RSA NETWITNESS® SUITE

Context Hub-Konfigurationsleitfaden

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

Funktionsweise von Context Hub

Context Hub ist ein Service, der Anreicherungsabfragefunktionen in den Ansichten für Reaktion und Untersuchungen bereitstellt. Ein Administrator kann den Context Hub-Service und die Datenquellen zum Aktivieren eines Analysten konfigurieren, der Kontextabfragen für die erforderlichen Datenquellen durchführt.

Der Context Hub-Service unterstützt standardmäßig Erweiterungsabfragen für Metadatentypen wie z. B. IP-Adresse, Benutzer, Domain, MAC-Adresse, Dateiname, Datei-Hash und Host.

Die folgenden Datenquellen werden von NetWitness Suite unterstützt und übergeben bei entsprechender Konfiguration angereicherte Daten.

Listen: Bietet kontextbezogene Informationen aus einer Liste von Blacklists, Whitelists oder Watchlists.

RSA Archer: Bietet wichtige Informationen zu einem Gerät oder einer bestimmte Ressource, basierend auf der IP-Adresse oder dem Host, der konstante Überwachung erfordert.

Active Directory: bietet kontextbezogene Informationen zu einem Benutzer, um zu bestimmen, ob dieser verdächtig ist oder nicht.

RSA NetWitness® Endpoint: Bietet Kontextinformationen zu Endpunktmodulen und Maschinen, um zu bestimmen, ob eines der Endpunktgeräte infiziert ist.

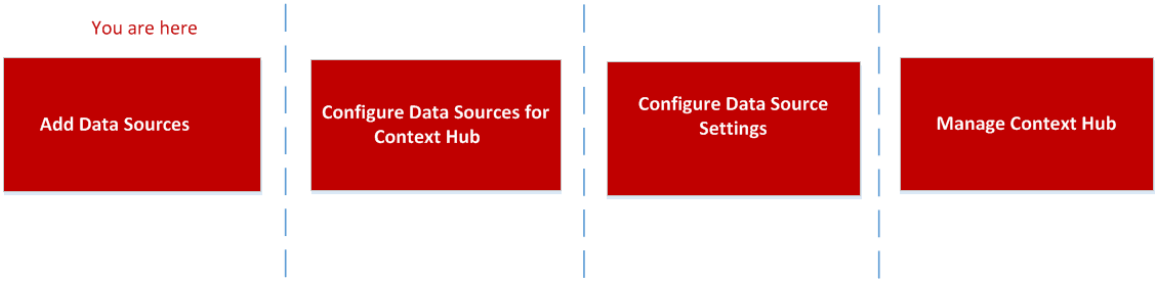
Respond: Bietet kontextbezogene Daten zu bestimmten Metadaten, die in Respond verfügbar sind und es Analysten ermöglichen, schneller und basierend auf Kontextdaten zu reagieren.

Live Connect: Bietet kontextbezogene Daten zu IP-Adressen, Domains und Datei-Hashes vom RSA Live Connect Threat Intelligence Community Server.

Übersicht über die Konfiguration von Context Hub

Der Administrator muss jeden Schritt in der richtigen Reihenfolge ausführen, um die Services so zu konfigurieren, dass Kontextabfragen effektiv durchgeführt werden. In der Ansicht **ADMIN** > **Services** > „Service-Konfiguration“ des Context Hub-Services kann ein Administrator Datenquellen für den Context Hub-Service konfigurieren. Der Administrator kann bei Bedarf Kontextabfragen für benutzerdefinierte Metaschlüssel konfigurieren. Darüber hinaus kann er Listen importieren oder exportieren.

Im folgenden Workflow wird beschrieben, wie der Context Hub-Service konfiguriert werden kann:



Der Context Hub-Service ist auf dem primären ESA-Host vorinstalliert und wird der Netwitness-Suite automatisch hinzugefügt.

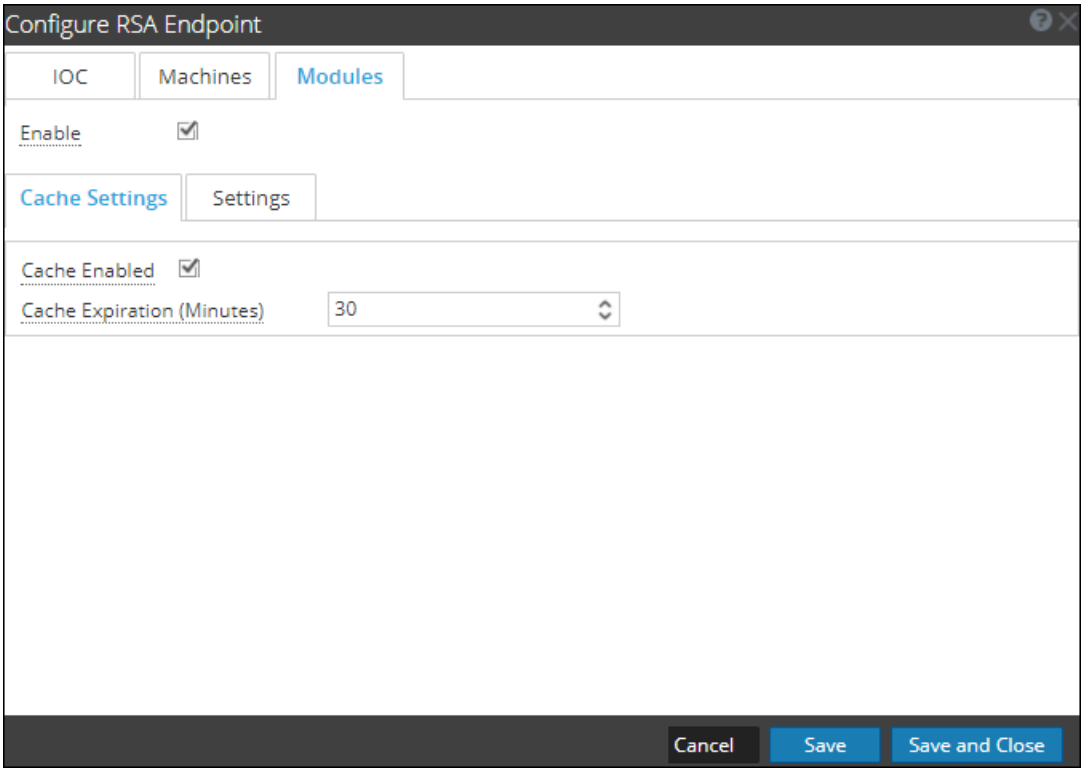
Hinweis: Sie können nur eine Instanz des Context Hub-Services in Ihrer NetWitness Suite-Bereitstellung aktivieren.Wenn mehrere ESA-Services in NetWitness Suite vorhanden sind, müssen Sie den entsprechenden ESA-Host für Context Hub auswählen.Für die Konfiguration von Context Hub auf einem ESA-Host sind mindestens 8 GB Speicherplatz erforderlich.

