RSA NETWITNESS® SUITE

Context Hub構成ガイド

バージョン 11.0

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/EMC-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、本使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしています。予告なく変更される場合があります。

2月 2018

目次

Context Hubの仕組み

Context Hubサービスは、対応ビューと調査ビューの両方で、エンリッチメント ルックアップ機能を提供します。管理者は、Context Hubサービスとデータ ソースを構成して、必要なデータ ソースのコンテキスト ルックアップをアナリストが行えるようにすることができます。

Context Hubサービスでは、IPアドレス、ユーザ、ドメイン、MACアドレス、ファイル名 、ファイル ハッシュ、ホストなどのメタ タイプに対するエンリッチメント ルックアップをデフォルトでサポートします。

次のデータ ソースはNetWitness Suiteのサポート対象であり、構成することでエンリッチなデータを提供します。

リスト: ブラック リスト、ホワイト リスト、ウォッチ リストからコンテキスト情報を提供します。

RSA Archer: 常時監視が必要なデバイス、またはIPやホストに基づく特定の資産の重要な情報を提供します。

Active Directory: 疑わしいユーザかどうかの判断を支援する、ユーザのコンテキスト情報を提供します。

RSA NetWitness® Endpoint: 侵害されたEndpointデバイスがあるかどうかの判断を支援する、エンドポイント モジュールやマシン インジケータのコンテキスト情報を提供します。

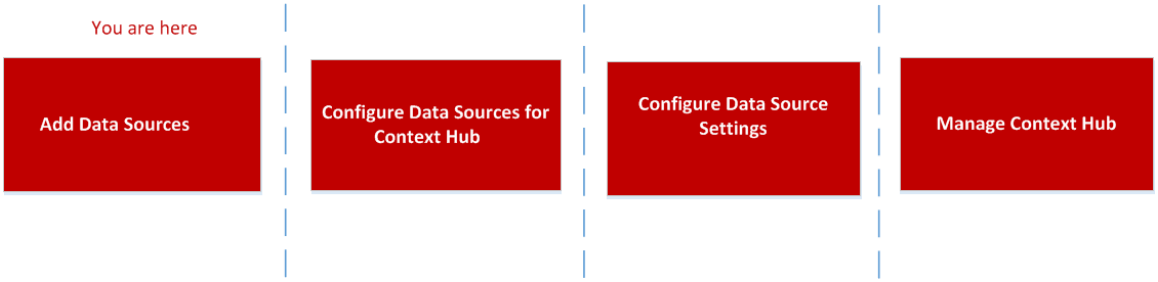
Respond: Respondで取得可能な特定のメタのコンテキスト情報を提供し、コンテキスト データに基づいてアナリストがより迅速に対応できるようにします。

Live Connect: RSA Live Connect脅威インテリジェンス コミュニティ サーバから受け取ったIPアドレス、ドメイン、ファイル ハッシュを提供します。

Context Hubの構成の概要

コンテキスト ルックアップを効果的に実施するために、管理者は各ステップを適切な順序で実行してサービスを構成する必要があります。**管理**＞[**サービス**]で、Context Hubサービスのデータソースは、Context Hubサービスの[構成]ビューで管理者が構成できます。管理者は、必要に応じて、カスタム メタ キーのコンテキスト ルックアップを構成できます。また、リストをインポートしたりエクスポートしたりできます。

次のワークフローでは、Context Hubサービスを構成する方法について説明します。



Context HubサービスはプライマリESAホストにプリインストールされており、NetWitness Suiteに自動的に追加されます。

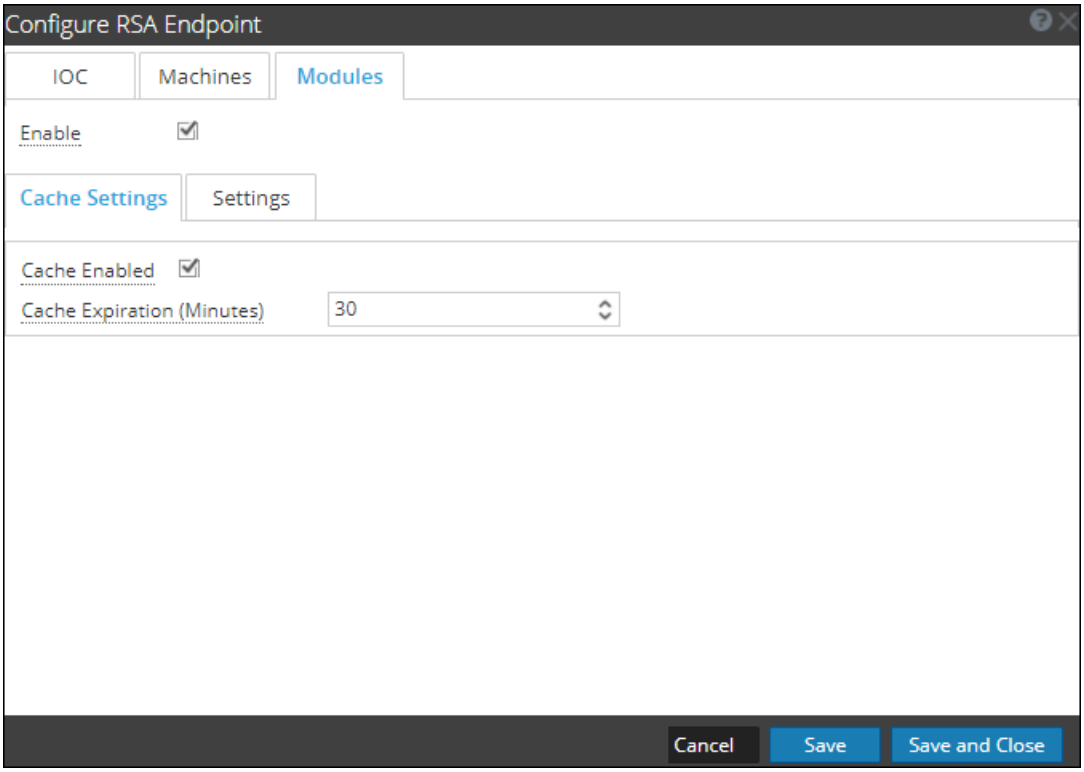
注：NetWitness Suite導入環境で使用できるContext Hubサービス インスタンスは1つのみです。NetWitness SuiteにESAサービスが複数ある場合は、Context Hub用の適切なESAホストを選択する必要があります。ESAホストでContext Hubを構成するには最低8 GBの領域が必要です。

