



RSA[®] NetWitness

Version 11.7

NetWitness Investigate ユーザガイド



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 Conferenceのロゴ、RSA、その他の商標は、RSA Security LLCまたはその関連会社(「RSA」)の商標です。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。その他の商標は、各社の商標または登録商標です。

使用許諾契約

本ソフトウェアと関連ドキュメントは、RSA Security LLCまたはその関連会社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

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

本文書に記載される、RSA Security LLCまたはその関連会社(「RSA」)のいかなるソフトウェアの使用、複製、配布にも、適切なソフトウェアライセンスが必要です。

RSAは、本文書に記載される情報が、発行日時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

本文書に記載される情報は、「現状有姿」の条件で提供されています。RSAでは、本文書に記載される情報に関するいかなる内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示的保証は提供しません。

© 2020 RSA Security LLC or its affiliates.All Rights Reserved.

12月 2021

目次

NetWitness Investigateの仕組み	14
メタデータ、メタ キー、メタ値、メタ エンティティ	14
調査のトリガー	15
調査のワークフロー	15
メタデータ、クエリ、時間に焦点を当てた調査	21
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	23
NetWitness Investigate 調査]ビュー	23
[ナビゲート]ビュー	23
[イベント]ビュー	24
[レガシー イベント]ビュー	26
イベントのコンテキスト情報	27
再構築とイベントの分析	29
NetWitnessの 調査]ビューおよび環境設定の構成	31
[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	32
一般的な設定の構成	32
[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	33
[ナビゲート]ビューでの値のロード パラメータの調整	35
[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	36
デフォルトのログ エクスポート形式の構成	37
デフォルトのメタ値エクスポート形式の構成	37
[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	37
Webコンテンツ再構築でのカスケードリング スタイルシート表示の有効化または無効化	38
検索オプションの構成	38
[イベント]ビューの構成	40
デフォルトの 調査]ビューの設定	40
[イベント]ビューのユーザ環境設定の設定	41
調査の開始	45
メタデータ、RAWイベント、イベント分析にフォーカス	45
ホストとファイルにフォーカス	46
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	46
ファイルのマルウェア スキャンにフォーカス	46
[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	47
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)	48
デフォルトのサービスの設定またはクリア	49
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)	50

調査するサービスまたはコレクションの変更	51
Workbenchのリストアコレクションの調査	52
[イベント]ビューでの調査の開始	54
[イベント]ビューへのアクセス	55
[イベント]ビューへのアクセス(バージョン11.0)	58
結果セットの絞り込み	59
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	60
Liveメタグループ	61
Default Meta Keysグループ(バージョン11.5の [イベント]ビュー)	63
カスタムメタグループ	63
[イベント]ビューでのメタグループの操作(バージョン11.5以降)	64
メタグループに含まれているメタキーの表示	64
メタグループの選択	67
カスタムメタグループの作成	68
カスタムメタグループの削除	71
カスタムメタグループの編集	72
メタグループのコピー(バージョン11.5以降)	75
メタグループフォルダ	78
メタグループフォルダの作成	79
メタグループフォルダの編集と移動	80
メタグループフォルダのコピー	80
メタグループのプライベートフォルダまたは共有フォルダのコピー	81
Liveから導入されたメタグループフォルダのコピー	82
メタグループフォルダの削除	84
[ナビゲート]ビューでのメタグループの操作	85
メタグループの作成とメタキーの追加	85
メタグループのコピーと編集	88
カスタムメタグループの編集	88
メタグループの削除	90
メタグループのエクスポート	90
メタグループのインポート	90
イベントリストでの列と列グループの使用	92
標準提供の列グループ	97
Live列グループ	97
カスタム列グループ	101
フォルダのフィルタ処理	102
列グループを管理するためのダイアログ	103
11.4以降の [イベント]ビューでの列と列グループの操作	104
手動での表示する列の選択と列の順序と幅の調整	104
[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(バージョン11.4)	105

列によるソート(バージョン11.4.1以降)	106
列によるソート(バージョン11.4)	108
列グループに含まれているメタキーの表示	109
列グループの選択	111
カスタムの列グループの作成	112
カスタム列グループの削除	116
カスタム列グループの編集	118
列グループのコピーの作成(バージョン11.5以降)	121
列グループフォルダの作成	124
列グループフォルダの編集と移動	125
列グループフォルダのコピー	125
Liveから導入されたグループフォルダのコピー	126
列グループフォルダの削除	127
列グループと列の選択(11.3以前の [イベント分析]ビュー)	128
[レガシー イベント]ビューでの列グループの操作	129
列グループの選択	129
[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	130
列グループの削除([レガシー イベント]ビュー)	133
列グループの編集([イベント]ビュー)	134
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)	137
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	139
標準提供クエリプロファイル	139
Liveクエリプロファイル	140
カスタムクエリプロファイル	140
クエリプロファイルを管理するためのダイアログ	141
クエリプロファイルの詳細の表示([イベント]ビュー)	143
クエリプロファイルの適用([イベント]ビュー)	145
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)	146
カスタムクエリプロファイルの削除([イベント]ビュー)	151
クエリプロファイルのコピー(バージョン11.5以降)	154
クエリプロファイルフォルダの作成	156
クエリプロファイルフォルダの編集と移動	156
クエリプロファイルフォルダのコピー	157
Liveから導入されたクエリプロファイルグループフォルダのコピー	158
クエリプロファイルフォルダの削除	158
[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)	159
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)	160
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)	162
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)	163
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)	163

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)	164
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)	164
[イベント]ビューでのメタデータのドリルダウン(ベータ版)	165
動作モード	166
[イベントの絞り込み]パネルでメタデータを表示する	167
メタ グループの最大値を表示する	169
[イベントの絞り込み]パネルで [コンテキスト ルックアップ]パネルを表示する	170
表示可能なメタデータについて	171
メタ データのロードを停止して再開する	172
1つのメタ キーを除くすべてのメタ キーを閉じる(バージョン11.5.1以降)	173
メタ値の並べ替え方法を設定する	174
メタ値をドリルダウンする	176
メタ キーのメタ値をコピーする	178
選択したメタ値をRSA Liveで表示する	180
メタ値の調査を再フォーカスする	180
[イベント]ビューでの結果のフィルタリング	183
クエリバーを使用した初期フィルタ	183
[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)	184
[イベント]パネルでの結果の絞り込み	185
クエリビルダの概念	186
ガイド モードとフリーフォーム モード	187
複数のフィルタの編集に関する概念	188
バージョン11.3以前のクエリビルダ	190
バージョン11.4のクエリビルダ	190
メタ キーのキャッシュによるロードの高速化	191
テキスト フィルタ	191
テキストを手入力する代わりにペースト	191
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)	191
最近のクエリの使用	191
高度な演算子の使用	192
AND/OR演算子の使いやすさ	192
括弧の不均衡の自動修正	193
使用可能な値に関するヒント	193
CIDR表記と略記	193
値の範囲またはリスト	193
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)	194
時間範囲を選択	194
クエリの送信	195
クエリの実行のキャンセル	196
クエリのステータスの表示	196

ガイド モードでのクエリの作成	198
ガイド モードで使用するキーボード操作	199
ガイド モードでの視覚的なフィードバック	201
ガイド モードでのシンプルなフィルタの追加	204
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)	209
データ セット内の任意の場所で値を検索するためのテキスト フィルタの追加(バージョン11.4以降)	210
クエリ バーで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)	213
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)	213
最近のクエリに基づくフィルタの挿入(バージョン11.4以降)	215
ガイド モードでのフィルタの編集	216
ガイド モードで選択したフィルタを使用したクエリ	217
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	218
フリーフォーム モードでのクエリの作成	219
[クビゲート]ビューでの結果のフィルタリング	221
時間範囲の設定	221
メタ キー結果の集計方法とソート順の設定	223
Investigationでのデフォルト メタ キーの管理と適用	224
[クビゲート]ビューのタイム チャートでのデータのドリル ダウン	226
[値]パネルでのデータのドリルダウン	227
[レガシー イベント]ビューでの結果のフィルタリング	235
[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	235
[レガシー イベント]ビューでのイベントのページ移動	236
[クビゲート]ビューと [レガシー イベント]ビューでのクエリの作成	237
基本的な方法を使用したクエリの作成	237
高度な方法を使用したクエリの作成	238
最近実行したクエリの適用	240
[クビゲート]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	242
キーワード テキスト検索	242
検索の動作を制御するオプション	243
正規表現検索の構文	245
Rawテキスト キーワード検索	245
検索手順	245
[クビゲート]ビューでの検索	245
[レガシー イベント]ビューでの検索	245
URL統合を使用したクエリの表示と変更	246
サービスIDが分かる場合	246
ホストとポート番号がわかる場合	246
例	247
追加の注意事項	247

イベントの再構築と分析	248
[イベント]ビューでのイベント詳細の調査	251
各イベントタイプのイベントの詳細	251
テキストの再構築	252
パケットの再構築	257
ファイルの再構築	259
ホスト情報	260
メールの再構築	263
[イベント]ビューでのイベントの分析	266
結果のロードとソートの方法	266
イベントリストを絞り込むためのアクション	267
イベントを分析するためのアクション	268
[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	268
イベントの分析タイプの選択	269
リクエストとレスポンスの表示を調整する	269
イベントの関連メタデータを表示する	270
イベントヘッダーを表示または非表示にする	273
[パケット]および [テキスト]タブでのイベントのページ移動	274
[テキスト]タブ内のトランケートされたテキストエントリーの展開	275
URLとBase64のエンコーディングおよびデコーディングの [テキスト]タブでの実行	275
HTTPネットワークセッションの解凍テキストの [テキスト]タブでの表示	277
ツリー形式のJSON文字列の [テキスト]タブでの表示(バージョン11.5.1)	279
[パイロードのみ]オプションの [パケット]タブでの使用	280
[パケット]タブでのバイトのハイライト表示	281
一般的なファイルタイプの [パケット]タブでのハイライト表示	283
[レガシー イベント]ビューでのイベントの再構築	285
イベントIDを使用したイベントの再構築	285
[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	286
セッションを左右/上下に並べて表示	288
表示するイベント情報の選択	288
イベントの再構築のタイプの選択	288
メールの添付ファイルの表示またはダウンロード	289
イベントをPCAPファイルとしてエクスポート	289
再構築されたイベントからのファイルの抽出	290
結果の追加のコンテキストを検索	291
[コンテキスト ルックアップ]パネルを開く	292
ホワイトリストへのエンティティの追加	295
リストの作成([イベント]ビュー)	296
[調査] > [ナビゲート]への移行([イベント]ビュー)	296
Archerへの移行([イベント]ビュー)	297

NetWitness Endpoint Thick Clientへの移行([イベント]ビュー)	297
[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	298
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)	298
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)	299
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)	299
メタ キーのルックアップの起動	301
[イベント]ビューでのEndpoint Thick Clientルックアップの起動	301
[ナビゲート]ビューでのEndpoint Thick Clientルックアップの起動	302
イベントでのメタ値のルックアップの実行	304
[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	306
[ナビゲート]ビューからのMalware Analysisスキャンの起動	308
[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	310
ネットワーク セッションの分割	311
セッション サイズと時間の分割	311
トランザクション処理の分割	312
セッション フラグメントの強調表示	313
関連ネットワーク セッション	313
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	314
イベント リストでの関係の表示と非表示	315
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)	316
[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	318
メタデータを座標表示チャートに追加する	320
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	320
座標表示で利用できるRSAメタ グループ	320
座標表示チャートの表示	321
座標表示チャートで使用するメタ キーの選択	322
座標表示チャートの最適化	327
使用例	329
大量データセットのチャートの例	330
ドリルダウン ポイントのInformerでのビジュアル表示	332
結果のダウンロードと処理	333
[イベント]ビューでのデータのダウンロード	334
イベントまたはメタデータの [イベント]パネルでのダウンロード	334
テキスト再構築でのログのダウンロード	337
テキスト再構築またはパケット再構築でのネットワーク イベント データのダウンロード	339
ファイル再構築でのネットワーク イベントからのファイルのダウンロード	340
メール再構築からの添付ファイルのダウンロード	342
[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	346
[レガシー イベント]ビューでのイベントのエクスポート	348
[イベント]ビューでのインシデントへのイベントの追加	349

[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	351
NetWitness Investigateのトラブルシューティング	353
[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	353
[イベント]ビューの問題	354
調査の参考情報	360
[イベントをインシデントに追加]ダイアログ	361
ワークフロー	361
実行したいことは何ですか?	361
関連トピック	362
簡単な説明	363
[リストへの追加/削除]ダイアログ	366
ワークフロー	366
実行したいことは何ですか?	367
関連トピック	368
[イベント]ビューの簡単な説明	368
[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	370
[列グループ]ダイアログ	372
関連トピック	373
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	373
簡単な説明 - [列グループの管理]ダイアログ	377
[コンテキスト ルックアップ]パネル	379
ワークフロー	379
実行したいことは何ですか?	379
関連トピック	380
([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	381
インシデント	382
アラート	382
リスト	383
エンドポイント	383
[イベント]ビューの簡単な説明(バージョン11.2以降)	383
[リスト]タブ	386
[Archer]タブ	387
[Active Directory]タブ	388
[NetWitness Endpoint]タブ	389
[アラート]タブ	391
[インシデント]タブ	392
[Live Connect]タブ	394
[ファイルレピュテーション]タブ	399
[↑I]タブ	400

[REST API] タブ	401
[インシデントの作成] ダイアログ	402
ワークフロー	402
実行したいことは何ですか?	402
関連トピック	403
簡単な説明	403
[イベント] ビュー	405
ワークフロー	405
実行したいことは何ですか?	405
関連トピック	406
簡単な説明	407
[イベントの絞り込み] パネル	410
クエリコンソール	411
タイムライン	413
バージョン11.0.0.x(生産終了)の簡単な説明	414
[イベント] ビュー - [メール] タブ	416
ワークフロー	416
関連トピック	416
簡単な説明	416
[イベント] ビュー - [ファイル] タブ	418
ワークフロー	418
実行したいことは何ですか?	418
関連トピック	419
簡単な説明	419
[イベント] ビュー - [ホスト] タブ	421
ワークフロー	421
実行したいことは何ですか?	421
関連トピック	422
簡単な説明	422
[イベント] ビュー - [パケット] タブ	424
ワークフロー	424
実行したいことは何ですか?	424
関連トピック	425
簡単な説明	425
[イベント] ビュー - [テキスト] タブ	428
ワークフロー	428
実行したいことは何ですか?	428
関連トピック	429
簡単な説明	430
調査] ダイアログ	432

ワークフロー	432
実行したいことは何ですか?	432
関連トピック	433
簡単な説明	434
調査]タブ - [ユーザー環境設定]パネル	436
関連トピック	436
簡単な説明	436
調査]ビュー	440
[レガシー イベントの再構築]ビュー	441
実行したいことは何ですか?	441
関連トピック	442
簡単な説明	442
[レガシー イベント]ビュー	445
実行したいことは何ですか?	445
関連トピック	446
簡単な説明	446
詳細説明	449
デフォルトのメタ キーの管理]ダイアログ	452
関連トピック	452
簡単な説明	452
[メタグループ]ダイアログ	454
関連トピック	454
簡単な説明 - [メタグループ]メニュー、[メタグループの作成]ダイアログ、[メタグループの詳細] ダイアログ	454
簡単な説明 - [メタグループの管理]ダイアログ	457
[ヒビゲート]ビュー	460
ワークフロー	460
実行したいことは何ですか?	461
関連トピック	462
簡単な説明	462
ツールバー	463
一時停止/再ロード ボタンと階層リンク	466
(オプション) デバッグ情報	467
時間バナー	467
ビジュアル画像	467
タイムライン チャート	467
座標表示チャート	469
値パネル	471
[値]パネルのロード動作	472
反復的結果	473

部分的結果	473
デバッグ情報	473
ロード完了	474
クエリ]ダイアログ	475
実行したいことは何ですか?	475
関連トピック	476
簡単な説明	476
[サンプル]ビュー	477
[詳細]ビュー	477
[最近実行したクエリ]ビュー	478
クエリプロファイル]ダイアログ	480
関連トピック	480
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	481
簡単な説明 - [プロファイルの管理]ダイアログ	483
調査]ビューの設定ダイアログ	486
関連トピック	486
簡単な説明	486
[サビゲート]ビューの [設定]ダイアログ	487
[レガシー イベント]ビューの [設定]ダイアログ	488
[イベント]ビューの [環境設定]ダイアログ	490

NetWitness Investigateの仕組み

NetWitness Investigateは、NetWitnessによって収集されたイベントを分析する手段をアナリストに提供します。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、環境内の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。アナリストは複数のビューを使用して、環境内のデータをさまざまな視点から把握できます。すべてのビューに共通する重要な要素は、メタ データです。

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は、環境内のすべてのデータ通信を監査および監視します。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に、メタ データを作成します。もう1つのタイプのサービスは、Concentratorと呼ばれ、メタデータのインデックスを作成して格納し、あらゆるタイプのメタデータを効率的に検索できるようにします。

メタデータは、元のデータに含まれる重要な参照ポイントをアナリストに提供するために作成されます。これによりアナリストは、イベントの詳細をすべて調べなくても、何が発生したかをすばやく把握できるようになります。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(192.168.1.1)は、`ip.src`がタグ付けされたメタ値です。[調査]ビュー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(メタ値)が表示されます。標準提供のメタ キーもあれば、管理者が定義した環境固有のカスタム キーもあります。データの提供元に関係なく、すべてのメタデータはRSA NetWitness Platformの統合 データ モデルに正規化され、同様のメタデータの概念が同様のメタ キーにグループ化されます (<https://community.rsa.com/community/products/netwitness/rsa-content/udm>を参照)。

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。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。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、クエリ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、メタ エンティティを使用して、ユーザ ロールとユーザに適用するクエリプレフィックスを定義できます(『システム セキュリティとユーザ管理ガイド』を参照)。「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。

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、RAWログまたはエンドポイント イベント、あるいはネットワーク イベントの完全な再構築が必要な場合にのみDecoderが使用されます。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。

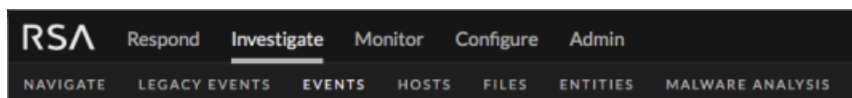
調査のトリガー

調査のトリガーの例をいくつか示します。

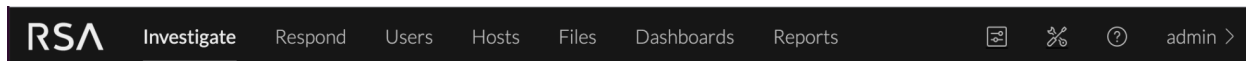
- 新しいActive Directoryハッキングに関するインテリジェンス情報が送られてきます。[イベント]ビューを開き、そのインテリジェンス情報を使用して、Active Directoryの過去24時間のすべてのRAWログデータに対して検索を実行します。
- SOCマネージャーから、話題になっているPokemon Goマルウェアを検索するように依頼されます。[ナビゲート]ビューを開き、SOCマネージャーがセキュリティブログで見つけたマルウェアに関連する特定のユーザエージェントを使用したHTTPセッションを検索するクエリを作成します。
- インシデント対応者が、特定のホストに関連したいくつか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(または[イベント]ビューの[イベントの絞り込み]パネル)を開き、ネットワークメタデータのドリルダウンを開始し、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ーアカウント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。[ユーザ]ビューを開き、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づけられています。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、[ファイル]ビュー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によって収集されたデータを調査し、NetWitnessダッシュボード上の情報、スプリングボード(バージョン11.5以降)、NetWitness Respondのインシデントまたはアラート、NetWitness 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、アナリストはさまざまなビュー([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、[ユーザ(エンティティ)]ビュー、[Malware Analysis]ビュー)をシームレスに移動することができます。デフォルトでは、[ナビゲート]ビューと[レガシー イベント]ビューは無効になっています。次の図は、バージョン11.4以前のNetWitness Investigateサブメニューを示しています。



次の図は、[ユーザ]、[ホスト]、[ファイル]が最上位メニューに移動し、アナリストのワークフローに最適化された、バージョン11.5の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。11.5より前のバージョンでは、[調査]ビューのサブメニューでした。
- [ユーザ]ビューはバージョン11.2以降で使用できます。バージョン11.4では、[エンティティ]ビューという名前でした。11.5より前のバージョンでは、[調査]ビューのサブメニューでした。
- [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。
- バージョン11.6では、[イベント]ビューの [イベントの絞り込み] パネルがこの機能を提供するため、デフォルトでは [ナビゲート]ビューは無効になっています。[ナビゲート]ビューを有効にするには、「[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。
- ユーザがNetWitnessを使用して調査やマルウェアの解析を実施するには、特定のユーザ ロールおよび権限が必要です。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。

1つのビューから別のビューに移動する必要を減らすため、ビューは緊密に統合されています。調査の開始場所はユースケースごとに決まりますが、見つけようとしている情報の種類に応じて状況は変化します。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。経験豊富なアナリストは、[ナビゲート]ビューまたは [イベント]ビューで調査を開始する傾向があります。経験の浅いアナリストは、ダッシュボード、[対応]ビュー、またはスプリングボード(バージョン11.5以降)から開始できます。これらのビューでは、インシデントとアラートのリンクをクリックして、別のビューに詳細情報と分析を表示できます。

開始場所	調査の焦点
[ナビゲート]ビュー	[ナビゲート]ビュー(バージョン11.5以前)には、ログ、エンドポイント、およびネットワークイベントのメタキーとメタ値が表示されるため、特定の時間範囲に環境で起こったことの概要を把握するのに適しています。メタ値をドリルダウンした後、[イベント]ビューに移動してRAWイベントを確認します(「 [ナビゲート]ビューでの結果のフィルタリング 」を参照)。

開始場所	調査の焦点
[イベント]ビュー	<p>[イベント]ビュー (デフォルトの [調査]ビュー) は、アナリストがイベントをインタラクティブに操作するためのワークフローであり、隣接するパネルに同じデータのさまざまな側面を表示します。バージョン11.6では、[イベント]ビューの [イベントの絞り込み] パネルがこの機能を提供するため、メタ値をドリルダウンするために [ナビゲート]ビューに移動する必要はありません。</p> <p>(「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)。</p>

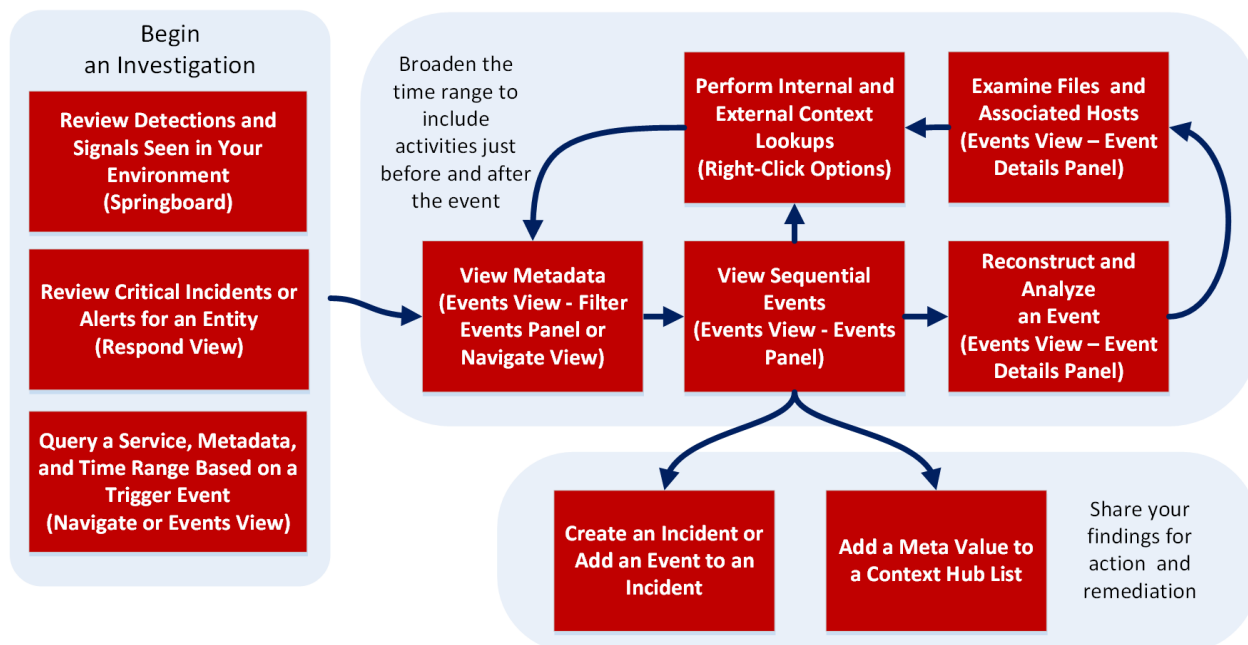
開始場所	調査の焦点
[レガシー イベント]ビュー	<p>[レガシー イベント]ビューは、バージョン 11.0～11.3.x.x では、イベントの詳細を確認するワークフローでした。[レガシー イベント]ビューは、11.4以降は [イベント]ビューに置き換えられ、管理者が有効にしない限り非表示になります。</p> <p>(「結果セットの絞り込み」、「イベントの再構築と分析」、「結果のダウンロードと処理」を参照してください)。</p>
[ホスト]ビュー	<p>[ホスト]ビューは、バージョン 11.5でメインメニューに移動しました。</p> <p>NetWitness Endpointエージェントが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。</p> <p>(『<i>NetWitness Endpoint ユーザガイド</i>』を参照。)</p>

開始場所	調査の焦点
[ファイル]ビュー	<p>[ファイル]ビューは、バージョン11.5でメインメニューに移動しました。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。 (『<i>NetWitness Endpoint</i> ユーザガイド』を参照。)</p>
[マルウェア分析]ビュー	<p>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、コミュニティー、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。 (『<i>Malware Analysis</i> ユーザガイド』を参照してください。)</p>

開始場所	調査の焦点
[ユーザ]ビュー	<p>[ユーザ]ビュー (バージョン11.4では [エンティティ]ビュー) は、バージョン11.5でメインメニューに移動しました。このビューでは、NetWitness UEBAを使用して、エンタープライズ全体で危険な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)。</p>

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、NetWitness 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。

1. 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、フィルタリングされたイベントの1つ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。標準提供のクエリプロファイル、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クエリプロファイルを選択すると、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。
2. イベントを詳しく確認する場合は、その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、イベントを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、別のクエリを実行できます。つまり、再度ワークフローの先頭から開始します。
3. 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します。
4. 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、ファイルに対して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表示されたサービスのスキャンを開始します。

簡単なユースケースは次のとおりです。特定の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、次のメタ値から開始します。Upload without change request followed by download alert. 始めに [ナビゲート] ビューまたは [イベント] ビューで、アラートが生成された時間範囲のデータを、特定のIPアドレスの値で絞り込みます。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るため、別のメタ値をクリックして、イベントリストを絞り込んだ後で、イベントを再構築できます。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ある下線付きのエンティティにカーソルを合わせて、調査]への移行アクションを選択します。[イベント]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。定義済みのメタキーでクエリが実行され、収集されたパケット、ログ、エンドポイント イベントが [イベント]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します。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。
- 対応] > [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、およびこれらのビューで使用できるコンテキスト情報、イベントの詳細、再構築について説明します。[マルウェア分析]ビューの機能については、『*Malware Analysis ユーザガイド*』を参照してください。

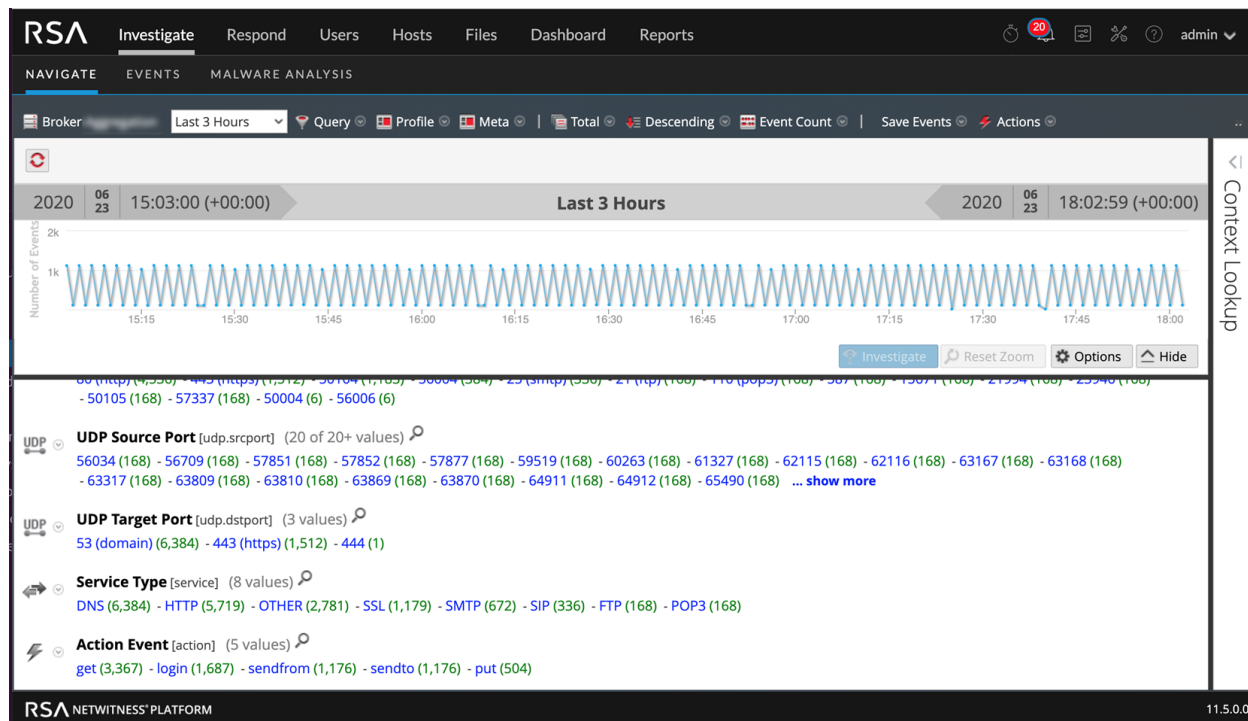
[ナビゲート]ビュー

注：バージョン11.6では、[イベント]ビューの [イベントの絞り込み] パネルがこの機能を提供するため、デフォルトで [ナビゲート]ビューは無効になっています。[ナビゲート]ビューを有効にするには、[「\[ナビゲート\]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。

[ナビゲート]ビューでは、Broker、Concentrator、Decoder上にあるネットワーク、ログ、エンドポイント イベントのメタデータをドリルダウンし、クエリを実行することができます(ただし、Decoderに対する調査は一般的ではありません)。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。[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。次の図は、[ナビゲート]ビューを示しています。

- リスト内の各メタキーには、それらの値を持つイベントの数に基づいて上位20個の値が表示されます。

- 値を連続して左クリックまたは右クリックしてメタ値をドリルダウンすると、クリックした各値が追加のフィルタとしてクエリに適用されます。ドリルダウンするに伴い、表示されるメタデータのサブセットは、適用したフィルタに基づいて小さくなります。たとえば、HTTP(service=80) のみを表示するようにフィルタリングした場合、表示される残りのメタデータはすべて、指定したHTTPイベント内に含まれるものになります。
- 結果を絞り込んで少なくしたら、[イベント]ビューに移動してイベントの詳細をさらに調べたり、NetWitness Platformの外で追加のルックアップを実行してさらに洞察を得ることができます。



[イベント]ビュー




[イベント]ビューでは、イベントのリストをシーケンシャルに表示し、RAWイベント データとメタデータを分析し、(バージョン11.5以降では) [ナビゲート]ビューと同様にメタデータをドリルダウンすることができます。

- [イベント]パネルには、ネットワーク イベント、エンドポイント イベント、ログ イベントのリストが時間順に表示されます。RAWイベントの表示、フィルタリング、ソート、検索、詳細と再構築の表示、イベントのダウンロードを行うことができます。イベントをクリックすると、そのイベントの [イベントの詳細]パネルが開きます。[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、Webなどのさまざまな再構築を表示できます。
- [イベント メタ]パネルで、[イベントの詳細]パネルで開いているイベントの関連メタデータを表示できます。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

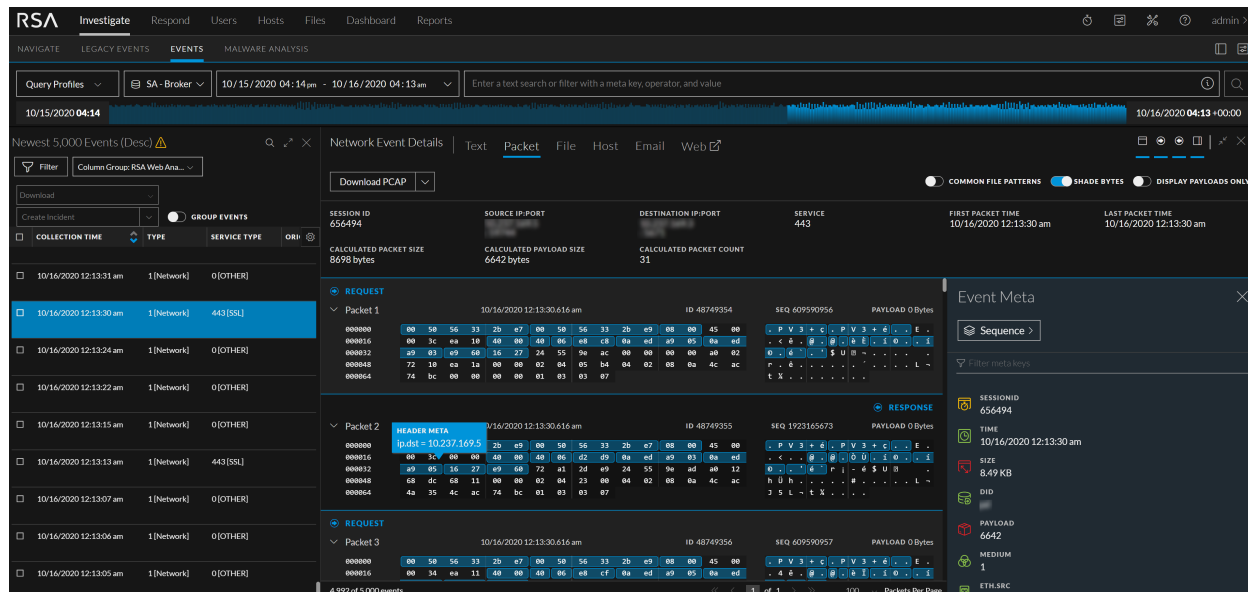
的確に追跡することができます。メタデータのリストは、出現した順やアルファベット順に並べ替えることができます。

- **【イベントの絞り込み】**パネル(バージョン11.5のベータ機能)では、リスト内のイベントのメタ値をドリルダウンして、結果を**【イベント】**パネルに反映できます。**【イベントの絞り込み】**パネルをブラウザの幅いっぱい展開表示すると、**【イベント】**パネルにイベントを表示する前に、メタ値をドリルダウンして特定の情報を探することができます(**【ナビゲート】**ビューでデータをドリルダウンする機能に相当)。(バージョン11.5.1) **【イベントの絞り込み】**パネルでは、メタ値の結果の閾値は100000です。結果が閾値を超えている場合は、~または>を使用して示されます。たとえば、「(>100000)」は、結果がカウントに基づいてソートされ、閾値よりも大きいことを示します。同様に、「(~100000)」は、結果がサイズに基づいてソートされ、閾値よりも大きいことを示します。
- **【イベントの詳細】**パネルでは、ネットワーク、ログ、またはエンドポイント イベントの詳細を表示し、元の形式に似た形式でイベントを安全に再構築できます。このパネルのタブは、**【テキスト】**、**【パケット】**、**【ファイル】**、**【ホスト】**、**【ユーザ】**、**【メール】**、**【Web】**です。
- **【イベント】**ビューのさまざまなポイントから、スタンドアロンEndpointに移行したり、Liveを検索したり、その他の内部ルックアップを実行したりできます。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。
- (バージョン11.5) ネットワーク イベントがEndpointの情報で拡充され、Endpointエージェントの拡張ネットワーク可視化が構成されている場合、ネットワーク イベントのホスト情報も、**【イベント】**ビューのヘッダーと**【ホスト】**タブに表示されます。

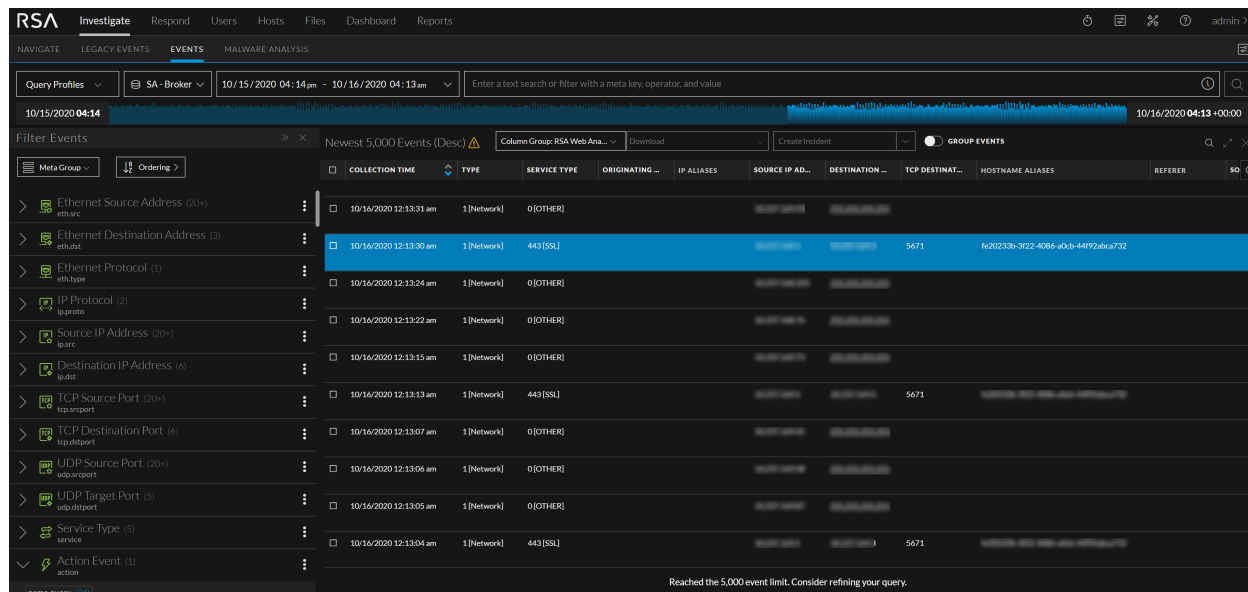
注：拡張ネットワーク可視化を使用する場合は、Endpoint Log DecoderのデータをEndpoint Concentratorで集計するために使用するサービス ユーザー アカウントに、decoder.manage権限が割り当てられている必要があります。ルールと権限を割り当てる方法の詳細については、『RSA NetWitness Platformホストおよびサービス スタート ガイド』の「サービスの **【セキュリティ】**ビュー - Aggregationルール」を参照してください。

- 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、Threat Intelligence、値が記載されたその他のソースが含まれます。
- さまざまなタイプのデータをエクスポートできます。**【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。メール再構築を表示している場合は、添付ファイルをダウンロードできます。テキスト再構築からログをダウンロードし、パケット再構築からパケットをエクスポートできます。**【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。
- (バージョン11.6) ダウンロード ジョブを表示するには、 をクリックします。**【レガシー イベント】**および**【ナビゲート】**ページの アイコンとは異なり、ジョブトレイは開きません。**【ジョブ】**ページが開き、すべてのジョブが一覧表示されます。ジョブトレイを表示するには、**【調査】** > **【ナビゲート】**(バージョン11.5以前) または **【調査】** > **【レガシー イベント】**(バージョン11.3以前) に移動して、 (ジョブ) アイコンをクリックします。

次の図は、[イベント]リストで選択されたネットワークイベントが中央のパネルで分析され、関連するメタデータが右側のパネルに表示された [イベント]ビューの例です。



次の図は、左側に [イベントの絞り込み] パネルが開いた [イベント]ビューを示しています。このビューでは、メタ値をドリルダウンして結果セットをフィルタリングします。



[レガシーイベント]ビュー

[レガシーイベント]ビューは、アナリストがRAWイベント データを調べるために使用する以前のユーザー インターフェイスでした(11.0~11.3.x.x)。[レガシー イベント]ビューはバージョン11.4では不要になり、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。[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。

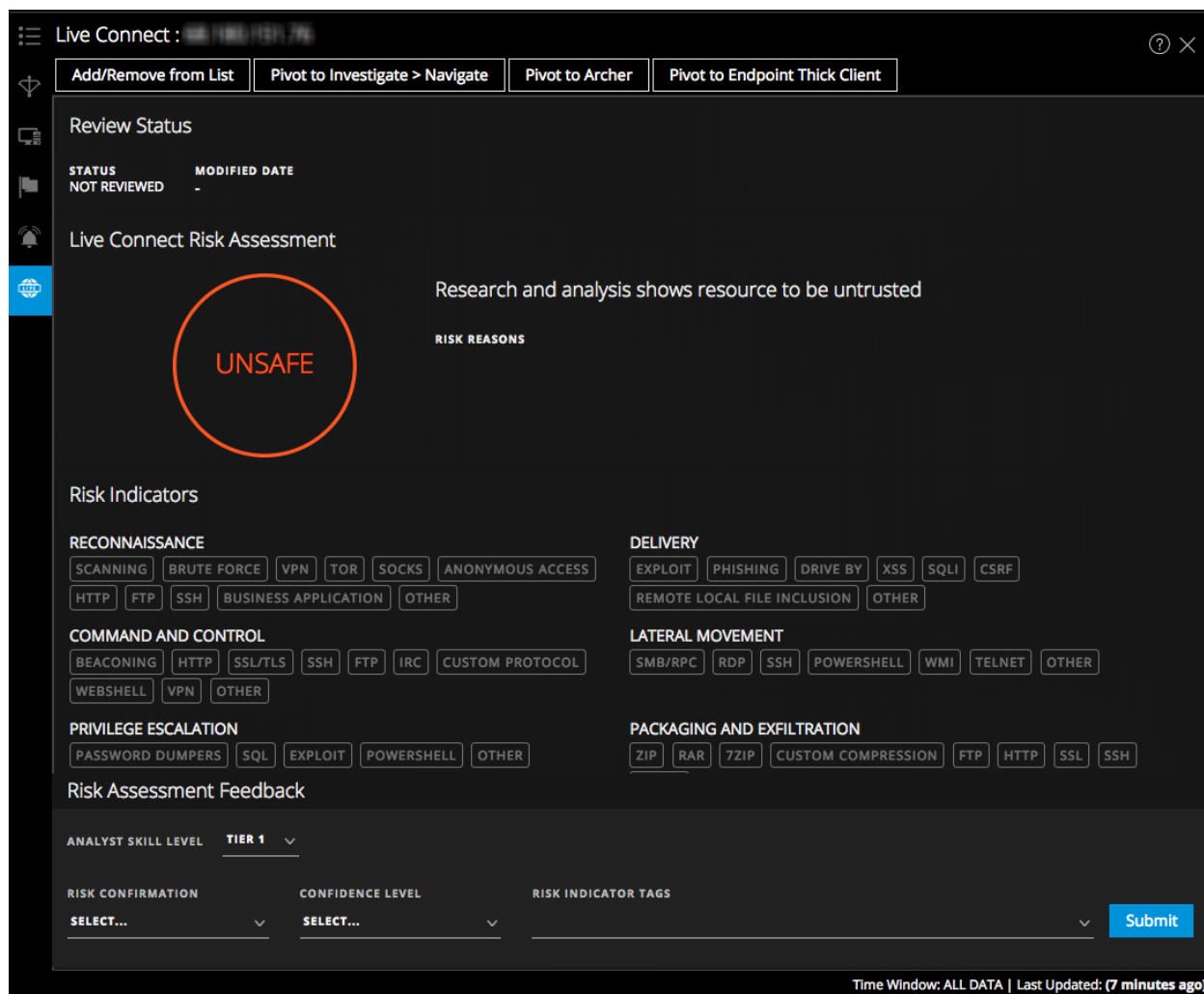
イベントのコンテキスト情報

[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。

イベントの要素をインタラクティブに操作して、関連するインシデント、アラート、カスタム リスト、Archer 資産、Active Directoryの詳細、NetWitness Endpoint IIOC、STIXデータ ソース(つまり、ファイル、TAXIIサーバ、RESTサーバ)などのより深い洞察を得ることができます(「[結果の追加のコンテキストを検索](#)」を参照)。

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 [イベント]パネルの右側に表示される [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 [イベント]リストの右側に表示される [コンテキスト ルックアップ]パネルを示しています。

The screenshot shows the 'Context Lookup' window for IP address 10.162.30.26. The interface includes a search bar, a sort dropdown set to 'Date - Newest to Oldest', and a refresh button. The alerts are listed as follows:

Severity	Alert Title	Created	Incident ID	Sources	Events
20	Alert without Incident	2019/03/05, 23:32 (0 days ago)		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:32 (0 days ago)	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:31 (0 days ago)		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:31 (0 days ago)	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:29 (0 days ago)		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:29 (0 days ago)	INC-698	Event Stream Analysis	1

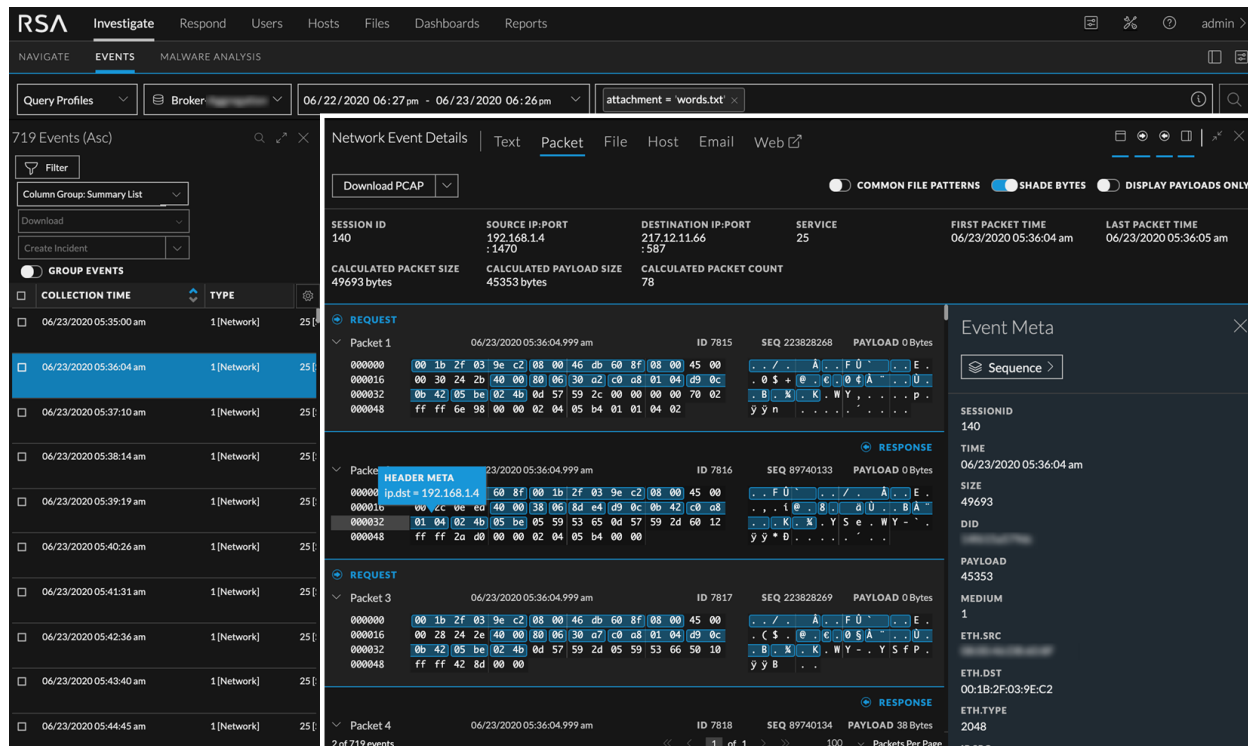
50 Alerts (First 50 Results)

再構築とイベントの分析

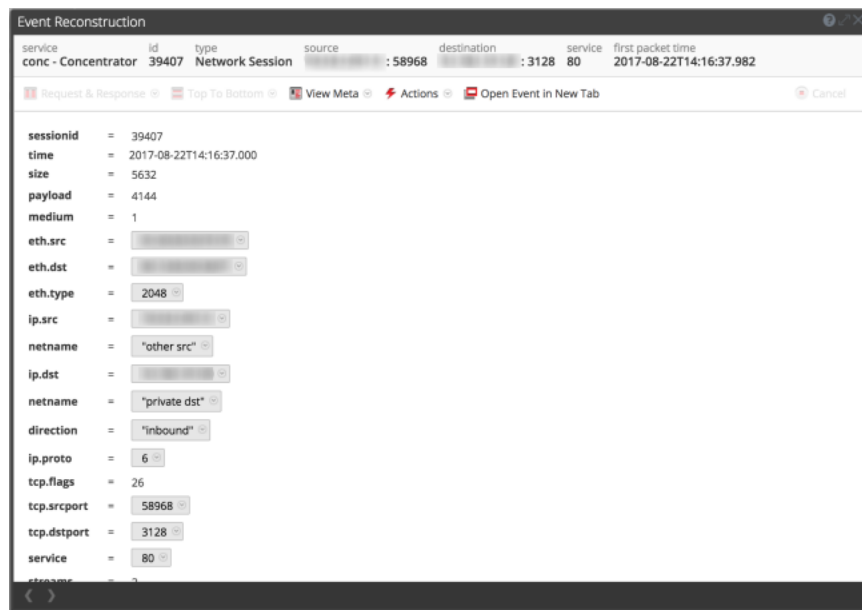
追加の調査に値するイベントを発見した場合は、そのイベントのコンテンツに最も適した形式で分析できます。分析の形式によっては、パケット、テキスト、メール、Webコンテンツなど、元の形式と同様の形式でイベントを安全に再構築します。イベントの表示中は、お使いのシステムやブラウザへの悪影響を制限するため、イベントに含まれる動的コードまたはアクティブコードの使用は制限されます。キャッシュを使用して、以前に表示されたイベントを表示するときのパフォーマンスを向上させることができます。各アナリストには再構築データ用に個別のキャッシュがあり、自身のキャッシュにある再構築イベントにのみアクセスできます。

Endpointが導入されており、Endpointエージェントに拡張ネットワーク可視化が構成されている場合は、一部のネットワークイベントにはホストデータが付加されます。このようなイベントでは、ホストの詳細を表示できます。

「イベント」ビューを使用すると、イベントをインタラクティブに分析して、RAWデータ、メタ キー、メタ値を調べることができます。次の図は、「イベント」ビューでパケットとして表示されているネットワークイベントの例です。



「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。



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内の次の2つの場所にあり、どちらの場所でも変更を行っても、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。
- **プロフィール** > **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。

デフォルトでは、従来の「ナビゲート」ビューは無効になっています。調査の「ナビゲート」タブを有効にするには、次の手順を実行します。



1. (管理) > **システム** > **調査** > **ナビゲート**に移動します。
2. **ナビゲートの有効化**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。

次の図は、従来の「ナビゲート」ビューを有効にできるページを示しています。

The screenshot shows the 'Investigation' settings page in NetWitness Investigate. The 'Enable Navigate' checkbox is checked and highlighted with a red box. Below it are 'Render Threads Setting' and 'Parallel Coordinates Settings' sections, each with an 'Apply' button.

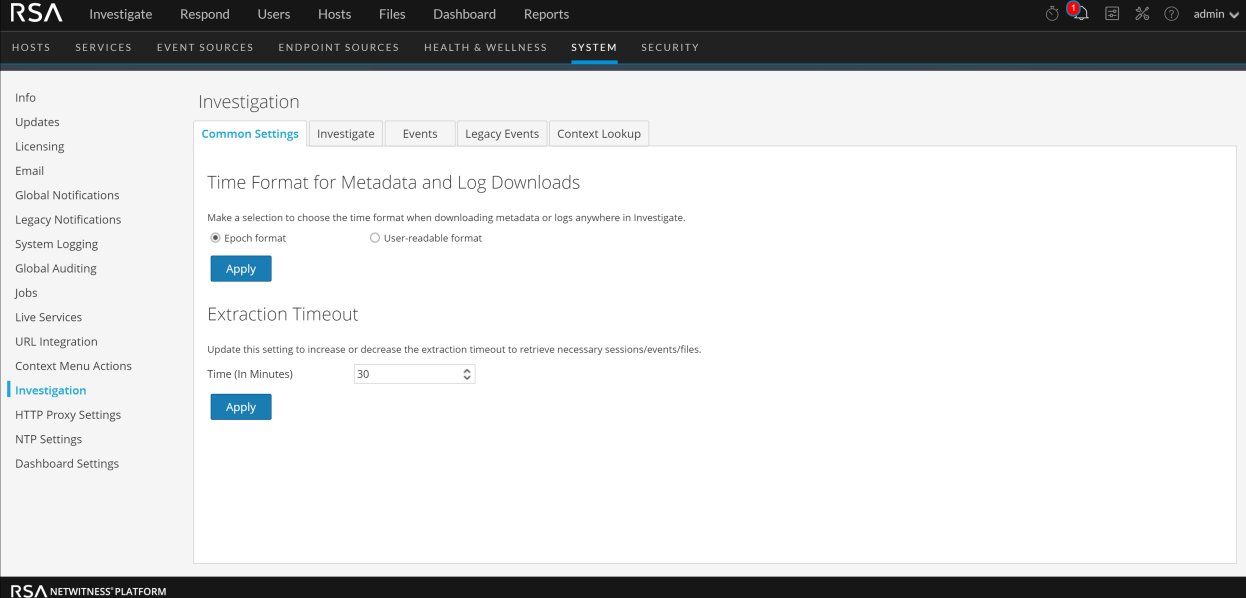
一般的な設定の構成

バージョン11.5以降では、「一般的な設定」タブを使用して、ナビゲートビュー、イベントビュー、およびレガシー イベントビューに適用する設定を構成できます。メタデータとログをダウンロードするときに使用する時間形式、および抽出タイムアウト設定を設定できます。

デフォルトでは、ダウンロードの時間形式はエポック形式であり、UNIXのエポック(1970年1月1日)からの秒数を表す数値で時間を示します。このように表示された時間を理解するには変換が必要です。設定を変更して、ユーザ設定のタイムゾーン、日付形式、および時間形式を組み合わせ、可能な場合は業界標準のISO 8601表現に従ったわかりやすい形式にすることができます。

この設定は、11.5のすべての [調査]ビューに適用されます。

 (管理) > [システム]に移動して、オプション パネルで [調査]を選択します。
[調査構成]パネルが表示されます。

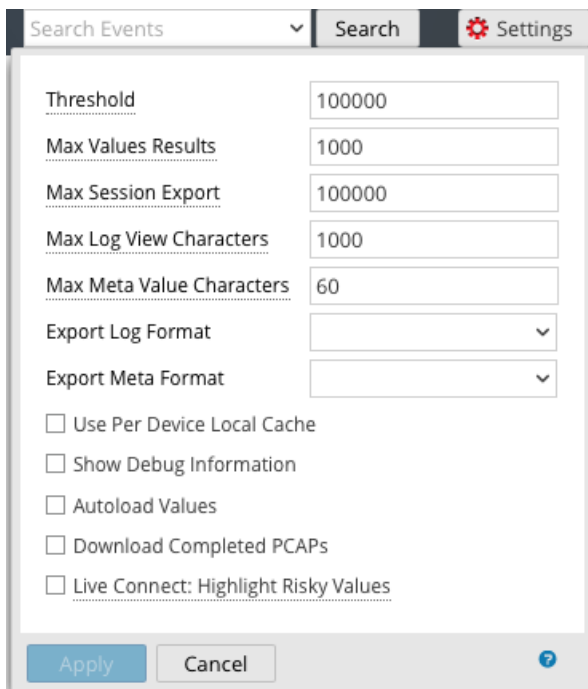


The screenshot shows the NetWitness Investigate interface. The top navigation bar includes 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. The main navigation menu on the left lists various system settings, with 'Investigation' highlighted. The 'Investigation' settings panel is open, showing two sections: 'Time Format for Metadata and Log Downloads' and 'Extraction Timeout'. In the first section, 'Epoch format' is selected with a radio button. In the second section, the 'Time (In Minutes)' dropdown is set to '30'. Both sections have an 'Apply' button.

[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

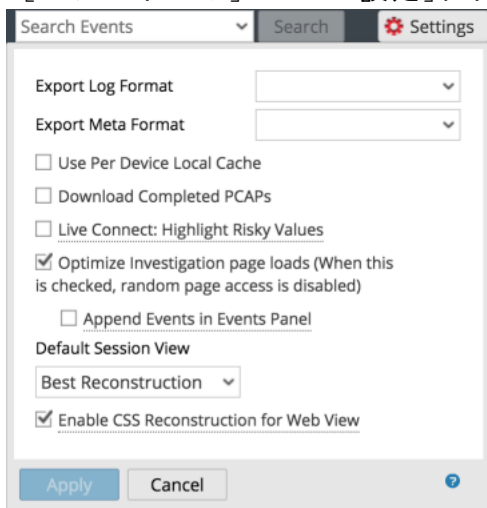
設定にアクセスするには、次のいずれかを実行します。

- [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。

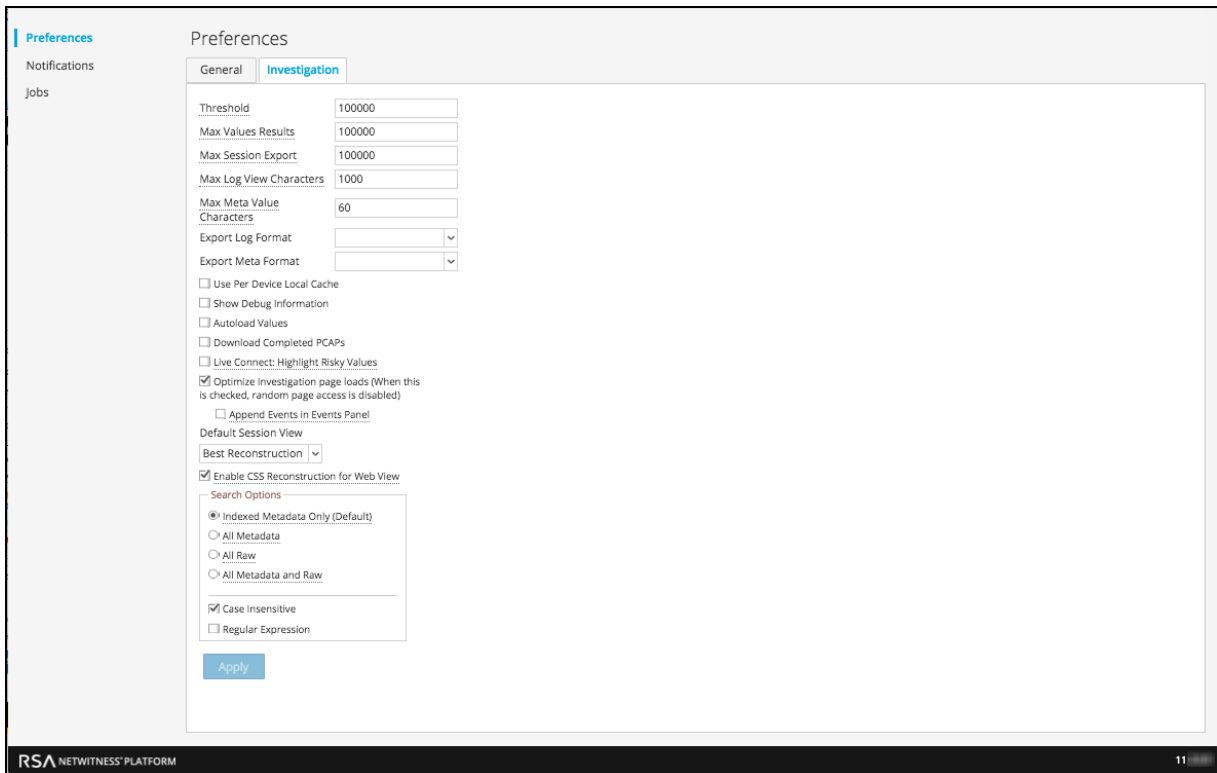
- 「レガシーイベント」ビューのツールバーで、「設定」オプションを選択します。「レガシーイベント」ビューの「設定」ダイアログが表示されます。



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の右上で、 > 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**：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。
 - **セッション エクスポートの最大数**：単一のPCAPファイルまたはログファイルで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の [ナビゲート]ビューで階層リンクの下にwhere句を表示する場合、またBrokerで集計したサービスごとに経過した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 [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、「 [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の [ナビゲート]ビューで選択したサービスの値を自動的にロードするには、このオプションをオンにします。このオプションを選択しない場合、NetWitnessには **値のロード** ボタンが表示され、ロードする値の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。
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アドレスのみをハイライト表示して表示する場合は、このオプションをオンにします。選択しない場合、NetWitnessではすべてのIPアドレスが表示されます。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** :**リスクのある値をハイライト表示** :このオプションをオフにすると、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。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呼び出すときに、NetWitness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呼び出すときに、NetWitnessで選択のダイアログが表示されます。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 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。

注 :バージョン11.5.2にアップグレードする場合、**メタ形式のエクスポート**]設定は保持されず、空白にリセットされます。バージョン11.5.2にアップグレードした後、この値を再構成する必要があります。

[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]ビューでのNetWitnessによるイベントの取得と再構築の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、以下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。
 - **[Investigationページのロードの最適化]** : ページ表示の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せん。
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、**[Investigation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)の使用を有効にできます。有効にすると、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。

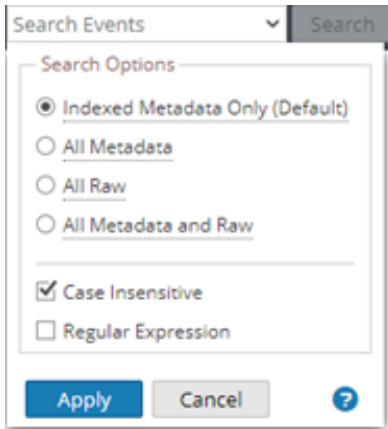
このオプションを有効化または無効化するには、次の手順を実行します。

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

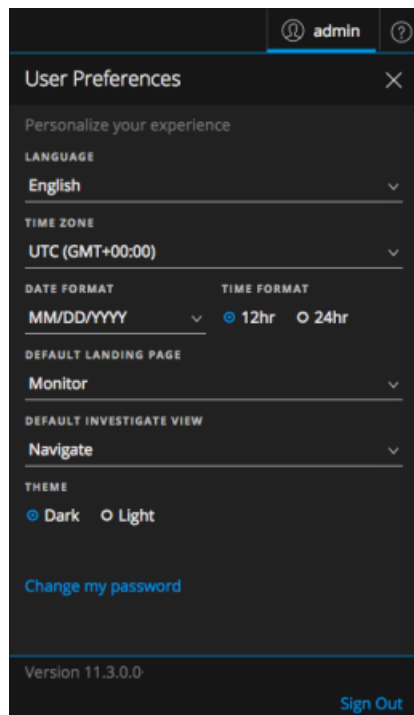
注：このピックに記載されている情報はNetWitness バージョン11.1以降に適用されます。

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、との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

ここで、「調査」ビューを開いた時に表示されるデフォルトのビューを選択できます。「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、「Malware Analysis」ビューのいずれかを選択します。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。



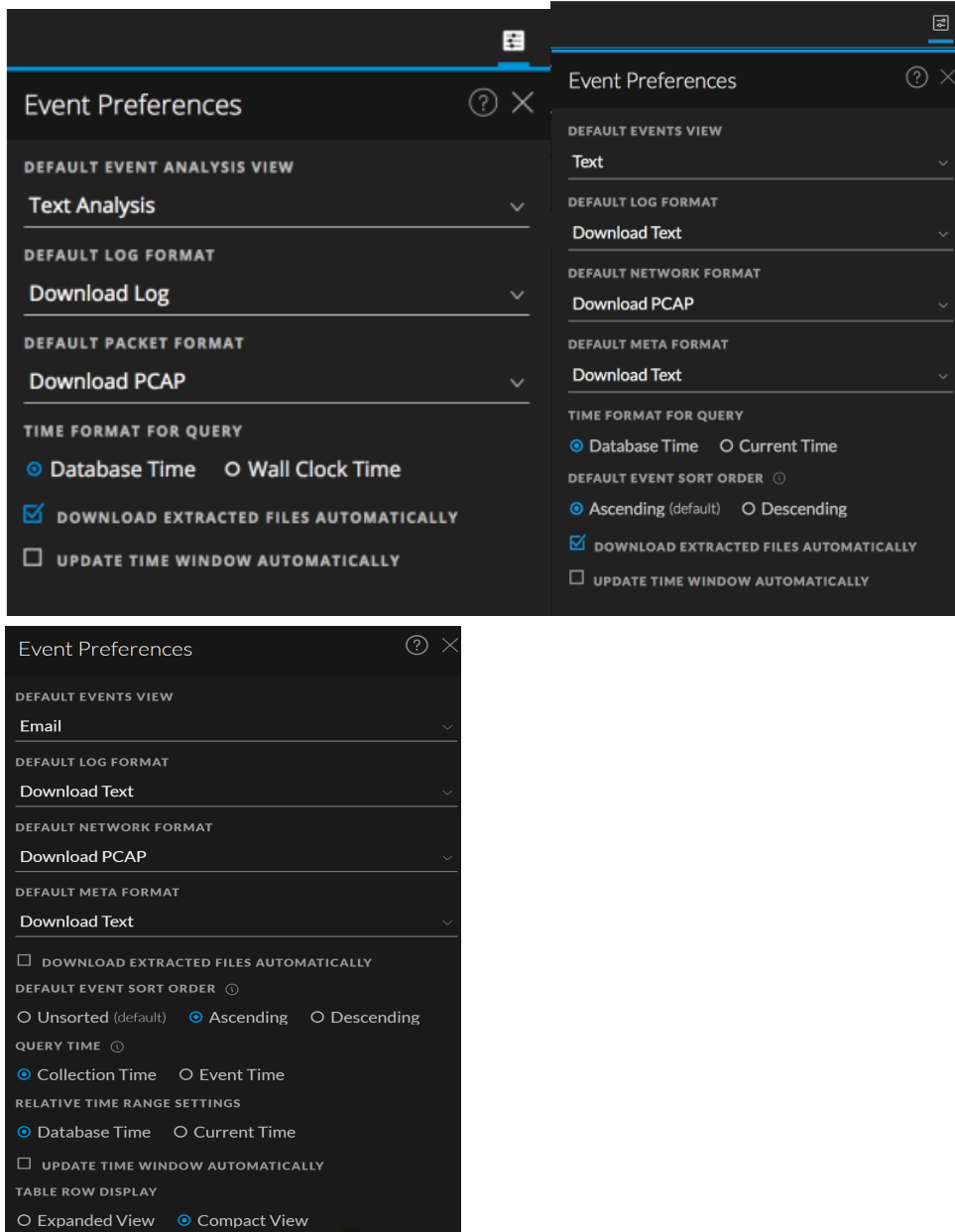
【イベント】ビューのユーザ環境設定の設定

【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、バージョンによって、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2つの図は、それぞれバージョン11.3と11.4のダイアログの例です。3番目の図は、バージョン11.6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]**、(バージョン11.5以降)**[ホスト]** または **[メール]** のいずれかを選択します。
デフォルトの再構築タイプを選択しなかった場合は、ログ イベントおよびエンドポイント イベントではテキスト分析が、それ以外のイベントではパケット分析がデフォルトの再構築タイプとして選択され、パケット分析が表示されます。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ため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]**、**[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。
6. (バージョン11.5.1以降) クエリ送信時に照合する時間の設定を変更するには、**[クエリ時間]** フィールドでオプションを選択します。
 - **[収集時間]** が選択されている場合、イベントの時間は、イベントがシステムで受信され、保存された時間を反映します。デフォルトではこの設定になっています。
 - **[イベント時間]** が選択されている場合、イベントの時間は、イベントが実際に発生した時間を反映します。イベント時間を使用するのに適しているのは、ログまたはエンドポイントを調査し、同じ時間帯に発生したイベントを探す場合です。イベント時間を使用すると、すべてのネットワーク イベントが除外されます。


注 : デフォルトでは、クエリの時間範囲は、Decoderがイベントを消費した時間に基づいています。これは、イベントが発生した時間と常には同じではありません。収集時間ではなく実際のイベント時間を **[イベント]ビュー** に表示するには、**[イベント時間]** を選択します。

注：イベント時間設定を有効にしてクエリを実行する場合は、収集時間列とタイムゾーン列を使用する必要があります。これは、イベントが順番に一覧表示されているかどうかを区別するのに役立ちます。このシナリオが生じるのは、イベント時間をログに記録する際に従うべきグローバル標準がないために、さまざまなソースからのさまざまなイベントがさまざまなタイムゾーンに存在する場合です。

7. (バージョン11.5.1以降) **相対時間範囲の設定**]で、**データベース時間**]または **現在の時刻**]を選択します。[イベント]ビューでは、相対的な時間範囲(過去2時間、過去30日など)に基づいて結果を表示できます。時間範囲は、イベントが受信されてシステムに保存された時間、または現在のタイムゾーンのクロック時間に基づいて設定できます。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、時間範囲は、最後に保存されたイベントの時間を基準に計算されます。
 - **現在の時刻 (Current Time)**] (バージョン11.3以前は **現在の時刻 (Wall Clock Time)**)]を選択した場合、時間範囲は、ユーザ環境設定のタイムゾーンの現在の時刻を基準に計算されます。

注：(バージョン11.6) **現在の時刻**]は、**相対時間範囲の設定**]のデフォルトです。以前のバージョンでは、**データベースの時間**]がデフォルト値でした。これにより、[イベント]ビュー(デフォルトとして **現在の時刻**]を使用)と [ナビゲート]ビュー(デフォルトとして **データベースの時間**]を使用)の間で時間範囲の不一致が生じる可能性があることに注意してください。この変更は既存のユーザには影響せず、新しいユーザにのみ適用されます。

8. (バージョン11.4と11.5) **クエリの時間形式**]で、**データベースの時間**]または **現在の時刻**]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、クエリの終了時刻はイベントが保存された時刻が基準になります。
 - **現在の時刻 (Current Time)**] (バージョン11.3以前は **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を基準にクエリが行われます。
9. (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で、リストのヘッダー列を操作して、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) :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、処理が高速になります。これは、一致するイベントが見つかったら即座に表示するのと、すべてのコア サービスの応答を待ってから指定された順に結果を並べ替えて表示する違いによるものです。

- **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。
10. 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。
 11. (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。
 12. (バージョン11.6以降) 複数行のデータがあり、イベントのコンテンツをワードラップまたはアンラップする場合は、 **コンパクト ビュー**] または **展開ビュー**] のいずれかを選択します。選択内容に基づいて、行がコンパクト表示または展開表示されます。

調査の開始

何を探しているかによって、NetWitness Investigateには、[\[サビゲート\]](#)ビュー(バージョン11.5以前)、[\[イベント\]](#)ビュー、[\[レガシー イベント\]](#)ビュー(バージョン11.3以前)、[\[ホスト\]](#)ビュー、[\[ファイル\]](#)ビュー、[\[ユーザ\(エンティティ\)\]](#)ビュー、[\[Malware Analysis\]](#)ビューという、さまざまなビューが用意されています。

ユーザーがNetWitnessで調査を実行するには、特定のユーザー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。

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)。11.5より前のバージョンでは、[\[調査\]](#)ビューのサブメニューでした。
- [\[ユーザ\]](#)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)。バージョン11.4では、[\[エンティティ\]](#)ビューという名前でした。11.5より前のバージョンでは、[\[調査\]](#)ビューのサブメニューでした。
- [\[レガシー イベント\]](#)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。
- バージョン11.6では、[\[イベント\]](#)ビューの [\[イベントの絞り込み\]](#)パネルがこの機能を提供するため、デフォルトでは [\[サビゲート\]](#)ビューは無効になっています。[\[サビゲート\]](#)ビューを有効にするには、「[\[サビゲート\]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。
- ユーザーがNetWitnessを使用して調査やマルウェアの解析を実施するには、特定のユーザーロールおよび権限が必要です。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。
- 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、[\[調査\]](#) > [\[サビゲート\]](#)、[\[調査\]](#) > [\[イベント\]](#)、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クエリによって、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](#)
- [\[サビゲート\]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、**ホスト**] (バージョン11.5) または **調査**] > **ホスト**] (バージョン11.4) 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ー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)。

高リスクのユーザー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ー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、**ユーザー**] (バージョン11.5)、**調査**] > **エンティティ**] (バージョン11.4)、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**] > **ユーザー**] に移動します。悪意のあるユーザーや不正ユーザーの検出、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、コミュニティー、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。このユーザー環境設定は、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、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ー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 **プロフィール** > **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。

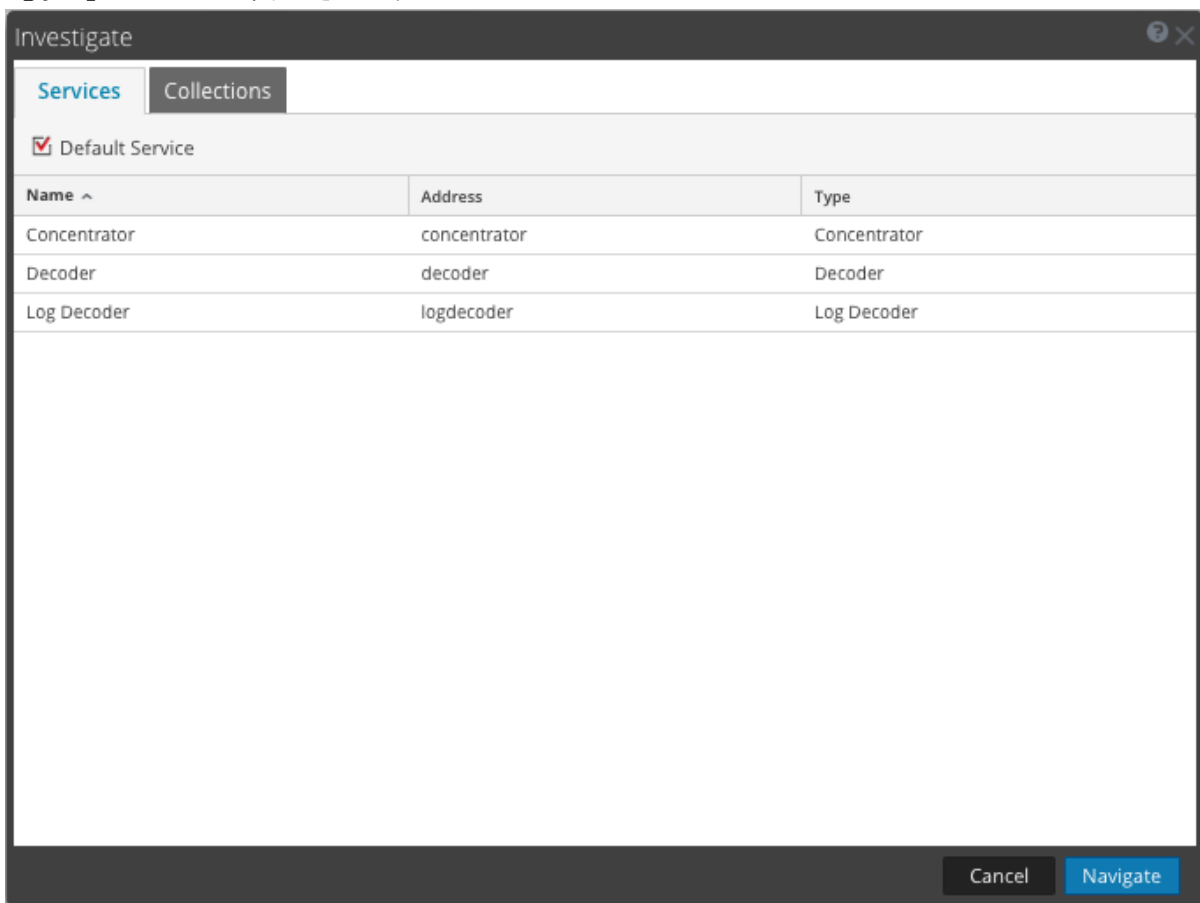
このトピックの後半では、サービスのデータの調査を開始するための手順について説明します。

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。

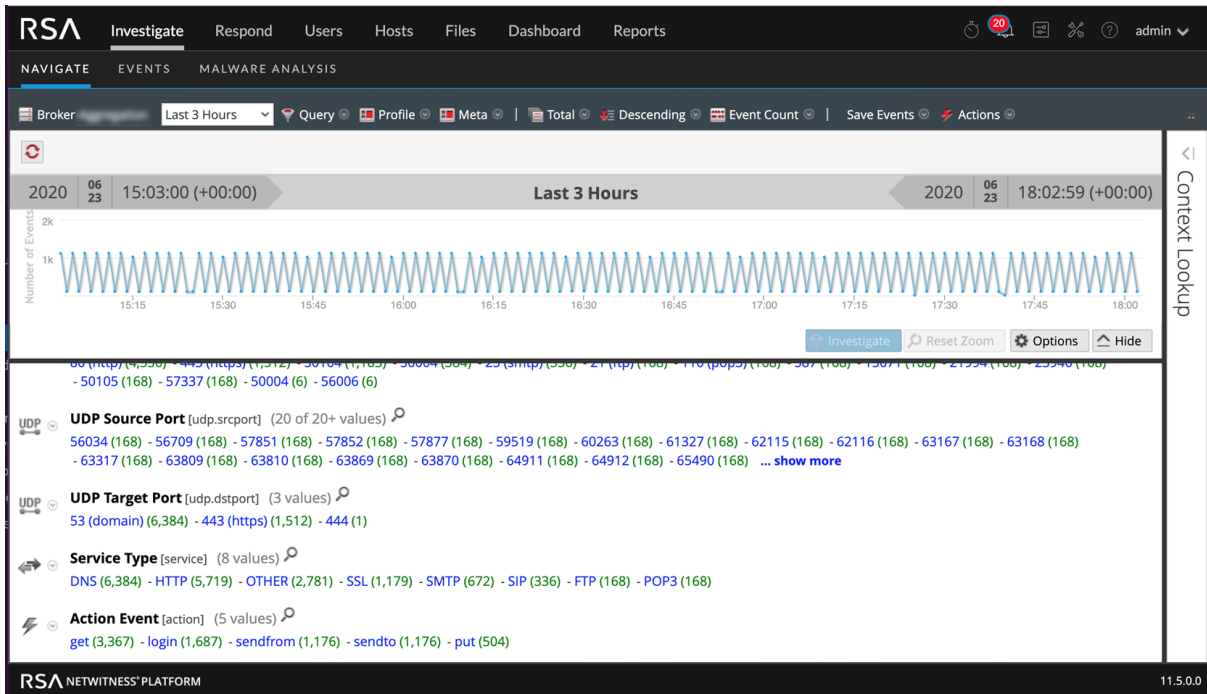
「ナビゲート」ビューまたは「レガシー イベント」ビューでデータをロードした後、結果の絞り込み、イベントの再構築と分析、結果のダウンロードと処理を行います（「[結果セットの絞り込み](#)」、「[イベントの再構築と分析](#)」、「[結果のダウンロードと処理](#)」を参照）。

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。

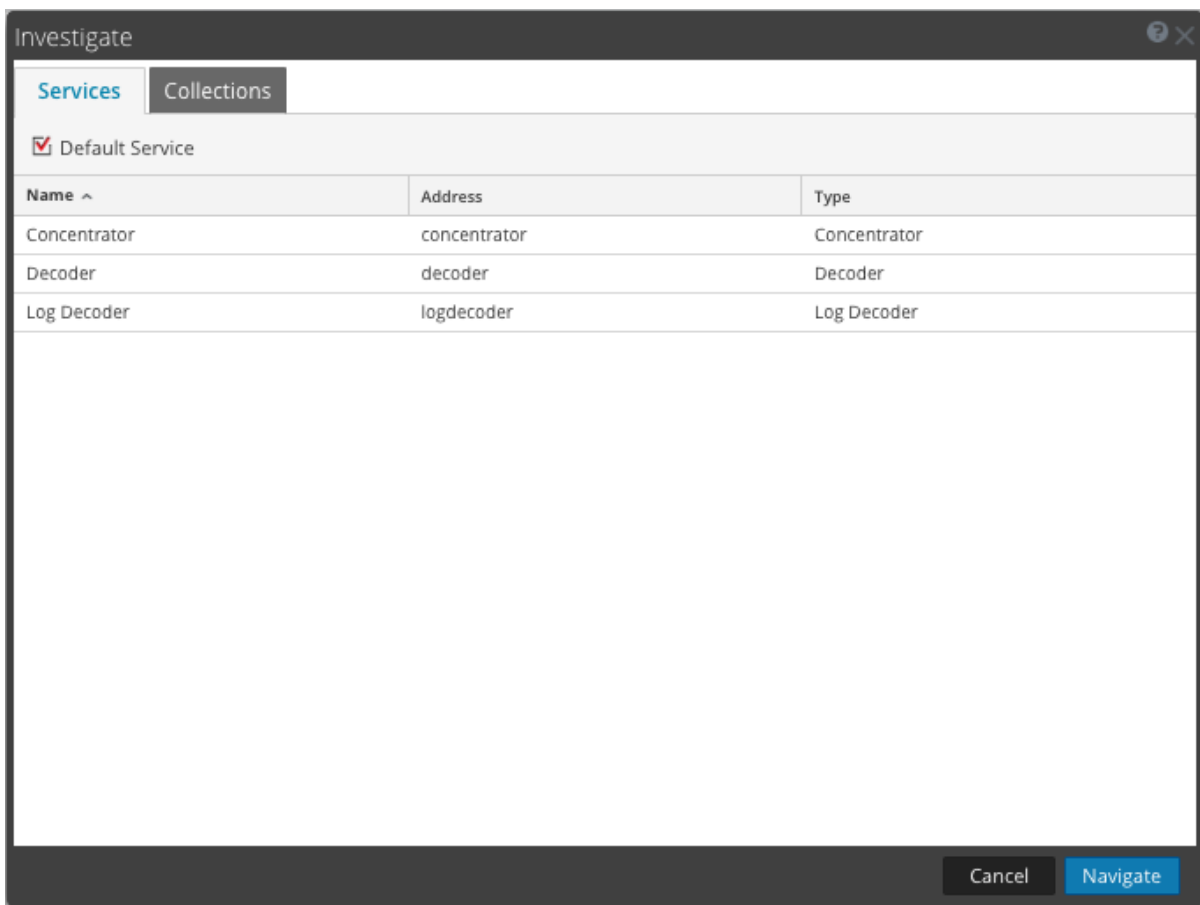


サービスを選択して、データがロードされたら、データを分析する準備が整います。

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。

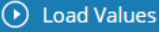


2. [サービス] グリッドでサービスを選択し、 Default Service をクリックします。
このサービスがデフォルトになります(サービス名の後に括弧に囲まれてデフォルトと表示されます)。
3. デフォルトのサービスの選択をクリアするには、グリッドでデフォルトのサービスを選択して、 Default Service をクリックし、[キャンセル] をクリックしてダイアログを閉じます。
デフォルトのサービスに設定されたサービスは存在しません。

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。

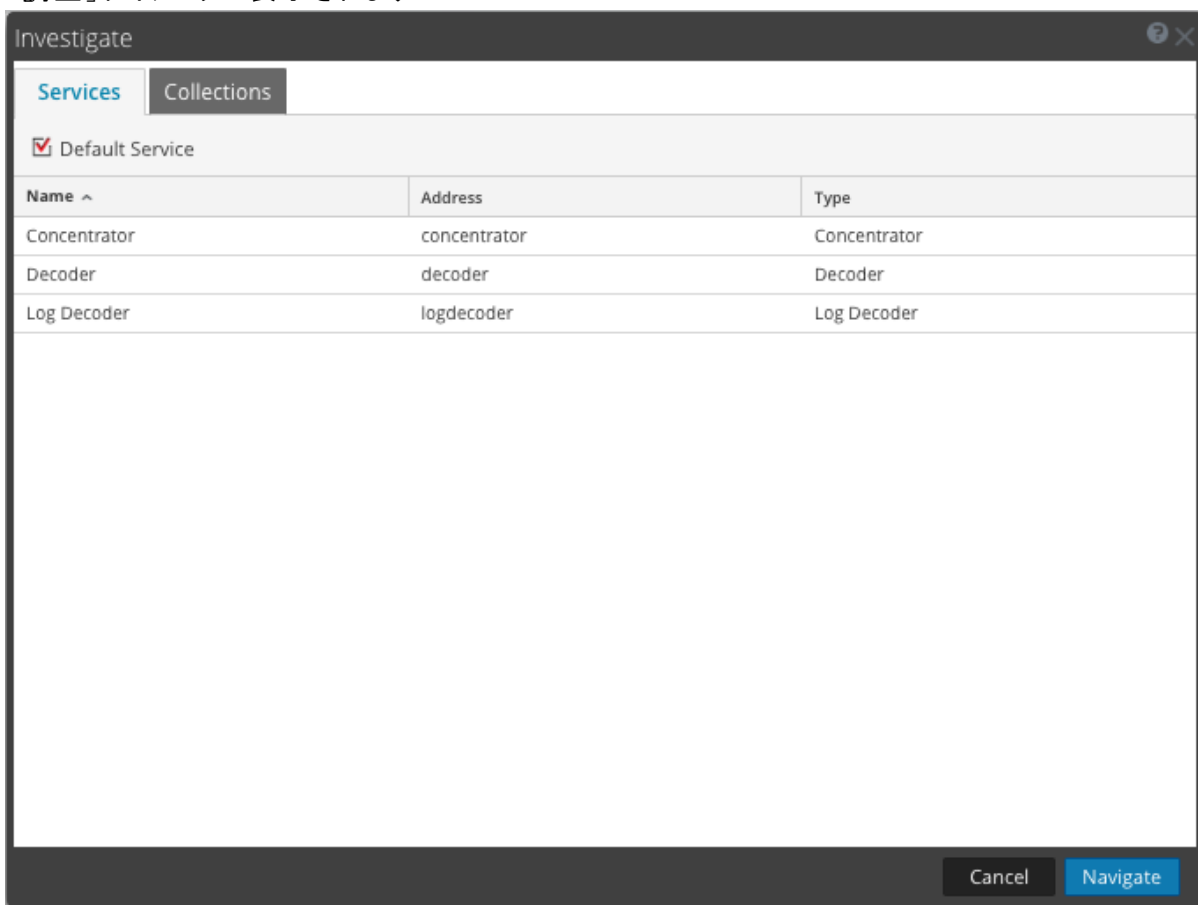
調査の開始(デフォルトのサービスが指定されている場合)


1. [調査] > [ナビゲート] または [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。[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せん。

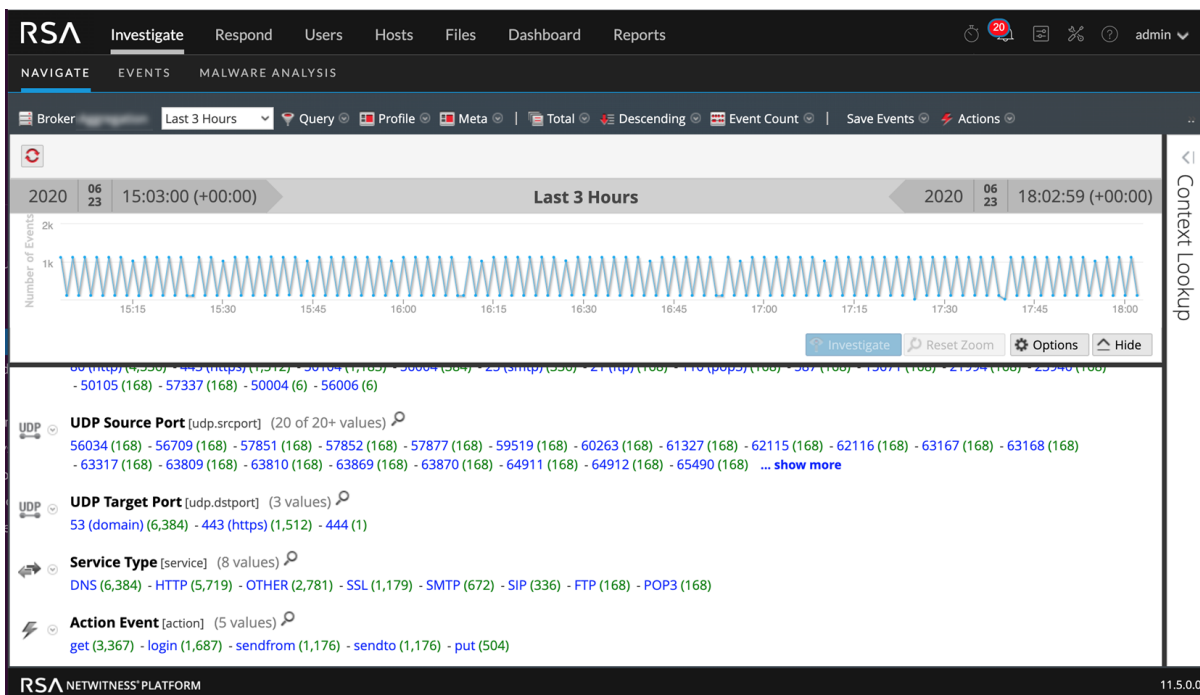
- データをロードする前に、[ナビゲート]ビューの調査オプションを変更することができます。たとえば、カスタムプロファイルの作成または変更、別の時間範囲の適用、メタグループの作成または適用、カスタムクエリの実行などです。
- 準備が完了したら、 をクリックします。
選択したオプションに従って、サービスからデータがロードされます。サービスを選択して、データがロードされたら、データを分析する準備が整います。

調査するサービスまたはコレクションの変更

- [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。



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



サービスが選択され、データがロードされて、データを解析する準備が整います。

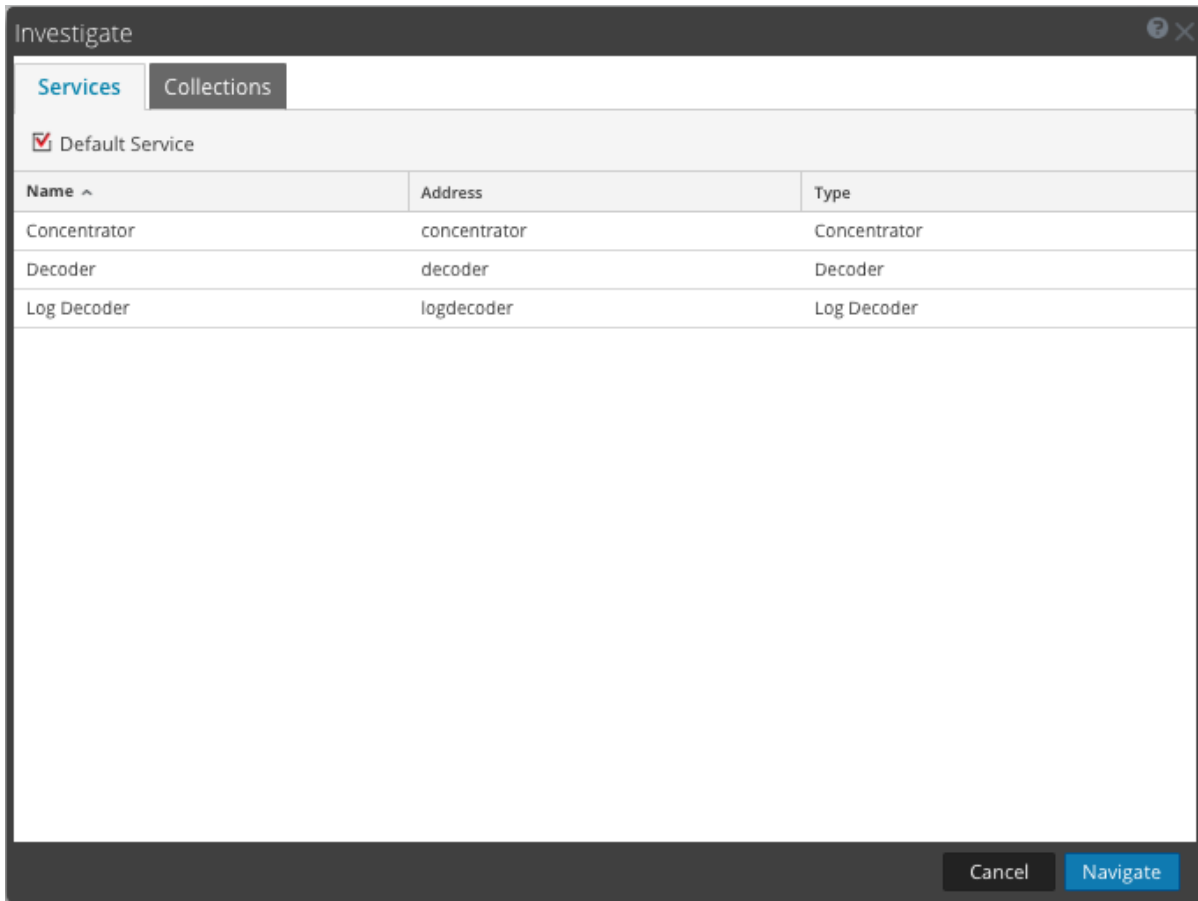
Workbenchのリストアコレクションの調査

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**] > **サビゲート**]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。

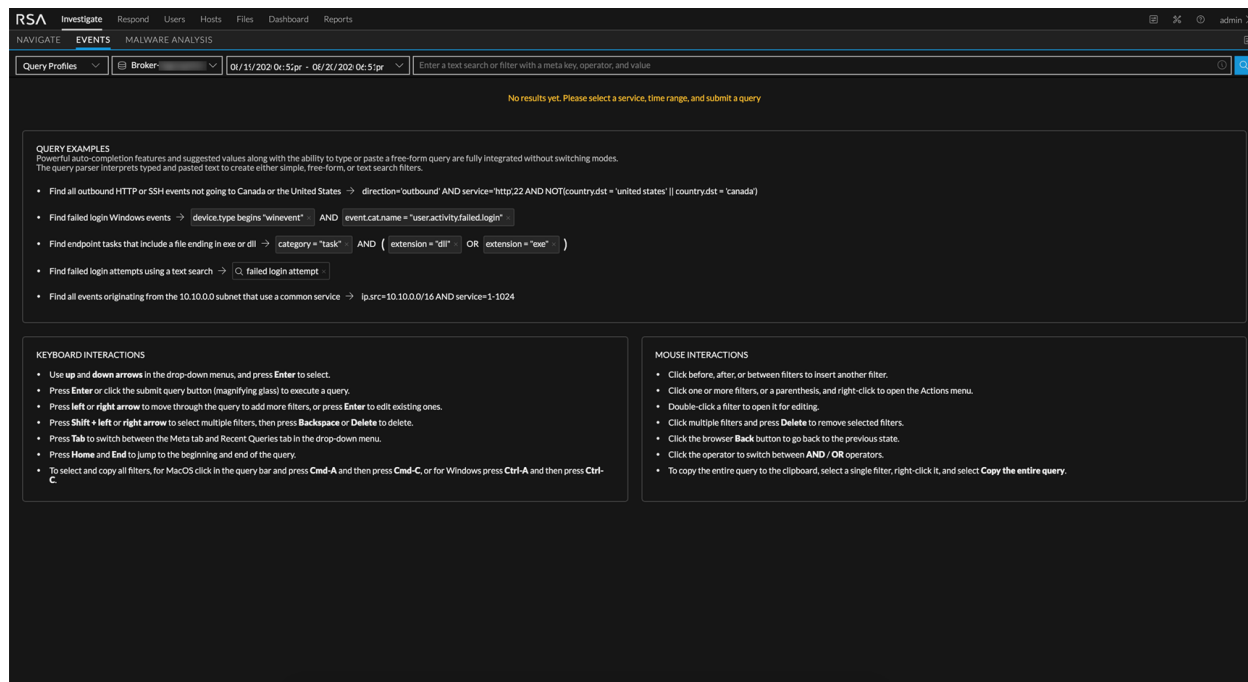


2. 調査するWorkbenchサービスとWorkbench名を選択します。
3. **ナビゲート**]をクリックして、選択したWorkbenchサービスに対する調査を実行します。
キャンセル]をクリックして、調査する別のWorkbenchサービスを選択できます。
調査]ビューが表示されます。コレクションを選択して、データがロードされたら、データを分析する準備が整います。

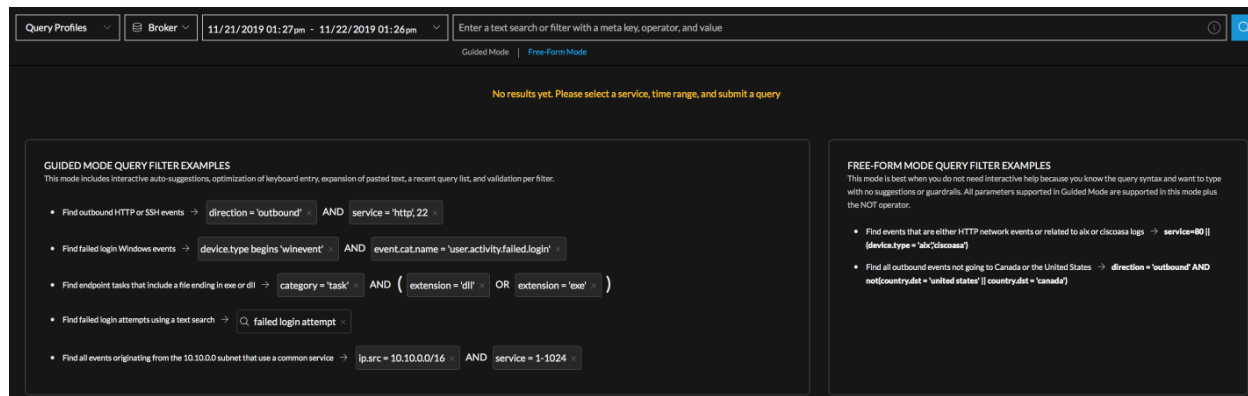
「イベント」ビューでの調査の開始

「イベント」ビューでは、「ナビゲート」ビューと「ラガシー 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。「ラガシー 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。「[イベントの再構築と分析](#)」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、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11.7では、アナリストが、[ブローカー]の下のリストにあるデバイスまたはサービスを選択するか、選択解除し、特定のブローカーに対してクエリを実行できます。これにより、機能していないサービスを含めたり、除外したりして、稼働中のサービスに対してクエリを実行できます。ブローカー サービスと関連サービスは、ネストされた形式で階層構造として一覧表示されます。

表示されるステータスは、次の3種類です。

- 緑 : サービスが稼働中またはオンラインであることを示す
- 赤 : サービスがダウンしているか、オフラインであることを示す
- オレンジ : サービスのステータスが不明であることを示す

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」ビューでのイベントの分析](#)」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」ビューでのイベントの分析](#)」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。

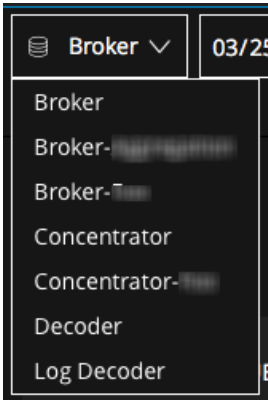
The screenshot shows the NetWitness Investigate interface with the 'EVENTS' tab selected. A search bar at the top shows a query for '08/19/2020 07:04 pm - 08/20/2020 07:03 pm'. Below the search bar, there are options for 'Filter', 'Column Group: RSA Outbound...', and 'Download'. The main area displays a table of 979 events. The table has columns for 'COLLECTION TIME', 'TYPE', 'DECODER...', 'TRAFFIC F...', 'SERVICE T...', 'HOSTNAM...', 'SOURCE IP...', 'DESTINATI...', 'IP ALIASES', 'SOURCE O...', 'DESTINATI...', 'SOURCE C...', 'DESTINATI...', 'SOURCE D...', and 'DES'. The table contains several rows of event data, including network traffic and SSL connections.


COLLECTION TIME	TYPE	DECODER...	TRAFFIC F...	SERVICE T...	HOSTNAM...	SOURCE IP...	DESTINATI...	IP ALIASES	SOURCE O...	DESTINATI...	SOURCE C...	DESTINATI...	SOURCE D...	DES
08/20/2020 06:21:38 pm	1 [Network]	nh	lateral	0 [OTHER]		10.237.169.48								
08/20/2020 06:21:38 pm	1 [Network]	nh	lateral	0 [OTHER]		10.237.169.40	10.237.169.87							
08/20/2020 06:21:37 pm	1 [Network]	nh	lateral	0 [OTHER]		0.0.0	10.237.168.0							
08/20/2020 06:21:38 pm	1 [Network]	nh	lateral	443 [SSL]		10.237.169.87	10.237.169.40							
08/20/2020 06:21:38 pm	1 [Network]	nh	lateral	443 [SSL]		10.237.169.87	10.237.169.40							
08/20/2020 06:21:38 pm	1 [Network]	nh	lateral	443 [SSL]		10.237.169.87	10.237.169.40							
08/20/2020 06:21:41 pm	1 [Network]	nh	lateral	0 [OTHER]		10.237.169.91	10.237.169.40							
08/20/2020 06:21:41 pm	1 [Network]	nh	lateral	0 [OTHER]		10.237.169.91	10.237.169.40							
08/20/2020 06:21:42 pm	1 [Network]	nh	lateral	443 [SSL]		10.237.169.40	10.237.169.87							
08/20/2020 06:21:43 pm	1 [Network]	nh	lateral	0 [OTHER]		10.237.169.40	10.237.169.87							
08/20/2020 06:21:43 pm	1 [Network]	nh	lateral	0 [OTHER]		10.237.169.87	10.237.169.40							

「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。

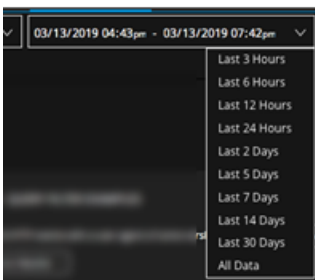
1. **調査** > 「イベント」に移動します。
 サービスが選択された状態で「イベント」ビューが開きます。データは表示されません。ドロップダウンリストには、アルファベット順で使用可能なサービスのリストが表示されます。「サービスの選択」フィールドでは、サービスリストの先頭のサービス、または最後に選択されたサービスがデフォルトで選択されます。デフォルトで、使用可能なサービスのリストは12時間ごとに取得され、NetWitness Server上にキャッシュされます。次の取得の前にNetWitness Serverにサービスを追加または削除した場合は、キャッシュが最新のサービスリストに更新されます。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



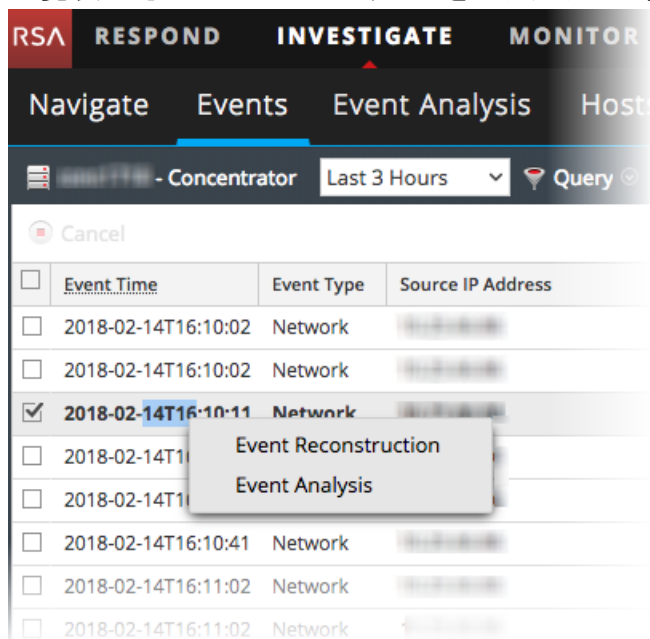
このサービスに選択した時間範囲はブラウザに保存されます。サービスごとに異なる時間範囲を設定できます。

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なら、 ([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詳細の調査](#)」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. 次のいずれかの操作を実行します。
 - 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詳細の調査](#)」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]ビューおよびバージョン11.5以降の[イベント]ビューでは、メタグループを使用して、[ナビゲート]ビュー([値] パネル) および [イベント]ビュー([イベントの絞り込み] パネル) に表示されるデータをフィルタリングできます。同じ共有メタグループを両方のビューで使用できます。[イベント]ビューで作成されたプライベートメタグループは、[ナビゲート]ビューまたは[レガシーイベント]ビューのクエリプロファイルで使用できません。

注： [ナビゲート]ビューと [レガシーイベント]ビューでは、インデックスなしのメタキー(またはインデックスにまったく含まれていないキー)をメタグループまたは列グループに手動で追加できます。インデックスなしのメタキーは、[ナビゲート]ビューと [レガシーイベント]ビューでは完全に使用可能(管理および表示可能)ですが、[イベント]ビューでは部分的にのみ使用可能([イベントの絞り込み] パネルに表示可能)です。[イベント]ビュー([イベントの絞り込み] パネル)には、メタグループにすでに含まれているインデックスなしのメタキーのデータを表示できますが、メタグループの編集にインデックスなしのメタキーを追加することはできません。列グループ内のインデックスなしのメタキーは列にデータを表示せず、新しいインデックスなしのメタキーを [イベント]ビューの列グループに追加することはできません。

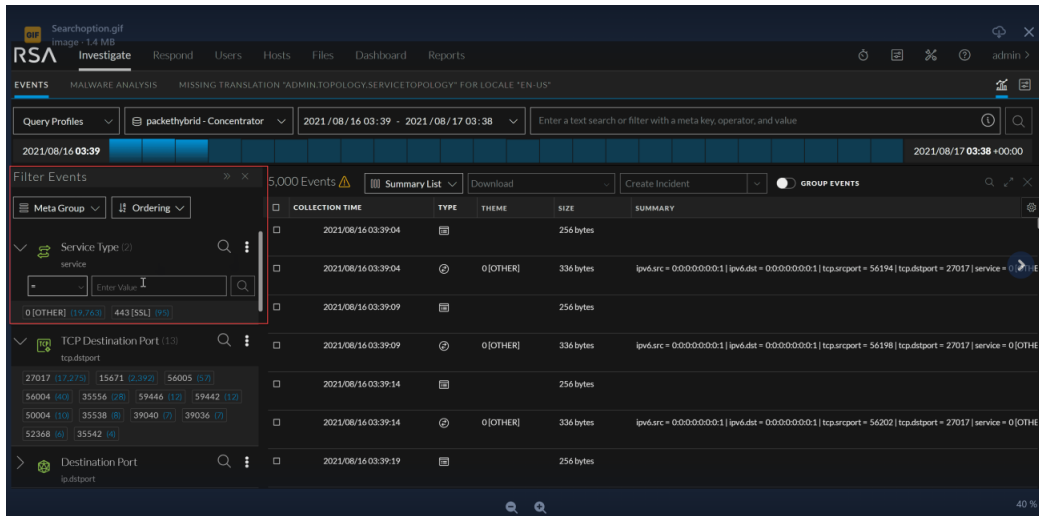
調査中にメタグループが有効になっている場合、[値]パネルまたは[イベントの絞り込み]パネルの情報には、選択されたグループのメタキーのみが表示されます。座標表示チャートを[ナビゲート]ビューで開くと、メタキーとメタエンティティが軸として左から右に表示されます。カスタムメタグループごとに2つのバージョンを作成しておくのが便利です。1つはメタ値の分析に使用し、もう1つはメタキーを減らしたサブセットを作成し、座標表示チャートの表示に使用します。

NetWitness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は複製できますが、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のコピーを編集し、カスタムグループを作成することもできます。

[ナビゲート]ビューのすべてのグループは共有され、サービスのすべてのユーザに表示されます。グループをエクスポートして任意のサービスにインポートできますが、そのサービスで使用可能なメタキーによって制限されます。バージョン11.5の[イベント]ビューの[イベントの絞り込み]パネルでは、共有カスタムメタグループとプライベートカスタムメタグループの両方を作成できます。[ナビゲート]ビューでは、共有グループのみが表示され、使用できます。

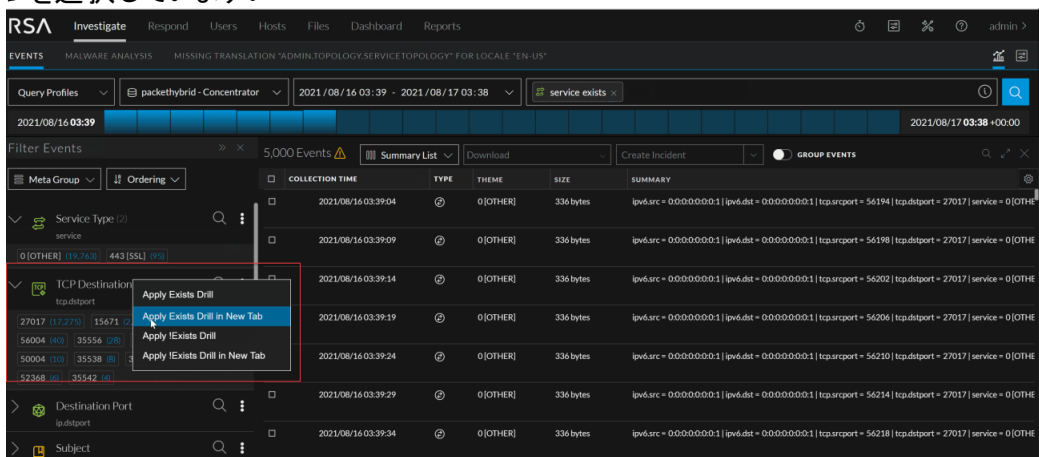
バージョン11.7では、イベントUIでメタキーごとの検索オプションを使用して、特定のメタキーのクイック検索をアナリストが実行できるため、イベントフィルタパネルのメタキーとクエリバーの間で複数回クリックする必要がありません。

たとえば、この画像では、アナリストが特定のサービスタイプメタを検索しています。



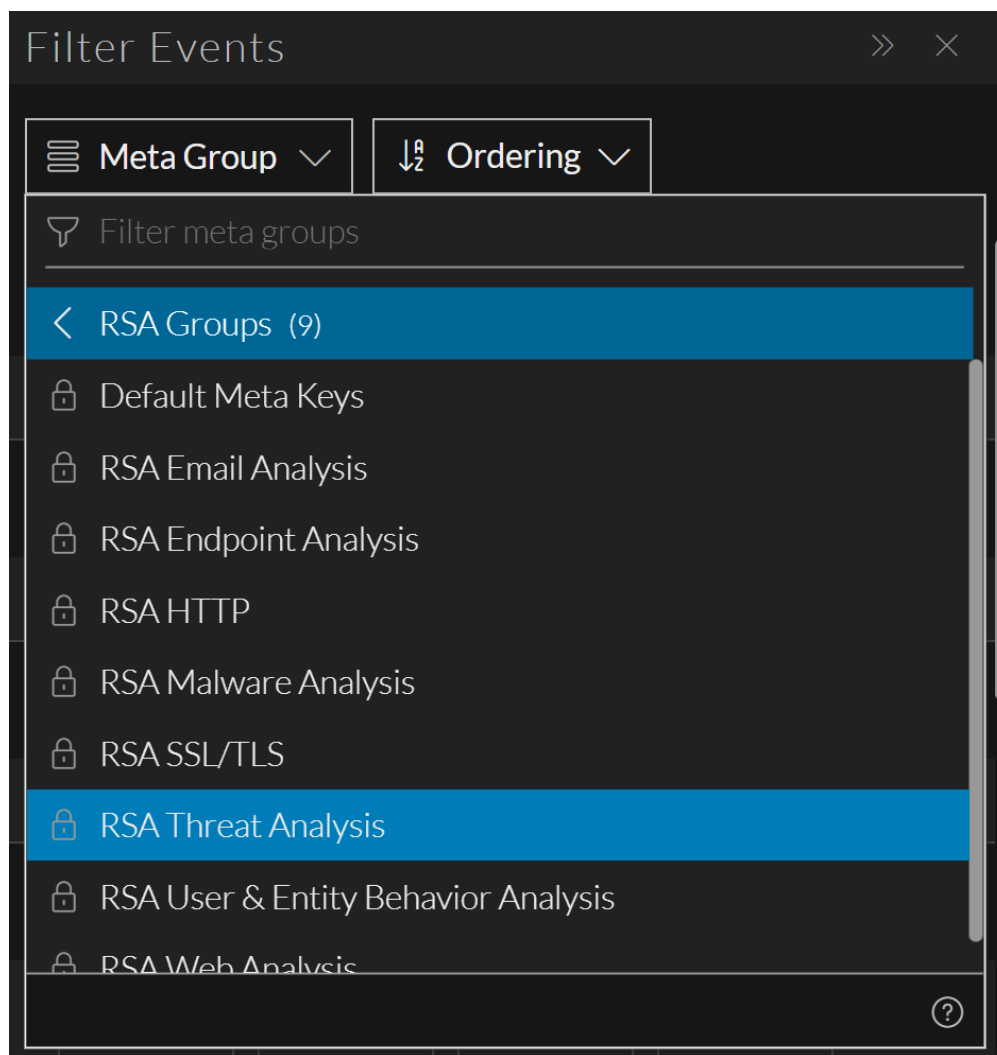
さらに、アナリストは、メタキーの説明を右クリックして、existsおよび!existsドリルを実行することにより、イベント フィルタ パネルから直接操作できます。メタ キー名を左クリックすると、クエリに追加され、クエリが実行されます。アナリストが複数のクエリを実行する場合は、Shiftキーを押したままで左クリックすると、クエリへの追加のみが実行されます。

たとえば、この画像では、アナリストがTCP宛先メタを選択し、新しいタブでExistsドリルダウン]オプションを選択しています。



Liveメタ グループ

11.6以降では、NetWitnessはLiveからの調査コンテンツの導入をサポートしています。メタグループは、RSAグループ(RSA LiveコンテンツおよびRSA OOTBグループ)と共有グループに分類されます。Liveから導入されたコンテンツは、Live記号()でマークされて表示されます。コンテンツはフォルダー構造で表示されます。グループは、編集不可能なフォルダーとサブフォルダーとして表示されます。()内の数字はフォルダー内のコンテンツの数を示し、>記号はフォルダー内をドリルダウンするために使用されます。



標準提供メタグループ

RSA NetWitnessには、名前が「RSA」で始まり、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。これらのグループをコピーし、コピーに新しい名前を付けてから、コピーを編集できます。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、プロセス、ファイル、ユーザ、NetWitness Endpoint(NWE) ホストからの接続に関するインサイト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 HTTPには、外部へのWebトラフィックのインサイトを提供するメタキーが含まれています。
- RSA 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 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 キーが含まれています。
- 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。

Default Meta Keysグループ(バージョン11.5の [イベント]ビュー)

Default Meta Keysメタ グループは、現在選択されているサービスのすべてのメタ キーで構成される特殊なタイプの標準提供メタ グループであり、サービスのインデックス ファイルに表示される順序で結果が返されます。Default Meta Keysグループは、常に [メタ グループ]メニューのリストの一番上に表示されます。

Default Meta Keysグループは、メタ グループが選択されておらず、ローカルストレージにメタ グループが存在しない場合に、[イベントの絞り込み]パネルに表示されるメタ キーを選択するために使用されます。他のグループと同様に、このグループを選択することもできます。[イベントの絞り込み]パネルでDefault Meta Keysグループを使用すると、値を持つ最初の30個のメタ キーのみが開かれ、残りは閉じられます。

カスタム メタ グループ

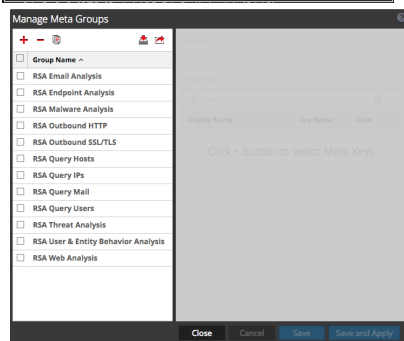
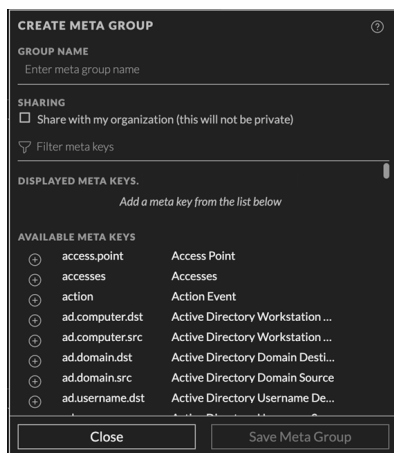
カスタム メタ グループを作成して、調査中に頻繁に使用するシナリオをサポートできます。管理者が、サービスのカスタム インデックス ファイルを編集して、カスタム メタ グループを手動で追加した場合、サービスの再起動後に新しいメタ グループが利用可能になります。カスタム メタ グループは、共有またはプライベートにすることができます。共有メタ グループは、[ナビゲート]ビューと[イベントの絞り込み]パネルで組織内でグローバルに使用できます。共有のカスタム メタ グループを編集する場合、変更はグローバルに適用されます。共有のカスタム メタ グループを削除すると、そのグループは削除され、すべてのアナリストが使用できなくなります。[ナビゲート]ビューでは、共有グループのみがサポートされています。[イベント]ビューでカスタム メタ グループを作成する時に、共有するかプライベート(デフォルト)にするか選択できます。共有グループをプライベートに変更したり、プライベート グループを共有に変更することはできません。

注： [イベント]ビューで作成されたプライベート カスタム メタ グループは、[ナビゲート]ビューで表示または使用できません。

[メタ グループ]メニューでは、グループ タイプはアイコンで識別されます。次の図は、行の最後に編集アイコンが表示された各カスタム メタ グループ タイプの例です。



[ナビゲート]ビューと [イベント]ビューのメタ 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) [メタ グループの作成]ダイアログと([ナビゲート]ビューの) [メタ グループの管理]ダイアログを示しています。



【イベント】ビューの [メタグループ] メニュー(バージョン11.5以降)のオプションを使用して、以下を実行できます。

- 適用するメタグループの選択
- メタグループの詳細の確認
- カスタムメタグループの作成、編集、削除
- 標準提供またはカスタムのメタグループをコピーして、コピーを編集

【ナビゲート】ビューの [メタグループの管理] ダイアログのオプションを使用すると、上記のすべてを実行できるだけでなく、メタグループをインポートおよびエクスポートすることもできます。

このピックの残りの部分では、11.5の【イベント】ビューと【ナビゲート】ビューでメタグループを操作する手順について説明します。

【イベント】ビューでのメタグループの操作(バージョン11.5以降)

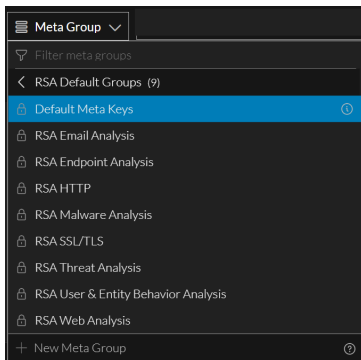
バージョン11.5以降にアップグレードした後、既存のすべてのメタグループ(標準提供とカスタムの両方)が、【イベントの絞り込み】パネルでイベントのフィルタリングに使用できるようになります。メタグループの選択は、ブラウザのキャッシュがクリアされない限り、再ログイン時にも維持されます。


メタグループに含まれているメタキーの表示

メタ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。

2. [イベントの絞り込み]パネルを表示するには、[イベント]パネルの上の **Filter** をクリックします。
[イベント]パネルの左側に [イベントの絞り込み]パネルが開きます。
3. [メタグループ]メニューを表示するには、[メタグループ]メニュー タイトルをクリックします。メニュー タイトルは、メタグループ (Default Meta KeysまたはMeta Group :<現在選択されているメタグループ >) のいずれかです。ログイン後に初めてアクセスした場合は、Default Meta Keyグループが選択されています。2回目以降のアクセスでは、前のセッションで選択されたメタグループが使用されます。前のセッションで選択したメタグループが削除された場合は、ログイン時にDefault Meta Keysグループが選択されます。このグループを開くと、標準提供のメタグループ (RSA)、共有カスタムメタグループ、プライベート カスタムメタグループのリストがメニューに表示されます。リストの上にある表示オプションとフィルタを使用すると、特定のメタグループを見つけやすくなります。



4. (オプション) リストに表示されたメタグループを名前でもフィルタリングするには、**[メタ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。
リストが更新され、完全に一致するテキストを含んだグループ名のみが表示されます。
5. メタグループ名にカーソルを合わせて、情報アイコン() をクリックし、グループに含まれているメタキーを確認します。
左の図は、RSA HTTPメタグループの列を示しています。右の図は、Default Meta Keysメタグループの列を示しています。

META GROUP DETAILS 📄 ?

