicken Sie auf den Namen des Diagramms, um die Diagrammdetails zu diesem Datum anzuzeigen.

# Testen eines Diagramms

Sie können ein Diagramm in der Ansicht **Diagramm testen** testen.

So testen Sie ein Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Symbolleiste **Diagramm** auf .
   - Doppelklicken Sie im Bereich **Diagramm** auf ein Diagramm oder wählen Sie ein Diagramm aus und klicken Sie auf .
   - Klicken Sie im Bereich **Diagrammliste** auf > **Bearbeiten**.
     Die Registerkarte „Diagramm erstellen“ wird angezeigt.
4. Klicken Sie auf **Diagramm testen**, um das Diagramm anzuzeigen.
   Die Registerkarte der Ansicht Diagramm anzeigen wird angezeigt.
5. Wählen Sie **Von** und **Bis** für den Datumsbereich aus.
6. Wählen Sie die **Serie** aus, entweder **Zeitserien** oder **Zusammenfassung**.
7. Wählen Sie aus der Drop-down-Liste **Diagrammtyp** den Diagrammtyp aus.
8. Klicken Sie auf **Test ausführen**, um den Test auszuführen.
   Die Diagrammdaten (falls vorhanden) für den ausgewählten Zeitbereich werden angezeigt.

# Untersuchen eines Diagramms

Sie können das Diagramm untersuchen, indem Sie vom Diagramm aus direkt zum Modul „Investigation“ navigieren.

So untersuchen Sie ein Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Klicken Sie in der Symbolleiste **Diagramm** auf **Alle Diagramme anzeigen**.
   Alle ausgeführten Diagramme für das ausgewählte Datum im Bereich **Diagrammoptionen** werden in einer neuen Registerkarte angezeigt.
4. Klicken Sie auf den Namen des Diagramms, um die Details des Diagramms wie den Ausführungszeitpunkt des Diagramms und die für die Ausführung des Diagramms verwendete Standarddatenquelle anzuzeigen.
5. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf einen Datenpunkt im Diagramm, um diesen zu untersuchen.
   - Klicken Sie in der Symbolleiste auf **Untersuchen**, um den gesamten Zeitraum zu untersuchen.

# Managen einer Diagrammgruppe und eines Diagramms

Sie können Diagrammgruppen und Diagramme mithilfe der folgenden Verfahren managen.

## Managen einer Diagrammgruppe

Abhängig von den Zugriffsberechtigungen für die Benutzerrolle können Sie ein Diagramm ändern oder löschen, importieren und exportieren, per Drag-and-drop verschieben und eine Diagrammgruppe aktualisieren.

### Ändern einer Diagrammgruppe

So ändern Sie eine Diagrammgruppe im Standardordner oder Untergruppen unter einer Diagrammgruppe:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammgruppen** eine Diagrammgruppe aus, die geändert werden soll.
   Die ausgewählte Diagrammgruppe wird geändert und kann im Bereich „Diagrammgruppen“ angezeigt werden.

### Löschen einer Diagrammgruppe

So löschen Sie eine Diagrammgruppe im Standardordner oder Untergruppen unter einer Diagrammgruppe:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammgruppen** die Gruppe und klicken Sie auf .
   Sie werden in einem Dialogfeld aufgefordert zu bestätigen, dass Sie die ausgewählte Gruppe löschen möchten.
4. Klicken Sie auf **Ja**, um die Gruppe zu löschen.
   Die ausgewählte Gruppe wird aus dem Bereich „Diagrammgruppen“ gelöscht.

### Importieren einer Diagrammgruppe

So importieren Sie Diagrammgruppen aus anderen Instanzen von NetWitness Suite:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammgruppen** einen Ordner aus, in den die Datei importiert werden soll.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im Bereich „Diagrammgruppen“ auf  > **Importieren**.
     Das Dialogfeld **Diagramm importieren** wird angezeigt. Sie können mehrere Diagrammgruppen gleichzeitig importieren. Um mehrere Diagrammgruppen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Diagrammgruppen aus, die importiert werden sollen.
5. Klicken Sie auf **Durchsuchen**, um die Binärdatei auszuwählen.
   NetWitness bietet eine Dateisystemansicht der Dateien.
6. Suchen Sie die Binärdatei und klicken Sie auf **Öffnen**.
   Die Datei wird der Liste „Diagramm importieren“ hinzugefügt.
7. (Optional) Aktivieren Sie das Kontrollkästchen**Regel**,wenn Sie beim Import eine beliebige vorhandene Regel in der Bibliothek mit einer identisch benannten Regel in der Binärdatei überschreiben möchten. Wenn Sie die Option Überschreiben nicht auswählen und eine identische Regel in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.
8. (Optional) Aktivieren Sie das Kontrollkästchen**Liste**, wenn Sie beim Import eine beliebige vorhandene Liste in der Bibliothek mit einer identisch benannten Liste in der Binärdatei überschreiben möchten. Wenn Sie die Option „Überschreiben“ nicht auswählen und eine identische Liste in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.
9. (Optional) Um ein beliebiges vorhandenes Diagramm in der Bibliothek mit einem gleichnamigen Diagramm in der Binärdatei zu überschreiben, aktivieren Sie das Kontrollkästchen **Diagramm**. Wenn Sie die Option „Überschreiben“ nicht auswählen und ein identisches Diagramm in der Binärdatei vorhanden ist, wird die Binärdatei importiert und keine Fehlermeldung angezeigt.
10. Klicken Sie auf **Importieren**, um die Binärdatei zu importieren.

## Exportieren einer Diagrammgruppe

So exportieren Sie ausgewählte Diagrammgruppen:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammgruppen** eine Diagrammgruppe aus, klicken Sie auf  und führen Sie einen der folgenden Schritte aus:
   - **Exportieren**: Mit dieser Auswahl wird ein Diagramm in eine ZIP-Datei exportiert.
   - **Als Text exportieren**: Mit dieser Auswahl werden alle Inhalte aus der Reporting Engine in eine ZIP-Datei exportiert, welche die Daten im Textformat enthält.

   Sie können mehrere Diagrammgruppen gleichzeitig exportieren. Um mehrere Diagrammgruppen auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Diagrammgruppen aus, die exportiert werden sollen. Die exportierte Datei wird auf dem lokalen Laufwerk gespeichert.

## Ziehen eines Diagramms zu einer Gruppe

So ziehen Sie ein Diagramm per Drag-and-drop aus dem Bereich „Diagrammliste“ in eine Gruppe des Bereichs „Diagrammgruppen“:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammliste** ein Diagramm aus und ziehen Sie dieses per Drag-and-drop in eine Gruppe im Bereich **Diagrammgruppen**.
   Das Diagramm wird in die Gruppe im Bereich „Diagrammgruppen“ kopiert.

## Aktualisieren einer Diagrammgruppe

So aktualisieren Sie Diagrammgruppen:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Verschieben Sie die Gruppe im Bereich **Diagrammgruppen** per Drag-and-drop.
   Die Diagrammgruppe wird zum neuen Standort verschoben.

4. Klicken Sie im Bereich **Diagrammgruppen** auf  .

   Die Diagrammgruppe wird aktualisiert.

# Managen eines Diagramms

Abhängig von den Zugriffsberechtigungen für die Benutzerrolle können Sie Diagramme ändern oder löschen, duplizieren, importieren und exportieren, aktivieren oder deaktivieren, nach vorhandenen Diagrammen suchen und eine Diagrammliste aktualisieren.

# Zugriffskontrolle für ein Diagramm

So legen Sie Zugriffsberechtigungen für ein Diagramm fest:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammliste** ein Diagramm aus.
4. Klicken Sie auf  > **Berechtigungen**.
   Das Dialogfeld „Diagrammberechtigungen“ wird angezeigt.
5. Wählen Sie aufgrund der Benutzerrolle die entsprechenden Schaltflächen aus.
6. (Optional) Aktivieren Sie das Kontrollkästchen, wenn abhängigen Regeln die Zugriffsberechtigung zum Lesen zugewiesen werden soll.

   **Hinweis:** Wenn das Kontrollkästchen aktiviert ist, erhalten alle abhängigen Regeln ohne Zugriffsberechtigung die Zugriffsberechtigung LESEN.
7. Klicken Sie auf **Speichern**.
   Die Bestätigungsmeldung, dass die Berechtigung für das ausgewählte Diagramm erfolgreich festgelegt wurde, wird angezeigt.

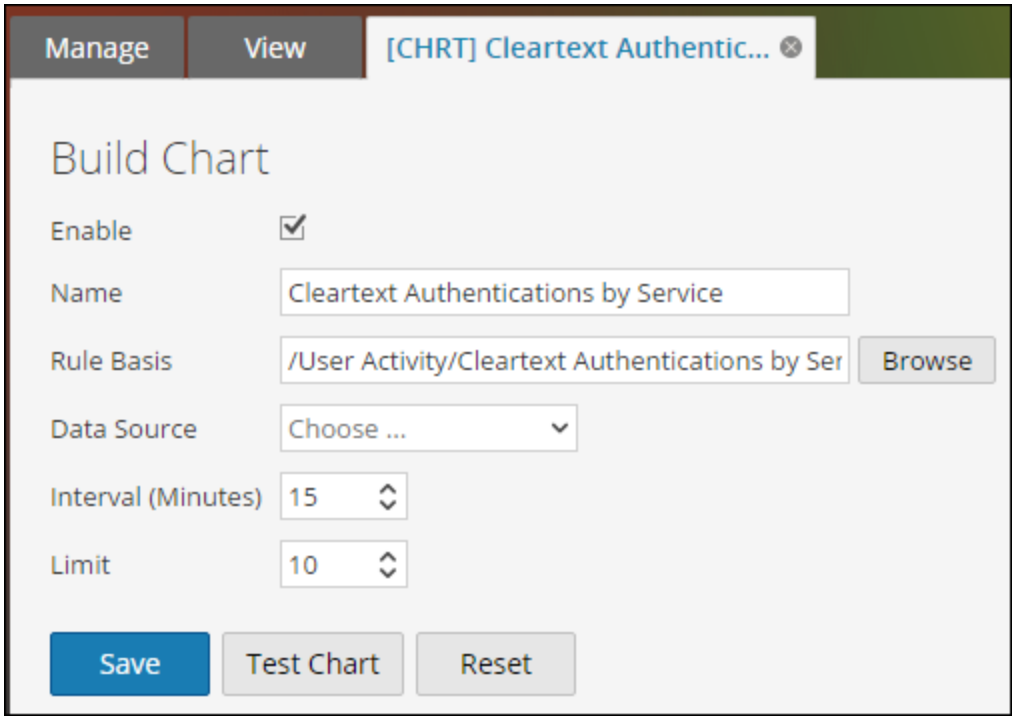
## Ändern eines Diagramms

So ändern Sie ein Diagramm in einer Gruppe oder Untergruppe:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Führen Sie im Bereich **Diagrammliste** einen der folgenden Schritte aus:
   - Doppelklicken Sie auf ein Diagramm oder wählen Sie ein Diagramm aus und klicken Sie auf  .

- Wählen Sie ein Diagramm aus und klicken Sie auf  > **Bearbeiten**.

  Die Registerkarte „Diagramm erstellen“ wird angezeigt.




4. Ändern Sie den Namen des Diagramms.
5. Um der Reporting Engine das Sammeln von Daten und Erzeugen von Diagrammergebnissen zu ermöglichen, aktivieren Sie das Kontrollkästchen **Aktivieren**.
6. (Optional) Gehen Sie im Feld **Regelbasis** wie folgt vor:
   a. Klicken Sie auf **Durchsuchen**.
      Das Dialogfeld „Regel hinzufügen“ wird angezeigt.
   b. Navigieren Sie in der Regelstruktur und wählen Sie eine Regel aus.
   c. Klicken Sie auf **Auswählen**.
      Die Regel wird im Feld Regelbasis angezeigt.
7. Wählen Sie die Datenquelle aus der Drop-down-Liste **Datenquelle** aus.

   **Hinweis:** Wenn die Datenquelle nicht aufgelistet ist, stellen Sie sicher, dass Sie die **Leseberechtigung** für die Datenquelle haben. Dies gilt nur für NWDB- und Warehouse-Datenquellen. Weitere Informationen finden Sie im Thema **Konfigurieren von Datenquellenberechtigungen** im *Leitfaden zur Host- und Servicekonfiguration.*
8. (Optional) Um den Intervallwert zu ändern, klicken Sie auf die Pfeile nach oben oder nach unten.

9. Wählen Sie den Grenzwert, um die Anzahl der anzuzeigenden Datensätze zu begrenzen.
10. Klicken Sie auf **Speichern**.
    Eine Bestätigungsmeldung, dass das Diagramm erfolgreich geändert wurde, wird angezeigt.

## Löschen eines Diagramms

So löschen Sie ein Diagramm in einer Gruppe oder Untergruppe:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Führen Sie im Bereich **Diagrammliste** einen der folgenden Schritte aus:
   - Wählen Sie die Diagramme aus und klicken Sie auf .
   - Klicken Sie auf > **Löschen**.
     Sie werden aufgefordert zu bestätigen, dass Sie das ausgewählte Diagramm löschen möchten.
4. Klicken Sie auf **Ja**, um das Diagramm zu löschen.
   Eine Bestätigungsmeldung wird angezeigt, dass das Diagramm gelöscht wurde. Das ausgewählte Diagramm wird aus dem Bereich „Diagrammliste“ entfernt.

## Duplizieren eines Diagramms

So duplizieren Sie ein vorhandenes Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammliste** ein zu duplizierendes Diagramm aus.
4. Klicken Sie in der Symbolleiste **Diagramm** auf .
   Das Diagramm wird dupliziert und im Bereich Diagrammliste hinzugefügt.

## Importieren eines Diagramms

So importieren Sie Diagramme aus anderen Instanzen von NetWitness:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammgruppen** einen Ordner aus, aus dem die Datei importiert werden soll.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Diagrammsymbolleiste auf  > **Importieren**.
     Das Dialogfeld **Diagramm importieren** wird angezeigt. Sie können mehrere Diagramme gleichzeitig importieren. Um mehrere Diagramme auszuwählen, halten Sie die STRG-Taste gedrückt und wählen Sie die Diagramme aus, die importiert werden sollen.
5. Klicken Sie auf **Durchsuchen**, um die Binärdatei auszuwählen.
   NetWitness bietet eine Dateisystemansicht der Dateien.
6. Suchen Sie die Binärdatei und klicken Sie auf **Öffnen**.
   Die Datei wird der Liste „Diagramm importieren“ hinzugefügt.
7. (Optional) Aktivieren Sie das Kontrollkästchen**Regel**, wenn Sie beim Import eine beliebige vorhandene Regel in der Bibliothek mit einer identisch benannten Regel in der Binärdatei überschreiben möchten. Wenn Sie die Option Überschreiben nicht auswählen und eine identische Regel in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.
8. (Optional) Aktivieren Sie das Kontrollkästchen**Liste**, wenn Sie beim Import eine beliebige vorhandene Liste in der Bibliothek mit einer identisch benannten Liste in der Binärdatei überschreiben möchten. Wenn Sie die Option „Überschreiben“ nicht auswählen und eine identische Liste in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.
9. (Optional) Um ein beliebiges vorhandenes Diagramm in der Bibliothek mit einem gleichnamigen Diagramm in der Binärdatei zu überschreiben, aktivieren Sie das Kontrollkästchen **Diagramm**. Wenn Sie die Option „Überschreiben“ nicht auswählen und ein identisches Diagramm in der Binärdatei vorhanden ist, wird die Binärdatei importiert und keine Fehlermeldung angezeigt.
10. Klicken Sie auf **Importieren**, um die Binärdatei zu importieren.

## Exportieren eines Diagramms

So exportieren Sie ausgewählte Diagramme in eine externe Datei:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammliste** ein Diagramm aus, klicken Sie auf  und führen Sie einen der folgenden Schritte aus:
   - **Exportieren**: Mit dieser Auswahl wird ein Diagramm in eine ZIP-Datei exportiert.
   - **Als Text exportieren**: Mit dieser Auswahl wird ein Diagramm aus der Reporting Engine in eine ZIP-Datei exportiert, welche die Daten im Textformat enthält.

   Sie können mehrere Diagramme gleichzeitig exportieren. Um mehrere Diagramme auszuwählen, aktivieren Sie die Kontrollkästchen für die Diagramme, die exportiert werden sollen. Die exportierte Datei wird auf dem lokalen Laufwerk gespeichert.

## Aktivieren eines Diagramms

So aktivieren Sie ein Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammliste** ein Diagramm oder mehrere Diagramme aus, die in der Spalte **Aktiviert** mit ○ gekennzeichnet sind.
4. Klicken Sie auf ●.
   In einer Meldung wird bestätigt, dass der Diagrammstatus erfolgreich geändert wurde.

## Deaktivieren eines Diagramms

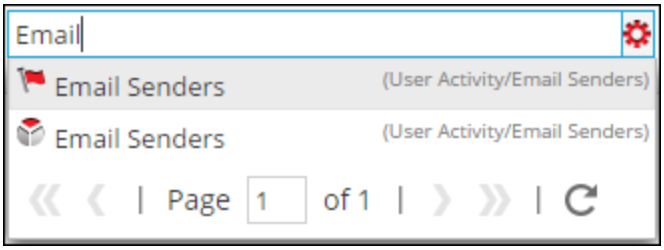
So deaktivieren Sie ein Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Wählen Sie im Bereich **Diagrammliste** ein Diagramm oder mehrere Diagramme aus, die in der Spalte **Aktiviert** mit ● gekennzeichnet sind.
4. Klicken Sie auf ○.
   In einer Meldung wird bestätigt, dass der Diagrammstatus erfolgreich geändert wurde.

## Ein bestehendes Diagramm suchen

So suchen Sie ein bestehendes Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Geben Sie in der Symbolleiste **Diagramm** im Textfeld „Suche“ einen Text ein.
4. Klicken Sie auf  > **Diagramm**.
   Die Diagramme, deren Namen die Teilzeichenfolge enthalten, werden in der Drop-down-Liste der Suche angezeigt.




## Aktualisieren eines Diagramms

So aktualisieren Sie ein Diagramm:

1. Wählen Sie **Monitor** > **Berichte** aus.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Diagramme**.
   Die Ansicht „Diagramm“ wird angezeigt.
3. Verschieben Sie die Diagramme im Bereich **Diagrammliste** per Drag-and-drop zu der gewünschten Gruppe im Bereich „Diagrammgruppen“.
   Die Diagramme werden zum neuen Standort verschoben.
4. Gehen Sie folgendermaßen vor:
   - Klicken Sie im Bereich **Diagrammliste** auf  .
   - Wählen Sie im Bereich **Symbolleiste Diagramme** die Option **Automatisch aktualisieren** aus.
     Die Diagrammliste wird aktualisiert.

# Übersicht über Warnmeldungen

Warnmeldungen können verwendet werden, um zeitnahe Einblicke in aktuelle Sicherheitsprobleme und Schwachstellen zu erzeugen. Wenn z. B. eine schädliche E-Mail von einem gefährdeten Konto gesendet wird, würden Sie eine Warnmeldung benötigen, die Sie beim Eintreten eines solchen Ereignisses automatisch benachrichtigt.

Die folgenden Warnmeldungskonzepte helfen Ihnen, Warnregeln, Bedingungen, Benachrichtigungen und Vorlagen besser zu verstehen.

## Warnmeldungsregeln

Warnmeldungsregeln geben die Logik für die Erzeugung von Warnmeldungen an. Mithilfe von Warnmeldungsregeln können Sie Schwellenwerte einrichten und definieren, wie Sie benachrichtigt werden möchten, wenn diese Grenzwerte überschritten werden. So können Sie beispielsweise eine Regel einrichten, um benachrichtigt zu werden, wenn die CPU-Auslastung 5 Minuten oder länger ungewöhnlich hoch bleibt.

## Warnmeldungsdefinitionen

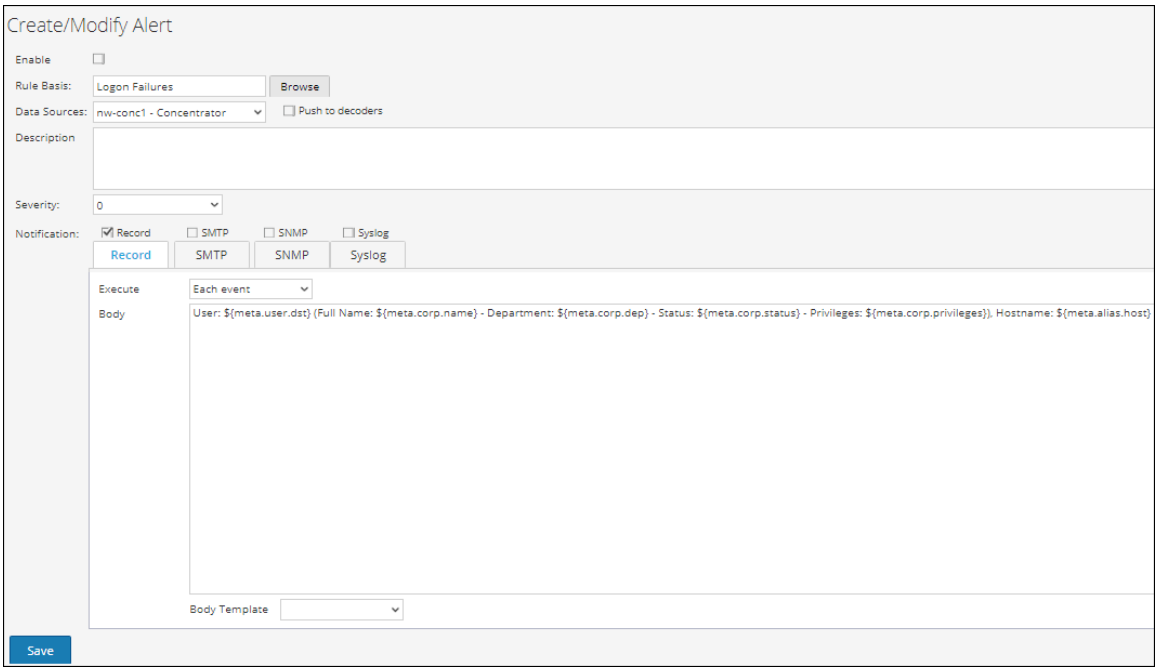
Die Warnmeldungsdefinition ähnelt dem Definieren von Regeln für Berichte. Diese Regeln müssen basierend auf Ihrem Anwendungsbeispiel definiert werden. Warnmeldungsdefinitionen werden durch die Auswahl von Warnregeln erstellt, die Sie in der Ansicht „Regel erstellen“ definieren. Beim Definieren einer Warnmeldung wählen Sie diese Regel aus.

**Hinweis:** Sie können Warnmeldungen nur mithilfe von Regeln ausgeben, die für die NetWitness-Datenquelle definiert sind.

Sobald eine Warnmeldung erstellt wurde, werden diese Daten von der Reporting Engine gesammelt und in der Benutzeroberfläche angezeigt.

Sobald eine Warnmeldung definiert wurde, können Sie die Warnmeldung so planen, dass sie jede Minute (Standardeinstellung) oder derzeit oder in der nahen Zukunft ausgeführt wird.

**Hinweis:** In der NetWitness-Benutzeroberfläche entsprechen das Datum und die Uhrzeit, wo immer sie angezeigt werden, immer dem vom Benutzer ausgewählten Zeitzonenprofil.




# Warnmeldungsbenachrichtigungen

Im Folgenden sind die Komponenten aufgeführt, die zum Konfigurieren von Warnmeldungsbenachrichtigungen erforderlich sind:

- Benachrichtigungsserver: Ein Benachrichtigungsserver wird verwendet, um Warnmeldungsbenachrichtigungen zu senden, z. B. ein SMTP-Mailserver. 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: Warnmeldungsausgaben, die in den Formaten E-Mail, SMTP, SNMP und Syslog erfolgen können.
- Vorlagen: das vordefinierte Format einer Warnmeldung.

Immer wenn die Regelbedingung erfüllt wird, werden Warnmeldungen basierend auf dem Schweregrad generiert und der Benutzer wird abhängig von der Benachrichtigungsmethode benachrichtigt, die für diese spezielle Warnmeldung festgelegt wurde. Im Folgenden sind die verschiedenen Benachrichtigungsmethoden aufgeführt:

- E-Mail/SMTP: Simple Mail Transfer Protocol (SMTP) sendet Warnmeldungs-E-Mails für die Systemaktivität. E-Mail-Warnmeldungen können durch Auswählen von SMTP als Benachrichtigungstyp an ihre gewünschten Empfänger gesendet werden.

- SNMP: Simple Network Management Protocol (SNMP) sendet Warnmeldungen an mehrere Computer für SNMP-Traps. SNMP-Warnmeldungen können durch Auswählen von SNMP als Benachrichtigungstyp an andere Computer gesendet werden.
- Syslog: Syslog-Warnmeldungen erzeugen Benachrichtigungen aus Syslog-Meldungen. Syslog-Warnmeldungen können durch Auswählen von Syslog als Benachrichtigungstyp gesendet werden.

Warnmeldungen können so konfiguriert werden, dass Warnungen bei Ereignissen gesendet werden, die Aufmerksamkeit erfordern, oder als Mechanismen zur Durchführung automatisierter Aktionen basierend auf in einer Warnmeldung konfigurierten Bedingungen. Wenn Bedingungen innerhalb der Entität die Kriterien erfüllt haben, die für die Warnmeldung ausgewählt wurden, wird eine Warnmeldung gesendet. Die Benachrichtigungskriterien bestimmen, wann und wie oft die Warnmeldung erzeugt wird.

## Warnmeldungsvorlagen

Warnmeldungsvorlagen sind ein vordefiniertes Format für eine Warnmeldung. Sie können diese Vorlagen verwenden, um Warnmeldungen zu erstellen.

## Zugriffskontrolle für Warnmeldungen

Je nach Benutzerrolle erhält der Benutzer einen bestimmten Satz von Zugriffsberechtigungen, um eine Warnmeldung zu managen. Der Administrator managt die Zugriffsrechte, die jeder Benutzerrolle bereitgestellt werden, auf der Registerkarte **Administration > Sicherheit > Rollen**. Sie können Zugriffsberechtigungen für die Benutzerrollen festlegen, um eine Warnmeldung zu managen. Das Modul „Reporting“ stellt Zugriffskontrolle auf dem Level der Warnmeldung bereit.

**Hinweis:** Reporting Engine-Warnmeldungsberechtigungen tragen das Präfix „RE“, um sie von ESA (Event Streaming Analysis) unterscheiden zu können.

Wenn Sie Benutzer und Benutzerrollen erstellen, stellen Sie sicher, dass die von Ihnen für bestimmte Aufgaben erstellten Rollen Zugriff auf alle erforderlichen Berechtigungen haben. Dies könnte Berechtigungen auf verschiedenen Levels der Rollenhierarchie erfordern.

Warnmeldungen können mit einem spezifischen Satz von Benutzerrollen kombiniert werden, sodass ein Benutzer, wenn er sich bei NetWitness einloggt, nur auf die Warnmeldungen Zugriff hat, zu deren Rolle der Benutzer gehört. Benutzer, die zu einer Benutzerrolle mit der Zugriffsberechtigung **Lesen & Schreiben** gehören, können Warnmeldungen definieren. Der Zugriff kann weiter eingeschränkt werden, sodass nur die Benutzer mit der Berechtigung **Schreibgeschützt** Zugriff auf Warnmeldungen haben.

Auf dem Level der Warnmeldungen können Sie die folgenden Zugriffsberechtigungen für die Benutzerrollen in NetWitness angeben:

- Lesen & Schreiben
- Schreibgeschützt
- Kein Zugriff

**Hinweis:** Vor dem Anwenden von Warnmeldungsberechtigungen lautet der standardmäßige Zugriffsstatus für alle Benutzerrollen **Kein Zugriff** und das Kontrollkästchen ist nicht aktiviert.

Wenn Sie die Zugriffsberechtigung für eine bestimmte Benutzerrolle ändern möchten, müssen Sie diese auf dem Level der Warnmeldungen festlegen. Der Standardberechtigungssatz für alle Benutzerrollen außer Administratoren lautet **Kein Zugriff**.

Die beiden Szenarien werden kurz erläutert:

- Szenario 1: Berechtigungen werden basierend auf der Benutzerrolle auf Warnmeldungen/Regeln angewendet.
- Szenario 2: Leseberechtigung wird auf Regeln in der Warnmeldung angewendet.

| | **Rolle (Analysten)** | **Auf Warnmeldungen/Regeln angewandte Berechtigungen auf Basis der Benutzerrolle** | **Auf Regeln in der Warnmeldung angewandte Berechtigung (Schreibgeschützt)** |
|---|---|---|---|
| **Warnmeldung** | **Lesen & Schreiben** | **Lesen & Schreiben** | **Lesen & Schreiben** |
| **Regeln** | **Lesen** | **Lesen** | **Lesen** |

Der Warnmeldung wird die Rolle eines Security Analyst zugewiesen und die Berechtigungen werden auf **Lesen & Schreiben-Warnmeldungen** eingestellt.

In Szenario 1 verfügt jedes der Level über einen Berechtigungssatz auf Basis der Benutzerrolle. In Szenario 2 wird die Berechtigung **Lesen** für die Regeln festgelegt. Hierbei gilt, dass die für die Regeln festgelegte Berechtigung keine höhere Stufe als die für die Warnmeldungen haben darf.

Wenn die Berechtigung für die Regeln eine höhere Stufe als die für die Warnmeldungen hat, wird sie nicht angewendet. Wenn Sie zum Beispiel die Berechtigung für Warnmeldungen auf **Kein Zugriff** festlegen und dann die Option *Leseberechtigung auf Regeln in Berichten anwenden* angeben, wird die Leseberechtigung für die Regeln nicht festgelegt.

## Zugriffskontrolle einer Warnmeldung bei der Auswahl von Mehrfachwarnmeldungen

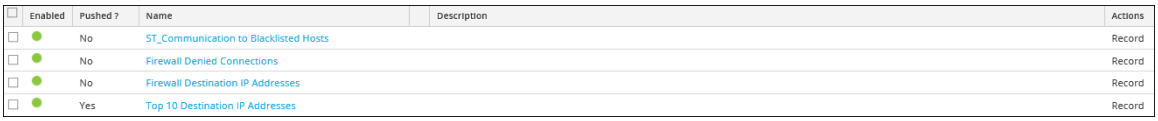
Wenn Sie die Zugriffsberechtigungen von Mehrfachwarnmeldungen ändern wollen, wählen Sie mehrere Warnmeldungen aus und legen Sie deren Zugriffsberechtigungen fest, indem Sie den Bereich „Warnmeldungsberechtigungen“ verwenden. Die von Ihnen ausgewählte Zugriffsberechtigung wird auf alle ausgewählten Warnmeldungen angewendet.

## Melden Sie sich als ein bestimmter Benutzer an und zeigen Sie die Zugriffsdetails an

Wenn Sie sich in der Benutzeroberfläche von NetWitness als ein Benutzer mit Zugriffsberechtigung **Lesen** einloggen, werden alle Warnmeldungen mit dem Symbol (📖) versehen. Wenn Sie anschließend auf das Symbol klicken, wird das Callout 'Schreibgeschützt' im Bereich „Warnmeldungsliste“ angezeigt.

Wenn Sie sich in der Benutzeroberfläche von NetWitness als ein Benutzer ohne Berechtigung **Lesen & Schreiben** für eine Warnmeldung anmelden, werden alle Warnmeldungen mit dem Symbol ( 👁 ) versehen und im Bereich „Warnmeldungsliste“ markiert angezeigt.

Die nachfolgenden Abbildungen zeigen den Bereich „Warnmeldungsliste“ bei einer Anmeldung mit einer minimalen Zugriffsberechtigung **Lesen & Schreiben**.



| Enabled | Pushed ? | Name | Description | Actions |
|---|---|---|---|---|
| | No | ST_Communication to Blacklisted Hosts | | Record |
| | No | Firewall Denied Connections | | Record |
| | No | Firewall Destination IP Addresses | | Record |
| | Yes | Top 10 Destination IP Addresses | | Record |

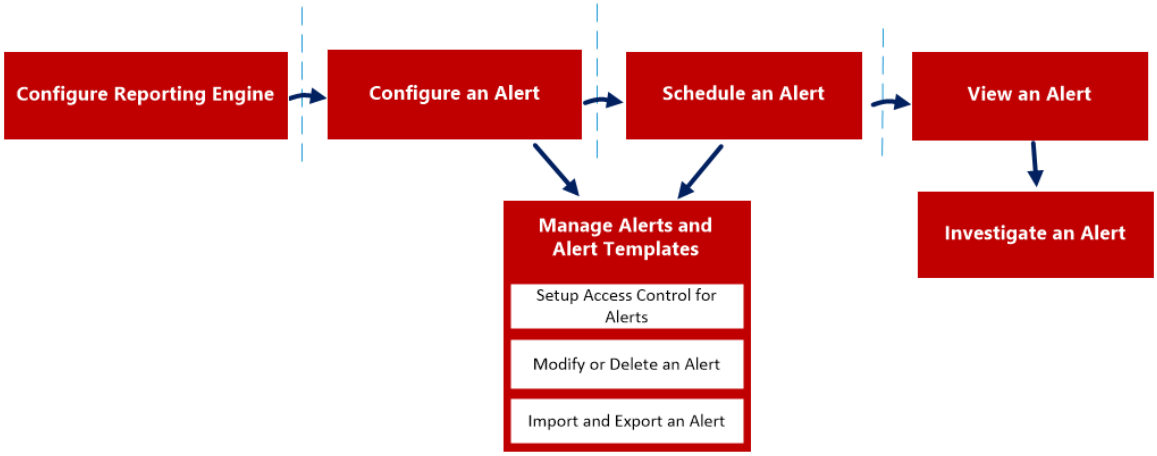
**Hinweis:** Wenn ein Benutzer (der nicht ADMIN ist) eine Warnmeldung erstellt, kann ADMIN auf diese Warnmeldung nicht zugreifen.

In der nachfolgenden Tabelle werden die verschiedenen Spalten im Bereich „Warnmeldungsberechtigungen“ aufgelistet:

| Spalte | Beschreibung |
|---|---|
| Rollen | Die Rolle des an der NetWitness-Benutzeroberfläche angemeldeten Benutzers. |
| Lesen & Schreiben | Der Benutzer kann auf der Seite „Warnmeldungen“ auf die Warnmeldung zugreifen, sie anzeigen, bearbeiten, importieren, exportieren und löschen. Außerdem kann der Benutzer die Berechtigung für die Warnmeldung ändern. |
| Schreibgeschützt | Der Benutzer kann auf die Warnmeldung auf der Seite der Warnmeldungen ausschließlich zugreifen und diese ansehen. |

| Spalte | Beschreibung |
| --- | --- |
| Kein Zugriff | Der Benutzer kann mit dieser Berechtigung weder auf die Warnmeldung zugreifen noch diese ansehen. |
| Nur-Lesen-Berechtigungen auf Regeln in den Warnmeldungen anwenden | Der Benutzer kann Berechtigungen automatisch auf die Regeln in den Warnmeldungen anwenden. |

Es folgt eine Übersicht über den gesamten Prozess der Warnmeldungen:




Führen Sie zum Konfigurieren und Erzeugen einer Warnmeldung in Reporting Engine die folgenden Aufgaben durch:

1. Konfigurieren der Reporting Engine
2. Konfigurieren einer Warnmeldung
3. Planen einer Warnmeldung
4. Anzeigen einer Warnmeldung
5. Ermitteln einer Warnmeldung
6. Managen einer Warnmeldung und Warnmeldungsvorlage

# Konfigurieren der Reporting Engine

Stellen Sie Folgendes sicher:

- Bevor Sie eine Warnmeldungsregel erstellen, haben Sie Decoder mit dem Concentrator verbunden, der zur Reporting Engine für die ausgewählte Datenquelle hinzugefügt wurde.
- Sie haben einen Syslog-Server installiert und konfiguriert, der TCP/TLS in Ihrer Umgebung unterstützt. zum Beispiel WinSyslog. Sie können die Reporting Engine so konfigurieren, dass bei Auslösen einer Warnmeldung Syslog-Meldungen über TCP mit Transport Layer Security (TLS) gesendet werden.

So konfigurieren Sie die Reporting Engine zum Senden von Syslog-Warnmeldungen über TCP mit Transport Layer Security (TLS):

1. Rufen Sie die erforderlichen Zertifikate ab.
2. Fügen Sie das CA-Zertifikat an die Datei „ca.pem“ auf dem NetWitness-Server an.
3. Konfigurieren Sie den Syslog-Server so, dass Nachrichten von Client-Rechnern akzeptiert werden.
4. Konfigurieren Sie die Zustellung von Nachrichten in der NetWitness-Benutzeroberfläche.

## Aufgabe 1: Abrufen der erforderlichen Zertifikate

So erzeugen Sie Zertifikate, mit denen die Reporting Engine zum Senden von Syslog-Meldungen über TCP mit TLS konfiguriert wird:

1. Erzeugen Sie ein CA-Zertifikat (Certifying Authority, Zertifizierungsstelle). Weitere Informationen erhalten Sie unter http://www.rsyslog.com/doc/tls_cert_ca.html.

**Hinweis:** Sie können diesen Schritt ignorieren, wenn bereits ein CA-Zertifikat in Ihrer Umgebung ausgeführt wird.

2. Erzeugen Sie ein Schlüsselpaar für den Syslog-Server. Weitere Informationen erhalten Sie unter http://www.rsyslog.com/doc/tls_cert_machine.html.

**Hinweis:** Sie können diesen Schritt ignorieren, wenn Sie die Sicherheit für den Syslog-Server mithilfe des Schlüssels und der von derselben Zertifizierungsstelle erzeugten Zertifikate bereits konfiguriert haben.

## Aufgabe 2: Fügen Sie das CA-Zertifikat an die Datei „ca.pem“ auf dem NetWitness-Server an.

So hängen Sie ein vorhandenes CA-Zertifikat an die Datei „ca.pem“ an:

1. Hängen Sie den Inhalt des CA-Zertifikats, das Sie erzeugt haben, manuell an die Datei **/etc/pki/CA/certs/ca.pem** an.
2. Führen Sie auf dem NetWitness-Server den folgenden Befehl aus, damit das Zertifikat im Truststore aufgefüllt wird:
   `keytool -import -file /etc/pki/CA/certs/ca.pem -keystore cacerts`

## Aufgabe 3: Konfigurieren Sie den Syslog-Server so, dass Nachrichten von Client-Rechnern akzeptiert werden.

Konfigurieren Sie den Syslog-Server so, dass Nachrichten von Client-Rechnern akzeptiert werden, welche die gleichen CA-Zertifikate besitzen:

1. Kopieren Sie die folgenden Dateien an Ihren sicheren TCP-Server-Zielspeicherort:
   - ca_cert.pem
   - server_cert.pem
   - server_key.pem

   Wobei Folgendes gilt:

   *ca_cert.pem* ist das CA-Zertifikat

   *server_cert.pem* - ist das Serverzertifikat

   *server_key.pem* - ist der Serverschlüssel

   Weitere Informationen finden Sie in Ihrer Dokumentation zu Ihrem Syslog-Server. Wenn Sie rsyslog verwenden, finden Sie unter http://www.rsyslog.com/doc/tls_cert_server.html weitere Informationen.

## Aufgabe 4: Konfigurieren der Zustellung von Warnmeldungen in NetWitness

Konfigurieren Sie Reporting Engine, um bei Auslösen einer Warnmeldung Syslog-Meldungen über TCP mit Transport Layer Security (TLS) zu senden. Aktivieren Sie hierzu **SECURE_TCP** auf der Registerkarte **Ausgabeaktionen** für den Reporting Engine-Service in der Ansicht „Service-Konfiguration“ der Reporting Engine. Informationen finden Sie im Thema **Reporting Engine-Ausgabeaktionen** im *Leitfaden zur Host- und Servicekonfiguration*.

# Konfigurieren einer Warnmeldung

Sie können eine Warnmeldung konfigurieren, indem Sie Warnbenachrichtigungen einrichten und eine Benachrichtigungsmethode zu einer Regel hinzufügen.

**Hinweis:** Nur Administratoren können diese Benachrichtigungen einrichten.

So konfigurieren Sie eine Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie in der Symbolleiste **Warmeldung** auf  .
   Der Bereich „Warnmeldung erstellen/ändern“ wird angezeigt.
4. Klicken Sie auf **Aktivieren**, um die Warnmeldung zu aktivieren.
5. Führen Sie im Feld **Regelbasis** folgende Schritte aus:
   a. Klicken Sie auf **Durchsuchen**.
      Das Dialogfeld „Regelbasis suchen“ wird angezeigt.
   b. Navigieren Sie in der Regelstruktur und wählen Sie eine Regel aus.
   c. Klicken Sie auf **OK**.
      Der Name der Regel wird im Feld „Regelbasis“ angezeigt.
6. Wählen Sie in der Drop-down-Liste **Datenquellen** eine Datenquelle aus.

   **Hinweis:** Wenn die Datenquelle nicht aufgelistet ist, stellen Sie sicher, dass Sie die Berechtigung **Lesen** für die Datenquelle festgelegt haben. Dies gilt nur für NWDB- und Warehouse Connector-Datenquellen. Weitere Informationen finden Sie unter **Konfigurieren von Datenquellenberechtigungen** im *Leitfaden zur Host- und Servicekonfiguration.*
7. Aktivieren Sie das Kontrollkästchen **Per Push an die Decoder übertragen**, damit die Reporting Engine die Regel an den Decoder sendet.
8. (Optional) Geben Sie im Feld **Beschreibung** eine Beschreibung der Warnmeldung ein.
9. Wählen Sie in der Drop-down-Liste **Schweregrad** den Schweregrad aus.
10. Führen Sie im Feld **Benachrichtigung** folgende Schritte aus:
    a. Wählen Sie die entsprechende Benachrichtigung aus.
       Die Registerkarte für die ausgewählte Benachrichtigung wird im Dialogfeld

„Warnmeldung erstellen/ändern“ angezeigt.

b. (Optional) Deaktivieren Sie die Benachrichtigung, um die Registerkarte für die Benachrichtigung zu deaktivieren.

c. Definieren Sie eine Aktion auf einer der Registerkarten **Benachrichtigung**:

   i. Führen Sie im Feld **Datensatz** folgende Schritte aus:

      a. Wählen Sie in der Drop-down-Liste **Ausführen** aus, wie oft eine Warnmeldung aufgezeichnet werden soll.

      b. Geben Sie die Aufzeichnungsmeldung ein. Sie können eine neue Meldung erstellen oder eine Vorlage im Feld **Textkörpervorlage** auswählen und die Vorlage hier ändern.

      c. (Optional) Wenn Vorlagen definiert wurden, wählen Sie eine Vorlage für die Aufzeichnungsmeldung aus, die Sie unbearbeitet verwenden oder ändern können.

   ii. Führen Sie im Feld **SMTP** folgende Schritte aus:

      a. Wählen Sie in der Drop-down-Liste **Ausführen** einen Wert aus, der angibt, wie oft E-Mail-Nachrichten für die Warnmeldung gesendet werden sollen.

      b. Geben Sie eine E-Mail-Adresse oder eine durch Kommas getrennte Liste von E-Mail-Adressen ein, an die diese Warnmeldung gesendet werden soll.

      c. Geben Sie den Betreff der E-Mail-Nachricht ein.

      d. Geben Sie den Nachrichtentext ein. Sie können eine neue Meldung erstellen oder eine Vorlage im Feld **Textkörpervorlage** auswählen und die Vorlage hier ändern.

   iii. Führen Sie im Registerkartenfeld **SNMP** folgende Schritte aus:

      a. Wählen Sie in der Drop-down-Liste **Ausführen** einen Wert aus, der angibt, wie oft SNMP-Meldungen für die Warnmeldung gesendet werden sollen.

