RSA NETWITNESS® PLATFORM

NetWitness Investigate ユーザ ガイド

RSA NetWitness® Platform 11.4

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、https://www.rsa.com/ja-jp/company/rsa-trademarks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、Dell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、民事および刑事上の責任が課せられる可能性があります。

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

本製品はRSA 以外のサードパーティ製ソフトウェアを実装している場合があります。本製品を使用することにより、本製品のユーザは、本製品に含まれているサード 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

掲載される情報は、公開した時点でDellが正確であるとみなす情報であり、この情報は予告なく変更されることがあります。

10月 2020

目次

NetWitness Investigateの仕組み

NetWitness Investigateは、RSA NetWitness® Platformのデータ分析機能を提供します。アナリストはInvestigateを使用して、パケット、ログ、エンドポイント データを検証し、セキュリティとITインフラストラクチャに対する内部または外部からの潜在的な脅威を特定することができます。

注: バージョン11.1以降では、[ホスト]ビューおよび[ファイル]ビューにエンドポイント データが表示されます。以前のバージョンでは、スタンドアロンのNetWitness Endpointサーバを経由してエンドポイント データにアクセスできます。

メタデータ、メタ キー、メタ値、メタ エンティティ

RSA NetWitness Platformは、ネットワーク上のすべてのトラフィックを監査および監視できます。サービスの1つであるDecoderは、ネットワークからキャプチャされたパケット、デバイスから転送されたログ、エンドポイント エージェントが観察したエンドポイント イベントを取得、解析、保存します。

Decoderに構成されたルール、パーサ、フィードは、取得したログ、パケット、エンドポイント データをアナリストが調査できるよう、*メタデータ*を作成します。別のタイプのサービスであるConcentratorは、メタデータのインデックスを作成し、保存します。

メタデータは、*メタ キー*とその*メタ値*で構成されます。たとえば、`ip.src`はメタ キーであり、トラフィックのソースIPアドレスには、`ip.src`がタグ付けされます。Investigateでデータを表示すると、メタ キー`ip.src`と、そのキーがタグ付けされているすべてのIPアドレス(値) が表示されます。標準提供のメタ キーもあれば、管理者が定義したカスタム キーもあります。

メタ エンティティは、バージョン11.1以降で使用できます。*メタ エンティティ*は、異なるメタ キーの結果をグループ化するエイリアスです。メタ エンティティは、同様のメタ キーを単一の使いやすいメタ タイプにまとめます。一部のメタ エンティティはデフォルトで提供されますが、管理者がカスタム メタ エンティティを作成することもできます。アナリストは、クエリ、メタ グループ、列グループ、プロファイルの中でメタ エンティティを使用できます。座標表示チャートはメタ エンティティをサポートしていません。管理者は、ユーザのロールとユーザに適用するクエリ プレフィックスの定義で、メタ エンティティを使用することができます。「*Decoder構成ガイド*」に、メタ エンティティの作成に関する追加情報と、ルールでの使用方法が記載されています。

注: メタ エンティティは、すべてのアップストリームのConcentratorで構成する必要があります。いずれかのConcentratorにメタ エンティティが構成されていない場合、Brokerでクエリを実行すると、そのメタ エンティティは空になります。

たとえば、デフォルトのコア データベース言語には、ソースIP用と宛先IP用に別々のメタ キーが含まれています。標準提供のメタ エンティティの1つである`ip.all`は、ソースIPと宛先IPを合わせたすべてのIPアドレスを表します。

アナリストは通常、脅威を検出するためにBrokerまたはConcentratorに対してクエリを実行します。Concentratorはクエリを処理し、セッションの完全な再構築やRAWログが必要な場合にのみ、Decoderにアクセスします。ESA、Malware Analysis、Reporting EngineもConcentratorに対してクエリを実行し、各Decoderをクエリすることなく、イベントに関連づけられたすべてのメタデータをすばやく取得して、情報を生成できます。一部の特殊なケースでは、アナリストがDecoderに対してクエリを実行することがあります。

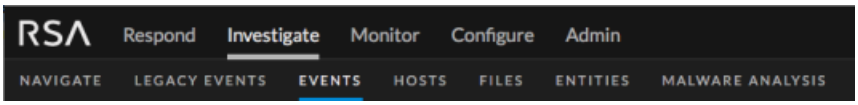
調査のトリガー

調査のトリガーの例をいくつか示します。

- 新しいActive Directoryハッキングに関するインテリジェンス情報が送られてきます。[イベント]ビューを開き、そのインテリジェンス情報を使用して、Active Directoryの過去24時間のすべてのRAWログ データに対して検索を実行します。
- SOCマネージャーから、話題になっているPokemon Goマルウェアを検索するように依頼されます。[ナビゲート]ビューを開き、SOCマネージャーがセキュリティ ブログで見つけたマルウェアに関連する特定のユーザ エージェントを使用したHTTPセッションを検索するクエリを作成します。
- インシデント対応者が、特定のホストに関連したいくつかの不自然なインジケータを示すチケットをエスカレーションします。[ホスト]ビューを開き、そのホストを調査してより明確な情報を探します。
- 新しいゼロデイ攻撃を探すため、[ナビゲート]ビューを開き、ネットワーク メタデータの調査を開始し、会社の外へ向かう異常な自動化セッションを探します。
- 解雇されて間もない従業員のユーザ アカウント`jarvis`に関連した情報を検索するようにSOCマネージャーから依頼されます。[調査]>[エンティティ]>[ユーザ]タブ(UEBA) を開き、そのユーザ名でフィルタリングし、そのユーザのアクティビティがなくなったことを確認し、そのユーザが解雇される前に通常の動作から逸脱していなかったかどうかを調べることができます。
- 検出されたフィッシング攻撃には、添付ファイルが関連付けられています。環境内のどのデバイスでそのファイルが閲覧されたかを調べるため、[調査]>[ファイル]でファイル ハッシュを検索します。
- 悪意のあるファイルが環境内で自動的に検出されたため、そのファイルに対する静的および動的な分析と、そのファイルに感染したシステムの数を確認する必要があります。[調査]>[マルウェア分析]を開き、分析結果を確認できます。

調査のワークフロー

アナリストは、NetWitness Platformによって収集されたデータを調査し、NetWitness Platformダッシュボード上の情報、NetWitness Respondのインシデントまたはアラート、NetWitness Platform Reporting Engineによって作成されたレポート、またはサード パーティ アプリケーションの情報を掘り下げて調べることができます。調査の過程で、アナリストは[調査]ビュー([ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビュー、[ホスト]ビュー、[ファイル]ビュー、[エンティティ]ビュー、[マルウェア分析]ビュー) をシームレスに移動することができます。次の図は、NetWitness Investigateの[調査]ビューのサブメニューを示しています。



注:
- [ファイル]ビューと[ホスト]ビューはバージョン11.1以降で使用可能です。
- [ユーザ]ビューはバージョン11.2および11.3で使用可能です。バージョン11.4では、[エンティティ]ビューに名称変更されました。
- [レガシー イベント]ビューはバージョン11.4ではデフォルトで無効になっていますが、『*システム構成ガイド*』の説明に従って管理者が有効にできます。
- ユーザがNetWitness Platformで調査とマルウェア分析を行うには、特定のユーザ ロールと権限が必要です。ビューを表示できない場合は、管理者によりロールや権限の変更が必要となる可能性があります。

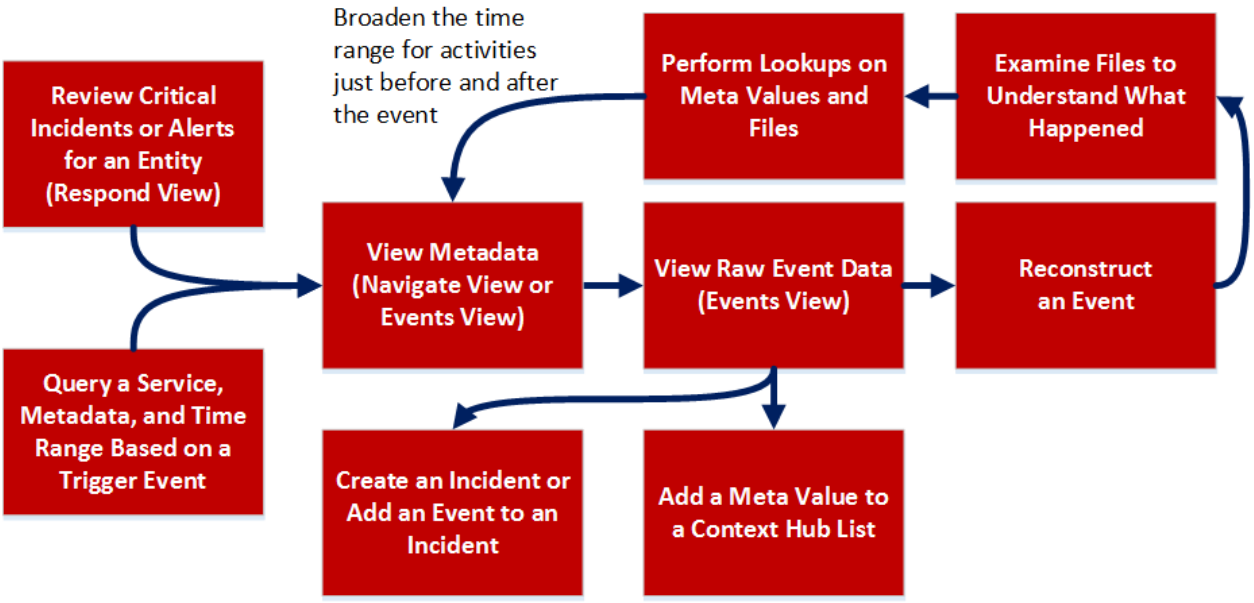
各ビューには、[調査]ビューのサブメニューや他の[調査]ビューからアクセスすることができます。NetWitness Respondの[対応]ビューから[調査]ビューに直接移動したり、[調査]ビューから[対応]ビューやスタンドアロンNetWitness Endpointに直接移動することができます。ユースケースによって、調査の起点が決まります。一般的に、調査の対象となるようなイベントには、他とは異なる特徴を見いだすことができます。何かを突き止めてから、その結果に基づいて次の調査ポイントに移動する必要があるため、多くの調査は、1つのビューで始まって、別のビューで終わります。次の表は、さまざまなユースケースの開始ビューに関する一般的なガイダンスを示しています。

開始場所	調査の焦点
[ナビゲート]ビュー	メタ キーと、メタ キー別にグループ分けされたログ、エンド ポイント、パケットのメタ値。データをピボット分析して結果を絞り込んでから、[イベント]ビューに移動するか、マルウェア分析またはLiveで検索することができます。このビューは、[調査]ビューのデフォルトのビューです(「結果セットの絞り込み」と「結果のダウンロードと処理」を参照してください)。
[イベント]ビュー	イベントをインタラクティブに操作するアナリストのデフォルトのワークフローは、できるだけビューを切り替える必要がないよう最適化されています。11.3の[イベント分析]ビューに主要な機能が追加され、デフォルトの[イベント]ビューになりました。 [イベント]ビューでは、イベントは時系列に表示されます。RAWイベントと関連メタデータの表示、リストのソートと検索、着目点(着目すべきバイト、ファイル タイプ、エンコード データ)の特定に役立つヒントを示す再構築の表示、イベントとファイルのダウンロードを行えます。スタンドアロンEndpoint Serverへの移動、Liveでの検索、その他の内部ルックアップと外部ルックアップの実行が可能です。外部ルックアップでは、調査したいメタ値をインターネット上で検索したり、IPアドレスに関連したパッシブDNS情報を特定したり、URLがブラックリストに登録されているかどうかを確認したり、他のサード パーティ製品とコンテキスト統合することができます(「結果セットの絞り込み」、「イベントの再構築と分析」、「結果のダウンロードと処理」を参照してください)。

開始場所	調査の焦点
[レガシー イベント]ビュー	[レガシー イベント]ビューは、過去のバージョン(11.0～11.3.x.x) では、[イベント]ビューと呼ばれていました。[レガシー イベント]は不要になり、管理者が有効にしない限り、非表示になります。デフォルトでは、[イベント]ビューのみがメニューに表示されますが、[レガシー イベント]ビューが有効になっている場合は、[イベント]ビューと[レガシー イベント]ビューの両方がメニュー バーに表示されます。 RAWイベントと関連メタデータを表示したり、再構築を表示したり、イベントとファイルをダウンロードすることができます(「結果セットの絞り込み」、「イベントの再構築と分析」、「結果のダウンロードと処理」を参照してください) 。
[ホスト]ビュー	NetWitness Endpointエージェントが実行されているホストが表示されます。ホストごとに、プロセス、ドライバ、DLL、ファイル(実行可能ファイル) 、サービス、異常、実行中のAutorun、ログイン ユーザに関連する情報が表示されます。[ホスト]ビューからは、[ナビゲート]ビュー、[イベント]ビュー、および[エンティティ]ビューに移動できます。(『*NetWitness Endpointユーザ ガイド*』を参照。)
[ファイル]ビュー	導入環境内のPE、Macho、ELFなどのファイルが表示されます。ファイルごとに、ファイル名、レピュテーション ステータス、ファイルのステータス、リスク スコア、署名、チェックサムなどの詳細を表示できます。[ファイル]ビューからは、[ナビゲート]ビューと[イベント]ビューに移動できます。(『*NetWitness Endpointユーザ ガイド*』を参照。)
[マルウェア分析]ビュー	Malware Analysisアプライアンスを実行している場合は、ファイルをスキャンして、4種類の分析(ネットワーク、静的、コミュニティ、サンドボックス) の結果を表示できます。ファイルがマルウェアの場合は、[ホスト]ビューに移動して、どのホストがそのファイルをダウンロードしたかを確認することができます。(『*Malware Analysis ユーザ ガイド*』を参照してください。)
[エンティティ]ビュー	バージョン11.2および11.3では、[ユーザ]ビューと表示されていました。NetWitness UEBAを使用して、エンタープライズ全体で高リスク ユーザの行動を可視化できます。環境内の高リスク ユーザのリストと、高リスク行動を示す上位アラートのサマリーが表示されます。ユーザまたはアラートを選択すれば、高リスク行動の詳細と、発生のタイムラインを表示できます。管理者またはUEBAアナリスト ロールを割り当てられたNetWitness Platformユーザは、このビューにアクセスできます(『*RSA NetWitness UEBAユーザ ガイド*』を参照してください) 。

メタデータ、クエリ、時間に焦点を当てた調査

次の図は、メタデータ、クエリ、時間範囲に焦点を当てた調査のワークフローを示しています。



アナリストは、インシデント対応ワークフローを進めるために必要なイベントを追跡したり、別のツールがイベントを生成した後で戦略的な分析を行う場合に、Nwtwitness Investigateを使用します。[ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビューのいずれかを開き、次のように調査します。

- まず、サービスから特定の時間範囲のデータを取得するクエリを実行します。次に、結果をフィルタリングしてイベントのサブセットを取得し、その中の1つのイベントを再構築または分析し、別のイベントに対しても再構築または分析の処理を繰り返します。標準提供のプロファイル、メタ グループ、列グループは、適切な開始点となります。たとえば、RSA Email Analysisプロファイルを選択して、メールのリスクを調査するときに役立つメタデータのみを表示することができます。
- 詳細な確認が必要なイベントを見つけた場合、イベントに関連するコンテキストを表示し、インシデントを作成するか、既存のインシデントに追加するかを決定します。イベントをインシデントに追加しない場合は、さらに洞察を進めるため、別のクエリを実行します。つまり、再度ワークフローの先頭から開始します。
- ネットワーク内の特定のホストでの疑わしいアクティビティまたはファイルに気付いた場合は、[ホスト]ビューと[ファイル]ビューまたはスタンドアロンNetWitness Endpoint Serverで、ホストとそのホストで見つかったファイルに関する追加情報を収集できます。
- マルウェアを含む可能性があるファイルまたはイベントを見つけた場合は、ファイルのマルウェア分析スキャンを実行するか、[マルウェア分析]ビューを開いてイベントが見つかったサービスのスキャンを開始することができます。

シンプルなユースケースを1つ示します。たとえば、外国との不審なトラフィックを危惧する場合、Destination Countryメタ キーを確認することにより、実際のすべての宛先と通信の頻度を明らかにすることができます。これらの値を掘り下げていくと、送信元と宛先のIPアドレスなど、トラフィックの特性が分かります。他のメタ データを調べると、この2つのIPアドレス間で交換されているファイルの特性を明らかにできる場合があります。疑わしいIPアドレスを特定したら、時間範囲を広げて[ナビゲート]ビューまたは[イベント]ビューでそのアドレスを調べ、調査対象のイベントの前後に起きた手がかりを得ることができます。

もう1つのユースケースとして、特定のIPアドレスから知的財産や機密データを窃取しているネットワーク内の悪意のある内部関係者を検出するアラートを調査します。調査は、メタ値「Upload without change request followed by download alert」から開始します。[ナビゲート]ビューを開き、アラートが生成された時間範囲で、IPアドレスの値でデータをフィルタリングします。[ナビゲート]ビューのAlertsメタデータには、リスク インジケータがメタ値として表示されます。異なるメタ値をクリックして、イベントを再構築することができます。次にファイルを抽出し、ファイルを調べて何が起きたかを理解します。この情報を元に、時間範囲を広げて、同じIPアドレスのデータをフィルタリングし、イベントの前後のアクティビティを表示することができます。

[対応]ビューのインシデントとアラートに焦点を当てた調査

[対応]ビューで、インシデントまたはアラートを処理するアナリストは、[調査]ビュー([ナビゲート]ビュー) でインシデントを開いて、イベントまたはアラートのより深い分析を実行できます。

- 通常、インシデント対応のワークフローは[対応]ビューから始まります。このビューでインシデントを調査するアナリストは、[調査]ビューでインシデントに関するインテリジェンス情報を収集する必要があります。IPアドレスなど、インシデントまたはアラートに表示される下線付きのエンティティの上にマウス ポインタを移動し、[[調査]>[ナビゲート]に移行]アクションを選択します。[ナビゲート]ビューが開き、選択したエンティティでフィルタされたデータが表示されます。[対応]ビューから調査を開始すると、定義されたメタ キーを使用してクエリが実行され、一致するパケット、ログ、エンドポイント イベントが[ナビゲート]ビューに表示されます。
- インシデントに関連したイベントを見つけた場合は、NetWitness Respondのインシデントにイベントを追加できます。[調査]ビューで見つけたイベントから、Respondの新しいインシデントを作成することもできます。
- Respondの[インシデントの詳細]ビューの[インジケータ]パネルから、「イベント」ビューを開いて、インジケータのイベントをよりよく理解することができます。

NetWitness Investigate[調査]ビュー

このセクションでは、[ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビューの簡単な説明と例を示します。また、検出したデータに関して追加のコンテキスト情報を提供する[コンテキスト ルックアップ]パネル、[イベントの再構築]ビューについても説明します。

他の[調査]ビューの詳細については、次のガイドを参照してください。

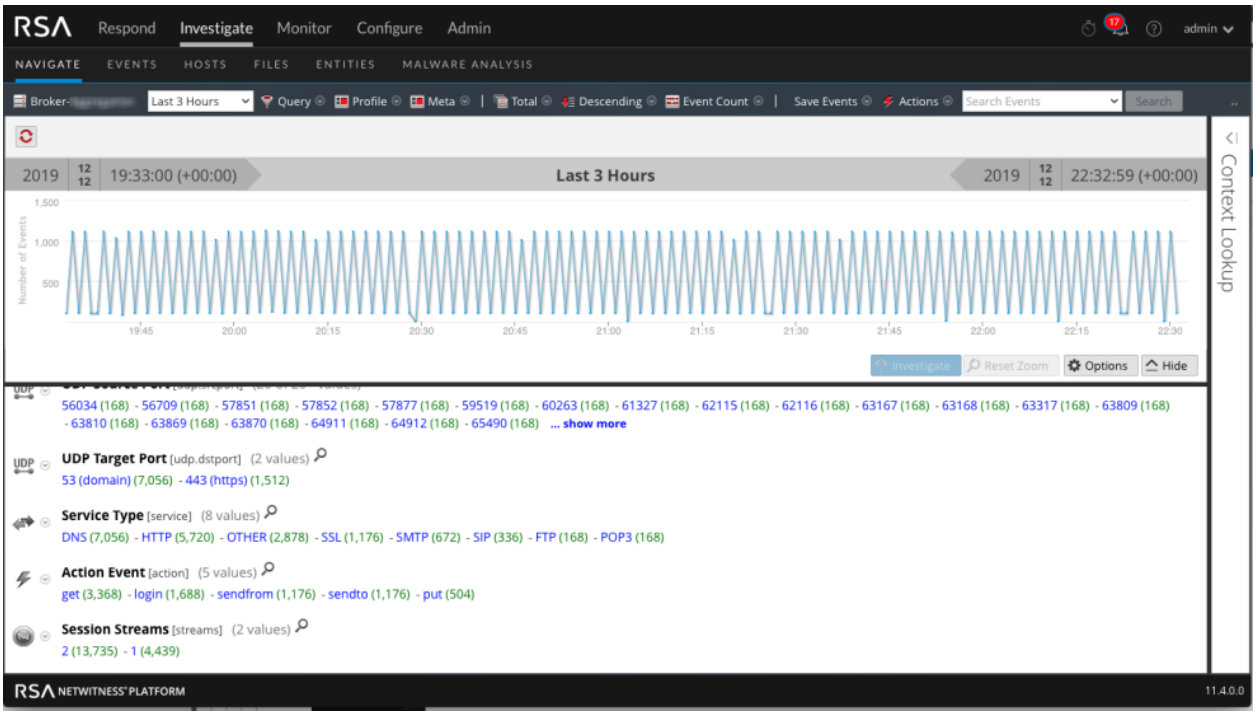
- 『*NetWitness Endpointユーザ ガイド*』では、[ホスト]ビューと[ファイル]ビューの機能について説明します。
- 『*NetWitness UEBAユーザ ガイド*』では、[エンティティ]ビュー(以前の[ユーザ]ビュー) の機能について説明します。
- 『*Malware Analysisユーザ ガイド*』では、[マルウェア分析]ビューの機能について説明します。

[ナビゲート]ビュー

[ナビゲート]ビューでは、Broker、Concentrator、Decoder上にある収集されたパケット、ログ、エンドポイント イベントのコンテンツにドリル ダウンし、クエリを実行する機能を提供します(ただし、Decoderに対する調査は一般的ではありません) 。

- サービスと時間範囲を選択すると、そのサービスから指定されたメタ キーがクエリされ、メタ値とイベント数が返されます。1つの値をクリックすると、その他の値が除外され、より絞り込んだデータ セットが表示されます。この操作を、データのドリルダウンと呼びます。
- IPアドレスやホスト名などの特定の構成済みメタ キーの場合は、Context Hubを使用して値に関する追加のコンテキスト情報を表示できます。追加のコンテキストには、インシデント、アラート、値が記載されたその他のソースが含まれます。この追加のコンテキスト情報は、元のデータとは別の情報源から取得され、アナリストがイベントを広い視点でとらえることを可能にします。コンテキスト情報の例として、関連するインシデントとアラートは、このイベントまたは同様のイベントが以前に確認または処理されたかどうかを伝えます。メタデータと一致するリストは、そのメタデータが既知の攻撃者のブラックリストに存在しないか、別のアナリストが発見した典型的な利用規約違反ユーザのリストに存在しないかを判別するのに役立ちます。
- [ナビゲート]ビューでは、データを時系列にビジュアル化して表示することもできます。期間を選択してズーム インで表示できます。

次の図は、[ナビゲート]ビューを示しています。

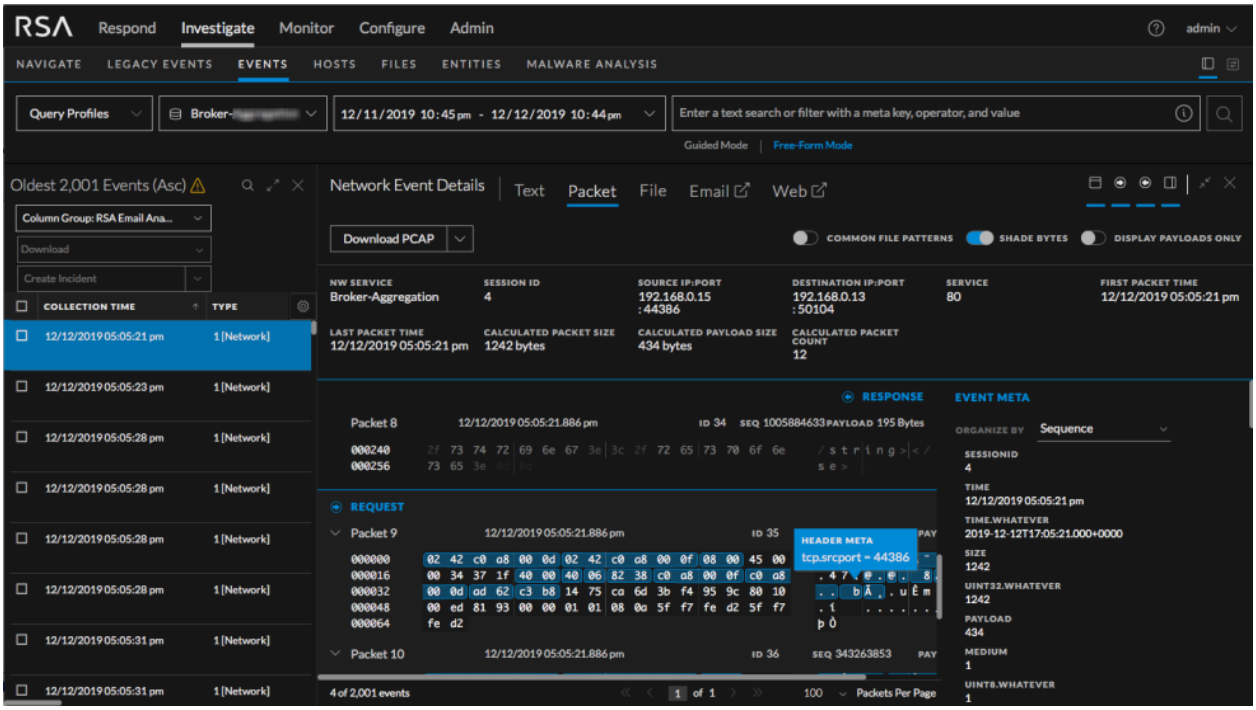


[イベント]ビュー

イベントをインタラクティブに操作するアナリストのデフォルトのワークフローは、できるだけビューを切り替える必要がないよう最適化されています。以前は[イベント分析]ビューと[イベント]ビューという2つの異なるワークフローで提供していた機能を組み合わせることにより(詳細はこのドキュメント内でさらに説明) 、アナリストは単一のワークフローでイベントを分析できるようになりました。以前のワークフローは、デフォルトでは[調査]メニューに表示されませんが、既存のアナリストのために移行期間を設ける必要がある場合は、管理者が再度有効にすることができます。イベントが時系列で表示されます。

- [イベント]リストには、イベントのRAWデータが表示されます。ここでは、ソートやフィルタリングを行うことができます。列グループを適用して、ビューに表示する列と列の配置を制御することもできます。クエリプロファイルを使用して、標準提供またはカスタムの列グループとプレクエリをこのビューに適用できます。
- [イベント]リストの結果に関連するメタデータは、[イベント メタ]パネルに表示されます。メタデータを確認するアナリストは、メタデータの表示順序を変更して、目的のメタデータをより的確に追跡することができます。メタデータのリストは、必要に応じて、出現した順やアルファベット順に並べ替えることができます。
- イベントをクリックすると、そのイベントの再構築が開きます。[イベント]ビューでは、着目点(着目すべきバイト、ファイル タイプ、エンコード データなど)の特定に役立つヒントとともに、パケット、テキスト、ファイル、メールなどのさまざまな再構築を表示できます。バージョン11.4.1の[イベント]ビューには、[メール]パネルが追加されました。以前のバージョンでは、メールの再構築は[レガシー イベント]ビューで開きます。Webの再構築は、引き続き[レガシー イベント]ビューのウィンドウで開きます。
- IPアドレスやホスト名などの特定の構成済みメタ キーの場合は、Context Hubを使用して値に関する追加のコンテキスト情報を検索できます。追加のコンテキストには、インシデント、アラート、値が記載されたその他のソースが含まれます。
- スタンドアロンEndpoint Serverへの移動、Liveでの検索、その他の内部ルックアップと外部ルックアップの実行が可能です。外部ルックアップでは、調査したいメタ値をインターネット上で検索したり、IPアドレスに関連したパッシブDNS情報を特定したり、URLがブラックリストに登録されているかどうかを確認したり、他のサード パーティ製品とコンテキスト統合することができます
- [ファイル]ビューでは、ローカル ファイル システムにzipアーカイブでファイルをエクスポートできます。
- [テキスト]ビューからログをダウンロードし、[パケット]ビューからパケットをエクスポートすることができます。[イベント]リストから複数のイベントをダウンロードすることができます。

次の図は、右側のパネルにパケット再構築が開いている[イベント]ビューの例です。[イベント]リストは左側のパネルに表示されます。

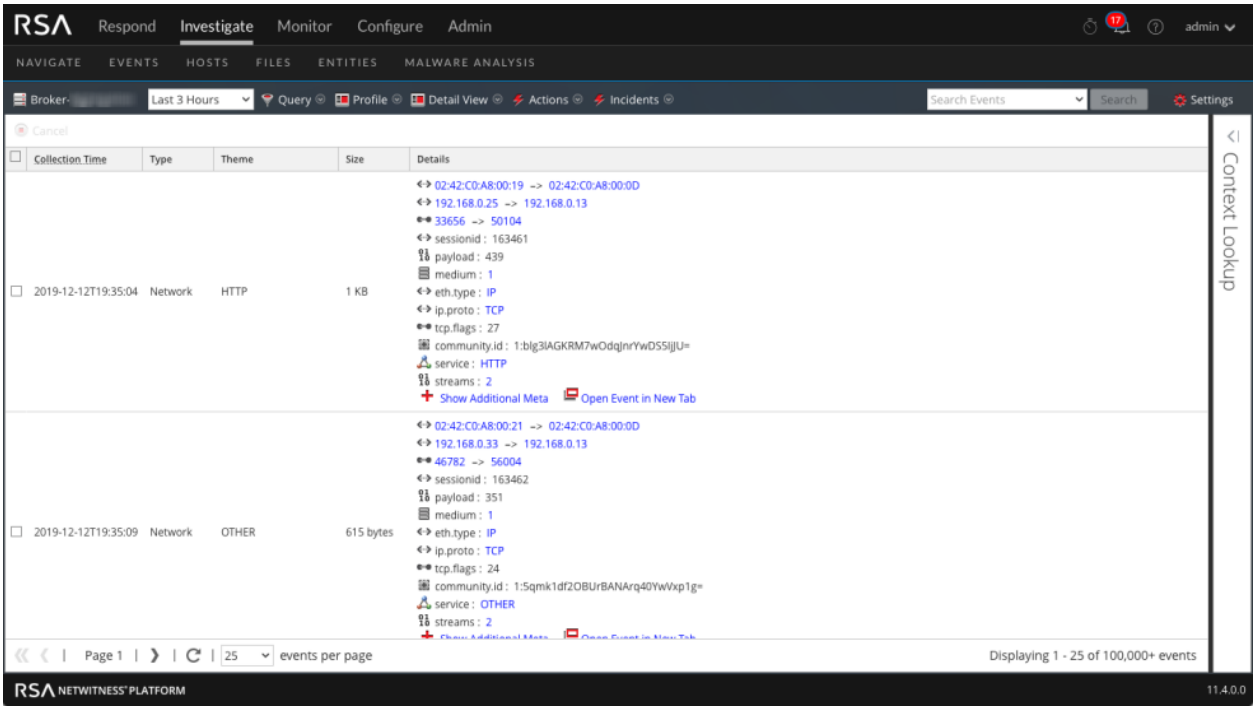


[レガシー イベント]ビュー

[レガシー イベント]ビューは、過去のバージョン(11.0～11.3.x.x) では、[イベント]ビューと呼ばれていました。[レガシー イベント]ビューは不要になり、管理者が『*システム構成ガイド*』の「調査の設定の構成」の説明に従って有効にしない限り、表示されません。[レガシー イベント]ビューには、イベントのシーケンシャル表示と安全な再構築を行えるよう、パケット、ログ、エンドポイント イベントがリスト形式で表示されます。

- [ナビゲート]ビューで表示しているメタ値の[レガシー イベント]ビューを開くことができます。
- アナリストにサービスをナビゲートするための十分な権限がない場合、[レガシー イベント]ビューを単独の[調査]ビューとして使用できます。アナリストは、最初にメタデータをドリル ダウンすることなく、NetWitness Platformコア サービスのネットワーク、ログ、エンドポイント イベントのリストにアクセスできます。
- [レガシー イベント]ビューでは、イベント情報が3つの標準形式(イベントの簡単なリスト、イベントの詳細なリスト、ログ ビュー) で表示されます。
- IPアドレスやホスト名などの特定の構成済みメタ キーの場合は、Context Hubを使用して値に関する追加のコンテキスト情報を表示できます。追加のコンテキストには、インシデント、アラート、値が記載されたその他のソースが含まれます。
- イベントや関連ファイルをエクスポートしたり、イベントからインシデントを作成することができます。

次の図は、[レガシー イベント]ビューを示しています。



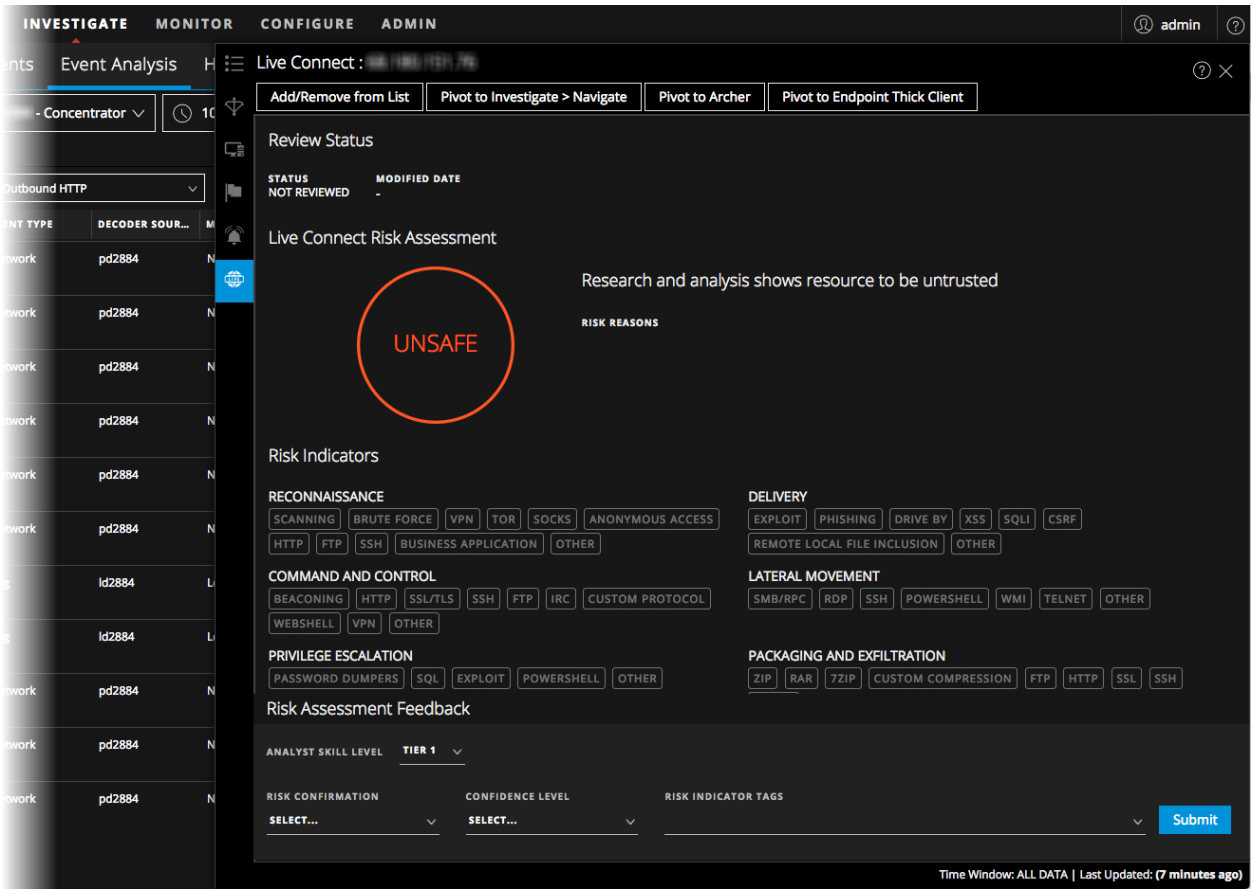
イベントのコンテキスト情報

[ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビューの[コンテキスト ルックアップ]パネルには、Context Hubに定義されたイベントの構成要素(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 ハッシュのメタ タイプ)に関する詳細情報が表示されます。さらに、時間を除くすべてのメタ キーを右クリックして、追加のコンテキストを表示することもできます。

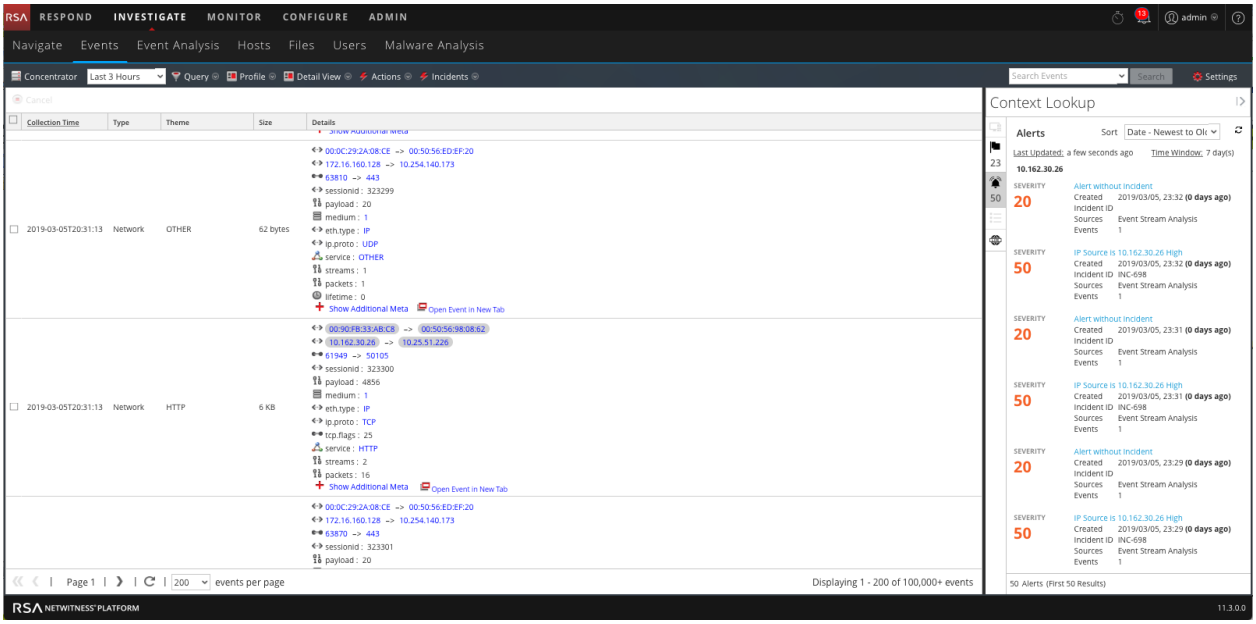
- イベントの洞察を深めるため、イベントの構成要素のデータを、関連するインシデント、アラート、カスタム リスト、Archerの資産情報、Active Directoryの詳細情報、NetWitness Endpoint IIOCなどから入手することができます。
- データ ポイントをクリックして[ナビゲート]ビューと[レガシー イベント]ビューに移動できます。

注: Archer資産情報とActive Directory詳細情報は、[イベント]ビューのコンテキスト ルックアップで使用できます。エンドポイントのコンテキスト ルックアップは、NetWitness Endpoint 4.4.0.2以降のホストで使用でき、NetWitness Endpoint 11.1以降のホストでは使用できません。

次の図は、[イベント]ビューの[コンテキスト ルックアップ]パネルを示しています。



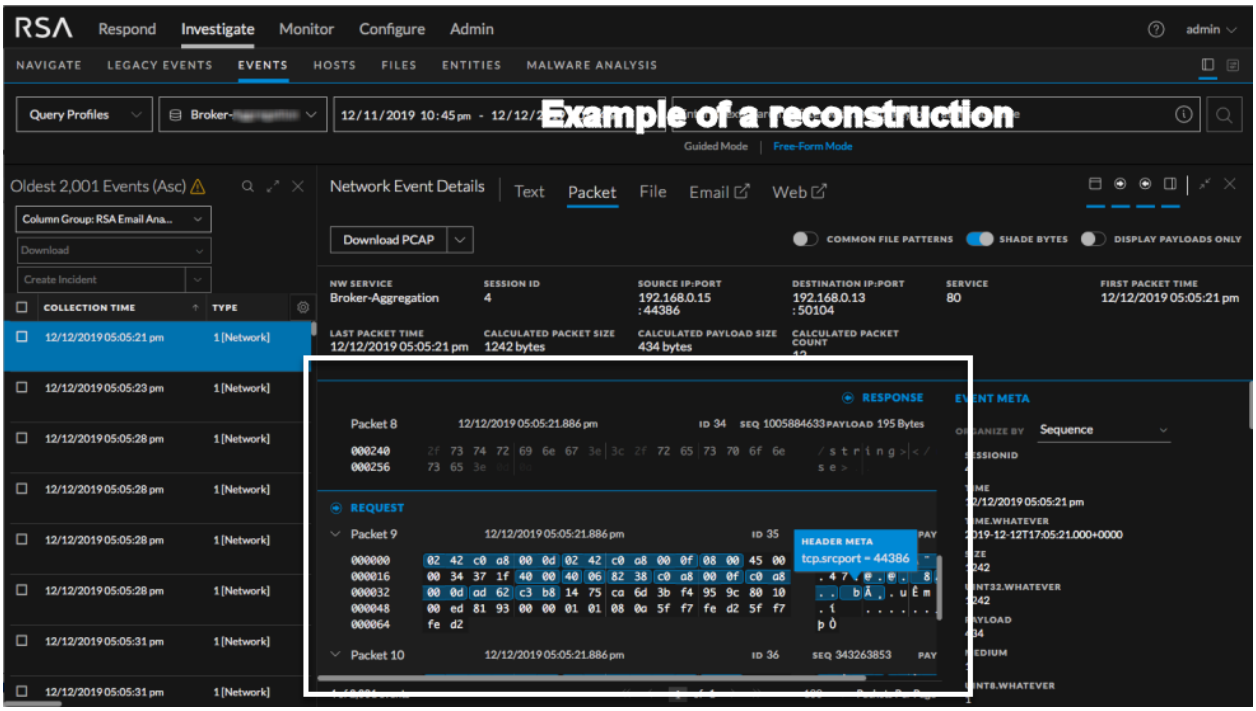
次の図は、[レガシー イベント]ビューの[コンテキスト ルックアップ]パネルを示しています。



イベント再構築

複数のビューでイベントの再構築を使用できます。さらなる調査が必要なイベントを検出した場合は、イベント本来の形式と同様の形式で安全にイベントを再構築することができます。イベントのレンダリングでは、お使いのシステムやブラウザに対する悪影響を制限するため、イベントに含まれる動的コードまたはアクティブ コードの使用は制限されます。以前に表示されたイベントを表示する場合のパフォーマンスを向上させるため、キャッシュが使用されます。各アナリストには再構築データ用に個別のキャッシュがあり、自身のキャッシュにある再構築イベントにのみアクセスできます。

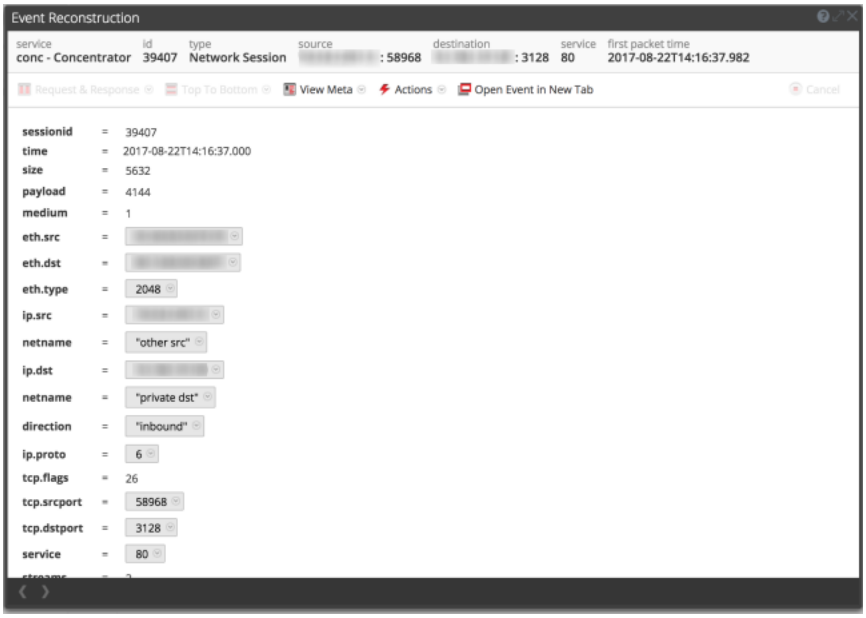
[イベント]ビューには、RAWデータ、メタ キーとメタ値を含む、対話形式のイベント再構築が表示されます。次の図は、[イベント]ビューの再構築の例です。



[イベント]ビューの再構築では、次の操作を実行できます。

- データのタイプ(メタデータ、テキスト、16進数、パケット、ファイル) に合わせてさまざまな方法でイベントを再構築します。
- ヘッダーとペイロードのハイライト表示されている情報の詳細を確認します。
- デコードおよびエンコードされたペイロードを表示し、一般的なファイル シグネチャを確認します。
- メタ キーまたはメタ値の場所を再構築の中から検索します。
- イベントとファイルをエクスポートします。

[レガシー イベント]ビューのイベント再構築には、イベントのRAWデータ、メタ キーとメタ値がリスト形式で表示されます。次の図は、イベントの再構築の例です。



[レガシー イベント]ビューの再構築では、次の操作を実行できます。

- 再構築の画面で次ページに移動すると、次のイベントの再構築が同じ形式で表示されます。

  データのタイプに合わせたさまざまな形式(メタデータ、テキスト、16進数、パケット、Web、メール、ファイル)を指定するか、もしくは、最適な形式を自動選択して、イベントを再構築します。

- パケット キャプチャ ファイルをエクスポートしたり、ファイルを抽出したり、イベントのメタ値をエクスポートします。

NetWitnessの[調査]ビューおよび環境設定の構成

アナリストは、NetWitnessの[調査]ビューと動作を構成できます。[調査]ビューの外観や表示される情報のタイプ、結果表示やイベント再構築のパフォーマンスに影響する要素はカスタマイズすることができます。構成可能な設定にはいずれも、ほとんどの環境で適切に機能するデフォルト値が設定されていますが、それらの値は、アナリストが必要に応じて調整できます。

[調査]ビューを使用するアナリストのユーザ アカウントには、適切なシステム ロールと権限を付与する必要があります。管理者は『*システム セキュリティとユーザ管理ガイド*』の説明に従って、ロールと権限を設定する必要があります。

次のトピックで、詳細を説明しています:

- [ナビゲート]ビューおよび[レガシー イベント]ビューの構成
- [イベント]ビューの構成

[ナビゲート]ビューおよび[レガシー イベント]ビューの構成

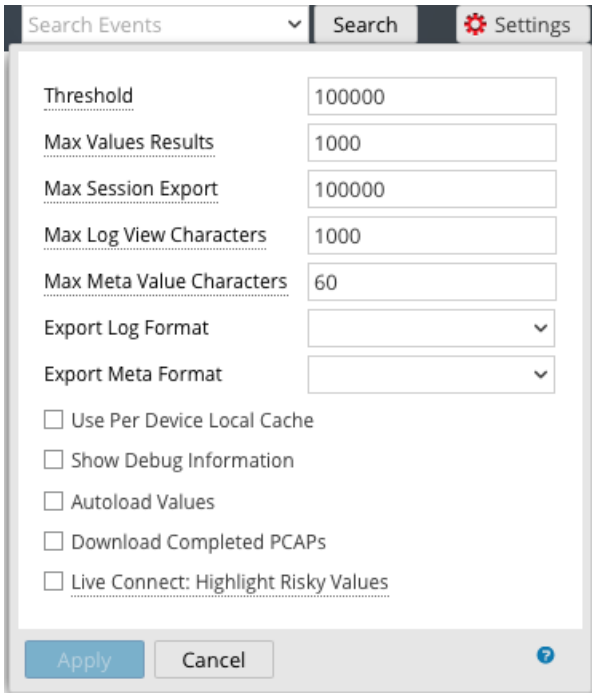
アナリストは、[ナビゲート]ビューと[レガシー イベント]ビューを使用する際の、NetWitness Platformのパフォーマンスや動作に影響する環境設定を変更できます。これらの設定の一部はNetWitness Platform内の次の2つの場所にあり、どちらの場所で変更を行っても、もう一方のビューに変更が適用されるようになっています。

- [ナビゲート]ビューおよび[レガシー イベント]ビューにある[調査]ビュー> [設定]ダイアログ。
- [プロファイル] > [環境設定]パネル> [調査]タブ。
- [ナビゲート]ビューと[レガシー イベント]ビューの[検索オプション]ドロップダウン。

[ナビゲート]ビューと[レガシー イベント]ビューの[設定]へのアクセス

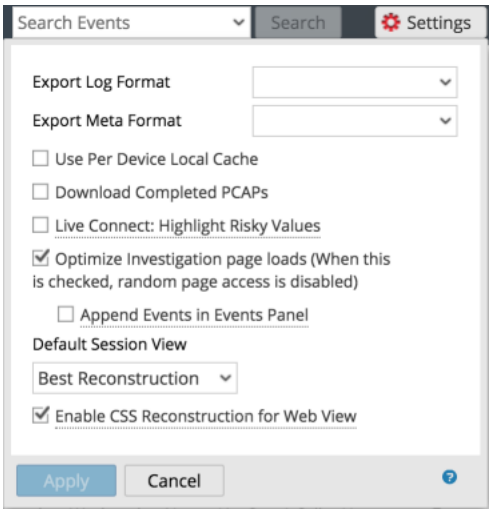
設定にアクセスするには、次のいずれかを実行します。

- [**ナビゲート**]ビューのツールバーで、[**設定**]オプションを選択します。
  [ナビゲート]ビューの[設定]ダイアログが表示されます。



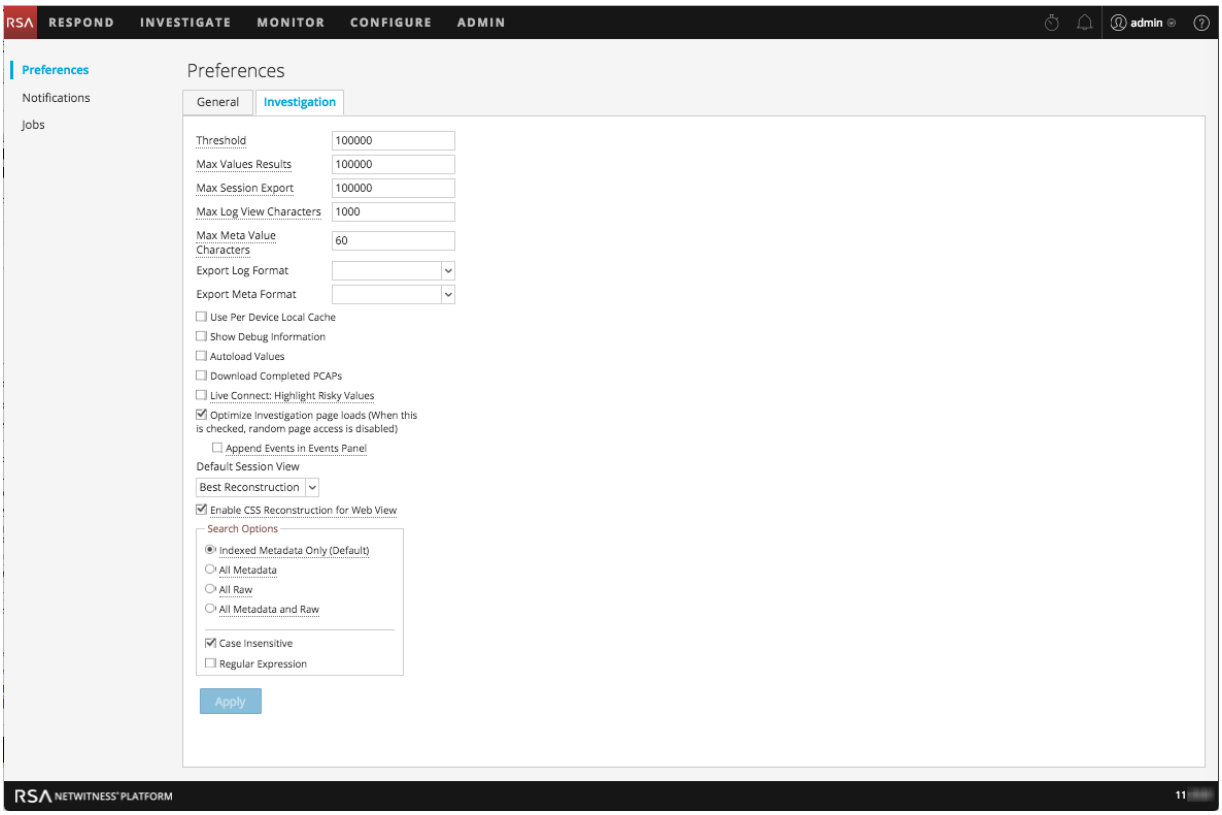
注: バージョン11.0で追加された[イベント パネルのイベントを挿入モードで表示]オプションの設定は、バージョン11.1では[レガシー イベント]ビューの[設定]パネルに移動しました。

- [**レガシー イベント**]ビューのツールバーで、[**設定**]オプションを選択します。
  [レガシー イベント]ビューの[設定]ダイアログが表示されます。



注： バージョン11.1以降、[イベント パネルのイベントを挿入モードで表示]オプションの設定が追加されました。

- NetWitness Platformの右上で、 > [Profile]に移動し、[**環境設定**]パネルの[**調査**]タブをクリックします。
[調査]パネルが表示されます。次の図は、[調査]パネルを示しています。



[ナビゲート]ビューでの値のロード パラメータの調整

いくつかの設定は、[値]パネルで値をロードする際のNetWitness Platformのパフォーマンスに影響します。デフォルト値は一般的な使用方法に基づいて設定されているため、アナリストはこれらの設定を自分の調査内容に合わせて調整できます。これらの設定を調整するには、次の手順を実行します。

1. [**環境設定**]パネル>[**調査**]タブに移動するか、[ナビゲート]ビューの[**設定**]ダイアログに移動します。
2. 次のパラメータを調整します。
   - **閾値**:[値]パネルでメタ キー値にロードするセッションの最大数の閾値を設定します。閾値を高くすると、値が正確にカウントされますが、その分ロード時間が長くなります。デフォルト値は**100000**です。
   - **結果の最大数**:[ナビゲート]ビューで開いているメタ キーについて、[メタ キー]メニューで[最大まで表示]オプションを選択した場合にロードする値の最大数を設定します。デフォルト値は**1000**です。
   - **最大セッション エクスポート**:単一のPCAPファイルまたはログ ファイルにエクスポートできるイベントの数を指定します。
   - **ログ ビューの最大文字数**:[**調査**]>[**イベント**]>[**ログ テキスト**]に表示する最大文字数を設定します。デフォルト値は**1000**です。
   - **メタ値の最大文字数**:[ナビゲート]ビューの[値]パネルに表示されるメタ値名の最大文字数を設定します。デフォルト値は**60**です。
   - **デバッグ情報の表示**:NetWitness Platformの[ナビゲート]ビューの階層リンクの下に、`where`句と、Brokerで集計した各サービスのロード時間を表示する場合は、このチェックボックスをオンにします。デフォルト値は**オフ**です。
   - **イベント パネルのイベントを挿入モードで表示**:このオプションは[レガシー イベント]ビューのページングに影響します。詳細については、「[レガシー イベント]ビューでの取得とデフォルトの再構築の調整」で説明します。
   - **値の自動ロード**:NetWitness Platformの[ナビゲート]ビューで選択したサービスから値を自動的にロードする場合は、このオプションをオンにします。このチェックボックスをオフにすると、NetWitness Platformは[**値のロード**]ボタンを表示し、ロード前にオプションを変更する機会を提供します。デフォルト値は**オフ**です。
3. [**適用**]をクリックします。
   設定はすぐに反映され、次に値をロードしたときに表示されます。

[ナビゲート]ビューおよび[レガシー イベント]ビューのパラメータの構成

いくつかの設定は、NetWitness Platformが[ナビゲート]ビューと[レガシー イベント]ビューに値をロードするパフォーマンスに影響します。デフォルト値は一般的な使用方法に基づいて設定されているため、アナリストはこれらの設定を自分の調査内容に合わせて調整できます。[ナビゲート]ビューと[レガシー イベント]ビューでこれらのパラメータを別々に設定できます。1つのビューで構成された設定が自動的にもう1つのビューに適用されることはありません。これらの設定を調整するには、次の手順を実行します。

1. [**環境設定**]パネル>[**調査**]タブに移動するか、[ナビゲート]ビューまたは[レガシー イベント]ビューの[**設定**]ダイアログに移動します。
2. 次のパラメータを調整します。
   - **Live Connect:リスクのある値を強調表示**:NetWitness PlatformでRSAコミュニティにより高リスクと見なされるIPアドレスのみを強調表示する場合は、このオプションをオンにします。選択しない場合、NetWitness Platformはすべての IPアドレスを表示します。このオプションはデフォルトでは**オフ**になっています。
   - **デバイスごとのローカル キャッシュを使用**:選択したサービスから取得したデータをローカル キャッシュに保存し、使用することができます。このオプションはデフォルトでは**オフ**になっています。オフにすると、最初のロード後に[調査]ビューにキャッシュされたデータを表示するのではなく、新しいクエリがデータベースに送信されます。オンにすると、ローカルにキャッシュされたデータを[調査]ビューに表示します。
   - **完了したPCAPのダウンロード**:[ナビゲート]ビューと[レガシー イベント]ビューで抽出されたPCAPのダウンロードを自動化できます。これにより、抽出されたPCAPがブラウザによりダウンロードされ、PCAPファイルのデフォルトのアプリケーション(Wiresharkなど)で開くことができます。このオプションはデフォルトでは**オフ**になっています。このオプションを有効にする場合は、PCAPを開くことができるアプリケーションがローカル ファイル システムにインストールされており、PCAPファイル形式を処理するデフォルトのアプリケーションとして設定されていることを確認します。
   - **Live Connect:リスクのある値を強調表示**:このオプションをオフにすると、Live Connectに使用可能なコンテキスト情報を持つすべてのメタ値が、[ナビゲート]ビューの[値]パネルで強調表示されます。このオプションをオンにすると、Live Connectにコンテキスト情報を持つメタ値のうち、コミュニティによって高リスク/不審である/安全でないと判断された値のみが強調表示されます。デフォルトでは、このオプションはチェックが外れています(**オフ**)。
3. [**適用**]をクリックします。
   設定はすぐに反映されます。

デフォルトのログ エクスポート形式の構成

[ナビゲート]ビューと[レガシー イベント]ビューでは、テキスト、XML、カンマ区切り値(CSV)、JSONの各形式でログをエクスポートできます。ログ エクスポート形式のデフォルト設定はありません。ここで形式を選択しない場合、ログのエクスポートを実行するときに、NetWitness Platformが選択のダイアログを表示します。ログのエクスポート形式を選択するには、次の手順を実行します。

1. [**環境設定**]パネル>[**調査**]タブに移動するか、[ナビゲート]ビューまたは[レガシー イベント]ビューの[**設定**]ダイアログに移動します。
2. [**ログのエクスポート形式**]ドロップダウン メニューからオプションを1つ選択します。
3. [**適用**]をクリックします。
   設定がすぐに反映されます。

デフォルトのメタ値エクスポート形式の構成

[ナビゲート]ビューと[レガシー イベント]ビューでは、テキスト、CSV、タブ区切り値(TSV)、JSONの形式でメタ値をエクスポートできます。メタ値エクスポート形式のデフォルト設定はありません。ここで形式を選択しない場合、メタ値のエクスポートを実行するときに、NetWitness Platformが選択のダイアログを表示します。メタ値のエクスポート形式を選択するには、次の手順を実行します。

1. [**環境設定**]パネル>[**調査**]タブに移動するか、[ナビゲート]ビューまたは[レガシー イベント]ビューの[**設定**]ダイアログに移動します。
2. [**メタの エクスポート形式**]ドロップダウン メニューからオプションを1つ選択します。
3. [**適用**]をクリックします。
   設定がすぐに反映されます。

[レガシー イベント]ビューでの取得とデフォルトの再構築の調整

[レガシー イベント]ビューでNetWitness Platformがイベントを取得する方法と、再構築する方法を制御するパラメータをいくつか構成できます。これらのパラメータを調整するには、次の手順を実行します。

1. [**環境設定**]パネル>[**調査**]タブに移動するか、[レガシー イベント]ビューの[**設定**]ダイアログに移動します。
2. 次のパラメータを構成します。
   - **調査ページのロードの最適化**: ページング オプションを設定します。最適化した場合、可能な限り高速に結果が返されますが、イベント リストのページ移動機能が無効になります。このボックスをオフにすると、イベント リストのページ移動機能が有効になり、リストの特定のページ(または最後のページ)に移動できるようになります。デフォルト値は[**有効**]です。
   - **デフォルト セッション表示**: [レガシー イベント]ビューでのデフォルトの再構築のタイプを選択します。デフォルト値は[**最適な表示**]で、イベントに最も適した表示方法でイベントが表示されます。
3. [**環境設定**]パネル>[**調査**]タブに移動するか、[ナビゲート]ビュー(11.1)または[レガシー イベント]ビュー(11.2以降)の[**設定**]ダイアログに移動して、[**イベント パネルのイベントを挿入モードで表示**]オプションを設定します。このオプションを選択すると、[イベント]パネルに表示されるイベントは段階的に追加されます。たとえば、次のページ アイコンをクリックするたびに、イベントの次の増分が追加されていき、最初は1～25で、次が1～50、その次が1～75などのように増えてきます。このオプションは、[**調査ページのロードの最適化**]オプションが有効な場合にのみ使用できます。
4. 変更をすぐに有効にするには、[**適用**]をクリックします。

Webコンテンツ再構築でのカスケーディング スタイル シート表示の有効化または無効化

アナリストは、Webコンテンツ再構築の際のCSS(カスケーディング スタイル シート) の使用を有効化できます。有効化すると、Webの再構築にCSSスタイルとイメージが含まれるようになり、再構築の表示と元のWebブラウザの表示が一致するようになります。これには、関連するイベントのスキャンと再構築、ターゲット イベントで使用されるスタイル シートとイメージの検索が含まれます。このオプションは、デフォルトで有効化されています。特定のWebサイトの表示に問題がある場合は、このオプションを無効化してください。

注: 関連するイメージとスタイル シートが見つからないか、Webブラウザのキャッシュからロードされた場合は、再構築されたコンテンツの見た目が元のWebページと完全には一致しない可能性があります。また、セキュリティ上の理由から、クライアント側のすべてのjavascriptが削除されるため、クライアント側のjavascriptにより動的に実行されるレイアウトまたはスタイルは、再構築では表示されません。

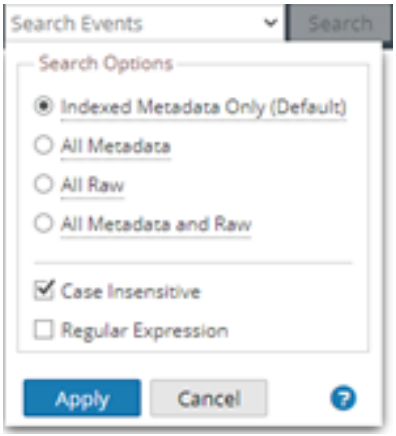
このオプションを有効化または無効化するには、次の手順を実行します。

1. [**環境設定**] パネル > [**調査**] タブに移動します。
2. [**WebビューのCSS再構築を有効化**] チェックボックスをオンにします。
3. [**適用**] をクリックします。
   設定がただちに有効になり、次のWebコンテンツ再構築時に表示されます。

検索オプションの構成

[検索] フィールドに検索文字列を入力するときに適用される検索オプションを構成することができます。[プロファイル] > [環境設定] パネル > [調査] タブ、または [ナビゲート] および [レガシー イベント] ビューの [検索オプション] ドロップダウン メニューで検索オプションを編集します。検索オプションの構成には、次の手順を実行します。

1. 検索オプションに移動します。
   次の図は、バージョン11.2以降の [検索オプション] ドロップダウン メニューを示しています。



2. 検索に適用するオプションを選択します。各オプションの詳細については、「[ナビゲート] ビューと [レガシー イベント] ビューでのテキスト パターンの検索」を参照してください。

3. 検索オプションの設定を保存するには、[**適用**]をクリックします。
   環境設定が保存され、ただちに有効になります。

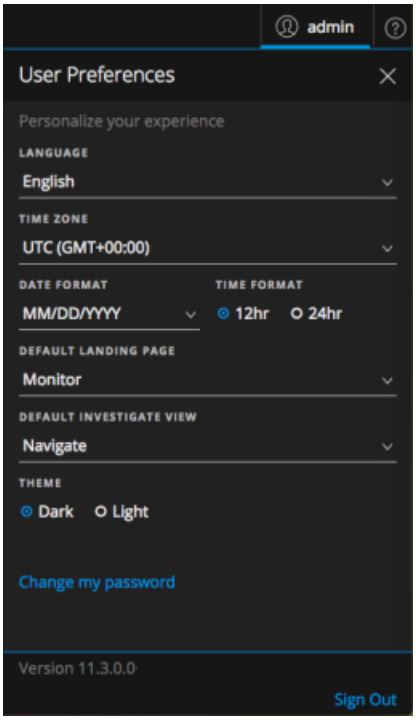
[イベント]ビューの構成

注: このトピックに記載されている情報はRSA NetWitness® Platform バージョン11.1以降に適用されます。

アナリストは、[調査]>[イベント]ビューを使用する際の、NetWitness Platformの動作に影響する環境設定を変更できます。[イベント]ビューを開いている場合は、  とという2つのボタンから、[環境設定]ダイアログにアクセスできます。[ユーザ]メニュー() はタイム ゾーンなどのグローバルなユーザ環境設定が中心であるのに対して、[イベント環境設定]メニュー() は[イベント]ビューの動作に関するユーザ環境設定が中心です。このセクションの後半では、両方の環境設定について説明します。

デフォルトの[調査]ビューの設定

[調査]ビューを開いたときに表示されるデフォルトのビューを、[ナビゲート]ビュー、[イベント]ビュー、[ホスト]ビュー、[ファイル]ビュー、[エンティティ]ビュー、[マルウェア分析]ビューから選択できます。デフォルトの[調査]ビューは、グローバルな[ユーザ環境設定]ダイアログ(NetWitness Platformブラウザ ウィンドウの右上にある  を選択) で設定します。
グローバルなユーザ環境設定については、『*NetWitness Platformスタート ガイド*』に詳細が記載されています。

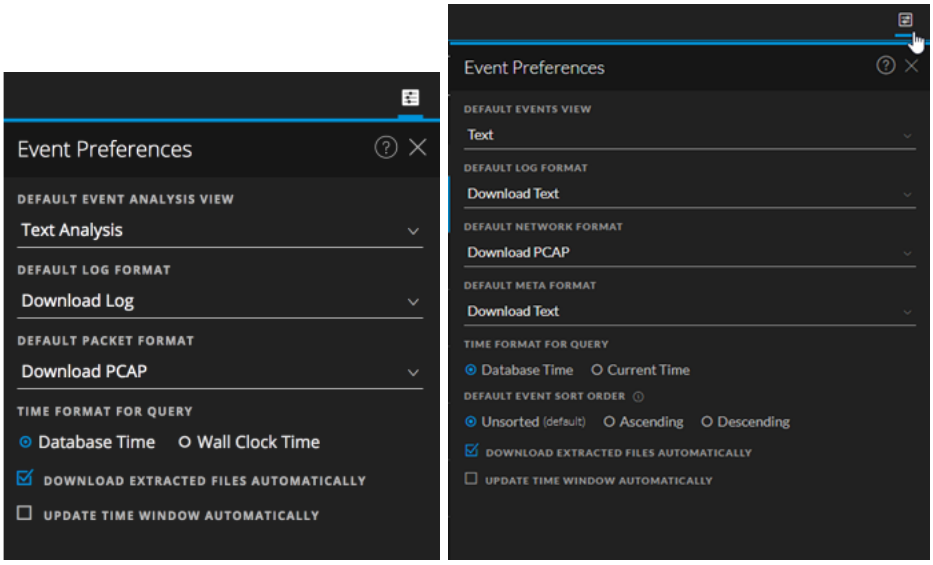


[イベント]ビューのユーザ環境設定の設定

[イベント]ビューに関連するユーザ独自の環境設定を指定できます。選択した環境設定は、ユーザ単位で管理され、特定のユーザがログインするたびに適用されます。

[イベント]ビュー使用時のデフォルト値を設定するには、次の手順を実行します。

1. [**イベント**]ビューで、をクリックします。
   [イベント環境設定]ダイアログが表示されます。次の図に示すように、バージョン11.3と11.4では、このダイアログに表示されるラベルと選択可能なオプションが異なります。最初の図はバージョン11.3のダイアログを示し、2番目の図はバージョン11.4のダイアログを示しています。



2. [**デフォルトの[イベント]ビュー**]フィールドで、[イベント]パネルでイベントを開いたときに表示するデフォルトの再構築タイプを選択します。[**テキスト**]、[**パケット**]、[**ファイル**]、[**メール**]のいずれかを選択します。
   イベントを開いたときのデフォルトの分析タイプを選択しなかった場合、デフォルトの再構築タイプはパケット分析になります。ただし、ログイベントとエンドポイント イベントの場合はテキスト分析が開きます。デフォルトの再構築タイプを選択した場合は、指定したタイプが、デフォルトの再構築タイプとして使用されます。どちらの場合も、デフォルトの再構築タイプは出発点であり、作業中にタイプを変更して、選択したタイプで再構築を表示することができます。

3. [**デフォルトのログ形式**]フィールドで、ログをエクスポートするときのダウンロード形式を選択します。[**ログのダウンロード**](11.3)または[**テキストのダウンロード**](11.4)、[**XMLのダウンロード**]、[**CSVのダウンロード**]、[**JSONのダウンロード**]のいずれかを選択します。ここで形式を選択しなかった場合、デフォルトのダウンロード形式は[**テキストのダウンロード**]です。これらのオプションは、ダウンロード時にドロップダウン メニューから選択することもできます。

4. [**デフォルトのパケット形式**](11.3)または[**デフォルトのネットワーク形式**](11.4)フィールドで、パケットをダウンロードするときのデフォルトの形式を選択します。ここで形式を選択しなかった場合、デフォルトのダウンロード形式は[**PCAPのダウンロード**]です。これらのオプションは、ダウンロード時にドロップダウン メニューから選択することもできます。

- **PCAPのダウンロード**：イベント全体をパケット キャプチャ(*.pcap) ファイルとしてダウンロードします。
- **すべてのペイロード のダウンロード**(11.3) または**ペイロード のダウンロード**(11.4) : ペイロードを*.payloadファイルとしてダウンロードします。
- **リクエスト ペイロード のダウンロード**：リクエスト ペイロードを*.payload1ファイルとしてダウンロードします。
- **レスポンス ペイロード のダウンロード**：レスポンス ペイロードを*.payload2ファイルとしてダウンロードします。

5. (バージョン11.4以降) [**デフォルト のメタ形式**] フィールドで、メタデータをエクスポートするときのダウンロード形式を選択します。[**テキスト のダウンロード**]、[**CSV のダウンロード**]、[**TSV のダウンロード**]、[**JSON のダウンロード**] のいずれかを選択します。ここで形式を選択しなかった場合、デフォルトのダウンロード形式は[**テキスト のダウンロード**] です。
6. [**クエリの時間形式**] では、[**データベースの時間**] と[**現在の時刻**](11.4) のいずれかを選択します。[イベント] ビューには、データベースの時間または現在の時刻に基づいて結果を表示できます。時間形式を設定すると、ユーザ固有の環境設定として、再度変更されるまで設定が維持されます。この環境設定のデフォルト設定は[**データベースの時間**] です。これは[ナビゲート] ビューと[レガシー イベント] ビューでクエリ結果を表示するために使用される時間形式と同じです。
   - [**データベースの時間**] を選択した場合、クエリの開始時刻と終了時刻はイベントが保存された時刻に基づきます。
   - [**現在の時刻(Current Time)**](バージョン11.3以前では[**現在の時間(Wall Clock Time)**]) を選択した場合は、ユーザ環境設定に設定されたタイムゾーンの現在の時刻に基づいてクエリが実行されます。現在の時刻は、PCAPでアップロードされるデータではなく、リアルタイムに投入される収集したデータに重点を置いています。
7. (バージョン11.4以降) [イベント] パネルに表示されるイベントを収集時間によってソートする方法を設定するには、[**デフォルト のイベント ソート順**] のいずれかのオプションを選択します。環境設定を選択した後は、テーブルの列見出しを操作して、結果を別の方法でソートすることもできます(「イベント リストでの列と列グループの使用」を参照)。
   - **ソートしない**(バージョン11.4.1のデフォルト) : コア サービスによって処理された順にイベントをリストに表示します。[ソートしない] は、すべてのコア サービスの応答を待ってから選択された順序で結果を表示するのではなく、一致が見つかり次第イベントを返すため、処理がより高速です。
   - **昇順**(バージョン11.4以前のデフォルト) : 収集時間が最も古いイベントをリストの最初に配置します。昇順の場合は、最も古いイベントが最初に表示されます。
   - **降順**：収集時間が最も新しいイベントをリストの最初に配置します。降順の場合は、最も新しいイベントが最初に表示されます。ログを調査する時には、ソート順を変更して、最も新しい収集時間のログを先頭に表示したい場合があります。

   結果がイベント数の上限を超えている場合、すべてのイベントをロードすることはできません。結果として[イベント] パネルにロードされるイベントは、ソート順の設定と一致しています。つまり、昇順が選択されている時は、イベントの最も古い方から順にロードされ、降順が選択されている時は、イベントの最も新しい方から順にロードされます。[ソートしない] を選択すると、最も古いイベントから照合され、ソートしないでリストに表示されます。
   イベントがロードされた後でソート順を変更した場合は、ビューをリフレッシュして新しいソート順を反映させる必要があります。

8. 抽出したすべてのファイルを自動的にダウンロードする場合は、[**抽出したファイルを自動ダウンロード**]チェックボックスを選択します。抽出したファイルを表示するには、ジョブ キューに移動します。
9. (バージョン11.3以降) サービスをポーリングするタイミング(1分間隔) で、クエリ バーの時間範囲を自動的に更新し、新しい時間範囲の結果を取得する場合は、[**時間範囲を自動的に更新**]チェックボックスを選択します。時間範囲が更新されたときに、  (クエリの送信) ボタンがアクティブになり、クエリを送信して最新の結果を取得できるようになります。クエリ バーの時間範囲と現在の結果の同期を維持するには、チェックボックスを選択解除(デフォルト) します。

調査の開始

どのような答えを探しているかによって、NetWitness Investigateには、[ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビュー、[ホスト]ビュー、[ファイル]ビュー、[エンティティ]ビュー、[マルウェア分析]ビューという、さまざまな開始点が用意されています。

ユーザがNetWitness Platformで調査を実行するには、特定のユーザ ロールと権限が必要です。タスクを実行できないか、ビューを表示できない場合は、管理者によりロールや権限の変更が必要となる可能性があります。

- [ホスト]ビューと[ファイル]ビューは、バージョン11.1以降で使用できます(詳細については、『*NetWitness Endpointクイック スタート ガイド*』および『*NetWitness Endpointユーザ ガイド*』を参照してください)。
- [エンティティ]ビュー(以前の[ユーザ]ビュー)は、バージョン11.2以降で使用できます(詳細については、『*NetWitness UEBAクイック スタート ガイド*』および『*NetWitness UEBAユーザ ガイド*』を参照してください)。
- 11.4の[イベント]ビューは、イベントを調査するためのデフォルトのビューです。イベントをインタラクティブに操作するアナリストのデフォルトのワークフローは、できるだけビューを切り替える必要がないよう最適化されています。以前は[イベント分析]ビューと[イベント]ビューという2つの異なるワークフローで提供していた機能を組み合わせることにより、アナリストは単一のワークフローでイベントを分析できるようになりました。[イベント]ビューに追加された新機能により、[レガシー イベント]ビューは不要になりました。デフォルトで、以前のワークフローは[調査]メニューに表示されなくなりましたが、管理者は『*システム構成ガイド*』の「調査の設定の構成」の説明に従って再度有効にすることができます。

メタデータ、RAWイベント、イベント分析にフォーカス

インシデント対応ワークフローを進めるために必要なイベントを追跡したり、別のツールがイベントを生成した後で戦略的な分析を行う場合は、**[調査]>[ナビゲート]**、**[調査]>[イベント]**、または**[調査]>[レガシー イベント]**に移動します。単一のBrokerまたはConcentratorのメタデータとRAWイベントを調査できます。これらのビューでは、クエリを実行し、時間範囲の絞り込みとメタデータの検索により、結果をフィルタリングできます。次のトピックでは、各ビューでの調査の開始について説明しています。

- [[イベント]ビューでの調査の開始]
- [[ナビゲート]ビューまたは[レガシー イベント]ビューでの調査の開始]

ホストとファイルにフォーカス

Endpointエージェントを実行しているホストの情報を探すには、**[調査]>[ホスト]**に移動します。それぞれのホストについて、実行中のプロセス、ドライバ、DLL、ファイル(実行可能ファイル)、サービス、Autorun、ログインしているユーザに関連する情報が表示されます。導入環境にあるファイルの調査を開始するには、**[調査]>[ファイル]**に移動します(詳細については、『*NetWitness Endpointユーザ ガイド*』を参照)。

高リスクのユーザおよびエンティティの振る舞いにフォーカス

ネットワーク環境のすべてのユーザとエンティティによる高リスクの振る舞いを検出、調査、監視するには、**[調査]>[エンティティ]**またはNetWitness UEBA(User and Entity Behavior Analytics) に移動します。バージョン11.3以前では、**[調査]>[ユーザ]**に移動します。悪意のあるユーザや不正ユーザの検出、リスクの高い振る舞いの特定、攻撃の発見、新たなセキュリティ脅威の調査を行うことができます (詳細については、『*NetWitness UEBAユーザ ガイド*』を参照) 。

ファイルのマルウェア スキャンにフォーカス

ファイルの潜在的なマルウェアをスキャンしたり、サービスの定期的なスキャンを設定する場合は、**[調査]>[マルウェア分析]**に移動します。スキャン結果には、ネットワーク、静的、コミュニティ、サンドボックスの4つのタイプの分析が表示され、IOC(セキュリティ侵害インジケータ) の評価も示されます。マルウェア分析は、次の方法で開始することもできます。

- [監視]ビューの[マルウェア分析]ダッシュレットからマルウェア分析を開始すると、最もリスクの高い潜在的な脅威をすばやく確認することができます。
- [ナビゲート]ビューでメタ キーを右クリックし、[**マルウェアのスキャン**]を選択できます。

詳細については、『*Malware Analysisユーザ ガイド*』を参照してください。

[ナビゲート]ビューまたは[レガシー イベント]ビューでの調査の開始

[ナビゲート]ビューは、別のビューが選択されない限り、[調査]ビューのデフォルト ビューです。このユーザ環境設定[は、アプリケーション レベルの設定です。詳細は、「NetWitnessの[調査]ビューおよび環境設定の構成」を参照してください。[ナビゲート]ビューと[レガシー イベント]ビューでは、クエリを実行して、興味のあるイベントをハンティングします。[ナビゲート]ビューでは、メタ キーとメタ値をクリックして結果を絞り込むこともできます。興味のあるイベントを発見したら、他の[調査]ビューでそのイベントをより詳しく調べることができます。

[ナビゲート]ビューまたは[レガシー イベント]ビューで調査を開始するには、サービスを指定する必要があります。

- ユーザがデフォルトのサービスを指定している場合は、そのサービスが選択された状態で[ナビゲート]ビューまたは[レガシー イベント]ビューが開きます。
- デフォルトのサービスが指定されておらず、URLにサービスIDも含まれていない場合、調査するサービスまたはコレクションを選択するダイアログが表示されます。
- サービスを手動で選択した場合も、デフォルトのサービスが指定されている場合も、[ナビゲート]ビューまたは[レガシー イベント]ビューのツールバーでサービス名をクリックして、調査するサービスまたはコレクションを変更できます。ダイアログが表示され、調査するサービスを選択できます。

注: 調査の実行時にユーザ操作のパフォーマンス低下を最小限に抑えるために、Archiverサービスは[ナビゲート]ビューに表示されません。Archiverは[レガシー イベント]ビューで使用でき、ログのエクスポートや強化された検索を実行できます。

サービスまたはコレクションを選択すると、サービスまたはコレクションからデータをロードする準備が整います。結果のロードを高速化できるよう、時間範囲も選択することをお勧めします。[ナビゲート]ビューおよび[レガシー イベント]ビューの[設定]ダイアログまたは[プロファイル]>[環境設定]パネル>[調査]タブのいくつかの設定がロード処理に影響します。このような設定には、[閾値]、[結果の最大数]、[デバッグ情報の表示]、[値の自動ロード]、[調査ページのロードを最適化]などが含まれます(「NetWitnessの[調査]ビューおよび環境設定の構成」を参照してください)。

注: [レガシー イベント]ビューでは、データが自動的にロードされます。[ナビゲート]ビューでは、環境設定で[値の自動ロード]を選択している場合、データが自動的にロードされます。それ以外の場合は、[値のロード]ボタンをクリックする必要があります。[ナビゲート]ビューの[値]パネルにメタデータがロードされ、ほぼ即時に結果が表示されます。

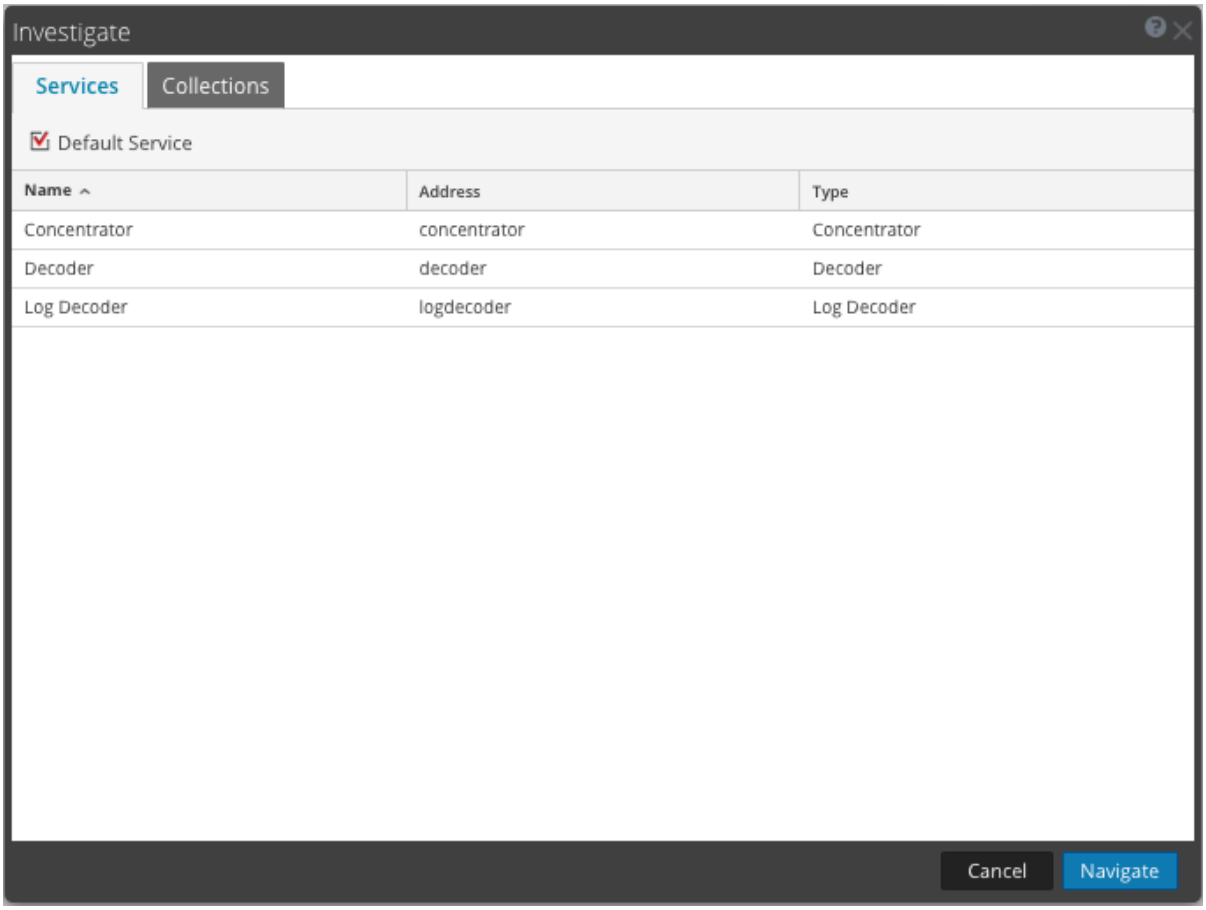
このトピックの後半では、サービスのデータの調査を開始するための手順について説明します。

注: コレクションを作成できるのは管理者ロールを持つユーザだけであり、コレクションを調査できるのはコレクションの作成者だけです。

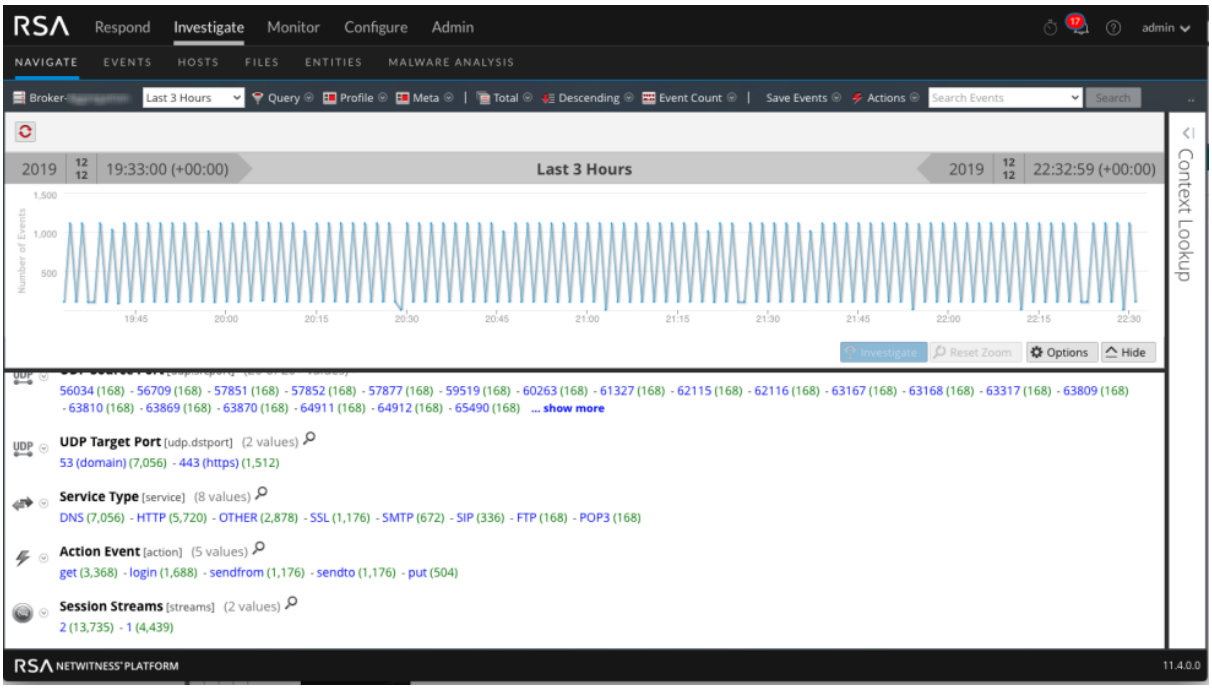
[ナビゲート]ビューまたは[レガシー イベント]ビューでデータをロードした後、結果の絞り込み、イベントの再構築と分析、結果のダウンロードと処理を行います(「結果セットの絞り込み」、「イベントの再構築と分析」、「結果のダウンロードと処理」を参照)。

調査の開始 (デフォルトのサービスが指定されていない場合)

1. **[調査]>[ナビゲート]**または[**レガシー イベント**]に移動します。
   [調査]ダイアログが表示されます。



2. サービス(通常はConcentrator)をダブルクリックするか、選択して、[**ナビゲート**]をクリックします。
   データが[レガシー イベント]ビューに自動的にロードされます。[ナビゲート]ビューでは、結果パネルに、選択したサービスのアクティビティが表示されますが、データは自動的にロードされません。
3. (推奨)結果がより速くロードされるように、特定の時間範囲を選択します。
4. データをロードする前に、調査のオプションを変更することができます。たとえば、カスタム プロファイルの作成または変更、別の時間範囲の適用、メタ グループの作成または適用、カスタム クエリの実行(詳細は「結果セットの絞り込み」を参照)などです。また、オプションは調査中にいつでも変更することができます。
5. [ナビゲート]ビューにデータをロードするには、Load Valuesをクリックします。
   選択したサービスからデータのロードが開始されます。

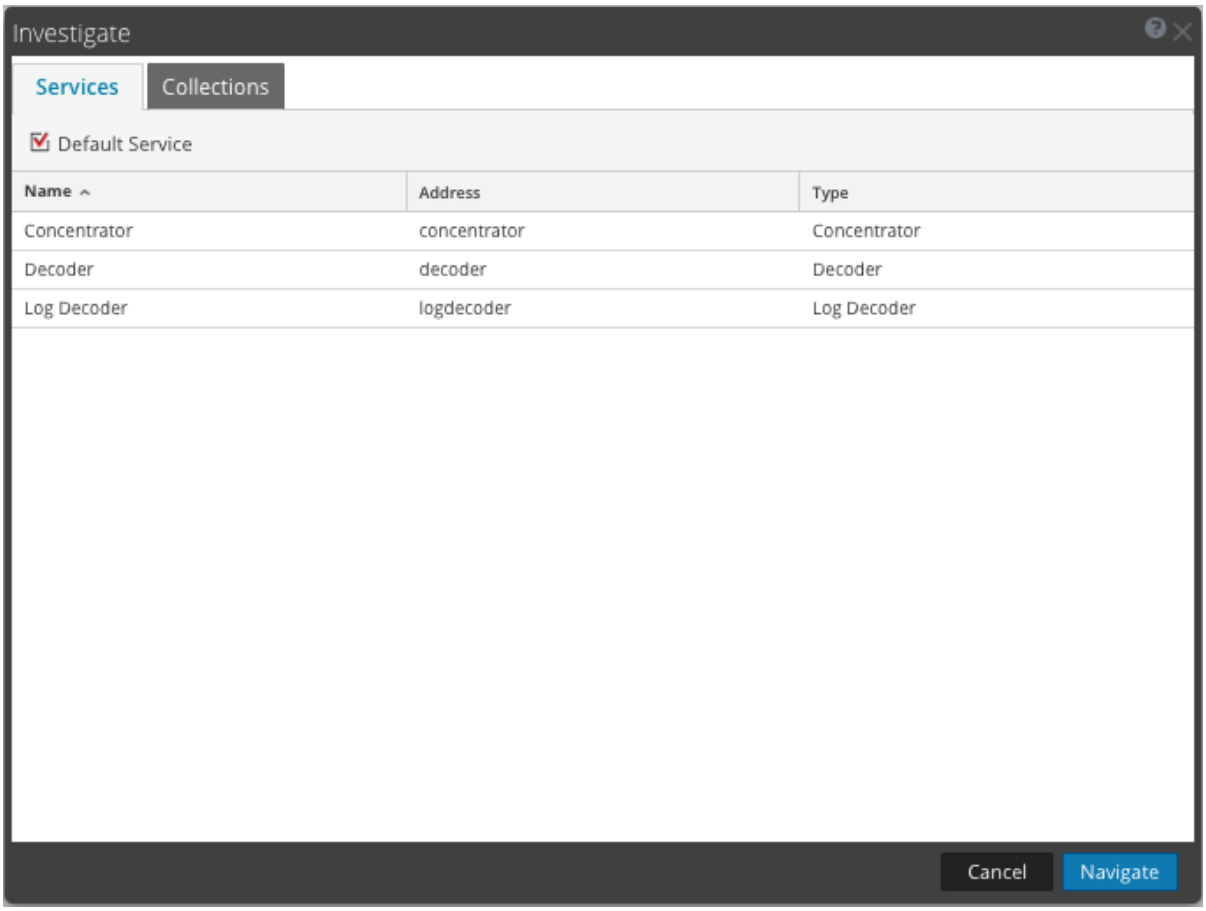


サービスを選択して、データがロードされたら、データを分析する準備が整います。

デフォルトのサービスの設定またはクリア

[調査]ダイアログで、デフォルトのサービスを設定およびクリアできます。

1. ツールバーでサービス名をクリックします。
   [調査]ダイアログが表示されます。



2. [**サービス**] グリッドでサービスを選択し、Default Service をクリックします。
このサービスがデフォルトになります(サービス名の後に括弧に囲まれて**デフォルト**と表示されます) 。
3. デフォルトのサービスの選択をクリアするには、グリッドでデフォルトのサービスを選択して、
Default Service をクリックし、[**キャンセル**] をクリックしてダイアログを閉じます。
デフォルトのサービスに設定されたサービスがない状態になります。

> **注**: [キャンセル] をクリックしても、デフォルトのサービスの選択はキャンセルされません。グリッド内で現在選択されているサービスに移動することなく、ダイアログが閉じます。現在調査中のサービスとは異なるサービスをデフォルトに設定しても、[ナビゲート] ビューは更新されません。別のサービスを明示的に選択してそのサービスに移動する必要があります。

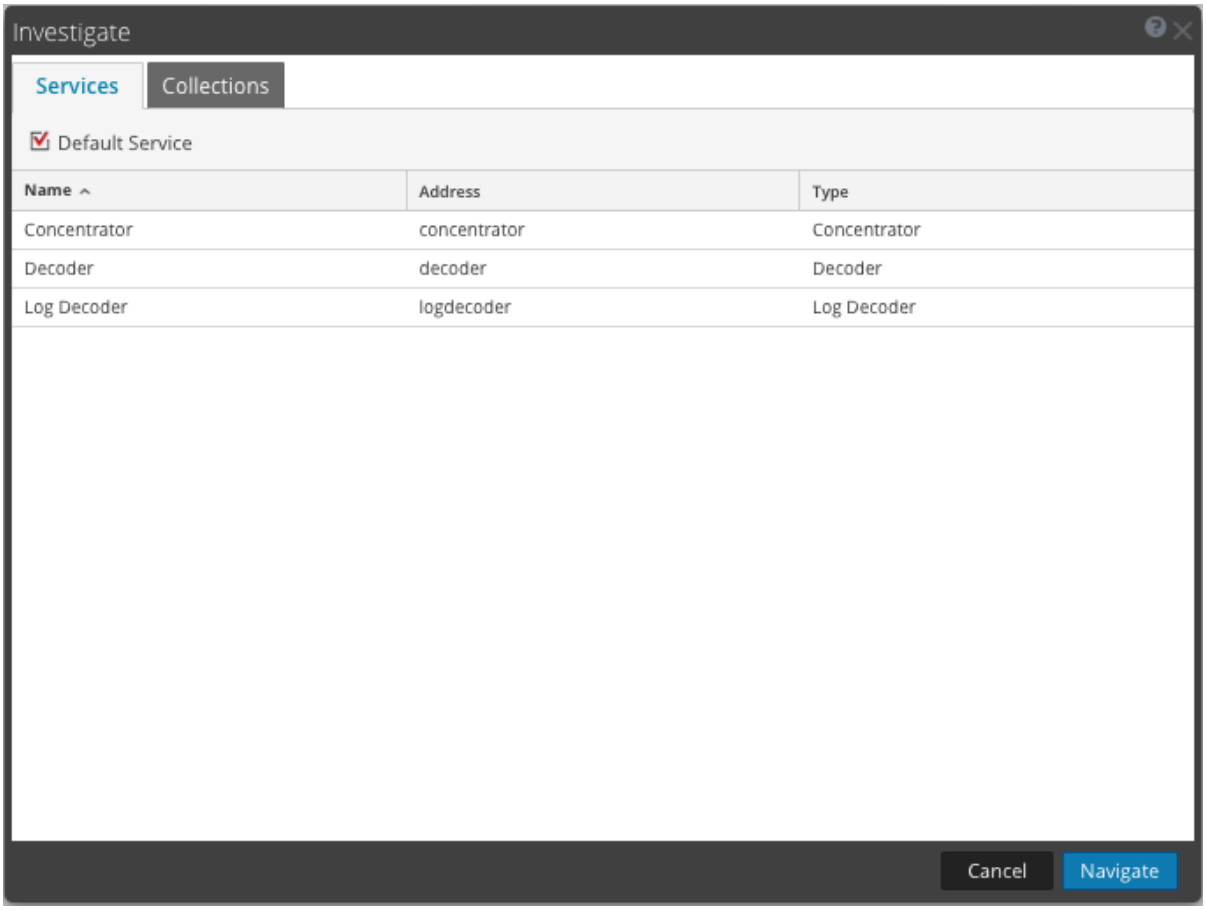
調査の開始 (デフォルトのサービスが指定されている場合)

1. **[調査] > [ナビゲート]** または **[レガシー イベント]** に移動します。
[値の自動ロード] がオフの場合、[ナビゲート] ビューが表示され、デフォルトのサービスが選択された状態になり、データをロードする準備が整います。[値の自動ロード] がオンの場合、ステップ3に示すように、値がロードされます。[レガシー イベント] ビューでは、データが自動的にロードされます。

2. データをロードする前に、[ナビゲート]ビューの調査オプションを変更することができます。たとえば、カスタム プロファイルの作成または変更、別の時間範囲の適用、メタ グループの作成または適用、カスタム クエリの実行などです。
3. 準備が完了したら、Load Valuesをクリックします。
選択したオプションに従って、サービスからデータがロードされます。サービスを選択して、データがロードされたら、データを分析する準備が整います。

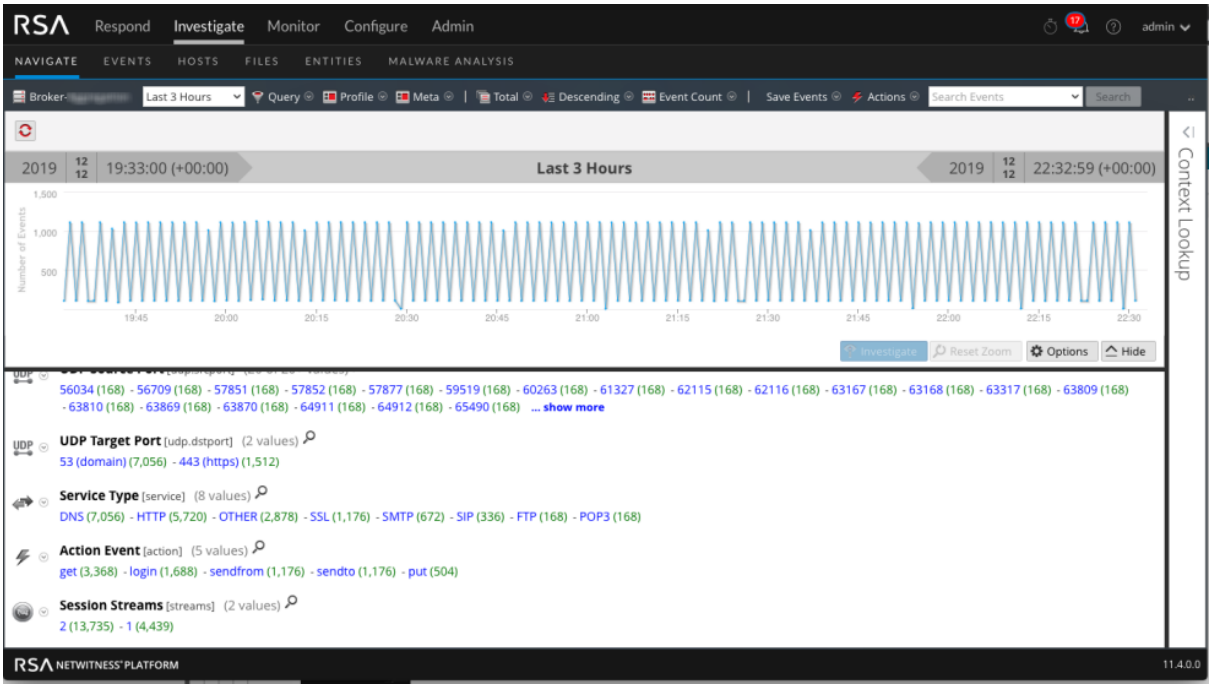
調査するサービスまたはコレクションの変更

1. [ナビゲート]ビューまたは[レガシー イベント]ビューで、オプション パネルの上部のサービス名をクリックします。
[調査]ダイアログが表示されます。



2. サービスをダブル クリックするか、またはサービスを選択して、[**ナビゲート**]をクリックします。選択したサービスからデータが結果パネルに表示されます。
[値の自動ロード]がオンの場合は、ステップ3に示すように値がロードされます。オンでない場合は[ナビゲート]ビューが表示され、デフォルトのサービスが選択された状態になり、データをロードする準備が整います。[レガシー イベント]ビューでは、データが自動的にロードされます。

3. 準備が完了したら、Load Valuesをクリックします。
   選択したオプションに従って、サービスから値のロードが開始されます。



   サービスを選択して、データがロードされたら、データを分析する準備が整います。

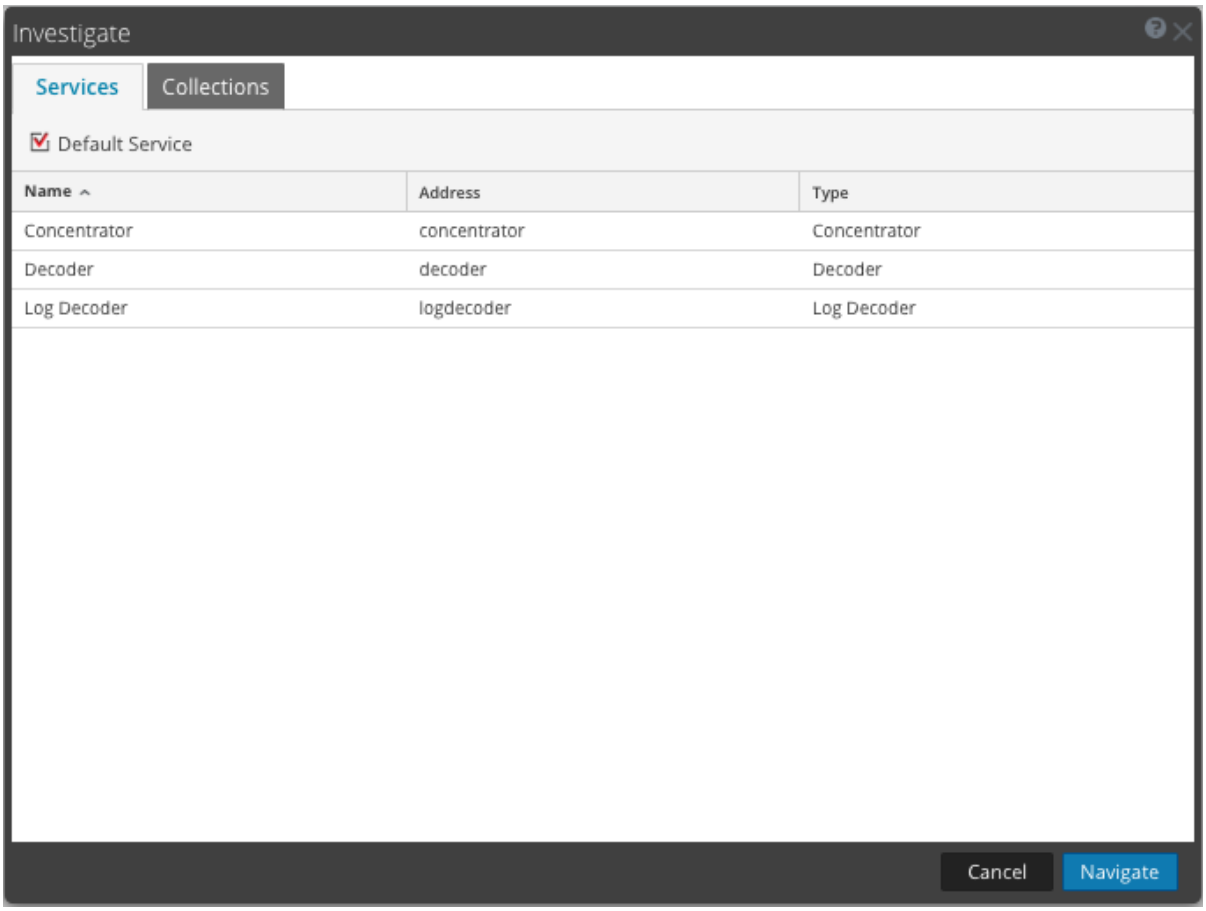
Workbenchのリストア コレクションの調査

管理者がこの手順を実行すると、既存のコレクションからコンテンツを選択して、再調査のために再度処理することができます。この手順は、Workbenchサービスを使用するDecoderに適用されます。

注： コレクションを作成できるのは管理権限を持つユーザだけです。また表示できるのは自身が作成したコレクションだけです。

再調査のためにデータを再度処理するには、次の手順を実行します。

1. [**調査**] > [**ナビゲート**]または[**レガシー イベント**]に移動します。
   [調査]ダイアログが表示されます。

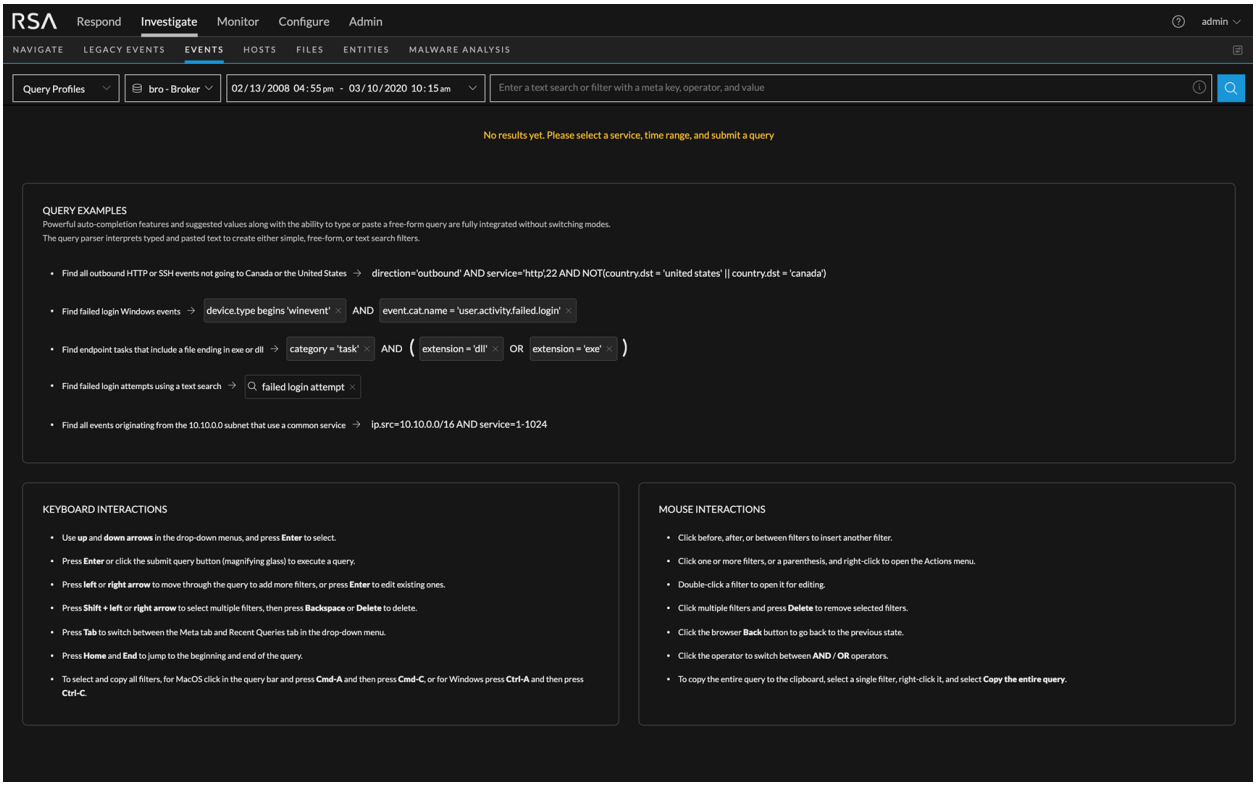


2. 調査するWorkbenchサービスとWorkbench名を選択します。
3. [**ナビゲート**]をクリックして、選択したWorkbenchサービスに対する調査を実行します。
   [**キャンセル**]をクリックして、調査する別のWorkbenchサービスを選択できます。
   [調査]ビューが表示されます。コレクションを選択して、データがロードされたら、データを分析する準備が整います。

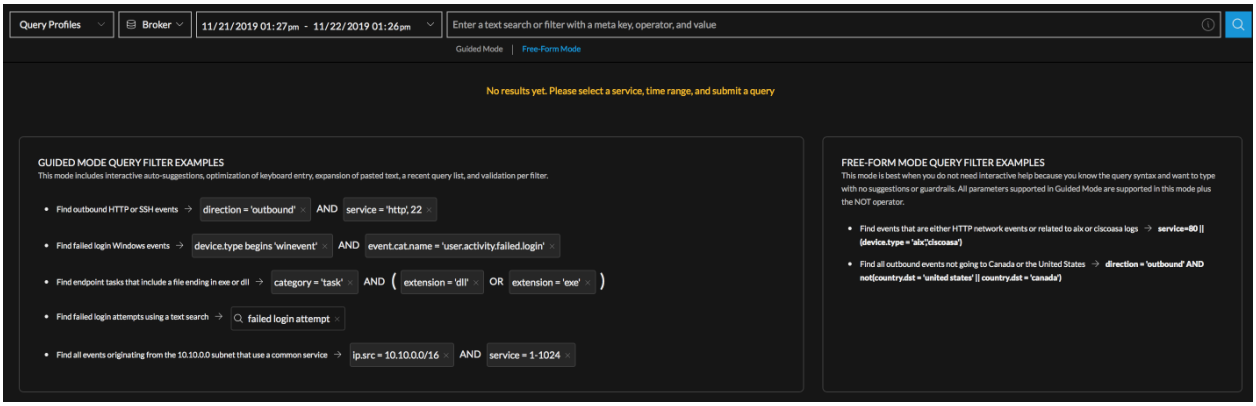
[イベント]ビューでの調査の開始

[イベント]ビューでは、[ナビゲート]ビューと[レガシー イベント]ビューの両方で使用可能な機能のほとんどが提供されます。[ナビゲート]ビューと同様に、ログ、エンドポイント、パケットのメタ キーとメタ値を表示するビューがあります。[レガシー イベント]ビューと同様に、イベント リストにイベントを時系列で表示し、RAWイベント、関連メタデータ、イベントの再構築を表示することができます。イベントの再構築では、着目点の特定に役立つヒントが表示されます。「[イベント]ビューでのイベントの分析」を参照してください。

次の図は、初期状態の[イベント]ビューを示しています。クエリの例と、キーボードとマウスの操作に関する情報が表示されています。次の図は、バージョン11.4.1の初期ビューを示しています。



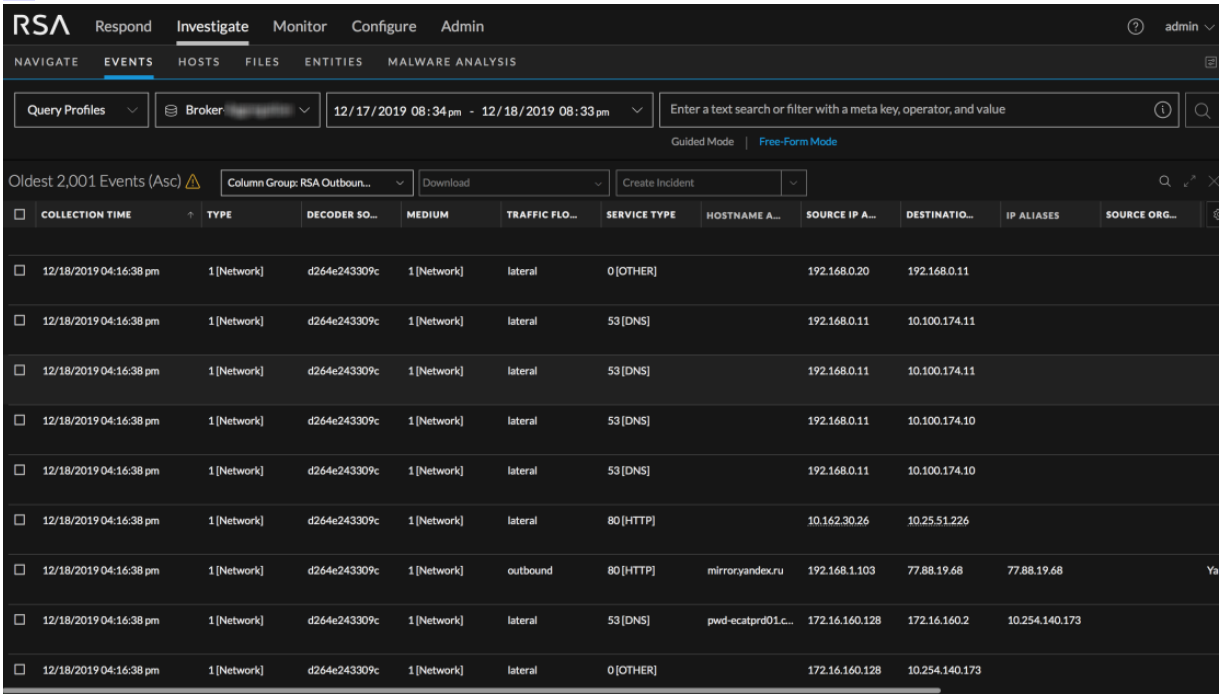
次の図は、バージョン11.4の初期ビューを示しています。11.4には、クエリを作成する2つのモードがあります。



[イベント]ビューへのアクセス

バージョン11.1以降では、いくつかの方法で[イベント]ビューにアクセスすることができます。

- **[調査]>[イベント]**に移動するか、[イベント]ビューが調査のデフォルト ビューに設定されている場合は、メイン メニューの[**調査**]オプションを選択します。詳細な手順は、後述します。
- [ナビゲート]ビューで、メタ値のカウント(メタ値の後の緑色の数字)をクリックします。[イベント]ビューが開き、選択したドリルダウン ポイントのイベントのリストが表示されます。「イベントの再構築と分析」の説明に従って分析を開始できます。
- カウントを右クリックし、[**新しいタブで[イベント]を開く**]をクリックします。新しいタブに[イベント]ビューが開き、選択したドリルダウン ポイントのイベントのリストが表示されます。「イベントの再構築と分析」の説明に従って分析を開始できます。次の図はイベント リストの例です。

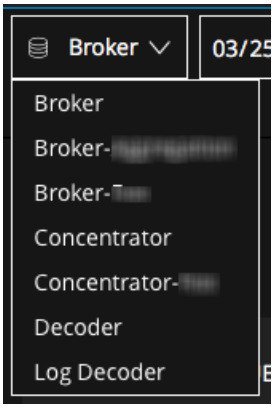


[イベント]ビューに直接アクセスして、調査を開始するには、次の手順を実行します。

1. [**調査**]>[**イベント**]に移動します。
   サービスが選択された状態で[イベント]ビューが開きます。データは表示されません。ドロップダウン リストには、アルファベット順で使用可能なサービスのリストが表示されます。[**サービスの選択**]フィールドでは、サービス リストの先頭のサービス、または最後に選択されたサービスがデフォルトで選択されます。デフォルトで、使用可能なサービスのリストは12時間ごとに取得され、NetWitness Server上にキャッシュされます。次回の取得の前にNetWitness Serverにサービスを追加または削除した場合は、キャッシュが最新のサービス リストに更新されます。アイコンにサービスのステータスが示されます。

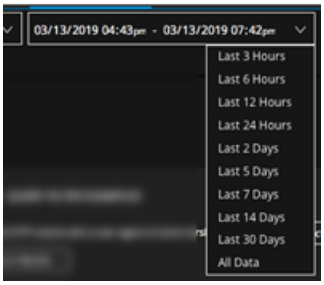
- と選択されたサービス名 = サービスが選択されています。
- = 選択されたサービスへの接続を試みています。
- = 選択したサービスへの接続中にエラーが発生したか選択したサービスにデータがありません。この状態では、サービス セレクタ コントロールも赤色に変わり、ツールチップに、接続の試行が失敗した理由と、別のサービスを選択するように勧めるメッセージが表示されます。

2. (オプション) ドロップダウン リストからサービス(通常はBrokerまたはConcentrator) を選択します。



時間範囲セレクタには、デフォルトの24時間、またはこのサービスに対して最後に選択された時間範囲が表示されます。(クエリ送信) ボタンがアクティブになり、フィルタを作成できるようになります。フィルタを作成しないでクエリを実行すると、選択された時間範囲が使用されます。

3. (オプション)「[イベント]ビューでの結果のフィルタリング」の説明に従って、時間範囲を編集します。



このサービスに選択した時間範囲はブラウザに保存されます。サービスごとに異なる時間範囲を設定できます。

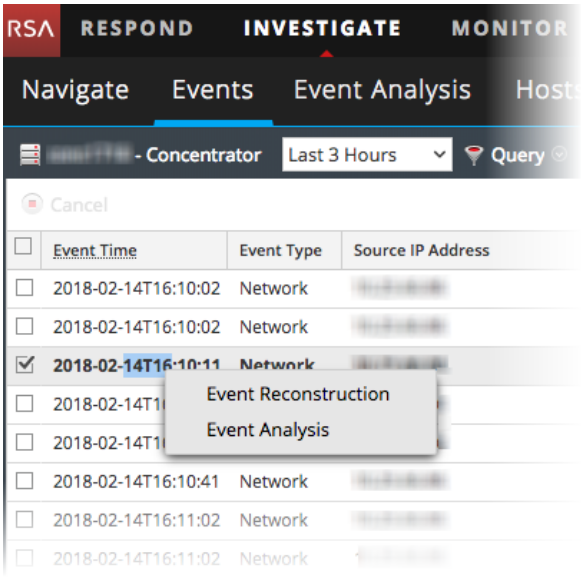
4. クエリを作成します。クエリは、1つまたは複数のフィルタで構成され、各フィルタは、メタ キー、演算子、値(オプション) で構成されます。クエリの作成方法の詳細については、「[イベント]ビューでの結果のフィルタリング」を参照してください。

5. クエリを送信する準備ができたら、([**クエリ送信**]) をクリックします。
管理者によってロールに割り当てられた権限に応じて、選択したサービス、時間範囲、クエリのデータが[イベント]ビューに表示されます。データの分析を開始する準備ができました。[イベント]ビューでの作業方法については、「[イベント]ビューでのイベントの再構築」および「[イベント]ビューでのイベントの分析」を参照してください。

[イベント]ビューへのアクセス(バージョン11.0)

[イベント]ビューでイベントを開くには、次の手順を実行します。

1. [**調査**]>[**イベント**]に移動します。
2. 次のいずれかを実行します。
   a. 一覧表示されたイベントのいずれかを右クリックし、[**イベント分析**]を選択します。



   b. 一覧表示されたイベントのいずれかを右クリックし[**イベント再構築**]を選択します。再構築で[**イベント分析**]ボタンをクリックします。

[イベント]ビューでの作業方法については、「[[イベント]ビューでのイベントの再構築](#)」および「[[イベント]ビューでのイベントの分析](#)」を参照してください。

結果セットの絞り込み

調査を実施するときに、結果を絞り込んで結果の数を少なくすると、結果のロードが速くなり、探しているデータを見つけやすくなります。時間範囲を制限して、適切なクエリを送信すると、より関連性の高い結果が得られ、質問の答えを見つけられるようになります。このセクションの残りの部分で説明する方法を組み合わせて使用すると、必要な情報をすばやく入手できます。

- メタ グループを使用して関連性の高いメタ キーにフォーカス
- イベント リストでの列と列グループの使用
- クエリ プロファイルを使用した調査の共通領域のカプセル化
- [イベント]ビューでの結果のフィルタリング
- [ナビゲート]ビューでの結果のフィルタリング
- [レガシー イベント]ビューでの結果のフィルタリング
- [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成
- URL統合を使用したクエリの表示と変更
- [ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索

メタ グループを使用して関連性の高いメタ キーにフォーカス

メタ グループは、選択されたメタ キーとメタ エンティティをグループにまとめ、メタ キーとメタ エンティティが見つかったデータのみを表示します。[ナビゲート]ビューでは、[ナビゲート]ビューの[値]パネルに表示するメタキーを制限するため、メタ グループを使用できます。NetWitness Platformの新規インストールには、調査の対象のデータ セットを見つけるために役立つ、標準提供のメタ グループが含まれています。標準提供のメタ グループ名には、識別のためにRSAのプレフィックスが付いており、複製できますが、編集または削除することはできません。独自のグループを作成することや、標準提供のグループを複製して編集し、カスタム グループを作成することができます。

調査中にメタ グループが有効になっている場合、[値]パネルの情報には、選択されたグループのメタ キーのみが表示されます。座標表示チャートを開くと、メタ キーとメタ エンティティが軸として左から右に表示されます。カスタム メタ グループごとに2つのバージョンを作成しておくと便利です。1つはメタ値の分析に使用し、もう1つはメタ キーを減らしたサブセットを作成し、座標表示チャートの表示に使用します。

カスタム メタ グループは、サービスのすべてのユーザが利用でき、エクスポートして異なるサービスにインポートすることもできます(ただし、そのサービスで利用可能なメタ キーに限定されます) 。

注: 管理者が、サービスのカスタム インデックス ファイルを編集して、カスタム メタ グループを手動で追加した場合、サービスの再起動後に、調査で新しいグループが利用可能になります。

このセクションでは、特定のサービスでナビゲート時に使用するカスタム メタ グループを追加、編集、インポート、エクスポート、削除する方法について説明します。

標準提供メタ グループ

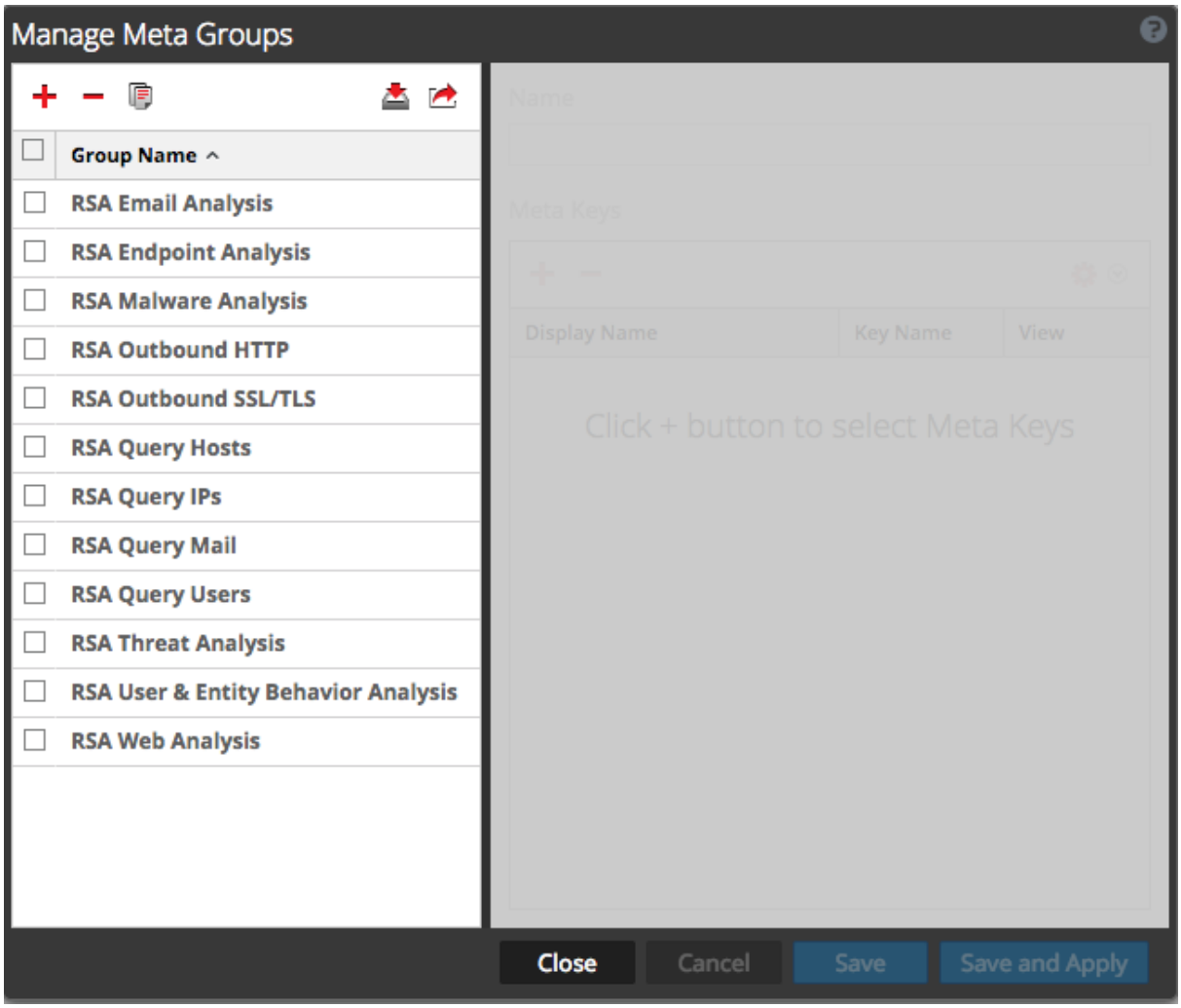
RSA NetWitness Platformには、インストール後すぐに使用可能な標準提供のメタ グループがあります。標準提供メタ グループは、一般的なユースケースでの調査に焦点を当て、RSA Hunting Packを使用した脅威検出をサポートするために役立ちます。標準提供メタ グループは次のとおりです。

- RSA Email Analysisには、メールのやり取りで使用されるメタ キーが含まれています。
- RSA Endpoint Analysisには、NetWitness Endpoint(NWE) ホストのプロセス、ファイル、ユーザ、接続に関する洞察を提供するメタ キーが含まれています。
- RSA Malware Analysisには、イベントに含まれるファイルのセキュリティ侵害インジケータをマークするメタ キーが含まれています。
- RSA Outbound HTTPには、外部へのWebトラフィックに関する洞察を提供するメタ キーが含まれています。
- RSA Outbound SSL/TLSには、暗号化されたWebトラフィックに焦点を当てたメタ キーが含まれています。
- RSA Query Hostsには、ホストを見つけるために使用されるすべてのメタ キーが包含されています。
- RSA Query IPsには、IPアドレスを見つけるために使用されるすべてのメタ キーが包含されています。
- RSA Query Mailには、メールを見つけるために使用されるすべてのメタ キーが包含されています。
- RSA Query Usersには、ユーザを見つけるために使用されるすべてのメタ キーが包含されています。

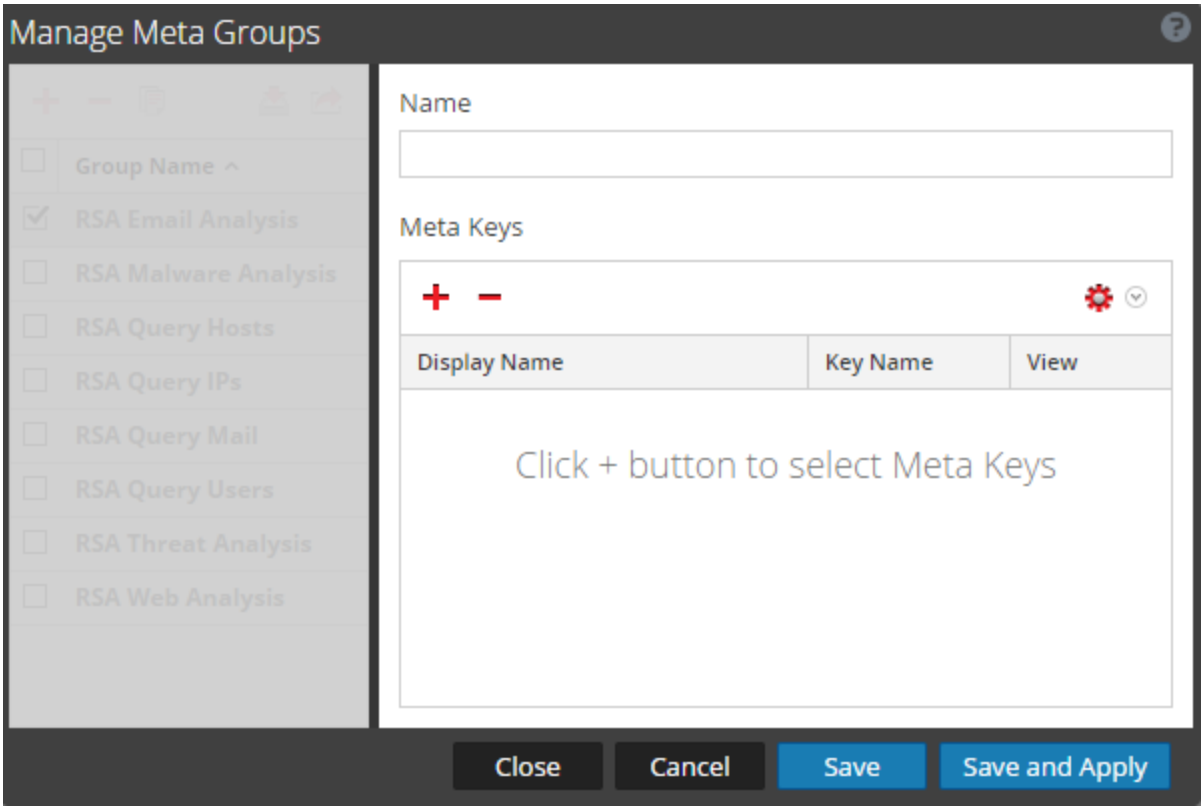
- RSA Threat Analysisには、データセット内の潜在的な脅威をマークするメタ キーが含まれています。
- RSA User & Entity Behavior Analysisには、ユーザとエンティティの振る舞いを分析するために使用されるすべてのメタ キーが包含されています。
- RSA Web Analysisには、Webトラフィックの異常をマークするメタ キーが含まれています。

メタ グループの作成とメタ キーの追加

1. [**ナビゲート**]ビューでサービスを調査しているときに、ツールバーで、[**メタ**]＞[**メタ グループの管理**]を選択します。
   [メタ グループの管理]ダイアログが表示されます。初期状態では標準提供のグループのみが構成され、グループ名の下に一覧表示されます。他のカスタム グループが構成されている場合は、それらもグループ名の下に一覧表示されます。

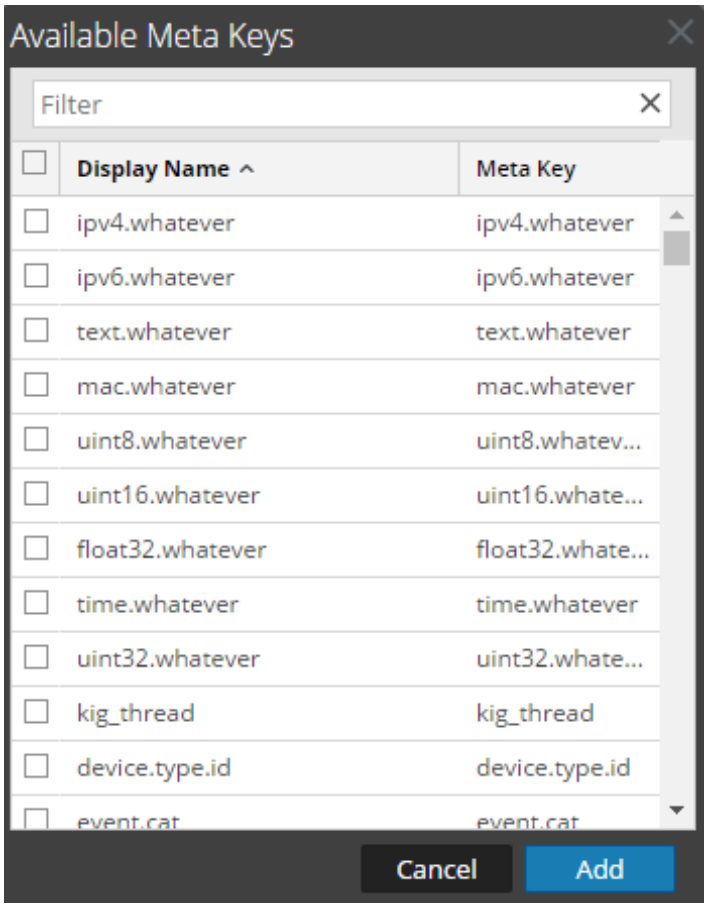


2. [メタ グループ]リストの上にあるツールバーで、＋をクリックします。
右側にフォームが開いて編集可能な状態になります。



3. [**名前**]フィールドに新しいメタ グループの名前を入力します。

4. [**メタ キー**]セクションのツールバーで、＋をクリックします。
[利用可能なメタ キー]ダイアログに、キーがアルファベット順で表示されます。

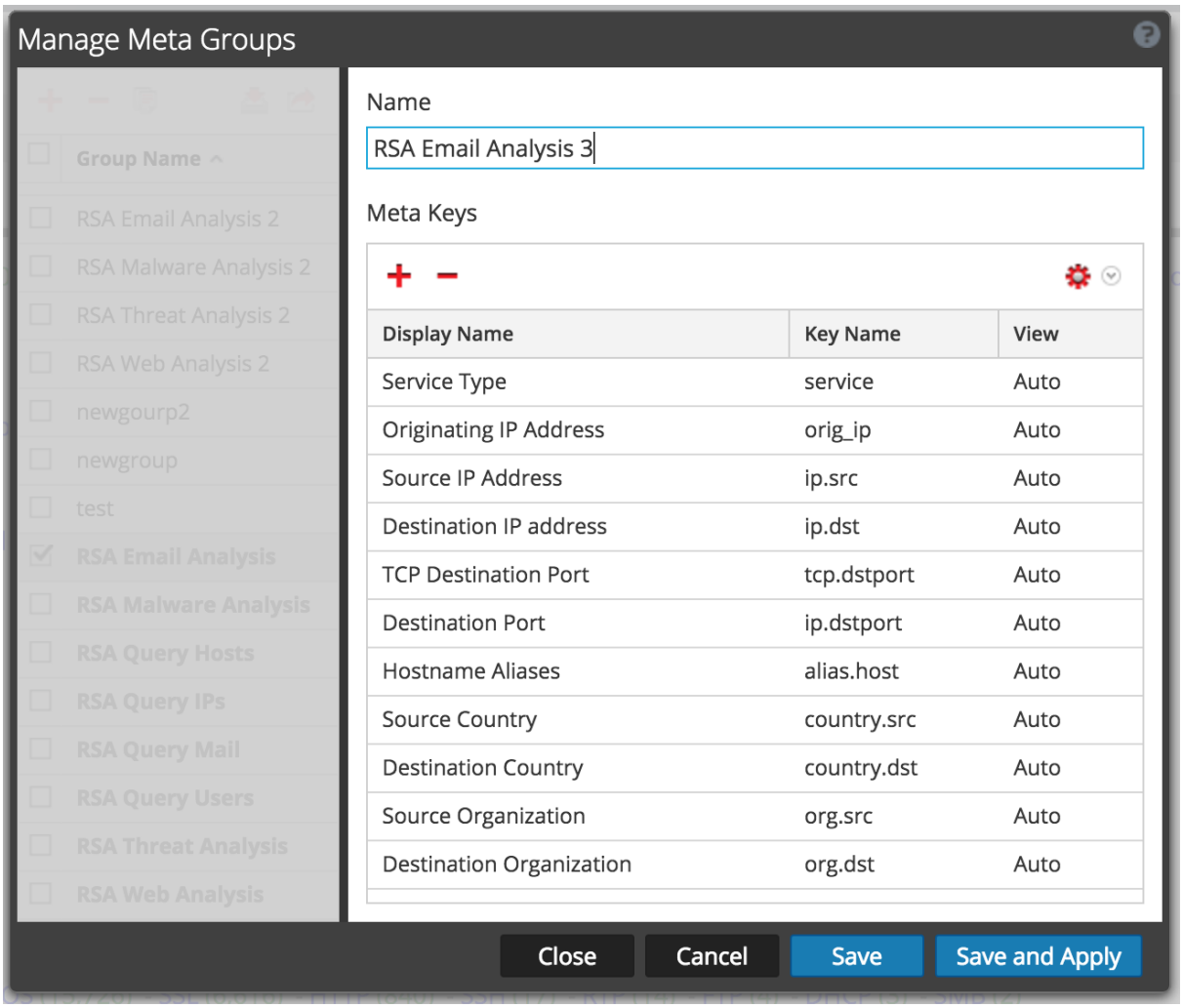


5. メタ キーのリストを絞り込むには、[**フィルタ**]フィールドに単語またはフレーズを入力し、**Enter**キーを押します。
   一致するメタ キーがリストに表示されます。大文字と小文字は区別されません。[フィルタ]フィールドのテキストを削除して**Enter**キーを押すと、フィルタを削除できます。
6. メタ グループに追加するメタ キーを個別に選択するには、チェックボックスをオンにします。すべてのメタ キーを選択するには、タイトル バーのチェックボックスをオンにして[**追加**]をクリックします。
   選択したメタ キーが[メタ キー]リストに追加されます。
7. (オプション) メタ キーをロードして表示する順序を変更したい場合は、メタ キーをクリックして、新しい位置にドラッグします。同時に複数のメタ キーを選択できます。
8. メタ グループの作成を終了するには、次のいずれかを実行します。
   a. メタ グループを保存するには、[**保存**]をクリックします。
      グループが作成され、使用可能になります。
   b. メタ グループを保存して、現在の[調査]ビューに適用するには、[**保存して適用**]をクリックします。
      グループが作成され、現在の[調査]ビューにすぐに適用されます。
9. [**閉じる**]をクリックします。