Context Hubのデータ ソース設定の構成

必要なデータ ソースを構成した後は、お客様の要件に基づいて、データ ソースの設定をカスタマイズできます。

設定にアクセスし構成するには、次のようにします。

1. [**管理**]＞[**サービス**]に移動します。
   [サービス]ビューが表示されます。
2. [サービス]パネルで、Context Hubサービスを選択し、＞[**表示**]＞[**構成**]をクリックします。
   Context Hubの[サービス]の[構成]ビューが表示されます。
3. 設定を構成するデータ ソースを選択し、[アクション]列で をクリックします。
   次のスクリーンショットの例は、NetWitness Endpointの設定ダイアログです。



4. 次のフィールドを設定します。

フィールド	説明
有効化	このオプションはデフォルトで有効(オン)に設定されています。選択したデータソースからのレスポンスを有効化または無効化することができます。
キャッシュ設定	Context Hubからのすべてのルックアップは、構成した時間Context Hubのキャッシュに保存できます。一致する以後のリクエストに対するレスポンスは、Context Hubのキャッシュからフェッチされます。クエリのルックアップでは、次のキャッシュ設定を定義するためにこのセクションを使用します。 • **キャッシュ有効**:デフォルトでは、このチェックボックスが選択されていて、クエリのレスポンスをキャッシュします。 • **キャッシュ有効期間(分)**:クエリのルックアップがキャッシュに保持される最大時間。デフォルトの時間は30分、構成可能な最大数は7200分です。
リスト値の有効期間	**有効化**:リスト値を使用可能にする必要のある日数を定義するには、[有効化]を選択します。デフォルトで、このオプションは無効になっており、値は保持されます。 **有効期間(日数)**:リスト値を保持する日数を入力します。
メタマッピング	Context Hubに格納されている任意のリストは、ルックアップに使用できる必要があります。Context Hubのルックアップは、メタタイプやエンティティに基づいて行われます。例:IP、HOST、MAC ADDRESS、DOMAIN、FILE_NAME、FILE_HASH、USER。 **メタタイプ**:Context Hubで使用可能なエンティティ。 **Context Hubフィールド**:リストデータソースの追加時に追加したCSVファイルの列ヘッダー。
最小IIOCスコア	NetWitness Endpontモジュールのコンテキスト情報をフェッチする場合に考慮すべき最小IIOCスコア。
クエリの対象期間(日数)	コンテキストデータをクエリする必要のある期間(日数)。
制限	コンテキストルックアップの実行時に表示するレコードの最大数。
繰り返し間隔	必要なインターバルでコンテキストデータの取得と保存を行う繰り返しスケジュールを構成します。

5. 次のオプションのいずれかをクリックします。
   - **キャンセル**: 変更をキャンセルするには、このオプションを選択します。
   - **保存**: 変更を保存するには、このオプションを選択します。
   - **保存して閉じる**: 保存してダイアログを閉じるには、このオプションを選択します。

選択したデータソースに基づいてレスポンスグループは異なります。次の表では、すべてのデータソースのレスポンスグループについて説明します。

データソース(接続)	サポートされているレスポンスグループ	フィールドの設定
 リスト	リスト	メタマッピング メタタイプ Context Hubフィールド 設定 データプリフェッチ設定 繰り返し作業のスケジュール設定 リスト値の有効期限 キャッシュ設定 キャッシュ有効 キャッシュ有効期間(分):最小30分、最大7200分
 RSA Archer	Archer	キャッシュ設定 キャッシュ有効 キャッシュ有効期間(分)
 Active Directory	ユーザ	メタマッピング メタタイプ Context Hubフィールド 設定 データプリフェッチ設定 繰り返し作業のスケジュール設定 リスト値の有効期間 キャッシュ設定 キャッシュ有効 キャッシュ有効期間(分):最小30分、最大7200分