Konfigurieren der Einstellungen von Datenquellen für den Context Hub

Nachdem Sie die erforderlichen Datenquellen konfiguriert haben, können Sie die Einstellungen für die Datenquellen entsprechend Ihren Anforderungen anpassen.

So rufen Sie Einstellungen auf und konfigurieren sie:

1. Navigieren Sie zu **ADMIN** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie im Bereich **Services** den Context Hub-Service aus und klicken Sie auf Ansicht > **Konfiguration**.
   Die Ansicht „Service-Konfiguration“ von Context Hub wird angezeigt.
3. Wählen Sie die Datenquelle aus, für die Sie die Einstellungen konfigurieren möchten, und klicken Sie auf  in der Spalte „Aktionen“.
   Der folgende Screenshot zeigt ein Beispiel des Dialogfelds für NetWitness Endpoint-Einstellungen:



4. Konfigurieren Sie die folgenden Felder:

Feld	Beschreibung
Aktivieren	Diese Option ist standardmäßig aktiviert und kann verwendet werden, um die Antwort von der ausgewählten Datenquelle zu aktivieren oder zu deaktivieren.
Cacheeinstellungen	Alle Abfragen von Context Hub können eine konfigurierte Zeit lang im Context Hub-Cache gespeichert werden. Antworten auf nachfolgende übereinstimmende Anforderungen werden aus dem Context Hub-Cache abgerufen. Verwenden Sie diesen Abschnitt, um die folgenden Cacheeinstellungen für Abfragen zu definieren: • **Cache aktiviert**: Standardmäßig ist dieses Kontrollkästchen aktiviert und die Abfrageantwort wird zwischengespeichert. • **Cacheablauf (Minuten)**: Die maximale Zeit, die die Abfrage im Cache aufbewahrt wird. Der Standardwert lautet 30 Minuten und maximal können Sie 7200 Minuten konfigurieren.
Ablaufdatum des Listenwerts	**Aktivieren**: Wählen Sie „Aktivieren“ aus, um die Anzahl an Tagen zu definieren, für die die Listenwerte verfügbar sein müssen. Diese Option ist standardmäßig deaktiviert und die Werte werden beibehalten. **Lebensdauer (Tage)**: Geben Sie die Anzahl an Tagen ein, für die die Listenwerte beibehalten werden sollen.
Metazuordnung	Listen, die in Context Hub gespeichert werden, müssen für eine Abfrage verfügbar gemacht werden. Die Abfrage in Context Hub wird je nach Metatyp oder Einheiten durchgeführt. Beispiele für IP, HOST, MAC-ADRESSE, DOMAIN, FILE_NAME, FILE_HASH, BENUTZER. **Metadatentyp**: Verfügbare Einheiten in Context Hub. **Context Hub-Felder**: Die Spaltenüberschrift aus der CSV-Datei, die Sie beim Hinzufügen der Listendatenquelle hinzugefügt haben.

Feld	Beschreibung
IIOC-Mindestwert	Der IIOC-Mindestwert, der für das Abrufen der Kontextinformationen von NetWitness Endpoint-Modulen zu berücksichtigen ist.
Letzte Abfrage (Tage)	Die Dauer (in Tagen), für die Kontextdaten abgefragt werden müssen.
Einschränkung	Die maximale Anzahl von Datensätzen, die bei einer Kontextabfrage angezeigt werden können.
Wiederholungsintervall	Konfigurieren Sie wiederkehrende Pläne, um Kontextdaten für die erforderlichen Intervallen abzurufen und zu speichern.

5. Klicken Sie auf eine der folgenden Optionen:
   - **Abbrechen** – Wählen Sie diese Option, um die Änderungen zu verwerfen.
   - **Speichern** – Wählen Sie diese Option, um die Änderungen zu speichern.
   - **Speichern und schließen** – Wählen Sie diese Option, um zu speichern und das Dialogfeld zu schließen.

Basierend auf der Datenquelle, die Sie auswählen, unterscheiden sich die Antwortgruppen. Die folgende Tabelle beschreibt die Antwortgruppen für jede Datenquelle.

Datenquelle (Verbindung)	Unterstützte Antwortgruppen	Feldeinstellungen
 Liste	Liste	Meta-Zuordnung Metatyp Context Hub-Felder Einstellungen Daten-Pre-Fetch-Einstellungen Geplante Wiederholung Ablaufdatum des Listenwerts Cache-Einstellungen Cache aktiviert Cache-Ablauf (Minuten) [Min. sind 30 Minuten, Max. sind 7200 Minuten]

Datenquelle (Verbindung)	Unterstützte Antwortgruppen	Feldeinstellungen
RSA Archer	Archer	Cache-Einstellungen Cache aktiviert Cache-Ablauf (Minuten)
Active Directory	Benutzer	Metazuordnung Metadatentyp Context Hub-Felder Einstellungen Einstellungen Daten-Pre-Fetch Geplante Wiederholung Ablaufdatum des Listenwerts Cacheeinstellungen Cache aktiviert Cache-Ablauf (Minuten) [Min. sind 30 Minuten, Max. sind 7200 Minuten]
RSA Endpoint	IOC Rechner Module	Cache-Einstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen Einstellungen Kontextbereich Cache-Einstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen Einstellungen Kontextbereich Cache-Einstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen IIOC-Mindestwert Einstellungen Kontextbereich

