NetWitness® Platform

バージョン12.5

Investigateユーザー ガイド

NETWITNESS
Platform

連絡先

NetWitnessコミュニティ(https://community.netwitness.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およびその他の商標は、RSA Security LLCまたはその関連会社(「RSA」) の商標または登録商標です。RSAの商標のリストについては、https://www.rsa.com/en-us/company/rsa-trademarksを参照してください。その他の商標は、それぞれの所有者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。

サードパーティのリポジトリを展開したり、サポートされているNetWitnessバージョンに含まれない基盤となるNetWitnessオペレーティング システムに変更を加えたりしないことをお勧めします。NetWitnessが承認したイメージ以外でのこのような変更は、サービスまたは機能の競合を引き起こす可能性があり、NetWitnessを最適化された機能状態に戻すにはNetWitnessシステムの再イメージ化が必要になる場合があります。サードパーティのリポジトリが展開された場合、またはNetWitnessの承認なしに顧客がサポートされていない変更を行った場合、トラブルシューティングの取り組みまたはサービスの再イメージ化によって問題が解決されるまで、システムの誤動作については顧客が全責任を負います。

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、NetWitnessコミュニティ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、本製品のユーザーは、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。

ディストリビューション

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

この資料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は、この資料に記載される情報に関する、どのような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への適応性に対する黙示的保証はいたしません。

その他

この製品、このソフトウェア、関連ドキュメント、およびそのコンテンツは、このドキュメントの発行日時点で有効なNetWitnessの標準利用規約に従うものとし、これらの利用規約は https://www.netwitness.com/standard-form-agreements/ で確認できます。

© 2024 RSA Security LLC or its affiliates.All Rights Reserved.

2024年9月

目次

NetWitness Investigateの仕組み 15

メタデータ、メタ キー、メタ値 、メタ エンティティ 15

調査のトリガー 16

調査のワークフロー 16

メタデータ、クエリ、時間に焦点を当てた調査 22

[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 24

NetWitness Investigate [調査]ビュー 24

ナビゲートビュー 24

[イベント]ビュー 25

[レガシー イベント]ビュー 27

イベントのコンテキスト情報 28

再構築とイベントの分析 30

NetWitnessの [調査]ビューおよび環境設定の構成 32

[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 33

一般的な設定の構成 33

[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 34

[ナビゲート]ビューでの値のロード パラメータの調整 36

[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 37

デフォルトのログ エクスポート形式の構成 38

デフォルトのメタ値エクスポート形式の構成 38

[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 38

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 39

検索オプションの構成 39

[イベント]ビューの構成 41

デフォルトの [調査]ビューの設定 41

[イベント]ビューのユーザ環境設定の設定 41

[イベント]ビューのメタ値ロード パラメーターの設定 45

調査の開始 47

メタデータ、RAWイベント 、イベント分析にフォーカス 47

ホストとファイルにフォーカス 47

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 48

ファイルのマルウェア スキャンにフォーカス 48

[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 49

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) 50

デフォルトのサービスの設定またはクリア 51

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) 52
調査するサービスまたはコレクションの変更 53
Workbenchのリストア コレクションの調査 54
[イベント]ビューでの調査の開始 56
[イベント]ビューへのアクセス 56
タイムラインでの調査 59
タイムラインを展開する 60
タイムライン設定を使用する 61
タイムラインをズームする 62
タイムラインをパンする 63
時間範囲の選択 63
結果セットの絞り込み 65
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 66
Liveメタ グループ 66
デフォルトのメタ キー グループ 67
カスタム メタ グループ 68
[イベント]ビューでのメタ グループの操作 69
メタ グループに含まれているメタ キーの表示 69
メタ グループの選択 70
カスタム メタ グループの作成 71
カスタム メタ グループの削除 73
カスタム メタ グループの編集 74
メタ グループをコピーする 76
メタ グループ フォルダ 80
メタ グループ フォルダの作成 80
メタ グループ フォルダの編集と移動 81
メタ グループ フォルダのコピー 81
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 82
Liveから導入されたメタ グループ フォルダのコピー 83
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 84
メタ グループの作成とメタ キーの追加 84
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 99
Live列グループ 100

カスタム列 グループ 102
フォルダのフィルタ処 理 103
列 グループを管 理するためのダイアログ 103
［イベント］ビューでの列と列 グループの操 作 105
手 動での表 示する列 の選 択と列 の順 序と幅 の調 整 105
［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 106
列 による並 べ替 え 106
列 による並 べ替 え 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 114
カスタム列 グループの編 集 116
列 グループのコピーを作 成 する 118
列 グループ フォルダの作 成 121
列 グループ フォルダの編 集と移 動 121
列 グループ フォルダのコピー 121
Liveから導 入 されたグループ フォルダのコピー 122
列 グループ フォルダの削 除 123
［レガシー イベント］ビューでの列 グループの操 作 124
列 グループの選 択 124
［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 125
列 グループの削 除 (［レガシー イベント］ビュー) 128
列 グループの編 集 (［イベント］ビュー) 129
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) 132
保 存 済みクエリを使 用した調 査 の共 通 領 域 のカプセル化 134
標 準 提 供 の保 存 済みクエリ 134
Live保 存 済みクエリ 135
カスタム保 存 済みクエリ 135
保 存 済みクエリを管 理するためのダイアログ 136
保 存 済みクエリの詳 細 の表 示 (［イベント］ビュー) 138
保 存 済みクエリの適 用 (［イベント］ビュー) 140
カスタム保 存 済みクエリの作 成 または編 集 (［イベント］ビュー) 141
カスタム保 存 済みクエリの削 除 (［イベント］ビュー) 144
保 存 済みクエリのコピー 145
保 存 済みクエリ フォルダの作 成 147
保 存 済みクエリ フォルダの編 集と移 動 148
保 存 済みクエリ フォルダのコピー 149
Liveから導 入 された保 存 済みクエリ グループ フォルダのコピー 150
保 存 済みクエリ フォルダの削 除 151

[イベント]ビューでのスプリングボード パネルの追加 152
[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) 154
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) 155
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) 157
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) 158
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) 158
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) 159
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) 159
イベントビューでメタデータのドリルダウン 160
動作モード 161
[イベント メタ]パネルでメタデータを表示する 162
メタ グループの最大値を表示する 163
[イベント メタ]パネルで [コンテキスト ルックアップ]パネルを表示する 164
表示可能なメタデータについて 165
メタ データのロードを停止して再開する 166
1つを除き、すべてのメタ キーを閉じるには 166
メタ値の並べ替え方法を設定する 167
メタ値をドリルダウンする 170
メタ キーのメタ値をコピーする 172
選択したメタ値をLiveで表示する 173
[統合]パネルでのメタ値の調査の追加および再フォーカス 173
[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 184
[イベント]パネルでの結果の絞り込み 185
[イベント メタ]パネルを使用したメタ情報の絞り込み 185
クエリー ビルダーの概念 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
クエリビルダー 190
メタ キーのキャッシュによるロードの高速化 190
テキスト フィルタ 190
テキストを手入力する代わりにペースト 190
すべてのフィルタの選択とすべてのフィルタのコピー 190
最近のクエリの使用 190
高度な演算子の使用 191
AND/OR演算子の使いやすさ 191
括弧の不均衡の自動修正 191
使用可能な値に関するヒント 192
CIDR表記と略記 192

値の範囲またはリスト 192
メタキーと演算子の後にスペースを空ける必要はありません 192
時間範囲を選択 193
クエリの送信 196
クエリの実行のキャンセル 197
クエリーのステータスの表示 197
ガイド モードでのクエリの作成 199
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 202
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 208
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 210
クエリ バーですべてのフィルタを選択し、すべてのフィルタをコピーする 212
クエリー バーでテキストの貼り付け 213
最近のクエリーに基づくフィルターの挿入 214
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 216
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 217
詳細モードでのクエリーの作成 218
フリーフォーム モードでのクエリの作成 219
[ナビゲート]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
[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 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 234
[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 234
[レガシー イベント]ビューでのイベントのページ移動 235
[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 236
基本的な方法を使用したクエリの作成 236
高度な方法を使用したクエリの作成 237
最近実行したクエリの適用 239
[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 241
キーワード テキスト検索 241
検索の動作を制御するオプション 242
正規表現検索の構文 244
Rawテキスト キーワード検索 244
検索手順 244
[ナビゲート]ビューでの検索 244

[レガシー イベント]ビューでの検索 244
URL統合を使用したクエリの表示と変更 245
サービスIDが分かる場合 245
ホストとポート番号がわかる場合 245
例 246
追加の注意事項 246
イベントビューから将来のアラートを作成する 247
イベントビューからレポートを生成する 249
レポートの作成 251
レポートのスケジュール設定 254
チャートを作成する 259
調査ビューからイベント ウィジェットを作成する 262
イベントの再構築と分析 269
[イベント]ビューでのイベント詳細の調査 272
各イベント タイプのイベントの詳細 272
テキストの再構築 273
パケットの再構築 277
ファイルの再構築 278
ホスト情報 279
メールの再構築 282
ウェブ再構築 283
イベントビューでイベントを分析する 285
結果のロードとソートの方法 285
イベント リストを絞り込むためのアクション 286
イベントを分析するためのアクション 286
イベントの分析タイプの選択 287
リクエストとレスポンスの表示を調整する 287
イベントの関連メタデータを表示する 287
イベント ヘッダーを表示または非表示にする 292
[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 292
[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 293
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 294
[テキスト]タブで検索パターンを作成する 297
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 300
ツリー形式のJSON文字列の [テキスト]タブでの表示 301
[ペイロードのみ]オプションの [パケット]タブでの使用 302
[パケット]タブでのバイトのハイライト表示 303
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 304
ファイルのVirusTotalルックアップの開始 305
[レガシー イベント]ビューでのイベントの再構築 307

イベントIDを使用したイベントの再構築 308
[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 308
セッションを左右/上下に並べて表示 310
表示するイベント情報の選択 310
イベントの再構築のタイプの選択 310
メールの添付ファイルの表示またはダウンロード 311
イベントをPCAPファイルとしてエクスポート 311
再構築されたイベントからのファイルの抽出 312
結果の追加のコンテキストを検索 313
[コンテキスト ルックアップ]パネルを開く 314
ホワイト リストへのエンティティの追加 317
リストの作成([イベント]ビュー) 318
Archerへの移行([イベント]ビュー) 319
[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 320
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) 321
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) 322
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) 322
メタ キーのルックアップの起動 323
[ナビゲート]ビューでのEndpoint Thick Clientルックアップの起動 323
イベントでのメタ値のルックアップの実行 325
イベント再構築ビューでのMITRE ATT&CK©ルックアップ 327
[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 329
[ナビゲート]ビューからのMalware Analysisスキャンの起動 331
[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 333
ネットワーク セッションの分割 333
セッション サイズと時間の分割 334
トランザクション処理の分割 334
セッション フラグメントの強調表示 335
関連ネットワーク セッション 336
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 337
イベント リストでの関係の表示と非表示 338
[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 339
メタデータを座標表示チャートに追加する 341
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 341
座標表示で使用できるRSAメタ グループ 341
座標表示チャートの表示 342
座標表示チャートで使用するメタ キーの選択 343
座標表示チャートの最適化 348
使用例 350
大量データセットのチャートの例 351

ドリルダウン ポイントのInformerでのビジュアル表示 353
結果のダウンロードと処理 354
[イベント]ビューでのデータのダウンロード 355
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 355
テキスト再構築でのログのダウンロード 360
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 362
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 364
メール再構築からの添付ファイルのダウンロード 366
[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 368
[レガシー イベント]ビューでのイベントのエクスポート 370
[イベント]ビューでのインシデントへのイベントの追加 371
[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 374
NetWitness Investigateのトラブルシューティング 376
[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 376
[イベント]ビューの問題 377
イベント レポートの問題を調査する 381
調査の参考情報 384
[イベントをインシデントに追加]ダイアログ 386
ワークフロー 386
実行したいことは何ですか？ 386
関連トピック 387
簡単な説明 388
[リストへの追加/削除]ダイアログ 391
ワークフロー 391
実行したいことは何ですか？ 392
関連トピック 393
[イベント]ビューの簡単な説明 393
[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 396
[列グループ]ダイアログ 398
関連トピック 399
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 399
簡単な説明 - [列グループの管理]ダイアログ 401
[コンテキスト ルックアップ]パネル 403
ワークフロー 403
実行したいことは何ですか？ 404
関連トピック 405
([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 405
インシデント 406
アラート 406

リスト 407
[イベント]ビューの簡単な説明 407
[リスト]タブ 409
[Archer]タブ 410
[Active Directory]タブ 412
[アラート]タブ 413
[インシデント]タブ 415
[ファイル レピュテーション]タブ 416
[TI]タブ 417
[REST API]タブ 418
[インシデントの作成]ダイアログ 420
ワークフロー 420
実行したいことは何ですか？ 420
関連トピック 421
簡単な説明 421
[イベント]ビュー 425
ワークフロー 425
実行したいことは何ですか？ 425
関連トピック 426
簡単な説明 427
[イベント メタ]パネル 430
クエリ コンソール 431
クエリーの例 432
現在のクエリー 432
最近のクエリー 433
タイムライン 433
[メタ設定]パネル 434
[イベント]ビュー - [メール]タブ 436
ワークフロー 436
関連トピック 436
簡単な説明 436
[イベント]ビュー - [ファイル]タブ 438
ワークフロー 438
実行したいことは何ですか？ 438
関連トピック 439
簡単な説明 439
[イベント]ビュー - [ホスト]タブ 441
ワークフロー 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
[イベント]ビュー - [パケット]タブ 444
ワークフロー 444
実行したいことは何ですか？ 444
関連トピック 445
簡単な説明 445
[イベント]ビュー - [テキスト]タブ 448
ワークフロー 448
実行したいことは何ですか？ 448
関連トピック 449
簡単な説明 450
[調査]ダイアログ 451
ワークフロー 451
実行したいことは何ですか？ 451
関連トピック 452
簡単な説明 453
[調査]タブ - [ユーザー環境設定]パネル 455
関連トピック 455
簡単な説明 455
[調査]ビュー 459
[レガシー イベントの再構築]ビュー 460
実行したいことは何ですか？ 460
関連トピック 461
簡単な説明 461
[レガシー イベント]ビュー 464
実行したいことは何ですか？ 464
関連トピック 465
簡単な説明 465
詳細説明 468
[デフォルトのメタ キーの管理]ダイアログ 471
関連トピック 471
簡単な説明 471
[メタ グループ]ダイアログ 473
関連トピック 473
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 473
簡単な説明 - [メタ グループの管理]ダイアログ 476
[ナビゲート]ビュー 479
ワークフロー 479
実行したいことは何ですか？ 480

関連トピック 481
簡単な説明 481
ツールバー 481
一時停止/再ロード ボタンと階層リンク 485
(オプション) デバッグ情報 486
時間バナー 486
ビジュアル画像 486
タイムライン チャート 486
座標表示チャート 488
値パネル 490
[値]パネルのロード動作 491
反復的結果 492
部分的結果 492
デバッグ情報 492
ロード完了 493
[クエリ]ダイアログ 494
実行したいことは何ですか? 494
関連トピック 495
簡単な説明 495
[シンプル]ビュー 496
[詳細]ビュー 496
[最近実行したクエリ]ビュー 497
[保存済みクエリ]ダイアログ 499
関連トピック 499
簡単な説明 - [保存済みクエリ]メニュー、[保存済みクエリの作成]ダイアログ、[保存済みクエリの詳細]ダイアログ 500
簡単な説明 - [プロファイルの管理]ダイアログ 503
[スプリングボード パネルの作成]ダイアログ 506
実行したいことは何ですか? 506
関連トピック 506
簡単な説明 : [スプリングボード パネルの作成]ダイアログ 506
[将来のアラートを作成]ダイアログ 508
実行したいことは何ですか? 509
関連トピック 509
簡単な説明 - [将来のアラートを作成]ダイアログ 509
[イベント]ビューの [レポートのスケジュール設定]ダイアログ 510
実行したいことは何ですか? 510
関連トピック 511
簡単な説明 - [レポートのスケジュール設定]ダイアログ 511
[イベント]ビューの [チャートの作成]ダイアログ 514

実行したいことは何ですか？ 514
関連トピック 514
簡単な説明 - [イベント]ビューの [チャートの作成]ダイアログ 514
[タイムライン設定]パネル 517
実行したいことは何ですか？ 517
関連トピック 517
簡単な説明 - [タイムライン設定]パネル 517
[検索パターンの作成]ダイアログ 519
実行したいことは何ですか？ 519
関連トピック 519
簡単な説明 - [検索パターンの作成]ダイアログ 519
調査ビューの設定ダイアログ 521
関連トピック 521
簡単な説明 521
[ナビゲート]ビューの [設定]ダイアログ 521
[レガシー イベント]ビューの [設定]ダイアログ 523
[イベント]ビューの [環境設定]ダイアログ 525

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。

メタデータ、メタ キー、メタ値、メタ エンティティ

NetWitnessは、環境内のすべてのデータ通信を監査し、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 イベントの取得、解析、保存を行います。Decoderに構成されたルール、パーサ、フィードは、取得したログ、パケット、エンドポイント データをアナリストが調査できるよう、*メタデータ*を作成します。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.netwitness.com/t5/netwitness-platform-unified-data/tkb-p/netwitness-udmを参照) 。

*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

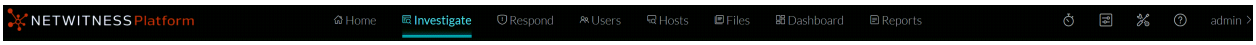
調査のトリガーの例をいくつか示します。

- 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、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。

この図はバージョン12.5のメニューを示しており、NetWitnessではデフォルトのランディング ページとして [ホーム] タブが追加されています。



注：
- 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。

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、Respondビュー、またはSpringboardから始めることができます。これらのビューでは、クリック可能なインシデントとアラートが、さまざまなビューの詳細情報と分析にリンクされます。

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	[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。イベント ビューのフィルター イベント パネルでこの機能が提供されるため、メタ値を詳細に調べ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。 (「結果セットの絞り込み」、「イベントの再構築と分析」、および「結果のダウンロードと処理」を参照してください。)

開始場所	調査の焦点
[レガシー イベント]ビュー	レガシー イベントは **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。 (「結果セットの絞り込み」、「イベントの再構築と分析」、および「結果のダウンロードと処理」を参照してください。)
[ホスト]ビュー	NetWitness Endpointエージェントが実行されているホストが表示されます。ホストごとに、プロセス、ドライバ、DLL、ファイル(実行可能ファイル)、サービス、異常、実行中のAutorun、ログイン ユーザに関連する情報が表示されます。(*NetWitness Endpointユーザー ガイド*を参照してください。)

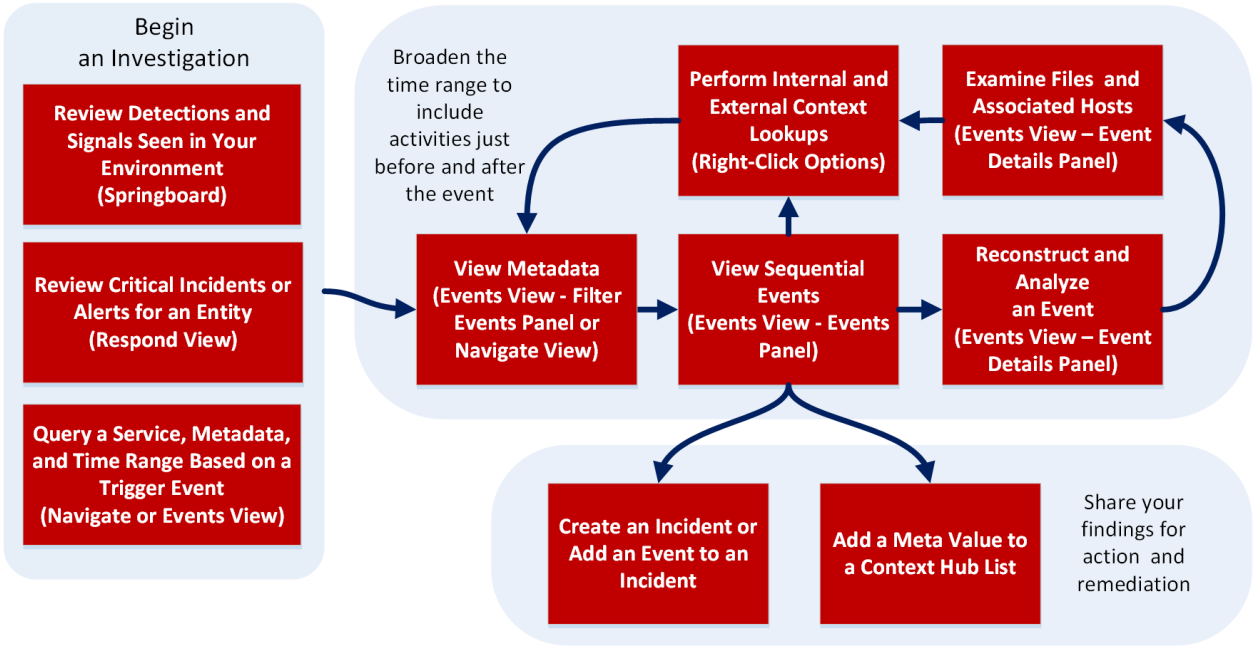
開始場所	調査の焦点
[ファイル]ビュー	導入環境内のPE、Macho、ELFなどのファイルが表示されます。ファイルごとに、ファイル名、レピュテーション ステータス、ファイルのステータス、リスク スコア、署名、チェックサムなどの詳細を表示できます。(『*NetWitness Endpointユーザ ガイド*』を参照。)

開始場所	調査の焦点
[マルウェア分析]ビュー	Malware Analysisアプライアンスを実行している場合は、ファイルをスキャンして、4種類の分析(ネットワーク、静的、コミュニティー、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。(*マルウェア分析ユーザー ガイド*を参照してください。)

開始場所	調査の焦点
[ユーザ]ビュー	[ユーザ]ビューでは、NetWitness UEBAを使用して、エンタープライズ全体で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)。

メタデータ、クエリ、時間に焦点を当てた調査

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



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

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。

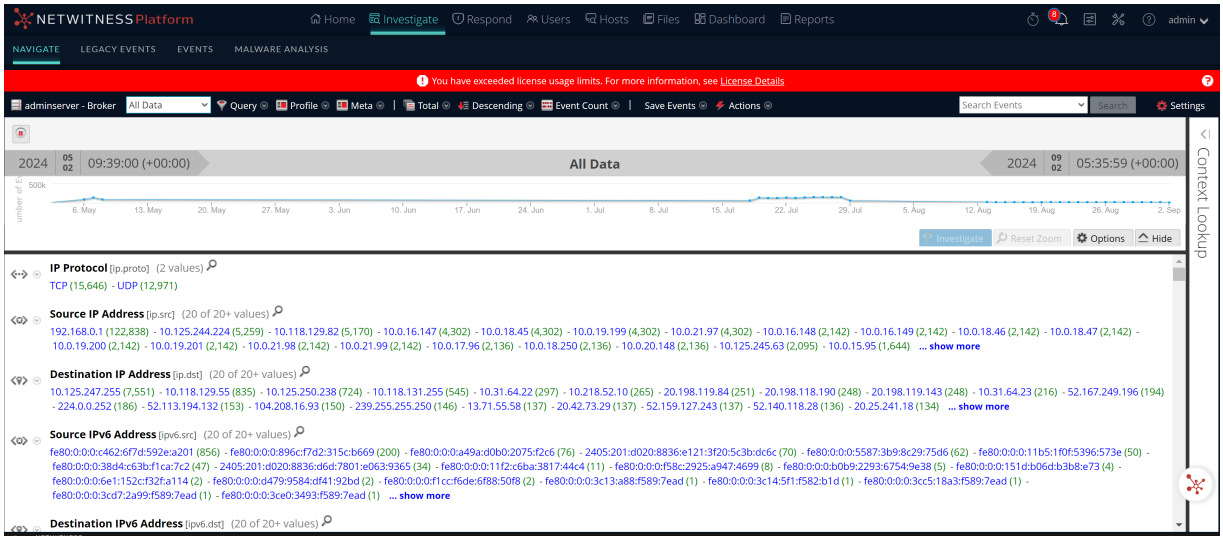
ナビゲートビュー

注：デフォルトでは、イベント ビューのイベント メタ パネルがこの機能を提供するため、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の内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、［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、エンドポイント、ログ イベン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 メタ］パネルでは、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 メタ パネルがブラウザーの全幅に拡張されている場合、イベント パネルにイベントをリストする前に、メタ値をドリルダウンして特定の情報を探すことができます (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します)。
  ［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

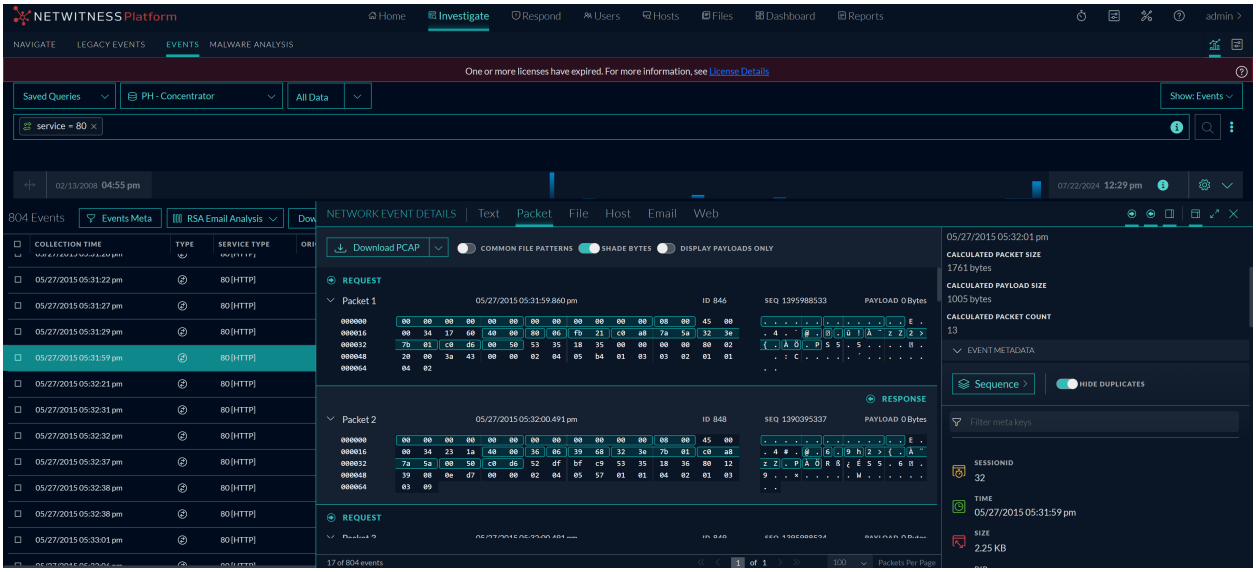
ソートされ、閾値よりも大きいことを示します。同様に、「**(~100000)**」は、結果がサイズに基づいてソートされ、閾値よりも大きいことを示します。

- [**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
- 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は、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。

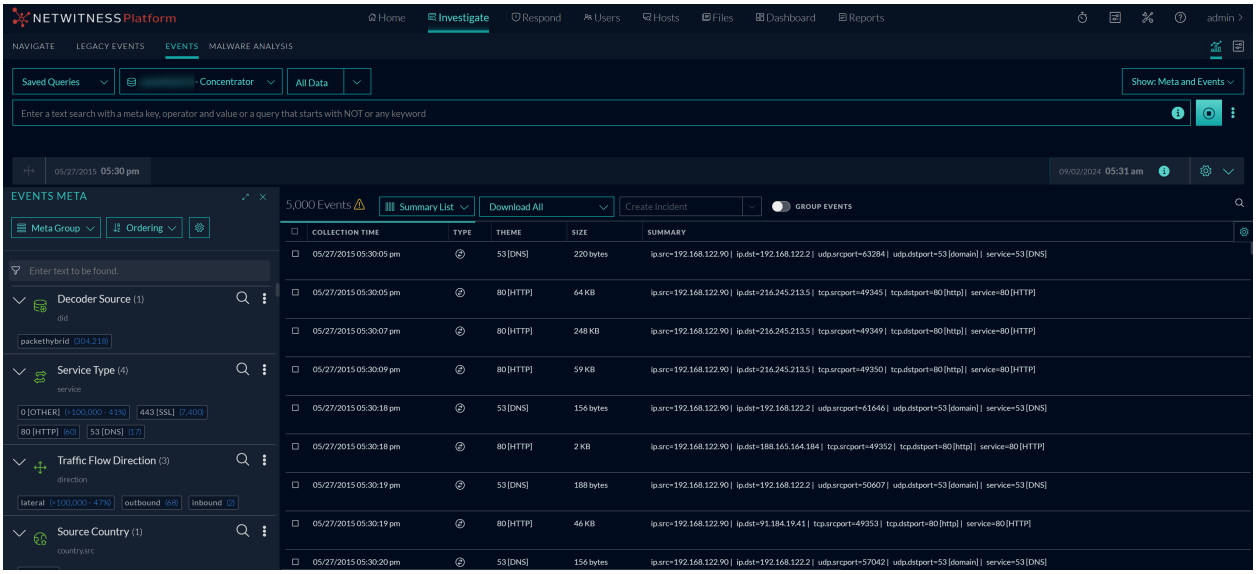
> **注**：拡張ネットワーク可視化を使用する場合は、Endpoint Log DecoderのデータをEndpoint Concentratorで集計するために使用するサービス ユーザー アカウントに、`decoder.manage`権限が割り当てられている必要があります。ロールと権限を割り当てる方法の詳細については、『NetWitness Platformホストおよびサービス スタート ガイド』の「サービスの[セキュリティ]ビュー - Aggregationロール」を参照してください。

- 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。
- 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」**または**「調査」**>**「レガシー イベント」**に移動し、 (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 メタ］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。

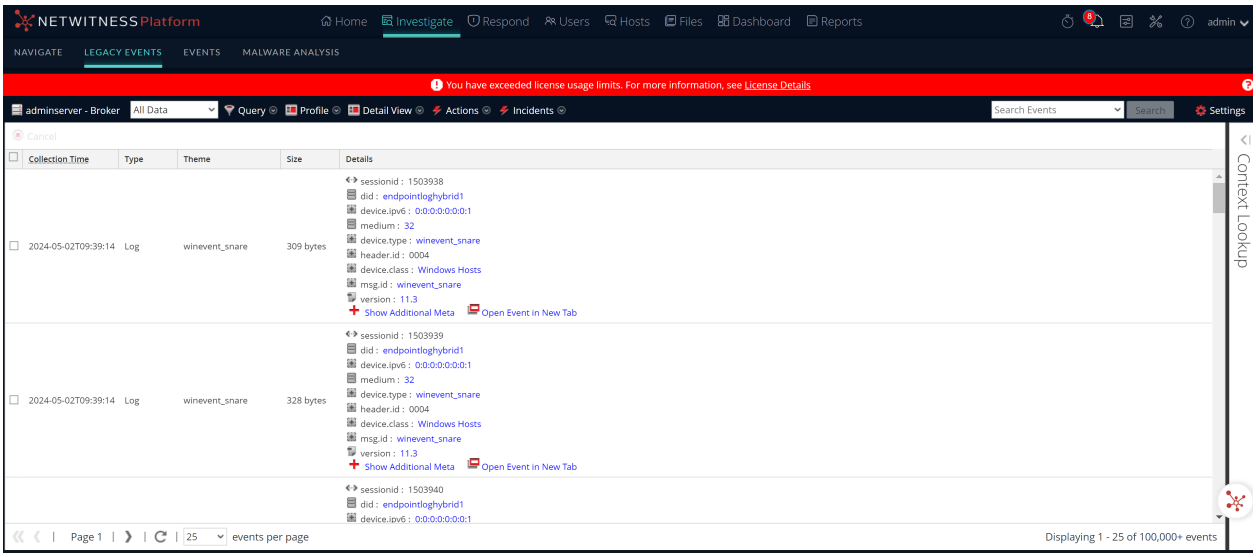


［レガシー イベント］ビュー

［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。バージョン12.5では、レガシー イベント ビューは不要になりました。*システム構成ガイド*の「調査設定の構成」で説明されているように、管理者が有効にしない限り、非表示になります。［レガシー イベント］ビューが有効になっている場合は、［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。



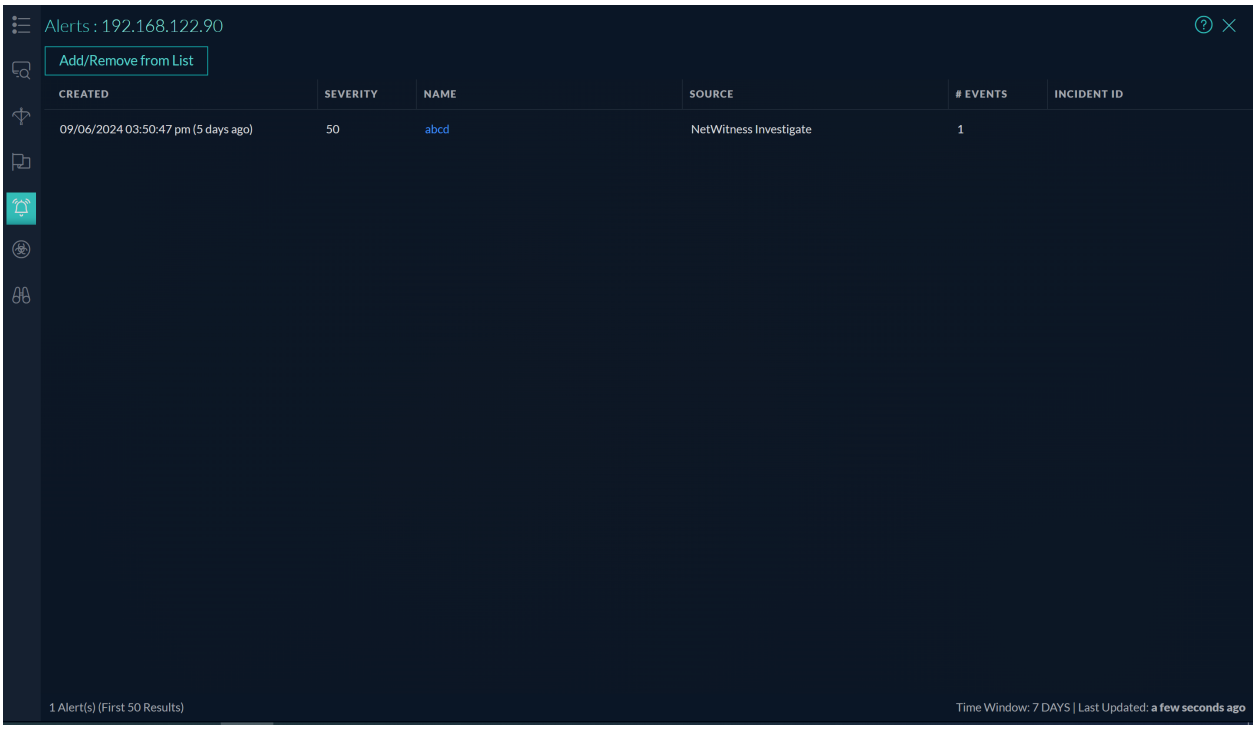
イベントのコンテキスト情報

［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。

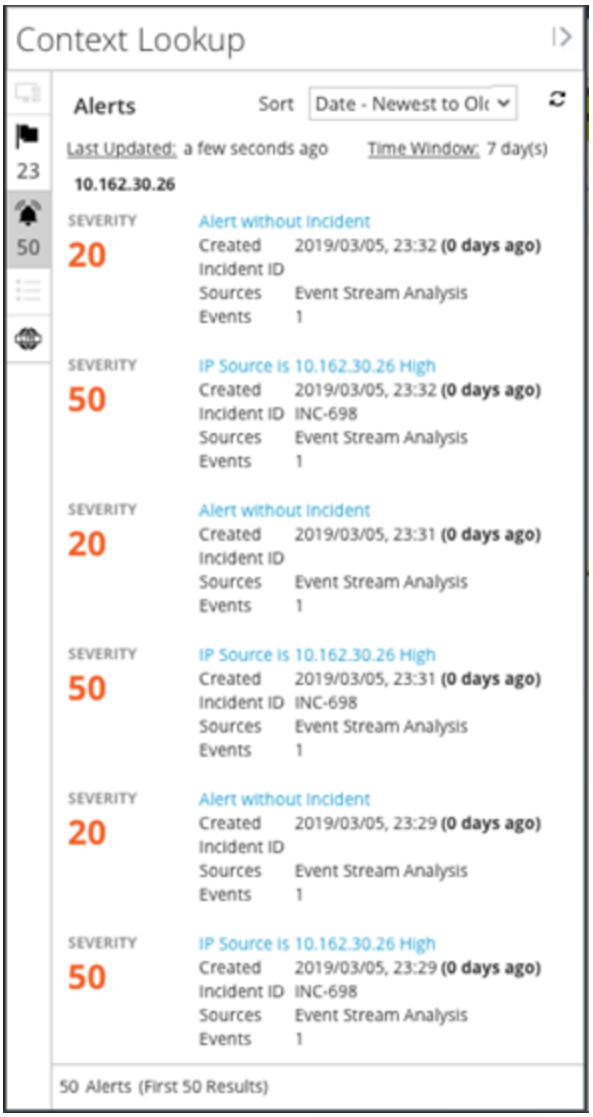
イベントの要素をインタラクティブに操作して、関連するインシデント、アラート、カスタム リスト、Archer資産、Active Directoryの詳細、NetWitness Endpoint IIOC、STIXデータ ソース(つまり、ファイル、TAXIIサーバ、RESTサーバ)などのより深い洞察を得ることができます(「結果の追加のコンテキストを検索」を参照)。

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。

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。

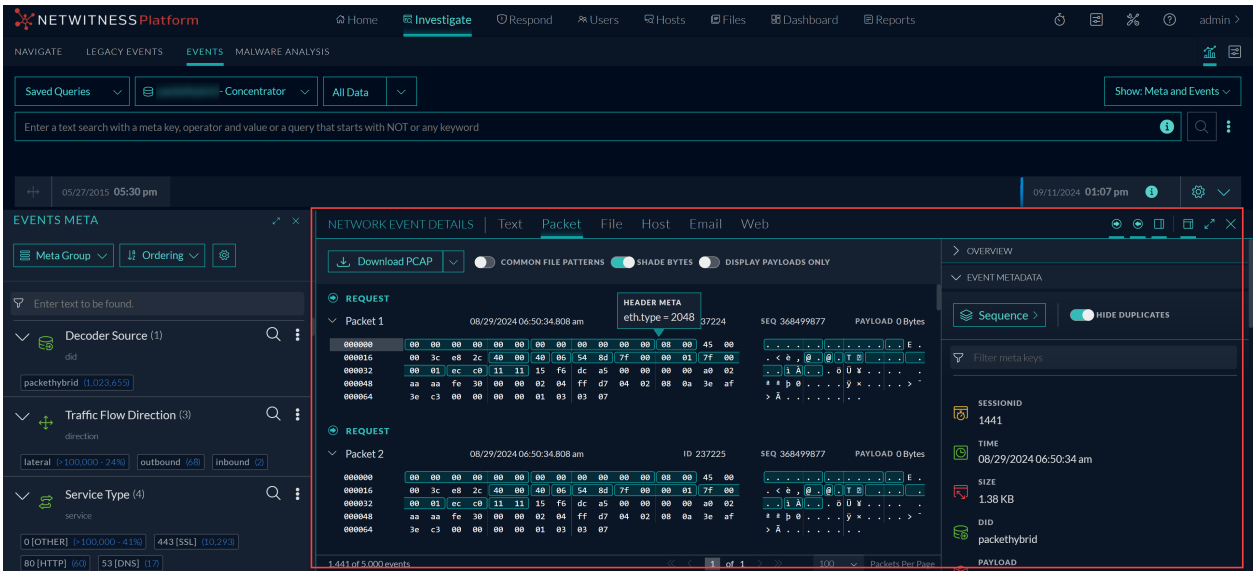


再構築とイベントの分析

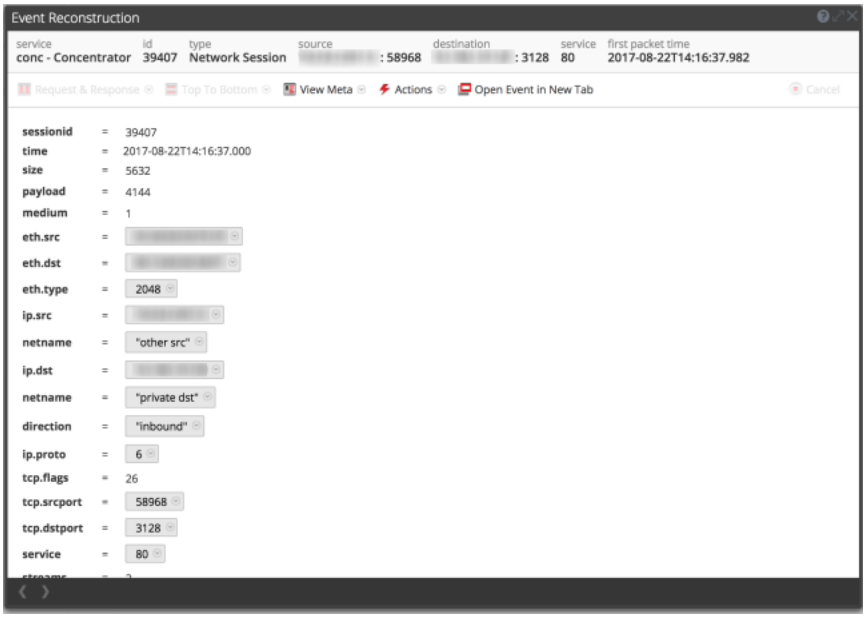
追加の調査に値するイベントを発見した場合は、そのイベントのコンテンツに最も適した形式で分析できます。分析の形式によっては、パケット、テキスト、メール、Webコンテンツなど、元の形式と同様の形式でイベントを安全に再構築します。イベントの表示中は、お使いのシステムやブラウザへの悪影響を制限するため、イベントに含まれる動的コードまたはアクティブ コードの使用は制限されます。キャッシュを使用して、以前に表示されたイベントを表示するときのパフォーマンスを向上させることができます。各アナリストには再構築データ用に個別のキャッシュがあり、自身のキャッシュにある再構築イベントにのみアクセスできます。

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

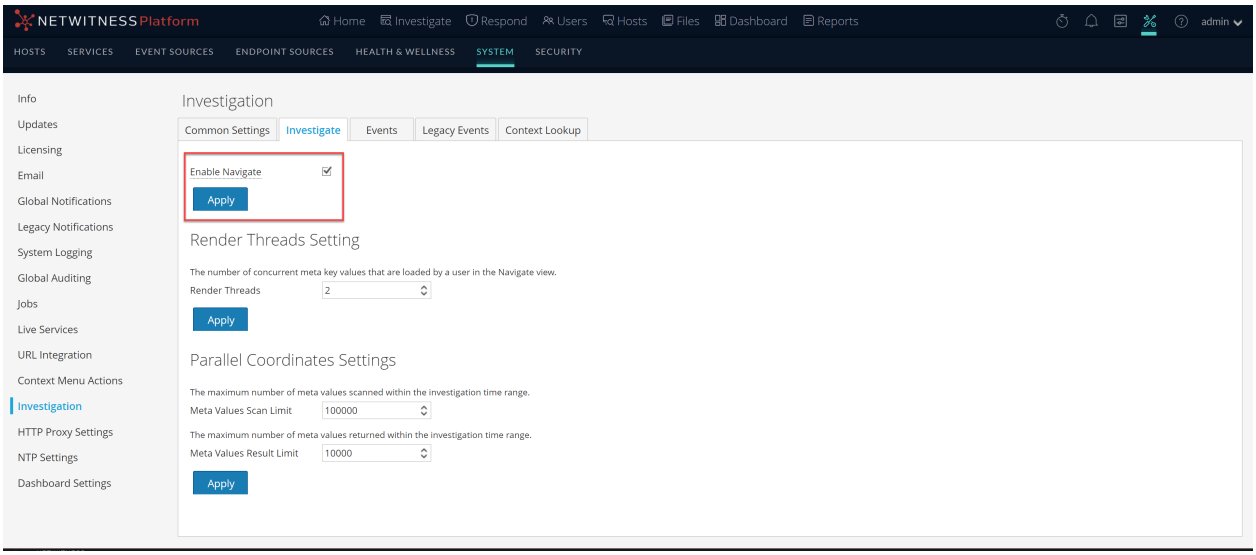
アナリストは、 [ナビゲート]ビューと [レガシー イベント]ビューを使用する際の、NetWitnessのパフォーマンスや動作に影響する環境設定を変更できます。これらの設定の一部はNetWitness内の次の2つの場所にあり、どちらの場所で変更を行っても、もう一方のビューに変更が適用されるようになっています。

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

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**]に移動します。
2. 左側のパネルで、 [**Investigation**]をクリックします。
3. [**Investigation**]ウィンドウで、 [**調査**]タブを選択します。
4. [**ナビゲートの有効化**]チェックボックスをオンにします。
5. [**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。



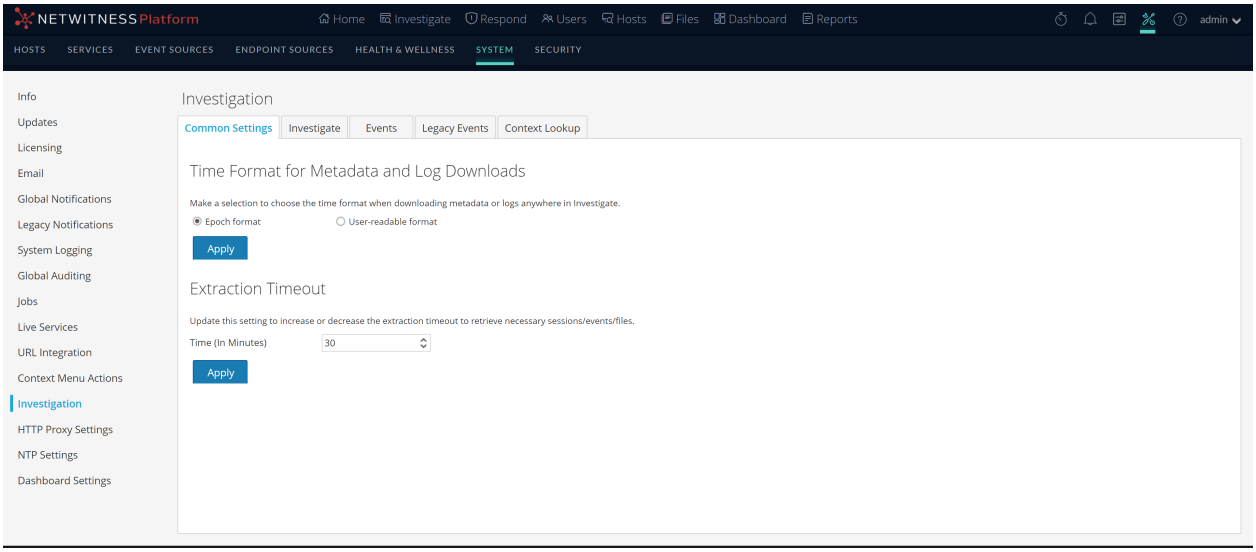
一般的な設定の構成

[**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て、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。

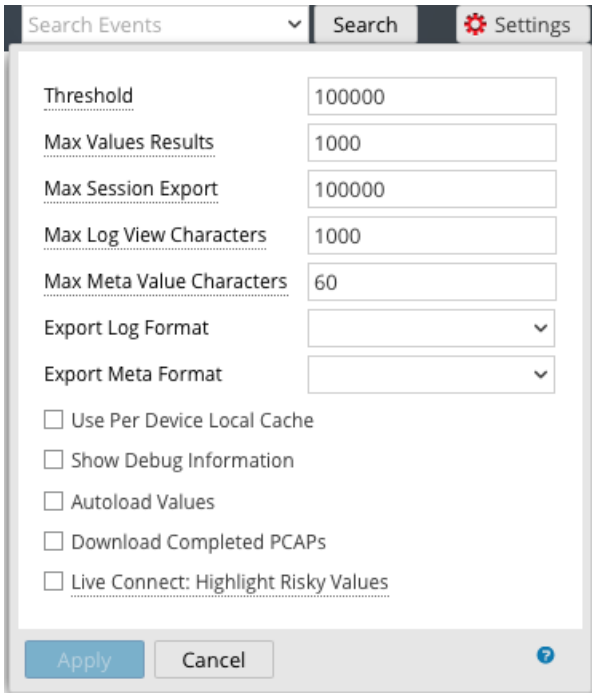
(**管理**)> [**システム**]に移動して、オプション パネルで [**調査**]を選択します。
[調査構成]パネルが表示されます。



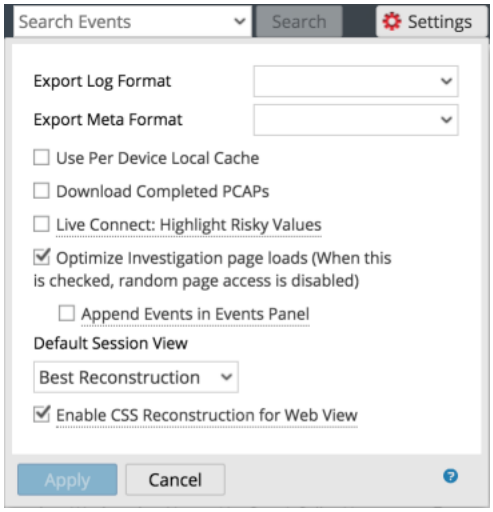
[ナビゲート]ビューと [レガシー イベント]ビューの [設定]へのアクセス

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。

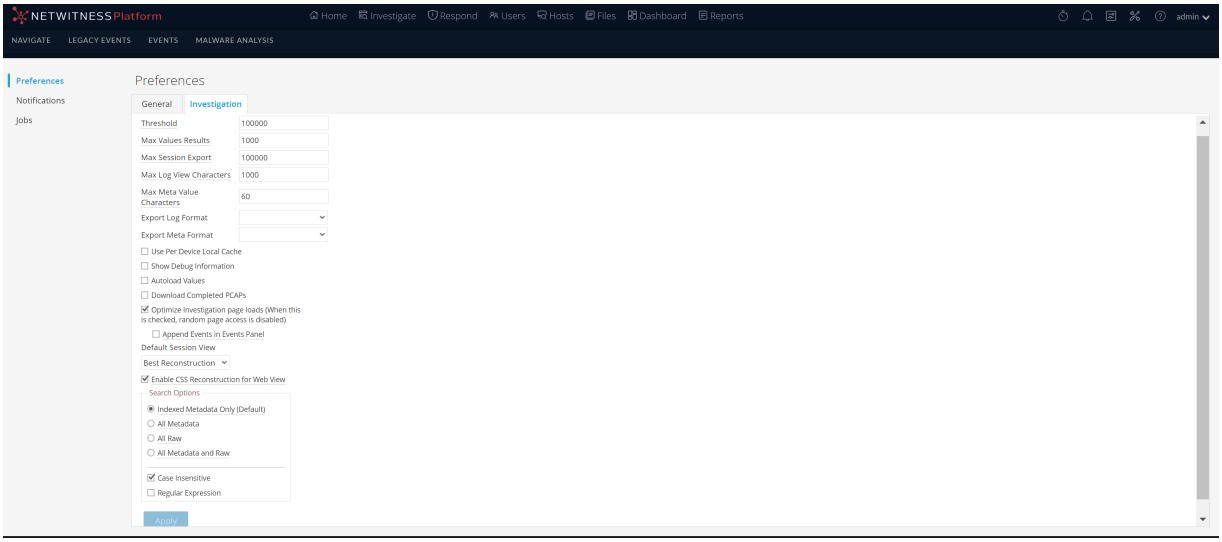


- **[レガシー イベント]**ビューのツールバーで、 **設定**]オプションを選択します。
  [レガシー イベント]ビューの 設定]ダイアログが表示されます。



- NetWitnessの右上で、 > [Profile]に移動し、 **環境設定**]パネルの **調査**]タブをクリックします。

[調査]パネルが表示されます。次の図は、[調査]パネルを示しています。



[ナビゲート]ビューでの値のロード パラメータの調整

いくつかの設定は、[値]パネルで値をロードする際のNetWitness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コミュニティによってリスクが高いと見なされるIPアドレスのみをNetWitnessでハイライトして表示する場合は、このオプションをオンにします。オンにしない場合は、すべてのIPアドレスがNetWitnessで表示されます。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がブラウザー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. **[メタ形式のエクスポート]**ドロップダウン メニューからいずれかのオプションを選択します。
3. [**適用**]をクリックします。
   設定がすぐに反映されます。

[レガシー イベント]ビューでの取得とデフォルトの再構築の調整

[レガシー イベント]ビューでの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す。

3. [環境設定]パネル > [調査]タブに移動するか、[ナビゲート]ビューまたは [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。

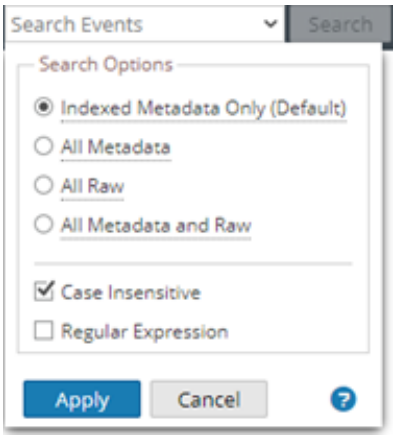
このオプションを有効または無効にするには

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、検索オプションのドロップダウン メニューを示しています。



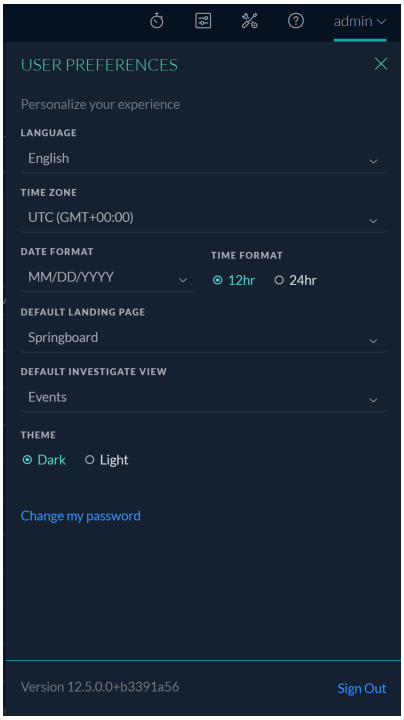
2. 検索に適用するオプションを選択します。各オプションの詳細については、「 [ナビゲート]ビューと [レガシー イベント]ビューでのテキスト パターンの検索」を参照してください。
3. 検索オプションの設定を保存するには、 **[適用]**をクリックします。
環境設定が保存され、ただちに有効になります。

[イベント]ビューの構成

アナリストは、 [調査] > [イベント]ビューを使用する際に、NetWitnessの動作に影響する環境設定を指定できます。 [イベント]ビューを開いている場合は、admin >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(admin >) 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、レガシー ビュー、またはマルウェア分析ビュー。デフォルトの [調査]ビューは、グローバルな [ユーザー環境設定]ダイアログ(NetWitnessブラウザー ウィンドウの右上にあるadmin >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。



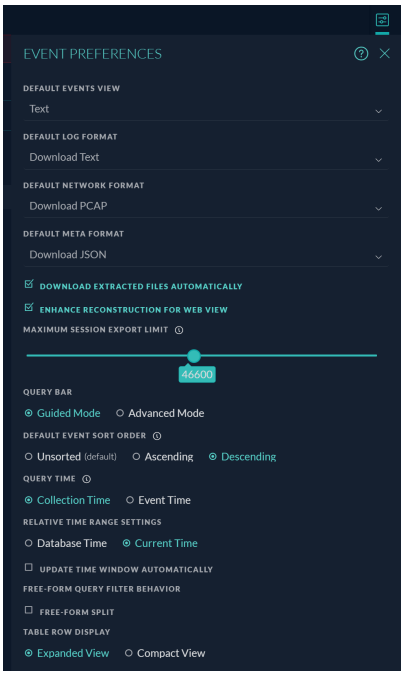
[イベント]ビューのユーザ環境設定の設定

[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、このダイアログに表示される

ラベルと使用可能なオプションはバージョンによって異なります。



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**、**ホスト**、**電子メール**、または**Web**。
デフォルトの分析タイプを選択していない場合、イベントを開いたときのデフォルトの再構築タイプはパケット分析です。ただし、ログ イベントとエンドポイント イベントの場合はテキスト分析が開きます。デフォルトの再構築タイプを選択した場合は、指定したタイプが、デフォルトの再構築タイプとして使用されます。どちらの場合も、デフォルトの再構築タイプは出発点であり、作業中にタイプを変更して、選択したタイプで再構築を表示することができます。

3. **[デフォルトのログ形式]**フィールドで、ログをエクスポートするときのダウンロード形式を選択します。**ログをダウンロード** または **テキストをダウンロード**、**XMLをダウンロード**、**CSVをダウンロード**、または**JSONをダウンロード**。ここで形式を選択しない場合、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**になります。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]**または **[デフォルトのネットワーク形式]**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をダウンロード** すると、イベント全体がパケット キャプチャ (*.pcap) ファイルとしてダウンロードされます。
   - **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**によって、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 ペイロードをダウンロード** すると、リクエスト ペイロードが *.payload1ファイルとしてダウンロードされます。

- **レスポンスペイロードをダウンロード** すると、レスポンスペイロードが *.payload2ファイルとしてダウンロードされます。

5. [**デフォルトのメタ形式**]フィールドで、メタデータをエクスポートするときのダウンロード形式を選択します。 [**テキストのダウンロード**]、 [**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い場合、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**になります。
6. 抽出され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、**[抽出されたファイルを自動的にダウンロードする]** チェックボックスをオンにします。抽出されたファイルを表示するには、ジョブ キューに移動できます。
7. (バージョン12.5以降) 新しい設定 [**Webビューの再構築の強化**]を有効にすると、CSS、画像、リンクでビューをフォーマットすることでイベントを再構築するWebサイトの再現が改善され、アナリストがイベントのコンテキストや詳細をより理解しやすくなります。ただし、これにより再構築の速度が遅くなる可能性があります。このオプションは、デフォルトで有効です。

  注：
  - 関連するイベントは、 [**システム**] > **調査**] > [**イベント**]タブにある [Webビュー再構築設定]で [**Webビューでサポート ファイルを有効化します(無効化すると、ユーザー設定より優先されます)**]が有効になっている場合にのみスキャンおよび再構築されます。
  - 関連画像やスタイル シートが見つからない場合や、Webブラウザーのキャッシュから読み込まれた場合は、再構築されたコンテンツの外観が元のWebページと完全に一致しないことがあります。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。

8. 新しい設定である **最大セッション エクスポート制限** を使用すると、アナリストはこの設定を更新して、**すべてダウンロード** メニュー オプションを使用してエクスポート可能なセッションの数を調整できます。デフォルトの制限は**10,000**に設定されています。ただし、アナリストは要件に基づいてこの制限を増減できます。許可される最小制限は**1,000**、最大制限は**100,000**です。この機能強化により、エクスポートされたセッションの数が、イベント テーブルに表示されるセッションの数に依存しなくなりました。
9. クエリを送信するときに一致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。

10. **「相対時間範囲設定」**で、**「データベース時間」**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。
    - **[現在の時間]**が選択されている場合、時間範囲はユーザー設定で設定されたタイムゾーンの現在時刻を基準とします。

注 :現在の時刻 は **相対時間範囲設定**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。

11. **「クエリの時刻形式」**で、**「データベース時刻」**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。

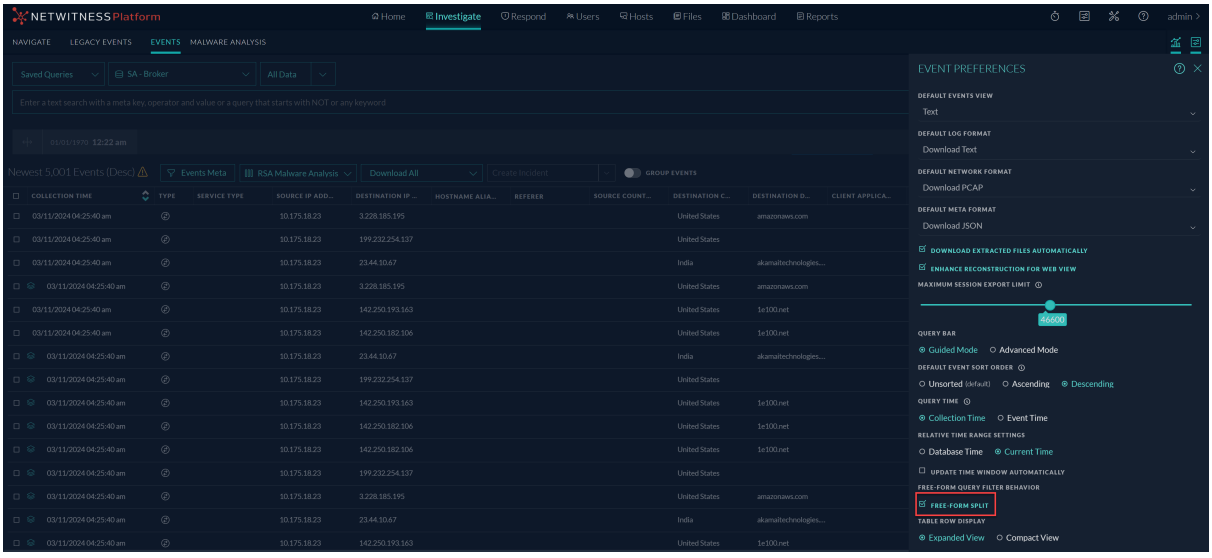
    - **[データベースの時間]**を選択した場合、クエリの終了時刻はイベントが保存された時刻が基準になります。
    - **[現在の時間]**を選択した場合は、ユーザー環境設定に設定されたタイムゾーンの現在の時刻に基づいてクエリが実行されます。

12. イベント パネルにリストされているイベントの収集時間による並べ替え順序を設定するには、**「デフォルトのイベント並べ替え順序」**の下でオプションを1つ選択します。設定を選択した後、テーブルの列ヘッダーを操作して、イベント リストでの列と列グループの使用」で説明されているように、結果を再度異なる順序で並べ替えるように要求することもできます。

    - **ソートしない** :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** :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。

13. 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。
14. 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。
15. 新しい環境設定でアナリストは、自由形式のクエリーを複数のガイド付きフィルターに分割するか、単一の自由形式クエリーを使用するかを選択できます。これらのモードは、 **［自由形式の分割**］チェックボックスを使用して切り替えることができます。

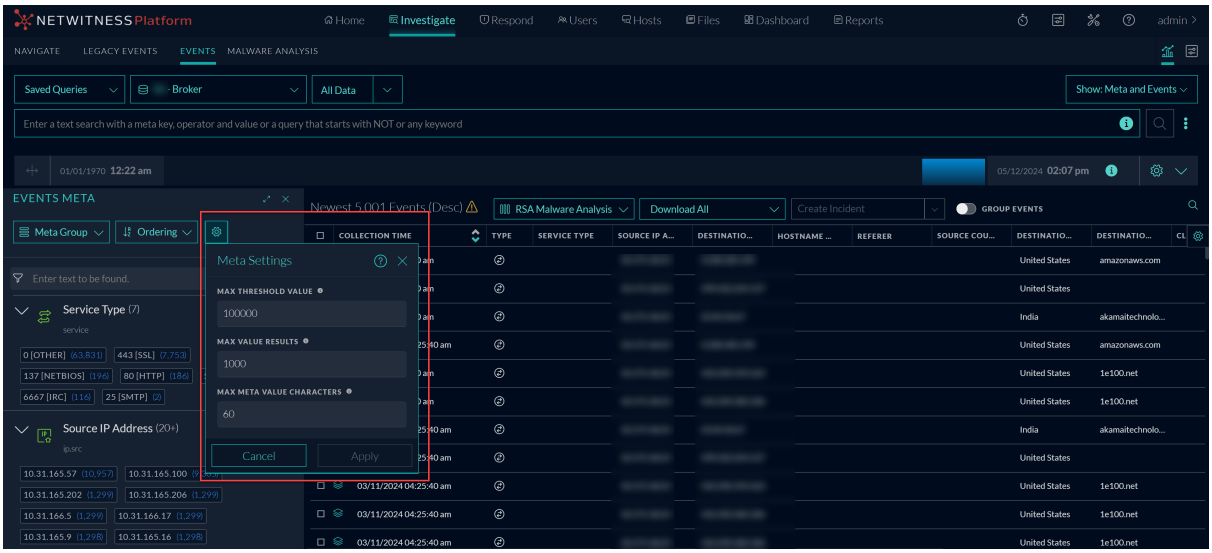


［イベント］ビューのメタ値ロード パラメーターの設定

NetWitnessでは、 **調査**］> ［**イベント**］ビューの下に、新しい ［**メタ設定**］パネルが導入されています。アナリストは、このパネルを使用して、 ［イベント］ビュー内で特定のメタ キー値に必要なセッション数を設定できます。ただし、いくつかの設定は、値が ［イベント］ビューにロードされるときに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。

[イベント メタ設定]パネルでの設定の調整

1. NetWitness Platformにログインします。
2. [イベント メタ] >  (**メタ設定**) をクリックします。
   [メタ設定]ダイアログが表示されます。



3. 次のパラメーターを変更します。
   - **最大閾値**：[イベント]パネルでメタ キー値にロードされ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、ロード時間が長くなります。最大閾値は、**1～2147483647**の範囲内である必要があります。デフォルト値は**100,000**です。
   - **結果の最大数**:開いているメタ キーの [メタ キー]メニューで [最大まで表示]オプションを選択したときに [イベント]ビューにロードする値の最大数を設定します。結果の最大数は、**100～100000**の範囲内である必要があります。デフォルト値は**1000**です。
   - **メタ値の最大文字数**：[イベント メタ]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。メタ値の最大文字数は、**60～512**の範囲内である必要があります。デフォルト値は**60**です。
4. [**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。

調査の開始

何を探しているかによって、NetWitness Investigateには、ナビゲート ビュー、イベント ビュー、レガシー イベント ビュー、ホスト ビュー、ファイル ビュー、ユーザー ビュー、マルウェア分析ビュー。

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

注：
- デフォルトでは、レガシー イベント ビューは無効になっていますが、*システム構成ガイド*に記載されているように、管理者が有効にすることができます。
- デフォルトでは、イベント ビューのイベント メタ パネルがこの機能を提供するため、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。ビューが表示されない場合は、管理者がユーザーに対して設定されている役割と権限を調整する必要がある可能性があります。
 - イベント ビューは、イベントを調査するためのデフォルトのビューです。イベントをインタラクティブに操作するアナリストのデフォルトのワークフローは、できるだけビューを切り替える必要がないよう最適化されています。以前は [イベント分析]ビューと [イベント]ビューという2つの異なるワークフローで提供していた機能を組み合わせることにより、アナリストは単一のワークフローでイベントを分析できるようになりました。 [イベント]ビューに追加された新機能により、 [レガシー イベント]ビューは不要になりました。デフォルトで、以前のワークフローは [調査]メニューに表示されなくなりましたが、管理者は『*システム構成ガイド*』の「調査の設定の構成」の説明に従って再度有効にすることができます。

メタデータ、RAWイベント、イベント分析にフォーカス

インシデント対応ワークフローを進めるために必要なイベントを追跡したり、別のツールがイベントを生成した後で戦略的な分析を行う場合は、 **[調査]** > **[ナビゲート]**、 **[調査]** > **[イベント]**、または **[調査]** > **[レガシー イベント]**に移動します。単一のBrokerまたはConcentratorのメタデータとRAWイベントを調査できます。これらのビューでは、クエリを実行し、時間範囲の絞り込みとメタデータのクエリによって、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
- [ナビゲート]ビューまたは [レガシー イベント]ビューでの調査の開始

ホストとファイルにフォーカス

エンドポイント エージェントが実行されているホストに関する情報を検索するには、**「ホスト」に移動します**。それぞれのホストについて、実行中のプロセス、ドライバ、DLL、ファイル(実行可能ファイル) 、サービス、Autorun、ログインしているユーザに関連する情報が表示されます。導入環境にあるファイルの調査を開始するには、 **[ファイル]**に移動します(詳細については、*NetWitness Endpointユーザー ガイド* を参照してください。)

高リスクのユーザおよびエンティティの振る舞いにフォーカス

ネットワーク環境のすべてのユーザ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**］またはNetWitness UEBA(User and Entity Behavior Analytics) に移動します。悪意のあるユーザや不正ユーザの検出、リスクの高い振る舞いの特定、攻撃の発見、新たなセキュリティ脅威の調査を行うことができます(詳細については、*NetWitness PlatformのUEBAユーザー ガイド* を参照してください。)

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

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

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

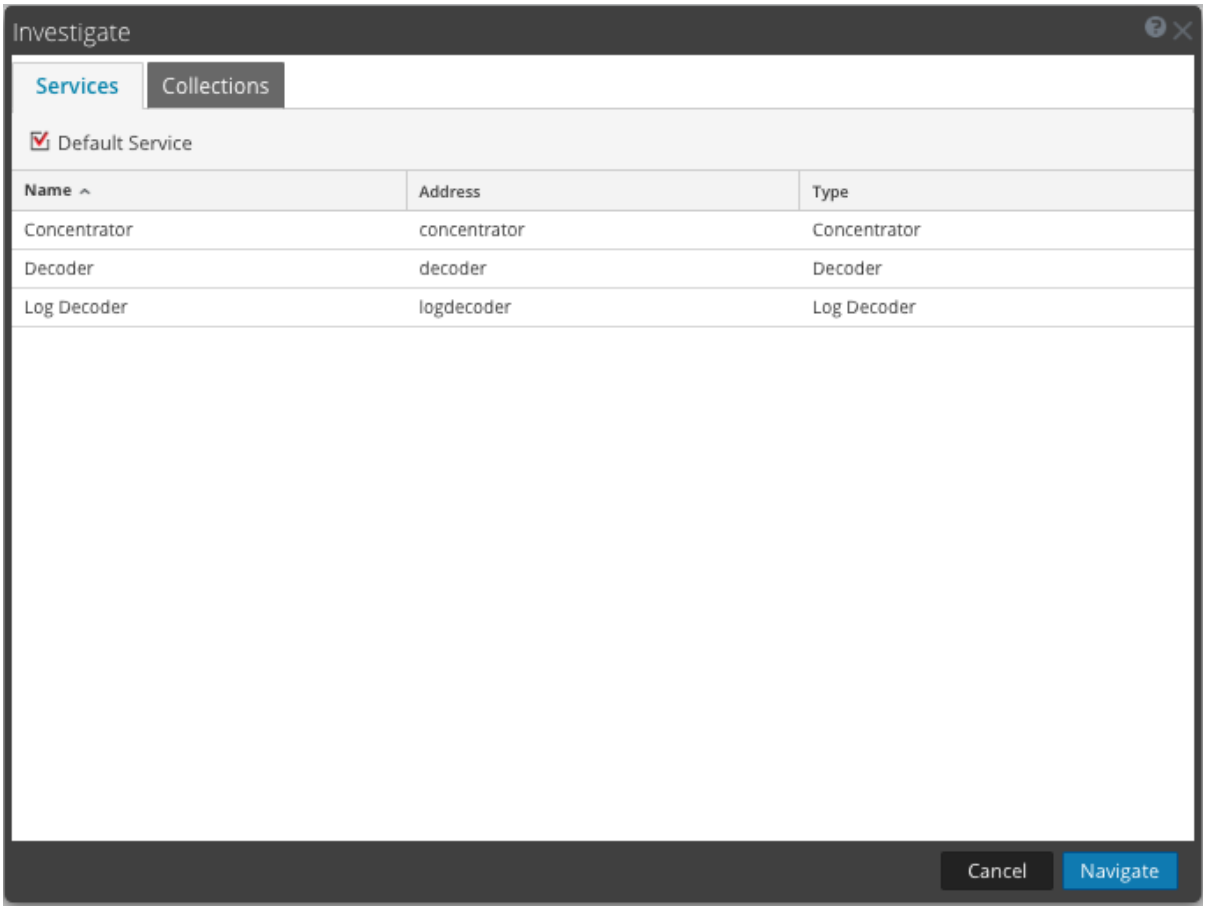
このトピックの後半では、サービスのデータの調査を開始するための手順について説明します。

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

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

調査の開始(デフォルトのサービスが指定されていない場合)

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



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

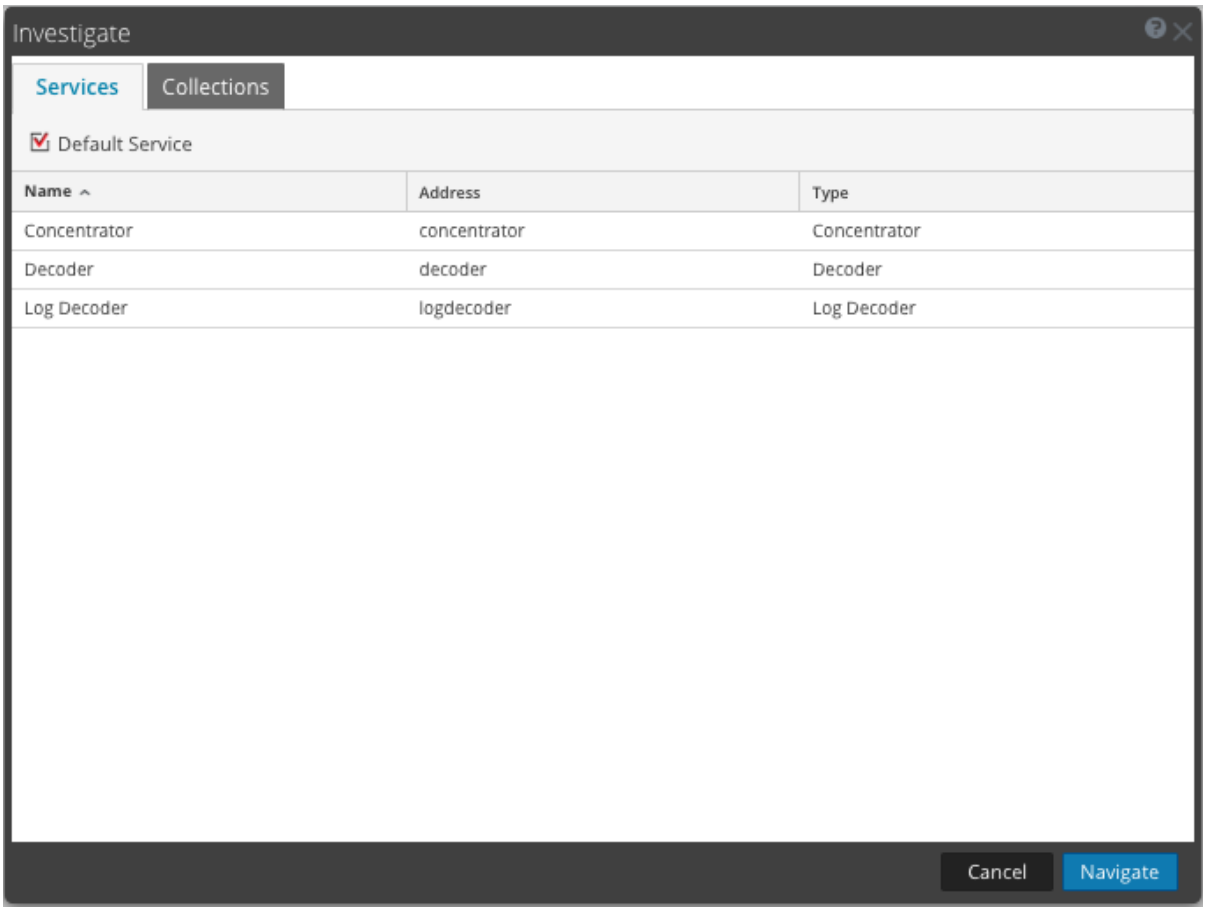


サービスが選択され、データがロードされて、データを解析する準備が整います。

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)

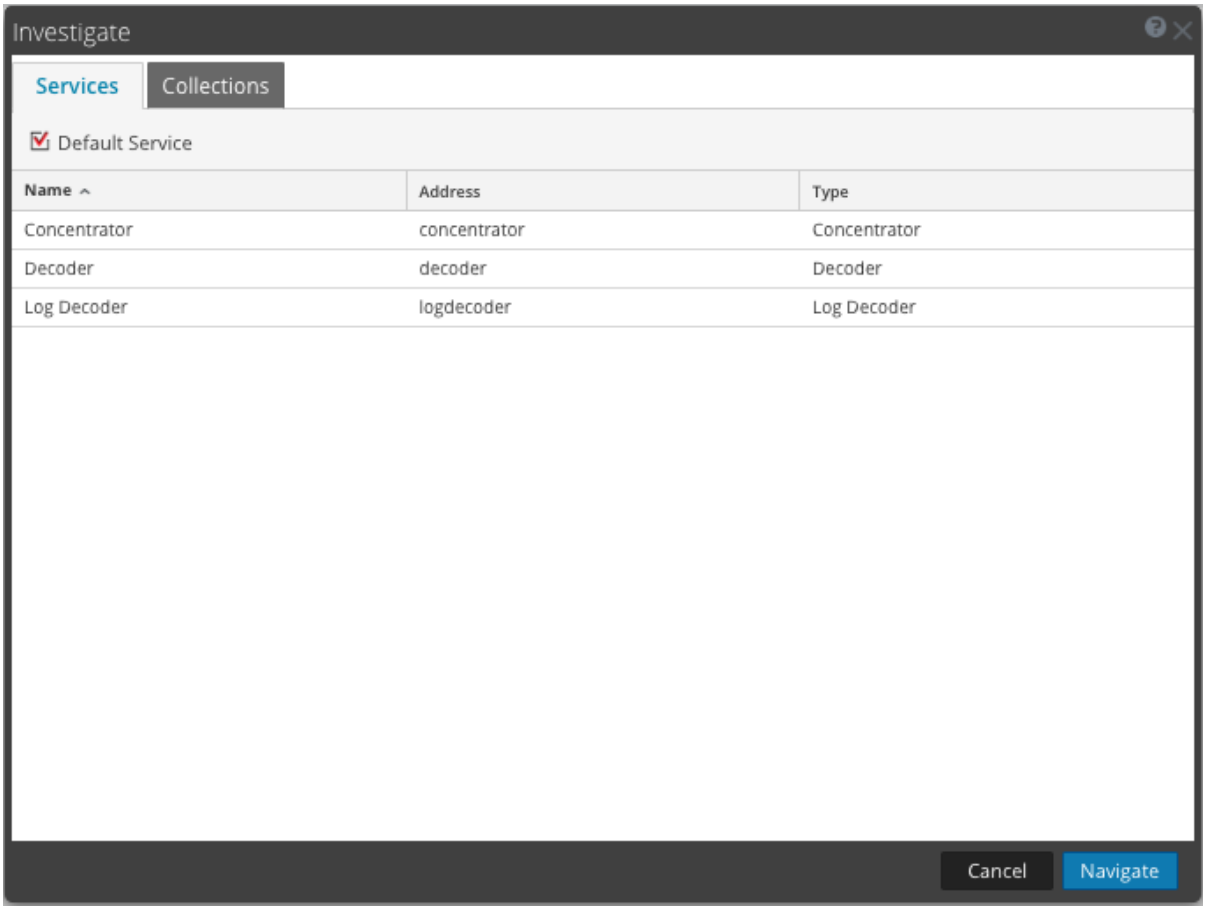
1. [**調査**]>[**ナビゲート**]または[**レガシー イベント**]に移動します。
[値の自動ロード]がオフの場合、[ナビゲート]ビューが表示され、デフォルトのサービスが選択された状態になり、データをロードする準備が整います。[値の自動ロード]がオンの場合は、ステップ3に示すように値がロードされます。[レガシー イベント]ビューでは、データが自動的にロードされます。

2. データをロードする前に、［ナビゲート］ビューの調査オプションを変更することができます。たとえば、カスタム プロファイルの作成または変更、別の時間範囲の適用、メタ グループの作成または適用、カスタム クエリの実行などです。

3. 準備が完了したら、Load Valuesをクリックします。
選択したオプションに従って、サービスからデータがロードされます。サービスを選択して、データがロードされたら、データを分析する準備が整います。

調査するサービスまたはコレクションの変更

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



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

3. 準備が完了したら、Load Valuesをクリックします。
選択したオプションに従って、サービス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。

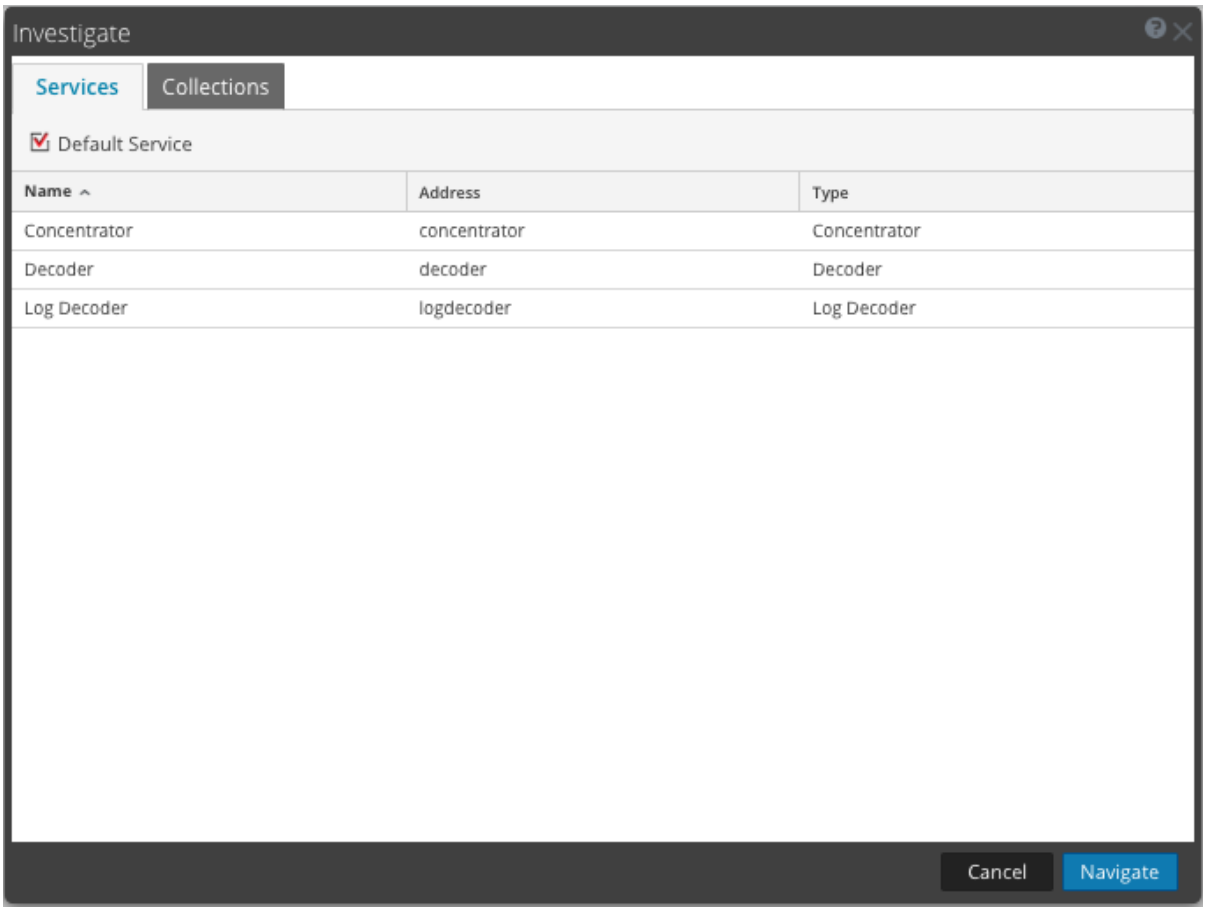
Workbenchのリストア コレクションの調査

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

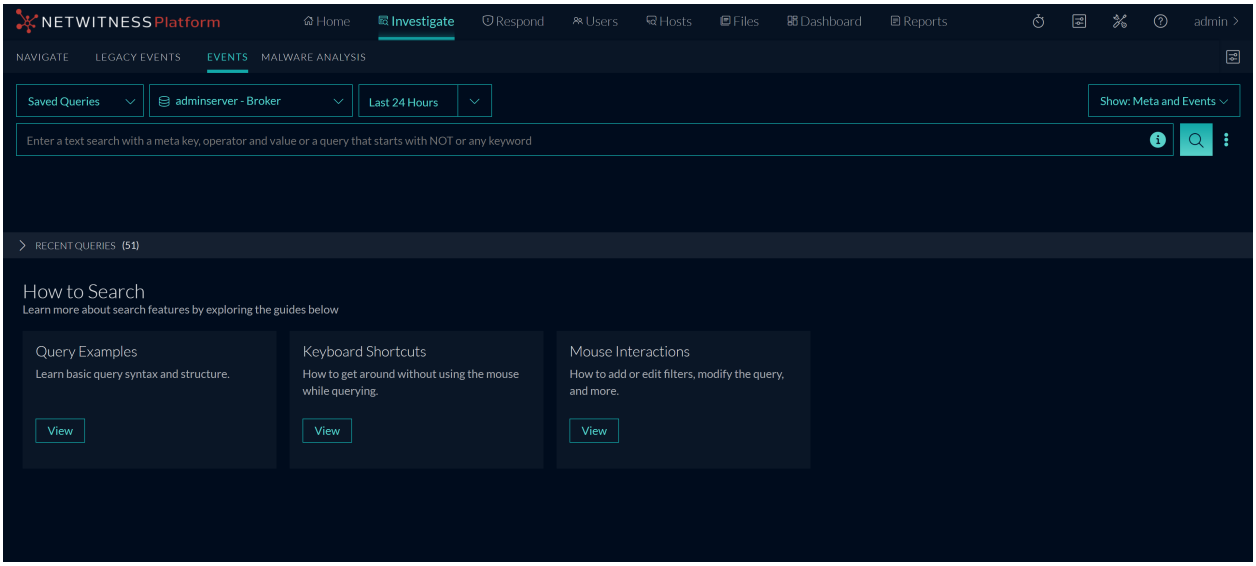


2. 調査するWorkbenchサービスとWorkbench名を選択します。
3. [**ナビゲート**]をクリックして、選択したWorkbenchサービスに対する調査を実行します。
   [**キャンセル**]をクリックして、調査する別のWorkbenchサービスを選択できます。
   [調査]ビューが表示されます。コレクションを選択して、データがロードされたら、データを分析する準備が整います。

