RSA NETWITNESS® PLATFORM

Context Hub-Konfigurationsleitfaden

für Version 11.2

Kontaktinformationen

RSA Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie 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 Dell 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 Dell 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

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

February 2019

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 Platform unterstützt und übergeben bei entsprechender Konfiguration angereicherte Daten.

Lists: 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.

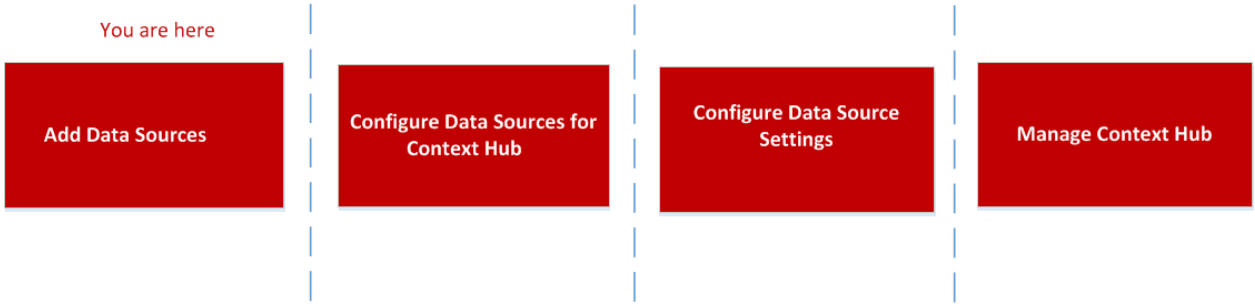
Respond: Bietet kontextbezogene Daten zu bestimmten Metadaten, die in Respond verfügbar sind und es Analysten ermöglichen, schneller und basierend auf Kontextdaten zu reagieren.

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 NetWitness Platform automatisch hinzugefügt.

Hinweis: Sie können nur eine Instanz des Context-Hub-Services in Ihrer NetWitness Platform-Bereitstellung aktivieren.Wenn mehrere ESA-Services in NetWitness Platform 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 von Listen als Datenquelle

Listen als Datenquellen nutzen den Context-Hub-Service, um kontextbezogene Informationen für die Metadatentypen abzurufen, die eine Kontextabfrage unterstützen. Sie können eine oder mehrere Listen erstellen und ihnen entsprechende Listenwerte hinzufügen. Stellen Sie sicher, dass Sie aussagekräftige Listen erstellen, z. B. schwarze oder weiße Listen für IPs. Die Listen können unterstützte Einheiten wie IP-Adresse, MAC-Adresse, Benutzername, Hostname, Domainname, Dateiname oder Datei-Hash enthalten. Sie können eine einspaltige Liste oder eine Liste mit mehreren Spalten von der Registerkarte „Datenquelle“ importieren. Außerdem werden alle erstellten Feeds (ausgenommen STIX-Feeds) in Listen umgewandelt und in der Kontextabfrage angezeigt. Wenn Context Hub nicht konfiguriert oder der Service heruntergefahren ist, werden die Feeds zur Verfügung gestellt, wenn Context Hub betriebsbereit ist. Weitere Informationen zum Erstellen von Feeds finden Sie im *Handbuch zum Live-Services-Management*.

Hinweis: Wenn Sie einen Feed erstellen, wird automatisch eine Liste mit dem gleichen Namen wie der Feed erstellt. Wenn der Listenname bereits vorhanden ist, wird dem Namen der neuen Liste die Zahl „2“ vorangestellt. Wenn der Name des vorhandenen Feeds „test1.csv“ lautet, wird die neue Liste „test2.csv“ benannt.

Listenwerte sind im CSV-Format an einem externen Speicherort verfügbar. Für den Zugriff stehen die folgenden zwei Methoden zur Verfügung:

- **Lokaler Dateispeicher**: Sie können eine Datei von einem lokalen Standort aus freigeben.
- **HTTP(S)**: Sie können eine Datei von einem Speicherort auf einem Webserver aus freigeben.

Hinweis: Sie können während der Konfiguration von Meta-Zuordnungen mithilfe der Pre-Fetch-Einstellungen auch einen wiederkehrenden Job einrichten, der Daten in regelmäßigen Abständen abruft.

Voraussetzungen

Bevor Sie eine Lists-Datenquelle konfigurieren, stellen Sie Folgendes sicher:

- Benutzer sollten über Administratorberechtigungen verfügen.
- Der Context-Hub-Service ist in der Ansicht **ADMIN** > **Services** von NetWitness Platform verfügbar.
- Wenn Sie einen lokalen Dateispeicher oder einen HTTP(S)-Server verwenden, sollte der erwähnte Pfad die CSV-Datei enthalten.
  Im Falle eines lokalen Remote-Dateispeichers muss die Datei gemountet oder auf dem lokalen Laufwerkspeicherort `/var/lib/netwitness/contexthub-server/data` abgelegt werden.
- Der NetWitness-Benutzer muss für den Zugriff auf die Datei über Leseberechtigung verfügen.

Achtung: Wenn Sie eine Context Hub-Liste erstellen, die als Anreicherungsquelle in ESA verwendet werden soll, darf der Name der Liste keine Leerzeichen oder Sonderzeichen enthalten bzw. nicht mit einer Zahl beginnen. Wenn Sie dieser Namenskonvention nicht folgen, wird eine Fehlermeldung angezeigt, wenn Sie versuchen, die Liste als Anreicherungsquelle in ESA hinzuzufügen, und Sie dürfen die Liste nicht hinzufügen.

Hinzufügen von Listendatenquellen über lokalen Dateispeicher

So fügen Sie eine Liste als Datenquelle hinzu:

1. Navigieren Sie zu **ADMIN > Services**.

   Die Ansicht „Services“ wird angezeigt.

2. Wählen Sie den Context Hub-Service aus und klicken Sie auf > **Ansicht** > **Konfiguration**.

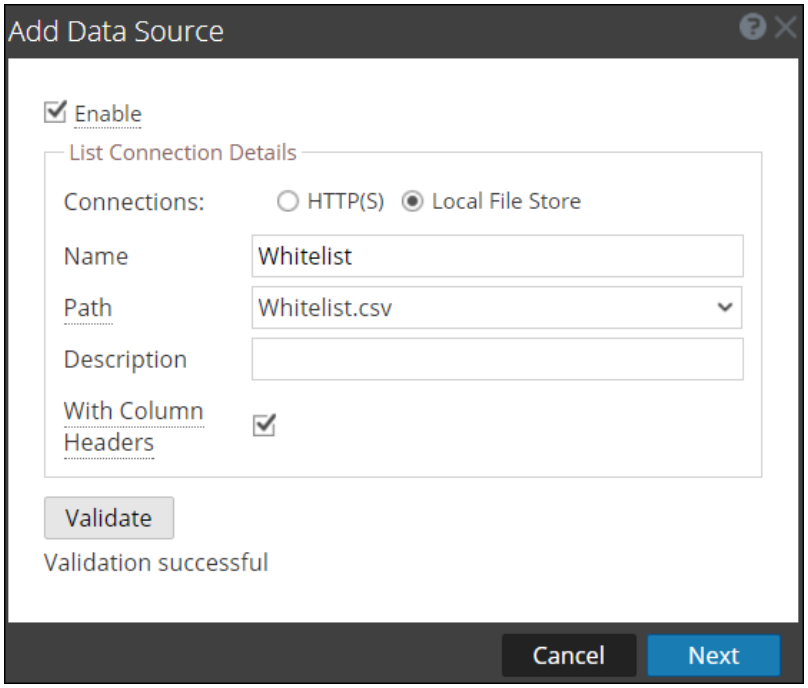
   Die Ansicht „Service-Konfiguration“ von Context Hub wird angezeigt.

3. Klicken Sie auf der Registerkarte **Datenquellen** auf > **LISTEN**.

   Das Dialogfeld **Datenquelle hinzufügen** wird angezeigt

4. Das Kontrollkästchen **Aktivieren** ist standardmäßig ausgewählt. Wenn diese Option nicht aktiviert wird, ist die Schaltfläche zum Speichern deaktiviert. Sie können keine Datenquelle hinzufügen, die Liste nicht auf der entsprechenden Registerkarte abrufen und keine kontextbezogenen Informationen anzeigen.

5. Wählen Sie den Verbindungstyp **Lokaler Dateispeicher**.



6. Geben Sie die folgenden Datenbankverbindungsdetails an. Füllen Sie die folgenden Felder für den Verbindungstyp „Lokaler Dateispeicher“ aus:

   - **Name:** Geben Sie einen Namen für die Datenquelle an.
   - **Pfad:** Dieses Feld zeigt alle Datendateien an, die im Datenordner `/var/lib/netwitness/contexthub-server/data` verfügbar sind, wo der Context-Hub-Service ausgeführt wird. Wählen Sie den Dateinamen in der Drop-down-Liste aus.

Maximal 32 Spalten werden für die CSV-Datei unterstützt, die den RFC1480-Standards entspricht.

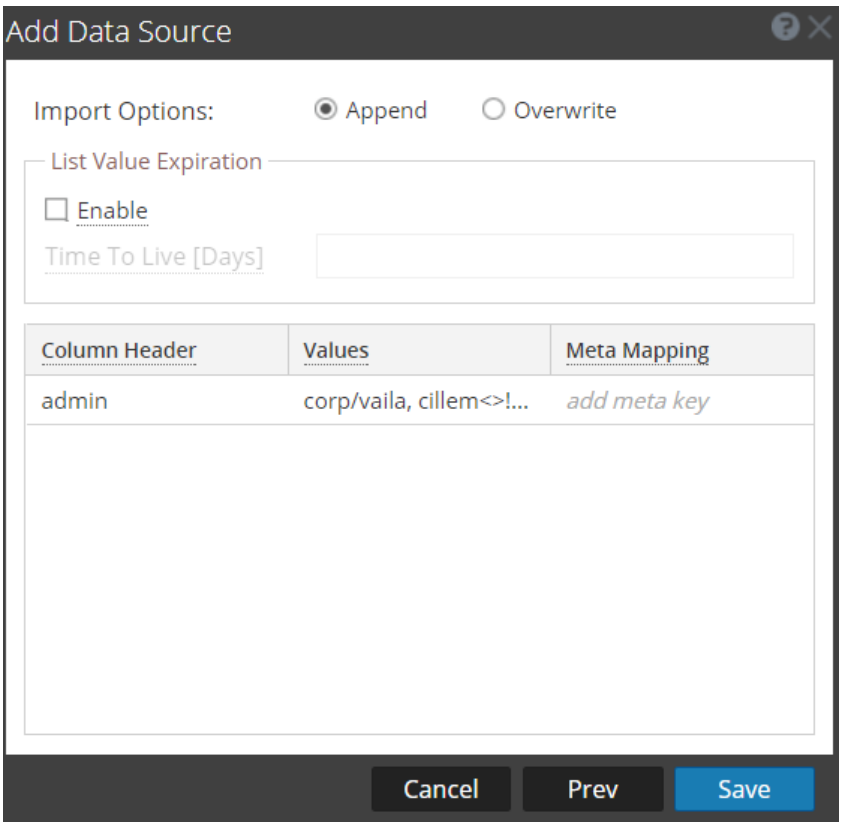
- (Optional) **Beschreibung**: Fügen Sie eine Beschreibung für die ausgewählte Datei hinzu.
- **Mit Spaltenüberschriften**: Wählen Sie diese Option aus, um die erste Zeile aus der CSV-Datei als Spaltenüberschrift zu verwenden. Wenn Sie diese Option nicht auswählen, müssen Sie die Spaltenüberschriften am nächsten Bildschirm eingeben.

7. Klicken Sie auf **Überprüfen**.

   Wenn die Validierung fehlschlägt, können Sie die Datenquelle nicht hinzufügen.

8. Klicken Sie auf **Weiter**.

   Das nächste Dialogfeld wird angezeigt.



9. Wählen Sie eine der folgenden Optionen aus:

   - **Append** – Wählen Sie diese Option, um die importierten Werte einer vorhandenen Liste hinzuzufügen.
   - **Überschreiben** – Wählen Sie diese Option, um die Werte in einer vorhandenen Liste durch die importierten Werte zu ersetzen.

10. Im Abschnitt **Ablaufdatum des Listenwerts** ist die Option **Aktivieren** standardmäßig deaktiviert. Wenn Sie die gesuchten Listenwerte für eine bestimmte Anzahl von Tagen im Cache speichern möchten, markieren Sie das Kontrollkästchen **Aktivieren** und geben die Anzahl der Tage, für die Listenwerte aufbewahrt werden sollen, in das Feld **Lebensdauer (Tage)** ein.