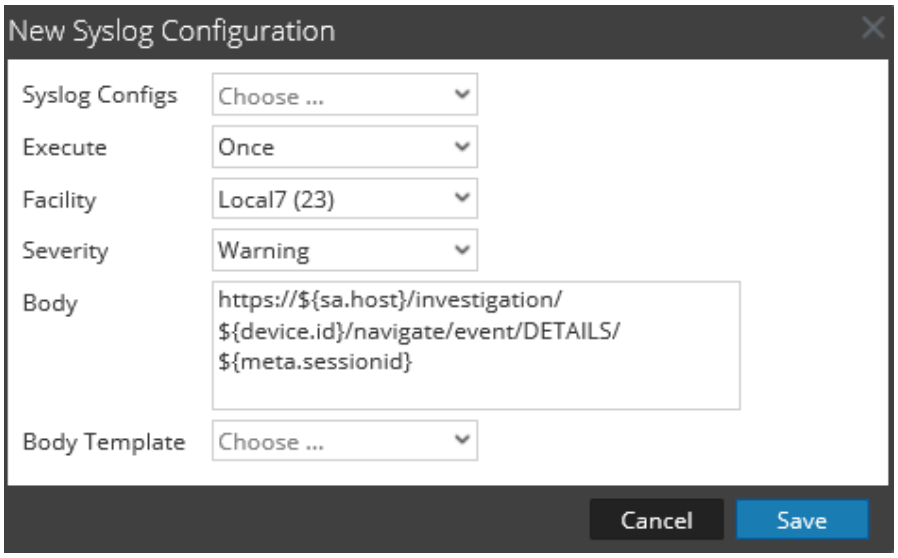
      b. Geben Sie die SNMP-Meldung ein. Sie können eine neue Meldung erstellen oder eine Vorlage im Feld **Textkörpervorlage** auswählen und die Vorlage hier ändern.

   iv. Führen Sie im Registerkartenfeld **Syslog** folgende Schritte aus:

> **Hinweis:** Sie können im Bereich „Syslog-Konfiguration“ mehrere Syslog-Server konfigurieren. Weitere Informationen finden Sie im Thema **Reporting Engine-Ausgabeaktionen** im *Leitfaden zur Host- und Servicekonfiguration.*

a. Klicken Sie auf +.

Das Dialogfeld „Neue Syslog-Konfiguration“ wird angezeigt.




b. Wählen Sie in der Drop-down-Liste **Syslog-Konfigurationen** einen Wert für die Syslog-Konfiguration aus.

c. Wählen Sie in der Drop-down-Liste **Ausführen** einen Wert aus, der angibt, wie oft Syslog-Meldungen für die Warnmeldung gesendet werden sollen.

d. Wählen Sie in der Drop-down-Liste **Komponente** die Komponente aus.

e. Wählen Sie in der Drop-down-Liste **Schweregrad** den Schweregrad aus.

f. Geben Sie die Syslog-Meldung ein. Sie können eine neue Meldung erstellen oder eine Vorlage im Feld **Textkörpervorlage** auswählen und die Vorlage hier ändern.

**Hinweis:** Um einen Metadatenschlüssel hinzuzufügen, geben Sie diesen im folgenden Format an: ${meta.metakey}. Beispiel: ${meta.ip.dst}.

g. Klicken Sie auf **Speichern**.

Die Syslog-Konfiguration wird der Warnmeldung hinzugefügt.

11. Klicken Sie auf **Erstellen**.

NetWitness erstellt eine Warnmeldung und gibt in einer Bestätigungsmeldung an, dass die Warnmeldung erfolgreich gespeichert wurde. NetWitness generiert die Warnmeldung und führt die Ausgabeaktionen jede Minute durch.

# Planen einer Warnmeldung

Sie müssen eine Warnmeldung planen, um in regelmäßigen Abständen Ereignisse zu suchen.

Sp planen Sie eine Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen.
2. Klicken Sie auf **Warnmeldungen**, um die Warnmeldungsansicht anzuzeigen.
3. Wählen Sie eine Warnmeldung aus, die geplant werden soll.
4. Klicken Sie auf der Symbolleiste **Warnmeldung** auf **Aktivieren**.
   Die ausgewählte Warnmeldung wird geplant.

# Anzeigen einer Warnmeldung

Sie können eine Warnmeldung oder eine Liste aller Warnmeldungen anzeigen.

Sie können die ausgelösten Warnmeldungen anzeigen und alle Warnmeldungen im Modul „Investigation“ untersuchen und diese Ansichten so anpassen, dass Warnmeldungen für einen bestimmten Zeitraum angezeigt werden, und die maximale Anzahl der Warnmeldungen festlegen, die auf einer Seite angezeigt werden.

So zeigen Sie eine Warnmeldung an:

1. Wählen Sie **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen.
2. Klicken Sie auf **Warnmeldungen**, um die Warnmeldungsansicht anzuzeigen.
3. Klicken Sie in der Symbolleiste **Warnmeldung** auf **Warnmeldungen anzeigen**.
   Die Ansicht „Warnmeldungen anzeigen“ wird angezeigt.

# Ermitteln einer Warnmeldung

Sie können jede Warnmeldung untersuchen, die in der Warnmeldungsansicht ausgelöst wird. Für eine detailliertere Untersuchung einer bestimmten Warnmeldung können Sie die Warnmeldung im Modul „Investigation“ anzeigen.

So untersuchen Sie eine Warnmeldung:

1. Klicken Sie in der Symbolleiste des Abschnitts **Warnmeldung** auf **Warnmeldungen anzeigen**, um zur Ansicht „Warnmeldungen anzeigen“ zu navigieren.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf die Schaltfläche  neben der Warnmeldung, die Sie untersuchen möchten.
     Im Modul Investigation werden die Details der ersten Sitzung, für die eine Entsprechung gefunden wurde, zur sofortigen Analyse angezeigt.
   - Klicken Sie auf den Namen der Warnmeldung, die Sie untersuchen möchten.
     Im Modul Investigation werden alle Entsprechungen für die betreffende Warnmeldung angezeigt, die in der Stunde um die registrierte Warnmeldung aufgetreten sind.

# Managen einer Warnmeldung und Warnmeldungsvorlage

Sie können Warnmeldungen, geplante Warnmeldungen und Warnmeldungsvorlagen anhand der folgenden Verfahren managen.

## Managen einer Warnmeldung

Abhängig von den Zugriffsberechtigungen für die Benutzerrolle können Sie Warnmeldungen ändern oder löschen, importieren und exportieren, aktivieren oder deaktivieren und eine Liste der Warnmeldungen anzeigen oder aktualisieren.

### Zugriffskontrolle für eine Warnmeldung, wenn eine einzelne Warnmeldung ausgewählt ist

So legen Sie Zugriffsberechtigungen für eine Warnmeldung fest:

1. Wählen Sie **Monitor> Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Wählen Sie im Bereich Warnmeldungsliste eine Warnmeldung aus.
4. Klicken Sie auf > **Berechtigungen**.
   Das Dialogfeld „Warnmeldungsberechtigungen“ wird angezeigt.
5. Wählen Sie aufgrund der Benutzerrolle die entsprechenden Optionen aus.
6. (Optional) Aktivieren Sie das Kontrollkästchen, wenn Sie abhängigen Regeln automatisch Lesezugriff gewähren möchten.

**Hinweis:** Wenn das Kontrollkästchen aktiviert ist, erhalten alle abhängigen Regeln ohne Zugriffsberechtigung die Zugriffsberechtigung LESEN.

7. Klicken Sie auf **Speichern**.
   In einer Meldung wird bestätigt, dass die Berechtigung für die ausgewählte Warnmeldung erfolgreich festgelegt wurde.

### Zugriffskontrolle einer Warnmeldung bei der Auswahl von Mehrfachwarnmeldungen

So ändern Sie Berechtigungen für mehrere Warnmeldungen:

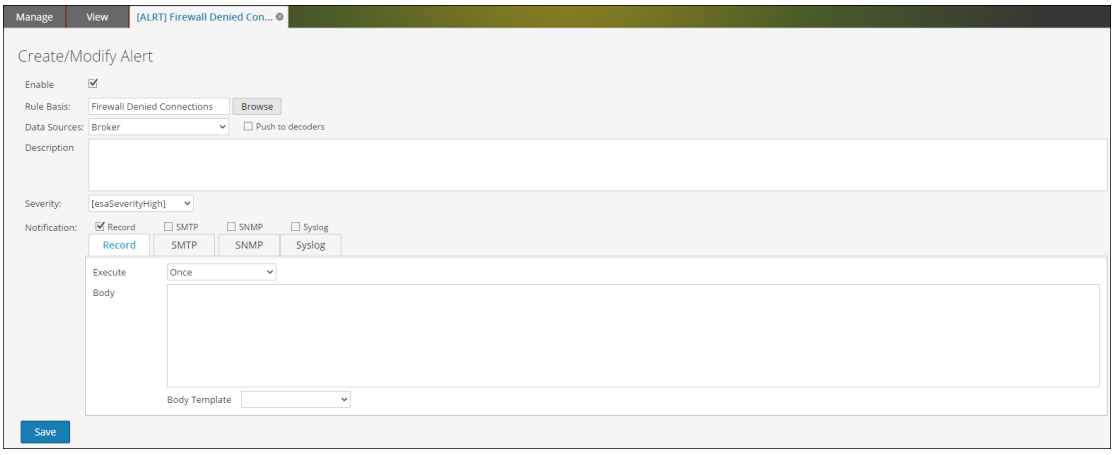
1. Wählen Sie im Bereich „Warnmeldungsliste“ alle Warnmeldungen aus, deren Berechtigungen festgelegt werden müssen.
2. Klicken Sie auf > **Berechtigungen**.
   Das Dialogfeld „Warnmeldungsberechtigungen“ wird angezeigt.
3. Wählen Sie die Berechtigung aus, die für die jeweilige Benutzerrolle festgelegt werden soll.
4. Klicken Sie auf **Speichern**.
   In einer Meldung wird bestätigt, dass die Berechtigung für alle ausgewählten Warnmeldungen erfolgreich festgelegt wurde.

## Bearbeiten einer Warnmeldung

Wenn Sie z. B. per E-Mail unter einer anderen E-Mail-ID über die Warnmeldung informiert werden möchten, müssen Sie den Bereich „Warnmeldungsbenachrichtigung“ mit den Details der neuen E-Mail-ID ändern, um über eine E-Mail benachrichtigt zu werden, wenn eine Warnmeldung erzeugt wird. Darüber hinaus können Sie auch die Beschreibung der Warnmeldung und die Warnmeldungsbenachrichtigung im Bereich „Warnmeldung erstellen oder ändern“ ändern.

So bearbeiten Sie eine Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Wählen Sie im Bereich **Warnmeldungsliste** eine Warnmeldung aus und klicken Sie auf .
   Die Registerkarte „Warnmeldung erstellen/ändern“ wird angezeigt.




4. Navigieren Sie im Feld **Regelbasis** durch die Regelbaumstruktur und wählen Sie eine andere Regel aus.
   Der Name der Regel wird im Feld „Regelbasis“ angezeigt.

5. (Optional) Wählen Sie die Datenquelle aus der Drop-down-Liste **Datenquellen** aus.

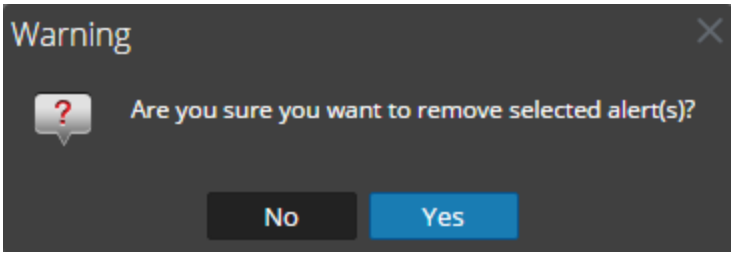
   **Hinweis:** Wenn die Datenquelle nicht aufgelistet ist, stellen Sie sicher, dass Sie die **Leseberechtigung** für die Datenquelle haben. Dies gilt nur für NWDB- und Warehouse-Datenquellen. Weitere Informationen finden Sie unter **Konfigurieren von Datenquellenberechtigungen** im *Leitfaden zur Host- und Servicekonfiguration*.

6. (Optional) Ändern Sie die Warnmeldungsbeschreibung im Feld **Beschreibung**.
7. Ändern Sie die entsprechenden Registerkarten **Benachrichtigung** – **Datensatz**, **SMTP**, **SNMP**, und **Syslog**.
8. Klicken Sie auf **Speichern**.
   In einer Meldung wird bestätigt, dass die Warnmeldung erfolgreich geändert wurde.

## Löschen einer Warnmeldung

So löschen Sie eine Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Wählen Sie im Bereich **Warnmeldungsliste** die Warnmeldung aus und klicken Sie auf .
   Sie werden in einem Warndialogfeld aufgefordert zu bestätigen, dass Sie die ausgewählten Warnmeldungen entfernen möchten.




4. Klicken Sie auf **Ja**, um die Warnmeldung zu löschen.
   Über eine Meldung wird bestätigt, dass die Warnmeldung gelöscht wurde. Die ausgewählte Warnmeldung wird aus dem Bereich „Warnmeldungsliste“ gelöscht.

## Importieren einer Warnmeldung

So importieren Sie eine Warnmeldung aus anderen Instanzen von NetWitness in den Bereich „Warnmeldungsliste“:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie in der Symbolleiste **Warnmeldung** auf > **Importieren**.
   Das Dialogfeld „Warnmeldung importieren“ wird angezeigt.
4. Klicken Sie auf **Durchsuchen**, um die Binärdatei auszuwählen.
   NetWitness bietet eine Dateisystemansicht der Dateien. Sie können mehrere Warnmeldungen gleichzeitig importieren. Wenn Sie mehrere Warnmeldungen auswählen möchten, aktivieren Sie das Kontrollkästchen der Warnmeldung, die importiert werden soll.
5. Suchen Sie die Binärdatei und klicken Sie auf **Öffnen**.
   Die Datei wird der Liste „Warnmeldung importieren“ hinzugefügt.
6. (Optional) Aktivieren Sie das Kontrollkästchen „Warnmeldung“, wenn Sie vorhandene Warnmeldungen in der Bibliothek beim Import durch Warnmeldungen mit demselben Namen in der Binärdatei überschreiben möchten. Wenn Sie die Option „Überschreiben“ nicht auswählen und eine identische Warnmeldung in der Binärdatei gefunden wird, wird die Binärdatei importiert und keine Fehlermeldung wird angezeigt.
7. Klicken Sie auf **Importieren**, um die Binärdatei zu importieren.

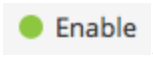
## Exportieren einer Warnmeldung

So exportieren Sie eine Warnmeldung in eine externe Datei, die später in NetWitness importiert werden kann:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Wählen Sie im Bereich **Warnmeldungsliste** eine Warnmeldung aus und klicken Sie auf und führen Sie einen der folgenden Schritte aus:
   - **Exportieren**: Mit dieser Auswahl wird eine Warnmeldung in eine ZIP-Datei exportiert.
   - **Als Text exportieren**: Mit dieser Auswahl werden alle Inhalte aus der Reporting Engine in eine ZIP-Datei exportiert, welche die Daten im Textformat enthält.
     Sie können mehrere Warnmeldungen gleichzeitig exportieren. Wenn Sie mehrere Warnmeldungen auswählen möchten, aktivieren Sie das Kontrollkästchen der Warnmeldung, die exportiert werden soll.
4. Klicken Sie auf > **Exportieren**.
   Die exportierte Binärdatei wird auf dem lokalen Laufwerk gespeichert.

## Aktivieren einer Warnmeldung

So aktivieren Sie eine Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Wählen Sie im Bereich **Warnmeldungsliste** die Warnmeldung aus, bei der ○ in der Spalte **Aktiviert** angezeigt wird.
4. Klicken Sie auf 

.
   Eine Bestätigungsmeldung zeigt an, dass die Änderung an dem Warnmeldungsstatus erfolgreich war.

## Deaktivieren einer Warnmeldung

So deaktivieren Sie eine Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Wählen Sie im Bereich **Warnmeldungsliste** die Warnmeldung aus, bei der ● in der Spalte **Aktiviert** angezeigt wird.
4. Klicken Sie auf ○ Disable.
   Eine Bestätigungsmeldung gibt an, dass die Statusänderung der Warnmeldung(en) erfolgreich war.

## Anzeigen einer Liste der Warnmeldungen

So zeigen Sie eine Liste der Warnmeldungen an:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie in der Symbolleiste **Warnmeldung** auf **Warnmeldungen anzeigen**.
   Die Ansichtsregisterkarte „Warnmeldungen anzeigen“ wird angezeigt.
4. Wählen Sie aus der Drop-down-Liste den letzten Eintrag aus.

5. Navigieren Sie im Feld **Regelbasis** durch die Regelbaumstruktur und wählen Sie eine andere Regel aus.
   Die Warnmeldungsliste basierend auf dem gewählten Filterwert wird angezeigt.

## Aktualisieren einer Warnmeldungsliste

So aktualisieren Sie die Liste der Warnmeldungen:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie in der Symbolleiste „Warnmeldungen“ auf  , um die Warnmeldungsliste zu aktualisieren.
   Der Bereich „Warnmeldungsliste“ wird aktualisiert.

# Managen einer geplanten Warnmeldung

Sie können eine geplante Warnmeldung aktivieren oder deaktivieren und alle geplanten Warnmeldungen anzeigen.

## Aktivieren einer geplanten Warnmeldung

So aktivieren Sie eine geplante Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie auf 
   
   .
   Die Ansichtsregisterkarte „Warnmeldungsplanung anzeigen“ wird angezeigt.
4. Wählen Sie im Bereich **Liste Warnmeldungsplanung** die geplanten Warnmeldungen aus, die aktiviert werden sollen.
5. Klicken Sie auf  .
   In einer Meldung wird bestätigt, dass der Warnmeldungsstatus erfolgreich geändert wurde und dass die Warnmeldung nun im Bereich „Warnmeldungsliste“ verfügbar ist.

## Deaktivieren einer geplanten Warnmeldung

So deaktivieren Sie eine geplante Warnmeldung:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie auf 
   
   .
   Die Ansichtsregisterkarte „Warnmeldungsplanung anzeigen“ wird angezeigt.
4. Wählen Sie im Bereich **Liste Warnmeldungsplanung** die geplanten Warnmeldungen aus, die deaktiviert werden sollen.
5. Klicken Sie auf  .
   In einer Meldung wird bestätigt, dass der Warnmeldungsstatus erfolgreich geändert wurde und dass die Warnmeldung nun im Bereich „Warnmeldungsliste“ verfügbar ist.

## Anzeigen aller geplanten Warnmeldungen

So zeigen Sie alle geplanten Warnmeldungen an:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.

2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie in der Symbolleiste **Warnmeldung** auf **Planung anzeigen**.
   Die Ansicht „Warnmeldungsplanung anzeigen“ wird mit einer Liste aller geplanten Warnmeldungen angezeigt.

# Managen einer Warnmeldungsvorlage

Sie können eine Warnmeldungsvorlage ändern oder löschen und alle Warnmeldungsvorlagen anzeigen.

## Bearbeiten einer Warnmeldungsvorlage

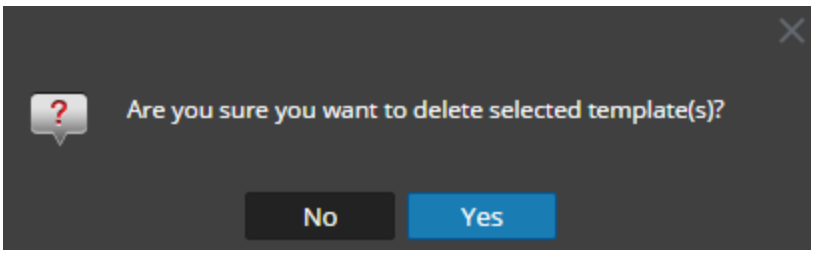
So bearbeiten Sie eine Warnmeldungsvorlage:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie auf Template.
   Die Ansicht „Vorlage“ wird angezeigt.
4. Wählen Sie im Bereich **Vorlagenliste** eine Vorlage aus und klicken Sie auf .
   Das Dialogfeld „Vorlage erstellen/ändern“ wird angezeigt.
5. Klicken Sie auf **Speichern**.
   Eine Bestätigungsmeldung, dass die Vorlage erfolgreich geändert wurde, wird angezeigt.

## Löschen einer Warnmeldungsvorlage

So löschen Sie eine Warnmeldungsvorlage:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie auf Template.
   Die Registerkarte der Ansicht „Vorlage“ wird angezeigt.
4. Wählen Sie im Bereich **Vorlagenliste** eine Vorlage aus und klicken Sie auf .
   Ein Bestätigungsdialogfeld wird angezeigt.



5. Klicken Sie auf **Ja**, um die Vorlage zu löschen.
   Eine Meldung mit der Bestätigung, dass die Vorlage erfolgreich gelöscht wurde, wird angezeigt.

## Anzeigen aller Warnmeldungsvorlagen

So zeigen Sie alle Nachrichten zu Warnmeldungsvorlagen an:

1. Wählen Sie **Monitor**> **Berichte**.
   Die Registerkarte „Managen“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.
   Die Warnmeldungsansicht wird angezeigt.
3. Klicken Sie in der Symbolleiste **Warnmeldung** auf **Vorlage**.
   Die Registerkarte mit der Vorlagenansicht wird angezeigt und enthält eine Liste der Vorlagen.

# Reporting-Referenzen

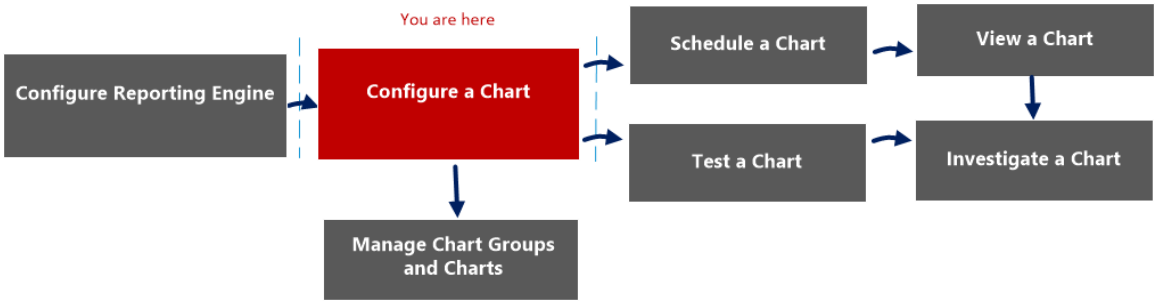
Dieser Abschnitt enthält Informationen über die Reporting-Benutzeroberfläche. Sie können Ihre Stelle im Workflow für das Erstellen und Erzeugen eines Berichts mit NetWitness Suite betrachten, einen kurzen Blick auf die wichtigen Funktionen werfen und Links zu den detaillierten Konzepten und Verfahren folgen.

## Ansicht Diagramm erstellen

In der Ansicht „Diagramm erstellen“ können Sie ein Diagramm definieren und testen. Sie können ein Diagramm erstellen, indem Sie ihm einen Namen zuweisen und dann eine Regel wählen.

**Hinweis:** Nur die Netwitness-DB-Regeln können in Diagrammen verwendet werden.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms* | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms | Managen einer Diagrammgruppe und eines Diagramms |

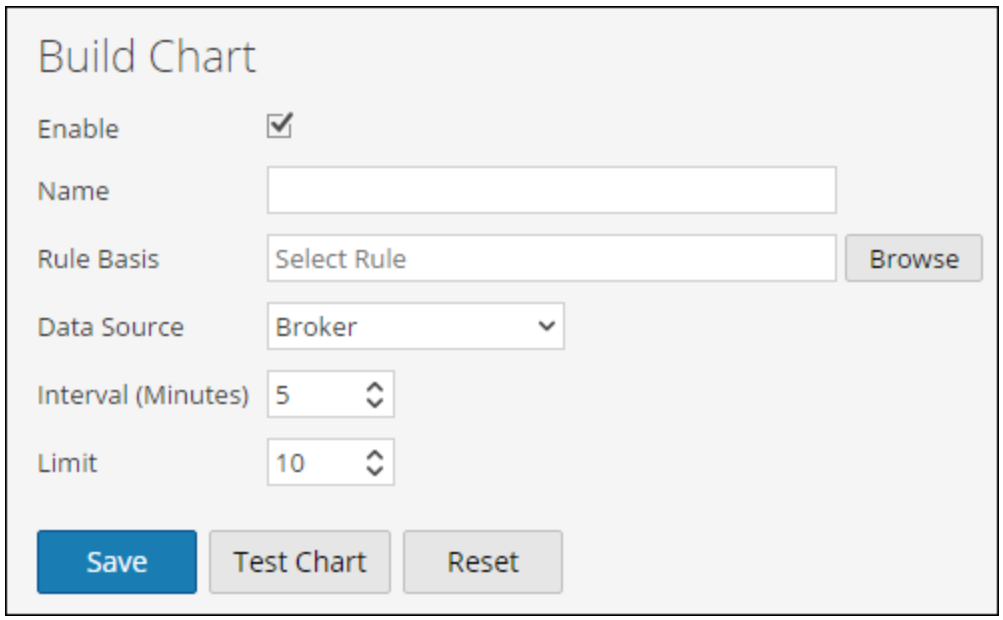
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms

## Schnellansicht

Die folgende Abbildung zeigt ein Beispiel für die Ansicht „Diagramm erstellen“.




In der folgenden Tabelle sind die Funktionen in der Ansicht „Diagramm erstellen“ beschrieben.

| Feld | Beschreibung |
|---|---|
| Aktivieren | Gibt an, ob Reporting Engine die Daten sammeln und die Diagrammergebnisse erzeugen soll. Wenn das Kontrollkästchen **Aktivieren** nicht aktiviert ist, werden die Ergebnisse nicht gerendert. |

| Feld | Beschreibung |
|---|---|
| Diagrammname | Identifiziert den Namen des Diagramms. |
| Regelbasis | Zeigt das Dialogfeld „Regeln hinzufügen“ an, aus dem Sie eine Regel als Grundlage für dieses Diagramm auswählen. Sie müssen eine Regel auswählen, die nicht nach „Keine“ sortiert ist. |
| Datenquelle | Wenn die Standarddatenquelle in Reporting Engine konfiguriert ist, wird die Datenquelle auf der Seite „Diagramm erstellen“ angezeigt. Wenn ein Diagramm für die Ausführung in einer anderen Datenquelle konfiguriert ist, wird diese Datenquelle auf der Seite „Diagramm erstellen“ anstelle der Standarddatenquelle angezeigt. Das Reporting-Modul funktioniert mit den folgenden Datenquellen:<br>• Broker<br>• Concentrator<br>• Decoder<br>• Log Decoder<br>• Log Collector |
| Intervall (Minuten) | Das Aktualisierungsintervall der Diagrammdaten in Minuten |
| Einschränkung | Die Anzahl der Datensätze, für die ein Diagramm erzeugt wird |
| Speichern | Speichert ein Diagramm in der Datenbank. |
| Diagramm testen | Zeichnet ein Testdiagramm basierend auf der Diagrammdefinition. |
| Zurücksetzen | Setzt die Diagrammdetails zurück. |

## Ansicht Liste aufbauen

In der Ansicht „Liste aufbauen“ können Sie Werte für eine Liste eingeben, speichern oder zurücksetzen. Sie können Listen verwenden, wenn Sie Reporting-Regeln schreiben, um den Prozess für das Angeben von Werten in der Regel zu vereinfachen.

# Workflow

Dieser Workflow zeigt das Verfahren zum Definieren von Listen oder Listengruppen. Sie können den Zugriff auf der Listen- oder Listengruppenebene festlegen, damit nur Benutzer mit bestimmten Rollen auf die Listen zugreifen können.

Sie müssen sicherstellen, dass Reporting Engine konfiguriert ist NetWitness Suite.


# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel* | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen von Berichten | Erstellen und Planen eines Berichts |

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

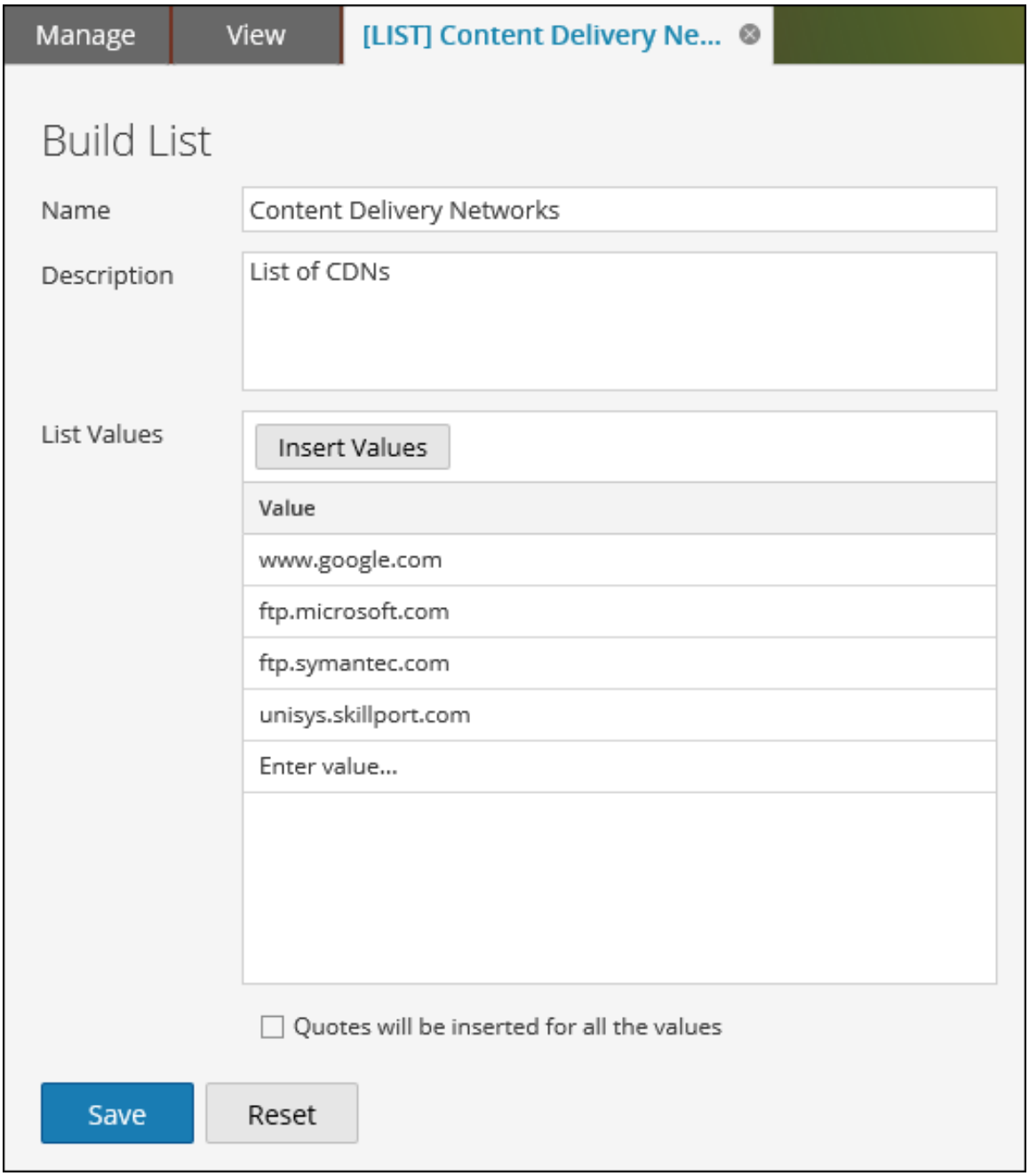
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren einer Regel
- Managen von Listen, Regeln oder Berichten
- Listenansicht
- Dialogfeld „Listenberechtigungen“

## Schnellansicht

Die folgende Abbildung zeigt die Ansicht „Liste aufbauen“.




So greifen Sie auf diese Ansicht zu

1. Wählen Sie **Monitor > Berichte**.

   Die Registerkarte Managen wird angezeigt.

2. Klicken Sie auf **Listen**.

   Die Listenansicht wird angezeigt.

3. Klicken Sie in der Symbolleiste **Liste** auf  .

   Die Registerkarte „Liste aufbauen“ wird angezeigt.

In der folgenden Tabelle sind die Funktionen in der Ansicht Liste aufbauen beschrieben.

| Funktion | Beschreibung |
|---|---|
| Name | Identifiziert und kennzeichnet die Liste. |
| Beschreibung | Liefert eine kurze Beschreibung der Liste. |
| Listenwerte | Das Raster mit Werten, die der ausgewählten Liste im Bereich Listenbibliothek zugeordnet sind. Sie können diese Werte aus einer Datei oder der Liste importieren. Sie können Werte auch manuell eingeben. |
| Anführungszeichen werden für alle Werte eingefügt. | Fügt für die Werte zur Laufzeit automatisch Anführungszeichen ein. Wenn das Kontrollkästchen nicht aktiviert ist und ein Wert in der Liste ein Komma enthält, muss dieser Wert in einfache Anführungszeichen eingeschlossen werden. Jeder Listenwert für eine IPDB-Regel muss in einfache Anführungszeichen eingeschlossen werden. Diese Syntax gilt nicht für die Listenwerte für NWDB-Regeln. |
| Speichern | Speichert die Regel, die verwendet werden kann, um einen Bericht, ein Diagramm oder einen Alarm zu erstellen. |
| Zurücksetzen | Mit dieser Option werden alle Informationen aus den Feldern gelöscht. |

## Ansicht Bericht erstellen

In der Ansicht „Bericht erstellen“ können Sie einen Bericht erstellen, Text und Regeln hinzufügen und den Bericht planen.

## Workflow

Dieser Workflow zeigt das Verfahren zum Erstellen und Planen von Berichten.


## Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts* | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

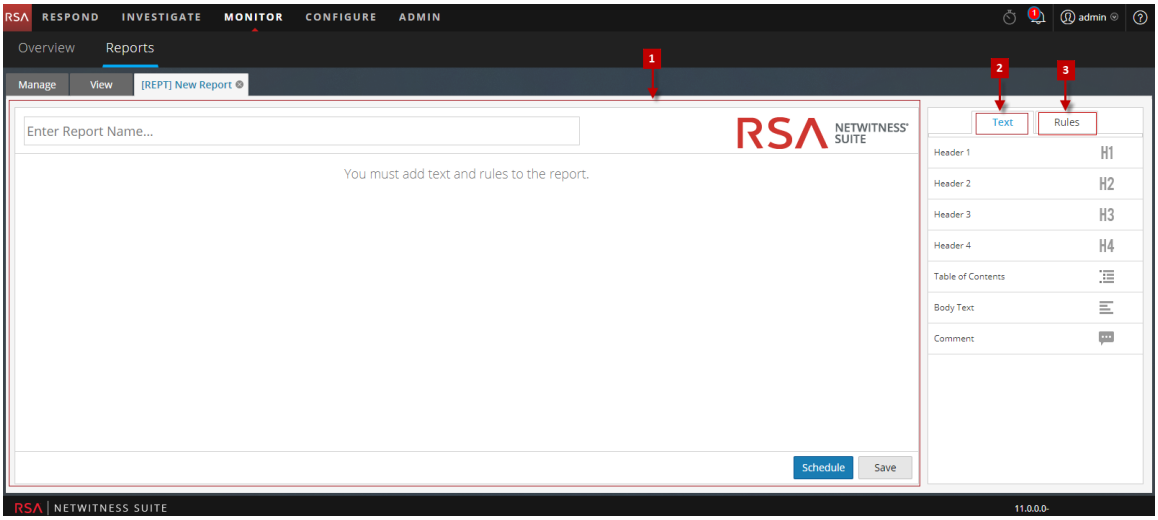
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht
- Ansicht Geplante Berichte
- Dialogfeld „Berichtberechtigungen“

## Schnellansicht

Die folgende Abbildung zeigt die Ansicht „Bericht erstellen“.




So greifen Sie auf diese Ansicht zu

1. Wählen Sie **Monitor > Berichte**.

   Die Registerkarte Managen wird angezeigt.

2. Klicken Sie auf **Berichte**.

   Die Ansicht „Berichte“ wird angezeigt.

3. Klicken Sie in der Symbolleiste **Bericht** auf + .

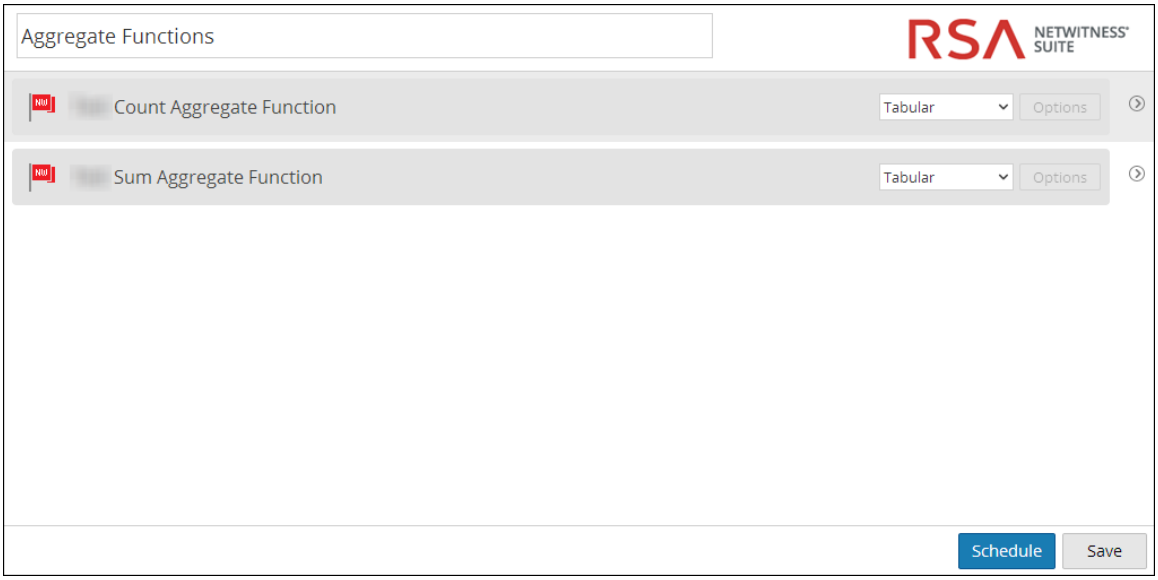
   Die Registerkarte „Bericht erstellen“ wird angezeigt.

Die Ansicht Bericht erstellen umfasst folgende Bereiche:

| | |
|---|---|
| 1 | Berichtsbereich |
| 2 | Textbereich |
| 3 | Regelbereich |

## Berichtsbereich

Im Berichtsbereich können Sie einen Bericht erstellen, indem Sie dem Bericht einen Namen zuweisen. Der Inhalt in einem Bericht hängt von den Elementen ab, die im Text- und Regelbereich ausgewählt wurden.




Wenn Sie einem Bericht Regeln hinzufügen, können Sie das Ausgabeformat dieser Regeln auf Tabelle, Bereich, Linie oder Kreis ändern, indem Sie auf die Schaltfläche ˅ klicken.

In der folgenden sind die Funktionen des Bereichs „Bericht“ mit einer Beschreibung aufgeführt.

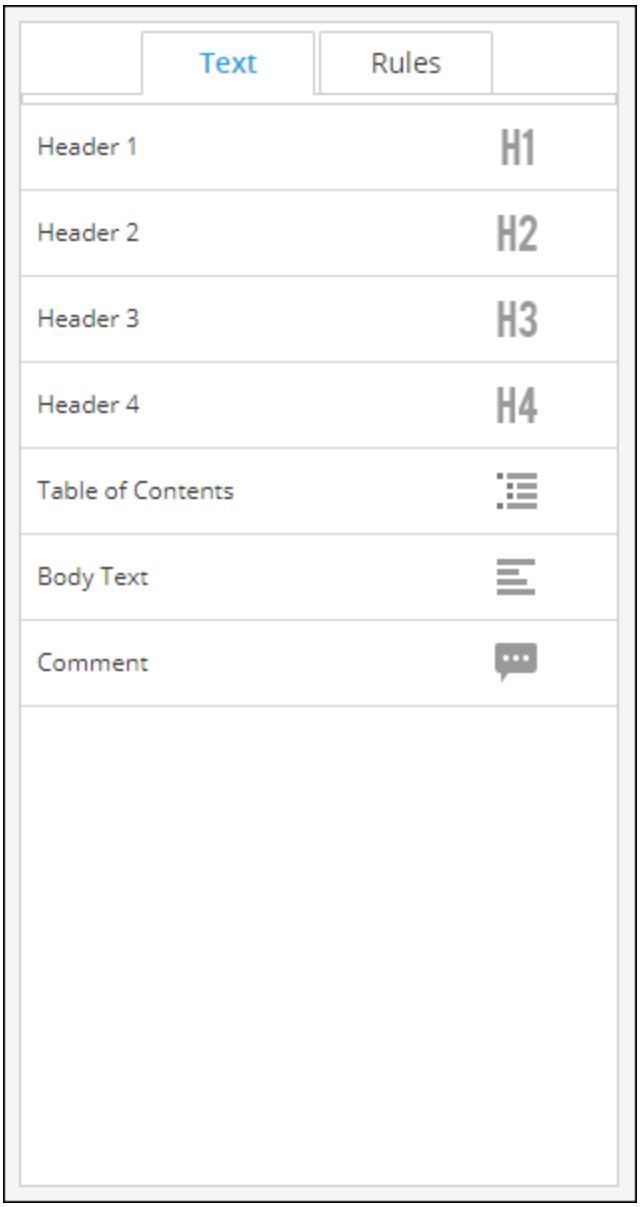
| Funktion | Beschreibung |
|---|---|
| Name | In diesem Feld können Sie den Namen des Berichts eingeben. |

| Funktion | Beschreibung |
|---|---|
| Optionen | In diesem Feld können Sie das Ausgabeformat des Berichts wählen, wie Tabellarisch, Bereich, Balken, Blase, Spalte, Linie, Kreis, Schrittlinie, Schrittbereich, Spline-Bereich und Spline. |
| Schedule | Durch Klicken auf diese Option wird der Bericht erzeugt. |
| Speichern | Durch Klicken auf diese Option wird der Bericht gespeichert. |

## Textbereich

Der Textbereich besteht aus einer Liste der Textelemente, die zur Gestaltung des Berichts beitragen. Mit diesen Textelementen können Sie den Bericht formatieren.

- Um Berichte besser zu strukturieren, können Sie mit Hilfe der Überschriften, die im Textbereich definiert werden, Text bis zu vier Ebenen tief einrücken. Dadurch können Sie spezifische Abschnitte in einem Bericht identifizieren, die in das Inhaltsverzeichnis aufgenommen werden können, um die Navigation im Berichtsergebnis zu erleichtern.
- Wenn Sie dem Berichtsbereich Überschriften hinzufügen möchten, ziehen Sie je nach gewünschter Einzugsebene H1, H2, H3 oder H4 in den Berichtsbereich.




In der folgenden Tabelle werden die Textelemente aufgelistet, mit denen ein Bericht formatiert wird:

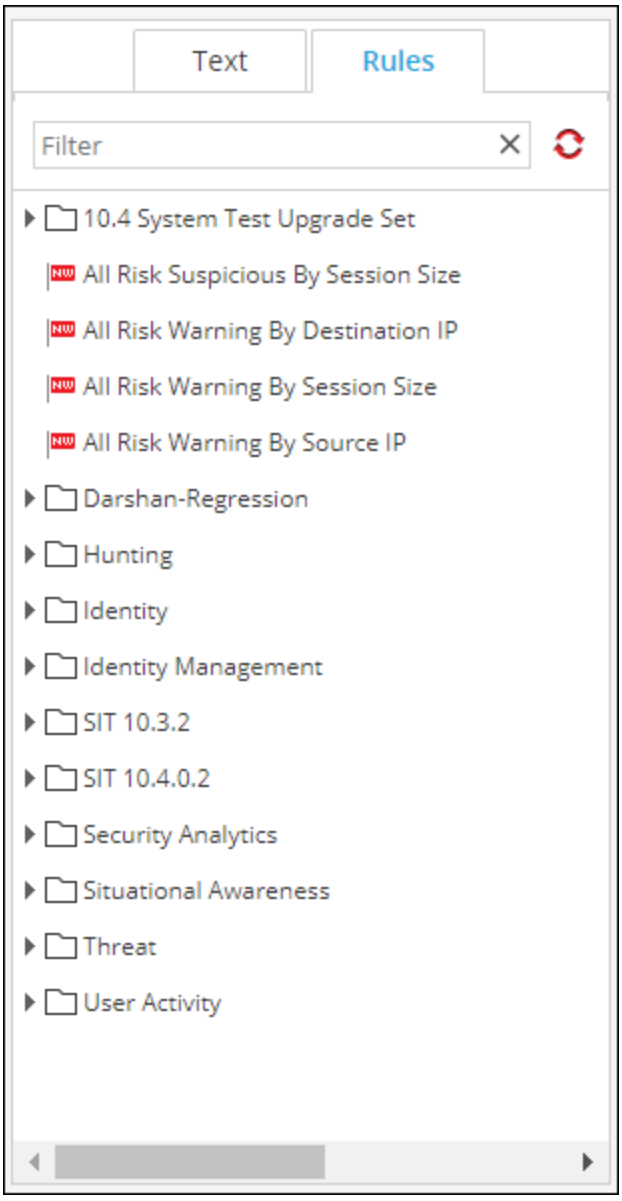
| Textelemente | Beschreibung |
|---|---|
| Überschrift 1<br>H1 | Das Element Überschrift 1 fügt der Berichtdefinition eine Überschrift auf erster Ebene hinzu. |

| Textelemente | Beschreibung |
|---|---|
| Überschrift 2  | Das Element Überschrift 2 fügt der Berichtdefinition eine Überschrift auf zweiter Ebene hinzu. |
| Überschrift 3  | Das Element Überschrift 3 fügt der Berichtdefinition eine Überschrift auf dritter Ebene hinzu. |
| Überschrift 4  | Das Element Überschrift 4 fügt der Berichtdefinition eine Überschrift auf vierter Ebene hinzu. |
| Inhaltsverzeichnis  | Das Inhaltsverzeichnis fügt der Berichtdefinition ein Inhaltsverzeichnis hinzu. |
| Textkörper  | Das Element Textkörper fügt der Berichtdefinition Fließtext hinzu. |
| Anmerkung  | Das Element Anmerkung fügt der Berichtdefinition Anmerkungen hinzu.<br>**Hinweis:** Das Element Anmerkung wird nicht angezeigt, wenn Sie alle Berichte anzeigen. |

## Regelbereich

Der Regelbereich besteht aus einer Liste von Regeln, die im Regelbereich definiert werden. Sie können Regeln aus der Regelliste ziehen und im Berichtsbereich ablegen, um sie mit dem Bericht zu verknüpfen.