標準提供メタ グループの複製と編集

標準提供のメタ グループをカスタマイズする場合は、グループを複製してから、複製を編集する必要があります。

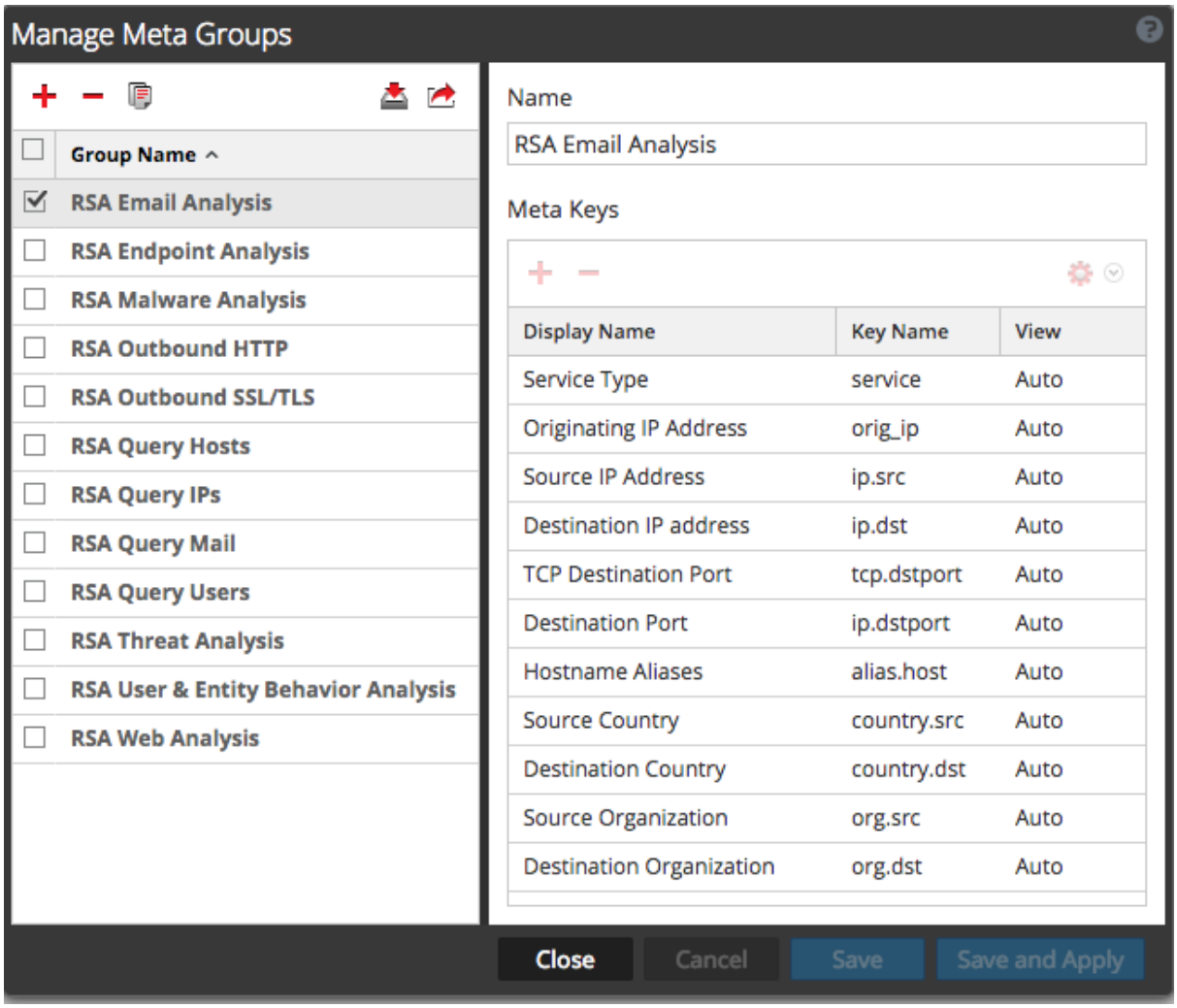
1. [メタ グループの管理]リストから標準提供のメタ グループを選択し、 をクリックします。
   右側に編集可能なフォームが開き、標準提供グループ内のすべてのメタ キーが表示されます。



2. 新しいグループの名前を入力し、次の「メタ グループの編集」の説明に従い編集を続けます。

メタ グループの編集

1. [**メタ グループ**]リストからグループを選択します。
   右側のフォームが開いて編集可能な状態になります。



2. (オプション) グループの[名前]を編集します。
3. (オプション) 前述の「メタ グループの作成とメタ キーの追加」の説明に従って、新しいメタ キーを追加します。
4. (オプション) キーの順序を変更する場合は、キーをドラッグ&ドロップします。同時に複数のキーを選択できます。
5. (オプション) メタ キーの初期表示を変更するには、  をクリックして、いずれかの初期表示オプションを選択します。
   メタ グループを変更するとき、[開く]に設定できないキーがあります。メタ グループのデフォルトの初期表示を[開く]に変更し、一部のメタ キーがインデックスされていない場合、インデックスされていないメタ キーの設定は自動的に[自動]に戻ります。その結果、メタ キーがインデックスされている場合のみ自動的にロードされます。インデックスされていないメタ キーは手動で開くまで閉じた状態で表示されます
   初期表示の値は[表示]列に表示されます。
6. 変更を保存するには、[**保存**]をクリックします。
7. 現在の[ナビゲート]ビューに変更を適用するには、[**保存して適用**]をクリックします。

メタ グループの削除

1. [**メタ グループ**]リストで、削除するグループを選択します。
2. －をクリックします。
   確認のダイアログが表示され、ここで削除をキャンセルするか、続行するかを選択できます。
3. [**はい**]をクリックします。
   メタ グループが削除されます。削除するメタ グループを使用していた場合には、デフォルトのメタ キーを使用して表示が更新されます。

メタ グループのエクスポート

ユーザ定義のメタ グループは、各サービスに作成されます。メタ グループを別のサービスで使用できるようにするには、ローカル ファイル システムにメタ グループをエクスポートする必要があります。メタ グループをエクスポートするには、次の手順を実行します。

1. [**メタ グループ**]リストで、エクスポートするグループを1つ以上選択します。
2.  をクリックします。
   選択したグループが**MetaGroups.jsn**というファイル名で、ローカル ファイル システムにダウンロードされます。ダウンロード先に以前ダウンロードした同名のファイルが存在する場合は、上書きを避けるため、ファイル名に数字が付加されます。

メタ グループのインポート

別のサービスのユーザ定義メタ グループを、現在調査中のサービスで使用するには、ローカル ファイル システムから`MetaGroups.jsn`ファイルをインポートする必要があります。メタ グループをインポートする時、既存のメタ グループが含まれていると、エラー メッセージが表示されます。重複したグループをインポートするには、まず既存のグループを削除しておかなければなりません。プロファイルで使用されているメタ グループは削除できません。

メタ グループをインポートするには、次の手順を実行します。

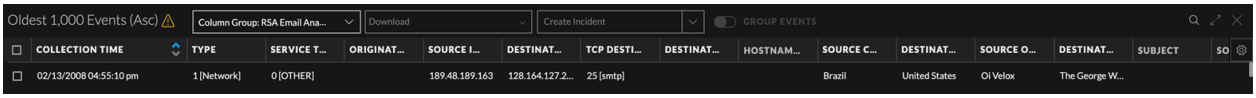
1. [**メタ グループ**]リストで、インポートするファイルを選択し、  をクリックします。
   選択ダイアログが表示されます。

2. [**参照**]をクリックし、ローカル ファイル システム上の、ダウンロードした`MetaGroups.jsn`ファイルが格納されているディレクトリに移動します。ファイルを選択し、[**開く**]をクリックします。
   [ファイルのアップロード]フィールドにファイル名が表示されます。

3. [**アップロード**]をクリックします。
   アップロード プロセスが開始され、アップロードが正常に完了したことを示すメッセージが表示されます。[メタ グループ]リストにグループが追加されます。ファイル内のメタ グループが既存のメタ グループと重複する場合は、メタ グループがすでに存在することを通知するダイアログが表示されます。

イベント リストでの列と列グループの使用

調査のイベント リストにイベントが読み込まれると、各列にメタ キーの値が表示されます。イベント リストに表示されるメタ キーの変更は、調査のフォーカスを絞り込むための便利な方法です。たとえば、同じイベントの異なる列を表示する2つの図で比較してみましょう。最初の図には、**Collection Time**、**Type**、**Theme**、**Size**、**Summary**という5つの列があります。これらは基本的な情報であり、特殊な情報ではありません。2番目の図には、メールを調査する際に役立つ情報を含んだ、より多くの列があります。右にスクロールして、追加の列を表示できます。



イベント リストでは、表示する別の列の選択、列の順序の変更、列幅の変更、リストをソートする列の選択などの調整を、作業しながら加えることができます。手動調整は、どのメタ キーが重要であるかがわかっていれば簡単ですが、現在のセッションにしか適用されません。

[レガシー イベント]ビューと[イベント]ビューでイベントを調べるときに、重要なメタ キーをすばやく確認できるようにするには、列グループを適用して、表示されるメタ キーのセットを変更します。列グループは、列として表示されるメタ キーまたはメタ エンティティ、イベント リスト内の列の位置、列のデフォルトの幅を定義します。列グループは、それ自体でも有益ですが、メタ グループおよびプレクエリと組み合わせてクエリ プロファイルを定義する場合はさらに役立ちます(「クエリ プロファイルを使用した調査の共通領域のカプセル化」を参照)。

注: バージョン11.4には、以前のバージョンで[イベント分析]ビューと呼ばれていた単一の[イベント]ビューがあります。バージョン11.3以前の[レガシー イベント]ビューは、管理者が『*システム構成ガイド*』の説明に従ってこのビューを有効にしている場合は、引き続き使用できます。[レガシー イベント]ビューが有効になっている場合は、[調査]サブメニューから両方のビューにアクセスできます。

同じ列グループが[レガシー イベント]ビューと[イベント]ビューの間で共有され、すべてのユーザに対してグローバルに表示されます。列グループをインポートする場合、インポートされるグループは、調査対象のサービスで使用可能なメタ キーに限定されます。

各メタ キーの値がイベント リストにロードされるため、大規模な列グループは、データのロード時にパフォーマンスに影響する可能性があります。パフォーマンスへの影響を最小限に抑えるため、[イベント]ビューには列グループ内のメタ キーの数に対して固定された制限があります。列グループ内のメタ キーの最大数は40個です。デフォルトのキーが含まれているため、40個を超えるメタ キーが画面に表示されることがあります。列グループには少なくとも1つの列が必要です。選択した列グループに含まれていないメタ キーは、イベント リストにロードされません。デフォルトでは、グループ内のすべての列がロードされますが、表示されるのは15列のみです。

[レガシー イベント]ビューには、列グループ内のメタ キーの数の制限がなく、40個を超えるメタ キーを列グループに含めることができます。[レガシー イベント]ビューで作成された40個を超えるメタ キーを含む列グループを適用すると、すべての列が[イベント]ビューにロードされます。ただし、制限を超えた列グループを編集する場合は、固定制限の40に従うよう、列の数を減らす必要があります。

注： バージョン11.3では、列グループは[イベント]ビューで作成および管理され、[イベント分析]ビューで使用できます。標準提供とカスタムの両方の既存の列グループが、11.4の[イベント]ビューで使用可能です。11.4の[レガシー イベント]ビューでは、完全な列グループ管理機能を使用できます。11.4の[イベント]ビューでは、列グループの複製、インポート、エクスポート以外のすべての機能を使用できます。

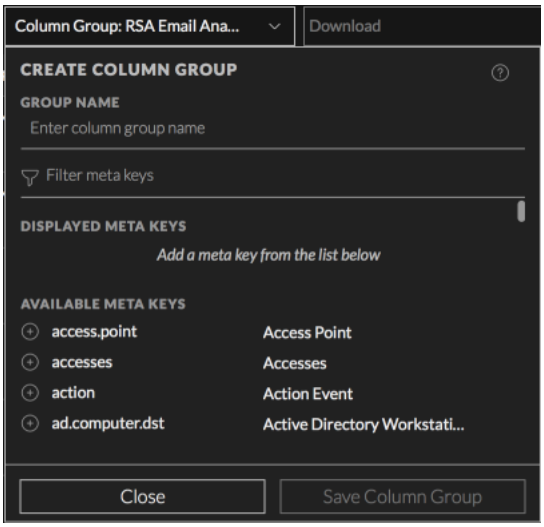
NetWitness Platformには、特定のタイプの調査に役立つメタ キーを含んだ標準提供の列グループがあります。標準提供のグループを編集または削除することはできませんが、グループのコピーを作成して、コピーを編集できます。[列グループ]メニューには、列グループがアルファベット順で表示され、インポートまたは作成したカスタム グループと標準提供のグループを区別できます。[レガシー イベント]ビューでは、標準提供の列グループの名前は「RSA」で始まります。[イベント]ビュー(バージョン11.4以降) では、名前が「RSA」で始まり、ロック記号() が表示されます。標準提供の列グループは次のとおりです。

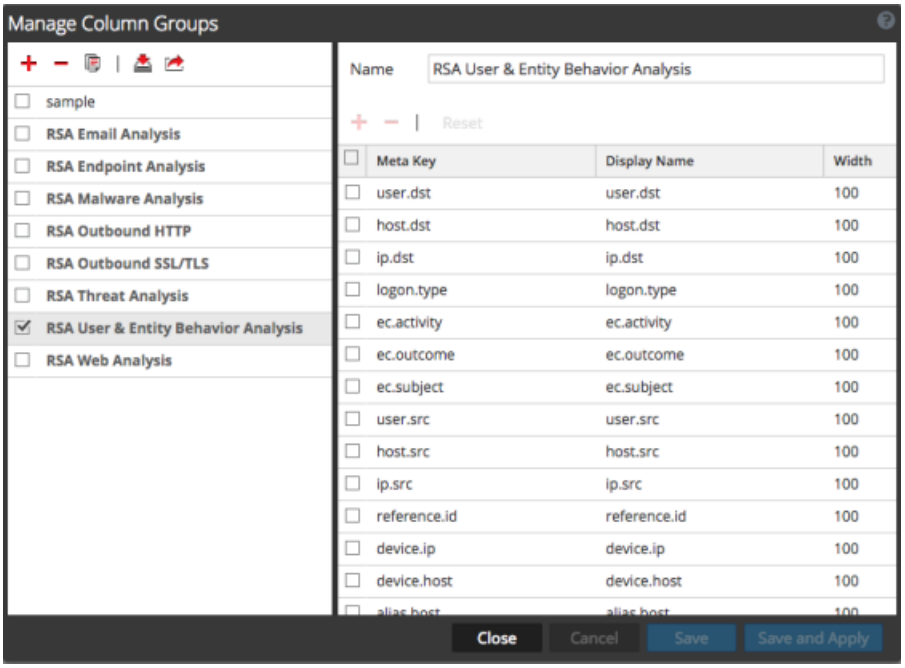
- **RSA Email Analysis**: メール関連のメタデータの調査に役立つメタ キーが含まれます。
- **RSA Endpoint Analysis**: エンドポイント関連のメタデータの調査に役立つメタ キーが含まれます。
- **RSA Malware Analysis**: 潜在的なマルウェアの調査に役立つメタ キーが含まれます。
- **RSA Outbound HTTP**: アウトバウンドHTTP関連の調査に役立つメタ キーが含まれます。
- **RSA Outbound SSL/TLS**: アウトバウンドSSL/TLS関連の調査に役立つメタ キーが含まれます。
- **RSA Threat Analysis**: データセット内の潜在的な脅威をマークするメタ キーが含まれます。
- **RSA User and Entity Behavior Analysis**: UEBAデータの調査に役立つメタ キーが含まれます。
- **RSA Web Analysis**: Webトラフィックの異常をマークするメタ キーが含まれます。
- **Summary List**: 一般的な調査に役立つメタ キーが含まれます。これは、デフォルトの列グループです。

カスタム列グループを作成して、調査中に頻繁に使用するシナリオをサポートできます。カスタム列グループを編集する場合、変更はグローバルに適用されます。カスタム列グループを削除すると、そのグループは削除され、すべてのアナリストが使用できなくなります。管理者が、サービスのカスタム インデックス ファイルを編集して、カスタム列グループを手動で追加した場合、サービスの再起動後に、調査で新しいグループが利用可能になります。

列グループを管理するためのダイアログ

[レガシー イベント]ビューと[イベント]ビューの列グループの機能は似ていますが、ユーザ インタフェースと一部の手順が異なります。次の図は、([イベント]ビューの) [列グループの作成]ダイアログと([レガシー イベント]ビューの) [列グループの管理]ダイアログを示しています。





[列グループの作成]ダイアログと[列グループの管理]ダイアログのオプションを使用して、次の操作を実行できます。

- 列グループの詳細を表示します。
- カスタム列グループを作成、編集、削除します。

[列グループの管理]ダイアログのオプションを使用すると、上記のすべての機能に加えて、次の機能を実行できます。

- 標準提供またはカスタムの列グループを複製して、編集します。
- 列グループをインポートおよびエクスポートします。

このトピックの残りの部分では、11.4の[イベント]ビュー、11.3以前の[イベント分析]ビュー、[レガシー イベント]ビューで列グループを操作する手順について説明します。

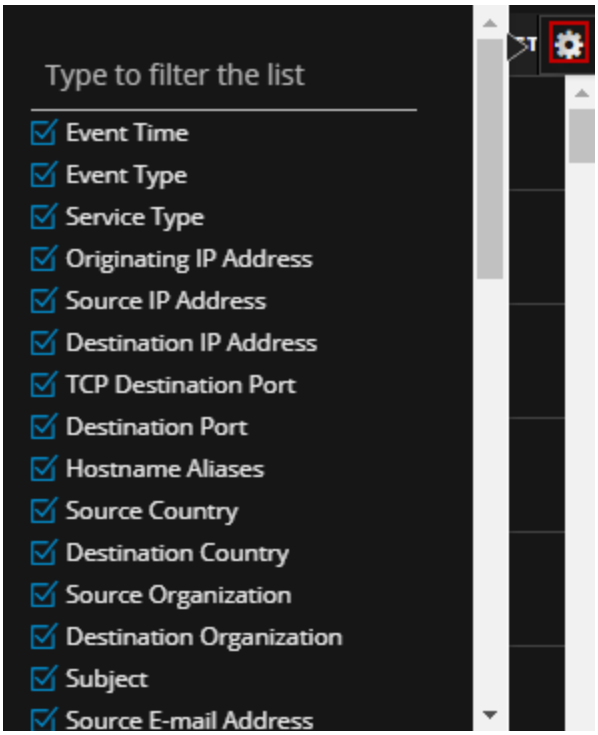
11.4の[イベント]ビューでの列と列グループの操作

バージョン11.4にアップグレードした後、既存のすべての列グループ(標準提供とカスタムの両方)が[イベント]ビューで管理できるようになります。特に記載のない限り、このセクションの手順は[イベント]ビューについて説明しています。

手動での表示する列の選択と列の順序と幅の調整

注: 列セレクターは、11.3の[イベント分析]ビューでも使用できました。管理者がブラックリスト(非表示)に登録しているメタ キーの列が列グループに含まれている場合、その列のデータは表示できません。この列は列セレクターで選択することができず、[イベント]パネルにも表示されません。

1. [イベント]リストが開き、列グループが適用された状態で、をクリックして列セレクターを表示します。



2. 列に追加したいメタ キーを選択するか、メタ キーの名前を入力します。
3. 列に表示しないメタ キーを選択解除します。
   選択した列を使用してデータが再表示されます。
4. イベント リストの列の幅を変更するには、列のタイトルの上にカーソルを合わせて、列の境界線を右または左にドラッグします。
5. イベント リストの列の配置を変更するには、列のタイトルの上にカーソルを合わせ、列を右または左にドラッグします。

イベント リストで行った変更は、現在のセッション中は有効ですが、列グループの一部としては保存されません。列グループを次回適用したときには、元の構成と列の順序が適用されます。

[イベント]パネルでイベントをソートするための列の選択

注: 接続されているサービスがすべて11.4以降に更新されている場合は、結果のロードが完了した後で、[イベント]パネルでイベントをソートできます。接続されたサービスで以前のバージョンのNetWitness Platformが実行されている場合、列によるソートは無効になります。バージョン11.4.1では、列見出しのソート トグルがわかりやすくなり、ソートなしで結果を表示する機能が追加されていますが、それ以外はバージョン11.4と同じです。

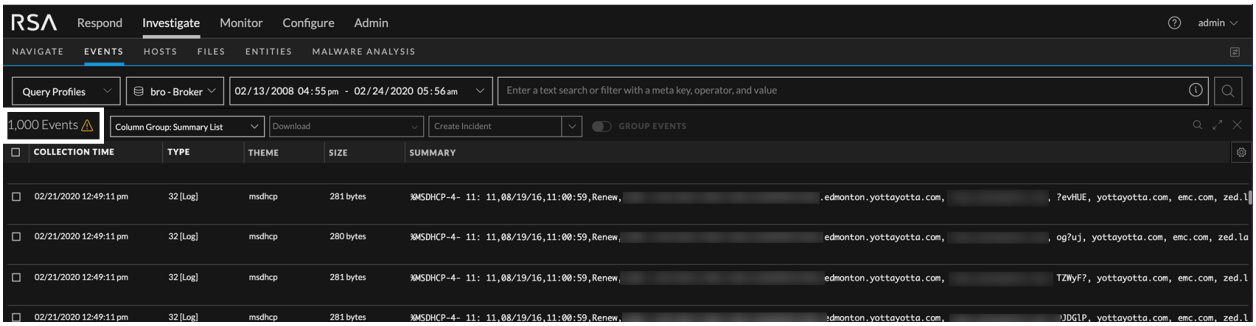
[イベント]パネルのイベント リストの順序は、イベント内のメタ キーの値によって変更できます。各列のタイトルはメタ キーを表し、表示されているイベントのメタ キーに値があれば、列に読み込まれます。バージョン11.4では、[イベント]パネルのイベントは、[イベント環境設定]ダイアログで選択した方法(昇順または降順)でソートされます。ソート方法が選択されていない場合、デフォルトの順序は昇順です(「[イベント]ビューの構成」を参照)。バージョン11.4.1では、[イベント]パネルのイベントがソートされるのは、[イベント環境設定]ダイアログでソート順が選択され、それが昇順または降順のいずれかである場合だけです。[イベント環境設定]でソート順を選択していない場合、または[ソートしない]を選択した場合、イベントはソートされません。

その列でソートできるかどうかは、BrokerおよびConcentratorのインデックス ファイルでのメタ キーの定義によって決まります。値でインデックスされたメタ キーの列はソート可能です。メタ キーがインデックスされていない場合、メタキーでインデックスされている場合、または同じイベント内に複数の値を持つ場合、そのメタ キーではソートできません。

- 値でインデックスされた、ソート可能なキーの例としては、`time`、`eth.type`、`city.src`、 `ip.src`、`ipv6.dst`、 `ipv6.src`があります。
- メタ エンティティはソートできません。たとえば、メタ エンティティ`ipv6.all`でソートできないのは、`ipv6.dst`と `ipv6.src`が含まれ、1つのイベントに`ipv6.dst`と `ipv6.src`の両方のメタ値が含まれるためです。
- ソートできない複数値のメタ キーの例としては、 `filename`、`filetype`、`attachment`があります。単一のイベントに複数のファイルが含まれる可能性があるため、`filename`、`filetype`、`attachment`の値が複数になる場合があります。
- インデックスされていない、または値レベルでインデックスされていないためにソートできないメタ キーの例としては、`password`、`query`、`size`があります。

バージョン11.4.1の列によるソート

環境設定でソート順が[ソートしない]に設定され、列によるソートが行われていない場合、[イベント]リストの初期ビューのタイトルには、イベント数が表示されるだけで、ソート順は表示されません。次の例では、1,000件を超えるイベントがクエリに一致しましたが、コア サービスが処理した順に1,000件のイベントのみが表示されています。黄色の三角形の警告をクリックすると、説明が表示されます。環境設定でソート順が[昇順]に設定されている場合、カウント ラベルには「最も古い1,000イベント」と表示されます。環境設定でソート順が[降順]に設定されている場合、カウント ラベルには「最も新しい1,000イベント」と表示されます。環境設定のソート順の設定については、「[イベント]ビューの構成」を参照してください。



列のタイトルの上にマウスを移動すると、ソート可能な列の列タイトルの後に1組の矢印が表示されます。上矢印は昇順を、下矢印は降順を表します( ) 。ソート列1つとソートの方向を選択できます。青色の上矢印( ) は、昇順のソート順が有効になっていることを示します。つまり、最も古いイベントや最も低い数値、または「A」で始まるテキスト文字列が最初に表示されます。青色の下矢印( ) は、降順のソート順が有効になっていることを示します。つまり、最も新しいイベントや最も高い数値、または「Z」で始まるテキスト文字列が最初に表示されます。

- 列に青色の矢印が表示されている場合は、白色の矢印をクリックしてソート順を変更できます。ソート順を変更すると、進捗状況を示す青色の進捗状況バーが[イベント]リストのタイトル バーに表示されます。ソートが始まると、タイトルバーの左端に青色の短いバーが表示されます。ソートが進むにつれて、青色のバーが右に延び、タイトルバーの右端で終了します。方向矢印は、選択したソート順でイベントが再ソートされるまで変わりません。
- その列のソートを解除する場合は、青色の矢印をクリックします。両方の矢印が白に変わり、その列がソートされていないことを示します。次の図は、昇順でソートされた[Type]列を示しています。

- 列がソート可能でない場合、列のタイトルの上にマウスを合わせても矢印は表示されません。その代わりに、ソートできない理由を説明したツールチップが表示されます。

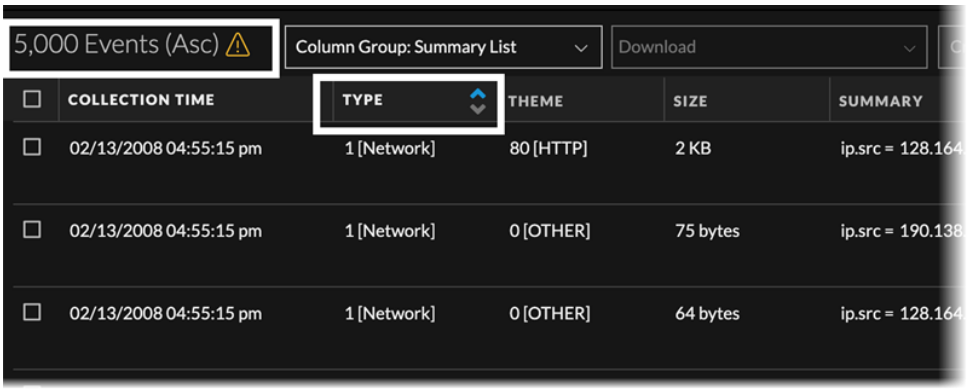
表示された結果の数が、管理者によって設定されたイベント数の上限よりも少ない場合、列のソートは、クエリを再実行することなくクライアント側で実行されます。結果の数がイベント数の上限を超過したために表示されない結果が存在する場合は、新しいソート順で、同じサービス、時間範囲、フィルタを使用して新しいクエリが送信されます。現在の結果が削除され、スピナーに進行状況が示されます。[キャンセル]ボタンが使用可能になり、再構築が終了し、進行状況がクエリコンソールに表示されます。

注： 元のクエリの結果の数が表示するイベントの閾値よりも少ない場合、イベントの再ソートはブラウザで行われます。

ソート順またはソート列を変更するには、次の手順を実行します。

1. 列のタイトルの上にマウスを移動すると、ソート可能な列を見つけることができます。
   列がソート可能でない場合は、その理由を説明するツールチップが表示されます。

2. リストを列でソートするには、ソート可能な列にマウスを移動し、上下どちらかの矢印( ) をクリックします。
   矢印が青色に変わり、選択した順序でイベントが再ロードされます。両方の矢印が白色の場合、その列はイベント リストのソートに使用されていません。一方の矢印が青色の場合は、その列がイベント リストのソートに使用されており、ソート順(昇順または降順) がタイトル バーのイベント数の横に表示されます。次の図は、昇順でソートされた列を示しています。降順の場合は、[(降順)] がイベント数の横に表示されます。



   a. 白色の矢印をクリックすると、その順序でイベント リストがソートされます。

   b. 青色の矢印をクリックすると、ソートなしの状態に戻ります。

バージョン11.4の列によるソート

列のタイトルの上にマウスを移動すると、ソート可能な列のタイトルの後に上矢印または下矢印(または) が表示されます。ソート列1つとソートの方向を選択できます。上矢印は、昇順のソート順が有効になっていることを示します。つまり、最も古いイベントや最も低い数値、または「A」で始まるテキスト文字列が最初に表示されます。下矢印は、降順のソート順が有効になっていることを示します。つまり、最も新しいイベントや最も高い数値、または「Z」で始まるテキスト文字列が最初に表示されます。ソート列を選択すると、その列によりデフォルトの降順でソートされ、メタ キーの値がNullのイベントが最初に表示されます。

- イベント リストのソートに使用されている列には、ソート可能な方向を示す明るい白色の矢印が表示されます。昇順に変更する場合は、 をクリックし、降順に変更する場合は、 をクリックします。 をクリックして昇順に変更すると、イベントが昇順で再ソートされるまで、方向矢印は変わりません。これと同じ動作は、 をクリックして降順に変更した場合にも当てはまります。

- ソート可能な列がイベント リストのソートに使用されていない場合、矢印はグレー表示になります。列がソート可能でない場合、列のタイトルの上にマウスを合わせても矢印は表示されません。その代わりに、ソートできない理由を説明したツールチップが表示されます。
- 別の列の矢印をクリックすると、それまでアクティブであったソート列と同じソート順でソートされます。別のソート順を選択することもできます。

表示された結果の数が、管理者によって設定されたイベント数の上限よりも少ない場合、列のソートは、クエリを再実行することなくクライアント側で実行されます。結果の数がイベント数の上限を超過したために表示されない結果が存在する場合は、新しいソート順で、同じサービス、時間範囲、フィルタを使用して新しいクエリが送信されます。現在の結果が削除され、スピナーに進行状況が示されます。[キャンセル]ボタンが使用可能になり、再構築が終了し、進行状況がクエリコンソールに表示されます。

注: 元のクエリの結果の数が表示するイベントの閾値よりも少ない場合、イベントの再ソートはブラウザで行われます。時間が完全に一致しているイベントがある場合、これらのイベントの順序は、ソート順を逆にしたときのようには変更されません。

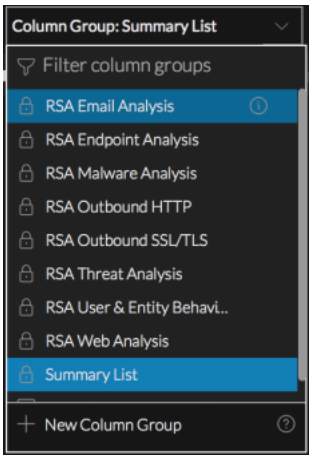
ソート順またはソート列を変更するには、次の手順を実行します。

1. 列のタイトルの上にマウスを移動すると、ソート可能な列を見つけることができます。
   列がソート可能でない場合は、その理由を説明するツールチップが表示されます。
2. リストを列でソートするには、次の手順を実行します。
   a. ソート可能な列にマウスを移動し、矢印(または) をクリックします。
      イベントが正しいソート順でソートされます。列のタイトルの上にカーソルを合わせると、矢印の色がグレーでなくなったことを確認できます。イベント リストのソートに使用されている列には、明るい白色の矢印が表示され、これをクリックしてソートの方向を変更できます。
   b. ソート順を変更するには、をクリックして昇順に変更するか、をクリックして降順に変更します。
      矢印の方向が変わり、選択した順序でイベントが再ロードされます。

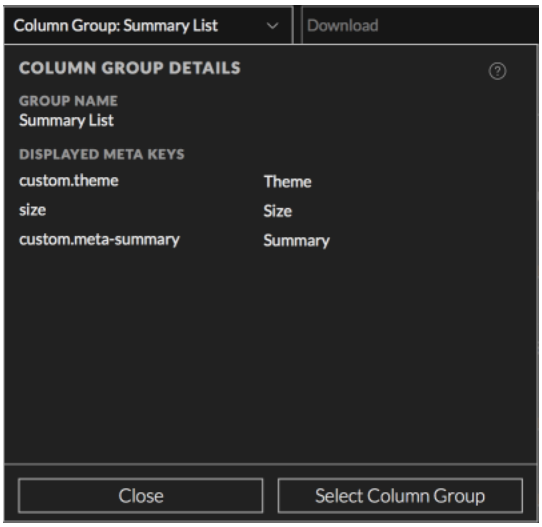
列グループに含まれているメタ キーの表示

列グループの詳細を表示するには、次の手順を実行します。

1. **[調査]＞[イベント]**に移動し、をクリックしてイベントをロードします。
   デフォルト サービスとデフォルトの時間範囲のイベントが[イベント]パネルにロードされます。
   [Summary List]列グループまたは前回のセッションで使用されていた列グループがリストに適用されます。[列グループ]メニューのタイトルに、選択した列グループの名前が表示されます。次の図は、[Summary List]がデフォルトで選択され、リスト内の最初の列グループがハイライト表示されている、初期状態のメニューを示しています。



2. グループに含まれている列を確認するには、[**Summary List**]グループの上にカーソルを合わせて情報アイコン( ) をクリックします。
次の図は、[Summary List]の列を示しています。Collection TimeとTypeの2つは常にイベント リストの先頭の2列に表示されますが、[列グループの詳細]ダイアログには表示されません。

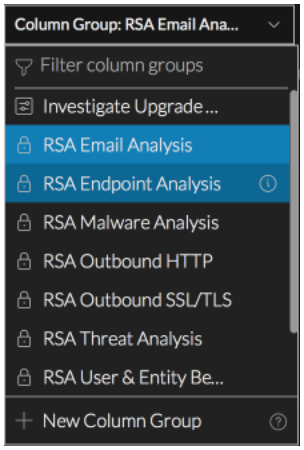


3. 次のいずれかの操作を実行します。
   a. ダイアログを閉じるには、[**閉じる**]をクリックします。
   b. 列グループを適用する場合は、[**列グループの選択**]をクリックします。
   ダイアログが閉じ、選択した列グループを反映するようにイベント リストが更新されます。

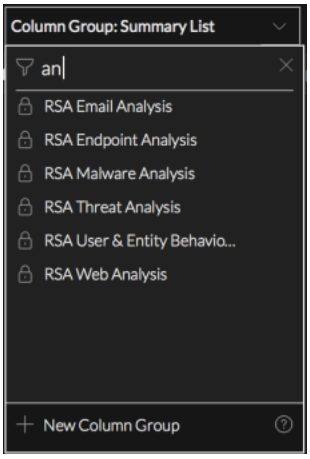
列グループの選択

1. 11.4の[イベント]ビューで[イベント]パネルを開き、[**列グループ**]メニュー タイトルをクリックします。
メニューがドロップダウンし、列グループのリストが表示されます。列グループの絞り込みオプションと、[新しい列グループ]オプションも表示されます。標準提供の列グループは「RSA」で始まり(Summary Listを除く) 、グループを編集できないことを示すロック アイコン( ) が表示されます。カスタム アイコン( ) は、カスタムの列グループの名前の前に表示されます。リストはアルファベット順にソートさ

れ、メニュー ラベルには選択中の列グループ名が表示されます。リストの最初のオプションがハイライト表示されます。選択中の列グループの背景色は、ハイライト表示されている列グループとわずかに異なります。
次の図は、[RSA Email Analysis]が選択中で、[RSA Endpoint Analysis]をハイライト表示した状態のメニューを示しています。[Investigate Upgrade]はカスタム列グループの例です。



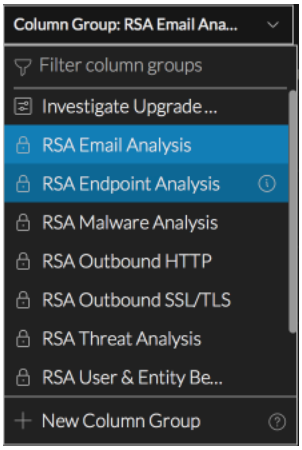
2. 次のいずれかを実行します。
   a. ハイライト表示されているグループを適用するには、**ENTER**キーを押します。
   b. 列グループ名を検索するには、[**列グループの絞り込み**]フィールドにテキストを入力します。入力に合わせてリストが絞り込まれ、入力した文字列を含む列グループ名のみが表示されます。



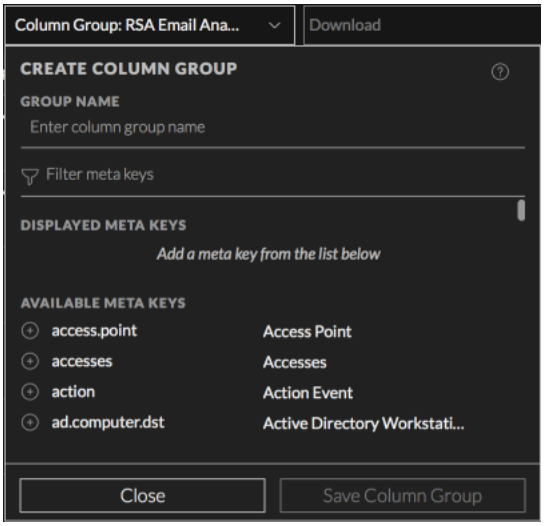
適用するグループが表示されたら、グループをクリックするか、下矢印または上矢印を使ってグループをハイライト表示して**ENTER**キーを押します。
イベント リストが更新され、選択した列グループに含まれる列のみが表示され、選択した列グループ名がメニューのタイトルに表示されます。[イベント]ビューから移動しても、選択内容は保持されます。イベント リストでの列の順序は、列グループ内のメタ キーの順序を反映しています。列グループには、右にスクロールしないと表示されない追加の列が含まれている場合があります。表示を最適化するため、列グループを選択すると、デフォルトで最初の15列が表示されます。

カスタムの列 グループの作 成

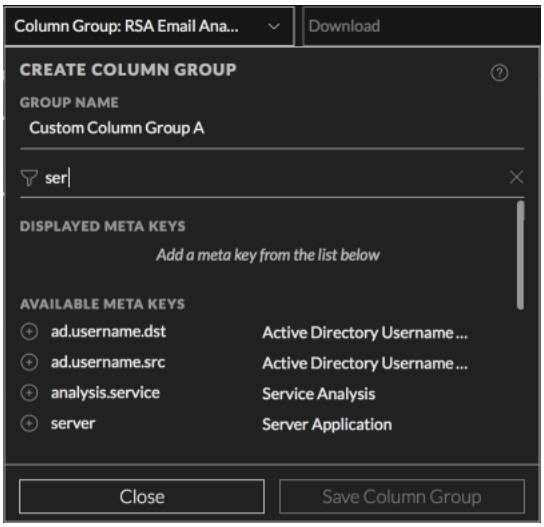
1. **[調査]＞[イベント]**に移 動して、クエリを送 信し、[イベント]パネルにデータをロードします。
2. [イベント]パネルのツールバーで、[**列グループ**]メニュー タイト ルをクリックします。
   メニューがド ロップダウンし、列 グループのリスト が表 示されます。[列 グループの絞り込 み]フィールド がー 番 上 に、[+ 新しい列 グループ]オプションがー 番 下 に表 示されます。リスト の最 初 のグループが ハイライト表 示されます。ハイライト表 示と選 択 中 の違いがわかるよう、次 の図 は、[RSA Email Analysis]が選 択 中 で、[RSA Endpoint Analysis]をハイライト表 示した状 態 のメニューを示 してい ます。



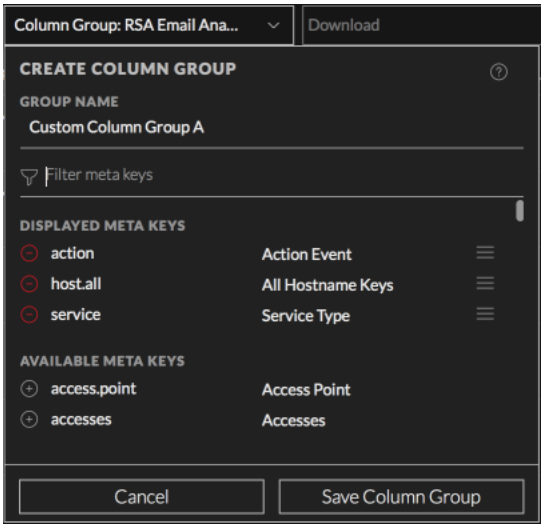
3. [+ **新しい列 グループ**]を選 択します。
   [列 グループの作 成]ダイアログが表 示されます。



4. [**グループ名**]フィールド に、新しい列 グループの一 意 の名 前(最 大256文 字) を入 力します(たとえば 「**Custom Column Group A**」) 。
5. 列 グループにメタ キーを追 加 するには、次 のように各 メタ キーを選 択して追 加します。
   a. [**メタ キーの絞り込 み**]フィールド にテキスト 文 字 列を入 力すると、そのテキストを含 んでいるメタ キーが[**選 択 可 能なメタ キー**]リストに表 示されます。

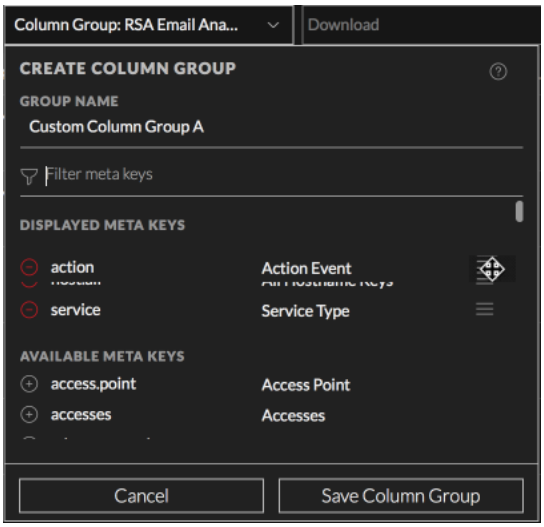


b. 追加するメタ キーが表示されたら、メタ キー名の前にある追加アイコン( ) をクリックします。[表示するメタ キー]リストの最後尾にメタ キーが追加されます(このリストも、入力したテキストで絞り込み表示されます) 。列グループに追加できるメタ キーの最大数は40個です。[表示するメタ キー]リストに含まれるメタ キーがすでに40個に達しているときに別のメタ キーを追加しようとすると、グループのメタ キーが最大数に達していることを示すメッセージが表示されます。



6. (オプション) 列グループ内のメタ キーを検索して削除するには、[**メタ キーの絞り込み**]フィールドにテキスト文字列を入力し、そのテキストを含んでいるメタ キーを[**表示するメタ キー**]リストから検索します。[**表示するメタ キー**]リストに削除したい列が表示されたら、メタ キー名の前にある削除アイコン( ) をクリックします。
メタ キーが[選択可能なメタ キー]リストに戻ります。
7. (オプション) [表示するメタ キー]リストでメタ キーの表示順を変更するには、リストの順序アイコン( ) の上にカーソルを置きます。カーソルがドラッグ アンド ドロップ アイコン( ) に変わったら、リス

ト内でメタ キーを上 下 にドラッグします。



8. 次 のいずれかを実 行します。
   a. カスタム列 グループを作 成せずにダイアログを閉じるには、[**キャンセル**]をクリックします。
   b. グループを作 成するには、[**列 グループを保 存**]をクリックします。
   新しい列 グループが保 存され、すべてのアナリストが使 用できるようになります。ボタンが[閉じる]と[列 グループを選 択]に変 わります。
9. 次 のいずれかを実 行します。
   a. ダイアログを閉じるには、[**閉じる**]をクリックします。
   b. ダイアログを閉じて新しい列 グループを選 択するには、[**列 グループを選 択**]をクリックします。
   新しいグループが[列 グループ]メニューに(アルファベット順 で) 追 加され、[イベント]リストが更 新されて、新しい列 グループの列 が表 示されます。

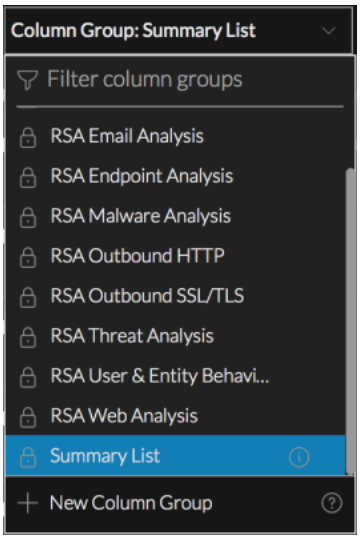
カスタム列 グループの削 除

[イベント]リストで現 在 適 用されていないカスタムの列 グループを削 除できます。標 準 提 供 の列 グループは読み取り専 用であり、削 除することはできません。カスタムの列 グループを削 除すると、標 準 提 供 の列 グループと削 除されていないグループのみが列 グループ メニューに表 示されます。

注 意 : 列 グループの削 除 の影 響 はグローバルであり、すべてのアナリストがそのグループを使 用できなくなります。

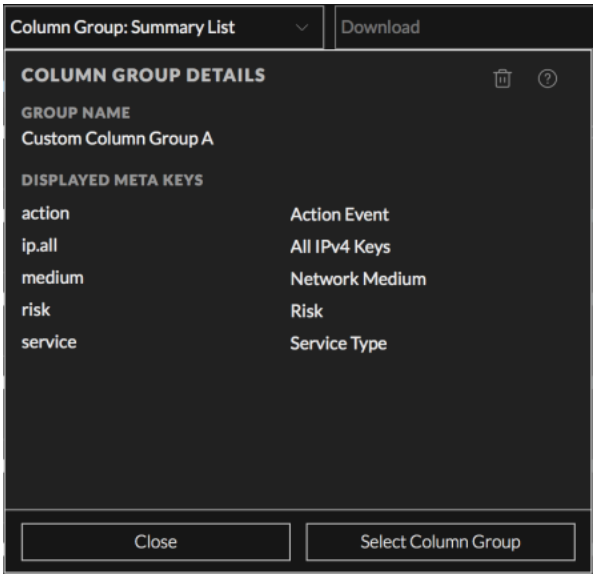
カスタムの列 グループを削 除するには、次 の手 順を実 行します。

1. **[調 査]＞[イベント]**に移 動し、 をクリックしてイベントをロードします。
   デフォルト サービスとデフォルトの時 間 範 囲 のイベントが[イベント]パネルにロードされます。
   [Summary List]列 グループまたは前 回 のセッションで使 用していた列 グループがリストに適 用されます。次 の図 は、[Summary List]列 グループが選 択されている初 期 状 態 のビューを示しています。
   [列 グループ]メニューのラベルに、選 択した列 グループの名 前 が表 示されます。



2. 列グループを削除するには、次の図に示すようにカスタム列グループをハイライト表示し、名前の右側の編集アイコン( ) をクリックします。

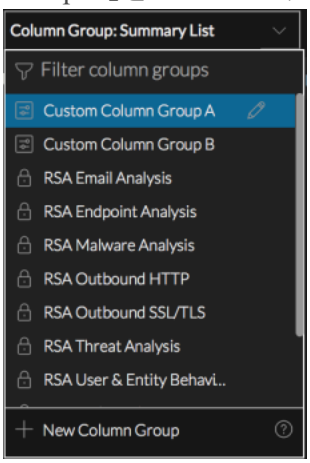
3. [列グループの詳細]ダイアログが開き、選択したグループの情報が表示されます。



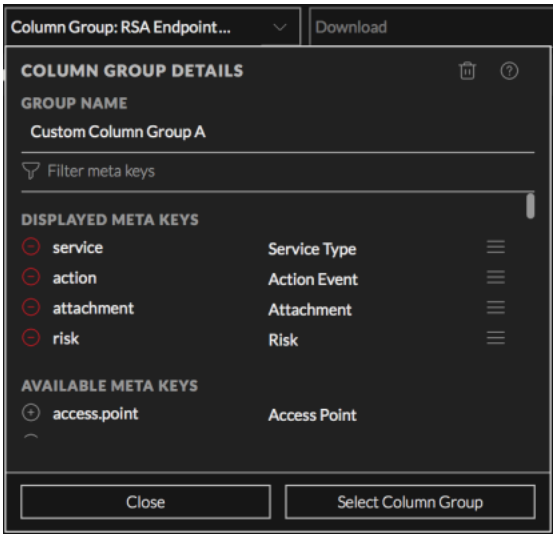
4. グループの削除アイコン( ) をクリックします。
列グループが現在使用中の場合は、次のメッセージが表示されます:`This column group cannot be deleted because it is currently active.`
列グループが使用中ではなく、標準提供の列グループではない場合、グループはただちに削除され、[列グループ]メニューから削除されます。削除した列グループは、調査を行うアナリストには表示されなくなります。列グループを削除する前に確認を求めるメッセージは表示されません。

カスタム列 グループの編 集

1. **[調査]＞[イベント]**に移 動して、クエリを送 信し、[イベント]パネルにデータをロードします。
2. [イベント]パネルのツールバーで、[**列グループ**]メニュー タイト ルをクリックします。
   メニューがド ロップダウンし、列 グループのリスト が表 示されます。[列 グループの絞り込み]フィールド がー 番 上 に、[+ 新しい列 グループ]オプションがー 番 下 に表 示されます。リスト の最 初 のグループがハイライト表 示され、選 択 中 のグループの背 景 は薄い青 色 になります。
3. 編 集する列 グループをハイライト表 示します。次 の図 は、ハイライト表 示された「Custom Column Group A」を示しています。編 集アイコンが右 側 に表 示されます。



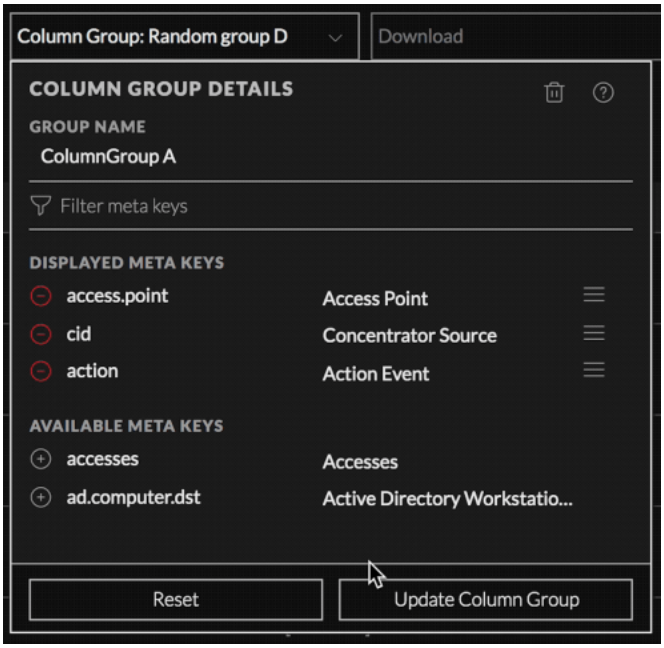
4. 編 集アイコン( ) をクリックします。
   [列 グループの詳 細]ダイアログが表 示され、グループ名 と表 示するメタ キーを編 集できるようになります。メタ キーの追 加または削 除に加え、リスト 内 のメタ キーの順 序 の変 更 が可 能です。



5. (オプション) [**グループ名**]フィールド で、列 グループの名 前を編 集します。
6. (オプション) 列 グループにメタ キーを追 加するには、次 のように各 メタ キーを選 択して追 加します。

a. [**メタ キーの絞り込み**]フィールドにテキスト文字列を入力すると、そのテキストを含んでいるメタ キーが[**選択可能なメタ キー**]リストに表示されます。または、リストをスクロールしてメタ キーを見つけます。

b. 追加したいメタ キーが表示されたら、メタ キー名の前にある追加アイコン( ) をクリックします。
[表示するメタ キー]リストの最後尾にメタ キーが追加されます(このリストも、入力したテキストで絞り込み表示されます) 。次の図は、グループ名が[Column Group A]に変更され、`access.point`が[表示するメタ キー]リストに追加された状態を示しています。



7. (オプション) 列グループ内のメタ キーを検索して削除するには、[**メタ キーの絞り込み**]フィールドにテキスト文字列を入力し、そのテキストを含んでいるメタ キーを[**表示するメタ キー**]リストから検索します。もしくは、単にリストをスクロールします。削除したい列が表示されたら、[**表示するメタ キー**]リストでメタ キー名の前にある削除アイコン( ) をクリックします。
メタ キーが[選択可能なメタ キー]リストに戻ります。
8. (オプション) [表示するメタ キー]リストでメタ キーの表示順を変更するには、リストの順序アイコン( ) の上にカーソルを置きます。カーソルがドラッグ アンド ドロップ アイコン( ) に変わったら、リスト内でメタ キーを上下にドラッグします。
9. 次のいずれかを実行します。
a. カスタムの列グループに対する変更を保存せずにダイアログを閉じるには、[**リセット**]をクリックします。
b. 列グループの編集内容を保存するには、[**列グループを更新**]をクリックします。
更新された列グループがすべてのアナリストに対してグローバルに保存され、ボタンが[閉じる]と[列グループを選択]に変わります。

10. 次のいずれかを実行します。
    a. ダイアログを閉じるには、[**閉じる**]をクリックします。
    b. ダイアログを閉じて更新された列グループを選択するには、[**列グループを選択**]をクリックします。
    列グループが更新され、[イベント]リストが更新されて新しい列グループの列が表示されます。

列グループと列の選択(11.3以前の[イベント分析]ビュー)

11.3以前の[イベント分析]ビューでは、[イベント]リストに適用する列グループを選択できます。標準提供の列グループと[レガシー イベント]ビューで作成されたカスタムの列グループがあります。

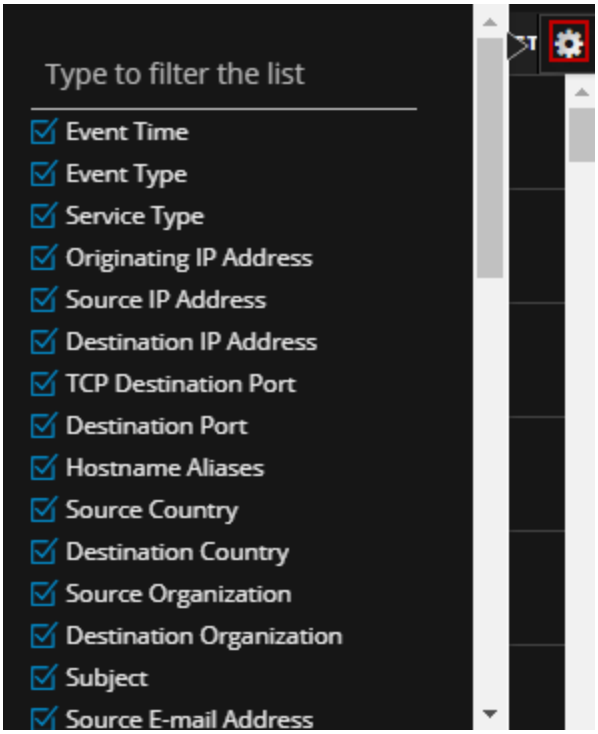
列グループを選択するには、次の手順を実行します。

[列グループ]メニューで、次のいずれかを実行します。

1. 列グループを選択します(たとえば[**Summary List**])。
2. 列グループのリストを絞り込むには、列グループ名を入力します。1文字を入力すると、その文字を含む列グループのリストが表示されます。入力を続けると、入力に合わせてリストが絞り込まれていきます。目的の列グループが表示されたら、それをクリックして選択します。フィルタのテキストをクリアするには、[**X**]をクリックするか、入力したテキストを削除します。
   選択した列グループに含まれる列のデータが[イベント]パネルに表示されます。

表示する列を選択するには、次の手順を実行します。

1. [イベント]リストが開き、列グループが選択された状態で、⊞をクリックして列セレクターを表示します。



2. 列に追加したいメタ キーを選択するか、メタ キーの名前を入力します。

3. 列に表示したくないメタ キーがある場合は、メタ キーの選択を解除します。
   選択した列を使用してデータが再表示されます。

[レガシー イベント]ビューでの列グループの操作

このセクションでは、11.4の[レガシー イベント]ビュー(および11.3の[イベント]ビュー) の操作手順について説明します。ハードコードされた列を含む3種類のイベント リストが組み込まれており、それぞれ詳細ビュー、リスト ビュー、ログ ビューと呼ばれます。列の削除、列の順序の変更、幅の変更を行うことができます。標準提供またはカスタムの列グループも使用できます。これにより、列をより柔軟に選択できるようになります。

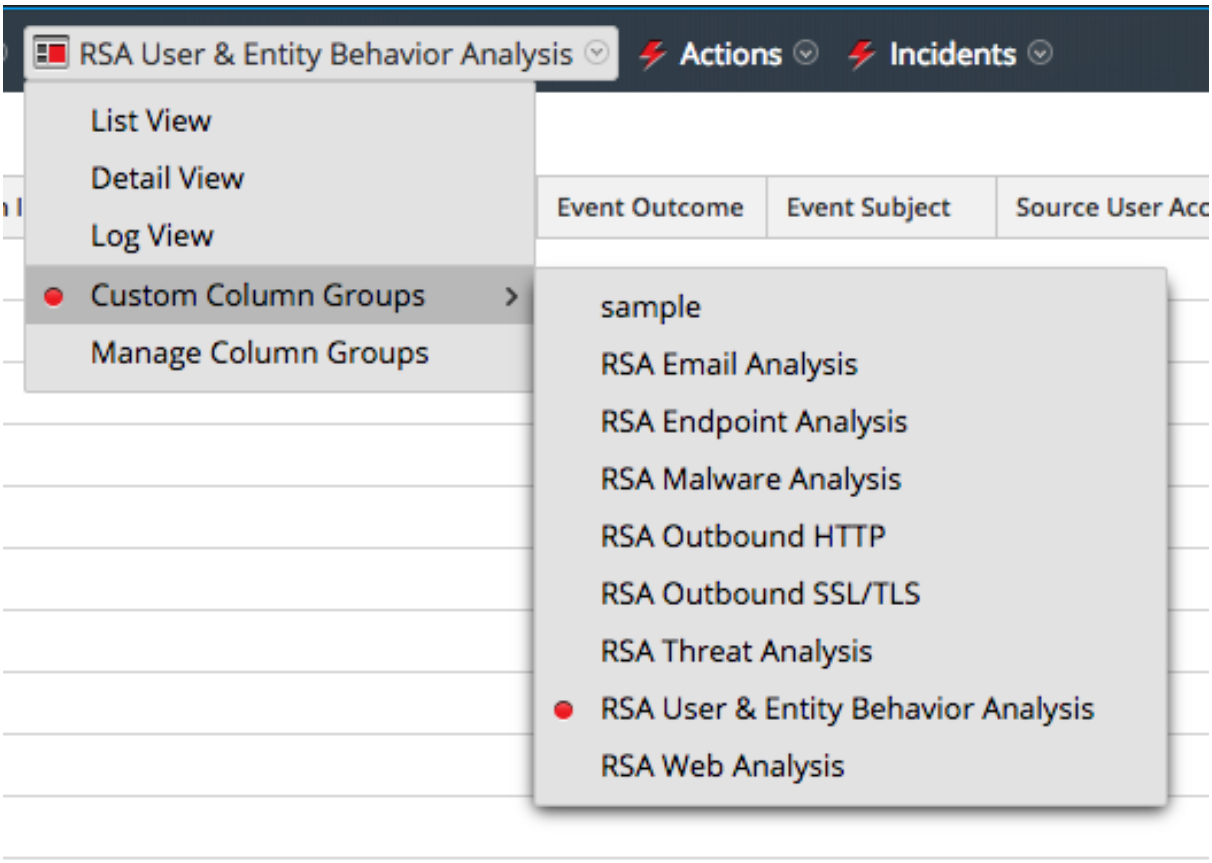
列グループは、調査の中で、グローバルに共有され、サービスごとに定義されます。カスタムの列グループに対して行った変更はすべてグローバルに適用され、サービスを使用しているすべてのアナリストに影響します。列グループを削除すると、サービスを調査するすべてのアナリストがその列グループを使用できなくなります。

列グループの選択

注: 調査のプロファイルに、カスタム列グループを含めることができます。カスタム列グループがプロファイルで使用されていて、カスタム列グループを使用して[レガシー イベント]ビューでイベントを表示している場合は、ビューのタイプ(詳細、リスト、ログ) を変更できません。

列グループを選択するには、次の手順を実行します。

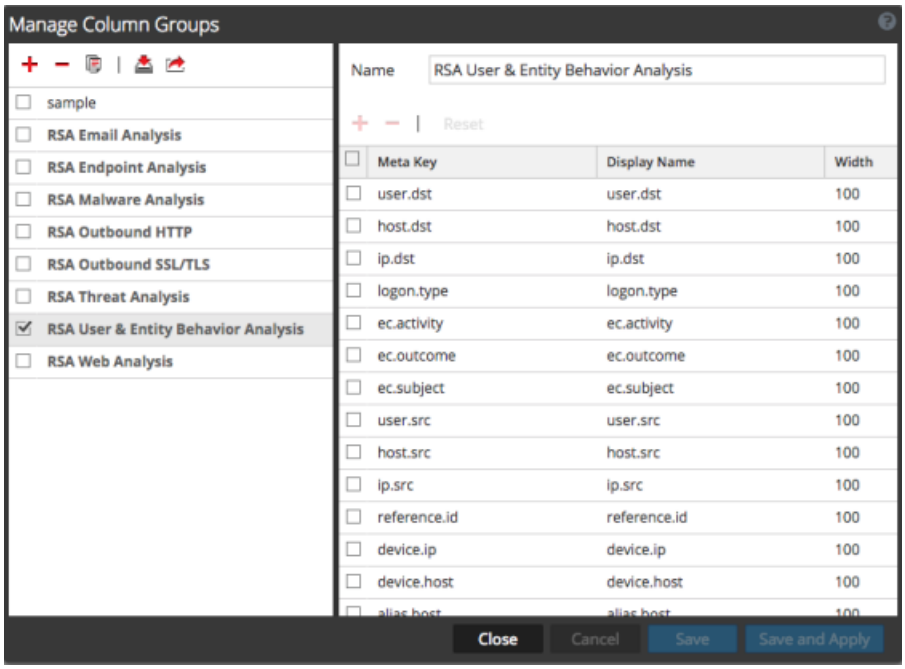
1. [レガシー イベント]ビューを開き、[**ビュー**]ドロップダウン メニューから[**カスタム列グループ**]を選択します。メニュー ラベルには、選択中のオプション(詳細ビュー、リスト ビュー、ログ ビュー、現在選択されている列グループ) が表示されます。



2. サブメニューから列 グループのいずれかを選 択します。
レガシー イベントビューが更 新され、カスタムの列 グループが反 映されます。

[レガシー イベント]ビューでのカスタム列 グループの作 成

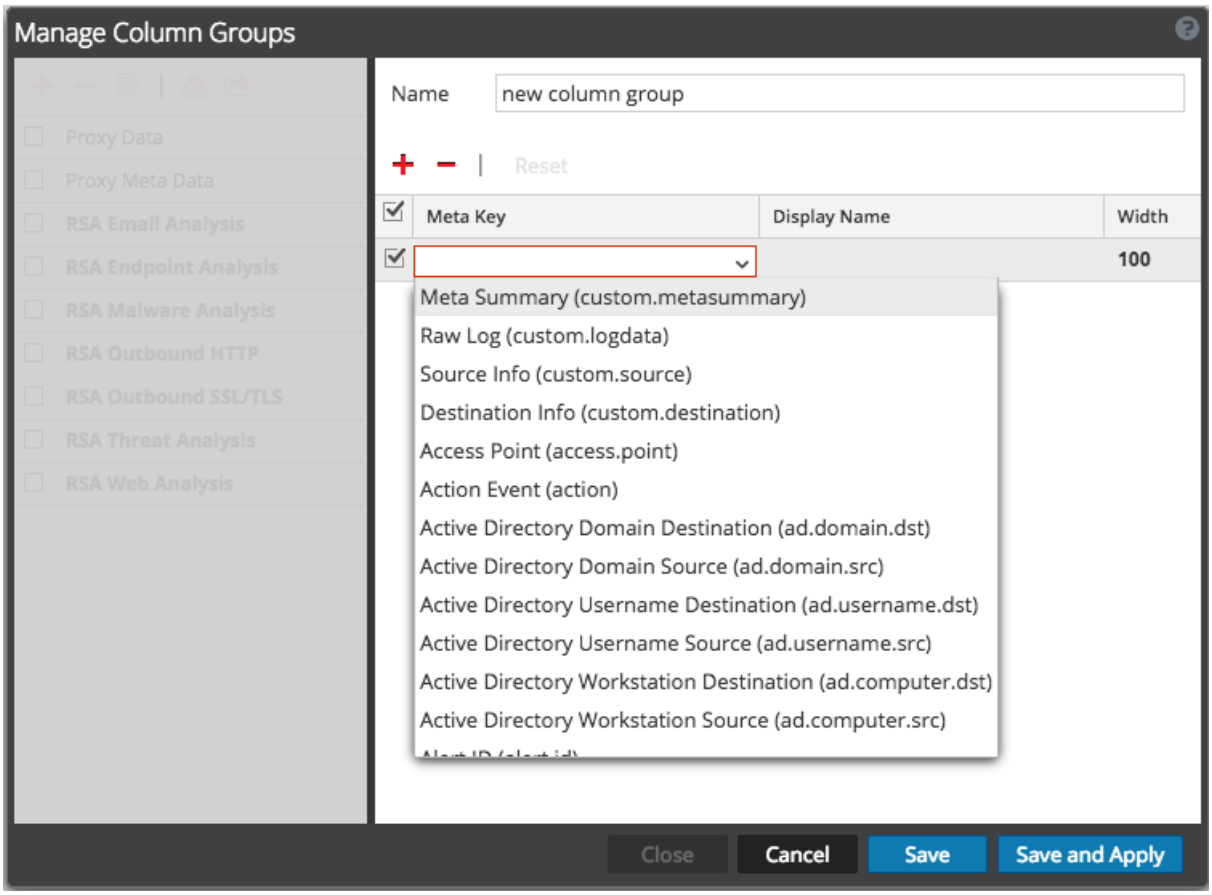
1. **[調 査]＞[レガシー イベント]**に移 動します。
2. [**ビュー**]ドロップダウン メニューから[**列 グループの管 理**]を選 択します。[ビュー]ドロップダウン メニューのラベルには、現 在 選 択 中 のオプション(詳 細ビュー、リスト ビュー、ログ ビュー、現 在 選 択 されている列 グループ名 など) が表 示されます。
[列 グループの管 理]ダイアログが表 示されます。



3. 列グループ パネルに新しい列グループを追加するには、＋をクリックし、表示されたフィールドに新しいグループの名前を入力します。
   列定義パネルが右側に表示され、グループ名が入力されます。グループ名を編集することもできます。

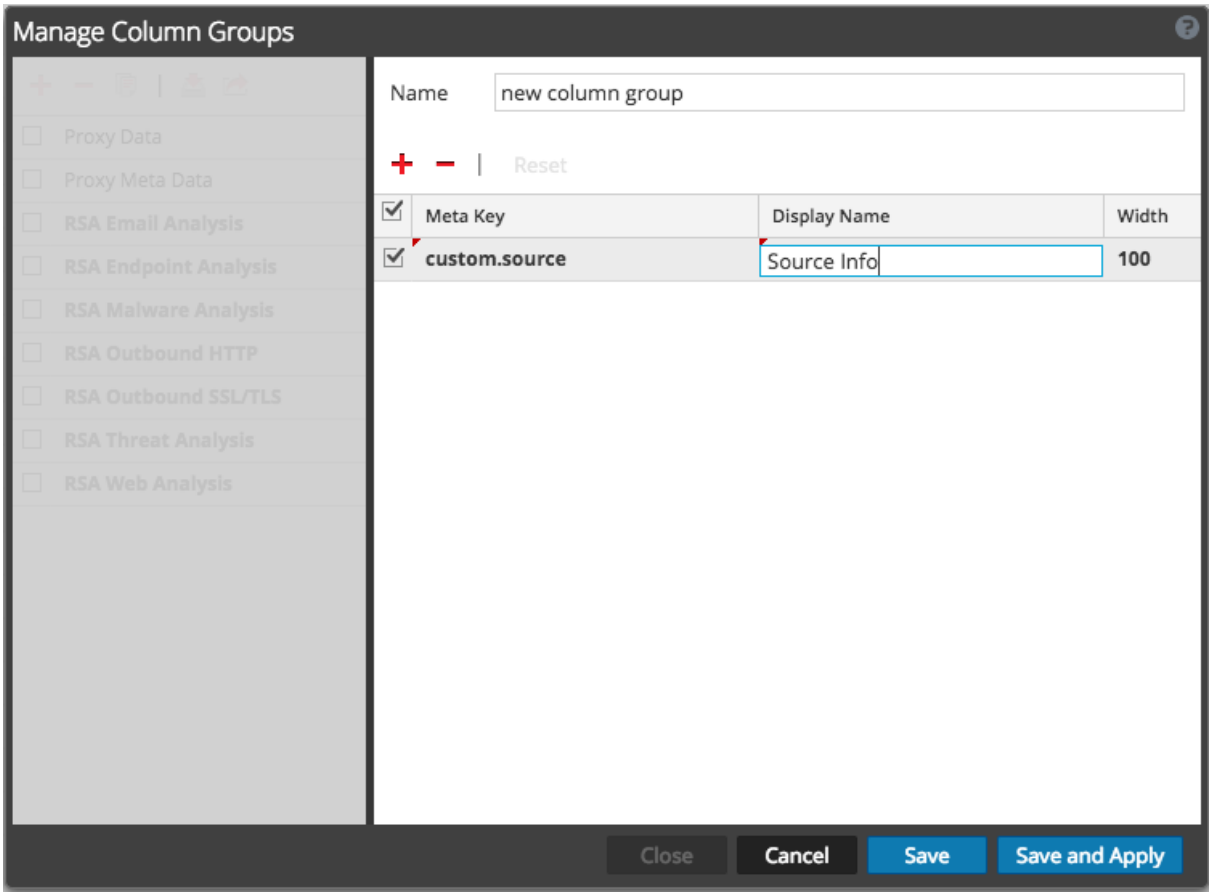
4. グループに列を追加するには、＋をクリックします。追加された空の[**メタ キー**]フィールドをクリックし、[**メタ キー**]ドロップダウン リストを表示します。リストからメタ キー フィールドを選択します。この

手順を、列セットが完成するまで繰り返します。



5. (オプション) 列グループからメタ キーを削除するには、−をクリックします。
6. (オプション) [イベント] リストに表示される列の順序を変更するには、メタ キーをドラッグして適切な位置に移動します。

7. (オプション) 列のデフォルトの幅を設定するには、[**幅**]列にある目的の値をクリックして、新しい列の幅を入力します。

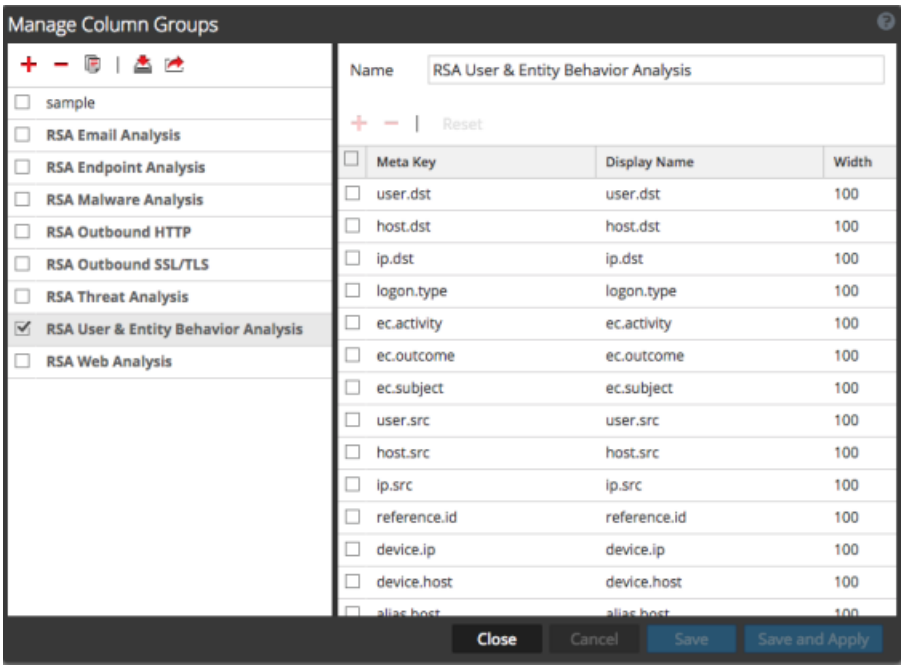


8. (オプション) 列グループを以前の設定に復元し、これまでに加えた変更をすべて取り消すには、[**キャンセル**]をクリックします。
9. 保存する準備ができたら、次のいずれかを実行します。
   a. 編集した列グループを保存し、その列グループの設定を使って[レガシー イベント]ビューを更新するには、[**保存して適用**]をクリックします。
   b. [レガシー イベント]ビューを更新せずに、編集した列グループを保存するには、[**保存**]をクリックします。

列グループの削除 ([レガシー イベント]ビュー)

1. [**調査**]>[**レガシー イベント**]に移動します。
2. [**ビュー**]ドロップダウン メニューから[**列グループの管理**]を選択します。[ビュー]ドロップダウン メニューのラベルには、現在選択中のオプション(詳細ビュー、リスト ビュー、ログ ビュー、現在選択されている列グループ名など)が表示されます。

[列グループの管理]ダイアログが表示されます。

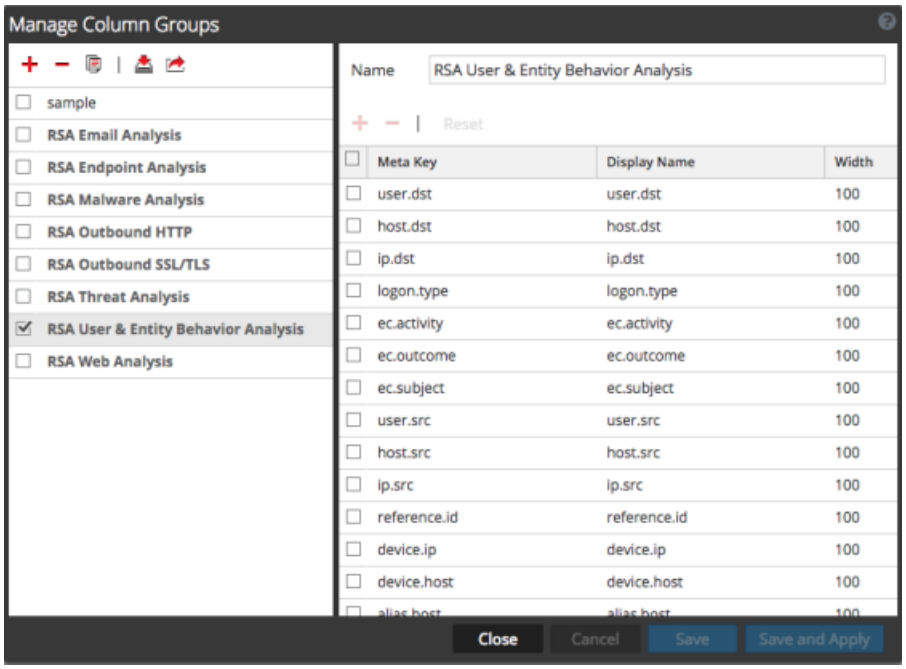


3. 列グループ パネルでカスタム列グループを削除するには、1つまたは複数のカスタム列グループを選択し、ツールバーの－をクリックします。
確認を求めるメッセージが表示されます。
4. 次のいずれかを実行します。
   a. 列グループを削除して[レガシー イベント]ビューを更新するには、[**はい**]をクリックします。
   b. 列グループを削除しない場合は、[**いいえ**]をクリックします。
   選択した列グループが削除され、どこにも表示されなくなります。

列グループの編集 ([イベント]ビュー)

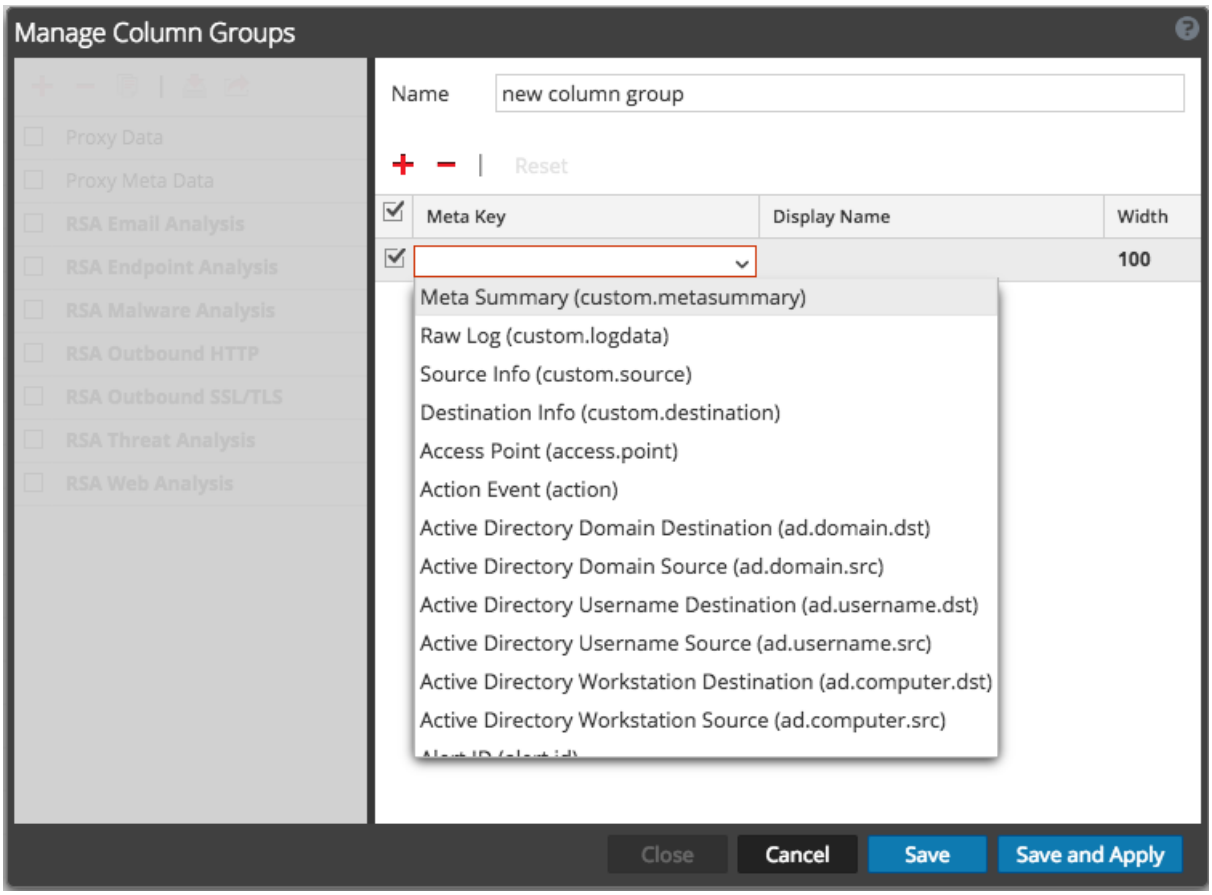
1. **[調査]＞[レガシー イベント]**に移動します。
2. [**ビュー**]ドロップダウン メニューから[**列グループの管理**]を選択します。[ビュー]ドロップダウン メニューのラベルには、現在選択中のオプション(詳細ビュー、リスト ビュー、ログ ビュー、現在選択されている列グループ名など) が表示されます。

[列グループの管理]ダイアログが表示されます。



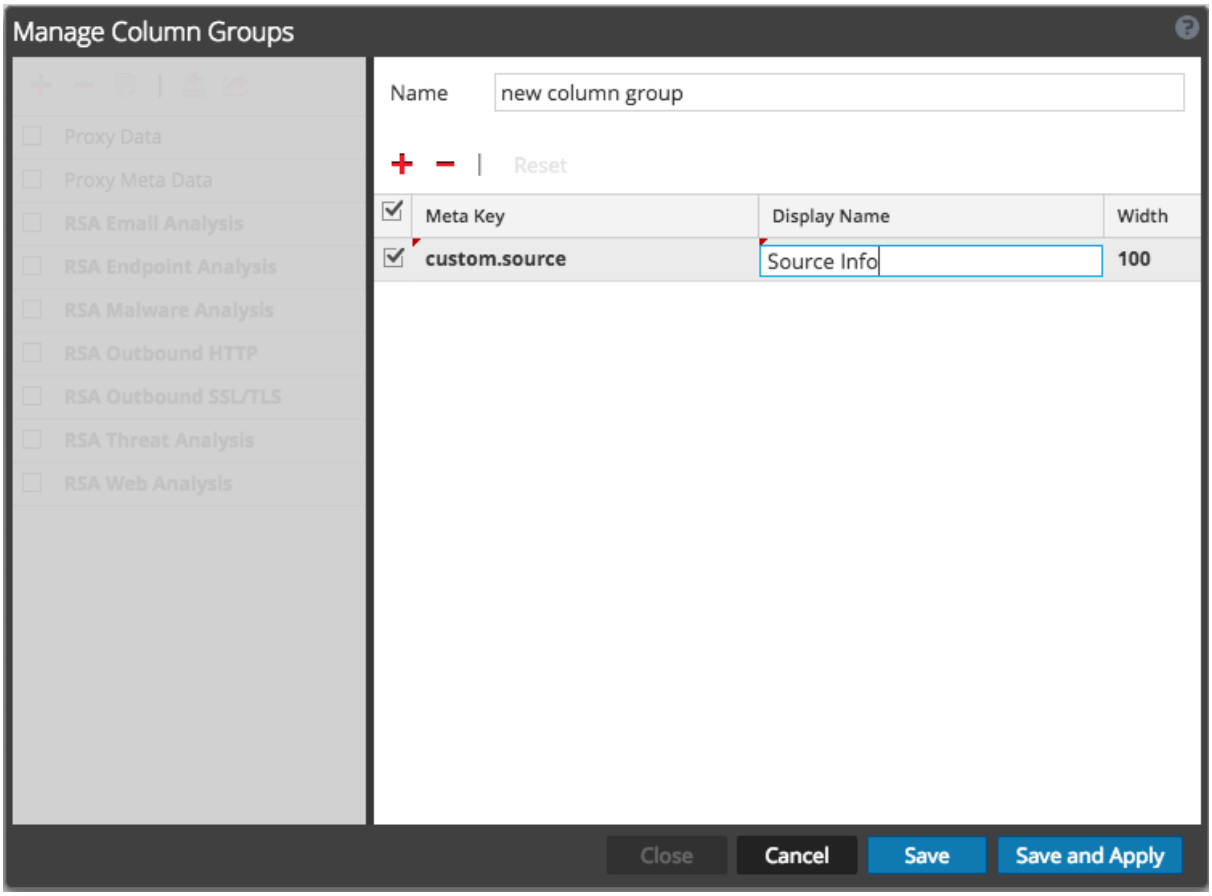
3. 次のいずれかを実行します。
   a. 列グループ パネルでカスタム列グループを編集するには、名前の前にあるチェックボックスを選択します。
      列定義パネルが右側に表示されます。
   b. 標準提供の列グループまたはカスタムの列グループを複製してから編集するには、名前の前にあるチェックボックスを選択して、複製アイコン( ) をクリックします。
      列定義パネルが右側に表示されます。
4. (オプション) グループの複製を編集している場合は、グループの新しい名前を入力します。
5. グループに列を追加するには、 をクリックします。追加された空の[**メタ キー**]フィールドをクリックし、[**メタ キー**]ドロップダウン リストを表示します。リストからメタ キー フィールドを選択します。この

手順を、列セットが完成するまで繰り返します。



6. (オプション) 列グループからメタ キーを削除するには、−をクリックします。
7. (オプション) [イベント] リストに表示される列の順序を変更するには、メタ キーをドラッグして適切な位置に移動します。

8. (オプション) 列のデフォルトの幅を設定するには、[**幅**]列にある目的の値をクリックして、新しい列の幅を入力します。



9. (オプション) 列グループを以前の設定に復元し、これまでに加えた変更をすべて取り消すには、[**キャンセル**]をクリックします。
10. 保存する準備ができたら、次のいずれかを実行します。
    a. 編集した列グループを保存し、その列グループの設定を使って[レガシー イベント]ビューを更新するには、[**保存して適用**]をクリックします。
    b. [レガシー イベント]ビューを更新せずに、編集した列グループを保存するには、[**保存**]をクリックします。

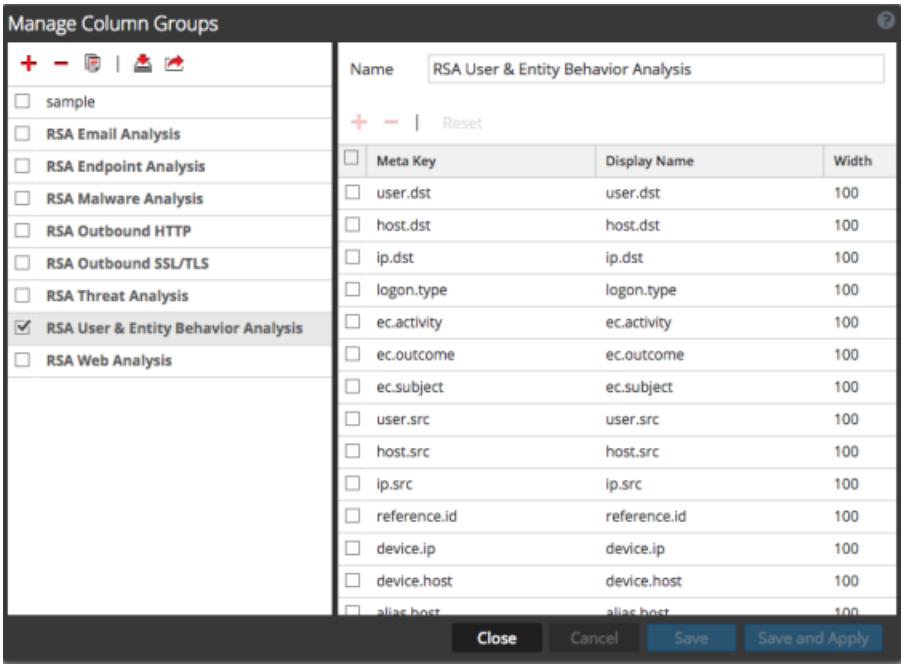
列グループのインポートとエクスポート([レガシー イベント]ビュー)

カスタムの列グループをエクスポートして他のチーム メンバーと共有できます。エクスポートしたファイルのコピーを他のアナリストに提供すれば、そのアナリストは列グループをインポートできます。

列グループをエクスポートするには、次の手順を実行します。

1. [**調査**]>[**レガシー イベント**]に移動します。
2. [**ビュー**]ドロップダウン メニューから[**列グループの管理**]を選択します。[ビュー]ドロップダウン メニューのラベルには、現在選択中のオプション(詳細ビュー、リスト ビュー、ログ ビュー、現在選択さ

れている列グループ名など) が表示されます。これらのビューはそれぞれ異なる形式のイベント リストであり、各列が1つのメタ キーを表します。
[列グループの管理]ダイアログが表示されます。



3. 列グループをエクスポートするには、名前の前にあるチェックボックスを選択して、[エクスポート]オプション( ) をクリックします。
列グループが.jsnファイル(たとえばCustomColumnGroupsExport.jsn) としてローカルのファイル システムにエクスポートされます。別のグループをエクスポートする場合は、その次のファイルには、重複を避けるためCustomColumnGroupsExport-2.jsnという名前が付けられます。

4. ローカル ファイル システムに保存した列グループをインポートするには、[インポート]オプション( ) をクリックします。
[列グループのインポート]ダイアログが表示されます。

5. ローカルドライブを参照して列グループ(jsnファイル) を見つけて、[**アップロード**]をクリックします。
列グループがリストに追加されます。同名の既存の列グループが存在する場合は、メッセージが表示され、列グループはインポートされません。

クエリ プロファイルを使 用した調 査 の共 通 領 域 のカプセル化

クエリ プロファイルは、[ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビューに適 用 できるメタ グループ、列 グループ、および制 限 クエリ(プレクエリ) を迅 速 かつ簡 単 に定 義 する方 法 を提 供 します。

注 : バージョン11.4には、以 前 のバージョンで[イベント分 析]ビューと呼 ばれていた単 一 の[イベント] ビューがあります。バージョン11.3以 前 の[レガシー イベント]ビューは、管 理 者 が『*システム構 成 ガイド*』の説 明 に従 ってこのビューを有 効 にしている場 合 は、引 き続 き使 用 できます。[レガシー イベント] ビューが有 効 になっている場 合 は、[調 査]サブメニューから両 方 のビューにアクセスできます。

NetWitness Platformには、RSA Email Analysis、RSA Endpoint Analysis、RSA File Analysis、RSA Threat Analysis、RSA User & Entity Behavior Analysis、RSA Web Analysisいう標 準 提 供 のプロファイ ルがあります。標 準 提 供 プロファイルはそれぞれ、標 準 提 供 のメタ グループや列 グループを指 定 し、調 査 のタイプに適 したプレクエリが含 まれる場 合 もあります。標 準 提 供 のクエリ プロファイルを使 用 すると、 特 定 の分 野 のクエリを簡 単 に行 うことができます。たとえば、標 準 提 供 のRSA Email Analysisプロファイ ルを選 択 すると、メール アクティビティの調 査 に最 も役 立 つメタ キー、メタ グループ、メタ列 が自 動 的 に 選 択 されます。メタ キーに慣 れてきたら、独 自 のカスタム クエリ プロファイルを作 成 できます。

クエリ プロファイルでは、次 の処 理 が行 われます。

- メタ グループは、クエリ対 象 のメタ キーを定 義 します(「メタ グループを使 用 して関 連 性 の高 いメタ キーにフォーカス」を参 照) 。
- 列 グループは、メタ グループのどのメタ キーを[イベント]リストの列 として表 示 するかを定 義 します。デ フォルトでは、列 グループの最 初 の15列 のみが表 示 されます。これをベースに、列 の追 加 、削 除 、並 べ替 えを行 うことができます(列 グループの詳 細 については、「イベント リストでの列 と列 グループの使 用 」を参 照 してください) 。
- プレクエリは、ユーザが作 成 するクエリの先 頭 に制 限 フィルタを追 加 します。

標 準 提 供 プロファイル名 は、「RSA」で始 まり、[Default Profiles]の下 に表 示 されます。標 準 提 供 プロ ファイルを編 集 または削 除 することはできませんが、[ナビゲート]ビューまたは[レガシー イベント]ビュー で既 存 のプロファイルをコピーして、コピーを編 集 できます。[**ナビゲート**]ビューまたは[**レガシー イベント**] ビューのツールバーで、**[プロファイル]＞[プロファイルの管 理]**を選 択 します。

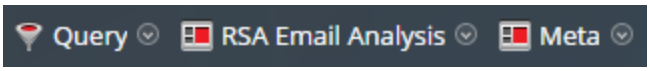
注 : クエリ プロファイルは[ナビゲート]ビュー、[レガシー イベント]ビュー、[イベント]ビューで使 用 で き、ユーザ間 でグローバルに共 有 されます。あるユーザがクエリ プロファイルを変 更 または削 除 すると、 その他 のユーザにも影 響 を与 えます。

[クエリ プロファイルの作 成]ダイアログと[プロファイルの管 理]ダイアログでは、独 自 のカスタム プロファイ ルを作 成 できます。[プロファイルの管 理]ダイアログには、[クエリ プロファイルの作 成]ダイアログに表 示 されないオプションがあります。

- [プロファイルの管 理]ダイアログ([ナビゲート]ビューと[レガシー イベント]ビュー) では、プロファイルと プロファイル グループの構 成 、追 加 、削 除 、インポート、エクスポートを行 うことができます。カスタムの クエリ プロファイルをプロファイル グループに整 理 できます(バージョン11.2以 降) 。以 前 のバージョンか らバージョン11.4にアップグレードする場 合 、プロファイルを含 んだプロファイル グループのみがインポート されます。
- [クエリ プロファイル]メニュー(11.4の[イベント]ビュー) では、クエリ プロファイルを選 択 して適 用 できま す。このメニューのオプションを使 用 して、カスタム クエリ プロファイルの作 成 ([クエリ プロファイルの作

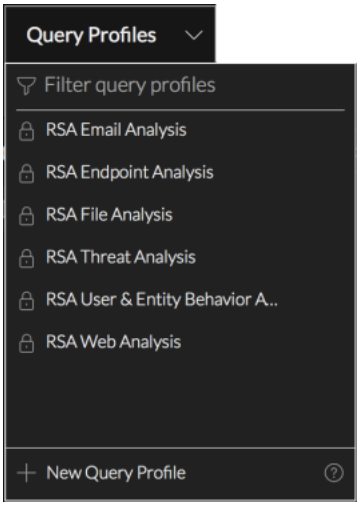
成]ダイアログ)、編集、削除([クエリ プロファイルの詳細]ダイアログ)を行うことができます。バージョン11.4の[イベント]ビューでは、他のビューで定義されたメタ グループやプロファイル グループは使用されません。

次の図は、[ナビゲート]ビューまたは[レガシー イベント]ビューで「RSA Email Analysis」クエリ プロファイルが選択された状態を示しています。クエリ プロファイル名は、[クエリ]オプションの右側に表示されます。クエリ プロファイルがアクティブである場合、[プロファイル]メニューのラベルには、アクティブなクエリ プロファイル名が表示されます。



バージョン11.2以降の[ナビゲート]ビューと[レガシー イベント]ビューでは、クエリ プロファイルをグループ化できます。標準提供のクエリ プロファイルは、[Default Profiles]グループに含まれ、変更することはできません。アナリストは新しいクエリ プロファイル グループを作成して、誰でも使用できるようにすることができます。プロファイルの作成後、プロファイル グループを編集して、プロファイルの追加、削除、別のグループへの移動を行うことができます。プロファイルを作成しても、デフォルトではプロファイル グループには追加されません。

次の図は、バージョン11.4の[イベント]ビューに表示される[クエリ プロファイル]メニューを示しています。このメニューには、[ナビゲート]ビューおよび[レガシー イベント]ビューで使用するのと同じプロファイルのリストが表示されます。プロファイルの作成、編集、削除、適用が可能です。



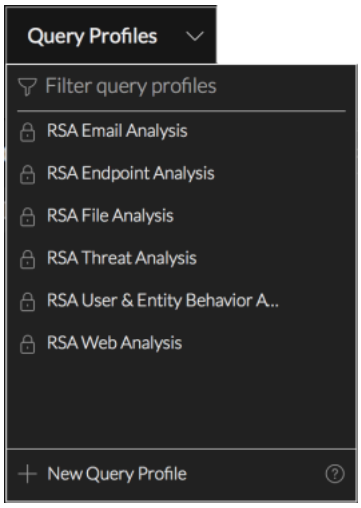
[レガシー イベント]ビューで作成されたクエリ プロファイルが、列グループではなくログ ビュー、詳細ビュー、リスト ビューを使用している場合、11.4の[イベント]ビューの同じプロファイルは、[Summary List]列グループを使用します。

クエリ プロファイルの詳細の表示([イベント]ビュー)

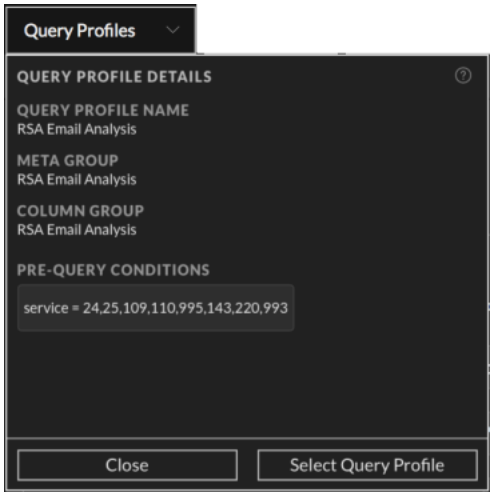
クエリ プロファイルにどのメタ グループ、列グループ、制限クエリ(プレクエリ)が定義されているかを確認する場合は、プロファイルの詳細を表示します。

詳細を確認するには、次の手順を実行します。

1. **[調査]>[イベント]**に移動し、クエリ バーの[**クエリ プロファイル**]をクリックします。
   [クエリ プロファイル]メニューが開き、使用可能なプロファイルのリストが表示されます。



2. クエリ プロファイルの上にカーソルを合わせ、情報アイコン( ) をクリックすると、プロファイルに構成されたメタ グループ、列 グループ、プレクエリが表示されます。
次の図は、標準提供プロファイルの1つであるRSA Email Analysisプロファイルの詳細を示しています。

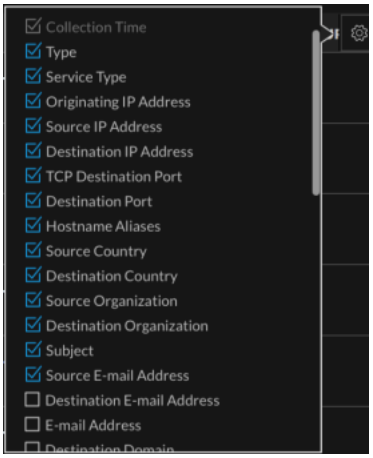


3. 次のいずれかを実行します。

   a. ダイアログを閉じるには、[**閉じる**]をクリックします。

   b. プロファイルを適用する場合は、[**クエリ プロファイルを選択**]をクリックします。
   ダイアログが閉じます。選択したクエリ プロファイルが反映され、[イベント]リストの表示が更新されます。プロファイルで別の列 グループが使用されている場合は、選択されたプロファイルのプレクエリと列 グループを使用してクエリが再実行されます。プレクエリのみが異なる場合は、クエリ バーの既存のフィルタが削除され、プレクエリ フィルタ(例 : 「`service=24,25,109,110,995,143,220,993`」) がクエリ バーに追加されます。[イベント]リストには、関連づけられた列 グループの最初の15列が表示されます。クエリを実行する前に、列を調整したり、別のフィルタを作成して追加することができます。

c. 関連づけられた列グループから別の列を選択する場合は、右側の[イベント]リストの上にあるをクリックします。
列の選択リストが表示され、表示する列を最大40個選択できます(「イベント リストでの列と列グループの使用」を参照してください)。



クエリ プロファイルの適用([イベント]ビュー)

十分な結果または適切な結果が[イベント]ビューに表示されない場合は、適用されたプロファイルがプレクエリで結果を制限している可能性があります。プレクエリが適用されている場合は、クエリ バーの先頭にプレクエリ フィルタが表示されます。

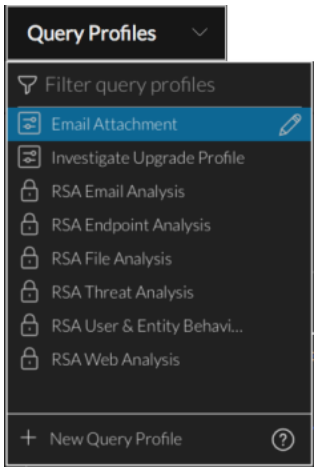
クエリ プロファイルを選択するには、次の手順を実行します。

1. [**イベント**]ビューのツールバーで、[**クエリ プロファイル**]をクリックします。
[クエリ プロファイル]メニューが開き、使用可能なプロファイルのリストが表示されます。
2. 上下矢印キーまたはマウスを使用して、プロファイルをハイライト表示します。
3. ハイライト表示されたプロファイルをクリックします。
クエリ プロファイルの設定がただちに適用されます。選択したクエリ プロファイルが反映され、[イベント]リストの表示が更新されます。プロファイルで別の列グループが使用されている場合は、選択されたプロファイルのプレクエリと列グループを使用してクエリが再実行されます。プレクエリのみが異なる場合は、クエリ バーの既存のフィルタが削除され、プレクエリ フィルタがクエリ バーに追加されます。ボタンがアクティブになり、新しいプレクエリ フィルタを使用してクエリを再送信できるようになります。クエリを再送信する前または後に、通常どおりに他のフィルタを追加できます。

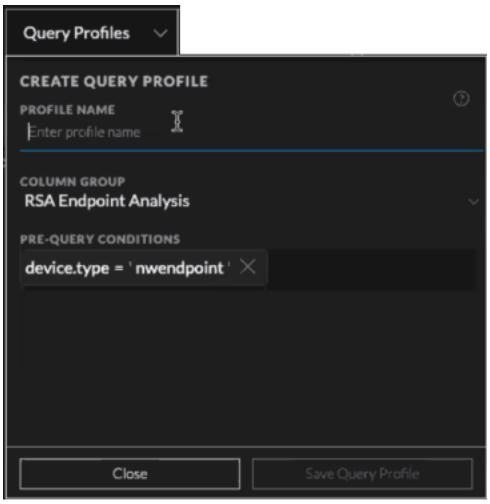
カスタム クエリ プロファイルの作成または編集([イベント]ビュー)

カスタム クエリ プロファイルを作成または編集するには、次の手順を実行します。

1. [**イベント**]ビューのツールバーで、[**クエリ プロファイル**]をクリックします。
[クエリ プロファイル]メニューが開き、使用可能なプロファイルのリストが表示されます。



2. 次のいずれかを実行します。
   a. 新しいクエリ プロファイルを作成するには、[+ **新しいクエリ プロファイル**]をクリックします。
   b. 既存のクエリプロファイルを編集するには、メニュー内のカスタム クエリ プロファイルをハイライト表示し、編集( ) アイコンをクリックします。
   [クエリ プロファイルの作成]ダイアログまたは[クエリ プロファイルの詳細]ダイアログが表示されます。次の図は、クエリ バーの既存のフィルタがプレクエリとして追加された、新しい空のプロファイルを示しています。

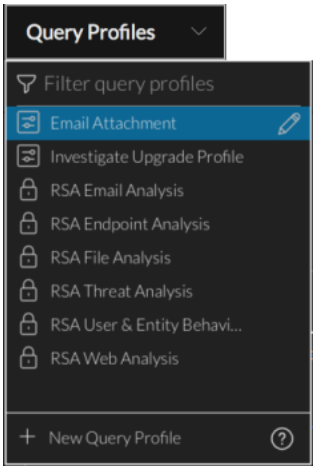


3. [**プロファイル名**]フィールドに、80文字以下の一意のプロファイル名を入力します。
4. [**列グループ**]ドロップダウン リストから列グループを選択します。
5. [**プレクエリ**]フィールドで、クエリ バーからコピーされたデフォルトのプレクエリを確認し、必要に応じてフィルタを追加します。
6. [**クエリ プロファイルを保存**]または[**クエリ プロファイルを更新**]をクリックします。
   新しいプロファイルが保存されるか、編集したプロファイルが更新されます。
7. ダイアログを閉じるには、[**閉じる**]をクリックします。

カスタム クエリ プロファイルの削 除 ([イベント]ビュー)

カスタム クエリ プロファイルを削 除 するには、次 の手 順 を実 行 します。

1. [**イベント**]ビューのツールバーで、[**クエリ プロファイル**]をクリックします。
   [クエリ プロファイル]メニューが開き、使 用 可 能 なプロファイルのリストが表 示 されます。

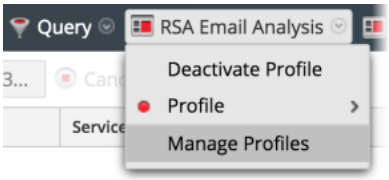


2. 削 除 するカスタム クエリ プロファイルをメニューでハイライト表 示 して、編 集 ( ) アイコンをクリックします。
   [クエリ プロファイルの詳 細]ダイアログが表 示 されます。

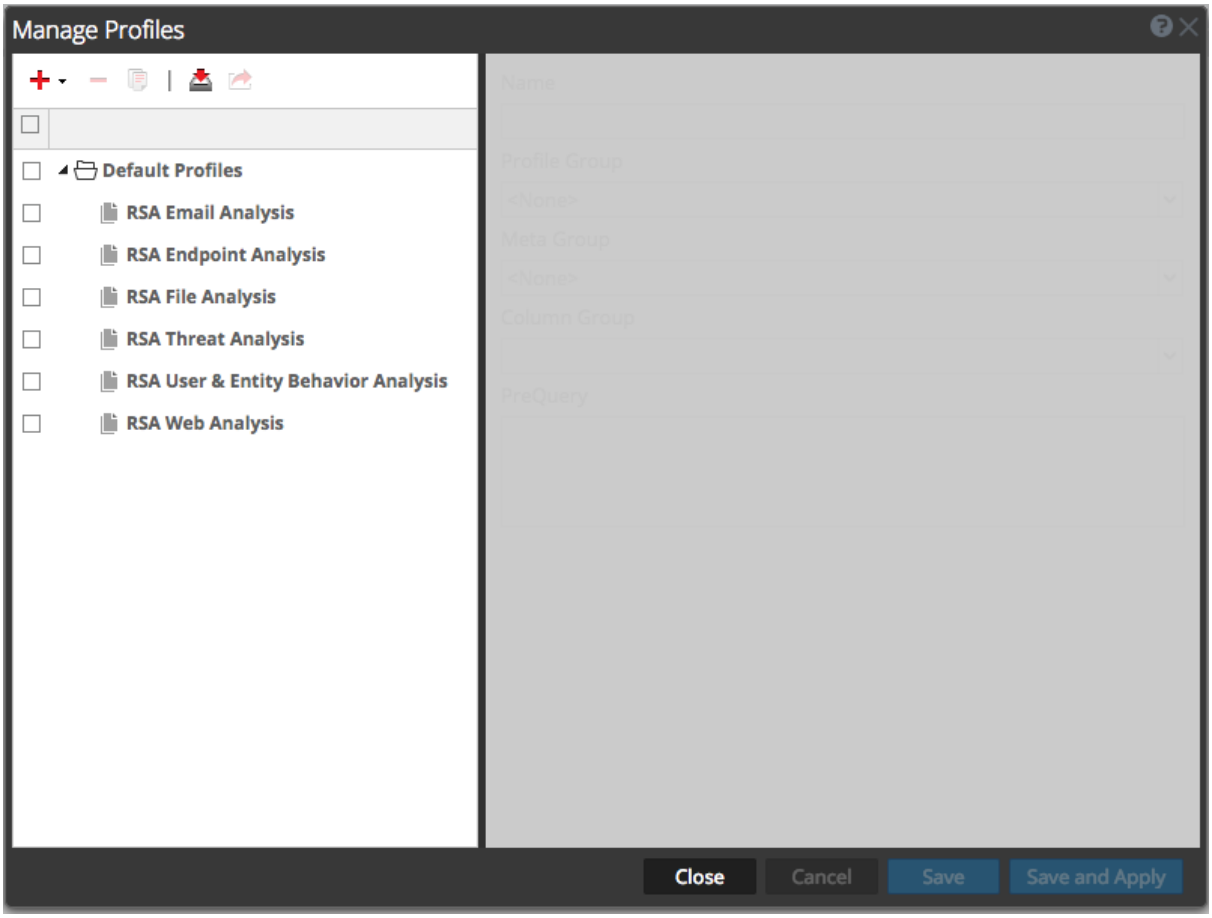
3. 削 除 アイコン( ) をクリックします。
   プロファイルが削 除 されます。この操 作 を元 に戻 すことはできません。すべてのアナリストがこのプロファイルを使 用 できなくなります。

[プロファイルの管 理]ダイアログの表 示([ナビゲート]ビューと[レガシー イベント]ビュー)

1. [**調 査**]＞[**ナビゲート**]または[**レガシー イベント**]に移 動します([**調 査**]ダイアログが表 示されている場 合 は、サービスを選 択して[**ナビゲート**]をクリックします) 。
2. ツールバーで、[**プロファイル**]＞[**プロファイルの管 理**]を選 択します。



[プロファイルの管 理]ダイアログが表 示されます。



プロファイル グループの作成、編集、削除 ([ナビゲート]ビューまたは[レガシー イベント]ビュー)

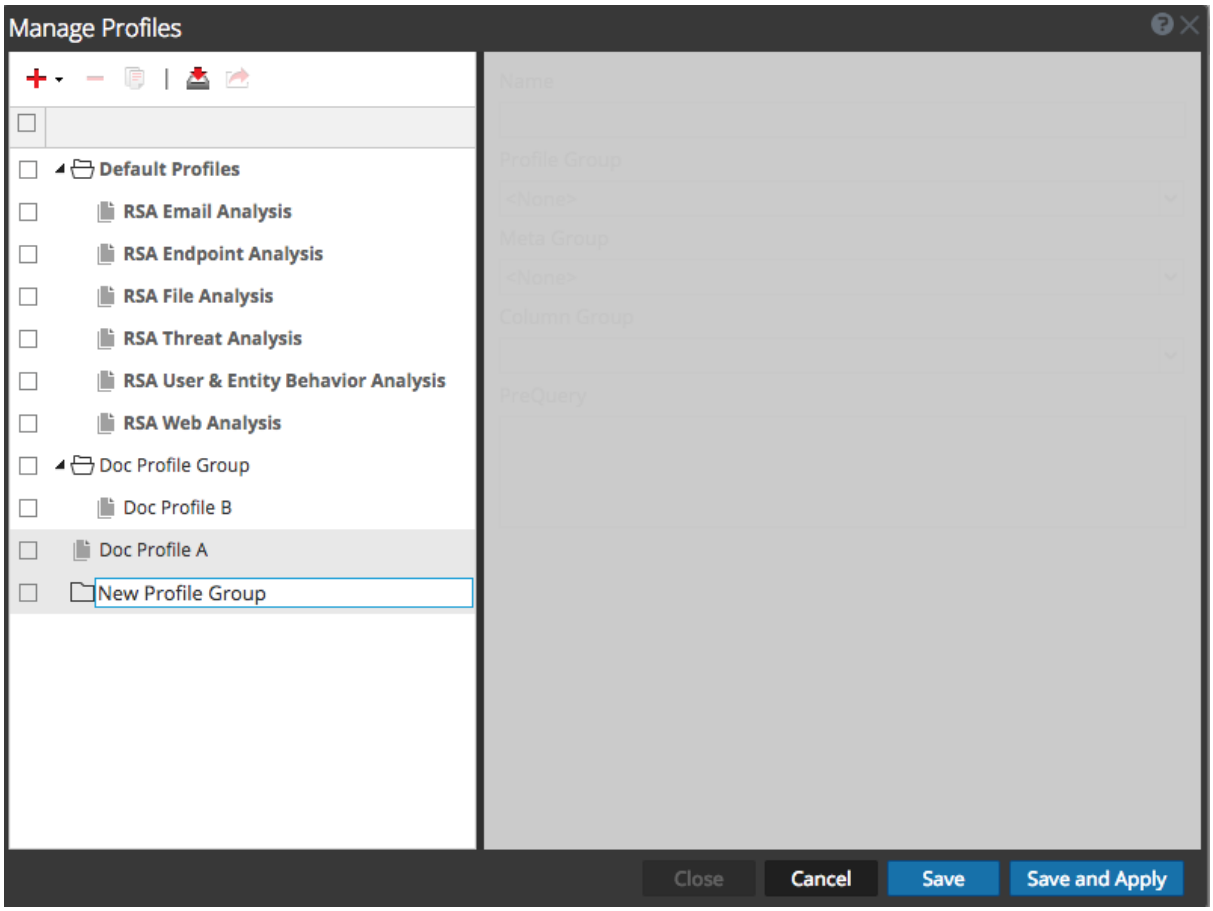
カスタム プロファイル グループを作成して、異なるプロファイルを整理することができます。作成後、プロファイル グループに対して直接行える編集は、プロファイル グループの名前の編集だけです。グループにプロファイルを追加または削除するには、プロファイルを編集し、別のプロファイル グループを割り当てます(詳細は、「プロファイルの作成と編集([ナビゲート]ビューまたは[レガシー イベント]ビュー) 」を参照) 。

注 : プロファイル グループをバージョン11.3から移行した場合、空のグループは移行されません。

1. [**プロファイルの管理**]ダイアログで、次のいずれかを実行します。
   - 編集する既存のプロファイル グループを選択するには、プロファイル グループをダブル クリックします。
   - 新しいプロファイル グループを追加するには、  をクリックして、[**新しいプロファイル グループの追加**]を選択します。

注 : 標準提供のプロファイル グループのいずれかを編集する場合は、  をクリックして、編集可能なコピーを作成します。

フォルダと空 白 のフィールド が、左 側 のプロファイル リスト の下 部 に表 示 されます。



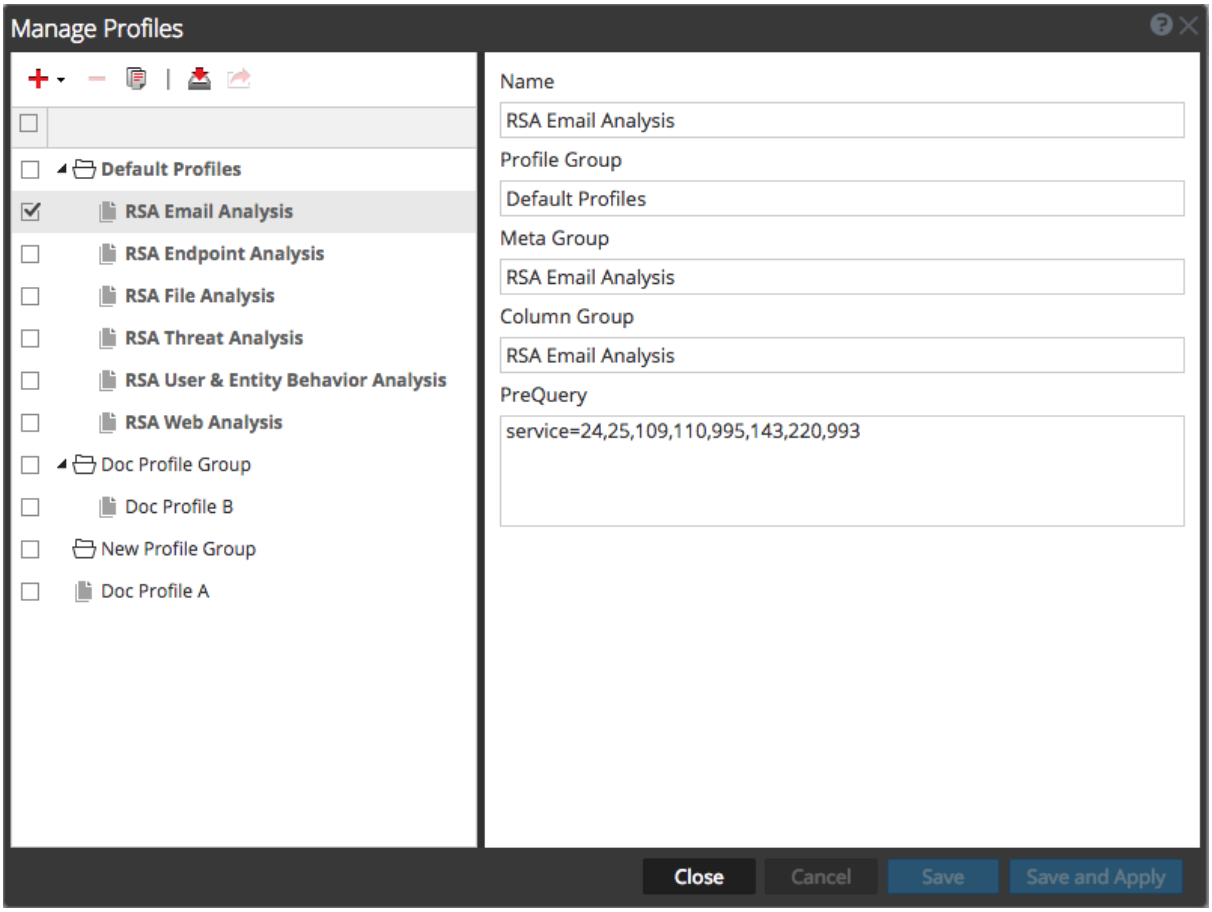
2. プロファイル グループの名 前を編 集 または入 力 するには、プロファイル グループをダブル クリックし、入 力 フィールド に入 力 します。名 前 は2～80文 字 の長 さにする必 要 があります。
プロファイルグループ名 は、新 しいプロファイル グループまたは編 集 したプロファイル グループに適 用 されます。プロファイルを設 定 するときに、プロファイル グループを使 用 できるようになります。
3. プロファイル グループを削 除 するには、次 のいずれかの操 作 を行 います。
   - プロファイルを削 除 することなく、プロファイル グループを削 除 する場 合 は、グループのチェックボックスをクリックし、グループ内 のプロファイルのチェックボックスをオフにして、[削 除]をクリックします。
   - プロファイル グループとグループに含 まれるプロファイルを削 除 する場 合 は、グループのチェックボックスをクリックし、削 除 したいプロファイルのチェックボックスもオンのままにします。
グループの削 除 を確 認 するダイアログ ボックスが表 示 されます。プロファイルの横 にあるチェックボックスをオンのままにすると、グループだけでなく、グループ内 の プロファイルも 削 除 されます。プロファイルのチェックボックスをオフにした場 合 は、プロファイル グループのみが削 除 され、プロファイルはグループ外 に移 動 し、別 のプロファイル グループに追 加 することができます。

プロファイルの作成と編集 ([ナビゲート]ビューまたは[レガシー イベント]ビュー)

1. [**プロファイルの管理**]ダイアログで、次のいずれかを実行します。
   - 編集する既存のプロファイルを選択するには、名前の横にあるチェックボックスをクリックします。
   - バージョン11.2以降で新しいプロファイルを追加するには、+をクリックするか、+の横にある下向き矢印をクリックし、[**新しいプロファイルの追加**]を選択します。
   - 11.2より前のバージョンで新しいプロファイルを作成するには、+をクリックします。

   注: 標準提供プロファイルのいずれかを編集する場合は、をクリックしてコピーを作成し、コピーを編集します。

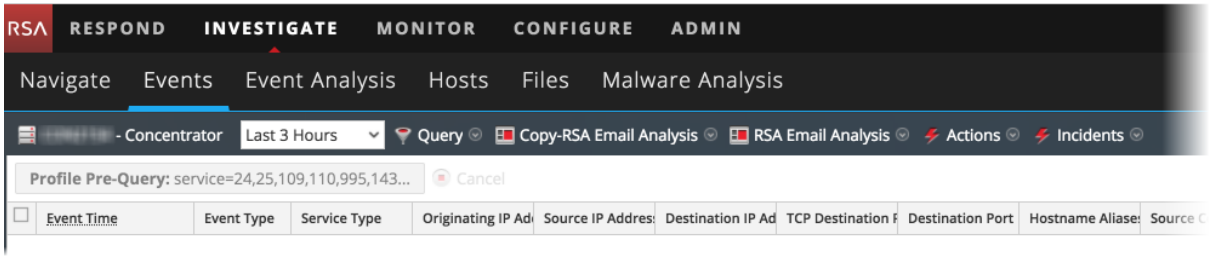
   プロファイルの定義は、右側のパネルで編集できます。次の図は、標準提供プロファイルの1つの定義を示しています。



2. [**名前**]フィールドで、プロファイル名を編集または入力します。名前は2～80文字の長さにする必要があります。
3. (バージョン11.2以降のオプション) プロファイルをプロファイル グループに追加する場合は、[**プロファイル グループ**]ドロップダウン リストからプロファイル グループを選択します。

プロファイル グループを選択すると、変更を保存するときにプロファイルがグループに追加されます。プロファイル グループを選択しない場合、そのプロファイルはどのグループにも属しません。

4. [**メタ グループ**]ドロップダウン リストからメタ グループを選択します。「メタ グループを使用して関連性の高いメタ キーにフォーカス」の説明に従って、カスタム メタ グループを追加できます。
5. [**列グループ**]ドロップダウン リストから列グループを選択します。「イベント リストでの列と列グループの使用」の説明に従って、カスタム列グループを追加できます。
6. 結果をフィルタリングするためのクエリを[**プレクエリ**]フィールドに入力します。プレ クエリの構文はクエリビルダと同じです。図のプレクエリには、「**service = 24,25,109,110,995,143,220,993**」というフィルタが指定されています。
7. プロファイルを使用しないで保存するには[**保存**]をクリックし、プロファイルを保存してただちに使用するには[**保存して適用**]をクリックします。
[**保存して適用**]をクリックすると、選択したプロファイルを適用する前に確認ダイアログが表示されます。バージョン11.2以降では、[プロファイルの管理]ダイアログで入力したプレクエリが階層リンクに表示されます。



プロファイルの削除 ([ナビゲート]ビューまたは[レガシー イベント]ビュー)

1. [**プロファイルの管理**]ダイアログで、名前の横にあるチェックボックスをクリックしてプロファイルを選択します。

> **注:** 標準提供プロファイルを削除することはできません。

2. **−**をクリックします。
プロファイルを削除するかどうかを確認するメッセージが表示され、プロファイルが削除されます。削除したプロファイルが使用中であった場合は、ツールバーのオプション名が[**プロファイル**]に戻り、プロファイルが有効になっていないことが示されます。

アクティブなプロファイルの変更 ([ナビゲート]ビューまたは[レガシー イベント]ビュー)

[ナビゲート]ビューまたは[レガシー イベント]ビューに十分な結果または正しい結果が表示されない場合は、アクティブ プロファイルがプレ クエリを適用している可能性があります。プロファイルを使用しない場合は、[**プロファイル**]ドロップダウン メニューの[**プロファイルの非アクティブ化**]をクリックします。

別のプロファイルを使用する場合は、次の手順を実行します。

1. [**ナビゲート**]ビューまたは[**レガシー イベント**]ビューのツールバーで、[**プロファイル**]ドロップダウン メニューを開きます。
2. [**プロファイル**]オプションにマウス ポインターを置くと、使用可能なプロファイルのドロップダウン リストが表示されます。
3. 使用するプロファイルを選択します。
   そのプロファイル設定が即座に適用されます。

[プロファイルの管理]ダイアログでアクティブ プロファイルを変更する場合は、次の手順を実行します。

1. [**ナビゲート**]ビューまたは[**レガシー イベント**]ビューのツールバーで、[**プロファイル**]＞[**プロファイルの管理**]を選択します。
   [プロファイルの管理]ダイアログが表示されます。
2. 左側のパネルでプロファイルを選択し、[**保存して適用**]をクリックします。
   確認のダイアログが表示されます。
3. [**はい**]をクリックします。
   そのプロファイル設定が即座に適用されます。

プロファイルのインポート ([ナビゲート]ビューまたは[レガシー イベント]ビュー)

[ナビゲート]ビューと[レガシー イベント]ビューで、別のサービスからダウンロードした.jsnファイルをアップロードまたはインポートできます。プロファイル グループをエクスポートしてインポートすると、プロファイルのグループ化を維持できます。

1. [**プロファイルの管理**]ダイアログで、左側のパネルのツールバーにある  をクリックします。
   [プロファイルのインポート]ダイアログが表示されます。
2. [**参照**]または[**ファイルのアップロード**]フィールドをクリックして、PC上のファイルを選択します。
3. ファイルを選択したら、[**アップロード**]をクリックします。
   プロファイルが左側のパネルに表示されます。

プロファイルのダウンロード ([ナビゲート]ビューまたは[レガシー イベント]ビュー)

[ナビゲート]ビューと[レガシー イベント]ビューでは、プロファイルを.jsnファイルとしてダウンロードできます。

1. [**プロファイルの管理**]ダイアログで、左側のパネルから1つまたは複数のプロファイルを選択します。
2. 左側のパネルのツールバーで  をクリックします。
   ダウンロードがすぐに始まります。

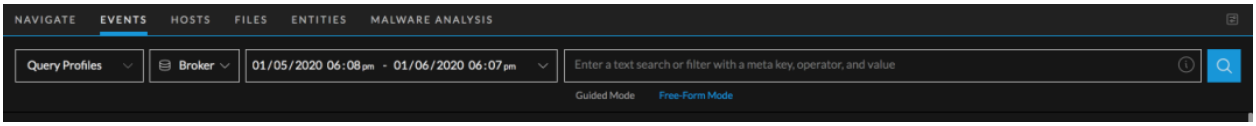
[イベント]ビューでの結果のフィルタリング

注: このセクションはバージョン11.1以降に適用されます。

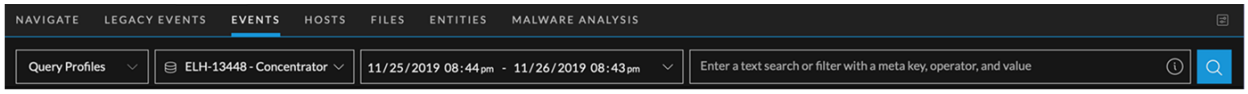
クエリ バーでサービスと時間範囲を選択し、調査中のサービスに対してクエリを実行することにより、[イベント]ビューのイベントをフィルタリングできます。イベントをフィルタリングすることにより、より関連性の高い少数のイベントに調査の重点を絞り込むことができます。

バージョン11.4では、列グループを使用して、イベントに含まれる属性(メタ キー、メタ グループ、メタ エンティティ)の中から調べる必要のある属性の数を最適化することもできます(「イベント リストでの列と列グループの使用」を参照)。

次の図は、イベント リストの結果をフィルタリングするツールを備えたバージョン11.4以前のクエリ バーを示しています。ガイド モードとフリーフォーム モードという2つのモードを使用できます。



次の図は、ガイド モードとフリーフォーム モードが不要になったバージョン11.4.1以降のクエリ バーを示しています。シンプルになったフィルタ入力フォームでは、高度な自動提案オプションの使用と、フリーフォーム クエリの入力も可能です。

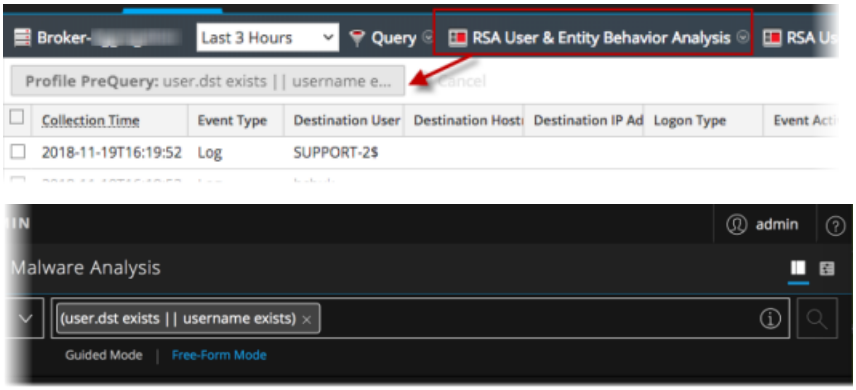


[調査]>[イベント]に移動すると、クエリ バーには、[クエリ プロファイル]メニュー、サービスと時間範囲のセレクター、クエリ ビルダ フィールドが表示されます。

- [クエリ プロファイル]メニューは、バージョン11.4以降で使用できます。クエリと列グループをプロファイルにカプセル化することにより、有用な属性の組み合わせを簡単に再使用して、イベント リストのイベントに適用できます(「クエリ プロファイルを使用した調査の共通領域のカプセル化」を参照)。
- デフォルトで、最初のサービスが自動的に選択されます(以前にサービスを選択し、そのサービスがブラウザのキャッシュに存在する場合を除く)。「[イベント]ビューでの調査の開始」の説明に従って、サービスを選択することもできます。
- 時間範囲を選択しない場合は、デフォルトの時間範囲(24時間)が使用されます。
- クエリ ビルダ フィールドは、時間範囲セレクターの右側にある空のフィールドです。ここでは、フィルタを作成することによってクエリを作成します。をクリックすると、クエリが送信され、選択したサービスにデータ ロード要求が送信されます。バージョン11.3以降では、(コンソール アイコン)をクリックすると、クエリ コンソールが開き、クエリの詳細なステータスが表示されます。

[レガシー イベント]または[レガシー イベント]ビューから[イベント]ビューに移動したときに、プロファイルのプレクエリが有効になっている場合、階層リンクに表示されていたプレクエリが編集可能なフィルタとして[イベント]ビューのクエリ ビルダに表示されます。サービス、時間範囲、各フィルタを変更することができます。

イベントを右クリックまたはダブルクリックして[イベント]ビューに移動したときに、[レガシー イベント]ビューでプロファイルが選択されていた場合は、そのプロファイルのフィルタ(プレクエリ)が編集可能なフィルタとしてクエリビルダ フィールドに追加されます。次の図は、[レガシー イベント]ビューのプレクエリと、[イベント]ビューの最初のフィルタとして追加された同じクエリを示しています。



クエリビルダの概念

クエリビルダでは、シンプル、フリーフォーム、テキストの3種類のフィルタを作成して、関心のあるイベントを絞り込むことができます。

各フィルタの基本的な構文は、`<meta key><operator><meta value>`です。たとえば「`direction = 'outbound'`」のように入力します。

バージョン11.4では、クエリバーにクエリを入力またはペーストすると、テキストの解析により、個々のフィルタに分割され、解析エンジンが必要と判断した場合には、各フィルタの間にAND演算子が追加されます。以前のバージョンでは、フィルタ間にはAND演算子のみが使用されるため、論理演算子は表示されません。

- 「`action = 'get' action = 'put'`」と入力すると、結果はANDで区切られた2つのフィルタになります。
- 「`action = 'get' OR action = 'put'`」と入力すると、結果はORで区切られた2つのフィルタになります。

`event.time`のフィルタを入力またはペーストするときは、次のいずれかの形式を使用します。

- `event.time = '2020-DEC-02 23:00:00'`
- `event.time = '2000-12-20 21:00:00.000'`
- `event.time = '2000-12-20 21:00:00'`

バージョン11.4では、クエリバーに長いテキスト文字列を入力またはペーストすると、解析エンジンによって個別のフィルタに変換されます。解析できない部分は、フリーフォーム フィルタに変換されます。以前のバージョンでは、長いテキスト文字列は単一のフィルタとしてクエリバーに追加されます。バージョン11.4.1ではさらに機能が強化され、メタ キーと演算子または演算子と値などの任意のクエリのテキストをフリーフォーム クエリとして入力し続けることができます。フリーフォーム クエリは通常どおりに解析されます。

- クエリバーに「`action = 'GET' OR action is 20 || action = 'PUT'`」と入力した場合は、フリーフォーム オプションが使用されます。このテキストの一部は解析できないため、結果はORで区

切られた3つのフィルタになります。

- バージョン11.4.1では、メタ キー、演算子、値のシーケンスを入力し、Enterキーを押さずに入力を続けると、フリーフォーム オプションが自動的に使用されるため、そのままクエリを入力し続けることができます。たとえば、ORの前にEnterキーを押さずに、「medium = 1 OR medium = 2」と入力することができます。入力中はフリーフォーム オプションがハイライト表示され、最後にEnterキーを押すと、クエリバーにフリーフォーム フィルタが作成されます。
- テキスト フィルタ(バージョン11.4以降) は、スペースを含まないテキスト文字列です。すべてのメタ キーではなく、インデックスされたメタ キーの完全一致をデータ セットから検索できます。failed, login,、attemptはその例です。

注: メタ キーと演算子のステートメントとほぼ一致するテキスト フィルタを入力しているときに、そのメタ キーと演算子を使用するフィルタが自動提案機能によって誤って提案されることがあります。この問題を回避するには、テキストの入力を開始し、自動提案機能によってテキストがメタ キーと演算子に変換されるポイントで[テキスト フィルタ]を選択します。たとえば、cryptoというメタ キーとcontainsという演算子がある場合に、cryptocurrencyを検索するテキスト フィルタを作成するとします。この場合、「c-r-y-p-t-o」と入力し、それに続く「currency」の「c」を入力すると、contains演算子がトリガーされ、1つの単語として入力を続けられなくなります。テキスト フィルタを完成させるには、contain演算子をトリガーするcurrencyの「c」を入力する直前に、[テキスト フィルタ]オプションをハイライト表示します。これによって、システムは入力をテキスト フィルタとみなします。

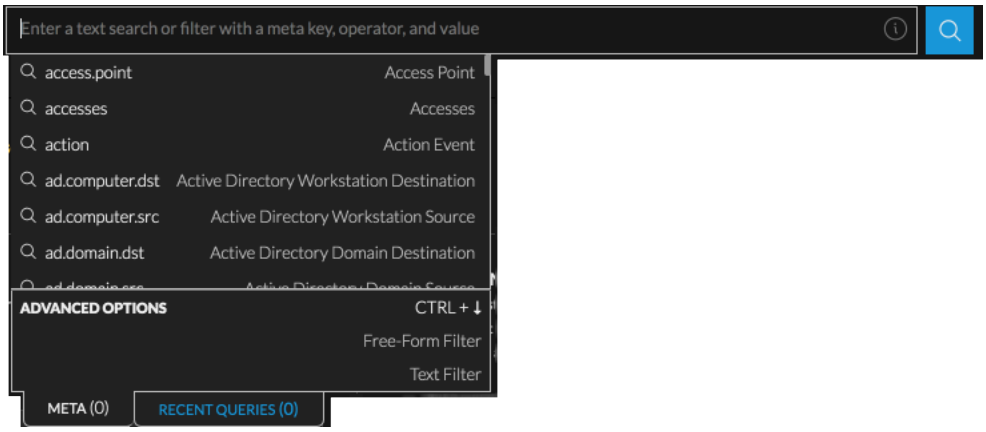
クエリビルダでは、各フィルタは編集可能なフィールドです。フィルタは、作成した順に左から右に並びます。追加したフィルタは1行に入りきらなくなると、次の行に折り返され、入力領域が縦に広がります。このため、右にスクロールしなくても、すべてのフィルタを表示できます。

RSA NetWitness® Platform 11の後続バージョンでは、11.1の初期のクエリバーに多くの機能追加が行われ、バージョン11.4では、クエリ作成を支援する広範なヘルプ機能を提供しています。

ガイド モードとフリーフォーム モード

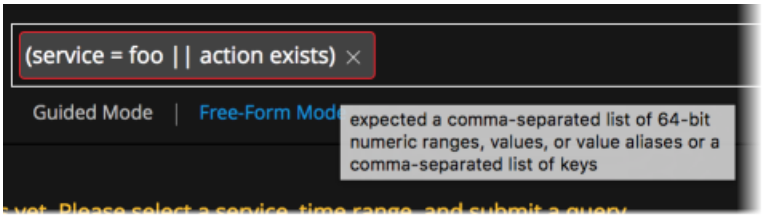
注: バージョン11.4には、フィルタ入力フォームにクエリを入力する方法として、ガイド モードとフリーフォーム モードの2つがありました。バージョン11.4.1以降では、ガイド モードの強力なオートコンプリート機能および値候補表示機能と、フリーフォーム クエリを入力またはペーストする機能が完全に統合されました。このドキュメントでガイド モードとフリーフォーム モードを区別して説明している箇所は、バージョン11.4.0.x以前を使用するアナリスト向けです。

ガイド モードでは、オートコンプリート機能により表示される有効なメタ キー、演算子、値の候補の中から選択することによりフィルタを作成できます。バージョン11.4では、直接入力、ペースト、最近のクエリの選択、またはドロップダウン メニューからの選択が可能です。以前のバージョンでは、テキストのペーストと最近のクエリはサポートされていません。これは、11.4のフィルタ入力フォームの例です。



フィルタを作成すると、各フィルタの構文が検証され、無効なフィルタは赤い枠線でマークされます。フィルタの上にマウスを合わせると、エラーについて説明するメッセージが表示されます。