Datenquelle (Verbindung)	Unterstützte Antwortgruppen	Feldeinstellungen
Reagieren	-Warnmeldungen Incidents	Einstellungen Kontextbereich Daten-Pre-Fetch-Einstellungen Abfrage der letzten [Tage Cache-Einstellungen Cache aktiviert Cache-Ablauf (Minuten)
Live Connect	Domain Datei IP	Cache-Einstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen Einstellungen Kontextbereich

Hinweis: Nach dem Konfigurieren der Datenquelleneinstellungen können Sie die Parameter für die Context Hub-Konfiguration konfigurieren, indem Sie zu **ADMIN** > **Services** > **Ansicht** > **Durchsuchen** navigieren. Stellen Sie sicher, dass Sie den Context Hub-Service neu starten, wenn Sie in der Ansicht „Durchsuchen“ Konfigurationsänderungen vornehmen.

Importieren oder Exportieren von Listen für Context Hub

Als Administrator können Sie eine Liste importieren oder exportieren, die im Context Hub-Service konfiguriert wird und von einem Analysten verwendet werden kann. Bei der Datei, die importiert oder exportiert wird, handelt es sich um eine CSV-Datei. Sie können mehrere Listen als Datenquellen hinzufügen.

Voraussetzungen

Stellen Sie sicher, dass Context Hub aktiviert ist und dass der Service in der Ansicht **Admin** > **Services** von NetWitness Suite verfügbar ist.

Importieren einer Liste

Nachdem Sie eine Liste importiert haben, können Sie die folgenden Aufgaben ausführen:

- Importieren von Werten in eine vorhandene Liste
- Hinzufügen von Zeilen zu einer Liste
- Bearbeiten von Name und Beschreibung einer Liste
- Bearbeiten von Werten aus einer Liste
- Löschen einer Liste
- Löschen von Zeilen aus einer Liste

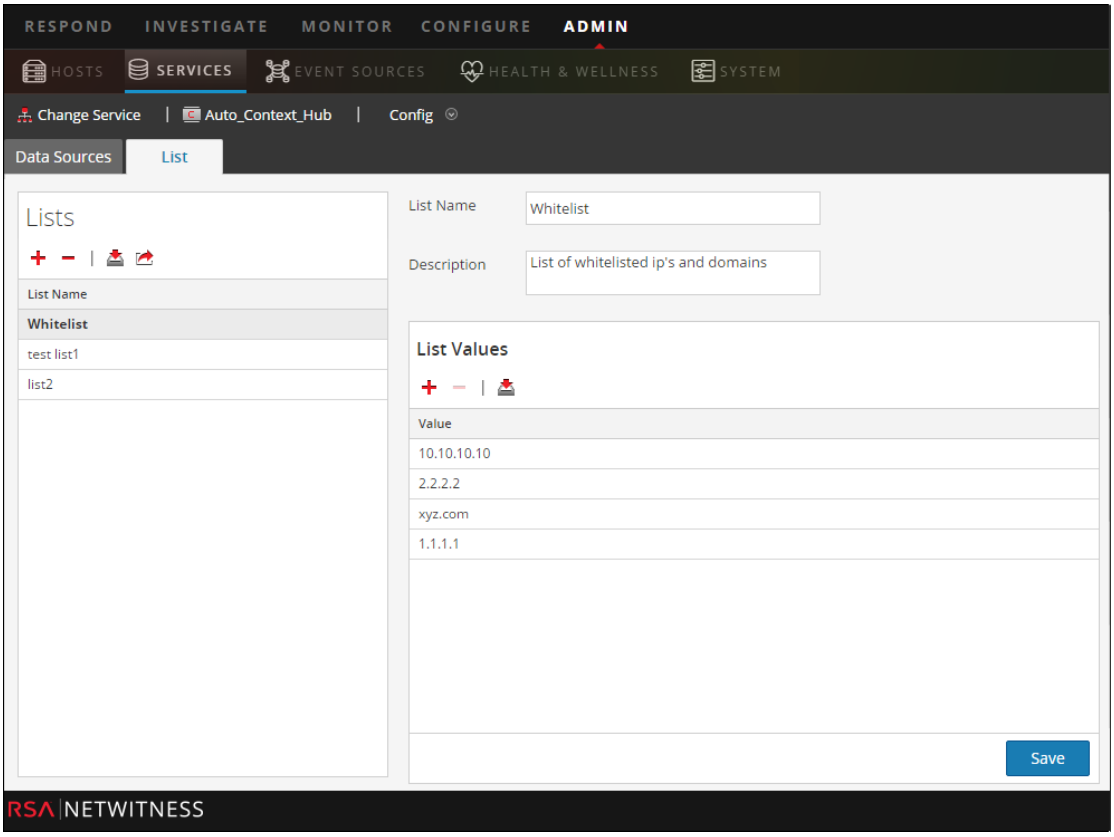
Hinweis: Sie müssen dieselben Änderungen an der entsprechenden CSV-Datei vornehmen, damit diese beim nächsten Mal berücksichtigt werden, wenn der Plan erneut durchgeführt wird. Anderenfalls werden beim Importieren von Werten in eine bestehende Liste mit einer oder mehreren Spalten die Daten aus der Quelldatei überschrieben, wenn der Plan das nächste Mal durchgeführt wird.

Importieren einer einspaltigen Liste

So importieren Sie eine Liste:

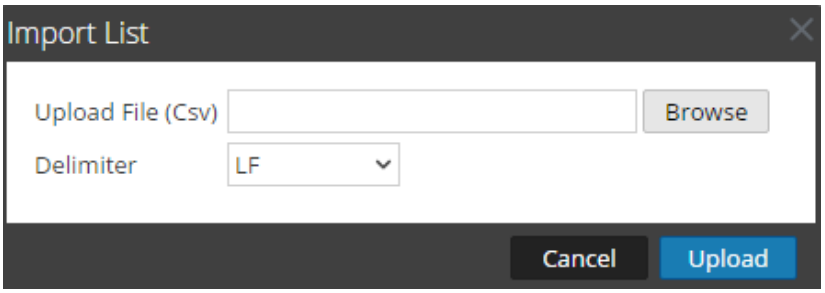
1. Wählen Sie ADMIN > **Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie im Bereich **Services** den Context Hub-Service aus und klicken Sie auf  > **Ansicht** > **Konfiguration**.
   Die Ansicht „Services“ > „Konfiguration“ des Context Hub-Services wird angezeigt.
3. Klicken Sie auf die Registerkarte **Listen**.
   Die Registerkarte „Listen“ besteht aus dem Bereich **Listen** und dem Bereich **Listenwerte**.