Mit dem Suchtextfeld im Regelbereich können Sie nach einer bestimmten Regel suchen.


Text
Rules
Filter
10.4 System Test Upgrade Set
All Risk Suspicious By Session Size
All Risk Warning By Destination IP
All Risk Warning By Session Size
All Risk Warning By Source IP
Darshan-Regression
Hunting
Identity
Identity Management
SIT 10.3.2
SIT 10.4.0.2
Security Analytics
Situational Awareness
Threat
User Activity

## Ansicht „Regel erstellen“

Die Ansicht „Regel erstellen“ erläutert die Aktionen und die entsprechenden Verfahren, die Sie unter Regeln durchführen können.

# Workflow

Dieser Workflow zeigt das Verfahren zum Erstellen oder Bereitstellen von Regeln.


# Was möchten Sie tun?

| Rolle | Ich möchte... | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel* | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

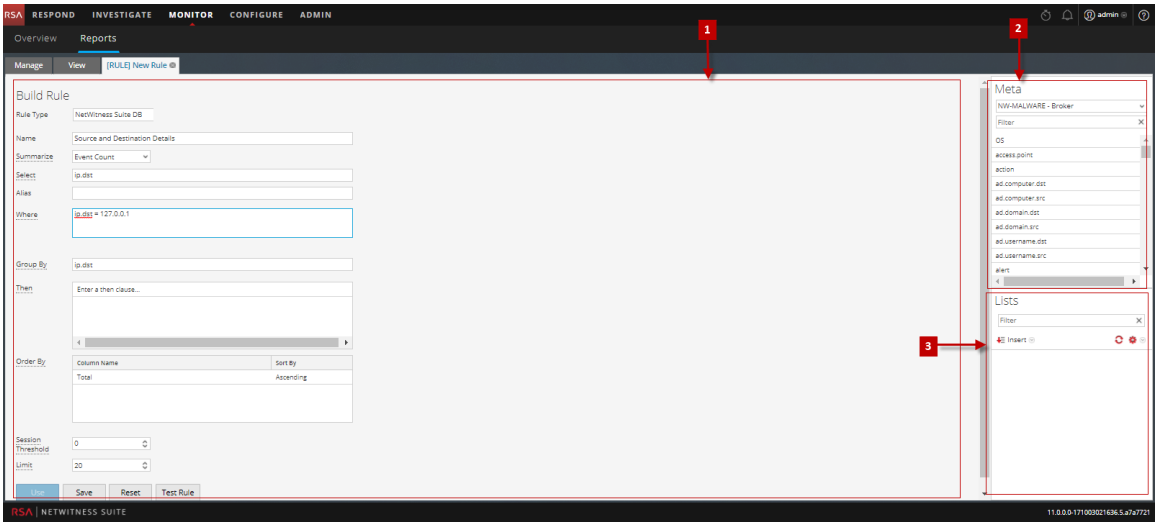
| Rolle | Ich möchte... | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren einer Regel
- Managen von Listen, Regeln oder Berichten
- Dialogfeld „Regelberechtigungen“
- Ansicht Regeln

## Schnellansicht




So greifen Sie auf die Ansicht „Regel erstellen“ zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie in der Symbolleiste „Regeln“ auf + NetWitnessDB
   . Die Registerkarte der Ansicht Regel erstellen wird angezeigt

## Funktionen

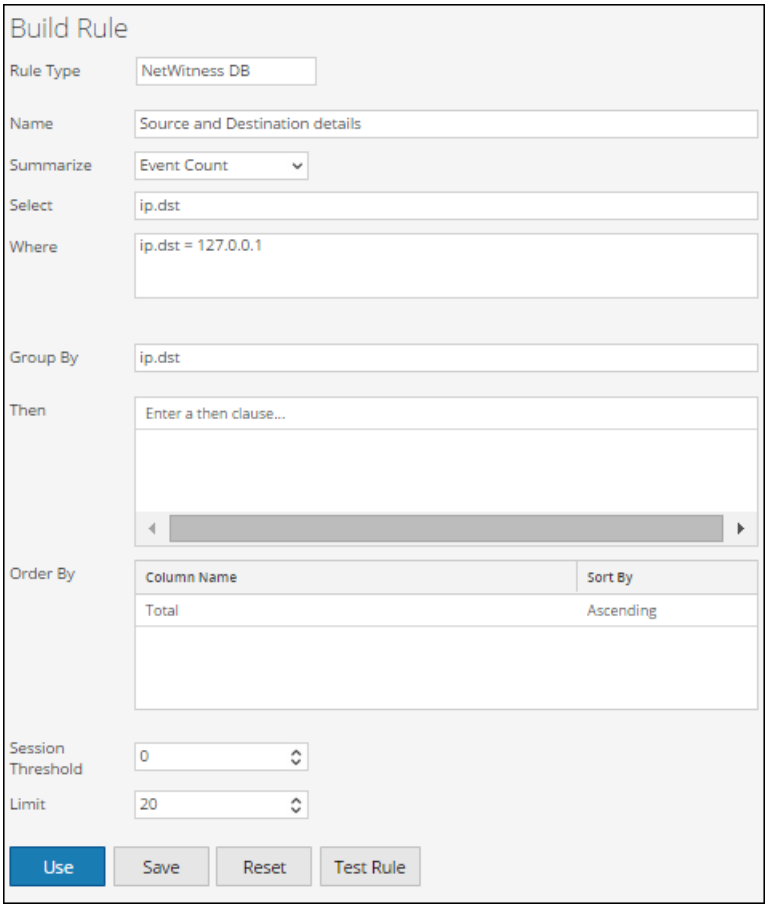
Die Ansicht „Regel erstellen“ enthält die folgenden Bereiche:

1. Regelbereich
2. Metabereich
3. Listenbereich

## Regelbereich

Im Regelbereich können Sie eine Regel für den ausgewählten Datenbanktyp erstellen.

Die folgende Abbildung zeigt den Bereich „Regel“.




In der folgenden Tabelle werden die Funktionen im Bereich „Regel“ beschrieben.

| Funktion | Beschreibung |
|---|---|
| Regeltyp | Eine Drop-down-Liste der unterstützten Datenbanktypen, für die Sie Regeln erstellen können. Es sind folgende Optionen verfügbar: „NetWitness-DB“, „IPDB“ und „Warehouse-DB“. |
| Name | Der Name der Regel, die Sie erstellen. |

| Funktion | Beschreibung |
|---|---|
| Zusammenfassung | Eine Drop-down-Liste mit Optionen für die Zusammenfassung. Es sind folgende Optionen verfügbar: „Keine“, „Ereignisanzahl“, „Paketanzahl“, „Sitzungsanzahl“ und „Benutzerdefiniert“. |
| Auswählen | Der Metaschlüssel für den Sie die Aggregatwerte benötigen; z. B. „ip.dest“. |
| Dabei gilt Folgendes: | Eine „Where“-Klausel, in der die Bedingungen definiert sind, die die Regelausführung auslösen, z. B. „ip.dest = 127.0.0.1“. |
| Gruppieren nach | Die Gruppierungsmethode für die Ergebnisse. Beispiel: Das Angeben von „ip.dest“ führt zu einem Bericht, in dem identische „ip.dest“-Werte gruppiert werden. |
| Gehen Sie dann wie folgt vor | Eine „Then“-Klausel, in der die Regelaktionen für die weitere Verarbeitung definiert sind. |
| Sortieren nach | Die Sortiermethode, die beim Anzeigen der Ergebnisse verwendet wird. Beispiel: Wenn für „Sortieren nach“ der Wert in der Spalte „Gesamt“ und „Aufsteigend“ angegeben wird, wird ein Bericht erzeugt, in dem die Ergebnisse in aufsteigender Reihenfolge basierend auf dem Wert in der Spalte „Gesamt“ sortiert sind. |
| Sitzungsschwellenwert | Eine Auswahlliste für den Sitzungsschwellenwert, der die maximale Anzahl der Sitzungen angibt, die für Aggregatfunktionen verarbeitet werden sollen. |
| Einschränkung | Eine Auswahlliste für die maximale Anzahl der Ergebniszeilen, die abgerufen werden sollen. |
| Verwenden Sie | Durch Klicken auf „Verwenden“ können Sie die Regel verwenden, um einen Bericht, eine Warnmeldung oder ein Diagramm zu erstellen. |

| Funktion | Beschreibung |
|---|---|
| Speichern | Durch Klicken auf „Speichern“ wird die bearbeitete Regel gespeichert und der Bereich „Regel erstellen“ bleibt geöffnet. Bevor Sie eine Regel testen, müssen Sie diese speichern, wenn Sie Ihre Änderungen beibehalten möchten. |
| Zurücksetzen | Durch Klicken auf „Zurücksetzen“ werden alle Feldinformationen gelöscht. |
| Regeltest | Durch Klicken auf „Regeltest“ wird das Dialogfeld „Regeltest“ geöffnet. |

## Dialogfeld „Regeltest“

So greifen Sie auf die Ansicht „Regeltest“ zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Führen Sie im Bereich „Regelliste“ einen der folgenden Schritte aus:
   - Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste „Regeln“ auf  .
   - Klicken Sie auf  Bearbeiten
     . Die Registerkarte der Ansicht Regel erstellen wird angezeigt.

3. Klicken Sie auf **Regel testen**.
   Die Ansicht „Regel testen“ wird angezeigt.


In der folgenden Tabelle werden die Funktionen im Bereich „Regel testen“ beschrieben.

| Funktion | Beschreibung |
|---|---|
| Datenquelle | Eine Drop-down-Liste der Datenquellen für den Typ der getesteten Regel. Mögliche Datenquellen sind: Concentrator, Broker, Decoder oder Log Decoder. |
| Format | Eine Drop-down-Liste der Formate für das Anzeigen der Ergebnisse für die Regel. Mögliche Formate sind: Tabellarische, Bereich, Balken, Blase, Spalte, Zeile, Kreis, Schrittlinie, Schrittbereich, Spline-Bereich und Spline. |

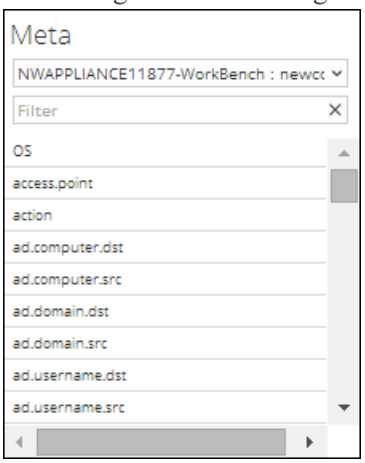
| Funktion | Beschreibung |
| --- | --- |
| Zeitbereich | Eine Drop-down-Liste mit Methoden zum Festlegen des Zeitbereichs.<br><br>• Bei Auswahl von „Letzte“ können Sie eine Anzahl von Jahren, Monaten, Wochen, Tagen oder Stunden angeben. Beispiel: Stunden, Tage, Wochen, Monate oder Jahre.<br>• Bei Auswahl von „Bereich“ können Sie einen Datumsbereich und einen Zeitraum angeben. Beispiel: Startdatum bis Enddatum.<br><br>Die in der Benutzeroberfläche angezeigte Uhrzeit und das angezeigte Datum sind abhängig vom Zeitzonenprofil, das durch den Benutzer ausgewählt wurde. |
| Relative Zeitberechnung verwenden | Bei Auswahl dieser Option wird der Zeitraum relativ zur aktuellen Uhrzeit berechnet. |
| X-Achse | X-Achse und Y-Achse werden zur Angabe der Metadaten verwendet, die in die Diagramme dargestellt werden sollen.<br>In der Drop-down-Liste „X-Achse“ sind die Metadatentypen für die Einstellung `Group by` in der Regel aufgelistet. Sie können mehrere Metadatentypen auswählen, wenn die Regel über eine einzige Einstellung `Group by` verfügt.<br>Für benutzerdefinierte Regeln mit mehreren `Group by`-Werten können Sie nur den ersten Metadatentyp für die X-Achse auswählen. |
| Y-Achse | In der Drop-down-Liste „Y-Achse“ sind die in der Regel verwendeten Aggregatfunktionen aufgelistet. „Sum“, „Count“, „Countdistinct“ und „Average“ sind die für Regeln unterstützten Aggregatfunktionen.<br>Sie können eine oder mehrere Aggregatfunktionen auswählen. |

| Funktion | Beschreibung |
|---|---|
| Test ausführen | Durch Klicken auf „Test ausführen“ wird ein Test der Regel ausgeführt, die zuletzt im Dialogfeld „Regelerstellung“ gespeichert wurde. Wenn der Test abgeschlossen ist, werden die Regeldaten (sofern vorhanden) für den ausgewählten Zeitbereich angezeigt. |

## Metabereich

Der Metabereich enthält eine Liste der verfügbaren Metadatentypen, mit denen Sie die Regel erstellen können. Sie können die Metadatentypen in den Select-, Where- und Then-Klauseln verwenden. Die Reporting Engine unterhält eine aktive Liste der verfügbaren Metanamen, indem eine kontinuierliche Synchronisierung mit der verknüpften Datenquelle vorgenommen wird.

In der folgenden Abbildung ist der Bereich Meta dargestellt.




In der folgenden Tabelle werden die Funktionen im Bereich „Meta“ beschrieben.

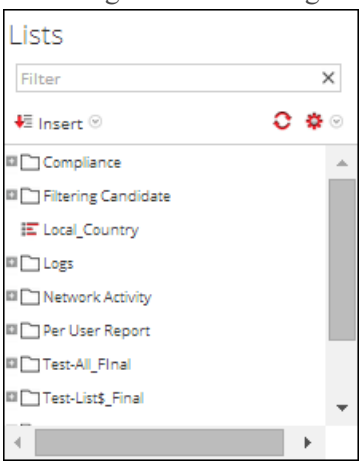
| Vorgang | Beschreibung |
|---|---|
| Auswählen | Die verfügbaren Datenquellen werden basierend auf dem ausgewählten Regeltyp in der Drop-down-Liste des Bereichs Meta angezeigt. Wählen Sie die erforderliche Datenquelle aus. Die verfügbaren Metadatentypen für die Datenquelle werden angezeigt. Meta auswählen. |
| Filter | Filtern Sie die Metadaten nach einem bestimmten Metawert. |

## Listenbereich

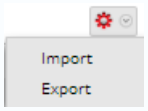
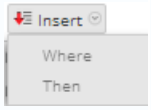
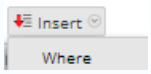
Eine Liste ist ein Platzhalter für einen Wertesatz, den Sie in Metadaten oder in einer Variablen verwenden können. Sie können zum Beispiel eine Liste mit allen IP-Adressen der Ereignisquelle in der Whitelist definieren. Wenn die Liste definiert wurde, können Sie den Listennamen in der Regel verwenden. Dies bietet die Flexibilität beim Hinzufügen, Ändern und Löschen der Listenwerte.

Der Listenbereich enthält eine Sammlung von Listen. Die Reporting Engine unterhält eine aktive Liste der verfügbaren Listennamen, indem eine kontinuierliche Synchronisierung mit der verknüpften Sammlung vorgenommen wird.

In der folgenden Abbildung ist der Bereich Listen dargestellt.



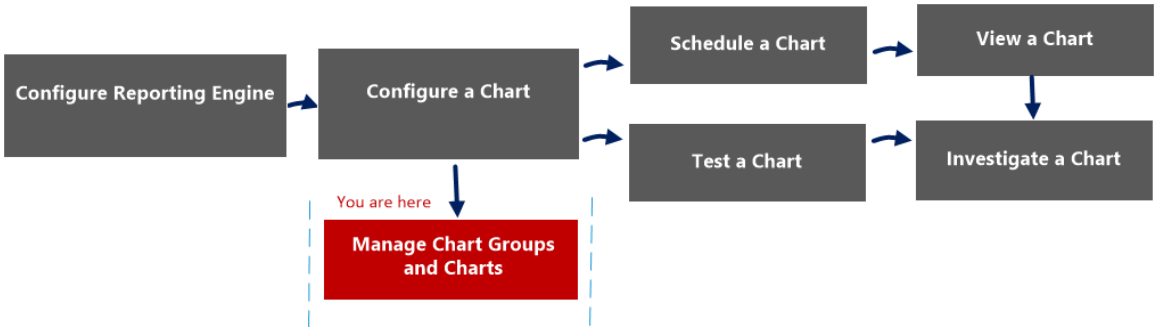

In der folgenden Tabelle werden die Funktionen im Bereich „Listen“ beschrieben.

| Vorgang | Beschreibung |
|---|---|
|  | Importieren oder Exportieren von Listen. |
|  | Aktualisiert die Liste. |
|  | Wenn Sie den Regeltyp **NetWitness-DB** auswählen, werden die Optionen „Where“ und „Then“ angezeigt. Fügen Sie die Liste in die Where- oder Then-Klausel der Regel ein. |
|  | Wenn Sie den Regeltyp **Warehouse-DB** auswählen, wird die Option „Where“ angezeigt. Fügen Sie die Liste in die Where-Klausel der Regel ein. |

## Dialogfeld „Diagrammberechtigungen“

Im Dialogfeld „Diagrammberechtigungen“ können Sie auf Diagramm- Diagrammgruppenebene Zugriffsberechtigungen managen. Nur Benutzer mit Lese- und Schreibrechten können das Diagramm im Reporting-Modul konfigurieren.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms* | Managen einer Diagrammgruppe und eines Diagramms |

*Sie können diese Aufgaben hier durchführen.

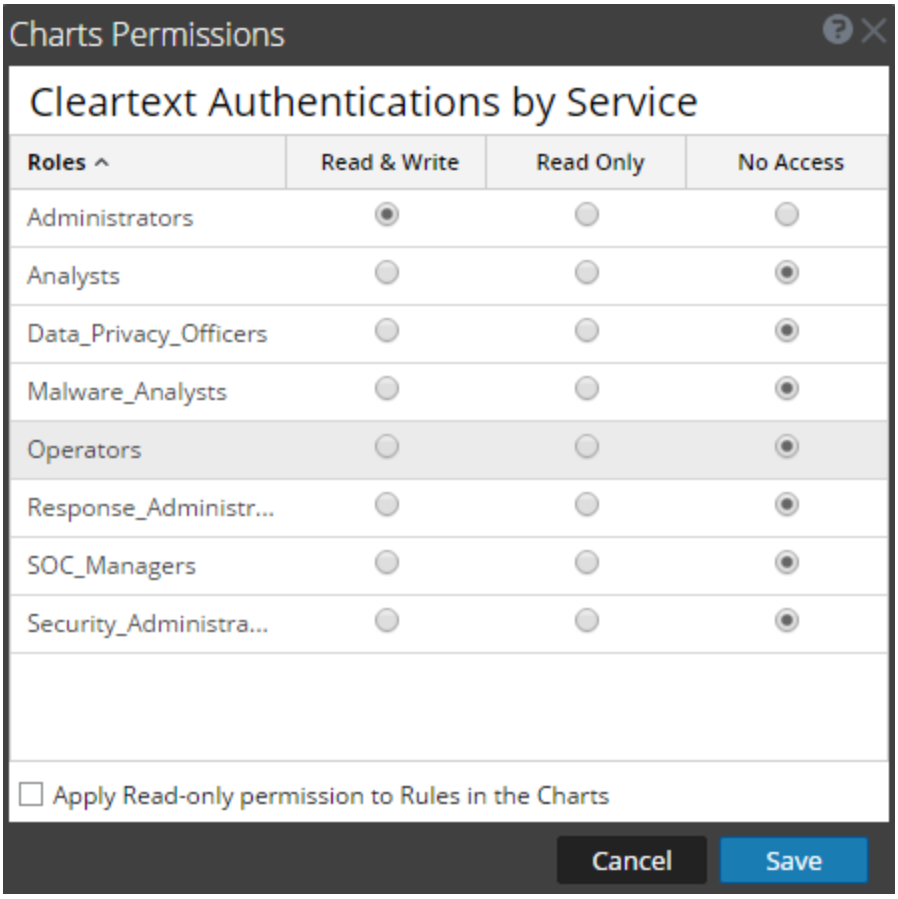
## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms
- Anzeigen eines Diagramms
- Testen eines Diagramms
- Untersuchen eines Diagramms
- Managen einer Diagrammgruppe und eines Diagramms

## Schnellansicht

Im Dialogfeld „Diagrammberechtigungen“ können Sie je nach Benutzerrolle Diagrammberechtigungen festlegen.

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.



1. Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen.
2. Klicken Sie auf **Diagramme**, um die Ansicht „Diagramme“ zu öffnen.
3. Wählen Sie im Bereich **Diagrammliste** einen Bericht aus und klicken Sie auf > **Berechtigungen.** Das Dialogfeld „Diagrammberechtigungen“ wird angezeigt.
4. Wählen Sie aufgrund der Benutzerrolle die entsprechenden Optionen aus.
5. (Optional) Aktivieren Sie das Kontrollkästchen, wenn Sie abhängigen Regeln automatisch Lesezugriff gewähren möchten.
6. Klicken Sie auf **Speichern**.

In der folgenden Tabelle werden die verschiedenen Spalten im Dialogfeld Diagrammberechtigungen aufgelistet.

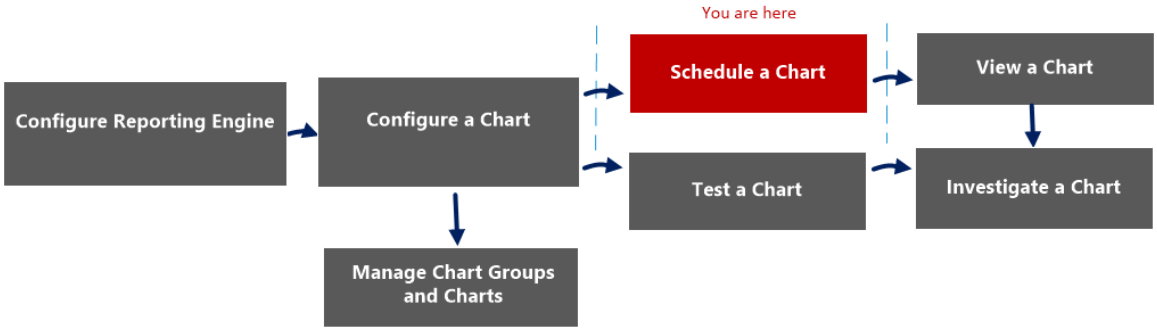
| Spalte | Beschreibung |
|---|---|
| Rollen | Zeigt alle Benutzerrollen in der NetWitness-Benutzeroberfläche an. |
| Lesen & Schreiben | Ermöglicht die Anwendung der Berechtigung „Lesen und Schreiben“ für den Zugriff auf das Diagramm. |
| Schreibgeschützt | Ermöglicht die Anwendung der Berechtigung „Lesen“ für den Zugriff auf die Warnmeldung. |
| Kein Zugriff | Wenn Sie diese Berechtigung auswählen, können Sie nicht auf das Diagramm zugreifen oder es anzeigen. |
| ☐Diese Berechtigungen auf Untergruppen und Diagramme in dieser Gruppe anwenden | Wendet die ausgewählten Berechtigungen auf die Diagrammgruppe, Untergruppen in der Gruppe und Diagramme in der Gruppe an.<br>**Hinweis:** Das Kontrollkästchen wird nur gefüllt, wenn Zugriffsberechtigungen für eine Diagrammgruppe festgelegt werden. |
| ☐Nur-Lese-Berechtigungen auf Regeln in Diagrammen anwenden | Ermöglicht, Berechtigungen automatisch auf die Regeln in den Diagrammen anzuwenden. |

| Spalte | Beschreibung |
| --- | --- |
| Abbrechen | Verwirft alle an den Berechtigungen vorgenommen Änderungen. |
| Speichern | Speichert die Auswahl und bietet basierend auf dieser Auswahl Zugriff auf die Rollen. |

## Ansicht Diagramm

In der Ansicht „Diagramm“ sehen Sie die verfügbaren Diagramme und Gruppen in einem Raster und hier können Sie sie planen, indem Sie die Diagramme aktivieren.

# Workflow




# Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms | Managen einer Diagrammgruppe und eines Diagramms |

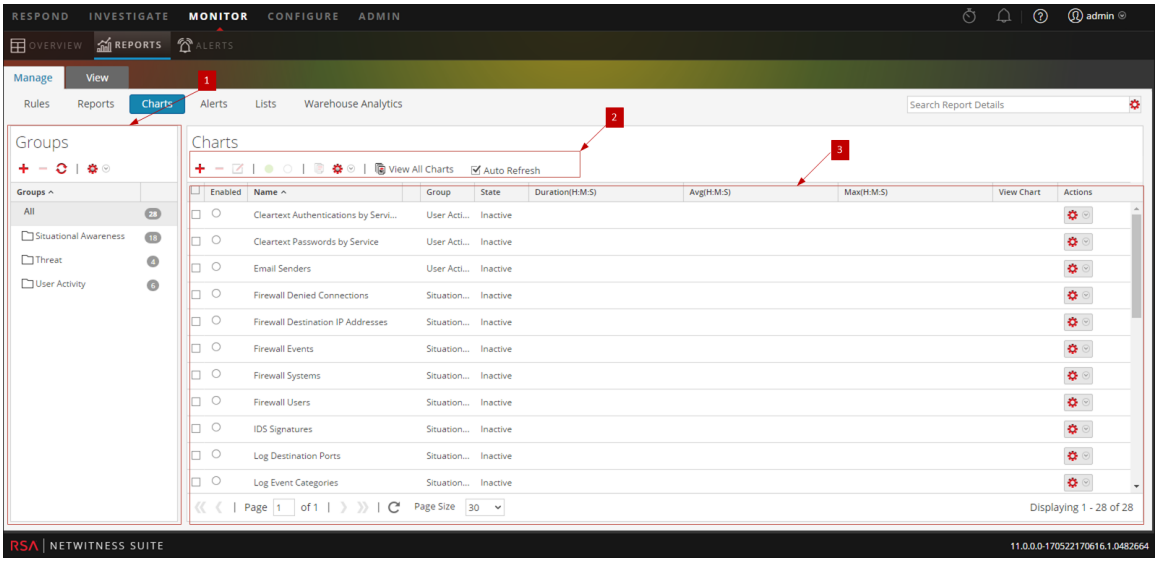
*Sie können diese Aufgaben hier durchführen.

# Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms

# Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.

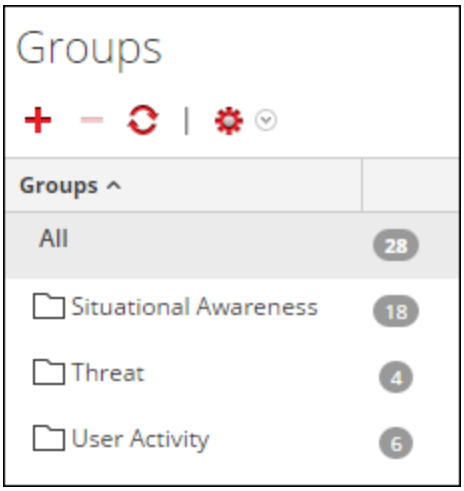



Die Ansicht Diagramm umfasst folgende Bereiche:

| | |
|---|---|
| 1 | Bereich Diagrammgruppen |
| 2 | Symbolleiste „Diagramme“ |
| 3 | Bereich Anzeigen eines Diagramms |

## Bereich Diagrammgruppen

Im Bereich „Diagrammgruppen“ können Sie Diagramme in Gruppen organisieren. Sie können eine Gruppe erstellen, der Gruppe Diagramme hinzufügen und Diagramme zwischen Gruppen verschieben. Der Bereich Diagrammgruppen wird in der folgenden Abbildung gezeigt.




Der Bereich „Diagrammgruppen“ enthält die folgenden Optionen:

| Funktion | Beschreibung |
|---|---|
| + | Fügt ein neues Diagramm zum Reporting-Modul hinzu. |
| − | Löscht eines oder mehrere ausgewählte Diagramme. |
| | Bearbeiten eines Diagramms |
| | Aktualisiert die Ansicht. |
| | Bietet die folgenden Optionen: „Importieren“, „Exportieren“ und „Berechtigungen“. |

## Symbolleiste „Diagramme“

Über die Symbolleiste „Diagramme“ können Sie Diagramme hinzufügen, ändern, löschen, duplizieren, aktivieren, deaktivieren, importieren und exportieren. Sie können auch Zugriffsberechtigungen für Diagramme in einer Gruppe festlegen.

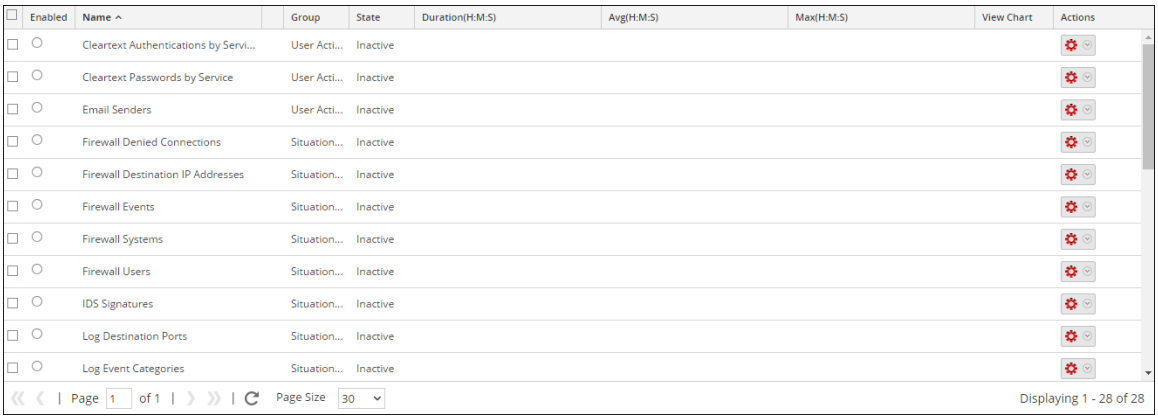

Die Symbolleiste „Diagramme“ umfasst die folgenden Optionen:

| Funktion | Beschreibung |
|---|---|
| + | Fügt ein neues Diagramm zum Reporting-Modul hinzu. |

| Funktion | Beschreibung |
|---|---|
|  | Löscht eines oder mehrere ausgewählte Diagramme. |
|  | Diagramm bearbeiten. |
|  | Aktiviert die ausgewählten Diagramme. |
|  | Deaktiviert die ausgewählten Diagramme. |
|  | Erstellt eine Kopie des ausgewählten Diagramms. |
|  | Bietet die folgenden Optionen: Importieren, exportieren, exportieren als Text und Berechtigungen. |
| Alle Diagramme anzeigen | Zeigt alle ausgeführten Diagramme. |
| Automatisch aktualisieren | Aktualisiert automatisch die Liste der Diagramme. |

## Bereich „Anzeigen eines Diagramms“

Im Bereich „Anzeigen eines Diagramms“ werden alle Diagramme im Tabellen- oder Rasterformat aufgeführt.




In der folgenden Tabelle sind die verschiedenen Spalten im Bereich „Anzeigen eines Diagramms“ aufgeführt.

| Funktion | Beschreibung |
|---|---|
| Aktiviert | ● - Das Diagramm ist aktiviert.<br>○ - Das Diagramm ist deaktiviert. |
| Name | Der Name des Diagramms |
| Gruppe | Die Diagrammgruppe, zu der das Diagramm gehört |
| Status | Der Status des Diagramms:<br>• Queued<br>• Abgeschlossen<br>• Fehlgeschlagen |
| Dauer (Std:Min:Sek) | Die Ausführungsdauer des letzten Diagramms |
| Durchschn. (Std:Min:Sek) | Die durchschnittliche Dauer für die Diagrammausführung |
| Max (Std:Min:Sek) | Die maximale Dauer für die Diagrammausführung |
| Diagramm anzeigen | Dies ist ein Hyperlink, der zum Bereich „Anzeigen eines Diagramms“ führt. |
|  | Das Aktionsmenü enthält die folgenden Optionen: Aktivieren, Deaktivieren, Anzeigen, Löschen, Bearbeiten und Exportieren. |

## Bereich Ausführungsverlauf

Im Bereich Ausführungsverlauf können Sie Verlaufsdetails abrufen und anzeigen.

# Workflow

Dieser Workflow zeigt das Verfahren, um Berichte oder Berichtsgruppen anzuzeigen.


# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen von Berichten | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen* | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

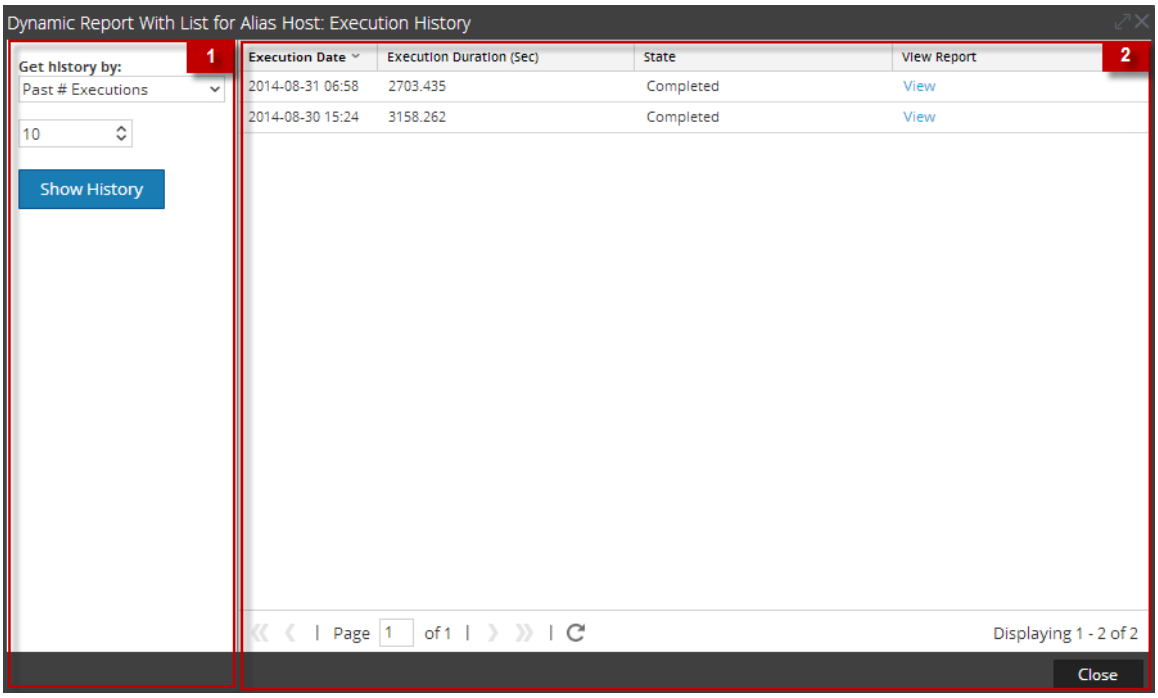
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Bereich „Liste erzeugen“
- Ansicht Geplante Berichte

## Schnellansicht

Die folgende Abbildung zeigt ein Beispiel der Ansicht „Ausführungsverlauf“.




# Funktionen

Die Ansicht Ausführungsverlauf verfügt über die folgenden Bereiche:

1 Bereich Ausführungsverlaufsoptionen

2 Bereich Ausführungsverlaufsausgabe

So greifen Sie auf diese Ansicht zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Führen Sie im Bereich „Regelliste“ einen der folgenden Schritte aus:
   - Bewegen Sie den Mauszeiger über einen Bericht und klicken Sie auf > **Geplante Berichte anzeigen**.
   - Klicken Sie auf die Spalte **#Schedules**.
     Die Ansicht „Berichte planen“ wird mit dem Status jedes geplanten Berichts angezeigt.
3. Wählen Sie einen geplanten Bericht aus und führen Sie einen der folgende Schritte aus.
   - Klicken Sie auf > **Ausführungsverlauf**.
   - Klicken Sie auf von dem Symbolleistenbereich Geplante Berichte.

## Bereich Ausführungsverlaufsoptionen

Im Bereich „Ausführungsverlaufsoptionen“ können Sie die Verlaufsdetails basierend entweder auf den letzten n (Anzahl) geplanten Berichten oder auf einem bestimmten Datumsbereich abrufen.

In der folgende Tabelle werden die Vorgänge im Bereich „Ausführungsverlaufsoptionen“ aufgeführt:

| Vorgang | Beschreibung |
|---|---|
| Verlauf abrufen nach: | Dies sind die Kriterien, um den Ausführungsverlauf anzuzeigen:<br>• **Anz. vergangene Ausführungen**: Die Anzahl (n) der vergangenen geplanten Berichte. Diese Option ist standardmäßig angezeigt.<br>• **Bereich (spezifisch)**: Das Startdatum und Enddatum für den Datumsbereich.<br>**Hinweis:** Die Felder **Von** und **Bis** werden in der Benutzeroberfläche nur dann ausgefüllt, wenn Sie Bereich (spezifisch) aus der Liste NetWitness Suite **Verlauf abrufen** nach auswählen. |
| Von | Das Startdatum für den Datumsbereich. |
| An | Das Enddatum für den Datumsbereich. |
| Count | Die anzuzeigende Anzahl des Ausführungsverlaufs des geplanten Berichts. |

| Vorgang | Beschreibung |
| --- | --- |
| Show History | Zeigt die Verlaufsdetails basierend auf den ausgewählten Kriterien an. |

## Bereich Ausführungsverlaufsausgabe

Der Bereich „Ausführungsverlaufsausgabe“ zeigt die Verlaufsdetails mit dem Ausführungsdatum, der Ausführungsdauer (Sekunden), dem Status des geplanten Berichts und einem Link zur Anzeige des Berichts an.

In der folgende Tabelle werden die verschiedenen Spalten im Bereich „Ausführungsverlaufsausgabe“ aufgeführt:

| Spalte | Beschreibung |
| --- | --- |
| Ausführungsdatum | Das Datum, an dem der geplante Bericht ausgeführt wurde.<br>Standardmäßig ist das Ausführungsdatum in absteigender Reihenfolge. |
| Ausführungsdauer (Sek) | Die Zeit, die die Ausführung des geplanten Berichts gedauert hat. |

| Spalte | Beschreibung |
|---|---|
| State | Der Status des geplanten Berichts:<br><br>• Geplant: Wenn ein Bericht für die stündliche, tägliche, wöchentliche, monatliche oder eine spätere Ausführung geplant wird, wird der Status des Berichts für die erste Ausführung als „Geplant“ angezeigt.<br>• In der Warteschlange: Wenn die Ausführung eines Bericht noch aussteht, wird als Status des Berichts In der Warteschlange angezeigt.<br>• „Wird ausgeführt“: Wenn der geplante Bericht verarbeitet wird, wird als Status des Berichts „Wird ausgeführt“ angezeigt.<br>• Teilweise: Wenn in einem Bericht mit mehreren Regeln die Ausführung einer einzigen Regel, eine Ausgabeaktion oder die Erstellung einer PDF-/CSV-Datei fehlgeschlagen ist, wird als Status des Berichts Teilweise angezeigt. Beispiel: In einem Bericht mit fünf Regeln werden<br>vier Regeln erfolgreich ausgeführt und eine schlägt fehl. Als Status wird daher „Teilweise“ angezeigt.<br>• Failed: Wenn in einem Bericht mit mehreren Regeln alle Regelausführungen fehlschlagen, wird der Status des Berichts als Fehlgeschlagen angezeigt.<br>• Abgeschlossen: Wenn eine Berichtplanung erfolgreich ausgeführt wird, wird als Status des Berichts „Abgeschlossen“ angezeigt.<br>• Abgebrochen: Wenn eine Anforderung zum Abbruch erfolgreich ausgeführt wurde, wird als Status des Berichts „Abgebrochen“ angezeigt.<br>• Inaktiv: Wenn eine Berichtplanung deaktiviert ist, wird als Status des Berichts Inaktiv angezeigt.<br>• „Nicht verfügbar“: Wenn die Ausführungsinformationen zu einer Berichtplanung nicht verfügbar sind, wird der Status des Berichts als „Nicht verfügbar“ angezeigt. |
| Bericht anzeigen | Der Hyperlink zu Anzeigen eines Berichts im Vollbildmodus. |
| Schließen | Schließt die Ansicht Ausführungsverlauf. |

## Bereich „Liste erzeugen“

Im Dialogfeld „Liste erzeugen“ können Sie eine Liste erzeugen und anpassen.

# Workflow

Dieser Workflow zeigt das Verfahren zum Erstellen und Planen von Berichten.


# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts* | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte* | Managen von Listen, Regeln oder Berichten |

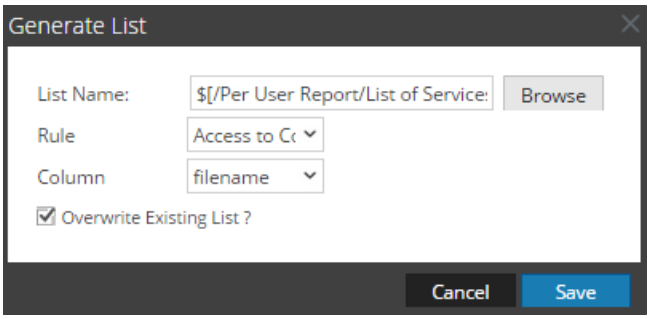
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Erstellen und Planen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Listenansicht
- Ansicht Liste aufbauen
- Dialogfeld „Listenberechtigungen“

## Schnellansicht

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




So greifen Sie auf diese Ansicht zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus und klicken Sie auf > **Berichtplan**.
   Die Ansichtsregisterkarte Einen Bericht planen wird angezeigt.

4. Klicken Sie im Bereich **Dynamische Liste** auf +.

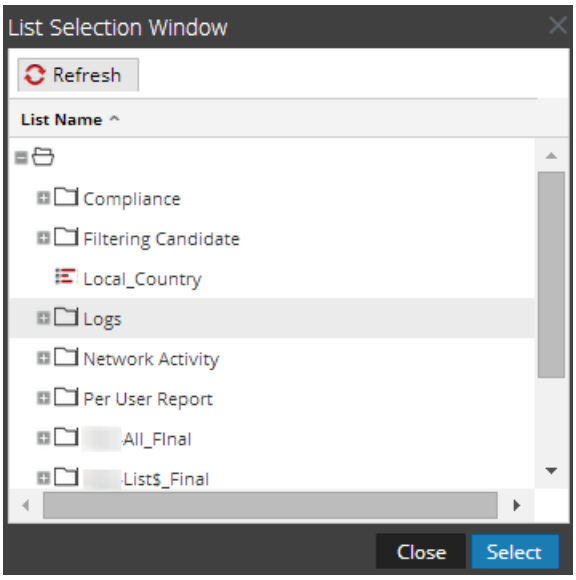
   Das Dialogfeld „Liste erzeugen“ wird angezeigt.