GROUP NAME
RSA HTTP

SHARING
Shared

DISPLAYED META KEYS

did	Decoder Source	Open
medium	Medium	Auto
direction	Traffic Flow Direction	Auto
service	Service Type	Auto
alias.host	Hostname Aliases	Auto
ip.src	Source IP Address	Auto
ip.dst	Destination IP Address	Auto
alias.ip	IP Aliases	Auto
org.src	Source Organization	Auto
org.dst	Destination Organization	Auto
country.src	Source Country	Auto
country.dst	Destination Country	Auto
domain.src	Source Domain	Auto

Close Select Meta Group

META GROUP DETAILS 📄 ?

GROUP NAME
Default Meta Keys

SHARING
Shared

DISPLAYED META KEYS

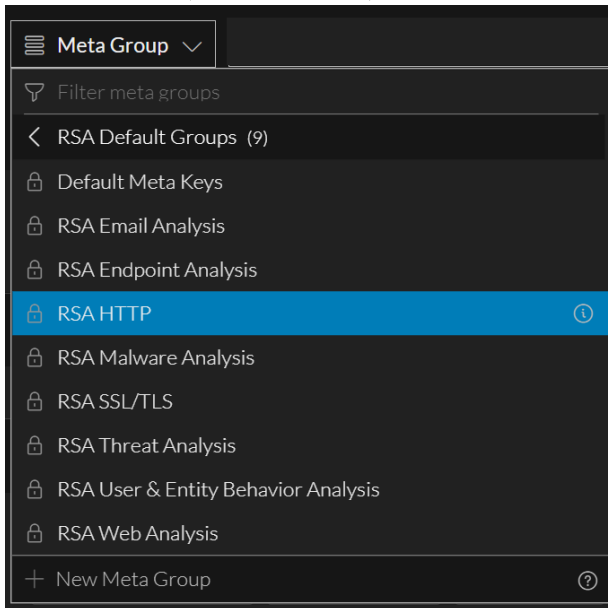
sessionid	Session ID	Hidden
size	Data Size	Hidden
payload	Payload Size	Hidden
medium	Network Medium	Hidden
eth.src	Ethernet Source Address	Auto
eth.dst	Ethernet Destination Address	Auto
eth.type	Ethernet Protocol	Auto
ip.proto	IP Protocol	Auto
ip.src	Source IP Address	Auto
ip.dst	Destination IP Address	Auto
ipv6.src	Source IPv6 Address	Auto
ipv6.dst	Destination IPv6 Address	Auto
tcp.srcport	TCP Source Port	Auto

Close Select Meta Group

6. 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. メタグループを適用する場合は、**メタグループの選択**]をクリックします。
ダイアログが閉じ、選択したメタグループのメタキーを反映するように **イベントの絞り込み**]パネルが更新されます。

メタグループの選択

1. バージョン11.5の **イベント**]ビューで **イベントの絞り込み**]パネルを開き、**メタグループ**]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、メタグループとフォルダーのリストが表示されます。**メタグループの絞り込み**]オプションと、**新しいメタグループ**]オプションも表示されます。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メタグループ名が表示されます。次の図は、RSA HTTPがハイライトされた後(ただし未選択)のメニューを示しています。



2. 次のいずれかの操作を実行します。
 - 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**を押します。
 - b. メタグループ名を検索するには、**メタ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フィルタリングされ、入力した文字列を含むメタ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**を押します。
イベントの絞り込み]パネルが更新され、選択したメタグループに含まれるメタキーのみが表示され、選択したメタ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。

注：メタグループ内のメタキーが、選択したサービスでサポートされない場合、それらのメタキーは [イベントの絞り込み] パネルまたは [イベント] パネルには表示されません。

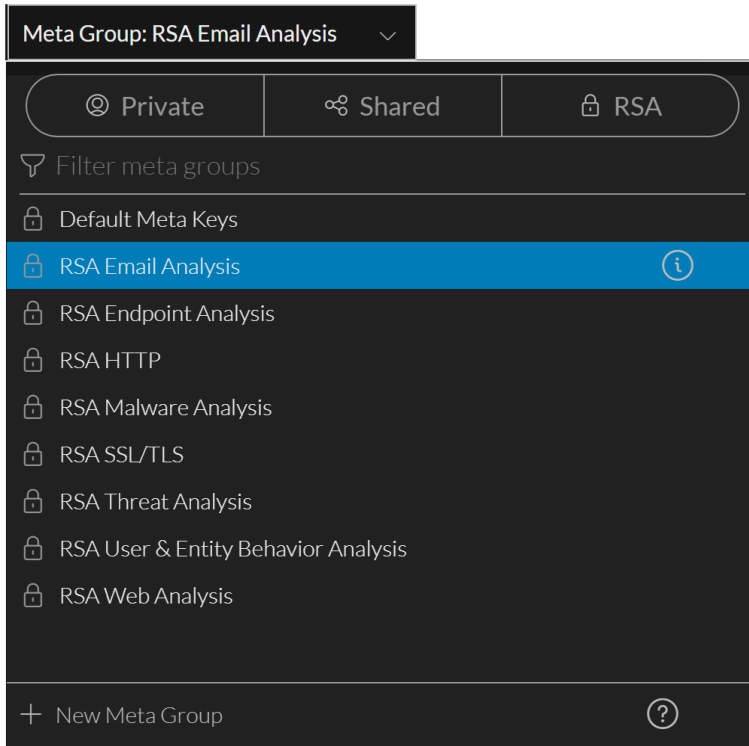
カスタムメタグループの作成

カスタムメタグループには、最大80文字の一意的な名前と、少なくとも1つのメタキーが必要です。共有かプライベートかにかかわらず、入力した名前のメタグループが他にある場合は、別の名前を使用する必要がありますことを知らせるメッセージが表示されます。これらの条件が満たされると、[メタグループの保存] ボタンが有効になります。[表示するメタキー] リストでキーをドラッグして、グループ内のメタキーの順序を調整できます。

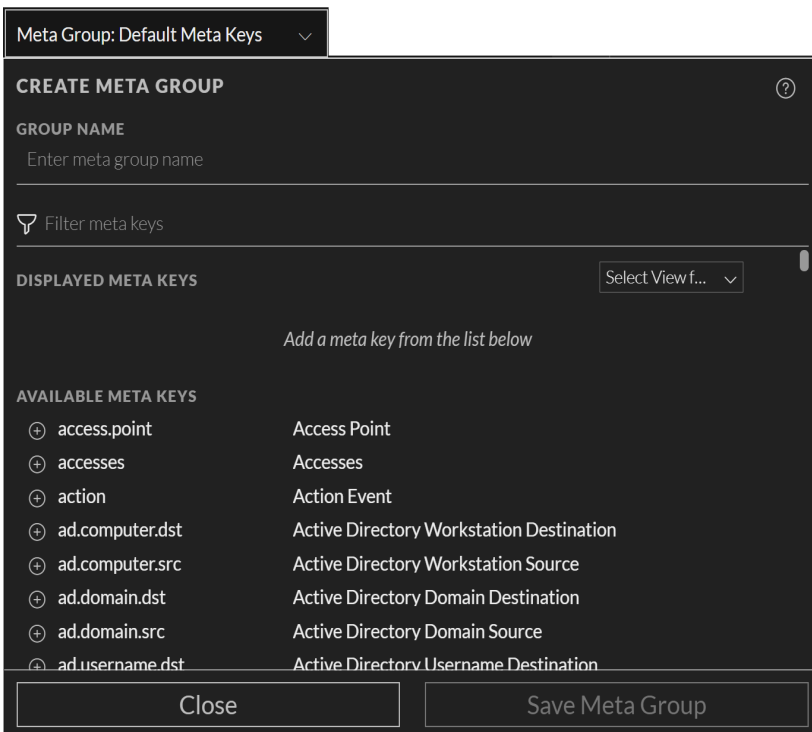
各メタキーの初期ビュー([開く]、[閉じる]、[隠す]、または [自動] (デフォルト設定)) を設定することもできます。

注：また、同じ値をすべてのメタキーに一度に設定することもできます。すべてのメタキーの値を変更すると、パフォーマンスに影響する可能性があることに注意してください。

- [自動] に設定されている場合、メタキーはインデックスされてい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閉じたままになります。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。
 - [開く] に設定したメタキーは、[イベントの絞り込み] パネルに一覧表示され、値がロードされます。
 - [閉じる] に設定したメタキーは、[イベントの絞り込み] パネルに一覧表示されますが、メタキーを開くまでメタ値はロードされません。
 - [隠す] に設定したメタキーは、[イベントの絞り込み] パネルに表示されません。この機能は、複数のメタグループを作成する代わりに、単一のメタグループを複数の目的で使用している場合に役立ちます。メタグループから削除せずに特定のキーをオフにすることができます。[隠す] は、新しいメタキーをテストする場合や、まだ使用できない新しいメタキーを含んだメタグループを準備する場合にも使用できます。[自動]、[開く]、[閉じる] を選択した場合に発生するエラーを回避できます。
1. 11.5の [イベント] ビューで [イベントの絞り込み] パネルを開いて、[メタグループ] 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、メタグループとフォルダーのリストが表示されます。[メタグループの絞り込み] フィールドが一番上に、[新しいメタグループとフォルダー アイコン] オプションが一番下に表示されます。




2. 「新しいメタグループ」を選択します。
「メタグループの作成」ダイアログが表示されます。

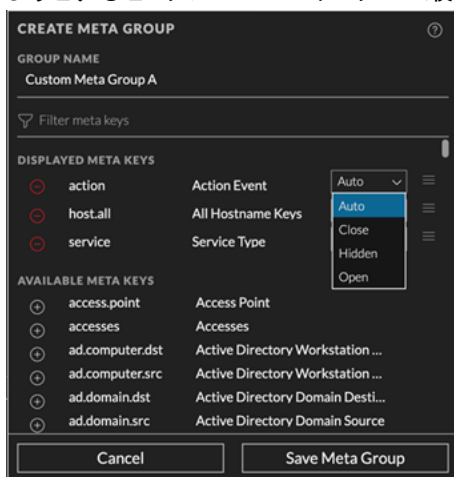





3. 「グループ名」フィールドに、新しいメタグループの一意の名前(最大256文字)を入力します(たとえば「Custom Meta Group A」)。

4. 新しいメタグループを組織内で共有する場合は、**組織内で共有**]オプションを設定します。
5. メタ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、入力したテキストを使用してフィルタ処理されます)。メタグループ内のメタキーの最大数は500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500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) 各メタキーの横で、メタキーの初期表示状態(**開く**]、 **閉じる**]、 **隠す**]、または **自動**])を選択します。
7. (オプション) メタ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。削除したいメタキーが表示されたら、 **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. 次のいずれかの操作を実行します。
 - a. カスタムメタ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、 **メタグループの保存**]をクリックします。
新しいメタグループが保存されます。新しいグループが共有されている場合は、すべてのアナリストが使用できるようになります。プライベートの場合は、自分だけがそのメタグループを使用できます。ボタンが **閉じる**]と **メタグループを選択**]に変わります。

10. 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. ダイアログを閉じて新しいメタグループを選択するには、**メタグループを選択**]をクリックします。新しいグループが**メタグループ**]メニューに(アルファベット順で)追加されます。**メタグループの選択**]をクリックした場合は、**イベントの絞り込み**]パネルが更新されて、新しいメタグループのメタキーと値が表示されます。

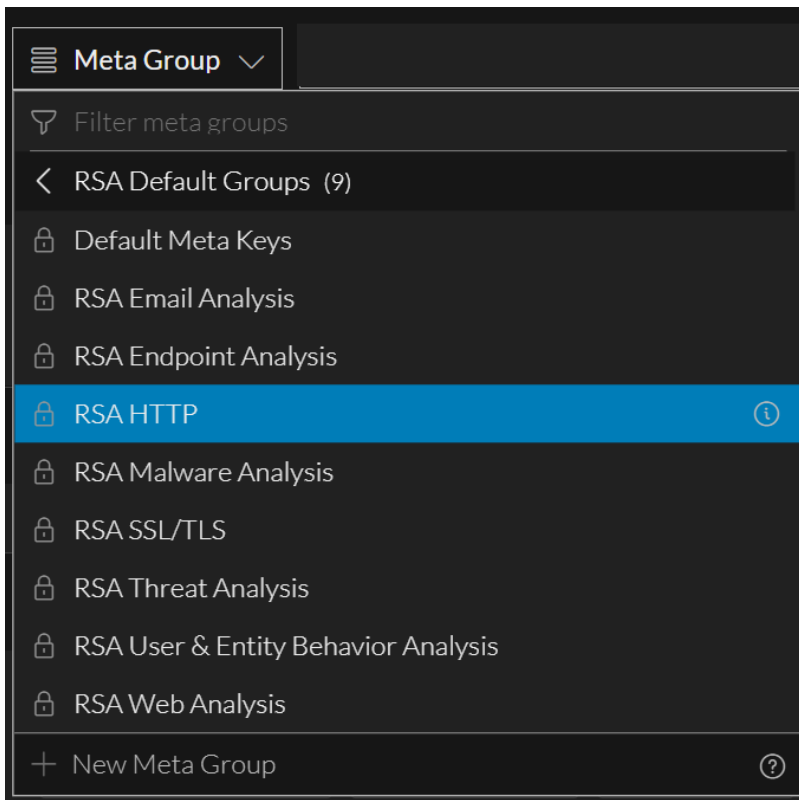
カスタムメタグループの削除

現在イベントリストに適用されておらず、クエリプロファイルで使用されていないカスタムメタグループは、共有かプライベートにかかわらず削除できます。**削除**]ボタンをクリックすると、確認メッセージが表示され、削除を確認またはキャンセルできます。クエリプロファイルでメタグループが使用されている場合、**削除**]ボタンは無効になり、メタグループが使用されているクエリプロファイルを示すメッセージが表示されます。標準提供のメタ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。

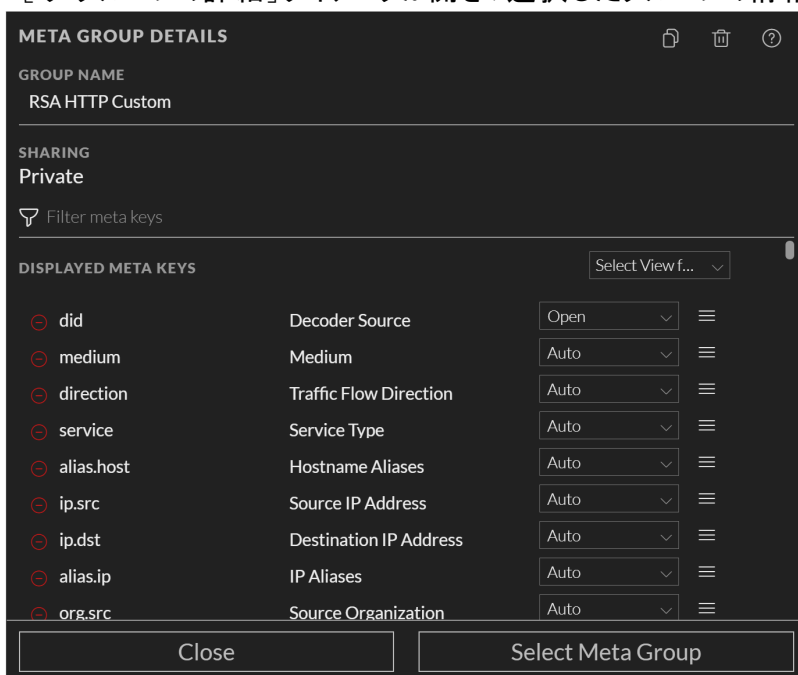
注意：共有メタグループの削除の影響はグローバルであり、すべてのアナリストがそのグループを使用できなくなります。

カスタムメタグループを削除するには、次の手順を実行します。

1. 11.6の**イベント**]ビューで**イベントの絞り込み**]パネルを開いて、**メタグループ**]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、メタグループとフォルダのリストが表示されます。**メタグループの絞り込み**]フィールドが一番上に、**新しいメタグループ**]オプションが一番下に表示されます。



2. メタグループを削除するには、カスタムメタ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. [メタグループの詳細]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。

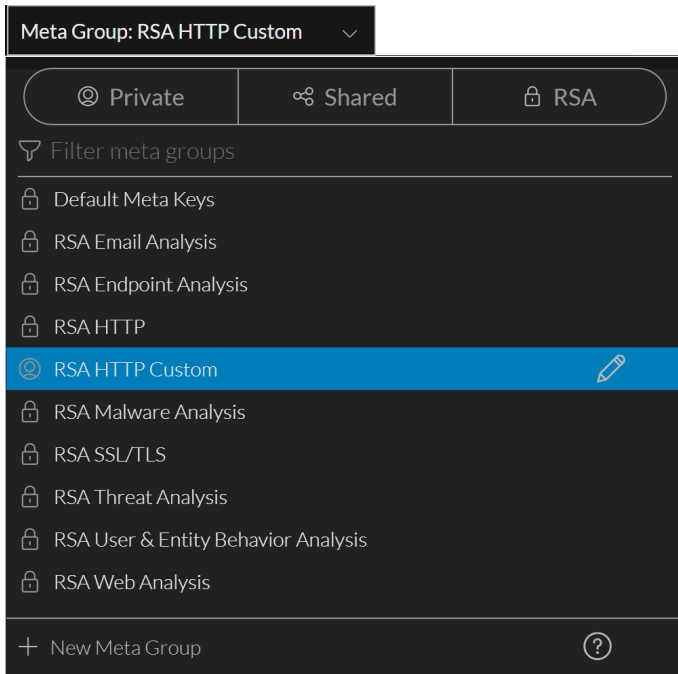


4. グループの削除アイコン(🗑️)をクリックします。
メタグループが現在有効になっている場合は、次のメッセージが表示されます。This meta group cannot be deleted because it is currently active.
バージョン11.5では、確認メッセージが表示され、削除を確認するかキャンセルすることができます。
[キャンセル]または[メタグループの削除]をクリックします。
グループが削除され、[メタグループ]メニューに表示されなくなります。削除したメタグループは、調査を行うすべてのアナリストに表示されなくなります。

カスタムメタグループの編集

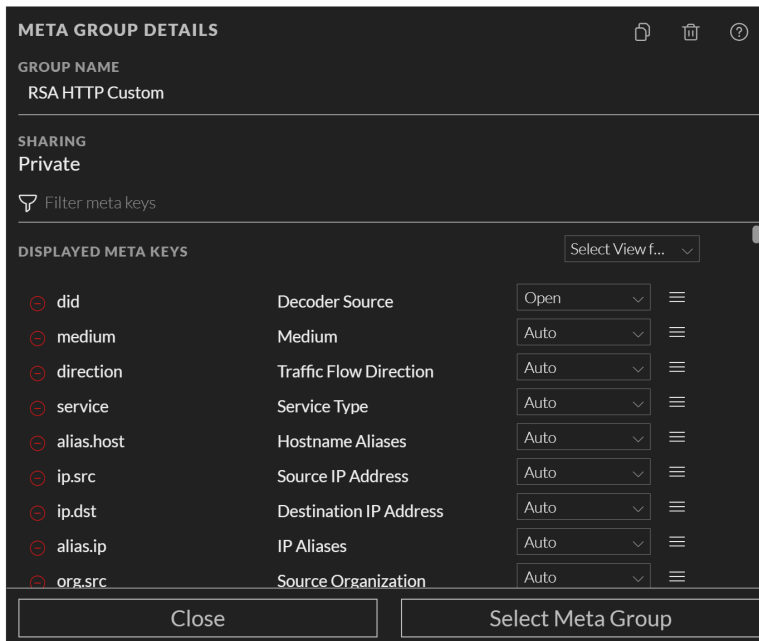
共有カスタムメタグループ、自分のプライベートメタグループ、標準提供メタグループのコピー、またはLiveメタグループのコピーを編集できます。

1. 11.5の[イベント]ビューで[イベントの絞り込み]パネルを開いて、[メタグループ]メニュータイトルをクリックし、編集するメタ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プライベートメタグループRSA HTTP Customと、その右側に表示された編集アイコンを示しています。



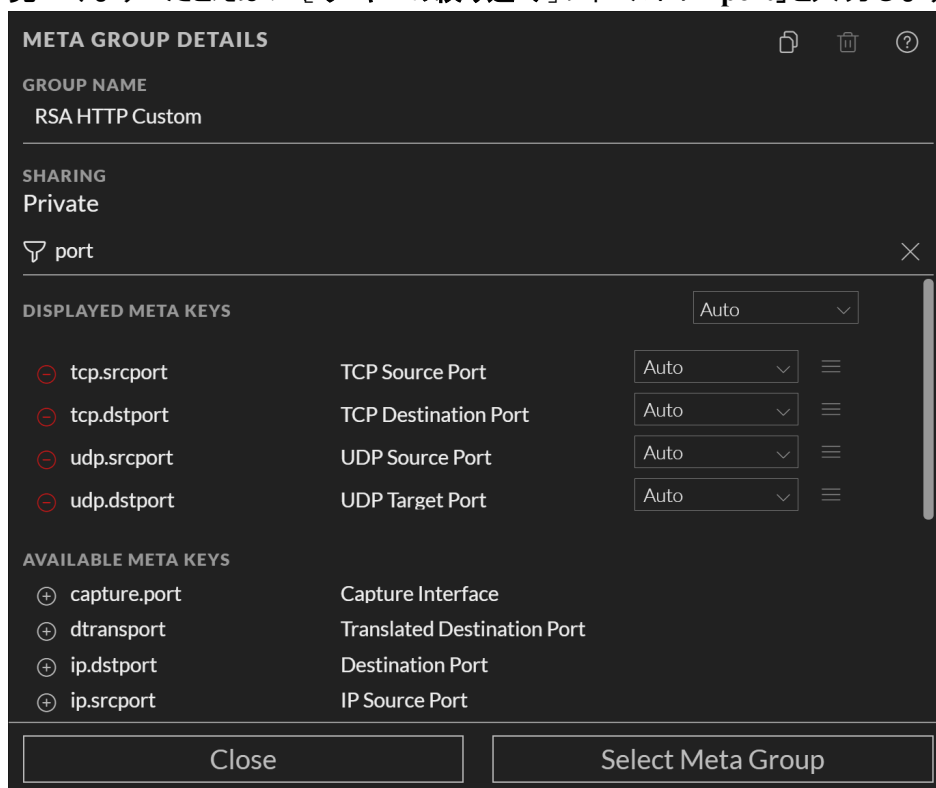
2. 編集アイコン(✎)をクリックします。





メタグループの詳細ダイアログが表示され、場所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。



3. (オプション) **グループ名** フィールドで、メタグループの名前と場所を編集します。
4. (オプション) メタ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。たとえば、**メタ キーの絞り込み** フィールドに「port」と入力します。



- 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。
5. (オプション) メタ 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。削除したいメタ キーが表示されたら、**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。
6. (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() になったら、リスト内でメタ キーを上下にドラッグします。
7. 次のいずれかの操作を実行します。
 - a. カスタムのメタ 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. メタ グループの編集を保存するには、**メタ グループの更新** をクリックします。更新されたメタ グループが保存され、ダイアログが閉じられます。

メタグループのコピー(バージョン11.5以降)

進行中の未保存の編集がない限り、標準提供またはカスタム、Liveメタグループ、共有またはプライベートのいずれかにかかわらず、任意のメタグループをコピーできます。この機能は、標準提供グループのカスタマイズされたバージョンが必要な場合に便利です。また、カスタムグループをプライベートから共有に、または共有からプライベートに変更することはできないため、コピーを作成することで、別の共有設定を選択できるようになります。メタグループをコピーすると、同じ名前が使用され、番号が付記されます。たとえば、RSA HTTPを2回コピーすると、最初のコピーの名前はRSA HTTP-1になり、2番目のコピーの名前はRSA HTTP-2になります。グループをコピーした後は、コピーを編集して新しい名前を指定し、グループ内のメタキーを管理することができます。



注： [レガシー イベント]ビューで作成された一部のメタグループには、 [イベント]ビューのメタグループの制限を上回る、500個を超えるメタキーが含まれている場合があります。500個を超えるメタキーを持つグループをコピーする場合は、メタグループの編集時に余分なメタキーを削除する必要があります。

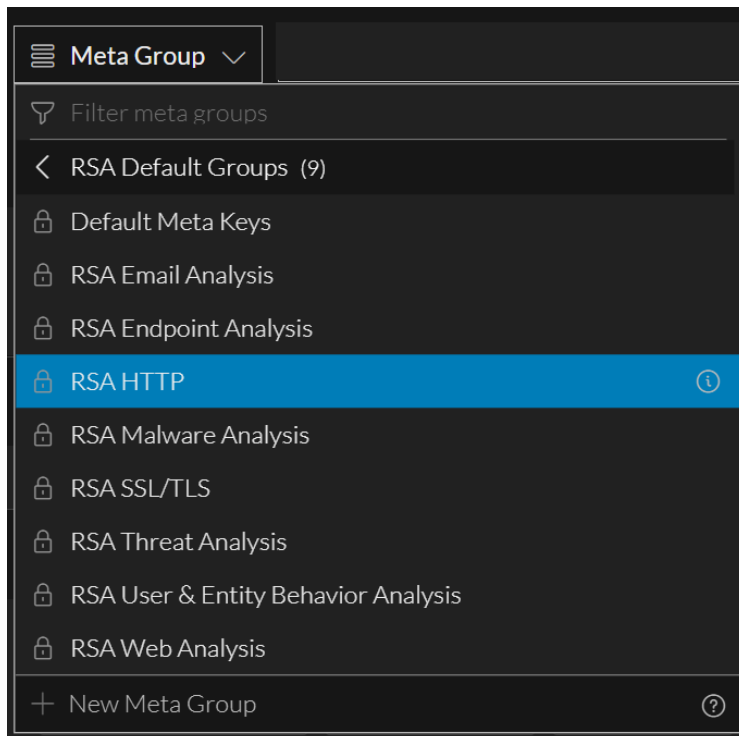
メタグループをコピーするには、次の手順を実行します。

1. 11.6の [イベント]ビューで [イベントの絞り込み] パネルを開き、 [メタグループ] メニュータイトルをクリックします。

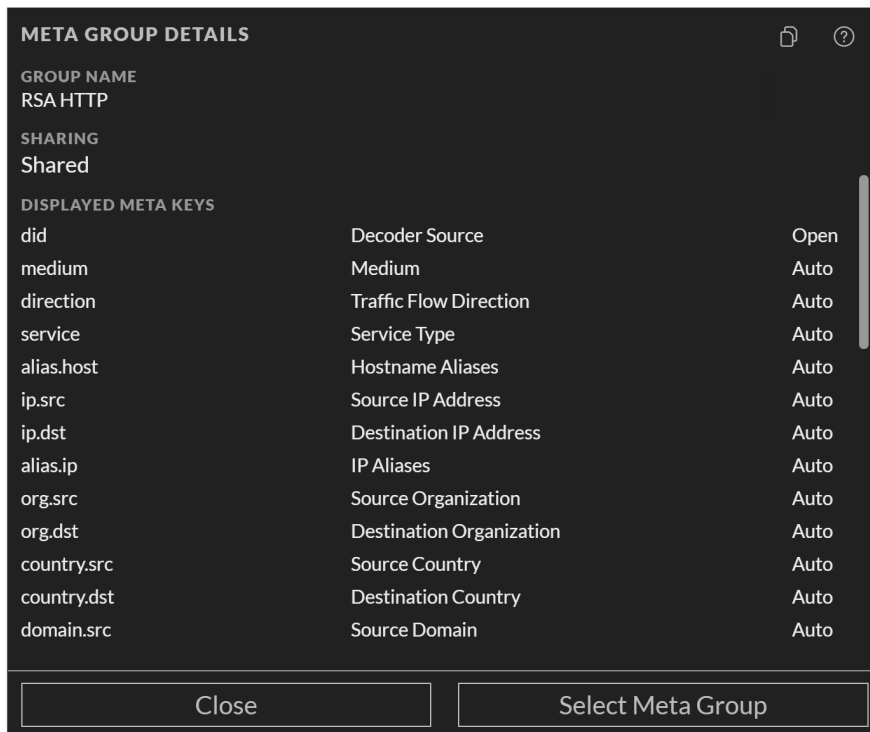
メニューがドロップダウンし、メタグループとフォルダーのリストが表示されます。

2. コピーするメタグループをハイライト表示します。

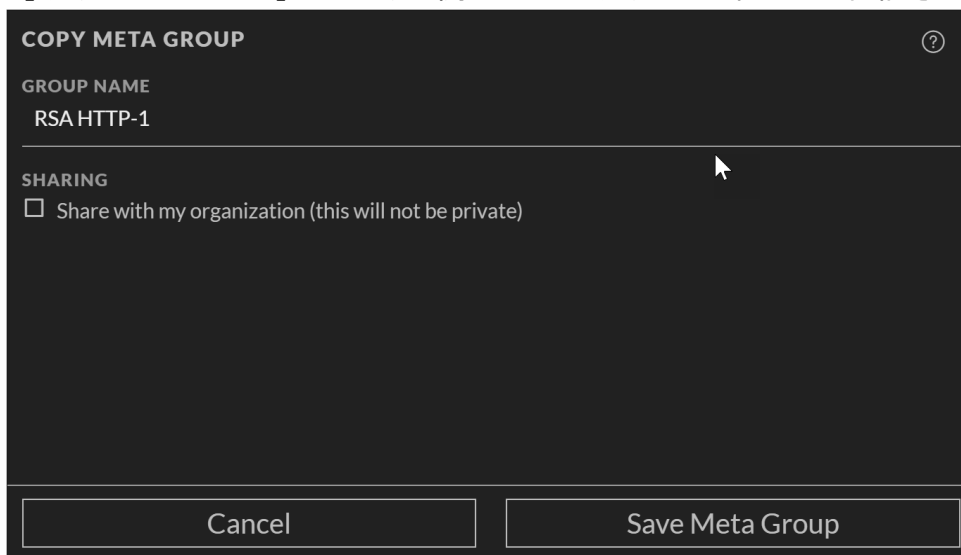
標準提供メタグループをハイライト表示した場合は、情報アイコン() が右側に表示されます。カスタムメタグループをハイライト表示した場合は、編集アイコン() が右側に表示されます。この図は、RSA HTTPがハイライト表示されていることを示しています。



3. 次のいずれかの操作を実行します。
 - a. 情報アイコン(📄)をクリックします。
 - b. 編集アイコン(✎)をクリックします。
[メタグループの詳細]ダイアログが表示されます。この図は、標準提供グループのダイアログを示しています。

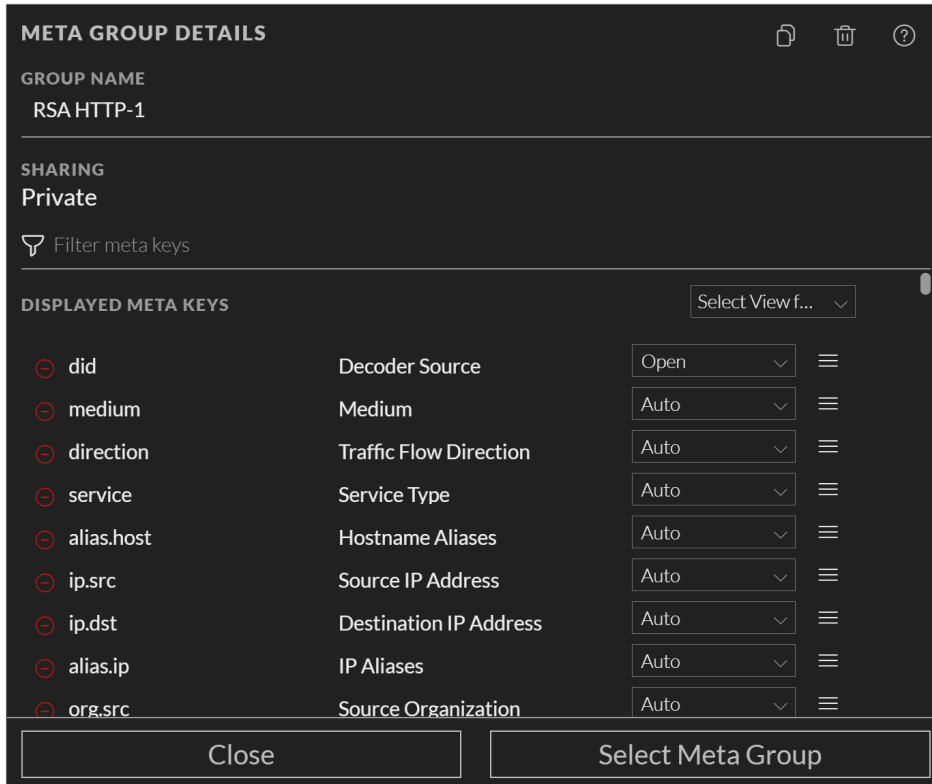


4. コピーアイコン(📄)をクリックします。
[メタグループのコピー]ダイアログが開き、元のメタグループ名に-nが付記されて表示されます。



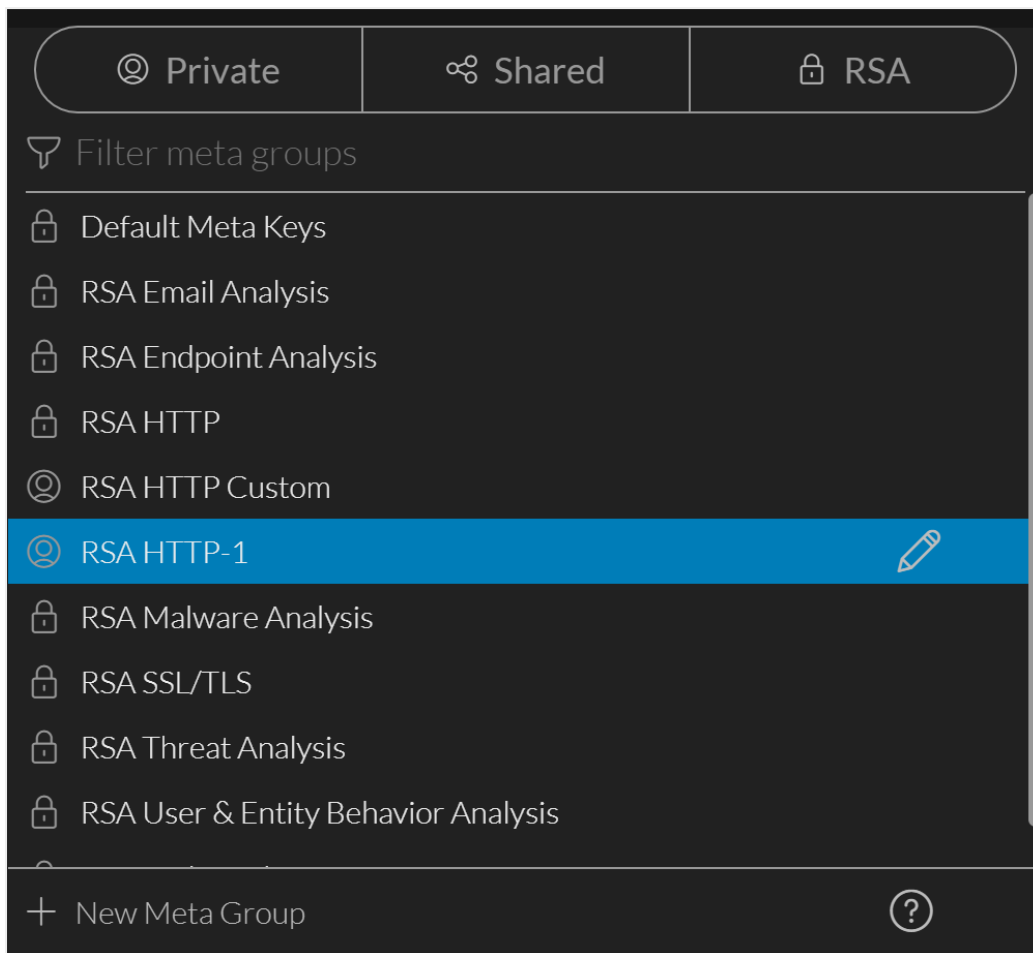
5. (オプション) [グループ名]フィールドで、メタグループの名前と場所を編集します。

6. 次のいずれかの操作を実行します。
 - a. グループをコピー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. メタグループのコピーを保存するには、**メタグループの保存**]をクリックします。
メタグループのコピーが保存され、コピーしたグループの **メタグループの詳細**]ダイアログが表示されます。



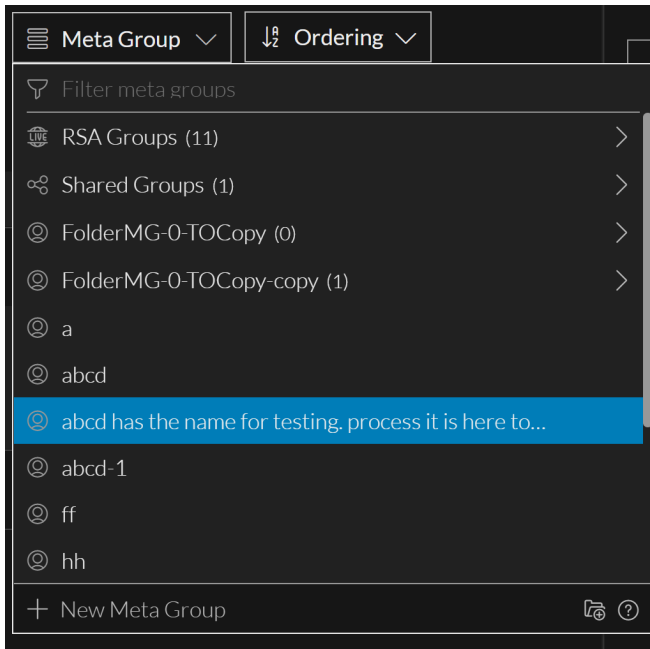
7. 次のいずれかの操作を実行します。
 - a. 編集しないでダイアログを閉じるには、**閉じる**]をクリックします。
 - b. ダイアログを閉じてメタグループのコピーを選択するには、**メタグループの選択**]をクリックします。
メタグループ]メニューにグループが追加されます。次の図は、RSA HTTPメタグループのプライ

ベート コピーを示しています。



メタグループフォルダ


ユーザは、編集可能な共有グループフォルダとプライベートグループフォルダを作成できます。プライベートグループフォルダとその内容は、RSAグループおよび共有グループフォルダの外部に表示されます。たとえば、次の画像は、共有グループフォルダの下位にあるプライベートコンテンツを示しています。

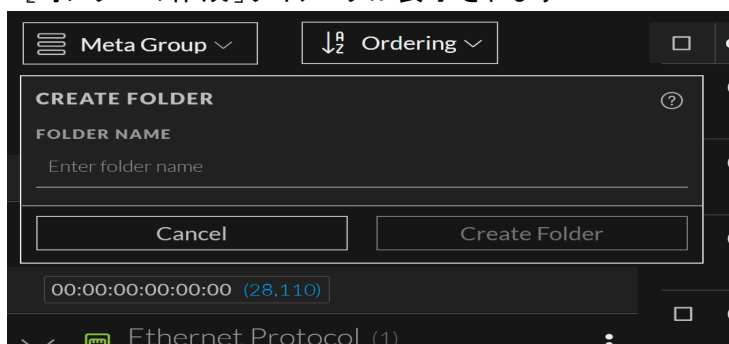


このセクションでは、カスタム メタ グループとフォルダを追加、編集、インポート、エクスポート、コピー、および削除する方法について説明します。

メタ グループ フォルダの作成

メタ グループ フォルダを共有フォルダおよびプライベート フォルダとして作成できます。また、フォルダ名がすでに存在する場合は、一意の名前を入力するように求められます。


1. [イベント]ビューで [イベントの絞り込み] パネルを開いた状態で、[メタ グループ] メニューの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て、メタ グループとフォルダのリストが表示されます。
2.  をクリックします。
[フォルダーの作成] ダイアログが表示されます。

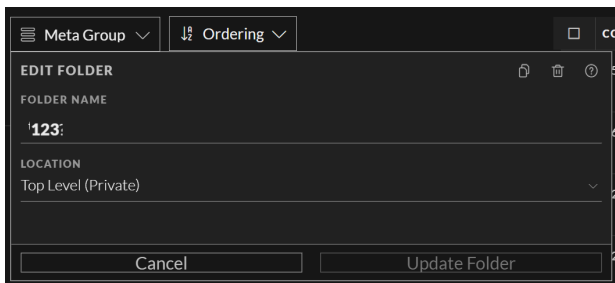


3. [フォルダ名] フィールドに、新しいメタ グループ フォルダの一意の名前を入力します。
4. [フォルダの作成] をクリックします。

メタ グループ フォルダの編集と移動

メタ グループ フォルダを作成した後、それを編集または移動できますが、RSAグループ(RSA LiveコンテンツおよびRSA OOTBグループ) 内のフォルダは編集も移動もできません。プライベート フォルダおよび共有フォルダ内のフォルダは、それぞれのグループ内でのみ編集および移動できます。たとえば、共有フォルダをプライベート フォルダに移動したり、その逆を行ったりすることはできません。



- 11.6の [イベント]ビューで [イベントの絞り込み] パネルを開いた状態で、[メタ グループ]メニュータイトルをクリックし、編集するメタ グループをハイライト表示します。
- をクリックします。
[フォルダの編集]ダイアログが表示されます。

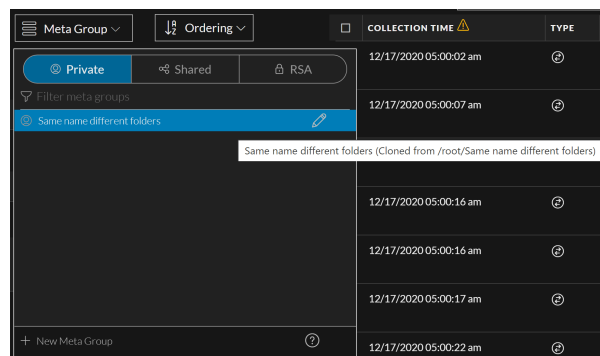


- [フォルダ名]フィールドに、メタ グループ フォルダの一意の名前を入力します。
- 編集するフォルダの場所を選択します。
- [フォルダの更新]をクリックします。

メタ グループ フォルダのコピー



ユーザは、RSA、共有、プライベートなど、あらゆるタイプのメタ グループ フォルダをコピーできます。ただし、RSAグループのデフォルトでは、コピー フォルダはプライベート セクション(ルート レベル)にコピーを作成しますが、フォルダの場所を共有フォルダまたはその他のプライベート フォルダに変更できます。クロー

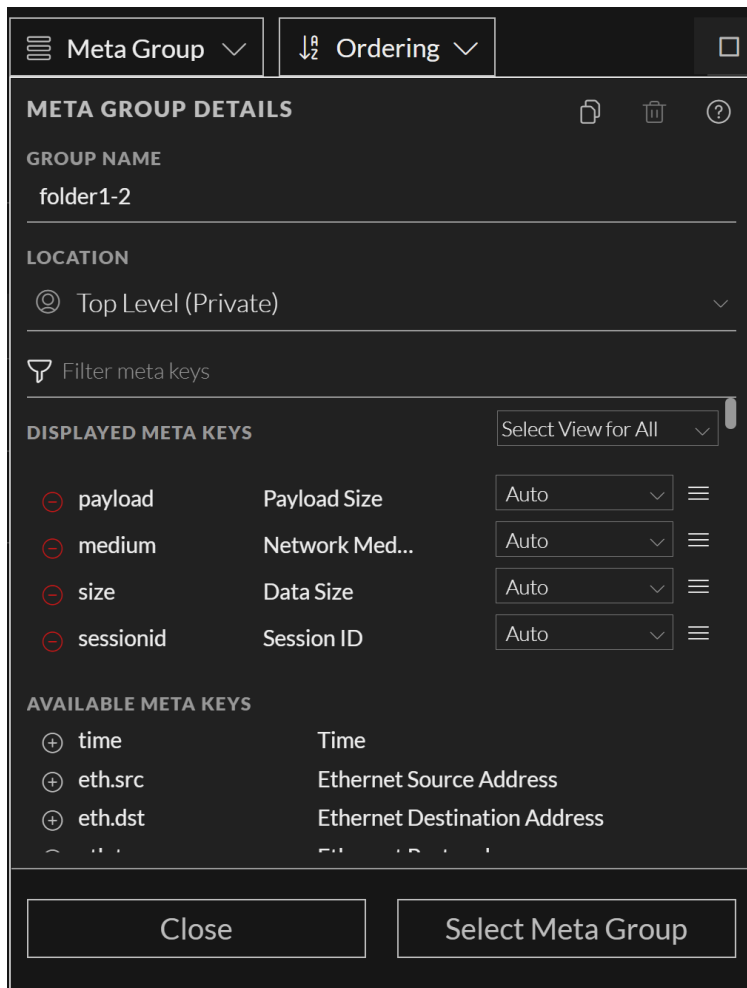
ンアイコン()をクリックすると、メタ グループをコピーできます。コピー後、メタ グループ フォルダは選択した場所([共有]または [プライベート]カテゴリ)に表示されます。コピーしたアイテムにカーソルを合わせると、メタ グループのコピー元のパスを示すツールチップが表示されます。特定のメタ グループを検索する必要がある場合は、フォルダレベルのフィルタ フィールド()にメタ グループの名前を入力すると、選択したフォルダからメタ グループがフィルタ処理されます。



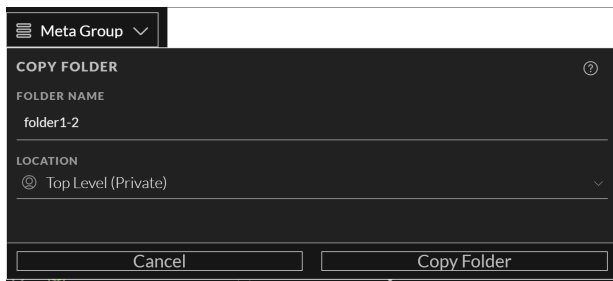
メタグループのプライベートフォルダまたは共有フォルダのコピー

メタグループフォルダを、RSAグループからプライベート、RSAグループから共有、プライベートから共有、プライベートからプライベート、共有から共有、共有からプライベートグループにコピーできます。フォルダをコピーすると、そのフォルダの内容はサブフォルダを除いてコピーされます。プライベートフォルダを共有フォルダにコピーすると、フォルダとその内容はプライベートのままではなくなります。

1. [イベント]ビューで [イベントの絞り込み] パネルを開いた状態で、[メタグループ]メニューの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て、メタグループとフォルダのリストが表示されます。
2. コピーするフォルダを選択します。
3. 編集  をクリックして、コピー  をクリックします。



[フォルダのコピー] ダイアログが表示されます。



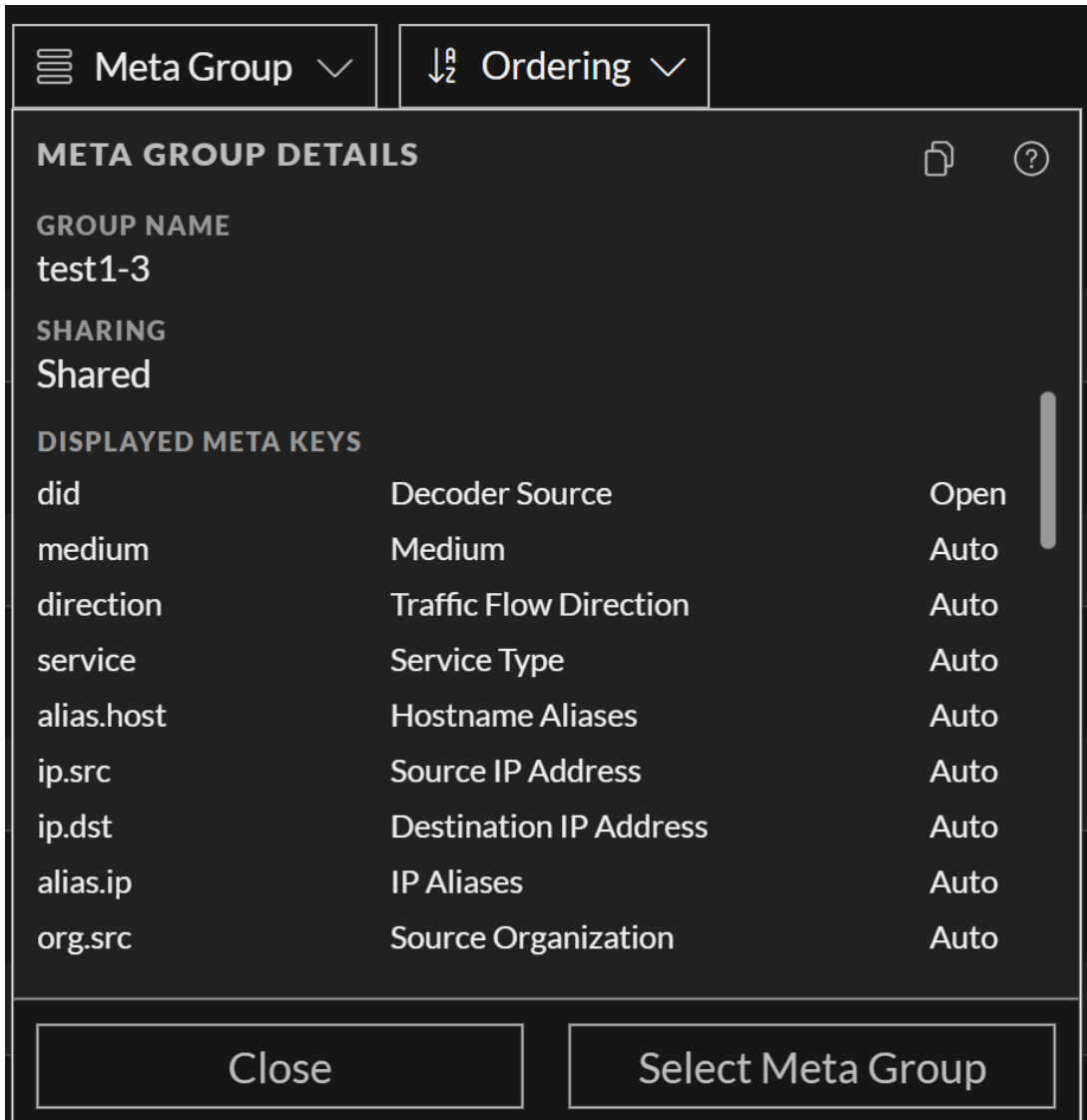
4. [フォルダ名] フィールドに、新しいメタグループフォルダの一意の名前を入力します。
5. コピーするフォルダの場所を選択します。
6. [フォルダのコピー] をクリックします。

Liveから導入されたメタグループフォルダのコピー

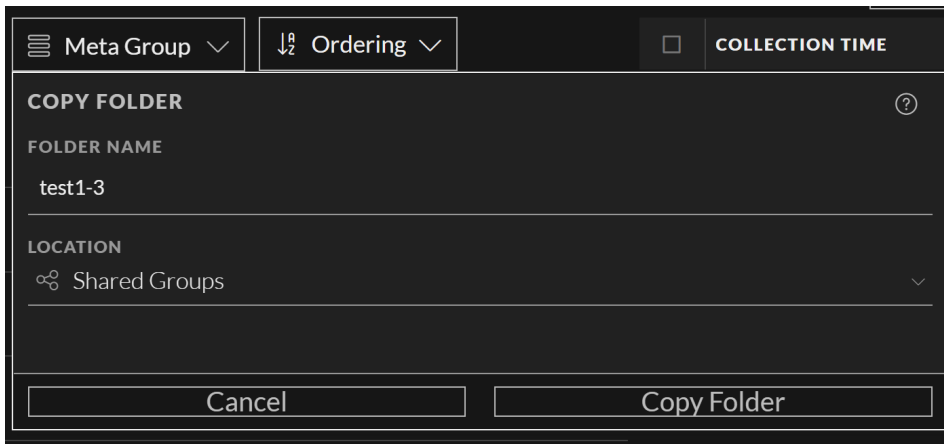
RSA Groupsカテゴリーの下にあるLiveから導入されたメタグループフォルダを、共有グループなどの他の場所またはプライベートフォルダにコピーできます。

1. [イベント] ビューで [イベントの絞り込み] パネルを開いた状態で、[メタグループ] メニューの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て、メタグループとフォルダのリストが表示されます。
2. RSAグループをクリックし、コピーするLiveメタグループフォルダを選択します。

3. ⓘ をクリックして、コピー 📄 をクリックします。




[フォルダのコピー] ダイアログが表示されます。

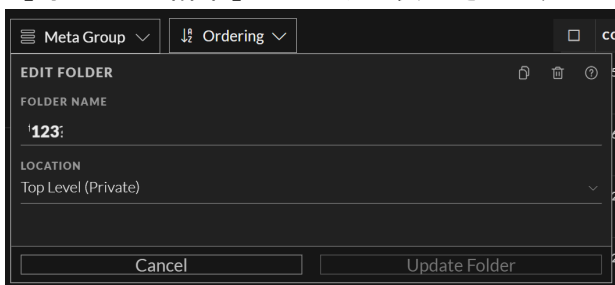


4. コピーするフォルダの場所を選択します。
5. [フォルダのコピー]をクリックします。
フォルダーと第1レベルの内容がコピーされ、サブフォルダーはコピーされません。コピーされたメタグループフォルダーとその内容が、元のメタグループ名に-nが付記された名前が表示されます。

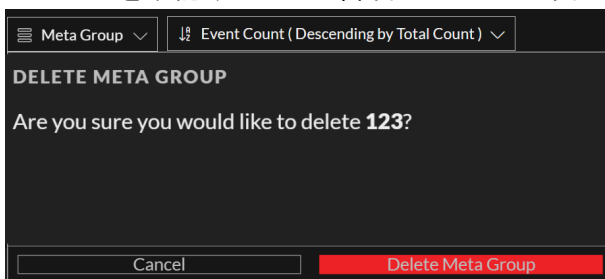
メタグループフォルダの削除

保持したくないフォルダは削除できます。ただし、フォルダを削除すると、そのフォルダを取得できなくなります。

1. [イベント]ビューで [イベントの絞り込み] パネルを開いた状態で、[メタグループ]メニューの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て、メタグループとフォルダのリストが表示されます。
2. 削除するフォルダを選択します。
3. 編集  をクリックします。
[フォルダーの編集]ダイアログが表示されます。



4. 削除  をクリックします。
アクションを確認するための警告メッセージが表示されます。



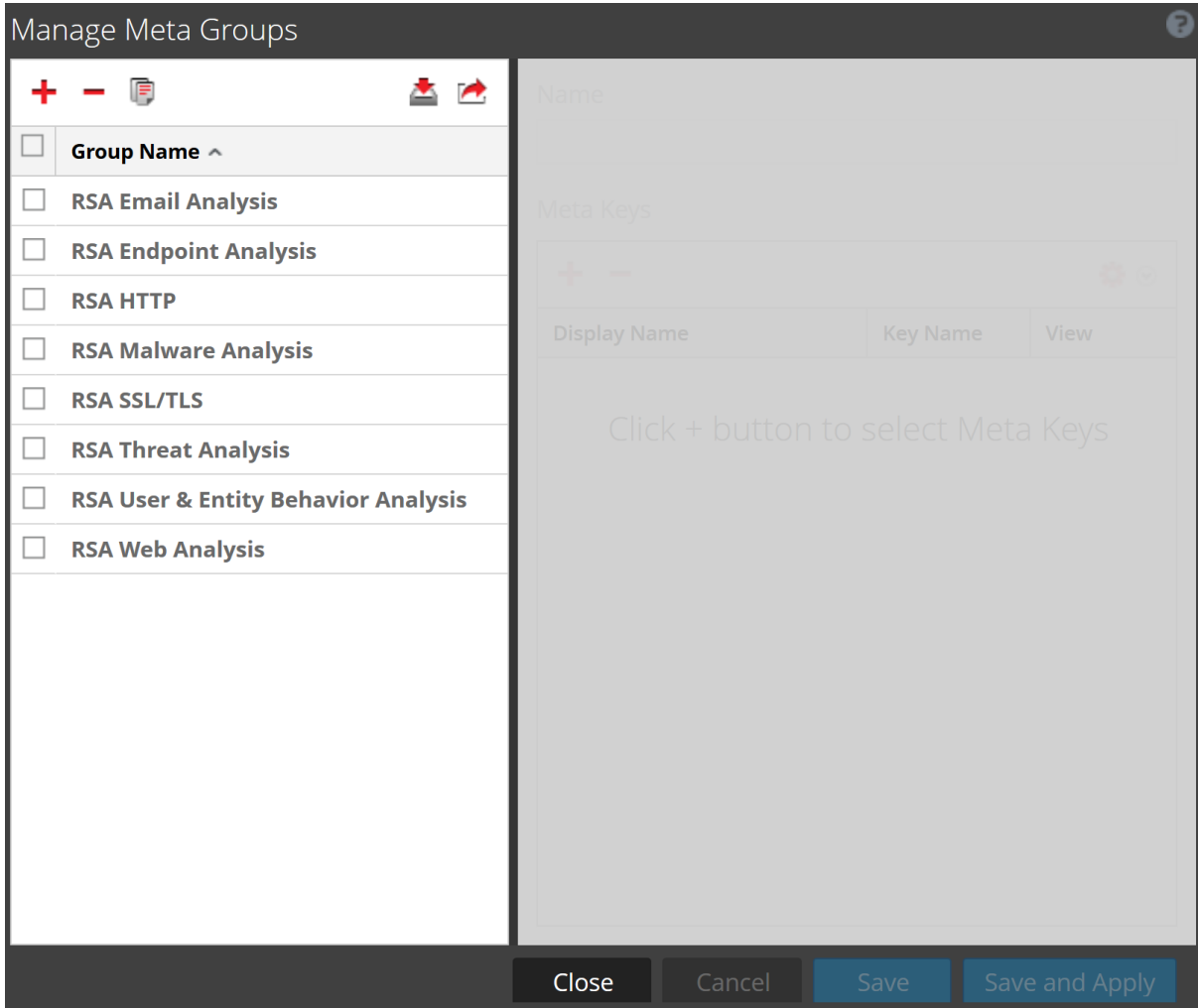
5. (オプション) 選択したフォルダ内のすべてのコンテンツとともにフォルダを削除する場合は、このチェックボックスを選択します。
チェックボックスを選択しないと、必要なフォルダが削除された後で、コンテンツは親フォルダに移動されます。
6. [OK]をクリックして削除します。

「ナビゲート」ビューでのメタグループの操作

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。最初は標準提供グループのみがサービス用に構成され、グループ名の下に一覧表示されています。他のカスタムグループが構成されると、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。

Manage Meta Groups

Group Name ^

RSA Email Analysis

RSA Malware Analysis

RSA Query Hosts

RSA Query IPs

RSA Query Mail



RSA Query Users

RSA Threat Analysis

RSA Web Analysis

Name

Meta Keys

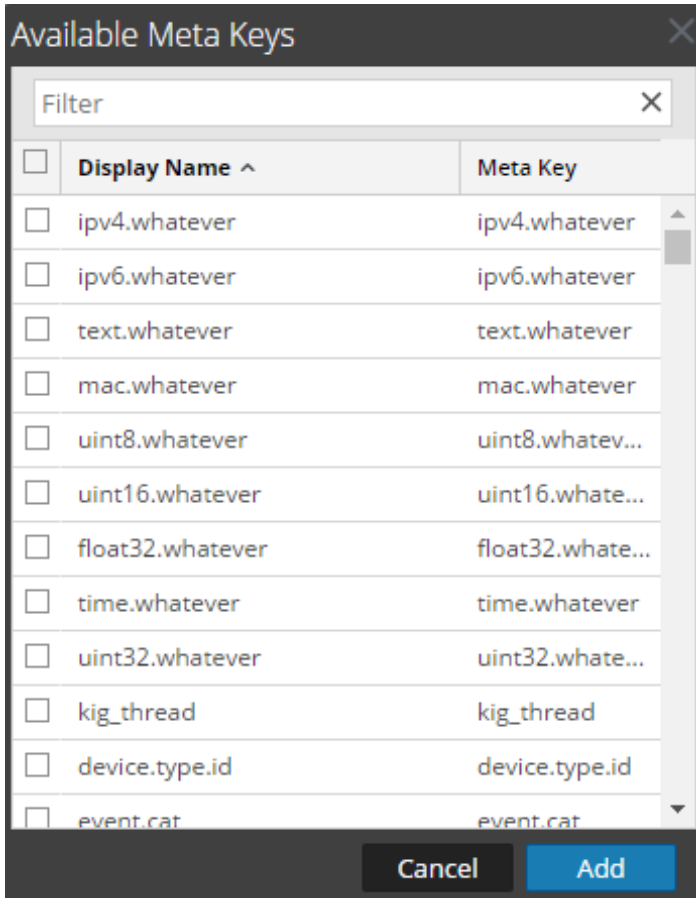
+ -  

Display Name	Key Name	View
Click + button to select Meta Keys		

Close Cancel Save Save and Apply

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] 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。
- 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。
 - 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。

メタグループのコピーと編集

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。



Manage Meta Groups

Group Name ^

- RSA Email Analysis 2
- RSA Malware Analysis 2
- RSA Threat Analysis 2
- RSA Web Analysis 2
- newgourp2
- newgroup
- test
- RSA Email Analysis
- RSA Malware Analysis
- RSA Query Hosts
- RSA Query IPs
- RSA Query Mail
- RSA Query Users
- RSA Threat Analysis
- RSA Web Analysis

Name

Meta Keys

+ -
 

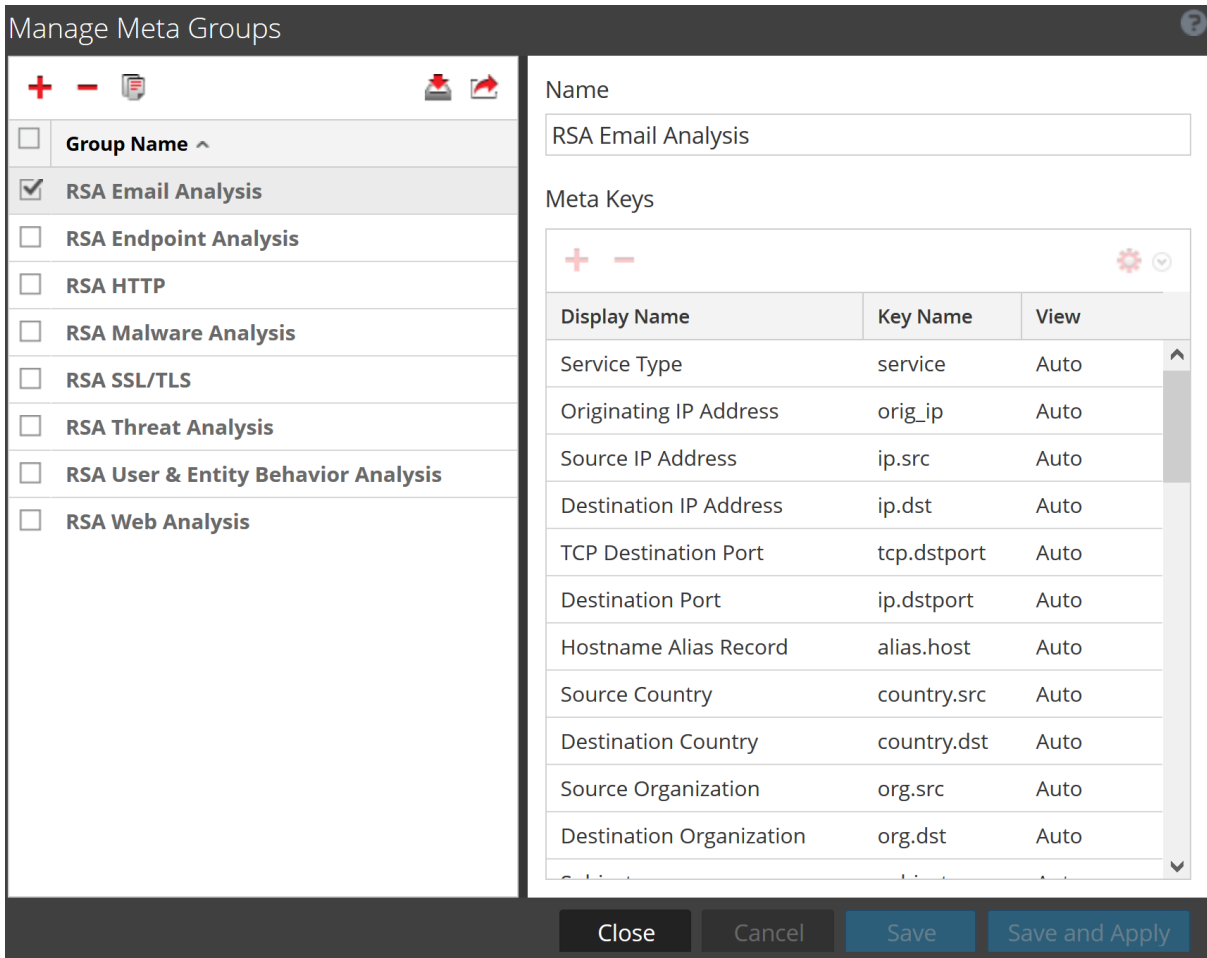
Display Name	Key Name	View
Service Type	service	Auto
Originating IP Address	orig_ip	Auto
Source IP Address	ip.src	Auto
Destination IP address	ip.dst	Auto
TCP Destination Port	tcp.dstport	Auto
Destination Port	ip.dstport	Auto
Hostname Aliases	alias.host	Auto
Source Country	country.src	Auto
Destination Country	country.dst	Auto
Source Organization	org.src	Auto
Destination Organization	org.dst	Auto



Close
Cancel
Save
Save and Apply

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。


カスタムメタグループの編集

1. [メタグループ]リストからカスタム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。




- (オプション) グループの [名前] を編集します。
- (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。
- (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。
- (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。
- 変更を保存するには、**保存**]をクリックします。
- 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。

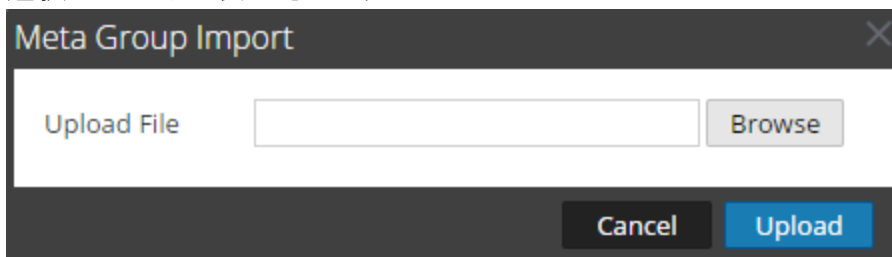
1. [メタグループ]リストで、エクスポートするグループを1つ以上選択します。
2.  をクリックします。
選択したグループがMetaGroups.jsonというファイル名で、ローカルファイルシステムにダウンロードされます。ダウンロード先に以前ダウンロードした同名のファイルが存在する場合は、上書きを避けるため、ファイル名に数字が付加されます。

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.json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.json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。

COLLECTION TIME	TYPE	THEME	SIZE	SUMMARY
12/04/2019 06:04:51 am	1 [Network]	80 [HTTP]	745 bytes	ip.src = 172.24.0.11 ip.dst = 172.24.0.22 tcp.srcport = 50104 tcp.dstport = 40718 service = 80 [HTTP]

COLLECTION TIME	TYPE	SERVICE TYPE	ORIGINATING IP ADDRESS	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	TCP DESTINATION PORT	DESTINATION PORT	HOSTNAME ALIASES	SOURCE COUNTRY	DESTINATION COUNTRY	SERVICE TYPE
12/04/2019 06:04:51 am	1 [Network]	80 [HTTP]		172.24.0.11	172.24.0.22	40718					

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。どのメタ キーが重要かわかっている場合は、手動で簡単に調整できます。手動調整は、バージョン11.5の現在のセッションにのみ適用されます。バージョン11.5.1では、列幅は例外です。調整した列幅は個人設定として保持され、[イベント] リストで列が使用されるたびに適用され、デフォルトの列幅が上書きされます。

バージョン11.6では、表示しているメタ キーのデータを含む追加の列を選択できます。これにより、[イベントの絞り込み] パネルから関連するすべてのメタ キー情報を取得できますが、推奨事項は選択したメタ グループに基づいて変更される場合があります。次の図は、推奨メタ キー セクションの下の追加のメタ キー情報を示しています。

COLLECTION TIME	TYPE	DECODER SOURCE	MEDIUM	TRAFFIC FLOW DIRECTION	SERVICE TYPE	HOSTNAME ALIASES	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	IP ALIASES	SOURCE ORGANIZATION	DESTINATION ORGANIZATION	SOURCE COUNTRY
2016/04/07 03:45:23	Decoder	DA829301	1 [Network]	lateral	443 [SSL]	EC2AMAZ-UNAHUCV0	70.140.23.5	172.24.221.187	180.51.26.47	XYZ Corporation	XYZ Corp	United States
2016/04/07 03:45:45	Decoder	DA829301	1 [Network]	lateral	0 [OTHER]	EC2AMAZ-UNAHUCV0	172.24.221.187	157.44.28.140	56.33.169.186	ABC Organization	ABC Org	United States
2016/04/07 03:45:56	EndpointLogHybrid...	32 [Endpoint]	outbound			EC2AMAZ-UNAHUCV0	70.140.23.5	78.97.233.182	98.187.83.217	XYZ Corporation	ABC Org	United States
2016/04/07 03:47:12	LogDecoder-DA82...	32 [Log]				EC2AMAZ-UNAHUCV0	172.24.221.187	79.146.185.178	155.241.12.67	XYZ Corporation	XYZ Corp	United States
2016/04/07 03:48:07	Decoder-DA829301	1 [Network]	lateral	0 [OTHER]	EC2AMAZ-UNAHUCV0	EC2AMAZ-UNAHUCV0	172.24.221.187	70.140.23.5	236.232.86.10	XYZ Corporation	XYZ Corp	United States
2016/04/07 03:50:45	EndpointLogHybrid...	32 [Endpoint]	outbound			EC2AMAZ-UNAHUCV0	128.251.33.240	144.241.158.83	106.225.149.249	XYZ Corporation	ABC Org	United States
2016/04/07 03:52:56	LogDecoder-DA82...	32 [Log]				EC2AMAZ-UNAHUCV0	70.140.23.5	142.75.98.251	10.10.188.236	ABC Organization	ABC Org	United States
2016/04/07 03:53:41	Decoder-DA829301	1 [Network]	lateral	443 [SSL]	EC2AMAZ-UNAHUCV0	EC2AMAZ-UNAHUCV0	70.140.23.5	172.24.221.187	137.80.72.65	XYZ Corporation	XYZ Corp	United States
2016/04/07 03:54:16	LogDecoder-DA82...	32 [Log]				EC2AMAZ-UNAHUCV0	172.24.221.187	172.24.221.187	131.92.254.246	ABC Organization	XYZ Corp	United States
2016/04/07 03:55:32	Decoder-DA829301	1 [Network]	lateral	443 [SSL]	EC2AMAZ-UNAHUCV0	EC2AMAZ-UNAHUCV0	70.140.23.5	95.227.214.103	214.232.238.47	XYZ Corporation	XYZ Corp	United States
2016/04/07 03:55:59	Decoder-DA829301	1 [Network]	lateral	0 [OTHER]	EC2AMAZ-UNAHUCV0	EC2AMAZ-UNAHUCV0	98.187.83.217	172.24.221.187	97.181.183.141	XYZ Corporation	XYZ Corp	United States
2016/04/07 03:56:01	EndpointLogHybrid...	32 [Endpoint]	outbound			EC2AMAZ-UNAHUCV0	172.24.221.187	88.364.93	128.251.33.240	ABC Organization	XYZ Corp	United States
2016/04/07 03:56:16	LogDecoder-DA82...	32 [Log]				EC2AMAZ-UNAHUCV0	70.140.23.5	145.195.139.31	71.212.157.113	ABC Organization	ABC Organization	United States
2016/04/07 03:56:33	Decoder-DA829301	1 [Network]		443 [SSL]	EC2AMAZ-UNAHUCV0	EC2AMAZ-UNAHUCV0	172.24.221.187	99.221.9.235	244.101.28.21	XYZ Corporation	XYZ Corporation	United States
2016/04/07 03:57:02	LogDecoder-DA82...	32 [Log]				EC2AMAZ-UNAHUCV0	128.251.33.240	172.24.221.187	122.183.36.252	XYZ Corporation	XYZ Corporation	Madagascar

[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。列グループには少なくとも1つの列が必要です。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)。

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。 [イベント]ビューで作成されたプライベート列グループは、 [レガシー イベント]ビューまたは [ビゲート]ビューのクエリプロファイルで使用できません。

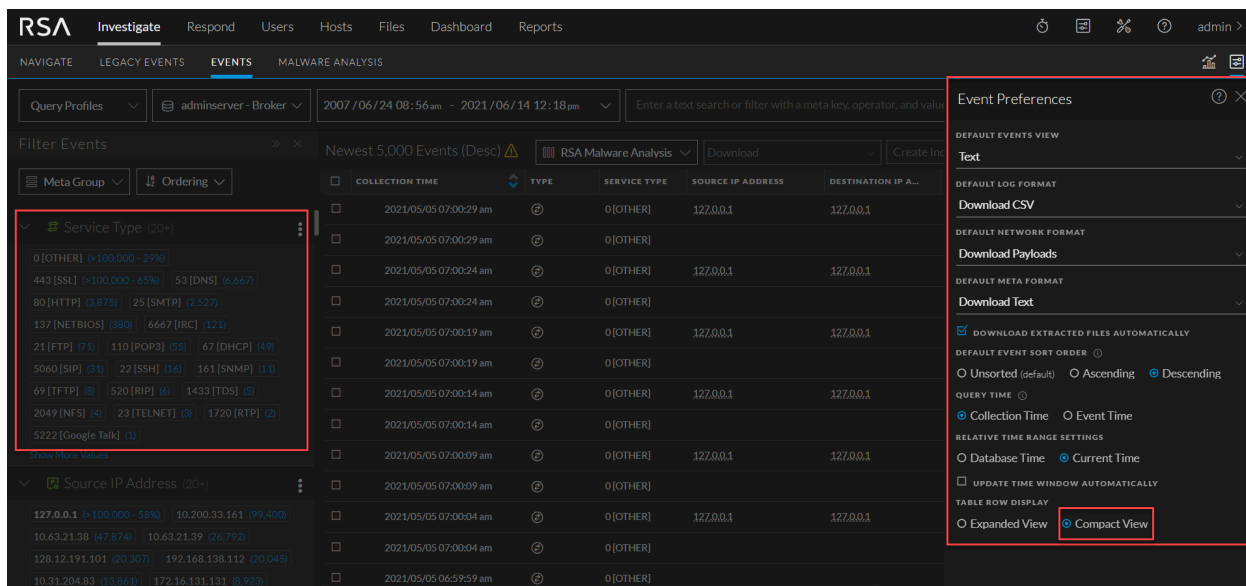
注： [ビゲート]ビューと [レガシー イベント]ビューでは、インデックスなしのメタ キー(またはインデックスにまったく含まれていないキー)をメタ グループまたは列グループに手動で追加できます。インデックスなしのメタ キーは、 [ビゲート]ビューと [レガシー イベント]ビューでは完全に使用可能(管理および表示可能)ですが、 [イベント]ビューでは部分的にのみ使用可能([イベントの絞り込み]パネルに表示可能)です。 [イベント]ビューの [イベントの絞り込み]パネルには、メタ グループにすでに含まれているインデックスなしのメタ キーのデータを表示できますが、メタ グループの編集集中にインデックスなしのメタ キーを追加することはできません。列グループ内のインデックスなしのメタ キーは列にデータを表示せず、新しいインデックスなしのメタ キーを [イベント]ビューの列グループに追加することはできません。

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です(デフォルトのメタ キーがいくつか含まれているため、40個を超えるメタ キーが画面に表示される場合があります)。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。

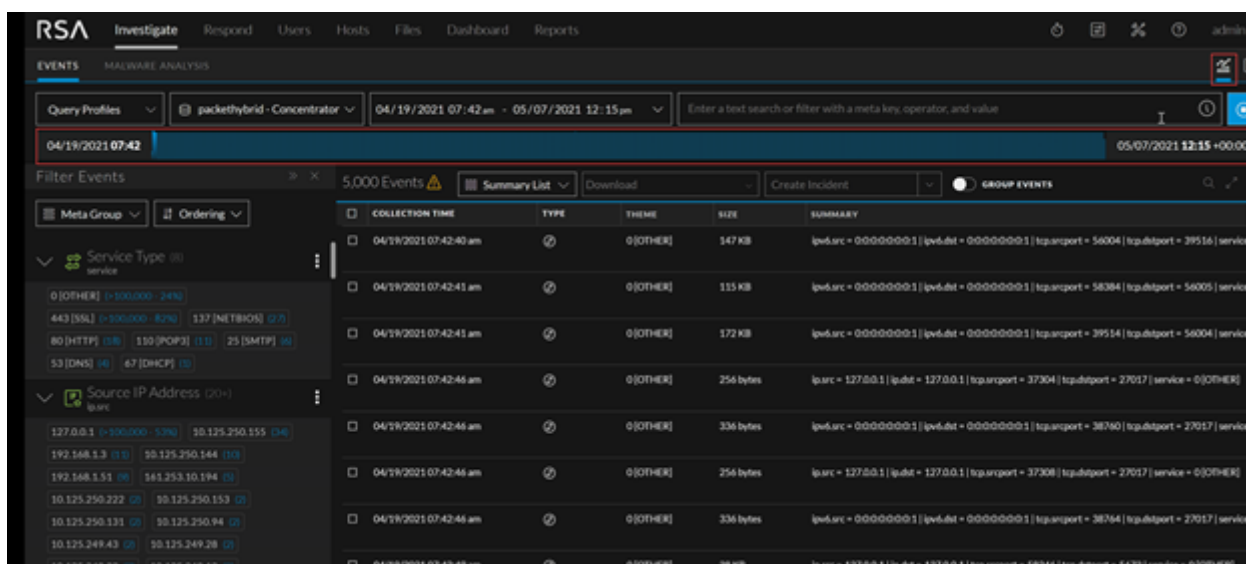
[レガシー イベント]ビューには、列グループ内のメタ キーの数の制限がなく、40個を超えるメタ キーを列グループに含めることができます。 [レガシー イベント]ビューで作成された40個を超えるメタ キーを含む列グループを適用すると、すべての列が [イベント]ビューにロードされます。500個を超える列を持つグループをコピーする場合は、列グループの編集時に余分な列を削除する必要があります。

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せん。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。バージョン11.5では、クローニングも [イベント]ビューで使用できますが、インポートとエクスポートは使用できません。

11.6.1では、スペースを最適に利用してアナリストが分析中のイベントに関連する詳細を最大限に表示できるように、 [調査] > [イベント環境設定]ビューが追加されました。

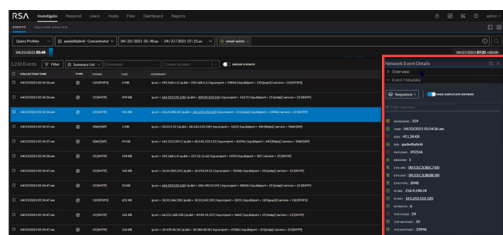


さらに、🕒アイコンをクリックしてイベントのタイムラインの詳細を表示できるようになりました。図に示すように、表示されたタイムラインをクリックすると、日付と時刻の範囲が表示されます。

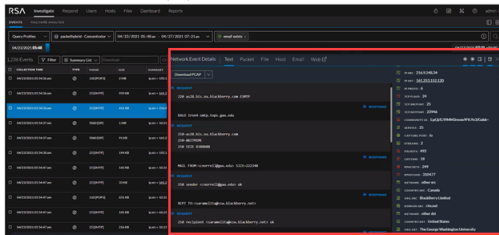


調査] > [イベントの再構築]パネルが変更され、展開と折りたたみが可能な 概要]タブと [タ]パネルタブを含むオーバーレイが表示されるようになりました。これにより、アナリストはイベントのヘッダーとメタパネルを最適に表示できます。重複イベントを表示しない]オプションを切り替えて、選択したイベントに関連する詳細のみを表示することもできます。

アナリストがこのページに移動すると、次のビューが表示されます。



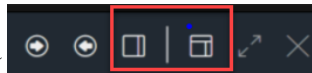
トグルボタン(☐)を使用して、選択したイベントに関連する詳細を表示できます。



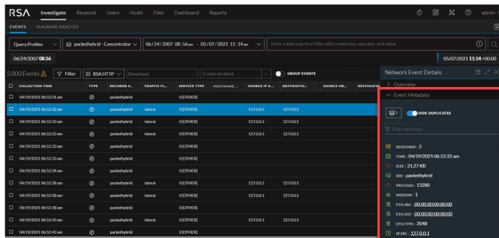
双眼鏡アイコンは、選択したイベントに関連する検索に対してイベント ペイロードが開いている場合にのみ有効になります。

概要]タブには特定のイベントに関連するすべてのヘッダーが表示され、[イベント メタデータ]パネルには選択したイベントに関連するすべてのメタデータが表示されます。

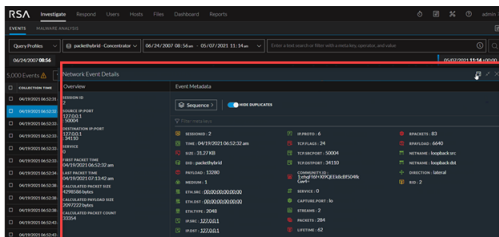
11.7では、メタパネルを開いて選択したイベントの詳細を表示すると、使用可能なすべてのヘッダーが



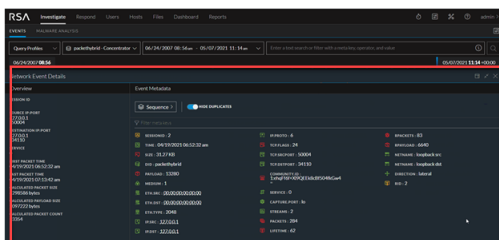
表示されます。メタパネルには 展開]ボタン(☐)があります。イベントをクリックすると、メタパネルが表示されます。表示する追加のヘッダーがない場合は、ヘッダー エラーに関するエラーが表示されます。



展開オプションを使用して、3つの異なるビューでメタパネルを拡大表示できます。外向きの矢印をクリックすると、概要]パネルと[イベント メタデータ]パネルに表示されるすべての詳細が展開されます。

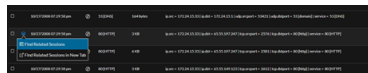


もう一度クリックすると、拡大表示されます。



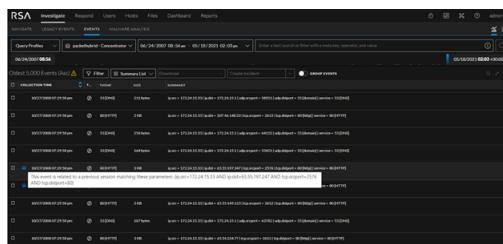
内向きの矢印のアイコン(☐)をクリックすると画面表示を元に戻すことができ、ウィンドウが前の位置に戻ります。これにより、各イベントの詳細を最適な方法で表示できます。

調査の一環として、特定のイベントに関連するセッションを検索できます。関連するセッションを検索するには、**調査**] > **イベント**] ページに移動します。アイコンをクリックし、ドロップダウンから **関連セッションを検索**] オプションまたは **新しいタブで関連セッションを検索**] オプションを選択します。



関連セッションを検索] オプションを選択すると、選択したイベントのクエリに一致するすべてのイベントが現在のウィンドウに表示されます。**新しいタブで関連セッションを検索**] オプションを選択すると、結果が新しいタブに表示されます。これにより、関連する各セッションについてさらに調査を行うことができます。

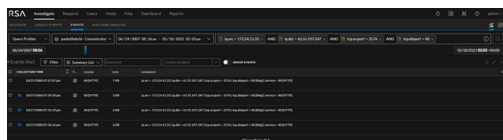
クエリは、イベントにカーソルを合わせると表示されるテキストの情報に基づきます。たとえば、次の図では、イベントに2つの分割セッションがあり、1つのイベントが別のセッションに分割されています。



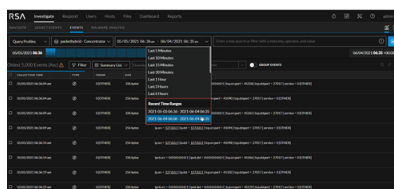
このケースでは、これらのパラメーターで検索を実行すると、次のクエリについての関連セッションが表示されます。



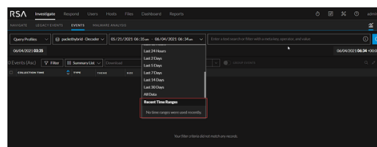
結果は次の形式で表示されます。



時間範囲の選択内容は保存されて **最近の時間範囲**] セクションに表示されるため、アナリストは最近使用した時間範囲を過去5つまで確認できます。ユーザーの選択内容はサービスごとに個別に保存されます。たとえば、Concentratorサービスの時間範囲として過去30日間を選択した場合、Concentratorの **最近の時間範囲**] セクションにエントリが作成され、次のセッションで同じサービスを選択したときに時間範囲が次のように表示されます。

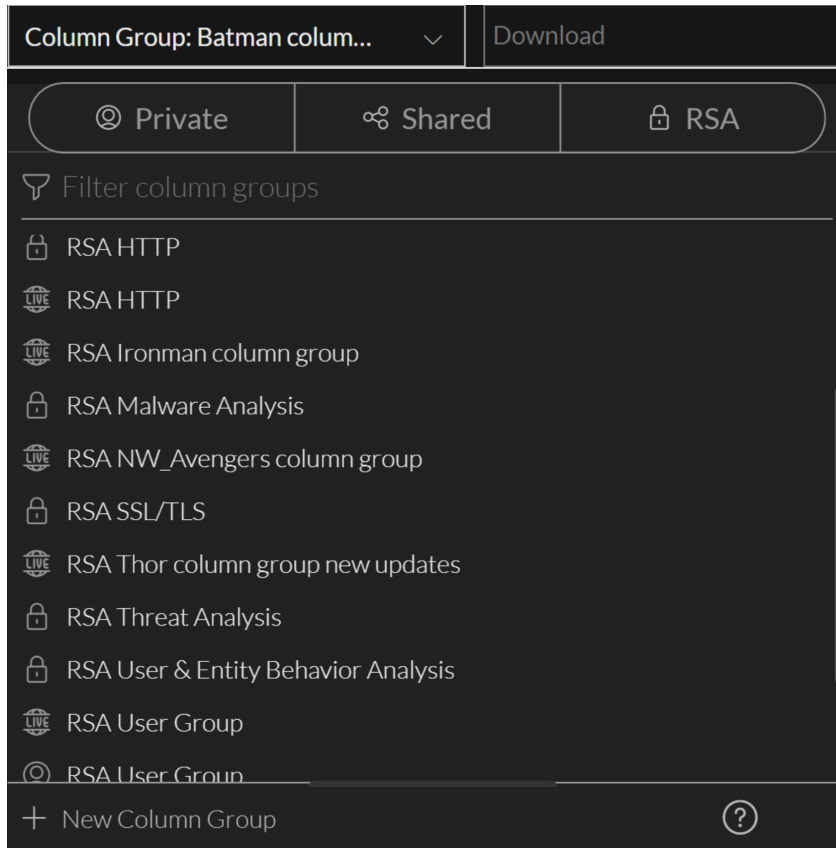


ここで、Decoderサービスを選択した場合、Decoderの詳細を最近表示していなければ、次に示すように時間範囲のドロップダウンに詳細は表示されません。




標準提供の列グループ

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。



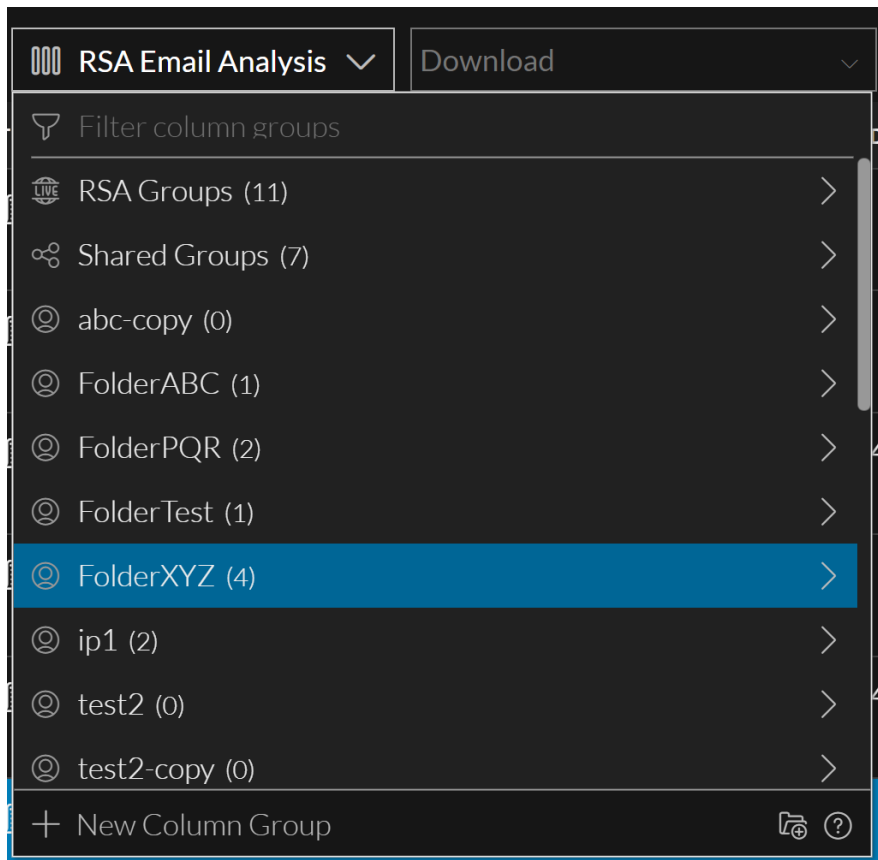
[レガシー イベント]ビューでは、標準提供の列グループの名前は「RSA」で始まります。[イベント]

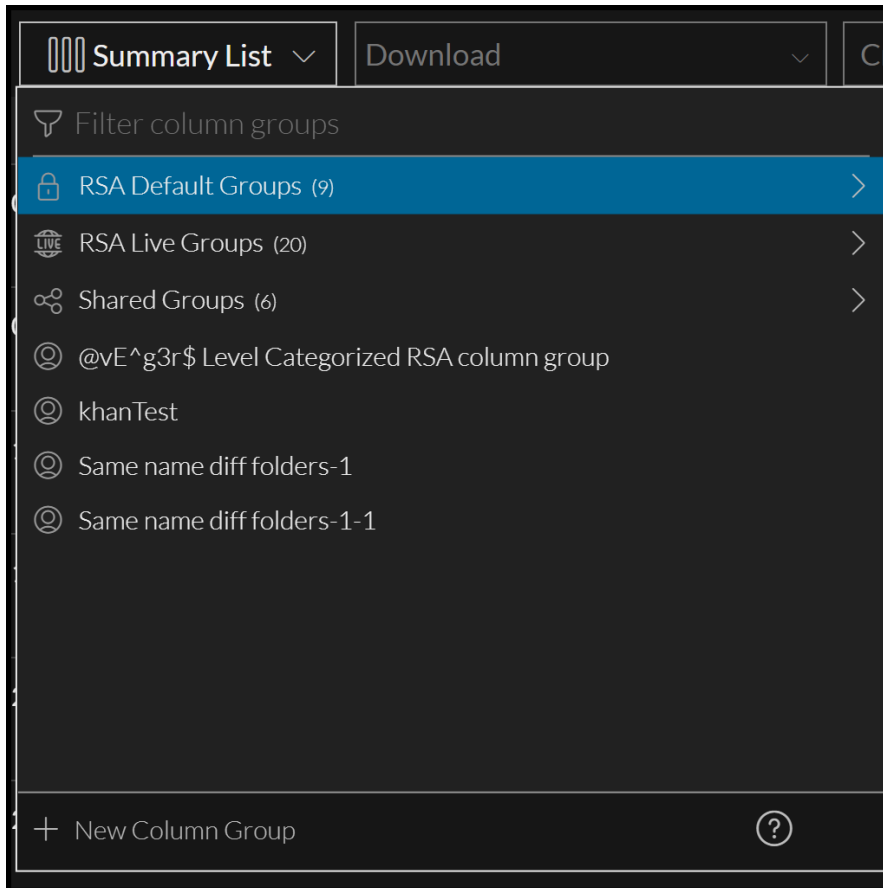
ビュー(バージョン11.4以降)では、名前が「RSA」で始まり、ロック記号()が表示されます。これは、[列グループ]メニューで選択した標準提供の列グループの例です。行の最後に情報アイコンが表示されます。

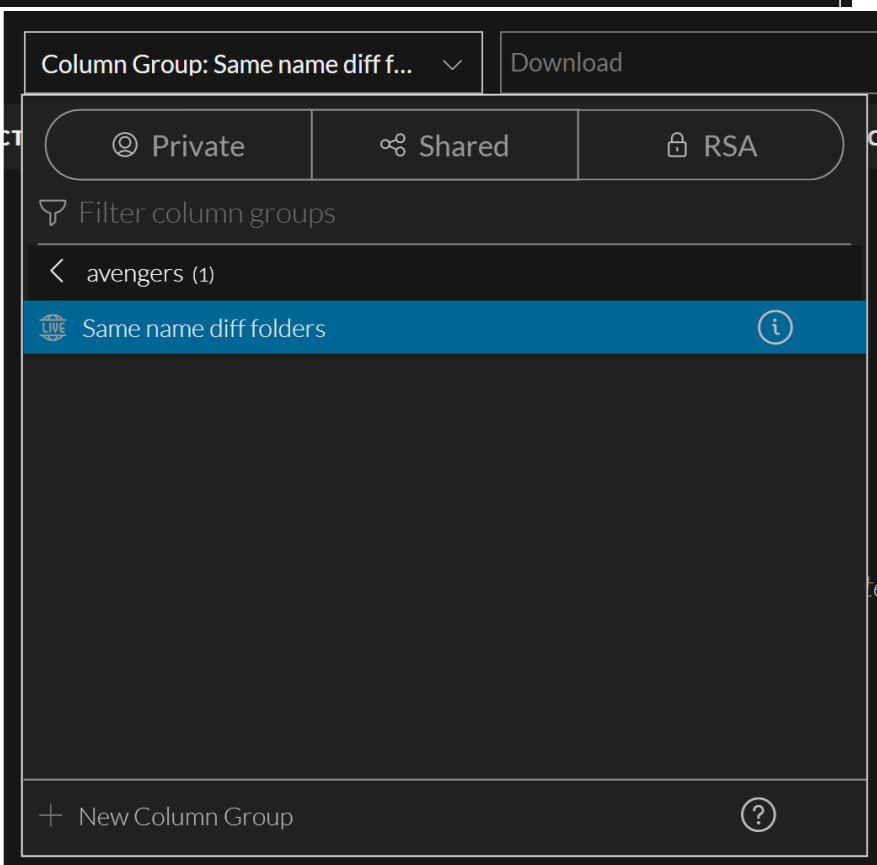
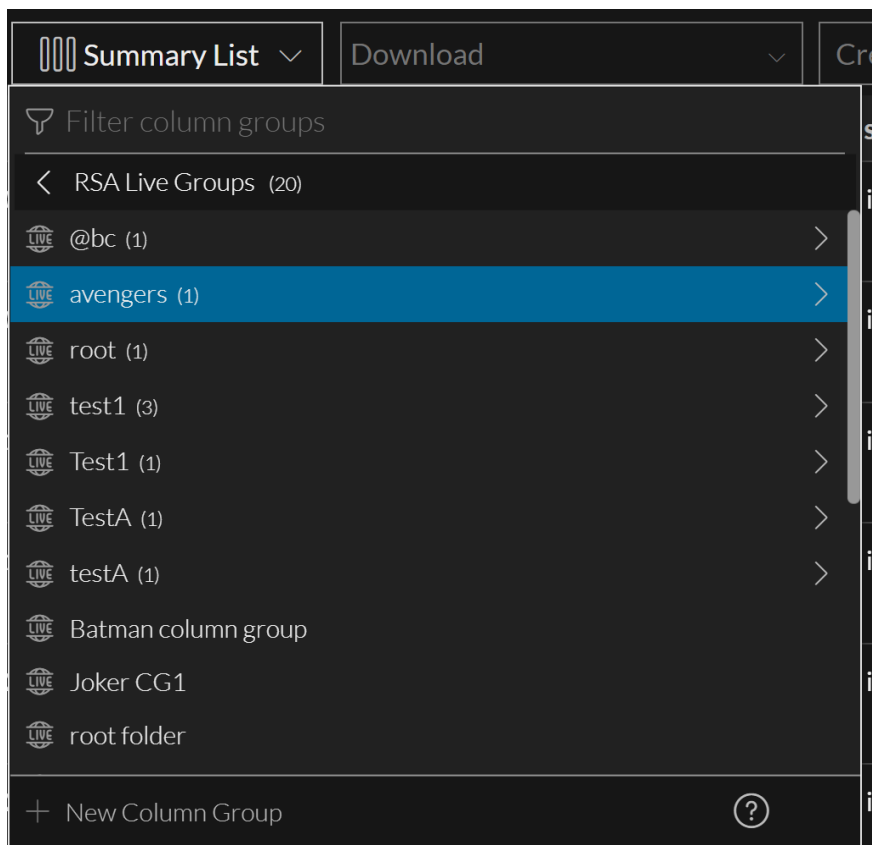



Live列グループ


11.6以降では、NetWitness Platformは、Liveからの調査コンテンツの導入をサポートしています。これらのコンテンツは、Live記号(())でマークされて表示されます。列グループは、RSAグループ(RSA LiveコンテンツおよびRSA OOTBグループ)と共有グループに分類されます。グループは、編集可能な共有グループを除いて、編集不可能なフォルダおよびサブフォルダとして表示されます。プライベートコンテンツはすべて、これらのグループの外部に表示されます。たとえば、次の画像は、共有グループフォルダの下位にあるプライベートコンテンツを示しています。()内の数字はフォルダ内のコンテンツの数を示し、>記号はフォルダ内をドリルダウンするために使用されます。

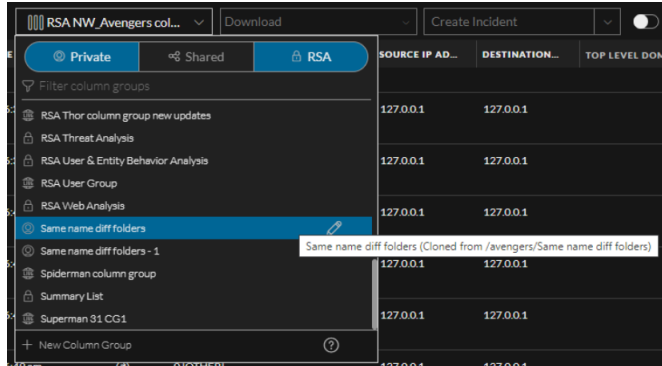






列グループをコピーするには、コピーアイコン() をクリックします。コピー後、コピーされた列グループは選択した場所(プライベートフォルダーまたは共有グループ)に表示されます。クローニングされたアイテムにカーソルを合わせると、列グループのクローニング元のパスを表示するツールチップが表示されます。

特定の列グループを検索する必要がある場合は、フォルダーレベルのフィルタフィールド() に列グループの名前を入力します。



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 HTTP** :HTTP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 SSL/TLS** :SSL/TLS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 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データを調査するときに役立つメタ 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

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。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新しいメタグループが列グループで利用可能になります。

バージョン11.4では、カスタム列グループが組織内でグローバルに共有されます。共有の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。共有の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。バージョン11.5以降では、共有列グループを以前と同様に作成できます。また、プライベート列グループを作成することもできます。バージョン11.5では、グループを作成する時に、共有するかプライベート(デフォルト)にするか選択できます。共有グループをプライベートに変更したり、プライベートグループを共有に変更することはできません。

注： [イベント]ビューで作成されたプライベート列グループは、[レガシー イベント]ビューで表示または使用できません。

列グループ]メニューでは、グループタイプはアイコンで識別されます。次の図は、行の最後に編集アイコンが表示された各カスタム列グループタイプの例です。



フォルダのフィルタ処理

フォルダが多い場合は、フォルダ名を入力して、特定のフォルダに絞り込むことができます。フィルタ処理は現在のレベルのフォルダに適用可能であり、サブフォルダ内で使用可能なフォルダは表示されません。サブフォルダ内のコンテンツを検索するには、特定のフォルダに移動してフィルタ処理する必要があります。

また、特定のフォルダを選択すると、選択したフォルダの内容が表示され、フィルタフィールドが空になります。フィルタフィールドに戻ると、最後に選択したフォルダが表示されます。次の例では、選択されたフォルダはその内容を含むRSAグループであり、列グループのドロップダウンにはフィルタ処理された要約リストフォルダが表示されます。

COLLECTION TIME	STATUS	DATA
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes
01/21/2021 05:04:30 am	0 [OTHER]	256 bytes

COLLECTION TIME	TYPE	THEME	SIZE	SUMMARY
01/21/2021 12:39:01 pm	⊕	0 [OTHER]	256 bytes	ip.src = 127.0.0.1 ip.dst = 127.0.0.1 tcp.srcport = 38062 tcp.dstport = 27017 service = 0 [OTHER]
01/21/2021 12:39:06 pm	⊕	0 [OTHER]	256 bytes	ip.src = 127.0.0.1 ip.dst = 127.0.0.1 tcp.srcport = 38064 tcp.dstport = 27017 service = 0 [OTHER]
01/21/2021 12:39:11 pm	⊕	0 [OTHER]	256 bytes	ip.src = 127.0.0.1 ip.dst = 127.0.0.1 tcp.srcport = 38066 tcp.dstport = 27017 service = 0 [OTHER]
01/21/2021 12:39:15 pm	⊕	0 [OTHER]	1 KB	ip.src = 127.0.0.1 ip.dst = 127.0.0.1 tcp.srcport = 52444 tcp.dstport = 4369 service = 0 [OTHER]
01/21/2021 12:39:16 pm	⊕	0 [OTHER]	1 KB	ip.src = 127.0.0.1 ip.dst = 127.0.0.1 tcp.srcport = 55409 tcp.dstport = 4369 service = 0 [OTHER]
01/21/2021 12:39:16 pm	⊕	0 [OTHER]	256 bytes	ip.src = 127.0.0.1 ip.dst = 127.0.0.1 tcp.srcport = 38068 tcp.dstport = 27017 service = 0 [OTHER]
01/21/2021 12:39:21 pm	⊕	0 [OTHER]	256 bytes	ip.src = 127.0.0.1 ip.dst = 127.0.0.1 tcp.srcport = 38070 tcp.dstport = 27017 service = 0 [OTHER]

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。バージョン11.5以降のダイアログには、共有オプションが含まれています。

Column Group: RSA Email Ana... Download

CREATE COLUMN GROUP

GROUP NAME
Enter column group name

SHARING
 Share with my organization (this will not be private)

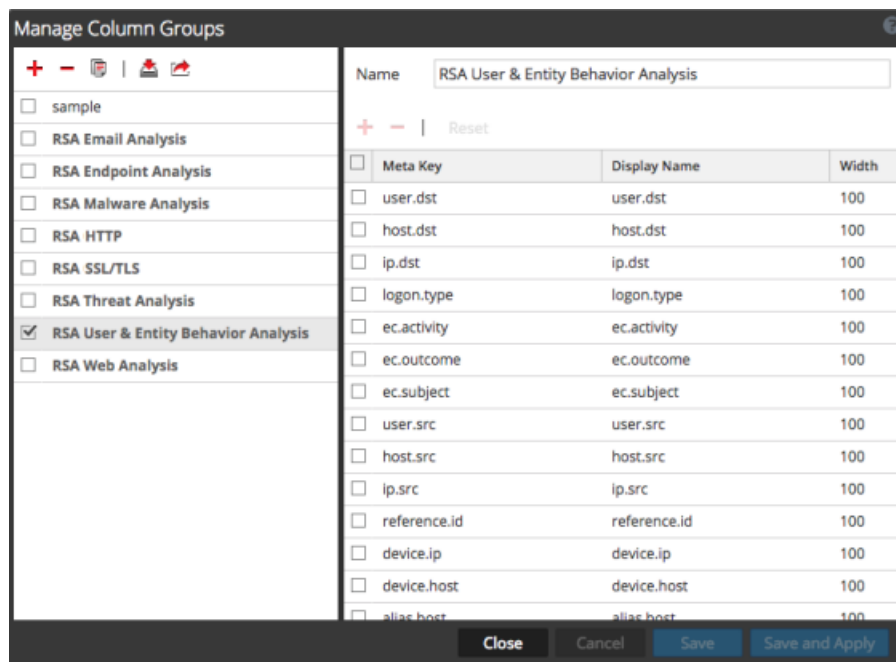
Filter meta keys

DISPLAYED META KEYS. (MAXIMUM 40 KEYS)
Add a meta key from the list below

AVAILABLE META KEYS

- access.point Access Point
- accesses Accesses
- action Action Event
- ad.computer.dst Active Directory Workstatio...
- ad.computer.src Active Directory Workstatio...
- ad.domain.dst Active Directory Domain De...
- ad.domain.src Active Directory Domain So...
- ad.username.dst Active Directory Username ...
- ad.username.src Active Directory Username ...