Die Abbildung unten zeigt ein Beispiel für eine einspaltige Liste.



4. Klicken Sie im Bereich **Listen** auf  .

   Das Dialogfeld **Liste importieren** wird angezeigt.



5. Schließen Sie im Dialogfeld **Liste importieren** die folgenden Schritte ab:

   a. Suchen Sie im Feld **Datei hochladen (CSV)** nach der `CSV`-Datei und wählen Sie diese aus.

   b. Wählen Sie im Feld **Trennzeichen** das Trennzeichen zum Trennen der Werte in einer Liste aus den Optionen **Komma**, **CR** (Wagenrücklauf) und **LF** (Zeilenvorschub) aus.

6. Klicken Sie auf **Hochladen**, um die CSV-Datei zu Context Hub hochzuladen.

Diese Listen werden als Datenquellen für das Abrufen von Kontextinformationen betrachtet. Sie können jedoch Daten an eine vorhandene Liste mit mehreren Spalten anhängen. Die Daten werden nur dann angehängt, wenn die Anzahl der Spalten übereinstimmt.

Hinweis: Sie können durch Import keine neuen Listen mit mehreren Spalten erstellen. Informationen zum Importieren von Listen mit mehreren Spalten finden Sie unter Konfigurieren von Listen als Datenquelle für Context Hub.

Importieren von Werten in eine vorhandene Liste

Beim Importieren von Werten in eine bestehende Liste mit mehreren Spalten werden die Daten aus der Quelldatei überschrieben, wenn der Plan das nächste Mal durchgeführt wird.

So importieren Sie Werte in eine Liste:

1. Navigieren Sie zu **ADMIN** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Klicken Sie auf  > **Ansicht** > **Konfiguration**.
   Die Ansicht „Services“ > „Konfiguration“ des Context Hub-Services wird angezeigt.
3. Klicken Sie auf die Registerkarte **Listen**.
   Die Registerkarte „Listen“ besteht aus dem Bereich **Listen** und dem Bereich **Listenwerte**.
4. Wählen Sie im Bereich „Listen“ eine Liste aus, für die Sie Werte importieren möchten.
5. Klicken Sie im Bereich **Listenwerte** auf  .
   Das Dialogfeld **Liste importieren** wird angezeigt.
6. Schließen Sie im Dialogfeld **Liste importieren** die folgenden Schritte ab:
   a. Suchen Sie im Feld **Datei hochladen (CSV)** nach der `CSV`-Datei und wählen Sie diese aus.
   b. Wählen Sie im Feld **Trennzeichen** das Trennzeichen zum Trennen der Werte in einer Liste aus den Optionen **Komma**, **CR** (Wagenrücklauf) und **LF** (Zeilenvorschub) aus.
7. Klicken Sie auf **Hochladen**,um die CSV-Datei nach NetWitness Suite hochzuladen.

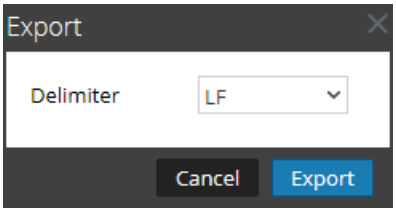
Die Listenwerte werden in die ausgewählte Liste importiert. Diese Listen werden als Datenquellen für das Abrufen von Kontextinformationen betrachtet. Sie können jedoch Daten an eine vorhandene Liste mit mehreren Spalten anhängen. Die Daten werden nur dann angehängt, wenn die Anzahl der Spalten übereinstimmt.

Exportieren einer Liste für Context Hub

So exportieren Sie eine Liste:

1. Klicken Sie in der Ansicht „Service-Konfiguration“ des Context Hub-Services auf der Registerkarte **Liste** auf  .

   Das Dialogfeld **Exportieren** wird angezeigt.



2. Wählen Sie im Feld **Trennzeichen** das Trennzeichen zum Trennen der Werte in einer exportierten Liste aus dem Drop-down-Menü **Komma**, **CR** (Wagenrücklauf) und **LF** (Zeilenvorschub) aus.
3. Klicken Sie auf **Exportieren**.

Im Falle einer einspaltigen Liste können Sie das Trennzeichen auswählen. Im Falle einer Liste mit mehreren Spalten wird die Liste als CSV-Datei auf dem lokalen Rechner exportiert.

Konfigurieren der Metadatentyp-Zuordnung für Context Hub

Als Administrator verwalten Sie die Zuordnung der Context Hub-Metadatentypen zu Netwitness-Metaschlüsseln.

Der Context Hub-Service stellt eine Kontextabfrage für Metawerte in den Respond- und Investigation-Ansichten bereit. Diese Metawerte werden basierend auf der Kategorie, zu der Sie gehören, in Metadatentypen gruppiert. Beispiel: Metaschlüssel von NetWitness Suite Respond und Investigation, wie `ip.src` und `ip.dst`, werden in Context Hub im Metadatentyp `IP` gruppiert. Der Metadatentyp `IP` wiederum ist Metawerten wie `alert.events.source.device.ip_address` und `alert.events.destination.device.ip_address` in der Reagieren-Datenbank zugeordnet.

In der Ansicht **ADMIN**> **System** > **Investigation** kann der Administrator auf der Registerkarte „Kontextabfrage“ die Zuordnung der Investigation-Metaschlüssel und des Investigation-Metadatentyps konfigurieren. Der Administrator kann Metaschlüssel zur Liste der von Context Hub unterstützten Metadatentypen hinzufügen oder entfernen.