## Funktionen

In der folgenden Tabelle sind die Felder im Dialogfeld „Liste erzeugen“ aufgeführt.

| Feld | Beschreibung |
|---|---|
| Listenname | Der Name der Liste, die aus dem Listenauswahlbereich ausgewählt wurde. |
| **Browse** | Klicken Sie auf diese Schaltfläche, um eine Liste aus dem Dialogfeld Listenauswahlfenster auszuwählen. |
| Regel | Wählen Sie eine Regel aus, die bei der Erstellung der Liste verwendet wird. |
| Spalte | Wählen Sie einen Wert für die Spalte aus. |
| Vorhandene Liste überschreiben? | Überschreibt die bestehende Liste. |
| **Speichern** | Fügt die gewünschte Liste dem Bereich Liste erzeugen der Ansicht Bericht planen hinzu. |

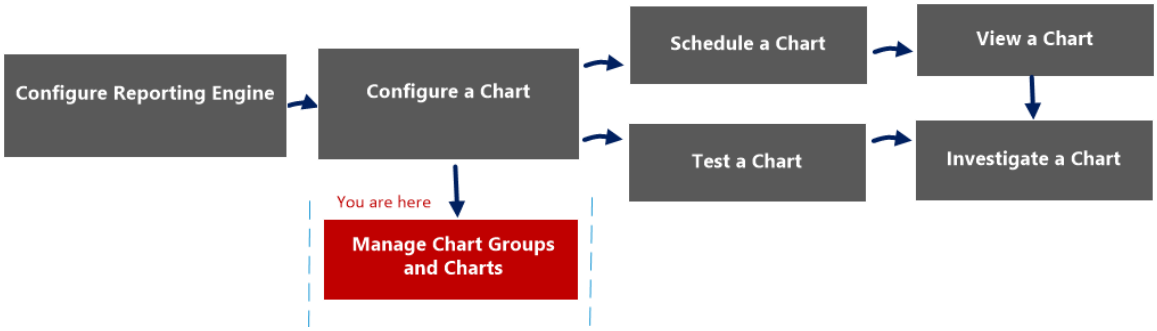
Das Dialogfeld Listenauswahlfenster enthält die im Bereich Listen definierten Listen. Hier können Sie eine Liste auswählen und mit dem Bericht verknüpfen. In der folgenden Abbildung ist das Dialogfeld dargestellt.


List Selection Window
Refresh
List Name
Compliance
Filtering Candidate
Local_Country
Logs
Network Activity
Per User Report
All_FInal
List$_Final
Close
Select

## Dialogfeld „Diagramm importieren“

Im Dialogfeld „Diagramm importieren“ können Sie Diagramme mit Untergruppen und Diagramme aus anderen NetWitness-Instanzen in den Bereich „Diagrammgruppen“ importieren. Diagramme müssen als gültige Binärdatei vorliegen, die aus einer anderen NetWitness-Instanz exportiert wurde.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms* | Managen einer Diagrammgruppe und eines Diagramms |

*Sie können diese Aufgaben hier durchführen.

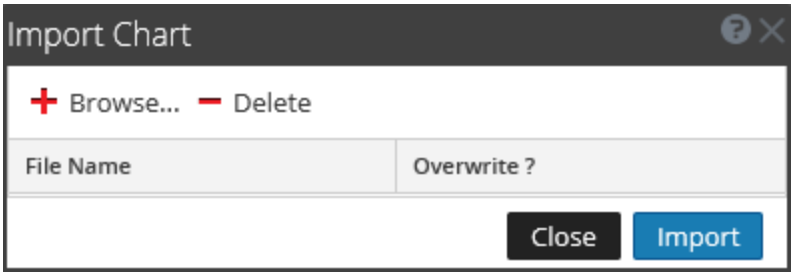
## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms
- Anzeigen eines Diagramms
- Testen eines Diagramms
- Untersuchen eines Diagramms
- Managen einer Diagrammgruppe und eines Diagramms

## Schnellansicht

Dieses Dialogfeld zeigt unterschiedliche Optionen an, wenn Sie es zum Importieren von Gruppen mit Untergruppen und von Diagrammen aus anderen NetWitness-Instanzen in den Bereich „Diagrammgruppen“ verwenden.

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




1. Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen.
2. Klicken Sie auf **Diagramme**, um die Ansicht „Diagramme“ zu öffnen.
3. Wählen Sie im Bereich **Diagrammgruppen** einen Ordner für das Importieren der Datei aus.
4. Klicken Sie im Bereich „Diagrammgruppen“ oder in der Symbolleiste „Diagramm“ auf  **importieren**, um die Datei zu importieren.

In der folgenden Tabelle werden die Funktionen im Dialogfeld „Diagramm importieren“ beschrieben.

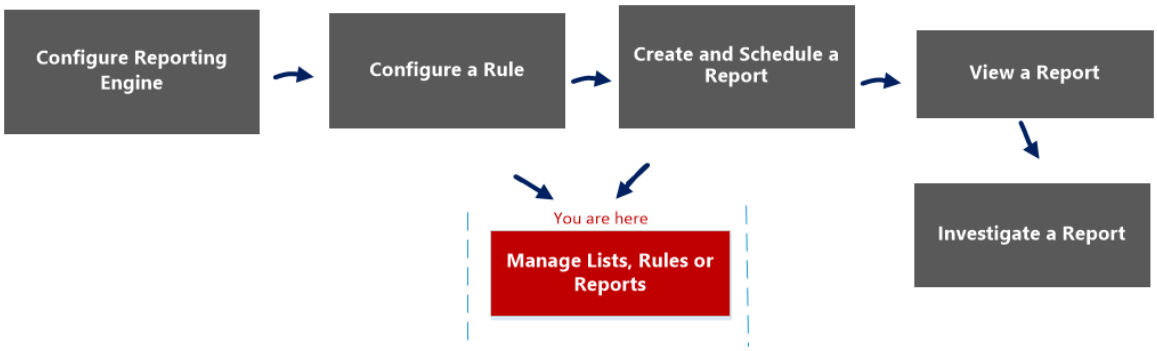
| Funktion | Beschreibung |
|---|---|
| Durchsuchen | Zeigt eine Ansicht des lokalen Dateisystems, damit Sie die zu importierende Warnmeldung auswählen können. |
| Löschen | Löscht einen importierten Bericht aus der Liste der importierten Diagramme. |
| Dateiname | Zeigt eine Liste der Diagrammdateien an, die an das Modul Diagramme importiert werden sollen, wenn Sie auf „Importieren“ klicken. |
| Überschreiben? | Ermöglicht die Auswahl der Option zum Überschreiben einer vorhandenen Version des Diagramms, das Sie importieren. Wenn Sie die Option „Überschreiben“ nicht auswählen, wird ein Duplikat der Datei importiert und es wird keine Fehlermeldung angezeigt. |
| Schließen | Schließt das Dialogfeld. Wenn Sie Diagramme für den Import ausgewählt haben, aber nicht auf „Importieren“ geklickt haben, werden die Diagramme nicht importiert und nicht in diesem Dialogfeld gespeichert. |
| Importieren | Importiert die ausgewählten Tabellen in Ihr Modul Diagramme. |

## Dialogfeld „Bericht importieren“

Im Dialogfeld „Bericht importieren“ können Sie Gruppen mit Untergruppen und Berichten aus anderen Instanzen NetWitness Suite in den Bereich „Berichtsgruppen“ importieren. Berichte müssen als gültige Binärdatei vorliegen, die aus einer anderen NetWitness Suite-Instanz exportiert wurde.

## Workflow

Dieser Workflow zeigt das Verfahren zum Managen der Berichte oder Berichtsgruppen.




## Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |

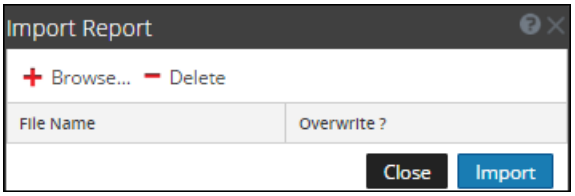
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte* | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht
- Ansicht Bericht erstellen
- Dialogfeld „Berichtberechtigungen“

## Schnellansicht




So rufen Sie das Dialogfeld „Bericht importieren“ auf:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.

3. Wählen Sie im Bereich **Berichtsgruppen** einen Ordner aus, in den die Datei importiert werden soll.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie zum Importieren einer Gruppe im Bereich **Berichtsgruppen** auf  > **Importieren** .
   - Klicken Sie zum Importieren eines Berichts in der Symbolleiste **Bericht** auf  > **Importieren**.

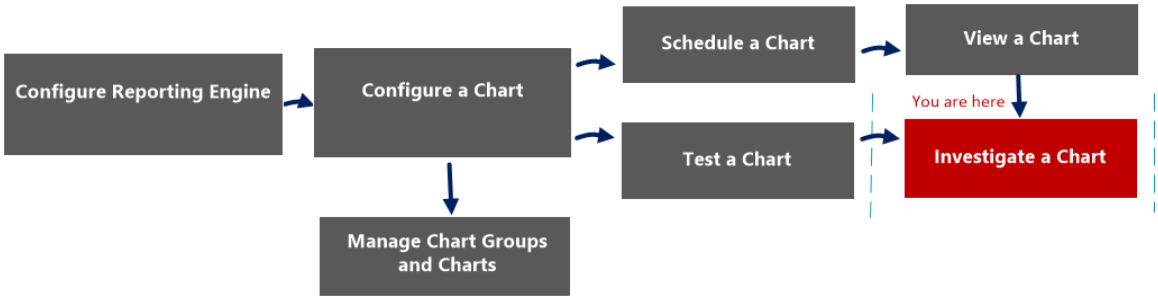
In der folgenden Tabelle werden die Funktionen im Dialogfeld „Bericht importieren“ aufgelistet.

| Funktion | Beschreibung |
|---|---|
| Browse | Diese Option zeigt eine Ansicht des lokalen Dateisystems, damit Sie den zu importierenden Bericht auswählen können. |
| Delete | Mit dieser Option wird ein importierter Bericht aus der Liste der importierten Berichte gelöscht. |
| Dateiname | Zeigt eine Liste der Berichtdateien an, die in das Berichtsmodul importiert werden sollen, wenn Sie auf „Importieren“ klicken. |
| Überschreiben? | Ermöglicht die Auswahl der Option zum Überschreiben einer vorhandenen Version des Berichts, den Sie importieren. Wenn Sie die Option „Überschreiben“ nicht auswählen, wird ein Duplikat der Datei importiert und es wird keine Fehlermeldung angezeigt. |
| Schließen | Mit dieser Option wird das Dialogfeld geschlossen. Wenn Sie einen Bericht ausgewählt und nicht auf „Importieren“ geklickt haben. werden die Berichte nicht importiert und nicht in diesem Dialogfeld gespeichert. |
| Import | Mit dieser Option werden die ausgewählten Berichte in das Modul Reports importiert. |

## Ansicht „Untersuchen eines Diagramms“

In der Ansicht „Untersuchen eines Diagramms“ können Sie Diagrammdetails aufrufen und untersuchen. Es gibt Optionen zum Filtern und Sortieren der Informationen im Diagramm sowie Optionen für den Typ des Diagramms, die Anzahl der darzustellenden Elemente und die Diagrammanzeigewerte oder Gesamtwerte. Beim Anzeigen eines Diagramms können Sie die im Diagramm dargestellten Sitzungen im Modul Investigation öffnen und das Diagramm als PDF-Datei speichern.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms* | Untersuchen eines Diagramms |

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms | Managen einer Diagrammgruppe und eines Diagramms |

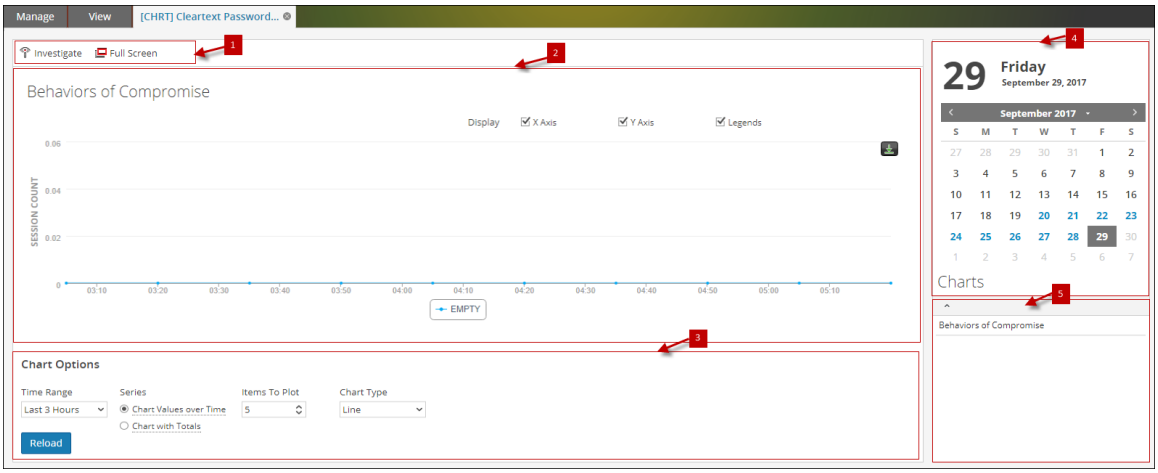
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms
- Anzeigen eines Diagramms
- Testen eines Diagramms
- Untersuchen eines Diagramms

## Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




Der Bereich Anzeigen eines Diagramms umfasst folgende Bereiche:

| | |
|---|---|
| 1 | Symbolleiste „Diagramme“ |
| 2 | Bereich Diagrammausgabe |
| 3 | Bereich Diagrammkalender |
| 4 | Bereich Diagrammoptionen |

5 Liste Ausgeführte Diagramme

## Symbolleiste „Diagramme“

Die Symbolleiste „Diagramme“ enthält Optionen für das Untersuchen sowie das Anzeigen des Diagramms auf einem anderen Bildschirm.


In der folgenden Tabelle sind die Optionen der Symbolleiste „Diagramme“ aufgelistet.

| Vorgang | Beschreibung |
|---|---|
| Untersuchung | Untersucht die Diagrammdetails näher. |
| Vollbild | Zeigt das Diagramm als Vollbild an. |

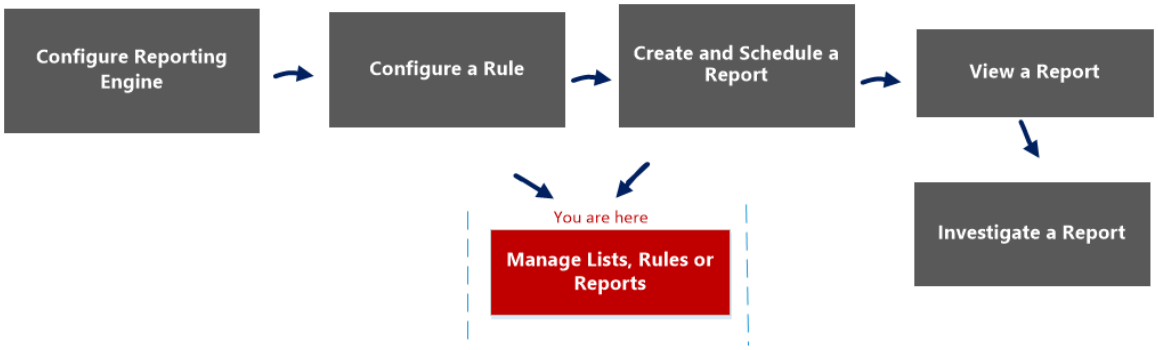
## Dialogfeld „Listenberechtigungen“

Im Dialogfeld „Listenberechtigungen“ können Sie auf Ebene der Liste oder Listengruppe Zugriffsberechtigungen managen. Nur Benutzer mit **Lese- und Schreibrechten** können die Liste im Reporting-Modul konfigurieren.

## Workflow

Dieser Workflow zeigt das Verfahren zum Managen von Listen oder Listengruppen. Sie können den Zugriff auf der Listen- oder Listengruppenebene festlegen, damit nur Benutzer mit bestimmten Rollen auf die Listen zugreifen können. Sie können Listen verwenden, um Regeln für das Generieren von Berichten, Diagrammen und Warnmeldungen zu definieren.

Sie müssen sicherstellen, dass Reporting Engine konfiguriert ist NetWitness Suite.




## Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen von Berichten | Erstellen und Planen eines Berichts |

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte* | Managen von Listen, Regeln oder Berichten |

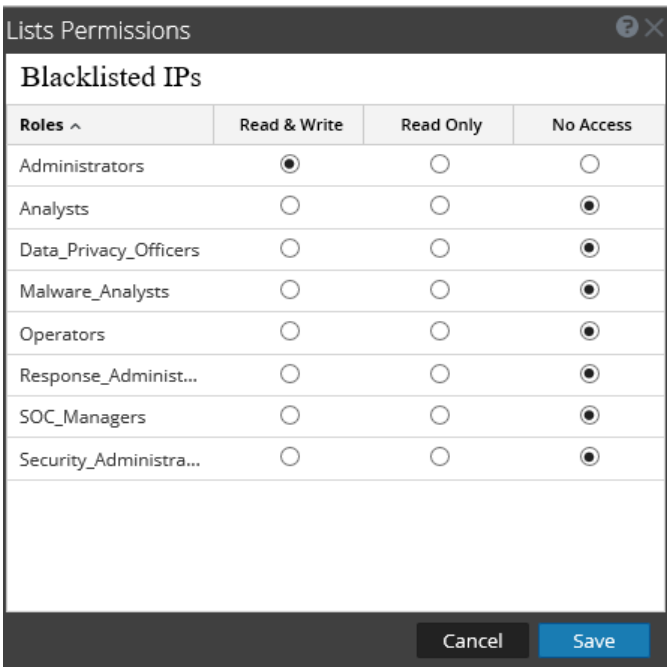
*Sie können diese Aufgaben hier durchführen.

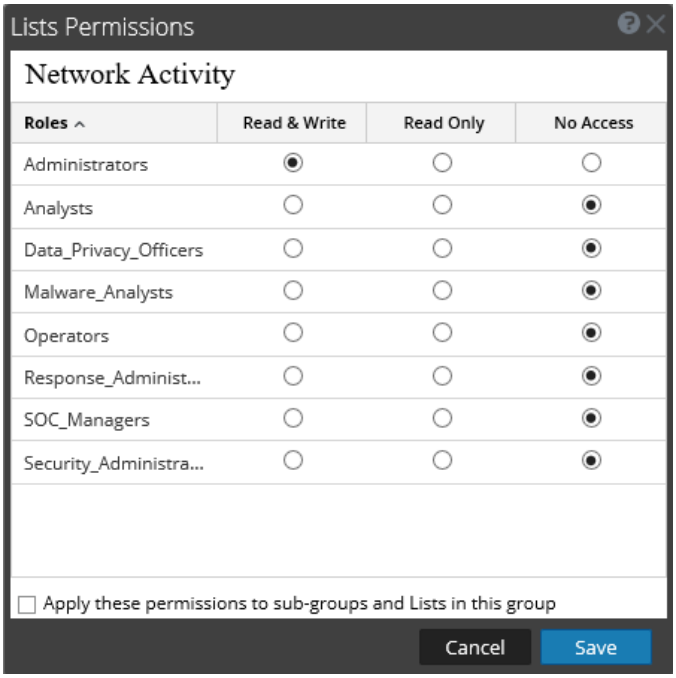
## Verwandte Themen

- Konfigurieren einer Regel
- Managen von Listen, Regeln oder Berichten
- Listenansicht
- Liste von Berechtigungen finden Sie unter „Rollenberechtigungen“ im *Handbuch Systemsicherheit und Benutzerverwaltung*.

## Schnellansicht

Die folgenden Abbildungen sind Beispiele für die Dialogfelder „Listenberechtigungen“ und „Listengruppenberechtigungen“:




So greifen Sie auf diese Ansicht zu

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Listen**.
   Die Listenansicht wird angezeigt.
3. Wählen Sie in der Ansicht **Liste** einen Bericht aus.

4. Klicken Sie in der **Listensymbolleiste** auf  > **Berechtigungen**.

   Das Dialogfeld „Berichtberechtigungen“ wird angezeigt.

In der folgenden Tabelle werden die Funktionen im Dialogfeld „Listenberechtigungen“ beschrieben.

| Funktion | Beschreibung |
|---|---|
| Rollen | Beschreibt die Rollen der Benutzer, die bei der NetWitness Suite-Benutzeroberfläche angemeldet sind. |
| Lesen & Schreiben | Der Benutzer kann in der Listenansicht auf Listen zugreifen, sie anzeigen, bearbeiten, löschen, importieren und exportieren. Der Benutzer kann die Berechtigungen für die Regel ebenfalls ändern. |
| Schreibgeschützt | Der Benutzer kann in der Listenansicht nur auf die Liste zugreifen und sie anzeigen. |
| Kein Zugriff | Ermöglicht es Benutzern nicht, Listen aufzurufen oder anzuzeigen. |
| Diese Berechtigungen auf Untergruppen und Listen in dieser Gruppe anwenden | Wendet automatisch Berechtigungen auf die Untergruppen und Listen in den Gruppen an, wenn das Kontrollkästchen aktiviert ist. |
| Abbrechen | Verwirft alle an den Berechtigungen vorgenommen Änderungen. |
| Speichern | Speichert die Auswahl und bietet basierend auf dieser Auswahl Zugriff auf die Rollen. |

## Listenansicht

In der Liste sehen Sie verfügbare Listen und Gruppen in einem Raster.

## Workflow

Dieser Workflow zeigt das Verfahren zum Definieren von Listen oder Listengruppen. Sie können den Zugriff auf der Listen- oder Listengruppenebene festlegen, damit nur Benutzer mit bestimmten Rollen auf die Listen zugreifen können. Sie können Listen verwenden, um Regeln für das Generieren von Berichten, Diagrammen und Warnmeldungen zu definieren.

Sie müssen sicherstellen, dass Reporting Engine konfiguriert ist NetWitness Suite.


## Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel* | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen von Berichten | Erstellen und Planen eines Berichts |

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

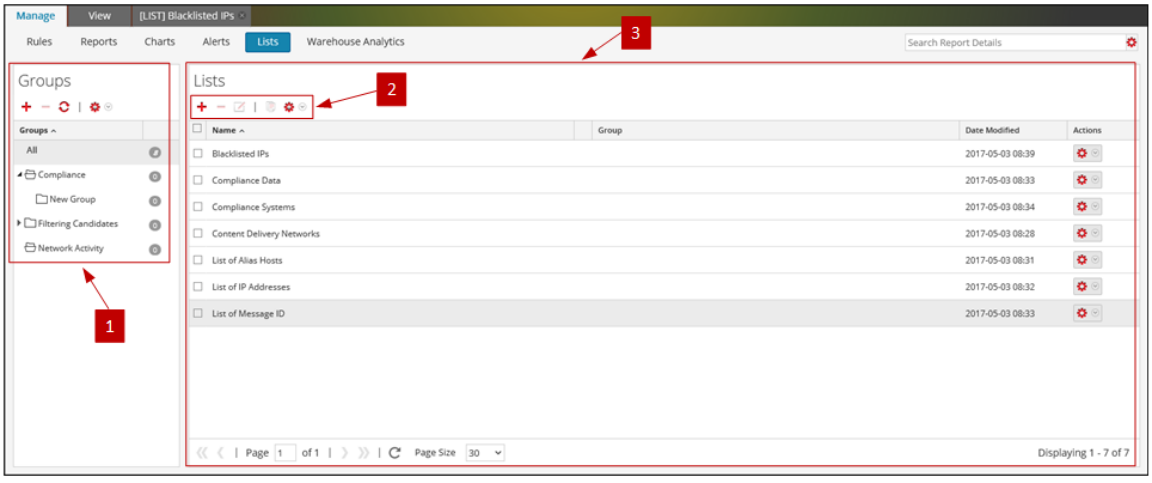
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren einer Regel
- Managen von Listen, Regeln oder Berichten
- Dialogfeld „Listenberechtigungen“
- Ansicht Liste aufbauen

## Schnellansicht

Die folgende Abbildung zeigt die Listenansicht.




So greifen Sie auf diese Ansicht zu

1. Wählen Sie **Monitor > Berichte**.

   Die Registerkarte Managen wird angezeigt.

2. Klicken Sie auf **Listen**.

   Die Listenansicht wird angezeigt.

Die Listenansicht umfasst folgende Bereiche:

1. Bereich mit Listengruppen
2. Symbolleiste Liste
3. Bereich „Listenansicht“

## Bereich mit Listengruppen

Der Bereich „Listengruppen“ enthält eine Liste von Gruppen, die zum Organisieren von Listen verwendet werden, und verfügt über eine Symbolleiste, in der Sie Gruppen erstellen und verwalten können.

| Funktion | Beschreibung |
|---|---|
|  | Mit dieser Option können Benutzer eine neue Regel zum Reporting-Modul hinzufügen. |
|  | Ermöglicht Benutzern, Gruppen zu löschen. |
|  | Aktualisiert die Ansicht. |
|  | Ermöglicht Benutzern den Zugriff auf folgende Optionen: „Importieren“, „Exportieren“ und „Berechtigungen“. |

Sie können im Bereich Listengruppen folgende Aktionen ausführen:

- Aktualisieren der Listen in einer Gruppe
- Verschieben von Listen zwischen verschiedenen Gruppen. Sie können eine Liste von einer Gruppe in eine andere verschieben, indem Sie sie ziehen und in der gewünschten Gruppe ablegen.
- Erstellen von Listengruppen.
- Löschen einer Listengruppe.
- Exportieren einer Listengruppe.
- Exportieren einer Listengruppe.
- Festlegen der Zugriffskontrolle für Listengruppen.

## Symbolleiste Liste

| Funktion | Beschreibung |
|---|---|
|  | Mit dieser Option können Benutzer eine neue Liste zum Reporting-Modul hinzufügen. |
|  | Mit dieser Option können Sie eine oder mehrere ausgewählte Listen löschen. |
|  | Ermöglicht Listen zu bearbeiten. |
|  | Erstellt eine Kopie der ausgewählten Liste. |
|  | Ermöglicht Benutzern den Zugriff auf folgende Optionen: „Importieren“, „Exportieren“ und „Berechtigungen“. |

## Bereich „Listenansicht“

Im Bereich Listenansicht werden alle definierten Listen in einem tabellarischen Format angezeigt.

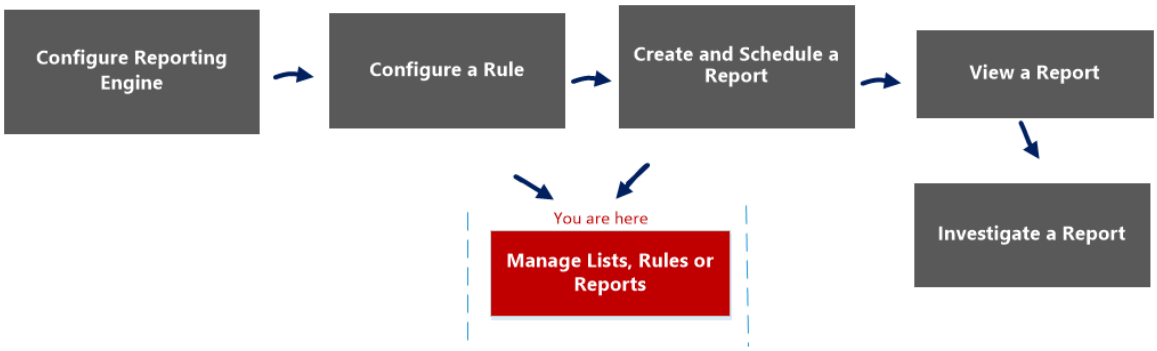
| Spalte | Beschreibung |
|---|---|
| Name | Zeigt den Namen der Liste an.<br><br>**Hinweis:** Für das Feld **Name** wird am Ende des Spaltenfelds kein Symbol zur Erweiterung der Spaltengröße angezeigt. Sie müssen die Maus ein wenig nach links bewegen, um das Symbol zur Erweiterung der Spalte zu sehen. |
| Gruppe | Zeigt die Listengruppe, zu der die Liste gehört, an. |
| Änderungsdatum | Zeigt Datum und Uhrzeit der Änderung der Liste an. |

## Dialogfeld „Berichtberechtigungen“

Im Dialogfeld „Berichtberechtigungen“ können die Benutzer mit der Zugriffsberechtigung „Lesen & Schreiben“ Berechtigungen konfigurieren.

## Workflow

Dieser Workflow zeigt das Verfahren zum Managen der Berichte oder Berichtsgruppen.




## Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

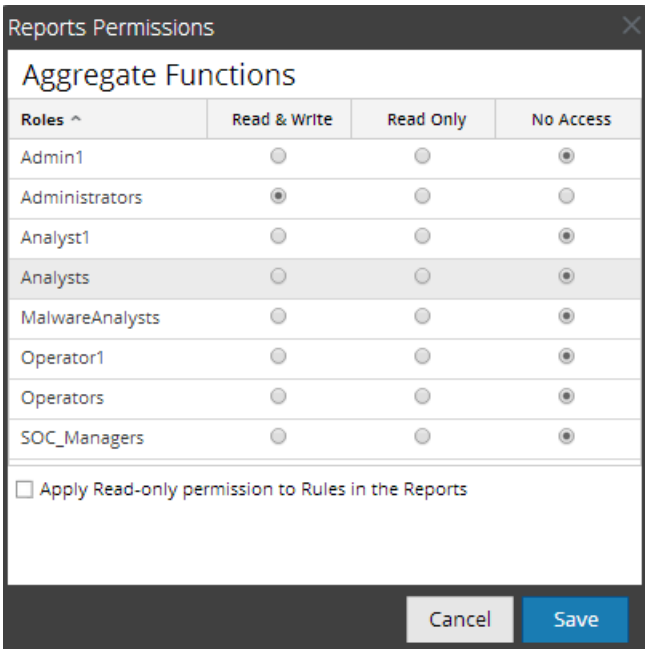
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte* | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht
- Ansicht Bericht erstellen
- Dialogfeld „Bericht importieren“

## Schnellansicht




So greifen Sie auf das Dialogfeld „Berichtberechtigungen“ zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus.
4. Klicken Sie auf Berechtigungen
   . Das Dialogfeld „Berichtberechtigungen“ wird angezeigt.

**Hinweis:** Wenn Sie das Kontrollkästchen aktivieren, wird allen abhängigen Regeln die Zugriffsberechtigung LESEN zugewiesen, sofern die Berechtigungen für den Bericht höher als die Berechtigungen für die Regeln sind.

In der folgenden Tabelle werden die Funktionen im Dialogfeld „Berichtberechtigungen“ beschrieben.

| Funktion | Beschreibung |
|---|---|
| Rollen | Zeigt alle Rollen an, die Zugriff auf die Berechtigungen erhalten können |
| Lesen/Schreiben | Ermöglicht den Erhalt der Zugriffsberechtigung „Lesen und Schreiben“ für die Regeln in den Berichten |

| Funktion | Beschreibung |
| --- | --- |
| Schreibgeschützt | Ermöglicht den Erhalt der Berechtigung „Schreibgeschützt“ für die Regeln in den Berichten |
| Kein Zugriff | Wenn Sie diese Option auswählen, erhalten Sie keine Berechtigung für die Regeln in den Berichten. |
| Nur-Lese-Berechtigungen auf Regeln in Berichten anwenden | Ermöglicht das Festlegen der Berechtigung „Schreibgeschützt“ für die Regeln in Berichten für alle Rollen. |
| Abbrechen | Mit dieser Option werden alle an den Berechtigungen vorgenommen Änderungen abgebrochen. |
| Speichern | Diese Option speichert die Auswahl und bietet basierend auf dieser Auswahl Zugriff auf die Rollen. |

## Ansicht Bericht

In der Ansicht „Bericht“ können Sie Berichtsgruppen erstellen und organisieren.

# Workflow

Dieser Workflow zeigt das Verfahren zum Erstellen und Planen von Berichten.


# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts* | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

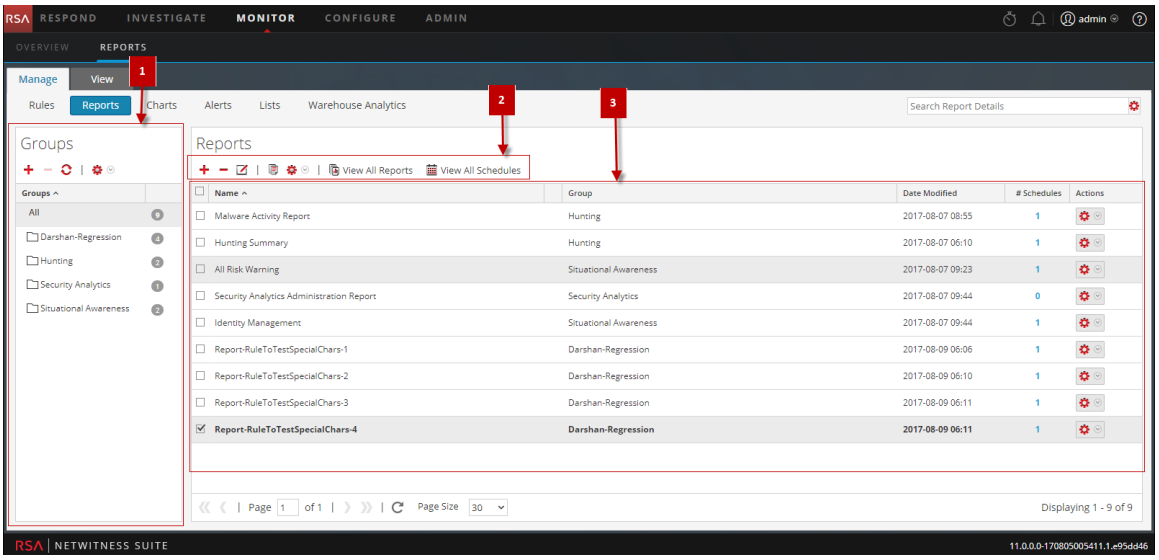
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht erstellen
- Dialogfeld „Bericht importieren“
- Ansicht Geplante Berichte
- Dialogfeld „Berichtberechtigungen“

## Schnellansicht




So greifen Sie auf diese Ansicht zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.

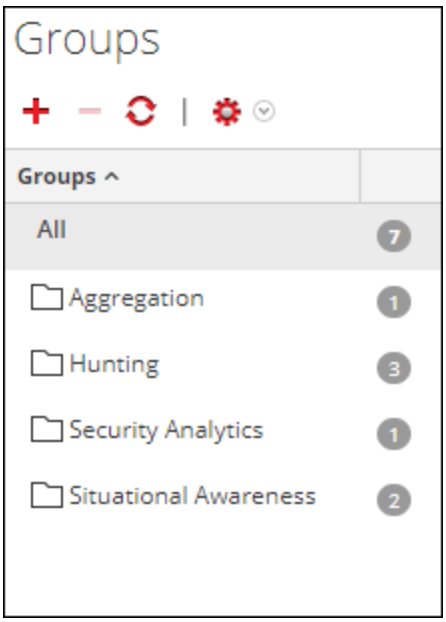
# Funktionen

Die Ansicht „Berichte“ umfasst die folgenden Abschnitte:

| | |
|---|---|
| 1 | Bereich Berichtsgruppen |
| 2 | Symbolleiste für Berichte |
| 3 | Bereich Berichtsliste |

## Bereich Berichtsgruppen

Im Bereich Berichtsgruppen können Sie Berichte in einer Gruppe organisieren. Sie können eine Berichtsgruppe erstellen, der Gruppe Berichte hinzufügen und Berichte zwischen Gruppen verschieben. Sie können sämtliche Berichte anzeigen, indem Sie unter der Spalte „Gruppen“ die Option „Alle“ auswählen.




| Funktion | Beschreibung |
|---|---|
| + | Mit dieser Option können Sie einen neuen Bericht zum Reporting-Modul hinzufügen. |

| | |
|---|---|
| | Mit dieser Option können Sie einen oder mehrere ausgewählte Berichte löschen. |
| | Mit dieser Option wird die Ansicht aktualisiert. |
| | Das Aktionsmenü enthält die folgenden Optionen: „Importieren“, „Exportieren“ und „Berechtigungen“. |

## Symbolleiste für Berichte

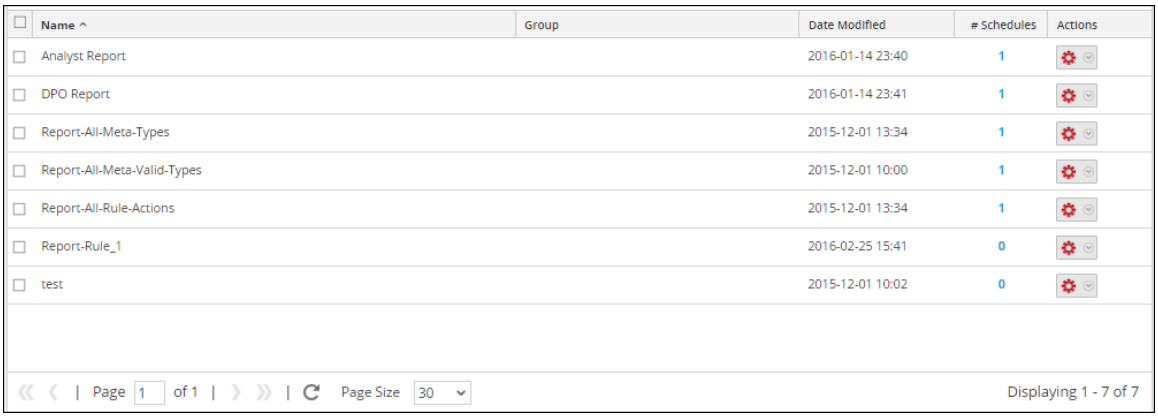
Über die Symbolleiste für Berichte können Sie Berichte hinzufügen, ändern, löschen, duplizieren, importieren und exportieren. Sie können auch Zugriffsberechtigungen für einen Bericht in einer Gruppe festlegen.


| Funktion | Beschreibung |
|---|---|
| | Mit dieser Option können Sie einen neuen Bericht zum Reporting-Modul hinzufügen. |
| | Mit dieser Option können Sie einen oder mehrere ausgewählte Berichte löschen. |
| | Mit dieser Option können Sie ein Diagramm bearbeiten. |
| | Mit dieser Option wird eine Kopie des ausgewählten Berichts erstellt. |
| | Das Aktionsmenü enthält die folgenden Optionen: Importieren, exportieren, exportieren als Text und Berechtigungen. |
| View All Reports | Mit dieser Option können Sie eine Liste von Berichten zusammen mit ihrem Zeitplannamen und ihrer Zeit anzeigen. |

| | |
|---|---|
| View All Schedules | Mit dieser Option können Sie alle geplanten Berichte anzeigen. |

## Bereich Berichtsliste

Im Bereich Berichtsliste werden sämtliche Berichte in tabellarischem Format aufgeführt.




In der folgenden Tabelle werden die Spalten im Bereich Berichtsliste beschrieben:

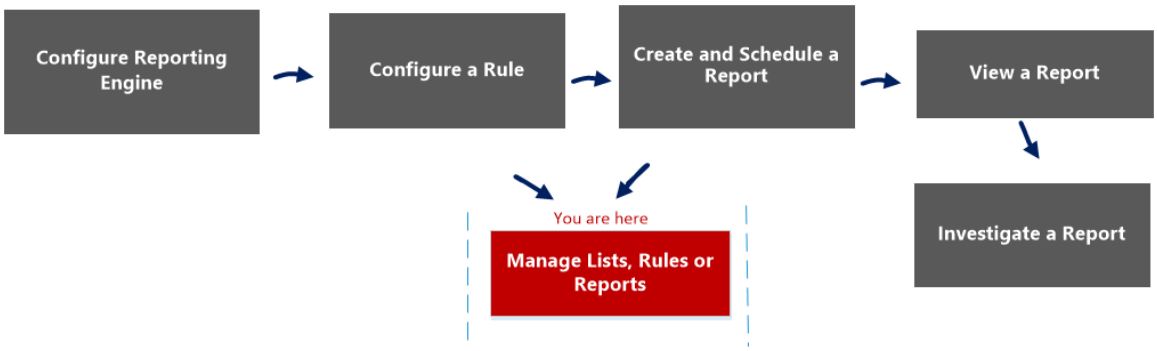
| Spalte | Beschreibung |
|---|---|
| Name | Der Name des Berichts |
| Gruppe | Die Gruppe, zu der der Bericht gehört. |
| Änderungsdatum | Das Datum und die Uhrzeit der Änderung des Berichts. |
| Anz. Pläne | Diese Zahl gibt die Anzahl der für einen Bericht erstellten Pläne an. |
| Actions | Das Aktionsmenü enthält die folgenden Optionen: „Bericht Planen“, „Geplante Berichte anzeigen“, „Löschen“, „Bearbeiten“ und „Exportieren“. |

## Dialogfeld „Regelberechtigungen“

Das Modul Reporting stellt die Zugriffskontrolle auf Regelebene zur Verfügung. Nur ein Benutzer mit den entsprechenden Berechtigungen kann Aufgaben für die Regel durchführen. Der Administrator muss beim Erstellen von Benutzerrollen darauf achten, dass die für bestimmte Aufgaben erstellten Rollen über alle in der Rollenhierarchie höher angesiedelten Zugriffsberechtigungen verfügen.

# Workflow

Dieser Workflow zeigt das Verfahren zum Managen von Regeln oder Regelgruppen.




# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte* | Managen von Listen, Regeln oder Berichten |

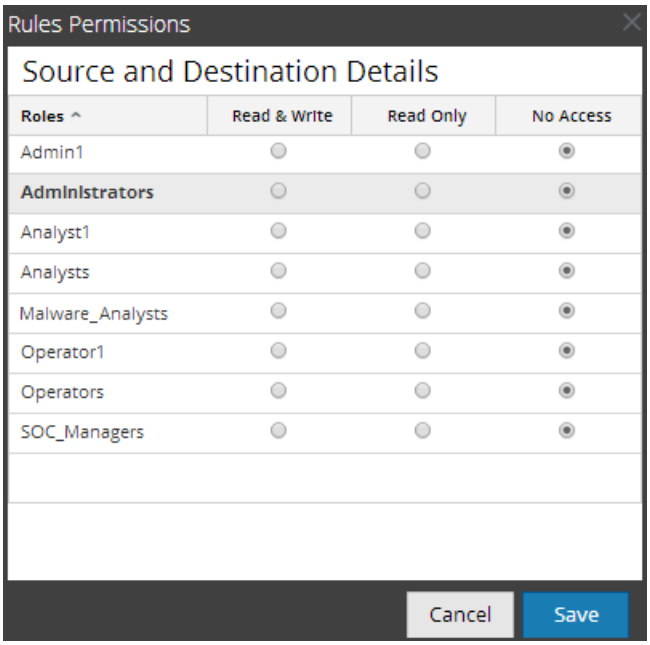
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

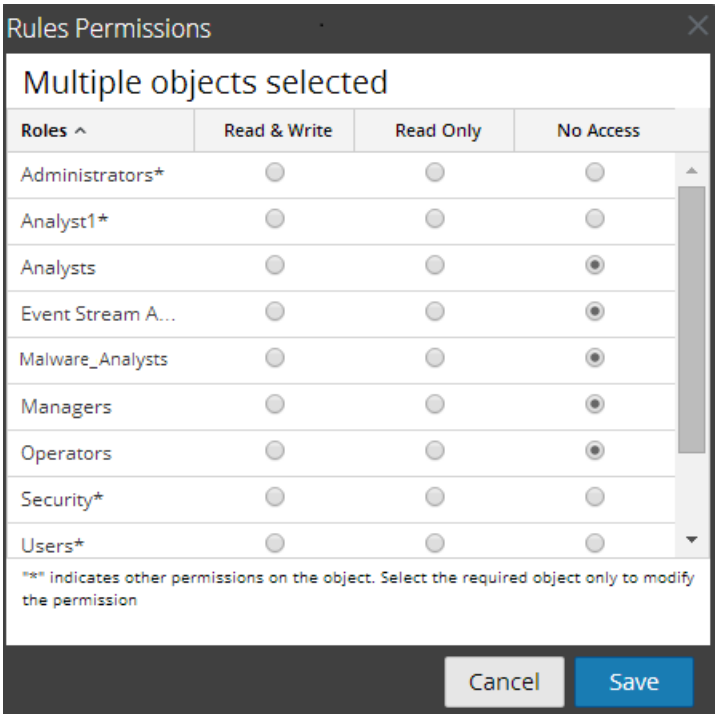
- Konfigurieren einer Regel
- Managen von Listen, Regeln oder Berichten
- Ansicht Regeln

## Schnellansicht

Diese Abbildung zeigt das Dialogfeld „Regelberechtigungen“ für eine einzelne Regel.



Diese Abbildung zeigt das Dialogfeld „Regelberechtigungen“ bei mehreren ausgewählten Regeln.