Close Save Column Group



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、バージョン11.4以降の [イベント]ビュー、11.3以前の [イベント分析]ビュー、[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。

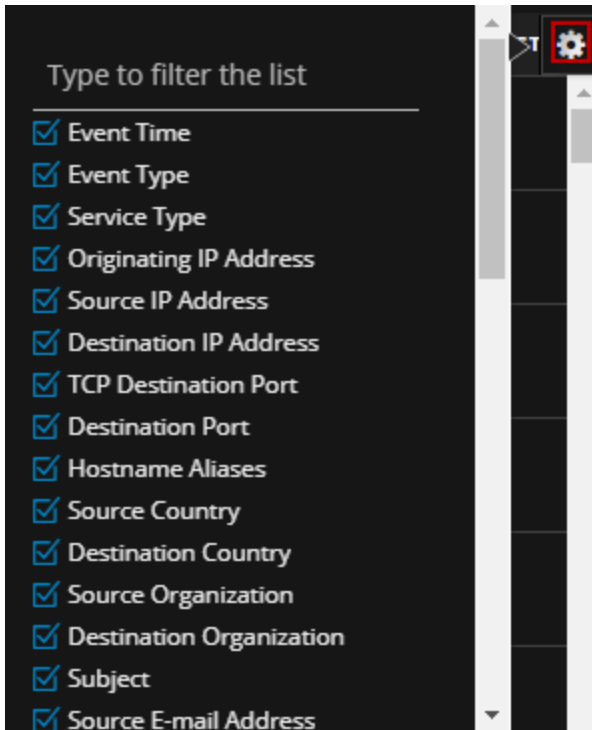
11.4以降の [イベント]ビューでの列と列グループの操作

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(バージョン11.4)

注：接続されているすべてのサービスが11.4以降にアップデートされている場合は、結果のロードが完了した後、【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は次のとおりです。それは、time、eth.type、city.src、ip.src、ipv6.dst、ipv6.srcです。
- 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。

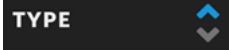
列によるソート(バージョン11.4.1以降)

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。イベントのソート設定が昇順に設定されている場合、カウント ラベルは「最も古い1,000イベント」です。イベントのソート設定が降順に設定されている場合、カウント ラベルは「最も新しい1,000イベント」です。次の図では、昇順が有効になっており、2,001個を超えるイベントがクエリに一致し、最も古い2,001個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。ソート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。

COLLECTION TIME	TYPE	THEME	SIZE	SUMMARY
06/23/2020 05:34:52 am	1 [Network]	80 [HTTP]	1 KB	ip.src = 172.23.0.16 ip.dst = 172.23.0.11 tcp.srcport = 50604 tcp.dstport = 50104 service = 80 [HTTP]
06/23/2020 05:34:54 am	1 [Network]	80 [HTTP]	1 KB	ip.src = 172.23.0.18 ip.dst = 172.23.0.11 tcp.srcport = 53484 tcp.dstport = 50104 service = 80 [HTTP]
06/23/2020 05:34:54 am	1 [Network]	80 [HTTP]	1 KB	ip.src = 172.23.0.17 ip.dst = 172.23.0.11 tcp.srcport = 57304 tcp.dstport = 50104 service = 80 [HTTP]
06/23/2020 05:35:01 am	1 [Network]	80 [HTTP]	6 KB	ip.src = 10.162.30.26 ip.dst = 10.25.51.226 tcp.srcport = 61949 tcp.dstport = 50105 service = 80 [HTTP]
06/23/2020 05:35:01 am	1 [Network]	80 [HTTP]	954 KB	ip.src = 172.16.160.128 ip.dst = 72.21.81.253 tcp.srcport = 53700 tcp.dstport = 80 [http] service = 80 [HTTP]

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。

5,000 Events (Asc) 		Column Group: Summary List	Download		
<input type="checkbox"/>	COLLECTION TIME	TYPE 	THEME	SIZE	SUMMARY
<input type="checkbox"/>	02/13/2008 04:55:15 pm	1 [Network]	80 [HTTP]	2 KB	ip.src = 128.164
<input type="checkbox"/>	02/13/2008 04:55:15 pm	1 [Network]	0 [OTHER]	75 bytes	ip.src = 190.138
<input type="checkbox"/>	02/13/2008 04:55:15 pm	1 [Network]	0 [OTHER]	64 bytes	ip.src = 128.164

- 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。

列によるソート(バージョン11.4)



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、方向を示す明るい白色の矢印が表示され、これを選択して次のようにソートできます。昇順に変更するには  をクリックし、降順に変更するには  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表示されます。[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。

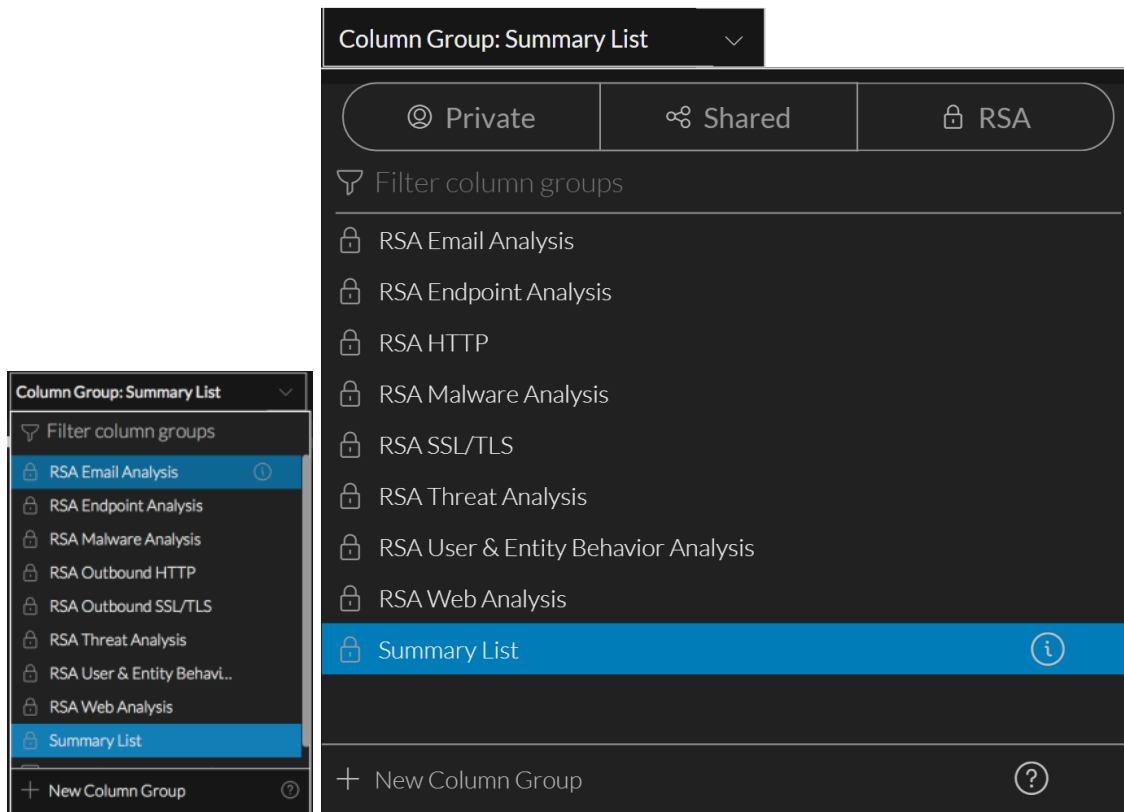
1. 列のタイトルの上にマウスを移動すると、ソート可能な列を見つけることができます。列がソート可能でない場合は、その理由を説明するツールチップが表示されます。
2. リストを列でソートするには、次の手順を実行します。
 - a. ソート可能な列にマウスを移動し、矢印( または ) をクリックします。イベントが正しいソート順でソートされます。列のタイトルの上にカーソルを合わせると、矢印の色がグレーでなくなったことを確認できます。イベント リストのソートに使用されている列には、明るい白色の矢印が表示され、これをクリックしてソートの方向を変更できます。

- 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。

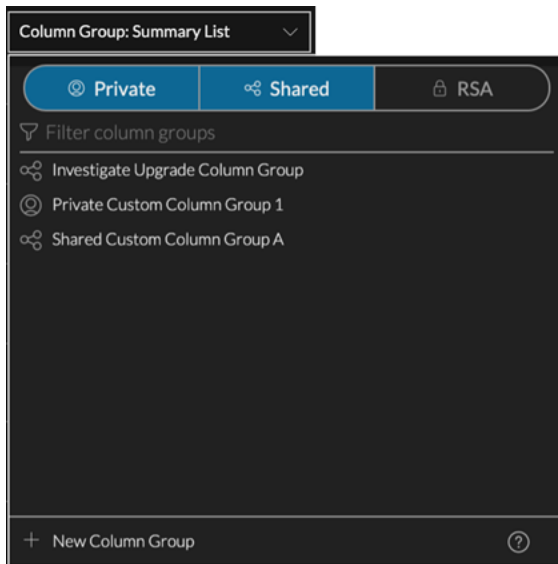
列グループに含まれているメタキーの表示


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。

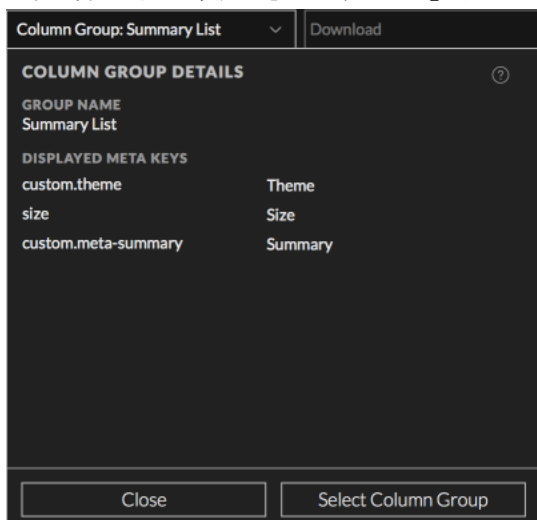
1. **調査**] > **イベント**]に移動し、をクリックしてイベントをロードします。
デフォルト サービスとデフォルト の時間範囲のイベントが **イベント**]パネルにロードされます。
[Summary List]列グループまたは前回のセッションで使用していた列グループがリストに適用されません。
2. **列グループ**]メニューを表示するには、**列グループ**]メニュー タイトルをクリックします。 **列グループ**]メニューのタイトルに、現在選択されている列グループのタイトルが表示されます。ログイン後に初めてアクセスした場合は、Summary Listグループが選択されています。2回目以降のアクセスでは、前のセッションで選択された列グループが使用されます。メニューを開くと、標準提供列グループ(RSA)、共有カスタム列グループ、およびプライベート カスタム列グループのリストが表示されます。表示オプション(バージョン11.5)とフィルタ フィールドを使用すると、特定の列グループを見つけやすくなります。左の図は、[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、初期状態のバージョン11.4メニューを示しています。右の図は、[Summary List]がデフォルトで選択され、すべての列グループタイプ(プライベート、共有、RSA)が表示されている、初期状態のバージョン11.6メニューを示しています。



3. (オプション) リストに表示される列グループのタイプを制御するには、表示オプションを任意に組み合わせ使用します(青 = 選択済み、黒 = 未選択)。
プライベート = 自分だけが管理できるプライベートグループを表示
共有 = 組織内の誰でも管理できる共有グループを表示
RSA = RSAのみが管理できる標準提供グループを表示
 表示オプションは「列グループの絞り込み」フィールドと連動します。表示オプションによって標準提供グループ(グループ名に「RSA」を含むグループ)が非表示になっている場合に、「RSA」を含んだ名前を検索すると、リストは空になります。次の図は、選択されたプライベートおよび共有の表示オプションを示しています。



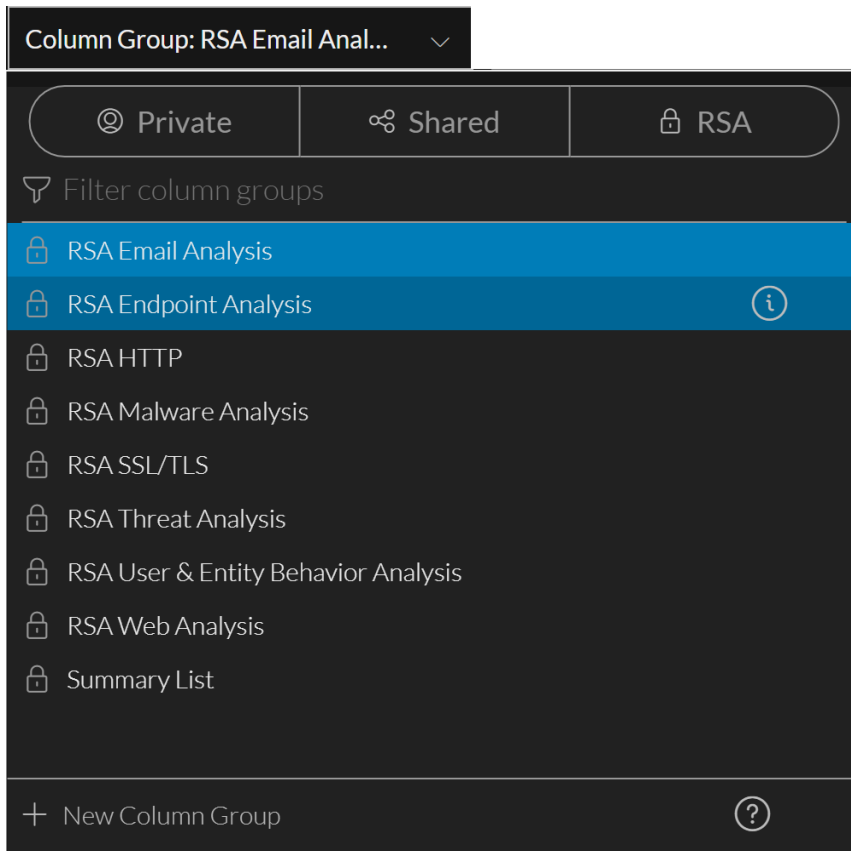
4. グループに含まれている列を確認するには、「Summary List」グループの上にカーソルを合わせて情報アイコン()をクリックします。
 次の図は、「Summary List」の列を示しています。Collection TimeとTypeの2つは常にイベントリストの先頭の2列に表示されますが、「列グループの詳細」ダイアログには表示されません。



5. 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以降の [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。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。



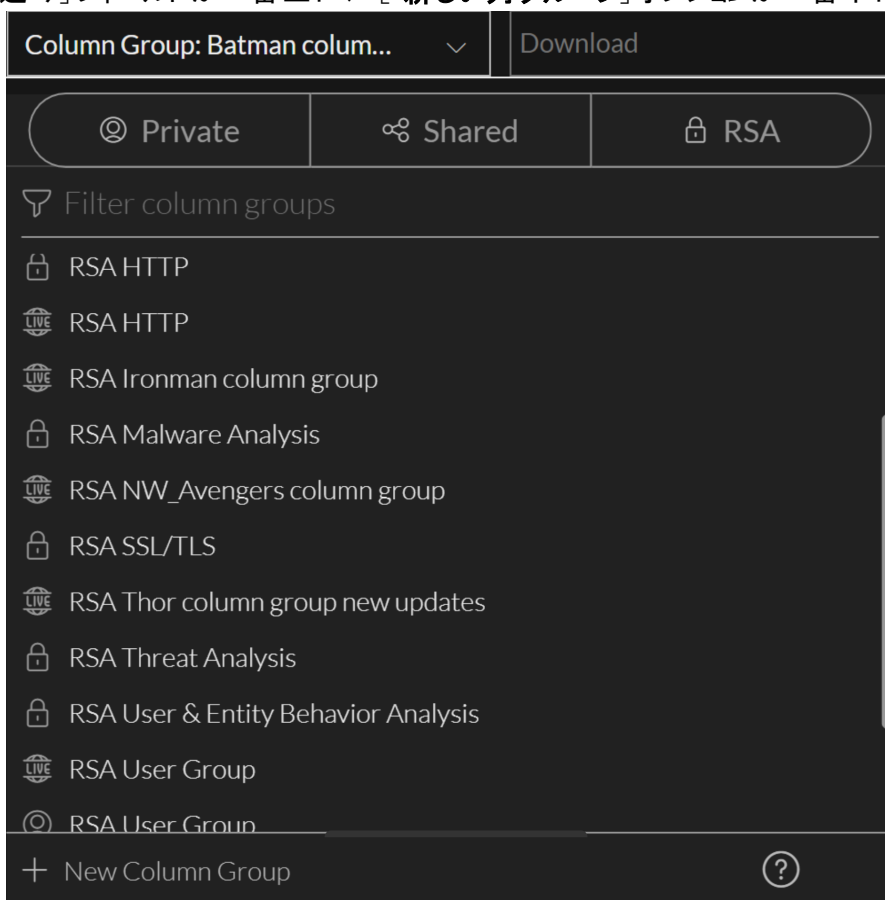
2. 次のいずれかの操作を実行します。
 - a. ハイライト表示されているグループを適用するには、**ENTER**を押します。
 - b. (バージョン11.5以降) 特定の種類のグループのみを表示する場合は、表示オプション(**プライベート**]、**共有**]、**[RSA]**)を使用して1つまたは2つのグループ タイプを非表示にします。

- c. 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。

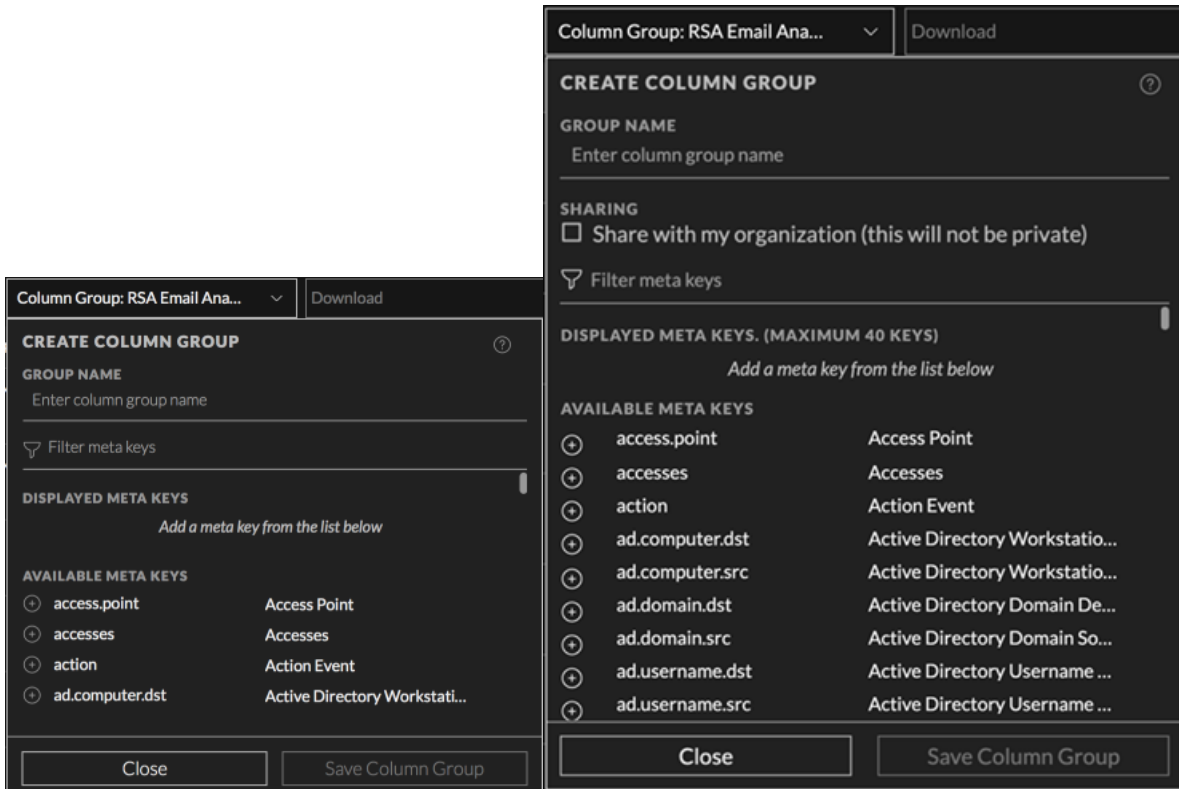
注：列グループ内のメタ キーが、選択したサービスでサポートされない場合、それらのメタ キーは [イベントの絞り込み] パネルまたは [イベント] パネルには表示されません。

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。表示オプションと列グループの絞り込みフィールドが一番上に、**新しい列グループ**オプションが一番下に表示されます。

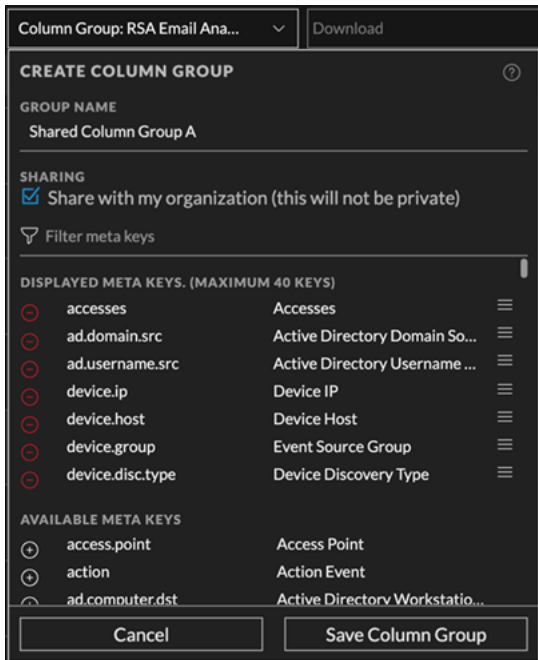


3. 「新しい列グループ」を選択します。
「列グループの作成」ダイアログが表示されます。バージョン11.5には、共有オプションが含まれていません。

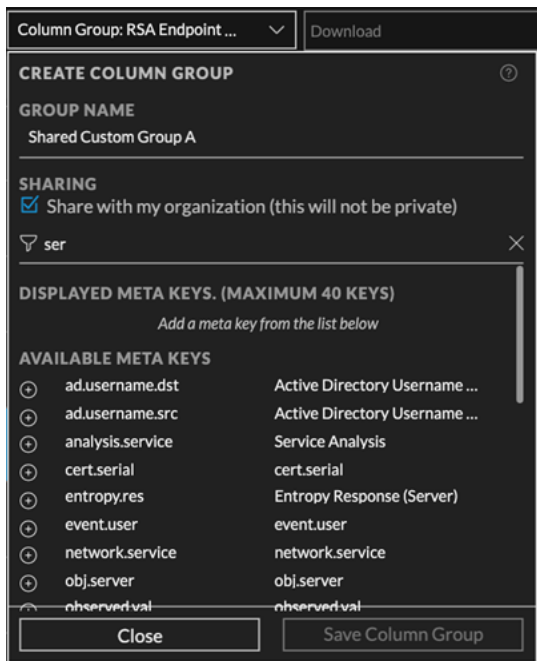


4. 「グループ名」フィールドに、新しい列グループの一意の名前(最大256文字)を入力します(たとえば「Custom Column Group A」)。

5. (バージョン11.5以降) 新しい列グループを組織内で共有する場合は、**組織内で共有**]オプションを設定します。

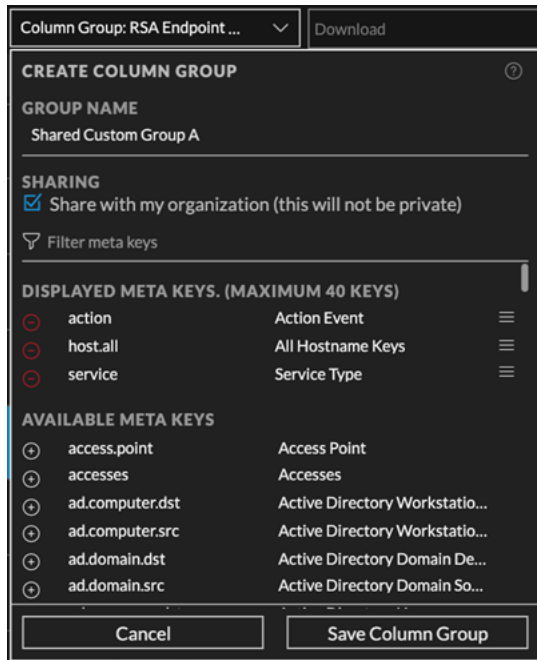


6. 列グループにメタ キーを追加するには、次のように各メタ キーを選択して追加します。
- a. **メタ キーの絞り込み**]フィールドにテキスト文字列を入力すると、そのテキストを含んでいるメタ キーが **選択可能なメタ キー**]リストに表示されます。



- 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

を使用してフィルタ処理されます)。列グループ内の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。




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。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. 次のいずれかの操作を実行します。
 - 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。
10. 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. 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。

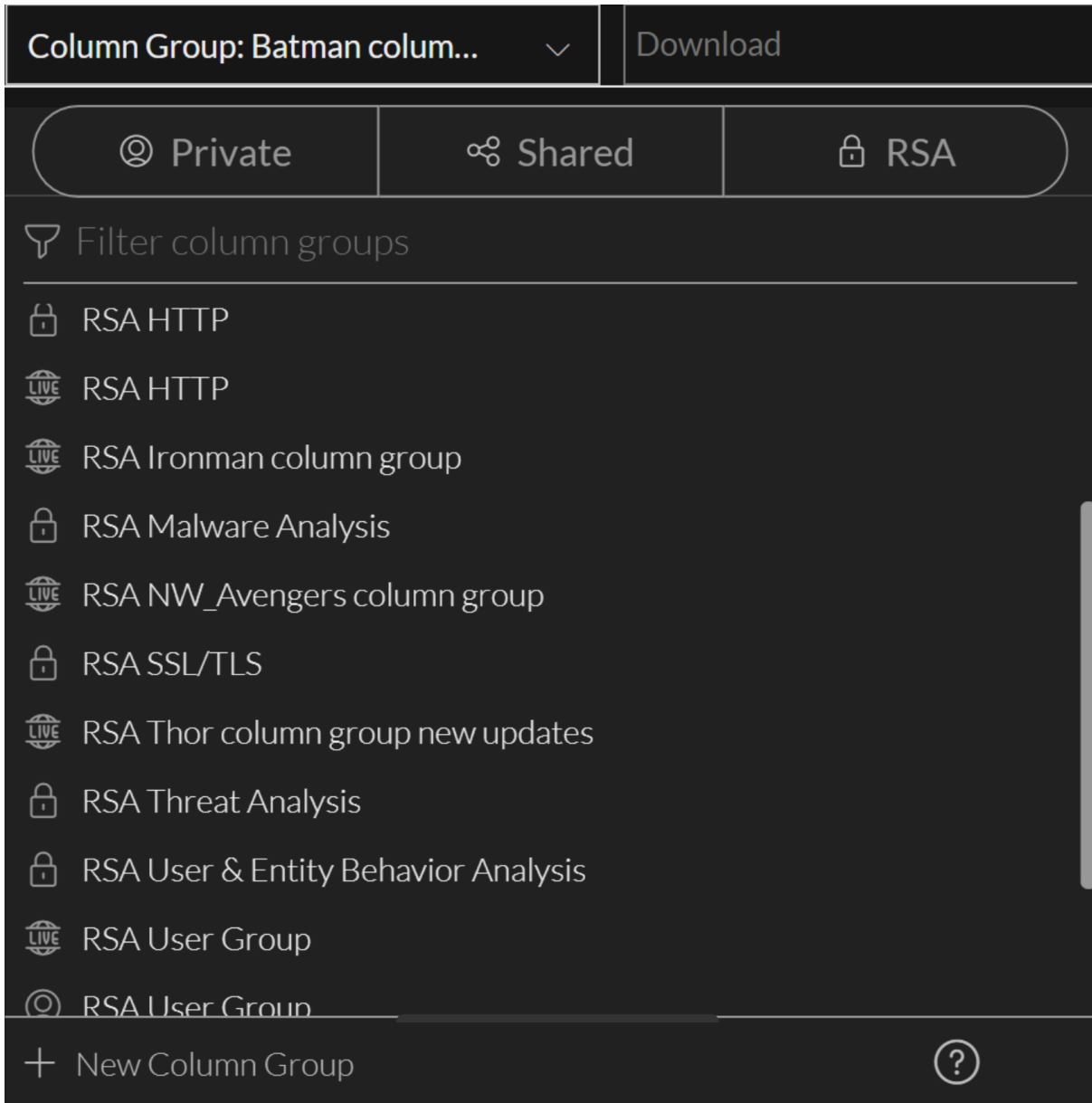
カスタム列グループの削除

現在イベント リストに適用されておらず、クエリプロファイルの一部になっていないカスタム列グループは削除できます。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。バージョン 11.5以降では、確認メッセージが表示され、削除を確認またはキャンセルできます。カスタム列グループを削除すると、その列グループは [列グループ] メニューから削除されます。

注意：カスタム列グループ(バージョン11.4)または共有列グループ(バージョン11.5)を削除すると、影響がグローバルに及び、そのグループはどのアナリストも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。

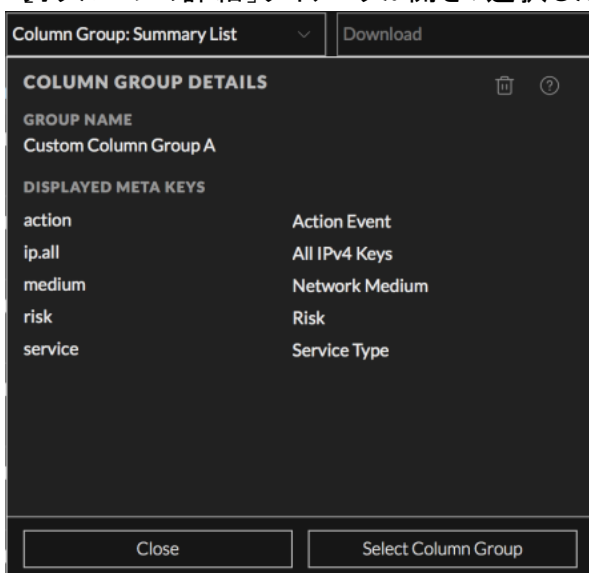
1. **調査**] > **イベント**]に移動し、をクリックしてイベントをロードします。
デフォルト サービスとデフォルト の時間範囲のイベントが [イベント] パネルにロードされます。
[Summary List] 列グループまたは前回のセッションで使用していた列グループがリストに適用されま
す。次の図は、[Summary List] 列グループが選択されている初期状態のビューを示しています。
[列グループ] メニューのラベルに、選択した列グループの名前が表示されます。



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。

Custom Column Grou... ✎

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。



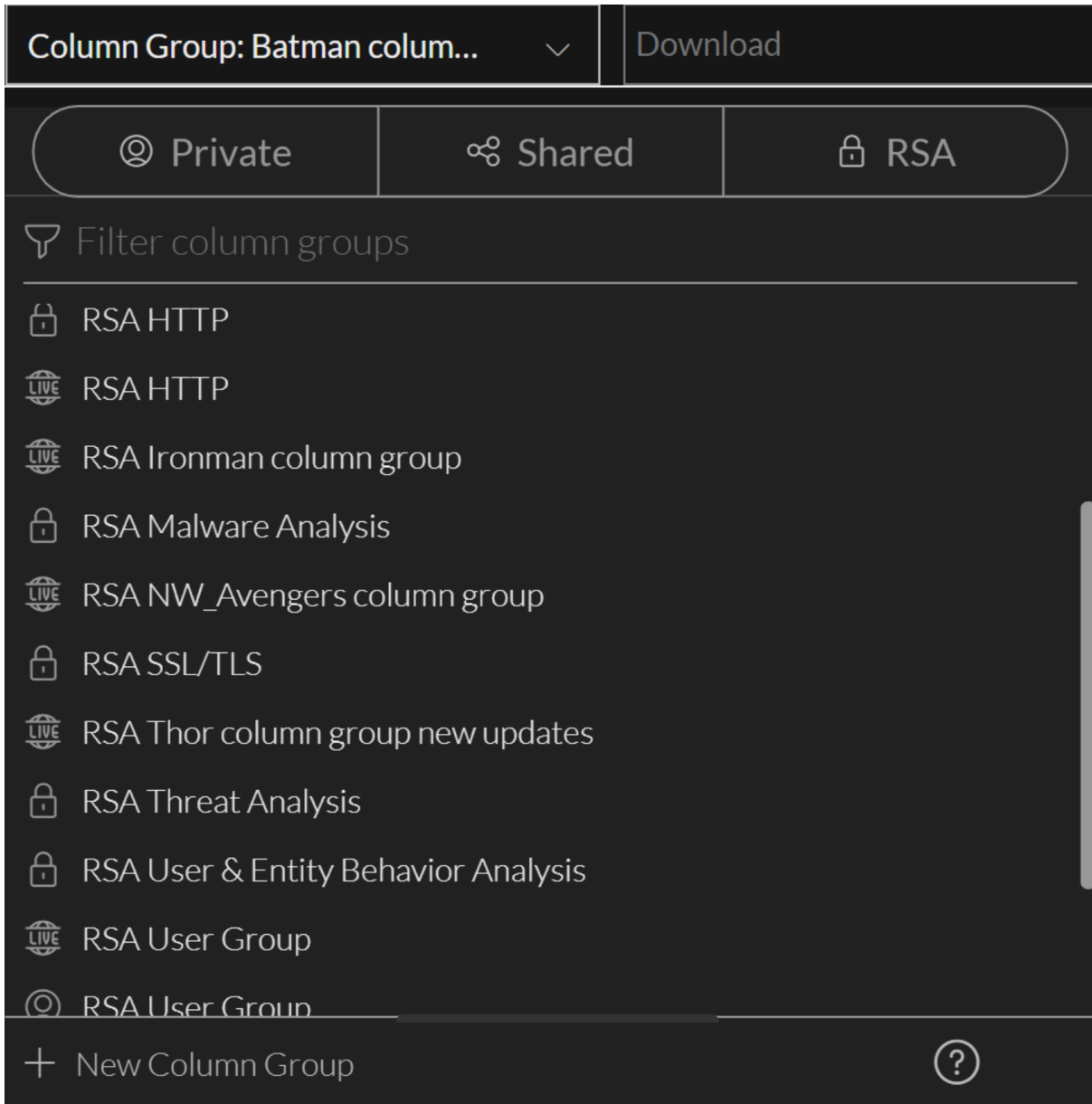
4. グループの削除アイコン(🗑️)をクリックします。
列グループが現在有効になっている場合は、次のメッセージが表示されます。This column group cannot be deleted because it is currently active.
バージョン11.5では、確認メッセージが表示され、削除を確認するかキャンセルすることができます。
[キャンセル]または [列グループの削除]をクリックします。
バージョン11.4では、列グループが有効でなく、標準提供の列グループでもない場合、列が削除される前の確認を求められません。
グループが削除され、[列グループ]メニューから削除されます。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。



カスタム列グループの編集

編集用を開いていない列グループの共有コピーまたはプライベート コピーを作成できます。コピーを作成したら、通常の方法で新しいグループを編集できます。

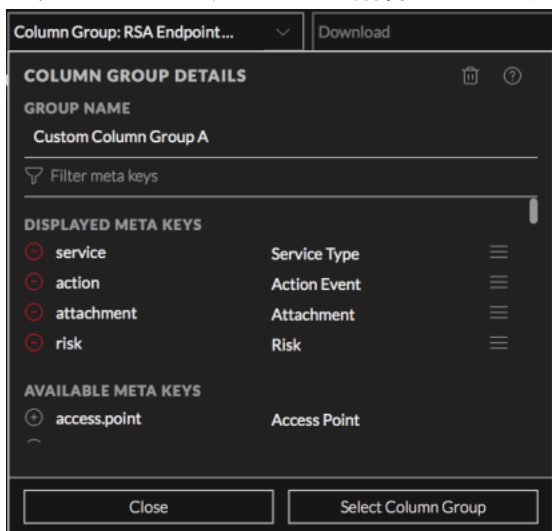
1. [調査] > [イベント]に移動して、クエリを送信し、[イベント]パネルにデータをロードします。


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て、列グループのリストが表示されます。

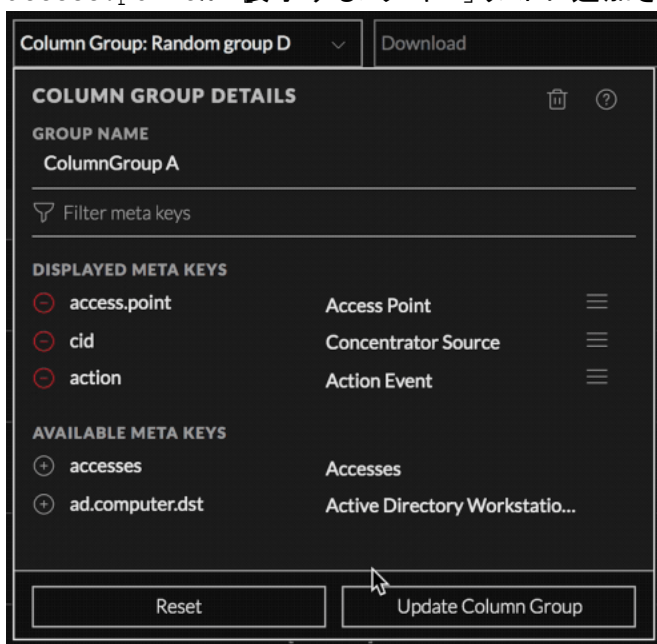





3. 編集する列グループをハイライト表示します。次の図では、カスタム列グループがハイライト表示され、右側に編集アイコンが表示されています。
- 
- The screenshot shows a single item in a list: "Custom Column Group A" with a blue background and a pencil icon to its right.
4. 編集アイコン()をクリックします。
[列グループの詳細]ダイアログが表示され、グループ名と表示するメタ キーを編集できるようになり

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、入力したテキストを使用してフィルタ処理されます)。次の図は、グループ名がColumn Group C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ことを示しています。



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. 次のいずれかの操作を実行します。
 - 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. 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。

列グループのコピーの作成(バージョン11.5以降)

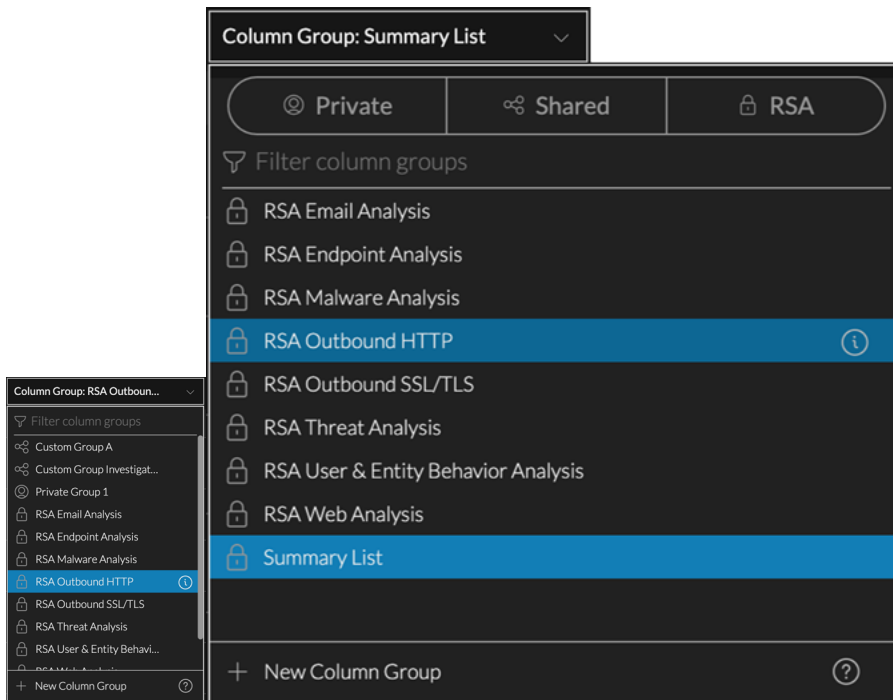
未保存の編集が進行中でない限り、標準提供またはカスタム、共有またはプライベートのいずれかにかかわらず、任意の列グループをコピーできます。この機能は、標準提供グループのカスタマイズされたバージョンが必要な場合に便利です。また、カスタム グループをプライベートから共有に、または共有からプライベートに変更することはできないため、コピーを作成することで、別の共有設定を選択できるようになります。列グループのコピーを作成すると、同じ名前が使用され、番号が付記されます。たとえば、RSA HTTPをコピーすると、最初のコピーの名前はRSA HTTP-1になり、同じグループの2番目のコピーの名前はRSA HTTP-2になります。コピーを作成した後は、新しいグループを編集して新しい名前を指定し、グループ内のメタ キーを管理することができます。

注： **[ラギー イベント]**ビューで作成された一部の列グループには、**[イベント]**ビューの列グループの制限を上回る、40個を超える列が含まれている場合があります。500個を超える列を持つグループをコピーする場合は、列グループの編集時に余分な列を削除する必要があります。

列グループをコピーするには、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、**[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**]フィールドが一番上に、**[新しい列グループ]**オプションが一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。

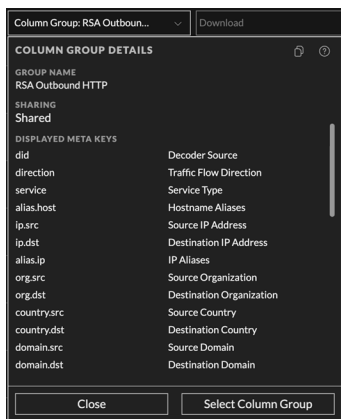
3. コピーする列グループをハイライト表示します。この図は、RSA HTTPがハイライト表示されていることを示しています。情報アイコン(📘)が右側に表示されます。左側はバージョン11.4のメニューで、右側はバージョン11.6以降のメニューです。



4. 次のいずれかの操作を実行します。

- a. 情報アイコン(📘)をクリックします。
- b. 編集アイコン(✎)をクリックします。

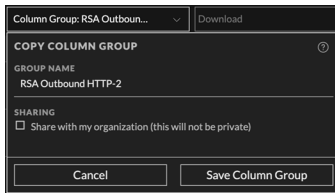
列グループの詳細]ダイアログが表示されます。この図は、標準提供グループのダイアログを示しています。



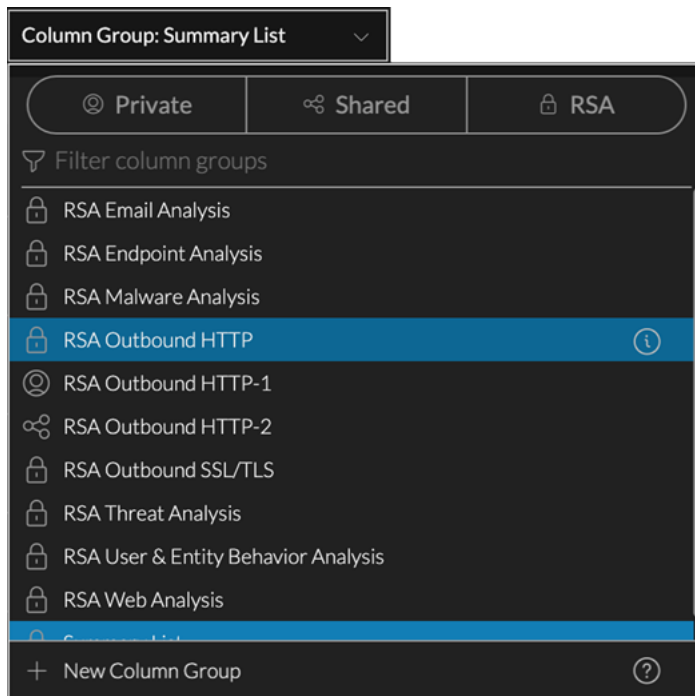
5. コピーアイコン(📄)をクリックします。

列グループのコピー]ダイアログが開き、列グループ名に-nが付記されて表示されます。次の図で

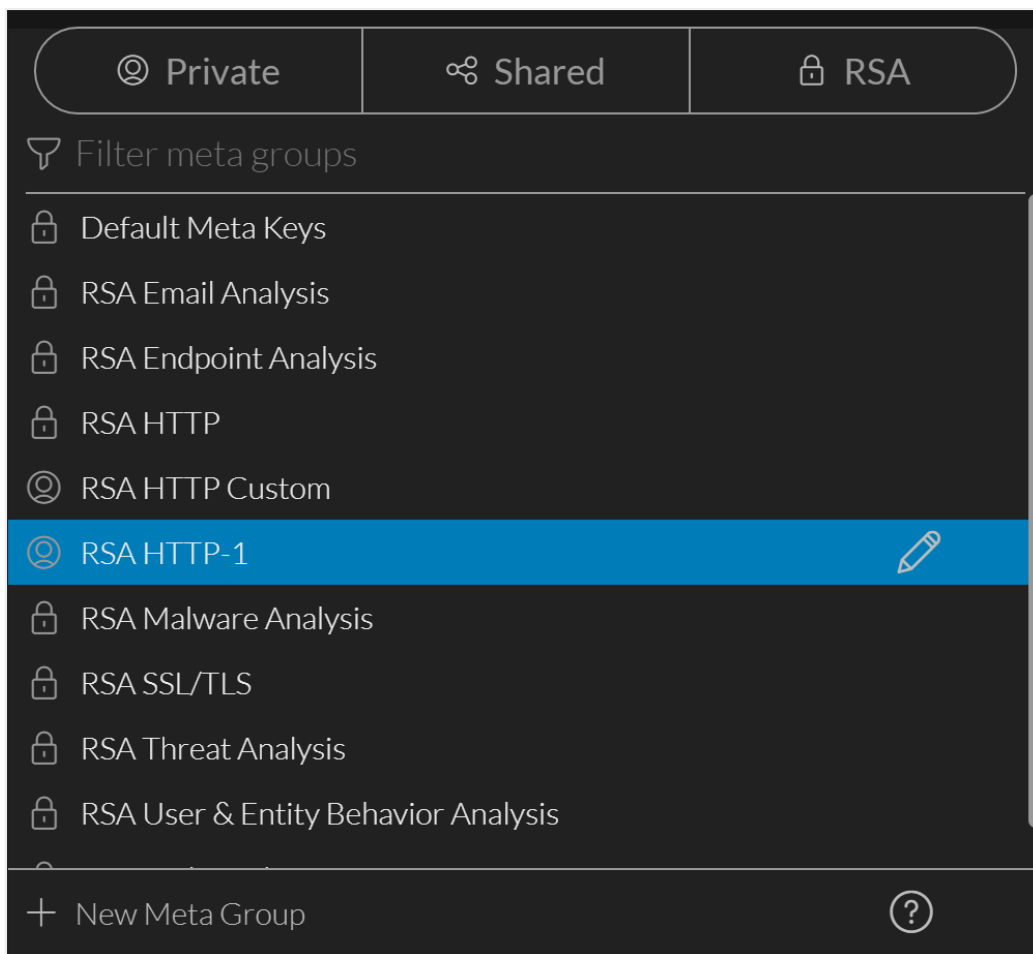
は、この列グループの2番目のコピーであることを示す-2になります。



6. (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。
7. 新しい列グループを組織内で共有する場合は、**組織内で共有** オプションを設定します。デフォルトで、新しいグループはプライベートです。
8. 次のいずれかの操作を実行します。
 - a. グループをコピー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. 列グループのコピーを保存するには、**列グループの保存** をクリックします。列グループのコピーが保存され、ボタンが **閉じる** と **列グループを選択** に変わります。
9. 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. ダイアログを閉じて列グループのコピーを選択するには、**列グループを選択** をクリックします。列グループがコピーされ、**イベント** リストが更新されて列グループのコピーの列が表示されます。次の図には、RSA HTTP列グループの2つのコピーがあり、1つは共有、もう1つはプライベートです。




1. 次のいずれかの操作を実行します。
 - a. 編集しないで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メタグループのコピーを選択するには、**メタグループの選択**]をクリックします。
メタグループ]メニューにグループが追加されます。次の図は、RSA HTTPメタグループのプライベートコピーを示しています。



列グループフォルダの作成

現在のレベルに存在し、プライベートフォルダまたは共有フォルダとして追加されるカスタム列グループフォルダを作成できます。また、フォルダ名がすでに存在する場合は、一意の名前を入力するように求められます。


1. [イベント]ビューで [イベントの絞り込み]パネルを開いた状態で、[列グループ]メニューの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て、列グループとフォルダのリストが表示されます。
2.  をクリックします。
[フォルダの作成]ダイアログが表示されます。
3. [フォルダ名]フィールドに、新しいメタグループフォルダの一意の名前(最大255文字)を入力し

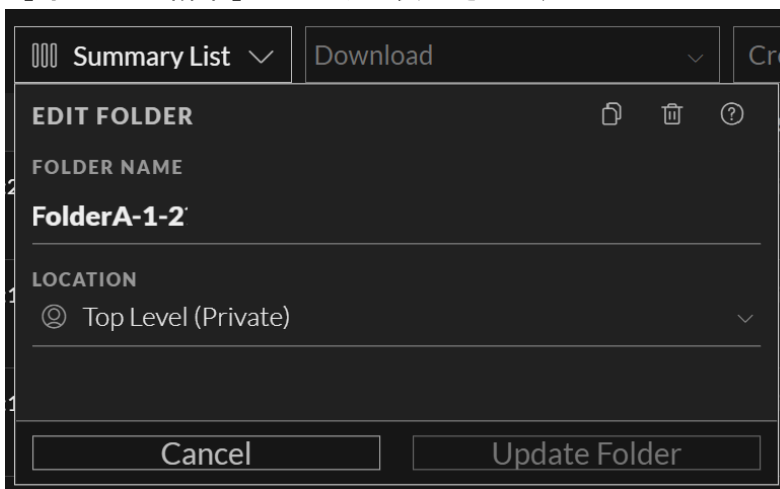
ます。

4. **フォルダの作成** をクリックします。

列グループ フォルダの編集と移動

列グループ フォルダを作成した後、それを編集または移動できますが、RSAグループ (RSA LiveコンテンツおよびRSA OOTBグループ) 内のフォルダは編集も移動もできません。プライベート フォルダおよび共有フォルダ内のフォルダは、それぞれのグループ内でのみ編集および移動できます。たとえば、共有フォルダをプライベート フォルダに移動したり、その逆を行ったりすることはできません。

1. **イベント** ビューで **イベントの絞り込み** パネルを開いた状態で、**列グループ** メニュー タイトルをクリックし、編集する列グループをハイライト表示します。
2.  をクリックします。
フォルダの編集 ダイアログが表示されます。





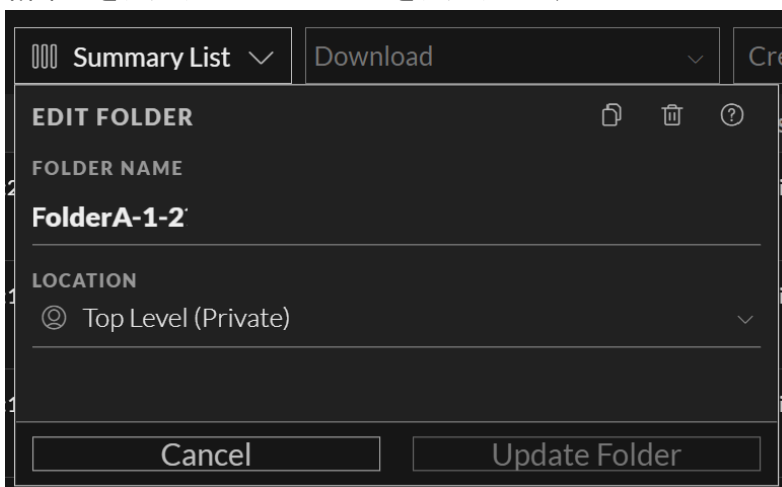
3. **フォルダ名** フィールドに、列グループ フォルダの一意の名前を入力します。
4. 編集するフォルダの場所を選択します。
5. **フォルダの更新** をクリックします。

列グループ フォルダのコピー

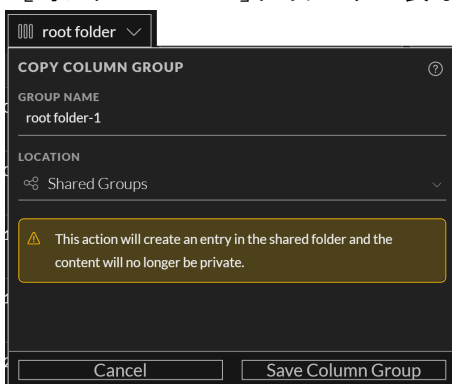
列グループ フォルダをプライベート から共有、プライベート からプライベート、共有 から共有、共有 からプライベート グループにコピーできます。フォルダをコピーすると、そのフォルダの内容がコピーされます。プライベート フォルダを共有フォルダにコピーすると、フォルダとその内容はプライベート のままではなくなります。

1. **イベント** ビューで **イベントの絞り込み** パネルを開いた状態で、**列グループ** メニューの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て、列グループとフォルダのリストが表示されます。
2. コピーするフォルダを選択します。

3. 編集  をクリックして、コピー  をクリックします。



「フォルダーのコピー」ダイアログが表示されます。



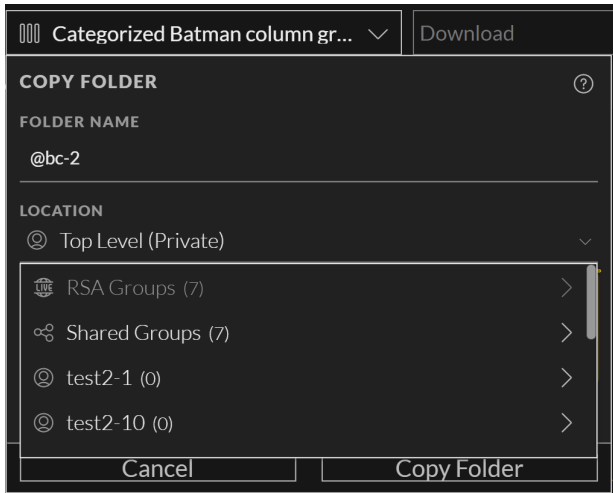
4. 「フォルダ名」フィールドに、新しいメタグループフォルダの一意の名前を入力します。
5. 編集するフォルダの場所を選択します。
6. 「フォルダのコピー」をクリックします。

Liveから導入されたグループフォルダのコピー

RSA Groupsカテゴリーの下にあるLiveから導入された列グループフォルダを、共有グループなどの他の場所またはプライベートフォルダにコピーできます。

1. 「イベント」ビューで「イベントの絞り込み」パネルを開いた状態で、「列グループ」メニューの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て、列グループとフォルダのリストが表示されます。
2. コピーするLive列グループフォルダをクリックします。


3. ⓘ をクリックします。
「フォルダのコピー」ダイアログが表示されます。

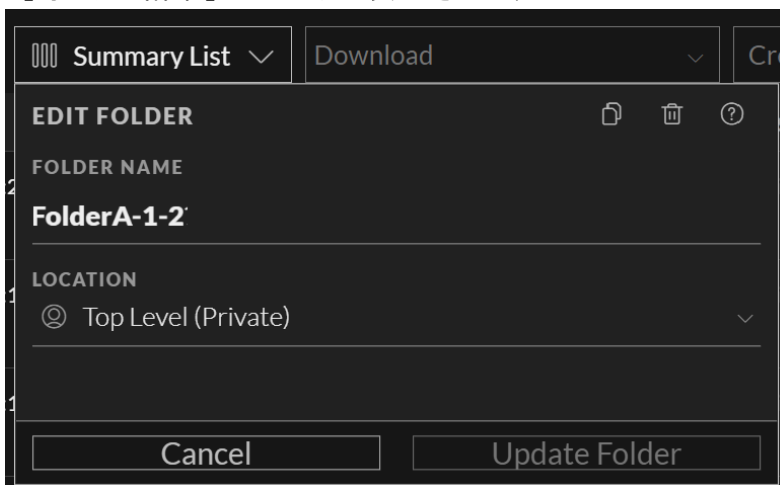



4. コピーするフォルダの場所を選択します。
5. 「フォルダのコピー」をクリックします。
フォルダがフォルダの元の名前で作成され、最後に「copy」が追加されます。

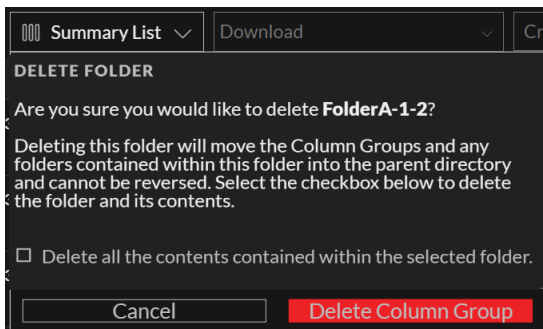
列グループフォルダの削除

保持したくないフォルダは削除できます。ただし、フォルダを削除すると、そのフォルダを取得できなくなります。

1. [イベント]ビューで [イベントの絞り込み] パネルを開いた状態で、[列グループ]メニューの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て、列グループとフォルダのリストが表示されます。
2. 削除するフォルダを選択します。
3. 編集  をクリックします。
「フォルダの編集」ダイアログが表示されます。



- 削除  をクリックします。
アクションを確認するための警告メッセージが表示されます。



- (オプション) 選択したフォルダ内のすべてのコンテンツとともにフォルダを削除する場合は、このチェックボックスを選択します。
チェックボックスを選択しないと、必要なフォルダが削除された後で、コンテンツは親フォルダに移動されます。
- OK** をクリックして削除します。

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。

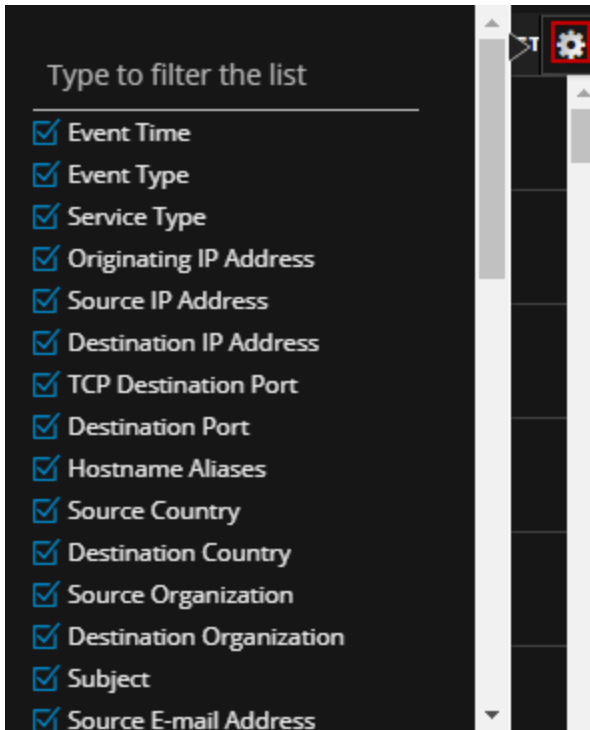
列グループを選択するには、次の手順を実行します。

[列グループ]メニューで、次のいずれかの操作を実行します。

- 列グループを選択します(たとえば [Summary List])。
- 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。

- [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。

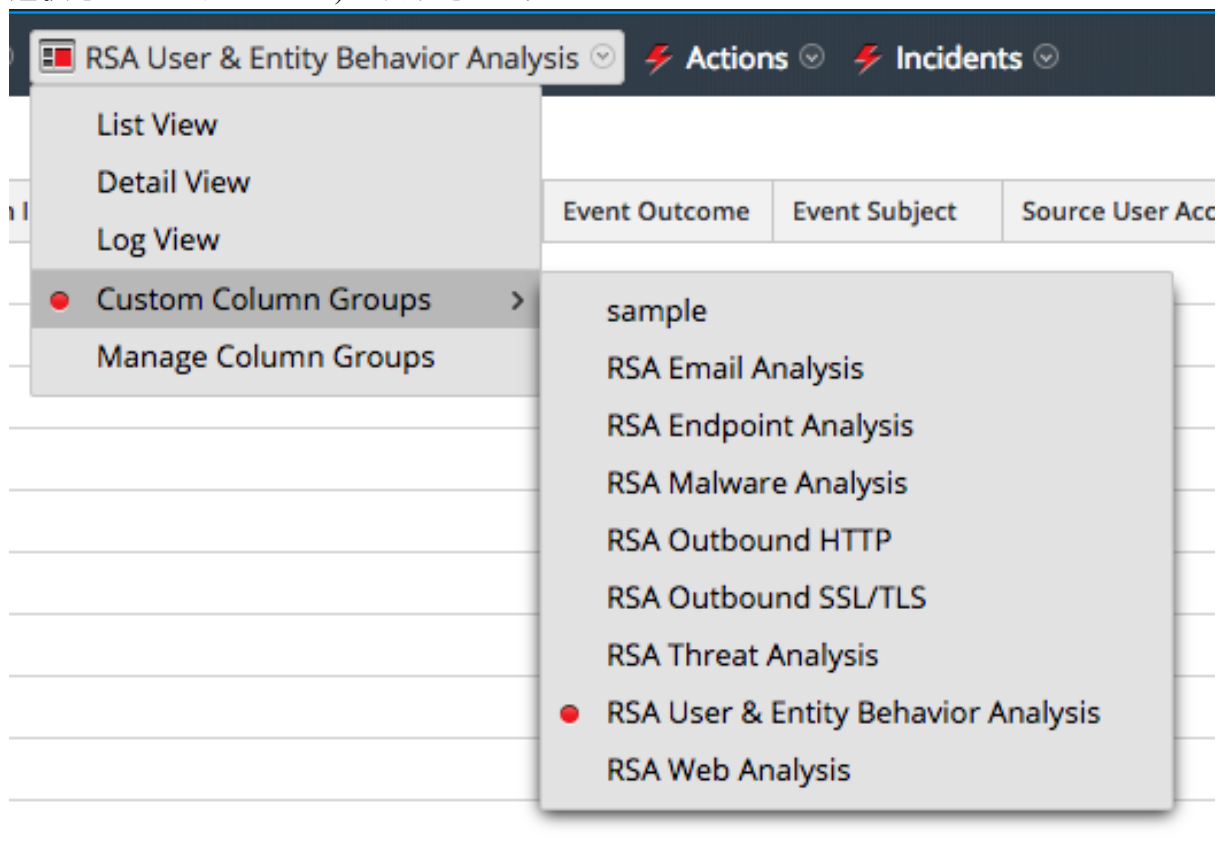
列グループの選択

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、選択したオプション(詳細ビュー、リスト ビュー、ログビュー、または現在

選択されている列グループ)が反映されます。

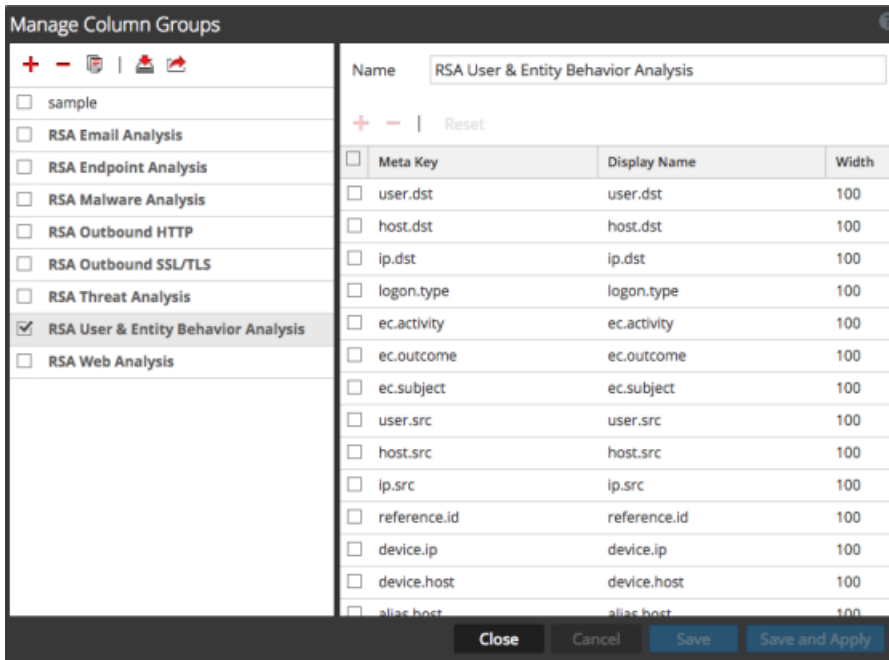


2. サブメニューから列グループのいずれかを選択します。
[レガシー イベント]ビューが更新され、カスタム列グループが反映されます。

[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

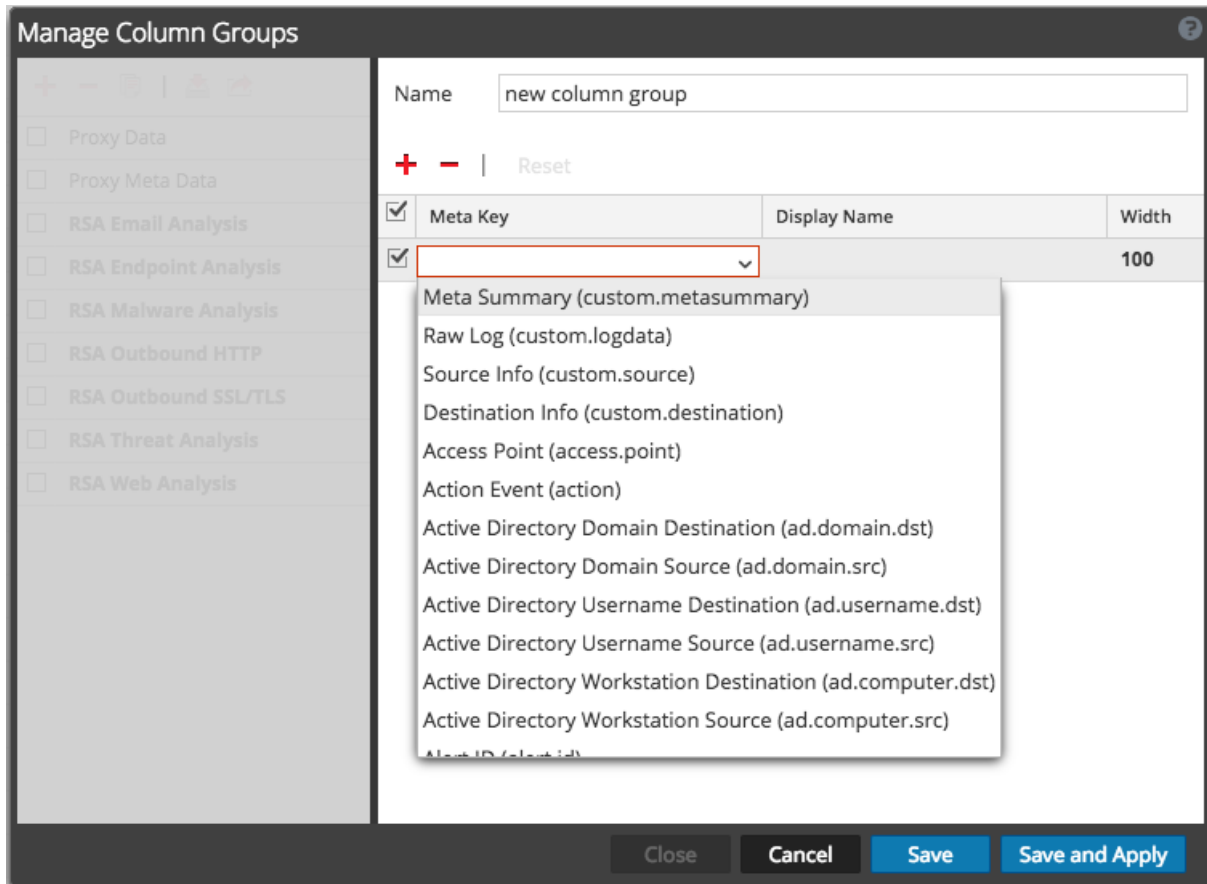
1. **調査**] > **レガシー イベント**]に移動します。
2. **ビュー**]ドロップダウンメニューから **列グループの管理**]を選択します。[ビュー]ドロップダウンメニューのラベルには、現在選択中のオプション(詳細ビュー、リストビュー、ログビュー、現在選択されている列グループ名など)が表示されます。

「列グループの管理」ダイアログが表示されます。



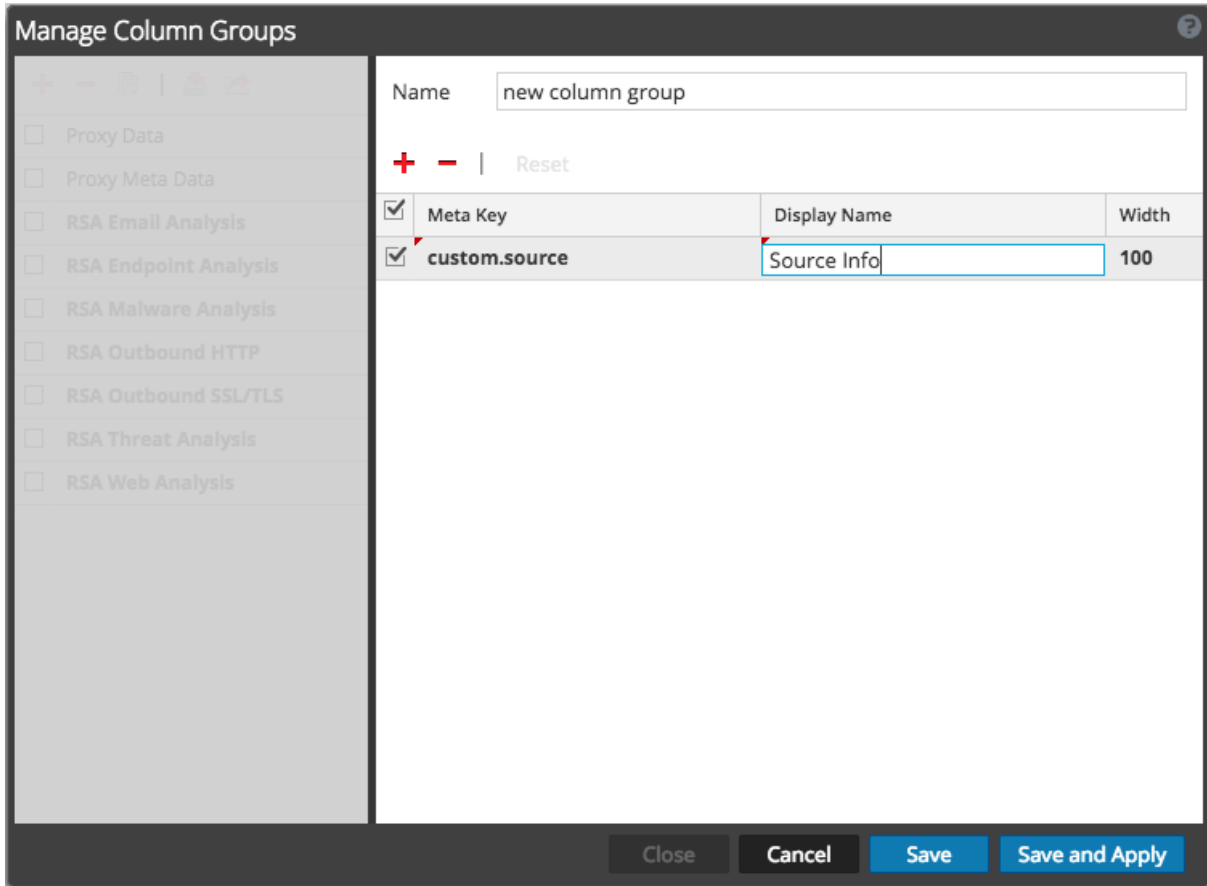
- 列グループ パネルに新しい列グループを追加するには、**+** をクリックし、表示されたフィールドに新しいグループの名前を入力します。
列定義 パネルが右側に表示され、グループ名が入力されます。グループ名は編集できます。
- グループに列を追加するには、**+** をクリックします。追加された空の **[メタ キー]** フィールドをクリックし、**[メタ キー]** ドロップダウン リストを表示します。リストからメタ キー フィールドを選択します。この

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。

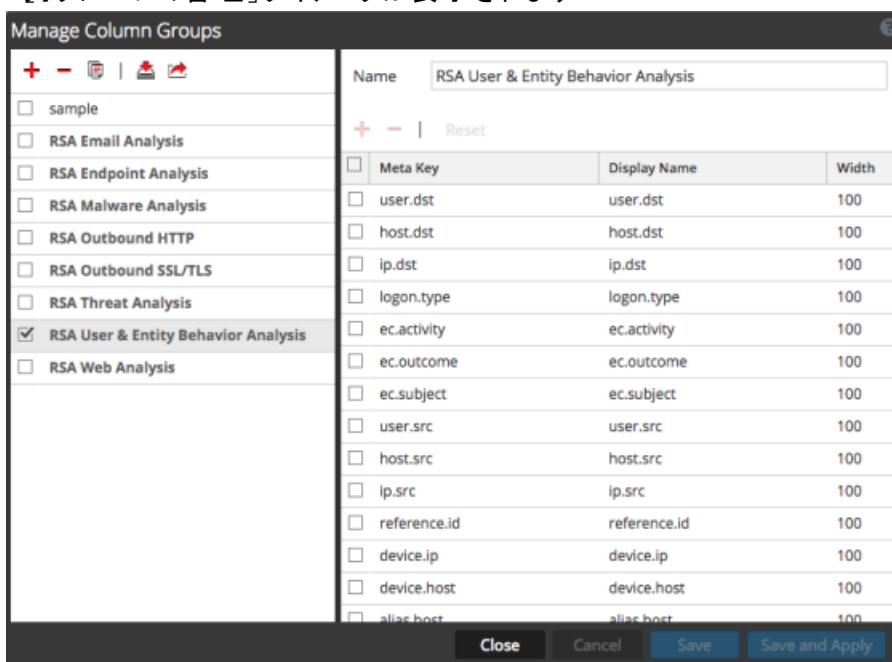


8. (オプション) 列グループを以前の設定に復元し、これまでに加えた変更をすべて取り消すには、**キャンセル**をクリックします。
9. 保存する準備ができたなら、次のいずれかの操作を実行します。
- 編集した列グループを保存し、その列グループの設定を使って **レガシー イベント**ビューを更新するには、**保存して適用**をクリックします。
 - レガシー イベント**ビューを更新せずに、編集した列グループを保存するには、**保存**をクリックします。

列グループの削除(**レガシー イベント**ビュー)

- 調査** > **レガシー イベント**に移動します。
- 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。

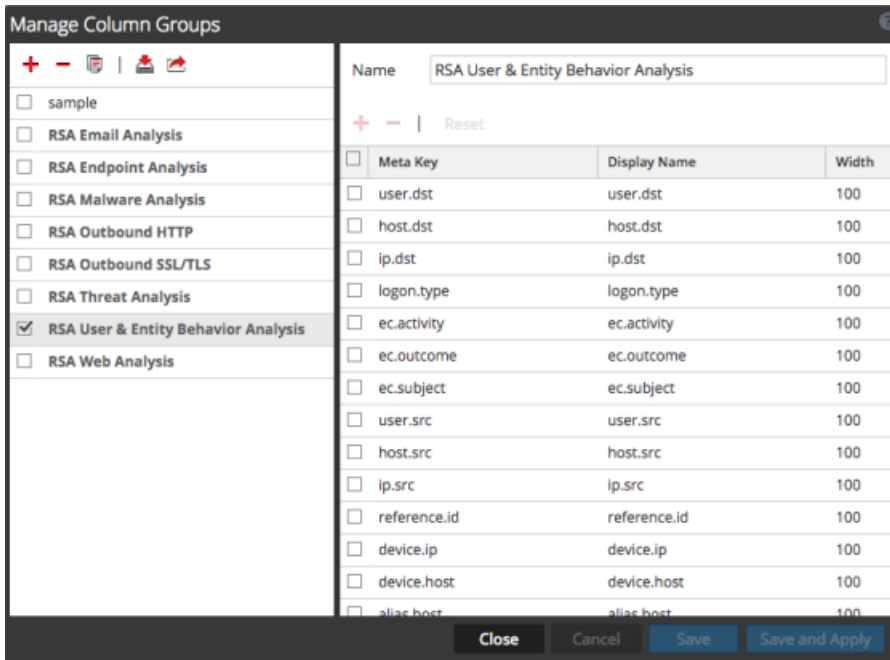




3. 列グループ パネルでカスタム列グループを削除するには、1つまたは複数のカスタム列グループを選択し、ツールバーの **-** をクリックします。
確認を求めるメッセージが表示されます。
4. 次のいずれかの操作を実行します。
 - a. 列グループを削除して [レガシー イベント] ビューを更新するには、**[はい]** をクリックします。
 - b. 列グループを削除しない場合は、**[いいえ]** をクリックします。
選択した列グループが削除され、どこにも表示されなくなります。

列グループの編集([イベント] ビュー)

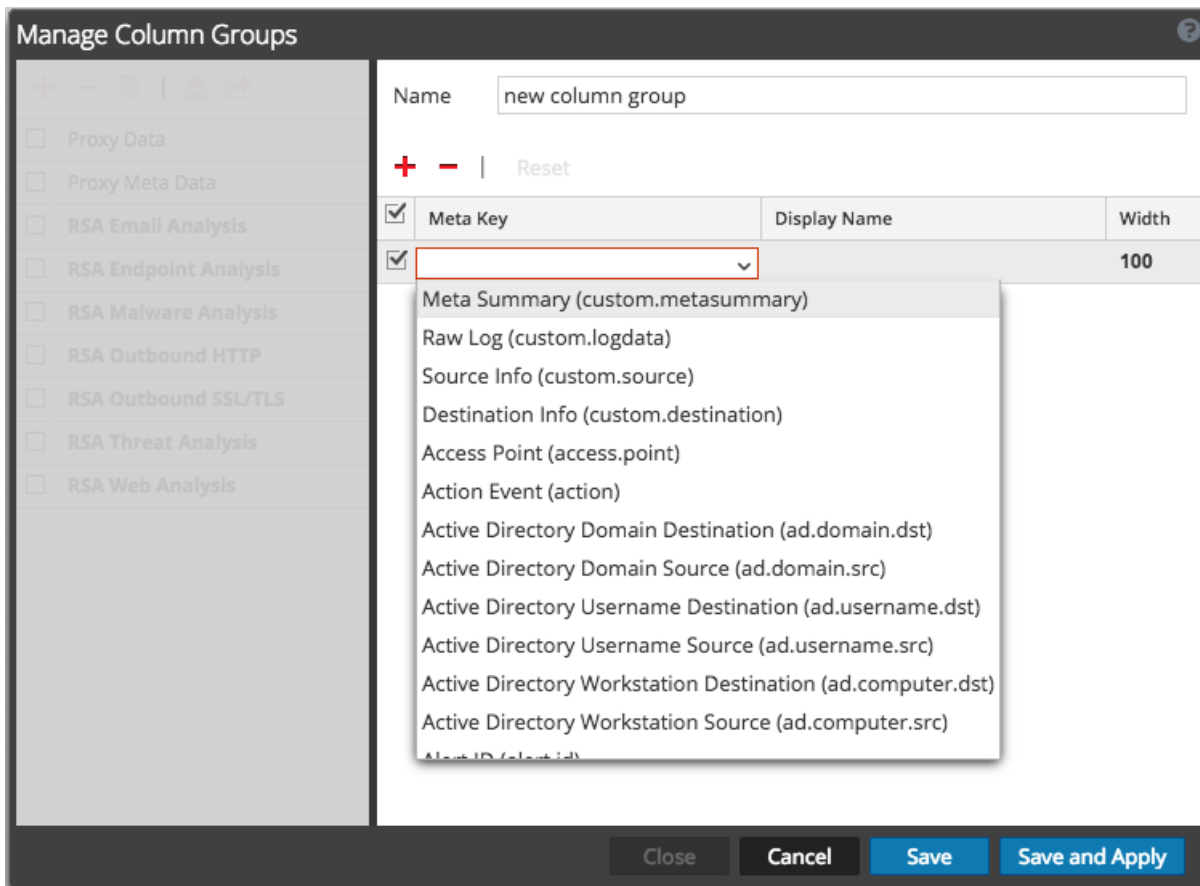
1. **調査** > **[レガシー イベント]** に移動します。
2. **[ビュー]** ドロップダウンメニューから **列グループの管理** を選択します。 **[ビュー]** ドロップダウンメニューのラベルには、現在選択中のオプション(詳細ビュー、リスト ビュー、ログビュー、現在選択されている列グループ名など) が表示されます。

「列グループの管理」ダイアログが表示されます。



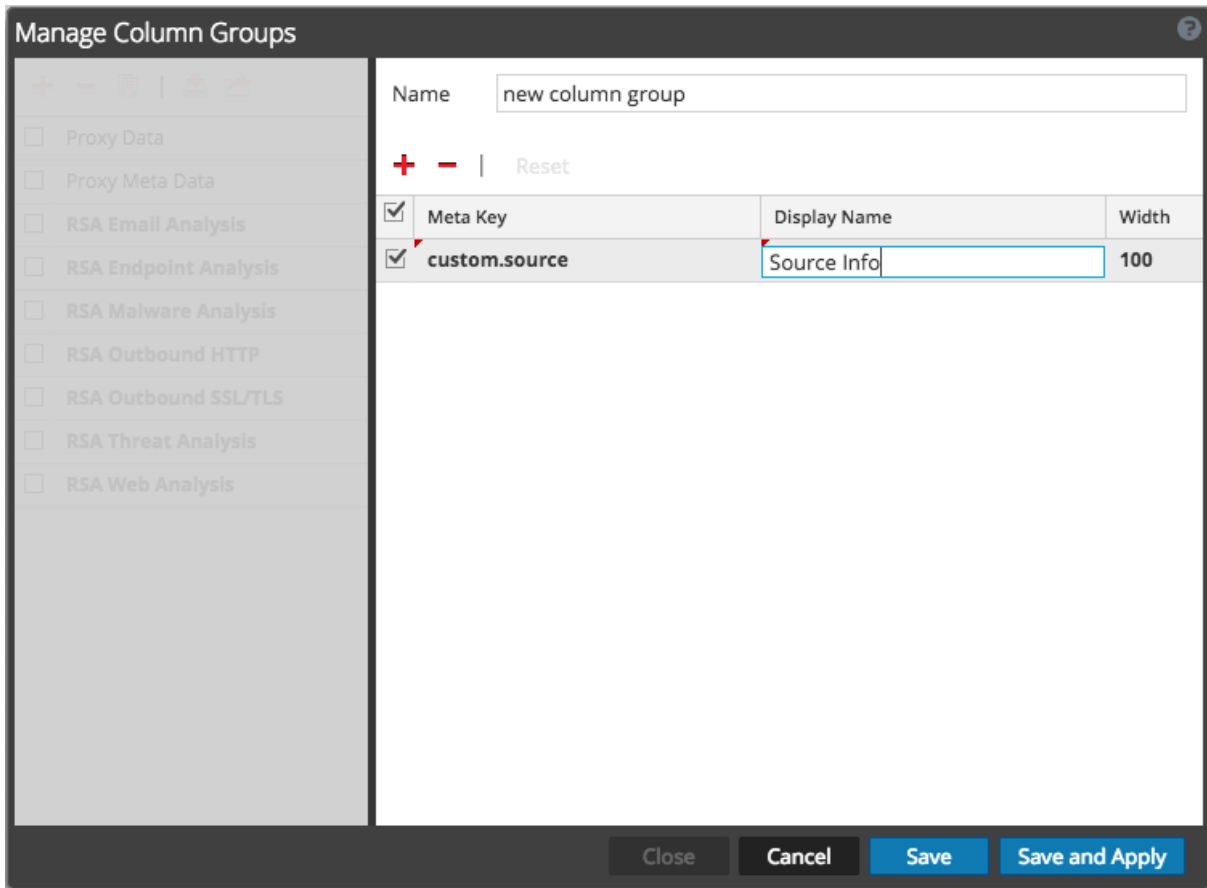
3. 次のいずれかの操作を実行します。
 - a. 列グループパネルでカスタム列グループを編集するには、名前のあるチェックボックスを選択します。
列定義パネルが右側に表示されます。
 - b. 標準提供の列グループまたはカスタムの列グループを複製してから編集するには、名前のあるチェックボックスを選択して、複製アイコン() をクリックします。
列定義パネルが右側に表示されます。
4. (オプション) グループの複製を編集している場合は、グループの新しい名前を入力します。
5. グループに列を追加するには、 をクリックします。追加された空の「メタキー」フィールドをクリックし、「メタキー」ドロップダ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



- (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。
- (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なら、次のいずれかの操作を実行します。
- 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。
 - 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)

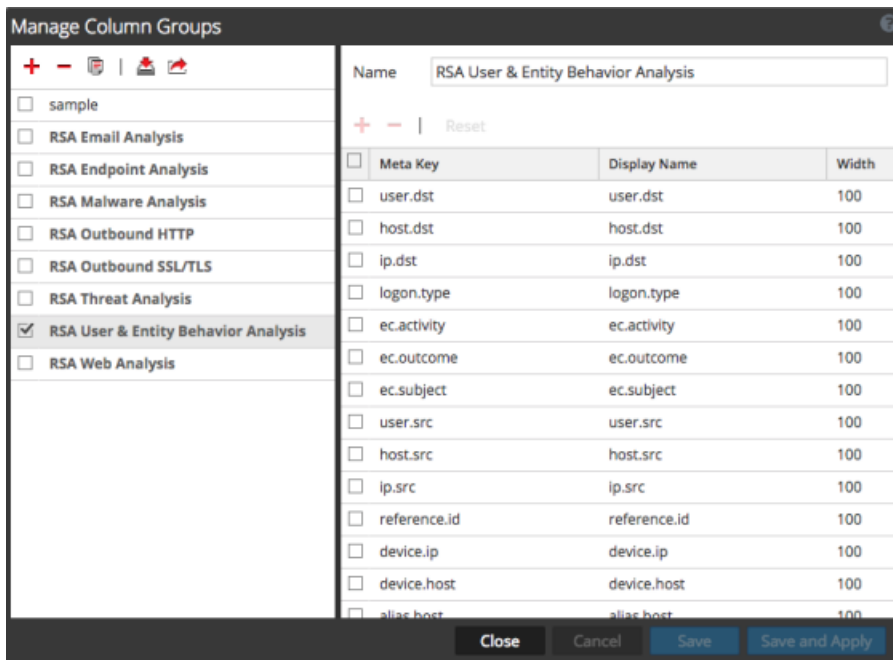
カスタムの列グループをエクスポートして他のチームメンバーと共有できます。エクスポートしたファイルのコピーを他のアナリストに提供すれば、そのアナリストは列グループをインポートできます。



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。

- 調査** > **レガシー イベント**に移動します。
- 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。



- 列グループをエクスポートするには、名前の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。
- 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。
- 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、および制限フィルタ(プレクエリ条件)を迅速かつ簡単に定義する方法を提供します。同じクエリプロファイルはすべてのビューで共有され、スプリングボード(バージョン11.5)のパネルで使用できます。[イベント]ビューで作成されたプライベート クエリプロファイルは、それを作成したアナリストの [イベント]ビューでのみ使用可能になります。

クエリプロファイルはそれぞれ、メタグループや列グループを指定し、場合によっては、調査のタイプに適したプレクエリ条件を含んでいます。

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。(「[イベント リストでの列と列グループの使用](#)」を参照)。
- クエリプロファイルを有効にすると、オプションのプレクエリ条件によって、クエリバーに制限フィルタが追加されます。制限フィルタを編集または削除してから、クエリに対して追加のフィルタを作成できます(「[\[イベント\]ビューでの結果のフィルタリング](#)」を参照)。

標準提供クエリプロファイル

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、[レガシー イベント]ビュー、または [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]ビューでは、標準提供プロファイル名は「RSA」で始まり、[デフォルト プロファイル]の下に表示されます。[イベント]ビューでは、クエリプロファイルのグループ化はサポートされていません。次の図は、[クエリプロファイル]メニューに表示された標準提供クエリプロファイルの例です。



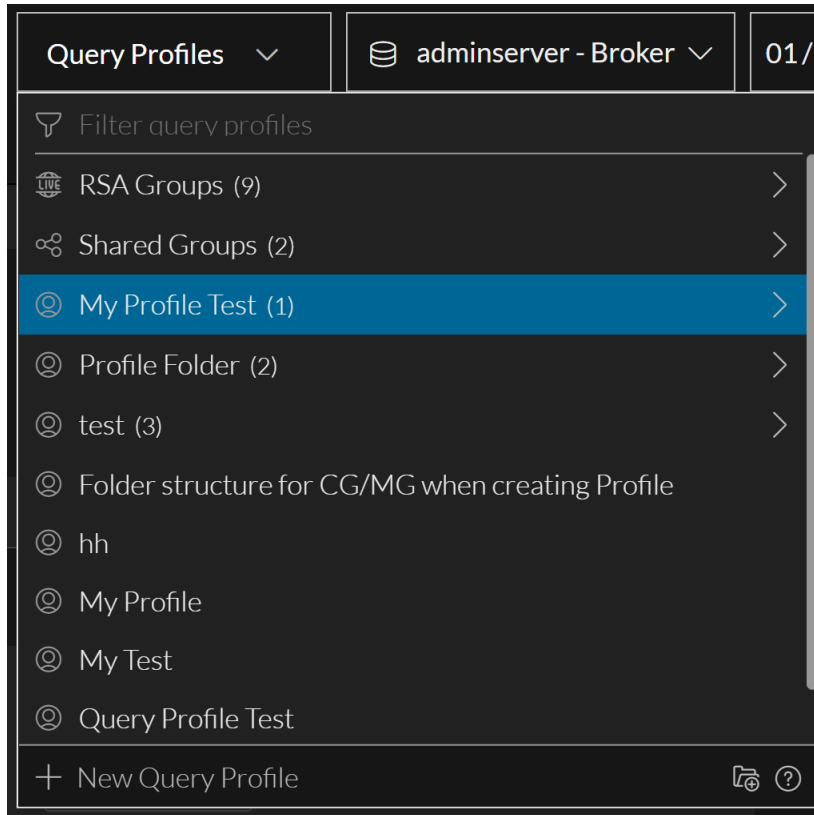
NetWitness Platformには、次のような標準提供プロファイルがあります。

- RSA Email Analysis
- RSA Endpoint Analysis
- RSA File Analysis
- RSA Threat Analysis
- RSA User & Entity Behavior Analysis
- RSA Web Analysis

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グループ、列グループ、およびプレクエリ条件が自動的に指定されます。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。

Liveクエリプロファイル

11.6以降では、NetWitnessは、Liveからの調査コンテンツの導入をサポートしています。これらのコンテンツは、クエリプロファイルグループのドロップダウンの下にLive記号 (L) でマークされて表示されます。クエリプロファイルは、RSAグループ (RSA LiveコンテンツおよびRSA OOTBグループ) と共有グループに分類されます。グループは、編集可能な共有グループを除いて、編集不可能なフォルダおよびサブフォルダとして表示されます。プライベート コンテンツはすべて、これらのグループの外部に表示されます。たとえば、次の画像は、共有グループ フォルダの下位にあるプライベート コンテンツを示しています。()内の数字はフォルダー内のコンテンツの数を示し、>記号はフォルダー内をドリルダウンするために使用されます。



カスタム クエリプロファイル

バージョン11.4では、カスタム クエリプロファイルが組織内でグローバルに共有されます。バージョン11.5以降では、共有クエリプロファイルを以前と同様に作成できます。また、プライベート クエリプロファイルを作成することもできます。共有のカスタム クエリプロファイルを編集する場合、変更はグローバルに適用されます。共有のカスタム クエリプロファイルを削除すると、そのプロファイルは削除され、すべてのアナリストが使用できなくなります。

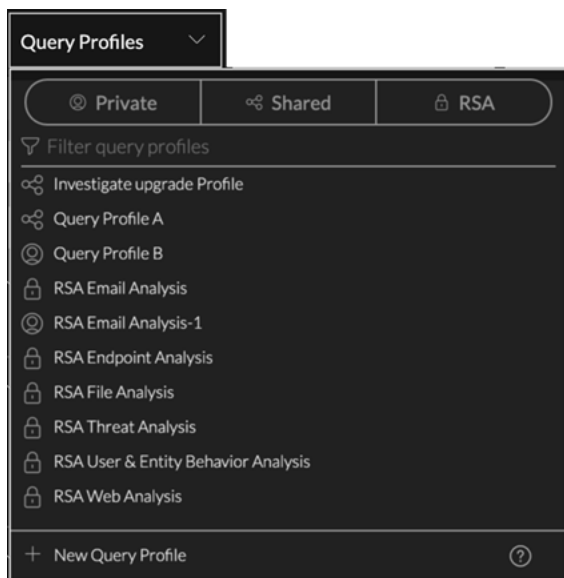
注：スプリングボード パネルでクエリプロファイルがフィルタとして使用されている場合、プロファイルを編集することはできませんが、[イベント]ビューで削除することはできません。ただし、[ナビゲート]ビューまたは [レガシー イベント]ビューでのプロファイルの削除は何によっても妨げられません。この場合、削除されたクエリプロファイルをフィルタとして使用するスプリングボード パネルは引き続き機能しますが、フィルタが削除され、予期しない結果がパネルに表示されることがあります。詳細については、『NetWitness Platformスタート ガイド』の「スプリングボードの管理」を参照してください。

バージョン11.5では、クエリプロファイルを作成する時に、共有するかプライベート(デフォルト)にするか選択できます。共有プロファイルをプライベートに変更したり、プライベートプロファイルを共有に変更することはできません。プライベート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、またはスプリングボードでは表示または使用できません。[クエリプロファイル]メニューでは、プロファイルタイプはアイコンで識別されます。以下は、[クエリプロファイル]メニューに表示され、行の最後に編集アイコンを持つ共有およびプライベートのカスタムクエリプロファイルの例です。

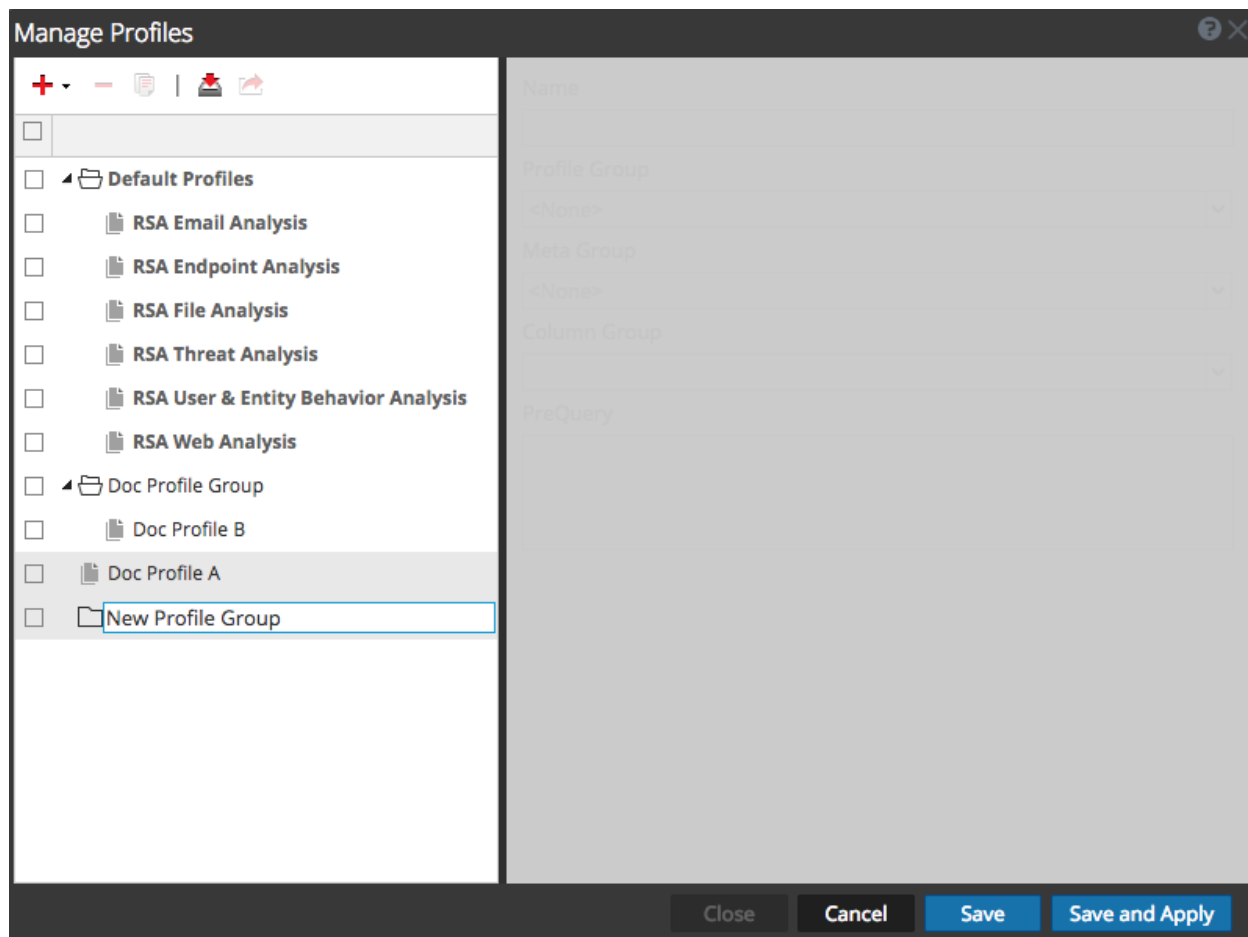


クエリプロファイルを管理するためのダイアログ

[クエリプロファイル]メニューには、プロファイル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プロファイルと標準提供のプロファイルを区別できます。クエリプロファイルを管理するための機能は[ナビゲート]ビュー、[レガシーイベント]ビュー、および[イベント]ビューで似ていますが、ダイアログは異なります。次の図は、バージョン11.5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、コピー、編集、削除、適用が可能です。上部のフィルタリングボタン(プライベート、共有、RSA)を使用してプロファイルのリストをフィルタリングし、プライベート、共有、および標準提供のクエリプロファイルを任意の組み合わせで表示できます。



次の図は、[ナビゲート]ビューおよび[レガシーイベント]ビューでの[プロファイルの管理]ダイアログの例です。



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、バージョン11.4.1以前では、ユーザ間でグローバルに共有されます。ユーザがカスタム 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。「イベント」ビューでは、「クエリプロファイル」メニューを使用してプロファイル进行操作します。「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」>「管理」を選択して「プロファイルの管理」ダイアログを開きます。バージョン11.5では、カスタム プロファイルをグローバルに共有できますが、「イベント」ビューで作成されたプライベート カスタム プロファイルは、「ナビゲート」ビューまたは「レガシー イベント」ビューでは使用できません。

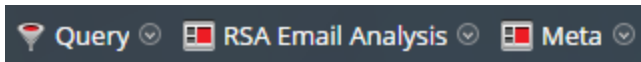
「クエリプロファイル」メニュー(11.4以降の「イベント」ビュー)を使用して、次の操作を実行できます。

- クエリプロファイルを適用し、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を作成(「クエリプロファイルの作成」ダイアログ)、コピー、編集、削除(「クエリプロファイルの詳細」ダイアログ)できます。
- プロファイルを選択すると、メタグループ、列グループ、プレクエリ条件が適用され、「メタグループ」メニュータイトル、「列グループ」メニュータイトル、クエリバーに表示されます。
- 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。バージョン11.5では、メタグループを使用できるほか、以前に使用可能であった共有カスタム クエリプロファイルに加えて、独自のカスタム クエリプロファイルを作成できます。

- [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、[イベント]ビューの同じプロファイルは、[サマリー リスト]列グループを使用します。

[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)を使用して、次の操作を実行できます。

- 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。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。
- プロファイルを選択すると、メタグループ、列グループ、プレクエリ条件が適用され、[プロファイル]メニューのラベルがクエリプロファイル名に置き換わります。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。

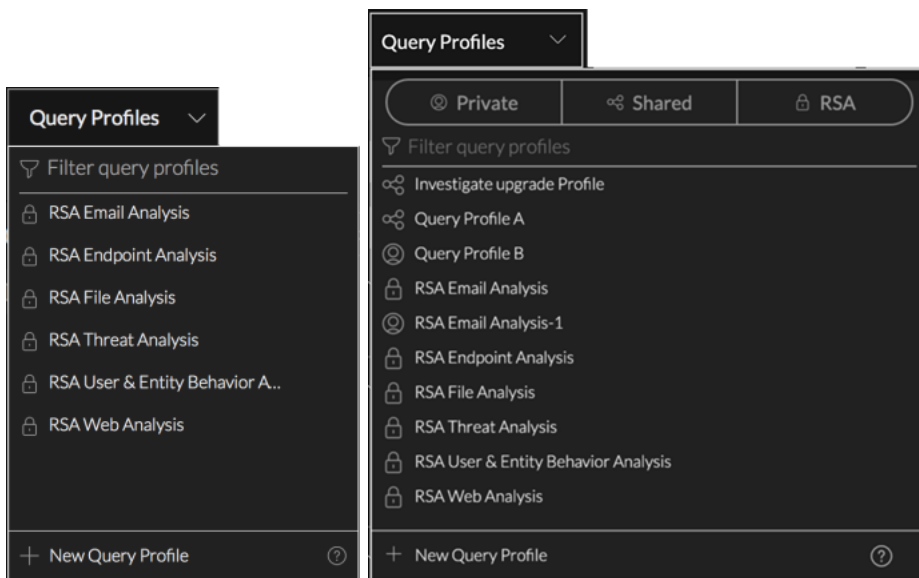



クエリプロファイルの詳細の表示([イベント]ビュー)

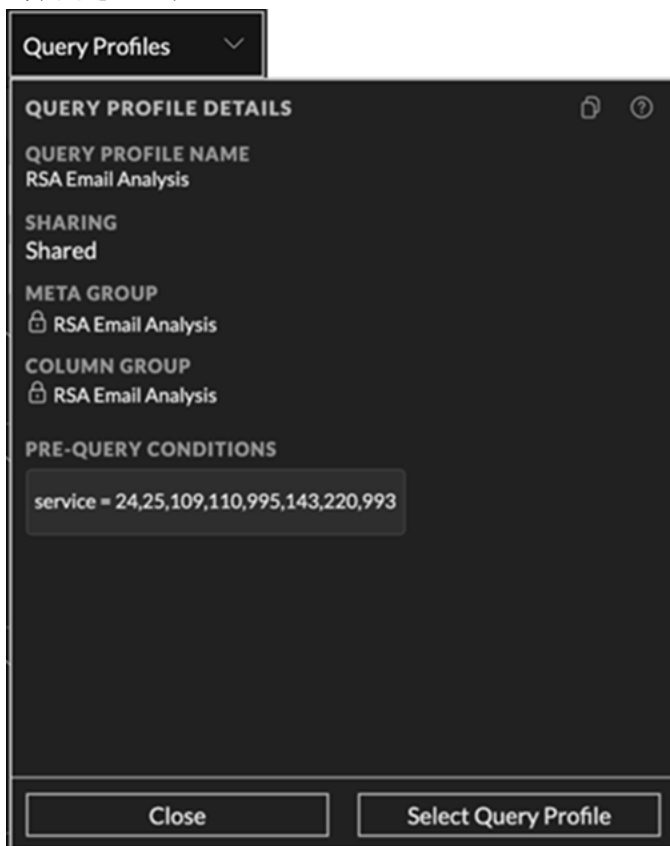
クエリプロファイルにどのメタグループ、列グループ、制限フィルタ(プレクエリ条件)が定義されているかを確認する場合は、プロファイルの詳細を表示します。

詳細を表示するには、次のようにします。

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。バージョン11.5のメニューには、標準提供クエリプロファイル(RSA)、共有カスタムプロファイル、プライベートカスタムプロファイルのリストが表示され、絞り込みフィールドにより特定のクエリプロファイルを簡単に見つけることができます。左の図は、バージョン11.4のメニューを示しています。右の図は、プライベート、共有、RSAというすべてのプロファイルタイプが表示された、バージョン11.5の初期状態のメニューを示しています。




- リスト内の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、プレクエリ条件が表示されます。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。バージョン11.5.1では、メタグループと列グループのタイプ(共有、プライベート、RSA)がアイコンで識別されます。

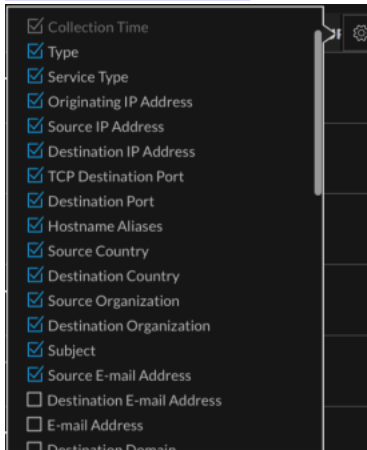


3. 次のいずれかの操作を実行します。

- a. ダイアログを閉じるには、**閉じる**]をクリックします。
- b. 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条件と列グループを使用してクエリが再実行されます。プレクエリ条件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、プレクエリ条件(たとえば、このフィルタ:service=24,25,109,110,995,143,220,993)がクエリバーに追加されますが、クエリは送信されません。**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。
 - i. (オプション) クエリを実行する前に、クエリバーに追加のフィルタを作成します(「[イベント\]ビューでの結果のフィルタリング](#)」を参照)。

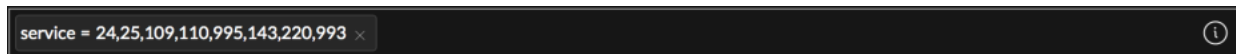


- ii. (オプション) クエリを実行する前に、関連づけられた列グループから別の列を選択する場合は、右側の**イベント**]リストの上にあるをクリックします。
列の選択リストが表示され、表示する列を最大40個選択できます(「[イベント\]リストでの列と列グループの使用](#)」を参照)。



クエリプロファイルの適用(**イベント**]ビュー)

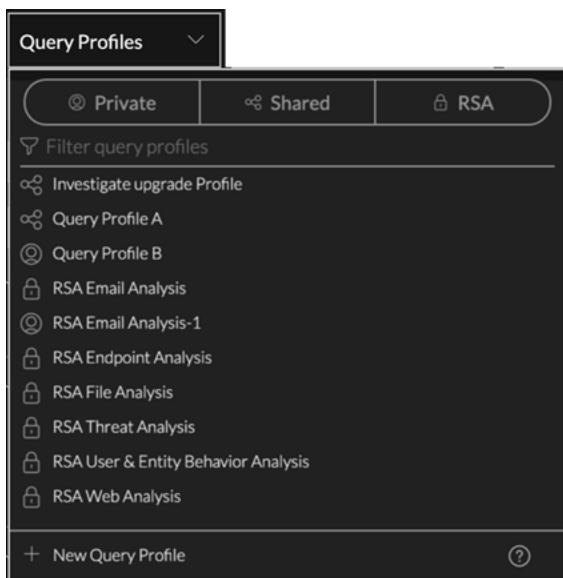
クエリプロファイルが適用されると、**クエリプロファイル**]メニューにそのことは表示されませんが、列グループまたはメタグループが有効であるかどうかは確認できます。プレクエリ条件が適用されている場合は、次の図に示すように、クエリバーの先頭にフィルタが表示されます。



注: 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条件で結果を制限している可能性があります。

クエリプロファイルを適用するには、次のようにします。

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。

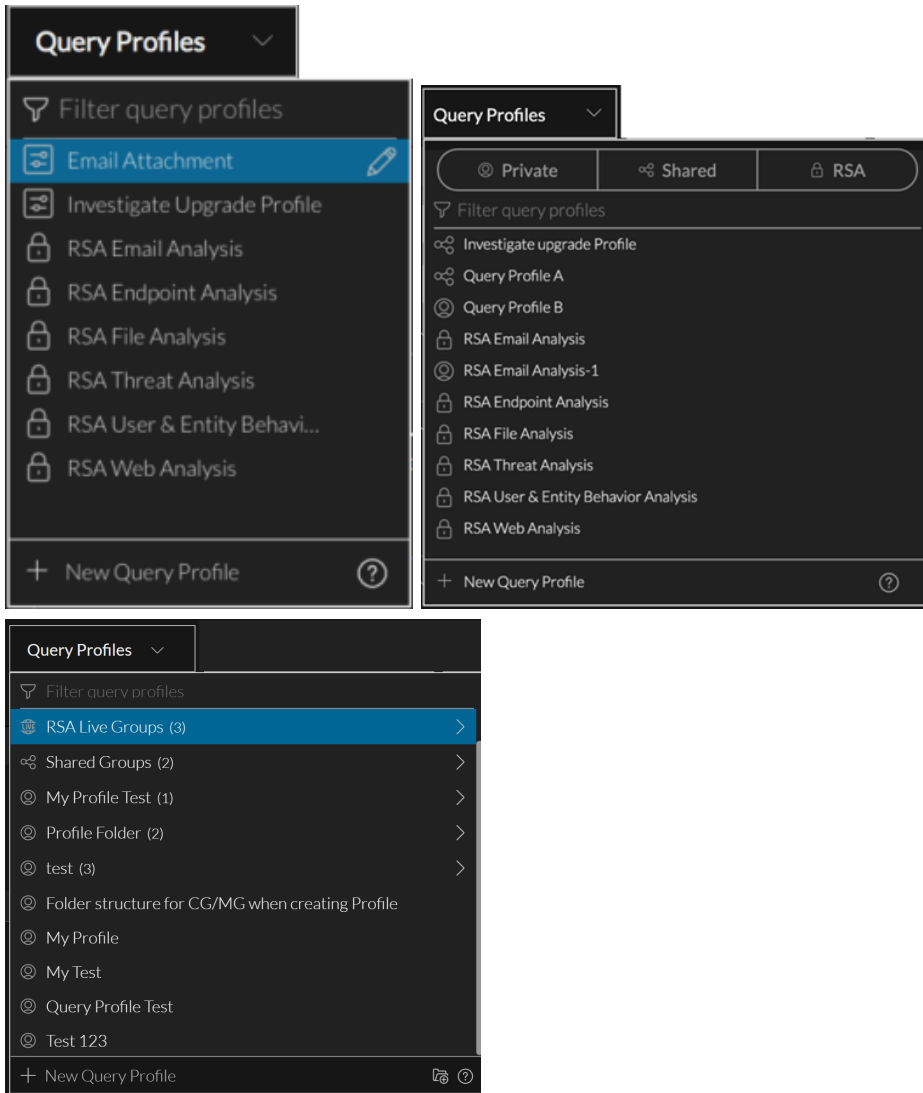


2. 上下矢印キーまたはマウスを使用して、プロフィールをハイライト表示します。
3. ハイライト表示されたプロフィールをクリックします。
クエリプロフィールの設定がただちに適用されます。選択したクエリプロフィールが反映され、[イベント]リストの表示が更新されます。プロフィールで別の列グループが使用されている場合は選択されたプロフィールのプレクエリ条件と列グループを使用してクエリが再実行されます。プレクエリ条件のみが異なる場合は、クエリバーの既存のフィルタが削除され、プレクエリ条件がクエリバーに追加されます。🔍 ボタンがアクティブになり、新しいプレクエリ条件を使用してクエリを再送信できるようになります。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. **調査**] > **イベント**]に移動し、クエリバーの **クエリプロフィール**]をクリックします。
[クエリプロフィール]メニューが開き、使用可能なプロフィールのリストが表示されます。バージョン11.6(右の図)とバージョン11.5(中央の図)は、プライベートと共有の両方のカスタムプロフィールをサポートします。バージョン11.4(左の図)は、共有カスタムプロフィールのみをサポートします。



2. 次のいずれかの操作を実行します。

- 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。
[クエリプロファイルの作成]ダイアログが表示されます。**[クエリの作成]**ダイアログには、現在選択されているメタグループ、列グループ、およびクエリバーにプレクエリ条件として現在入力しているフィルタを含む新しい空のプロファイルが表示されます。

Query Profiles

CREATE QUERY PROFILE ⓘ

QUERY PROFILE NAME
Enter query profile name

SHARING
 Share with my organization (this will not be private)

META GROUP
RSA Email Analysis

COLUMN GROUP
RSA Email Analysis

PRE-QUERY CONDITIONS
service = 24,25,109,110,995,143,220,993 ×

Close Save Query Profile

バージョン11.6では、メタグループと列グループはフォルダー構造のドロップダウンに表示されません。

Query Profiles ▾

CREATE QUERY PROFILE ⓘ

QUERY PROFILE NAME
Enter query profile name

META GROUP
SAS ▾

- 🔒 RSA Default Groups (9) >
- 🏠 RSA Live Groups (2) >
- 🔗 Shared Groups (1) >
- 📁 FolderMG-0-TOCopy (0) >

Close Save Query Profile

Query Profiles ▾

CREATE QUERY PROFILE ⓘ

QUERY PROFILE NAME
Enter query profile name

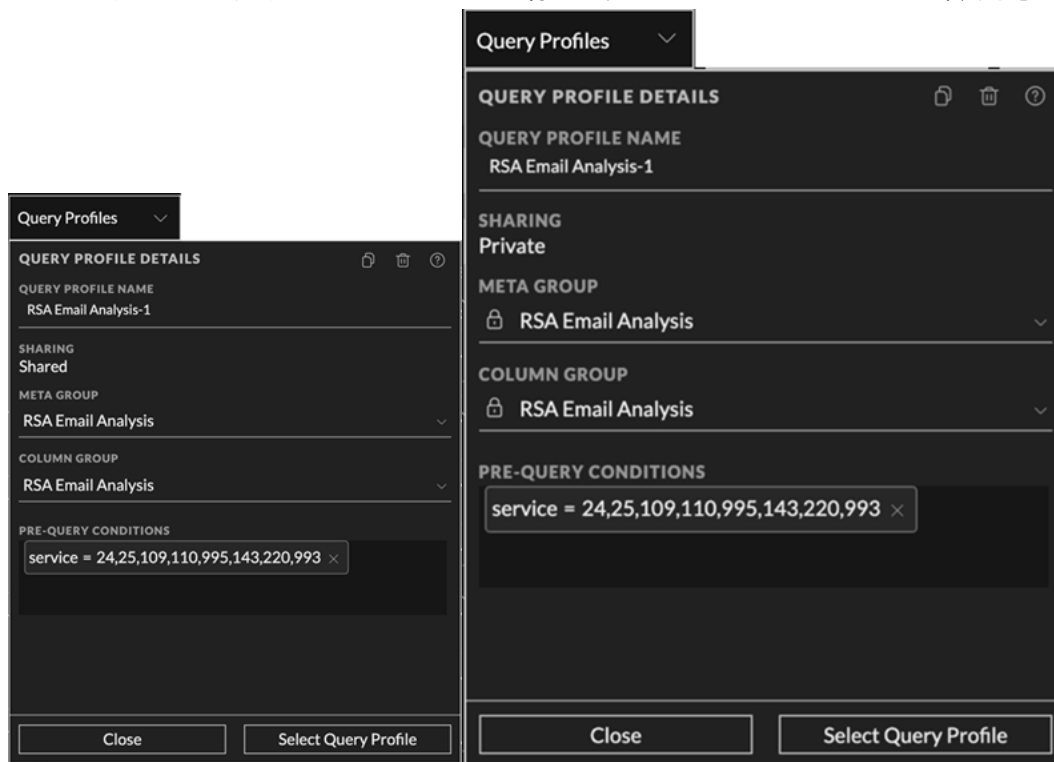
META GROUP
SAS ▾

COLUMN GROUP
RSA Endpoint Analysis ▾

- 🔒 RSA Default Groups (9) >
- 🏠 RSA Live Groups (2) >
- 🔗 Shared Groups (7) >
- 📁 abc-copy (0) >

- 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詳細」ダイアログが表示されます。バージョン11.5.1のダイアログ(右側)では、メタグループと列グループのタイプが共有、プライベート、またはRSAとして識別されます。



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。
「クエリの作成」ダイアログの「クエリプロファイルの保存」ボタンがアクティブになります。「クエリプロファイルの詳細」ダイアログでは、「クエリプロファイルの選択」ボタンのラベルが「クエリプロファイルの更新」に変更されています。
4. (バージョン11.5以降) 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組織内で共有する場合は、「組織内で共有」オプションを設定します。作成後、クエリプロファイルを共有からプライベートに変更することはできません。
 - b. 自分だけが表示して管理できるプライベート クエリプロファイルを作成するには、「組織内で共有」チェックボックスを空白のままにします。作成後、クエリプロファイルをプライベートから共有に変更することはできません。
5. (バージョン11.5以降) 「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。共有グループとプライベートグループの名前が同じである場合、プライベートグループは共有グループの前に表示されます。バージョン11.5.1では、グループ名の前にあるアイコンでプライベートと共有を区別できます。
6. 「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。バージョン11.5には、共有グループまたはプライベートグループがあり、同じ名前を付けることができます。この例では、プライベートグループが共有グループの前に表示されています。バージョン11.5.1では、グループ名の前にあるアイコンでプライベートと共有を区別できます。

7. **プレクエリ条件**]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フィルタを確認し、必要に応じてフィルタを追加または削除します。
8. **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。
9. ダイアログを閉じるには、**閉じる**]をクリックします。

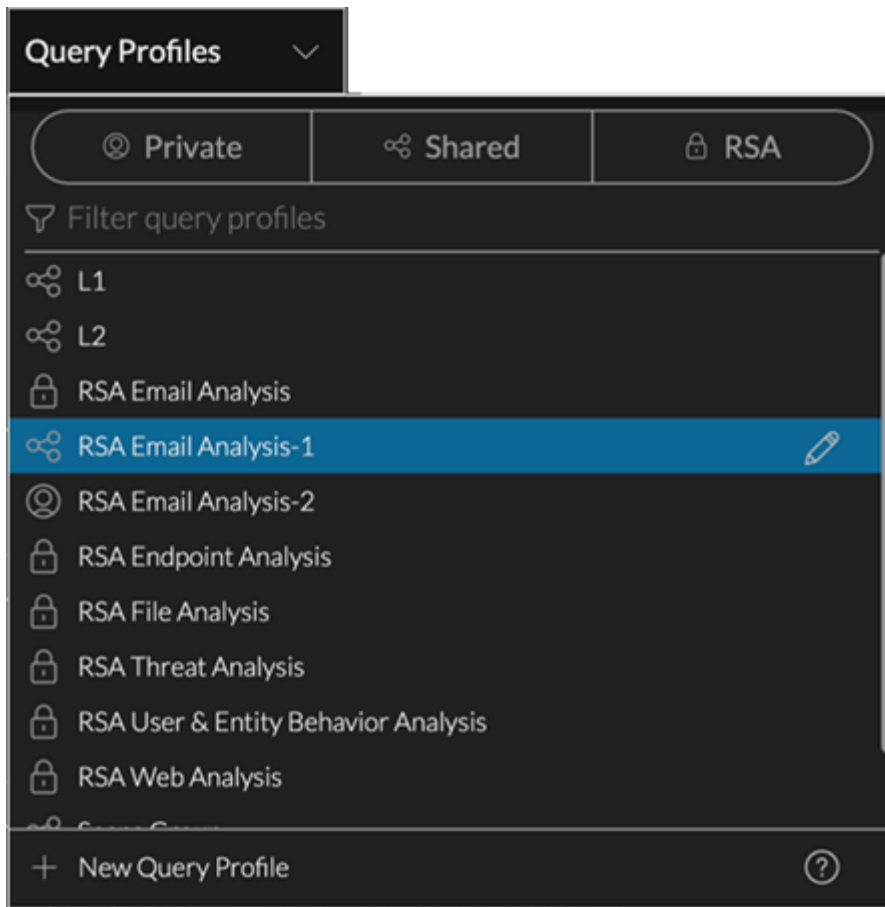
カスタム クエリ プロファイルの削除(**イベント**]ビュー)

標準提供クエリプロファイルは読み取り専用であり、削除することはできませんが、カスタムクエリプロファイルは削除できます。確認メッセージが表示され、削除を確認またはキャンセルできます。共有クエリプロファイル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プロファイルを使用できなくなります。

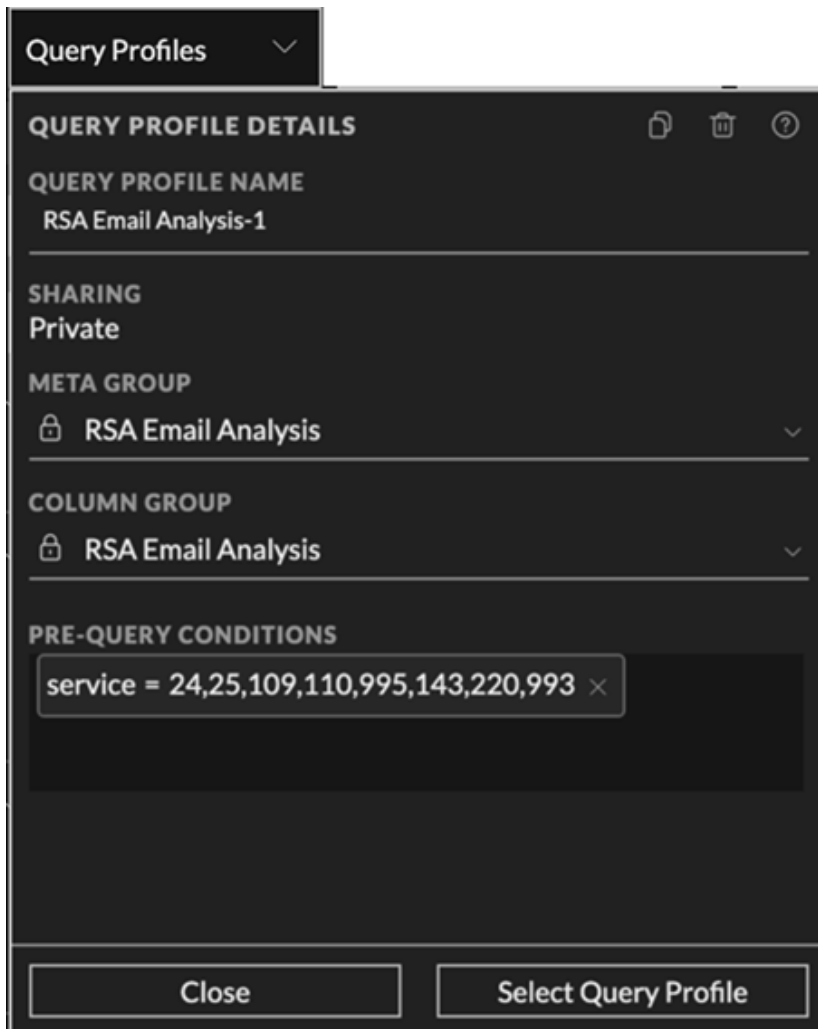
注：スプリングボード パネルでクエリプロファイルがフィルタとして使用されている場合、プロファイルを編集することはできますが、**イベント**]ビューで削除することはできません。ただし、**ナビゲート**]ビューまたは**レガシー イベント**]ビューでのプロファイルの削除は何によっても妨げられません。この場合、削除されたクエリプロファイルをフィルタとして使用するスプリングボード パネルは引き続き機能しますが、フィルタが削除され、予期しない結果がパネルに表示されることがあります。詳細については、『*NetWitness Platform* スタート ガイド』の「スプリングボードの管理」を参照してください。


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. **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. 削除するカスタム クエリ プロファイルをハイライト 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。




- 削除アイコン() をクリックします。
バージョン11.5では、確認メッセージが表示され、削除を確認するかキャンセルすることができます。
[キャンセル] または [クエリプロファイルの削除] をクリックします。
バージョン11.4では、クエリプロファイルが標準提供プロファイルでない場合に確認は求められません。
プロファイルが削除され、[クエリプロファイル] メニューに表示されなくなります。削除したプロファイルは、調査を行うアナリストには表示されなくなります。

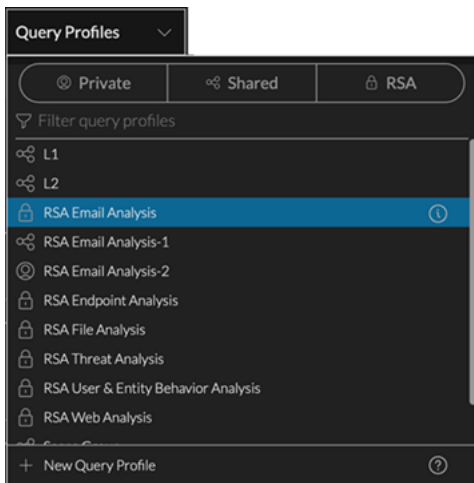
クエリプロファイルのコピー(バージョン11.5以降)



未保存の編集が進行中でない限り、標準提供またはカスタム、共有またはプライベートのいずれかにかかわらず、任意のクエリプロファイルをコピーできます。この機能は、標準提供プロファイルのカスタマイズされたバージョンが必要な場合に便利です。また、カスタムプロファイルをプライベートから共有に、または共有からプライベートに変更することはできないため、コピーを作成することで、別の共有設定を選択できるようになります。プロファイルをコピーすると、同じ名前が使用され、番号が付記されます。たとえば、RSA Email Analysisをコピーした場合、最初のコピーはRSA Email Analysis-1という名前になり、同じプロファイルの2番目のコピーはRSA Email Analysis-2という名前になります。コピーを作成したら、新しいプロファイルを編集して新しい名前を付け、プロファイル内のプレクエリ条件、メタグループ、および列グループを編集できます。

注：プライベートメタグループまたは列グループを使用するプライベートクエリプロファイルの共有コピーを作成している場合は、メタグループまたは列グループの共有コピーが作成され、クエリプロファイルで使用されていることを通知するメッセージが表示されます。プライベートメタグループまたは列グループをコピーする必要がある場合は、クエリプロファイルのコピーに少し時間がかかることがあります。