Der Context Hub-Service ist mit einer Standardzuordnung von Metadatentyp und Metaschlüssel vorkonfiguriert, die erwartungsgemäß mit den meisten Bereitstellungen funktioniert, solange keine benutzerdefinierten Zuordnungen für Ihre spezielle Bereitstellung erstellt werden.

Hinweis: Sie können keinen neuen Metadatentyp hinzufügen.

Die Standardzuordnung ist unten beschrieben:

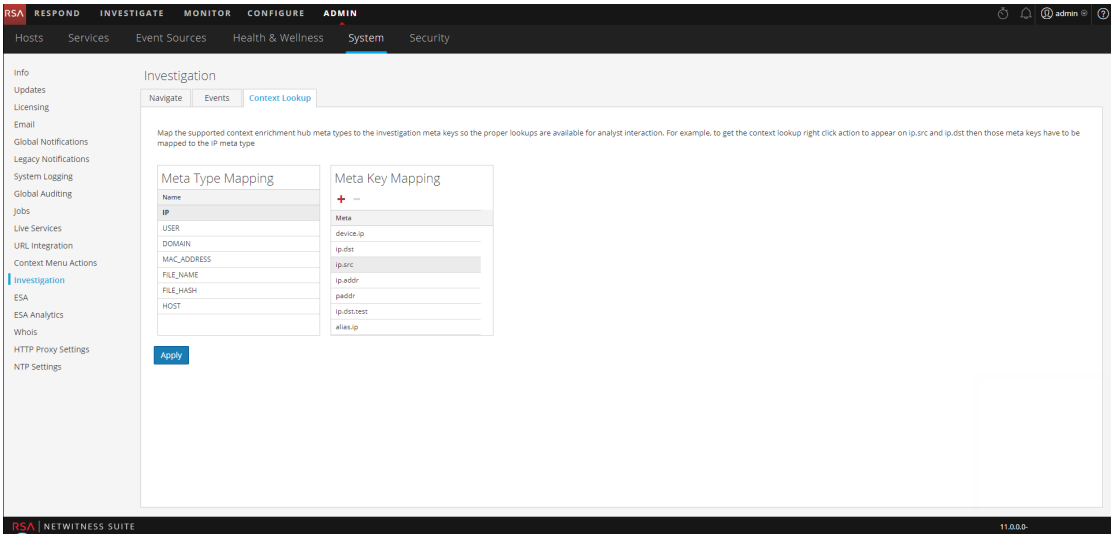
Name des Metadatentyps	Metaschlüssel
IP	device.ip, ip.src, ip.dst, ip.addr,ipv6.src, alias.ip, ipv6.addr, device.ipv6,forward.ip, forward.ipv6,ipv6.dst, ipv6.addr, stransaddr, transaddr
USER	user.src, user.dst, username, event user
DOMAIN	domain.src, domain.dst,fqdn, web.domain, domain, sdomain, ddomain
MAC_ADDRESS	eth.dst, eth.src, alias.mac
FILE_NAME	filename, sourcefile
FILE_HASH	checksum
HOST	device.host, alias.host, host.src, host.dst

Verfahren

So managen Sie die Metaschlüsselzuordnung:

1. Navigieren Sie zu ADMIN > **System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Investigation** aus.

   Der Bereich Investigation-Konfiguration wird angezeigt.
3. Wählen Sie die Registerkarte **Kontextabfrage** aus.



4. Wählen Sie einen Metadatentyp aus, um die Standardmetaschlüssel anzuzeigen, die diesem Metadatentyp zugeordnet sind.
5. Um einen Metaschlüssel hinzuzufügen, klicken Sie auf + und geben Sie den Metaschlüssel ein.
6. Um einen Metaschlüssel zu entfernen, wählen Sie den Metaschlüssel aus und klicken auf −.
7. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.
8. Um neue Metadaten hinzufügen, müssen diese in der benutzerdefinierten Indexdatei für den Concentrator enthalten sein. Beispiel: Wenn Sie einen Metatyp „**Fqdn**“ hinzufügen möchten, müssen Sie einen neuen Eintrag hinzufügen: **<key name="fqdn" description="Fully Qualified Domain Name="IndexValues" form-at="Text" valueMax="100" />**. Weitere Informationen zum Hinzufügen neuer Metadaten in der Indexdatei finden Sie unter „Indexanpassung“ im *Tuningleitfaden für die Core-Datenbank*. Nachdem Sie die neuen Metadaten hinzugefügt haben, können Sie die kontextbezogenen Informationen anzeigen, indem Sie in der Ansicht „Reagieren“ auf die Option „Zu Ermittlungen wechseln“ klicken.

Falls ein neuer Metaschlüssel hinzugefügt wird, wird unter diesem Metaschlüssel die Menüoption „Kontextabfrage“ aktiviert. Weitere Informationen finden Sie im Thema Bereich „Investigation-Konfigurationsbereich“ im *Systemkonfigurationsleitfaden*.

Referenzen zu Context Hub

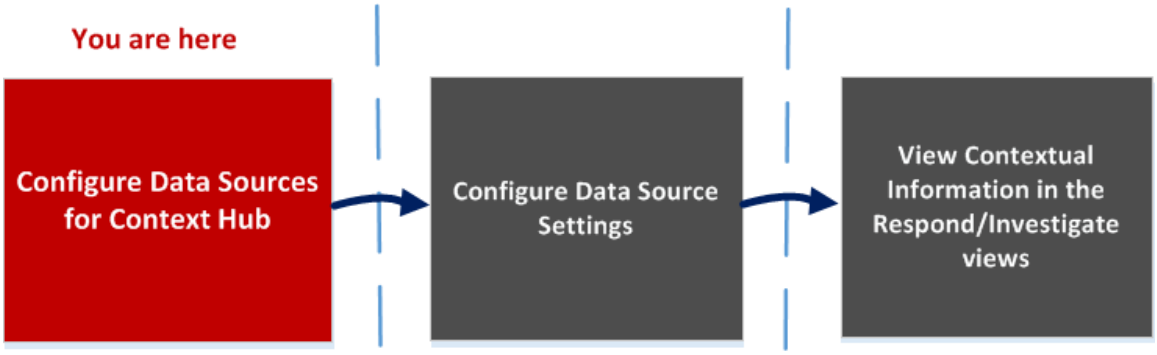
Nachdem Sie den Context Hub-Service und die erforderliche Datenquelle konfiguriert haben, können Sie die Einstellungen für jede Datenquelle managen. Dies hilft bei der Optimierung und Anpassung der Abfrageergebnisse.