バージョン11.3以降では、フリーフォーム フィルタがサーバ側で検証されるため、余分に時間がかかる場合があります。サーバからフィルタ検証結果がされる前にクエリを送信した場サーバからフィルタ検証結果が返される前にクエリを送信した場合、はスピナー アイコンに変わります。サーバの検証結果が返されると、無効なフィルタを含んでいないクエリの場合は、実行が開始されます。クエリに無効なフィルタが含まれている場合は、実行が終了し、無効なフィルタが赤い枠線でマークされます。これは、無効なクエリの例です。



フリーフォーム モードでは、長いテキスト文字列を入力またはペーストできます。自動提案機能はなく、クエリを送信するとサーバ側で検証が実行されます。エラーが見つかった場合、クエリは実行されません。

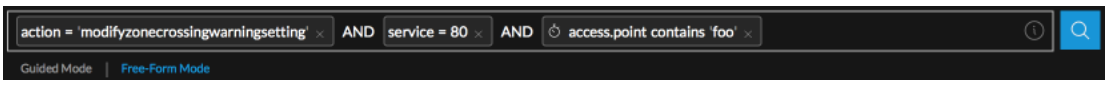
注： バージョン11.3より前のバージョンでは、ボタンのラベルが異なります。以前は[**クエリ イベント**]と呼ばれていました。

[ガイド モード]または[フリーフォーム モード]をクリックすると、モードが切り替わります。最後にログインしたときにフリーフォーム モードを選択した場合、この選択はブラウザのキャッシュに保存され、ブラウザのキャッシュがクリアされない限り使用されます。

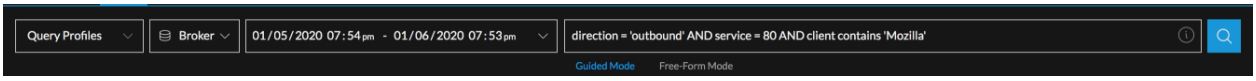
- ガイド モードからフリーフォーム モードに切り替えると、ガイド モードで作成したフィルタはフリーフォームのテキスト クエリに変換されます。
- フリーフォーム モードからガイド モードに切り替えると、入力済みのクエリが個別のシンプルなフィルタとしてクエリ バーに追加されます。ただし、自動提案オプションは表示されません。

  注： バージョン11.3以前は、フリーフォーム フィルタは、ガイド モードでは編集できませんでした。

次の図は、ガイド モードのクエリ ビルダといくつかのフィルタを含むクエリ バーの例です。

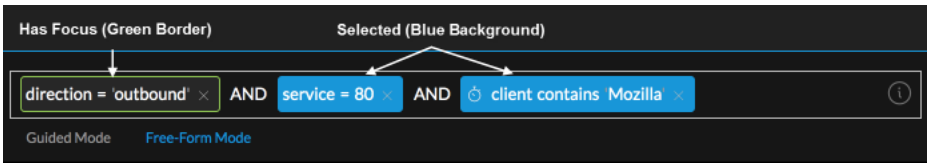


次の図は、フリーフォーム クエリビルダ使用中の例です。



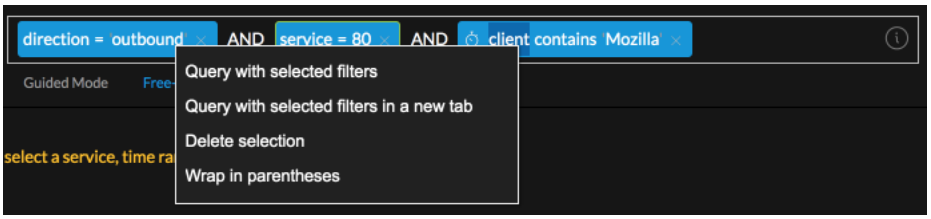
複数のフィルタの編集に関する概念

クエリビルダで作業する際は、編集のフォーカスがあるフィルタは緑色の枠線でマークされ、選択中のフィルタには青色の背景が表示されます。この機能は、右クリック アクションに対して複数のフィルタを選択できる点で便利ですが、一度に編集できるフィルタは1つだけです。次の図は、フォーカスされたフィルタが緑色の枠線でマークされ、選択中の2つのフィルタが青色の背景で表示されている状態を示しています。



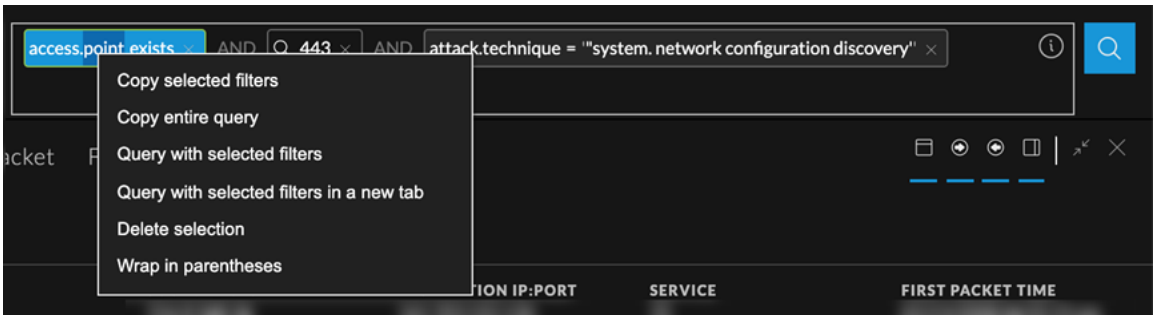
次の図は、先ほどと同じフィルタを使用し、今度はすべてのフィルタを選択し(青色の背景)、そのうちの1つのフィルタにフォーカスした(青色の背景と緑色の枠線)状態を示しています。

ドロップダウン メニューの右クリック アクションは、選択したすべてのフィルタに適用されます。次の図は、バージョン11.4のオプションを示しています。



バージョン11.4.1のメニューには、次の図に示すように、新しいコピー オプションが2つあります。これらのオプションを使用すると、クリップボードの内容を他のアナリストと共有したり、コンテンツをクエリ バーにペーストしたりすることができます。次の操作を実行できます。

- 1つのフィルタを選択して右クリックし、クエリ全体をローカルのクリップボードにコピーします。
- 複数のフィルタを選択し、そのうちの1つを右クリックして、選択したフィルタをコピーします。



以下は、クエリビルダでの作業方法について説明した基本的な概念です。

- 複数のフィルタを選択できますが、フォーカスできるのは1つのフィルタのみであり、最後に選択したフィルタで必ずフォーカスがアクティブになります。
- フィルタを選択してフォーカスするには、フィルタをクリックします。フィルタを選択解除してフォーカスを解除するには、フィルタを再度クリックするか、**Esc**を押すか、またはページ内の別の場所をクリックします。
- フィルタを追加するには、既存のフィルタの前後をクリックします。フォーカス中のフィルタの前後に新しいフィルタを作成するには、右矢印キーまたは左矢印キーを押します。
- 編集するフィルタを開くには、フィルタをダブルクリックするか、フィルタをクリックして**Enter**を押します。変更を保存せずに終了し、フィルタにフォーカスしたままにするには、**Esc**を押します。
- フィルタを削除するには、フィルタをクリックして**Delete**を押すか、フィルタで[**X**]をクリックします。

バージョン11.3以前のクエリビルダ

バージョン11.1では、ユーザ インタフェースのガイドに従ってシンプルなフィルタ(`<meta key> <operator> <meta value>`)を作成および編集します。ユーザ インタフェースでは、シンプルなフィルタのみがサポートされています。[レガシー イベント]ビューまたは[ナビゲート]ビューからイベントを開き、フィルタに複数の演算子(`||`、`&&`、`()`、`REGEX`、`LENGTH`)が含まれている場合、フィルタは追加されますが、[イベント]ビューでの編集はサポートされません。詳細については、『NetWitness Platform 11.3 Investigateユーザ ガイド』を参照してください。PDF形式のドキュメントには、RSA NetWitness Platform バージョン11 総合目次からアクセスできます。

バージョン11.2では、ユーザ インタフェースにガイド モードとフリーフォーム モードの2つのモードがあります。ガイド モードでは、シンプルなフィルタ(`<meta key> <operator> <meta value>`)を作成および編集できます。デフォルトのモードはガイド モードで、自動提案と検証オプションが含まれます。長いテキスト文字列はフリーフォーム モードで入力できます。フリーフォーム モードの検証は、クエリを実行するときに行われます。詳細については、『NetWitness Platform 11.2 Investigateユーザ ガイド』を参照してください。PDF形式のドキュメントには、RSA NetWitness Platformバージョン11のマスター目次からアクセスできます。

バージョン11.3では、ユーザ インタフェースに次の機能が追加されました。

- [ナビゲート]または[イベント]ビューから[イベント]ビューに移動したときに、プロファイルのプレクエリが有効になっている場合、階層リンクに表示されていたプレクエリが編集可能なフィルタとして[イベント]ビューのクエリビルダに表示されます。
- ユーザ インタフェースの自動提案オプションは、フリーフォーム フィルタを作成できる[詳細オプション]セクションで補強されています。フリーフォーム モードは、長いテキスト文字列全体をペーストする場合にも役立ちます。
- クエリは、実行中にキャンセルできます。
- クエリ コンソールで、実行中のクエリの詳細なステータス情報を確認できます。

バージョン11.4のクエリビルダ

直接入力のほか、ドロップダウン メニューからのメタ キー、演算子、値の選択、クエリ バーへのフィルタのペーストを行えます。以下のセクションでは、ガイド モードのフィルタ入力フォームに追加された11.4の機能について詳しく説明します。

メタ キーのキャッシュによるロードの高速化

[イベント]ビューを開くときに、接続されているすべてのサービスのメタ キーがキャッシュされるため、データのロードが高速になります。これらのメタ キーは、ユーザ インタフェースでメタ キーを自動提案するために使用されます。(列グループまたはプロファイルを作成しているときに、本来は表示されるべきメタ キーが表示されない場合は、キーが追加されているサービスを選択して、キャッシュを強制的に更新します。通常、この問題は、メタ キーが追加されていないConcentratorが存在する場合にのみ発生します)。

テキスト フィルタ

データ セット内のテキスト文字列を検索するテキスト フィルタを作成できます。テキスト フィルタは、値を格納するメタ キーについての知識がなくても使用できます。クエリあたり1つのテキスト フィルタがサポートされています。テキスト フィルタが検索の対象とするのは、すべてのメタ キーではなく、インデックスされたメタ キーです。

テキストを直接入力する代わりにペースト

フィルタを作成するときに、フィルタ入力フォームにメタ キーまたは値をペーストできます。フィルタ入力フォームにテキストを直接入力するのではなく、ペーストすると、テキストが適切に解析され、1つまたは複数のフィルタが作成されます。解析できない部分は、フリーフォーム フィルタに変換されます。

すべてのフィルタの選択とすべてのフィルタのコピー(バージョン11.4.1)

[イベント]ビューのクエリ バーでフィルタを作成するときに、キーボード コマンドを使用して、すべてのフィルタを選択(MacOSの場合はCmd-A、Windowsの場合はCtrl-A)してから、選択内容をクリップボードにコピー(MacOSの場合はCmd-c、Windowsの場合はCtrl-C)できます。クリップボードのテキストは、他のアナリストと共有したり、Cmd-VまたはCtrl-Vを使用してクエリ バーにペーストしたりできます。

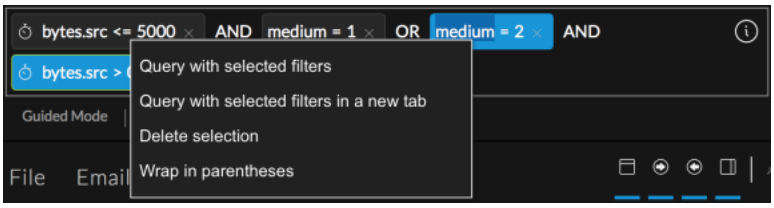
最近のクエリの使用

フィルタ入力フォームには、[メタ]タブと[最近のクエリ]タブという、メタ キー、演算子、値を入力する2つの方法があります。[メタ]タブは、以前のバージョンのフィルタ入力フォームと同じですが、条件に一致するメタ キーの数が[メタ]タブのラベルに表示されるようになった点と、各メタ キーのアイコンにより、キーでインデックスされているか、値でインデックスされているか、インデックスされていないかが表示されるようになった点が異なります。[最近のクエリ]タブには、最大100個の最近のクエリが表示されます。リストは入力されたテキストによって絞り込まれ、入力されたテキストを含んだクエリのみが表示されます。このリストからクエリを選択できます。

高度な演算子の使用

自動提案機能の解析エンジンは、フィルタ入力フォームにペーストまたは手入力された高度な演算子(<、 >、<=、>=、OR、||、AND、&&、()、regex、length)を解析できます。テキストは複数のフィルタとして解析されます。たとえば、「medium > 0 && medium <= 100」を直接入力またはペーストした場合、このテキストは、明示的なAND演算子を使用する2つのシンプルなフィルタ(medium > 0 AND medium <= 100)として解析されます。「bytes.src <= 5000 && medium = 1 || medium = 2 && bytes.src > 0」を直接入力またはペーストした場合は、ANDおよびOR演算子で区切られた4つのシンプルなフィルタ(bytes.src <= 5000 AND medium = 1 OR medium = 2 AND bytes.src > 0)と解析され、できる限り多くの有効なフィルタが作成されます。

このフィルタは、括弧を追加するのに適したフィルタの例です。「medium = 2」と「bytes.src > 0」を選択して右クリックし、ドロップダウン メニューから[**括弧で囲む**]を選択します。括弧内にテキスト フィルタを追加することは、サポートされていません。



結果として生成されるクエリは、bytes.src <= 5000 AND medium = 1 OR (medium = 2 AND bytes.src > 0)です。

フィルタの作成中にエラーが発生する場合は、ツールチップ メッセージを参照するか、ドキュメントを確認してください。

AND/OR演算子の使いやすさ

「||」および「&&」と入力すると、クエリ バーに「OR」および「AND」と表示されます。それぞれの演算子をクリックして、ORをANDに変更したり、ANDをORに変更することができます。フィルタを追加するためにカーソルを挿入すると、カーソルの前にAND演算子が追加されます。フィルタを削除すると、孤立したORおよびAND演算子も削除されます。テキスト フィルタは常にクエリとAND条件で処理されるため、テキスト フィルタの演算子はANDでなければなりません。

括弧の不均衡の自動修正

クエリビルダでフィルタを作成して編集するときは、括弧の不均衡が入力時に自動的に修正されます。編集中のフィルタ内、または選択したフィルタの前に開き括弧を入力した場合は、そのフィルタの最後に閉じ括弧が追加されます。ネストされた括弧がある場合に、括弧の両側と括弧の間に新しいフィルタを追加できるよう、この機能は入力に応じて直感的に機能します。孤立した括弧は自動的に削除されます。括弧を追加することによって無効なフィルタが作成される場合、括弧は追加されません。選択したフィルタを右クリックして[括弧で囲む]オプションを使用することによって、括弧を追加することもできます。このオプションは、結果が有効なフィルタになる場合にのみ使用できます。

使用可能な値に関するヒント

適切にインデックスされたメタ キーについては、クエリの時間範囲から選択可能な値の候補がユーザ インタフェースに表示されます。最大100個の候補値が返されます。テキストを入力すると、100個の値のリストが絞り込まれ、一致する値のみがリストに表示されます。一致する値がない場合は、「候補が見つかりません」というメッセージが表示されます(候補値は時間範囲のみに基づいています。クエリ内の他のフィルタは100個の値のリストの絞り込みには使用されません) 。

CIDR表記と略記

フィルタにIPアドレスの値を指定する場合は、CIDR表記を使用して、アドレスの範囲を指定することができます。

IPv4 CIDRブロックの範囲は0～32です。たとえば、`10.20.30.0/24`は、サブネット マスクが`255.255.255.0`の`10.20.30.0`を指定します。これは、`10.20.30.0`から`10.20.30.255`までの範囲のIPと一致します。

IPv6 CIDRブロックの範囲は0～128です。たとえば、
`1203.0fe1:fe82:b896:89b0:8a7c:99bf:323d/32`は
`1203:0fe1:0000:0000:0000:0000:0000:0000`から
`1203:0fe1:ffff:ffff:ffff:ffff:ffff:ffff`までを意味します。

また、略記を使用して、IPv6アドレスの連続したゼロや先頭のゼロを削除することもできます。たとえば、次のように指定できます。

`1203:fe1::`

IPアドレスとCIDRマスクの間にスペースを挿入しないでください。

値の範囲またはリスト

数値データを含むメタ キーの場合は、値の範囲、値のリスト、またはその両方を使用して、フィルタに指定することができます。たとえば、「`src.port = 0-1023, 1024-1050, 65535`」というクエリでは、カンマ区切りのリストを指定し、リスト内の2つは値の範囲です。カンマが値の一部である場合は、値を引用符で囲む必要があります。たとえば、`get,post`は2つの個別の値として解釈され、`'get,post'`は1つの値として解釈されます。値の範囲は、正の整数の有効な範囲でなければならず、ダッシュで区切ります(ダッシュの前後のスペースの有無は問いません) 。範囲の最初の数字は2番目の数字より小さくする必要があります。たとえば、`0-1023`と`0 - 1023`は有効な範囲ですが、`-10 - 50`、`50 - 10`、`50.8 - 60.2`、`50 - 70x`は有効な範囲ではありません。

メタ キーと演算子の後に区切り文字のスペースは不要(バージョン11.4.1)

クエリ バーのフィルタには、メタ キーと演算子の間、および演算子と値の間にスペースが必要です。フィルタ入力フォームで演算子と値の自動提案機能を使用するには、演算子の前後で区切り文字のスペースを入力する必要がありました。クエリ入力時のユーザ エクスペリエンスを向上させるため、フィルタ入力フォームでは、メタ キーの後に区切り文字のスペースなしに演算子を入力できます。区切り文字のスペースなしで演算子を入力した場合、候補値が通常どおりに自動的に表示され、メタ キーと演算子の間にはスペースが追加されます。演算子と値の間に区切り文字のスペースを挿入していない場合、演算子と値の間に自動的にスペースが追加されます。

時間範囲を選択

[時間範囲]セレクターは、[イベント]ビューに返されるイベントを特定の時間範囲に制限します。時間範囲は、「開始時間 – 終了時間」の形式で表示され、ユーザのプロファイルに構成されたタイムゾーン設定に基づいて、現在のタイムゾーンの日付、時間、分を表示します。バージョン11.3以降では、現在の収集時間に対して相対的な時間範囲を選択するか、またはカスタムの時間範囲を指定できます。

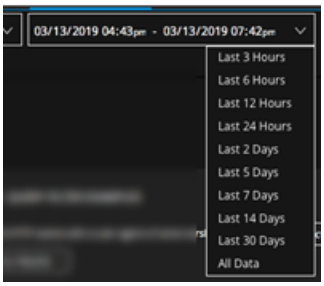
時刻と日付の形式は、[イベント]ビューの[ユーザ環境設定]ダイアログ(> [**プロファイル**]を選択)の設定に基づきます。

- デフォルトの日付形式は、MM/DD/YYYYです。この形式は、[ユーザ環境設定]ダイアログでDD/MM/YYYYまたはYYYY/MM/DDに変更できます。
- 開始時間と終了時間はHH:MM形式で指定します。秒は表示されませんが、開始時間の値は常にHH:MM:00秒に、終了時間の値は常にHH:MM:59秒にデフォルトで設定されます。たとえば、「6:45 pm - 7:45 pm」という時間範囲は「06:45:00 - 07:45:59 pm」として解釈されます。
- デフォルトの時間範囲は24時間制です。12時間制に変更することができます。

クエリの時間形式は、[イベント]ビューの[イベント環境設定]ダイアログ(を選択)の設定に基づきます。時間形式は、データベースの時間または現在の時間のどちらかに設定することができます。[データベースの時間]を選択した場合、クエリの開始時刻と終了時刻は、イベントが収集された時刻(収集時間)に基づく時刻になります。[現在の時間]を選択した場合、クエリの実行に使用される終了時刻は現在のブラウザの時刻に基づく時刻になり、開始時刻は終了時刻と時間範囲に基づいて計算されます。その他の[イベント]ビューの環境設定については、「[イベント]ビューの構成」を参照してください。

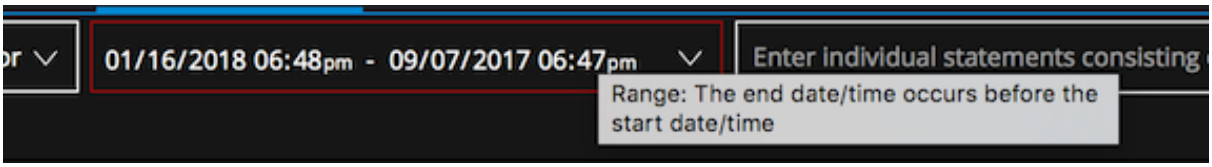
時間範囲を編集するには、次のいずれかを実行します。

1. [**時間範囲**]セレクターの内側にあるドロップダウン矢印をクリックして、リストから時間範囲を選択します。分単位、時間単位、日単位のオプションを選択するか、すべてのデータを選択できます。

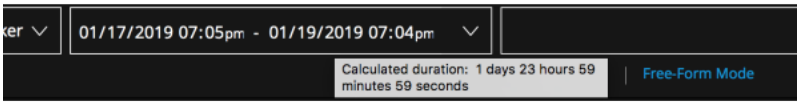


2. (バージョン11.3以降)クエリバーに表示されている年、月、日、時間、分をクリックして時間範囲を直接編集します。値がハイライト表示されたら、開始時間または終了時間のいずれかの新しい値を入力します。時間形式の環境設定が12時間制に設定されている場合は、[**午前**]または[**午後**]をクリックして2つのオプションを切り替えます。

時間範囲が無効な場合(開始時間が終了時間よりも後である場合など)は、時間範囲セレクターに赤い枠線が表示されます。クエリが不可能になったためボタンが無効化され、何を変更する必要があるかを説明したエラー メッセージがツールチップに表示されます。次の図は、時間範囲が無効な状態を示しています。



選択した時間範囲は、クエリの対象となるサービスごとにブラウザに保存されます。サービスごとに異なる時間範囲を設定できます。ツールチップには、計算されたクエリ期間が表示されます。次の図にツールチップの例を示します。



クエリの送信

ボタンは、クエリバーの右端に表示され、必要に応じてクエリを送信するためにアクティブになります。バージョン11.3以前では、をクリックすると、すべてのフィルタがANDで連結され、ボタンが非アクティブになります。バージョン11.4では、AND以外の演算子もクエリに含まれている可能性があるため、クエリはそのまま送信されます。ボタンは、以下の場合に再びアクティブになります。

- クエリバーでサービスを変更するか、[イベント]パネルで列グループを変更した時。[イベント]パネルの再構築のためのデータをネットワーク経由で取得する場合、新しいクエリを送信するまでは、以前のサービス、時間範囲、およびメタデータ フィルタが引き続き使用されます。ボタンは、ビュー内のデータが古くなっていることを示すインジケータとしてアクティブになります。
- 1分以上経過し、元のクエリの時間範囲を指定しても同じ結果セットが生成されそうにない場合は、結果が古くなっている可能性があることを示すインジケータとして、ボタンがアクティブになります。バージョン11.3以降では、[イベント]ビューの環境設定で[時間範囲を自動的に更新]オプションを有効または無効にすることにより、この動作が決まります(「[イベント]ビューの構成」を参照)。

クエリの実行のキャンセル

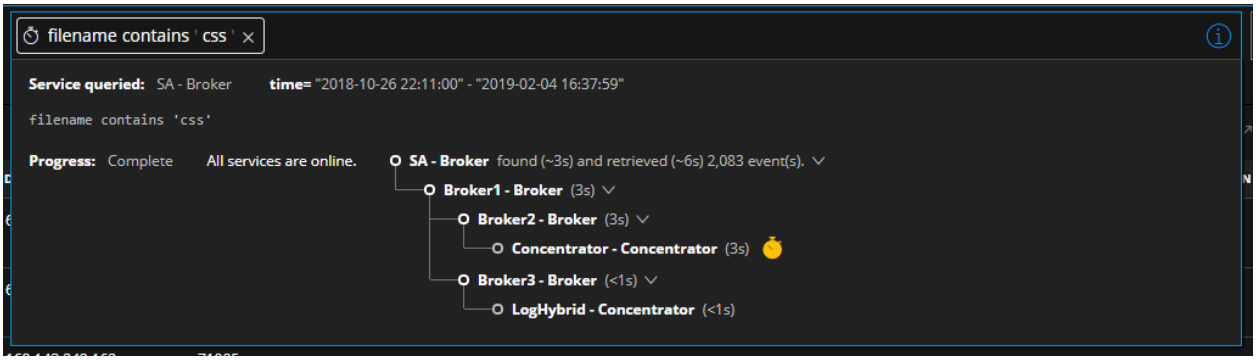
をクリックしてクエリを送信すると、ボタンが(クエリ停止オプション) に変わります。クエリ停止オプションは、すべてのイベントが[イベント]パネルにロードされるまで表示されたままになります。クエリをキャンセルするには、をクリックします。

すべての結果が返される前にクエリがキャンセルされた場合は、イベント リストの結果の最後に「クエリがキャンセルされたため、部分的な結果のみを表示しています」というメッセージが表示されます。

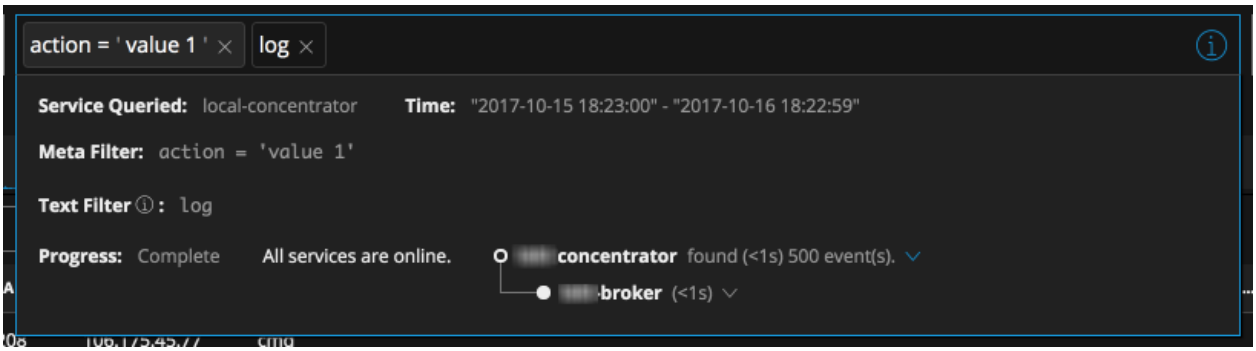
クエリのステータスの表示

クエリコンソールを開くには、クエリを送信した後でクエリバーの情報アイコン( ) をクリックします。クエリコンソールでは、クエリによって照会されたサービス、時間範囲、メタデータのほか、クエリのステータスに関するリアルタイム情報も確認できます。クエリコンソールに表示される時間範囲の日付は、常にYYYY-MM-DDの形式で表示されます。「"2014-09-20 20:57:00"-"2018-11-02 18:57:59"」は、クエリコンソールに表示される時間範囲の例です。

次の図は、クエリが正常に実行された場合のバージョン11.3のクエリ コンソールの例です。最も低速のサービスには黄色のストップウォッチ マークが表示されます。



次の図は、テキスト フィルタを含むクエリを実行した後でバージョン11.4のクエリ コンソールに表示される情報の例です。[メタ フィルタ]と[テキスト フィルタ]という2つのフィールドにクエリが表示されていることに注意してください。



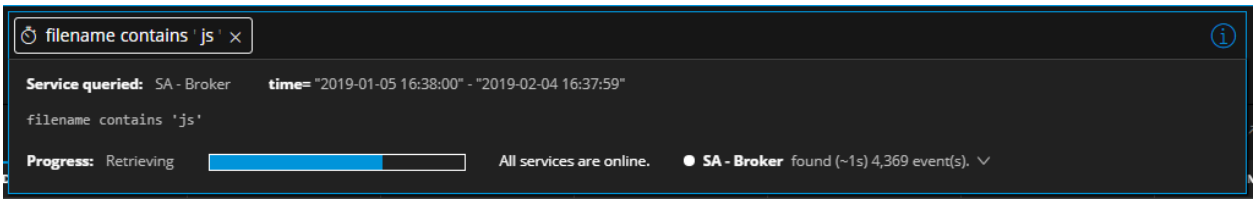
クエリが実行されている間、コンソールの下部にある進行状況バーには、クエリの完了率が表示されます。ステータス情報からは、クエリで今行われている処理(実行中、キューに登録済み、クエリ対象サービスのインデックス ファイルの読み取り中、イベントの取得中、完了など)についての詳細を知ることができます。ステータスと致命的でないメッセージは受信するとすぐに表示され、致命的でないエラーの場合は、クエリ バーの枠線が黄色に変わります。

アイコンは、個々のサービスに関する追加情報を示します。

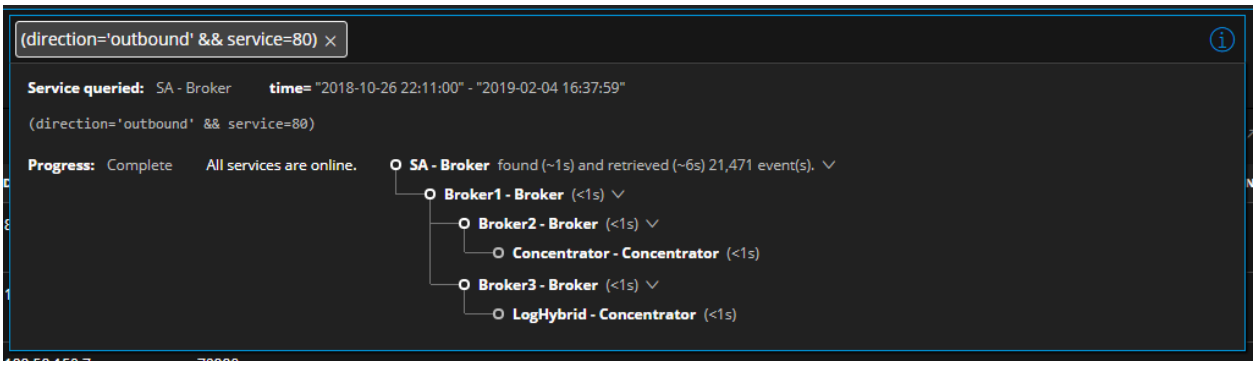
- 黄色のストップウォッチは、最も低速なサービスを示します。
- 黄色の三角形は警告を受信したことを示します。
- 赤い三角形は、サービスに対してクエリを実行しようとしたときにエラーが発生したことを示します。

イベントを検索するための実行とインデックス ファイルの読み取り。クエリの最初のステージは、クエリ対象サービスで結果が見つかったときに完了します。クエリ コンソールでは、クエリ対象のすべてのサービスがネスト構造の階層リストに表示され、どのサービスがオンラインかオフラインかを示すインジケータ、各サービスが結果を見つけるまでに要した時間(秒単位)も表示されます。

イベントの取得と[イベント]パネルへのロード。見つかったイベントを取得し、[イベント]パネルにロードしている間、進行状況バーには、視覚的なインジケータと現在実行中の処理を説明するテキストが表示されます。次の図は、結果が見つかり、取得中であることを示しています。

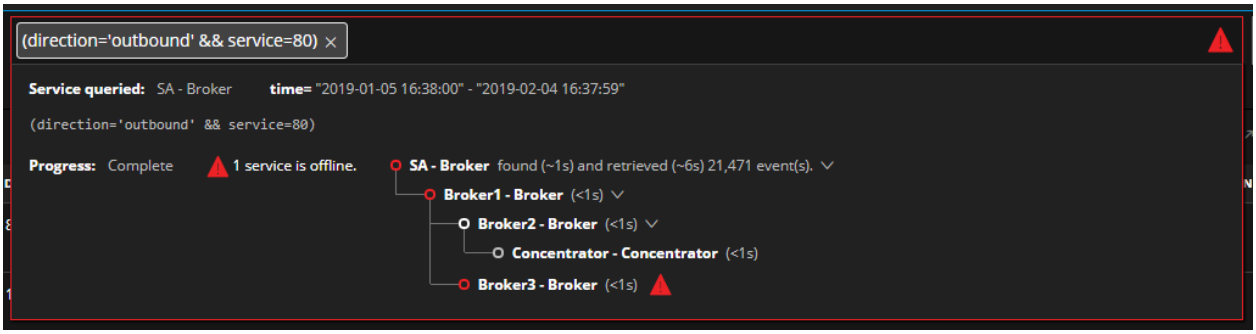


要求の完了。エラーまたは警告なしでロードが完了した場合、クエリコンソールの枠線は青色になり、表示中のデータが最新であることを示すインジケータとしてボタンが無効になります。次の図は、エラーまたは警告なしにクエリが完了したときのクエリコンソールの例です。



エラーと警告。致命的なエラー(クエリの構文エラー、クエリ対象サービスがオフラインなど) が発生すると、クエリの実行が停止されます。クエリが失敗したことを示す赤い三角形がクエリコンソールの右上隅に表示され、赤い枠線が表示されます。クエリ対象サービスがオフラインの場合は、クエリ対象サービスのみが階層なしでクエリコンソールに表示され、赤い三角形でマークされます。

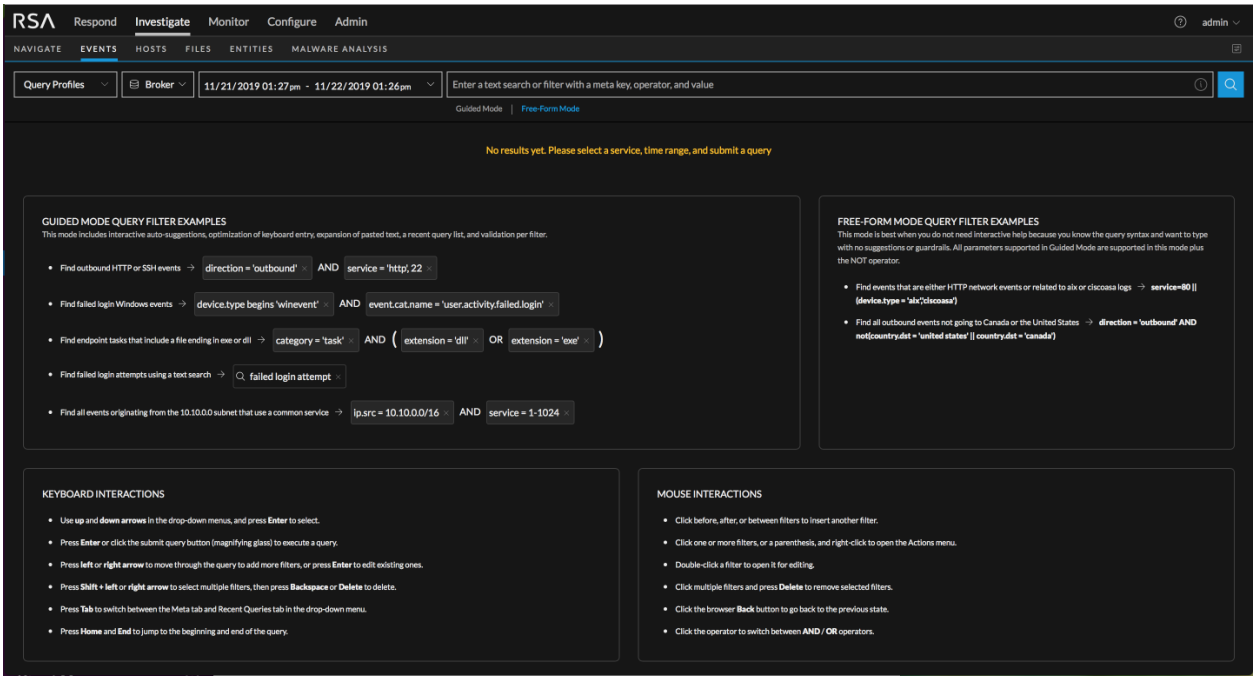
致命的でないエラーが発生しても、クエリの実行は妨げられません。クエリは実行され、イベントはロードされますが、クエリコンソールの右上隅に赤い三角形が表示され、警告を示す赤い枠線が表示されます。次の図は、クエリ対象サービスが別のオフライン状態のサービスのプロキシになっている場合に表示されるクエリコンソールの例です。



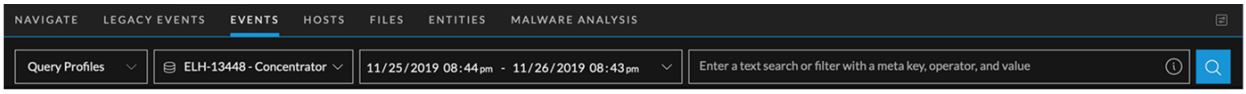
警告が発生しても、クエリの実行は妨げられません。クエリは実行され、イベントはロードされますが、クエリコンソールの右上隅に黄色の三角形が表示され、黄色の枠線が表示されます。

ガイド モードでのクエリの作成

ガイド モードは、様々な支援機能を備えており、アナリストが有効なクエリを作成する最も簡単な方法です。次の図は、クエリ バーでガイド モードが有効になった初期状態の[イベント]ビューを示しています(バージョン11.3以前)。



バージョン11.4.1には、すべてのガイド モード機能とその他の改善が組み込まれているため、ガイド モードを選択する必要がなくなりました。次の図は、バージョン11.4.1のクエリ バーを示しています。



ガイド モードで使用するキーボード操作

ガイド モードのクエリ ビルダでは、マウスを使用しなくても、キー操作でフィルタの入力、編集、削除ができます。マウスも使用できますが、キーボードだけで操作することもできます。この表は、カーソルをクエリ バーに合わせたときにガイド モードで使用できるキーボード操作を示しています。サービス セレクターと時間範囲には適用されません。

操作	キーボードへの入力
すべてのフィルタをコピーする(バージョン11.4.1以降)	クエリ バー(ただし、編集中のフィルタ以外)にカーソルを合わせ、すべてのフィルタが選択された状態で、**Ctrl-C**(Windows OS)または**Cmd-C**(MacOS)を押します。

操作	キーボードへの入力
フィルタ内の文字を削除する	選択した文字 : クエリ バーで文字を選択して、**Delete**または**Backspace**を押します。 前の文字(バージョン11.4以降) : クエリ バーで文字の横にカーソルを置いて、**Backspace**(Windows OS) または**Delete**(MacOS) を押します。 すべての文字(バージョン11.4以降) : フィルタにカーソルを合わせて、**Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。
フィルタを削除する	選択したフィルタ: 1 つまたは複数のフィルタを選択して、次のいずれかを実行します。 • **右クリック> [選択したフィルタを削除]**または**[選択項目を削除]**を選択します(11.4以降) 。 • **Delete**を押します。 • **Backspace**を押します。 フォーカスしたフィルタ(バージョン11.4以降) : フォーカスしたフィルタにカーソルを合わせて、**Backspace**(Windows OS) または**Delete**(MacOS) を押します。フォーカスしたフィルタが削除され、フォーカスが左側に移動します。 フォーカスしたフィルタ(バージョン11.4 以降) : フォーカスしたフィルタにカーソルを合わせて、**Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。フォーカスしたフィルタが削除され、フォーカスが右側に移動します。
フィルタ内の括弧を削除し、括弧の中身は削除しない(バージョン11.4以降)	括弧の中身は選択せずに、括弧を選択した状態で、**Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。選択した括弧が削除されますが、括弧の中身は残ります。
フィルタ内の括弧とその中身を削除する(11.4以降)	選択した括弧 : 括弧を選択して、次のいずれかを実行します。 • **右クリック> [選択項目を削除]**を選択します。 • **Backspace**(Windows OS) または**Delete**(MacOS) を押します。選択した括弧とその中身が削除され、フォーカスが左側に移動します。 • **Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。選択した括弧とその中身が削除され、フォーカスが右側に移動します。
すべてのフィルタの選択を解除する	フィルタを選択した状態で、**Esc**を押します。
選択したフィルタを編集する	単一のフィルタを選択した状態で、**Enter**を押します。
クエリ バーの先頭に新しいフィルタを挿入して、編集用に開く(バージョン11.4以降)	フィルタを選択した状態で、**Home**(Windows OS) または**Fn** + **左矢印**(MacOS) を押します。

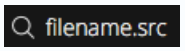
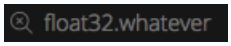
操作	キーボードへの入力
クエリ バーの最後尾に新しいフィルタを挿入し、編集用に開く(バージョン11.4以降)	フィルタを選択した状態で、**End**(Windows OS) または**Fn** + **右矢印**(MacOS) を押します。
選択したフィルタの左隣に新しいフィルタを挿入して、編集用に開く	フィルタを選択した状態で、**Shift** + **左矢印**を押します。
選択したフィルタの右隣に新しいフィルタを挿入して、編集用に開く	フィルタを選択した状態で、**Shift** + **右矢印**を押します。
選択したフィルタの左隣に新しいフィルタを挿入する	フィルタを選択した状態で、**左矢印**を押します。
選択したフィルタの右隣に新しいフィルタを挿入する	フィルタを選択した状態で、**右矢印**を押します。
選択したフィルタを新しいタブで使用する	フィルタを選択した状態で、**右クリック**>[**新しいタブで、選択したフィルタでクエリを実行**]を選択します。
選択したフィルタでクエリを実行する	フィルタを選択した状態で、**右クリック**>[**選択したフィルタでクエリを実行**]を選択します。
括弧の中身でクエリを実行する(バージョン11.4以降)	括弧を選択した状態で以下を実行します。 • 選択した括弧の中身でクエリを実行するには、括弧の片側を選択して、**右クリック**>[**選択したフィルタでクエリを実行**]を選択します。 • ブラウザの新しいタブを開いて、選択した括弧の中身でクエリを実行するには、括弧の片側を選択して、**右クリック**>[**新しいタブで、選択したフィルタでクエリを実行**]を選択します。
クエリ バーのすべてのフィルタを選択する(バージョン11.4.1以降)	クエリ バー(ただし、編集中のフィルタ以外) にカーソルを合わせて、**Ctrl-A**(Windows OS) または**Cmd-A**(MacOS) を押します。
現在のフィルタの左側にあるすべてのフィルタを選択する	(バージョン11.3.x以前) フィルタを選択した状態で、**Shift** + **上矢印**を押します。 (バージョン11.4以降) フィルタを選択した状態で、**Shift** + **左矢印**を2回押します。
現在のフィルタの右側にあるすべてのフィルタを選択する	(バージョン11.3.x以前) フィルタを選択した状態で、**Shift** + **下矢印**を押します。 (バージョン11.4以降) フィルタを選択した状態で、**Shift** + **右矢印**を2回押します。
左隣のフィルタ(ある場合) を選択する	フィルタを選択しないで、**左矢印**キーを押します。

操作	キーボードへの入力
右隣のフィルタ(ある場合) を選択する	フィルタを選択しないで、**右矢印**キーを押します。
クエリを送信します。	クエリ バーをフォーカスし、保留中のフィルタがない状態で、**Enter**を押します。

ガイド モードでの視覚的なフィードバック

ガイド モードは、クエリの作成中に視覚的なフィードバックを提供します。次の表は、可能性のあるフィードバックを特定して説明します。

フィードバック	アイコン	説明
フィルタの青色の背景		フィルタが選択されていることを示します。
2つのフィルタ間の緑色の丸		(バージョン11.3以前) 緑色の丸は、2つの既存のフィルタの間にカーソルの位置があることを示します。クリックすると、この場所に新しいフィルタが挿入されます。 (バージョン11.4) 太字のカーソルは、挿入ポイントを示します。
緑色のフィルタ枠線		単一のフィルタがフォーカスされ、編集できることを示します。複数のフィルタが選択され、このフィルタがフォーカスされている場合は、青色の背景と組み合わせて表示されます。
赤色のフィルタ枠線		フィルタが無効であることを示します。エラーを説明するツール チップが表示されます。

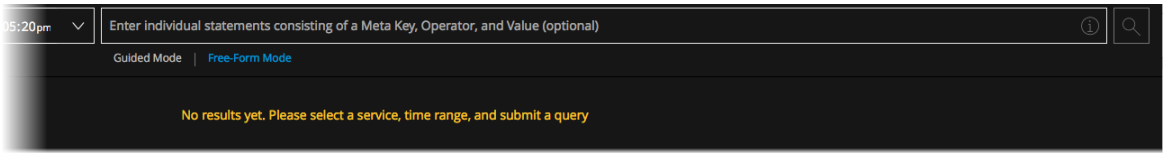
フィードバック	アイコン	説明
[メタ]タブのインデックス インジケータ		(バージョン11.4以降) [メタ]タブでメタ キーのインデックス レベルを示します。これにより、そのメタ キーをフィルタで使用できるかどうかが決まります。  このメタ キーはメタ値でインデックスされており、フィルタで使用できます。  このメタ キーはメタ キーによってインデックスされており、フィルタで使用できます。  このメタ キーはインデックスされておらず、フィルタには使用できません。 sessionIDメタ キーは特殊なケースです。インデックスされていない他のメタ キーとは異なり、構成できませんが、フィルタで使用できるため、鍵記号が表示されます。サポートされる演算子は、exists、!exists、=、!=です。
クエリ送信ボタン		クエリの送信、クエリのステータスの表示、クエリのキャンセルに使用します。このボタンには次の3つの状態があります。  クエリビルダのフィルタを使用してクエリを送信する準備ができています。  クエリを実行する前のサーバの検証が完了するのを待っています。  クエリが実行中です。実行をキャンセルする場合にクリックします。
低速サービス アイコン		クエリ コンソールで、クエリの結果のロードに最も長い時間を要したサービスに表示されます。

フィードバック	アイコン	説明
イベント リストのスピナー		クエリが現在処理中であることを示します。この状態の間、[**クエリ送信**]ボタンは無効になります。
ストップウォッチ		メタ キー/演算子の組み合わせが、非常に時間のかかる組み合わせであることを示します。クエリは実行可能ですが、より効率的なメタ キーまたは演算子の使用を推奨します。

ガイド モードでのシンプルなフィルタの追加

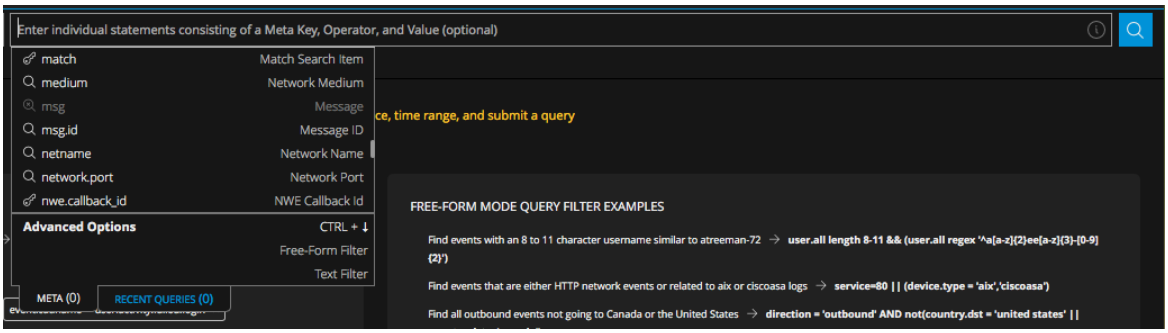
ガイド モードでシンプルなフィルタを作成するには、次の手順を実行します。

1. [**イベント**]ビュー(バージョン11.3以前では[イベント分析]ビュー)に移動し、次のいずれかを実行します。
   a. (バージョン11.4.1以降)クエリ バーをクリックし、フィルタ入力フォームが表示されたら、[メタ]タブを選択します(まだ選択されていない場合)。
   b. (バージョン11.4以降)[**ガイド モード**]を選択して、クエリ バーをクリックし、フィルタ入力フォームが表示されたら、[メタ]タブを選択します(まだ選択されていない場合)。
   c. (バージョン11.2以降)[**ガイド モード**]を選択して、クエリ バーをクリックします。
   d. (バージョン11.1)空のクエリ バーをクリックするか、既存のフィルタの前後をクリックします。次の図は、フィルタの入力を開始する前のガイド モードの空のクエリ バーの例です。



挿入ポイントが2つのフィルタの間にある場合は、緑色の丸(バージョン11.3以前)または太字のカーソル(バージョン11.4以降)によって挿入ポイントがマークされます。挿入ポイントがクエリ バーの最後尾にある場合は、エントリー ポイントに点滅するカーソルが表示されます。ドロップダウン リストには、調査対象のサービスから取得した使用可能なメタ キーがアルファベット順に表示さ

れます。次の図は、バージョン11.4のフィルタ入力フォームを示しています。

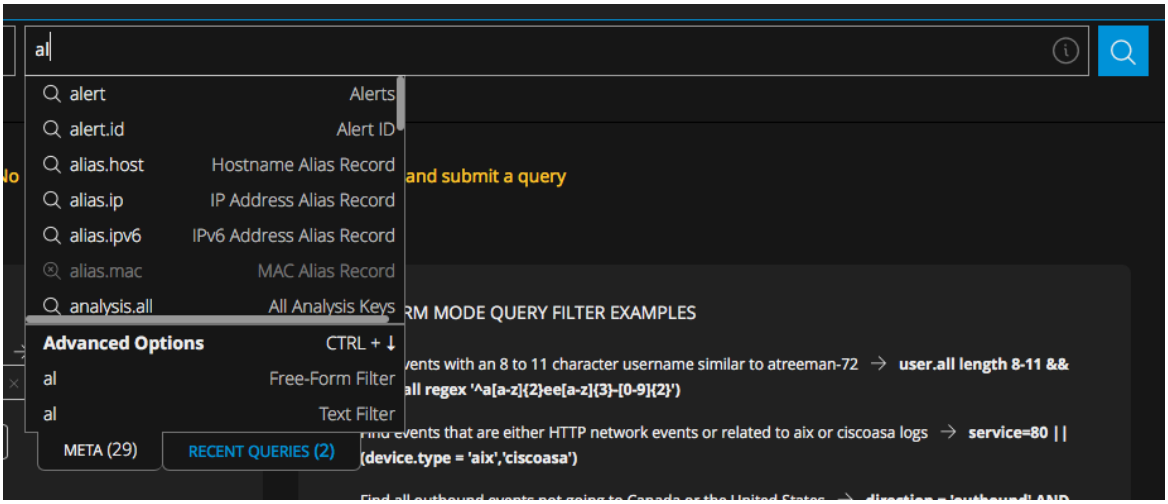


2. メタ キーを選択するには、次のいずれかを実行します。

   a. ドロップダウン リストにオプションが1つしかない場合は、**Enter**を押します。

   b. ドロップダウン リストに複数のオプションがある場合は、メタ キーをクリックするか、上/下矢印を使ってメタ キーを選択してから、**Enter**を押します。

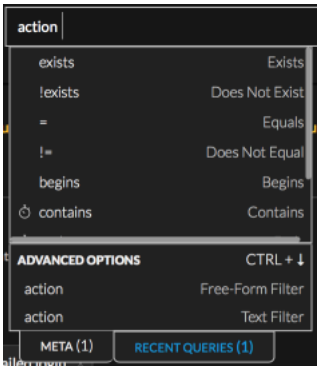
   c. メタ キーの入力を開始します。入力に合わせて、入力したテキストを含んだメタ キーのみが表示されるようにリストが絞り込まれます。[メタ(0)]タブのラベルに表示されるカウントは、入力されたテキストに一致するインデックスされたメタ キーの数を反映して変化します。インデックスが作成されていないキーは無効化されて選択できず、カウントには含まれません。たとえば、次の図の`alias.mac`はインデックスが作成されていないため、グレー表示になっています。メタ キーをクリックするか、上/下矢印を使ってメタ キーを選択してから、**Enter**を押します。



   d. ハイライト表示されているメタ キーを選択するには、**Enter**を押します。
   [メタ]ラベルのカウントが1に変わります。

注 : ドロップダウン リストでメタ キーが選択されておらず、選択できるメタ キーがリストにない場合は、クエリ バーですでに入力されている内容に応じて、フリーフォーム フィルタまたはテキスト フィルタのいずれかのオプションがハイライト表示されます。
--クエリ バーに入力されたテキストに、ユーザ インタフェースでまだサポートされていない形式のクエリ構文や演算子が含まれている場合は、フリーフォーム フィルタ オプションがハイライト表示され、フリーフォーム フィルタを作成できるようになります。バージョン11.3以前では、`**`、`&&`、`||`、`()`、`AND`、`OR`、`comma`、`-`、`length`、`regex`の各演算子は、ユーザ インタフェースでサポートされていません。バージョン11.4のユーザ インタフェースでは、これらの演算子がサポートされています。フリーフォーム フィルタがハイライト表示されておらず、クエリ バーに既存のテキスト フィルタがない場合は、テキスト フィルタがハイライト表示され、作成できるようになります。
--最初の条件がtrueで、テキスト フィルタがすでに1つある場合は、フリーフォーム フィルタ オプションがハイライト表示され、フリーフォーム フィルタを作成できるようになります。

e. メタ キーを編集または削除する場合は、**Backspace**または**Delete**を押します。
キーを押して文字を削除するのに合わせて、メタ キー ドロップダウン リストが絞り込まれ、残りの文字を含むメタ キーが表示されます。メタ キーを選択するには、**Enter**を押します。
メタ キーがフィルタ入力フォームに追加され、選択したメタ キーに対して有効な演算子のリストが表示されます。処理時間が長い演算子には、(ストップウォッチ アイコン) が表示されます。
次の図は、ストップウォッチ アイコンが表示された`contains`演算子を示しています。



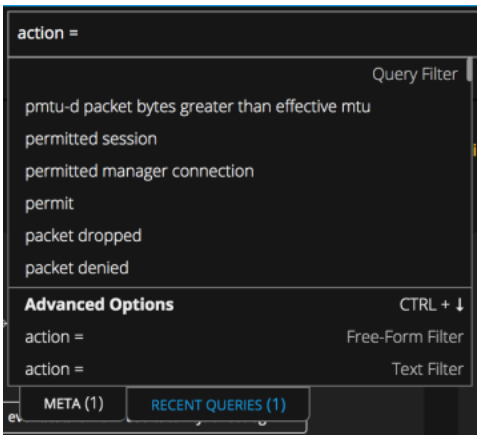
3. 演算子を選択するには、次のいずれかを実行します。

   a. 演算子ドロップダウン リストにオプションが1つしかない場合は、**Enter**を押してオプションを選択します。

   b. 演算子ドロップダウン リストに複数のオプションがある場合は、演算子をクリックするか、上/下矢印を使って演算子を選択してから、**Enter**を押します。

   c. 演算子を直接入力して、**Enter**を押します。入力に合わせて、演算子ドロップダウン リストが絞り込まれ、入力したテキストを含む演算子のみがリストに表示されます。演算子をクリックするか、上/下矢印を使って演算子を選択してから、**Enter**を押します。
   フィルタ入力フォームに演算子が追加されます。バージョン11.4以降では、演算子に値を指定できる場合は、候補値のドロップダウン リストが表示されます。以前のバージョンでは、値を入力

できるように、フィルタ入 力フォームにカーソルが置 かれたままになります。

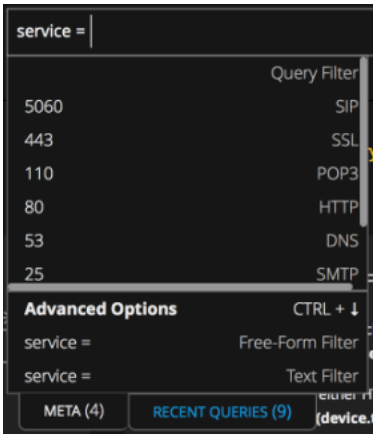


4. (オプション) フィルタ入 力フォームの選 択された演 算 子に値を指 定できる場 合は、次のいずれかを実 行します。

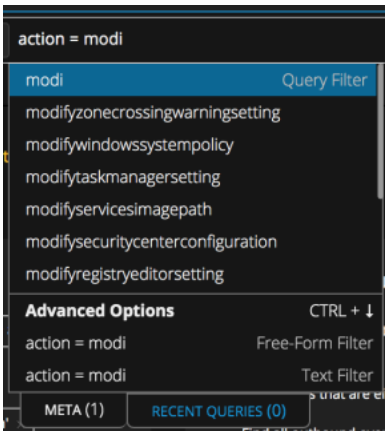
   a. バージョン11.3以 前では、値を直 接 入 力して**Enter**を押します。

   b. バージョン11.4以 降では、コピーした値をペーストして**Enter**を押します。

   c. バージョン11.4以 降では、[**クエリ フィルタ**]フィールドに入 力し始めます。
   入 力に合 わせて、メタ値ドロップダウン リストが絞り込まれ、入 力したテキストで始まる、最 大100個 のインデックスされた値 が表 示されます。候 補 値は時 間範 囲のみに基づいています。クエリ内 の他 のフィルタは100個 の値 のリストの絞り込みには使 用されません。自 動 提 案 機 能は、(最 大1万 件 の) ダウンロードされたイベントだけでなく、現 在 のデータ セット内 のすべてのイベントから一 致を検 索します。リスト内 に完 全 に一 致するものがない場 合は、[クエリ フィルタ]フィールドに入 力したテキストがハイライト表 示され、候 補 が見 つからなかったことがメッセージに示されます。`service`メタ キーの整 数 値のように、一 部の値にはサービス タイプの定 義も表 示されます。

   完 全 一 致がある場 合は、その値 がハイライト表 示されます。次の例では、入 力されたテキスト「modi」と完 全 に一 致する値 がありません。

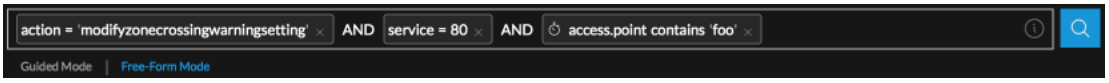


i. 入力したテキストをフィルタで使用する場合は、**Enter**を押します。

ii. クエリを実行したい値がリストに含まれているが、ハイライト表示されていない場合は、その値をクリックするか、上/下矢印を使ってその値をハイライト表示します。その後、**Enter**を押します。

iii. 値を編集または削除する場合は、**Backspace**または**Delete**を押します。
キーを押して文字を削除するのに合わせて、メタ値ドロップダウン リストが絞り込まれ、残りの文字で始まる値が表示されます。値を選択するには、**Enter**を押します。
値がフィルタ入力フォームに追加されます。

5. フィルタを作成するには、**Enter**を押します。**Enter**を押す前にボックスの外側をクリックした場合、フィルタは作成されません。
新しいフィルタが挿入され、最後のフィルタの後ろで点滅するカーソルが再フォーカスされ、メタ キーのドロップダウン リストが表示されます。フィルタにエラーがある場合は、赤色の枠が表示されます。フィルタにポインターを合わせると、ツール チップにエラーが表示されます。この図は、エラーなしで作成されたクエリを示しています。



6. フィルタにエラーがない場合は、クエリ バーでクエリを実行する準備ができています。をクリックします。
結果が返され、[イベント]パネルにロードされます。クエリに一致する最初の1万イベントの[イベント]パネルへのロードが開始されます。イベントがロードされる間、上部にあるステータス バーで進行状況を確認できます。リストの一番下までスクロールして、完了ステータスを確認できます。

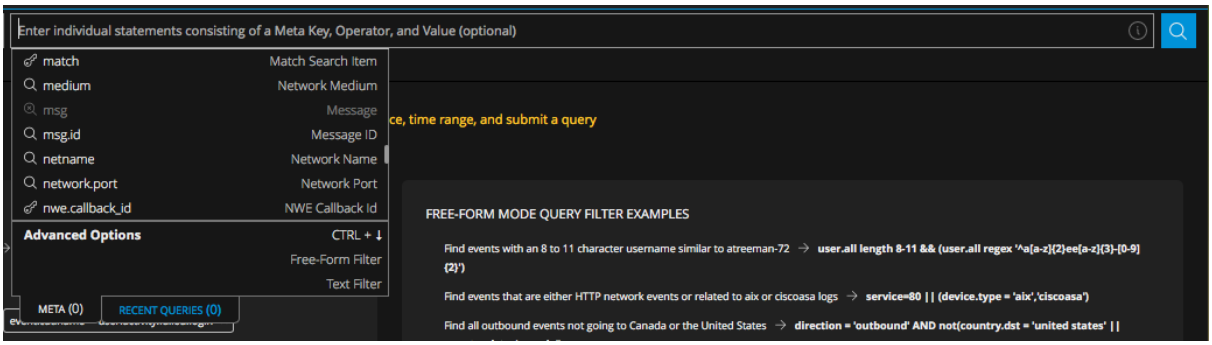
7. (バージョン11.3以降のオプション) クエリ コンソールで詳細ステータスを表示するには、(情報アイコン) をクリックします。

8. (バージョン11.3以降のオプション) 実行が完了する前にクエリをキャンセルする場合は、をクリックします。
クエリが実行を停止し、クエリがキャンセルされたことを示す通知が表示されます。

ガイド モードでのフリーフォーム フィルタの追加 (バージョン11.3以降)

ガイド モードでフリーフォーム フィルタを使用して、[イベント]ビューに表示されるデータをフィルタリングするには、次の手順を実行します。

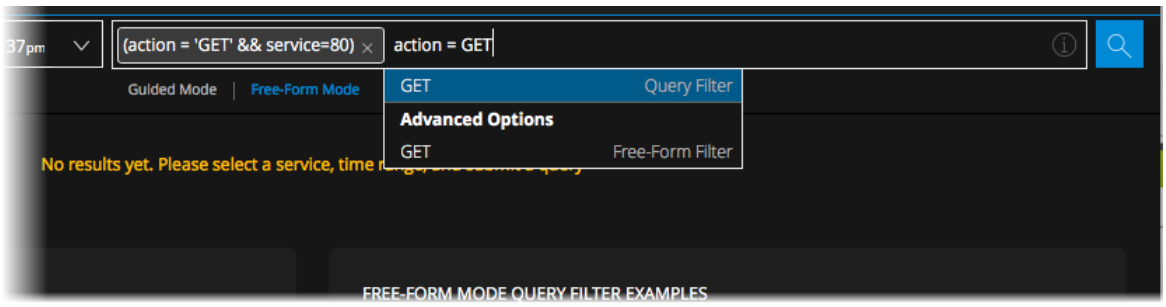
1. [**イベント**]ビューに移動し、クエリ バーの下にある[**ガイド モード**]を選択して、クエリビルダ フィールドをクリックします(バージョン11.4.1の場合は、クエリビルダ フィールドを単にクリックします) 。
   挿入ポイントが2つのフィルタの間にある場合は、緑色の丸または太字のカーソルによって挿入ポイントがマークされます。挿入ポイントがクエリ バーの最後尾にある場合は、エントリー ポイントに点滅するカーソルが表示されます。ドロップダウン リストには、調査対象のサービスから取得した使用可能なメタ キーがアルファベット順に表示されます。



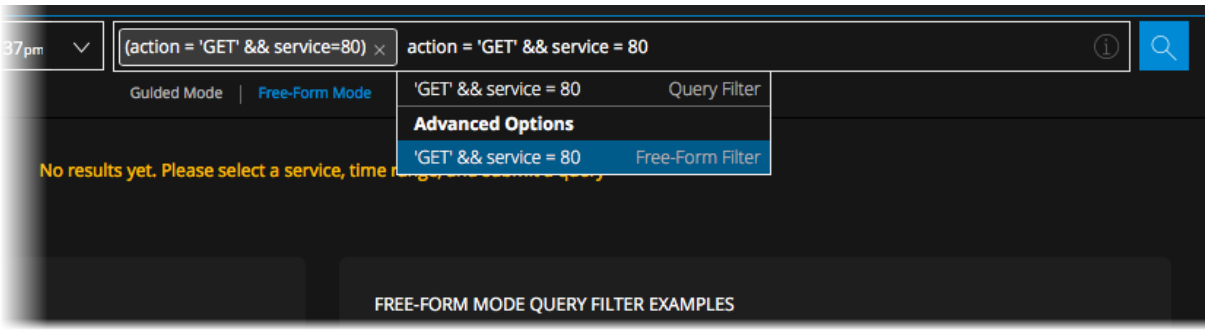
2. 次のいずれかを実行します。

   a. [**フリーフォーム フィルタ**]フィールドにカーソルを置き、クエリの入力を開始します。

   b. メタ キーまたは開き括弧で始まるフィルタの入力を開始します。クエリビルダでフィルタを追加したり、編集するときは、括弧の不均衡が自動的に修正されます。開き括弧を入力した場合、閉じ括弧がフィルタに追加されます。
   一致するメタ キーまたは演算子がドロップダウン メニューにない場合は、[フリーフォーム フィルタ]オプションが使用可能になり、入力したテキストが[**フリーフォーム フィルタ**]フィールドに表示されます。

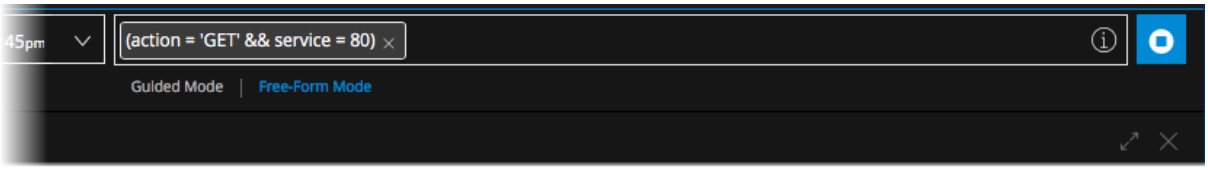


3. 式全体の入力を続けて、**Enter**を押します
   (**Enter**を押す前にボックスの外側をクリックした場合、フィルタは作成されません) 。次の図は、値「GET」の後を入力し続けることによって作成されたフリーフォームの式を示しています。



新しいフィルタが挿入され、最後のフィルタの後で点滅カーソルが再びフォーカスされて、新しいフィルタ入力フォームが表示されます。フィルタにエラーがある場合は、赤色の枠が表示されます。フィルタにポインターを合わせると、ツール チップにエラーが表示されます。

4. クエリを実行するには、をクリックします。クエリの実行中は、ボタンがに変わります。



5. 実行が完了する前にクエリをキャンセルする場合は、をクリックします。
クエリをキャンセルしない場合は、をクリックしてクエリの実行ステータスを表示できます。クエリの実行が完了すると、[イベント]パネルにクエリの適切な結果が表示されます。

データ セット内の不特定の場所から値を検索するテキスト フィルタの追加(バージョン11.4以降)

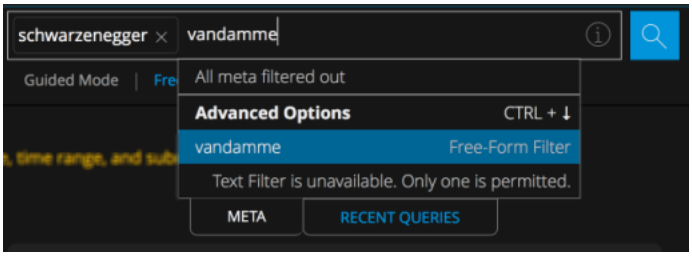
バージョン11.4以降では、テキスト フィルタを使用して、現在のデータ セット(エンドポイント、ログ、ネットワーク イベント)から特定の値を検索できます。テキスト フィルタを使用すると、値でインデックスされたすべてのメタ キーのデータに対して、大文字と小文字を区別しない検索が実行されます。テキスト フィルタでは、メタ キーによってインデックスされた値とインデックスなしの値は検索対象とならないため、すべての結果が表示されるわけではありません。次のメッセージが表示されます「`Results may be limited by a text filter, which matches only indexed meta keys. If you want to conduct a more exhaustive search against raw events, click here and choose the appropriate options in the Search Events drop-down menu.`」。ドロップダウン リストのアイコンは、各メタ キーのインデックス レベルを示しています。

- filename.size - メタ キーによってインデックス
- filename.src - メタ値によってインデックス
- float32.whatever - インデックスなし

注: クエリ対象の階層内のサービス(Broker、Concentrator、Decoder)はすべて、バージョン11.3以降でなければなりません。階層内にバージョン11.3より前のサービスがある場合は、ドロップダウン メニューでテキスト フィルタを選択できません。

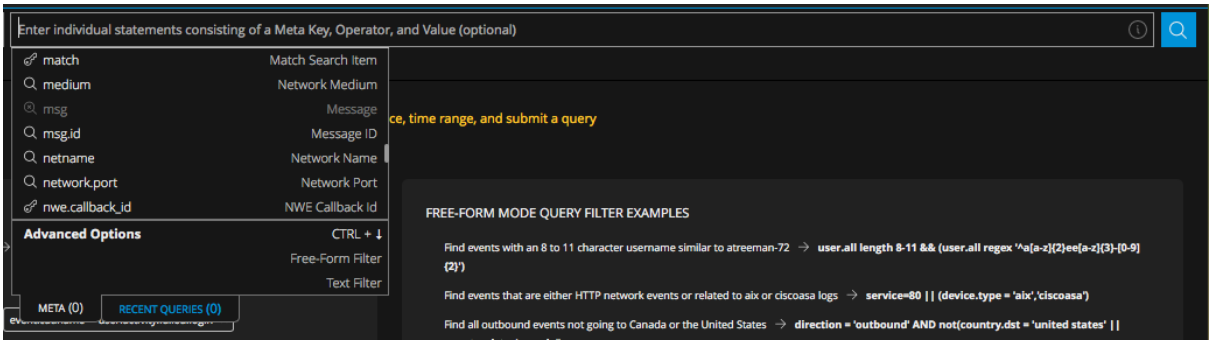
テキスト フィルタは、どこを探すべきか(どのメタ キーまたはサービスか) がわからなくても、探しているものについてある程度わかっている場合に役立ちます。たとえば、ファイル名を検索したい場合、クエリ バーをクリックして、テキスト文字列全体を入力し、[**テキスト フィルタ**]をクリックします。テキスト フィルタは、調査対象のサービスと時間範囲内で、インデックスにあるすべてのデータを検索し、テキスト文字列の完全一致 を返します。

クエリには、テキスト フィルタ1つと、シンプル フィルタとフリーフォーム フィルタの任意の組み合わせを含めることができます。テキスト フィルタは、クエリに含まれる他のすべてのフィルタの結果に対するフィルタとして機能するため、テキスト フィルタの演算子はANDでなければなりません。クエリ バーにテキスト フィルタがすでにある場合は、次の図に示すように[テキスト フィルタ]オプションが無効になります。テキスト フィルタを、括弧内に追加することはできません。

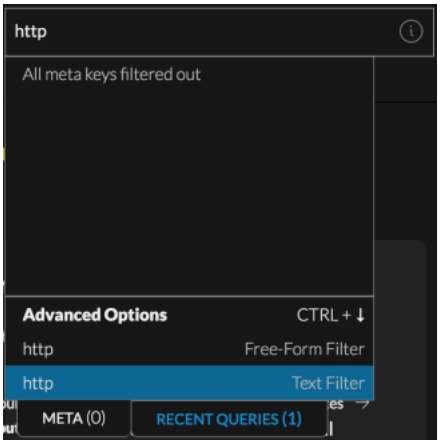


テキスト フィルタを作成するには、次の手順を実行します。

1. [**イベント**]ビューに移動して、クエリ バーをクリックします。
   クエリ入力フォームが表示されます。

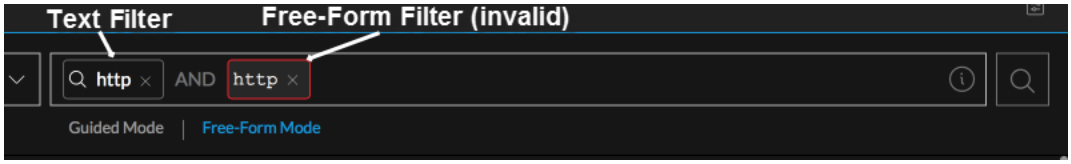


2. 検索するテキスト文字列を入力します(たとえば「`http`」) 。
   テキスト文字列がメタ キー ドロップダウン リストの[詳細オプション]の下に表示されます。

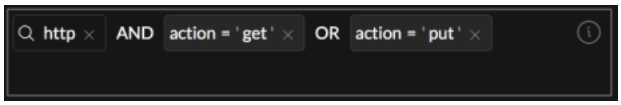


3. [**詳細オプション**]の下にある[**テキスト フィルタ**]をクリックします。
   テキスト フィルタがクエリ バーに追加されます。次の図は、テキスト フィルタとフリーフォーム フィルタの

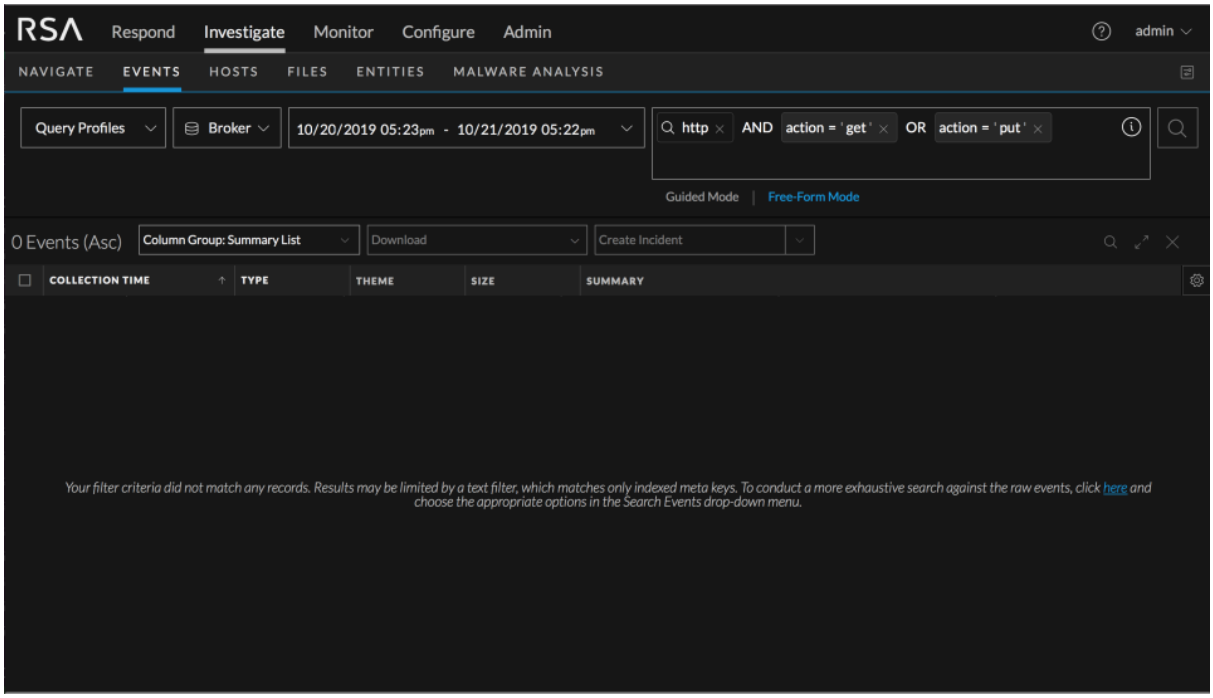
表示の違いを示しています。フリーフォーム フィルタは、固定スペース フォントで表示され、赤色の枠線で囲まれます。フリーフォーム フィルタでは有効な式を入力する必要があるため、赤色の枠線は構文エラーがあることを示しています。テキスト フィルタには、検索アイコンが表示されます。テキスト フィルタには、構文の要件は適用されません。



4. (オプション) シンプルまたはフリーフォームのフィルタをクエリ バーに追加します。クエリに使用できるテキスト フィルタは1つだけです。この例は、「`http`」をテキスト フィルタとして入力し、「`action = 'get' OR action = 'put'`」という2つのフィルタを追加して、クエリを完成しています。

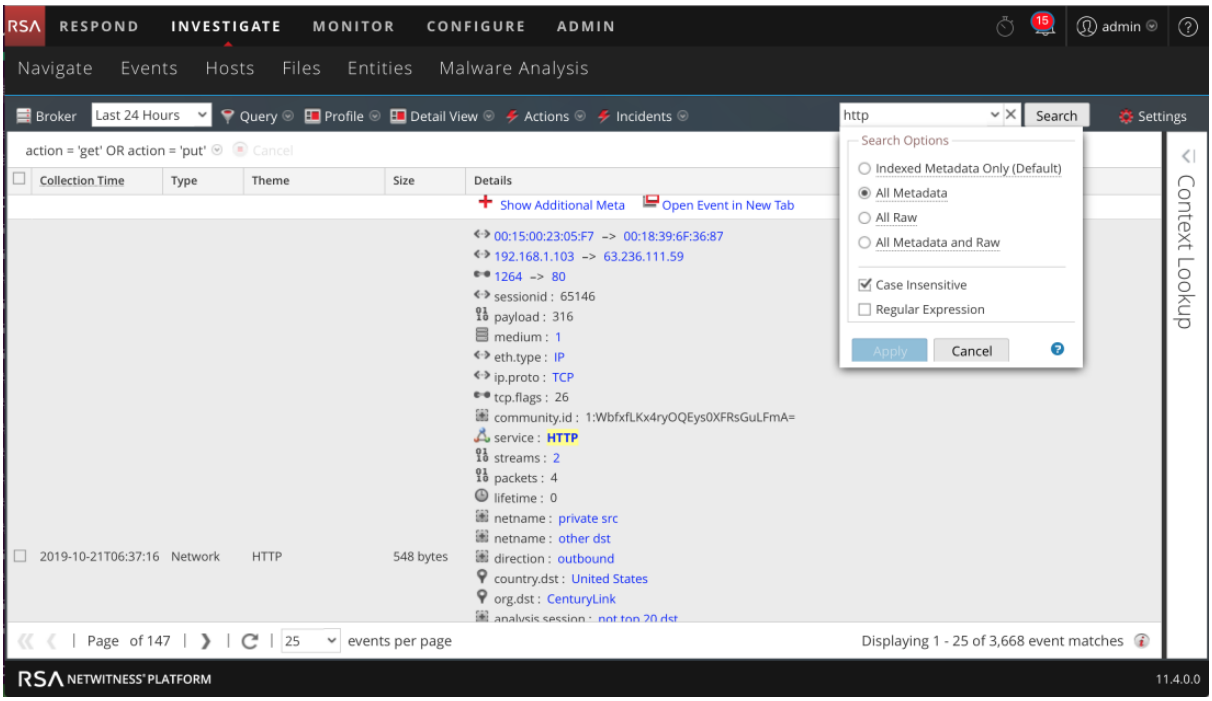


5. クエリを送信するには、  をクリックします。
結果が[イベント]パネルに表示されます。次の図は、結果が見つからなかった[イベント]パネルと、結果を改善する方法を説明したメッセージを示しています。テキスト フィルタを使用するたびに、検索を拡張するためのリンクを提供するこのメッセージが、結果の下部に表示されます。

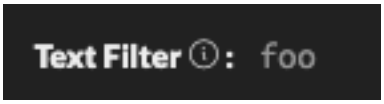


6. メッセージ内の[ここ]リンクをクリックします。
新しいブラウザ タブが開き、クエリの結果が[レガシー イベント]ビューに表示されます。ここでは、検索を改善するための追加のオプションを使用できます。次の図は、インデックスなしのメタデータも対

象に含めて同じクエリを実行した結果を示しています。



7. クエリのステータスを表示するには、クエリ コンソールで(情報アイコン) をクリックします。次の図は、クエリ コンソールに表示されたテキスト フィルタを示しています。



クエリ バーのすべてのフィルタの選択とすべてのフィルタのコピー(バージョン11.4.1以降)

[イベント]ビューのクエリ バーでフィルタを作成するときに、キーボード コマンドを使用して、すべてのフィルタを選択(Windows OSの場合はCtrl-A、MacOSの場合はCmd-A) してから、選択内容をローカルのクリップボードにコピー(Windows OSの場合はCtrl-C、MacOSの場合はCmd-C) できます。

すべてのフィルタを選択してクリップボードにコピーするには、次の手順を実行します。

1. [**イベント**]ビューの[**イベント**]パネルで、フォーカスされた丸またはクエリ入力フォームをクリックして、**Ctrl-A**(Windows OS) または**Cmd-A**(MacOS) を押します。
   クエリ バーのすべてのフィルタが選択されます。
2. 選択したフィルタをクリップボードにコピーするには、**Ctrl-C**(Windows OS) または**Cmd-C**(MacOS) を押します。
   クリップボードの内容を他のアナリストと共有したり、コンテンツをクエリ バーにペーストしたりすることができます。

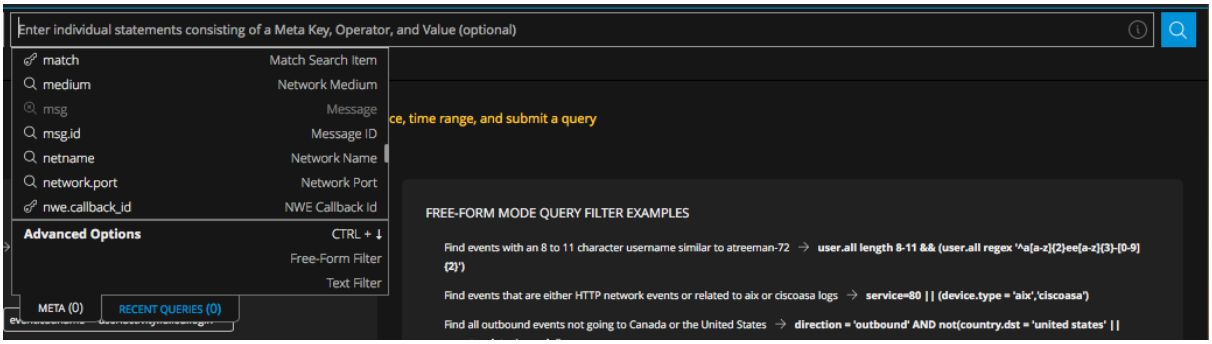
クエリ バーへのテキストのペースト(バージョン11.4以 降)

[イベント]ビューのクエリ バーでフィルタを作 成するときに、フィルタ全 体を直 接 入 力する代 わりに、他 の場 所 からコピーしたテキストをペーストすることができます。テキストを空 のクエリ バーにペーストするか、クエリ バーの既 存 のフィルタの横 にペーストできます。すでに入 力 済 みのテキストに応じて、クエリ解 析 エンジンはペーストされた情 報 を解 析 し、新しいフィルタを作 成します。これには、シンプル フィルタ、フリーフォーム フィルタ、テキスト フィルタが含 まれます。

- 「`<valid meta key> <valid operator> <optional value>`」の形 式 のテキスト文 字 列 が追 加された場 合 、クエリ バーには新しいシンプル フィルタが追 加されます。「`alias.host contains 's'`」はその例 です。
- 「`<valid meta key> <valid operator> <optional value> && <valid meta key> <valid operator> <optional value>`」の形 式 のテキスト文 字 列 が追 加された場 合 、クエリ バーには2つのシンプル フィルタが追 加されます。「`alias.host contains 's' && action exists`」はその例 であり、「`alias.host contains 's' AND action exists`」に変 換されます。
- 解 析 不 可 能なテキストを含 んだテキスト文 字 列 は、フリーフォーム フィルタに変 換されます。たとえば、ガイド モード のフィルタの作 成 では、「`NOT (device.ip = 10.10.10.10)`」という形 式 はサポートされていないため、フリーフォーム フィルタに変 換されます。フリーフォーム フィルタは、クエリ送 信 時 にサーバによって検 証されます。
- フィルタ構 文 に準 拠していないテキストは、フリーフォーム フィルタとして追 加されます。

テキストをペーストしてフィルタを作 成するには、次 の手 順を実 行します。

1. [**イベント**]ビュー> [**イベント**]パネルに移 動し、クエリ バーの下 にある[**ガイド モード**]を選 択して、クエリ バーをクリックします(バージョン11.4.1の場 合 は、クエリ バーを単 にクリックします) 。
   クエリ入 力フォームが表 示されます。



2. **Ctrl-V**(Windows OS) または**Cmd-V**(MacOS) を押 すか、**右 クリック**して[**ペースト**]を選 択して、クリップボード にコピーしたテキストをペーストします。次 のいずれかを実 行します。
   a. ペーストしたテキストが解 析 可 能なステートメントである場 合 は、1つまたは複 数 のシンプル フィルタが作 成されます。
   ペーストしたテキストが解 析 不 可 能なステートメントである場 合 は、新しいフリーフォーム フィルタが作 成されます。
   ペーストしたテキストがステートメントではなく、有 効なメタキ ーではない場 合 は、無 効な構 文 エラーが表 示されます。

新しいフィルタで使用する有効なメタ キーをペーストした場合は、ドロップダウン リストでメタ キーがハイライト表示されます。演算子と値を入力することによって、通常どおりにフィルタの作成を続行できます。
有効なメタ キーと有効な演算子(`city.dst =`など) を選択した後にペーストした場合、メタ キーがテキスト値をサポートしていれば、ペーストされたテキストはテキスト文字列として扱われ、フィルタが1つ作成されます。メタ キーがテキスト値をサポートしていない場合は、クエリ バー内のすべてのテキストが、前述の手順の説明に従って解析されます。

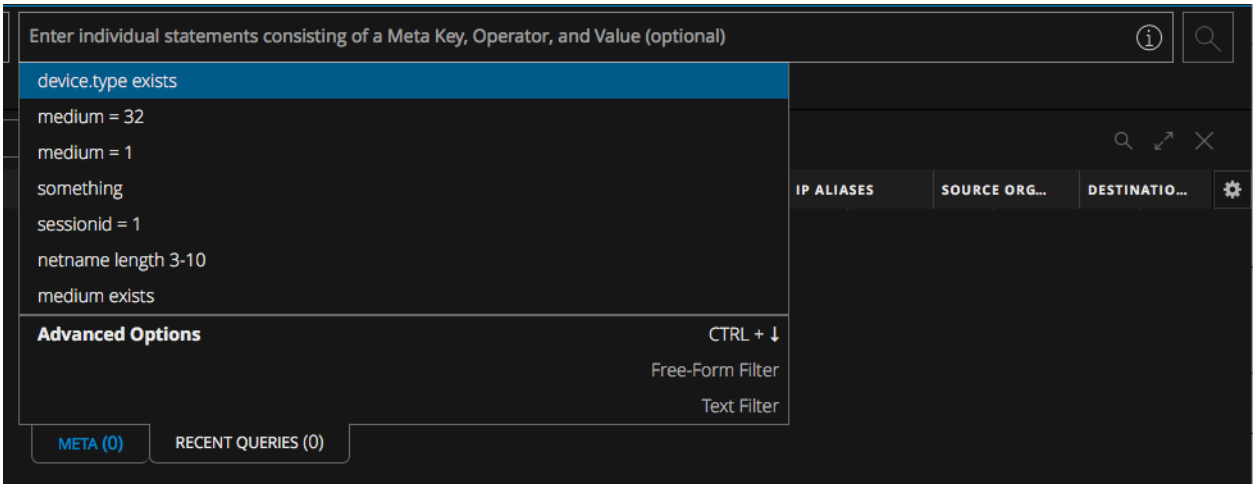
3. 必要に応じてクエリ バーにさらにフィルタを追加し、クエリを送信します。
クエリが実行されます。

最近のクエリからのフィルタの挿入 (バージョン11.4以降)

ガイド モードのクエリ バーでは、最近実行したクエリからフィルタを挿入できます。[最近のクエリ] タブを開いた時、クエリ バーに何も入力されていない場合は、最近実行した最大100件のクエリがスクロール可能なリストに表示されます。最新のクエリが一番上に表示されるようにリストがソートされ、[最近のクエリ] タブのカウントは0に設定されます。入力を開始すると、入力と一致するテキストを含んだ最大100件のクエリがクエリ履歴データベースから表示されます。テキストが一致していれば、最新の100件のクエリに含まれていない場合でも表示されます。[最近のクエリ] カウントは、入力と一致するクエリの数を反映して変化します。

デフォルトで、リストの一番上の項目がハイライト表示されます。最近のクエリを選択するには、上下矢印を使用してハイライト表示を上下に移動するか、目的のクエリの上にマウスを合わせます。入力に合わせて、リストが絞り込まれ、ハイライト表示がリストの一番上に戻ります。クエリをクリックするか、クエリがハイライト表示された状態でEnterを押すと、選択したクエリのテキストを含んだ新しいフィルタが作成されます。

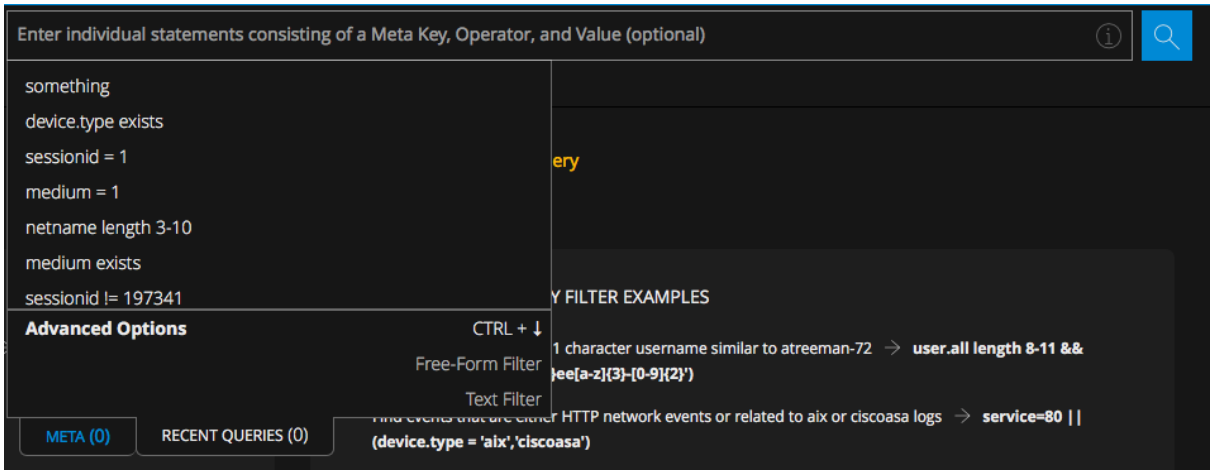
クエリを送信するたびに、リストがソートされ、そのクエリが最新のクエリとして一番上に追加されます。



最近のクエリからフィルタを作成するには、次の手順を実行します。

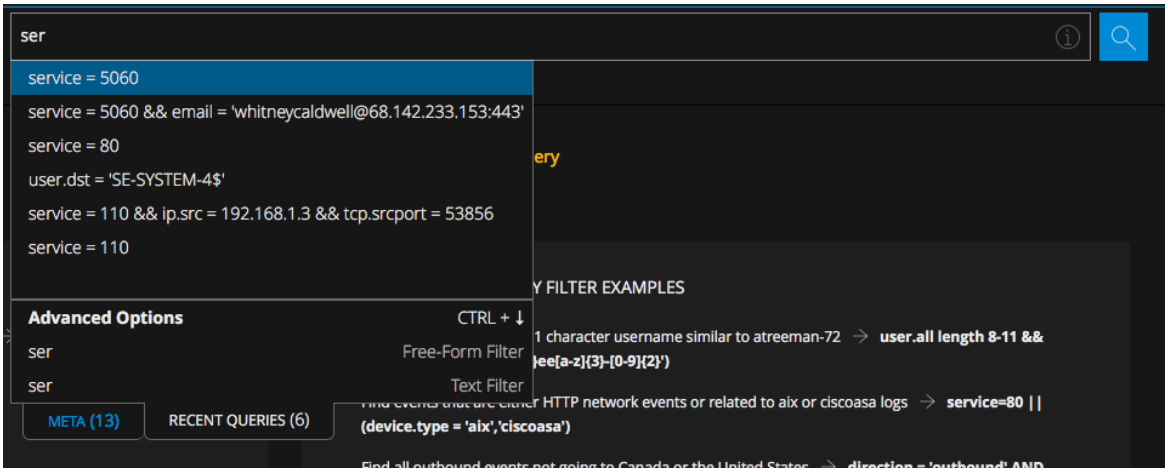
1. [**イベント**] ビューに移動し、クエリ バーの下にある[**ガイド モード**] を選択して、クエリ バーをクリックします(バージョン11.4.1の場合は、クエリ バーを単にクリックします) 。
[メタ キー] ドロップダウン リストが[メタ] タブに表示されます。

2. [**最近のクエリ**]タブを選択します。
[最近のクエリ]ドロップダウン リストが表示され、カウントには0が表示されます。



3. 最近のクエリを検索するには、次のいずれかを実行します。

   a. テキストの入力を開始します。
   文字の入力に合わせて、またはBackspaceキーを押して文字を削除するのに合わせて、リストが絞り込まれ、入力したテキストを含む最近のクエリが表示されます。[最近のクエリ]ラベルのカウントは、入力と一致するクエリの数を反映して変化します。



   b. クエリを選択して新しいフィルタを追加するには、入力を続けて、新しいフィルタとして使用したいクエリを見つけ、上下矢印でハイライト表示します。

   c. クエリをハイライト表示して**Enter**を押すか、リストに表示されているクエリを単にクリックします。
   フィルタがクエリ バーに追加されます。

4. 必要に応じてクエリ バーにさらにフィルタを追加したら、クエリを送信します。
クエリが実行され、リストがソートされ、そのクエリが最新のクエリとして一番上に追加されます。

ガイド モードでのフィルタの編集

ガイド モードのクエリ バーで、フィルタを編集できます。フィルタを編集するには、次の操作を行います。

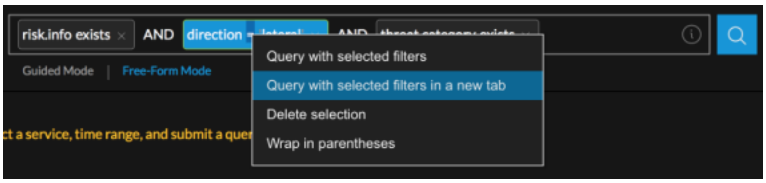
1. フィルタをダブルクリックするか、フィルタをクリックしてEnterを押します。
2. フィルタを編集します。編集が終了したら、Enterを押してフィルタを更新します。
3. クエリを再度実行する場合は、をクリックします。
   更新されたフィルタの結果が[イベント]パネルに表示されます。

ガイド モードで選択したフィルタを使用したクエリ

ガイド モードのクエリ バーに1つまたは複数のフィルタがある場合は、選択したフィルタのみを含むクエリを再フォーカスし、現在のブラウザ タブまたは新しいブラウザ タブに結果を表示できます。バージョン11.4では、フィルタにネスト構造の括弧を使用した式が含まれる場合があり、そのようなフィルタの一部分を再フォーカスできます。選択したフィルタのみを使用してクエリを更新するには、次のいずれかを実行します。

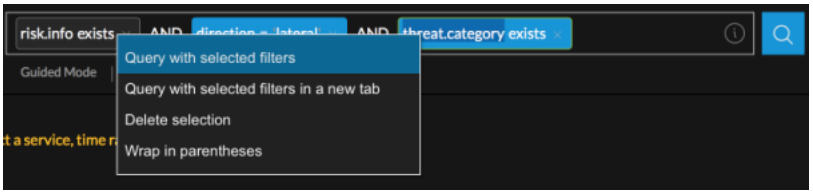
1. 1つ以上のシンプル フィルタを含むクエリを使用します。たとえば、`risk.info exists`、`direction ='lateral'`、`threat.category exists`という3つのフィルタを含んだクエリを使用します。

   a. `direction = 'lateral'`を選択し、右クリックして[**新しいタブで、選択したフィルタでクエリを実行**]をドロップダウン メニューで選択します。

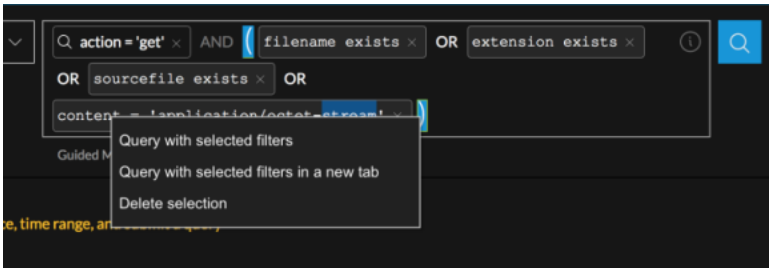
   選択したフィルタの結果が新しいタブに表示され、元のクエリは以前のタブにそのまま残ります。

   b. 選択したフィルタを使用して、同じタブでクエリを実行するには、`direction = "lateral"`と`threat.category exists`を選択します。次に、右クリックして[**選択したフィルタでクエリを実行**]をドロップダウン メニューで選択します。

   選択したフィルタのみを含むクエリが送信され、残りのすべてのフィルタが削除されます。

2. (バージョン11.4) ネスト構造の括弧を使用したフィルタを含むクエリの場合(たとえば、`action = 'get' AND (filename exists OR sourcefile exists OR content = 'application/octet-stream')`)は、次のいずれかを実行します。

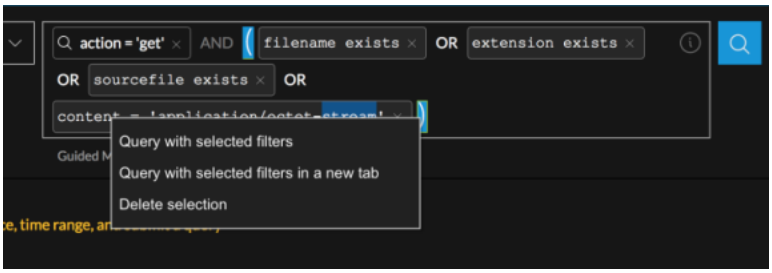
a. `'application/octet-stream'`の後の閉じ括弧を選択し、右クリックして[**新しいタブで、選択したフィルタでクエリを実行**]を選択します。
`(filename exists OR sourcefile exists OR content = 'application/octet-stream')`の結果が新しいタブに表示されます。

b. 同じものを選択し、右クリックして[**選択したフィルタでクエリを実行**]を選択します。
`(filename exists OR sourcefile exists OR content = 'application/octet-stream')`の結果が現在のタブに表示されます。

ガイド モードでのフィルタの削除とフィルタ内のテキストまたは括弧の削除

バージョン11.4では、キー操作による編集機能が使用可能になりました。これらの機能は、各ステップに明記されています。

1. フィルタを削除するには、次のいずれかを実行します。
   a. フィルタの[**X**]をクリックします。
   b. フィルタを選択して、**Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。
   c. (バージョン11.4以降) フィルタを選択して、**Backspace**(Windows OS) または**Delete**(MacOS) を押します。
   d. 1つまたは複数のフィルタを右クリックし、ドロップダウン メニューで[**選択したフィルタを削除**]または[**選択項目の削除**](バージョン11.4以降) を選択します。
   フィルタとフィルタの右または左にある演算子が削除され、クエリ バーに余分な演算子が残っていないことが確認されます。
2. (バージョン11.4以降) フィルタ内の文字、またはフィルタ内の括弧とその中身を削除するには、次のいずれかの手順を実行します。
   a. 前の文字を削除する場合 : クエリ バーで文字の横にカーソルを置いて、**Backspace**(Windows OS) または**Delete**(MacOS) を押します。
   b. すべての文字を削除する場合 : フィルタにカーソルを合わせて、**Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。
   c. 選択した文字を削除する場合 : クエリ バーで文字を選択して、**Delete**または**Backspace**を押します。
   d. 括弧内の文字を残して括弧を削除するには、括弧のいずれかを選択して**Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。
   e. 括弧とその中身(たとえば「`(filename exists OR sourcefile exists OR content = 'application/octet-stream')`」) を削除するには、`get`の後の括弧を選択して、右クリックし、[**選択項目の削除**]を選択します。

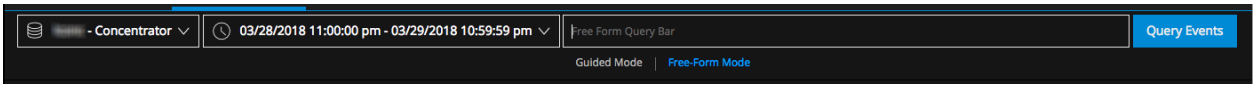


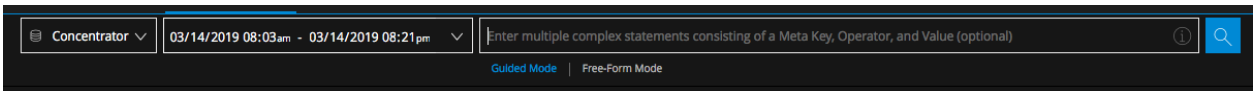
`action = 'get'`以外のすべてが削除されます。

フリーフォーム モードでのクエリの作成

フリーフォーム モードはバージョン11.2、11.3、11.4で使用されますが、バージョン11.4.1では使用できなくなりました。

フリーフォーム クエリが役立つのは、保存された長いテキスト文字列をペーストしたい場合や、すばやく入力したいクエリがあり、そのメタ キー、有効な演算子、値を入力するための正しい構文がわかっている場合です。次の図は、フリーフォーム クエリビルダのフィールドが空になっている、初期状態の[イベント]ビューを示しています。最初の例はバージョン11.2で、2番目の例はバージョン11.3です。





点滅するカーソルは、クエリを入力できることを示しています。ここにテキストを自由に入力できます。式を追加してゆき、1行に表示しきれなくなると、次の行に折り返され、入力領域が縦に広がります。このため、右にスクロールしなくても、すべてのフィルタを表示できます。

フリーフォーム モードで入力できるクエリの例を次に示します。

atreeman-72に類似した8～11文字のユーザ名でイベントを検索する場合:

```
user.all length 8-11 && (user.all regex '^a[a-z]{2}ee[a-z]{3}-[0-9]{2}')
```

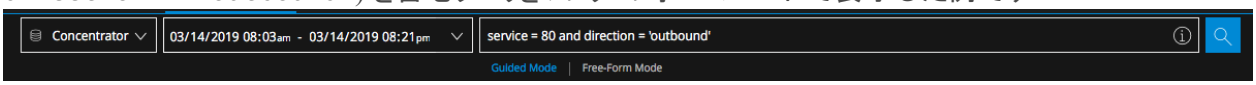
HTTPネットワーク イベントとaixまたはciscoasaログに関連するイベントを検索する場合:

```
service=80 || (device.type = 'aix','ciscoasa')
```

カナダまたは米国以外に向けたアウトバウンド イベントを検索する場合:

```
direction = 'outbound' AND not(country.dst = 'united states' || country.dst = 'canada')
```

ガイド モードで送信済みのクエリがある場合、[フリーフォーム モードに切り替える]をクリックすると、クエリがテキストに変換されます。次の図は、ガイド モードで送信した2つのフィルタ(`service = 80`および`direction = 'outbound'`)を含むクエリを、フリーフォーム モードで表示した例です。



クエリビルダの右側の  ボタンは、必要に応じてクエリを送信するために表示されます。クエリは、  をクリックすると送信されます。その時点でクエリが検証され、構文およびロジックのエラーが表示されます。

より多くの処理時間を必要とする演算子は、ガイド モードのようにハイライト表示されませんが、次の表は負荷の高い演算子の概要を示しています。

インデックス方法	テキスト以外の値	テキスト値	普通の演算子	高負荷の演算子
キー	✓		exists、!exists	eq、!eq
キー		✓	exists、!exists	eq、!eq、begins、ends、contains
値	✓		exists、!exists、eq、!eq	高負荷の演算子なし
値		✓	exists、!exists、eq、!eq、begins	ends、contains
なし	sessionidの特別なケース		exist、!exits、eq、!eq	高負荷の演算子なし

[ナビゲート]ビューでの結果のフィルタリング

[ナビゲート]ビューで調査を実施する場合は、メタ キーの値を[ナビゲート]ビューにロードする時に、いくつかの方法で表示する結果を絞り込むことができます。このトピックの後半では、基本的なデータのフィルタリング方法を中心に説明します。

- 時間範囲の設定
- メタ キー結果の集計方法とソート順の設定
- 調査でのデフォルト メタ キーの管理と適用
- [ナビゲート]ビューのタイム チャートでのデータのドリル ダウン
- [値]パネルでのデータのドリルダウン

時間範囲の設定

[ナビゲート]ビューで調査を実施する際、返される結果を制限するには、時間範囲のオプション設定を使用します。次のオプションを選択できます。

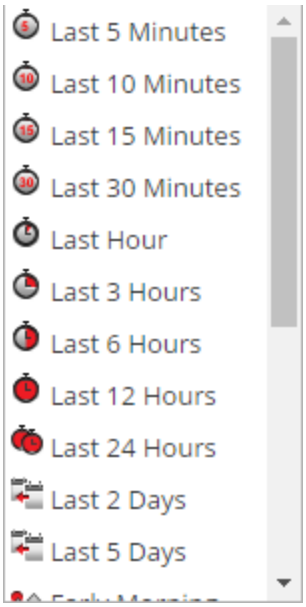
- 収集データの時間範囲。最後に収集されたデータの時刻を基準にして、一定の時間範囲を選択します。
- カレンダーの日付を基準にした時間範囲。
- カスタムの時間範囲。
- すべてのデータ。

選択した日付範囲が[ナビゲート]ビューのツール バーに時間範囲ラベルとして表示されます。デフォルトのラベルは[**直近3時間**]です。タイムライン バナーに表示される時間範囲には、メタデータに使用されている日付範囲の最初と最後のタイムスタンプが表示されます。

注： 時間範囲の設定で使用する日付と時刻は、『*RSA NetWitness Platform スタート ガイド*』の「ユーザ環境設定の設定」で説明されているように、[プロファイル]の[環境設定]パネルに構成されている[タイム ゾーン]をベースとしています。

標準提供の時間範囲を選択するには、次の手順に従います。

1. [ナビゲーション]ビューのツールバーの[**時間範囲**]オプションをクリックします。デフォルトの時間範囲は[**直近3時間**]ですが、すでに選択リストから別の値([**すべてのデータ**]、[**直近1時間**]など)が選択され、オプション パネルのラベルとして表示されている場合があります。
   時間範囲の選択リストが表示されます。



2. 次のいずれかを実行します。
   - すべてのデータを表示する場合は、[**すべてのデータ**]を選択します。
   - 時間範囲を収集に対する分、時間、日単位で設定する場合は、[**直近10分**]、[**直近3時間**]、[**直近5日**]のような値を選択します。
   - 現在からの相対的な時間範囲を設定する場合は、[**昨日**]、[**今週**](バージョン11.1)、[**先週**](バージョン11.1)、[**終日**]、または[**早朝**]、[**午前**]、[**午後**]、[**夕方**]のような1日の一部を選択します。
   - カスタムの日付範囲を設定する場合は、[**時間範囲**]メニューの[**カスタム**]を選択し、以下の手順を実行します。
     選択した時間範囲は値パネルの上部にも表示されます。

カスタム時間範囲を指定するには、次の手順に従います。

1. [**時間範囲**]メニューで[**カスタム**]を選択します。
   日付選択オプションはツールバーに表示されます。

2. [**開始日**]および[**終了日**]フィールド内で、次の手順を実行して日付と時間を指定します。
   a. カレンダーから日付をクリックします。
   b. (オプション)[時間]および[分]フィールドから時間を選択するか、[**現在**]をクリックします。時間の選択は、デフォルトで日の現在時間となります。

注: 開始時刻の秒は常に:00に、終了時刻の秒は常に:59に変更されます。たとえば、時間を使用して問題にドリルダウンする場合、ドリル時間は「HH:MM:00～HH:MM:59」と解釈されます。

3. 範囲を適用するには、[**表示**]をクリックします。
   選択した時間範囲が、[値]パネルの現在の結果に適用されます。

メタ キー結果の集計方法とソート順の設定

[ナビゲート]ビューで各メタ キーの結果をどのようにカウントし、ソートするかを選択できます。

注: メタ グループでメタ エンティティ(バージョン11.1以降) が使用されている場合は、メタ エンティティに含まれるメタ キーのいずれかと一致する上位20の値が結果に表示されます。

[ナビゲート]ビューにある各メタ キーのセクションには、各メタ キーの値([値]) とそのカウント([件数]) が一定の順序でリストされます。次の設定を行うことができます。

- 各メタ キー セクションの結果を[値]または[合計]のどちらに基づいてソートするか。
- 結果を昇順でソートするか降順でソートするか。
- 各メタ キーに表示される値をパケット数で集計([パケット数]) するか、セッションまたはログ数で集計するか([イベント数で集計]) 、イベントのサイズで集計([イベント サイズで集計]) するか。

注: Log DecoderとPacket Decoderの両方のメタを表示している場合、実際の算出される数はキーのタイプによって異なります。パケット数で集計することを選択した場合にログを調べると、[ナビゲート]ビューの出力は、[イベント数で集計]を選択した場合と同じ出力になります(詳細については、「[ナビゲート]ビュー」を参照してください) 。

次の図では、「Event Type」というメタ キーは、[**合計**]の**降順**で表示されています。一致件数の最も多い値が最初に表示されています。値failure auditは一致件数が71件であり、先頭に表示されています。値logonは一致件数が1件しかなく、最後に表示されています。集計方法は[**イベント数**]です。

次の図では、「Event Type」というメタ キーが[**値**]の**降順**で表示されています。アルファベットの最後の文字から順に、値が表示されていることが分かります。値success auditが先頭に表示されています。値connectが最後に表示されています。集計方法は[**イベント数**]です。

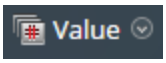
[ナビゲート]ビューでメタ キーを集計する方法と結果の表示順を選択するには、次の手順を実行します。

1. ツールバーで、[**イベント数**]、[**イベント サイズ**]、[**パケット数**]のいずれかをクリックし、ドロップダウン メニューで集計オプションを1つ選択します。選択したオプションがメニューのラベルに表示されます。

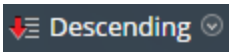
   

   選択内容に応じて現在のビューが再ロードされます。

2. ツールバーで、[**合計**]または[**値**]をクリックし、ドロップダウン メニューからいずれかのソート条件を選択します。選択したオプションがメニューのラベルに表示されます。

   選択内容に応じて現在のビューが再ロードされます。

3. ツールバーで、[**昇順**]または[**降順**]をクリックし、ドロップダウン メニューからいずれかのソート順を選択します。選択したオプションがメニューのラベルに表示されます。
   選択内容に応じて現在のビューが再ロードされます。
   

調査でのデフォルト メタ キーの管理と適用

収集したデータの調査をアナリストがInvestigateで実施する際は、メタ キーのデフォルトのセットが[ナビゲート]ビューの[値]パネルにデフォルトの順序でロードされて表示されます。デフォルトのコンテンツと順序は、調査対象のサービスのメタ キーに基づきます。アナリストは、デフォルトのメタ キーを選択するかユーザ定義のメタ キーのグループを選択することにより、調査の際に表示するメタ キーを指定でき、メタ キーの定義や表示を柔軟に行うことができます。これにより、目的のデータにより直接的にドリル ダウンできるようになります。また、現在の調査には関係のないメタをロードせずに済むため、ロードの時間の短縮にも役立ちます。

注: バージョン11.1以降では、メタ キーを使用可能な場所では、構成済みのメタ エンティティも使用できます。

有効なカスタム メタ グループがない場合は、[デフォルトのメタ キーの管理]ダイアログの表示オプションで指定されたメタが表示されます。[ナビゲート]ビューの[値]パネルでのメタ キーのロードを最適化するために、NetWitness Platformはデフォルトではインデックスなしのメタ キーを展開しません。インデックスなしのメタ キーを[値]ビューで展開すると、NetWitness Platformによってそのメタ キーの値のロードが開始されます。ロード時間が長くなりすぎると、メッセージが表示されてメタ キーのロードはタイムアウトになります。インデックスなしのメタ キーのタイトル、値、数は、[値]パネルでは詳しく調べることができません。Investigationでラベル付けを行い、インデックスなしのメタ キーを識別します。

調査に使用するメタ キーを選択するには、次のいずれかの手順を実行します。

- デフォルトのメタ キーを選択する。
- メタ キー セット(メタ グループ)を選択する。

注: 調査には、標準提供のメタ グループとユーザ定義のメタ グループがあります。作成したユーザ定義のメタ グループは、編集と削除が可能であるほか、エクスポートやインポートが可能です。これらの手順については、「メタ グループを使用して関連性の高いメタ キーにフォーカス」という別のトピックで説明されています。

[デフォルトのメタ キー]ダイアログでは、[調査]>[ナビゲート]ビューで特定のサービスについて調査するときに、メタ キーのデフォルト表示オプションを指定できます。キーごと、またはすべてのキーについて、デフォルトの表示を次のように設定できます。

- [非表示]: デフォルトのメタ キーの結果を非表示にし、ロードしません。
- [展開表示]: デフォルトのメタ キーの結果を展開し、値と数(セッションの合計)を表示します。
- [折りたたみ表示]: デフォルトのメタ キーの結果を折りたたみ、メタの名前だけが表示されるようにします。
- [自動]: デフォルトのメタ キーのロードをインデックス レベルで制御します。そのためには、値によってインデックスされている必要があります。

デフォルトのメタ キーはさまざまなサービス向けに変更できるため、別のサービスのドリルダウン ポイントに移動したときに、同じデフォルトのメタ キーのセットが表示されないことがあります。デフォルトのメタ キーを使用する場合は、この点に注意してください。目的のデータが表示されない場合は、デフォルトのメタ キーの初期表示を変更する必要があります。

デフォルトのメタ キーの初期状態を[ナビゲート]ビュー内で変更した場合、変更はそのサービスに対して持続されます。コア サービスのカスタム インデックス ファイル(たとえば、`concentrator-custom-index.xml`、`decoder-custom-index.xml`など) に新しいキーを追加する場合、その新しいキーは、デフォルトのメタ キーのリストに追加されます。[ナビゲート]ビューで設定された変更は、現在のサービスにのみ適用されます。

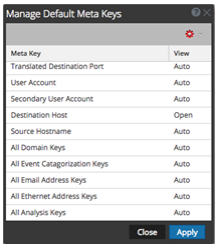
初期の[ナビゲート]ビューがデフォルトのメタ キーを使用して開くように指定するには、次の手順を実行します。

1. [**調査**]>[**ナビゲート**]に移動します。
2. サービスを選択し、[**ナビゲート**]を選択します。
3. [**メタ**]メニューで、[**デフォルトのメタ キーを使用**]を選択します。
   調査がすでに進行中である場合、データが現在のビューに再ロードされ、選択したオプションには目印のアイコンが表示されます。まだデータがロードされていない場合、デフォルトのメタ キーが次回のロードに使用されます。

デフォルトのメタ キーの構成

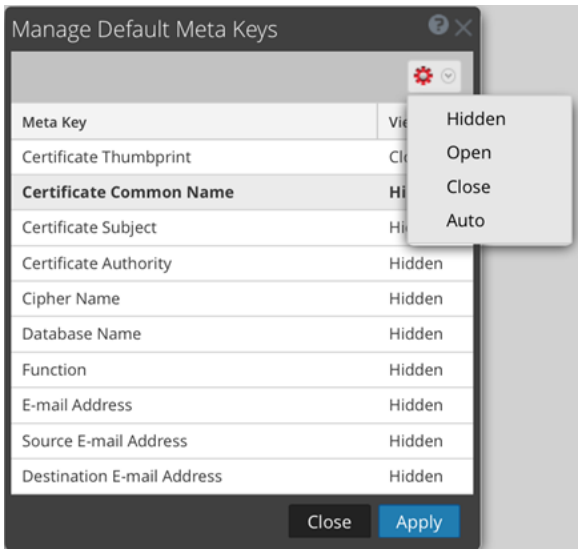
[ナビゲート]ビューでデフォルトのメタ キーのデフォルトの表示を構成するには、次の手順を実行します。

1. [**ナビゲート**]ビューのツールバーで、[**メタ**]>[**デフォルトのメタ キーの管理**]を選択します。
   [デフォルトのメタ キーの管理]ダイアログが表示され、サービスで利用可能なメタ キーのリストが表示されます。



2. (オプション) キーの順序を変更するには、1つ以上のキーを選択し、上方向または下方向にドラッグします。
3. 次のいずれかを実行します。
   - (オプション) すべてのメタ キーのデフォルトの表示を変更するには、キーが選択されていないことを確認して、ツールバーで を選択します。
   - (オプション) 1つ以上のキーのデフォルトの表示を変更するには、キーを選択して、ツールバーで を選択します。

すべてのデフォルトのメタ キーに使用可能な初期表示のドロップダウン メニューが表示されます。



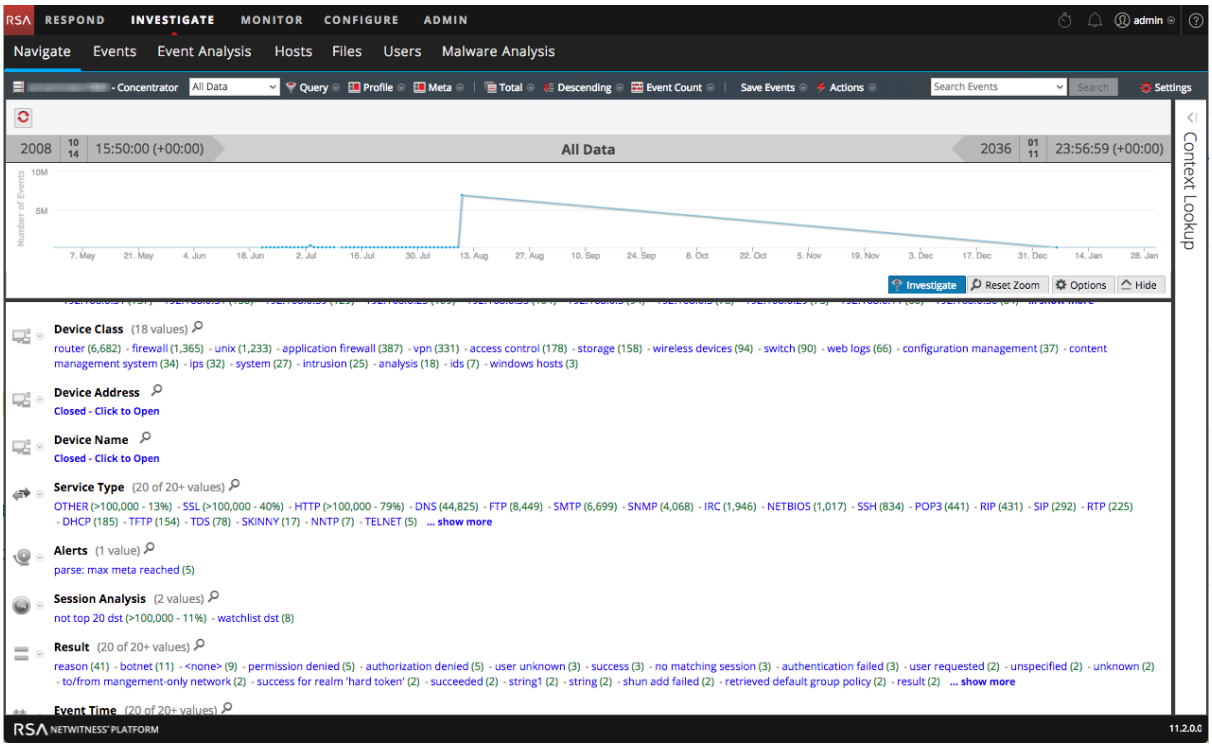
- (オプション) メタ キーをサービス インデックス ファイルで指定されているとおりのデフォルトの表示に戻すには、キーが選択されていないことを確認して、ツールバーで ⚙ > [**自動**]を選択します。
  インデックスなしのメタ キーのデフォルト ビューを変更する場合、キーを展開表示に設定できません。メタ グループのデフォルト ビューを展開表示に変更し、一部のメタ キーがインデックスなしであった場合、インデックスなしのメタ キーは自動的に自動に戻ります。したがって、メタ キーはインデックス付きである場合にのみ自動的にロードされます。インデックスなしのメタ キーは手動で開くまで折りたたみ表示になります。

4. いずれかの表示方法を選択します。
5. [**適用**]をクリックして、変更を保存します。
   [ナビゲート]ビューに表示されるメタ キーは、指定された内容で設定されます。デフォルトのメタ キーが非表示の場合、そのメタ キーの値は調査では一切表示されません。デフォルトのメタ キーが折りたたみ表示の場合、そのメタ キーの値はデフォルトではロードされません。ただし、[ナビゲート]ビューで個々のメタ キーを手動でロードすることはできます。

[ナビゲート]ビューのタイム チャートでのデータのドリル ダウン

アナリストは、タイム チャートを使用して、時間の経過に従ってアクティビティを可視化することができます。時間範囲を選択して、[調査]オプションを選択して、データにズーム インすることができます。その後、ズーム インの前に有効であった時間範囲にナビゲーションをリセットできます。

1. [**調査**] > [**ナビゲート**]に移動します。
   現在のドリルダウン ポイントおよび選択した時間範囲のタイム チャートが表示されます。



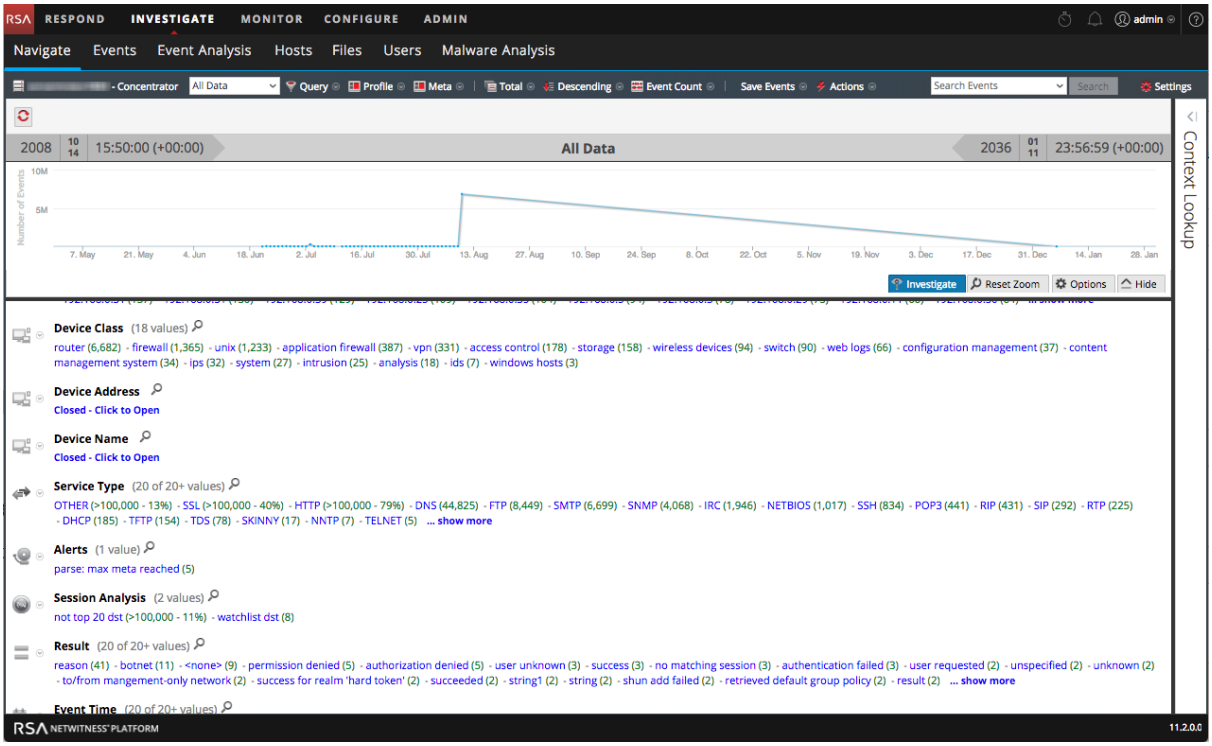
2. タイム チャート上でマウスのクリックとドラッグを行い、目的の時間範囲を選択します。選択した時間範囲がハイライト表示されます。
   選択した時間範囲のタイム チャートが再描画されます。ただし、メタ値は変更されません。
3. 選択した時間範囲のデータにドリル ダウンするには、[**調査**]をクリックします。
   URLが更新され、新しい時間範囲が反映されます。さらに、調査オプション パネルでは、時間範囲がカスタム時間範囲に変更されます。選択した時間範囲を使用して、タイム チャートが再描画され、メタ値がロードされます。
4. タイム チャートを元の時間範囲にリセットするには、[**ズームのリセット**]をクリックします。
   URLが、データのズームを行う前の元のURLに戻ります。また、調査オプション パネルでは、時間範囲がズームを行う前の時間範囲に戻ります。元の時間範囲を使用して、タイム チャートが再描画され、メタ値がロードされます。

[値]パネルでのデータのドリルダウン

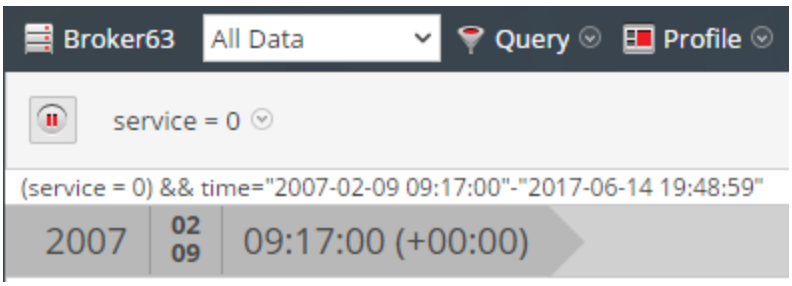
NetWitness Platformでは、[調査]>[ナビゲート]ビューに、選択したサービスのアクティビティと値が表示されます。調査のためにアナリストがメタ キーまたはメタ値をクリックしてデータをドリルダウンすると、クエリが実行されます。[値]パネルで、各クエリは階層リンクのデータに追加されます。これにより、各クエリへのリンクを含む階層リンクが画面上部に表示されます。階層リンクを編集して、クエリを挿入したり、削除したりできます。

メタデータのサブセットにドリルダウンするには、次の手順を実行します。

1. 調査を開始して、[ナビゲート]ビューにメタデータを表示します。

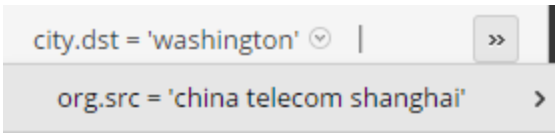


2. メタ データをドリル ダウンするには、次の操作を任意の組み合わせで実行します。
   a. **メタ キー**、たとえば、[**Service Type**]をクリックします。
   b. 結果内の**メタ値**(青色のテキストで表示)をクリックします。たとえば、[**OTHER**]をクリックします。
      メタ キーまたはメタ値をクリックするたびに、データを絞り込む焦点(ドリルダウン ポイント)を狭めながらクエリが実行されます。ドリルダウン ポイントごとに結果パネルが更新され、新しいドリルダウン ポイントが階層リンクに表示されます。次の図は、初期の階層リンクの例です。



      次の図は、ツールバーに収まらない長い階層リンクの例です。ツールバーの最後のクエリの後ろにドロップダウン メニューが表示され、その中にツールバーに収まらなかった他のクエリのリストが表示されます。このドロップダウン リストからクエリを選択して、ドリルダウン ポイントを選択するこ

とができます。

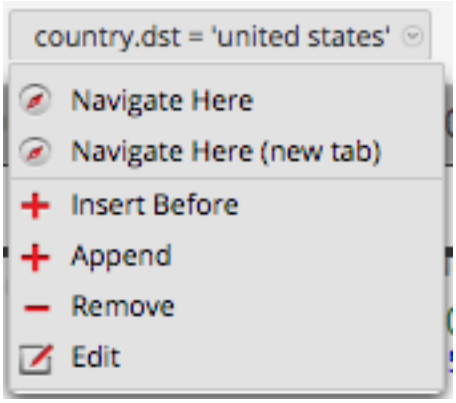


階層リンクでクエリを追加するには、次の手順を実行します。

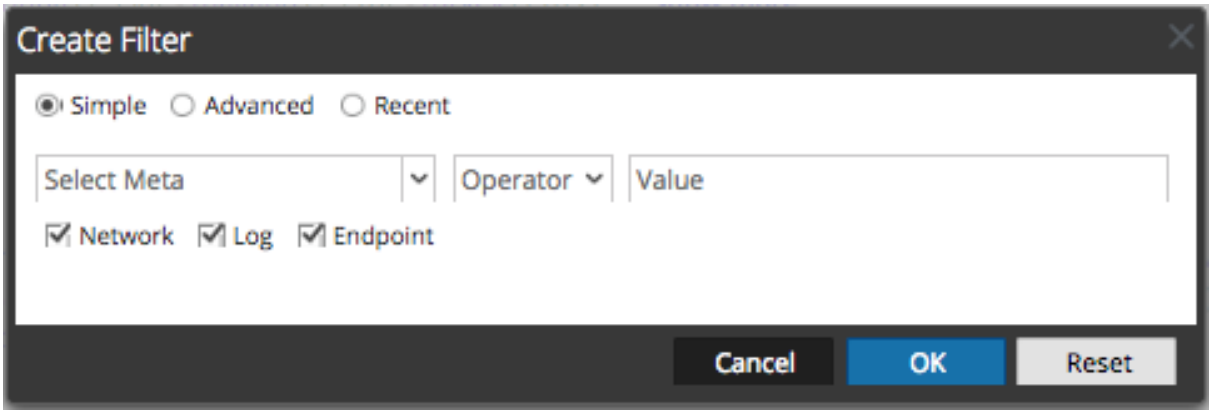
階層リンクにある任意のクエリをクリックすると、クエリメニューを表示できます。クエリの前に新しいクエリを挿入することや、階層リンクの末尾に新しいクエリを追加することができます。階層リンクを編集すると、その都度、NetWitness Platformによって結果が更新されます。

階層リンクでクエリを追加するには、次の手順を実行します。

1. 階層リンクにある任意のクエリをクリックします。
   階層リンクメニューが表示されます。



2. クエリを追加するには、[**後にクエリを挿入**]または[**前にクエリを挿入**]を選択します。
   [フィルタの作成]ダイアログが表示されます。



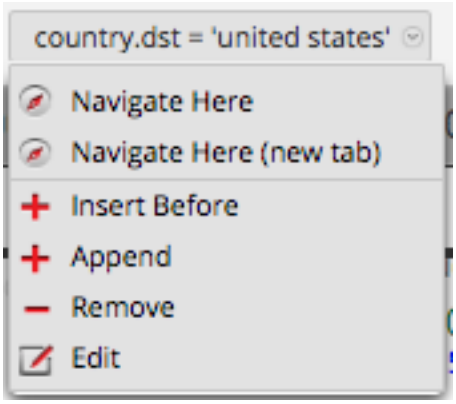
3. 「[[ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成](#)」の記載に従って、クエリを作成します。

階層リンクでのクエリを編集するには、次の手順を実行します。

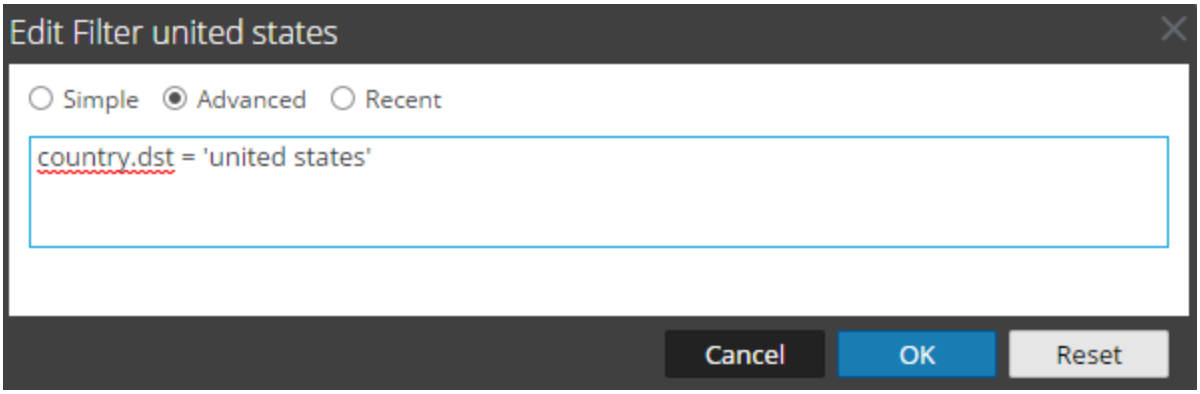
階層リンクにある任意のクエリをクリックすると、クエリメニューを表示できます。クエリを削除したり、クエリを編集することができます。階層リンクを編集すると、その都度、NetWitness Platformによって結果が更新されます。

階層リンク内のクエリを操作するには、次の手順を実行します。

1. 階層リンクにある任意のクエリをクリックします。
   階層リンク メニューが表示されます。



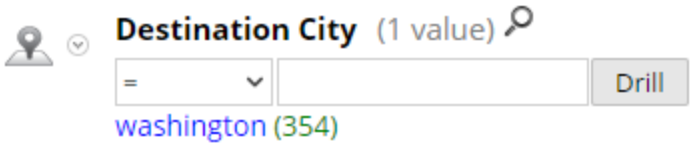
2. クエリを編集するには、[**編集**]を選択します。
   [作成]ダイアログに、選択したクエリの編集画面が表示されます。



3. 「[ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成」の記載に従って、フィールドを編集します。

メタ キー内でクイック検索を実行するには、次の手順を実行します。

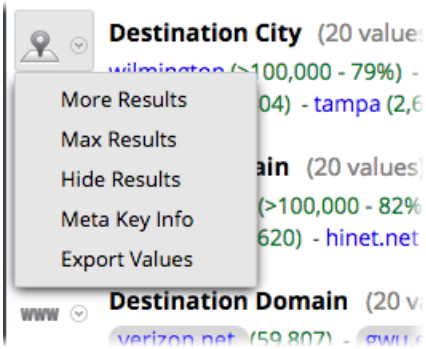
1. メタ キー セクションに移動し、虫眼鏡アイコンをクリックします。
   [クイック検索]フォームが開きます。演算子とテキスト入力ボックスが表示され、検索条件を指定できます。



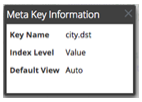
2. (オプション) この検索フォームを閉じるには、虫眼鏡アイコンをもう一度クリックしてください。
3. 左のドロップダウン リストから演算子を選択し、検索するテキスト値を入力します。[**ドリル ダウン**]をクリックすると、検索が実行されます。
   指定したメタキーとメタ値を使用して現在表示中のメタデータが絞り込まれ、結果が表示されます。

メタ キー情報を表示して、メタ キーのメタ値をコピーするには、次の手順を実行します。

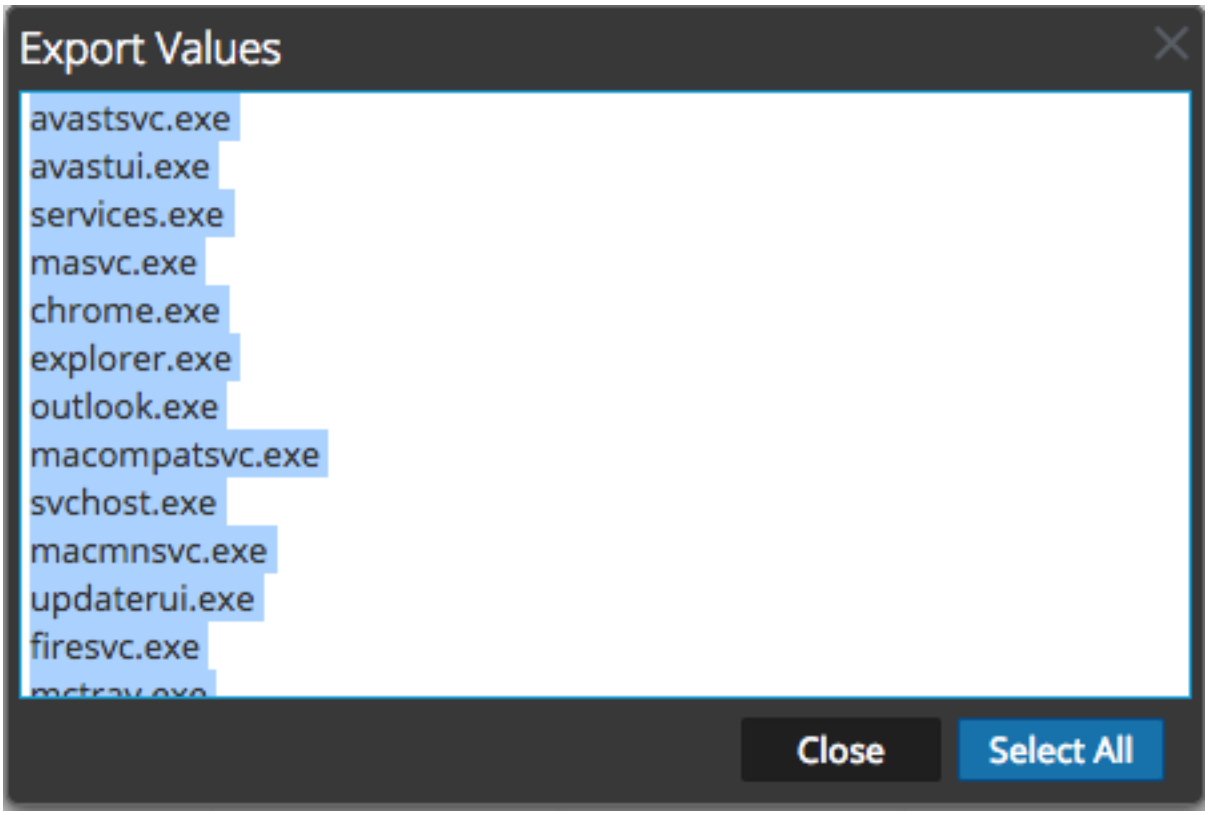
1. キー名、メタ キー表示用に設定されたインデックス レベル、メタ キーに設定されたデフォルト ビューを表示するには、メタ キーの横に表示されるドロップダウン メニューをクリックします。次の図は、バージョン11.1以降のドロップダウン メニューを示しています。