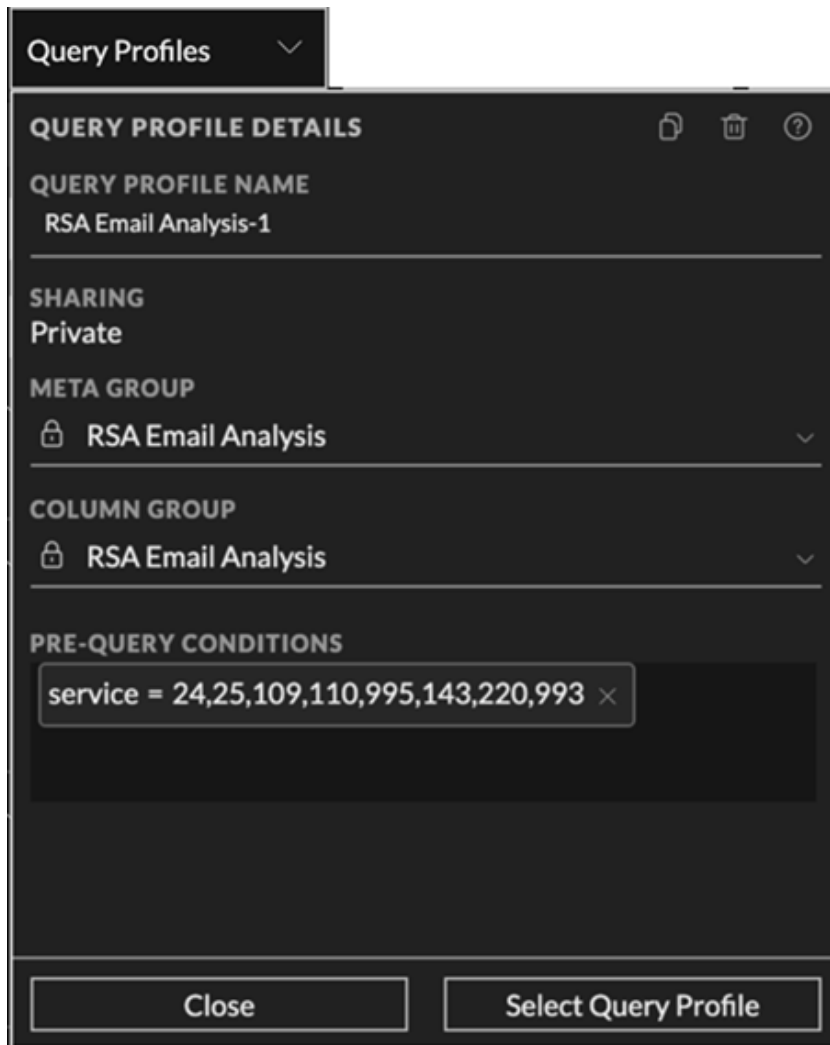
クエリプロファイルをコピーするには、次の手順を実行します。

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. コピーするクエリプロファイルをハイライト表示します。この図は、RSA Email Analysisがハイライト表示されていることを示しています。情報アイコン() が右側に表示されます。



3. 次のいずれかの操作を実行します。
 - a. 情報アイコン() をクリックします。
 - b. カスタムプロファイルの場合は、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。この図は、標準提供プロファイルのダイ

アログを示しています。



4. コピーアイコン(📄)をクリックします。
[クエリプロファイルのコピー]ダイアログが開き、プロフィール名に番号が付記されて、すべてのクエリプロファイル間で一意の名前が作成されます。




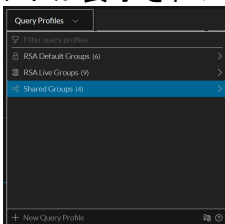
5. (オプション) [クエリプロファイル名]フィールドで、クエリプロファイルの名前を編集します。
6. 新しいプロフィールを組織内で共有する場合は、[組織内で共有]オプションを設定します。デフォルトで、新しいプロフィールはプライベートです。コピー対象のプロファイルにプライベート列グループまたはメタグループがある場合は、共有コピーが作成され、プロフィールのコピーで使用されます。


7. 次のいずれかの操作を実行します。
 - a. プロファイルをコピー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. クエリ プロファイルのコピーを保存するには、**クエリ プロファイルの保存**]をクリックします。
クローンが保存され、クローン プロファイルの **クエリ プロファイルの詳細**]ダイアログが表示されま
す。
8. 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. ダイアログを閉じて新しいプロファイルを選択するには、**クエリ プロファイルの選択**]をクリックしま
す。
クエリ プロファイル]メニューにグループが追加されます。

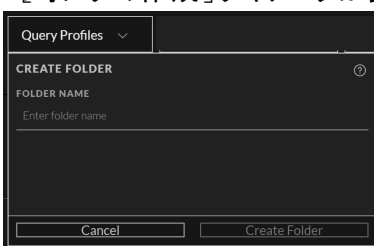
クエリ プロファイル フォルダの作成

最上位に存在し、プライベート フォルダまたは共有フォルダとして追加されるクエリ プロファイル フォルダ
を作成できます。また、フォルダ名がすでに存在する場合は、一意の名前を入力するように求められま
す。

1. **イベント**]ビューで、**クエリ プロファイル**]メニューのタイトルを選択します。メニューがドロップダウンし
て、メタグループとフォルダのリストが表示されます。上部に **クエリ プロファイルの絞り込み**]フィー
ルドが表示され、下部に  オプションが表示されます。




2.  をクリックします。
フォルダの作成]ダイアログが表示されます。

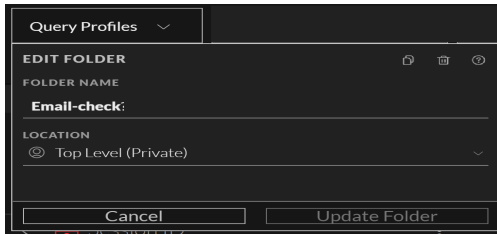


3. **フォルダ名**]フィールドに、新しいクエリ プロファイル グループ フォルダの一意の名前を入力します。
4. **フォルダの作成**]をクリックします。

クエリ プロファイル フォルダの編集と移動

クエリ プロファイル グループ フォルダーを作成した後、それを編集または移動できますが、RSAグループ
(RSA LiveコンテンツおよびRSA OOTBグループ) 内のフォルダは編集も移動もできません。プライベート
フォルダおよび共有フォルダ内のフォルダは、それぞれのグループ内でのみ編集および移動できます。た
とえば、共有フォルダをプライベート フォルダに移動したり、その逆を行ったりすることはできません。



1. [イベント]ビューで、編集する [クエリプロファイル]メニューのタイトルを選択します。
2. をクリックします。
[フォルダの編集]ダイアログが表示されます。

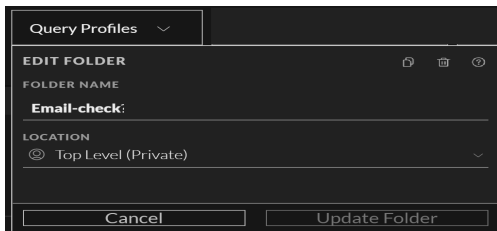


3. [フォルダ名]フィールドに、クエリプロファイルフォルダの一意の名前を入力します。
4. 編集するフォルダの場所を選択します。
5. [フォルダの更新]をクリックします。

クエリプロファイルフォルダのコピー

クエリプロファイルフォルダをプライベートから共有、プライベートからプライベート、共有から共有、共有からプライベート グループにコピーできます。フォルダをコピーすると、そのフォルダの内容はサブフォルダを除いてコピーされます。プライベート フォルダを共有フォルダにコピーすると、フォルダとその内容はプライベートのままではなくなります。

1. [イベント]ビューで、[クエリプロファイル]メニューの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て、クエリプロファイルとフォルダのリストが表示されます。
2. コピーするフォルダを選択します。
3. 編集 をクリックして、をクリックします。



[フォルダのコピー]ダイアログが表示されます。




4. [フォルダ名]フィールドに、新しいクエリプロファイルグループとフォルダの一意の名前(最大80文字)を入力します。

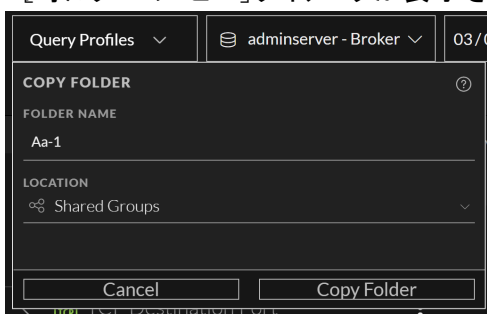
5. 編集するフォルダの場所を選択します。
6. 「フォルダのコピー」をクリックします。

Liveから導入されたクエリ プロファイル グループ フォルダのコピー

RSA Groupsカテゴリーの下にあるLiveから導入されたクエリ プロファイル グループ フォルダを、共有グループなどの他の場所またはプライベート フォルダにコピーできます。

1. 「イベント」ビューで、「クエリ プロファイル グループ」メニューの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て、クエリ プロファイル グループとフォルダのリストが表示されます。
2. コピーするLiveクエリ プロファイル グループ フォルダをクリックします。


3.  をクリックします。
「フォルダのコピー」ダイアログが表示されます。

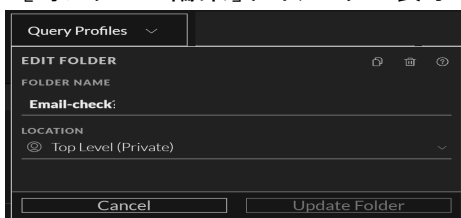


4. コピーするフォルダの場所を選択します。
5. 「フォルダのコピー」をクリックします。
フォルダの元の名前とその内容でフォルダが作成され、元のメタグループ名に-nが付記された名前が表示されます。

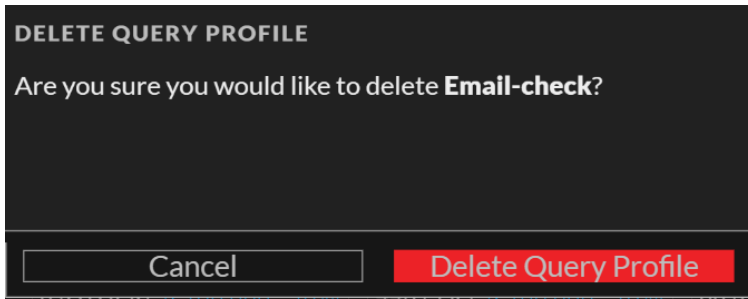
クエリ プロファイル フォルダの削除

保持したくないフォルダは削除できます。ただし、フォルダを削除すると、そのフォルダを取得できなくなります。

1. 「イベント」ビューで、「クエリ プロファイル」メニューの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て、クエリ プロファイル グループとフォルダのリストが表示されます。
2. 削除するフォルダを選択します。
3.  をクリックします。
「フォルダの編集」ダイアログが表示されます。



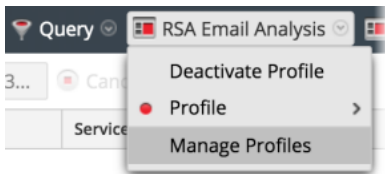
- 削除  をクリックします。
アクションを確認するための警告メッセージが表示されます。



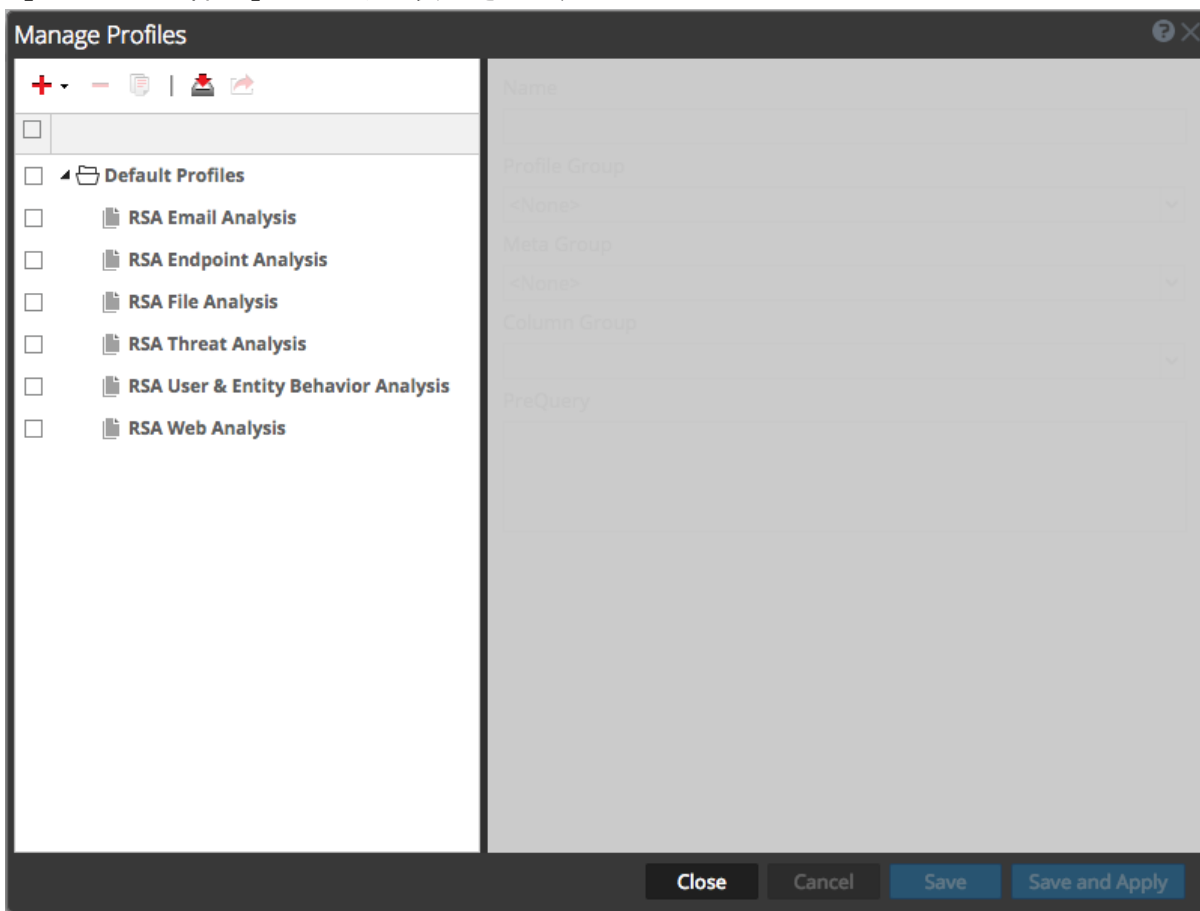
- (オプション) 選択したフォルダ内のすべてのコンテンツとともにフォルダを削除する場合は、このチェックボックスを選択します。
チェックボックスを選択しないと、必要なフォルダが削除された後で、コンテンツは親フォルダに移動されます。
- [OK] をクリックして削除します。

プロフィールの管理]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)

- 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)。
- ツールバーで、**プロフィール]** > **プロフィールの管理]** 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)

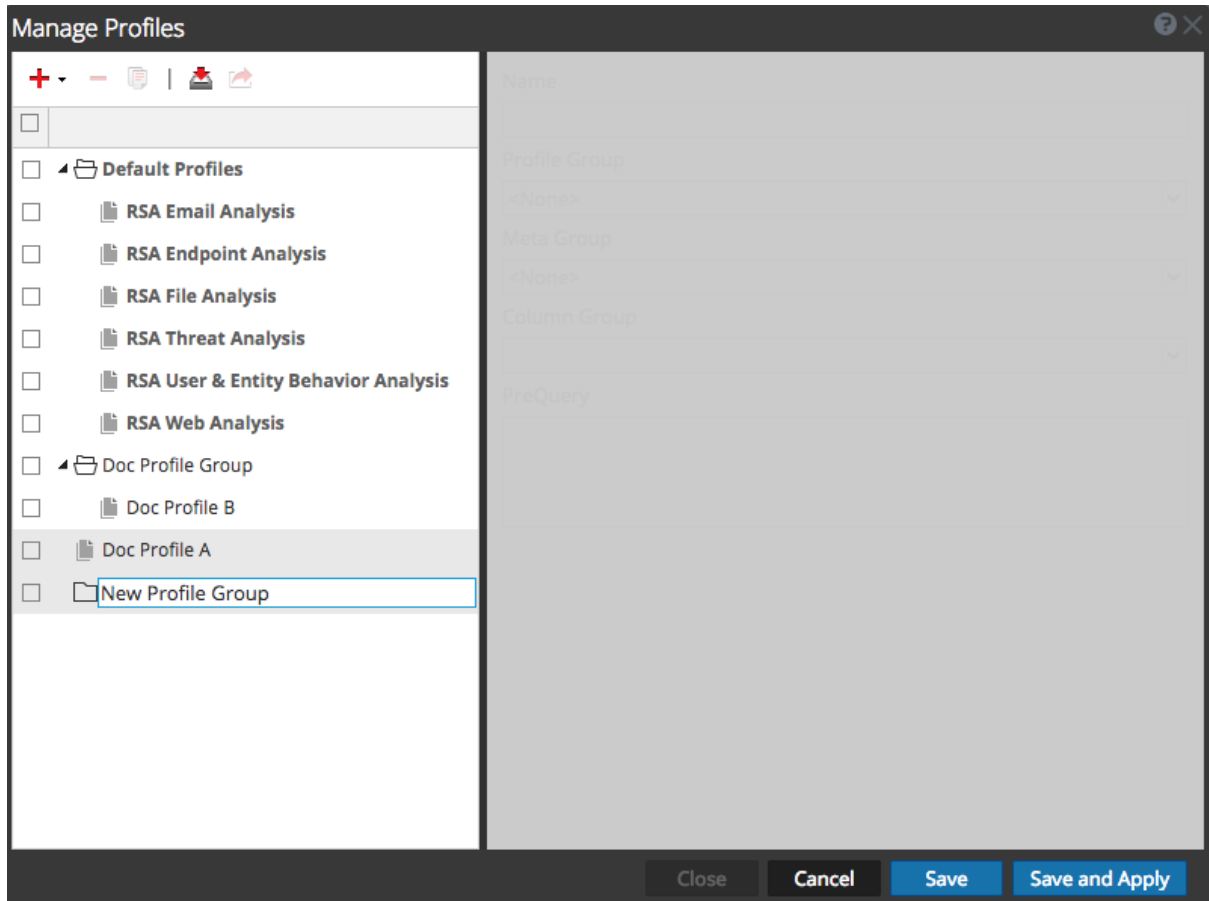
カスタムプロファイルグループを作成して、異なるプロファイルを整理することができます。作成後、プロファイルグループに対して直接行える編集は、プロファイルグループの名前の編集だけです。グループにプロファイルを追加または削除するには、プロファイルを編集し、別のプロファイルグループを割り当てます(詳細は、「[プロファイルの作成と編集\(「ナビゲート」ビューまたは「レガシーイベント」ビュー\)](#)」を参照)。

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。



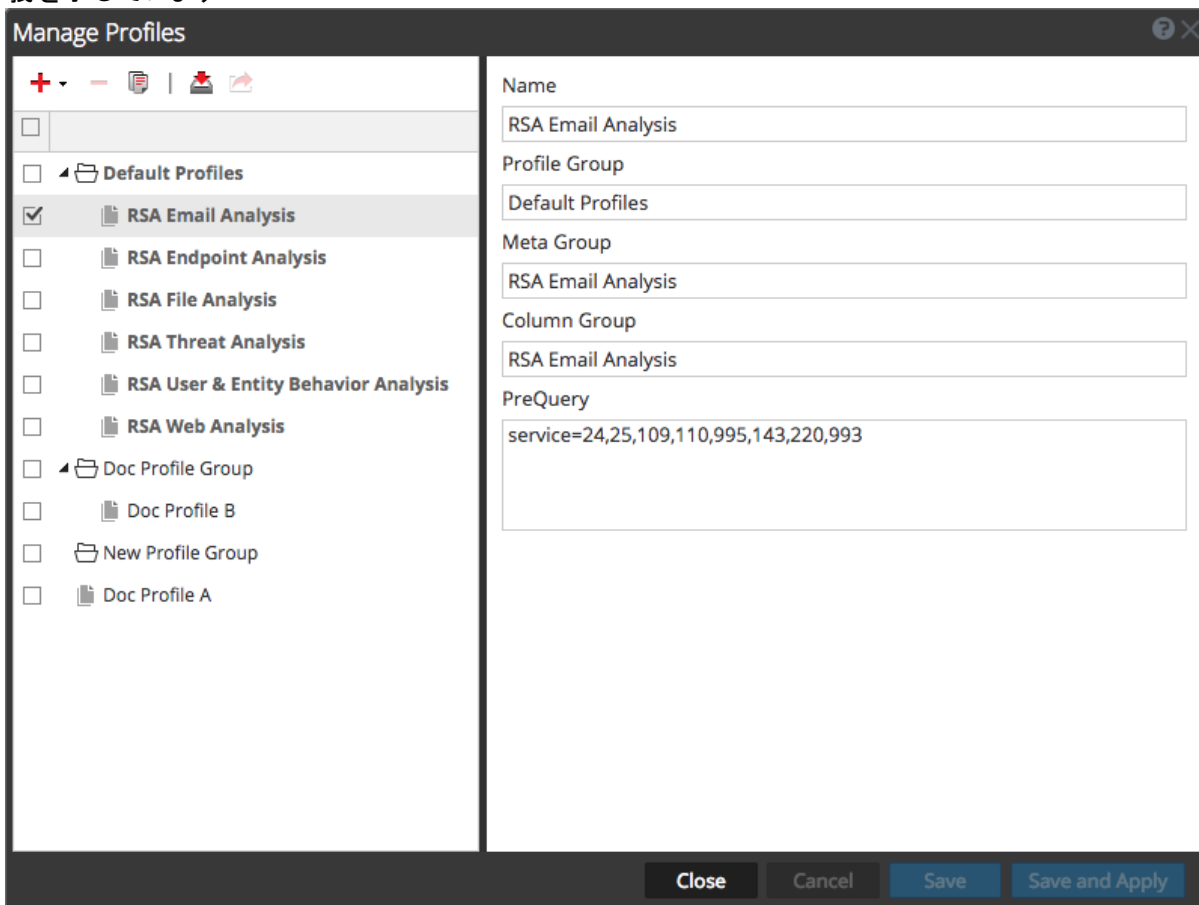
2. プロファイルグループの名前を編集または入力するには、プロファイルグループをダブルクリックし、入力フィールドに入力します。名前は2～80文字の長さにする必要があります。プロファイルグループ名は、新しいプロファイルグループまたは編集したプロファイルグループに適用されます。プロファイルを設定するときに、プロファイルグループを使用できるようになります。
3. プロファイルグループを削除するには、次のいずれかの操作を行います。
 - プロファイルを削除することなく、プロファイルグループを削除する場合は、グループのチェックボックスをクリックし、グループ内のプロファイルのチェックボックスをオフにして、**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フにしている場合、グループとグループ内のプロファイルは削除されます。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 [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。



The screenshot shows the 'Manage Profiles' dialog box. On the left, there is a list of profiles under 'Default Profiles'. 'RSA Email Analysis' is selected. On the right, the configuration for 'RSA Email Analysis' is shown:

Name	RSA Email Analysis
Profile Group	Default Profiles
Meta Group	RSA Email Analysis
Column Group	RSA Email Analysis
PreQuery	service=24,25,109,110,995,143,220,993

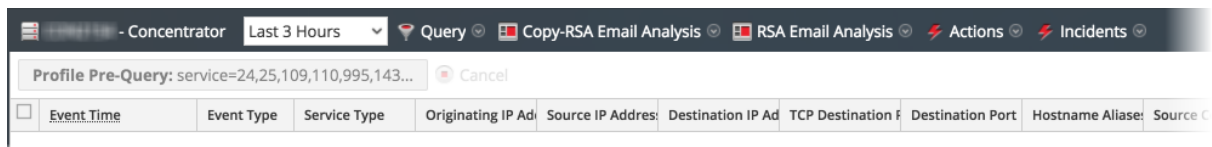
At the bottom, there are buttons for 'Close', 'Cancel', 'Save', and 'Save and Apply'.

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。カスタムメタグループを「[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](#)」で説明されているように追加できます。[イベント]ビューで作成されたプライベートメタグループは、[ナビゲート]ビューでは使用できません。
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。[イベント]ビューで作成されたプライベート列グループは、[ナビゲート]ビューでは使用できません。
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せずに保存するには **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. **プロフィール** オプションにマウス ポインターを置くと、使用可能なプロフィールのドロップダウン リストが表示されます。
3. 使用するプロフィールを選択します。
そのプロフィール設定が即座に適用されます。

プロフィールの管理 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、**プロフィール** > **プロフィールの管理** を選択します。
プロフィールの管理 ダイアログが表示されます。
2. 左側のパネルでプロフィールを選択し、**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。
そのプロフィール設定が即座に適用されます。


プロフィールのインポート(**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.jsonファイルをアップロードまたはインポートできます。プロフィール グループをエクスポートしてインポートすると、プロフィールのグループ化を維持できます。

1. **プロフィールの管理** 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。
プロフィールのインポート 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。
プロフィールが左側のパネルに表示されます。

プロフィールのダウンロード(**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、プロフィールを.jsonファイルとしてダウンロードできません。

1. **プロフィールの管理** 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ィールを選択します。
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】ビューでのメタデータのドリルダウン(ベータ版)

注：このセクションはバージョン11.5以降に適用されます。この機能は、デフォルトで有効になっているベータ機能であり、システム管理者が『システムセキュリティおよびユーザー管理ガイド』の説明に従って無効にすることができます。

【イベント】ビューでは、順番に並んだ関連イベントの可能な限り最小のセットに調査のフォーカスを当てます。クエリプロファイル、列グループ、メタグループ、およびクエリを使用して、【イベント】ビューに読み込まれる表示可能なイベントの数を減らすことができます。ただし、DecoderまたはLog Decoderに格納されている実際のイベントを確認する前に、Concentratorでインデックス付けされたメタデータを使用してデータセットを制限する方が効率的です。

バージョン11.4.x以前では、Concentratorでインデックス付けされたメタキーとメタ値を確認することから始め、【イベント】ビューでメタデータをドリルダウンして、関連するイベントのセットを見つけ、ドリルダウンまたはクエリのたびにデータセットをさらに制限するのが最善です。有意なデータセットまたはドリルダウンポイントがある場合は、【イベント】ビューで関連するイベントの詳細を順番に調べることができます。

バージョン11.5以降、【イベント】ビューを離れることなく、【イベントの絞り込み】パネルでメタデータをドリルダウンできます。表示されるメタキーとメタ値のリストは、クエリの時間範囲で環境に確認されたすべてのイベントに関連しています。【イベントの絞り込み】パネルで目的のドリルダウンポイントを見つけたら、【イベント】パネルを開いてシーケンシャルイベントを表示できます。【イベント】ビューに読み込まれるイベントの数が少なくなり、読み込みが速くなります。調査の流れが、ビュー間の切り替えが少なくなることで、スムーズになります。次の図は、【イベント】パネルの左側に開いたパネルを示しています。

The screenshot displays the NetWitness Investigate interface. On the left, a 'Filter Events' panel is open, showing a list of meta-groups with expandable options. The main area shows a table of events with the following columns: COLLECTION TIME, TYPE, SERVICE TYPE, ORIGINATING..., IP ALIASES, SOURCE IP AD..., DESTINATION..., TCP DESTINA..., and HOSTNAME ALIASES. The table contains several rows of event data, including collection times and various network-related details.

注： [イベントの絞り込み] パネルの結果が期待どおりにならない状況は2つあります。

- バージョン11.5のBrokerとRSA NetWitness Platformバージョン11.4以前の一部のCoreサービスを使用する混在モード環境では、テキスト フィルタが [イベントの絞り込み] パネルでサポートされていません。 [イベント] パネルのクエリにテキスト フィルタが含まれている場合は、 [イベント] パネルと [イベントの絞り込み] パネルの結果セットが異なることがあります。
- [イベント] ビュー クエリビルダーのクエリに論理 OR または && が含まれている場合は、 [イベント] ビューの結果が [ナビゲート] ビューおよび [レガシー イベント] ビューでの同じクエリの結果と異なることがあります。このような場合、 [ナビゲート] ビューと [レガシー イベント] ビューでは、論理 OR 式が括弧のセットで自動的に囲まれるのに対し、 [イベント] ビューでは、括弧を手動で追加する必要があります。論理 OR 式を追加の括弧のセットで囲むには、クエリバーでフィルタを2つ選択し、そのうちの1つを右クリックして、メニューで **括弧で囲む** を選択します。

注：(バージョン11.5.1) [イベントの絞り込み] パネルでは、メタ値の結果の閾値は100000です。結果が閾値を超えている場合は、~または>を使用して示されます。たとえば、「(>100000)」は、結果がカウントに基づいてソートされ、閾値よりも大きいことを示します。同様に、「(~100000)」は、結果がサイズに基づいてソートされ、閾値よりも大きいことを示します。

動作モード

[イベントの絞り込み] パネルには2つの動作モードがあります。


- **縮小モードの [イベントの絞り込み] パネル**は、データに対するファセット 検索ビューの一部です(上図に表示)。メタ値を左クリックまたは右クリックすると、新しいフィルタが追加され、新しいクエリが自動的に実行されて、一致するイベントがイベントのシーケンシャルリストに表示されます。両方のパネルが開いている場合は、 [イベントの絞り込み] パネルと [イベント] パネルの両方のデータをドリルダウンできます。 [イベントの絞り込み] パネルでメタ値を左クリックするたびに、式がクエリバーに追加され、デフォルトでクエリが実行されます。クエリ結果には、 [イベントの絞り込み] パネルでフィルタの基準にする新しいメタデータと、 [イベント] パネルのクエリに一致する結果のイベントが表示されます。 [イベント] パネルのサービスまたはその他のクエリ要素を変更する場合は、クエリを実行して [イベントの絞り込み] パネルを再ロードする必要があります。
- **完全展開モードの [イベントの絞り込み] パネル**は、ブラウザー ウィンドウの全幅を使用して、クエリをすぐに送信したり、シーケンシャル イベントを表示したりするというパフォーマンスの負荷なしに、メタデータを検索するための十分な表示領域を提供します。新しいメタ値をクリックしてメタ値をドリルダウンすると、各メタ値がクエリフィルタに追加され、 [イベントの絞り込み] パネルで実行されるため、表示されるイベントの数が少なくなります。 [イベント] パネルが閉じているため、 [イベント] パネルのクエリは更新されず、クエリは実行されません。 [イベントの絞り込み] パネルを元のサイズに折りたたむと、 [イベント] リストが開き、クエリが実行されます。これは、完全展開モードのパネルの例です。


The screenshot shows the NetWitness Investigate interface with the 'EVENTS' tab selected. The search criteria are 'SA - Broker' and the time range is '10/01/2020 02:55 pm - 10/16/2020 04:13 am'. The 'Filter Events' section is set to 'Event Count (Descending by Total Count)'. A callout box highlights the '25 [SMTP] (2,078)' event, with a tooltip showing 'Meta Value = 25 [SMTP]' and 'Event Count = 2,078'.

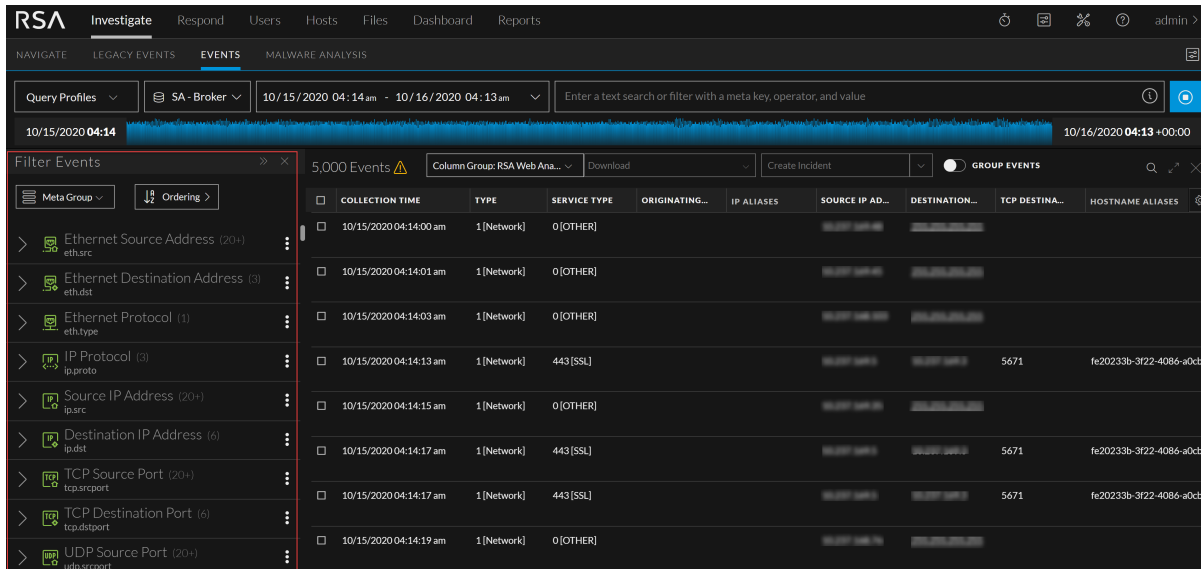
The screenshot shows the NetWitness Investigate interface with the 'EVENTS' tab selected. The search criteria are 'SA - Broker' and the time range is '10/01/2020 02:55 pm - 10/16/2020 04:13 am'. The 'Filter Events' section is set to 'Event Size (Descending by Total Size)'. A callout box highlights the '5061 (66.34 KB)' event, with a tooltip showing 'Meta Value = 5061' and 'Event Size = 66.34 KB'.

「イベントの絞り込み」パネルでメタデータを表示する




「イベントの絞り込み」パネルでメタデータを表示するには、次の手順を実行します。

1. **調査** > **イベント** に移動し、調査するサービスを選択して、時間範囲を選択します。
2. (オプション) 列グループまたはクエリプロファイルを選択します。
3.  をクリックして **イベント** パネルでイベントをロードします。
クエリが **イベント** パネルで実行され、一致するイベントが一覧表示されます。

4. [イベント]パネルで [フィルタ]ボタン()をクリックします。
[イベントの絞り込み]パネルが [イベント]パネルの左側に開きます。

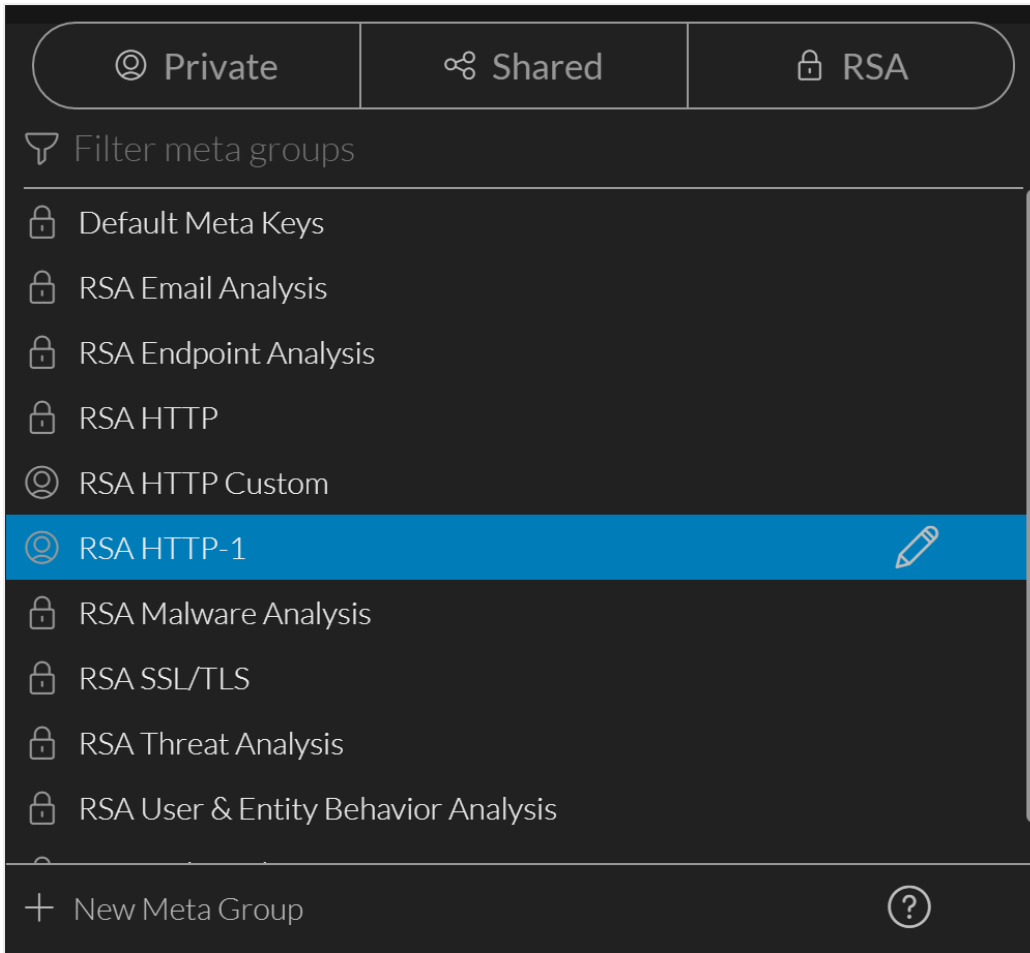


注：(バージョン11.6) [イベントの絞り込み]パネルは [イベント]ビューでデフォルトで開いています。パネルの最後に使用された状態(縮小または完全展開)は、セッション全体およびログイン間で保存されます。また、[イベントの絞り込み]パネルでは、読みやすさを向上させるため、メタキー、メタ値、およびメタカウント間の相違が明らかに示されています。

Default Meta Keysメタグループは、最初にログインしたときに有効になります。最後にログインしたときに別のメタグループを選択した場合は、ブラウザのキャッシュがクリアされるまで、そのメタグループが有効なままとなります。バージョン11.5.1では、以前に選択したメタグループはブラウザのキャッシュに保存されないため、変更しない限り有効なままです。メタグループの詳細については、「[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](#)」を参照してください。サービスのインデックスファイルの内容に基づいて、[イベントの絞り込み]パネルには最初の25個のメタキーが入力されます。これらのメタキーは少なくとも1つのメタ値を持ち、開かれます。[イベントの絞り込み]パネルでDefault Meta Keysグループを使用すると、値を持つ最初の30個のメタキーのみが開かれ、残りは閉じられます。閉じられたメタキーが一覧表示される場合がありますが、25個または30個のメタキーの総数にはカウントされません。値のないメタキーは、パネルの下部に一覧表示されます。標準のパネルコントロール(、 、および )を使用して、パネルを展開、折りたたみ、および閉じることができます。


1. 次のいずれかの操作を実行します。
 - a. 編集しないで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メタグループのコピーを選択するには、 **メタグループの選択** をクリックします。
[メタグループ]メニューにグループが追加されます。次の図は、RSA HTTPメタグループのプライ

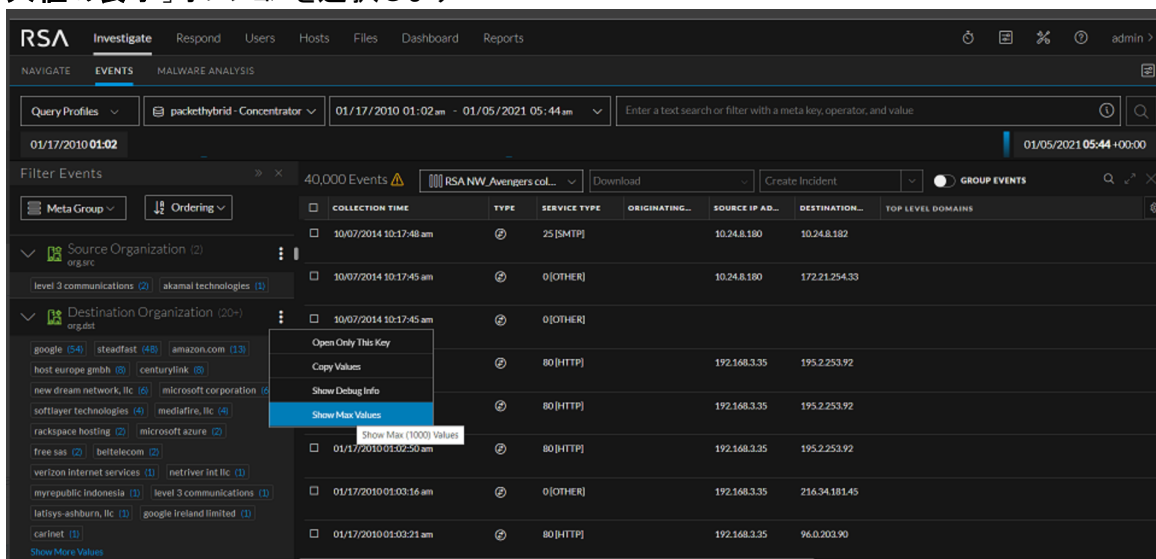
ベート コピーを示しています。



メタグループの最大値を表示する

すべての値がレンダリングされず表示されていない場合は、**最大値の表示**]をクリックして、すべての値を一度に表示できます。

- 11.6の「イベント」ビューで「イベントの絞り込み」パネルを開いた状態で、をクリックし、「最大値の表示」オプションを選択します。



The screenshot shows the NetWitness Investigate interface. The top navigation bar includes 'RSA Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this, there are tabs for 'NAVIGATE', 'EVENTS', and 'MALWARE ANALYSIS'. The main area displays a list of events with columns for 'COLLECTION TIME', 'TYPE', 'SERVICE TYPE', 'ORIGINATING...', 'SOURCE IP AD...', 'DESTINATION...', and 'TOP LEVEL DOMAINS'. A context menu is open over one of the events, showing options like 'Open Only This Key', 'Copy Values', 'Show Debug Info', and 'Show Max Values'.

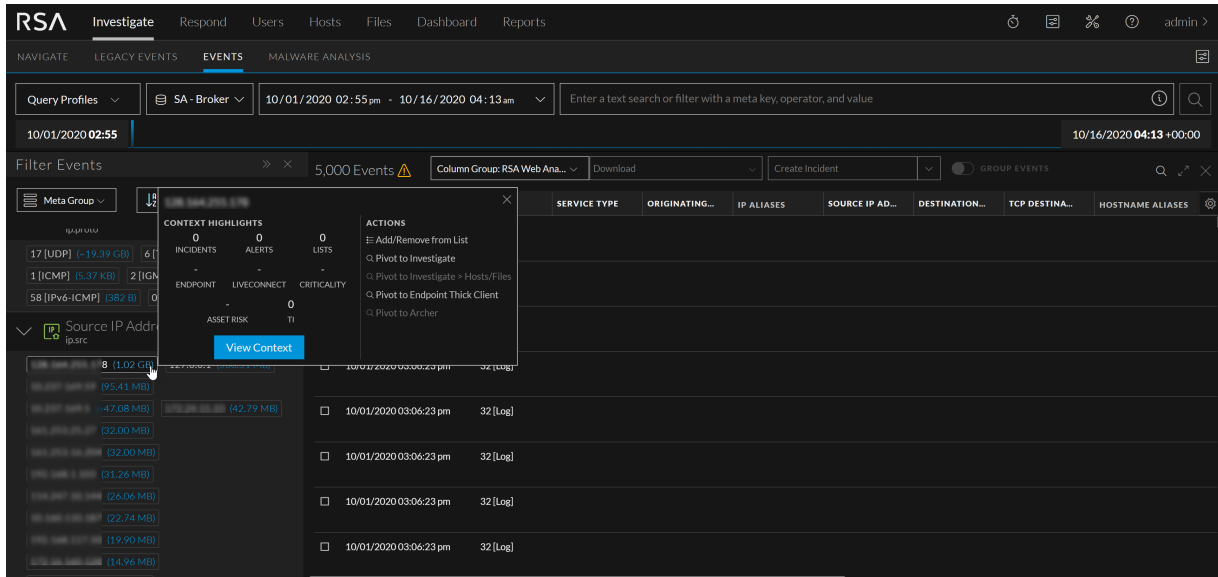
2. 以前にレンダリングされなかった値のロードが開始され、最大1,000件の結果が表示されます。

「イベントの絞り込み」パネルで「コンテキスト ルックアップ」パネルを表示する

「イベントの絞り込み」パネルで、メタ エンティティをクリックしてコンテキスト ツールチップを開くことができます。コンテキスト ツールチップは、Context Hubがサポートするエンティティとして定義されているメタキーでのみ使用できます。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「Context Hubのメタタイプ マッピングの構成」を参照してください。コンテキスト ツールチップには、次の2つのセクションが含まれています。

- **コンテキストのハイライト** - この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、Threat Intelligence (TI)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** - このセクションには、使用可能なアクションが表示されます。この例では、[リストへの追加/削除]、[調査への移行]、[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。



表示可能なメタデータについて

各メタキーにはメタ値のリストがあり、デフォルトで最大20個の値が表示されます。[表示する値を増やす]をクリックすると、メタ値を20個ずつ追加できます。パフォーマンスを最適化するためのハードコードされた最大値である合計1,000個まで追加できます。サービスで見つかった各メタキーのメタキー名と平易な英語名(入力済みと非入力の両方)が一覧表示されます。メタ値ごとに、現在の結果のうち値を含んでいるイベントの数(カウント)または現在の結果に含まれるイベントのサイズ(サイズ)を確認できます。たとえば、次のように表示されます。

```
Action Event [action] (3)
get(3016) login (1346) put (501)
```

この例では、メタキー名はactionで、英語名はAction Eventであり、このメタキーに対して3つのメタ値が見つかりました。getを含む3,016個のイベント、loginを含む1,346個のイベント、putを含む501個のイベントがありました。値は、カウントが最大の値が最初にリストされるように順番に並んでいます。

次の例では、これと同じメタキーの値が**バイト単位のイベント サイズ**に基づいて並べられています。最小のサイズが最初にリストされています。

```
Action Event [action] (3)
login (13,034,588) put (21,848,760) get (1,409,079,256)
```

各メタキー名の前のアイコンは、キーのインデックス付け方法を識別します。インデックス付け方法は、そのメタキーを使用して実行できるインタラクションとクエリのタイプを決定します。

- このメタキーは値でインデックス付けされています。🔍 Action Event [action] (40+)。緑色は、使用可能なすべてのインタラクションとクエリがサポートされていることを示します。メタ値を右クリックすると、コンテキストメニューで使用可能なインタラクションを確認できます。
- このメタキーはメタキーによってインデックス付けされています。🔍 Bytes Sent [bytes.src]。黄色は、使用可能なインタラクションのサブセットがサポートされていることを示しています。このメタキーに対するクエリは、値


でインデックス付けされたメタ キーよりも時間がかかる場合があります。メタ値を右クリックすると、コンテキスト メニューで使用可能なインタラクションを確認できます。

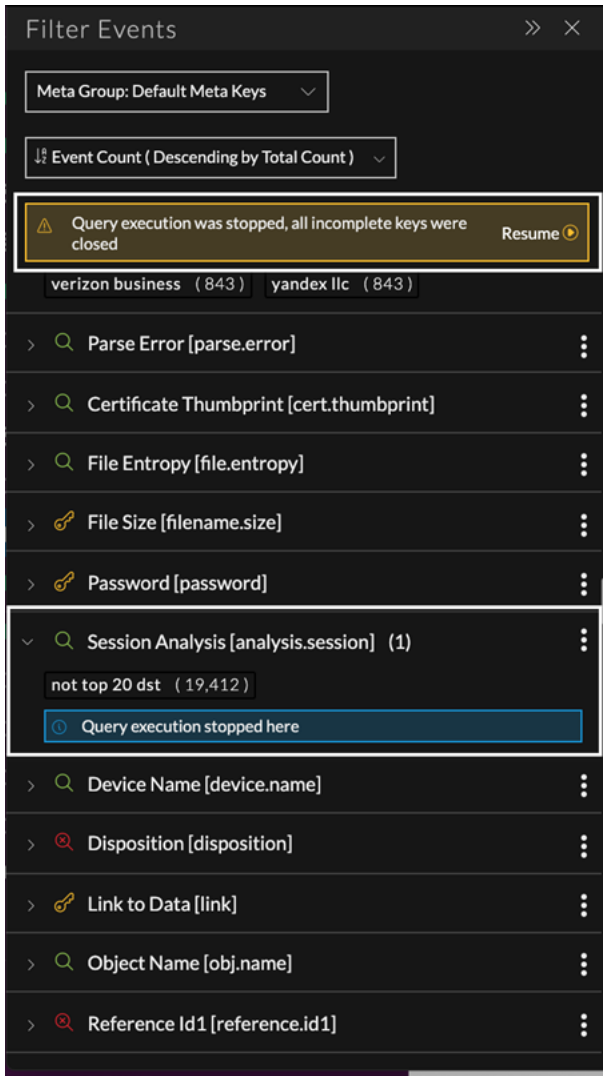
- このメタ キーにはインデックスが付けられていません。  MAC Alias Record [alias.mac]. インデックス付けされていないメタ キーの値を使用してクエリを実行することはできません。インデックス付けされていないメタ キーをクエリする場合、管理者はサービスのインデックス ファイルを編集して、値またはメタ キーでメタ キーをインデックス付けする必要があります。
- バージョン11.5.1では、200個を超えるメタ キー シンボルのセットが3つのインデックス付け方法シンボルに置き換わり、メタ キーの目的を視覚的に示します。メタ キー シンボルの色は、以前と同じ色 (緑、黄色、赤) を使用してインデックス付け方法を識別します。ツールチップもインデックス付け方法を識別し、アイコンの説明を表示します。アイコンは、統合データモデル (<https://community.rsa.com/community/products/netwitness/rsa-content/udm>) で説明するカテゴリーに基づいて定義されています。特定のメタ キーを持たないほとんどのカテゴリーの汎用アイコンと、新しいカスタムメタ キーが追加されたときに使用するデフォルトのメタ キー アイコンがあります。

メタ キーのロード中にエラーが発生した場合、他のメタ キーは通常どおりロードされ、ロードされなかったメタ キーにエラー メッセージが表示されます。新しいクエリを実行すると、一部のエラー メッセージが表示されなくなります。イベントのセットに値がないメタ キーは、パネルの下部に一覧表示されます。

メタ データのロードを停止して再開する

メタ キーと値のロード中に、バージョン11.5.1の [イベントの絞り込み] パネルでメタデータのロードを停止して再開できます。大量のメタ データをロードする場合、すべてのデータがロードされるのを待つ必要がないため、時間を節約できます。ロードを停止してから追加のメタデータを表示する必要が生じた場合は、ロードを再開し、必要なデータが表示されたら再度停止できます。

1. [イベントの絞り込み] パネルでデータをロードしているときに、クエリバーの [停止] ボタン() をクリックします。
メタ キーのロードが停止し、ロードが完了しなかったキーが閉じられます。メタ キーリストの上のメッセージでステータスが通知されます。下にスクロールして、最後のメタ キーを見つけてロードを完了することができます。この例では、セッション解析がロードを終了しました。以下のメタ キーはすべて閉じたままです。



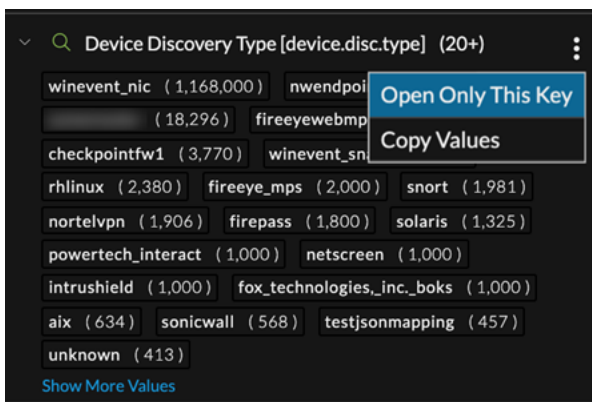
2. 次のいずれかの操作を実行します。
 - a. ロードが停止したメタ キーでロードを再開するには、**再開**]をクリックします。
 - b. クエリを再開せずに、ロードされなかった特定のメタ キーの値を確認する場合は、メタ キー名をクリックして任意のキーを開きます。

1つのメタ キーを除くすべてのメタ キーを閉じる(バージョン11.5.1以降)

「イベントの絞り込み」パネルが開いている場合、同時に多数のメタ キーを表示すると見づらいことがあります。

1つのメタ キーを除くすべてのメタ キーを閉じるには、次の手順を実行します。

1. エントリのメタ キー行で、**メタ キー オプション**] ボタン(Ⓜ) をクリックします。
メタ キー オプションが表示されます。



2. [このキーのみを開く]を選択します。

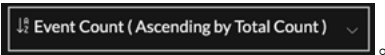
現在のメタ キーを除くすべてのメタ キーが閉じられます。選択したキーが閉じられている場合は、そのキーが開いてロードされ、他のキーはすべて閉じられます。

メタ値の並べ替え方法を設定する

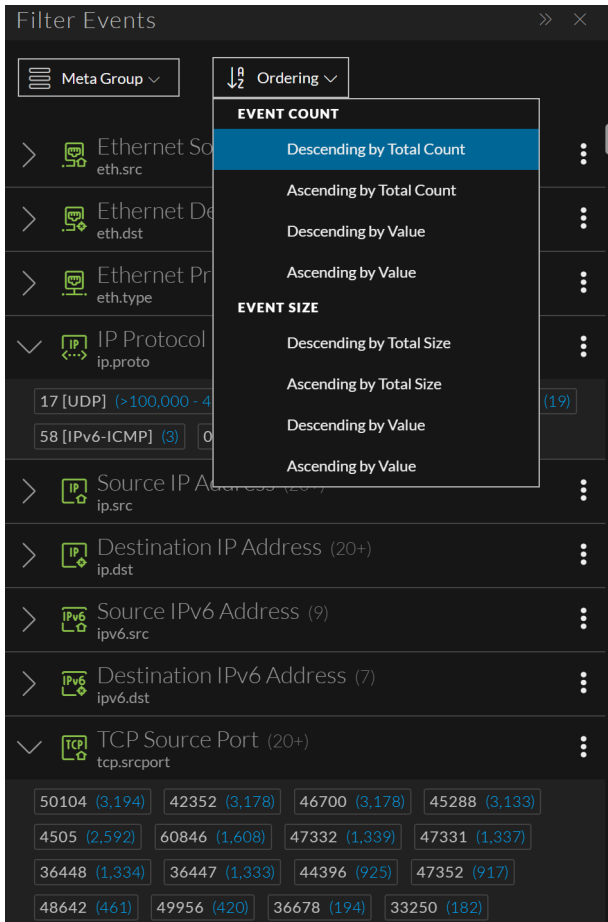
[イベントの絞り込み] パネルを開くと、値ごとにイベント数またはイベント サイズという2つのパラメーターを確認できます。各メタ キー エントリには、値の後の括弧内にイベント数またはイベント サイズのいずれかが含まれます。どちらの場合も、並べ替えには4つのオプションがあります。

並べ替えオプションを使用するには、次の手順を実行します。

1. [イベントの絞り込み] パネルを開いた状態で、選択した並べ替えオプションに応じて名前が付けられた並べ替えメニュー ラベルをクリックします。これは、イベント数の総数の昇順で並べられたメ

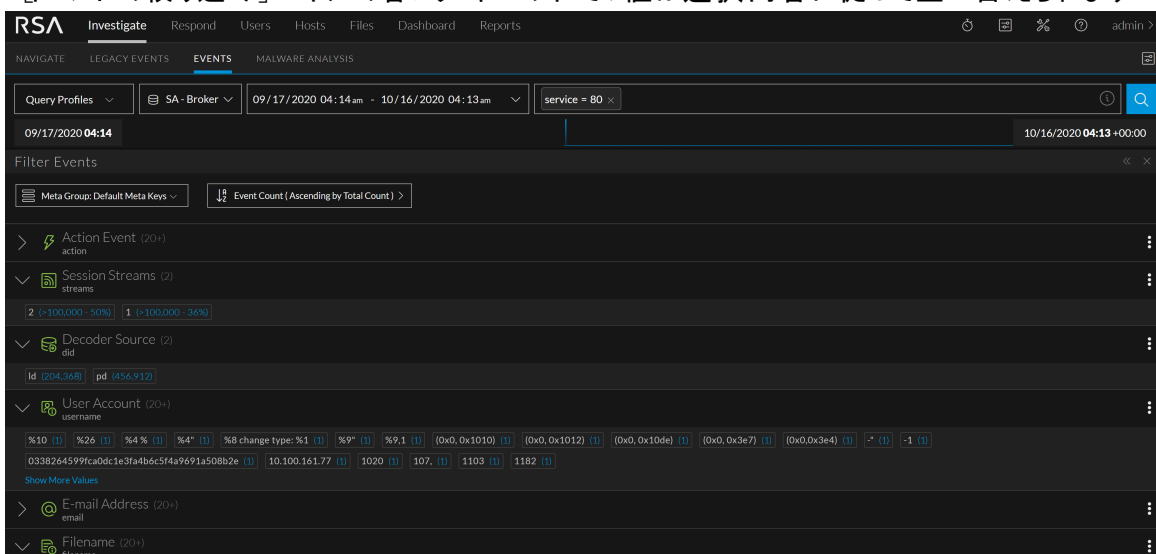
ニュー ラベルの例です。 

[並べ替え] メニューが表示されます。この図は、縮小バージョンのメニューを示しています。



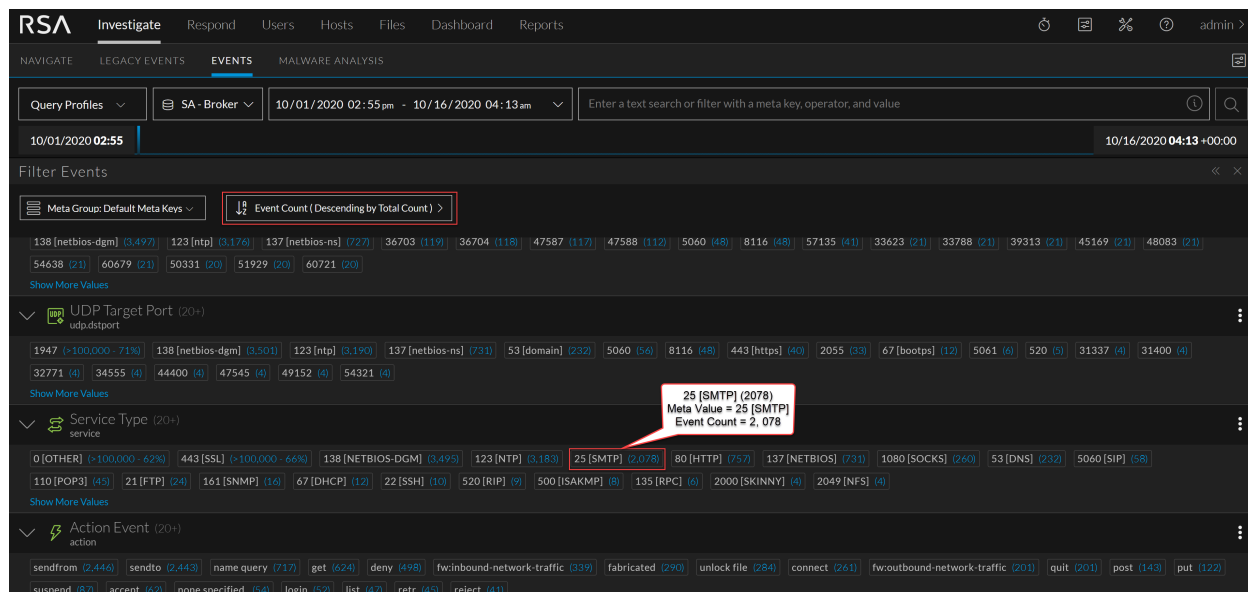
2. 各値の後の括弧内にイベント数を表示するには、次のオプションのいずれかを選択します。デフォルトで、メタキーは [イベント数] > [合計数の降順] 方法を使用して表示されます。
 - a. 値が見つかったイベントの合計数で並べ替えるには、[合計数の降順] または [合計数の昇順] のいずれかを選択します。
 - b. 値の名前で並べ替えるには、[値の昇順] または [値の降順] のいずれかを選択します。
3. 値が見つかったイベントのサイズをバイト単位で表示するには、次のオプションのいずれかを選択します。
 - a. 値が見つかったイベントの合計サイズで並べ替えるには、[合計サイズの降順] または [合計サイズの昇順] のいずれかを選択します。
 - b. 値の名前で並べ替えるには、[合計サイズの昇順] または [合計サイズの降順] のいずれかを選択します。

[イベントの絞り込み] パネルの各メタキーの下で、値が選択内容に従って並べ替えられます。



メタ値をドリルダウンする


[イベントの絞り込み] パネルを開いた状態で、メタ値をドリルダウンして、関連するイベントの可能な限り最小のセットに調査を集中させることができます。完全展開モードの [イベントの絞り込み] パネルをドリルダウンすると、クエリバーにフィルタが追加され、[イベントの絞り込み] パネルに表示されるメタデータが絞り込まれますが、[イベント] パネルでのクエリは実行されません。縮小モードのパネルを [イベント] パネルと並べてドリルダウンすると、クエリバーにフィルタが追加され、[イベント] パネルと [イベントの絞り込み] パネルでクエリが実行されます。この図は、メタデータがロードされた完全展開モードのパネルの例です。



【イベントの絞り込み】パネルでメタデータをドリルダウンして、関連するメタ値を見つけることができます。(=) 演算子を使用したシンプルなクエリでは、【イベントの絞り込み】パネルで使用されているメタ値が強調表示されます。これは、クエリに追加されたフィルタにメタデータを関連づけるのに役立ちます。たとえば次の図は、【イベントの絞り込み】パネルで強調表示されている、クエリフィルタに関連するメタキー値を示しています。

完全展開モードの【イベントの絞り込み】パネルでメタ値をドリルダウンするには、次の手順を実行します。

1. 目的のメタ値を探して、その値をクリックします。上の図を例にとると、他のサービスタイプを除外してSMTPサービスタイプだけを調査するには、**25[SMTP]**をクリックします。
他のサービスタイプは【イベントの絞り込み】パネルのメタデータから除外されますが、クエリは【イベント】パネルでは実行されません。
2. 目的のメタ値を探して、次のいずれかを実行します。
 - a. 値をクリックします。上の図を例にとると、他のサービスタイプを除外してSMTPサービスタイプだけを調査するには、**25[SMTP]**をクリックします。
フィルタがクエリバーの最後のフィルタとして追加され、他のサービスタイプが【イベントの絞り込み】パネルのメタデータから除外されます。【イベント】パネルを閉じられていると、ここではクエリは実行されません。
 - b. (バージョン11.5.1) 値を右クリックし、ドロップダウンメニューで **フィルタの追加 - クエリを実行しない** を選択します。
フィルタがクエリバーの最後のフィルタとして追加されますが、【イベントの絞り込み】パネルのメタデータから他のサービスタイプが除外されることはありません。【イベント】パネルを閉じられていると、ここではクエリは実行されません。
 - c. (バージョン11.5.1) **CTRL(Windows)** または **CMD(MacOS)** を押して、値をクリックします。
フィルタがクエリバーの最後のフィルタとして追加されますが、【イベントの絞り込み】パネルのメタデータから他のサービスタイプが除外されることはありません。【イベント】パネルを閉じられていると、ここではクエリは実行されません。


3. **Action Event [action]**メタ キーのwritetoexecutableなど、別のメタ値を使用して手順1を繰り返します。順番に表示するイベントのセット(ドリルダウン ポイント)が見つかるまで、値をドリルダウンし続けます。
4. ドリルダウン ポイントのシーケンシャル イベントを表示するには、をクリックして [イベントの絞り込み] パネルを縮小します。
[イベント] パネルが右側に開き、[イベント] パネルでクエリが実行されて、RAWイベントを順番に表示できるようになります。

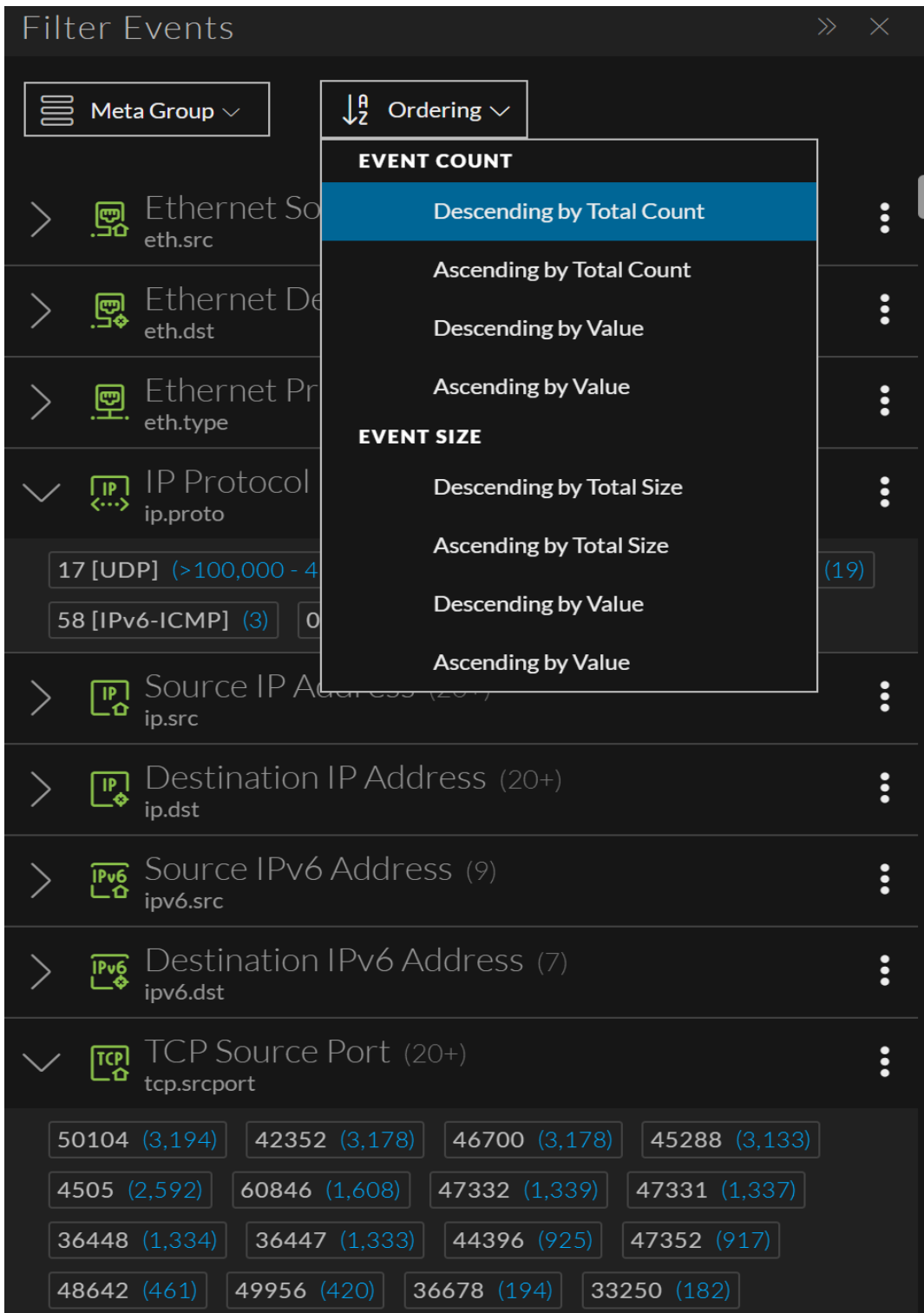
縮小モードの [イベントの絞り込み] パネルでメタ値をドリルダウンするには、次の手順を実行します。

1. 目的のメタ値を探して、次のいずれかを実行します。
 - a. 値をクリックします。上の図を例にとると、他のサービス タイプを除外してSMTPサービス タイプだけを調査するには、**[5[SMTP]]** をクリックします。
フィルタがクエリ バーの最後のフィルタとして追加され、他のサービス タイプが [イベントの絞り込み] パネルのメタデータから除外されて、[イベント] パネルにデータ セットが表示されます。
 - b. 値を右クリックし、ドロップダウン メニューで **[フィルタの追加 - クエリを実行しない]** を選択します。
フィルタはクエリ バーの最後のフィルタとして追加されますが、[イベントの絞り込み] パネルのメタデータから他のサービス タイプが除外されることはなく、クエリ ボタンをクリックしない限り [イベント] パネルでクエリは実行されません。
 - c. **CTRL(Windows) またはCMD(MacOS)** を押して、値をクリックします。
フィルタはクエリ バーの最後のフィルタとして追加されますが、メタデータから他のサービス タイプが除外されることはなく、クエリ ボタンをクリックしない限り [イベント] パネルでクエリは実行されません。
2. 値をクリックし続けて、イベントのセット(ドリルポイント)を絞り込みます。イベントのセットを絞り込むときは、[イベント] パネルで同じセットのRAWイベントを調べて再構築します。

メタ キーのメタ値をコピーする

メタ キーの表示されているメタ値をすべてコピーするには、次の手順を実行します。

1. エントリのメタ キー行で、**[メタ キー オプション]** ボタン() をクリックします。
メタ キー オプションが表示されます。現時点で唯一のオプションは **[値のコピー]** です。

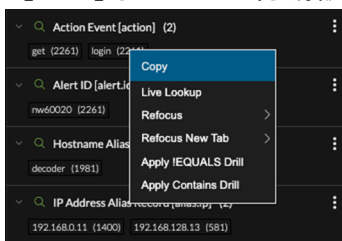


2. **値のコピー**をクリックします。

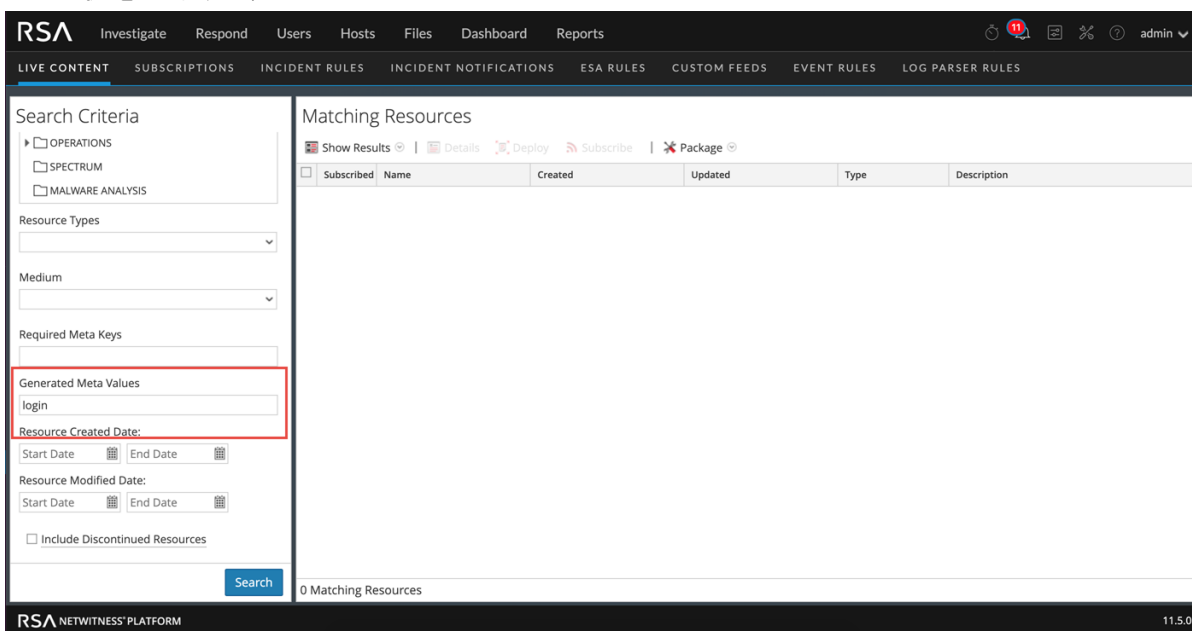
値のカンマ区切りリストがローカルのクリップボードにコピーされます。これは、クリップボードの内容の例です。"get", "login", "put".

選択したメタ値をRSA Liveで表示する

1. メタ値 (たとえばlogin) を右クリックします。
コピー オプションが初期設定で選択された [メタ値] ドロップダウン メニューが表示されます。



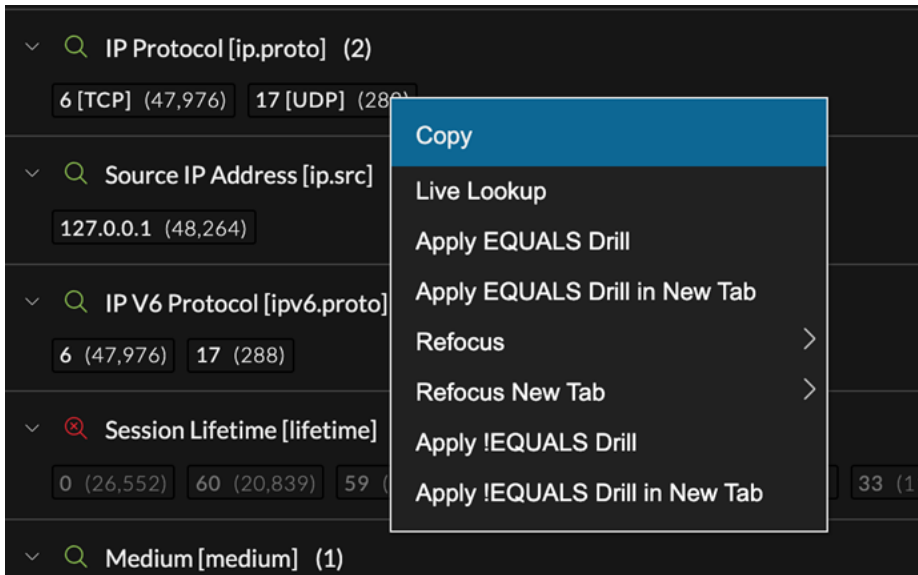
2. メタ値 (たとえばsuccess) をRSA Liveで検索するには、[Liveルックアップ] を選択します。
 Liveの [検索] ビューが開いて、入力したメタ値が [生成されるメタ値] フィールドに表示され、検索できる状態になります。



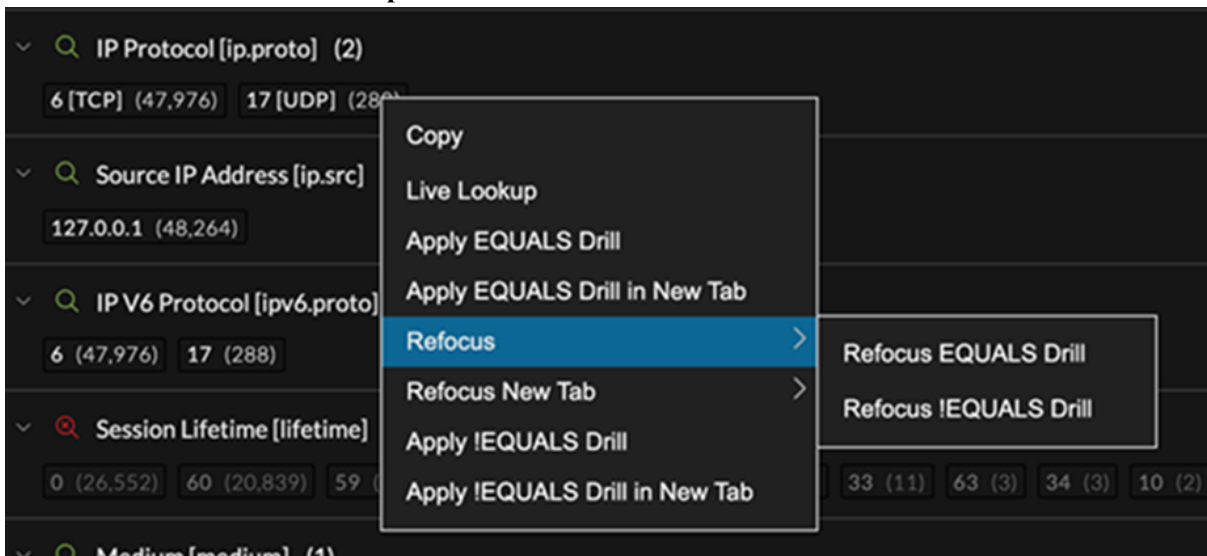
メタ値の調査を再フォーカスする

メタ キーの下にリストされている各値のフォーカスは<meta key> = <meta value>です。メタ値を右クリックすると、さまざまな再フォーカス オプションを含んだコンテキスト メニューが表示されます。すべての再フォーカスアクションは、[イベント] パネルと [イベントの絞り込み] パネルのドリルダウン ポイントを更新します。

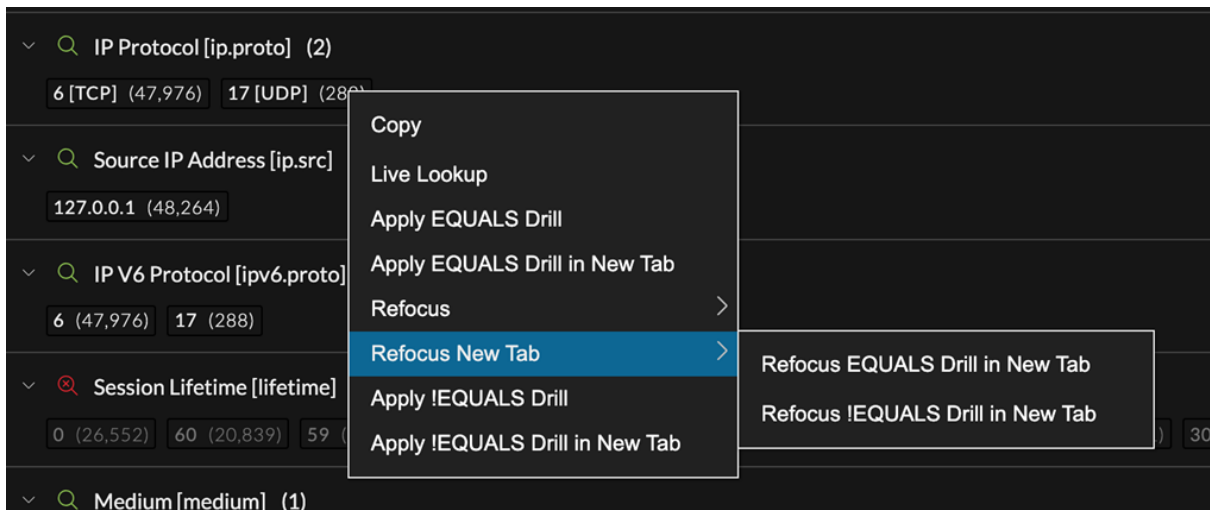
1. さまざまな演算子(=、!=、contains)を使用してキーと値のペアをクエリに追加するには、メタ値(たとえば、下の図のUDP)を右クリックして、**適用<operator>ドリルダウン**オプションのいずれかを選択します。



2. キーと値のペアと別の演算子(=、!=、contains)を使用してクエリを最初からやり直すには、値を右クリックして、**再フォーカス<operator>ドリルダウン**オプションのいずれかを選択します。



- キーと値のペアをクエリに追加するか、新しいブラウザ タブでキーと値のペアを最初からやり直すには、値を右クリックして、**新しいタブの再フォーカス** > **再フォーカス<operator>新しいタブのドリルダウン** または **再フォーカス<operator>新しいタブのドリルダウン** オプションのいずれかを選択します。



ドリルダウンのフォーカスが選択内容に応じて再設定され、[イベント] パネルで新しいクエリが実行されます。

【イベント】ビューでの結果のフィルタリング

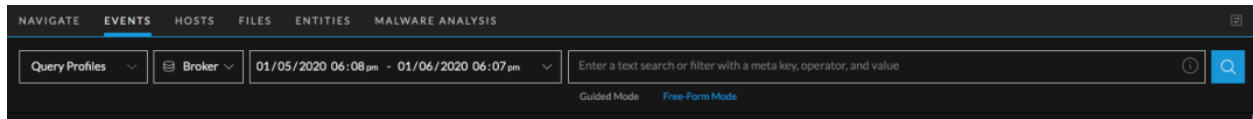
注：このセクションはバージョン11.1以降に適用されます。

【イベント】ビューでイベントをフィルタリングすると、より関連性の高い少数のイベントに調査を絞り込むことができます。【イベント フィルター】パネル(バージョン11.5以降)、クエリバーの各オプション、【イベント】パネルの各オプションを使用して【イベント】ビューでイベントをフィルタリングできます。

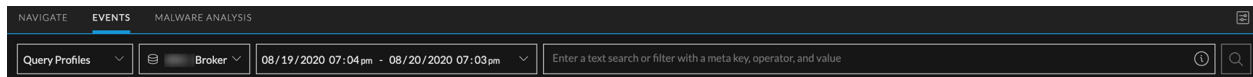
クエリバーを使用した初期フィルタ



最初に【イベント】ビューを開いたときの最も基本的なフィルタリングは、サービスと時間範囲を選択してから、クエリバーでサービスにクエリを実行することです。これにより、一致するイベントのリストが【イベント】パネルに返されます。また、クエリプロファイル(バージョン11.4以降)を選択し、クエリを作成して、特定のメタキー、メタ値、テキストを含むイベントをクエリバーで探すこともできます。

次の図は、バージョン11.4以前のクエリバーのほか、クエリプロファイル、サービス、時間範囲を選択してイベントをフィルタリングし、それを【イベント】パネルにロードするオプションを示しています。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。

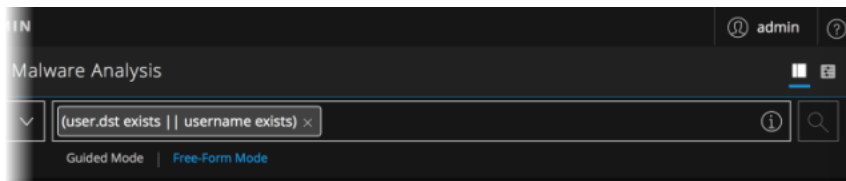
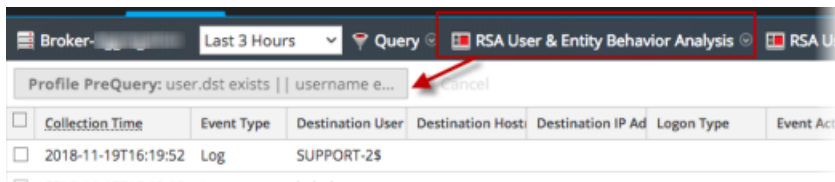


次の図は、ガイドモードとフリーフォームモードが不要になった、バージョン11.4.1以降のクエリバーを示しています。シンプルになったフィルタ入力フォームでは、高度な自動提案オプションの使用と、フリーフォームクエリの入力も可能です。



- 【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】パネル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。
- クエリビルドフィールドは、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]ビューまたは [ナビゲート]ビューから【イベント】ビューに移動すると、[レガシー イベント]ビューまたは [ナビゲート]ビューで選択されたサービス、時間範囲、フィルタがクエリバーに表示されます。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。

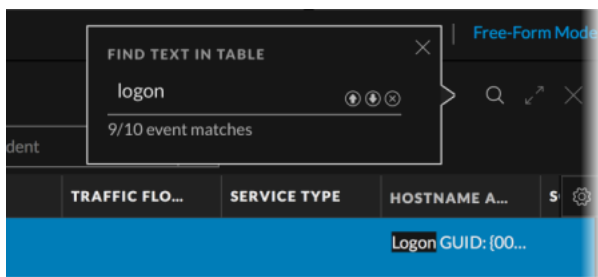
- イベントを右クリックまたはダブルクリックして [イベント]ビューに移動したときに、[レガシー イベント]ビューでプロファイルが選択されていた場合は、そのプロファイルのフィルタ(プレクエリ)が編集可能なフィルタとしてクエリビルダフィールドに追加されます。次の図は、[レガシー イベント]ビューのプレクエリと、[イベント]ビューの最初のフィルターとして追加された同じクエリを示しています。



[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)

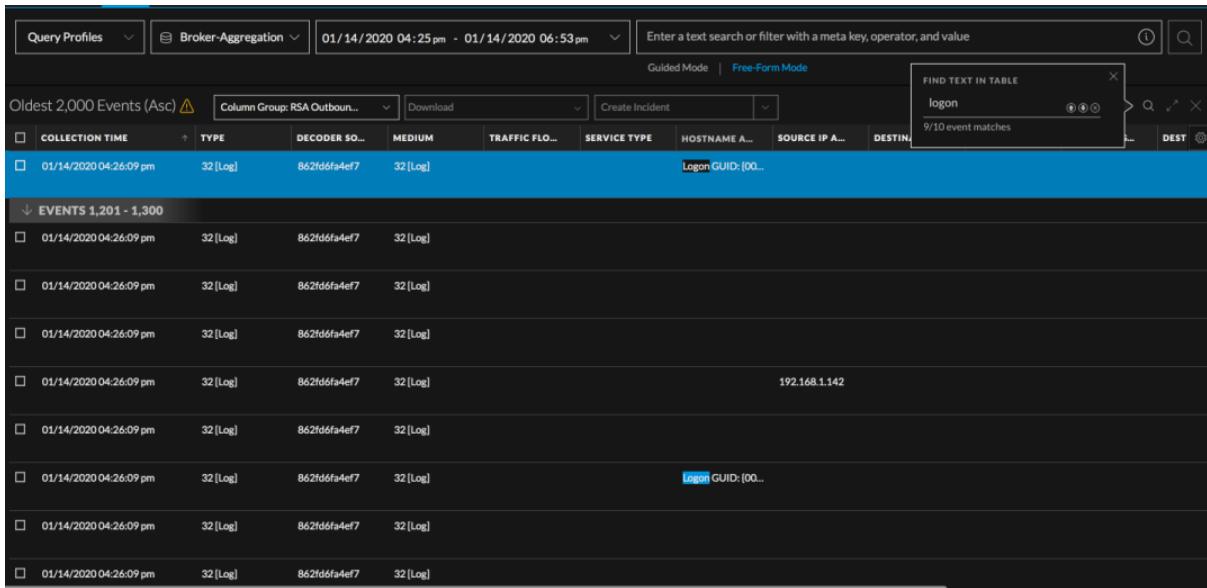
[イベント]パネルを開いた状態で、イベントのリストからテキスト文字列を検索できます。この検索は、ブラウザウィンドウでのCTRL-F検索と似ています。検索では、テーブルのすべての行のすべてのテキスト(表示可能な列のみ)で一致が検索され、一致するテキストがハイライト表示されます。表示されていない列は検索の対象となりません。[サマリー]列がテーブルの一部である場合、検索機能は無効になります。

- [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。



- 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「192.168」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】パネルでの結果の絞り込み

最初のフィルタとクエリの送信後に、クエリバーのオプションを引き続き使用して、結果をフィルタリングする、追加の2つの方法で結果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ができます(「[イベントリストでの列と列グループの使用](#)」を参照)。
- バージョン11.5以降では、ベータリリース機能の「イベントのフィルタリング」パネルの結果で、メタキーとメタ値を調べることにより、イベントをフィルタリングできます。これにより、「ナビゲート」ビューのようにメタデータを調査でき、ドリルポイントに基づいて「イベント」パネルで一致するイベントを順番にすぐに確認できるという追加の利便性が提供されます。管理者は、『システム構成ガイド』で説明されているように、この機能を有効または無効にすることができます。

クエリビルダの概念

クエリビルダーで、3種類(シンプル、フリーフォーム、テキスト)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、次のとおりです :<meta key><operator><meta value>.次に例を挙げます。direction = 'outbound'.

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。次の図はそれぞれ、バージョン11.4とバージョン11.6のクエリバーを示しています。



- 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。その例は、failed, login, やattempt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。

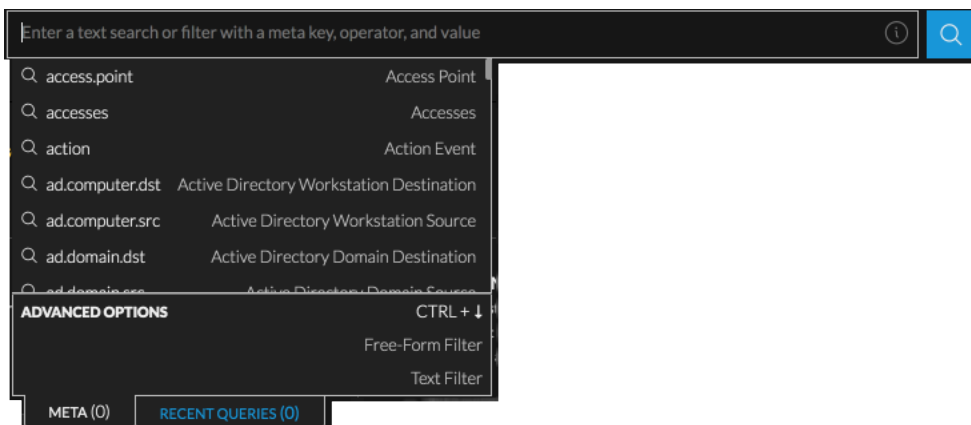
クエリビルダでは、各フィルタは編集可能なフィールドです。フィルタは、作成した順に左から右に並びます。追加したフィルタは1行に入りきらなくなると、次の行に折り返され、入力領域が縦に広がります。このため、右にスクロールしなくても、すべてのフィルタを表示できます。

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

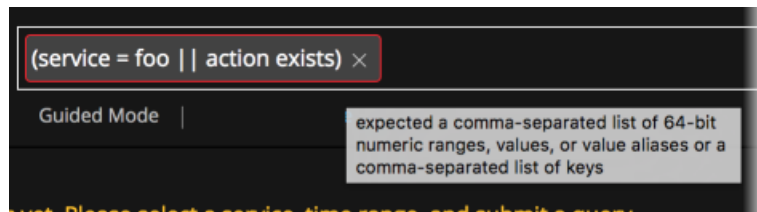
注：バージョン11.4には、フィルタ入力フォームにクエリを入力するための2つのモード、ガイド モードとフリーフォーム モードが用意されていました。バージョン11.4.1以降では、ガイド モードの強力なオートコンプリート機能および値候補表示機能と、フリーフォーム クエリを入力またはペーストする機能が完全に統合されました。このドキュメントでガイド モードとフリーフォーム モードを区別して説明している箇所は、バージョン11.4.0.x以前を使用するアナリスト向けです。

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、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。

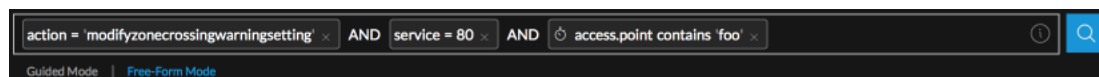
注：バージョン11.3より前のバージョンでは、 ボタンのラベルが異なります。以前は「クエリ イベント」と呼ばれていました。

「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。

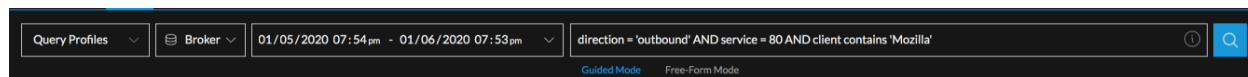
- ガイド モードからフリーフォーム モードに切り替えると、ガイド モードで作成したフィルタはフリーフォームのテキスト クエリに変換されます。
- フリーフォーム モードからガイド モードに切り替えると、入力済みのクエリが個別のシンプルなフィルタとしてクエリバーに追加されます。ただし、自動提案オプションは表示されません。

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。

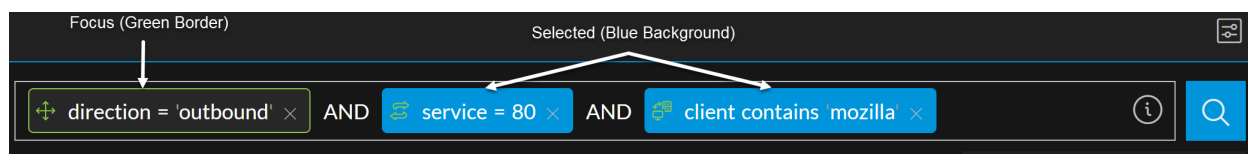


次の図は、フリーフォーム クエリビルダ使用中の例です。

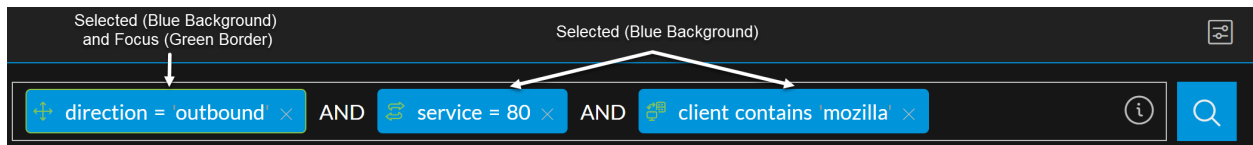


複数のフィルタの編集に関する概念

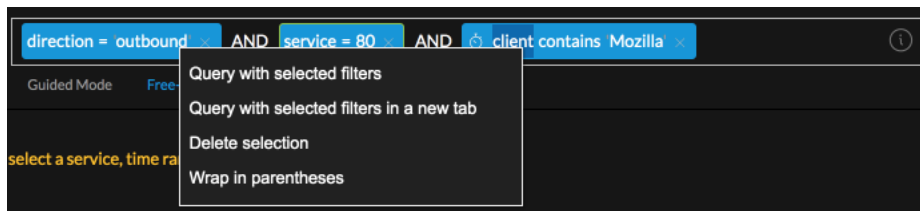
クエリビルダで作業する際は、編集のフォーカスがあるフィルタは緑色の枠線がマークされ、選択中のフィルタには青色の背景が表示されます。この機能は、右クリックアクションに対して複数のフィルタを選択できる点で便利ですが、一度に編集できるフィルタは1つだけです。次の図は、フォーカスされたフィルタが緑色の枠線でマークされ、選択中の2つのフィルタが青色の背景で表示されている状態を示しています。



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。



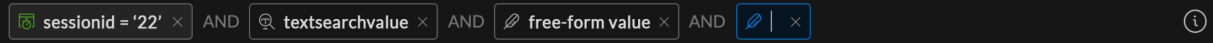
バージョン11.4.1のメニューには、次の図に示すように、新しいコピーオプションが2つあります。これらのオプションを使用すると、クリップボードの内容を他のアナリストと共有したり、コンテンツをクエリバーにペーストしたりすることができます。次の操作を実行できます。

- 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11.6) フィルタがユーザの入力を待っている場合は、フィルタが青色でハイライト表示されます.

- (バージョン11.6) 無効なフィルタは、赤い色でハイライト表示されます。



- クエリバーのフィルタにカーソルを合わせると、ツールチップメッセージが表示されます。

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である<meta key> <operator> <meta value>フィルタを作成し、編集することができます。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の『Investigate ユーザ ガイド』を参照してください。次のリンクからPDF形式で入手できます。[Master Table of Contents for RSA NetWitness Platform Version 11](#)

バージョン11.2では、ユーザ インタフェースに2つのモードがあります。ガイド モードとフリーフォーム モードが用意されていました。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の『Investigate ユーザ ガイド』を参照してください。次のリンクからPDF形式で入手できます。[Master Table of Contents for RSA NetWitness Platform Version 11](#)

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

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

☑で示されているデータ 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。

テキストを手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手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)

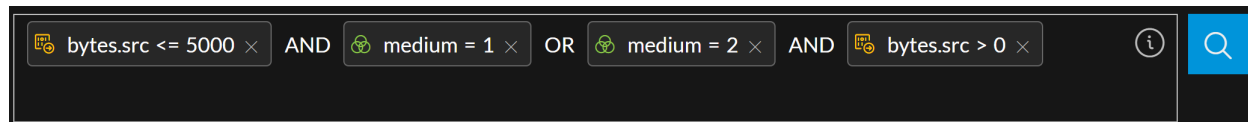
[イベント]ビューのクエリバーでフィルタを作成するときに、キーボード コマンド(MacOSの場合はCmd + A、Windowsの場合はCtrl + A)を使用してすべてのフィルターを選択してから、選択内容をクリップボードにコピー(MacOSの場合はCmd + C、Windowsの場合はCtrl + C)することができます。クリップボードのテキストは、他のアナリストと共有したり、Cmd-VまたはCtrl-Vを使用してクエリバーにペーストしたりできます。

最近のクエリの使用

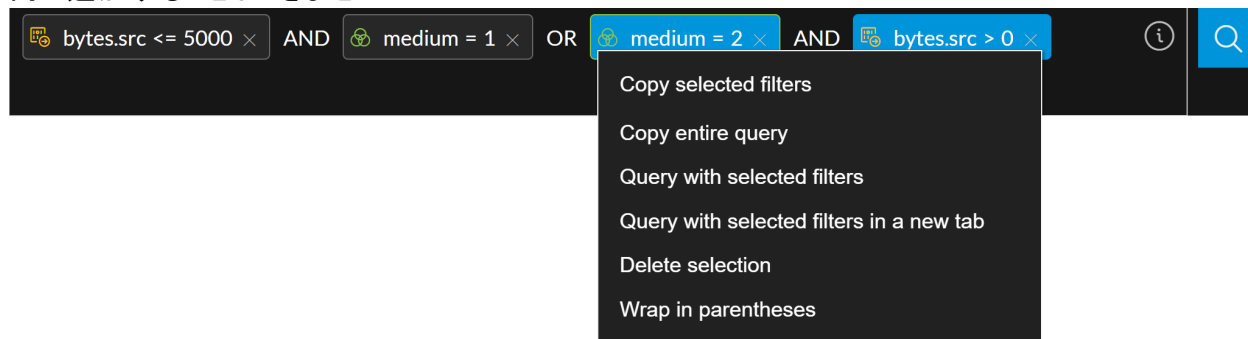
フィルタ入力フォームでは、メタ キー、演算子、値を入力する方法として、[メタ]タブと 最近のクエリ]タブの2つが用意されています。[メタ]タブは、以前のバージョンのフィルタ入力フォームと同じですが、条件に一致するメタ キーの数が [メタ]タブのラベルに表示されるようになった点と、各メタ キーのアイコンにより、キーでインデックスされているか、値でインデックスされているか、インデックスされていないかが表示されるようになった点が異なります。最近のクエリ]タブには、最大100個の最近のクエリが表示されます。リストは入力されたテキストによって絞り込まれ、入力されたテキストを含んだクエリのみが表示されます。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

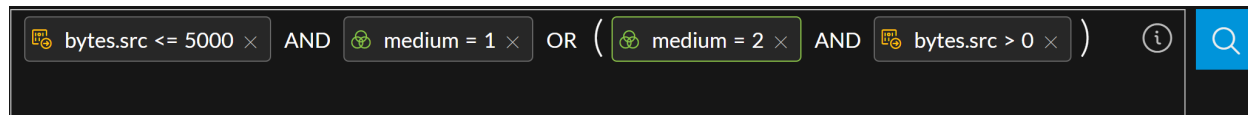
自動提案機能の解析エンジンは、フィルタ入力フォームにペーストまたはキー入力された高度な演算子である<、>、<=、>=、OR、||、AND、&&、()、regex、lengthを解析できます。テキストは複数のフィルタとして解析されます。たとえば、「medium > 0 && medium <= 100」をキー入力またはペーストした場合は、明示的なAND演算子を使用する2つのシンプルなフィルタとして解析されます。medium > 0 AND medium <= 100。「bytes.src <= 5000 && medium = 1 || medium = 2 && bytes.src > 0」をキー入力またはペーストした場合は、AND演算子とOR演算子で区切られた4つのシンプルなフィルター、bytes.src <= 5000 AND medium = 1 OR medium = 2 AND bytes.src > 0が作成されます。これは、できるだけ多くの有効なフィルタを作成するためです。



このフィルタは、括弧を追加すると便利なフィルタの例です。「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。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。



結果として、bytes.src <= 5000 AND medium = 1 OR (medium = 2 AND bytes.src > 0) というクエリが生成されます。



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ーインターフェイスに表示されます。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。一致する値が返されない場合は、「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によって、10.20.30.0がサブネットマスク 255.255.255.0とともに指定されます。これは、10.20.30.0～10.20.30.255の範囲内の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、以下は有効な範囲ではありません。-10 - 50, 50 - 10, 50.8 - 60.2, 50 - 70x。

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す。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、Start Time - End Timeの形式で表示され、ユーザのプロファイル用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、「[ユーザー環境設定]ダイアログ( > [プロファイル]を選択)の「イベント」ビュー向けの設定に基づきます。

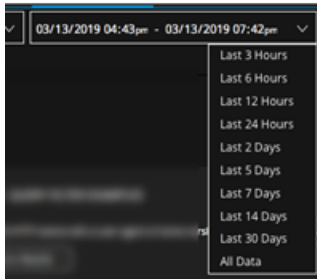
- デフォルトの日付形式は、MM/DD/YYYYです。この形式は、「[ユーザー環境設定]ダイアログでDD/MM/YYYYまたはYYYY/MM/DDに変更できます。
- 開始時間と終了時間はHH:MM形式で指定します。秒は表示されませんが、開始時間の値は常にHH:MM:00秒に、終了時間の値は常にHH:MM:59秒にデフォルトで設定されます。たとえば、「6:45 pm - 7:45 pm」という時間範囲は「06:45:00 - 07:45:59 pm」として解釈されます。
- デフォルトの時間範囲は24時間制です。12時間制に変更することができます。

注：デフォルトでは、ダウンロードの時間形式はエポック形式であり、UNIXのエポック(1970年1月1日)からの秒数を表す数値で時間を示します。このように表示された時間を理解するには変換が必要です。管理者は、ダウンロードの時間形式の設定を変更して、ユーザー環境設定のタイムゾーン、日付形式、時間形式を組み合わせ、業界標準のISO 8601表現に、可能な限り従った分かりやすい表現にすることができます。たとえば、US/Pacificタイムゾーン(GMT-7:00)の04/13/2020 09:17:36 amという時間の場合、ユーザーインターフェイスに表示される12時間制の時間は、次のようになります。04/13/2020 09:17:36 am.ダウンロードでは、この時間がエポック形式の「61547519856000」に変換されます。管理者がダウンロードの時間形式を判読可能な表現に設定している場合、これと同じ時間が、次のように表現されます。04-13-2020T09:17:36AM-07:00.