Das Dialogfeld verfügt über andere Darstellung für Regelgruppen im Vergleich zu Regeln. So rufen Sie das Dialogfeld auf:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Wählen Sie im Bereich **Regeln** eine oder mehrere Regeln oder eine Regelgruppe aus.
3. Klicken Sie in der Symbolleiste auf  Berechtigungen
   . Das Dialogfeld Regelberechtigungen wird angezeigt.

| Funktion | Beschreibung |
|---|---|
| Spalte „Rollen“ | Hier werden die integrierten und benutzerdefinierten NetWitness Suite-Benutzerrollen angezeigt. Jedem bei NetWitness Suite angemeldeten Benutzer wird eine Benutzerrolle zugewiesen.<br><br>Wenn mehrere Regeln ausgewählt sind, zeigt das Sternchen neben der Rolle (z. B. `Security*`) an, dass mit dieser Benutzerrolle andere Berechtigungen verfügbar sind. Um die anderen Berechtigungen zu ändern, müssen Sie die Benutzerrolle auswählen und die Zugriffsberechtigung ändern. |

| Funktion | Beschreibung |
| --- | --- |
| Spalte „Lesen & Schreiben“ | Wenn das Kontrollkästchen in dieser Spalte ausgewählt ist, verfügt die entsprechenden Benutzerrolle über die Berechtigung zum Anzeigen, Bearbeiten, Löschen, Importieren und Exportieren von Regeln in der Ansicht „Regeln“. Der Benutzer kann die Berechtigungen für die Regel ebenfalls ändern. |
| Spalte „Schreibgeschützt“ | Wenn das Kontrollkästchen in dieser Spalte ausgewählt ist, verfügt die entsprechende Benutzerrolle über die Berechtigung zum Anzeigen von Regeln in der Regelgruppe. |
| Spalte „Kein Zugriff“ | Wenn das Kontrollkästchen in dieser Spalte ausgewählt ist, kann die entsprechende Benutzerrolle die Regeln in der Regelgruppe weder anzeigen noch bearbeiten.<br>Bevor Rollenberechtigungen angewendet werden, ist dies die festgelegte Standardberechtigung für alle Benutzerrollen, obwohl das Kontrollkästchen deaktiviert ist. |
| Kontrollkästchen „Diese Berechtigungen auf Untergruppen und Regeln in dieser Gruppe anwenden“ | Bei Aktivierung werden Berechtigungen von NetWitness Suite auf Untergruppen und Regeln der Gruppe angewendet. |
| Option „Abbrechen“ | Durch Klicken auf „Abbrechen“ wird das Dialogfeld geschlossen, ohne dass Änderungen gespeichert werden. |

| Funktion | Beschreibung |
| --- | --- |
| Option „Speichern“ | Durch Klicken auf „Speichern“ wird das Dialogfeld geschlossen und die Regelgruppenberechtigungen für Benutzerrollen werden aktualisiert.<br>Sofern festgelegt, werden die Zugriffsberechtigungen auf Untergruppen und untergeordnete Objekte dieser Gruppe angewendet.<br>Wenn mehrere Regeln ausgewählt sind, wird die Zugriffsberechtigung auf alle ausgewählten Regeln angewendet. |

## Ansicht Regeln

Die Regelansicht ist die Benutzeroberfläche zum Regelmanagement.

## Workflow

Dieser Workflow zeigt das Verfahren zum Definieren von Regeln oder Regelgruppen.


## Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel* | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

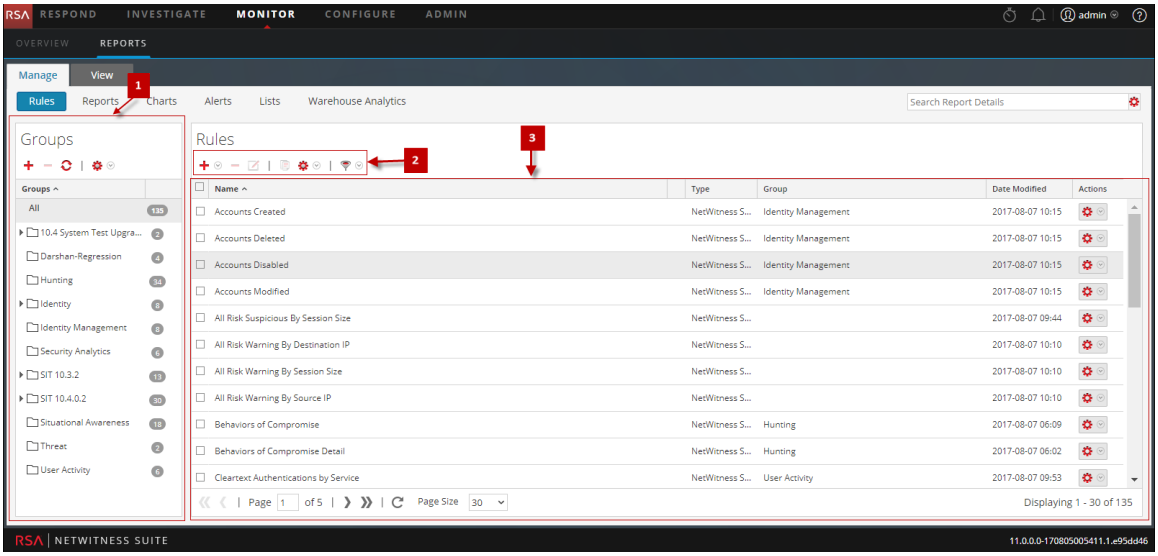
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren einer Regel
- Managen von Listen, Regeln oder Berichten
- Dialogfeld „Regelberechtigungen“
- Ansicht „Regel erstellen“

## Schnellansicht




So greifen Sie auf die Ansicht „Regeln“ zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Rules**.

   Die Ansicht „Regeln“ wird angezeigt.

Die Ansicht „Regeln“ umfasst folgende Bereiche:

1 Regelgruppen

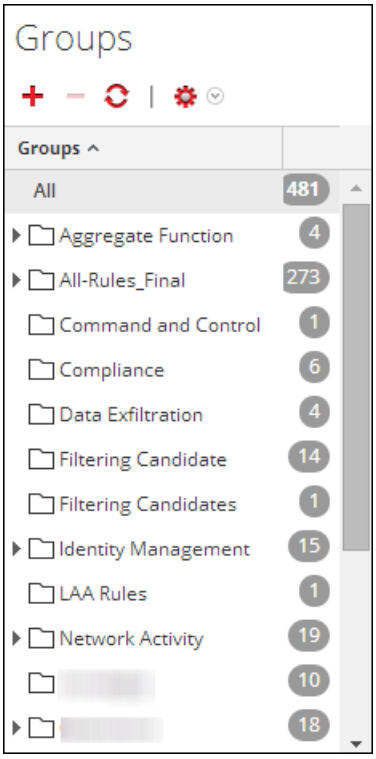
2 Regelliste

3 Symbolleiste Regeln

## Bereich Regelgruppen

Im Bereich Regelgruppen können Sie Regeln mithilfe der Optionen in der Symbolleiste in Gruppen organisieren. Sie können Gruppen und Untergruppen erstellen und diesen Regeln hinzufügen. Sie können auch Regeln gruppieren und zwischen verschiedenen Gruppen verschieben.

Die folgenden Abbildung zeigt die Gruppen im Bereich „Regelgruppen“:




In der folgenden Tabelle sind die Funktionen im Bereich „Regelgruppen“ beschrieben.

| Funktion | Beschreibung |
|---|---|
| + | Mit dieser Option können Sie eine neue Regel zum Reporting-Modul hinzufügen. |
| − | Mit dieser Option können Sie eine oder mehrere Regelgruppen löschen. |
| ↻ | Mit dieser Option wird die Regelgruppenliste aktualisiert. |
| ⚙ | Das Aktionsmenü enthält die folgenden Optionen: „Importieren“, „Exportieren“ und „Berechtigungen“. |

| Funktion | Beschreibung |
|---|---|
| All | Zeigt eine Liste aller Regelgruppen an. |

## Symbolleiste Regeln

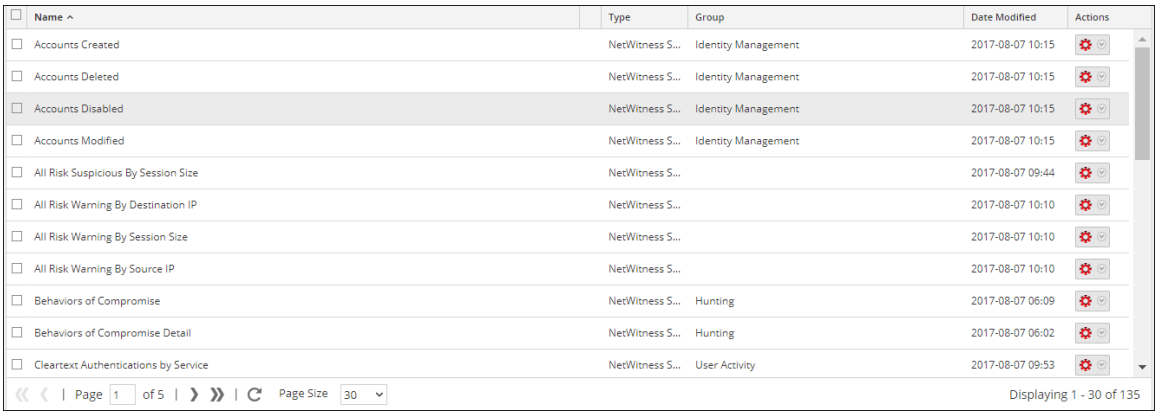
In der Symbolleiste Regeln können Sie Regeln hinzufügen, löschen, bearbeiten und duplizieren. In der nachstehenden Abbildung ist die Symbolleiste dargestellt.

In der folgenden Tabelle sind die Funktionen der Symbolleiste „Regel“ beschrieben.

| Funktion | Beschreibung |
|---|---|
|  | Mit dieser Option können Sie eine neue Regel zum Reporting-Modul hinzufügen. |
|  | Mit dieser Option können Sie eine oder mehrere ausgewählte Regeln löschen. |
|  | Mit dieser Option können Sie eine Regel bearbeiten. |
|  | Mit dieser Option können Sie eine Regel duplizieren. |
|  | Das Aktionsmenü enthält die folgenden Optionen: „Verwenden“, „Importieren“, „Exportieren“ und „Berechtigungen“. |
|  | Mit dieser Option können Sie den Regeltyp auswählen. |

## Bereich Regelliste

In der folgenden Abbildung sind die Regeln im Bereich Regelliste dargestellt.




In der folgenden Tabelle sind die Funktionen des Bereichs „Regelliste“ beschrieben.

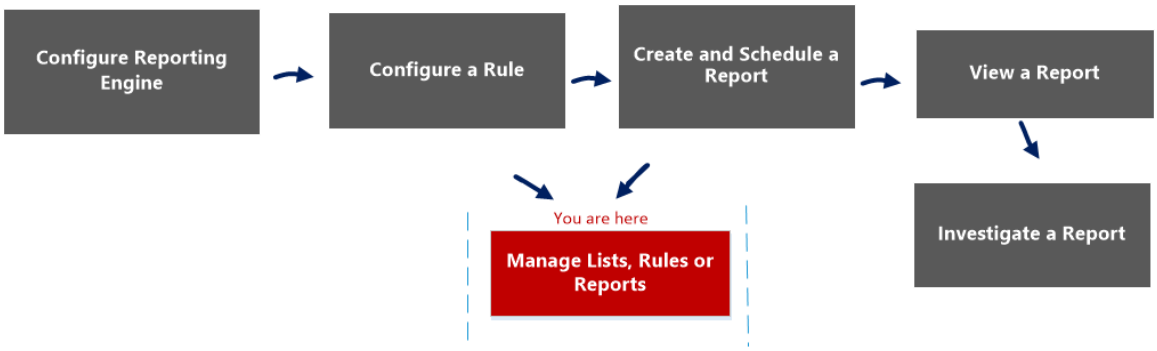
| Funktion | Beschreibung |
|---|---|
| Name | Zeigt den Namen der Regel an, die Sie erstellt oder bearbeitet haben.<br>**Hinweis:** Für das Feld **Name** wird am Ende des Spaltenfelds kein Symbol zur Erweiterung der Spaltengröße angezeigt. Sie müssen die Maus ein wenig nach links bewegen, um das Symbol zur Erweiterung der Spalte zu sehen. |
| Typ | Zeigt den unterstützten Datenbanktyp für die erstellte Regel an. |
| Gruppe | Zeigt die gruppierten Werte an. |
| Änderungsdatum | Zeigt das Datum der letzten Änderung der Regel an. |
| Actions | Zeigt das Aktionsmenü mit den folgenden Optionen an: „Warnmeldung erstellen“, „Diagramm erstellen“, „Bericht erstellen“, „Löschen“, „Bearbeiten“, „Exportieren“ und „Abhängige Elemente“. |

## Dialogfeld „Logo auswählen“

Im Dialogfeld „Logo auswählen“ können Sie ein neues Logo hochladen, das in der Reporting Engine-Ansicht „Serviceskonfiguration“ nicht verfügbar ist, oder ein bestehendes Logo aus der Reporting Engine-Ansicht „Serviceskonfiguration“ auswählen.

# Workflow

Dieser Workflow zeigt das Verfahren zum Managen der Berichte oder Berichtsgruppen.




# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |

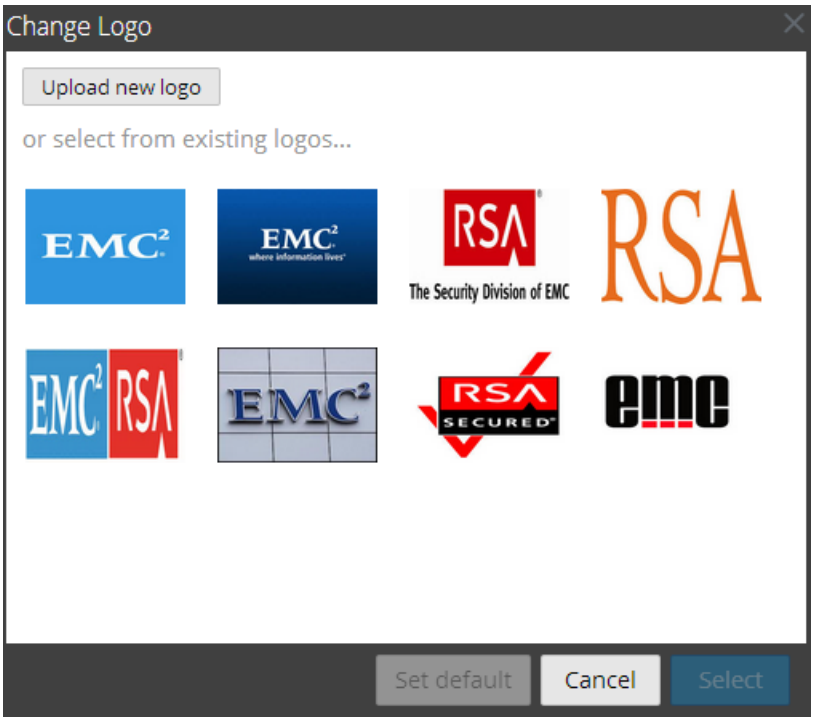
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte* | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Geplante Berichte
- Ansicht Bericht

## Schnellansicht




So rufen Sie dieses Dialogfeld auf:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Wählen Sie im Bereich **Berichtsliste** einen Bericht aus.
4. Klicken Sie auf Geplante Berichte anzeigen
   . Die Registerkarte Geplante Berichte anzeigen wird angezeigt.
5. Wählen Sie einen geplanten Bericht aus und klicken Sie auf Plan bearbeiten
   . Die Ansichtsregisterkarte Einen Bericht planen wird angezeigt.
6. Klicken Sie auf den Bereich **Logo**.
   Das Dialogfeld Logo ändern wird angezeigt.

In der folgenden Tabelle sind die Felder im Dialogfeld „Logo auswählen“ aufgeführt.

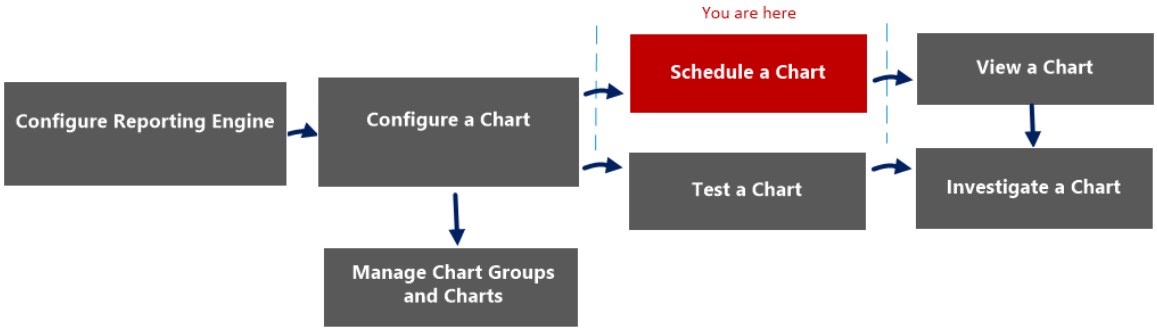
| Feld | Beschreibung |
|---|---|
| Neues Logo hochladen | Klicken Sie auf das Symbol, um ein neues Logo aus einem lokalen Verzeichnis hochzuladen. |

| Feld | Beschreibung |
| --- | --- |
| Auswählen | Wählen Sie ein Logo aus der bestehenden Liste aus, das in einem geplanten Bericht als Logo verwendet wird. |
| Abbrechen | Bricht die Auswahl eines Logos ab und kehrt zum Bereich Planen von Berichten zurück. |
| Als Standard festlegen | Wählen Sie ein Logo aus, um es als Standardlogo einzustellen. |

## Ansicht „Planen eines Diagramms“

In der Ansicht „Planen eines Diagramms“ können Sie ein Diagramm aktivieren oder deaktivieren.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms* | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms | Managen einer Diagrammgruppe und eines Diagramms |

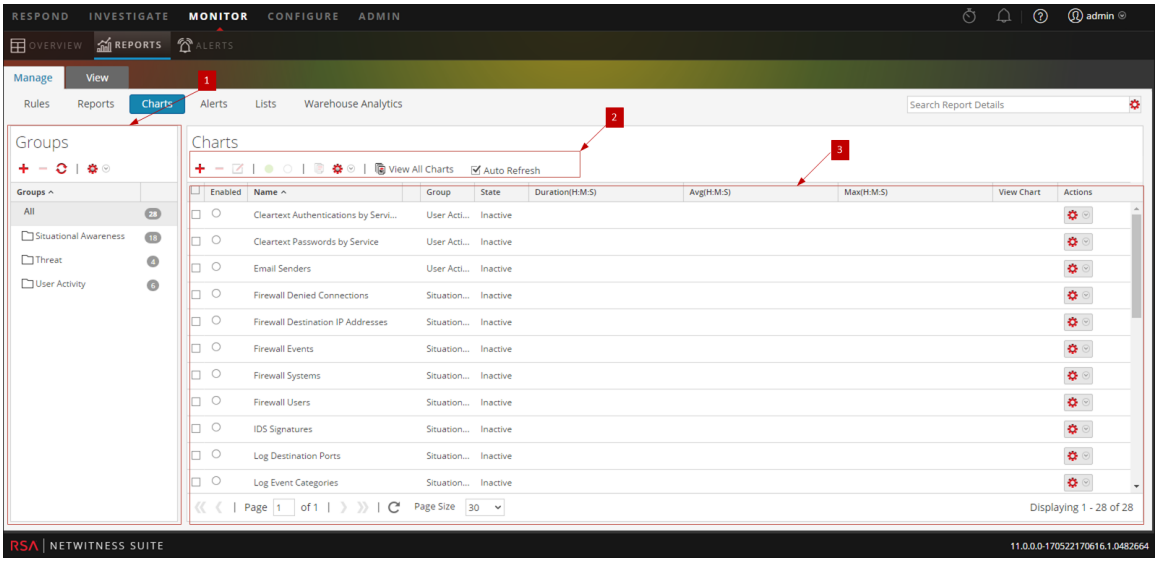
*Sie können diese Aufgaben hier durchführen.

# Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms

# Schnellansicht

Die folgende Abbildung zeigt die Ansicht „Planen eines Diagramms“.




Die Ansicht „Planen eines Diagramms“ umfasst folgende Bereiche:

| | |
|---|---|
| 1 | Bereich Diagrammgruppen |
| 2 | Symbolleiste „Diagramme“ |
| 3 | Bereich Anzeigen eines Diagramms |

## Symbolleiste „Diagramme“

Über die Symbolleiste „Diagramme“ können Sie Diagramme hinzufügen, ändern, löschen, duplizieren, aktivieren, deaktivieren, importieren und exportieren. Sie können auch Zugriffsberechtigungen für Diagramme in einer Gruppe festlegen.


Die Symbolleiste „Diagramme“ umfasst die folgenden Optionen:

| Funktion | Beschreibung |
|---|---|
|  | Fügt ein neues Diagramm zum Reporting-Modul hinzu. |
|  | Löscht eines oder mehrere ausgewählte Diagramme. |
|  | Diagramm bearbeiten. |
|  | Aktiviert die ausgewählten Diagramme. |
|  | Dektiviert die ausgewählten Diagramme. |
|  | Erstellt eine Kopie des ausgewählten Diagramms. |
|  | Bietet die folgenden Optionen: Importieren, exportieren, exportieren als Text und Berechtigungen. |
| Alle Diagramme anzeigen | Zeigt alle ausgeführten Diagramme. |
| Automatisch aktualisieren | Aktualisiert automatisch die Liste der Diagramme. |

## Bereich „Anzeigen eines Diagramms“

Im Bereich „Anzeigen eines Diagramms“ werden alle Diagramme im Tabellen- oder Rasterformat aufgeführt.


In der folgenden Tabelle sind die verschiedenen Spalten im Bereich „Anzeigen eines Diagramms“ aufgeführt.

| Funktion | Beschreibung |
|---|---|
| Aktiviert | - Das Diagramm ist aktiviert.<br>- Das Diagramm ist deaktiviert. |
| Name | Der Name des Diagramms |
| Gruppe | Die Diagrammgruppe, zu der das Diagramm gehört |
| Status | Der Status des Diagramms:<br>• Queued<br>• Abgeschlossen<br>• Fehlgeschlagen |
| Dauer (Std:Min:Sek) | Die Ausführungsdauer des letzten Diagramms |
| Durchschn. (Std:Min:Sek) | Die durchschnittliche Dauer für die Diagrammausführung |
| Max (Std:Min:Sek) | Die maximale Dauer für die Diagrammausführung |
| Diagramm anzeigen | Dies ist ein Hyperlink, der zum Bereich „Anzeigen eines Diagramms“ führt. |
|  | Das Aktionsmenü enthält die folgenden Optionen: Aktivieren, Deaktivieren, Anzeigen, Löschen, Bearbeiten und Exportieren. |

## Bereich „Bericht planen“

Im Bereich „Bericht planen“ können Sie angepasste Berichte planen. Vor dem Planen eines Berichts können Sie eine dynamische Liste der hinzugefügten Services erstellen (mit aktivierter Überschreiben-Option). Weitere Informationen erhalten Sie unter Erzeugen einer Liste aus dem geplanten Bericht unter Erstellen und Planen eines Berichts. Sie verwenden die Liste dann zum Generieren eines Berichts mit Details wie Services und Hostnamen.

# Workflow

Dieser Workflow zeigt das Verfahren zum Erstellen und Planen von Berichten.


# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts* | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |

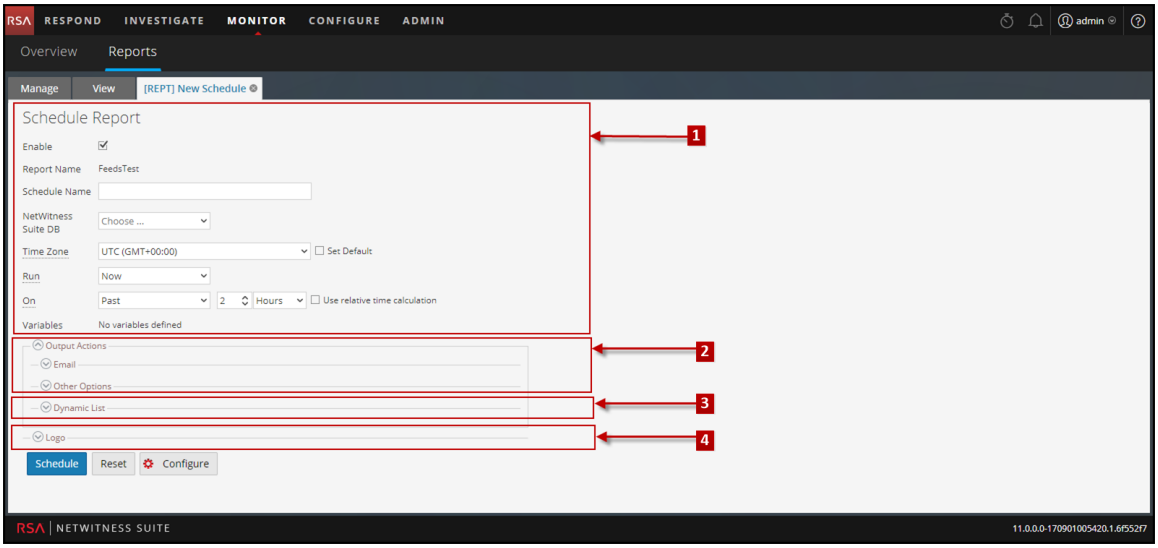
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht
- Ansicht Bericht erstellen
- Ansicht Geplante Berichte

## Schnellansicht




So greifen Sie auf diese Ansicht zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie im Bereich **Berichtsliste** auf  **Bericht planen**.

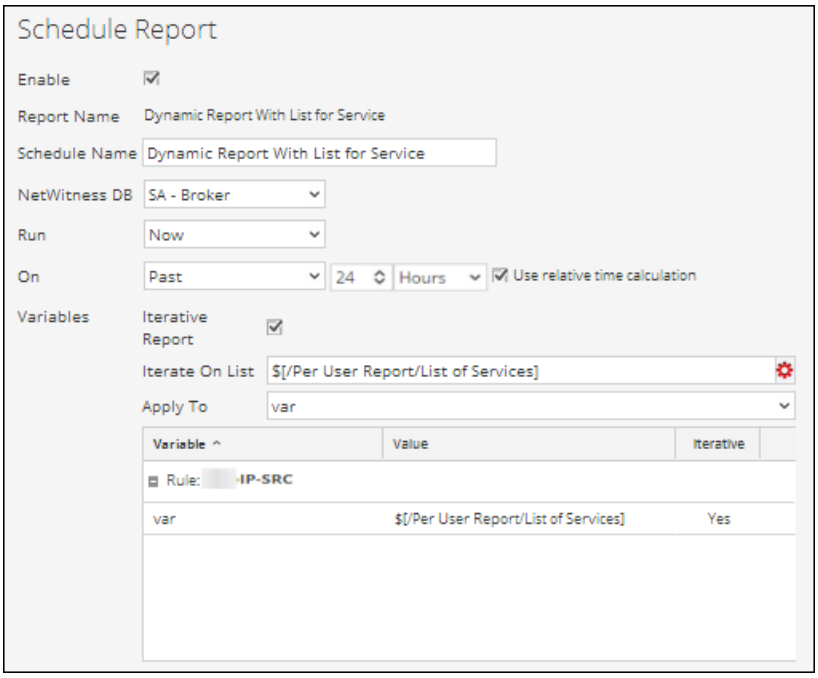
# Funktionen

Die Ansicht „Bericht planen“ besteht aus folgenden Bereichen:

1. Ansicht „Bericht planen“
2. Bereich „Ausgabeaktionen“
3. Bereich „Dynamische Liste“
4. Bereich „Logo“

## Ansicht „Bericht planen“

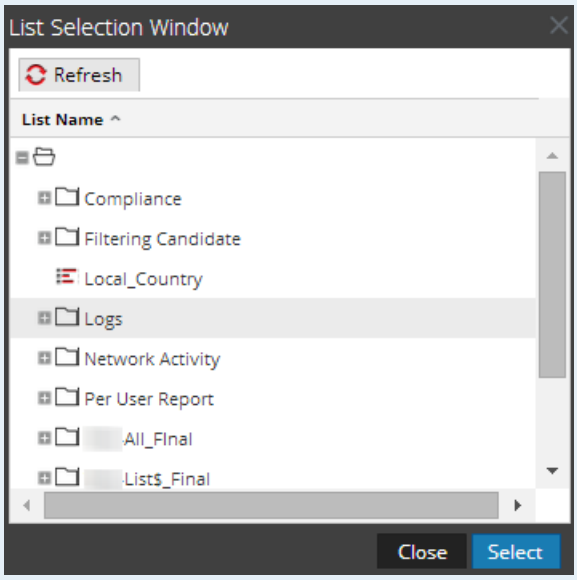
Im Bereich „Bericht planen“ können Sie Berichte planen.




Die folgende Tabelle enthält die Felder des Bereichs „Bericht planen“:

| Feld | Beschreibung |
|---|---|
| Aktivieren | Aktiviert die Berichtsplanungen und führt den Bericht aus. |

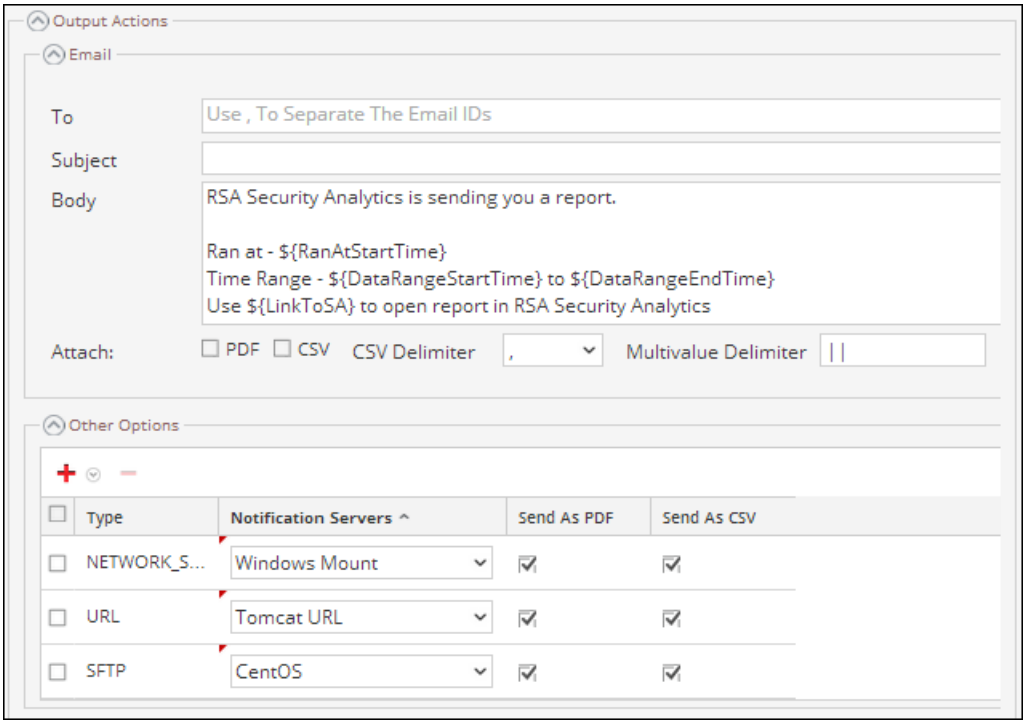
| Feld | Beschreibung |
|---|---|
| Berichtsname | Der Name des Berichts |
| Planname | Der Name der Konfiguration des geplanten Berichts. |
| NetWitness-DB | Die Datenbank kann je nach Auswahl in der Regeldefinition NWDB, IPDB und Warehouse-DB lauten. Wenn der Bericht Regeln von NWDB-, IPDB- und Warehouse-DB-Typen aufweist, werden alle Datenbanktypen oder Regeltypen angezeigt. |
| Warehouse-Ressourcenpool | Wenn der Bericht Warehouse-DB-Regeln aufweist, wird das Drop-down-Feld „Warehouse-Ressourcenpool“ angezeigt, in dem die in diesem Cluster verfügbaren Pools oder Warteschlangen ausgewählt werden können. Wurden für die Reporting Engine keine Pools oder Warteschlangen eingegeben, ist dieses Feld deaktiviert. Weitere Informationen erhalten Sie unter Schritt 5: „Konfigurieren des Aufgabenplaners für eine Reporting Engine“ im *Leitfaden zur Host- und Servicekonfiguration*. |
| Ausführen | Stellt den Planungstyp für die Ausführungskonfiguration bereit:<br>• Ad-hoc-Ausführung<br>• Stündliche Ausführung<br>• Tägliche Ausführung<br>• Wöchentliche Ausführung<br>• Monatliche Ausführung |
| Ein | Der Datenbereich, auf dem die Abfrage ausgeführt wird. |
| Relative Zeitberechnung verwenden | Verwendet die relative Zeitdauer zum Planen eines Berichts. |
| Iterativer Bericht | Aktivieren Sie dieses Kontrollkästchen, um einen Bericht für den ausgewählten Listenwert zu planen. |

| Feld | Beschreibung |
|---|---|
| Iterieren für Liste  | Klicken Sie auf diese Schaltfläche, um zum Listenauswahlbereich zu navigieren und eine Liste auszuwählen. In der folgenden Abbildung ist dieser Bereich dargestellt:<br>  <br>Der Listenauswahlbereich besteht aus einer Sammlung von Listen. Die Reporting Engine unterhält eine aktive Liste der verfügbaren Listennamen, indem eine kontinuierliche Synchronisierung mit der verknüpften Sammlung vorgenommen wird. |
| Anwenden auf | Wendet Listenwerte auf die ausgewählte Variable an, |
| Variablen | Zeigt die Regelvariablen zusammen mit den zugehörigen Werten und den iterativen Eigenschaften des Berichts an.<br>**Hinweis:** Abhängig von der ausgewählten Regel bei der Erstellung des Berichts können Sie die für diese Regel definierten dynamischen Variablen im Feld **Variablen** des Bereichs „Bericht planen“ einsehen. Test-Country ist zum Beispiel die Regel mit der dynamischen Variable var. |
| Schedule | Plant den Bericht. |

| Feld | Beschreibung |
|---|---|
| Zurücksetzen | Setzt den geplanten Bericht zurück. |
| Konfigurieren | Ändern der Reporting Engine-Konfigurationsdetails im Thema „Allgemeine Registerkarte Reporting Engine“ im *Leitfaden zur Host- und Servicekonfiguration*.<br><br>**Hinweis:** Diese Schaltfläche wird nur im Bereich „Bericht planen“ angezeigt, wenn Sie über die Zugriffsberechtigungen „Gerät managen“ des Reporting-Moduls verfügen. |

## Bereich „Ausgabeaktionen“

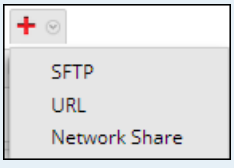
Im Bereich „Ausgabeaktionen“ werden Ausgabeaktionen zur Benachrichtigung des E-Mail-Empfängers bei Abschluss der Berichtsausführung festgelegt. Außerdem werden Berichte je nach Ihrer Auswahl im PDF- oder CSV-Format an die E-Mail angehängt.




Die folgende Tabelle enthält die Felder des Bereichs Ausgabeaktionen:

| Feld | Beschreibung |
|---|---|
| Aufgabe | Eine kommagetrennte Liste von E-Mail-Adressen, die die Ausgabe erhalten sollen. |

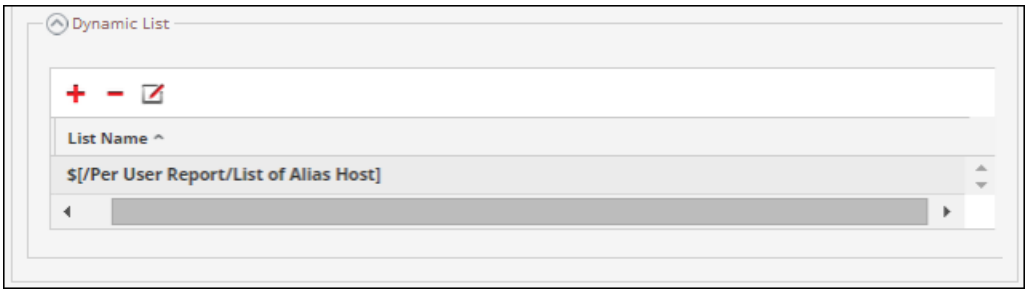
| Feld | Beschreibung |
|---|---|
| Betreff | Der Betreff für die E-Mail. |
| Body | Der Text der E-Mail. Standardmäßig ist hier vordefinierter Text enthalten, der Variablen für die Metadaten entsprechend dem generierten Bericht aufweist.<br>In der Reporting Engine werden diese Variablen durch tatsächliche Werte ersetzt.<br><br>• `${RanAtStartTime}`: Die Startzeit des Berichts<br>• `${DataRangeStartTime}`: Die Startzeit des Datenzeitbereichs<br>• `${DataRangeEndTime}`: Die Endzeit des Datenzeitbereichs<br>• `${LinkToSA}` : Der Link zum NetWitness SuiteHost in der E-Mail, über den der Bericht in der NetWitness Suite Benutzeroberfläche geöffnet wird.<br>• `${ReportName}`: Der Name des Berichts<br>• `${DataSource}`: Der Name der Datenquelle |
| Anbinden: | Das Ausgabeformat, in dem der Bericht an die E-Mail angehängt wird, wie z. B. PDF oder CSV. Dies kann im Dialogfeld Bericht planen konfiguriert werden. |

| Feld | Beschreibung |
|---|---|
| CSV-Trennzeichen | Das standardmäßige CSV-Trennzeichen ist ein Komma (,). Wenn der CSV-Inhalt selber Kommas enthält, müssen Sie ein eindeutiges Trennzeichen definieren, damit der Inhalt im ursprünglichen Format gespeichert werden kann. Beispiel: Der Bericht soll als CSV-Datei gespeichert werden und enthält eine Spalte namens msg. Der msg-Inhalt sieht wie folgt aus: `ASA-SSM-CSC-20 Module in slot 1," application reloading ""CSC SSM""," version ""6.2.1599.0"" CSC SSM scan services are reloading because of a pattern file or configuration update`<br><br>Der obige Inhalt ist aufgrund der Kommas auf drei Spalten verteilt. Um dies zu vermeiden, müssen Sie ein anderes Trennzeichen angeben, wie zum Beispiel ein Pipe-Zeichen: \|.<br><br>**Hinweis:** Um die CSV-Datei in Microsoft Excel zu importieren, verwenden Sie in Excel die Optionen Daten > Aus Text. Beim Import der CSV-Datei müssen Sie den Dateityp der zu importierenden Datei als „Getrennt“ angeben und das gleiche Trennzeichen verwenden, das Sie zum Generieren der CSV-Datei verwendet haben. |
| Trennzeichen für mehrere Werte | Die Daten in Feldern mit mehreren Werten werden durch das hier angegebene Trennzeichen getrennt. Das standardmäßige Trennzeichen für mehrere Werte sind zwei Pipe-Zeichen (\|\|). |
| Andere Optionen | Sie können einen in ((RE}} konfigurierten SFTP-, URL- oder Netzwerkfreigabe-Speicherort angeben und den Bericht je nach Anforderung im PDF- oder CSV-Format senden. |
|  | Wählen Sie diese Option aus, um den Bericht an den in der Ansicht „Konfiguration“ des Reporting Engine-Services konfigurierten SFTP-, URL- oder Netzwerkfreigabe-Speicherort zu senden. |

| Feld | Beschreibung |
|---|---|
| Typ | Der Typ der gewählten Ausgabeaktion. Beispiel: SFTP, URL oder Netzwerkfreigabe. |
| Ausgabeaktionen | Wählen Sie den in der Ansicht „Konfiguration“ des Reporting Engine-Services konfigurierten SFTP-, URL- oder Netzwerkfreigabenamen aus. |
| Als PDF senden / Als CSV senden | Wählen Sie diese Optionen, um den Bericht im PDF-, CSV- oder in beiden Formaten an den konfigurierten Benachrichtigungsserver zu senden (SFTP, URL oder Netzwerkfreigabe). |

## Bereich „Dynamische Liste“

Der Bereich Dynamische Liste füllt die erstellten Listen aus und Sie haben dort die Möglichkeit, Listen hinzuzufügen, zu bearbeiten oder zu löschen. Die Liste wird basierend auf dem geplanten Bericht generiert, der im Modul Listen angezeigt werden kann.




Die folgende Tabelle enthält die Elemente des Bereichs „Liste erzeugen“:

| Vorgang | Beschreibung |
|---|---|
| + | Fügt dem Bericht eine neue Liste hinzu. |
| − | Löscht alle dem Bericht hinzugefügten Listen. |
| ✎ | Zeigt das Dialogfeld Liste erzeugen an. |
| Listenname | Der Name der Liste, die aus dem Listenauswahlbereich ausgewählt wurde. Weitere Informationen zum Bereich „Listenauswahl“ erhalten Sie im Dialogfeld Bereich „Liste erzeugen“. |

## Bereich „Logo“

Im Bereich „Logo“ ist das Standardlogo aus dem Bereich „Logo auswählen“ enthalten. Weitere Informationen zur Auswahl eines Logos in diesem Bereich finden Sie unter „Managen“ und „Ein Berichtslogo auswählen“ unter Managen von Listen, Regeln oder Berichten.

Sie können das Standardlogo für eine Reporting Engine festlegen. Dies ist das Logo, das in den erzeugten Berichten verwendet wird. Weitere Informationen zur Auswahl eines Logos finden Sie unter Dialogfeld „Logo auswählen“

**Hinweis:** Wenn Sie kein Logo ausgewählt haben, wird im Bericht das RSA-Standardlogo verwendet. Die Option **Als PDF speichern** für bereits vorher ausgeführte Berichte unterstützt kein neues Kundenlogo. Stattdessen wird das RSA-Standardlogo angezeigt, wenn das Kundenlogo in der Ansicht Bericht planen angezeigt werden muss.

## Ansicht Geplante Berichte

In der Ansicht „Geplante Berichte“ können Sie geplante Berichte erstellen, anzeigen und managen.

# Workflow

Dieser Workflow zeigt das Verfahren zum Erstellen und Planen von Berichten.


# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts* | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen. | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

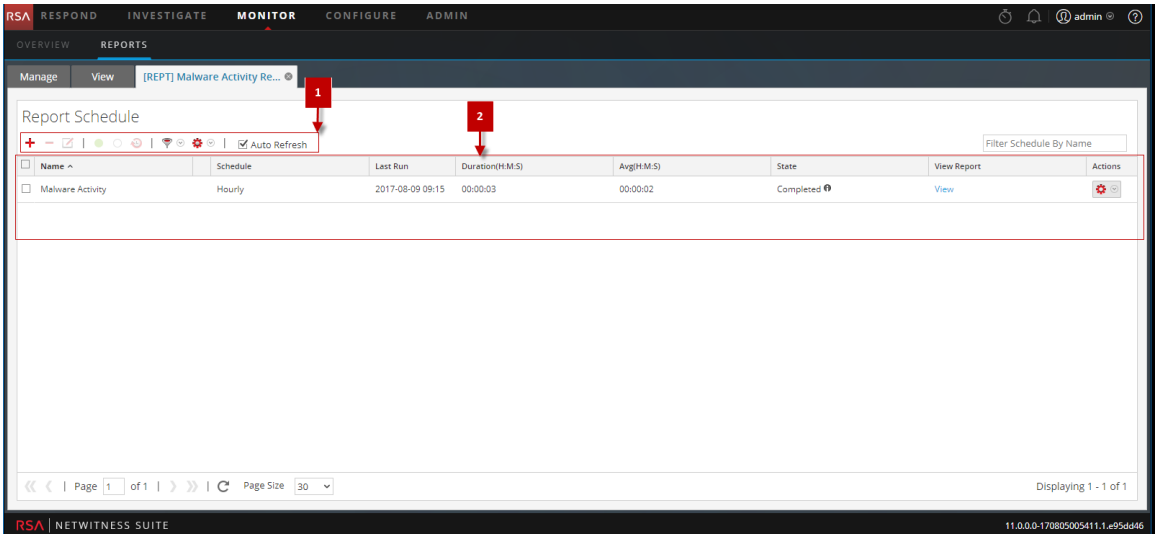
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte* | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Erstellen und Planen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht erstellen
- Ansicht Bericht
- Bereich „Bericht planen“
- Dialogfeld „Berichtberechtigungen“

## Schnellansicht




So greifen Sie auf diese Ansicht zu:

1. Wählen Sie **Monitor > Berichte**.

   Die Registerkarte Managen wird angezeigt.

2. Klicken Sie auf **Berichte**.

Die Ansicht Berichte wird angezeigt.

3. Führen Sie im Bereich **Berichtsliste** einen der folgenden Schritte aus:

   - Klicken Sie auf  **Geplante Berichte anzeigen**.
   - Klicken Sie auf die Spalte **#Planungen**.