11. Ordnen Sie im nächsten Bildschirm mindestens einen Metaschlüssel einem oder mehreren Metadatentypen zu, indem Sie eine Spaltenüberschrift mit Metadaten zuordnen. Die Beschreibung für jedes Feld lautet wie folgt:
    - **Spaltenüberschrift**: Zeigt die Kopfzeilen der CSV-Datei an, die einem Metadatentyp zugeordnet werden muss.
    - **Metazuordnung**: Ordnet einem Metadatentyp ein Spaltenüberschriftsfeld zu.
    - **Werte**: Zeigt die ersten drei Werte aus der importierten Liste an.
12. Klicken Sie auf **Speichern**.

Hinzufügen von Listendatenquellen mithilfe von HTTP(S)

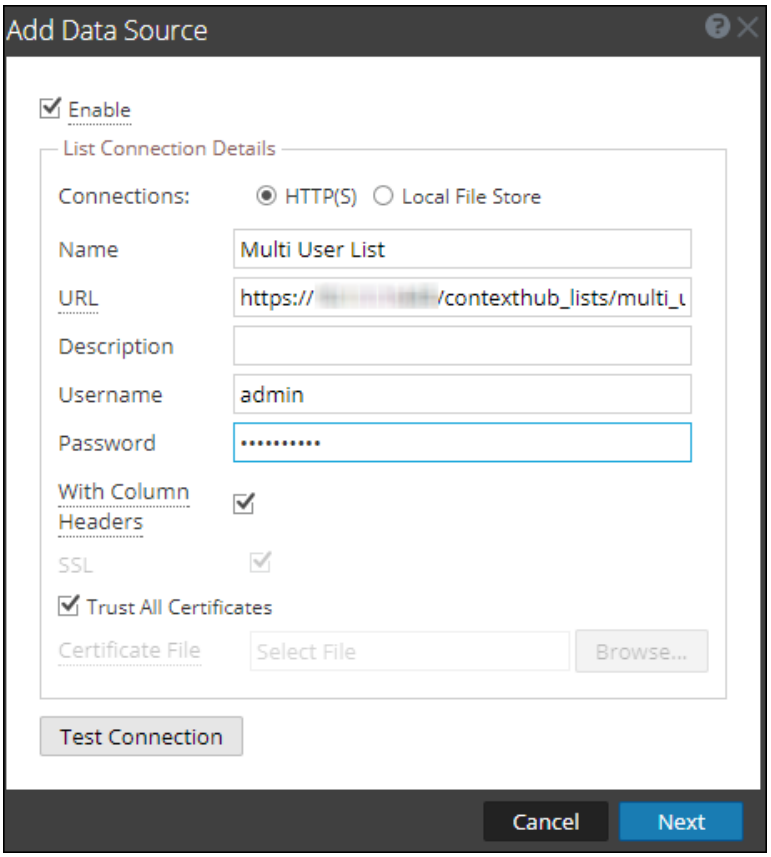
So fügen Sie eine Liste als Datenquelle hinzu:

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

   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie den Context-Hub-Service aus und klicken Sie auf  > **Ansicht** > **Konfiguration**.

   Die Ansicht „Service-Konfiguration“ von Context Hub wird angezeigt.
3. Klicken Sie auf der Registerkarte **Datenquellen** auf  > **LISTEN**.

   Das Dialogfeld **Datenquelle hinzufügen** wird angezeigt.
4. Wählen Sie den Verbindungstyp HTTP(S).



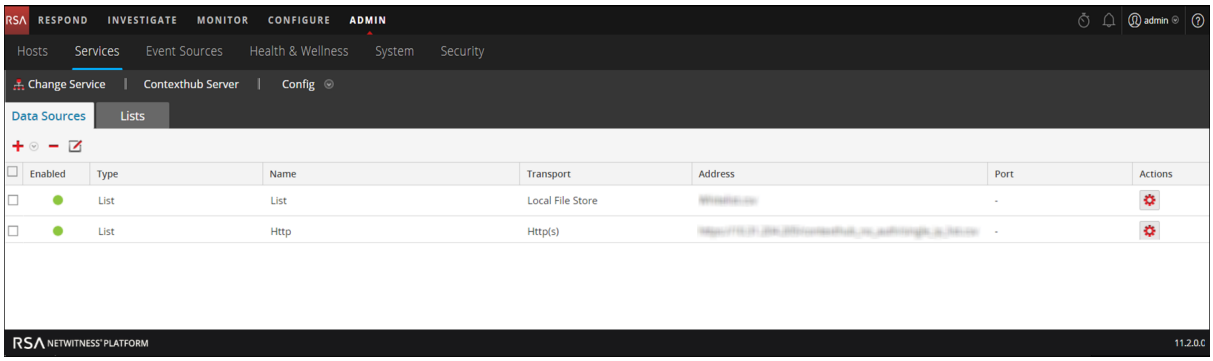
- Füllen Sie die folgenden Felder für den Verbindungstyp HTTP(S) aus:
  - **Name:** Geben Sie einen Namen für die Datenquelle an.
  - **URL**: Geben Sie neben dem Pfad der CSV-Datei auf dem HTTP(S)-Speicherort auch den Hostnamen oder die IP-Adresse der Remote-Maschine an, auf der die Liste gespeichert ist. Die URL ist in folgendem Format anzugeben: `https://<Hostname or IP-address of the HTTP(S)server>:<Port on which the HTTP(S) server is hosted>/<Absolute path of CSV file>`. Beispiel `https://10.1.1.1:443/contexthub_lists/multi_user_list.csv`
  - (Optional) **Beschreibung**: Fügen Sie eine Beschreibung für die ausgewählte Datei hinzu.
  - (Optional) **Benutzername:** Geben Sie den Benutzernamen für die Verbindung zum HTTP(S)-Server an, der grundlegende Authentifizierung erfordert.
  - (Optional) **Passwort:** Geben Sie das Passwort für die Verbindung zum HTTP(S)-Server an, der grundlegende Authentifizierung erfordert.
  - **Mit Spaltenüberschriften**: Wählen Sie diese Option, wenn Sie eine CSV-Datei mit Kopfzeilen importieren möchten. Wenn diese Option ausgewählt ist und Sie die CSV-Datei ohne Kopfzeilen importieren, so wird die erste Zeile, die bearbeitet werden kann, als Header betrachtet.
  - **SSL:** Wenn Sie eine URL mit HTTPS in dieses Feld eingeben, wird dieses automatisch ausgewählt. Wenn Sie eine URL mit HTTP eingeben, ist dieses Kontrollkästchen nicht

aktiviert.

- **Allen Zertifikaten vertrauen**: Markieren Sie dieses Kontrollkästchen, um die Datenquelle ohne Validierung des Zertifikats hinzuzufügen. Wenn Sie diese Option deaktivieren, müssen Sie ein gültiges HTTP(S)-Serverzertifikat im CER- oder CRT-Format hochladen, um erfolgreich eine Verbindung herstellen zu können.

5. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen Context Hub und Datenquelle zu testen.
6. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

   Die Liste wird als Datenquelle für den konfigurierten Context Hub hinzugefügt und auf der Registerkarte **Datenquellen** angezeigt.



Nächste Schritte:

- Fügen Sie Werte hinzu, bearbeiten Sie sie oder entfernen Sie sie aus einer bestimmten Liste.
- Konfigurieren Sie die Einstellungen für die Datenquelle, um die Datenquellenfelder zu bestimmen, die im Bereich „Kontext“ angezeigt werden sollen. Anweisungen finden Sie unter Konfigurieren der Einstellungen von Datenquellen für den Context Hub .
- Importieren und exportieren Sie Listen. Weitere Informationen finden Sie unter Importieren oder Exportieren von Listen für Context Hub.
- Zeigen Sie kontextbezogene Daten im Bereich „Kontextübersicht“ der Ansicht „Reagieren“ oder der Ansicht „Untersuchen“ an. Weitere Informationen finden Sie im *RSA NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu RSA NetWitness Investigation und Malware Analysis*.

Konfigurieren von Archer als Datenquelle

Sie können Archer als Datenquelle für Context Hub konfigurieren und mithilfe des Context Hub-Servers kontextbezogene Informationen aus Archer abrufen. Verwenden Sie die Verfahren in diesem Thema, um Archer als Datenquelle für den Context-Hub-Service hinzuzufügen, und konfigurieren Sie die Einstellungen (falls erforderlich) für Archer.

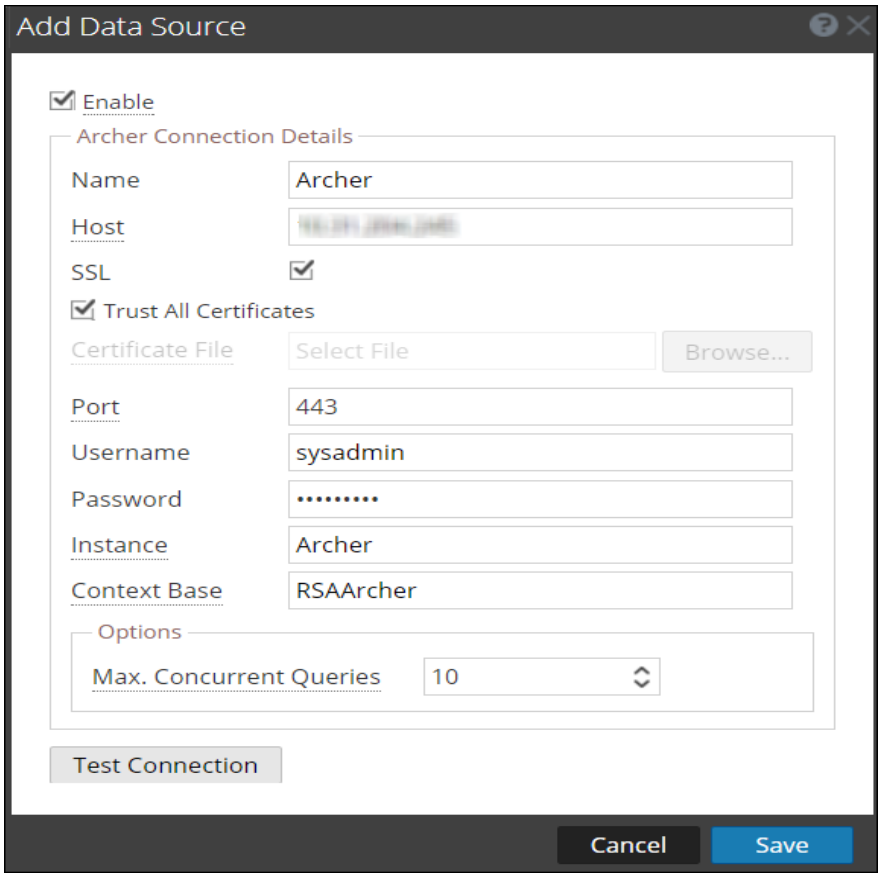
Voraussetzungen

Bevor Sie eine Archer-Datenquelle konfigurieren, stellen Sie Folgendes sicher:

- Der Context-Hub-Service ist in der Ansicht **ADMIN** > **Services** von NetWitness Platform verfügbar.
- Archer wird mit der Anwendung „Licensed Devices“ installiert.

So fügen Sie Archer als Datenquelle für Context Hub hinzu:

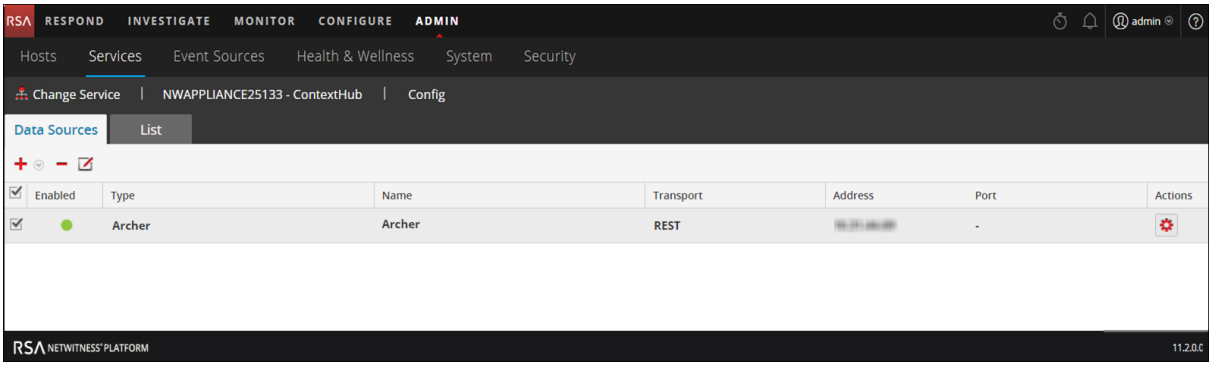
1. Gehen Sie zu **ADMIN** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie den Context-Hub-Service aus und klicken Sie auf > **Ansicht** > **Konfigurieren**.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Klicken Sie auf der Registerkarte **Datenquellen** auf > **Archer**.
   Das Dialogfeld **Datenquelle hinzufügen** wird angezeigt.