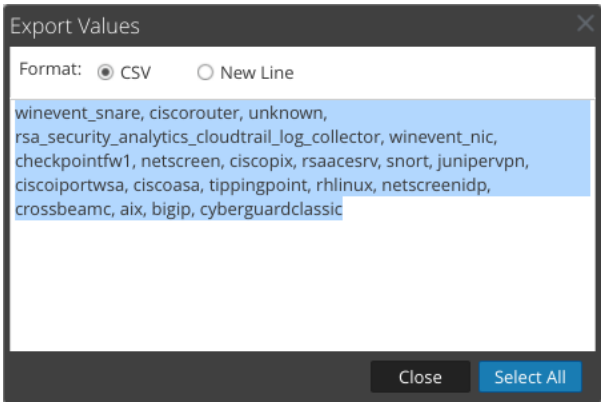
2. [**メタ キー情報**]を選択します。
[メタ キー情報]ダイアログが表示されます。



3. ダイアログを閉じるには、✕をクリックします。
4. (バージョン11.1以降ではオプション) メタ キーの見つかったメタ値をコピー可能なシンプルなリストで表示するには、メタ キーの横にあるドロップダウン メニューをクリックします。
[値のエクスポート]ダイアログが表示されます。
バージョン11.1のダイアログには、1行につき値を1つ含んだ値リストが表示されます。



バージョン11.3のダイアログでは、値を区切る方法(改行またはCSV)を選択できます。



5. コピーする値を選択し、[**値のエクスポート**]をクリックします。
   値がローカルのクリップボードにコピーされ、ファイルにペーストして保存したり共有したりできるようになります。
6. ダイアログを閉じるには、[**閉じる**]をクリックします。
7. (オプション) 現在のドリルダウン ポイントのメタ キーの結果を折りたたみ表示するには、メタ キーの横のドロップダウン メニューをクリックし、[**結果の折りたたみ表示**]をクリックします。

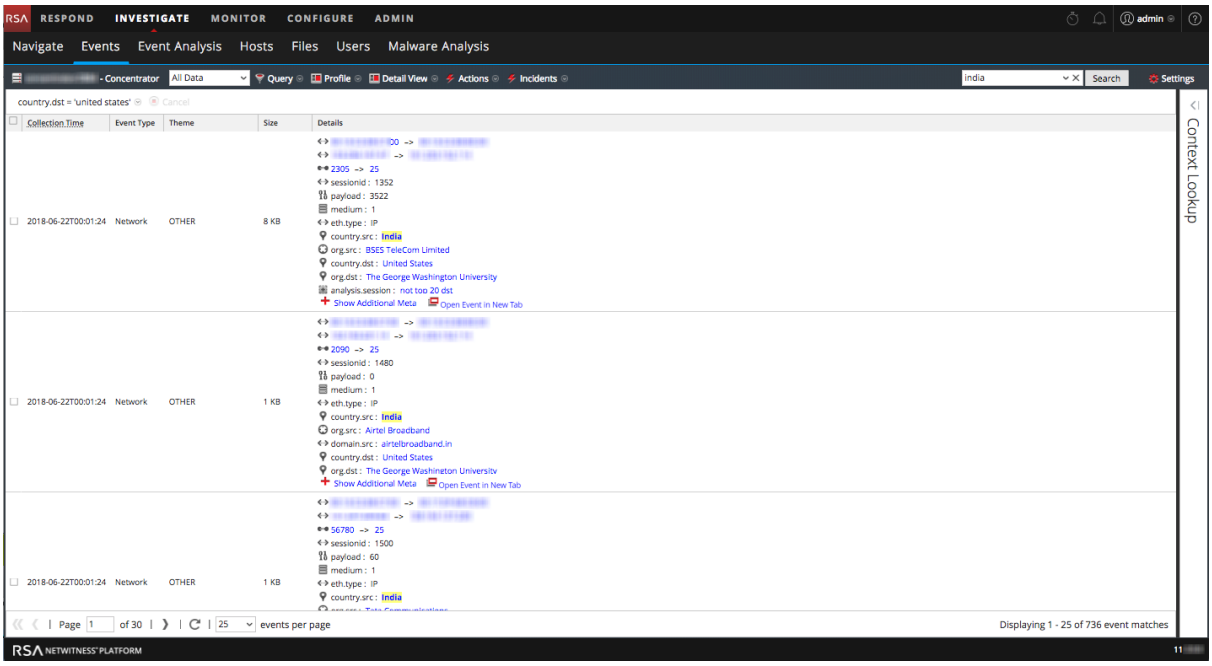
メタ値に関連づけられたイベントを表示するには、次の手順を実行します。

[イベント]ビューには、イベントに関する詳細な内容が2種類のビューで表示されます(イベント リストと詳細ビュー)。

1. [ナビゲート]ビューで、調査の対象となるメタ データまでドリルダウンします。
2. 青色のメタ値の横に表示されるカウント(緑色の数字)をクリックします。
   現在のドリルダウン ポイントに対応する[イベント]ビューが表示されます。
   [イベント]ビューで実行できる操作については、「結果のダウンロードと処理」で説明しています。

メタ値に関連づけられた特定のイベントを検索するには、次の手順を実行します。

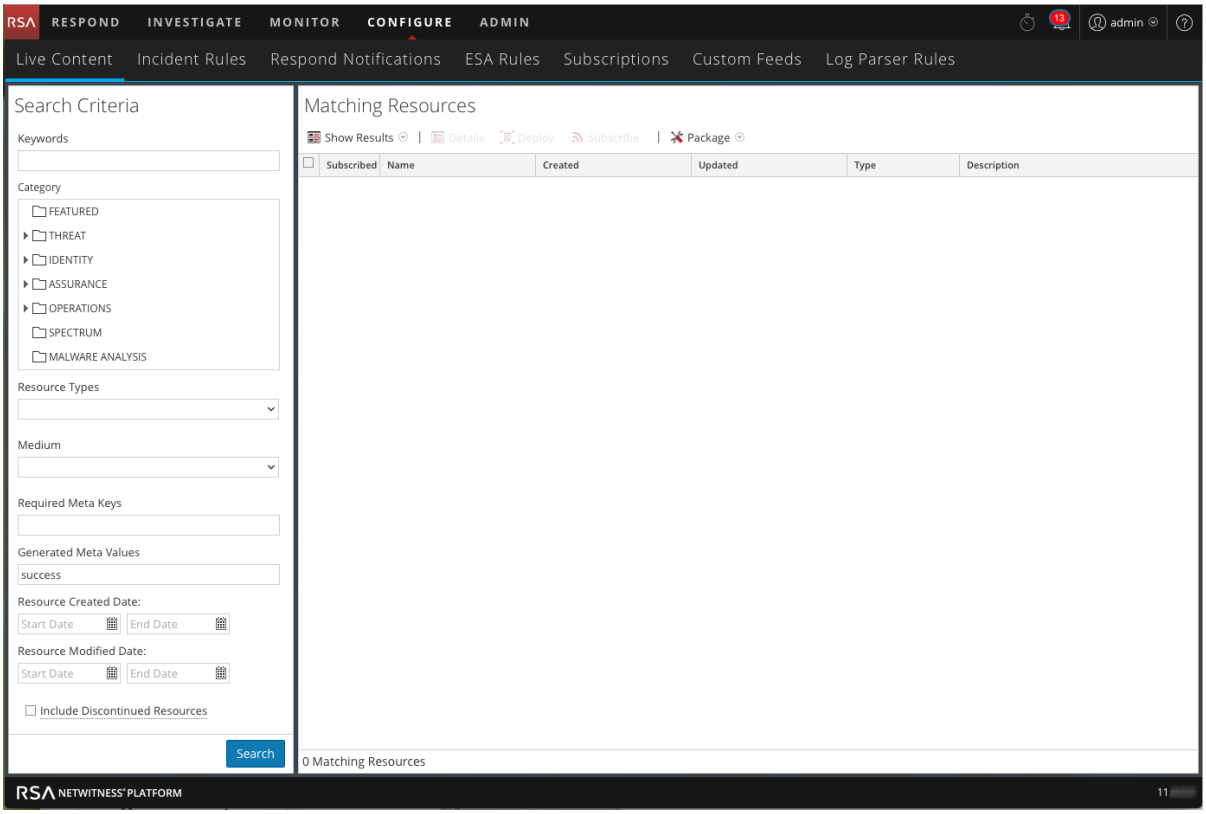
1. [**ナビゲート**]ビューで、調査の対象となるメタ データまでドリルダウンします(メタ値をクリックするか、クエリを追加します)。
2. [イベントの検索]ボックスに検索文字列を入力し、**Enter**を押すか、[**検索**]をクリックします。
   検索モード環境設定を選択して設定することもできます。検索情報の詳細については、「[ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索」を参照してください。
   [イベント]ビューの新しいタブが開き、検索結果が表示されます。ハイライト表示された検索語が見つからない場合は、[**追加のメタの表示**]をクリックします。時間範囲の選択とドリル(クエリ)が[イベント]ビューに継承されます。



選択したメタ値をRSA Liveで表示するには、次の手順を実行します。

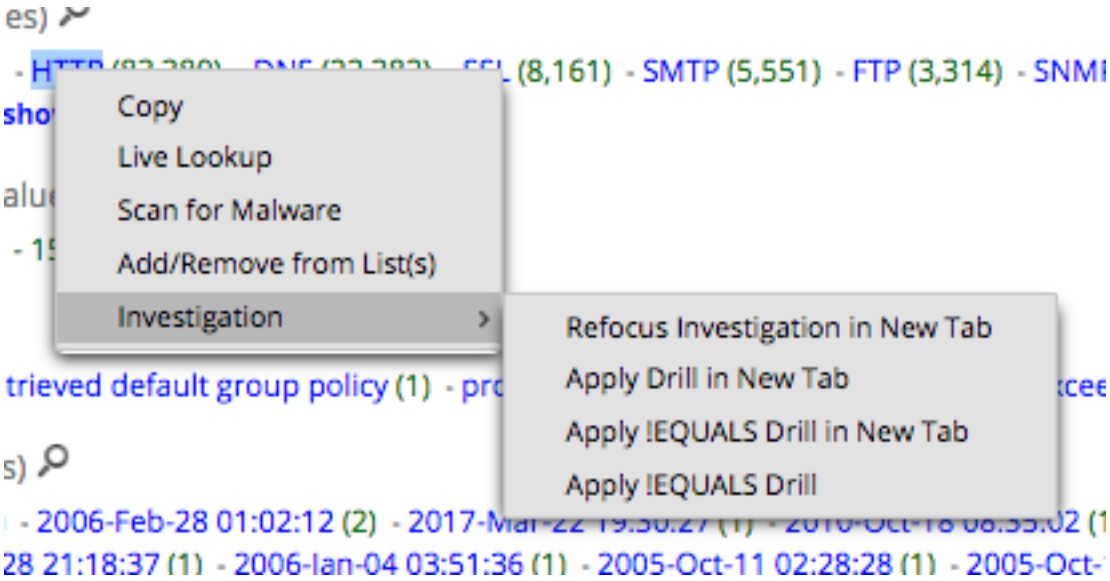
1. [ナビゲート]ビューで、調査の対象となるメタ データまでドリルダウンします。
2. メタ値(青色で表示されたテキスト)を右クリックします。
   [メタ値]ドロップダウン メニューが表示されます。
3. RSA Liveでメタ値を検索するには、[**Liveルックアップ**]を選択します。
   Liveの[検索]ビューが開いて、入力したメタ値が[生成されるメタ値]フィールドに表示され、検索

できる状 態になります。



ドリルダウン ポイントで調 査を再フォーカスするには、次 の手 順を実 行します。

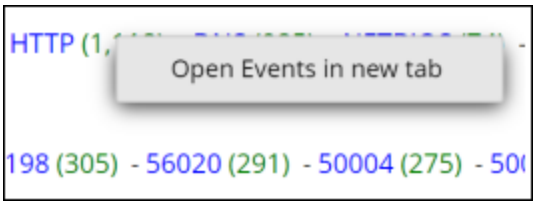
1. メタ値 (青 色 で表 示されたテキスト) を右 クリックします。
   [メタ値]ドロップダウン メニューが表 示されます。



2. いずれかの再 フォーカス オプションを選 択します。
   選 択 内 容 に応じてドリル ダウンの対 象 が再 設 定されます。

新しいタブで特定のカウントを表示するには、次の手順を実行します。

「レガシー イベント」ビューまたは[イベント]ビューでメタ値のカウントを表示するには、メタ値のカウント(青色のメタ値の後の緑色の数字)を右クリックします。
コンテキスト メニューが表示されます。



[レガシー イベント]ビューでの結 果 のフィルタリング

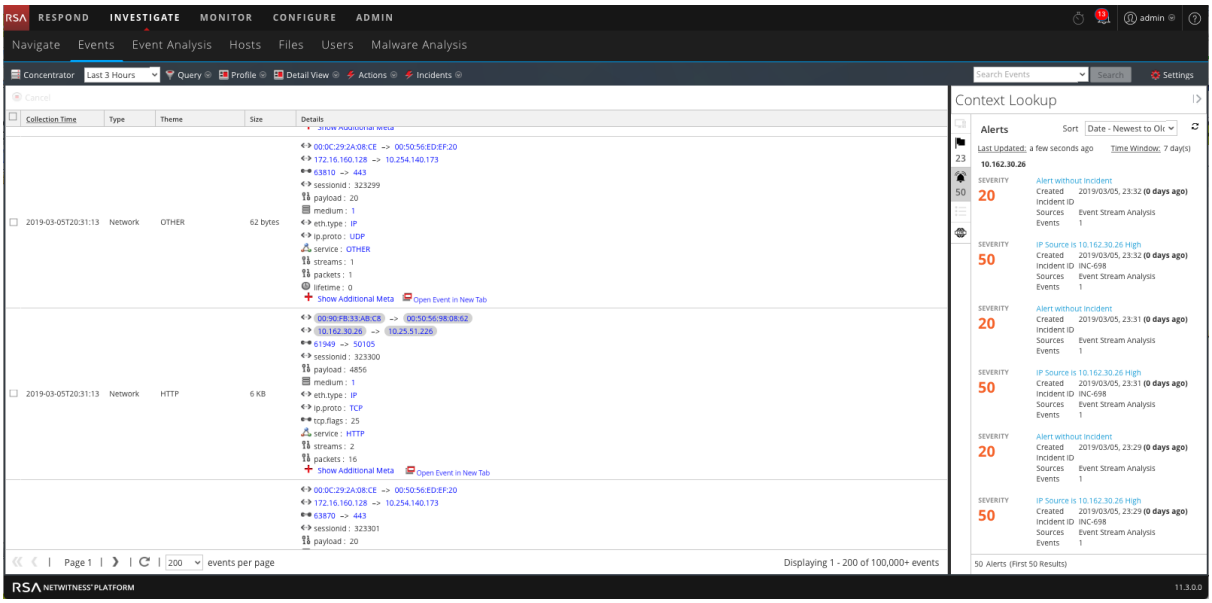
アナリストは、[レガシー イベント]ビューでイベントの検 索 、サービスの選 択 、時 間 範 囲 の設 定 、メタ データのクエリを行って、イベントをフィルタリングできます。[ナビゲート]ビューのドリルダウン ポイントから [レガシー イベント]ビューを開くと、デフォルトでイベントの詳 細ビューが表 示されます。[ナビゲート] ビューを使 用する権 限 がないアナリストは、[レガシー イベント]ビューからサービスに直 接 クエリを実 行 できます

注 : [レガシー イベント]ビューでサービスとしてArchiverを選 択して検 索を実 行した場 合 は、Brokerまたは Concentratorを対 象に検 索を実 行した場 合 よりも検 索 速 度 が遅くなります。通 常 、Archiver上のデータは圧 縮され、より多くのデータが存 在 するためです。

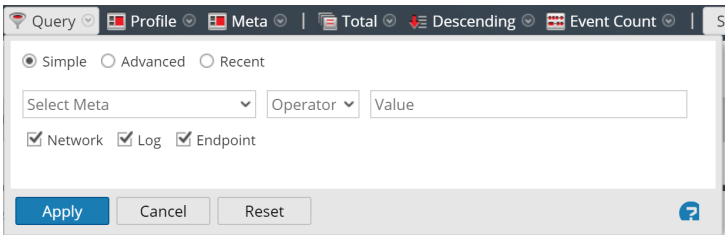
[レガシー イベント]ビューに表 示されるイベントのフィルタリング

[レガシー イベント]ビューに表 示されるデータをフィルタリングするには、次 の手 順を実 行します。

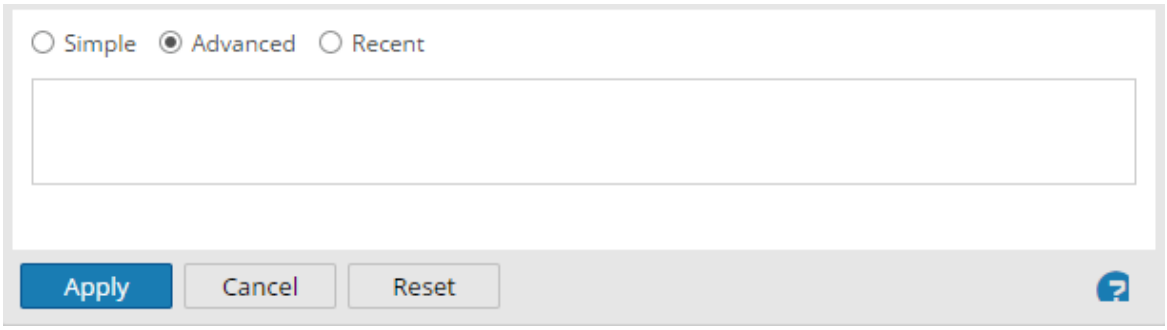
1. [**調 査**]>[**レガシー イベント**]に移 動します。
   [レガシー イベント]ビューが表 示されます。



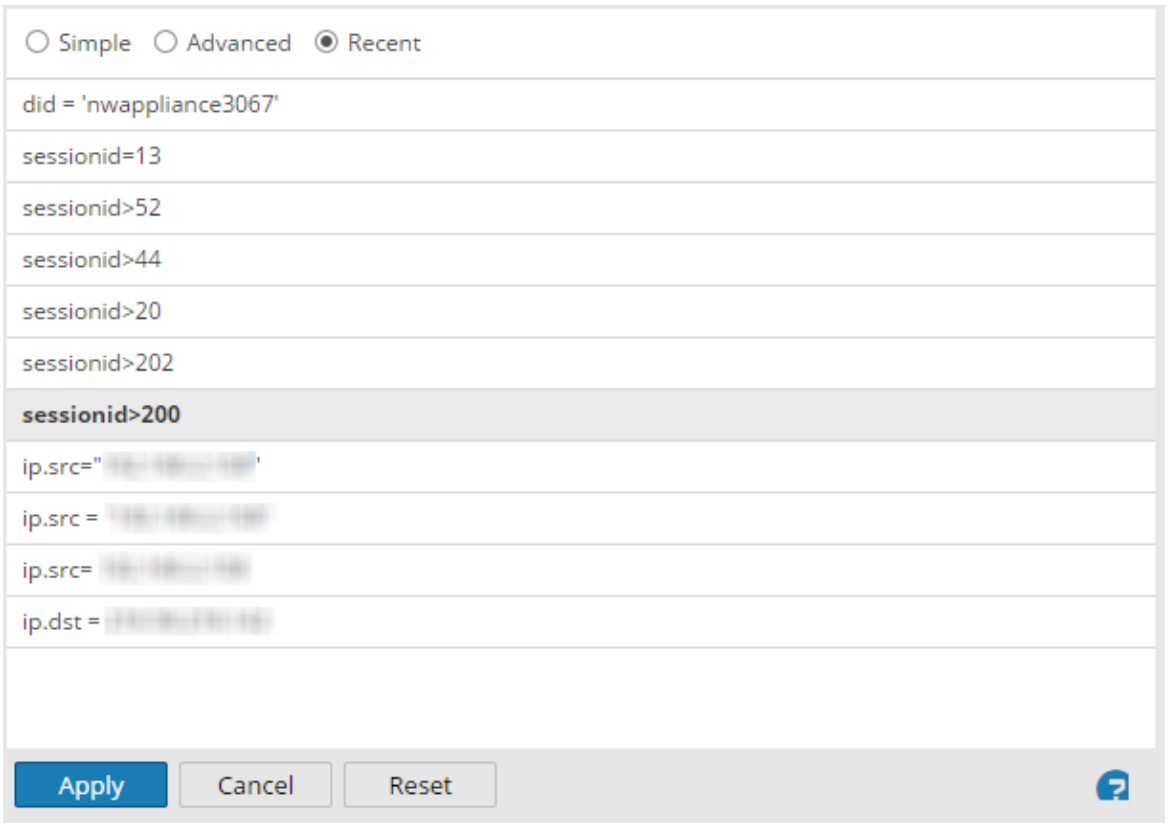
2. デフォルト(**直 近3時 間**) 以 外 の時 間 範 囲 を選 択 するには、ツールバーで[時 間 範 囲]フィールドをクリックし、値 を選 択します。たとえば、[**直 近1時 間**]を選 択します。
   選 択した時 間 範 囲 で[レガシー イベント]ビューが更 新されます。
3. 選 択したサービスと時 間 範 囲 を対 象としたクエリを入 力 するには、ツールバーで、[**クエリ**]をクリックします。
   [シンプルなクエリ]ダイアログが表 示されます。



4. オートコンプリート機能を使用してメタと演算子を選択し、シンプルなクエリを入力する場合は、次のいずれかを実行します。
   a. [**メタの選択**]フィールドをクリックし、ドロップダウン リストからメタ キーを選択します。
   b. [**演算子**]フィールドで、ドロップダウン リストから演算子を選択します。
   c. [**値**]**フィールドに、値を入力します**。
   d. [**ネットワーク**]データ、[**ログ**]データ、[**エンドポイント**]データのいずれかを選択して、[**適用**]をクリックします。
   条件に一致するデータが[レガシー イベント]ビューに表示されます。
5. メタ キーと演算子の知識があり、より複雑なクエリを入力する場合は、次の手順を実行します。
   a. [**詳細**]をクリックします。
   [詳細なクエリ]ダイアログが表示されます。



   b. クエリを入力します。クエリでメタ キーの先頭文字を入力すると、使用可能なメタ キーと演算子のドロップダウン リストが表示されます。終了したら、[**適用**]をクリックします。
6. 最近実行したクエリのリストからクエリを選択する場合:
   a. [**最近実行したクエリ**]を選択します。
   [最近実行したクエリ]ダイアログが表示されます。



b. クエリを選択して[**適用**]をクリックします。
[レガシー イベント]ビューの詳細ビューに、一致するクエリ結果が表示されます。該当するクエリが階層リンクに反映されます。

c. 階層リンクにある任意のクエリをクリックすると、クエリ メニューを表示できます。クエリの前に新しいクエリを挿入することや、階層リンクの末尾に新しいクエリを追加することができます。階層リンクを編集するたびに、結果がリフレッシュされます。

[レガシー イベント]ビューでのイベントのページ移動

ページ移動コントロールを使用すると、リスト ビュー、ログ ビュー、詳細ビューでイベント リストのページ移動を柔軟に実行できます。また、1ページあたりに表示するイベント数を選択できます。選択内容は、NetWitnessからログオフしても維持されます。アイコンを使用できないときは、グレー表示されます。たとえば、1ページ目を表示しているときは、《と«のアイコンは、グレー表示されます。

ページ移動アイコンを使用するには、次の手順を実行します。

1. [レガシー イベント]ビューに結果が表示された状態で、現在のページあたりのイベント数(**10**、**25**、**50**、**100**、**200**)をクリックして、ドロップダウン メニューから、新しいページあたりのイベント数を選択します。
2. ページを前後に移動するには、次のページ コントロール アイコンを使用します。
次のページに移動するには›をクリックします。
最後のページに移動するには»をクリックします。
前のページに移動するには‹をクリックします。

最初のページに移動するには«をクリックします。

3. 特定のページに移動するには、ページ番号フィールド | 3 | Page 3 |にページ番号を入力します。

[ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作 成

[ナビゲート]ビューまたは[レガシー イベント]ビューでは、適 用 可 能なメタ キーまたはメタ エンティティと演 算 子 のドロップダウン リストと構 文 ヘルプが備 わったダイアログを使 用してクエリを作 成 できます。

このドロップダウン リストを表 示したときに、各メタ グループを展 開したり折りたたんだりしてグループ内 の個 々 のメタ キーを表 示または非 表 示にできます。メタ グループを選 択 すると、そのグループ内 のすべてのメタ キーをORで条 件 指 定 する複 雑なクエリがNetWitness Platformによって生 成されます。メタグ ループにip.srcとip.dstが含 まれている場 合 は、ip.src = <value> OR ip.dst = <value>というクエリが生 成されます。異なるメタ値 のタイプを使 用するメタ キーがメタ グループに含 まれる場 合 、メタキー値 での条 件 指 定 は無 効 化され、クエリではexistsステートメントが使 用されます。たとえば、ip.src、ip.dst、alias.hostを含むメタ グループには、異なる値 のタイプを使 用するメタ キーが含 まれています。ip.srcとip.dstはIPアドレスですが、alias.hostはテキストです。この場 合 、生 成されるクエリはip.src exists OR ip.dst exists OR alias.host existsです。

基 本 的なクエリの形 式 は以 下 のようになります。

```
<metakey> <operator> [<metavalue>]
```

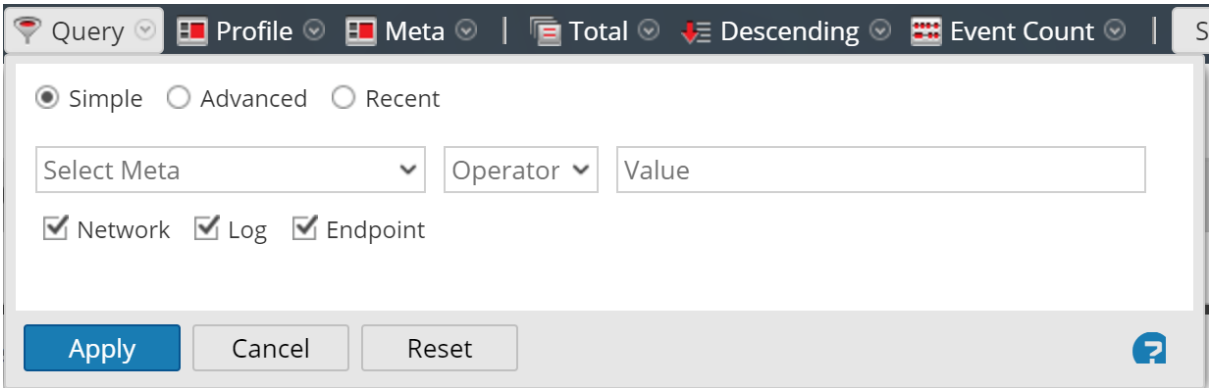
以 下 に、例をいくつか示します。

```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

基 本 的な方 法を使 用したクエリの作 成

基 本 的な方 法でクエリを作 成する場 合 は、メタ キーと演 算 子 のドロップダウン リストが表 示されます。

1. [**ナビゲート**]ビューまたは[**レガシー イベント**]ビューのツールバーで、[**クエリ**]を選 択します。
   [クエリ]ダイアログで[シンプル]オプションが選 択されます。

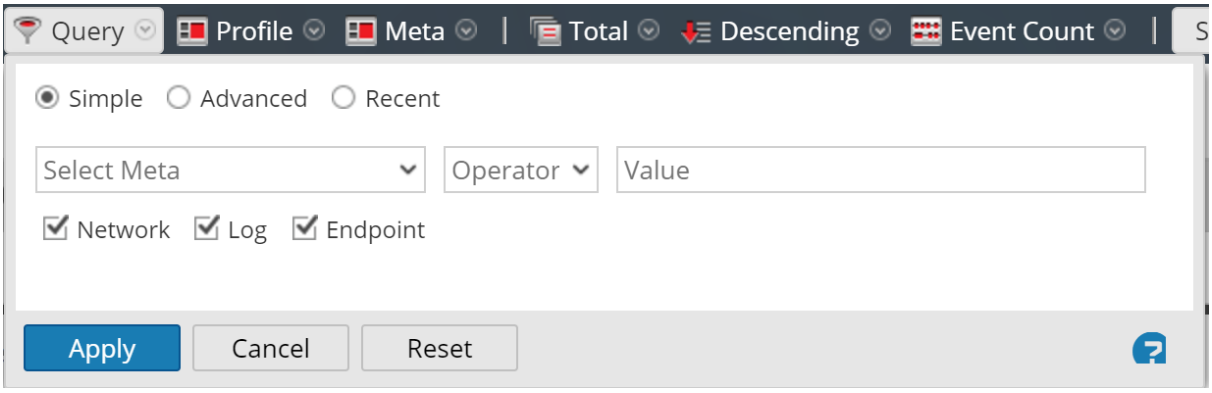


2. [**メタの選 択**]フィールドをクリックして、ドロップダウン リストを表 示します。ドロップダウン リストには、[メタ グループ]と[すべてのメタ]という2つのセクションがあります。
3. [**すべてのメタ**]で単 一 のメタ キーを選 択するか、[**メタ グループ**]でメタ グループを選 択します。メタ キーまたはメタ グループをこのフィールドに直 接 入 力することもできます。

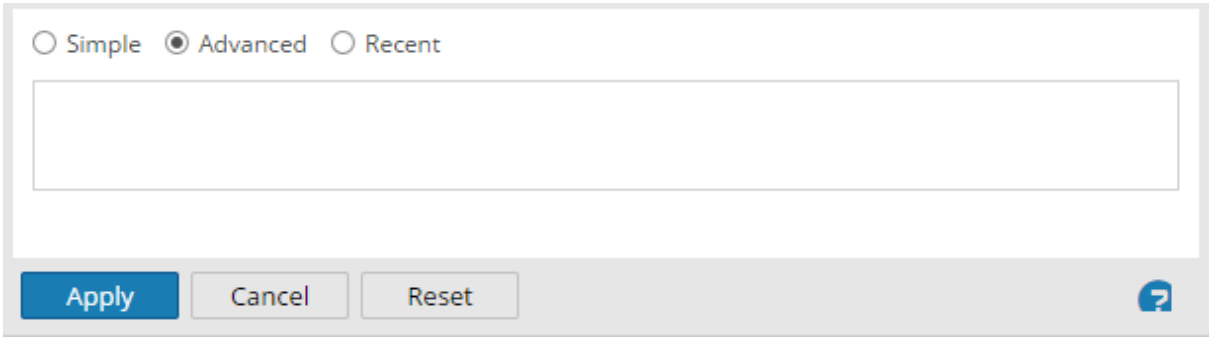
4. [**演算子**]フィールドで、演算子を直接入力するか、ドロップダウン リストをクリックして有効な演算子を選択します。
5. (オプション) 値が必要な演算子(=など)を選択した場合は、3つ目のフィールドにメタ キーの値を入力します。
6. [ネットワーク]、[ログ]、[エンドポイント]の各チェックボックスで、クエリの対象となるデータのタイプを選択します。次のいずれかを実行します。
   a. クエリの対象をパケットに限定する場合は、[**ネットワーク**]をオンにし、[**ログ**]と[**エンドポイント**]をオフにします。
   b. クエリの対象をログに限定する場合は、[**ログ**]をオンにし、[**ネットワーク**]と[**エンドポイント**]をオフにします。
   c. クエリの対象をエンドポイント イベントに限定する場合は、[**エンドポイント**]をオンにし、[**ネットワーク**]と[**ログ**]をオフにします。
   d. クエリをパケット、ログ、エンドポイントに適用する場合は、[**ネットワーク**]、[**ログ**]、[**エンドポイント**]をオンにします。
7. 次のいずれかを実行します。
   a. [**適用**]をクリックします。
   ウィンドウが閉じ、新しいクエリの結果がビューに表示されます。階層リンクにクエリが表示されます。
   b. [**キャンセル**]をクリックします。
   ウィンドウが閉じ、ビューや現在のクエリは何も変化しません。

高度な方法を使用したクエリの作成

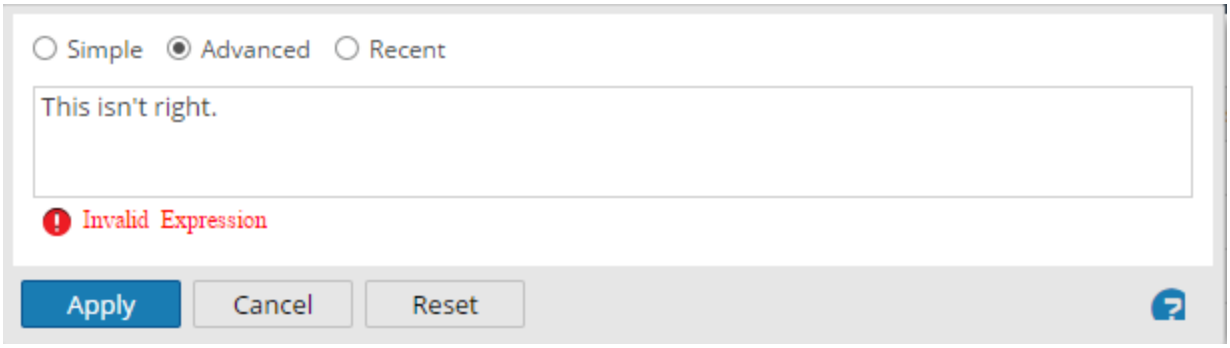
1. [**ナビゲート**]ビューまたは[**レガシー イベント**]ビューのツールバーで、[**クエリ**]を選択します。
[クエリ]ダイアログが表示されます。



2. [**詳細**]を選択します。
詳細なクエリのフィールドが表示されます。



3. このフィールドに、クエリを記述します。クエリには、メタ キー、演算子、値を含めることができます。このフィールドにメタ キーを入力し始めると、選択したサービスに対して使用可能なメタ キーのドロップダウン リストが表示されます。
4. クエリのメタ キーを選択します。
表示が更新されます。式がまだ完了していない場合、ステータスは、クエリが無効であることを示します。
5. 演算子もドロップダウン リストが表示され、必要に応じて値も表示されます。クエリ入力の進行に伴って表示が更新されます。**exists**や**!exists**など、値フィールドを使用しない演算子を入力すると値フィールドが無効化され、無効のステータスがクリアされます。=など、値フィールドを必要とする演算子を入力すると、値を入力するまでは無効のステータスのままになります。クエリが有効になると、無効のステータスは表示されなくなります。

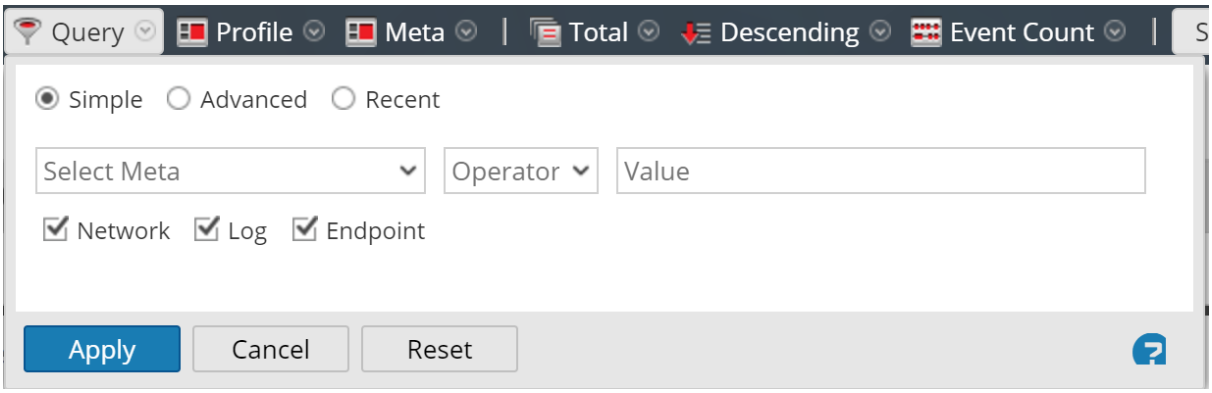


6. 次のいずれかを実行します。
   - [**適用**]をクリックします。
   ウィンドウが閉じ、新しいクエリの結果がビューに表示されます。階層リンクにクエリが表示されます。
   - [**キャンセル**]をクリックします。
   ウィンドウが閉じ、ビューや現在のクエリは何も変化しません。

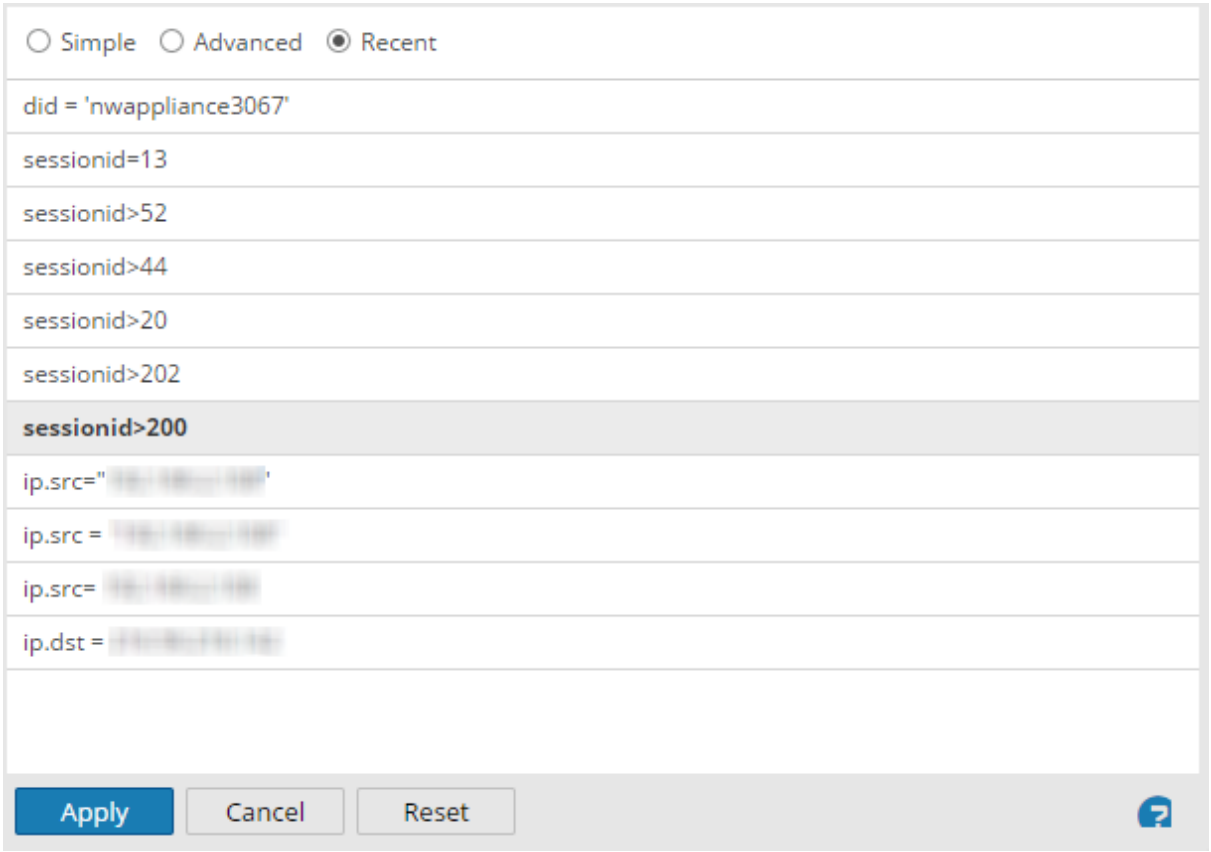
最近実行したクエリの適用

最近実行したクエリを表示し、いずれかを選択して現在調査中のサービスに適用できます。最近実行したクエリを選択するには、次の手順を実行します。

1. [**ナビゲート**]ビューまたは[イベント]ビューのツールバーで、[**クエリ**]を選択します。
[クエリ]ダイアログで[シンプル]オプションが選択されます。



2. [**最近**]オプションを選択します。
ダイアログの最後に、最近実行したクエリのリストが表示されます。



3. 最近実行したクエリのリストから、クエリをクリックして選択します。
4. 次のいずれかを実行します。
   - クエリをダブル クリックします。

- クエリを選 択して[**適 用**]をクリックします。
  ウィンドウが閉じ、新しいクエリの結 果 がビューに表 示されます。階 層 リンクにクエリが表 示されます。
- [**キャンセル**]をクリックします。
  ウィンドウが閉じ、ビューや現 在 のクエリは何も変 化しません。

[ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索

[ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビューで、現在のイベント セット内のテキスト パターンを検索できます。このセクションでは、[ナビゲート]ビューと[レガシー イベント]ビューでの検索について説明します。[イベント]ビューでの検索の詳細については、「[イベント]ビューでの結果のフィルタリング」を参照してください。

キーワード テキスト検索または、regex(正規表現)による検索が可能です。[ナビゲート]ビューでは、HTTPなどのメタ値をクリックしてデータをドリル ダウンし、[検索]フィールドに検索文字列を入力して、データ サブセット内のイベントを検索できます。検索すると[レガシー イベント]ビューにタブが開き、指定した絞り込み条件と時間範囲が表示され、検索結果が表示されます。また、検索を開始する前にクエリを使用してデータをドリル ダウンできます。検索を実行するには、[検索]ボックスに検索文字列を入力して、**Enter**を押すか[**検索**]をクリックします。

注: デフォルトで、検索結果には、インデックスされたデータで見つかった完全一致のみが含まれます。[イベントの詳細]ビューで青色のリンクで表示されるメタ値のみがインデックスされています。値にスペースが含まれる場合は、正規表現オプションを選択する必要があります。検索範囲を広げるには、[イベントの検索]ドロップダウン メニューでオプションを変更します。

キーワード テキスト検索

テキスト検索の機能は次のとおりです。

- スペースで区切られた単語はAND検索となり、すべての単語が検出されて初めて一致と見なされます。ただし、単語間の位置や順序は考慮されません。たとえば、「`Mark Albert`」を検索条件とした場合、セッションにMarkとAlbertの両方が存在している必要があります。ただし、1つのまとまりで出現している必要はなく、順序も問われません。
- 「OR」という単語は特殊な意味を持ちます。「`Mark OR Albert`」を検索した場合、MarkとAlbertのどちらか一方がセッションに見つかれば一致と見なされます。両方が存在する必要はありません。
- 1つの検索文字列で暗黙的なANDとORを組み合わせて検索することもできます。明示的に指定されたORは、暗黙的(スペースによる)ANDよりも優先されます。次の2つの例は、論理的には同じ意味を持ちます。つまり、「cheese」と「dumplings」の両方が存在し、「toast」か「bread」のどちらかが存在している必要があります。

  ```
  cheese toast OR bread dumplings
  cheese AND (toast OR bread) AND dumplings
  ```

- 検索結果から除外したい単語は、-演算子で指定できます。たとえば、「`cheese -toast`」を検索した場合、cheeseという単語を含んだ結果のうち、toastを含んでいない結果がすべて返されます。
- テキスト キーワード検索では、次のパターンの照合に対応しています。
  - **IPv4およびIPv6アドレス**。IPアドレスとして認識できる単語は、インデックスされたメタデータを検索できるように、メタデータ本来の形式に変換されます。
  - **IPv4 CIDR範囲**。CIDR表記を使用して範囲内のIPv4アドレスを検索できます。

- **タイムスタンプ**。タイムスタンプは、ネイティブのtimeメタデータ、およびTimeタイプのその他 のtimeメタ フィールド と照 合 されます。
- **数 字** 。検 索 条 件 に指 定 された10進 数 は自 動 的 に認 識 され、数 値 メタ フィールド と照 合 されま す。

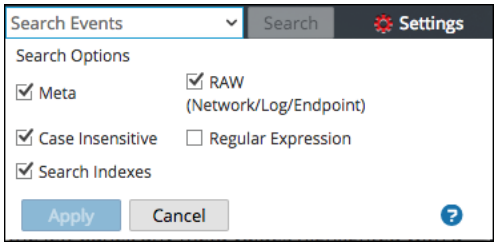
検 索 の動 作 を制 御 するオプション

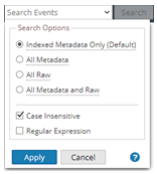
[ナビゲート]ビューまたは[レガシー イベント]ビューで検 索 ボックスと検 索 オプションにアクセスするには、 次 の手 順 を実 行 します。

1. ツールバーに、[イベント の検 索]フィールド が表 示 されます。

> **注** : ツールバーに[イベント の検 索]フィールド が表 示 されない場 合 は、ツールバーの右 端 の ..をク リックします。

2. [**イベント の検 索**]フィールド をクリックすると、[検 索 オプション]ドロップダウン メニューが表 示 されま す。バージョン11.2以 降 では、メニュー オプションは若 干 異 なります。最 初 の図 は、11.1以 前 のメ ニューを示 しています。2番 目 の図 は、バージョン11.2以 降 のメニューを示 しています。





このボックスで選 択 したオプションで、検 索 の実 行 方 法 を変 更 します。デフォルト の検 索 モード では、イン デックスされたメタデータとrawデータのみを検 索 します。

> **注** : [インデックス]または[インデックスされたメタデータのみ(デフォルト)]チェックボックスがデフォルト で選 択 されているため、インデックスされたデータに基 づいて検 索 結 果 が返 されます。メタデータまたは rawデータの完 全 なセット を検 索 する場 合 は、該 当 するチェックボックスをオンにして、[インデックス]ま たは[インデックスされたメタデータのみ(デフォルト)]チェックボックスをオフにします。このタイプの検 索 には時 間 がかかりますが、より完 全 なデータのセット が含 まれます。

次 の表 で、調 査 の検 索 オプションについて説 明 しています。

機能	説明
[**インデックスされたメタデータのみ(デフォルト)**]チェックボックス (バージョン11.2以降) [**インデックス**]ラジオ ボタン(バージョン11.1)	この検索では、インデックスされたデータの結果のみが返されます。インデックス検索は、大量のデータ セットから最も迅速にキーワードを見つける方法です。インデックス検索は、データ コレクションにある関連するすべてのインデックスを利用します。 **注意 :** サブストリングー致は、インデックス検索では検出されません。サブストリングー致を検出したい場合は、このチェック ボックスをオフにして、非インデックス検索モードを使用します。
[**すべてのメタデータ**]ラジオボタン(バージョン 11.2) [**メタ**]チェックボックス (バージョン11.1)	メタデータを検索します。キーワードや正規表現パターンは、解析済みメタデータと照合されます。
[**すべてのRAW**]ラジオ ボタン(バージョン11.2以降) [**RAW**](ネットワーク/ログ/エンドポイント) チェックボックス(バージョン 11.1)	ネットワーク、ログ、エンドポイントのイベント テキストを検索します。すべてのイベントがデコードされ、キーワードや正規表現パターンにー致するコンテンツが検索されます。 フィルタを指定せずにArchiver上のすべてのデータを検索対象にした場合、実行時間が極端に長くなり、警告が表示される場合があります。 **注意 :** ネットワークのRAWデータを検索すると、セッションがデコードされるため、非常に時間がかかります。ネットワーク データのみのコレクションを検索する場合は、RAWオプションを無効にしてもかまいません。
[**すべてのメタデータとRaw**]ラジオ ボタン (バージョン11.2)	メタデータ および ログまたはイベント テキストを検索します。このオプションは、バージョン11.1のメタとRAW(ネットワーク/ログ/エンドポイント) の2つのオプションの組み合わせで、一緒に選択することができます。バージョン11.2では、ラジオ ボタンを1つだけ選択できます。
大文字と小文字を区別しない	大文字と小文字を区別せずに検索します。
正規表現	検索で、テキストではなくPerlの正規表現が使用されます。デフォルトでは、テキスト検索が実行されます。正規表現検索を実行するには、[正規表現]オプションを選択する必要があります。 **注意 :** -正規表現検索は、非常に低速になる可能性があります。 -正規表現とインデックス検索オプションを組み合わせると、メタ値ではなく固有のインデックス値に対して正規表現パターンが照合されます。これにより、結果の生成は速くなりますが、すべてのメタデータまたはRAWデータを完全に検索した結果ではありません。
適用	[ナビゲート]ビューと[レガシー イベント]ビューでの検索に適用するデフォルトの検索オプションを設定します。これにより、プロファイルの調査設定([プロファイル] > [環境設定] > [調査]タブ) も更新されます。設定が保存され、すぐに反映されます。 デフォルトの検索設定を変更せずに、個別の検索に使用する検索オプションを選択できます。

正規表現検索の構文

正規表現検索には、Perlの正規表現の構文(http://perldoc.perl.org/perlre.htmlを参照) が使用されます。

Rawテキスト キーワード検索

Log Decoderには、パースされていないログ イベントのRawテキスト インデックスを作成する機能があります。この機能は、ConcentratorやArchiverなどのダウンストリーム サービス上にフル テキスト インデックスを形成する、メタデータ アイテムを作成します。検索オプションで[検索インデックス]を選択すると、自動的にこのテキスト インデックスを使用して検索が実行されます。テキスト インデックスのメタは、粒度が粗い点に注意してください。たとえば、デフォルトのテキスト インデックスの構成では、テキストの切り捨てが行われます。インデックスでの一致をRawデータと比較することにより、検索エンジンは正確な検索結果を得ることができます。ただし、検索オプションのRawチェックボックスをオフにすると、検索時間が短縮する可能性があります。この場合、結果は迅速に表示されますが、検索結果に誤検出が含まれる可能性があります。

検索手順

[ナビゲート]ビューでの検索

[ナビゲート]ビューに表示されているデータを検索するには、次の手順を実行します。

1. [検索]フィールドに検索文字列を入力し、**Enter**を押すか、[**検索**]をクリックします。
2. 検索ボックスをクリアして、検索によって結果がフィルタリングされていない以前の[ナビゲート]ビューに戻るには、検索ボックスの[**X**]をクリックします。

[レガシー イベント]ビューでの検索

[レガシー イベント]ビューに表示されているデータを検索するには、次の手順を実行します。

1. [イベントの検索]ボックスに検索文字列を入力し、**Enter**を押すか、[**検索**]をクリックします。
   検索結果が表示されます。検索条件に一致するイベントが、[イベント]リストに表示されます。詳細ビューとリスト ビューでは、一致した文字列が[詳細]列でハイライト表示されます。加えて、RAWを検索対象とした場合、一致した文字列が、ログ ビューの[ログ]列でハイライト表示されます。
2. 検索範囲を絞り込む場合は、クエリと時間を変更します。
3. 検索を中止して[レガシー イベント]ビューに戻る場合は、[**キャンセル**]をクリックします。
   表示されている結果はそのままとなります。
4. 検索ボックスをクリアして通常の[イベント]ビューに戻るには、検索ボックスの[**X**]をクリックします。

URL統合を使用したクエリの表示と変更

NetWitness Investigateは、外部URL統合機能を提供します。この機能により、NetWitness Platformアーキテクチャに対する検索が可能となり、サードパーティ製品との統合が容易になります。URIにクエリを記述することにより、カスタム リンクを作成可能なサード パーティ製品から、[調査]ビューの特定のドリルダウン ポイントに直接アクセスできます。この統合によって、ユーザのクエリをサード パーティ製品の内部で表示できます。

URL統合では、ユーザは、NetWitness Platformでの定義に従って、ホストIDまたはサービスとポートでサービスを識別できるようになります。NetWitness Platformがサービスを解決できない場合、アナリストは[ナビゲート]ビューにリダイレクトされ、[サービス選択]ダイアログが表示されます。サービスを選択すると、クエリに定義されているドリルダウン ポイントが[ナビゲート]ビューにロードされます。

サービスIDが分かる場合

調査に使用するサービスのIDが分かっている場合、URIには次のフォーマットでURLエンコードされたクエリを指定します。

```
http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

引数の意味

- `<sa host: port>`は、SAサーバのIPアドレスまたはDNS名で、必要に応じて、ポート(SSLまたは非SSL)を指定します。ポート番号は、プロキシ使用時など非標準ポートでアクセスを構成する場合にのみ必要です。
- `<deviceId>`はNetWitness Platformインスタンスの内部サービスIDで、クエリの対象を指定します。サービスIDは、常に整数です。サービスIDは、NetWitness Platformから[調査]ビューにアクセスする際にURLで確認できます。この値は、調査対象のサービスによって異なります。
- `<encoded query>`は、URLエンコードされたNetWitness Platformクエリです。クエリの長さはHTMLのURL制限で制限されています。
- `<start date>`および`<end date>`は、クエリの日付範囲を定義します。形式は`<yyyy-mm-dd>T<hh:mm:ss>Z`です。start date(開始日)とend date(終了日)は指定が必要なパラメータです。日付を指定しない場合、サービスのユーザ デフォルトが使用されます。相対日付範囲(たとえば、「直近1時間」など)はサポートされていません。すべての時間はUTCとして処理されます。
  例:
  `http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