# Funktionen

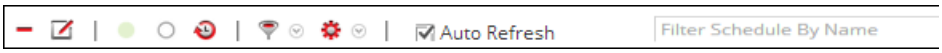
Die Ansicht „Geplante Berichte anzeigen“ enthält folgende Bereiche:

1 „Geplante Berichte“-Symbol

2 Bereich „Liste geplanter Berichte“

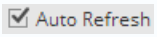
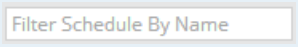
## „Geplante Berichte“-Symbol

„Geplante Berichte“ enthält Optionen zum Hinzufügen, Ändern und Löschen des geplanten Berichts sowie zum Aktivieren oder Deaktivieren der ausgewählten Ausführungskonfiguration.




In der folgenden Tabelle sind die in der Symbolleiste „Geplante Berichte“ verfügbaren Vorgänge aufgeführt.

| Vorgang | Beschreibung |
|---|---|
|  | Erstellen einer neuen Berichtplanung: |
|  | Löscht die ausgewählte Berichtplanung. |
|  | Ermöglicht die Bearbeitung der ausgewählten Berichtplanung.<br>**Hinweis:** Doppelklicken Sie auf eine gewünschte Berichtplanung, um sie zu bearbeiten. |
|  | Aktiviert die ausgewählte Berichtplanung. |
|  | Deaktiviert die ausgewählte Berichtplanung. |

| Vorgang | Beschreibung |
|---|---|
|  | Zeigt den Verlauf des geplanten Berichts an. |
|  | Filtert Planungen je nach Planungstyp (z. B.: Ad-hoc). |
|  | Ermöglicht das Festlegen von Berechtigungen für den ausgewählten geplanten Bericht. |
|   | Aktualisiert die Liste der geplanten Berichte automatisch. |
|   | Sucht nach Planungen anhand des Planungsnamens. |

## Bereich „Liste geplanter Berichte“

Im Bereich „Liste geplanter Berichte“ werden die geplanten Berichte in tabellarischer Form aufgeführt.

In der folgenden Tabelle sind die Spalten im Bereich „Liste geplanter Berichte“ aufgeführt:

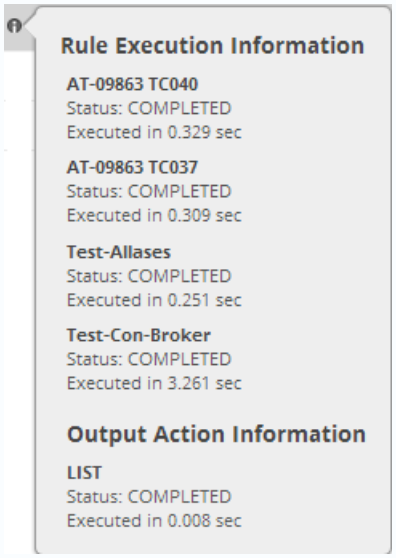
| Spalte | Beschreibung |
|---|---|
| Name | Der Name des geplanten Berichts. |

| Spalte | Beschreibung |
| --- | --- |
| Schedule | Der Typ der Planung für die Ausführungskonfiguration:<br>• Ad-hoc-Ausführung<br>• Stündliche Ausführung<br>• Tägliche Ausführung<br>• Wöchentliche Ausführung<br>• Monatliche Ausführung |
| Letzte Ausführung | Zeigt an, wann der Bericht zuletzt ausgeführt wurde. |
| Dauer (Std:Min:Sek) | Zeigt die Dauer für die letzte Ausführung des Berichts |
| Durchschn. (Std:Min:Sek) | Zeigt die durchschnittliche Dauer der Ausführung an. |

| Spalte | Beschreibung |
| --- | --- |
| State | Gibt den Status des geplanten Berichts an.<br>• Geplant: Wenn ein Bericht für die stündliche, tägliche, wöchentliche, monatliche oder eine spätere Ausführung geplant wird, wird der Status des Berichts für die erste Ausführung als „Geplant“ angezeigt.<br>• In der Warteschlange: Wenn die Ausführung eines Bericht noch aussteht, wird als Status des Berichts In der Warteschlange angezeigt.<br>• „Wird ausgeführt“: Wenn der geplante Bericht verarbeitet wird, wird als Status des Berichts „Wird ausgeführt“ angezeigt.<br>• Teilweise: Wenn in einem Bericht mit mehreren Regeln die Ausführung einer einzigen Regel, eine Ausgabeaktion oder die Erstellung einer PDF-/CSV-Datei fehlgeschlagen ist, wird als Status des Berichts Teilweise angezeigt. Beispiel: In einem Bericht mit fünf Regeln werden vier Regeln erfolgreich ausgeführt und eine schlägt |

| Spalte | Beschreibung |
| --- | --- |
| | fehl. Als Status wird daher „Teilweise“ angezeigt.<br>• Failed: Wenn in einem Bericht mit mehreren Regeln alle Regelausführungen fehlschlagen, wird der Status des Berichts als Fehlgeschlagen angezeigt.<br>• Abgeschlossen: Wenn eine Berichtplanung erfolgreich ausgeführt wird, wird als Status des Berichts „Abgeschlossen“ angezeigt.<br>• Abgebrochen: Wenn eine Anforderung zum Abbruch erfolgreich ausgeführt wurde, wird als Status des Berichts „Abgebrochen“ angezeigt.<br>**Hinweis:** Die Option Abbrechen funktioniert bei Warehouse Analytics-Jobs möglicherweise nicht. Sie müssen den Job manuell beenden. Im Folgenden sind die Schritte zum Beenden des Jobs aufgeführt:<br>**Für MapR**:<br>1. Rufen Sie die Job-ID aus den Jobprotokollen ab.<br>2. Melden Sie sich bei der Jobtracker-Benutzeroberfläche an und suchen Sie unter |

| Spalte | Beschreibung |
| --- | --- |
| | „Ausgeführte Jobs“ nach der zu beendenden Job-ID.<br>Beispiel-URL: http://<job-tracker-host>:50030/jobtracker.jsp<br>3. Beenden Sie die Job-ID.<br>• Wählen Sie die Job-ID unter „Zur Zeit ausgeführte Jobs“ und klicken Sie auf „Ausgewählte Jobs beenden“.<br>(oder)<br>• Klicken Sie auf den Link der Job-ID, scrollen Sie nach unten und klicken Sie auf den Link „Diesen Job beenden“.<br>• Inaktiv: Wenn eine Berichtplanung deaktiviert ist, wird als Status des Berichts Inaktiv angezeigt.<br>• Nicht verfügbar: Wenn die Ausführungsinformationen zu einer Berichtplanung nicht verfügbar sind, wird der Status des Berichts als nicht verfügbar angezeigt. |

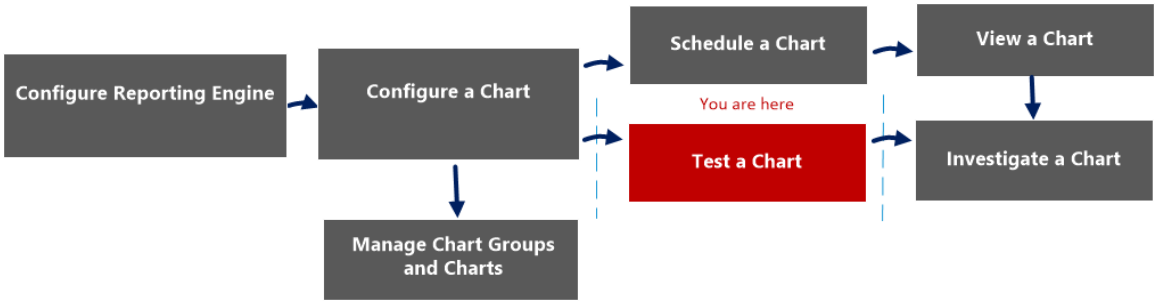
| Spalte | Beschreibung |
| --- | --- |
|  | Klicken Sie, um die Regelausführungsinformationen und Informationen zur Ausgabeaktion anzuzeigen. Diese Pop-up-Nachricht informiert über den Status mehrerer Regeln in einem Bericht und die Zeit für die Ausführung.<br><br>**Hinweis:** Sie können die Informationen zur Regelausführung und Ausgabeaktion für einen geplanten Bericht mit dem Status **Abgeschlossen**, **Wird ausgeführt**, **Teilweise** oder **Fehlgeschlagen** anzeigen. Standardmäßig ist „Ausgabeaktionen für abgeschlossenen Bericht“ auf der Seite „Reporting Engine-Konfiguration“ aktiviert, sodass Sie eine E-Mail bekommen, wenn der Berichtsstatus „Abgeschlossen“ ist. Um eine E-Mail zu Berichten mit dem Status **Fehlgeschlagen** oder **Teilweise** zu erhalten, müssen Sie diese Option deaktivieren. |

| Spalte | Beschreibung |
| --- | --- |
| Bericht anzeigen | Klicken Sie hierauf, um die Regelausführungsinformationen im Bereich Bericht anzeigen anzuzeigen. Für einen geplanten Bericht mit dem Status „Wird ausgeführt“ können Sie die Regelausführungsinformationen anzeigen. |

## Ansicht „Testen eines Diagramms“

Im Bereich „Testen eines Diagramms“ können Sie Diagramme anzeigen und testen.

# Workflow




# Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms* | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms | Managen einer Diagrammgruppe und eines Diagramms |

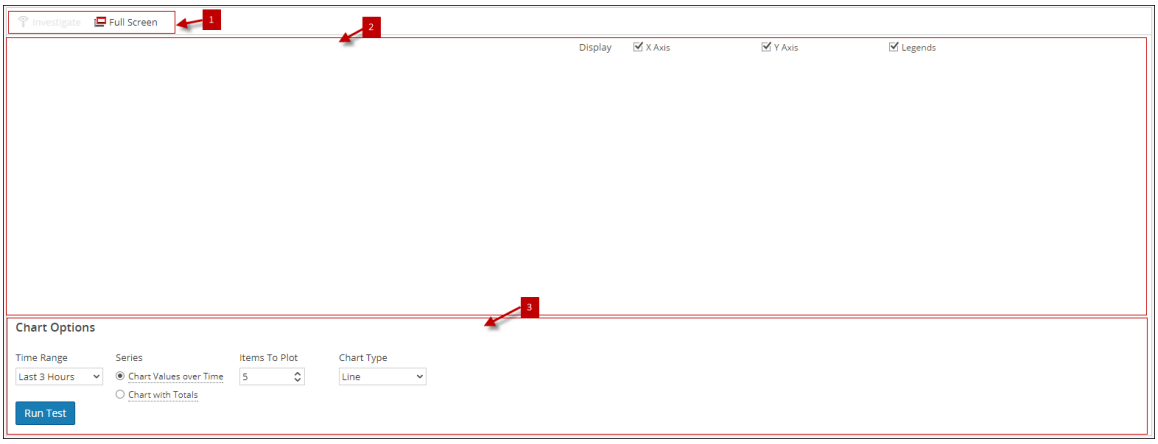
*Sie können diese Aufgaben hier durchführen.

# Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms
- Anzeigen eines Diagramms
- Testen eines Diagramms

# Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




Die Ansicht „Diagramm testen“ besteht aus folgenden Bereichen:

| | |
|---|---|
| 1 | Symbolleiste „Diagramme“ |
| 2 | Bereich Diagrammausgabe |
| 3 | Bereich Diagrammoptionen |

## Symbolleiste „Diagramme“

Mit der Symbolleiste „Diagramme“ können Sie ein bestimmtes Diagramm untersuchen und in den Vollbildmodus wechseln.


| Funktion | Beschreibung |
|---|---|
| Untersuchung | Führt eine Untersuchung im ausgewählten Diagramm durch. |
| Vollbild | Zeigt das Diagramm als Vollbild an. |

## Bereich Diagrammausgabe

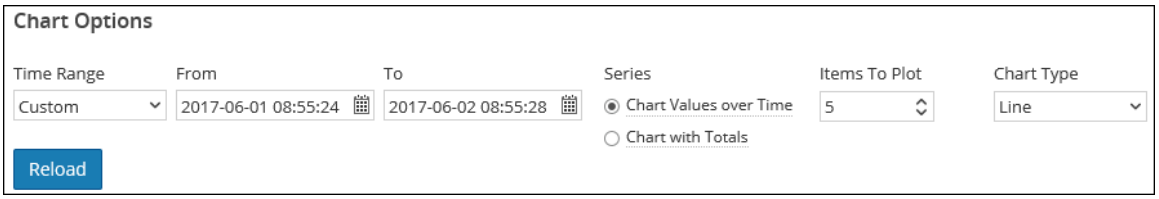
Im Bereich Diagrammausgabe werden die Informationen für die ausgewählten Zeitdiagrammoptionen im Diagrammformat angezeigt.

In der folgenden Tabelle sind die Funktionen der Ansicht „Testen eines Diagramms“ aufgeführt und erläutert.

| Funktion | Beschreibung |
|---|---|
| Video | Hier können Sie die anzuzeigenden Werte auswählen und haben die folgenden Optionen: X-Achse, Y-Achse und Legenden. |
| X-Achse | Zeigt die Sitzungsanzahl an. |
| Y-Achse | Zeigt die tatsächliche Ausgabe an. |
| Legenden | Zeigt die Liste der Variablen, die im Diagramm vorkommen, an. |

## Bereich Diagrammoptionen

In der folgenden Abbildung des Bereichs „Diagrammoptionen“ werden die Felder zu Zeitbereich, Serie und Diagrammtyp angezeigt, mit denen Sie die Diagrammanzeige konfigurieren können.




In der folgenden Tabelle sind die Felder im Bereich „Diagrammoptionen“ mit einer Beschreibung aufgelistet.

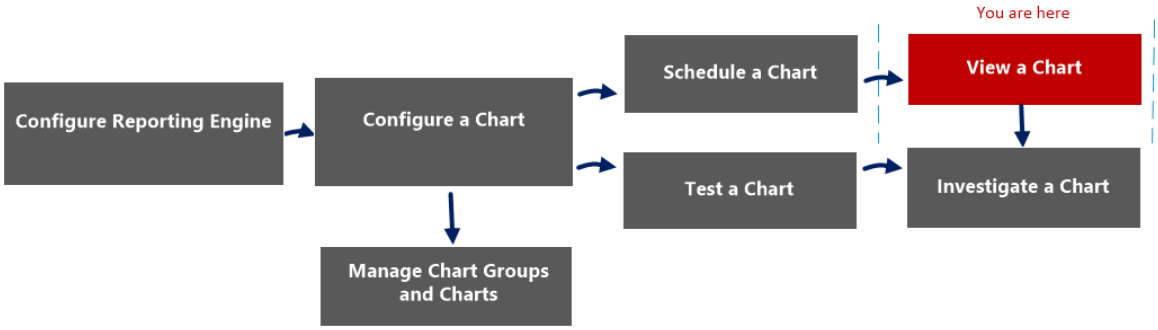
| Funktion | Beschreibung |
|---|---|
| Zeitbereich | Der Standardzeitbereich ist „Letzte 3 Stunden“. Sie können jedoch in der Drop-down-Liste einen anderen Wert auswählen, z. B. „Letzte Stunde“ oder „Letzte 6 Stunden“. Hierbei handelt es sich um die vordefinierten Werte. Oder Sie können den Wert durch Auswahl der Option „Letzte N Tage“ oder „Benutzerdefiniert“ anpassen. |
| Von | Startdatum und -uhrzeit (nur für benutzerdefinierte Option) |
| An | Enddatum und -uhrzeit (nur für benutzerdefinierte Option) |

| Funktion | Beschreibung |
| --- | --- |
| Serie | Im Feld Serie werden Ihnen zwei Optionen angeboten:<br>• Diagramm mit Werten im Zeitverlauf zeichnen: Erstellt das Diagramm für den gesamten ausgewählten Zeitraum.<br>• Diagramm mit Summen zeichnen: Stellt eine Zusammenfassung der Daten für den ausgewählten Datumsbereich dar. |
| Zu zeichnende Elemente | Die maximale Anzahl der Ereignisse, die der Benutzer auf dem Diagramm anzeigen möchten. |
| Diagrammtyp | Gibt an, ob die Daten als Flächen-, Balken-, Säulen-, Linien- oder Schrittlinien-, Schrittbereich-, Spline-Bereich oder Spline-Diagramm dargestellt werden sollen. |

## Bereich Anzeigen eines Diagramms

Im Bereich „Anzeigen eines Diagramms“ können Sie Diagramme anzeigen und managen. Es gibt Optionen zum Filtern und Sortieren der Informationen im Diagramm sowie Optionen für den Typ des Diagramms, die Anzahl der darzustellenden Elemente und die Diagrammanzeigewerte oder Gesamtwerte. Beim Anzeigen eines Diagramms können Sie die im Diagramm dargestellten Sitzungen im Modul Investigation öffnen und das Diagramm als PDF-Datei speichern.

# Workflow




# Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms* | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms | Managen einer Diagrammgruppe und eines Diagramms |

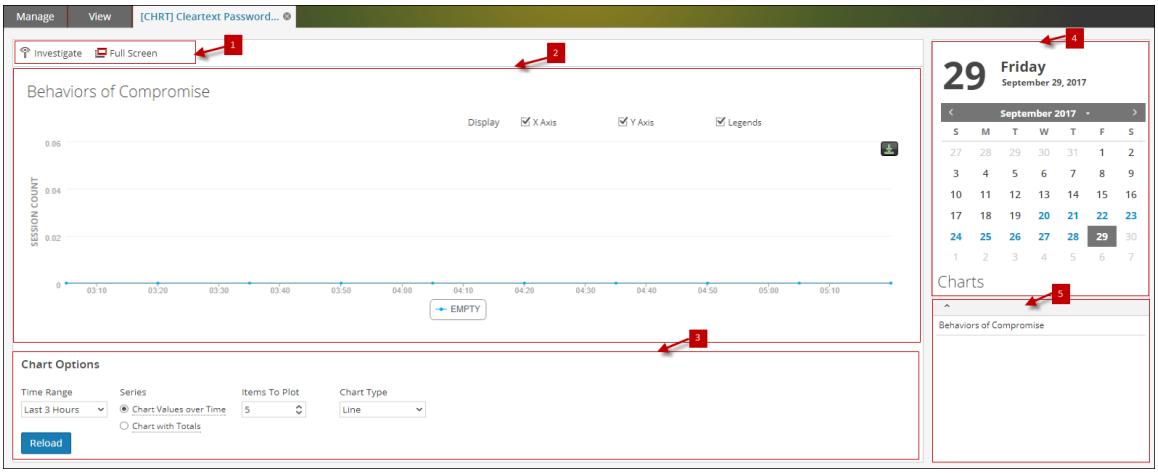
*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms
- Anzeigen eines Diagramms

## Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




Der Bereich Anzeigen eines Diagramms umfasst folgende Bereiche:

| | |
|---|---|
| 1 | Symbolleiste „Diagramme“ |
| 2 | Bereich Diagrammausgabe |
| 3 | Bereich Diagrammkalender |
| 4 | Bereich Diagrammoptionen |
| 5 | Liste Ausgeführte Diagramme |

## Symbolleiste „Diagramme“

Die Symbolleiste „Diagramme“ enthält Optionen für das Untersuchen sowie das Anzeigen des Diagramms auf einem anderen Bildschirm.


In der folgenden Tabelle sind die Optionen der Symbolleiste „Diagramme“ aufgelistet.

| Vorgang | Beschreibung |
|---|---|
| Untersuchung | Untersucht die Diagrammdetails näher. |
| Vollbild | Zeigt das Diagramm als Vollbild an. |

## Bereich Diagrammausgabe

Im Bereich Diagrammausgabe wird das Diagramm mit der Sortierung auf der Y-Achse, der Zeit auf der X-Achse und Legenden angezeigt.

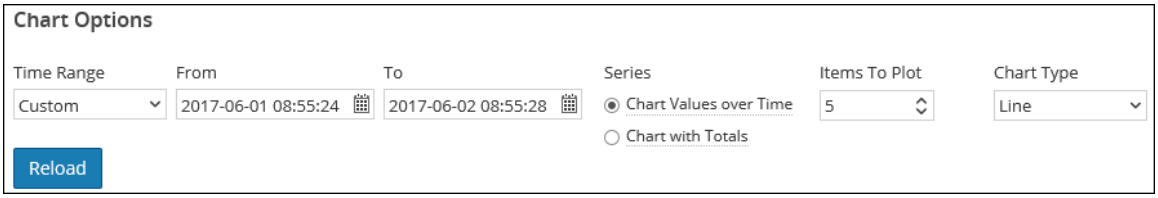
**Hinweis:** Mit dem Symbol im Bereich „Diagrammausgabe“ können Sie das Diagramm als PDF speichern.

## Bereich Diagrammkalender

Im Bereich „Diagrammkalender“ wird wie in der folgenden Abbildung dargestellt eine Diagrammliste für das Datum angezeigt, das Sie im Kalender auswählen.


## Bereich Diagrammoptionen

Im Bereich „Diagrammoptionen“ werden die Felder zu Zeitbereich, Serie und Diagrammtyp angezeigt, mit denen Sie die Diagrammanzeige konfigurieren können.




In der folgenden Tabelle sind die Felder im Bereich Diagrammoptionen aufgelistet.

| Feld | Beschreibung |
|---|---|
| Zeitbereich | Der Standardzeitbereich ist „Letzte 3 Stunden“. Sie können jedoch in der Drop-down-Liste einen anderen Wert auswählen, z. B. „Letzte Stunde“ oder „Letzte 6 Stunden“. Hierbei handelt es sich um die vordefinierten Werte. Oder Sie können den Wert durch Auswahl der Option „Letzte N Tage“ oder „Benutzerdefiniert“ anpassen.<br><br>**Hinweis:** Der von Ihnen ausgewählte Zeitraum für ein Diagramm wird gespeichert. Wenn Sie dasselbe Diagramm das nächste Mal öffnen, wird der gespeicherte Zeitbereich angezeigt. Dieses Verhalten gilt nicht für die benutzerdefinierte Option. |
| Von | Startdatum und -uhrzeit (nur für benutzerdefinierte Option) |
| An | Enddatum und -uhrzeit (nur für benutzerdefinierte Option) |
| Serie | Im Feld Serie werden dem Benutzer zwei Optionen angeboten:<br>• Diagramm mit Werten im Zeitverlauf zeichnen: Erstellt das Diagramm für den gesamten ausgewählten Zeitraum.<br>• Diagramm mit Summen zeichnen: Stellt eine Zusammenfassung der Daten für den ausgewählten Datumsbereich dar. |
| Zu zeichnende Elemente | Die maximale Anzahl der Ereignisse, die der Benutzer auf dem Diagramm anzeigen möchten. |
| Diagrammtyp | Der Typ des Diagramms, das dargestellt werden soll. Flächen-, Balken-, Säulen-, Linien- oder Schrittlinien-, Schrittbereich-, Spline-Bereich oder Spline-Diagramm. |

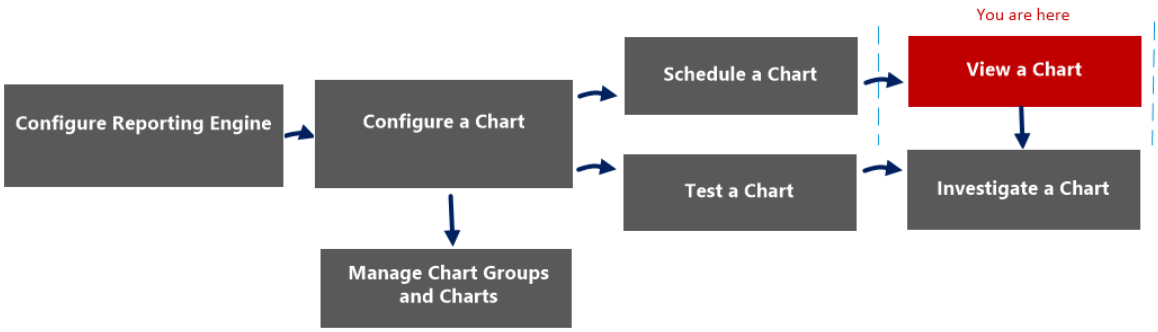
## Listenbereich „Ausgeführte Diagramme“

Im Listenbereich „Ausgeführte Diagramme“ werden alle Ausführungen eines bestimmten Diagramms für das ausgewählte Datum angezeigt. Wenn Sie auf eine Diagrammausführung doppelklicken, wird das Diagramm im Bereich Diagrammausgabe geladen. Standardmäßig wird im Bereich „Diagrammausgabe“ das zuletzt ausgeführte Diagramm angezeigt.

## Ansicht „Alle Diagramme anzeigen“

In der Ansicht „Alle Diagramme anzeigen“ können Sie Diagramme anzeigen, drucken, speichern und als E-Mail versenden.

# Workflow




# Was möchten Sie tun?

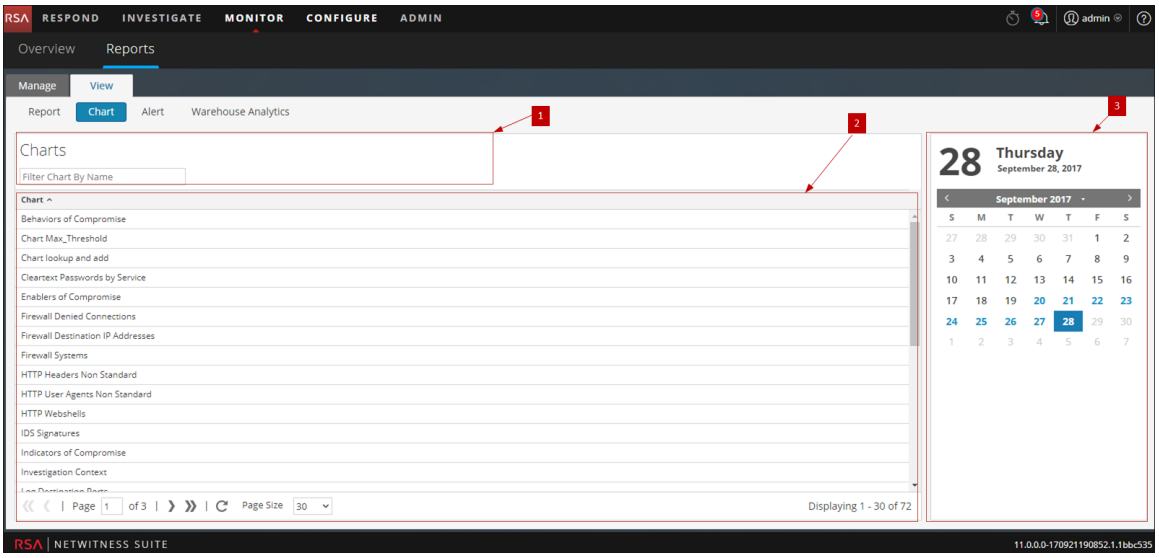
| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen finden Sie unter „Konfigurieren der Reporting Engine“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Konfigurieren eines Diagramms | Konfigurieren eines Diagramms |
| Administrator/Analyst | Planen eines Diagramms | Planen eines Diagramms |
| Administrator/Analyst | Anzeigen eines Diagramms* | Anzeigen eines Diagramms |
| Administrator/Analyst | Testen eines Diagramms | Testen eines Diagramms |
| Administrator/Analyst | Untersuchen eines Diagramms | Untersuchen eines Diagramms |
| Administrator/Analyst | Managen einer Diagrammgruppe und eines Diagramms | Managen einer Diagrammgruppe und eines Diagramms |

*Sie können diese Aufgaben hier durchführen.

# Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren eines Diagramms
- Planen eines Diagramms
- Anzeigen eines Diagramms

# Schnellansicht




Der Bereich „Alle Diagramme anzeigen“ umfasst folgende Bereiche:

| | |
|---|---|
| 1 | Diagrammsymbolleiste |
| 2 | Bereich Diagrammausgabe |
| 3 | Bereich Diagrammkalender |

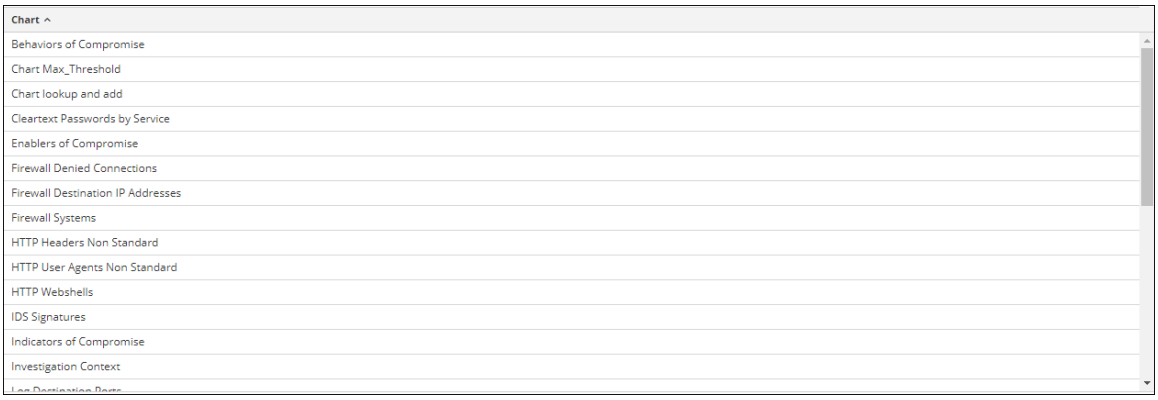
## Diagrammsymbolleiste

In der folgenden Tabelle sind die Optionen in der Symbolleiste „Alle Diagramme anzeigen“ aufgeführt:

| Vorgang | Beschreibung |
|---|---|
| Filter Chart By Name | Sucht basierend auf dem Namen des Diagramms für einen ausgewählten Kalendertag nach Zeitplänen. |

## Bereich Diagrammausgabe

Im Bereich Diagrammausgabe wird das Diagramm mit dem Namen des Zeitplans angezeigt.




| Funktion | Beschreibung |
|---|---|
| Diagramm | Dieses Feld zeigt alle erfolgreich ausgeführten Diagramme. |

## Bereich Diagrammkalender

Der Bereich Diagrammkalender wird verwendet, um ein Datum aus dem Kalender auszuwählen. Je nach ausgewähltem Datum werden die erfolgreich ausgeführten Diagramme für dieses Datum angezeigt.


28
Thursday
September 28, 2017
September 2017
S M T W T F S
27 28 29 30 31 1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
1 2 3 4 5 6 7

## Bereich Bericht anzeigen

Der Bereich Bericht anzeigen wird dazu verwendet, die Berichte zu prüfen.

# Workflow

Dieser Workflow zeigt das Verfahren, um Berichte oder Berichtsgruppen anzuzeigen.


# Was möchten Sie tun?

| Rolle | Ich möchte... | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen* | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

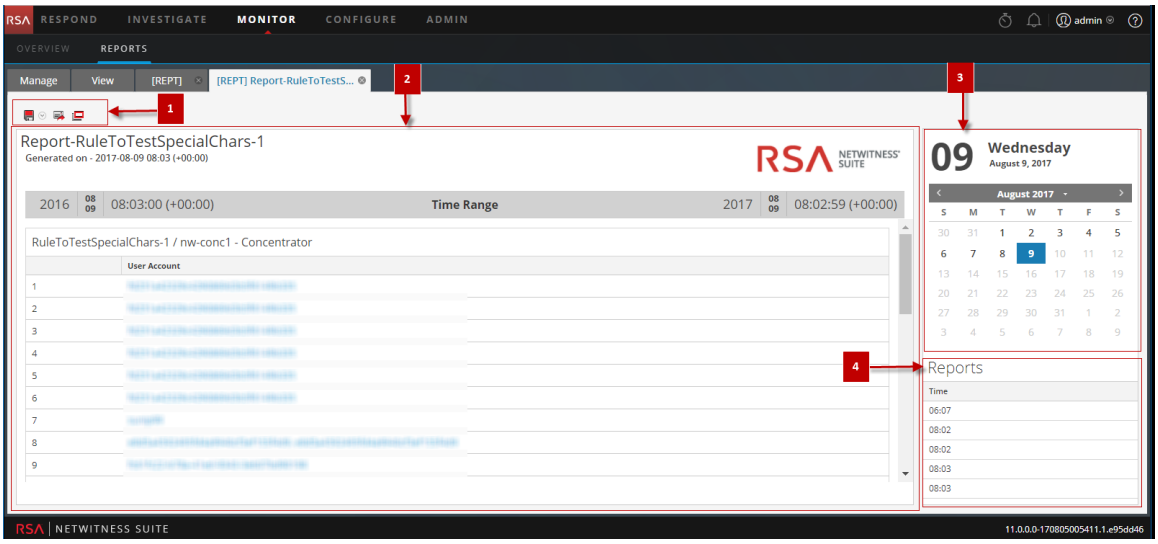
| Rolle | Ich möchte... | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht erstellen
- Dialogfeld „Bericht importieren“
- Ansicht Geplante Berichte
- Dialogfeld „Berichtberechtigungen“
- Ansicht „Alle Berichte anzeigen“
- Ansicht Bericht

## Schnellansicht




So greifen Sie auf diese Ansicht zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Führen Sie im Bereich **Berichtsliste** einen der folgenden Schritte aus:
   - Klicken Sie auf  **Geplante Berichte anzeigen**.
   - Klicken Sie auf die Spalte **#Planungen**.
     Die Ansicht „Berichtplan“ wird angezeigt.
4. Klicken Sie auf **Anzeigen**.

# Funktionen

Der Bereich Bericht anzeigen enthält die folgenden Abschnitte:

| | |
|---|---|
| 1 | Symbolleiste für Berichte |
| 2 | Bereich Berichtsausgabe |
| 3 | Bereich Berichtskalender |
| 4 | Bereich Berichtszeit |

## Symbolleiste für Berichte

Die Symbolleiste für Berichte ermöglicht es Ihnen, Berichte zu drucken, zu speichern, als E-Mail zu versenden oder diese im Vollbildmodus anzuzeigen.

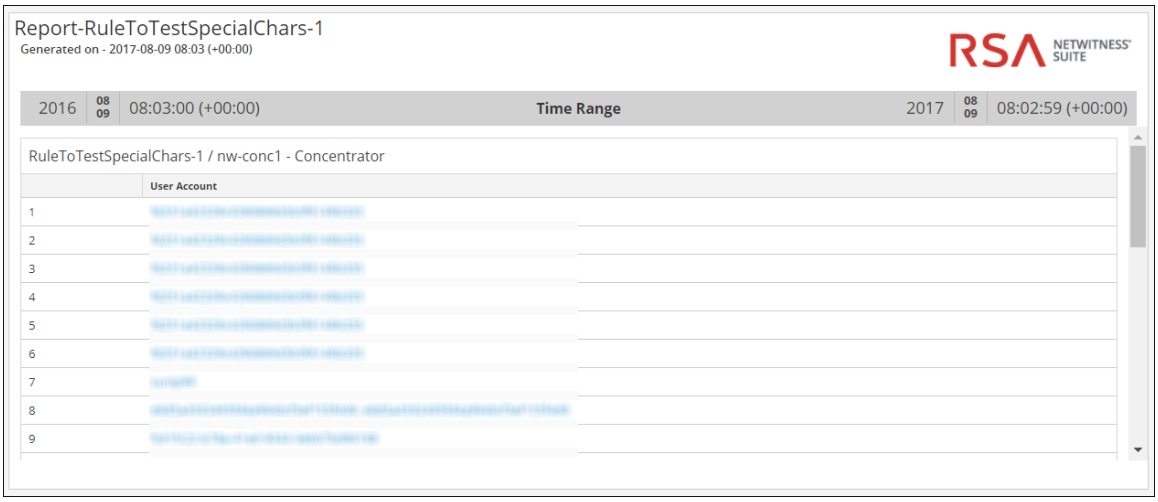
**Hinweis:** Die Reporting Engine ist für die Generierung der PDF- und CSV-Ausgaben der Berichte basierend auf der Berichtsdefinition verantwortlich. PDF-Dateien eines Berichts dürfen nicht mehr als 50.000 Zellen enthalten.

In der folgenden Tabelle sind die Optionen in der Symbolleiste „Berichte“ aufgeführt.

| Vorgang | Beschreibung |
|---|---|
| | Druckt den generierten Bericht. |
| | Speichert den Bericht als PDF- und CSV-Datei.<br>**Hinweis:** Die Option **Als PDF speichern** ist bei großen Berichten nicht verfügbar. Wenn das Erzeugen einer PDF-Datei für einen Bericht länger als angenommen dauert, wird eine Warnmeldung mit folgendem Inhalt angezeigt: **PDF-Generierung ist in Bearbeitung. Wiederholen Sie den Vorgang zu einem späteren Zeitpunkt**.<br>Wenn Sie auf die Schaltfläche „Als CSV-Datei herunterladen“ klicken, wird das Dialogfeld „Herunterzuladende Regel auswählen“ angezeigt. Sie müssen aus diesem Dialogfeld eine Regel auswählen, um das Regelergebnis als CSV-Datei herunterladen zu können.<br>Wenn die Datei-Generierung mehr Zeit in Anspruch nimmt, können Sie auf die Option **Benachrichtigen** klicken. Sie werden dann nach Fertigstellung der PDF- oder CSV-Datei benachrichtigt. Nachdem die PDF- oder CSV-Datei erzeugt wurde, können Sie die Statusbenachrichtigungen (wie unten demonstriert) anzeigen. |
| | Versendet den Bericht zusammen mit der PDF oder CSV-Datei als E-Mail. |
| | Öffnet den generierten Bericht in einem neuen Fenster. |

## Ansicht „Berichtsausgabe“

In der Ansicht „Berichtsausgabe“ wird der Bericht zusammen mit dem Berichtsplannamen, der Erzeugungszeit und dem eigentlichen Bericht mit den ausgewählten Regelvariablen angezeigt.



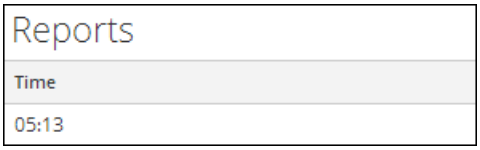

| Funktion | Beschreibung |
|---|---|
| Name | In diesem Feld wird der Name des geplanten Berichts angezeigt. |
| Zeit | In diesem Feld wird die Zeit angezeigt, wann der Bericht erzeugt wird. |
| Bericht | In diesem Feld wird der Detailbericht mit den ausgewählten Regelvariablen angezeigt. |

## Ansicht „Berichtskalender“

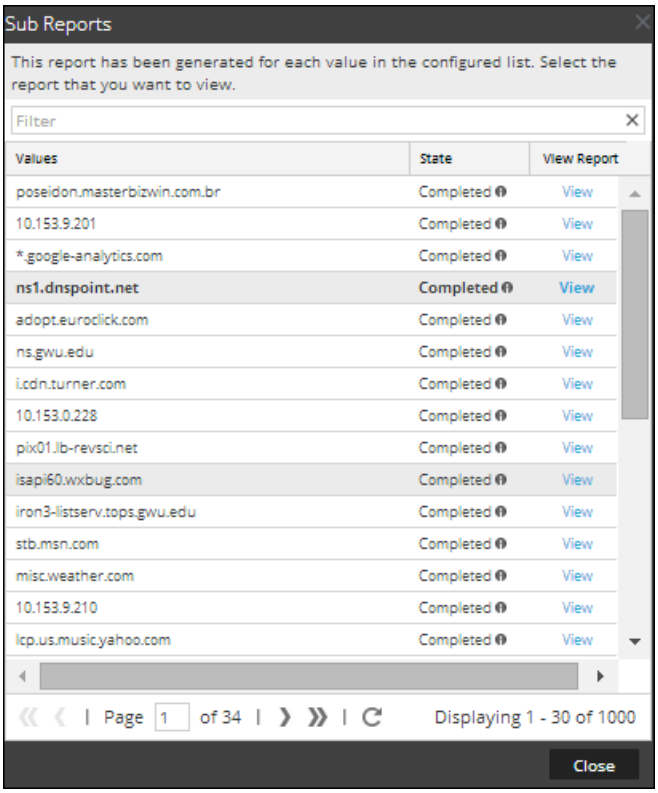
In der Ansicht „Berichtskalender“ kann ein Datum aus dem Kalender ausgewählt werden. Entsprechend des von Ihnen ausgewählten Datums erscheint eine Liste aller erfolgreich ausgeführten Berichte für dieses Datum.

## Ansicht „Berichtszeit“

Die Ansicht „Berichtszeit“ zeigt den Zeitpunkt an, an dem der Bericht ausgeführt wurde.




Wenn Sie im geplanten Bericht auf **Ansicht** klicken und die Option **Iterativ** ausgewählt haben, wird der Bereich **Unterberichte** angezeigt. Für jeden Wert in der konfigurierten Liste wird ein Bericht generiert.




In der folgenden Tabelle sind die Spalten im Bereich „Unterberichte“ aufgeführt.

| Spalte | Beschreibung |
|---|---|
| Werte | Listenwerte, die für eine dynamische Variable im Bereich Listenauswahl ausgewählt wurden |

| Spalte | Beschreibung |
| --- | --- |
| State | Zeigt den Staus des geplanten Berichts für jeden einzelnen Listenwert an<br><br>• Teilweise: Wenn in einem Bericht mit mehreren Regeln die Ausführung einer einzigen Regel, eine Ausgabeaktion oder die Erstellung einer PDF-/CSV-Datei fehlgeschlagen ist, wird als Status des Berichts „Teilweise“ angezeigt. Beispiel: In einem Bericht mit fünf Regeln werden vier Regeln erfolgreich ausgeführt und eine schlägt fehl. Als Status wird daher „Teilweise“ angezeigt.<br>• Failed: Wenn in einem Bericht mit mehreren Regeln alle Regelausführungen fehlschlagen sind, wird der Status des Berichts als „Fehlgeschlagen“ angezeigt.<br>• Abgeschlossen: Wenn ein Bericht erfolgreich ausgeführt wurde, wird als Status des Berichts „Fertiggestellt“ angezeigt. |
| View | Klicken Sie auf einen der aufgelisteten Berichtpläne oder Unterberichte und klicken Sie auf **Ansicht**, um den gewünschten Bericht anzuzeigen.<br><br>**Hinweis:** Sie können die fertiggestellten Regeln auf der Seite **Bericht anzeigen** auch anzeigen, während der Bericht ausgeführt wird. |

## Ansicht „Alle Berichte anzeigen“

In der Ansicht Alle Berichte anzeigen können Sie Berichte anzeigen, drucken, speichern und als E-Mail versenden.

# Workflow

Dieser Workflow zeigt das Verfahren, um Berichte oder Berichtsgruppen anzuzeigen.


# Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Weitere Informationen erhalten Sie unter Schritt 3: „Konfigurieren der Reporting-Engine-Datenquellen“ im *Konfigurationsleitfaden Reporting Engine*. |
| Administrator/Analyst | Erstellen einer Liste oder Listengruppe/Erstellen oder Bereitstellen einer Regel/Testen einer Regel | Konfigurieren einer Regel |
| Administrator/Analyst | Erstellen und Planen eines Berichts | Erstellen und Planen eines Berichts |
| Administrator/Analyst | Einen Bericht oder eine Liste aller Berichte anzeigen* | Anzeigen eines Berichts |
| Administrator/Analyst | Untersuchen eines Berichts | Untersuchen eines Berichts |

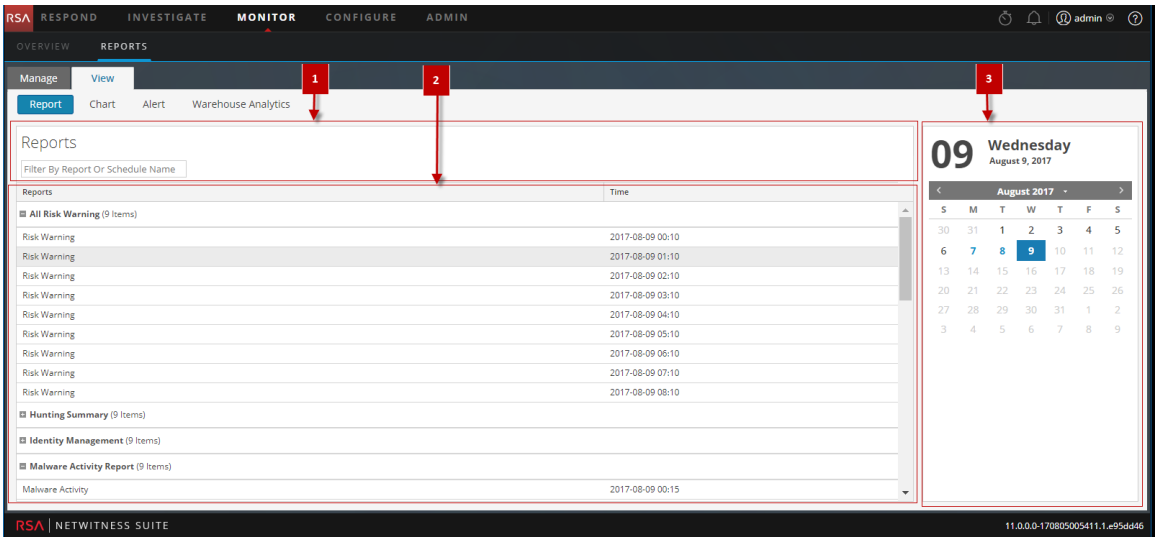
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Administrator/Analyst | Verwaltung von/Zugriffskontrolle auf Listen, Regeln oder Berichte | Managen von Listen, Regeln oder Berichten |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- Konfigurieren und Erzeugen eines Berichts
- Konfigurieren einer Regel
- Erstellen und Planen eines Berichts
- Anzeigen eines Berichts
- Untersuchen eines Berichts
- Managen von Listen, Regeln oder Berichten
- Ansicht Bericht erstellen
- Dialogfeld „Bericht importieren“
- Ansicht Geplante Berichte
- Dialogfeld „Berichtberechtigungen“
- Bereich Bericht anzeigen
- Ansicht Bericht

## Schnellansicht




So greifen Sie auf diese Ansicht zu:

1. Wählen Sie **Monitor** > **Berichte**.
   Die Registerkarte Managen wird angezeigt.
2. Klicken Sie auf **Berichte**.
   Die Ansicht „Berichte“ wird angezeigt.
3. Klicken Sie im Bereich **Bericht** auf **Alle Berichte anzeigen**.
   Der Bereich „Berichte“ wird angezeigt. Klicken Sie auf einen beliebigen Bericht in der Liste, um diesen anzuzeigen.