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()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」を選択した場合は、クエリの開始時刻と終了時刻が、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。

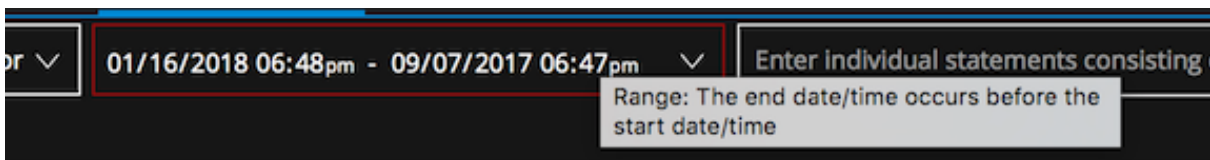
1. 「時間範囲」セクターの内側にあるドロップダウン矢印をクリックして、リストから時間範囲を選択します。分単位、時間単位、日単位のオプションを選択するか、すべてのデータを選択できます。



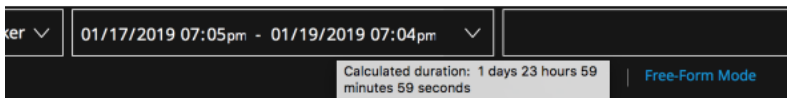
- (バージョン11.3以降) クエリバーに表示されている年、月、日、時間、分をクリックして時間範囲を直接編集します。値がハイライト表示されたら、開始時間または終了時間のいずれかの新しい値を入力します。時間形式の環境設定が12時間制に設定されている場合は、[午前]または[午後]をクリックして2つのオプションを切り替えます。



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、検索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

検索ボタンは、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、検索ボタンをクリックすると、すべてのフィルタがANDで連結され、検索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。検索ボタンは、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。検索ボタンは、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

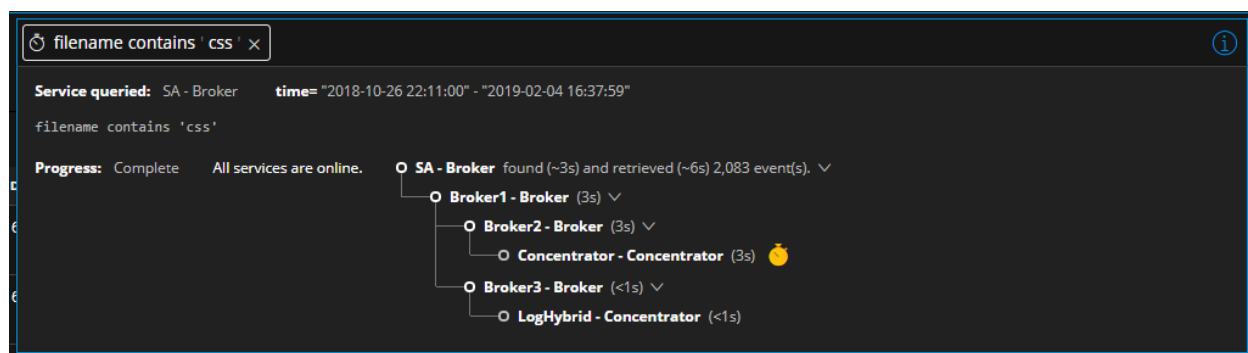
 をクリックしてクエリを送信すると、ボタンが  (クエリ停止オプション) に変わります。クエリ停止オプションは、すべてのイベントが [イベント] パネルにロードされるまで表示されたままになります。クエリをキャンセルするには、 をクリックします。

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] リストの結果の末尾に次のメッセージが表示されます。"クエリがキャンセルされたため、一部の結果しか表示されていません。"

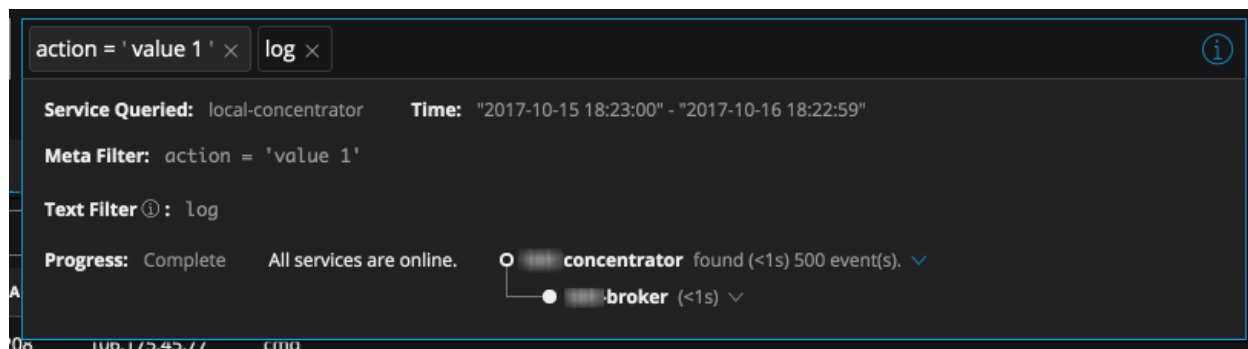
クエリのステータスの表示

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。クエリコンソールに表示される時間範囲は、次のようになります。"2014-09-20 20:57:00"-"2018-11-02 18:57:59"。)

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。



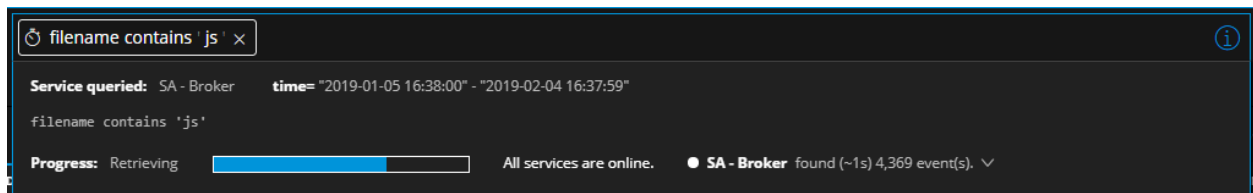
クエリが実行されている間、コンソールの下部にある進行状況バーには、クエリの完了率が表示されます。ステータス情報からは、クエリで今行われている処理(実行中、キューに登録済み、クエリ対象サービスのインデックスファイルの読み取り中、イベントの取得中、完了など)についての詳細を知ることができます。ステータスと致命的でないメッセージは受信するとすぐに表示され、致命的でないエラーの場合は、クエリバーの枠線が黄色に変わります。

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。

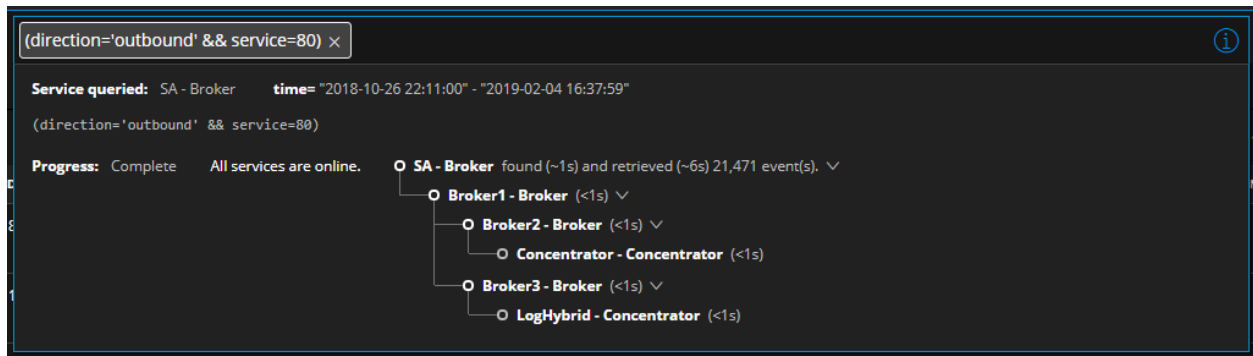
- 黄色のストップウォッチは、最も低速なサービスを示します。
- 黄色の三角形は警告を受信したことを示します。
- 赤い三角形は、サービスに対してクエリを実行しようとしたときにエラーが発生したことを示します。

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。

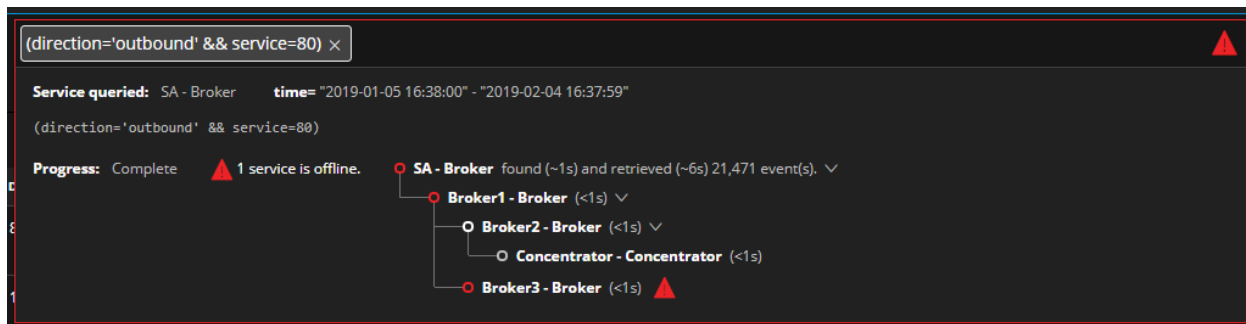


要求の完了。エラーまたは警告なしでロードが完了した場合、クエリコンソールの枠線は青色になり、表示中のデータが最新であることを示すインジケータとして 🔍 ボタンが無効になります。次の図は、エラーまたは警告なしにクエリが完了したときのクエリコンソールの例です。



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。

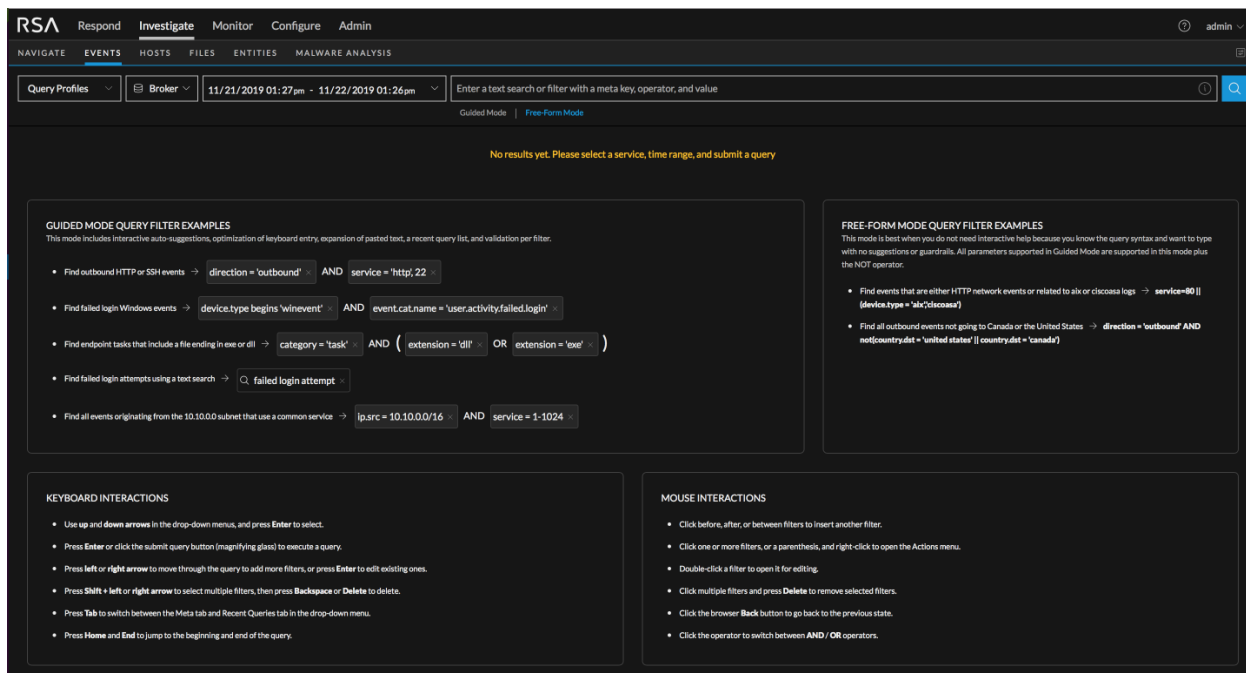
致命的でないエラーが発生しても、クエリの実行は妨げられません。クエリは実行され、イベントはロードされますが、クエリコンソールの右上隅に赤い三角形が表示され、警告を示す赤い枠線が表示されます。次の図は、クエリ対象サービスが別のオフライン状態のサービスのプロキシになっている場合に表示されるクエリコンソールの例です。



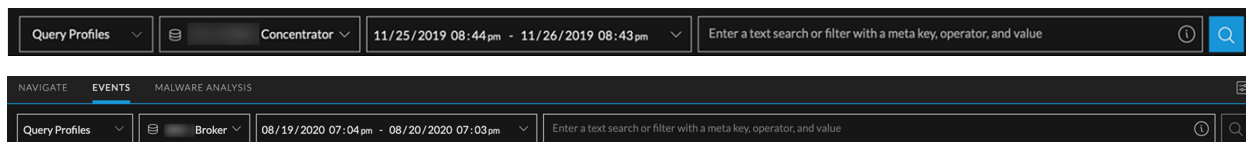
警告が発生しても、クエリの実行は妨げられません。クエリは実行され、イベントはロードされますが、クエリコンソールの右上隅に黄色の三角形が表示され、黄色の枠線が表示されます。

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 セレクタと時間範囲には適用されません。

アクション	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、編集中的フィルタ以外)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。
フィルタ内の文字を削除する	<p>選択した文字 :クエリバーで文字を選択し、DeleteまたはBackspaceキーを押します。</p> <p>前の文字(バージョン11.4以降) :クエリバーで、文字の隣にカーソルを置き、Backspace(Windows OS)またはDelete(MacOS)キーを押します。</p> <p>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、Delete(Windows OS)またはFn + Delete(MacOS)キーを押します。</p>
フィルタを削除する	<p>選択したフィルタ :1つ以上のフィルタを選択し、次のいずれかを実行します。</p> <ul style="list-style-type: none"> • 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。 <p>フォーカスしているフィルタ(バージョン11.4以降) :フォーカスしているフィルタにカーソルを合わせ、Backspace(Windows OS)またはDelete(MacOS)キーを押します。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。</p> <p>フォーカスしているフィルタ(バージョン11.4以降) :フォーカスしているフィルタにカーソルを合わせ、Delete(Windows OS)またはFn + Delete(MacOS)キーを押します。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。</p>
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。

アクション	キーボードへの入力
フィルタ内の括弧とその中身を削除する(11.4以降)	<p>選択した括弧 :1組の括弧を選択した状態で、次のいずれかを実行します。</p> <ul style="list-style-type: none"> • 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、編集用を開く(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。
クエリバーの最後尾に新しいフィルタを挿入し、編集用を開く(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、編集用を開く	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、編集用を開く	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。










アクション	キーボードへの入力
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。 <ul style="list-style-type: none"> 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、編集用のフィルタ以外)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 + 右矢印 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。
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。

フィードバック	アイコン	説明
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。

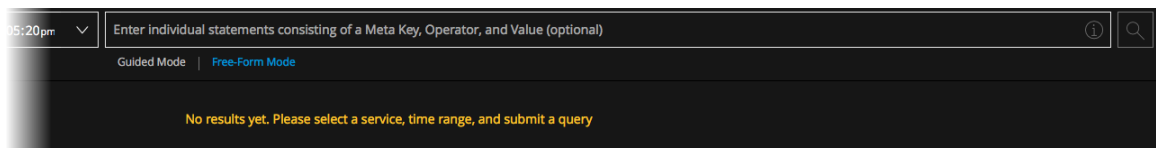
フィードバック	アイコン	説明
<p>「メタ」タブのインデックス インジケータ</p>		<p>(バージョン11.4以降) 「メタ」タブでメタ キーのインデックスレベルを示します。これにより、そのメタ キーをフィルタで使用できるかどうかが決まります。</p> <p> filename.src このメタ キーはメタ値でインデックスされており、フィルタで使用できます。</p> <p> filename.size このメタ キーはメタ キーによってインデックスされており、フィルタで使用できます。</p> <p> float32.whatever このメタ キーはインデックスされておらず、フィルタには使用できません。</p> <p>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。</p>
<p>クエリ送信ボタン</p>		<p>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。ボタンには、次の3種類の状態があります。</p> <p> クエリビルダーのフィルタを使用してクエリを送信できる状態です。</p> <p> 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。</p> <p> 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。</p>
<p>低速サービスアイコン</p>		<p>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。</p>

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		(バージョン11.5以前)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

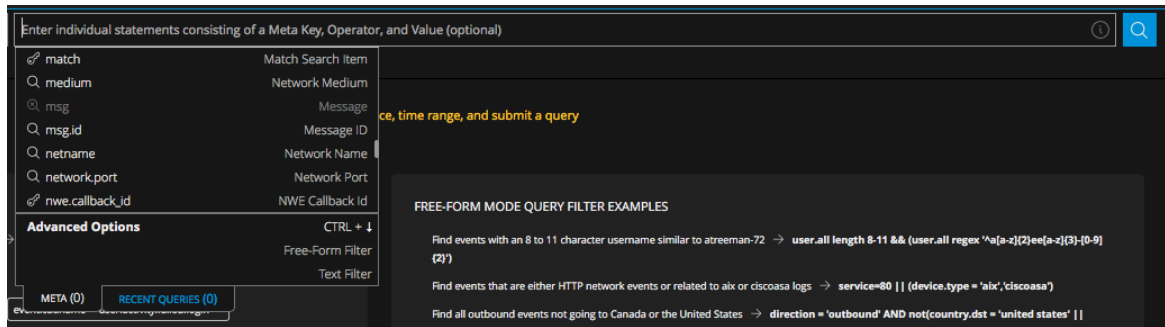
ガイド モードでシンプルなフィルタを作成するには、次の手順を実行します。

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。

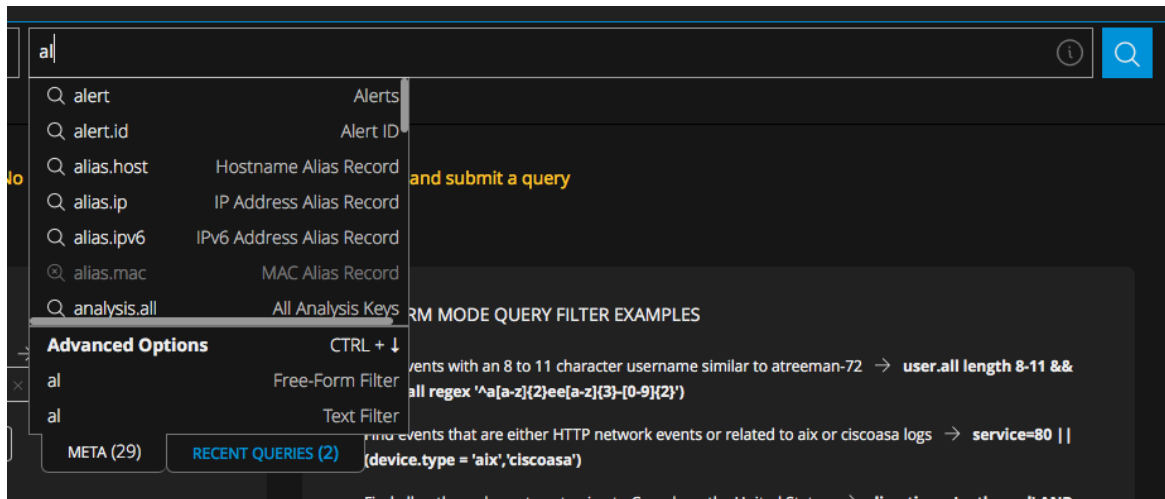


挿入ポイントが2つのフィルタの間にある場合は、緑色の丸(バージョン11.3以前)または太字のカーソル(バージョン11.4以降)によって挿入ポイントがマークされます。挿入ポイントがクエリバーの最後尾にある場合は、エントリーポイントに点滅するカーソルが表示されます。ドロップダウンリストには、調査中のサービスから渡された使用可能なメタキーがアルファベット順に表示

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。




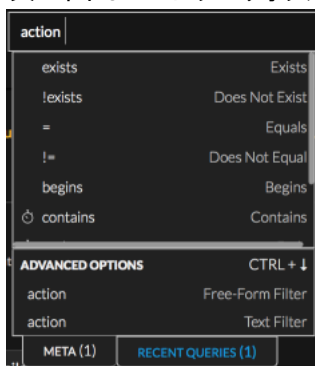
- d. ハイライト表示されているメタ キーを選択するには、**Enter**を押します。
[メタ]ラベルのカウントが1に変わります。

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。

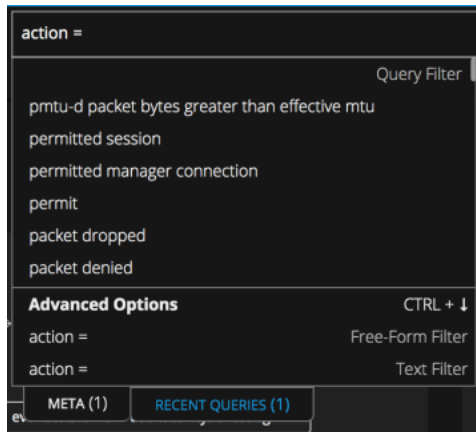
--最初の条件がtrueで、テキスト フィルタがすでに1つある場合は、フリーフォーム フィルタ オプションがハイライト 表示され、フリーフォーム フィルタを作成できるようになります。

- 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。



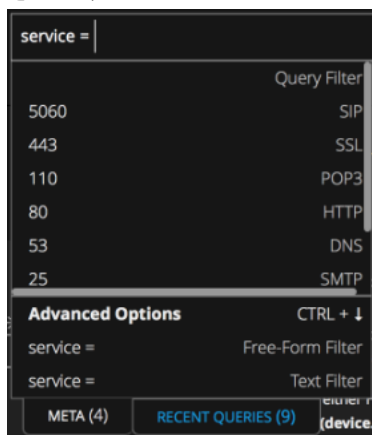
3. 演算子を選択するには、次のいずれかを実行します。
- 演算子ドロップダウン リストにオプションが1つしかない場合は、**Enter**を押してオプションを選択します。
 - 演算子ドロップダウン リストに複数のオプションがある場合は、演算子をクリックするか、上/下矢印を使って演算子を選択してから、**Enter**を押します。
 - 演算子を手入力して、**Enter**を押します。入力に合わせて、演算子ドロップダウン リストが絞り込まれ、入力したテキストを含む演算子のみがリストに表示されます。演算子をクリックするか、上/下矢印を使って演算子を選択してから、**Enter**を押します。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。

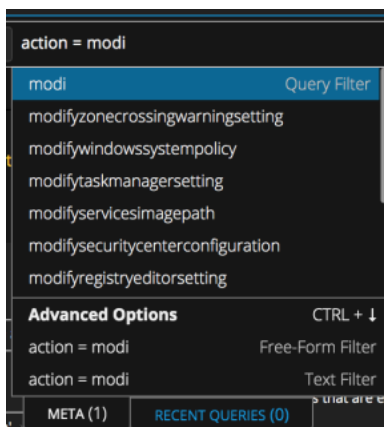


4. (オプション) フィルタ入力フォームの選択された演算子に値を指定できる場合は、次のいずれかを実行します。
 - a. バージョン11.3以前では、値を手入力してEnterを押します。
 - b. バージョン11.4以降では、コピーした値をペーストしてEnterを押します。
 - c. バージョン11.4以降では、**クエリフィルタ**フィールドに入力し始めます。

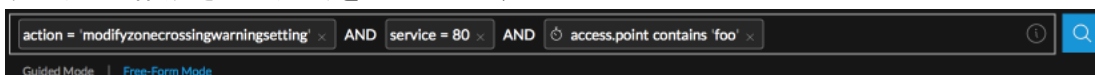
入力に合わせて、メタ値ドロップダウンリストが絞り込まれ、入力したテキストで始まる、最大100個のインデックスされた値が表示されます。候補値は、時間範囲のみに基づいています。クエリ内のフィルタは、100個の値のリストの絞り込みには使用されません。自動提案機能により、(最大10,000件の)ダウンロードされたイベントだけでなく、現在のデータセット内のすべてのイベントで一致が検索されます。リスト内に完全に一致するものがない場合は、**クエリフィルタ**フィールドに入力したテキストがハイライト表示され、候補が見つからなかったことがメッセージに示されます。serviceメタキーの整数値のように、一部の値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**キーを押します。
値がフィルタ入力フォームに追加されます。
5. フィルターを作成するには、**Enter**キーを押します。**Enter**を押す前にボックスの外側をクリックした場合は、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。フィルタにカーソルを合わせると、エラーの説明を含むツールチップが表示されます。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。

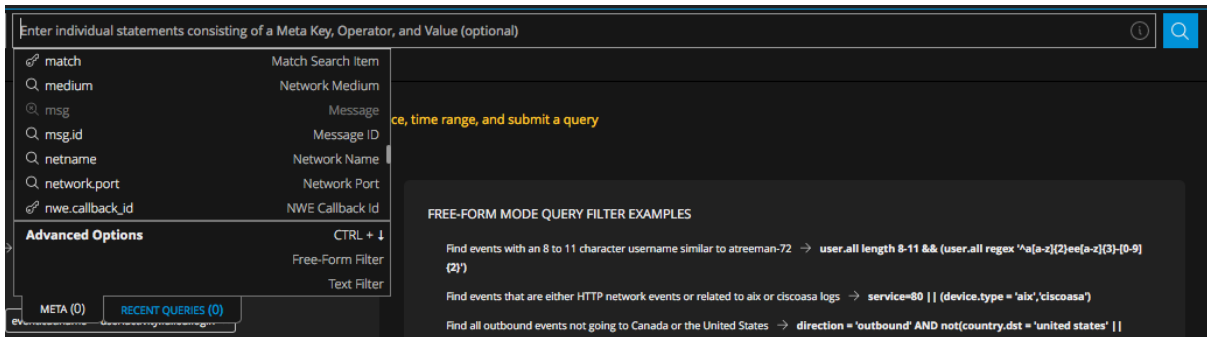


6. フィルタにエラーがない場合は、クエリバーでクエリを実行する準備ができています。をクリックします。
結果が返され、[イベント]パネルにロードされます。クエリに一致する最初の1万イベントの[イベント]パネルへのロードが開始されます。イベントがロードされる間、上部にあるステータスバーで進行状況を確認できます。リストの一番下までスクロールして、完了ステータスを確認できます。
7. (バージョン11.3以降のオプション) クエリコンソールで詳細ステータスを表示するには、 (情報アイコン) をクリックします。
8. (バージョン11.3以降のオプション) 実行が完了する前にクエリをキャンセルする場合は、 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。

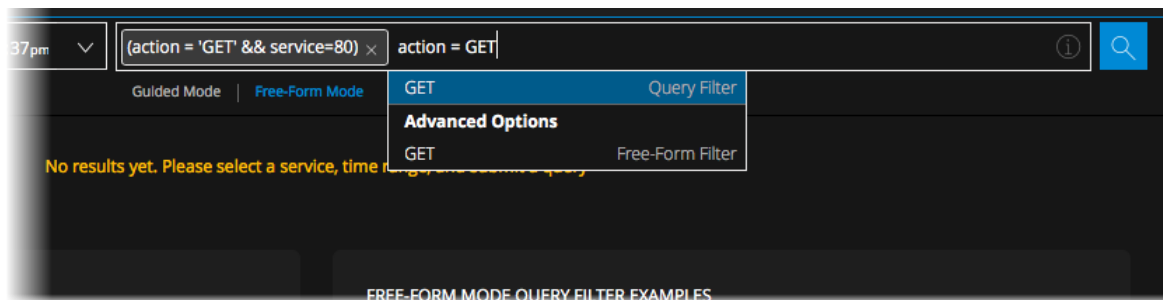
ガイド モードでのフリーフォーム フィルタの追加(バージョン11.3以降)

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。

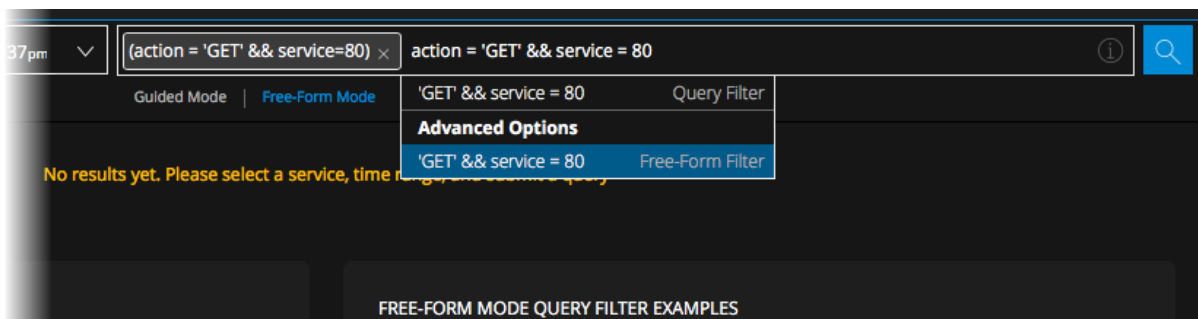
1. [イベント]ビューに移動し、クエリバーの下にある **ガイド モード** を選択して、クエリビルダフィールドをクリックします(バージョン11.4.1の場合は、クエリビルダフィールドを単にクリックします)。挿入ポイントが2つのフィルタの間にある場合は、緑色の丸または太字のカーソルによって挿入ポイントがマークされます。挿入ポイントがクエリバーの最後尾にある場合は、エントリーポイントに点滅するカーソルが表示されます。ドロップダウンメニューには、調査中のサービスから渡された使用可能なメタ キーがアルファベット順に表示されます。






2. 次のいずれかの操作を実行します。
 - 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。

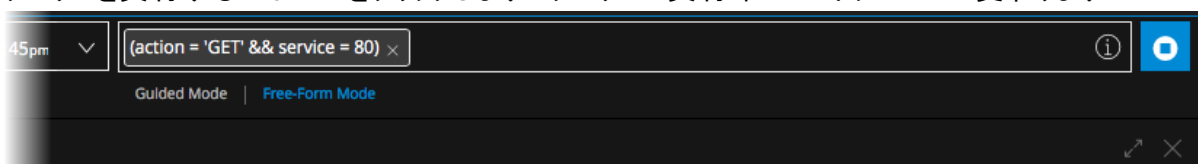




3. 式全体の入力を続けて、Enterを押します (Enterを押す前にボックスの外側をクリックした場合は、フィルタは作成されません)。次の図は、値GETの後に入力し続けることによって作成された自由形式の式を示しています。



新しいフィルタが挿入され、点滅しているカーソルが、最後のフィルタの後で再びフォーカスされ、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。フィルタにカーソルを合わせると、エラーの説明を含むツールチップが表示されます。




4. クエリを実行するには、 をクリックします。クエリの実行中に  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、クエリ実行の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。

データセット内の任意の場所で値を検索するためのテキスト フィルタの追加(バージョン11.4以降)

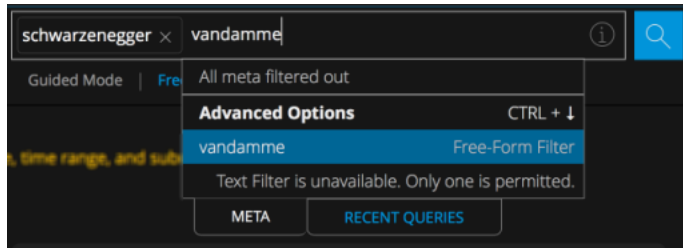
バージョン11.4以降では、テキスト フィルタを使用して、現在のデータセット(エンドポイント、ログ、ネットワーク イベント)内の特定の値を検索できます。テキスト フィルタは、値がインデックスされたすべてのメタ キーを対象に、大文字と小文字を区別せず、検索を実行します。テキスト フィルタでは、メタ キーによってインデックスされた値とインデックスなしの値は検索対象とならないため、すべての結果が表示されるわけではありません。"Results may be limited by a text filter, which matches only indexed meta keys. If you want to conduct a more exhaustive search against raw events, [click here](#) and choose the appropriate options in the Search Events drop-down menu."というメッセージのアドバイスが表示されます。ドロップダウン リスト内のアイコンは、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。

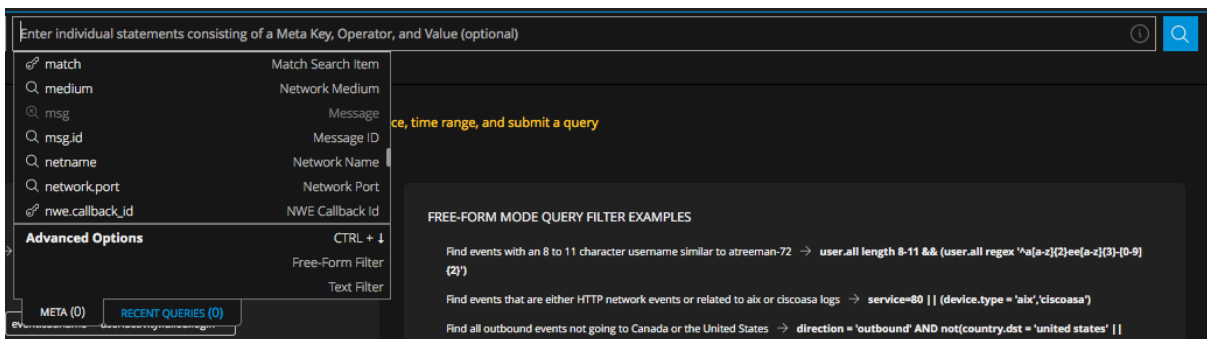
テキスト フィルタは、どこを探すべきか(どのメタ キーまたはサービスか)がわからなくても、探しているものについてある程度わかっている場合に役立ちます。たとえば、ファイル名を検索したい場合、クエリバーをクリックして、テキスト文字列全体を入力し、**テキスト フィルタ**をクリックします。テキスト フィルタは、調査対象のサービスと時間範囲内で、インデックスにあるすべてのデータを検索し、テキスト文字列と正確に一致するものを返します。

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。

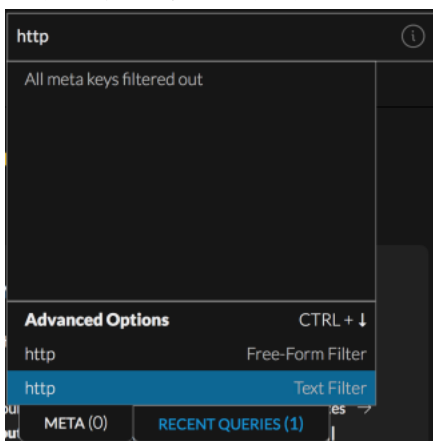


テキスト フィルタを作成するには、次の手順を実行します。

1. **イベント** ビューに移動し、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。

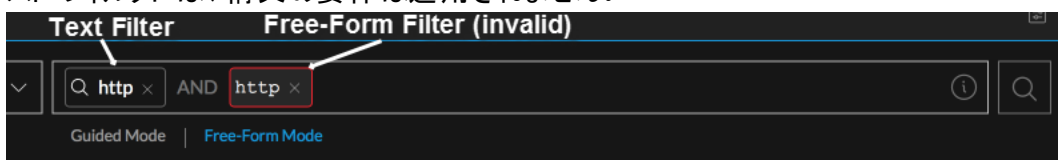


2. 検索するテキスト文字列を入力します(たとえば「http」)。テキスト文字列がメタ キードロップダウンリストの **詳細オプション**の下に表示されます。

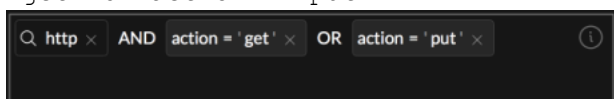


3. **詳細オプション**の下にある **テキスト フィルタ**をクリックします。テキスト フィルタがクエリバーに追加されます。次の図は、テキスト フィルタとフリーフォーム フィルタの


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。

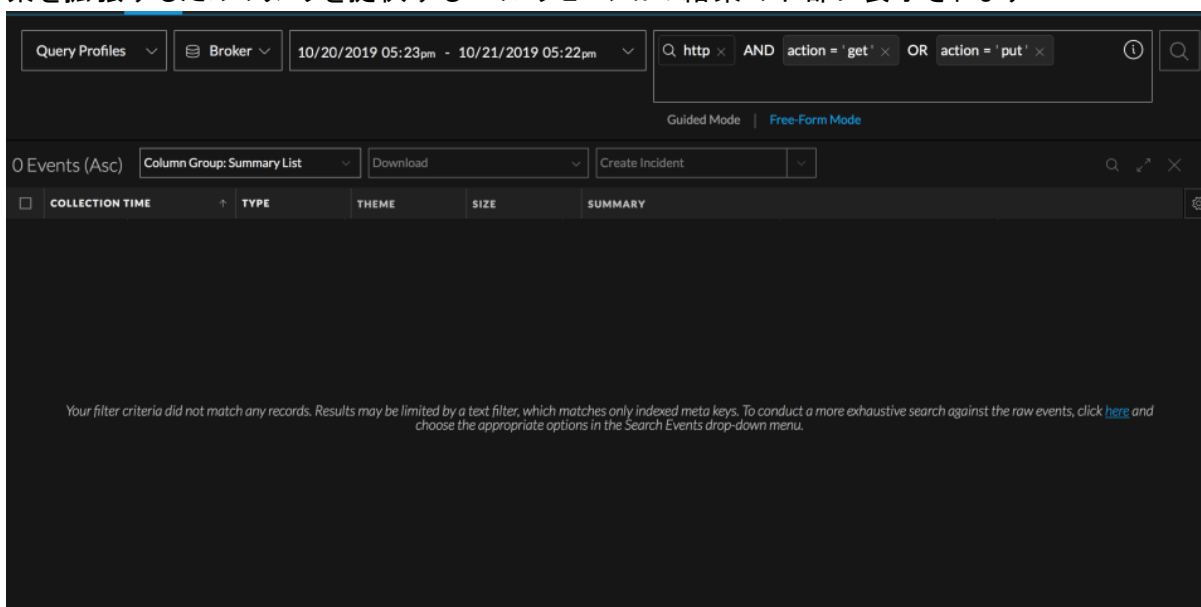


- (オプション) シンプルまたはフリーフォームのフィルタをクエリバーに追加します。クエリに使用できるテキストフィルタは1つだけです。この例は、「http」をテキストフィルタとして入力し、「action = 'get' OR action = 'put'」



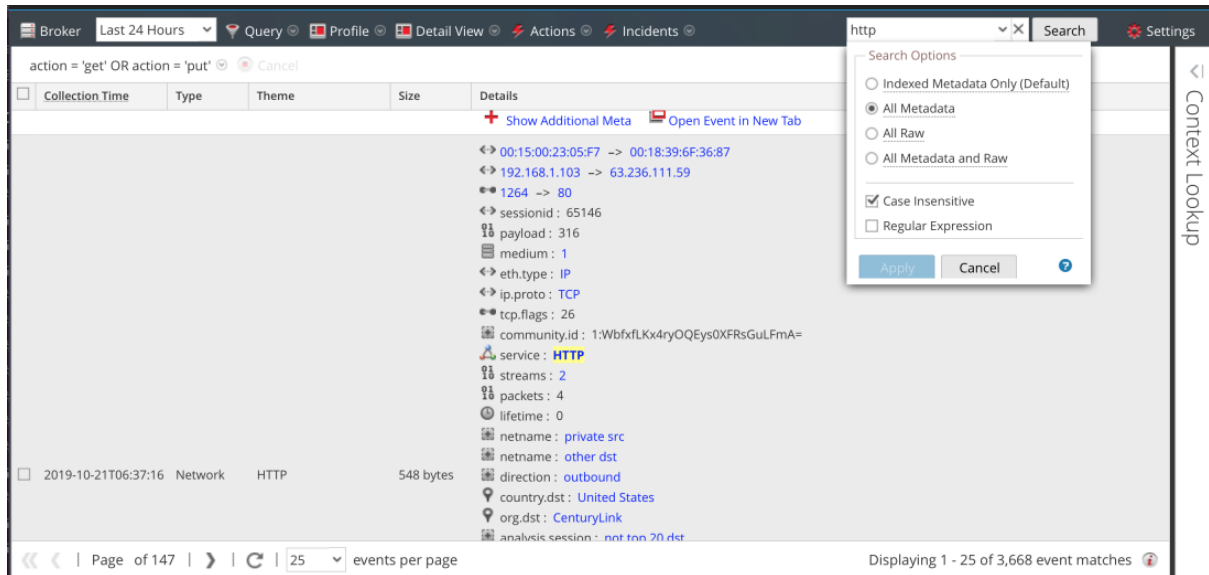
という2つのフィルタを追加して、クエリを完成しています。


- 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。

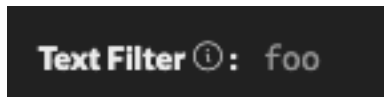


- メッセージ内の [ここ](#) リンクをクリックします。新しいブラウザタブが開き、クエリの結果が「ガシー イベント」ビューに表示されます。ここでは、検索を改善するための追加のオプションを使用できます。次の図は、インデックスなしのメタデータも対

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、クエリコンソールのテキストフィルタを示しています。



クエリバーで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、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、**Ctrl + A** (Windows OS) または **Cmd + A** (MacOS) キーを押します。
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。

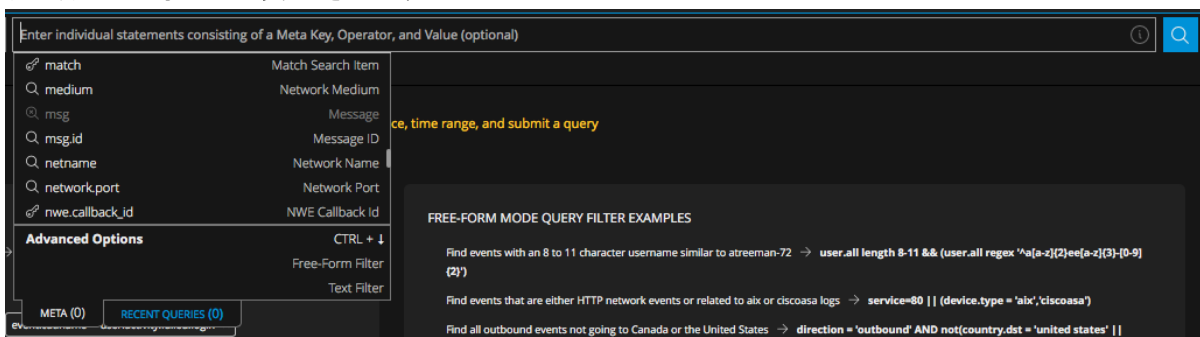
クエリバーへのテキストのペースト(バージョン11.4以降)

[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、手入力する代わりに、他の場所からコピーしたフィルタの完全な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。

- この形式のテキスト文字列が追加されると、新しいシンプルフィルタがクエリバーに追加されます。
<valid meta key> <valid operator> <optional value>.例を示します。alias.host contains 's'.
- この形式のテキスト文字列が追加されると、2つのシンプルなフィルタがクエリバーに追加されます。
<valid meta key> <valid operator> <optional value> && <valid meta key> <valid operator> <optional value>.例を示します。alias.host contains 's' && action exists. これは、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、ガイドモードで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、これは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。次のいずれかの操作を実行します。
 - 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は、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が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。

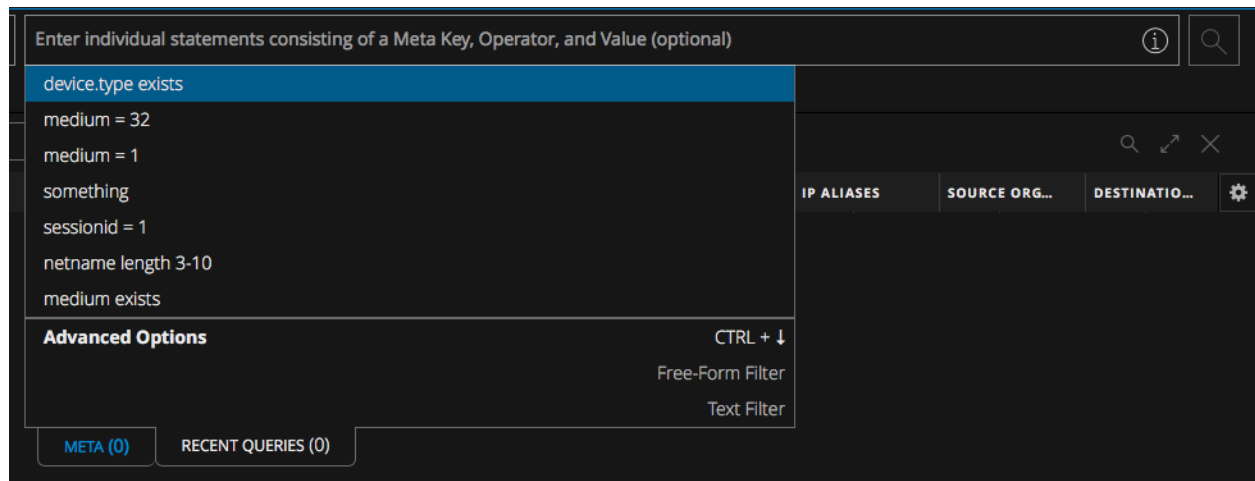
- 必要に応じてクエリバーにさらにフィルタを追加し、クエリを送信します。
クエリが実行されます。

最近のクエリに基づくフィルタの挿入(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に基づいて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。リストは、最新のものが一番上に表示されるようにソートされ、最近のクエリ数は0に設定されます。入力を開始すると、リストがフィルタリングされ、最近の100件のクエリに一致するものがない場合でも、一致するテキストを含むクエリ履歴データベースから最大100件のクエリが表示されます。最近のクエリ]カウントは、入力と一致するクエリの数を変化させます。

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。

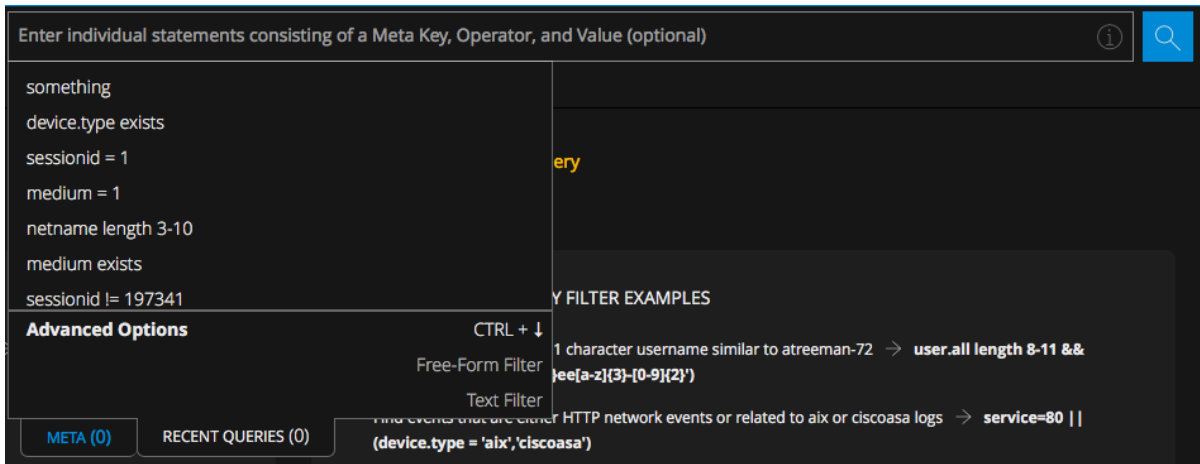
クエリを送信するたびに、リストがソートされ、そのクエリが最新のクエリとして一番上に追加されます。



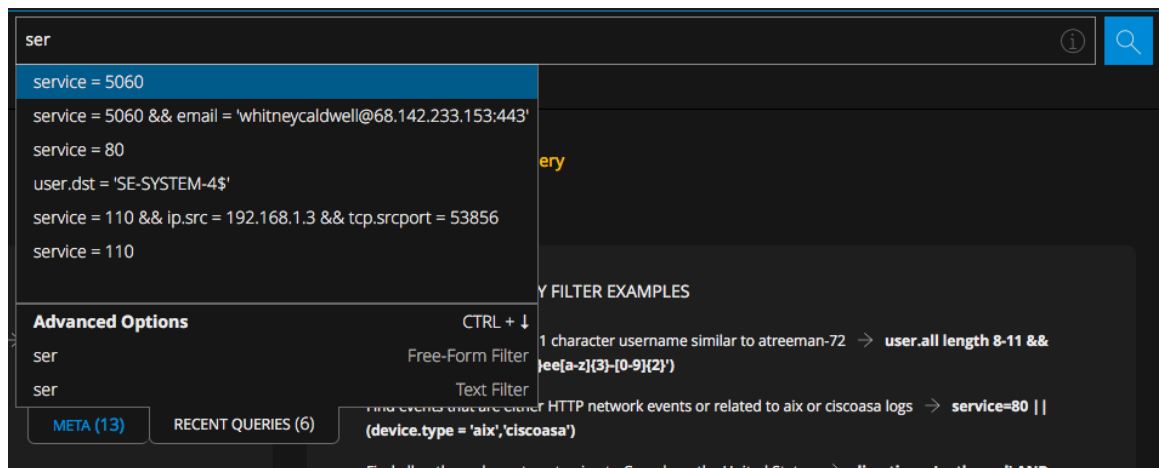
最近のクエリからフィルタを作成するには、次の手順を実行します。

- [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)。
[タキー]ドロップダウンリストが [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、その数は0です。




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変化して変化します。



- 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、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

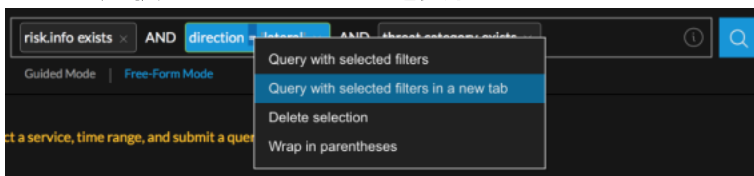
ガイド モードのクエリバーでクエリを使用すると、フィルタを編集できます。フィルタを編集するには、次の操作を行います。

1. フィルタをダブルクリックします。または、フィルタをクリックし、Enterキーを押します。
2. フィルタを編集します。編集が終了したら、Enterキーを押して、フィルターを更新します。
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

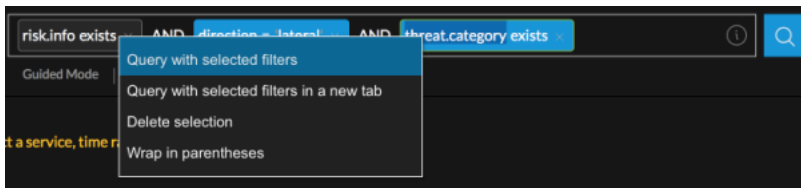
ガイド モードのクエリバーに1つまたは複数のフィルタがある場合は、選択したフィルタのみを含むクエリを再フォーカスし、現在のブラウザ タブまたは新しいブラウザ タブに結果を表示できます。バージョン11.4では、フィルタにネスト構造の括弧を使用した式が含まれる場合があり、そのようなフィルタの一部を再フォーカスできます。選択したフィルタのみを使用してクエリを更新するには、次のいずれかを実行します。

1. 1つ以上のシンプルな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つのフィルタを含むクエリを使用します。
 - a. `direction = 'lateral'`を選択し、右クリックします。次に、ドロップダウンメニューで **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。



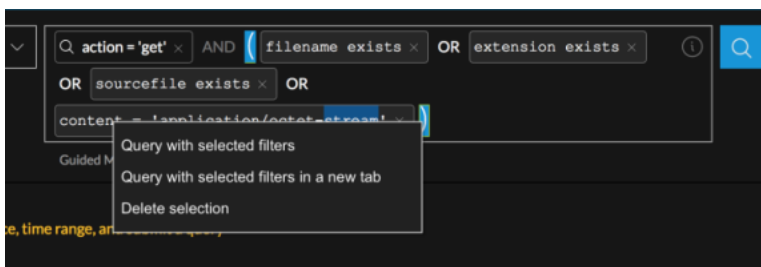
選択したフィルタの結果が新しいタブに表示され、元のクエリは、以前のタブにそのまま残ります。

- 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(`action = 'get' AND (filename exists OR sourcefile exists OR content = 'application/octet-stream')`)などの場合は、次のいずれかを実行します。



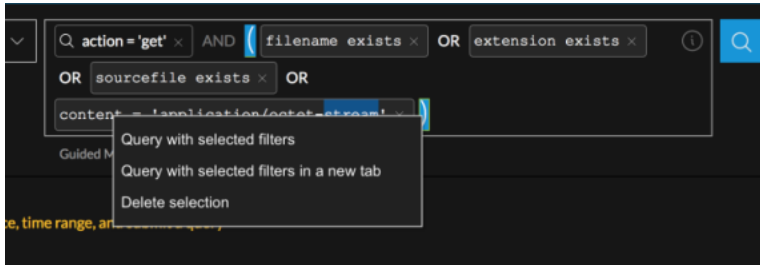
- a. 'application/octet-stream'の後の閉じ括弧を選択し、右クリックします。次に、**新しいタブで、選択したフィルタでクエリを実行**]を選択します。新しいタブが開いて、(filename exists OR sourcefile exists OR content = 'application/octet-stream')の結果が表示されます。
- b. 同じものを選択し、右クリックします。次に、**選択したフィルタでクエリを実行**]を選択します。現在のタブに、(filename exists OR sourcefile exists OR content = 'application/octet-stream')の結果が表示されます。

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には、クエリバーで、文字の隣にカーソルを置き、**Backspace**(Windows OS) または **Delete**(MacOS) キーを押します。
 - b. すべての文字を削除するには、フィルタにカーソルを合わせ、**Delete**(Windows OS) または **Fn + Delete**(MacOS) キーを押します。
 - c. 選択した文字を削除するには、クエリバーで文字を選択し、**Delete** または **Backspace** キーを押します。
 - 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. 1組の括弧とその内容((filename exists OR sourcefile exists OR content = 'application/octet-stream') など)を削除するには、getの後の括弧を選択し、右クリックします。次に、**選択項目の削除**]を選択します。

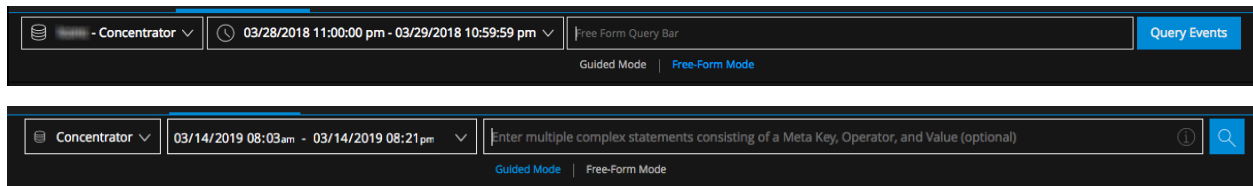


action = 'get'以外のすべてが削除されます。

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文字のユーザー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}')
```

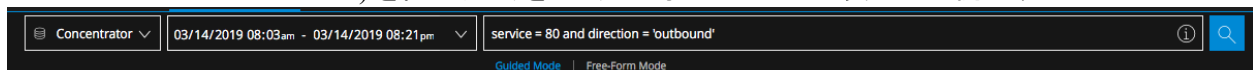
HTTPネットワークイベントとaixまたはciscoasaログに関連するイベントを検索する場合：

```
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せん。

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。

注：バージョン11.6では、「イベント」ビューの「イベントの絞り込み」パネルがこの機能を提供するため、デフォルトで「ナビゲート」ビューは無効になっています。「ナビゲート」ビューを有効にするには、「[「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。

- [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](#)
- [Investigation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。

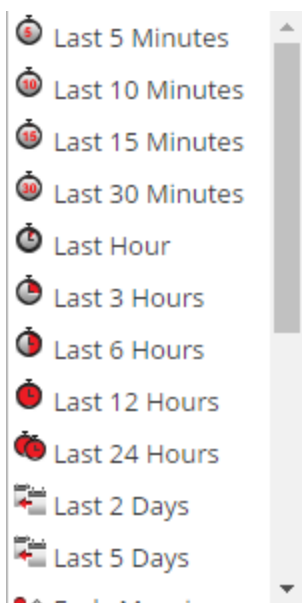
- 収集データの時間範囲。最後に収集されたデータの時刻を基準にして、一定の時間範囲を選択します。
- カレンダーの日付を基準にした時間範囲。
- カスタムの時間範囲。
- すべてのデータ。

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 スタートガイド』の「ユーザー環境設定の設定」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」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. 次のいずれかの操作を実行します。

- 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。
- 収集の時間範囲を分、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。
- 固有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**]、**分**]フィールドを選択するか、**現在**]をクリックします。時間の選択は、デフォルトで現在の時刻になっています。

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

[サビゲート]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。

[サビゲート]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、[サビゲート]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、[「サビゲート」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。

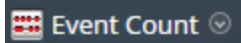


次の図では、「Event Type」というメタ キーが [値] の降順で表示されています。アルファベットの最後の文字から順に、値が表示されていることがわかります。値 success auditが先頭に表示されています。値 connectが最後に表示されています。集計方法は [イベント数] です。



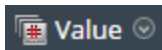
[サビゲート]ビューでメタ キーを集計する方法と結果の表示順を選択するには、次の手順を実行します。

- 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。



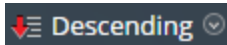
選択内容に応じて現在のビューが再ロードされます。

- 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。



Investigation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ー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きに、NetWitnessではそのメタキーの値のロードを開始します。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ー定義のメタグループがあります。作成したユーザー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](#)」を参照してください。

「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、値によるインデックス付けが設定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。

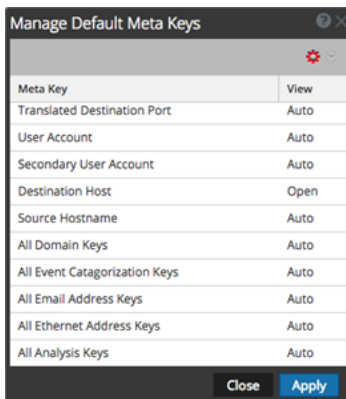
初期の [ナビゲート] ビューがデフォルトのメタ キーを使用して開くように指定するには、次の手順を実行します。

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

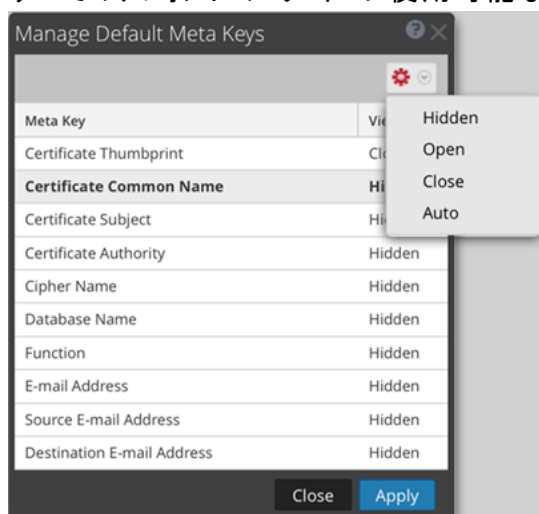
[ナビゲート] ビューでデフォルトのメタ キーのデフォルトの表示を構成するには、次の手順を実行します。

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. 次のいずれかの操作を実行します。
 - (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。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。

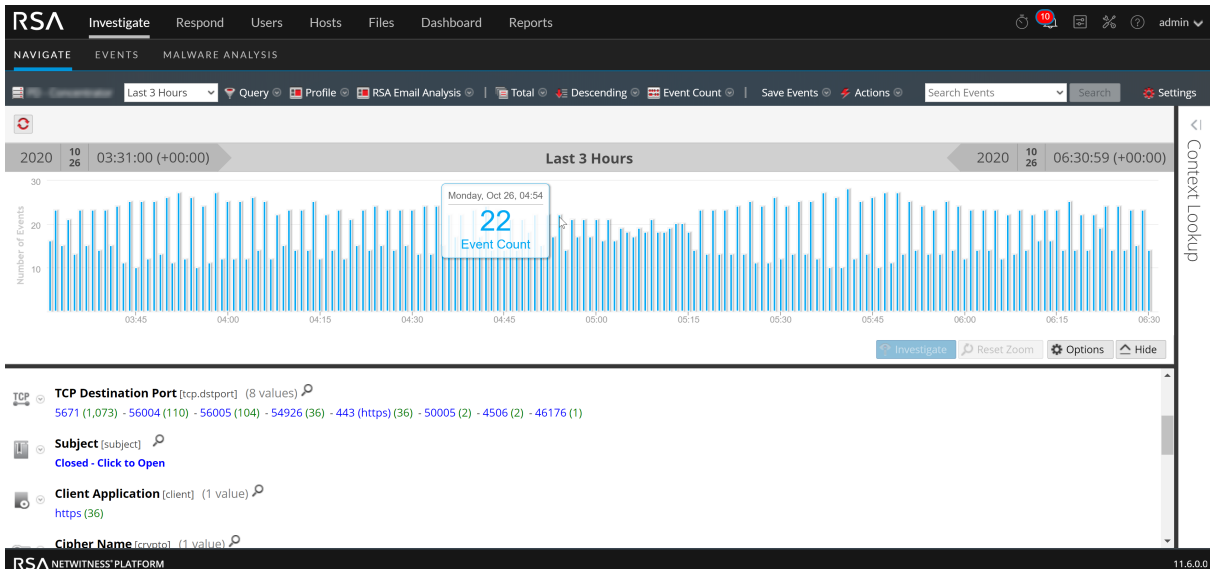
ナビゲート] ビューに表示されるメタ キーは、指定された内容で設定されます。デフォルトのメタ キーが非表示の場合、そのメタ キーの値は調査では一切表示されません。デフォルトのメタ キーが折りたたみ表示の場合、そのメタ キーの値はデフォルトではロードされません。ただし、 **ナビゲート**] ビューで個々のメタ キーを手動でロードすることはできます。

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。タイム チャートにカーソルを合わせると、特定の時間に発生したイベントの総数を表示できます。



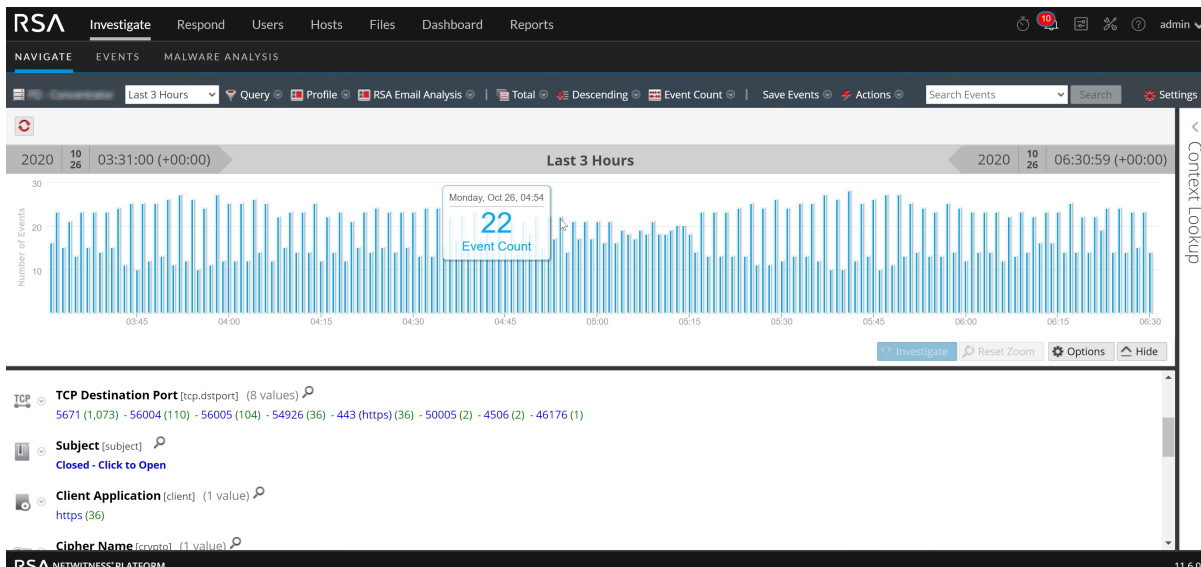
2. タイムチャート上でマウスのクリックとドラッグを行い、目的の時間範囲を選択します。選択した時間範囲がハイライト表示されます。
選択した時間範囲のタイムチャートが再描画されます。ただし、メタ値は変更されません。
3. 選択した時間範囲のデータにドリルダウンするには、**調査**]をクリックします。
URLが更新され、新しい時間範囲が反映されます。さらに、Investigationオプションパネルでは、時間範囲がカスタム時間範囲に変更されます。選択した時間範囲を使用して、タイムチャートが再描画され、メタ値がロードされます。
4. タイムチャートを元の時間範囲にリセットするには、**ズームのリセ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

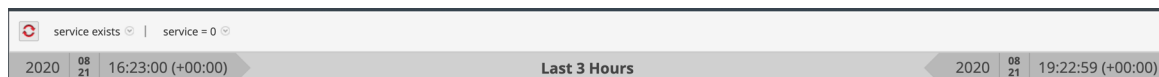
メタデータのサブセットにドリルダウンするには、次の手順を実行します。

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。

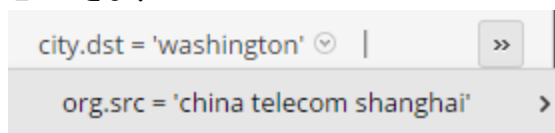


2. メタデータをドリルダウンするには、次の操作を任意の組み合わせで実行します。

- a. **メタキー**、たとえば、[サービスタイプ]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。

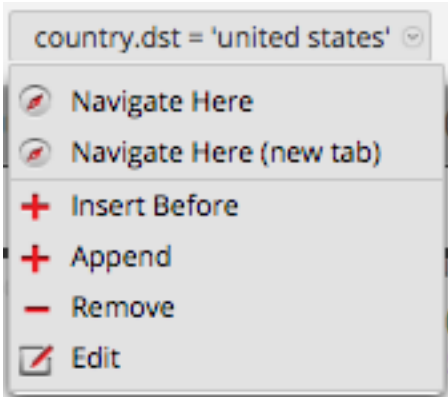


階層リンクでクエリを追加するには、次の手順を実行します。

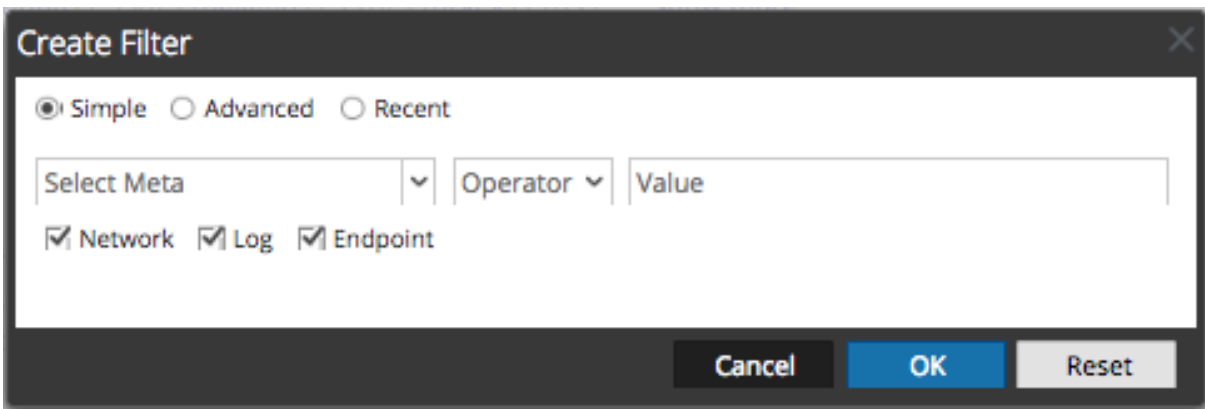
階層リンクにある任意のクエリをクリックすると、クエリメニューを表示できます。クエリの前に新しいクエリを挿入することや、階層リンクの末尾に新しいクエリを追加することができます。階層リンクを編集すると、その都度、NetWitnessによって結果が更新されます。

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. 階層リンクに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。



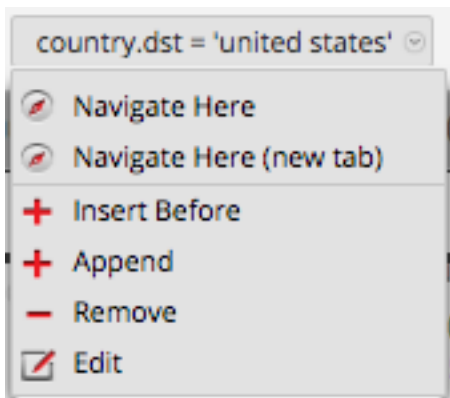
3. 「[\[サビゲート\]ビューと \[ガシー イベント\]ビューでのクエリの作成](#)」の説明に従って、クエリを作成します。

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。

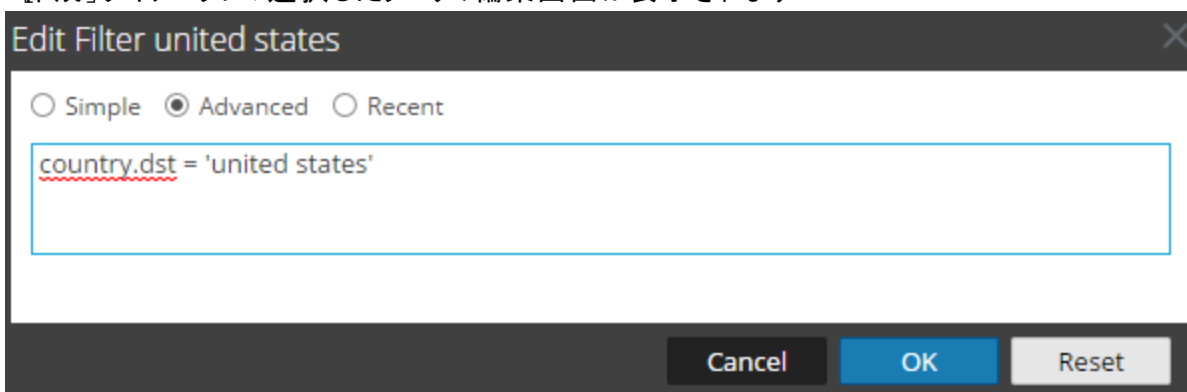
階層リンクにある任意のクエリをクリックすると、クエリメニューを表示できます。クエリを削除したり、クエリを編集することができます。階層リンクを編集すると、その都度、NetWitnessによって結果が更新されます。

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。



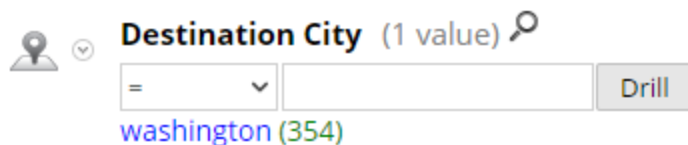
- 階層リンクのクエリを編集するには、**編集**を選択します。
作成]ダイアログに、選択したクエリの編集画面が表示されます。



- 「[ナビゲート\]ビューと \[ガシー イベント\]ビューでのクエリの作成](#)」の説明に従って、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。

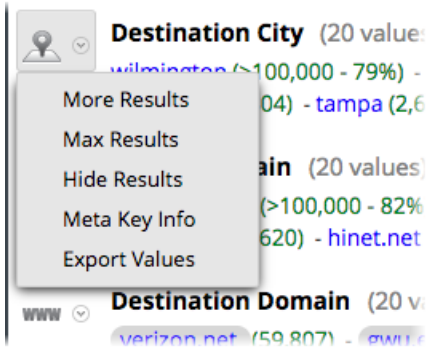
- メタ キー セクションに移動し、虫眼鏡アイコンをクリックします。
クイック検索]フォームが開きます。演算子とテキスト入力ボックスが表示され、検索条件を指定できます。



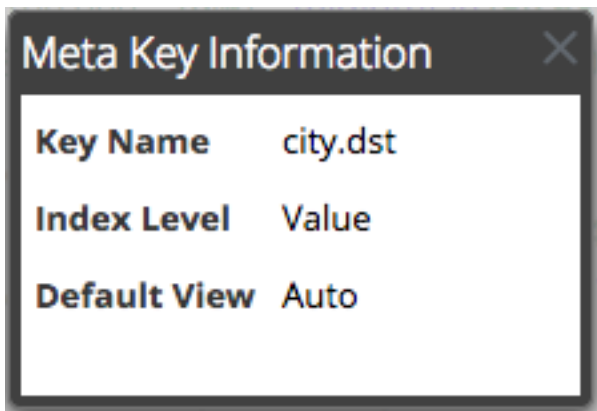
- (オプション) この検索フォームを閉じるには、虫眼鏡アイコンをもう一度クリックしてください。
- 左のドロップダウン リストから演算子を選択し、検索するテキスト値を入力します。[ドリルダウン]をクリックすると、検索が実行されます。
指定したメタキーとメタ値を使用して現在表示中のメタデータが絞り込まれ、結果が表示されま

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。

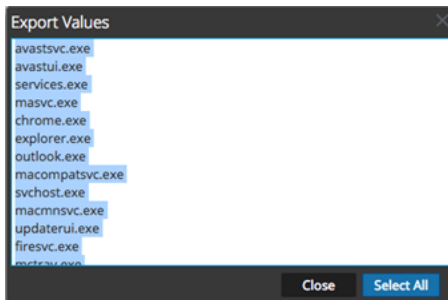
1. キー名、メタ キー表示用に設定されたインデックスレベル、メタ キーに設定されたデフォルト ビューを表示するには、メタ キーの横に表示されるドロップダウン メニューをクリックします。次の図は、バージョン11.1以降のドロップダウン メニューを示しています。



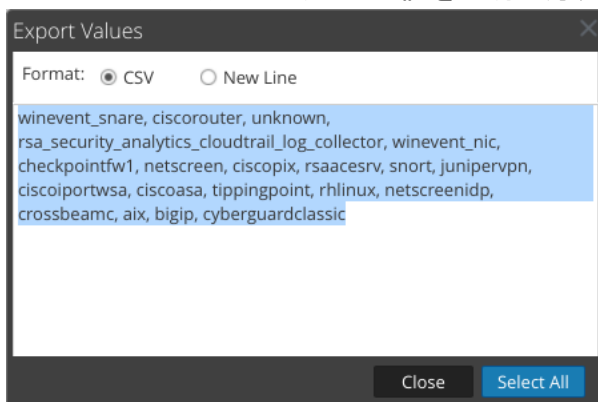
2. [メタ キー情報] を選択します。
[メタ キー情報] ダイアログが表示されます。



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ナ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。

[レガシー 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、「[イベントの再構築と分析](#)」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。

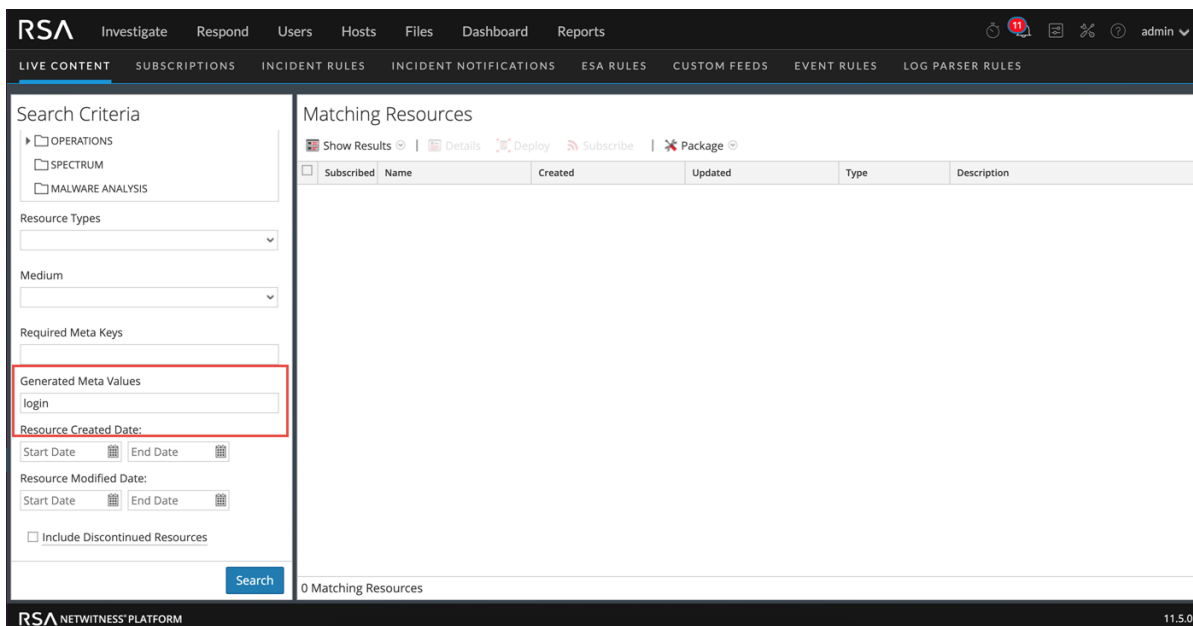
1. [ナビゲート]ビューで、調査の対象となるメタ データまでドリルダウンします(メタ値をクリックするか、クエリを追加します)。
2. [イベントの検索]ボックスに検索文字列を入力し、Enterを押すか、**検索**]をクリックします。
検索モード環境設定を選択して設定することもできます。検索情報の詳細については、「[ナビゲート\]ビューと \[レガシー イベント\]ビューでのテキスト パターンの検索](#)」を参照してください。
[イベント]ビューの新しいタブが開き、検索結果が表示されます。ハイライト表示された検索語が見つからない場合は、**追加のメタの表示**]をクリックします。時間範囲の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

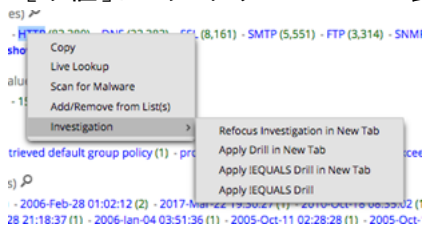
1. 「ナビゲート」ビューで、調査の対象となるメタデータまでドリルダウンします。
2. メタ値(青色で表示されたテキスト)を右クリックします。
メタ値]ドロップダウンメニューが表示されます。
3. RSA Liveでメタ値を検索するには、**「Liveルックアップ」**を選択します。
Liveの「検索」ビューが開いて、入力したメタ値が「生成されるメタ値」フィールドに表示され、検索

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。

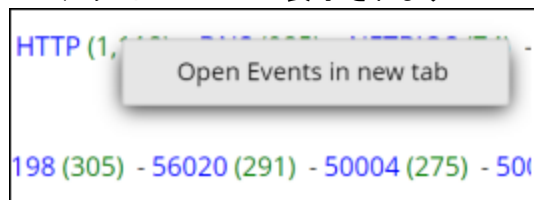
1. メタ値 (青色で表示されたテキスト) を右クリックします。
 [メタ値] ドロップダウンメニューが表示されます。



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を表示するには、メタ値のカウン (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

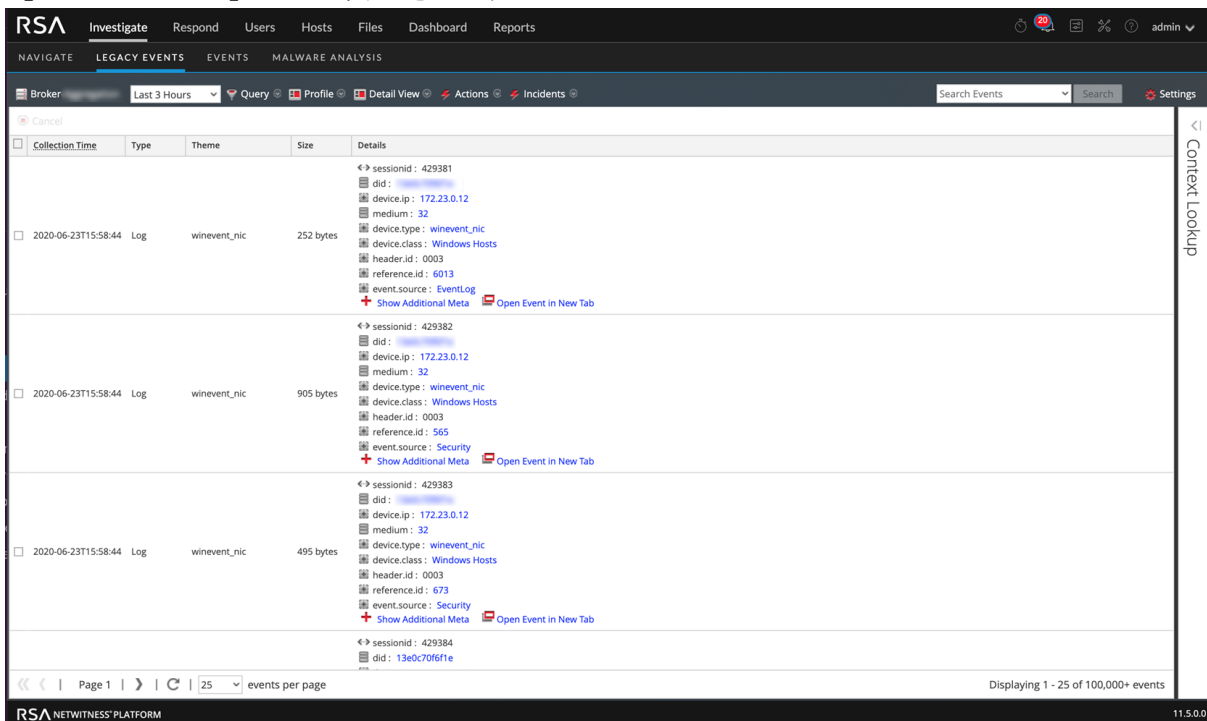
アナリストは、[レガシー イベント]ビューでイベントの検索、サービスの選択、時間範囲の設定、メタデータのクエリを行って、イベントをフィルタリングできます。[ナビゲート]ビューのドリルダウン ポイントから [レガシー イベント]ビューを開くと、デフォルトでイベントの詳細ビューが表示されます。[ナビゲート]ビューを使用する権限がないアナリストは、[レガシー イベント]ビューからサービスに直接クエリを実行できます

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. 「[\[ナビゲート\]ビューと \[レガシー イベント\]ビューでのクエリの作成](#)」の説明に従って、クエリを作成します。
[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。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条件で連結する複雑なクエリがNetWitnessによって生成されます。したがって、メタ グループにip.srcとip.dstが含まれる場合、生成されるクエリは「ip.src = <value> OR ip.dst = <value>」になります。異なる値タイプのメタ キーがメタ グループに含まれる場合、条件の値の入力は無効化され、existsステートメントを使用したクエリが生成されます。たとえば、ip.src、ip.dst、alias.hostを含むメタ グループは、異なる値タイプのメタ キーを含んでいます。ip.srcとip.dstはIPアドレスで、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>]
```

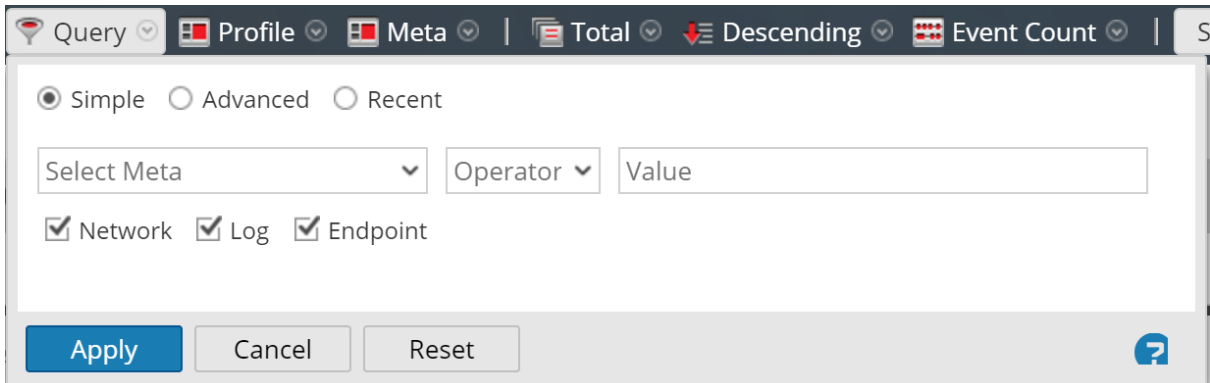
以下に、例をいくつか示します。

```
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」の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。次のいずれかの操作を実行します。
 - 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. 次のいずれかの操作を実行します。
 - 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せん。
 - 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 [ガシィ 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。

Query | Profile | Meta | Total | Descending | Event Count

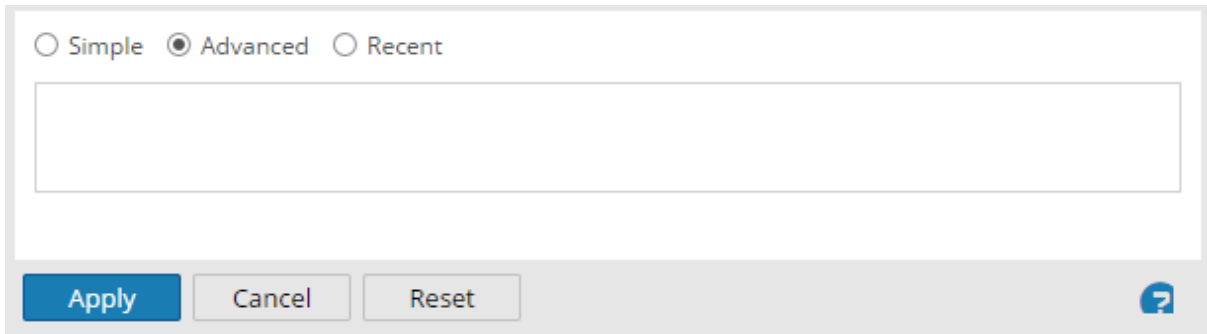
Simple Advanced Recent

Select Meta | Operator | Value

Network Log Endpoint

Apply Cancel Reset

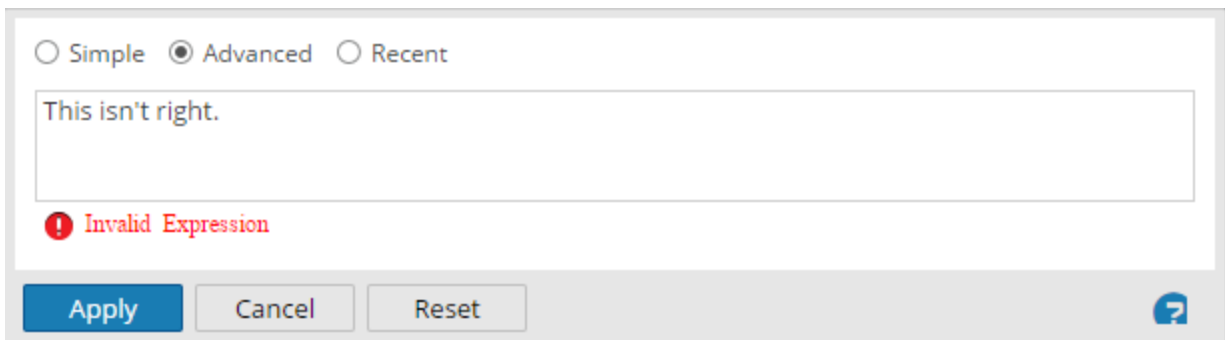
2. **詳細設定**を選択します。
詳細なクエリのフィールドが表示されます。



○ Simple ● Advanced ○ Recent

Apply Cancel Reset ?

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。



○ Simple ● Advanced ○ Recent

This isn't right.

! Invalid Expression

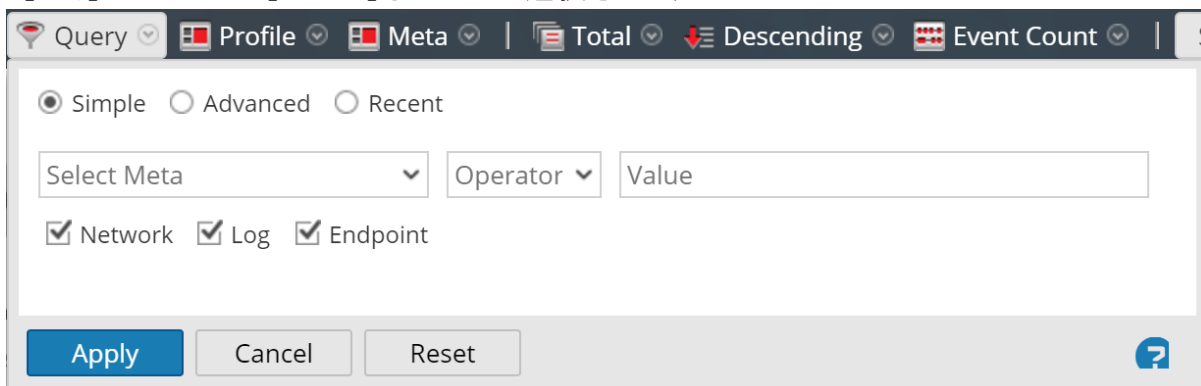
Apply Cancel Reset ?

6. 次のいずれかの操作を実行します。
 - **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。



Query Profile Meta | Total Descending Event Count

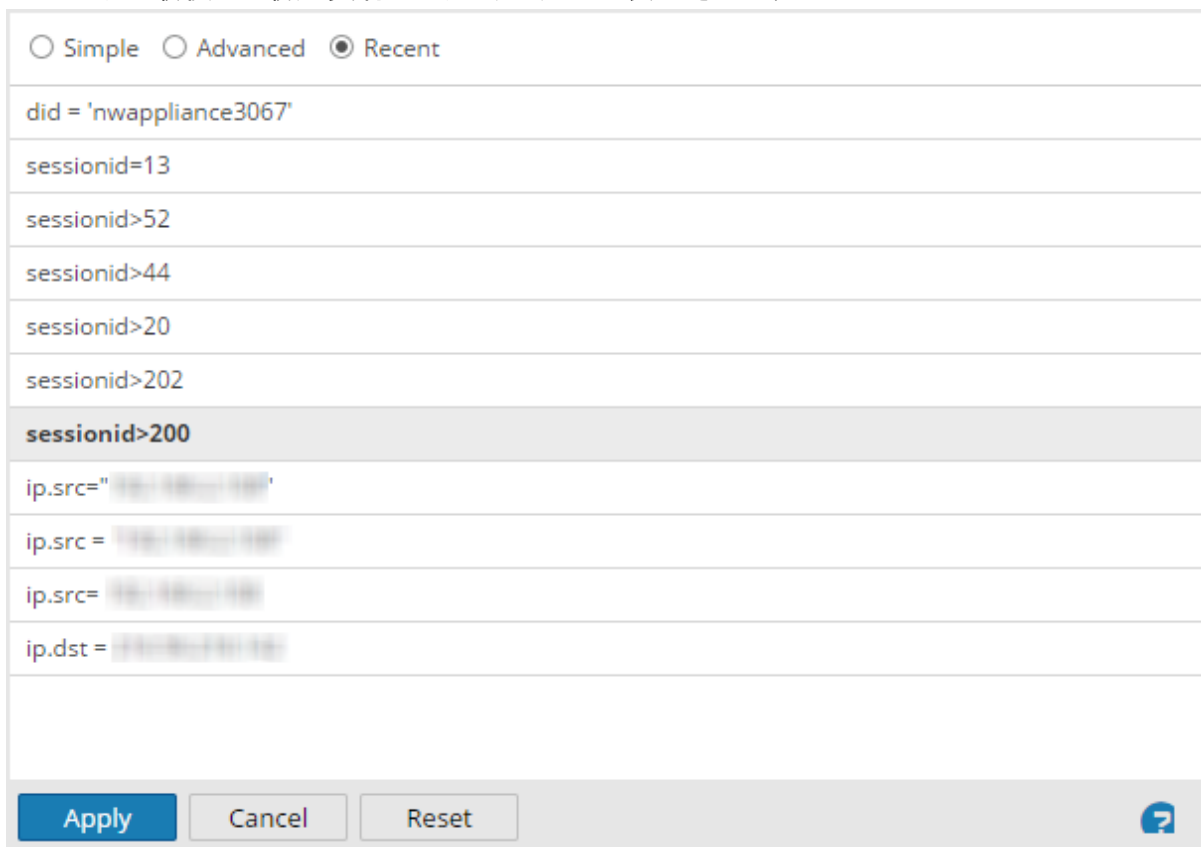
Simple Advanced Recent

Select Meta: Network Operator: > Value:

Network Log Endpoint

Apply Cancel Reset

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。



Simple Advanced Recent

did = 'nwappliance3067'

sessionId=13

sessionId>52

sessionId>44

sessionId>20

sessionId>202

sessionId>200

ip.src = '192.168.1.100'

ip.src = 192.168.1.100

ip.src = 192.168.1.100

ip.dst = 192.168.1.100

Apply Cancel Reset

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. 次のいずれかの操作を実行します。
 - 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せん。
 - **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。

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キーを押すか「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の両方が存在する必要があります。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」のどちらかが存在する必要があります。
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

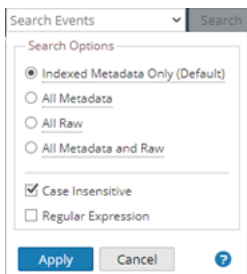
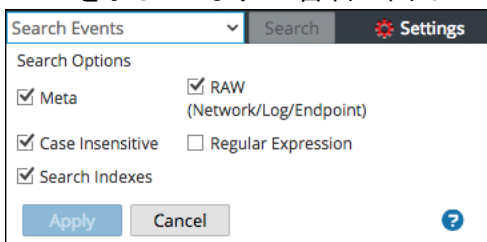
[ナビゲート]ビューまたは[レガシー イベント]ビューで検索ボックスと検索オプションにアクセスするには、次の手順を実行します。

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
<p>[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)</p> <p>[インデックス] ラジオ ボタン (バージョン11.1)</p>	<p>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。</p> <p>注意：サブストリンゲ一致は、インデックス検索では検出されません。サブストリンゲ一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。</p>
<p>[すべてのメタデータ] ラジオボタン (バージョン11.2)</p> <p>[メタ] チェックボックス (バージョン11.1)</p>	<p>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。</p>
<p>[すべてのRAW] ラジオボタン (バージョン11.2以降)</p> <p>[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)</p>	<p>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一致するコンテンツが検索されます。</p> <p>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。</p> <p>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。</p>
<p>[すべてのメタデータとRaw] ラジオ ボタン (バージョン11.2)</p>	<p>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。</p>
<p>大文字と小文字を区別しない</p>	<p>大文字と小文字を区別せずに検索します。</p>
<p>正規表現</p>	<p>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。</p> <p>注意：</p> <ul style="list-style-type: none"> -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。
<p>適用</p>	<p>[ナビゲート] ビューと [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。</p>

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キーを押すか、[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キーを押すか、[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には、NetWitnessアーキテクチャに対する検索を可能にすることによって、サードパーティ製品との統合を容易に構成できるようにする外部URL統合が含まれています。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、ユーザー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サーバーのIPアドレスまたはDNS名で、必要に応じて、ポート (SSLの場合など) 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サーバーのIPアドレスまたはDNS名で、必要に応じて、ポート (SSLの場合など) 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インスタンスで定義されているクエリ対象のサービスのホストとポートです。NetWitnessは、NetWitness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%27C%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

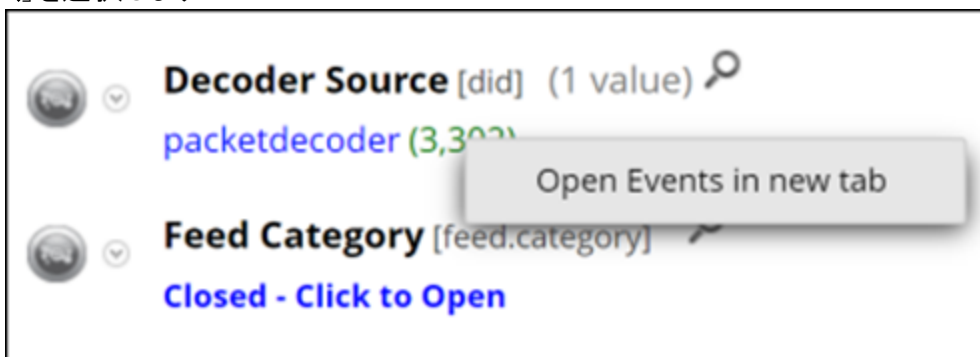
[ナビゲート]ビューまたは [イベント] リストでイベントを絞り込んだら(「[結果セットの絞り込み](#)」を参照)、次のステップは、イベントの再構築、添付ファイルの確認、サードパーティールックアップまたは内部ルックアップでの追加コンテキストの表示を行って、イベントについて詳しく理解することです。

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. **調査** > [イベント]に移動します。
2. **調査** > [ナビゲート](バージョン11.5以前)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のリストが [イベント] ビューに表示されます。

COLLECTION TIME	TYPE	DECODER	TRAFFIC F...	SERVICE T...	HOSTNAM...	SOURCE IP...	DESTINATI...	IP ALIASES	SOURCE O...	DESTINATI...	SOURCE C...	DESTINATI...	SOURCE D...	DES
08/20/2020 06:21:38 pm	1[Network]	nh	lateral	0[OTHER]		10.237.169.48								
08/20/2020 06:21:38 pm	1[Network]	nh	lateral	0[OTHER]		10.237.169.40	10.237.169.87							
08/20/2020 06:21:37 pm	1[Network]	nh	lateral	0[OTHER]		0.0.0	10.237.168.0							
08/20/2020 06:21:38 pm	1[Network]	nh		0[OTHER]										
08/20/2020 06:21:38 pm	1[Network]	nh	lateral	443[SSL]		10.237.169.87	10.237.169.40							
08/20/2020 06:21:38 pm	1[Network]	nh	lateral	443[SSL]		10.237.169.87	10.237.169.40							
08/20/2020 06:21:38 pm	1[Network]	nh	lateral	443[SSL]		10.237.169.87	10.237.169.40							
08/20/2020 06:21:41 pm	1[Network]	nh	lateral	0[OTHER]		10.237.169.91	10.237.169.40							
08/20/2020 06:21:41 pm	1[Network]	nh	lateral	0[OTHER]		10.237.169.91	10.237.169.40							
08/20/2020 06:21:42 pm	1[Network]	nh	lateral	443[SSL]		10.237.169.40	10.237.169.87							
08/20/2020 06:21:43 pm	1[Network]	nh	lateral	0[OTHER]		10.237.169.40	10.237.169.87							
08/20/2020 06:21:43 pm	1[Network]	nh	lateral	0[OTHER]		10.237.169.87	10.237.169.40							

このビューで使用できる再構築と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詳細の調査](#)」を参照してください。

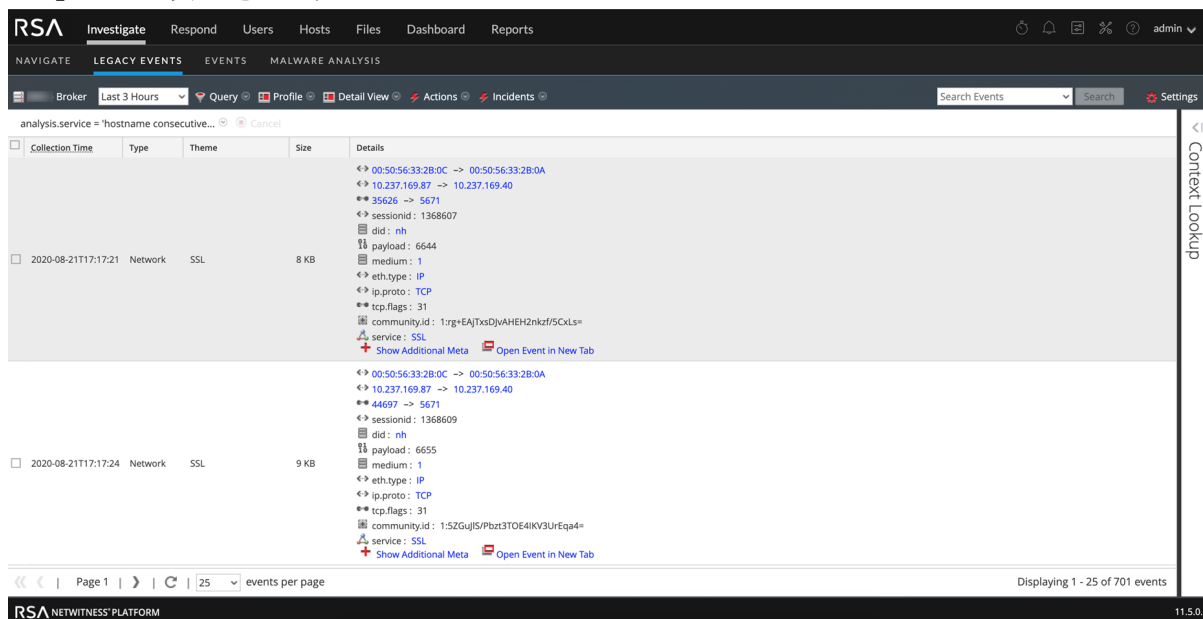
[レガシー イベント]ビューでイベントを表示するには、次のいずれかを実行します。

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(このオプションは、管理者がビューを有効にしている場合にのみ使用できます)。
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、**新しいタブで [レガシー イベント]を開く** をクリックします。

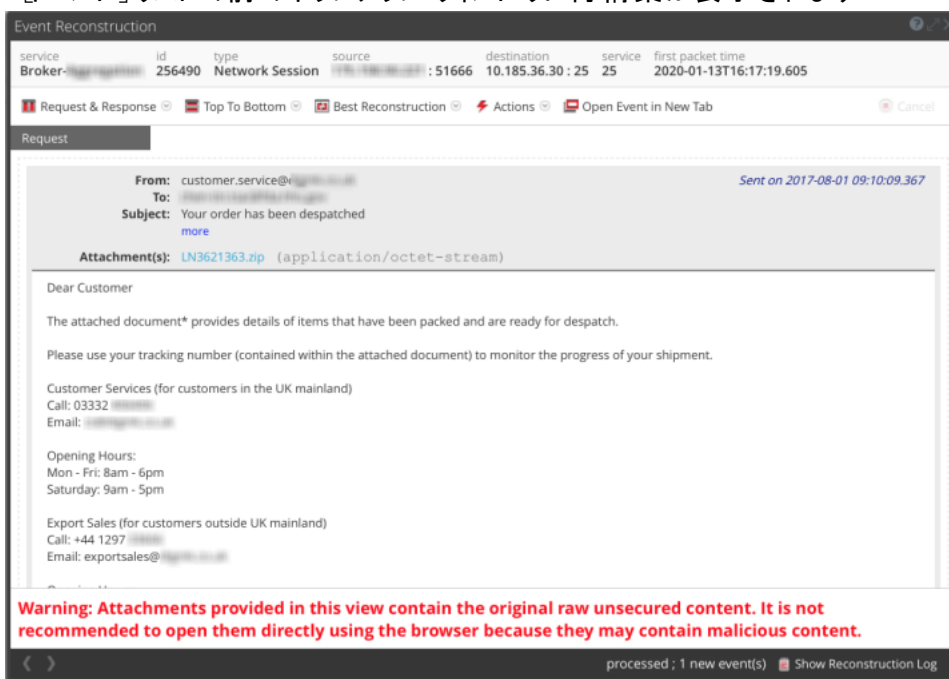
[レガシー イベント]ビューに、選択したメタ値のイベントが表示されます。[レガシー イベント]ビューには、詳細ビュー、リストビュー、ログビューという、標準提供の3種類の表示形式でイベントデータを表示できます。この図は詳細ビューの例です。[レガシー イベント]ビューに表示されるイベントをフィルタリングするには、クエリ、時間範囲設定、プロファイルを使用します。ファイルの抽出、イベントのエクスポート、ログのエクスポートを行うことができます。また、イベントをダブルクリックすると、**[イベントの再構築]**パネルが開きます。これらの機能の詳細については、「[結果のダウンロードと処理](#)」を参照してください。

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

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。



【イベント】ビューでのイベント詳細の調査

【ナビゲート】ビューまたは【イベント】ビュー > 【イベントの絞り込み】パネルで関心のあるセッションを見つけたら、【イベント】ビュー > 【イベント】パネルでセッションのシーケンシャルイベントのリストを確認できます。リスト内のイベントをクリックすると、そのイベントタイプに応じたネットワークイベントの詳細パネル（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）が開きます。【イベントの詳細】パネル内で、イベントの再構築（テキスト、パケット、ファイル、Eメール、およびWeb）を表示するタブを選択するか、（バージョン11.5以降）エンドポイントデータが付加されたネットワークイベントのホスト情報を表示するタブを選択できます。

注：（バージョン11.5以降）ネットワーク（パケット）導入環境内の既存のネットワークイベントのネットワーク可視性を拡張するため、ネットワークイベントには、エンドポイントデータ、つまりネットワークイベントをトリガーしたホストとプロセス、およびユーザ名、リスクスコア、レピュテーションなどの詳細が付加されています。

次の方法でエンドポイントデータを表示できます。

-（クイックビュー）**調査** > 【イベント】 - イベント サマリー ヘッダー

-（詳細ビュー）**調査** > 【イベント】 > **ホスト**

拡張ネットワーク可視性を有効にする方法の詳細については、『**エンドポイント構成ガイド**』の「グループとポリシーの作成」を参照してください。

注：拡張ネットワーク可視化を使用する場合は、Endpoint Log DecoderのデータをEndpoint Concentratorで集計するために使用するサービス ユーザー アカウントに、decoder.manage権限が割り当てられている必要があります。ロールと権限の割り当て方法の詳細については、『**システムセキュリティとユーザ管理ガイド**』の「ロールの追加と権限の割り当て」を参照してください。

各イベントタイプのイベントの詳細

次の表に示すように、【イベントの詳細】パネルでは、イベントタイプごとにさまざまなタブを使用できます。【イベントの詳細】パネルでの作業手順は、「[【イベント】ビューでのイベントの分析](#)」に記載されています。

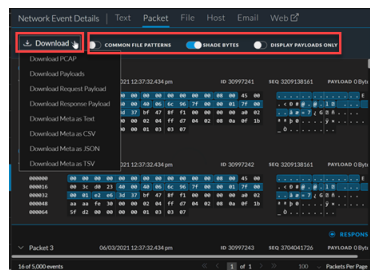
アクション	ネットワーク イベント	ログ イベント	エンドポイント イベント
テキストの再構成を表示します（最後に選択した内容でオーバーライドされない場合はデフォルト）	✓	✓	✓
ファイルの再構築を表示します	✓		
（バージョン11.5以降）拡張ネットワーク可視性で構成されたエンドポイントエージェントのホスト情報を表示します（「 ホスト情報 」を参照）。	✓		
パケットの再構築を表示します	✓		
Eメールの再構築を表示します	✓		
【レガシー イベント】ビューでWebの再構築を表示します（「 【レガシー イベント】ビューでのイベントの再構築 」を参照）	✓		

分析を強化するための設定が各タブにあります。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。

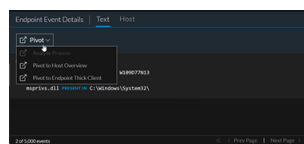
- 現在選択されている再構築 : テキスト、パケット、ファイル、(バージョン11.5以降) ホスト、Eメール。
- [イベント メタ] パネルの表示、非表示。
- [イベント] ヘッダーの表示、非表示。
- リクエスト、レスポンス、またはその両方の表示、非表示。
- パケットの再構築にパケット ペイロードをヘッダーなしで表示するかどうか。
- パケットの再構築でバイトを濃淡化するかどうか。
- パケットの再構築にその他の一般的なファイルタイプをハイライト表示するかどうか。
- パケットの再構築のページあたりのパケット数。
- テキストの再構築で圧縮したテキストと展開したテキストのどちらを表示するか。

テキストの再構築

11.7以降では、**調査**] > **イベント**] > **テキスト**] ビューの **ダウンロード**] ボタンにダウンロード形式を選択するドロップダウンがあり、アナリストはダウンロードするイベントのダウンロード形式を選択できます。また、**[パケット分析]** ページで使用可能な **[一般的なファイルパターン]**、**[バイトの濃淡化]**、および **[ペイロードのみ表示]** オプションは、使用可能な領域に基づいて画面上を移動するトグルボタンとして表示されます。



[エンドポイント イベントの詳細] の **テキスト分析]** ページで使用できる **移行]** オプションは、さらに調査を実行するための3つのオプションを含む **移行]** ドロップダウンメニューに置き換えられています。



テキスト] タブでは、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の再構築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。

Network Event Details

SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME	LAST PACKET TIME
789558	10.162.30.26 :51949	10.25.51.226 :50105	80	10/31/2016 08:02:44 pm	10/31/2016 08:02:56 pm
CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT			
5912 bytes	4856 bytes	16			

Showing 46%

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional/EN" "http://www.w3.org/TR/html4/loose.dtd"><html><head><style type="text/css">.forums {background: #919191;}body { margin: 0; padding: 10px; font-family: "Lucida Grande", Arial, sans-serif; font-size: small; background: #fbfbfb;}a { color: #77985c;}ul, ol { margin-top: 0em; margin-bottom: 0em; padding: 0 0 0 0; font-size: medium;}code { background: #eeeeee; border-left: 5px solid #666; margin: .2em .2em .2em 2em; padding: 0.5em 10px;}blockquote:before { color: #aaa; font-size: 4em; line-height: 0.1em; margin-right: 0.25em; vertical-align: -0.4em;}blockquote p { display: inline;}.mdTable table { position: relative; top: 0px; left: 0px; width: auto; border: 1px solid #000; background: #dddddd;}table { position: relative; top: 0px; left: 0px; width: 100%; border: 1px solid #000; background: #dddddd;}table caption { margin: 0; padding: 8px 20px; text-align: left; border: 1px solid #000; border-bottom: none; background: #fff;}table th { margin: 0; padding: 4px 4px; border-bottom: 2px solid #656565; color: blue;}table td { font-size: small; padding: 4px;}table .name { text-align: left;}table tr { background: #eeeeee;}table tr.alt { background: #fbfbfb;}table td a { display: block; font-weight: bold; text-decoration: none; } table td a:hover { text-decoration: underline;}</style><script type="text/javascript">function setValue(name, path) { var value = path; value += "?msg=set&value="; value += encodeURIComponent(documen
```

Event Meta

- SESSIONID: 789558
- TIME: 10/31/2016 08:02:44 pm
- SIZE: 5912
- DID: nh
- PAYLOAD: 4856
- MEDIUM: 1
- ETH.SRC: 00:90:FB:33:AB:C8
- ETH.DST: 00:50:56:98:08:62
- ETH.TYPE: 2048

Network Event Details

SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME	LAST PACKET TIME
1653	127.0.0.1 :43300	127.0.0.1 :36004	0	10/30/2020 07:22:05 am	10/30/2020 07:22:07 am
CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT			
34676 bytes	9926 bytes	375			

REQUEST

RESPONSE

REQUEST

RESPONSE

REQUEST

RESPONSE

Event Meta

- SESSIONID: 1653
- TIME: 10/30/2020 07:22:05 am
- SIZE: 53.80 KB
- DID: packethybrid
- PAYLOAD: 19852
- MEDIUM: 1
- ETH.SRC: 00:00:00:00:00:00
- ETH.DST: 00:00:00:00:00:00
- ETH.TYPE: 2048

注：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。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。

テキストの再構築では、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、テキストの再構築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] タブに表示されます。エンドポイント イベントには、エンドポイント イベントに関連する追加情報が含まれます。
- (バージョン11.5.1) RenderJSONオプションが有効になっている場合、JSONスニペットを含むログ イベントは、ネストされたインデントを持つ読みやすいJSONツリービューでレンダリングされます。

イベント ヘッダーと、イベントをダウンロードするオプションには、イベントのタイプ(ネットワーク、ログ、またはエンドポイント) ごとの違いがあります。以下は、各イベント タイプ(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) のテキストの再構成の例です。

Network Event Details | Text Packet File Host Email Web

Download PCAP ▼ DISPLAY COMPRESSED PAYLOADS

SESSION ID 789558	SOURCE IP:PORT 10.162.30.26 :61949	DESTINATION IP:PORT 10.25.51.226 :50105	SERVICE 80	FIRST PACKET TIME 10/31/2016 08:02:44 pm	LAST PACKET TIME 10/31/2016 08:02:56 pm
CALCULATED PACKET SIZE 5912 bytes	CALCULATED PAYLOAD SIZE 4856 bytes	CALCULATED PACKET COUNT 16			

Showing 46%

```

HTTP/1.1 200 OK
Content-Length: 1958
Connection: Keep-Alive
Content-Encoding: gzip
Pragma: no-cache
Expires: -1
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><head><style type="text/css">.forums {background: #919191;}body { margin: 0; padding:
10px; font-family: "Lucida Grande", Arial, sans-serif; font-size: small; background: #fbfbfb;}a
{ color: #77985c;}ul, ol { margin-top: 0em; margin-bottom: 0em;}h1, h2, h3, h4, h5, h6 { margin-top:
    
```

Event Meta

Sequence >

SESSIONID
789558

TIME
10/31/2016 08:02:44 pm

SIZE
5912

DID
nh

PAYLOAD
4856

MEDIUM

Network Event Details | Text Packet File Host Email Web

Download PCAP ▼ DISPLAY COMPRESSED PAYLOADS

SESSION ID 2460	SOURCE IP:PORT 103.66.103 :49520	DESTINATION IP:PORT 184.51.144.120 :80	SERVICE 80	FIRST PACKET TIME 11/06/2015 10:26:35 pm	LAST PACKET TIME 11/06/2015 10:26:45 pm
CALCULATED PACKET SIZE 47945 bytes	CALCULATED PAYLOAD SIZE 44669 bytes	CALCULATED PACKET COUNT 58			

Showing < 1%

```

GET /js/picad_4802.js?r=2411396 HTTP/1.1
Host: assets.picadmedia.com
Connection: keep-alive
Accept: /*/*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.111
Safari/537.36
content-language: en
Referer: http://3point5oz.com/
Accept-Encoding: gzip,deflate
Accept-Language: en-us,en;q=0.8
    
```

Event Meta

Sequence > HIDE DUPLICATE ENTRIES

Filter meta keys

SESSIONID
2460

TIME
11/06/2015 10:26:35 pm

SIZE
46.82 KB

DID
packethybrid

PAYLOAD
44669

MEDIUM
1

ETH.SRC
00:24:E8:2D:90:81

ETH.DST

2,460 of 5,000 events

Prev Page | Next Page

Log Event Details | [Text](#) 📄 🗑️ 🔍 ✕

[Download Log as Text](#) ▾

SESSION ID	DEVICE IP	DEVICE TYPE	DEVICE CLASS	EVENT CATEGORY	COLLECTION TIME
209	127.0.0.1	airdefense	Wireless Devices	Attacks.Access.Interception	07/16/2020 10:22:56 pm

EVENT TIME
06/17/2009 04:06:00 pm

RAW LOG

```
<4> Jun 17 16:06:25 Time=2009-06-17T16:06:00,Category=Exploits,CriticalityLevel=Critical,Desc=ASLeap Attack,device=00:a0:f8:c5:3e:ab(Symbol:c5:3e:ab[b,g]),sensor=00:15:70:a3:58:F4(ST03174Sensor1[a,b,g])
```

Event Meta ✕

[Sequence >](#)

- SESSIONID: 209
- TIME: 07/16/2020 10:22:56 pm
- SIZE: 243
- DID: lh
- DEVICE.IP: 127.0.0.1
- PAYLOAD.REQ: 203
- ANALYSIS.SESSION: session size 0-5k
- INV.CATEGORY: operations
- INV.CONTEXT: event analysis
- INV.CONTEXT: event analysis

209 of 5,000 events ⏪ < 1 > ⏩

Log Event Details | [Text](#) 📄 🗑️ 🔍 ✕

[Download Log as Text](#) ▾ RENDER JSON

SESSION ID	DEVICE TYPE	DEVICE CLASS	EVENT CATEGORY	COLLECTION TIME	EVENT TIME
1	rsacat	Anti Virus	Other.Default	10/19/2020 09:11:19 am	03/08/2016 09:14:54 am

RENDERED LOG

```
Mar 12 09:44:54 ECAT-SERVER CEF:0|RSA|RSA|ECAT|4.0.0.28535|SuspiciousEventIOC|EcatAlert|1|agentId=ceceff83-9134-a105-0fd2-9be4db69b17 shost=INSMITH src=176.119.147.225 smac=00:50:56:45:12:34 fname=explorer.exe fsize=23562 f10Hash=8d769c63427a8ce407d17946702c7626 InstantIOName=RSA-PoisonIvyIOC InstantIOLevel=0 rt=03/08/2016 09:14:54 machineScore=1001 gatewayip=10.10.10.1 remoteip=10.10.10.10 os=Microsoft Windows 7 Enterprise timeZone=Universal Coordinated Time
```

Event Meta ✕

[Sequence >](#) HIDE DUPLICATE ENTRIES

Filter meta keys

- SESSIONID: 1
- TIME: 10/19/2020 09:11:19 am
- SIZE: 484 B
- DID: logdecoder
- MEDIUM: 32
- DEVICE.TYPE: rsacat
- HEADER.ID: 0010
- DEVICE.CLASS: Anti Virus
- ALIAS.HOST: [REDACTED]

1 of 5,000 events ⏪ < Prev Page | Next Page >

Endpoint Event Details | Text Host

Pivot to Endpoint Thick Client | Analyze Process | Pivot to Host Overview

SESSION ID	HOST NAME	PROCESS	USER NAME	NWE CATEGORY	COLLECTION TIME
3881628	INENBOSEJL3C	chrome.exe	bosej	Network Event	08/24/2020 12:28:52 pm

EVENT TIME: 08/24/2020 12:28:15 pm
NETWORK REMOTE ADDRESS: :443

NETWORK EVENT

08/24/2020 12:28:15 pm INENBOSEJL3C CORP\bosej

chrome.exe MADE A NETWORK CONNECTION TO [REDACTED] RESOLVING TO learningstudio. [REDACTED] FROM 10.91.46.123

LARGE META VALUES