Registerkarte „Context Hub-Datenquellen“

Auf der Registerkarte **Datenquellen** können Sie eine oder mehrere Datenquellen für den Context Hub-Service konfigurieren. Navigieren Sie zu **ADMIN** > **SERVICES** > Context Hub-Service > **Ansicht** > **Konfiguration** > Registerkarte **Datenquellen**.

Workflow

Dieser Workflow zeigt das Verfahren zum Konfigurieren von Datenquellen für den Context Hub-Service zum Anzeigen von kontextbezogenen Informationen in den Ansichten „Reagieren“/ „Untersuchen“.



- Die erste Aufgabe besteht darin, eine Datenquelle hinzuzufügen.
- Die zweite Aufgabe ist das Konfigurieren von Datenquellen-Einstellungen zur Verbesserung Ihrer Bereitstellung. Diese Aufgabe ist optional, da die Einstellungen für jede Datenquelle bereits mit Standardwerten für eine optimale Performance konfiguriert sind.
- Und die dritte Aufgabe besteht darin, die kontextbezogenen Informationen im Bereich „Kontextübersicht“ der Ansichten „Reagieren“ oder „Untersuchen“ anzuzeigen und zu analysieren.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Datenquellen für Context Hub konfigurieren*	Konfigurieren von Datenquellen für Context Hub
Administrator	Hub-Dateneinstellungen konfigurieren*	Konfigurieren der Einstellungen von Datenquellen für den Context Hub

Rolle	Ziel	Details anzeigen
Analyst	Kontextbezogene Informationen in der Ansicht „Reagieren“ anzeigen	Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch*.
Analyst	Liste in der Ansicht „Reagieren“ oder „Untersuchen“ hinzufügen, erstellen und löschen	Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch*. Weitere Informationen finden Sie im *Leitfaden zu Investigation und Malware Analysis*.
Analyst	Einen Eintrag aus einer vorhandenen Liste hinzufügen oder löschen	Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch*.

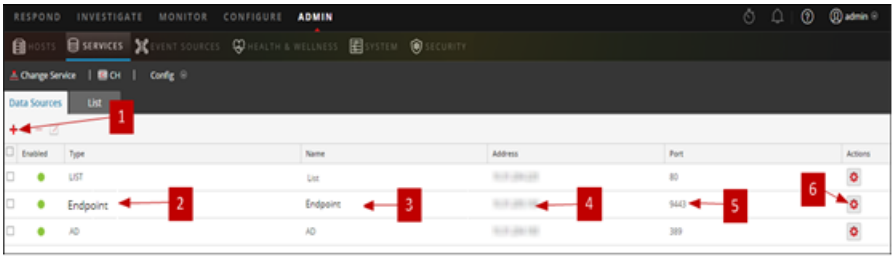
*Sie können diese Aufgabe hier abschließen (das ist die Registerkarte „Context Hub-Datenquellen“).

Verwandte Themen

- Konfigurieren von Listen als Datenquelle
- Konfigurieren von Archer als Datenquelle
- Konfigurieren einer Active Directory-Datenquelle
- Konfigurieren einer Endpunkt NetWitness-Datenquelle
- Konfigurieren einer Respond-Datenquelle
- Konfigurieren einer Live Connect-Datenquelle

Überblick

Das folgende Beispiel zeigt, wie Sie eine Datenquelle für den Context Hub-Service hinzufügen.



1 Klicken Sie auf +, um das Dialogfeld **Datenquelle hinzufügen** anzuzeigen.

2 Zeigt den Typ der Datenquelle an.

3 Name, der die Datenquelle identifiziert.

4 Die IP-Adresse oder der Hostname der Datenquelle.

5 Der Verbindungsport für die Datenquelle.

6 Öffnet das Dialogfeld **Einstellungen konfigurieren**. Sie können die im Bereich „Kontextübersicht“ anzuzeigenden Einstellungen in den Ansichten „Reagieren“ oder „Untersuchen“ anzeigen und bearbeiten.

7 Klicken Sie auf **Verbindung testen** um sicherzustellen, dass der Host mit dem Context Hub-Service verbunden ist.

Symbolleiste

In der folgenden Tabelle werden die Aktionen der Symbolleiste beschrieben.

Funktion	Beschreibung
	Öffnet das Dialogfeld Datenquelle hinzufügen, damit Sie eine Datenquelle hinzufügen können. Sie können nur eine Datenquelle für jeden Typ hinzufügen. Außer im Falle von Listen und Active Directory-Datenquellen, die in Vielfachen hinzugefügt werden können. Ausführliche Anweisungen zum Hinzufügen einer Datenquelle finden Sie unter Konfigurieren von Datenquellen für Context Hub.
	Löschen Sie eine Datenquelle. Wenn Sie eine Datenquelle löschen, berücksichtigt Context Hub den gelöschten Service nicht als Datenquelle. Alle zuvor abgerufenen kontextbezogenen Informationen sind nicht verfügbar.
	Öffnet das Dialogfeld „Datenquelle bearbeiten“. Eine Beschreibung der einzelnen Felder im Bereich „Datenquelle bearbeiten“ finden Sie unter Konfigurieren von Datenquellen für Context Hub.
	Öffnet das Dialogfeld „Einstellungen konfigurieren“. Sie können die Einstellungen für die Datenquellen anzeigen und bearbeiten. Eine Beschreibung der einzelnen Felder im Dialogfeld „Antworten konfigurieren“ finden Sie unter Konfigurieren der Einstellungen von Datenquellen.

Quelldatenkonfigurationen

In der folgenden Tabelle werden die aufgeführten Konfigurationen beschrieben.