データ ソース (接続)	サポートされているレスポンス グループ	フィールドの設定
RSA Endpoint	IOC コンピューター モジュール	キャッシュ設定 キャッシュ設定 設定 コンテキスト パネル設定 キャッシュ設定
Respond	アラート インシデント	コンテキスト パネル設定 データ プリフェッチ設定 クエリの対象期間(日数) キャッシュ設定 キャッシュ有効 キャッシュ有効期間(分)
Live Connect	ドメイン ファイル IP	キャッシュ設定 設定 コンテキスト パネル設定

注:データ ソースの設定を構成した後に、[**管理**]>[**サービス**]>[**ビュー**]>[**エクスプローラ**]に移動することで、Context Hubの構成パラメータを構成することができます。[エクスプローラ]ビューで構成に変更を加えた場合、Context Hubサービスを再起動することを確認します。

Context Hubのリストのインポートとエクスポート

管理者は、Context Hubサービスで構成されたリストをアナリストが使用できるようインポートまたはエクスポートできます。インポートまたはエクスポートするファイルはCSVファイルで、データソースとして複数のリストを追加できます。

前提条件

Context Hubサービスが有効化されていて、NetWitness Suiteの[**管理**]＞[**サービス**]ビューで使用できることを確認してください。

リストのインポート

リストをインポートした後は、次のタスクを実行することができます。

- 既存のリストへの値のインポート
- リストへの行の追加
- リストの名前と説明の編集
- リストの値の編集
- リストの削除
- リストの行の削除

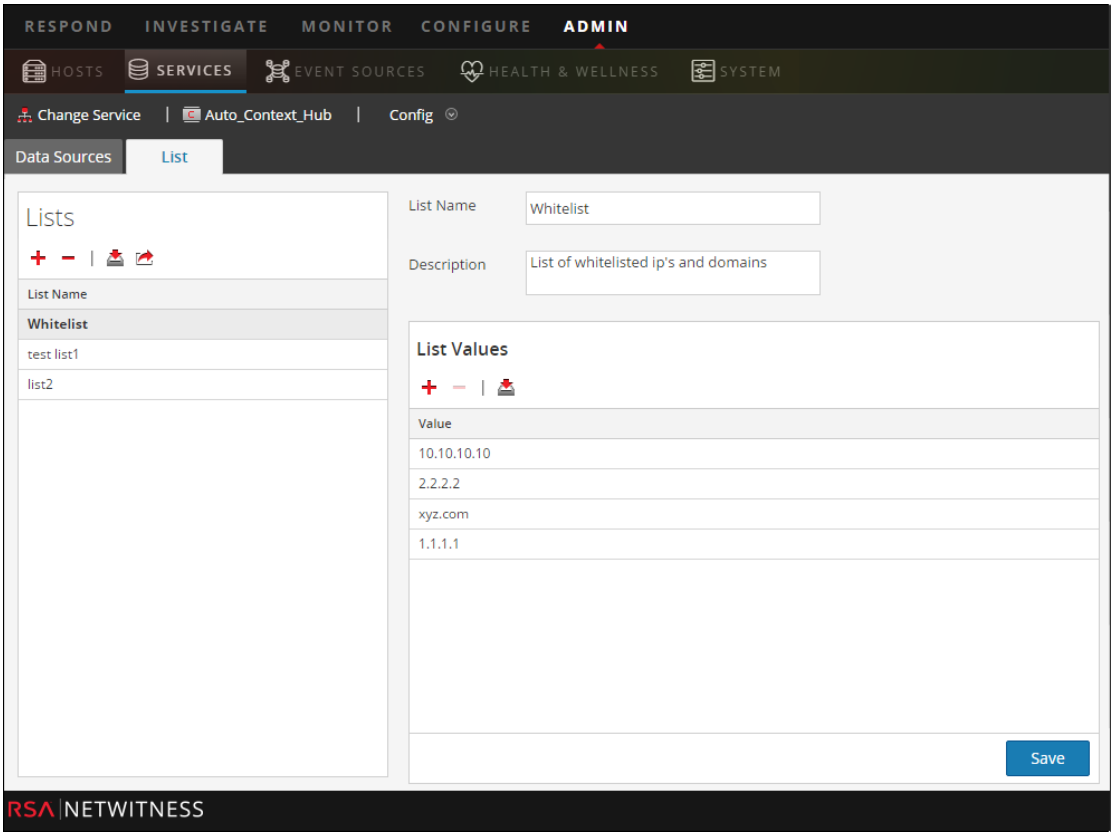
注：対応する.CSVファイルに対しても同じ変更を行う必要があります。同じ変更を行うことで、スケジュールが次に実行されたタイミングで変更が反映されます。同じ変更を行わずに既存の単一列または複数列のリストに値をインポートすると、スケジュールが次に実行されたタイミングで、データがソースファイルで上書きされます。