ホストとポート番号がわかる場合

調査に使用するサービスのホストとポートが分かっている場合、URIには次のフォーマットでURLエンコードされたクエリを指定します。

```
http://<sa host:port>/investigation/<device host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

引数の意味

- <sa host: port>は、SAサーバのIPアドレスまたはDNS名で、必要に応じて、ポート(SSLの場合等)を指定します。ポート番号は、プロキシ使用時など非標準ポートでアクセスを構成する場合にのみ必要です。
- <device host:port>は、NetWitness Platformインスタンスで定義されているクエリ対象サービスのホストとポートです。NetWitness Platformは、NetWitness Platformで定義されたサービスIDとしてホストとポートの解決を試みます。
- <encoded query>は、URLエンコードされたNetWitness Platformクエリです。クエリの長さはHTMLのURL制限で制限されています。
- <start date>と<end date>は、クエリの日付範囲を定義します。形式は<yyyy-mm-dd>T<hh:mm:ss>Zです。start date(開始日)とend date(終了日)は指定が必要なパラメータです。日付を指定しない場合、サービスのユーザ デフォルトが使用されます。相対日付範囲(たとえば、「直近1時間」など)はサポートされていません。すべての時間はUTCとして処理されます。
  例:
  http://localhost:9191/investigation/concentrator:50105/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z

例

次のクエリの例では、NetWitness Serverが192.168.1.10で、デバイスIDが2に指定されています。

2013年3月12日の午前5:00から午前6:00までのすべてのアクティビティで、alias host(ホスト名)が存在するデータ

- カスタム ピボット:alias.host exists
- https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z

2013年3月12日の午後5:00から午後5:10までのすべてのアクティビティで、IPアドレス10.10.10.3において送受信されるhttpトラフィック

- カスタム ピボット:service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)
- ピボットのエンコード:
  - service=80 => service&3D80
  - ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%
    2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z

追加の注意事項

一部の値はエンコードする必要がない場合があります。たとえば、クエリにip.srcとip.dstを指定する場合、これらのパラメータはエンコードせずに参照することが可能です。

イベントの再構築と分析

[ナビゲート]ビューまたは[イベント]リストでイベントを絞り込んだら(「結果セットの絞り込み」を参照)、次のステップは、イベントの再構築、添付ファイルの確認、サード パーティ ルックアップまたは内部ルックアップでの追加コンテキストの表示を行って、イベントについて詳しく理解することです。

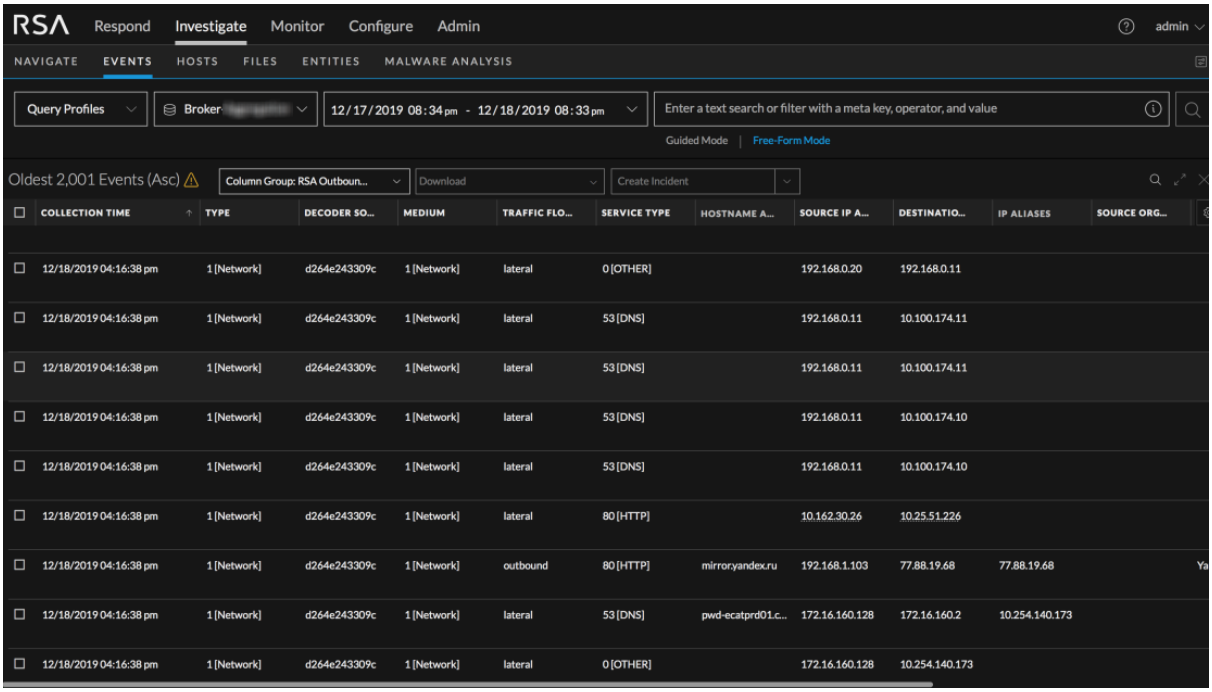
再構築は[イベント]ビューまたは[レガシー イベント]ビューで行います。[ナビゲート]ビューから開始する場合は、[イベント]ビューまたは[レガシー イベント]ビューに移動して再構築を表示する必要があります。

注: [レガシー イベント]ビューはデフォルトで無効になっています。管理者は、『*システム構成ガイド*』の「調査の設定の構成」の説明に従って有効にすることができます。

[イベント]ビューでイベントを表示するには、次のいずれかを実行します。

1. [イベント]ビューを開くには、[**調査**]>[**イベント**]に移動します。
2. [**調査**]>[**ナビゲート**]に移動して、メタ値のメタ数を右クリックします(メタ数は緑のテキストで表示されます)。コンテキスト メニューが表示されたら、[**イベントを新しいタブで開く**]を選択します。

選択したメタ値のイベントが[イベント]ビューに表示されます。

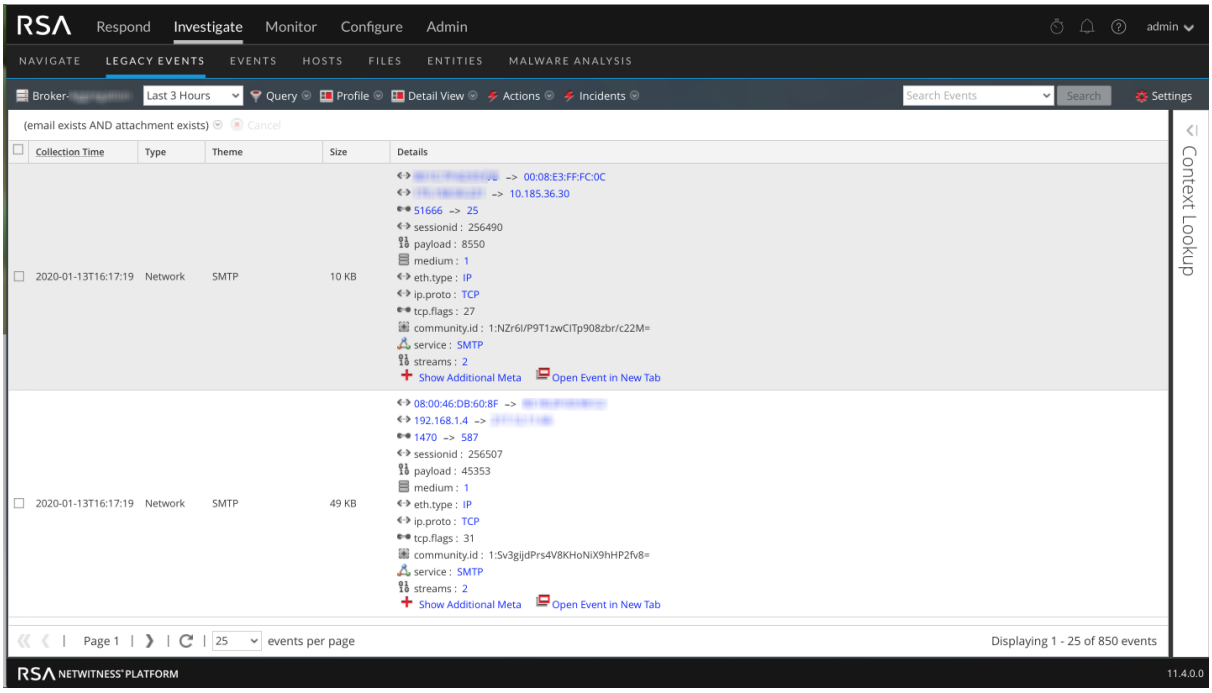


このビューで使用できる分析のタイプの詳細については、「[イベント]ビューでのイベントの再構築」を参照してください。

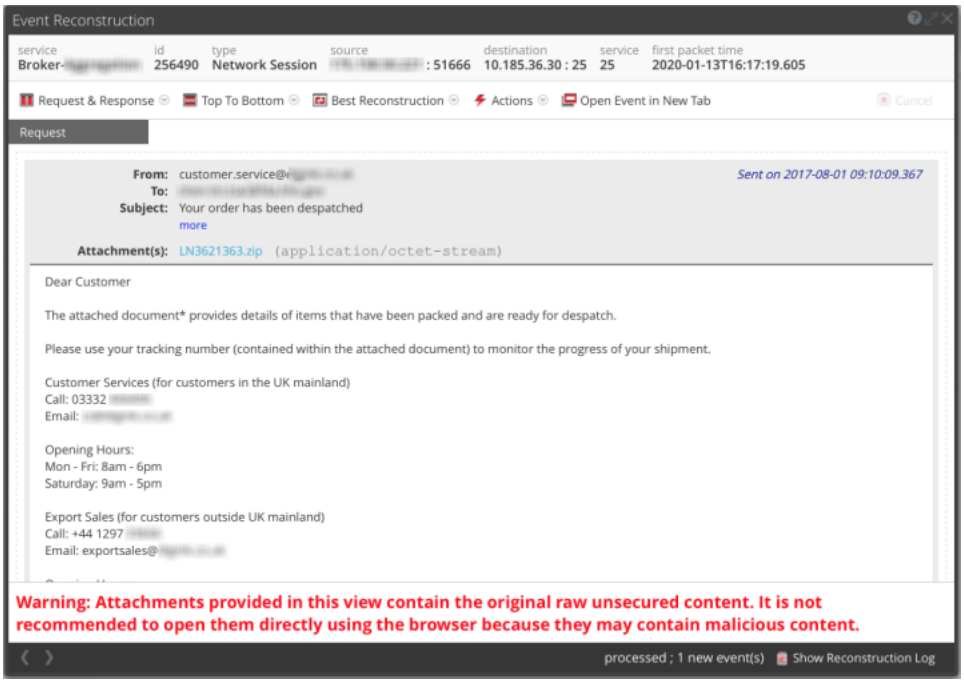
[レガシー イベント]ビューでイベントを表示するには、次のいずれかを実行します。

1. デフォルト サービスのデフォルト クエリを使用して[レガシー イベント]ビューを開くには、[**調査**]>[**レガシー イベント**]に移動します。

2. 特定のメタ値のイベントを[レガシー イベント]ビューに表示するには、**[調査]＞[ナビゲート]**に移動して、値パネルにイベントがロードされたら、メタ数をクリックします(メタ数は緑のテキストで表示されます)。メタ値のメタ数を右クリックすることもできます。コンテキスト メニューが表示されたら、**[レガシー イベントを新しいタブで開く]**をクリックします。
選択したメタ値のイベントが[レガシー イベント]ビューに表示されます。[レガシー イベント]ビューには、詳細ビュー、リスト ビュー、ログ ビューという、標準提供の3種類の表示形式でイベント データを表示できます。この図は詳細ビューの例です。[レガシー イベント]ビューに表示されるイベントをフィルタリングするには、クエリ、時間範囲設定、プロファイルを使用します。ファイルの抽出、イベントのエクスポート、ログのエクスポートを行うことができます。また、イベントをダブル クリックすると、[イベントの再構築]パネルが開きます。これらの機能の詳細については、「結果のダウンロードと処理」を参照してください。
NetWitness Platformは、デフォルトのサービス(設定されている場合)の直近3時間についてデフォルト クエリを実行するか、またはサービスを選択するダイアログを表示してからデフォルト クエリを実行します。デフォルト クエリではすべてのイベントが選択され、選択したサービスのイベントが古い順に[イベント]ビューに表示されます。



リスト内の最初のイベントの再構築を表示するには、そのイベントをダブルクリックします。
[イベント]リストの前のポップアップ ウィンドウに再構築が表示されます。

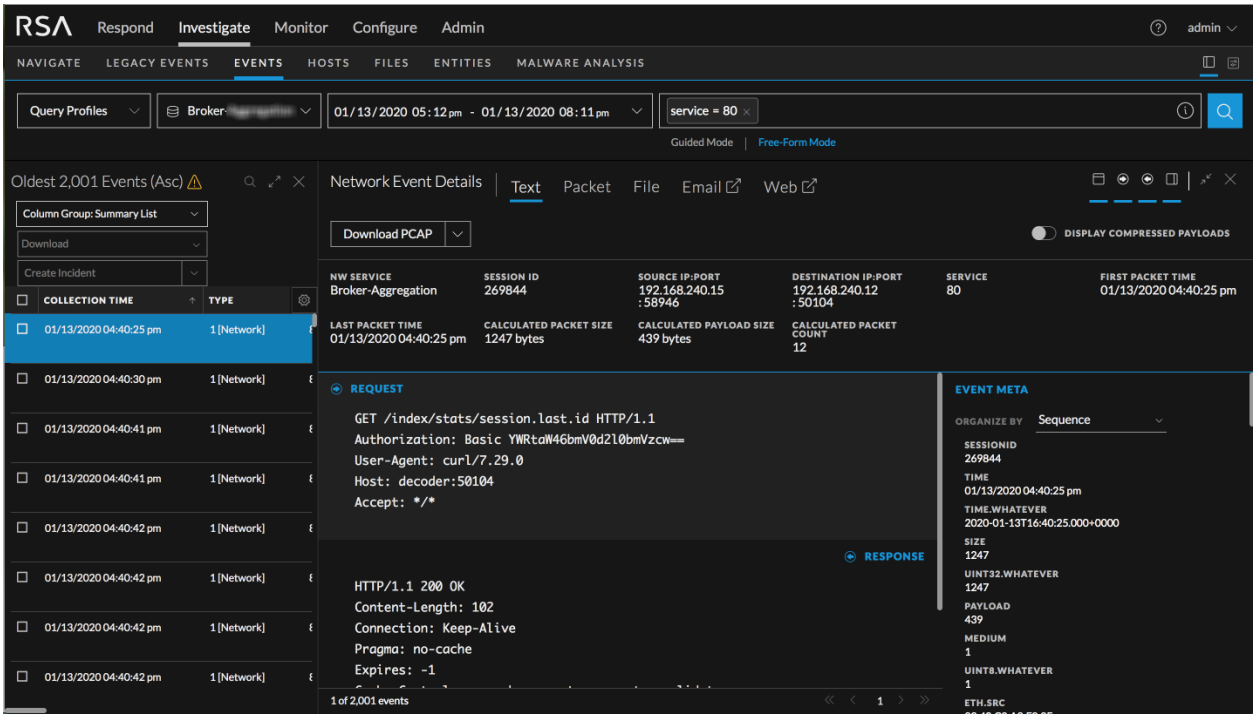

Event Reconstruction
service
Broker-
id
256490
type
Network Session
source
: 51666
destination
10.185.36.30 : 25
service
25
first packet time
2020-01-13T16:17:19.605
Request & Response
Top To Bottom
Best Reconstruction
Actions
Open Event in New Tab
Cancel
Request
From: customer.service@
To:
Subject: Your order has been despatched
more
Sent on 2017-08-01 09:10:09.367
Attachment(s): LN3621363.zip (application/octet-stream)
Dear Customer
The attached document* provides details of items that have been packed and are ready for despatch.
Please use your tracking number (contained within the attached document) to monitor the progress of your shipment.
Customer Services (for customers in the UK mainland)
Call: 03332
Email:
Opening Hours:
Mon - Fri: 8am - 6pm
Saturday: 9am - 5pm
Export Sales (for customers outside UK mainland)
Call: +44 1297
Email: exportsales@
Warning: Attachments provided in this view contain the original raw unsecured content. It is not recommended to open them directly using the browser because they may contain malicious content.
processed ; 1 new event(s)
Show Reconstruction Log

[イベント]ビューでのイベントの再構築

収集したネットワーク データ、ログ データ、エンドポイント データから脅威の可能性をハンティングするために、さまざまなポイントからドリル ダウンしてデータを分析することができます。特定のセッションに疑わしいイベントが含まれる場合は、そのセッションのイベントのリストを調査し、イベントの再構築を安全に表示し、パターンを特定することもできます。

[イベント]ビューでは、再構築の形式(パケット、ファイル、テキスト、メール、Web)を選択できます。ログ イベントまたはエンドポイント イベントでは、テキストの再構築のみ選択できます。ネットワーク イベントのデフォルトの再構築はテキストです。ただし、最後に開いていた再構築形式が、デフォルトを上書きします。メールとWebの再構築は、[レガシー イベント]ビューでイベントを開きます。「[レガシー イベント]ビューでのイベントの再構築」を参照してください。

次の図は、[ネットワーク イベントの詳細]の[テキスト]パネルをWebブラウザ ウィンドウで開いた例です。



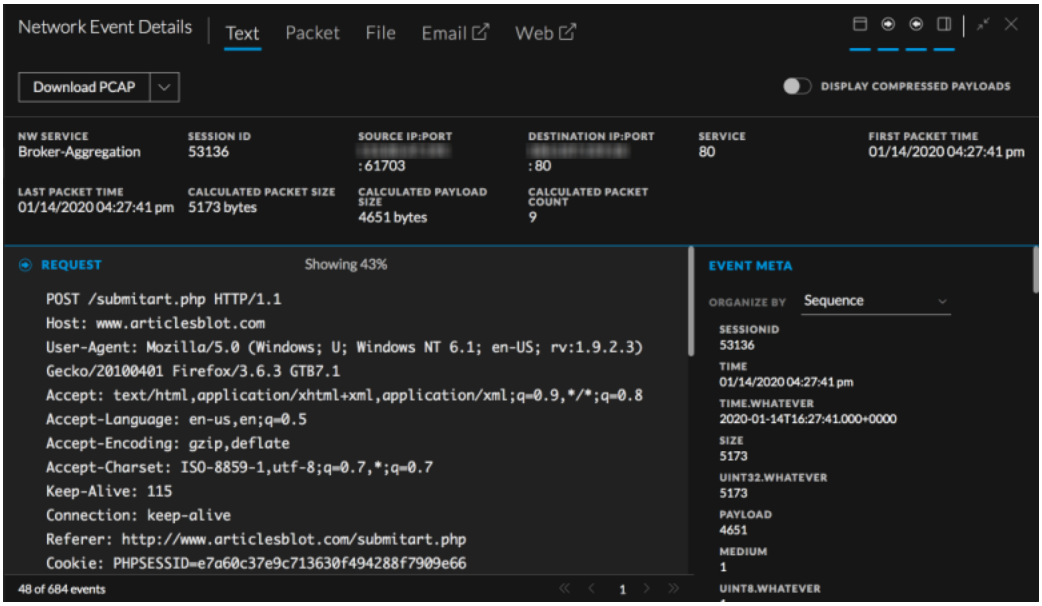
各タイプの分析では、分析機能を拡張するための設定が用意されています。設定の変更は、ブラウザの表示を更新しても、同じブラウザで再ログインしても、保持されます。次の設定が保持されます。

- 現在選択されている再構築:テキスト、パケット、ファイル、メール。
- [イベント メタ]パネルの表示、非表示。
- [イベント]ヘッダーの表示、非表示。
- リクエスト、レスポンス、またはその両方の表示、非表示。
- [パケット]パネルにパケット ペイロードをヘッダーなしで表示するかどうか。
- [パケット]パネルでバイトを濃淡化するかどうか。

- [パケット]パネルにその他の一般的なファイル タイプをハイライト表示するかどうか。
- [パケット]パネルのページあたりのパケット数。
- [テキスト]パネルで圧縮したテキストと展開したテキストのどちらを表示するか。

[テキスト]パネル

[テキスト]パネルでは、すべてのタイプのイベント(ネットワーク イベント、ログ イベント、エンドポイント イベント)を元々のテキスト形式で表示できます。ネットワーク イベントによっては[テキスト]パネルが非常に大きくなることがあります。最適なレンダリングを保証するために、過度に大きなペイロードは、収まるようにトランケートされます。再構築されたイベントで、1つの再構築された要求または応答が最大バイト数を超えた場合、ヘッダーは表示されているバイトの比率を示します。ページネーション コントロールは、イベントの再構築されたテキストをページングするときの柔軟性を高めます。この図は、最大バイト数(バージョン11.2以降)を超えているためにトランケートされた単一の応答を示しています。



バージョン11.1は大きなペイロードを異なる方法で処理します。1つのイベントのペイロードは2500パケットに制限されます。パケットの制限に達すると、フッターに警告が表示され、制限に達したことを通知し、イベント内のパケットの総数を示します。

注: バージョン11.1の場合、[さらに表示]オプションは、トランケートされたメッセージでも使用できます。ただし、RAWペイロードをダウンロードしないと、メッセージのテキスト全体が表示されません。

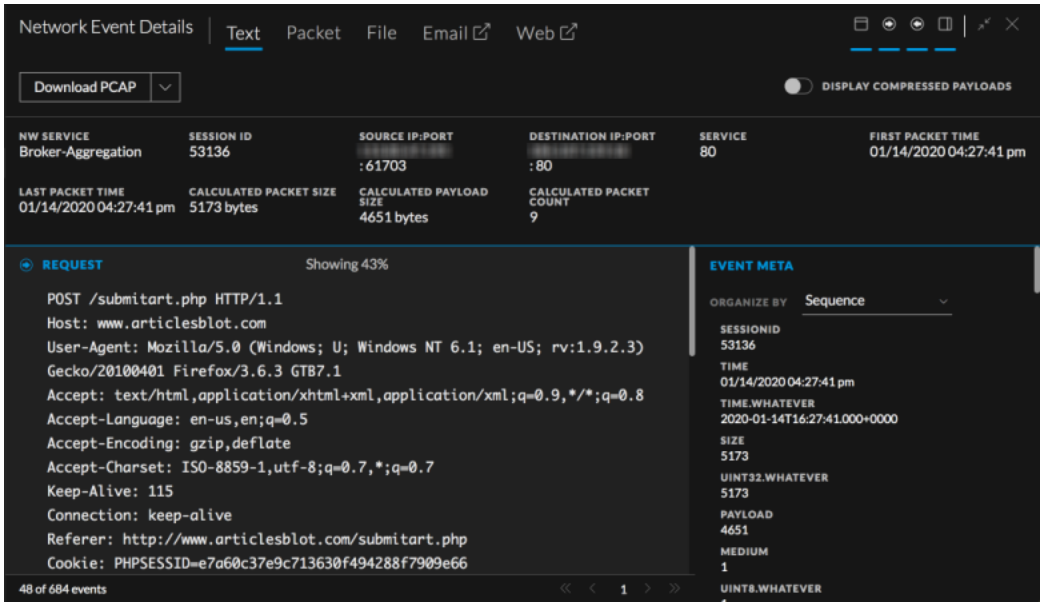
[テキスト]パネルでは、ネットワーク イベント、ログ イベント、エンドポイント イベントの表示は異なります。

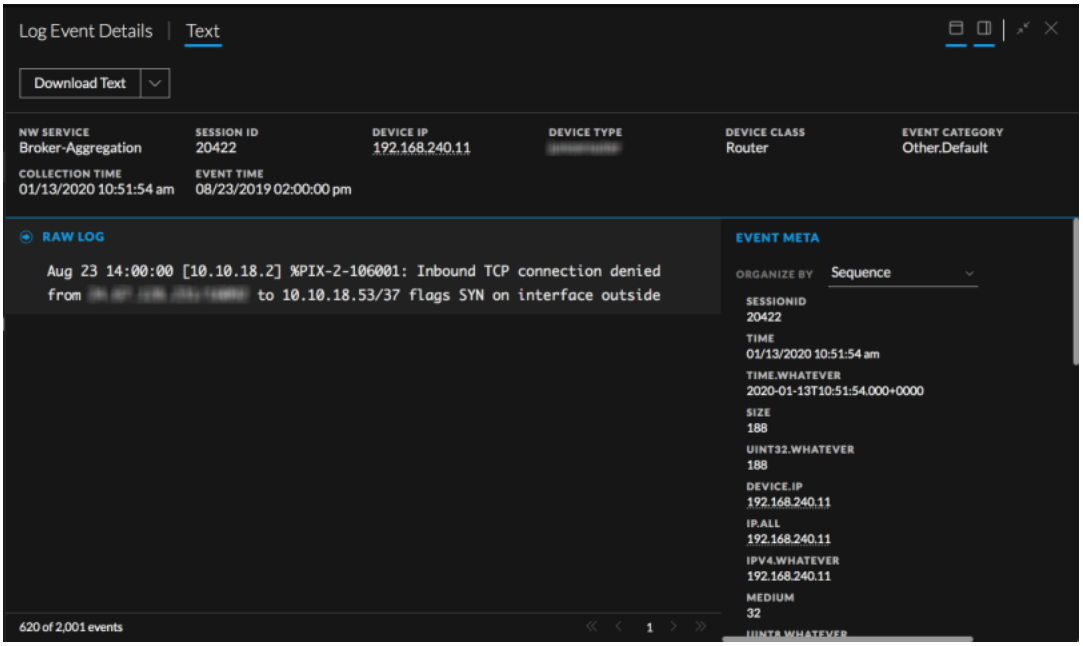
- ネットワーク イベントでは、パケットの方向(リクエストまたはレスポンス)と、各パケットの内容がテキスト形式で表示されます。ネットワーク イベントを再構築している場合は、[テキスト]パネルはスクロールできます。リクエストとレスポンスのラベルと同様にテキストの識別情報もスクロールして表示し続けることができます。
- ログ イベントとエンドポイント イベントにはリクエストまたはレスポンスがありません。RAWイベントのみが[テキスト]パネルに表示されます。

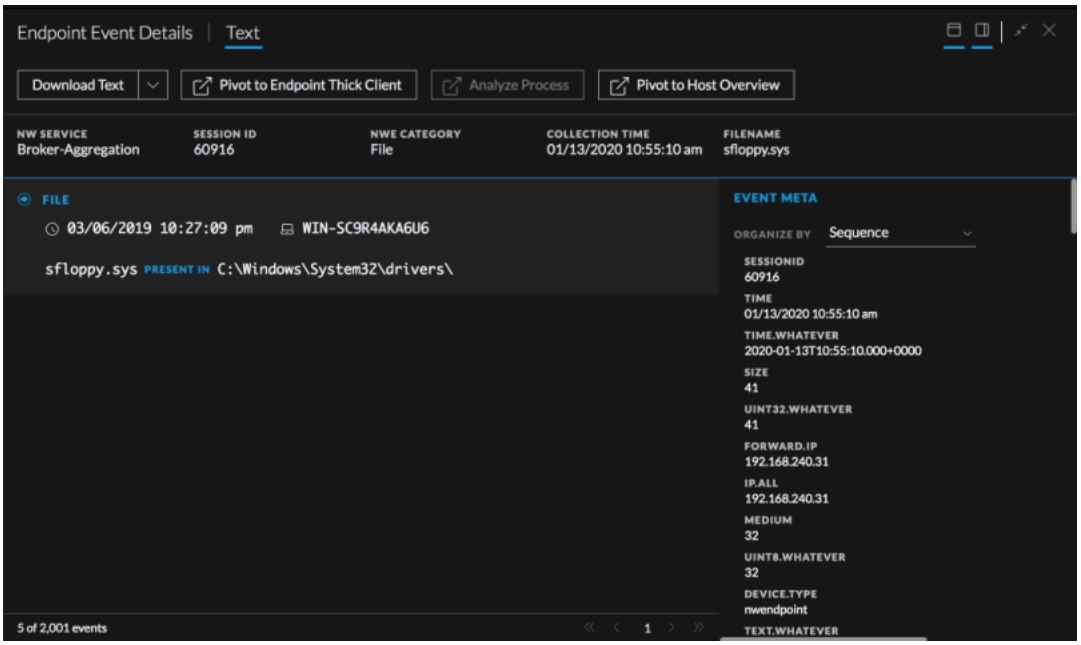
各タイプのイベント(ネット ワーク、ログ、エンド ポイント) には、いくつかの違いがあります。

- イベント のヘッダーには、各タイプのイベントに関連する情報が含まれています。
- エクスポート のオプションに違いがあります。

次に各タイプのイベント(ネット ワーク イベント、ログ イベント、エンド ポイント イベント) の[テキスト] パネルの例を示します。





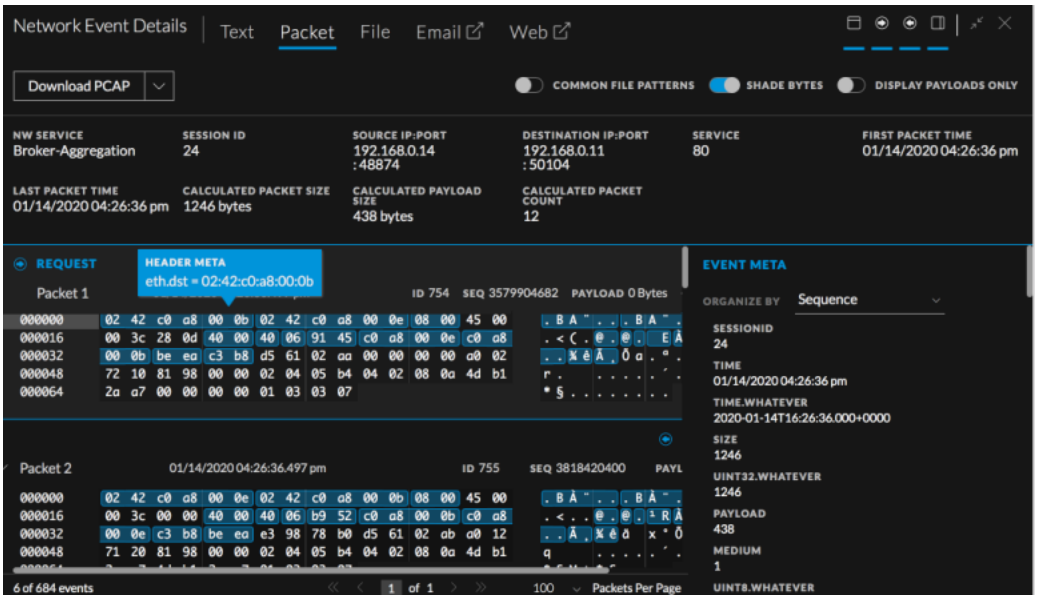


注： イベント ヘッダー内の計算済みパケット数、計算済みパケット サイズ、計算済みペイロード サイズが、[イベント メタ] パネル内の同じ統計と異なっている場合があります。これは、イベントのパースが完了する前にメタデータが書き込まれ、パケットが重複して計算されることがあるためです。

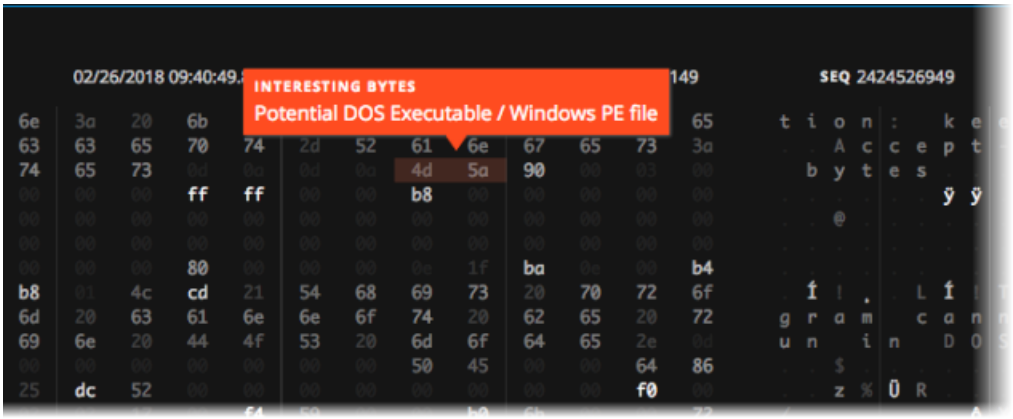
[パケット] パネル

[パケット] パネルは、ネットワーク イベントを対象としています。このパネルはスクロールできます。リクエストとレスポンスのラベルと同様にパケットの識別情報もスクロールして表示し続けることができます。[パケット] パネルの見出しには、パケットの方向 (リクエストまたはレスポンス)、パケット番号、パケットの開始時刻、パケットIDと順序、ペイロード サイズが表示されます。すべてのパケットはヘッダーで始まり、一部のパケットにはフッターがあります。ページ移動コントロールによって、パケットのページ移動が柔軟になります。

16進形式とASCII形式の両方で、メタデータは青色でハイライト表示されます。ハイライト表示されたメタデータ上にカーソルを合わせると、ポップアップにメタ キーとメタ値の情報が表示されます。

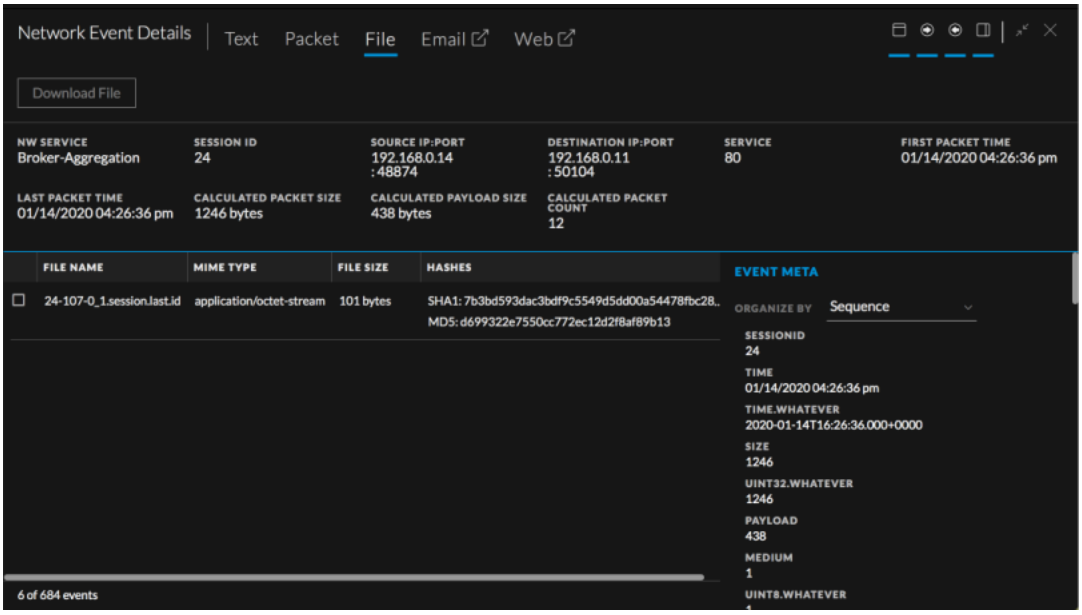


一般的なファイル シグネチャは、オレンジ色の背景色でハイライト表示されます。ハイライト表示されたテキスト上にカーソルを置くと、ポップアップにファイルのタイプの説明が表示されます。

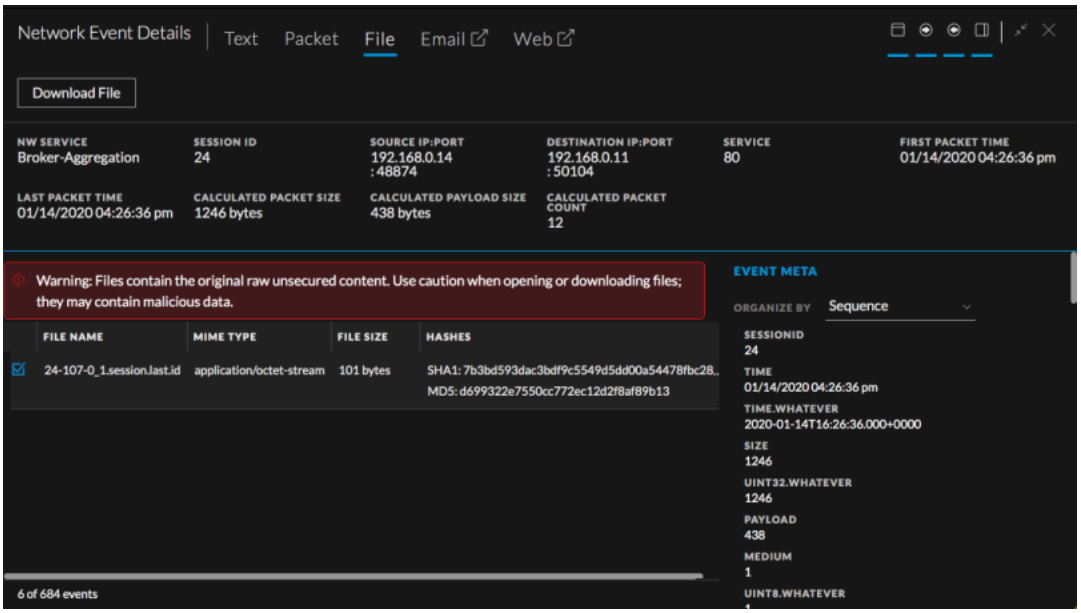


[ファイル] パネル

[ファイル] パネルは、選択したネットワーク イベントに関連づけられたファイルの一覧を表示します。これは、[ファイル] パネルの例です。



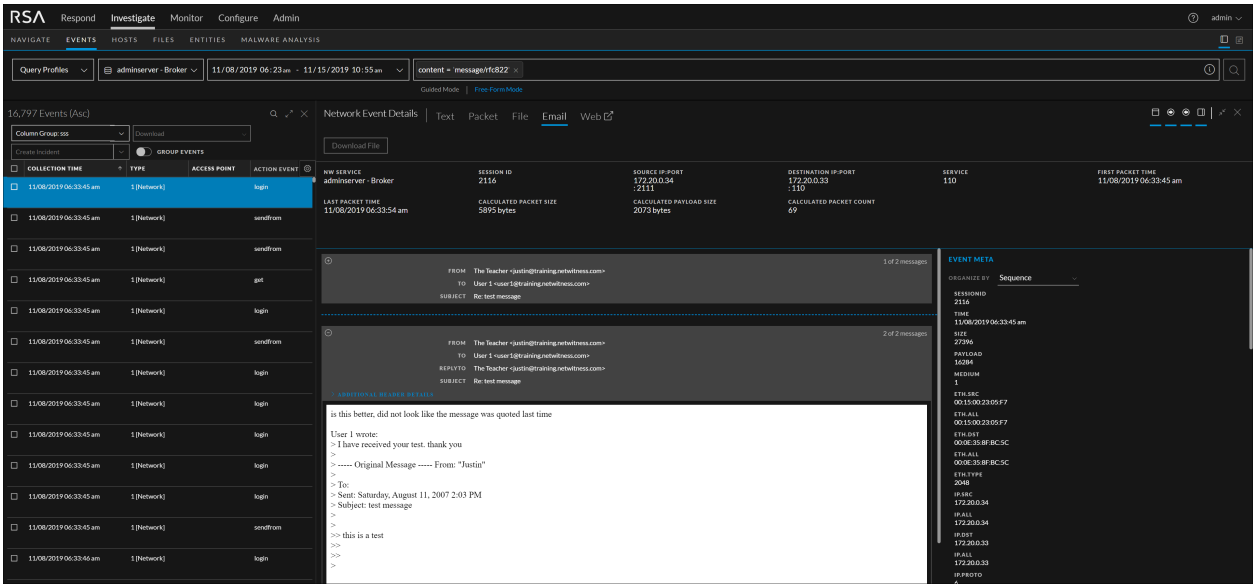
1つまたは複数のファイル、あるいはすべてのファイルを選択してローカル ファイル システムにエクスポートできます。ファイルを選択すると、[ファイルのダウンロード] がアクティブになり、選択したファイルの数が反映されます。



注意： デフォルトのアプリケーションに関連づけられているファイルを解凍または開くときは、十分に注意してください。たとえば、Excelスプレッドシートは、ファイルの安全性を検証する前にExcelで自動的に開かれる可能性があります。

[メール] パネル

[メール] パネルは、選択したネットワーク イベントに関連づけられたメールの一覧を表示します。これは、[メール] パネルの例です。



- デフォルトでは、1つのメールが展開され、複数のメールは折りたたまれます。
- 添付ファイルを含むメールは、次のいずれかの方法でダウンロードできます。
  - 1つまたは複数の添付ファイルをダウンロードするには、添付ファイルを選択し、[**ファイルのダウンロード**] をクリックします。
  - すべての添付ファイルをダウンロードするには、[**すべての添付ファイル**] を選択し、[**ファイルのダウンロード**] をクリックします。

  注意: メールから添付ファイルをダウンロードして開くと、悪意のあるデータがファイルに含まれている可能性があります。
- メール内の外部リンクにはアクセスできません。外部リンクをクリックすると、[**リンク アドレス**] ポップアップ ウィンドウが開き、実際のリンクが表示されます。
- メールの本文が長すぎると、メールの先頭に[**%を表示**] が表示されます。残りのコンテンツを表示するには、メールの最後尾にある[**残り%を表示**] をクリックします。
- `mail.google.com`、`mail.live.com`、または`mail.yahoo.com`を`alias.host`に含むWebメールのイベントの場合、[イベントの再構築] ページで関連するセッションの再構築を表示するリンクを含んだメッセージが表示されます。それ以外の場合は、「*このイベントではメール再構築を使用できません*」というメッセージが表示されます。

各 イベント タイプの分 析ツール

アナリストは[イベント]ビューの分 析ツールを使 用して、さまざまなタイプのイベント(ネット ワーク イベント、ログ イベント、エンド ポイント イベント) に関 連する情 報を検 索できます。この表 は、イベント タイプごとに実 行できるアクションを示します。このセクションの残りの部 分では、これらのアクションを実 行するための手 順を説 明します。

操 作	ネット ワーク イベント	ログ イベント	エンド ポイント イベント
[テキスト]パネルを表 示する	✓	✓	✓
[ファイル]パネルを表 示する	✓		
[パケット]パネルを表 示する	✓		
[メール]パネルを表 示する	✓		
パネルを開く、閉じる、サイズを調 整する	✓	✓	✓
リクエストとレスポンスの表 示を調 整する	✓		
[テキスト]パネルでイベント ヘッダーを表 示または非 表 示にする	✓	✓	✓
[テキスト]パネル内 のトランケートされたテキスト エントリーを展 開する	✓		
[テキスト]パネルでペイロード の圧 縮表 示と解 凍表 示を切り替 える	✓		
[パケット]パネルでバイトをハイライト表 示する	✓		
[パケット]パネルで一 般 的なファイル タイプをハイライト表 示する	✓		
[パケット]パネルにペイロード のみを表 示する	✓		
[パケット]パネルでペイロード のみを表 示するときバイトを濃 淡 化する	✓		
[テキスト]パネルでURLとBase64のエンコード およびデコード を実 行する	✓		
[テキスト]パネルでHTTPネット ワーク セッションの解 凍されたテキストを表 示する	✓		
[テキスト]パネルでイベント のイベント メタデータを表 示する	✓	✓	✓
[パケット]パネルまたは[テキスト]パネルでネット ワーク イベント(PCAPファイル、ペイロード のみ、リクエスト のみ、レスポンスのみ) をダウンロード する	✓		
[ファイル]パネルでネット ワーク イベント からファイルをエクスポート する	✓		
[テキスト]パネルでログ イベント のファイルをダウンロード する		✓	

操作	ネットワークイベント	ログイベント	エンドポイント イベント
[テキスト] パネルでエンド ポイント イベントのファイルをダウンロードする			✓
[テキスト] パネルで現在のエンド ポイント イベントを開く			✓
メールの添付ファイルをダウンロードする	✓		

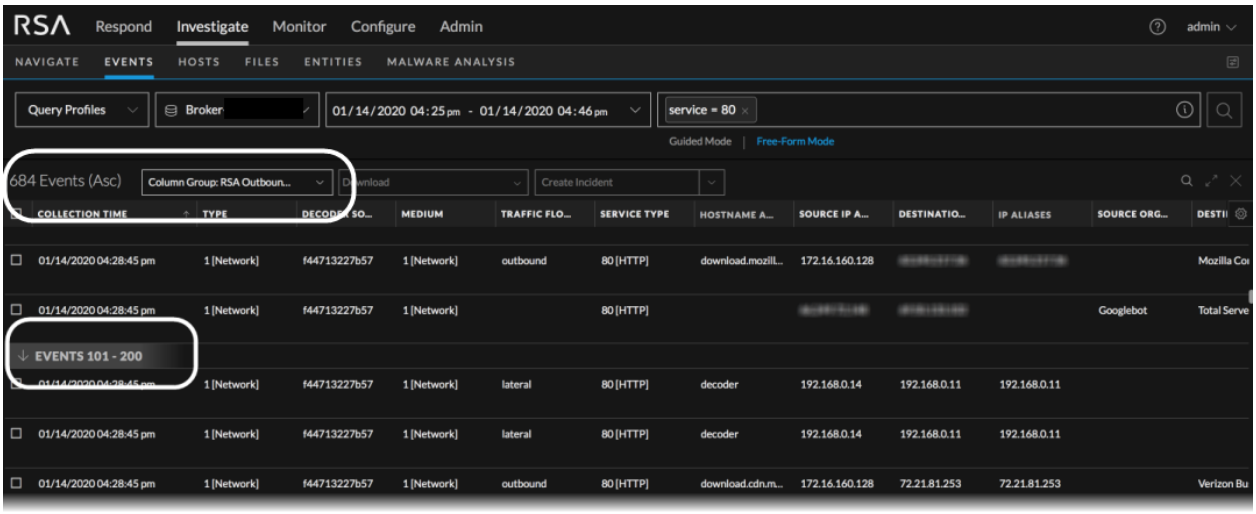
[イベント]ビューでのイベントの分析

注: バージョン11.4では、[イベント分析]ビューが[イベント]ビューとして名称変更され、イベント リストのデフォルト ビューとして[レガシー イベント]ビューを置き換えました。11.4より前の機能に関する情報は、11.3以前の[イベント分析]ビューにも適用されます。[レガシー イベント]ビューはデフォルトで無効になっていますが、管理者は、『*システム構成ガイド*』の「調査の設定の構成」の説明に従って有効にすることができます。以前のバージョンの詳細については、PDFドキュメント (https://community.rsa.com/docs/DOC-81328) を参照してください。

[イベント]ビューでクエリを送信すると、[イベント]パネルが開きます。[イベント]パネルでは、分析するイベントを選択できます。このパネルに表示されるイベントは、次の2つの条件を満たしています。

- 送信されたクエリと一致している。
- 選択した列グループに必要な1つまたは複数のメタ キーの値を含んでいる(イベント リストの表示中に列グループを変更すると、新しい列グループを使用した元のクエリが再送信されます。サービス、時間範囲、フィルタに対して行われた未送信のクエリの変更は無視されます)。

ロードできるイベント数には構成可能な制限があります。デフォルト値は5,000です。管理者は、『*システム構成ガイド*』の説明に従ってこの制限を設定します。[イベント]パネルへのイベントのロードが開始されます。イベントのロード中、リストの一番上の進行状況バーに進行状況が表示されます。最も古い収集時間のイベントが最初にロードされ、100個のイベントがロードされるたびに「イベントxxx-xxx」という形式の行番号インジケータがリストに挿入されます(次の図を参照)。



イベントのロード中はスピナーが表示されます。このカウントが閾値以上になると、閾値に達したことを伝え、クエリ コンソールで詳細を確認するよう求めるメッセージがスピナーの下に表示されます。データのロードが開始されると、メッセージが削除されます。すべてのイベントがロードされるまで、スピナーは表示されたままとなります。すべてのイベントがロードされると、次のいずれかのメッセージがリストの一番下に追加されます。

- 「すべてのイベントがロードされました。」
- 「上限の5,000件のイベントに達しました。クエリを絞り込んでください。」
- 「クエリをキャンセルする前に、4,000/5,000件のイベントを取得しました。」

バージョン11.3以降では、[イベント環境設定]ダイアログの[イベント]パネルに表示されているイベントのソート順を、「最も古い収集時間が最初」または「最も新しい収集時間が最初」に設定できます。デフォルト設定は「最も古い収集時間が最初」です。この設定は、ほとんどの調査に適しています。ログを調査するにあたり、ソート順を「最も新しい収集時間が最初」に変更する必要が生じることがあります。[イベント環境設定]ダイアログのこのユーザ設定は、データベースに保存され、ログアウトして再度ログインした後も維持されます。

バージョン11.4.1以降には、[ソートしない]という新しいオプションがあります。これは、コア サービスによって処理されたイベントを一覧表示する、デフォルトの環境設定です。[ソートしない]は、すべてのコア サービスの応答を待ってから結果を順番に表示するのではなく、一致が見つかり次第イベントを戻すため、処理がより高速です。

クエリに一致するイベントの数が5,000個の上限を超えると、タイム ウィンドウ内の最も新しいイベントまたは最も古いイベント5,000個が昇順でロードされます。どのイベントがロードされるかはソート順に基づいています。たとえば、30万個のイベントがクエリに一致し、ソート順が昇順に設定されている場合は、最も古い5,000個のイベントがデフォルトでロードされます。これを変更するには、ソート順を降順に変更し、最も新しい5,000個のイベントがロードされるようにします。

最も古いイベントを最初にロードする昇順のソートは、通常、ネットワーク イベントを調査するための最適な設定です。タイム ウィンドウ内の最も新しい5,000個のイベントを表示するには、[イベント環境設定]パネルで[ユーザ環境設定]のソート順を[降順]に変更します。設定の変更は、次回のクエリ送信時に有効になります。

リストの一番上には、ロードされたイベントの合計数と、5,000個のイベント数の上限に達したかどうかのメッセージが表示されます。

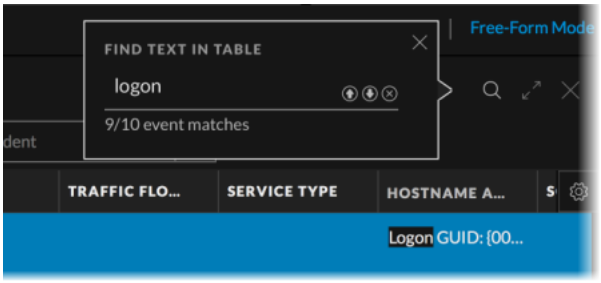
- リスト内のイベント数が5,000個未満の場合のメッセージは「xx,xxxイベント(昇順)」です。
- リスト内のイベント数が5,000個を超えている場合のメッセージは「最も古い10,000イベント(昇順)」です。

このビューからは、[イベント]パネルでイベントをソートするための列を選択して、特定のタイプの調査に役立つメタ キーを選択できます(列グループ)。Respondでイベントをダウンロードして、インシデントを作成できます。イベントをクリックすると、イベントの再構築がさまざまな形式(パケット、テキスト、ファイル、Web、メール)で開きます。[イベント]パネルと[再構築]パネルは同時に開くことができます。[パケット]パネルと[テキスト]パネルでは、追加機能を使用して、再構築の表示方法を調整したり、興味のあるデータを強調したりすることができます。

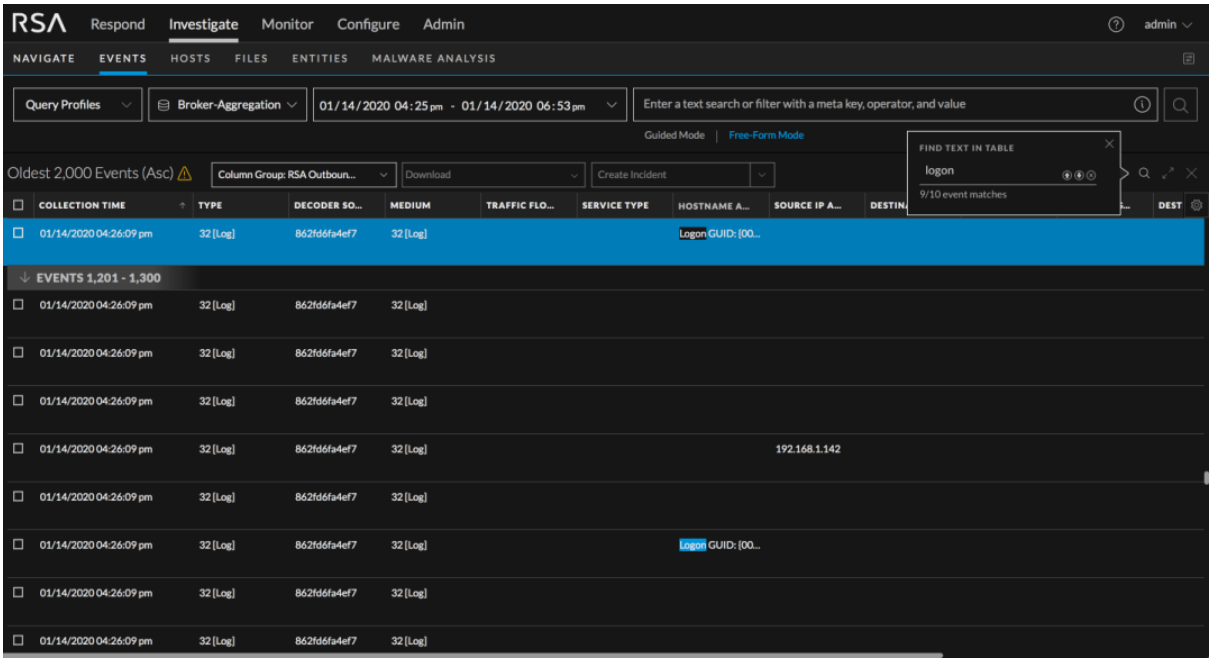
[イベント]パネルでのテキスト文字列の検索(バージョン11.4以降)

[イベント]パネルを開いた状態で、イベントのリストからテキスト文字列を検索できます。この検索は、ブラウザ ウィンドウでのCTRL-F検索と似ています。検索では、テーブルのすべての行のすべてのテキスト(表示可能な列のみ)で一致が検索され、一致するテキストがハイライト表示されます。表示されていない列は検索の対象となりません。[サマリー]列がテーブルの一部である場合、検索機能は無効になります。

1. [イベント]パネルにイベントがロードされた状態で、ツールバーの右側にある をクリックします。



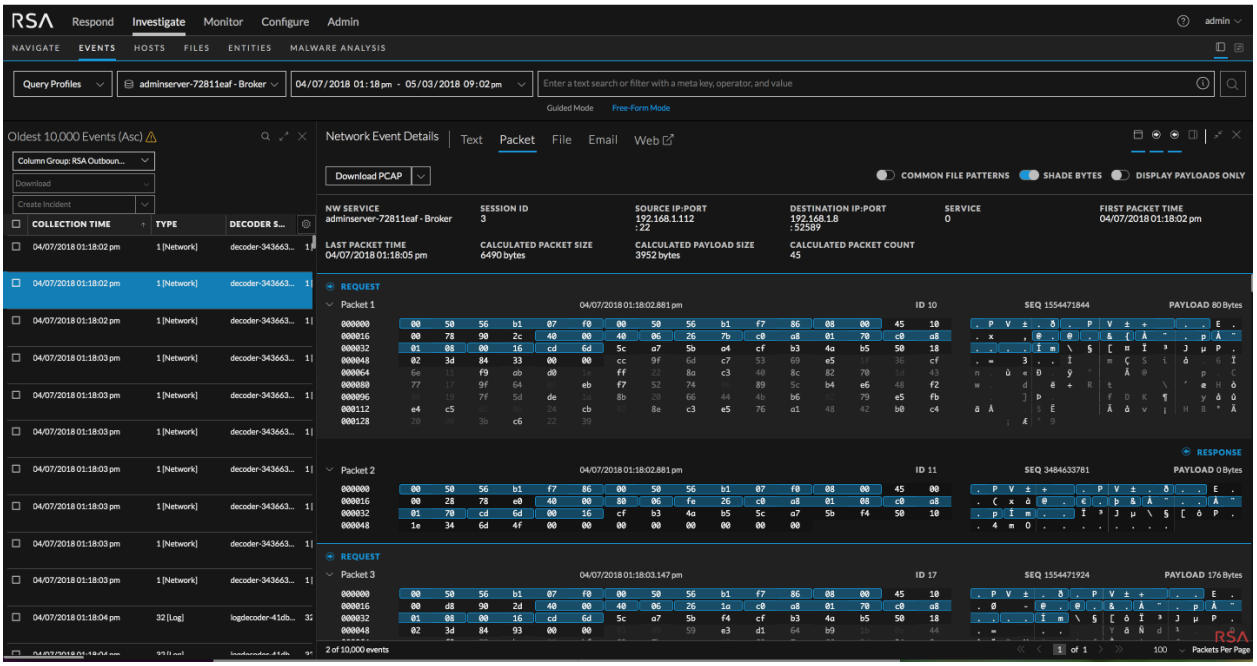
2. [**テーブルでテキストを検索**]ダイアログで、テキスト文字列を入力し始めます。
2文字を入力したところで、そのテキスト文字列の完全一致(大文字と小文字は区別しない)が[イベント]パネルでハイライト表示されます。テキストの入力を続けると、ハイライト表示されたイベントがさらに絞り込まれます。次の図は、[テーブルでテキストを検索]ダイアログで「logon」と入力した場合に見つかった結果の例を示しています。テキスト文字列が10個のイベントで検出されました。最初のイベントは青色でハイライト表示され、そのイベント内のテキスト文字列もハイライト表示されます。アイコンを使用して検索結果をナビゲートし、ダイアログを閉じることができます。



3. 検索結果をナビゲートするには、上矢印と下矢印をクリックします。
   - テキスト文字列が含まれている次のイベントを表示し、検索結果を下方向にナビゲートするには、下矢印をクリックします。最後の結果を表示しているときに下矢印をクリックすると、最初の結果がハイライト表示されます。
   - テキスト文字列が含まれている直前のイベントを表示し、検索結果を上方向にナビゲートするには、上矢印をクリックします。最初の結果を表示しているときに上矢印をクリックすると、最後の結果がハイライト表示されます。
4. 検索ダイアログを閉じるには、[X]をクリックするか、ESCAPEキーを押します。再構築を開いて、新しい列グループを選択するか、新しいクエリを実行した場合も、ダイアログが閉じます。

[イベント分]ビューを開く、閉じる、パネルのサイズを調整する

初期状態では、[ネットワーク イベントの詳細]、[ログ イベントの詳細]、[エンドポイント イベントの詳細]パネルは、デフォルトでウィンドウ幅の75%を占有します。

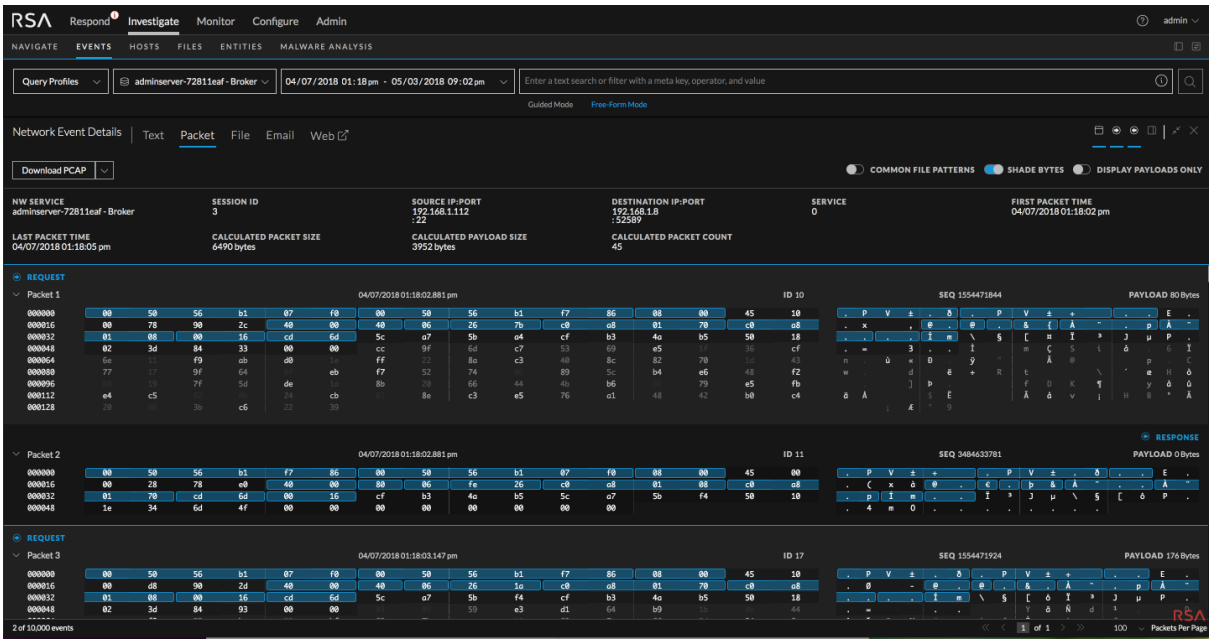


一方のパネルを拡大したり、縮小したり、閉じることにより、詳細パネルに対する[イベント]パネルのサイズの比率を調整し、読みやすさを改善することができます。閉じたパネルは、再度開くことができます。選択した比率は、その比率を変更するか、ブラウザを更新するまで維持されます。

表示を最適化するには、次の操作を実行します。

1. 2つのパネルのサイズの比率を調整するには、次のいずれかの操作を行います。
   a. 拡大するパネルのツール バーの  をクリックします。
   b. 縮小するパネルのツール バーの  をクリックします。
2. 一方のパネルを閉じて、もう一方の開いているパネルを幅いっぱいに表示するには、  をクリックします。

次の図は、ブラウザ ウィンドウの幅いっぱいに再構築を表示した例です。



3. [イベント]パネルを閉じた後で再度開くには、[イベント]ビューの右上隅にあるをクリックします。
   [イベント]パネルに前回閉じたときの状態(25%～75%または50%～50%)が表示されます。
4. [イベントの詳細]パネルを再度開くには、[イベント]パネル内のイベントをクリックします。

イベントの分析タイプの選択

イベントの分析タイプを選択するには、次のいずれかの操作を行います。

1. [イベント]ビューのツールバーで、分析タイプをクリックします。
2. ドロップダウン メニューで分析タイプ([**ファイル**]、[**テキスト**]、[**パケット**]、[**メール**]、[**Web**])を選択します。
   [**ファイル**]、[**テキスト**]、[**パケット**]、[**メール**]のいずれかを選択すると、データは選択したパネルに表示されます。
   [**Web**]を選択すると、単一イベントの再構築が新しいタブで開きます。これは、[レガシー イベント]ビューでのセッションの再構築と同じです。[レガシー イベント]ビューのWebの再構築の表示では追加の機能を利用でき、1つのイベントだけを表示するのではなく、別のイベントに移動することもできます(「[レガシー イベント]ビューでのイベントの再構築」を参照してください)。

注: パケット再構築は、ネットワーク イベントだけで使用可能です。

リクエストとレスポンスの表示を調整する

リクエストとレスポンスを含む分析タイプでは、いくつかの調整を行うことができます。

注： 分析タイプにリクエストとレスポンスがない場合は、このオプションは選択できません。[ファイル]パネルは、リクエストとレスポンスがない再構築のタイプの一例です。[テキスト]パネルで再構築されたログ イベントも、その一例です。

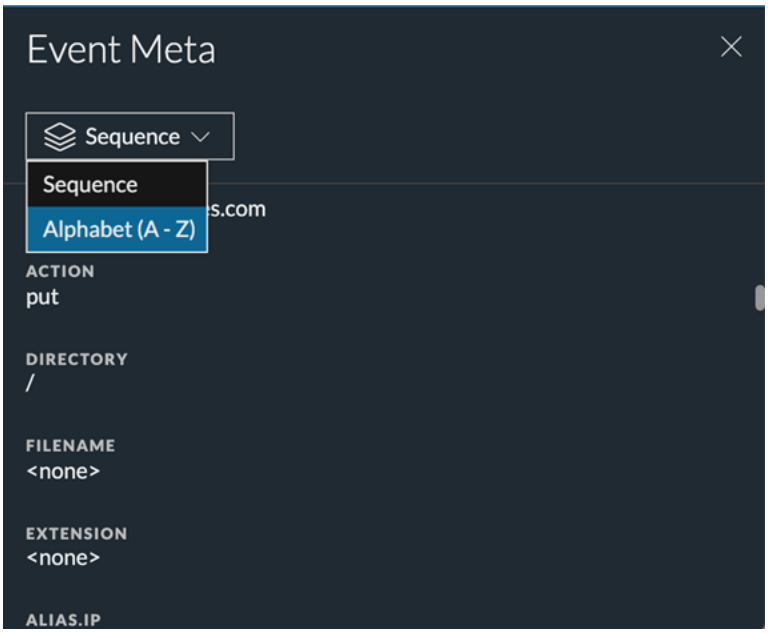
リクエスト( ) とレスポンス( ) のどちらか一方または両方を表示するように選択するには、矢印アイコンのいずれかまたは両方をクリックします。選択した情報で、再構築されたイベントが更新されます。

注： データが何も表示されない場合は、リクエストとレスポンスの両方の選択を解除している可能性があります。データを表示するには、2つのうちのいずれかは選択する必要があります。

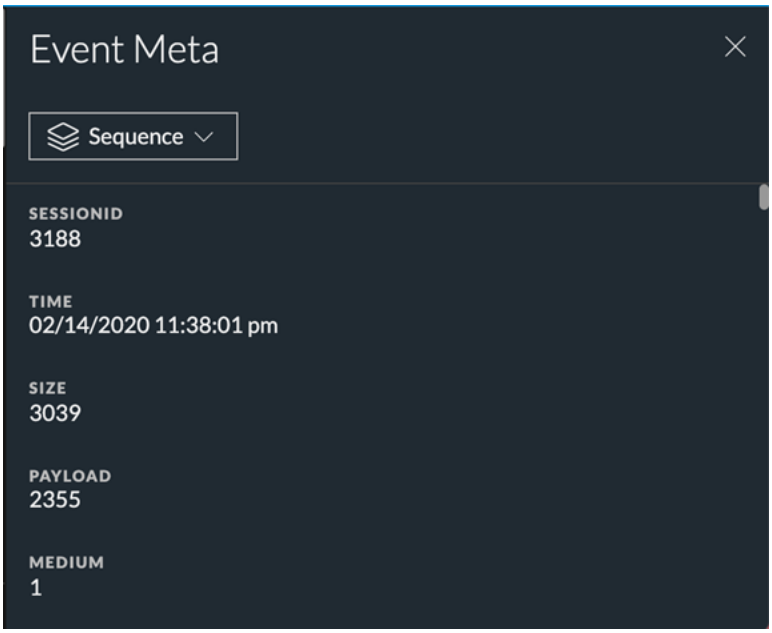
イベントの関連メタデータを表示する

[テキスト]パネル、[パケット]パネル、[ファイル]パネルでイベントを調査するときに、 をクリックして、隣接する[イベント メタ]パネルに関連するメタデータを表示できます。

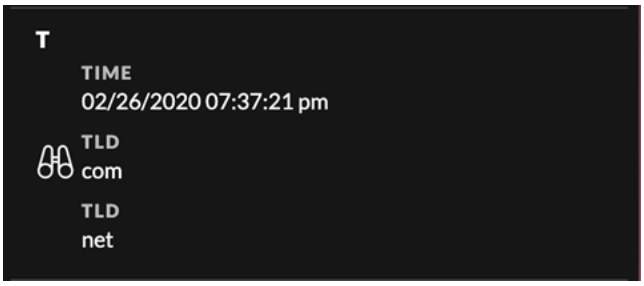
[イベント]ビューで結果に関連付けられたメタデータを確認するアナリストは、リスト内のメタデータの順序を変更して、探しているメタデータをより的確に見つけることができます。メタデータのリストのレイアウトがより直感的になり、必要に応じて、生成された順またはメタ キーのアルファベット順でメタデータを並べられるようになりました。次の図は、メタ キーのアルファベット順で並べたメタデータを示しています。



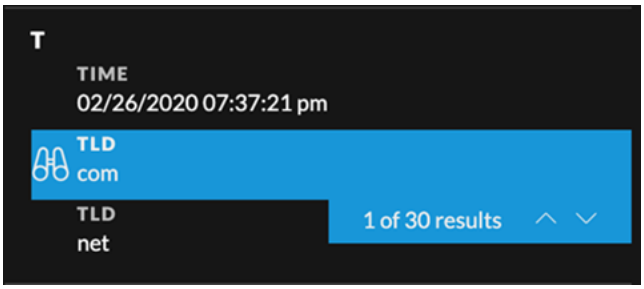
次の図は、同じメタデータをメタ キーの生成順で並べた場合を示しています。



[テキスト分析]パネルと[イベント メタ]パネルを表示しているときは、[イベント メタ]パネルのメタ キーとメタ値のペアにカーソルを合わせると、RAWテキストからメタ値を検索可能な場合は双眼鏡アイコンが表示されます。次の図は、検索可能なメタ キーをマークする、黒い背景色の白い双眼鏡アイコンの例です。



このアイコンをクリックすると、[テキスト]パネルでメタ キーとメタ値のペアの検索(大文字と小文字が区別されます)が開始され、検索結果がハイライト表示されます。次の図は、検索可能なメタ キー/メタ値の組み合わせをクリックすると表示される、青い背景色の白い双眼鏡アイコンの例です。

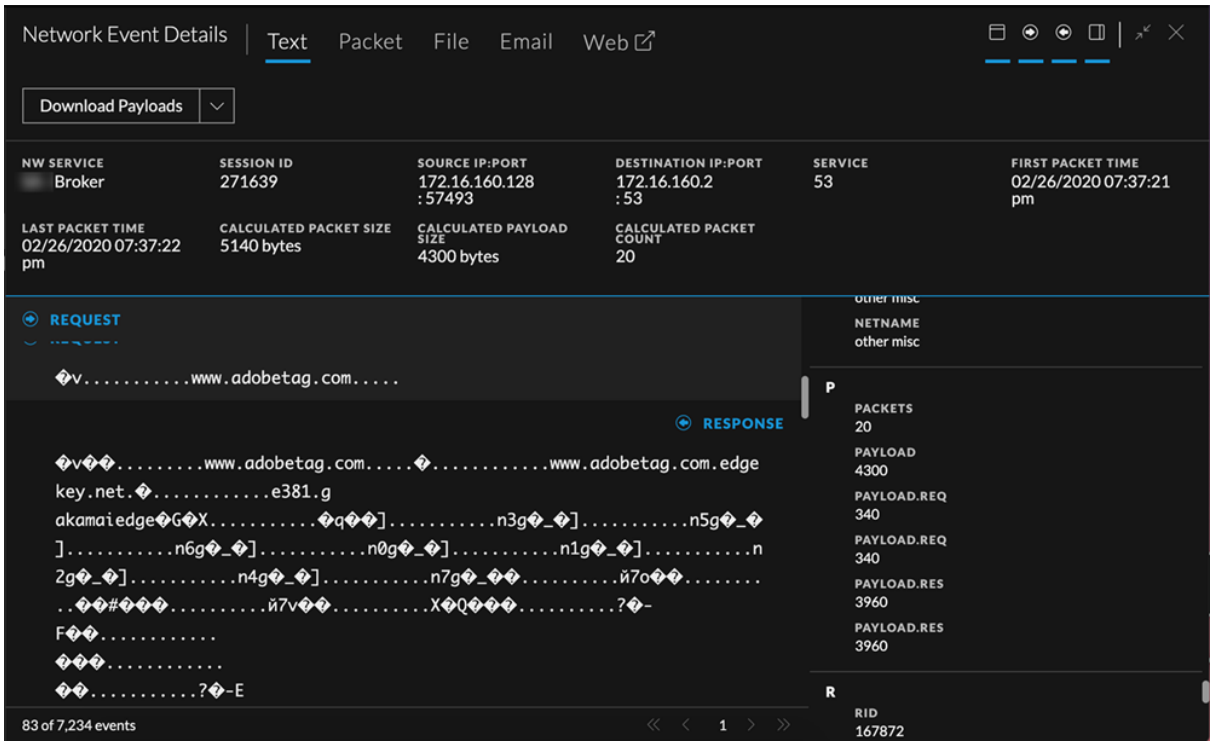


[イベント メタ]パネルには、ハイライト表示された行に結果の件数が示されるほか、[テキスト]パネルでそれぞれの結果に迅速に移動するために使用する上下矢印が表示されます。スクロール ボタンを使用すると、メタ キーの生成をトリガーしたデータがハイライト表示された場所を、1つずつ前に、または1つずつ後ろに移動して表示することができます。

RAWテキスト内に関連する値が存在するメタ キーのみを検索できます。一度に検索できるメタ キーは1つだけです。3000文字を超えるためトランケート表示されたテキスト エントリーは、検出されたメタ値が見えるよう展開して表示されます。

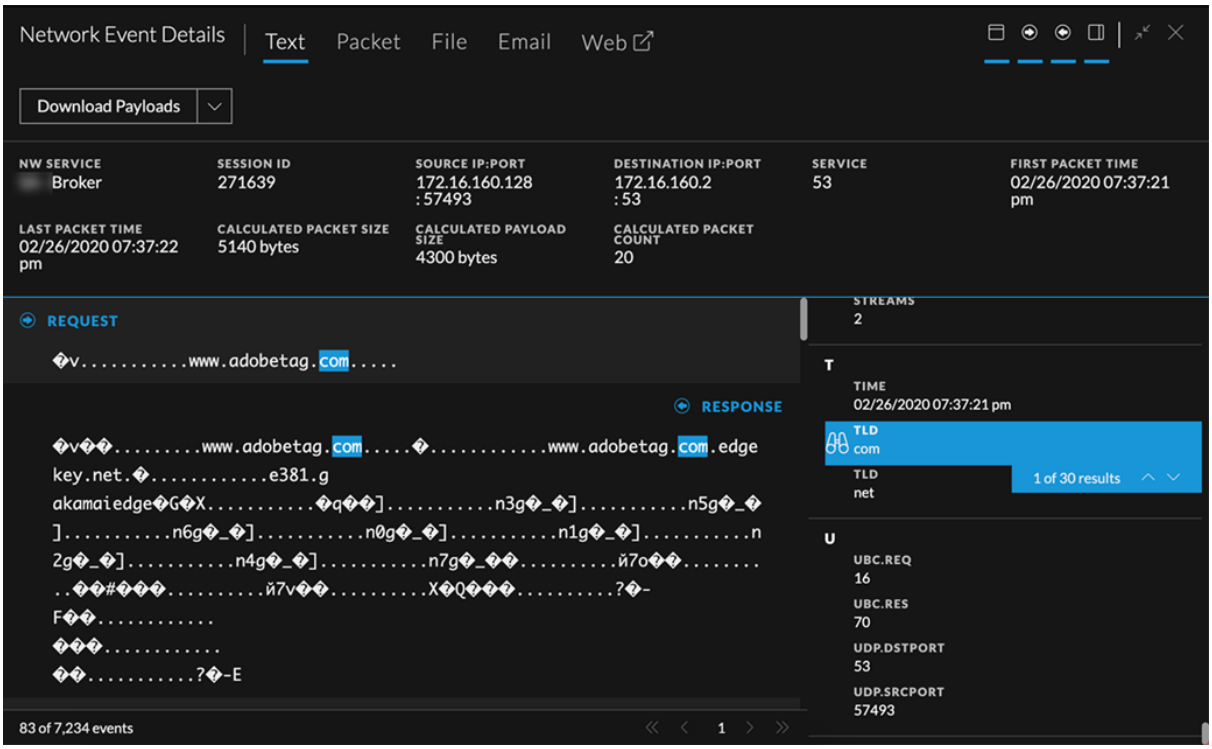
メタ キーの生成をトリガーしたメタ値をRAWテキストから検索するには、次の手順を実行します。

1. [テキスト]パネルでネットワーク イベントを開き、  をクリックして[イベント メタ]パネルを開きます。



2. メタ キーの横に双眼鏡アイコンが表示されるまで、リスト内のメタ キー/メタ値のペアの上にマウスを合わせます。
3. RAWテキストの値を検索するには、検索可能であることを示す双眼鏡アイコンが表示された行をクリックします。
   該当する値がテキストに含まれていない場合は、検索対象の値が[イベント メタ]パネルでハイライト表示され、[テキスト]パネルでは何もハイライト表示されません。
   [テキスト]パネルに関連する値が1つ以上見つかった場合は、値の場所がハイライト表示されます。[イベント メタ]パネルには検索対象の値がハイライト表示され、スクロール用の上下矢印が表

示されます。



4. ハイライト表示を消すには、[イベント メタ]パネルで同じメタ キーとメタ値のペアの双眼鏡アイコンをクリックするか、[イベント メタ]パネルで異なるメタ キーと値のペアの双眼鏡アイコンをクリックするか、[イベント メタ]パネルを閉じます。
RAWテキストからハイライト表示が消えます。

注： メタ値が255文字を超える場合、そのメタ キーの上にカーソルを合わせると、完全な値が表示されます。

イベント ヘッダーを表示または非表示にする

[パケット]パネル、[テキスト]パネル、[ファイル]パネルでイベント ヘッダーを非表示にして、データの表示領域を縦方向に拡大するには、  をクリックします。このアイコンをもう一度クリックすると、イベント ヘッダーが表示されます。

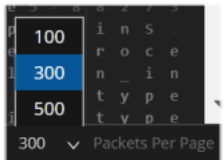
[パケット]および[テキスト]パネルでのイベントのページ移動

ページ移動コントロールで、パケットやテキストのリストのページ操作を柔軟に実行できます。[パケット]パネルでは、1ページあたりに表示するパケット数を選択できます。選択内容は、NetWitness Platformアプリケーションへのログイン間で維持されます。アイコンを使用できないときは、グレー表示されます。たとえば、1ページ目を表示しているときは、とのアイコンは、グレー表示されます。

注： ページ移動コントロールはバージョン11.2以降の[テキスト]パネルで使用できます。

ページ移動アイコンを使用するには、次の手順を実行します。

1. [イベント]ビューでイベントが開いた状態で、現在のページあたりのパケット数(**50**、**100**、**300**、**500**)をクリックして、ドロップダウン メニューから、新しいページあたりのパケット数を選択します。



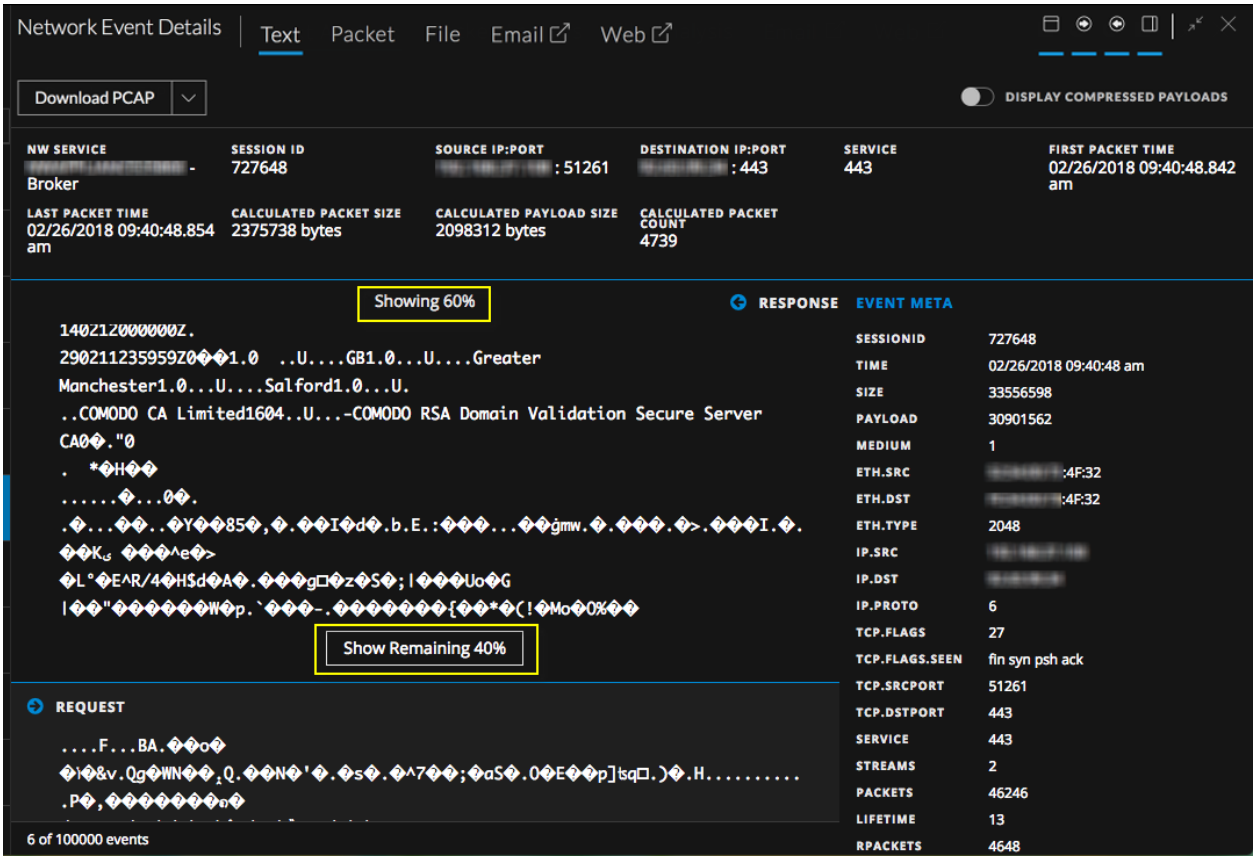
2. ページを前後に移動するには、次のページ コントロール アイコンを使用します。
   次のページに移動するには▶をクリックします。
   最後のページに移動するには⏭をクリックします。
   前のページに移動するには◀をクリックします。
   最初のページに移動するには⏮をクリックします。

3. 特定のページに移動するには、ページ番号フィールド(1 of 206)にページ番号を入力します。

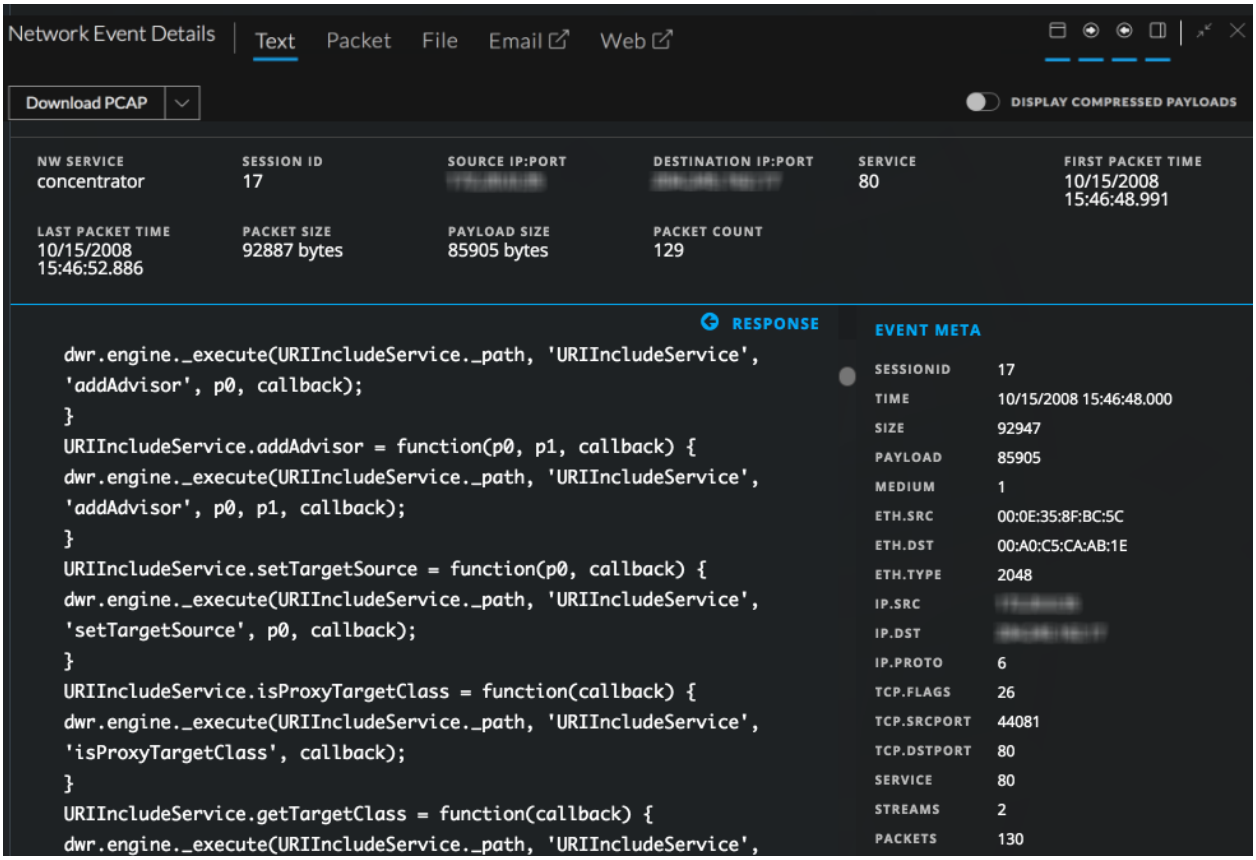
注:[テキスト]パネルでは、手動で最後のページまで移動しないと、最後のページ コントロール アイコンが使用可能になりません。

[テキスト]パネル内のトランケートされたテキスト エントリーを展開する

[テキスト]パネルでのネットワーク イベントの再構築には、何十万もの大量の文字からなるリクエストとレスポンスが含まれる場合があり、6,000文字を超えるような関係のない長いエントリーをスクロールすることは時間の無駄になる可能性があります。アナリストのエクスペリエンスを向上させるために、6000文字以上が含まれるすべてのテキスト エントリーは最初の2000文字のみを表示するようにトランケートされます。次の図は、2000文字より大きいエントリーの例です。ヘッダーのメッセージが総文字数の何%を表示しているかを示しています。



現在表示されているのは全体の60%(最初の2,000文字) であるため、残りのエントリーを表示するには、[**残り40%を表示**]をクリックします。



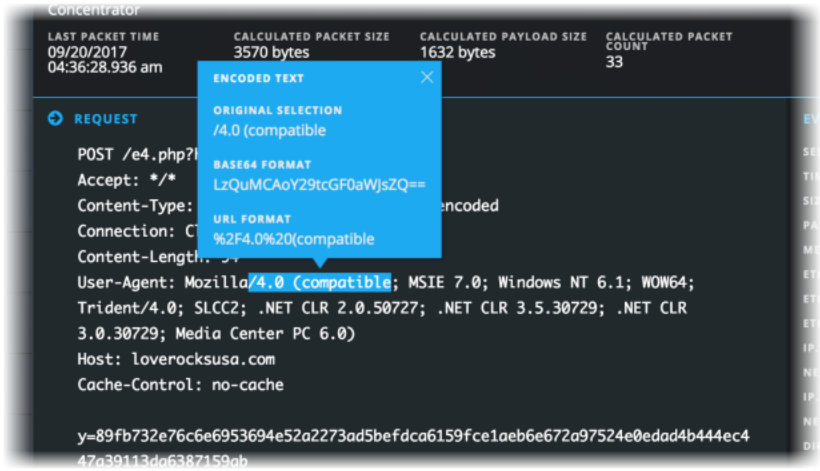
[テキスト]パネルでテキストがトランケートされた状態で、[イベント メタ]パネルに表示されているメタデータを検索した場合、トランケートされたテキストも検索対象に含まれます。非表示のテキスト内にメタデータが存在する場合、検出されたメタデータの場所がわかるようテキスト エントリーが展開されます。

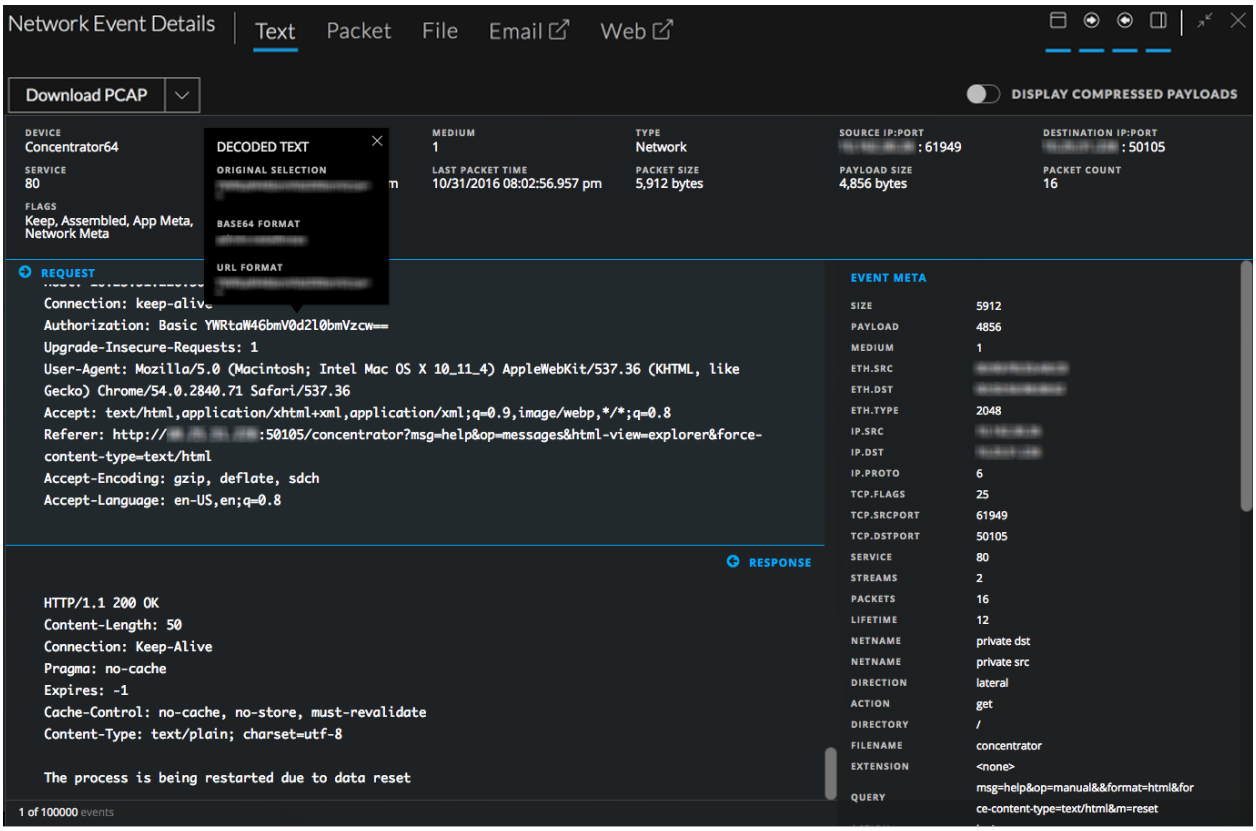
[テキスト分析]パネルでURLとBase64のエンコードおよびデコードを実行する

[テキスト]パネルで再構築されているネットワーク セッションにBase64またはURLエンコードされた文字列が含まれる場合、セッションをよく理解するために文字列をデコードすることができます。セッションにBase64またはURLのデコードされた文字列が含まれる場合、他のセッションに同じ文字列がエンコードされた形式で含まれていないかを検索するため、文字列をエンコードすることができます。

[テキスト]パネルでエンコードされたテキストが含まれるネットワーク セッションを表示している場合、1つのリクエストまたはレスポンス内のテキストの一部を選択して、エンコードまたはデコードした形式で表示することができます。Decoderにロードされたコンテンツによっては、セッション内にBase64かURLでエンコードされたデータがあることを示す追加のメタデータが含まれることがあります。

次の図は、URLエンコードとBase64エンコードされたテキストを表示するポップアップの例です。

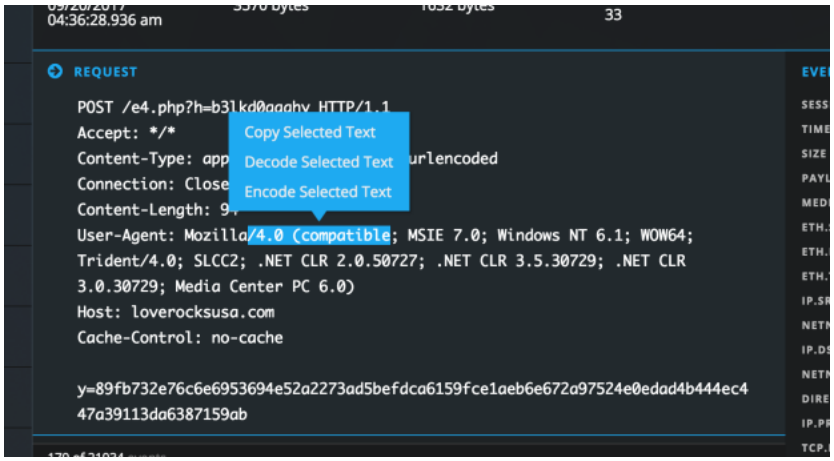




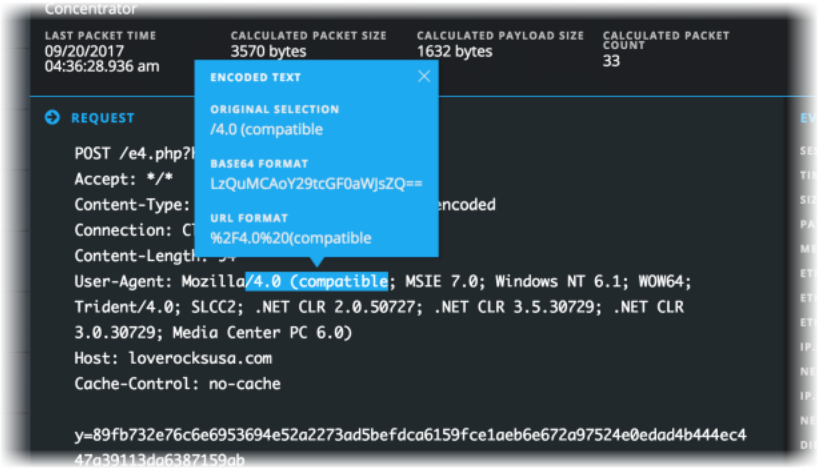
[テキスト]パネルでエンコードおよびデコードを実行するには、次の手順を実行します。

1. **[イベント]ビュー**で、エンコードまたはデコードされたコンテンツを含むセッションの[テキスト]パネルを表示します。
2. デコードされたテキストをエンコードされた形式で表示するには、1つのリクエストまたはレスポンス内でテキストをドラッグして選択します。

エンコードとデコードのオプションがメニューに表示されます。



3. [**選択したテキストをエンコード**]をクリックします。
ポップアップにエンコードされたテキストが表示されます。このポップアップは、✕をクリックするまで、[テキスト]パネル内の別のテキストを選択するまで、[イベント]パネルを閉じるまで、再構築する別のイベントを選択するまで、別の再構築ビューに切り換えるまで表示されます。



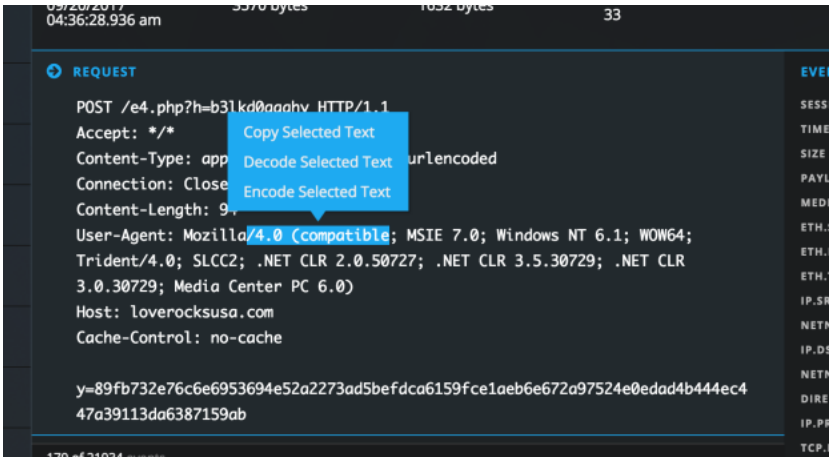
長いテキストを選択すると、ポップアップはスクロール可能になり、選択したテキストとデコードされたテキスト全体が収まる大きさになります。

4. セッションに含まれるエンコードされたテキストをデコードされた形式で表示したい場合は、1つのリクエストまたはレスポンス内でテキストをドラッグして選択します。
エンコードとデコードのオプションがメニューに表示されます。

5. [**選択したテキストをデコード**]をクリックします。
ポップアップにデコードされたテキストが表示されます。このポップアップは、✕をクリックするまで、[テキスト]パネル内の別のテキストを選択するまで、[イベント]パネルを閉じるまで、再構築する別のイベントを選択するまで、別の再構築ビューに切り換えるまで表示されます。

6. テキストの再構築から一部のテキストをコピーする場合は、次のいずれかの操作を行います。

   a. 一部のテキストをドラッグして選択し、右クリックして、ポップアップ メニューから[**選択したテキストをコピー**]を選択します。



b. テキストの一部をドラッグし選択し、[**選択したテキストをデコード**]または[**選択したテキストをエンコード**]のいずれかを選択します。ポップアップ内で目的のテキストを選択し、**Control-C**を押します。
選択したテキストがクリップボードにコピーされ、ペーストできるようになります。

7. 操作が終了したら、■をクリックしてポップアップを閉じます。

[テキスト]パネルでHTTPネットワーク セッションの解凍されたテキストを表示する

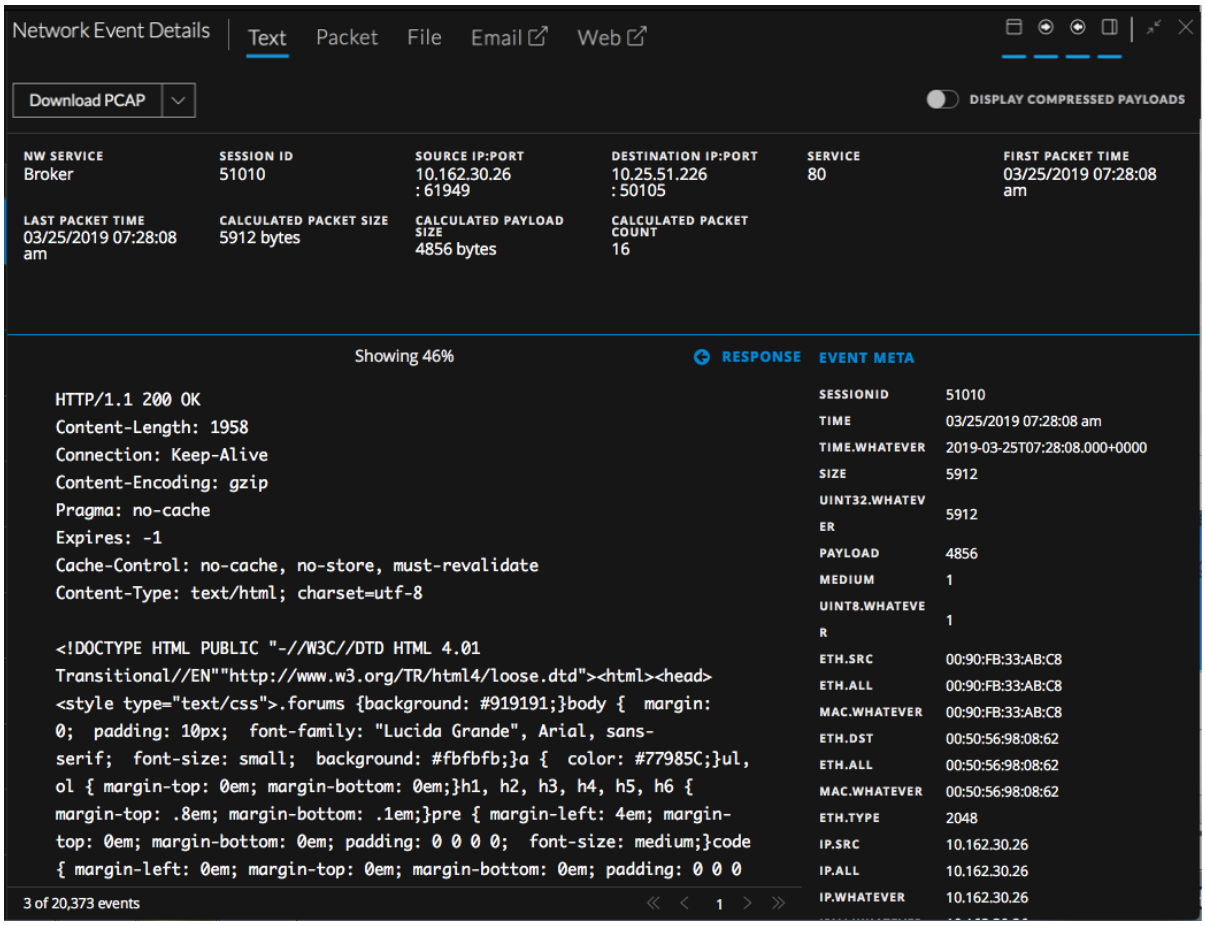
HTTPネットワーク セッションのコンテンツが圧縮されている場合、NetWitness Platformは[テキスト]パネルにデフォルトで解凍されたコンテンツを表示します。これにより、任意のパターンがあるか判断し、読み取り可能な文字を表示することができます。圧縮されたテキストを圧縮表示するか解凍表示するかを切り替えることができます。

注: 解凍されたテキストの表示は、[パケット]パネル、[ファイル]パネル、非HTTPネットワーク セッション、ログ データでは使用できません。

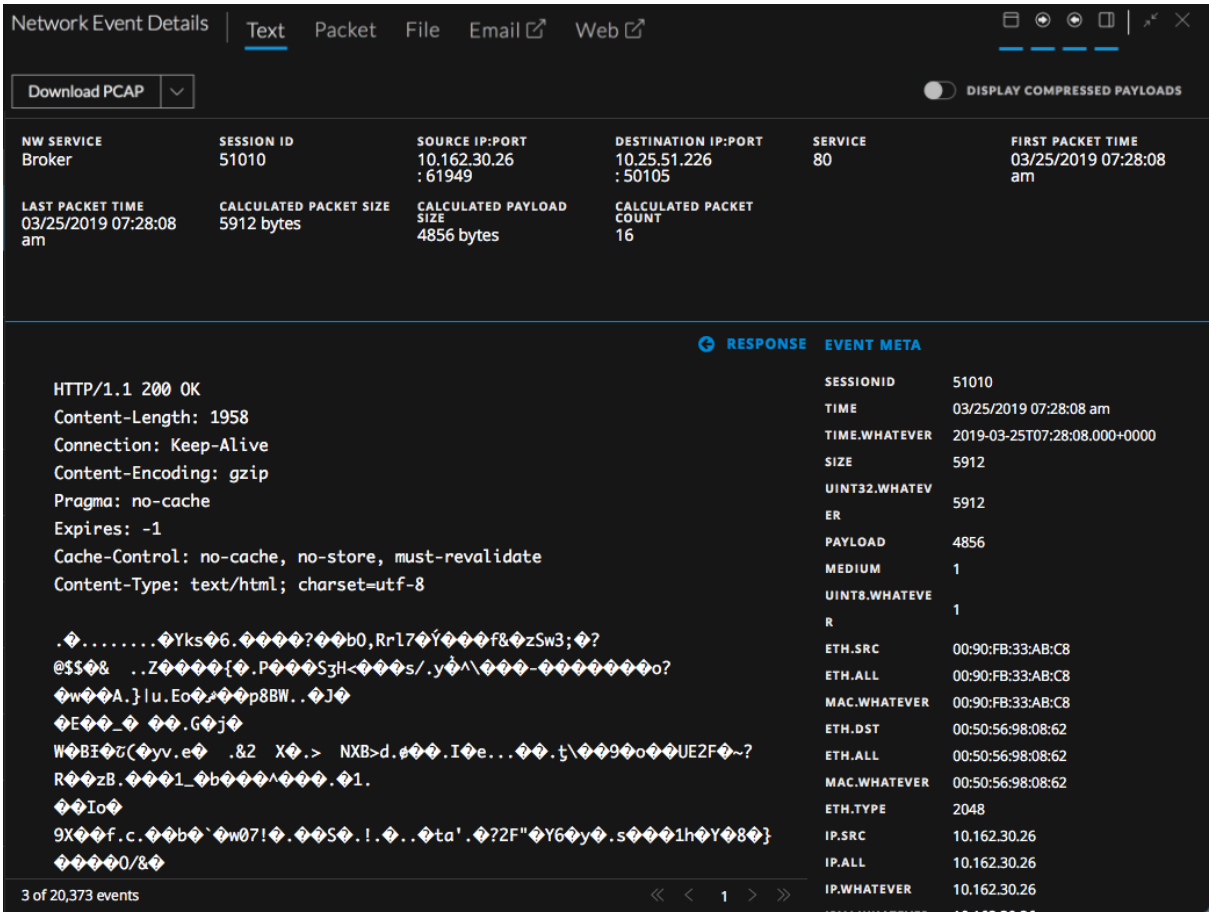
圧縮表示と解凍表示の切り替えボタンは、[テキスト]パネルのみに表示され、圧縮されたテキスト コンテンツがある場合にのみ有効になります。

1. 圧縮されたコンテンツを含むHTTPセッションの[テキスト]パネルを開きます。
デフォルトで、セッションはテキストが解凍された状態で再構築され、[**圧縮されたペイロードの表**

示]切り替えスイッチが再構築の上に表示されます。



2. 同じテキストを圧縮形式で表示するには、切り替えスイッチをクリックします。
表示が切り替わって、圧縮されたテキストが読めなくなり、スイッチの[圧縮されたペイロードの表示]がオンになります。



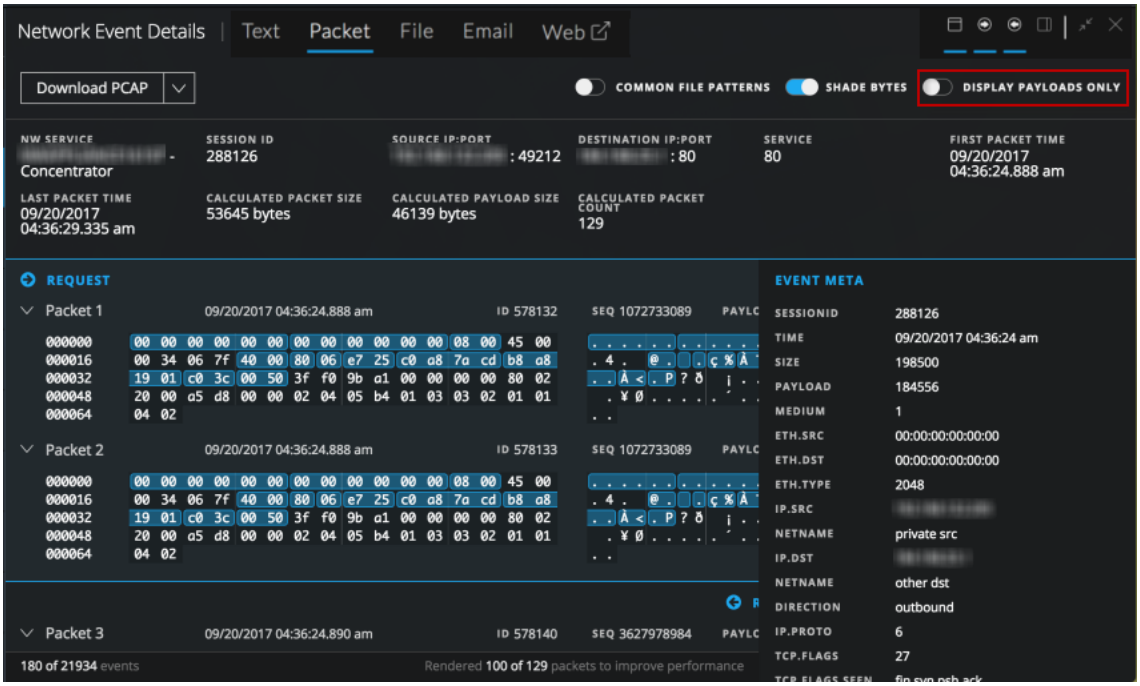
3. 解凍されたテキストの表示に戻すには、スイッチを再度クリックします。

ネットワーク セッションの[パケット]パネルで[ペイロードのみ]オプションを使用する

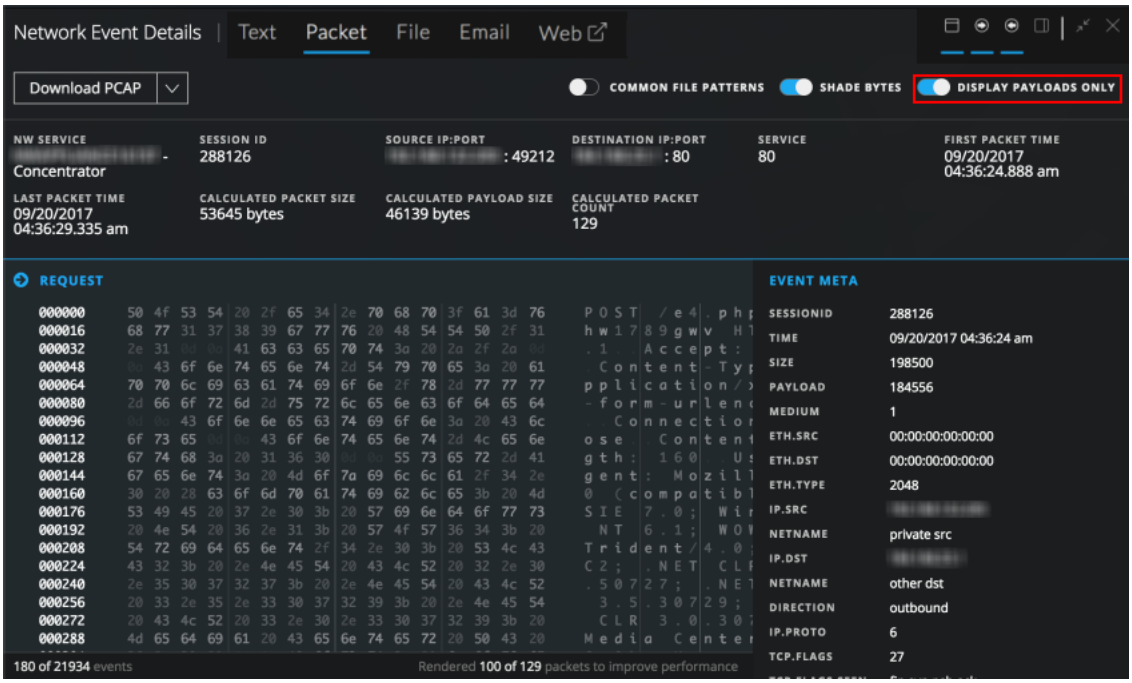
[パケット]パネルでネットワーク セッションの再構築を表示しているときは、各パケットの主なペイロードのみを表示することを選択できます。デフォルトでは、各パケットのヘッダーとフッターのバイトが表示されます。[ペイロードのみ表示]スイッチをクリックしてこれらを非表示にできます。ペイロード バイトのみを表示している場合、[ペイロードのみ表示]切り替えスイッチをオフに設定すると、デフォルト設定を復元できます。この設定は、それを変更するか、ブラウザを更新するまで保持されます。

- [ペイロードのみ表示]オプションをオフにすると、パケット番号、パケットのヘッダー、パケットのフッター、ペイロードが表示されます。
- [ペイロードのみ表示]オプションをオンにすると、パケットのヘッダーとフッターのバイトは表示されません。パケット コンテンツのみが、1行あたり16バイトの16進数とそれに対応するASCII文字で表示されます。

1. [**イベント**]ビューで、ネット ワーク セッションの[パケット]パネルに移動します。
デフォルト で、パケット ヘッダー、フッター、ペイロード が表 示された状 態 でセッションが再 構 築されます。

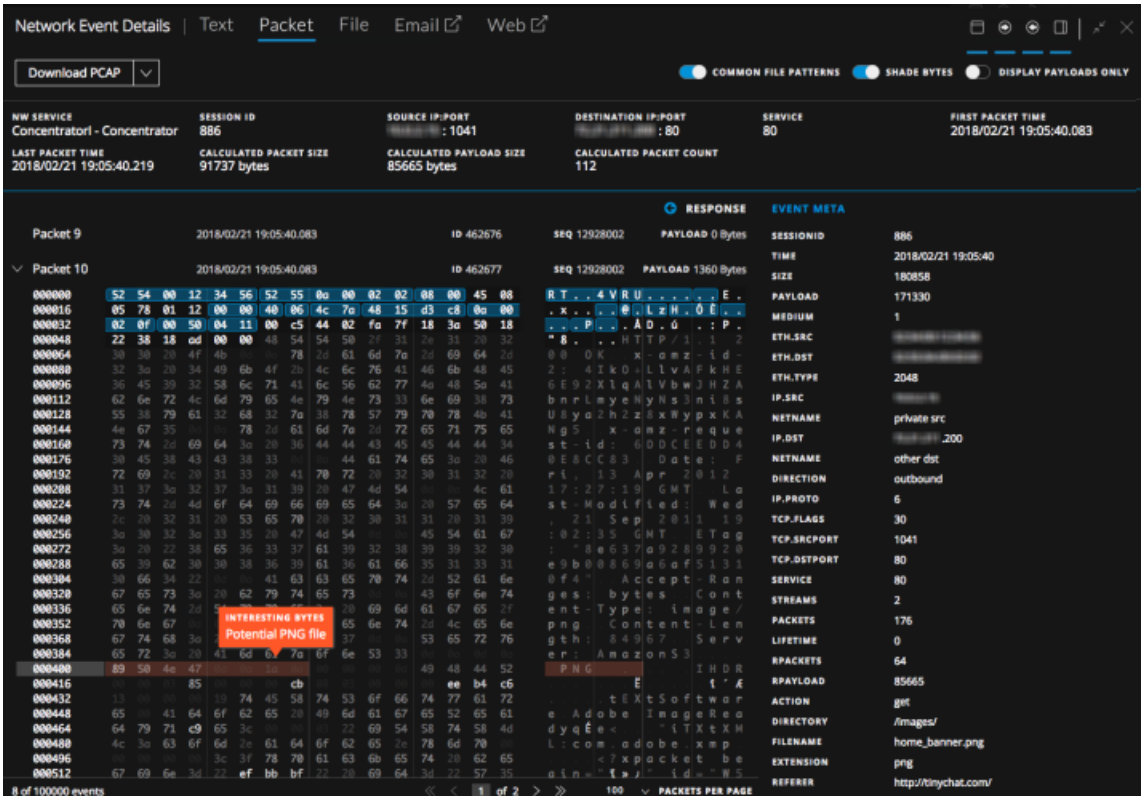


2. 各 パケット のペイロード のみを表 示 するようにビューを切り替 えるには、[**ペイロード のみ表 示**]切り替えスイッチをクリックします。
ビューが切り替 わり、ペイロード のみが表 示され、同じサイド の連 続したパケット が連 結されて、ペイロード がより読みやすく理 解しやすくなります。

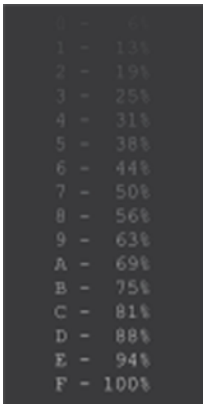


[パケット]パネルでバイトをハイライト表示する

[パケット]パネルで最初に再構築を開くと、各パケットの重要なヘッダー バイトは青色でハイライト表示され、パケットの内容を理解しやすくするために、ペイロード バイトは濃淡化により区別されます。次の図は、ハイライト表示とバイトの濃淡化が有効になったデフォルトのパケットです。



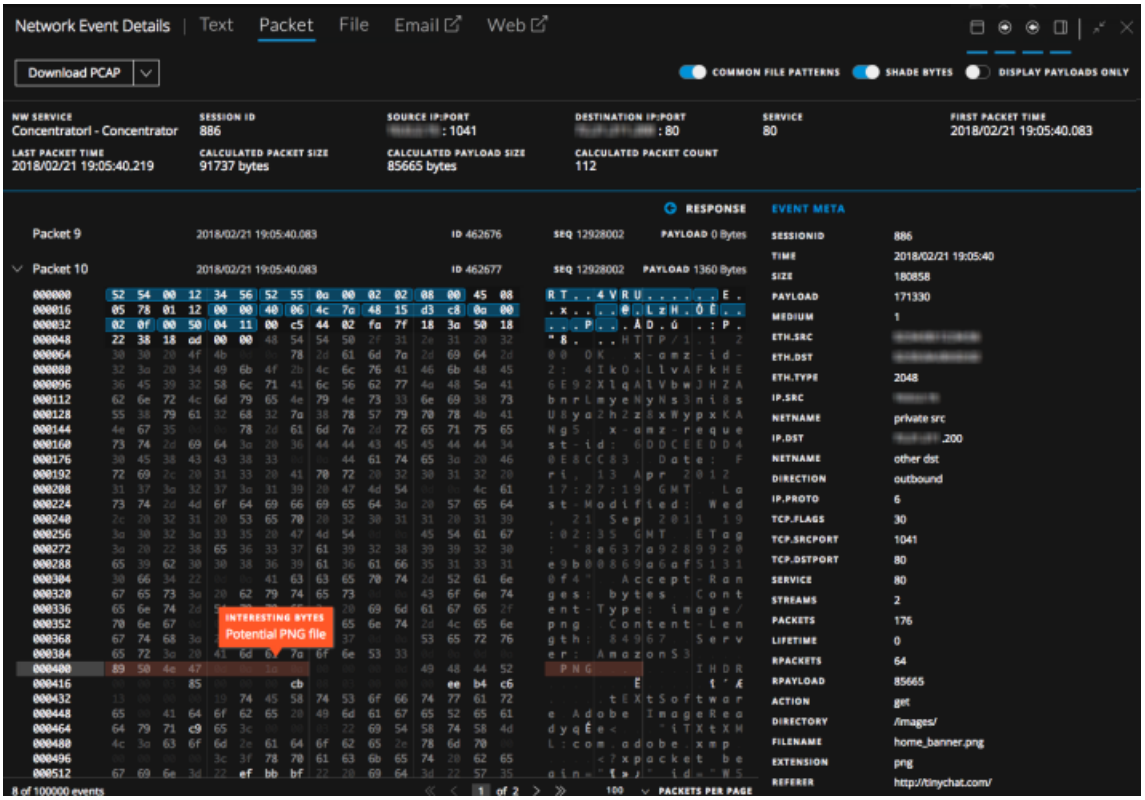
[バイトの濃淡化]オプションは、16進数バイト(00～FF) を識別しやすくするため濃淡を変えてバイトを表示する機能です。下のレンジのバイトほど薄い色で表示され、255に近いバイトは濃い色で表示されます。16進数およびASCIIの両方が濃淡化されます。次の図は、16進数の各バイトを濃淡化した例です。



[バイトの濃淡化]スイッチは、バイトの濃淡化を制御します。[バイトの濃淡化]をオンまたはオフに設定すると、設定を変更するか、ブラウザを更新するまでその設定が保持されます。

[パケット]パネルで一 般 的なファイル タイプをハイライト表 示 する

[パケット]パネルで、アナリストは、ファイル シグネチャに基 づいて特 定 のファイル タイプをハイライト表 示 したり、非 表 示 にしたりできます。[一 般 的なファイル パターン]機 能 がオンの場 合 は、ペイロード 内 にあるファイル シグネチャのマジック ナンバーのバイトがハイライト表 示 され、ハイライト表 示 にカーソルを合 わせると潜 在 的なファイル タイプが表 示 されます。この例 では、89 50 4e 47が16進 数 のペイロード でハイライト表 示 され、PNGがASCIIのペイロード でハイライト表 示 されています。ハイライト表 示 されているバイトにカーソルを合 わせると、ポップアップに、そのマジック ナンバーに関 連 する潜 在 的なファイル タイプが表 示 されます。



次 の表 は、ペイロード に存 在 する場 合 にハイライト表 示 されるファイル タイプと対 応 するマジック ナンバーです。

ファイル タイプ	16進 数 のシグネチャ	ASCIIエンコード
DOS実 行 可 能 プログラム/Windows PE	4D 5A	MZ
PNG(ポータブル ネット ワーク グラフィックス)	89 50 4E 47 0 D 0A 1A 0A	PNG
JPEG	FF D8 FF	JPEG
JPEG/JFIF	4A 46 49 46	JFIF
JPEG/Exif	45 78 69 66	Exif

ファイル タイプ	16進 数 のシグネチャ	ASCIIエンコード
GIF	47 49 46 38 37 61	GIF87a
GIF	47 49 46 38 39 61	GIF89a
移植性がない実行可能プログラム	5A 4D	ZM
BMP	42 4D	BM
PDF	25 50 44 46	%PDF
古いOfficeドキュメント(doc、xls、ppt、msg、その他)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
ZIPファイル形式、およびJAR、ODF、OOXMLなどのZIPに基づく形式	50 4B	PK..
7 ZIPファイル形式(7z)	37 7A BC AF 27 1C	7z¼¯'
Javaクラス ファイル、Mach-O Fatバイナリ	CA FE BA BE	Êþº¾
PostScript	25 21 50 53	%!PS
Unix/Linuxのシェル スクリプト	23 21	#!
ELF(実行可能プログラムおよびリンク可能な形式) の実行可能プログラム	7F 45 4C 46	.ELF

[パケット分析]パネルに一般的なファイル シグネチャを表示するには、次の手順を実行します。

1. [パケット分析]パネルに移動し、[**一般的なファイル パターン**]オプションをオンにします。
   ビューに複数のハイライト表示がある場合は、すべてが表示されます。
2. ポップアップを表示するには、ハイライト表示された場所にカーソルを置きます。

[レガシー イベント]ビューでのイベントの再構築

[レガシー イベント]ビューでイベントのリストを表示する際、イベントの元の形式と一致する読み取り可能な形式で安全にイベントを再構築することができます。再構築されたイベントの初期ビューには、最適な形式(「最適な表示」)がデフォルトで使用されます。たとえば、Webコンテンツは Webページとして再構築され、IMによる会話はチャットとして表示されます。再構築のデフォルト表示は、[プロファイル]>[環境設定]ビューで各ユーザが変更できます。

イベントのイベントIDがわかっている場合は、[ナビゲート]ビューから再構築を開くこともできます。

再構築では、次のことができます。

- 表示するイベント情報を選択。リクエスト データ、レスポンス データ、またはその両方を選択することができます。
- 再構築のタイプを選択。詳細、テキスト、16進数、パケット、Web、メール、IMのいずれかを選択できます。
- RAWログをエクスポート。
- イベントをPCAPファイルとしてエクスポート。
- イベントから任意のファイルを抽出。
- イベントに関連づけられたすべてのメタ データを抽出。

> **注意:** 再構築でファイルへのリンクをクリックするときは気を付けてください。そのファイルに関連づけられているアプリケーションがシステムに含まれる場合、またはブラウザでそのファイルを開くことができる場合、それが悪意のある添付ファイルだと、システムに悪影響を及ぼすことがあります。

- イベントを個別のウィンドウまたはタブで表示(使用しているブラウザの構成により異なる)。
- 現在のビューでプレビューとして再構築を表示している場合、左下隅にあるナビゲーション ボタンで前後のページのイベントに移動することができます。

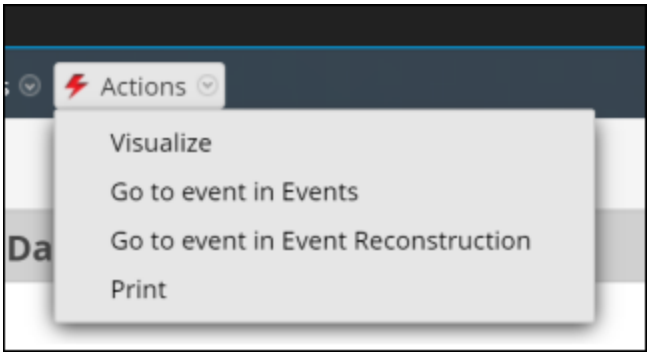
注: Investigationのアプリケーション パフォーマンスは、管理者が、[再構築の設定]と[再構築キャッシュの設定]で管理できます。アナリストが調査対象のセッションを再構築表示する場合、パフォーマンスと表示結果に影響を与える要素が2つあります。
イベントによっては、サイズが極めて大きく、ソース パケットが膨大な数に上ることがあります。このようなセッションを再構築すると、アプリケーションのパフォーマンスが低下する可能性があります。
再構築キャッシュの表示内容が不正確である場合があります。このような理由から、1日以上経過したキャッシュは、24時間おきにNetWitness Platformによって消去されます。日次のキャッシュ クリーニングの合間に特定のアクションを実行すると、古いキャッシュの情報を使用して再構築が行われる可能性があります。管理者は必要に応じて、NetWitness Serverに接続する1つ以上のサービスのキャッシュを手動でクリアできます。

イベントIDを使用したイベントの再構築

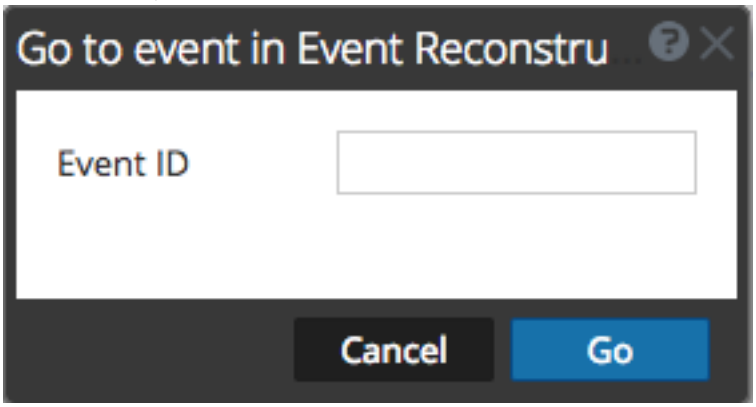
イベントIDがわかっている場合に、イベントを[ナビゲート]ビューから直接再構築できます。このオプションを使用すると、調査の開始時に通常必要となる、クエリの実行は必要ありません。`eventid`だけを使用してイベントに直接移動できるようにするには、サービスと時間範囲を選択する必要があります。

再構築またはイベント分析を[ナビゲート]ビューから直接表示するには、次の手順を実行します。

1. **調査＞ナビゲート**に移動して、**[アクション]＞[イベントでイベントに移動]**または**[イベントの再構築でイベントに移動]**を選択します。



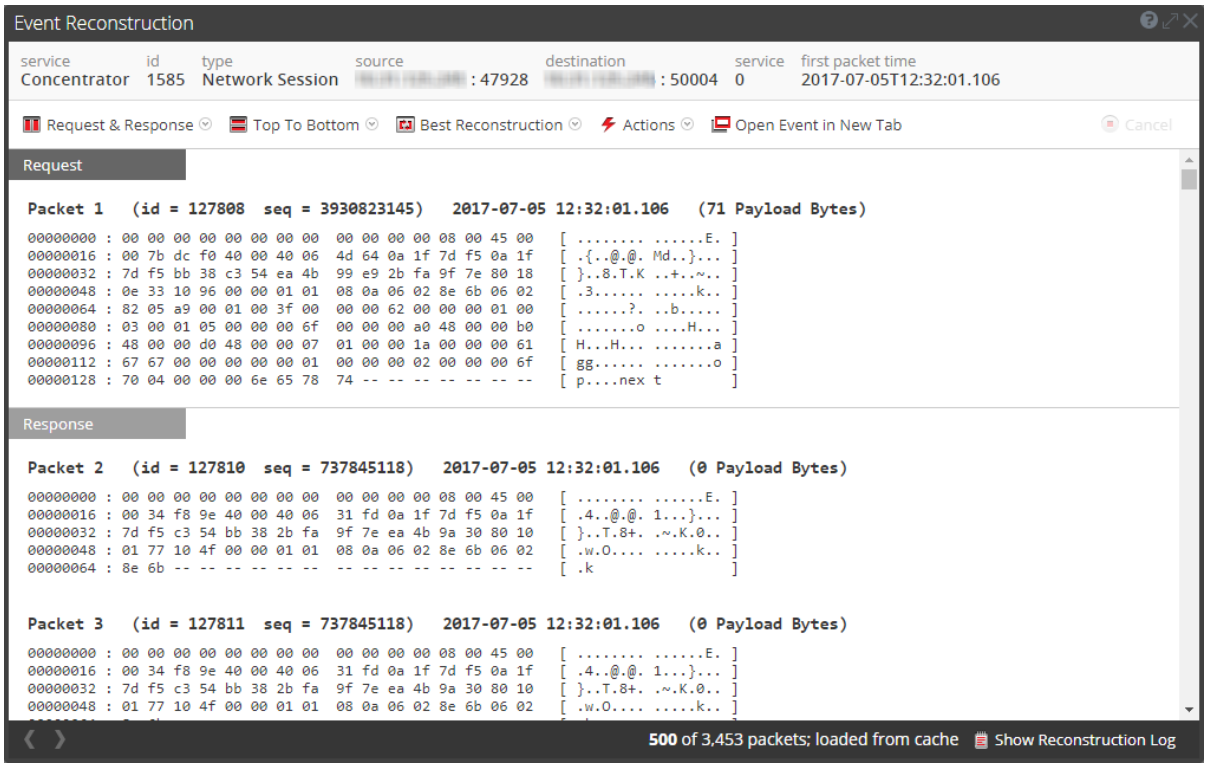
[イベントに移動]ダイアログが表示されます。ダイアログは2つ(イベント用とレガシー イベント再構築用に1つずつ)あります。いずれのダイアログでもイベントIDの入力を求められます。



2. [**イベントID**]フィールドにIDを入力して、[**移動**]をクリックします。
指定されたイベントがレガシーの[イベント再構築]ビューまたは[イベント]ビューで再構築されます。

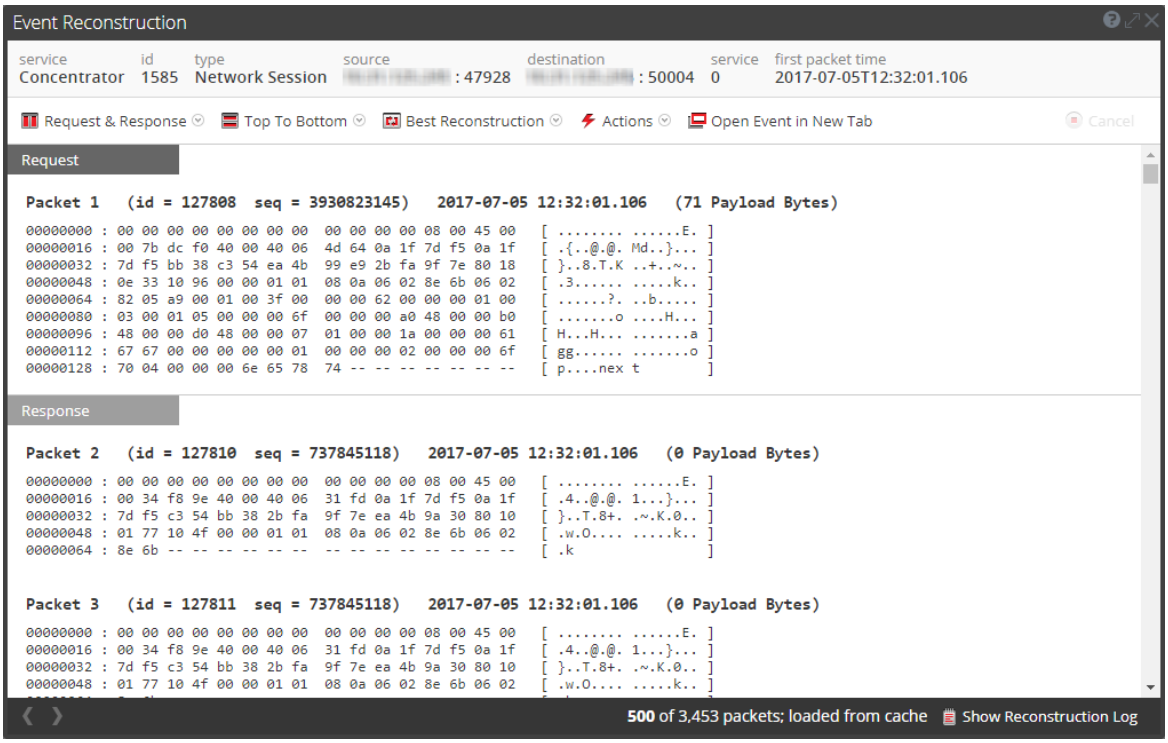
[ナビゲート]ビューでのドリルダウン ポイントからのイベントの再構築

1. [ナビゲート]ビューの値の数(値に続く緑色の数字)をクリックすると、[**イベント**]ビューでドリルダウン ポイントが開きます。
2. すべてのメタ データを表示するには、 + Show Additional Meta をクリックします。
3. [レガシー イベント]ビューでイベント再構築を表示するには、再構築するイベントを選択し、**[アクション]＞[イベントの表示]＞[インライン プレビュー]**を選択します。
同じビューのポップアップ ウィンドウに[イベントの再構築]が表示されます。デフォルトでは、イベントのコンテンツから判断されたイベントに最適な再構築形式か、NetWitness Platformの[デフォルト セッション表示]の設定で選択した再構築形式で表示されます。[イベントの再構築]ツールバーのオプションを使用して、再構築方法の変更、複数の結果の並行表示、イベントのエクスポート、メールの添付ファイルの表示、ファイルの抽出、新しいタブでのイベントの表示を行うことができます。ツールバーのオプションは、再構築中のイベントのタイプによって異なります(ネットワーク イベント、ログ イベント、エンドポイント イベント)。これは、ネットワーク イベントの再構築の例です。



4. 次のイベントの再構築をプレビューするには、再構築の左下隅で をクリックするか、前のイベントの再構築をプレビューするには、 をクリックします。
5. 新しいタブでイベントの再構築を表示するには、次のいずれかを実行します。
   a. 再構築するイベントを[**レガシー イベント**]ビューで選択し、[**アクション**]＞[**イベントの表示**]＞[**新しいタブで開く**]を選択します。
   b. プレビューした再構築の[**イベントの再構築**]ツールバーで、[**イベントを新しいタブで開く**]をクリックします。

[イベントの再構築]オプションが新しいタブに開かれます。



セッションを左右/上下に並べて表示

イベントのリクエストやレスポンスの表示方法を選択するには、次の手順を実行します。

1. [**イベントの再構築**]ツールバーで、[**セッションを上下に並べて表示**]または[**セッションを左右に並べて表示**]をクリックします。
2. ドロップダウン メニューで、イベントで表示する情報([**セッションを左右に並べて表示**]または[**セッションを上下に並べて表示**])を選択します。
   選択した情報で、再構築されたイベントが更新されます。

表示するイベント情報の選択

表示するイベント情報を選択するには、次の手順を実行します。

1. [**イベントの再構築**]ツールバーで、[**リクエストとレスポンス**]をクリックします。
2. ドロップダウン メニューで、イベントで表示する情報([**リクエストとレスポンス**]、[**リクエスト**]、[**レスポンス**])を選択します。
   選択した情報で、再構築されたイベントが更新されます。

イベントの再構築のタイプの選択

イベントの再構築のタイプを選択するには、次の手順を実行します。

1. [**イベントの再構築**]ツールバーで[**最適な表示**]をクリックします。
2. ドロップダウン メニューから、表示する再構築のタイプ(**メタ**、**テキスト**、**16進数**、**パケット**、Web、**メール**、**ファイル**) を選択します。
   再構築の表示が選択した再構築タイプで更新されます。

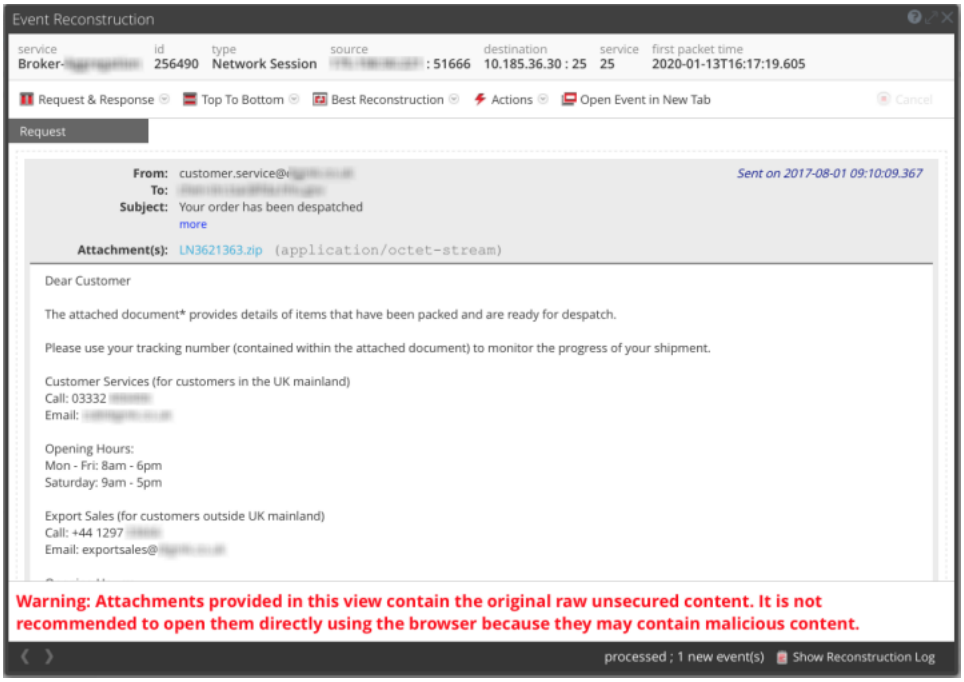
メールの添付ファイルの表示またはダウンロード

ファイルが添付されているメールの再構築を表示するときに、サポートされているファイル タイプを開くか、そのファイルをローカル システムにダウンロードできます。

注意: 添付ファイルを選択するときは気を付けてください。その添付ファイルに関連づけられているアプリケーションがシステムに含まれる場合、またはブラウザでそのファイルを開くことができる場合、それが悪意のある添付ファイルだと、システムに悪影響を及ぼすことがあります。

メールの添付ファイルを表示またはダウンロードするには:

1. [**イベントの再構築**]ツールバーで、[**表示**]ドロップダウンを選択し、[**メールの表示**]を選択します。
   [イベントの再構築]が表示されます。



2. メールの[**イベントの再構築**]セクションで、添付ファイルをクリックします。
   ファイル タイプがブラウザでサポートされている場合は、新しいタブで添付ファイルが開きます。
   ファイル タイプがサポートされていない場合は、添付ファイルをダウンロードできるように[ダウンロード]ダイアログが表示されます。

イベントをPCAPファイルとしてエクスポート

PCAPエクスポート オプションにより、現在の時間範囲のセッションおよびPCAPファイルへのドリルダウン ポイントをダウンロードできます。イベントをPCAPファイルとしてエクスポートするには、次の手順を実行します。

1. [**イベントの再構築**]ツールバーで、[**アクション**]をクリックします。
2. [**PCAPのエクスポート**]をクリックします。
3. 確認ダイアログが表示されます。
4. [**OK**]をクリックします。
   ジョブのスケジュールが設定され、完了すると、PCAPが生成されます。PCAPは、[プロファイル]＞[ジョブ]タブでダウンロードできます。

再構築されたイベントからのファイルの抽出

イベントに関連するファイルは、[ファイルの抽出]オプションで抽出し、ダウンロードすることができます。ファイルを抽出するには、次の手順を実行します。

1. [**イベントの再構築**]ツールバーで、[**アクション**]をクリックします。
2. [**ファイルの抽出**]をクリックします。
   [ファイルの抽出]ダイアログが表示されます。
3. 抽出するファイルのタイプを選択し、[**OK**]をクリックします。
4. ジョブのスケジュールが設定され、完了すると、選択したタイプのファイルが生成されます。このファイルは、[プロファイル]＞[ジョブ]タブでダウンロードできます。

結果の追加のコンテキストを検索

Context Hubは、複数の構成可能なデータ ソースからのエンティティに関するデータを統合する、一元化されたサービスです。このデータにより、特定のクエリで即座に得られる結果を超えて、追加のコンテキストで調査を拡張することができます。たとえば、Context Hubにより、指定したエンティティがインシデント、アラート、フィード、コミュニティ インテリジェンスの関連資料で言及されているかどうかを確認することができます。

コンテキスト情報の表示を有効にするには、管理者がContext HubサービスをRSA NetWitness Platformに追加し、『*Context Hub構成ガイド*』の説明に従って、Context Hubサービスのデータ ソースを構成する必要があります。『*システム セキュリティとユーザ管理ガイド*』の「ロールの権限」および「ロールと権限によるユーザの管理」の説明に従い、アナリストのロールで、`Context Lookup`権限を許可する必要があります。

Context Hubサービスが有効化され、構成されている場合、NetWitness Platformは、[ナビゲーション]ビュー、[イベント]ビュー、[レガシー イベント]ビューで直接NetWitness Respond、カスタム リスト、およびNetWitness Endpointからのエンリッチメント データを提供します。[調査]ビューではエンリッチメント データを使用できるメタ値はすぐにわかるようハイライト表示され、その値をクリックしてコンテキスト情報やインテリジェンスを検索できます。Context Hubでイベントに関連付けられた要素に関する詳細とインテリジェンスを検索することができます。これらの構成要素またはエンティティは、IPアドレス、ユーザ名、ホスト名、ドメイン名、ファイル名、ファイル ハッシュなどの識別子です。RSA NetWitness Endpointなどの構成されたソースからのデータは、何が起こっているのかを理解するために役立ちます。

さらに、Context Hubエンリッチメントのリストの追加と値の表示のほか、リストの表示、既存のリスト内のメタ値の編集、新しいリストの作成を実行できます。メタ値をリストに追加すると、コンテキスト ルックアップ オプションを使用してそのメタ値を調査できます。

注： バージョン11.2以前では、追加のコンテキストの検索を[ナビゲート]ビューまたは[レガシーイベント]ビューで行えますが、[イベント分析]ビューでは行えません。

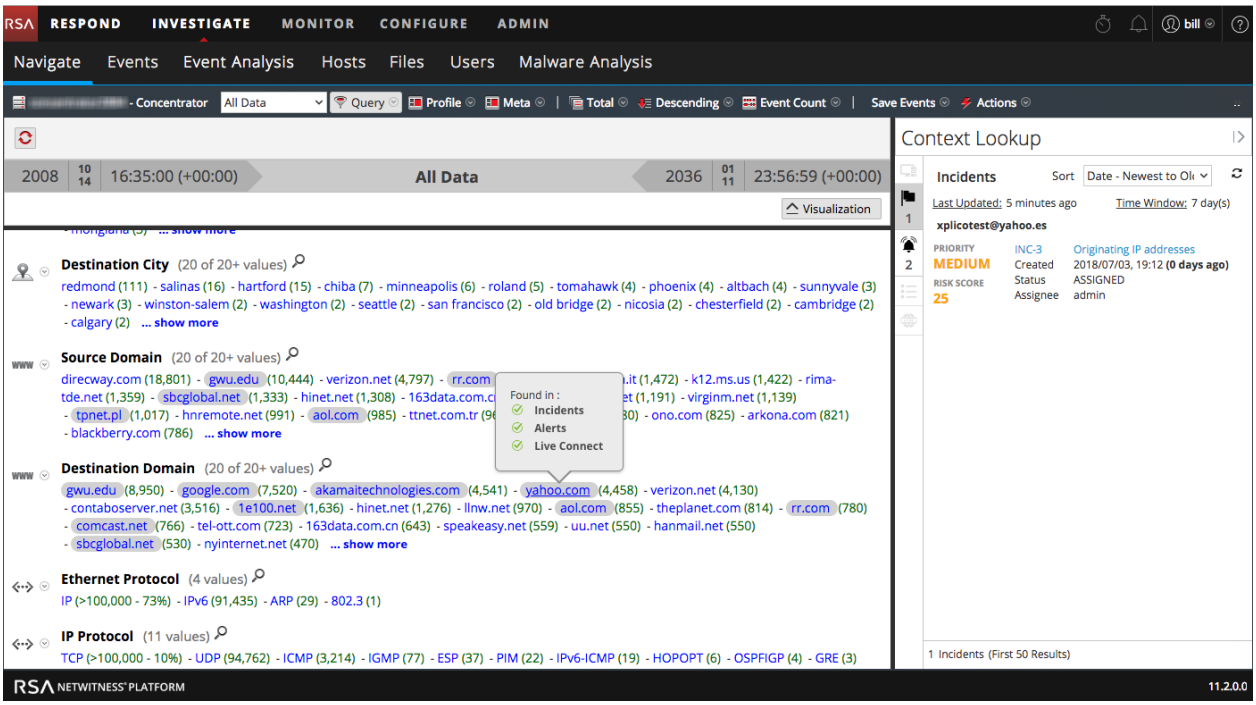
アナリストが[調査]でリストを管理するためには、管理者が次のタスクを完了する必要があります。

- Context Hubサービスを有効にします。
- [調査]ビューからコンテキスト ルックアップを実行するユーザに、`Manage List from Investigation`権限を含んだアナリストのロールを割り当てます。
- 「*システム セキュリティとユーザ管理ガイド*」にある「ロールの権限」と「ロールと権限によるユーザの管理」の説明に従って適切なロールと権限を設定します。

[コンテキスト ルックアップ]パネルを開く

[コンテキスト検索]パネルで、個々のデータ ソースを表示してさらに調べることができます。各データ ソースについて表示される情報の詳細については、「[コンテキスト ルックアップ]パネル」を参照してください。

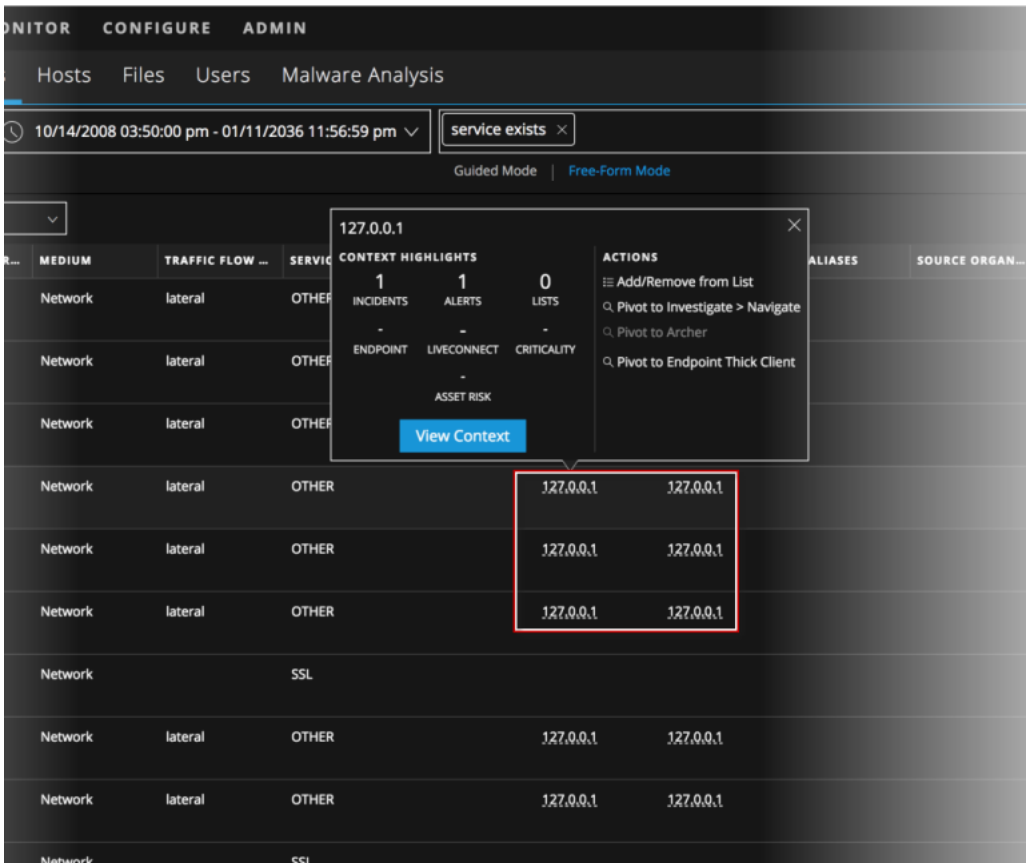
[ナビゲート]ビューと[レガシー イベント]ビューでは、関連づけられたコンテキスト データを持つエンティティが灰色の背景でハイライト表示されます。エンティティにカーソルを合わせると、使用可能なデータのサマリーを示すホバー ボックスが表示されます。エンティティを右クリックすると、Context Hubは構成されたデータ ソースに関連情報を照会し、[コンテキスト検索]パネルがブラウザ ウィンドウの右側から開きます。[コンテキスト検索]パネルには、利用可能になったContext Hubの情報が入力されます。別の検索を実行するには、別のエンティティを右クリックすると、そのエンティティの情報で[コンテキスト検索]パネルが更新されます。



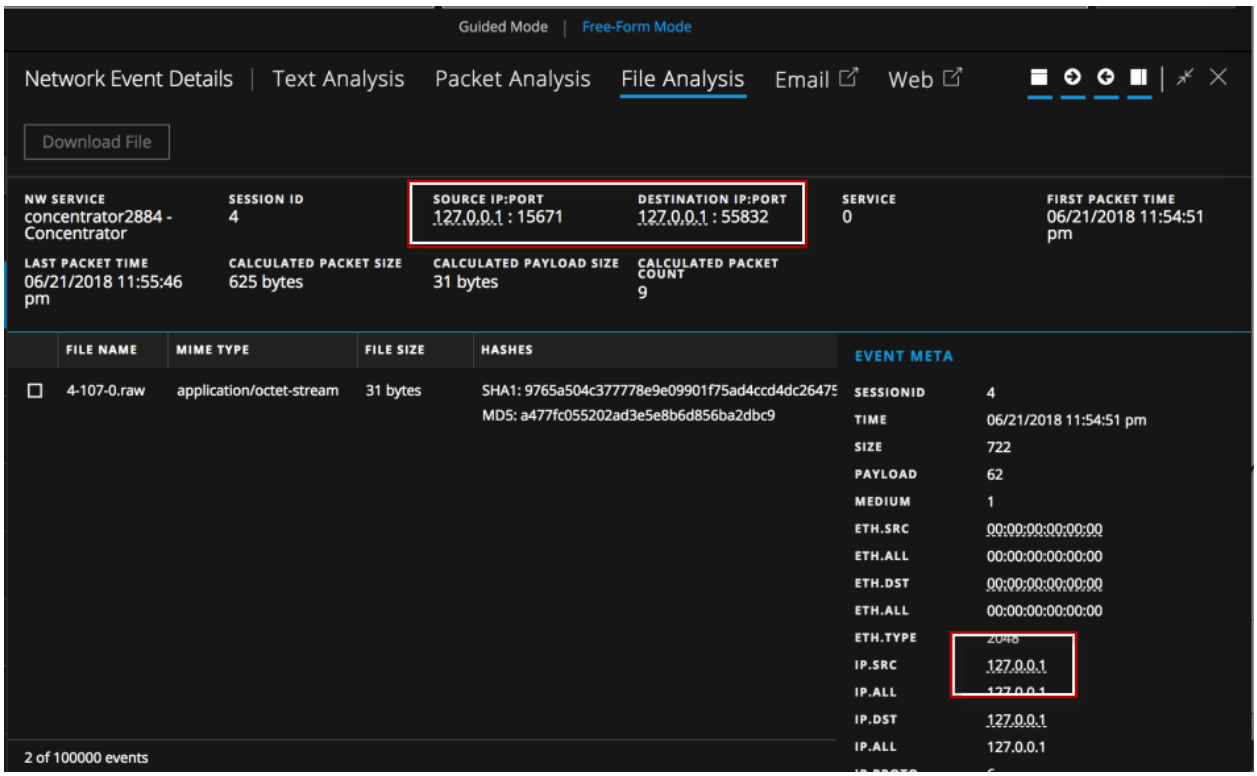
[イベント]ビューでは、下線付きエンティティが[イベント]パネル、イベント ヘッダー、[イベント メタ]パネルに表示されます。エンティティに下線がある場合、NetWitness PlatformがContext Hubにそのエンティティ タイプに関する情報を追加していることを意味します。つまり、Context Hubに、そのエンティティに関する追加情報が存在する可能性があります。

次の図は、コンテキスト ツールチップを開いた[イベント]パネルの下線付きエンティティを示しています。コンテキスト ツールチップには、[コンテキストのハイライト]と[アクション]という2つのセクションがあります。

- [コンテキストのハイライト]セクションの情報は、必要なアクションを判断するのに役立ちます。インシデント、アラート、リスト、エンドポイント、Live Connect、重要度、資産リスクの関連するデータを表示できます。データによっては、これらの項目をクリックして詳細を確認できます。
- [**アクション**]セクションには、使用可能なアクションが表示されます。例では、[リストへの追加/削除]、[[調査]>[ナビゲート]への移行]、[Archerへの移行]、[Endpoint Thick Clientへの移行]の各オプションを使用できます。



次の図は、イベント ヘッダーと[イベント メタ]パネルでの下線付きエンティティを示しています。

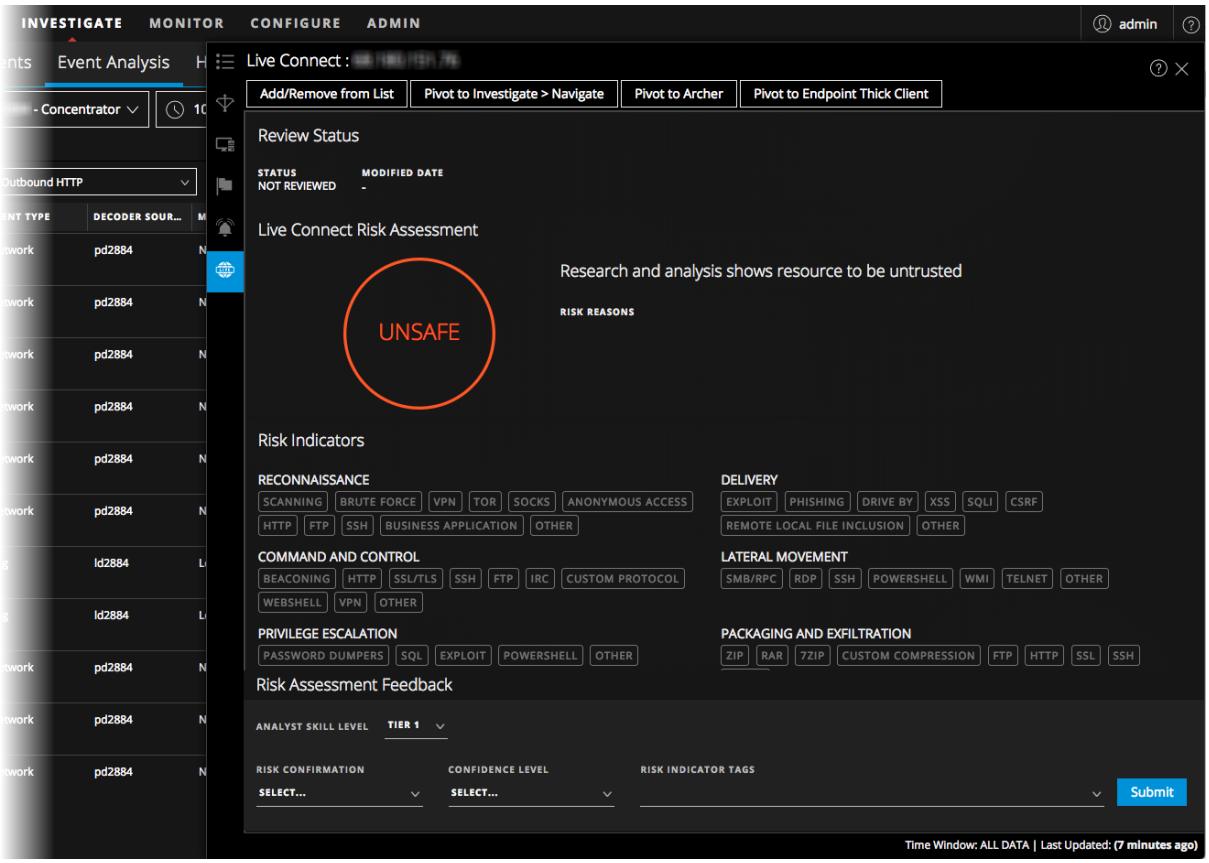


コンテキスト ツールチップの[コンテキストの表示]をクリックすると、Context Hubは構成されたデータ ソースに関連情報を照会し、[コンテキスト検索]パネルがブラウザ ウィンドウの右側から開きます。[コンテキスト検索]パネルには、利用可能になったContext Hubの情報が入力されます。別の検索を実行するには、別のエンティティで[コンテキストの表示]オプションを使用すると、そのエンティティの情報で[コンテキスト ルックアップ]パネルが更新されます。

また、「アクション」セクションで使用可能なアクションを実行することもできます。

「イベント」ビューの[コンテキスト ルックアップ]パネルで情報を表示するには、次の手順を実行します。

1. それぞれのメタ値にカーソルを合わせると、データが使用可能なデータ ソースが表示されます。
   コンテキスト ツールチップには、選択したメタ値に使用できるコンテキスト データのリストが表示されます。
2. コンテキスト ツールチップの[**コンテキストの表示**]をクリックして、[コンテキスト ルックアップ]パネルを開きます。
   ブラウザ ウィンドウの右側から[コンテキスト ルックアップ]パネルが開きます。[コンテキスト検索]パネルには、利用可能になったContext Hubの情報が入力されます。



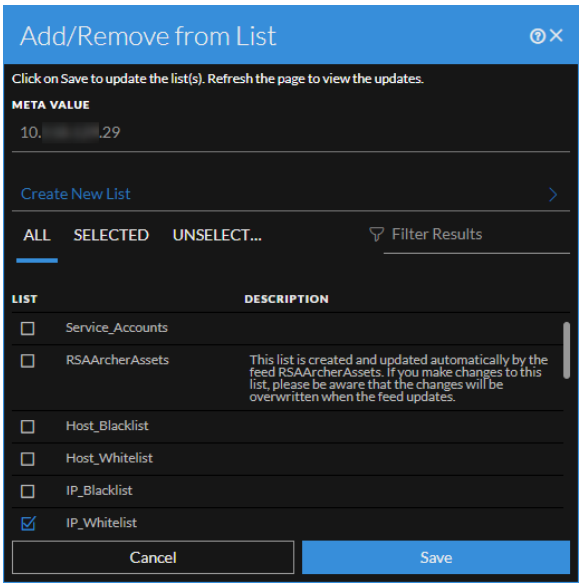
3. エンティティに対してアクションを実行するには、コンテキスト ツールチップで使用可能なアクション([リストへの追加/削除]、[[調査]>[ナビゲート]への移行]、[Archerへの移行]、[Endpoint Thick Clientへの移行]) のいずれかを選択します。詳細については、「[調査]>[ナビゲート]への移行([イベント]ビュー)」、「Archerへの移行([イベント]ビュー)」、「NetWitness Endpoint Thick Clientへの移行([イベント]ビュー)」、「ホワイト リストへのエンティティの追加」を参照してください。

注： Archerデータが使用できない場合、またはArcherデータ ソースが応答しない場合、[Archerへの移行]リンクは無効になります。RSA Archer設定が有効で、正しく設定されていることを確認します。

ホワイト リストへのエンティティの追加

下線付きの任意のエンティティを、コンテキスト ツールチップから、ホワイトリストまたはブラックリストなどのリストに追加できます。たとえば、誤検知を減らすために、下線付きのドメインをホワイトリストに追加して、関連エンティティから除外します。

1. [イベント]パネル、イベント ヘッダー、[イベント メタ]パネルのいずれかで、Context Hubのリストに追加する下線付きのエンティティにマウスを合わせます。
   使用可能なアクションを示すコンテキスト ツールチップが表示されます。
2. ツールチップの[**アクション**]セクションで、[**リストへの追加/削除**]をクリックします。
   [リストへの追加/削除]ダイアログに使用可能なリストが表示されます。



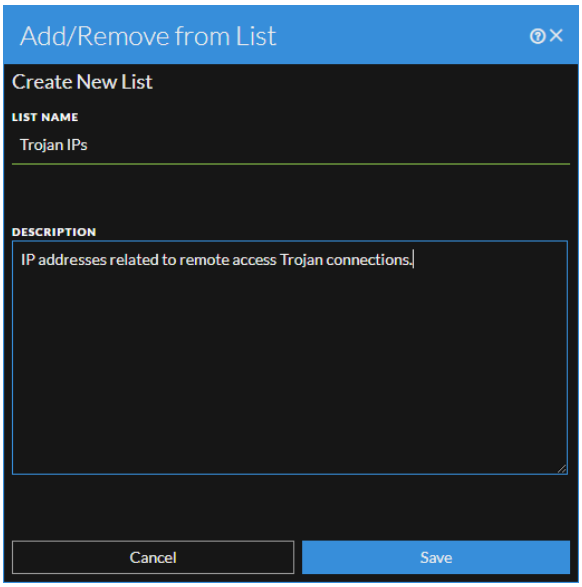
3. 1つ以上のリストを選択し、[**保存**]をクリックします。
   選択したリストにエンティティが追加されます。

リストの作成 ([イベント]ビュー)

[イベント]ビューから、Context Hubのリストを作成できます。エンティティのリストをホワイトリストおよびブラックリストとして使用するだけでなく、エンティティの異常な動作を監視するために使用できます。たとえば、調査中、疑わしいIPアドレスとドメインの可視性を高めるために、これらを2つの別々のリストに追加することができます。1つのリストは、コマンド&コントロールの接続に関連している疑いがあるドメインのリストとし、もう1つのリストは、リモート アクセスのトロイの木馬の接続に関連するIPアドレスのものとします。これらのリストを使用してセキュリティ侵害インジケータを特定できます。

Context Hubのリストを作成するには、次の手順を実行します。

1. [イベント]パネル、イベント ヘッダー、[イベント メタ]パネルのいずれかで、Context Hubのリストに追加する下線付きのエンティティにマウスを合わせます。
   使用可能なアクションを示すコンテキスト ツールチップが表示されます。
2. ツールチップの[**アクション**]セクションで、[**リストへの追加/削除**]をクリックします。
3. [リストへの追加/削除]ダイアログで、[**新しいリストの作成**]をクリックします。



4. リストの固有の[**リスト名**]を入力します。リスト名は大文字と小文字を区別しません。
5. (オプション) リストの[**説明**]を入力します。
   適切な権限を持つアナリストは、他のアナリストに送信してさらに追跡と分析を行うために、CSV形式でリストをエクスポートすることもできます。詳細については、『*Context Hub構成ガイド*』を参照してください。

[調査]>[ナビゲート]への移行([イベント]ビュー)

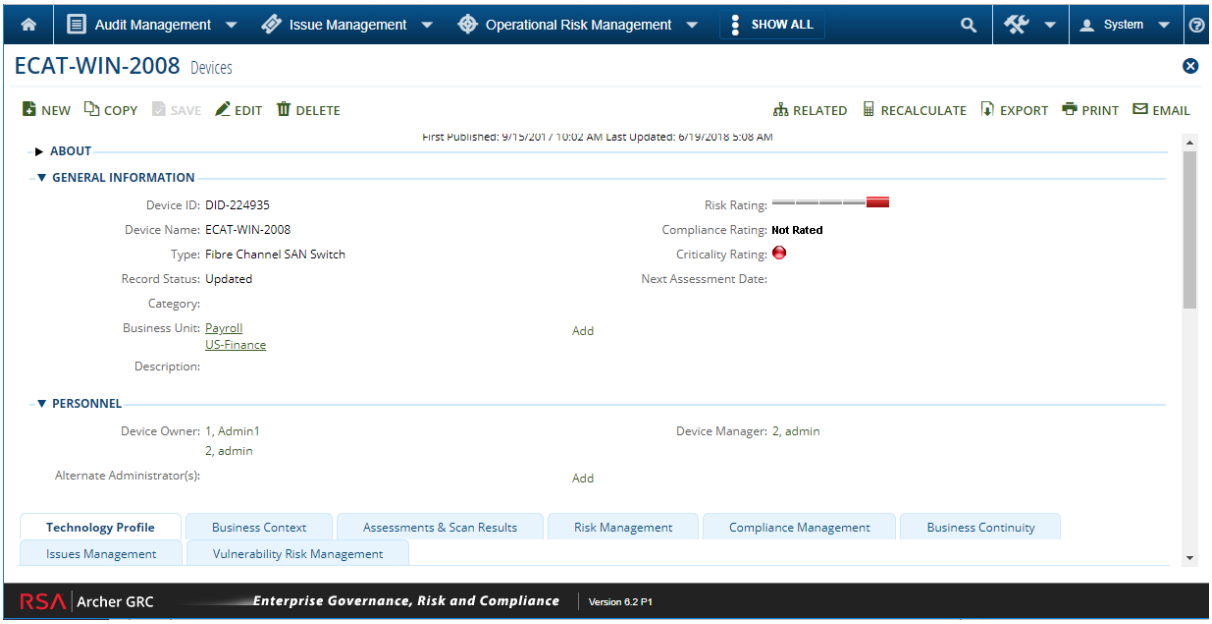
エンティティをより詳細に調査するには、[ナビゲート]ビューを開きます。

1. [イベント]パネル、イベント ヘッダー、[イベント メタ]パネルのいずれかで、下線付きのエンティティの上にマウスを合わせます。
2. ツールチップの[**アクション**]セクションで、[**[調査]>[ナビゲート]への移行**]を選択します。
   [ナビゲート]ビューが開き、より詳細な調査を実行できます。詳細については、「結果セットの絞り込み」を参照してください。

Archerへの移行([イベント]ビュー)

RSA Archer® Cyber Incident & Breach Responseでデバイスの詳細を表示するには、デバイスの詳細ページに移行できます。この情報は、IPアドレス、ホスト、およびMACアドレスに対してのみ表示されます。

1. [イベント] パネル、イベント ヘッダー、[イベント メタ] パネルのいずれかで、下線付きのエンティティ(IPアドレス、ホスト、MACアドレス) の上にマウスを合わせます。
2. ツールチップの[**アクション**] セクションで、[**Archerへの移行**] を選択します。
3. アプリケーションにログインしている場合は、「**RSA Archerサイバー インシデントおよび侵害対応**」が開き、それ以外の場合はログイン画面が表示されます。



注: Archerデータが使用できない場合、またはArcherデータソースが応答しない場合、[Archerへの移行] リンクは無効になります。RSA Archer設定が有効で、正しく設定されていることを確認します。

詳細については、『*Archerとの統合ガイド*』を参照してください。

NetWitness Endpoint Thick Clientへの移行([イベント] ビュー)

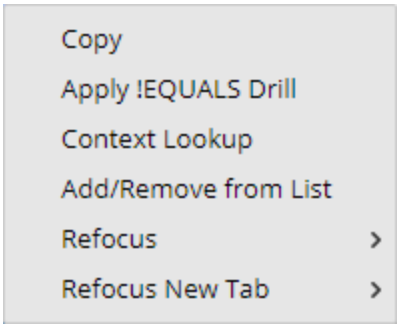
NetWitness Endpointシック クライアント アプリケーションがインストールされている場合は、コンテキスト ツールチップから起動できます。そこから、疑わしいIPアドレス、ホスト、MACアドレスをさらに調査できます。

1. [イベント] パネル、イベント ヘッダー、[イベント メタ] パネルのいずれかで、下線付きのエンティティの上にマウスを合わせます。
2. ツールチップの[**アクション**] セクションで、[**Endpoint Thick Clientへの移行**] を選択します。NetWitness Endpoint Thick Clientアプリケーションが、Webブラウザの外で開きます。

シック クライアントの詳細については、『*NetWitness Endpointユーザ ガイド*』を参照してください。

[ナビゲート]ビューまたは[レガシー イベント]ビューでの[コンテキスト ルックアップ]パネルの表示

1. それぞれのメタ値にカーソルを合わせると、データが使用可能なデータ ソースが表示されます。
   ホバー ボックスには、メタ データで使用可能なコンテキスト データを持つデータ ソースのリストが表示されます。データ ソースとして使用できるのは、NetWitness Endpoint、インシデント、アラート、ホスト、ファイル、フィード、Live Connectです。
2. メタ値を右クリックして、ドロップダウン メニューで[**コンテキスト ルックアップ**]をクリックして[コンテキスト ルックアップ]パネルを開きます。

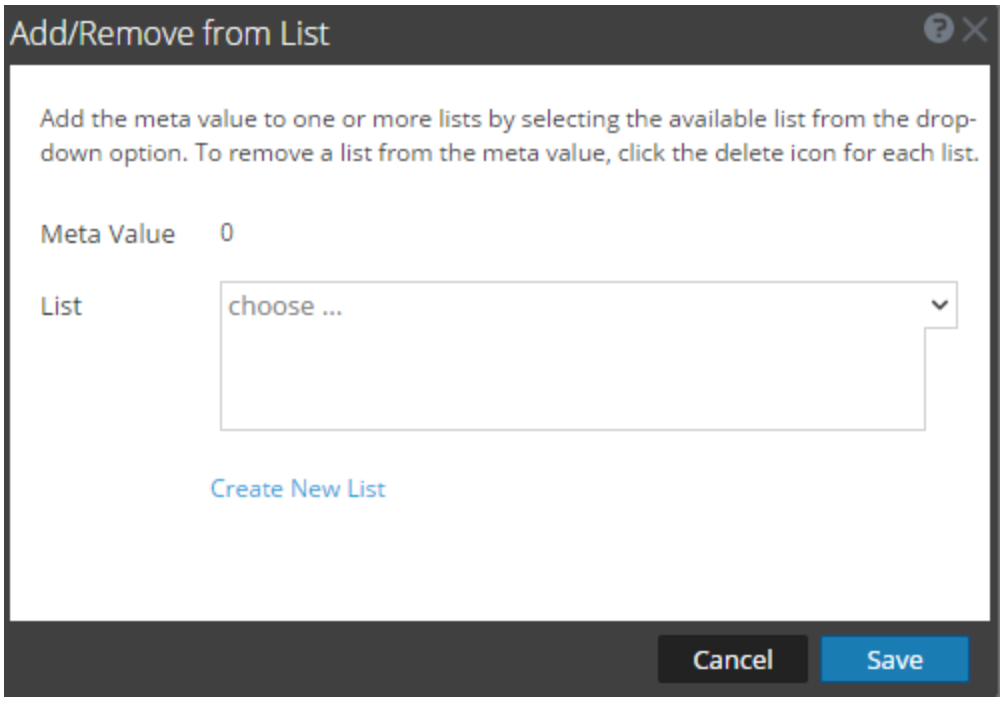
   

   ブラウザ ウィンドウの右側から[コンテキスト ルックアップ]パネルが開きます。[コンテキスト検索]パネルには、利用可能になったContext Hubの情報が入力されます。
3. [コンテキスト ルックアップ]パネルからアクションを実行するには、IPアドレスなどのエンティティを右クリックします。
   使用可能なオプションは、[リンクを新しいタブで開く]、[Investigateでクエリ]、[リンクのコピー]、[ペースト]、[Googleルックアップ]、[ウイルス合計ルックアップ]、[Endpointでクエリ]です。
4. [コンテキスト ルックアップ]パネルを閉じるには、パネルの✕をクリックします。

既存のリストへのメタ値の追加([ナビゲート]ビューと[レガシー イベント]ビュー)

Context Hubの既存のリストにメタ値を追加するには、次の手順を実行します。

1. [**ナビゲート**]ビューまたは[**レガシー イベント**]ビューでサービスを調査するとき、メタ値(たとえば、[Source IP]、[Destination IP]、または[Username]の値)を右クリックし、コンテキスト メニューから[**リストへの追加/削除**]を選択します。
   [リストへの追加/削除]ダイアログが表示されます。



2. [**リスト**]フィールドで、メタ値を追加するリストをドロップダウンから選択します。複数のリストを選択可能です。
3. [**保存**]をクリックします。
   選択したリストにメタ値が追加されます。

Context Hubリストからのメタ値の削除([ナビゲート]ビューと[レガシー イベント]ビュー)

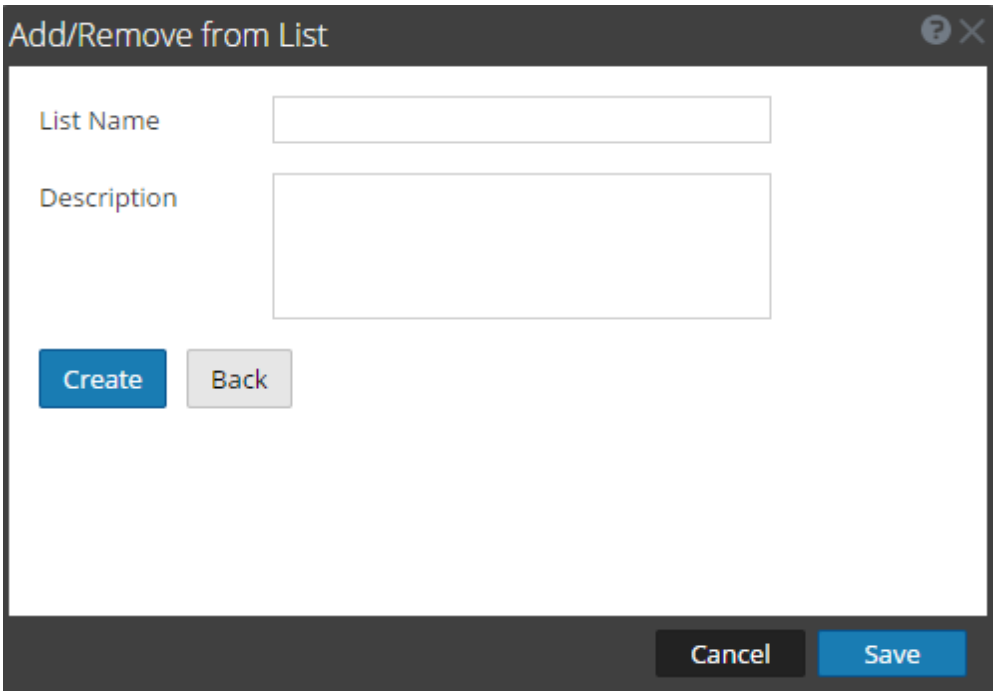
リストからメタ値を削除するには、次の手順を実行します。

1. [**リストへの追加/削除**]ダイアログの[**リスト**]フィールドで、メタ値を含むリストを表示します。
2. メタ値を削除したいリストの削除アイコン(x) をクリックします。
3. [**保存**]をクリックします。
   削除したリストから、メタ値が削除されます。

新しいリストの作成([ナビゲート]ビューと[レガシー イベント]ビュー)

[調査]でContext Hubリストを作成するには、次の手順を実行します。

1. [**リストへの追加/削除**]ダイアログで、[**新しいリストの作成**]をクリックします。



2. [**名前**]フィールドに、リストの一意の名前を入力します。
3. [**説明**]フィールドに、リストの説明を入力します。
4. [**作成**]をクリックしてリストを作成します。
5. [**保存**]をクリックして、作成したリストにメタ値を追加します。
これらのリストは、コンテキスト情報を取得するためのデータ ソースと見なされます。

メタ キーのルックアップの起動

[ナビゲート]ビュー、[イベント]ビュー、または[レガシー イベント]ビューで興味のあるデータが見つかったら、NetWitness EndpointやRSA Liveへの内部ルックアップを実行したり、SANS IP Historyや ThreatExpert検索などのコミュニティ リソースでメタ値の外部ルックアップを実行することができます。

アナリストは、外部ルックアップを使用して、調査の時間を短縮できます。外部ルックアップを使用するには、次のいずれかのメタ キーを右クリックします。IPアドレス(`ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip`)、`host (alias-host、, domain.dst)`、および`client, ip`および`host`の各メタ キーについては、NetWitness Platformに次の検索機能が組み込まれています。

- Google Malware : Google Malware検索を新しいタブで開きます。
- SANS IP History : SANS IP History検索を新しいタブで開きます。
- McAfee SiteAdvisor : McAfee SiteAdvisor検索を新しいタブで開きます。
- Endpoint Thick Client Lookup : NetWitness Endpoint Thick Client検索を新しいタブで開きます。
- BFK Passive DNS Collection : BFK Passive DNS Collection検索を新しいタブで開きます。
- CentralOps Whois(IPおよびホスト名検索) : CentralOps Whois(IPおよびホスト名検索を新しいタブで開きます。
- Malwaredomainlist.com検索 : Malwaredomainlist.com検索を新しいタブで開きます。
- Robtex IP検索 : Robtex IP検索を新しいタブで開きます。
- ThreatExpert検索 : ThreatExpert検索を新しいタブで開きます。
- IPVoid検索 : UrlVoid検索を新しいタブで開きます。

`file-hash`および`alias-host`の各メタ キーで外部ルックアップからGoogleを選択すると、Google検索が新しいタブで開きます。

`client`メタ キーでは、ブラウザと同じマシンにEndpoint Thick Clientがインストールされている場合、NetWitness Endpointルックアップ オプションによってEndpoint Thick Clientが新しいタブで開きます。

管理者は、外部ルックアップやその他のカスタム アクションを追加できます(「*システム構成ガイド*」の「コンテキスト メニューのカスタム アクションの追加」を参照してください)。

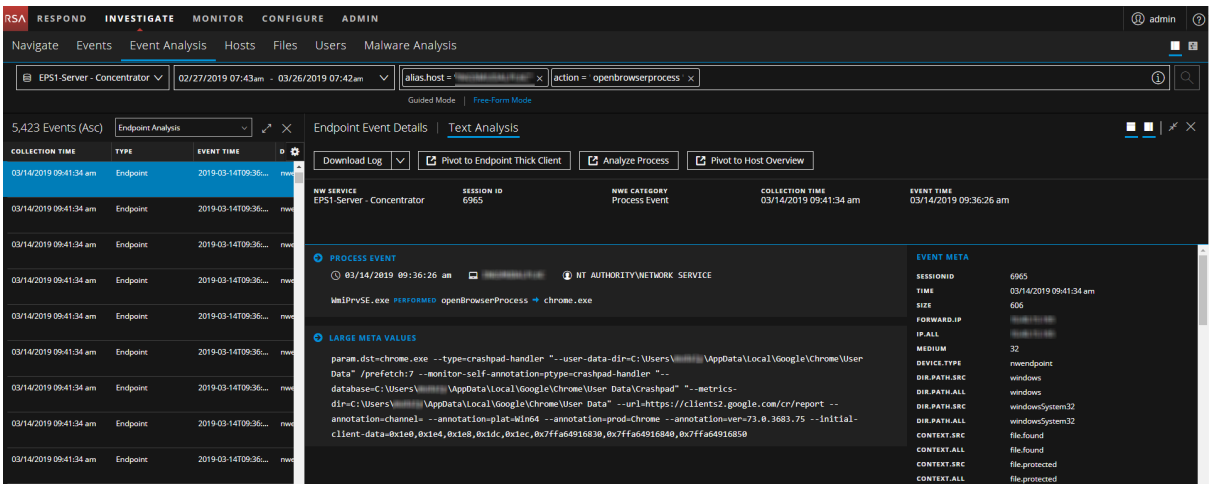
[イベント]ビューでのEndpoint Thick Clientルックアップの起動

[テキスト]パネルでエンドポイント イベントを表示しているときに、同じイベントを分析するためにNetWitness Endpointに移行できます。

> **注 :** バージョン4.4.0.xのNetWitness Endpoint(NWE) Thick Clientを同じサーバにインストールする必要があります。NWEメタ キーがLog Decoderの`table-map.xml`ファイル内に存在する必要があります。また、NWEメタ キーが`index-concentrator-custom.xml`ファイル内に存在する必要があります。NWE Thick Clientは、Windows専用のアプリケーションです。完全なセットアップ手順は、バージョン 4.4の『*NetWitness Endpointユーザ ガイド*』を参照してください。

NetWitness Endpointでイベントを開くには、次の手順を実行します。

1. [ナビゲート]ビューを開き、次の手順を実行します。
   a. [**クエリ**]ドロップダウンで、[**詳細**]を選択して、次のクエリのいずれかを入力します。
      `nwe.callback_id exists` または `device.type='nwendpoint'`
      エンドポイント データが[値]パネルに表示されます。
   b. イベントを右クリックし、メニューで[**イベント**]を選択します。
2. (バージョン11.1以降) [**調査**]>[**イベント**]に移動します。[**クエリ**]ドロップダウンで、[**詳細**]を選択して、次のクエリのいずれかを入力します。`nwe.callback_id exists` または `device.type='nwendpoint'`
   エンドポイント データが[値]パネルに表示されます。
3. イベントを選択します。
   [イベント]ビューが開き、選択したイベントが[テキスト]ビューに表示されます。



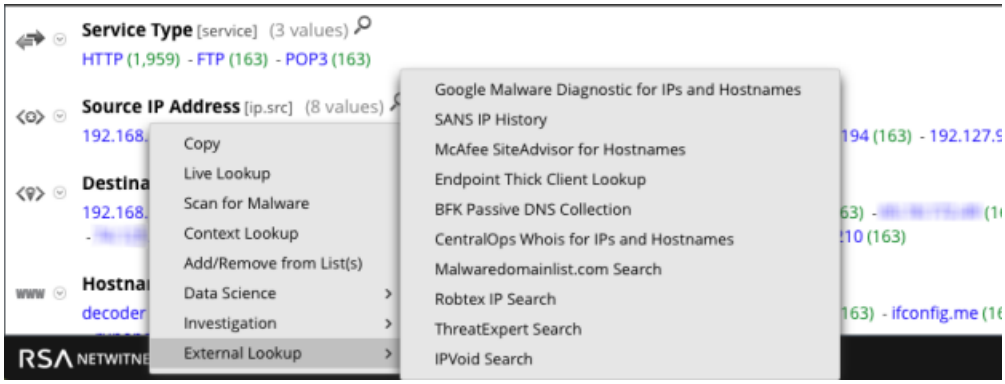
4. イベント ヘッダーで、[**エンドポイントへの移行**]をクリックします。
   新しいブラウザ タブでURL `ecatui://<id>`が開き、NWE Thick Clientが起動されます。
   NetWitness Endpoint Thick Clientがインストールされていない場合は、データが表示されず、次のメッセージが表示されます。`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`

[ナビゲート]ビューでのEndpoint Thick Clientルックアップの起動

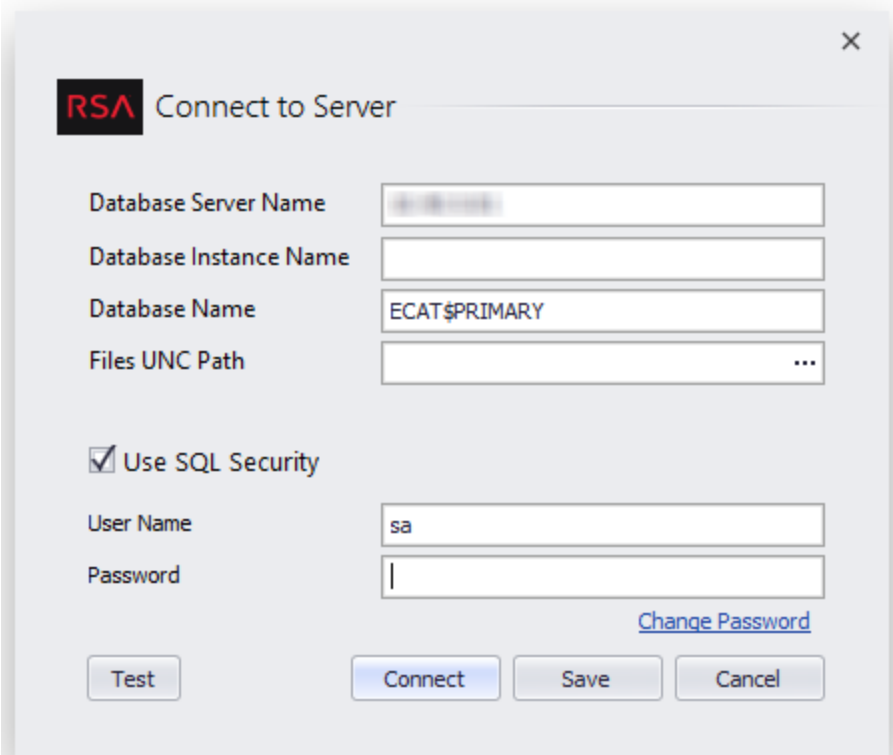
[ナビゲート]ビューからデータのEndpoint Thick Clientルックアップ機能を起動する方法:

1. 次のいずれかのメタ キーのメタ値を右クリックします。`ip-src`, `ip-dst`、`ipv6-src`、`ipv6-dst`、`orig_ip`、`alias-host`、`domain.dst`、または`client`.

2. コンテキスト メニューで[**外部 ルックアップ**]を選択します。
外部 ルックアップ オプションのサブメニューが表示されます。

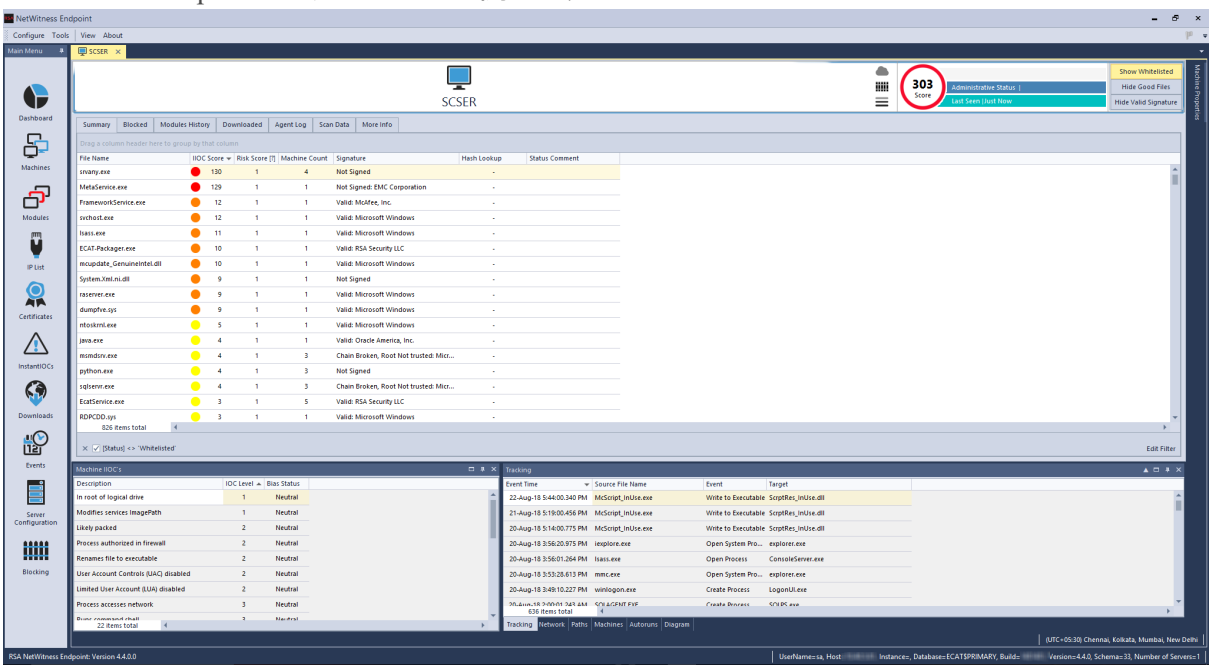


3. [**Endpoint Thick Client ルックアップ**]を選択します。
[サーバに接続]ダイアログが表示されます。



4. Endpoint Thick Clientへのログインに必要なユーザ名とパスワードを入力して、[**接続**]をクリックします。

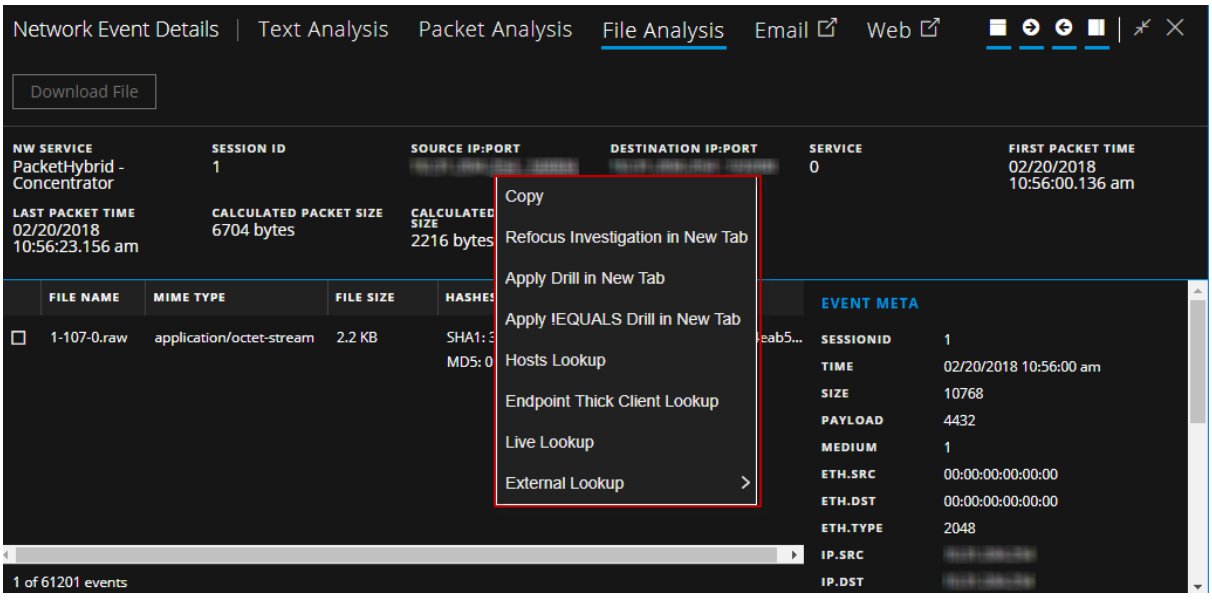
NetWitness Endpointでドリル ポイントが開きます。



イベントでのメタ値のルックアップの実行

[イベント]ビューでは、特定のメタ値を右クリックして、ドロップダウン メニューのオプションを使用することにより、イベント内のメタ値をさらに調査することができます。すべてのフィールドに右クリック アクションがあるわけではありません。内部ルックアップと外部ルックアップを実行するには、次の手順を実行します。

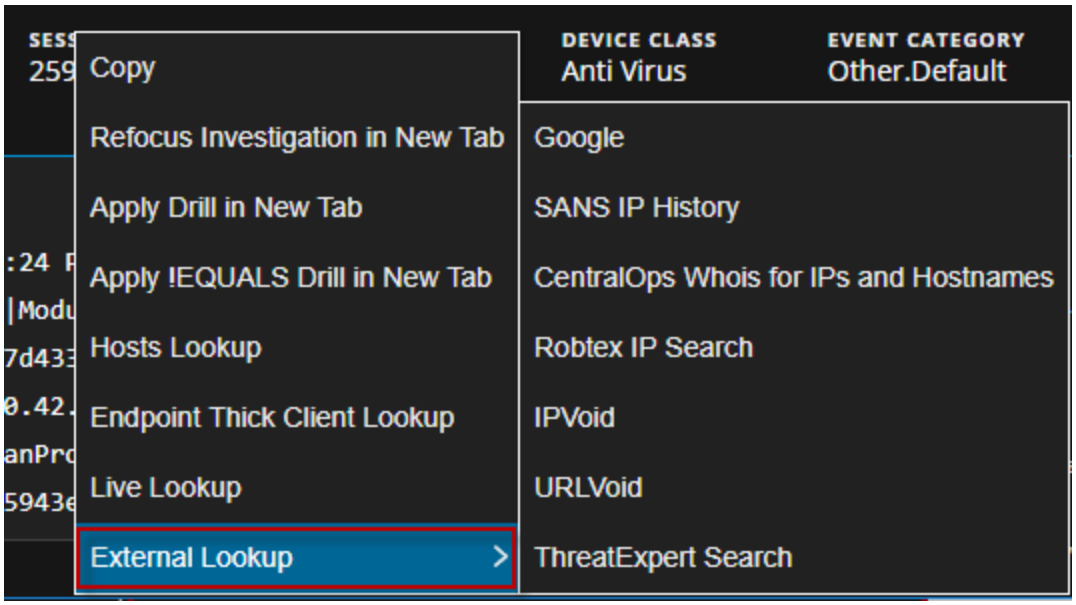
1. [イベント分]ビューで、イベント リスト、[イベント メタ]パネル、またはイベント ヘッダー内のメタ値を右クリックします。一部のメタ値にドロップダウン メニューがあります。



2. 次の内部ルックアップのいずれかを選択します。

- **コピー**: メタ値をクリップボードにコピーします。
- **新しいタブで再フォーカスして調査**: 新しいタブで、選択したメタ値に焦点を当てた別の調査を起動します。
- **新しいタブでドリルダウン**: ドリルダウンを適用して、新しいタブで起動し、[ナビゲート]ビュー内のデータをドリルダウンします。
- **新しいタブで!EQUALSドリルダウン**: (!EQUALS) をメタに適用して、新しいタブを起動すると、結果からメタ値が効率的に除外されます。
- **ホスト ルックアップ**: [調査]>[ホスト]ビューで値を検索します。
- **Endpoint Thick Clientルックアップ**: Endpoint Thick Clientでメタ値を分析します(Endpointエージェントがインストールされたクライアントの場合) 。
- **Liveルックアップ**: さらに分析するためにLiveでメタ値を検索します。

3. 外部ルックアップの場合は、メタ値にポインタを合わせて、右クリックし、[**外部ルックアップ**]を選択します。



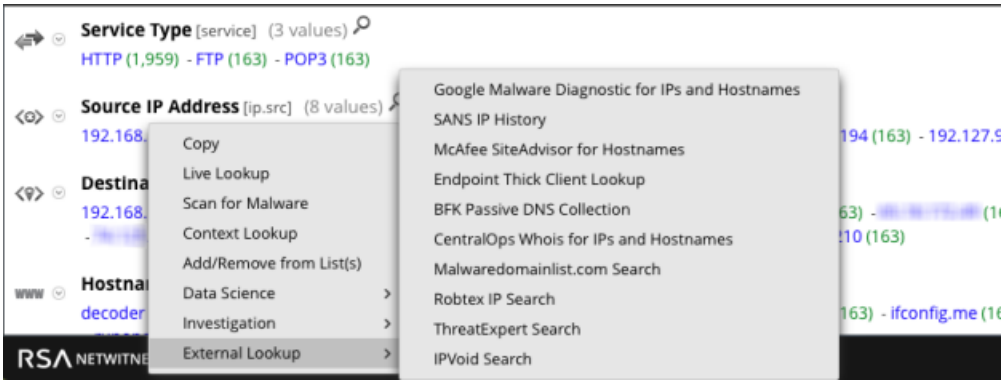
4. サブメニューで、使用可能な外部ルックアップのいずれかを選択します。
   - **Google**: Google.comでメタ値を検索します
   - **SANS IP History**: SANS IP Historyでメタ値を検索します(domain = http://isc.sans.org/ipinfo.html?ip=ipaddress)
   - **CentralOps Whois(IPおよびホスト名検索)** : CentralOps Whois(IPおよびホスト名検索) でメタ値を検索します(domain = http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true&net_whois=true)
   - **Robtex IP Search**: Robtext IP Searchでメタ値を検索します(domain = https://www.robtex.com/cidr/domain.ipaddress)
   - **IPVoid**: IPVoidでメタ値を検索します(domain = http://www.ipvoid.com/scan/domain/)
   - **URLVoid**: URLVoidでメタ値を検索します(domain = http://www.urlvoid.com/scan/ipaddress/)

- **ThreatExpert検索** : ThreatExpert検索でIPメタ値を検索します(domain = http://www.threatexpert.com/reports.aspx?find=IP address)

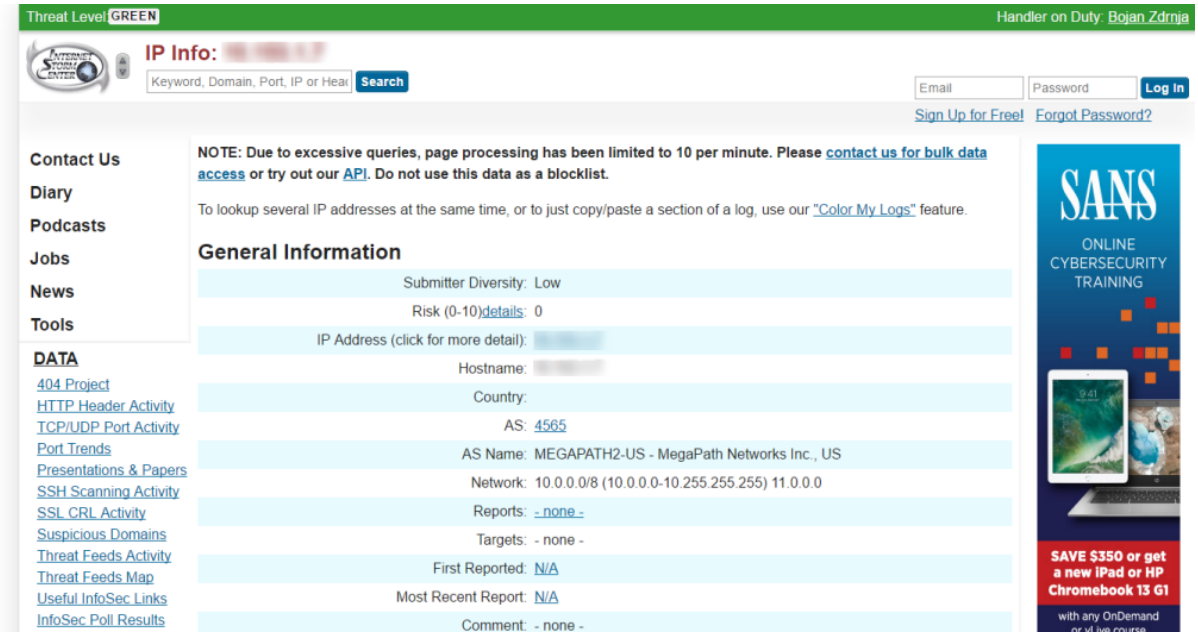
[ナビゲート]ビューからのその他の外部ルックアップの起動

[ナビゲート]ビューからデータの外部ルックアップ(NetWitness Endpoint Thick Clientルックアップ以外)を起動するには、次の手順を実行します。

1. 次のいずれかのメタ キーのメタ値を右クリックします。ip-src、ip-dst、ipv6-src、ipv6-dst、orig_ip、alias-host、domain.dst、またはclient.
2. コンテキスト メニューで[**外部ルックアップ**]を選択します。
   外部ルックアップ オプションのサブメニューが表示されます。



3. いずれかのルックアップ オプションを選択します。
   選択したメタ値が指定された検索機能で開きます。たとえば、SANS IP Historyを選択した場合は、ドリルダウン ポイントの情報がSANS Internet Storm Centerに表示されます。



[ナビゲート]ビューからのMalware Analysisスキャンの起動

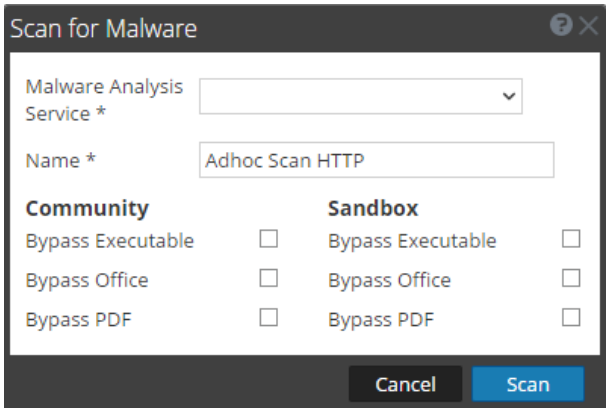
調査においてアナリストは、サービスとメタ値を選択し、コンテキスト メニューからオプションを選択することによって、オン デマンドMalware Analysisスキャンを開始できます。スキャンが完了すると、スキャンされたデータをMalware Analysisから確認できます。

[調査]>[ナビゲート]ビューからデータのMalware Analysisスキャンを起動するには、次の手順を実行します。

1. メタ値(OTHER、DNS、FTPなど)を右クリックして、コンテキスト メニューで[**マルウェアのスキャン**]を選択します。

   [マルウェアのスキャン]ダイアログが開き、オン デマンド スキャンの推奨名が表示されます。サービスは選択されていません。

2. [マルウェアのスキャン]ダイアログで、スキャンを実行するサービスを選択し、名前を編集して、[コミュニティ]と[サンドボックス]の下からバイパスするファイルのタイプを選択します。

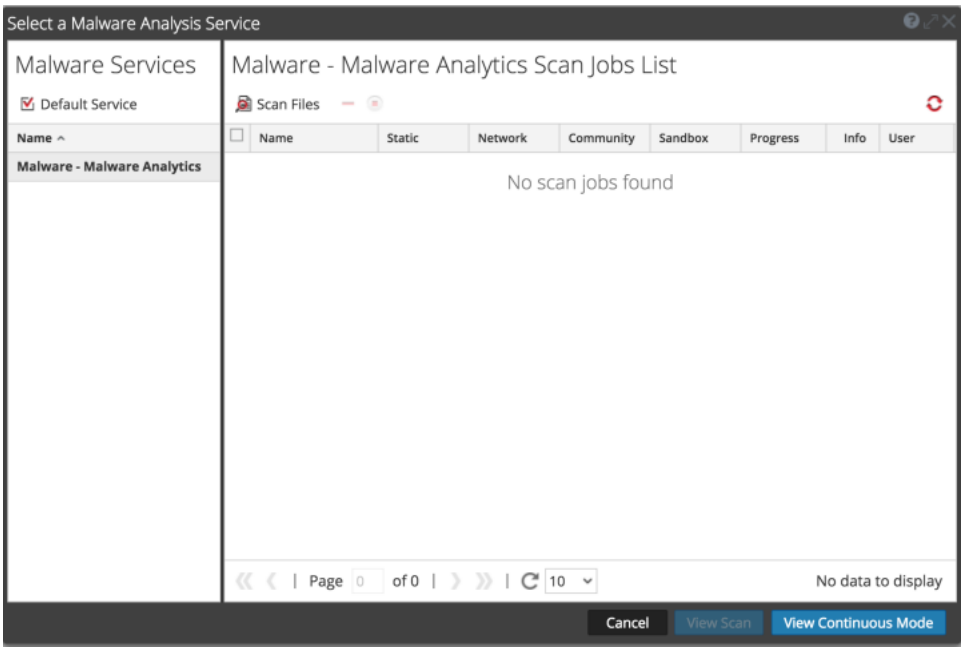


3. [**スキャン**]をクリックします。

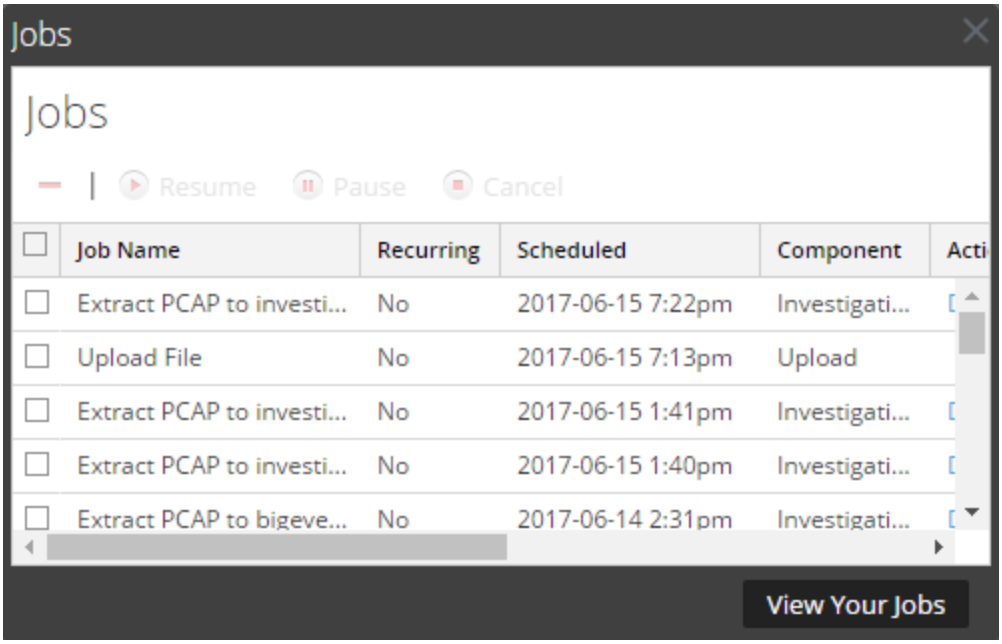
   スキャン リクエストが[スキャン ジョブ リスト]ダッシュレットとジョブ トレイに追加されます。このダイアログのバイパス設定は、Malware Analysisの基本構成のデフォルト設定を上書きします。

4. ジョブを表示するには、以下のいずれかを実行します。

   a. [マルウェア分析]ビューまたはUnifiedダッシュボードの[スキャン ジョブ リスト]に移動します。スキャンをダブル クリックして表示します。



b. ジョブ トレイのジョブを表 示 するには、NetWitness Platformツールバーで  をクリックします。ジョブが完 了したら、該 当 するジョブの[**表 示**]リンクをクリックします。



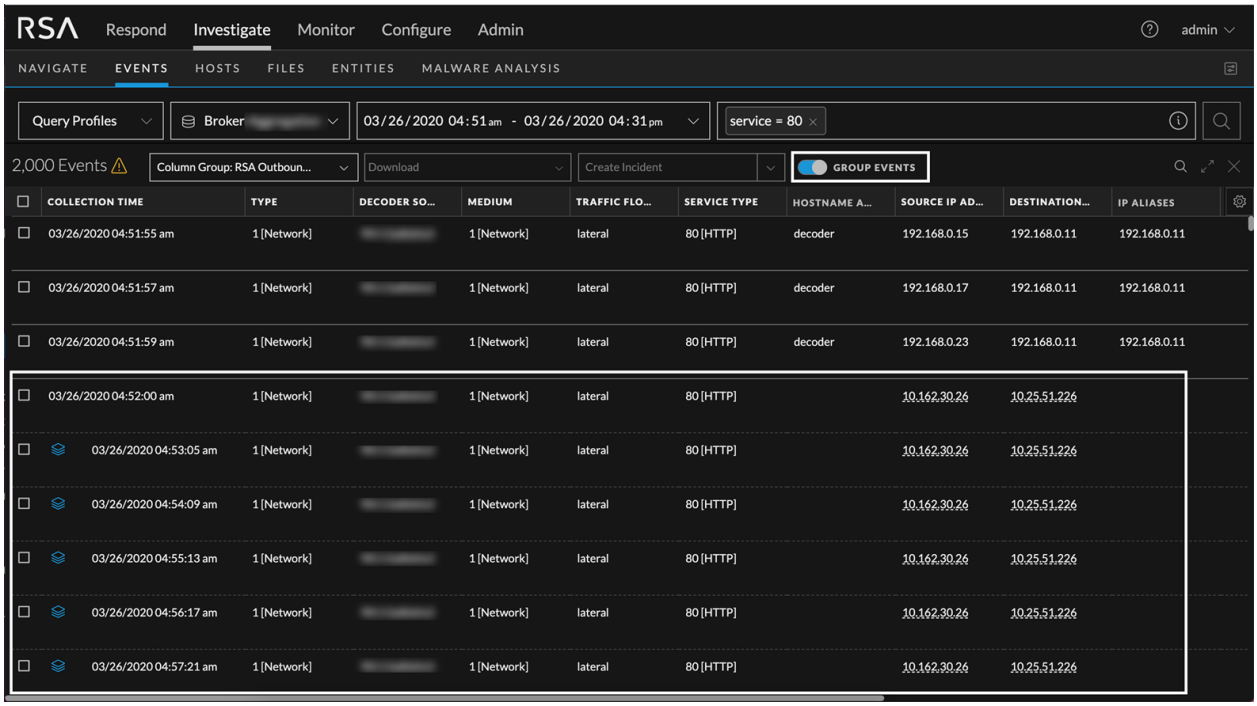
選 択されたスキャンの[イベントのサマリー]が表 示されます。また、このスキャンは、[調 査]>[マルウェア分 析]タブを開いたときの[Malware Analysisサービスの選 択]ダイアログで、[スキャンの選 択]リストに追 加され、そこから選 択して開くことができます。

[イベント]ビューと[レガシー イベント]ビューでの分 割 および関 連 セッションからのイベント のグループ化

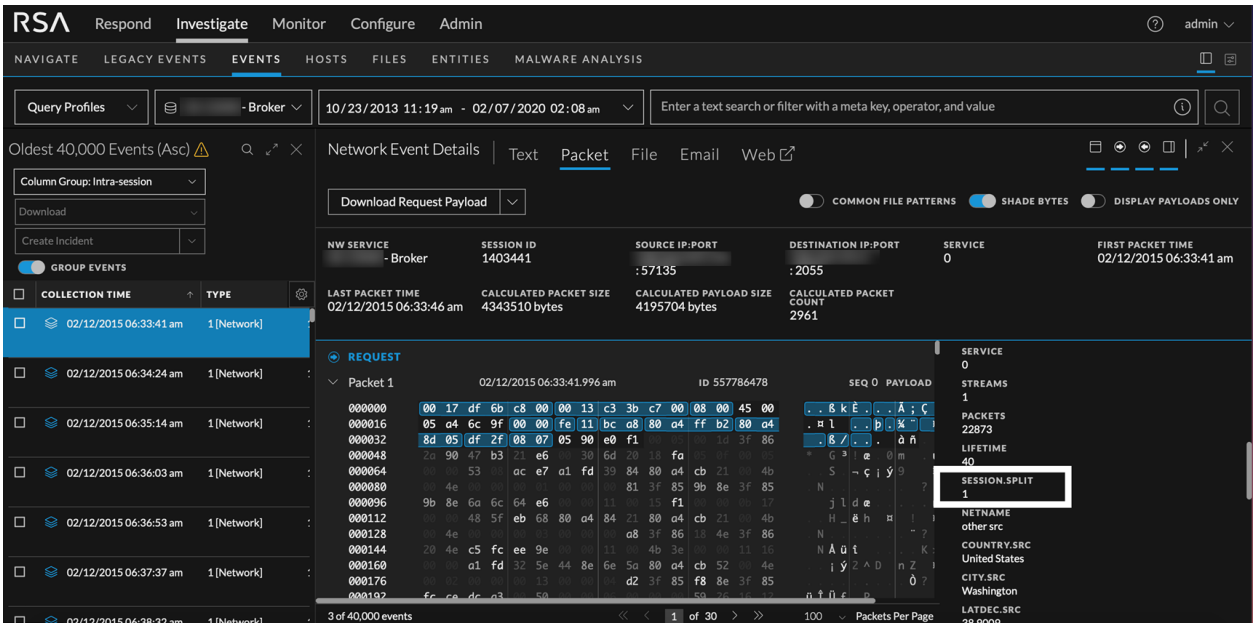
[イベント]ビューのイベント リストには、分 割 セッションと関 連 セッションからのイベントが、解 析 された順 序 で表 示 されるため、常 に一 緒 に表 示 されるとは限 りません。バージョン11.4.1以 降 では、[イベントのグループ化]オプションを使 用 して、収 集 したデータの関 係 をより簡 単 に検 出 できるように、イベントの表 示 順 を変 更 できます。イベントがグループ化 されている場 合 、最 初 のイベントは先 行 イベントと呼 ばれます。

ユーザ インタフェースは、グループ化 されたイベントを識 別 するよう設 計 されています。実 線 は関 連 するイベントのさまざまなグループを示 すのに対 し、点 線 は関 連 する同 じグループに属 するイベントを表 します。イベントのグループでは、先 行 イベントが最 初 に置 かれ、後 続 イベントは先 行 イベントの下 でネスト構 造 になり、後 続 イベントのインデントおよび関 係 アイコンが表 示 されます。関 係 アイコンの横 の数 字 は、セッション分 割 数 を区 別 します。

現 在 のデータ セットに先 行 イベントが含 まれていない場 合 でも、後 続 イベントは最 初 の後 続 イベントの下 でグループ化 されたままになります。先 行 イベントまたは最 初 のイベント(先 行 イベントがない場 合) のみがソートされ、インデントされたイベントはソートされません。後 続 イベント マーカー( ) にカーソルを合 わせると、関 係 を説 明 したツールチップが表 示 されます。次 の図 は、[イベント]リストに表 示 される関 連 イベントの例 を示 しています。



イベントがセッション フラグメントに基 づいて関 連 している場 合 に、後 続 イベントを選 択 して再 構 築 を開くと、[イベント メタ]パネルに`session.split`メタ キーが表 示 されます。



ネット ワーク セッションの分 割

次 のようなツールチップが表 示される場 合 、リスト内 のイベントは分 割 ネット ワーク セッションの一 部 です。

```
The event is part of a split session (session.split: #) matching these parameters: ip.src=127.0.0.1 AND ip.dst=127.0.0.1 AND tcp.srcport=25 AND tcp.dstport=1234.
```

分 割 の原 因 は次 のいずれかです。

- 元 のイベント内 のトランザクションごとに追 加 のイベントを作 成 することによって、元 のイベント がサブ パーツに分 割 された。
- ファイルのサイズがアセンブラーの最 大 サイズ(デフォルト = 32 MB) を上 回っているため、元 のセッション がNetwork Decoderに取 得 されるときに分 割 された。
- アセンブラーのタイムアウト セッション(デフォルト = 60秒) を超 えたため、元 のセッション がNetwork Decoderに取 得 されるときに分 割 された。

セッション サイズと時 間 の分 割

Network Decoderは、デフォルト のセッション サイズ(`assembler.size.max`) とセッション タイムアウト (`(assembler.timeout.session)`) を使 用 して構 成 されています。構 成 の詳 細 については、『*Decoder構 成 ガイド*』の「セッション分 割 タイムアウト の構 成 」を参 照 してください。セッション がいずれか の制 限 を超 えると、Network Decoderはセッション を分 割 し、後 続 のパケット はすべて新 しいセッション とし て処 理 されます。つまり、実 際 のネット ワーク セッション が複 数 のNetwork Decoderセッション に分 割 され ます。Network Decoderでは、より大 規 模 なネット ワーク セッション の断 片 としてセッション フラグメント を処 理 し、ソースおよび宛 先 アドレス、ポート 、アプリケーション プロトコル の関 連 付 けを改 善 するため、コ ンテキスト フラグメント が解 析 され、セッション フラグメント がハイライト表 示 されます。

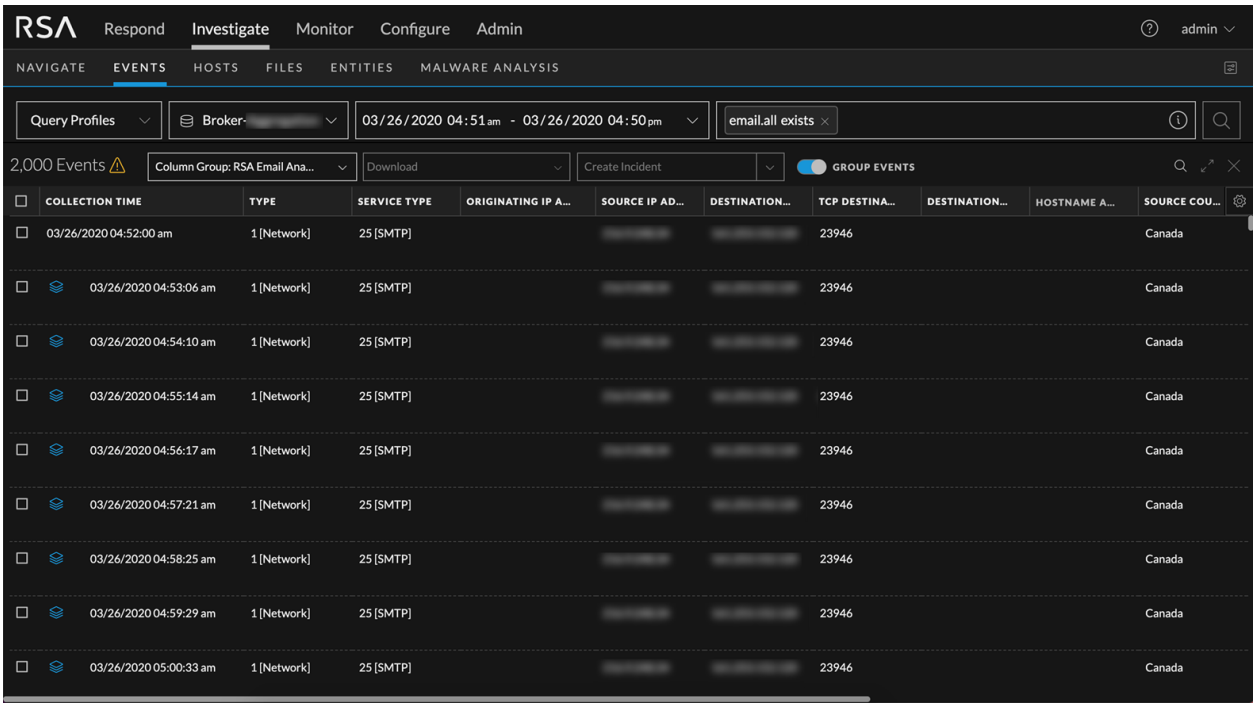
注 : [レガシー イベント]ビューでは、セッション フラグメントを見つけて、[イベント]リストに表示されているすべてのパケットを1つのPCAPにエクスポートできます。「[レガシー イベント]ビューでのフラグメントの検索と結合」を参照してください。

Network Decoderは、構成された最大セッション サイズ(デフォルト = 32 MB) 、または構成されたタイムアウト(デフォルト = 60秒) に基づいて、セッションの解析を完了します。パースが完了した時点で、パース結果には適切なアドレス方向とアプリケーション プロトコルが含まれます。その結果を後続のすべてのセッション フラグメントに追加することにより、元の論理的ネットワーク セッションとの一貫性を確保します。

トランザクション処理の分割

管理者は、Network Decoderを構成し、トランザクションの作成を目的としてLUA Parserを使用する場合に、受信セッションをより小さなトランザクション セッションに分割できます。構成の詳細については、『*Decoder構成ガイド*』の「Decoderでのトランザクション処理の構成」を参照してください。Decoderサービス構成ノードには、パーサがネットワーク セッション内のトランザクションを定義するときにNetwork Decoderの動作を制御するパラメータ`/decoder/parsers/config/parser.transaction.mode`があります。モードが`split`に設定されている場合に、パーサがメールなどのアプリケーションレベルのトランザクションを生成すると、複数のアプリケーションレベルトランザクションを含む大規模なセッションが分割されます。この例としては、複数のメールを含む大規模なセッションが挙げられます。メール(トランザクション) ごとに、新しいセッション項目 (分割セッション) が作成され、新しいセッションにネットワーク メタ項目がコピーされ、トランザクションでマークされたメタ項目が元のセッションから新しいセッションにコピーされます。

トランザクションを機能させるには、パーサのアップデートが必要であり、初期状態では、SMTPおよびHTTPパイプライン化のユースケースしかサポートされません。これは、元のイベント内の個々のメールに基づいて分離された、メールの再構築の例です。各トランザクションは単一のメールをハイライト表示し、トランザクションに関連づけられているメタデータはそのメールにのみ関連します。この機能を提供するために、元のパケットはネットワーク イベントに対して通常どおりNetwork Decoderに格納されますが、新しい関連トランザクション イベントはConcentratorで作成されます。その結果、ユーザ インタフェースにはアナリスト向けのビジュアル キューが表示され、以前はすべてバンドルされていた特定のEメールまたはEメール属性のみを検索するクエリを実行することも可能になります。クエリ結果から元のイベントを除外するため、`session.split`メタキーはインデックスされています。トランザクション分割がある場合、元のイベントにそのメタ キーは関連づけられませんが、関連するすべてのトランザクション イベントには関連づけられます。



セッション フラグメントの強調表示

どちらのタイプのセッション フラグメントにも、session.splitという追加のメタ キーがあります。最初のセッション フラグメントは0で、それ以降のタイムスタンプのセッション フラグメントには1から順に番号が設定されます(1、2、3など) 。session.splitメタ キーは、前のセッション フラグメントの数を示しますが、値が0の場合は、必ずしも後続のセッション フラグメントが存在するとは限りません。また、最大セッション サイズを超える前にセッションのパースが完了した場合は、セッションの最初のフラグメントにsession.splitメタデータが存在しない可能性もあります。

トランザクション分割は、session.splitの値1で始まります。セッションを表示するとき、session.splitメタ キーは、[イベント]ビューと[レガシー イベント]ビュー(イベント リストビューとイベント詳細ビュー) のフラグメントであるセッションを明確に識別します。

これがセッション サイズとタイムアウトの分割であった場合は、セッション フラグメントを表示して、分割セッションを再度1つに結合するための解析に必要な最大セッション サイズまたはセッション タイムアウトを決定できます。たとえば、32 MBのフラグメントが4つある場合は、128 MBを超える最大セッション サイズをテスト用のDecoder(通常は、本番サービスから切り離された仮想マシン構成) に構成する必要があります。この手順は、セッション タイムアウトに基づいてすべてのフラグメントを検索する手順と同じです。

関連ネットワーク セッション

次のようなツールチップが表示される場合は、IPソース、IP宛先、ソース ポート、宛先ポートを識別する4つの値が、Network Decoderによって処理される別々のイベントによって共有されています。