4. Stellen Sie folgende Informationen bereit:

- Das Kontrollkästchen **Aktivieren** ist standardmäßig ausgewählt. Wenn diese Option nicht aktiviert wird, ist die Schaltfläche zum Speichern deaktiviert. Sie können keine Datenquelle hinzufügen und keine kontextbezogenen Informationen anzeigen.
- Geben Sie Werte für die folgenden Felder ein:
  - **Name**: Geben Sie einen Namen für die Archer-Datenquelle ein.
  - **Host**: Geben Sie den Hostnamen oder die IP-Adresse ein, unter dem bzw. der der Archer-Server installiert ist.
  - **SSL**: Diese standardmäßig ausgewählte Option aktiviert die SSL-Kommunikation mit Archer.
  - **Allen Zertifikaten vertrauen**: Markieren Sie dieses Kontrollkästchen, um die Datenquelle ohne Validierung des Zertifikats hinzuzufügen. Wenn Sie diese Option deaktivieren, müssen Sie ein gültiges Endpunktserverzertifikat hochladen, um erfolgreich eine Verbindung herstellen zu können.
  - **Port:** Der Standardport ist 443.
  - **Benutzername**: Geben Sie den Benutzernamen für den Archer-Server ein.
  - **Passwort**: Geben Sie das Passwort für den Archer-Server ein.
  - **Instanz**: Geben Sie den Namen der Instanz ein, aus der Sie Daten extrahieren möchten. Eine RSA Archer-Instanz ist eine einzige Einrichtung, die einzigartige Inhalte in einer Datenbank, die Verbindung mit der Datenbank, die Schnittstelle und die Anmeldung enthält. Sie können individuelle Instanzen für jeden Bürostandort oder jede Region oder für Entwicklungs-, Test- und Produktionsumgebungen einrichten. In der Instanzendatenbank werden die RSA Archer-Inhalte für eine bestimmte Instanz gespeichert.
  - **Kontextbasis**: Geben Sie das virtuelle Verzeichnis ein, in dem die Dateien gespeichert werden. Zum Beispiel: „rsaarcher“ unter der RSA Archer-Internetadresse https://archer.company.com/**rsaarcher**/default.aspx. Wenn die Dateien unter der IIS-Standardinternetadresse https://archer.company.com/default.aspx gespeichert werden, muss dieses Feld leer bleiben.
  - **Max. gleichzeitige Anfragen:** Sie können die vom Context-Hub-Service definierte maximale Anzahl der gleichzeitigen Abfragen konfigurieren, die an den konfigurierten Datenquellen ausgeführt werden können. Der Standardwert ist 10.
5. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen Context Hub und Datenquelle zu testen.

6. Klicken Sie auf **Speichern**.
   Archer wird als Datenquelle für Context Hub hinzugefügt und auf der Registerkarte **Datenquellen** angezeigt.



Nach dem Hinzufügen der Datenquelle können Sie die Einstellungen für die Datenquelle konfigurieren. Anweisungen finden Sie unter Konfigurieren der Einstellungen von Datenquellen für den Context Hub . Sie können auch die kontextbezogenen Daten im Bereich „Kontextübersicht“ der Ansicht „Respond“ oder der Ansicht „Investigate“ anzeigen. Anweisungen hierzu finden Sie im *NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu Investigation und Malware Analysis*.

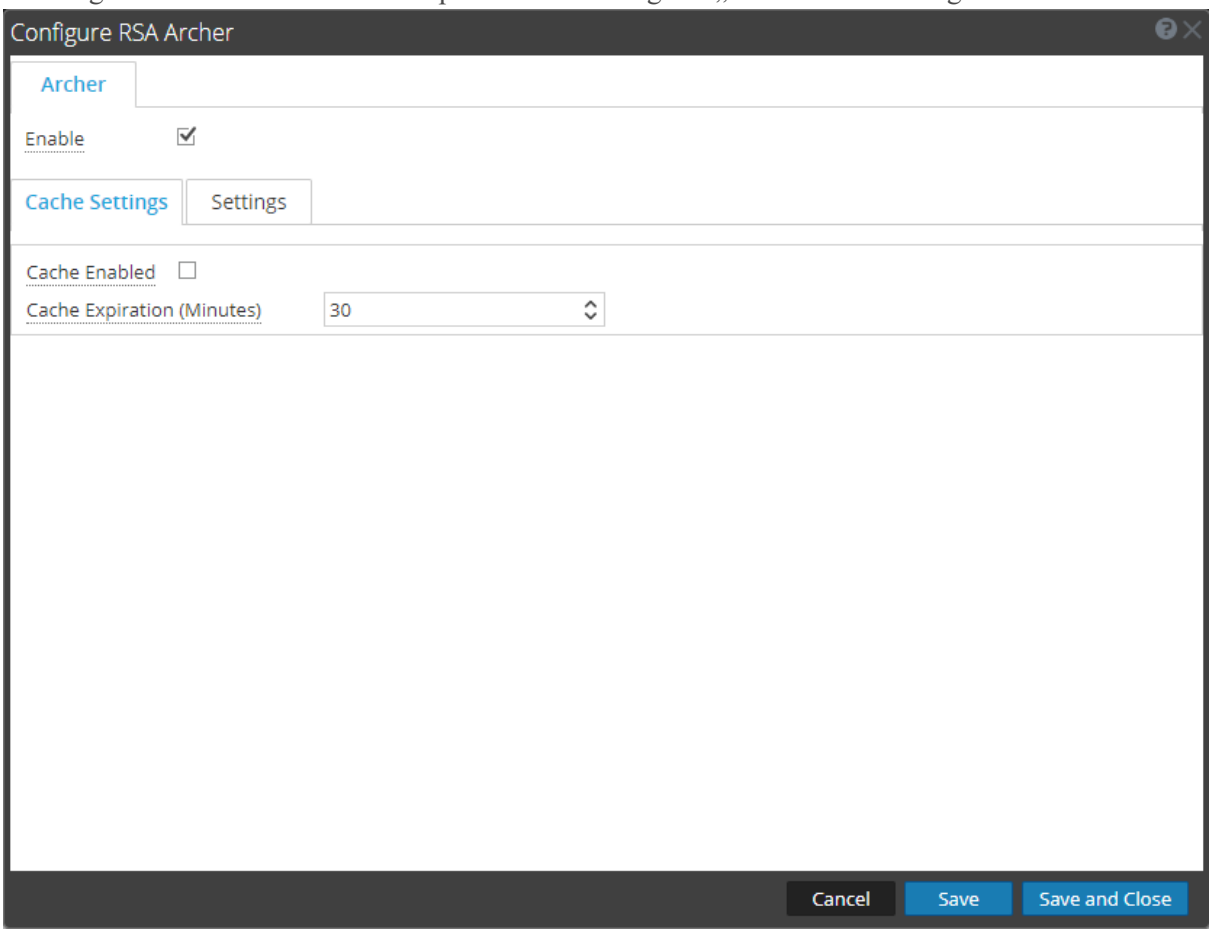
Konfigurieren von Archer-Datenquellen

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“.

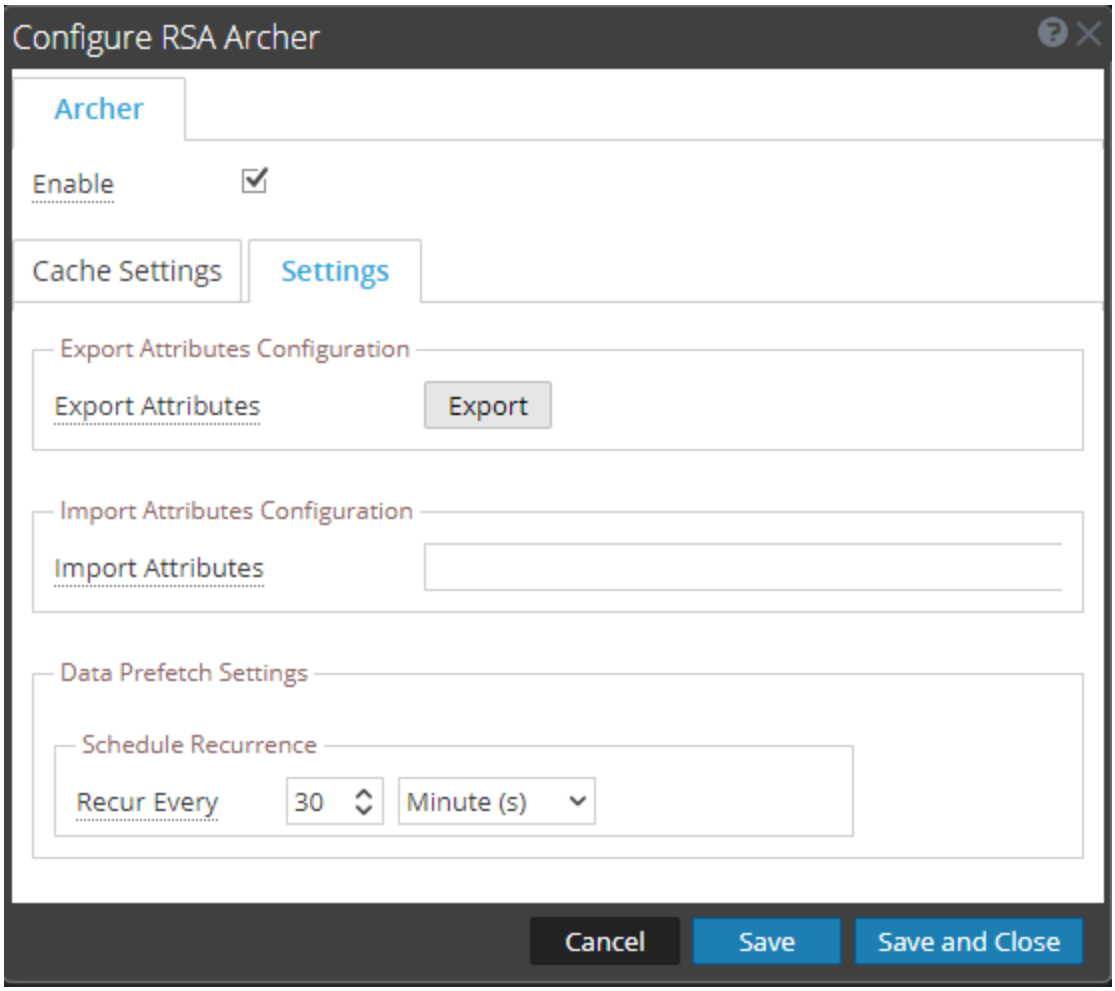
Der folgende Screenshot ist ein Beispiel für das Dialogfeld „RSA Archer konfigurieren“:



4. Auf der Registerkarte **Einstellungen**. 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.

5. Klicken Sie auf **Cacheeinstellungen**. Konfigurieren Sie die folgenden Felder



Feld	Beschreibung
Attributkonfiguration exportieren	Klicken Sie unter **Einstellungen**, **Attributkonfiguration exportieren** auf **Exportieren**, um die Archer-Attributkonfiguration zu exportieren. Dies sind die Attribute, die beim Anzeigen von Archer-Details für eine IP, einen Host oder einen Mac in der Kontextabfrage sichtbar sind. Eine JSON-Konfigurationsdatei wird heruntergeladen und die Reihenfolge der Attribute, die mit dem Bereich „Kontext“ synchron sind, wird in der JSON-Datei beibehalten.
Attributkonfiguration importieren	Wenn Sie die Konfigurationseinstellungen aktualisieren oder bearbeiten möchten, klicken Sie unter **Einstellungen**, **Attributkonfiguration importieren** auf **Durchsuchen**. Wählen Sie die JSON-Datei mit den Konfigurationsattributen aus. Die Attribute werden im Bereich „Kontextabfrage“ angezeigt, wenn ein Nutzer den Kontext in der Reihenfolge ansieht, in der er importiert wurde. **Hinweis**: Sie können die vorherigen Attribute sichern, bevor Sie Änderungen an bestehenden Attributen importieren.