```
param.src=chrome.exe --type=utility --utility-sub-type=network.mojom.NetworkService
--field-trial-handle=1488,3449324784461010832,10241472198844175243,131072 --lang=en-US
--service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1828 /prefetch:8
```

1 of 5,000 events

Event Meta

Sequence >

SESSIONID	3881628
TIME	08/24/2020 12:28:52 pm
SIZE	321
DID	eps1
FORWARD_IP	127.0.0.1

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。

パケットの再構築

パケットの再構築はネットワーク 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]タブの見出しには、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。

ファイルの再構築

ファイルの再構築では、選択されたネットワークイベントに関連づけられたファイルのリストが表示されます。以下は、ファイルの再構築の例です。

The screenshot shows the 'File' tab of the 'Network Event Details' window. It includes a 'Download File' button and a table of reconstructed files. The table has columns for 'FILE NAME', 'MIME TYPE', 'FILE SIZE', and 'HASHES'. One file is listed: '961285-107-0.raw' with a size of 40 bytes and three hash values (SHA1, SHA256, MD5).

SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME	LAST PACKET TIME
961285	10.237.169.3 :59042	:1947	0	08/04/2020 10:07:19 pm	08/04/2020 10:07:19 pm
CALCULATED PACKET SIZE		CALCULATED PAYLOAD SIZE		CALCULATED PACKET COUNT	
82 bytes		40 bytes		1	

	FILE NAME	MIME TYPE	FILE SIZE	HASHES
<input type="checkbox"/>	961285-107-0.raw	application/octet-stream	40 bytes	SHA1: 7d9d79e415bbce59f9f70979f52de22a12a508c SHA256: e51bf0ef7fb15839eaf8547809055b9bd4b5d9dfca9022dae654f1f06c MD5: 8b05fe98a6e0baf6cc47caa8376841a6

6 of 5,000 events

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。ファイルを選択したら、[ファイルのダウンロード]オプショ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。

Network Event Details | Text Packet **File** Host Email Web ↗

Download File

SESSION ID 961285	SOURCE IP:PORT 10.237.169.3 :59042	DESTINATION IP:PORT :1947	SERVICE 0	FIRST PACKET TIME 08/04/2020 10:07:19 pm	LAST PACKET TIME 08/04/2020 10:07:19 pm
CALCULATED PACKET SIZE 82 bytes	CALCULATED PAYLOAD SIZE 40 bytes	CALCULATED PACKET COUNT 1			

Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data. To avoid quarantine, the zip file is password protected with this password: netwitness.

FILE NAME	MIME TYPE	FILE SIZE	HASHES
<input checked="" type="checkbox"/> 961285-107-0.raw	application/octet-stream	40 bytes	SHA1: 7d9d79e415bbcb59f970979f52de22a12a508c SHA256: e51bf0ef7fb15839eaf8547809055b9bd4b5d9dfca9022dae654f1f06d. MD5: 8b05fe98a6e0baf6cc47caa8376841a6

6 of 5,000 events

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。

ホスト情報

ネットワークおよびエンドポイント イベントのホスト情報が、エンドポイント データとともに表示されます。


[イベントの絞り込み] パネル (バージョン11.5以降) を使用して、[イベント] ビューでイベントをフィルタ処理できます。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。

注：エンドポイント データが表示されるのは、Endpointが導入されており、Endpointエージェントに拡張ネットワーク可視化が構成されている場合だけです。ポリシーで拡張ネットワーク可視化を有効にする方法の詳細については、『 [エンドポイント構成ガイド](#) 』の「グループとポリシーの作成」を参照してください。

注：拡張ネットワーク可視化を使用する場合は、Endpoint Log DecoderのデータをEndpoint Concentratorで集計するために使用するサービス ユーザー アカウントに、decoder.manage権限が割り当てられている必要があります。ロールと権限の割り当て方法の詳細については、『 [システム セキュリティとユーザ管理ガイド](#) 』の「ロールの追加と権限の割り当て」を参照してください。

以下は、ホスト情報の例です。

- イベント サマリー ヘッダーには、エンドポイント データからの次の情報が含まれています。
 - ホスト名 - イベントの発生元ホスト。
 - プロセス - イベントをトリガーしたソース プロセス。
 - ユーザー - トリガーされたプロセスに関連づけられているユーザー。
- 最も一致するプロセスを持つホストがイベント時間の順にリストされます。
- デフォルトで最初のホストが展開され、次のような追加情報を確認できます。
 - ホストの詳細 - ホストのオペレーティング システムと、ホストに関連づけられている管理責任者 (ログインしているユーザー) の詳細が表示されます。

- ホスト名を調査するには、青色で強調表示されている **ホスト名** リンクをクリックします。詳細については、『*NetWitness Endpoint ユーザーガイド*』の「ホストの調査」を参照してください。
- ユーザーに関連づけられているアラートを調査するには、青色で強調表示されている **管理責任者** リンクをクリックします。詳細については、『*NetWitness UEBA ユーザーガイド*』の「ハイリスクエンティティの調査」を参照してください。
- プロセスの詳細 – リスクスコア、プロセス名、レピュテーション、イベント時間、オンホスト、署名済みステータス、プロセスID、署名者、ユーザー、起動の引数、SHA256、パスなどの詳細が表示されます。
 -  をクリックしてプロセスツリーを開きます。デフォルトでは、プロセスツリーによって過去14日間のプロセスの詳細が開かれます。プロセスツリーが使用不可の場合、プロセスツリーを開くためのアイコンは表示されません。
 - プロセスを調査するには、青色で強調表示されている **プロセス** リンクをクリックします。詳細については、『*NetWitness Endpoint ユーザーガイド*』の「ファイルの調査」を参照してください。
 - ユーザーに関連づけられているアラートを調査するには、青色で強調表示されている **ユーザー** リンクをクリックします。詳細については、『*NetWitness UEBA ユーザーガイド*』の「ハイリスクエンティティの調査」を参照してください。
- アラートの詳細 – ホストに関連づけられている最近の10個のアラートが表示されます。これらのアラートは、エンドポイント、ネットワーク、およびログイベントからのものです。ホストの詳細ページを開くには、**すべて表示** をクリックします。ホストの詳細ページには、リスクスコアに寄与するすべてのアラートが一覧表示されます。アラート名をクリックして、アラートの詳細を開くことができます。アラートを確認する方法については、『*NetWitness Respond ユーザーガイド*』の「アラートの確認」を参照してください。このセクションには次の詳細が表示されます。
 - 重大度 – アラートの重大度が表示されます。
 - 時刻 – アラートがトリガーされた日付と時刻。
 - イベント数 – アラートをトリガーしたイベントの数が表示されます。アラートに関連づけられているイベントを表示するには、青色で強調表示されている **イベント数** リンクをクリックします。**イベント数** リンクは、イベントが同じソースからのものである場合にのみ使用できます。
 - インシデント – 各アラートに関連づけられているインシデントが一覧表示されます。詳細を表示してインシデントに対応するには、青色で強調表示されている **インシデント** リンクをクリックします。詳細については、『*NetWitness Respond ユーザーガイド*』の「インシデントへの対応」を参照してください。

ホスト名、プロセス、ユーザー、管理責任者、SHA256のメタ値にカーソルを合わせると、特定のメタデータに関する追加情報を表示できます。コンテキストルックアップの詳細については、「[結果の追加のコンテキストを検索](#)」を参照してください。

以下は、選択したネットワークイベントに関連づけられている単一のホスト、プロセス、およびユーザーが表示された [ホスト情報] タブの例です。svch0st.exeは、ホスト INENJOHNAJI3Cとログインユーザー johnaに関連づけられたプロセスです。

The screenshot shows the NetWitness Investigate interface. The main content area displays a list of 2,198 events. The selected event is expanded to show details for host INENJOHNAJI3C. The process details section shows the process name svch0st.exe, user johna, and event time 06/04/2020 10:01:26 am. The event meta section shows session ID 57003, time 06/04/2020 10:20:27 am, size 7952, and payload 1904.

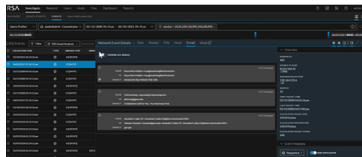
注：選択したネットワークイベントに対して複数のホストとプロセスがトリガーされる場合があります。このような場合、最初にイベントのトリガー元になったホストが最初にリストされ、次に同様のイベントがトリガーされた他のホストがリストされます。

たとえば、10.63.0.240というIPアドレスがHost1に割り当てられ、User1がマシンにログインし、Chromeを使用してwww.nyu.edu/にアクセスしているとします。その間、Host1の電源はオフになり(30分以内)、同じIPアドレスがHost2に割り当てられます。ログインしているユーザーはUser2で、Internet Explorerを使用してwww.nyu.edu/にアクセスしています。この場合、エンドポイントデータのネットワークイベントは次のとおりです。

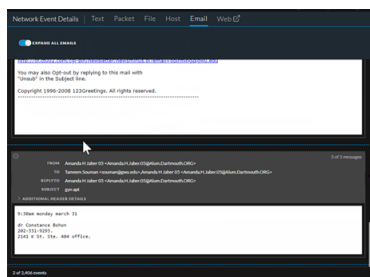
- ホスト名 - Host1、Host2
- プロセス - chrome.exe、iexplore.exe
- ユーザー - User1、User2

メールの再構築

11.7以降では、すべてのメールの内容を単一のセッションで確認する必要がある場合、アナリストは [調査] > [イベント] > [メール] ビューに移動して [すべてのメールを展開] トグル ボタンをクリックできます。

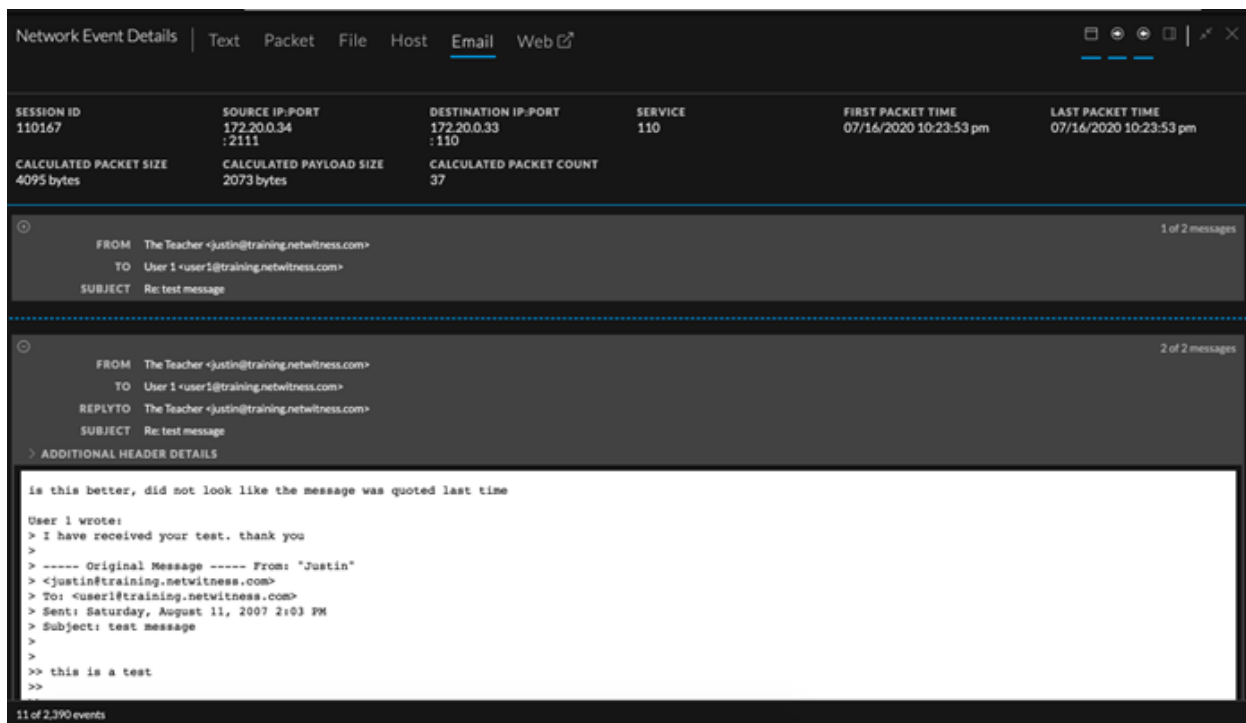


[すべてのメールを展開] トグル ボタンをオンにすると、メールの内容が展開された形式で表示されます。



「すべてのメールを展開」トグル ボタンをオフにすると、メールの内容が折りたたまれた形式で表示されます。表示するメールがない場合、トグル ボタンは無効になります。

メールの再構築では、選択されたネットワーク イベントに関連づけられたEメールのリストが表示されます。以下は、Eメールの再構築の例です。



- 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。
- Eメールに添付ファイルが含まれている場合は、「[\[イベント\]ビューでのデータのダウンロード](#)」の説明に従って添付ファイルをダウンロードできます。
- **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のalias.hostメタデータでサポートされているWebメールがイベントに含まれている場合、[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。

「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」ビューという名前に変更され、「レガシーイベント」ビューに代わって、イベント分析のデフォルトビューとなりました。11.4より前の「イベント」ビュー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。

「イベント」ビューでクエリーが送信された後に「イベント」パネルが開いてシーケンシャルイベントのリストが表示されます。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。

- 送信されたクエリーと一致している。
- 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ーが再送信されます。サービス、時間範囲、フィルターに対する未送信クエリーの変更は無視されます。

結果のロードとソートの方法

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、この制限を構成できます。「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。」

リストの一番上には、ロードされたイベントの合計数、イベント数が上限の5,000に達したかどうか、有効になっているソート方法を示すメッセージが表示されます。

- リストに表示されるイベントが5,000件未満の場合のメッセージは、"xx,xxxイベント"です。
- リストに表示されるイベントが5,000件を超える場合のメッセージは、"最も古い10,000イベント(昇順)"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]ダイアログで [デフォルトのイベントソート順]を [降順]に変更します。

リストのソート方法は [イベント環境設定]ダイアログで構成されます(「[\[イベント\]ビューの構成](#)」を参照)。設定の変更は、次のクエリ送信時に有効になります。[イベント環境設定]ダイアログの [デフォルトのイベントソート順]は、データベースに保存されており、ログアウトして再度ログインした後も維持されています。

- **ソートしない**(バージョン11.4.1のデフォルト) :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、処理が高速になります。これは、一致するイベントが見つかったら即座に表示するのと、すべてのコア サービスの応答を待ってから指定された順に結果を並べ替えて表示する違いによるものです。
- **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先頭に表示します。ほとんどの調査には、最も古い収集時間が適しています。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」に変更する必要があることがあります。
- **降順** :収集時間が最も新しいイベントをリストの先頭に表示します。多くの場合、最も新しい収集時間は、ログの調査に役立ちます。

イベント リストを絞り込むためのアクション

結果が [イベント]パネルにロードされたら、次のアクションを実行して結果を絞り込むことができます。

- イベントをソートする列を選択します(「[イベント リストでの列と列グループの使用](#)」)。
- 特定のタイプの調査に役立つメタ キーのセット(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](#)」)。
- クエリ プロファイルを適用します(「[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](#)」)。
- (バージョン11.5)メタデータを調査してイベントをフィルタリングします(「[\[イベント\]ビューでのメタデータのドリルダウン\(ベータ版\)](#)」)。

イベントを分析するためのアクション

このセクションの残りの部分では、[イベント]ビューで作業し、再構成を調整して、興味深いデータに重点を置く手順を説明します。



- 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]パネルでイベントをクリックすると、[イベントの詳細]パネルが開いて、イベントの再構築(テキスト、パケット、ファイル、電子メール、Web)を示すタブ、またはエンドポイントデータが付加されたネットワークイベントのホスト情報を示すタブ(バージョン11.5)が表示されます。
- [イベント]パネルと[イベントの詳細]パネルは同時に開くことができます。
- [パケット]タブと[テキスト]タブでは、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。

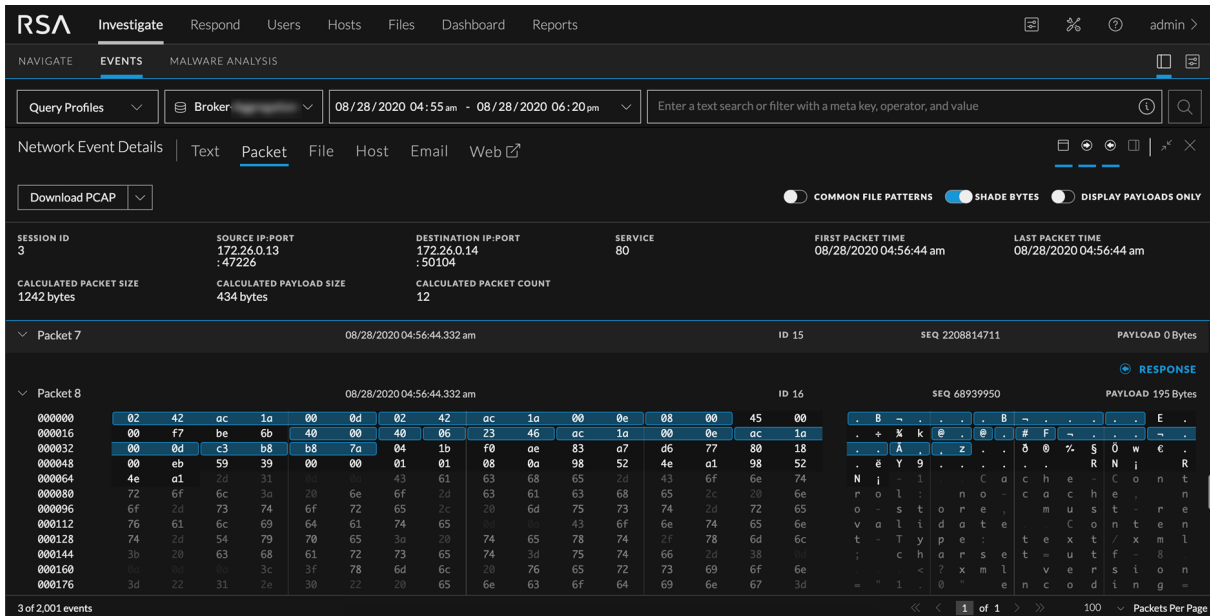
一方のパネルを拡大したり、縮小したり、閉じることにより、詳細パネルに対する[イベント]パネルのサイズの比率を調整し、読みやすさを改善することができます。閉じたパネルは、再度開くことができます。選択した比率は、その比率を変更するか、ブラウザを更新するまで維持されます。

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. どちらかのパネルを閉じて、もう一方の開いているパネルを最大幅で表示するには、をクリックします。

次の図は、ブラウザー ウィンドウの最大幅で再構築を表示した例です。



The screenshot shows the NetWitness Investigate interface. At the top, there are navigation tabs: Investigate, Respond, Users, Hosts, Files, Dashboard, Reports. Below that, there are filters for Query Profiles, Broker, and a time range of 08/28/2020 04:55 am - 08/28/2020 06:20 pm. The main area is divided into 'Network Event Details' and 'Packet' tabs. The 'Packet' tab is active, showing details for Packet 7 and Packet 8. Packet 8 is expanded to show hex and ASCII data. The hex data is: 000000 02 42 ac 1a 00 0d 02 42 ac 1a 00 0e 08 00 45 00. The ASCII data is: . B B E .

3. [イベント]パネルを閉じた後で再び開くには、[イベント]ビューの右上隅にあるをクリックします。前回閉じたときの状態(25%~75%または50%~50%)で[イベント]パネルが表示されます。
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、[イベントの詳細]パネルでイベントが開いた状態で選択するには、[テキスト]、[ファイル]、[ホスト]、[パケット]、[Eメール]、[Web]のいずれかのタブをクリックします。

- ホストを選択した場合は、拡張エンドポイント データからのホスト情報が表示されます。
- ファイル、テキスト、パケット、または [Eメール]を選択した場合は、再構成が表示されます。
- [Web]を選択した場合は、新しいタブで、単一のイベントの再構築が開かれます。これは、[レガシーイベント]ビューで使用されるセッションの再構築と同じものです。(「[レガシーイベント\]ビューでのイベントの再構築](#)」を参照)。


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

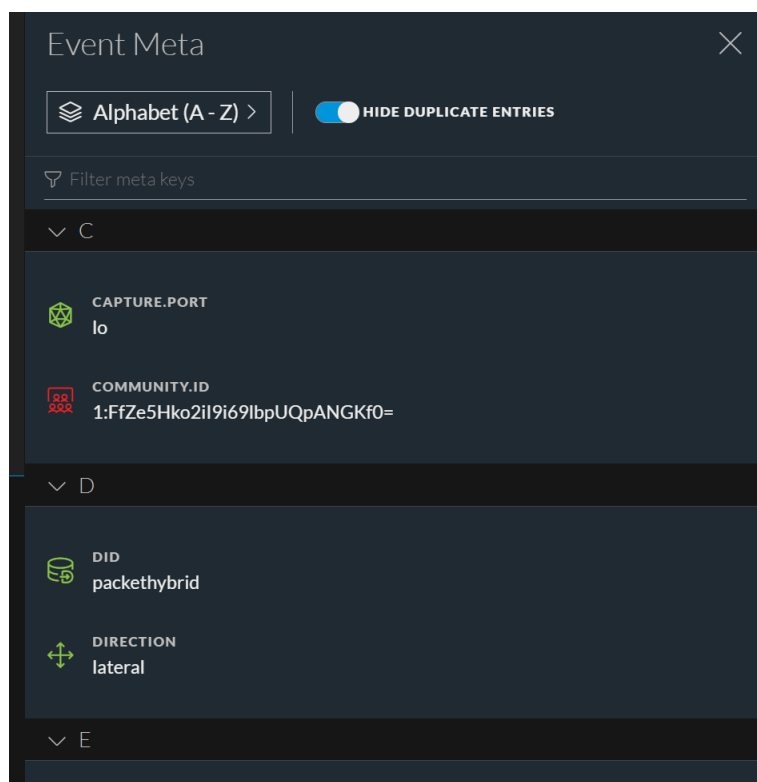
リクエストとレスポンスがある分析タイプの場合は、会話のどちら側(リクエスト、レスポンス、または両方)を表示するかを選択できます。方向アイコンのいずれかまたは両方をクリックします。選択した情報で、再構築されたイベントが更新されます。

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。

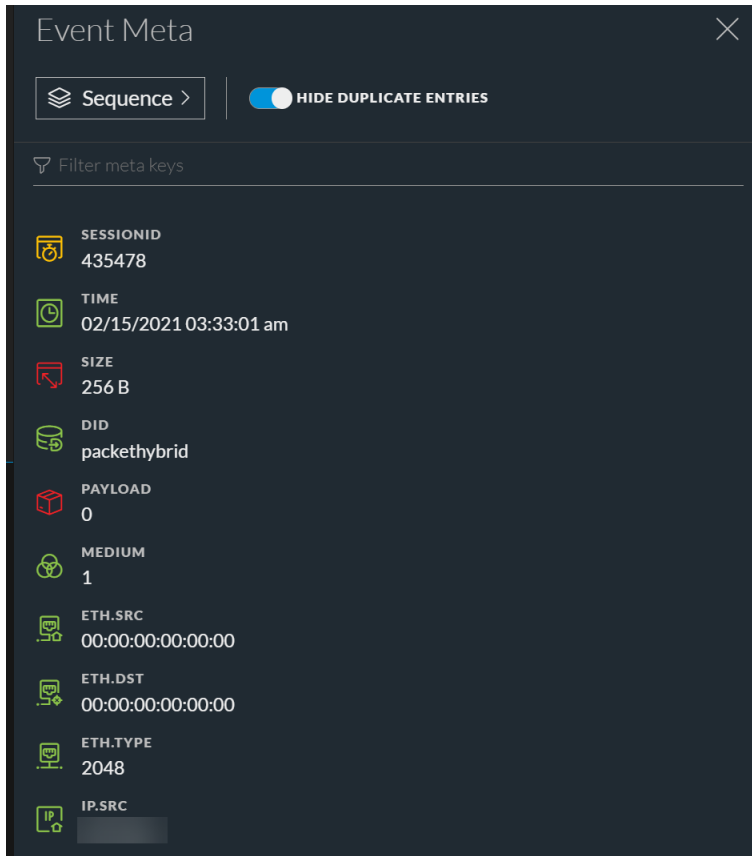
イベントの関連メタデータを表示する

テキスト]タブ、[パケット]タブ、[ファイル]タブのイベントを調べるときは、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することができます。[イベント メタ]パネル内のリストに表示されたメタデータは、表示順を変更して、探しているものを見つけやすることができます。メタデータは、生成された順序で整理することも、メタキーのアルファベット順に整理することもできます。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。

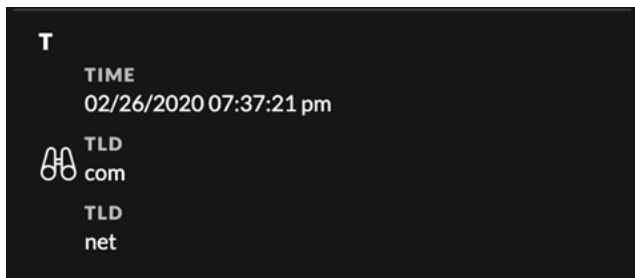
[イベント メタ]パネル内のリストに表示されたメタデータは、表示順を変更して、探しているものを見つけやすことができます。メタデータは、生成された順序で整理することも、メタキーのアルファベット順に整理することもできます。次の図は、メタキーのアルファベット順で並べたメタデータを示しています。



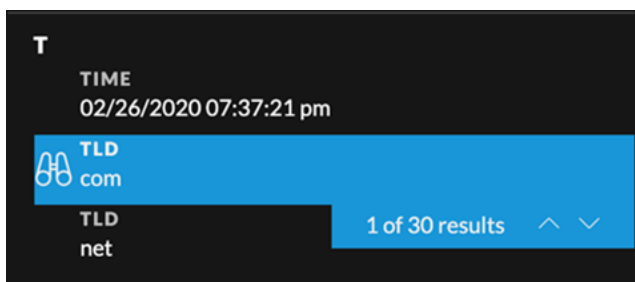
次の図は、生成された順に並べられた、同じメタデータを示しています。



テキスト再構成と [イベント メタ] パネルを表示しているときに、メタ キー/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できる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] タブでメタ キー/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。

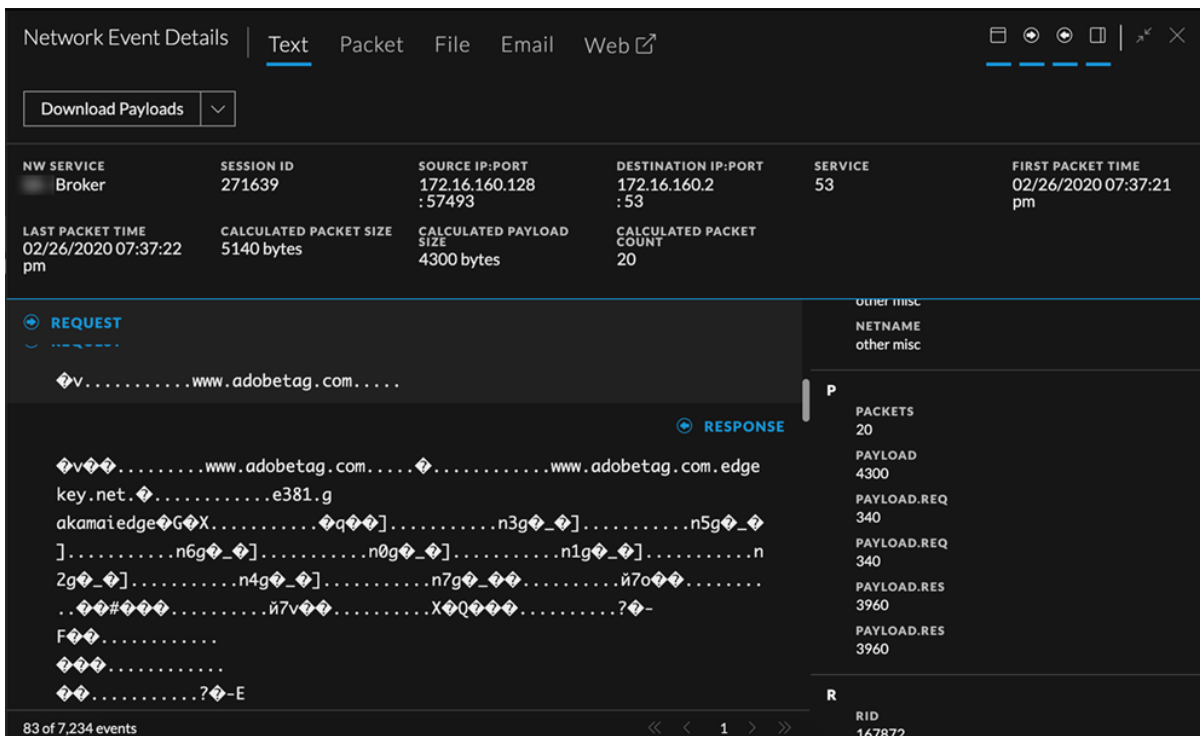


[イベント メタ] パネルには、ハイライト表示された行に結果の件数が示され、上下矢印が表示されます。この矢印を使用して、[テキスト] タブでそれぞれの結果にすばやく移動することができます。スクロールボタンを使用すると、メタ キーの生成をトリガーしたデータがハイライト表示された場所を、1つずつ前に、または1つずつ後ろに移動して表示することができます。

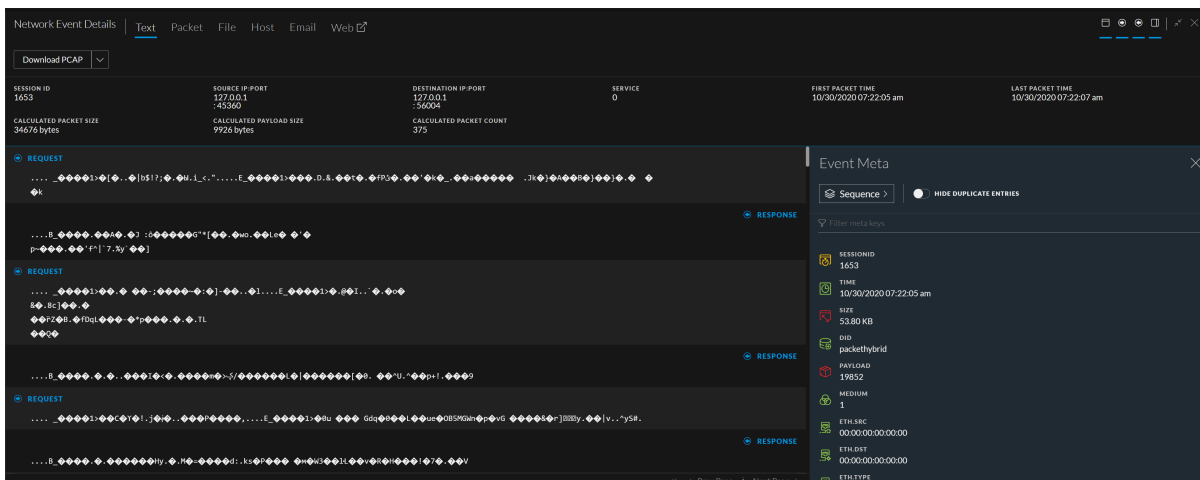
RAWテキスト内に関連する値が存在するメタ キーのみを検索できます。一度に検索できるメタ キーは1つだけです。3000文字を超えるためトランケート表示されたテキスト エントリーは、検出されたメタ値が見えるよう展開して表示されます。

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] タブでネットワーク 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。



11.6のイメージ



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] タブでは何もハイライト表示されません。
 関連する値が1つ以上、[テキスト] タブで見つかった場合は、各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。

The screenshot shows the 'Network Event Details' window with the 'Text' tab selected. The event details table is as follows:


NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
Broker	271639	172.16.160.128 :57493	172.16.160.2 :53	53	02/26/2020 07:37:21 pm
LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT		
02/26/2020 07:37:22 pm	5140 bytes	4300 bytes	20		

Below the table, the 'REQUEST' and 'RESPONSE' sections are visible. The 'REQUEST' section shows a search for 'www.adobetag.com'. The 'RESPONSE' section shows a list of search results, including 'www.adobetag.com.edge', 'key.net', and 'akamaiedge'. The 'EVENT METADATA' panel on the right shows 'TLD com' and 'TLD net' with a search result count of '1 of 30 results'.



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] タブ、[テキスト] タブ、[ファイル] タブでイベント 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。

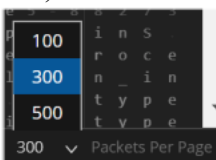
【パケット】および【テキスト】タブでのイベントのページ移動





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】タブでは、1ページあたりの表示パケット数を選択できます。選択内容は、NetWitness Platformアプリケーションにログインするたびに維持されています。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】タブで使用できます。【テキスト】タブでは、最後のページまで手動で移動した後に、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かれた状態で、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、ページあたりのパケット数をドロップダウンメニューで選択し直します。



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。

「テキスト」タブ内のトランケートされたテキスト エントリーの展開

「テキスト」タブでのネットワーク 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ます。重要で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。時間を節約するために、6,000文字を超えるテキスト エントリーはトランケートされ、最初の2,000文字のみが表示されます。次の図は、2,000文字を超えるエントリーの例で、ヘッダーのメッセージが、総文字数の何%が表示されているかを示しています。

The screenshot shows the NetWitness Investigate interface. The main panel displays network event details for a session ID 1653. The text is truncated with diamond symbols. An 'Event Meta' panel is open on the right, showing details for the selected event: SESSIONID 1653, TIME 10/30/2020 07:22:05 am, SIZE 53.80 KB, DID packethybrid, PAYLOAD 19859, MEDIUM 1, ETH SRC 00:00:00:00:00:00, ETH DST 00:00:00:00:00:00, and ETH TYPE 7058. The interface also shows search filters and navigation options.

全体の46%(最初の2,000文字)が表示されていることが分かります。**残り54%を表示**をクリックすると、エントリーの残りを表示することができます。

「テキスト」タブ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は、トランケートされたテキストが検索対象になります。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。

URLとBase64のエンコーディングおよびデコーディングの「テキスト」タブでの実行

「テキスト」タブ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、セッションを理解しやすく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。

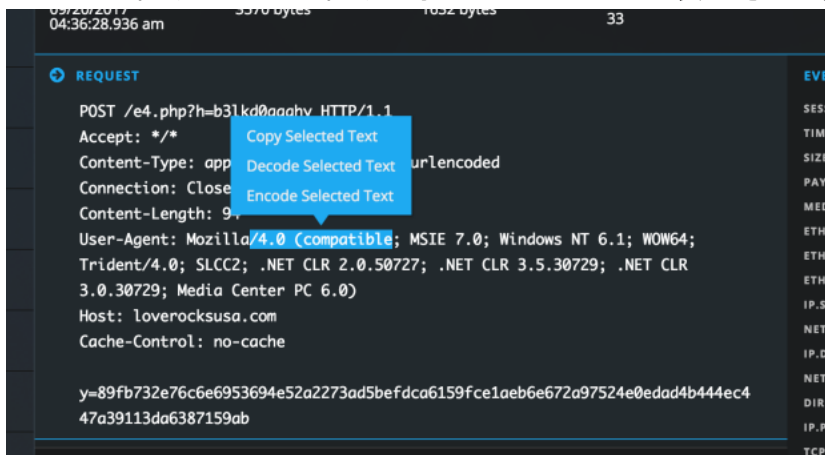
「テキスト」パネルでエンコードされたテキストが含まれるネットワーク セッションを表示しているときに、1つのリクエストまたはレスポンス内のテキストの一部を選択して、エンコードまたはデコードした形式で表示することができます。Decoderにロードされたコンテンツによっては、セッション内にBase64かURLでエンコードされたデータがあることを示す追加のメタデータが含まれることがあります。

「テキスト」タブでエンコーディングおよびデコーディングを実行するには、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再構築を表示します。

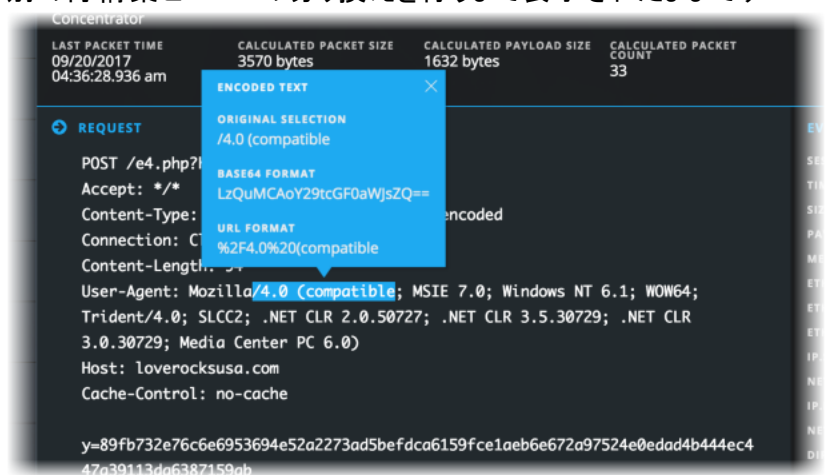
- デコードされたテキストを、エンコードされた形式で表示するには、1つのリクエストまたはレスポンス内でテキストをドラッグして選択します。

エンコーディングとデコーディングのオプションのメニューが表示されます。



- 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、のクリック、**[テキスト]**タブ内の別のテキストの選択、**[イベント]**パネルの終了、再構築する別のイベントの選択、または別の再構築ビューへの切り換えを行うまで表示されたままです。




長いテキストを選択すると、ポップアップが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がすべて収まる大きさになります。

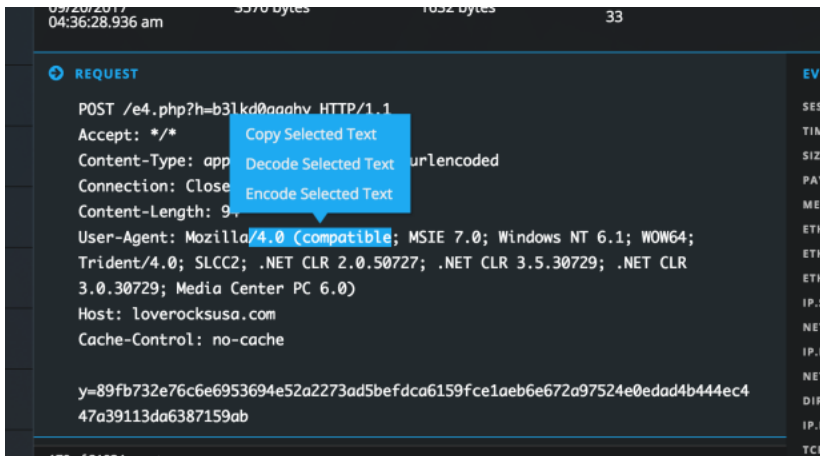
- セッションに含まれるエンコードされたテキストを、デコードされた形式で表示する場合は、1つのリクエストまたはレスポンス内でテキストをドラッグして選択します。


エンコーディングとデコーディングのオプションのメニューが表示されます。

- 選択したテキストをデコード]**をクリックします。

デコードされたテキストがポップアップで表示されます。このポップアップは、のクリック、**[テキスト]**タブ内の別のテキストの選択、**[イベント]**パネルの終了、再構築する別のイベントの選択、または**[イベントの詳細]**パネルの別のタブへの切り換えを行うまで表示されたままです。

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. いずれかのテキストをドラッグして選択し、右クリックします。次に、ポップアップメニューで **選択したテキストをコピー** を選択します。



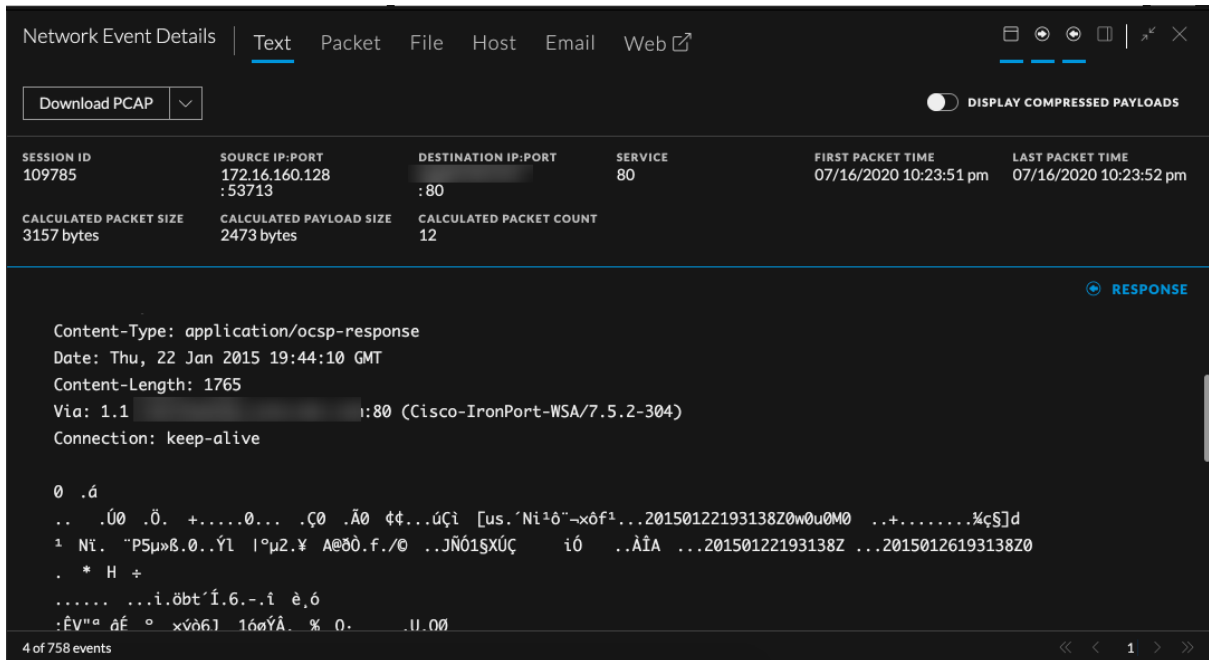
- b. テキストの一部をドラッグし選択し、 **Decode Selected Text** または **Encode Selected Text** のいずれかを選択します。目的のテキストを選択し、Ctrl + Cキーを押します。選択したテキストがクリップボードにコピーされ、クエリにペーストできるようになります。
7. 操作が終了したら、 をクリックしてポップアップを閉じます。

HTTPネットワークセッションの解凍テキストの [テキスト] タブでの表示

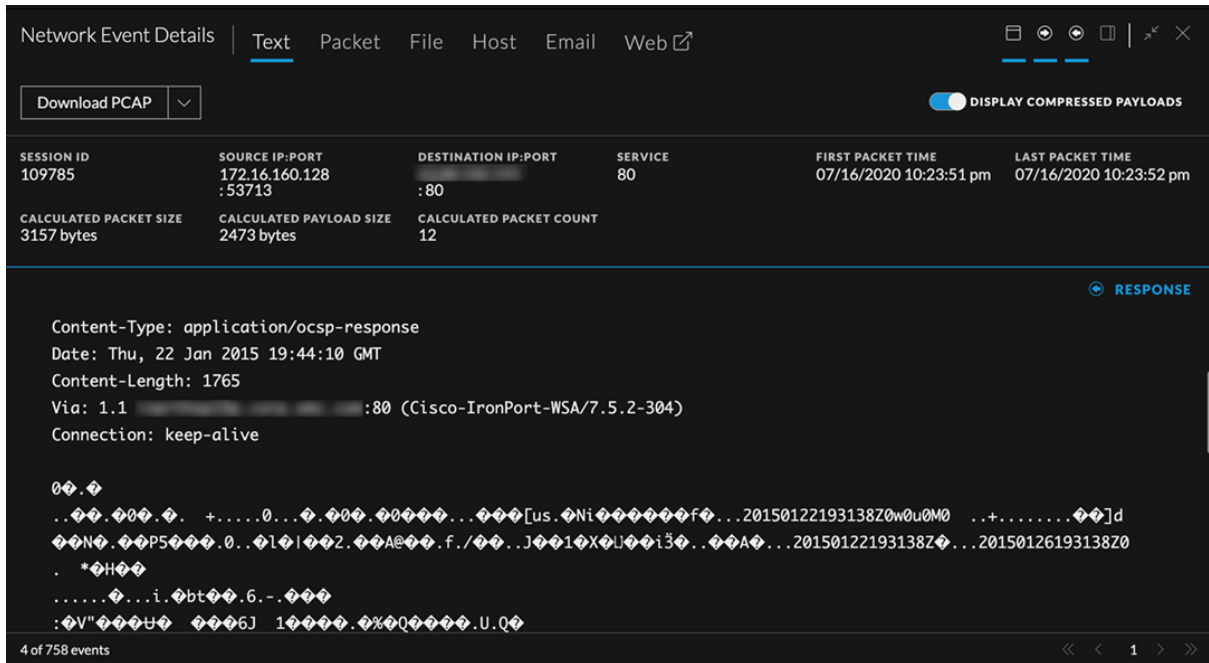
HTTPネットワークセッションのコンテンツが圧縮されている場合、NetWitnessでは、デフォルトで解凍されたコンテンツが [テキスト] タブに表示されます。これにより、任意のパターンがあるか判断し、読み取り可能な文字を表示することができます。圧縮されたテキストを圧縮表示するか解凍表示するかを切り替えることができます。

圧縮表示と解凍表示の切り替えスイッチは、[テキスト] タブのみに表示され、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] タブを開きます。デフォルトでは、解凍されたテキストでセッションが再構築され、**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判読不能になり、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。

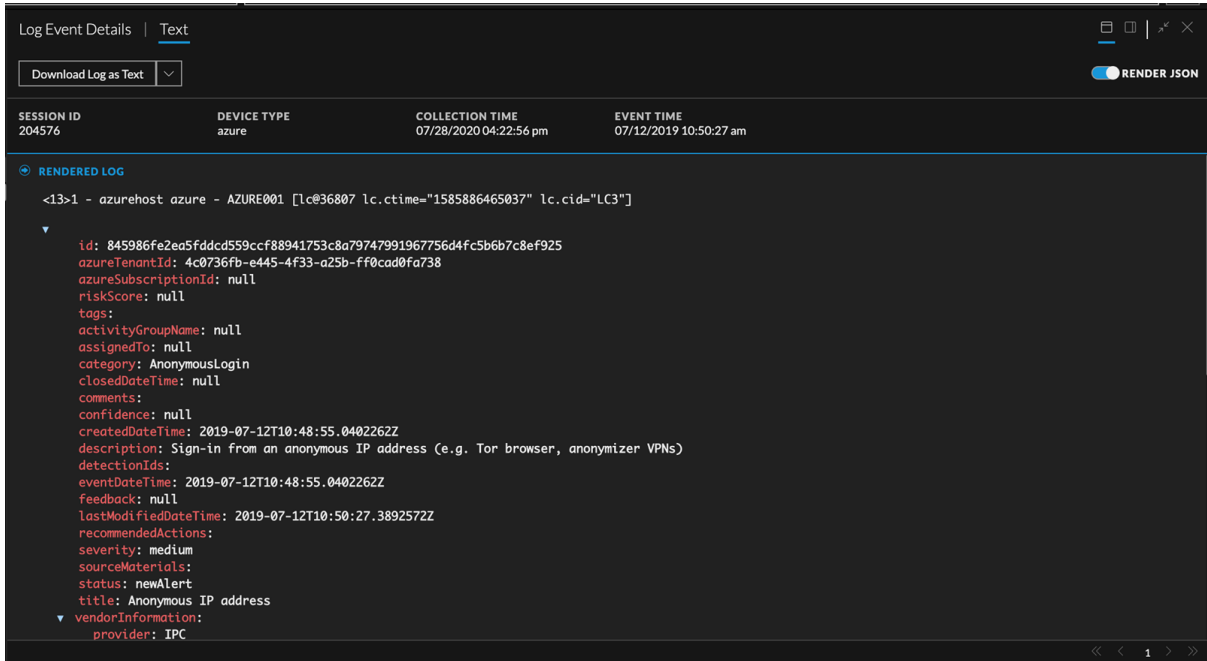


3. 解凍されたテキストの表示に戻すには、スイッチを再度クリックします。

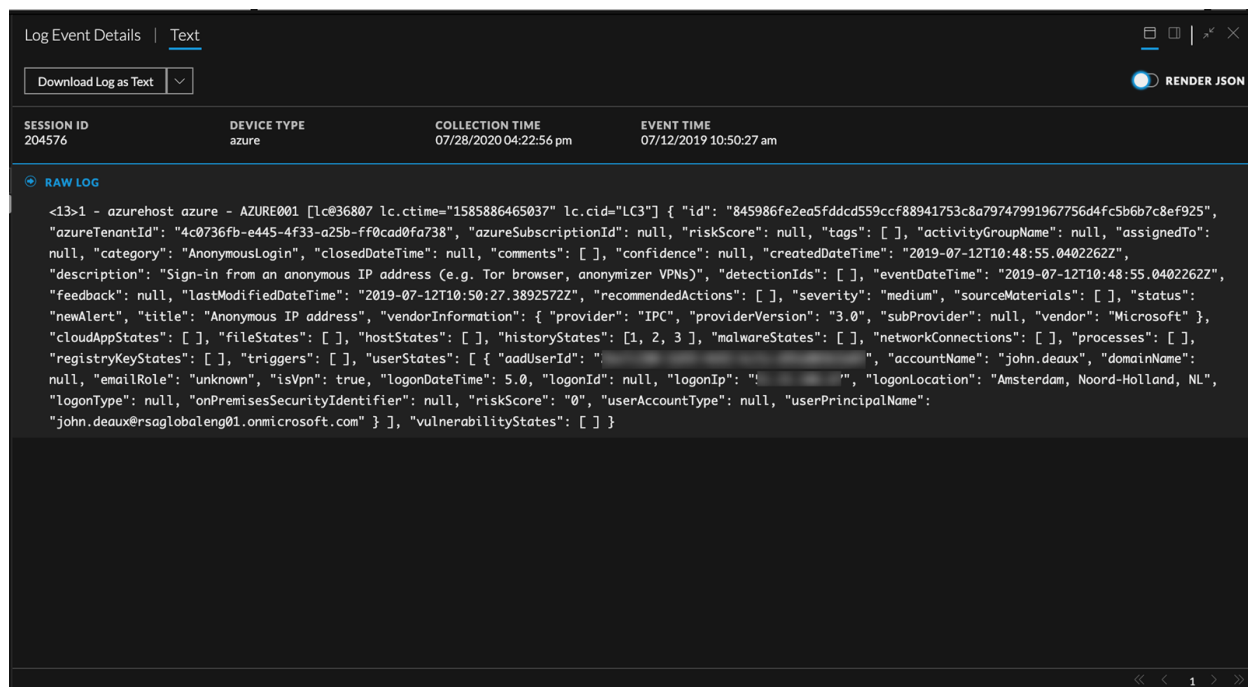
ツリー形式のJSON文字列の [テキスト] タブでの表示 (バージョン11.5.1)

【JSONの表示】切り替えスイッチを使用すると、未フォーマットのブロック形式ではなく、読みやすいJSON形式で、ログ イベントのテキスト再構成を表示できます。デフォルトでは、スイッチが有効になっており、ログ イベントのJSONスニペットが検出され、完全に展開されたツリー形式で表示されます。無効なJSONスニペットはRAWテキストとして表示されます。スイッチの設定を変更した場合でも、設定はローカルストレージに保持されています。

1. 【イベント】ビューの [テキスト] タブでログ イベントを開きます。
RAWログにJSON文字列が含まれており、【JSONの表示】スイッチが有効になっている場合は、見つかったすべてのJSON文字列がツリー形式で表示されます。



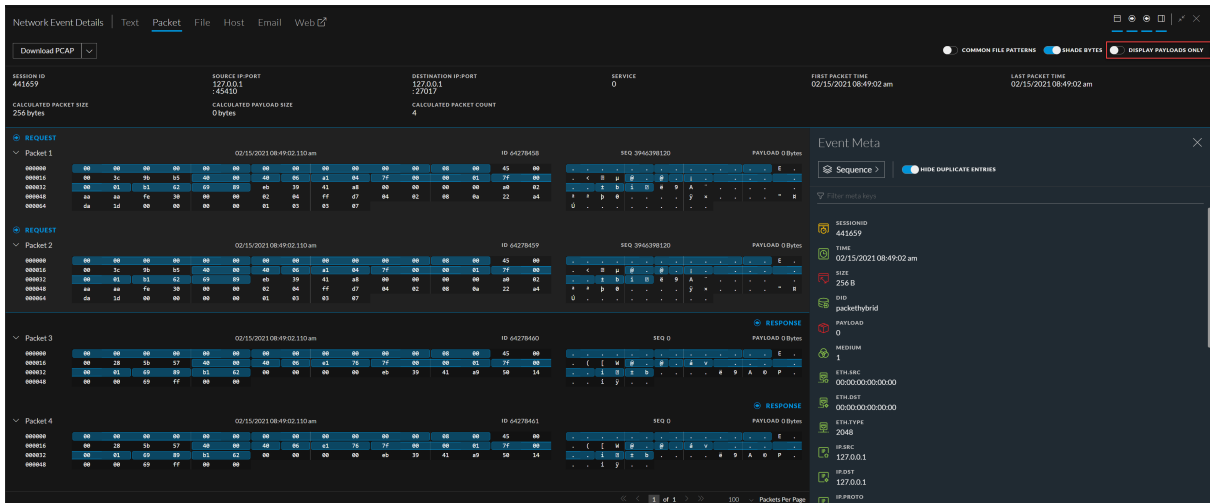
2. ログをRAWテキストとして表示する場合は、【JSONの表示】スイッチをクリックします。
ログは、ネストされたインデントのない単一のテキスト ブロックとして表示されます。設定は、変更されるまでは保持され、次のログイン時も、同じ状態です。



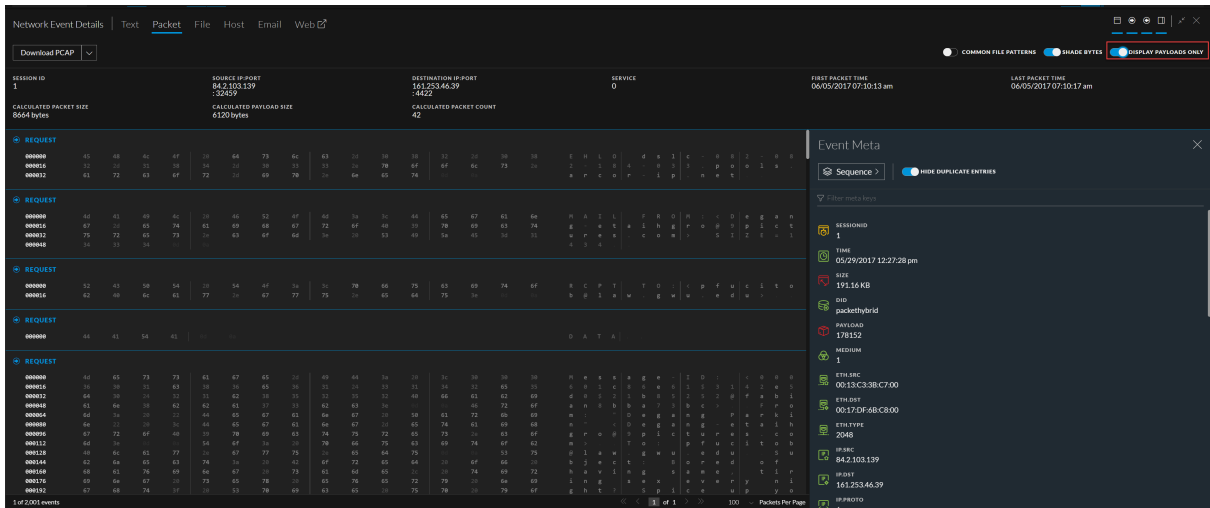
【ペイロードのみ】オプションの【パケット】タブでの使用

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に、ヘッダーバイトとフッターバイトを非表示にすることができます。ペイロードのみがビューに表示されるようになり、同じサイドの隣接パケットが連結されてペイロードが読みやすく、理解しやすくなります。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】タブに移動します。
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。



- 各パケットのペイロードのみが表示されるようにビューを変更するには、「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。ビューが変更されてペイロードのみが表示されます。



「パケット」タブでのバイトのハイライト表示

「パケット」タブで再構築を開くと、各パケットの重要なヘッダーバイトが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、ペイロードバイトが濃淡化で区別されています。次の図は、ハイライト表示とバイトの濃淡化を使用したパケット再構成のデフォルトの外観を示しています。

Network Event Details | Text Packet File Host Email Web ↗

Download PCAP ▾

COMMON FILE PATTERNS SHADE BYTES DISPLAY PAYLOADS ONLY

SESSION ID 10	SOURCE IP:PORT :16173	DESTINATION IP:PORT :25	SERVICE 25	FIRST PACKET TIME 08/28/2020 04:56:55 am	LAST PACKET TIME 08/28/2020 04:56:55 am
CALCULATED PACKET SIZE 245631 bytes	CALCULATED PAYLOAD SIZE 230199 bytes	CALCULATED PACKET COUNT 268			

REQUEST

Packet 54 08/28/2020 04:56:55.255 am ID 125 SEQ 1554890621 PAYLOAD 1460 Bytes

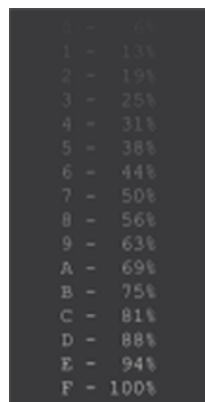
REQUEST

Packet 55 08/28/2020 04:56:55.255 am ID 126 SEQ 1554892081 PAYLOAD 1460 Bytes

000000	00 13 c3 3b c7 00 00 13 c3 3b be 00 08 00 45 00	. . Å ; Ç . . Å ; % . . . E .
000016	05 dc 3d a9 40 00 3f 06 67 35 a1 fd 98 78 d1 55	. Û = 0 @ . ? . g 5 i ý x Ñ U
000032	85 72 3f 2d 00 19 5c ad c5 31 d6 53 37 e7 50 10	r ? - . . \ A 1 0 S 7 ç P .
000048	44 70 cc 4d 00 00 41 49 51 41 42 67 51 45	D p Ì M . . A I Q A B g Q E
000064	42 41 55 45 42 67 6b 47 42 51 59 4a	B A U E B g U F B g k G B Q Y J
000080	43 77 67 47 44 41 77 4d 44 41 6f 4b 43 77 6f 4b	C w g G B g g L D A o K C w o K
000096	44 42 41 4d 44 41 77 4d 44 41 77 51 44 41 34 50	D B A M D A w M D A w Q D A 4 P
000112	45 41 38 4f 44 42 4d 54 46 42 51 54 45 78 77 62	E A 8 0 D B M T F B Q T E x w b
000128	47 78 73 63 45 48 42 77 63 4e 44 41 30 59 45 42	G x s c H x 8 f H x 8 f H x
000144	38 66 48 77 45 48 42 77 63 4e 44 41 30 59 45 42	8 f H w E H B w c N D A 0 Y E B
000160	41 59 47 68 55 52 46 52 6f 66 48 78 38 66 48 78	A Y G h U R F R o f H x 8 f H x
000176	38 66 48 78 38 66 48 78 38 66 48 78 38 66 48 78	8 f H x 8 f H x 8 f H x 8 f H x

10 of 2,001 events << < 1 of 3 > >> 100 Packets Per Page

「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。



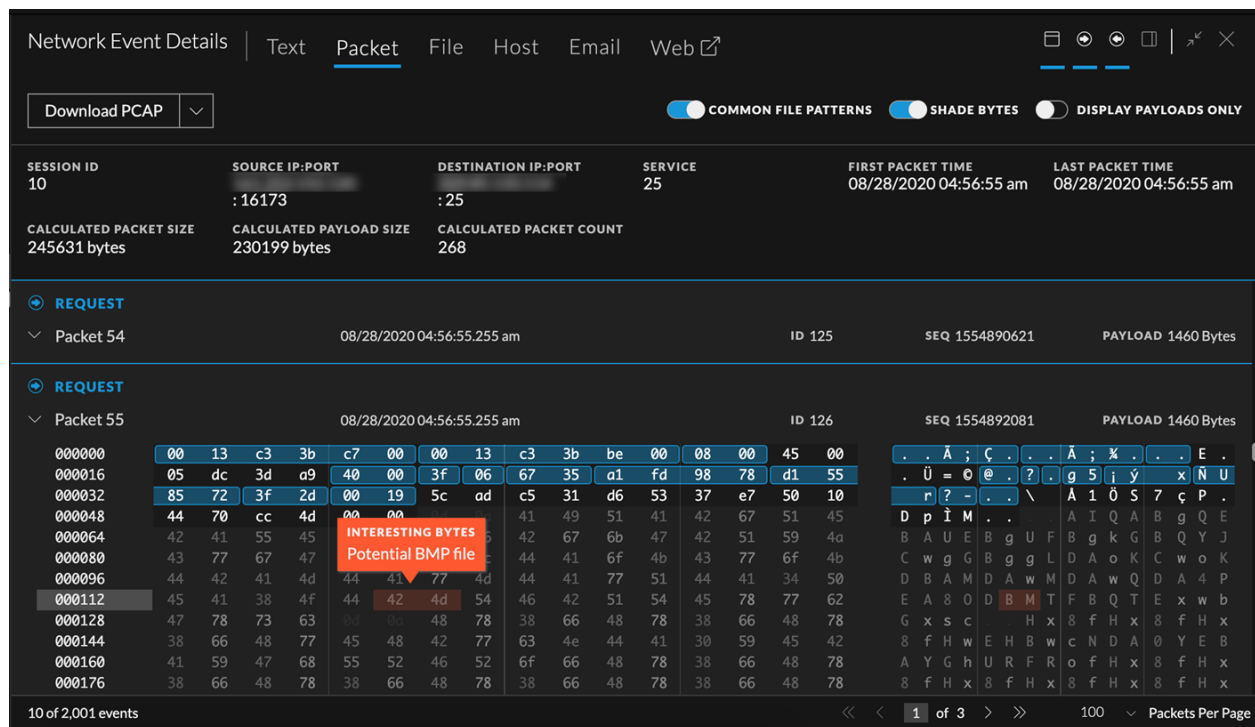
「バイトの濃淡化」スイッチは、バイトの濃淡化を制御します。「バイトの濃淡化」をオンまたはオフに設定すると、設定を変更するか、ブラウザを更新するまでその設定が保持されます。

一般的なファイルタイプの [パケット] タブでのハイライト表示

[パケット] タブでアナリストは、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、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、42 4dが16進数のペイロードでハイライト表示され、BM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。

一般的なファイルシグネチャを [パケット] タブに表示するには、次の手順を実行します。

- [パケット] タブで再構築を開いた状態で [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。
- 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。



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

ファイルタイプ	16進数のシグネチャ	ASCIIエンコード
JPEG/JFIF	4A 46 49 46	JFIF
JPEG/Exif	45 78 69 66	Exif
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	Đİ.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	Êp°¾
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

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、IMI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、[プロフィール] > [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。

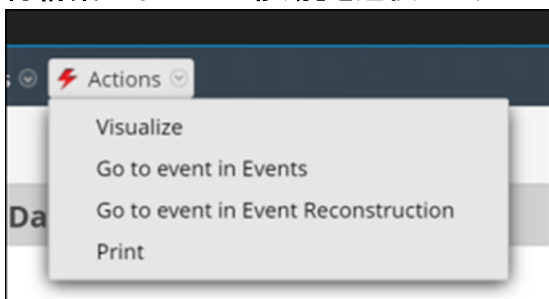
注：Investigationのアプリケーション パフォーマンスは、管理者が、[再構築の設定]と [再構築キャッシュの設定]で管理できます(『システム構成ガイド』で説明しています)。アナリストがセッションを再構築する場合、パフォーマンスと表示結果に影響を与える要素が2つあります。サイズが大きいイベントでは、ソース パケットが膨大な数に上ることがあります。それらのセッションを再構築すると、アプリケーションのパフォーマンスが低下する可能性があります。再構築キャッシュの表示内容が不正確である場合があります。このような理由から、1日以上経過したキャッシュは、24時間おきにNetWitnessによって消去されます。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

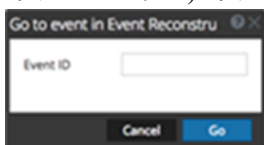
イベントIDがわかっている場合に、イベントを [ナビゲート]ビューから直接再構築できます。このオプションを使用すると、調査の開始時に通常必要となる、クエリの実行は必要ありません。eventidだけを使用してイベントに直接移動できるようにするには、サービスと時間範囲を選択する必要があります。

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。

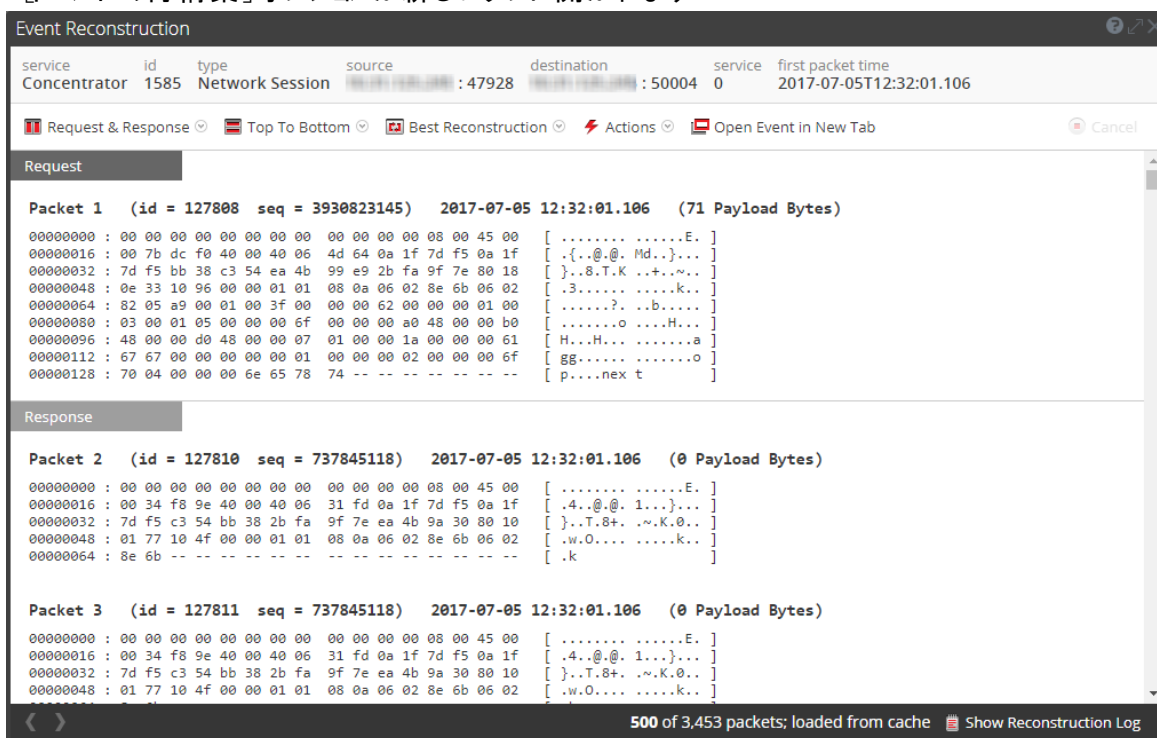
[ナビゲート]ビューでのドリルダウン ポイントからのイベントの再構築

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

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 [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から、イベントに表示する情報を選択します。[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] を選択できます。選択した情報で再構築の表示が更新されます。

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から、イベントに表示する情報を選択します。[リクエストとレスポンス]、[リクエスト]、[レスポンス] のいずれかを選択できます。選択した情報で再構築の表示が更新されます。

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を選択します。**メタ、テキスト、16進数、パケット、Web、メール、ファイル**のいずれかを選択できます。
再構築の表示が選択した再構築タイプで更新されます。

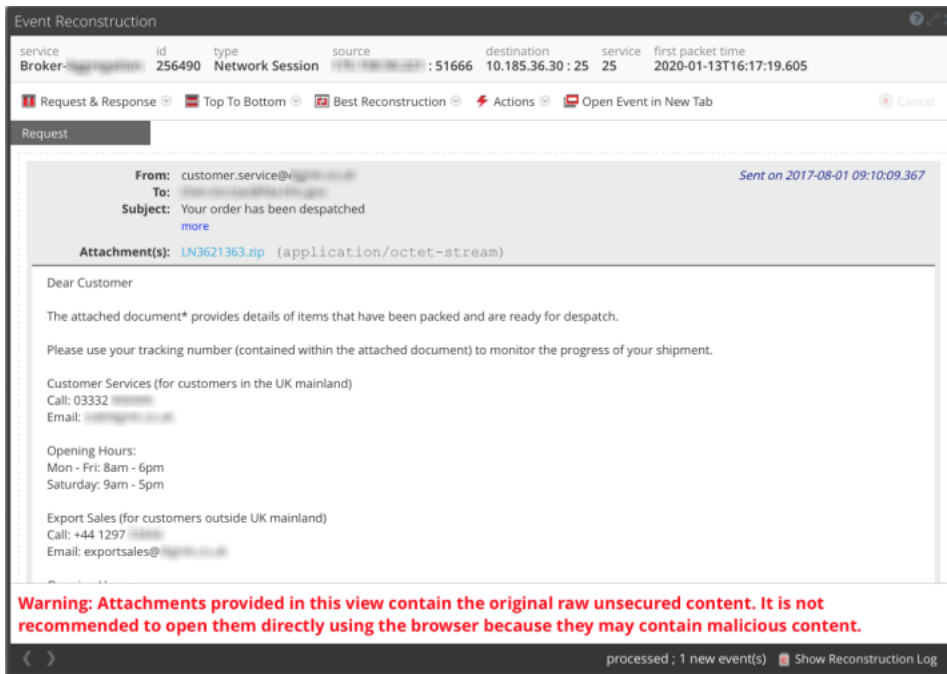
メールの添付ファイルの表示またはダウンロード

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 **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ドリルダウンポイントをPCAPファイルに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。PCAPI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、何が起きているのかを理解するために役立ちます。バージョン11.5以降では、コンテキスト ルックアップを使用してSTIXデータソースを追加し、関連データを表示できます。関連する要素は、IPアドレス、ファイル名、ファイルハッシュ、ドメイン名、およびURLです。

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。

バージョン11.6以降では、コンテキスト ルックアップを使用してREST APIデータソースを追加し、関連データを表示できます。また、管理者は、調査中にコンテキストを強調表示するために、特定のContext Hubソース(たとえば、特定のリスト、応答、エンドポイントなど)を構成できるようになりました。Context Hubソースのコンテキスト強調表示が無効になっている場合、アナリストはメタ値のコンテキストパネルを開いたときにすべてのデータソースからの結果を表示しますが、値は [調査]ビューで強調表示されません。ビュー コンテキストで次の処理が行われます。

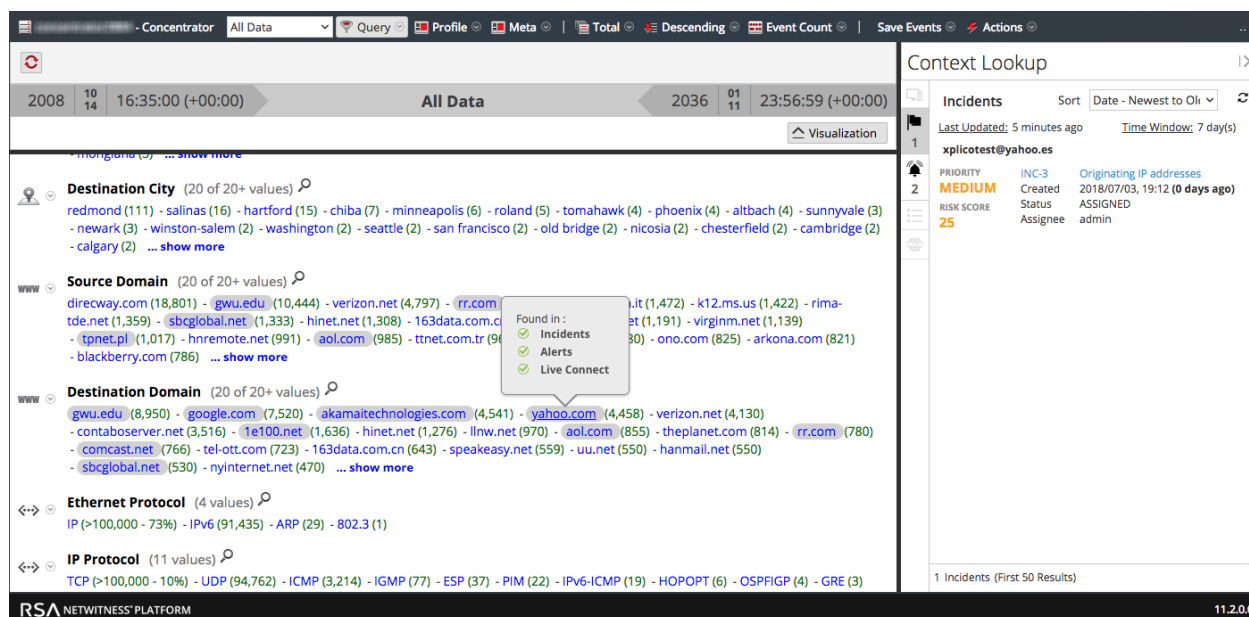
- メタ値が強調表示されていない場合、データは表示されません。

- 異なるデータソースに共通のエンティティがある場合、それらのエンティティのメタ値はすべてのデータソースで下線付きで表示されますが、データはコンテキストの強調表示が有効になっているデータソースに対してのみ表示されます。

「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。

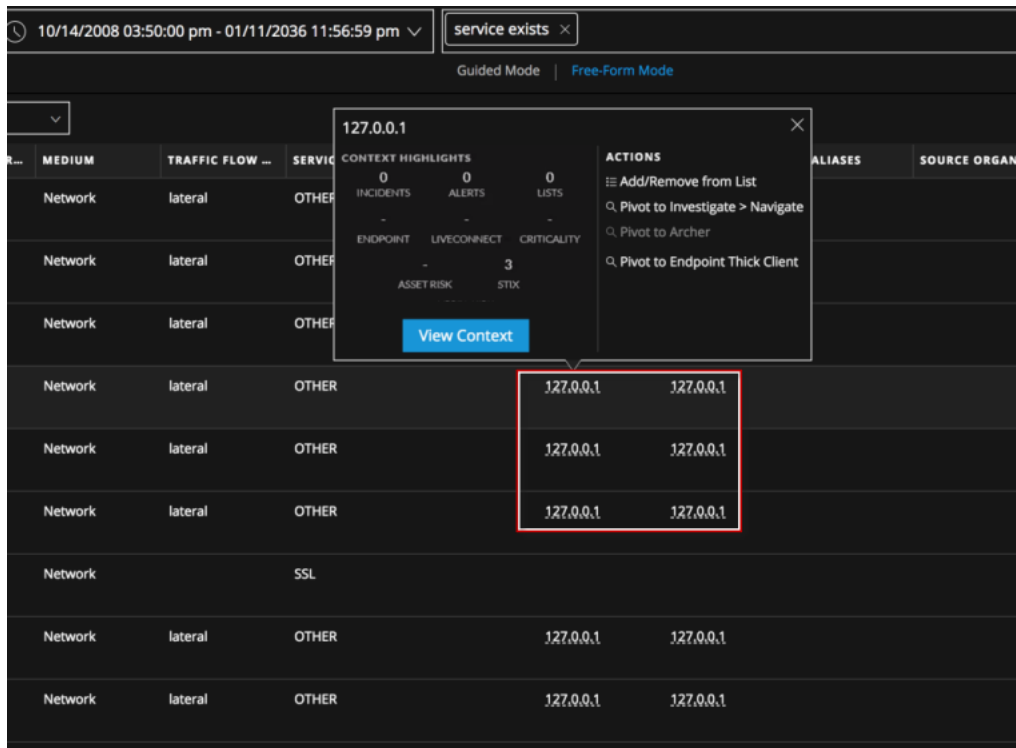


「イベント」ビューでは、下線付きエンティティが「イベント」パネル、イベント ヘッダー、「イベント メタ」パネルに表示されます。エンティティに下線がある場合、NetWitnessがContext Hubにそのエンティティタイプに関する情報を追加していることを意味します。つまり、Context Hubに、そのエンティティに関する追加情報が存在する可能性があります。

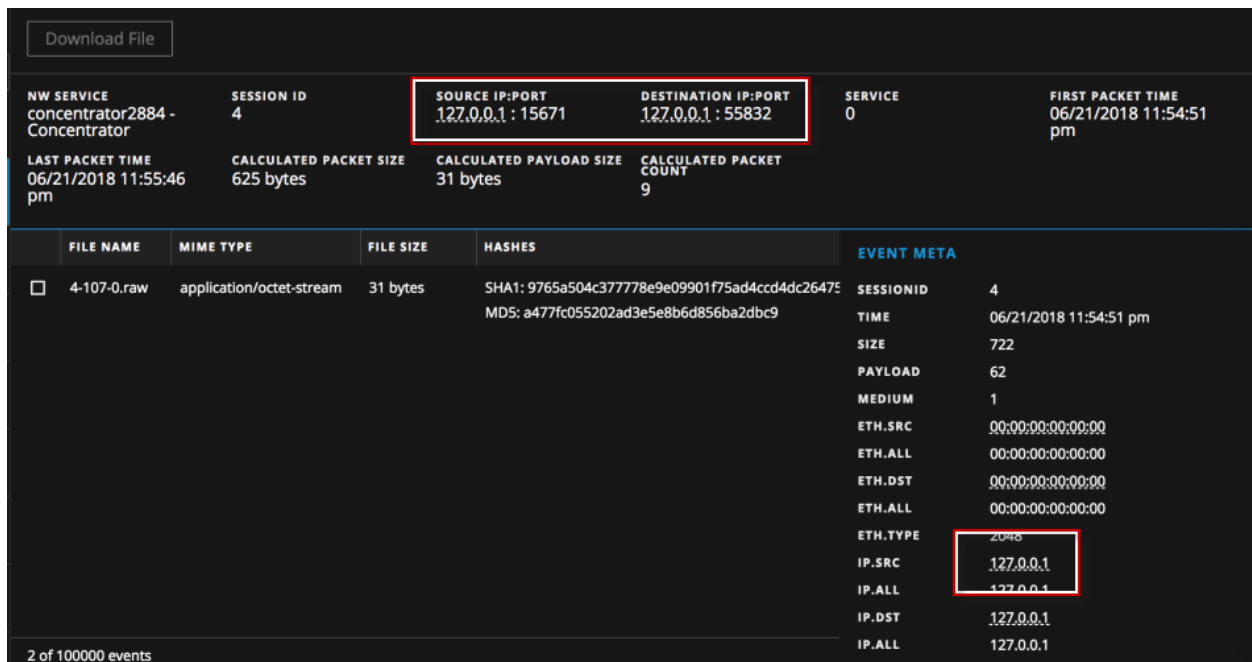
次の図は、コンテキスト ツールチップを開いた「イベント」パネルの下線付きエンティティを示しています。コンテキスト ツールチップには、2つのセクションがあります。「コンテキストのハイライト」と「アクション」です。

- 「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、STIX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。

The screenshot displays the 'Live Connect' interface. At the top, there are navigation buttons: 'Add/Remove from List', 'Pivot to Investigate > Navigate', 'Pivot to Archer', and 'Pivot to Endpoint Thick Client'. Below these is a 'Review Status' section showing 'STATUS NOT REVIEWED' and 'MODIFIED DATE'. The main section is titled 'Live Connect Risk Assessment' and features a large orange circle with the word 'UNSAFE' inside. To the right of the circle, it says 'Research and analysis shows resource to be untrusted' and 'RISK REASONS'. Below this, there are several categories of risk indicators, each with a list of specific indicators in button format: 'RECONNAISSANCE' (SCANNING, BRUTE FORCE, VPN, TOR, SOCKS, ANONYMOUS ACCESS, HTTP, FTP, SSH, BUSINESS APPLICATION, OTHER), 'DELIVERY' (EXPLOIT, PHISHING, DRIVE BY, XSS, SQLI, CSRF, REMOTE LOCAL FILE INCLUSION, OTHER), 'COMMAND AND CONTROL' (BEACONING, HTTP, SSL/TLS, SSH, FTP, IRC, CUSTOM PROTOCOL, WEBSHELL, VPN, OTHER), 'LATERAL MOVEMENT' (SMB/RPC, RDP, SSH, POWERSHELL, WMI, TELNET, OTHER), 'PRIVILEGE ESCALATION' (PASSWORD DUMPERS, SQL, EXPLOIT, POWERSHELL, OTHER), and 'PACKAGING AND EXFILTRATION' (ZIP, RAR, 7ZIP, CUSTOM COMPRESSION, FTP, HTTP, SSL, SSH). At the bottom, there is a 'Risk Assessment Feedback' section with dropdown menus for 'ANALYST SKILL LEVEL' (set to TIER 1), 'RISK CONFIRMATION', 'CONFIDENCE LEVEL', and 'RISK INDICATOR TAGS'. A 'Submit' button is located at the bottom right. The footer indicates 'Time Window: ALL DATA | Last Updated: (7 minutes ago)'.

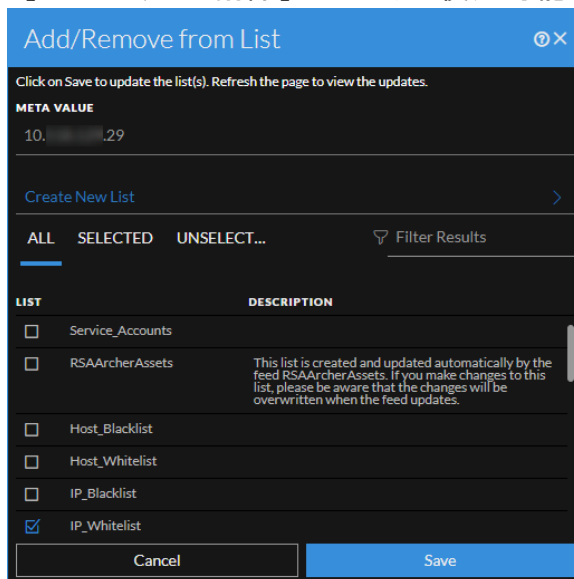
3. エンティティに対してアクションを実行するには、コンテキスト ツールチップで使用可能な次のアクションのいずれかを選択します。[リストへの追加/削除]、[調査] > [ナビゲート]への移行]、[Archerへの移行]、[Endpoint Thick Clientへの移行]。詳細については、「[\[調査\] > \[ナビゲート\]への移行\(\[イベント\]ビュー\)](#)」、「[\[Archerへの移行\(\[イベント\]ビュー\)](#)」、「[\[NetWitness Endpoint Thick Clientへの移行\(\[イベント\]ビュー\)](#)」、「[\[ホワイト リストへ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

- [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。
- 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。



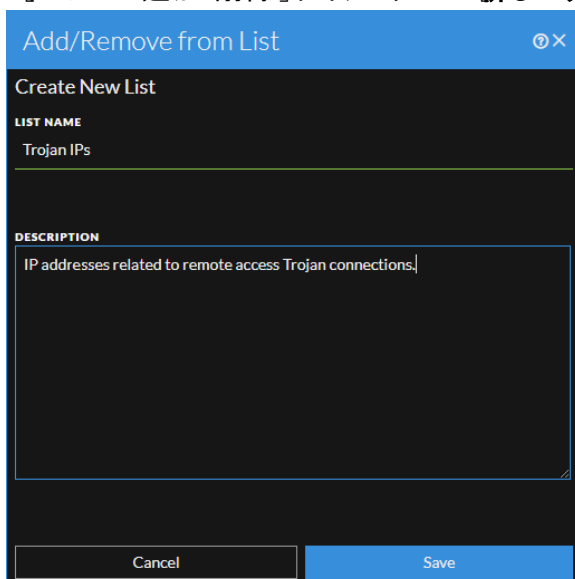
- 1つ以上のリストを選択し、**保存**]をクリックします。
選択したリストにエンティティが追加されます。

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、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. 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 > [サビゲート]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、[サビゲート]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、「[「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。

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)

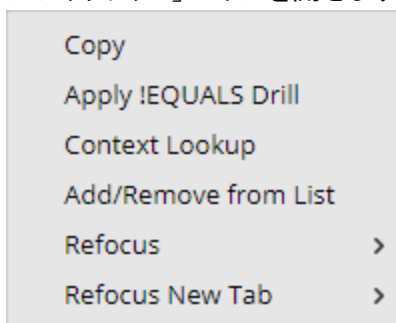
NetWitness Endpointシック クライアント アプリケーションがインストールされている場合は、コンテキスト ツールチップから起動できます。そこから、疑わしいIPアドレス、ホスト、MACアドレスをさらに調査できます。

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。選択可能なデータソースは次のとおりです。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。
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。



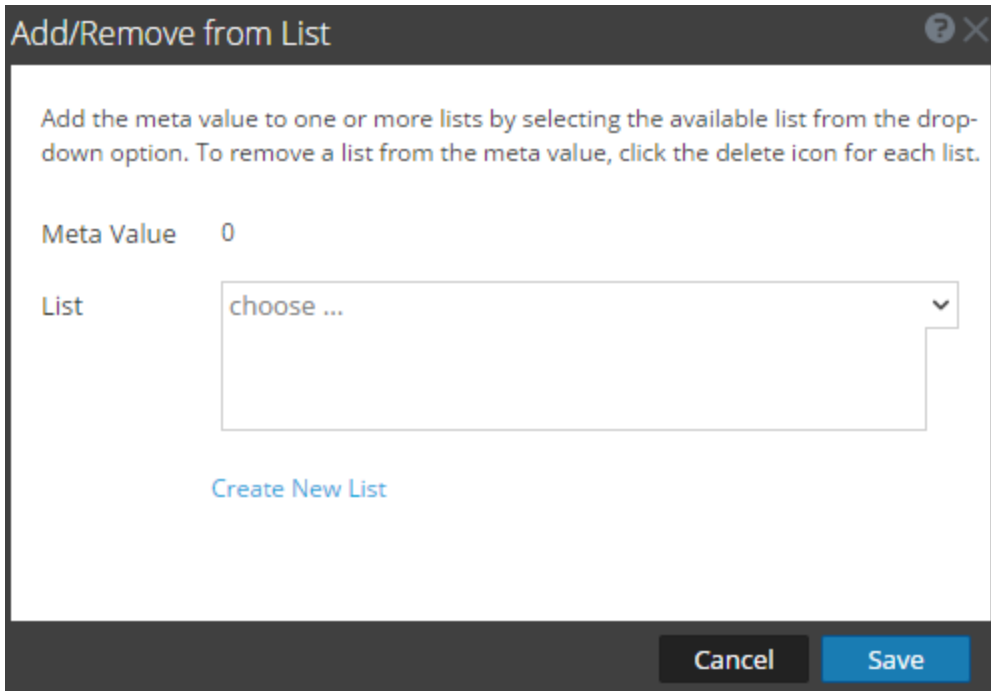
ブラウザ ウィンドウの右側から **[コンテキスト ルックアップ]パネル**が開きます。 **[コンテキスト 検索]パネル**には、利用可能になったContext Hubの情報が入力されます。

3. **[コンテキスト 検索]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 **[X]** 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 オプションから選択します。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([サビゲート]ビューと [レガシー イベント]ビュー)

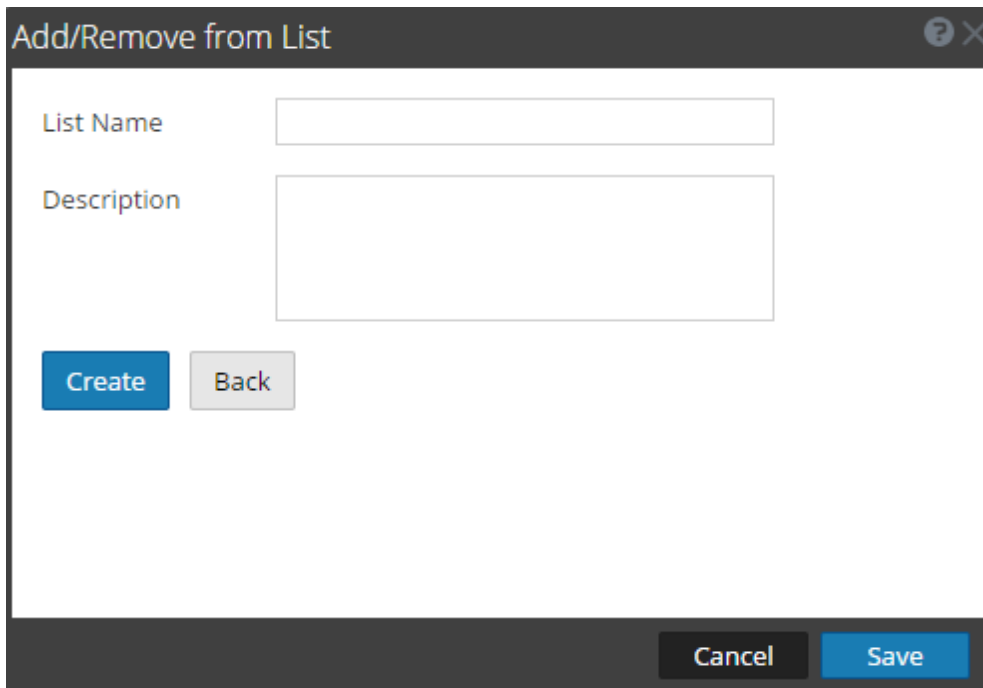
リストからメタ値を削除するには、次の手順を実行します。

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([サビゲート]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。



The screenshot shows a dialog box titled "Add/Remove from List". It features a "List Name" text input field and a "Description" text area. Below these fields are "Create" and "Back" buttons. At the bottom right of the dialog are "Cancel" and "Save" buttons.

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)、client、file-hash.)。

ipおよびhostの各メタ キーについては、NetWitness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ルックアップ :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 for IPs and Hostnames:CentralOps Whois for IPs and Hostnames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 :UrIvoid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)。

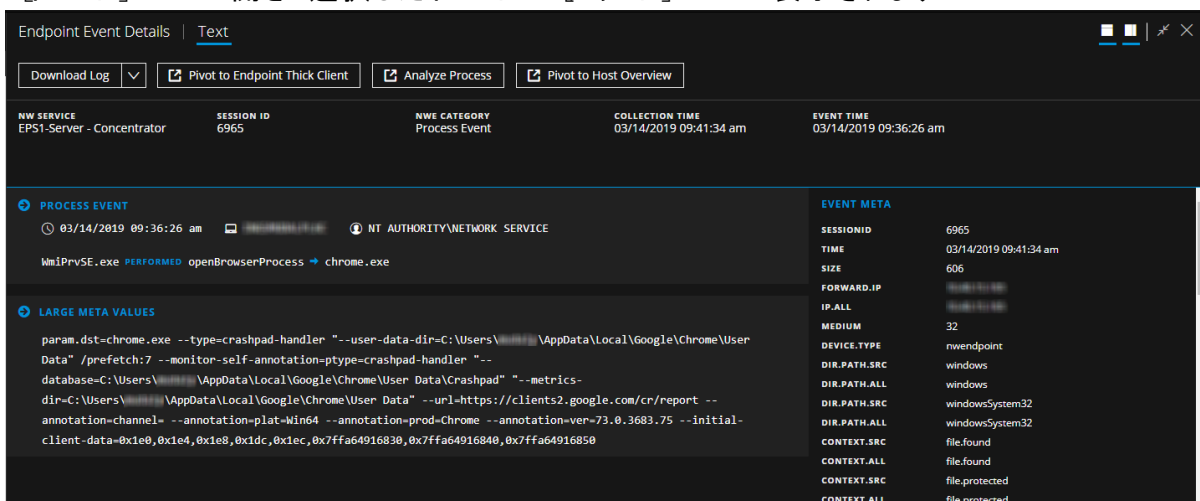
[イベント]ビューでのEndpoint Thick Clientルックアップの起動

[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ユーザー 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、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、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 [イベント]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。



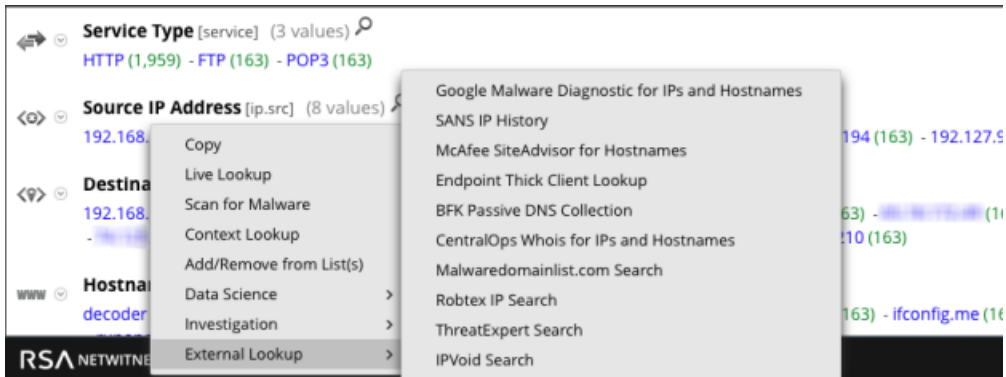
4. イベント ヘッダーで、[エンドポイントへの移行]をクリックします。
 新しいブラウザ タブでURL `ecatui://<id>`が開き、NWE Thick Clientが起動されます。
 NetWitness Endpoint Thick Clientがインストールされていない場合は、データが表示されず、次のメッセージが表示されます。
`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`

[ナビゲート]ビューでのEndpoint Thick Clientルックアップの起動

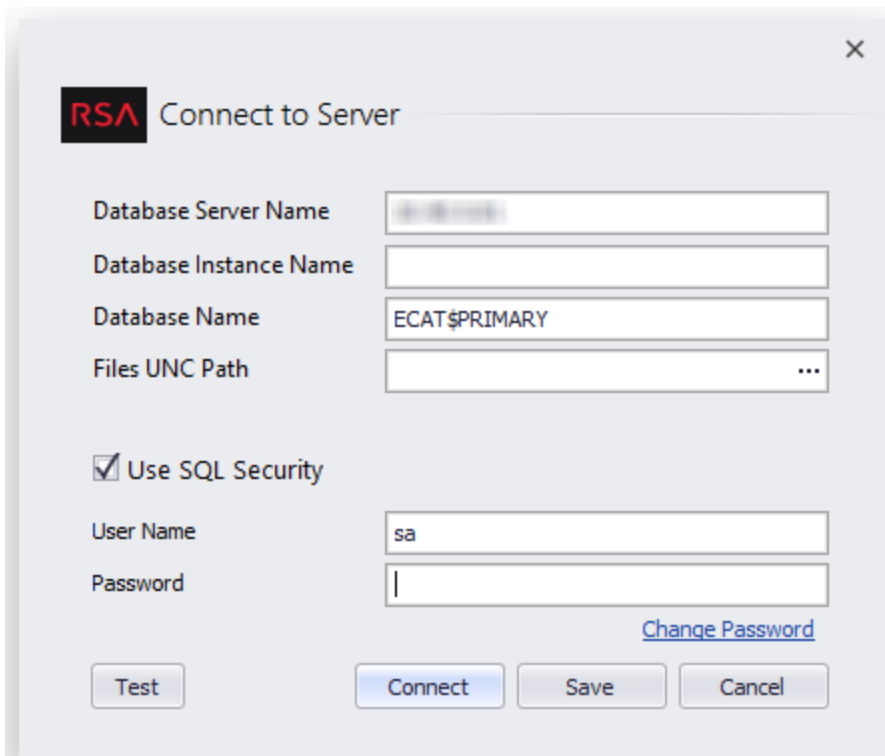
[ナビゲート]ビューからデータのEndpoint Thick Clientルックアップ機能を起動する方法：

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。

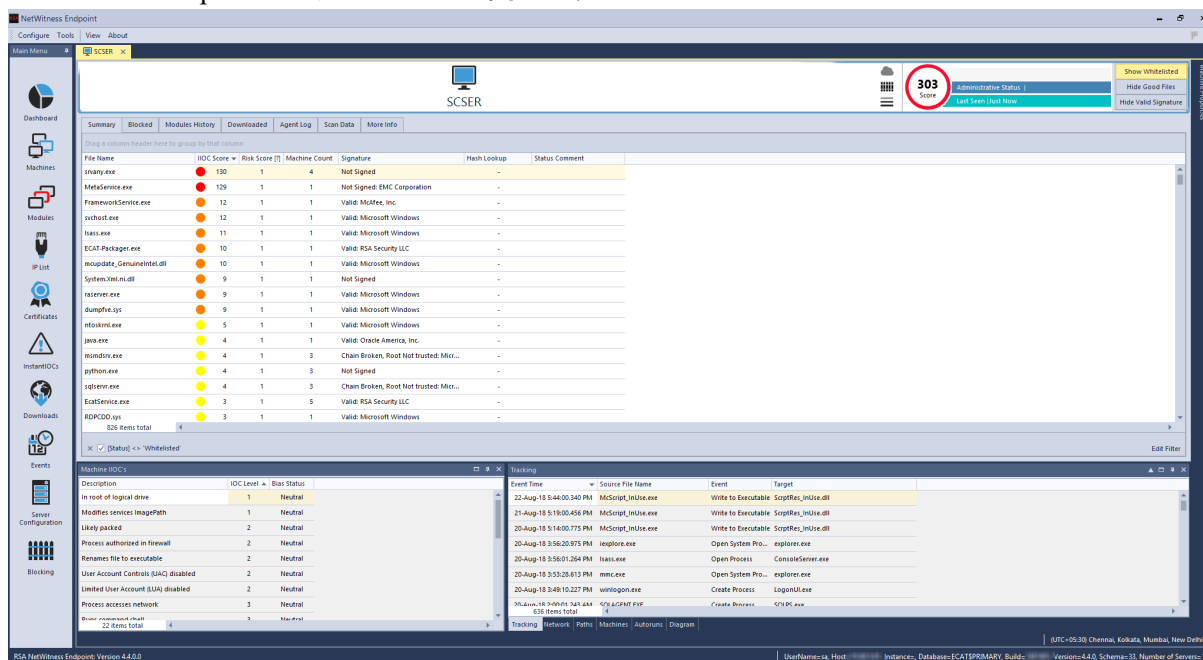


3. **Endpoint Thick Clientルックアップ** を選択します。
[サーバーに接続] ダイアログが表示されます。



4. Endpoint Thick Clientへのログインに必要なユーザー名とパスワードを入力して、**接続** をクリックします。

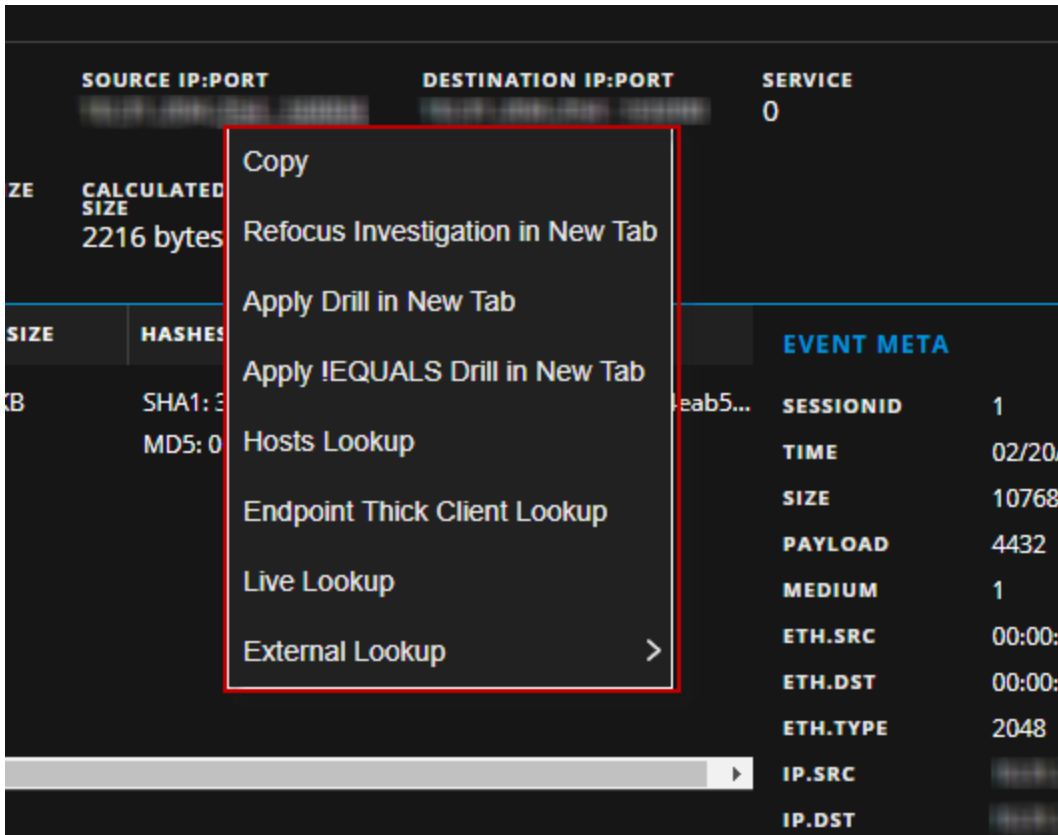
NetWitness Endpointでドリルポイントが開きます。



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** :新しいタブで、[ナビゲート]ビューを開き、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。

SESS	Copy	DEVICE CLASS	EVENT CATEGORY
259	Copy	Anti Virus	Other.Default
	Refocus Investigation in New Tab	Google	
	Apply Drill in New Tab	SANS IP History	
:24 P	Apply IEQUALS Drill in New Tab	CentralOps Whois for IPs and Hostnames	
Modu	Hosts Lookup	Robtex IP Search	
7d433	Endpoint Thick Client Lookup	IPVoid	
0.42	Live Lookup	URLVoid	
anPro	External Lookup	ThreatExpert Search	
5943e			

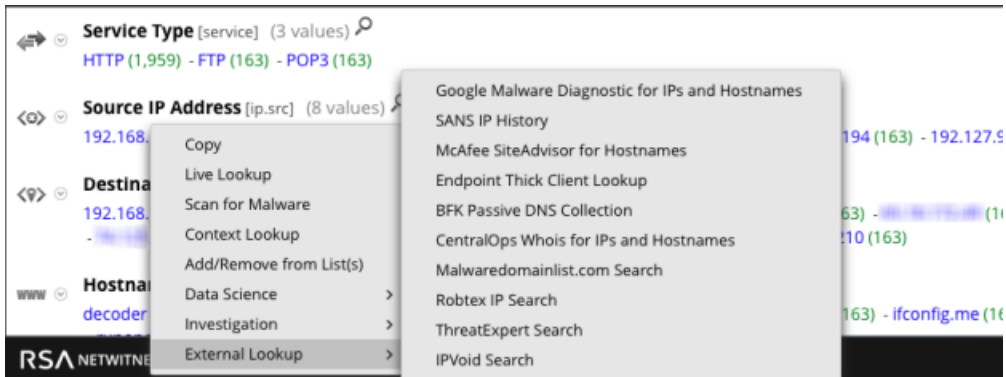
4. サブメニューで、使用可能な外部ルックアップのいずれかを選択します。
- **Google** :Google.comでメタ値を検索します。
 - **SANS IP History** :SANS IP Historyでメタ値を検索します(domain = <http://isc.sans.org/ipinfo.html?ip=ipaddress>)。
 - **CentralOps Whois for IPs and Hostnames** :CentralOps Whois(IPおよびホスト名検索)でメタ値を検索します(domain = http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true&net_whois=true)。
 - **Robtex IP Search** :Robtext IP Searchでメタ値を検索します(domain = <https://www.robtext.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 Search** :ThreatExpert検索(ドメイン = <http://www.threatexpert.com/reports.aspx?find=IPアドレス>)でIPメタ値を検索します。

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

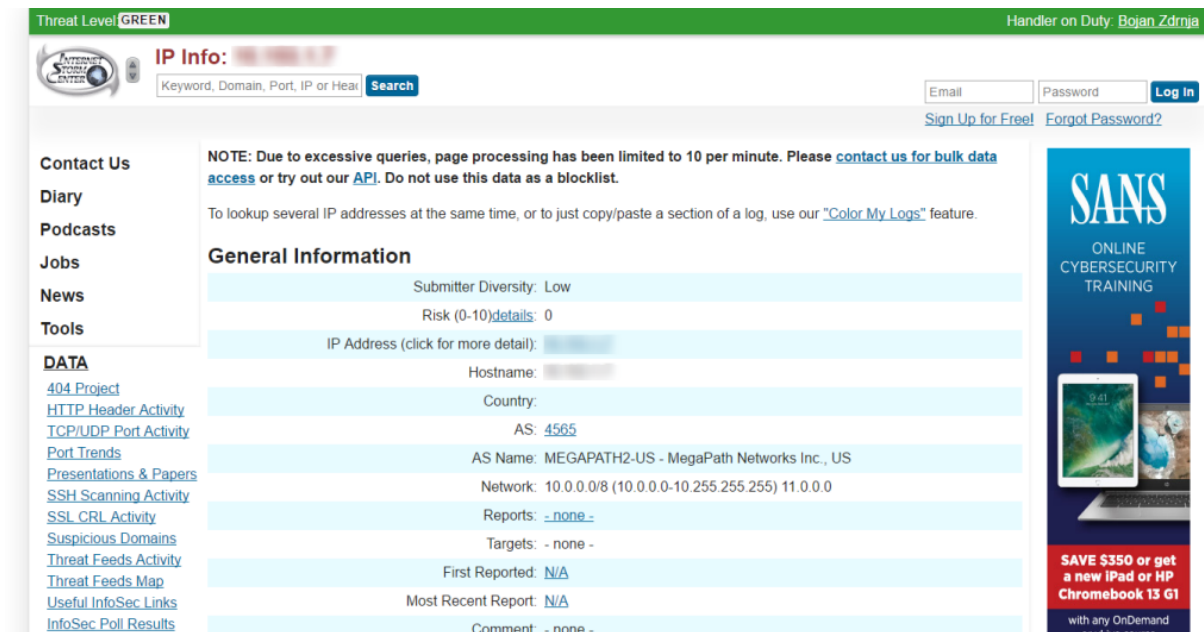
ナビゲート]ビューからデータの外部ルックアップ(NetWitness Endpoint Thick Clientルックアップ以外)を起動するには、次の手順を実行します。

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

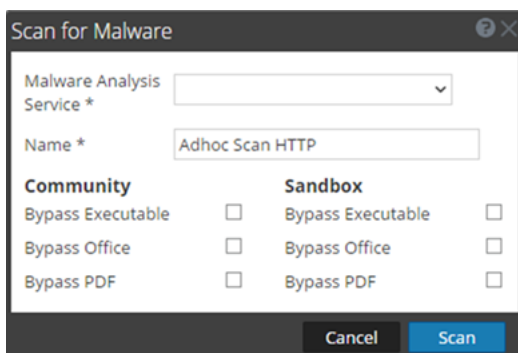
調査においてアナリストは、サービスとメタ値を選択し、コンテキストメニューからオプションを選択することによって、オンデマンドMalware Analysisスキャンを開始できます。スキャンが完了すると、スキャンされたデータをMalware Analysisから確認できます。

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。

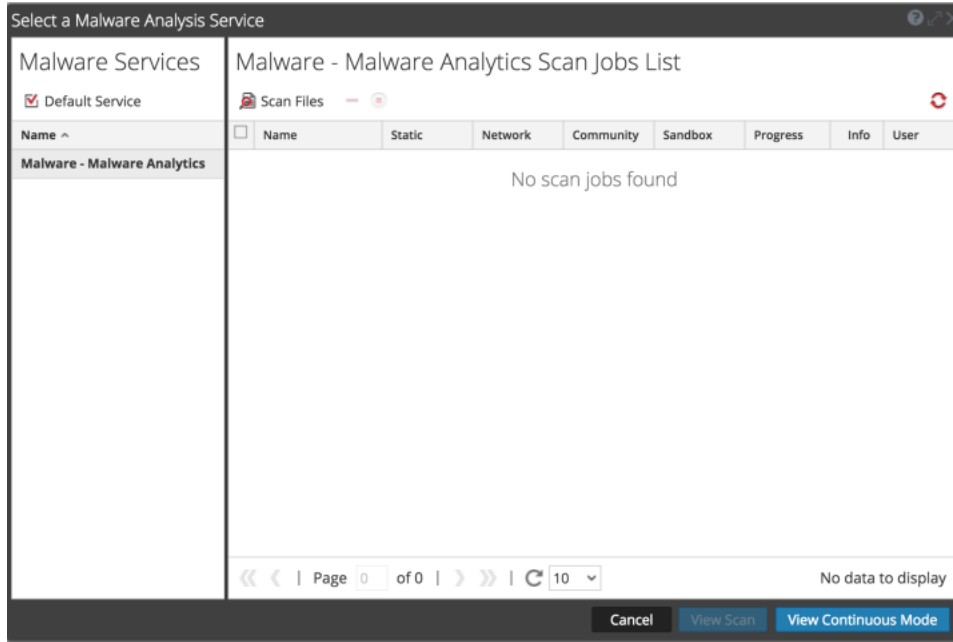
1. メタ値 (OTHER、DNS、FTPなど) を右クリックして、コンテキストメニューで **マルウェアのスキャン** を選択します。

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。

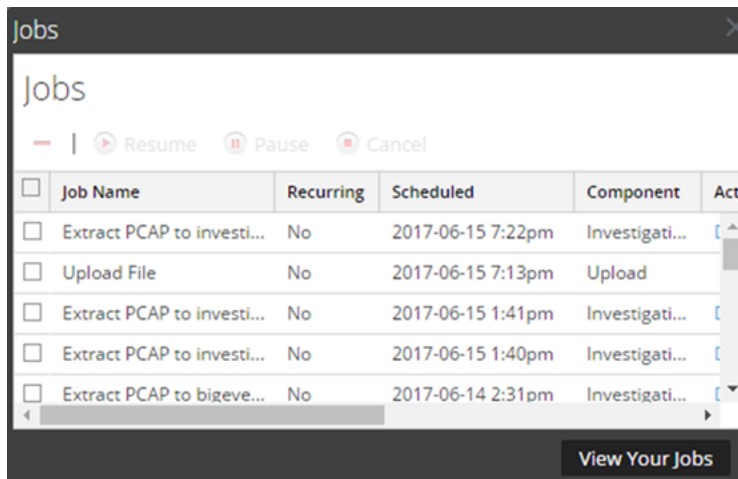
2. **マルウェアのスキャン** ダイアログで、スキャンを実行するサービスを選択し、名前を編集して、**コミュニティ**と**サンドボックス**の下からバイパスするファイルのタイプを選択します。



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、 をNetWitnessツールバーでクリックします。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「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

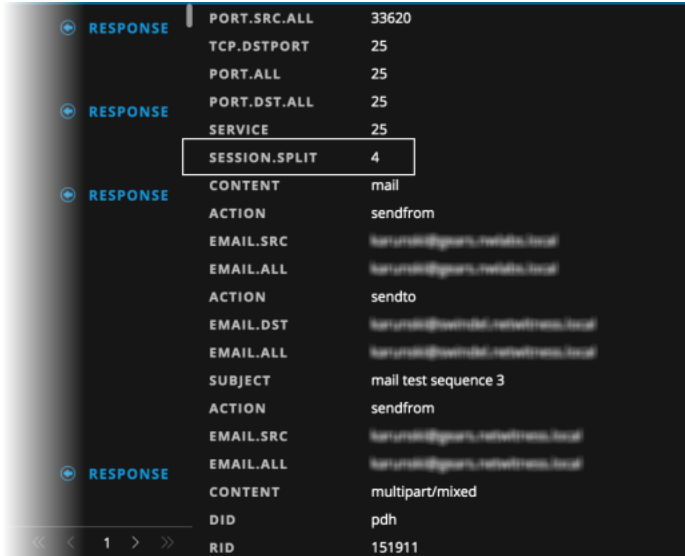
「イベント」ビューのイベント リストには、分割セッションと関連セッションからのイベントが、解析された順序で表示されるため、常に一緒に表示されるとは限りません。バージョン11.4.1以降では、「イベントのグループ化」オプションを使用して、収集したデータの関係をもっと簡単に検出できるように、イベントの表示順を変更できます。イベントがグループ化されている場合、最初のイベントは先行イベントと呼ばれます。

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。

COLLECTION TIME	TYPE	COMMUNITY ID	DESTINATION IP A...	SOURCE IP ADDRESS	SESSION SPLIT CO...	SESSION ID	TCP DESTINATION ...	TCP SOURCE
10/14/2008 04:06:22 pm	1[Network]	1nq5nS1sJ00ozB6J/8...	...	192.168.1.103		509054	80 [http]	1259
10/14/2008 04:06:22 pm	1[Network]	192.168.1.103	1	509055	80 [http]	1259
10/14/2008 04:06:23 pm	1[Network]	1ooDCLWnuTKg1kk...	...	192.168.1.103		509056	80 [http]	1260
10/14/2008 04:06:23 pm	1[Network]	192.168.1.103	1	509057	80 [http]	1260
10/14/2008 04:06:23 pm	1[Network]	192.168.1.103	2	509058	80 [http]	1260
10/14/2008 04:06:50 pm	1[Network]	1WbhfLKx4ryOQEys...	...	192.168.1.103		509067	80 [http]	1264
10/14/2008 04:06:50 pm	1[Network]	192.168.1.103	1	509068	80 [http]	1264
10/14/2008 04:06:50 pm	1[Network]	1at7QYm+7Mo4YOn...	...	192.168.1.103		509061	80 [http]	1263

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。

- 元のイベントに含まれるトランザクションごとに個別のイベントが作成されたため、元のイベントが複数のサブパーツに分割された。
- 元のセッションのサイズがAssembler Maximum Size(デフォルト=32 MB)を超えるため、Network Decoderが取り込む際に分割された。
- 元のセッションの時間がAssembler Timeout Session(デフォルト=60秒)を超えるため、Network Decoderが取り込む際に分割された。

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、ネットワークデコーダはセッションを分割し、後続パケットが新規セッションの一部となります。ネットワークセッションがフラグメントにより複数に分割され、複数のセッションになります。より大規模なネットワークセッションのフラグメントであるということで処理し、送信元および宛先アドレスやポートそしてアプリケーションプロトコルによる関連付けによって、ネットワークデコーダはフラグメントした各セッションを解析して、強調表示します。

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PCAPI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 では32 MB) または構成されたタイムアウト(デフォルト では60秒) に基づいて、セッションを分割する前にセッションのパーズを完了します。パーズが完了した時点でパーズ結果には、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せん。それらが、後続のすべてのセッション フラグメントに追加され、それらが表す論理的ネットワークセッションとの整合性が確保されます。

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Network Decoderの動作を制御するパラメーターがあります。

`/decoder/parsers/config/parser.transaction.mode` 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。

COLLECTION TIME	TYPE	SERVICE TYPE	ORIGINATING IP A...	SOURCE IP AD...	DESTINATION...	TCP DESTINA...	DESTINATION...	HOSTNAME A...	SOURCE COU...
03/26/2020 04:52:00 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 04:53:06 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 04:54:10 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 04:55:14 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 04:56:17 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 04:57:21 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 04:58:25 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 04:59:29 am	1 [Network]	25 [SMTP]				23946			Canada
03/26/2020 05:00:33 am	1 [Network]	25 [SMTP]				23946			Canada

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、次の追加のメタ キーがあります。session.split. 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、先行するセッション フラグメントの数を示します。ただし、値が0であっても、後続のセッション フラグメントが存在することを示しているとは限りません。最大セッション サイズを超える前にセッションが解析された場合は、セッションの最初のフラグメントにsession.splitメタデータがない可能性もあります。

トランザクション分割は、1というsession.split値で始まります。セッションが表示されると、session.splitメタ キーにより、[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 [イベントの詳細]ビュー)のフラグメントであるセッションが明確に特定されます。

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
```

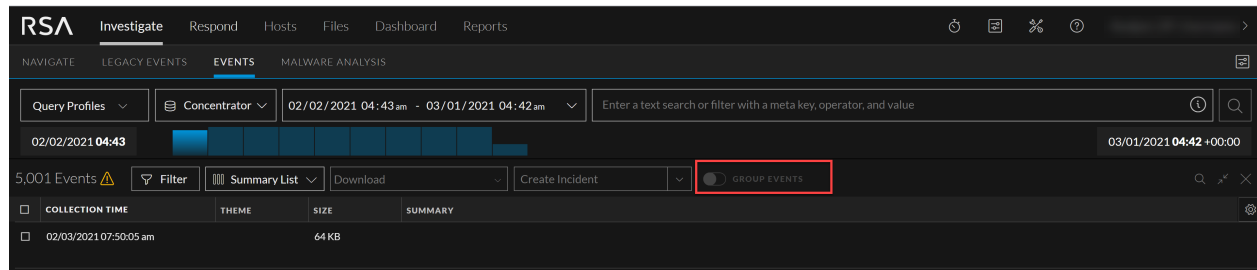
```
tcp.dstport=1234"Second category: Related Network Session
```

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。各イベントは同じソースIPアドレス、宛先IPアドレス、ソースポート、宛先ポートを持ちます。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

バージョン11.6では、データプライバシーが有効になっているときは、ログ、ネットワーク、エンドポイントからイベントを取得するグループ イベント オプションが無効になります。たとえば、管理者が'ip.src'をブラックリストに登録しているか、制限している場合は、次の図に示すオプションが無効になります。



このオプションは、次の12個のメタのうち、1つ以上が制限されている場合は無効になります。

'sessionid'

'nwe.callback_id'

'medium'

'session.split'

'ip.dst'

'ip.src'

'ipv6.src'

'ipv6.dst'

'tcp.dstport'

'tcp.srcport'

'udp.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。

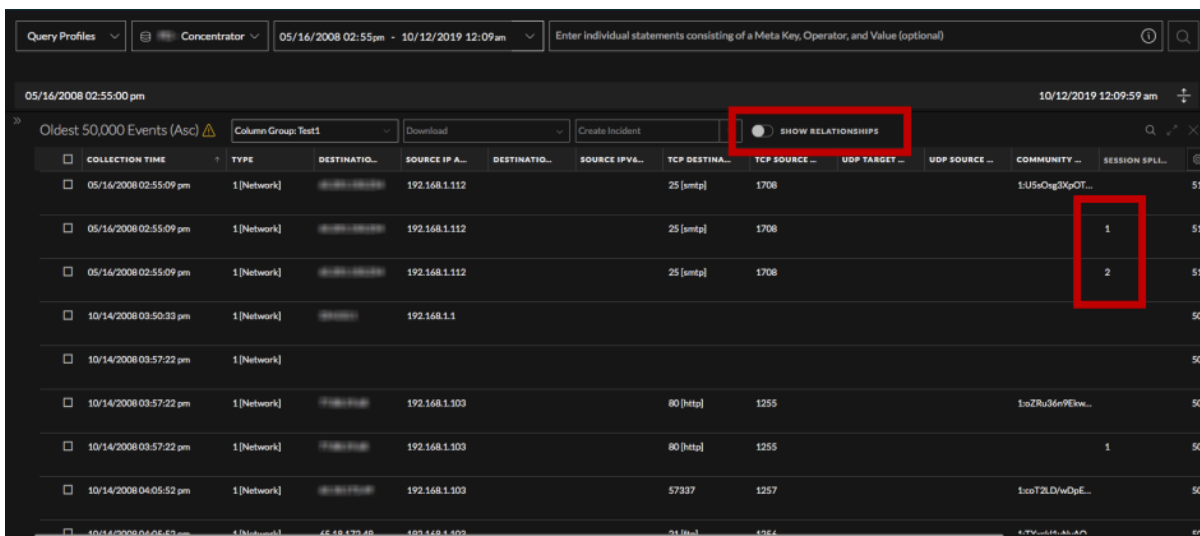
- プロキシ サーバをインラインで使用しているNetwork Decoderは、NetWitnessの認識に応じてイベント時間に基づいて単一セッションにバンドルされる多数のEメール接続を受信します。subject、email.src、email.dstをはじめとしたメールに関連するメタキーのメタ値はセッションごとに複数あり、正しく組み合わせるマッピングすることは困難です。セッションを先行イベントと後続イベントとして編成することで、アナリストは各メールの詳細を明確に把握できるようになります。
- アナリストは、セッションに関連づけられたすべてのメタデータのうち、どのIPアドレスがメタデータの生成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。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、次のコマンドを使用するHTTP接続があるとします。それは、`directory /keep/`、`directory /temp/`、`filename foo.txt`、`filename me.doc`、`action delete`、`action read`です。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の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

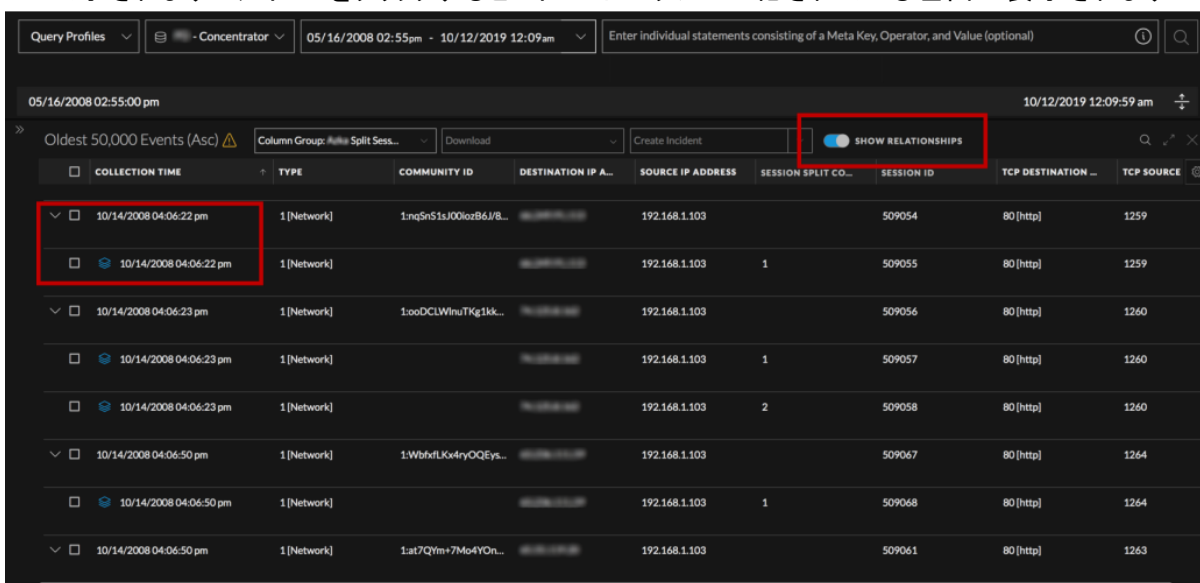
どちらのタイプの関連イベントについても、イベントの関係は [イベント]ビューの [イベント]リストで確認できます。 [イベント]リストが最初に表示されている場合は、 [イベント]リストの最上部にある [イベントのグループ化]スイッチを見て、結果に関連イベントが含まれているかどうかを確認できます。結果に関連イベントが含まれていない場合、このスイッチはグレー表示になります(次の図を参照)。

[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、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は、 [イベントのグループ化]スイッチがアクティブですが、有効にはなっていません。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。

RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN

Navigate Events Event Analysis Hosts Files Users Malware Analysis

Concentrator All Data Query Profile Detail View Actions Incidents

Cancel



Event Time	Event Type	Size	Details
2008-05-30T17:54:20	Network	12 MB	↔ 10.21.2.52 -> 204.9.165.82 ↔ 4550 -> 80  0
2008-05-30T17:54:09	Network	75 bytes	↔ 10.21.2.56 -> 123.201.79.215 ↔ 37082 -> 40835
2008-05-30T17:54:09	Network	75 bytes	↔ 10.21.2.56 -> 62.88.70.52 ↔ 37082 -> 53638
2008-05-30T17:54:10	Network	145 bytes	↔ 10.21.2.56 -> 121.233.184.2 ↔ 37082 -> 22161
2008-05-30T17:54:10	Network	145 bytes	↔ 10.21.2.56 -> 89.133.41.168 ↔ 37082 -> 64203
2008-05-30T17:54:10	Network	145 bytes	↔ 10.21.2.56 -> 85.226.79.3 ↔ 37082 -> 16608

RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN

Navigate Events Event Analysis Hosts Files Users Malware Analysis

Concentrator All Data Query Profile Detail View Actions Incidents

Cancel

Event Time	Event Type	Event Theme	Size	Details
2008-05-30T17:54:20	Network	HTTP	12 MB	↔ 00:0B:DB:0F:46:C1 -> 00:1A:70:8E:69:0D ↔ [redacted] -> [redacted] ↔ 4550 -> 80  session.split : 0 ↔ sessionid : 1 📄 payload : 11902591 📄 medium : 1 📄 tcp.flags : 26 📄 streams : 2 📄 packets : 12619 🕒 lifetime : 16 🚀 action : get 📁 directory : / + Show Additional Meta  View Details

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。

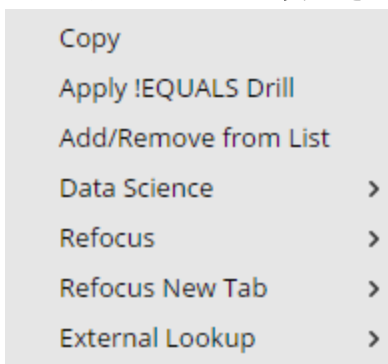
- ネットワークセッションのフラグメントであるセッションを特定する。
- 1つのセッション フラグメントから、元のネットワークセッションのすべてのセッション フラグメントを表示する。
- ネットワークセッション全体のパケットを1つのPCAPファイルとしてエクスポートする。

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]ビュー内で [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、現在のタイム ウィンドウ内で、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。

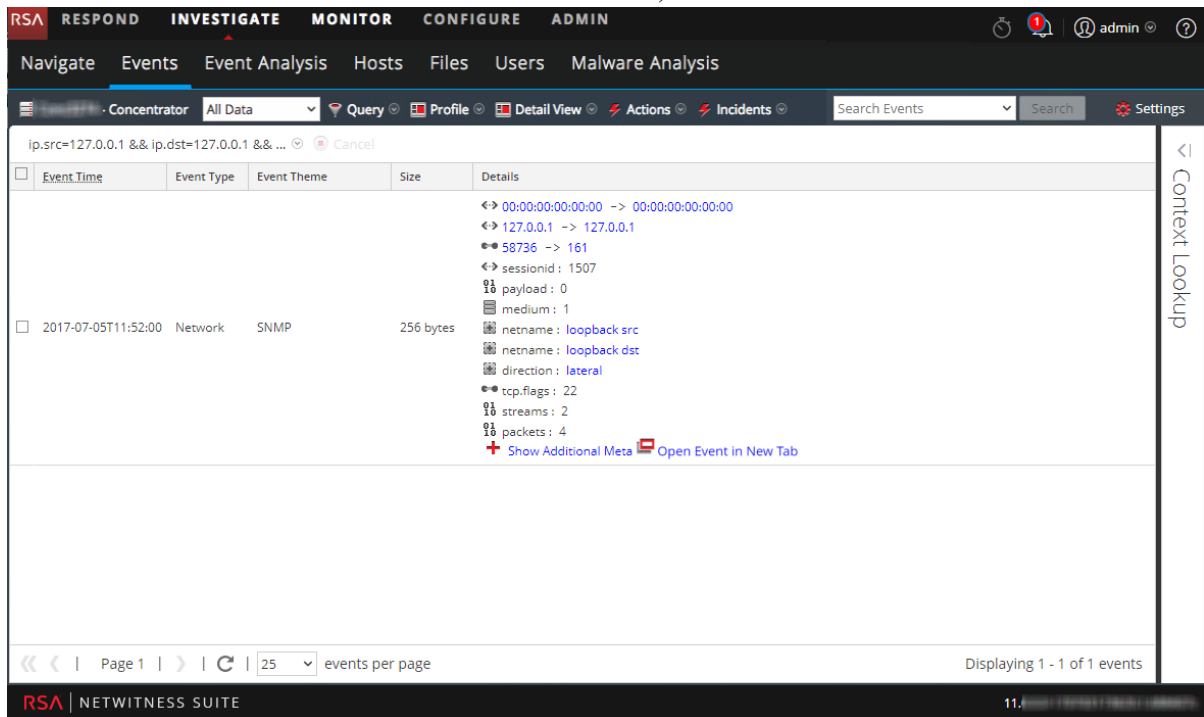
1. [レガシー イベント]ビューで、ソース アドレス、宛先アドレス、ポートの値 (`ip.src`、`ip.dst`、`ipv6.src`、`ipv6.dst`、`tcp.srcport`、`tcp.dstport`、`udp.srcport`、`udp.dstport`) および `session.split` 値のいずれかを右クリックします。コンテキスト メニューが表示されます。



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フラグメント(時間範囲10:30~10:35の1、2、3、4)が表示されている場合は、フラグメント0が存在するはずですが、時間範囲の開始時間を早く(この例では10:25に)して、さらにフラグメントが表示されるようにします。
 - 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場合があります。
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。

メタデータを座標表示チャートに追加する

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、メタ値の組み合わせ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。たとえば、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る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 .json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。プロファイルで使用されているメタ グループは削除できません。

NetWitness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。

座標表示で利用できるRSAメタ グループ

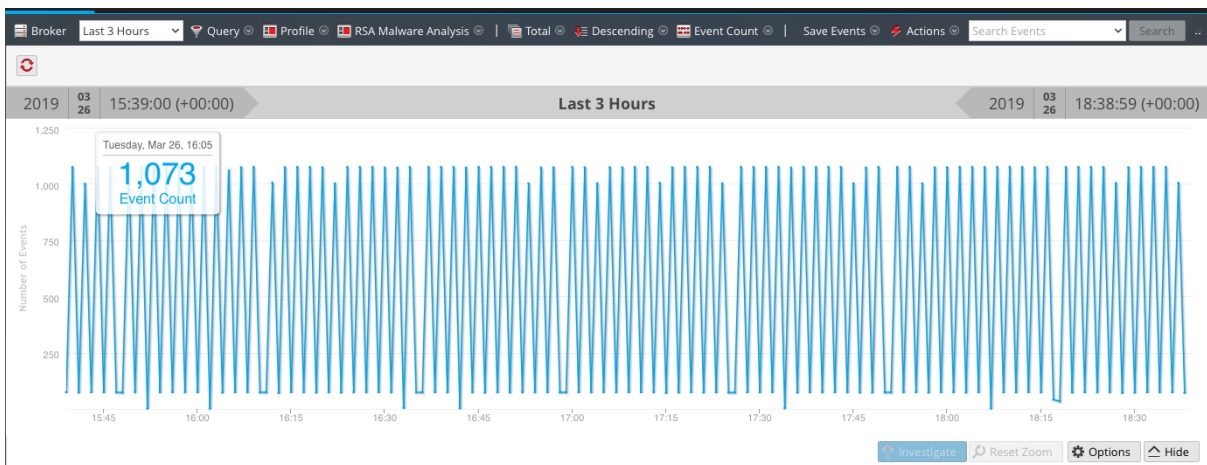
NetWitnessには、事前定義されたメタ グループのセットが含まれています。最新のバージョンを取得する場合は、[メタ グループの管理]ダイアログでメタ グループ ファイル(MetaGroups_oob_w_query.json)をインポートできます。座標表示チャートに適した標的型アクティビティとしては、次のようなものがあります。

- Botnet Beaconsing
- Covert Channels
- Email Analysis
- Encrypted Sessions
- Endpoint Analysis
- File Analysis
- Malware Analysis
- HTTP
- SSL/TLS
- SQL Injection Attacks
- Threat Analysis
- Web Analysis

座標表示チャートの表示

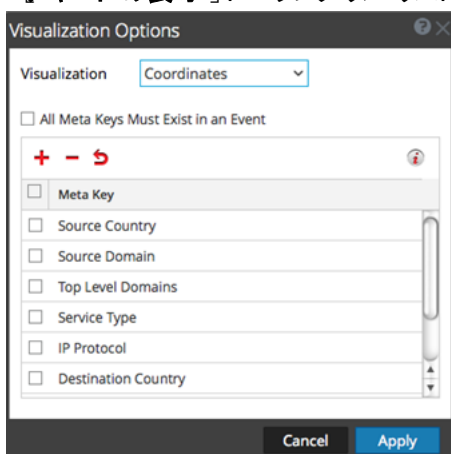
調査] > [ナビゲート]ビューで、次の手順を実行します。

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。

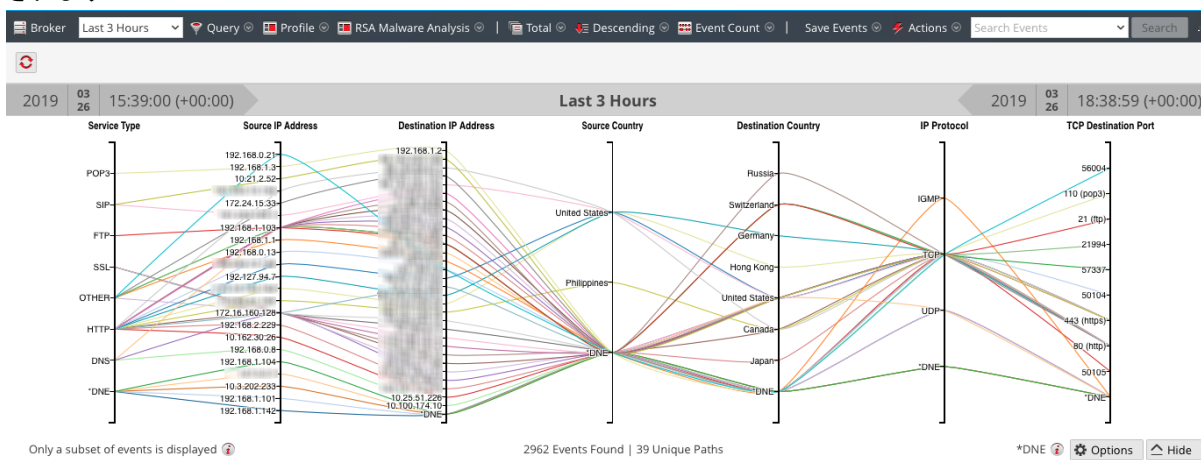


4. **チャート]パネルで [オプション]**]を選択します。
チャート オプション]ダイアログが表示されます。

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。



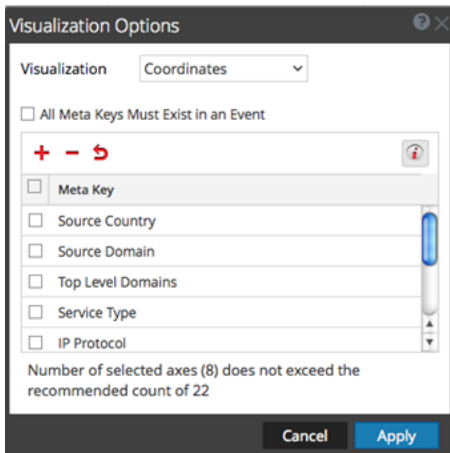
チャートがロードされます。この例では、2,962個のイベントが見つかり、39個の一意のパスが可視化されます。