[イベント]ビューでの調査の開始

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

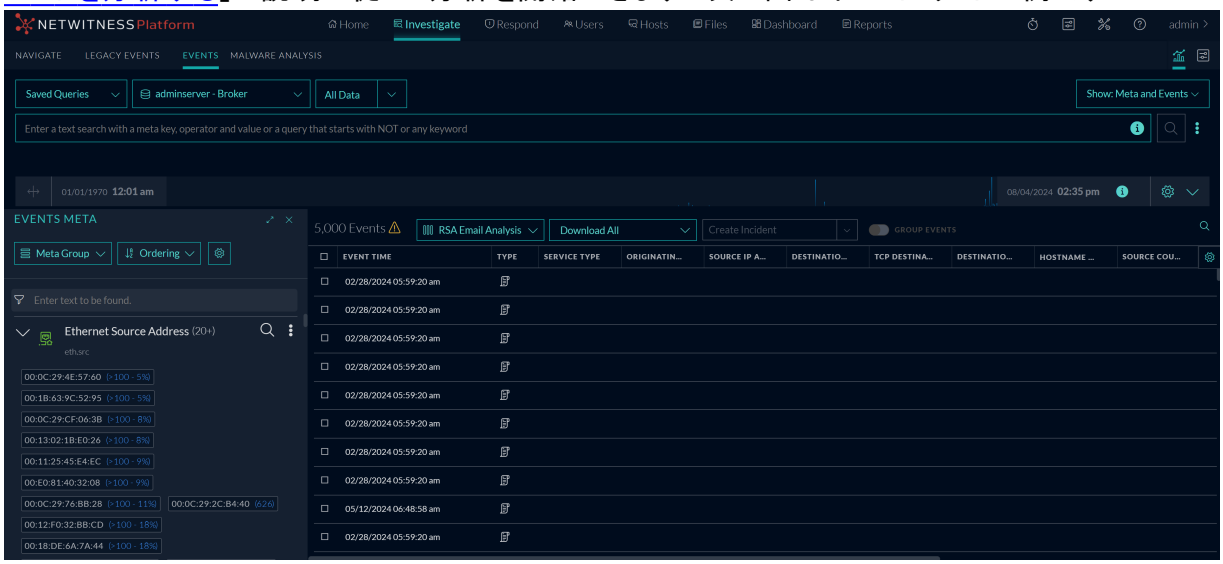


[イベント]ビューへのアクセス

イベント ビューにアクセスするにはいくつかの方法があります。

- **[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。
- イベント ビューで、カウント (メタ値の後の緑色の数字) にマウス カーソルを合わせてクリックします。 [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 ビューでイベントを分析する」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。「イベントビューでイ

ベントを分析する」の説明に従って分析を開始できます。次の図はイベント リストの例です。

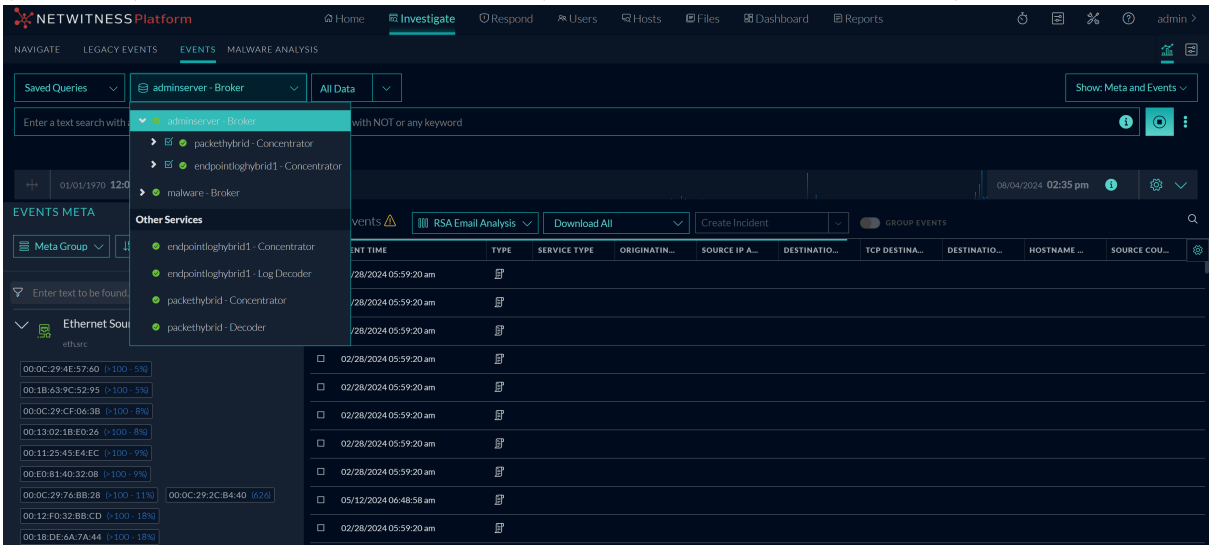


[イベント]ビューに直接アクセスして、調査を開始するには、次の手順を実行します。

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

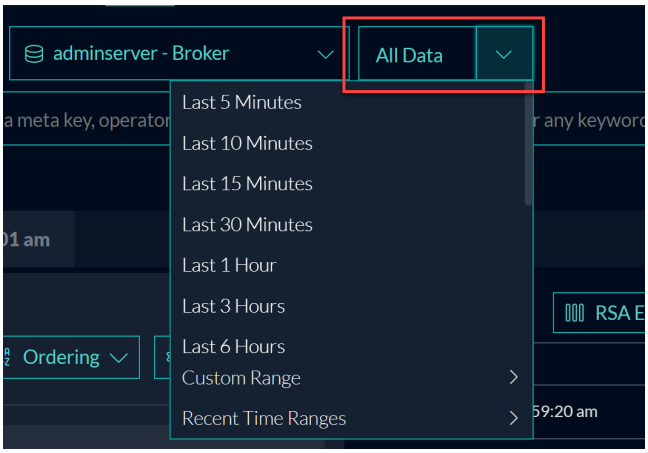
   -  と選択されたサービス名 = サービスが選択されています。
   -  = 選択されたサービスへの接続を試みています。
   -  = 選択したサービスへの接続中にエラーが発生したか選択したサービスにデータがありません。この状態では、サービス セレクタ コントロールも赤色に変わり、ツールチップに、接続の試行が失敗した理由と、別のサービスを選択するように勧めるメッセージが表示されます。

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



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

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

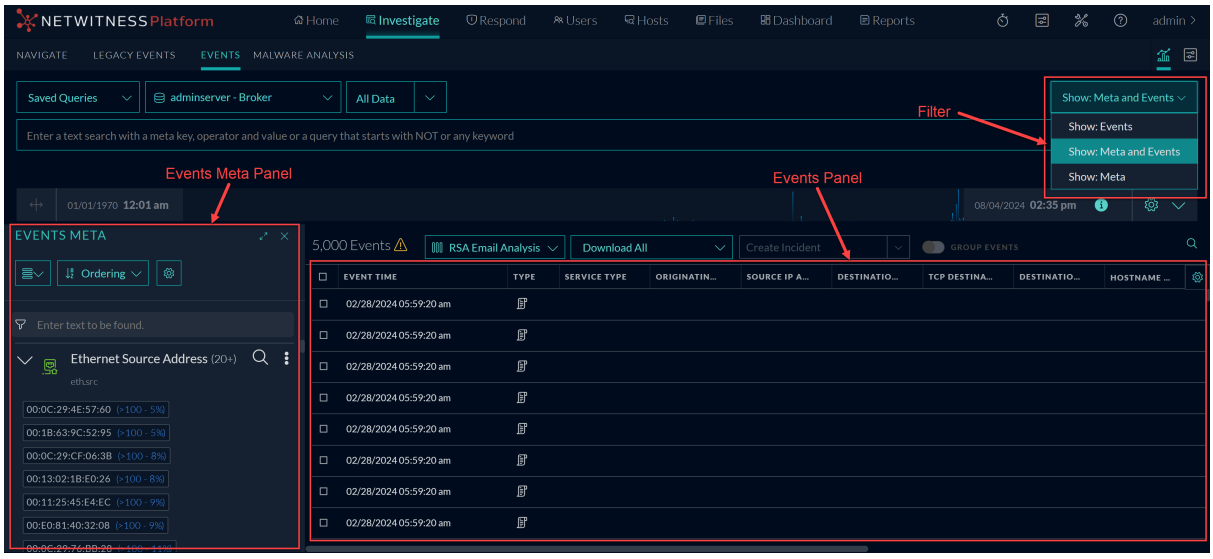


このサービスに選択した時間範囲はブラウザに保存されます。サービスごとに異なる時間範囲を設定できます。

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

5. ドロップダウン メニューから**クエリ結果パネル**のレイアウトを選択します。

たとえば、ドロップダウン メニューから **[表示 :メタとイベント]** オプションを選択すると、クエリ結果が2つの別々のパネル(**[メタ]** と **[イベント]**) に表示されます。



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

タイムラインでの調査

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。これにより、アナリストは異常を示している可能性のあるイベント数の急増を検出できます。視覚的表現を使用して、その特定の期間に発生したイベントをより詳細に調査することができます。

イベント ビューのタイムラインが改善され、ユーザがタイムラインを対話的に操作し、より豊富な洞察を獲得できるようになりました。強化されたタイムラインを使用すると、タイムラインの展開、タイムライン内の関心のあるゾーンのズームイン、軸設定の変更、要求された元のフォームへのクエリのリセットを行えるようになりました。

注 ミニ タイムラインはまだ対話型操作に対応していません。タイムラインを対話的に操作して特定のアクションを実行するには、タイムラインを展開する必要があります。



ユーザは展開されたタイムラインで次のアクションを実行できます。

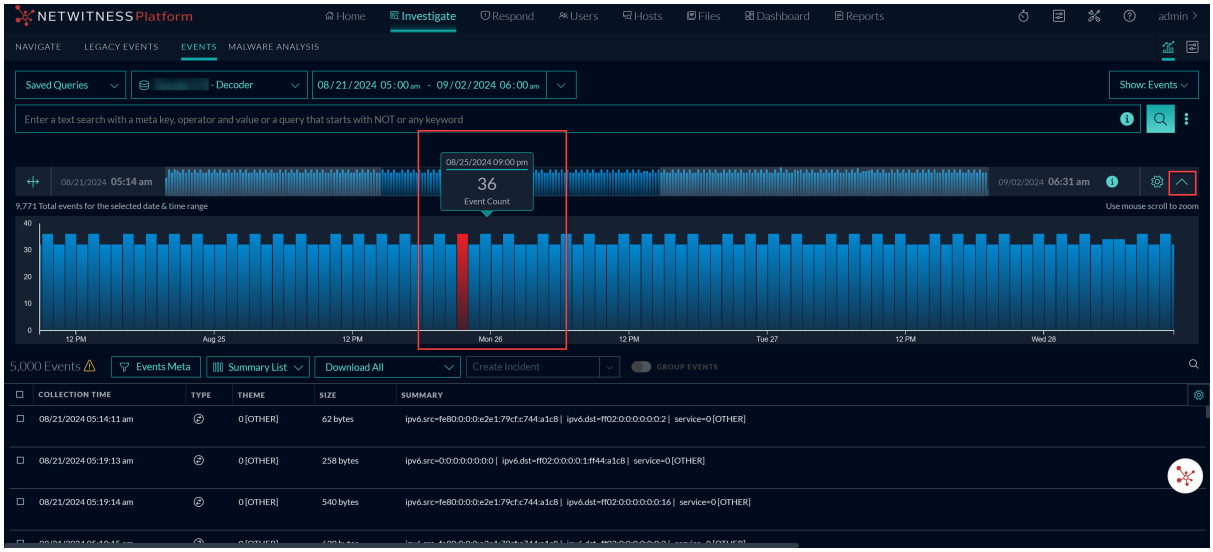
タイムラインを展開する

タイムラインの展開機能を使用すると、検索クエリに基づいてイベントの結果を対話的に操作できます。展開されたタイムライン ビューには、選択した日付と時刻範囲のイベントの合計数が表示されます。展開されたタイムラインでは、X軸は時間を示し、Y軸は、タイムライン上の特定の時間にサービスによって記録された、発生したイベントの総数またはファイル サイズを示します。

タイムラインを展開するには

1. NetWitness Platformにログインします。
2. ［**調査**］> ［**イベント**］に移動します。
3. (タイムラインの展開) をクリックしてタイムラインを展開し、タイムライン上の特定のゾーンまたは関心のあるゾーンを表示します。
4. 縦棒の上にマウスを置くと、イベント数とイベントが作成された時間が表示されます。

縦棒が赤で強調表示され、ツールチップ情報が関連付けられていることを示します。



タイムライン設定を使用する

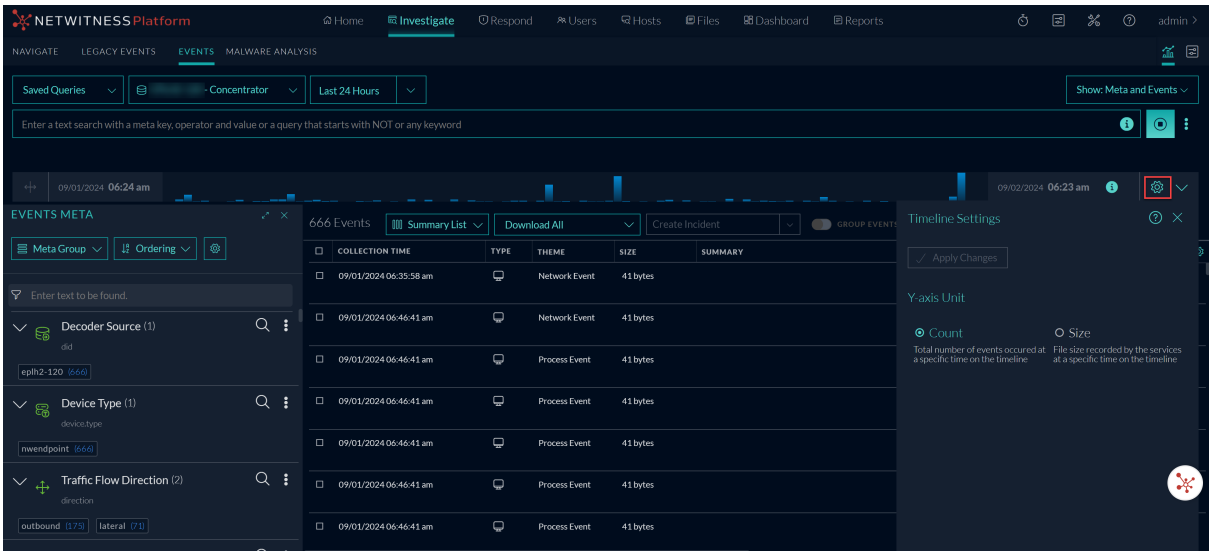
アナリストはタイムライン設定オプションを使用して、Y軸のデータ ディメンション(数またはサイズ) を変更し、タイムライン上に表示されるデータを確認できます。

ミニ タイムラインの右側にある(**情報**) ボタンをクリックすると、タイムラインのイベント データの表現(Y軸にどのような情報が表示されるかなど) を確認できます。

注 :X軸の設定を変更するには、［イベント環境設定］パネル内で設定されているクエリ時間オプションを変更する必要があります。クエリ時間の詳細については、「［イベント］ビューの構成」を参照してください。

タイムライン設定を変更するには、次の手順を実行します。

1. ［**タイムライン設定**］( ) をクリックします。
   ［タイムライン設定］ダイアログが表示されます。



2. 好みに基づいてY軸のデータ ディメンションを選択します。
   a. **数** :タイムライン上の特定の時間に発生したイベントの総数を表示します。
   b. **サイズ** :タイムライン上の特定の時間にサービスによって記録されたイベントの合計サイズを表示します。
3. [**変更の適用**]をクリックします。変更がタイムライン バーに反映されます。
4. [X]をクリックしてタイムライン設定を閉じます。

タイムラインをズームする

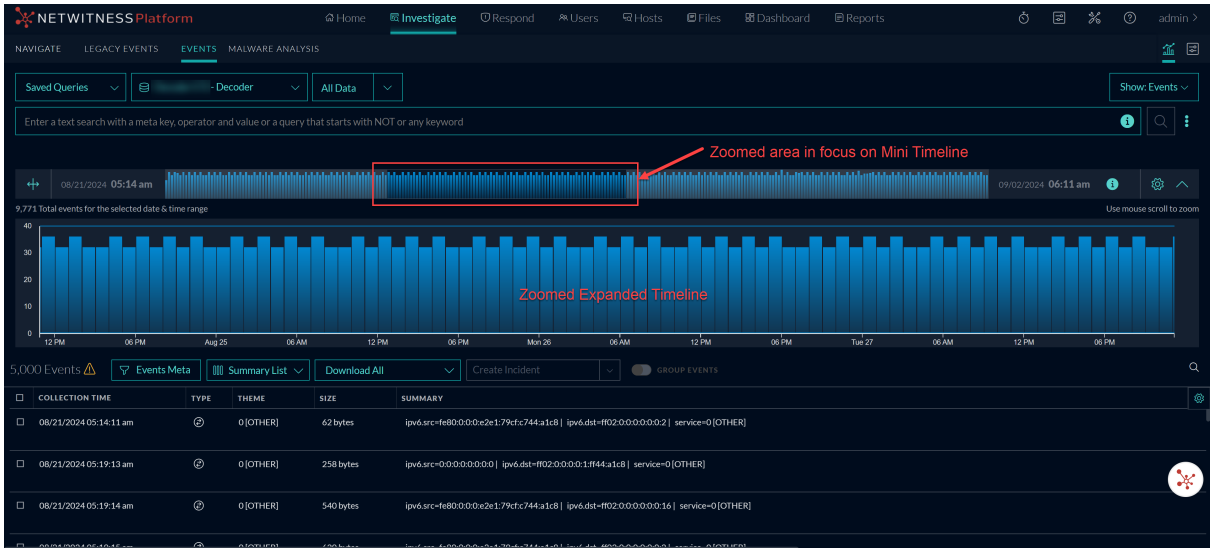
タイムライン内のズームインまたはズームアウト機能を使用すると、クエリ結果のうち特定の時間に発生したイベントに焦点を当てることができます。

タイムラインをズームインまたはズームアウトするには、次の手順を実行します。

1. 展開されたタイムライン上にカーソルを置き、マウスのスクロール ホイールを使用してタイムラインをズームインまたはズームアウトします。

   ズームイン領域の範囲がミニ タイムライン上でフォーカス モードになり、残りの領域は透明な白色

でマスクされます。



タイムラインをパンする

タイムライン内のパン機能を使用すると、ズーム モードのとき、または展開されたタイムライン上で特定の時間範囲選択モードのときに、タイムライン内を移動できます。

タイムラインをパンするには、次の手順を実行します。

1. ズームイン領域の縦棒の上にカーソルを置いて**右クリック**し、**右にドラッグ**または**左にドラッグ**してタイムライン内を移動します。

重要 :タイムラインをパンすると、ミニ タイムラインと拡張タイムラインでもフォーカス エリアが変化します。

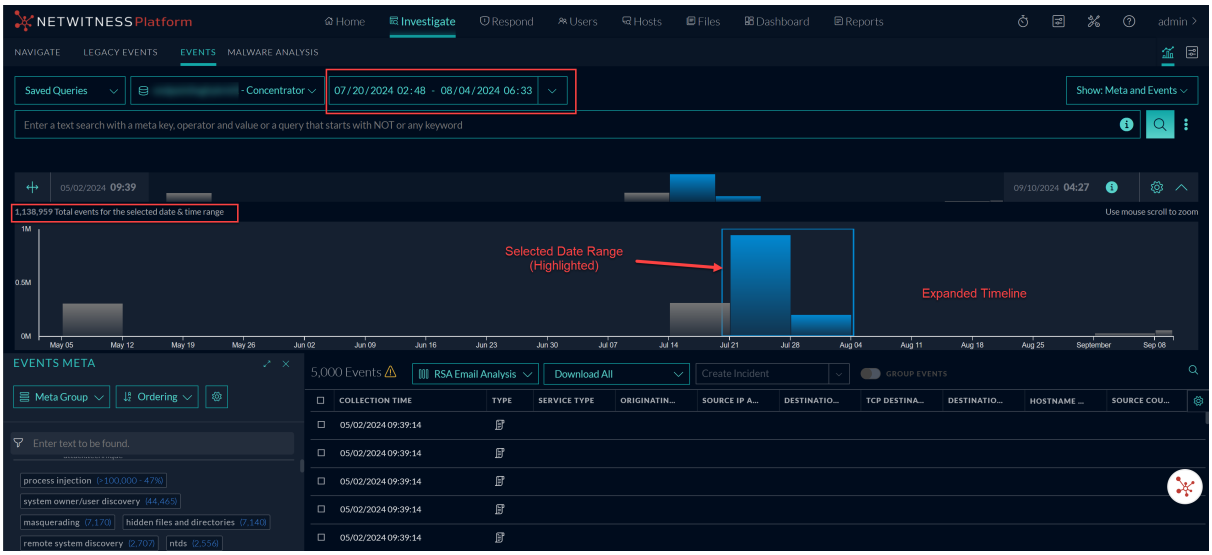
時間範囲の選択

時間範囲選択機能を使用すると、展開されたタイムライン上の関心のある領域またはフォーカス領域の選択内容に応じて、新しいクエリを作成できます。

展開されたタイムラインで時間範囲を選択するには、次の手順を実行します。

1. (ズームインまたはズームアウト モードで) 展開されたタイムラインを表示した状態で、**右クリック**して**右にドラッグ**または**左にドラッグ**して、焦点を当てて分析したいイベントの日付範囲を選択します。

   ミニ タイムラインと展開されたタイムラインの両方の選択されていない領域はグレーで淡色表示されます。選択した日付範囲のイベント数が展開されたタイムラインの左側に表示されます。



2. 選択内容を変更するには、選択内容をクリックして左または右にドラッグします。また、選択ボックスの左端または右端をクリックしてドラッグし、選択範囲を拡大または縮小することもできます。

   クエリバーの日付範囲が、選択したイベントの日付範囲を反映するように変更され、［検索］ボタンが強調表示されて新しいクエリ検索が開始されます。

3. 選択した時間範囲内のイベントをさらに分析したい場合は、［検索］ボタンをクリックして、関心のある領域またはフォーカス領域の選択内容に基づいて新しいクエリを開始します。

クエリ時間範囲のリセット

クエリ時間範囲のリセット機能を使用すると、当初の要求された状態にクエリをリセットできます。

最初のクエリの後でズームまたは選択を行った場合に、元のクエリ状態にすばやく戻るには、  （**クエリ時間範囲のリセット**）ボタンをクリックします。このアクションにより、タイムラインがズームアウトされ、選択内容が削除されて、クエリバーの時間範囲がリセットされます。

結果セットの絞り込み

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

- メタ グループを使用して関連性の高いメタ キーにフォーカス
- イベント リストでの列と列グループの使用
- 保存済みクエリ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
- [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
- URL統合を使用したクエリの表示と変更
- イベントビューから将来のアラートを作成する
- イベントビューからレポートを生成する
- 調査ビューからイベント ウィジェットを作成する

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 [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 メタ]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 メタ]パネルに表示可能) です。 [イベント]ビュー([イベント メタ]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。

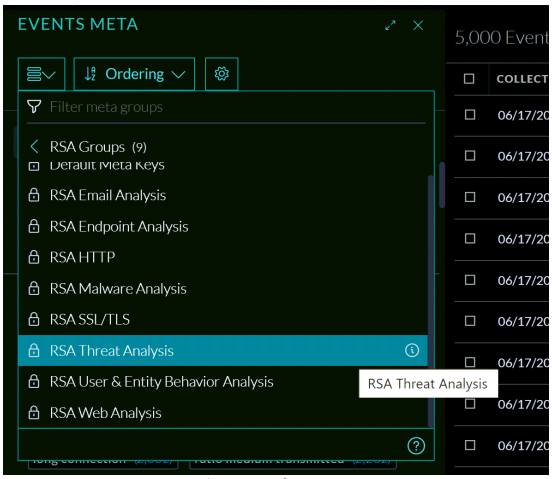
調査中にメタ グループが有効になっている場合、 [値]パネルまたは [イベントの絞り込み]パネルの情報には、選択されたグループのメタ キーのみが表示されます。座標表示チャートを [ナビゲート]ビューで開くと、メタ キーとメタ エンティティが軸として左から右に表示されます。カスタム メタ グループごとに2つのバージョンを作成しておくと便利です。1つはメタ値の分析に使用し、もう1つはメタ キーを減らしたサブセットを作成し、座標表示チャートの表示に使用します。

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。 [イベント]ビューの [イベント メタ]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。

Liveメタ グループ

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

NetWitnessには、名前が「RSA」で始まり、インストール直後から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 キーが包含されています。
- RSA Web Analysisには、Webトラフィックの異常をマークするメタ キーが含まれています。

デフォルトのメタ キー グループ

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組み込みメタグループで、サービスのインデックスファイルに記載されている順に表示されます。他の標準提供メタ グループとは異なり、このグループをコピーしたり、［メタ グループの詳細］ダイアログで情報を表示し、どのキーが含まれているかを確認することはできません。その代わりに、［詳細］ダイアログには、選択したサービスのすべてのメタ キーが含まれていることを示すメッセージが表示されます。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 メタ］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 メタ］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

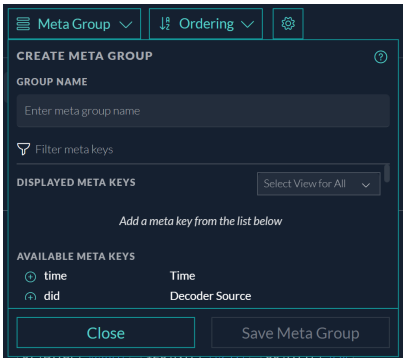
カスタム メタ グループを作成して、調査中に頻繁に使用するシナリオをサポートできます。管理者が、サービスのカスタム インデックス ファイルを編集して、カスタム メタ グループを手動で追加した場合、サービスの再起動後に新しいメタ グループが利用可能になります。カスタム メタ グループは、共有またはプライベートにすることができます。共有メタ グループは、[ナビゲート]ビューと[イベント メタ]パネルで、組織内でグローバルに使用できます。共有のカスタム メタ グループを編集する場合、変更はグローバルに適用されます。共有のカスタム メタ グループを削除すると、そのグループは削除され、すべてのアナリスト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。

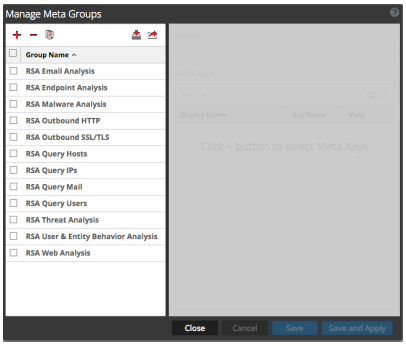
注：[イベント]ビューで作成されたプライベート カスタム メタ グループは、[ナビゲート]ビューで表示または使用できません。

[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カスタム メタ グループの例です。



[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。

このトピックの残りの部分では、[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。

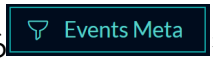
[イベント]ビューでのメタ グループの操作

NetWitness Platformの最新バージョンにアップグレードすると、組み込みとカスタムの両方の既存のメタ グループが、イベント メタ パネルでイベントをフィルタリングするため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。

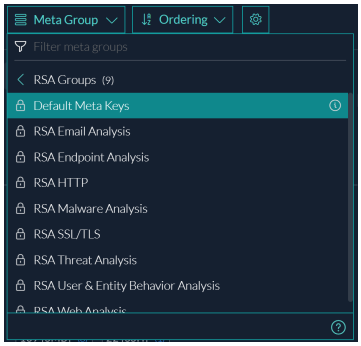
メタ グループに含まれているメタ キーの表示

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。

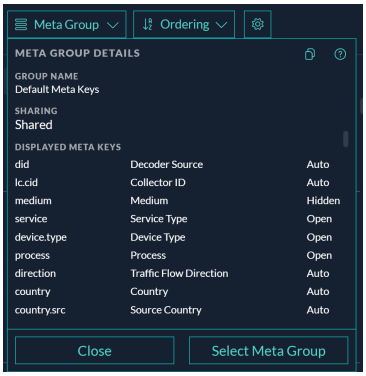
2. [イベント メタ]パネルを表示するには、[イベント]パネルの上にある 

をクリックします。
   [イベント]パネルの左側で [イベント メタ]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、正確なテキストを含むグループ名のみが表示されます。

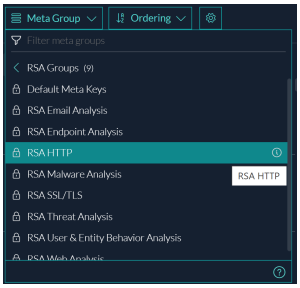
5. メタ グループ名 の上 にマウスを移 動し、情 報アイコン ( ) をクリックすると、グループに含 まれるメタ キーが表 示されます。
この図 は、Default Meta Keysメタ グループの列を示しています。



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、イベント メタ パネルが更 新され、選 択したメタ グループのメタ キーが反 映されます。

メタ グループの選 択

1. [イベント]ビューで [イベント メタ]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 グループのフィルター*** フィールド にテキストを入 力し始 めます。入 力すると、リスト がフィルターされ、その文 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、**ENTER**キーを押します。
   [イベント メタ]パネルの表 示が更 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。この選択は、イベントから移動した後も保持されます。

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

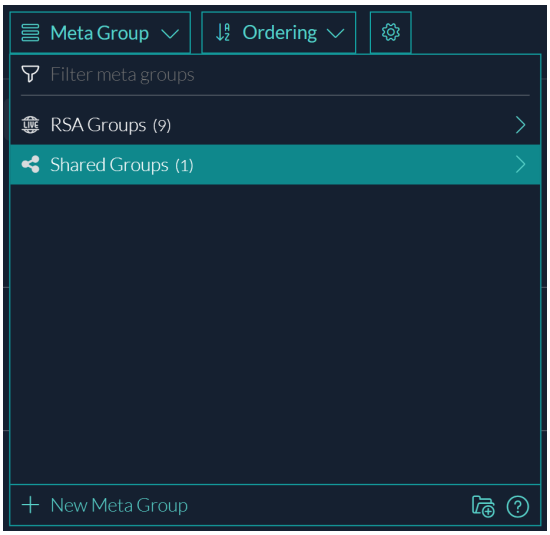
カスタム メタ グループには、最大80文字の一意の名前と、少なくとも1つのメタ キーが必要です。共有かプライベートかにかかわらず、入力した名前のメタ グループが他にある場合は、別の名前を使用する必要があることを知らせるメッセージが表示されます。上記の基準を満たしたら、 [メタ グループの保存] ボタンが有効になります。 [表示するメタ キー] リストでキーをドラッグして、グループ内のメタ キーの順序を調整できます。

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。

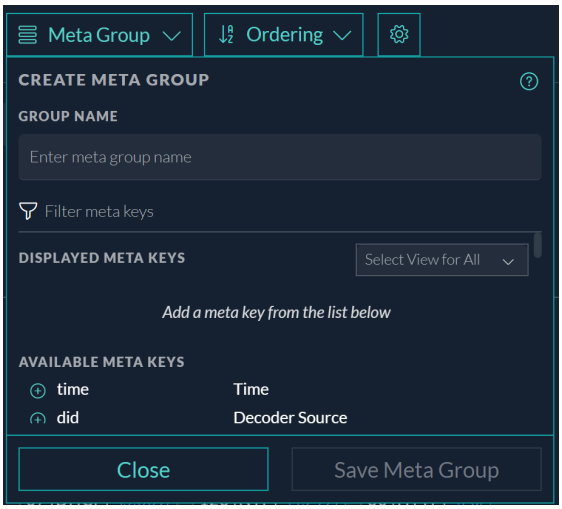
注 : また、同じ値をすべてのメタ キーに一度に設定することもできます。すべてのメタ キーの値を変更すると、パフォーマンスに影響する可能性があることに注意してください。

- [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] に変更すると、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 メタ] 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 メタ] 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 メタ] 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. [イベント] ビューで [イベント メタ] 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。

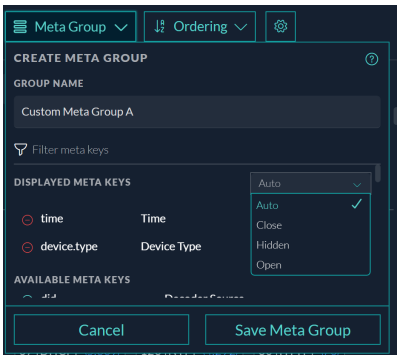


2. [**新しいメタ グループ**]を選択します。
   [メタ グループの作成]ダイアログが表示されます。



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 メタ]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。

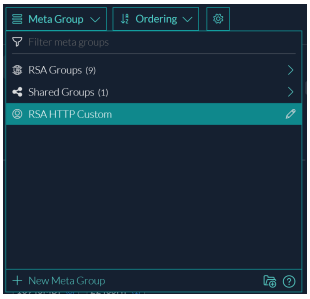
カスタム メタ グループの削除

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か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。

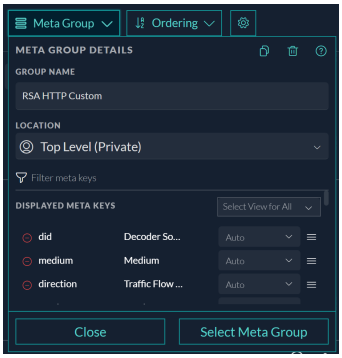
注意 :共有メタ グループの削除の影響はグローバルであり、すべてのアナリストがそのグループを使用できなくなります。

カスタム メタ グループを削除するには

1. ビューでイベント メタ パネルを開いた状態で、イベント 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、上部に [メタ グループのフィルター] フィールド、下部に [+ 新しいメタ グループ] オプションがあるメタ グループとフォルダーのリストが表示されます。



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。

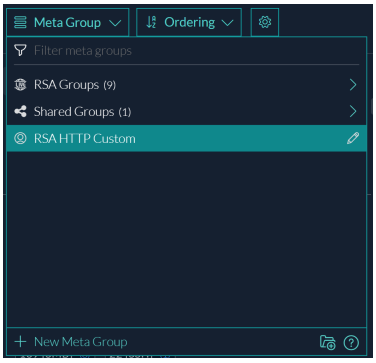


4. グループの削除アイコン( ) をクリックします。
   メタ グループが現在有効になっている場合は、次のメッセージが表示されます。`This meta group cannot be deleted because it is currently active.`
   確認メッセージが表示され、削除を確認またはキャンセルすることができます。 [**キャンセル**] または [**メタ グループの削除**] をクリックします。
   グループが削除され、 [メタ グループ] メニューに表示されなくなります。削除したメタ グループは、調査を行うすべてのアナリストに表示されなくなります。

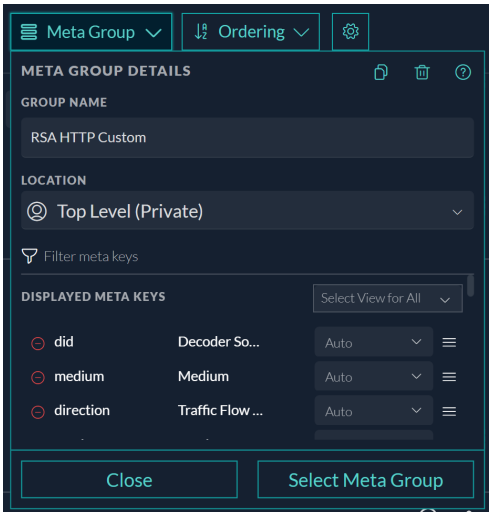
カスタム メタ グループの編集

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。

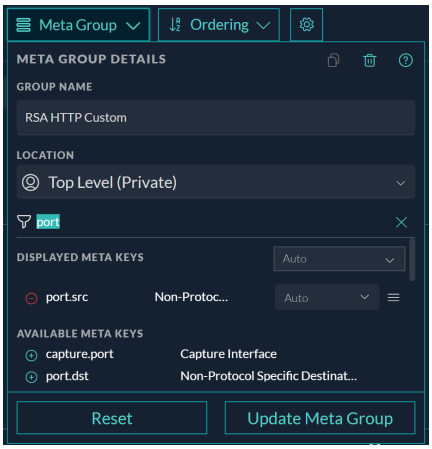
1. [イベント]ビューで [イベント メタ]パネルを開いた状態で、 [**メタ グループ**]メニュー タイトルをクリックし、編集するメタ グループをハイライト表示します。次の図は、ハイライト表示されたプライベート メタ グループRSA HTTP Customと、その右側に表示された編集アイコンを示しています。



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、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て、そのテキストを含むメタ キーを [**表示するメタ キー**]リストで検索します。または、単にリストをスクロールして探します。削除するメタ 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。

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 グループをコピーする

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。

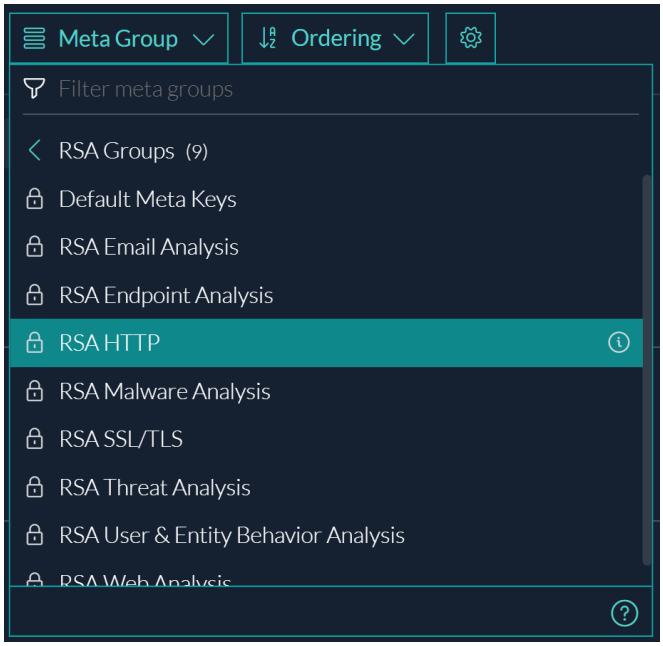
注： [レガシー イベント]ビューで作成された一部のメタ グループには、 [イベント]ビューのメタ グループの制限を上回る、500個を超えるメタ キーが含まれている場合があります。500個を超えるメタ キーを持つグループをコピーする場合は、メタ グループの編集時に余分なメタ キーを削除する必要があります。

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. [イベント]ビューで [イベント メタ]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。

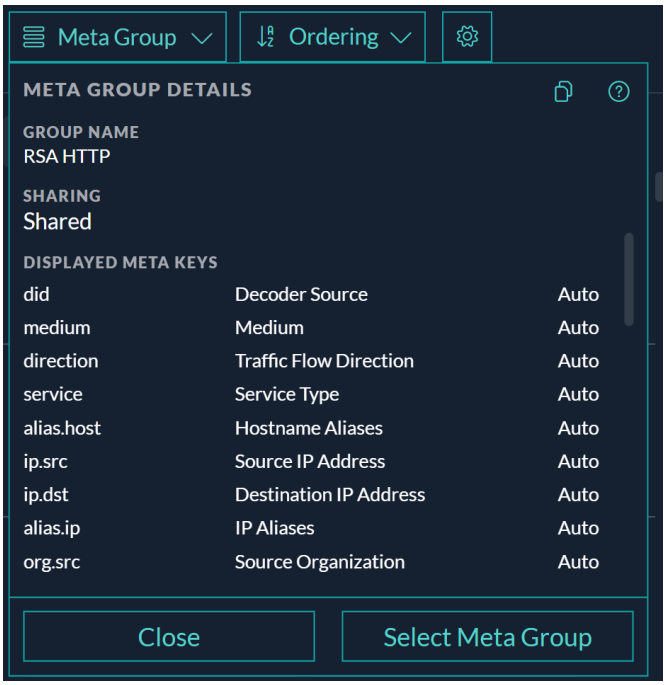


3. 次のいずれかの操作を実行します。

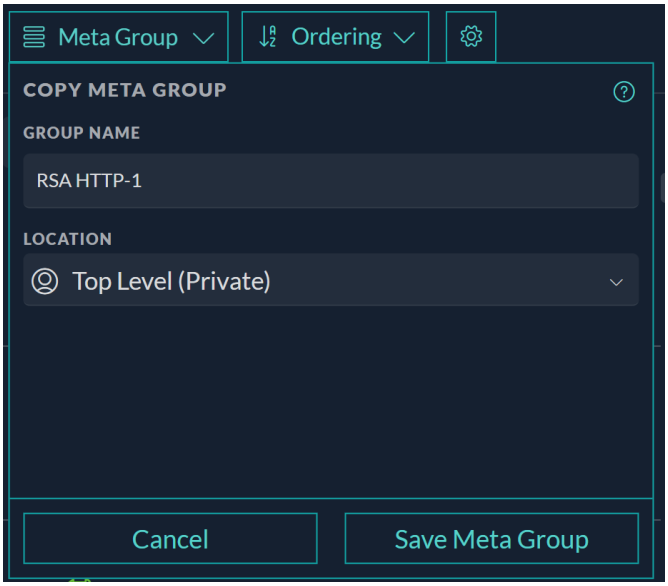
   a. 情報アイコン( ) をクリックします。

   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。

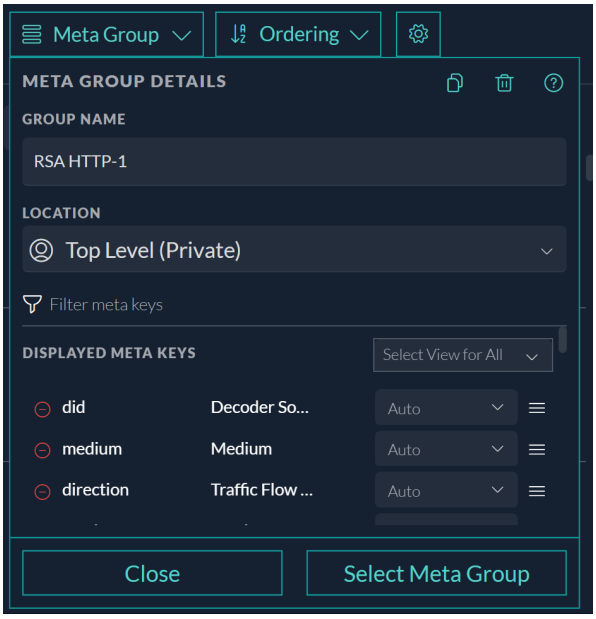


4. コピー アイコン( ) をクリックします。
   [メタ グループのコピー]ダイアログが開き、元のメタ グループ名に-nが付記されて表示されます。

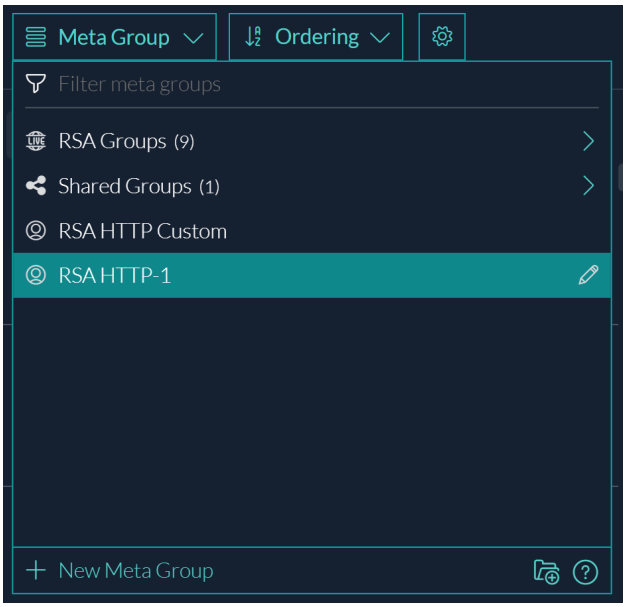


5. (オプション) [**グループ名**]フィールドで、メタ グループの名前と場所を編集します。
6. 次のいずれかの操作を実行します。
   a. グループをコピーせずにダイアログを閉じるには、[**キャンセル**]をクリックします。
   b. メタ グループのコピーを保存するには、[**メタ グループの保存**]をクリックします。
      メタ グループのコピーが保存され、コピーしたグループの [メタ グループの詳細]ダイアログが表示

されます。

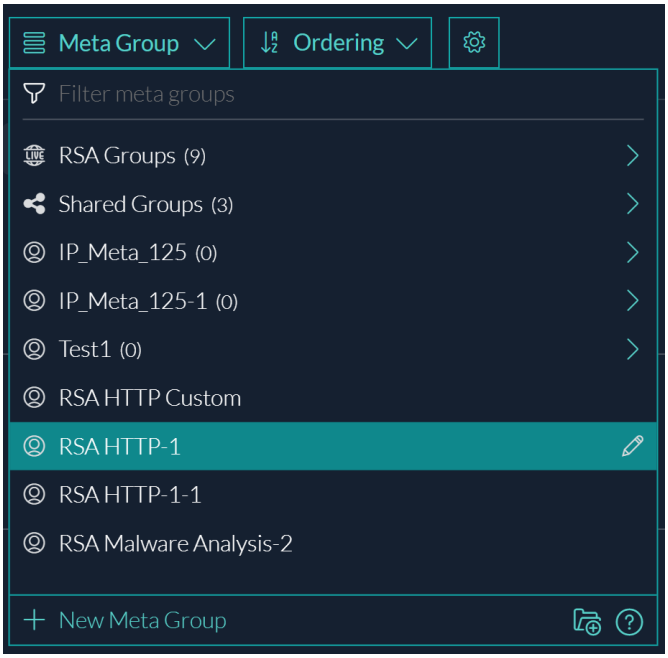


7. 次のいずれかの操作を実行します。
   a. 編集しないでダイアログを閉じるには、 **閉じる**]をクリックします。
   b. ダイアログを閉じてメタ グループのコピーを選択するには、 **[メタ グループの選択**]をクリックします。
      [メタ グループ]メニューにグループが追加されます。次の図は、RSA HTTPメタ グループのプライベート コピーを示しています。



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 フォルダーとプライベート 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 フォルダーとその内容は、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。

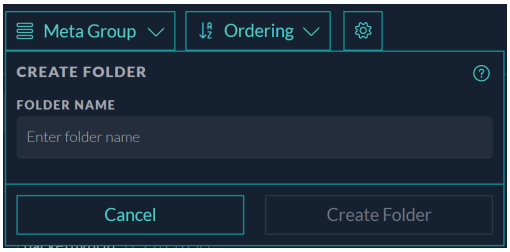


このセクションでは、カスタム メタ グループとフォルダを追加、編集、インポート、エクスポート、コピー、および削除する方法について説明します。

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。

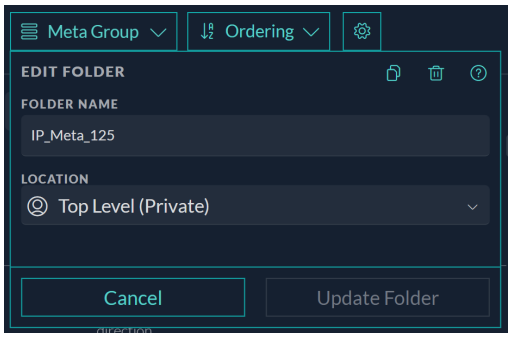


3. [**フォルダ名**]フィールドに、新しいメタ グループ フォルダの一意の名前を入力します。
4. [**フォルダの作成**]をクリックします。

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、共有フォルダーをプライベート フォルダーに移動したり、その逆を行ったりすることはできません。

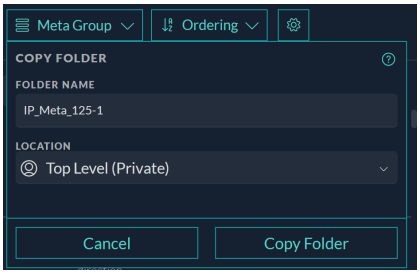
1. [イベント]ビューで [イベントの絞り込み]パネルを開いた状態で、 [メタ グループ]メニュー タイトルをクリックし、編集するメタ グループをハイライト表示します。
2.  をクリックします。
   フォルダー編集ダイアログが表示されます。



3. [**フォルダー名**]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。
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。

メタ グループ フォルダのコピー

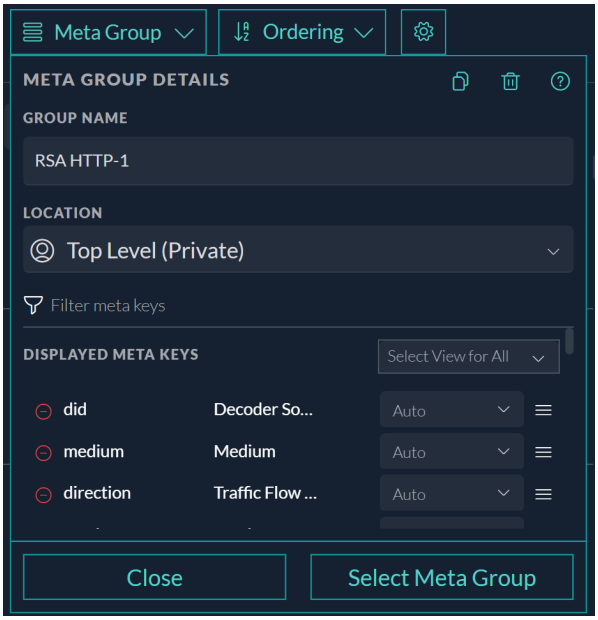
ユーザは、RSA、共有、プライベートなど、あらゆるタイプのメタ グループ フォルダをコピーできます。ただし、RSAグループのデフォルトでは、コピー フォルダはプライベート セクション(ルート レベル) にコピーを作成しますが、フォルダの場所を共有フォルダまたはその他のプライベート フォルダに変更できます。クローン アイコン( ) をクリックすると、メタ グループをコピーできます。コピー後、メタ グループ フォルダは選択した場所([共有]または [プライベート]カテゴリ) に表示されます。コピーしたアイテムにカーソルを合わせると、メタ グループのコピー元のパスを示すツールチップが表示されます。特定のメタ 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、選択したフォルダーからメタ グループがフィルタ処理されます。



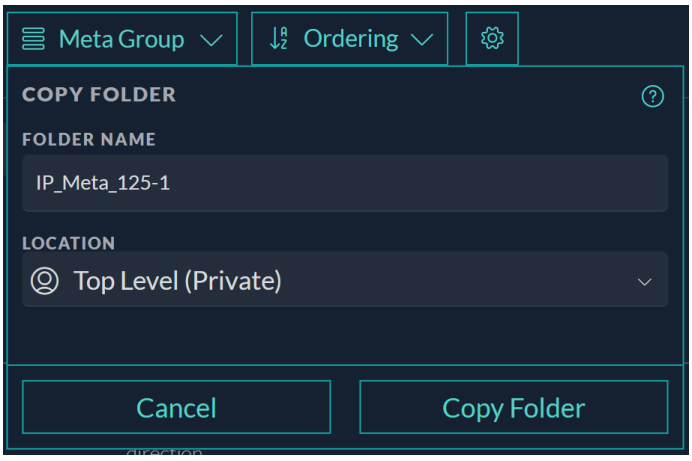
メタ グループのプライベート フォルダまたは共 有 フォルダのコピー

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 メタ 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。



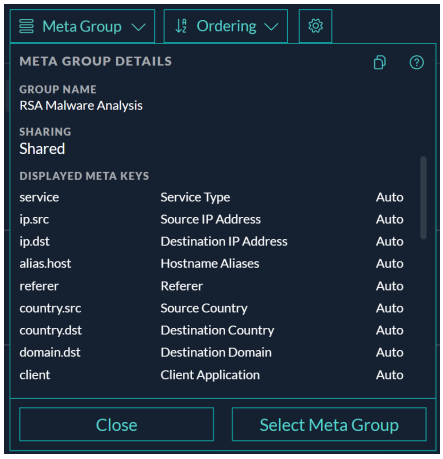
4. [**フォルダ名**] フィールドに、新しいメタ グループ フォルダの一 意 の名 前を入 力します。

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。

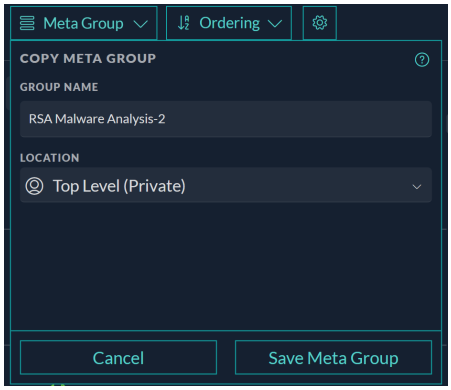
Liveから導 入 されたメタ グループ フォルダのコピー

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 メタ]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。

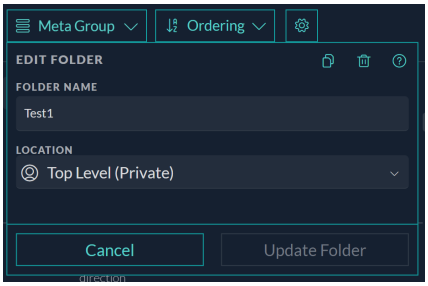


4. コピーするフォルダの場 所を選 択します。
5. [**フォルダのコピー**]をクリックします。
フォルダーと第 1レベルの内 容 がコピーされ、サブフォルダーはコピーされません。コピーされたメタ グループ フォルダーとその内 容 が、元 のメタ グループ名 に-nが付 記された名 前 で表 示されます。

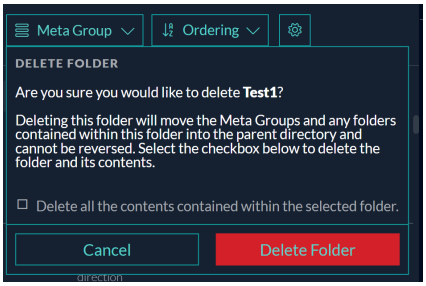
メタ グループ フォルダの削除

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 メタ 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。



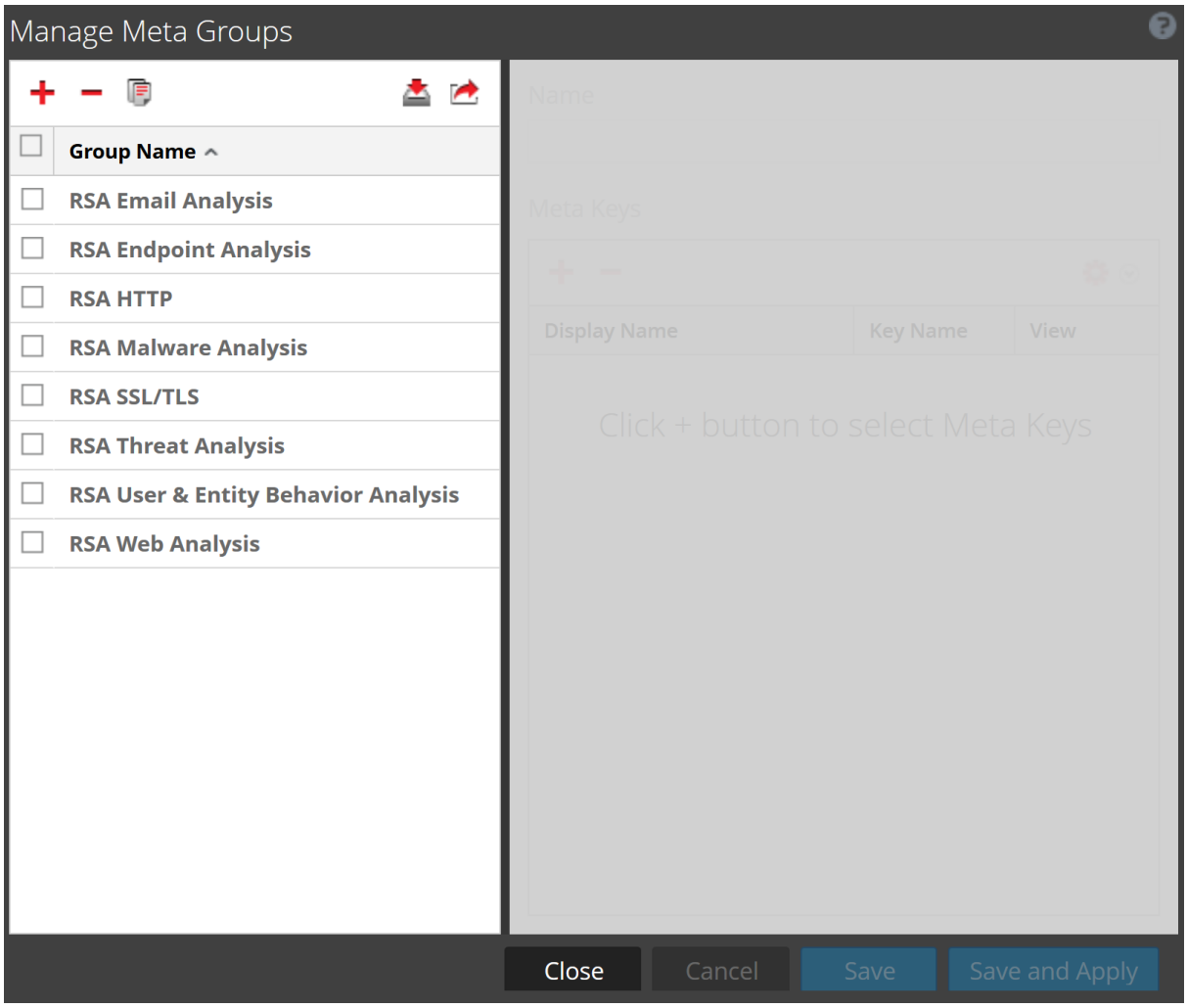
5. (オプション) 選択したフォルダ内のすべてのコンテンツとともにフォルダを削除する場合は、このチェックボックスを選択します。
   チェックボックスを選択しないと、必要なフォルダが削除された後で、コンテンツは親フォルダに移動されます。
6. 削除するには、**「フォルダーの削除」**をクリックします。

[ナビゲート]ビューでのメタ グループの操作

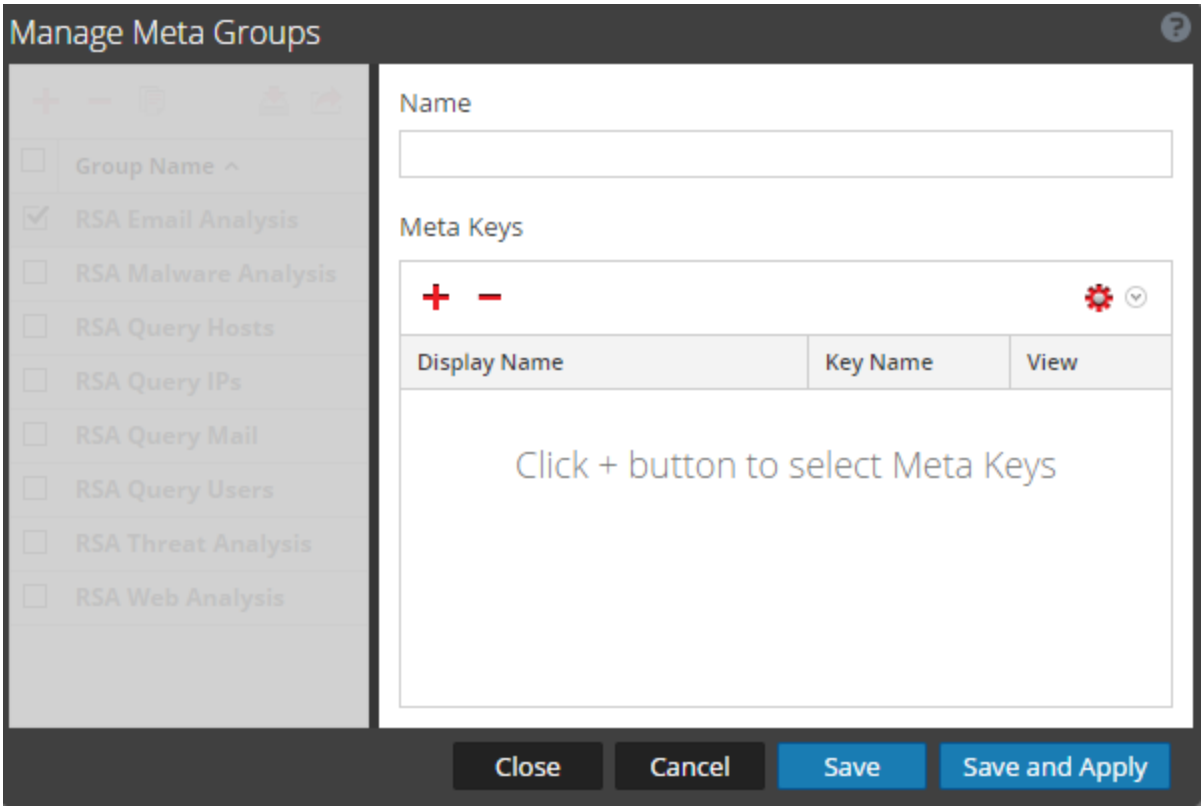
メタ グループの作成とメタ キーの追加

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。

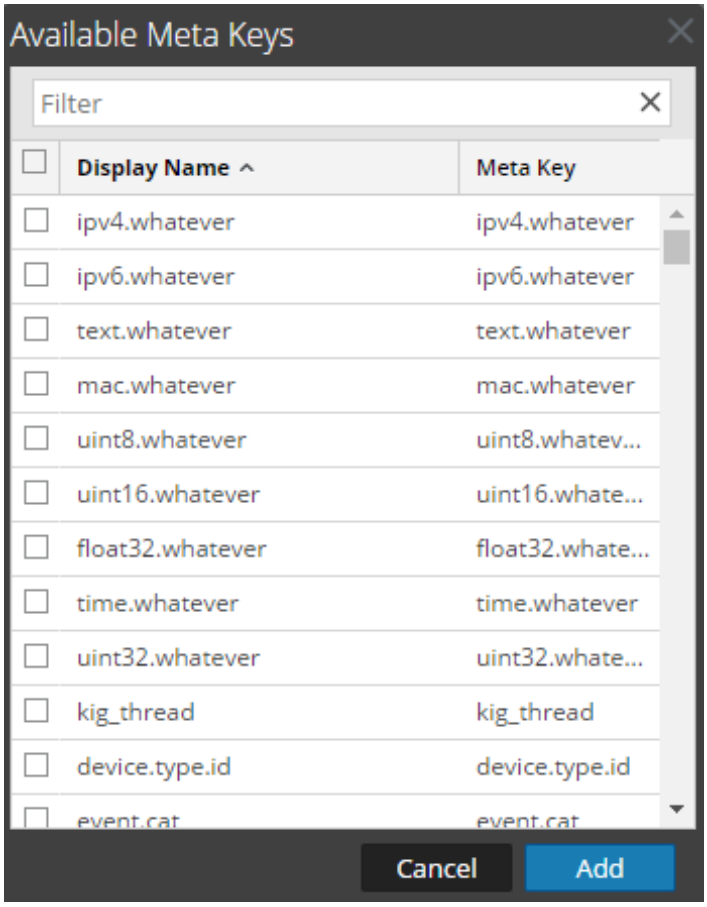


2. [メタ グループ]リストの上にあるツールバーで、 をクリックします。
右側にフォームが開いて編集可能な状態になります。



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。

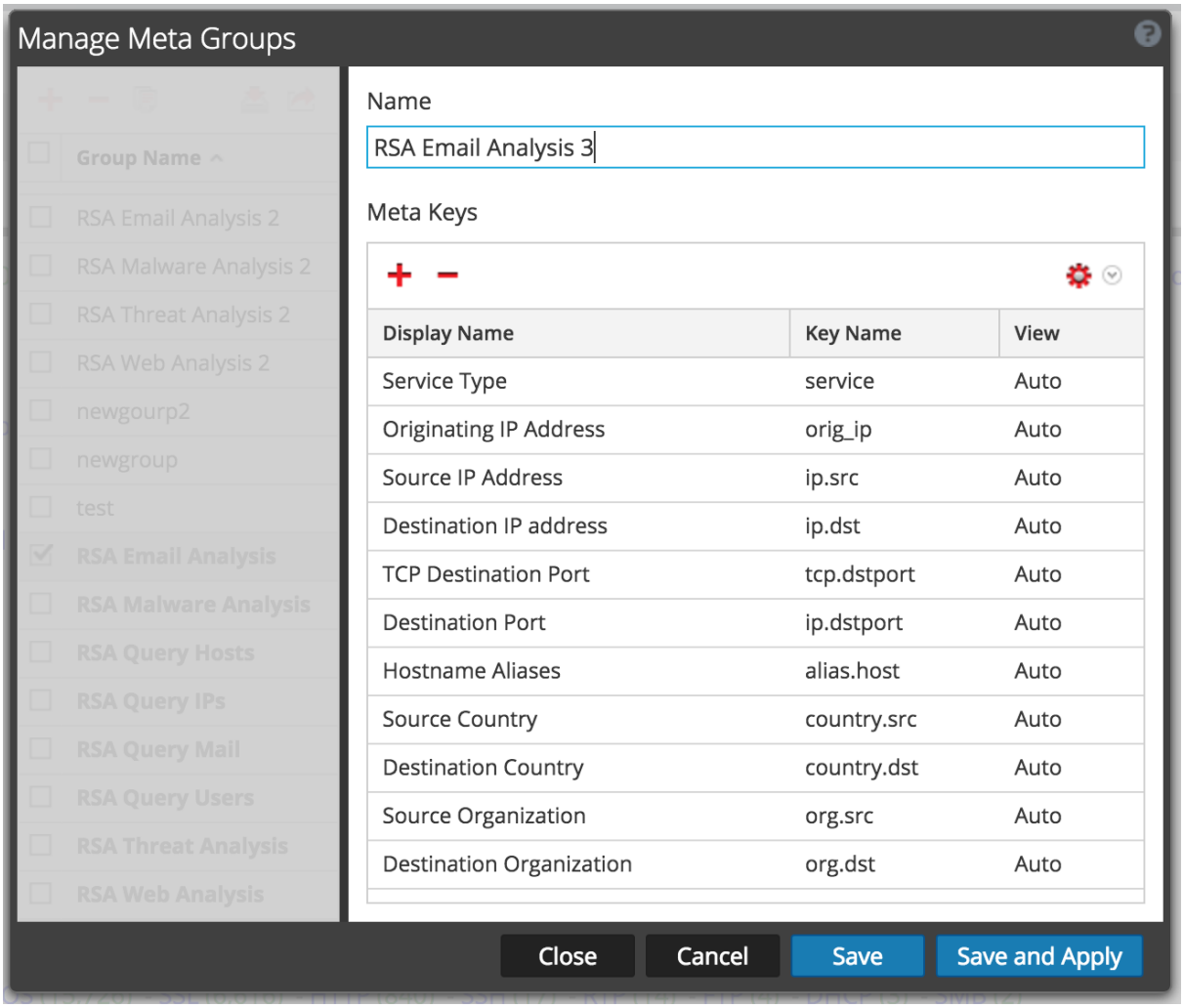


5. メタ キーのリストを絞り込むには、 [フィルタ]フィールドに単語またはフレーズを入力し、Enterキーを押します。
一致するメタ キーがリストに表示されます。大文字と小文字は区別されません。 [フィルタ]フィールドのテキストを削除してEnterキーを押すと、フィルタを削除できます。
6. メタ グループに追加するメタ キーを個別に選択するには、チェックボックスをオンにします。すべてのメタ キーを選択するには、タイトル バーのチェックボックスをオンにして [追加]をクリックします。
選択したメタ キーが [メタ キー]リストに追加されます。
7. (オプション) メタ キーをロードして表示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。
   a. メタ グループを保存するには、 [保存]をクリックします。
   グループが作成され、使用可能になります。
   b. メタ グループを保存して、現在の [調査]ビューに適用するには、 [保存して適用]をクリックします。
   グループが作成され、現在の [調査]ビューにすぐに適用されます。
9. [閉じる]をクリックします。

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。

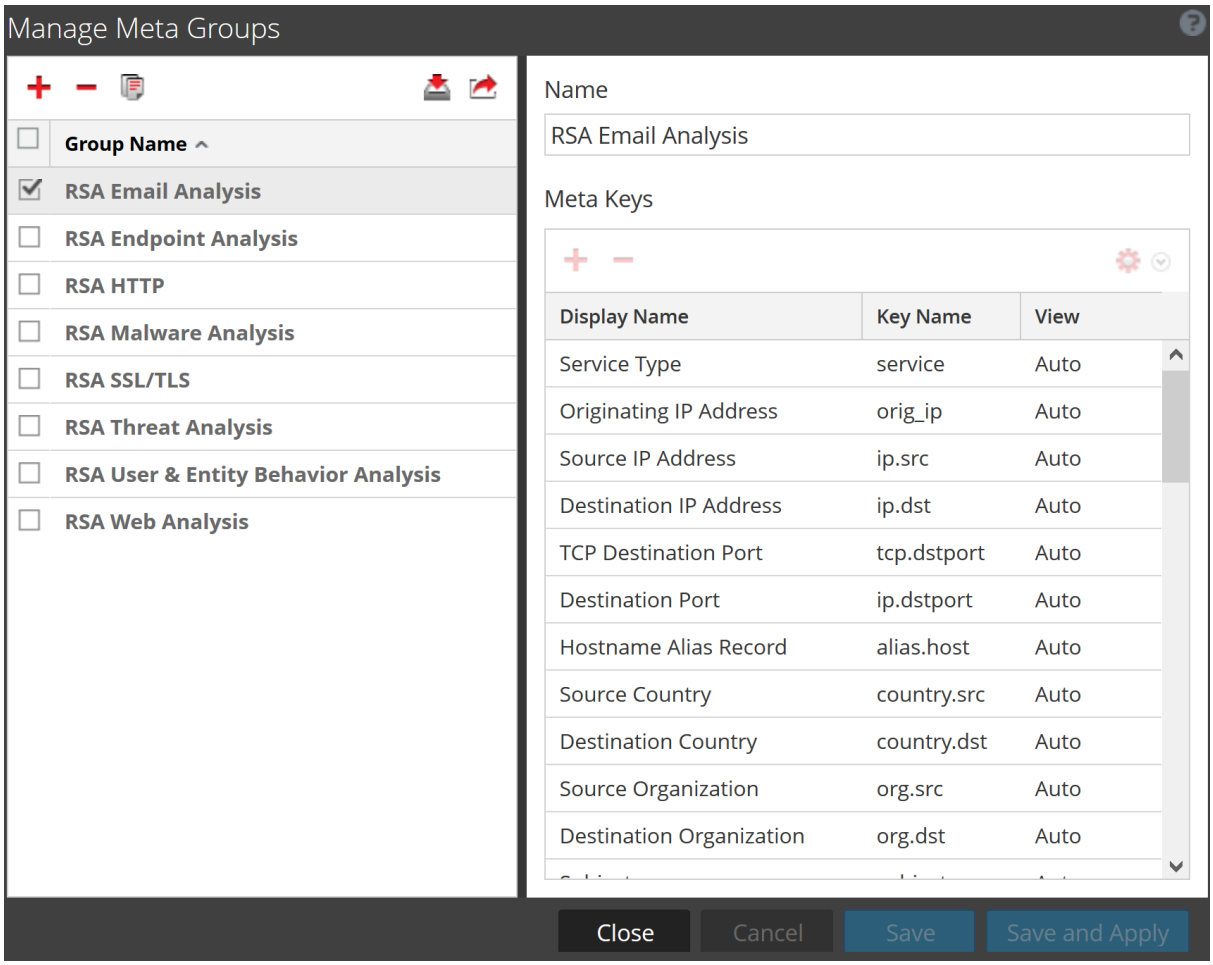
1. [メタ グループの管理]リストから標準提供のメタ グループを選択し、 をクリックします。
右側に編集可能なフォームが開き、標準提供グループ内のすべてのメタ キーが表示されます。



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。



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

メタ グループの削除

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

メタ グループのエクスポート

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

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

メタ グループのインポート

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

メタ グループをインポートするには

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



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

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

イベント リストでの列と列グループの使用

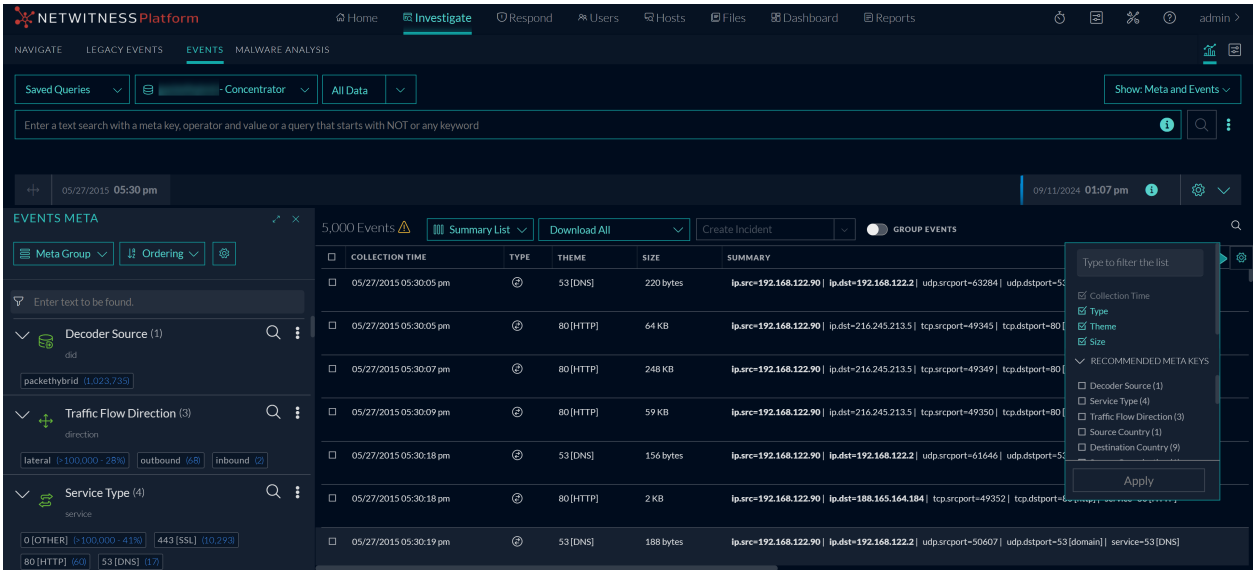
調査のイベント リストにイベントが読み込まれると、各列にメタ キーの値が表示されます。イベント リストに表示されるメタ キーの変更は、調査のフォーカスを絞り込むための便利な方法です。たとえば、同じイベントの異なる列を表示する2つの図で比較してみましょう。最初の図には、**Collection Time**、**Type**、**Theme**、**Size**、**Summary**という5つの列があります。これらは基本的な情報であり、特殊な情報ではありません。2番目の図には、メールを調査する際に役立つ情報を含んだ、より多くの列があります。右にスクロールして、追加の列を表示できます。





イベント リストでは、表示する別の列の選択、列の順序の変更、列幅の変更、リストをソートする列の選択などの調整を、作業しながら加えることができます。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。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。

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 メタ パネルから関連するすべてのメタ キー情報を取得できるようになりますが、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可能性があります。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。



[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便利ですが、メタ グループやpreQueriesと組み合わせてクエリ プロファイルを定義すると、さらに便利になります(「 保存済みクエリ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 [ナビゲート]ビューのクエリ プロファイルで使用できません。

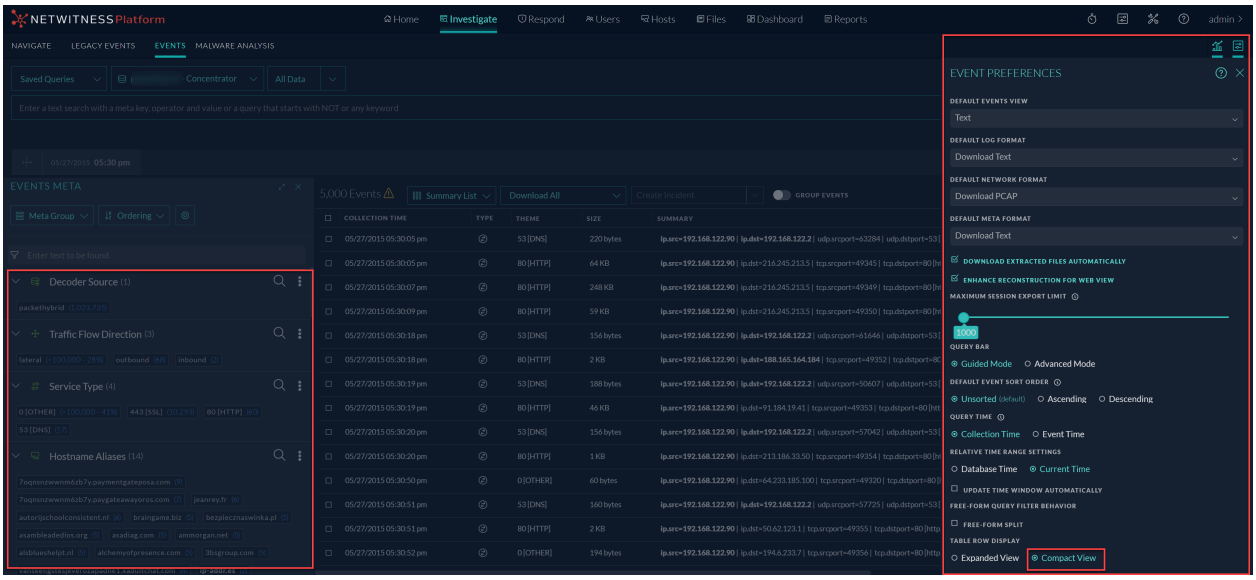
注： [ナビゲート]ビューと [レガシー イベント]ビューでは、インデックスなしのメタ キー(またはインデックスにまったく含まれていないキー) をメタ グループまたは列グループに手動で追加できます。インデックスなしのメタ キーは、 [ナビゲート]ビューと [レガシー イベント]ビューでは完全に使用可能(管理および表示可能) ですが、 [イベント]ビューでは部分的にのみ使用可能([イベントの絞り込み]パネルに表示可能) です。 [イベント]ビューの [イベントの絞り込み]パネルには、メタ グループにすでに含まれているインデックスなしのメタ キーのデータを表示できますが、メタ グループの編集中にイ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

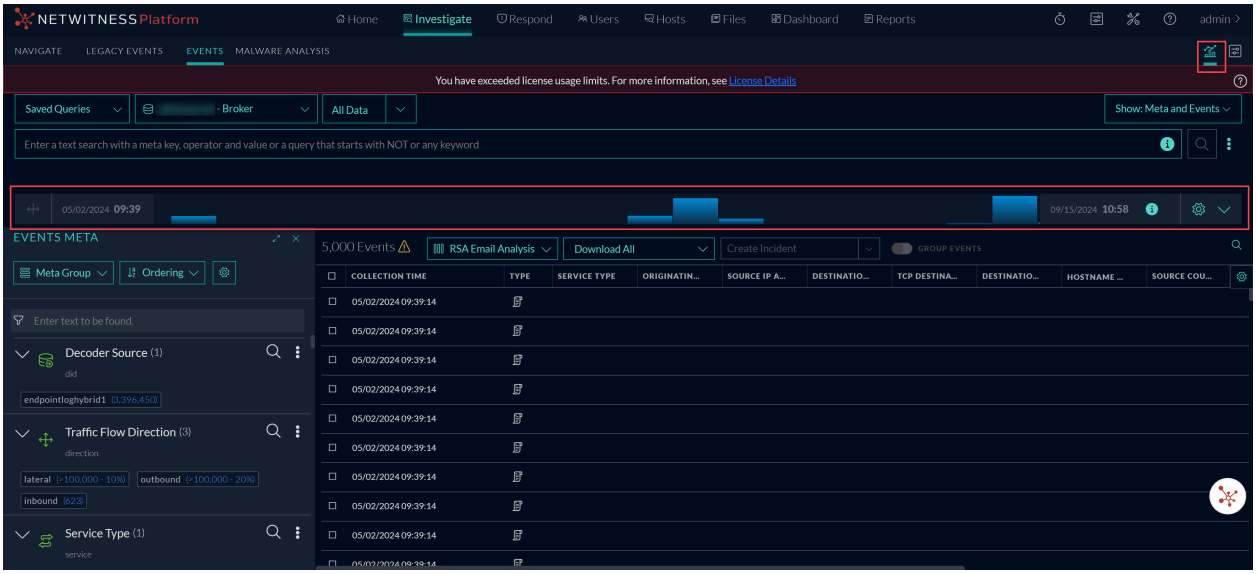
[レガシー イベント]ビューには、列グループ内のメタ キーの数の制限がなく、40個を超えるメタ キーを列グループに含めることができます。 [レガシー イベント]ビューで作成された40個を超えるメタ キーを含む列グループを適用すると、すべての列が [イベント]ビューにロードされます。500個を超える列を持つグループをコピーする場合は、列グループの編集時に余分な列を削除する必要があります。

注 : 組み込みとカスタムの両方の既存の列グループはすべて、イベント ビューで使用できます。 [レガシー イベント]ビューでは、完全な列グループ管理機能を使用できます。 [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。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。

アナリストが分析対象のイベントに関連する詳細情報を最大限に表示できるように、スペースを最適に活用するために、**調査イベント設定** ビューが追加されました。

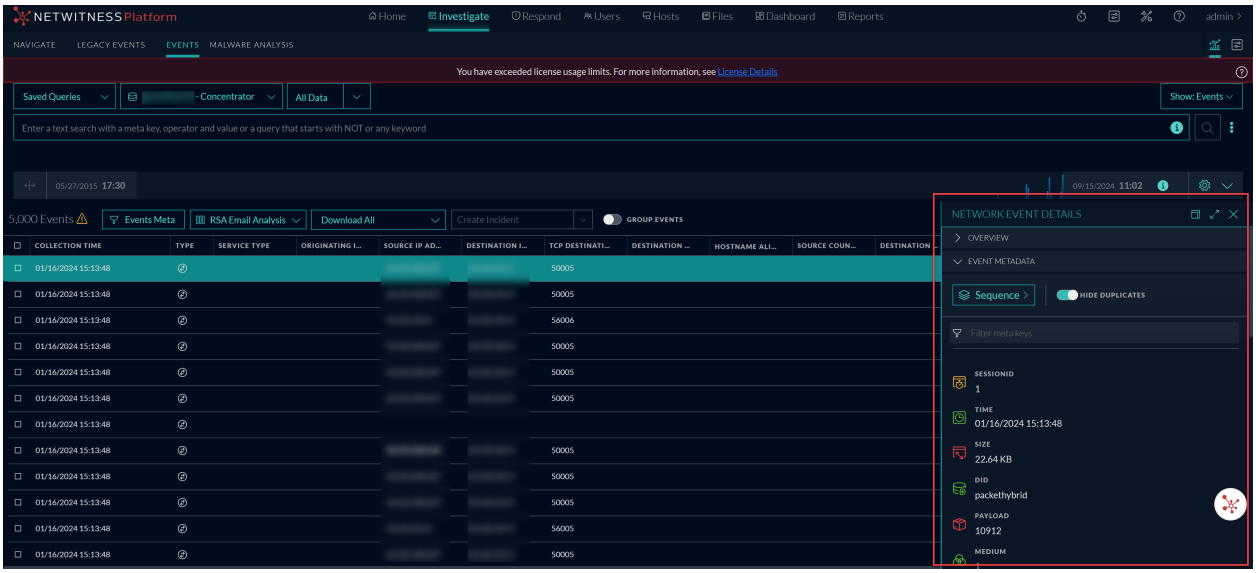


さらに、  アイコンをクリックして、イベントのタイム ラインの詳 細を表 示できるようになりました。図に示すように、表 示されたタイムラインをクリックすると、日 付と時 刻の範 囲が表 示されます。