```
 The event is related to a previous session matching these parameters:
ip.src=127.0.0.1 AND ip.dst=127.0.0.1 AND tcp.srcport=25 AND
tcp.dstport=1234"Second category: Related Network Session
```

この例では、Network Decoderが分割を挿入しておらず、どのイベントにもsession.splitメタデータが関連づけられていません。これらのイベントがグループ化されている理由は、パターンに基づいて精査に値するイベントを強調するためです。各イベントには、同じソースIPアドレス、同じ宛先IPアドレス、同じソース ポート、および同じ宛先ポートがあります。データ プライバシーを確保するため、4つのメタ キーのいずれかが難読化されている場合、関連イベントのグループ化は行われません。

関連ネットワーク セッションとしてイベントを分類するために一致する必要があるメタ キーの組み合わせを次に示します。

- ip.dst、ip.src、tcp.dstport、tcp.srcport
- ip.dst、ip.src、upd.dstport、udp.srcport
- ipv6.dst、ipv6.src、tcp.dstport、tcp.srcport
- ipv6.dst、ipv6.src、upd.dstport、udp.srcport

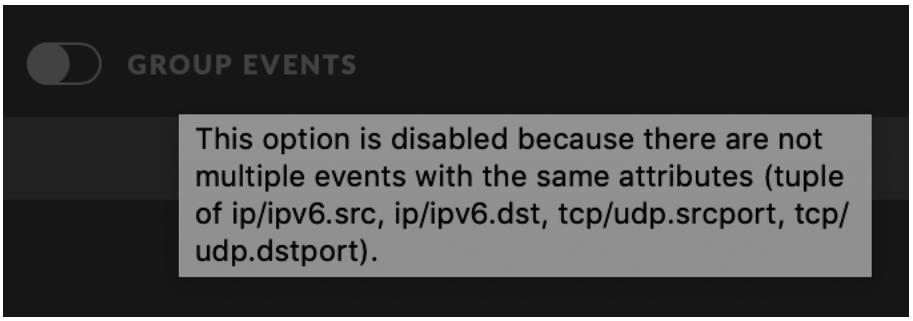
分割および関連ネットワーク セッションからのイベントを表示するための使用例

以下は、分割セッションからのイベントを表示するための実際的な使用例です。

- プロキシ サーバをインラインで使用しているNetwork Decoderは、NetWitnessの認識に応じてイベント時間に基づいて単一セッションにバンドルされる多数のEメール接続を受信します。subject、email.src、email.dstをはじめとしたメールに関連するメタ キーのメタ値はセッションごとに複数あり、正しく組み合わせてマッピングすることは困難です。セッションを先行イベントと後続イベントとして編成することで、アナリストは各メールの詳細を明確に把握できるようになります。
- アナリストは、セッションに関連づけられたすべてのメタデータのうち、どのIPアドレスがメタデータの生成またはアラートの原因となったかを理解しようとしていますが、IPアドレスが出力に含まれていません。たとえば、侵害の兆候を解析しているフィードでは、多くのIPアドレスを持つセッションで多くのトリガーが発生する可能性があります。アナリストは、先行イベントと後続イベントとして編成された完全なイベントを表示することにより、アラートをトリガーしたIPを把握できます。
- アナリストは、どのディレクトリからどのファイルが削除されたか、どのディレクトリでどのファイルが読み取られたかを把握する必要がありますが、セッションに複数のファイルとディレクトリが含まれています。たとえば、directory /keep/、directory /temp/、filename foo.txt、filename me.doc、action delete、action readのコマンドを使用するHTTP接続があるとします。先行イベントと後続イベントを表示すると、/temp/me.docが削除され、/keep/foo.txtが読み取られたことがわかります。これにより、アナリストまたは分析担当者は、これらのアクションの実際の影響についての判断を行えるようになります。
- 疑わしいアラートをトリガーしたイベントに関連している大容量ファイルをアナリストが取得しようとしています。ただし、転送されたファイルは大きすぎたため、Network Decoderによって100個の個別のセッションに分割されました。アナリストは、このグループ関連の分割セッションを表示する際に、セッションのPCAPをダウンロードし、より大規模なアセンブラー設定のDecoderまたはサード パーティ ツールでそれを実行することにより、元のファイルを抽出できます。

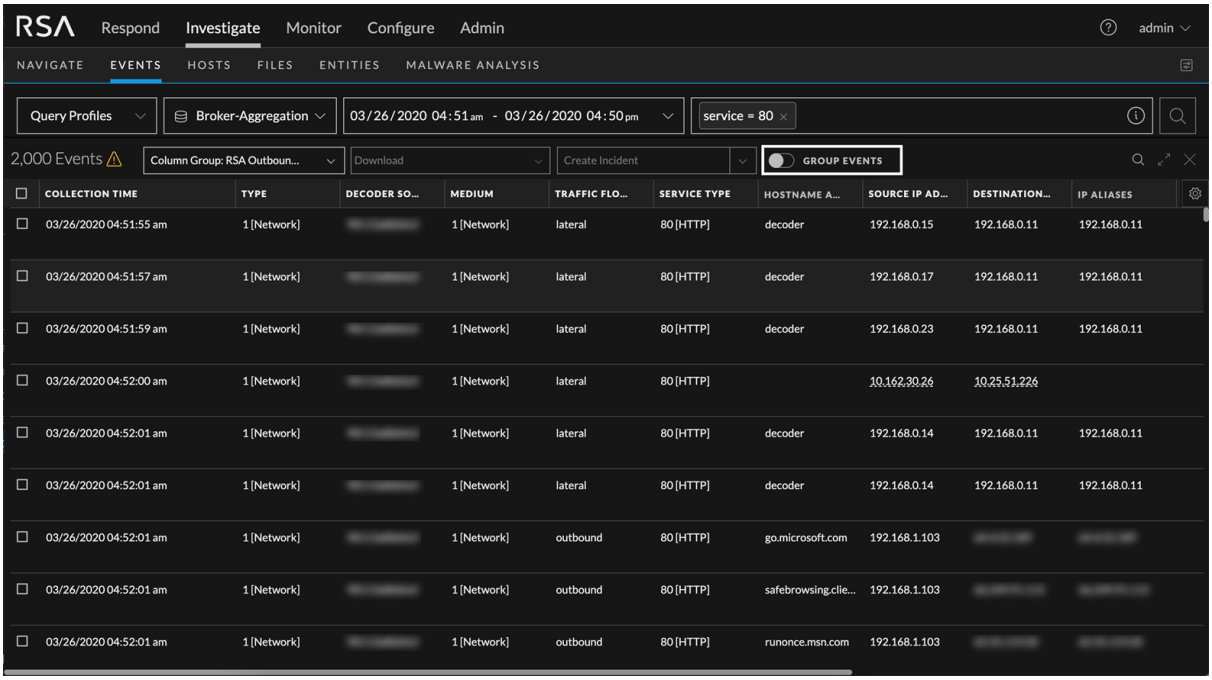
イベント リストでの関係の表示と非表示

どちらのタイプの関連イベントについても、イベントの関係は[イベント]ビューの[イベント]リストで確認できます。[イベント]リストが最初に表示されている場合は、[イベント]リストの最上部にある[イベントのグループ化]スイッチを見て、結果に関連イベントが含まれているかどうかを確認できます。結果に関連イベントが含まれていない場合、このスイッチはグレー表示になります(次の図を参照)。



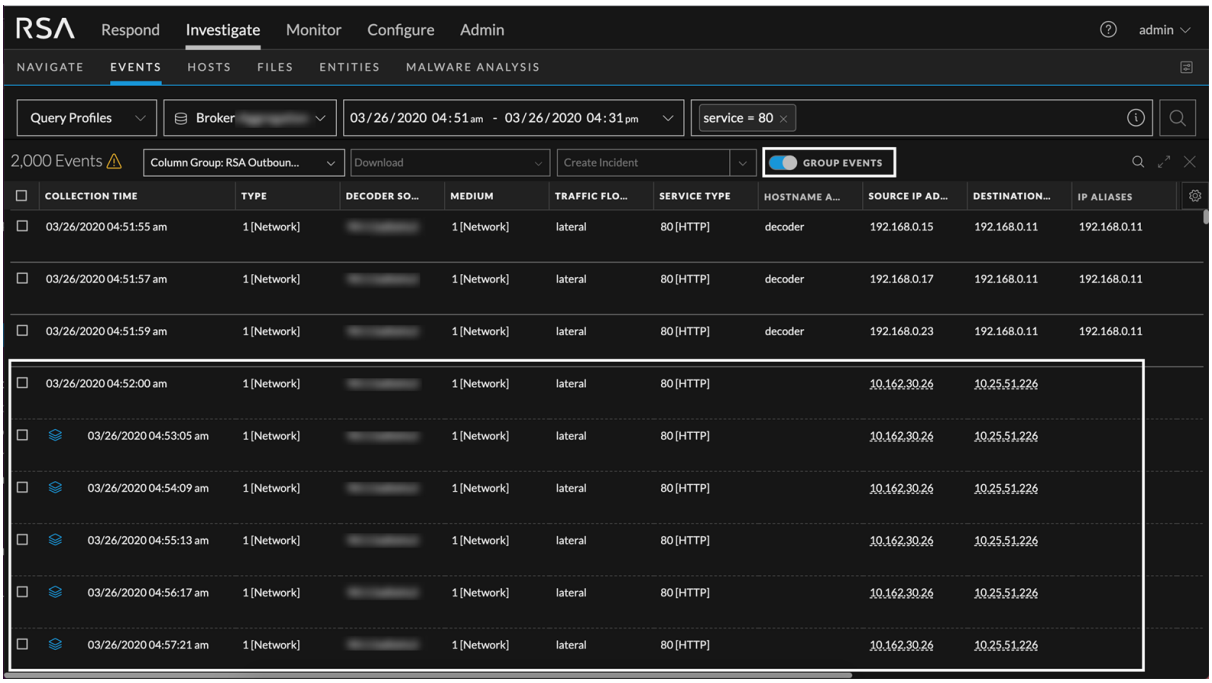
[イベント]リストで関連イベントを検索するには、次の手順を実行します。

1. [**調査**]>[**イベント**]に移動して、クエリを送信します。
   結果に関連イベントが含まれている場合、[イベントのグループ化]スイッチはアクティブですが、有効ではありません。次の図は、分割セッションを含む一連の結果を示しています。[イベントのグループ化]スイッチは無効になっています。関連イベントはネスト構造になっていません。



2. [**イベントのグループ化**]スイッチをクリックします。
   関連する後続イベントは、先行イベントの下にネストされます。後続イベントはインデントされ、アイ

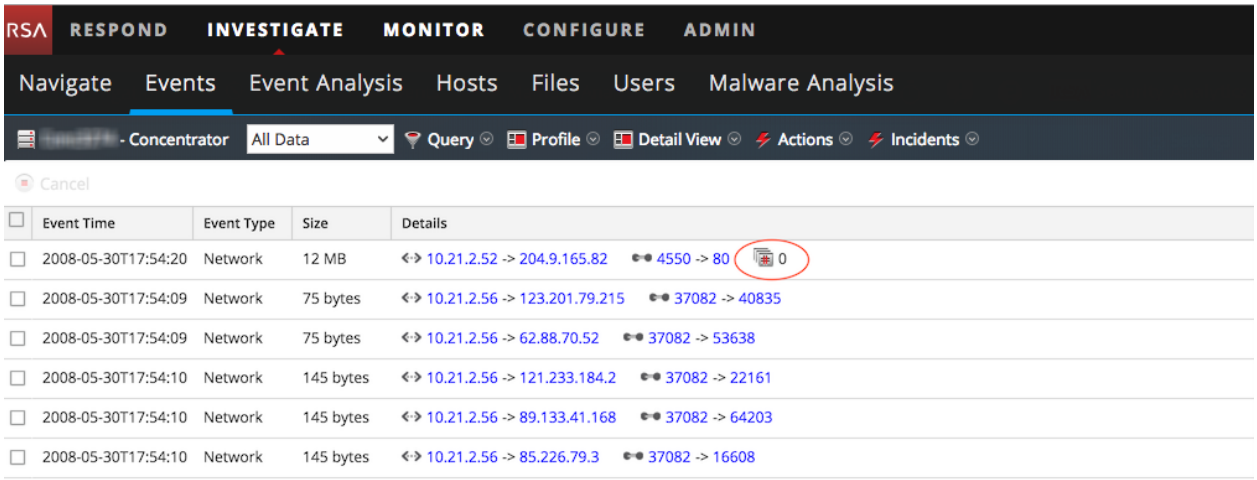
コンで示されます。アイコンをクリックすると、イベントがグループ化されている理由が表示されます。

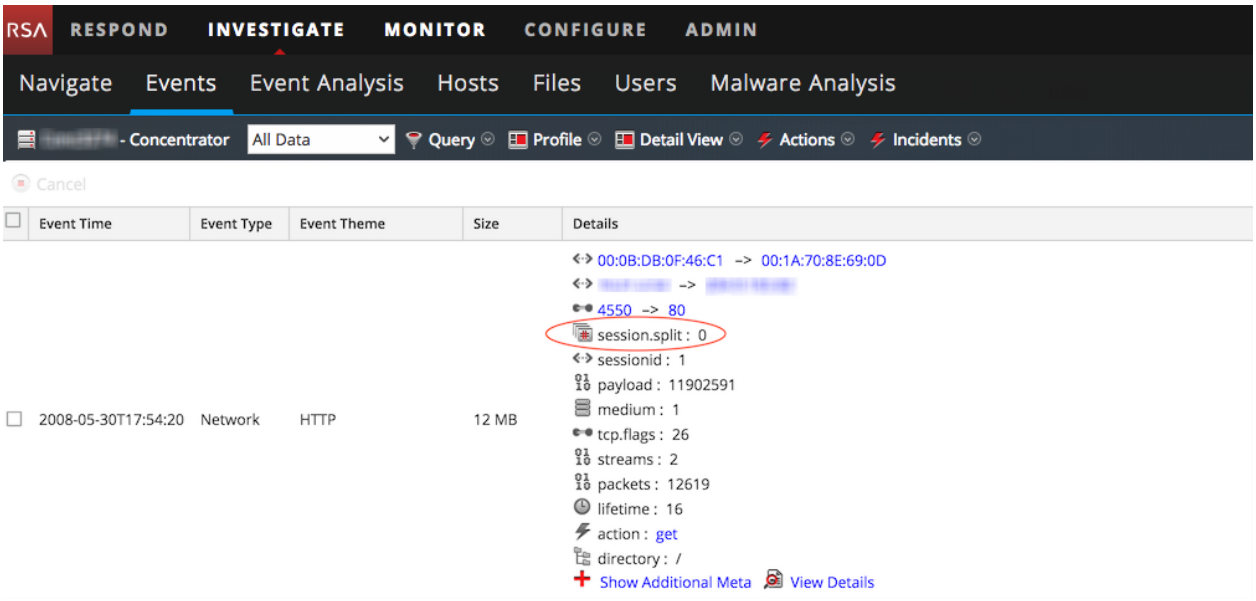


セッション フラグメントのハイライト表示 (11.3の[イベント]ビュー)

次の図は、分割されたセッション情報がハイライト表示されているイベント リストビューおよびイベント詳細ビューを示しています。

注: 以下の画面イメージを取得した環境では、最大セッション サイズは12 MBに構成されています。





注： 結果で分割セッションを見つけやすくするには、`session.split`メタ キーにインデックスを付ける必要があります。

`session.split`メタデータは、詳細ビュー([レガシー イベント]ビュー) ではアドレスとポート メタの直後に表示されます。この機能拡張により、次の操作をすぐに行うことができます。

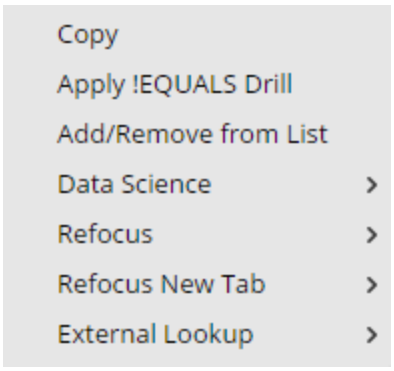
- ネットワーク セッションのフラグメントであるセッションを特定する。
- 1つのセッション フラグメントから、元のネットワーク セッションのすべてのセッション フラグメントを表示する。
- ネットワーク セッション全体のパケットを1つのPCAPファイルとしてエクスポートする。

[レガシー イベント]ビューでのフラグメントの検索と結合

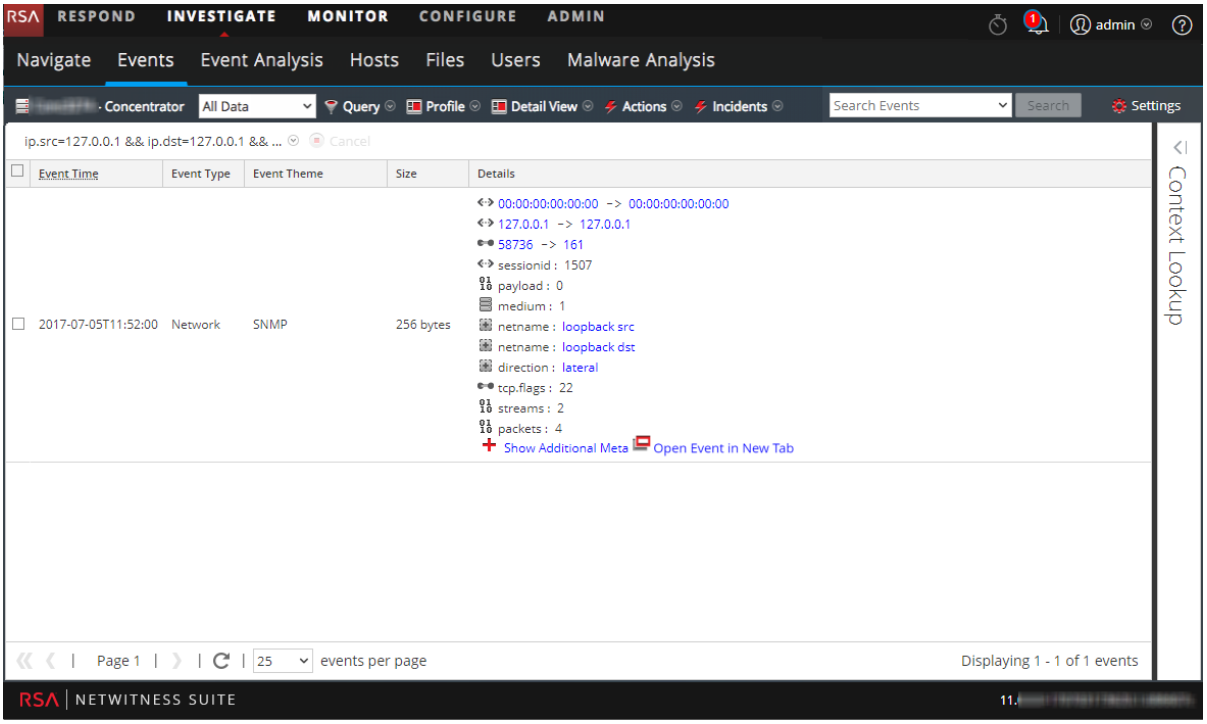
[レガシー イベント]ビューから、[再フォーカス] > [セッション フラグメントを検索]コンテキスト メニュー オプションを使用して、セッション フラグメントを見つけることができます。NetWitness Platformは、選択したセッションのソース アドレス、宛先アドレス、ポートを使用してクエリを作成し、現在の時間範囲内でそのクエリと一致するすべてのセッションを表示します。

セッション フラグメントを検索するには、次の手順を実行します。

1. [**レガシー イベント**]ビューで、ソース アドレス、宛先アドレス、ポートの値(`ip.src`、`ip.dst`、`ipv6.src`、`ipv6.dst`、`tcp.srcport`、`tcp.dstport`、`udp.srcport`、`udp.dstport`) または`session.split`値のいずれかを右クリックします。
   コンテキスト メニューが表示されます。



2. **[再フォーカス] > [セッション フラグメントを検索]**または**[新しいタブを再フォーカス] > [セッション フラグメントを検索]**を選択します。
NetWitness Platformでは、現在の時間範囲に存在する特定の1セッションのセッション フラグメントがイベント リストに表示されます。選択したオプションに応じて、再フォーカスは現在のビューに表示されるか、新しいタブに表示されます。(例の中で、時間範囲として「すべてのデータ」を選択している場合がありますが、本番システムでの使用は推奨されません) 。



3. 必要な場合は、時間範囲を調整して、現在の時間範囲の前後に存在する可能性があるすべてのセッション フラグメントを表示します。時間の境界の近くでフラグメントが発生した場合、特に最初に表示されるフラグメントのsplitの値が0(または、なし) でない場合は、時間範囲を広げる必要があることが分かります。また、最後に表示されるセッションのパケットを調査すれば、セッションが継続しているかどうかを判断できます。次に例を挙げます。

   a. 明らかに最初のフラグメントではないもの、たとえば10:30～10:35の時間範囲に、1、2、3、4のフラグメントが見つかった場合は、フラグメント0が存在するはずです。時間範囲の開始を早めると

(この例 では10:25) 、追 加 のフラグメントを見 つけることができます。

b. 最 後 のフラグメント のセッション サイズが最 大 セッション サイズ(この例 では12 MB) に近い場 合 は、それ以 降 の時 間 (この例 では10:40) を含 めるように時 間 範 囲 を広 げ、追 加 のフラグメントを 探します。
ネット ワーク セッションのすべてのセッション フラグメントを1つのイベント リスト に表 示 すると、リスト が複 数 ページにまたがることがあります。

4. (オプション) すべてのセッション フラグメント のパケット を1つのPCAPファイルにエクスポート するには、**[アクション] > [すべてのPCAPのエクスポート]** を選 択します。
PCAPがダウンロード 中 であることを示 すメッセージが表 示 されます。ダウンロード が完 了 すると、PCAPファイルには、分 割 されたネット ワーク セッションの全 体 が含 まれています。

座標表示チャートへのメタデータの追加

アナリストは、[ナビゲート]ビューで座標表示チャートを使用できます。これにより、異常なイベントの兆候を示し、調査する価値のあるメタ キー、メタ エンティティ、メタ値の組み合わを集中的に調査できるようになります。座標表示チャートは、調査の現在のドリルダウン ポイントをビジュアル化し、3個以上のメタ キーを同時に調査するために使用されます。複数のメタ キーを同時にビジュアル化すると、多変量パターンおよび比較に関連したセキュリティ問題を特定するうえで役立ちます。例えば、個々のメタ キーとメタ値には問題がなくても、それらを組み合わせたときに異常なパターンや関係が明らかになる場合があります。メタ グループ(「メタ グループを使用して関連性の高いメタ キーにフォーカス」を参照)を効果的に使用して、座標表示チャートに追加するメタ キーのコレクションを定義することができます。

効果的な座標表示チャートに関するベスト プラクティス

効果的な座標表示チャートを作成するには、以下の推奨事項を実行します。

- 新規インストールに含まれているRSA標準提供のメタ グループを使用します。
- すべてのデータを可視化しようとするのではなく、1つのドリルダウン ポイントから開始します。
- 必要に応じて時間範囲を制限します。
- 可能な限り少ない数の有益なメタ キーを軸として表示するよう選択します。
- メタ値間の異常性が強調されるように、チャート内の直線に沿って軸の順序を指定します。
- 有益なメタ キーとその順序を特定できる場合は、将来の調査で使用するカスタム メタ グループを作成します。たとえば、Windows実行可能ファイル タイプのカスタム メタ グループを作成できます。
- カスタム メタ グループを.jsnファイルとしてインポートおよびエクスポートすることによって、グループを再利用したり共有したりします。
- カスタム メタ グループごとに2つのバージョンを作成しておくと便利です。1つはメタ値の分析に使用し、もう1つは同じユースケースの小規模サブセットに重点を置いた座標表示チャートの作成に使用します。

注: メタ グループをインポートするとき、既存のメタ グループが含まれていると、エラー メッセージが表示されます。重複したグループをインポートするには、まず既存のグループを削除しておかなければなりません。プロファイルによって使用されているメタ グループは削除できません。

NetWitness Platformでは、効果的な座標表示チャートを構築するため、いくつかの最適化が可能です。

- アナリストは、すべてのメタ キーを含んでいるセッションのみをチャートで表示するよう指定できます。
- 管理者は、[管理]>[システム]ビュー>[調査]パネル>[ナビゲート]タブの[座標表示の設定]で、表示するメタ値の数を増やすことができます。

座標表示で使用できるRSAメタ グループ

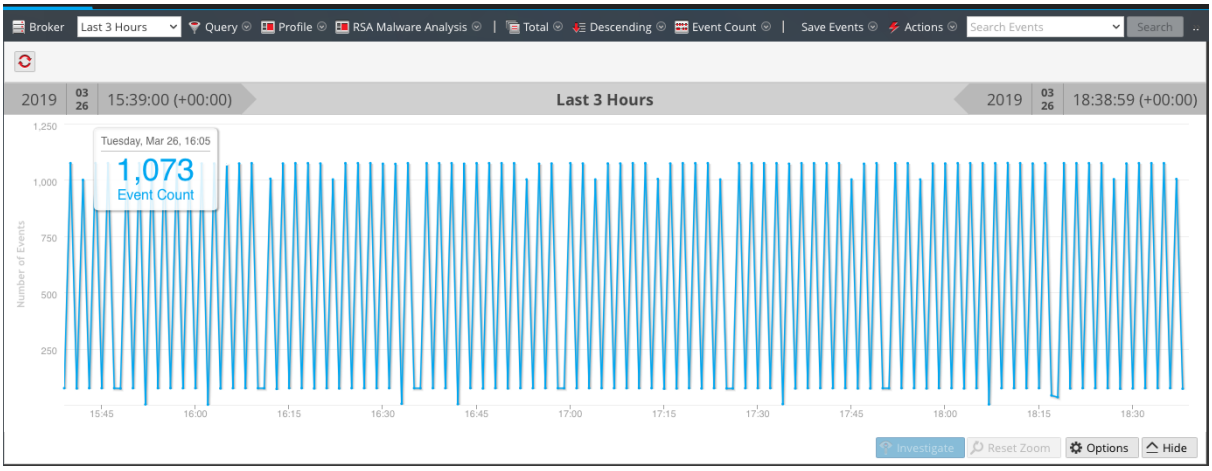
NetWitness Platformには、事前定義されたメタ グループのセットが含まれています。最新のバージョンを取得する場合は、[メタ グループの管理]ダイアログでメタ グループ ファイル(`MetaGroups_ootb_w_query.jsn`) をインポートできます。座標表示チャートに適した標的型アクティビティとしては、次のようなものがあります。

- Botnet Beaconing
- Covert Channels
- Email Analysis
- Encrypted Sessions
- Endpoint Analysis
- File Analysis
- Malware Analysis
- Outbound HTTP
- Outbound SSL/TLS
- SQL Injection Attacks
- Threat Analysis
- Web Analysis

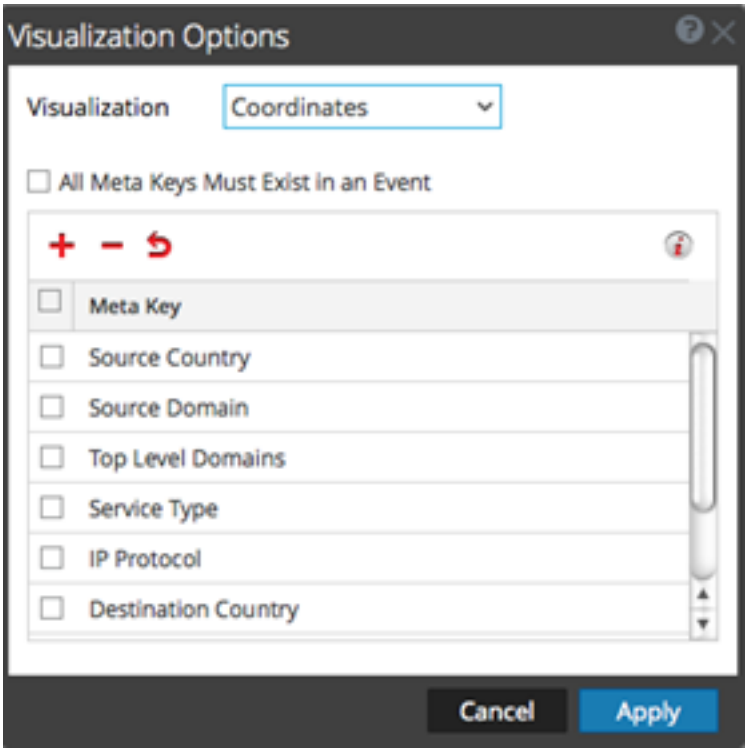
座標表示チャートの表示

[調査]>[ナビゲート]ビューで、次の手順を実行します。

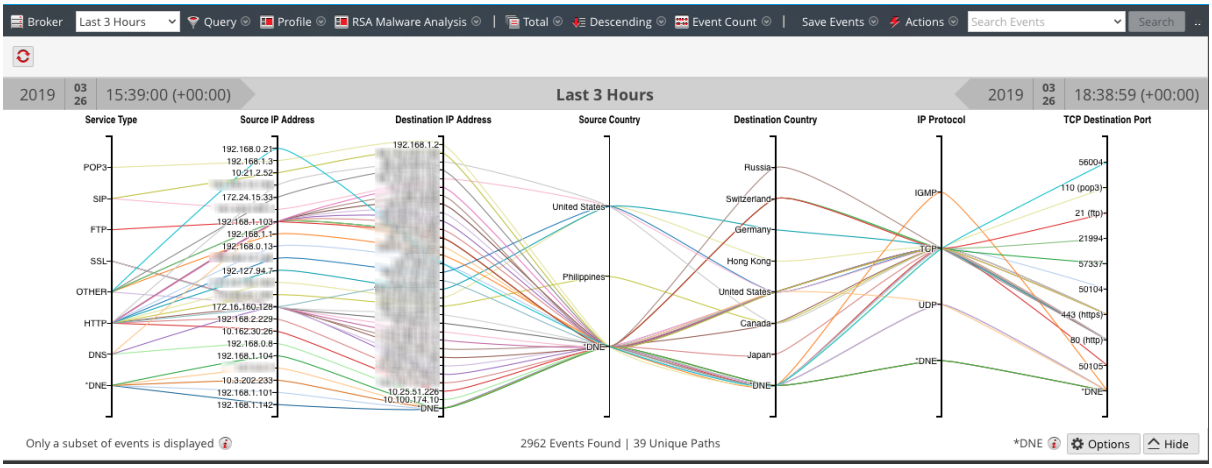
1. [値]パネルの上の[チャート]パネルが閉じられている場合は、[**チャートの表示**]を選択します。
2. ツールバーで、[**メタ**]>[**メタ グループの使用**]>[**RSA Malware Analysis**]を選択します。
3. 現在のドリルダウン ポイントのデフォルトのタイムライン チャートが表示されます。



4. [**チャート**]パネルで[**オプション**]を選択します。
[チャート オプション]ダイアログが表示されます。
5. [**チャートの表示**]ドロップダウン リストから[**座標表示**]を選択して、[**適用**]をクリックします。



チャートがロードされます。この例では、2,962個のイベントが見つかり、39個の一意のパスが可視化されます。

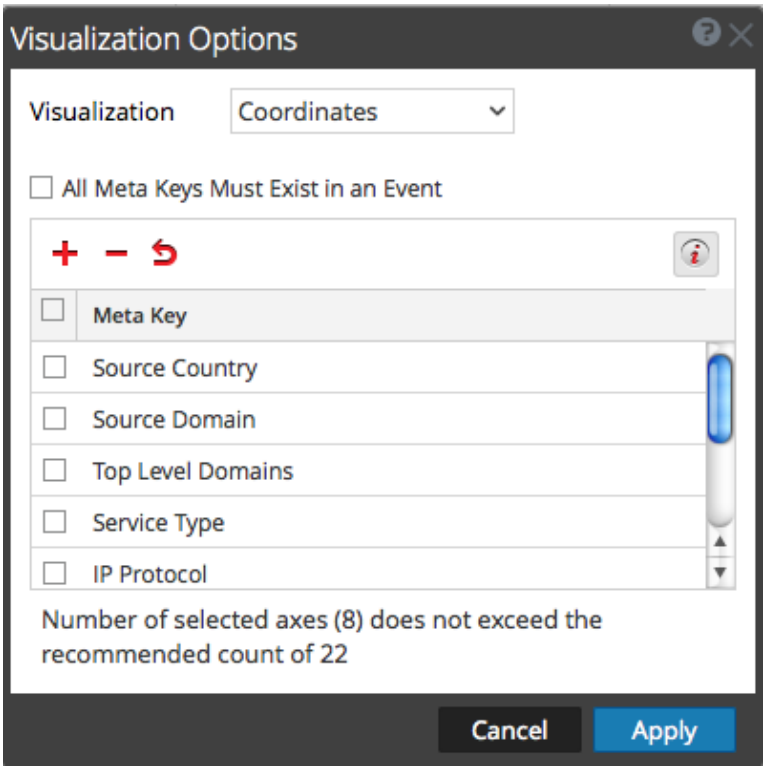


座標表示チャートで使用するメタ キーの選択

座標表示チャートが開いた状態で、次の操作を行います。

1. [チャート]パネルで[**オプション**]を選択します。
[チャート オプション]ダイアログが表示されます。ツールバーの をクリックすると、見やすいチャート

に適した軸数が表示されます。推奨される軸の数は、ブラウザのサイズによって変化します。ブラウザ ウィンドウを拡大すると、推奨される数は増加します。



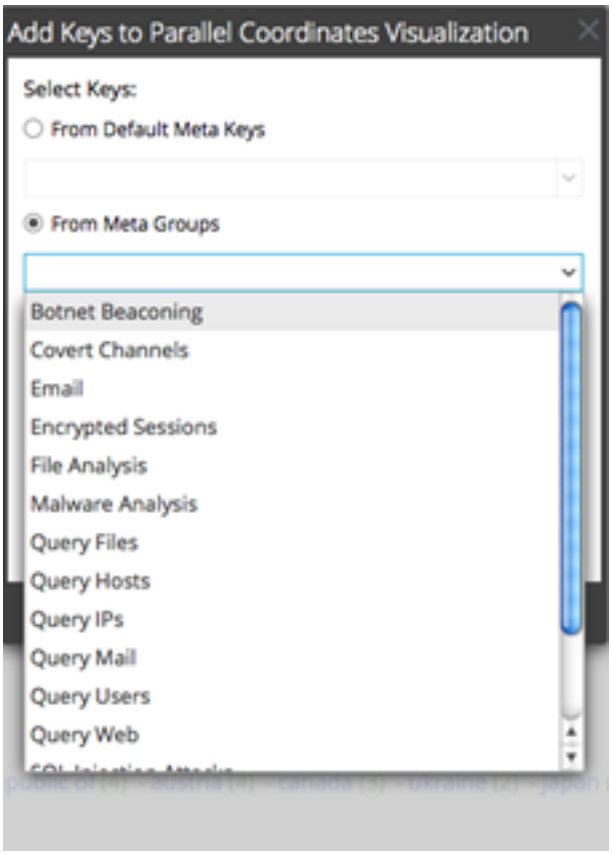
2. メタ キーの順序を変更するには、メタ キーを上下にドラッグして目的の順序に変更します。
3. メタ キーを削除するには、選択ボックス内をクリックして、 をクリックします。
   メタ キーが削除されますが、変更は適用されません。
4. 元の状態に戻すには、 をクリックします。
   削除したメタ キーがすべてリストアされ、行った変更がすべて削除されます。
5. メタ キーを個別に選択する場合は、 をクリックし、[**デフォルトのメタ キーから追加**]を選択し、ドロップダウン リストからメタ キーを選択します。

   選択したキーが表示されます。

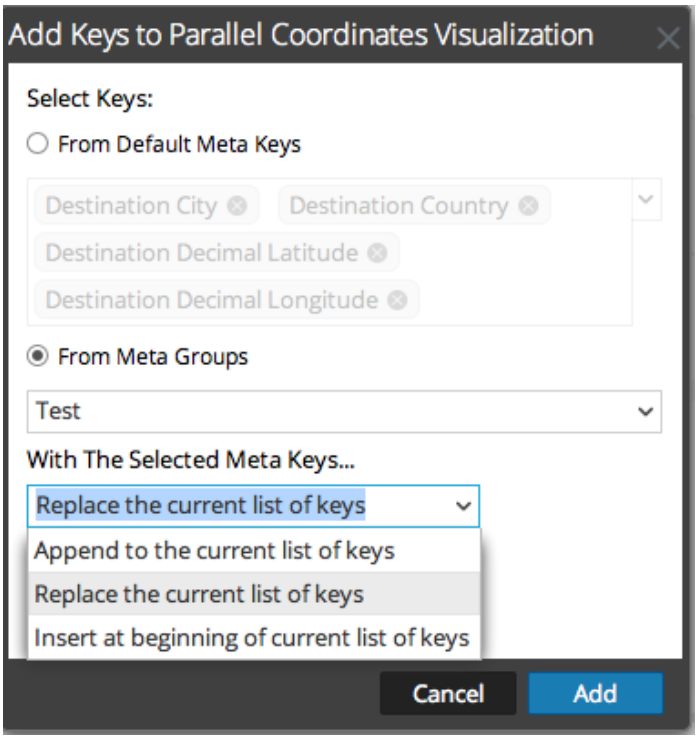
   

6. メタ グループ内のすべてのメタ キーを追加する必要がある場合、メタ キーを個別に追加する必要はありません。[**メタ グループから追加**]を選択して、ドロップダウン リストからグループを選択します。



選択したメタ グループがフィールドに表示されます。

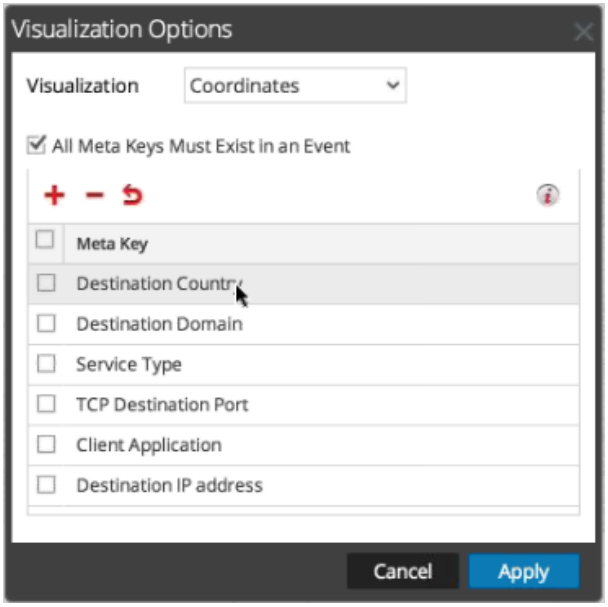
7. キーまたはグループの追加方法を、[**現在のキーのリストを置き換え**]、[**現在のキーのリストの後に挿入**]、[**現在のキーのリストの先頭に挿入**]から選択します。



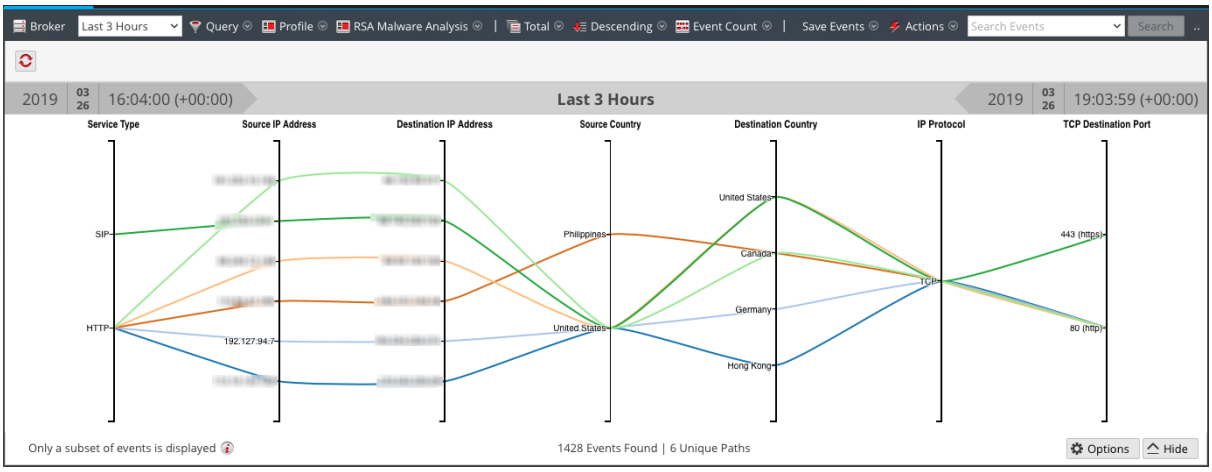
8. 手順を完了するには、[**追加**]をクリックします。
   [チャート オプション]ダイアログに、選択したメタ キーまたはメタ グループが表示されます。
9. 新しいチャートを表示するには、[**適用**]をクリックします。

座標表示チャートの最適化

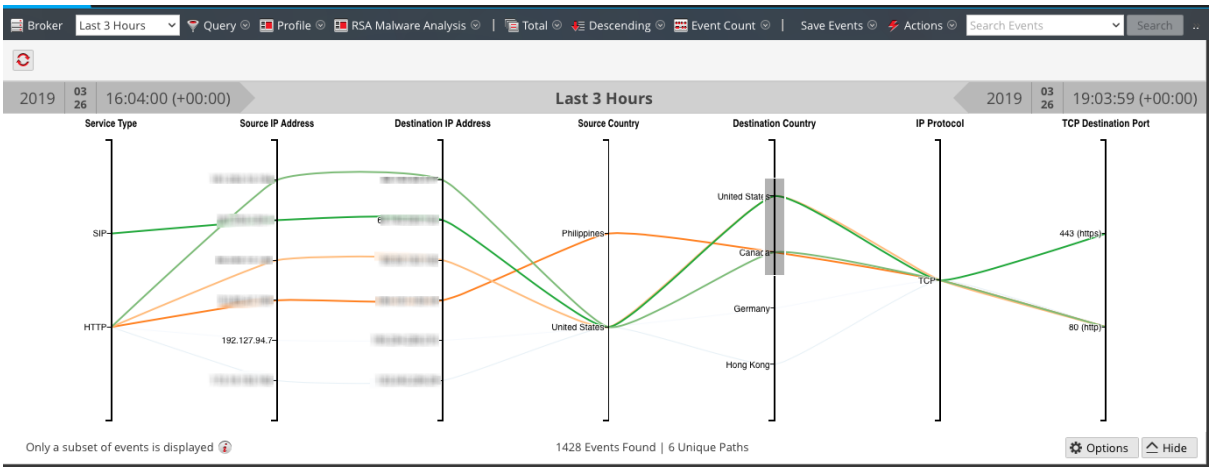
1. すべてのメタ キーを含んでいないイベントを削除することによってチャートを最適化するには、[**オプション**]を選択します。



2. [ビジュアル化オプション]ダイアログで[**すべてのメタ キーが1つのイベントに存在する必要があります**]を選択します。[**適用**]をクリックします。
結果として表示されるチャートは、見やすく便利になり、固有パスの数が減少します。



3. 少数の点を選択し、左右に伸びるパスをハイライト表示するには、軸をクリックします。カーソルが十字線に切り替わり、ドラッグして軸上の値を選択できるようになります。マウスを離すと、パスがハイライト表示されます。



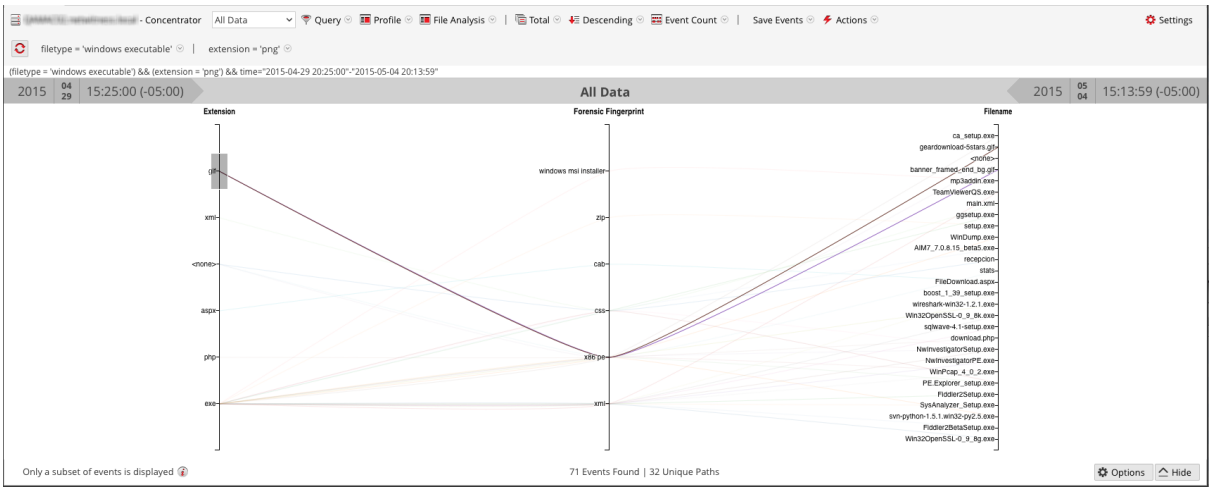
4. ビジュアル化を拡大するには、パネルの下縁を下方向にドラッグし、ブラウザ ウィンドウの右縁をドラッグして広げます。

使用例

次の例では、セッションのファイル メタデータを表すメタ キーを座標表示チャートに表示しています。左から右に、Extensions、Forensic Fingerprint、Filenameという3つのメタ キー(軸) があり、各軸に沿って値が表示されます。Extension軸の値はファイル拡張子を示し、Forensic Fingerprint軸の値はWindows実行可能ファイルのタイプを示します。通常、ファイル拡張子と、想定されるフォレンジック フィンガープリントは一致します。しかし、`gif`ファイル タイプがWindows実行可能ファイル フィンガープリントと組み合わせになることは異常です。`gif`ファイル拡張子は、ファイル タイプ(`x86pe`) 、3番目の軸の2つのファイル名との関連をハイライト表示するために選択されています。これにより、アナリストは調査に役立つファイルをすばやく特定できます。

このビューにアクセスするには、次の手順を実行します。

1. 値の昇順で並べ替えます。
2. 2つのフィルタ(file type = 'windows executable'およびextension = 'gif') を[ナビゲート]ビューに適用し、データの量を制限します。
3. 3つの軸(`file extension`、`forensic fingerprint`、`filename`) を選択して座標表示チャートを構成します。

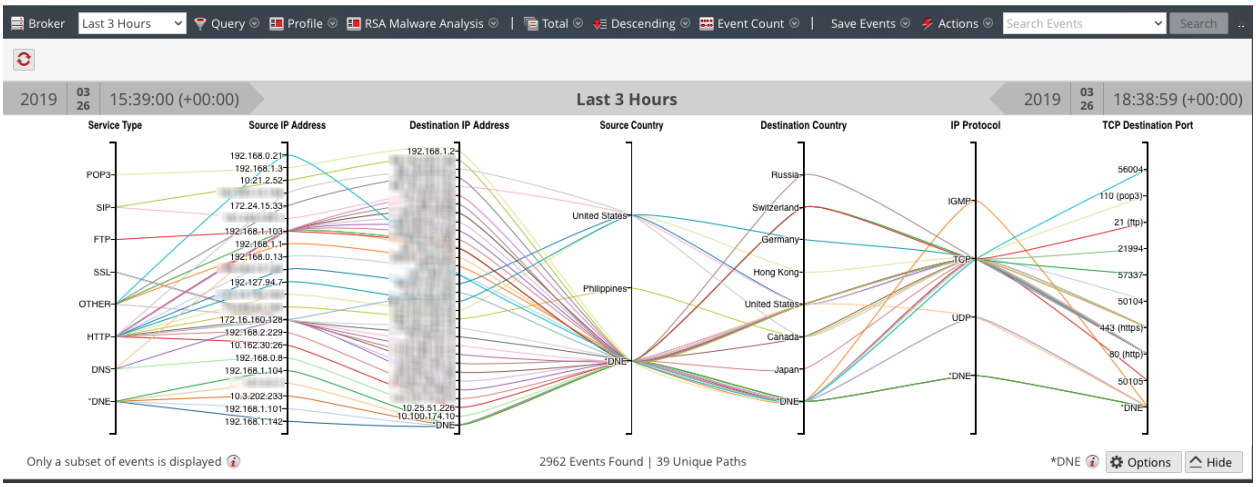


大量データセットのチャートの例

座標表示チャートに大量のデータセットを適用したこの例では、アナリストがチャートの内容を理解するうえで役立ついくつかのメッセージを示しています。

- チャートを作成するため、メタ値のスキャンがNetWitness Platformによって開始され、結果が返されます。典型的な時間範囲に含まれるメタ値の数は、最大で1,000万個に達する場合があります。返されるメタ値の数がメタ値の結果制限に達すると、メタ値のスキャン制限と等しい数のメタ値がNetWitness Platformによってスキャンされていない場合でも、チャートが表示されます。
- 座標表示チャートに表示できるデータ量には一定の制限があります。管理者は、[管理]>[システム]ビューの調査の設定で、座標表示の制限値を構成します。

大量データセットの場合、小量データセットとメタ キーの場合と比べて、座標表示チャートの処理に時間がかかります。NetWitness Platformは、パフォーマンスを維持するために、管理者が設定した制限値に達するまで、[値]パネルからのメタ値をチャートに表示します。制限値に達した場合は、「**イベントのサブセットのみが表示されます**」という情報メッセージが表示されます。



2,962個のイベントについてチャートされたすべてのデータのうち、一意の座標表示パスは39個だけです。イベントの中にはすべてのメタ キーを含まないものがあり、そのようなイベントには、メタデータが存在しないことを意味するDNEというラベルが付けられます。

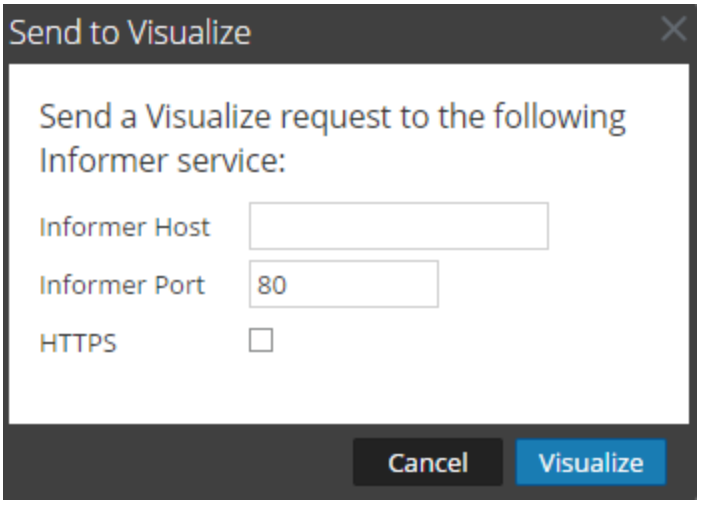
ドリルダウン ポイントのInformerでのビジュアル表 示

このトピックでは、[ナビゲート]ビューでドリル ポイントをInformerに送 信してビジュアル化 するための手 順について説 明します。

Informerがネット ワーク内 にインスト ールされ、調 査 中 のサービスからアクセスできる必 要 があります。NetWitness Platformと通 信 するために、Informerのホスト 名 とポートを指 定 する必 要 があります。

現 在 のドリルダウン ポイントをInformerでビジュアル表 示 するには、次 の手 順を実 行します。

1. [ナビゲート]ビューでドリルダウン ポイントが開いている状 態 で、**[アクション]＞[可 視 化]**をクリックします。
   [Visualizeに送 信]ダイアログが表 示 されます。



2. Informerのホスト 名 またはIPアドレスを入 力 し、Informerホストとの通 信 に使 用 するNetWitness Platformサーバ ポートを確 認します。
3. (オプション) Informerホスト がセキュリティで保 護 された通 信 を使 用 している場 合 、HTTPSオプションを選 択します。
4. [**Visualize**]をクリックします。
   新しいタブにデータがビジュアル表 示 されます。

結果のダウンロードと処理

Investigateで作業する際に、データを抽出して、他のアナリスト、インシデント対応者、SOCマネージャーなどと共有することができます。このセクションのトピックでは、結果をダウンロードする手順と、[対応]ビューに表示されるインシデントの作成手順について説明します。

- [イベント]ビューでのデータのダウンロード
- [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷
- [レガシー イベント]ビューでのイベントのエクスポート
- [イベント]ビューでのインシデントへのイベントの追加
- [レガシー イベント]ビューでのインシデントへのイベントの追加

[イベント]ビューでのデータのダウンロード

[イベント]ビューでは、[イベント]パネルと再構築からデータをダウンロードできます。バージョン11.4で使用可能な[イベント]パネルのダウンロード機能では、すべてのイベント タイプのログおよびネットワーク イベントが一括ダウンロードされます。バージョン11.4.1には、すべてのイベント タイプに対して表示可能なメタデータをダウンロードする機能が追加されています。再構築内からは、イベント、ログ、ファイルをダウンロードできます。

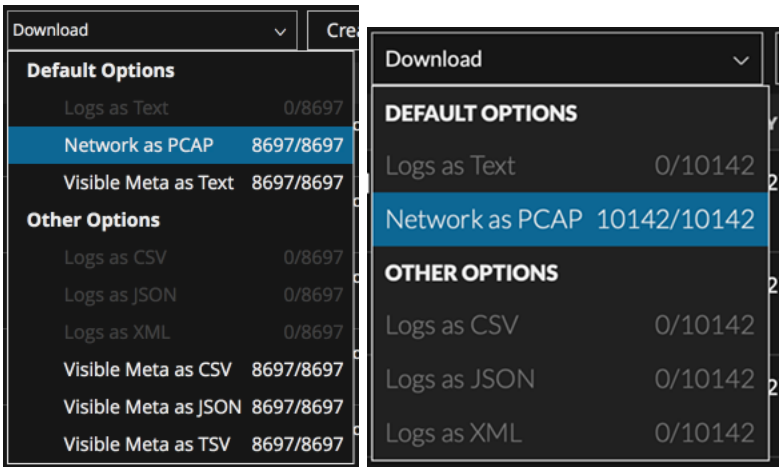
注: 表示およびダウンロードできる情報は、管理者が実装したロールベース アクセス制御(RBAC)によって管理されます。特定のデータがダウンロードされるのを防ぐようにRBACが設定されている場合、ダウンロード権限のないイベントが正常にダウンロードされたように見えることがありますが、サイズは0バイトです。特定のイベントが再構築されるのを防ぐようにRBACが設定されている場合、再構築は[イベント]パネルで無効になりますが、一括ダウンロード ボタンは有効なままになります。

[イベント]パネルでのログ、表示可能なメタデータ、ネットワーク イベントのダウンロード(バージョン11.4以降)

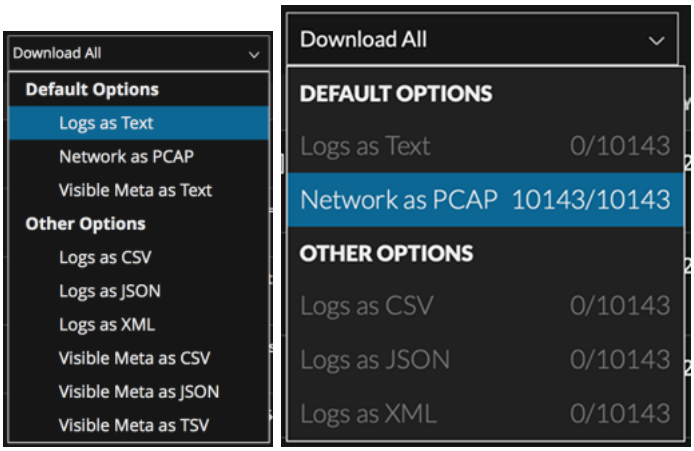
クエリの送信後は、イベントのログ、ネットワーク イベント、表示可能なメタデータを、[イベント]パネルから直接、指定した形式でダウンロードできます。環境設定は[イベント環境設定]ダイアログで設定され、変更はすべて[**ダウンロード**]メニューに反映されます。環境設定の詳細については、「[イベント]ビューの構成」を参照してください。

注: 表示可能なメタデータをダウンロードすると、[イベント]パネルの現在のソート順ではなく、収集時間の順でメタデータがソートされます。

[イベント]パネルでは、検索で返されたイベントを個別に選択するか、すべてのイベントを選択できます。選択チェックボックスは、イベントをダウンロードする権限がある場合にのみ表示されます。新しいクエリを送信すると、すべてのチェックボックスが選択解除されます。イベントを選択して[ダウンロード]をクリックすると、[ダウンロード]メニューが表示されます。各イベント タイプに対して選択されているイベントの数は、各オプションの横に「`Events of this type selected/ Total number of events selected`」形式で表示されます。イベント タイプでイベントが選択されていない場合は、対応するダウンロード オプションが無効になり、選択したイベントの数が「`0 / Total number of events selected`」として表示されます(次の図を参照)。バージョン11.4.1のメニューには、表示可能なメタデータをダウンロードするオプションがあり、バージョン11.4のメニューには、これらのオプションがありません。



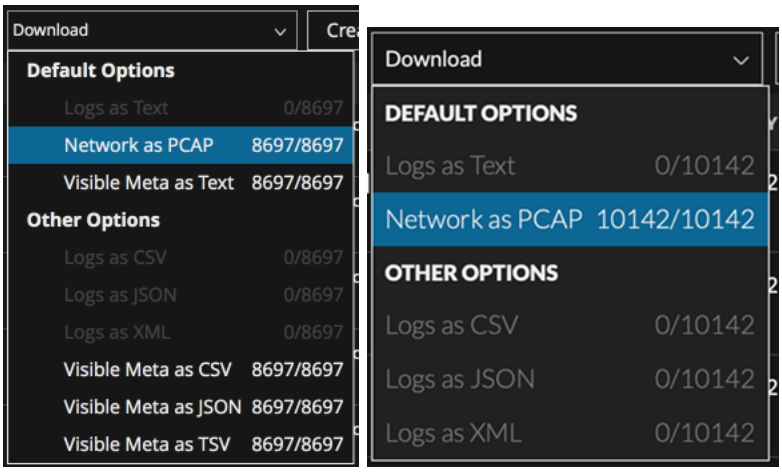
[イベント]リストですべてのチェックボックスが選択されている場合、イベント数はメニューに表示されなくなります(次の図を参照)。バージョン11.4.1のメニューには、表示可能なメタデータをダウンロードするオプションがあり、バージョン11.4のメニューには、これらのオプションがありません。



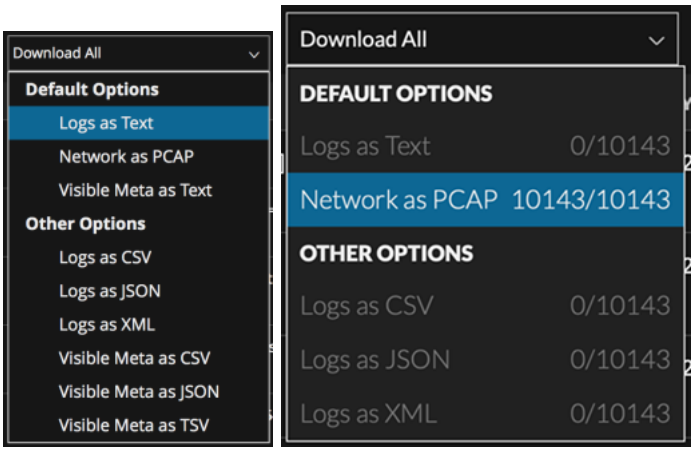
注: すべてのイベントをダウンロードするよう選択すると、現在の結果セット内のイベントのみがダウンロードされます。すべての結果が返される前にクエリをキャンセルした場合は、ロードされたイベントのみがダウンロードされます。

[イベント]パネルで単一イベント、複数イベント、またはすべてのイベントのイベント データをダウンロードするには、次の手順を実行します。

1. 次のいずれかを実行します。
   a. イベントを個別に選択するには、ダウンロードする各イベントの横にあるチェックボックスをオンにして、[**ダウンロード**]メニュー ラベルをクリックしてオプションを表示します。バージョン11.4.1のメニューには、表示可能なメタデータをダウンロードするオプションがあり、バージョン11.4のメニューには、これらのオプションがありません。

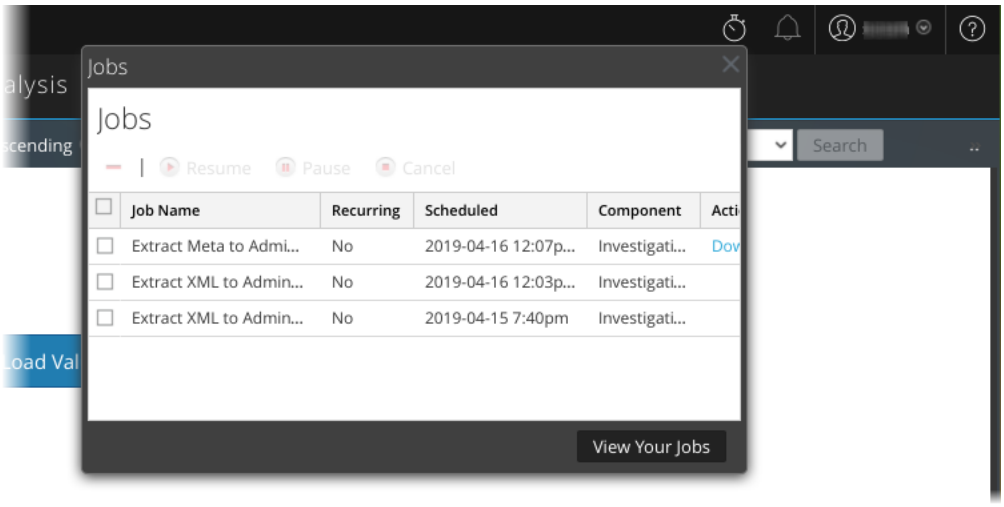


b. [イベント]パネルに表示されているすべてのイベントを選択するには、[イベント]パネルの上部にあるチェックボックスをオンにして、[**すべてダウンロード**]メニュー ラベルをクリックします。



2. メニューの上部で有効になっている[**デフォルトのオプション**]を確認します。デフォルトの形式を使用しない場合は、メニューの[**その他のオプション**]セクションで別の形式を選択できます。
   - [イベント環境設定]メニューで選択した形式(**テキスト形式のログ**、**CSV形式のログ**、**JSON形式のログ**、**XML形式のログ**)でログがダウンロードされます。このダウンロードに異なる形式を選択する場合は、メニューの下部にあるいずれかの形式を選択します。
   - ネットワーク イベントはPCAPとしてダウンロードされます。[イベント]パネルで複数のネットワーク イベントをダウンロードする場合、形式は常にPCAPとなります。[イベント環境設定]メニューで指定した形式(**PCAP形式のネットワーク**、**ペイロード形式のネットワーク**、**リクエスト ペイロード形式のネットワーク**、**レスポンス ペイロード形式のネットワーク**)はこのメニューでは無視されます。指定した形式は、ネットワーク再構築パネルでの単一ネットワーク イベントのダウンロードにのみ適用されます。
   - 表示可能なメタデータは、[イベント環境設定]メニューで選択した形式(**テキスト形式の表示可能なメタ**、**CSV形式の表示可能なメタ**、**JSON形式の表示可能なメタ**、**TSV形式の表示可能なメタ**)でダウンロードされます。このダウンロードに異なる形式を選択する場合は、メニューの下部にあるいずれかの形式を選択します。各イベントに対してダウンロードされるメタデータは、メタデータをダウンロードするときに表示される列に対応しています。[イベント]パネルでサマリー列グループが選択されている場合は、イベントのすべてのメタデータがダウンロードされます。

3. メニュー ラベル[**ダウンロード**]または[**すべてダウンロード**]をクリックします。
   [**抽出したファイルを自動ダウンロード**]が設定されている場合([**イベント**]ビュー>)、ダウンロードはブラウザ ウィンドウ内でただちに始まります。この環境設定が設定されていない場合は、選択したイベントのダウンロード ジョブがジョブ トレイに追加され、そこからイベントをダウンロードできるようになります。
   ダウンロードが失敗した場合は、ダウンロードが失敗した理由についてのフィードバックがメッセージに表示されます。ダウンロード ボタンが再度有効になり、選択したイベントが選択されたままになります。次の例は、ダウンロードが失敗した理由(X分後のタイムアウト、接続障害、イベント制限に到達、権限の拒否)の例です。
4. ジョブ トレイを表示するには、[**調査**]>[**ナビゲート**]または[**調査**]>[**イベント**]に移動して、ストップウォッチに似ているジョブ アイコン をクリックします。
   ジョブがジョブ トレイに表示されます。

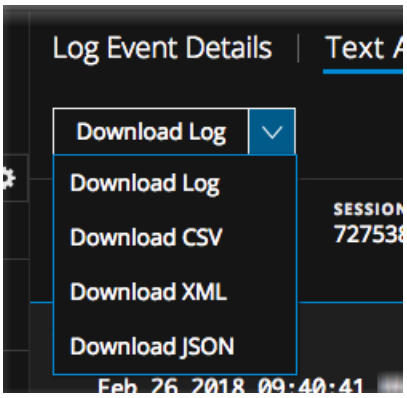


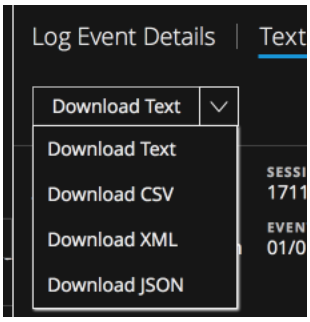
[テキスト]パネルでのログのダウンロード

[テキスト]パネルでログの再構築を表示しているときに、[ログのダウンロード]ドロップ ダウン メニューのオプションを使用して、次の形式でログ ファイルをダウンロードすることができます。

- RAWログ(ログ)。[**ログのダウンロード**](11.3)または[**テキストのダウンロード**](11.4以降)オプションを使用
- カンマ区切り値(CSV)。[**CSVのダウンロード**]オプションを使用
- 拡張可能マークアップ言語(XML)。[**XMLのダウンロード**]オプションを使用
- JavaScript Object Notation(JSON)。[**JSONのダウンロード**]オプションを使用

これは、[**ログのダウンロード**](11.3)または[**テキストのダウンロード**](11.4以降)メニュー オプションが表示されているログ再構築の例です。





注 : [**ログのダウンロード**] (11.3) または[**テキストのダウンロード**] (11.4以降) オプションは、少なくとも1つのメタ値が256文字を超えているエンドポイント イベントにのみ適用されます。エンドポイント イベントの場合、メタ値が256文字を超える場合にのみ、RAWログが取り込まれます。長時間実行されているか、履歴をダウンロードしたファイルはダウンロード可能ではありません。
たとえば、起動の引数のようなメタ値は256文字を超えることができます。この場合、256文字はメタ値として使用でき、完全な値はRAWログで表示できます。

ダウンロードしたログ ファイルにはログが含まれ、ログを収集したサービス、セッションID、ファイル タイプが識別できるようファイル名が付けられます。RAWログのファイル名は「**Concentrator_SID2.log**」のようになります。エクスポートされたログ ファイルの名前は、次の規則で決まります。

```
<service-ID or host name>_SID<n>.<filetype>
```

各項目の意味は次のとおりです。

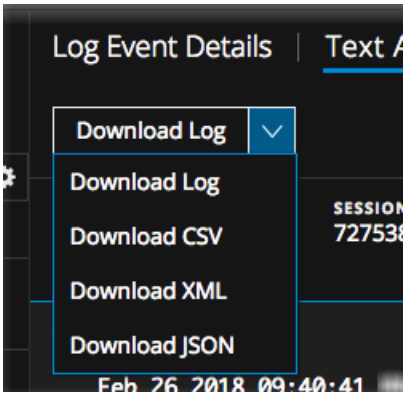
- `<service-ID or host name>`は、セッションが保存されたサービスの名前 (たとえばConcentratorまたはBroker) です。
- `SID<n>`は、セッションID番号です。
- `<filetype>`は、ダウンロードしたログの形式です。ログの形式には、RAWログ、CSV、XML、JSONがあります。デフォルトの形式は、RAWログです。

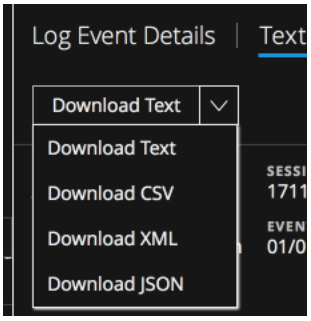
注 : 一部の形式では、タイム スタンプまたはイベントが生成されたデバイスIPが含まれません。このためCSV、XML、JSON形式でダウンロードされたログには、RAWログの内容とともに`timestamp`という追加の値が含まれます。追加の情報は「`Log timestamp="1490824512" source="10.12.35.65"`」形式でログに含まれます。

セッションのログをダウンロードするには、次の手順を実行します。

ログ イベントの[テキスト]パネルで、ダウンロードするログのファイル形式を選択します。

- RAWログ(デフォルト の形 式) としてログをダウンロード するには、[**ログのダウンロード**](または11.4では[**テキスト のダウンロード**]) をクリックします。
- 他 のいずれかの形 式 でログをダウンロード するには、[**ログのダウンロード**](11.3) または[**テキスト のダウンロード**](11.4以 降) ボタンの下 矢 印 をクリックして、ダウンロードしたログのいずれかのファイル形 式 を選 択します。





ログ ファイルは、指 定した形 式 で、ローカル ファイル システムにダウンロード されます。ダウンロードを選 択してから、ダウンロード が開 始 する前 にログを抽 出 している途 中 でブラウザのページを移 動 すると、ログはダウンロード されません。ジョブ キューからログをダウンロード できるというメッセージが通 知 されます。

[テキスト] パネルまたは[パケット] パネルでのネット ワーク イベント データのダウンロード

[パケット] パネルまたは[テキスト] パネルで再 構 築 されたネット ワーク イベントを表 示 しているときに、詳 細 な分 析 用 にネット ワーク データ ファイルをエクスポート することができます。ダウンロードには、現 在 の時 間 範 囲 やドリル ポイント のイベント が含 まれています。次 の形 式 でデータをダウンロード することができます。

- イベント 全 体 をパケット キャプチャ(`*.pcap`) ファイルとして。[**PCAPのダウンロード**]オプションを使 用 。
- ペイロードを`*.payload`ファイルとして。[**すべてのペイロード のダウンロード**](11.3) または[**ペイロード のダウンロード**](11.4) オプションを使 用 。
- リクエスト ペイロードを`*.payload1`ファイルとして。[**リクエスト ペイロード のダウンロード**]オプションを使 用 。

- レスポンス ペイロードを*.payload2ファイルとして。[**レスポンス ペイロード のダウンロード**]オプションを使用。

ダウンロード メニューボタンのラベルは、[イベント環境設定]ダイアログで選択した設定に基づいており、これらの形式のいずれかです。イベントにその日付のタイプがない場合、メニュー ボタンはグレー表示になります。メニュー ボタンをクリックして、どのオプションが使用可能かを確認できます。たとえば、イベントにリクエスト ペイロードがあり、レスポンス ペイロードがない場合、[レスポンス ペイロードのダウンロード]ボタンはグレー表示になります。ボタンをクリックして、[**リクエスト ペイロードのダウンロード**]をこのダウンロードに選択できます。有効な形式を選択した後でボタンをクリックすると、ダウンロードが実行されます。

PCAPファイルのファイル名は「C01 - Concentrator_SID1697309.pcap」のようになります。エクスポートされたネットワーク データ ファイルの名前は、次の規則で決まります。

```
<service-ID or host name>_SID<n>.<filetype>
```

各項目の意味は次のとおりです。

- <service-ID or host name>は、セッションが保存されたサービスの名前(たとえばConcentratorまたはBroker)です。
- SID<n>は、セッションID番号です。
- <filetype>は、pcap、payload、payload1、payload2のいずれかです。

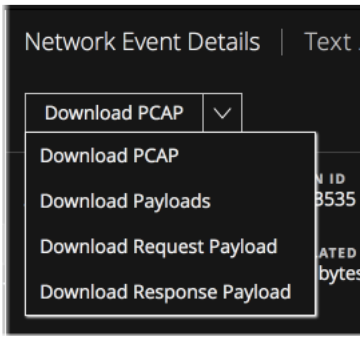
ネットワーク データは、ダウンロードが迅速な場合、ブラウザに直接ダウンロードされます。ネットワーク要因やファイル サイズによりダウンロードに時間がかかる場合、ファイルは、バックグラウンドでダウンロードされ、タスクはジョブキューでトラッキングされます。この場合は、キューでジョブを確認し、ダウンロードが完了するとファイルを取得できます。

注: ダウンロードを選択してから、ダウンロードが開始する前にファイルを抽出している途中でブラウザのページを移動すると、ファイルはダウンロードされません。ジョブ キューからファイルをダウンロードできるというメッセージが通知されます。

イベントをネットワーク データ ファイルにエクスポートするには、次の手順を実行します。

ネットワーク イベントの[パケット]パネルに移動し、[ダウンロード]メニュー ボタンをクリックします。ラベルは、[イベント環境設定]ダイアログで設定されているダウンロード オプションと同じです。選択可能なその他の形式を確認するには、[**ダウンロード**]メニュー ラベルをクリックします。

- イベントをPCAPファイル(システム定義のデフォルト形式)としてダウンロードするか、ユーザ定義のデフォルト形式でダウンロードするには、[**<形式>のダウンロード**]ボタンをクリックします。
- 他のいずれかの形式でイベントをダウンロードするには、ボタン上の下向き矢印をクリックして、ダウンロードしたイベント データのファイル形式を選択します。



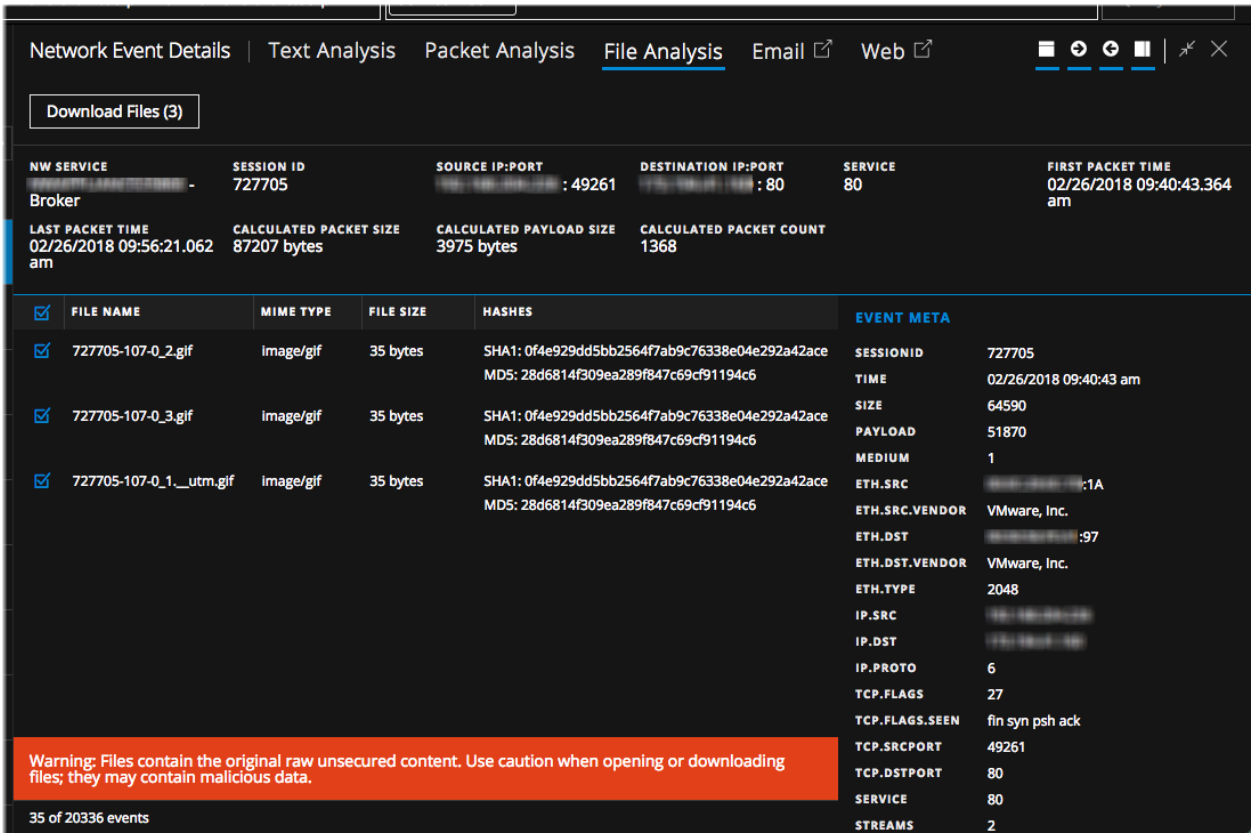
ネット ワーク データ ファイルは、指定した形式で、ローカル ファイル システムにダウンロードされます。

[ファイル] パネルでのネット ワーク イベントからファイルのダウンロード

[ファイル] パネルでファイルを含む再構築ネット ワーク イベント表示しているときに、1つまたは複数のファイル、すべてのファイルを選択してローカル ファイル システムにダウンロードすることができます。

注 : ダウンロードを選択してから、ダウンロードが開始する前にファイルを抽出している途中でブラウザのページを移動すると、ファイルはダウンロードされません。ジョブ キューからファイルをダウンロードできるというメッセージが通知されます。

ファイルを選択したら、[ファイルのダウンロード] ボタンがアクティブになり、選択したファイルの数が反映されます。



[ファイルのダウンロード] をクリックすると、選択したファイルがパスワード保護されたzipアーカイブとしてエクスポートされます。エクスポートされたアーカイブを開くためのパスワードは`netwitness`です。この形式でファイルをエクスポートすることにより、次のことが保証されます。

- アーカイブは、ウイルス対策ソフトウェアによって隔離されません。
- 悪意のある可能性のあるファイルがデフォルトのアプリケーションによって自動的に開かれたり、実行されません。

アーカイブのファイル名は「`C01 - Concentrator_SID1697309_FC1.zip`」のようになります。エクスポートされたアーカイブの名前には、次の規則を使用します。