Feld	Beschreibung
Einstellungen Daten-Pre-Fetch	Unter **Einstellungen**, **Einstellungen Daten-Pre-Fetch** können die Daten abgerufen werden. Konfigurieren Sie **Geplante Wiederholung**, um Daten schneller zur Verfügung zu stellen, wenn Sie mit der Maus auf die gewünschte Entity in Respond zeigen.
Geplante Wiederholung	Geben Sie im Feld **Wiederholungsintervall** einen Wert ein oder verwenden Sie das Drop-Down-Menü, um die Wiederholung für Prefetch zu konfigurieren. Die Standard-Zeitdauer kann aus der Drop-Down-Liste ausgewählt werden, um die Dauer der Wiederholung zu konfigurieren. Verfügbare Werte sind Minuten, Stunden, Tage oder Wochen.

6. 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.

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.

Konfigurieren von Active Directory als Datenquelle

Sie können Active Directory (AD) mittels LDAP als Datenquelle für Context Hub konfigurieren und mithilfe des Context Hub-Servers kontextbezogene Informationen aus AD abrufen. Verwenden Sie die Verfahren in diesem Thema, um AD als Datenquelle für den Context-Hub-Service hinzuzufügen, und konfigurieren Sie die Einstellungen (falls erforderlich) für AD.

Voraussetzungen

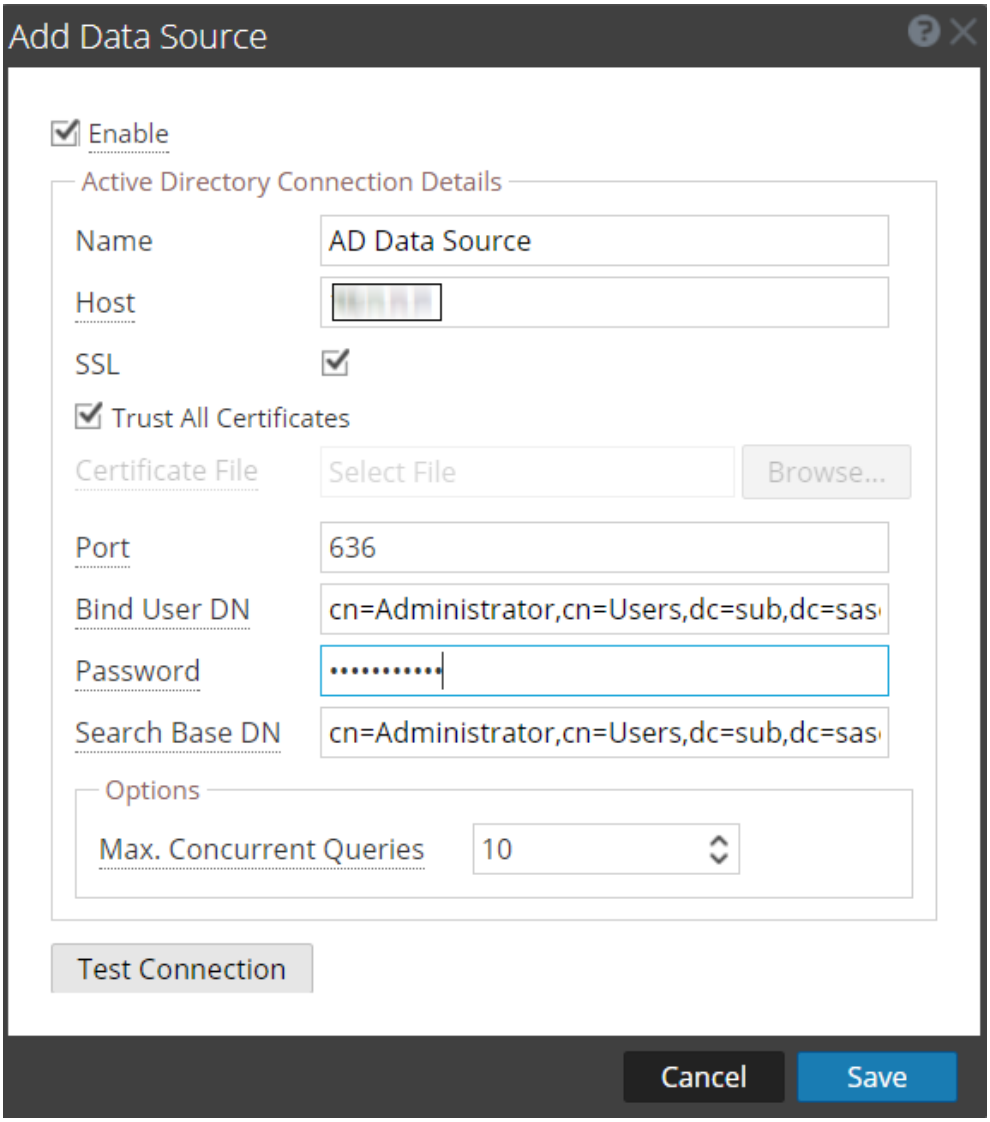
Bevor Sie eine Active Directory-Datenquelle konfigurieren, stellen Sie Folgendes sicher:

- Der Context-Hub-Service ist in der Ansicht **ADMIN** > **Services** von NetWitness Platform verfügbar.
- Active Directory ist verfügbar und wird unter Windows ausgeführt. Es werden die Versionen 2003, 2008 und 2012 unterstützt.

So fügen Sie AD als Datenquelle für Context Hub hinzu:

1. Navigieren Sie zu **ADMIN** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie den Context-Hub-Service aus und klicken Sie auf  > **Ansicht** > **Konfiguration**.
   Die Ansicht „Service-Konfiguration“ von Context Hub wird angezeigt.

3. Klicken Sie auf der Registerkarte **Datenquellen** auf + > **AD**.
   Das Dialogfeld **Datenquelle hinzufügen** wird angezeigt.



Sie müssen das Active Directory-Schema konfigurieren, um die folgenden Attribute zur Anzeige der Daten auf der Reagieren-Seite zu replizieren:

- Mitarbeiter-ID
- Abteilung
- Unternehmen
- Funktion
- Postleitzahl

Alle anderen Attribute werden automatisch repliziert.

6. Geben Sie die folgenden Datenbankverbindungsdetails an:

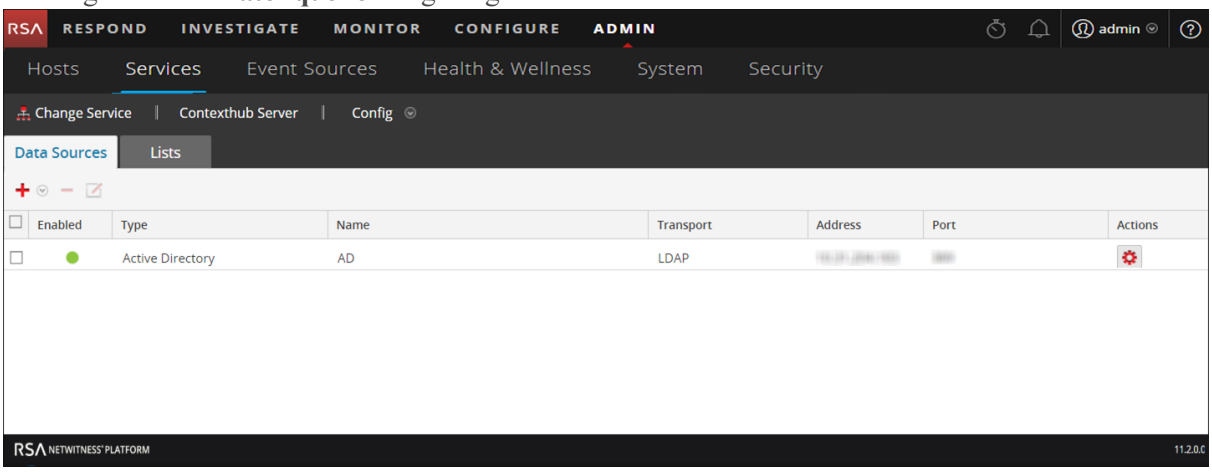
- Das Kontrollkästchen **Aktivieren** ist standardmäßig ausgewählt. Wenn diese Option nicht aktiviert wird, ist die Schaltfläche zum Speichern deaktiviert. Sie können keine Datenquelle hinzufügen und keine kontextbezogenen Informationen anzeigen.
- Geben Sie Werte für die folgenden Felder ein:
  - **Name:** Geben Sie einen Namen für die AD-Datenquelle ein.
  - **Host:** Geben Sie die IP-Adresse oder den Hostnamen von AD ein.
  - **SSL:** Standardmäßig wird hier Portnummer 636 eingetragen, was eine Verbindung mit der Datenquelle über Secure Sockets Layer (SSL) herstellt.
  - **Allen Zertifikaten vertrauen**: Markieren Sie dieses Kontrollkästchen, um die Datenquelle ohne Validierung des Zertifikats hinzuzufügen. Wenn Sie diese Option deaktivieren, müssen Sie ein gültiges Active Directory-Serverzertifikat im CER- oder CRT-Format hochladen, um erfolgreich eine Verbindung herstellen zu können. Wenn Sie mehrere Active Directory-Datenquellen mit SSL hinzufügen, sollten Sie entweder alle Datenquellen mit einem gültigen Zertifikat versehen oder allen Zertifikaten vertrauen.
  - **Port:** Der Standardport ist 636 mit SSL und 389 ohne SSL.
    Wenn Daten aus mehreren Domains abgerufen werden sollen, können Sie eine einzige Datenquelle mit dem globalen Katalogport konfigurieren (3269 mit SSL oder 3268 ohne SSL).

    Alternativ können Sie bei mehreren Domains eine einzige Datenquelle für jede Domain mit dem Standardport (389 mit SSL oder 636 ohne SSL) konfigurieren.

    Multi-Forest ist eine Sammlung mehrerer Domains. Wenn Daten aus Multi-Forest abgerufen werden sollen, müssen Sie jeden Forest mit dem globalen Katalogport konfigurieren (3269 mit SSL oder 3268 ohne SSL).
  - **Passwort:** Geben Sie ein Passwort für den Benutzer-DN ein, der zum Binden an AD verwendet wird.
  - **Bind-DN Benutzer:** Der Distinguished Name des Benutzers, der sich dem Suchverzeichnis gegenüber authentifiziert. Beispie: cn=Administrator,cn=Users,dc=sub,dc=saserver,dc=local.
  - **DN Suchbasis:** Der Basis-Distinguished Name oder Basis-DN, identifiziert den Eintrag im Verzeichnis, aus dem Suchvorgänge initiiert werden. Der Basis-DN wird häufig als Suchbasis bezeichnet. Beispiel: dc=sub,dc=saserver,dc=local.

7. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen Context Hub und Datenquelle zu testen.
8. Klicken Sie auf **Speichern**.
   AD wird als Datenquelle für Context Hub hinzugefügt. Die hinzugefügte AD-Datenquelle wird auf

der Registerkarte **Datenquellen** angezeigt.



Nach dem Hinzufügen der Datenquelle können Sie die Einstellungen für die Datenquelle konfigurieren. Anweisungen finden Sie unter Konfigurieren der Einstellungen von Datenquellen für den Context Hub .

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*.

Konfigurieren von NetWitness Endpoint als Datenquelle

Sie können NetWitness Endpoint als Datenquelle für Context Hub konfigurieren und mithilfe des Context Hub-Servers kontextbezogene Informationen aus NetWitness Endpoint abrufen. Verwenden Sie die Verfahren in diesem Thema, um NetWitness Endpoint als Datenquelle für den Context-Hub-Service hinzuzufügen, und konfigurieren Sie die Einstellungen (falls erforderlich) für NetWitness Endpoint.