Funktion	Beschreibung
Aktiviert	Zeigt an, ob die Datenquelle aktiviert oder deaktiviert ist. Ein vollfarbiger grüner Kreis zeigt an, dass die Datenquelle aktiviert ist ( ). Ein leerer weißer Kreis zeigt an, dass die Datenquelle deaktiviert ist.
Typ	Der Typ der Datenquelle. Z. B. Listen, Archer, Active Directory, Endpunkt, Respond oder Live Connect.
Name	Der eindeutige Name zur Identifizierung der Datenquelle. Beispielsweise „Respond \“.
Adresse	Die IP-Adresse oder der Hostname der Datenquelle.
Port	Der Verbindungsport für die Datenquelle variiert basierend auf der Datenquelle, die hinzugefügt wird. Beispielsweise lautet der Port für Endpunkt 9443, für Listen ist der Port 80 und so weiter.

Registerkarte „Context Hub-Listen“

Auf der Registerkarte **Listen** können Sie Listen für Context Hub erstellen und konfigurieren. Navigieren Sie zu **ADMIN** > **SERVICES** > Context Hub-Service > **Ansicht** > **Konfiguration** > Registerkarte **Listen**.

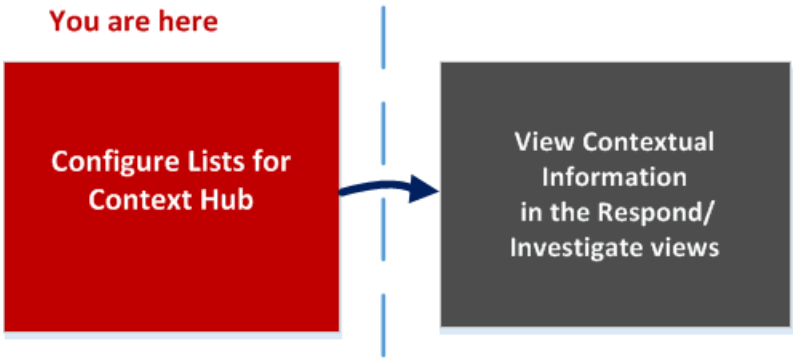
Auf der Registerkarte „Listen“ des Context Hub-Services können Sie eine oder mehrere Listen erstellen und der Liste entsprechende Listenwerte hinzufügen. Diese Listen werden automatisch als Datenquellen für den Context Hub-Service berücksichtigt.

Diese Listen können mit Elementen gefüllt werden. Dafür werden entweder CSV-Dateien importiert oder Metawerte mithilfe der Option „Zu Liste hinzufügen/Aus Liste entfernen“ in den Ansichten „Untersuchen“ und „Reagieren“ hinzugefügt.

Hinweis: Sie können Listen auch über die Ansichten „Reagieren“ und „Investigation“ erstellen und Listenwerte hinzufügen. Weitere Informationen finden Sie im *RSA NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu RSA NetWitness Investigation und Malware Analysis*.

Workflow

Dieser Workflow zeigt das Verfahren zum Konfigurieren von Listen für den Context Hub-Service und zum Anzeigen von kontextbezogenen Informationen in den Ansichten „Reagieren“ und „Untersuchen“.



Das Erstellen einer oder mehrerer Listen ist die erste Aufgabe in diesem Workflow. Die Listen können unterstützte Metadaten wie IP-Adresse, Benutzer, Host, Domain, MAC-Adresse, Dateinamen oder Datei-Hash enthalten. Die nächste Aufgabe ist das Analysieren oder Verwenden der Listendaten zum Anzeigen kontextbezogener Daten in den Ansichten „Reagieren“ und „Untersuchen“.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Listendatenquelle für Context Hub konfigurieren*	Konfigurieren von Listen als Datenquelle für Context Hub
Administrator/Analyst	Kontextbezogene Informationen in der Ansicht „Reagieren“ anzeigen	Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch*.
Administrator/Analyst	Listen und Listenwerte in Investigation managen	Weitere Informationen finden Sie im *Leitfaden zu Investigation und Malware Analysis*.
Administrator/Analyst	Eine Liste erstellen	Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu Investigation und Malware Analysis*.
Administrator/Analyst	Liste aktualisieren	Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu Investigation und Malware Analysis*.
Administrator/Analyst	Liste löschen	Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu Investigation und Malware Analysis*.
Administrator/Analyst	Eine Liste importieren	Importieren oder Exportieren von Listen für Context Hub
Administrator/Analyst	Exportieren von Listen	Importieren oder Exportieren von Listen für Context Hub

*Sie können diese Aufgabe hier abschließen (das ist die Registerkarte „Context Hub-Listen“).