```
<service-ID or host name>_SID<n>_FC<n>.zip
```

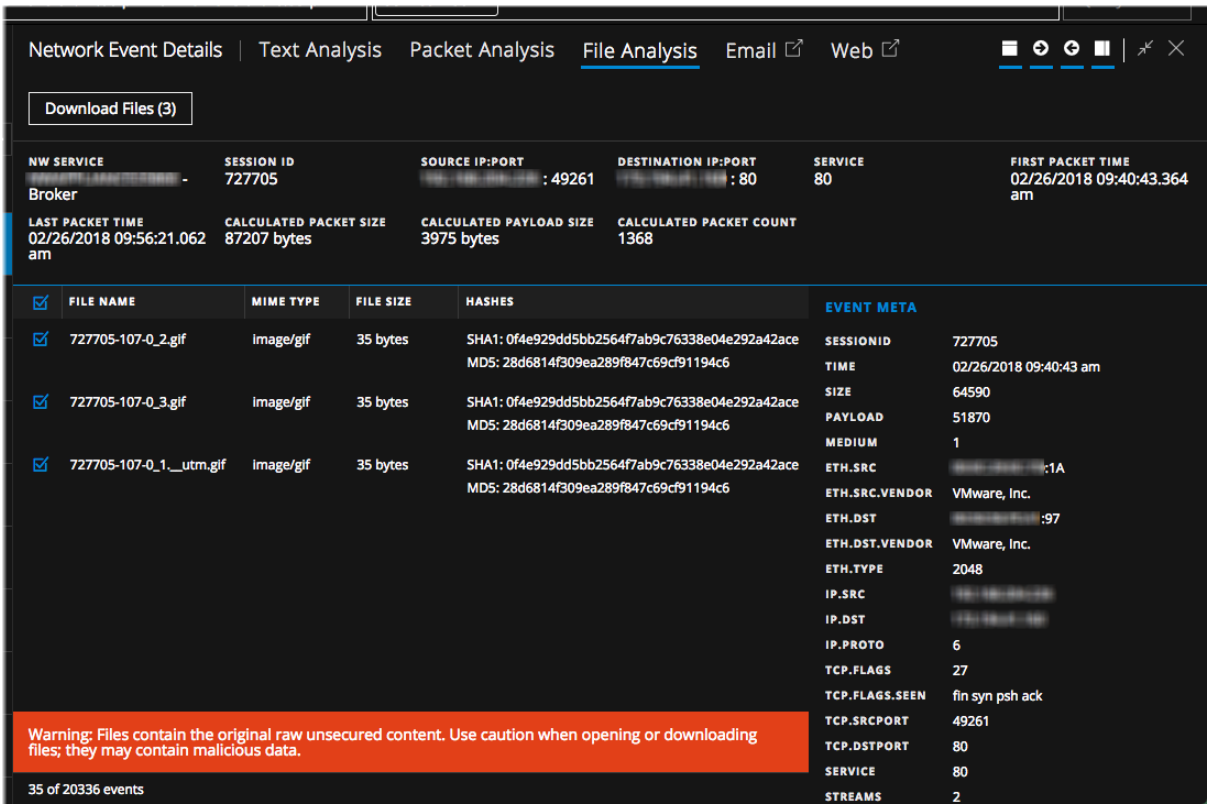
各項目の意味は次のとおりです。

- <service-ID or host name>は、セッションが保存されたサービスの名前(たとえばConcentratorまたはBroker)です。
- SID<n>は、セッションID番号です。
- FC<n>は、ファイル数またはアーカイブ内のファイルの数です。

注意: デフォルトのアプリケーションに関連づけられているファイルを解凍または開くときは、十分に注意してください。たとえば、Excelスプレッドシートは、ファイルの安全性を検証する前にExcelで自動的に開かれる可能性があります。

再構築されたイベントでファイルをエクスポートするには、次の手順を実行します。

1. [**イベント**]ビューで、ファイルを含んでいるイベントの[ファイル]パネルに移動します。



2. 抽出する1つまたは複数のファイルをクリックして、[**単一ファイルのダウンロード**]または[**複数ファイルのダウンロード**]をクリックします。
ジョブがスケジュールされ、完了すると、選択したファイルがパスワード保護されたzipアーカイブ形式でローカル ファイル システムにダウンロードされます。
3. ローカル ファイル システム上のアーカイブを開くには、プロンプトが表示されたら、パスワード netwitnessを入力します:

[ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷

NetWitness Investigationでは、[ナビゲート]ビューにドリルダウン ポイントのデータが表示されている場合、次のタスクを実行できます。

- セッションをファイルに抽出します。抽出するファイルのタイプ(アーカイブ、オーディオBitTorrent、ドキュメント、実行可能プログラム、イメージ、その他、ビデオ、Web) は指定できます。
- ドリルダウン ポイントをパケット キャプチャ(PCAP) ファイル、ログ ファイル、メタデータ ファイルとしてエクスポートします。
- ドリルダウン ポイントを印刷します。

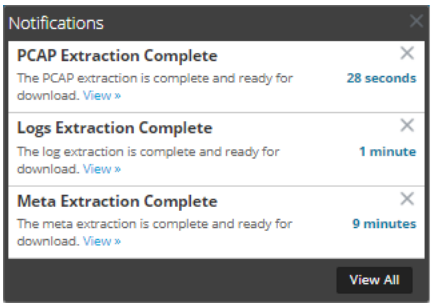
エクスポートされる内容は、エクスポートするときの時間範囲やドリルダウン ポイントによって変わります。

注: ドリルダウン ポイントをログ ファイルとしてエクスポートするときは、ログ セッションのみがエクスポートされます。ジョブのキューのメッセージでは、ログの数ではなく、ドリルダウン ポイントのセッションの数を参照します。たとえば、ドリルダウン ポイントに505のセッションがあり、またログ セッションは5つしかない場合、ジョブのキューのメッセージにはNetWitness Platformが505のセッションに対して5つのログを抽出していると表示されます。

[ナビゲート]ビューからドリルダウン ポイントをエクスポートするには、次の手順を実行します。

1. 目的のドリルダウン ポイントに達するまで調査を実施します。
2. バージョン11.0の場合は、ツールバーで**[アクション]**>**[エクスポート]**を選択し、[**PCAP**]、[**ログ**]、[**メタ**]のいずれかのエクスポート オプションを選択します。
   ドリルダウン ポイントが抽出され、ジョブがスケジュール設定されたことを示すメッセージが表示されます。ジョブのステータスについては、[ジョブ]ページを確認できます。
3. バージョン11.1の場合は、ツールバーで[**イベントの保存**]を選択し、[**PCAP**]>[**ログ**]>[**ファイル**]>[**メタ**]のいずれかのエクスポート オプションを選択します。
   ダイアログが表示され、ファイルのデフォルト ファイル名を編集できるようになります。デフォルトのファイル名のフォーマットは`investigation-Feb-21-15-44-33`です。PCAPをエクスポートする場合、ファイルはフォーマットの選択なしでエクスポートされます。他のエクスポート オプションのいずれかを使用している場合は、ダイアログが表示されます。
4. ダイアログで、次を選択します。
   - エクスポート ログの形式: **テキスト**、**XML**、**CSV**、**JSON**。
   - エクスポートするファイル タイプ: アーカイブ、音声、BitTorrent、ドキュメント、実行可能ファイル、イメージ、その他、動画、Webなど。
   - メタ形式: **テキスト**、**CSV**、**TSV**、**JSON**。

5. スケジュール設定されたファイルの抽出が完了すると、ジョブ通知トレイに表示されます。



6. [**自分のジョブを表示**]リンクをクリックしてジョブ トレイを開き、リクエストした抽出ファイルをダウンロードします。

現在のドリルダウン ポイントを印刷するには、次の手順を実行します。

[ナビゲート]ビューでは、現在のドリルダウン ポイントの内容を印刷しやすい形式でブラウザ ウィンドウに表示することができます。

現在のドリルダウン ポイントを印刷ビューで表示するには、次の手順を実行します。

1. [**ナビゲート**]ビューでドリルダウン ポイントが開いている状態で、ツールバーで[**アクション**]＞[**印刷**]を選択します。
新しいタブが作成され、現在のドリルダウン ポイントの印刷ビューが表示されます。

2. 印刷ビューをプリンタに送信するには、ブラウザの印刷オプションを使用してください。

[レガシー イベント]ビューでのイベントのエクスポート

[レガシー イベント]ビューの[アクション]メニューには、表示中のイベントからアーカイブにイベントをエクスポートするオプションがあります。

注: 表示またはアクセスの権限を持つファイルのみをエクスポートできます。

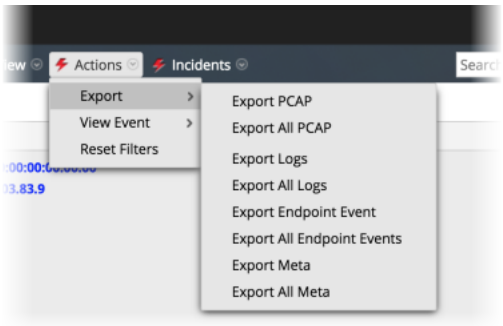
エクスポート機能では、サービスのクエリを実行し、選択した時間範囲とドリルダウン ポイントで指定したセッションをPCAPファイルにエクスポートします。エクスポートされる内容は、エクスポートするときの時間範囲やドリルダウン ポイントによって変わります。[ファイルの抽出]ダイアログでは、次の項目を選択してエクスポートできます。

- PCAP
- ログ
- NetWitness EndPointイベント
- メタ値

エクスポートされるアーカイブの形式(ZIPまたはGZIPファイル)。リクエストを送信すると、ジョブがスケジュールされ、ジョブ トレイでそのジョブのトラッキングができます。ログまたはPCAPをサービスから取得する際にエラーが発生すると、エラー通知が表示されます。

イベントからファイルを抽出するには、次の手順を実行します。

1. **[イベント]ビュー**で、イベントをクリックします。
2. **[アクション]＞[エクスポート]**をクリックします。



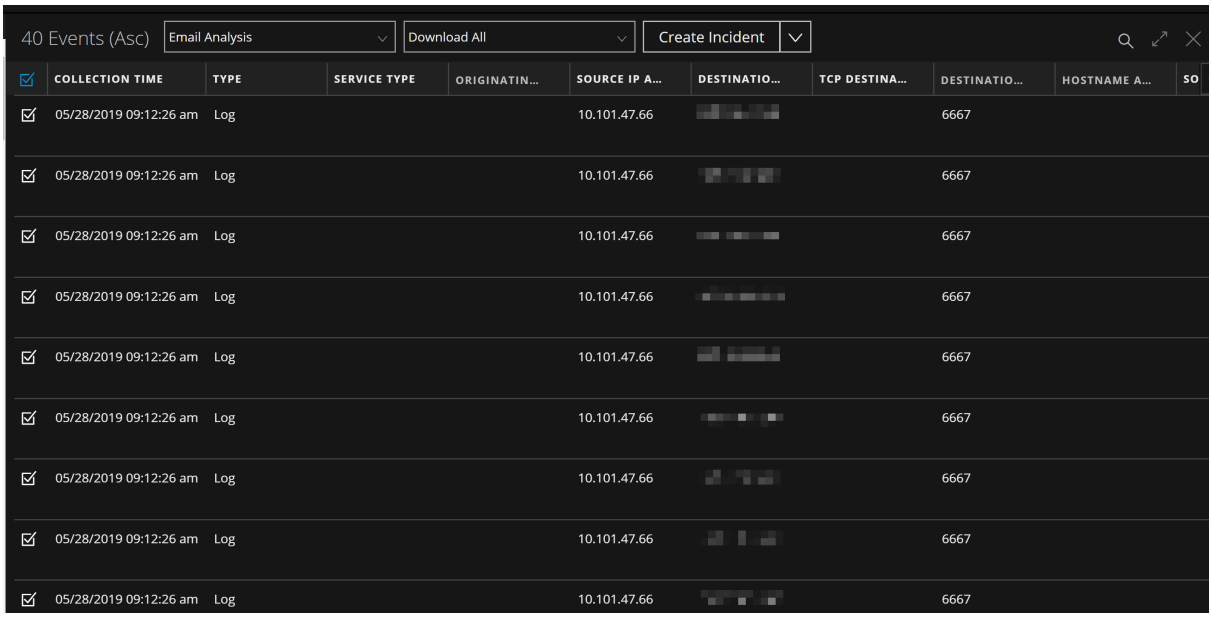
3. エクスポート オプションを選択します。
   PCAPがダウンロード中であることを示すメッセージが表示されます。

[イベント]ビューでのインシデントへのイベントの追加

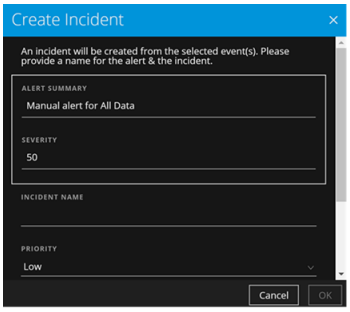
[イベント]ビューで調査を行うときに、1つ以上のイベントを選択して、インシデント対応者がRespondで利用可能なインシデントを作成できます。アクセス制限が有効になっている場合、インシデントの作成時に表示できるのは、自分がアクセス権を持っているインシデントのみです。たとえば、[調査]ビューからインシデントを作成する場合、アナリストはインシデントを自分に割り当てて、それらを[対応]ビューに表示する必要があります。また、アクセス権のある既存のRespondのインシデントにイベントを追加することもできます。

注： 管理者は、`respond-server.incident.manage`および`investigate-server.incident.manage`のロールと権限を構成する必要があります。詳細については、『*システム セキュリティとユーザ管理ガイド*』の「ロールの権限」と「ロールと権限によるユーザの管理」を参照してください。

1. **[調査]＞[イベント]**に移動します。
2. [イベント]ビューで、1つ以上のイベントを選択します。



3. [**インシデントの作成**]をクリックします。
[インシデントの作成]ダイアログが表示されます。[インシデントの作成]ダイアログに情報を入力します。



a. 重大度を選択します。アラート サマリー フィールドの値は事前に定義されており、自動入力されますが、必要に応じて編集することができます。

b. [**インシデント名**]フィールドに、インシデントの名前を入力します。

c. [**優先度**]ドロップダウン リストから、インシデントの優先度を選択します。たとえば、インシデントはクリティカル、高、中、低の優先度の場合があります。

d. インシデントの割り当て先をドロップダウン リストから選択します。このリストには、調査にアクセスできる組み込みのユーザと、システムに追加されたカスタム ユーザが含まれます。たとえば、このリストには、管理者、アナリスト、DPO、オペレーターのユーザや、インシデント対応担当者のユーザが含ま

れている場合があります。

e. [カテゴリー]ドロップダウン リストから、このインシデントに適用するイベントのカテゴリーを1つ以上選択します。

f. [**OK**]をクリックします。
調査で選択したイベントを使用してインシデントが作成されます。

4. 1つ以上のイベントを既存のインシデントに追加するには、1つ以上のイベントを選択してから、[**インシデントに追加**]をクリックします。

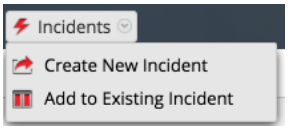
5. [インシデントに追加]ダイアログで、アラート サマリーと重大度を選択し、インシデントの追加先にする1つ以上の既存の未解決インシデントを選択します。インシデントIDまたはインシデント名で既存のインシデントを検索できます。準備が完了したら、[**OK**]をクリックします。選択したインシデントにイベントが追加され、Respondで更新されます。

[レガシー イベント]ビューでのインシデントへのイベントの追加

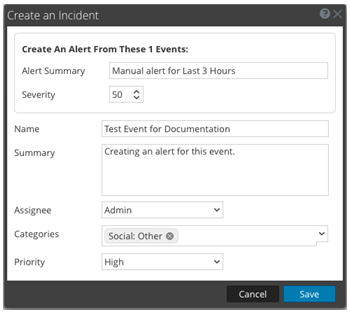
レガシー イベントで調査を行うときに、1つ以上のイベントを選択して、インシデント対応者がRespondで利用可能なインシデントを作成できます。アクセス制限が有効になっている場合、インシデントの作成時に表示できるのは、自分がアクセス権を持っているインシデントのみです。たとえば、[調査]ビューからインシデントを作成する場合、アナリストはインシデントを自分に割り当てて、それらを[対応]ビューに表示する必要があります。また、アクセス権のある既存のRespondのインシデントにイベントを追加することもできます。

注: 管理者は、『*システム セキュリティとユーザ管理ガイド*』にある「ロールの権限」と「ロールと権限によるユーザの管理」の説明に従って必要なロールと権限を設定する必要があります。

1. **[調査]** > **[レガシー イベント]**に移動します。
2. [レガシー イベント]ビューで、1つ以上のイベントを選択してから、**[インシデント]** > **[新しいインシデントの作成]**を選択します。



3. [インシデントの作成]ダイアログに情報を入力します。



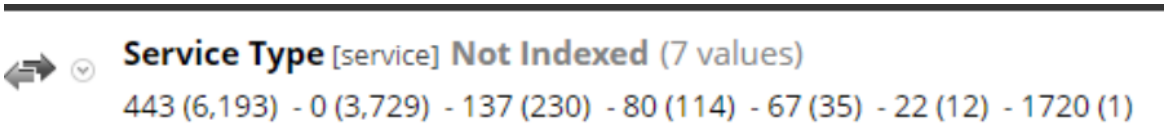
   a. 重大度を選択します。重大度は1～100の整数で、100が最も重大です。
   b. インシデントの名前を入力し、[**サマリー**]フィールドにインシデントの説明を入力します。
   c. インシデントの割り当て先をドロップダウン リストから選択します。このリストには、Respondにアクセスできる組み込みのロールと、システムに追加されたカスタム ロールが含まれます。たとえば、このリストには、管理者、アナリスト、DPO、オペレーターのロールや、インシデント対応担当者のロールが含まれている場合があります。
   d. [**カテゴリー**]ドロップダウン リストから、このインシデントに適用するアラートのカテゴリーを1つ以上選択します。
   e. [**優先度**]ドロップダウン リストから、インシデントのカテゴリーを選択します。たとえば、インシデントはクリティカル、高、中、低の優先度の場合があります。
   f. [**保存**]をクリックします。
   新しいインシデントが作成され、Respondの選択されたロールのインシデント キューですぐに利用できるようになります。

4. 1つ以上のイベントをインシデントに追加するには、1つ以上のイベントを選択してから、[**インシデント**]＞[**既存のインシデントへの追加**]を選択します。
5. [イベントをインシデントに追加]ダイアログで、重大度を選択し、イベントが追加される1つ以上のインシデントを選択します。インシデントIDまたはインシデント名で既存のインシデントを検索できます。準備ができたら、[**インシデントへの追加**]をクリックします。
   選択したインシデントにイベントが追加され、Respondで更新されます。

NetWitness Investigateのトラブルシューティング

このセクションでは、NetWitness Investigateの使用時に発生する可能性のある問題について説明します。

[ナビゲート]ビューおよび[レガシー イベント]ビューの問題

動作	通常、[ナビゲート]ビューで値を返すメタ キーは値を返しますが、メタ キー名の後に「`Not Indexed`」というメッセージが表示されます。たとえば、次の図のように、Service Typeメタ キーの後に「`Service Type[service] Not Indexed`」というメッセージが表示されます。 
問題	環境を初めてセットアップしたとき、または、稀にですが他の問題が原因でBrokerでデータ リセットを実行したときに、メタ キーがメタ キー レベルまたはメタ値レベルでインデックスされているにもかかわらず、インデックスなしと表示されます。
説明	Brokerの問題を解決するには、NetWitness Platformからログアウトして、もう一度ログインします。有効なセッションが表示されます。

メッセージ	`Not indexed; will experience longer than usual load times.`([メタ グループの管理]ダイアログ)
問題	[メタ グループの管理]ダイアログボックスのメタ キーが赤い感嘆符でマークされ、エラー メッセージが表示されます。これは、BrokerまたはDecoderを調査していて、サービスのインデックス ファイルまたはカスタム インデックス ファイルでインデックスされていないメタ キーを含むメタ グループを追加するときに発生する可能性があります。 Brokerの場合、それはBrokerがConcentratorからデータを集約し始めていないことを意味する可能性があります。この場合、Brokerは、集約サービスからのカスタム索引ファイルのコンテンツを持たず、キーは索引付けされません。 Decoderの場合、メタ キーがDecoderインデックスまたはカスタム インデックス ファイルでインデックスされていないことを意味します。
説明	Brokerで問題を解決するには、Brokerサービスからログアウトして、ログインし、再始動します。これで、接続されたConcentratorからメタ キー情報を集約できるようになります。Decoderの問題を修正するには、カスタム インデックス ファイルを編集してメタ キーのインデックスを作成し、Decoderサービスからログアウトして、ログインし、再起動します。

動作	[イベントの再構築]ビューからログおよびメタデータをダウンロードすると、[レガシー イベント]ビューで選択した形式に関係なく常にテキスト形式になります。
問題	[イベントの再構築]ビューでメタデータまたはログをダウンロードすると、[レガシー イベント]ビューで選択した形式が使用されません。エクスポートしたデータは、常にテキスト形式になります。
説明	テキスト形式以外の形式を使用する場合は、[レガシー イベント]ビューからメタデータとログをダウンロードします。

[イベント]ビューの問題

メッセージ	`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`
問題	[イベント]ビューで[**エンドポイントに移行**]をクリックすると、データが表示されず、メッセージが表示されます。
説明	バージョン4.4のNetWitness Endpoint Thick Clientを、同じサーバにインストールする必要があります。NWEメタ キーがLog Decoderの`table-map.xml`ファイルとConcentratorの`index-concentrator-custom.xml`ファイルに存在する必要があります。NWE Thick Clientは、Windowsのみのアプリケーションです。完全なセットアップ手順は、バージョン 4.4の『*NetWitness Endpointユーザ ガイド*』を参照してください。

動作	ダウンロード ジョブは、バージョン11.4へのソフトウェアのアップグレード中およびアップグレード後に、ジョブ トレイで待機状態または失敗状態になります。
問題	管理者によってソフトウェアがアップグレードされている間に、ダウンロード ジョブを実行していた場合は、アップグレードの進行中にジョブが待機状態で表示され、アップグレードの完了後に失敗状態で表示されることがあります。失敗したジョブを再開またはキャンセルすることはできません。
説明	失敗したジョブを削除するには、失敗したジョブをジョブ トレイで選択して、 をクリックします。

メッセージ	`Event Analysis requires all core services to be NetWitness 11.1. Connecting prior versions of services to the 11.1 NetWitness Server results in limited functionality (see "Investigate in Mixed Mode" in the *Physical Host Upgrade Guide*).`
問題	[イベント分析]ビューでバージョン11.1に更新されていないサービスを調査する場合、情報メッセージが表示されます。

説明	アナリストが混在モード(つまり、一部のサービスは11.1以降にアップグレードされているが、一部のサービスは11.0.0.xまたは10.6.xのまま) で[イベント分析]ビューを開くと、RBAC(ロールによるアクセス制御) が一律に適用されません。これは、コンテンツの表示とダウンロード、対話形式で階層リンクを操作する時のフィルタの検証に影響します。この情報メッセージは、[イベント]を開くときに表示されます。サービスを選択するとき、最新でないサービスは赤いボックスの中に表示され、サービスが最新でないというメッセージが表示されます。管理者が、接続されたすべてのサービスを11.1以降にアップグレードすると、これらの機能は正常に動作します。

メッセージ	`Forbidden. You cannot access the requested page.`
問題	[イベント]ビューにアクセスしようとすると、このメッセージが表示されます。
説明	[イベント]ビューにアクセスできないよう、管理者によってロールと権限が変更されました。

動作	[イベント]ビューでイベントをダウンロードできるが、0バイトのファイルが取得される場合は、管理者によってコンテンツへのアクセスが制限されている可能性があります。
問題	管理者によって適用されたロールベースのアクセス制御により、権限のないイベントをダウンロードできました。そのため、ダウンロードされたファイルは空でした。
説明	イベントにアクセスする必要があると考えられる場合は、管理者に連絡してください。

メッセージ	`Insufficient permissions for the requested data.`
問題	[イベント]ビューでイベントにアクセスしようとすると、このメッセージが表示されます。
説明	表示する権限がないイベントのイベントIDを入力しました。アクセスを制限するために、管理者がロールと権限により制限を設けた可能性があります。

メッセージ	`Invalid session ID: <<eventId>>`
問題	クエリ対象の`sessionId`と一致する`sessionId`がありません。
説明	無効なセッションIDが発生した原因はいくつか考えられます。例えば、手動でセッションIDを入力したが、そのようなセッションが存在しない可能性があります。また、Brokerに対してクエリを実行する場合、集計されたデータがしばらく更新されていないと、既に存在しなくなったセッションについてこのエラーが表示される可能性があります。

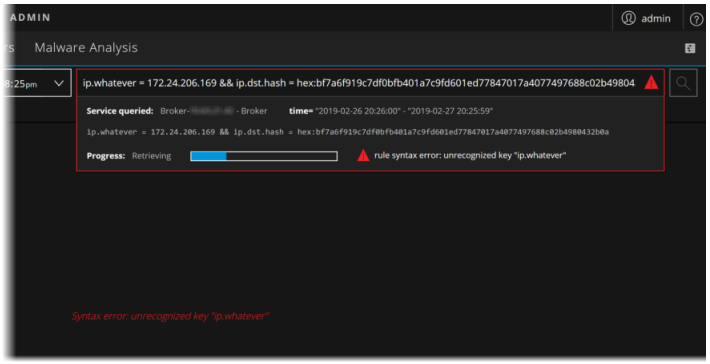
動	11.1のイベント分析に、調査プロファイルと標準提供の列グループが存在しません。

作	
問題	RSA NetWitness v11.1へのアップグレード後、デフォルトの列グループ(Endpoint Analysis、Outbound SSL、Outbound HTTP) が列グループに追加されていません。また、アップグレード後に一部の調査プロファイルが見つかりません。
説明	この問題は、11.1で新しく追加された標準提供の列グループと同じ名前でカスタム列グループを作成していた場合にのみ発生します。たとえば、11.0で「**RSA Endpoint Analysis**」というカスタム列グループを作成し、その後11.1へアップグレードしたとします。11.1には同じ名前が存在するため、標準提供の列グループとプロファイルがUIに表示されません。 この問題を解決するには、カスタム列グループの名前を標準提供の列グループと異なる名前に変更した後、NetWitness Serverで次のコマンドを実行して、jettyサーバを再起動します。 `systemctl restart jetty`

メッセージ	`Memory limit of <XXXXXX> GB reached, controlled by setting max.query.memory`
問題	結果セットが大きすぎて、`max.query.memory`で設定されたメモリ制限に達したため、送信したクエリが失敗しました。
説明	このエラーを回避するには、時間範囲の絞り込み、フィルタの追加、列グループの列数の削減によって、さらに結果を絞り込むようにします。また、返されるイベントの数を制限することを管理者に対して要求することもできます。

動作	コンテンツの再構築ではテキスト データは生成されませんでした。イベント データが破損しているか不正な可能性があります。または、管理者がEndpoint Serverの構成でエンドポイントのRAWイベントの送信を無効化している可能性があります。他の表示で再構築してください。
問題	[イベント]ビューでイベントをテキストとして再構築するとき、データが表示されず、このメッセージが表示されます。
説明	他の[イベント]ビューや[レガシー イベント]ビューの再構築でもRAWテキストが表示されず、データが破損していない、または無効でないと思われる場合、管理者がNetWitness Endpoint サーバでRAWエンドポイント イベントの送信を無効化した可能性があります。詳しくは、管理者にお問い合わせください。

メッセージ	`Rule Syntax error: Unrecognized key "<meta key or meta entity name>"` `Syntax error: Unrecognized key "<meta key or meta entity name>"`
問題	サービスのクエリ中、一致するイベントが表示されず、メッセージがクエリコンソールと[イベント]ビューに表示されます。

	
説明	入力したクエリは、正しく構成されていないメタ エンティティに対して実行されています。クエリ対象のBrokerに接続されているすべての上流デバイスに、同じエンティティ構成がなければなりません。このエラーは、エンティティ定義に不一致がある状態でBrokerが動作していることを示しています。『*Core データベース チューニング ガイド*』の「インデックスのカスタマイズ」で説明されている構成を確認するよう、管理者に依頼してください。

メッセージ	`Selected Column Group is no longer available. The default summary column group has been selected instead.`
問題	11.4にアップグレードする前に優先的に使用する列グループを設定していた場合、[イベント]ビューに初めてアクセスしたときに、列グループが使用可能またはデフォルト グループ(サマリー) であっても、フラッシュ メッセージが表示されます。この問題は、バージョン11.4.1で解決されました。
説明	この問題は一度だけ発生します。[イベント]ビューを再ロードすると、メッセージは表示されません。

メッセージ	`Session is unavailable for viewing.`
問題	イベントIDでクエリを実行した時に、イベントの再構築が表示されず、このメッセージが表示されます。
説明	入力したクエリは、制限されたデータを照会しようとしています。たとえば、ログ データの表示しか許可されていないときに、ネットワーク データへのリンクを使用しています。

メッセージ	`The query on channel <channel-number> was auto-canceled by the system for exceeding time usage limits. Check timeout values. Query running time was 00:05:00 (HH:MM:SS)`
問題	このタイムアウト メッセージが頻繁に表示される場合は、まずクエリコンソールを確認して、サービスの応答に要する時間の問題やインデックス エラー メッセージなど、クエリのレスポンス タイムを増やすために対処すべき警告があるかどうかを調べます。
説明	特定の警告を示すメッセージが表示されていない場合は、『*システム セキュリティとユーザ管理 ガイド*』の説明に従って、コア クエリ タイムアウトを5分から10分に増やすよう管理者に依頼し

	てください。

メッセージ	`The session id is too large to be handled:<<eventId>`
問題	[レガシー イベント]ビューまたは[ナビゲート]ビューで入力または取得したセッションIDが大きすぎます。
説明	[イベント]ビューでsessionIdを手動で入力したか、sessionIdを編集した場合、[イベント]ビューで処理するには大きすぎる整数値を指定した可能性があります。

動作	[イベント]ビュー>[パケット]パネルで大量のパケット(250個超)を使用してネットワーク イベントを再構築するときに、有効なペイロードのみを表示するオプションが有効になっており、ページあたりのパケット数の設定がデフォルト値(100個)を上回った場合、現在のブラウザ タブがペイロードの表示を処理している間、最大45秒間応答しません。
問題	クライアント マシンのリソース(メモリとCPU)の量とイベントのパケット数によっては、パケットの再構築でペイロードのみを表示すると、パフォーマンスが低下する場合があります。
説明	単一のイベントの再構築で処理されるデータの量を制限するには、フッターの[ページあたりのパケット数]設定を低い値に変更します。 

動作	バージョン11.4の[イベント]ビューで作業しているときに、[クエリ プロファイル]ドロップダウン メニューと[列グループ]ドロップダウン メニューが機能しません。
問題	列グループとプロファイルの読み取り権限がありません。デフォルトの列グループであるサマリー リストは[イベント]リストに適用され、列グループの変更、作成、削除はできません。
説明	この問題は、デフォルトのアナリスト ロールを割り当てる代わりに、管理者がカスタム ロールを作成した場合にのみ発生します。列グループの読み取りおよびプロファイルの読み取り権限をロールで有効にするよう管理者に依頼してください。

調査の参考情報

このセクションでは、NetWitness [調査]ビューの目的と用途について説明します。各ビューについて、その概要と、関連する手順へのリンクが記載された「実行したいことは何ですか？」の表を示します。また、参考情報の一部には、ワークフローと、ユーザ インタフェースでの重要な機能をハイライト表示するクイック ルックが含まれます。

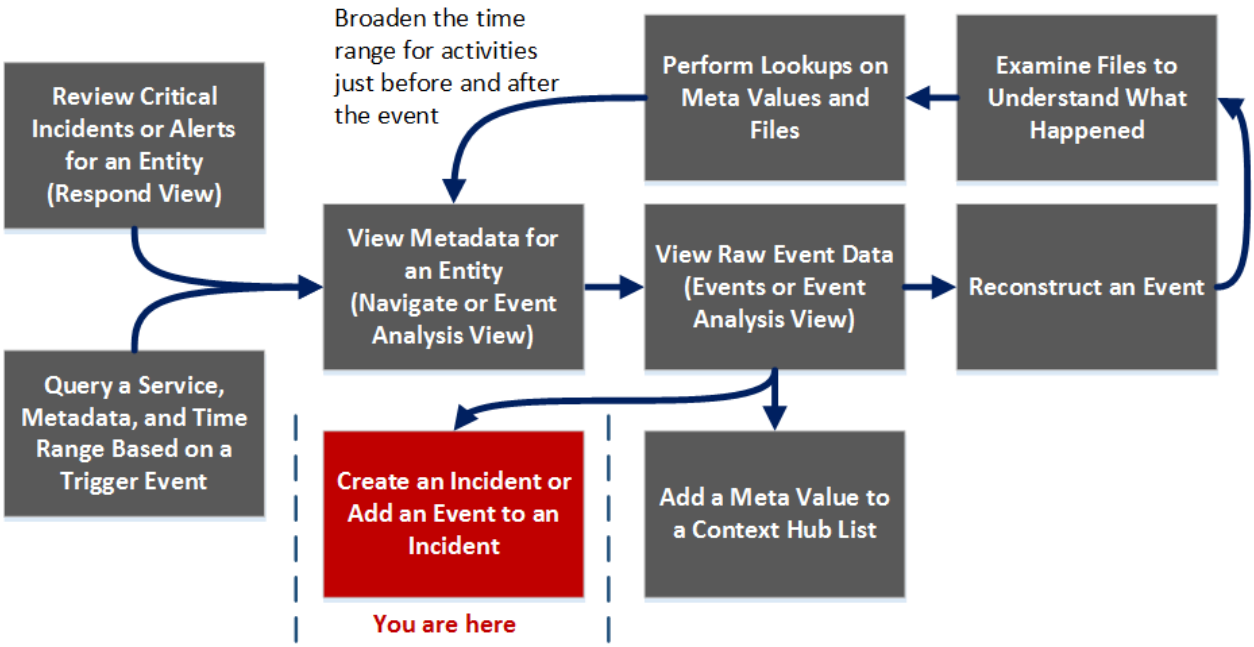
- [調査]ビュー
- [ナビゲート]ビュー
- [レガシー イベント]ビュー
- [イベント]ビュー
- [リストへの追加/削除]ダイアログ
- [イベントをインシデントに追加]ダイアログ
- [列グループ]ダイアログ
- [コンテキスト ルックアップ]パネル
- [インシデントの作成]ダイアログ
- [イベント]ビュー - [メール]パネル
- [イベント]ビュー - [テキスト]パネル
- [イベント]ビュー - [パケット]パネル
- [イベント]ビュー - [ファイル]パネル
- [調査]ダイアログ
- [調査]タブ: [ユーザ環境設定]パネル
- [レガシー イベントの再構築]ビュー
- [デフォルトのメタ キーの管理]ダイアログ
- [メタ グループの管理]ダイアログ
- [ナビゲート]ビュー
- [クエリ]ダイアログ
- [クエリ プロファイル]ダイアログ
- [調査]ビューの設定ダイアログ

[イベントをインシデントに追加]ダイアログ

[イベントをインシデントに追加]ダイアログで、アナリストは、インシデント対応者がインシデント対応時に関連するイベントを確認できるよう、既存のインシデントにアラートとして追加することができます。[イベント]ビューと[レガシー イベント]ビューでのサービスの調査中にこのダイアログにアクセスするには、「[イベント]ビューでのインシデントへのイベントの追加」と「[レガシー イベント]ビューでのインシデントへのイベントの追加」を参照してください。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング

ユーザ ロール	実行したいこと	手順
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加*	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加	結果の追加のコンテキストを検索

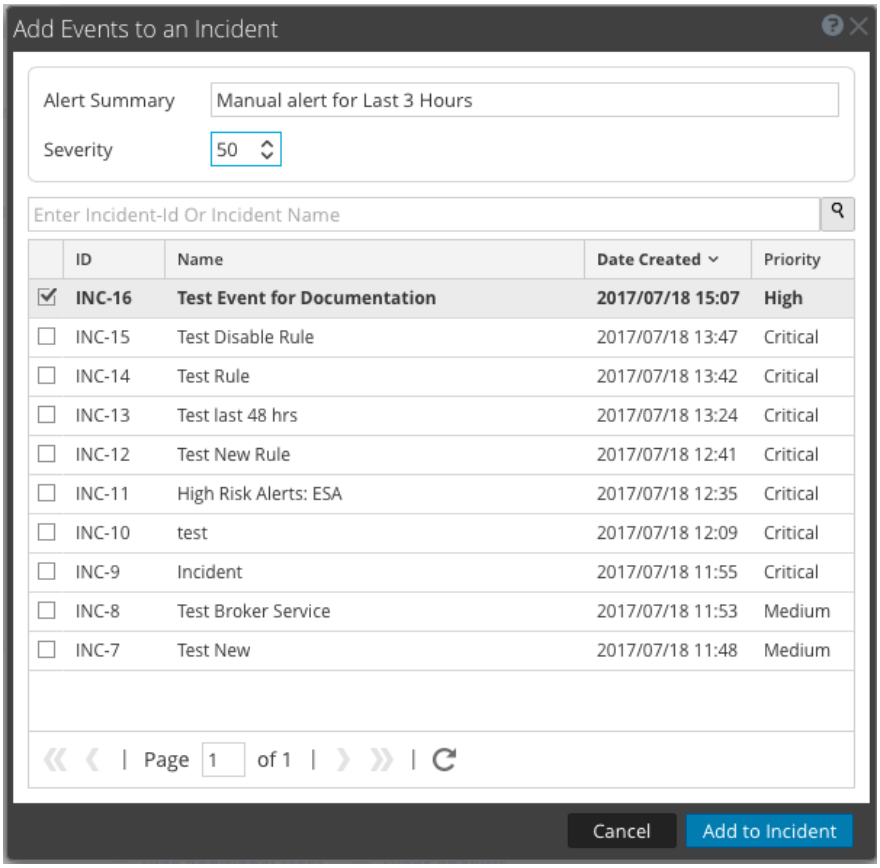
*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー
- [レガシー イベント]ビュー

簡単な説明

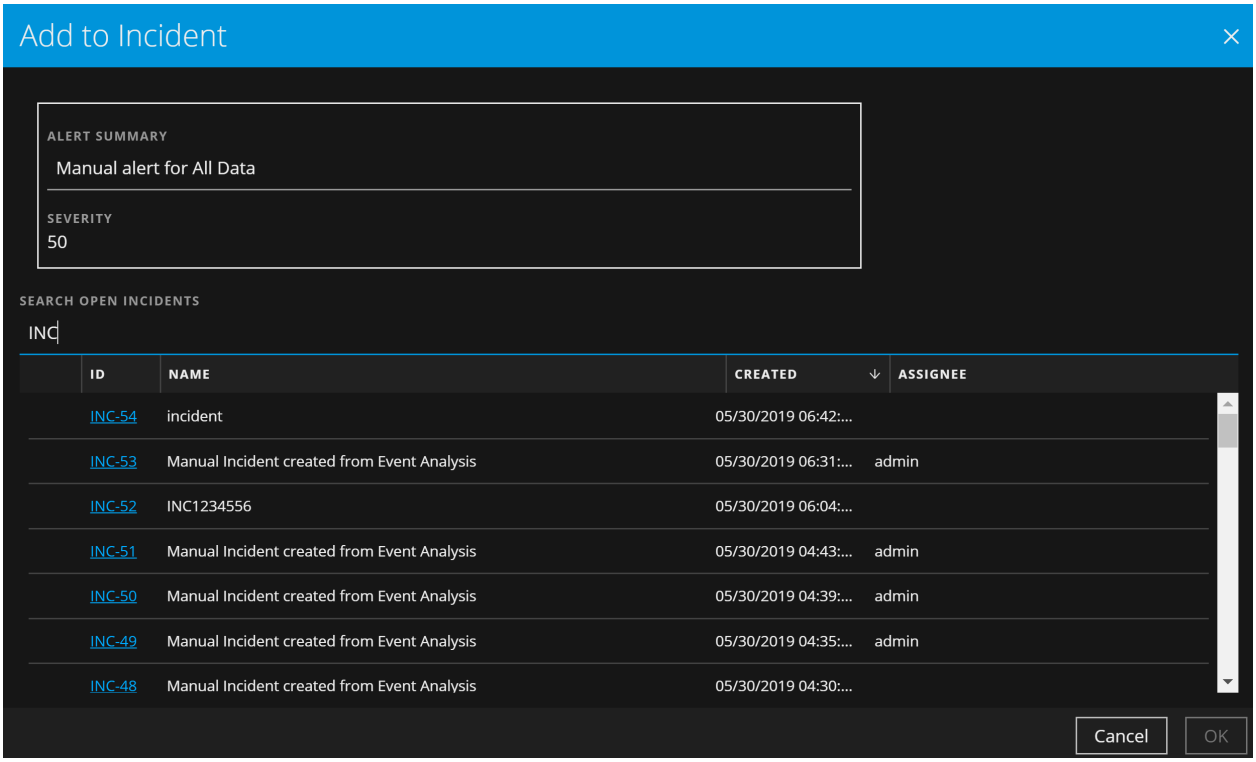
次の図は、レガシー イベントの[イベントをインシデントに追加]ダイアログの例です。表に、[イベントをインシデントに追加]ダイアログの情報およびオプションについて説明します。



機能	説明
アラート サマリ	[アラート サマリ]フィールドには、アラートを選択した時のクエリが自動入力されます。これは、このインシデントを作成する時に選択されていたクエリです。[重大度]フィールドには、選択したアラートの重大度として、1~100の整数が示されます。
検索	既存のインシデントを検索できます。
ID	インシデントのID。IDは昇順または降順にソートできます。
名前	インシデントの名前。名前は昇順または降順にソートできます。
作成日	インシデントが作成された日時が表示されます。日付は昇順または降順にソートできます。
優先	インシデントの優先度として[低]または[クリティカル]が表示されます。
キャンセル	変更を保存せずにダイアログを閉じます。

機能	説明
インシデントへの追加	アラートをインシデントに追加します。ダイアログには、アラートが正常に追加されたことが示されます。

次の図は、[イベント]ビューの[インシデントへの追加]ダイアログの例です。表に、[インシデントへの追加]ダイアログの情報およびオプションについて説明します。



機能	説明
アラート サマリ	[アラート サマリ]フィールドには、アラートを選択した時のクエリが自動入力されます。これは、このインシデントを作成する時に選択されていたクエリです。
重大度	[重大度]フィールドには、選択したアラートの重大度として、1~100の整数が示されます。
未解決インシデントの検索	既存のインシデントを検索できます。
ID	インシデントのID。
名前	インシデントの名前。
作成日時	インシデントが作成された日時が表示されます。
割り当て先	インシデントに現在割り当てられているチームのメンバーが表示されます。
キャンセル	変更を保存せずにダイアログを閉じます。

機能	説明
OK	アラートをインシデントに追加します。インシデントが正常に追加された後で、確認メッセージが表示されます

[リストへの追加/削除]ダイアログ

[リストへの追加/削除]ダイアログを使用すると、既存のContext Hubリストに対してエンティティもしくはメタ値を追加し、エンティティもしくはメタ値を削除し、またはエンティティもしくはメタ値を含む新しいContext Hubリストを作成できます。疑わしいIPアドレスや注意が必要なIPアドレスやその他のエンティティを見つけたときは、データ ソースとして追加されているリストにそのIPアドレスを追加できます。一般的に使用されるリストには、ホワイト リストやブラック リストがあります。これにより、疑わしいIPアドレスの可視性が向上し、誤検知が減るため、余計な調査の必要がなくなります。

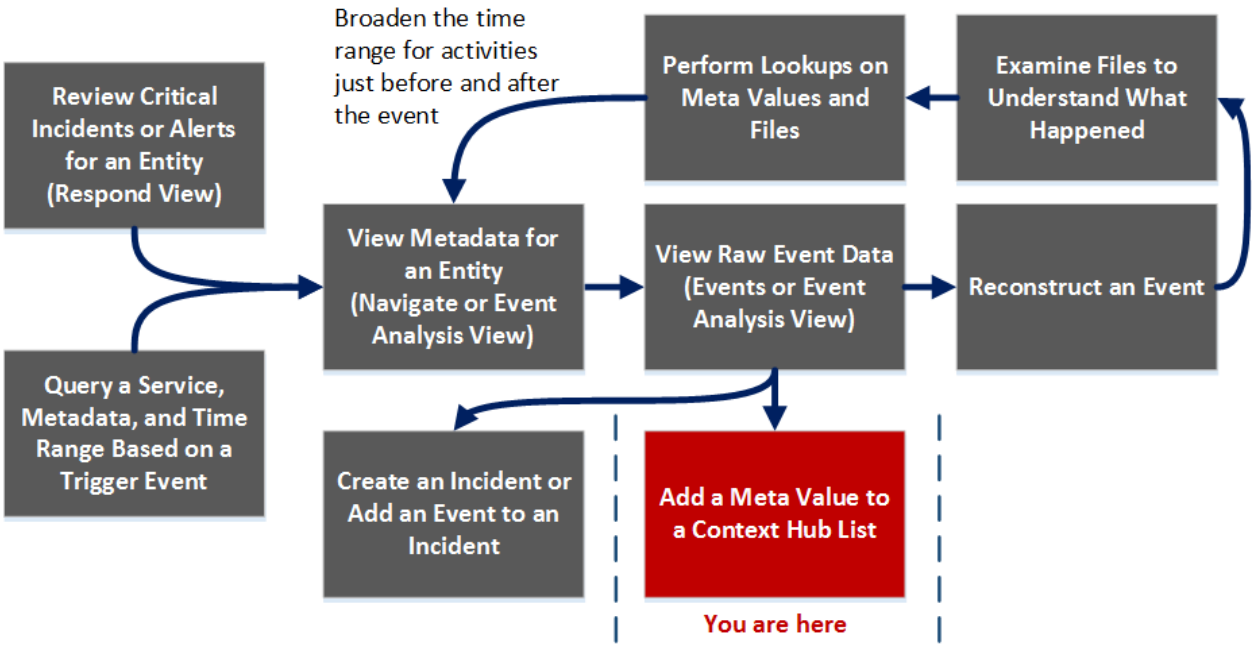
複数のリストにエンティティまたはメタ値を追加できます。たとえば、コマンド&コントロール接続に関連する問題のあるドメインのリストに追加し、別のリモート アクセスに関連するトロイの木馬接続のIPアドレスのリストにも追加することができます。リストがない場合は、リストを作成できます。

このダイアログは、NetWitness InvestigateおよびNetWitness Respondで使用できます。Investigateで作業しているときに、[ナビゲート]ビュー、[レガシー イベント]ビュー、または[イベント]ビューで、Source IP、Destination IP、またはUsernameメタ キーのメタ値を既存のContext Hubリストに追加したり、メタ値を含む新しいリストを作成したりできます。リストにメタ値を追加すると、それらのメタ値に関する追加のコンテキストを検索することができます。

- [ナビゲート]ビューや[レガシー イベント]ビューでダイアログを表示するには、Source IP、Destination IP、またはUsernameのメタ値を右クリックし、コンテキスト メニューで[**リストへの追加/削除**]を選択します。
- [イベント]ビューでダイアログを表示するには、値にカーソルを合わせ、コンテキスト ツールチップのアクション セクションで[**リストへの追加/削除**]を選択します。

ワークフロー

次のワークフロー図は、「リストへの追加」タスクがハイライト表示された調査のワークフローを示しています。このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築

ユーザ ロール	実行したいこと	手順
脅威ハンター	ファイルの検証	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加*	結果の追加のコンテキストを検索

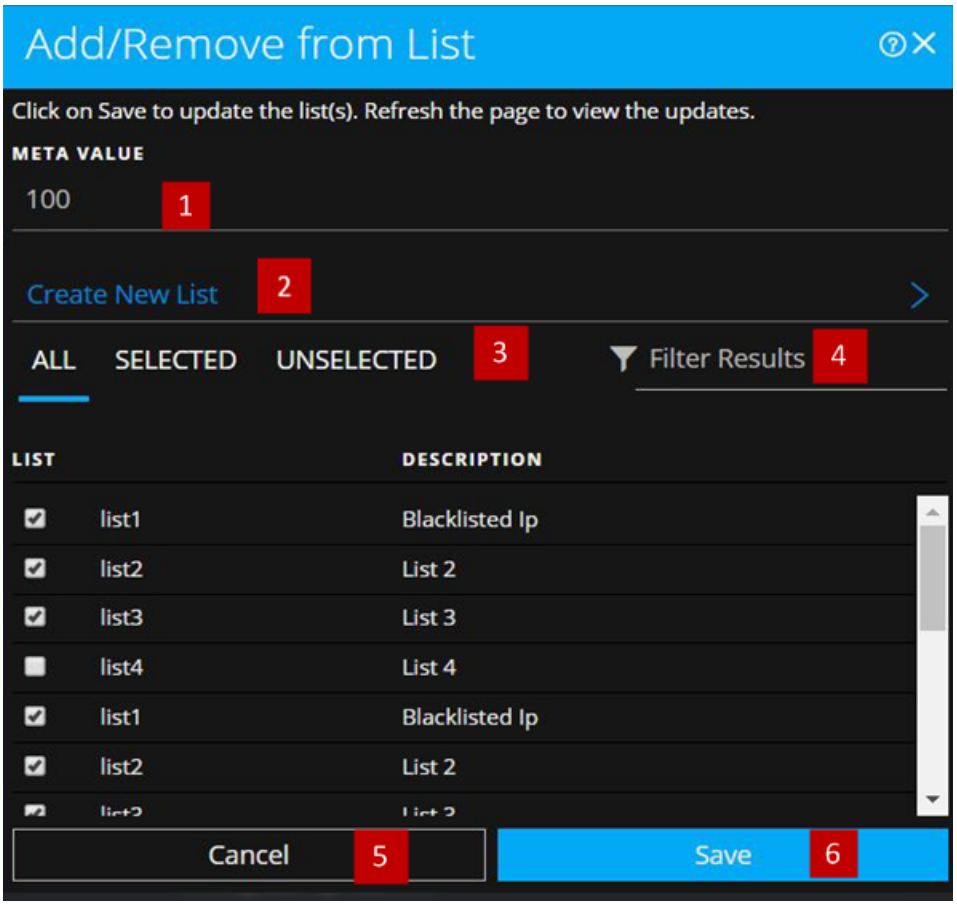
*このタスクは現在のビューで実行できます。

関連トピック

- 結果の追加のコンテキストを検索
- [ナビゲート]ビュー
- [レガシー イベント]ビュー
- [イベント]ビュー

[イベント]ビューの簡単な説明

[イベント]ビューの[**リストへの追加/削除**]ダイアログの例を次に示します。



1 追加または削除するエンティティまたはメタ値。
2 選択したメタを使用して新しいリストを作成します。
3 [すべて]、[選択済み]、[未選択]のいずれかのタブを選択します。
4 リストの名前または説明を使用して検索します。
5 アクションをキャンセルします。
6 保存してリストを更新するか、新しいリストを作成します。

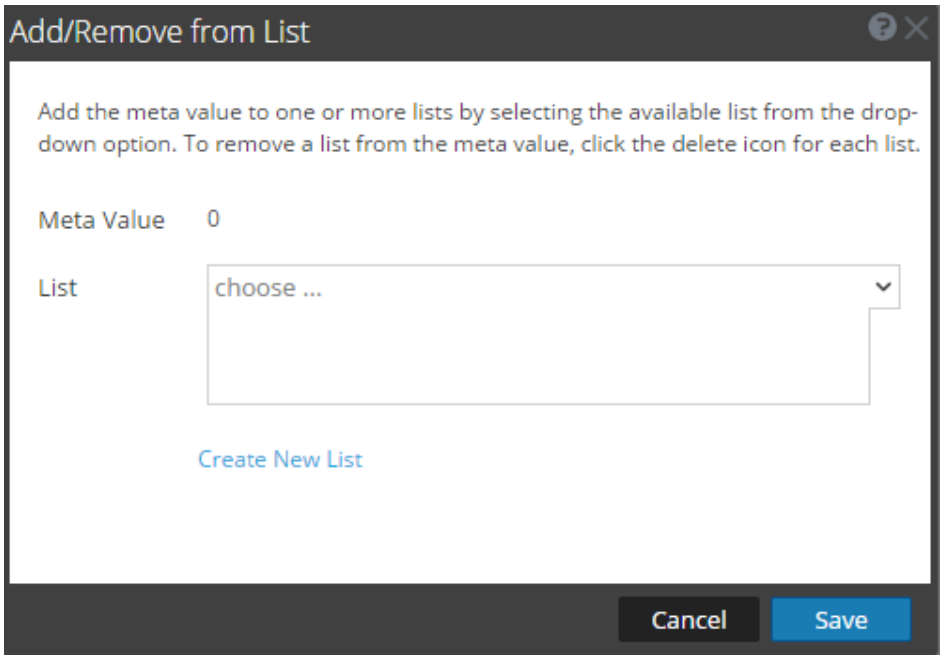
次の表に、[リストへの追加/削除]ダイアログのオプションを示します。

オプション	説明
メタ値	1つまたは複数のリストに追加、またはリストから削除する必要がある選択したエンティティまたはメタ値が表示されます。選択した値を使用して新しいリストを作成することもできます。
新しいリストの作成	選択されたメタ値を使用して新しいリストを作成するダイアログが表示されます。
ALL	使用できるContext Hubリストがすべて表示されます。選択したエンティティまたはメタ値を追加するリストを選択できます。リストにエンティティまたはメタ値を追加するには、チェックボックスを選択します。リストから削除するには、チェックボックスをオフにします。

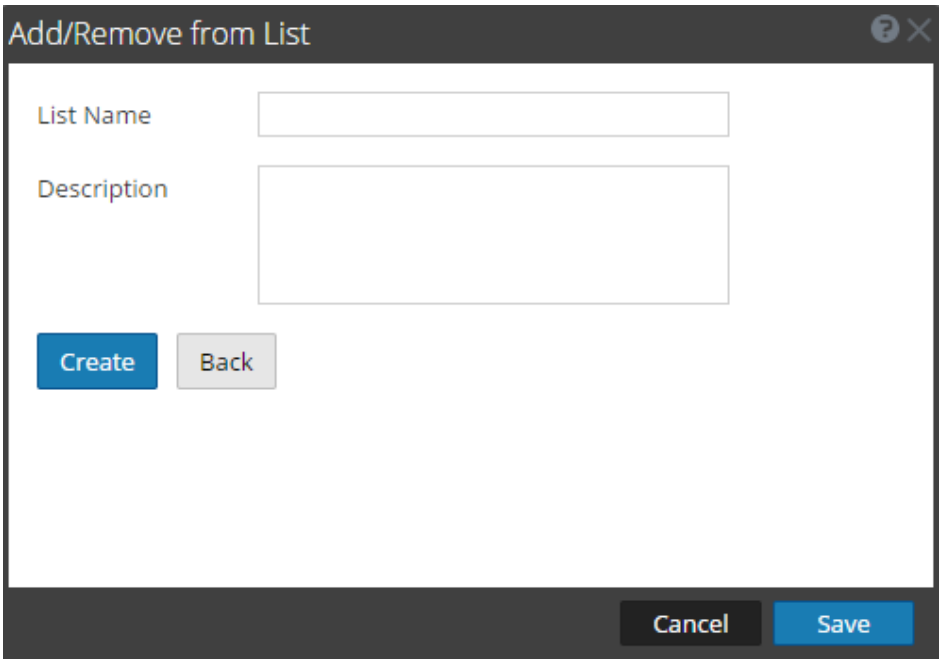
オプション	説明
選択済み	選択したエンティティまたはメタ値を含むリストのみが表示されます。(すべてのリストが選択されます。)
未選択	選択したエンティティまたはメタ値を含まないリストのみが表示されます。(すべてのリストが選択解除されます。)
結果のフィルタ処理	複数のリストから検索するため、特定のリストの名前または説明を入力します。
LIST	すべてのリストの名前を表示します。
説明	選択したリストに関する情報を表示します。「リストの作成時に指定した説明がこのダイアログに表示されます。」たとえば、「このリストには、ブラックリストのIPアドレスがすべて含まれます」などです。
キャンセル	操作をキャンセルします。
保存	変更を保存します。

[ナビゲート]ビューおよび[レガシー イベント]ビューの簡単な説明

次の図は、最初に開いたときの[リストへの追加/削除]ダイアログの例です。



次の図に[新しいリストの作成]を選択したときのダイアログを示します。



次の表で、[リストへの追加/削除]および[新しいリストの作成]の機能について説明します。

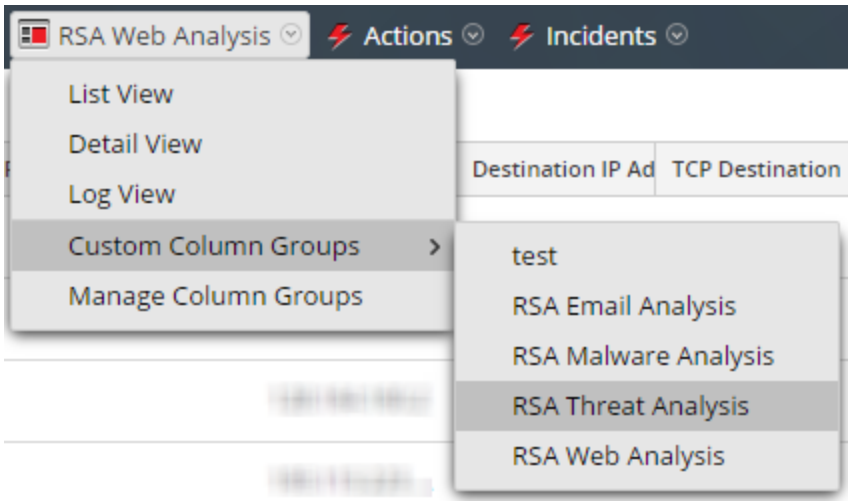
機能	説明
メタ値	既存のリストまたは新しいリストに追加される選択したメタ値。
リスト	選択したメタ値を追加するリスト。ドロップダウン メニューには、メタ値を追加できるリストが示されます。
新しいリストの作成	選択したメタ値を追加する新しいリストを作成するダイアログが開きます。
リスト名	新しいリストの名前。
説明	新しいリストの説明。
作成	必須入力フィールドを入力した後に新しいリストを作成します。
戻る	新しいリストの作成をキャンセルし、元のダイアログに戻ります。
キャンセル	リストへのメタ値の追加をキャンセルし、ダイアログ ボックスを閉じます。
保存	リストに加えた変更を保存し、ダイアログを閉じます。

[列 グループ] ダイアログ

列 グループを使 用すると、[イベント] ビューと[レガシー イベント] ビューに関 連 性 の高 いメタ キーのみが表 示 されるようイベント リストをフォーマット できます(「イベント リストでの列 と列 グループの使 用」を参照) 。調 査 のイベント リストにイベントが読 み込 まれると、各 列 にメタ キーの値 が表 示 されます。イベント リストに表 示 されるメタ キーの変 更 は、調 査 のフォーカスを絞 り込 むための便 利 な方 法 です。たとえば、デフォルトの列 グループには、**Collection Time**、**Type**、**Theme**、**Size**、**Summary**の列 が含 まれています。これらは基 本 的 な情 報 であり、特 殊 な情 報 ではありません。[RSA Email Analysis] グループには、メールを調 査 する際 に役 立 つ情 報 のみが含 まれています。

列 グループの定 義 には、列 タイトルとして使 用 するメタ キー、リスト内 での列 の位 置 、列 のデフォルトの幅 が含 まれます。列 グループの追 加 、削 除 、インポート、エクスポート、編 集 を行 うことができます。新 規 インストールには、標 準 提 供 の列 グループが含 まれます。標 準 提 供 の列 グループは、名 前 が「RSA」で始 まり、複 製 できますが、編 集 または削 除 することはできません。また、カスタム列 グループを作 成 することもできます。

- [列 グループの作 成] ダイアログは、11.4の[イベント] ビューから開 くことができます。このダイアログにアクセスするには、[**イベント**] ビューのツールバーで[**列 グループ**] > [**新 しい列 グループ**] を選 択 します。
- [列 グループの詳 細] ダイアログは、11.4の[イベント] ビューから開 くことができます。このダイアログにアクセスするには、[**イベント**] ビューのツールバーで[**列 グループ**] を選 択 して、カスタム列 グループ名 の横 の編 集 アイコン( ) をクリックします。
- [列 グループの管 理] ダイアログは、[レガシー イベント] ビュー(バージョン11.4) と[イベント] ビュー(バージョン11.4より前) から開 くことができます。[列 グループの管 理] ダイアログには、列 幅 の設 定 、インポート、エクスポートという、[列 グループの作 成] ダイアログではまだ使 用 できない機 能 があります。このダイアログにアクセスするには、[**調 査**] > [**レガシー イベント**] に移 動 して、[**ビュー**] ドロップダウン リストで[**列 グループの管 理**] を選 択 します。[**ビュー**] ドロップダウン メニューのラベルには、現 在 選 択 中 のオプション(詳 細 ビュー、リスト ビュー、ログ ビュー、現 在 選 択 されている列 グループ名 など) が表 示 されます。



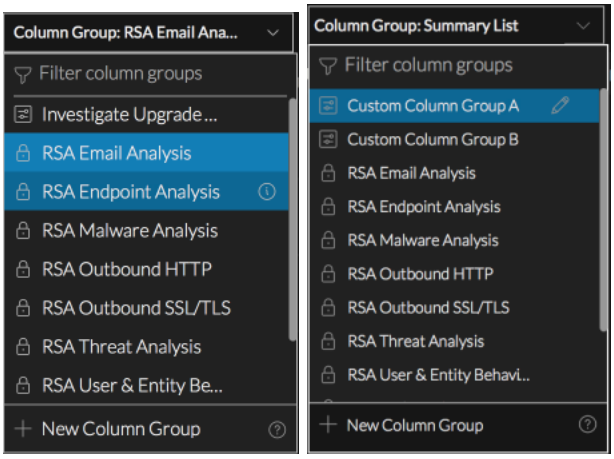
列 グループを定 義 したら、調 査 の他 のビューでも使 用 できます。[ナビゲート] ビューでは、プロファイルを使 用 して、プロファイルの適 用 時 に使 用 する列 グループを選 択 できます。[イベント] ビューと[レガシー イベント] ビューでは、[イベント] パネルに適 用 する列 グループを選 択 できます。

関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー
- [レガシー イベント]ビュー

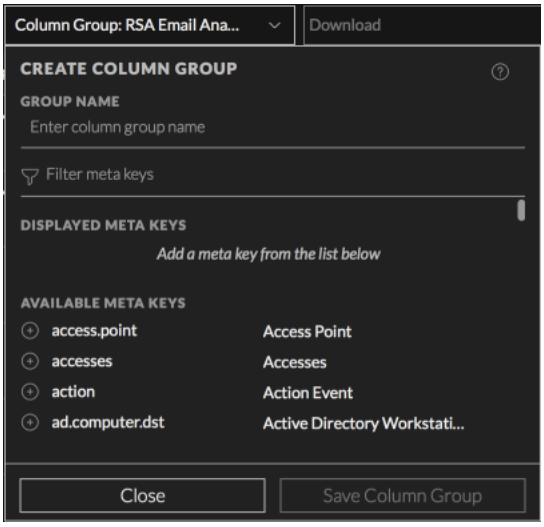
簡単な説明 - [列グループ]メニュー、[列グループの作成]ダイアログ、[列グループの詳細]ダイアログ

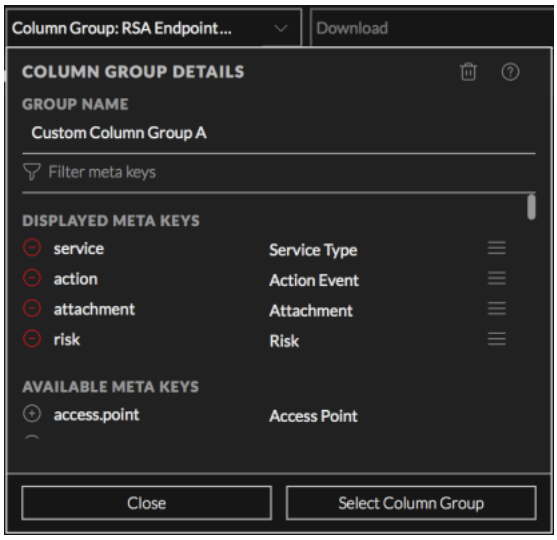
このセクションでは、[列グループ]メニュー、[列グループの作成]ダイアログ、[列グループの詳細]ダイアログについて説明します。次の図は、[列グループ]メニューの例です。左側の例では、標準提供の列グループがハイライト表示されているため、情報アイコンが表示されています。ハイライト表示された列グループ(RSA Endpoint Analysis) と選択中の列グループ(RSA Email Analysis) の色の違いに注目してください。右側の例では、カスタムの列グループがハイライト表示されているため、編集アイコンが表示されています。次の表に、オプションの説明を示します。



機能	説明
列グループの絞り込み	テキストを入力に合わせて、そのテキストを含んだグループ名のみが表示されるように、列グループのリストを絞り込みます。
列グループ リスト	列グループのリストには、カスタム グループと標準提供グループが表示されます。グループ名の前には両者を区別するアイコンが表示されます。2番目の例にある「Custom Column Group A」と「Custom Column Group B」はカスタム列グループです。「RSA」で始まる列グループは標準提供列グループです。
新しい列グループ	[列グループの作成]ダイアログを表示します。このダイアログでは、カスタム列グループを作成できます。

次の左側の図に示す[列グループの作成]ダイアログを使用して、カスタム列グループを定義できます。右側の図は、カスタム列グループの編集に使用できる[列グループの詳細]ダイアログを示しています。次の表は、ダイアログ内のフィールドとオプションについて説明したものです。

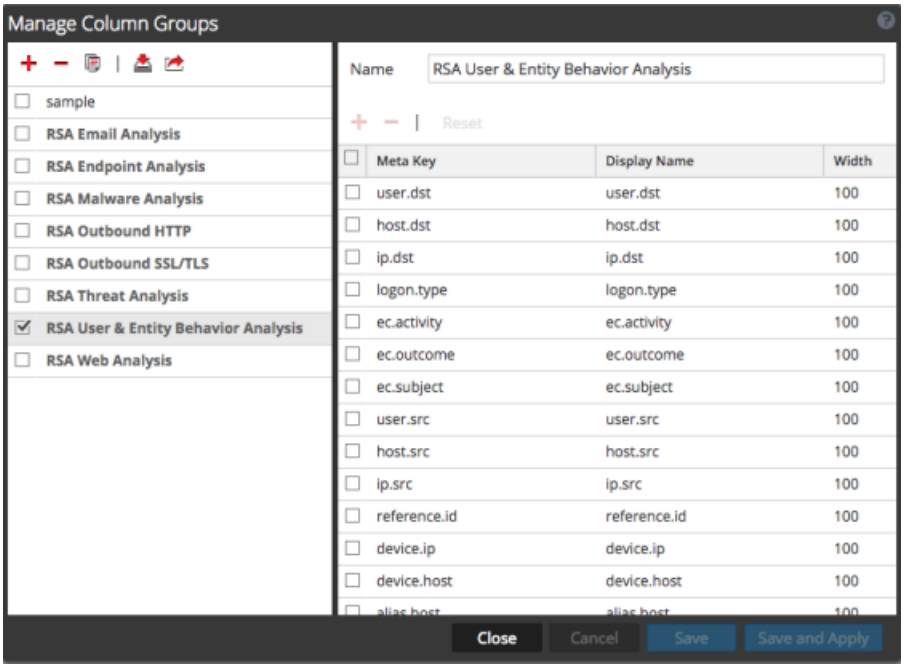




機能	説明
	[列グループの詳細]ダイアログでカスタム列グループを削除します。このアクションは元に戻すことができず、グローバルに適用されます。削除された列グループは、このサービスでこの列グループを使用しているどのユーザからも使用できなくなります。
グループ名	列グループの名前を表示します。64文字以内の一意の名前を指定してください。カスタム列グループの名前を編集する場合は、このフィールドに入力します。
メタ キーの絞り込み	入力されたテキストに基づいて、[表示するメタ キー]と[選択可能なメタ キー]のリストを絞り込みます。入力したテキストを含んでいるメタ キーのみが表示されます。
表示するメタ キー	カスタム列グループで使用するために選択されたメタ キーのスクロール可能なリストを表示します。[選択可能なメタ キー]リスト内のメタ キーをこのリストに追加したり、メタ キーをこのリストから削除したり( ) 、メタ キーを上下にドラッグしてこのリストでの順序を変更したりできます( ) 。
選択可能なメタ キー	カスタム列グループで使用するために、(そのサービスで) 選択可能なメタ キーのスクロール可能なリストを表示します。これらのメタ キーを[表示するメタ キー]リストに追加できます。メタ キー名の横にある をクリックすると、[表示するメタ キー]リストにそのメタ キーが追加されます。
[閉じる]ボタン	ダイアログを閉じます。
列グループを保存	[列グループを作成]ダイアログにのみ表示され、新しい列グループを保存します。
リセット	[列グループの詳細]ダイアログにのみ表示され、編集した列グループを前回保存された状態に戻します。
列グループを更新	[列グループの詳細]ダイアログにのみ表示され、編集した列グループに変更を適用します。

機能	説明
列グループを選択	列グループを適用します。

簡単な説明 - [列グループの管理]ダイアログ



[列グループの管理]ダイアログには、[グループ]と[設定]という2つのパネルがあります。ダイアログの下部には、[閉じる]、[キャンセル]、[保存]、[保存して適用]という4つのボタンがあります。

左側のパネルは[グループ]パネルです。ここでは、列グループの追加、削除、インポート、エクスポートを行うことができます。パネルの上部には、ツールバーがあります。ツールバーの下には、追加された列グループのリストが表示され、グループを選択できるようになっています。

次の表は、ツールバーで選択できるアクションを示しています。

操作	説明
+	列グループを追加します。このボタンをクリックすると、右側の[設定]パネルがハイライト表示されます。[設定]パネルでは、列グループに名前をつけたり、メタ キーを追加または削除したりすることができます。グループを追加するには、少なくとも1個のメタ キーが必要です。
−	列グループを削除します。選択したグループが削除される前に、確認のダイアログが表示されます。標準提供の列グループは削除できません。
	選択された列グループのコピーを作成します。
	[列グループのインポート]ダイアログを表示します。このダイアログでは、アップロードするファイルを選択できます。

操作	説明
	選択されたグループをローカル ファイル システムにエクスポートします。

右側のパネルは[設定]パネルです。ここでは、列グループを作成して編集できます。このパネルには、[名前]フィールド、ツールバー、リストがあります。次の表で、[設定]パネルの各機能について説明します。

機能	説明
名前	選択した列グループの名前。
	メタ キーのリストに新しい行を追加します。新しい行では、ドロップダウン メニューを開いて新しいメタ キーを選択できます。
	選択されたメタ キーを削除します。削除する前に確認のダイアログを表示します。
リセット	列グループを前回保存された設定に戻します。
メタ キー	選択した列グループに追加されたメタ キーを一覧表示します。
表示名	[ナビゲート]、[イベント]、[イベント分析]の各ビューに表示されるメタ キーの名前を一覧表示します。
幅	各メタ キーの列の幅を指定します。幅には10～1000の値を設定できます。デフォルトの幅は100です。

次の表にアクション ボタンの説明を示します。

機能	説明
閉じる	保存しないでダイアログを閉じます。
キャンセル	未保存の変更をすべて取り消します。
保存	ダイアログを閉じることなく、すべての変更を適用します。
保存して適用	すべての変更を保存して、列グループをただちに適用し、ダイアログを閉じます。

[コンテキスト ルックアップ] パネル

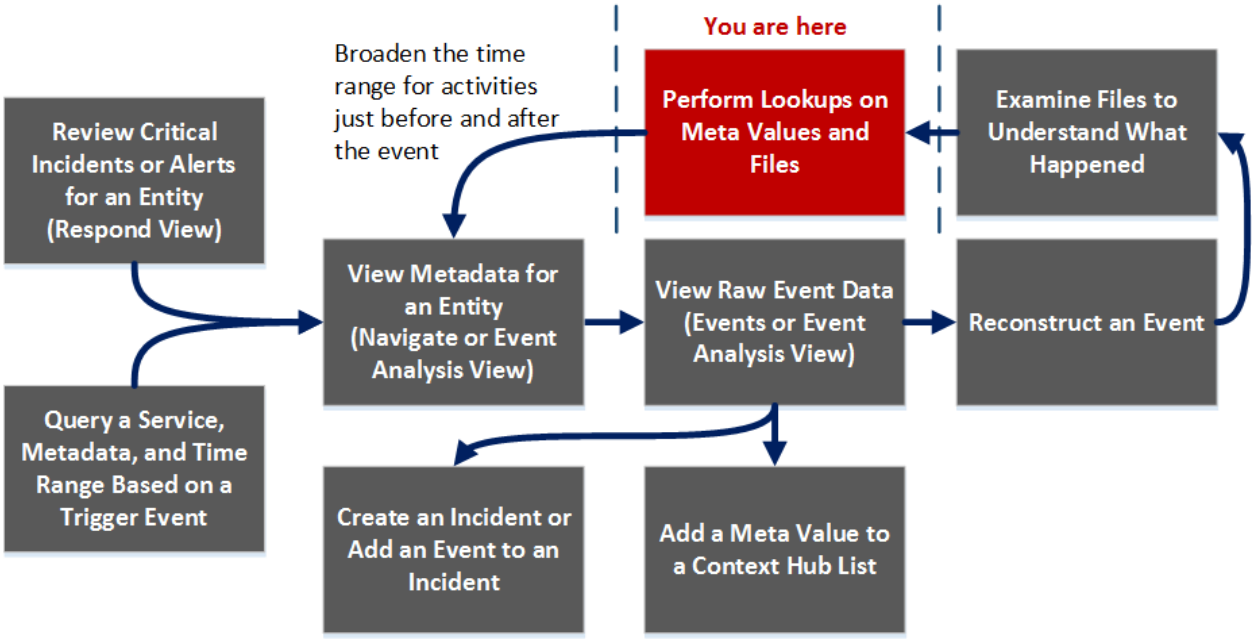
管理者がContext Hubサービスを構成した後、[ナビゲート]ビュー、[レガシー イベント]ビュー、[イベント]ビュー(バージョン11.2以降)に、メタ値に関するコンテキスト情報を表示できます。Context Hubサービスでは、メタ タイプとメタ キーのデフォルトのマッピングが事前に構成されています。Context Hubのメタ値と調査のメタ キーのマッピングの詳細については、『*Context Hub構成ガイド*』の「メタ タイプとメタ キーのマッピングの管理」を参照してください。

[コンテキスト ルックアップ] パネルは、[ナビゲート]ビュー、[レガシー イベント]ビュー、[イベント]ビューの右側に表示されます。Context Hubリストに追加されているメタ値は、[ナビゲート]ビューまたは[レガシー イベント]ビューの結果中で灰色でハイライト表示されます。[イベント]ビューでは、下線でマークされます。ハイライト表示されている値を右クリックし、[**コンテキスト ルックアップ**]を選択すると、表示されるコンテキスト メニューで、選択したメタ値の構成済みのソースの[コンテキスト ルックアップ] パネルにルックアップ結果が表示されます。[コンテキスト ルックアップ] パネル アイコン バーでソースを選択すると、コンテキスト情報を表示できます。

「ナビゲート」ビューまたは「イベント」ビューで開いたときと、[イベント]ビューで開たときとでは、[コンテキスト ルックアップ] パネルの外観と内容にいくつかの違いがあります。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか？

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行*	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加*	[レガシー イベント]ビューでのインシデントへのイベントの追加 [レガシー イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加	結果の追加のコンテキストを検索

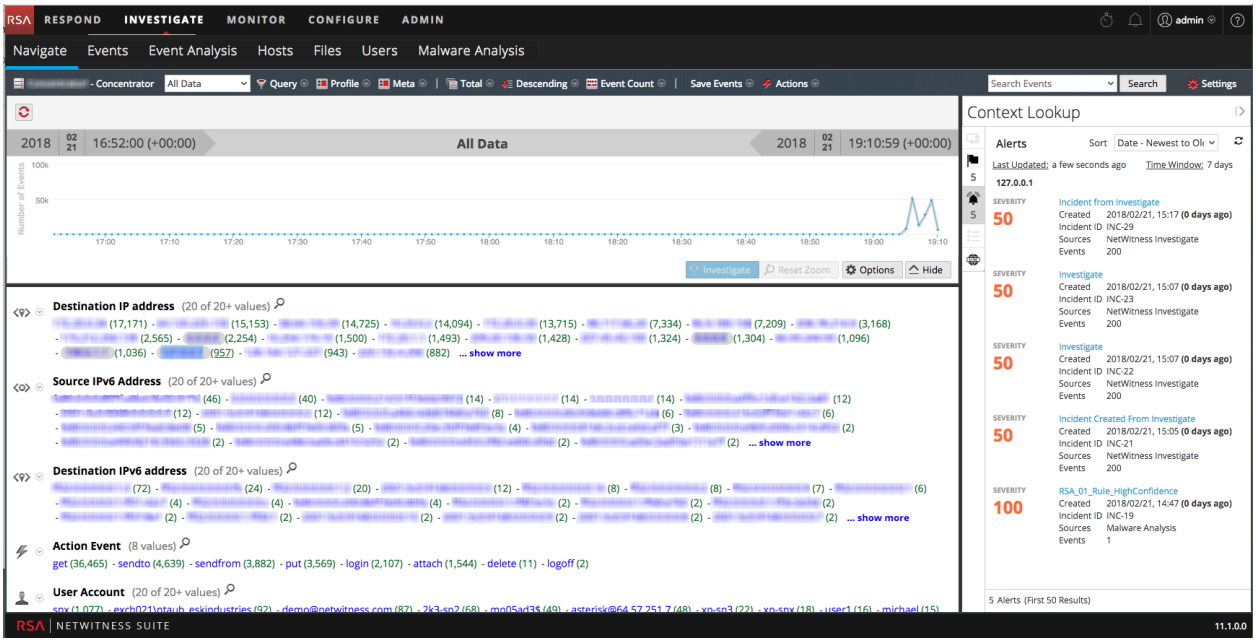
*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [レガシー イベント]ビュー
- [ナビゲート]ビュー
- [イベント]ビュー
- 「*Live サービス管理ガイド*」の「NetWitnessのフィードバックとデータ共有」

([ナビゲート]ビューおよび[レガシー イベント]ビューでの) 簡単な説明

次の図は、[ナビゲート]ビューと[レガシー イベント]ビューに表示される[コンテキスト ルックアップ]パネルの例です。コントロールと機能については、表で説明します。



機能	説明
ソース オプション バー	使用可能なソース(エンドポイント、インシデント、アラート、リスト) のアイコンが表示されます。
ソース名	選択したアイコンに基づいてソース名が表示されます。 • エンドポイント • インシデント • アラート • リスト • Live Connect

機能	説明
ソート	表示されたコンテキスト情報をソートするオプションをドロップダウンで選択できます。ソート オプションには[重大度 - 高い順]、[重大度 - 低い順]、[日付 - 古い順]、[日付 - 新しい順]があり、ソースのタイプによって異なります。
	ルックアップ結果を更新します。
<n件のアイテム>(最初の<n>件の結果)	フッターに現在表示されている結果の件数と結果の総数が表示されます。たとえば、[5件のアラート(最初の50件の結果)]のように表示されます。

インシデント

インシデントは時間順(新しい順)に表示され、さらに優先度のステータスでソートされます。インシデントのルックアップでは、次の情報が表示されます。

- インシデントの名前とID
- インシデントの優先度のステータス
- インシデントのリスク スコアの値
- インシデントが作成された日付
- インシデントのステータス
- インシデントの割り当て先
- 最終更新日コンテキスト データを最後にデータ ソースからフェッチして、キャッシュを更新した時刻を示します。
- タイム ウィンドウ: これは[Respondの構成]ウィンドウの[クエリの対象期間(日数)]フィールドに設定された値に基づいています。詳細については、『*Context Hub構成ガイド*』の「データ ソースとしてのRespondの構成」を参照してください。
- ソート:このドロップダウン フィールドのオプションを使用して、時間または優先度に基づいて結果のソートを変更できます。

アラート

アラートが重大度に基づいて表示されます。アラートのルックアップでは、次の情報が表示されます。

- アラート名
- アラートの重大度の値
- アラートが作成された日付
- インシデントID:アラートが関連づけられているインシデントのIDです(該当する場合)。
- ソース:イベント ソース名
- アラートに関連するイベントの数。

- 更新日: コンテキスト データを最後にデータ ソースからフェッチして、キャッシュを更新した時刻を示します。
- タイム ウィンドウ: これは[Respondの構成]ウィンドウの[クエリの対象期間(日数)]フィールドに設定された値に基づいています。詳細については、『*Context Hub構成ガイド*』の「データ ソースとしてのRespondの構成」を参照してください。
- ソート: このドロップダウン フィールドのオプションを使用して、時間または優先度に基づいて結果のソートを変更できます。

リスト

リストのルックアップでは、次の情報が表示されます。

- リスト名
- リストを作成したオーナー
- 作成日
- 最終更新日
- リストの説明

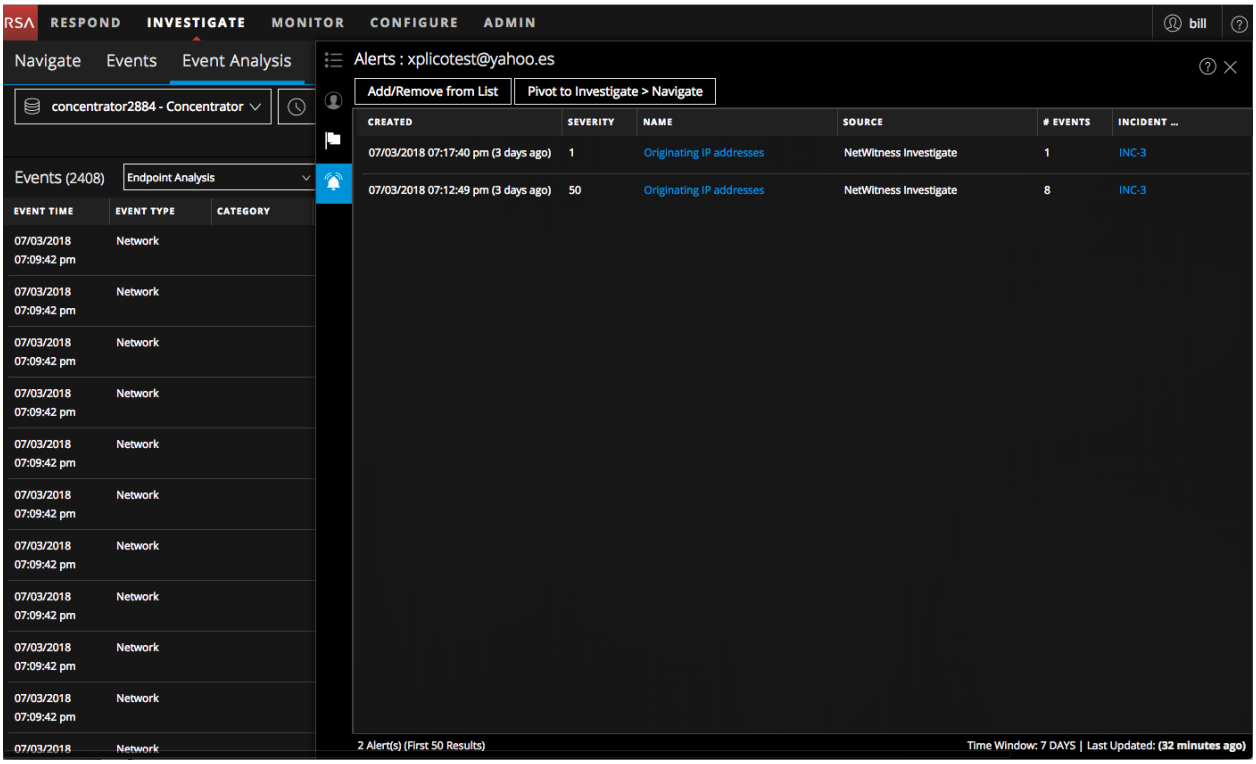
エンドポイント

エンドポイントのルックアップでは、次の情報が表示されます。

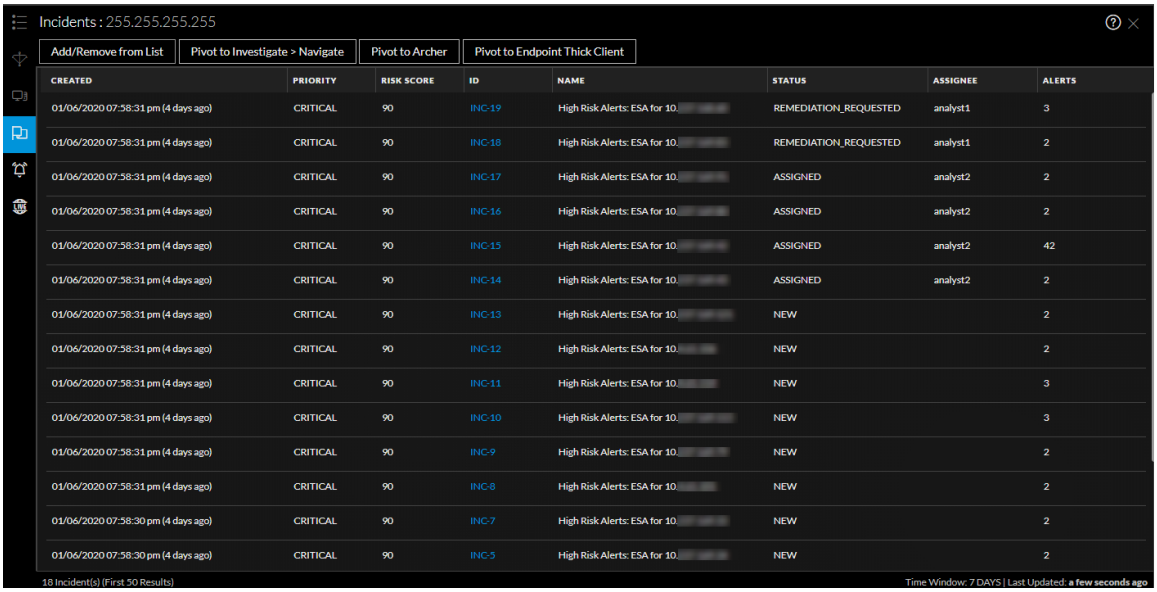
- マシン名とマシンのIPアドレス。
  IPまたはエンドポイント マシン名をクリックすると、エンドポイントUIに移動してさらに詳しい調査を実行できます。
- 更新日: コンテキスト データを最後にデータ ソースからフェッチして、キャッシュを更新した時刻を示します。
- マシン スコア: モジュールのスコアに基づいてマシンのIIOCスコアが集計されます。
- モジュール数: 選択したマシンのアクティブなファイルの数。
- 最終更新日: エンドポイント データベースでスキャン結果が最後に更新された時刻を示します。
- 最後にログインしたユーザ
- マシンのMACアドレス
- オペレーティング システムのバージョン
- 管理メモ(該当する場合)
- 管理ステータス(該当する場合)
- 最も疑わしいモジュール(IIOCスコアが500を超えるモジュール)。これは[エンドポイントの構成]ウィンドウの[最小IIOCスコア]フィールドに設定された値に基づいています。[最小IIOCスコア]のデフォルト値は500です。
- マシンIIOCレベル

[イベント]ビューの簡単な説明(バージョン11.2以降)

次の図は、[イベント]ビューに表示される[コンテキスト ルックアップ]パネルの例です。



[コンテキスト ルックアップ] パネルに表示されるコンテキスト情報やクエリの結果は、選択したエンティティと関連するデータ ソースに依存します。[コンテキスト ルックアップ] パネルには、データ ソースごとに個別のタブがあります。タブには、[データ ソースのリスト]、[Archer]、[Active Directory]、[エンドポイント]、[インシデント]、[アラート]、[Live Connect] があります。次の図は、[インシデントの詳細] ビューで選択したエンティティの[コンテキスト ルックアップ] パネルを示しています。



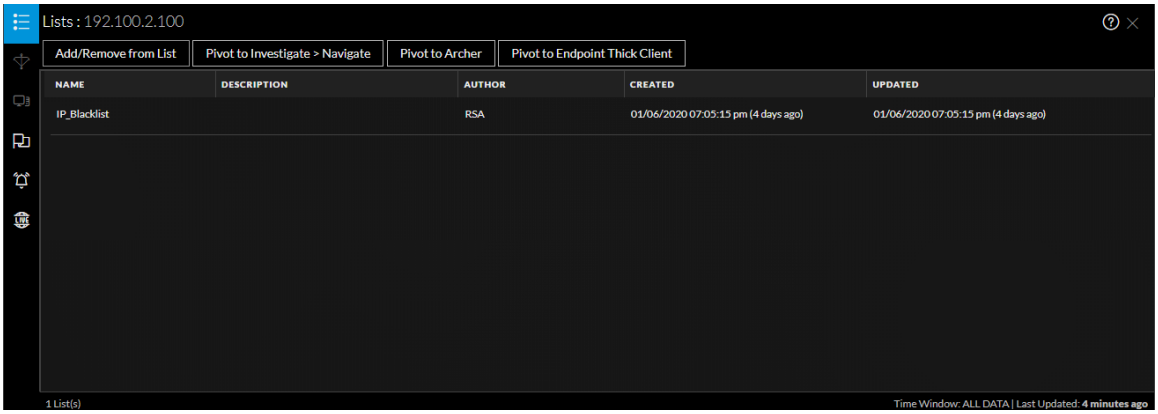
次の表は、各タブおよびサポートされるエンティティで使用可能なデータを示しています。

タブ	説明	サポートされるエンティティ
(リスト)	選択したエンティティまたはメタ値に関連付けられているすべてのリストのデータを表示します。リストの最終更新日時によってソートされます。	すべてのエンティティ
(Archer)	Archerデータ ソースから、重要度評価と資産情報を表示します。	IP、ホスト、MAC
(Active Directory)	選択したユーザのすべてのユーザ情報を表示します。	ユーザ
(NetWitness Endpoint)	マシン、モジュール、IIOCレベルを含む選択したエンティティまたはメタ値の NetWitness Endpointデータ ソースの情報を表示します。モジュールは最大IOCスコアから最小IIOCスコアの順にソートされ、IIOCレベルは最高IOCレベルから最低IOCレベルの順にソートされます。	IP、MACアドレス、ホスト

タブ	説明	サポートされるエンティティ
(インシデント)	選択したエンティティまたはメタ値に関連付けられているインシデントのリストを表示します。最新のインシデントから最も古いインシデントの順にソートされます。	すべてのエンティティ
(アラート)	選択したエンティティまたはメタ値に関連付けられているアラートのリストを表示します。最新のアラートから最も古いアラートの順にソートされます。	すべてのエンティティ
(Live Connect)	Live Connectから関連する情報を表示します。	IP、ドメイン、Filehash
(ファイル レピュテーション)	Filehashエンティティのファイル レピュテーションのステータスを表示します。	Filehashエンティティ

[リスト]タブ

[コンテキスト ルックアップ]パネルの[リスト]タブには、選択したエンティティまたはメタ値に関連する1つ以上のリストが表示されます。次の図は、[コンテキスト ルックアップ]パネルの[リスト]タブの例です。表にはフィールドの説明が記載されています。

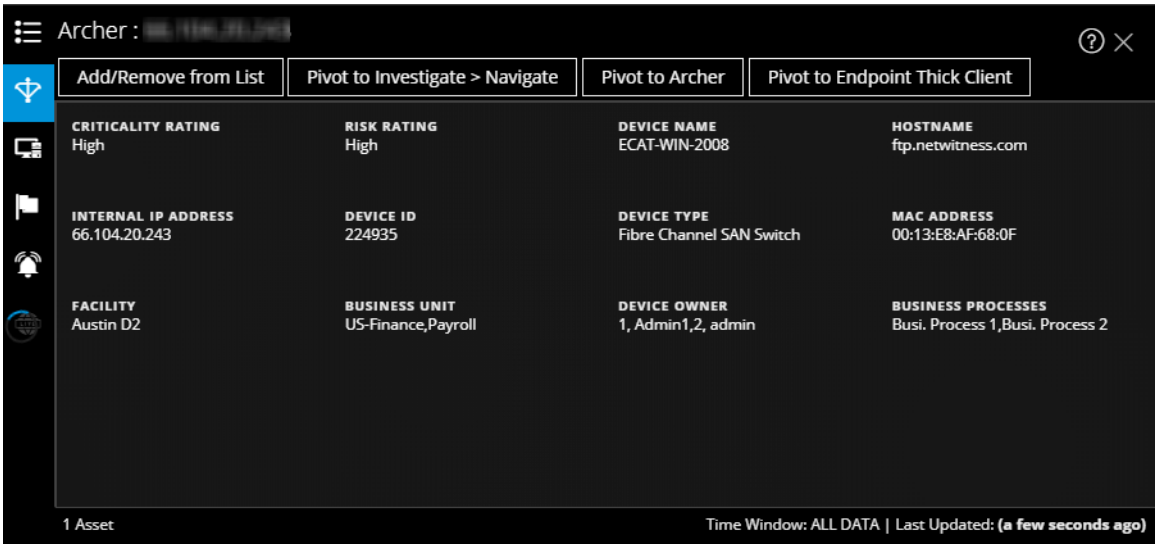


フィールド	説明
名前	リストの名前(リストの作成時に定義)。
説明	リストの説明(リストの作成時に定義)。
作成者	リストを作成したオーナー。
作成日時	リストが作成された日付。

フィールド	説明
更新日	リストが最後に更新または変更された日付。
件数	選択したエンティティまたはメタ値が使用可能なリストの数。
タイム ウィンドウ	[レスポンスの構成]ダイアログの[クエリの対象期間]フィールドに設定された値に基づくタイム ウィンドウ。デフォルトでは、[リスト]のすべてのデータがフェッチされます。
最終更新日	Context Hubがルックアップ データをフェッチしてキャッシュに保存した時刻。

[Archer]タブ

[コンテキスト ルックアップ]パネルの[Archer]タブには、IP、ホスト、およびMACのエンティティについて、Archerデータ ソースから取得した重要度評価と資産情報が表示されます。次の図は、[コンテキスト ルックアップ]パネルの[Archer]タブの例です。表には各フィールドの説明が記載されています。



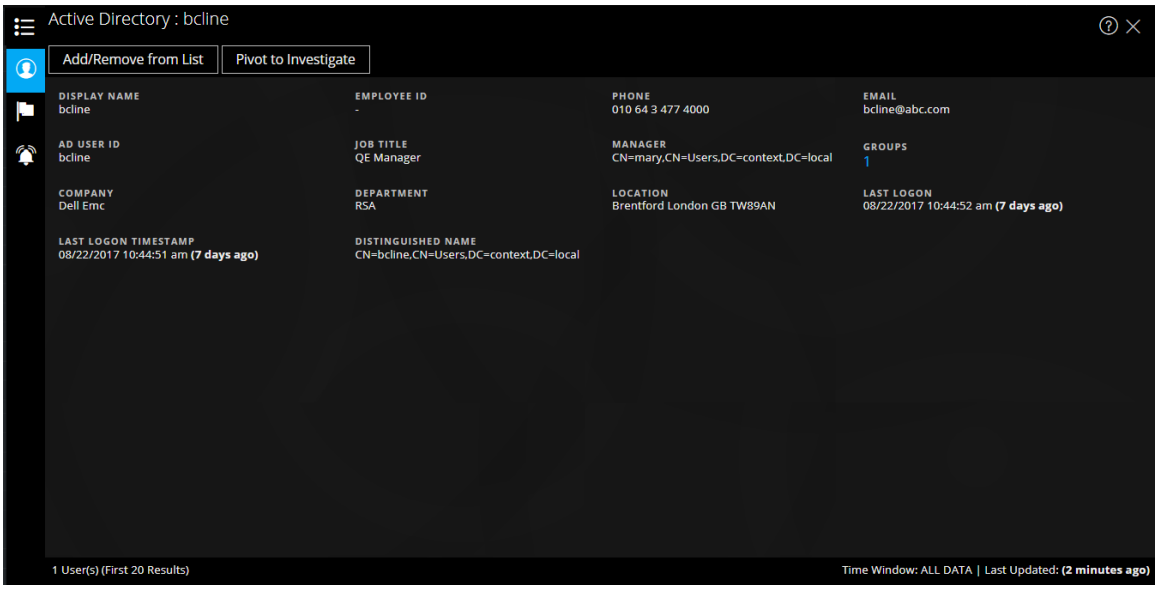
フィールド	説明
重要度評価	デバイスがサポートするアプリケーションに基づいて算出されたデバイスの業務上の重要度。重要度評価は、未評価、低、中-低、中、中-高、高のいずれかに設定できます。
リスク評価	最新のアセスメント結果と、このデバイスを使用する施設の平均リスク評価から、デバイスのリスク評価を計算します。リスク評価は、重大、高、中、低、軽微のいずれかに設定できます。
デバイス名	デバイスの固有の名前。
host Name	デバイスのホスト名。
IPアドレス	デバイスのプライマリ内部IPアドレス。

フィールド	説明
デバイスID	システム内のすべてのアプリケーションにおいてデバイス レコードを一意に識別する、自動的に設定された値。
タイプ	サーバ、ラップトップ、デスクトップなどのデバイスの種類。
施設(Facilities)	このデバイスに関連する施設アプリケーション内のレコードへのリンク。
ビジネス ユニット (Business Unit)	このデバイスに関連するビジネス ユニット アプリケーション内のレコードへのリンク。3を越えるビジネスユニットの値については、フィールドにカーソルを合わせると表示されます。
デバイス管理責任者	デバイスを担当し、レコードの読み取りおよび更新権限を持つデバイスの管理責任者。
件数	使用可能な資産の数。
タイム ウィンドウ	[レスポンスの構成]ダイアログの[クエリの対象期間]フィールドに設定された値に基づいたタイム ウィンドウ。デフォルトでは、Archerのすべてのデータをフェッチします。
最終更新日	Context Hubがルックアップ データをフェッチしてキャッシュに保存した時刻。

注: ローカライズ版で表示されるのは、重要度評価、リスク評価、デバイス管理責任者、ビジネス ユニット、ホスト名、MACアドレス、施設、IPアドレス、タイプ、デバイスID、デバイス名、ビジネス プロセスの12個のフィールドのみです。

[Active Directory]タブ

次の図は、Active Directoryの[コンテキスト ルックアップ]パネルの例です。



Active Directoryの[コンテキスト ルックアップ]パネルには、ユーザのすべての関連情報、インシデント、アラートが表示されます。次の形式を使用して検索を実行できます。

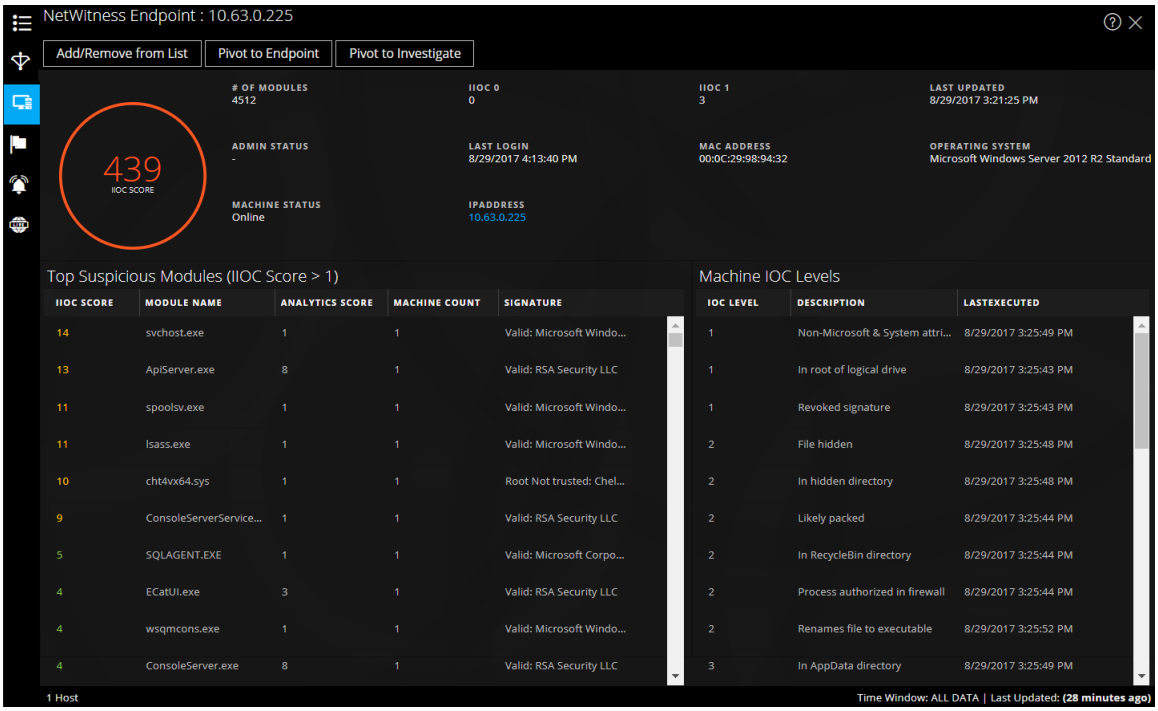
- userPrincipalName
- Domain\UserName
- sAMAccountName

Active Directoryについて次の情報が表示されます。

フィールド	説明
表示名	ユーザの名前。
従業員ID	ユーザの従業員ID。
電話	ユーザの電話番号。
メール	ユーザのメールID。
ADユーザID	組織内の特定ユーザの固有ID。
役職	ユーザの役職。
マネージャー	ユーザのマネージャの名前。
グループ	ユーザが所属するグループのリスト。
会社(Company)	ユーザの会社の名前。
部門	ユーザが所属する組織内の部門名。
場所	ユーザの場所。
最終ログオン	ユーザがシステムにログインした時刻(グローバル カタログが定義されている場合のみ) 。
最終ログオンのタイムスタンプ	ユーザがシステムにログインした時刻。
識別名	ユーザに割り当てられている固有の名前。
件数	ユーザの数。
タイム ウィンドウ	[データ ソース設定の構成]ダイアログの[クエリの対象期間]フィールドに設定された値に基づくタイム ウィンドウ。デフォルトでは、Active Directoryのすべてのデータをフェッチします。
最終更新日	Context Hubがルックアップ データをフェッチしてキャッシュに保存した時刻。

[NetWitness Endpoint]タブ

次の図は、[コンテキスト ルックアップ]パネルの[NetWitness Endpoint]タブの例です。



IIOCについて次の情報が表示されます。

フィールド	説明
モジュール数	検索されたモジュール数。
管理ステータス	管理ステータス(該当する場合)。
最終更新日	データが最後に更新された時刻。
最終ログイン	ユーザが最後にログインした時間。
MACアドレス	マシンのMACアドレス。
オペレーティング システム	NetWitness Endpointマシンで使用されるオペレーティング システムのバージョン。
マシン ステータス	表示されているモジュールの状態(オンライン、オフライン、アクティブ、非アクティブ)。
IPアドレス	特定のモジュールのIPアドレス。

モジュールについて次の情報が表示されます。

フィールド	説明
IIOCスコア	マシンIIOCスコアは、モジュールのスコアに基づいて集計されたスコアです。これは[Context Hubデータ ソース設定]ダイアログの[最小IIOCスコア]フィールドに設定された値に基づいています。[最小IIOCスコア]のデフォルト値は500です。「*Context Hub構成ガイド*」の「Context Hubのデータ ソース設定の構成」を参照してください。

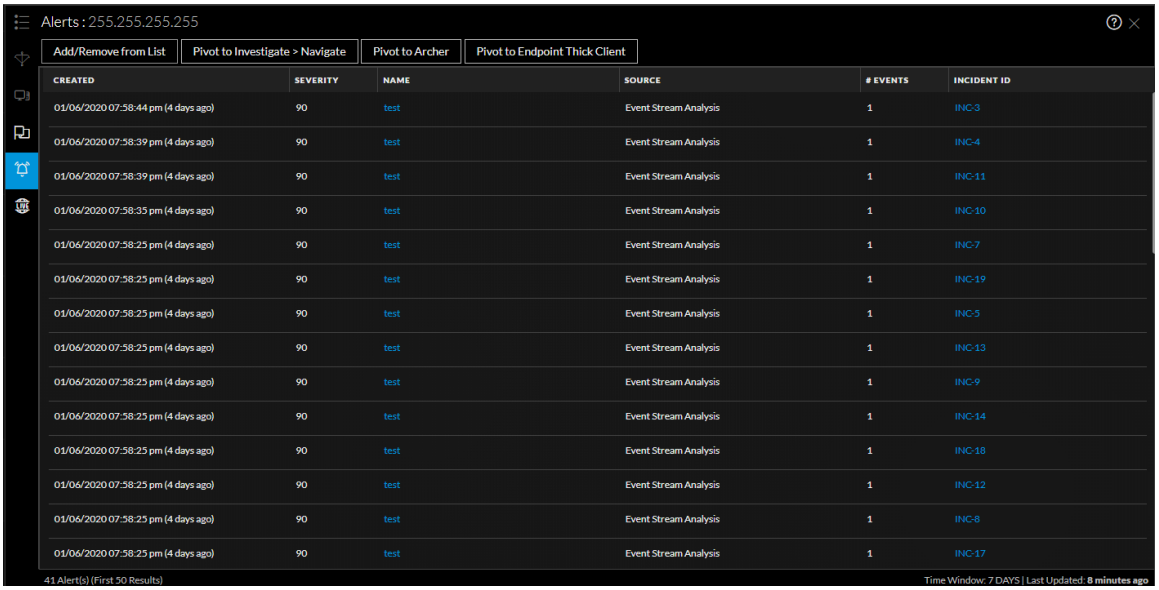
フィールド	説明
モジュール名	検索されたモジュールの名前。
解析スコア	選択したマシンのアクティブなファイルの数。
マシン数	特定のIOCがトリガーしたマシンの数。
署名	ファイルが署名されているかどうかと、有効か無効かを示し、署名情報を提供します。たとえば、Google、Appleなど。

マシンについて次の情報が表示されます。

フィールド	説明
IOCレベル	IOCレベル。
説明	IOCレベルの説明(使用可能な場合)。
前回の実行	アクションが実行された時刻。
件数	検索されているホスト数。
タイム ウィンドウ	[データ ソース設定の構成]ダイアログの[クエリの対象期間]フィールドに設定された値に基づいたタイム ウィンドウ。デフォルトでは、NetWitness Endpointのすべてのデータがフェッチされます。
最終更新日	NetWitness Endpointデータベースでスキャン結果が最後に更新された時刻。

[アラート]タブ

次の図は、最初に時間(新しい順)、次に重大度に基づいて表示された[アラート]の[コンテキスト]パネルの例です。

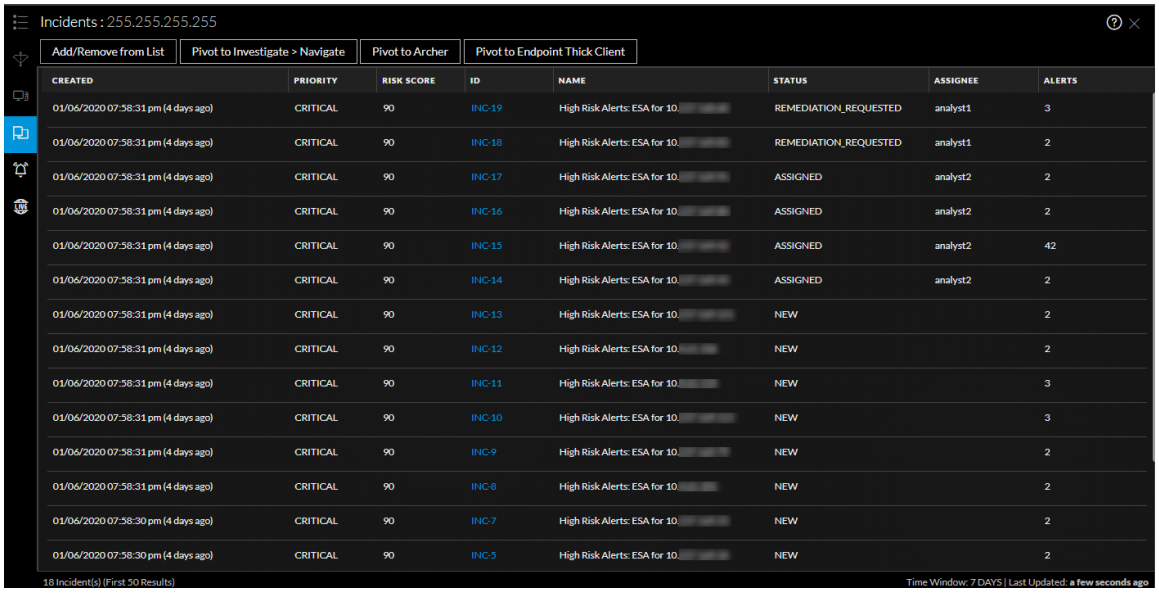


[コンテキスト ルックアップ]パネルの[アラート]タブには以下の情報が表示されます。

フィールド	説明
作成日時	アラートが作成された日時。
重大度	アラートの重大度の値
名前	アラートの名前。名前をクリックすると特定のアラートの詳細が表示されます。
ソース	アラートをトリガーしたアラート ソースの名前。
イベント数	アラートに関連するイベントの数。
インシデント ID	アラートが関連づけられているインシデントのID(該当する場合)。IDをクリックすると特定のアラートの詳細が表示されます。
件数	アラート数デフォルトでは、最初の100件のアラートのみが表示されます。設定の構成方法の詳細については、『*Context Hub構成ガイド*』の「Context Hubのデータ ソース設定の構成」を参照してください。
タイム ウィンドウ	[データ ソース設定の構成]ダイアログの[クエリの対象期間]フィールドに設定された値に基づいたタイム ウィンドウ。デフォルトでは、過去7日間のアラートデータをフェッチします。
最終更新日	データ ソースからコンテキスト データを最後に取得した時刻。

[インシデント]タブ

次の図は、最初に時間(新しい順)次に優先度のステータスに基づいた[コンテキスト ルックアップ]パネルの[インシデント]タブの例です。

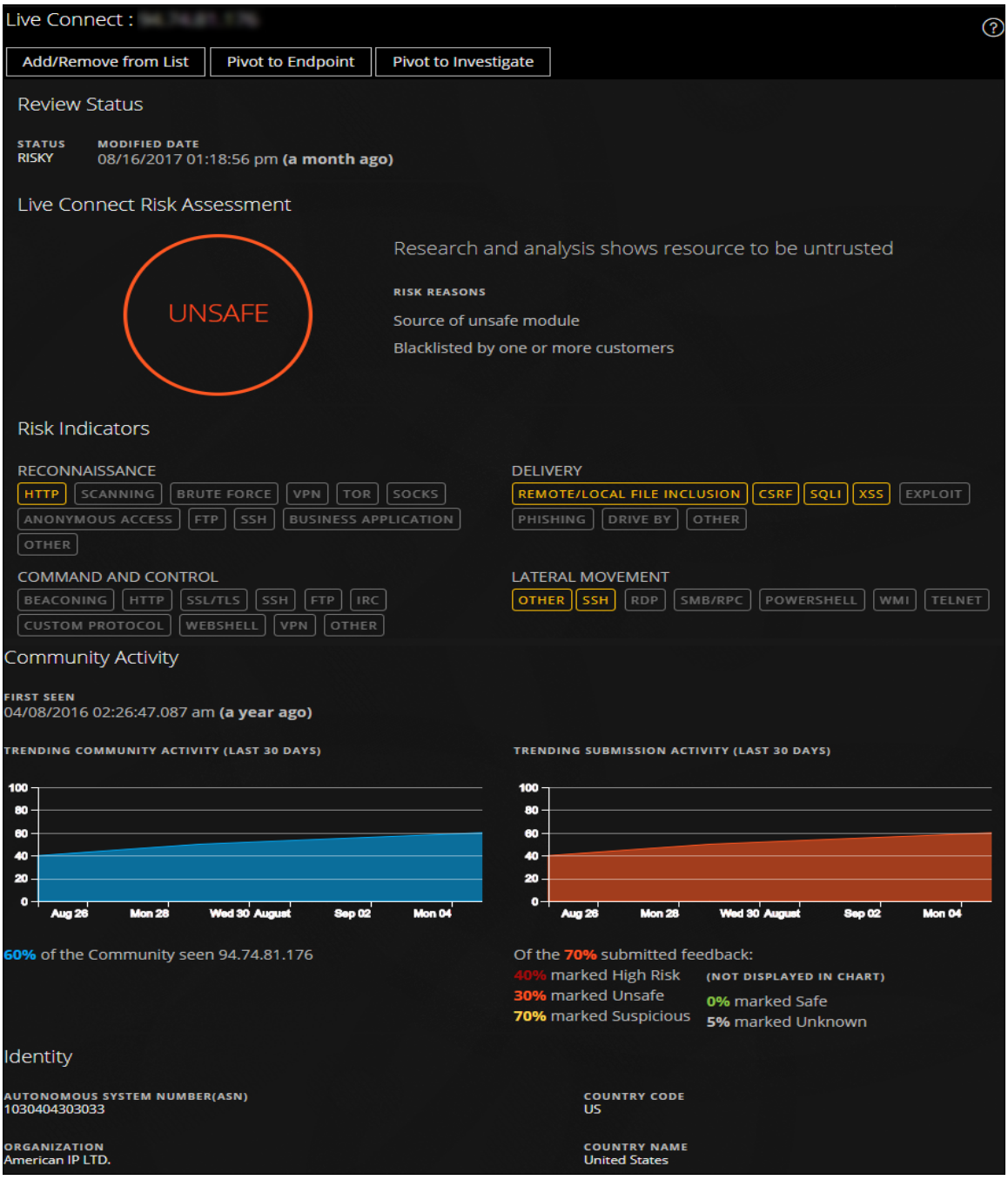


[コンテキスト ルックアップ]パネルの[インシデント]タブには以下の情報が表示されます。

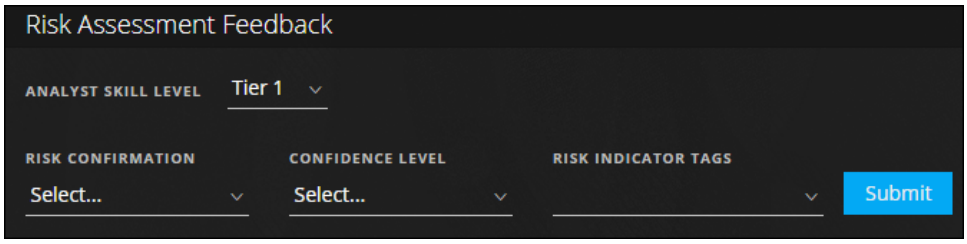
フィールド	説明
作成日時	インシデントが作成された日付。
優先	インシデントの優先度のステータス。
リスク スコア	インシデントのリスク スコア。
ID	インシデントのインシデントID。IDをクリックするとインシデントの詳細が表示されます。
名前	インシデントの名前。
ステータス	インシデントのステータス。
割り当て先	インシデントの現在のオーナー。
アラート	インシデントに関連するアラートの数。
件数	インシデントの数。デフォルトでは、最初の100件のインシデントのみが表示されます。設定の構成方法の詳細については、『*Context Hub構成ガイド*』の「Context Hubのデータ ソース設定の構成」を参照してください。
タイム ウィンドウ	[データ ソース設定の構成]ダイアログの[クエリの対象期間]フィールドに設定された値に基づいたタイム ウィンドウ。デフォルトでは、過去7日間のアラート データをフェッチします。
最終更新日	データ ソースからコンテキスト データを最後に取得した時刻。

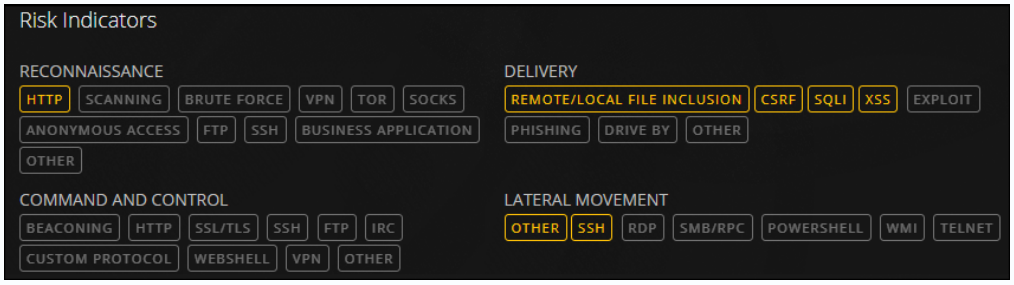
[Live Connect]タブ

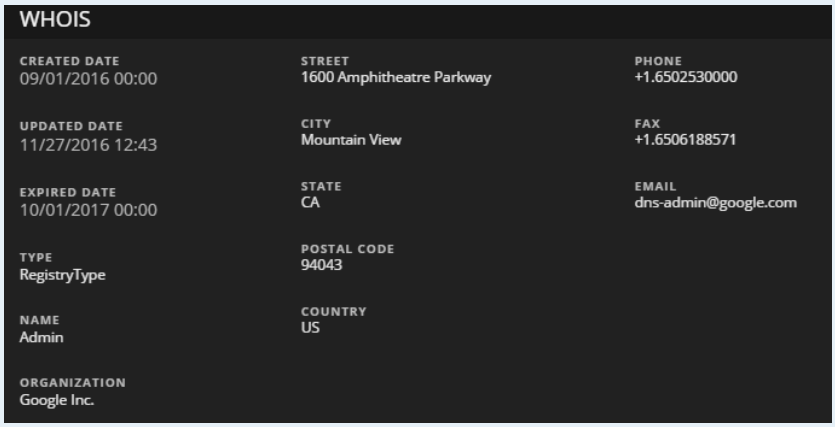
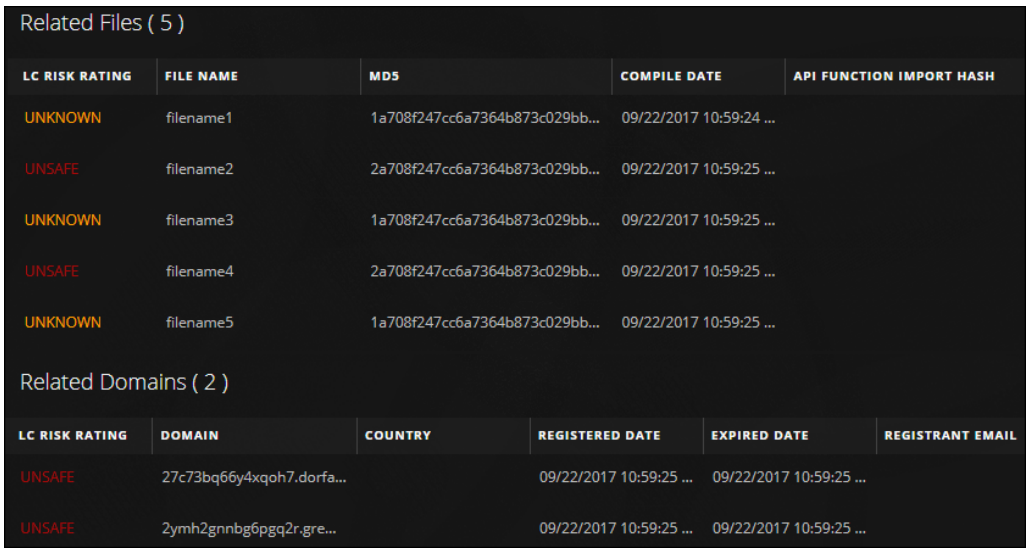
次の図は、[コンテキスト]パネルの[Live Connect]タブの例であり、表では表示される以下の情報について説明しています。



フィールド	説明
レビューステータス	選択したLive Connectエンティティ(IP、ファイル、ドメイン) をアナリストがレビューしたステータス。これにより、組織内で、アナリストのアクティビティの可視性が高まります。 **ステータス** ステータスのタイプを以下に示します。 • **新規**:IPアドレスのルックアップの結果が組織内で最初に表示された場合。 • **表示済み**:組織内のアナリストがIPアドレスのルックアップの結果をすでに表示済みの場合。 • **安全と判定**:組織内のアナリストがIPアドレスのルックアップの結果をすでに表示済みで安全と判定している場合。 • **高リスクと判定**:組織内のアナリストがIPアドレスのルックアップの結果をすでに表示済みで高リスクと判定している場合。
リスク アセスメント	Live Connectの分析とアナリスト フィードバックに基づく、選択したLive Connectエンティティ(IP、ファイル、ドメイン) のリスク評価を表示します。リスク評価のカテゴリは次のとおりです。 • **安全**:Live Connectエンティティは、安全であると見なされています。 • **不明**:Live Connectには、リスクを計算するためのこのエンティティに関する十分な情報がありません。 • **高リスク**:コミュニティによる分析とリスクの理由に基づいて「高リスク」と判定します。「高リスク」と判定されたエンティティは、直ちに注意を要します。 • **疑わしい**:コミュニティによる分析とリスクの理由に基づいて「疑わしい」と判定します。分析は、アクションを必要とする脅威となる可能性のあるアクティビティを示しています。 • **危険**:コミュニティによる分析とリスクの理由に基づいて「危険」と判定します。 高リスク、疑わしい、危険と評価されたエンティティには、適宜関連するリスクの理由が表示されます。

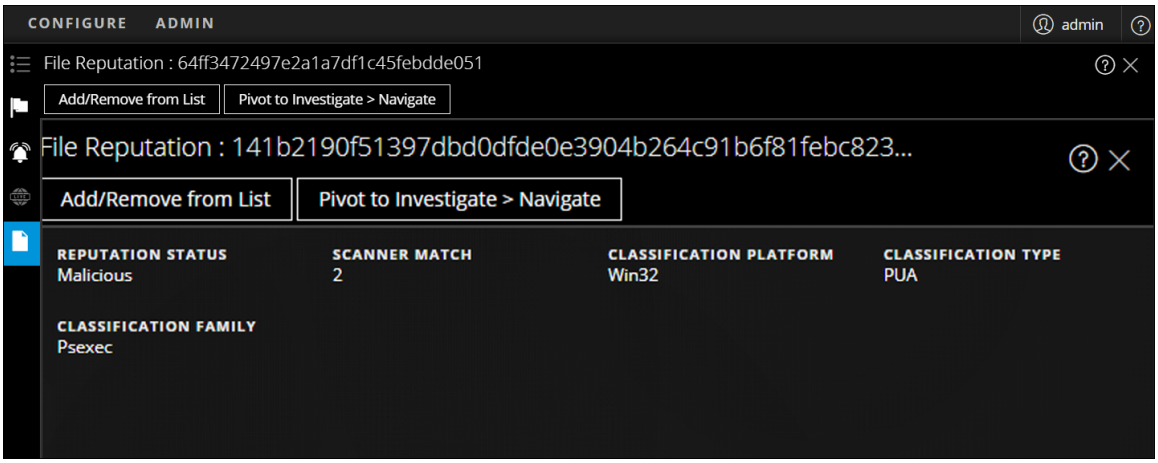
フィールド	説明
リスク評価のフィードバック	 リスク評価のフィードバックにより、アナリストはエンティティに関する脅威インテリジェンスのフィードバックをLive Connectサーバに送信できます。 • **アナリスト スキル レベル** アナリスト スキル レベルのオプションを以下に示します。 ◦ **Tier 1**: このレベルのアナリストは改善のための処理手順を定義し、SOC(セキュリティ オペレーション センター) の他の領域にインシデントをエスカレーションする必要があるかどうかを判断します。これがデフォルト値です。 ◦ **Tier 2**: アナリストはインシデントを調査し、インテリジェンスを収集し、SOC内のさまざまなワークフローにフィードバックします。 ◦ **Tier 3**: 調査結果をSOC組織と共有するアナリストです。一般的にインシデントを管理し、インシデント対応に必要なスキルとツールに関する幅広く深い知識があります。 **注 :** NetWitness Platform(アナリスト) の新しいユーザを作成するときに、管理者はユーザをTier 1、Tier 2、Tier 3のアナリストとして特定できる必要があります。 • **リスクの確認** : 選択したLive Connectエンティティ(IP、ファイル、ドメイン) のリスクを確認します。リスクの確認のカテゴリは次のとおりです。 ◦ **安全 :** Live Connectエンティティは、安全であると見なされています。 ◦ **不明** : リスクの確認を行うために十分な情報がアナリストにありません ◦ **高リスク**: コミュニティによる分析とリスクの理由に基づいて「高リスク」と判定します。「高リスク」と判定されたエンティティは、直ちに注意を要します。 ◦ **疑わしい**: コミュニティによる分析とリスクの理由に基づいて「疑わしい」と判定します。分析は、アクションを必要とする脅威となる可能性のあるアクティビティを示しています。 ◦ **危険 :** コミュニティによる分析とリスクの理由に基づいて「危険」と判定します。 • **信頼度レベル**: Live Connectエンティティのフィードバックに対するアナリストの信頼度レベルです。信頼度レベルのカテゴリーは、高、中、低です。 • **リスク インジケータ タグ**: 分析に基づいてタグ カテゴリを選択できます。

フィールド	説明
コミュニティ アクティビティ	次のようなコミュニティ アクティビティ: • コミュニティで最初に表示された日付。 • IP/ファイル/ドメインが最初に表示された時間からの経過時間(現在の時間-初めて表示された時間)。 **コミュニティ アクティビティのトレンドが表示されます。** RSAコミュニティの中で、IPアドレスが分かっている場合は、次のコミュニティ アクティビティのトレンドのグラフィカル表示が表示されます。 • 所定の期間にLive Connectコミュニティで IPアドレスを閲覧したユーザの割合(%単位)。 • IPアドレスに関するフィードバックを送信したユーザの割合(%単位)。 • 所定の期間にIPアドレスを安全でないとしてマークしたユーザの割合(%単位)。
リスク インジケータ	 リスク インジケータは、コミュニティによってエンティティ(IPアドレス、ファイル、ドメイン)に割り当てられたタグに基づいてハイライト表示されます。 タグのカテゴリーは、スキャン、デリバリー、コマンド & コントロール、ラテラル ムーブメント、特権エスカレーション、パッケージ & 漏洩です。 これらのタグはサンプルであり、Live Connectサーバがコミュニティから受信した入力によって異なります。アナリストは、レビューのフィードバックを提供する時に、適切なリスク指標タグを選択できます。ハイライト表示されたタグは、選択したエンティティがその特定のカテゴリとタグに関連づけられていることを示します。ハイライト表示されているタグをクリックすると、タグの説明が表示されます。
ID	選択したエンティティまたはメタ値の次の識別情報を提供します。 IPアドレスの場合:ASN(自律システム番号)、プレフィックス、国コードと国名、登録者(組織)、日付。 ファイル ハッシュの場合:ファイル名、ファイル サイズ、MD5、SH1、SH256、コンパイル時刻、Mimeタイプ。 ドメインの場合:ドメイン名と関連IPアドレス。
証明書情報	選択したファイル ハッシュに関する証明書情報(証明書発行元、証明書の有効性、署名アルゴリズム、証明書シリアル番号)を提供します。

フィールド	説明
WHO IS情報	 **WHO IS**情報は、特定のドメインの所有権の詳細を提供します。 ドメイン所有者に関する情報(作成日、更新日、期限切れの日付、タイプ(登録タイプ)、名前、組織、郵便番号と住所、国、電話、ファックス、メール)が表示されます。
関連ファイル	関連ファイルはエンティティ タイプがIPおよびドメインの場合に表示されます。既知の関連ファイルのリストが、Live Connectのリスク評価(安全、高リスク、不明)、ファイル名、MD5、コンパイル時刻と日付、API関数、インポート ハッシュ、Mimeタイプとともに表示されます。
関連ドメイン	関連ドメインはエンティティ タイプがIPおよびファイルの場合に表示されます。既知の関連ドメインのリストが、Live Connectのリスク評価(安全、高リスク、不明)、ドメイン名、国名、登録日、期限切れの日付、登録者のメール アドレスとともに表示されます。
関連IP	 関連IPはエンティティ タイプがドメインおよびファイルの場合に表示されます。既知の関連IPのリストが、Live Connectのリスク評価(安全、高リスク、不明)、IPアドレス、ドメイン名、国コードと国名、国名、登録日、期限切れの日付、登録者のメール アドレスとともに表示されます。

[ファイル レピュテーション] タブ

[ファイル レピュテーション] の [コンテキスト ルックアップ] パネルには、そのファイルのレピュテーションのステータスが表示されます。



フィールド	説明
レピュテーション ステータス	filehashのレピュテーション ステータス。レピュテーションのステータスの詳細については、『*UEBAユーザ ガイド*』の「ファイル レピュテーションの表示」を参照してください。
スキャナーー致	最後のスキャンで、マルウェアまたは疑わしいアクティビティを検出したスキャナーの数。
分類プラットフォーム	プラットフォームに基づき、クエリされたfilehashのクラス分け。たとえば、プラットフォームをWin 32にすることができます。
分類タイプ	タイプに基づき、クエリされたfilehashのクラス分け。
分類ファミリー	マルウェア ファミリー名に基づき、クエリされたfilehashのクラス分け。

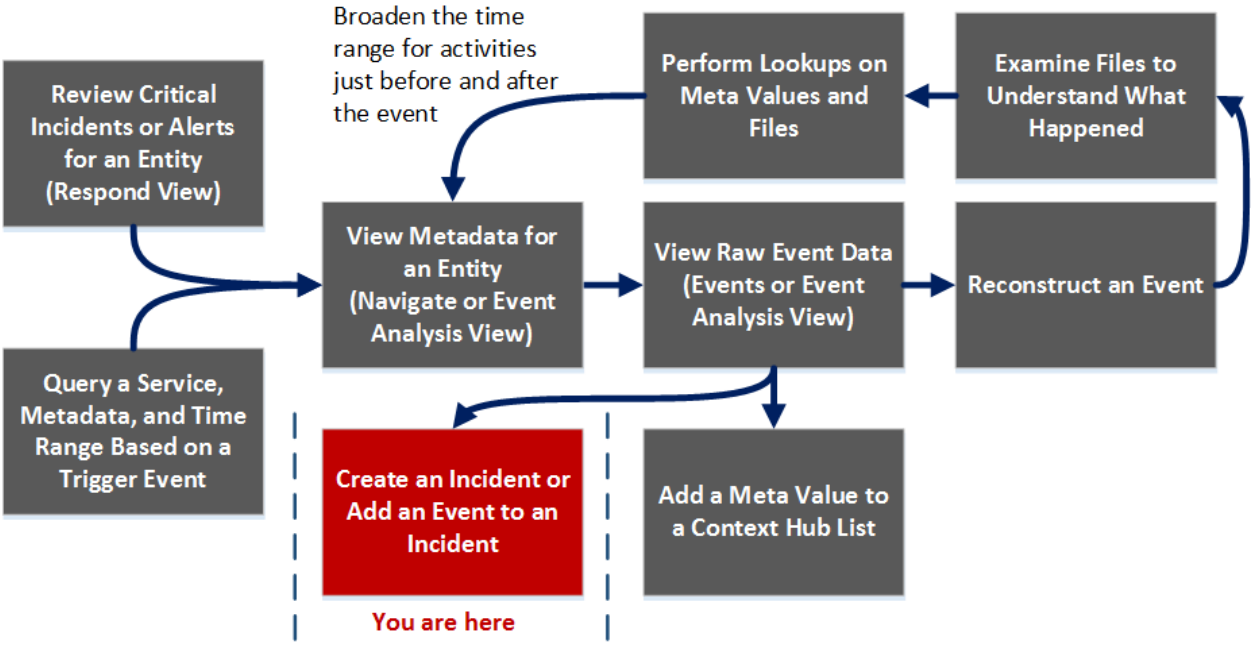
[インシデントの作成]ダイアログ

[インシデントの作成]ダイアログでは、アナリストは[イベント]ビューで選択したイベントからインシデントを作成できます。インシデントは[対応]ビューで作業しているインシデント対応者が使用できるようになります。

このダイアログにアクセスするには、[調査]>[イベント]ビューで、ツールバーから**[インシデント]>[新しいインシデントの作成]**を選択します。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング

ユーザ ロール	実行したいこと	手順
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加*	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加	結果の追加のコンテキストを検索

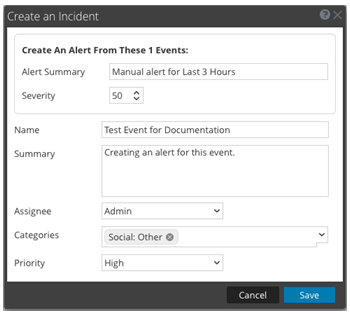
*このタスクは現在のビューで実行できます。

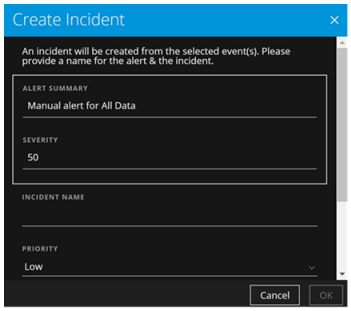
関連トピック

- NetWitness Investigateの仕組み
- [ナビゲート]ビュー
- [レガシー イベント]ビュー

簡単な説明

次の図に、[インシデントの作成]ダイアログの例を示します。機能は表で説明します。





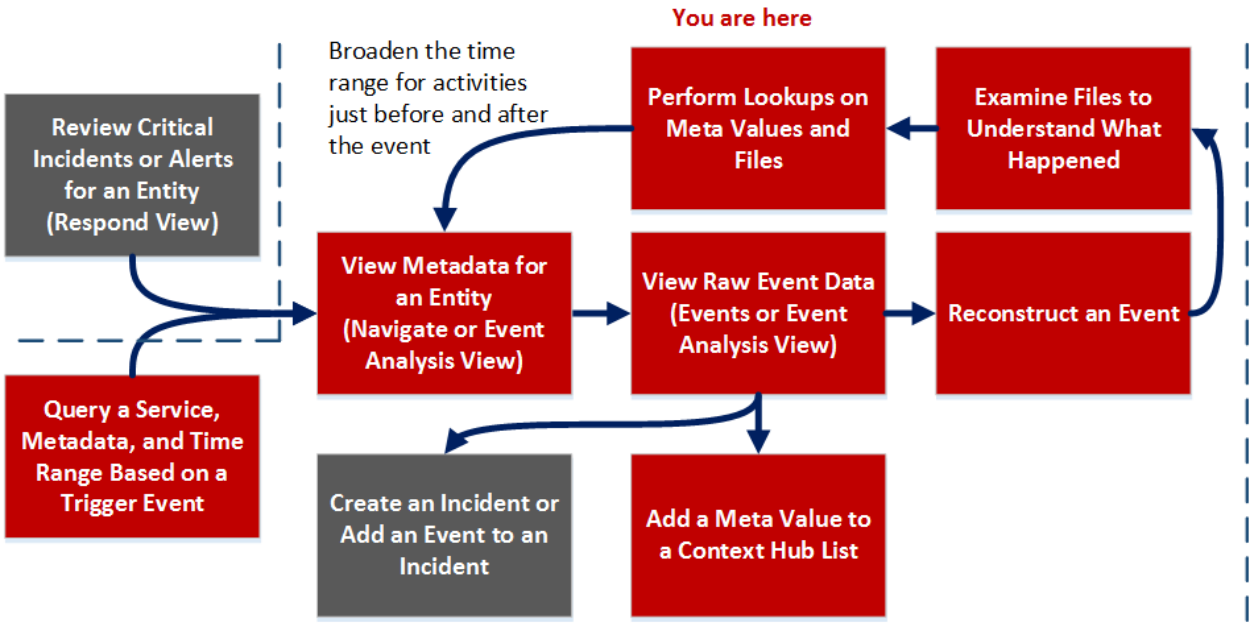
機能	説明
アラートの作成	[アラート サマリ]フィールドには、アラートを選択した時のクエリが自動入力されます。これは、このインシデントを作成する時に選択されていたクエリです。[重大度]フィールドには、選択したアラートの重大度として、1~100の整数が示されます。
名前	(必須) インシデントを識別する名前を指定します。この例では、名前は「Sample Incident」です。このインシデントに追加されるイベントの特性を明確に識別する名前を指定します。
まとめ	(オプション) インシデントのオプションの説明を指定します。優れたサマリを指定すると、他のアナリストや対応者がインシデントを明確に識別することができます。
割り当て先	(オプション) インシデントをSOC内のユーザに割り当てます。[割り当て先]をクリックすると、インシデントに対応するSOC担当者のユーザ名がドロップダウン リストに表示されます。
カテゴリ	(オプション) インシデントのカテゴリーを識別します。[カテゴリー]をクリックすると、インシデントのカテゴリーとサブカテゴリーのドロップダウン リストが表示されます。インシデントが属するカテゴリー(複数可)を選択できます。カテゴリーは、[Environmental]、[Error]、[Hacking]、[Malware]、[Misuse]、[Social]の主要グループに分類されます。
優先	インシデントの優先度を識別します。[優先]をクリックすると、優先度(重要、高、中、低)のドロップダウンリストが表示されます。
キャンセル	変更を保存せずにダイアログを閉じます。
保存	インシデントを保存して、ダイアログ ボックスを閉じます。インシデントが正常に作成されたことを示すメッセージが表示されます。

[イベント]ビュー

[イベント]ビューでは、アナリストは、イベントのリストを表示し、分析対象イベントを選択するほか、データ内の重要なパターンを的確に特定するインタラクティブな機能を使用して、RAWイベントとメタデータを表示することができます。これは、静的な[レガシー イベント]ビューと[イベント再構築]ビューの代わりに使用することをお勧めします。[イベント]ビューでは、ネットワーク、ログ、エンドポイント イベントを表示できます。[イベント]ビューには、パケット、テキスト、ログ、メールの再構築が表示されます。イベントのWeb再構築を開くと、[レガシー イベント]ビューで使用したものと同じWeb再構築が表示されます。

ワークフロー

次の図は、NetWitnessの[調査]で実行できるタスクを示す概要レベルのワークフローです。[イベント]ビューのタスクが赤色でハイライト表示されています。このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』

ユーザ ロール	実行したいこと	手順
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行*	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示*	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示*	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築*	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証*	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行*	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加*	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加*	結果の追加のコンテキストを検索

*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー - [パケット]パネル
- [イベント]ビュー - [テキスト]パネル
- [イベント]ビュー - [ファイル]パネル
- [イベント]ビュー - [メール]パネル

簡単な説明

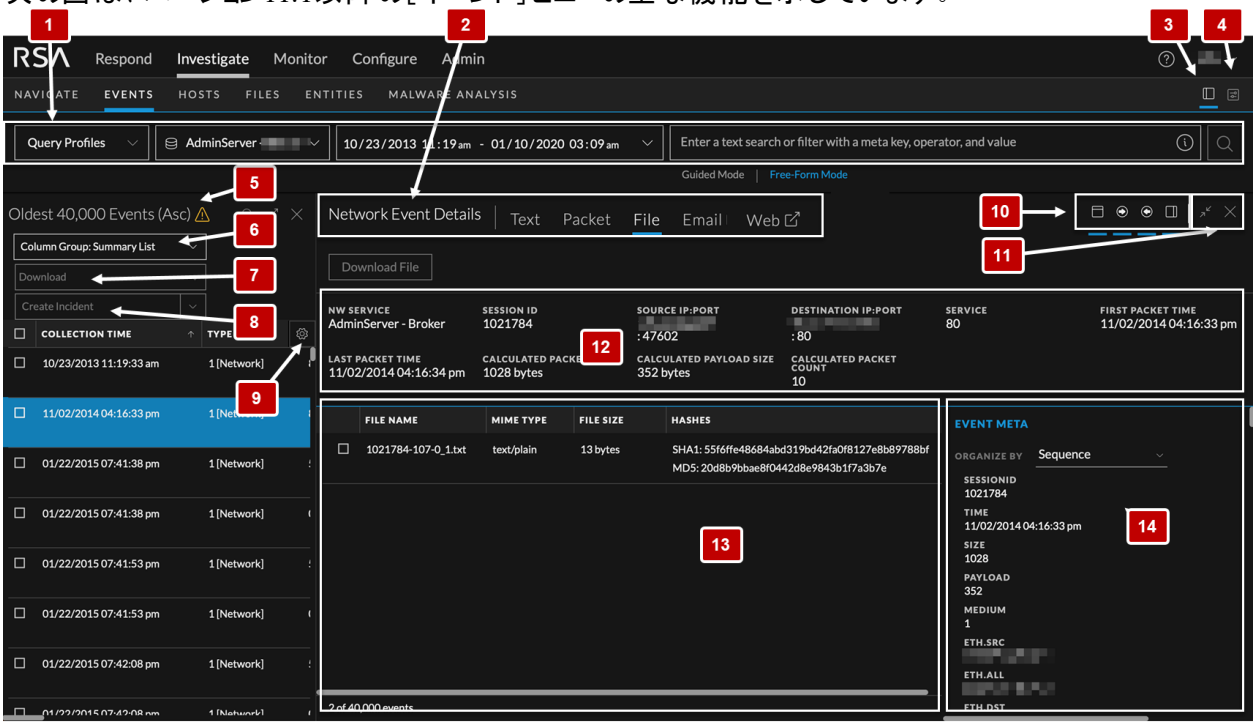
このビューには複数のアクセス ポイントがあります。詳細については「[イベント]ビューでの調査の開始」を参照してください。[対応]ビューから[イベント]ビューにアクセスすると、インシデント内の選択したイベントの分析を確認できます。オプションは、[調査]ビュー内からイベントを開いたときに使用できるオプションのサブセットです。機能を完全に有効化し、他のイベントを確認するには、[イベント]ビューに直接移動します([調査]>[イベント])。

[イベント]ビューの[イベント]パネルには、イベントが時間の昇順で表示されます。表示されるイベントは、[[ナビゲート]ビュー]ビューまたは[レガシー イベント]ビューのドリルダウン ポイントの結果、または[イベント]ビューのクエリ バーで入力されたクエリの結果です。

クエリの入力フィールドが表示されるので、サービスや時間範囲を選択し、オプションのクエリを入力できます。クエリを送信すると、調査対象のサービスによって、最大10,000イベントの結果がカウントされ、10,000個のネットワーク、ログ、エンドポイント イベントが[イベント]パネルにロードされます。表示される列は、選択した列グループによって異なります。列の並べ替えやサイズ変更、標準提供またはカスタムの列グループの選択、表示する列の個別の選択を行えます。関心のあるイベントが見つかった場合は、イベントをクリックすると、新しいパネルで再構築(パケット、テキスト、ファイル)が開きます。

注: 11.3より前のバージョンでは、最初の100イベントがロードされます。リストをスクロールして、リストの最後尾にある[**次の100イベントを表示**]をクリックします。次のページに含まれているイベントが100個より少ない場合は、残りのイベント数を反映してボタンの表示が変わります。

次の図は、バージョン11.1以降の[イベント]ビューの主な機能を示しています。



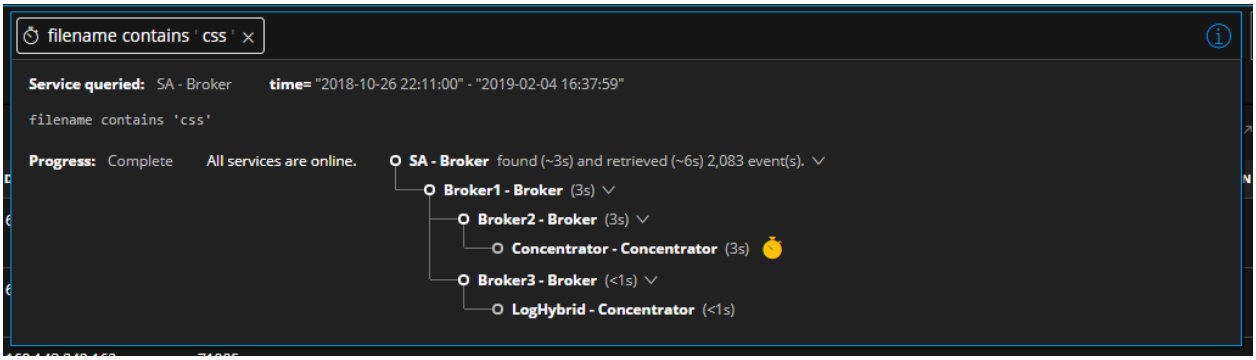
1 **クエリ バー**: サービスを選択すると、サービス セレクター、時間範囲セレクター、入力したクエリが表示されます。「[イベント]ビューでの調査の開始」の説明に従ってサービスを選択し、「[イベント]ビューでの結果のフィルタリング」の説明に従ってクエリを調整できます。をクリックすると、クエリが送信され、選択したサービスに対してデータ ロードの要求が送信されます。バージョン11.3以降では、(コンソール アイコン)をクリックすると、クエリ

	コンソールが開き、クエリの詳細なステータスが表示されます(後掲の「クエリ コンソール」を参照) 。
2	分析対象イベントのタイプと再構築のタイプは、見出しに反映されます。 • イベント タイプには、**ネットワーク イベントの詳細**、**ログ イベントの詳細**、**エンドポイント イベントの詳細**があります。 • イベント タイプで使用できる分析のタイプは、テキスト、パケット、ファイル、メール、Webです。ネットワーク イベントでは、テキスト、パケット、ファイル、メール(バージョン11.4.1以降) のすべてのタイプの分析を使用できます。ログおよびエンドポイントのイベントでは、テキスト分析のみを使用します。メール タイプ(バージョン11.4.0.x以前) とWebタイプでは、[イベント]ビューで現在のイベントがメールまたはWebの再構築として開かれます。詳細については、「[イベント]ビューでのイベントの再構築」を参照してください。
3	[イベント]パネルが閉じている場合に再度開きます。詳細については、「[イベント]ビューでのイベントの分析」を参照してください。
4	[イベント]ビューの環境設定を設定します(「[イベント]ビューの構成」を参照) 。
5	[イベント]パネルのタイトル。 • バージョン11.3以降では、[イベント]パネルのタイトルが以前のバージョンのタイトルとわずかに異なり、行番号インジケータが追加されました。タイトルには、イベント数とソート順が表示されます。たとえば、[**24,000イベント(昇順)**]は、24,000個のイベントが見つかったことと、それらが昇順で表示されていることを意味します。10,000個を超えるイベントが見つかった場合は、最も古い10,000イベントのみが昇順で表示され、ロードされなかったイベントがあることを示す黄色の三角形が表示されます。これは、クエリを絞り込む必要があることを示している可能性があります。ここに表示されるイベントを絞り込む方法の詳細については、「[イベント]ビューでの結果のフィルタリング」を参照してください。 • 11.3より前のバージョンでは、見つかったイベントの数が表示され、一度に100イベントをロードできます。バージョン11.4以降では、  をクリックすると、[テーブルでテキストを検索]ダイアログが開きます。
6	[列グループ]ドロップダウンには、[イベント]パネルに適用できる標準提供の列グループとカスタム列グループが表示されます。標準提供の列グループは、バージョン間で更新されることがあります。標準提供の列グループには、Email Analysis、Endpoint Analysis、Malware Analysis、Outbound HTTP、Outbound SSL/TLS、Summary Listなどがあります。デフォルトの列グループはSummary Listです。詳細については、「イベント リストでの列と列グループの使用」を参照してください。
7	[ダウンロード]ドロップダウン メニューには、イベント データのダウンロードに使用できるオプションが表示されます。オプションはそれぞれ、[ログ]、[表示可能なメタ]、[ネットワーク]です(「結果のダウンロードと処理」を参照) 。[イベント環境設定]ダイアログでは、イベント タイプ データで優先的に使用する形式を変更できます(「[イベント]ビューの構成」を参照) 。
8	[インシデントの作成]ボタンをクリックして、イベントからインシデントを作成できます。[インシデントへの追加]ボタンを使用すると、既存の未解決インシデントに選択したイベントを追加できます(「[イベント]ビューでのインシデントへのイベントの追加」と「[レガシー イベント]ビューでのインシデントへのイベントの追加」を参照) 。
9	列の選択設定が表示され、[イベント]パネルに表示する列を個別に選択できます。詳細については、「イベント リストでの列と列グループの使用」を参照してください。

10	イベント ヘッダーの表示/非表示、リクエストとレスポンスの表示/非表示、イベント メタ パネルの表示を行うコントロール。詳細については、「[イベント]ビューでのイベントの分析」を参照してください。
11	パネルのサイズを変更して、パネルを閉じるコントロール。詳細については、「[イベント]ビューでのイベントの分析」を参照してください。
12	イベント ヘッダーには、現在分析中のイベントに関するサマリー情報が表示されます。選択したイベントが、[イベント]パネルで青色の背景でハイライト表示されます。サマリー情報は、イベント タイプ(パケット、ログ、エンドポイント)によって異なります。
13	現在分析中のイベントのイベント データ。
14	[イベント メタ]パネルには、データで見つかったメタ キーと値が表示されます。このデータは、アルファベット順と生成順という2つの方法でソートできます。一部のメタ データは検索可能です。双眼鏡アイコンをクリックすると、関連するデータがイベント データでハイライト表示されます(「[イベント]ビューでのイベントの分析」を参照)。 • パケットの場合、データはペイロードと呼ばれ、リクエストとレスポンスの形式で表示されます。 • ログ イベントの場合、データはRAWログからのテキスト行です。 • エンドポイント イベントの場合、イベント データは、ネットワーク内のホストで実行されているNetWitness Endpointエージェントからのデータに関連します。たとえば、単一プロセス、ドライバ、DLL、ファイル(実行可能ファイル)、サービス、Autorunのほか、ログインしているユーザに関連した情報などです(エンドポイント イベント データの詳細については、『*NetWitness Endpointユーザ ガイド*』を参照してください)。

クエリ コンソール

(コンソール アイコン)をクリックすると、クエリ コンソールが開き、クエリの詳細なステータスが表示されます。



クエリ コンソールでは、クエリによって照会されたサービス、時間範囲、メタデータのほか、クエリのステータスに関するリアルタイム情報も確認できます。コンソールの下部にある進行状況バーには、クエリの完了率が表示されます。ステータス情報からは、クエリで今行われている処理(実行中、キューに登録済み、クエリ対象サービスのインデックス ファイルの読み取り中、イベントの取得中、完了など)についての詳細を知ることができます。ステータスと致命的でないメッセージは受信されるとすべて表示され、致命的でないエラーが発生すると、境界線の色が変わります。詳細については、「クエリのステータスの表示」を参照してください。

クエリ コンソールに表示されるメッセージの中には、追加の説明が必要なものがあります。

メッセージ: インデックス スライス%3%のメタ キー%2%で%1%の最大値制限(valueMax)に達しました

説明: クエリ対象インデックスで、指定されたメタ キーのvalueMaxプロパティに到達しました。管理者は、ADMIN > Services > [Service Name] > Files > index-[service type].xmlまたはindex-[service type]-custom.xmlのインデックス ファイルでこの値を設定します。たとえば、インデックス ファイルの次のステートメントでは、clientというメタ キーの値の数がデフォルトで250,000に制限されています。