単一列のリストのインポート

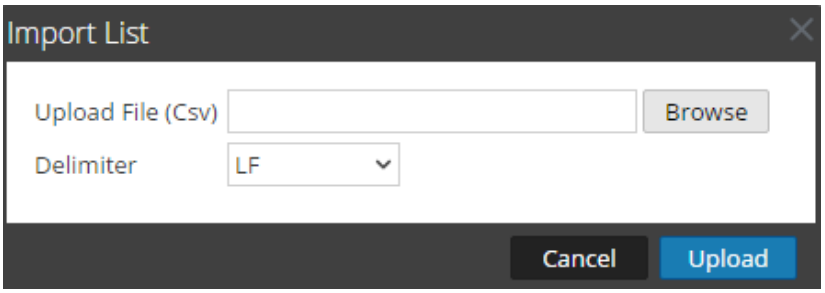
リストをインポートするには、次の手順を実行します。

1. 管理＞[**サービス**]を選択します。
   [サービス]ビューが表示されます。
2. [**サービス**]パネルで、Context Hubサービスを選択し、  ＞[**表示**]＞[**構成**]をクリックします。
   Context Hubサービスの[構成]ビューが表示されます。
3. [**リスト**]タブをクリックします。
   [リスト]タブには、[**リスト**]パネルと[**リスト値**]パネルがあります。

次のイメージは、単一列のリストの例です。



4. [**リスト**]パネルの  をクリックします。
   [**リストのインポート**]ダイアログが表示されます。



5. [**リストのインポート**]ダイアログで、次の手順を実行します。
   a. [**ファイルのアップロード(.CSV)**]フィールドで、CSVファイルを参照して選択します。
   b. [**改行コード**]フィールドで、リストの値を区切る区切り文字を選択します。[**Comma**]、[**CR**](キャリッジ リターン)、[**LF**](改行)のオプションから選択できます。
6. [**アップロード**]をクリックして、CSVファイルをContext Hubにアップロードします。

これらのリストは、コンテキスト情報を取得するデータソースとして考慮されます。既存の複数列のリストに追加することができます。列数が一致している場合にのみ、データが追加されます。

注:インポート操作で新しい複数列リストを作成することはできません。複数列リストをインポートする方法については、「Configure List Data Source for Context Hub」を参照してください。。

既存のリストへの値のインポート

既存の複数列リストにインポートすると、スケジュールが次に実行されたタイミングでデータが上書きされます。

値をリストにインポートするには:

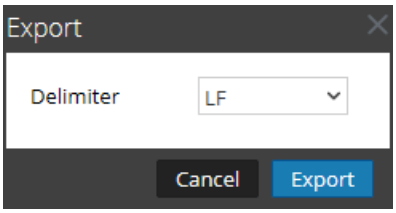
1. **管理**>[**サービス**]に移動します。
   [サービス]ビューが表示されます。
2. サービスを選択し、  >[**表示**]>[**構成**]をクリックします。
   Context Hubサービスの[構成]ビューが表示されます。
3. [**リスト**]タブをクリックします。
   [リスト]タブには、[**リスト**]パネルと[**リスト値**]パネルがあります。
4. [リスト]パネルで、値をインポートするリストを選択します。
5. [**リスト値**]パネルの  をクリックします。
   [**リストのインポート**]ダイアログが表示されます。
6. [**リストのインポート**]ダイアログで、次の手順を実行します。
   a. [**ファイルのアップロード(CSV)**]フィールドで、CSVファイルを参照して選択します。
   b. [**改行コード**]フィールドで、リストの値を区切る区切り文字を選択します。[**Comma**]、[**CR**](キャリッジリターン)、[**LF**](改行)のオプションから選択できます。
7. [**アップロード**]をクリックして、CSVファイルをNetWitness Suiteにアップロードします。

選択したリストにリスト値がインポートされます。これらのリストは、コンテキスト情報を取得するデータソースとして考慮されます。既存の複数列のリストに追加することができます。列数が一致している場合にのみ、データが追加されます。

Context Hubのリストのエクスポート

リストをエクスポートするには、次の手順を実行します。

1. Context Hubサービスの[構成]ビューにある[**リスト**]タブで、  をクリックします。
   [**エクスポート**]ダイアログが表示されます。



2. [**改行コード**]フィールドで、エクスポートしたリストの値を区切る区切り文字を選択します。[**Comma**]、[**CR**](キャリッジ リターン)、[**LF**](改行)をドロップダウンから選択できます。
3. [**エクスポート**]をクリックします。

単一列リストの場合は区切り文字を指定できます。複数列リストの場合は、リストがCSVファイルとしてローカル マシンにエクスポートされます。

Context Hubのメタ タイプ マッピングの構成

管理者として、NetWitnessメタ キーを使用してContext Hubのメタ タイプ マッピングを管理します。

Context Hubサービスを使用すると、[Respond]および[調査]ビューでメタ値のコンテキスト ルックアップを実行できます。これらのメタ値は、それぞれが属するカテゴリーに基づいてメタ タイプにグループ化されます。たとえば、`ip.src`や`ip.dst`のようなNetWitness SuiteRespondおよびInvestigationのメタ キーは、Context Hubのメタ タイプ`IP`にグループ化されます。そのメタ タイプ`IP`は、対応データベースでは`alert.events.source.device.ip_address`や`alert.events.destination.device.ip_address`などのメタにマッピングされます。

管理＞[**システム**]＞[**Investigation**]ビューの[コンテキスト ルックアップ]では、NetWitnessメタ キーとメタ タイプのマッピングを構成することができます。管理者は、Context Hubでサポートされるメタ タイプのリストにメタ キーを追加したり、それらを削除したりできます。