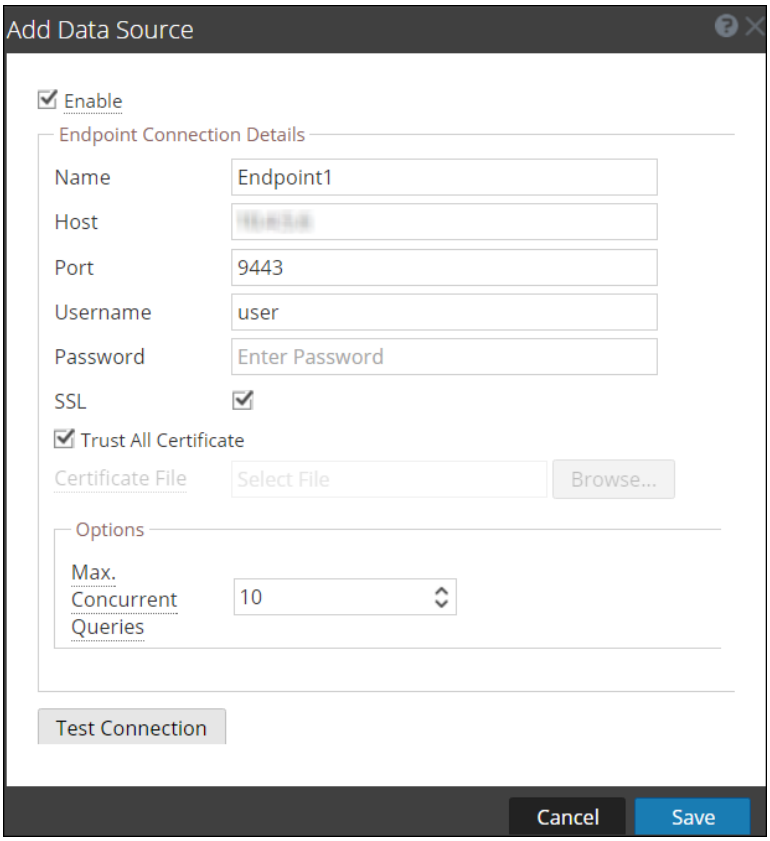
Voraussetzungen

Bevor Sie eine NetWitness Endpoint-Datenquelle konfigurieren, stellen Sie Folgendes sicher:

- Der Context-Hub-Service ist in der Ansicht **Admin** > **Services** von NetWitness Platform verfügbar.
- NetWitness Endpoint (v4.1.1 zu 4.3.0.5) ist installiert und konfiguriert.
  Weitere Informationen zum Installieren und Konfigurieren sowie detaillierte Informationen zu NetWitness Endpoint finden Sie in den NetWitness Endpoint-Dokumenten auf RSA Link.

So fügen Sie NetWitness Endpoint als Datenquelle für Context Hub hinzu:

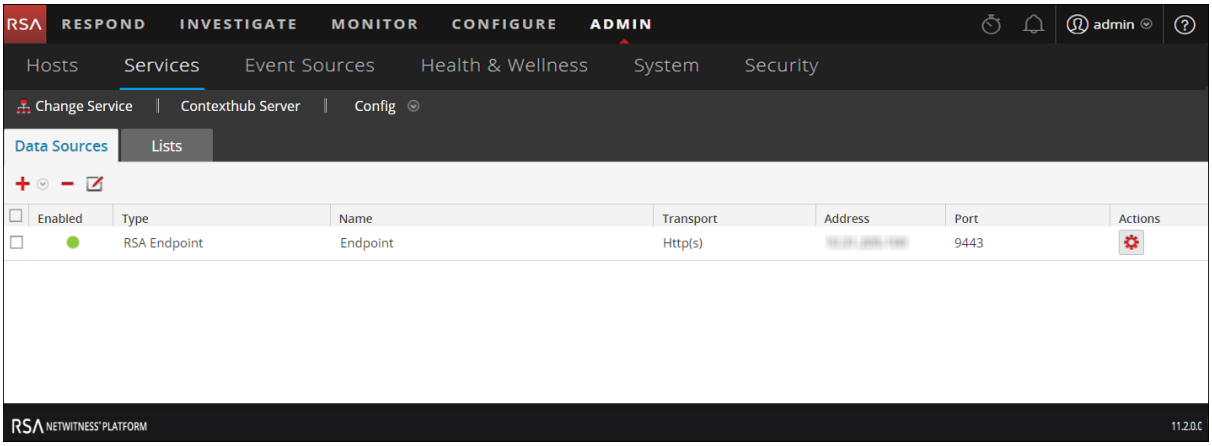
1. Navigieren Sie zu **Admin** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie den Context-Hub-Service aus und klicken Sie auf > **Ansicht** > **Konfiguration**.
   Die Ansicht „Service-Konfiguration“ wird angezeigt.
3. Klicken Sie auf der Registerkarte **Datenquellen** auf > **RSA Endpoint**.
   Das Dialogfeld **Datenquelle hinzufügen** wird angezeigt.



4. Stellen Sie folgende Informationen bereit:

- Das Kontrollkästchen **Aktivieren** ist standardmäßig ausgewählt. Wenn diese Option nicht aktiviert wird, ist die Schaltfläche zum Speichern deaktiviert. Sie können keine Datenquelle hinzufügen und keine kontextbezogenen Informationen anzeigen.
- Geben Sie Werte für die folgenden Felder ein:
  - **Name**: Geben Sie einen Namen für die NetWitness Endpoint-Datenquelle ein.
  - **Host**: Geben Sie den Hostnamen oder die IP-Adresse ein, unter dem bzw. der der NetWitness Endpoint-API-Server installiert ist.
  - **Port:** Der Standardport ist 9443.
  - **SSL**: Wählen Sie SSL aus, wenn Sie möchten, dass NetWitness Platform mit dem Host mithilfe von SSL kommuniziert. Dies ist standardmäßig aktiviert.
  - **Benutzername**: Geben Sie den Benutzernamen für den NetWitness Endpoint-API-Server ein.
  - **Passwort**: Geben Sie das Passwort für den NetWitness Endpoint-API-Server ein.
  - **Allen Zertifikaten vertrauen**: Markieren Sie dieses Kontrollkästchen, um die Datenquelle ohne Validierung des Zertifikats hinzuzufügen. Wenn Sie diese Option deaktivieren, müssen Sie ein gültiges erzeugtes oder von einer Zertifizierungsstelle ausgestelltes Zertifikat hochladen, um die Verbindung mit den unterstützten Formaten .cer oder .crt und Base64-[PEM] oder DER-Codierung zu authentifizieren.
  - **Max. gleichzeitige Anfragen:** Sie können die maximale Anzahl der gleichzeitigen Abfragen konfigurieren, die an den konfigurierten Datenquellen ausgeführt werden können. Der Standardwert ist 10.

5. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen Context Hub und NetWitness Endpoint zu testen.
6. Klicken Sie auf **Speichern**.
   NetWitness Endpoint wird als Datenquelle für Context Hub hinzugefügt und auf der Registerkarte **Datenquellen** angezeigt.



Nächste Schritte

Nach dem Hinzufügen der Datenquelle können Sie die Einstellungen konfigurieren. Weitere Informationen erhalten Sie unter Konfigurieren der Einstellungen von Datenquellen für den Context Hub .

Sie können auch die kontextbezogenen Daten im Bereich „Kontextübersicht“ der Ansicht „Respond“ oder der Ansicht „Investigate“ anzeigen. Weitere Informationen finden Sie im *RSA NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu RSA NetWitness Investigation und Malware Analysis*.

Konfigurieren von Respond als Datenquelle

Sie können Respond als Datenquelle für Context Hub konfigurieren und mithilfe des Context Hub-Servers kontextbezogene Informationen aus dem Respond-Service abrufen. Wenn der Respond-Service bereits konfiguriert ist, werden die Konfigurationsdetails beim Hinzufügen von Respond als Datenquelle eingetragen. Verwenden Sie die Verfahren in diesem Thema, um Respond als Datenquelle für den Context-Hub-Service hinzuzufügen, und konfigurieren Sie die Einstellungen.

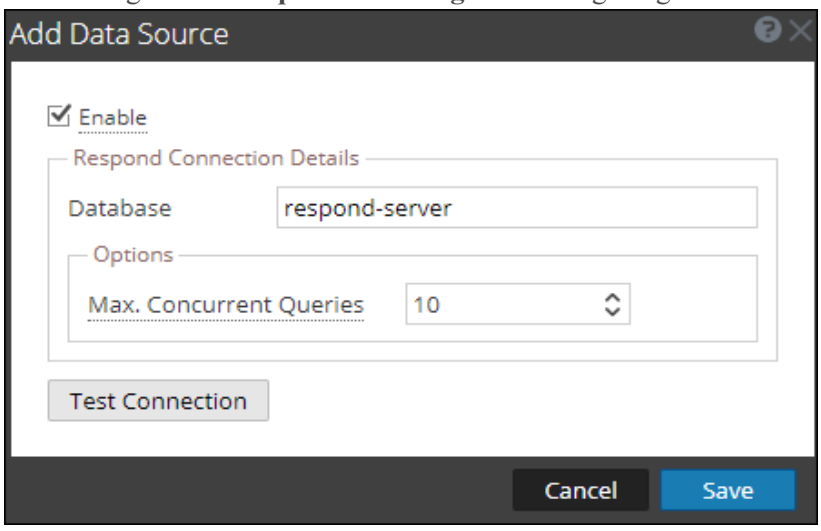
Voraussetzungen

Bevor Sie eine Respond-Datenquelle konfigurieren, stellen Sie Folgendes sicher:

- Der Context-Hub-Service ist in der Ansicht **ADMIN** > **Services** von NetWitness Platform verfügbar.
- Der Respond-Service ist verfügbar.

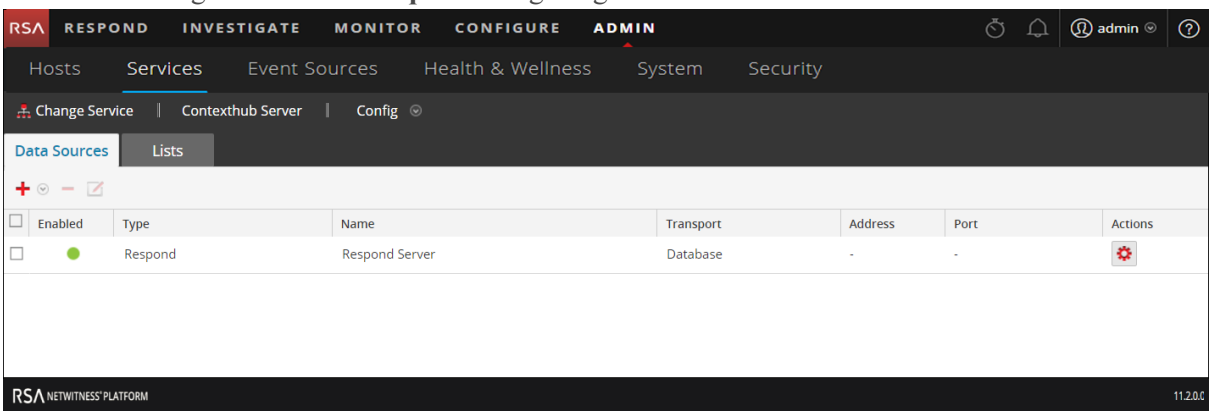
So fügen Sie Respond als Datenquelle für Context Hub hinzu:

1. Navigieren Sie zu **Admin** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie den Context-Hub-Service aus und klicken Sie auf > **Ansicht** > **Konfiguration**.
   Die Servicekonfigurationsansicht von Context Hub wird angezeigt.
3. Klicken Sie auf der Registerkarte **Datenquellen** auf > **Respond**.
   Das Dialogfeld **Datenquelle hinzufügen** wird angezeigt.



   Die erforderlichen Felder zum Konfigurieren der Respond-Datenquelle werden automatisch aktualisiert.
4. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen Context Hub und Datenquelle zu testen.
5. Klicken Sie auf **Speichern**.
   Respond wird als Datenquelle für Context Hub hinzugefügt. Die hinzugefügte Respond-Datenquelle

wird auf der Registerkarte **Datenquellen** angezeigt.



Nach dem Hinzufügen der Datenquelle können Sie die Einstellungen konfigurieren. Weitere Informationen erhalten Sie unter Konfigurieren der Einstellungen von Datenquellen für den Context Hub .

Nächste Schritte

Nach Abschluss der Konfiguration können Sie die kontextbezogenen Daten im Bereich „Kontextübersicht“ der Ansicht „Reagieren“ oder der Ansicht „Untersuchen“ anzeigen. Weitere Informationen finden Sie im *RSA NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu RSA NetWitness Investigation und Malware Analysis*.

Konfigurieren von Live Connect als Datenquelle für Context Hub

In diesem Thema wird das Verfahren zum Konfigurieren von Live Connect-Datenquellen für Context Hub beschrieben.

Bei RSA Live Connect handelt es sich um einen cloudbasierten Bedrohungsinformationsservice. Dieser Service erfasst, analysiert und bewertet Intelligence-Daten zu Bedrohungen wie beispielsweise IP-Adressen, Domains und Dateien, die aus verschiedenen Quellen erfasst werden, unter anderem aus der Kunden-Community von RSA NetWitness® Platform und RSA NetWitness® Endpoint.

RSA Live Connect ist ein Teil der Live Services und kann aus dem Bereich „System > Live Services-Konfiguration“ heraus konfiguriert werden. Weitere Informationen zur Konfiguration von Live Services finden Sie im Thema **Konfigurieren der Einstellungen von Live Services** im *Systemkonfigurationsleitfaden*.