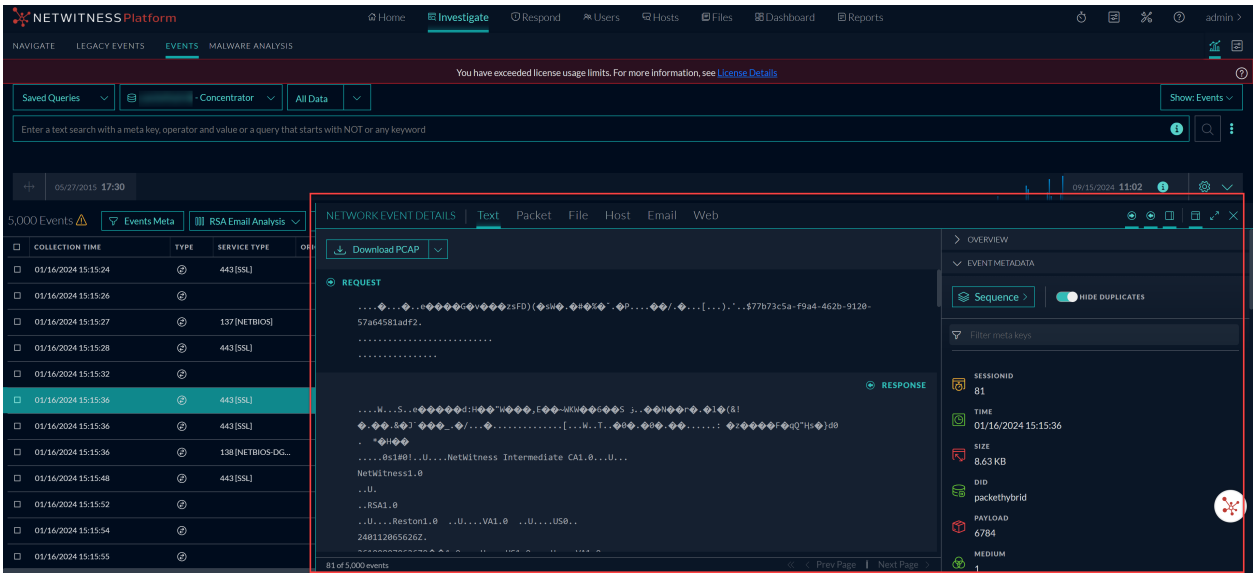


調査]> [**イベント**]の再 構 築パネルが変 更され、展 開と折りたたみが可 能な [概 要]タブと [メタ]パネル タブを含むオーバーレイが表 示されるようになりました。これにより、アナリストはイベントのヘッダーとメタ パネルを最 適に表 示できます。 [**重 複イベントを表 示しない**]オプションを切り替えて、選 択したイベントに関 連する詳 細のみを表 示することもできます。

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。



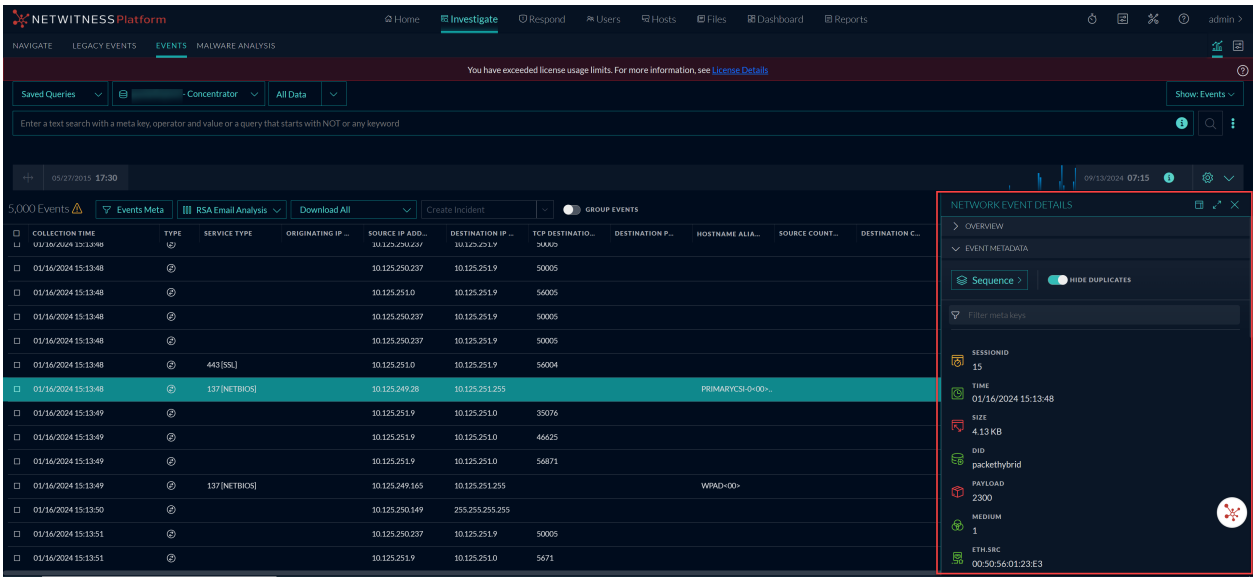
アナリストは、トグル ボタン ( ) を使用して、選択したイベントに関連する詳細を表示できます。



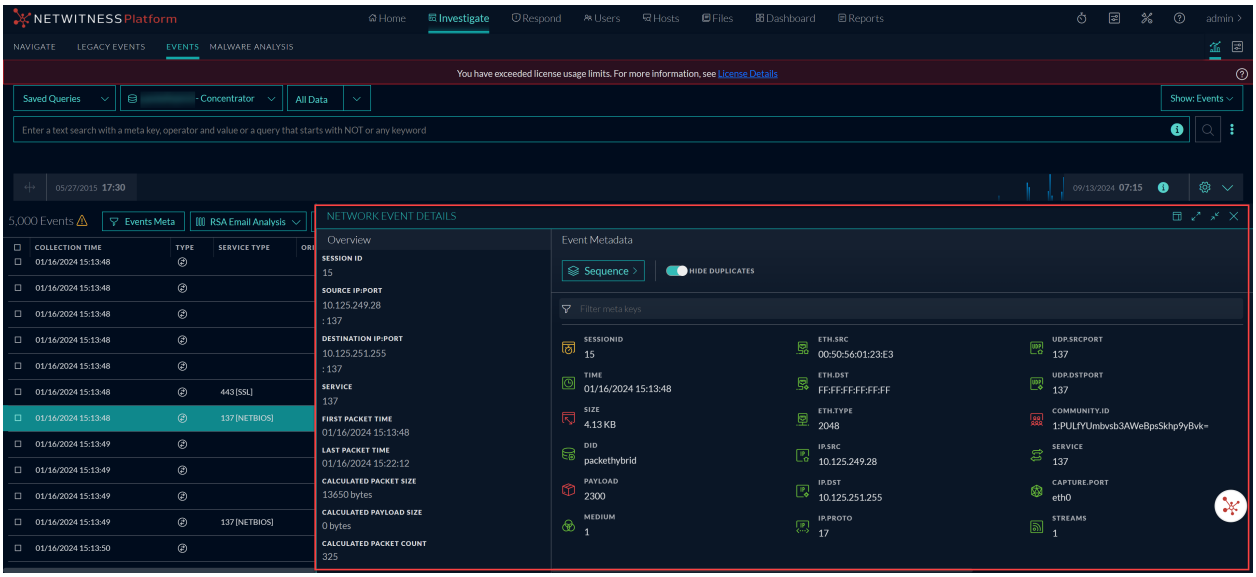
双眼鏡アイコンは、選択したイベントに関連する検索に対してイベント ペイロードが開いている場合にのみ有効になります。

[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、イベントの [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。

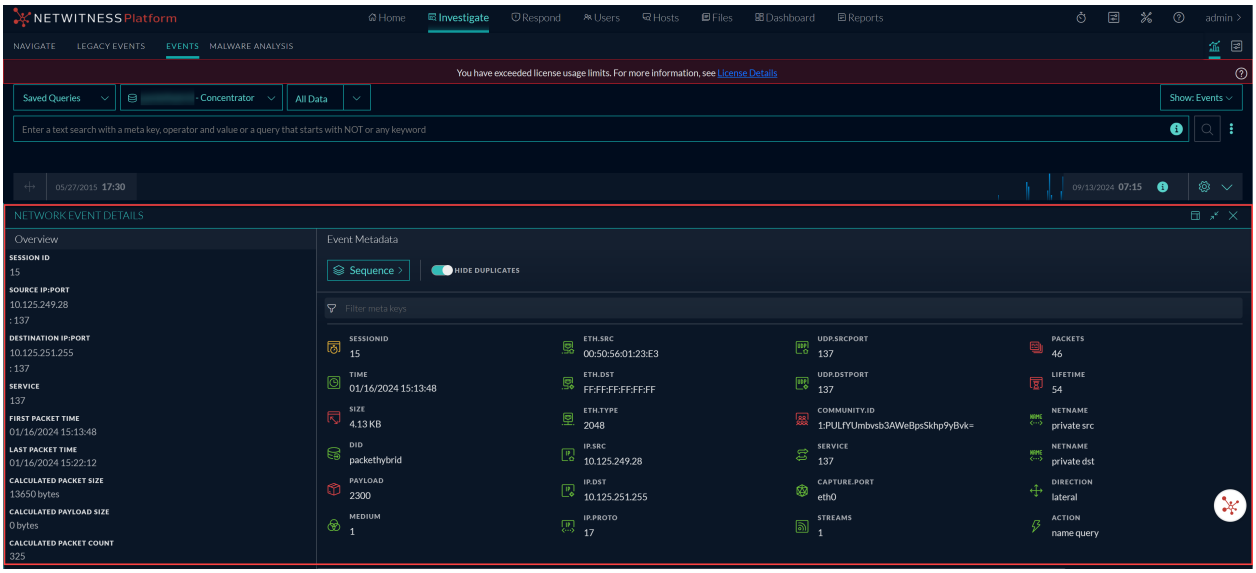
メタパネルを開いて選択したイベントの詳細を表示すると、使用可能なすべてのヘッダーが表示されます。メタ パネルには 展開]ボタン() があります。イベントをクリックすると、メタ パネルが表示されます。表示する追加のヘッダーがない場合は、ヘッダー エラーに関するエラーが表示されます。



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。



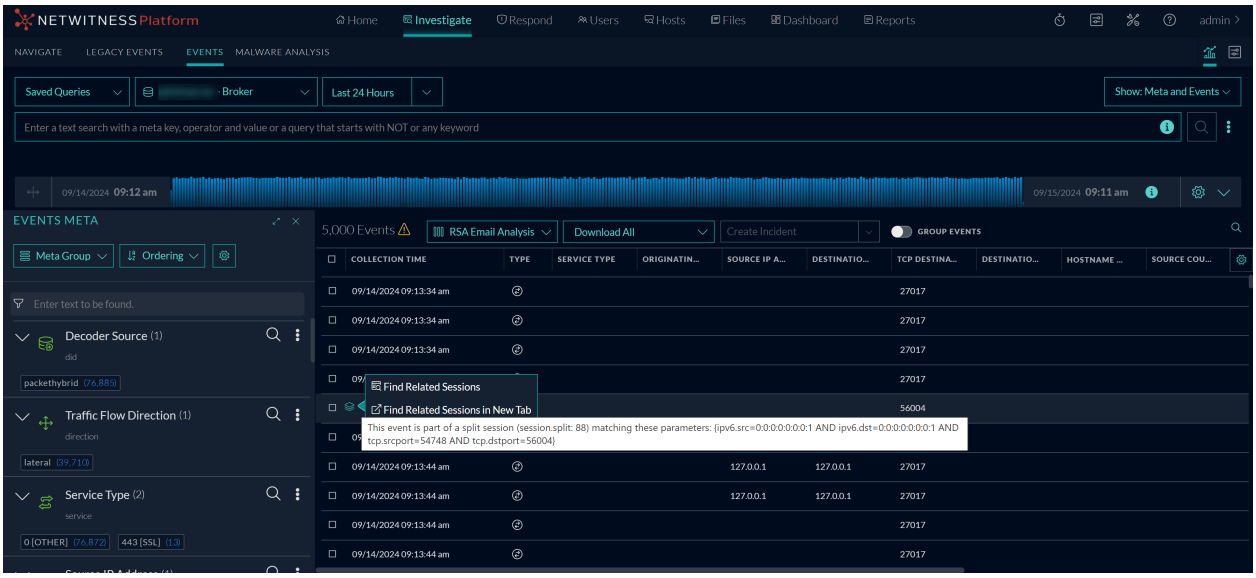
内向きの矢印のアイコン をクリックすると画面表示を元に戻すことができ、ウィンドウが前の位置に戻ります。これにより、各イベントの詳細を最適な方法で表示できます。

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。

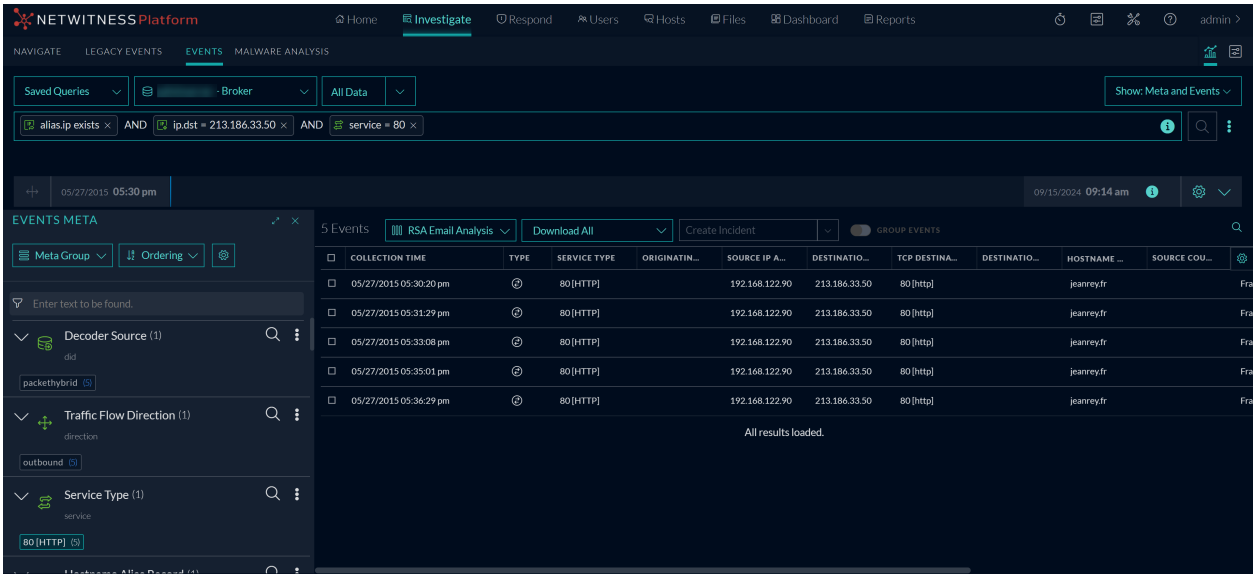
クエリは、イベントにカーソルを合わせると表示されるテキストの情報に基づきます。たとえば、次の図では、イベントに2つの分割セッションがあり、1つのイベントが別のセッションに分割されています。



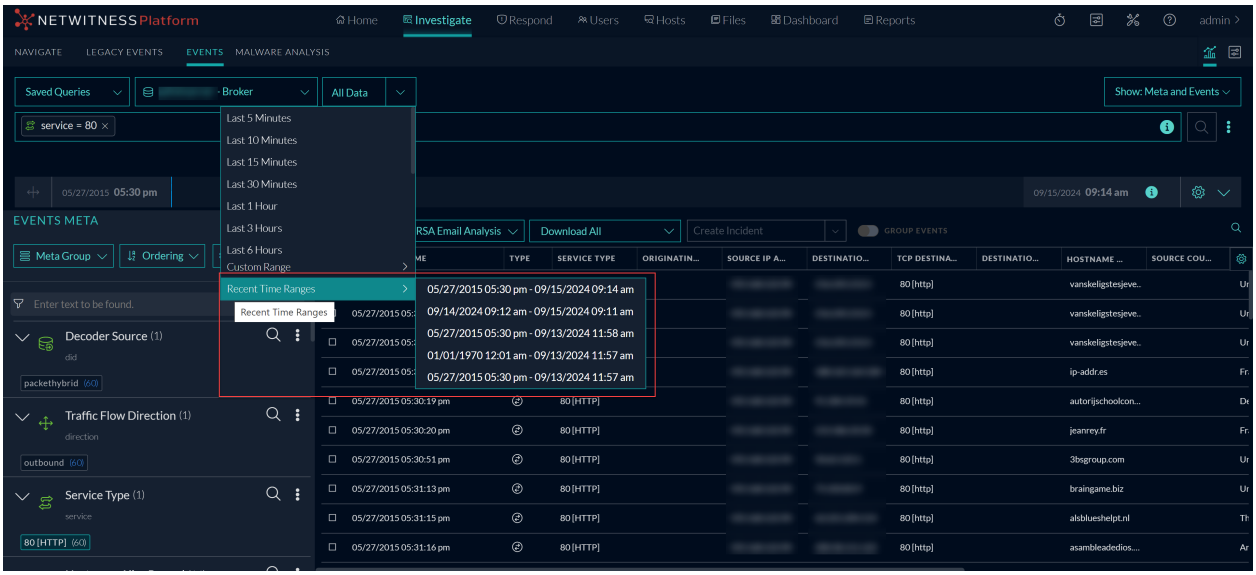
このケースでは、これらのパラメーターで検索を実行すると、次のクエリについての関連セッションが表示されます。



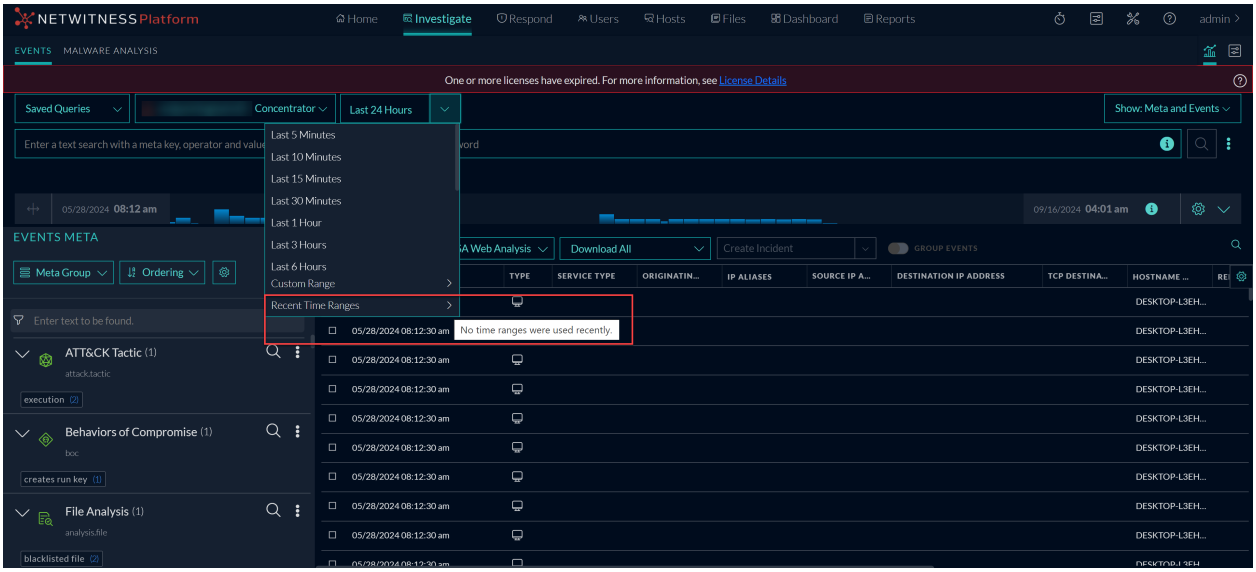
結果は次の形式で表示されます。



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、次回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。

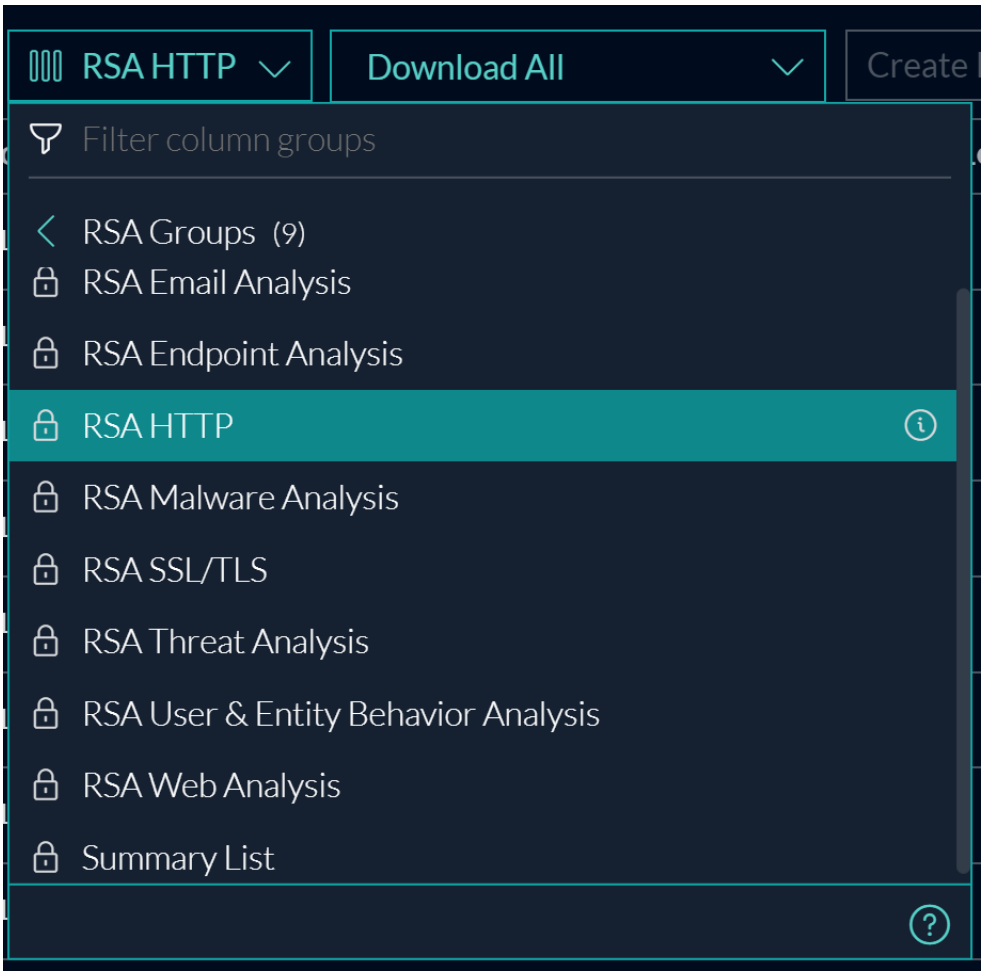


ここで、Concentratorサービスを選択し、Concentratorの詳細を最近表示していない場合は、次に示すように、時間範囲のドロップダウンに詳細が表示されません。



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。

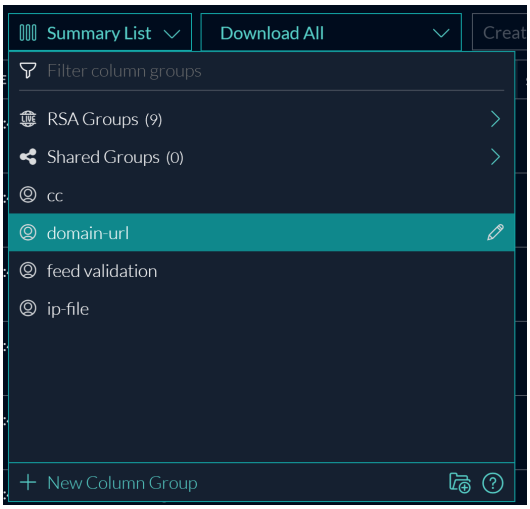


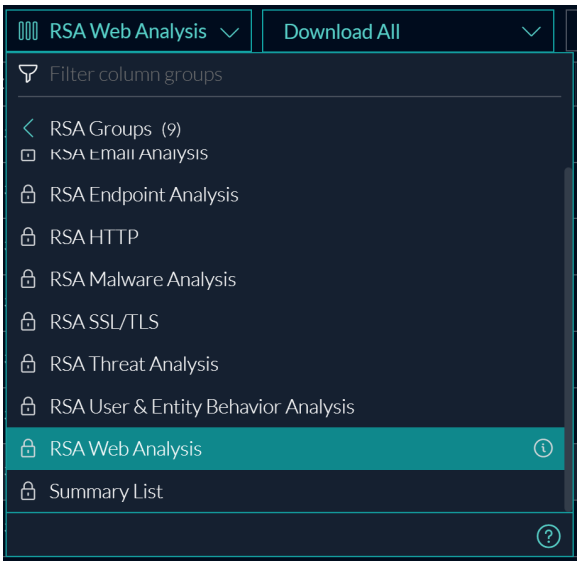
レガシー イベント ビューでは、組み込み列グループの名前の前に「RSA」が付きます。イベント ビューでは、名前の前にRSAが付き、グループはロック記号 ( ) でマークされます。これは、 [列グループ]メニューで選択した標準提供の列グループの例です。行の最後に情報アイコンが表示されます。



Live列グループ

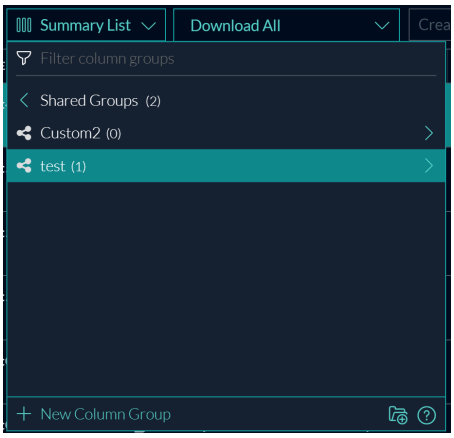
NetWitness Platformはライブからの調査コンテンツの展開をサポートしており、ライブ シンボル ( ) でマークされています。列グループは、RSAグループ(RSA Liveコンテンツおよび RSA OOTBグループ) と共有グループに分類されます。グループは、編集可能な共有グループを除いて、編集不可能なフォルダおよびサブフォルダとして表示されます。プライベート コンテンツはすべて、これらのグループの外部に表示されます。たとえば、次の画像は、共有グループ フォルダの下位にあるプライベート コンテンツを示しています。()内の数字はフォルダー内のコンテンツの数を示し、>記号はフォルダー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





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 したツールチップが表 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 レベルのフィルター フィールド ( ) に列 グループの名 前 を入 力 できます。



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。

カスタム列グループは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。これまでと同様に共有列グループを作成できるほか、プライベート列グループを作成することもできます。グループを作成するときに、共有するか非公開(デフォルト)にするかを選択できます。共有グループを非公開にしたり、非公開グループを共有グループに変更したり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。

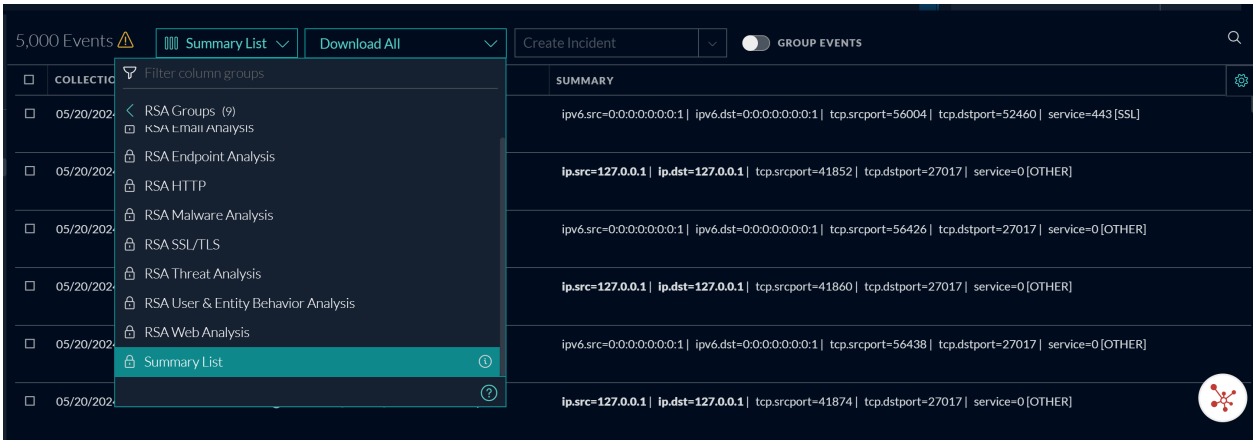
[列グループ]メニューでは、グループ タイプはアイコンで識別されます。これは、行の末尾に編集アイコンが表示されたカスタム列グループの例です。



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。

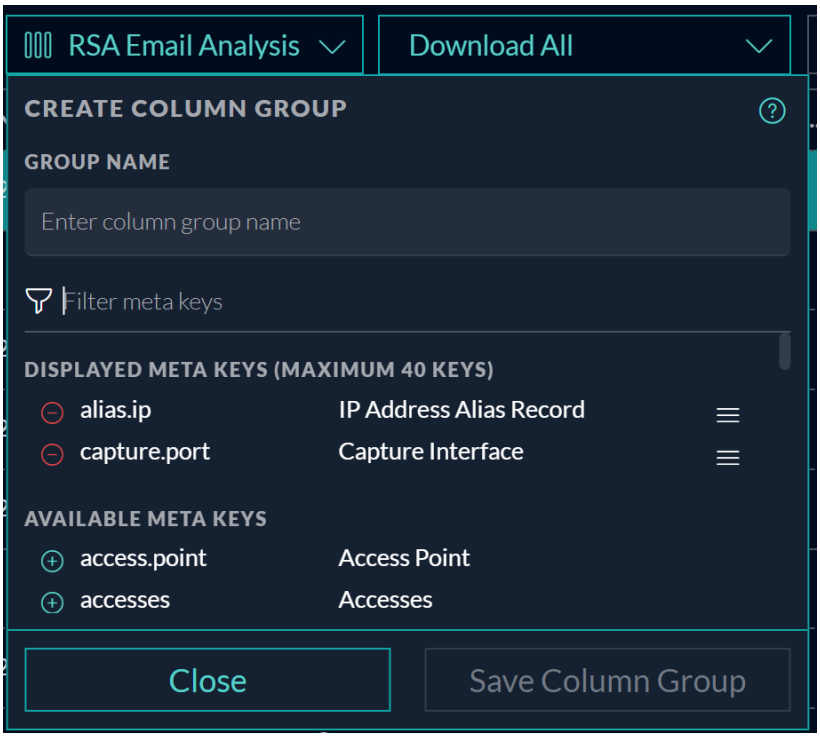
また、特 定 のフォルダを選 択 すると、選 択したフォルダの内 容 が表 示され、フィルタ フィールド が空 になり ます。フィルタ フィールドに戻 ると、最 後 に選 択したフォルダが表 示されます。次 の例 では、選 択された フォルダはその内 容 を含 むRSAグループであり、列 グループのドロップダウンにはフィルタ処 理 された要 約 リスト フォルダが表 示されます。

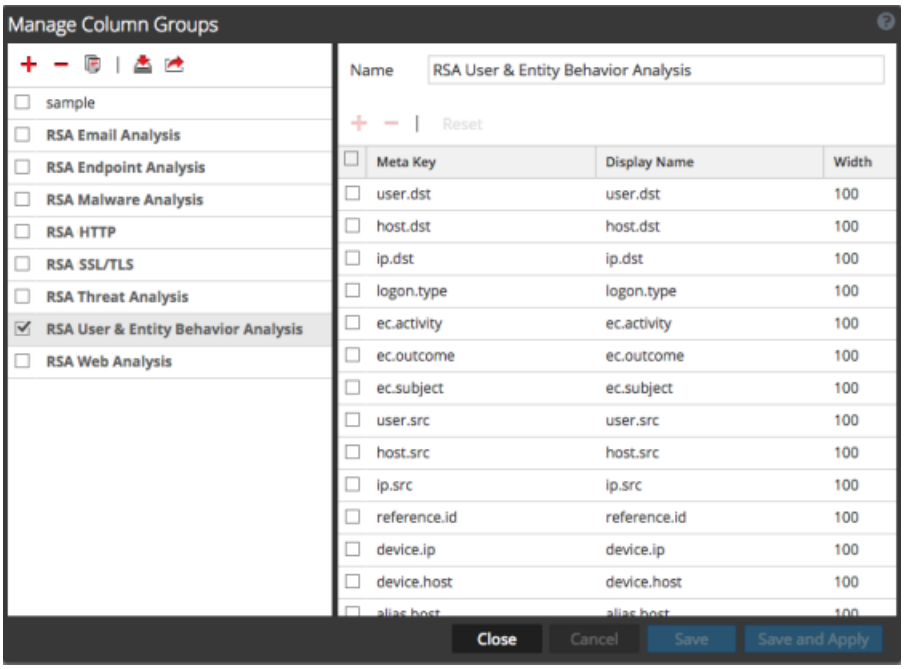




列 グループを管 理 するためのダイアログ

［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 とー 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。ダイアログには共 有 オプションが 含 まれています。





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

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

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

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

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

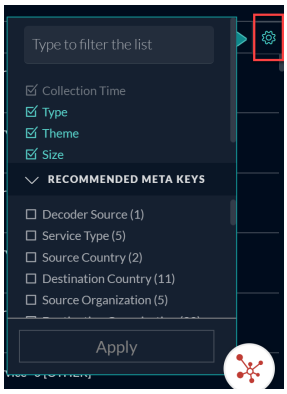
[イベント]ビューでの列と列グループの操作

最新バージョンにアップグレードした後は、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:管理者がブラックリスト(非表示)に登録しているメタ キーの列が列グループに含まれている場合、その列のデータは表示できません。この列は列セレクターで選択することができず、[イベント]パネルにも表示されません。

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



2. 列に追加したいメタ キーを選択するか、メタ キーの名前を入力します。
3. 列に表示しないメタ キーを選択解除します。
   選択した列を使用してデータが再表示されます。
4. イベント リストの列の幅を変更するには、列のタイトルの上にカーソルを合わせて、列の境界線を右または左にドラッグします。
5. イベント リストの列の配置を変更するには、列のタイトルの上にカーソルを合わせ、列を右または左にドラッグします。
   イベント リストで行った変更は、現在のセッション中は有効ですが、列グループの一部としては保存されません。列グループを次回適用したときには、元の構成と列の順序が適用されます。

[イベント]パネルでイベントをソートするための列の選択

注 :接続されているすべてのサービスが12.5以降に更新されている場合、結果の読み込みが完了した後、イベント パネルでイベントを並べ替えることができます。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。

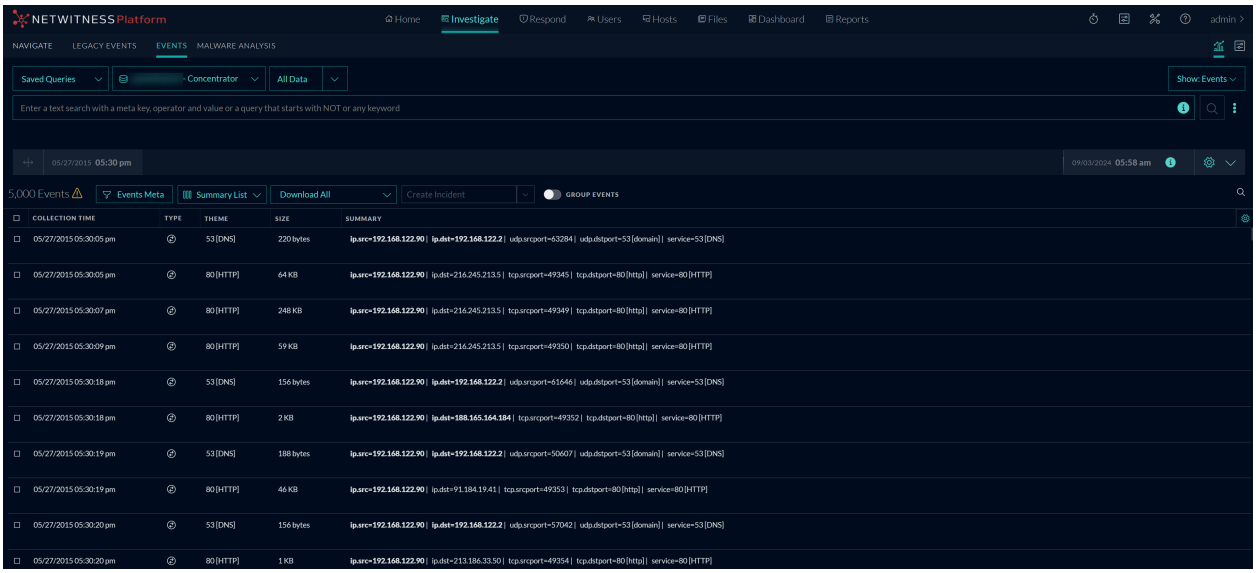
[イベント]パネルのイベント リストの順序は、イベント内のメタ キーの値によって変更できます。各列のタイトルはメタ キーを表し、表示されているイベントのメタ キーに値があれば、列に読み込まれます。イベント パネル内のイベントは、イベント設定ダイアログで選択した方法を使用して並べ替えられます。(昇順または降順)でソートされます。並べ替え方法が選択されていない場合、デフォルトの順序は昇順になります([イベント]ビューの構成 を参照)。イベント パネル内のイベントは、イベント設定ダイアログで並べ替え設定が昇順または降順のいずれかに選択されている場合にのみ並べ替えられます。 [イベント環境設定]でソー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。

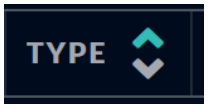
列による並べ替え

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。



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。

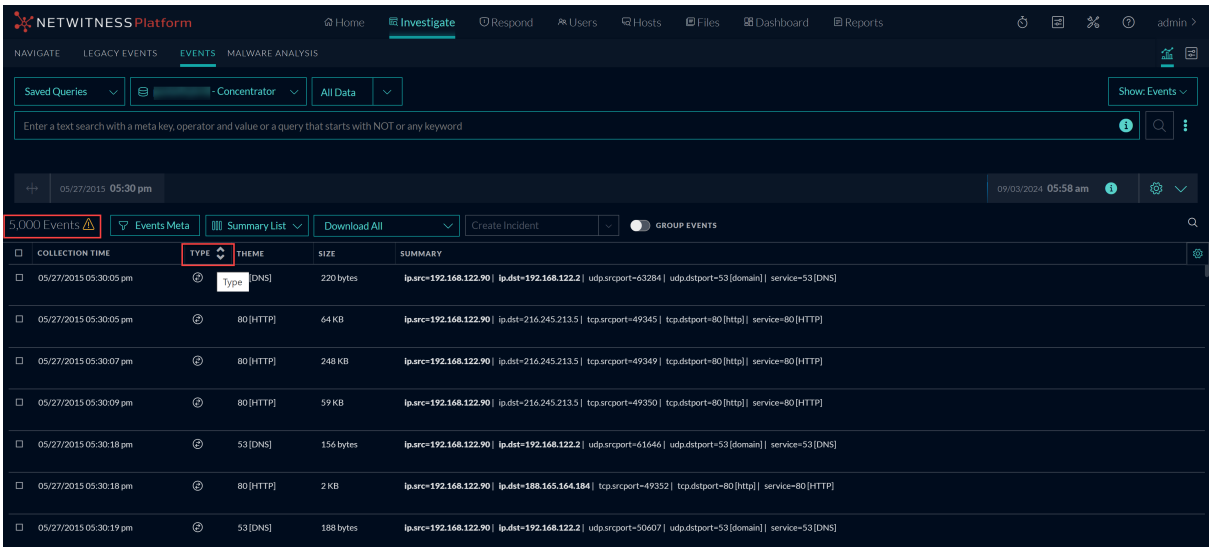
表示された結果の数が、管理者によって設定されたイベント数の上限よりも少ない場合、列のソートは、クエリを再実行することなくクライアント側で実行されます。結果の数がイベント数の上限を超過したために表示されない結果が存在する場合は、新しいソート順で、同じサービス、時間範囲、フィルタを使用して新しいクエリが送信されます。現在の結果が削除され、スピナーに進行状況が示されます。［キャンセル］ボタンが使用可能になり、再構築が終了し、進行状況がクエリコンソールに表示されます。

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

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

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



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

   b. 青色の矢印をクリックすると、ソートなしの状態に戻ります。

列による並べ替え

マウスを列タイトルの上に移動すると、並べ替え可能な列には、列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示されます。 [キャンセル]ボタンが使用可能になり、再構築が終了し、進行状況がクエリコンソールに表示されます。

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

ソート順またはソート列を変更するには、次の手順を実行します。

1. 列のタイトルの上にマウスを移動すると、ソート可能な列を見つけることができます。
   列がソート可能でない場合は、その理由を説明するツールチップが表示されます。
2. リストを列でソートするには、次の手順を実行します。

   a. ソート可能な列にマウスを移動し、矢印( または )をクリックします。
   イベントが正しいソート順でソートされます。列のタイトルの上にカーソルを合わせると、矢印の色がグレーでなくなったことを確認できます。イベント リストのソートに使用されている列には、明るい白色の矢印が表示され、これをクリックしてソートの方向を変更できます。

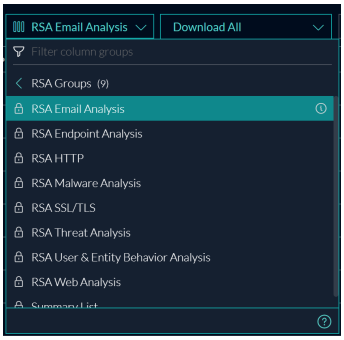
   b. ソート順を変更するには、  をクリックして昇順に変更するか、  をクリックして降順に変更します。
   矢印の方向が変わり、選択した順序でイベントが再ロードされます。

列グループに含まれているメタ キーの表示

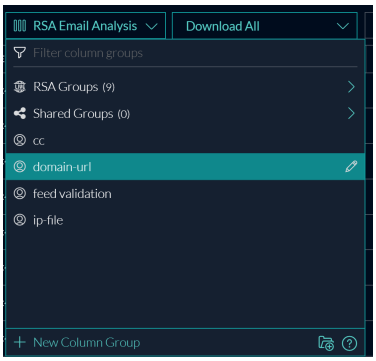
列グループの詳細を表示するには、次の手順を実行します。

1. [**調査**] > [**イベント**]に移動し、  をクリックしてイベントをロードします。
   デフォルト サービスとデフォルトの時間範囲のイベントが [イベント]パネルにロードされます。 [Summary List]列グループまたは前回のセッションで使用していた列グループがリストに適用されます。
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

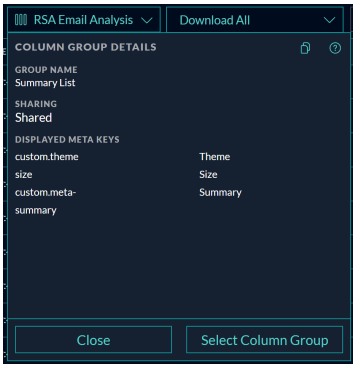
す。次の図は、概要リストがデフォルトで選択され、すべての種類の列グループが表示されているときのメニューの初期状態を示しています。。



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。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。



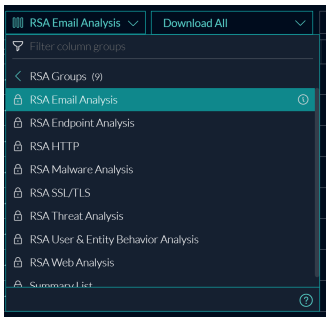
4. グループに含まれている列を確認するには、 [**Summary List**] グループの上にカーソルを合わせて情報アイコン( ) をクリックします。
次の図は、 [Summary List] の列を示しています。Collection TimeとTypeの2つは常にイベント リストの先頭の2列に表示されますが、 [列グループの詳細] ダイアログには表示されません。



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. [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。

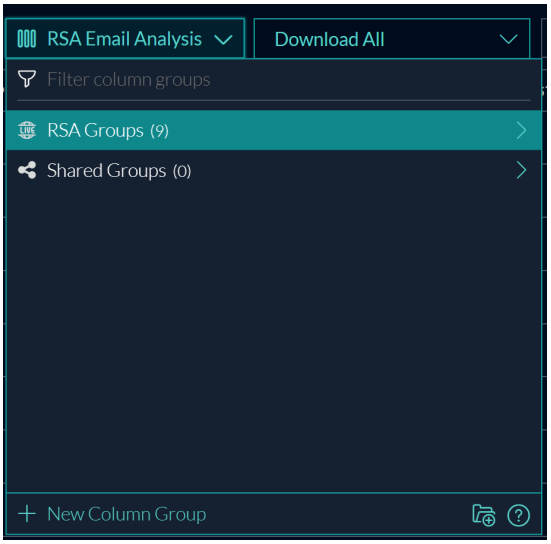


2. 次のいずれかの操作を実行します。
   a. ハイライト表示されているグループを適用するには、**ENTER**を押します。
   b. 特定の種類のグループのみを表示する場合は、表示オプション([**プライベート**]、 [**共有**]、 [**RSA**]) を使用して1つまたは2つのグループ タイプを非表示にします。
   c. 列グループ名を検索するには、最初に [**列グループの絞り込み**]フィールドにテキストを入力します。入力すると、リストが絞り込まれて、その文字列が名前に含まれる列グループのみが表示されます。
      適用するグループが表示されたら、グループをクリックするか、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、**ENTER**キーを押します。
      [イベント]リストの表示が更新され、選択した列グループに含まれる列のみが表示され、選択したグループ名がメニューのタイトルに表示されます。この選択は、 [イベント]ビューから移動した後も保持されます。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。

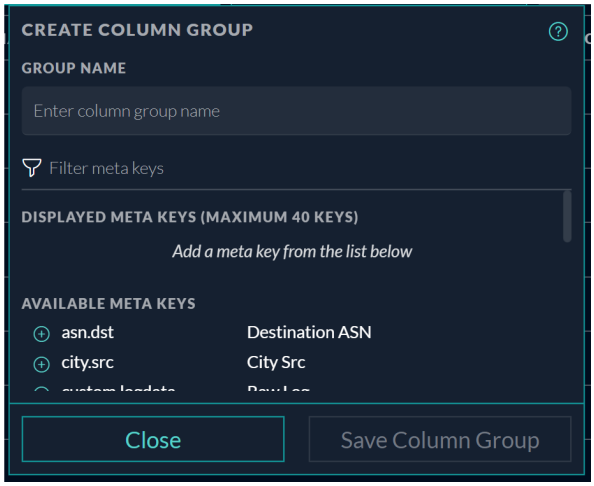
> **注** :列グループ内のメタ キーが、選択したサービスでサポートされない場合、それらのメタ キーは [イベント メタ]パネルまたは [イベント]パネルには表示されません。

カスタムの列 グループの作 成

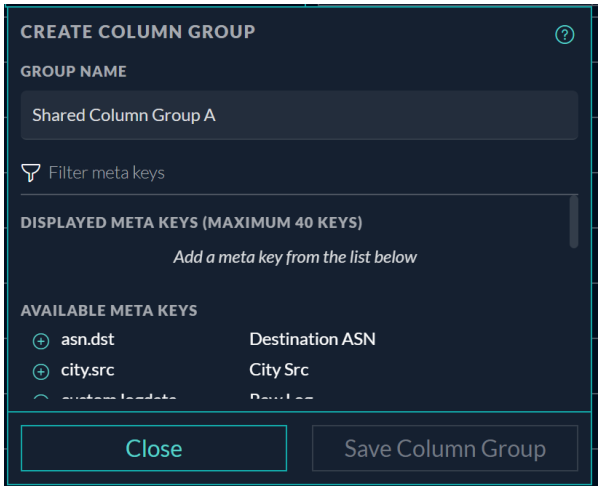
1. **調 査**] > [**イベント**]に移 動して、クエリを送 信し、 [イベント]パネルにデータをロードします。
2. [イベント]パネルのツールバーで、 [**列 グループ**]メニュー タイト ルをクリックします。
メニューがド ロップダウンし、列 グループのリスト が表 示されます。 [表 示オプションと列 グループの絞り込み]フィールド がー 番 上 に、 [+ **新しい列 グループ**]オプションがー 番 下 に表 示されます。



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

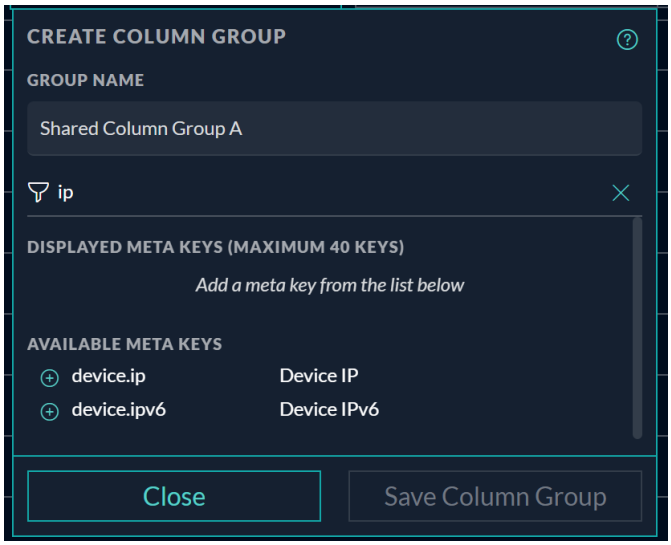


4. [**グループ名**]フィールドに、新しい列グループの一意の名前(最大256文字)を入力します(たとえば「**Custom Column Group A**」)。



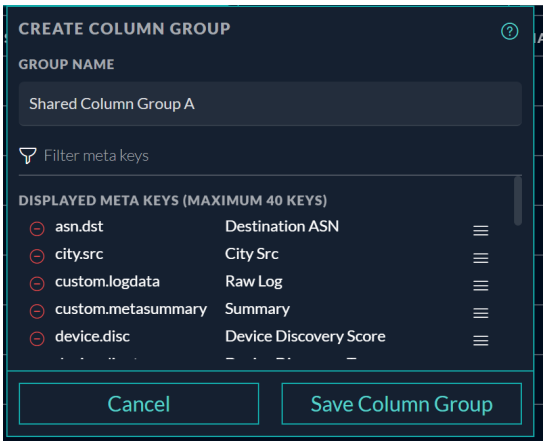
5. 列グループにメタ キーを追加するには、次のように各メタ キーを選択して追加します。

   a. [**メタ キーの絞り込み**]フィールドにテキスト文字列を入力すると、そのテキストを含んでいるメタ キーが [**選択可能なメタ キー**]リストに表示されます。



   b. 追加したいメタ 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。



6. (オプション) 列グループ内のメタ キーを検索して削除するには、 [**メタ キーの絞り込み**]フィールドにテキスト文字列を入力し、そのテキストを含んでいるメタ キーを [**表示するメタ キー**]リストから検索します。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。
7. (オプション) [表示するメタ キー]リストでメタ キーの表示順を変更するには、リストの順序アイコン( ) の上にカーソルを置きます。カーソルがドラッグ アンド ドロップ アイコン( ) に変わったら、リスト内でメタ キーを上下にドラッグします。
8. 次のいずれか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。
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。

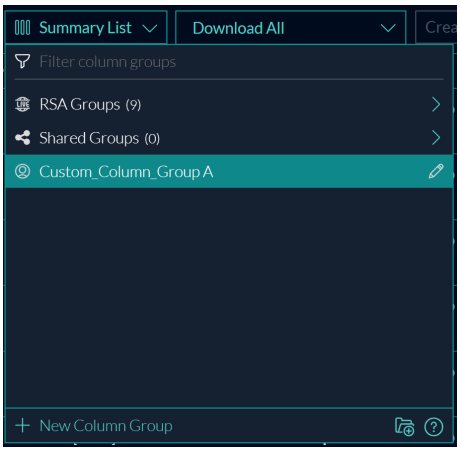
カスタム列グループの削除

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。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または共有列グループを削除すると、その影響はグローバルになり、どのアナリストもそのグループを使用できなくなります。

カスタムの列グループを削除するには

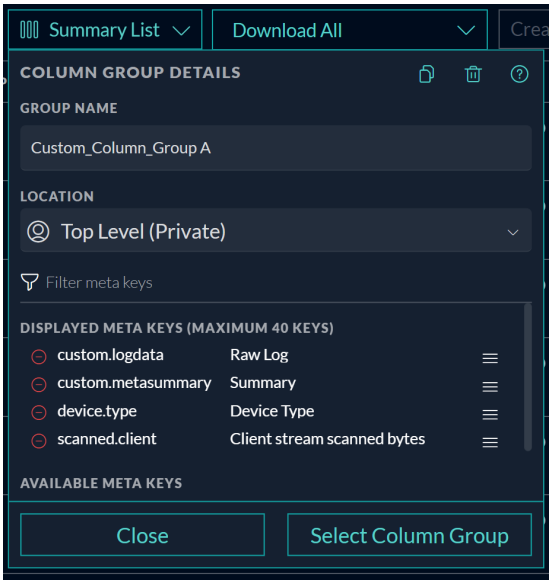
1. **調査**] > [**イベント**]に移動し、  をクリックしてイベントをロードします。
   デフォルト サービスとデフォルトの時間範囲のイベントが、[イベント]パネルにロードされます。
   [Summary List]列グループまたは前回のセッションで使用していた列グループがリストに適用されます。次の図は、[Summary List]列グループが選択されている初期状態のビューを示しています。
   [列グループ]メニューのラベルに、選択した列グループの名前が表示されます。



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



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



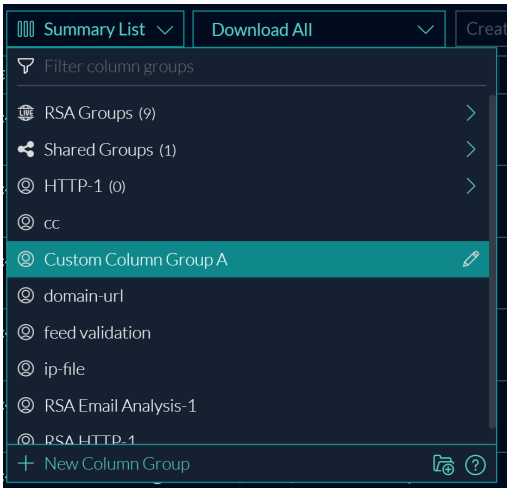
4. グループの削除アイコン()をクリックします。
   列グループが現在有効になっている場合は、次のメッセージが表示されます。`This column group cannot be deleted because it is currently active.`
   確認メッセージが表示され、削除を確認またはキャンセルすることができます。「**キャンセル**」または

「列グループの削除」をクリックします。
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

編集用に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。

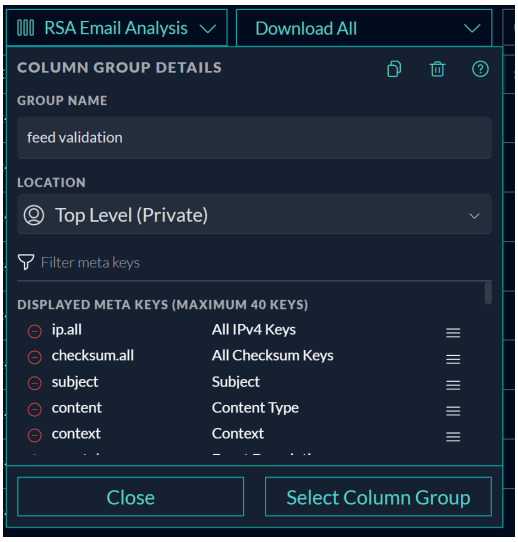


3. 編集する列グループをハイライト表示します。次の図では、カスタム列グループがハイライト表示され、右側に編集アイコンが表示されています。

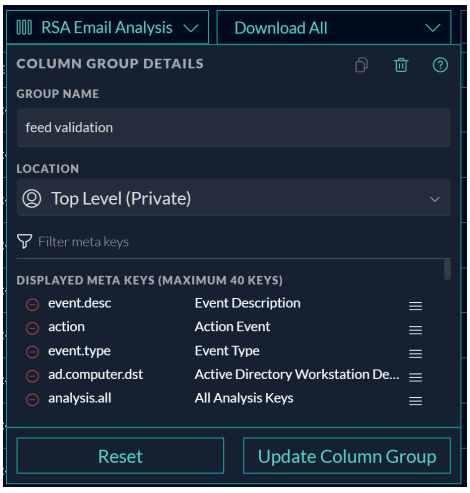


4. 編集アイコン( ) をクリックします。
[列グループの詳細]ダイアログが表示され、グループ名と表示するメタ キーを編集できるようになり

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feed validationに変更され、`ad.computer.dst`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、**「列グループの選択」**をクリックします。
   列グループが更新され、「列グループの選択」をクリックした場合は、イベント リストが更新され、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を作成する

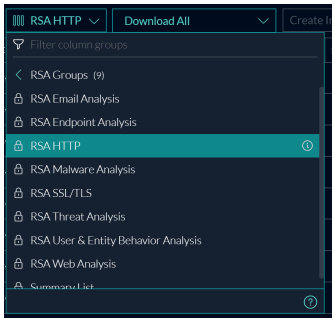
未保存の編集が進行中でない限り、標準提供またはカスタム、共有またはプライベートのいずれかにかかわらず、任意の列グループをコピーできます。この機能は、標準提供グループのカスタマイズされたバージョンが必要な場合に便利です。また、カスタム グループをプライベートから共有に、または共有からプライベートに変更することはできないため、コピーを作成することで、別の共有設定を選択できるようになります。列グループのコピーを作成すると、同じ名前が使用され、番号が付記されます。たとえば、RSA HTTPをコピーすると、最初のコピーの名前はRSA HTTP-1になり、同じグループの2番目のコピーの名前はRSA HTTP-2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

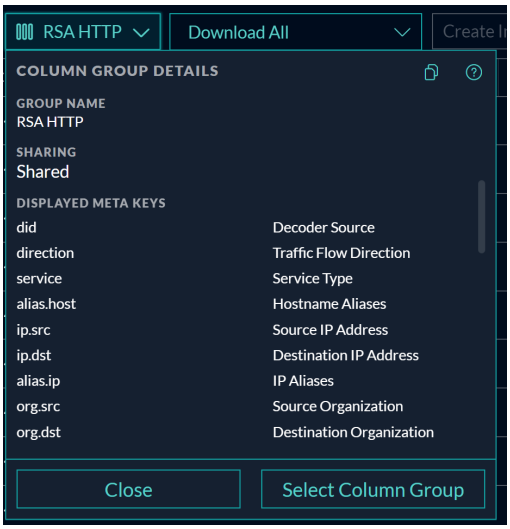
3. コピーする列グループをハイライト表示します。この図は、RSA HTTPがハイライト表示されていることを示しています。情報アイコン( ) が右側に表示されます。



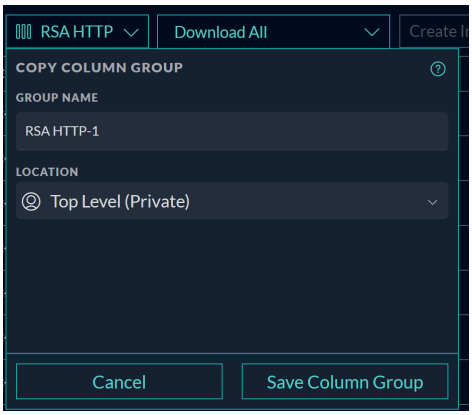
4. 次のいずれかを実行します。

   a. 情報アイコン( ) をクリックします。

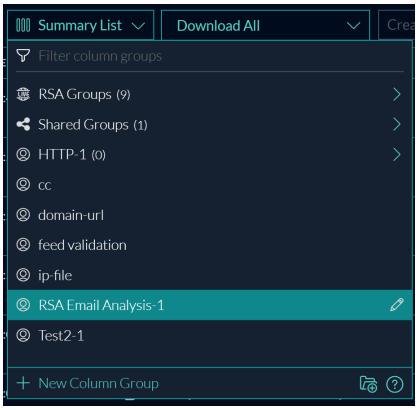
   b. 編集アイコン( ) をクリックします。
   [列グループの詳細]ダイアログが表示されます。この図は、標準提供グループのダイアログを示しています。



5. コピーアイコン( )をクリックします。
   -nが付加された列グループ名を含む[列グループのコピー]ダイアログが表示されます。次の図が-1になっているのは、この列グループの1つ目のコピーであるためです。



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。
10. 次のいずれかを実行します。
    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 グループを選択」**をクリックします。
    グループがメタ グループ メニューに追加されます。下の図には、RSA Email Analysisメタ グループのプライベート コピーがあります。



列グループ フォルダの作成

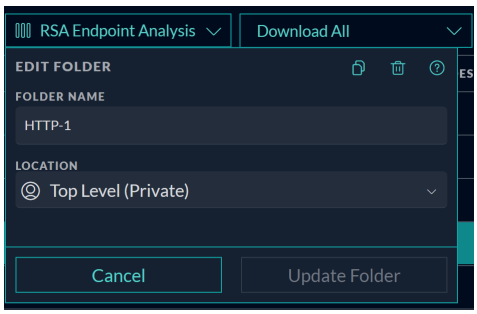
現在のレベルに存在し、プライベート フォルダまたは共有フォルダとして追加されるカスタム列グループ フォルダを作成できます。また、フォルダ名がすでに存在する場合は、一意の名前を入力するように求められます。

1. イベント ビューでイベント メタ 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、共有フォルダーをプライベート フォルダーに移動することはできません。またその逆も同様です。

1. [イベント]ビューで [イベント メタ]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。
   フォルダー編集ダイアログが表示されます。

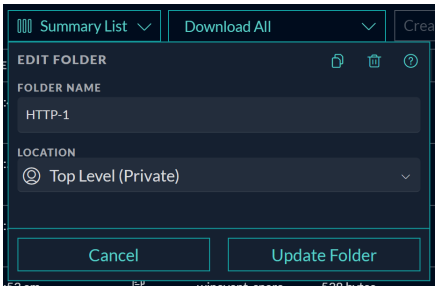


3. [**フォルダ名**]フィールドに、列グループ フォルダの一意の名前を入力します。
4. 編集するフォルダの場所を選択します。
5. [**フォルダの更新**]をクリックします。

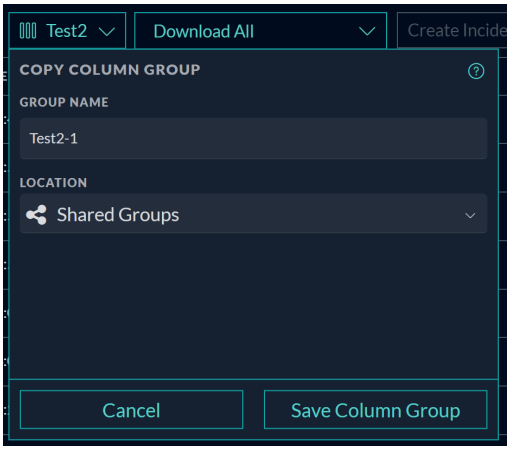
列グループ フォルダのコピー

列グループ フォルダー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 メタ 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。



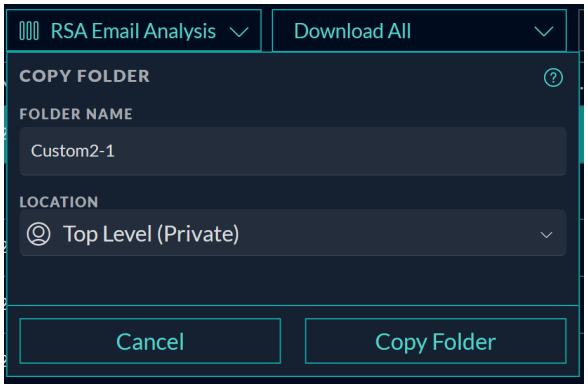
4. [**フォルダ名**] フィールドに、新しいメタ グループ フォルダの一意の名前を入力します。
5. 編集するフォルダの場所を選択します。
6. [**フォルダのコピー**] をクリックします。

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 メタ 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。

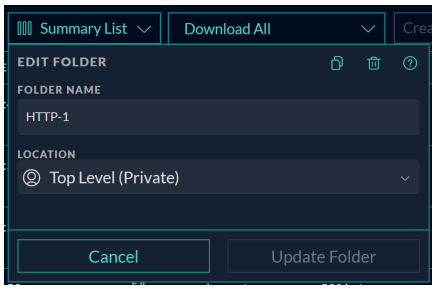


4. コピーするフォルダの場所を選択します。
5. [**フォルダのコピー**]をクリックします。
   フォルダがフォルダの元の名前で作成され、最後に「copy」が追加されます。

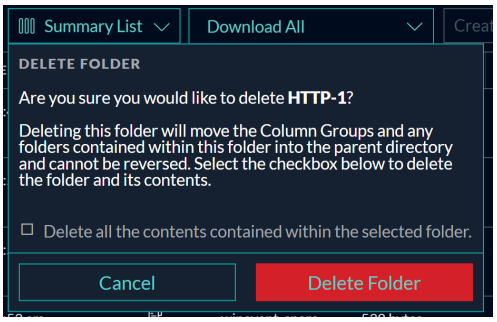
列グループ フォルダの削除

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 メタ 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. 削 除 するには、**「フォルダの削 除 」**をクリックします。

[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、レガシー イベント ビューで作 業 するための手 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。

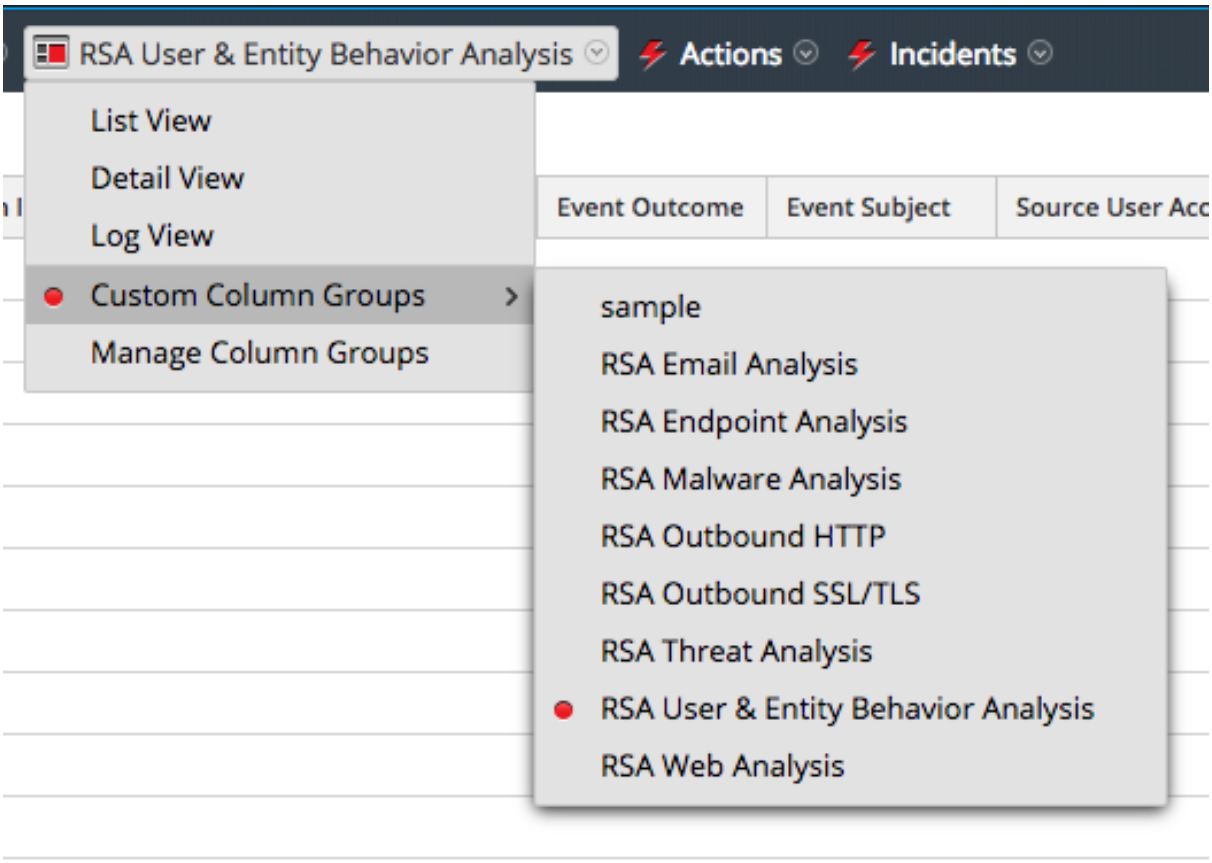
列 グループは、調 査 の中 で、グローバルに共 有 され、サービスごとに定 義 されます。カスタムの列 グループに対して行った変 更 はすべてグローバルに適 用 され、サービスを使 用 しているすべてのアナリストに影 響 します。列 グループを削 除 すると、サービスを調 査 するすべてのアナリストがその列 グループを使 用 できなくなります。

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。

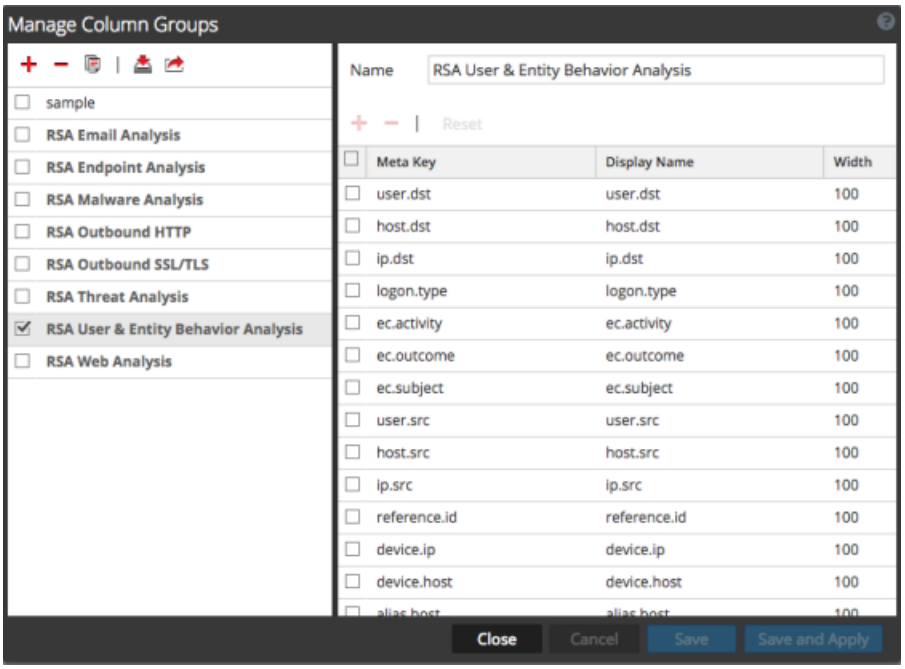


2. サブメニューから列グループのいずれかを選択します。
   [レガシー イベント]ビューが更新され、カスタム列グループが反映されます。

[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。

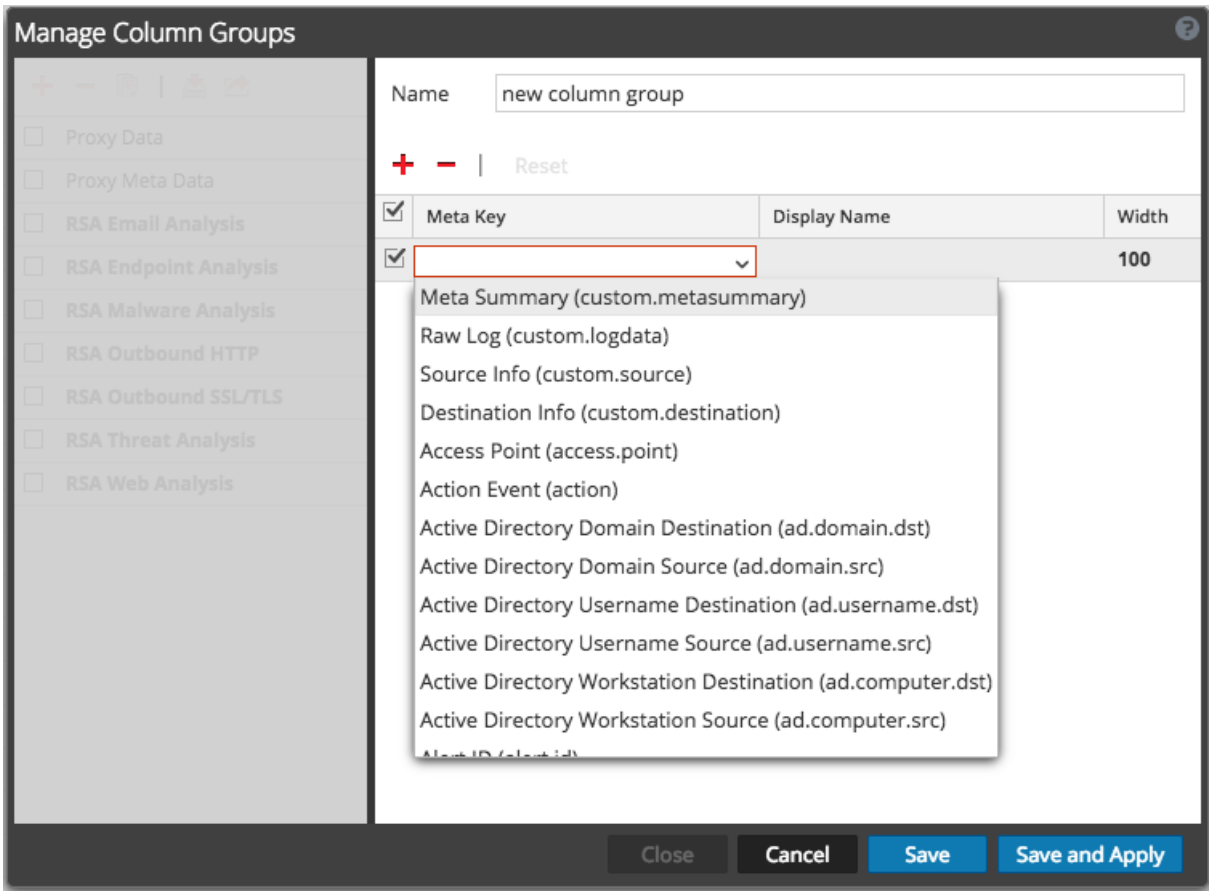
[列グループの管理]ダイアログが表示されます。



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

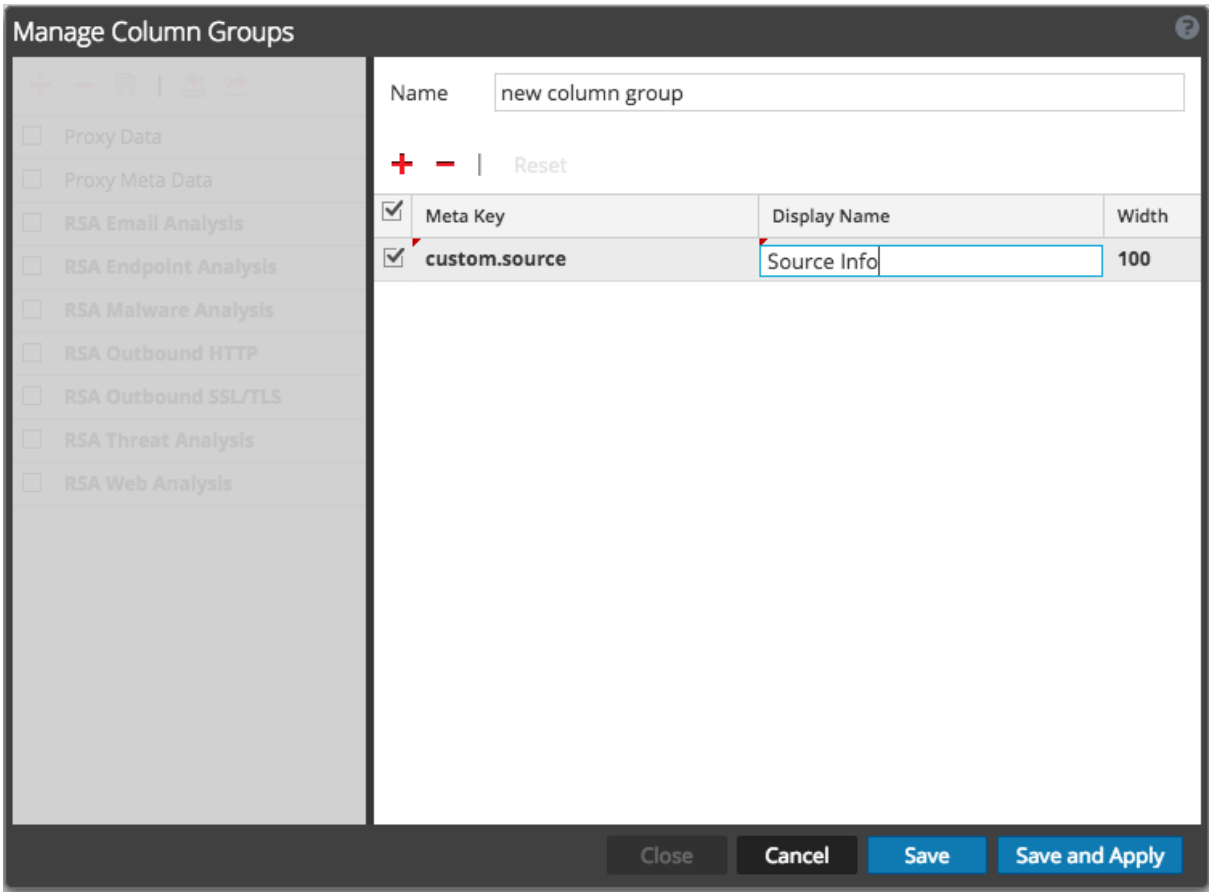
4. グループに列を追加するには、＋をクリックします。追加された空の [**メタ キー**]フィールドをクリックし、 [**メタ キー**]ドロップダウン リストを表示します。リストからメタ キー フィールドを選択します。この

手順を、列セットが完成するまで繰り返します。



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

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

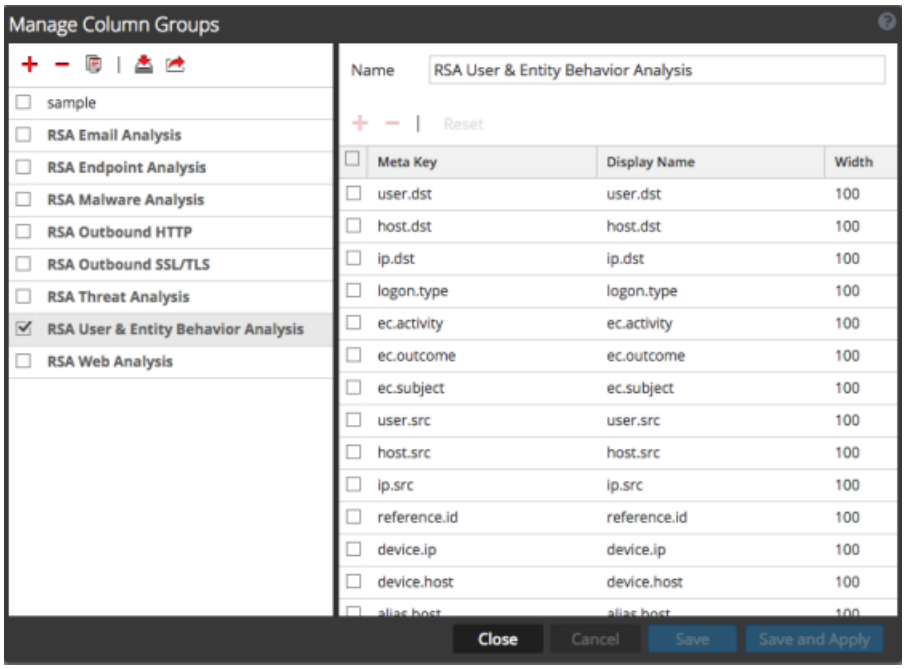


8. (オプション) 列グループを以前の設定に復元し、これまでに加えた変更をすべて取り消すには、[**キャンセル**]をクリックします。
9. 保存する準備ができたら、次のいずれかの操作を実行します。
   a. 編集した列グループを保存し、その列グループの設定を使って [レガシー イベント]ビューを更新するには、 [**保存して適用**]をクリックします。
   b. [レガシー イベント]ビューを更新せずに、編集した列グループを保存するには、 [**保存**]をクリックします。

列グループの削除([レガシー イベント]ビュー)

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

[列グループの管理]ダイアログが表示されます。

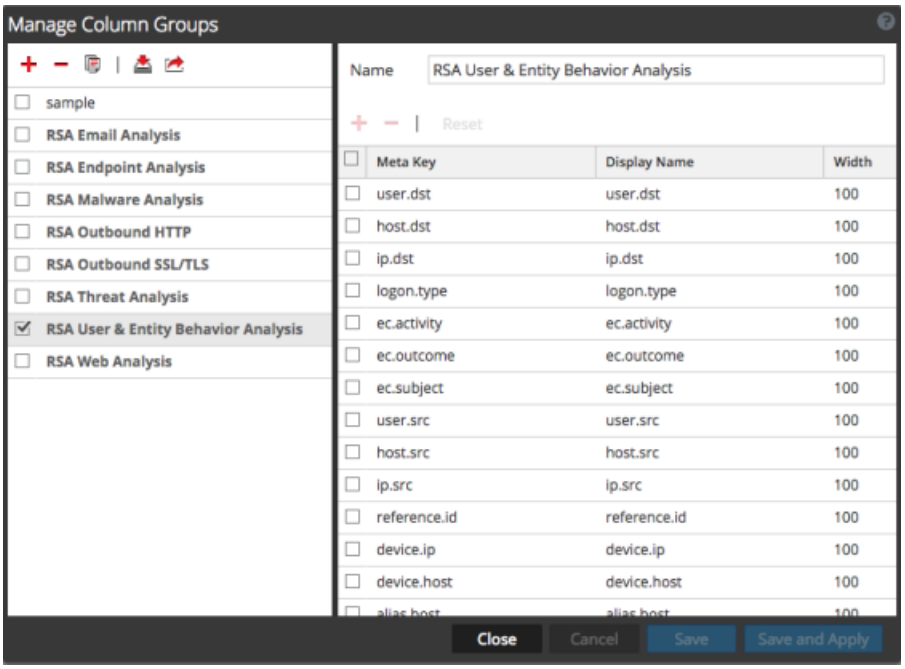


3. 列グループ パネルでカスタム列グループを削除するには、1つまたは複数のカスタム列グループを選択し、ツールバーの－をクリックします。
   確認を求めるメッセージが表示されます。
4. 次のいずれかの操作を実行します。
   a. 列グループを削除して[レガシー イベント]ビューを更新するには、[**はい**]をクリックします。
   b. 列グループを削除しない場合は、[**いいえ**]をクリックします。
      選択した列グループが削除され、どこにも表示されなくなります。

列グループの編集([イベント]ビュー)

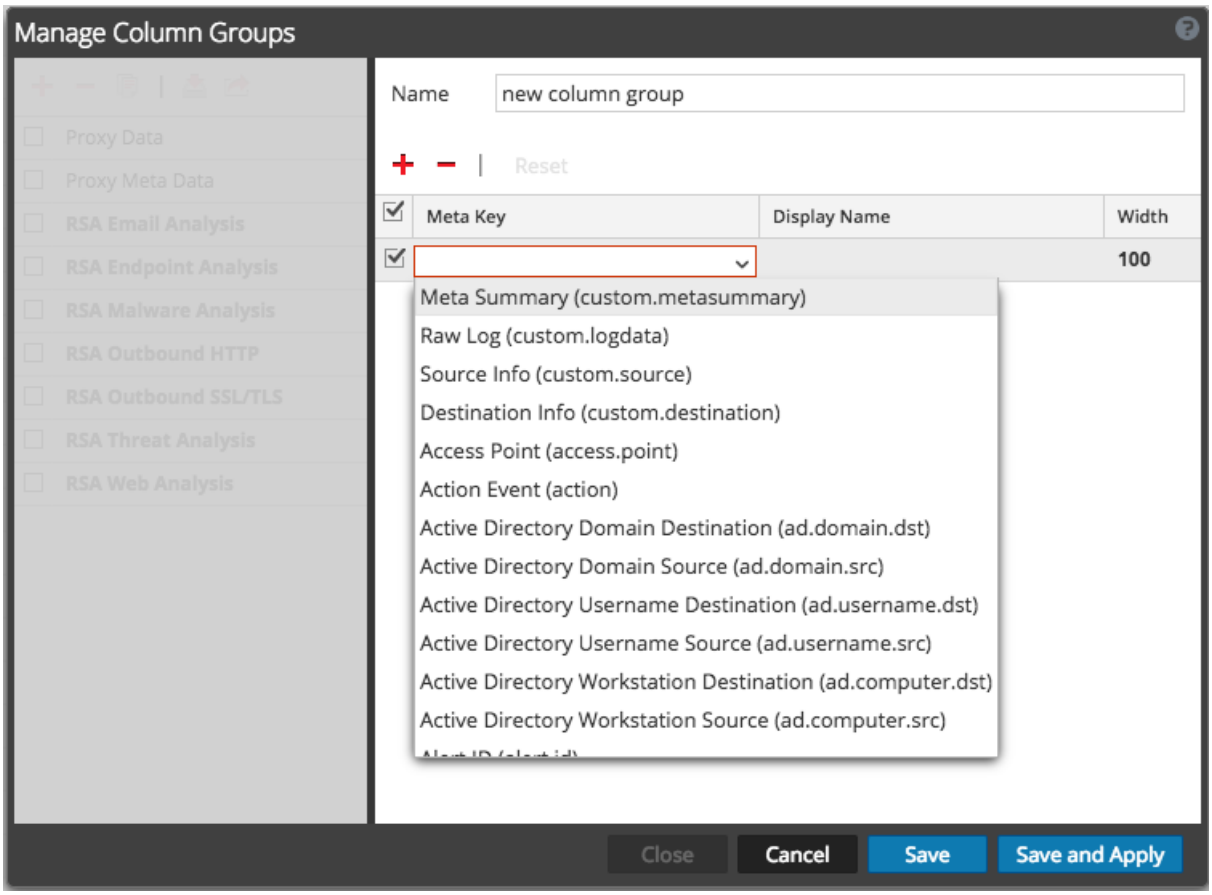
1. [**調査**] > [**レガシー イベント**]に移動します。
2. [**ビュー**]ドロップダウン メニューから[**列グループの管理**]を選択します。[ビュー]ドロップダウン メニューのラベルには、現在選択中のオプション(詳細ビュー、リスト ビュー、ログ ビュー、現在選択されている列グループ名など)が表示されます。