```
<key description="Client Application" level="IndexValues" name="client"
format="Text" valueMax="250000" />
```

メッセージ: チャネル%2%のクエリは、時間の使用制限を超過しているため、システムによって自動でキャンセルされました。タイムアウト値を確認してください。

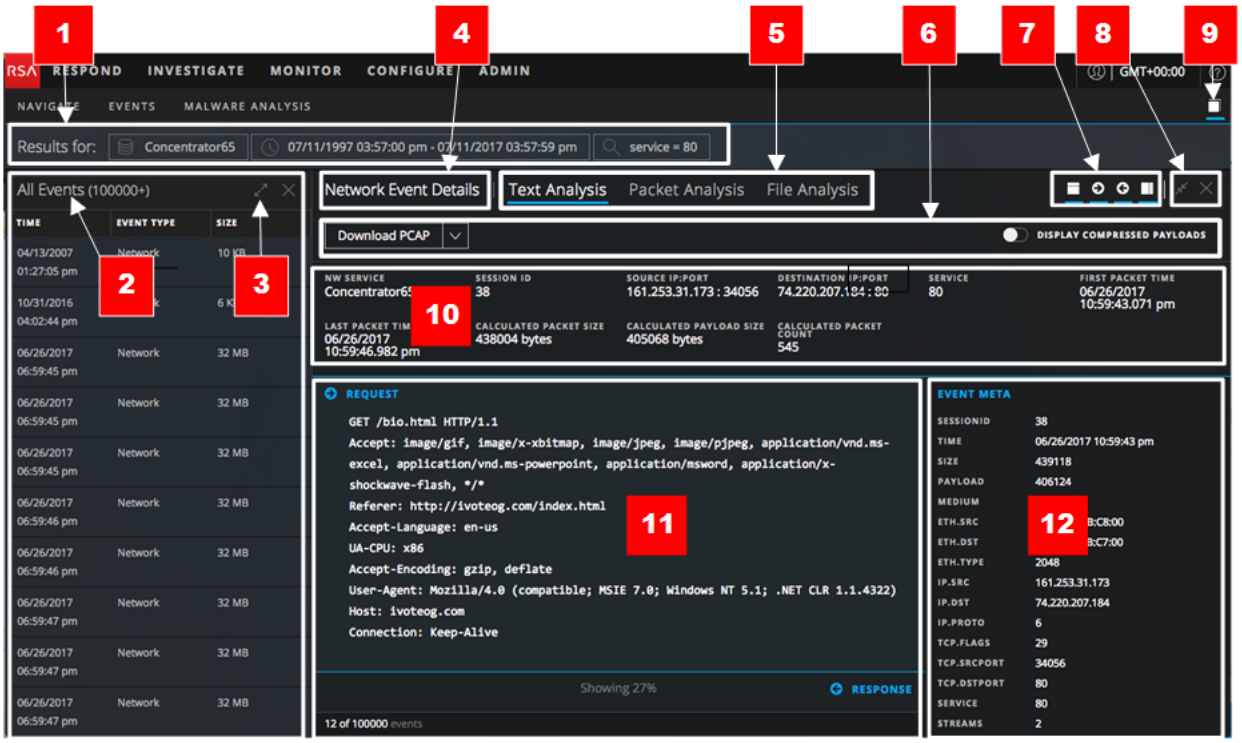
実行時間に対する操作あたりの制限がサーバにあり、要求された操作がこの制限を超過しました。このエラーを回避するには、小さい時間範囲などの小さな要素に操作を分割します。

メモリ制限の%1%に達しました。これは、max.query.memoryを設定することによって制御されます

メモリ使用率に対する操作あたりの制限がサーバにあり、要求された操作がこの制限を超過しました。この制限はサーバのメモリ容量に関連しており、管理者はこの値を[**管理**]>[**サービス**]>[<**サービス名**>]>[**sdk**]>[**config**]で調整できます。このエラーを回避するには、小さい時間範囲などの小さな要素に操作を分割します。

バージョン11.0.0.x(生産終了)の簡単な説明

次の図は、バージョン11.0.0.xの[イベント分析]ビューの主な機能を示します。



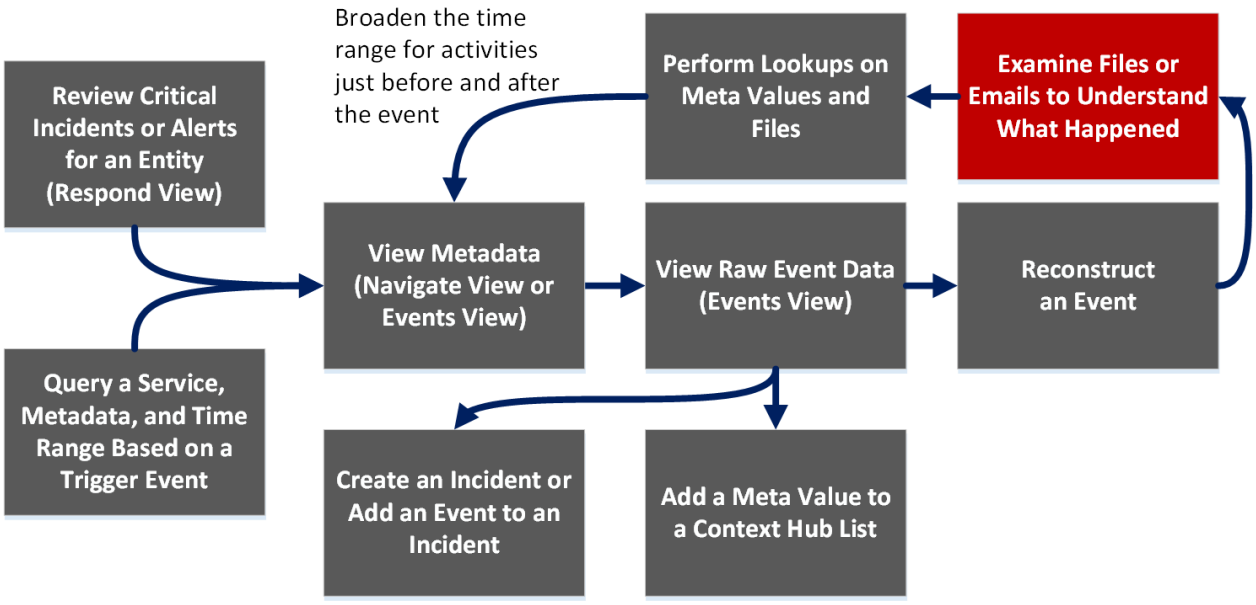
1 読み取り専用階層リンクは、選択されたサービス、時間範囲、[ナビゲート]ビューまたは[イベント]ビューに入力されたクエリを表示します。

2	これは、[ナビゲート]または[イベント]ビューで作成されたクエリに基づくイベントの読み取り専用リストです。[イベント]パネルにはイベントの数が表示されます。列の並べ替えとサイズ変更ができます。リストの一番下までスクロールし、イベントをさらにロードすることができます(「[イベント]ビューでのイベントの分析」を参照)。
3、8	パネルのサイズを変更して、パネルを閉じるコントロール。
4	分析対象イベントのタイプは、ネットワーク イベントの詳細、ログ イベントの詳細、エンドポイント イベントの詳細の各見出しに反映されます。各ビューの詳細については、「[イベント]ビューでのイベントの分析」を参照してください。
5	イベント タイプに利用可能な分析のタイプ。ネットワーク イベントは、テキスト、パケット、ファイルの全3種類の分析を使用できます。ログおよびエンドポイントのイベントでは、テキスト分析のみを使用します。
6	これらのオプションは、分析のタイプによって異なります。詳細については、「[イベント]ビューでのイベントの分析」を参照してください。
7	イベント ヘッダーの表示/非表示、リクエストと応答の表示/非表示、イベント メタ パネル(12) の表示を行うコントロール。これらのコントロールの詳細については、「[イベント]ビューでのイベントの分析」を参照してください。
9	[イベント]パネルまたは[イベント メタ]パネルが閉じている場合に再度開きます。
10	イベント ヘッダーには、イベントに関するサマリ情報が表示されます。この情報は、イベント タイプ(パケット、ログ、エンドポイント) によって異なります。
11	イベント データ(パケットのペイロードと呼ばれる場合があります) 。ログ イベントまたはエンドポイント イベントのイベント データは、パケットに示されるリクエストと応答ではなく、通常、RAW ログからのテキスト行です。
12	[イベント メタ]パネルには、データで見つかったメタ キーと値が表示されます。一部のメタ データは検索可能です。双眼鏡アイコンをクリックすると、関連するデータがイベント データでハイライト表示されます(「[イベント]ビューでのイベントの分析」を参照)。

[イベント]ビュー - [メール]パネル

[メール]パネル([**イベント**]＞[**メール**]) では、イベントについて受信したメールとそれに関連づけられている添付ファイルのリストを表示できます。

ワークフロー

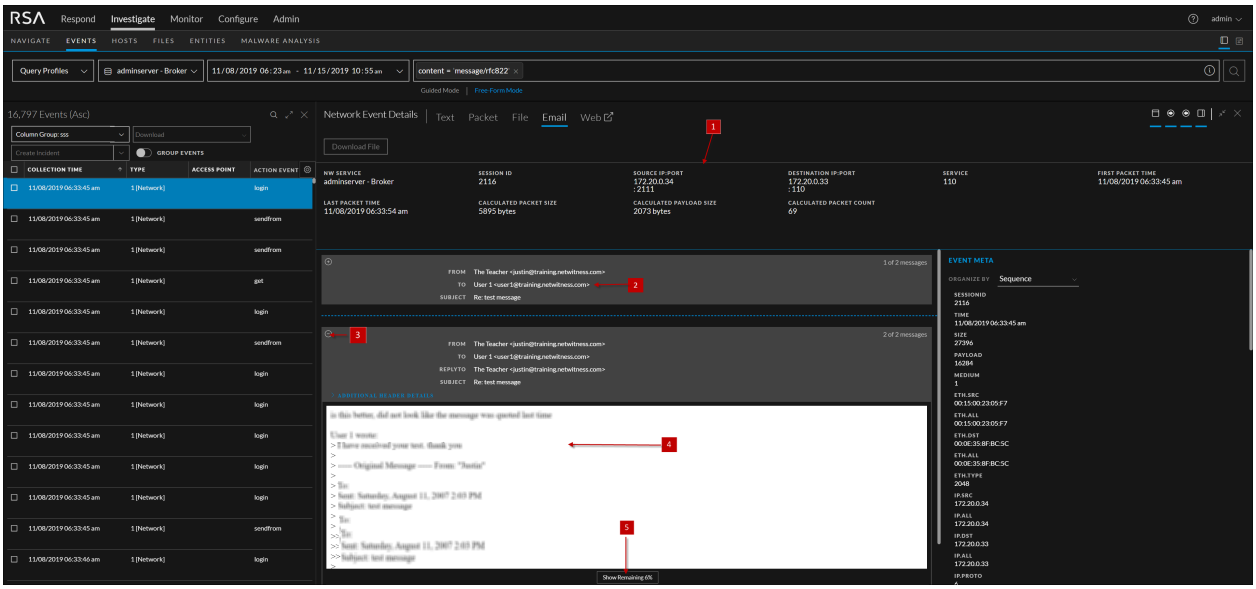


関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー
- [イベント]ビュー - [テキスト]パネル
- [イベント]ビュー - [パケット]パネル
- [イベント]ビュー - [ファイル]パネル

簡単な説明

[メール]パネルには、ネットワーク イベントに関連づけられているメールのリストが表示されます。アナリストがメールを開くと、メール再構築が、そのメールに関連づけられた添付ファイルと追加のヘッダー詳細 (ある場合) とともに表示されます。
次の図は、メール再構築の機能を示しています。



1 選択したイベントの詳細が表示されます。
2 メール ヘッダーの詳細が表示されます。
3 これをクリックすると、メールの展開表示と折りたたみ表示が切り替わります。
4 メールの内容が表示されます。
5 [**残り%を表示**]をクリックすると、メール全体が表示されます。

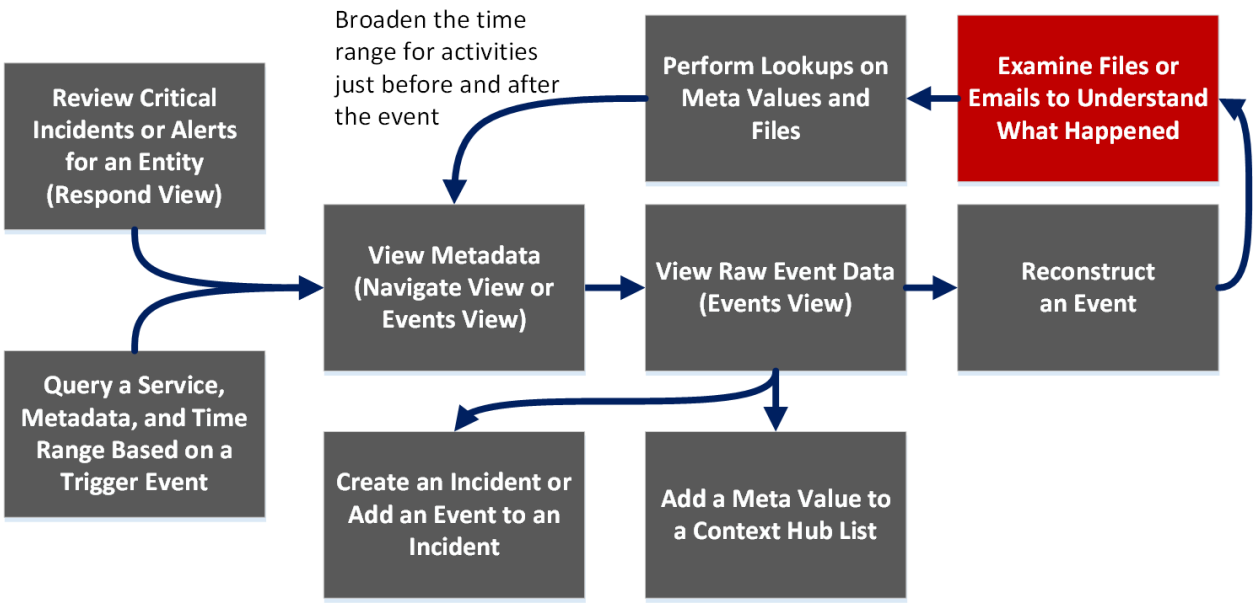
次の表は、メール内のすべてのフィールドについて説明しています。

フィールド	説明
変更前	メールの送信者のメール アドレスが表示されます。
To	メールの受信者のメール アドレスが表示されます。
CC(カーボン コピー)	メールの追加の受信者のメール アドレスが表示されます。このフィールドが表示されるのは、送信されたメールに値が含まれており、メール アドレスが受信者に表示される場合だけです。
BCC	追加の受信者のメール アドレスが非公開で表示されます。このフィールドが表示されるのは、送信されたメールに値が含まれており、メール アドレスが受信者に表示されない場合だけです。
件名	メールの件名が表示されます。
添付ファイル	送信者によって共有され、受信者がダウンロードできるファイルが表示されます。このフィールドが表示されるのは、メールに添付ファイルが含まれている場合だけです。
追加のヘッダー情報	受信日時、送信者、メッセージIDなどのメール イベントの追加の詳細が表示されます。

[イベント]ビュー - [ファイル]パネル

[ファイル]パネル([**イベント**]＞[**ファイル**])では、安全にファイルのリストを表示し、イベントの1つまたは複数のファイルをダウンロードできます。

ワークフロー



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み

ユーザ ロール	実行したいこと	手順
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証*	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加	結果の追加のコンテキストを検索

*このタスクは現在のビューで実行できます。

関連トピック

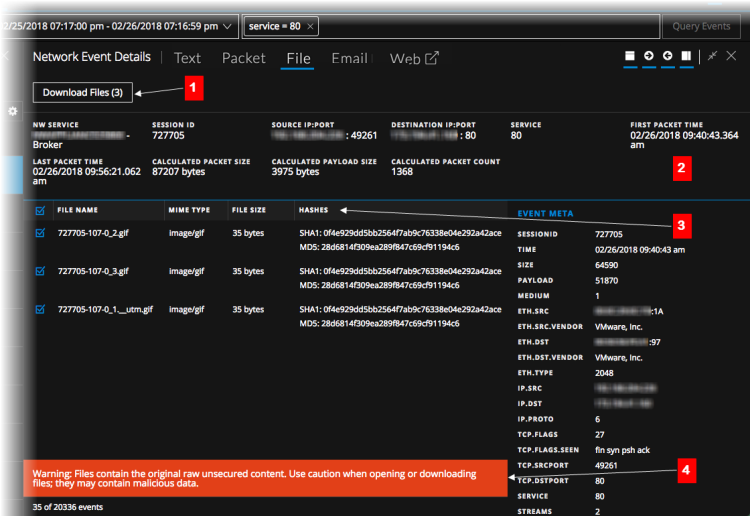
- NetWitness Investigateの仕組み
- [イベント]ビュー
- [イベント]ビュー - [テキスト]パネル
- [イベント]ビュー - [パケット]パネル

簡単な説明

[ファイル]パネルには、ネットワーク イベントに関連づけられているファイルのリストが表示されます。このビューでファイルをダウンロードすることができます。

[ファイル]パネルの例を次に示します。各機能にラベルを付けています。

注: この図の上部に表示されているメールとWebの再構築タイプは、バージョン11.1以降で使用できます。



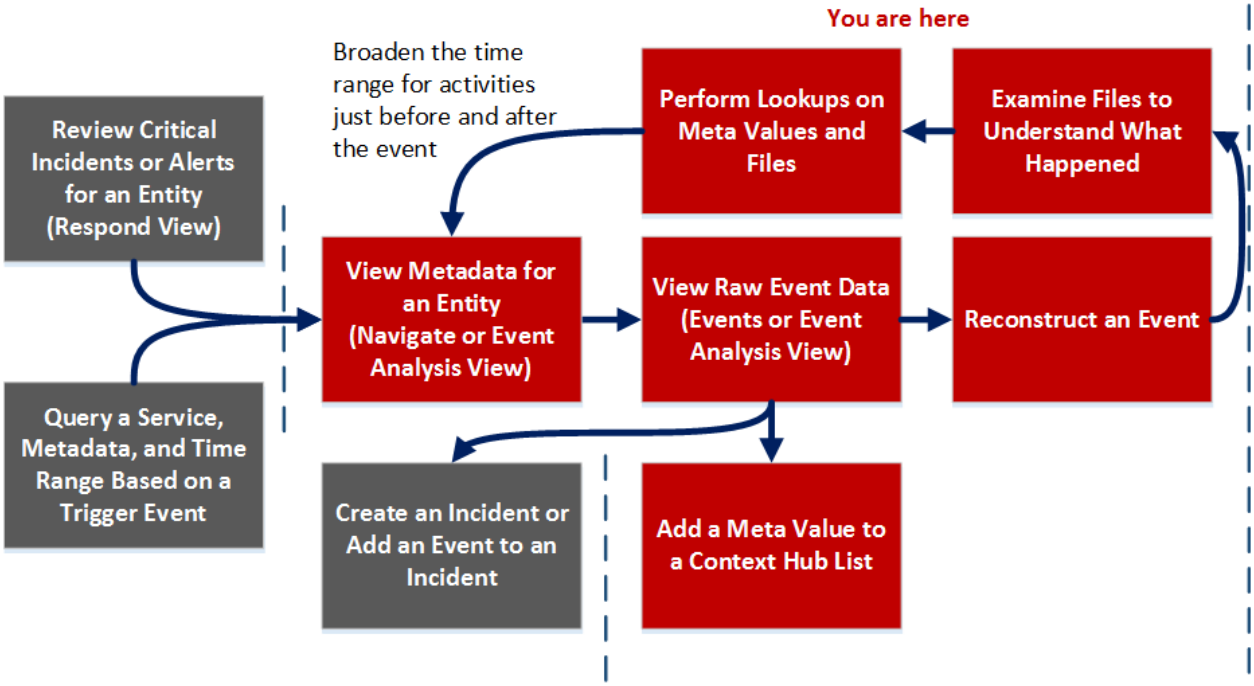
1 クリックして1つまたは複数の選択したファイルをダウンロードします。
2 イベント ヘッダーには、ファイルを含むネットワーク イベントのサマリ情報が表示されます。
3 選択してダウンロードできる、関連づけられているファイルのスクロール可能なリスト。
4 悪意のある可能性があるファイルをダウンロードするときに警告を通知する必要がある確認事項。

[イベント]ビュー - [パケット]パネル

[パケット]パネル(**[イベント]>[パケット]**) では、イベントのパケットとペイロードを安全に表示し、対話形式で分析できます。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示*	[イベント]ビューでのイベントの分析 結果セットの絞り込み

ユーザ ロール	実行したいこと	手順
脅威ハンター	RAWイベント データの表示*	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築*	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証*	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行*	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加*	結果の追加のコンテキストを検索

*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー
- [イベント]ビュー - [テキスト]パネル
- [イベント]ビュー - [ファイル]パネル
- [イベント]ビュー - [メール]パネル

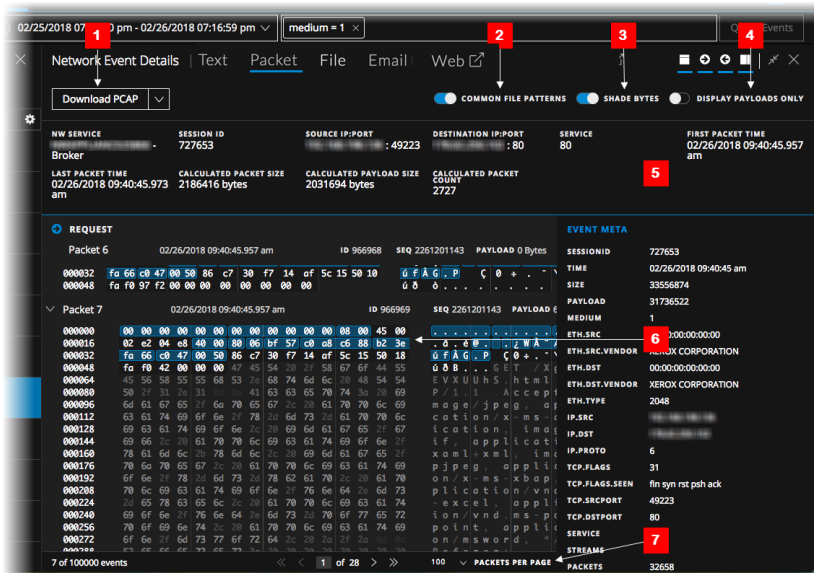
簡単な説明

[パケット]パネルでは、ネットワーク イベントのみを分析できます。[パケット]パネルには、イベントの各パケットが表示されます。パケットのリストはスクロール可能です。スクロールすると、リクエストとレスポンスのラベルと同様にパケットまたはテキストの識別情報も、スクロールされて見えなくならず表示され続けます。

バージョン11.1以降では、ページ移動コントロールを使用して、前後のページへの移動、特定のページへの移動、1ページあたりに表示するパケット数(50、100、300、500)の選択ができます。

一般的なファイル パターン(重要なヘッダーとペイロードのバイト数、16進数とASCIIのバイト数、一般的なファイル シグネチャ) を識別しやすいように、各パケットは塗りつぶしとハイライト表示を使用して表示されます。また、リクエスト/レスポンスの表示、パケット サマリの表示または非表示を調整することができます。

[パケット]パネルの例を次に示します。各機能にラベルを付けています。各機能の詳しい説明と例については、「[イベント]ビューでのイベントの分析」を参照してください。



1	ネットワーク イベントをエクスポートするためのオプションです。より詳細な分析のため、PCAP、すべてのペイロード、要求ペイロード、レスポンス ペイロードをエクスポートし、他者と共有できます。
2	一般的なファイル シグネチャを識別するためのオプションはデフォルトでアクティブ化されます。一般的なファイル シグネチャはオレンジ色でハイライト表示されます。ハイライト表示にカーソルを合わせると、ファイル タイプが表示されます。
3	[バイトの濃淡化]オプションは、16進数バイト(00～FF) を識別しやすくするため濃淡を変えてバイトを表示する機能です。
4	ペイロードを表示するオプションは、パケット ヘッダーのみを非表示にして、ペイロードのスペースを多く残します。
5	イベント ヘッダー。
6	重要なバイトは、青色の背景でハイライト表示されます。ハイライト表示にカーソルを合わせると、吹き出しにメタデータが表示されます。
7	(バージョン11.1以降) ページ操作コントロールで、パケットのリストのページ操作を柔軟に実行できます。使用できないコントロールのイメージはグレー表示になります。たとえば、ページ1を表示しているときには、<<と<のコントロールがグレー表示になります。 << - 最初のページに移動 < - 前のページに移動 1 of 206 - 特定のページに移動 > - 次のページに移動 >> - 最後のページに移動

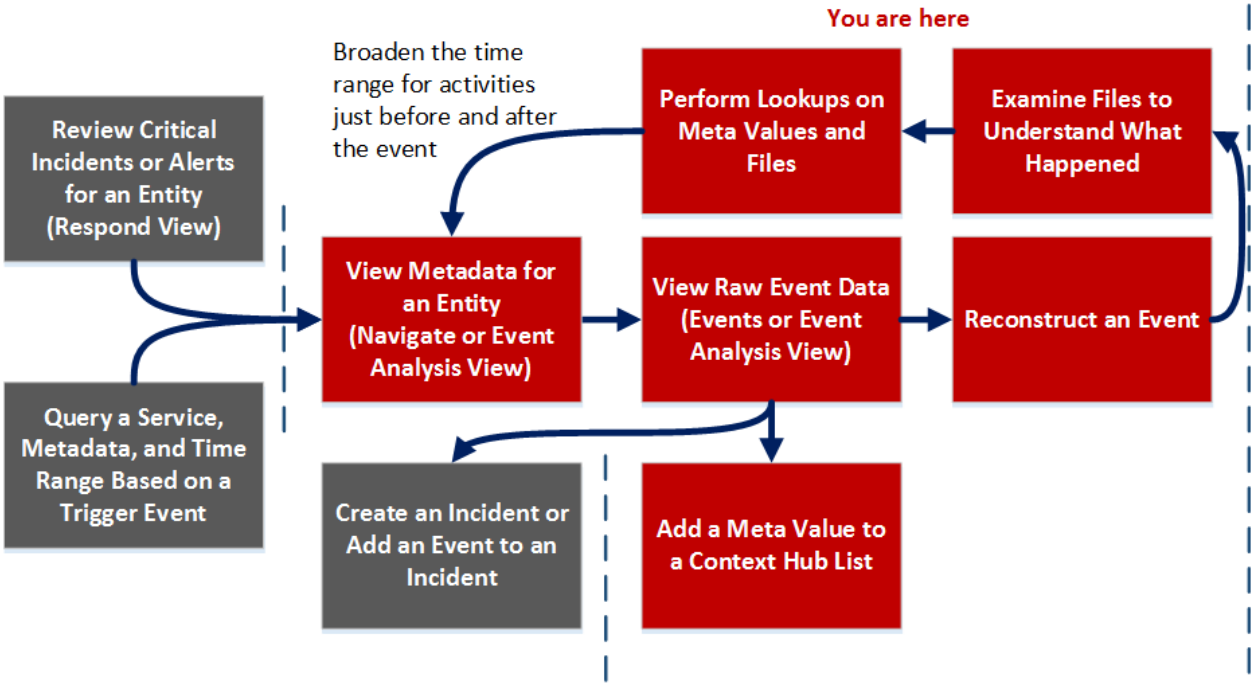
- 1ページあたりのパケット数を選択大量のパケットを再構築している場合は、この制限の値を小さくすることで、パフォーマンスを向上させることができます。

[イベント]ビュー - [テキスト]パネル

[テキスト]パネル(**[イベント]>[テキスト]**) では、イベントのRAWテキスト ペイロードを安全に表示し、分析できます。テキスト再構築には、解凍または圧縮済みのテキストの表示、トランケートされたエントリーの展開、URLとBase64のエンコーディング/デコーディングの実行、ネットワーク イベント、ログ、エンドポイント イベントのダウンロードを実行できる機能が含まれています。テキスト再構築はすべてのタイプのイベント(ネットワーク、ログ、エンドポイント) に使用できます。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』

ユーザ ロール	実行したいこと	手順
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示*	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示*	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築*	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証*	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行*	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加*	結果の追加のコンテキストを検索

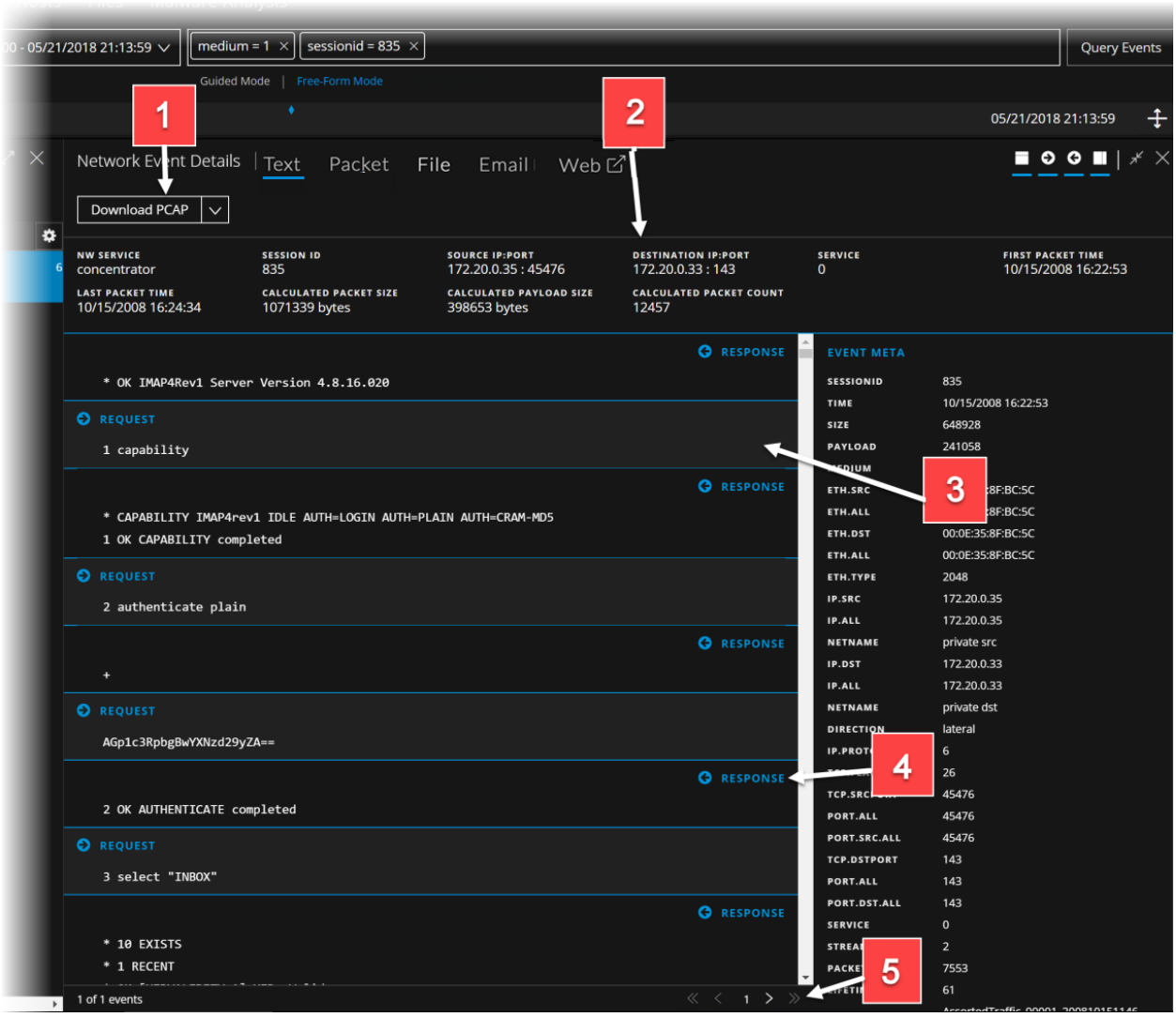
*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー
- [イベント]ビュー - [パケット]パネル
- [イベント]ビュー - [ファイル]パネル
- [イベント]ビュー - [メール]パネル

簡単な説明

[イベント]ビューは、[テキスト]パネルに1つのイベントのテキストを表示します。イベント リスト パネルでイベントをクリックすると、隣接するパネルにテキスト再構築が表示されます。ログ イベントとエンドポイント イベントのRAWログのみが[テキスト]パネルに表示されます。ネットワーク イベントでは、パケットの方向(リクエストまたはレスポンス)と各パケットの内容がテキスト形式で提供されます。テキストのその他の例については、「イベントの再構築と分析」を参照してください。詳細な手順については、「[イベント]ビューでのイベントの分析」を参照してください。



1	ログ、PCAP、ファイルをエクスポートして、より詳細な分析や、他のユーザとの共有を行うためのオプションです。このダウンロード メニューはネットワーク データ用です。
2	イベントのヘッダー情報。
3	ネットワーク イベントのペイロードには、リクエストとレスポンスが含まれています。これは、パケットのリクエスト側です。
4	これは、パケットのレスポンス側です。
5	(バージョン11.2以降)ページ操作コントロールで、イベントのリストのページ操作を柔軟に実行できます。使用できないコントロールのイメージはグレー表示になります。たとえば、ページ1を表示

しているときには、  とのコントロールがグレー表示になります。

 - 最初のページに移動

 - 前のページに移動

 - 次のページに移動

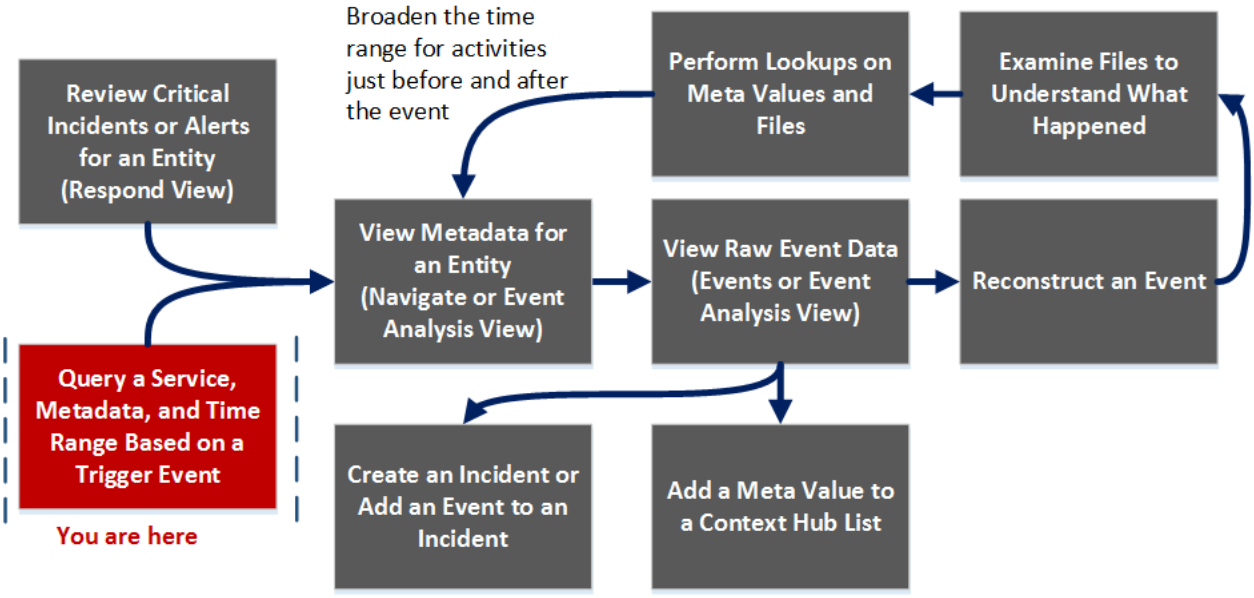
 - 最後のページに移動(最後のページにすでに移動した後でのみ利用可能)

[調査]ダイアログ

[調査]ダイアログでは、アナリストは調査するサービスまたはコレクションを選択できます。このダイアログは、最初に[ナビゲート]ビューまたは[レガシー イベント]ビューに移動したときに、調査するデフォルト サービスを選択していない場合に自動的に表示されます。現在の調査からこのダイアログにアクセスするには、ツールバーで現在のサービス名を選択します。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行*	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み

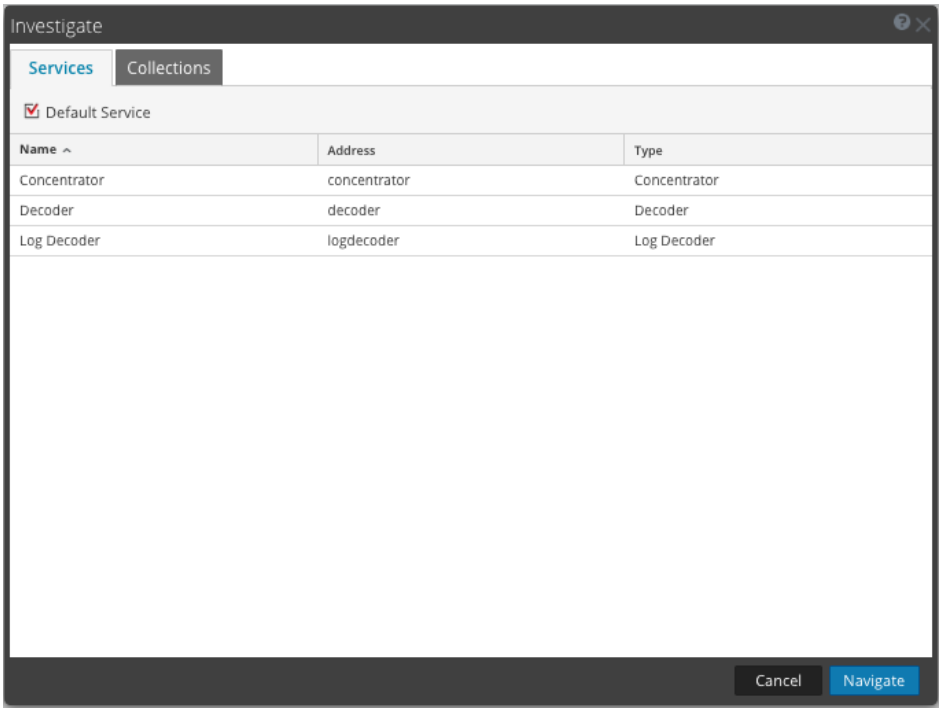
ユーザ ロール	実行したいこと	手順
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加	結果の追加のコンテキストを検索

*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [ナビゲート]ビュー
- [レガシー イベント]ビュー

簡単な説明



[調査]タブには、[サービス]と[収集]の2つのタブがあります。

注： 収集は、Workbenchコレクションと呼ばれることもあります。表示できるのは、自分が作成したWorkbenchコレクションだけです。また、Workbenchコレクションを作成できるのは管理者だけです。

[サービス]タブには、調査で使用可能なサービスのリストと3つのボタンがあります。次の表で、すべての機能について説明します。

機能	説明
デフォルト サービス	このボタンをクリックすると、調査するデフォルト サービスが設定またはクリアされます。サービスがデフォルト サービスとして設定されると、サービス名に「(デフォルト)」という表記が追加されます。
名前	サービスの名前です。
住所	サービスのIPアドレス。
タイプ	サービスのタイプ。
キャンセル	ダイアログを閉じます。
ナビゲート	選択したサービスを[ナビゲート]または[レガシー イベント]ビューで開きます。

[収集]タブには2つのボタンと、[Workbench]と[収集]という2つのパネルがあります。

[Workbench] パネルには、使用可能なWorkbenchサービスの名前がリストされます。Workbenchサービスを選択すると、[収集] パネルから収集を選択できます。

[収集] パネルには、調査する使用可能な収集がリストされます。収集を選択すると、[ナビゲート] をクリックして収集を表示できます。

次の表は、[収集] パネルの機能について説明しています。

機能	説明
名前	収集の名前。
タイプ	収集のタイプ。
サイズ	収集のサイズ。
データ タイプ	収集内のデータのタイプ。
作成日	収集が作成された日付。

[調査]タブ: [ユーザ環境設定]パネル

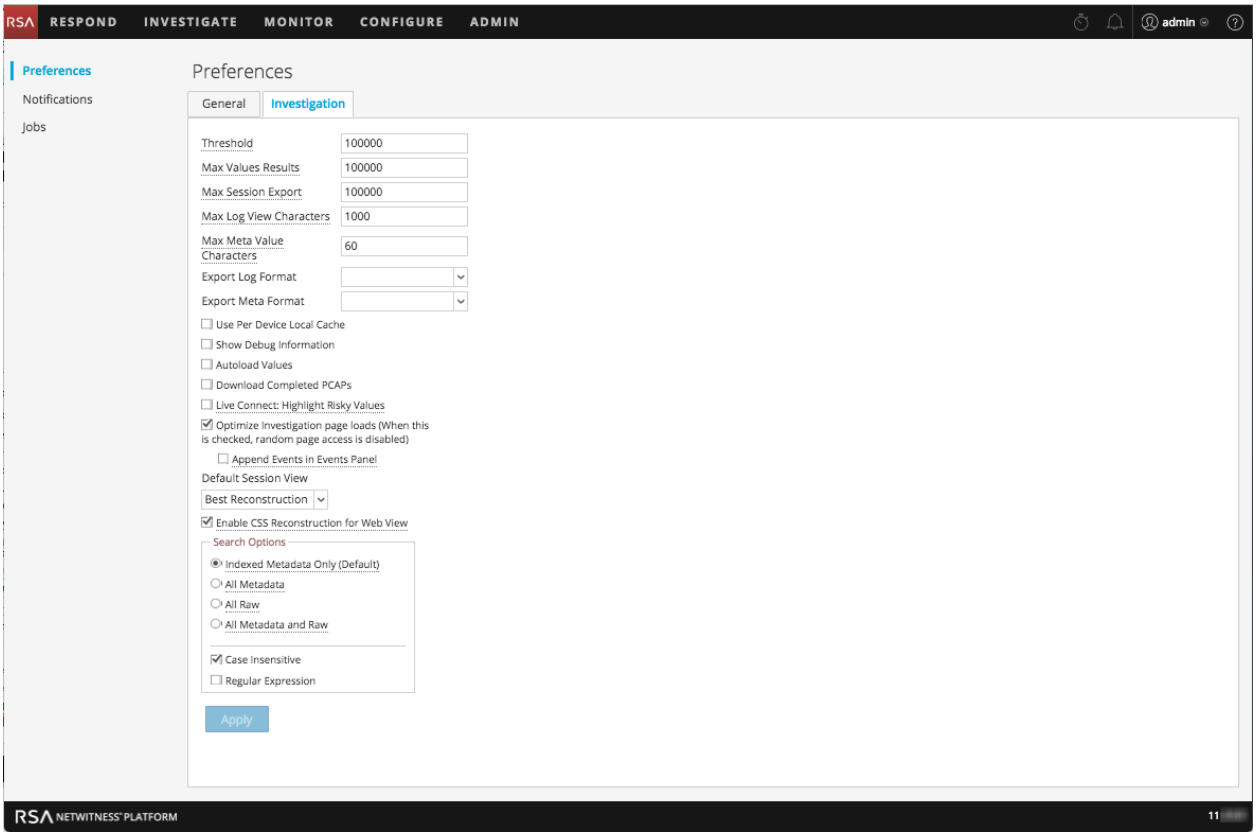
[プロファイル]ビュー> [環境設定]パネル> [調査]タブで、NetWitness Investigateでのデータの分析、イベントの表示、イベントの再構築時のNetWitness Platformのパフォーマンスと動作に影響を与える、いくつかの環境設定を行うことができます。このタブにアクセスするには、[ナビゲート]ビューまたは[レガシー イベント]ビューから> Profileを選択します。[プロファイル]ビューが表示されたら、**[環境設定]>[調査]**を選択します。ユーザ環境設定は、NetWitness Platformで作業しているときにいつでも変更できます。

関連トピック

- NetWitness Investigateの仕組み
- [ナビゲート]ビュー
- [レガシー イベント]ビュー

簡単な説明

この図は、[調査]タブの例です。次の表では、調査に影響する環境設定について説明します。バージョン11.1の検索設定とそれより後のバージョンの検索設定には若干の違いがあり、これについては「[ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索」で説明されています。



機能	説明
閾値	この設定は、[ナビゲート]ビューでのロード中にメタ キー値に表示されるカウントを制御します。閾値を高くすると、計算値が正確になります。ただし、閾値を高くすると、ロードにかかる時間が長くなります。閾値に達すると、NetWitness Platformは、計算値とその計算値に達するまでにかかった時間のパーセンテージ(その値ですべてのセッションをロードするために必要な時間と比較したパーセンテージ) を表示します。 たとえば、**(>100000 - 18%)** と表示された場合、閾値が100000に設定され、閾値が設定されていない場合にロードにかかると想定された時間の18%しかロードの時間がかからなかったことを意味します。デフォルト値は**100000**です。
結果の最大数	この設定は、[ナビゲート]ビューで開いているメタ キーについて、[メタ キー]メニューで[最大まで表示]を選択した場合にロードする値の最大数を制御します。デフォルト値は**1000**です。
最大セッション エクスポート	この設定で、エクスポート可能なセッションの最大数を制御します。デフォルト値は**100000**です。
ログ ビューの最大文字数	この設定は、**[調査]>[レガシー イベント]>[ログ テキスト]**に表示するログ テキストの最大文字数を制御します。デフォルト値は**1000**です。
ログのエクスポート形式	この設定は、調査時にログをエクスポートするためのデフォルトの形式を指定します。使用可能なオプションは、**テキスト**、**XML**、**CSV**、**JSON**です。ログ エクスポート形式のデフォルト値はありません。ここでログの形式を選択しない場合、ログのエクスポートを呼び出すときに、NetWitness Platformで選択のダイアログが表示されます。[ログのエクスポート形式]ドロップダウン メニューから1つのオプションを選択し、[適用]をクリックすると、設定がすぐに反映されます。
メタのエクスポート形式	この設定は、調査時にメタ値をエクスポートするためのデフォルトの形式を指定します。使用可能なオプションは、テキスト、XML、CSV、JSONです。メタ エクスポート形式のデフォルト設定はありません。ここでメタ値のエクスポート形式を選択しない場合、メタ値のエクスポートを呼び出すときに、NetWitness Platformで選択のダイアログが表示されます。[メタのエクスポート形式]ドロップダウン メニューから1つのオプションを選択し、[適用]をクリックすると、設定がすぐに反映されます。
デバイスごとのローカル キャッシュを使用	選択したサービスからローカルにキャッシュされるデータの使用を指定することができます。このチェックボックスはデフォルトでオフになっているため、初回ロード後に[調査]ビューにキャッシュされたデータを表示するのではなく、新しいクエリがデータベースに送信されます。このオプションを選択すると、ローカル キャッシュのデータが使用されます。
デバッグ情報の表示	このオプションが設定されている場合、NetWitness Platformは`where`句を[ナビゲート]ビューの階層リンクの下に表示します。ロードされるメタ値ごとに、ロード時間が表示されます。サービスがBrokerの場合は、各集計サービスでの経過時間が報告されます。デフォルト値は**オフ**です。

機能	説明
イベント パネルの イベント を挿入 モードで 表示	このオプションを設定すると、[**イベント**] **パネル**に表示されるイベントは、現在表示されて いるイベントを上書きするのではなく、段階的に追加されます。次のページ アイコンをクリッ クするたびに、1～25、次が1～50、その次が1～75などのように前のイベントに追加のイベ ントが付加されます。 **注**: このオプションは、[調査ページのロードを最適化する]オプションが有効な場合に のみ使用できます。
値の自 動ロード	このオプションが設定されている場合、[ナビゲート]ビューにサービスから値が自動的に ロードされます。設定されていない場合、NetWitness Platformには[**値のロード**]ボタンが 表示され、値をロードする前に表示オプションを変更できるようになります。デフォルト値は **オフ**です。
完了した PCAPの ダウン ロード	この設定は、抽出されたPCAPのダウンロードを自動化します。これにより、PCAPファイル をダウンロードしてPCAP形式のデータを扱えるアプリケーション(Wiresharkなど) で開くまで の操作を手動で実行する必要がなくなります。
Live Connect: リスクの ある値を 強調表示	NetWitness PlatformでRSAコミュニティによりリスクが高いと見なされるIPアドレスのみを強 調表示する場合は、このオプションを設定します。有効にしない場合、NetWitness Platformではすべてのアドレスが表示されます。デフォルトでは、このオプションはオフに なっています。
調査 ページの ロードを 最適化 する	[レガシー イベント]ビューでイベントを取得する方法を制御します。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。有効にした場合、イベント リストには可能な 限り高速に結果が返されますが、イベント リストのページ移動機能が無効になります。こ のチェックボックスをオフにすると、イベント リストのページ移動機能が有効になり、リストの 特定のページ(または最後のページ) に移動できるようになります。リスト内の任意のペー ジに移動できるようにすると、イベントを事前に判断するための追加のオーバーヘッドが生 じます。
デフォル ト セッ ション表 示	この設定では、セッションの再構築を表示する時のデフォルトの再構築のタイプを選択し ます。デフォルトでは、そのイベントに最適な再構築タイプでイベントが再構築されます。
Web ビューの CSS再 構築を 有効化	この設定では、Webコンテンツの再構築の実行方法が制御されます。有効化すると、 Webの再構築にカスケード スタイル シート(CSS) とイメージが含まれるようになり、再構築 の表示と元のWebブラウザの表示が一致するようになります。これには、イベントに関連す るスキャニングと再構築、ターゲット イベントで使用されるスタイル シートとイメージの検索 が含まれます。このオプションは、デフォルトで有効化されています。特定のWebサイトの 表示で問題がある場合は、このチェックボックスをオフにします。 **注**: 関連するイメージとスタイル シートが見つからないかWebブラウザのキャッシュにロー ドされていない場合は、再構築されたコンテンツの外観が元のWebページと一致しない 場合があります。また、クライアント側のすべてのjavascriptがセキュリティ目的で削除さ れるため、クライアント側のjavascriptを経由して動的に実行されるレイアウトまたはスタ イルは、再構築では表示されません。

機能	説明
検索オプション	この設定によりデフォルト検索オプションが指定されて、[ナビゲート]ビューおよび[レガシー イベント]ビューでの検索に適用されます。詳細については、「[ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索」を参照してください。
適用	環境設定を保存すると、即座に反映されます。

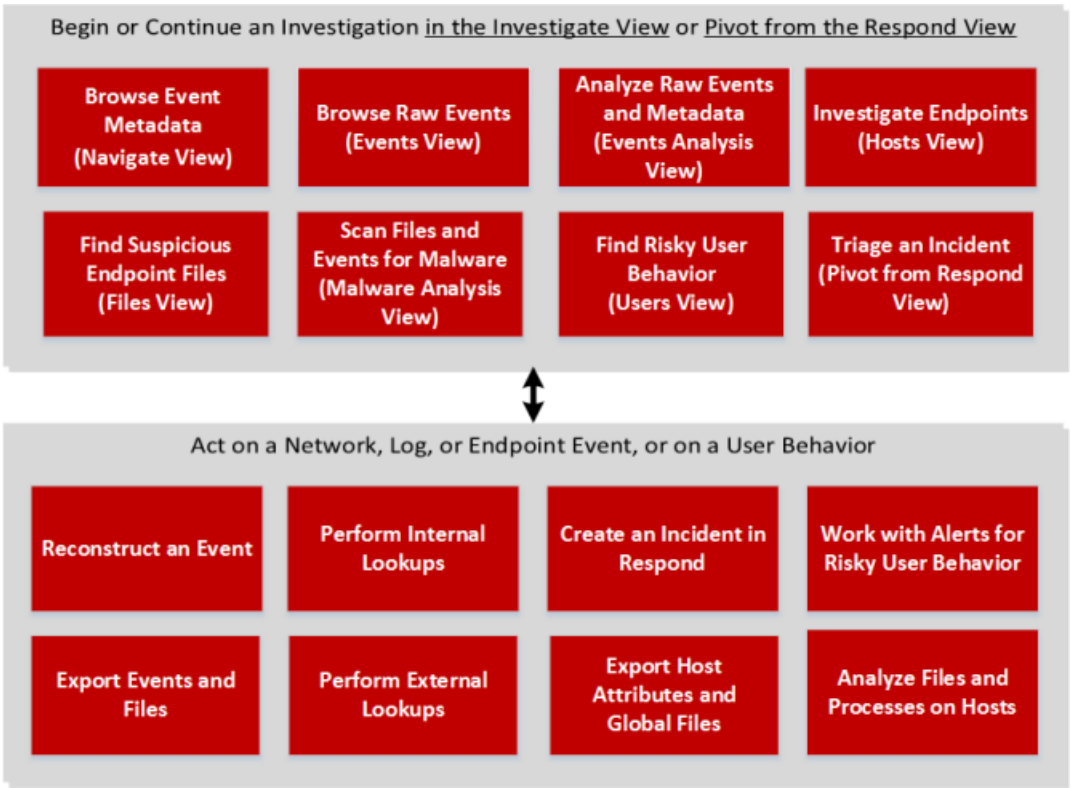
[調査]ビュー

[調査]ビューは、NetWitness Investigateへのプライマリ エントリー ポイントです。[調査]ビューには6つのサブメニューがあり、それぞれ異なる視点からイベントを分析できるビューを開きます。サブメニューには、[ナビゲート]、[レガシー イベント]、[イベント](以前の[イベント分析])、[ホスト]、[ファイル]、[エンティティ](以前の[ユーザ])、[マルウェア分析]があります。

注: [レガシー イベント]ビューは、過去のバージョン(11.0～11.3.x.x)では、[イベント]ビューと呼ばれていました。バージョン11.4以降では、[レガシー イベント]は不要になり、管理者が有効にしない限り、非表示になります。デフォルトでは、[イベント]ビューのみがメニューに表示されますが、[レガシー イベント]ビューが有効になっている場合は、[イベント]ビューと[レガシー イベント]ビューの両方がメニュー バーに表示されます。

ワークフロー

次の図は、[調査]ビューで実行できるタスクの概要を示しています。このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



サブメニュー オプションを使用して、ビュー間を移動できます。

- [ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビューには相互リンクがあるので、現在の結果をさまざまな視点から確認できます。これにより、ビューを切り替えるときの調査の継続性が保

たれます。

- [ホスト]ビューと[ファイル]ビューでは、NetWitness Endpointが調査に組み込まれています。それぞれ、NetWitness Endpointエージェントがインストールされているすべてのホストと、導入環境で検出された固有の実行可能ファイルが表示されます。
- [エンティティ]ビュー(以前の[ユーザ]ビュー) では、NetWitness UEBAを使用して、エンタープライズ全体で高リスク ユーザの行動を可視化できます。環境内の高リスク ユーザのリストと、高リスク行動を示す上位アラートのサマリーが表示されます。ユーザまたはアラートを選択すれば、高リスク行動の詳細と、発生のタイムラインを表示できます。
- [マルウェア分析]ビューでは、他のいずれかのビューで検出されたファイル、またはネットワークトラフィックの継続的スキャンにより収集されたファイルをスキャンできます。

目的のイベントまたはファイルを見つけたら、より詳細な調査を続行するためのさまざまなアクションを実行できます。たとえば、イベントの再構築と分析、イベントとファイルのエクスポート、内部および外部リソースでのルックアップの実行、インシデントとアラートの作成を行うことができます。

実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
脅威ハンター	イベント メタデータを参照する	[ナビゲート]ビューまたは[レガシー イベント]ビューでの調査の開始
脅威ハンター	RAWイベントを参照する	[イベント]ビューでの調査の開始 [ナビゲート]ビューまたは[レガシー イベント]ビューでの調査の開始
脅威ハンター	RAWイベントとメタデータを分析する	[イベント]ビューでの調査の開始
脅威ハンター	エンドポイントを調査する(バージョン11.1以降)	*NetWitness Endpointユーザ ガイド*
脅威ハンター	不審なエンドポイント ファイルを探す(バージョン11.1以降)	*NetWitness Endpointユーザ ガイド*
脅威ハンター	高リスクなユーザ行動を検索する	*NetWitness UEBAユーザ ガイド*
脅威ハンター	ファイルとイベントをスキャンしてマルウェアを探す	*Malware Analysisユーザ ガイド*

関連トピック

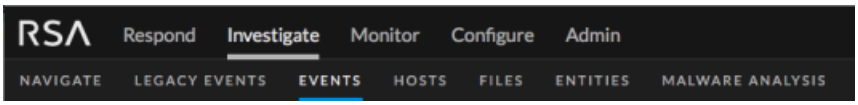
- NetWitness Investigateの仕組み
- 調査の開始

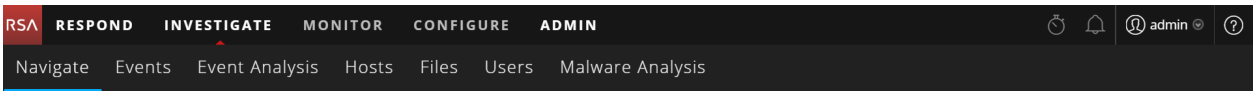
- NetWitnessの[調査]ビューおよび環境設定の構成
- [ナビゲート]ビュー
- [レガシー イベント]ビュー
- [イベント]ビュー
- *NetWitness Investigateクイック スタート ガイド*
- *NetWitness Endpointクイック スタート ガイド*
- *NetWitness UEBAクイック スタート ガイド*
- *Malware Analysisユーザ ガイド*

簡単な説明

[調査]ビューを構成する6つのビューは、それぞれ異なるデータ分析方法を表しています。デフォルトでは、[調査]では[ナビゲート]ビューが開きます。デフォルト ビューは、他のいずれかのビューに変更できます(「NetWitnessの[調査]ビューおよび環境設定の構成」を参照)。各ビューの使用法については、「NetWitness Investigateの仕組み」を参照してください。次の図は、バージョン11.4の[調査]ビューのサブメニューを示しています。2番目の図は、以前のバージョンのメニューを示しています。

注: [ホスト]および[ファイル]サブメニューはバージョン11.1以降で使用できます。[エンティティ](以前の[ユーザ])メニューはバージョン11.2以降で使用できます。表示されるサブメニューは、ユーザのロールと権限によって決まります。





[レガシー イベントの再構築]ビュー

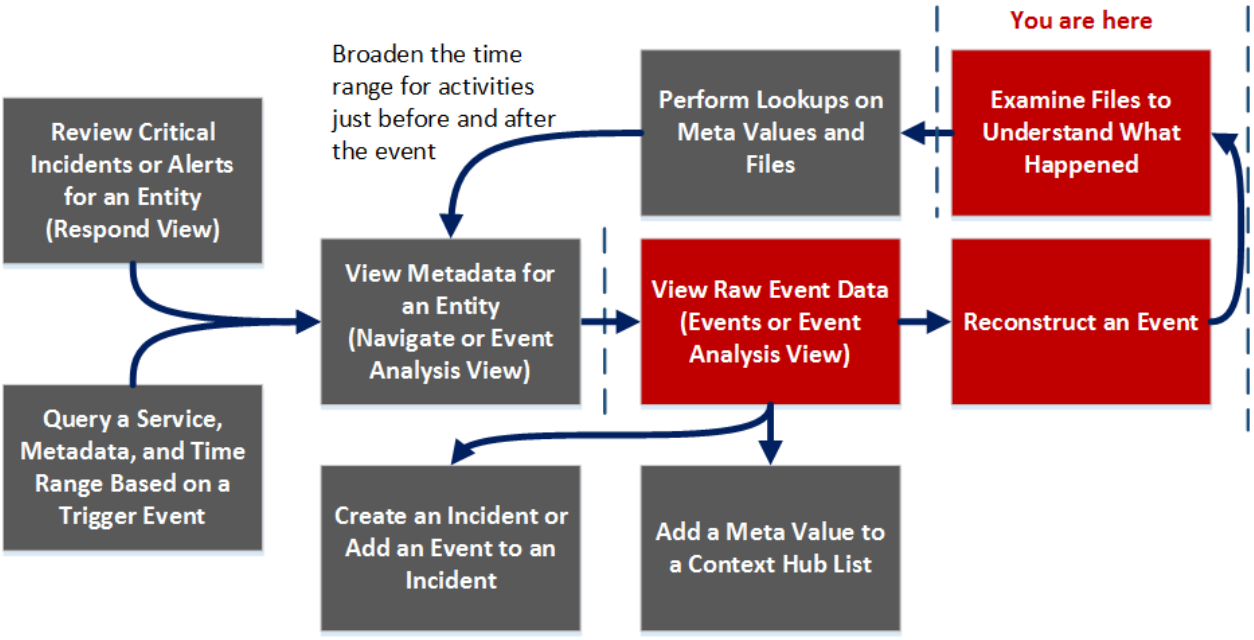
[イベントの再構築]ビューでは、[レガシー イベント]ビューから選択したイベントの再構築を提供します。デフォルトでは、NetWitness Platformはイベントのコンテンツから判断されたイベントに最適な再構築形式か、Investigateの[デフォルト セッション表示]の設定で選択したデフォルトの再構築形式を表示します。[イベントの再構築]ツールバーのオプションを使用して、再構築方法の変更、複数の結果の上下または並行表示、リクエストとレスポンス ビューの選択、イベントのエクスポート、メタ値のエクスポート、ファイルの展開、メールの添付ファイルの表示、新しいタブでのイベントの表示を行うことができます。

このビューにアクセスするには、次のいずれかを実行します。

- 任意の[レガシー イベント]ビューで、イベントをダブルクリックします。
- 詳細ビューを選択した[レガシー イベント]ビューで、イベントの最後の[**イベント**]を右クリックし、[**イベントの再構築**]を選択します。
- プレビューした再構築の[イベント再構築]ツールバーで、[**イベントを新しいタブで開く**]をクリックします。
- [ナビゲート]ビューで、**[アクション]＞[イベント再構築に移動]**を選択し、イベントIDを入力します。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respondユーザ ガイド*』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示*	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築*	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証*	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加	結果の追加のコンテキストを検索

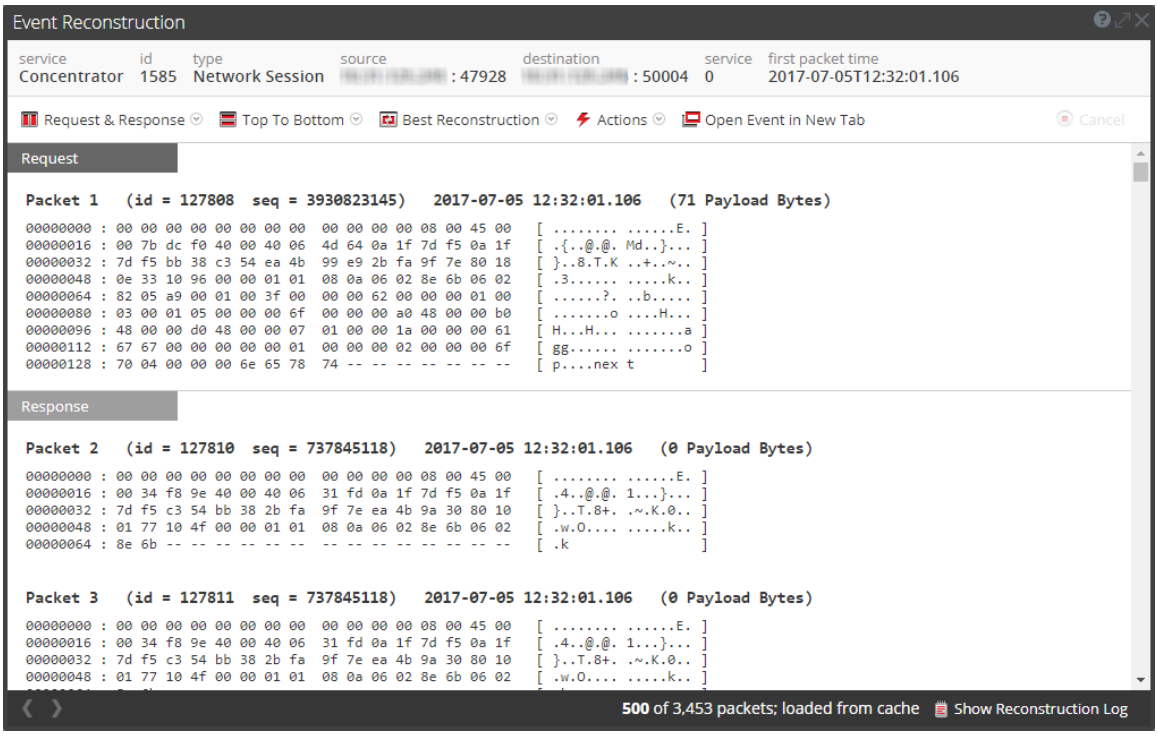
*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー

簡単な説明

次の図は、[イベントの再構築]ビューの例です。次の表に、ツールバーのオプションを示します。



機能	説明
リクエストとレスポンス	ビューで次の項目を表示するかどうかを選択するためのドロップダウン メニューを表示します。 • リクエストとレスポンス • リクエスト • レスポンス
構成	情報を上下に並べて表示するか、左右に並べて表示するかを選択するためのドロップダウン メニューを表示します。

機能	説明
[再構築]ビュー	表示する情報を選択するためのドロップダウン メニューを表示します。デフォルトでは[最適な表示]が選択されています。その他のオプションは次のとおりです。 • メタの表示 • テキストの表示 • 16進数の表示 • パケットの表示 • Webの表示 • メールの表示 • ファイルの表示
アクション	[イベントの再構築]ビューで利用できるアクションが、ドロップダウン メニューに表示されます(PCAPのエクスポート、ファイルの抽出、メタのエクスポート) 。
イベントを新しいタブで開く	新しいブラウザ タブでイベントを開きます。
イベント分析	[イベント分析]ビューでイベントを開きます。

ツールバーの下にはメタ キーと値の一覧が表示されます。いくつかのキーでは、利用できるアクションがドロップダウン メニューに表示されます。

ビューの下部に表示されるバーには、いくつかのオプションが表示されます。

機能	説明
❮	前のイベントが表示されます。
❯	次のイベントが表示されます。
再構築ログの表示	ビューの下部に再構築ログが表示されます。このボタンをクリックすると、[再構築ログの非表示]に変わります。

[レガシー イベント]ビュー

[レガシー イベント]ビューでは、セッションに関連づけられているイベントのリストを表示できます。このビューは、RAWイベントを時系列で表示するために最適化されています。イベントのリストは複数の形式で表示できます。イベントのフィルタ、イベントの検索、イベントの再構築の表示も可能です。

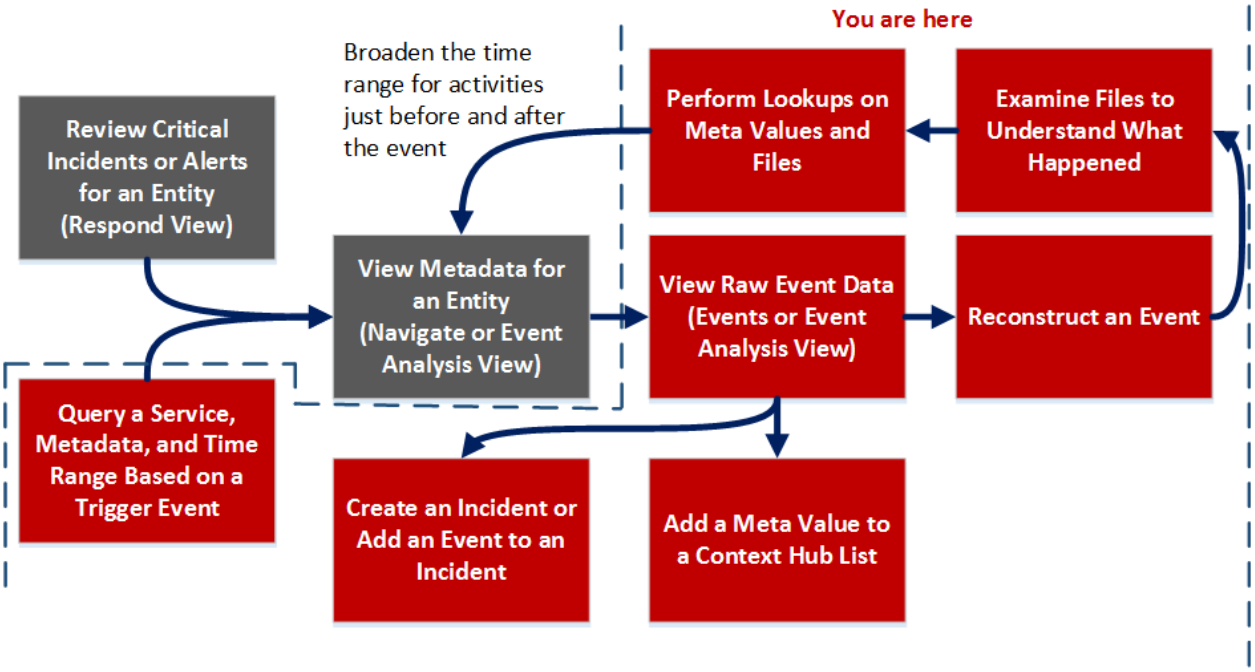
[レガシー イベント]ビューを表示するには、次の2つの方法があります。

- **[調査]>[レガシー イベント]**に移動します。NetWitness Platformは、デフォルトのサービス(設定されている場合)の直近3時間についてデフォルト クエリを実行するか、またはサービスを選択するダイアログを表示してからデフォルト クエリを実行します。デフォルト クエリではすべてのイベントが選択され、選択したサービスのイベントが古い順に[レガシー イベント]ビューに表示されます。
- [**ナビゲート**]ビュー内でイベントをダブル クリックします。[レガシー イベント]ビューには、[ナビゲート]ビューのドリルダウン ポイントに基づいて、選択したサービスのイベントが表示されます。

注: [レガシー イベント]ビューは、過去のバージョン(11.0～11.3.x.x)では、[イベント]ビューと呼ばれていました。[レガシー イベント]は不要になり、管理者が有効にしない限り、非表示になります。デフォルトでは、[イベント]ビューのみがメニューに表示されますが、[レガシー イベント]ビューが有効になっている場合は、[イベント]ビューと[レガシー イベント]ビューの両方がメニュー バーに表示されます。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行*	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示*	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築*	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証*	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行*	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加*	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加*	結果の追加のコンテキストを検索

*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [レガシー イベント]ビューでの結果のフィルタリング
- 結果のダウンロードと処理

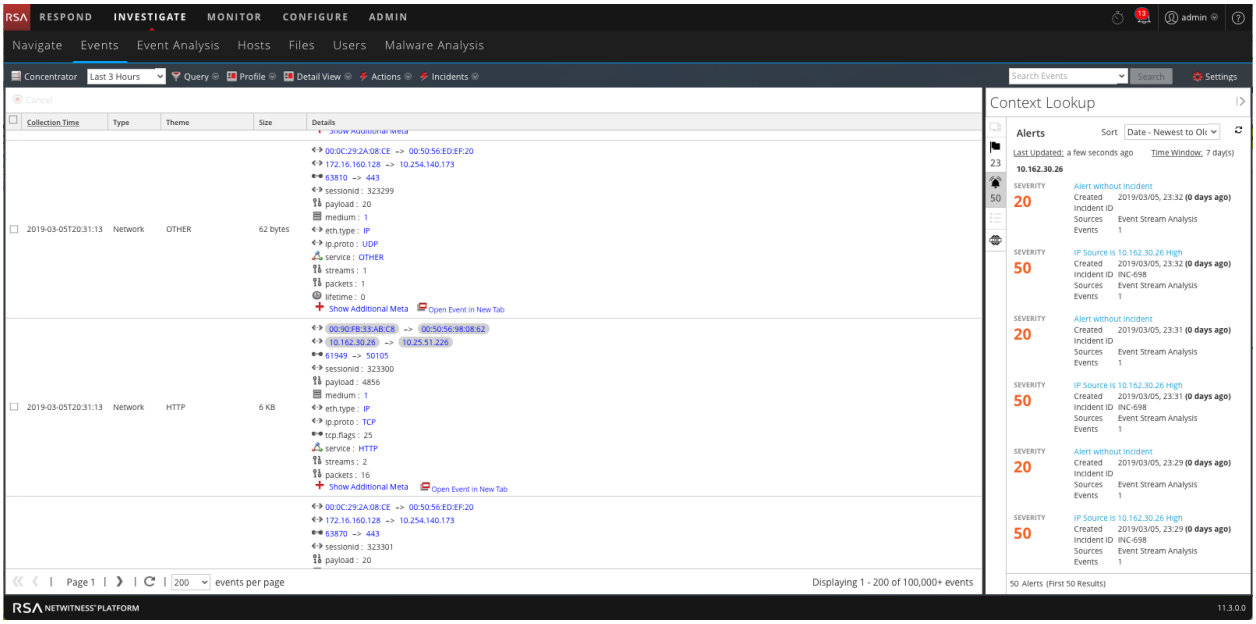
簡単な説明

[レガシー イベント]ビューには、詳細ビュー、リスト ビュー、ログ ビューという、標準提供の3種類の表示形式でイベント データを表示できます。リスト ビューおよび詳細ビューでは、タイムスタンプ、イベント タイプ、イベント テーマ、サイズなど、各イベントの詳細な情報が確認できます。

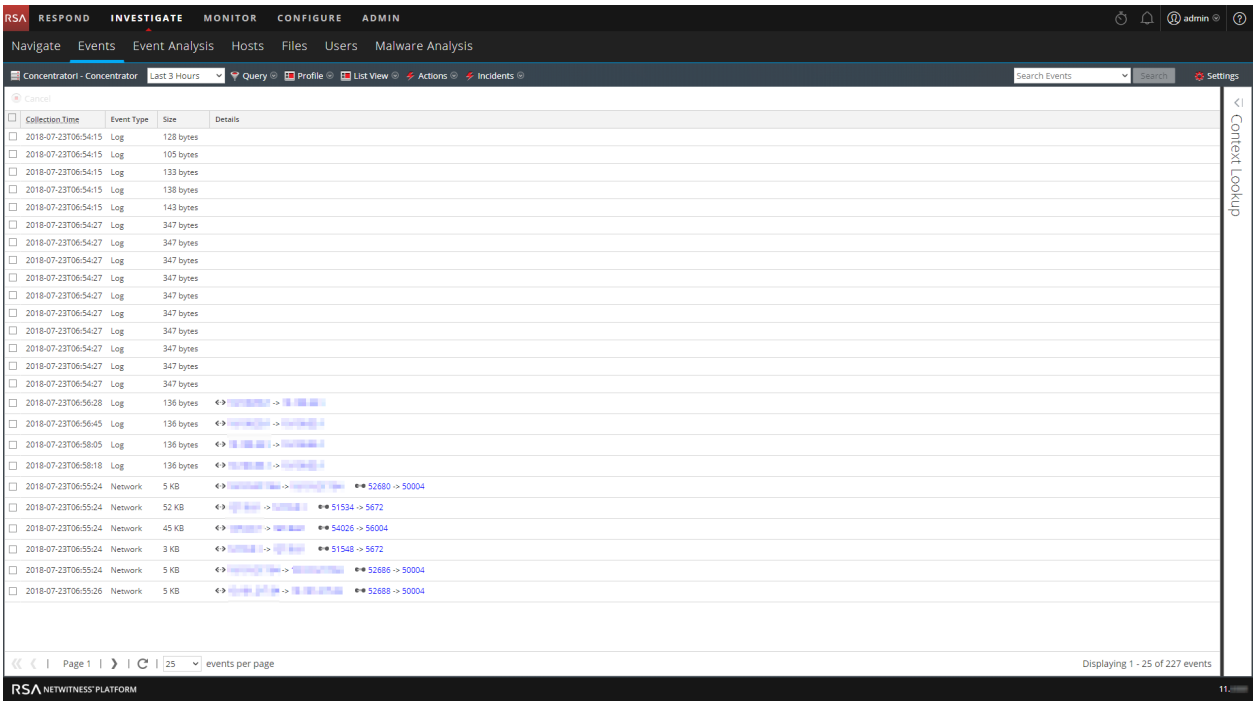
- リスト ビューでは、イベントのソース アドレスおよび宛先 アドレスとポート番号がグリッドに表示されます。
- 詳細ビューでは、イベントについて収集された主なメタデータがページ ビュー形式で表示されます。
- ログ ビューは、ログおよびエンドポイント情報の表示のために最適化されたビューであり、タイムスタンプ、イベント タイプ、サービス タイプ、サービス クラス、ログなど、各ログの詳細情報が確認できます。

[レガシー イベント]ビューの表示をフィルタするには、クエリ、時間範囲設定、プロファイルを使用します。[レガシー イベント]ビューのいずれの表示形式からも、ファイルの抽出、イベント、エンドポイント イベント、ログ、メタ値のエクスポート、[イベントの再構築]パネルの表示を行うことができます。[詳細]ビューでは、[イベント]ビューでイベントを開くこともできます。

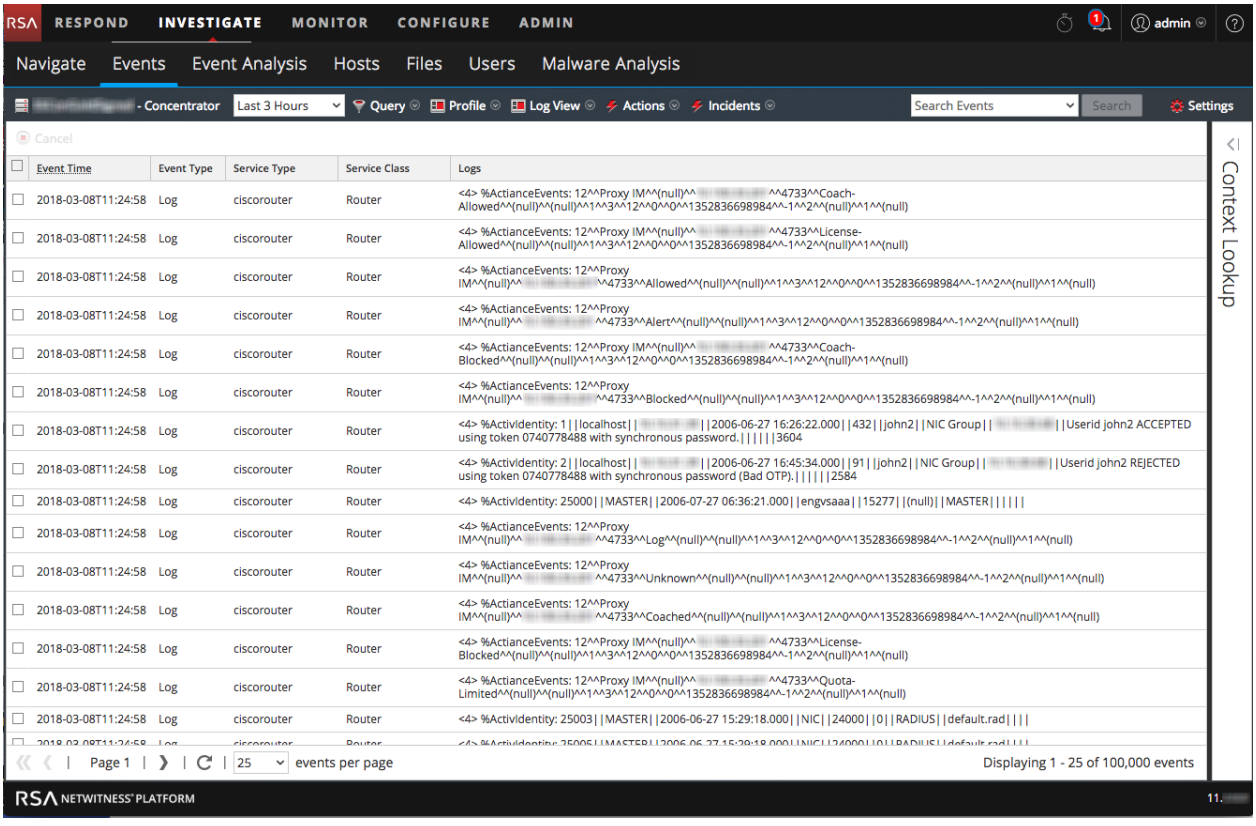
次の図は、詳細ビューのイベントの例です。[コンテキスト ルックアップ]パネルはContext Hubサービスが構成されている場合にのみ表示されます。



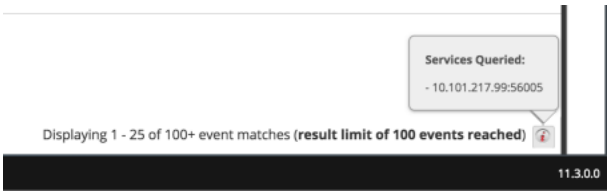
次の図は、リスト ビューのイベントの例です。



次の図は、ログ ビューの例です。



次の図は、バージョン11.3以降のフッターに追加された情報を示しています。



詳細説明

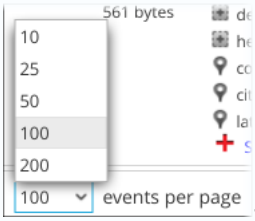
[レガシー イベント]ビューには、上部に以下のオプションを備えたツールバーがあります。

機能	説明
サービスを選択	アイコンの横に選択したサービス名が表示されます。[調査]ダイアログを開きます。このダイアログでは、イベント リストを表示するサービスを選択できます。
時間範囲	イベント リストに適用する時間範囲を選択するためのドロップダウン メニューが表示されます。標準的なオプションのなかから1つを選択するか、カスタム時間範囲を指定できます。
クエリ	[クエリ]ダイアログが表示されます。ここでは、データをドリルダウンするのではなくクエリレガシー イベント]ビュー クエリを直接入力できます(「[ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成」を参照してください)。
プロファイル	[プロファイル]メニューを表示します。現在選択されているプロファイルがツールバーに表示されます。メニュー オプションには、標準提供(デフォルト)プロファイルとカスタム プロファイル、およびプロファイルを管理するためのオプションが含まれます。各プロファイルには、メタ グループ、列グループ、イベントの調査時に[ナビゲート]ビュー(メタ グループとクエリ)と[レガシー イベント]ビュー(列グループとクエリ)に適用される開始クエリを含めることができます(「クエリ プロファイルを使用した調査の共通領域のカプセル化」を参照してください)。
ビューの選択のドロップダウン	イベント ビューのタイプを選択するためのドロップダウン メニューを表示します。 • 詳細ビューでは、各イベントの詳細情報がページ形式で表示されます。 • リスト ビューでは、各イベントのサマリーが1行ずつテーブル形式で表示されます。 • ログ ビューでは、各ログのサマリが1行ずつログ専用のイベント グリッドに表示されます。 • カスタム列グループでは、ドロップダウン リストから選択した列グループを使用してイベント リストを表示します。 • 列グループの管理では、カスタム列グループの作成および編集のためのダイアログが表示されます。

機能	説明
アクション	[レガシー イベント]ビューのアクションが、ドロップダウン メニューに表示されます。 • PCAPファイルとしてのイベントのエクスポート、ログのエクスポート、エンドポイント イベントのエクスポート、メタ値のエクスポートを行います。 • ポップアップ ウィンドウまたは新しいタブにイベントの再構築を表示します。 • [レガシー イベント]ビューのフィルタをすべてリセットします。
インシデント	Respondで新しいインシデントを作成して選択したイベントを追加するか、Respondの既存のインシデントに選択したイベントを追加します。
検索	[イベントの検索]オプションを表示します。これにより、エクスポートログを指定し、「[ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索」で説明されている追加のオプションを使用してメタ値形式をエクスポートすることができます。
設定	[レガシー イベント]ビューに関する調査オプションを設定します([プロファイル]ビューでも設定可能です)。これにより、[レガシー イベント]ビューから移動せずに調査の設定を変更できます。[レガシー イベント]ビューで変更した設定は、[プロファイル]ビューでも変更されます(「[ナビゲート]ビューおよび[レガシー イベント]ビューの構成」を参照してください)。

この表では、[レガシー イベント]ビューのその他の機能について説明します。

機能	説明
Show Additional Meta (イベントの詳細ビュー)	イベントの残りのメタデータを表示します。
Event Analysis (イベントの詳細ビュー)	選択したイベントを[イベント]ビューで開きます。

機能	説明
 (フッター)	ページ移動コントロールを使用すると、イベント リストのページをより柔軟に操作できます。使用できないコントロールのイメージはグレー表示になります。たとえば、ページ1を表示しているときには、《と〈のコントロールがグレー表示になります。 《- 最初のページに移動 〈- 前のページに移動 | 3 Page 3 |- 特定のページに移動 〉- 次のページに移動 》- 最後のページに移動  - 1ページあたりのパケット数を選択 1ページあたりのイベント数を選択すると、設定はブラウザのキャッシュに保存されるため、優先的に使用するイベント数をログインのたびに選択する必要がありません。この設定は、ログ ビュー、リスト ビュー、詳細ビューのすべてのビューに適用されます。
100,000個のイベントのうち 1～100個を表示(フッター) 100個以上の一致したイベントのうち1～25個を表示(結果制限の100イベントに到達) (フッター)	表示されているイベントの数と、一致したイベントの合計数を表示します。バージョン11.3以降では、管理者によって設定された結果の制限に達した場合、他にも利用可能な結果があるが表示できないことを知らせる通知がフッターに表示されます。追加の結果を表示するには、フィルタを絞り込んで結果を減らす必要があります。フッターの情報アイコン をクリックすると、クエリ対象のすべてのサービスのIPアドレスと接続ポート番号が表示されます。

[デフォルト のメタ キーの管 理]ダイアログ

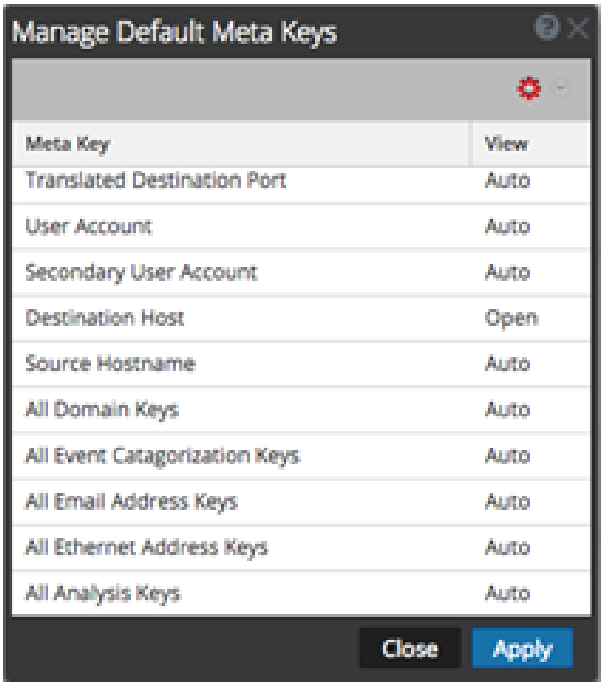
[デフォルト のメタ キーの管 理]ダイアログでは、アナリストは[ナビゲート]ビューの[値]パネルに表 示するメタ キーを指 定できます(「調 査でのデフォルト メタ キーの管 理と適 用」を参 照)。これにより必 要なデータをさらに迅 速に見 つけることができ、関 係のないメタ キーはロードされません。このダイアログにアクセスするには、[**ナビゲート**]ビューのツールバーで、[**メタ**]>[**デフォルト のメタ キーの管 理**]を選 択します。

関 連トピック

- NetWitness Investigateの仕 組み
- メタ グループを使 用して関 連性の高いメタ キーにフォーカス

簡 単な説 明

次の図は、[デフォルト のメタ キーの管 理]ダイアログを示します。これには、メタ キーのリスト、ツールバー、[閉じる]ボタン、[適 用]ボタンがあります。リストでは、デフォルト のメタ キーを表 示、ソート、管 理できます。メタ キーをクリックしてドラッグすると、並 べ替 えることができます。次の表は、リスト の列を説 明したものです。



列	説 明

列	説明
メタ キー	この列には、サービスで使用できるメタ キーが表示されます。バージョン11.1以降では、デフォルトのメタ エンティティも含まれます。たとえば、[All Domain Keys]や[All Email Address Keys]などです。
表示	この列には、各メタ キーに割り当てられているビューのタイプが表示されます。各行でビューをクリックすると、メタ キーを別のデフォルト ビューに割り当てることができます。4つの表示タイプがあります。 • [自動]: サービス インデックス ファイルで指定されている、メタ キーのデフォルトのビューに復元します。 • [折りたたみ表示]: このメタ キーの値はデフォルトで折りたたみ表示され、手動で展開することができます。 • [非表示]: これらのメタ キーはデフォルトで非表示になり、調査では一切表示されません。 • [展開表示]: このメタ キーの値はデフォルトで表示されます。インデックスなしのメタ キーのデフォルト メタ キーを変更する場合、キーを[**展開表示**]に設定できません。メタ グループのデフォルト ビューを[**展開表示**]に変更し、一部のメタ キーがインデックスなしであった場合、インデックスなしのメタ キーは自動的に[**自動**]に戻ります。したがって、メタ キーはインデックス付きである場合にのみ自動的にロードされます。インデックスなしのメタ キーは手動で開くまで**折りたたみ表示**になります。

次の表に、ツールバー オプションとボタンの説明を示します。

機能	説明
	すべてのメタ キーのデフォルト ビューの変更に使用できるドロップダウン メニューが表示されます。4つの表示タイプがあります。 • [自動]: サービス インデックス ファイルで指定されている、メタ キーのデフォルトのビューに復元します。 • [折りたたみ表示]: このメタ キーの値はデフォルトで折りたたまれています。 • [非表示]: このメタ キーの値はデフォルトで非表示になっています。 • [展開表示]: このメタ キーの値はデフォルトで表示されます。
閉じる	ダイアログを閉じます。保存していない変更はすべて失われます。
適用	変更を適用します。適用した変更はただちに有効になります。

[メタ グループの管 理]ダイアログ

[調 査]>[ナビゲート]ビューでは、調 査 のために表 示 するデータをフィルタ処 理 するため、メタ グループを使 用 できます。NetWitness Platformの新 規 インストールには、調 査 の対 象 のデータ セットを見 つけるために役 立 つ、OOTB(すぐに利 用 可 能 な) メタ グループが含 まれています。OOTBメタ グループは、識 別 のためにRSAのプレフィックスが付 いており、複 製 できますが、編 集 または削 除 することはできません。独 自 のグループを作 成 することや、OOTBグループを複 製 して編 集 し、カスタム グループを作 成 することができます。調 査 中 にメタ グループが有 効 になっている場 合 、[値]パネルの情 報 には、選 択 されたグループのメタ キーのみが表 示 されます。[メタ グループの管 理]ダイアログでは、メタ グループの追 加 、削 除 、インポート、エクスポートを行うことができます(「調 査 でのデフォルト メタ キーの管 理 と適 用」を参 照) 。

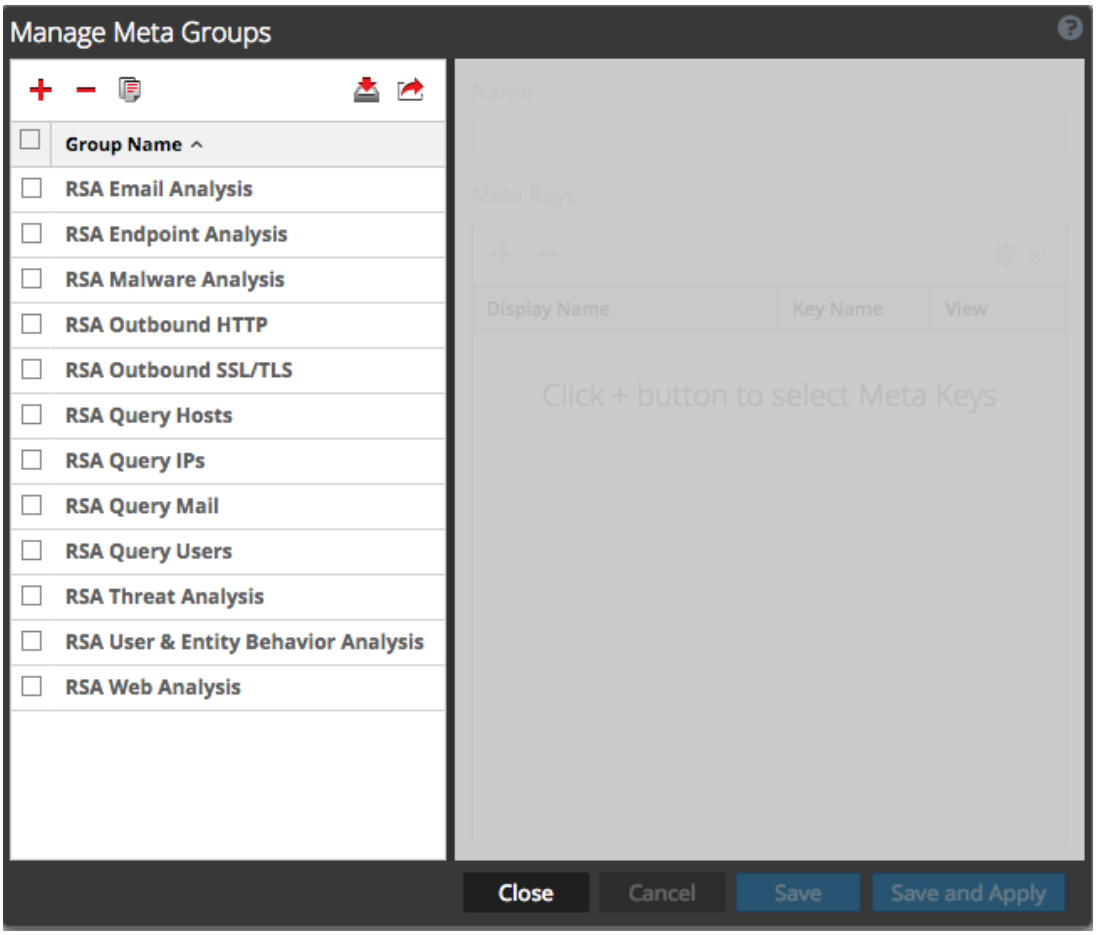
このダイアログにアクセスするには、**[調 査]>[ナビゲート]ビュー**ツールバーで、**[メタ]>[メタ グループの管 理]**を選 択 します。

関 連トピック

- [ナビゲート]ビューでの結 果 のフィルタリング
- NetWitness Investigateの仕 組 み

簡 単な説 明

次 の図 は、[メタ グループの管 理]ダイアログの例 です。



[メタ グループ] パネルは[メタ グループの管 理]ダイアログの左 側にあります。このパネルではメタ グループの追 加、削 除、インポート、エクスポートを行うことができます。次 の表 は、[メタ グループ] パネルの機能を説 明しています。

機 能	説 明
+	[メタ グループの管 理]ダイアログの右 側にある[設 定]パネルを使ってメタ グループを追 加します。
−	選 択されたメタ グループを削 除します。メタ グループが削 除される前 に、確 認ダイアログが表 示されます。
	選 択されたメタ グループのコピーを作 成します。
	[メタ グループのインポート]ダイアログを表 示します。このダイアログではファイルのアップロードを行うことができます。
	選 択したメタ グループをコンピューターにエクスポートします。
グループ名	すべてのメタ グループの名 前を一 覧 表 示します。

[設定]パネルは[メタ グループの管理]ダイアログの右側にあります。このパネルではメタ グループの作成と編集を行うことができます。[名前]フィールドの下にメタ キーのリストがあります。次の表で、[設定]パネルの各機能について説明します。

機能	説明
名前	選択したメタ グループの名前を表示します。
	[利用可能なメタ キー]ダイアログを表示します。このダイアログではグループに追加するメタ キーを選択することができます。
	選択されたメタ キーを削除します。
	ドロップダウン メニューを表示します。このドロップダウン メニューを使うと、すべてのメタ キーのビューを選択することができます。4つのオプションがあり、defaultActionプロパティの値に対応しています。defaultAction プロパティは、サービスのカスタム インデックス ファイルのキーを定義するために使用します。 • [非表示]:これらのメタ キーはデフォルトで非表示になり、調査では一切表示されません。 • [展開表示]:このメタ キーの値はデフォルトで表示されます。 • [折りたたみ表示]:このメタ キーの値はデフォルトで折りたたみ表示され、手動で展開することができます。 • [自動]:サービス インデックス ファイルで指定されている、メタ キーのデフォルトのビューに復元します。
表示名	[調査]ビューでキーに表示される名前を示します。サービスのカスタム インデックス ファイルで、キーの説明プロパティにより定義されます。
キーの名前	サービスのカスタム インデックス ファイルで定義される、メタ キーの名前を示します。
表示	メタ キーが設定されるビューを示します。次の変更が可能です。 • [ビュー]列ヘッダーで  をクリックして、ドロップダウン メニューからビューを選択することによって、すべてのメタ キーのビューを変更できます。 • [ビュー]列で単一のメタ キーをクリックし、  をクリックして、ドロップダウン メニューからビューを選択することによって、単一のメタ キーのビューを変更できます。

次の表は、ダイアログの下部にあるボタンについて説明しています。

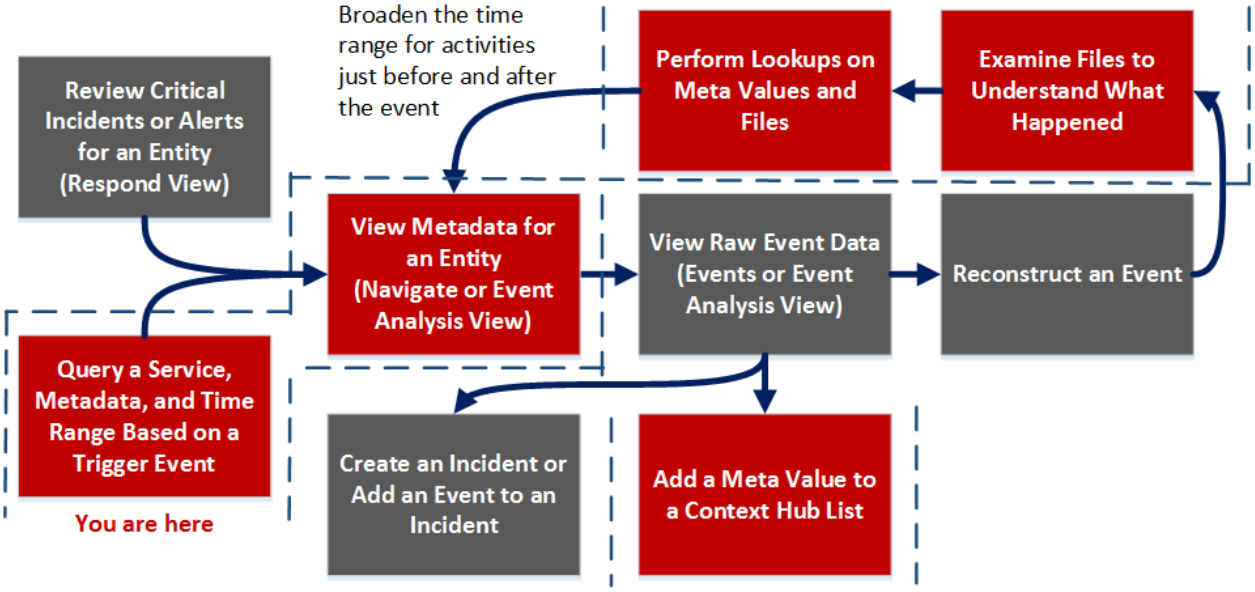
機能	説明
閉じる	ダイアログを閉じます。
キャンセル	すべての変更をキャンセルします。
保存	すべての変更を保存します。
保存して適用	すべての変更を保存して、直ちに適用します。

[ナビゲート]ビュー

[ナビゲート]ビュー([**調査**] > [ナビゲート]) には、選択したサービスの収集データで検出されたイベント メタデータ(メタ キーとメタ値) が表示されます。データは、プロファイル、時間範囲、メタ グループ、クエリで設定したオプションに基づいて、フィルタおよび表示されます。メタ キーとメタ値をクリックして、データをドリルダウンすることもできます。[ナビゲート]ビューは、NetWitness Investigateへのデフォルトのエントリー ポイントです。プロファイルの環境設定でデフォルトのエントリー ポイントを他のビューに変更することができます。

ワークフロー

次の図は、イベント メタデータを調査するための概要レベルのワークフローを示しています。このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



[ナビゲート]ビューでは、次のタスクを実行できます。

- [値]パネルでイベントのメタデータを表示する。
- タイムラインまたは座標表示チャートでイベントを可視化する。
- イベントの保存、イベントIDを使用したイベントへの移動、イベントの可視化、イベントの印刷を行う。
- メタ キーと値の追加のコンテキスト データを表示する。
- [レガシー イベント]または[イベント]ビューでドリルダウン ポイントまたはイベントを開く。

実行したいことは何ですか？

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行*	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	メタデータの表示*	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証*	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行*	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加*	結果の追加のコンテキストを検索

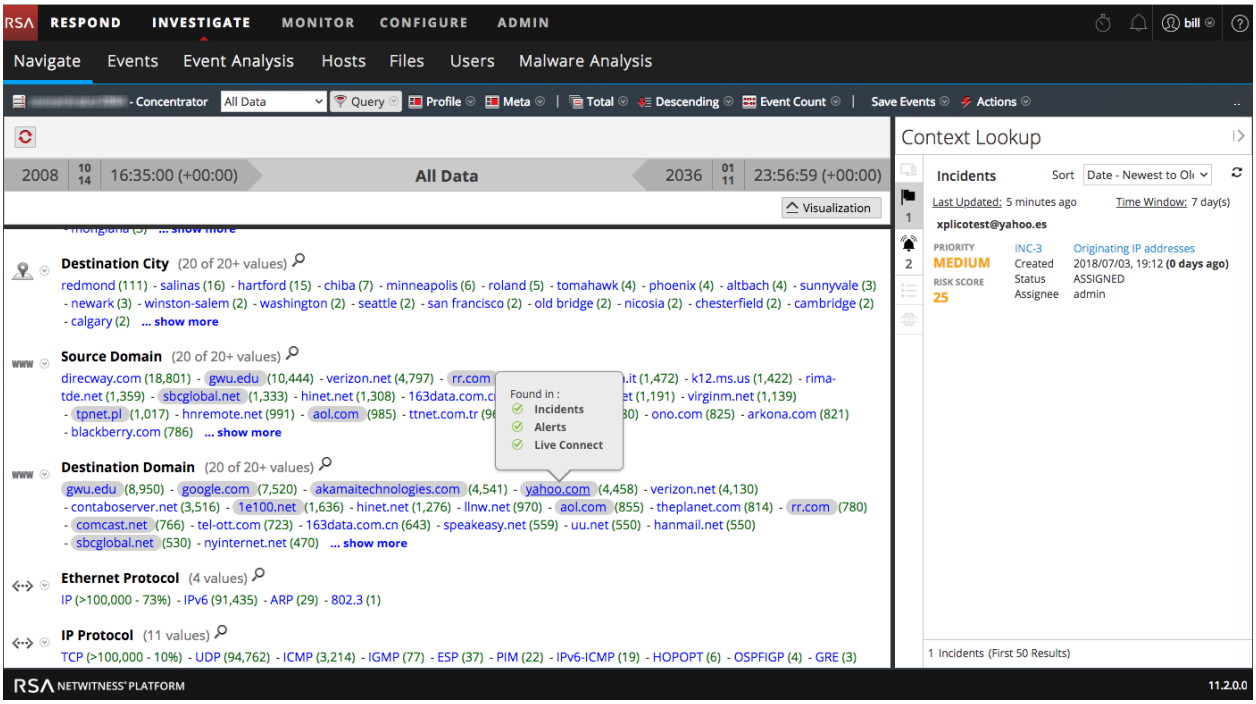
*このタスクは現在のビューで実行できます。

関連トピック

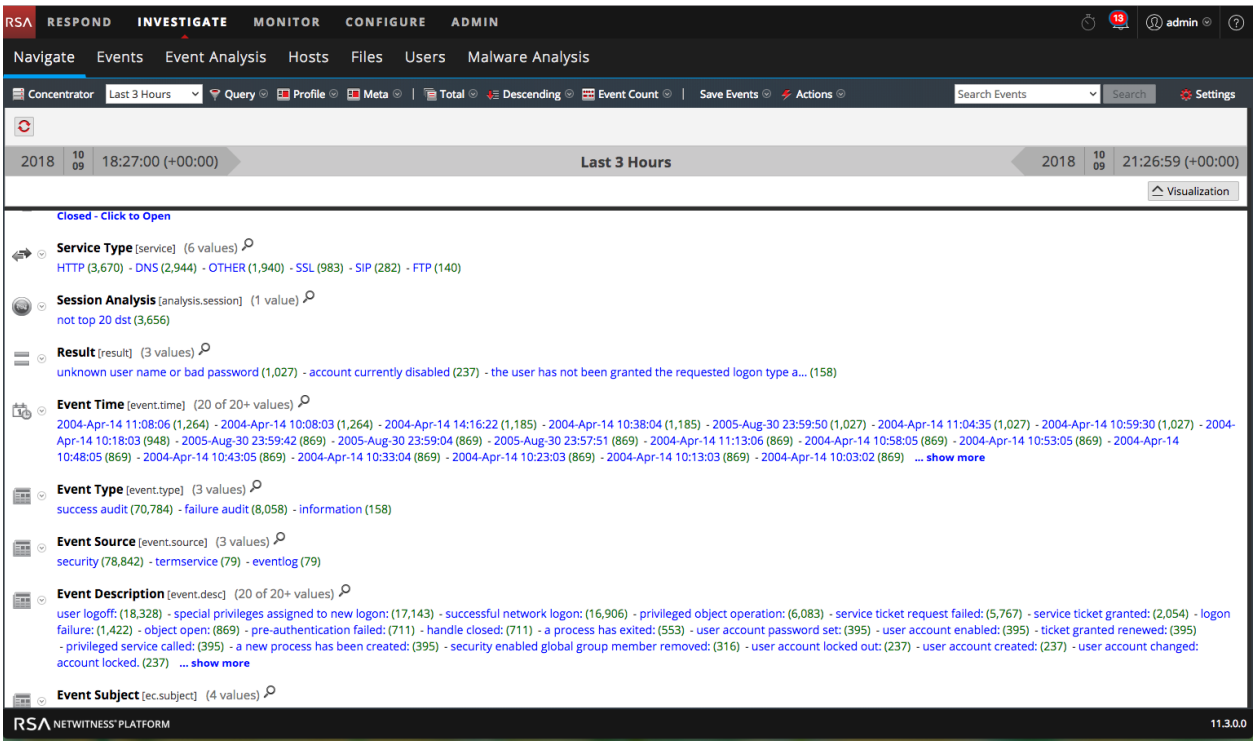
- NetWitness Investigateの仕組み
- [レガシー イベント]ビュー
- [イベント]ビュー

簡単な説明

次の図は、11.2の[ナビゲート]ビューを示しています。



次の図は、11.3の[ナビゲート]ビューを示しています。



[ナビゲート]ビューは次の機能で構成されます。

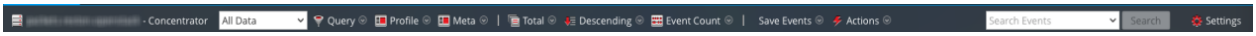
- ツールバー
- 一時停止/再ロード ボタンと階層リンク
- 時間バナー
- オプションのデバッグ情報
- 折りたたみ可能なチャート パネル
- 値パネル
- [コンテキスト ルックアップ]パネル
- コンテキスト メニュー

ツールバー

次の図はツールバーの例です。ツールバーからは以下の操作を行うことができます。

- 調査するサービスを変更する。
- 表示されるデータの範囲を制御する。使用プロファイルの選択、時間範囲の設定、メタ グループの使用、データに適用するクエリの作成が可能です。
- 値パネルのデータの集計方法とソート方法を設定する。

- 結果に対してアクションを実行する。結果のエクスポートや印刷、イベントIDが分かっているイベントの[レガシー イベント]ビューまたは[イベント]ビューでの表示、Informerへのクエリの送信が可能です。
- [調査]ビューを表示したまま調査の設定を構成する。



ツールバーの一部のオプション ラベルでは、そのオプション名が表示されるのではなく、デフォルト値または選択された値がラベル表示されます。たとえば、前の図の例の時間範囲オプションは、現在選択されている値を反映して、「**直近5分**」というラベルで表示されています。これは、ツールバーのオプションです。

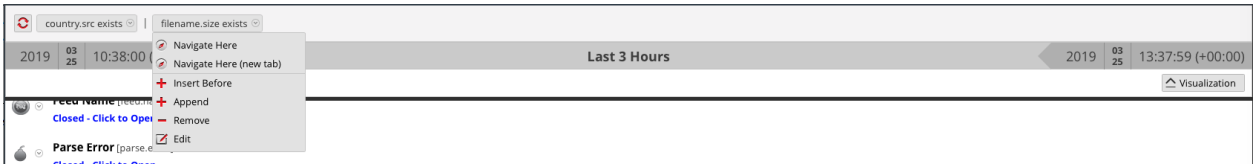
オプション	説明
	アイコンの横に選択したサービス名が表示されます。このアイコンをクリックすると、[サービスの調査]ダイアログが開きます。このダイアログで、調査するサービスを選択したり、調査するデフォルト サービスを設定したりできます(「[ナビゲート]ビューまたは[レガシー イベント]ビューでの調査の開始」を参照してください)。サービスを変更しても、データが再ロードされるわけではありません。
時間範囲	時間範囲オプションが表示されます。ツールバーには現在選択されているオプションが表示されます(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。選択可能なオプションは次のとおりです。 • すべてのデータ • 直近5、10、15、30分 • 直近1、3、6、12、24時間 • 直近2、5日間 • 早朝 • 午前 • 午後 • 夕方 • 終日 • 昨日 • 今週 • Last Week • カスタム **注**: カスタムの開始時刻と終了時刻を秒単位で指定しても、開始時刻の秒は常に:00に、終了時刻の秒は常に:59に変更されます。たとえば、時間を使用して問題にドリルダウンする場合、ドリル時間は「HH:MM:00～HH:MM:59」と解釈されます。Investigate機能では、この形式で秒が表示されます。

オプション	説明
クエリ	[クエリ]ダイアログが表示されます。ここでは、データをドリルダウンするのではなく、カスタム クエリを直接入力できます。このダイアログの詳細については、「[クエリ]ダイアログ」を参照してください。
プロファイル	[プロファイル]メニューを表示します。現在選択されているプロファイルがツールバーに表示されます。プロファイルでは、カスタム メタ グループ、デフォルトの列グループ、プレクエリなどを管理および使用できます。プロファイルは、[ナビゲート]ビュー(メタ グループとクエリ)、[レガシー イベント]ビュー、および[イベント]ビュー(列グループとクエリ)に適用されます。詳細については、「クエリ プロファイルを使用した調査の共通領域のカプセル化」を参照してください。
メタ	[メタ グループ]メニューを表示します。デフォルトのメタ キーまたはカスタム メタ グループを使用できます。両方のグループ タイプで、設定を変更することができます(「メタ グループを使用して関連性の高いメタ キーにフォーカス」を参照してください)。
整列フィールド	[ソート フィールド]メニューが表示されます。ツールバーには現在選択されているオプションが表示されます。このメニューには、[合計で並べ替え]と[値で並べ替え]という2つのオプションがあります。ソート フィールドはソート順オプションと一緒に使用します。各メタ キーのデータが、合計(緑の数字)またはメタ値(青のテキスト)に基づいて並べ替えられます(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。
ソート順	[ソート順]メニューが表示されます。ツールバーには現在選択されているオプションが表示されます。このメニューには、[昇順でソート]と[降順でソート]という2つのオプションがあります。ソート順はソート フィールド オプションと一緒に使用します。各メタ キーについて選択したソート フィールドが昇順または降順で並べ替えられます(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。
集計方法	[集計方法]メニューが表示されます。ツールバーには現在選択されているオプションが表示されます。集計方法は、[値]パネルのメタ キーの結果にのみ適用されます。タイムラインには適用されません。 ドロップダウン メニューには、メタ値の個数(括弧で囲まれた緑色の数字)を計算するための、[イベント数で集計]、[イベント サイズで集計]、[パケット数で集計]という3つのオプションがあります(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。 これらのオプションがどのように適用されるかは、表示されているデータのタイプによって異なります。 パケット データの場合: • [イベント数で集計]を選択すると、セッション数が示されます。 • [イベント サイズで集計]を選択すると、サイズ(バイト)が示されます。 • [パケット数で集計]を選択すると、パケット数が示されます。 ログ データの場合: • [イベント数で集計]を選択すると、ログの数が示されます。 • [イベント サイズで集計]を選択すると、サイズ(バイト)が示されます。 • [パケット数で集計]を選択すると、ログの数が示されます。

オプション	説明
イベントの保存	[イベントの保存]メニューが表示されます。このメニューには、イベントに関連づけられているファイルを抽出するオプション、現在のドリルダウン ポイントをPCAPファイルとしてエクスポートするオプション、現在のドリルダウン ポイントをログ ファイルとしてエクスポートするオプションがあります(「ドリルダウン ポイントのエクスポート」を参照してください)。
アクション	アクション メニューには、[ナビゲート]ビューで実行できるアクションが表示されます(「結果セットの絞り込み」を参照してください)。バージョン11.1以降では、オプションは[可視化]、[イベント再構築に移動]、[イベント ビューに移動]、[印刷]です。
イベントの検索	現在のイベント セット内でテキスト パターンを検索できます。[検索]フィールドをクリックすると、検索オプションを示すドロップダウン メニューが表示されます。[適用]をクリックすると、選択したオプションが保存され、[レガシー イベント]ビューと[調査]プロファイルの検索オプションも更新されます(「[ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索」を参照してください)。
設定	[ナビゲート]ビューの設定([プロファイル]ビューでも編集可能)が表示されます。これにより、[ナビゲート]ビューから移動せずに調査の設定を変更できます。[ナビゲート]ビューで変更した設定は、[プロファイル]ビューでも変更されます(「[ナビゲート]ビューおよび[レガシー イベント]ビューの構成」を参照してください)。

一時停止/再ロード ボタンと階層リンク

階層リンクでは、サービスのメタデータをドリル ダウンするときに、各クエリがトラッキングされます。次の図は階層リンクの例です。



各クエリは、ドロップダウン メニューにパイプ区切りの文字列として表示されます。最後尾のクエリが現在のドリルダウン ポイントです。チップとも呼ばれます。階層リンクの横のアイコンを使用して、メタ値のロードを一時停止したり、メタ値を再ロードしたりすることができます。階層リンクにはサービス名は含まれず、有効なクエリがある場合にのみクエリが表示されます。表示するドリル ポイントが多すぎて、表示しきれない場合には、階層リンクの最後尾に二重山括弧(>>)が表示されます。階層リンクの各ドロップダウン メニューは、リンクの位置に応じた多少の違いがあります。

次の表は、階層リンクのコントロールとメニュー オプションについて説明したものです。

機能	説明
Pause	一時停止/再ロード ボタン。ビューへのデータのロードを制御します。ロードの一時停止、ロードの続行、再ロードという3つの機能を備えています。
ここからナビゲート	選択されているドリルダウン ポイントを現在の値パネルで開きます。
ここからナビゲート(新しいタブ)	選択されているドリルダウン ポイントを新しいタブで開きます。

機能	説明
前にクエリを挿入	現在のドリルダウン ポイントの前にクエリを挿入します。[フィルタの作成]ダイアログが開き、階層リンクに挿入するカスタム クエリを定義できるようになります(「[ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成」を参照してください)。
後にクエリを挿入	現在のドリルダウン ポイントの後にクエリを追加します。[フィルタの作成]ダイアログが開き、階層リンクに挿入するカスタム クエリを定義できるようになります(「[ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成」を参照してください)。
削除	選択されているドリルダウン ポイントを階層リンクから削除します。
編集	選択されているドリルダウン ポイントが[フィルタの作成]ダイアログで開き、クエリを編集できるようになります。
>>	二重山括弧をクリックすると、階層リンクに表示しきれなかったドロップ ポイントがドロップダウン メニューに表示されます。

(オプション) デバッグ情報

[デバッグ情報の表示]設定を有効化していて、ナビゲートしているサービスがBroker(NetWitness Platform) である場合、階層リンクの下にデバッグ情報が表示されます。

デバッグ情報とは、現在のクエリに含まれているWHERE句を指します。[時間範囲]オプションで[すべてのデータ]が選択され、ドリルダウン ポイントがない場合に限ってWHERE句は表示されません。Brokerにオフラインの集計サービスが少なくとも1つある場合は、デバッグ情報にもオフラインのサービスが表示されます。

次に例を挙げます。

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info exists)$$time='2014-05-04 18:50:00"-"2014-05-09 18:59:59(attachment exists) && (tcp.dstport = '80') && (risk.info exists) && time="2014-05-04 18:50:00"-"2014-05-09 18:50:59"
```

また、ロードに要する時間は値パネルの各メタ キーの末尾に表示されます。

時間バナー

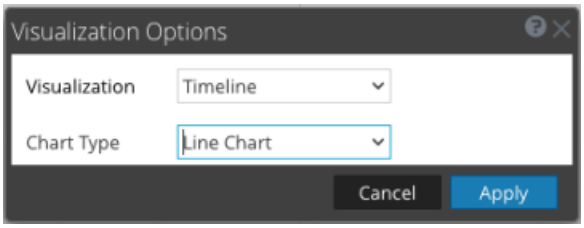
階層リンクとデバッグ情報(ある場合) のすぐ下にある時間バナーには、チャートの作成に使用される時間範囲が示されます。次の図は時間バナーの例です。

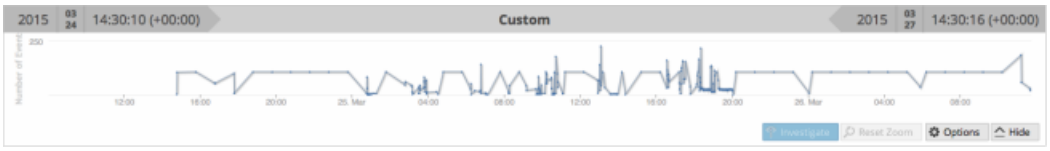
ビジュアル画像

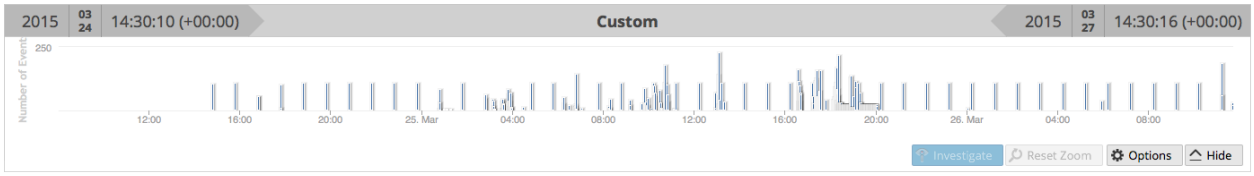
[ナビゲート]ビューの上部には、現在のドリルダウン ポイントが表示されます。これを使用して、[チャート]パネルのデータをドリル ダウンできます(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。チャートの表示と非表示を切り替えて、[タイムライン]または[座標]のいずれかのチャート オプションを選択できます。最初に表示されるのは、前回保存したチャート設定です。

タイムライン チャート

タイムラインは、特定のインスタンスで発生するイベント数のカウントです。タイムラインでは、イベント数が特定のポイント インタイムで急増したかどうかを確認できるように、イベントのカウントを提供します。タイムラインには、指定したサービスと時間範囲のアクティビティが表示されます。表示の形式は、[オプション]メニューでの選択に応じて、折れ線グラフか棒チャートになります。2番目の図は折れ線チャート、3番目の図は棒チャートを示しています。





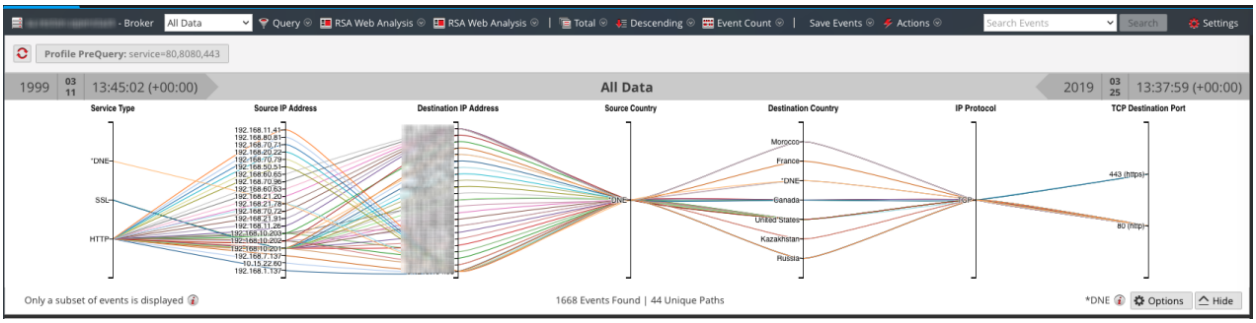


タイムラインには、指定したサービスと時間範囲のアクティビティが表示されます。表示の形式は、[オプション]メニューでの選択に応じて、折れ線グラフか棒チャートになります。

機能	説明
イベント数(タイムライン)	チャートのY軸はイベント数を表しています。
時間軸(タイムライン)	チャートのX軸は、イベントが発生した時刻を表しています。
イベント ポイント(タイムライン)	特定の時間範囲のセッションについて調査する場合は、チャートから範囲を選択します。新しい時間範囲がチャートに反映されます。
Investigate(タイムライン)	選択した時間範囲のメタ値が結果パネルに表示されます。
ズームのリセット(タイムライン)	元の時間範囲に戻るには、[ズームのリセット]をクリックします。
オプション	[チャート オプション]ダイアログが表示されます。データ ポイントは折れ線チャート(デフォルト)、棒チャート、座標チャートのいずれかで表示できます。チャートのタイプを選択すると、関連するオプションが表示されます。
非表示	チャートを折りたたみます。

座標表示チャート

座標表示チャートは、現在のドリルダウン ポイントをビジュアル化するために[オプション]メニューから選択できるオプションの1つです。[チャート オプション]ダイアログで[座標表示]が選択されている場合は、表示するメタ データを選択できます(「座標表示チャートへのメタデータの追加」を参照してください)。便利な座標表示チャートを表示するには、次の図に示すように、プロファイル グループを選択します。



機能	説明
軸	各軸はメタ キーです。メタ キーの数は、チャートのロード時間に影響します。すべてのメタ キーがロードされますが、メタ キーあたりのイベント数は制限されています。
行	線はイベントを表し、軸上の値を接続することで、複数のメタ キー間の相関関係を示します。
オプション	[チャート オプション]ダイアログが表示されます。データ ポイントは折れ線チャート(デフォルト)、棒チャート、座標チャートのいずれかで表示できます。チャートのタイプを選択すると、関連するオプションが表示されます。
イベントのサブセットのみが表示されます。	このメッセージは、値パネルのすべてのイベントがチャートに表示されているわけではないことを示す通知メッセージです。値パネルで軸を削除するか、データをフィルタすると、すべてのイベントを表示できる場合があります。
見つかったイベントの数 | 一意のパスの数	チャートに表示されているイベントの総数とチャートに表示されている一意のパスの数の比率が表示されます。[すべてのメタ キーが1つのイベントに存在する必要があります]オプションを設定すると、チャートが再描画され、目的が明確で分かりやすくなります。
DNE	このメタ キーの値がイベント内にないことを示します。

座標表示の[チャート オプション]ダイアログでは、チャートに含めるメタ キーを選択できます。

機能	説明
チャートの選択	チャート タイプ([タイムライン]と[座標])のドロップダウン リストを表示します
すべてのメタ キーが1つのイベントに存在する必要があります	チャートに表示するデータを、選択したメタ キーをすべて含んでいるイベントのみに制限します。これにより、目的が明確で整然としたチャートになります。

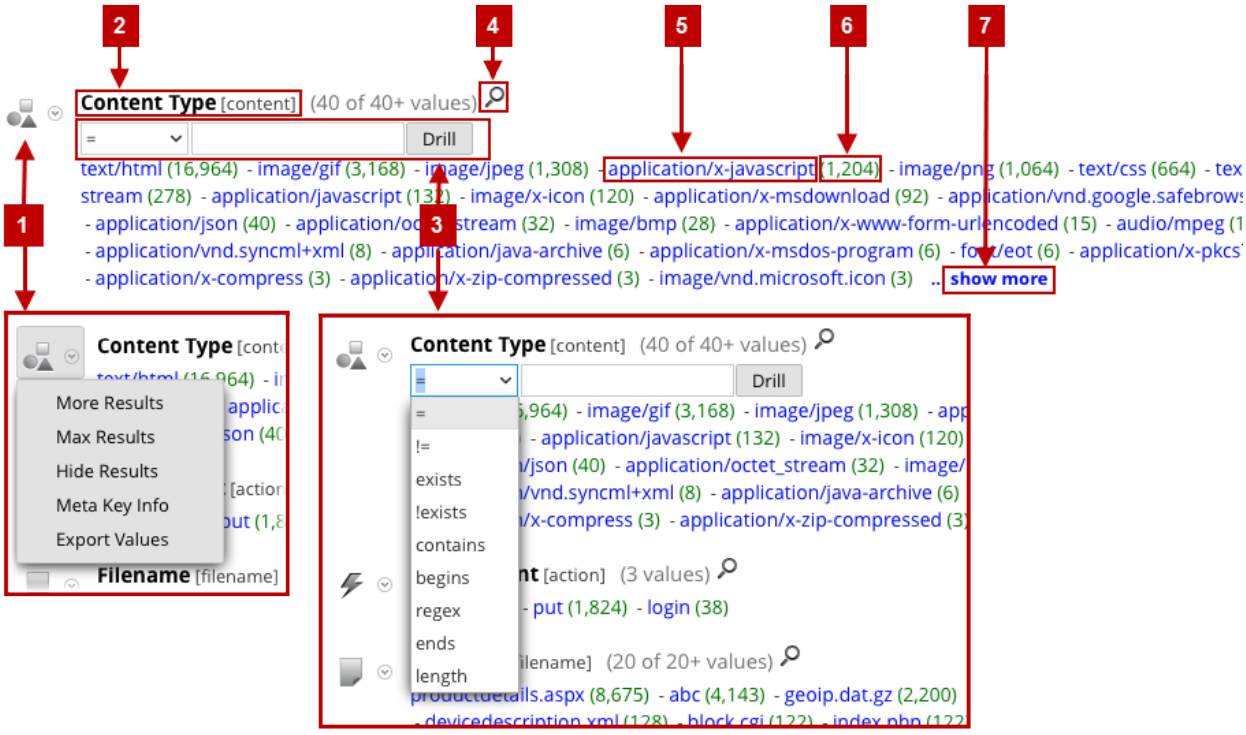
機能	説明
	[座標表示チャートへのキーの追加]ダイアログが表示され、チャートに軸を追加できるようになります。この機能は、デフォルトのメタ キーと追加のメタ キーとの間の関係を調べる場合に便利です。
	選択したキーを削除して、チャートの軸に表示されないようにします。これにより、チャートが整然とし、より多くのデータ ポイントをチャートに含められるようになります。
	チャートのメタ キーを、現在のドリルダウン ポイント内のすべてのメタ キーで構成されるデフォルト値に戻します。
	選択された軸の数と推奨される軸の数の比較に関する追加情報の表示を制御します。これにより、軸を削除することによるパフォーマンス向上の可能性について認識できます。
軸	チャートで軸として選択されているメタ キーが表示されます。
キャンセル	チャート オプションに対して加えられたすべての変更を取り消します。
適用	チャート オプションに対する変更を保存し、現在のチャートに変更を適用します。

[座標表示チャートへのキーの追加]ダイアログでは、座標表示チャートの軸として使用するメタ キーまたはメタ グループを選択できます。

機能	説明
チャートの選択	キーの選択 : メタ キーを選択するためのオプションは次の2つです。 • デフォルトのメタ キーから追加 • メタ グループから追加 いずれのオプションにも、メタ キーを選択するためのドロップダウン リストがあります。
選択したメタ キーの追加オプション	メタ キーの追加方法に関するオプションにより、次の操作を実行できます。 • 現在のキーのリストを置き換え • 現在のキーのリストの後に挿入 • 現在のキーのリストの先頭に挿入
キャンセル	キーを追加せずにダイアログが閉じられます。
追加	ダイアログが閉じられ、選択したキーが指定したとおりに追加されます。

値パネル

[ナビゲート]ビューの主要機能である[値]パネルには、調査中のサービスで見つかったメタ キーとメタ値が表示されます。[値]パネルでのデータの分析手順については、「[ナビゲート]ビューでの結果のフィルタリング」を参照してください。



注： インデックスなしのメタ キーについては、タイトル、値、数でのドリル ダウンができません。これらのメタ キーの値と数は黒いテキストで表示されます。

1 [値]パネルのメタ キーには、そのメタ キーに適用できるアクションを含んだドロップダウン メニューがあります。オプションを選択して、現在のビューにおけるメタ キーの結果の表示方法を変更できます。現在のビューのメタ キー表示に対して行った変更は、ページの表示を更新するか、[ナビゲート]ビューのツールバーで新しいサービスを選択するまで維持されます。「[値]パネルでのデータのドリルダウン」を参照してください。

ページの表示を更新すると、[デフォルトのメタ キーの管理]ダイアログで定義されているとおりに、メタ キーの現在のビューが復元されます(「調査でのデフォルト メタ キーの管理と適用」を参照してください)。[デフォルトのメタ キーの管理]ダイアログで変更を行ったことがない場合は、コア サービスに設定されているデフォルトのメタ キーがNetWitness Platformによって復元されます。

- 表示範囲の拡大
- 最大まで表示
- 結果を折りたたみ表示
- メタ キー情報
- 値のエクスポート

2 値が表示されているメタ キーの名前。バージョン11.3以降では、メタ キーのユーザ フレンドリー名が、角括弧で囲まれたメタ キーのインデックス ファイル名とともに表示されます。たとえば、**Content Type [content]**は、`content`メタ キーのユーザ フレンドリー名と、括弧で囲まれたインデックス ファイル名を表しています。メタ グループの場合、グループ名は

	英語で表記され、括弧で囲まれたメタ グループ名とともに表示されます。**All User Keys [users.all]**は、[値]パネルに表示されるメタ グループ名の例です。
3および4	インデックス付きのメタ キーに対して🔍をクリックすると、[検索]ダイアログが開き、現在のメタ キーに適用するフィルタを入力できるようになります。検索機能は、インデックスなしのメタ キーでは使用できず、エイリアスではなく実際のメタの値に基づいています。エイリアスを使用した[検索]ダイアログのドリル ダウンはサポートされていません。 注 : 調査でメタ キーに使用されるエイリアスのリストを取得するには、管理者に問い合わせてください。エイリアスが使用されると、[検索]ダイアログには結果が表示されません。メタ キーのクエリには、エイリアスを使用するのではなく、右クリックのクエリ機能または[クエリ]ダイアログを使用する必要があります。
5	見つかったメタ キーに関連づけられたメタ値。設定に応じて、メタ値の名前順、またはメタ値が見つかったイベント数順に表示されます。
6	メタ値を含むイベントの数。
7	ロードする値の数は、調査の環境設定の表示スレッド値によって指定されます。前の例では、メタ キーは**Content Type**で、40個以上ある値のうちの40個が現在表示されています。[**表示範囲の拡大**]をクリックすると、追加の値を表示できます。セッションで特定のメタに対して見つかったインスタンスの数。

[値]パネルのロード動作

デフォルトのビューは、デフォルトのメタ キーと折りたたみ表示されたインデックスなしのメタ キーで構成され、過去3時間の収集データが表示されます。メタ グループ内のメタ キーは、NetWitness Platformによるキーのクエリ順に表示されます。NetWitness Platformは、[値]パネルへのデータのロード中に、結果の一部、ロードの進行状況、サービスのステータスを表示するよう最適化されています。

ロード動作は、複数の構成設定によって決まります。管理者によって構成された設定が最も優先されます。それらは次のとおりです。

- このユーザに許可されているクエリの最大実行時間(クエリ タイムアウト)。
- NetWitness Platformがセッション内のメタ値のカウントを停止する限界値(セッション閾値)。セッションの閾値を設定し、実際にユーザによるスキャンが閾値に達した場合、[ナビゲート]ビューは閾値に達したこと、またロードされた結果の割合を表示します。割合を表示しないセッションは正確であり、処理が完了しています。割合がある場合は、処理が完了した割合を反映しています。表示される割合は、残りの作業量を考慮し、処理が完了した時点の値から推定することよって見積もられます。推定があまり必要ないため、一般的に大きな割合ほど正確です
- NetWitness Platformがセッション内のメタ値のカウントを停止する限界値(セッション閾値)。セッションの閾値を設定し、実際にユーザによるスキャンが閾値に達した場合、[ナビゲート]ビューは閾値に達したこと、また閾値に達するまでに要したクエリの時間の割合を表示します。

注 : インデックスなしのメタ キーの値は、値パネルにロードされるのに時間がかかります。ロードを最適化するため、NetWitness Platformでは、インデックスなしのメタ キーはデフォルトで展開されません。調査での非インデックス メタ キーの詳細については、「調査でのデフォルト メタ キーの管理と適用」を参照してください。

サービスの調査を開始すると、NetWitness Platformによって結果が値パネルに表示されます。

1. NetWitness Platformによってメタ キーとメタ値が値パネルにロードされます。各メタ キーのロードは次の段階に分けて行われます。

a. **ロードの待機中**、または**折りたたみ表示**：折りたたみ表示の場合、そのキーのデータはロードされません。

b. **ロード中**

i. **ロードの進行状況**：NetWitness Platformによって進行状況メッセージが受信され、表示されます。

ii. **部分的結果**：NetWitness Platformによって値のメッセージが受信され、部分的な結果が値パネルに表示されます。

c. **ロード完了**：すべての結果のロードが完了しました。

2. 各メタ キーのロードが完了すると、最終的な値が表示され、次のメタ キーのロードが開始されます。メタ キーごとに同時にロードされる値の数は、調査の環境設定の表示スレッド値によって指定されます。すべてのキーのロードが完了するまで、ロードが継続します。

3. [**デバッグ情報の表示**]が有効で、ナビゲートしているサービスが10.4以降のBrokerの場合、NetWitness Platformでは、各メタ キーの値の下にロード時間情報が表示され、サービス集計でのロードの詳細情報が表示されます。また、NetWitness Platformでは階層リンクの下にデバッグ情報も表示されます。

反復的結果

反復的結果では、クエリのステータスに関するフィードバックがインタフェース内に表示され、データ ロードの所要時間とサービス データの欠落の有無についてのコンテキストが提供されます。たとえば、2つのConcentratorから集計しているBrokerに対してクエリを実行する場合、2番目のConcentratorからの結果を待っている途中でも、最初のConcentratorからの結果が利用可能になり次第、NetWitness Platformは結果を表示します。

また、反復的結果には、サービスにアクセスできないことが原因でサービス データが欠落している場合に、そのことを示す通知も表示されます。

部分的結果

完全ではない部分的な値がコアサービスから返されると、値のロードの進行状況を示すメッセージがメタ キー リストの末尾に表示されます。たとえば、現在38 ip.src値を処理中(71%) とは、メタ キー値のロードが71%完了していることを示しています。

デバッグ情報

[デバッグ情報の表示]設定が有効な場合、値の末尾にあるフィールドには、NetWitness Platform内でクエリしている各システムのステータスが表示されます。たとえば、複数のConcentratorからデータを集計している10.4 Brokerに対してクエリを実行している場合は、各Concentratorに対するクエリのステータスがNetWitness Platformに表示され、各Concentratorからのデータ ロードの相対的な速度を把握できます。クエリで使用される各サービスは、クエリ全体の経過時間とともに表示されます。

クエリで使用される各サービスは、クエリ全体の経過時間とともに表示されます。前掲の例では、2つのサービスが3.207秒で結果を返し、localhost:50005は結果を2秒で返していることを示しています。また、階層リンクの下には、クエリのWHERE句も表示されます。この構文は、アプリケーション ルールまたはルールのレポート WHERE句に直接コピーできます。

ロード完了

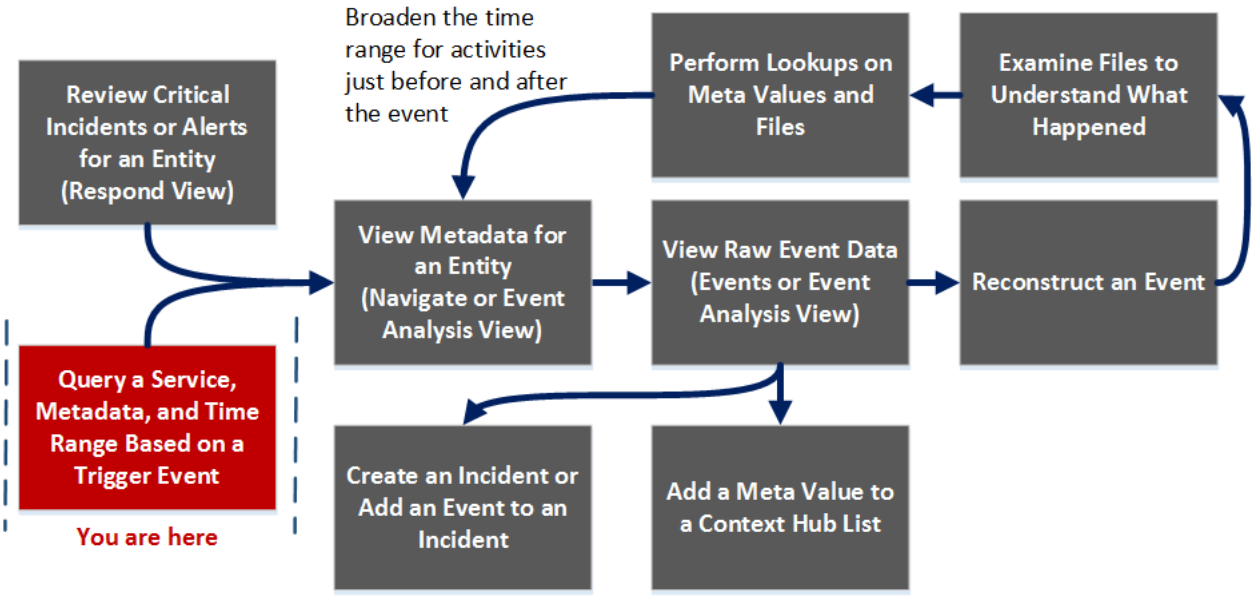
現在のドリルダウン ポイントで見つかった各メタ キーの値 (青のテキスト) とその数 (緑のテキスト) のリストが表示されます。表示されているデータの特定のサブセットを詳しく調べるには、調査する値をクリックします。表示が更新され、新しいドリルダウン ポイントに移動します。ツールバーのオプションを使用して、値のソート方法と集計方法を指定することもできます。

[クエリ]ダイアログ

[ナビゲート]ビューまたは[レガシー イベント]ビューでは、メタ キーや値をクリックする代わりにクエリを作成して、メタ データをドリル ダウンすることができます。クエリ作成のためのダイアログには、使用可能なメタ キーや演算子がドロップダウン リストで表示される構文ヘルプが用意されています。このダイアログにアクセスするには、[**ナビゲート**]ビューまたは[**レガシー イベント**]ビューのツールバーで、[**クエリ**]を選択します。

ワークフロー

このワークフローでは、バージョン11.4で名称変更されたビューが参照されています。[イベント分析]ビューは[イベント]ビューになり、[イベント]ビューは[レガシー イベント]ビューになりました。



実行したいことは何ですか?

ユーザ ロール	実行したいこと	手順
インシデント対応者	重要なインシデントまたはアラートの確認	『*NetWitness Respond*ユーザ ガイド』
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行*	[イベント]ビューでの結果のフィルタリング [ナビゲート]ビューでの結果のフィルタリング [ナビゲート]ビューと[レガシー イベント]ビューでのクエリの作成 [レガシー イベント]ビューでの結果のフィルタリング

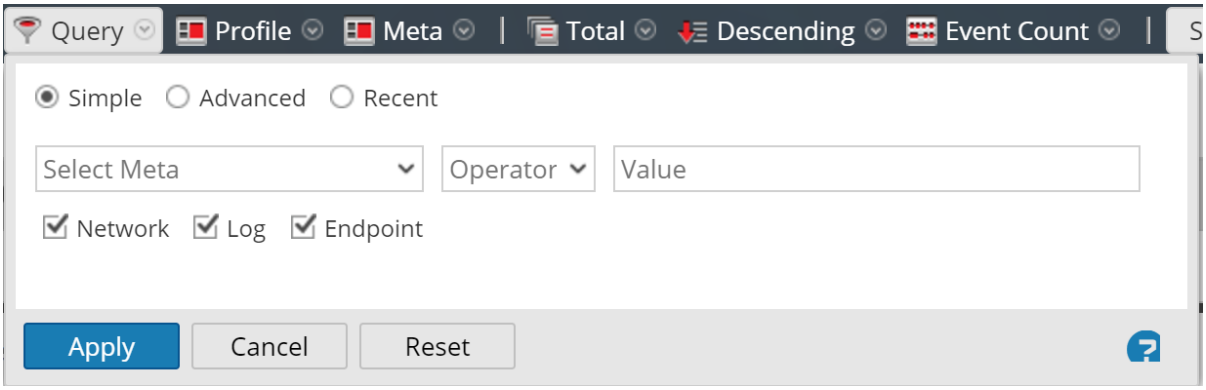
ユーザ ロール	実行したいこと	手順
脅威ハンター	メタデータの表示	[イベント]ビューでのイベントの分析 結果セットの絞り込み
脅威ハンター	RAWイベント データの表示	[イベント]ビューでの結果のフィルタリング [イベント]ビューでのイベントの分析 [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築	[イベント]ビューでのイベントの分析 [イベント]ビューでのイベントの再構築 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルの検証	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威ハンター	インシデントの作成またはインシデントへの追加	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威ハンター	Context Hubリストへのメタ値の追加	結果の追加のコンテキストを検索

*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [ナビゲート]ビュー
- [レガシー イベント]ビュー

簡単な説明

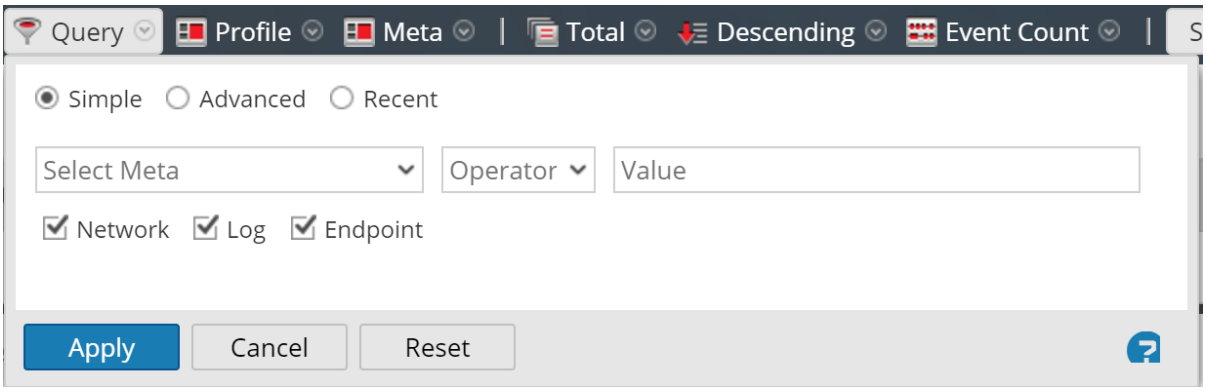


[クエリ] ダイアログには次の3つのビューがあります。

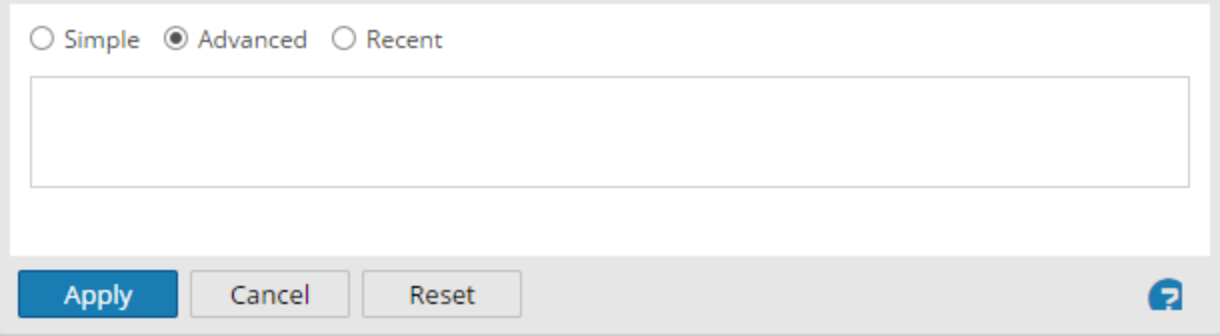
- シンプル
- 拡張
- 最近実行したクエリ

[シンプル] ビューでは、ダイアログに表示されているオプションを使用してクエリを作成できます。[詳細] ビューでは、ガイダンスなしでクエリを作成できます。[最近実行したクエリ] では、最近実行したクエリのドロップダウン リストからクエリを選択できます。

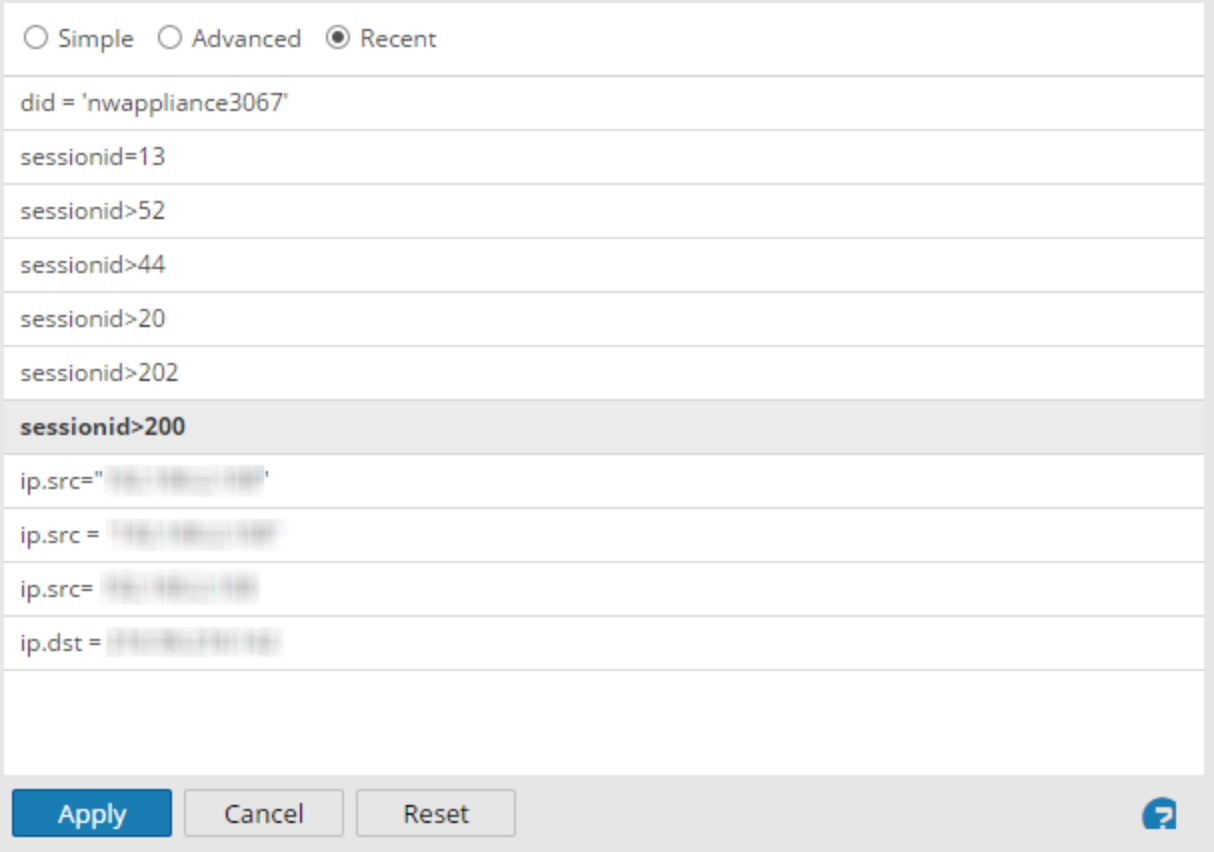
[シンプル] ビュー



[詳細]ビュー



[最近実行したクエリ]ビュー



次の表は、[クエリ]ダイアログの機能について説明しています。

機能	説明
メタの選択	メタ グループのドロップダウン リストを表示します。
演算子	演算子 (=、NetWitness Platform!=、NetWitness Platformexists、NetWitness Platform!exists)のドロップダウン リストを表示します。

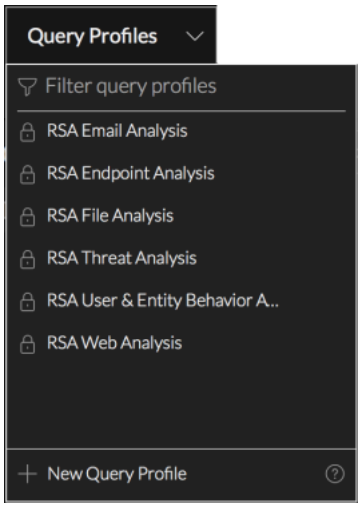
機能	説明
値	クエリを完成させるための値を入力します。
ネットワーク	[ログ]が選択されていない場合に、クエリの対象をパケットに限定します。
ログ	[ネットワーク]が選択されていない場合に、クエリの対象をログに限定します。
クエリ ボックス	[詳細]ビューで、クエリを入力できます。入力を開始すると、サービスで使用可能なメター キーのドロップダウン リストが表示され、入力内容に応じて演算子のドロップダウン リストが表示されます。クエリ ボックスに入力されている式が無効な場合は、ボックスの近くに警告が表示されます。クエリが有効になると、警告は消えます。
クエリ リスト	[最近実行したクエリ]ビューで、最近実行したクエリのリストからクエリを選択します。クエリをダブル クリックすると、自動的に適用されます。
適用	現在の[調査]ビューに、新しいクエリを適用します。
キャンセル	変更を加えずにダイアログを閉じます。
リセット	すべてのフィールドをリセットします。

[クエリ プロファイル]ダイアログ

クエリプロファイルを使用すると、メタ グループ、列グループ、および制限クエリに基づいて、[ナビゲート]ビュー、[イベント]ビュー、[レガシー イベント]ビューのカスタム ビューを設定できます(「クエリ プロファイルを使用した調査の共通領域のカプセル化」を参照)。標準提供プロファイルは、初めてログインしたときに使用できます。標準提供プロファイルの名前は、「RSA」で始まり、[Default Profiles]の下にグループ化されています。標準提供プロファイルを編集または削除することはできません。

標準提供プロファイルとカスタム プロファイルの管理は、[プロファイルの管理]ダイアログ、[クエリ プロファイルの作成]ダイアログ、[クエリ プロファイルの詳細]ダイアログで行えます。

- [プロファイルの管理]ダイアログは、[ナビゲート]ビュー、[レガシー イベント]ビュー(バージョン11.4)、[イベント]ビュー(バージョン11.3以前)で開くことができます。[プロファイルの管理]ダイアログでは、プロファイルのメタ グループの選択、プロファイルのインポートとエクスポート、プロファイルのコピーと編集、プロファイル グループへのプロファイルの分類という、[クエリ プロファイル]ダイアログにない機能を実行できます。このダイアログにアクセスするには、[**ナビゲート**]ビューまたは[**レガシー イベント**]ビューのツールバーで**[プロファイル]＞[プロファイルの管理]**を選択します。
- [クエリ プロファイルの作成]ダイアログは、11.4の[イベント]ビューから開くことができます。このダイアログにアクセスするには、[**イベント**]ビューのツールバーで**[クエリ プロファイル]＞[新しいクエリ プロファイル]**を選択します。



- [クエリ プロファイルの詳細]ダイアログは、11.4の[イベント]ビューから開くことができます。このダイアログにアクセスするには、[**イベント**]ビューのツールバーで[**クエリ プロファイル**]を選択して、カスタム プロファイル名の横の編集アイコン( ) をクリックします。

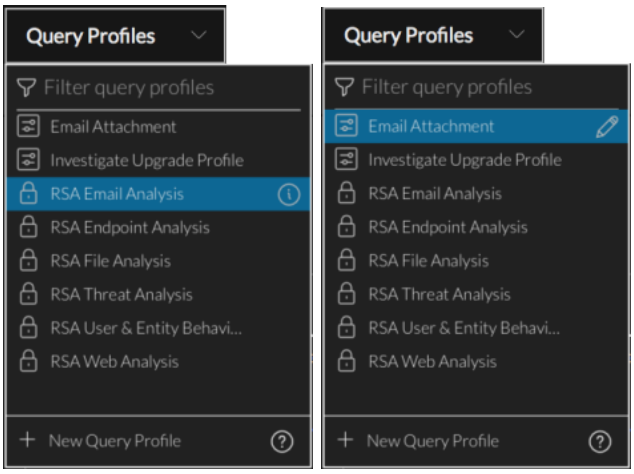
関連トピック

- NetWitness Investigateの仕組み
- [ナビゲート]ビュー

- [イベント]ビュー
- [レガシー イベント]ビュー

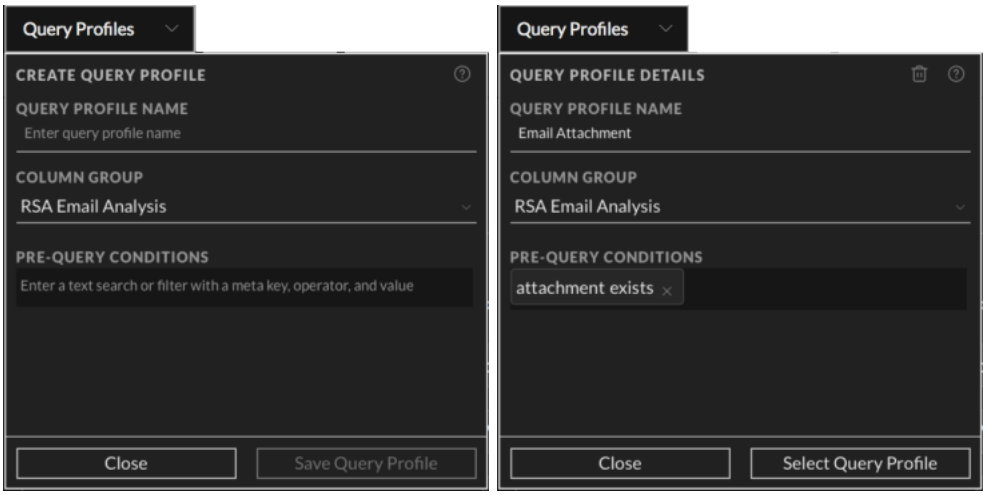
簡単な説明 - [クエリ プロファイル]メニュー、[クエリ プロファイルの作成]ダイアログ、[クエリ プロファイルの詳細]ダイアログ

このセクションでは、[クエリ プロファイル]メニュー、[クエリ プロファイル]ダイアログ、[クエリ プロファイルの詳細]ダイアログについて説明します。次の図は、[クエリ プロファイル]メニューの例です。表にはオプションの説明が記載されています。左側の例では、標準提供プロファイルがハイライト表示されているため、情報アイコンが表示されています。右側の例では、カスタム プロファイルがハイライト表示されているため、編集アイコンが表示されています。



機能	説明
クエリ プロファイルの絞り込み	テキストの入力に合わせて、そのテキストを含んだプロファイル名のみが表示されるように、プロファイルのリストを絞り込みます。
クエリ プロファイル リスト	プロファイルのリストには、カスタム プロファイルと標準提供プロファイルが含まれています。プロファイル名の前に表示されるアイコンで両者を区別できます。この例では、[Email Attachment]と[Investigate Upgrade Profile]がカスタム プロファイルです。「RSA」で始まるプロファイルは標準提供プロファイルです。
新しいクエリ プロファイル	[クエリ プロファイルの作成]ダイアログを表示します。このダイアログでは、カスタム プロファイルを作成できます。

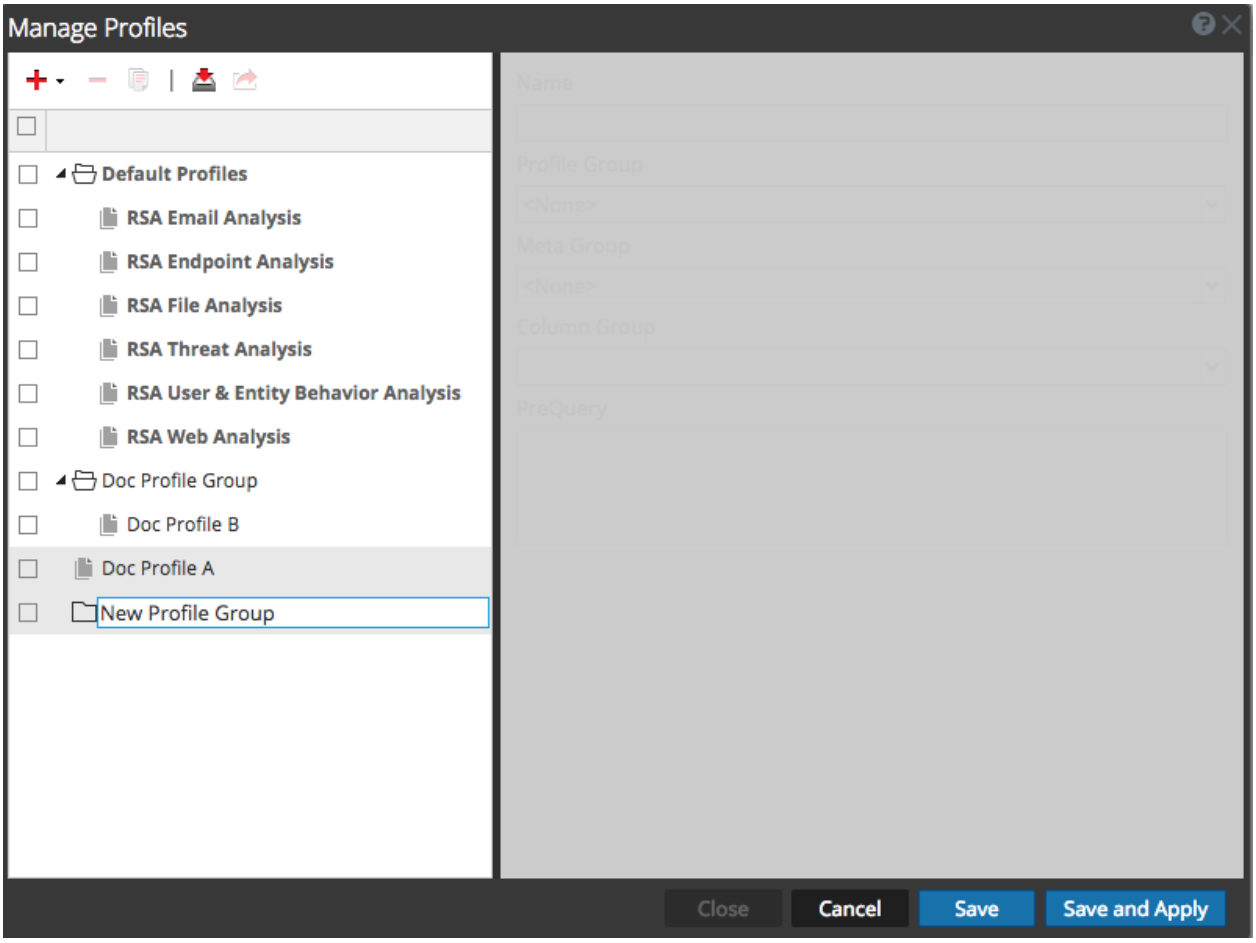
左側の図に示す[クエリ プロファイルの作成]ダイアログを使用して、カスタム プロファイルを定義できます。右側の図に示す[クエリ プロファイルの詳細]ダイアログでは、カスタム プロファイルを編集できます。次の表は、ダイアログ内のフィールドとオプションについて説明したものです。



機能	説明
🗑	[クエリ プロファイルの詳細]ダイアログでカスタム プロファイルを削除します。このアクションは元に戻すことができず、グローバルに適用されます。このサービスで削除されたプロファイルを使用しているすべてのアナリストが、このプロファイルを使用できなくなります。
クエリ プロファイル名	プロファイルの名前を表示します。64文字以内の一意の名前を指定してください。カスタム プロファイルでは、名前を編集できます。
列グループ	使用可能な列グループのリストがドロップダウン メニューに表示されます。イベント リストで現在選択中の列グループが選択された状態で表示されます。カスタム プロファイルでは、列グループを変更できます。
プレクエリ条件	調査する結果をフィルタするための制限クエリを定義します。新しいプロファイルの作成を開始したときにクエリ バーにアクティブなクエリが存在する場合は、そのクエリが[プレクエリ]フィールドに追加されます。カスタム プロファイルでは、[プレクエリ]フィールドで、事前入力されたプレクエリの削除、テキスト検索用の追加のテキストや追加のクエリの入力を行うことができます。このクエリは、このプロファイルが適用されているときに使用されます。プレクエリは、[ナビゲート]ビューおよび[イベント]ビューで実行されるすべてのクエリに適用されます。プレクエリの例を次に示します。 `'service=80,25,110'`
[閉じる]ボタン	ダイアログを閉じます。
クエリ プロファイルを保存	[クエリ プロファイルの作成]ダイアログにのみ表示され、新しいプロファイルを保存します。
リセット	[クエリ プロファイルの詳細]ダイアログにのみ表示され、編集したプロファイルを前回保存した状態に戻します。
クエリ プロファイルを更新	[クエリ プロファイルの詳細]ダイアログにのみ表示され、編集したプロファイルに変更を適用します。
クエリ プロファイルを選択	クエリ プロファイルを適用します。

簡単な説明 - [プロファイルの管理]ダイアログ

次の図は[プロファイルの管理]ダイアログの例で、複数のプロファイル グループが表示されています。



ダイアログの左側にある[プロファイル]パネルには、使用できるプロファイルが表示されます。ここでは、プロファイルを追加、削除、インポート、エクスポートできます。次の表は、[プロファイル]パネルのフィールドについて説明しています。

フィールド	説明
	[プロファイルの管理]ダイアログの右側にある[設定]パネルを使用して、新しいプロファイルを追加します。
	選択したプロファイルを削除します。プロファイルが削除される前に、確認ダイアログが表示されます。
	選択されたプロファイルのコピーを作成します。
	[プロファイルのインポート]ダイアログを表示します。ここでファイルをアップロードできます。

フィールド	説明
	選択したプロファイルをPCにエクスポートします。
プロファイル名	すべてのプロファイル名のリストを表示します。

ダイアログの右側にある[設定]パネルには、プロファイルを構成するためのオプションが表示されます。このパネルは、1つのプロファイルが選択されている場合にのみ使用できます。次の表は、[設定]パネルのフィールドについて説明しています。

機能	説明
名前	プロファイルの名前を表示します。
メタ グループ	使用できるメタ グループのリストが表示されたドロップダウン メニューを表示します。
列グループ	使用できる列グループのリストが表示されたドロップダウン メニューを表示します。標準提供の列グループと以下の3つのグループをデフォルトで使用できます。 • リスト ビュー • 詳細ビュー • ログ ビュー
プレ クエリ	調査する結果をフィルタするための制限クエリを定義します。このクエリは、このプロファイルが適用されている間使用されます。プレクエリは、[ナビゲート]ビューおよび[イベント]ビューで送信されるすべてのクエリに適用されます。プレクエリの例を次に示します。 `'service=80,25,110'`

以下の表は、ボタンについての説明です。

フィールド	説明
閉じる	ダイアログを閉じます。
キャンセル	すべての変更をキャンセルします。
保存	すべての変更を保存します。
保存して適用	すべての変更を保存してすぐに適用します。

[調査]ビューの設定ダイアログ

NetWitness Platformバージョン11.0では、設定ダイアログは、[ナビゲート]ビュー用のものと[レガシー イベント]ビュー用のものの2つがあります。バージョン11.1では、[イベント]ビュー用の設定ダイアログが追加されたので、調査の設定ダイアログは3つあります。

このダイアログの設定は、[プロファイル]＞[環境設定]パネル＞[調査]タブで行う調査の設定のサブセットです。アナリストは、[調査]ビューでこれらの設定を編集することにより、時間を節約できます。ここで設定を変更すると、[プロファイル]ビューで同じ設定が変更されます。[プロファイル]ビューで設定を変更すると、この場所の同じ設定が変更されます。

このダイアログにアクセスするには、[**ナビゲート**]ビューまたは[**レガシー イベント**]ビューに移動し、ツールバーの[**設定**]オプションを選択します。

[プロファイル]＞[環境設定]パネルには、[イベント]ビューの設定に対応する設定はありません。

関連トピック

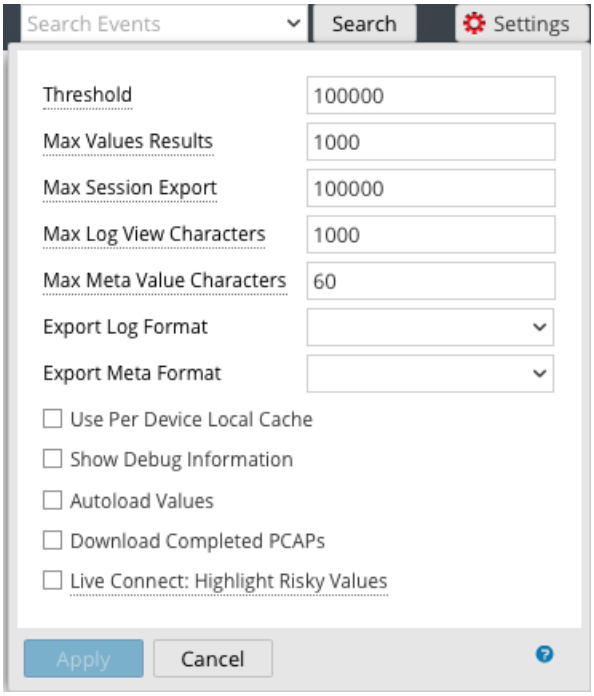
- NetWitness Investigateの仕組み

簡単な説明

ここでは、[ナビゲート]ビュー、[レガシー イベント]ビュー、[イベント]ビューの設定ダイアログについて簡単に説明します。

[ナビゲート]ビューの[設定]ダイアログ

次の図は、[ナビゲート]ビューの[設定]ダイアログを示しています。[値]パネルで値をロードするときのパフォーマンスに影響を与える設定には、一般的な使用方法に基づくデフォルト値があり、アナリストはこれらの設定を自分の調査内容に合わせて調整できます。以下の表は、機能についての説明です。

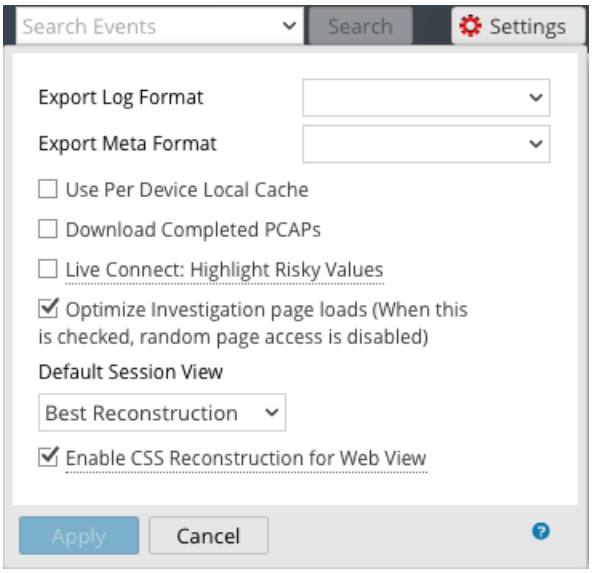


機能	説明
閾値	[値]パネルでメタ キー値にロードするセッションの最大数の閾値を設定します。閾値を高くすると、値が正確にカウントされますが、その分ロード時間が長くなります。デフォルト値は**100000**です。
結果の最大数	この設定は、[ナビゲート]ビューで開いているメタ キーについて、[メタ キー]メニューで[最大まで表示]を選択した場合にロードする値の最大数を制御します。デフォルト値は**1000**です。
最大セッション エクスポート	エクスポートできるセッションの最大数を設定します。デフォルト値は**100000**です。
ログのエクスポート形式	エクスポートされたログのファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト**: RAWログ形式。 • **SML**: 構造化マークアップ言語形式。 • **CSV**: カンマ区切り値(CSV)形式。 • **JSON**: JavaScript Object Notation(JSON)形式。

機能	説明
メタのエクスポート形式	エクスポートされたメタ値のファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト**: RAWログ形式。 • **SML**: 構造化マークアップ言語形式。 • **CSV**: カンマ区切り値(CSV) 形式。 • **JSON**: JavaScript Object Notation(JSON) 形式。
デバイスごとのローカル キャッシュを使用	このチェックボックスをオフにすると、初回ロード後に[調査]ビューにキャッシュされたデータを表示するのではなく、新しいクエリがデータベースに送信されます。チェックボックスをオンにすると、ローカル キャッシュのデータを使用します。
デバッグ情報の表示	このオプションは、階層リンクの下の`where`句の表示と、Brokerで集計したサービスごとの経過したロード時間の表示を制御します。チェックボックスをオンにすると、デバッグ情報が表示されます。デフォルト値は**オフ**(チェックの外れた状態) です。
値の自動ロード	このオプションは、[ナビゲート]ビューで選択したサービスの値の自動ロードを制御します。チェックボックスをオンにすると、調査するサービスを選択したときに、値が自動的にロードされます。チェックボックスをオフにすると、[**値のロード**]ボタンが表示されます。値をロードする前に、オプションを変更することができます。デフォルト値は**オフ**です。
完了したPCAPのダウンロード	この設定は、調査で抽出されたPCAPのダウンロードを自動化します。これにより、PCAPファイルをダウンロードし、PCAPフォームのデータを処理できるアプリケーション(Wiresharkなど) で抽出して開く操作を手動で実行する必要がなくなります。チェックボックスをオンにすると、オプションが有効になります。デフォルト設定は無効(チェックボックスはオフ) です。
Live Connect: リスクのある値を強調表示	このオプションのチェックボックスをオフにすると、Live Connectで使用可能なコンテキストを持つすべてのメタ値が、[ナビゲート]ビューの[値]パネルでハイライト表示されます。チェックボックスをオンにすると、Live Connectでコンテキストを持つ値のうち、コミュニティによってリスクが高い/不審である/安全でないと判断された値のみが強調表示されます。デフォルトでこのオプションは無効(チェックボックスはオフ) になっています。
適用	設定をただちに適用します。設定は、次回に値をロードしたときに表示されます。また、同じ変更が、[プロファイル]ビューにも適用されます。
キャンセル	編集操作をキャンセルし、設定を変更せずにダイアログを閉じます。

[レガシー イベント]ビューの[設定]ダイアログ

次の図は[レガシー イベント]ビューの[設定]ダイアログの例です。また、その機能について表で説明します。

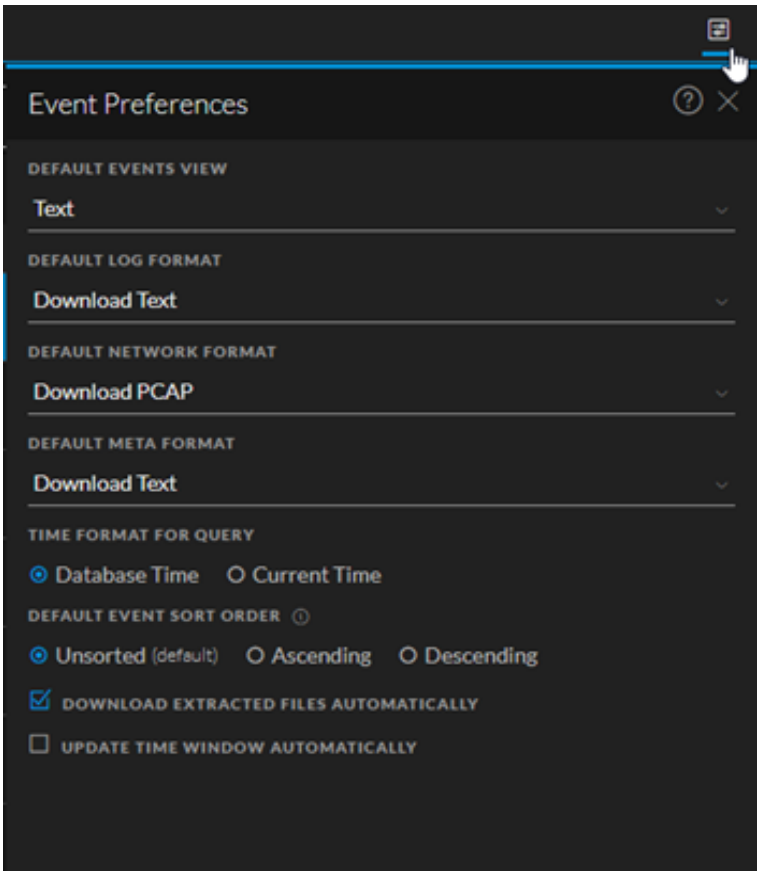


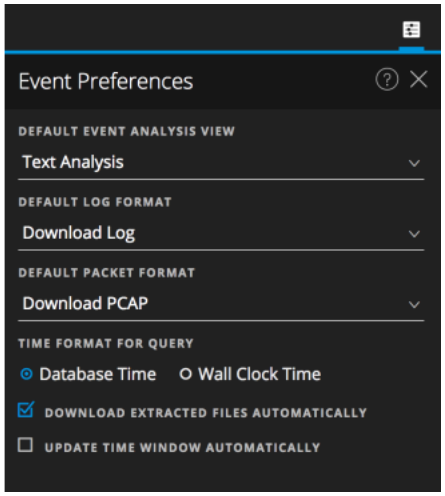
機能	説明
ログのエクスポート形式	エクスポートされたログのファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト**: RAWログ形式。 • **SML**: 構造化マークアップ言語形式。 • **CSV**: カンマ区切り値(CSV) 形式。 • **JSON**: JavaScript Object Notation(JSON) 形式。
メタのエクスポート形式	エクスポートされたメタ値のファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト**: RAWログ形式。 • **SML**: 構造化マークアップ言語形式。 • **CSV**: カンマ区切り値(CSV) 形式。 • **JSON**: JavaScript Object Notation(JSON) 形式。
完了したPCAPのダウンロード	この設定は、調査で抽出されたPCAPのダウンロードを自動化します。これにより、PCAPファイルをダウンロードし、PCAPフォームのデータを処理できるアプリケーション(Wiresharkなど) で抽出して開く操作を手動で実行する必要がなくなります。
Live Connect: リスクのある値を強調表示	チェックボックスをオンにすると、フィルタを使用して、RSAコミュニティによってリスクが高いとみなされているIPアドレスのみがフェッチされます。チェックボックスをオフにすると、NetWitness Platformによってすべてのアドレスが表示されます。デフォルトでこのオプションは無効(チェックボックスはオフ) になっています。

機能	説明
調査ページのロードを最適化	ページング オプションを設定します。最適化した場合、イベント リストで可能な限り速く結果が返されますが、イベント リストのページ移動機能が無効になります。このチェックボックスをオフにすると、イベント リストのページ移動機能が有効になり、リストの特定のページ(または最後のページ)に移動できるようになります。デフォルト値は有効(チェックボックスはオン)です。
イベント パネルのイベントを挿入モードで表示	このオプションは、[レガシー イベント]パネルのページングに影響し、以前のリリースでは[ナビゲート]ビューの[設定]ダイアログにありました。チェックボックスをオンにすると、次のイベント グループがすでに表示されているイベントに追加されます。チェックボックスをオフにすると、前のイベントのページが次のページに置き換えられます。デフォルト値はオフ(チェックの外れた状態)です。
デフォルト セッション表示	[イベント]ビューでのデフォルトの再構築のタイプを選択します。デフォルト値は[**最適な表示**]で、イベントに最も適した表示方法でイベントが表示されます。
WebビューのCSS再構築を有効化	この設定では、Webコンテンツの再構築の実行方法が制御されます。有効化すると、Webの再構築にカスケード スタイル シート(CSS)とイメージが含まれるようになり、再構築の表示と元のWebブラウザの表示が一致するようになります。これには、イベントに関連するスキャニングと再構築、ターゲット イベントで使用されるスタイル シートとイメージの検索が含まれます。このオプションは、デフォルトで有効化されています。特定のWebサイトの表示に問題がある場合は、チェックボックスをオフにしてこのオプションを無効化してください。
適用	設定をただちに適用します。この設定は、次回にイベントを表示したときに示されます。また、同じ変更が、[プロファイル]ビューにも適用されます。
キャンセル	編集操作をキャンセルし、設定を変更せずにダイアログを閉じます。

[イベント]ビューの[環境設定]ダイアログ

バージョン11.1から、[イベント]ビューにユーザ環境設定が追加されました。この環境設定は、[イベント]ビュー>[イベント環境設定]ダイアログで設定できます。これらの設定は保持されるため、ログインして[イベント]ビューに移動するたびに適用されます。次の図は、バージョン11.3とバージョン11.4.1のダイアログの例です。次の表に、オプションの説明を示します。





機能	説明
デフォルトの[イベント]ビュー	[イベント]ビューを開くたびに表示されるデフォルトのイベント分析ビューを選択します。たとえば[ファイル]を選択すると、[イベント]ビューでイベントを調査するたびに[ファイル分析]パネルがハイライト表示されます。次にオプションを示します。 • **テキスト**:イベントのRAWテキスト ペイロードを表示および分析します。 • **パケット**:イベントのパケットとペイロードを表示し、対話形式で分析します。 • **ファイル**:イベントのファイルのリストを表示し、1つまたは複数のファイルをダウンロードします。
デフォルトのログ形式	ログをダウンロードする際のデフォルトの形式を選択します。 • **ログのダウンロード**または**テキストのダウンロード**:RAWログ(ログ)形式。 • **CSVのダウンロード**:カンマ区切り値(CSV)形式。 • **XMLのダウンロード**:拡張可能マークアップ言語(XML)形式。 • **JSONのダウンロード**:JavaScript Object Notation(JSON)形式。

機能	説明
デフォルトのパケット形式またはデフォルトのネットワーク形式	パケットをダウンロードする際のデフォルトの形式を選択します。 • **PCAPのダウンロード**：イベント全体をパケット キャプチャ(*.pcap) ファイルとしてダウンロードします。 • **すべてのペイロードのダウンロード**または**ペイロードのダウンロード**：ペイロードを*.payloadファイルとしてダウンロードします。 • **リクエスト ペイロードのダウンロード**：リクエスト ペイロードを*.payload1ファイルとしてダウンロードします。 • **レスポンス ペイロードのダウンロード**：レスポンス ペイロードを*.payload2ファイルとしてダウンロードします。
デフォルトのメタ形式	メタデータをダウンロードする際のデフォルトの形式を選択します。 • **CSVのダウンロード**：カンマ区切り値(CSV) 形式。 • **JSONのダウンロード**：JavaScript Object Notation(JSON) 形式。 • **テキストのダウンロード**：プレーン テキスト形式。 • **TSVのダウンロード**：タブ区切り値(TSV) 形式。
クエリの時間形式	[イベント]ビューには、データベースの時間または現在の時間に基づいて結果を表示できます。この環境設定のデフォルト設定は[データベースの時間]です。これは[ナビゲート]ビューと[イベント]ビューでクエリ結果を表示するために使用される時間形式と同じです。 [**データベース時間**]を選択した場合、クエリの開始時刻と終了時刻は、イベントが収集された時刻(収集時間) に基づく時刻になります。 [**現在の時間(Current Time)**](バージョン11.3以前では[**現在の時間(Wall Clock Time)**]) を選択した場合、クエリの実行に使用される終了時刻は現在のブラウザの時刻に基づく時刻になり、開始時刻は終了時刻と時間範囲に基づいて計算されます。
イベントのソート順(バージョン11.4以降)	[イベント]パネルに表示されているイベントの収集時間に基づいて、ソート順を設定します。結果がイベント数の上限を超えている場合、すべてのイベントをロードすることはできません。結果として返されて[イベント]パネルにロードされるイベントの一部は、ソート順の設定と一致しています。つまり、イベントの最も古い部分は、昇順が選択されているときにロードされ、イベントの最も新しい部分は、降順が選択されているときにロードされます。この設定の変更は、次回のクエリ送信時に有効になります。 **ソートなし**：バージョン11.4.1のデフォルトのソート方法。Coreサービスによって処理されたとおりにイベントを一覧表示します。[ソートしない]は、すべてのコアサービスの応答を待ってから選択された順序で結果を表示するのではなく、一致が見つかり次第イベントを戻すため、処理がより高速です。 **昇順**：バージョン11.4のデフォルトのソート方法。収集時間が最も古いイベントをリストの最初に配置します。 **降順**：収集時間が最も新しいイベントをリストの最初に配置します。ログを調査するにあたり、ソート順を「最も新しい収集時間が最初」に変更する必要が生じることがあります。

機能	説明
抽出したファイルを自動ダウンロード	[イベント環境設定]ダイアログの[**デフォルトのログ形式**]フィールドと[**デフォルトのパケット形式**]フィールドで選択したデフォルト形式のファイルの自動ダウンロードを有効にします。 選択した形式のファイルをローカル ファイル システムに自動的にダウンロードするには、このチェックボックスを選択します。このチェック ボックスを選択しない場合、ダウンロード ジョブがジョブ キューに入れられるのでファイルを手動でダウンロードできます。
タイム ウィンドウを自動的に更新	(バージョン11.3以降) サービスがポーリング(1分間隔) されたときのクエリ バーの時間範囲ウィンドウの自動更新を有効にして、最新の結果が送信されるようにします。デフォルト設定はdisabledです。 チェックボックスをオンにすると、時間範囲が更新されたときに、  (クエリの送信) ボタンがアクティブになり、クリックして最新の結果を取得できるようになります。 チェックボックスをオフにすると、自動更新は無効になり、階層リンクの時間範囲ウィンドウが現在の結果と同期を維持します。