Bedrohungseinblicke durch RSA Live Connect ermöglichen Analysten das Abrufen von Daten zu Bedrohungen (z. B. IP-bezogene Informationen) vom Live Connect-Service, um sie bei Ermittlungen zu nutzen. **Bedrohungseinblicke** ist im Abschnitt **Weitere Live-Services** standardmäßig aktiviert. Wenn der Context-Hub-Service konfiguriert wurde, wird Live Connect automatisch als Datenquelle für Context Hub hinzugefügt.

Voraussetzungen

Stellen Sie Folgendes sicher:

- Context Hub ist aktiviert und der Service ist in der Ansicht „Admin > Services“ von NetWitness Platform verfügbar.
- Das RSA Live-Konto ist verfügbar.

Hinweis: Hinweise zum Erstellen eines Live-Kontos finden Sie im Thema **Schritt 1. Erstellen eines Live-Kontos** im *Handbuch Live-Services-Management*.

Bedrohungseinblicke ist im Abschnitt **Weitere Live-Services** standardmäßig aktiviert. Stellen Sie vor dem Einrichten von Live Connect-Datenquellen sicher, dass Sie sich beim Live-Konto mit Ihren Anmeldedaten für das Live-Konto angemeldet haben und dass Context Hub aktiviert ist. Live Connect wird automatisch als Datenquelle für Context Hub hinzugefügt.

Weitere Informationen zur Konfiguration von Live-Konto und Live-Services finden Sie im Thema **Konfigurieren der Einstellungen von Live-Services** im *Systemkonfigurationsleitfaden*.

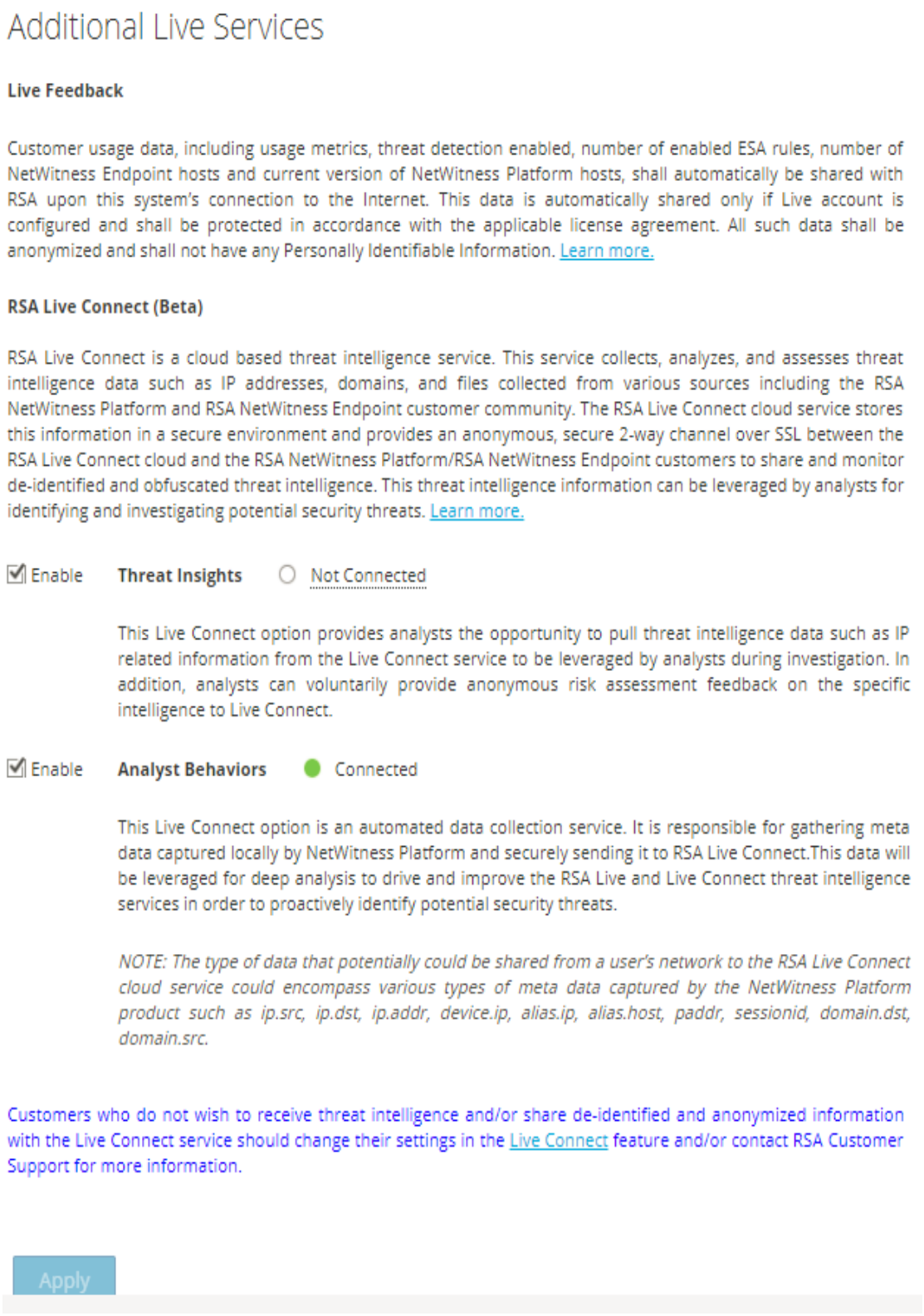
Informationen zur Konfiguration des Context-Hub-Service finden Sie im Thema **Schritt 1. Hinzufügen des Context-Hub-Services** im *Context Hub-Konfigurationsleitfaden*.

Aktivieren und Deaktivieren von Live Connect als Datenquelle

So aktivieren bzw. deaktivieren Sie Live Connect als Datenquelle für Context Hub:

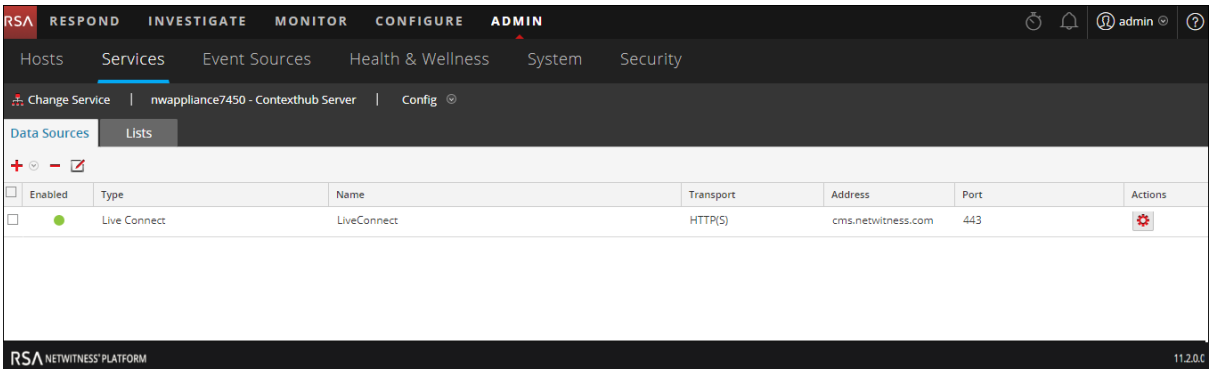
1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im linken Navigationsbereich **Live-Services** aus.

3. Aktivieren Sie im Abschnitt **Weitere Live-Services** die Option **Bedrohungseinblicke**.



4. Klicken Sie auf **Anwenden**.
   Die Live Connect-Datenquelle wurde für den Context-Hub-Service aktiviert.

5. Um dies zu überprüfen, navigieren Sie zur Registerkarte **Datenquellen** und zeigen die verfügbaren Quellen an.
   Die Live Connect-Quelle muss der Liste der verfügbaren Quellen hinzugefügt werden und das Feld **Enabled** muss einen grünen Kreis ( ) aufweisen.



6. Um eine Live Connect-Datenquelle zu deaktivieren, deaktivieren Sie **Bedrohungseinblicke** im Bereich „Weitere Live-Services“ und klicken auf **Anwenden**.

   Die Live Connect-Datenquelle wurde für den Context-Hub-Service deaktiviert.

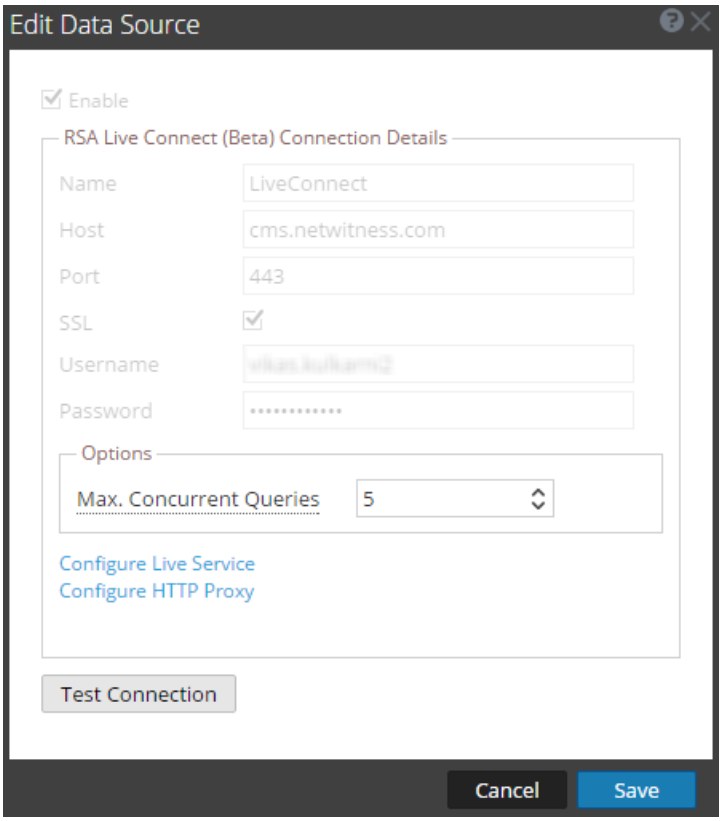
> **Hinweis:** Wenn „Bedrohungseinblicke“ deaktiviert ist, zeigt der Bereich „Kontextabfrage“ für Live Connect (in den Ansichten „Investigation > Navigieren“ und „Ereignis“) eine Nachricht an, die Live Connect-Datenquelle zu konfigurieren. Um kontextbezogene Daten für Live Connect anzuzeigen, müssen Sie Bedrohungseinblicke aktivieren.

Bearbeiten der Einstellungen für eine Live Connect-Datenquelle

So bearbeiten Sie eine Live Connect-Datenquelle für Context Hub:

1. Wählen Sie im Hauptmenü die Optionen **Admin > Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie im Bereich **Services** den Context-Hub-Service und klicken Sie auf > **Ansicht > Konfiguration**.
   Die Ansicht „Services-Konfiguration“ wird angezeigt.
3. Wählen Sie auf der Registerkarte **Datenquellen** die Live Connect-Datenquelle aus und klicken Sie auf .

   Das Dialogfeld **Datenquelle bearbeiten** wird angezeigt.



4. Bearbeiten Sie die erforderlichen Felder:

Feld	Beschreibung
Max. gleichzeitige Anfragen	Sie können die vom Context-Hub-Service definierte maximale Anzahl der gleichzeitigen Abfragen konfigurieren, die an den konfigurierten Datenquellen ausgeführt werden können. Der Standardwert ist 25.