[列グループの管理]ダイアログが表示されます。



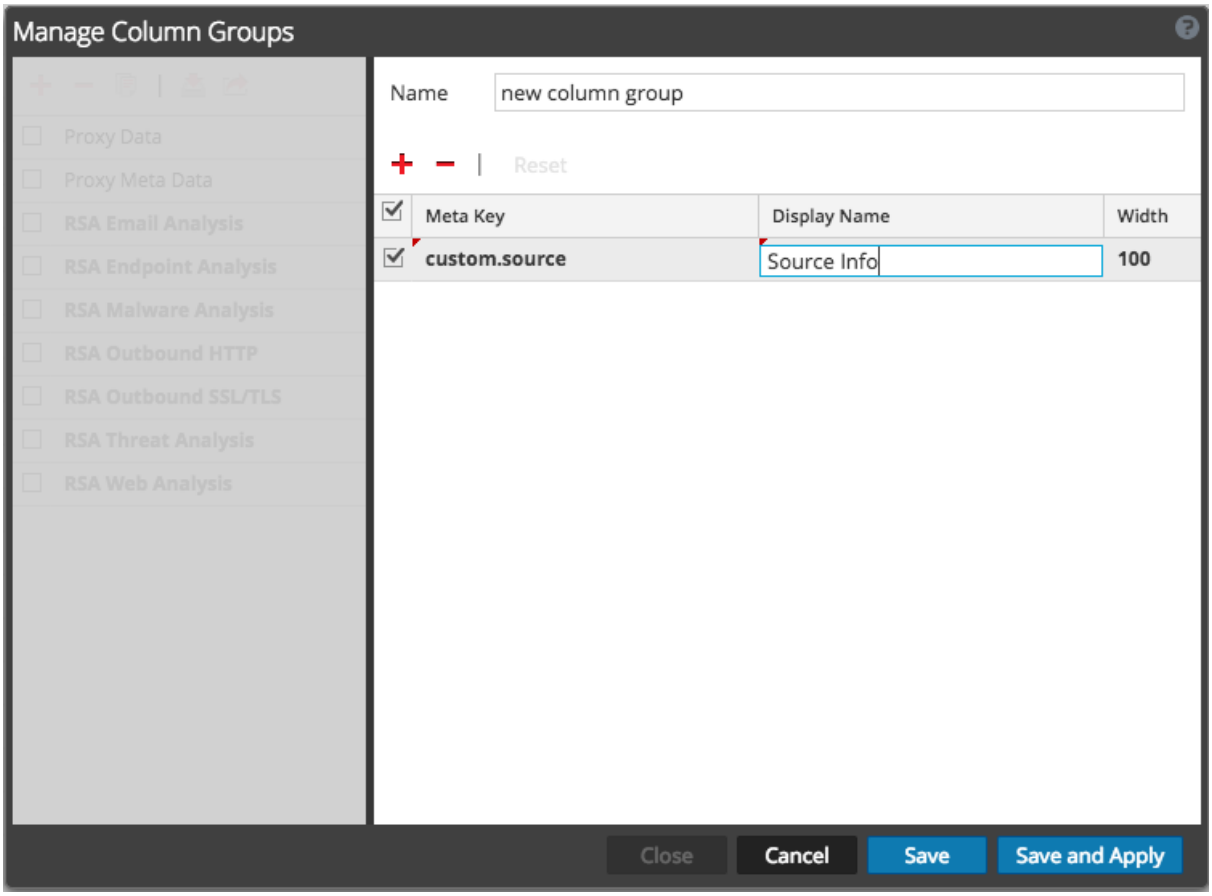
3. 次のいずれかの操作を実行します。
   a. 列グループ パネルでカスタム列グループを編集するには、名前の前にあるチェックボックスを選択します。
      列定義パネルが右側に表示されます。
   b. 標準提供の列グループまたはカスタムの列グループを複製してから編集するには、名前の前にあるチェックボックスを選択して、複製アイコン( ) をクリックします。
      列定義パネルが右側に表示されます。
4. (オプション) グループの複製を編集している場合は、グループの新しい名前を入力します。
5. グループに列を追加するには、 をクリックします。追加された空の [**メタ キー**]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

手順を、列セットが完成するまで繰り返します。



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

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



9. (オプション) 列グループを以前の設定に復元し、これまでに加えた変更をすべて取り消すには、[**キャンセル**]をクリックします。

10. 保存する準備ができたら、次のいずれかの操作を実行します。

    a. 編集した列グループを保存し、その列グループの設定を使って [レガシー イベント]ビューを更新するには、 [**保存して適用**]をクリックします。

    b. [レガシー イベント]ビューを更新せずに、編集した列グループを保存するには、 [**保存**]をクリックします。

列グループのインポートとエクスポート([レガシー イベント]ビュー)

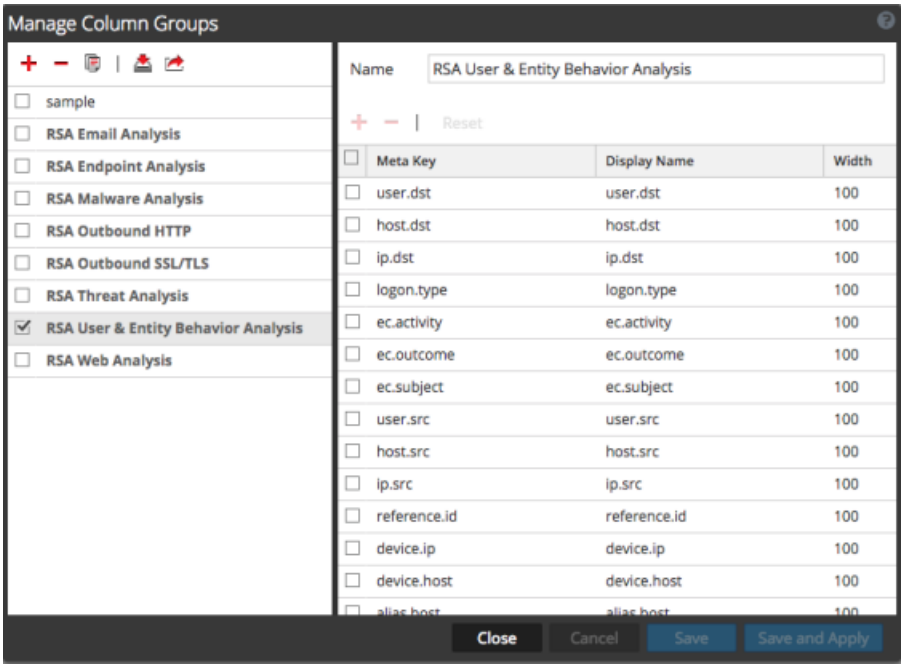
カスタムの列グループをエクスポートして他のチーム メンバーと共有できます。エクスポートしたファイルのコピーを他のアナリストに提供すれば、そのアナリストは列グループをインポートできます。

列グループをエクスポートするには

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

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

[列グループの管理]ダイアログが表示されます。



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

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

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

保存済みクエリを使用した調査の共通領域のカプセル化

保存済みクエリを使用すると、[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できます。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の保存済みクエリは、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。

保存済みクエリはそれぞれ、メタ グループや列グループを指定しており、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ることもあります。

保存済みクエリには次のような特徴があります。

- 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)。
- 保存済みクエリを有効にすると、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)。

標準提供の保存済みクエリ

標準提供クエリ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、コピーを編集することができます。[ナビゲート]ビューでは、標準提供クエリ名は「RSA」で始まり、[デフォルト クエリ]の下に表示されます。[イベント]ビューでは、保存済みクエリのグループ化はサポートされていません。次の図は、[保存済みクエリ]メニューに表示された標準提供クエリの例です。



NetWitness Platformには、次のような標準提供クエリがあります。

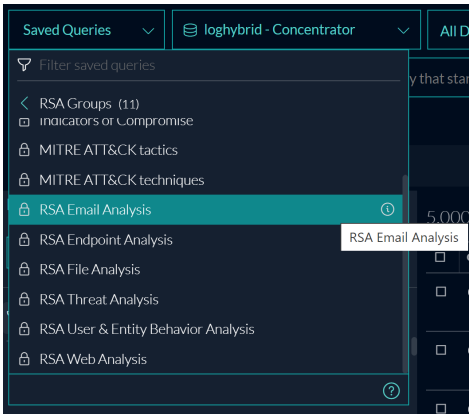
- RSA Email Analysis
- RSA Endpoint Analysis
- RSA File Analysis
- RSA Threat Analysis
- RSA User & Entity Behavior Analysis
- RSA Web Analysis
- Behaviors of Compromise
- Enablers of Compromise
- Indicators of Compromise

- MITRE ATT&CK tactics
- MITRE ATT&CK techniques

標準提供の保存済みクエリを使用すると、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クエリを選択すると、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、独自のカスタム保存済みクエリを作成できます。

Live保存済みクエリ

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、保存済みクエリ グループのドロップダウンの下にLive記号( ) でマークされて表示されます。保存済みクエリは、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。



カスタム保存済みクエリ

カスタムの保存済みクエリは、組織内でグローバルに共有されます。共有の保存済みクエリは以前と同様に作成できるほか、プライベートの保存済みクエリも作成することができます。共有のカスタム保存済みクエリを編集すると、その変更はグローバルに適用されます。共有のカスタム保存済みクエリ プロファイルを削除すると、そのクエリは削除され、すべてのアナリストが使用できなくなります。

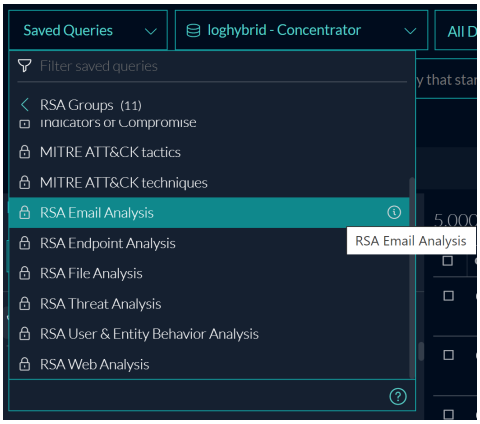
注 :スプリングボード パネルで保存済みクエリがフィルタとして使用されている場合、そのプロファイルを編集することはできますが、[**イベント**]ビューで削除することはできません。ただし、[ナビゲート]ビューまたは [レガシー イベント]ビューでは、プロファイルの削除を妨げるものはありません。この場合、削除された保存済みクエリをフィルタとして使用するスプリングボード パネルは引き続き機能しますが、フィルタが削除され、予期しない結果がパネルに表示されることがあります。詳細については、『NetWitness Platformスタート ガイド』の「スプリングボードの管理」を参照してください。

保存済みクエリを作成する際には、共有するかプライベート(デフォルト)にするかを選択できます。共有の保存済みクエリをプライベートに変更したり、プライベートの保存済みクエリを共有に変更したりすることはできません。プライベート保存済みクエリは、［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。［保存済みクエリ］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、［保存済みクエリ］メニューに表示される共有およびプライベートのカスタム保存済みクエリの例です。行の末尾には編集アイコンが表示されます。

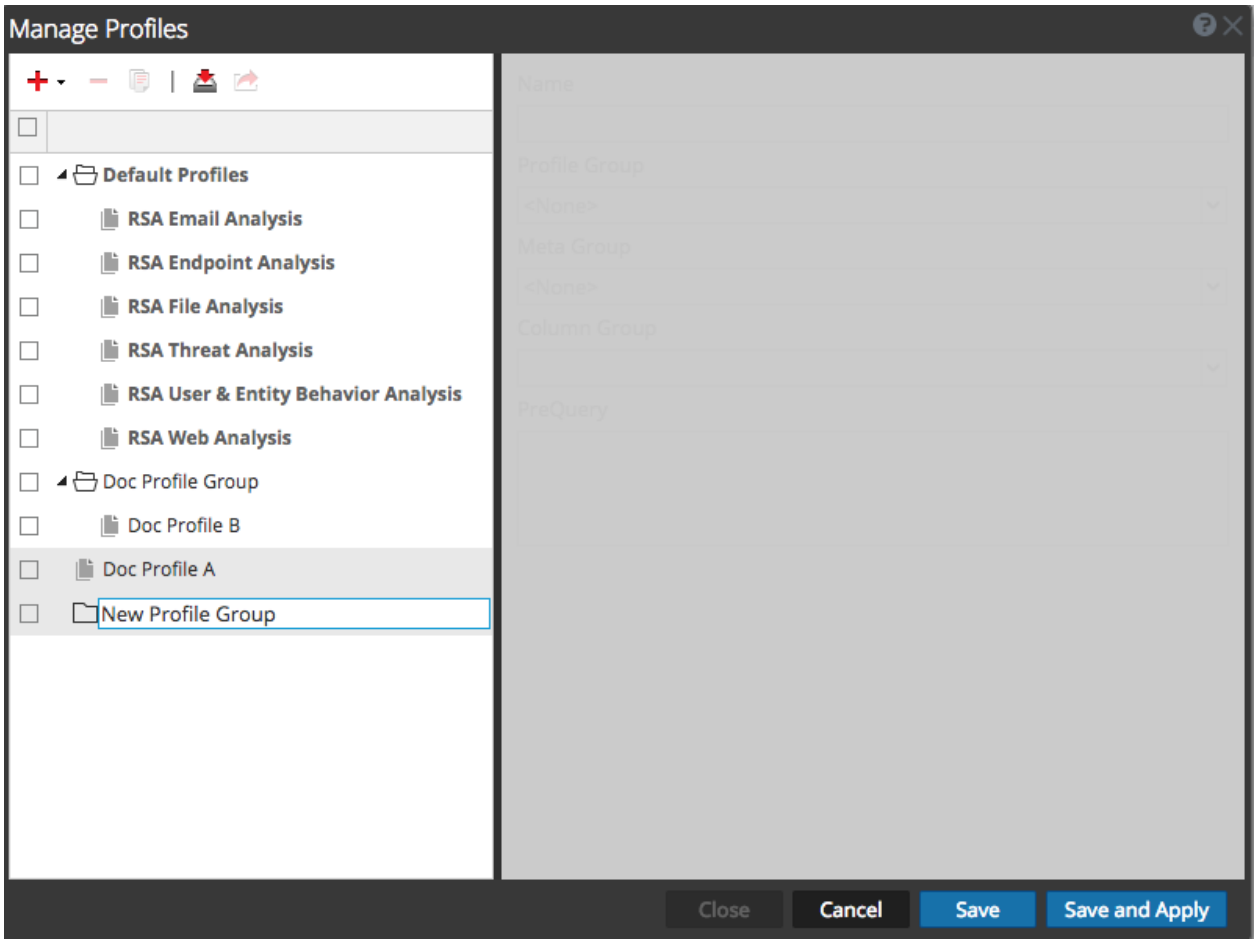


保存済みクエリを管理するためのダイアログ

［保存済みクエリ］メニューには、保存済みクエリ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。保存済みクエリ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12.5イベント ビューの [保存されたクエリ] 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］ビューで使用できるものと同じクエリが一覧表示されます。プロファイルの作成、コピー、編集、削除、適用が可能です。



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、およびイベント ビューで使 用できます。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を操 作します。 **[ナビゲート]** または **[レガシー イベント]** ビュー ツールバーで、 **[プロファイル]** > **[プロファイルの管 理]** を選択して、[プロファイルの管 理] ダイアログを開きます。カスタム プロファイルはグローバルに共 有できるようになりましたが、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。

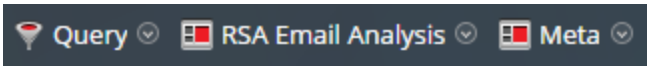
クエリ プロファイル メニュー (イベント ビュー) から:

- 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。
- [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。これにより、メタ グループを使 用したり、以 前 から使 用 可 能だった共 有カスタム クエリ プロファイルに加 えて、プライベート カスタム クエリ プロファイルを作 成したりできるようになります。

- [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 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。以前のバージョンから最新バージョンにアップグレードする場合、プロファイルを含むプロファイル 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、プレクエリー条件が適用され、[プロファイル]メニューのラベルがクエリー プロファイル名に置き換えられます。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」クエリー プロファイルが選択された状態を示しています。

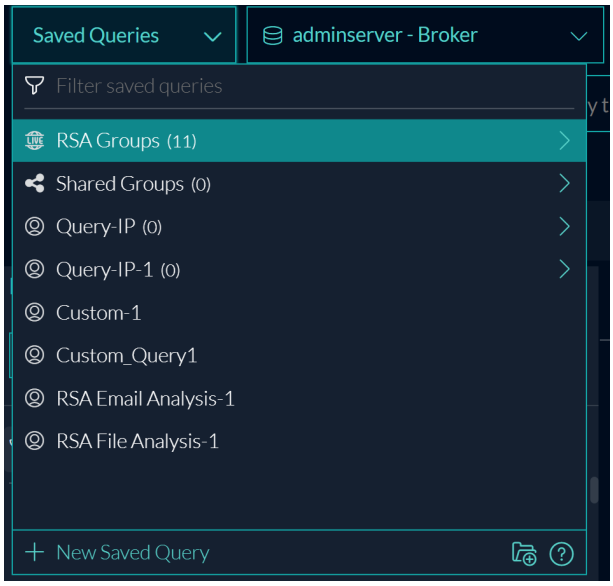


保存済みクエリの詳細の表示([イベント]ビュー)

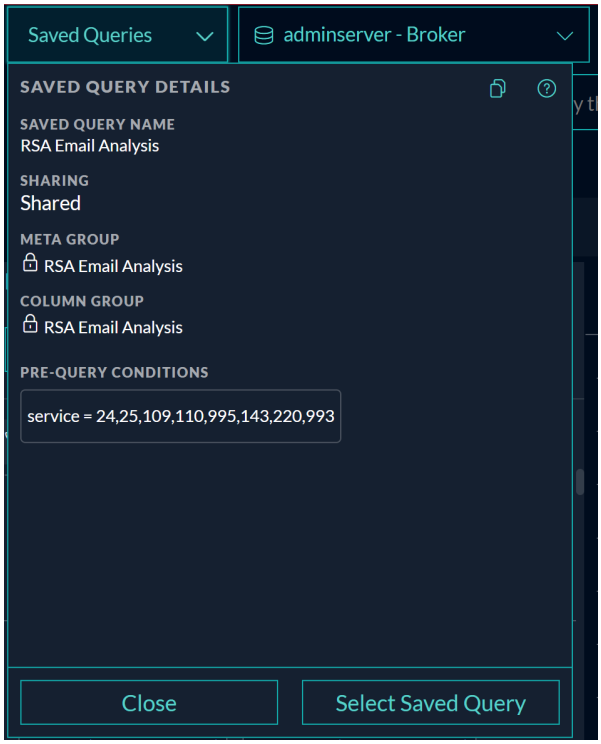
保存済みクエリにどのメタ グループ、列グループ、制限フィルタ(プレクエリ条件) が定義されているかを確認するには、プロファイルの詳細を表示します。

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 [**保存済みクエリ**]をクリックします。
   [保存済みクエリ]メニューが開き、使用可能なクエリのリストが表示されます。このメニューには、標準提供の保存済みクエリ(RSA) 、共有のカスタム保存済みクエリ、プライベートのカスタム保存済みクエリの一覧が表示されるため、絞り込みフィールドを使用して特定のクエリを簡単に見つけることができます。



2. リスト内の保存済みクエリにカーソルを合わせ、情報アイコン( ) をクリックして、クエリに構成されたメタ グループ、列グループ、プレクエリー条件を表示します。
次の図は、標準提供の保存済みクエリの1つであるRSA Email Analysisプロファイルの詳細を示しています。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) は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。

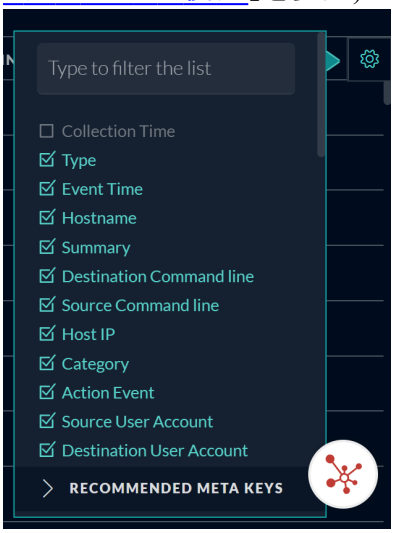
   a. ダイアログを閉じるには、 **閉じる**]をクリックします。

   b. プロファイルを適用する場合は、 **保存済みクエリを選択**]をクリックします。
   ダイアログが閉じます。選択した保存済みクエリが反映され、 [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)。

保存済みクエリの適用([イベント]ビュー)

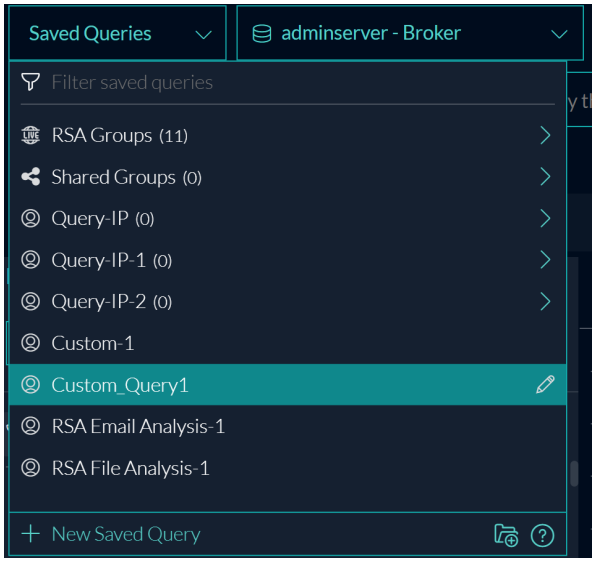
保存済みクエリが適用されても、 [保存済みクエリ]メニューにそのことは表示されませんが、列グループまたはメタグループが有効であるかどうかは確認できます。プレクエリ条件が適用されている場合は、次の図に示すように、クエリバーの先頭にフィルタが表示されます。



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、適用されたクエリ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。

保存済みクエリを適用するには、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 [保存済みクエリ]をクリックします。
   [保存済みクエリ]メニューが開き、使用可能な保存済みクエリのリストが表示されます。

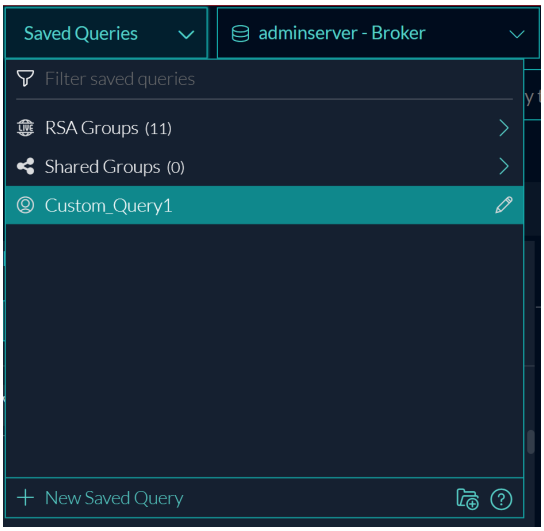


2. 上下矢印キーまたはマウスを使用して、保存済みクエリをハイライト表示します。
3. ハイライト表示されたクエリをクリックします。
   保存済みクエリの設定がただちに適用されます。選択したクエリが反映され、[イベント]リストの表示が更新されます。クエリで別の列グループが使用されている場合は、選択されたクエリのプレクエリ条件と列グループを使用してクエリが再実行されます。プレクエリ条件のみが異なる場合は、クエリ バーの既存のフィルタが削除され、プレクエリ条件がクエリ バーに追加されます。 ボタンがアクティブになり、新しいプレクエリ条件を使用してクエリを再送信できるようになります。クエリを再送信する前または後に、通常どおりに他のフィルタを追加できます。

カスタム保存済みクエリの作成または編集([イベント]ビュー)

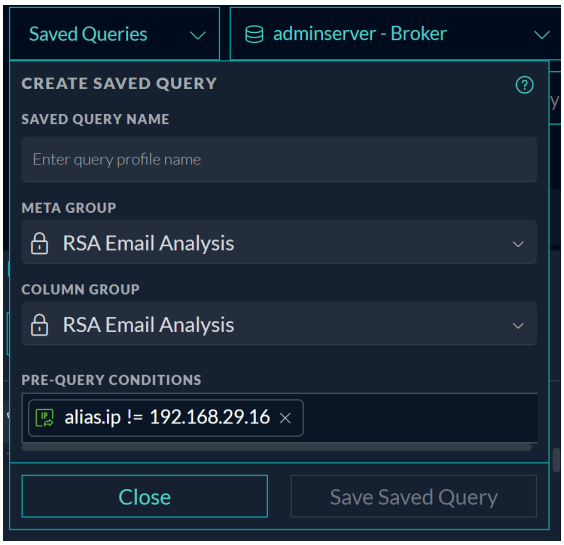
カスタム保存済みクエリを作成または編集するには

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



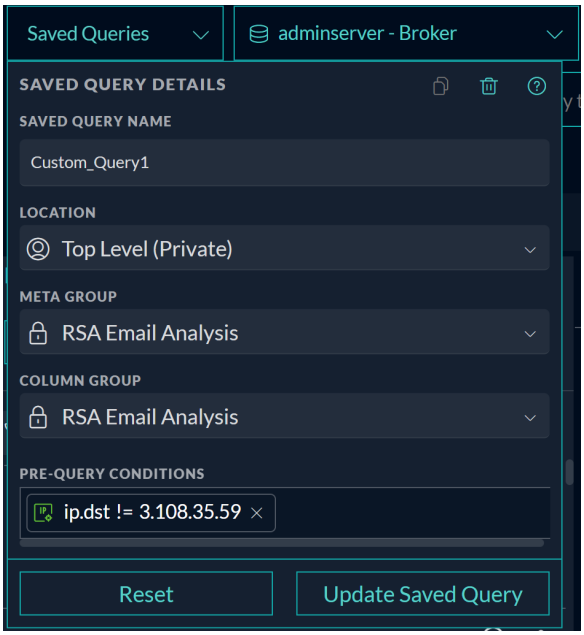
2. 次のいずれかの操作を実行します。

   a. 新しい保存済みクエリを作成するには、 [+ **新しい保存済みクエリ**]をクリックします。
   [保存済みクエリの作成]ダイアログが表示されます。 [保存済みクエリの作成]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クエリが表示されます。



   b. 既存の保存済みクエリを編集するには、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。

[保存済みクエリの詳細]ダイアログが表示されます。



3. **[保存済みクエリ名]**フィールドに、80文字以下の一意のクエリ名を入力します。
[保存済みクエリの作成]ダイアログの [保存済みクエリの保存]ボタンがアクティブになります。
4. 次のいずれかの操作を実行します。
   a. 新しい保存済みクエリを組織内で共有する場合は、ドロップダウン メニューで **[場所]**を [共有グループ]に設定します。保存済みクエリは作成後に、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保存済みクエリを作成するには、 **[場所]**を [最上位(プライベート)]のままにしておきます。保存済みクエリは作成後に、プライベートから共有に変更することはできません。
5. **[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。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。グループ名の前にあるアイコンで、プライベートと共有が区別されます。
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. **[保存済みクエリを保存]**または **[保存済みクエリを更新]**をクリックします。
新しい保存済みクエリが保存されるか、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。

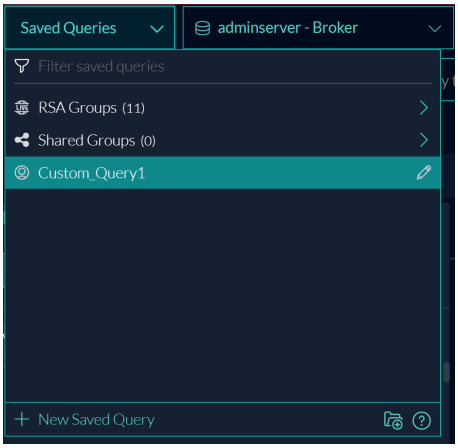
カスタム保存済みクエリの削除([イベント]ビュー)

標準提供の保存済みクエリは読み取り専用であり、削除することはできませんが、カスタム保存済みクエリは削除できます。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。共有保存済みクエリ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。

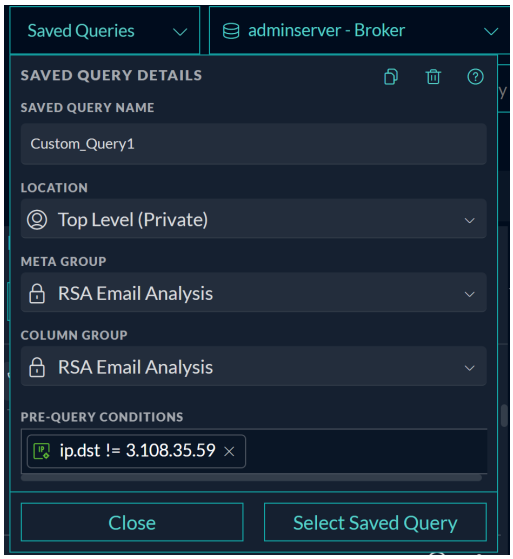
注 :スプリングボード パネルで保存済みクエリがフィルタとして使用されている場合、そのクエリ プロファイルを編集することはできますが、 [イベント]ビューで削除することはできません。ただし、 [ナビゲート]ビューまたは [レガシー イベント]ビューでは、プロファイルの削除を妨げるものはありません。この場合、削除された保存済みクエリ プロファイルをフィルタとして使用するスプリングボード パネルは引き続き機能しますが、フィルタが削除され、予期しない結果がパネルに表示されることがあります。詳細については、『NetWitness Platformスタート ガイド』の「スプリングボードの管理」を参照して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

カスタム保存済みクエリを削除するには

1. **[調査]** > **[イベント]**に移動し、クエリ バーの **[保存済みクエリ]**をクリックします。
   [保存済みクエリ]メニューが開き、使用可能なクエリのリストが表示されます。



2. 削除するカスタム保存済みクエリをハイライト表示して、編集() アイコンをクリックします。
   [保存済みクエリの詳細]ダイアログが表示されます。



3. 削除アイコン( ) をクリックします。
   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 [**保存済みクエリの削除**] をクリックします。
   保存済みクエリが削除され、 [保存済みクエリ] 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。

保存済みクエリのコピー

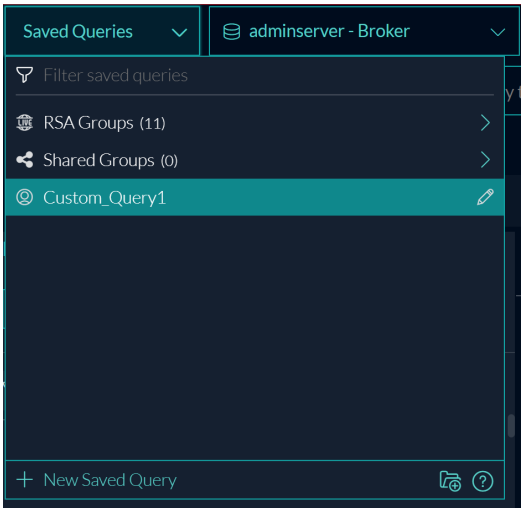
未保存の編集が進行中でない限り、標準提供またはカスタム、共有またはプライベートのいずれかにかかわらず、任意の保存済みクエリをコピーできます。この機能は、標準提供プロファイルのカスタマイズされたバージョンが必要な場合に便利です。また、カスタム プロファイルをプライベートから共有に、または共有からプライベートに変更することはできないため、コピーを作成することで、別の共有設定を選択できるようになります。プロファイルをコピーすると、同じ名前が使用され、番号が付記されます。たとえば、RSA Email Analysisをコピーした場合、最初のコピーはRSA Email Analysis-1という名前になり、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。

保存済みクエリ プロファイルをコピーするには

1. [**調査**] > [**イベント**] に移動し、クエリ バーの [**保存済みクエリ**] をクリックします。
   [保存済みクエリ] メニューが開き、使用可能なクエリのリストが表示されます。

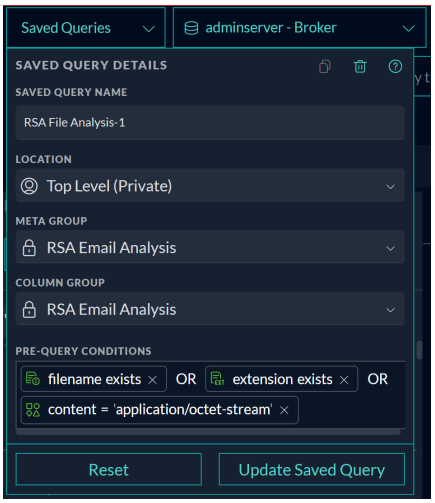
2. コピーする保存済みクエリをハイライト表示します。この図では、Custom_Query1が強調表示されています。情報アイコン( ) が右側に表示されます。



3. 次のいずれかの操作を実行します。

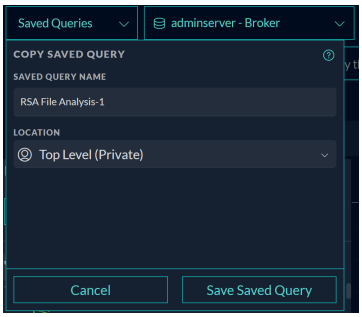
   a. 情報アイコン( ) をクリックします。

   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。
   [保存済みクエリの詳細]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。
   [保存済みクエリのコピー]ダイアログが開き、クエリ名に番号が付記されて、すべての保存済みクエ

リ間で一意の名前が作成されます。

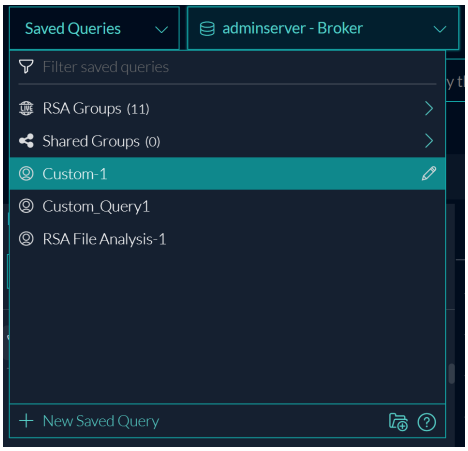


5. (オプション) [**保存済みクエリ名**]フィールドで、保存済みクエリの名前を編集します。
6. 新しい保存済みクエリを組織内で共有する場合は、ドロップダウン メニューで [**場所**]を [共有グループ]に設定します。デフォルトでは、新しい保存済みクエリはプライベートになります。コピー対象のプロファイルにプライベート列グループまたはメタ グループがある場合は、共有コピーが作成され、クエリのコピーで使用されます。
7. 次のいずれかの操作を実行します。
   a. 保存済みクエリをコピーせずにダイアログを閉じるには、 [**キャンセル**]をクリックします。
   b. 保存済みクエリのクローンを保存するには、 [**保存済みクエリの保存**]をクリックします。
   クローンが保存され、クローン クエリの [保存済みクエリの詳細]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保存済みクエリを選択するには、 [**保存済みクエリの選択**]をクリックします。
   [保存済みクエリ]メニューにクローンが追加されます。

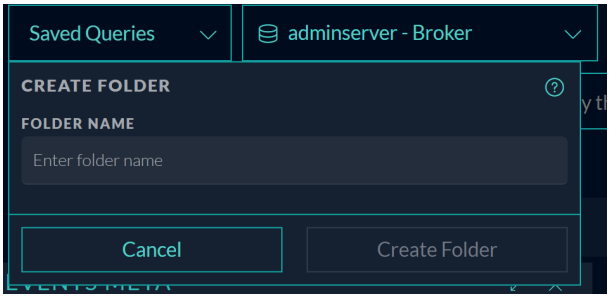
保存済みクエリ フォルダの作成

保存済みクエリ用のフォルダを作成できます。このフォルダは最上位に配置され、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、 [保存済みクエリ]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 [保存済みクエリの絞り込み]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。

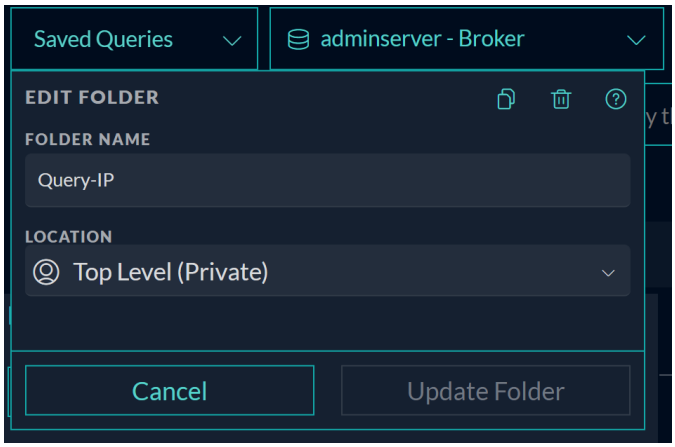


3. [**フォルダ名**]フィールドに、新しい保存済みクエリ グループ フォルダの一意の名前を入力します。
4. [**フォルダの作成**]をクリックします。

保存済みクエリ フォルダの編集と移動

保存済みクエリ グループ フォルダは、作成した後に編集または移動することができますが、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 [保存済みクエリ]メニューのタイトルを選択します。
2. をクリックします。
フォルダー編集ダイアログが表示されます。

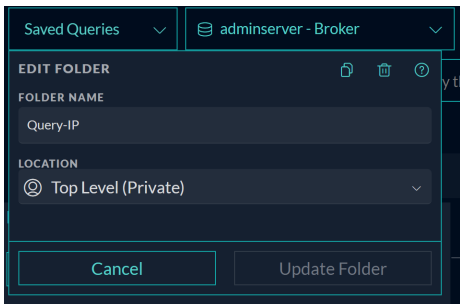


3. [**フォルダ名**]フィールドに、クエリ プロファイル フォルダの一意の名前を入力します。
4. 編集するフォルダの場所を選択します。
5. [**フォルダの更新**]をクリックします。

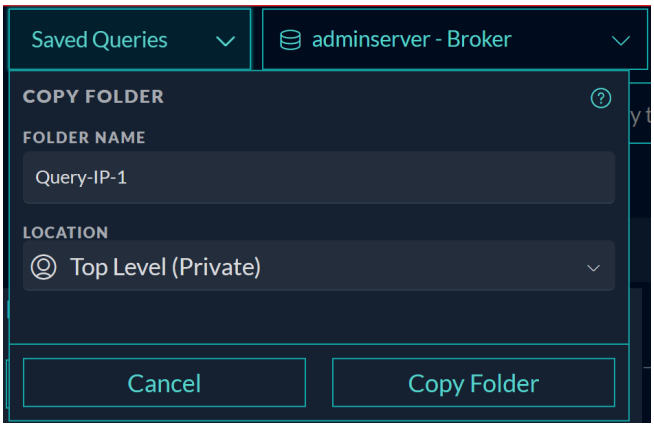
保存済みクエリ フォルダのコピー

保存済みクエリ フォルダは、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の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、[保存済みクエリ]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、保存済みクエリ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。

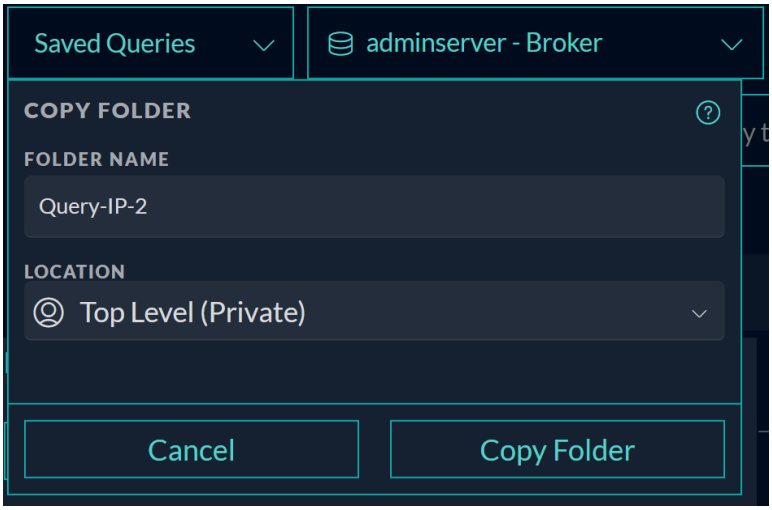


4. [**フォルダ名**]フィールドに、新しい保存済みクエリグループとフォルダの一意の名前(最大80文字)を入力します。
5. 編集するフォルダの場所を選択します。
6. [**フォルダのコピー**]をクリックします。

Liveから導入された保存済みクエリグループ フォルダのコピー

RSA Groupsカテゴリーの下にあるLiveから導入された保存済みクエリグループ フォルダは、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、[保存済みクエリグループ]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、保存済みクエリ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の保存済みクエリグループ 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。



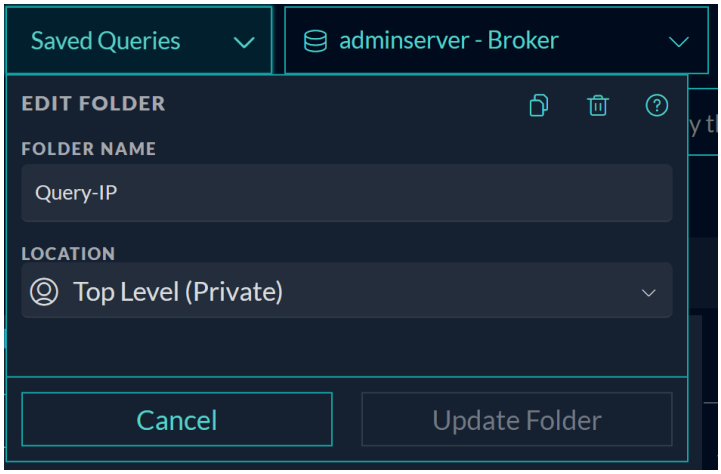
4. コピーするフォルダの場所を選択します。

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が付記された名前で表示されます。

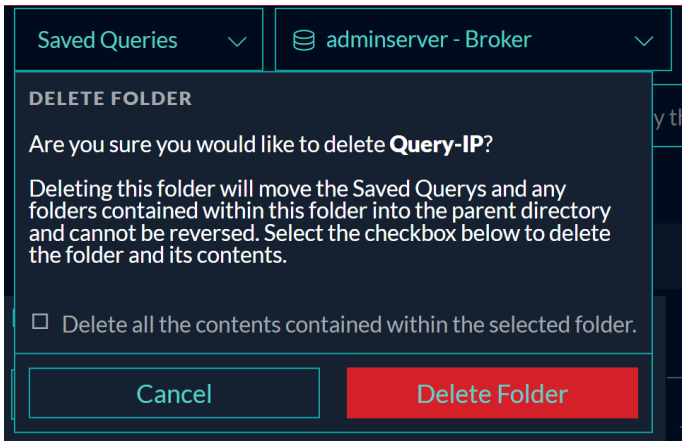
保存済みクエリ フォルダの削除

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、[保存済みクエリ]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. 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。



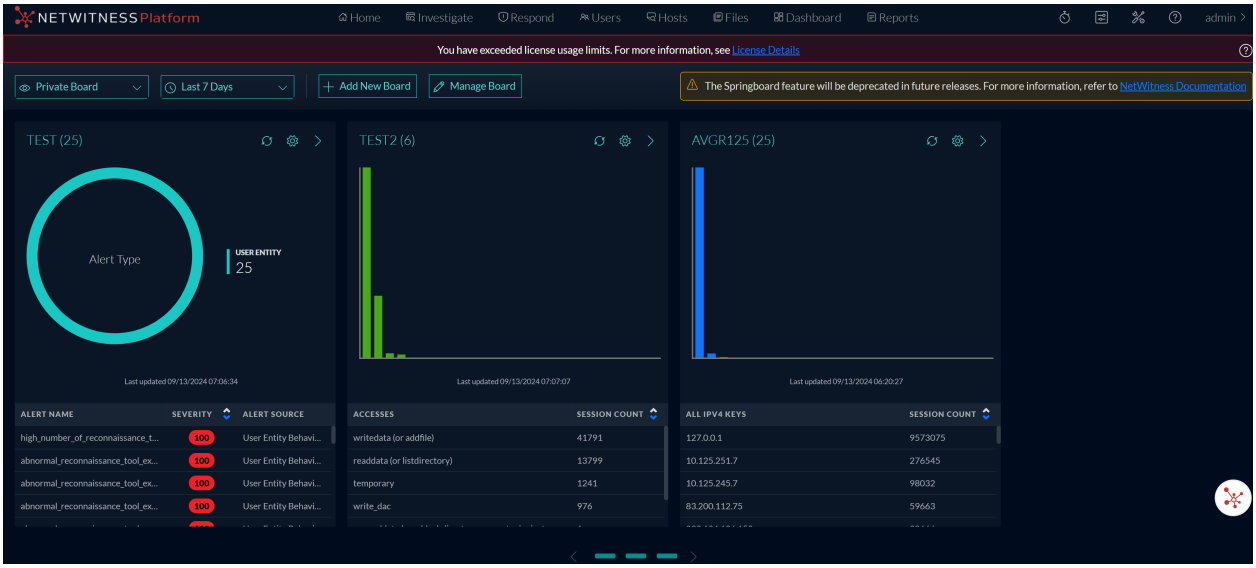
5. (オプション) 選択したフォルダ内のすべてのコンテンツとともにフォルダを削除する場合は、このチェックボックスを選択します。

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。

[イベント]ビューでのスプリングボード パネルの追加

管理者やアナリストが、[調査] > [イベント]ビューでスプリングボード パネルを作成できるようになりました。任意の数のフィルターをクエリー バーで追加し、それらを、重要なシステム インジケーターを含むスプリングボード パネルに変換して、脅威のハンティングと調査を実行できます。

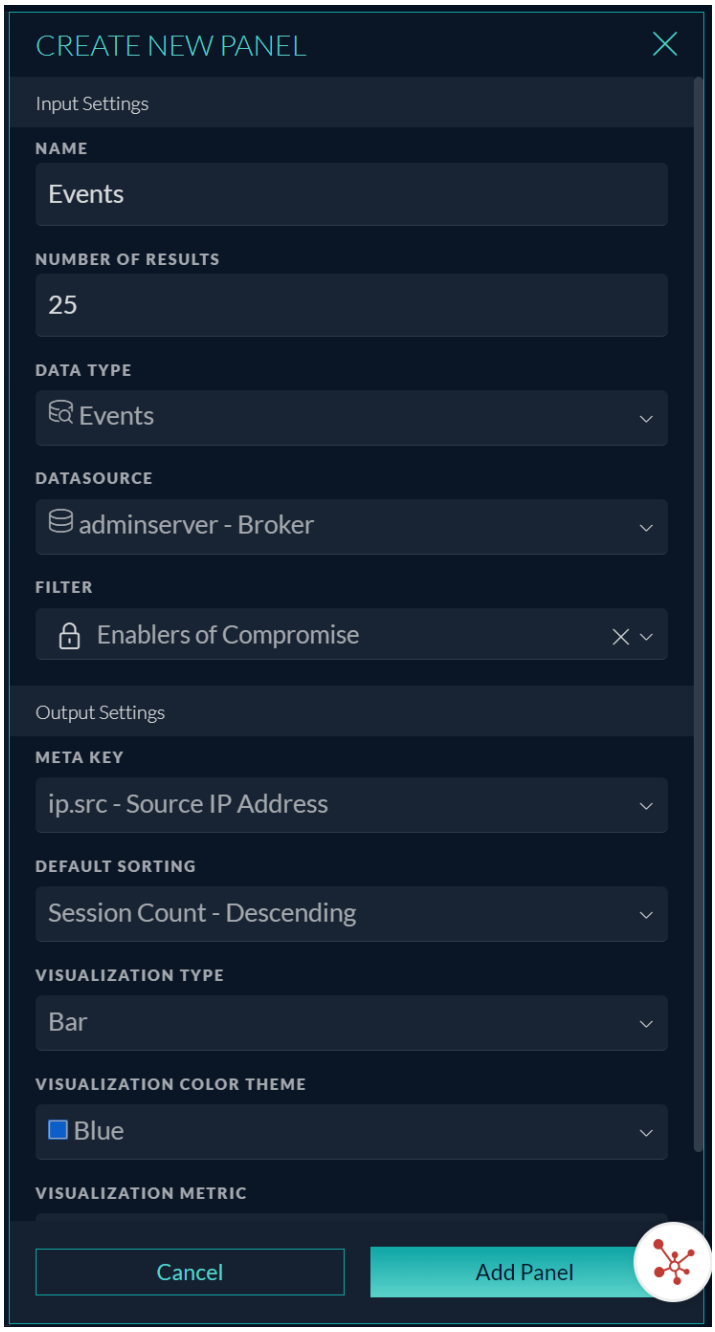


重要 :スプリングボード パネルを追加するには、必ず、カスタム プライベート ボードを最初に作成してください。

注 :アナリストは、**視覚化カラー テーマ**オプションを使用して、さまざまな色のパネルを作成できます。これにより、アナリストはデータをより効果的に可視化し、分析や調査をより効率的に行えるようになります。

[イベント]ビューでスプリングボード パネルを追加するには

1. [調査] > [イベント]に移動します。
2. メタキー、演算子、およびオプションの値を含む1つ以上のフィルターで構成されるクエリを作成します。
3.  > [スプリングボード パネルの作成]をクリックします。
   [パネルを新規作成]ダイアログが表示されます。



4. 次の詳細情報を入力します。
   - **名前**:パネルの一意の名前を入力します。名前には、英字、数字、スペース、特殊文字(_、-、(、)、[、]など) を含めることができます。

     注 :クエリー プロファイルは、スプリングボード パネルと同じ名前で作成されます。
   - **メタ グループ** :これはデフォルトで選択されています。
   - **列グループ** :これはデフォルトで選択されています。
   - **場所** :クエリー プロファイルが保存される場所です。

- **プレクエリー条件** :クエリー検索パネルに入力した入力基準に基づいて表示されます。
- **メタ キー** :ドロップダウン リストから適切なメタ キー値を選択します。
- **デフォルトのソート順** :ドロップダウン リストから適切なソート順を選択します。
- **チャートのタイプ** :ドロップダウン リストから適切なチャート タイプを選択します。
- **チャート カラー テーマ** :ドロップダウン リストから適切なチャート カラー テーマを選択します。

  注：[複数]カラー オプションはドーナツ チャートでのみ使用できます。

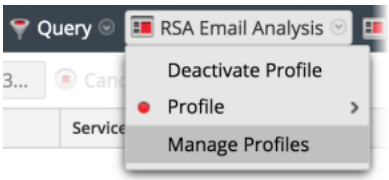
- **チャートのメトリック** :ドロップダウン リストから適切なチャート メトリックを選択します。

5. **[保存]**をクリックします。

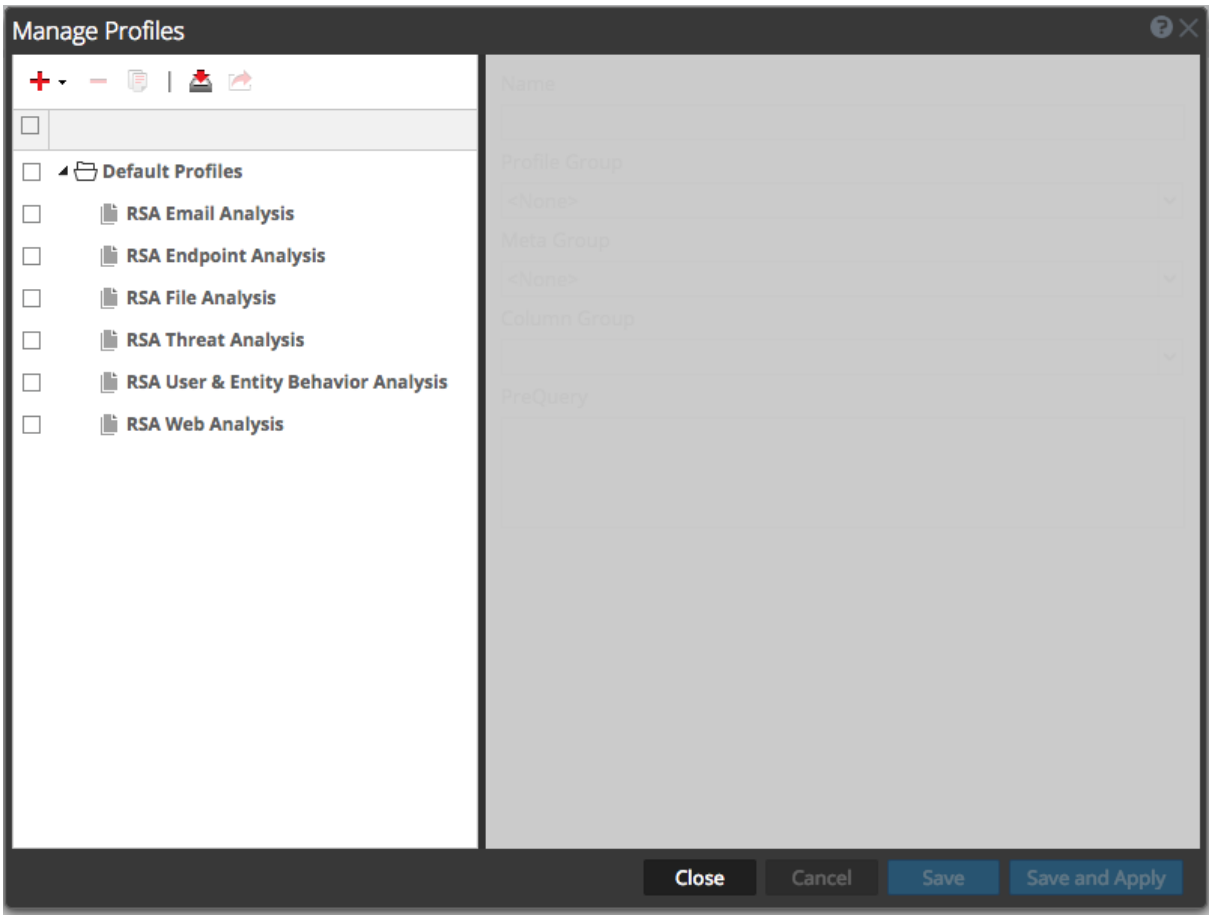
パネルが、スプリングボード内のカスタム プライベート ボードに正常に追加されます。

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

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



[プロファイルの管理]ダイアログが表示されます。



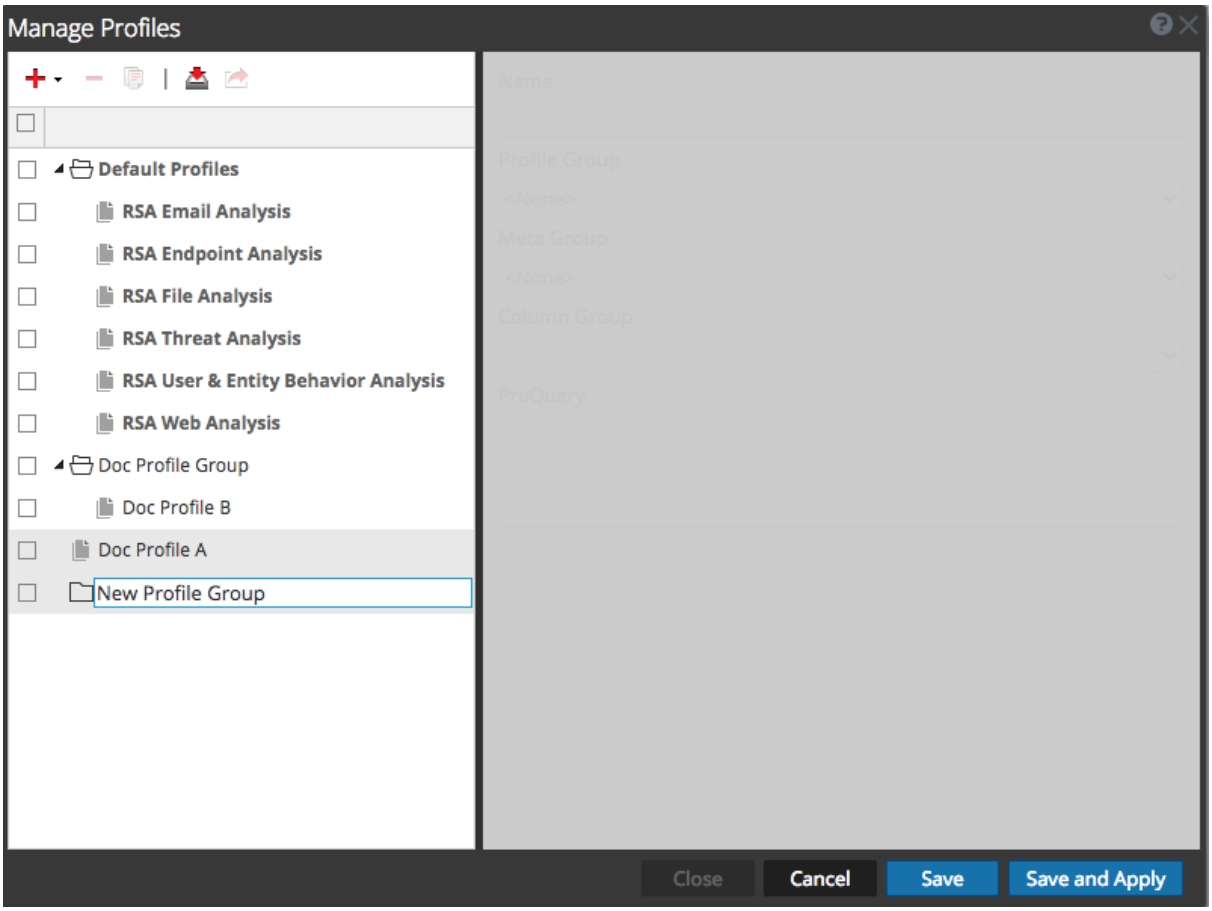
プロファイル グループの作成、編集、削除([ナビゲート]ビューまたは [レガシー イベント]ビュー)

カスタム プロファイル グループを作成して、異なるプロファイルを整理することができます。作成後、プロファイル グループに対して直接行える編集は、プロファイル グループの名前の編集だけです。グループ内のプロファイルを追加または削除するには、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)の説明に従って、プロファイルを編集し、別のプロファイル グループに割り当てます。

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。



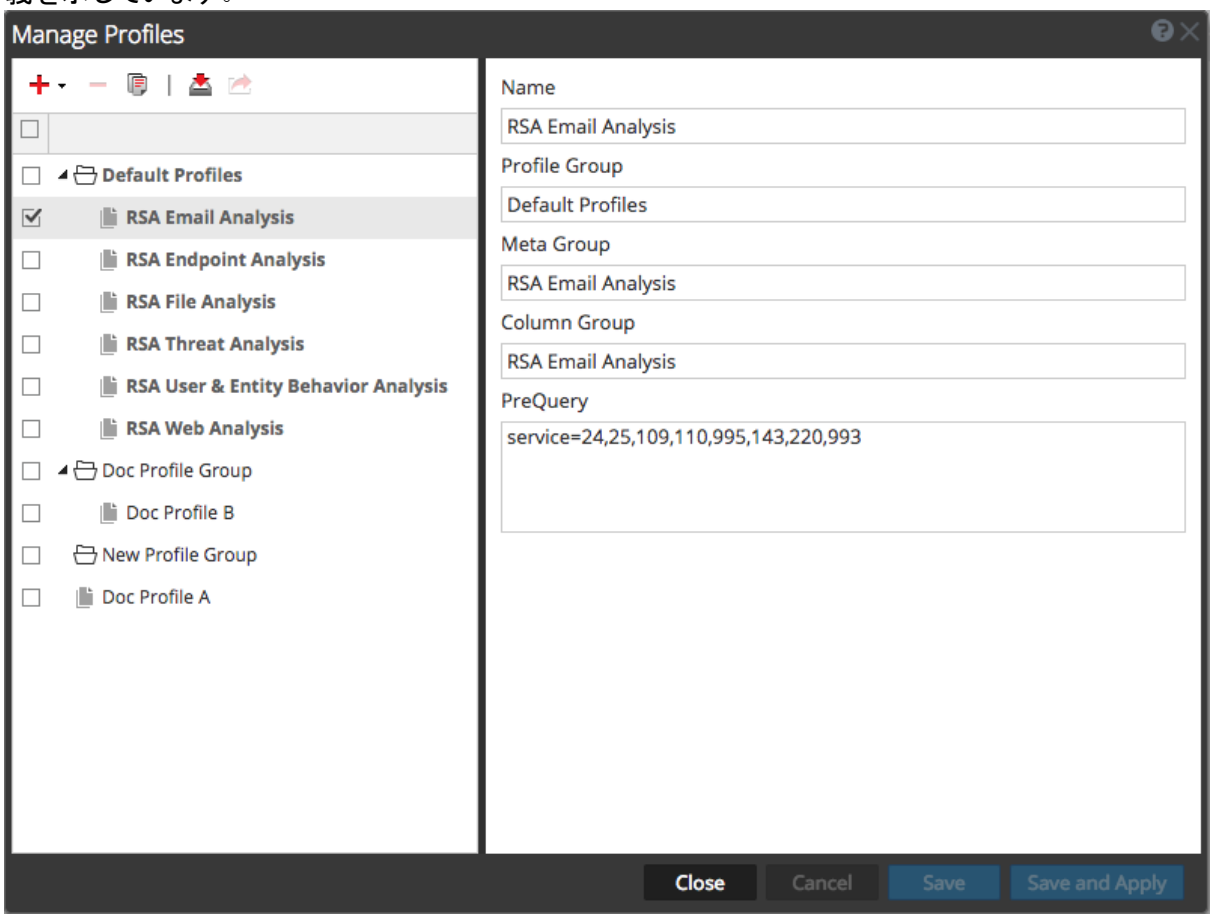
2. プロファイル グループの名前を編集または入力するには、プロファイル グループをダブル クリックし、入力フィールドに入力します。名前は2～80文字の長さにする必要があります。
プロファイルグループ名は、新しいプロファイル グループまたは編集したプロファイル グループに適用されます。プロファイルを設定するときに、プロファイル グループを使用できるようになります。
3. プロファイル グループを削除するには、次のいずれかの操作を行います。
   - プロファイルを削除することなく、プロファイル グループを削除する場合は、グループのチェックボックスをクリックし、グループ内のプロファイルのチェック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

1. ［**プロファイルの管理**］ダイアログで、次のいずれかを実行します。
   - 編集する既存のプロファイルを選択するには、名前の横にあるチェックボックスをクリックします。
   - 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。

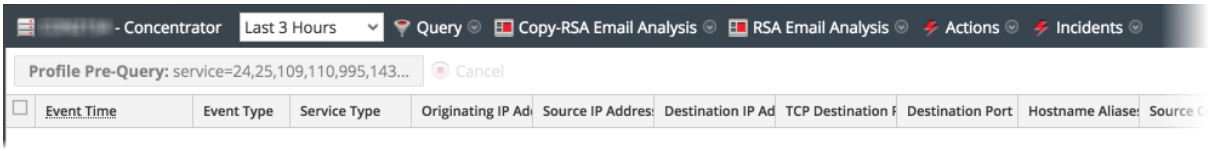
注 標準提供プロファイルのいずれかを編集する場合は、をクリックしてコピーを作成し、コピーを編集します。

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



2. **名前** フィールドに入力して、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. (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。最新バージョンでは、 [プロファイルの管理]ダイアログで入力したプレクエリが階層リンクに表示されます。



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

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

> **注** 標準提供プロファイルを削除することはできません。

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

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

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

別のプロファイルを使用する場合は、次の手順を実行します。

1. [**ナビゲート**]ビューまたは [**レガシー イベント**]ビューのツールバーで、 [**プロファイル**]ドロップダウン メニューを開きます。
2. [**プロファイル**]オプションにマウス ポインターを置くと、使用可能なプロファイルのドロップダウン リストが表示されます。

3. 使用するプロファイルを選択します。
   そのプロファイル設定が即座に適用されます。

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

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

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

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

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

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

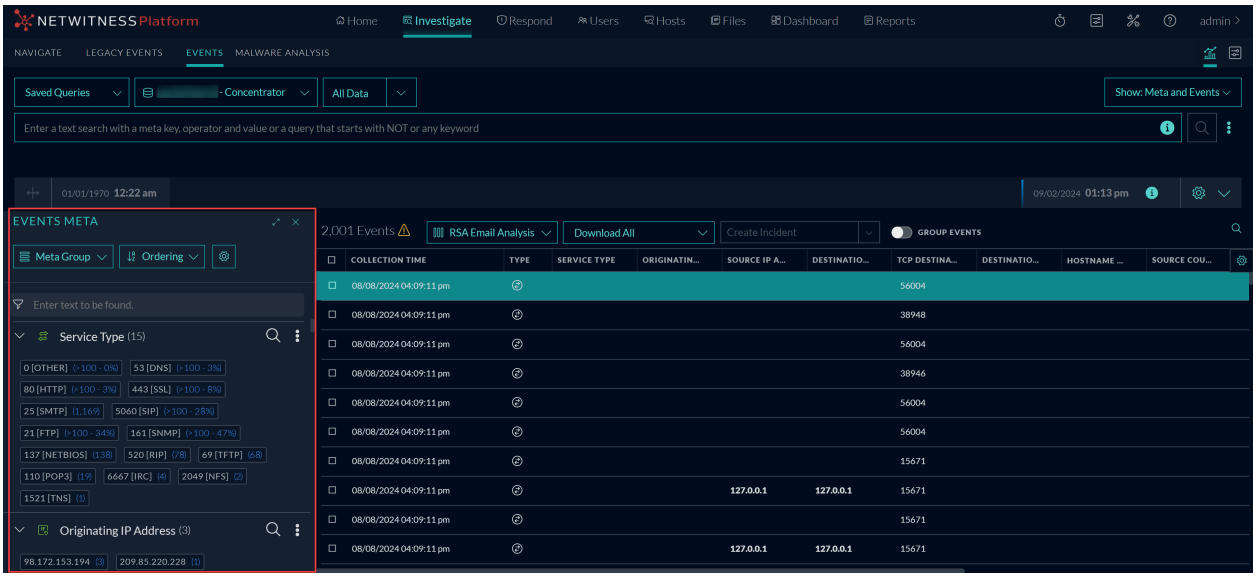
［ナビゲート］ビューと［レガシー イベント］ビューでは、プロファイルを.jsnファイルとしてダウンロードできます。

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

イベントビューでメタデータのドリルダウン

［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。保存済みクエリ、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。

イベント ビューを離れることなく、イベント メタ パネルでメタデータをドリルダウンすることができます。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 メタ］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。



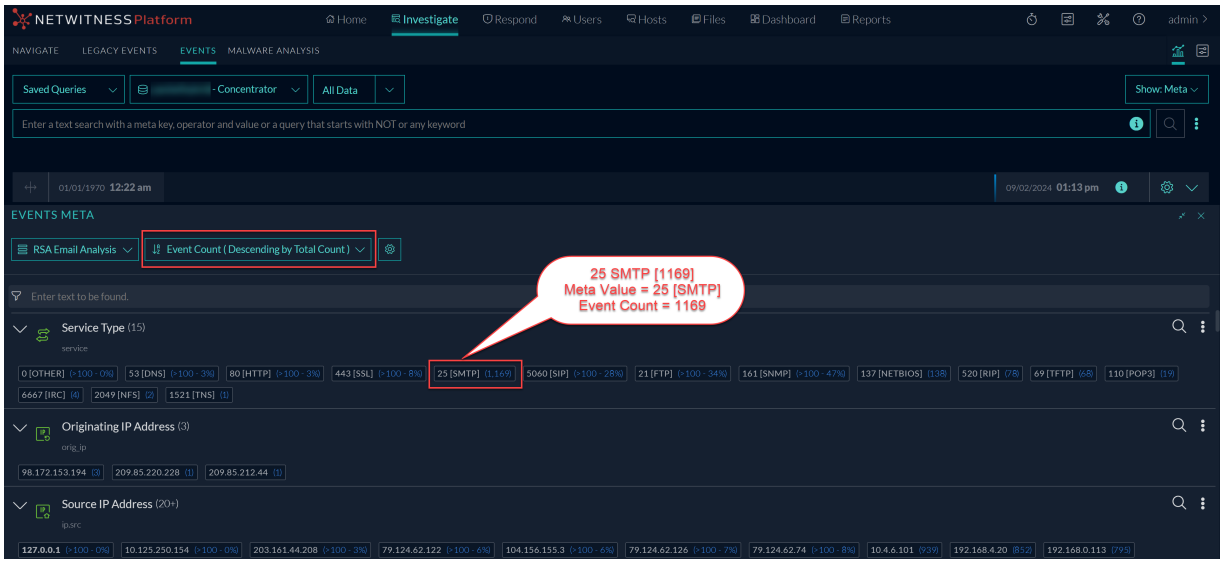
注：［イベント メタ］パネルの結果が期待どおりにならない可能性がある状況は以下の2つです。
- ［イベント］パネルのクエリにテキスト フィルタが含まれている場合は、［イベント］パネルと［イベント メタ］パネルの結果セットが異なることがあります。
- ［イベント］ビュー クエリ ビルダーのクエリに論理ORまたは&&が含まれている場合は、［イベント］ビューの結果が［ナビゲート］ビューおよび［レガシー イベント］ビューでの同じクエリの結果と異なることがあります。このような場合、［ナビゲート］ビューと［レガシー イベント］ビューでは、論理OR式が括弧のセットで自動的に囲まれるのに対し、［イベント］ビューでは、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。

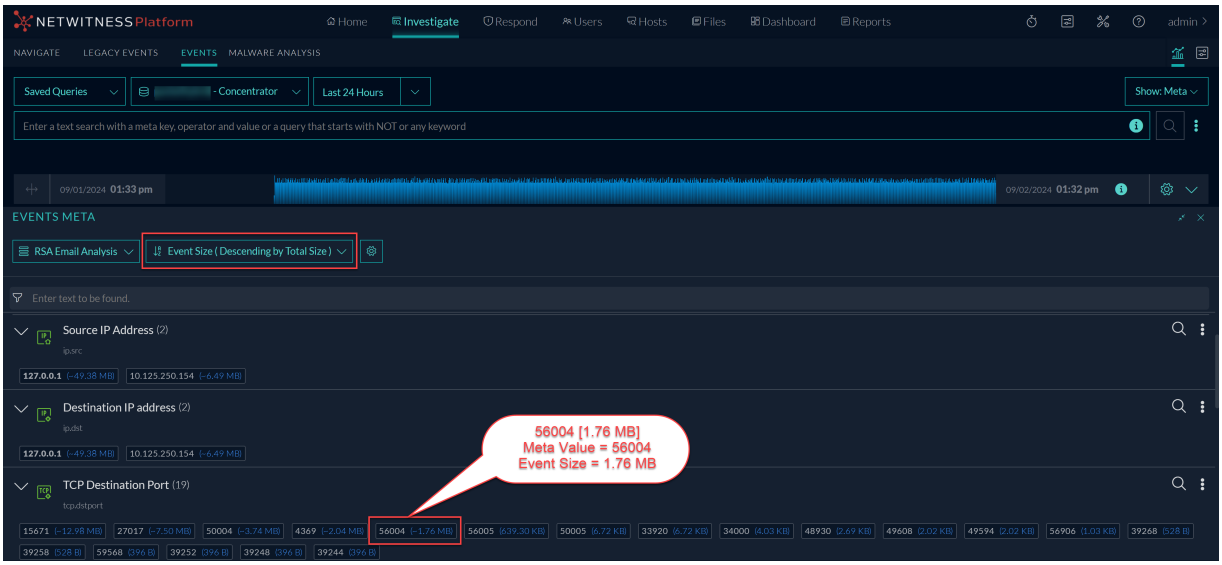
注：イベント メタ パネルでは、メタ値の結果しきい値は100000です。結果がしきい値を超える場合は、 ~ または > **を使用して示されます**。たとえば、「**(>100000)**」は、結果がカウントに基づいてソートされ、閾値よりも大きいことを示します。同様に、「**(~100000)**」は、結果がサイズに基づいてソートされ、閾値よりも大きいことを示します。

動作モード

[イベント メタ]パネルには2つの操作モードがあります。

- **縮小モード**の [イベント メタ]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 メタ]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 メタ]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 メタ]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 メタ]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 メタ]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 メタ]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 メタ]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。

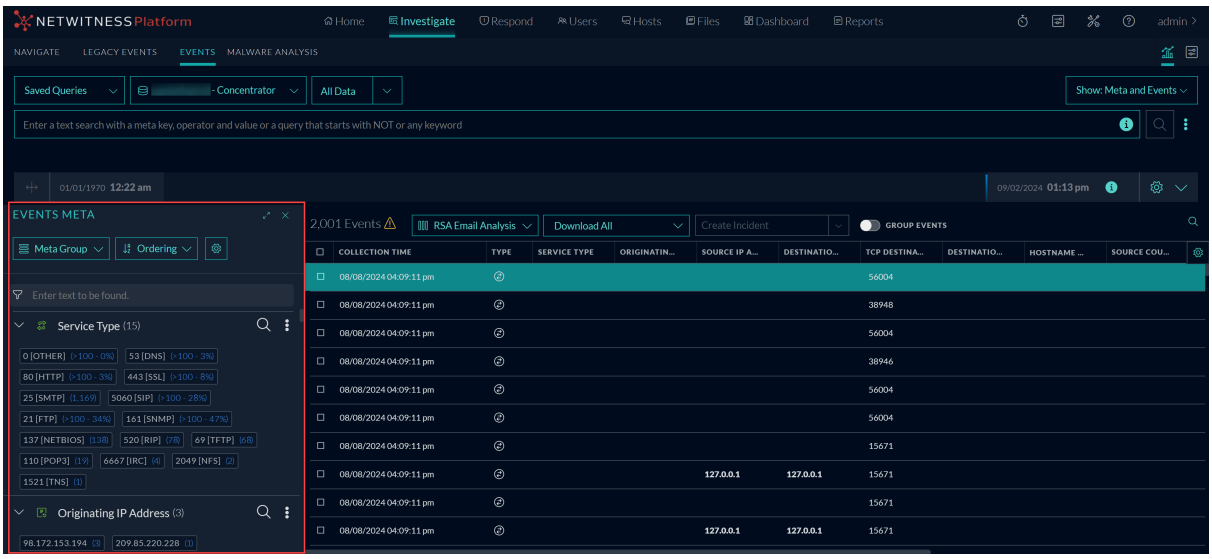




[イベント メタ] パネルでメタデータを表示する

[イベント メタ] パネルでメタデータを表示するには

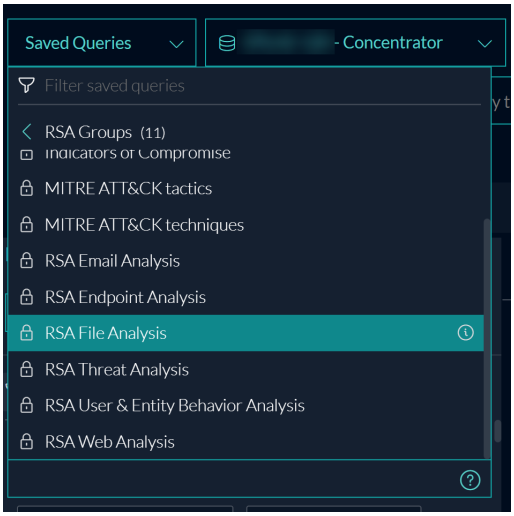
1. **[調査]** > **[イベント]** に移動し、調査するサービスを選択して、時間範囲を選択します。
2. (オプション) 列グループまたはクエリ プロファイルを選択します。
3. をクリックして [イベント] パネルでイベントをロードします。
   クエリが [イベント] パネルで実行され、一致するイベントが一覧表示されます。
4. イベント パネルのイベント メタ ボタン (Events Meta) をクリックします。
   イベント パネルの左側にイベント メタ パネルが開きます。



注 :デフォルトでは、イベント メタ パネルはイベント ビューで開きます。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、ブラウザー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。以前選択したメタ グループはブラウザー キャッシュに保存されないため、変更するまで有効のままになります。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、少なくとも1つのメタ値を持ち、開いている最初の25個のメタ キーがイベント メタ パネルに入力されます。[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。

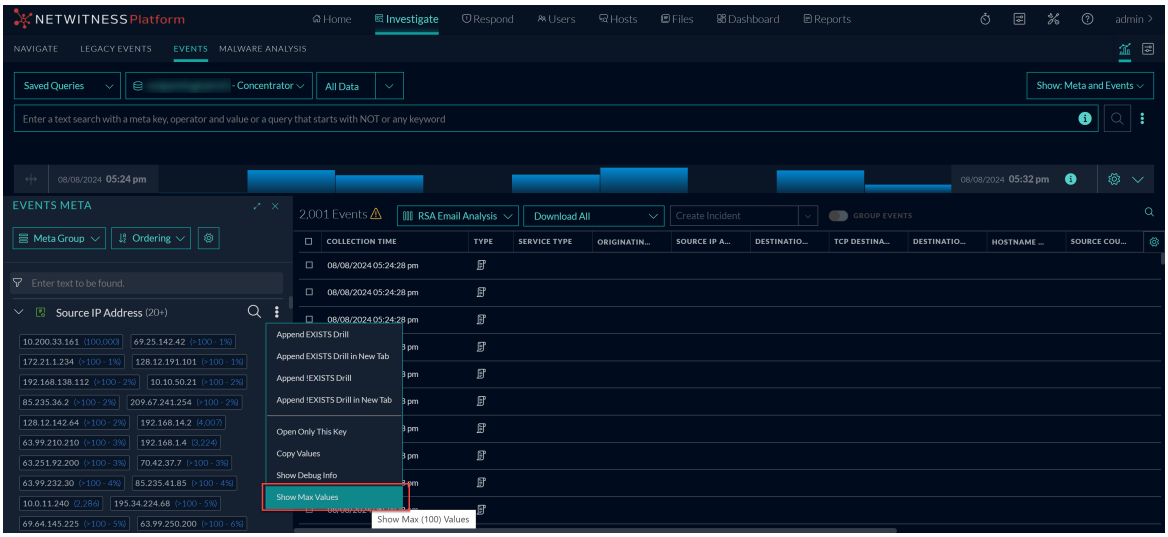
1. 次のいずれかの操作を実行します。
   a. 編集しないでダイアログを閉じるには、 **[閉じる]**をクリックします。
   b. ダイアログを閉じてメタ グループのコピーを選択するには、 **[メタ グループの選択]**をクリックします。
      [メタ グループ]メニューにグループが追加されます。次の図は、RSA HTTPメタ グループのプライベート コピーを示しています。



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。

1. イベント ビューでイベント メタ パネルを開いた状態で、  をクリックして、 **[最大値を表示]** オプションを選択します。



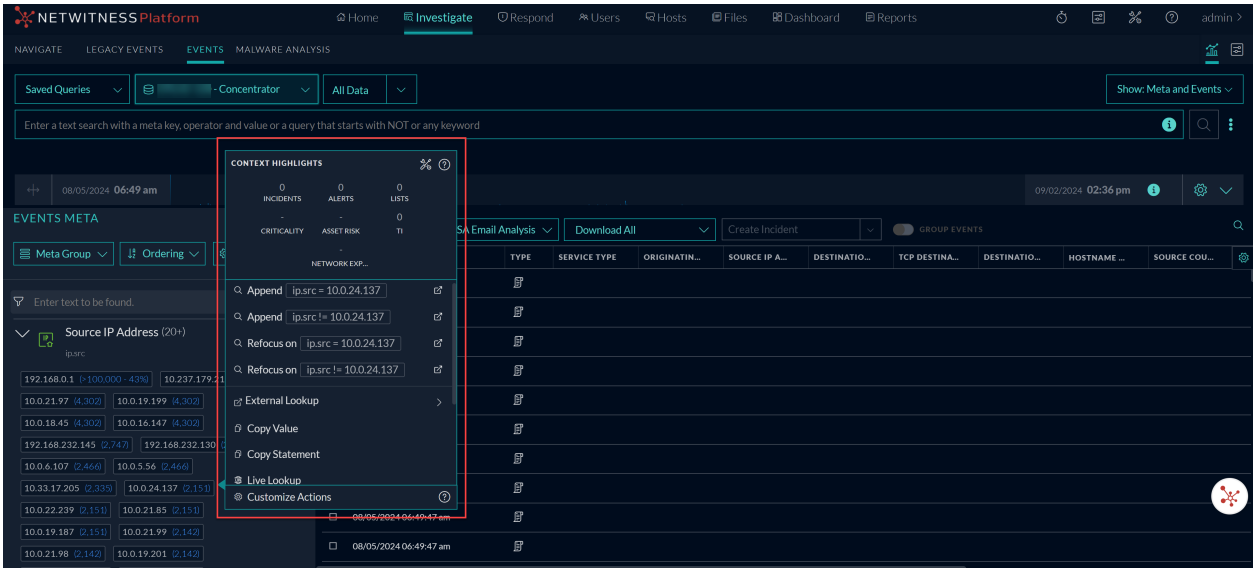
2. 以前にレンダリングされなかった値のロードが開始され、最大1,000件の結果が表示されます。

[イベント メタ]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 メタ]パネルでは、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、重要度、資産リスク、脅威インテリジェンス (TI) の関連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。

また、 [外部ルックアップ]、 [値のコピー]、 [ステートメントのコピー]、 [Liveルックアップ]、 [コンテキスト ルックアップ]、 [調査] > [ホスト/ファイル]への移行]、 [Archerへの移行]、 [リストへの追加/削除]などの他のオプションも表示できます。



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。

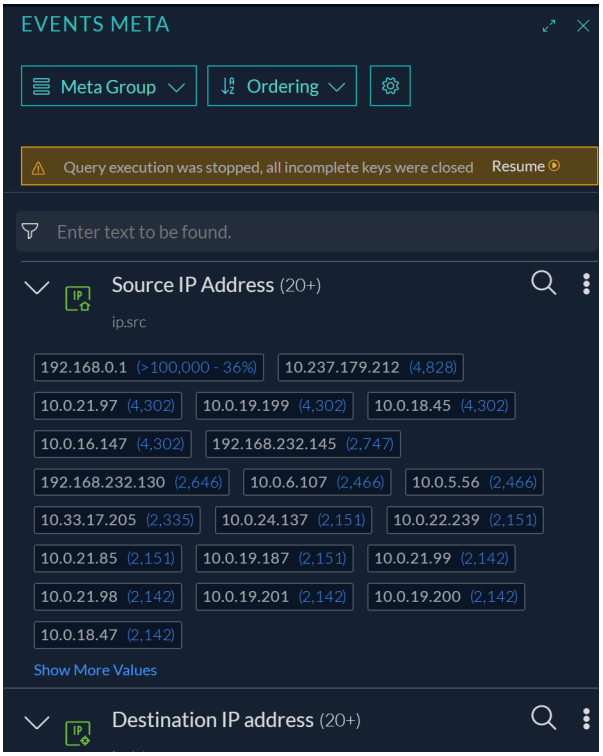
- このメタ キーは値でインデックス付けされています。Action Event [action] (40+).緑色は、使用可能なすべてのインタラクションとクエリがサポートされていることを示します。メタ値を右クリックすると、コンテキスト メニューで使用可能なインタラクションを確認できます。
- このメタ キーはメタ キーによってインデックス付けされています。Bytes Sent [bytes.src].黄色は、使用可能なインタラクションのサブセットがサポートされていることを示しています。このメタ キーに対するクエリは、値でインデックス付けされたメタ キーよりも時間がかかる場合があります。メタ値を右クリックすると、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。
- 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.netwitness.com/t5/netwitness-platform-unified-data/tkb-p/netwitness-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

[イベント メタ]パネルでは、メタ キーと値のロード中に、メタデータのロードを停止、再開することができます。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 メタ]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。



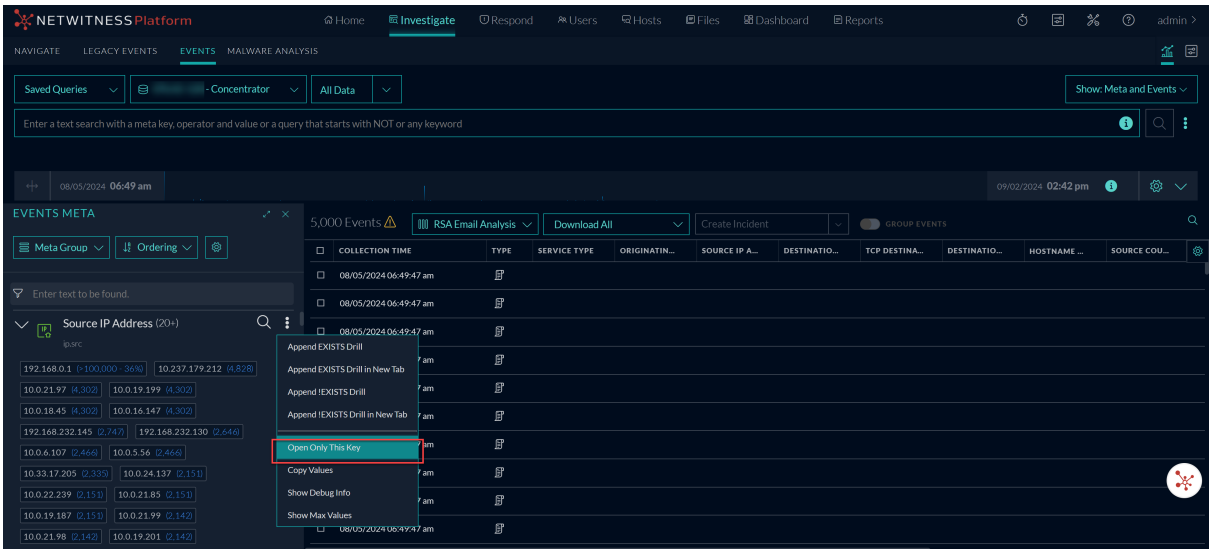
2. 次のいずれかの操作を実行します。
   a. ロードが停止したメタ キーでロードを再開するには、 [再開]をクリックします。
   b. クエリを再開せずに、ロードされなかった特定のメタ キーの値を確認する場合は、メタ キー名をクリックして任意のキーを開きます。