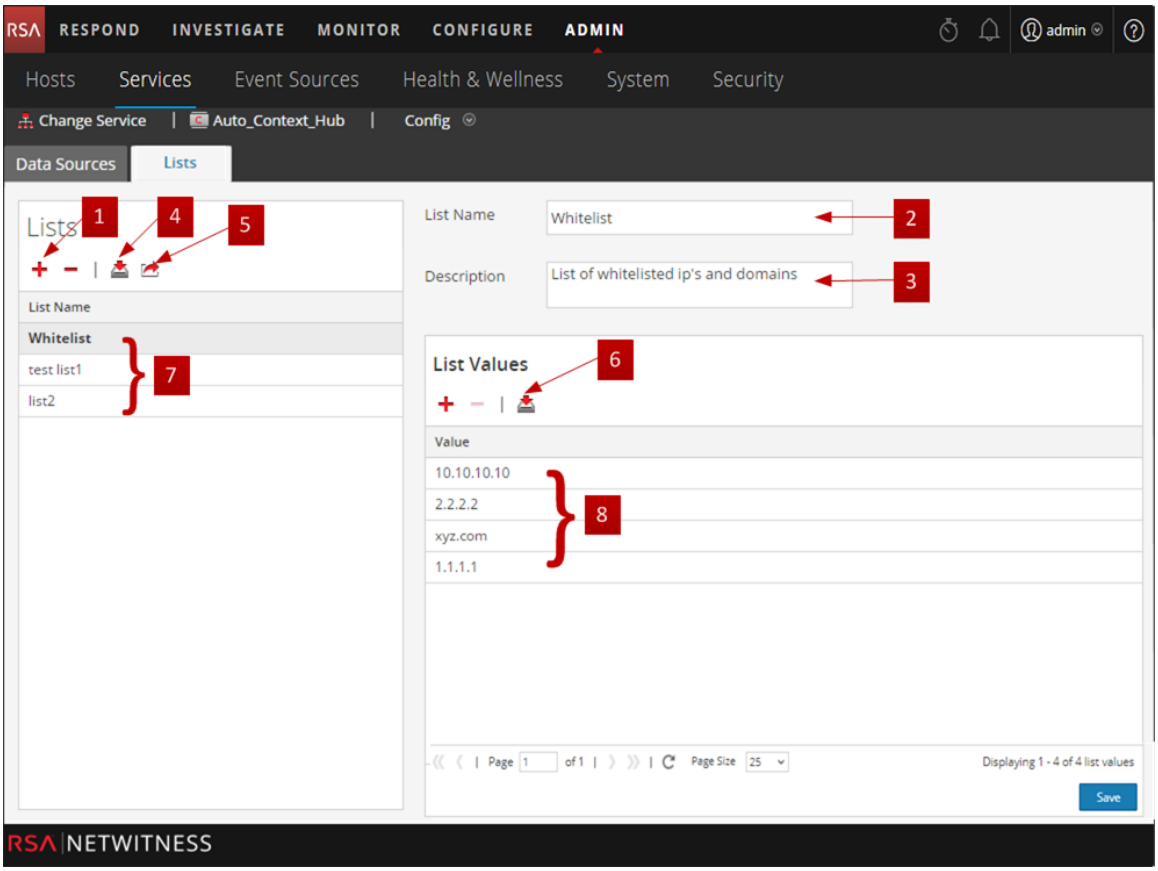
Verwandte Themen

- Registerkarte „Context Hub-Datenquellen“

Überblick

Das folgende Beispiel zeigt, wie Sie Listen für den Context Hub-Service hinzufügen.

Die Registerkarte „Liste“ besteht aus dem Bereich **Listen** und dem Bereich **Listenwerte**. Der Bereich **Listen** verfügt über eine Symbolleiste mit Optionen zum Hinzufügen, Löschen, Importieren und Exportieren von Listen. Die Einträge unter **Listenname** sind Listen, die für den Context Hub-Service hinzugefügt oder importiert werden.
Der Bereich **Listenwerte** verfügt über eine Symbolleiste mit Optionen zum Hinzufügen, Löschen und Importieren von Listenwerten für die ausgewählte Liste. Die Einträge unter **Wert** identifizieren jeden in der Liste enthaltenen Listeneintrag.



1	Klicken Sie auf ✚, um eine neue Liste hinzuzufügen.
2	Name, der die Liste identifiziert.
3	Beschreibung der Liste

4 Klicken Sie auf , um Listen in Context Hub zu importieren.

5 Klicken Sie auf , um eine Liste auf den lokalen Rechner zu exportieren.

6 Klicken Sie auf , um Listenwerte in eine ausgewählte Liste zu importieren.

7 Zeigt die benutzerdefinierte(n) Liste(n), die Context Hub hinzugefügt wird/werden.

8 Zeigt die Listenwerte an, die der ausgewählten Liste hinzugefügt werden.

Symbolleiste

In der folgenden Tabelle werden die Aktionen der Symbolleiste beschrieben.

Funktion	Beschreibung
+	Fügen Sie eine neue Liste hinzu. Weitere Informationen finden Sie unter Konfigurieren von Listen als Datenquelle.
−	Löschen einer Liste. Wenn Sie eine Liste aus Context Hub löschen, wird die Liste nicht mehr als Datenquelle für das Abrufen von kontextbezogenen Informationen betrachtet.
	Importieren Sie Listen in Context Hub. Weitere Informationen finden Sie unter Importieren oder Exportieren von Listen für Context Hub.
	Exportieren Sie eine Liste auf den lokalen Rechner. Weitere Informationen finden Sie unter Importieren oder Exportieren von Listen für Context Hub.

Optionen der Ansicht „Liste“

In der folgenden Tabelle werden die Listenkonfigurationen beschrieben.

Funktion	Beschreibung
Listenname	Eindeutiger Name zur Identifizierung der Liste
Beschreibung	Beschreibung der Liste
Speichern	Speichert die an der Liste durchgeführten Änderungen.

Nächste Schritte

Nach Abschluss der Konfiguration können Sie die kontextbezogenen Daten im Bereich „Kontextübersicht“ der Ansicht „Reagieren“ oder der Ansicht „Untersuchen“ anzeigen. Anweisungen dazu finden Sie im Thema **Navigieren zum Bereich Kontextübersicht und Anzeigen von zusätzlichem Kontext** im *Leitfaden zu Investigation und Malware Analysis*.

Troubleshooting

In diesem Thema finden Sie Informationen zu möglichen Problemen, auf die NetWitness Suite-Benutzer beim Einrichten ihres NetWitness Suite-Services in Security Analytics stoßen können.

Mögliche Probleme

Problem	Lösung
SSL-Handshake mit Archer-Zertifikat schlägt fehl, wenn Sie es als Datenquelle hinzufügen.	Verwenden Sie ein von Archer generiertes Zertifikat mit konfigurierter Option „Allen Zertifikaten vertrauen“.
Die Option „Zu Ermittlungen wechseln“ auf der Respond-Seite führt nicht zum richtigen Link.	Wenn Sie den RabbitMQ-Server beenden und neustarten, ist die auf dem Bildschirm „Reagieren“ angezeigte Option „Zu Ermittlungen wechseln“ nicht sichtbar. Der Bereich „Kontext“ für „Zu Ermittlungen wechseln“ öffnet die gleiche Seite. Sie müssen den Jetty-Service auf dem NetWitness-Server neustarten. Melden Sie sich beim NetWitness-Serverhost an und geben Sie den Befehl zum Neustart des Jetty-Services ein.