5. Führen Sie folgende Schritte aus, um die Live-Verbindung und Proxy-Einstellungen zu bearbeiten:
   - Hinweise zum Bearbeiten der Live-Verbindungseinstellungen finden Sie im Thema **Bereich „Konfiguration der Live-Services“** im *Systemkonfigurationsleitfaden*.
   - Hinweise zum Bearbeiten der Proxy-Einstellungen finden Sie im Thema **Bereich „HTTP-Proxyeinstellungen“** Thema im *Systemkonfigurationsleitfaden*.
6. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen Context Hub und Datenquelle zu testen.
7. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Nächste Schritte

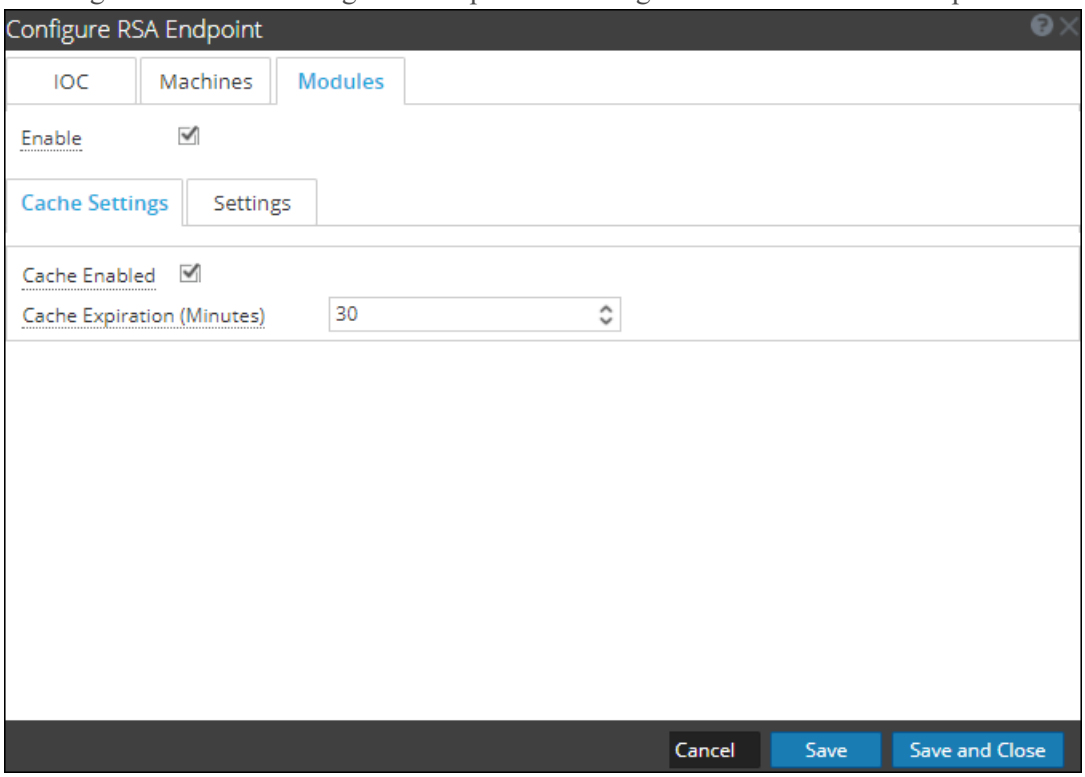
Nach Abschluss der Konfiguration können Sie die kontextbezogenen Daten im Bereich „Kontextübersicht“ der Ansicht „Reagieren“ oder der Ansicht „Untersuchen“ anzeigen. Weitere Informationen finden Sie im *RSA NetWitness Respond – Benutzerhandbuch* und dem *Leitfaden zu RSA NetWitness Investigation und Malware Analysis*.

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 Erstellen einer Liste hinzugefügt haben.
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 Cacheeinstellungen Cache aktiviert Cache-Ablauf (Minuten) [Min. sind 30 Minuten, Max. sind 7200 Minuten]
RSA Archer	Archer	Cacheeinstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen Attributkonfiguration exportieren Exportattribute Einstellungen Daten-Pre-Fetch Geplante Wiederholung
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]

Datenquelle (Verbindung)	Unterstützte Antwortgruppen	Feldeinstellungen
RSA Endpoint	IOC Rechner Module	Cacheeinstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen Einstellungen Kontextbereich Cacheeinstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen Einstellungen Kontextbereich Cacheeinstellungen Cache aktiviert Cache-Ablauf (Minuten) Einstellungen IIOC-Mindestwert Einstellungen Kontextbereich
Reagieren	-Warnmeldungen Incidents	Einstellungen Kontextbereich Daten-Pre-Fetch-Einstellungen Abfrage der letzten [Tage Cacheeinstellungen Cache aktiviert Cache-Ablauf (Minuten)
Live Connect	Domain Datei IP	Cacheeinstellungen 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 Platform 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

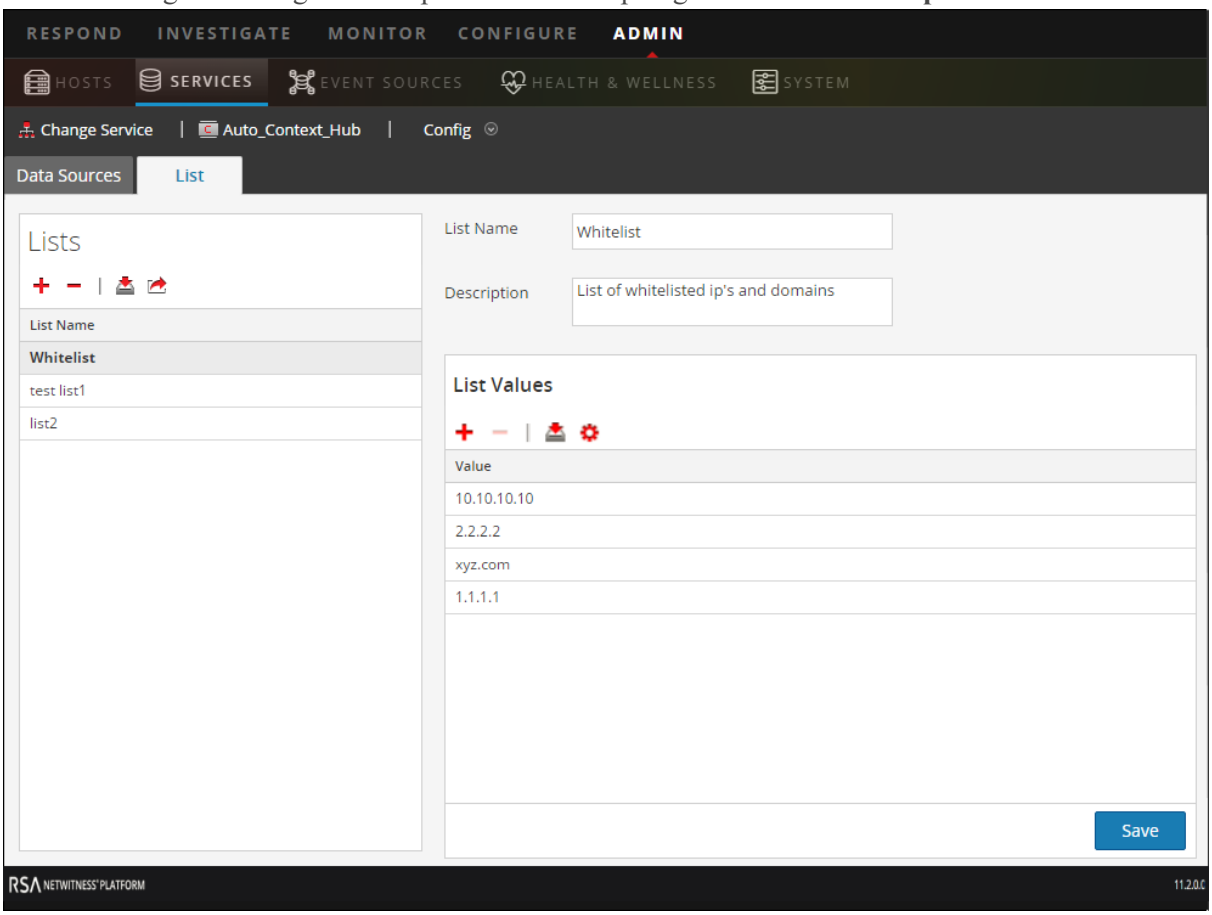
Hinweis: Sie müssen dieselben Änderungen an der entsprechenden CSV-Datei vornehmen, damit diese beim nächsten Mal berücksichtigt werden, wenn der Plan erneut durchgeführt wird. Anderenfalls werden beim Importieren von Werten in eine bestehende Liste mit einer oder mehreren Spalten die Daten aus der Quelldatei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

Importieren einer einspaltigen Liste

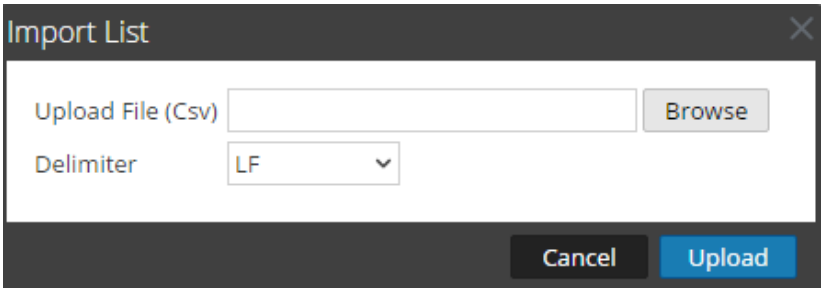
So importieren Sie eine Liste:

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. **<need an updated screenshot>**



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 direktes Importieren einer CSV-Datei keine neue Liste mit mehreren Spalten erstellen. Allerdings werden alle Feeds, die in Listen mit mehreren Spalten umgewandelt werden, auf der Registerkarte „Liste“ angezeigt. Informationen zum Importieren von Listen mit mehreren Spalten finden Sie unter Konfigurieren von Listen als Datenquelle.

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:

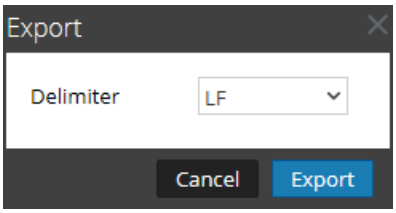
1. Navigieren Sie zu **ADMIN** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Klicken Sie auf  > **Ansicht** > **Konfiguration**.
   Die Ansicht „Services“ > „Konfiguration“ des Context-Hub-Services wird angezeigt.
3. Klicken Sie auf die Registerkarte **Listen**.
   Die Registerkarte „Listen“ 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 Platform 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.

Hinweis: Wenn ein benutzerdefinierter Feed in eine Context-Hub-Liste umgewandelt wird, müssen Sie mindestens einen Metaschlüssel mit einer oder mehreren Entitätszuordnungen für eine Spaltenüberschrift mit Metadaten zuordnen. Wenn Sie jedoch weitere Entitäten hinzufügen oder bearbeiten möchten, können Sie dazu auf ⚙ klicken.

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 Platform 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:

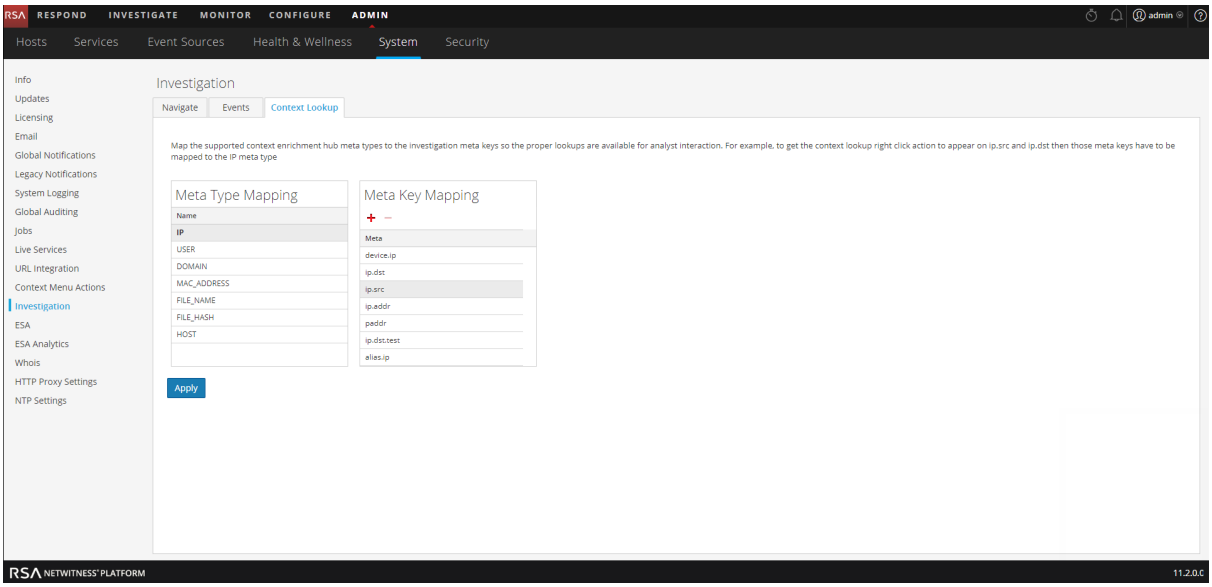
Name des Metadatentyps	Metaschlüssel
IP	device.ip, ip.src, ip.dst, ip.addr,ipv6.src, alias.ip, ipv6.addr, device.ipv6,forward.ip, forward.ipv6,ipv6.dst, ipv6.addr, stransaddr, transaddr
USER	user.src, user.dst, username, event user
DOMAIN	domain.src, domain.dst,fqdn, web.domain, domain, sdomain, ddomain
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

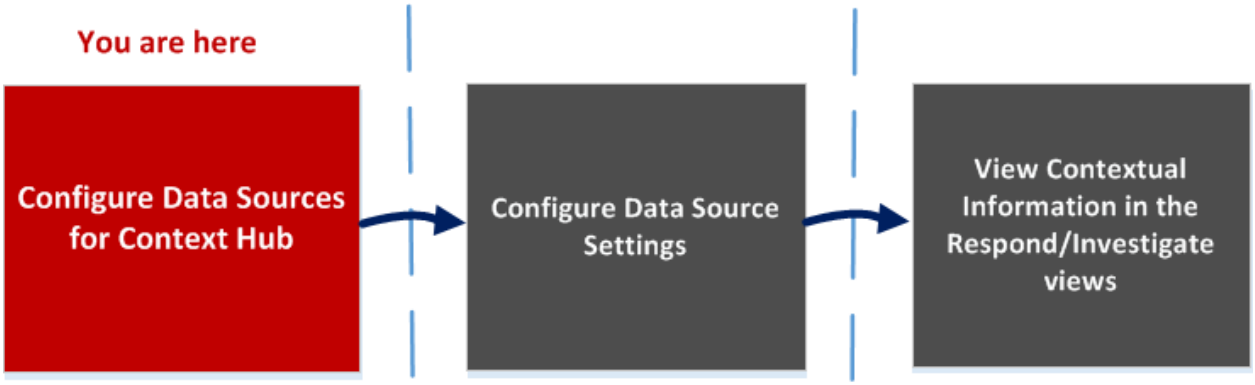
Nachdem Sie den Context-Hub-Service und die erforderliche Datenquelle konfiguriert haben, können Sie die Einstellungen für jede Datenquelle managen. Dies hilft bei der Optimierung und Anpassung der Abfrageergebnisse.