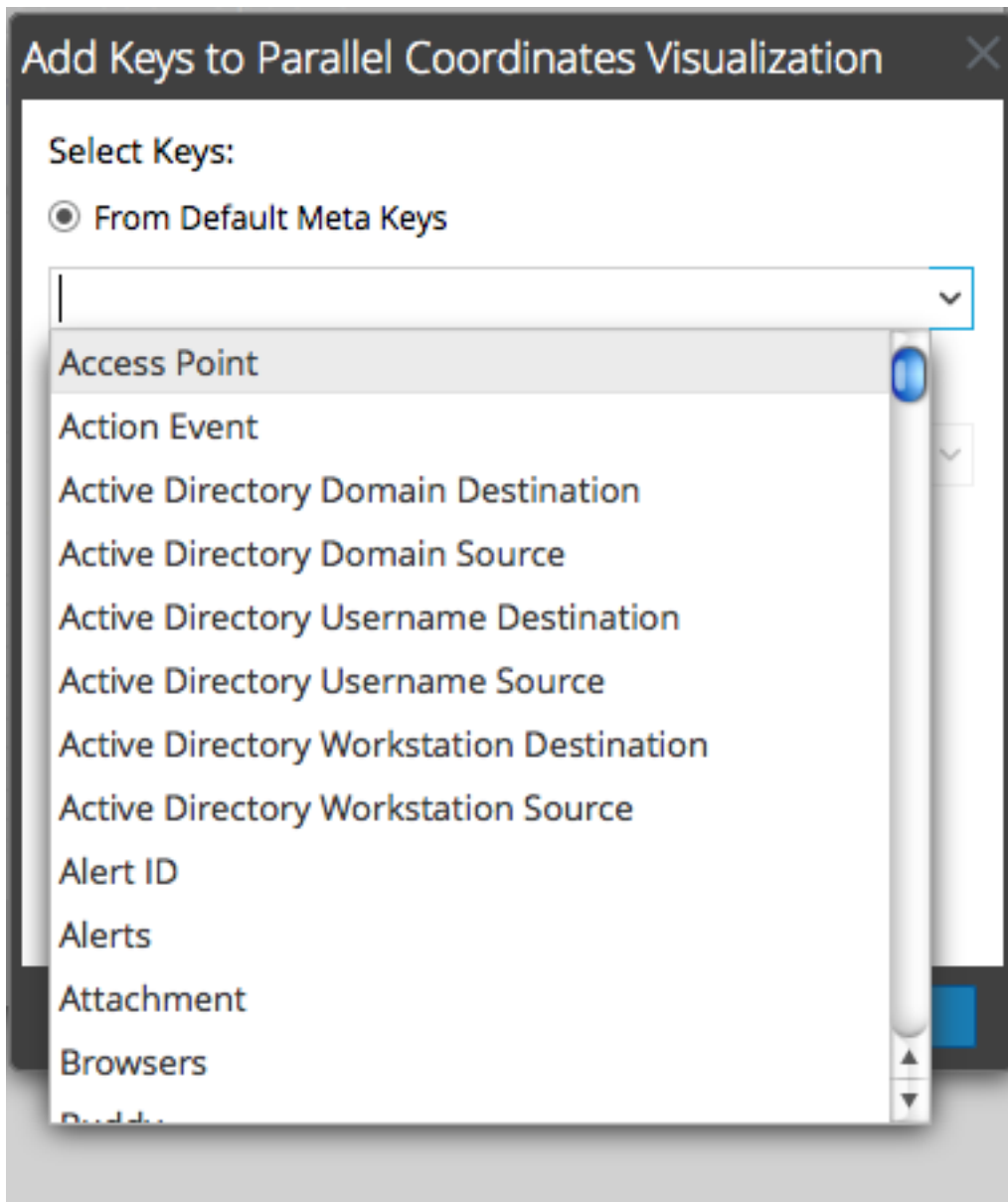
座標表示チャートで使用するメタキーの選択

座標表示チャートが開いた状態で、次の操作を行います。

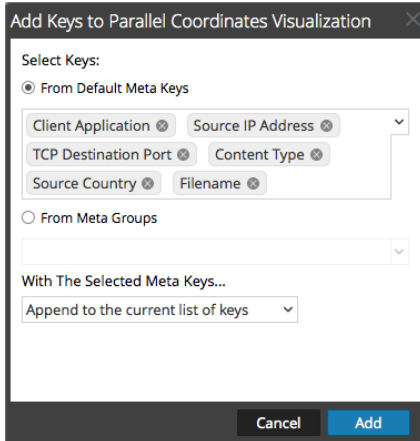
1. **チャート**]パネルで **オプション**]を選択します。
チャート オプション]ダイアログが表示されます。ツールバーの ⓘ をクリックすると、見やすいチャートに適した軸数が表示されます。推奨される軸の数は、ブラウザのサイズによって変化します。ブラウザウィンドウを拡大すると、推奨される数は増加します。



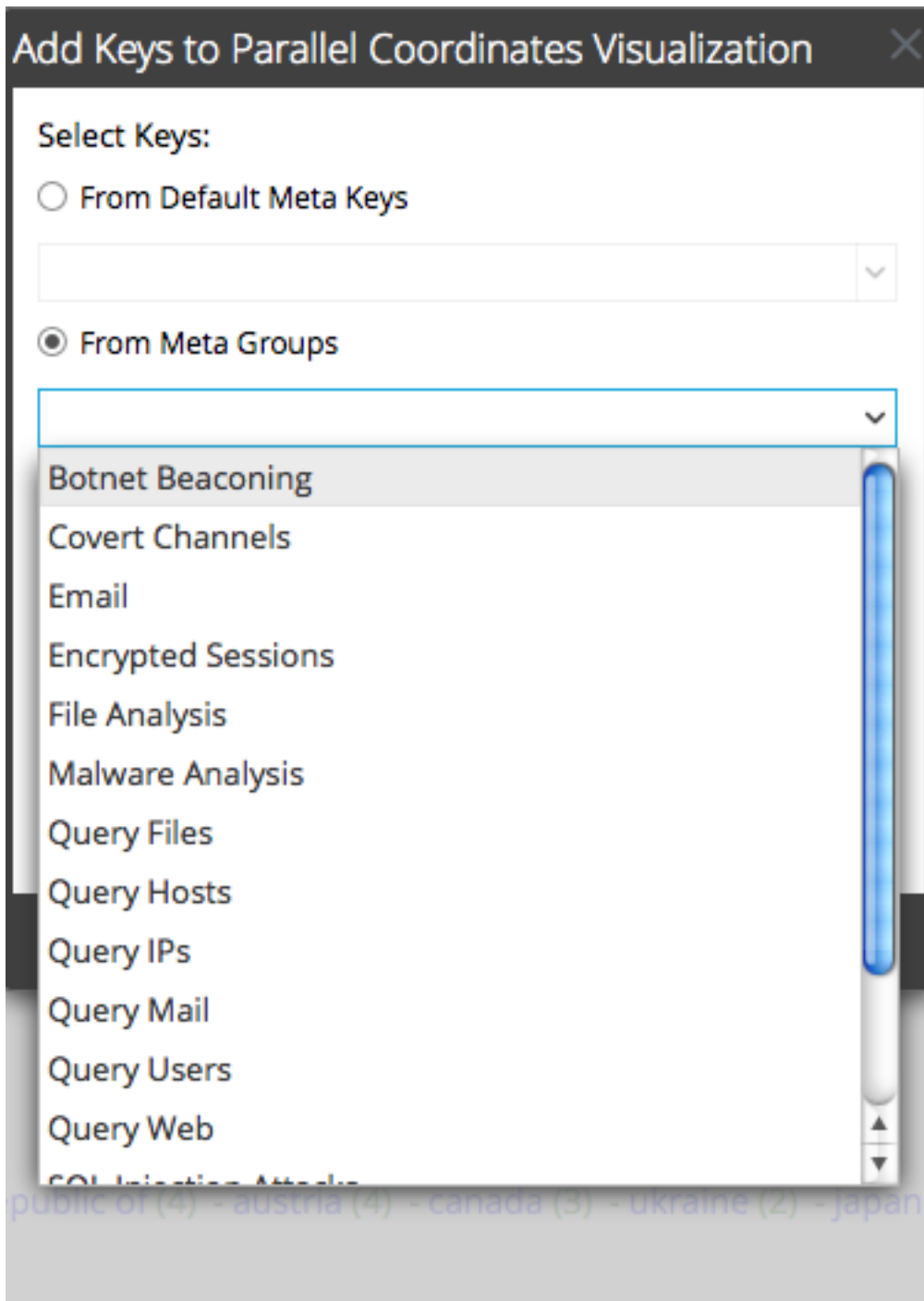
2. メタ キーの順序を変更するには、メタ キーを上下にドラッグして目的の順序に変更します。
3. メタ キーを削除するには、選択ボックス内をクリックして、**-** をクリックします。メタ キーが削除されますが、変更は適用されません。
4. 元の状態に戻すには、**↺** をクリックします。削除したメタ キーがすべてリストアされ、行った変更がすべて削除されます。
5. メタ キーを個別に選択する場合は、**+** をクリックし、**[デフォルトのメタ キーから追加]** を選択し、ドロップダウン リストからメタ キーを選択します。



選択したキーが表示されます。

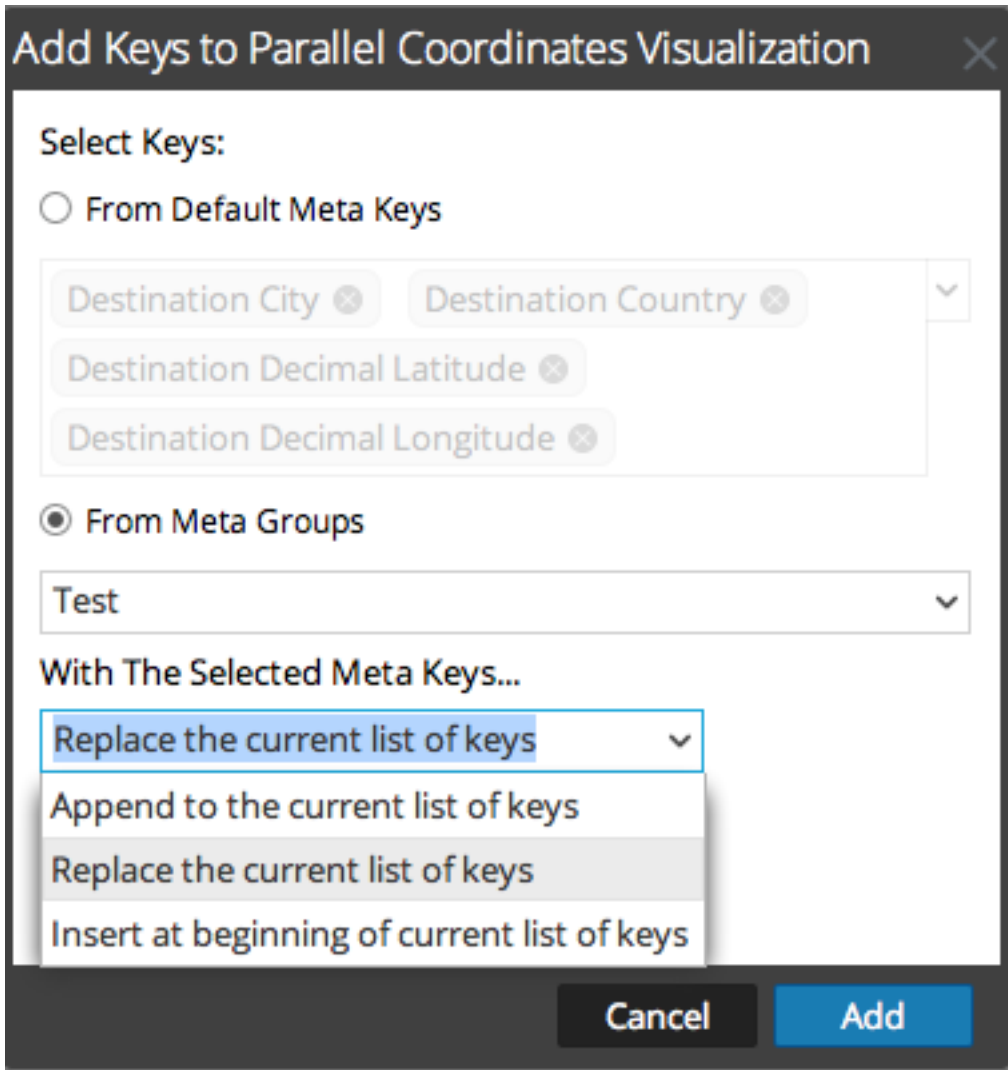


6. メタグループ内のすべてのメタキーを追加する必要がある場合、メタキーを個別に追加する必要はありません。[メタグループから追加]を選択して、ドロップダウンリストからグループを選択します。



選択したメタグループがフィールドに表示されます。

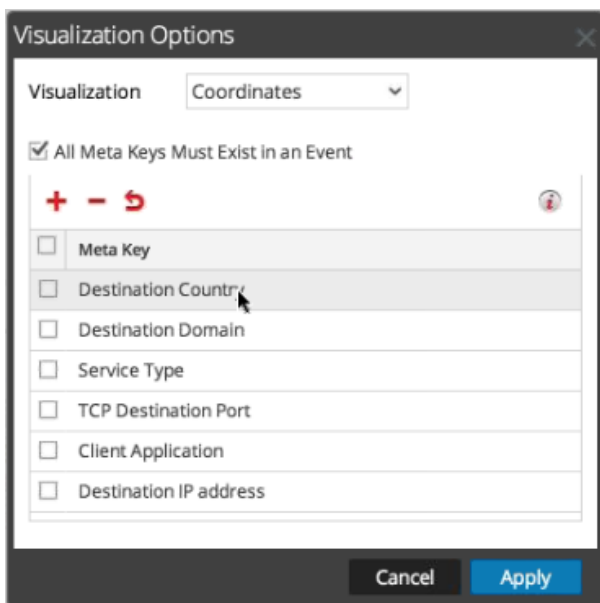
7. キーまたはグループの追加方法を、**現在のキーのリストを置き換え**、**現在のキーのリストの後に挿入**、**現在のキーのリストの先頭に挿入**から選択します。



8. 処理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 キーを備えていないイベントを削除することによってビジュアル化を最適化するには、**オプション**を選択します。

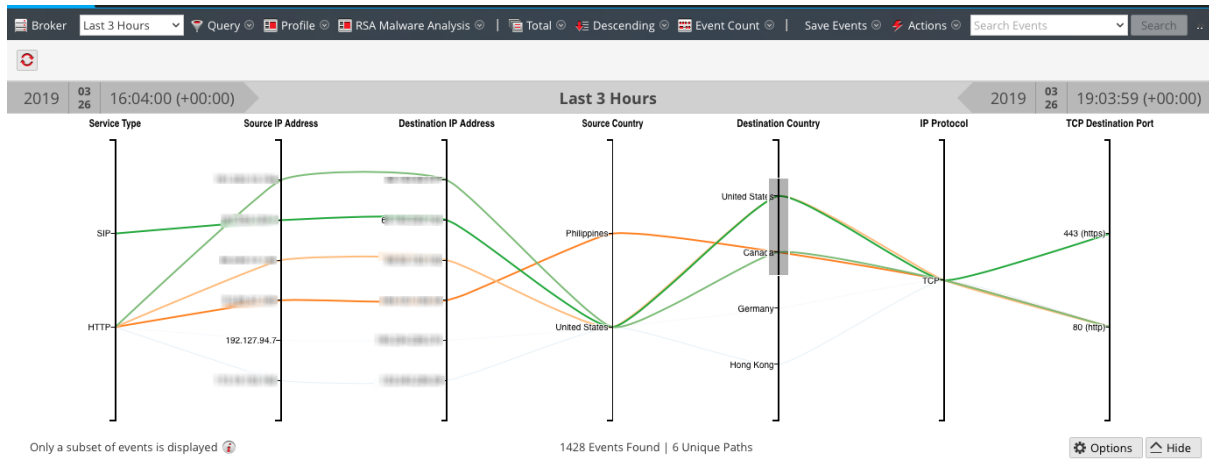


2. [ビジュアル化オプション]ダイアログで **すべてのメタ キーが1つのイベントに存在する必要があります]**を選択します。 **適用]**をクリックします。
結果として表示されるチャートは、見やすく便利になり、固有パスの数が減少します。



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。

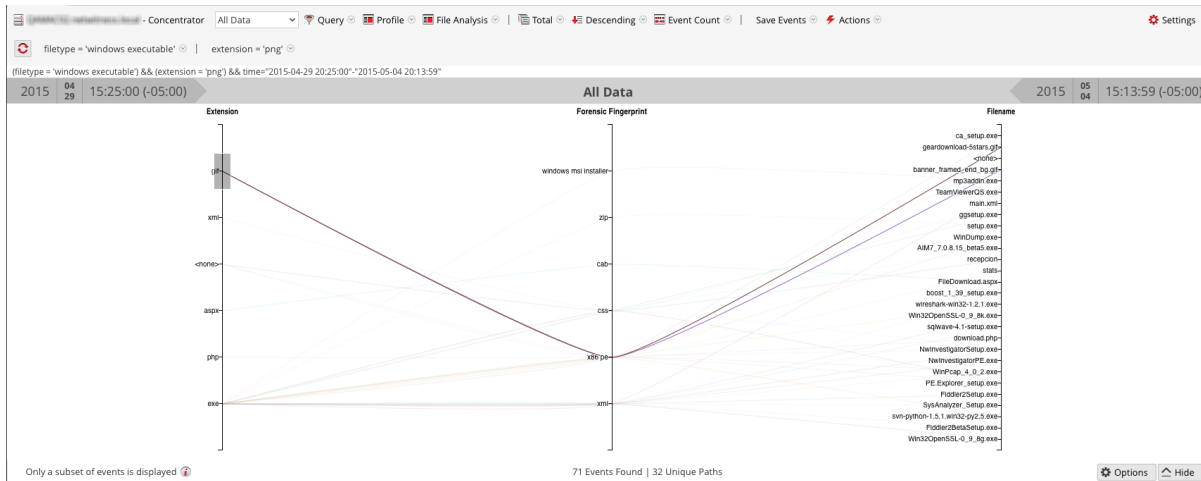
使用例

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つの軸を選択して座標表示チャートを構成します。file extension、forensic fingerprint、filename。

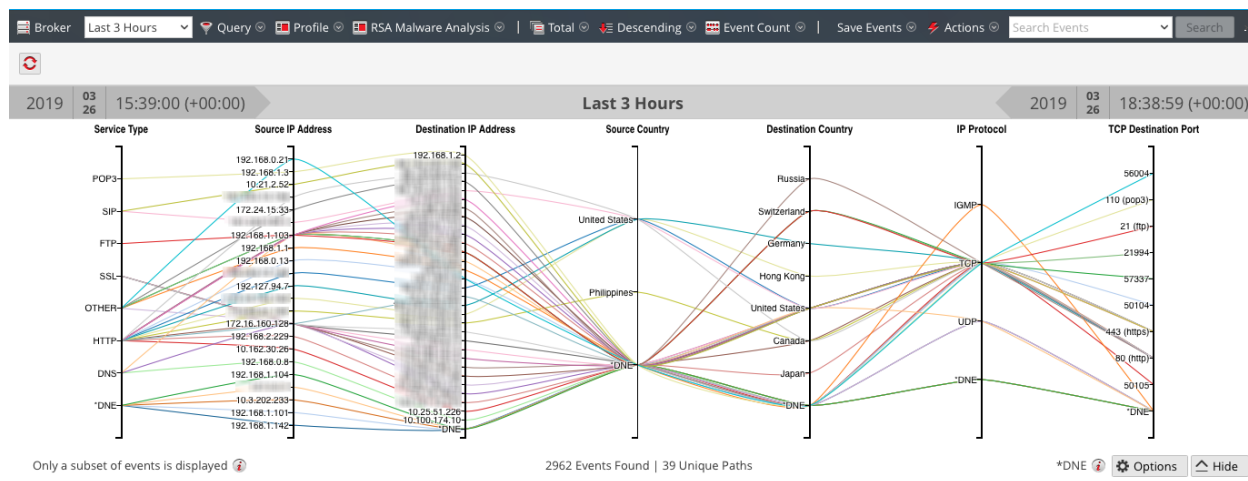


大量データセットのチャートの例

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、次のような情報メッセージが表示されます：イベントのサブセットのみが表示されます。



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

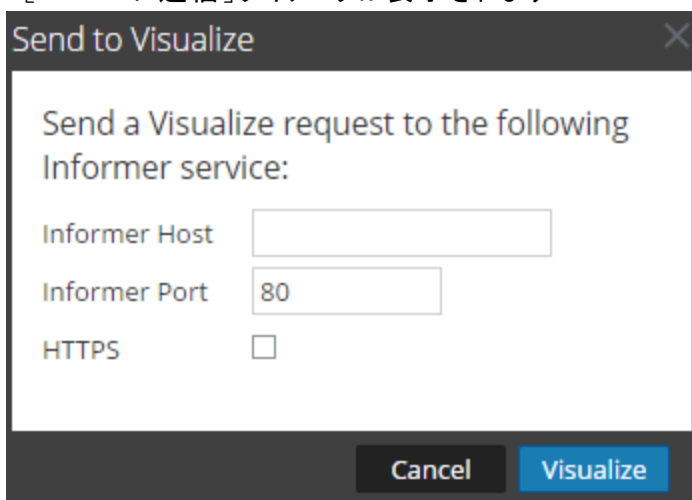
このピックでは、[ナビゲート]ビューでドリルポイントを送信してビジュアル化するための手順について説明します。

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送信して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] > [Visualize]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](#)
- [\[サビゲート\]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以降で使用可能な【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 タイプについ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。
- バージョン11.5には、【イベント】パネルおよびイベント再構築ですべてのイベント タイプの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。

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。

イベントまたはメタデータの【イベント】パネルでのダウンロード

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(バージョン11.4.1)またはすべてのメタデータ(バージョン11.5)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。

【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11.5には、すべてのメタデータまた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11.4.1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ますが、バージョン11.4メニューには、これらのオプションはありません。

【イベント】リストの【すべて選択】チェックボックスがオンの場合、【すべてダウンロード】オプションが使用可能です。すべてのログまたはネットワーク イベントをダウンロードするオプションに加えて、バージョン11.5には、すべてのメタデータまた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ますが、バージョン11.4のメニューには、メタデータのオプションはありません。

【すべてのメタ】オプションと【表示可能なメタ】オプションの違いは、次のとおりです。

- バージョン11.4.1以降では、選択したイベントの表示可能なメタデータが、【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』)、またはダウンロード時に [ダウンロード]メニューの [その他のオプション]で選択した形式でダウンロードされます。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。表示可能な列は、選択した列グループと列セクターによって決定されます。列の選択の詳細については、「[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。[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。表示可能なメタのダウンロード]オプションのいずれかを使用すると、ダウンロードしたメタデータは、[イベント]パネルの現在のソート順ではなく、収集時間順でソートされます。

- バージョン11.5以降では、選択したイベントの表示可能なメタデータが、[イベント環境設定]メニューで選択したデフォルトの形式([テキスト形式のすべてのメタ』、『CSV形式のすべてのメタ』、『JSON形式のすべてのメタ』、『TSV形式のすべてのメタ』)、またはダウンロード時に [すべてダウンロード]メニューの [その他のオプション]で選択した形式でダウンロードされます。ダウンロードには、イベント リストに表示される列に関係なく、選択したイベントのメタデータがすべて含まれます。たとえば、メタ データベースに40個のメタ キーがある場合、列グループによりイベント リストに10個の列が表示されている場合でも、そのイベントの40個のメタ キーがすべてダウンロードしたファイルに含まれます。
- バージョン11.5.1以降では、選択したイベントの表示可能なメタデータが、[イベント環境設定]メニューで選択したデフォルトの形式([テキスト形式のすべてのメタ』、『CSV形式のすべてのメタ』、『JSON形式のすべてのメタ』、『TSV形式のすべてのメタ』、『ファイルのダウンロード』)、またはダウンロード時に [すべてダウンロード]メニューの [その他のオプション]で選択した形式でダウンロードされます。ダウンロードには、イベント リストに表示される列に関係なく、選択したイベントのメタデータがすべて含まれます。たとえば、メタ データベースに40個のメタ キーがある場合、列グループによりイベント リストに10個の列が表示されている場合でも、そのイベントの40個のメタ キーがすべてダウンロードしたファイルに含まれます。

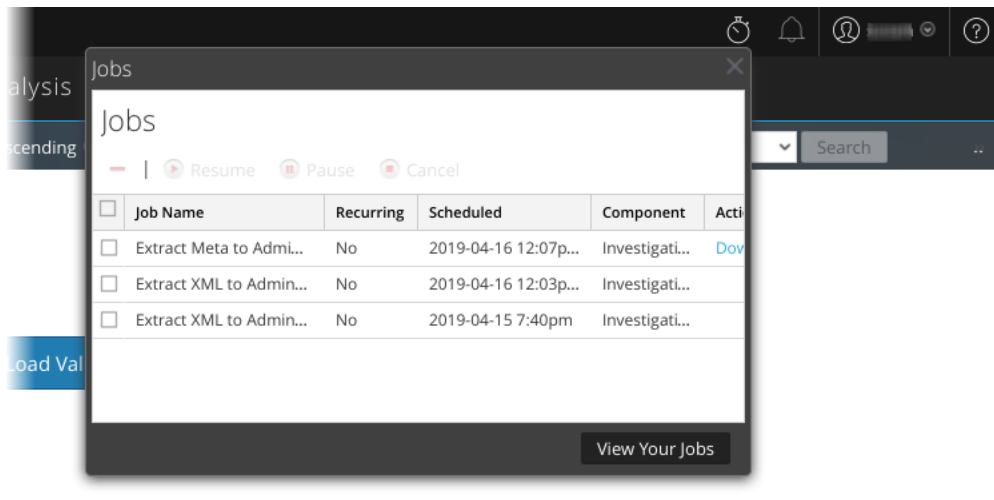
注：すべてのイベントをダウンロードするよう選択すると、現在の結果セット内のイベントのみがダウンロードされます。すべての結果が返される前にクエリをキャンセルした場合は、ロードされたイベントのみがダウンロードされます。

[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。

- 次のいずれかの操作を実行します。
 - 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隣にあるチェックボックスをオンにし、 [ダウンロード]メニュー ボタンの下向き矢印をクリックしてオプションを表示します。
 - [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、 [すべてダウンロード]メニュー ボタンをクリックします。
- 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別の形式を選択する場合は、[その他のオプション]で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別の形式を選択する場合は、[その他のオプション]で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。
 - すべてのメタデータが、[イベント環境設定]メニューで選択した形式(テキスト形式のすべてのメタ、[CSV形式のすべてのメタ]、[JSON形式のすべてのメタ]、[TSV形式のすべてのメタ]、[ファイルのダウンロード])でダウンロードされます。このダウンロードに別の形式を選択する場合は、[その他のオプション]でいずれかの形式を選択します。各イベントについてダウンロードされたメタデータには、表示可能な列だけでなく、すべてのメタデータが含まれます。
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 > )は、ブラウザウィンドウ内でただちにダウンロードが始まります。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。以下は、ダウンロードが失敗する理由の例です。時間経過によるタイムアウト、接続の失敗、イベント数の上限、アクセス拒否。
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** > **レガシーイベント** に移動し、ストップウォッチのような  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。



テキスト再構築でのログのダウンロード

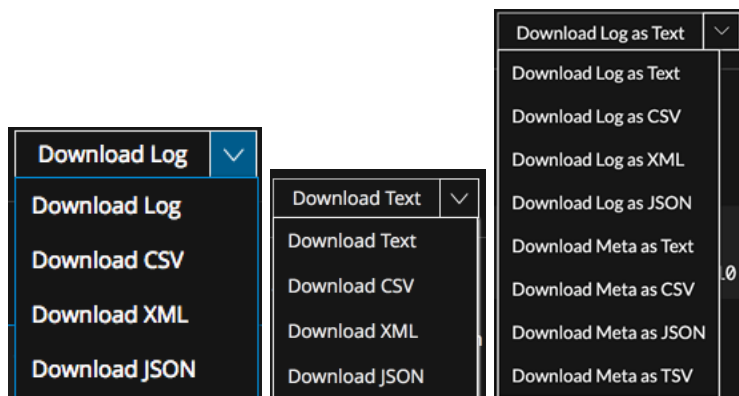
ログ イベントのテキスト再構築を表示しているときに、[ログのダウンロード]メニューのオプションを使用して、次の形式でログ ファイルをダウンロードすることができます。

- RAWログ(ログ)([ログのダウンロード](11.3)、**テキストのダウンロード**](11.4以降)、または **テキスト形式でログをダウンロード**](11.5以降) オプションを使用)。
- コンマ区切り値(CSV)([CSVのダウンロード]または [CSV形式でログをダウンロード](11.5以降) オプションを使用)。
- 拡張マークアップ言語(XML)([XMLのダウンロード]または [XML形式でログをダウンロード](11.5以降) オプションを使用)。
- JavaScriptオブジェクト表記(JSON)([JSONのダウンロード]または [JSON形式でログをダウンロード](11.5以降) オプションを使用)。

バージョン11.5以降では、次のいずれかのオプションを使用して、ログのメタデータをダウンロードすることもできます。

テキスト形式でメタをダウンロード]、**CSV形式でメタをダウンロード**]、**JSON形式でメタをダウンロード**]、**TSV形式でメタをダウンロード**]

以下は、[ログのダウンロード](11.3)、**テキストのダウンロード**](11.4以降)、**テキスト形式でログをダウンロード**](11.5以降) オプションを含むメニューの例です。バージョン11.5には、選択したログのメタデータをダウンロードするための追加オプションがあります。



注：エンドポイント イベントの場合、**[ログのダウンロード]**、**[テキストのダウンロード]**、または **[テキスト形式でログをダウンロード]** オプションは、256文字を超えるメタ値が少なくとも1つある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、以前にダウンロードされているファイルはダウンロードできません。たとえば、起動の引数のようなメタ値は256文字を超える場合があります。この場合、256文字はメタ値として使用できますが、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にファイル名が付けられます。RAWログのファイル名は次のようになります :Concentrator_SID2.log。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。使用可能なログタイプは、RAWログ、CSV、XML、JSONです。デフォルトの形式は、RAWログです。

注：いくつかの形式では、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。追加の情報は次の形式でログに含まれます :Log timestamp="1490824512" source="10.12.35.65".

ログまたはログのメタデータをダウンロードするには、次の操作を実行します。

ログ イベントのテキスト再構築で、次のいずれかを実行します。

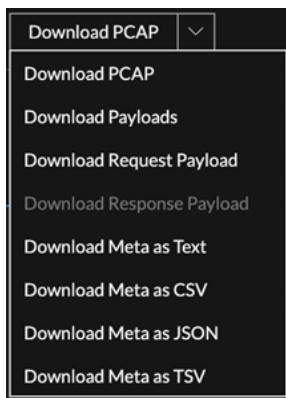
1. RAWログ(デフォルトの形式)でログをダウンロードするには、**[ログのダウンロード]**、**[テキストのダウンロード]**、または **[テキスト形式でログをダウンロード]** をクリックします。
2. 他のいずれかの形式でログをダウンロードするには、**[ログのダウンロード]**、**[テキストのダウンロード]**、または **[テキスト形式でログをダウンロード]** ボタンの下向き矢印をクリックし、ダウンロードするログのファイル形式を選択します。

3. ログのメタデータをダウンロードするには、**ログのダウンロード**、**テキストのダウンロード**、または **テキスト形式でログをダウンロード** ラベルの下向き矢印をクリックします。次に、**テキスト形式でメタをダウンロード**、**CSV形式でメタをダウンロード**、**JSON形式でメタをダウンロード**、または **TSV形式でメタをダウンロード** を選択します。

ログファイルまたはログのメタデータが、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。

テキスト再構築またはパケット再構築でのネットワーク イベント データのダウンロード

ネットワーク イベントのパケット再構築またはテキスト再構築を表示しているときに、詳細に分析するためにネットワーク データ ファイルをエクスポートすることができます。バージョン11.5以降では、再構築されたイベントのメタデータをダウンロードすることもできます。



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。
- (バージョン11.5) イベントのメタデータ。次のいずれかのオプションを使用。 **テキスト形式でメタをダウンロード**、**CSV形式でメタをダウンロード**、**JSON形式でメタをダウンロード**、**TSV形式でメタをダウンロード**

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。そのデータのタイプがイベントにない場合は、メニューボタンがグレー表示になります。メニューボタンの下向き矢印をクリックして、使用可能なオプションを確認することができます。たとえば、イベントにリクエストペイロードがあるが、レスポンスペイロードがない場合は、[レスポンスペイロードのダウンロード]ラベルがグレー表示になります。ボタンの下向き矢印をクリックし、このダウンロード用の[リクエストペイロードのダウンロード]を選択することができます。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次のようになります :C01 - Concentrator_SID1697309.pcap.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ない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としてエクスポートするか、イベントのメタデータをダウンロードするには、次の操作を実行します。

ネットワークイベントのパケット再構築に移動し、次のいずれかを実行します。

1. 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、ユーザー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。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。
2. 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。
3. 他のいずれかの形式でイベントのメタデータ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、ダウンロードするメタデータのファイル形式を選択します。

指定した形式でネットワークデータファイルがローカルファイルシステムにダウンロードされるか、指定された形式でイベントのメタデータがダウンロードされます。

ファイル再構築でのネットワークイベントからのファイルのダウンロード

ファイル再構築の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つ以上のファイルまた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。

The screenshot shows the 'Network Event Details' window with the 'File' tab selected. A 'Download Files (2)' button is visible. Below it, a summary table shows session details for session ID 9. A warning message states: 'Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data. To avoid quarantine, the zip file is password protected with this password: netwitness.' Below the warning is a table of files for download.

FILE NAME	MIME TYPE	FILE SIZE	HASHES
words.txt	text/plain	1.0 KB	SHA1: 5da32e1be64e159733a39ede07dd1d3d8f83cc01 SHA256: a5e3aba74847e34edee282bd666d3a7606393118b0874e63682 MD5: d881c34fa5283a3e8a0cd9f973d0c495
related_patch	application/octet-stream	33.4 KB	SHA1: 9eb585a98f83d0e05e6a81b0b71406778d35b6ec SHA256: 359641873610597882317aee0f72104ed54fe8aa82d6fa323a54 MD5: 5ffd2afab8388f042296b32368b6e0e1

[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。

ファイル再構築からファイルをダウンロードする場合、エクスポートされるアーカイブの形式は<service-name>SID<service ID><file-count> FILES FILESです(例 :Broker_SID8_1_FILES_FILES.zip)。zipアーカイブを開くためのパスワードは"netwitness" です。

<service-ID or host name>_SID<n>_<file-count>FILES_FILES.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。
- <file-count> FILESは、アーカイブ内のファイルの数です。
- FILESは、ファイルのダウンロード元の再構築タイプを示します。

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。

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、ファイルを含むイベントのファイル再構築に移動します。

Network Event Details | Text Packet **File** Email Web

Download Files (2)

SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME	LAST PACKET TIME
9	192.168.14 :1470	:587	25	05/22/2020 04:11:07 am	05/22/2020 04:11:07 am

CALCULATED PACKET SIZE: 49693 bytes
CALCULATED PAYLOAD SIZE: 45353 bytes
CALCULATED PACKET COUNT: 78

Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data. To avoid quarantine, the zip file is password protected with this password: netwitness.

FILE NAME	MIME TYPE	FILE SIZE	HASHES
<input checked="" type="checkbox"/> words.txt	text/plain	1.0 KB	SHA1: 5da32e1be64e159733a39ede07dd1d3d8f83cc01 SHA256: a5e3aba74847e34edee282bd666d3a706393118b0874e63682 MD5: d881c34fa5283a3e8a0cd9f973d0c495
<input checked="" type="checkbox"/> related.patch	application/octet-stream	33.4 KB	SHA1: 9eb585a98f83d0e05e6a81b0b71406778d35b6ec SHA256: 359641873610597882317aee0f72104ed54fe8aa82d6fa323a54 MD5: 5ffd2afab8388f042296b32368b6e0e1

9 of 2,001 events

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、次のパスワードを入力します :netwitness.

メール再構築からの添付ファイルのダウンロード

添付ファイルを含むメール再構成を表示しているときに、1つ以上の添付ファイル、またはすべての添付ファイル(バージョン11.4.1.x)を選択してローカルファイルシステムにダウンロードできます。この機能により、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。

メール再構築からファイルをダウンロードするときのファイル名の形式は<service-name>_SID<n>_EMAILです(例 Broker_SID34_EMAIL.zip)。zipアーカイブを開くためのパスワードは"netwitness"です。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>_EMAIL.zip

各項目の意味は次のとおりです。

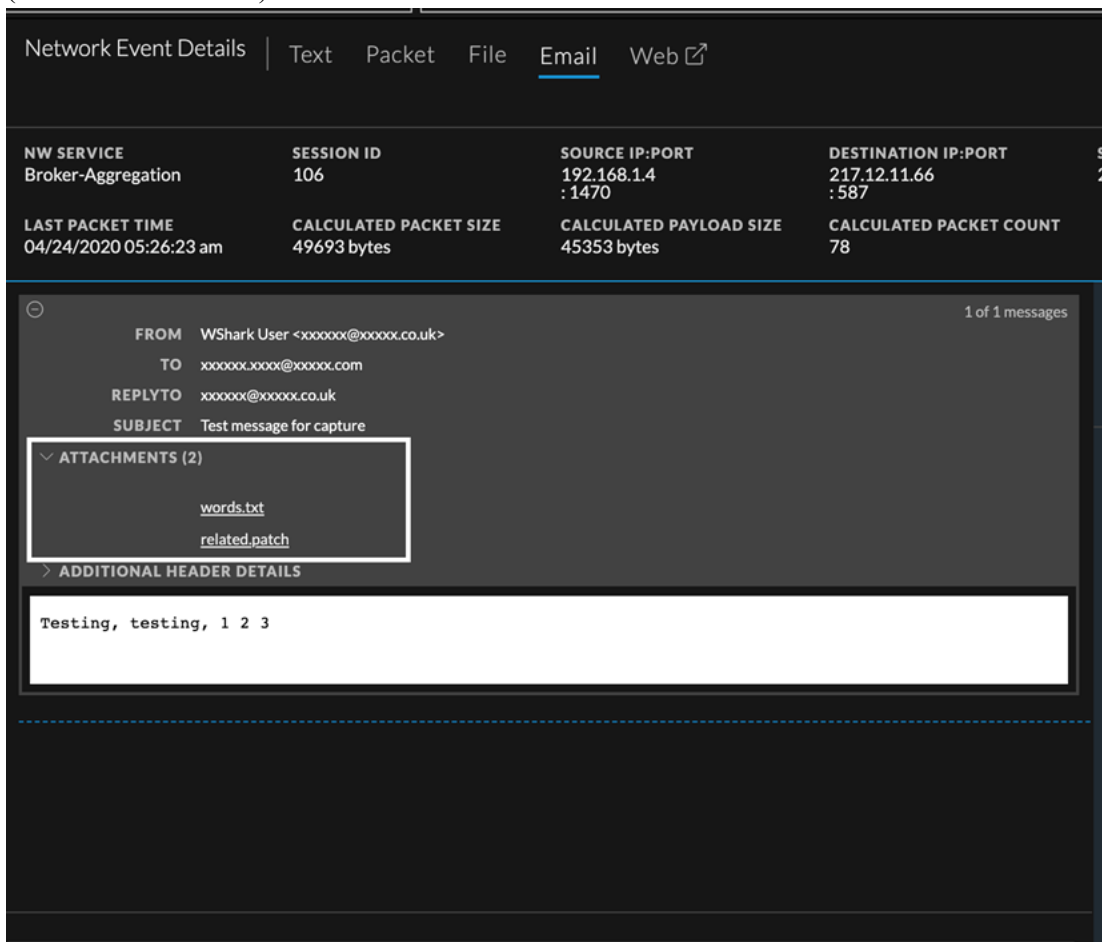
- <service-ID or host name>は、セッションが保存されたサービスの名前(たとえばConcentratorまたはBroker)です。
- SID<n>は、セッションID番号です。
- EMAILは、ファイルのダウンロード元の再構築タイプです。

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。

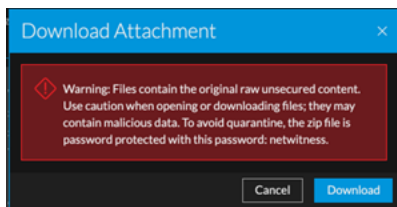
メールの添付ファイルをダウンロードするには、次の操作を実行します。

1. **イベント**ビューに移動し、ファイルが添付されたメールを含むイベントをクリックしてメール再構築を開きます。

2. **添付ファイル**ドロップダウン リストを展開し、次のいずれかを実行します。
 - a. (バージョン11.5以降) 添付ファイルへのリンクをクリックします。



ダウンロードするメールの添付ファイルに、悪意のあるデータが含まれている可能性があることを警告するダイアログが表示され、ダウンロードのキャンセルまたは確定が求められます。ダウンロードを実行する場合は **ダウンロード** をクリックします。それ以外の場合は、 **キャンセル** をクリックしてダウンロードをキャンセルします。



- b. (バージョン11.4.1.x) 1つ以上の添付ファイルまたは **すべての添付ファイル** を選択します。

The screenshot shows the 'Network Event Details' view for an email. The 'Email' tab is selected. A 'Download File' button is visible. Below the button is a table with the following data:

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT
bro - Broker	11403	:25	:23946
LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
02/13/2008 04:55:17 pm	88633 bytes	82079 bytes	112

A warning message is displayed in a red box: "Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data." Below the warning is an email preview with the following headers:

FROM: [redacted]
 TO: [redacted]
 REPLY TO: [redacted]
 CC: [redacted]
 SUBJECT: Resume for [redacted]

Under 'ATTACHMENTS', there are two items: 'All Attachments' and 'Resume for [redacted]', both with checked boxes. Below the attachments is a link for 'ADDITIONAL HEADER DETAILS'. The email body text is:

Good morning, All
 [redacted] asked me to send
 Thank you,
 [redacted]

再構築に警告メッセージが表示されます。[ファイルのダウンロード]または[ファイルのダウンロード]ボタンをクリックします。添付ファイルがダウンロードされ、これ以降にキャンセルすることはできません。

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。

- セッションからファイルを抽出します。抽出するファイルのタイプを選択します。(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) が指定できます。
- 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。

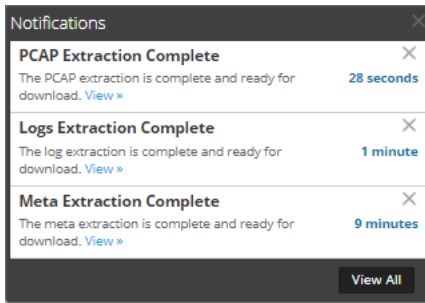
エクスポートされる内容は、エクスポートするときの時間範囲やドリルダウン ポイントによって変わります。

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では、ツールバーで、**アクション]** > **エクスポート]**を選択して、エクスポート オプションのいずれかを選択します。**PCAP]**、**ログ]**、**メタ]**のいずれかです。
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では、ツールバーで、**イベントの保存]**を選択して、エクスポート オプションのいずれかを選択します。**PCAP]**、**ログ]**、**ファイル]**、**メタ]**のいずれかです。
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。
 - ログのエクスポート形式：**Text]**、**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。
 - メタフォーマット：**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を開き、ツールバーの [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。

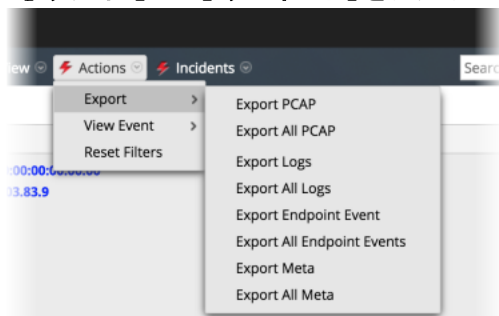
エクスポート機能では、サービスのクエリを実行し、選択した時間範囲とドリルダウンポイントで指定したセッションをPCAPファイルにエクスポートします。エクスポートされる内容は、エクスポートするときの時間範囲やドリルダウンポイントによって変わります。[ファイルの抽出]ダイアログでは、次の項目を選択してエクスポートできます。

- PCAP
- ログ
- NetWitness EndPointイベント
- メタ値

エクスポートす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：管理者が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。

<input checked="" type="checkbox"/>	COLLECTION TIME	TYPE	SERVICE TYPE	ORIGINATING IP	SOURCE IP	DESTINATION IP	TCP DESTINATION	DESTINATION	HOSTNAME	SO
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		
<input checked="" type="checkbox"/>	05/28/2019 09:12:26 am	Log			10.101.47.66			6667		

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。

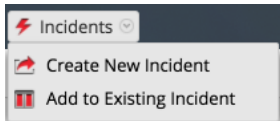
- a. 重大度を選択します。アラート サマリー フィールドの値は事前に定義されており、自動入力されますが、必要に応じて編集することができます。
 - b. **【インシデント名】**フィールドに、インシデントの名前を入力します。
 - c. **【優先度】**ドロップダウン リストから、インシデントの優先度を選択します。たとえば、インシデントはクリティカル、高、中、低の優先度の場合があります。
 - d. インシデントの割り当て先をドロップダウン リストから選択します。このリストには、InvestigateIにアクセスできる組み込みのユーザと、システムに追加されたカスタム ユーザが含まれます。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】**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ー管理ガイド』にある「ロールの権限」と「ロールと権限によるユーザーの管理」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 screenshot of the 'Create an Incident' dialog box. The dialog has a title bar 'Create an Incident' and a close button. The main content area is titled 'Create An Alert From These 1 Events:'. It contains several input fields: 'Alert Summary' (Manual alert for Last 3 Hours), 'Severity' (50), 'Name' (Test Event for Documentation), 'Summary' (Creating an alert for this event.), 'Assignee' (Admin), 'Categories' (Social: Other), and 'Priority' (High). At the bottom, there are 'Cancel' and 'Save' buttons.

- 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]フィールドでインシデントについて説明します。
- 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。準備ができたなら、**「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 [ガシー イベント]ビューの問題


動作	<p>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メタキーの後に次のメッセージが表示されます。Service Type[service] Not Indexed.</p> 
問題	<p>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。</p>
説明	<p>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。</p>

メッセージ	<p>Not indexed; will experience longer than usual load times. ([メタグループの管理]ダイアログ)</p>
問題	<p>[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。</p> <p>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。</p> <p>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。</p>
説明	<p>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、再起動します。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。</p>

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 User Guide」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	同じクエリの結果を表示する場合、「イベントの絞り込み」パネルと「イベント」パネルのイベント数が異なることがあります。
問題	「イベントの絞り込み」パネルは、インデックスデータのみを使用してイベントのカウントを生成し、「イベント」パネルよりも精度が低くなります。「イベント」パネルの結果は、メタデータベースから取得したデータと完全に一致するようにフィルタを適用されるため、処理に時間

	がかかります。
説明	最悪の場合、違いは検出漏れではなく、[イベントの絞り込み]パネルの誤検出にあります。そのため、イベントを見落とすことはありません。

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 <i>Physical Host Upgrade Guide</i>).
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。

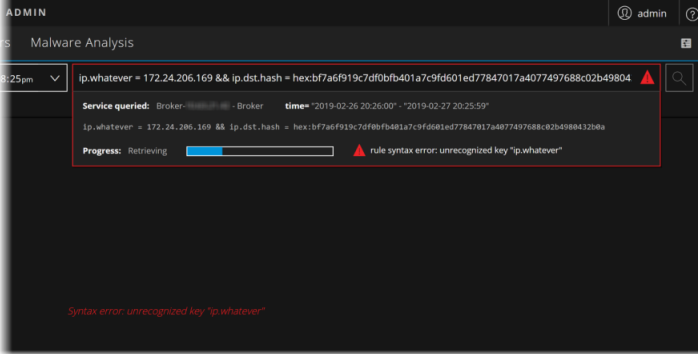
メッセージ	Insufficient permissions for the requested data.
問題	[イベント]ビューでイベントにアクセスしようとすると、このメッセージが表示されます。
説明	表示する権限がないイベントのイベントIDを入力しました。アクセスを制限するために、管理者がロールと権限により制限を設けた可能性があります。

メッセージ	Invalid session ID: <<eventId>>
問題	クエリを実行した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。

動作	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。
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 <XXXXXXX> 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	<pre>Rule Syntax error: Unrecognized key "<meta key or meta entity name>" Syntax error: Unrecognized key "<meta key or meta entity name>"</pre>
問題	<p>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。</p>  <p>The screenshot shows a query in the console: <code>ip.whatever = 172.24.206.169 && ip.dst.hash = hex:bf7a6f919c7df0bfb401a7c9fd601ed77847017a4077497688c02b49804</code>. Below the query, a message states: <code>Service queried: Broker - Broker time= "2019-02-26 20:26:00" - "2019-02-27 20:25:59"</code>. A progress bar is shown with the text <code>Progress: Retrieving</code>. At the bottom, a red error message reads: <code>Syntax error: unrecognized key "ip.whatever"</code>.</p>
説明	<p>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。</p>


メッセージ	<pre>Selected Column Group is no longer available. The default summary column group has been selected instead.</pre>
問題	<p>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。</p>
説明	<p>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。</p>

メッセージ	<pre>Session is unavailable for viewing.</pre>
問題	<p>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。</p>
説明	<p>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。</p>

メッセージ	<pre>The query on channel <channel-number> was auto-canceled by the system for exceeding time usage limits. Check timeout values. Query running</pre>
-------	---

シ	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分を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。

問題	[調査] > [イベント]ビュー > [ホスト]タブで使用可能な一致するエンドポイント データがありません。
----	--

次のいずれかの理由により、エンドポイント データが利用できない場合があります。

- **エンドポイントが導入されていない** – Endpoint Log Hybridをインストールする必要があります。『物理ホスト インストールガイド』の「RSA NetWitness Endpoint」を参照してください。
- **選択したネットワーク イベントに関連づけられたホストのエンドポイント データが収集されていない** - NetWitness Endpoint Agentがインストールされていること、およびネットワーク イベントを追跡するように拡張ネットワーク可視性が構成されていることを確認します。拡張ネットワーク可視性を有効にするには、『NetWitness Endpoint構成ガイド』の「グループとポリシーの作成」を参照してください。

注：拡張ネットワーク可視化を使用する場合は、Endpoint Log DecoderのデータをEndpoint Concentratorで集計するために使用するサービス ユーザー アカウントに、decoder.manage権限が割り当てられている必要があります。ロールと権限を割り当てる方法の詳細については、『RSA NetWitness Platformホストおよびサービス スタート ガイド』の「サービスの [セキュリティ]ビュー - Aggregationロール」を参照してください。

- **ConcentratorまたはEndpointサービスがオフラインであるか、非常に遅い** – ヘルス モニターのサービスのステータス(オンラインまたはオフライン)を確認する必要があります。サービスがオンラインの場合は、Endpointサーバ ログと(Endpoint) Concentratorログで詳細を確認する必要があります。
- **選択したネットワーク イベントに関連づけられたホストのEndpointデータがロールオーバーされている** - 設定されたデータ保持期間により、Endpointデータがロールオーバーされる場合があります。エンドポイント データを長期間保持できるよう、データ保持期間を構成する必要があります。詳細については、『データ プライバシー管理ガイド』の「データ保持の構成」を参照してください。

調査の参考情報

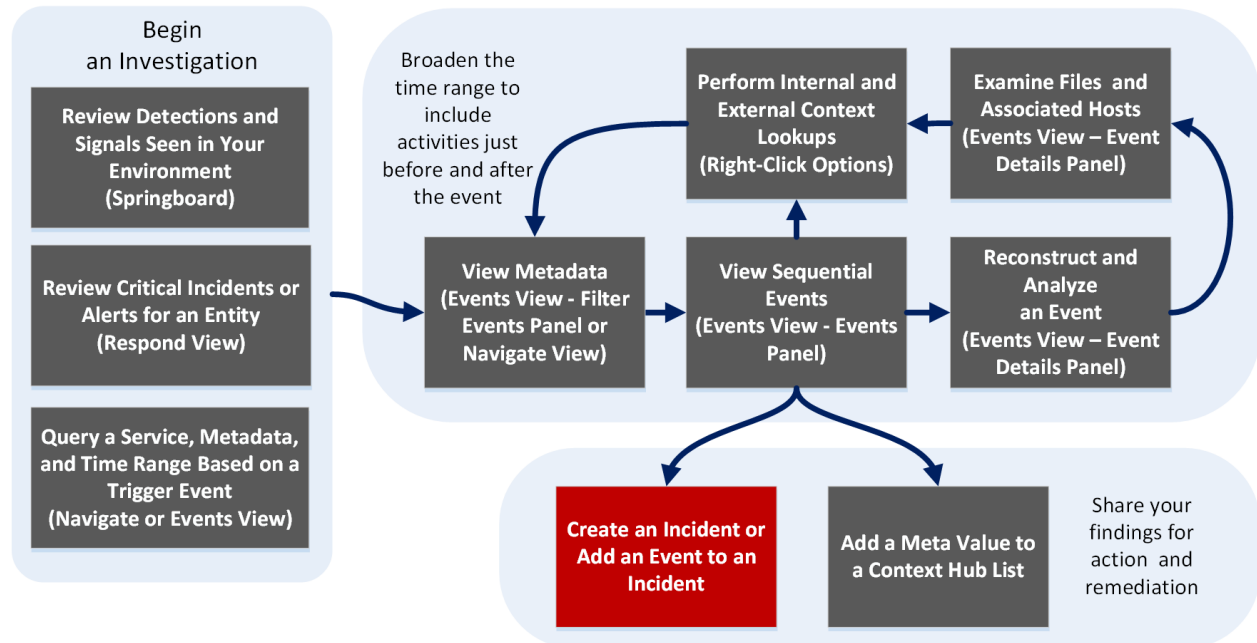
このセクションでは、NetWitness 調査]ビューの目的と用途について説明します。各ビューについて、その概要と、関連する手順へのリンクが記載された「実行したいことは何ですか？」の表を示します。また、参考情報の一部には、ワークフローと、ユーザ インタフェースでの重要な機能をハイライト表示するクイック ルックが含まれます。

- [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\]タブ](#)
- [イベント\]ビュー - テキスト\]タブ](#)
- [イベント\]ビュー - パケット\]タブ](#)
- [イベント\]ビュー - ファイル\]タブ](#)
- [調査\]ダイアログ](#)
- [調査\]タブ - ユーザー環境設定\]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\]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



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
インシデント対応者 脅威ハンター	重要なインシデントまたはアラートの確認 サービス、メタデータ、時間範囲のクエリを実行	NetWitness Respond ユーザー ガイド 「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

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	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストの調査	[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

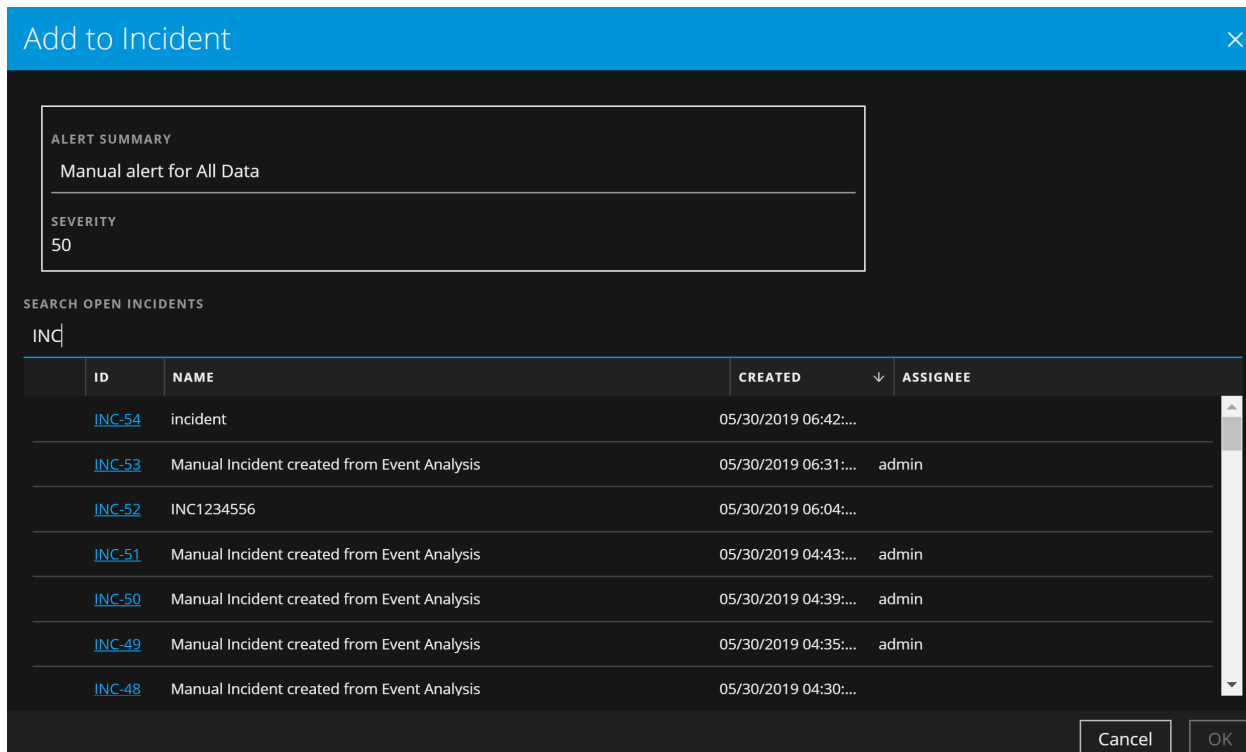
次の図は、レガシー イベントの [イベントをインシデントに追加] ダイアログの例です。表に、[イベントをインシデントに追加] ダイアログの情報およびオプションについて説明します。

	ID	Name	Date Created	Priority
<input checked="" type="checkbox"/>	INC-16	Test Event for Documentation	2017/07/18 15:07	High
<input type="checkbox"/>	INC-15	Test Disable Rule	2017/07/18 13:47	Critical
<input type="checkbox"/>	INC-14	Test Rule	2017/07/18 13:42	Critical
<input type="checkbox"/>	INC-13	Test last 48 hrs	2017/07/18 13:24	Critical
<input type="checkbox"/>	INC-12	Test New Rule	2017/07/18 12:41	Critical
<input type="checkbox"/>	INC-11	High Risk Alerts: ESA	2017/07/18 12:35	Critical
<input type="checkbox"/>	INC-10	test	2017/07/18 12:09	Critical
<input type="checkbox"/>	INC-9	Incident	2017/07/18 11:55	Critical
<input type="checkbox"/>	INC-8	Test Broker Service	2017/07/18 11:53	Medium
<input type="checkbox"/>	INC-7	Test New	2017/07/18 11:48	Medium

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の整数が表示されます。
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。
優先度	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の整数が表示されます。
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。

機能	説明
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。
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

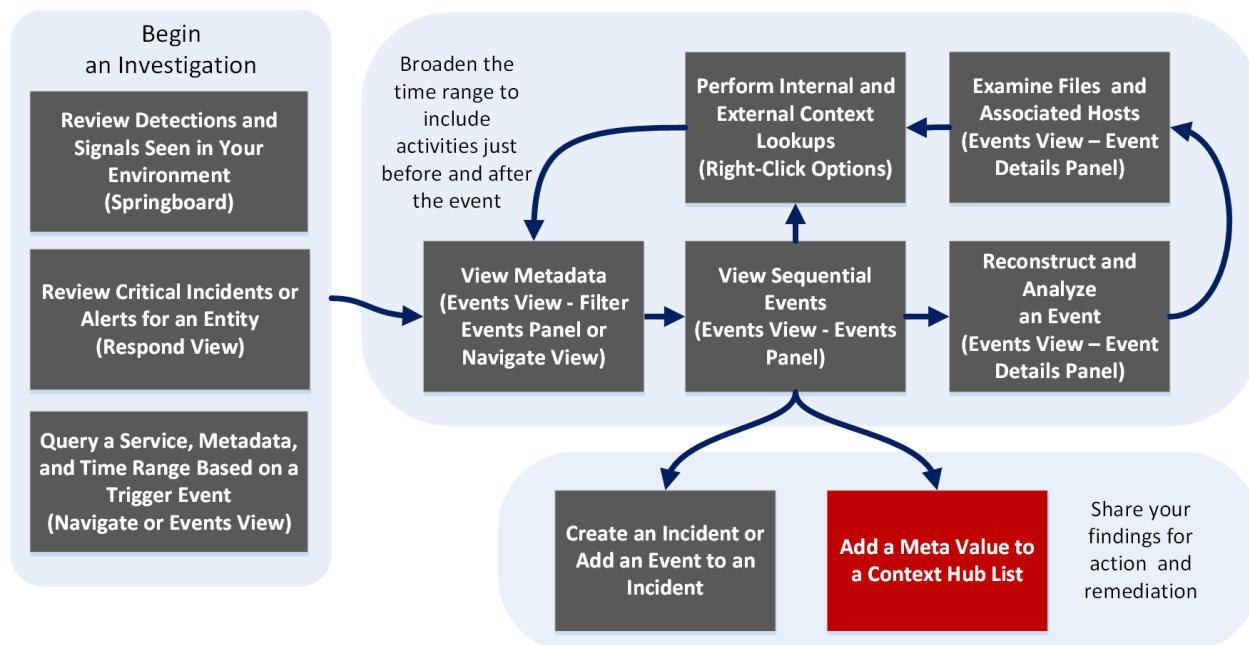
「リストへの追加/削除」ダイアログを使用すると、既存のContext Hubリストに対してエンティティもしくはメタ値を追加し、エンティティもしくはメタ値を削除し、またはエンティティもしくはメタ値を含む新しいContext Hubリストを作成できます。疑わしいIPアドレスや注意が必要なIPアドレスやその他のエンティティを見つけたときは、データソースとして追加されているリストにそのIPアドレスを追加できます。一般的に使用されるリストには、ホワイトリストやブラックリストがあります。これにより、疑わしいIPアドレスの可視性が向上し、誤検知が減るため、余計な調査の必要がなくなります。

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



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
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 ユーザー 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	メタデータの表示	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストの調査	[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

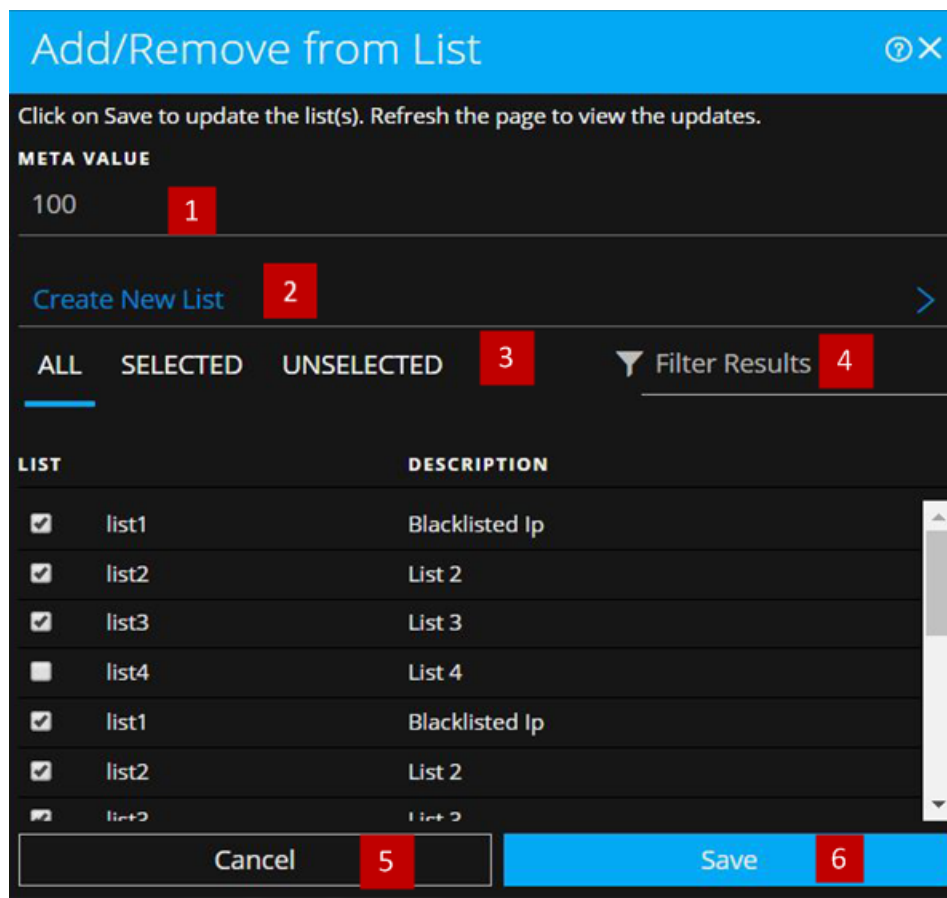
*このタスクは現在のビューで実行できます。

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 任意のタブを選択します。[すべて]、[選択済み]、[未選択]のいずれかです。
- 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。
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。」以下に例を示します。「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。」
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
----	----

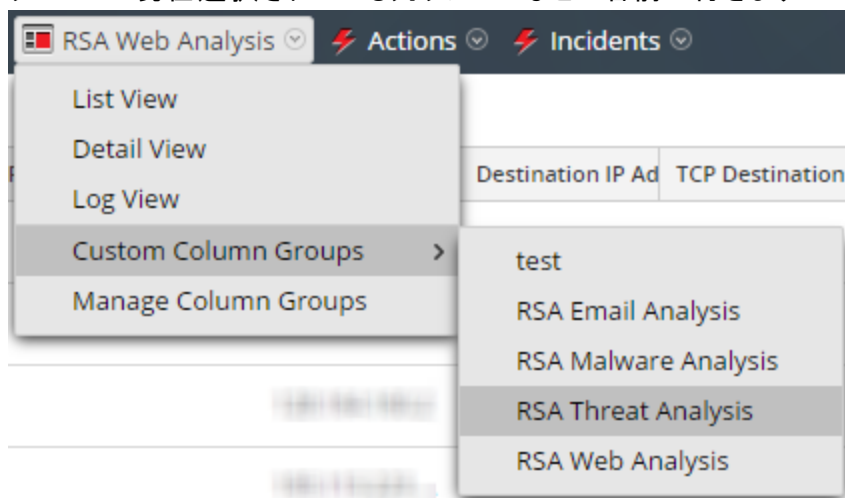
機能	説明
メタ値	既存のリストまたは新しいリストに追加される選択したメタ値。
リスト	選択したメタ値を追加するリスト。ドロップダウンメニューには、メタ値を追加できるリストが示されます。
新しいリストの作成	選択したメタ値を追加する新しいリストを作成するダイアログが開きます。
リスト名	新しいリストの名前。
説明	新しいリストの説明。
を作成	必須入力フィールドを入力した後に新しいリストを作成します。
戻る	新しいリストの作成をキャンセルし、元のダイアログに戻ります。
キャンセル	リストへのメタ値の追加をキャンセルし、ダイアログボックスを閉じます。
保存	リストに加えた変更を保存し、ダイアログを閉じます。

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以降の [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以降の [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]オプションは、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などの名前が付きます。



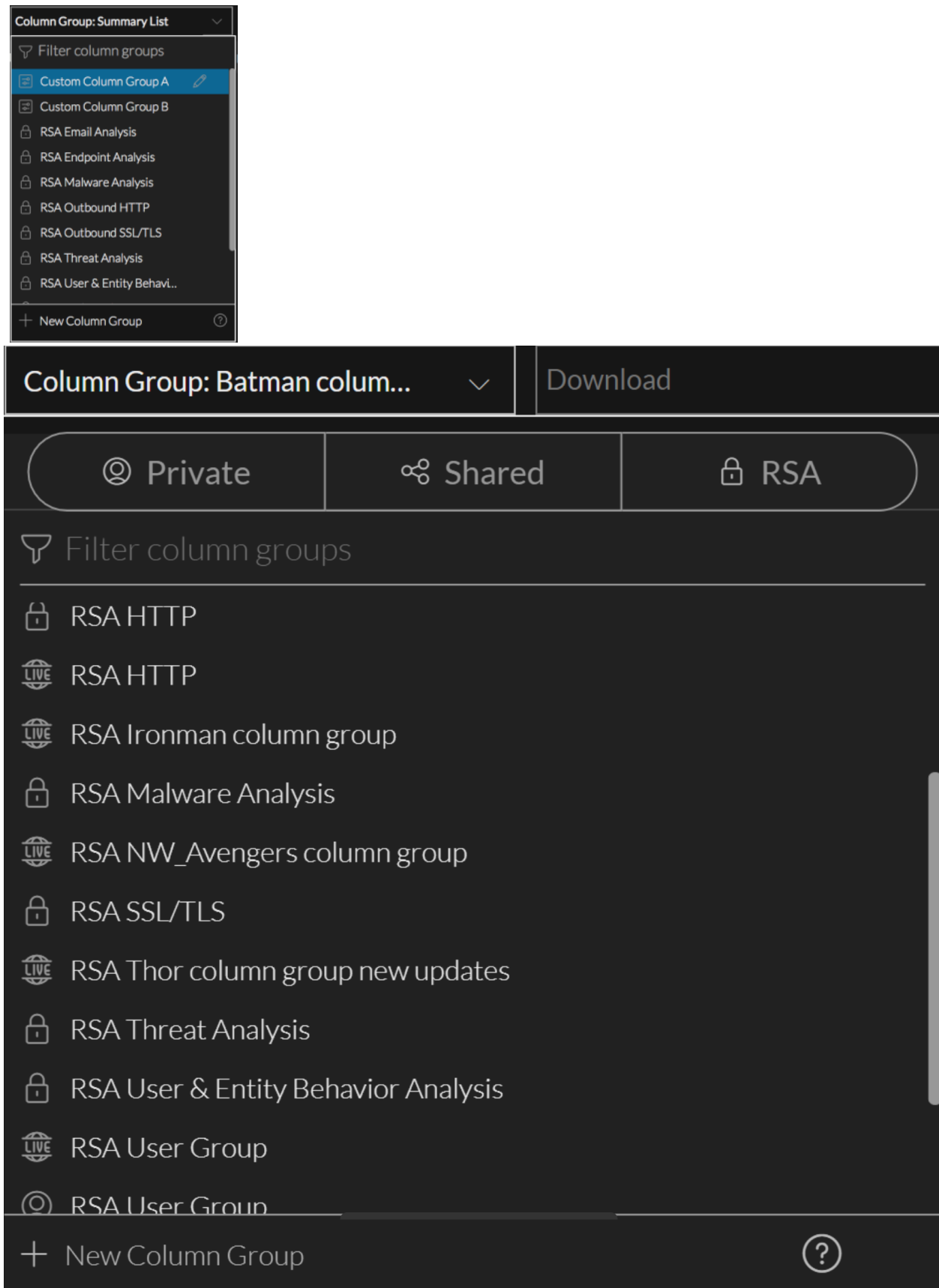
列グループを定義したら、調査の他のビューでも使用できます。[ナビゲート]ビューでは、クエリプロファイルを使用して、プロファイルの適用時に使用する列グループを選択できます。[イベント]ビューと[レガシー イベント]ビューでは、[イベント]パネルに適用する列グループを選択できます。

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](#)

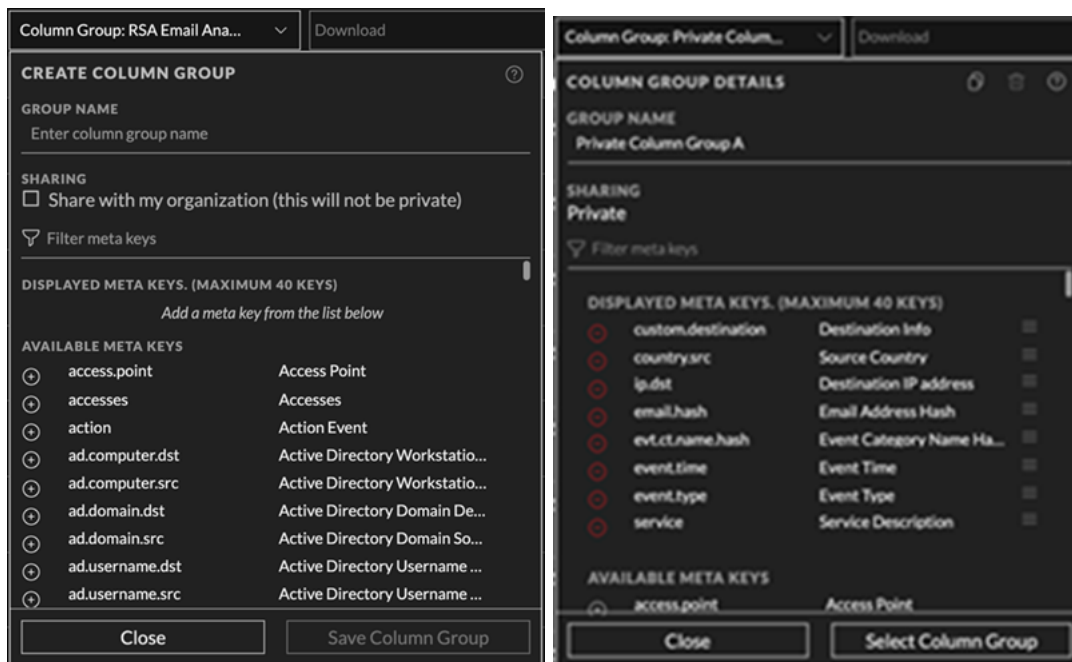
簡単な説明 - [列グループ]メニュー、[列グループの作成]ダイアログ、[列グループの詳細]ダイアログ





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(バージョン11.4)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。右側の例(バージョン11.5)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。次の表に、オプションの説明を示します。



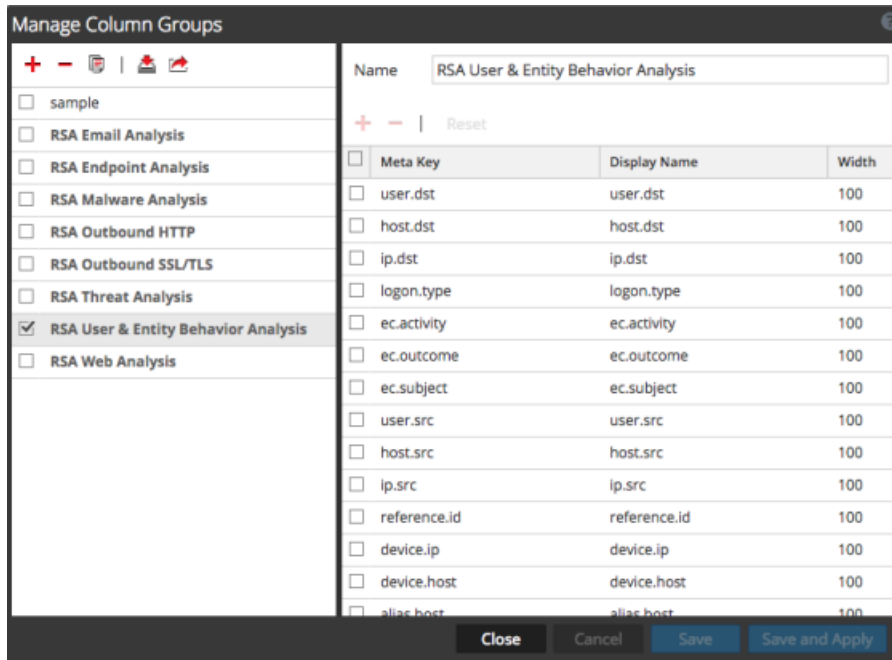
機能	説明
可視性オプション	(バージョン11.5以降)リストに表示される列グループのタイプを制御するには、表示オプションを任意に組み合わせて使用します(青 = 選択済み、黒 = 未選択)。 プライベート = 自分だけが管理できるプライベートグループを表示 共有 = 組織内の誰でも管理できる共有グループを表示 RSA = RSAのみが管理できる標準提供グループを表示 表示オプションは [列グループの絞り込み] フィールドと連動します。表示オプションによって標準提供グループ(グループ名に「RSA」を含むグループ)が非表示になっている場合に、「RSA」を含んだ名前を検索すると、リストは空になります。
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。バージョン11.5以降では、カスタムグループを共有またはプライベートにすることができます。「RSA」で始まる列グループは標準提供列グループです。プライベート カスタムグループ、共有カスタムグループ、標準提供グループはアイコンで区別されます。
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。
共有	バージョン11.5以降では、共有またはプライベートの列グループを作成できます。この設定は、初めてグループを作成するときに使用できます。作成後、共有列グループをプライベートに変更したり、プライベート列グループを共有に変更したりすることはできません。
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。
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。この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。

アクション	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。
	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。

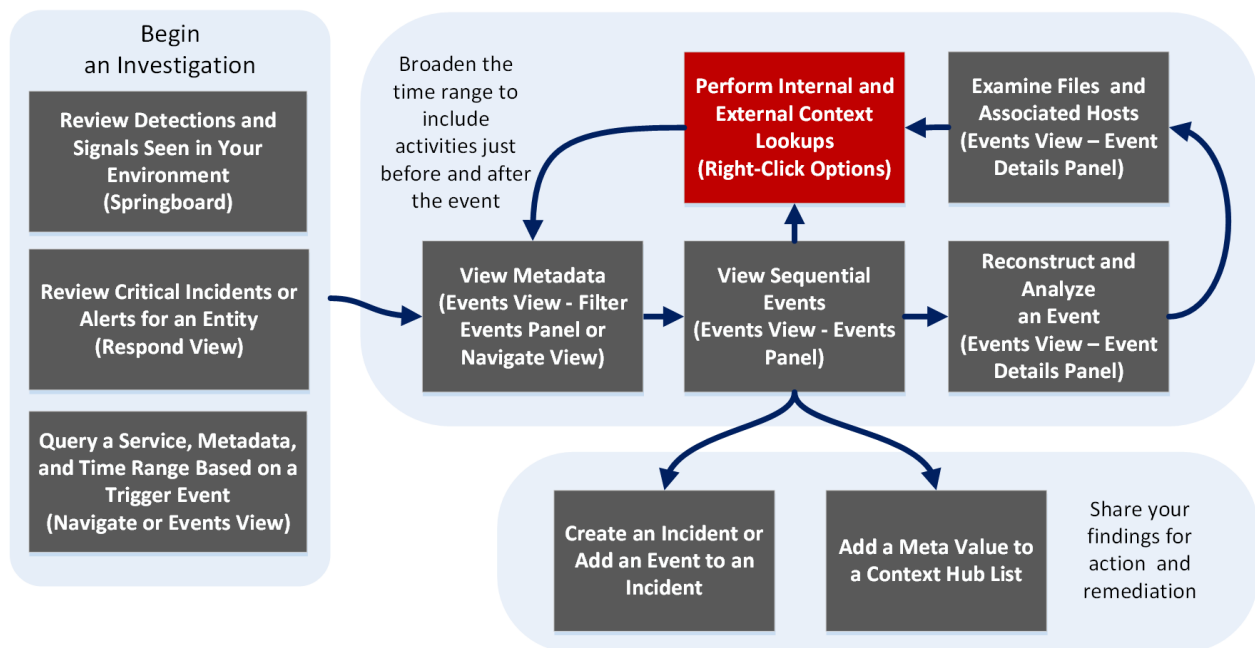
「コンテキスト ルックアップ」パネル

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」ビューで開いたときとは、「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



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	NetWitness Platform スタート ガイド

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 ユーザー 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	メタデータの表示	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストの調査	[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

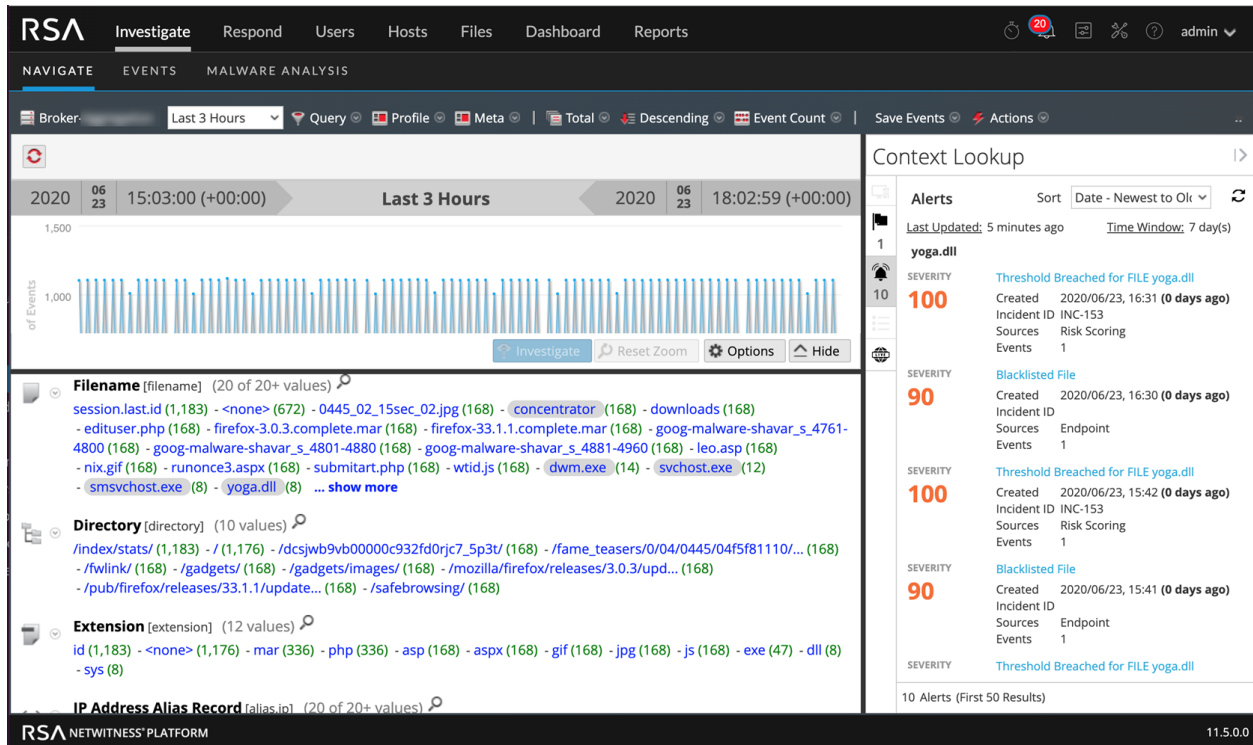
*このタスクは現在のビューで実行できます。


関連トピック

- [NetWitness Investigateの仕組み](#)
- [\[レガシー イベント\]ビュー](#)
- [\[ナビゲート\]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	使用可能なソースのアイコンが表示されます。エンドポイント、インシデント、アラート、リストを示します。
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。 <ul style="list-style-type: none"> • エンドポイント • インシデント • アラート • リスト • Live Connect
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。

機能	説明
<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
- 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] のトピック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] のトピック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

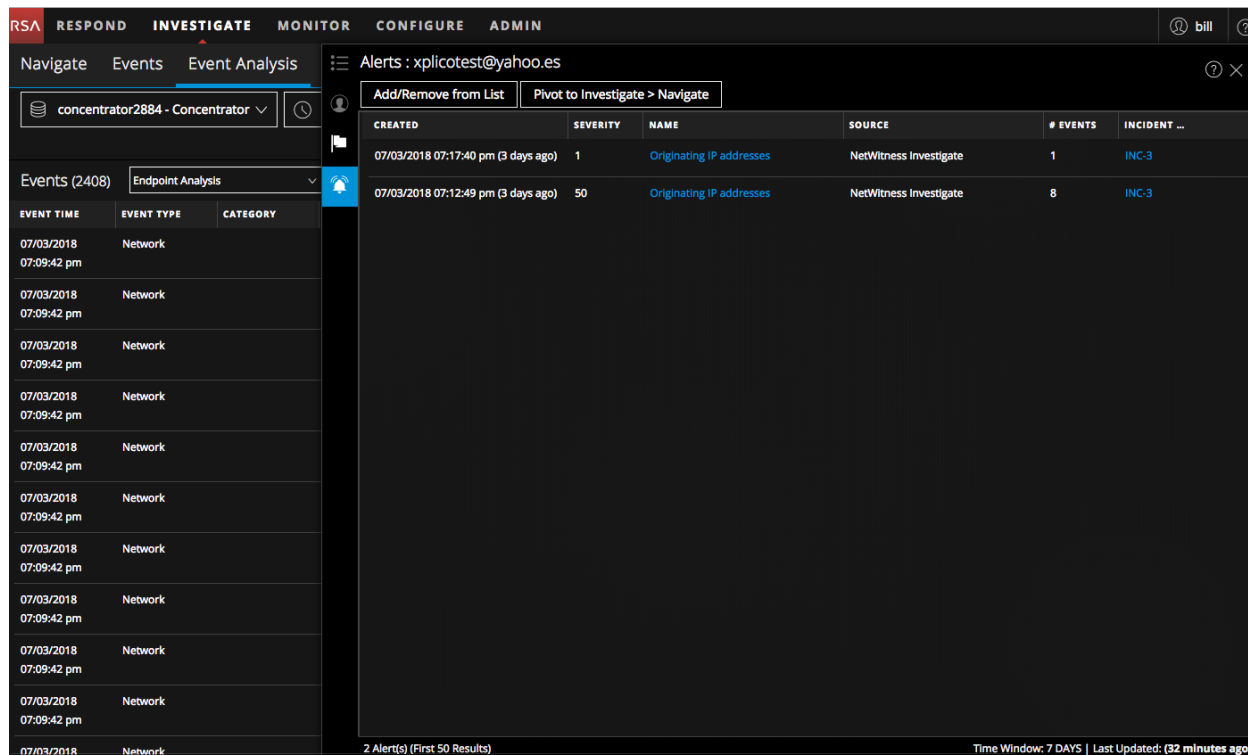
エンドポイント

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。

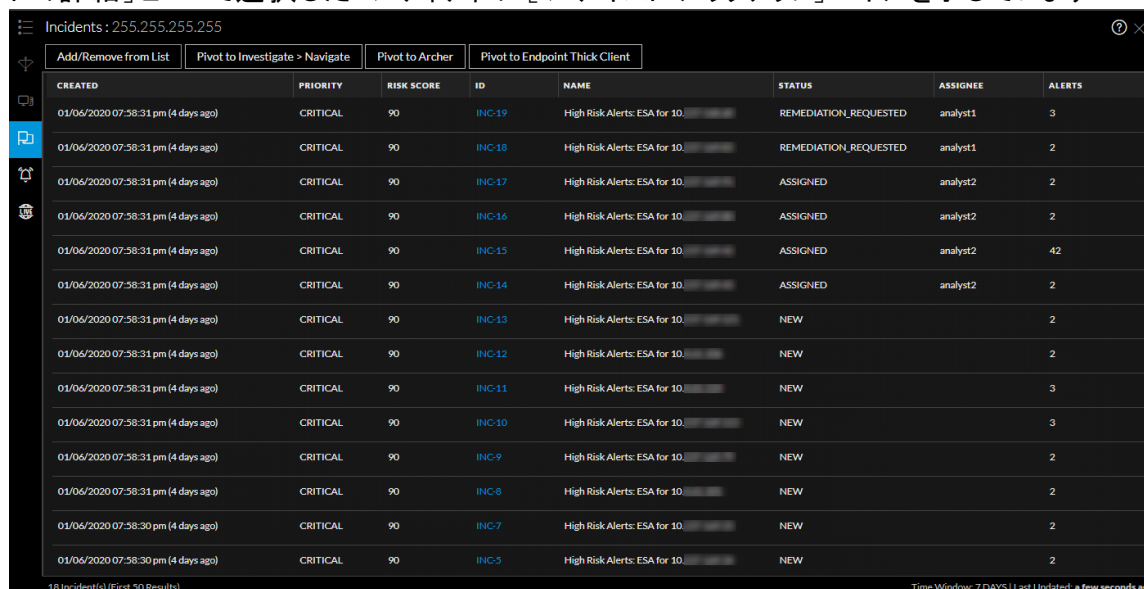
- **マシン名とマシンのIPアドレス**。
IPまたはエンドポイント マシン名をクリックすると、エンドポイントUIに移動してさらに詳しい調査を実行できます。
- **更新日** :コンテキスト データを最後にデータ ソースからフェッチして、キャッシュを更新した時刻を示します。
- **マシン スコア** :マシンHIOCスコアは、モジュールのスコアに基づいて集計されます。
- **モジュールの数** :選択したマシンのアクティブなファイルの数。
- **更新日** :エンドポイント データベースのスキャン結果が最後に更新された時刻を示します。
- **最後にログインしたユーザ**
- **マシンの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(HIOC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HIOC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HIOCスコア** のデフォルト値は500です。
- **マシンHIOC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】、【REST API】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。



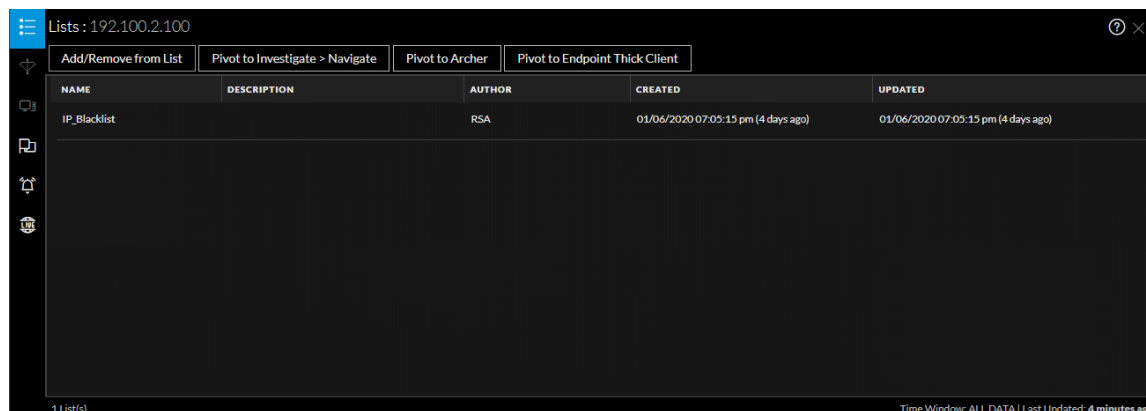
次の表は、各タブおよびサポートされるエンティティで使用可能なデータを示しています。

タブ	説明	サポートされるエンティティ
 (Lists)	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IIOCレベルの順にソートされます。	IP、MACアドレス、ホスト
 (Incidents)	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
 (Alerts)	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

タブ	説明	サポートされるエンティティ
 TI	STIXデータソースの情報を表示します。	IPアドレス、メール アドレス、ドメイン、ファイル名、URL、ファイル ハッシュ。 注：メール アドレスとURLのコンテキスト ルックアップは、これらのメタがマップされている場合にのみ表示されます。  (管理)] > システム] > 調査] > コンテキスト ルックアップ] に移動します。
 REST API	選択したエンティティに関連づけられているREST API(Context Hubで有効) のリストを表示します。	すべてのエンティティ

「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。
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。

フィールド	説明
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。

The screenshot shows the Archer tab interface with the following data:

CRITICALITY RATING	RISK RATING	DEVICE NAME	HOSTNAME
High	High	ECAT-WIN-2008	ftp.netwitness.com
INTERNAL IP ADDRESS	DEVICE ID	DEVICE TYPE	MAC ADDRESS
66.104.20.243	224935	Fibre Channel SAN Switch	00:13:E8:AF:68:0F
FACILITY	BUSINESS UNIT	DEVICE OWNER	BUSINESS PROCESSES
Austin D2	US-Finance,Payroll	1, Admin1,2, admin	Busi. Process 1, Busi. Process 2

1 Asset | Time Window: ALL DATA | Last Updated: (a few seconds ago)

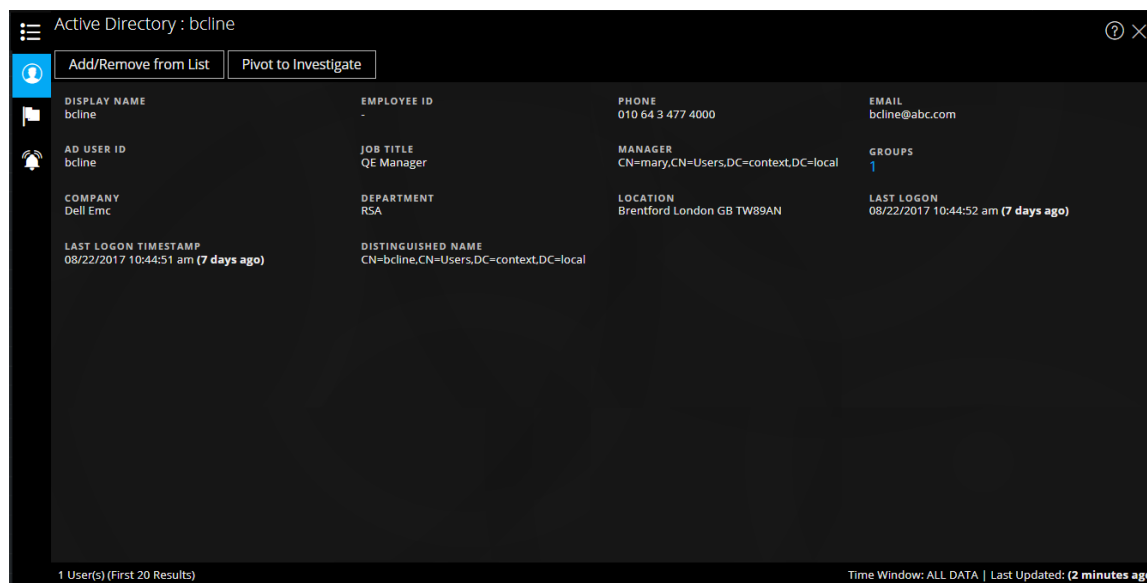
フィールド	説明
重要度評価	デバイスがサポートするアプリケーションに基づいて算出されたデバイスの業務上の重要度。重要度評価は、未評価、低、中-低、中、中-高、高のいずれかに設定できます。
Risk Rating	最新のアセスメント結果と、このデバイスを使用する施設の平均リスク評価から、デバイスのリスク評価を計算します。リスク評価は、重大、高、中、低、軽微のいずれかに設定できます。
デバイス名	デバイスの固有の名前。
host Name	デバイスのホスト名。
IPアドレス	デバイスのプライマリ内部IPアドレス。
デバイスID	システム内のすべてのアプリケーションにおいてデバイスレコードを一意に識別する、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。

フィールド	説明
施設	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	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：ローカライズバージョンでは、次の12個のフィールドのみが表示されます。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、およびビジネス プロセス。

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

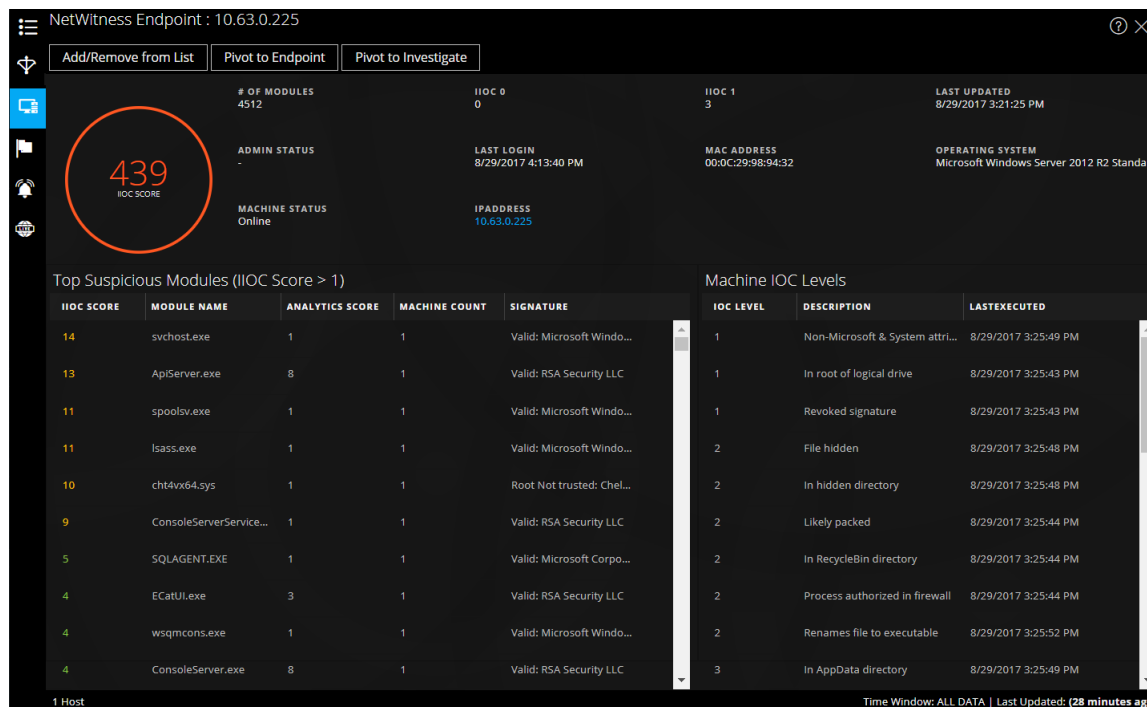
- sAMAccountName

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。
メール	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	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	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、または非アクティブ。
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、有効か無効かのインジケータ。GoogleやAppleなどの署名情報。

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
IOCLレベル	IOCLレベル。
説明	IOCL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。

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	INCIDENT ID
01/06/2020 07:58:44 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-3
01/06/2020 07:58:39 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-4
01/06/2020 07:58:39 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-11
01/06/2020 07:58:35 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-10
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-7
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-19
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-5
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-13
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-9
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-14
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-18
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-12
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-8
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-17

[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。

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-19	High Risk Alerts: ESA for 10. [redacted]	REMEDIATION_REQUESTED	analyst1	3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-18	High Risk Alerts: ESA for 10. [redacted]	REMEDIATION_REQUESTED	analyst1	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-17	High Risk Alerts: ESA for 10. [redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-16	High Risk Alerts: ESA for 10. [redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-15	High Risk Alerts: ESA for 10. [redacted]	ASSIGNED	analyst2	42
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-14	High Risk Alerts: ESA for 10. [redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-13	High Risk Alerts: ESA for 10. [redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-12	High Risk Alerts: ESA for 10. [redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-11	High Risk Alerts: ESA for 10. [redacted]	NEW		3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-10	High Risk Alerts: ESA for 10. [redacted]	NEW		3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-9	High Risk Alerts: ESA for 10. [redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-8	High Risk Alerts: ESA for 10. [redacted]	NEW		2
01/06/2020 07:58:30 pm (4 days ago)	CRITICAL	90	INC-7	High Risk Alerts: ESA for 10. [redacted]	NEW		2
01/06/2020 07:58:30 pm (4 days ago)	CRITICAL	90	INC-5	High Risk Alerts: ESA for 10. [redacted]	NEW		2

[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。
優先度	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。


Live Connect : ?

Add/Remove from List
Pivot to Endpoint
Pivot to Investigate

Review Status

STATUS MODIFIED DATE
 RISKY 08/16/2017 01:18:56 pm (a month ago)

Live Connect Risk Assessment



UNSAFE

Research and analysis shows resource to be untrusted

RISK REASONS

- Source of unsafe module
- Blacklisted by one or more customers

Risk Indicators

RECONNAISSANCE

HTTP
SCANNING
BRUTE FORCE
VPN
TOR
SOCKS

ANONYMOUS ACCESS
FTP
SSH
BUSINESS APPLICATION

OTHER

COMMAND AND CONTROL

BEACONING
HTTP
SSL/TLS
SSH
FTP
IRC

CUSTOM PROTOCOL
WEBSHELL
VPN
OTHER

DELIVERY

REMOTE/LOCAL FILE INCLUSION
CSRF
SQLI
XSS
EXPLOIT

PHISHING
DRIVE BY
OTHER

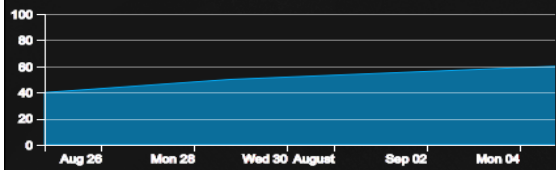
LATERAL MOVEMENT

OTHER
SSH
RDP
SMB/RPC
POWERSHELL
WMI
TELNET

Community Activity

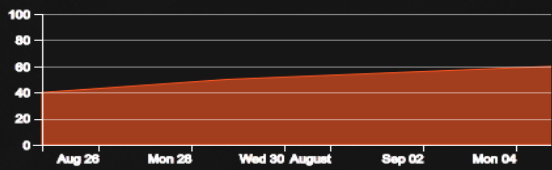
FIRST SEEN
04/08/2016 02:26:47.087 am (a year ago)

TRENDING COMMUNITY ACTIVITY (LAST 30 DAYS)



60% of the Community seen 94.74.81.176

TRENDING SUBMISSION ACTIVITY (LAST 30 DAYS)



Of the 70% submitted feedback:

- 40% marked High Risk (NOT DISPLAYED IN CHART)
- 30% marked Unsafe
- 70% marked Suspicious
- 0% marked Safe
- 5% marked Unknown

Identity

AUTONOMOUS SYSTEM NUMBER(ASN)
1030404303033

ORGANIZATION
American IP LTD.

COUNTRY CODE
US

COUNTRY NAME
United States

フィールド	説明
レビュー ステータス	<p>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。</p> <p>ステータス ステータスのタイプを以下に示します。</p> <ul style="list-style-type: none"> • 【New】 :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	<p>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。</p> <ul style="list-style-type: none"> • 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、このエンティティのリスクを計算するための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。

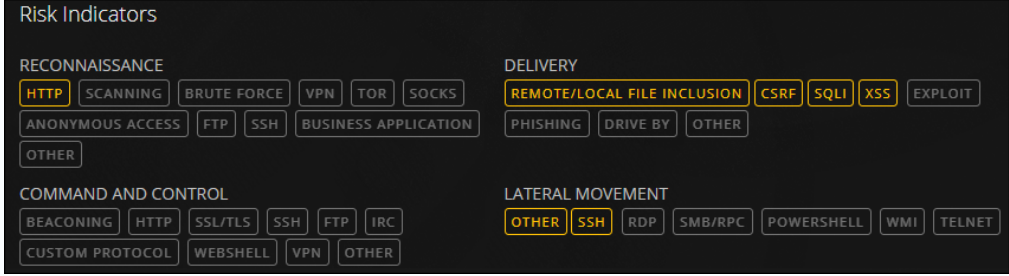
- **アナリスト スキルレベル**

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(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)のリスクの確認です。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を提供することによ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は次のとおりです。[高]、[中]、[低]。
- **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	<p>コミュニティ アクティビティについて次の情報が表示されます。</p> <ul style="list-style-type: none"> • 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)。 <p>トレンドのコミュニティ アクティビティ：</p> <p>RSAコミュニティの既知のIPアドレスである場合は、次のようなコミュニティ アクティビティのトレンドがグラフィカル表示されます。</p> <ul style="list-style-type: none"> • 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(%)。 • IPアドレスに関するフィードバックを送信したユーザーの割合(%)。 • 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	 <p>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。</p> <p>タグは次のように分類されます。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。</p> <p>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。</p>
ID	<p>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。</p> <p>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。</p> <p>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。</p> <p>ドメインの場合 :ドメイン名と関連IPアドレス。</p>
証明書情報	<p>選択したファイルハッシュの次の証明書情報を示します。証明書の発行者、証明書の有効性、署名アルゴリズム、証明書のシリアル番号。</p>

フィールド **説明**

WHO IS 情報

WHOIS		
CREATED DATE 09/01/2016 00:00	STREET 1600 Amphitheatre Parkway	PHONE +1.6502530000
UPDATED DATE 11/27/2016 12:43	CITY Mountain View	FAX +1.6506188571
EXPIRED DATE 10/01/2017 00:00	STATE CA	EMAIL dns-admin@google.com
TYPE RegistryType	POSTAL CODE 94043	
NAME Admin	COUNTRY US	
ORGANIZATION Google Inc.		