Context Hubサービスでは、メタ タイプとメタ キーのデフォルトのマッピングが事前に構成されています。デフォルトのマッピングは、特定の環境向けにカスタム マッピングを作成する必要がある場合を除き、ほとんどの構成環境に使用できます。

注：新しいメタ タイプを追加することはできません。

デフォルトのマッピングは次のとおりです。

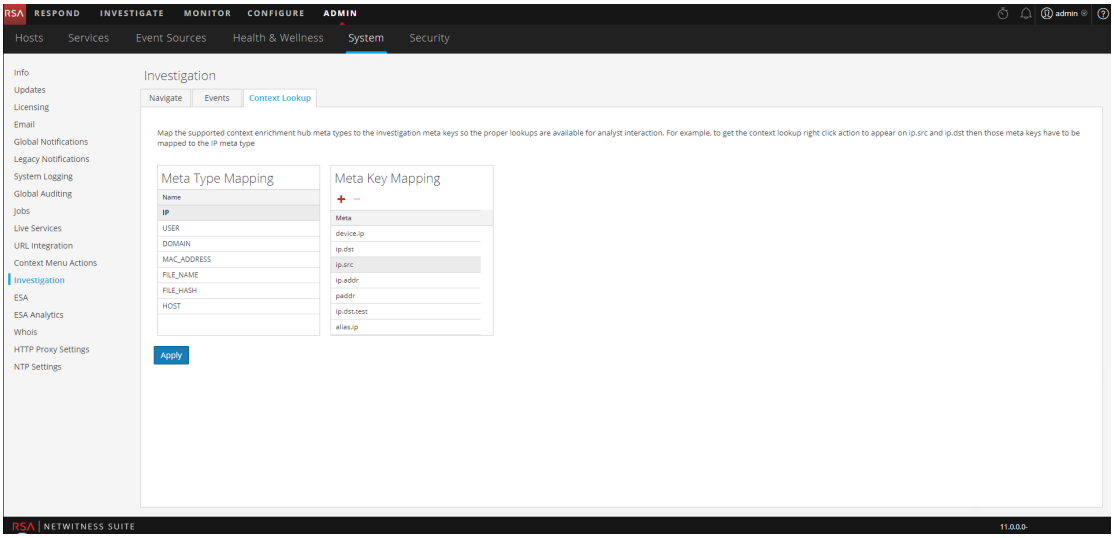
メタ タイプの名前	メタ キー
IP	device.ip、ip.src、ip.dst、ip.addr、ipv6.src、alias.ip、ipv6.addr、device.ipv6、forward.ip、forward.ipv6、ipv6.dst、ipv6.addr、stransaddr、transaddr
USER	user.src、user.dst、username、event user
DOMAIN	domain.src、domain.dst、fqdn、web.domain、 domain、sdomain、ddomain
MAC_ ADDRESS	eth.dst、eth.src、alias.mac
FILE_ NAME	filename、sourcefile
FILE_ HASH	checksum
HOST	device.host、alias.host、host.src、host.dst

手順

Investigationのメタ キーのマッピングを管理するには、次の手順を実行します。

1. 管理＞[**システム**]に移動します。
2. [オプション]パネルで、[**Investigation**]を選択します。

   [Investigation]パネルが表示されます。
3. [**コンテキスト ルックアップ**]タブを選択します。



4. メタ タイプを選択すると、そのメタ タイプがマッピングされているデフォルトのメタ キーが表示されます。
5. メタ キーを追加するには、＋をクリックしてメタ キーを入力します。
6. メタ キーを削除するには、メタ キーを選択して －をクリックします。
7. [**適用**]をクリックして、変更を保存します。
8. 新しいメタを追加するには、Concentratorのカスタム インデックス ファイルに含まれる必要があります。たとえば、メタ「**fqdn**」を追加する場合は、新しいエントリ―**<key name="fqdn" description="Fully Qualified Domain Name="IndexValues" form-at="Text" valueMax="100" />**をインデックス ファイルに追加する必要があります。インデックス ファイルに新しいメタを追加する方法の詳細については、「*Core Database Tuning Guide*」の「Index Customization」トピックを参照してください。新しいメタを追加した後は、ピボットをクリックしてコンテキスト情報を表示し、[対応]ビューのオプションを調査することができます。

新しいメタ キーを追加した場合、そのメタ キーのメタ値に対応する[コンテキスト ルックアップ]メニュー オプションが有効になります。詳細については、「*システム構成ガイド*」の「Investigation Configurationパネル」トピックを参照してください。