# Funktionen

Der Bereich „Alle Berichte anzeigen“ umfasst folgende Funktionen:

| | |
|---|---|
| 1 | Symbolleiste für Berichte |
| 2 | Bereich Berichtsausgabe |
| 3 | Bereich Berichtskalender |

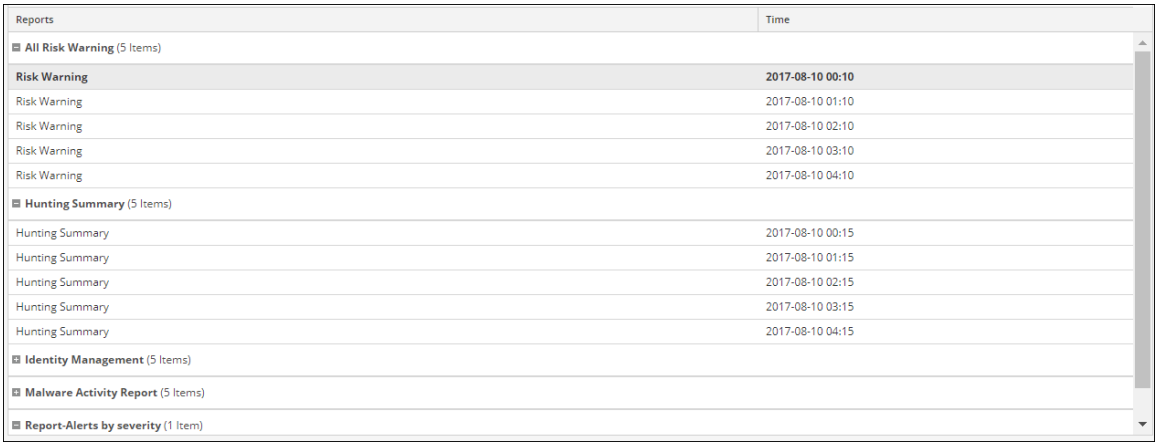
## Symbolleiste für Berichte

In der folgenden Tabelle sind die Optionen in der Symbolleiste „Alle Berichte anzeigen“ aufgeführt:

| Vorgang | Beschreibung |
| --- | --- |
| Filter By Report Or Schedule Name | Sucht basierend auf dem Berichtsnamen oder Plannamen nach Zeitplänen für einen ausgewählten Kalendertag. |

## Bereich Berichtsausgabe

Im Bereich Berichtsausgabe wird der Bericht zusammen mit dem Berichtsplannamen und der Erzeugungszeit angezeigt.




| Funktion | Beschreibung |
| --- | --- |
| Berichte | In diesem Feld wird der Detailbericht mit den ausgewählten Regelvariablen angezeigt. |
| Uhrzeit | In diesem Feld wird die Zeit angezeigt, wann der Bericht erzeugt wird. |

## Ansicht „Berichtskalender“

In der Ansicht „Berichtskalender“ kann ein Datum aus dem Kalender ausgewählt werden. Entsprechend des von Ihnen ausgewählten Datums erscheint eine Liste aller erfolgreich ausgeführten Berichte für dieses Datum.


10
Thursday
August 10, 2017
August 2017
S M T W T F S
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9

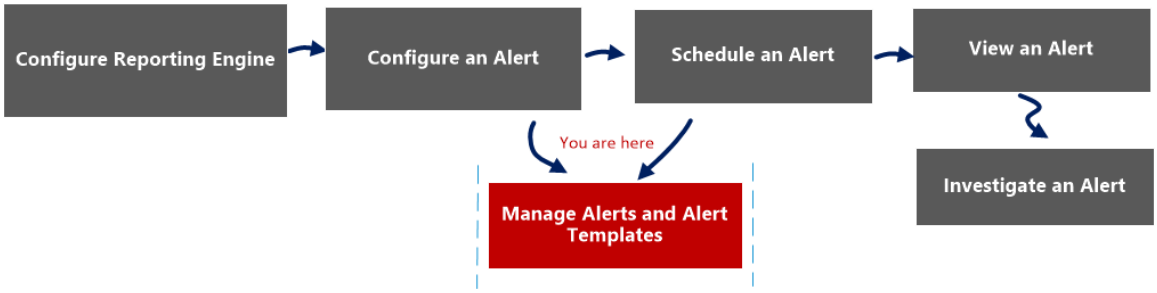
# Warnmeldungsreferenzen

Über die Benutzeroberfläche des Reporting-Moduls haben Sie Zugriff auf NetWitness-Warnmeldungen. In diesem Thema wird die Benutzeroberfläche beschrieben. Außerdem enthält es Referenzinformationen zum Verwalten von Warnmeldungen.

## Ansicht „Warnmeldungsliste“

In der Ansicht „Warnmeldungsliste“ können Sie Warnmeldungen importieren, exportieren, managen und hinzufügen.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | die Reporting Engine konfigurieren | Konfigurieren der Reporting Engine |
| Administrator/Analyst | eine Warnmeldung konfigurieren | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung planen | Planen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung anzeigen | Anzeigen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung ermitteln | Ermitteln einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung und eine Warnmeldungsvorlage managen* | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

Übersicht über Warnmeldungen

Konfigurieren einer Warnmeldung

Planen einer Warnmeldung

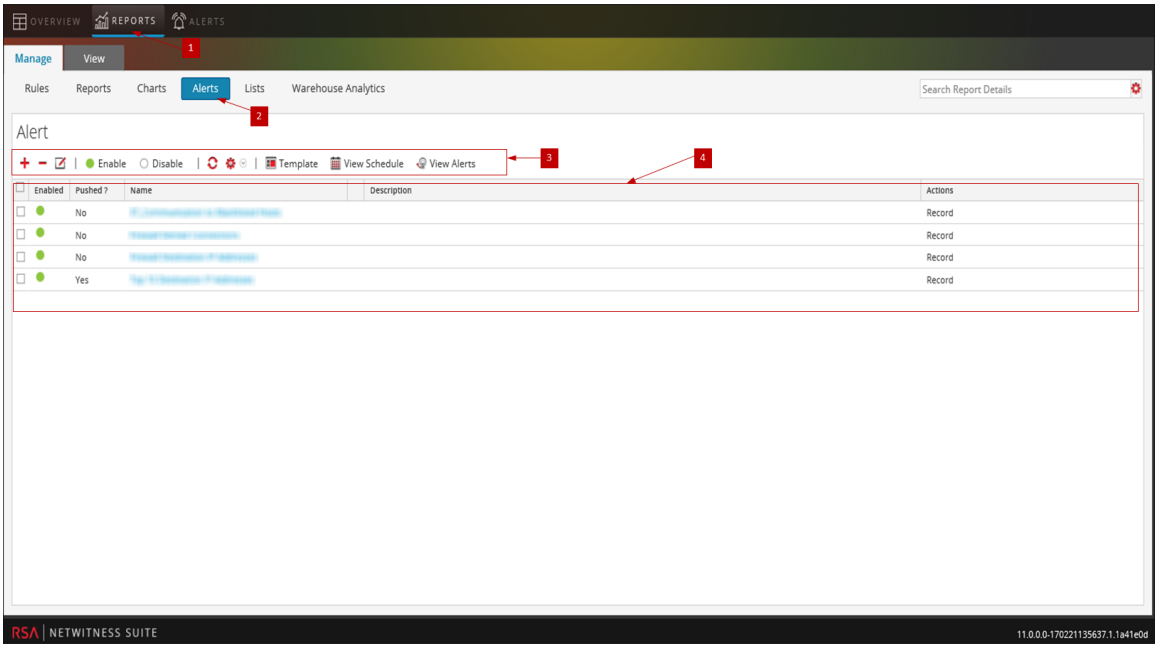
Anzeigen einer Warnmeldung

Ermitteln einer Warnmeldung

Managen einer Warnmeldung und Warnmeldungsvorlage

# Schnellansicht

Die folgende Abbildung zeigt ein Beispiel, in dem die wichtigsten Funktionen bezeichnet sind.




| | |
|---|---|
| 1 | Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen. |
| 2 | Klicken Sie auf **Warnmeldungen**, um die Ansicht „Warnmeldung“ anzuzeigen. |
| 3 | Mit der Symbolleiste „Warnmeldung“ können Sie eine Warnmeldung hinzufügen, ändern, löschen, aktivieren, deaktivieren, aktualisieren, importieren und exportieren. In dieser Symbolleiste können Sie auch Zugriffsberechtigungen für die ausgewählte Warnmeldung festlegen. |
| 4 | Im Bereich „Warnmeldungsliste“ werden alle Warnmeldungen tabellarisch aufgeführt. |

Die Ansicht „Warnmeldungsliste“ enthält die folgenden Bereiche:

- Symbolleiste „Warnmeldung“
- Warnmeldungsliste

## Symbolleiste „Warnmeldung“

Der Symbolleistenbereich „Warnmeldungen“ umfasst folgende Funktionen:

| Funktion | Beschreibung |
|---|---|
| + | Fügt eine neue Warnmeldung zum Reporting-Modul hinzu. |

| Funktion | Beschreibung |
|---|---|
|  | Löscht eine oder mehrere ausgewählte Warnmeldungen. |
|  | Bearbeitet eine Warnmeldung. |
| Aktivieren | Aktiviert die ausgewählten Warnmeldungen. |
| Deaktivieren | Deaktiviert die ausgewählten Warnmeldungen. |
|  | Aktualisiert die Ansicht. |
|  | Aktiviert die folgenden Optionen: „Importieren“, „Exportieren“ und „Berechtigungen“. |

## Warnmeldungsliste

Im Bereich „Warnmeldungsliste“ werden alle Warnmeldungen tabellarisch aufgeführt. Die folgende Tabelle enthält eine Auflistung und die Beschreibung der Spalten im Bereich „Warnmeldungsliste“.

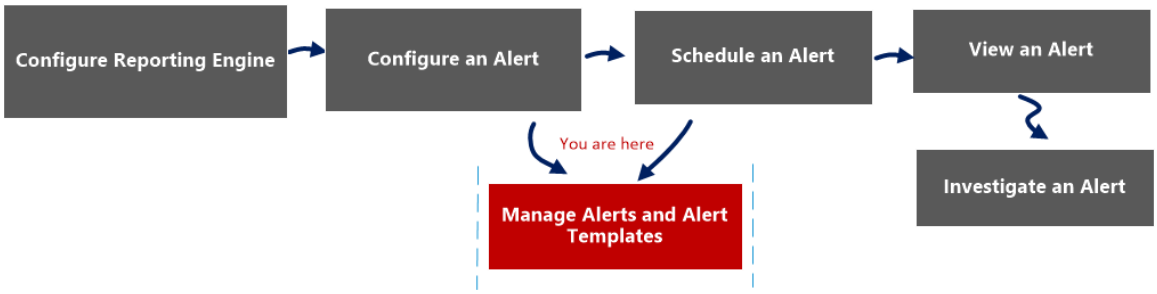
| Funktion | Beschreibung |
|---|---|
| Aktiviert | Zeigt den Status der Warnmeldung an:<br>• Aktiviert – Die Warnmeldung ist aktiv und wird basierend auf der zugewiesenen Regel ausgelöst.<br>• Deaktiviert – Die Warnmeldung ist nicht aktiv. |
| Übertragen? | Gibt an, ob eine Warnmeldung an einen Decoder oder Log Decoder gesendet wird oder nicht:<br>• Ja – Die Warnmeldung wird an einen Decoder oder Log Decoder übertragen.<br>• Nein – Die Warnmeldung wird nicht an einen Decoder oder Log Decoder übertragen. |
| Name | Identifiziert den Namen der Warnmeldung. Durch Klicken auf den Warnmeldungsnamen wird die Regel, auf der die Warnmeldung basiert, im Bereich Regeln definieren angezeigt. |

| Funktion | Beschreibung |
| --- | --- |
| Beschreibung | Gibt die Beschreibung der Warnmeldung an. |
| Aktionen | Gibt die Aktion an, die das System ausführt, wenn eine Warnmeldung ausgelöst wird.<br>Die verschiedenen verfügbaren Aktionstypen sind:<br>• Datensatz<br>• SMTP<br>• SNMP<br>• Syslog |

## Dialogfeld „Warnmeldungsberechtigungen“

Benutzer mit der Zugriffsberechtigung „Lesen und Schreiben“ zum Festlegen von Zugriffsberechtigungen für eine Warnmeldung können die Berechtigungen im Dialogfeld „Warnmeldungsberechtigungen“ konfigurieren.

# Workflow




# Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | die Reporting Engine konfigurieren | Konfigurieren der Reporting Engine |
| Administrator/Analyst | eine Warnmeldung konfigurieren | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung planen | Planen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung anzeigen | Anzeigen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung ermitteln | Ermitteln einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung und eine Warnmeldungsvorlage managen* | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

# Verwandte Themen

Übersicht über Warnmeldungen

Konfigurieren einer Warnmeldung

Planen einer Warnmeldung

Anzeigen einer Warnmeldung

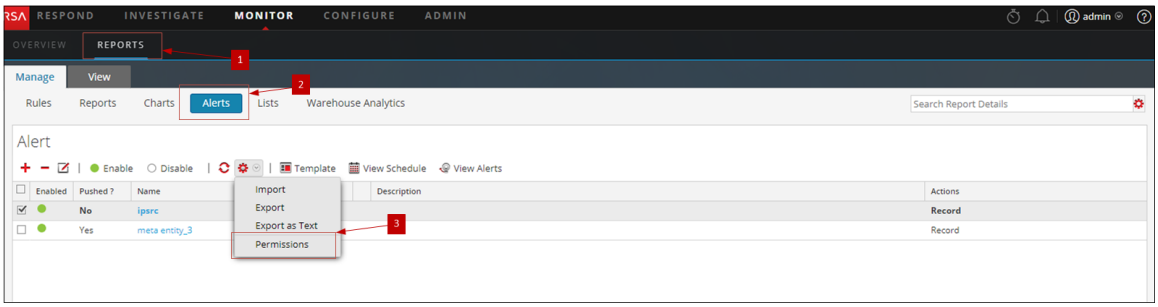
Ermitteln einer Warnmeldung

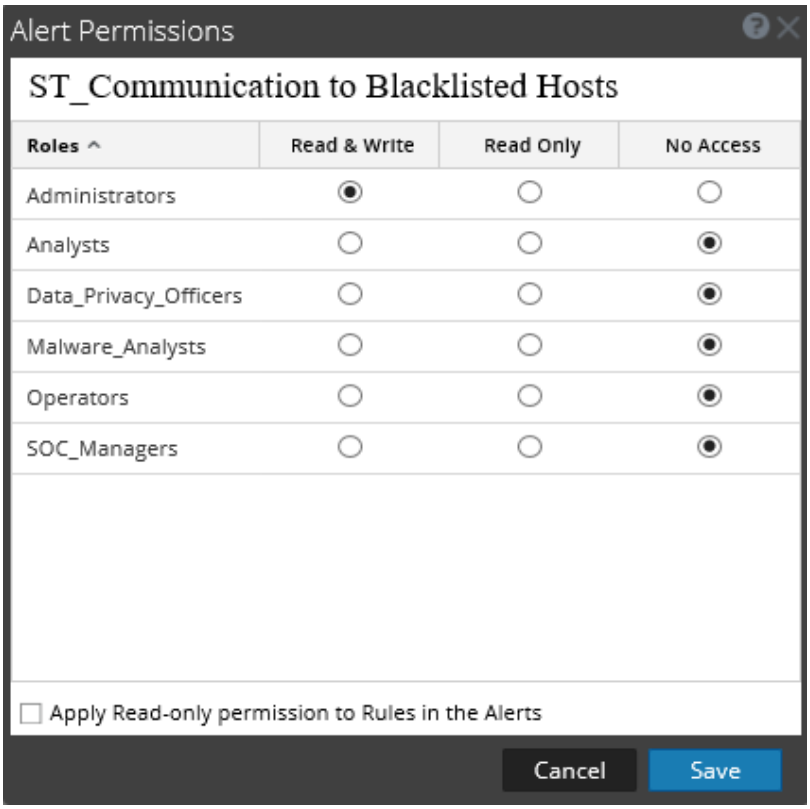
Managen einer Warnmeldung und Warnmeldungsvorlage

# Schnellansicht

Im Dialogfeld „Warnmeldungsberechtigungen“ können Sie je nach Benutzerrolle Warnmeldungsberechtigungen festlegen.

Die folgende Abbildung zeigt ein Beispiel, in dem die wichtigsten Funktionen bezeichnet sind.




1. Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen.
2. Klicken Sie auf **Warnmeldungen**, um die Ansicht „Warnmeldung“ anzuzeigen.
3. Klicken Sie auf > **Berechtigungen**. Das Dialogfeld „Warnmeldungsberechtigungen“ wird angezeigt.
4. Wählen Sie die jeweiligen Optionen entsprechend der Benutzerrolle aus.

5 (Optional) Aktivieren Sie das Kontrollkästchen, wenn Sie abhängigen Regeln automatisch Lesezugriff gewähren möchten.

6 Klicken Sie auf **Speichern**.

**Hinweis:** Wenn ein Benutzer (Superuser ausgenommen) eine Warnmeldung erstellt, können Superuser nicht auf die Warnmeldung zugreifen.

In der folgenden Tabelle sind die Spalten im Bereich „Warnmeldungsberechtigungen“ aufgeführt.

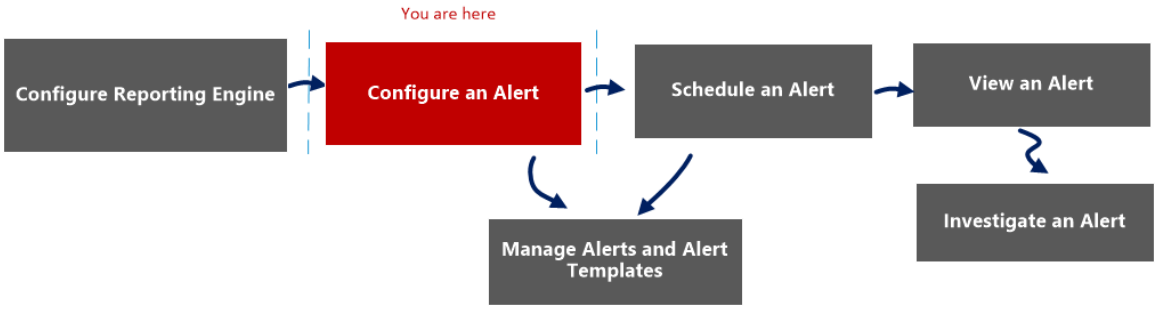
| Spalte | Beschreibung |
|---|---|
| Rollen | Zeigt alle Benutzerrollen in der NetWitness-Benutzeroberfläche an. |
| Lesen & Schreiben | Ermöglicht die Anwendung der Berechtigung „Lesen und Schreiben“ für den Zugriff auf die Warnmeldung. |
| Schreibgeschützt | Ermöglicht die Anwendung der Berechtigung „Lesen“ für den Zugriff auf die Warnmeldung. |
| Kein Zugriff | Wenn Sie diese Berechtigung auswählen, können Sie auf die Warnmeldung weder zugreifen noch diese anzeigen. |
| Berechtigung „Schreibgeschützt“ auf Regeln in den Warnmeldungen anwenden | Ermöglicht, Berechtigungen automatisch auf die Regeln in den Warnmeldungen anzuwenden. |
| Abbrechen | Verwirft alle an den Berechtigungen vorgenommen Änderungen. |
| Speichern | Speichert die Auswahl und bietet basierend auf dieser Auswahl Zugriff auf die Rollen. |

# Ansicht „Warnmeldungspläne“

In der Ansicht „Warnmeldungspläne“ können Sie alle geplanten Warnmeldungen anzeigen. Alternativ können Sie geplante Warnmeldungen auch deaktivieren.

## Workflow

Die folgende Workflow zeigt die Aufgaben beim Erstellen oder Ändern einer Warnmeldung.




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | die Reporting Engine konfigurieren | Konfigurieren der Reporting Engine |
| Administrator/Analyst | eine Warnmeldung konfigurieren* | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung planen | Planen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung anzeigen | Anzeigen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung ermitteln | Ermitteln einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung und Warnmeldungsvorlage managen | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

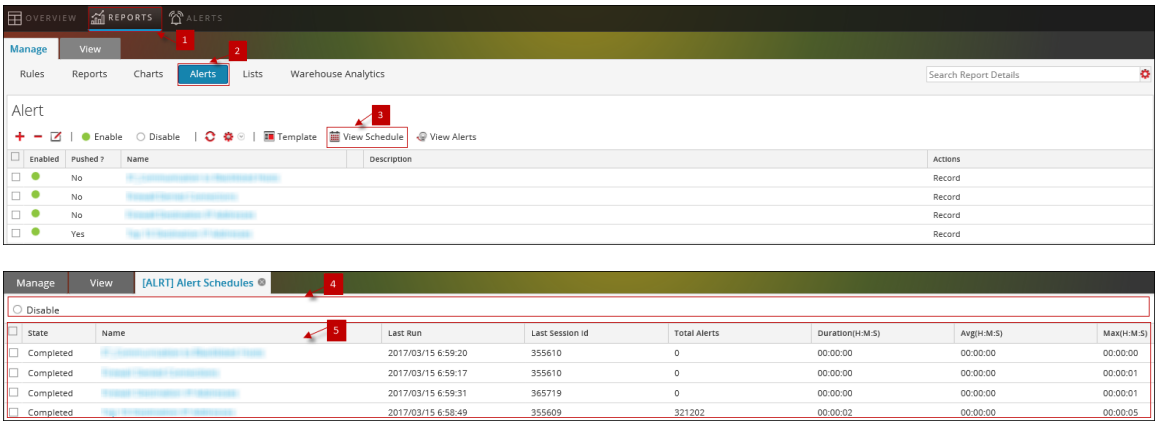
## Verwandte Themen

Übersicht über Warnmeldungen

Konfigurieren einer Warnmeldung

## Schnellansicht

Das folgende Beispiel zeigt, wie Sie auf die Ansicht „Warnmeldungszeitpläne“ zugreifen.




| | |
|---|---|
| 1 | Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen. |
| 2 | Klicken Sie auf **Warnmeldungen**, um die Ansicht „Warnmeldung“ anzuzeigen. |
| 3 | Klicken Sie auf **Zeitplan anzeigen**, um die Ansicht „Warnmeldungszeitpläne“ anzuzeigen. |
| 4 | In der Symbolleiste „Warnmeldungszeitpläne“ können Sie den Zustand der geplanten Warnmeldung ändern. |
| 5 | In der Liste „Warnmeldungszeitpläne“ werden nur die aktivierten Warnmeldungen im Tabellenformat aufgeführt. |

# Funktionen

Die Ansicht „Warnmeldungszeitpläne“ enthält die folgenden Bereiche:

- Symbolleistenbereich „Warnmeldungszeitpläne“
- Listenbereich „Warnmeldungszeitpläne“

## Symbolleistenbereich „Warnmeldungszeitpläne“

Im Symbolleistenbereich „Warnmeldungszeitpläne“ wird durch Klicken auf „Deaktivieren“ die ausgewählte Warnmeldung deaktiviert. Wenn geplante Warnmeldungen nicht mehr benötigt werden oder sich als ineffektiv erwiesen haben, können Sie diese deaktivieren, damit sie nicht mehr ausgeführt werden. Sie können eine oder mehrere zu deaktivierende Warnmeldungen auswählen. Eine deaktivierte Warnmeldung wird aus der Liste der geplanten Warnmeldungen entfernt, sodass sie hier nicht mehr angezeigt wird, und nur dann erneut ausgeführt, wenn Sie die Warnmeldung manuell ausführen oder einen neuen Zeitplan dafür einrichten.

## Listenbereich „Warnmeldungszeitpläne“

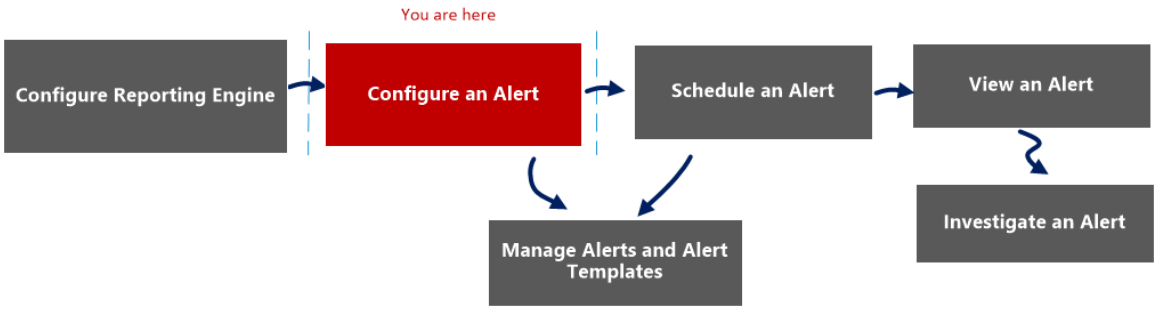
In der folgenden Tabelle sind die Spalten der Liste „Warnmeldungsplanung“ mit einer Beschreibung aufgeführt.

| Spalte | Beschreibung |
| --- | --- |
| State | Der Status der geplanten Warnmeldung:<br>• Abgeschlossen<br>• Fehlgeschlagen |
| Name | Der Name der geplanten Warnmeldung |
| Letzte Ausführungszeit | Die letzte Uhrzeit, zu der die geplante Warnmeldung ausgeführt wurde |
| ID der letzten Sitzung | Die Sitzungs-ID der letzten geplante Warnmeldung |
| Warnmeldungen insgesamt | Die Gesamtzahl der Ereignisausführungen |
| Dauer | Wie lange die Ausführung der geplanten Warnmeldung gedauert hat |
| Durchschn. (s) | Wie lange die Ausführung der geplanten Warnmeldung durchschnittlich gedauert hat |
| Max. (s) | Wie lange die Ausführung der geplanten Warnmeldung höchstens gedauert hat |

## Bereich „Warnmeldung erstellen oder ändern“

Der Bereich „Warnmeldung erstellen oder ändern“ ist ein Bereich in der Ansicht „Warnmeldungsliste“. In diesem Bereich können Sie eine Warnmeldung entsprechend den Anforderungen erstellen oder ändern.

# Workflow




# Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Konfigurieren der Reporting Engine |
| Administrator/Analyst | Konfigurieren einer Warnmeldung* | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | Planen einer Warnmeldung | Planen einer Warnmeldung |
| Administrator/Analyst | Anzeigen einer Warnmeldung | Anzeigen einer Warnmeldung |
| Administrator/Analyst | Untersuchen einer Warnmeldung | Ermitteln einer Warnmeldung |
| Administrator/Analyst | Managen einer Warnmeldung und Warnmeldungsvorlage | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

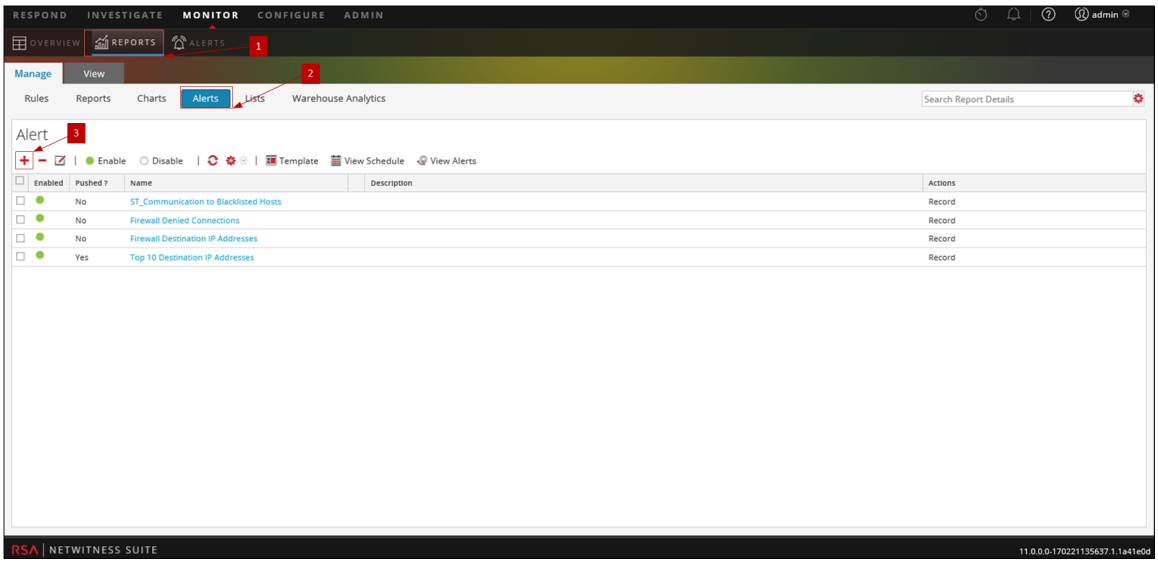
# Verwandte Themen

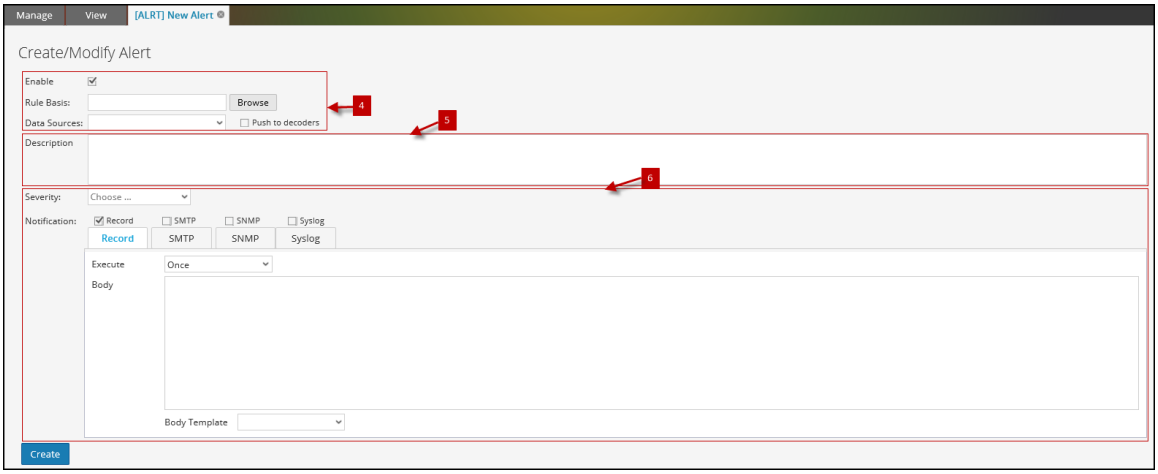
Übersicht über Warnmeldungen

Konfigurieren einer Warnmeldung

# Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




| | |
|---|---|
| 1 | Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen. |
| 2 | Klicken Sie auf **Warnmeldungen**, um die Warnmeldungsansicht anzuzeigen. |
| 3 | Klicken Sie auf +, um zum Bereich „Warnmeldungen erstellen oder bearbeiten zu navigieren. |
| 4 | Aktivieren Sie die Warnmeldung, navigieren Sie zur Regel und wählen Sie eine Datenquelle für die Warnmeldung. |
| 5 | Geben Sie eine kurze Beschreibung der Warnmeldung ein. |
| 6 | Definieren Sie die Methoden für Warnmeldungsbenachrichtigungen (Datensatz, SMTP, SNMP, Syslog), wenn eine Warnmeldungsbedingung vorliegt. |

Der Bereich „Erstellen oder Ändern von Warnmeldungsansichten“ enthält folgende Bereiche:

- Warnmeldungsdefinition
- Beschreibung der Warnmeldung
- Warnmeldungsbenachrichtigung

## Warnmeldungsdefinition

In der nachstehenden Tabelle sind die Felder des Bereichs „Warnmeldungsdefinition“ beschrieben.

| Feld | Beschreibung |
|---|---|
| Aktivieren | • Die Option **Aktivieren** aktiviert die Warnmeldung. Die Warnmeldung wird ausgeführt und sendet Ausgabeaktionen im Minutentakt (standardmäßig), wenn die Bedingungen für die Warnmeldung erfüllt sind.<br>• Die Option **Deaktivieren** deaktiviert eine Warnmeldung. Die Warnmeldung wird nicht ausgeführt und sendet keine Ausgabeaktionen. |
| Regelbasis | Klicken Sie auf **Durchsuchen**, um den Bereich „Regelbibliothek“ anzuzeigen, von dem aus Sie die Regelbasis für diese Warnmeldung auswählen.<br>Sie müssen eine Regel auswählen, die eine eindeutige Where-Klausel für eine Warnmeldung enthält. |
| Datenquellen | Gibt die Datenquelle der Warnmeldung an. |
| Per Push an die Decoder übertragen | Überträgt die „Where“-Klausel der Warnmeldungsregel per Push auf die Decoder, die mit der ausgewählten NWDB-Datenquelle verbunden sind. Hierbei handelt es sich um die empfohlene Option zur Erstellung einer RE-Warnmeldung, da die Warnmeldungsbedingungen auf dem Decoder selbst überprüft werden und die Warnmeldungsabfragen in NWDB vergleichsweise schneller sind.<br>Wenn Sie diese Option deaktivieren, wird die Warnmeldungsregel mit der Where-Klausel auf der gewählten NWDB-Datenquelle abgefragt. Basierend auf der Komplexität und der Metas in der Where-Klausel der Regel kann die Ausführung der Warnmeldungsabfragen in NWDB mehr Zeit in Anspruch nehmen.<br>**Hinweis:** NetWitness sendet die Regeln nicht automatisch an den Decoder. |

## Beschreibung der Warnmeldung

In der nachstehenden Tabelle sind die Felder des Bereichs „Warnmeldungsbeschreibung“ beschrieben:

| Feld | Beschreibung |
|---|---|
| Beschreibung | Beschreibt die Regel. |
| Erstellen | Erstellt eine Warnmeldung. (Diese Option wird bei der Erstellung einer Warnmeldung angezeigt.) |
| Speichern | Speichert die an einer Warnmeldung durchgeführten Änderungen. (Diese Option wird bei der Änderung einer Warnmeldung angezeigt.) |

## Warnmeldungsbenachrichtigung

Durch die Warnmeldungsbenachrichtigung können Sie die Benachrichtigungsaktion definieren, die NetWitness durchführt, wenn eine Warnmeldung ausgelöst wird, z. B. Warnmeldungen mithilfe einer der festgelegten Ausgabeaktionen aufzeichnen oder senden. Die Ausgabeaktionen sind Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP) oder Syslog-Meldungen.

Die Benachrichtigung enthält die Standardregisterkarte „Datensatz“, die Sie zum Erstellen einer Warnmeldung nutzen. Durch das Symbol neben der Registerkarte „Datensatz“ können Sie den Benachrichtigungstyp aus der Drop-down-Liste für die Ausgabe aussuchen, den Sie für diese Warnmeldung angeben möchten. SMTP, SNMP, oder Syslog.

Je nachdem, welchen Benachrichtigungstyp Sie ausgewählt haben, wird der Bereich „Benachrichtigung“ mit einem vordefinierten Text ausgefüllt, der bestimmte Variablen enthält, die passende Metadaten zur Warnmeldung hinzufügen. In der Reporting Engine werden diese Variablen durch tatsächliche Werte ersetzt. In der folgenden Tabelle sind die Variablen mit Beschreibung aufgelistet.

| Variable | Beschreibung |
|---|---|
| `${meta.<metakey>}` | Der Metaschlüsselwert.<br><br>**Hinweis:** Wenn der <Metaschlüssel> keinen Wert abgerufen hat, wird eine leere Zeichenfolge ("") gedruckt.<br>Standardmäßig werden in Reporting Engine alle wiederholten Werte für einen Metaschlüssel angezeigt. Wenn Metawerte in der Warnmeldungsausgabe nicht wiederholt werden sollen, aktivieren Sie die Option „removeRepeatedMetaValue“. Navigieren Sie dazu in der Ansicht **Konfiguration** > **Warnmeldungskonfiguration**, verfügbar für die Reporting Engine in der Ansicht Service-Konfiguration > Durchsuchen.<br>Beispiel: In einer HTTP-Sitzung wird der Wert für eine Aktion als „get, get, put, put, post, get“ angezeigt. Wenn diese Option aktiviert ist, wird der Wert als „get, put, post“ angezeigt. |
| `${meta.time}` / `${meta.time:<time_format>}` | `${meta.time}`: Die Sitzungszeit wird im Format „jjjj-MMM-dd HH:mm:ss“ gedruckt.<br>`${meta.time:<time_format>}` : Die Sitzungszeit wird im vom Benutzer angegebenen benutzerdefinierten Zeitformat gedruckt. Zum Beispiel `${meta.time:dd-MM-yyyy HH:mm:ss}`.<br>Weitere Informationen über das unterstützte Zeitformat erhalten Sie unter<br>http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html<br><br>**Hinweis:** Wenn das vom Benutzer angegebene Zeitformat ungültig ist, wird das Standardzeitformat angewendet. Das Standardzeitformat ist „JJJJ-MMM-TT hh:mm:ss“. |
| `${name}` | Name der Warnmeldung, der in der Reporting Engine definiert ist. |
| `${count}` | Anzahl, wie oft eine Warnmeldung in einem vorgegebenen Zeitraum erkannt wird. (Standardmäßig ist es eine Minute) |
| `${nw.host}` | NetWitness-Hostname, wie in der Reporting Engine konfiguriert. |
| `${device.id}` | Die NetWitness-Geräte-ID der Datenquelle. |

Die Warnmeldungsbenachrichtigung verfügt über vier Registerkarten:

## Registerkarte Datensatz

In der Registerkarte Datensatz können Sie die Frequenz zur Aufnahme einer Warnmeldung und der Meldung angeben, die Sie beim Auslösen einer Warnmeldung erzeugt werden soll.


In der folgenden Tabelle werden die Felder der Registerkarte „Datensatz“ mit den jeweiligen Beschreibungen aufgelistet.

| Feld | Beschreibung |
|---|---|
| Ausführen | Die Frequenz, mit der eine Warnmeldung aufgezeichnet wird.<br>• **Einmal** – Zeichnet die Warnmeldung nur einmal auf, basierend auf dem Warnmeldungsintervall und unabhängig davon, wie oft die Warnmeldung ausgelöst wird. NetWitness zeichnet auf, wie oft die Warnmeldung tatsächlich während des Intervalls in der Protokolldatei ausgelöst wurde, sodass die Analysten wissen, wie oft die Warnmeldung einen Treffer innerhalb eines angegeben Tages registriert hat.<br>• **Jedes Ereignis** – Zeichnet die Warnmeldung jedes Mal auf, wenn diese ausgelöst wird. Wenn eine Warnmeldung unzählig oft an einem Tag ausgelöst wird, wird diese Warnmeldung oft als Störung behandelt und kann ignoriert werden, es sei denn, es handelt sich um eine Warnmeldung, die eine kontinuierliche Überwachung erfordert, wie zum Beispiel Änderungen der Netzwerkkonfiguration und DDoS-Angriffe.<br>**Hinweis:** Wählen Sie die Einstellung **Jedes Ereignis** aus der Drop-down-Liste **Ausführen** für SNMP- und Syslog-Ausgabeaktionen aus. |
| Textkörper | Der Nachrichtentext. |
| Textkörpervorlage | (Optional) Wenn Vorlagen definiert wurden, können Sie für die Warnmeldung eine Vorlage auswählen. |

## Registerkarte SMTP

In der Registerkarte SMTP können Sie die SMTP-(E-Mail)-Ausgabe für diese Warnmeldung definieren.


In der folgenden Tabelle werden die Felder der Registerkarte SMTP mit entsprechender Beschreibung aufgelistet.

| Feld | Beschreibung |
|---|---|
| Führen Sie folgenden Befehl aus | Die Häufigkeit, in der für die Warnmeldung eine E-Mail gesendet wird.<br>• **Einmal** – Sendet nur eine E-Mail pro Intervall, wenn Warnmeldungen in diesem Intervall ausgelöst werden, unabhängig davon, wie viele Warnmeldungen ausgelöst wurden.<br>• **Jedes Ereignis** – Sendet eine E-Mail mit der Warnmeldung für jedes Ereignis, auf das die Regelkriterien zutreffen. |
| An | Die E-Mail-Adressen, an die diese Warnmeldung gesendet werden soll. |
| Betreff | Der Betreff der E-Mail. |
| Textkörper | Der Nachrichtentext. |
| Textkörpervorlage | (Optional) Wenn Vorlagen definiert wurden, wählen Sie eine Vorlage für die SMTP-Meldung aus, die Sie so, wie sie ist, verwenden oder ändern können. |

## Registerkarte SNMP

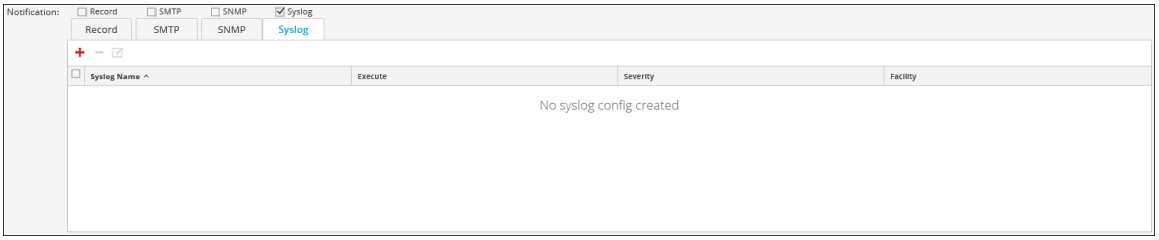
In der Registerkarte SNMP können Sie die SNMP-Ausgabe für die Warnmeldung definieren.


In der folgenden Tabelle werden die verschiedenen Felder der Registerkarte „SNMP“ mit entsprechender Beschreibung aufgelistet.