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 Listen als Datenquelle Konfigurieren von Archer als Datenquelle Konfigurieren von Active Directory als Datenquelle Konfigurieren von NetWitness Endpoint als Datenquelle Konfigurieren von Respond als Datenquelle Konfigurieren von Live Connect als Datenquelle für Context Hub

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

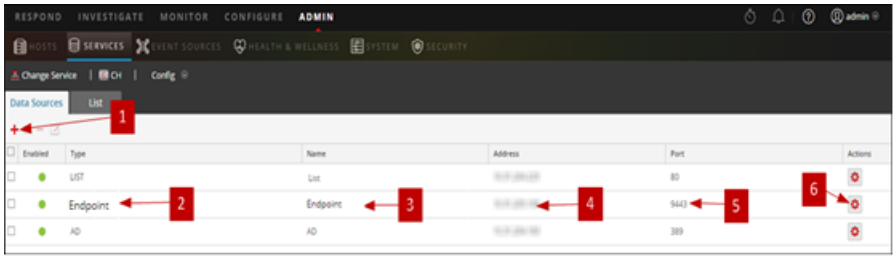
*Sie können diese Aufgabe hier abschließen (das ist die Registerkarte „Context Hub-Datenquellen“).

Verwandte Themen

- Konfigurieren von Listen als Datenquelle
- Konfigurieren von Archer als Datenquelle
- Konfigurieren von Active Directory als Datenquelle
- Konfigurieren von NetWitness Endpoint als Datenquelle
- Konfigurieren von Respond als Datenquelle
- Konfigurieren von Live Connect als Datenquelle für Context Hub

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 Listen als Datenquelle.
	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 Live Connect als Datenquelle 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 für den Context Hub.

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**.

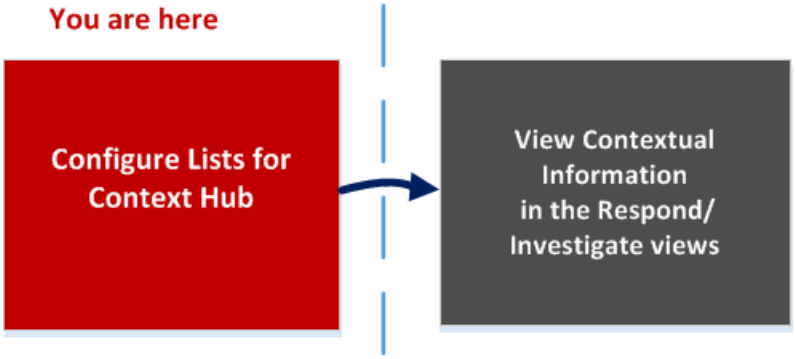
Auf der Registerkarte „Listen“ des Context-Hub-Services können Sie eine oder mehrere Listen erstellen und der Liste entsprechende Listenwerte hinzufügen. Diese Listen werden automatisch als Datenquellen für den Context-Hub-Service berücksichtigt.

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

Rolle	Ziel	Details anzeigen
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“
- „Troubleshooting für NetWitness Investigate“ im *NetWitness Investigate – Benutzerhandbuch*

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.

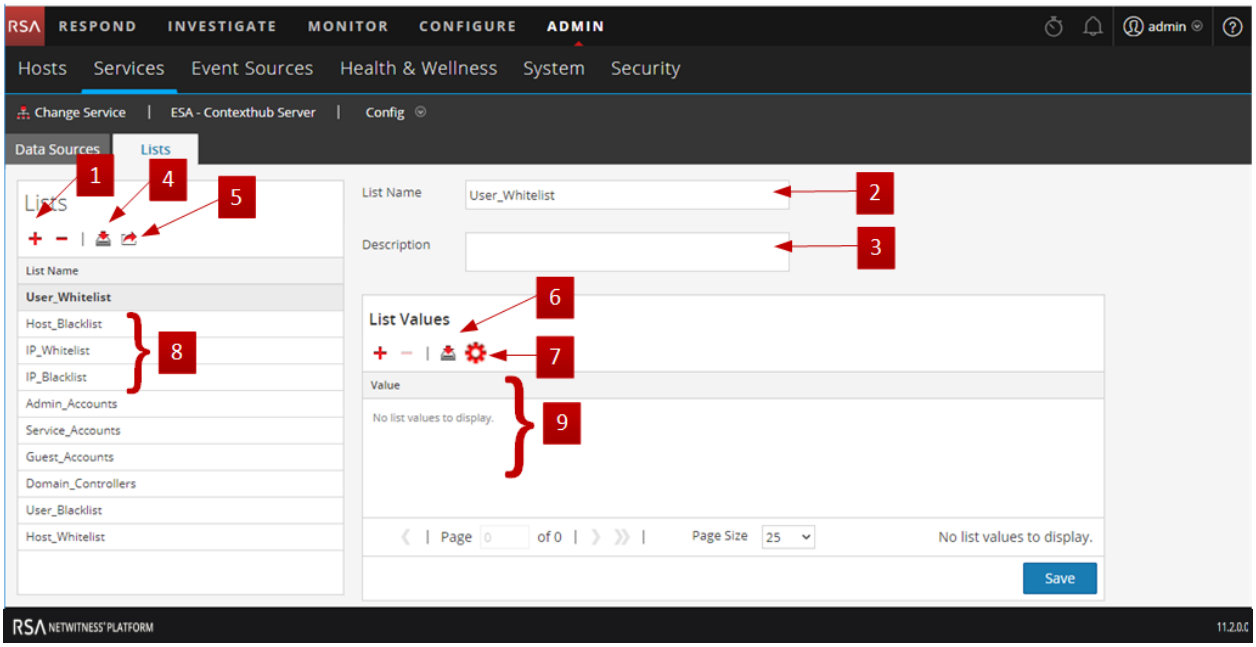
Standardmäßig sind 10 leere Einspaltenlisten in RSA NetWitness Platform11.1 verfügbar. Diese Listen sind leer und Sie müssen diesen Listen Informationen hinzufügen. Die standardmäßigen 10 Listennamen werden in den ESA-Regeln verwendet. Weitere Informationen zu den ESA-Regeln finden Sie im *Warnmeldungen mit ESA-Korrelationsregeln – Benutzerhandbuch*. Nutzern, die ein Upgrade von früheren Versionen durchführen, werden diese neuen Listen zusätzlich zu ihren zuvor erstellten Listen angezeigt. Die standardmäßig verfügbaren Listen sind:

- Admin_Accounts
- Guest_Accounts

- Service_Accounts
- User_Blacklist
- User_Whitelist
- Host_Whitelist
- Domain_Controllers
- IP_Blacklist
- IP_Whitelist
- Host_Blacklist

Hinweis: Wenn bereits vor der Aktualisierung oder Installation von RSA NetWitness Platform11.2 eine Liste mit dem gleichen Namen existiert, dann wird diese Liste beibehalten. Entweder benennen Sie diese Liste vor der Aktualisierung auf 11.1 um oder aktualisieren die Inhalte so, dass sie in ESA-Regeln verwendet werden können.

Die Listen sind auf der Registerkarte „ESA-Regeln“ in „KONFIGURIEREN > ESA-Regeln > Einstellungen > Erweiterungsquellen“ verfügbar. Weitere Informationen zu den ESA-Regeln finden Sie im *Handbuch zum Versenden von Warnmeldungen mit ESA für Version 11.1.*
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 Klicken Sie auf , um eine Entitätszuordnung hinzuzufügen oder zu bearbeiten.

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

9 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 Platform-Nutzer beim Einrichten ihres Context-Hub-Service stoßen können.

Mögliche Probleme

Problem	Lösung
Der Vorabruf für die Liste kann nicht ausgeführt werden, wenn die Liste im Modus „Anhängen“ erstellt wird. Die folgende Fehlermeldung wird in Protokollen angezeigt, die darauf hinweisen, dass Einträge in der Liste das zulässige Maximum überschreiten. `Error setting data source entries com.rsa.asoc.contexthub.exception.ContextHubException: total.entries.exceed.max` „Integrität und Zustand“ legt diesen Status ebenfalls fest: `Contexthub.Datasource.Health.Data-Sources-Health`auf `Unhealthy` und zeigt die Namen der Listen an, für die der Vorabruf fehlgeschlagen ist. Die Anzahl der Einträge in der Liste beträgt beispielsweise 50001 und die Anzahl der Datensätze in der CSV-Datei ist 50001, da der Nutzer die CSV-Datei seit dem letzten Vorabruf nicht geändert hat. Die Obergrenze für die Anzahl der Einträge in der Liste beträgt 100.000. Beim Vorabruf versucht Context Hub nun, 50001 Einträge an die Liste anzuhängen, aber da 50001 + 50001 > 100.000 ist, kann der Vorabruf nicht ausgeführt werden.	Fügen Sie in der CSV-Datei nur die Einträge hinzu, die an die vorhandene CSV-Daten angehängt werden sollen. Wenn Sie keine Einträge an die Liste anhängen möchten wollen, führen Sie eine dieser Optionen aus, falls zutreffend: • Wenn Sie die Liste mit Überschriften erstellt haben, entfernen Sie mit Ausnahme der Überschrift alle Zeilen aus der CSV-Datei. • Wenn Sie eine Liste ohne Überschrift erstellt haben, sollte die CSV-Datei 0 Zeilen enthalten.
Der SSL-Handshake mit dem 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“ in der Ansicht „Reagieren“ führt nicht zum richtigen Link.	Sie müssen den Jetty-Service auf dem NetWitness-Server neu starten. Melden Sie sich beim NetWitness-Serverhost an und geben Sie den Befehl `service jetty restart` ein.

Problem	Lösung
Wenn Sie eine Liste mit fehlenden Anführungszeichen in den Listenelementen importieren, z. B. 172.16.0.0, wird die Liste ohne anzuzeigende Daten gespeichert. Der Grund ist, dass die CSV-Dateien aufgrund eines Apache-Fehlers (CSV-141) mit einem falschen Format analysiert werden.	Importieren Sie eine Liste mit korrekten Anführungszeichen, um zu vermeiden, dass eine leere Datei angezeigt wird. Beispiel: “172.16.0.0”, “host.mycompany.com” usw.
Das Erhöhen der Anzahl der zulässigen Warnmeldungen und Incidents führt zu einem Abfragefehler. Die Anzahl der angezeigten Warnmeldungen und Incidents ist standardmäßig auf 50 begrenzt.	Wenn der Grenzwert erhöht wird, kann die größere Anzahl abgefragter Metadaten für Warnmeldungen und Incidents aufgrund einer internen Datenbankbeschränkung zu einem Abfragefehler führen. Um dies zu beheben, stellen Sie die Standardeinstellungen wieder her, die die Anzahl der angezeigten Warnmeldungen und Incidents auf 50 begrenzen.