Context Hubの参考情報

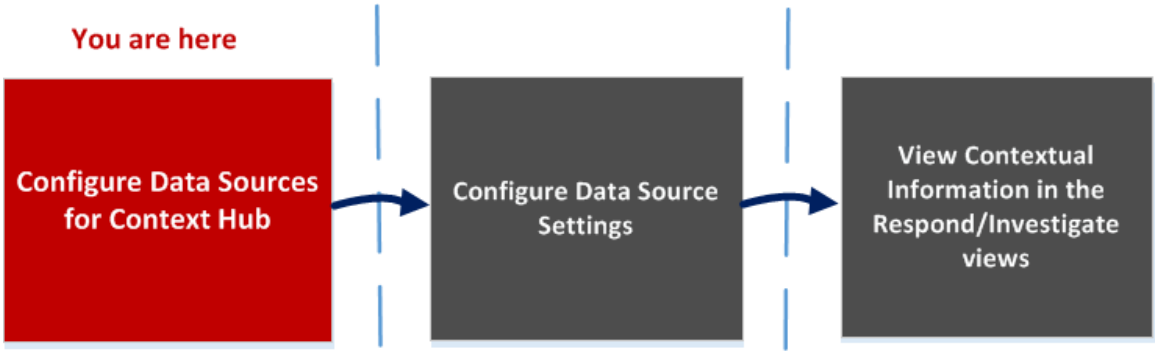
Context Hubサービスと必要なデータソースを構成した後は、各データソースの設定を管理できます。これにより、検索結果の最適化とカスタマイズができます。

Context Hubの[データ ソース]タブ

[**データソース**]タブで、Context Hubサービスの1つまたは複数のデータ ソースを構成することができます。[**管理**]＞[**サービス**]＞Context Hubサービスの選択＞[**ビュー**]＞[**構成**]＞[**データ ソース**]タブに移動します。

ワークフロー

このワークフローは、[対応]ビューまたは[調査]ビューのコンテキスト情報を表示するようにContext Hubサービスのデータ ソースを構成する手順を示しています。



- 最初のタスクでは、データ ソースを追加します。
- 2番目のタスクでは、導入環境を機能拡張するためにデータ ソースの設定を構成します。各データ ソースの設定は、パフォーマンスが最適になるようにデフォルト値が事前に設定されているので、このタスクはオプションです。
- 3番目のタスクでは、[対応]ビューまたは[調査]ビューの[コンテキスト サマリ]パネルにコンテキスト情報を表示して分析します。

実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	Context Hubのデータ ソースの構成	Context Hubのデータ ソースの構成
管理者	Hubのデータ設定の構成*	Context Hubのデータ ソース設定の構成

ロール	実行したいこと	手順
Analyst	[対応]ビューでのコンテキスト情報の表示	「*Netwitness Respondユーザガイド*」を参照してください。
Analyst	[対応]ビューまたは[調査]ビューのリストの追加、作成、削除	「*Netwitness Respondユーザガイド*」を参照してください。 「*調査およびマルウェア解析ユーザガイド*」を参照してください。
Analyst	既存のリストのエントリーの追加または削除	「*Netwitness Respondユーザガイド*」を参照してください。

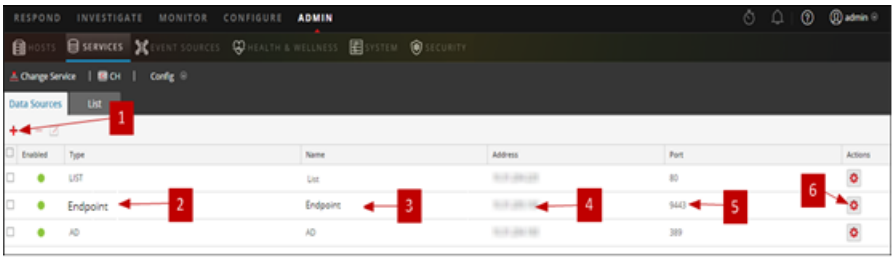
*このタスクはここ(つまり、Context Hubの[データソース]タブ) で完了できます。

関連トピック

- データソースとしてのリストの構成
- Configure Archer as Data Source
- Configure Active Directory Data Source
- Configure NetWitness Endpoint Data Source
- Configure Respond Data Source
- Configure Live Connect Data Source

簡単な説明

次の例では、Context Hubサービスのデータソースを追加する方法を示しています。



1. ➕をクリックして[**データソースの追加**]ダイアログを表示します。
2. データソースのタイプを表示します。
3. データソースを識別する名前。
4. データソースのIPアドレスまたはホスト名。

5 データソースの接続ポート。

6 **[設定の構成]**ダイアログを開きます。[対応]ビューまたは[調査]ビューの[コンテキストサマリ]パネルに表示される設定を表示して編集できます。

7 **[テスト接続]**をクリックして、Context Hubサービスにホストが接続されていることを確認します。

ツールバー

次の表は、ツールバーのアクションについて説明しています。

機能	説明
	[データソースの追加]ダイアログが開き、データソースを追加できます。データソースはタイプごとに1つだけ追加できます。複数をまとめて追加できるリストおよびActive Directoryデータソースの場合を除きます。データソースを追加する詳細な手順については、「Context Hubのデータソースの構成」を参照してください。
	データソースを削除します。 データソースを削除すると、削除したサービスがContext Hubでデータソースとして考慮されなくなります。それまでにフェッチされたすべてのコンテキスト情報が使用できなくなります。
	[データソースの編集]ダイアログが開きます。[データソースの編集]パネルの各フィールドの詳細については、「Context Hubのデータソースの構成」を参照してください。
	[設定の構成]ダイアログを開きます。データソースの設定を表示および編集できます。[レスポンスの構成]パネルの各フィールドの詳細については、「データソース設定の構成」を参照してください。