1つを除き、すべてのメタ キーを閉じるには

イベント メタ パネルが開いているときに、同時に多くのメタ キーが表示されると、気が散る可能性があります。

1つを除き、すべてのメタ キーを閉じるには

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。

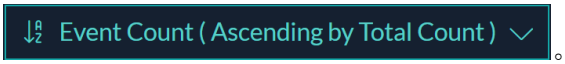


2. ［**このキーのみを開く**］を選択します。
   現在のメタ キーを除くすべてのメタ キーが閉じられます。選択したキーが閉じられている場合は、そのキーが開いてロードされ、他のキーはすべて閉じられます。

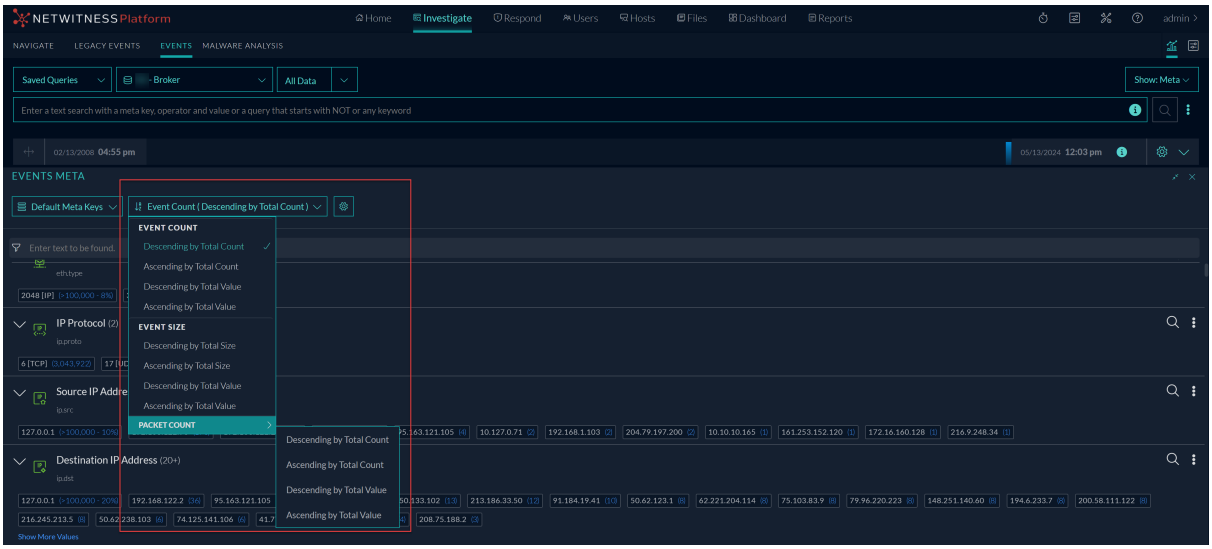
メタ値の並べ替え方法を設定する

イベント メタ パネルを開くと、各値の3つのパラメータを確認できます。イベント数、イベント サイズ、またはパケット数。各メタ キー エントリには、値の後の括弧内にイベント数、イベント サイズ、またはパケット数のいずれかが含まれます。いずれの場合も、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

1. ［イベント メタ］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。 

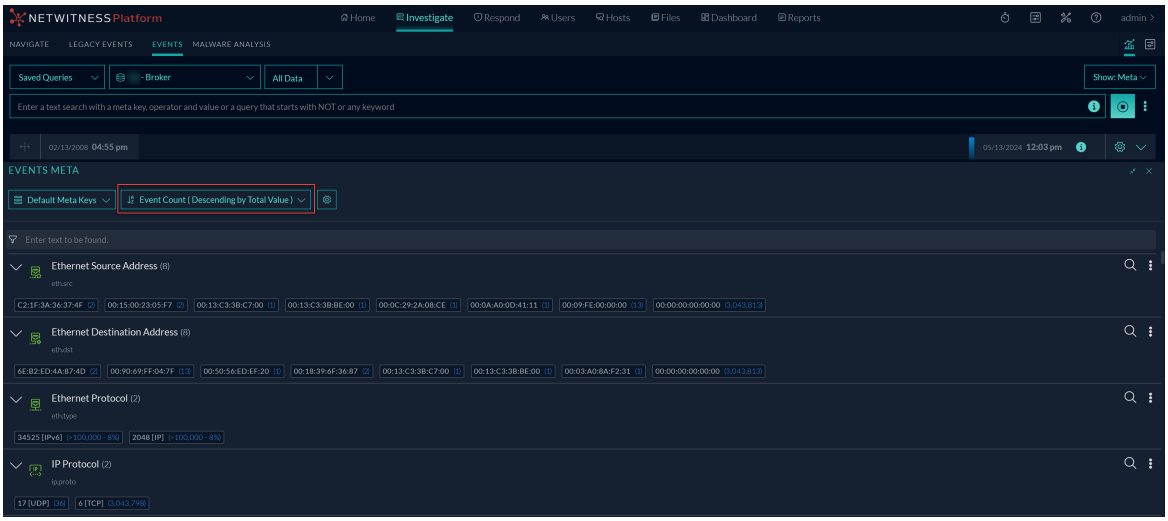
   。
   ［並べ替え］メニューが表示されます。この図は、縮小バージョンのメニューを示しています。



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、［**合計値の昇順**］または［**合計値の降順**］のいずれかを選択します。

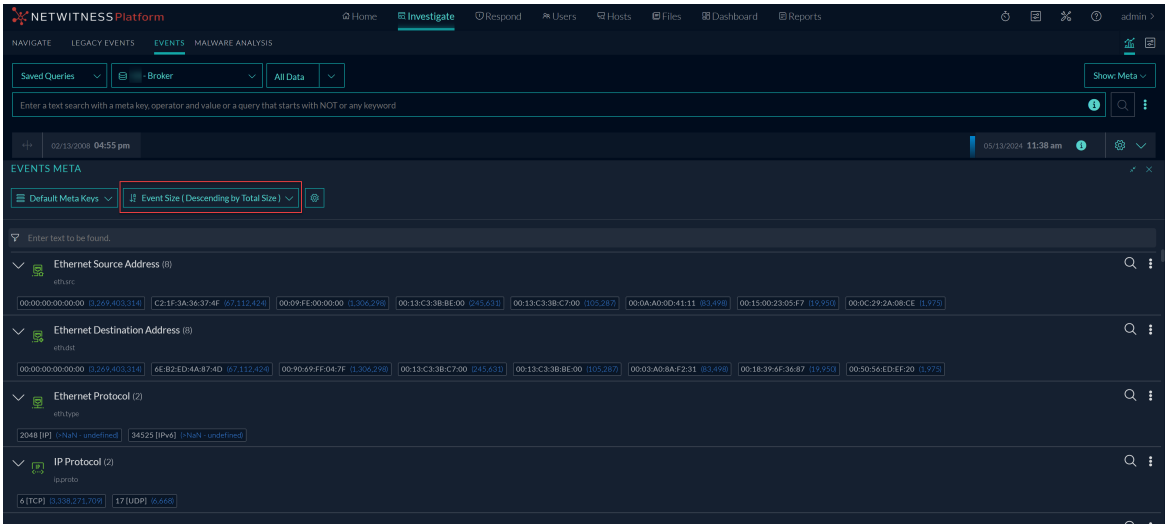


3. 値が見つかったイベントのサイズをバイト単位で表示するには、次のオプションのいずれかを選択します。

   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。

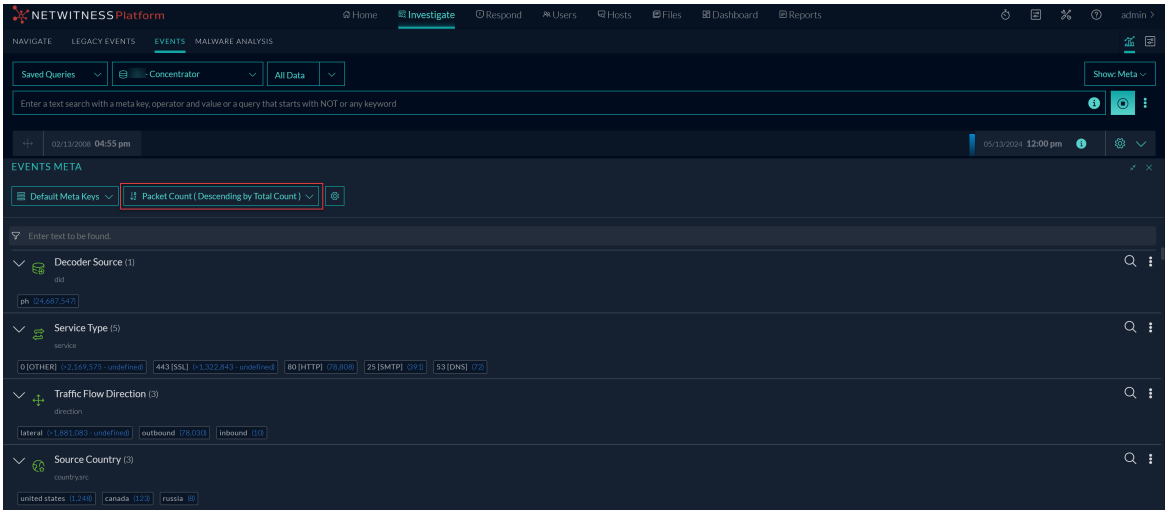
   b. 値の名前で並べ替えるには、［**合計サイズの昇順**］または［**合計サイズの降順**］のいずれかを選択します。

［イベント メタ］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。



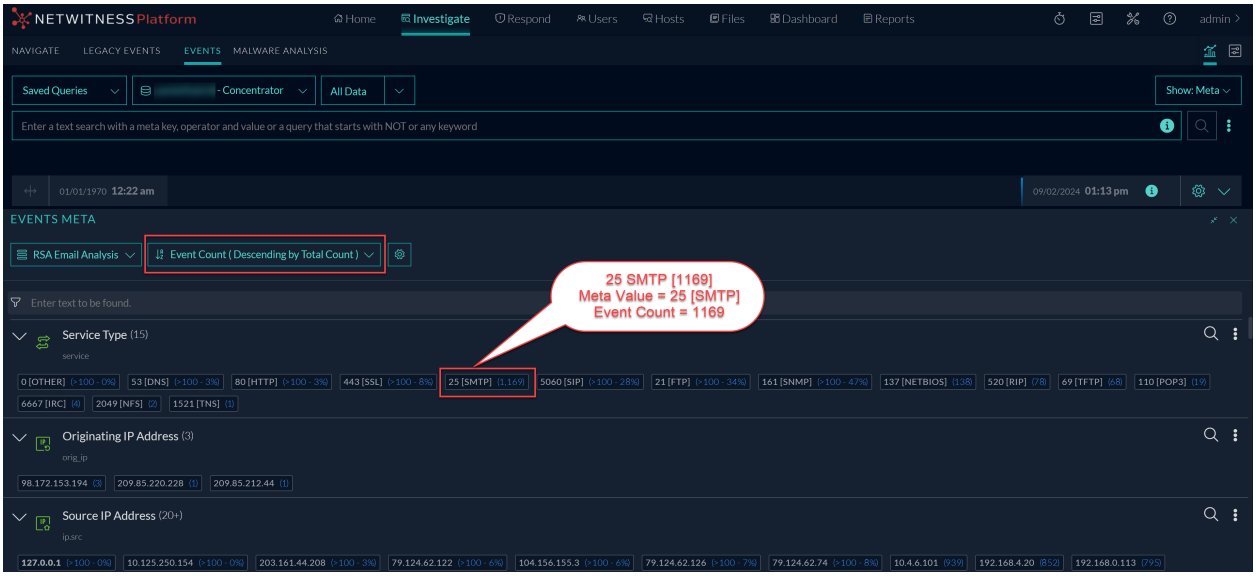
4. メタ キーのパケット数を確認する場合は、次のいずれかのオプションを選択します。
   a. 値が見つかったパケットの合計数で並べ替えるには、［**合計数の降順**］または［**合計数の昇順**］のいずれかを選択します。
   b. 値の名前で並べ替えるには、［**合計値の昇順**］または［**合計値の降順**］のいずれかを選択します。

注：パケット数 フィルタリング オプションは、NetWitness Platform 12.5以降のバージョンでサポートされています。

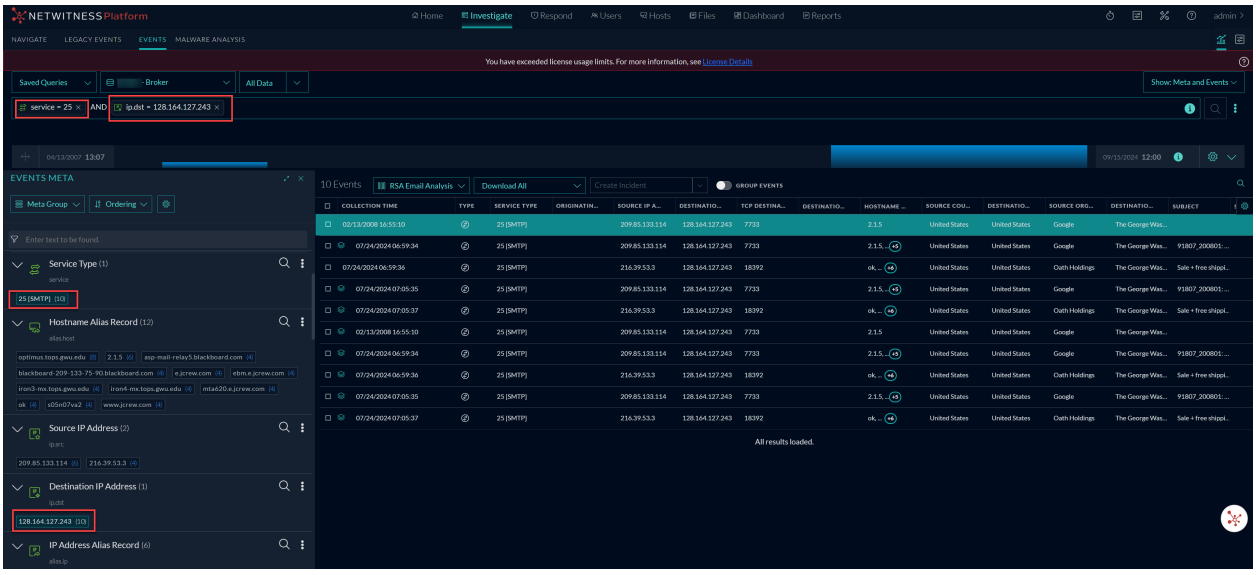


メタ値をドリルダウンする

[イベント メタ]パネルを開いた状態で、メタ値をドリルダウンし、関連するイベントのできるだけ小さな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 メタ]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 メタ]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 メタ]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 メタ]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 メタ]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 メタ パネルで強調表示された、クエリ フィルターに関連するメタ キー値を示しています。



完全に展開された［イベント メタ］パネルでメタ値をドリルダウンするには

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 メタ］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 メタ］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、そこではクエリは実行されません。
   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 メタ］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、そこではクエリは実行されません。
   c. **CTRL (Windows)** または **CMD (MacOS)** を押しながら値をクリックします。
   フィルターはクエリ バーの最後のフィルターとして追加されますが、イベント メタ パネルのメタデータから他のサービス タイプはフィルター処理されません。［イベント］パネルを閉じられていると、そ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 メタ］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 メタ］パネルでメタ値をドリルダウンするには

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。
   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 メタ］パネルのメタデータから除外されて、［イベント］パネルでクエリが実行されます。
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 メタ］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 メタ］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。

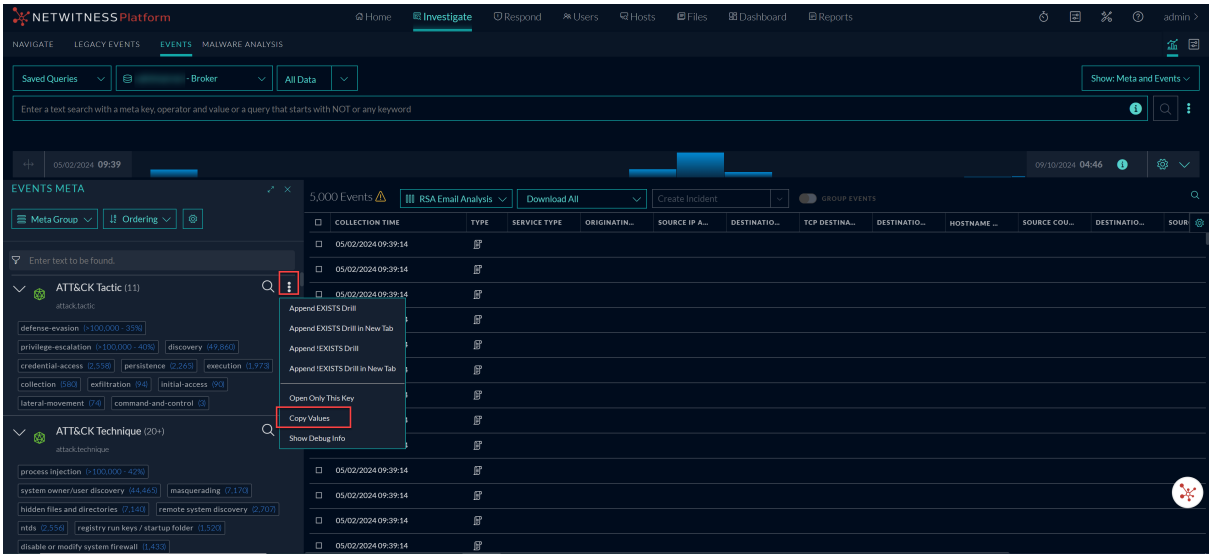
c. **CTRL(Windows)** または**CMD(MacOS)** を押して、値をクリックします。
フィルタはクエリ バーの最 後 のフィルタとして追 加されますが、メタデータから他 のサービス タイプが除 外されることはなく、クエリ ボタンをクリックしない限り [イベント] パネルでクエリは実 行 されません。

3. 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

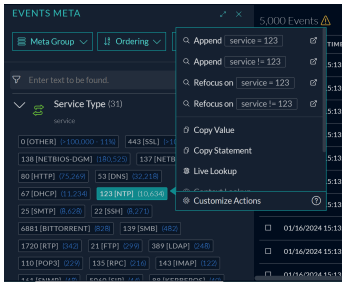
1. エントリのメタ キー行 で、 [メタ キー オプション] ボタン( ) をクリックします。
メタ キー オプションが表 示されます。現 時 点で唯 一 のオプションは [値 のコピー] です。



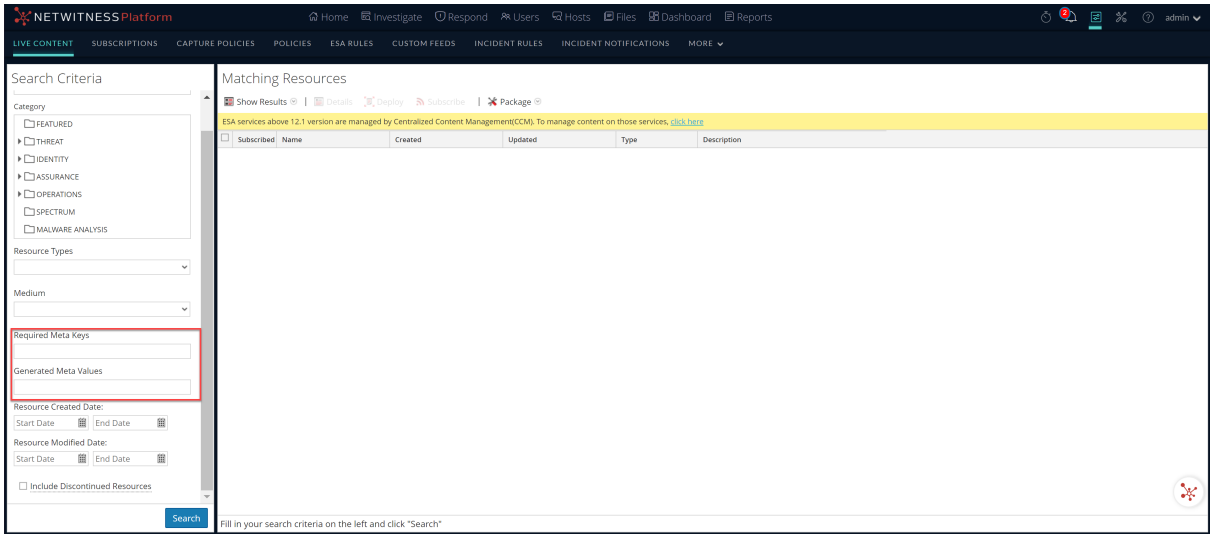
2. [**値 のコピー**] をクリックします。
値 のカンマ区 切りリスト がローカルのクリップボード にコピーされます。これは、クリップボード の内 容 の例 です。`"get", "login", "put".`

選択したメタ値をLiveで表示する

1. メタ値を左クリックまたは右クリックします (例: **NTP**)。
   メタ値のドロップダウン メニューが表示されます。



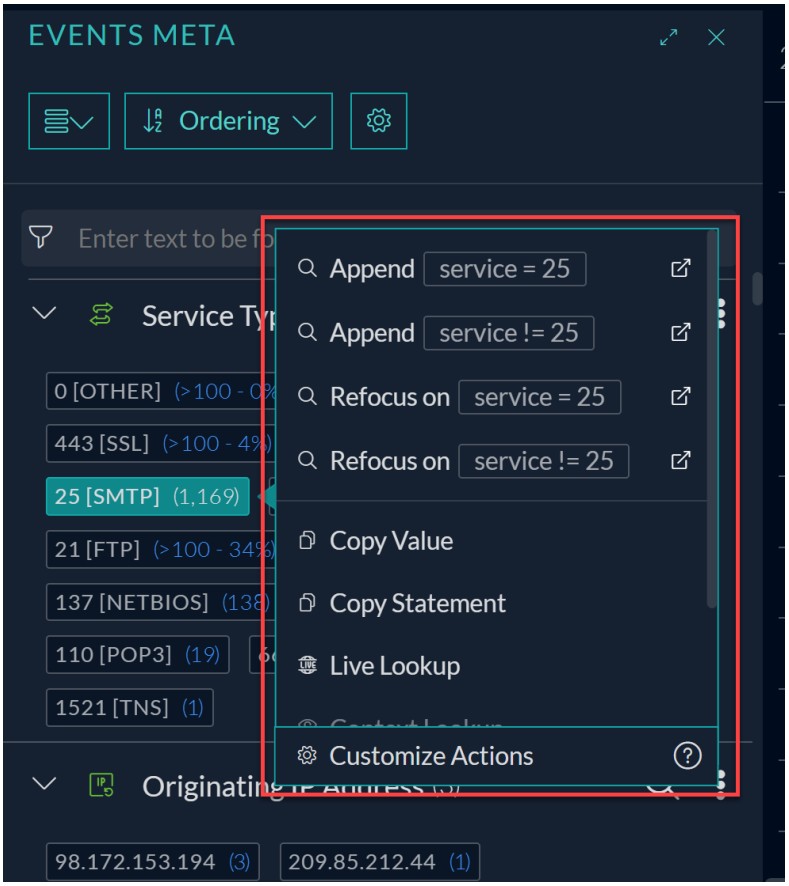
2. **success**などのメタ値をLiveで検索するには、 [**Liveルックアップ**]を選択します。
   Liveの [検索]ビューが開いて、入力したメタ値が [生成されるメタ値]フィールドに表示され、検索できる状態になります。



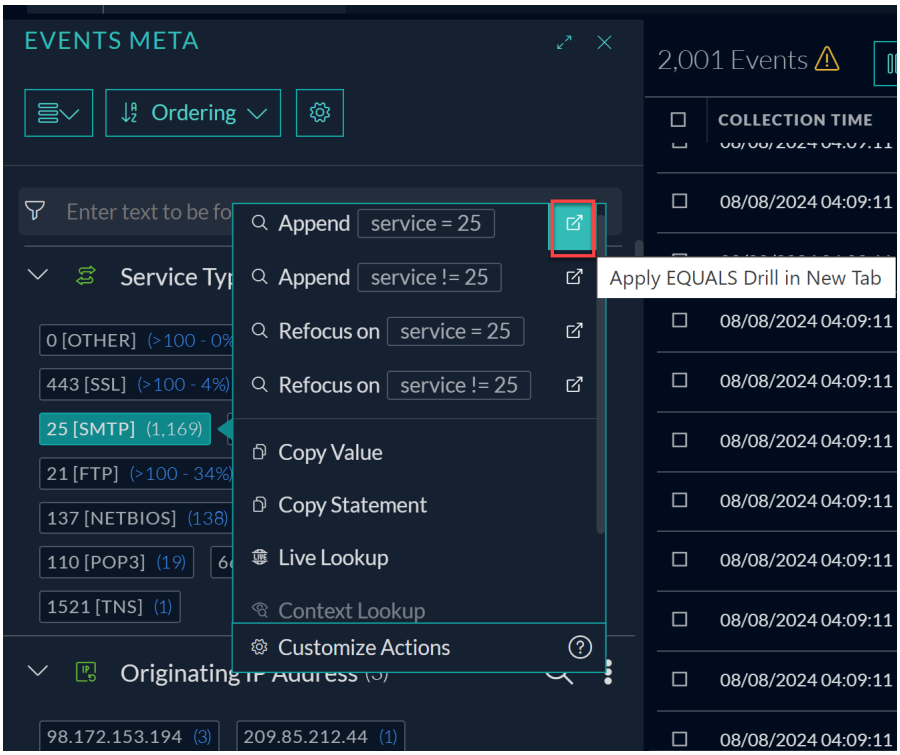
[統合]パネルでのメタ値の調査の追加および再フォーカス

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、さまざまな追加オプションと再フォーカス オプションを含むコンテキスト メニューが表示されます。すべての追加アクションと再フォーカス アクションにより、 [イベント]パネル、 [イベント メタ]パネル、 [メタ イベント]パネルのドリルダウン ポイントが更新されます。

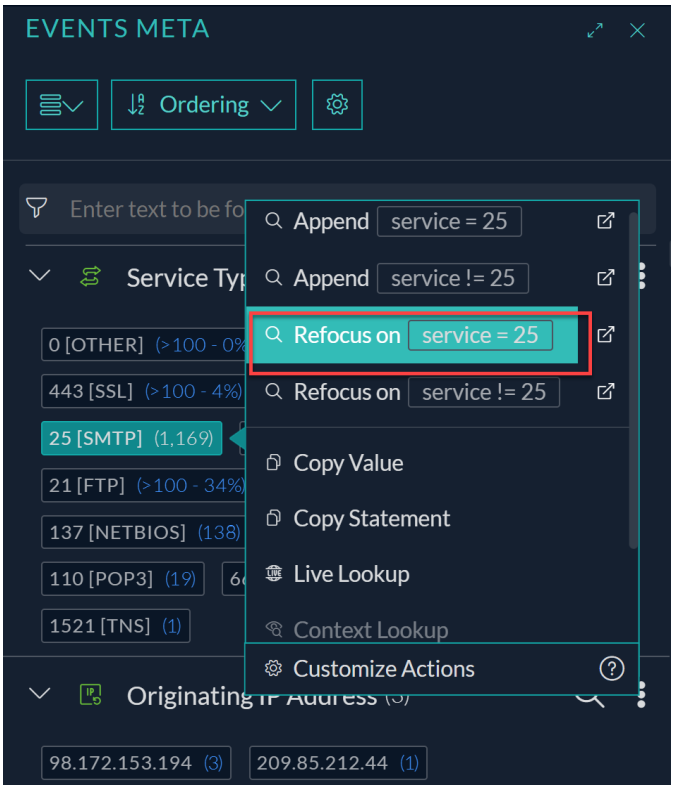
1. さまざまな演算子(=、 !=、contains) を使用して、キーと値のペアをクエリーに追加するには、メタ値(下の図のSMTPなど) を右クリックし、 **[適用<operator>ドリルダウン]**オプションのいずれかを選択します。



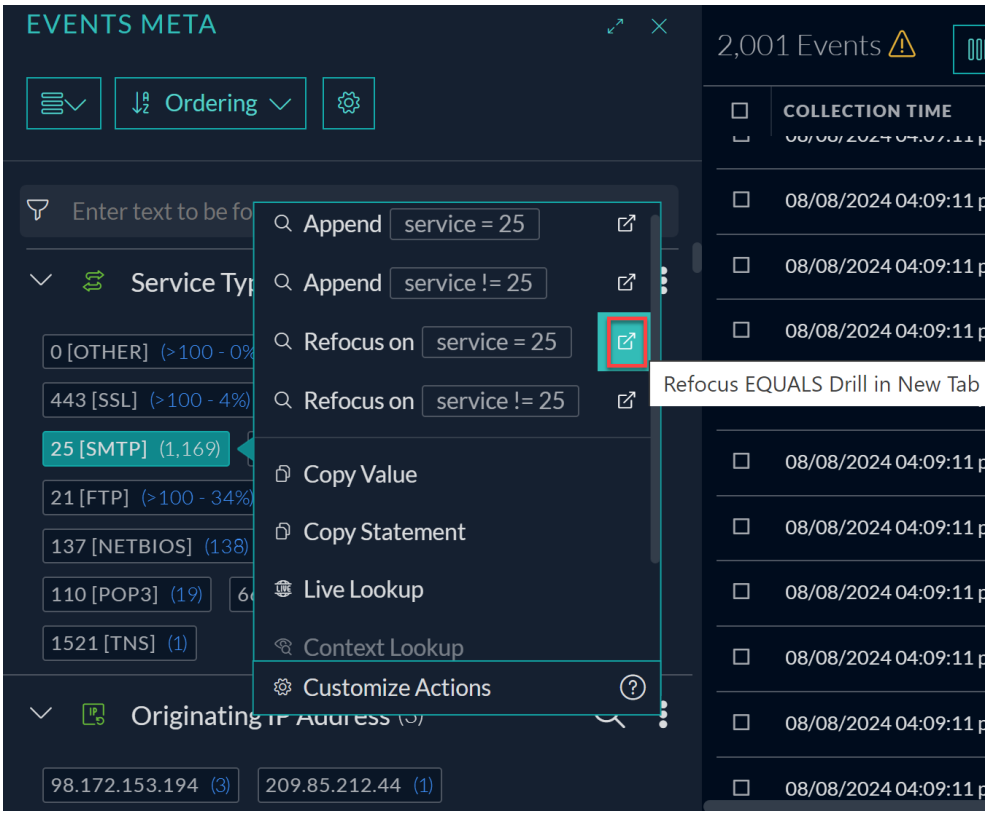
2. キーと値のペアをクエリーに追加するか、新しいブラウザー タブで、キーと値のペアを最初から開始するには、値を右クリックし、 **[新しいタブの追加]** > **[新しいタブに<operator>ドリルダウンを追加]**のいずれか、または複数の **[新しいタブに<operator>ドリルダウンを追加]**オプションを選択します。



3. キーと値 のペアと別 の演 算 子(=、 !=、contains) を使 用してクエリーを最 初 からやり直 すには、値 を右 クリックし、 [**<operator>ドリルダウンの再 フォーカス**] オプションのいずれかを選 択します。

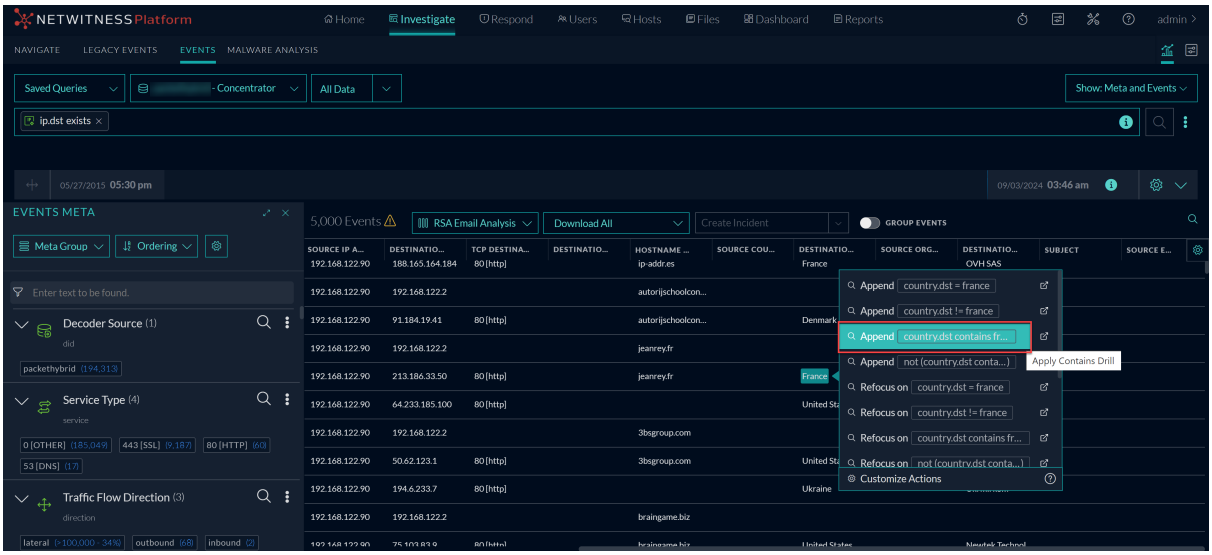


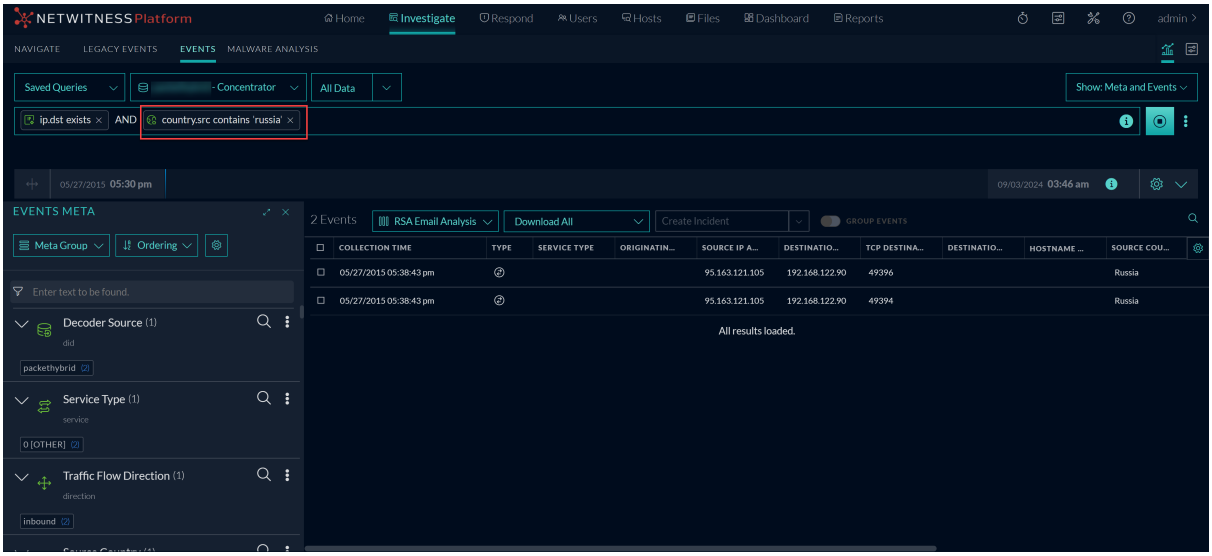
4. キーと値 のペアをクエリーに追 加 するか、新しいブラウザー タブで、キーと値 のペアを最 初 から開 始 するには、値 を右 クリックし、 **新しいタブの再 フォーカス**] > **新しいタブの<operator>ドリルダウンの再 フォーカス**]のいずれか、または複 数 の **新しいタブの<operator>ドリルダウンの再 フォーカス**]オプションを選 択 します。



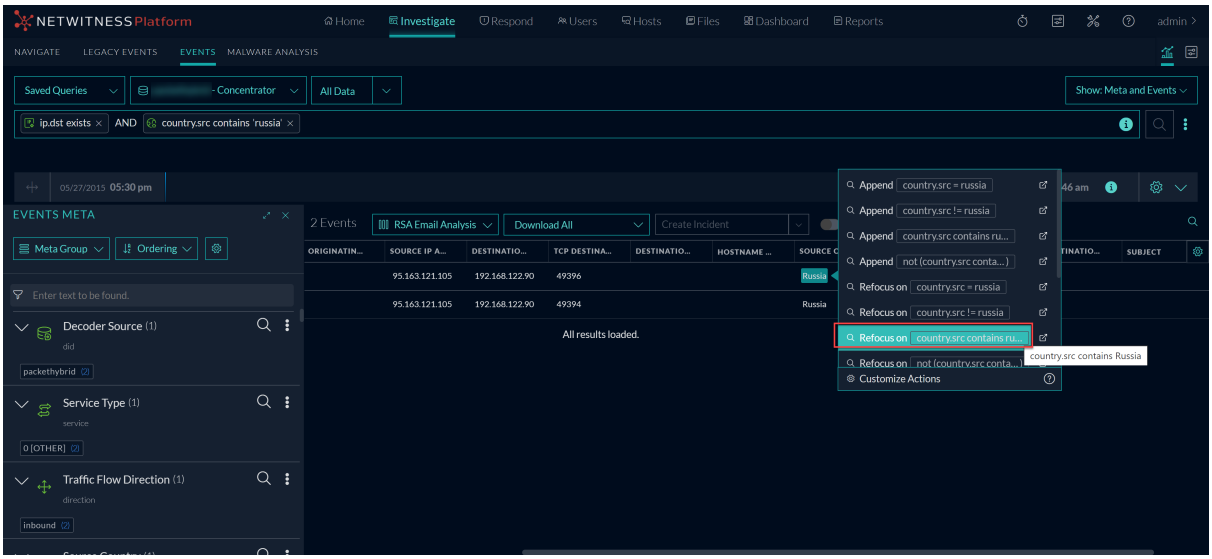
ドリルダウンのフォーカスが選 択 内 容 に応 じて再 設 定 され、 [イベント]パネルで新 しいクエリが実 行 されます。

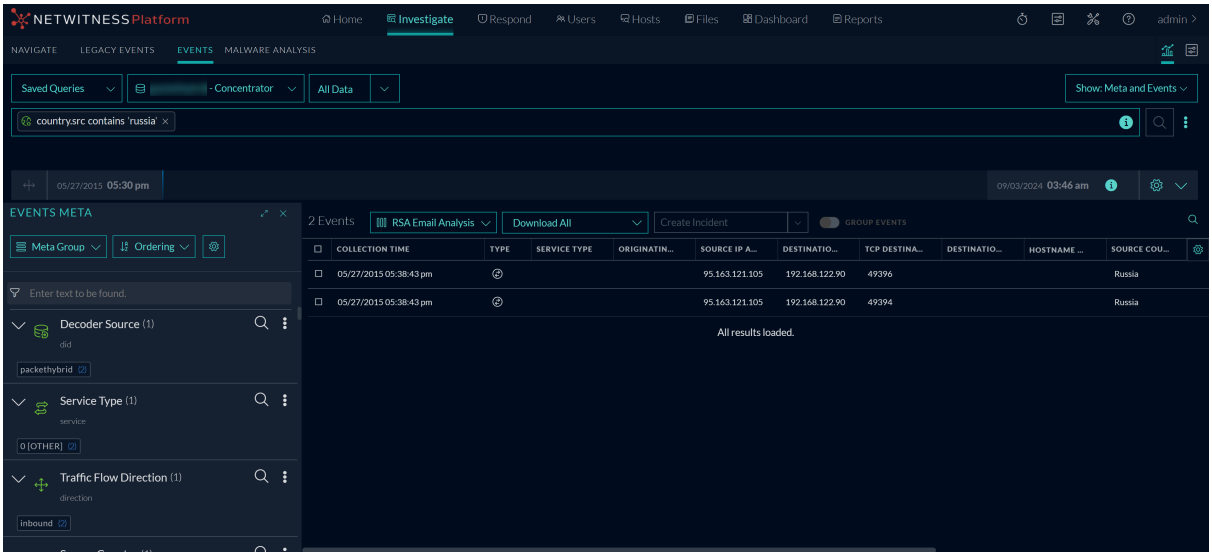
5. **追 加**]を使 用 してメタ値 を選 択 する(「メタ」にはメタ値 が含 まれます) と、表 示 される検 索 結 果 内 の新 しいクエリー フィルターとともに、既 存 のクエリーが更 新 されます。



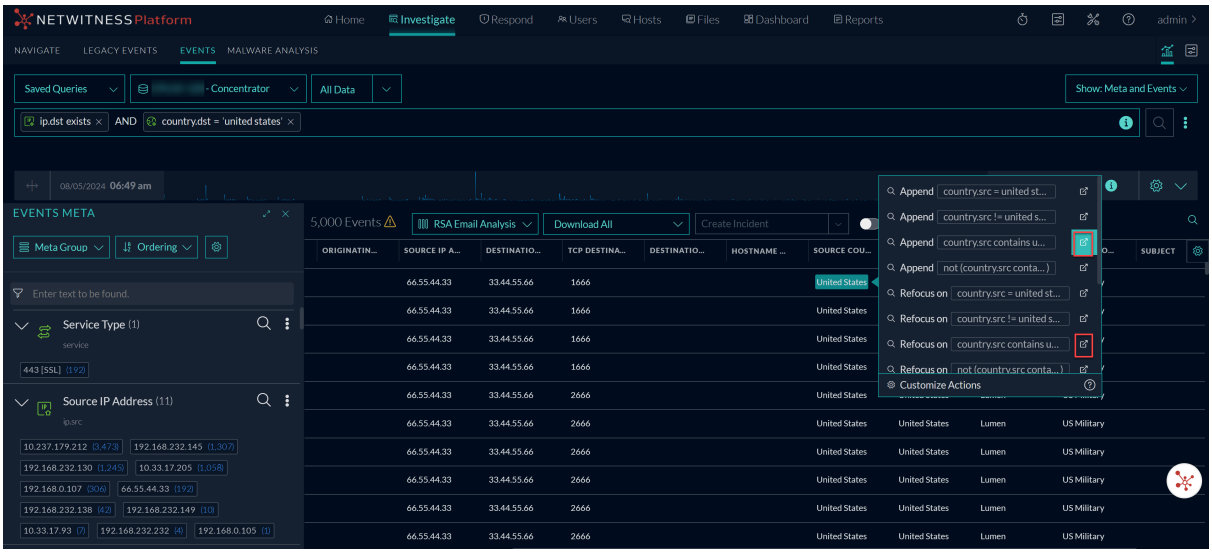


6. [**再フォーカス**]を使用してメタ値を選択する(「メタ」にはメタ値が含まれます)と、既存のクエリーが検索結果から削除され、指定したメタ値の結果が表示されます。





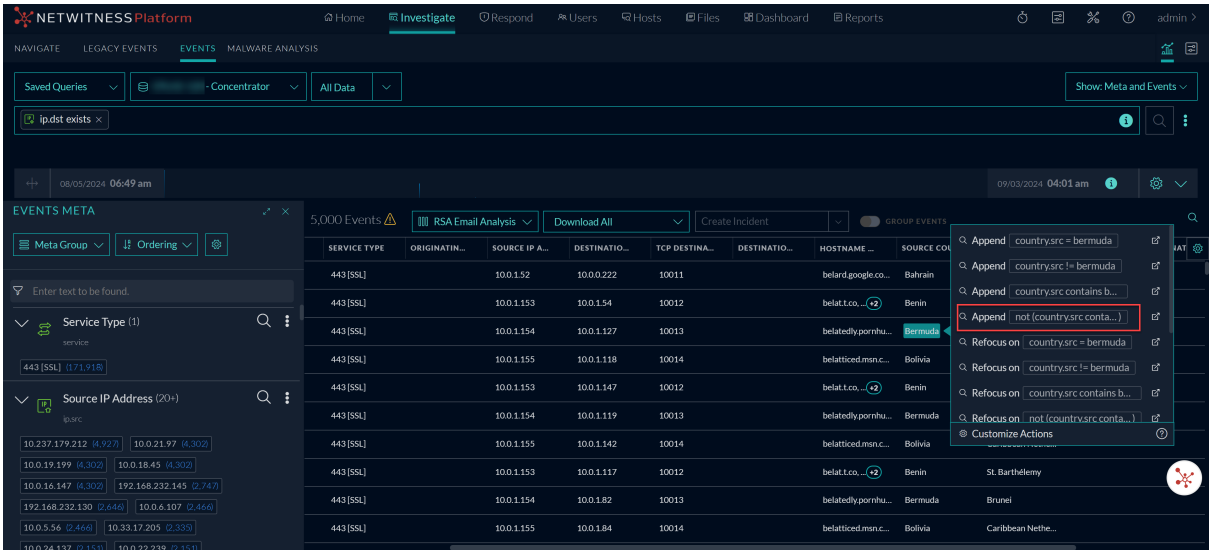
7. また、下に示す新規タブオプションを使用して、contains［含める］オプションでメタ値の追加および再フォーカスを実行することもできます。

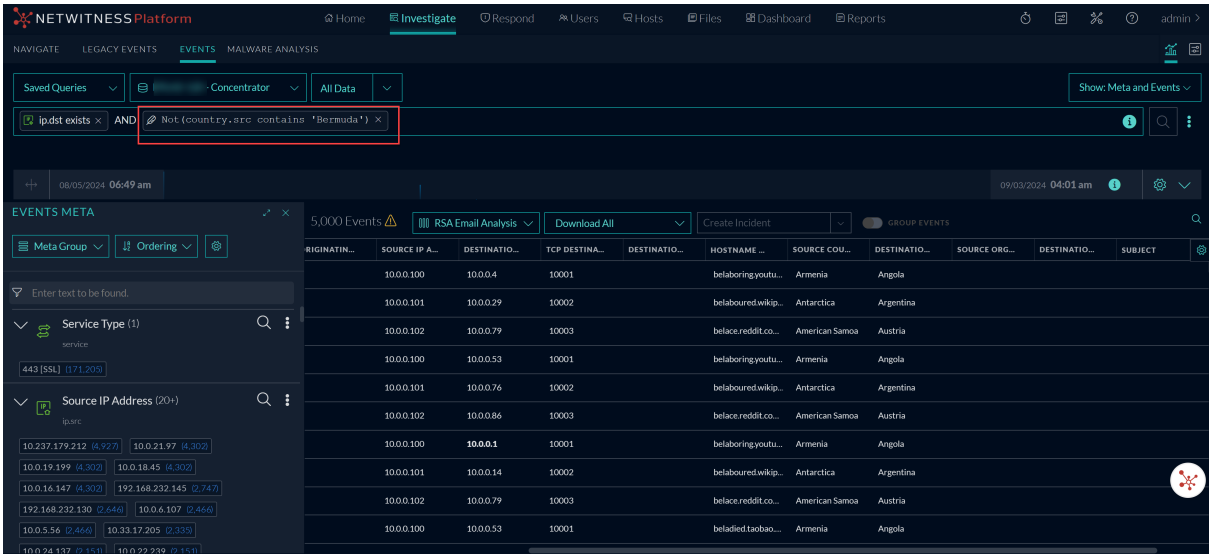


統合の調査のパネルにある［NOT］(「メタ」にはメタ値が含まれます) オプションを使用してアナリストがクエリーを実行するときに、特定のメタ値を除外できるようになりました。NOT(‘メタキー’ contains ‘メタ値’) が［**追加**］または［**再フォーカス**］オプションで使用された場合、指定したメタ値がクエリー結果から削除されます。特定のメタ値に対して、［追加］または［再フォーカス］オプションで［NOT］(「メタ」にはメタ値が含まれます) を使用しないと、指定したメタ値がクエリー結果から削除されます。この機能拡張によりアナリストは、必要なデータ結果を最適化された方法で表示できるだけでなく、より詳細な調査を効率よく実施することができます。

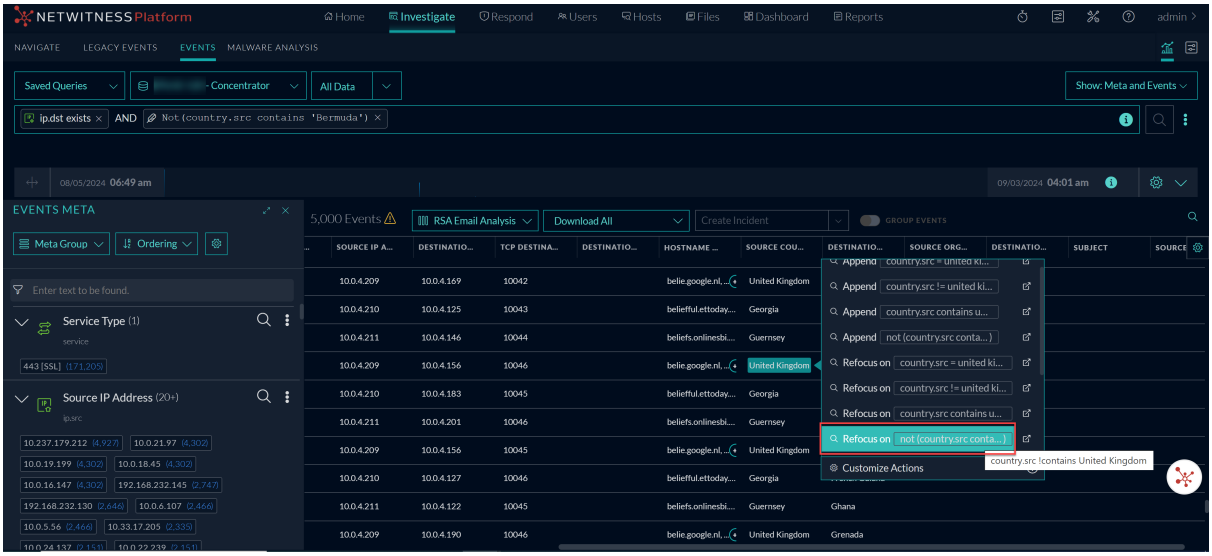
［イベント］ビューでは、特定のメタ値を左クリックまたは右クリックし、ドロップダウン メニューのオプションを使用することで、イベント内のメタ値をさらに調査できます。

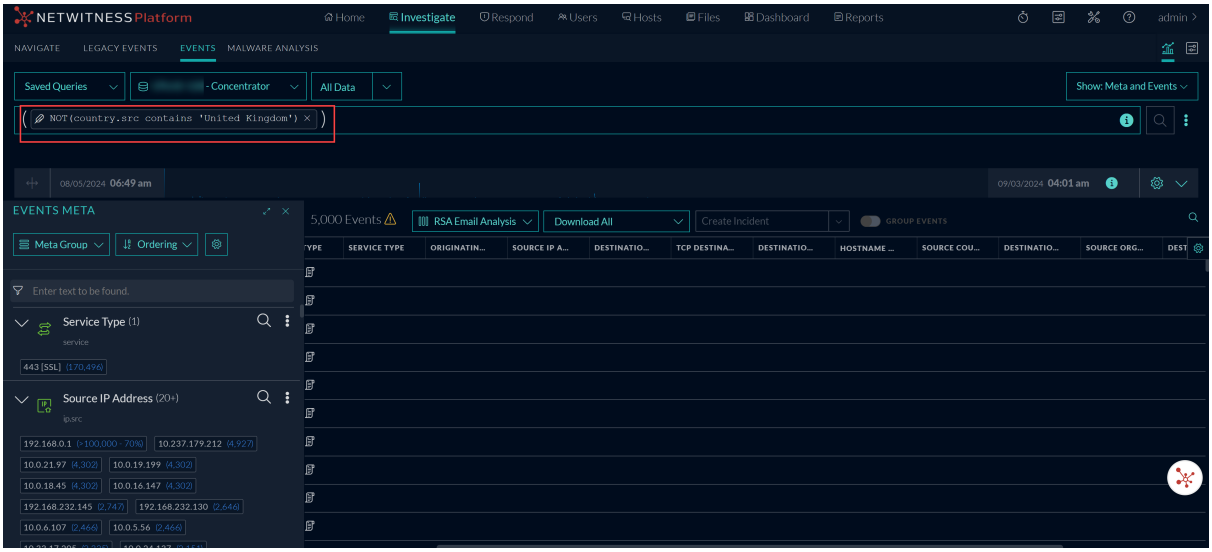
1. **Append** NOT(「メタ」にはメタ値 が含 まれます) を使 用してメタ値を選 択 すると、特 定 のクエリーが削 除され、新 しいクエリー フィルタが追 加されて、NOTにメタ値 が含 まれる結 果となります。



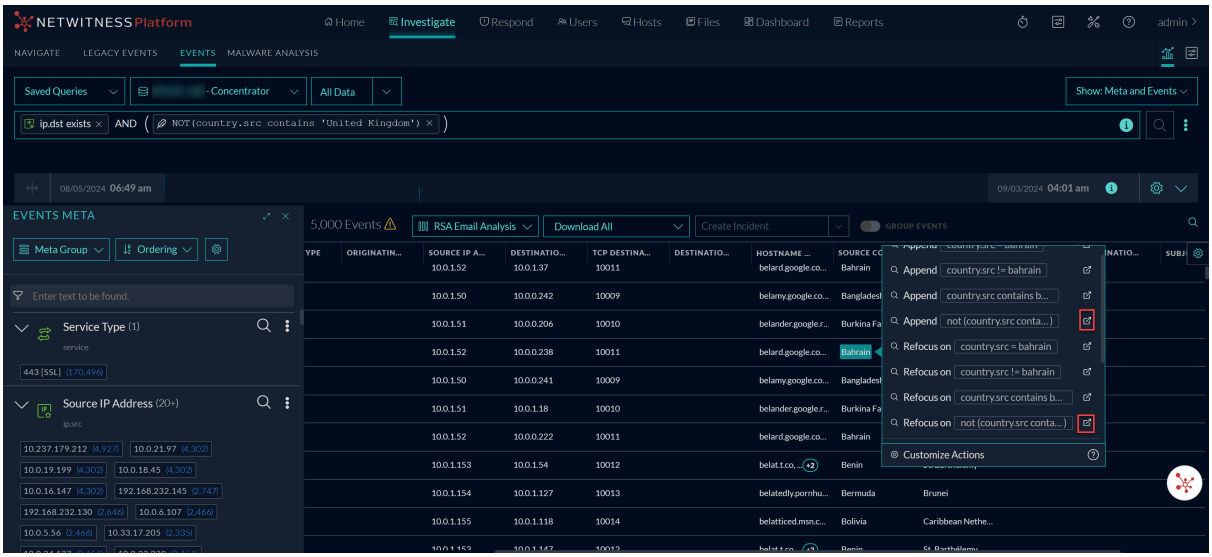


2. Refocus NOT (‘メタキー’ contains ‘メタ値’)を使用すると、特定のメタ値が削除された結果が表示されます。 **再フォーカス**<と [NOT](「メタ」にはメタ値が含まれます) を使用してメタ値を選択すると、検索クエリーの結果から、特定のメタ値が削除されます。





3. また、下に示す新規タブオプションを使用して、 [含めない]オプションでメタ値の追加および再フォーカスを実行することもできます。


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
NAVIGATE
LEGACY EVENTS
EVENTS
MALWARE ANALYSIS
Saved Queries
- Concentrator
All Data
Show: Meta and Events
ip.dst exists
AND
NOT(country.src contains 'United Kingdom')
08/05/2024 06:49 am
09/03/2024 04:01 am
EVENTS META
5,000 Events
RSA Email Analysis
Download All
Create Incident
GROUP EVENTS
Meta Group
Ordering
Enter text to be found.
Service Type (1)
service
443 [SSL] (170,496)
Source IP Address (20+)
ip.src
10.237.179.212 (4,927)
10.0.21.97 (4,302)
10.0.19.199 (4,302)
10.0.18.45 (4,302)
10.0.16.147 (4,302)
192.168.232.145 (2,747)
192.168.232.130 (2,646)
10.0.6.107 (2,466)
10.0.5.56 (2,466)
10.33.17.205 (2,335)
ORIGINATIN...
SOURCE IP A...
DESTINATIO...
TCP DESTINA...
HOSTNAME ...
Append country.src != bahrain
Append country.src contains b...
Append not (country.src conta...)
Refocus on country.src = bahrain
Refocus on country.src != bahrain
Refocus on country.src contains b...
Refocus on not (country.src conta...)
Customize Actions

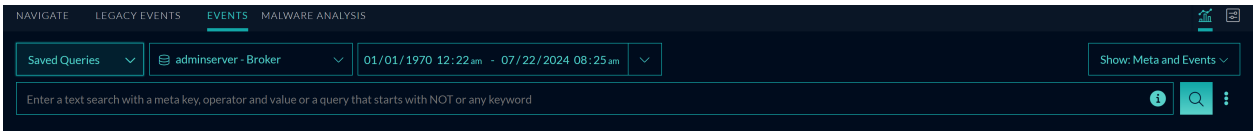
[イベント]ビューでの結果のフィルタリング

[イベント]ビューで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]ビューでイベントをフィルタリングするには、 [メタ イベント]パネル、クエリ バーの各オプション、および [イベント]パネルの各オプションを使用します。

クエリ バーを使用した初期フィルタ

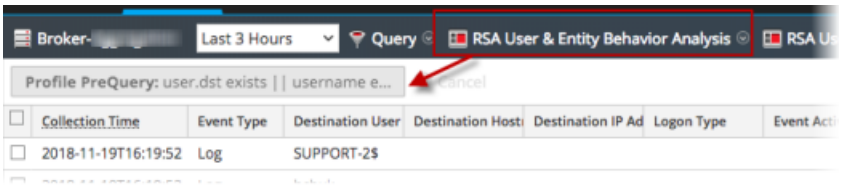
最初に [イベント]ビューを開いたときの最も基本的なフィルタリングは、サービスと時間範囲を選択してから、クエリ バーでサービスにクエリを実行することです。これにより、一致するイベントのリストが [イベント]パネルに返されます。また、クエリ プロファイルを選択し、クエリを作成して、特定のメタ キー、メタ値、テキストを含むイベントをクエリ バーで探すこともできます。

次の図は、ガイド モードとフリーフォーム モードが不要になったクエリ 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。



- プロファイルにクエリと列グループをカプセル化することで、有用な属性の組み合わせを簡単に呼び出して、イベント パネルの一連のイベントに適用することができます (「 保存済みクエリを使用した調査の共通領域のカプセル化 」を参照)。
- デフォルトで、最初のサービスが自動的に選択されます(以前にサービスを選択し、そのサービスがブラウザのキャッシュに存在する場合を除く) 。「 [イベント]ビューでの調査の開始 」の説明に従って、サービスを選択することもできます。
- 時間範囲を選択しない場合は、デフォルトの時間範囲(24時間) が使用されます。
- クエリ ビルダ フィールドは、時間範囲セレクターの右側にある空のフィールドです。ここでは、フィルタを作成することによってクエリを作成します。 をクリックすると、クエリが送信され、選択したサービスにデータ ロード要求が送信されます。 (**クエリ コンソール**) > **現在のクエリ** タブをクリックすると、現在のクエリの詳細なステータスが表示されます (以下の [イベント]ビューでの結果のフィルタリング を参照)。
- [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、フィルタがクエリー 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

りと、［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。



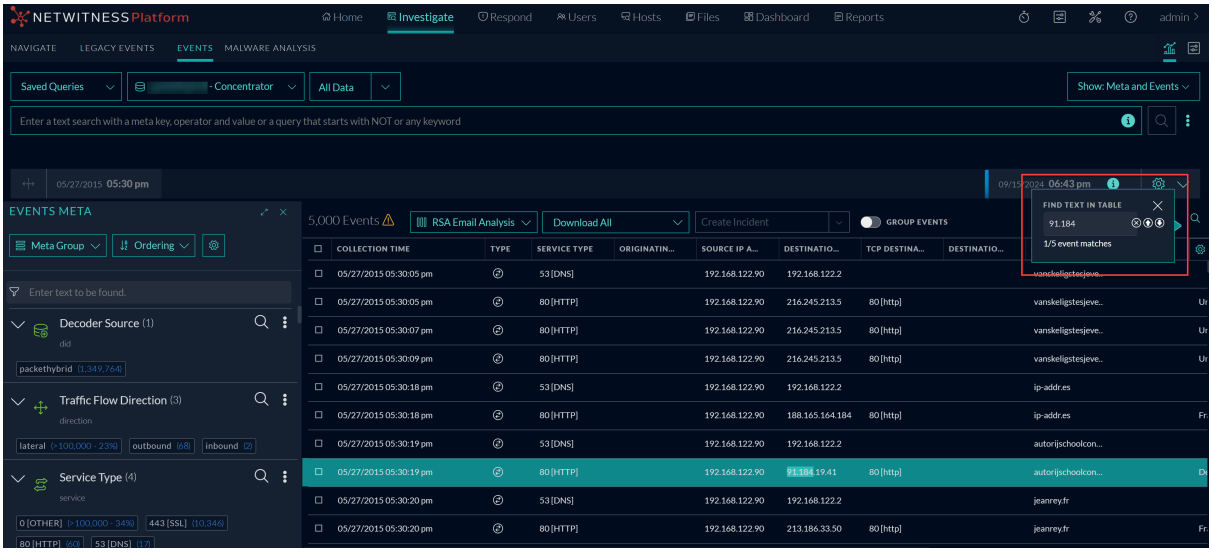
［イベント］パネルでのテキスト文字列の検索

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

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



2. ［テーブルでテキストを検索］ダイアログで、テキスト文字列を入力し始めます。
2文字を入力したところで、そのテキスト文字列の完全一致(大文字と小文字は区別しない)が［イベント］パネルでハイライト表示されます。テキストの入力を続けると、ハイライト表示されたイベントがさらに絞り込まれます。次の図は、［テーブルでテキストを検索］ダイアログで「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352個のイベントで検出されました。最初のイベントは青色でハイライト表示され、そのイベント内のテキスト文字列もハイライト表示されます。アイコンを使用して検索結果をナビゲートし、ダイアログを閉じることができます。



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

[イベント]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。

- 列グループを使用すると、特定のイベントで確認する数や属性 (メタキー、メタグループ、メタエンティティ) を最適化できます (「 イベント リストでの列と列グループの使用」を参照)。
- イベント メタ パネルの結果でメタ キーとメタ値を調べることで、イベントをフィルターできます。これにより、 [ナビゲート]ビューで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。

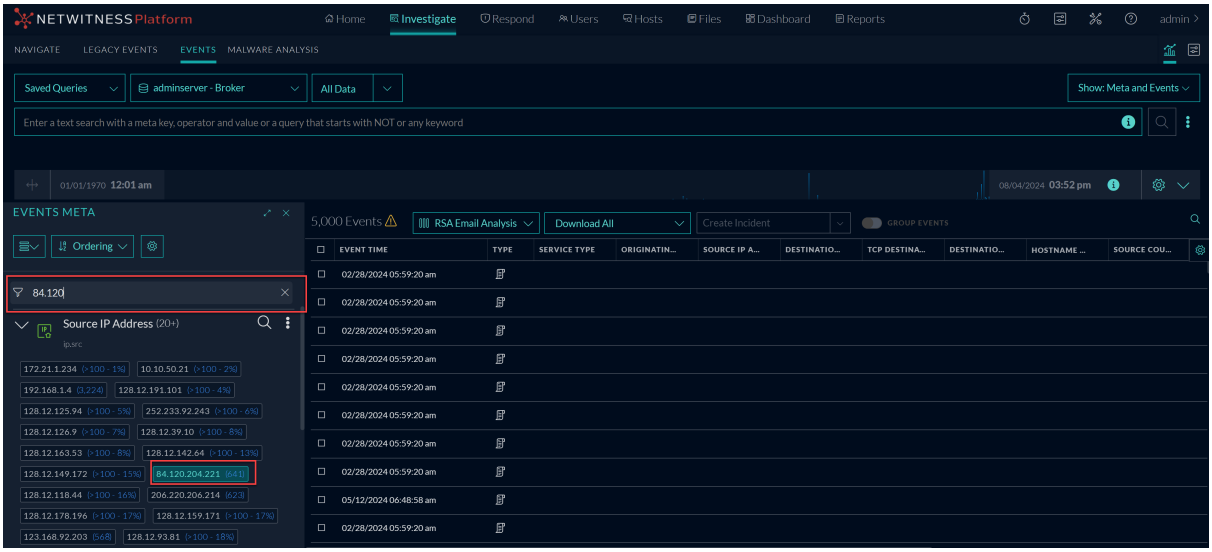
[イベント メタ]パネルを使用したメタ情報の絞り込み

アナリストは、新しく追加されたフィルター オプションを使用して、イベント メタ パネルからメタ キーとメタ値をフィルターできます。この機能強化により、アナリストは、特定のメタ値またはキーを入力して検索結果を絞り込むことができ、メタデータの長いリストをスクロールすることなく、シームレスに調査できるようになります。

[イベント メタ]パネルでメタ キーまたはメタ値を絞り込むには

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。
   選択したサービスと、選択した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 メタ]パネルを表示するには、「イベント」パネルの前に **[フィルタ]**をクリックします。
   [イベント]パネルの左側で [イベント メタ]パネルが開きます。
3. リストに表示されたメタ値またはメタ キーを名前で絞り込むには、 [フィルタ]フィールドにテキストを入力します。リストが更新されて、完全に一致するテキストを含むグループ名のみが、青の背景で

強調されて表示されます。



クエリー ビルダーの概念

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'`.

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`のフィルターを入力または貼り付ける場合は、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'`

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。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、バージョン12.5のクエリ バーをそれぞれ示しています。



- メタ キー、演算子、値のシーケンスを入力し、Enterキーを押すことなく入力を続けた場合、自動的にフリー フォーム モードのオプションが有効になり、クエリの入力を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 オプションが強調表示され、最後にEnterキーを押すと、クエリ バーにフリーフォーム フィルターが作成されます。
- テキスト フィルター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。

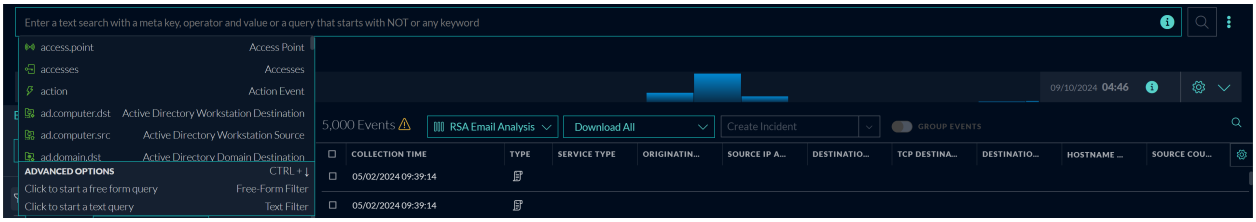
注 :メタ キーと演算子のステートメントとほぼ一致するテキスト フィルタを入力しているときに、そのメタ キーと演算子を使用するフィルタが自動提案機能によって誤って提案されることがあります。この問題を回避するには、テキストの入力を開始し、自動提案機能によってテキストがメタ キーと演算子に変換されるポイントで ［テキスト フィルタ］を選択します。たとえば、cryptoというメタ キーとcontainsという演算子がある場合に、cryptocurrencyを検索するテキスト フィルタを作成するとします。この場合、「c-r-y-p-t-o」と入力し、それに続く「currency」の「c」を入力すると、contains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。

ガイド モードとフリーフォーム モード

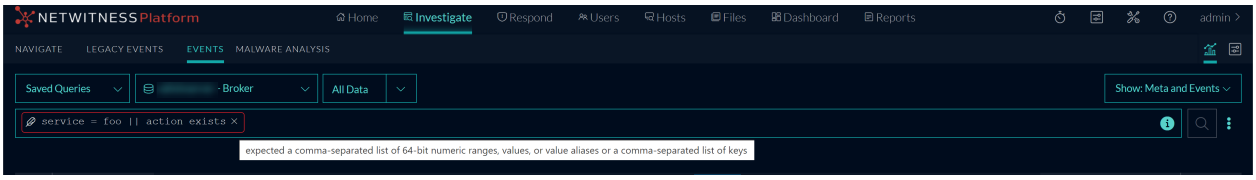
注 : NetWitnessでは、フィルター入力フォームにクエリを入力するための2つのモードが提供されています。ガイド モードとフリーフォーム モードが用意されていました。ガイド モードの強力なオートコンプリート機能および値候補表示機能と、フリーフォーム クエリを入力またはペーストする機能が完全に統合されました。このドキュメント内のガイド モードとフリー フォーム モードを区別する参照はアナリスト向けです。

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。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。これはフィルター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。

自由形式のフィルターはサーバー側で検証されるため、追加の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。

[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。

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。

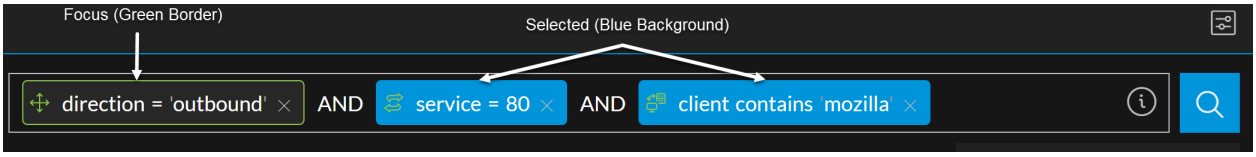


次の図は、フリーフォーム クエリ ビルダ使用中の例です。



複数のフィルタの編集に関する概念

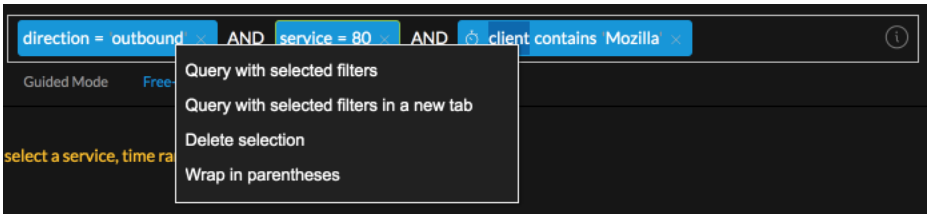
クエリ ビルダで作業する際は、編集のフォーカスがあるフィルタは緑色の枠線がマークされ、選択中のフィルタには青色の背景が表示されます。この機能は、右クリック アクションに対して複数のフィルタを選択できる点で便利ですが、一度に編集できるフィルタは1つだけです。次の図は、フォーカスされたフィルタが緑色の枠線でマークされ、選択中の2つのフィルタが青色の背景で表示されている状態を示しています。



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。

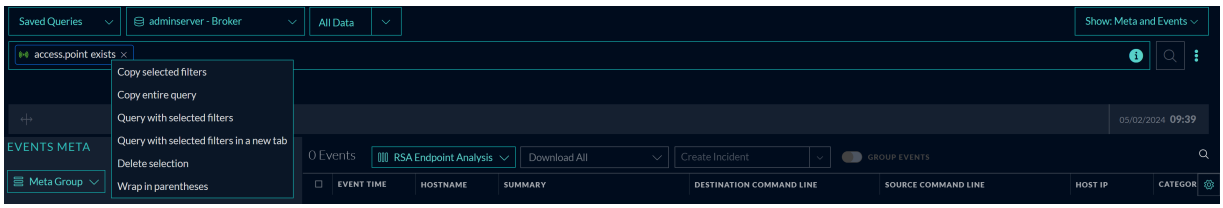


ドロップダウン メニューの右 クリック アクションは、選 択したすべてのフィルタに適 用されます。次 の図 はオプションを示しています。



次 の図 に示 すように、メニューには2つの新 しいコピー オプションがあります。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。
- フィルタがユーザーの入 力 を待 っている場 合 は、フィルタがティール色  でハイライト表 示 されます。



- 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。

クエリビルダー

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。ガイド モード フィルター入力フォームに追加された機能については、以下で詳しく説明します。

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

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

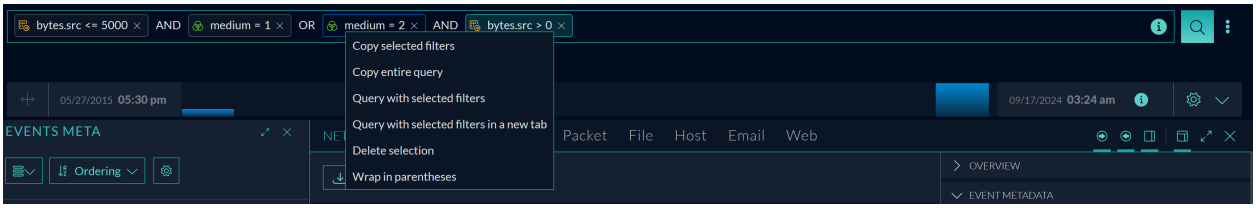
フィルタ入力フォームでは、メタ キー、演算子、値を入力する方法として、［メタ］タブと［最近のクエリ］タブの2つが用意されています。［メタ］タブは、以前のバージョンのフィルタ入力フォームと同じですが、条件に一致するメタ キーの数が［メタ］タブのラベルに表示されるようになった点と、各メタ キーのアイコンにより、キーでインデックスされているか、値でインデックスされているか、インデックスされていないかが表示されるようになった点が異なります。［最近のクエリ］タブには、最大100個の最近のクエリが表示されます。リストは入力されたテキストによって絞り込まれ、入力されたテキストを含んだクエリのみが表示されます。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 インタフェースに表示されます。最大100個の候補値が返されます。テキストを入力すると、100個の値のリストが絞り込まれ、一致する値のみがリストに表示されます。一致する値が返されない場合は、"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スペースを空ける必要はありません

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

時間範囲を選択

［時間範囲］セレクターは、［イベント］ビューに返されるイベントを特定の時間範囲に制限します。時間範囲は、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。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。

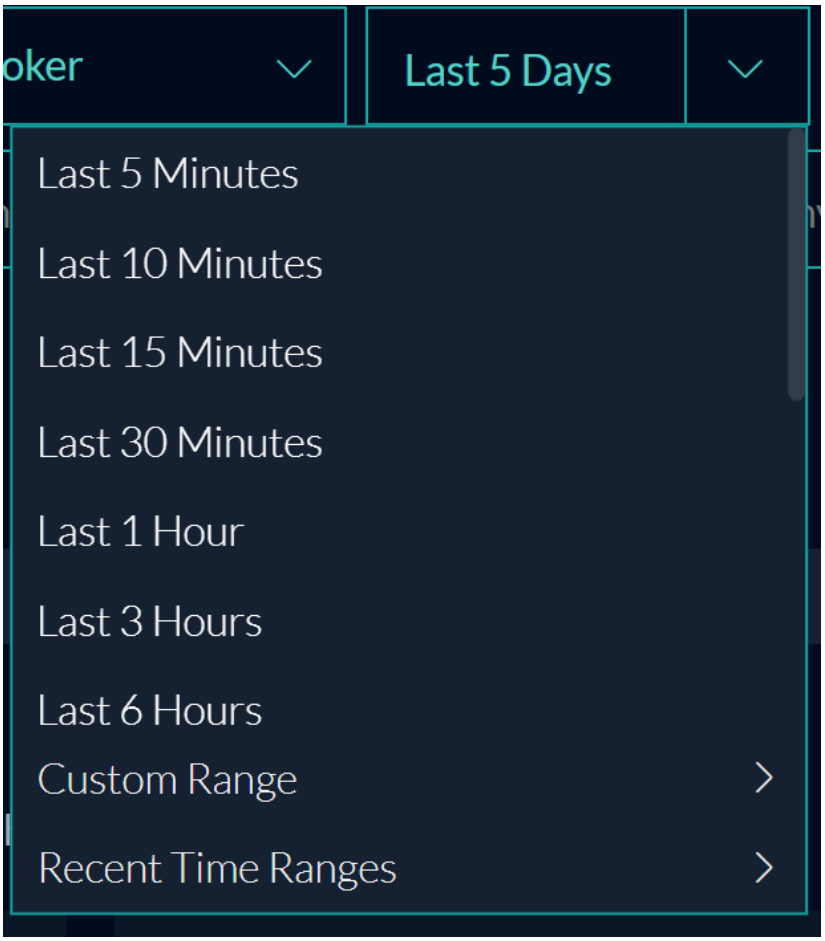
- デフォルトの日付形式は、MM/DD/YYYYです。この形式は、［ユーザ環境設定］ダイアログでDD/MM/YYYYまたはYYYY/MM/DDに変更できます。
- 開始時間と終了時間はHH:MM形式で指定します。秒は表示されませんが、開始時間の値は常にHH:MM:00秒に、終了時間の値は常にHH:MM:59秒にデフォルトで設定されます。たとえば、「6:45 pm - 7:45 pm」という時間範囲は「06:45:00 - 07:45:59 pm」として解釈されます。
- デフォルトの時間範囲は24時間制です。12時間制に変更することができます。

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て、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(を選択) の設定に基づきます。時間形式は、データベースの時間または現在の時間のどちらかに設定することができます。［データベースの時間］を選択した場合は、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。

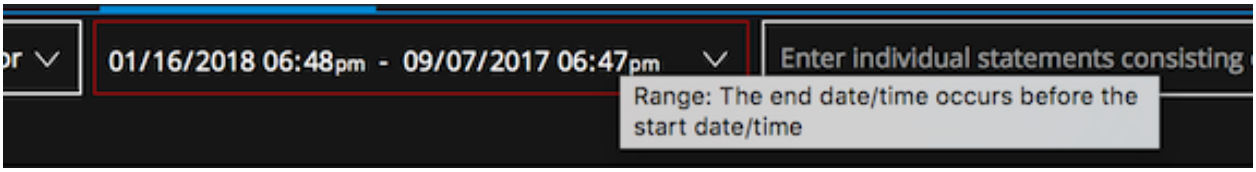
1. ［**時間範囲**］セレクターの内側にあるドロップダウン矢印をクリックして、リストから時間範囲を選択します。分単位、時間単位、日単位のオプションを選択するか、すべてのデータを選択できます。



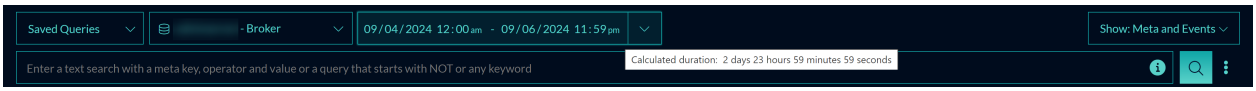
クエリ バーに表 示されている年 、月 、日 、時 間 、分をクリックして、時 間 範 囲を直 接 編 集します。値 がハイライト表 示されたら、開 始 時 間 または終 了 時 間 のいずれかの新しい値を入 力します。時 間 形 式の環 境 設 定 が12時 間 制 に設 定されている場 合 は、 [**午 前**]または [**午 後**]をクリックして2つのオプションを切り替 えます。



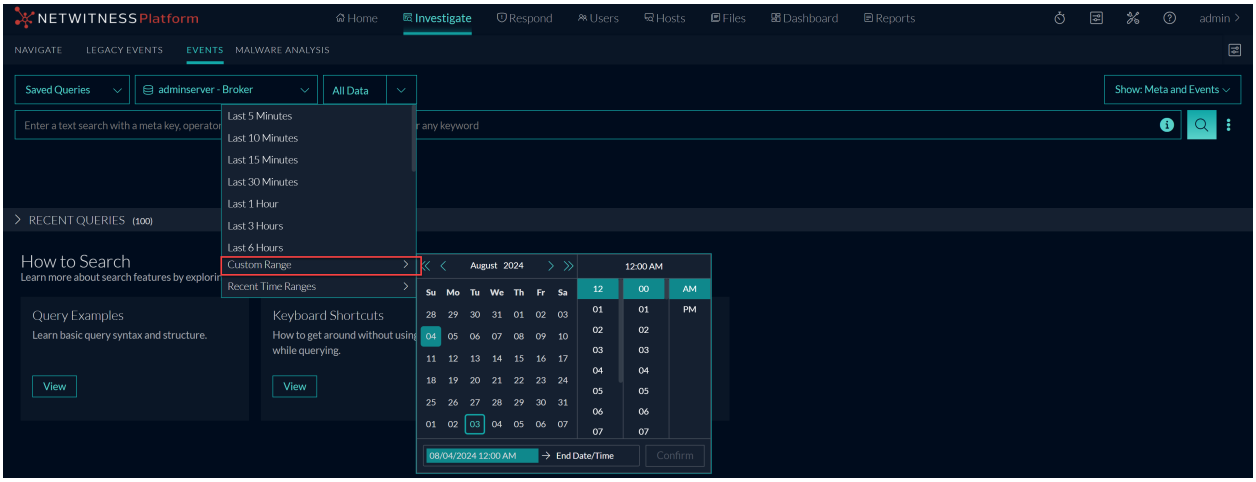
時 間 範 囲が無 効な場 合 (開 始 時 間 が終 了 時 間 よりも後 である場 合 など) は、時 間 範 囲 セレクターに赤い枠 線 が表 示されます。クエリが不 可 能になったため ボタンが無 効 化 され、何を変 更する必 要があるかを説 明したエラー メッセージがツールチップに表 示されます。次 の図 は、時 間 範 囲が無 効な状態を示しています。



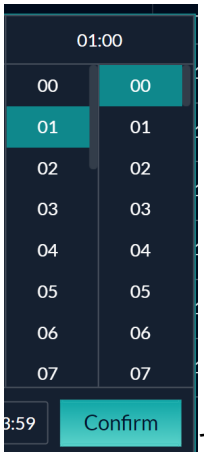
選 択した時 間 範 囲は、クエリの対 象 となるサービスごとにブラウザに保 存されます。サービスごとに異なる時 間 範 囲を設 定できます。ツールチップには、計 算されたクエリ期 間 が表 示されます。次 の図 にツールチップの例を示します。

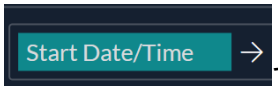


既存のオプションに加えて、[イベントの調査] ビューの **[カスタム範囲]** オプションを使用すると、アナリストは特定の時間、日付、月、年、または日付範囲を選択してクエリを実行し、イベントをフィルター処理できます。 **[カスタムの範囲]** オプションをクリックすると、現在の日、時間、日付の詳細を含むカレンダー ビューが表示されます。この機能拡張により、アナリストが手作業で入力することなく、すばやく日時を選択できるため、人為的なエラー(入力ミス) が防止されます。

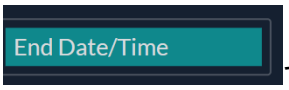


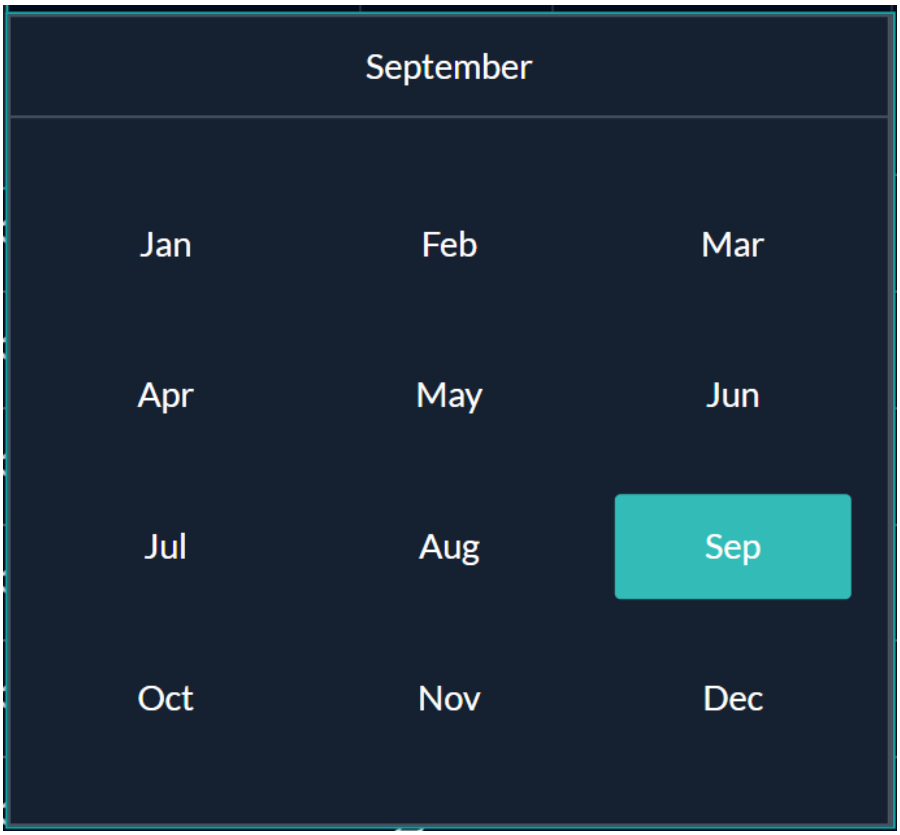
アナリストは、以下を使用してカレンダー内を移動できます。

-  と  で月を切り替える。
-  と  で年を切り替える。
- 

で、特定の時間を選択する。
- 

で開始日時を選択する。

- 

で終了日時を選択する。
- 

- で、年と年の範囲を選択する。
- [確認]をクリックして選択内容を保存します。

クエリの送信

クエリー バーの右側にある  ボタンは、クエリーを送信する必要がある場合はアクティブになります。クエリにはAND以外の演算子が含まれる場合があるため、クエリはそのまま送信されます。  ボタンは、以下の場合に再びアクティブになります。

- クエリ バーでサービスを変更するか、[イベント]パネルで列グループを変更した時。[イベント]パネルの再構築のためのデータをネットワーク経由で取得する場合、新しいクエリを送信するまでは、以前のサービス、時間範囲、およびメタデータ フィルタが引き続き使用されます。  ボタンは、ビュー内のデータが古くなっていることを示すインジケータとしてアクティブになります。
- 1分以上経過し、元のクエリの時間範囲で同じ結果セットが生成されなくなった場合は、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ーとして  ボタンがアクティブになります。イベント ビューの設定で、[相対時間ウィンドウを自動的に更新]オプションを有効または無効にすることで、この動作を決定します(「[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。"

クエリーのステータスの表示

クエリーを送信した後は、クエリー バーで [**クエリー コンソール**] アイコン( ) > [**現在のクエリー**] をクリックして、クエリー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、クエリーのステータスと、照会されたサービスに関するリアルタイム情報も確認することができます。クエリー 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。"2024-09-02 08:51:00" - "2024-09-03 08:50:59".)