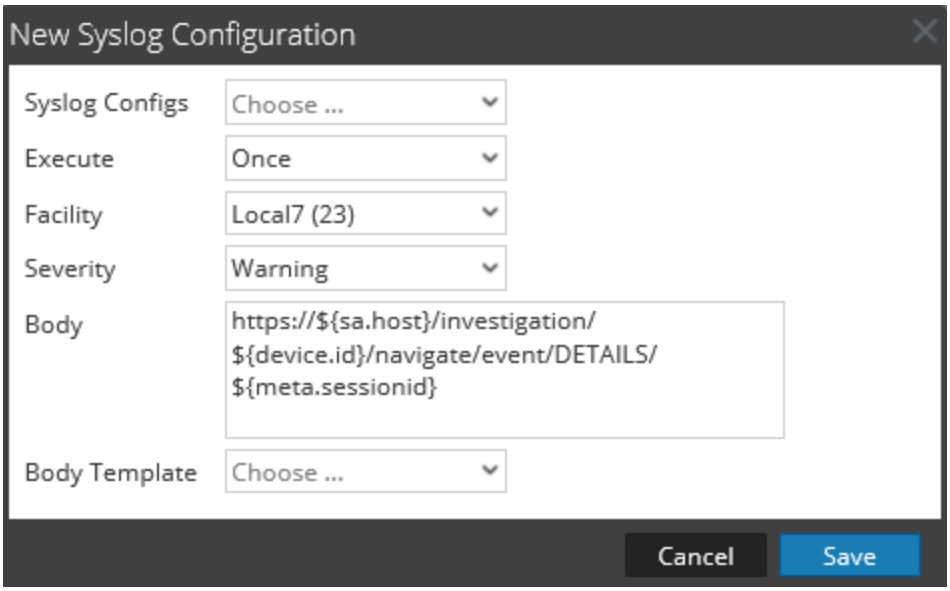
| Feld | Beschreibung |
|---|---|
| Führen Sie folgenden Befehl aus | Die Häufigkeit, in der eine für eine Warnmeldung SNMP-Ausgabe gesendet wird.<br>• **Einmal** – Sendet eine SNMP-Meldung in einer E-Mail für ein Intervall, wenn in diesem Intervall eine Warnmeldung ausgelöst wird, unabhängig davon, wie viele Warnmeldungen ausgelöst wurden.<br>• **Jedes Ereignis** – Sendet eine SNMP-Meldung mit der Warnmeldung für jedes Ereignis, auf das die Regelkriterien zutreffen. |
| Textkörper | Der Nachrichtentext. |
| Textkörpervorlage | (Optional) Wenn Vorlagen definiert wurden, wählen Sie eine Vorlage für die SNMP-Meldung aus, die Sie so, wie sie ist, verwenden oder ändern können. |

## Registerkarte „Syslog“

In der Registerkarte „Syslog“ können Sie die Syslog-Meldungsausgabe für diese Warnmeldung definieren.




Klicken Sie auf , um eine Syslog-Konfiguration zu einer Warnmeldung hinzuzufügen. Das Dialogfeld „Neue Syslog-Konfiguration“ wird angezeigt:




In der folgenden Tabelle sind die verschiedenen Felder des Dialogfelds „Neue Syslog-Konfiguration“ beschrieben:

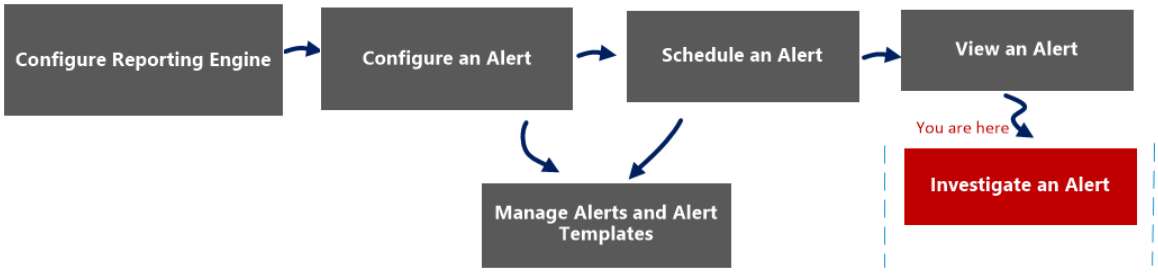
| Feld | Beschreibung |
|---|---|
| Syslog-Konfigurationen | Die Syslog-Konfiguration im Bereich „Syslog-Konfiguration“ der Ansicht „Gerätekonfiguration“. |
| Ausführen | Gibt an, wie oft Sie eine Syslog-Ausgabe für die Warnmeldung senden möchten.<br>• **Einmal** – Sendet eine Syslog-Ausgabe mit einer E-Mail für ein Intervall, wenn es in diesem Intervall zu einer Warnmeldung kommt, unabhängig davon, wie viele Warnmeldungen ausgelöst wurden.<br>• **Jedes Ereignis** – Sendet eine Syslog-Ausgabe mit der Warnmeldung für jedes Ereignis, auf das die Regelkriterien zutreffen. |
| Gerät | Gibt den Programmtypen der Meldungs-Protokollierung an. Einige Beispiele von Programmtypen: Syslog, Daemon, Mail, Kernel. |

| Feld | Beschreibung |
| --- | --- |
| Schweregrad | Schweregrad der generierten Warnmeldungen.<br>• Notfall<br>• Warnmeldungen<br>• Kritisch<br>• Error<br>• Warnung<br>• Hinweis<br>• Informational<br>• Debuggen |
| Textkörper | Der Nachrichtentext. |
| Textkörpervorlage | (Optional) Wenn Vorlagen definiert wurden, wählen Sie eine Vorlage für die Syslog-Nachricht aus, die Sie so, wie sie ist, verwenden oder ändern können. |

## Ansicht „Untersuchen einer Warnmeldungsansicht“

In der Ansicht „Untersuchen einer Warnmeldungsansicht“ können Sie Warnmeldungsdetails aufrufen und untersuchen. Wenn Sie eine Warnmeldung untersuchen, können Sie die Sitzungen im Modul „Untersuchen“ für weitere Untersuchungen öffnen.

# Workflow




# Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Konfigurieren der Reporting Engine |
| Administrator/Analyst | Konfigurieren einer Warnmeldung | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | Planen einer Warnmeldung | Planen einer Warnmeldung |
| Administrator/Analyst | Anzeigen einer Warnmeldung | Anzeigen einer Warnmeldung |
| Administrator/Analyst | Untersuchen einer Warnmeldung* | Ermitteln einer Warnmeldung |
| Administrator/Analyst | Managen einer Warnmeldung und Warnmeldungsvorlage | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

# Verwandte Themen

Übersicht über Warnmeldungen

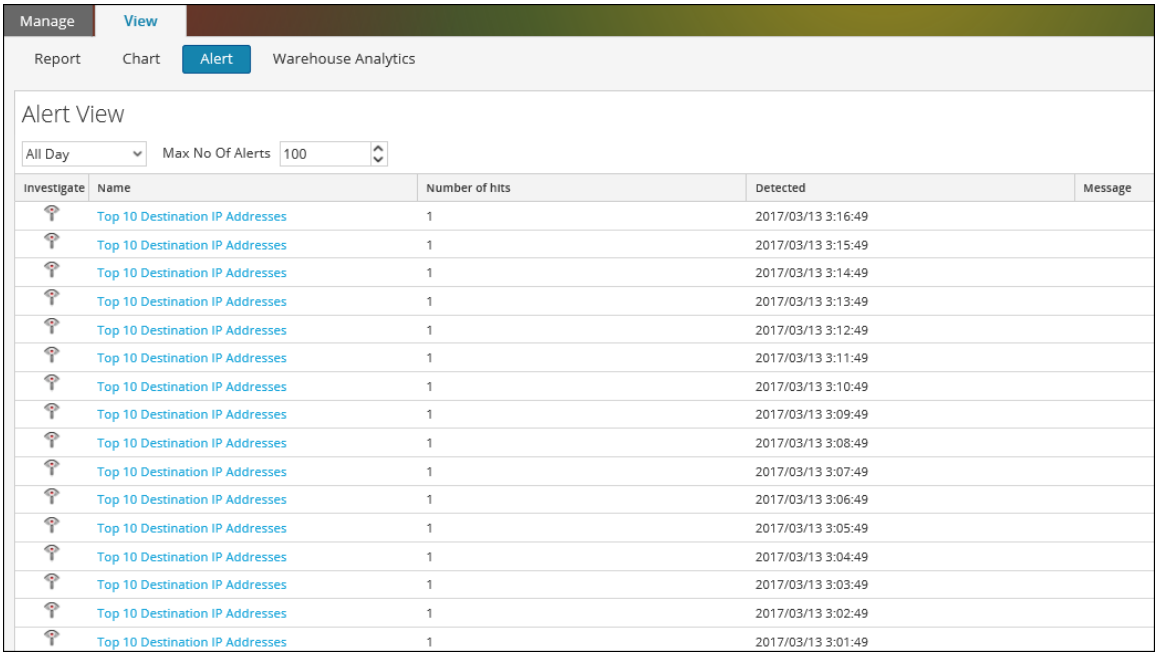
Konfigurieren einer Warnmeldung

Planen einer Warnmeldung

Anzeigen einer Warnmeldung

# Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




Die Ansicht „Warnmeldungen anzeigen“ umfasst die folgenden Bereiche:

- Symbolleiste „Warnmeldungen anzeigen“
- Liste der Warnmeldungen anzeigen

## Liste der Warnmeldungen anzeigen

In der folgenden Tabelle sind die verschiedenen Spalten im Bereich „Liste der Warnmeldungen anzeigen“ aufgeführt.

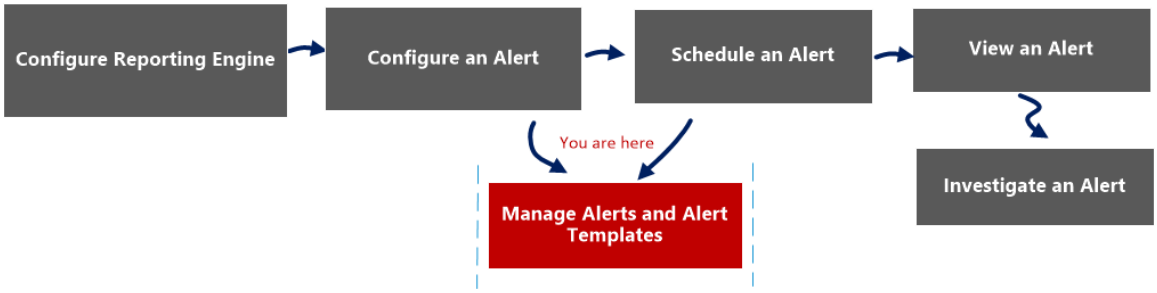
| Spalte | Beschreibung |
|---|---|
|  | Durch Klicken auf die Schaltfläche wird das Modul Investigation geöffnet, in dem die Details der ersten Sitzung, in der die Übereinstimmung mit der Warnmeldung registriert wurde, zwecks einer genauen Analyse angezeigt werden.<br><br>**Hinweis:** In folgenden Fällen werden Sie nicht an das Modul Investigation weitergeleitet:<br>- Sie konfigurieren eine Datenquelle für eine vorhandene Warnmeldung erneut und führen eine Warnmeldung für die neue Datenquelle aus.<br>- Sie geben einen Hostnamen anstelle einer IP-Adresse im Datenquellfeld ein. |

| Spalte | Beschreibung |
|---|---|
| Name | Der Name der Warnmeldung, die die Übereinstimmung registriert hat. Über den Hyperlink zu dem Namen wird das Modul Investigation geöffnet, in dem alle Übereinstimmungen innerhalb der Stunde um die registrierte Warnmeldung angezeigt werden. |
| Anzahl der Treffer | Die Häufigkeit, mit der die Warnmeldung erzeugt wird. |
| Detected | Datum und Uhrzeit der Warnmeldung. |
| Meldung | Der Text der Warnmeldung |

## Dialogfeld „Warnmeldung importieren“

Im Dialogfeld „Warnmeldung importieren“ können Sie ein Warnmeldungsarchiv importieren und angeben, ob vorhandene Regeln, Listen und Warnmeldungen überschrieben werden sollen.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Konfigurieren der Reporting Engine |
| Administrator/Analyst | Konfigurieren einer Warnmeldung | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | Planen einer Warnmeldung | Planen einer Warnmeldung |
| Administrator/Analyst | Anzeigen einer Warnmeldung | Anzeigen einer Warnmeldung |
| Administrator/Analyst | Untersuchen einer Warnmeldung | Ermitteln einer Warnmeldung |
| Administrator/Analyst | Managen einer Warnmeldung und Warnmeldungsvorlage* | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

Übersicht über Warnmeldungen

Konfigurieren einer Warnmeldung

Planen einer Warnmeldung

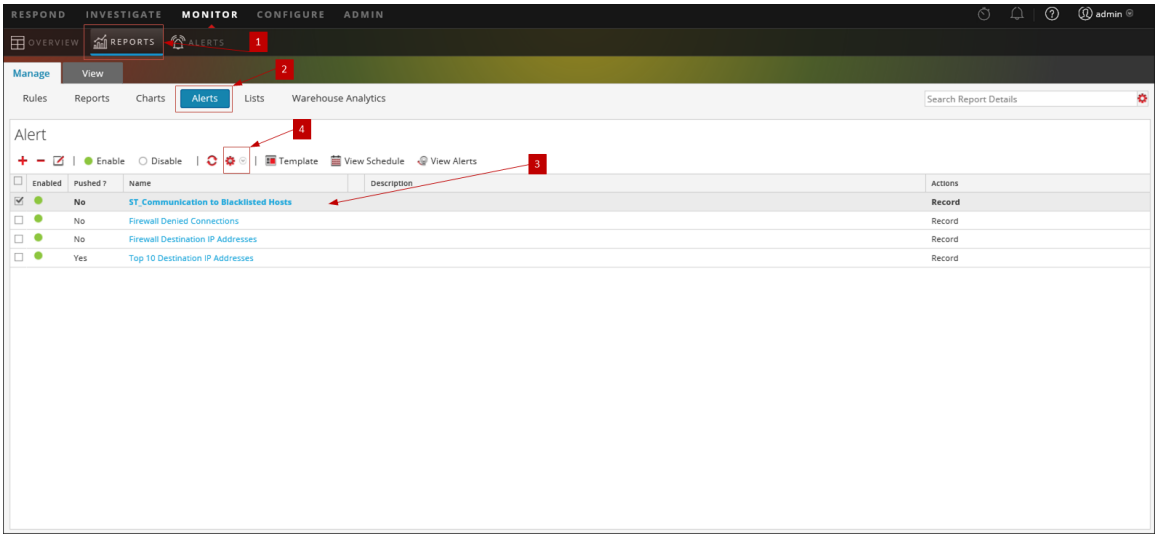
Anzeigen einer Warnmeldung

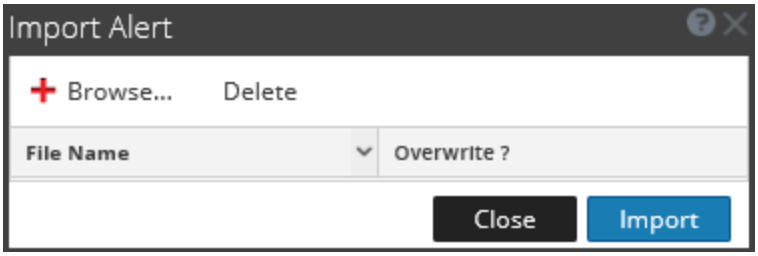
Ermitteln einer Warnmeldung

Managen einer Warnmeldung und Warnmeldungsvorlage

## Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




1. Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen.
2. Klicken Sie auf **Warnmeldungen**, um die Warnmeldungsansicht anzuzeigen.
3. Wählen Sie im Bereich **Warnmeldung** einen Ordner aus, um die Datei zu importieren.
4. Klicken Sie in der Symbolleiste **Warnmeldung** auf > **Importieren**, um eine Warnmeldung zu importieren.

In der folgenden Tabelle sind die Aktionen des Dialogfelds „Warnmeldung importieren“ aufgeführt und erläutert.

| Aktionen | Beschreibung |
|---|---|
| Browse... | Zeigt eine Ansicht des lokalen zip-Dateisystems, damit Sie die zu importierende Warnmeldung auswählen können. |
| − | Löscht die ausgewählte Warnmeldung aus dem Dialogfeld „Warnmeldung importieren“. |

| Aktionen | Beschreibung |
|---|---|
| Dateiname | Name der importierten binären Datei an. |
| Überschreiben? | Ermöglicht die Auswahl der Option zum Überschreiben einer vorhandenen Version der Warnmeldung, die Sie importieren. Wenn Sie die Option „Überschreiben“ nicht auswählen, wird ein Duplikat der Datei importiert und es wird keine Fehlermeldung angezeigt. |
| Schließen | Schließt das Dialogfeld Warnmeldung importieren. |
| Importieren | Importiert die Warnmeldung mit einer Bestätigungsmeldung. |

# Referenzen für Warnmeldungsvorlagen

In der Benutzeroberfläche des Moduls „Reporting“ können Sie auf NetWitness-Warnmeldungen und Warnmeldungsvorlagen zugreifen. In diesem Thema finden Sie Beschreibungen der Benutzeroberfläche sowie andere Referenzinformationen, die Benutzern das Management von Warnmeldungsvorlagen erleichtern.

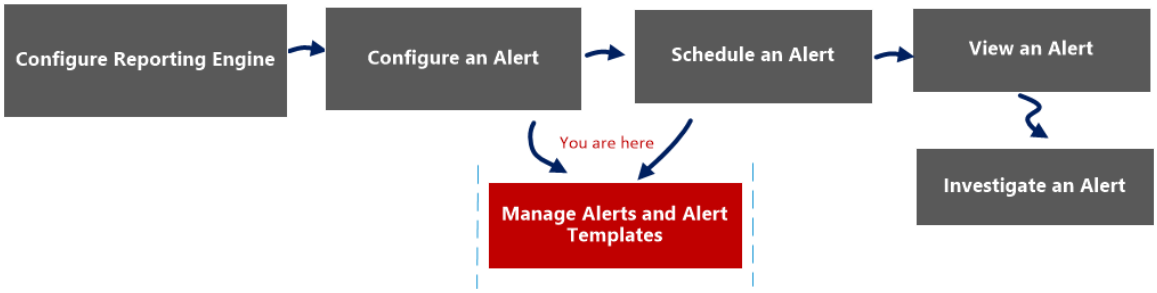
Themen:

- Ansicht „Vorlage erstellen oder ändern“
- Ansicht „Vorlage“

### Ansicht „Warnmeldungsvorlage“

In der Ansicht „Vorlage“ können Sie Warnmeldungsvorlagen hinzufügen, anzeigen und löschen.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | die Reporting Engine konfigurieren | Konfigurieren der Reporting Engine |
| Administrator/Analyst | eine Warnmeldung konfigurieren | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung planen | Planen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung anzeigen | Anzeigen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung ermitteln | Ermitteln einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung und eine Warnmeldungsvorlage managen* | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

Übersicht über Warnmeldungen

Konfigurieren einer Warnmeldung

Planen einer Warnmeldung

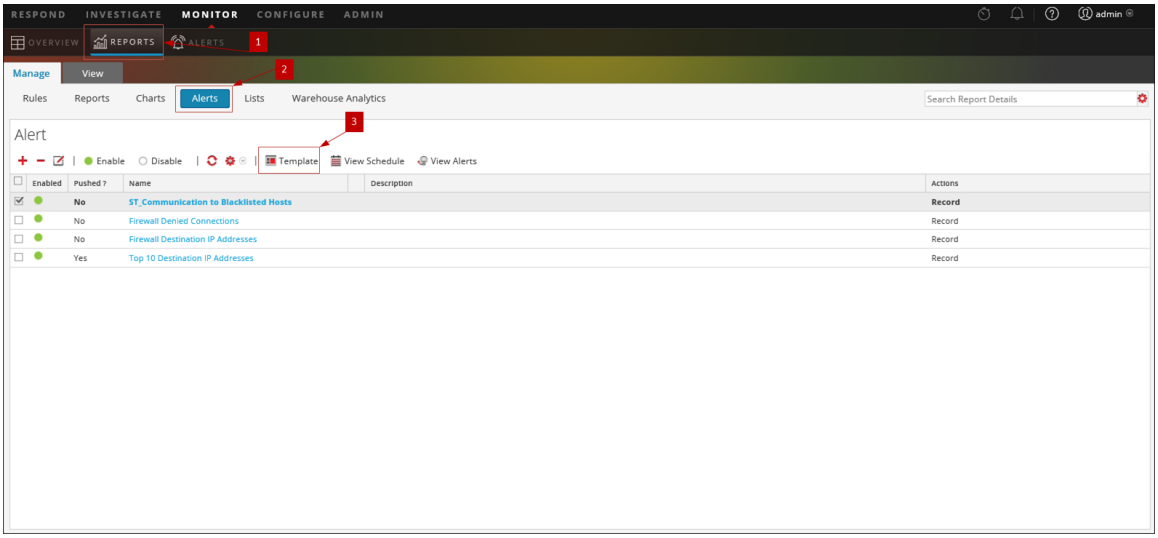
Anzeigen einer Warnmeldung

Ermitteln einer Warnmeldung

Managen einer Warnmeldung und Warnmeldungsvorlage

## Schnellansicht

Die folgende Abbildung zeigt ein Beispiel, in dem die wichtigsten Funktionen bezeichnet sind.





| | |
|---|---|
| 1 | Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen. |
| 2 | Klicken Sie auf **Warnmeldungen**, um die Ansicht „Warnmeldung“ anzuzeigen. |
| 3 | Klicken Sie auf Template, um die Ansicht „Vorlage“ zu öffnen. |
| 4 | Mit der Symbolleiste „Vorlage“ können Sie Warnmeldungsvorlagen hinzufügen, ändern und löschen. |
| 5 | Im Bereich „Vorlagenliste“ können Sie eine Liste aller Vorlagen in einem tabellarischen Format anzuzeigen. |

Die Ansicht „Warnmeldungsvorlage“ umfasst die folgenden Bereiche:

- Symbolleiste „Vorlage“
- Vorlagenliste

## Symbolleiste „Vorlage“

Nachdem die Vorlagen definiert wurden, können Sie eine Vorlage auswählen, um das Definieren und Ändern von Warnmeldungen zu erleichtern.

Die folgende Tabelle enthält eine Auflistung und die Beschreibung der Aktionen des Dialogfelds „Vorlage“.

| Aktionen | Beschreibung |
|---|---|
|  | Erstellt eine neue Warnmeldungsvorlage. |
|  | Löscht die ausgewählte Warnmeldungsvorlage. |
|  | Bearbeitet eine vorhandene Warnmeldungsvorlage. |

## Vorlagenliste

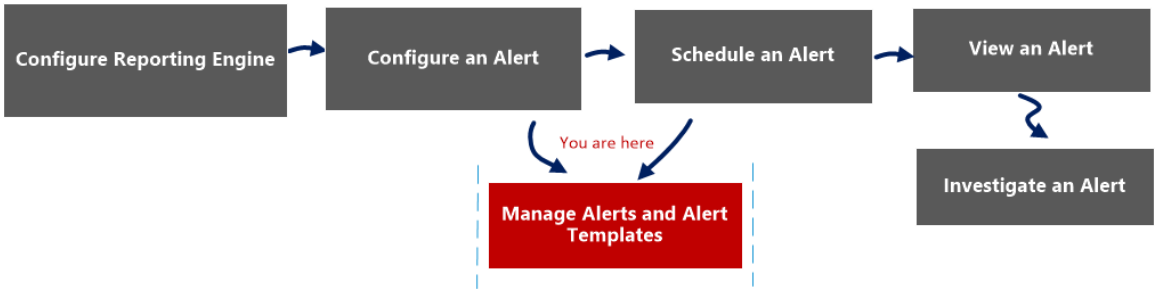
In der folgenden Tabelle sind die Spalten im Bereich „Vorlagenliste“ beschrieben.

| Spalte | Beschreibung |
|---|---|
| Name | Name der Vorlage. |
| Meldung | Die für eine Vorlage definierte Warnmeldung. |

### Ansicht „Vorlage erstellen oder ändern“

In der Ansicht „Vorlage erstellen/ändern“ können Sie Warnmeldungsvorlagen für das Erstellen von Warnmeldungen anpassen.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | die Reporting Engine konfigurieren | Konfigurieren der Reporting Engine |
| Administrator/Analyst | eine Warnmeldung konfigurieren | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung planen | Planen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung anzeigen | Anzeigen einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung ermitteln | Ermitteln einer Warnmeldung |
| Administrator/Analyst | eine Warnmeldung und eine Warnmeldungsvorlage managen* | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

Übersicht über Warnmeldungen

Konfigurieren einer Warnmeldung

Planen einer Warnmeldung

Anzeigen einer Warnmeldung

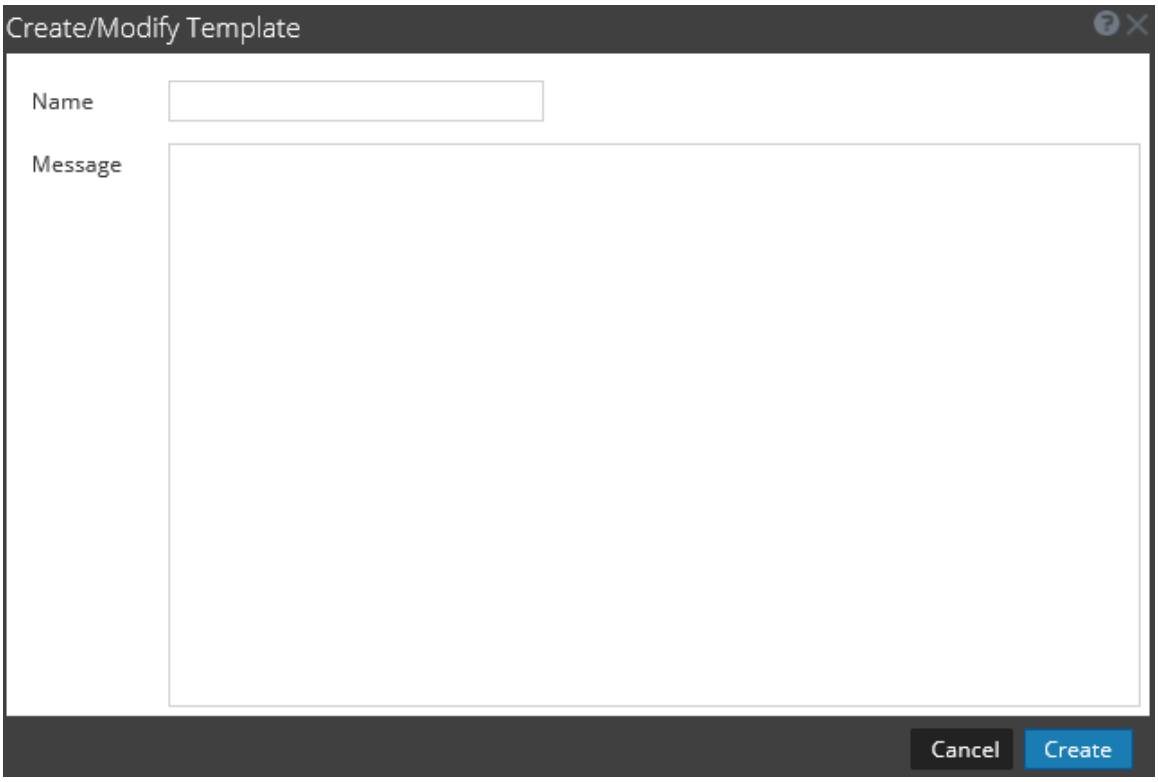
Ermitteln einer Warnmeldung

Managen einer Warnmeldung und Warnmeldungsvorlage

## Schnellansicht

Sie können den Namen einer Warnmeldungsvorlage und die Meldung in dieser Ansicht erstellen oder ändern.

Die folgende Abbildung zeigt ein Beispiel für das Dialogfeld „Warnmeldungsvorlage erstellen/ändern“.




In der folgenden Tabelle sind die Felder des Dialogfelds „Warnmeldungsvorlage erstellen/ändern“ beschrieben.

| Funktion | Beschreibung |
|---|---|
| Name | Zeigt den Namen der Vorlage für Reporting-Warnmeldungen an. Beispielsweise Quell-IP. |
| Meldung | Legt die Meldung fest, die bei Auslösung einer Warnmeldung gesendet wird. |
| Erstellen | Die Vorlage wird mit einer Bestätigungsmeldung erstellt und ist sofort für die Verwendung in Reporting verfügbar. |
| Speichern | Speichert die Vorlage mit den bearbeiteten Details oder wenn eine neue Vorlage erstellt wird. Diese Schaltfläche ist nur im Bearbeitungsmodus sichtbar. |

| Funktion | Beschreibung |
| --- | --- |
| Abbrechen | Schließt das Dialogfeld ohne Speichern der Vorlage oder der Änderungen an der Vorlage. |

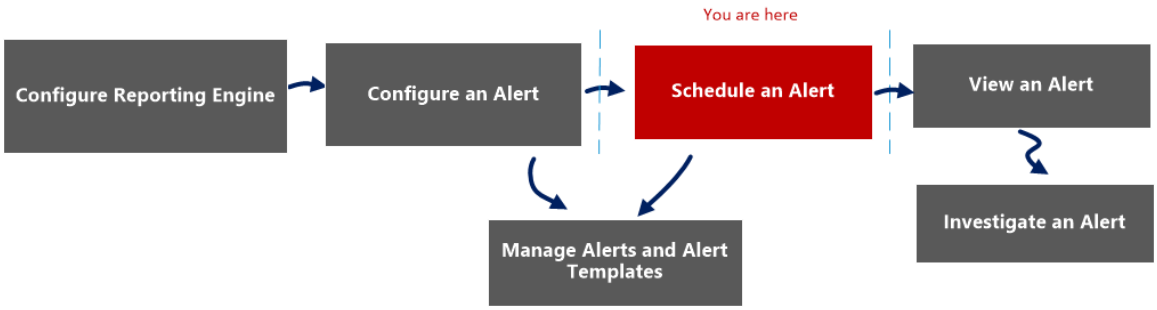
## Ansicht Warnmeldungsplanung anzeigen

In der Ansicht „Warnmeldungsplanung anzeigen“ können Sie die folgenden Informationen zu jeder geplanten Warnmeldung anzeigen.

- Abschlussstatus, Name, letzte Ausführungszeit, letzte Sitzungs-ID, ausgelöste Warnmeldungen insgesamt.
- Statistiken zur Dauer der Ausführung der geplanten Warnmeldung: Dauer, durchschnittliche Dauer, maximale Dauer.

**Hinweis:** Sie können auch geplante Warnmeldungen deaktivieren.

# Workflow




# Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Konfigurieren der Reporting Engine |
| Administrator/Analyst | Konfigurieren einer Warnmeldung | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | Planen einer Warnmeldung* | Planen einer Warnmeldung |
| Administrator/Analyst | Anzeigen einer Warnmeldung | Anzeigen einer Warnmeldung |
| Administrator/Analyst | Untersuchen einer Warnmeldung | Ermitteln einer Warnmeldung |
| Administrator/Analyst | Managen einer Warnmeldung und Warnmeldungsvorlage | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

# Verwandte Themen

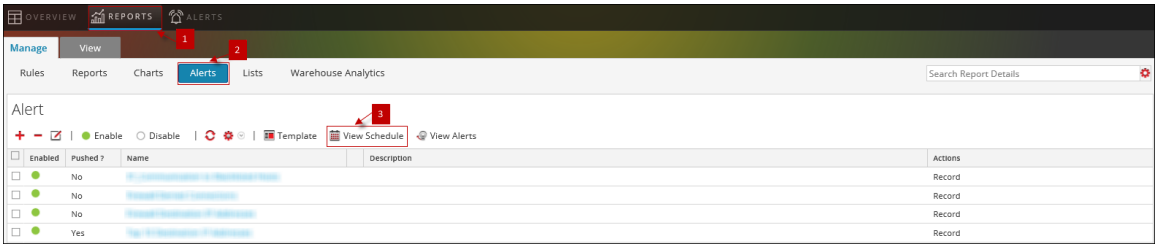
Übersicht über Warnmeldungen

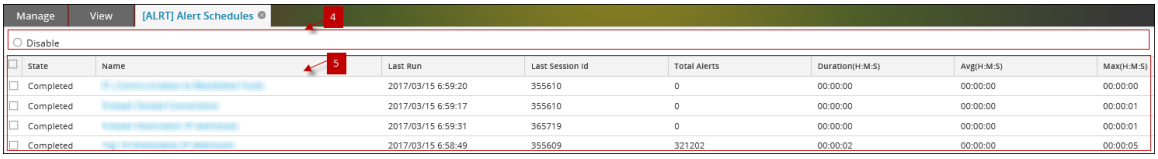
Konfigurieren einer Warnmeldung

Planen einer Warnmeldung

# Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




| | |
|---|---|
| 1 | Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen. |
| 2 | Klicken Sie auf **Warnmeldungen**, um die Warnmeldungsansicht anzuzeigen. |
| 3 | Klicken Sie auf **Zeitplan anzeigen**, um alle geplanten Warnmeldungen anzuzeigen. |
| 4 | In der Symbolleiste „Warnmeldungszeitpläne“ können Sie die geplante Warnmeldung deaktivieren. |
| 5 | In der Liste „Warnmeldungszeitpläne“ können Sie die Details der geplanten Warnmeldungen aufrufen. |

Die Ansicht „Warnmeldungsplanung anzeigen“ umfasst folgende Bereiche:

1. Symbolleiste „Warnmeldungsplanung“
2. Liste „Warnmeldungsplanung“

## Symbolleiste „Warnmeldungsplanung“

Im Symbolleistenbereich „Warnmeldungsplanung“ können Sie den Zustand der geplanten Warnmeldung ändern.

| Funktion | Beschreibung |
|---|---|
| Deaktivieren | Durch Klicken auf **Deaktivieren** wird die ausgewählte Warnmeldung deaktiviert.<br>Wenn geplante Warnmeldungen nicht mehr benötigt werden oder sich als ineffektiv erwiesen haben, können Sie diese deaktivieren, damit sie nicht mehr ausgeführt werden. Sie können eine oder mehrere zu deaktivierende Warnmeldungen auswählen. Wenn eine Warnmeldung deaktiviert wird, wird sie aus der Liste der geplanten Warnmeldungen entfernt, sodass sie hier nicht mehr einsehbar ist, und wird nur dann erneut ausgeführt, wenn Sie die Warnmeldung manuell ausführen oder einen neuen Zeitplan für sie einrichten. |

## Listenbereich Warnmeldungsplanung

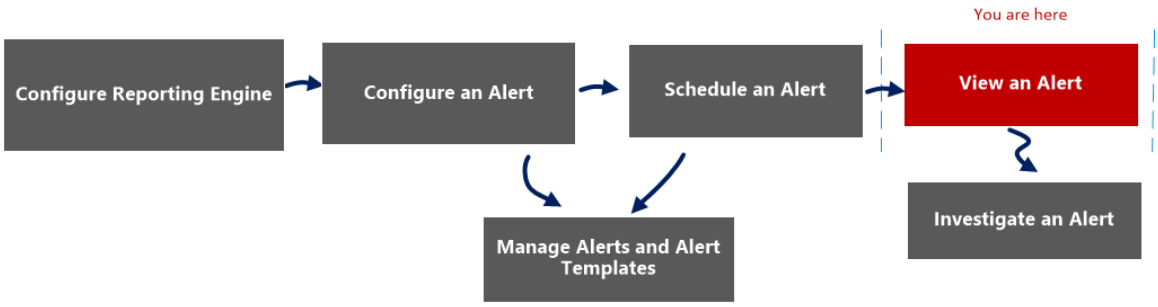
Im Listenbereich „Warnmeldungsplanung“ werden nur die aktivierten Warnmeldungen im Tabellenformat aufgelistet. In der folgenden Tabelle sind die Spalten der Liste „Warnmeldungsplanung“ mit einer Beschreibung aufgeführt.

| Funktion | Beschreibung |
|---|---|
| State | Der Status der geplanten Warnmeldung:<br>• Abgeschlossen<br>• Fehlgeschlagen |
| Name | Der Name der geplanten Warnmeldung |
| Letzte Ausführungszeit | Die letzte Uhrzeit, zu der die geplante Warnmeldung ausgeführt wurde |
| ID der letzten Sitzung | Die Sitzungs-ID der letzten geplante Warnmeldung |
| Warnmeldungen insgesamt | Die Gesamtzahl der Ereignisausführungen |
| Dauer | Wie lange die Ausführung der geplanten Warnmeldung gedauert hat |
| Durchschn. (s) | Wie lange die Ausführung der geplanten Warnmeldung durchschnittlich gedauert hat |
| Max. (s) | Wie lange die Ausführung der geplanten Warnmeldung höchstens gedauert hat |

## Ansicht „Warnmeldungen anzeigen“

In der Ansicht „Warnmeldungen anzeigen“ können Sie alle Warnmeldungen aufrufen. Sie können auch die Ansicht zum Anzeigen von Warnmeldungen für einen bestimmten Zeitraum anpassen und die maximale Anzahl der Warnmeldungen festlegen, die auf einer Seite angezeigt werden.

## Workflow




## Was möchten Sie tun?

| Rolle | Ziel | Dokumentation |
|---|---|---|
| Administrator/Analyst | Konfigurieren der Reporting Engine | Konfigurieren der Reporting Engine |
| Administrator/Analyst | Konfigurieren einer Warnmeldung | Konfigurieren einer Warnmeldung |
| Administrator/Analyst | Planen einer Warnmeldung | Planen einer Warnmeldung |
| Administrator/Analyst | Anzeigen einer Warnmeldung* | Anzeigen einer Warnmeldung |
| Administrator/Analyst | Untersuchen einer Warnmeldung | Ermitteln einer Warnmeldung |
| Administrator/Analyst | Managen einer Warnmeldung und Warnmeldungsvorlage | Managen einer Warnmeldung und Warnmeldungsvorlage |

*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

Übersicht über Warnmeldungen

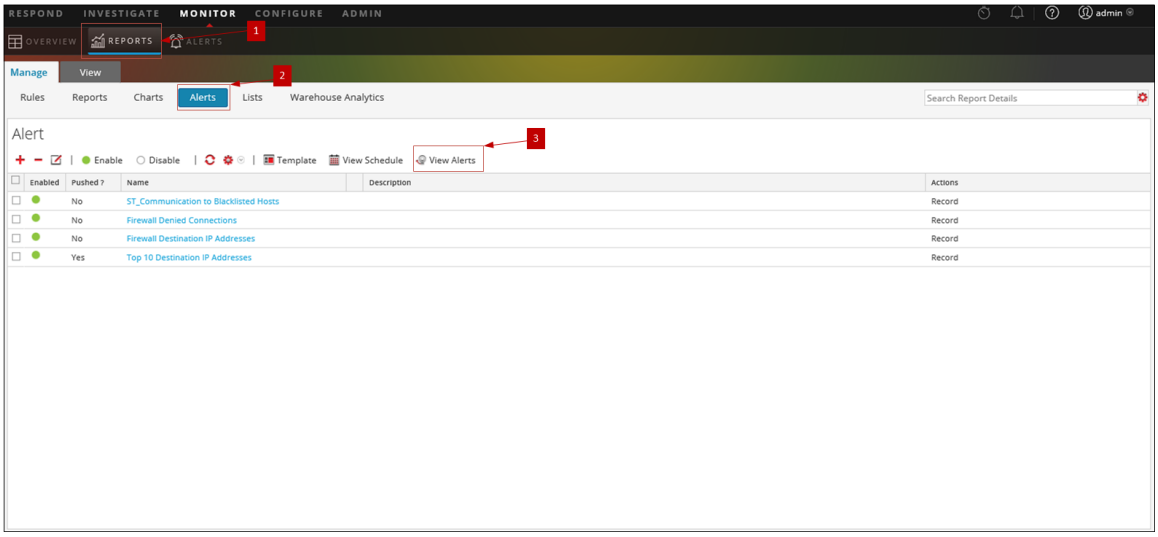
Konfigurieren einer Warnmeldung

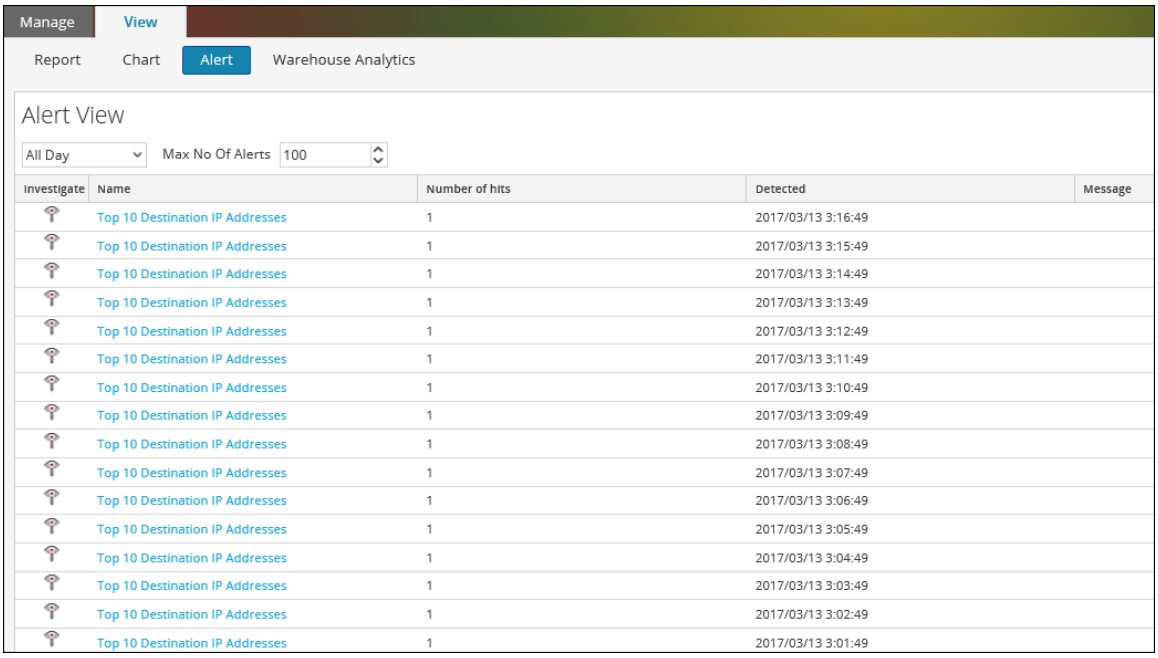
Planen einer Warnmeldung

Anzeigen einer Warnmeldung

# Schnellansicht

Die folgende Abbildung zeigt ein Beispiel mit der Bezeichnung der wichtigsten Funktionen.




| | |
|---|---|
| 1 | Klicken Sie auf **Monitor**> **Berichte**, um die Registerkarte „Managen“ anzuzeigen. |
| 2 | Klicken Sie auf **Warnmeldungen**, um die Warnmeldungsansicht anzuzeigen. |
| 3 | Klicken Sie auf **Warnmeldungen anzeigen**, um die verschiedenen Bereiche unter „Warnmeldungen anzeigen“ aufzurufen. |
| 4 | In der Symbolleiste im Bereich „Warnmeldungen anzeigen“ können Sie Warnmeldungen nach Anzahl oder Start- und Enddatum der Warnmeldungen filtern. |

5 Im Bereich „Liste der Warnmeldungen anzeigen“ werden alle gefilterten Warnmeldungen in tabellarischer Form aufgeführt.

Die Ansicht „Warnmeldungen anzeigen“ umfasst die folgenden Bereiche:

- Symbolleiste „Warnmeldungen anzeigen“
- Liste der Warnmeldungen anzeigen

## Symbolleiste „Warnmeldungen anzeigen“

In der folgenden Tabelle sind die Vorgänge in der Symbolleiste „Warnmeldungen anzeigen“ aufgeführt.

| Option | Beschreibung |
|---|---|
| Daten der letzten Stunde(n) | Die Daten, die seit der letzten Ausführung abgerufen wurden. |
| Max. Anzahl von Warnmeldungen | Die maximale Anzahl von Warnmeldungen, die von der Reporting Engine für einen bestimmten Zeitraum abgerufen werden sollen. |

## Liste der Warnmeldungen anzeigen

In der folgenden Tabelle sind die verschiedenen Spalten im Bereich „Liste der Warnmeldungen anzeigen“ aufgeführt.

| Spalte | Beschreibung |
|---|---|
|  | Durch Klicken auf die Schaltfläche wird das Modul Investigation geöffnet, in dem die Details der ersten Sitzung, in der die Übereinstimmung mit der Warnmeldung registriert wurde, zwecks einer genauen Analyse angezeigt werden.<br>**Hinweis:** In folgenden Fällen werden Sie nicht an das Modul Investigation weitergeleitet:<br>- Sie konfigurieren eine Datenquelle für eine vorhandene Warnmeldung erneut und führen eine Warnmeldung für die neue Datenquelle aus.<br>- Sie geben einen Hostnamen anstelle einer IP-Adresse im Datenquellfeld ein. |
| Name | Der Name der Warnmeldung, die die Übereinstimmung registriert hat. Über den Hyperlink zu dem Namen wird das Modul Investigation geöffnet, in dem alle Übereinstimmungen innerhalb der Stunde um die registrierte Warnmeldung angezeigt werden. |

| Spalte | Beschreibung |
| --- | --- |
| Anzahl der Treffer | Die Häufigkeit, mit der die Warnmeldung erzeugt wird. |
| Detected | Datum und Uhrzeit der Warnmeldung. |
| Meldung | Der Text der Warnmeldung |