データソースの構成

次の表に、表示される構成の説明を示します。

機能	説明
有効	データソースが有効か無効かを示します。緑色で塗りつぶされた丸は、データソースが有効になっていることを示します(●)。塗りつぶされていない白い丸は、データソースが無効になっていることを示します。
タイプ	データソースのタイプ。たとえば、リスト、Archer、Active Directory、Endpoint、Respond、Live Connect。
名前	データソースを識別する一意の名前。たとえば、Respond \。
アドレス	データソースのIPアドレスまたはホスト名。
ポート	データソースの接続ポートは追加されるデータソースに応じて変わります。たとえば、Endpointのポートは9443、リストのポートは80です。

Context Hubの[リスト]タブ

[リスト]タブで、Context Hubのリストを作成して構成することができます。[**管理**]>[**サービス**]>[Context Hubサービスの選択]>[**ビュー**]>[**構成**]>[**リスト**]タブに移動します。

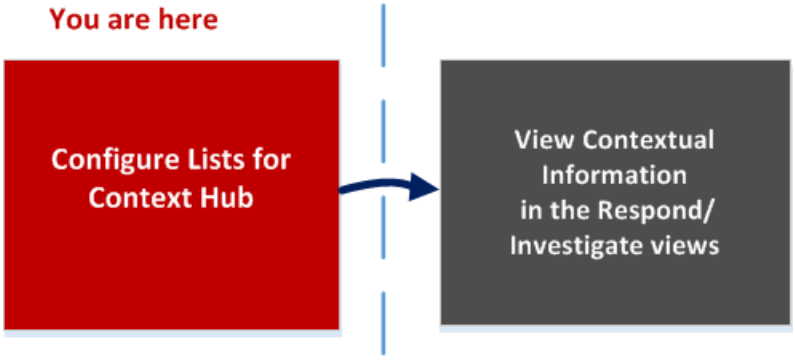
Context Hubサービスの[リスト]タブでは、1つ以上のリストを作成し、リストに値を追加できます。これらのリストは、自動的にContext Hubサービスのデータソースとみなされます。

これらのリストのアイテムは、CSVファイルをインポートするか、Investigationおよび[対応]ビューで[リストへの追加/削除]オプションを使用してメタ値を追加することで設定できます。

注:リストの作成やリスト値の追加は、RespondおよびInvestigationビューからも実行できます。詳細については、「*RSA Netwitness Respondユーザガイド*」と「*RSA Netwitness調査およびマルウェア解析ガイド*」を参照してください。

ワークフロー

このワークフローは、[対応]ビューおよび[調査]ビューのコンテキスト情報を表示するようにContext Hubサービスのリストを構成する手順を示しています。



1つまたは複数のリストを作成することが、このワークフローの最初のタスクです。リストには、IPアドレス、ユーザ、ホスト、ドメイン、MACアドレス、ファイル名、ファイルハッシュなどのサポートされているメタを含めることができます。次のタスクでは、リストのデータを分析または使用して、Respondおよび[調査]ビューにコンテキストデータを表示します。

実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	Context Hubのリストデータソースの構成*	Context Hubのデータソースとしてのリストの構成

ロール	実行したいこと	手順
管理者/アナリスト	[対応]ビューでのコンテキスト情報の表示	「*Netwitness Respondユーザガイド*」を参照してください。
管理者/アナリスト	Investigationでのリストとリスト値の管理	「*調査およびマルウェア解析ユーザガイド*」を参照してください。
管理者/アナリスト	リストの作成	「*Netwitness Respondユーザガイド*」と「*調査およびマルウェア解析ユーザガイド*」を参照してください。
管理者/アナリスト	リストの更新	「*Netwitness Respondユーザガイド*」と「*調査およびマルウェア解析ユーザガイド*」を参照してください。
管理者/アナリスト	リストの削除	「*Netwitness Respondユーザガイド*」と「*調査およびマルウェア解析ユーザガイド*」を参照してください。
管理者/アナリスト	リストのインポート	Context Hubのリストのインポートとエクスポート
管理者/アナリスト	リストのエクスポート	Context Hubのリストのインポートとエクスポート