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クエリ コンソールに表示される情報の例です。クエリがメタ フィルターとして表示されていることに注意してください。



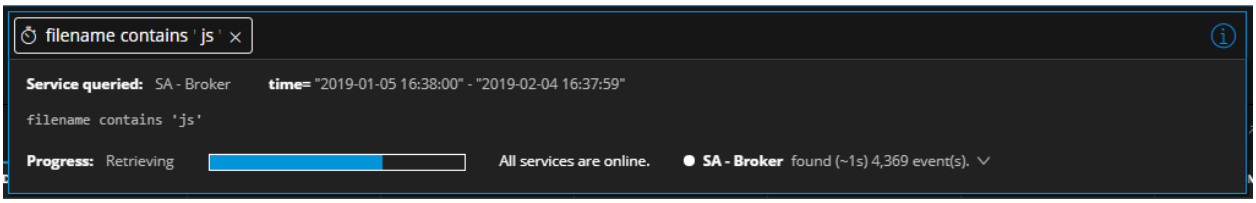
クエリが実行されている間、コンソールの下部にある進行状況バーには、クエリの完了率が表示されます。ステータス情報からは、クエリで今行われている処理(実行中、キューに登録済み、クエリ対象サービスのインデックス ファイルの読み取り中、イベントの取得中、完了など) についての詳細を知ることができます。ステータスと致命的でないメッセージは受信するとすぐに表示され、致命的でないエラーの場合は、クエリ バーの枠線が黄色に変わります。

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。

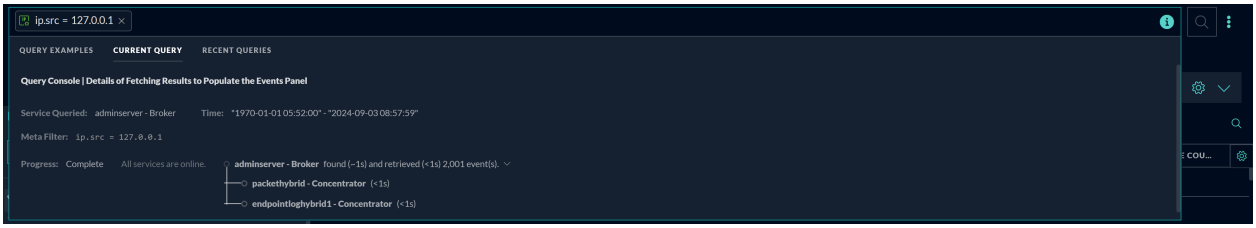
イベントを検索するための実行とインデックス ファイルの読み取り。クエリの最初のステージは、クエリ対象サービスで結果が見つかったときに完了します。クエリ コンソールでは、クエリ対象のすべてのサービスがネスト構造の階層リストに表示され、どのサービスがオンラインかオフラインかを示すインジケータ、各サービスが結果を見つけるまでに要した時間(秒単位) も表示されます。

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。



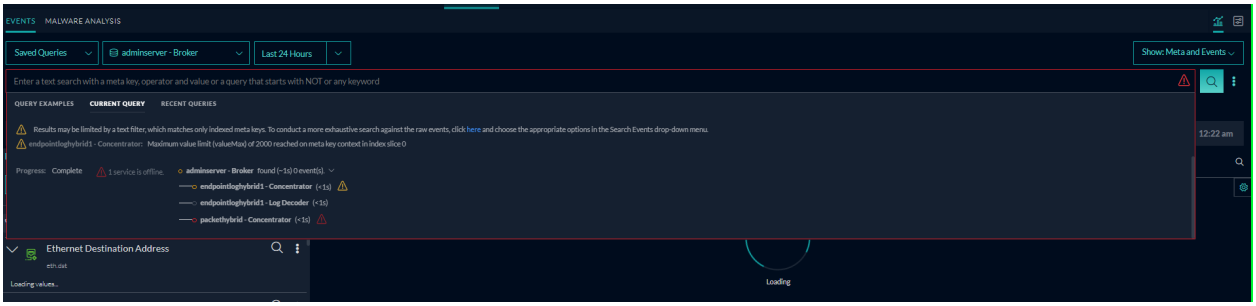
要求の完了。エラーまたは警告なしでロードが完了した場合、クエリコンソールの枠線は青色になり、

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。

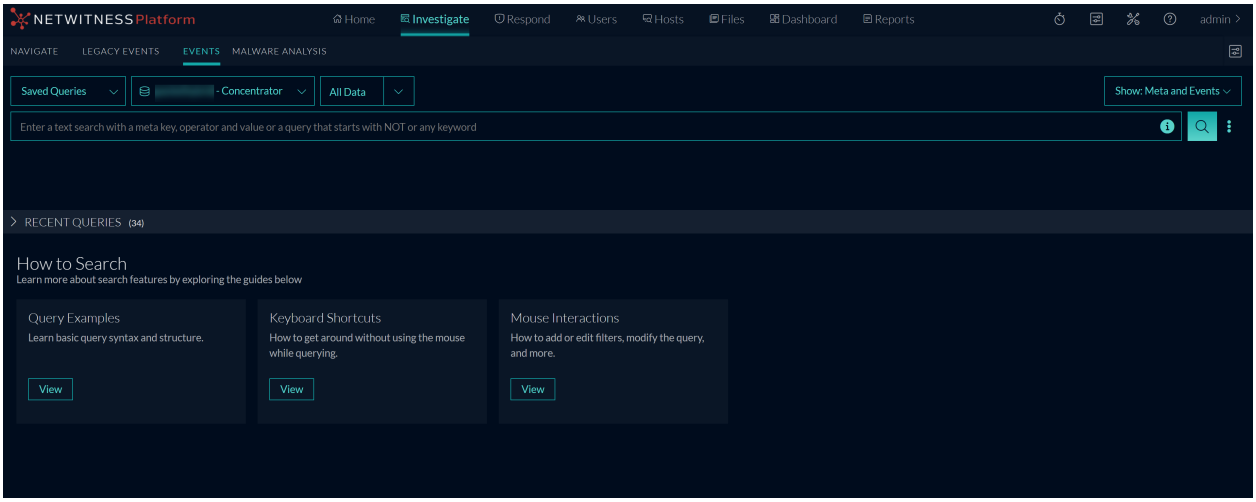
致命的でないエラーが発生しても、クエリの実行は妨げられません。クエリは実行され、イベントはロードされますが、クエリコンソールの右上隅に赤い三角形が表示され、警告を示す赤い枠線が表示されます。次の図は、クエリ対象サービスが別のオフライン状態のサービスのプロキシになっている場合に表示されるクエリコンソールの例です。



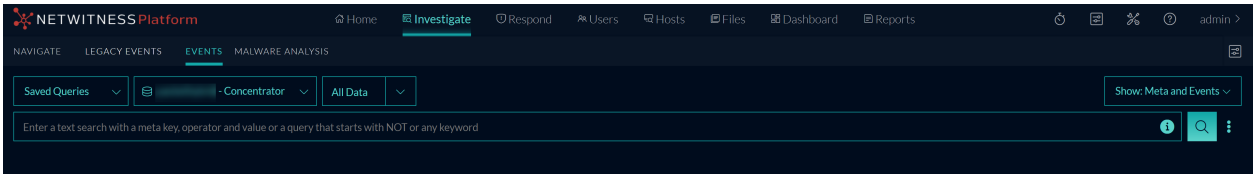
警告が発生しても、クエリの実行は妨げられません。クエリは実行され、イベントはロードされますが、クエリコンソールの右上隅に黄色の三角形が表示され、黄色の枠線が表示されます。

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 バーで有効になっている、ガイド モードの最初の［イベント］ビューの例です。



次の図は、クエリ バーを示しています。



ガイド モードで使用するキーボード操作

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

アクション	キーボードへの入力
すべてのフィルターをコピー	クエリ バー(ただし、編集中のフィルタ以外) にカーソルを合わせ、すべてのフィルタが選択された状態で、**Ctrl-C** (Windows OS)または**Cmd-C** (MacOS)を押します。
フィルタ内の文字を削除する	選択した文字 :クエリ バーで文字を選択し、**Delete**または**Backspace**キーを押します。 前のキャラクター: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。 全文字: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。

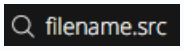
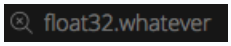
アクション	キーボードへの入力
フィルタを削除する	選択したフィルタ :1つ以上のフィルタを選択し、次のいずれかを実行します。 • **右クリックして> 選択内容を削除します**。 • **削除を押します**。 • **Backspace** キーを押します。 フォーカスのあるフィルター:フォーカスしているフィルタにカーソルを合わせ、**Backspace**(Windows OS) または**Delete**(MacOS) キーを押します。フォーカスしたフィルタが削除され、フォーカスが左側に移動します。 フォーカスのあるフィルター:フォーカスしているフィルタにカーソルを合わせ、**Delete**(Windows 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。
フィルタ内の括弧を削除しますが、内容は削除しません	括弧のセットがあり、内容が選択されていない場合は、**Delete** (Windows OS) または **Fn** + **Delete** (MacOS) を押します。選択した括弧が削除されますが、括弧の中身は残ります。
フィルター内の括弧とその内容を削除する	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。 • **右クリック> 選択項目を削除**]を選択します。 • **Backspace**(Windows OS) または**Delete**(MacOS) を押します。選択した括弧とその中身が削除され、フォーカスが左側に移動します。 • **Delete**(Windows OS) または**Fn** + **Delete**(MacOS) を押します。選択した括弧とその中身が削除され、フォーカスが右側に移動します。
すべてのフィルタの選択を解除する	フィルタを選択した状態で、**Esc**を押します。
選択したフィルタを編集する	単一のフィルタを選択した状態で、**Enter**を押します。
クエリバーの先頭に新しいフィルタを挿入して、編集用に開く	フィルターを選択した状態で、**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て、編集用に開く	フィルターを選択した状態で、**End** (Windows OS) または **Fn** + **右矢印** (MacOS) を押します。
選択したフィルタの左隣に新しいフィルタを挿入して、編集用に開く	フィルタを選択した状態で、**Shift** + **左矢印**を押します。
選択したフィルタの右隣に新しいフィルタを挿入して、編集用に開く	フィルタを選択した状態で、**Shift** + **右矢印**を押します。

アクション	キーボードへの入力
選択したフィルタの左隣に新しいフィルタを挿入する	フィルタを選択した状態で、**左矢印**を押します。
選択したフィルタの右隣に新しいフィルタを挿入する	フィルタを選択した状態で、**右矢印**を押します。
選択したフィルタを新しいタブで使用する	フィルタを選択した状態で、**右クリック**> **新しいタブで、選択したフィルタでクエリを実行**]を選択します。
選択したフィルタでクエリを実行する	フィルタを選択した状態で、**右クリック**> **選択したフィルタでクエリを実行**]を選択します。
括弧の内容を含むクエリ	括弧を選択した状態で以下を実行します。 • 選択した括弧の中身でクエリを実行するには、括弧の片側を選択して、**右クリック**> **選択したフィルタでクエリを実行**]を選択します。 • ブラウザの新しいタブを開いて、選択した括弧の中身でクエリを実行するには、括弧の片側を選択して、**右クリック**> **新しいタブで、選択したフィルタでクエリを実行**]を選択します。
クエリバーですべてのフィルタを選択する	クエリバー(ただし、編集中のフィルタ以外の場所)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	フィルターを選択した状態で、**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	フィルターを選択した状態で、**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、**左矢印**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
ティール フィルターの背景		フィルタが選択されていることを示します。
2つのフィルタ間の緑色の丸		太字のカーソルは、挿入ポイントを示します。
緑色のフィルタ枠線		単一のフィルタがフォーカスされ、編集できることを示します。複数のフィルタが選択され、このフィルタがフォーカスされている場合は、青色の背景と組み合わせて表示されます。
赤色のフィルタ枠線		フィルタが無効であることを示します。エラーを説明するツール チップが表示されます。

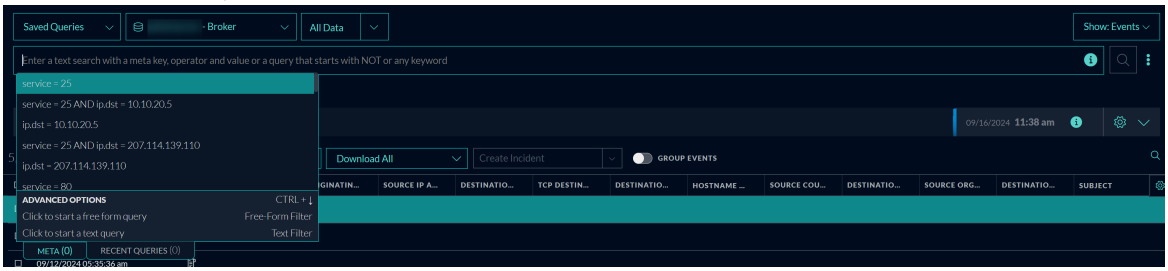
フィードバック	アイコン	説明
[メタ]タブのインデックス インジケータ		メタ タブでメタ キーのインデックス レベルを指定します。これにより、フィルターで使用できるかどうかが決まります。  このメタ キーはメタ値でインデックスされており、フィルタで使用できます。  このメタ キーはメタ キーによってインデックスされており、フィルタで使用できます。  このメタ キーはインデックスされておらず、フィルタには使用できません。 `sessionID`メタ キーは特殊なケースです。インデックスされていない他のメタ キーとは異なり、構成できませんが、フィルタで使用できるため、鍵記号が表示されます。サポ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

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

ガイド モードでのシンプルなフィルタの追加

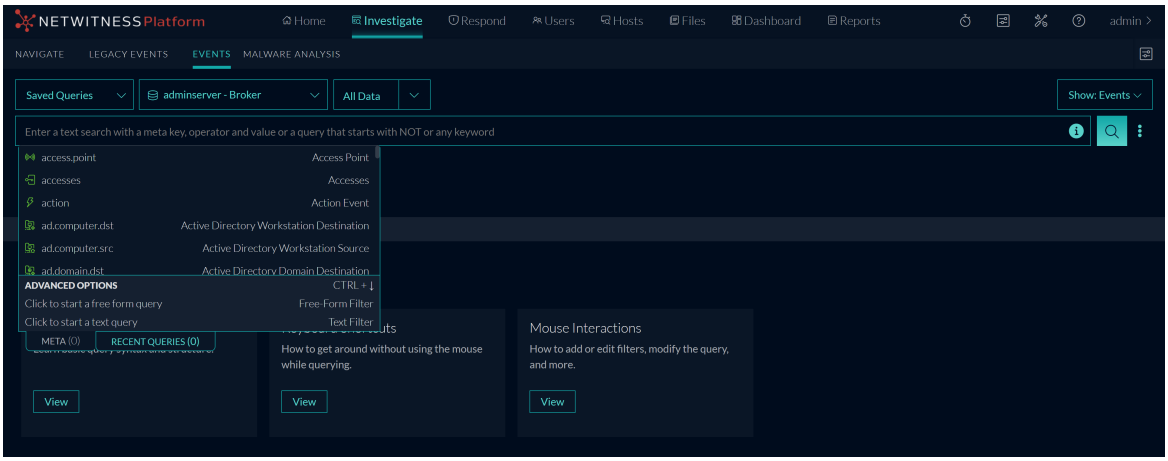
ガイド モードでシンプルなフィルタを作成するには、次の手順を実行します。

1. **イベント** ビューに移動し、次のいずれかを実行します。
   a. 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)。



挿入ポイントが2つのフィルタの間にある場合は、太字のカーソルによって挿入ポイントがマークされます。挿入ポイントがクエリ バーの最後尾にある場合は、エントリー ポイントに点滅するカーソルが表示されます。ドロップダウン リストには、調査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。この図はバージョン12.5のフィルター入力フォームを示し

ています。

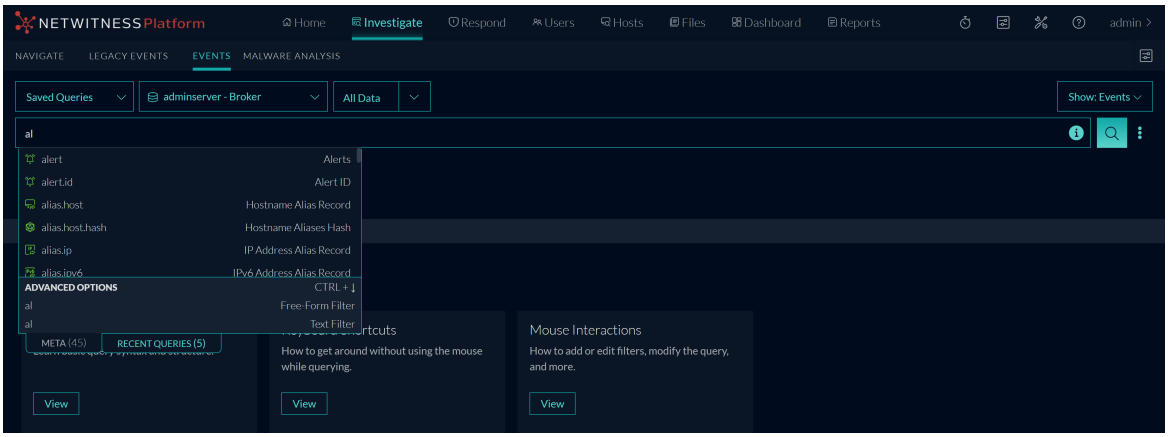


2. メタ キーを選 択するには、次 のいずれかを実 行します。

   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キーを押します**。

   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。

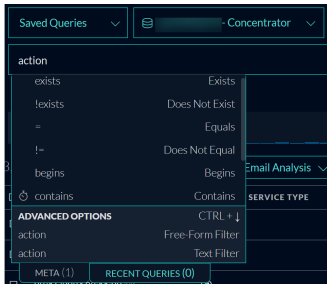
   c. メタ キーの入 力を開 始します。入 力に合 わせて、入 力したテキストを含 んだメタ キーのみが表 示されるようにリスト が絞り込まれます。 [メタ(0)]タブのラベルに表 示されるカウントは、入 力されたテキストに一 致するインデックスされたメタ キーの数を反 映して変 化します。インデックスが作 成されていないキーは無 効 化されて選 択できず、カウントには含 まれません。たとえば、次 の図のalias.macはインデックスが作 成されていないため、グレー表 示になっています。メタ キーをクリックするか、上 /下 矢 印を使ってメタ キーを選 択してから、**Enter**を押しま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



   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。`**`、`&&`、`||`、`()`、`AND`、`OR`、`comma`、`-`、`length`、`regex` 演算子は、ユーザー インターフェイスでサポートされています。フリーフォーム フィルタがハイライト表示されておらず、クエリ バーに既存のテキスト フィルタがない場合は、テキスト フィルタがハイライト表示され、作成できるようになります。
--最初の条件がtrueで、テキスト フィルタがすでに1つある場合は、フリーフォーム フィルタ オプションがハイライト表示され、フリーフォーム フィルタを作成できるようになります。

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

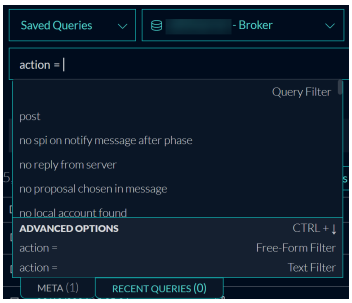


3. 演算子を選択するには、次のいずれかを実行します。

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

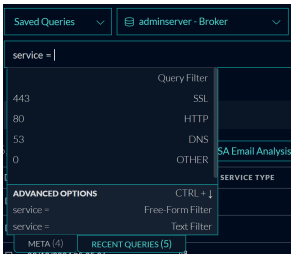
   b. 演算子ドロップダウン リストに複数のオプションがある場合は、演算子をクリックするか、上/下矢印を使って演算子を選択してから、**Enter**を押します。

   c. 演算子を手入力して、**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/下矢印を使用して演算子を選択し、**Enter** を押します。
   演算子がフィルター入力フォームに追加されます。オペレーターが値を受け入れると、推奨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。

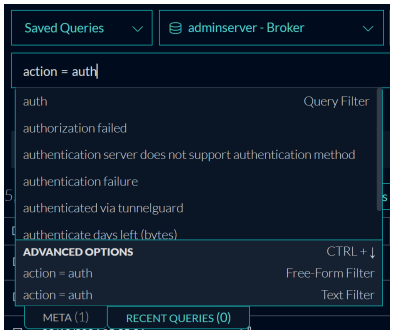


4. (オプション) フィルター入力フォームで選択した演算子が値を受け入れる場合は、次の操作を行います。

   a. 「クエリ フィルター」フィールドで入力を開始します。
   入力すると、メタ値のドロップダウン リストがフィルター処理され、入力したテキストで始まる適切にインデックス付けされた値が最大100個返されます。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。

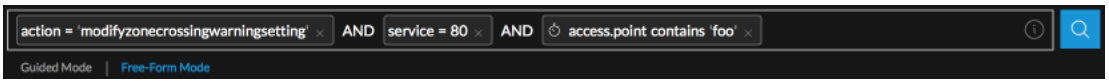
   i. 入力したテキストをフィルタで使用する場合は、**Enter**を押します。

   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。

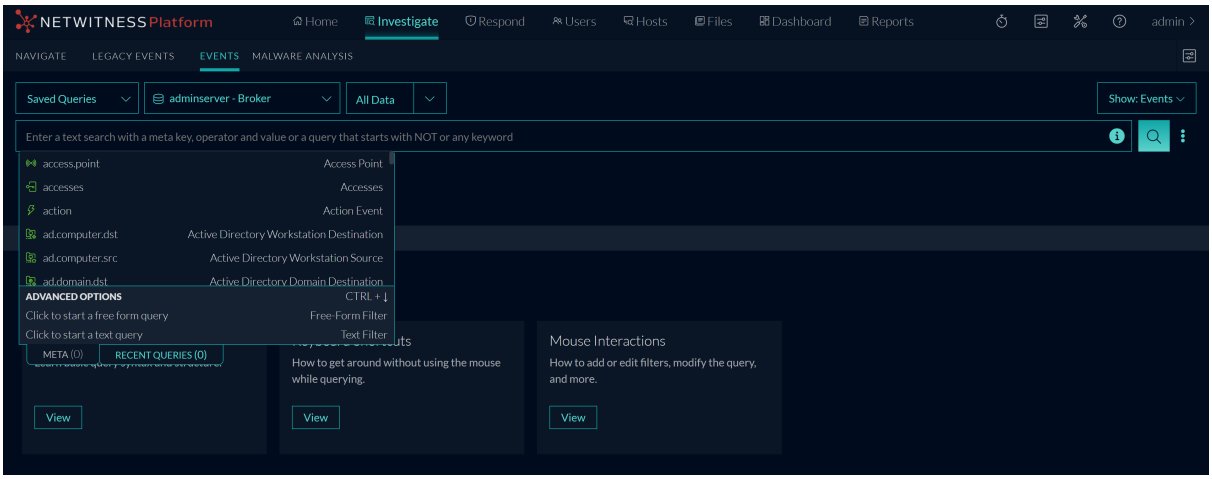
7. [**クエリー コンソール**] > [**現在のクエリー**] で詳細ステータスを表示する場合は、情報アイコン をクリックします。

8. 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。
クエリの実行が停止し、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

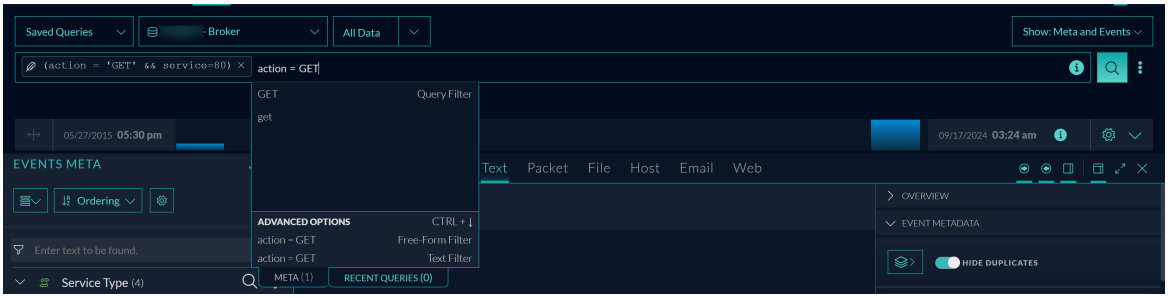
ガイド モードでフリーフォーム フィルタを使用して、 [イベント] ビューに表示されるデータをフィルタリングするには、次の手順を実行します。

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。

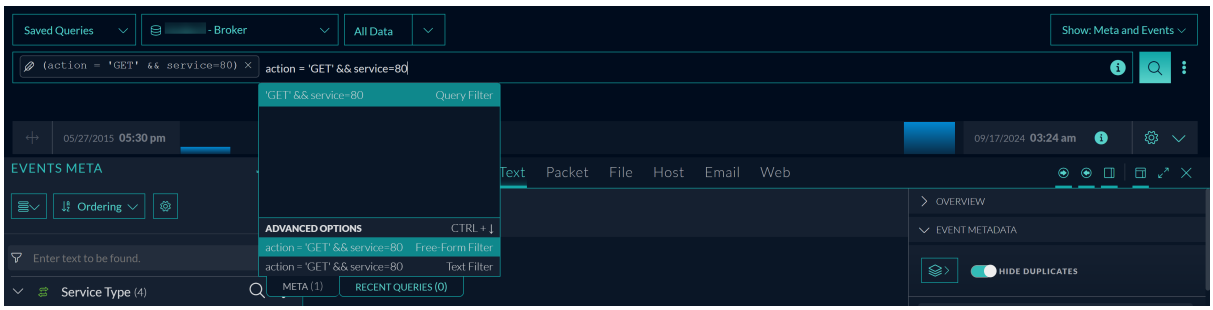


2. 次のいずれかの操作を実行します。
   a. [**フリーフォーム フィルタ**] フィールドにカーソルを置き、クエリの入力を開始します。
   b. メタ キーまたは開き括弧で始まるフィルタの入力を開始します。クエリ ビルダでフィルタを追加したり、編集するときは、括弧の不均衡が自動的に修正されます。開き括弧を入力した場合、

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、新しいフィルター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. クエリーを実行するには、  をクリックします。クエリーの実行中に  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。

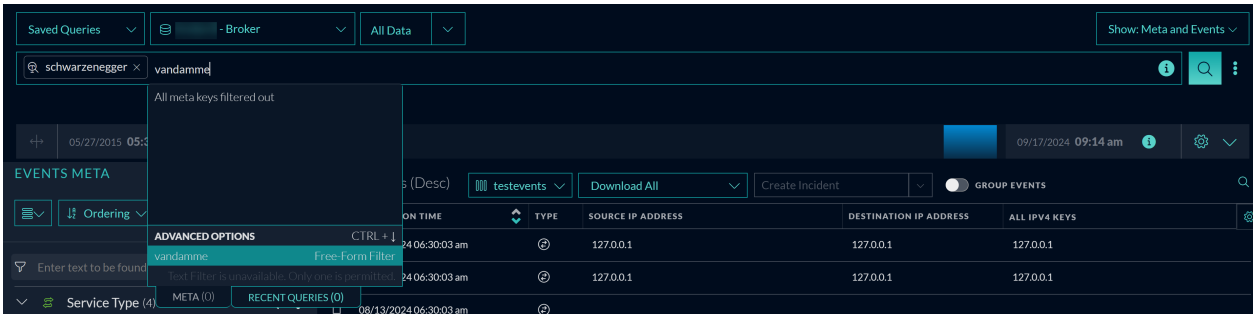
データ セット内の任意の場所で値を検索するためのテキスト フィルタの追加

テキスト フィルターを使用すると、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) 内の特定の値を見つけることができます。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, clickhere 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 - メタキーでインデックス付け
- filename.src - メタ値でインデックス付け
- float32.whatever - インデックスなし

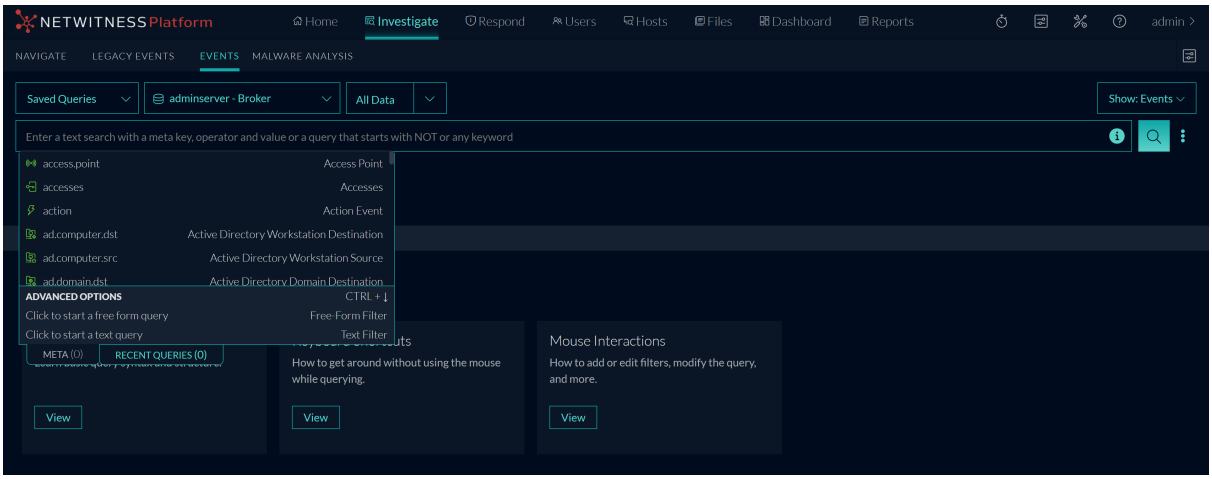
テキスト フィルタは、どこを探すべきか(どのメタ キーまたはサービスか) がわからなくても、探しているものについてある程度わかっている場合に役立ちます。たとえば、ファイル名を検索したい場合、クエリ バーをクリックして、テキスト文字列全体を入力し、 [**テキスト フィルタ**]をクリックします。テキスト フィルタは、調査対象のサービスと時間範囲内で、インデックスにあるすべてのデータを検索し、テキスト文字列と正確に一致するものを返します。

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。

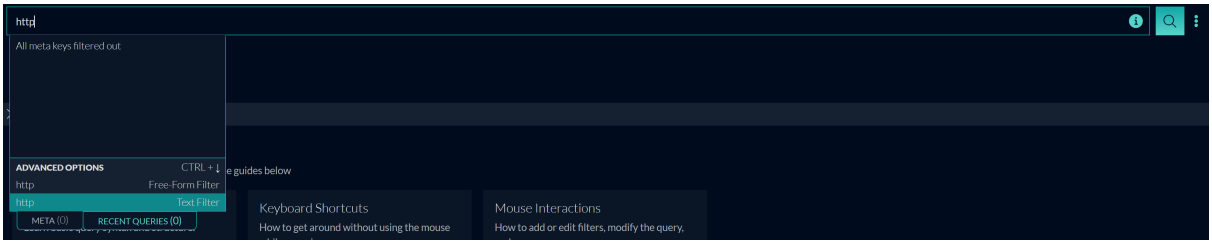


テキスト フィルタを作成するには、次の手順を実行します。

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。



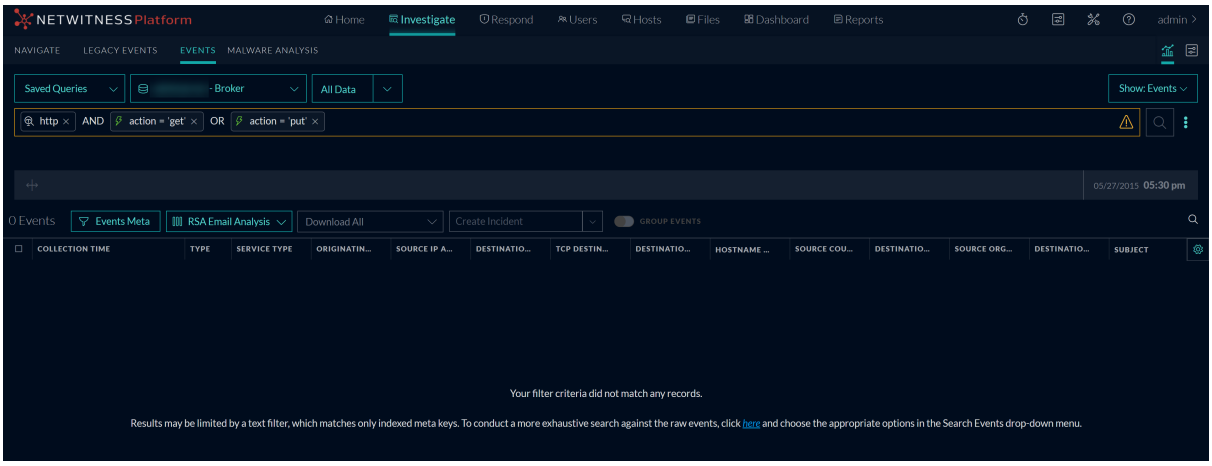
3. **詳細オプション**］の下にある **テキスト フィルタ**］をクリックします。
テキスト フィルタがクエリ バーに追加されます。次の図は、テキスト フィルタとフリーフォーム フィルタの表示の違いを示しています。フリーフォーム フィルタは、固定スペース フォントで表示され、赤色の枠線で囲まれます。フリーフォーム フィルタでは有効な式を入力する必要があるため、赤色の枠線は構文エラーがあることを示しています。テキスト フィルタには、検索アイコンが表示されます。テキスト フィルタには、構文の要件は適用されません。



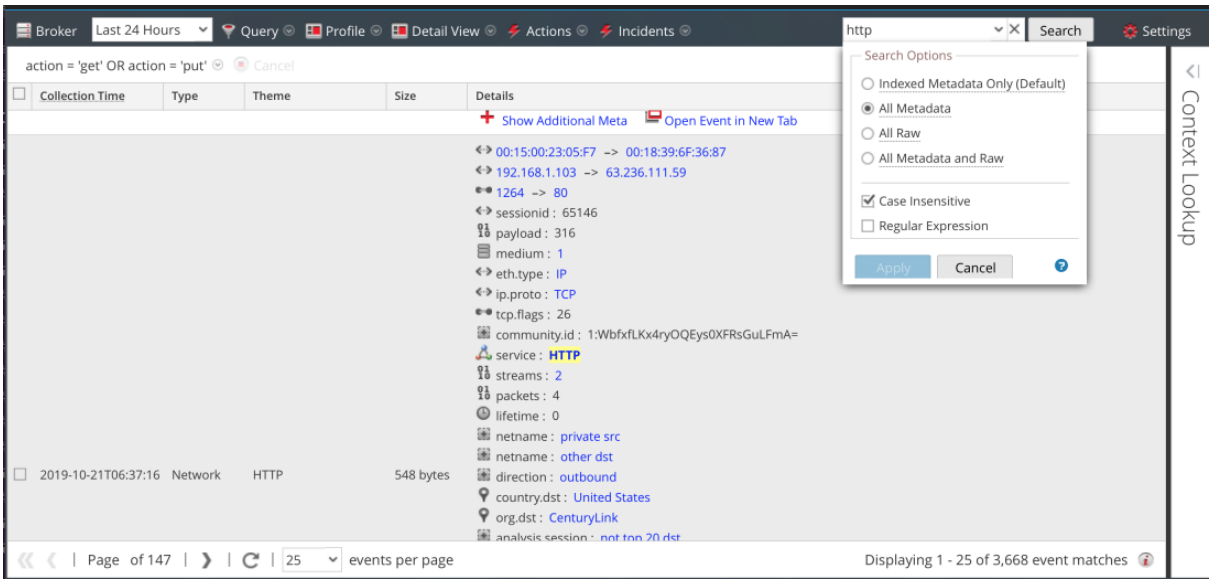
4. (オプション) シンプルまたはフリーフォームのフィルタをクエリ バーに追加します。クエリに使用できるテキスト フィルタは1つだけです。この例は、「`http`」をテキスト フィルタとして入力し、「`action = 'get' OR action = 'put'`」という2つのフィルタを追加して、クエリを完成しています。



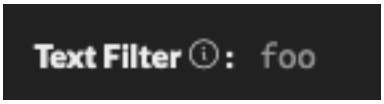
5. クエリを送信するには、  をクリックします。
結果が［イベント］パネルに表示されます。次の図は、結果が見つからなかった［イベント］パネルと、結果を改善する方法を説明したメッセージを示しています。テキスト フィルタを使用するたびに、検索を拡張するためのリンクを提供するこのメッセージが、結果の下部に表示されます。



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



7. クエリのステータスを表示するには、クエリ コンソールで(情報アイコン) をクリックします。この図は、クエリ コンソールのテキスト フィルターを示しています。



クエリ バーですべてのフィルタを選択し、すべてのフィルタをコピーする

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

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

1. [イベント]ビューの [イベント]パネルで、フォーカスされた丸またはクエリ入力フォームをクリックし、**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。

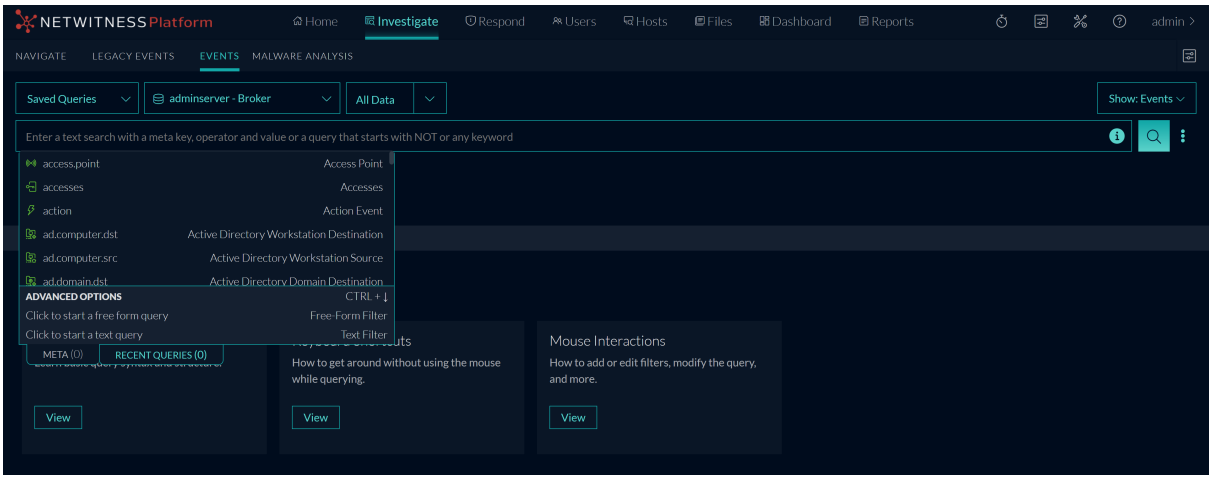
クエリー バーでテキストの貼り付け

[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、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。
   クエリ入力フォームが表示されます。



2. 他の場所からクリップボードにコピーしたテキストを貼り付けるには、**Ctrl-V** (Windows OS)、**Cmd-V** (MacOS) と入力するか、**右クリック**して**貼り付け**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。

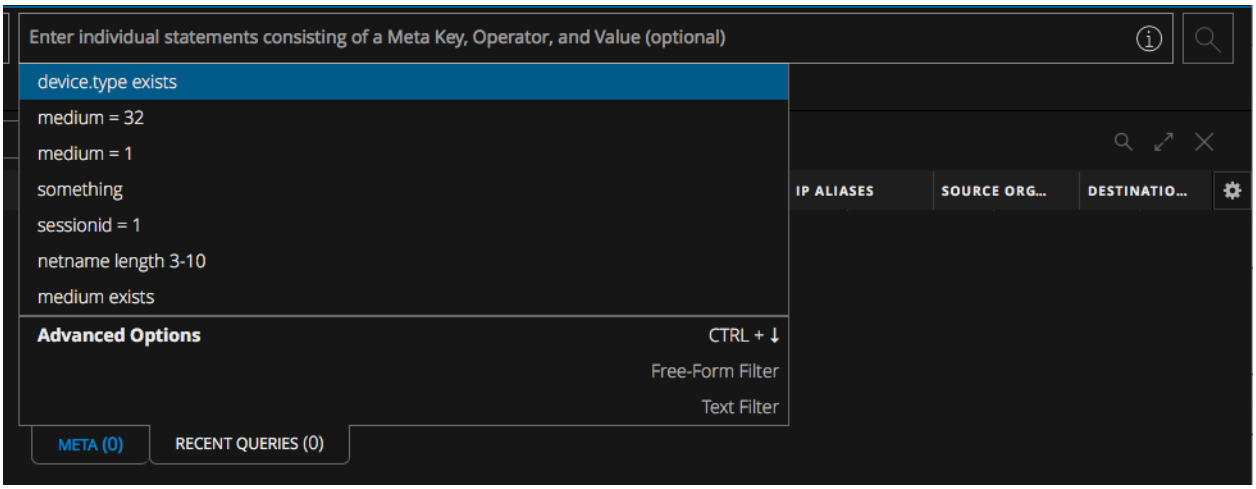
3. 必要に応じてクエリ バーにさらにフィルタを追加し、クエリを送信します。
   クエリが実行されます。

最近のクエリーに基づくフィルターの挿入

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反映して変化します。

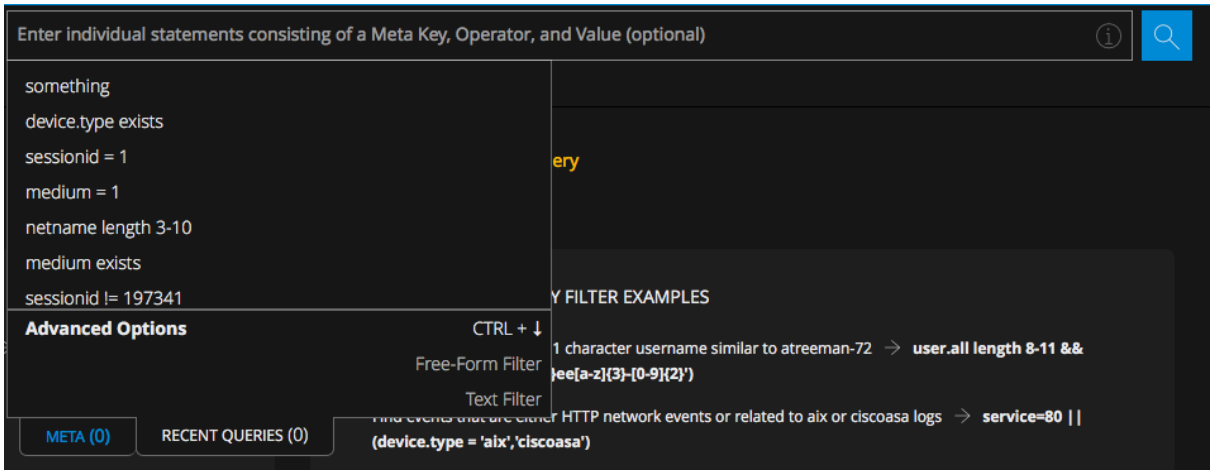
デフォルトで、リストの一番上の項目がハイライト表示されます。最近のクエリを選択するには、上下矢印を使用してハイライト表示を上下に移動するか、目的のクエリの上にマウスを合わせます。入力に合わせて、リストが絞り込まれ、ハイライト表示がリストの一番上に戻ります。クエリをクリックするか、クエリがハイライト表示された状態でEnterを押すと、選択したクエリのテキストを含んだ新しいフィルタが作成されます。

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

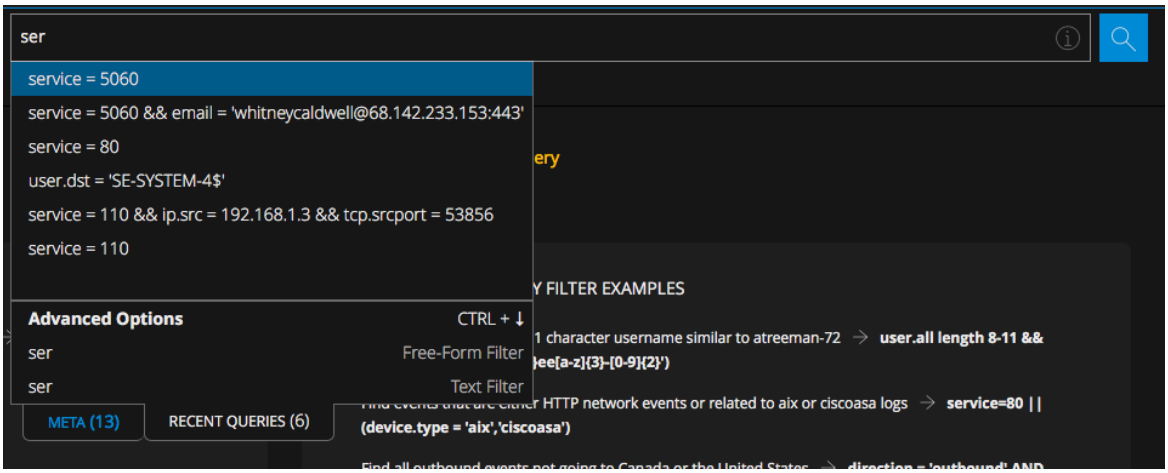


最近のクエリーに基づいてフィルターを作成するには

1. [**イベント**]ビューに移動し、クエリー バーの下にある [**ガイド モード**]を選択し、クエリー バーをクリックします。
   メタ キー ドロップダウン リストがメタ タブに表示されます。
2. [**最近のクエリ**]タブを選択します。
   [最近のクエリ]ドロップダウン リストが表示され、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反映して変化します。



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

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

4. 必要に応じてクエリバーにさらにフィルタを追加し、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。

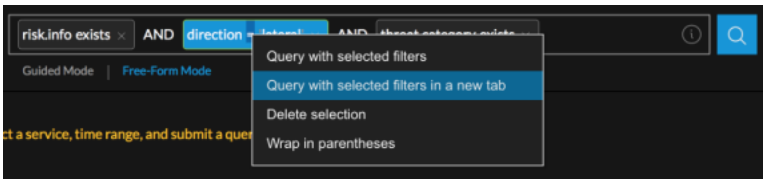
1. フィルタをダブルクリックします。または、フィルタをクリックし、**Enter**キーを押します。
2. フィルタを編集します。編集が終了したら、**Enter**キーを押して、フィルターを更新します。
3. クエリを再度実行する場合は、  をクリックします。
更新されたフィルタの結果が［イベント］パネルに表示されます。

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。一部のフィルターにはネストされた括弧を含む式が含まれており、ネストされた括弧を含むフィルター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。

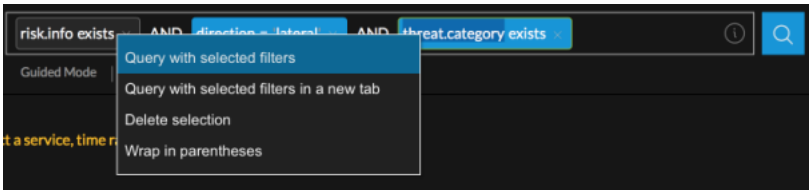
1. 1つ以上のシンプルなフィルタを含むクエリを使用します。たとえば、`risk.info exists`、`direction ='lateral'`、`threat.category exists`という3つのフィルタを含むクエリを使用します。

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。



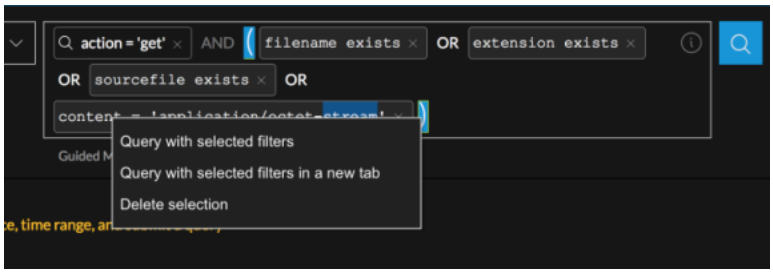
選択したフィルタの結果が新しいタブに表示され、元のクエリは、以前のタブにそのまま残ります。

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、ドロップダウン メニューで **[選択したフィルターを使用したクエリ]** を選択します。



選択したフィルターのみを含むクエリが送信され、残りのフィルターはすべて削除されます。

2. 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

キー操作による編集機能が使用可能です。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. 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 [**選択項目の削除**]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. 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。

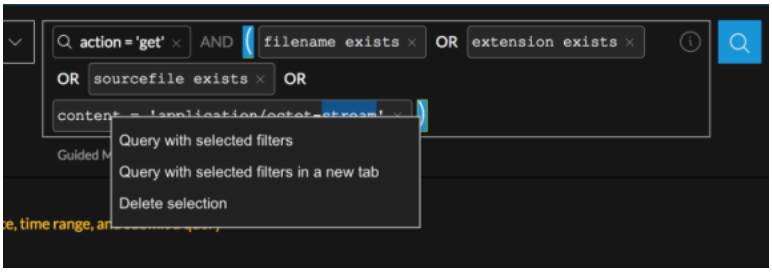
a. 前の文字を削除するには、クエリ バーで、文字の隣にカーソルを置き、**Backspace**(Windows OS) または**Delete**(MacOS) キーを押します。

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。

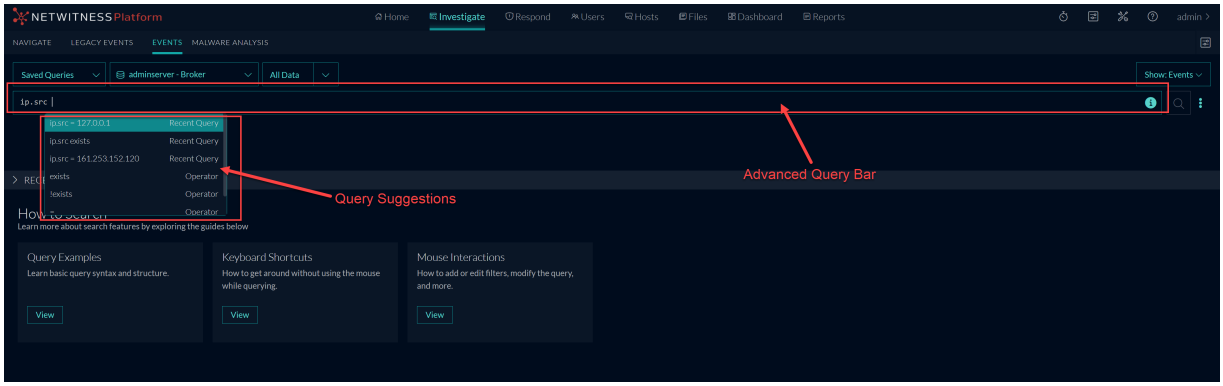
詳細モードでのクエリーの作成

NetWitnessでは、ガイド モードのクエリー バーに加えて、新しい詳細モードのクエリー バーをバージョン12.3で導入して、クエリー作成中のシームレスなエクスペリエンスをユーザーに提供します。詳細モードのクエリー バーには、ガイド モードの丸ベースのエントリーではなく、統合開発環境(IDE) のようにテキスト形式でクエリーを作成できる機能を備えた検索バーがあります。

上級ユーザーは、新しいクエリーをすばやく作成したり、既存のクエリーを変更したりして、一致するイベントのリストを取得できるようになりました。クエリーの作成中にユーザーは、Enterキーを押さずにクエリーの入力を続けることができます。詳細モードのクエリー バーには、他にも優れた機能があります。

- **構文またはエラーの強調表示** :各クエリーの構文が検証され、無効なフィルタが、赤い枠でマークされます。
- **自動提案** :クエリーの構築に役立つメタ キー、メディアのエイリアス、演算子のドロップダウン リストなどの提案。

- **最近のクエリー** :最近のクエリーを表示します。



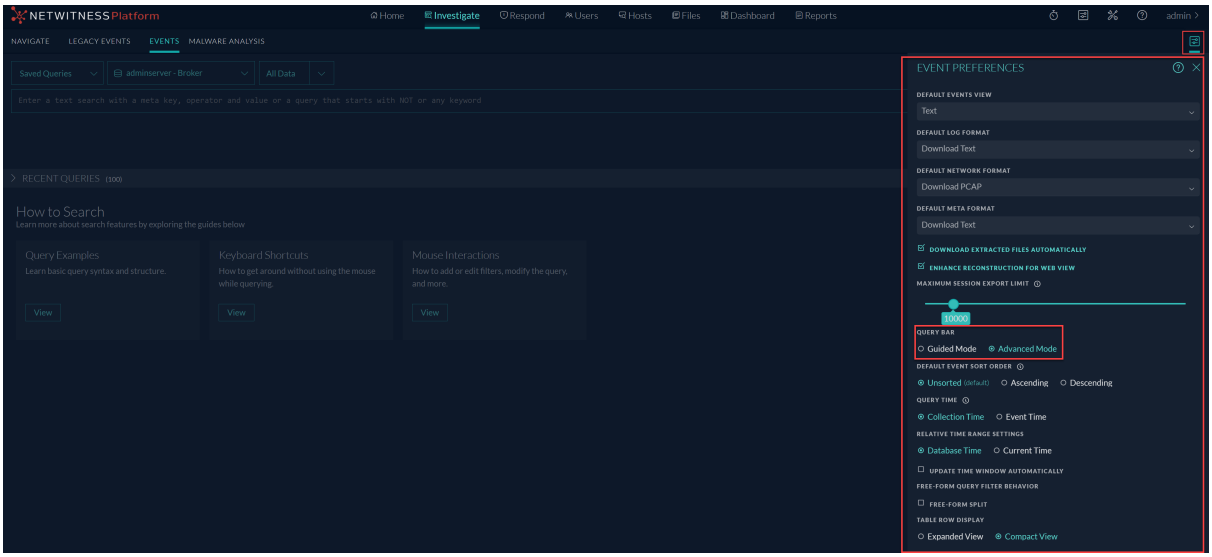
高度なクエリー バーを有効にするには：

1. **調査**]に移動し、(**イベント環境設定**) 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。

2. [イベント環境設定]ダイアログで **詳細モード**]を選択します。

   クエリーの作成または編集を行うと、クエリー バーに候補が表示されます。**Tab**キーを押すか、強調表示された候補のいずれかをクリックして選択します。



注 :高度なクエリー バーでは、クエリーの入力中に、ガイド付きクエリー バーほど多くのエラーを修正できない場合があります。

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 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。示されている例はバージョン12.5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。

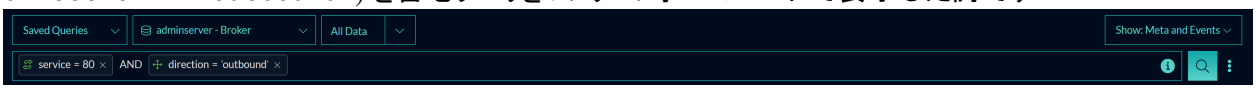
フリーフォーム モードで入力できるクエリの例を次に示します。

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す。

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

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

[ナビゲート]ビューでの結果のフィルタリング

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

注：デフォルトでは、イベント ビューのイベント メタ パネルがこの機能を提供するため、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。

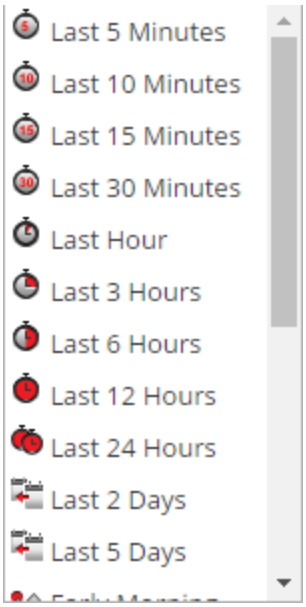
- 収集データの時間範囲。最後に収集されたデータの時刻を基準にして、一定の時間範囲を選択します。
- カレンダーの日付を基準にした時間範囲。
- カスタムの時間範囲。
- すべてのデータ。

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、『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]パネルで構成されている [タイム ゾーン]に基づいています。

組み込まれている時間範囲を選択するには

1. [ナビゲーション]ビューのツールバーで [**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。
   - 今日を基準とした時間範囲を設定する場合は、**昨日**、**今週**、**先週**、**終日**、または**早朝**、**午前**、**午後**、**夕方**などの一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

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

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

注：メタ グループでメタ エンティティが使用されている場合、結果には、メタ エンティティに含まれるメタ キーのいずれかに一致する上位20個の値が表示されます。

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

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

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

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



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



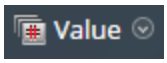
[ナビゲート]ビューでメタ キーを集計する方法と結果の表示順を選択するには、次の手順を実行します。

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

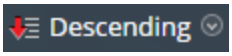
   

   選択内容に応じて現在のビューが再ロードされます。

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

   選択内容に応じて現在のビューが再ロードされます。

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


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 :メタ キーが使用される場合は、構成されたメタ 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 グループとユーザ定義のメタ グループがあります。作成したユーザ定義のメタ グループは、編集と削除が可能であるほか、エクスポートやインポートが可能です。これらの手順については、「メタ グループを使用して関連性の高いメタ キーにフォーカス」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。

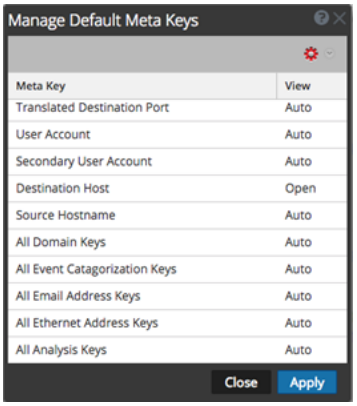
初期 [ナビゲート]ビューがデフォルトのメタ キーを使用して開くように指定するには

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は、データが現在のビューに再ロードされ、選択したオプションには目印のアイコンが表示されます。まだデータがロードされていない場合、デフォルトのメタ キーが次回のロードに使用されます。

デフォルトのメタ キーの構成

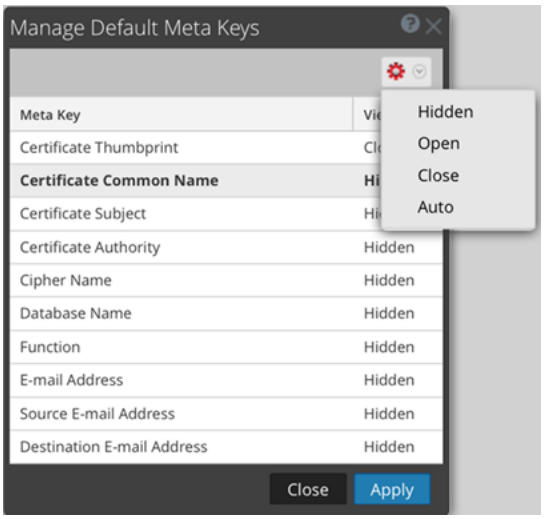
[ナビゲート]ビューでデフォルトのメタ キーのデフォルトの表示を構成するには、次の手順を実行します。

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



2. (オプション) キーの順序を変更するには、1つ以上のキーを選択し、上方向または下方向にドラッグします。
3. 次のいずれか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ー切表示されません。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。時間チャートにマウスを合わせると、特定の時間に発生したイベントの合計数が表示されます。



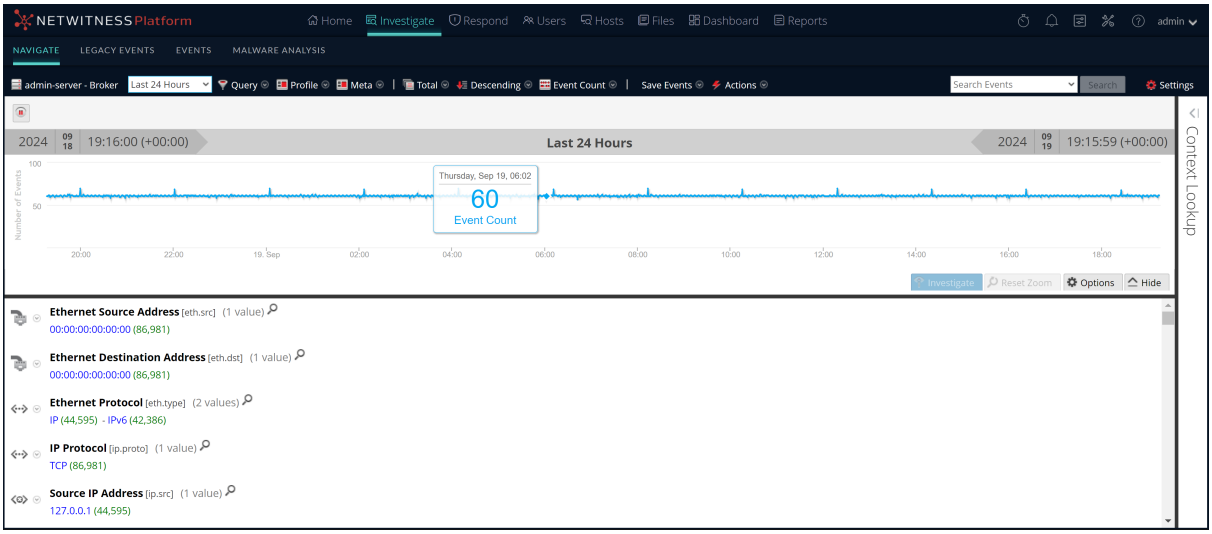
2. タイム チャート上でマウスのクリックとドラッグを行い、目的の時間範囲を選択します。選択した時間範囲がハイライト表示されます。
   選択した時間範囲のタイム チャートが再描画されます。ただし、メタ値は変更されません。
3. 選択した時間範囲のデータにドリル ダウンするには、 **調査**］をクリックします。
   URLが更新され、新しい時間範囲が反映されます。さらに、Investigationオプション パネルでは、時間範囲がカスタム時間範囲に変更されます。選択した時間範囲を使用して、タイム チャートが再描画され、メタ値がロードされます。
4. タイム チャートを元の時間範囲にリセット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

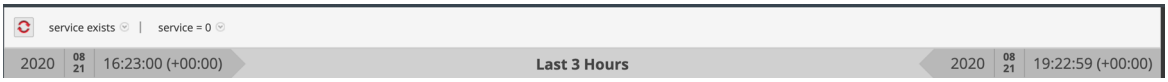
NetWitnessでは、 調査］> ナビゲート］ビューに、選択したサービスのアクティビティと値が表示されます。調査のためにアナリストがメタ キーまたはメタ値をクリックしてデータをドリルダウンすると、クエリが実行されます。 値］パネルで、各クエリは階層リンクのデータに追加されます。これにより、各クエリへのリンクを含む階層リンクが画面上部に表示されます。階層リンクを編集して、クエリを挿入したり、削除したりできます。

メタデータのサブセットにドリルダウンするには

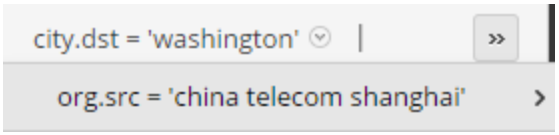
1. 調査を開始して、［ナビゲート］ビューにメタデータを表示します。



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ろにドロップダウン メニューが表示され、その中にツールバーに収まらなかった他のクエリのリストが表示されます。ツールバーに収まらなかった(オーバーフロー)クエリー内のドリルダウン ポイントを選択するには、オーバーフロー アイコンと、ドロップダウン リスト内のクエリーをクリックします。

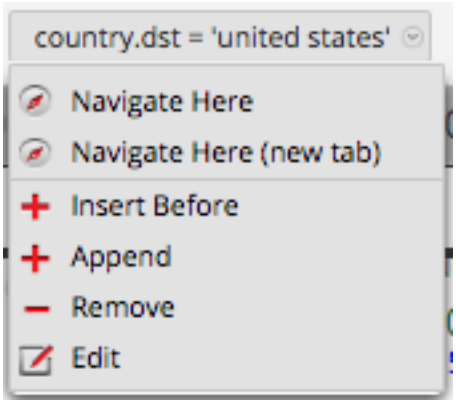


階層リンクでクエリーを追加するには

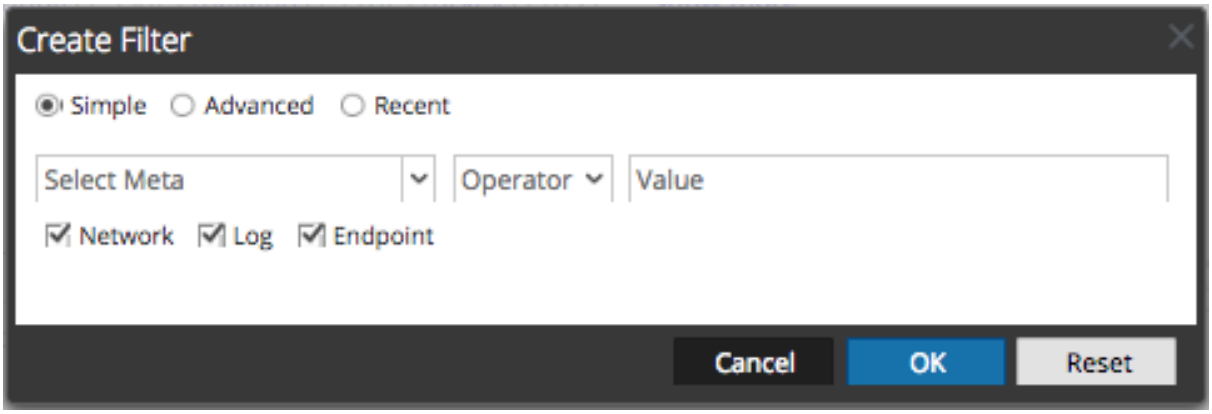
階層リンクにある任意のクエリをクリックすると、クエリ メニューを表示できます。クエリの前に新しいクエリを挿入することや、階層リンクの末尾に新しいクエリを追加することができます。階層リンクを編集すると、その都度、NetWitnessによって結果が更新されます。

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。



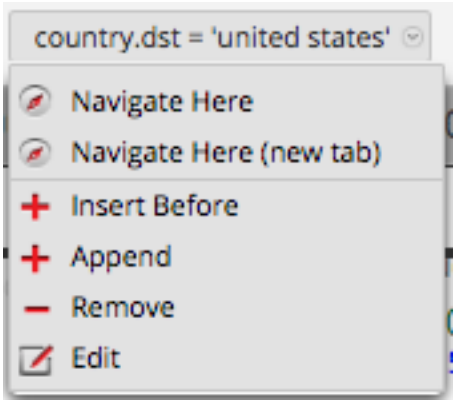
3. 「[ナビゲート]ビューと [レガシー イベント]ビューでのクエリの作成」の説明に従って、クエリを作成します。

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。

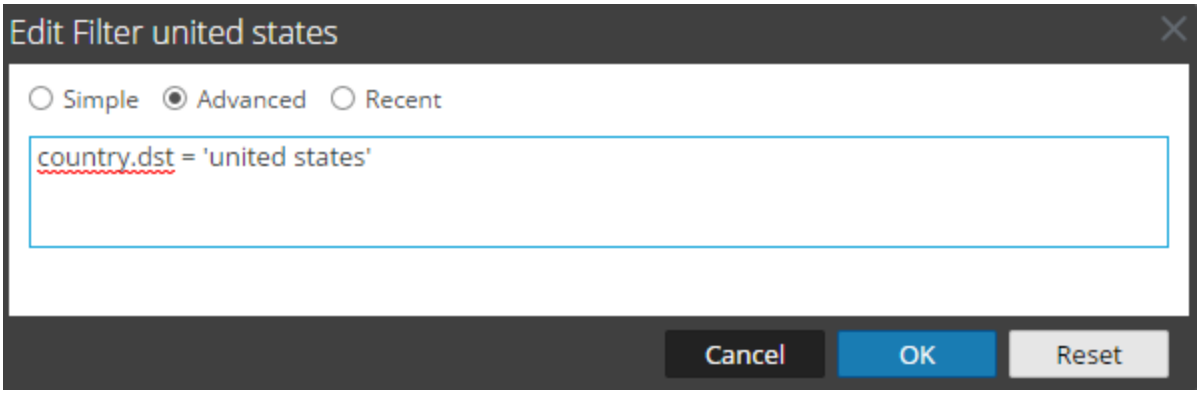
階層リンクにある任意のクエリをクリックすると、クエリ メニューを表示できます。クエリを削除したり、クエリを編集することができます。階層リンクを編集すると、その都度、NetWitnessによって結果が更新されます。

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。



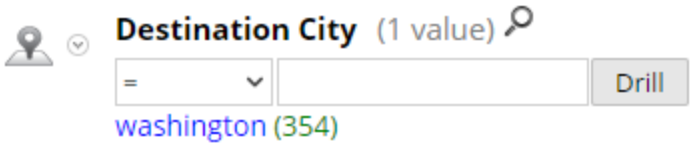
2. 階層リンクのクエリを編集するには、 **編集**]を選択します。
   [作成]ダイアログに、選択したクエリの編集画面が表示されます。



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、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

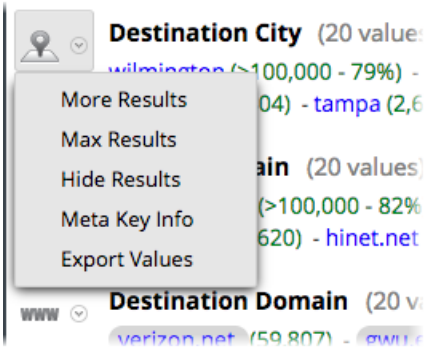
1. メタ キー セクションにマウスを合わせ、虫眼鏡アイコンをクリックします。
   [クイック検索]フォームが開きます。演算子とテキスト入力ボックスが表示され、検索条件を指定できます。



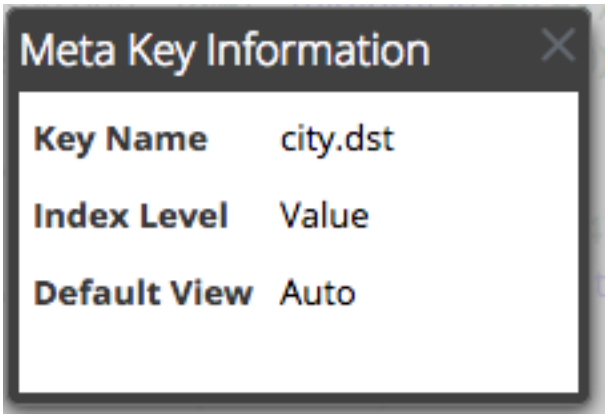
2. (オプション) この検索フォームを閉じるには、虫眼鏡アイコンをもう一度クリックしてください。
3. 左のドロップダウン リストから演算子を選択し、検索するテキスト値を入力します。 **ドリル ダウン**]をクリックすると、検索が実行されます。
   指定したメタキーとメタ値を使用して現在表示中のメタデータが絞り込まれ、結果が表示されます。

メタ キー情報を表示し、メタ キーのメタ値をコピーするには

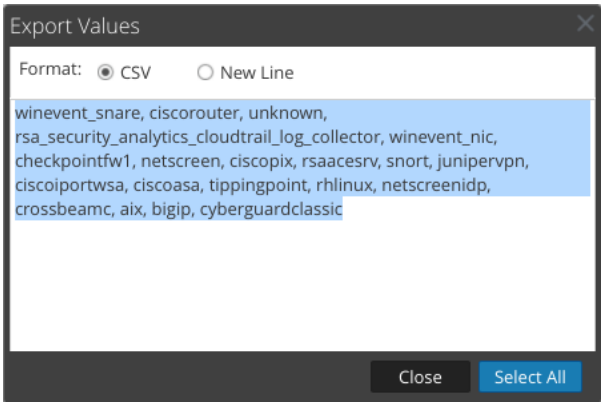
1. キー名、メタ キー表示用に設定されたインデックス レベル、メタ キーに設定されたデフォルト ビューを表示するには、メタ キーの横に表示されるドロップダウン メニューをクリックします。



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. (オプション) メタ キーの見つかったメタ値をコピー可能なシンプルなリストで表示するには、メタ キーの横にあるドロップダウン メニューをクリックします。
［値のエクスポート］ダイアログが表示されます。



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 ポイントでメタ キーの結果を折りたたみ表示にするには、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。

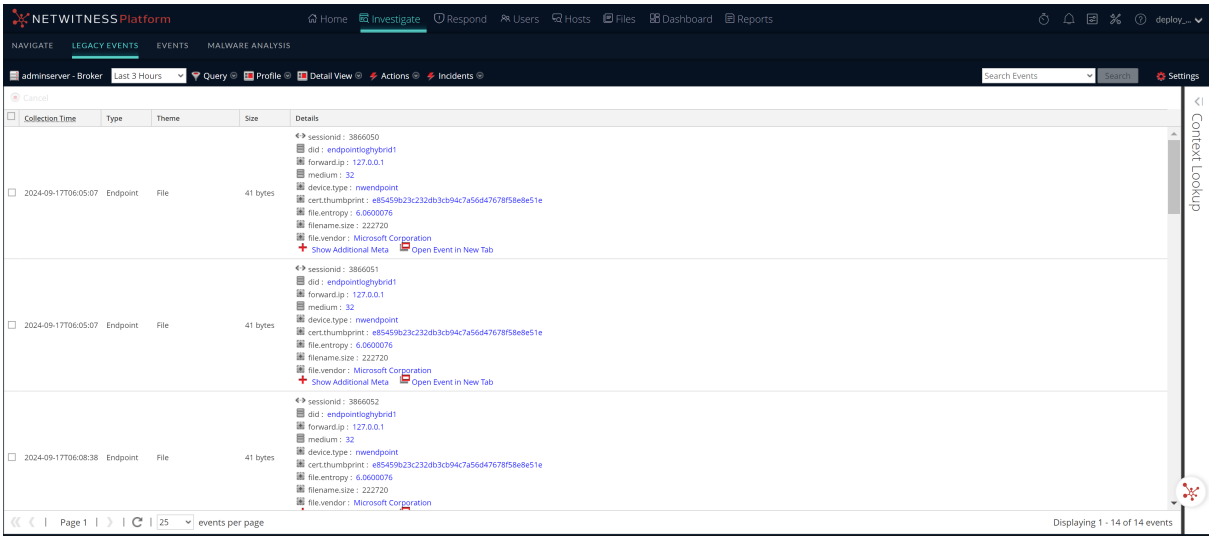
メタ値に関連づけられたイベントを表示するには

[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。

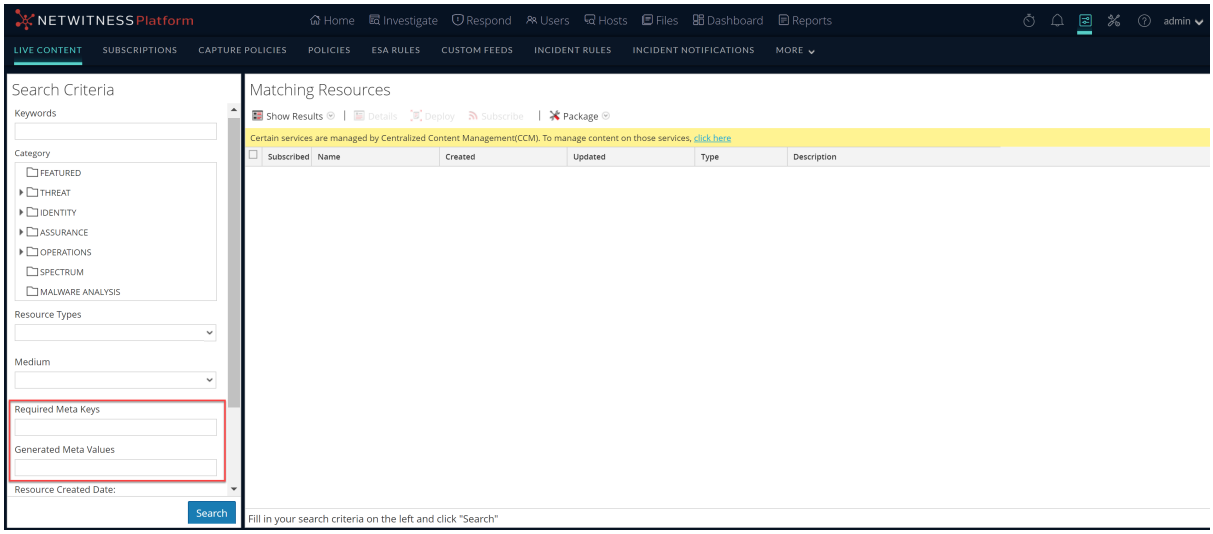
メタ値に関連づけられた特定のイベントを検索するには

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、クエリーを追加します)。
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。



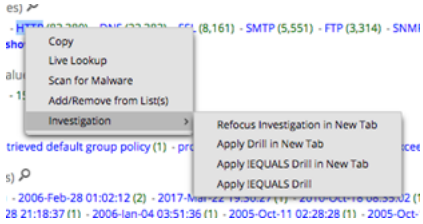
NetWitness Liveで選択したメタ値を表示するには

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。
   メタ値のドロップダウン メニューが表示されます。
3. NetWitness Liveでメタ値を検索するには、**Live Lookup** を選択します。
   Liveの [検索]ビューが開いて、入力したメタ値が [生成されるメタ値]フィールドに表示され、検索できる状態になります。



ドリルダウン ポイントで調査を再フォーカスするには、次の手順を実行します。

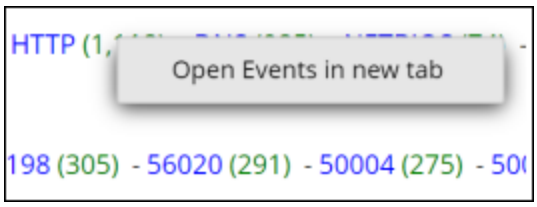
1. メタ値(青色で表示されたテキスト)を右クリックします。
   [メタ値]ドロップダウン メニューが表示されます。



2. いずれかの再フォーカス オプションを選択します。
   選択内容に応じてドリル ダウンの対象が再設定されます。

新しいタブで特定のカウントを表示するには、次の手順を実行します。

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



[レガシー イベント]ビューでの結果のフィルタリング

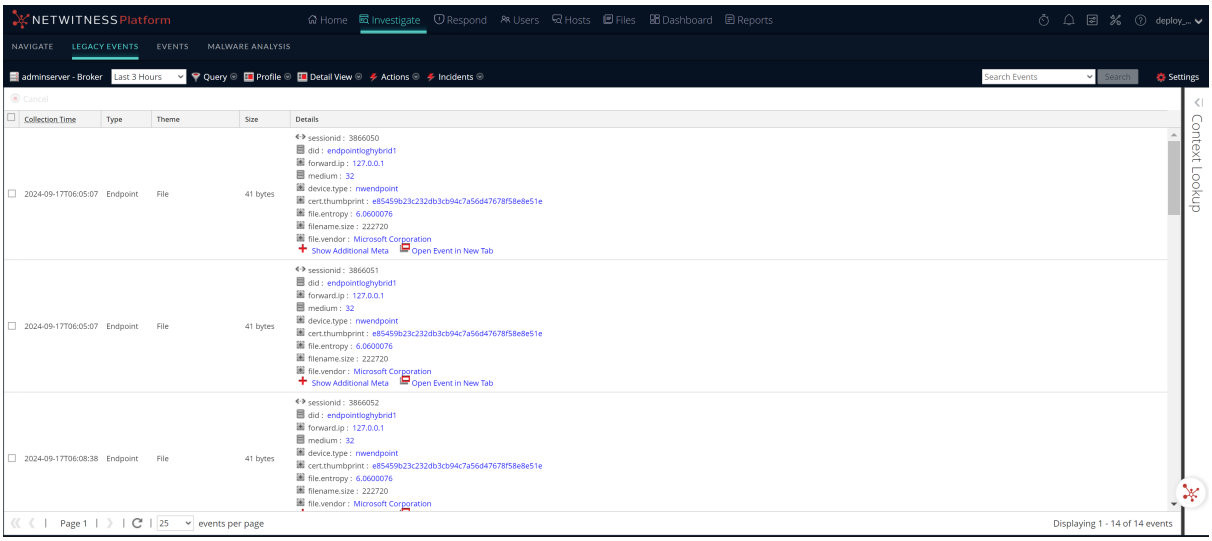
アナリストは、[レガシー イベント]ビューでイベントの検索、サービスの選択、時間範囲の設定、メタデータのクエリを行って、イベントをフィルタリングできます。[ナビゲート]ビューのドリルダウン ポイントから[レガシー イベント]ビューを開くと、デフォルトでイベントの詳細ビューが表示されます。[ナビゲート]ビューを使用する権限がないアナリストは、[レガシー イベント]ビューからサービスに直接クエリを実行できます

注：[レガシー イベント]ビューでサービスとしてArchiverを選択して検索を実行した場合は、BrokerまたはConcentratorを対象に検索を実行した場合よりも検索速度が遅くなります。通常、Archiver上のデータは圧縮され、より多くのデータが存在するためです。

[レガシー イベント]ビューに表示されるイベントのフィルタリング

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

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



2. デフォルト(**[直近3時間]**) 以外の時間範囲を選択するには、ツールバーで [時間範囲]フィールドをクリックし、値を選択します。たとえば、 **[直近1時間]**を選択します。
   選択した時間範囲で [レガシー イベント]ビューが更新されます。
3. 「[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>]
```

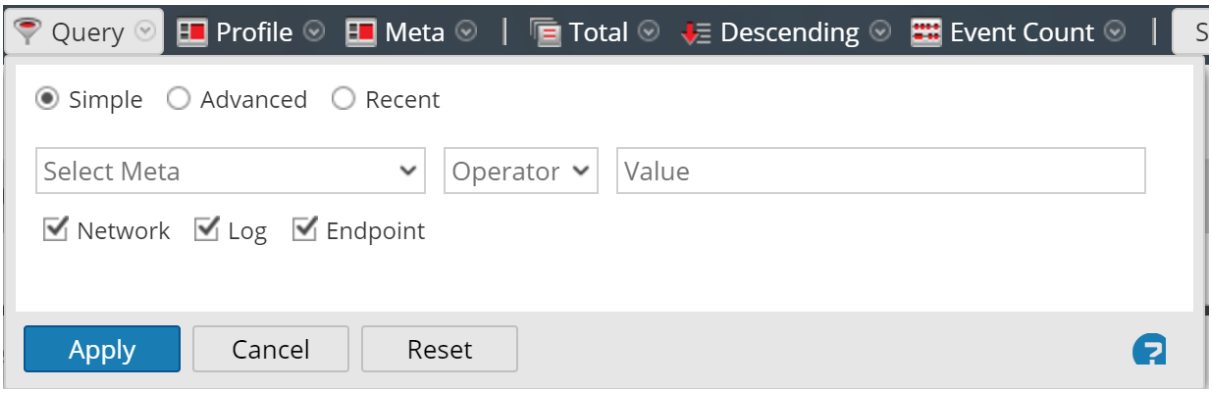
以下に、例をいくつか示します。

```
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。

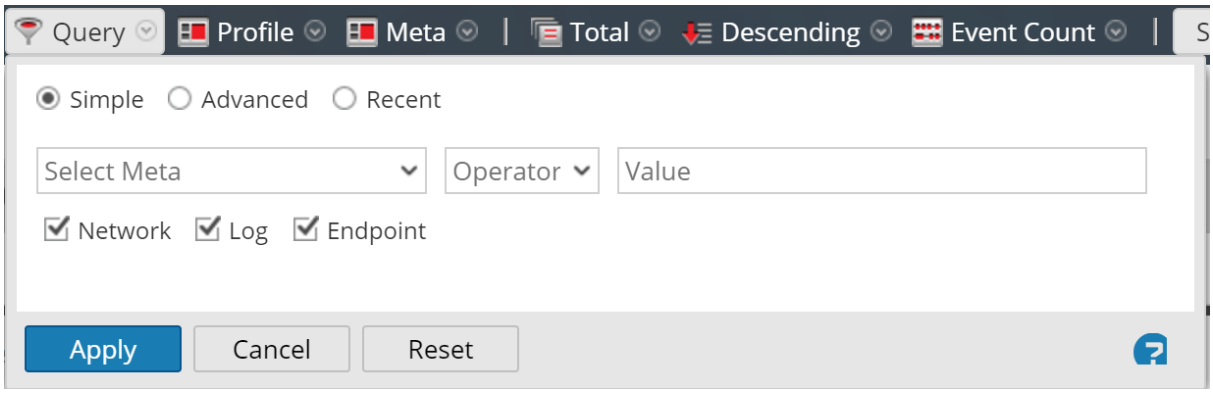


2. [メタの選択]フィールドをクリックして、ドロップダウン リストを表示します。ドロップダウン リストには、[メタ グループ]と [すべてのメタ]の2つのセクションがあります。
3. [すべてのメタ]で単一のメタ キーを選択するか、 [メタ グループ]でメタ グループを選択します。メタ キーまたはメタ グループをこのフィールドに直接入力することもできます。
4. [演算子]フィールドで、演算子を直接入力するか、ドロップダウン リストをクリックして有効な演算子を選択します。