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。ドメイン所有者の次の情報が表示されます。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、ファクス、メール。

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。既知の関連するファイルのリストが、次の情報とともに表示されます。Live Connectのリスク評価(安全、危険、または不明)、ファイル名、MD5、コンパイル日時、API関数、インポートハッシュ、Mimeタイプ。

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。既知の関連するドメインのリストが、次の情報とともに表示されます。Live Connectのリスク評価(安全、危険、または不明)、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。

関連IP

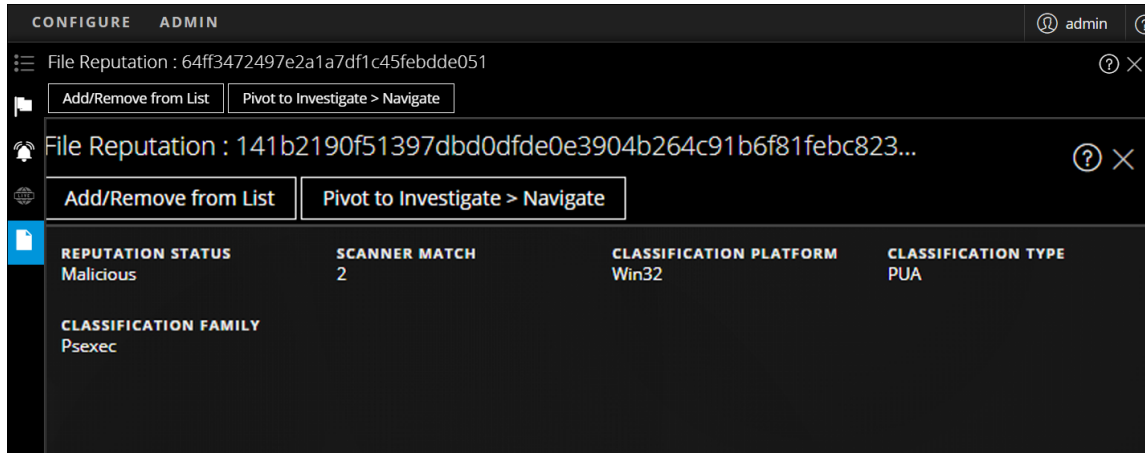
Related Files (5)					
LC RISK RATING	FILE NAME	MD5	COMPILE DATE	API FUNCTION IMPORT HASH	
UNKNOWN	filename1	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:24 ...		
UNSAFE	filename2	2a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		
UNKNOWN	filename3	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		
UNSAFE	filename4	2a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		
UNKNOWN	filename5	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		

Related Domains (2)					
LC RISK RATING	DOMAIN	COUNTRY	REGISTERED DATE	EXPIRED DATE	REGISTRANT EMAIL
UNSAFE	27c73bq66y4xqoh7.dorfa...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	
UNSAFE	2ymh2gnnbg6pgq2r.gre...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	

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。既知の関連するファイルのリストが、次の情報とともに表示されます。Live Connectのリスク評価(安全、危険、または不明)、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。

[ファイルレピュテーション]タブ

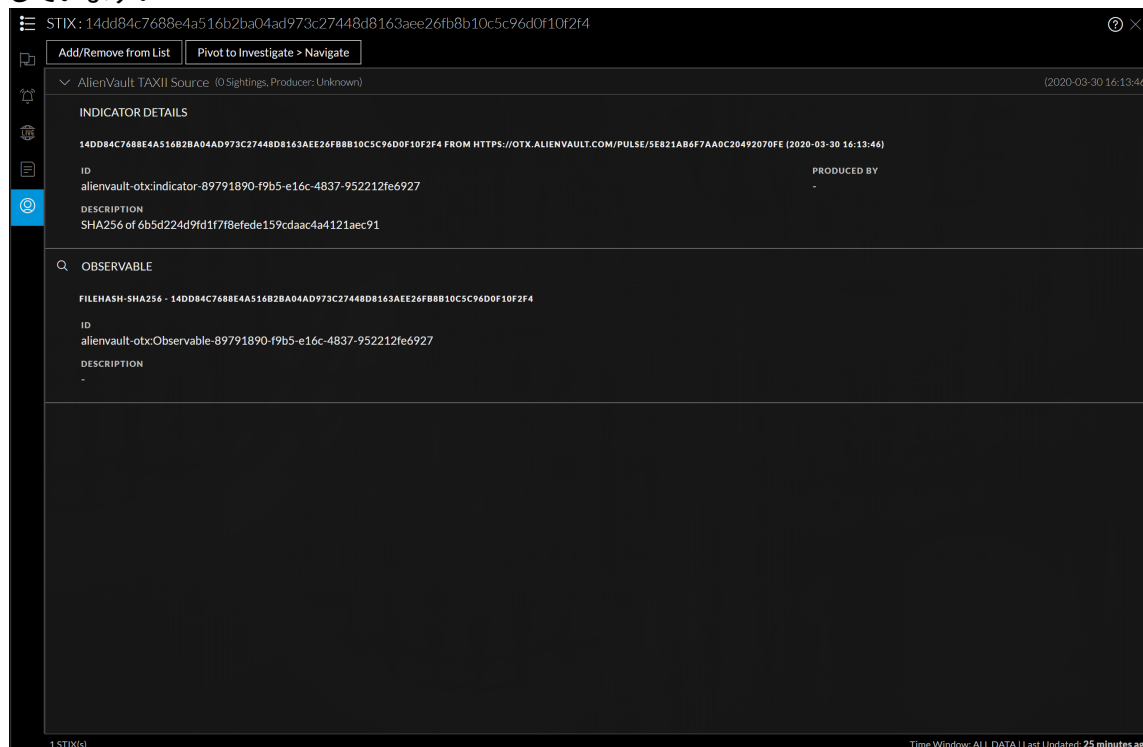
[ファイルレピュテーション]の[コンテキスト ルックアップ]パネルには、そのファイルのレピュテーションのステータスが表示されます。



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。
スキャナー一致	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。

🔍 タブ

次の図は、[コンテキスト]パネルの 🔍 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。



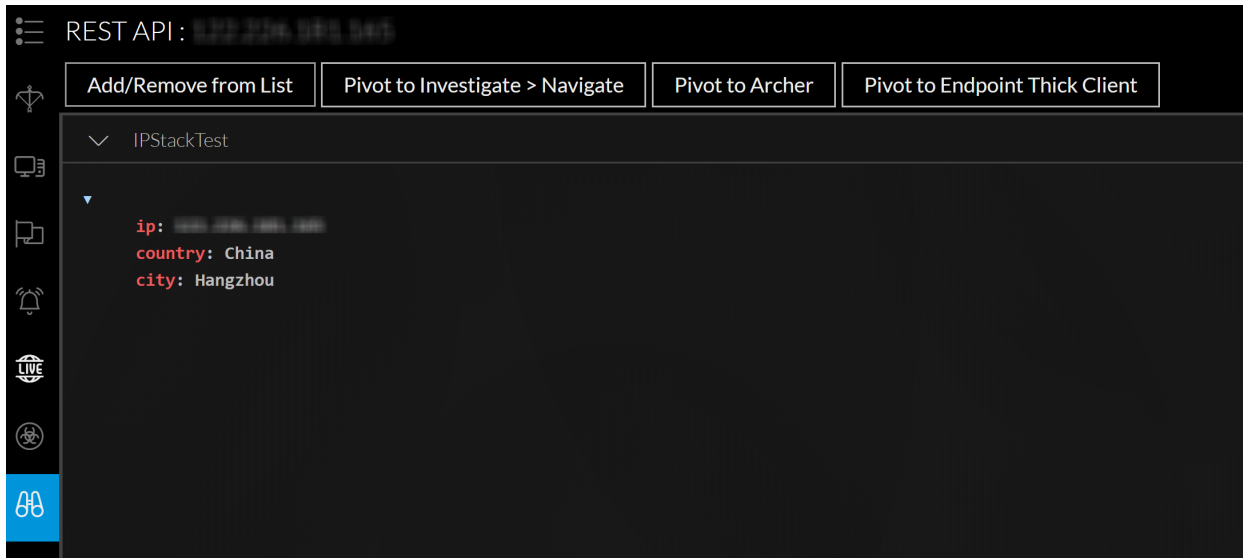
フィールド	説明
データソース名	データの取得元であるSTIXデータソース名を表示します。
Timestamp	イベントが作成された時刻。
インジケータの詳細	<p>インジケータタイトル :疑わしいまたは悪意のあるサイバー活動を検出するために使用できるパターンを含む詳細を表示します。</p> <p>ID :選択したインジケータのIDを表示します。</p> <p>作成者 :STIXデータを要求したユーザーロールを表示します。</p> <p>説明 :監視リストにある選択したIPアドレスの詳細を表示します。</p>
観測事象	<p>観測事象タイトル :STIX Cyber-observable Object(SCO)を使用して、ファイル、システム、ネットワークなどのサイバーセキュリティ関連エンティティに関する情報を表示および伝達します。</p> <p>ID :選択した観測事象のIDを表示します。</p>
(オプション) SightingsREST	<p>観測タイトル :観測ソースの名前を表示します。</p> <p>信頼度 :観測の重要度を表示します。</p> <p>参照 :観測ソースの参照URLを表示します。</p>

REST API] タブ

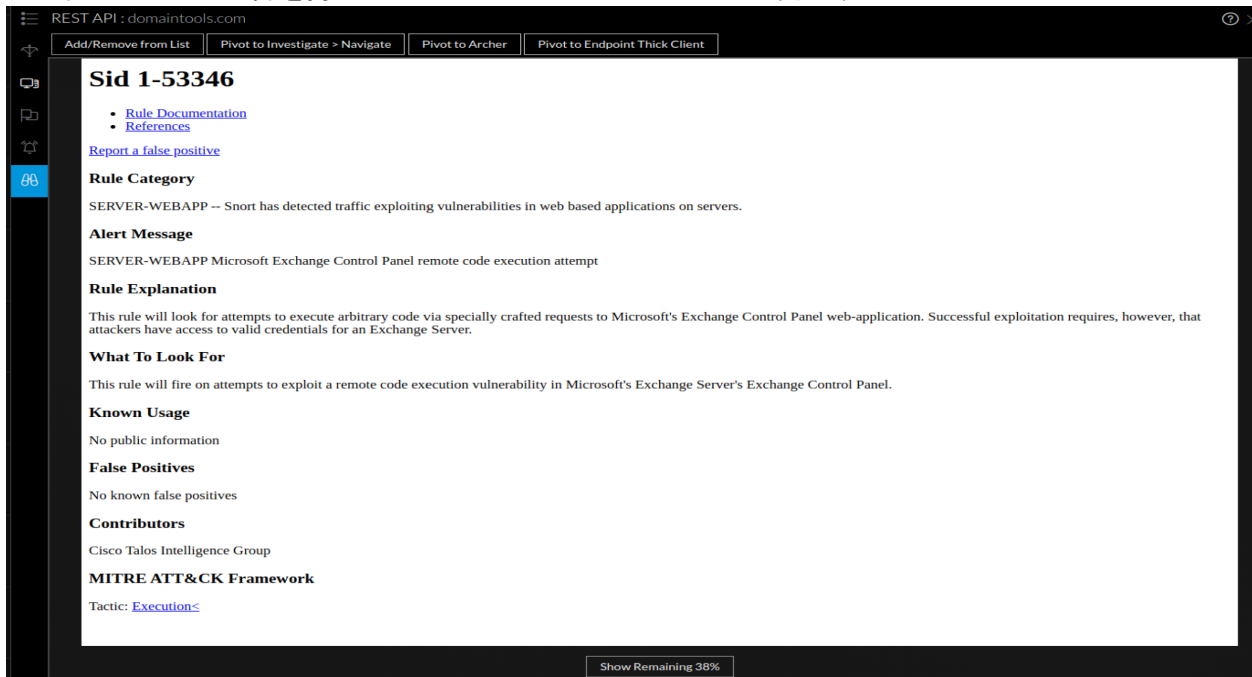
REST APIのコンテキスト ルックアップ パネルには、選択したエンティティまたはメタ値に関連づけられたHTMLまたはJSON応答(構成された応答タイプに基づく)が表示されます。

注: JSON応答タイプの場合、(REST API構成中に)フレンドリ名でマップされたフィールドはコンテキスト ルックアップでのみ表示されます。フィールドをマップしていない場合は、コンテキスト ルックアップですべてのフィールドが表示されます。

次の図は、JSON応答を持つREST APIのコンテキスト パネルの例です。



次の図は、JSON応答を持つREST APIのコンテキスト パネルの例です。

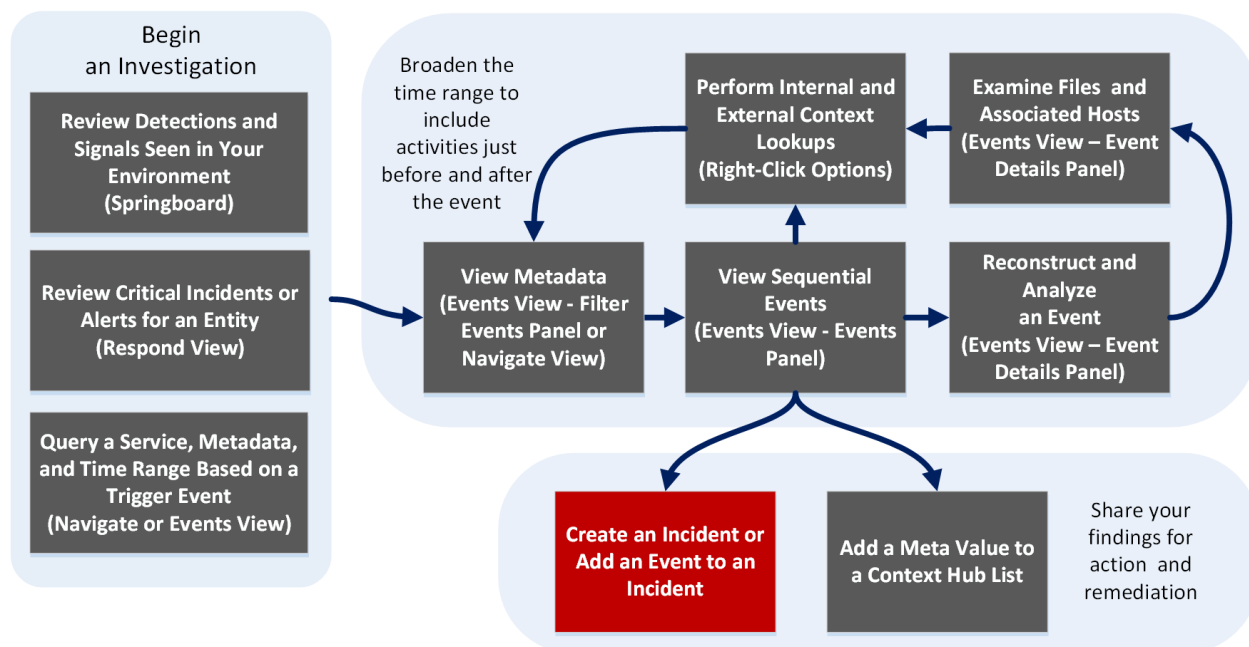


【インシデントの作成】ダイアログ

【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



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタートガイド
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 ユーザーガイド
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】ビューでの調査の開始 【ナビゲート】ビューまたは【ガシイーイベント】ビューでの調査の開始

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	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント 詳細の調査 [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	ファイルと関連ホストの調査	[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

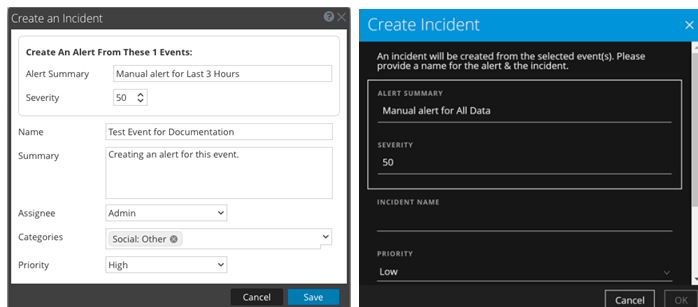
*このタスクは現在のビューで実行できます。

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。



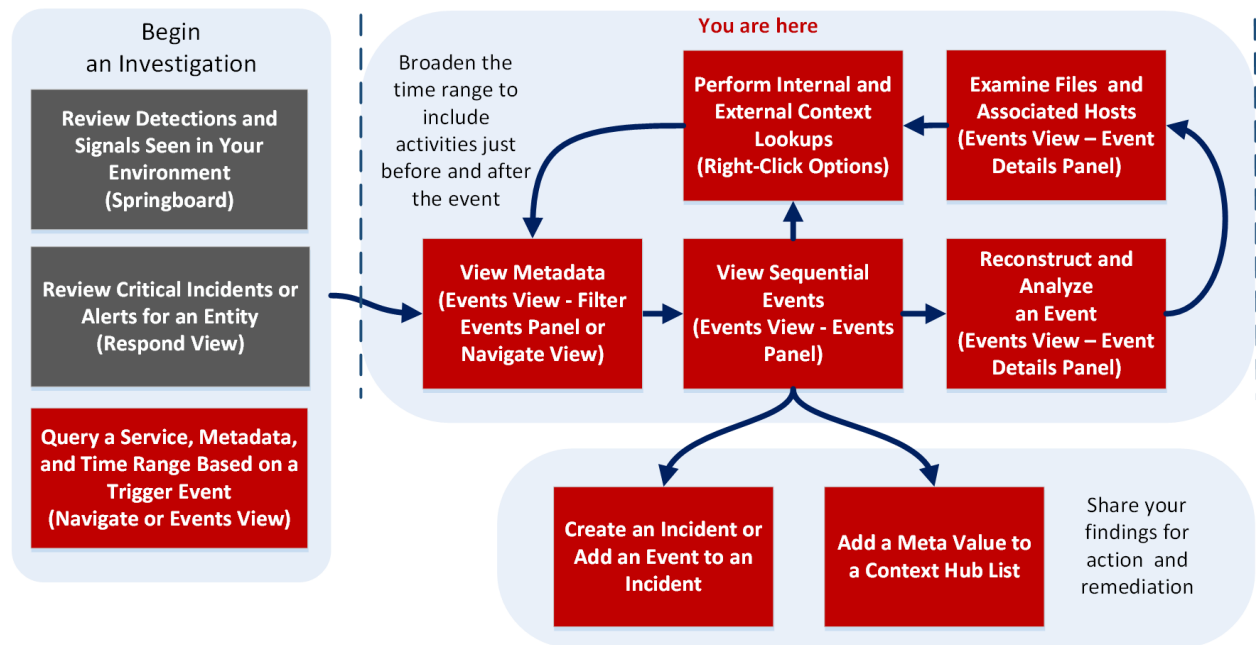
機能	説明
アラートの作成	[アラート サマリ] フィールドには、アラートを選択した時のクエリが自動入力されます。これは、このインシデントを作成する時に選択されていたクエリです。 [重大度] フィールドには、選択したアラートの重大度として、1~100の整数が示されます。
名前	(必須) インシデントを識別する名前を指定します。この例では、名前は「Sample Incident」です。このインシデントに追加されるイベントの特性を明確に識別する名前を指定します。
サマリ	(オプション) インシデントのオプションの説明を指定します。優れたサマリを指定すると、他のアナリストや対応者がインシデントを明確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を識別します。 [カテゴリ] をクリックすると、インシデントのカテゴリとサブカテゴリ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(複数可)を選択できます。カテゴリは主要なグループ(環境、エラー、ハッキング、マルウェア、誤用、ソーシャル)に分類されます。
優先度	インシデントの優先度を識別します。 [優先度] をクリックすると、優先度のドロップダウンリストが開きます。ドロップダウンリストには、[クリティカル]、[高]、[中]、[低]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、ネットワーク、ログ、およびエンドポイント イベントのシーケンシャルリストを表示し、再構築および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。バージョン11.5以降では、リストされたイベントのメタデータをドリルダウンできます。【イベント】ビューには、パケット、ファイル、ホスト、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一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。



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
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	<i>NetWitness Respond</i> 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]ビューでの調査の開始 [サビゲート]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	メタデータの表示*	[サビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン (ベータ版)
脅威ハンター	シーケンシャル イベントを表示する*	[イベント]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
脅威ハンター	イベントの再構築と分析*	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストを調査する*	[イベント]ビューでのデータのダウンロード [サビゲート]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 - \[パケット\]タブ](#)
- [\[イベント\]ビュー - \[テキスト\]タブ](#)
- [\[イベント\]ビュー - \[ファイル\]タブ](#)
- [\[イベント\]ビュー - \[メール\]タブ](#)
- [\[イベント\]ビュー - \[ホスト\]タブ](#)

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、[サビゲート]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。

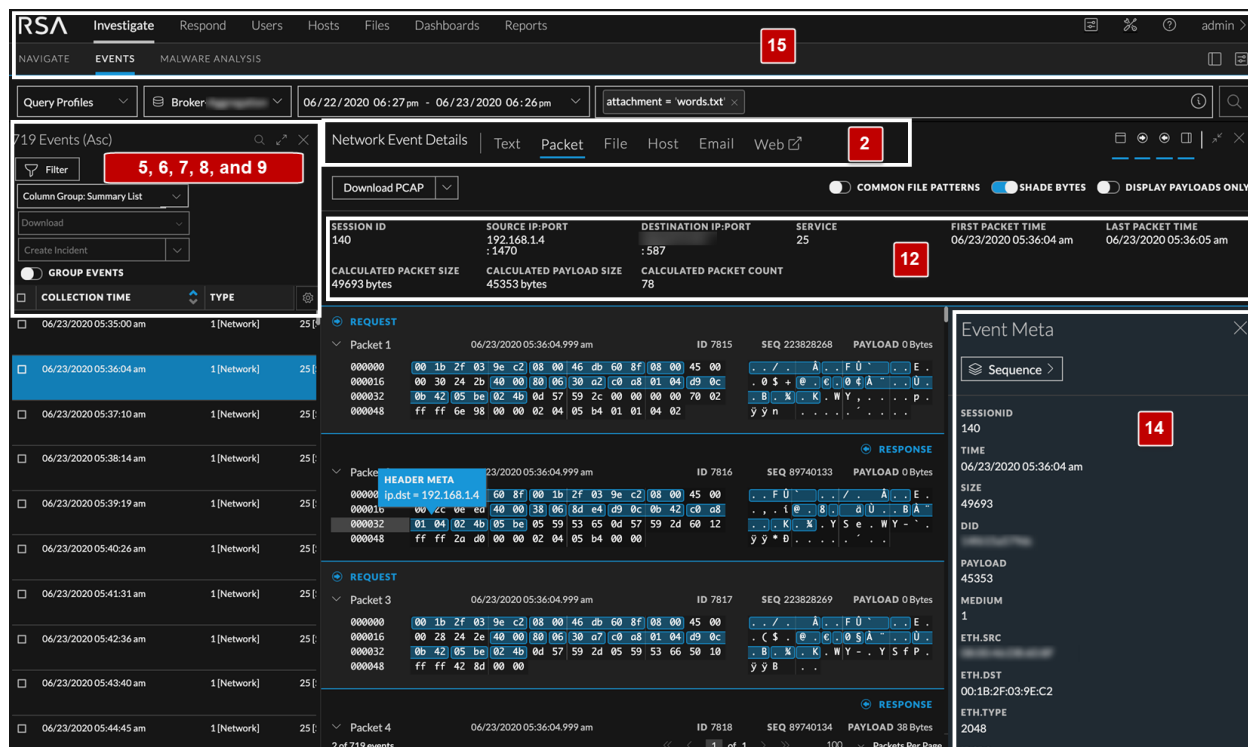
The screenshot shows the NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate', 'Monitor', 'Configure', and 'Admin'. Below it is a search bar with 'Query Profiles' and 'AdminServer' selected. The main area displays a list of events on the left and a detailed view of a selected event on the right. Red callout boxes (1-14) highlight various UI elements: 1. Search bar, 2. Filter dropdown, 3. Refresh button, 4. Close button, 5. Column Group dropdown, 6. Download button, 7. Create Incident dropdown, 8. Incident creation options, 9. Event list item, 10. Event detail tabs (Text, Packet, File, Email, Web), 11. Event detail view controls, 12. Event detail table, 13. File details table, 14. Event meta panel.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
AdminServer	1021784	:47602	:80	80	11/02/2014 04:16:33 pm


FILE NAME	MIME TYPE	FILE SIZE	HASHES
1021784-107-0_1.txt	text/plain	13 bytes	SHA1: 55f6ffe48684abd319bd42fa0f8127e8b89788bf MD5: 20d8b9bbae8f0442d8e9843b17a3b7e

EVENT META	
ORGANIZE BY	Sequence
SESSIONID	1021784
TIME	11/02/2014 04:16:33 pm
SIZE	1028
PAYLOAD	352
MEDIUM	1
ETH.SRC	
ETH.ALL	
ETH.DST	

次の図は、バージョン11.5以降で変更された要素を示しています。




- 1 クエリバー :サービスを選択すると、サービスセレクト、時間範囲セレクト、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(後掲の「[\[イベント\]ビュー](#)」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。
 - イベントタイプで利用できる分析のタイプは、テキスト、パケット、ファイル、ホスト、メール、Webです。ネットワークイベントは、すべての分析タイプ(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))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詳細の調査](#)」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、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。バージョン11.5では、冗長NWサービスが削除されています。
- 13 現在分析中のイベントのイベントデータ。
- 14 [\[イベントメタ\]](#)パネルはバージョン11.5で再設計されていますが、バージョン11.4と同じ機能を備えています。「[イベントメタ]」パネルは、データで見つかったメタキーと値を一覧表示します。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

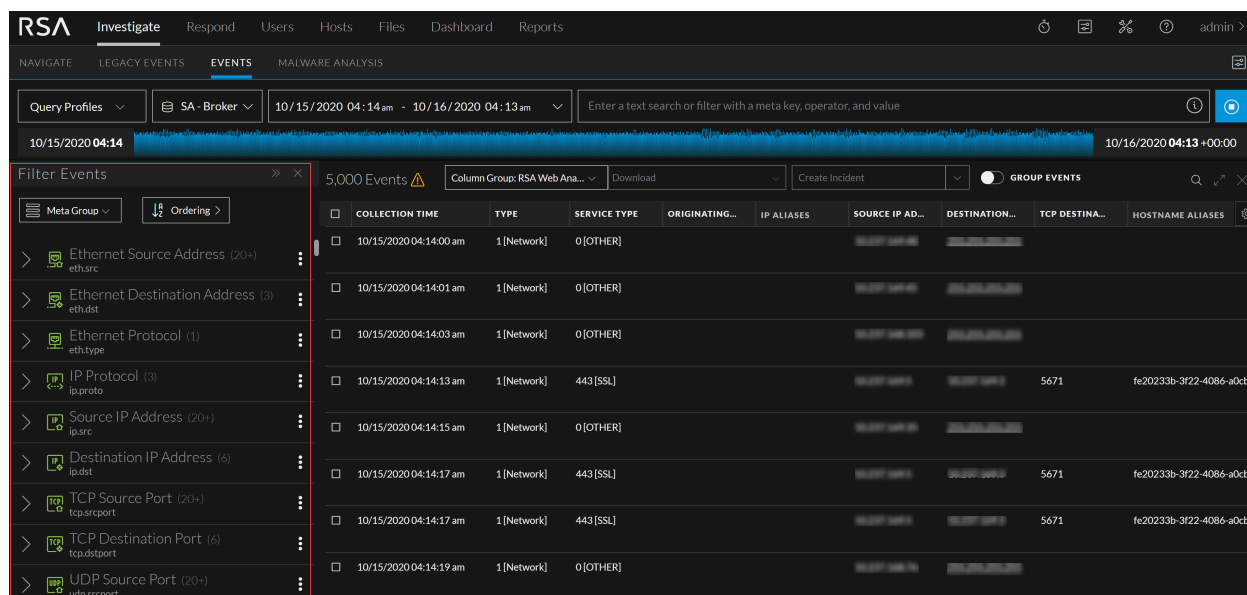
ンしているユーザに関連した情報などです(エンドポイント イベント データの詳細については、『*NetWitness Endpoint ユーザガイド*』を参照してください)。

15 RSA NetWitness Platformのバージョン11.5のメインメニューでは、ホスト、ファイル、ユーザ(エンティティ)のオプションが再配置され、アクセスしやすくなっています。

「イベントの絞り込み」パネル




「イベントの絞り込み」パネルはバージョン11.5から追加されたベータ機能です。「イベント」パネルの「フィルタ」ボタン( Filter)をクリックすると、パネルが開き、データセットで見つかったメタキーとメタ値が表示されます。(バージョン11.6)「イベントの絞り込み」パネルは「イベント」ビューでデフォルトで開いています。ユーザ設定(開く、閉じる、または完全展開)は、セッション間とログイン間で保存されます。メタデータのドリルダウンの詳細については、「[「イベント」ビューでのメタデータのドリルダウン\(ベータ版\)](#)」を参照してください。

注:(バージョン11.6)「イベントの絞り込み」パネルは「イベント」ビューでデフォルトで開いています。パネルの最後に使用された状態(縮小または完全展開)は、セッション全体およびログイン間で保存されます。また、「イベントの絞り込み」パネルでは、読みやすさを向上させるため、メタキー、メタ値、およびメタカウント間の相違が明らかに示されています。




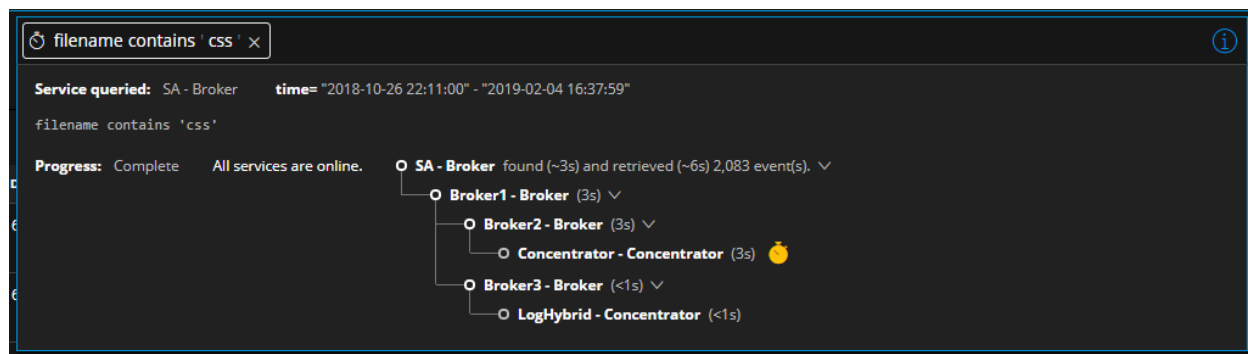
COLLECTION TIME	TYPE	SERVICE TYPE	ORIGINATING...	IP ALIASES	SOURCE IP AD...	DESTINATION...	TCP DESTINA...	HOSTNAME ALIASES
10/15/2020 04:14:00 am	1 [Network]	0 [OTHER]						
10/15/2020 04:14:01 am	1 [Network]	0 [OTHER]						
10/15/2020 04:14:03 am	1 [Network]	0 [OTHER]						
10/15/2020 04:14:13 am	1 [Network]	443 [SSL]					5671	fe20233b-3f22-4086-a0cb-
10/15/2020 04:14:15 am	1 [Network]	0 [OTHER]						
10/15/2020 04:14:17 am	1 [Network]	443 [SSL]					5671	fe20233b-3f22-4086-a0cb-
10/15/2020 04:14:17 am	1 [Network]	443 [SSL]					5671	fe20233b-3f22-4086-a0cb-
10/15/2020 04:14:19 am	1 [Network]	0 [OTHER]						

「メタグループ」メニュー 「イベントの絞り込み」パネルを開いた状態で、メタグループを選択して、「イベントの絞り込み」パネルに表示されるメタキーを定義できます。デフォルトのメタキーメタグループは、最初にログインしたときに有効になります。前回ログインしたときに別のメタグループを選択した場合は、ブラウザのキャッシュがクリアされない限りそのメタグループが有効なままになります。バージョン11.5.1では、以前に選択したメタグループはブラウザのキャッシュに保存されないため、変更しない限り有効なままです。メタグループの詳細については、「[「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](#)」を参照してください。

メニューの並べ替え	<p>[イベントの絞り込み] パネルを開くと、値ごとにイベント数またはイベントサイズという2つのパラメータを確認できます。各メタキー エントリには、値の後の括弧内にイベント数またはイベントサイズのいずれかが含まれます。どちらの場合も、並べ替えには4つのオプションがあります。</p> <ul style="list-style-type: none"> デフォルトで、メタキーは [イベント数] > [合計数の降順] 方法を使用して表示されます。各値のイベント数を表示する場合は、合計数の降順、合計数の昇順、値の昇順、値の降順で並べ替えることができます。 値を含んだイベントのサイズを確認したい場合は、イベントサイズによる4つの並べ替えオプション(合計サイズの降順、合計サイズの昇順、値の昇順、値の降順)のいずれかを使用できます。
メタキーオプション] ボタン (H)	<p>[メタキーオプション] ボタンは、個々のメタキーに対して実行できるアクションを提供します。バージョン11.5では、唯一のアクションは、メタキーについて表示されているメタ値をすべてコピーすることです。</p>
メタキーリスト	<p>各メタキー名の前のアイコンは、キーのインデックス付け方法を識別します。インデックス付け方法は、そのメタキーを使用して実行できるインタラクションとクエリのタイプを決定します。</p> <ul style="list-style-type: none"> このメタキーは値でインデックス付けされています。  Action Event [action] (40+)。緑色は、使用可能なすべてのインタラクションとクエリがサポートされていることを示します。メタ値を右クリックすると、コンテキストメニューで使用可能なインタラクションを確認できます。 このメタキーはメタキーによってインデックス付けされています。  Bytes Sent [bytes.src]。黄色は、使用可能なインタラクションのサブセットがサポートされていることを示しています。このメタキーに対するクエリは、値でインデックス付けされたメタキーよりも時間がかかる場合があります。メタ値を右クリックすると、コンテキストメニューで使用可能なインタラクションを確認できます。 このメタキーにはインデックスが付けられていません。  MAC Alias Record [alias.mac]。インデックス付けされていないメタキーの値を使用してクエリを実行することはできません。インデックス付けされていないメタキーをクエリする場合、管理者はサービスのインデックスファイルを編集して、値またはメタキーでメタキーをインデックス付けする必要があります。

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 :チャンネル%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。

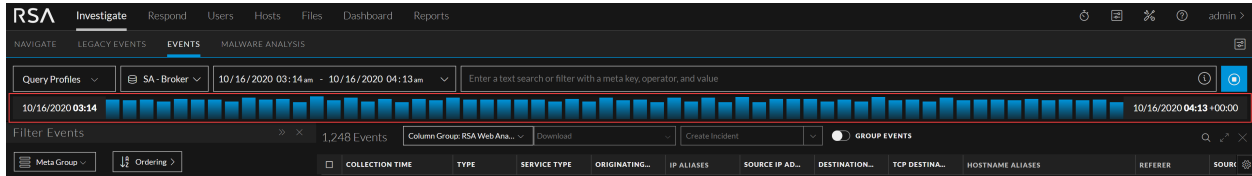
実行時間に対する操作あたりの制限がサーバにあり、要求された操作がこの制限を超過しました。このエラーを回避するには、小さい時間範囲などの小さな要素に操作を分割します。

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] > [dk] > [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。

タイムライン

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の数を可視化します。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棒グラフで表示されます。



タイムラインの主な機能は次のとおりです。

- 開始時刻と終了時刻がタイムラインの両側に表示され、クエリの期間中の一致したイベントが示されます。タイムラインの右側には、UTCからのオフセットを示すことによってタイムゾーンも表示されます。
- イベント データに一致するタイムラインのセクションは強調表示されます。データは、指定されたしきい値まで強調表示されます。データが時間でソートされていない場合は、タイムライン全体が強調表示されます。また、データが特定の順序でソートされていない場合、イベントは時間で並べ替えられないため、タイムラインの個々のバーが強調表示されることがあります。
- しきい値を超えるクエリ結果は灰色で表示されます。イベントが時間でソートされている場合、しきい値の強調表示は、ソートの設定に応じて左 (昇順) から右 (降順) にシフトします。
- タイムラインにカーソルを合わせると、クエリされた期間中に発生したイベントの総数が表示されます。タイムラインの個々のバーにカーソルを合わせると、特定の時間に発生したイベントの総数を取得できます。
- イベントをソートしても、タイムラインは更新されません。タイムラインを更新するには、クエリを再度実行する必要があります。
- タイムラインのすべての機能は、ユーザが収集時間 (time) を使用してクエリを実行している場合、または基本設定がイベント時間 (event.time) を使用するように設定されている場合に正しく動作します。

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。

The screenshot shows the NetWitness Investigate interface with the following callouts:

- 1**: Search filters for service, time range, and search term.
- 2**: Event list table with columns for time, event type, and size.
- 3**: Close button for the event list panel.
- 4**: Analysis tabs (Network Event Details, Text Analysis, Packet Analysis, File Analysis).
- 5**: Download PCAP button.
- 6**: Display compressed payloads toggle.
- 7**: Event header controls (show/hide).
- 8**: Close button for the event details panel.
- 9**: Close button for the event meta panel.
- 10**: Summary information table for the selected event.
- 11**: Request details section.
- 12**: Event meta details section.

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 分析されているイベントのタイプは、ヘッダーに反映されます。(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)が開きます。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、3つの分析タイプ(テキスト、パケット、およびファイル)をすべて使用できます。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 閉じている場合、「イベント」パネルまたは「イベントメタ」パネルを再度開きます。

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

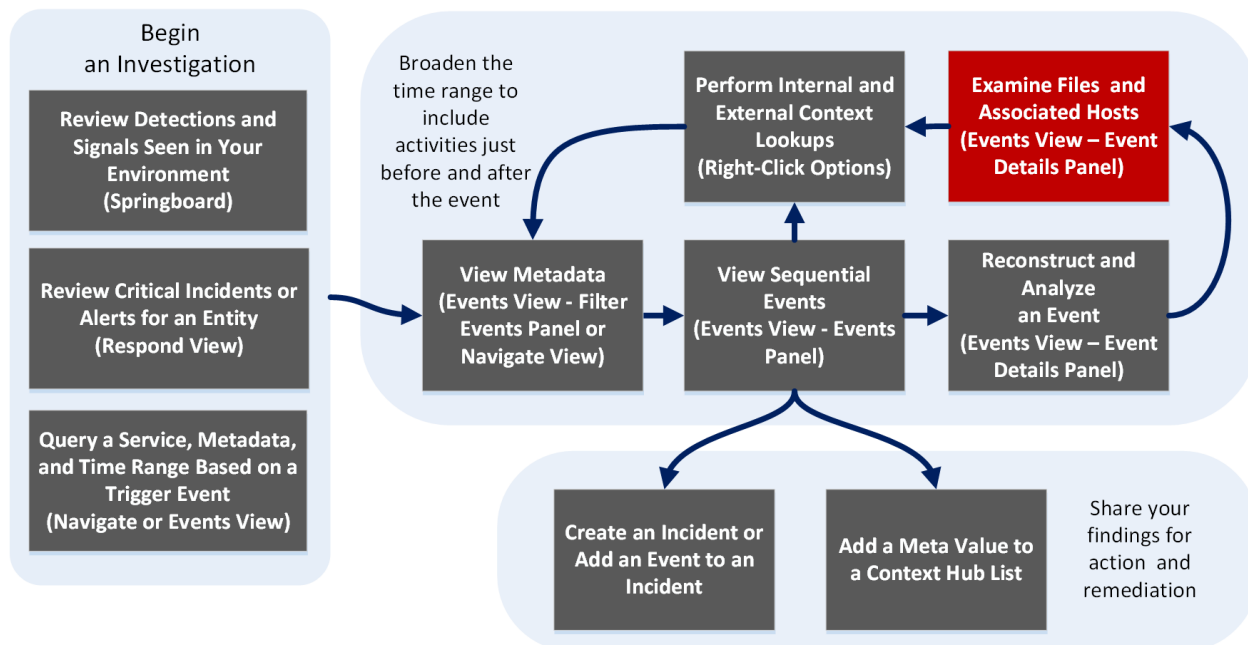
ログからのテキスト行です。

- 12 [イベント メタ] パネルは、データで見つかったメタ キーと値を一覧表示します。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】タブ

【メール】タブは【イベントの詳細】パネルにあります。ここで、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 - 【パケット】タブ](#)
- [【イベント】ビュー - 【テキスト】タブ](#)
- [【イベント】ビュー - 【ファイル】タブ](#)
- [【イベント】ビュー - 【メール】タブ](#)
- [【イベント】ビュー - 【ホスト】タブ](#)

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、メール再構築の例を示しています。

The screenshot displays the 'Network Event Details' window for an email event. At the top, it shows session information: SESSION ID 1, SOURCE IP:PORT 84.2.103.139:52459, DESTINATION IP:PORT :4422, SERVICE 0, FIRST PACKET TIME 06/09/2017 07:10:13 am, and LAST PACKET TIME 06/09/2017 07:10:17 am. Below this, it lists calculated sizes: CALCULATED PACKET SIZE 8664 bytes, CALCULATED PAYLOAD SIZE 6120 bytes, and CALCULATED PACKET COUNT 42.

The main area shows a list of messages with headers: FROM, TO, and SUBJECT. The first message is from 'Degang Parkin <Degang.etalgro@pictures.com>' to 'pfuchon@law.gsu.edu' with the subject 'Board of having same, string see every right? Spice up your life, add inches to your d33r and increase her pleasure.' The second message is from 'Jansoop Kerber <revelles195@pictures.com>' to 'pfuchon@law.gsu.edu' with the subject 'Have the hardest, longest and thickest erect 10n ever.' The third message is from 'albe Nixon <revelles1981@pictures.com>' to 'pfuchon@law.gsu.edu' with the subject 'The only supplement proven in studies worldwide to add up to 4 inches to your manhood.' The fourth message is from 'MINDUNGOO Pawlek <revelles1981@pictures.com>' to 'pfuchon@law.gsu.edu' with the subject 'Tired of lacking confidence because you have a small dick?'. Below the messages, there is an 'ADDITIONAL HEADER DETAILS' section with a link: 'Don't be ashamed of having a small member, you can add inches today easily.'

On the right side, the 'Event Meta' panel shows details for the selected event: SESSIONED 1, TIME 05/29/2017 12:27:28 pm, SIZE 191.6 KB, SID packetHybrid, PAYLOAD 178152, MEDIUM 1, ETH SRC 00:13:C3:38:C7:00, ETH DST 00:17:0F:68:C8:00, ETH TYPE 2048, IP SRC 84.2.103.139, IP DST, and IP PROTO 6.

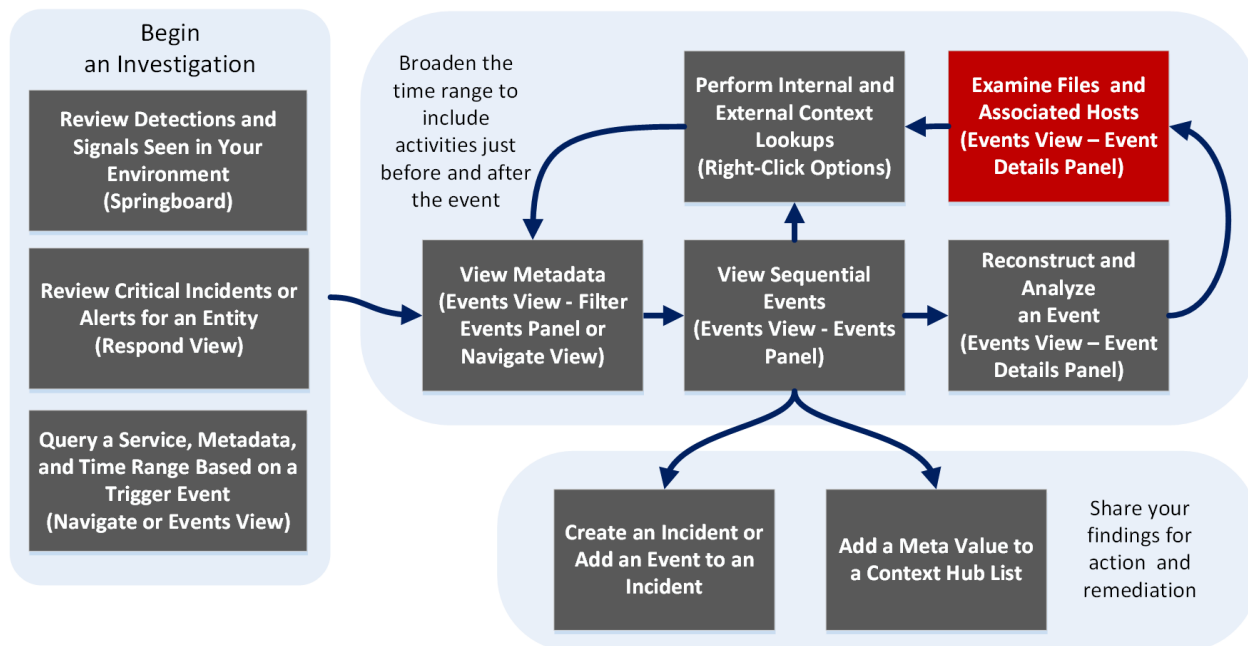
次の表は、メール内のすべてのフィールドについて説明しています。

フィールド	説明
差出人	メールの送信者のメールアドレスが表示されます。
変更後	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。
返信先	返信を受信するように指定されたアドレス、つまり送信者アドレスが表示されます。
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。メールの添付ファイルのダウンロードの詳細については、「 [イベント]ビューでのデータのダウンロード 」を参照してください。
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」タブ

「ファイル」タブは「イベントの詳細」パネルにあります。ここで、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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタートガイド
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 ユーザーガイド
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」ビューでの調査の開始 「サビゲート」ビューまたは「ガシー イベント」ビューでの調査の開始
脅威ハンター	メタデータの表示	「サビゲート」ビューでの結果のフィルタリング 「イベント」ビューでのメタデータのドリルダウン(ベータ版)

ユーザ ロール	実行したいこと	手順
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストを調査する*	[イベント]ビューでのデータのダウンロード [サビゲート]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 - \[パケット\]タブ](#)
- [\[イベント\]ビュー - \[テキスト\]タブ](#)
- [\[イベント\]ビュー - \[ファイル\]タブ](#)
- [\[イベント\]ビュー - \[メール\]タブ](#)
- [\[イベント\]ビュー - \[ホスト\]タブ](#)

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。

Network Event Details | Text Packet **File** Email Web

Download Files (2)

SESSION ID 9	SOURCE IP:PORT 192.168.1.4 :1470	DESTINATION IP:PORT :587	SERVICE 25	FIRST PACKET TIME 05/22/2020 04:11:07 am	LAST PACKET TIME 05/22/2020 04:11:07 am
CALCULATED PACKET SIZE 49693 bytes	CALCULATED PAYLOAD SIZE 45353 bytes	CALCULATED PACKET COUNT 78			

Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data. To avoid quarantine, the zip file is password protected with this password: netwitness.

<input type="checkbox"/>	FILE NAME	MIME TYPE	FILE SIZE	HASHES
<input checked="" type="checkbox"/>	words.txt	text/plain	1.0 KB	SHA1: 5da32e1be64e159733a39ede07dd1d3d8f83cc01 SHA256: a5e3aba74847e34edee282bd666d3a7606393118b0874e63682 MD5: d881c34fa5283a3e8a0cd9f973d0c495
<input checked="" type="checkbox"/>	related.patch	application/octet-stream	33.4 KB	SHA1: 9eb585a98f83d0e05e6a81b0b71406778d35b6ec SHA256: 359641873610597882317aee0f72104ed54fe8aa82d6fa323a54 MD5: 5ffd2afab8388f042296b32368b6e0e1

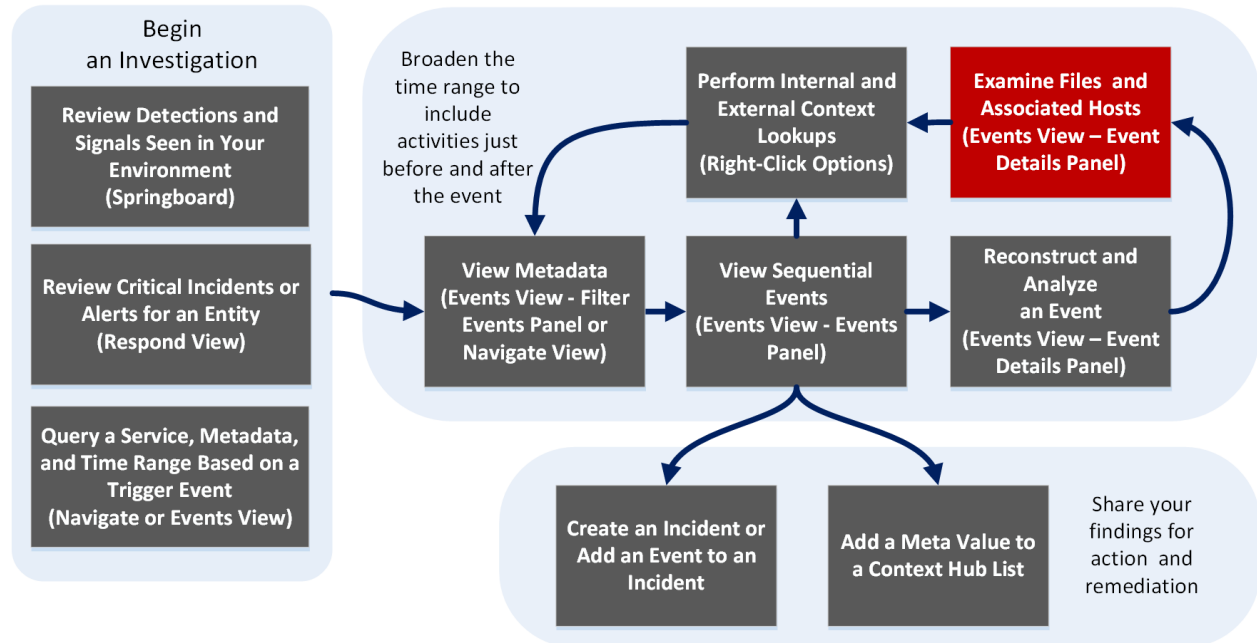
9 of 2,001 events

機能	説明
「ファイルのダウンロード」ボタン	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。
イベント ヘッダー	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。
ファイル リスト	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。

「イベント」ビュー - 「ホスト」タブ

「ホスト」タブは「イベントの詳細」パネルにあります。ここで、ネットワーク イベントとそれに付加されたエンドポイント データを確認できます。たとえば、選択したネットワーク イベントをトリガーしたホストやプロセスのほか、リスク スコア、レピュテーション、ログインしているユーザーなどの詳細が表示されます。「ホスト」パネルは、エンドポイント データがあるネットワーク イベントでのみ使用できます。

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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
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 ユーザー 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

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	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析*	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストの調査	[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 - \[パケット\]タブ](#)
- [\[イベント\]ビュー - \[テキスト\]タブ](#)
- [\[イベント\]ビュー - \[ファイル\]タブ](#)
- [\[イベント\]ビュー - \[メール\]タブ](#)
- [\[イベント\]ビュー - \[ホスト\]タブ](#)

簡単な説明

[ホスト]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。

The screenshot shows the NetWitness Investigate interface. At the top, there's a navigation bar with 'Investigate' and menu items like 'Respond', 'Users', 'Hosts', 'Files', 'Dashboards', and 'Reports'. Below that, there's a search bar with filters for 'Query Profiles', 'NetworkHybrid - Concentrator', and a date range '06/02/2020 11:25 am - 06/05/2020 01:57 pm'. A search filter 'ipsrc = 10.91.32.138' is applied. On the left, there's a list of 2,198 events. One event is selected, and its details are shown in the main panel. The event details are categorized into 'HOST DETAILS' and 'PROCESS DETAILS'. The 'HOST DETAILS' section shows the host name 'INENBOSEJL3C', operating system 'Microsoft Windows 10 Enterprise', and owner 'bossj'. The 'PROCESS DETAILS' section shows the process name 'chrome.exe' and user 'bossj'. An 'Event Meta' panel on the right shows session ID '57003', time '06/04/2020 10:20:27 am', size '7952', and DID. Red boxes and arrows highlight the host name and process name in the event details.

1 イベント ヘッダーには、エンドポイント データが付加されたネットワーク イベントの概要が表示されます。以下のファイルが含まれます。

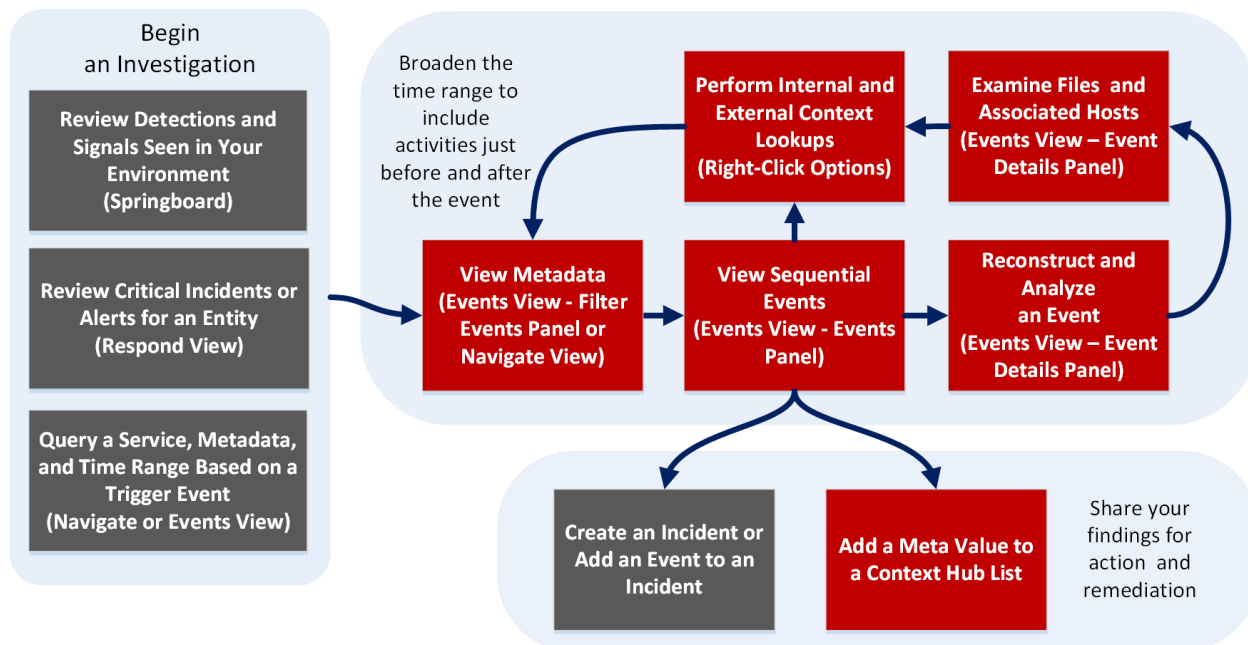
- ホスト - イベントの発生元ホスト。
- プロセス - イベントをトリガーしたソース プロセス。
- ユーザー - トリガーされたプロセスに関連づけられているユーザー。

2 ホストとプロセスに関する追加の詳細を表示できます。詳細については、「[ホスト情報](#)」を参照してください。

【イベント】ビュー - 【パケット】タブ

【パケット】タブは 【イベントの詳細】パネルにあります。イベントのパケットとペイロードを表示し分析できます。

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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
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 ユーザー 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	メタデータの表示*	【ナビゲート】ビューでの結果のフィルタリング 【イベント】ビューでのメタデータのドリルダウン(ベータ版)

ユーザ ロール	実行したいこと	手順
脅威ハンター	シーケンシャル イベントを表示する*	[イベント]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
脅威ハンター	イベントの再構築と分析*	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストを調査する*	[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 - \[パケット\]タブ](#)
- [\[イベント\]ビュー - \[テキスト\]タブ](#)
- [\[イベント\]ビュー - \[ファイル\]タブ](#)
- [\[イベント\]ビュー - \[メール\]タブ](#)
- [\[イベント\]ビュー - \[ホスト\]タブ](#)

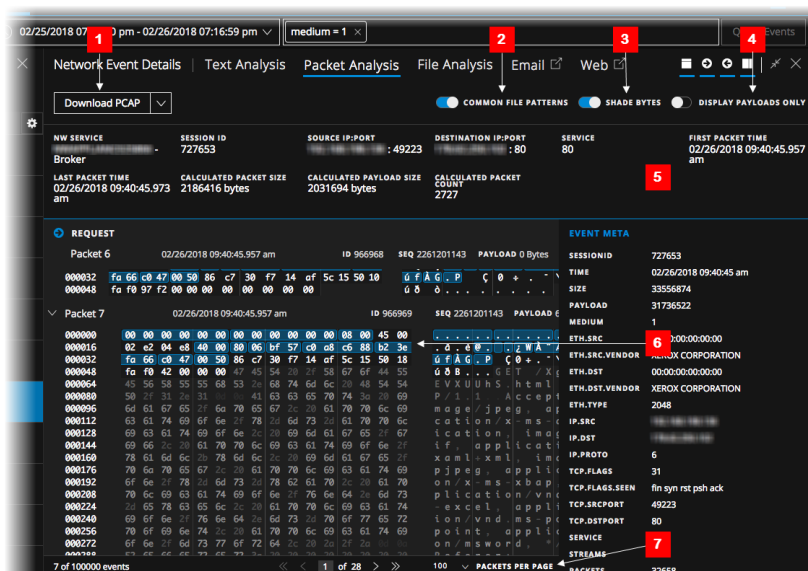
簡単な説明

[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。

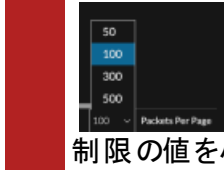
バージョン11.1以降では、ページ移動コントロールを使用して、前後のページへの移動、特定のページへの移動、1ページあたりに表示するパケット数(50、100、300、500)の選択ができます。

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、各パケットは濃淡化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(以前の〔パケット分析〕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。各機能の詳細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化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

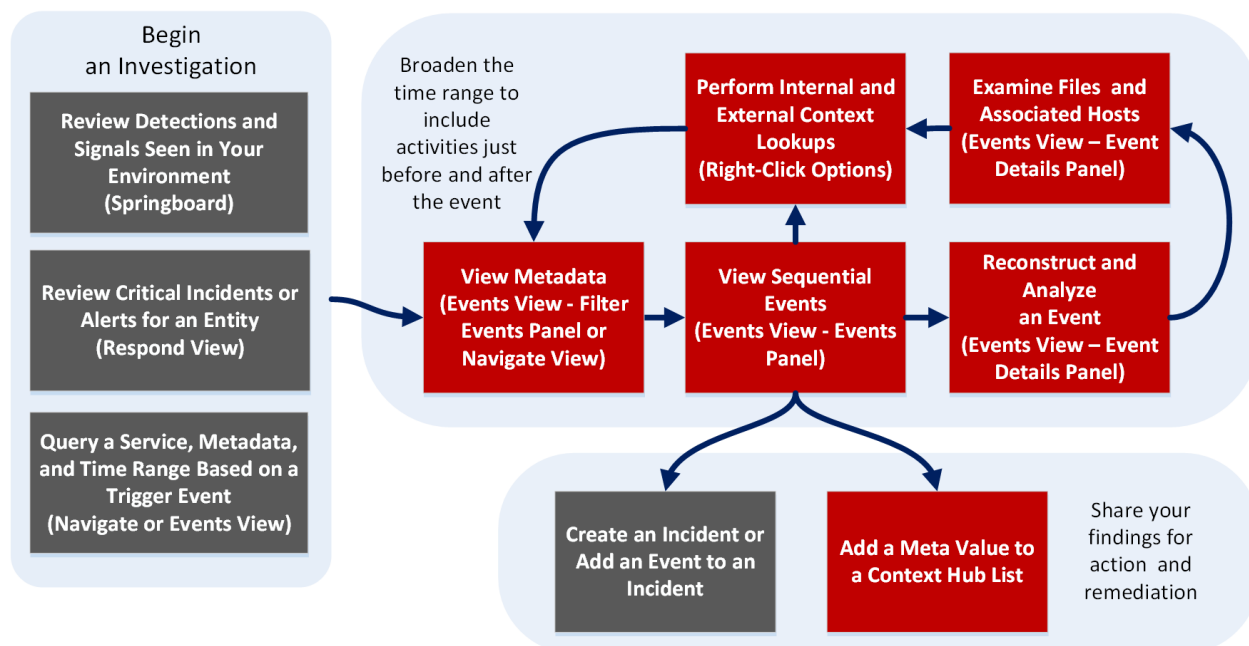


- 1ページあたりのパケット数を選択大量のパケットを再構築している場合は、この制限の値を小さくすることで、パフォーマンスを向上させることができます。

【イベント】ビュー - テキスト】タブ

【テキスト】タブは【イベントの詳細】パネルにあります。イベントのRAWテキストペイロードを表示し、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



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタートガイド
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 ユーザーガイド
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】ビューでの調査の開始 【サービス】ビューまたは【ガシー イベント】ビューでの調査の開始

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*	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャル イベントを表示する*	[イベント]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
脅威ハンター	イベントの再構築と分析*	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストを調査する*	[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 - \[パケット\]タブ](#)
- [\[イベント\]ビュー - \[テキスト\]タブ](#)
- [\[イベント\]ビュー - \[ファイル\]タブ](#)
- [\[イベント\]ビュー - \[メール\]タブ](#)
- [\[イベント\]ビュー - \[ホスト\]タブ](#)

簡単な説明

【イベント】ビューは、【テキスト】パネル(以前の【テキスト分析】)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。

The screenshot displays the NetWitness Investigate interface for a specific event. The top navigation bar includes 'Network Event Details', 'Text Analysis', 'Packet Analysis', 'File Analysis', 'Email', and 'Web'. A 'Download PCAP' button is highlighted with a red box labeled '1'. The event details table shows session ID 835, source IP:port 172.20.0.35:45476, and destination IP:port 172.20.0.33:143. The event meta table on the right lists session ID, time, size, payload, and various network layer details. The main content area shows a sequence of events: a REQUEST for 'capability', a RESPONSE, a REQUEST for 'authenticate plain', a RESPONSE, a REQUEST for 'select "/>

- 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

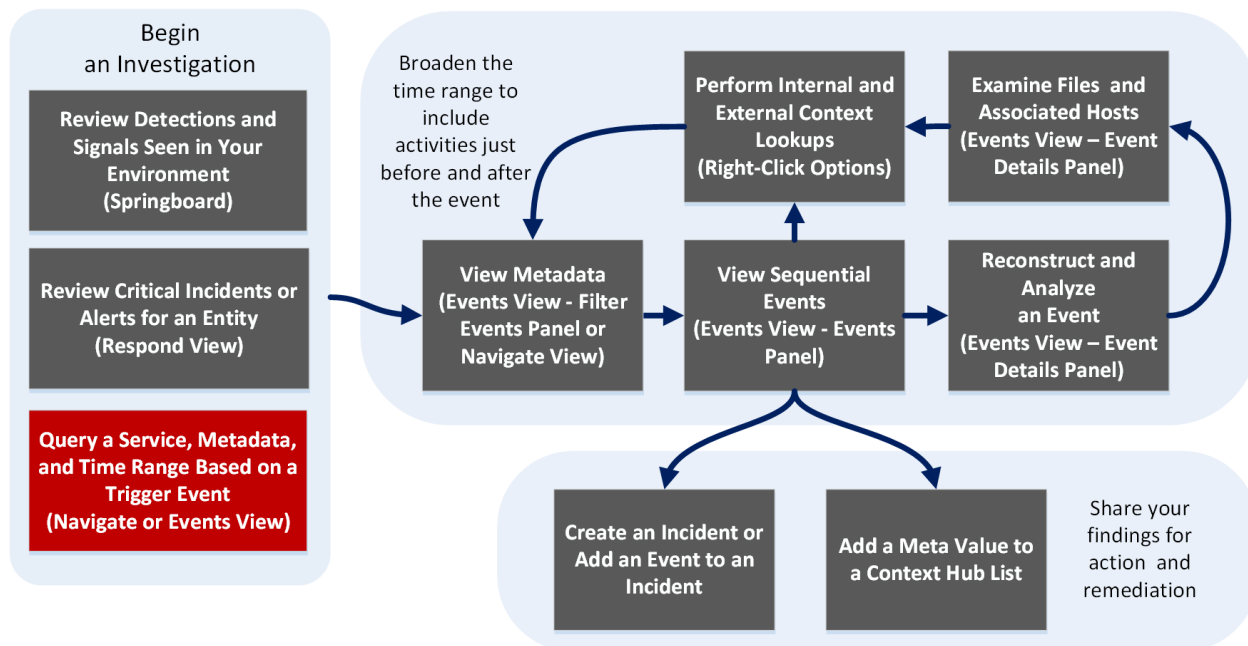
▶ - 次のページに移動

▶ - 最後のページに移動(最後のページまで既に移動した後にのみ利用可能)

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



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
インシデント対応者 脅威ハンター	重要なインシデントまたはアラートの確認 サービス、メタデータ、時間範囲のクエリを実行*	<i>NetWitness Respond</i> ユーザガイド [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

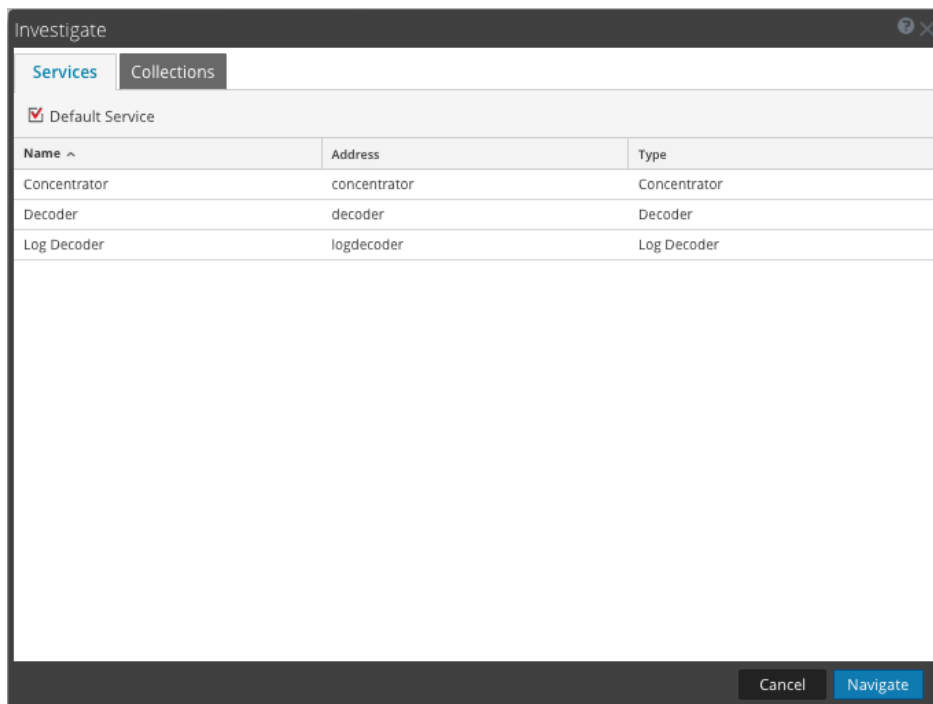
ユーザ ロール	実行したいこと	手順
脅威ハンター	メタデータの表示	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン (ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]ビューでの結果のフィルタリング [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルと関連ホストの調査	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [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



[Investigate] ダイアログには [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。
アドレス	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] の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 - [ユーザー環境設定]パネル

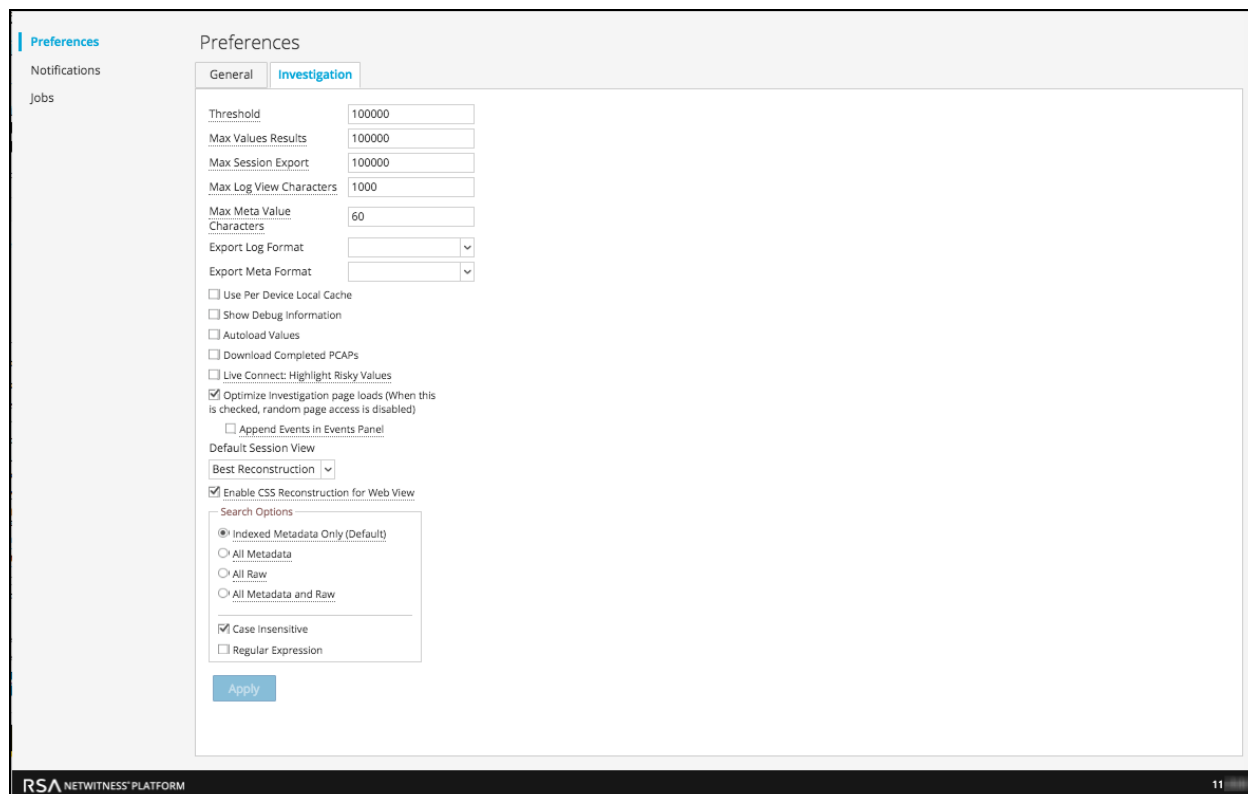
[プロファイル]ビュー> [環境設定]パネル> 調査]タブで、NetWitness Investigateでのデータの分析、イベントの表示、イベントの再構築時のNetWitnessのパフォーマンスと動作に影響を与える、いくつかの環境設定を行うことができます。このタブにアクセスするには、[サビゲート]ビューまたは[レガシー イベント]ビューから  >  Profileを選択します。[プロファイル]ビューが表示されたら、[環境設定]> [調査]を選択します。ユーザー環境設定は、NetWitnessで作業しているときにいつでも変更できます。

関連トピック

- [NetWitness Investigateの仕組み](#)
- [\[サビゲート\]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「[\[サビゲート\]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。



The screenshot shows the 'Preferences' window in NetWitness Investigate, with the 'Investigation' tab selected. The left sidebar shows 'Preferences', 'Notifications', and 'Jobs'. The main area contains the following settings:

Setting	Value
Threshold	100000
Max Values Results	100000
Max Session Export	100000
Max Log View Characters	1000
Max Meta Value Characters	60
Export Log Format	[Dropdown]
Export Meta Format	[Dropdown]

Below the input fields are several checkboxes:

- Use Per Device Local Cache
- Show Debug Information
- Autoload Values
- Download Completed PCAPs
- Live Connect: Highlight Risky Values
- Optimize Investigation page loads (When this is checked, random page access is disabled)
- Append Events in Events Panel

Default Session View: Best Reconstruction [Dropdown]

Enable CSS Reconstruction for Web View:

Search Options:

- Indexed Metadata Only (Default)
- All Metadata
- All Raw
- All Metadata and Raw

Additional checkboxes:

- Case Insensitive
- Regular Expression

An 'Apply' button is located at the bottom of the settings area.

機能	説明
閾値	<p>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。</p> <p>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。</p>
結果の最大数	<p>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。</p>
最大セッション エクスポート	<p>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。</p>
ログビューの最大文字数	<p>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。</p>
ログのエクスポート形式	<p>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。</p>
メタのエクスポート形式	<p>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。</p>
	<p>注：バージョン11.5.2にアップグレードする場合、[メタ形式のエクスポート]設定は保持されず、空白にリセットされます。バージョン11.5.2にアップグレードした後、この値を再構成する必要があります。</p>
デバイスごとのローカル キャッシュを使用	<p>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。</p>
デバッグ情報の表示	<p>このオプションが設定されている場合、NetWitness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。</p>

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	<p>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。</p> <p>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。</p>
値の自動ロード	<p>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(こは 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。</p>
完了したPCAPのダウンロード	<p>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。</p>
Live Connect リスクのある値を強調表示	<p>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IP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。</p>
調査ページのロードを最適化する	<p>[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。</p>
デフォルトセッション表示	<p>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。</p>
WebビューのCSS再構築を有効化	<p>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ヤニングと再構築、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。</p> <p>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。</p>

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。バージョン11.5では、いくつかの 調査]サブメニューがアクセスしやすいようにメイン メニューに移動しています。バージョン11.5より前の 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が開きました。調査]の下サブメニューには、[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])、[Malware Analysis]があります。[ホスト]、[ファイル]、[ユーザー](以前の [エンティティ])の各ビューには、分析ワークフローの向上のため、メインメニューからアクセスできるようになっています。

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。

調査]ビューで使用可能なすべての機能の概要については、「[NetWitness Investigateの仕組み](#)」を参照してください。

レガシー イベントの再構築]ビュー

「イベントの再構築」ビューは廃止され、「イベント」ビューに置き換えられました。「レガシー イベント」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、調査の「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。

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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
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 ユーザー 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	メタデータの表示	「ナビゲート」ビューでの結果のフィルタリング 「イベント」ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャル イベントを表示する*	「イベント」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
脅威ハンター	イベントの再構築と分析*	「イベント」ビューでのイベント詳細の調査 「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	ファイルと関連ホストを調査する*	[イベント]ビューでのデータのダウンロード [サビゲート]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

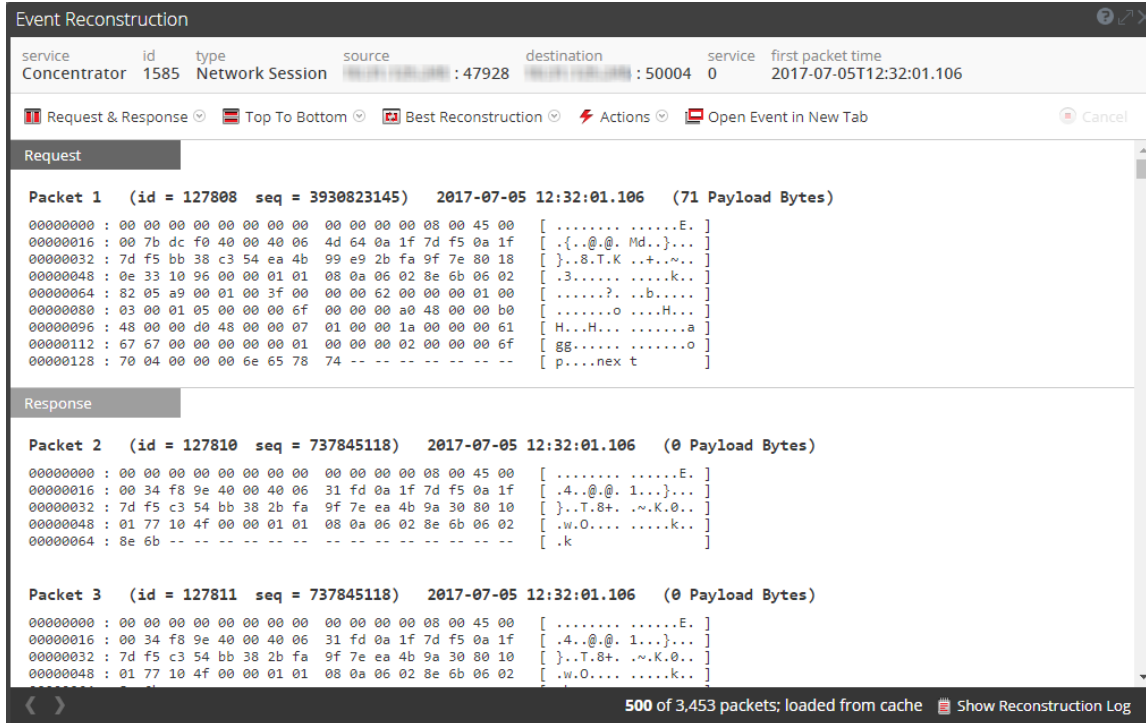
*このタスクは現在のビューで実行できます。

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。 <ul style="list-style-type: none"> 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。
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。 <ul style="list-style-type: none"> 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

機能	説明
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]ビューは廃止され、[イベント]ビューに置き換えられました。[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。

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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタートガイド
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	<i>NetWitness Respond</i> 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	メタデータの表示	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン(ベータ版)
脅威ハンター	シーケンシャルイベントを表示する*	[イベント]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
脅威ハンター	イベントの再構築と分析*	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストを調査する*	[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。

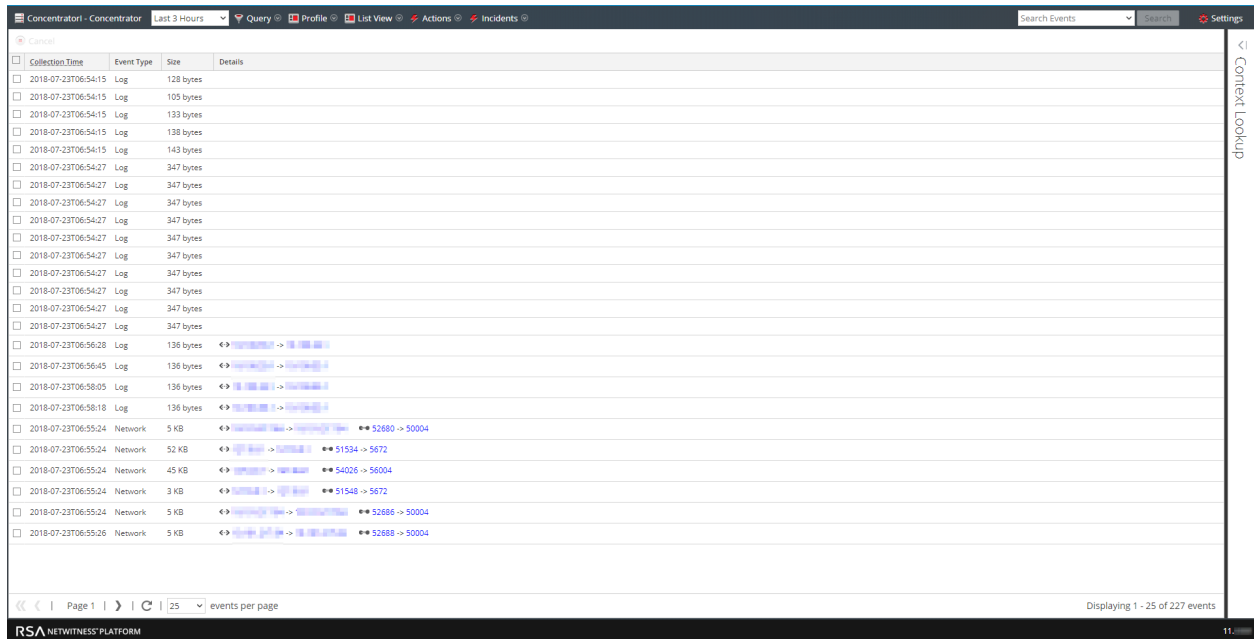
次の図は、詳細ビューのイベントの例です。[コンテキスト ルックアップ]パネルはContext Hubサービスが構成されている場合にもみ表示されます。

The screenshot displays the 'Context Lookup' window in NetWitness Investigate. The window title is 'Context Lookup' with a navigation arrow. Below the title, there is a search bar and a 'Sort' dropdown menu set to 'Date - Newest to Oldest'. The interface shows a list of alerts for the IP address 10.162.30.26. The alerts are sorted by date, with the most recent at the top. Each alert entry includes a severity level (20 or 50), a title, a creation timestamp (all from 2019/03/05), an incident ID, the source (Event Stream Analysis), and the number of events (1). The alerts alternate between severity 20 and 50. The bottom of the window indicates '50 Alerts (First 50 Results)'.

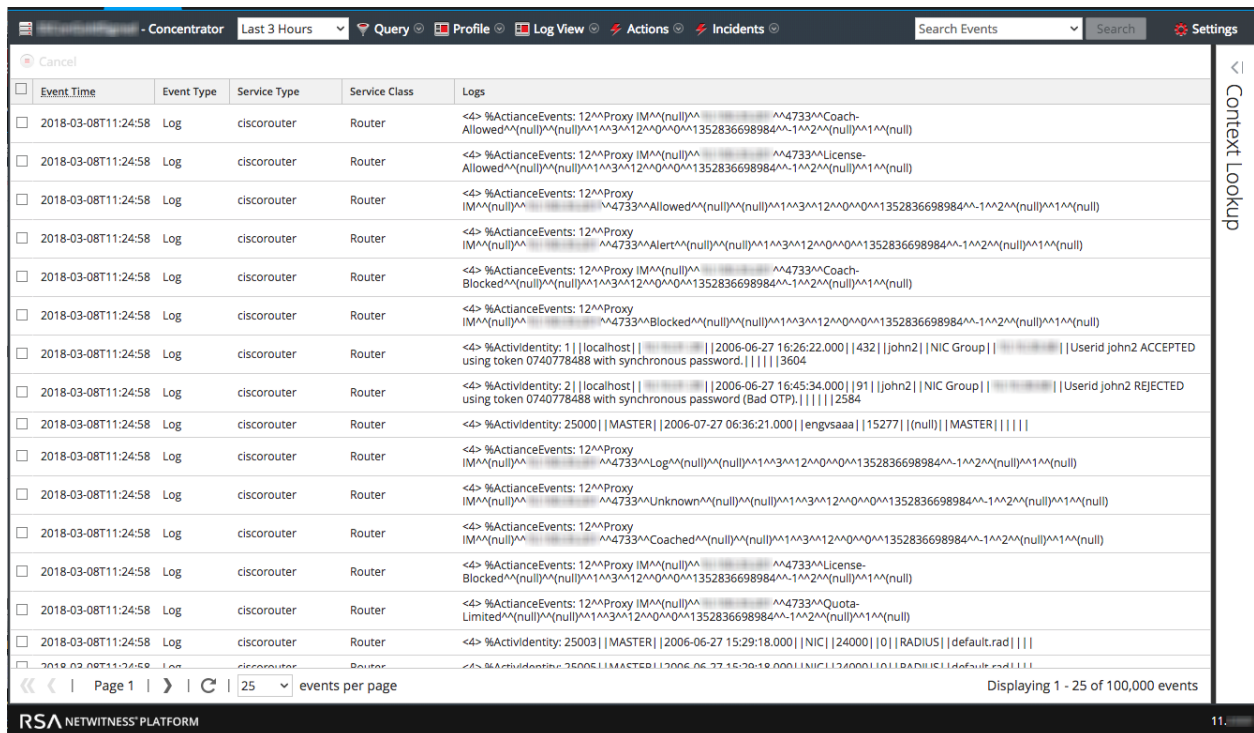
Severity	Title	Created	Incident ID	Sources	Events
20	Alert without Incident	2019/03/05, 23:32 (0 days ago)		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:32 (0 days ago)	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:31 (0 days ago)		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:31 (0 days ago)	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:29 (0 days ago)		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:29 (0 days ago)	INC-698	Event Stream Analysis	1

次の図は、リスト ビューのイベントの例です。

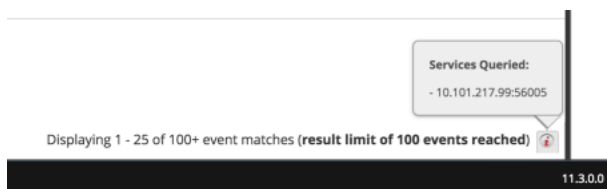
NetWitness Investigate ユーザガイド



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


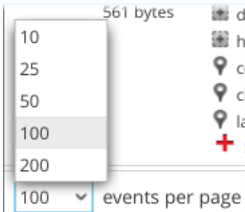
「レガシー イベント」ビューには、上部に以下のオプションを備えたツールバーがあります。

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(「 「サブジェクト」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)。
プロフィール	「プロフィール」メニューを表示します。現在選択されているプロフィー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)プロフィールとカスタム プロフィール、およびプロフィールを管理するためのオプションが含まれます。各プロフィールには、メタグループ、列グループ、イベントの調査時に「サブジェクト」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(「 クエリプロフィー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	<p>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。</p> <ul style="list-style-type: none"> 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、各ログのサマリーが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	<p>[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。</p> <ul style="list-style-type: none"> 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
<p>  (フッター) </p>	<p> 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。 </p> <ul style="list-style-type: none"> 《 - 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 <p>  1ページあたりのイベント数を選択 </p> <p> 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、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。 </p>
<p> 100,000個のイベントのうち1～100個を表示(フッター) </p> <p> 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) </p>	<p> 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。 </p>

デフォルトのメタ キーの管理]ダイアログ

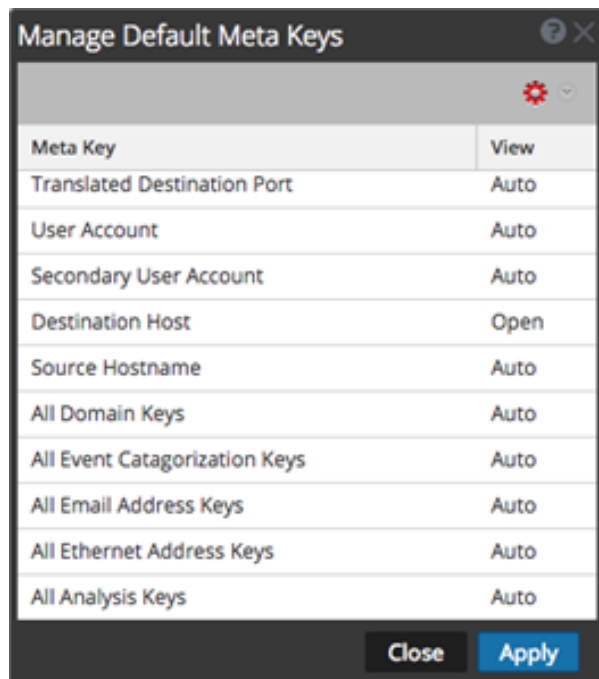
デフォルトのメタ キーの管理]ダイアログでは、アナリストは [ナビゲート]ビューの [値]パネルに表示するメタ キーを指定できます(「[Investigationでのデフォルト メタ キーの管理と適用](#)」を参照)。これにより必要なデータをさらに迅速に見つけることができ、関係のないメタ キーはロードされません。このダイアログにアクセスするには、[ナビゲート]ビューのツールバーで、[メタ] > **デフォルトのメタ キーの管理]**を選択します。

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	<p>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。</p> <ul style="list-style-type: none"> • 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は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は非表示で、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
 	<p>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。</p> <ul style="list-style-type: none"> • 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は表示されます。
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]ダイアログ

メタグループを使用して、調査に表示されるデータをフィルタ処理できます。NetWitness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、複製できませんが、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、[ナビゲート]ビューと[イベント]ビューの情報には、選択されたグループのメタキーのみが含まれます。

[ナビゲート]ビューと[イベント]ビューのメタ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。

[イベント]ビューの[メタグループ]メニュー(バージョン11.5以降)のオプションを使用して、以下を実行できます。

- 適用するメタグループの選択
- メタグループの詳細の確認
- カスタムメタグループの作成、編集、削除
- 標準提供またはカスタムのメタグループを複製して、編集します。

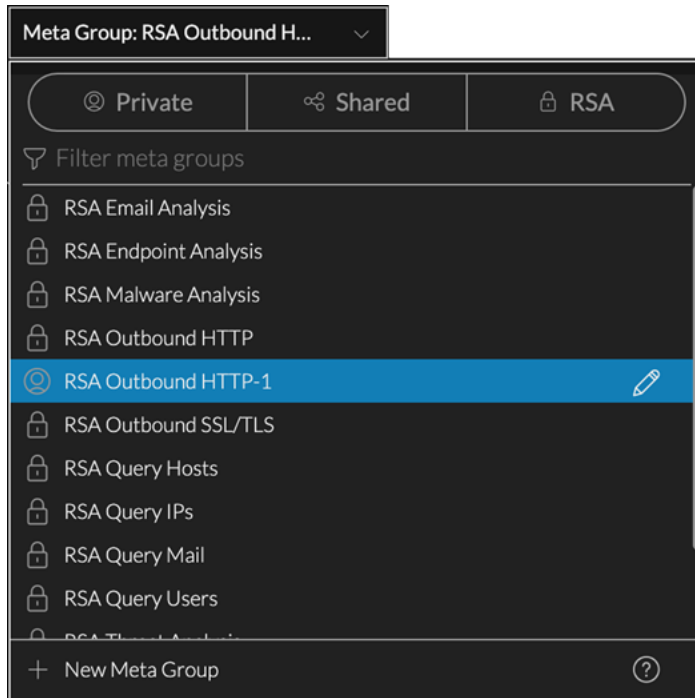
[ナビゲート]ビューの[メタグループの管理]ダイアログのオプションを使用すると、上記のすべてを実行できるだけでなく、メタグループをインポートおよびエクスポートすることもできます。詳細については、「[メタグループを使用して関連性の高いメタキーにフォーカス](#)」を参照してください。

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](#)
- [\[ナビゲート\]ビューでの結果のフィルタリング](#)

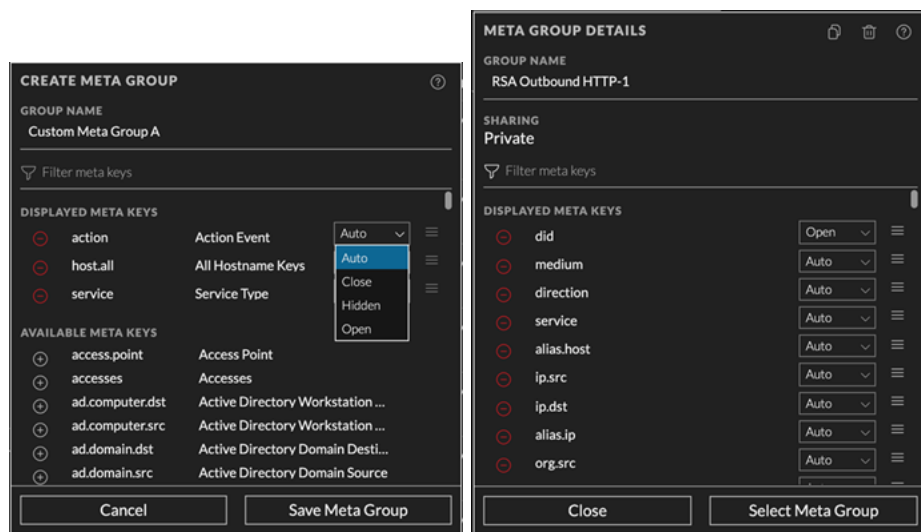
簡単な説明 - [メタグループ]メニュー、[メタグループの作成]ダイアログ、[メタグループの詳細]ダイアログ

このセクションでは、[メタグループ]メニュー、[メタグループの作成]ダイアログ、[メタグループの詳細]ダイアログについて説明します。次の図は、[メタグループ]メニューの例です。次の表に、オプションの説明を示します。





機能	説明
可視性オプション	<p>リストに表示されるメタグループのタイプを制御します。可視性オプション([プライベート]、[共有]、[RSA])を任意に組み合わせて使用できます(青 = 選択済み、黒 = 未選択)。初期状態では、どのボタンも選択されていないため、すべてのメタグループタイプが表示され、3つのボタンすべてが選択されている場合と同じ結果になります。表示オプションは、[メタグループの絞り込み]フィールドのテキストと連動します。表示オプションによって標準提供グループ(グループ名に「RSA」を含むグループ)が非表示になっている場合に、「RSA」を含んだ名前を検索すると、リストは空になります。</p> <p>プライベート = 自分だけが管理できるプライベートグループを表示 共有 = 組織内の誰でも管理できる共有グループを表示 RSA = RSAのみが管理できる標準提供グループを表示</p>
メタグループの絞り込み	<p>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、メタグループのリストを絞り込みます。</p>
メタグループリスト	<p>メタグループのリストは、カスタムグループと標準提供グループで構成されています。カスタムメタグループは、共有またはプライベートにすることができます。RSAメタグループは標準提供のメタグループです。これらを編集または削除することはできませんが、コピーを作成して編集することはできます。メタグループ名の前にあるアイコンは、プライベートグループ、共有グループ、および直接提供グループを区別します。</p>
新しいメタグループ	<p>[メタグループの作成]ダイアログを表示します。このダイアログでは、カスタムメタグループを作成できます。</p>

次の左側の図に示す [メタグループの作成] ダイアログを使用して、カスタムメタグループを定義できます。右側の図は、カスタムメタグループの編集に使用できる [メタグループの詳細] 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。

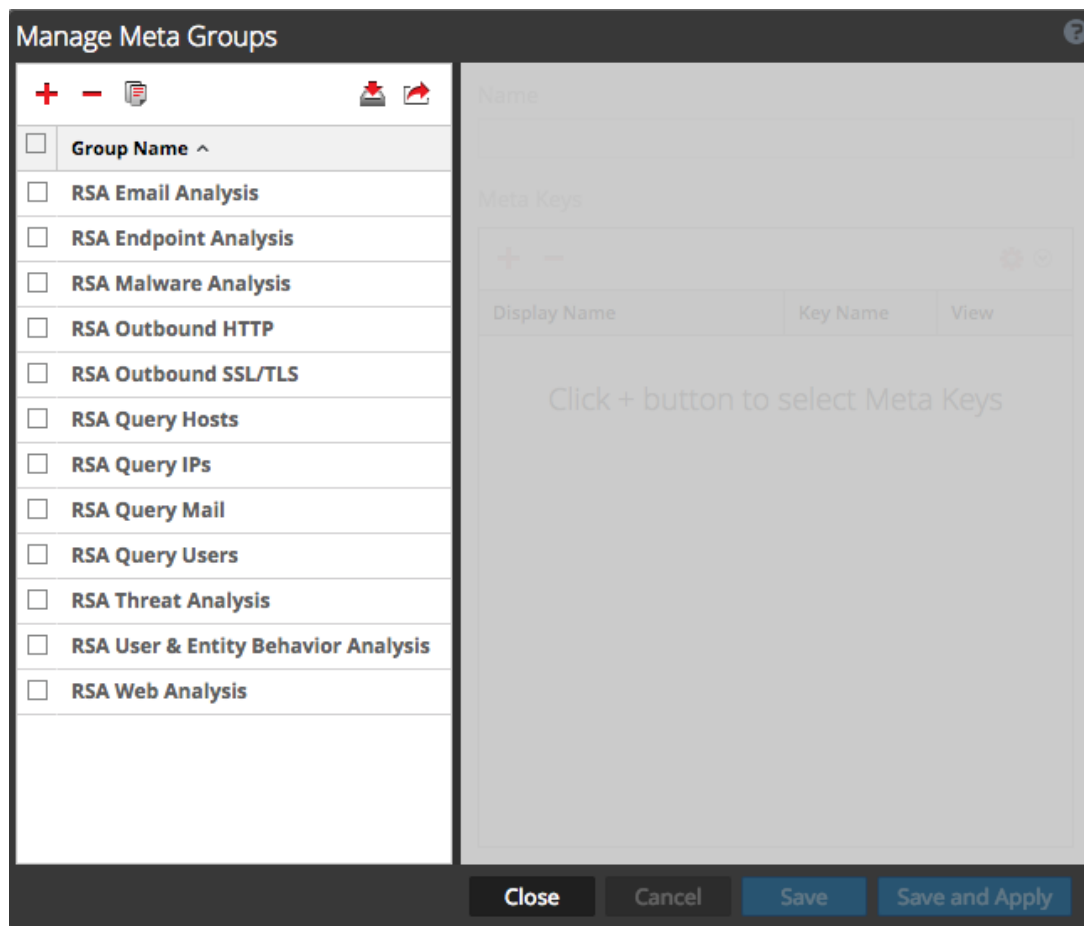


機能	説明
	コピーを編集できるように、メタグループのコピーを作成します。これは、標準提供グループの独自のコピー、プライベートグループの共有コピー、または共有グループのプライベートコピーが必要な場合に役立ちます。
	現在編集中のカスタムメタグループを削除します。このアクションは元に戻せず、グローバルに適用されます。メタグループが共有グループの場合は、誰も使用できなくなります。
グループ名	メタグループの名前を表示します。64文字以内の一意の名前を指定してください。カスタムメタグループの名前を編集する場合は、このフィールドに入力します。
共有	メタグループを共有するかプライベートにするかを指定します。この設定は、初めてグループを作成するときに使用できます。作成後、共有列グループをプライベートに変更したり、プライベート列グループを共有に変更したりすることはできません。
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	カスタムメタ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()。[メタキーの絞り込み]フィールドにテキストを入力すると、ドラッグアンドドロップは無効になります。表示されるメタキーごとに、以下を選択できます。






機能	説明
選択可能なメタキー	<p>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。各メタキーの初期ビュー([開く]、 [閉じる]、 [隠す]、または [自動])(デフォルト設定))を設定することもできます。</p>
初期表示オプション	<p>メタキーごとに、初期表示オプションを次のように設定できます。</p> <ul style="list-style-type: none"> - [自動] に設定されている場合、メタキーは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。インデックスなしのメタキーは手動で開くまで閉じたままになります。メタグループのデフォルトの初期表示状態を [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。 - [開く] に設定したメタキーは、[イベントの絞り込み] パネルに一覧表示され、値がロードされます。 - [閉じる] に設定したメタキーは、[イベントの絞り込み] パネルに一覧表示されますが、メタキーを開くまでメタ値はロードされません。 - [隠す] に設定したメタキーは、[イベントの絞り込み] パネルに表示されません。この機能は、複数のメタグループを作成する代わりに、単一のメタグループを複数の目的で使用している場合に役立ちます。メタグループから削除せずに特定のキーをオフにすることができます。[隠す] は、新しいメタキーをテストする場合や、まだ使用できない新しいメタキーを含んだメタグループを準備する場合にも使用できます。[自動]、[開く]、[閉じる] を選択した場合に発生するエラーを回避できます。
	<p>[表示するメタキー] リストにメタキーをドラッグアンドドロップして、希望の順序でデータを表示できます。</p>
閉じる] ボタン	<p>ダイアログを閉じます。</p>
メタグループの保存	<p>[メタグループを作成] ダイアログにのみ表示され、新しいメタグループを保存します。</p>
リセット	<p>[メタグループの詳細] ダイアログにのみ表示され、編集したメタグループを前回保存された状態に戻します。</p>
メタグループの更新	<p>[メタグループの詳細] ダイアログにのみ表示され、編集したメタグループに変更を適用します。</p>
メタグループの選択	<p>メタグループを適用します。[イベントの絞り込み] パネルが更新され、選択したメタグループのメタキーのみが表示されます。</p>

簡単な説明 - [メタグループの管理] ダイアログ









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。このプロパティは、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。 <ul style="list-style-type: none"> 非表示] :これらのメタキーはデフォルトでは非表示で、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は表示されます。 折りたたみ表示] :このメタキーの値はデフォルトでは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description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name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。 <ul style="list-style-type: none"> 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。

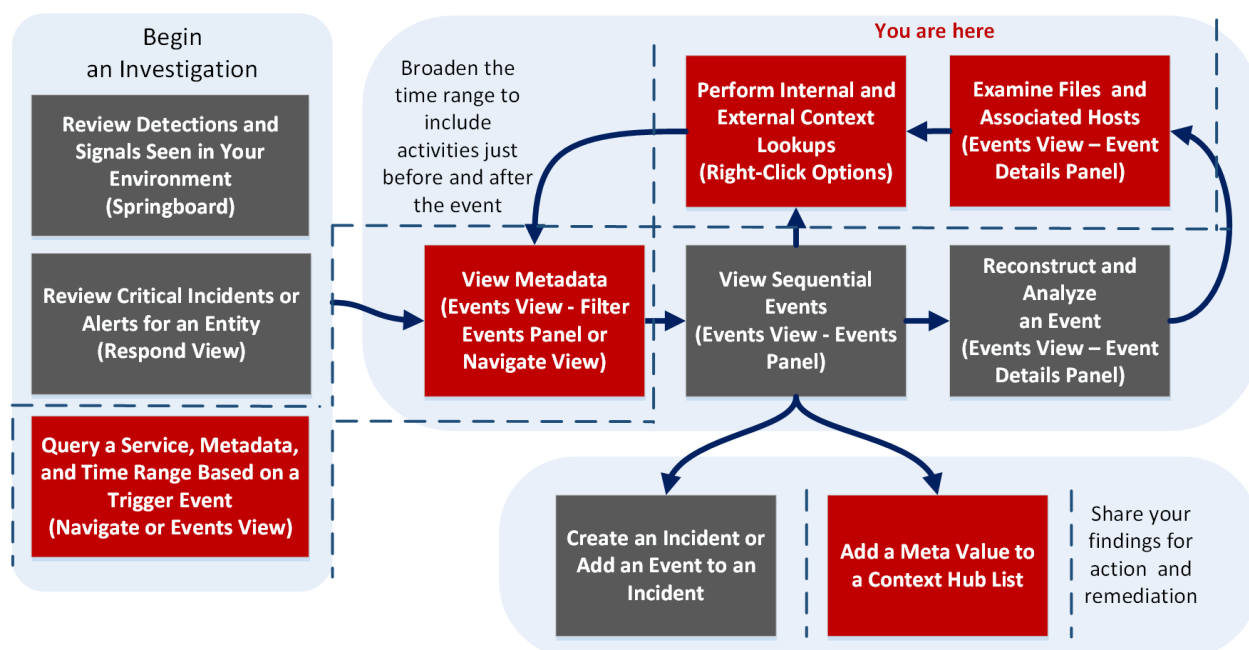
機能	説明
閉じる	ダイアログを閉じます。
キャンセル	すべての変更をキャンセルします。
保存	すべての変更を保存します。
保存して適用	すべての変更を保存して、直ちに適用します。

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。

注：バージョン11.6では、[イベント]ビューの[イベントの絞り込み]パネルがこの機能を提供するため、デフォルトでナビゲート]ビューは無効になっています。ナビゲート]ビューを有効にするには、「[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。

ワークフロー



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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	<i>NetWitness Platform</i> スタート ガイド
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	<i>NetWitness Respond</i> 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	メタデータの表示*	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン (ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストを調査する*	[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

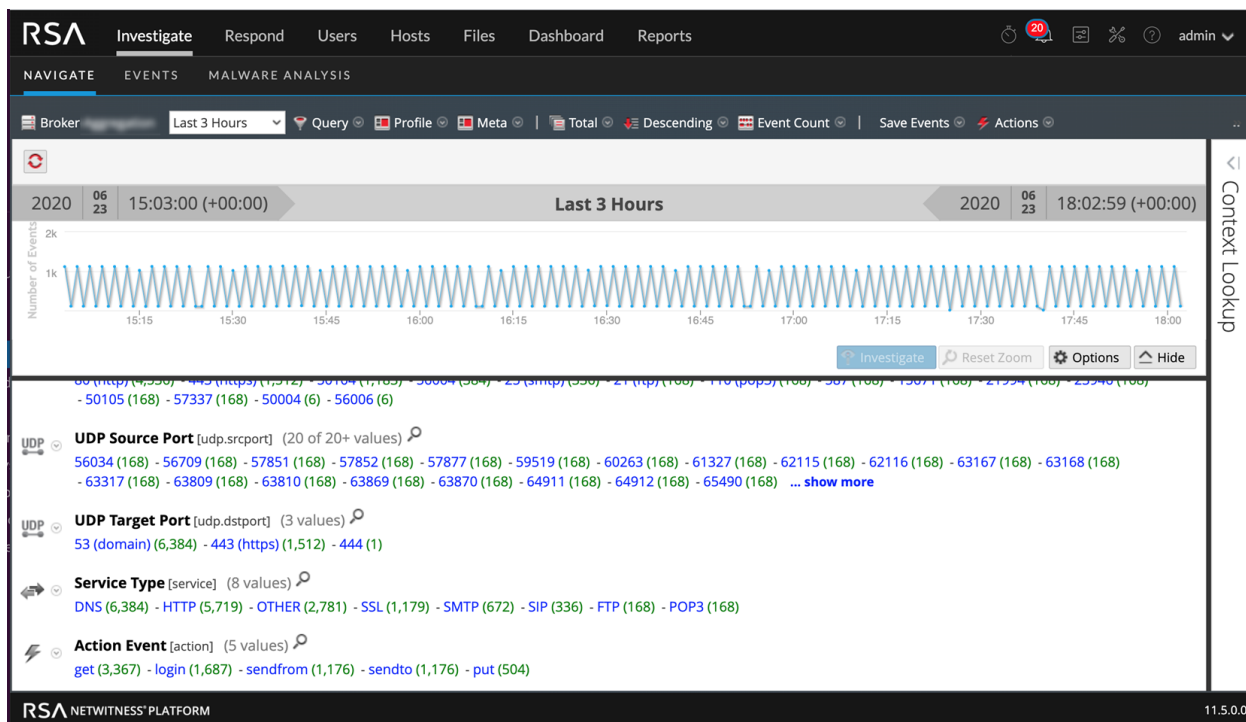
*このタスクは現在のビューで実行できます。

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、バージョン11.5の [レガシー イベント]ビューを示しています。



[レガシー イベント]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。
- 表示するデータの範囲を調整する。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
	<p>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(「[サビゲート] 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。</p>

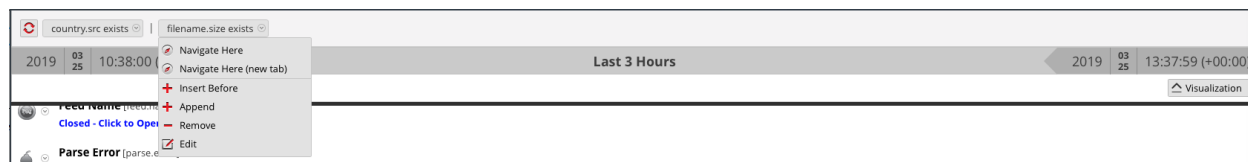
オプション	説明
時間範囲	<p>時間範囲オプションが表示されます。ツールバーには現在選択されているオプションが表示されます(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。選択可能なオプションは次のとおりです。</p> <ul style="list-style-type: none"> • すべてのデータ • 直近5、10、15、30分 • 直近1、3、6、12、24時間 • 直近2、5日間 • 早朝 • 午前 • 午後 • 夕方 • 終日 • 昨日 • 今週 • Last Week • カスタム <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>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。</p> </div>
クエリ	<p>[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。</p>
プロファイル	<p>[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)、[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。</p>
メタ	<p>[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)。</p>

オプション	説明
整列フィールド	<p>「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。メニューには次の2つのオプションがあります。「合計で整列」と「値で整列」です。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(「「サビゲート」ビューでの結果のフィルタリング」を参照してください)。</p>
ソート 順	<p>「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。メニューには次の2つのオプションがあります。「昇順でソート」と「降順でソート」です。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(「「サビゲート」ビューでの結果のフィルタリング」を参照してください)。</p>
集計方法	<p>「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、メタ値の数量(かっこで囲まれた緑色の数字)を計算するための3つのオプション、[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]が表示されます(「「サビゲート」ビューでの結果のフィルタリング」を参照してください)。</p> <p>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。</p> <p>パケット データの場合：</p> <ul style="list-style-type: none"> • [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。 <p>ログ データの場合：</p> <ul style="list-style-type: none"> • [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。
イベントの保存	<p>「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)。</p>
アクション	<p>アクションメニューには、[サビゲート]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。</p>
イベントの検索	<p>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(「「サビゲート」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)。</p>

オプション	説明
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、各クエリがトランッキングされます。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。
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)。
追加	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。

機能	説明
>>	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、ナビゲートしているサービスがBroker(NetWitness)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。

以下に例を示します。

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info exists)$stime='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。

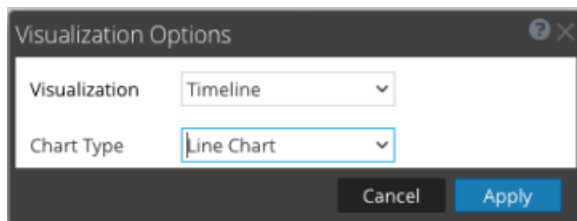


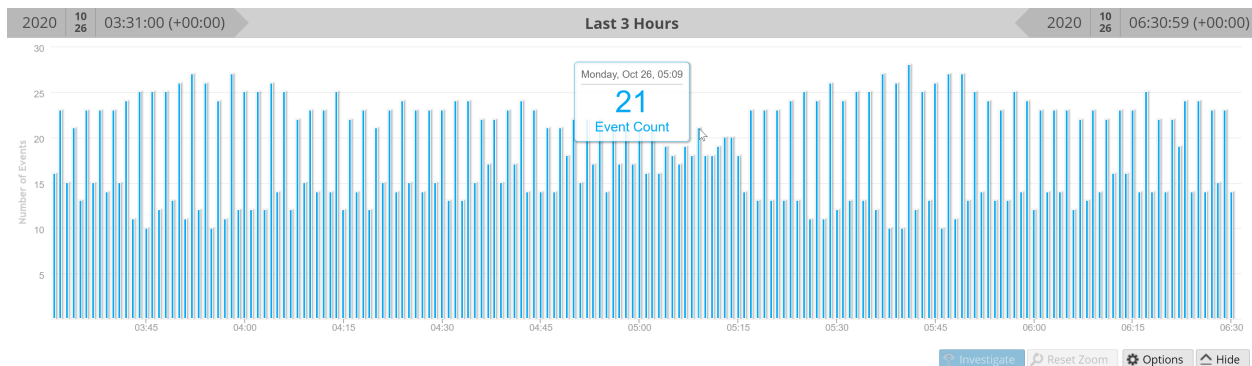
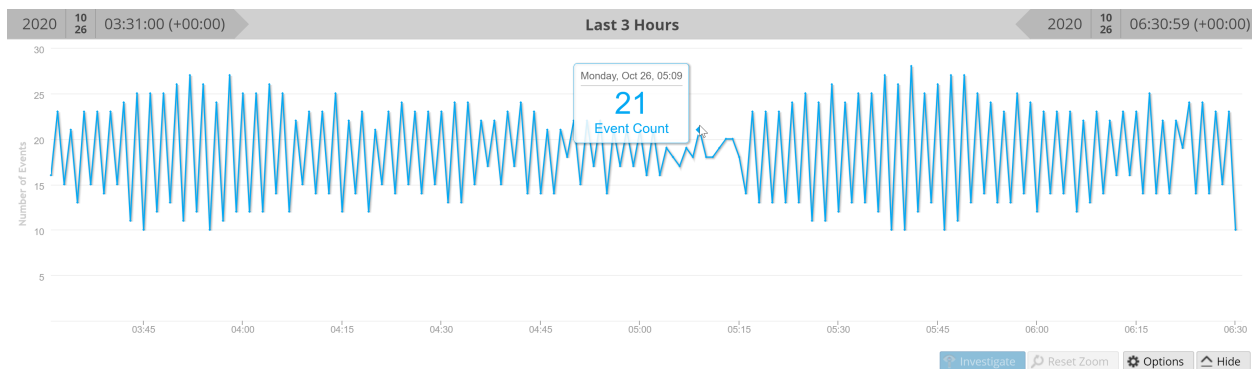
ビジュアル画像

「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)。チャートの表示では、表示と非表示を切り替えたり、オプション(タイムライン表示または座標表示のいずれか)を選択することができます。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。



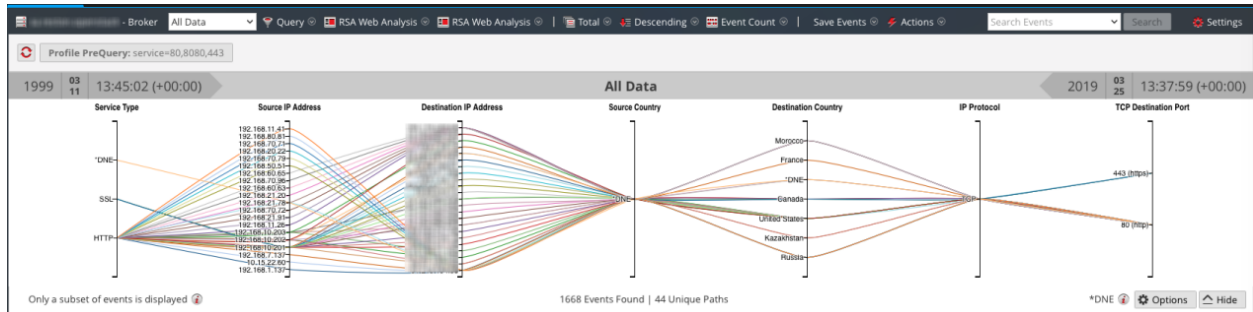


タイムラインには、指定したサービスと時間範囲のアクティビティが表示されます。表示の形式は、[オプション]メニューでの選択に応じて、折れ線グラフか棒チャートになります。

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(「[メタデータを座標表示チャートに追加する](#)」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、プロフィー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。
見つけたイベントの数 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	ビジュアル化タイプのドロップダウンリストを表示します。タイムライン表示と座標表示

機能	説明
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。
	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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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（「[Investigation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

	<ul style="list-style-type: none"> • 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。この例では、 値 パネルに表示されるメタグループ名は All User Keys [users.all] 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によるキーのクエリ順に表示されます。NetWitness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に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によって結果が値パネルに表示されます。

1. NetWitness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の場合は、NetWitnessでは各メタ キーの値の下にロード時間情報が表示され、集計されたサービスに関するロードの詳細情報が表示されます。また、NetWitnessでは階層リンクの下には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。

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または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	NetWitness Platform スタート ガイド
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	メタデータの表示	[ナビゲート]ビューでの結果のフィルタリング [イベント]ビューでのメタデータのドリルダウン (ベータ版)
脅威ハンター	シーケンシャル イベントを表示する	[イベント]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
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [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	ファイルと関連ホストの調査	[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

ユーザロール	実行したいこと	手順
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
- 直近

[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

Query Profile Meta Total Descending Event Count S

Simple Advanced Recent

Select Meta Operator Value

Network Log Endpoint

Apply Cancel Reset ?

詳細]ビュー

Simple Advanced Recent

Apply Cancel Reset ?

最近実行したクエリ]ビュー

Simple
 Advanced
 Recent

did = 'nwappliance3067'

sessionid=13

sessionid>52

sessionid>44

sessionid>20

sessionid>202


sessionid>200

ip.src=" [IPアドレス] "

ip.src = [IPアドレス]

ip.src= [IPアドレス]

ip.dst = [IPアドレス]



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!=、NetWitnessexists、NetWitness!exists) のドロップダウンリストを表示します。
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。

機能	説明
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、および制限フィルター(プレクエリ条件)を迅速かつ簡単に定義する方法を提供します(「[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)。同じクエリプロファイルはすべてのビューで共有され、スプリングボード(バージョン11.5)のパネルで使用できます。[イベント]ビューで作成されたプライベート クエリプロファイルは、それを作成したアナリストの [イベント]ビューでのみ使用可能になります。

クエリプロファイルはそれぞれ、メタグループや列グループを指定し、場合によっては、調査のタイプに適したプレクエリ条件を含んでいます。

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。(「[イベント リストでの列と列グループの使用](#)」を参照)。
- クエリプロファイルを有効にすると、オプションのプレクエリ条件によって、クエリバーに制限フィルタが追加されます。制限フィルターを編集または削除してから、クエリに対して追加のフィルターを作成できます(「[\[イベント\]ビューでの結果のフィルタリング](#)」を参照)。

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。

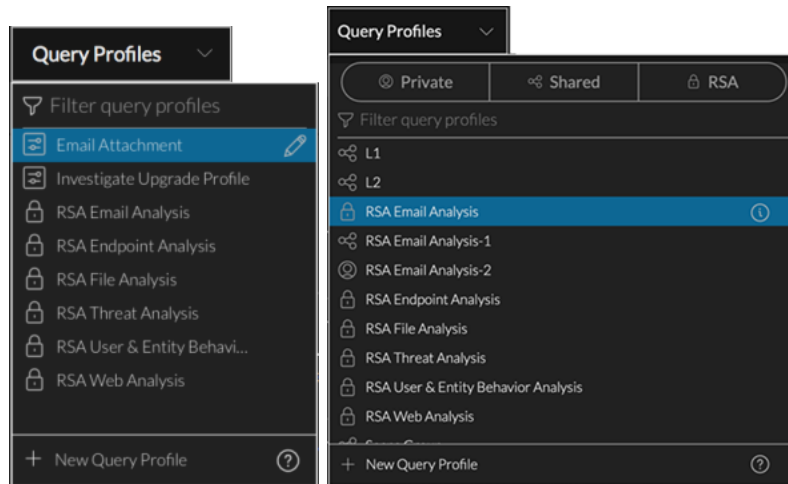
- [プロファイルの管理]ダイアログは、[ナビゲート]ビュー、[レガシー イベント]ビュー(バージョン11.4以降)、[イベント]ビュー(バージョン11.3以前)で開くことができます。このダイアログにアクセスするには、[ナビゲート]ビューまたは [レガシー イベント]ビューのツールバーで [プロファイル] > [プロファイルの管理]を選択します。
- [クエリプロファイルの作成]ダイアログは、11.4以降の [イベント]ビューから開くことができます。このダイアログにアクセスするには、[イベント]ビューのクエリバーで [クエリプロファイル] > [新しいクエリプロファイル]を選択します。
- [クエリプロファイルの詳細]ダイアログは、11.4以降の [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]ビューのクエリバーで [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](#)
- [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](#)
- [\[ナビゲート\]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

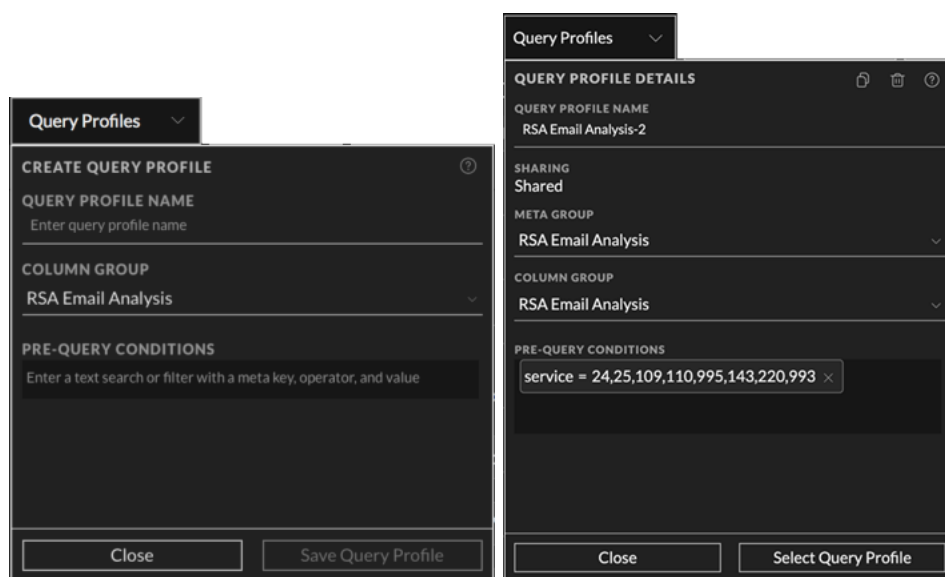
このセクションでは、クエリプロファイル]メニュー、クエリプロファイル]ダイアログ、クエリプロファイルの詳細]ダイアログについて説明します。次の図は、クエリプロファイル]メニューの例です。表にはオプションの説明が記載されています。左側の例では、標準提供プロファイルがハイライト表示されているため、情報アイコンが表示されています。左側はバージョン11.4のメニューで、右側はバージョン11.5のメニューです。



機能	説明
可視性オプション	<p>リストに表示されるクエリプロファイルのタイプを制御します。可視性オプション(プライベート]、 共有]、 RSA])を任意に組み合わせて使用できます(青 = 選択済み、黒 = 未選択)。初期状態では、どのボタンも選択されていないため、すべてのプロファイルタイプが表示され、3つのボタンすべてが選択されている場合と同じ結果になります。表示オプションは、クエリプロファイルの絞り込み]フィールドのテキストと連動します。表示オプションによって標準提供プロファイル(名前に「RSA」を含むグループ)が非表示になっている場合に、「RSA」を含んだ名前を検索すると、リストは空になります。</p> <p>プライベート = 自分だけが管理できるプライベート グループを表示 共有 = 組織内の誰でも管理できる共有グループを表示 RSA = RSAのみが管理できる標準提供グループを表示</p>
クエリプロファイルの絞り込み	<p>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、クエリプロファイルのリストを絞り込みます。</p>

機能	説明
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、RSA Email Analysis-1とRSA Email Analysis-2がカスタム プロファイルです。RSA Email Analysis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。

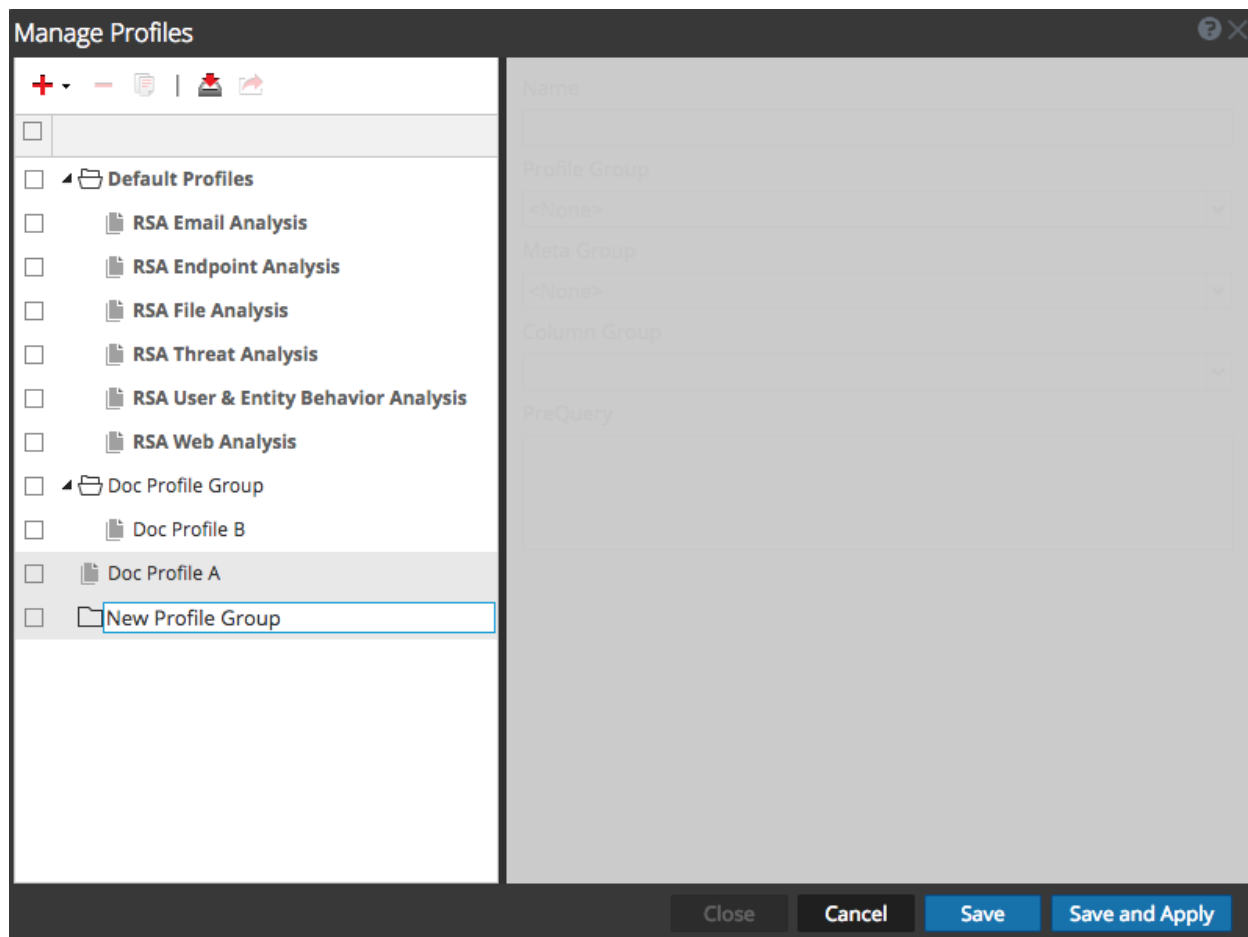


機能	説明
📄	コピーを編集できるように、メタグループのクローンを作成します。これは、標準提供グループの独自のコピー、プライベートグループの共有コピー、または共有グループのプライベートコピーが必要な場合に役立ちます。
🗑️	[クエリプロファイルの詳細] ダイアログでカスタム プロファイルを削除します。このアクションは元に戻すことができず、グローバルに適用されます。このサービスで削除されたプロファイルを使用しているすべてのアナリストが、このプロファイルを使用できなくなります。






機能	説明
クエリ プロ ファイ ル名	プロフィー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。カスタムプロフィールでは、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。カスタムプロフィールでは、列グループを変更できます。
プレク エリの 条件	[イベント]ビューの結果の制限フィルターを定義します。新しいプロフィー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。カスタムプロフィールでは、[プレクエリの条件] フィールドで、事前入力されたプレクエリ条件の削除、テキスト検索用の追加のテキストや追加のフィルターの入力を行うことができます。プレクエリ条件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	[クエリプロフィールの作成]ダイアログにのみ表示され、新しいプロフィールを保存します。
リセッ ト	[クエリプロフィールの詳細]ダイアログにのみ表示され、編集したプロフィー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	[クエリプロフィールの詳細]ダイアログにのみ表示され、編集したプロフィールに変更を適用します。
クエリ プロ ファイ ルを 選択	クエリプロフィールを適用します。

簡単な説明 - [プロフィールの管理]ダイアログ

次の図は [プロフィールの管理]ダイアログの例で、複数のプロフィー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。
	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。 <ul style="list-style-type: none"> • 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、[サビゲート]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。 <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> • 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。
	<p>注：バージョン11.5.2にアップグレードする場合、メタ形式のエクスポート設定は保持されず、空白にリセットされます。バージョン11.5.2にアップグレードした後、この値を再構成する必要があります。</p>
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、[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 :リスクの高いIPのハイライト表示	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、[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。

[ラグシー イベント]ビューの 設定]ダイアログ

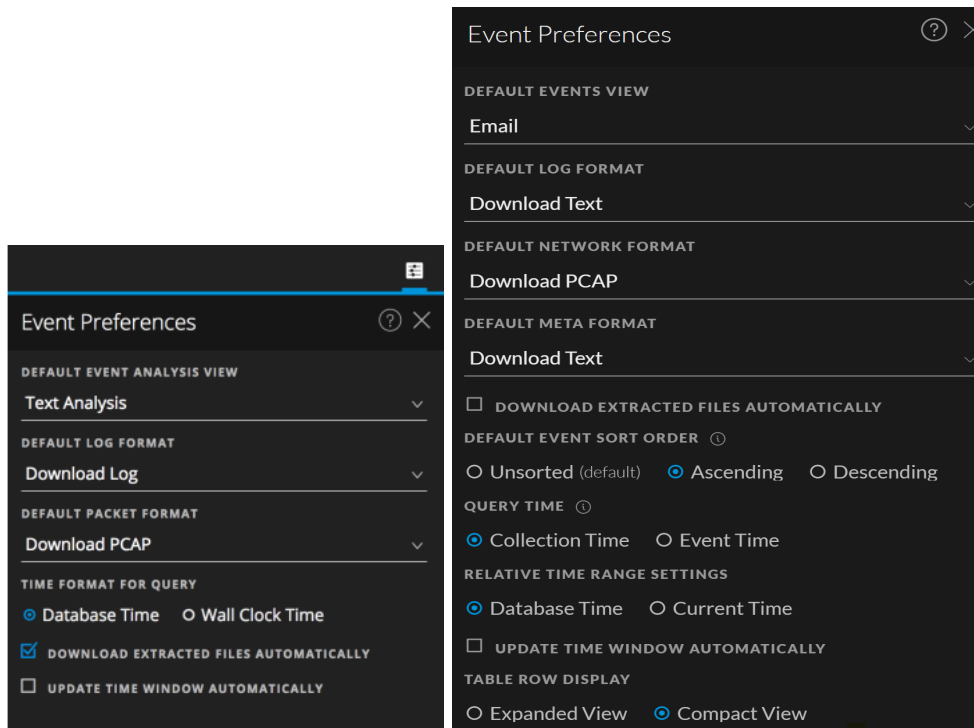
次の図は [ラグシー イベント]ビューの 設定]ダイアログの例です。また、その機能について表で説明します。

機能	説明
ログのエクスポート形式	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p>
Live Connect :リスクの高いIPのハイライト表示	<p>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によってすべてのIP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。</p>

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、[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ようになります。これには、イベントに関連するスキャンングと再構築、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、[プロフィール] 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] ビューにユーザー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11.6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	<p>[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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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(log)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 packets 形式またはデフォルトのネットワーク形式	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>[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。</p> <div data-bbox="467 1035 1417 1314" style="border: 1px solid green; padding: 5px;"> <p>注 :(バージョン11.6) 現在の時刻]は、相対時間範囲の設定]のデフォルトです。以前のバージョンでは、データベースの時間]がデフォルト値でした。これにより、[イベント]ビュー(デフォルトとして 現在の時刻]を使用)と[ナビゲート]ビュー(デフォルトとして データベースの時間]を使用)の間で時間範囲の不一致が生じる可能性があることに注意してください。この変更は既存のユーザーには影響せず、新しいユーザーにのみ適用されます。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。</p> </div> <p>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。</p>

機能	説明
<p>イベントのソート順 (バージョン11.4以降)</p>	<p>[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 [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。この設定の変更は、次のクエリ送信時に有効になります。</p> <p>ソートしない :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、処理が高速になります。これは、一致するイベントが見つかったら即座に表示するのと、すべてのコアサービスの応答を待ってから指定された順に結果を並べ替えて表示する違いによるものです。</p> <p>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。</p> <p>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」に変更する必要があります。</p>
<p>抽出したファイルを 自動ダウンロード</p>	<p>[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。</p> <p>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。</p>
<p>タイム ウィンドウを 自動的に更新</p>	<p>(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。</p> <p>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。</p> <p>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。</p>