*このタスクはここ(つまり、Context Hubの[リスト]タブ) で完了できます。

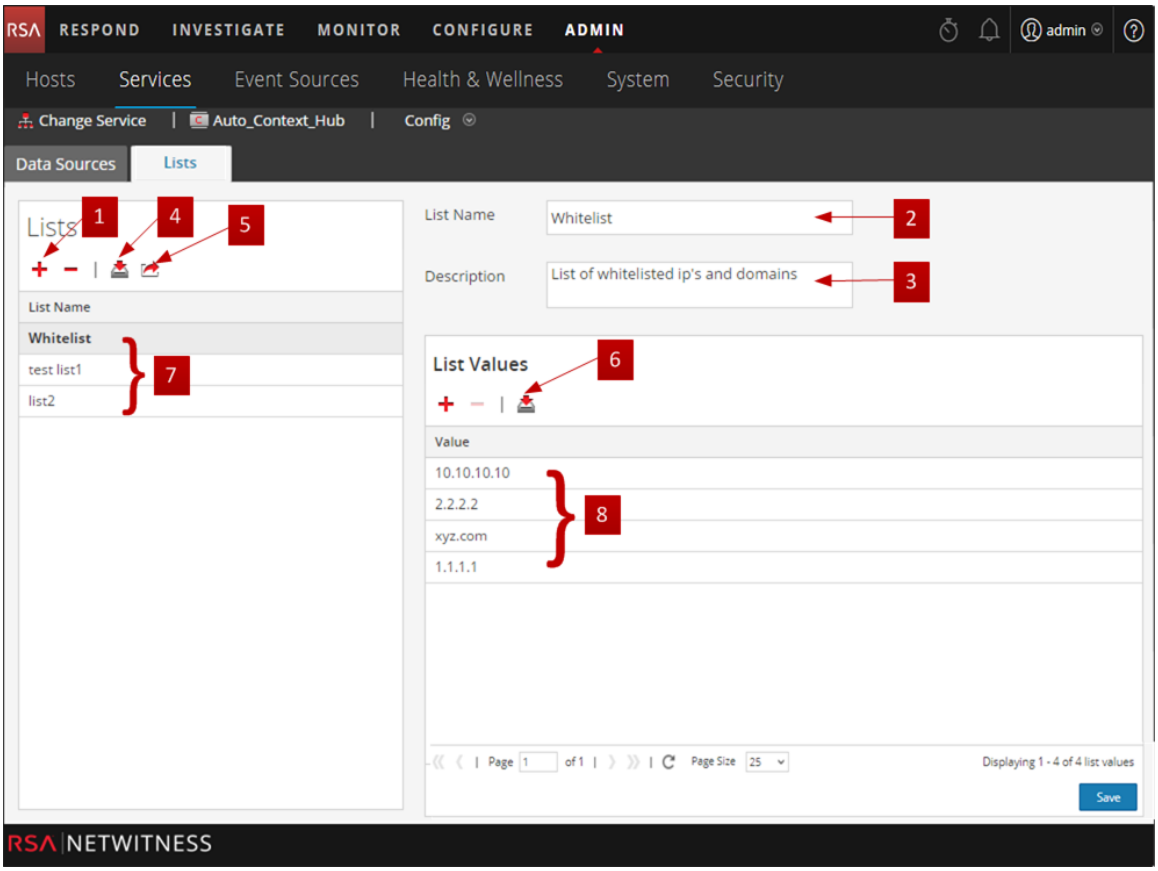
関連トピック

- Context Hubの[データ ソース]タブ

簡単な説明

次の例では、Context Hubサービスのリストを追加する方法を示しています。

[リスト]タブは、[**リスト**]パネルと[**リスト値**]パネルで構成されます。[**リスト**]パネルのツールバーには、リストを追加、削除、インポート、エクスポートするためのオプションがあります。[**リスト名**]の下に、Context Hubサービス用に追加またはインポートされたリストの一覧が表示されます。[**リスト値**]パネルのツールバーには、選択したリストのリスト値を追加、削除、インポートするためのオプションがあります。[**値**]の下に、リストに含まれる値の一覧が表示されます。



1	＋をクリックして新しいリストを追加します。
2	リストを識別する名前。
3	リストの説明。
4	をクリックしてContext Hubにリストをインポートします。
5	をクリックしてローカル マシンにリストをエクスポートします。
6	をクリックして選択したリストにリスト値をインポートします。
7	Context Hubに追加されているカスタム リストを表示します。
8	選択したリストに追加されているリスト値を表示します。

ツールバー

次の表は、ツールバーのアクションについて説明しています。

機能	説明
	新しいリストを追加します。 詳細については、「データ ソースとしてのリストの構成」を参照してください。
	リストを削除します。 Context Hubからリストを削除すると、そのリストはコンテキスト情報のデータ ソースとみなされなくなります。
	Context Hubにリストをインポートします。 詳細については、「Context Hubのリストのインポートとエクスポート」を参照してください。
	ローカル マシンにリストをエクスポートします。 詳細については、「Context Hubのリストのインポートとエクスポート」を参照してください。

[リスト]ビューのオプション

次の表に、リストの構成の説明を示します。

機能	説明
リスト名	リストを識別する一意な名前。
説明	リストの説明。
保存	リストに加えた変更を保存します。

次のステップ

構成を完了すると、[対応]ビューまたは[調査]ビューの[コンテキスト サマリ]パネルにコンテキスト データを表示できます。手順については、「*調査およびマルウェア解析ユーザ ガイド*」の「**[コンテキスト サマリー]パネルへの移動と追加コンテキストの表示**」を参照してください。

トラブルシューティング

このトピックでは、NetWitness SuiteユーザがNetWitness SuiteでContext Hubサービスを設定するときに発生する可能性のある問題について説明します。

発生する可能性のある問題

問題	解決策
Archer証明書をデータソースとして追加したにもかかわらず、Archer証明書を用いたSSLハンドシェイクに失敗します。	Archerで生成された証明書を[すべての証明書を信頼]オプションを設定した状態で使用します。
[対応]ページの[調査への移行]オプションが、適切なリンクに移動しません。	RabbitMQサーバを停止して再起動すると、[対応]画面で[調査への移行]オプションは表示されません。また、[調査への移行]のコンテキスト パネルで、同じページが再度開きます。NetWitnessサーバのjettyサービスを再起動する必要があります。Netwitnessサーバ ホストにログインして、service jetty restartコマンドを入力する必要があります。