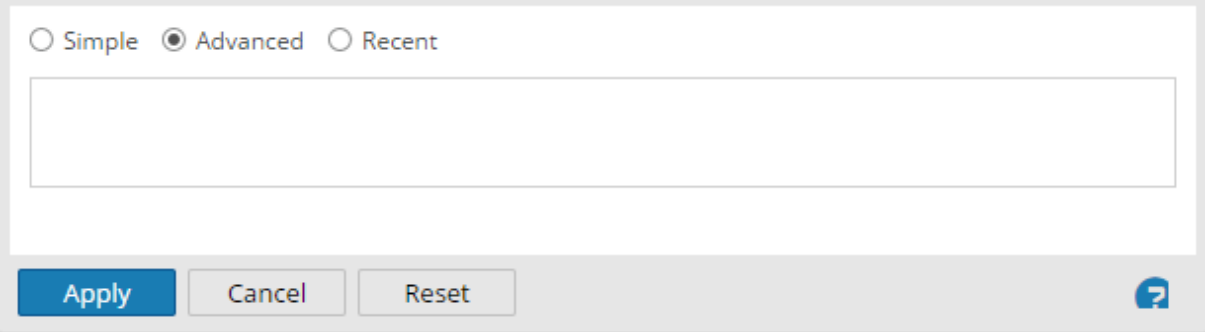
5. (オプション) 値が必要な演算子(=など)を選択した場合は、3つ目のフィールドにメタ キーの値を入力します。
6. [ネットワーク]、[ログ]、[エンドポイント]の各チェックボックスで、クエリの対象となるデータのタイプを選択します。次のいずれかの操作を実行します。
   a. クエリの対象をパケットに限定する場合は、[**ネットワーク**]をオンにし、[**ログ**]と[**エンドポイント**]をオフにします。
   b. クエリの対象をログに限定する場合は、[**ログ**]をオンにし、[**ネットワーク**]と[**エンドポイント**]をオフにします。
   c. クエリの対象をエンドポイント 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す。
   b. [**キャンセル**]をクリックします。
   ウィンドウが閉じ、ビューや現在のクエリは何も変化しません。

高度な方法を使用したクエリの作成

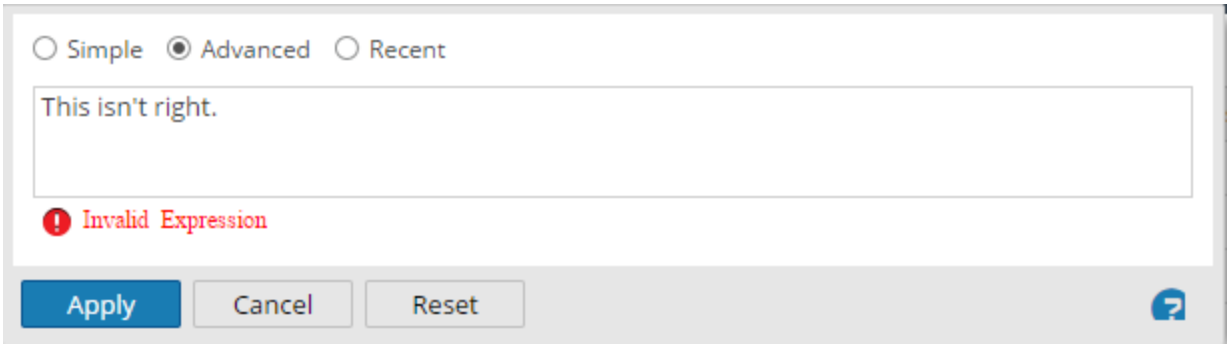
1. [**ナビゲート**]ビューまたは[**レガシー イベント**]ビューのツールバーで、[**クエリ**]を選択します。[クエリ]ダイアログが表示されます。



2. **詳細設定**]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。



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

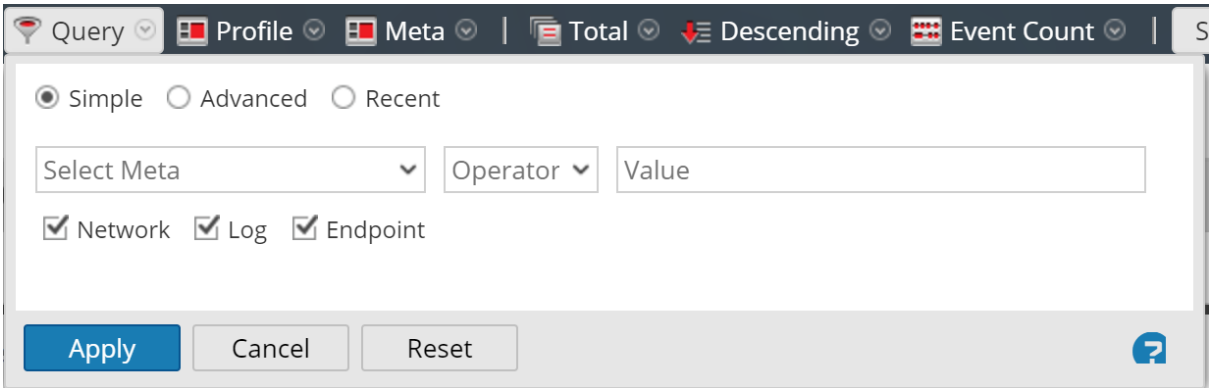


6. 次のいずれかの操作を実行します。
   - **適用**]をクリックします。
   ウィンドウが閉じ、新しいクエリの結果がビューに表示されます。階層リンクにクエリが表示されます。
   - **キャンセル**]をクリックします。
   ウィンドウが閉じ、ビューや現在のクエリは何も変化しません。

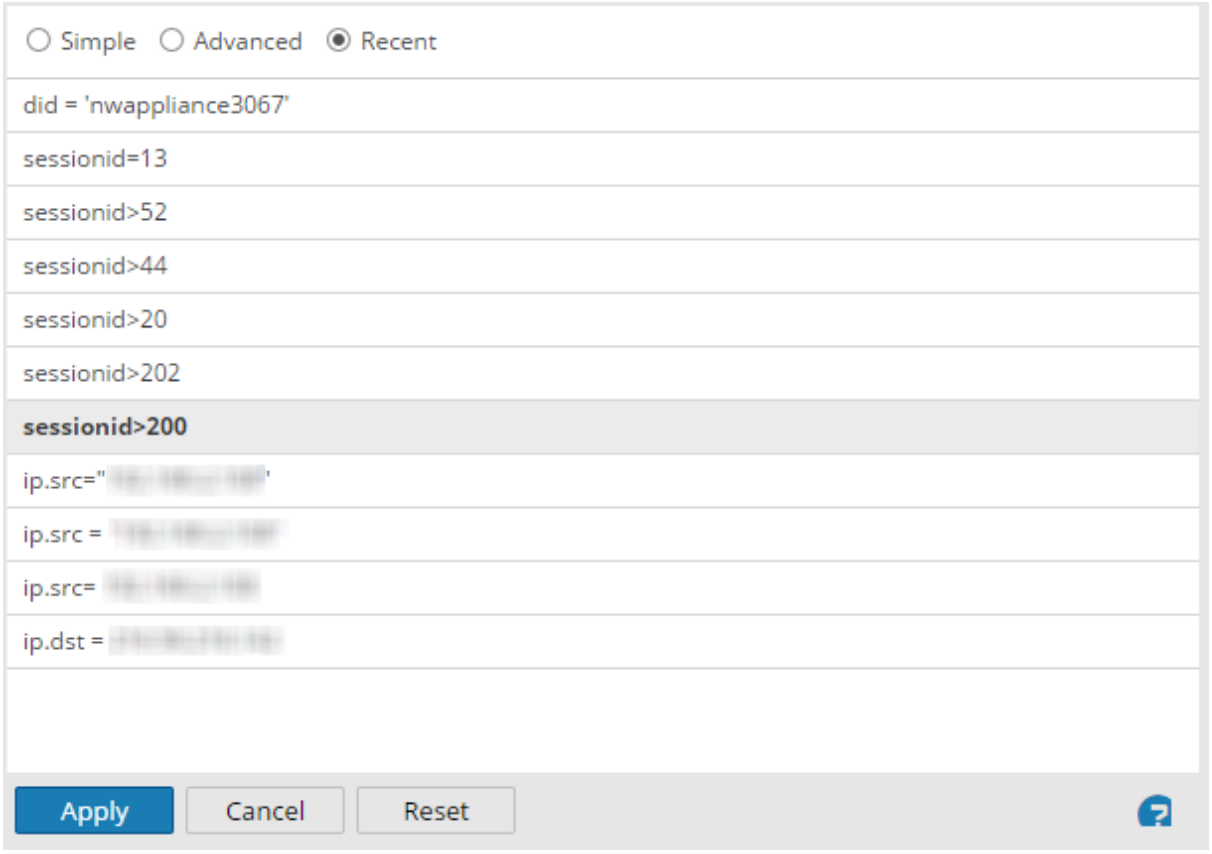
最近実行したクエリの適用

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。



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



3. 最近実行したクエリのリストから、クエリをクリックして選択します。

4. 次のいずれか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す。
   - ［**キャンセル**］をクリックします。
     ウィンドウが閉じ、ビューや現在のクエリは何も変化しません。

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

[ナビゲート]ビュー、 [イベント]ビュー、 [レガシー イベント]ビューで、現在のイベント セット内のテキスト パターンを検索できます。このセクションでは、 [ナビゲート]ビューと [レガシー イベント]ビューでの検索について説明します。

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

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

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

- **タイムスタンプ**。タイムスタンプは、ネイティブのtimeメタデータ、およびTimeタイプのその他 のtimeメタ フィールドと照 合されます。
- **数字**。検索条件に指定された10進数は自動的に認識され、数値メタ フィールドと照合されます。

検索の動作を制御するオプション

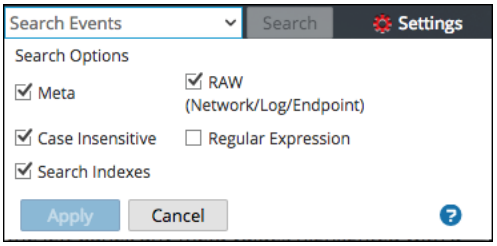
［ナビゲート］ビューまたは［レガシー イベント］ビューで検索ボックスと検索オプションにアクセスするには、次の手順を実行します。

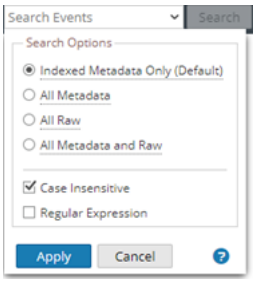
1. ツールバーに、［イベントの検索］フィールドが表示されます。



> **注**：ツールバーに［イベントの検索］フィールドが表示されない場合は、ツールバーの右端の..をクリックします。

2. ［**イベントの検索**］フィールドをクリックすると、［検索オプション］ドロップダウン メニューが表示されます。





このボックスで選択したオプションで、検索の実行方法を変更します。デフォルトの検索モードでは、インデックスされたメタデータとrawデータのみを検索します。

> **注**：［インデックス］または［インデックスされたメタデータのみ(デフォルト) ］チェックボックスがデフォルトで選択されているため、インデックスされたデータに基づいて検索結果が返されます。メタデータまたはrawデータの完全なセットを検索する場合は、該当するチェックボックスをオンにして、［インデックス］または［インデックスされたメタデータのみ(デフォルト) ］チェックボックスをオフにします。このタイプの検索には時間がかかりますが、より完全なデータのセットが含まれます。

次の表で、調査の検索オプションについて説明しています。

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

正規表現検索の構文

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

Rawテキスト キーワード検索

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

検索手順

[ナビゲート]ビューでの検索

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

1. [検索]フィールドに検索文字列を入力し、**Enter**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%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z

追加の注意事項

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

イベントビューから将来のアラートを作成する

管理者とアナリストは［調査］>［イベント］ページを選択して、不審なアクティビティに関するアラートルールを作成できます。侵害の疑いのあるアクティビティや構成ミスのあるサーバーなど、ネットワークからの幅広いイベントやシステム情報をカバーする柔軟なクエリーを使用して、ルールを作成できます。サービス(Decoder) を使用して一致したポリシーにルールが適用されると、一致が見つかるたびにアラートが生成され、アナリストがさらに調査できるようになります。

ワークフロー

脅威を示している具体的なアクティビティ(ユーザのアカウント、IPアドレス、ドメインなど) を特定したら、指定されたメタ値のアプリケーション ルールを作成して、その動作が検出されたときに警告が発せられるようにすることができます。アラート ルールが作成されると、そのルールはCCMによって管理されているサービス(Decoder) を使用して一致するポリシーに適用されます。ルールは、新しい一致がないかどうかを受信データ ストリームをリアルタイムに監視し始めます。指定されたメタ値に条件が一致すると、［対応］ページにアラートが生成されます。各アラートをドリルダウンして特定のポリシー違反を表示し、必要なアクションを実行できます。

重要：［アラートの作成］オプションがユーザに対して有効になるのは、Decoderサービスがポリシーベースのコンテンツー元管理によって管理されており、ユーザが**investigate-server.alert.manage**権限を有効にしている場合だけです。

前提条件

- アラート ルールを作成する前にクエリーを追加する必要があります。
- デフォルトでは、管理者のみがアラート ルールを作成できます。アナリストがアクセスできるようにするには、アナリストから管理者に連絡する必要があります。

注：管理者は、アナリストがアプリケーション ルールを作成できるように、ソース サーバ上で**investigate-server.alert.manage**権限と**source-server.centralpolicy.manage**権限を有効にし、コアデバイス上で**rules.manage**権限を有効に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」トピックを参照してください。

注：
- 自由形式のクエリーまたはテキスト クエリーを使用してアラート ルールを作成することはできません。
- 無効なクエリーを使用してアラート ルールを作成することはできません。
- ルールによるアラートの発行を効率的に行って、［対応］ページのアラート リストの過負荷状態やシステム パフォーマンスの問題を防ぐため、NetWitnessでは汎用アプリケーション ルールを作成しないことをお勧めします。例：**ip.src exists**

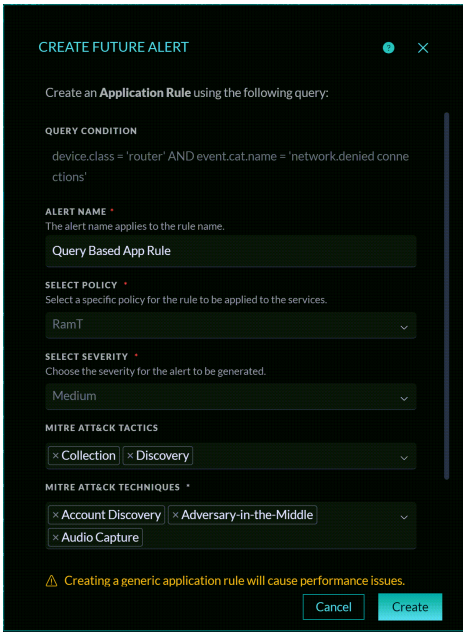
アラート ルールを作成するには

1. NetWitness Platformにログインします。
2. ［調査］>［イベント］に移動します。
3. メタキー、演算子、値(オプション) を含む1つまたは複数のフィルタで構成されるクエリを作成します。例：*(device.class = 'router') AND (event.cat.name = 'network.denied connections')*

注 :ルールのクエリー条 件 が検 索 バーで定 義されていない場 合 、 [**アラートの作 成**]オプションは無 効になります。

4. > [**将 来 のアラートを作 成**]をクリックします。

   [**将 来 のアラートを作 成**]ダイアログが表 示されます。



5. アラートを識 別 するためのわかりやすい名 前を指 定 するか、形 式 [**クエリー ベースのアプリケーション ルール**]を使 用して自 動 的 に入 力 されるデフォルト名 のままにします。

   この方 法 は多 数 のルールの中 からアナリストが作 成したルールを見 つけるのに役 立ちます。

注 :アプリケーション ルールには同じ名 前 が適 用されます。ルール名 は一 意 でなければなりません。

6. ドロップダウン リストからアプリケーション ルールに固 有 のポリシーを選 択します。

重 要 :ポリシーにグループやサービスが関 連 付 けられていない場 合 、またはCCMによって管 理されていないサービスがある場 合 、ポリシーは使 用できません。このような場 合 は、管 理 者 に連 絡 する必 要 があります。

注 :
- このアラートを生 成 するルールは、コンテンツ ポリシー ライブラリーで利 用 可 能 な既 存 のルールのリストに追 加されます。
- アプリケーション ルールは、ポリシー基 準 に一 致 するサービスに適 用され、UIに表 示されます。この情 報 に基 づいて、アプリケーション ルールが適 用されるサービスの数を特 定 できます。

7. ドロップダウン メニューから、生 成 されるアラートの重 大 度 を選 択します。オプションは以 下 のとおりです。

   - 低
   - 中

- 高
- クリティカル

注 :重大度はデフォルトで「低」に設定されています。

8. [**MITRE ATT&CK戦術**]ドロップダウン リストから1つまたは複数の戦術を選択します。戦術を選択すると、適切なテクニックとサブテクニックを選択するオプションが表示されます。
9. [**MITRE ATT&CKテクニック**]ドロップダウン リストから1つまたは複数のテクニックとサブテクニックを選択します。
10. [**作成**]をクリックします。

    ルール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。
11. 成功メッセージから、ハイパーリンク [**ここをクリック**]をクリックして、ルールが適用されるポリシー ページに移動できます。

注 :同じルールのプロパティを変更する必要がある場合は、管理者にお問い合わせください。

イベントビューからレポートを生成する

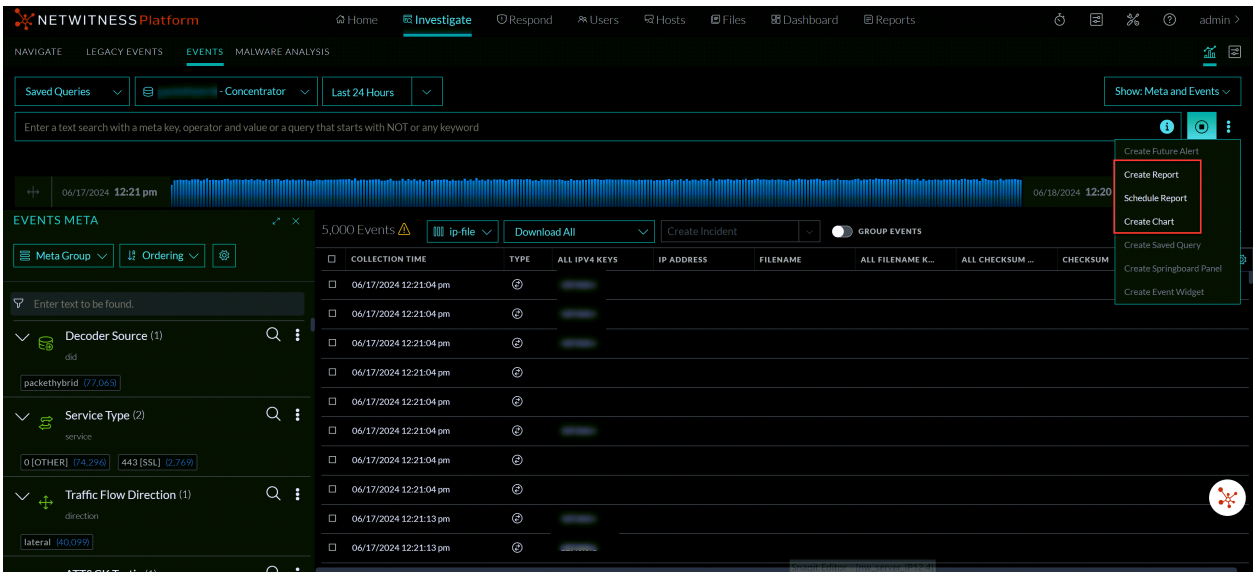
管理者とアナリストは、**「調査」**>**「イベント」**ビューからレポートを直接作成またはスケジュールできます。シンプルまたは複雑なレポートを作成して、レポートをスケジュール設定することで、実行に関するプロパティを構成できます。管理者とアナリストは、レポートを生成して、過去または現在のリソース ニーズ、あるいは予測されるリソース ニーズについての詳細を取得し、同じレポートを複数の異なる時間帯に実行するようスケジュール設定することができます。たとえば、ユーザの要件に応じてレポートを毎時間、毎日、毎週、または毎月実行するようにスケジュール設定できます。さらに管理者とアナリストは、レポートのチャートを構成することができます。この機能を使用すると、管理者とアナリストは [**イベント数**]、[**セッション サイズ**]、[**パケット数**]、および [**メタ キー**]のオプションに基づいて、さまざまなタイプのチャートを作成できます。

たとえば、上位のソースの国と宛先の国を特定する場合や、通常のカテゴリへの変更または悪意のあるアクティビティを持つ可能性のあるユーザとサービスを監視するために上位の脅威とリスクのトレンドを特定する場合などです。

レポートは次のような複数の目的に使用できます。

- ネットワークのセキュリティ ステータスの確認と評価
- ネットワーク セキュリティの問題、脅威、脆弱性の特定
- セキュリティ インシデントとマルウェア アクティビティの監視

注：
• 管理者がタイム ゾーンを設定していない場合、レポートはデフォルトでUTCタイム ゾーンに従います。
• 管理者が［ユーザ環境設定］パネルでタイム ゾーンを設定した場合、レポートは管理者が設定したタイム ゾーンに従います。詳細については、『*NetWitnessスタート ガイド*』の「ユーザ環境設定の設定」を参照してください。
• デフォルトでは、管理者のみがレポートを作成またはスケジュール設定できます。管理者は、データソースの構成中にアナリストがレポートを生成できるように、適切な権限を有効にする必要があります。
詳細については、『*NetWitness Reporting構成ガイド*』の「データ ソースの権限の構成」を参照してください。
• 生成される出力レポートには、表形式で最大100件の結果を含めることができます。
• レポートの作成とスケジュール設定は、レポートを作成したユーザのみが行えます。管理者は、レポートを表示するための適切な権限を他のロールに与えることもできます。それを行うには、**［レポート］＞［管理］＞［レポート］**を選択し、フォルダーを選択して ⚙ ＞ **［権限］**を選択し、ロールを選択して**［保存］**を選択します。
詳細については、『*NetWitness Reportingユーザガイド*』の「［レポートの権限］ダイアログ」を参照してください。



詳細については、以下のトピックを参照してください。

- レポートの作成
- レポートのスケジュール設定。
- チャートを作成する

レポートの生成中に問題が発生した場合は、「NetWitness Investigateのトラブルシューティング」の「**イベント レポートの問題を調査する**」を参照してください。

レポートの作成

［レポートの作成］ダイアログを使用すると、レポートを即座に作成できます。管理者やアナリストがレポートを作成するには、フィルタのデータ ソース、時間範囲、およびクエリを選択する必要があります。さらに管理者とアナリストは、レポートのチャートを構成することができます。この機能を使用すると、管理者とアナリストは［**イベント数**］、［**セッション サイズ**］、［**パケット数**］、および［**メタ キー**］に基づいて、さまざまなタイプのチャートを作成できます。

注：インスタント レポート生成の場合は、必要な時間範囲を［**サービス**］の横にある［**時間範囲**］ドロップダウン リストから選択します(たとえば、［直近30分］)。

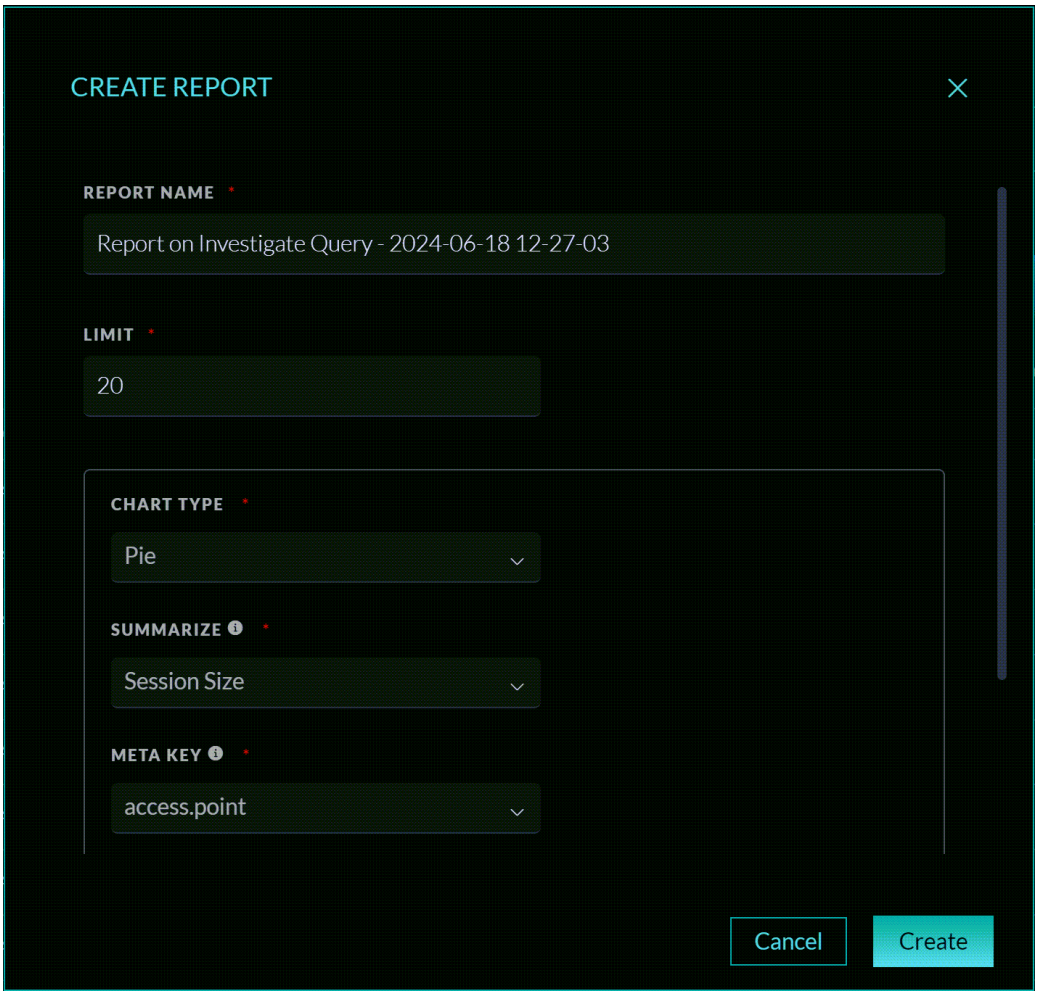
レポートを作成するには

1. NetWitness Platformにログインします。
2. ［**調査**］> ［**イベント**］に移動します。
3. メタキー、演算子、値(オプション)を含む1つまたは複数のフィルタで構成されるクエリを作成します。

   注：イベントが表示されたら、昇順または降順でイベントを並べ替えることができ、設定された制限に基づいてレポートが生成されます。

4.  > ［**レポートの作成**］をクリックします。

   ［**レポートの作成**］ダイアログが表示されます。



5. 最初はタイムスタンプ付きのデフォルトのレポート名が表示されます(「**調査クエリに関するレポート - 2023-02-25 10-16-09**」など)。

注：
• 要件に応じてレポート名をカスタマイズできますが、レポートを作成するには名前が一意でなければなりません。
• レポート名には/ \ :* ?" < > |などの特殊文字を含めることはできません。

6. [**制限**]フィールドのデフォルトのレコード数は**20**。生成するレコード数を1～100の範囲で指定します。
7. [**チャートのタイプ**]セクションで、次の操作を行います。
   a. 表示するチャートのタイプを選択し、データを可視化します。オプションは以下のとおりです。
      - 表形式(デフォルト)
      - 円
      - 領域
      - 棒

- バブル
- 列
- 折れ線
- ステップ折れ線
- ステップ面
- スプライン面
- スパイン

注：
- チャート タイプの選択内容に基づいて、 [**サマライズ**]オプションと [**メタ キー**]オプションが有効になります。
- **表形式**オプションの場合、 [**サマライズ**]オプションと [**メタ キー**]オプションは有効になりません。

b. サマライズ :これらの組み込み集計メタ オプション(イベント数、セッション サイズ、またはパケット数) のいずれかを選択して、目的のメタ値をサマライズしたものを取得します。

- **イベント数** :特定の時間に発生したイベントの総数。
- **セッション サイズ** :特定の時間にサービスによって記録されたイベントの合計サイズ。
- **パケット数** :送信または受信されたパケットの総数。

c. メタ キー :ドロップダウン メニューからメタ値を選択します。

注 : 一度に選択できるメタ値は1つだけです。

重要 : ユーザにレポートを送信するには、SMTPメール サーバが構成されていることを確認してください。

8. (オプション) [**メール出力アクション**]をクリックして、生成されたレポートの送信先にするメール アドレスを入力します。

   複数の有効なメールIDをカンマで区切って入力できます。たとえば、「**email1@example.com,email2@example.com,email3@example.com**」のように入力します。

9. [**作成**]をクリックします。

   成功メッセージが画面に表示されます。

注 : レポートの生成に要する時間は、データの量によって異なる場合があります。要求したレポートが作成されるまでお待ちください。

10. レポートを表示するには、以下のいずれかを実行します。
    - 成功メッセージ バナーのハイパーリンク [**ここをクリック**]をクリックして [**レポート**]タブでレポートを直接開きます。
    - [**レポート**] > [**管理**] > [**レポート**] > [**すべてのレポートを表示**]に移動します。

注：
• 将来のオフライン ニーズに備えて、PDFまたはCSVファイル形式でレポートをダウンロードできます。
• レポートが生成されると、レポートはPDFとしてメールに添付され、レポート作成プロセス中に設定したすべてのユーザに送信されます。

レポートのスケジュール設定

［レポートのスケジュール設定］ダイアログを使用して、レポートのスケジュールを作成できます。レポートは、毎時間、毎日、毎週、または毎月にスケジュール設定できます。管理者やアナリストが特定の時刻、または日次、週次、月次ベースでレポートをスケジュール設定するには、［レポートのスケジュール設定］ダイアログでスケジュール オプションを設定する必要があります。さらに管理者とアナリストは、レポートのチャートを構成することができます。この機能を使用すると、管理者とアナリストは［**イベント数**］、［**セッション サイズ**］、［**パケット数**］、および［**メタ キー**］に基づいて、さまざまなタイプのチャートを作成できます。

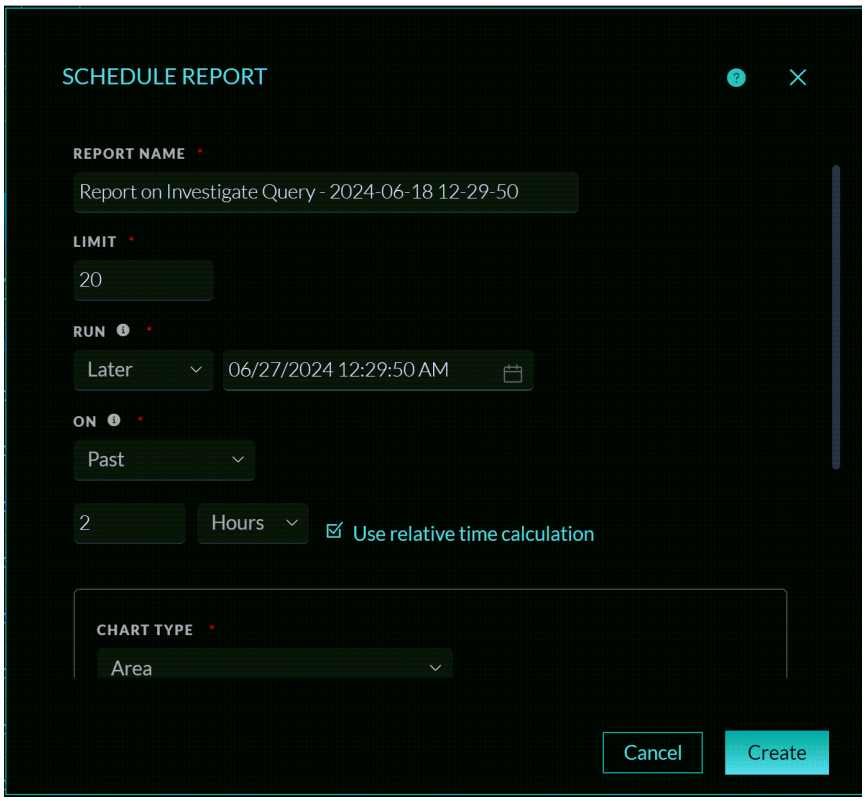
注：レポートには、選択した時間間隔のデータのみが含まれます。この間隔は次回のレポート実行時以降に変更できます。

レポートをスケジュール設定するには

1. NetWitness Platformにログインします。
2. ［**調査**］> ［**イベント**］に移動します。
3. メタキー、演算子、値(オプション)を含む1つまたは複数のフィルタで構成されるクエリを作成します。

   注：イベントが表示されたら、昇順または降順でイベントを並べ替えることができ、設定された制限に基づいてレポートが生成されます。

4.  > ［**レポートのスケジュール設定**］をクリックします。
   ［**レポートのスケジュール設定**］ダイアログが表示されます。



5. 最初はタイムスタンプ付きのデフォルトのレポート名が表示されます(「**調査クエリに関するレポート - 2023-04-25 10-18-26**」など)。

> **注：**
> • 要件に応じてレポート名をカスタマイズできますが、レポートをスケジュール設定するには名前が一意でなければなりません。
> • スケジュール時間は、管理者のユーザ環境設定で選択されているユーザのタイム ゾーンに基づいて表示されます。
> 詳細については、『*NetWitness スタート ガイド*』の「ユーザ環境設定の設定」を参照してください。
> • 名前には/ \ :* ?" < > |などの特殊文字を含めることはできません。
> • クエリ フィルタのレポートをスケジュール設定し、生成されるレポートに、値を返さなかったルールが含まれている場合は、その特定のクエリのデータが利用できないことを意味します。

6. **制限**]フィールドのデフォルトのレコード数は**20**。生成するレコード数を1～100の範囲で指定します。
7. スケジュールを設定するには、次のパラメーターを指定します。

   実行スケジュールのタイプによって、次のいずれかを選択します。

フィールド	説明
実行	スケジュール設定されたジョブの実行に使用する時間間隔： • **指定日時**：実行スケジュールに［**指定日時**］を選択した場合は、表示された各フィールドで日付の値を指定する必要があります。 • **毎時**：実行スケジュールに［**毎時**］を選択した場合は、［**分**］フィールドに分を指定する必要があります。たとえば、レポートの実行スケジュールを50分に設定した場合は、50分ごとにレポートが作成されます。 **注**：最大値である59分まで選択できます。 • ［**日単位**］：実行スケジュールに［**毎日**］を選択した場合は、［**時間**］フィールドに値を入力する必要があります。たとえば、レポートの実行スケジュールを04:25に設定すると、レポートは毎日午前4:25に作成されます。 • ［**週単位**］：実行スケジュールに［**毎週**］を選択した場合は、［**曜日**］フィールドに値を入力し、曜日を選択する必要があります。 **注**：レポートは、スケジュールが開始される日の曜日に実行されます。たとえば、スケジュール設定したレポートの初回実行日が月曜日の場合、レポートは毎週月曜日に実行されます。 • ［**月単位**］：実行スケジュールに［**毎月**］を選択した場合は、［**日**］フィールドで日を選択する必要があります。たとえば、25日の場合は「25」を選択すると、レポートが毎月25日に作成されるようになります。 **注**：29以上の値を［日］で選択した場合は、月次レポートの生成プロセス中にメッセージが表示され、選択した日を含んでいる月にレポートがスケジュール設定されることが通知されます。

フィールド	説明
オン	• **過去**：[**過去**]オプションを選択した場合は、**時間**、**日**、**週**、**月**、**年**に基づいてレポートをスケジュール設定できます。たとえば、現在の日付の3日前にレポートを開始するようにスケジュール設定する場合は、次の操作を実行します。 • [**オン**]フィールドで [**過去**]を選択します。 • フィールドに「**3**」と入力して、ドロップダウン リストから [**日**]を選択します。 このフィールドは、 [**実行**]フィールドで [**指定日時**]を選択した場合にのみ表示されます。 **注：** • このフィールドは、 [実行]フィールドで [指定日時]、 [毎時間]、 [毎日]、 [毎週]、 [毎月]を選択した場合に表示されます。 • [毎時間]の場合、許容最大値は168(24時間x 7日) で、合計時間としてカウントされます。 • **範囲(特定)** ：[範囲(日時指定)]オプションを選択した場合は、 [**開始**]と [**終了**]に値を指定する必要があります。 たとえば、2023年2月1日午前12:00:00～2023年2月15日午前12:00:00の特定の日時範囲でレポートをスケジュール設定すると、レポートは指定した期間のデータに対して実行されます。 **注 :** このフィールドは、 [実行]フィールドで [指定日時]を選択した場合にのみ表示されます。 • **範囲(時間指定)** ：**範囲(時間指定)**]オプションを選択した場合は、 [**開始**]と [**終了**]に値を指定する必要があります。 たとえば、毎日04:00～10:00の時間範囲でレポートをスケジュール設定すると、レポートは指定した期間のデータに対して実行されます。 **注 :** このフィールドは、 [実行]フィールドで [指定日時]、 [毎日]、 [毎週]、 [毎月]を選択した場合にのみ表示されます。 **注 :** レポートのスケジュール時に、 [**過去**]オプションを選択した場合、または **範囲(日時指定) /範囲(時間指定)**]オプションで終了時間を現在の時間に非常に近い時間に設定した場合は、データ ソースから集計データを取得できることを確認してください。データ ソースでの集計が遅延する場合は、遅延を考慮した終了時間を選択する必要があります。そうでないと、レポートにはその時間範囲の未集計データが含まれません。

フィールド	説明
相対時間計算の使用	• デフォルトでは、 **[相対時間計算の使用]**オプションが有効になっており、レポートのスケジュール設定に相対的な期間が使用されます。 たとえば、相対時間で過去1時間のデータに対してレポートをスケジュール設定する場合、その時間はレポートの実行時までの厳密に1時間を指します。現在時刻が午後3時の場合は、過去60分間、つまり今日の午後2時から午後3時までの間に発生したイベントが報告されます。 • このオプションの選択を解除して、レポートをスケジュール設定することもできます。 たとえば、過去3時間のデータに対してレポートを実行するようにスケジュール設定した場合は、現在の時刻を除いた過去3時間のデータが取得されます。現在時刻が午後6:30の場合は、レポートがスケジュール設定された時間までに発生したイベント、つまり今日の午後3時から午後6時までの間に発生したイベントが報告されます。

8. **[チャートのタイプ]**セクションで、次の操作を行います。
   a. 表示するチャートのタイプを選択し、データを可視化します。オプションは以下のとおりです。
      - 表形式(デフォルト)
      - 円
      - 領域
      - 棒
      - バブル
      - 列
      - 折れ線
      - ステップ折れ線
      - ステップ面
      - スプライン面
      - スパイン

注：
- チャート タイプの選択内容に基づいて、 [サマライズ]オプションと [メタ キー]オプションが有効になります。
- 表形式オプションの場合、 [サマライズ]オプションと [メタ キー]オプションは有効になりませ

ん。

b. サマライズ :これらの組み込み集計メタ オプション(イベント数、セッション サイズ、またはパケット数) のいずれかを選択して、目的のメタ値をサマライズしたものを取得します。

- **イベント数** :特定の時間に発生したイベントの総数。
- **セッション サイズ** :特定の時間にサービスによって記録されたイベントの合計サイズ。
- **パケット数** :送信または受信されたパケットの総数。

c. メタ キー :ドロップダウン メニューからメタ値を選択します。

注 :一度に選択できるメタ値は1つだけです。

重要 :ユーザにレポートを送信するには、SMTPメール サーバが構成されていることを確認してください。

9. (オプション) [**メール出力アクション**]をクリックして、生成されたレポートの送信先にするメール アドレスを入力します。

   複数の有効なメールIDをカンマで区切って入力できます。たとえば、「**email1@example.com,email2@example.com,email3@example.com**」のように入力します。

10. [**作成**]をクリックします。

    成功メッセージが画面に表示されます。

注 :レポートの生成に要する時間は、データの量によって異なる場合があります。要求したレポートが作成されるまでお待ちください。

11. レポートを表示するには、以下のいずれかを実行します。

- 成功メッセージ バナーのハイパーリンク [**ここをクリック**]をクリックして、 [**レポート**]タブに移動し、生成されたレポートを開きます。
- [**レポート**] > [**管理**] > [**レポート**] > [**すべてのレポートを表示**]に移動します。

注 :
• 将来のオフライン ニーズに備えて、PDFまたはCSVファイル形式でレポートをダウンロードできます。
• レポートが生成されると、PDFとして電子メールに添付され、レポート作成プロセス中に構成されたすべてのユーザーに送信されます。

チャートを作成する

管理者とアナリストは、 [**調査**] > [**イベント**]ページのリアルタイム データに基づいてチャートを作成できます。この機能拡張を使用すると、 [**イベント数**]、 [**セッション サイズ**]、 [**パケット数**]、 [**メタ キー**]の各サマライズ オプションに基づいて、さまざまなタイプのチャートを作成することが可能になります。これはアナリストが傾向を追跡するためのオールインワン ソリューションとなります。さらに、アナリストはこれらのリアルタイム チャートをデフォルトのダッシュボードに追加できるため、組織内の重要なデータをシームレスに追跡することができます。

前提条件

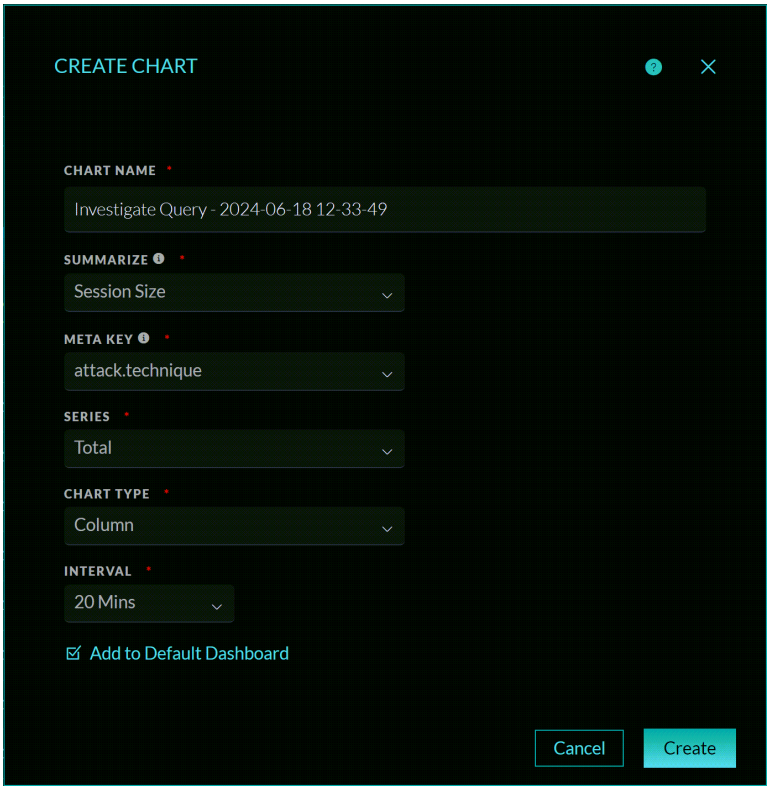
デフォルトでは、管理者のみがグラフを作成できます。管理者は、データ ソースの構成中にアナリストがグラフを生成できるように、適切な権限を有効にする必要があります。詳細については、「*NetWitness Reporting構成ガイド*」の「データ ソースの権限の構成」を参照してください。

注：グラフの作成中にエラーが見つかった場合、サーバがオフラインになっている可能性があります。その場合は、**respond-server.log**、**investigate-server.log**、**sa.log**で詳細を確認して、問題を解決してください。

重要：管理者はデフォルトのダッシュボードのコピーをアナリストと共有するときは常に、**ルール**と**チャート**の権限も提供して、アナリストがリアルタイムのチャートを表示できるようにする必要があります。詳細については、「「ルールの権限」ダイアログ」と「「チャートの権限」ダイアログ」のトピックを参照してください。

「イベント」ビューからチャートを作成するには

1. NetWitness Platformにログインします。
2. **調査**」> 「**イベント**」に移動します。
3. **検索**」をクリックします。
4.  > 「**チャートの作成**」をクリックします。
   「**チャートの作成**」ダイアログが表示されます。



5. 最初はタイムスタンプ付きのデフォルトのチャート名が表示されます(**調査クエリ - 2023-09-04 03-20-22**) 。

   注：
   • 要件に応じてレポート名をカスタマイズできますが、レポートを作成するには名前が一意でなければなりません。
   • レポート名には/ \ :* ?" < > |などの特殊文字を含めることはできません。

6. これらの組み込み集計メタ オプション(イベント数、セッション サイズ、またはパケット数) のいずれかを [**サマライズ**]ドロップダウン メニューから選択して、目的のメタ値をサマライズしたものを取得します。

   - **イベント数** :特定の時間に発生したイベントの総数。
   - **セッション サイズ** :特定の時間にサービスによって記録されたイベントの合計サイズ。
   - **パケット数** :送信または受信されたパケットの総数。

7. [**メタ キー**]ドロップダウン メニューからメタ値を選択します。

   注：一度に選択できるメタ値は1つだけです。

8. 表示するチャートの [**系列**]オプションをドロップダウン メニューから選択します。

   - **合計** :チャートには、選択した時間帯の各集計値の合計が表示されます。
   - **値** :チャートには、選択した時間帯の値の変化が表示されます。

   注：このオプションは、 [**デフォルトのダッシュボードに追加**]チェックボックスを選択した場合にのみ使用可能になります。

重要：
- レポート チャート ビューでは、レンダリング済みのチャートがチャートのデフォルト設定を使用して表示されます。これは、デフォルトの時間範囲(3時間) 、デフォルト オプションの系列(時系列チャート) 、プロットするアイテム(5) 、およびチャート タイプ(折れ線) がチャートで使用されることを意味します。
- デフォルトのダッシュボード ビューでは、設定された値を使用してチャートが表示されます。これは、チャートで指定されているデフォルトの時間範囲(過去24時間) 、系列、および間隔のオプションがチャートで使用されることを意味します。

9. レンダリングするチャートのタイプを [**チャート タイプ**]ドロップダウンメニューから選択し、データを可視化します。

   注：
   - このオプションは、 [**デフォルトのダッシュボードに追加**]チェックボックスを選択した場合にのみ使用可能になります。
   - デフォルトでは、棒タイプのチャートが選択されています。
   - 選択した [**系列**]オプションに応じて、チャートが自動表示されます。
   - [**合計**]オプションの場合：[**円**]および [**棒**]チャートのみが有効になっています。
   - [**値**]オプションの場合：[**エリア**]、 [**棒**]、 [**折れ線**]、 [**ステップ折れ線**]、 [**ステップ面**]、 [**スプライン面**]、 [**スプライン**]の各チャートが有効になっています。

10. [**間隔**]ドロップダウンメニューから時間範囲を選択します。

    間隔には10分から180分の時間範囲を指定でき、各間隔の間に10分の隔たりがあります。

注 :デフォルトでは、各チャートに表示されるレコード(上位)の数は**15**個です。

11. (オプション) [**ダッシュボード**] > [**デフォルト ダッシュボード**]ビューにチャートを追加するには、[**デフォルトのダッシュボードに追加**]チェックボックスを選択します。

注 :チャートを作成した後、デフォルトのダッシュボード ビューで追加の設定を実行できます。

12. [**作成**]をクリックします。

成功メッセージが画面に表示されます。

13. レポートを表示するには、以下のいずれかを実行します。

- **レポート チャート ビューの場合** :表示される成功メッセージで[**チャートの表示**]ハイパーリンクをクリックします。[**管理**] > [**ルール**]ページが表示されます。[**チャート**] > [**チャートの調査**]フォルダーをクリックすると、生成されたグラフが表示されます。
- **デフォルト ダッシュボード ビューの場合** :表示される成功メッセージで[**チャートの表示**]ハイパーリンクをクリックすると、[**ダッシュボード**] > [**デフォルトのダッシュボード**]ページでチャートを直接開くことができます。

調査ビューからイベント ウィジェットを作成する

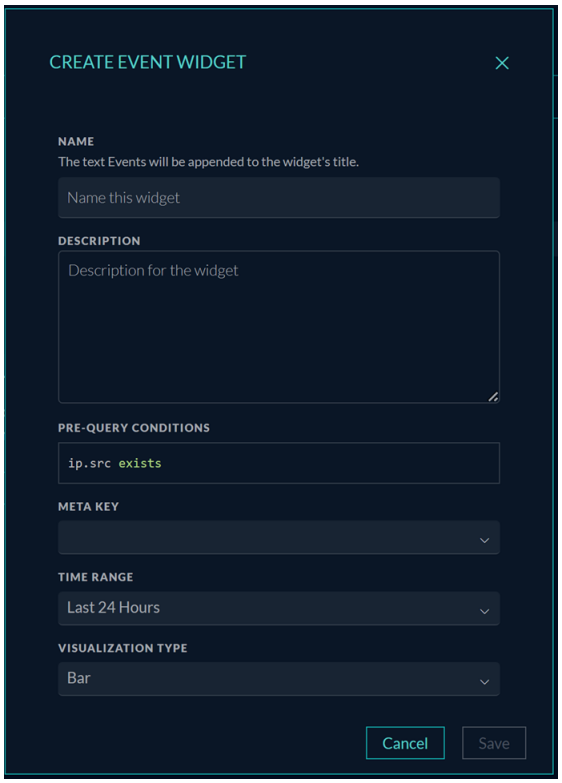
NetWitness Platform 12.5以降では、ユーザーは **[調査]** > **[イベント]** ビューからイベント ウィジェットを作成できるようになりました。ユーザーは、クエリ検索バーにメタ キーと演算子を含む任意の数のクエリ フィルターを追加し、それらを脅威ハンティングと調査のための重要なシステム指標を含んだイベント ウィジェットに変換できます。

まず、[**調査**] > [**イベント**]ビューを使用して、特定のメタを照会し、イベント ウィジェットを作成する必要があります。2番目のステップは、**ホーム** ページのダッシュボード レイアウトにイベント ウィジェットを追加することです。その後、ユーザーは自分の好みに応じてイベント ウィジェットをカスタマイズして配置できます。

ステップ1：[調査]ビューからイベント ウィジェットを作成する

1. NetWitness Platformにログインします。
2. [**調査**] > [**イベント**]に移動します。
3. メタキー、演算子、およびオプションの値を含む1つ以上のフィルターで構成されるクエリを作成します。たとえば、**ip.srcが存在します**。
4. 3つのドット( )アイコン > [**イベント ウィジェットの作成**]をクリックします。

[イベント ウィジェットの作成]ダイアログが表示されます。



5. 次の詳細情報を入力します。
   a. **名前**:ウィジェットの一意の名前を入力します。名前には、アルファベット、数字、スペース、_ - ( ) [ ] などの特殊文字を含めることができます。

      注 :イベントというテキストがウィジェットのタイトルに追加されます。たとえば、名前 **ipv4**を入力すると、ウィジェットのタイトルは **イベント - IPV4**として表示されます。

   b. **説明**:構成の簡単な説明を入力します。

      注 :右側のテキスト ボックスの下隅にカーソルを置いてボックスをドラッグすると、テキスト領域のサイズを大きくすることができます。

   c. **プレクエリー条件** :クエリー検索パネルに入力した入力基準に基づいて表示されます。

   d. **メタキー**:ドロップダウン リストから、サービスで使用可能な必要なメタ キーを選択します。たとえば、 [**ip.all – すべてのIPV4キー**]などです。

   e. [**時間範囲**] :ドロップダウン メニューから特定の期間を選択すると、その期間のデータが表示されます。**過去5分間**から**過去7日間**までの任意の時間範囲を過択できます。デフォルトでは、**過去24時間** が選択されています。

   f. **チャートのタイプ** :ドロップダウン メニューから必要な視覚化タイプを選択します。 [**棒**]または [**ドーナツ**]を選択できます。

6. 「**保存**」をクリックします。

7. ダイアログを閉じるには、**X** または **キャンセル** をクリックします。

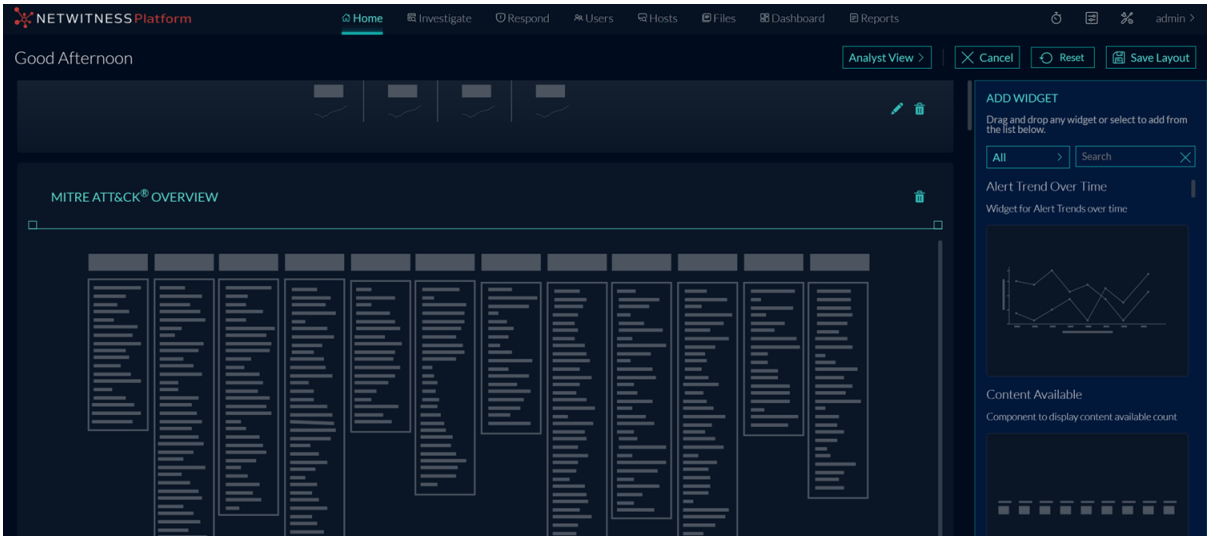
   ウィジェットに加えた編集内容は、変更を行ったユーザーにのみ反映されます。

ステップ2 :ダッシュボードレイアウトにイベントウィジェットを追加する

ユーザーはダッシュボードにイベント ウィジェットを追加できます。追加できるウィジェットの数に制限はありません。

ダッシュボードにイベントウィジェットを追加するには

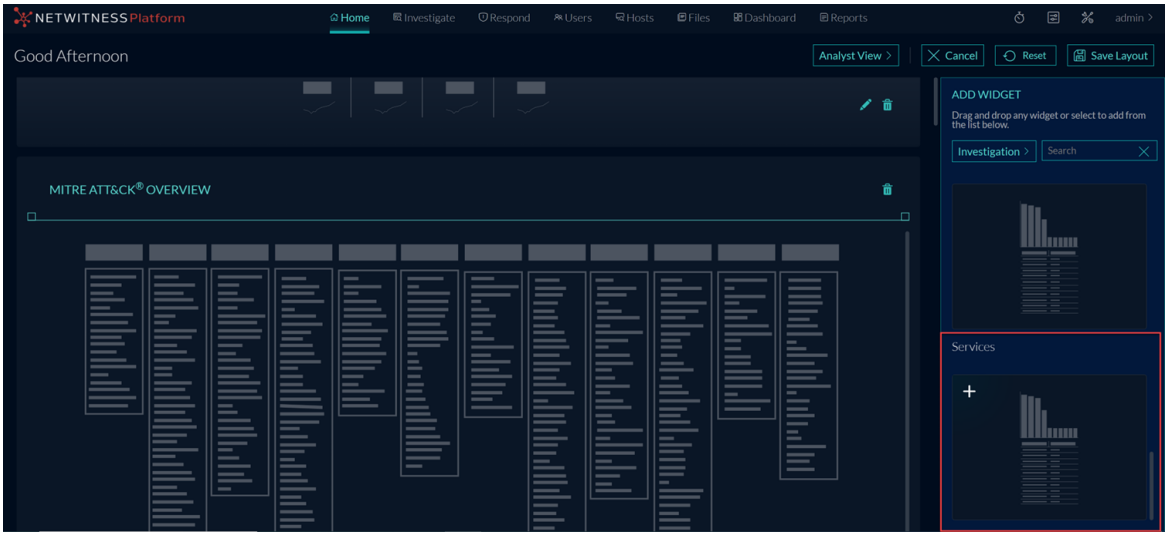
1. [ホーム]ページに移動します。
2. **ホーム** ページの右上隅にあるドロップダウン メニューから、追加するビュー (**管理者**、**アナリスト**、または **マネージャー**) を選択します。
3. 右上隅にある **レイアウトの編集** ボタンをクリックします。**ウィジェットの追加** パネルには、使用可能なすべてのウィジェットが表示されます。



注 :イベント ウィジェットをすばやく見つけるには、次のいずれかを実行します。
- 検索フィールドに名前を入力します。入力するとウィジェットがフィルターされ、一致する結果のみが表示されます。
- ドロップダウン メニューから、**調査**を選択します。イベントの調査に関連するウィジェットが表示されます。

4. イベント ウィジェットを追加するには、次のいずれかの手順に従います。
   a. イベント ウィジェットの上にカーソルを移動すると、左上隅に + (追加) アイコンが表示されます。+ アイコンをクリックして、イベント ウィジェットを追加します。これにより、レイアウトの下部にイベント ウィジェットが追加されます。
   b. または、ウィジェットをクリックしてダッシュボード上の目的の場所にドラッグします。ウィジェットをド

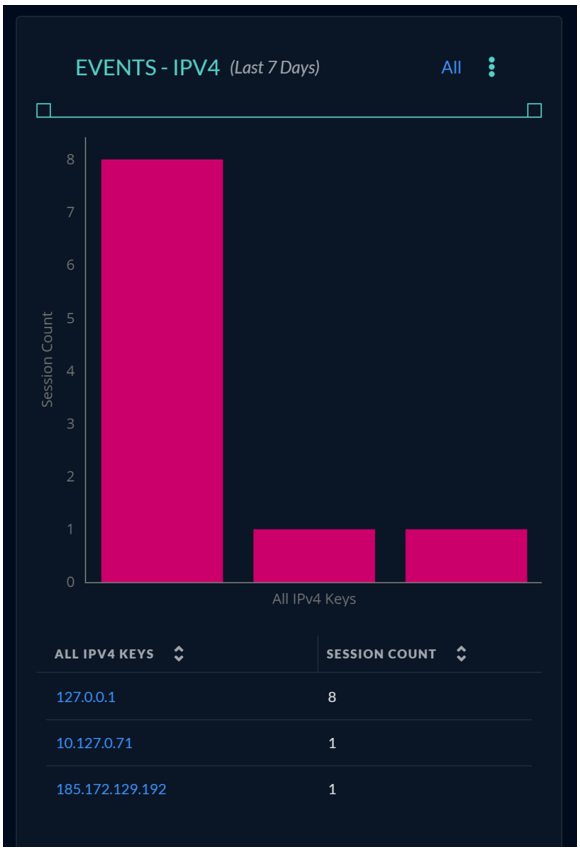
ラッグすると、ダッシュボードにターゲットの位置が表示されます。



5. [**レイアウトを保存**]をクリックして、イベント ウィジェットをダッシュボード レイアウトに追加します。

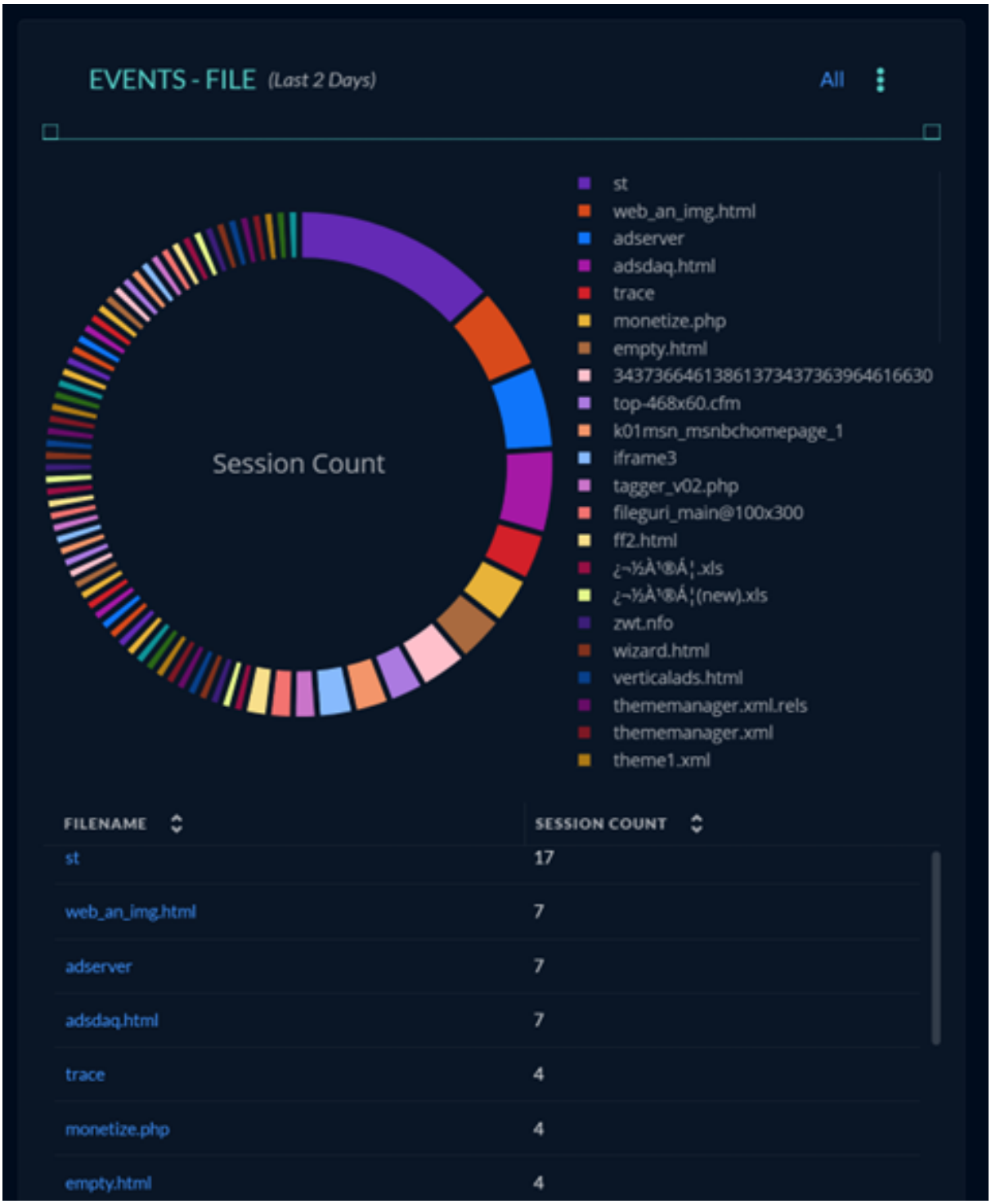
イベント ウィジェットがダッシュボード レイアウトに正常に追加されました。

注：
- [キャンセル] ボタンをクリックすると、ダッシュボード レイアウトに加えられた未保存の変更はすべて破棄され、パネルが閉じられます。
- 指定された時間範囲でメタ値のデータが利用できない場合は、チャートにデータは表示されません。



ウィジェットの右上隅にある3つのドット( )アイコンをクリックし、 **構成**]をクリックして、好みに応じてイベント ウィジェットをカスタマイズします。

以下は、ファイル名メタ用に構成された **イベント** ウィジェットの例です。簡単に識別できるように、各ファイル名をドーナツ チャートで異なる色で表示します。



組み込みのイベント ウィジェットのトピックには、構成オプション、ウィジェットに表示される情報、イベントで実行できるアクションに関する詳細が記載されています。詳細については、イベント ウィジェットを参照してください。

注 :レイアウトの変更は、それを行ったユーザーにのみ適用されます。

レイアウト のカスタマイズの詳 細については、『NetWitness Platform 12.5スタート ガイド』の「**ホーム ウィジェット の管 理** 」トピックで「**ダッシュボード レイアウト のカスタマイズ**」セクションを参 照してくださ い。

イベントの再構築と分析

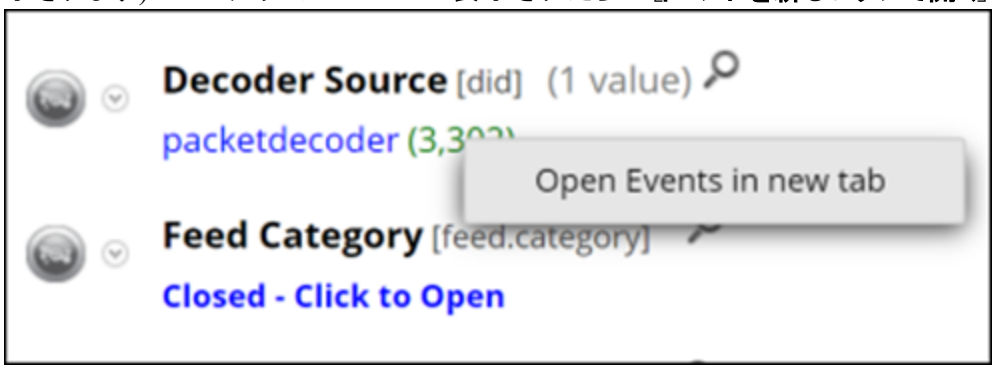
[ナビゲート]ビューまたは [イベント]リストでイベントを絞り込んだら(「結果セットの絞り込み」を参照)、次のステップは、イベントの再構築、添付ファイルの確認、サード パーティー ルックアップまたは内部ルックアップでの追加コンテキストの表示を行って、イベントについて詳しく理解することです。

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。

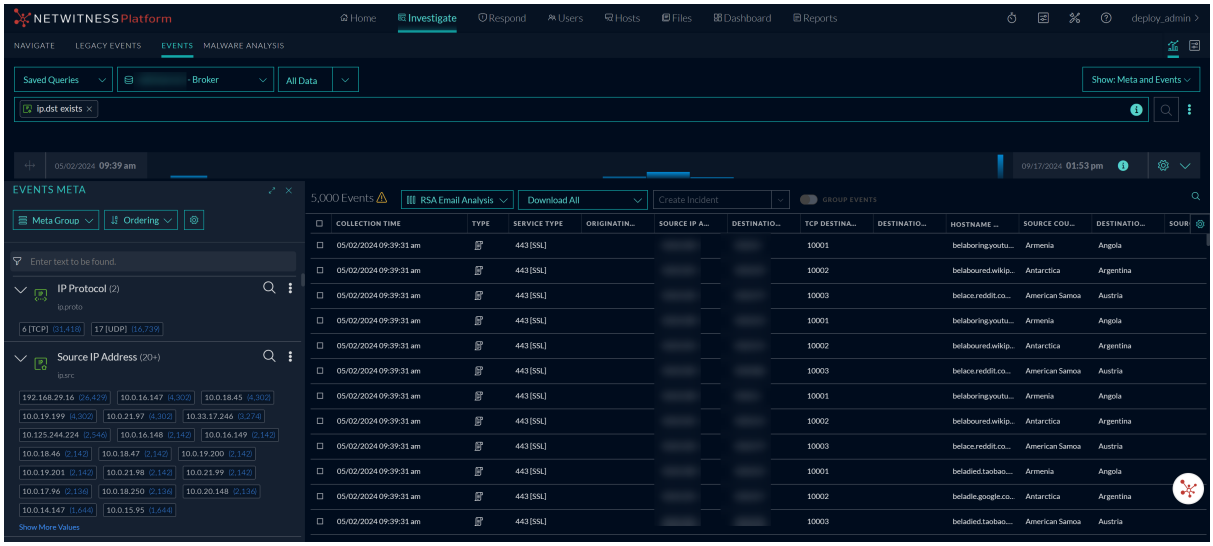
注： [レガシー イベント]ビューはデフォルトで無効になっています。管理者は、『*システム構成ガイド*』の「調査の設定の構成」の説明に従って有効にすることができます。

[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**]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。



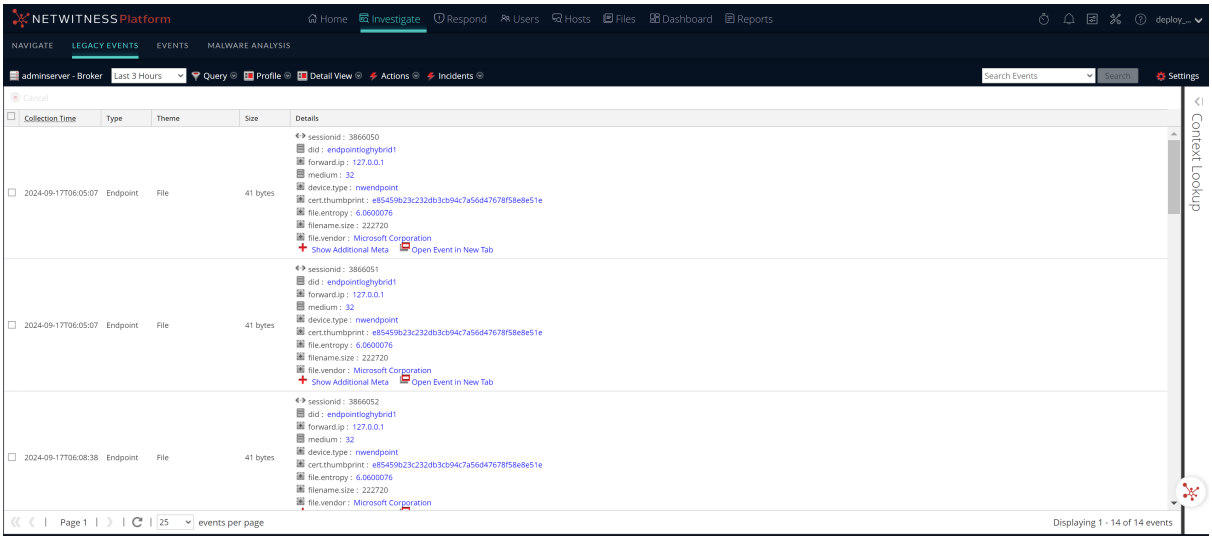
選択したメタ値のイベントのリストが [イベント]ビューに表示されます。



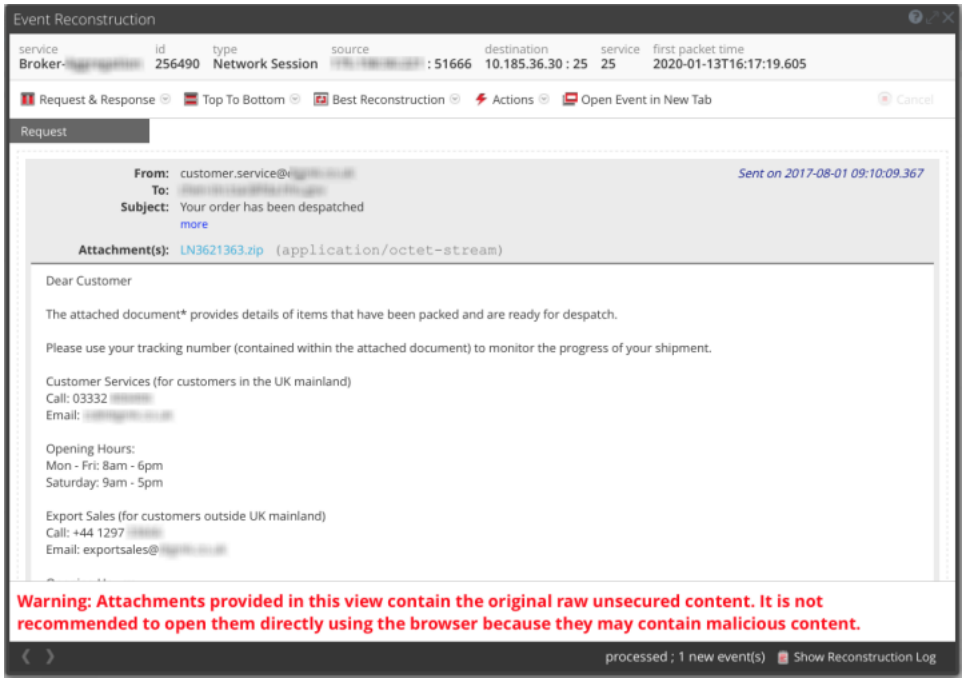
このビューで使用できる再構築と分析のタイプの詳細については、「 [イベント]ビューでのイベント詳細の調査」を参照してください。

[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 クエリーではすべてのイベントが選択され、選択したサービスのイベントが古い順に [イベント]ビューに表示されます。



3. 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 メタ]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では、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) を表示するタブ、またはエンドポイント データで強化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: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、「イベントビューでイベントを分析する」に記載されています。

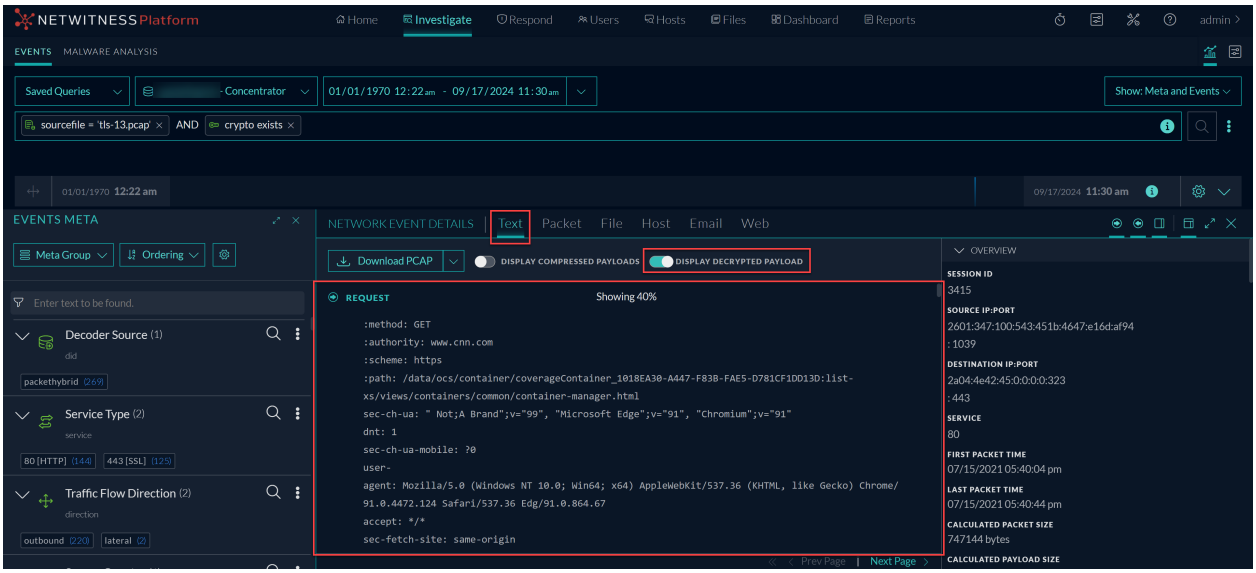
アクション	ネットワーク イベント	ログ イベント	エンドポイント イベント
テキストの再構成を表示します(最後に選択した内容でオーバーライドされない場合はデフォルト)	✓	✓	✓
ファイルの再構築を表示します	✓		
拡張ネットワーク可視性で構成されたエンドポイント エージェントのホスト情報を表示します(「ホスト情報」を参照)。	✓		
パケットの再構築を表示します	✓		
Eメールの再構築を表示します	✓		
(バージョン12.5以降) Web再構築を表示	✓		

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。

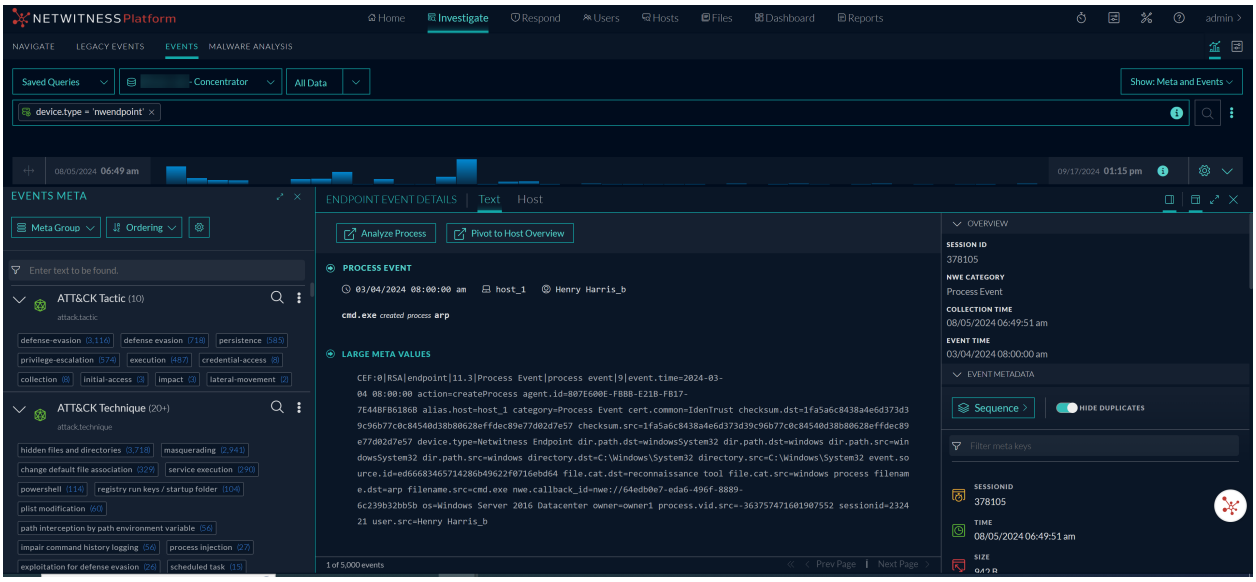
- 現在選択されている再構築 :テキスト、パケット、ファイル、ホスト、Eメール、Web(バージョン12.5以降)
- [イベント メタ]パネルの表示、非表示。
- [イベント]ヘッダーの表示、非表示。
- リクエスト、レスポンス、またはその両方の表示、非表示。
- パケットの再構築にパケット ペイロードをヘッダーなしで表示するかどうか。
- パケットの再構築でバイトを濃淡化するかどうか。
- パケットの再構築にその他の一般的なファイル タイプをハイライト表示するかどうか。
- パケットの再構築のページあたりのパケット数。
- テキストの再構築で圧縮したテキストと展開したテキストのどちらを表示するか。

テキストの再構築

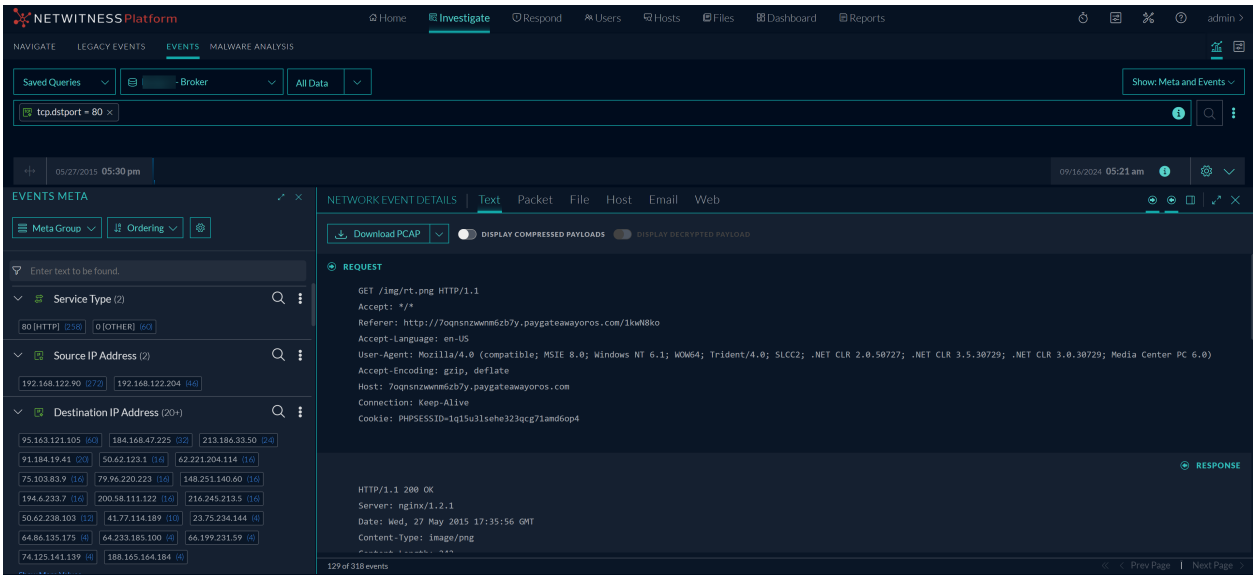
[**復号化されたペイロードの表示**]トグル オプションで切り替えて、暗号化されたデータを、アナリストが直接、復号化された形式で表示できます。ただし、復号化された形式でデータを表示できるのは、[**イベント**] > [**テキスト**]タブのDecoderサービスでTLSキーを使用できる場合のみです。この機能により、アナリストは、より短時間で重要なデータに集中し、最適な精度と品質で、選択したイベントの調査を実施することができます。

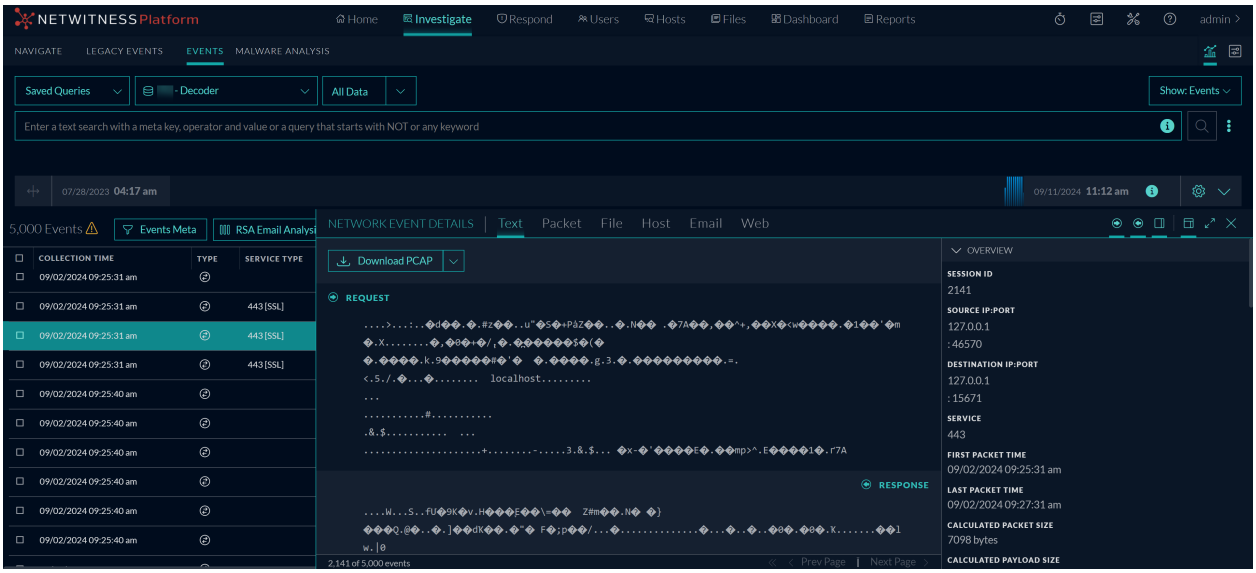


エンドポイント イベントの詳細については、[**プロセスの分析**]および[**ホストの概要に移行**]オプションをクリックして、さらに詳しい調査を実行できます。



［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。





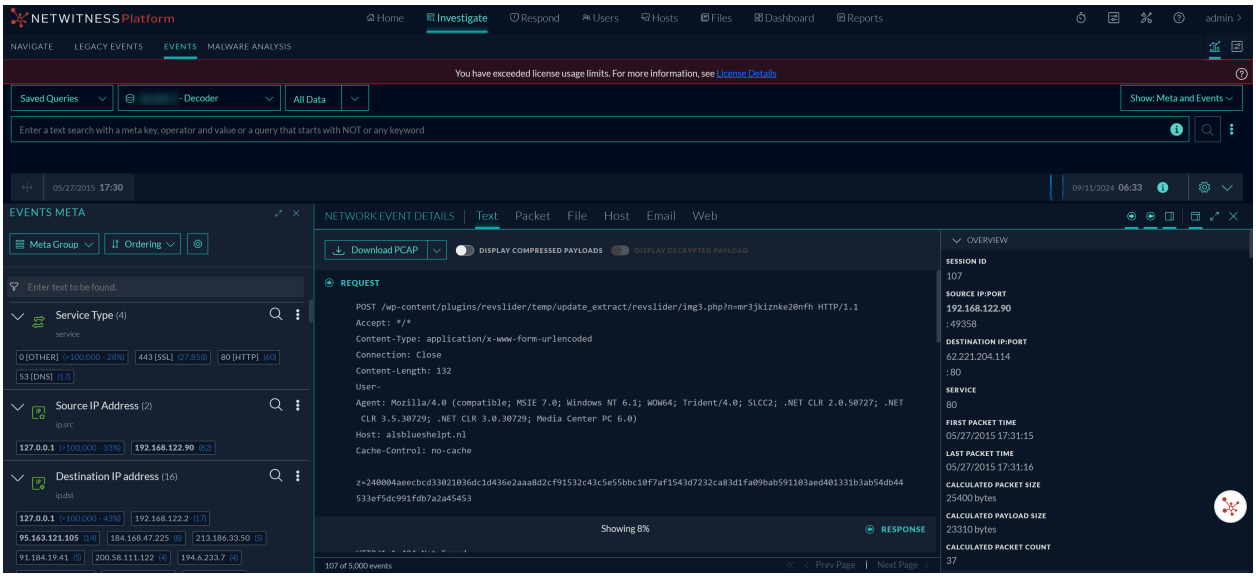
注 :大きなペイロードは異なる方法で処理されます。1つのイベントのペイロードは2,500パケットに制限されます。パケットの制限に達すると、フッターに警告が表示され、制限に達したことを通知し、イベント内のパケットの総数を示します。 [さらに表示]オプションは、トランケートされたメッセージでも使用できます。ただし、RAWペイロードをダウンロードしないと、メッセージのテキスト全体が表示されません。

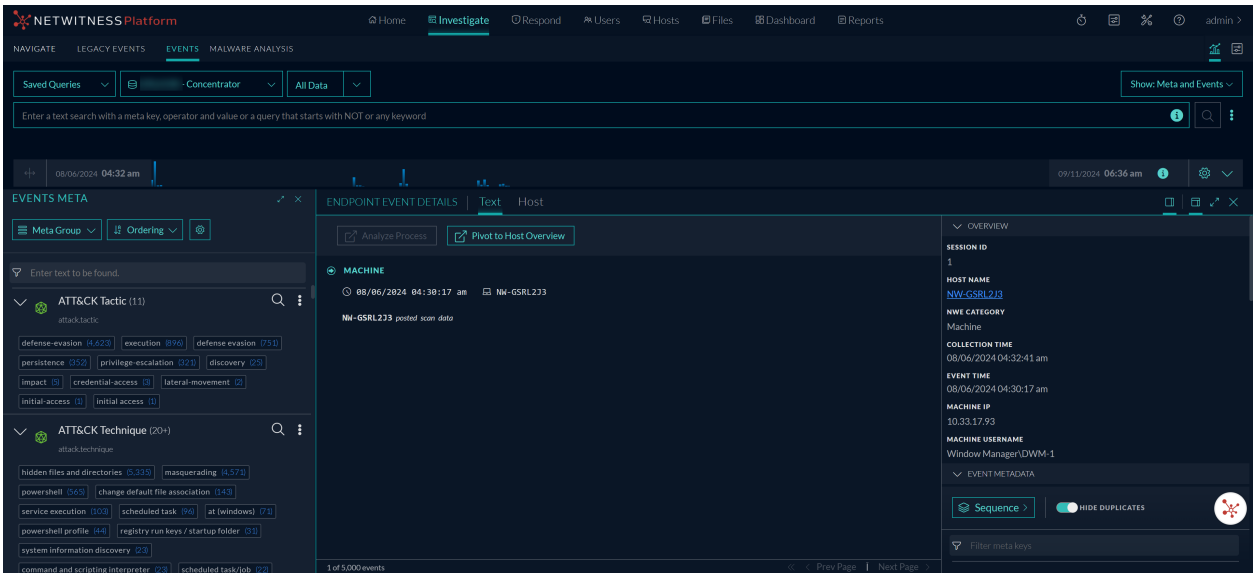
テキストの再構築では、ネットワーク イベント、ログ イベント、エンドポイント イベントの表示は異なります。

- 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。
- 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含む読みやすいJSONツリー ビューでレンダリングされます。

概要］パネルと、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。





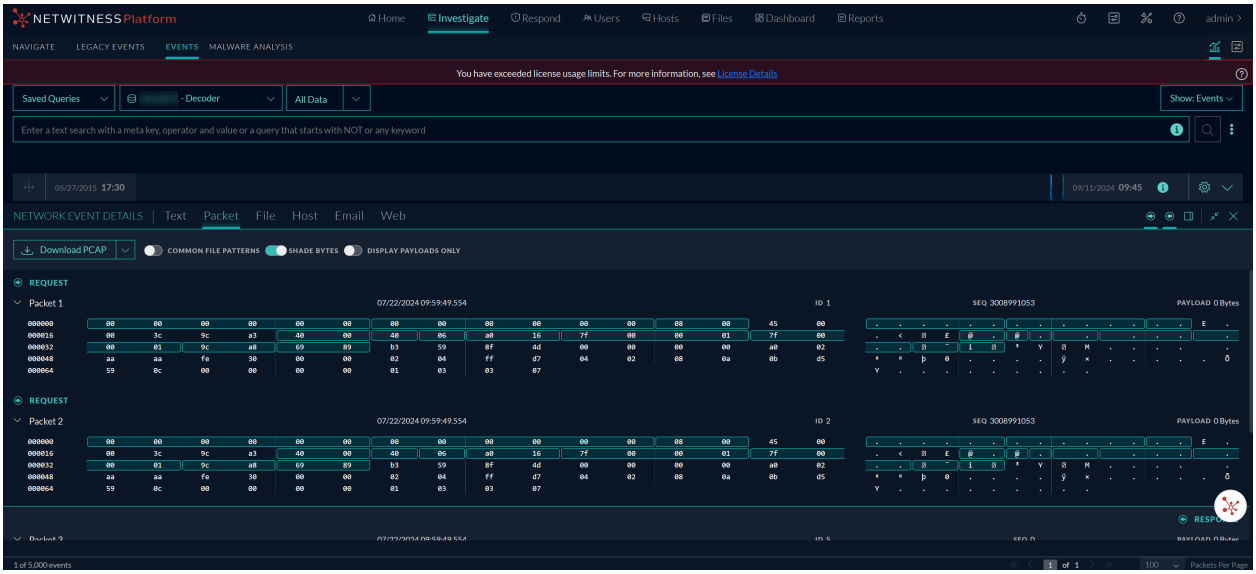


注 :イベント ヘッダー内の計算済みパケット数、計算済みパケット サイズ、計算済みペイロード サイズが、 [イベント メタ] パネル内の同じ統計と異なっている場合があります。これは、イベントのパースが完了する前にメタデータが書き込まれ、パケットが重複して計算されることがあるためです。

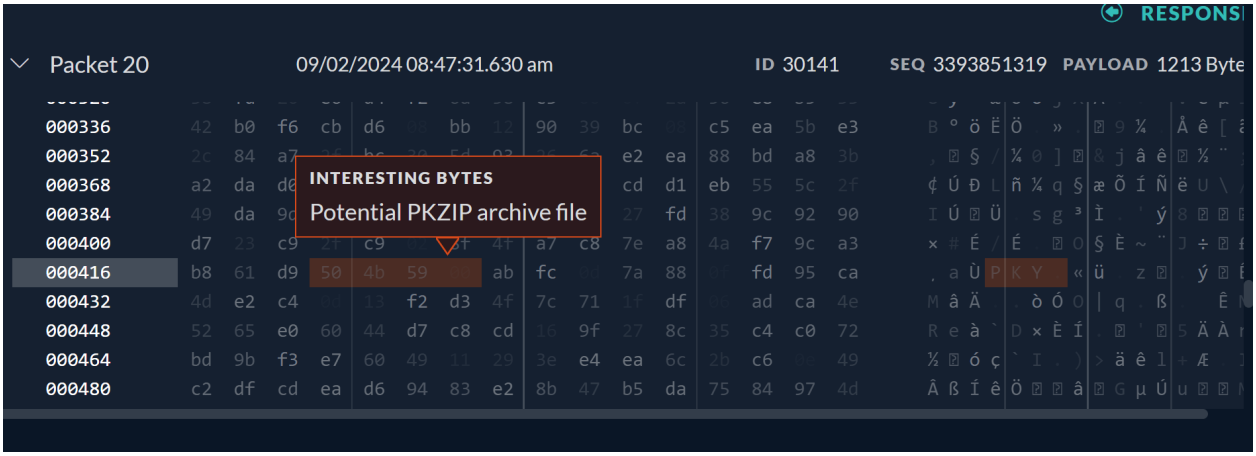
パケットの再構築

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。

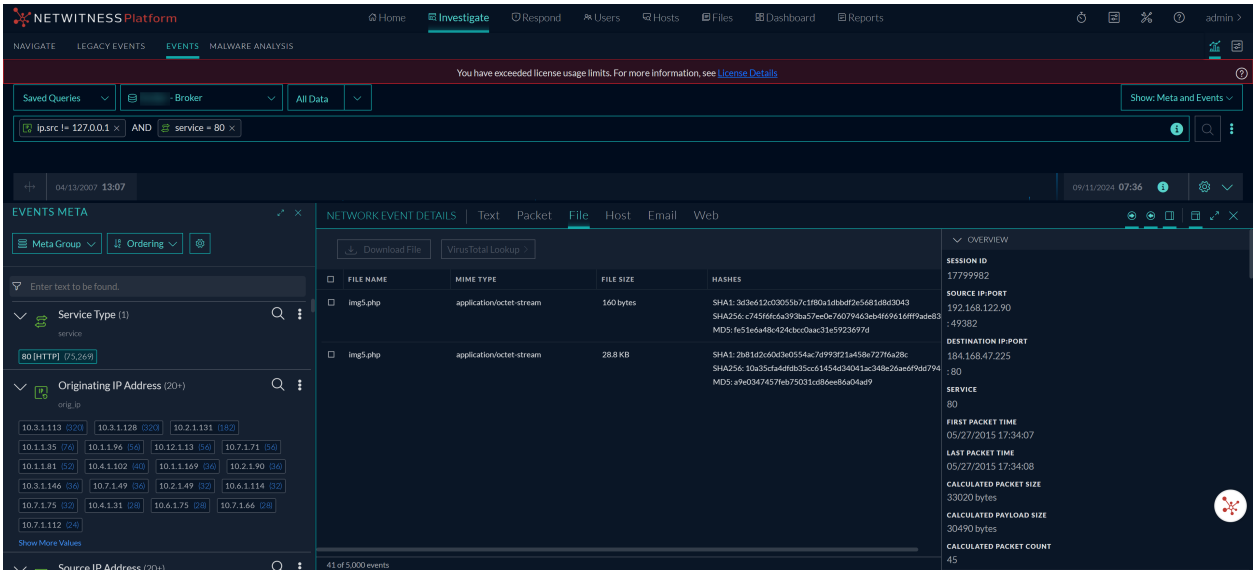


一般的なファイル シグネチャは、オレンジ色の背景色でハイライト表示されます。ハイライト表示されたテキスト上にカーソルを置くと、ポップアップにファイルのタイプの説明が表示されます。

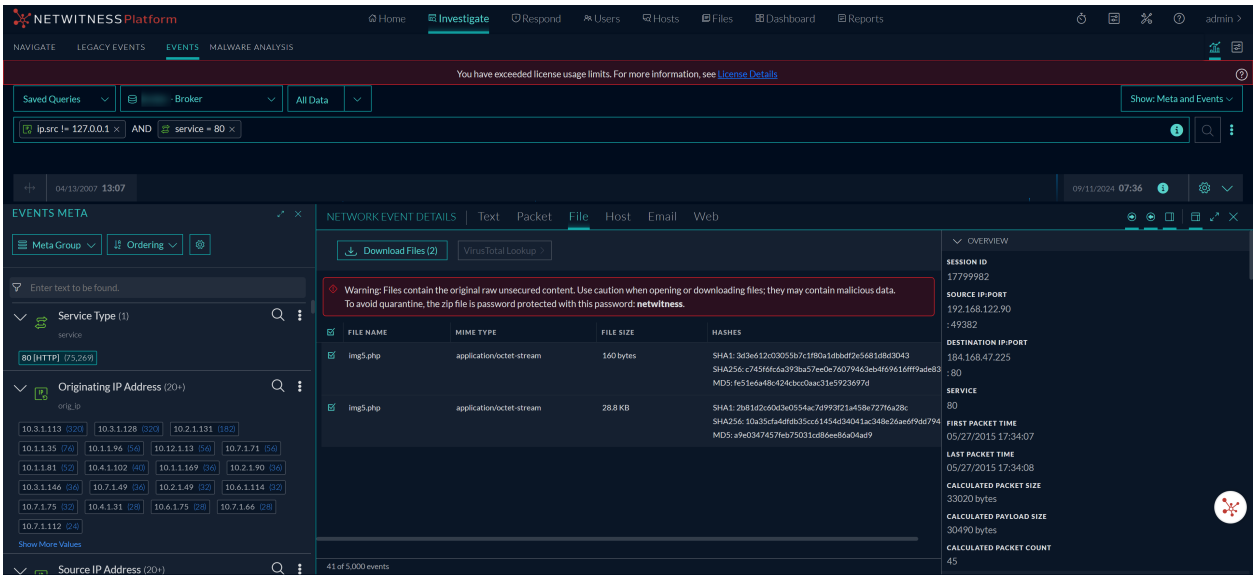


ファイルの再構築

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。



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。



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

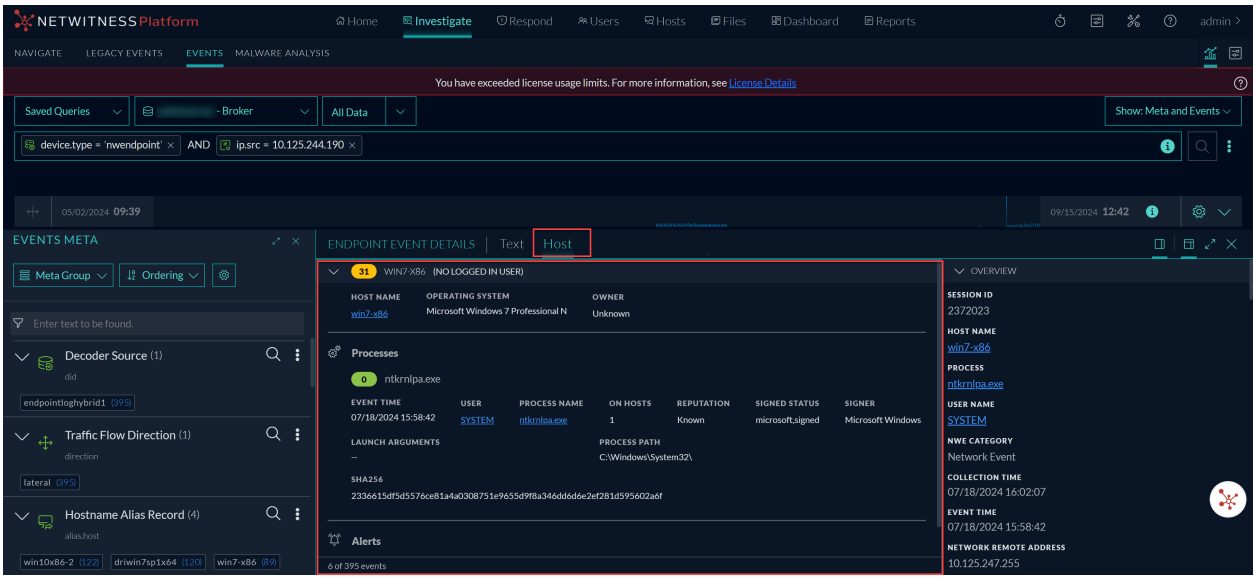
ネットワークおよびエンドポイント イベントのホスト情報が、エンドポイント データとともに表示されます。

イベント メタ パネルを使用して、イベント ビュー内のイベントをフィルターできます。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。



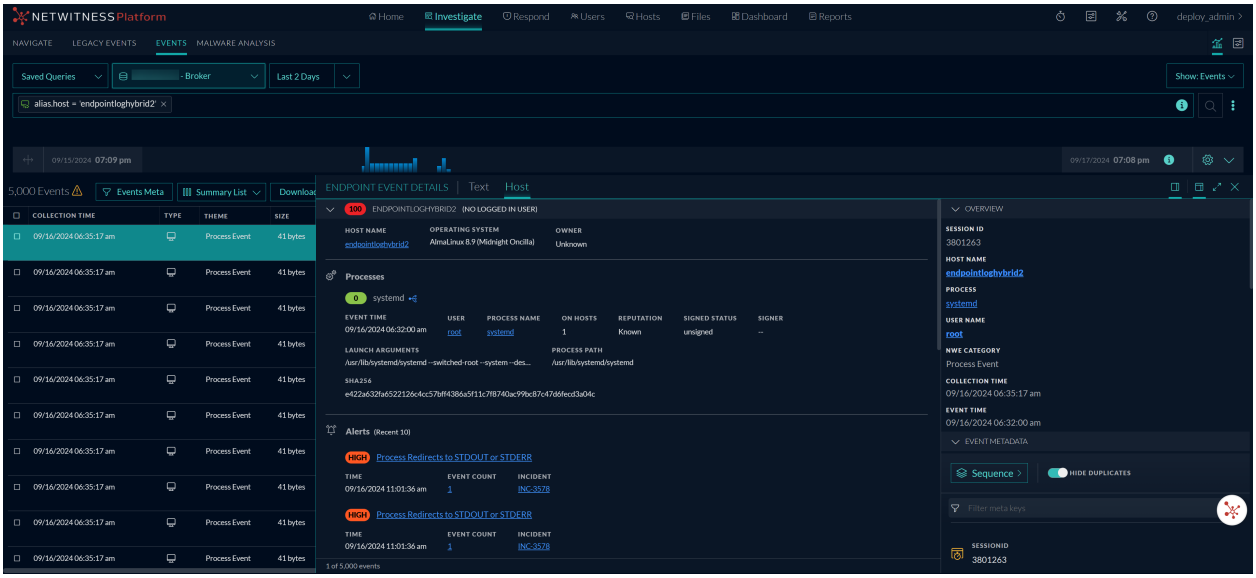
- 最も一致するプロセスを持つホストがイベント時間の順にリストされます。
- デフォルトで最初のホストが展開され、次のような追加情報を確認できます。
  - ホストの詳細 – ホストのオペレーティング システムと、ホストに関連づけられている管理責任者 (ログインしているユーザー) の詳細が表示されます。
    - ホスト名を調査するには、青色で強調表示されている [**ホスト名**] リンクをクリックします。詳細については、『*NetWitness Endpointユーザー ガイド*』の「ホストの調査」を参照してください。
    - ユーザーに関連づけられているアラートを調査するには、青色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 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、『*Net Witness 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、ティール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。

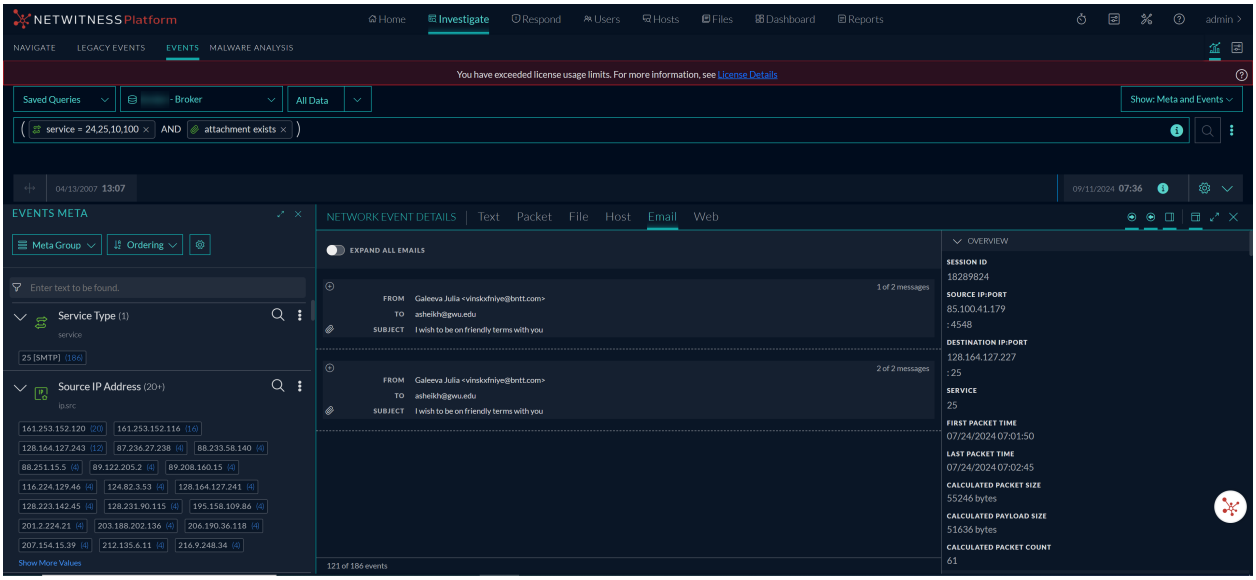
以下は、選択したネットワーク イベントに関連づけられている単一のホスト、プロセス、およびユーザーが表示された［ホスト情報］タブの例です。`systemd` は、ホスト `endpointloghybrid2` およびログインしたユーザー `root`に関連付けられたプロセスです。



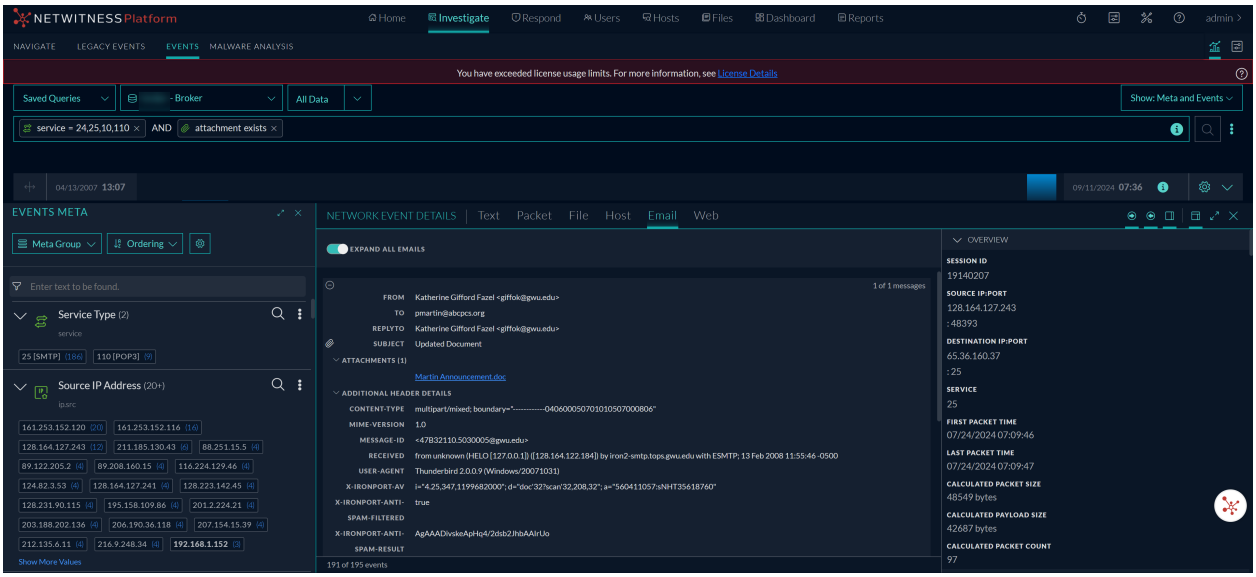
注 :選択したネットワーク イベントに対して複数のホストとプロセスがトリガーされる場合があります。このような場合、最初にイベントのトリガー元になったホストが最初にリストされ、次に同様のイベントがトリガーされた他のホストがリストされます。
たとえば、`10.63.0.240`というIPアドレスがHost1に割り当てられ、User1がマシンにログインし、Chromeを使用して`www.nyu.edu/`にアクセスしているとします。その間、Host1の電源はオフになり(30分以内)、同じIPアドレスがHost2に割り当てられます。ログインしているユーザはUser2で、Internet Explorer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 - `User1`、`User2`

メールの再構築

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。

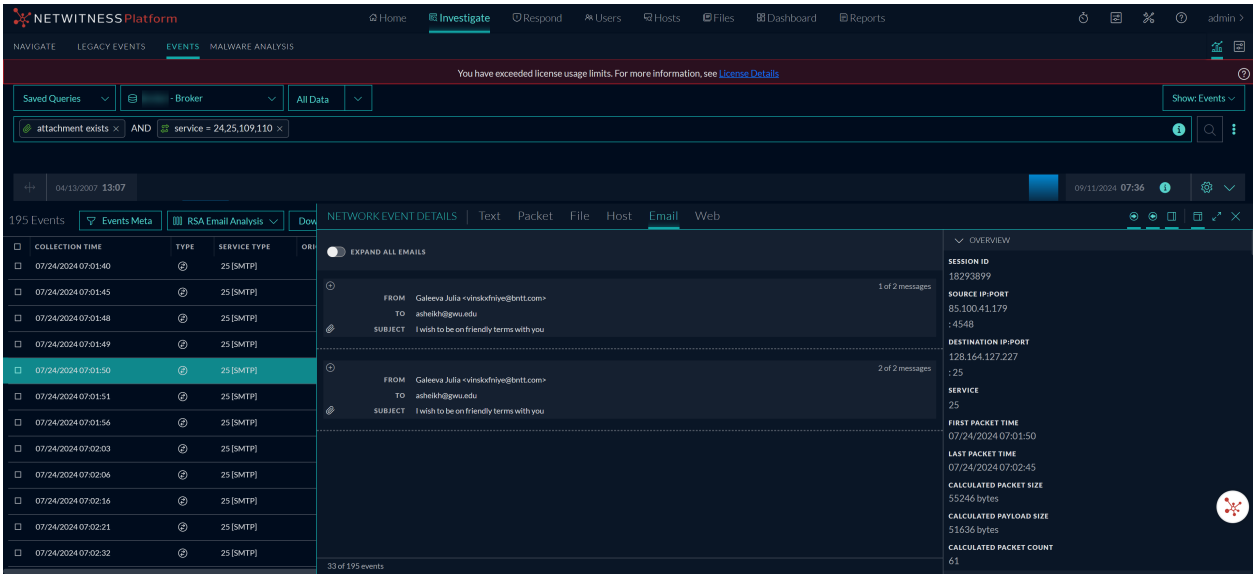


［すべてのメールを展開］トグル ボタンをオンにすると、メールの内容が展開された形式で表示されます。



［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。
- Eメールの本文が長すぎると、E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。そうでない場合は、「*このイベントでは電子メールの再構築は利用できません*」というメッセージが表示されます。

ウェブ再構築

NetWitness Platformバージョン12.5以降では、ユーザーが特定のイベントに関連するWebページにアクセスした場合、アナリストは[**イベント**]> [**Web再構築**]ビューから対象イベントのWebビューを安全に再構築できます。NetWitnessは、パケット内で利用可能なデータを使用してWebページを表示し、それをイメージやCSSスタイルにできるだけ正確に関連付けることで、同じWebページを再構築できます。このWeb再構築プロセスにより、アナリストは実行されたWebアクティビティに関する貴重な洞察を得ることができ、効果的な分析と調査が容易になります。

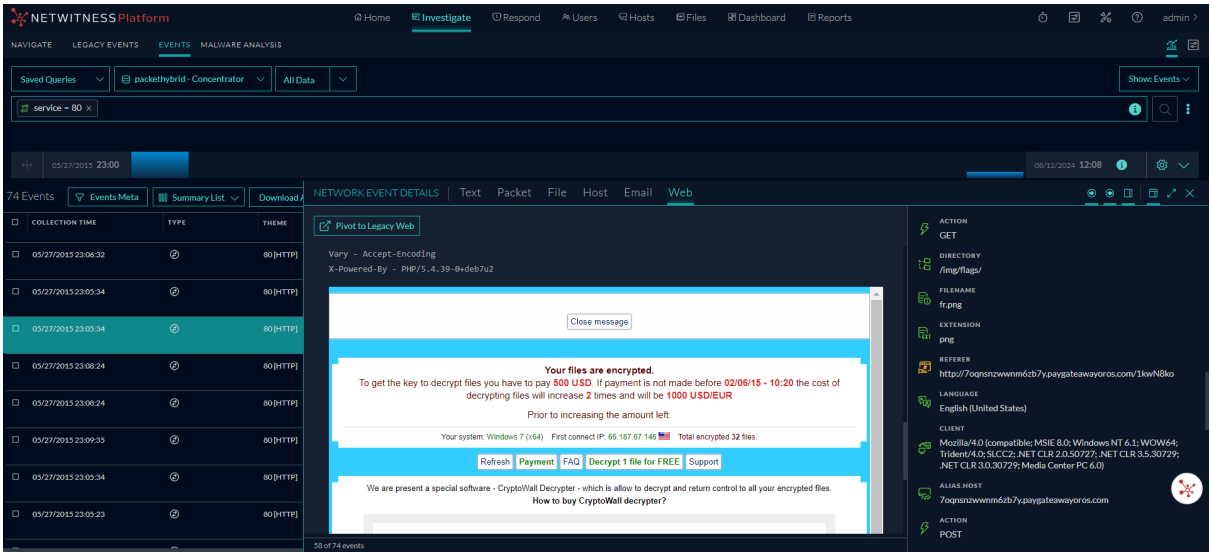
注：NetWitnessでは、アナリストがWeb再構築を確認する際に、潜在的に悪意のある要素が動的コンテンツによって誤って実行されるのを防ぐため、Webページ全体は表示されません。

たとえば、アナリストが特定のWebページにアクセスするユーザーに関連するイベントを調べる場合、再構築されたイベントをクリックしてコンテンツ内を移動し、ネットワークトラフィックから抽出されたHTMLコンテンツ、CSSスタイル、画像、JavaScriptコードなどの貴重な情報を表示して、コンテキストをより深く理解することができます。このインタラクティブな再構築アプローチにより、アナリストは複雑なWeb再構築の相互作用を簡単かつ効率的に調査できます。

イベントビューでWebイベントを再構築するには

1. NetWitness Platformにログインします。
2. [**調査**] > [**イベント**]に移動します。
3. ネットワーク イベントを含むセッションのWeb再構築に進みます。

   Web再構築では、選択したネットワーク イベントに関連付けられたWebセッションのレンダリングが示されます。これはWeb再構築の例です。



4. (オプション) [**レガシーWebに移行**]をクリックして、Web再構築のレガシー ビューに移動します。

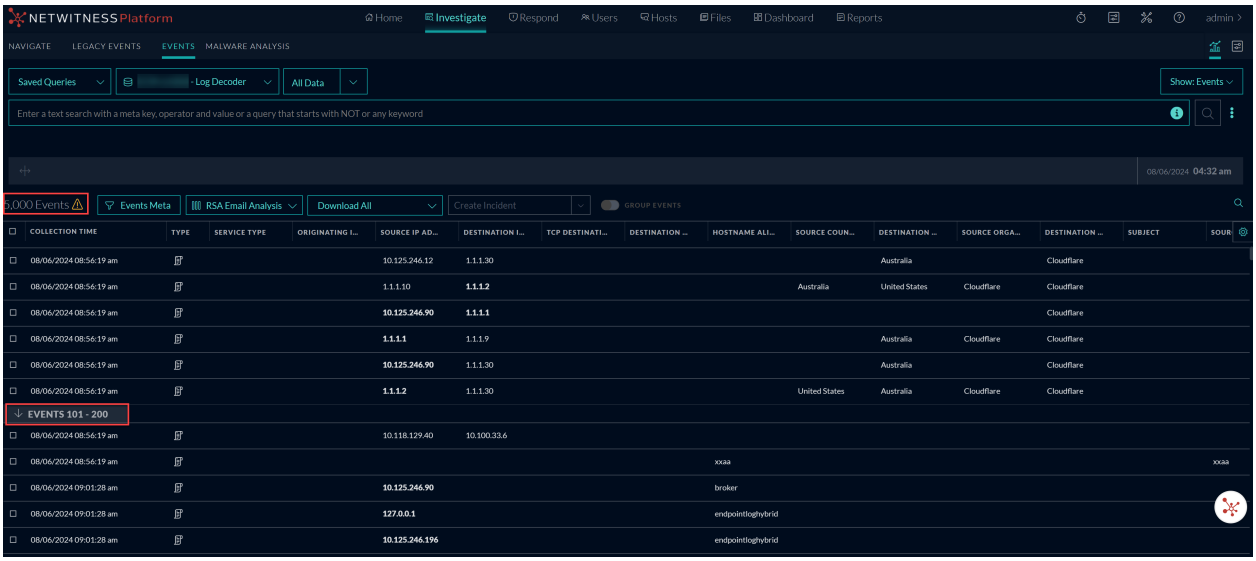
イベントビューでイベントを分析する

［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。昇順のソートは、最も古いイベントを最初にロードしますが、これは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、次回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**: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**: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」に変更する必要が生じることがあります。
- **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(「保存済みクエリを使用した調査の共通領域のカプセル化」)。
- 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(「イベントビューでメタデータのドリルダウン」)。

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] パネルが開き、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) を表示するタブ、またはエンドポイント データで強化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。

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

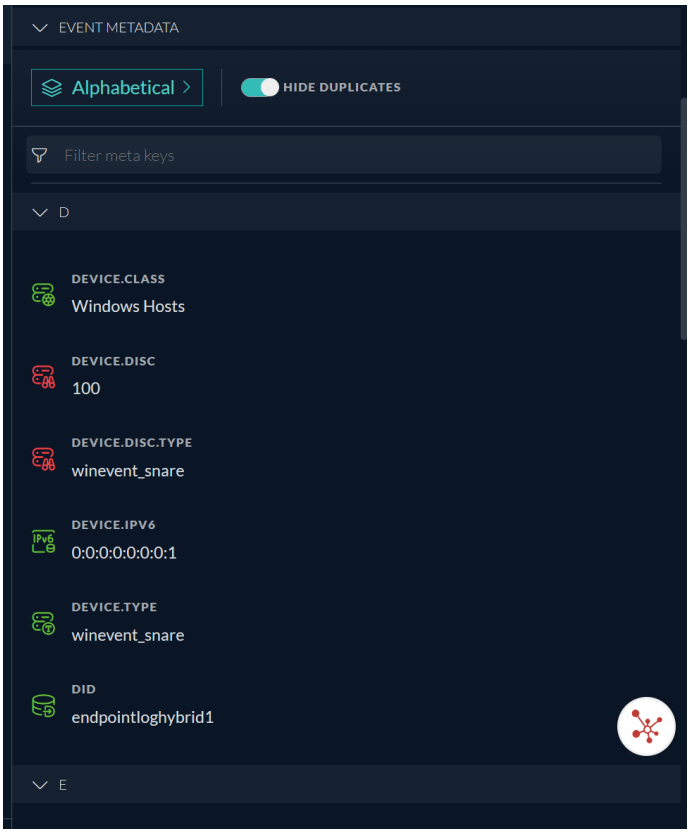
リクエストとレスポンスがある分析タイプの場合は、会話のどちら側 (リクエスト、レスポンス、または両方) を表示するかを選択できます。方向アイコンのいずれかまたは両方をクリックします。選択した情報で、再構築されたイベントが更新されます。

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。

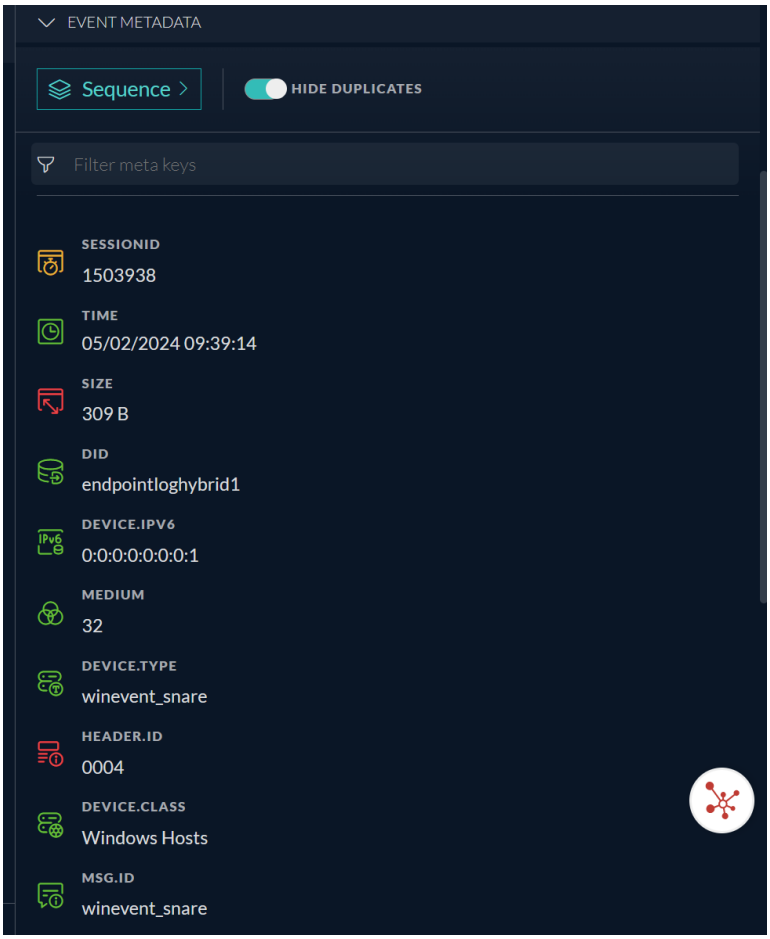
イベントの関連メタデータを表示する

[テキスト] タブ、[パケット] タブ、[ファイル] タブでイベントを調査しているときに、をクリックして、隣接する [イベント メタ] パネルに関連するメタデータを表示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く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。

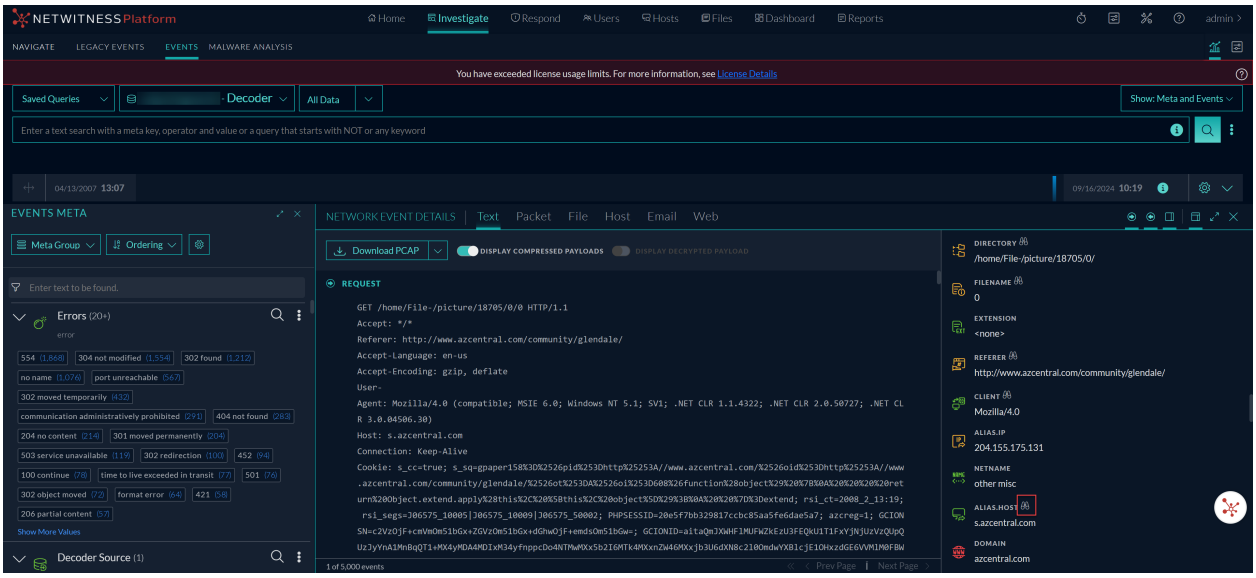
探しているものをより簡単に見つけられるように、イベント メタデータ パネルにリストされているメタデータの順序を変更できます。メタデータは、生成された順序で整理することも、メタ キーのアルファベット順に整理することもできます。次の図は、メタ キーのアルファベット順で並べたメタデータを示しています。



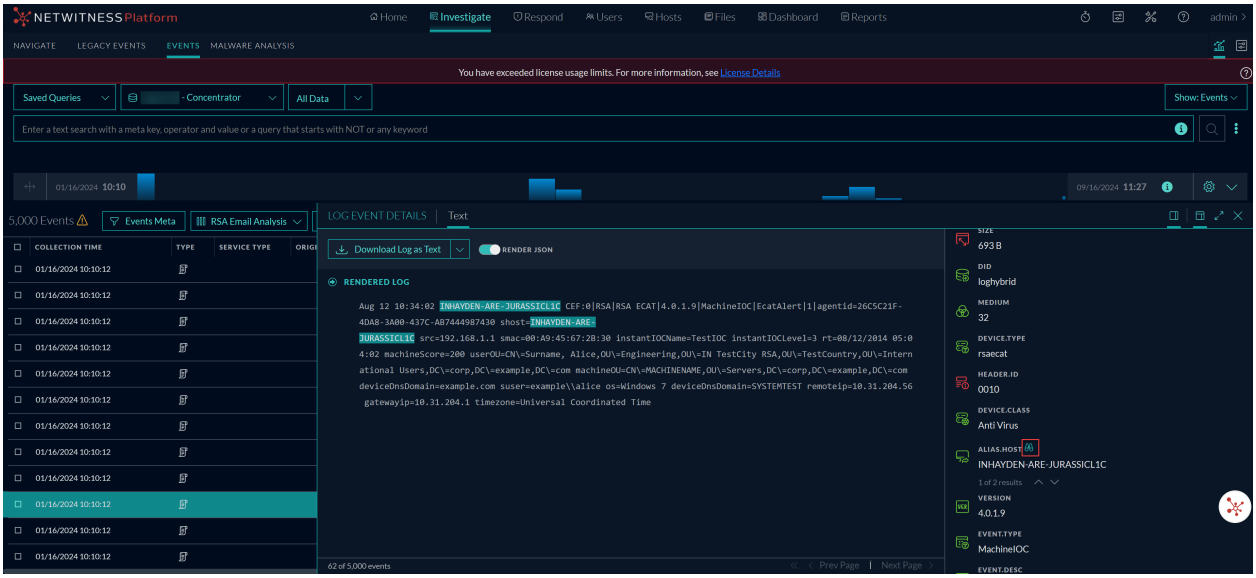
次の図は、生成された順に並べられた、同じメタデータを示しています。



［イベント メタ］パネルでテキスト再構築再構成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、検索オプションを示す双眼鏡アイコンが表示されます。この機能拡張により、アナリストは検索可能なメタを探すために、すべてのメタデータを調べる代わりに、双眼鏡アイコンで確認することができるようになりました。この機能拡張により、アナリストに双眼鏡アイコンで直接、検索機能が表示されるため、検索可能なものを探すために、すべてのメタデータのリストを調べる必要がなくなります。次の図は、検索可能なメタ キーを示すマークする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 のペアをクリックすると表 示 される、青 い背 景 の双 眼 鏡 アイコンの例 です。

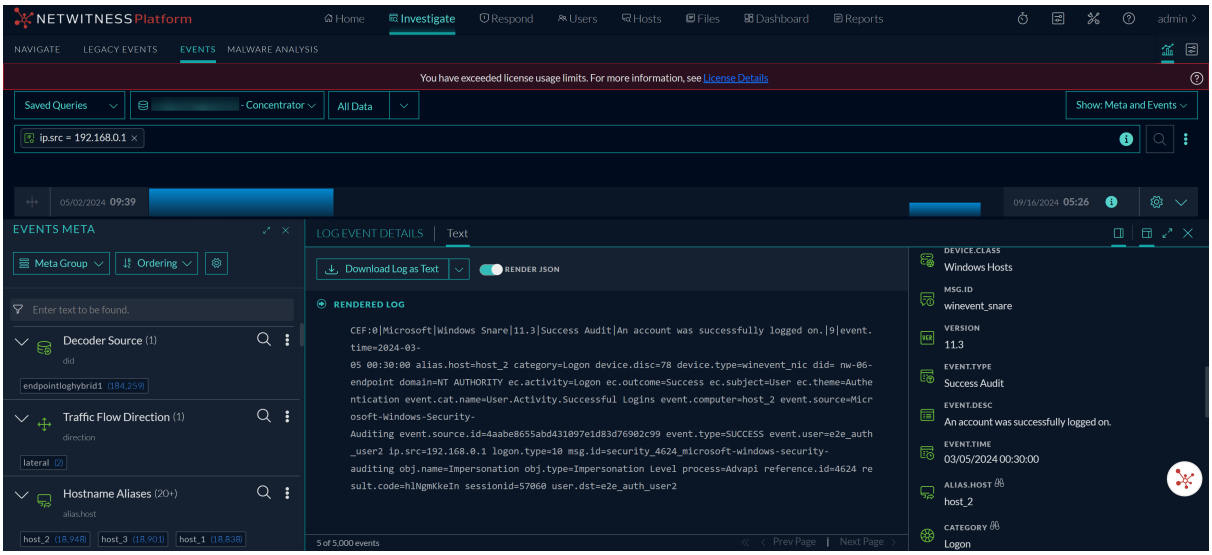


［イベント メタ］パネルには、ハイライト表 示 された行 に結 果 の件 数 が示 され、上 下 矢 印 が表 示 されます。この矢 印 を使 用 して、［テキスト］タブでそれぞれの結 果 にすばやく移 動 することができます。スクロール ボタンを使 用 すると、メタ キーの生 成 をトリガーしたデータがハイライト表 示 された場 所 を、1つずつ前 に、または1つずつ後 ろに移 動 して表 示 することができます。

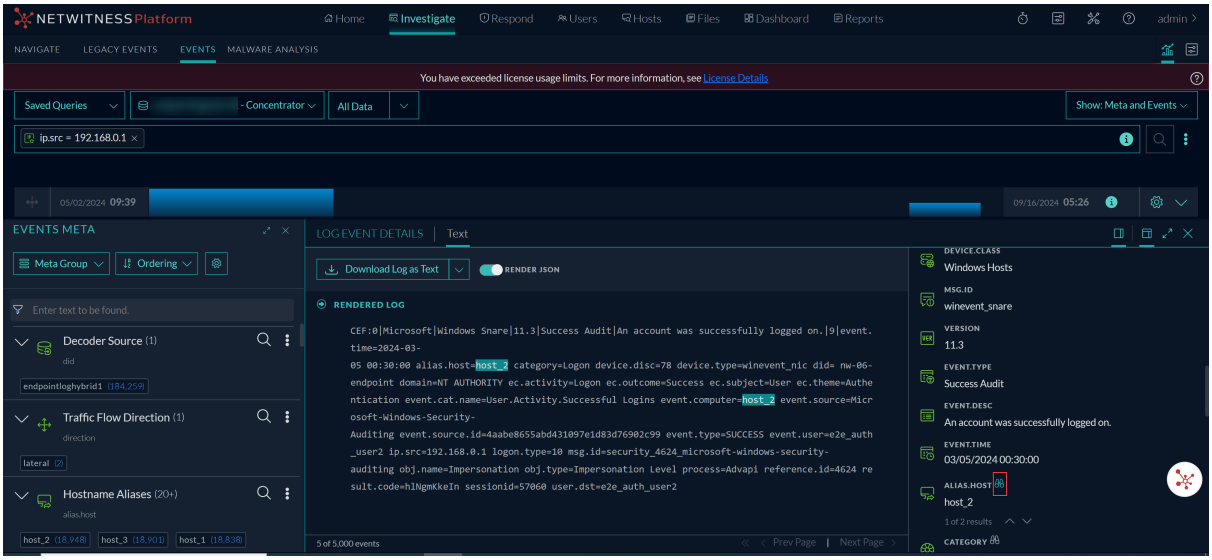
RAWテキスト内 に関 連 する値 が存 在 するメタ キーのみを検 索 できます。一 度 に検 索 できるメタ キーは1つだけです。3000文 字 を超 えるためトランケート表 示 されたテキスト エントリーは、検 出 されたメタ値 が見 えるよう展 開 して表 示 されます。

メタ キーの生成をトリガーしたメタ値のRAWテキストを検索するには

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。



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/メタ値のペアにカーソルを合わせたままにします。
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。



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。

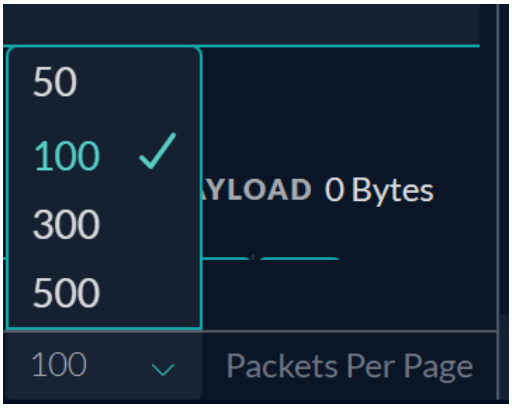
[パケット]および[テキスト]タブでのイベントのページ移動

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。

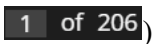
注：ページ区切りコントロールは「テキスト」タブで使用できます。[テキスト]タブでは、最後のページまで手動で移動した後に、最後のページ コントロール アイコンが使用可能になります。

ページ移動アイコンを使用するには

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

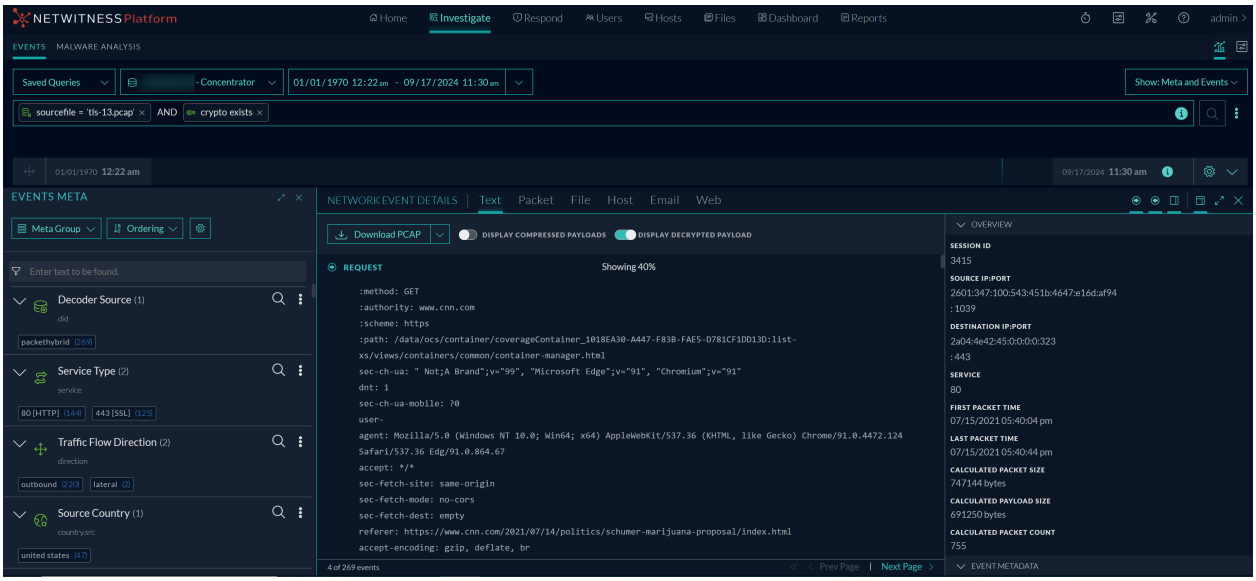


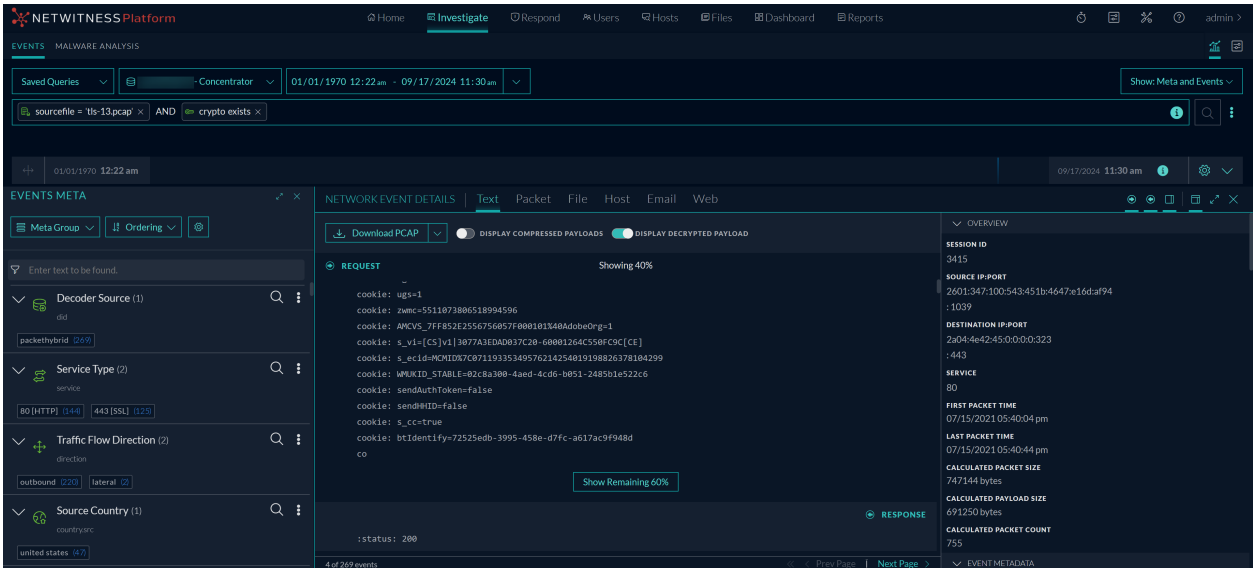
2. ページを前後に移動するには、次のページ コントロール アイコンを使用します。
次のページに移動するには  をクリックします。
最後のページに移動するには  をクリックします。
前のページに移動するには  をクリックします。
最初のページに移動するには  をクリックします。

3. 特定のページに移動するには、ページ番号フィールド() 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、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。





文字数の40% (最初の2000文字) が表示されています。**[残りの60%を表示]** をクリックすると、エントリの残りの部分が表示されます。

[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

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



3. **「選択したテキストをエンコード」**をクリックします。



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



長いテキストを選択すると、ポップアップ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。

4. セッションに含まれるエンコードされたテキストを、デコードされた形式で表示する場合は、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。

5. **「選択したテキストをデコード」をクリックします。**

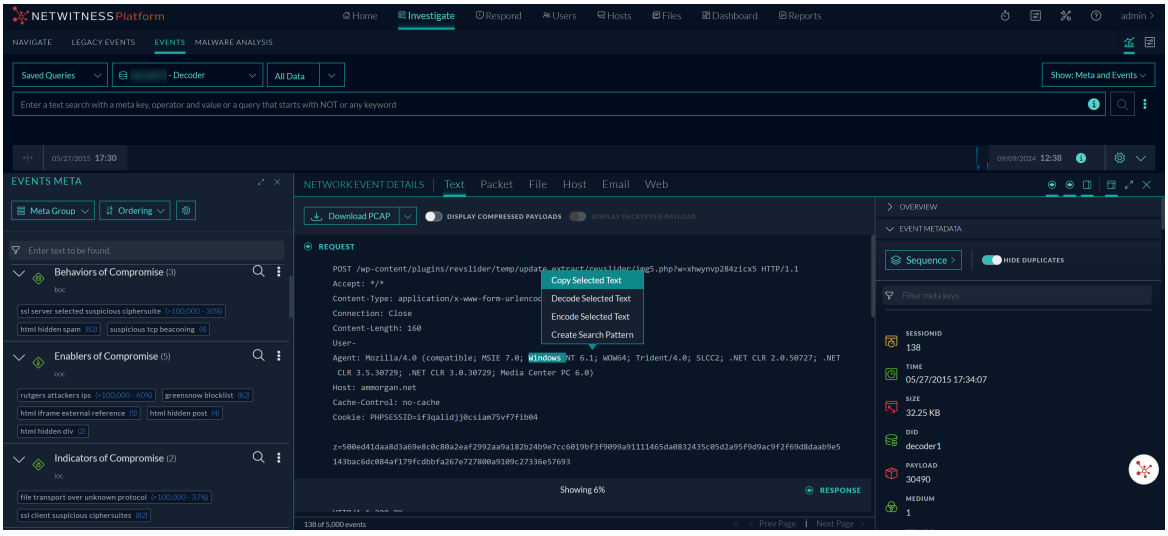


デコードされたテキストがポップアップで表示されます。このポップアップは、[redacted]のクリック、［テキスト］タブ内の別のテキストの選択、［イベント］パネルの終了、再構築する別のイベントの選択、または［イベントの詳細］パネルの別のタブへの切り換えを行うまで表示されたままです。



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



   b. テキストの一部をドラッグし選択し、［**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. 完了したら、 をクリックしてホバー ボックスを閉じます。

[テキスト]タブで検索パターンを作成する

管理者とアナリストは、ネットワーク上の機密データを検索するための検索パターン ルールを作成できます。これらのルールはキーワードを使用してパターンを識別し、正確なキーワード文字列に基づいて照合されます。サービス(Decoder) と一致するポリシーにパターンが適用されると、ネットワークトラフィック内でそのパターンが検索されます。一致が検出されると、2つの重要なメタデータ(**found**と**match**) が生成されます。

- **found** :ストリーム内で一致(キーワード) が識別された場合は、検索パターン ルールの名前がfoundメタデータとして追加されます。
- **match** :キーワードが一致として検出された場合は、識別された特定のキーワードがmatchメタとして追加されます。

アナリストはこのメタデータを使用してさらに調査し、機密データが悪意を持って使用されていないかどうかを判断できます。さらに、アナリストはネットワークトラフィックをリアルタイムで可視化し、潜在的な脅威がないかどうかプロアクティブに監視できます。

以下は、ネットワーク内の機密データを見つけるために使用できる検索パターンの例です。

キーワード :キーワードは、機密データに関連付けられることが多い単語または語句です。たとえば、**クレジット カード**というキーワードを使用すると、クレジット カード番号を含むネットワークトラフィックを検索できます。

重要 :バージョン12.3.1以前の **search.ini** ファイルを使用して作成したカスタム検索パターンは、バージョン12.5以降で使用される新しい **search.xml** ファイル形式に移行されません。その結果、バージョン12.5以降にアップグレードすると、カスタム検索パターンは**コンテンツ ライブラリ**> [**その他**]> **検索パターン ルール**]タブから利用できなくなります。

たとえば、環境内にCCMが有効でポリシーに公開されている4つのDecoderがあるとします。ただし、これらのDecoderのうち検索パーサが有効になっているのは3つだけで、1つのDecoderでは検索パーサが有効になっていません。その結果、検索パーサが有効になっている3つのDecoderのみが、foundメタ キーとmatchメタ キーを生成します。

前提条件

- デフォルトでは、管理者のみが検索パターンを作成できます。アナリストがアクセスできるようにするには、アナリストから管理者に連絡する必要があります。
- メタ キー**found**および**match**を生成するには、**検索パーサ**(foundとmatch) を有効にする必要があります。これはデフォルトでは無効になっています。これを行うには、 (**管理者**) > [**サービス**]に移動して、 [**Decoder**]サービス> > **構成**]> [**全般**]を選択し、 [**パーサ構成**]セクションで**検索パーサ**を有効にします。

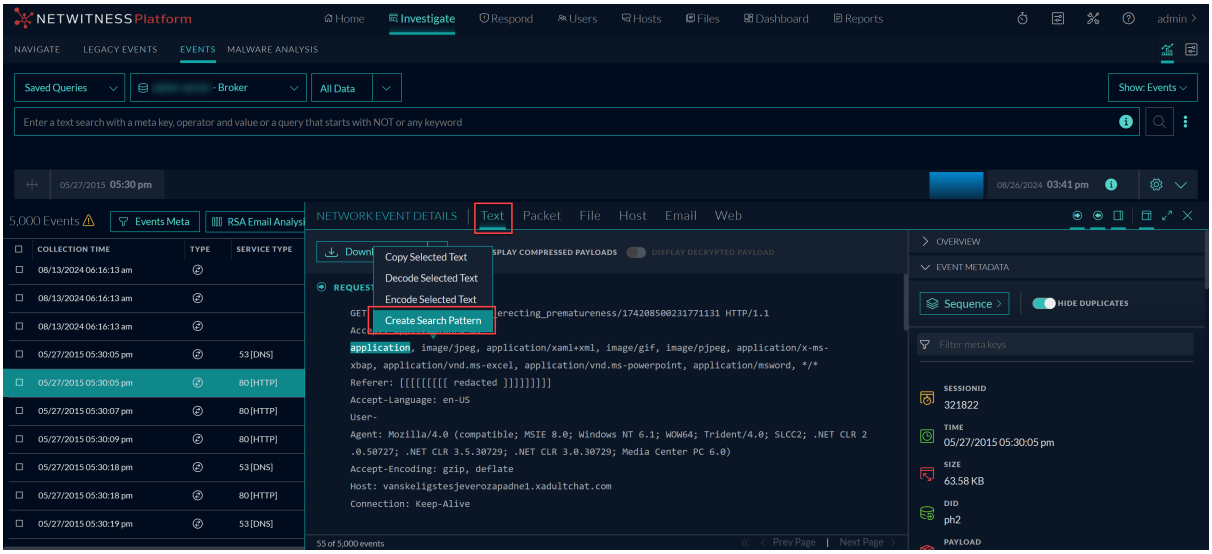
注 :汎用パターン ルールを作成すると、パフォーマンスの問題が発生します。

注 :管理者は、アナリストが検索パターン ルールを作成できるように、ソース サーバー上で **investigate-server.searchpatternrule.manage**権限と**source-server.centralpolicy.manage**権限を有効にし、コア デバイス上で**rules.manage**権限を有効に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ー管理ガイド*』の「ロールの権限」トピックを参照してください。

重要 :ユーザーは、次の2つの条件が満たされている場合にのみ、検索パターン ルールをポリシーに追加して公開できます。
- Decoderサービスがポリシー ベースの集中コンテンツ管理によって管理されている。
- ユーザーの**investigate-server.searchpatternrule.manage**権限が有効になっている。

[テキスト]タブで検索パターンを作成するには

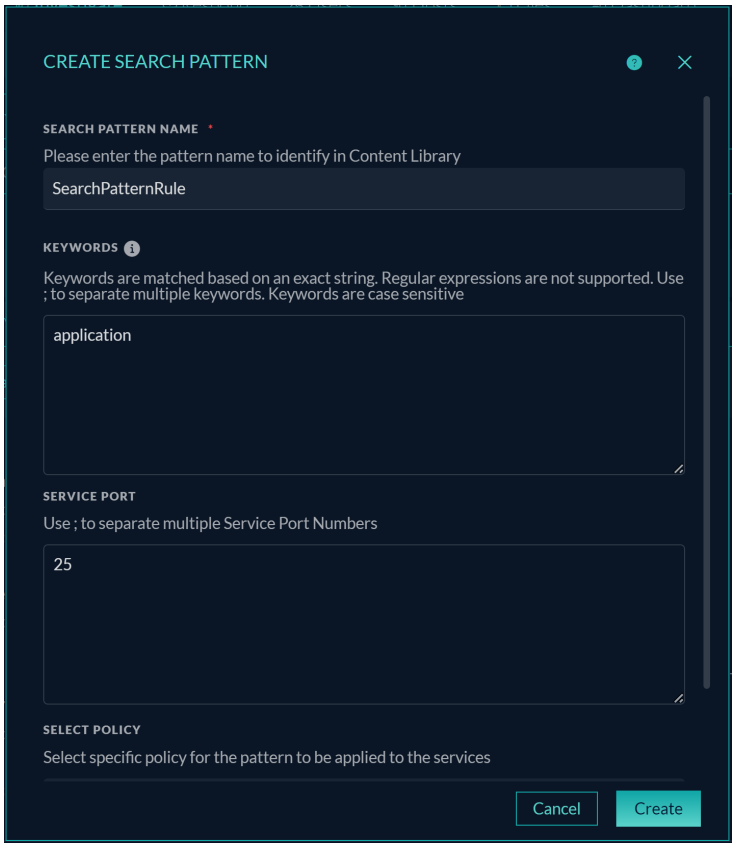
1. NetWitness Platformにログインします。
2. [**調査**] > [**イベント**]に移動します。
3. ネットワーク イベントを含むセッションのテキスト再構築に進みます。



4. テキストまたはrawバイトのサブセットを選択し、ポップアップ メニューから [**検索パターンの作成**]を選択します。

注 :非ASCII文字(é、€、★など)はサポートされていません。検索パターンの作成時に選択または入力できるのは、ASCII文字のみです。

[検索パターンの作成]ダイアログが表示されます。



5. [コンテンツ ライブラリー]ページでパターンを識別するためのパターン名を入力します。256文字以内の一意の名前を指定してください。文字と数字のみを使用してください。

   注：検索パターン名にスペースを含めることはできません。

6. [キーワード]フィールドに1つ以上のキーワードを入力します。キーワードは、正確な文字列のみに基づいて照合されます。正規表現(Regex) はサポートされていません。複数のキーワードを区切るにはセミコロン(;) を使用します。たとえば、「**CreditCard;VISA;US**」のように入力します。

   キーワードでは大文字と小文字が区別されます。1つ以上のキーワードを入力して、正規表現の一致を検出する可能性を高めることができます。

7. [**サービス ポート**]フィールドに 1 つ以上のポート番号を入力します。複数のポート番号を区切るにはセミコロン(;) を使用します。たとえば、「**20;21;23**」のように入力します。

   ポート番号は**1**～**65535**の間でなくてはなりません。

8. 適用するパターンのドロップダウン メニューから特定のポリシーを選択します。

   重要：ポリシーにグループやサービスが関連付けられていない場合、またはCCMによって管理されていないサービスがある場合、ポリシーは使用できません。このような場合は、パターンのみを**作成**してから、[**コンテンツ ライブラリー**] > [**ポリシー**]ページに移動し、ポリシーを作成して適用できるオプションがあります。

注：
- パターンを**作成して公開**するオプションは、ドロップダウン メニューからポリシーを選択した場合にのみ使用できます。
- [X]オプションを使用して、 **ポリシー**]ドロップダウン メニューから選択したポリシーを削除できます。

9. **作成と公開**]をクリックします。

   パターン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。

10. 成功メッセージから、 **コンテンツ ライブラリー**]ハイパーリンクをクリックし、 **詳細**] > **検索パターン ルール**]タブに移動すると、パターンが作成されます。

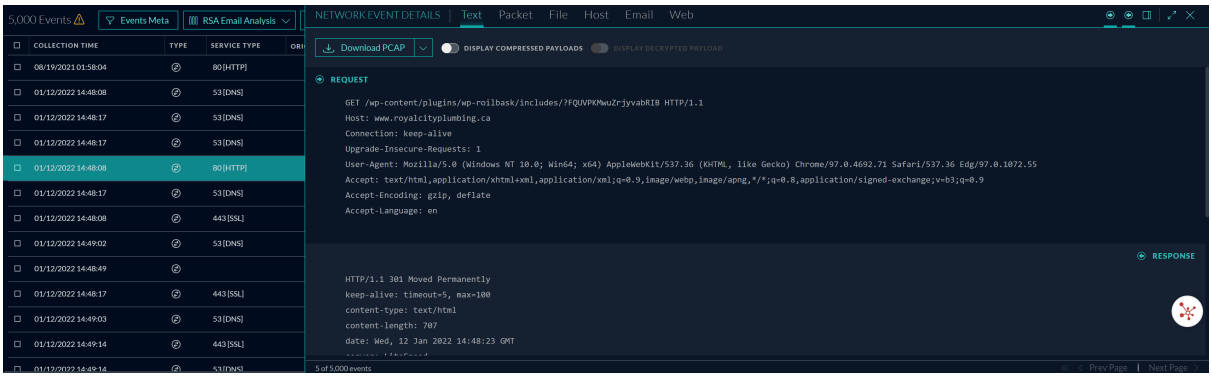
    同じ検索パターンのプロパティを変更する必要がある場合は、管理者にお問い合わせください。

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

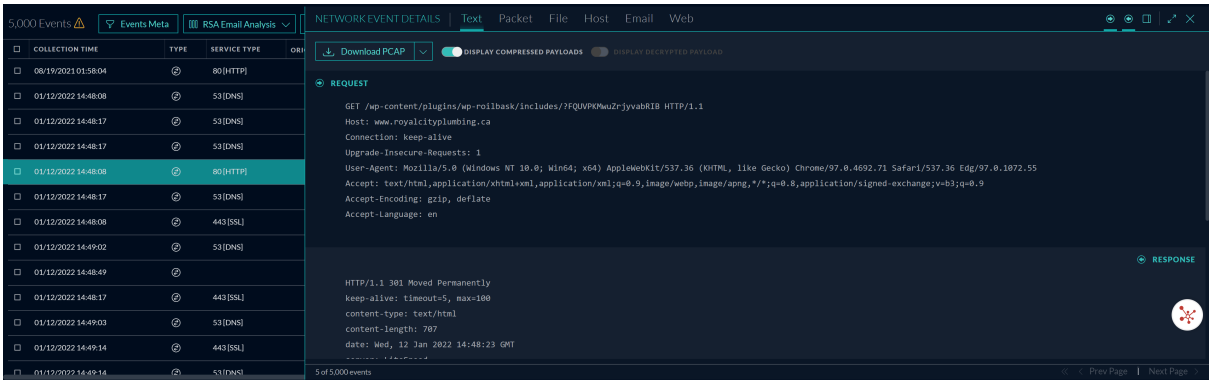
HTTPネットワーク セッションのコンテンツが圧縮されている場合、NetWitnessでは、デフォルトで解凍されたコンテンツが [テキスト]タブに表示されます。これにより、任意のパターンがあるか判断し、読み取り可能な文字を表示することができます。圧縮されたテキストを圧縮表示するか解凍表示するかを切り替えることができます。

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、トグル スイッチをクリックします。
表示が変わり、圧縮されたテキストは判読できなくなり、スイッチは「圧縮されたペイロードの表示」がオンになっていることを示します。

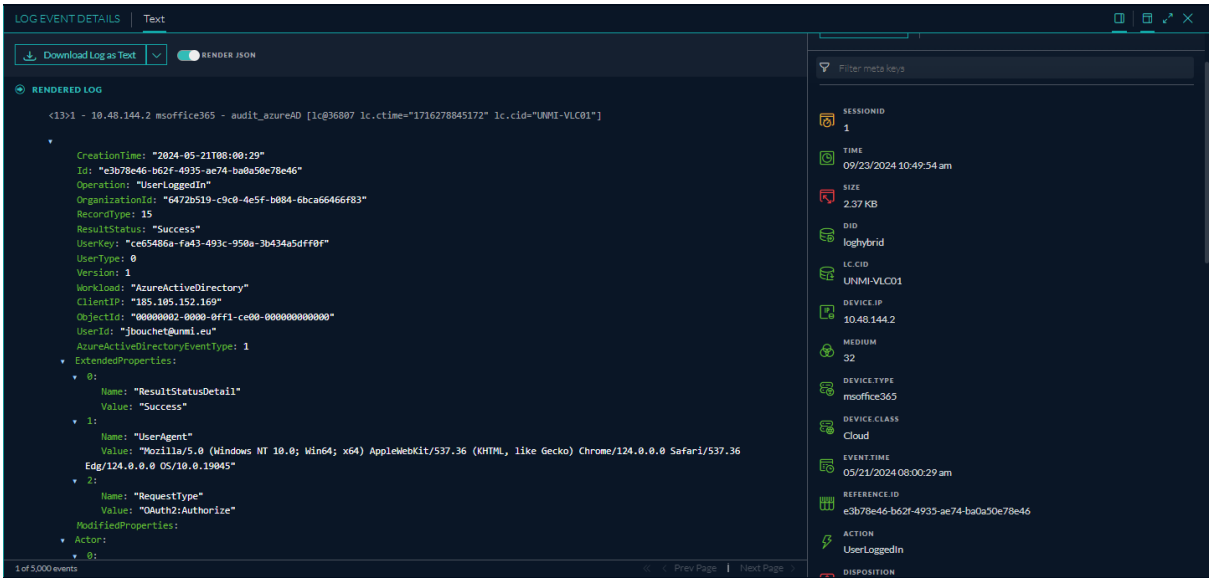


3. 解凍されたテキストの表示に戻すには、スイッチを再度クリックします。

ツリー形式のJSON文字列の［テキスト］タブでの表示

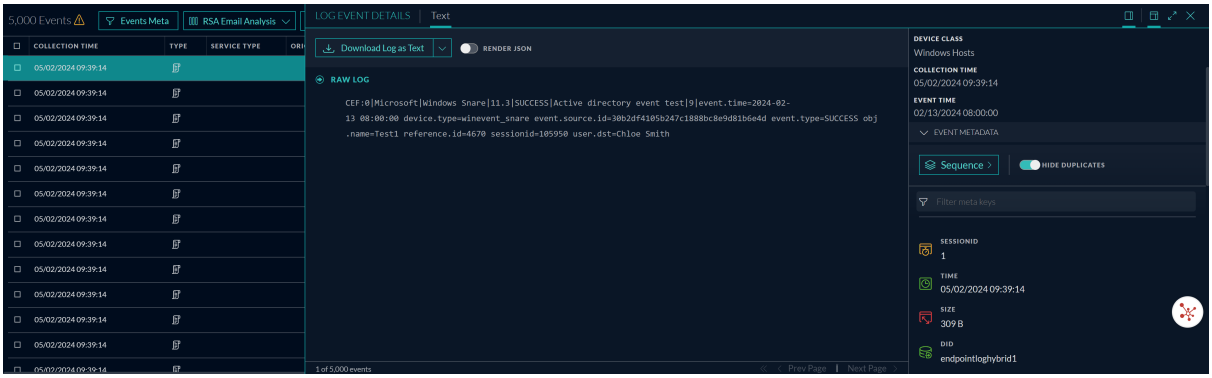
［JSONの表示］切り替えスイッチを使用すると、未フォーマットのブロック形式ではなく、読みやすいJSON形式で、ログ イベントのテキスト再構成を表示できます。デフォルトでは、スイッチが有効になっており、ログ イベントのJSONスニペットが検出され、完全に展開されたツリー形式で表示されます。無効なJSONスニペットはRAWテキストとして表示されます。スイッチの設定を変更した場合でも、設定はローカル ストレージに保持されています。

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、次回のログイン時も、同じ状態です。

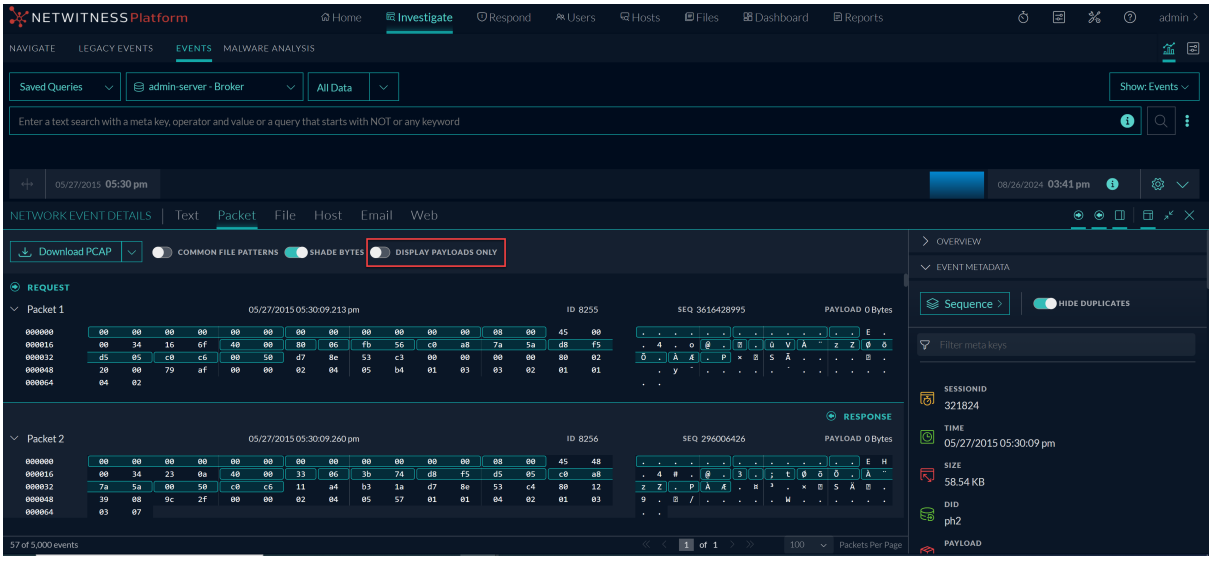


[ペイロードのみ]オプションの [パケット]タブでの使用

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。

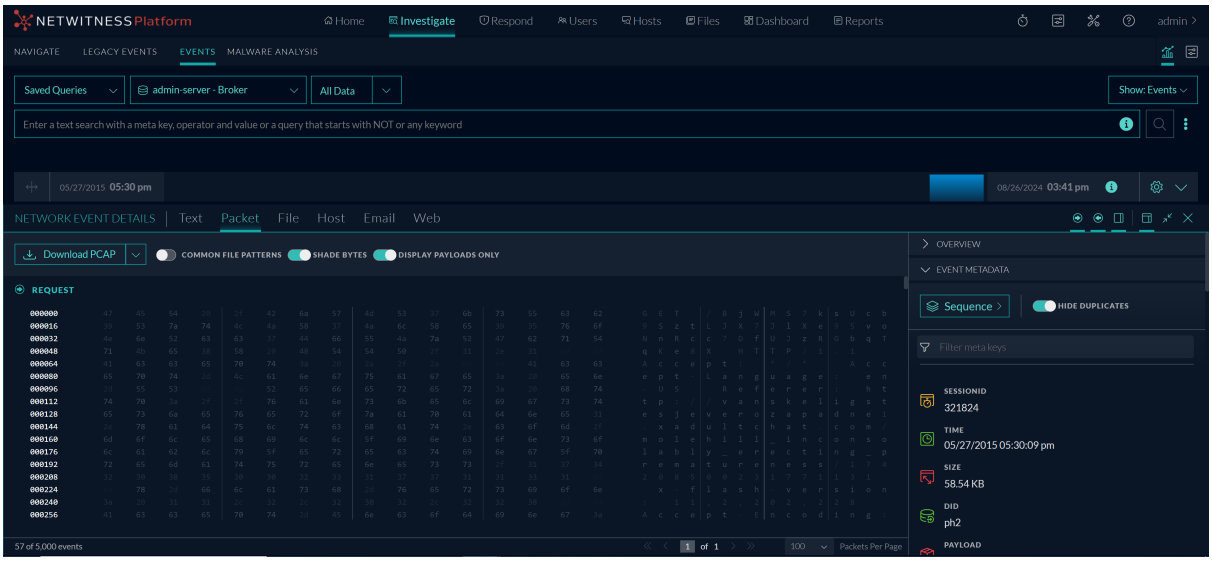
- [ペイロードのみ表示]オプションをオフにすると、パケット番号、パケットのヘッダー、パケットのフッター、ペイロードが表示されます。
- [ペイロードのみ表示]オプションをオンにすると、パケットのヘッダーとフッターのバイトは表示されません。パケット コンテンツのみが、1行あたり16バイトの16進数とそれに対応するASCII文字で表示されます。

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。



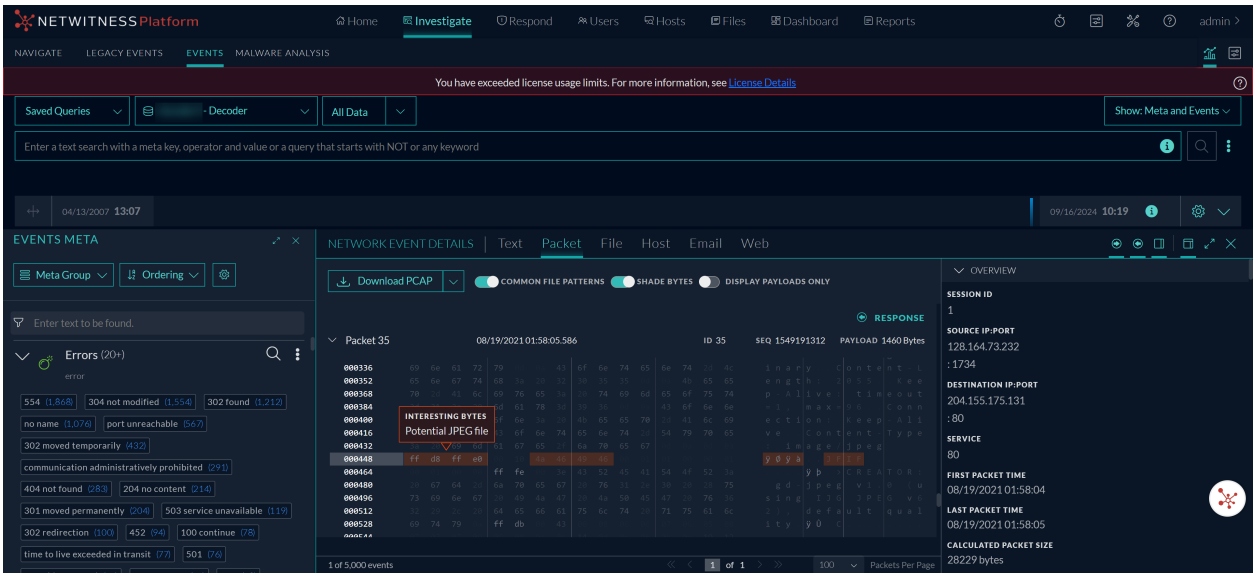
2. 各パケットのペイロードのみが表示されるようにビューを変更するには、 [**ペイロードのみ表示**]切り替えスイッチをクリックします。

ビューが変更されてペイロードのみが表示されます。

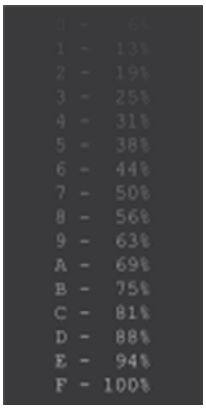


[パケット]タブでのバイトのハイライト表示

[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。



[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。



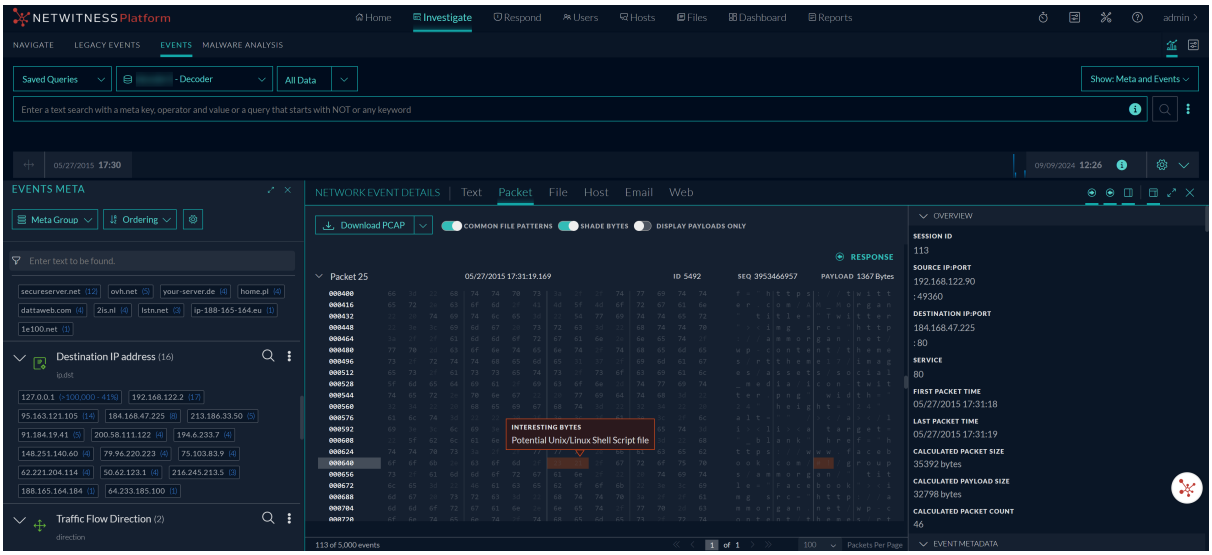
［バイトの濃淡化］スイッチは、バイトの濃淡化を制御します。［バイトの濃淡化］をオンまたはオフに設定すると、設定を変更するか、ブラウザを更新するまでその設定が保持されます。

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］機能がオンの場合は、ペイロード内にあるファイル シグネチャのマジック ナンバーのバイトがハイライト表示され、ハイライト表示にカーソルを合わせると潜在的なファイル タイプが表示されます。この例では、23 21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。

1. ［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。
2. ポップアップを表示するには、ハイライト表示された場所にカーソルを置きます。



次の表は、ペイロードに存在する場合にハイライト表示されるファイル タイプと対応するマジック ナンバーです。

ファイル タイプ	16進数のシグネチャ	ASCIIエンコード
DOS実行可能プログラム/Windows PE	4D 5A	MZ
PNG(ポータブル ネットワーク グラフィックス)	89 50 4E 47 0 D 0A 1A 0A	PNG
JPEG	FF D8 FF	JPEG
JPEG/JFIF	4A 46 49 46	JFIF
JPEG/Exif	45 78 69 66	Exif
GIF	47 49 46 38 37 61	GIF87a
GIF	47 49 46 38 39 61	GIF89a
移植性がない実行可能プログラム	5A 4D	ZM
BMP	42 4D	BM
PDF	25 50 44 46	%PDF
古いOfficeドキュメント(doc、xls、ppt、msg、その他)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
ZIPファイル形式、およびJAR、ODF、OOXMLなどのZIPに基づく形式	50 4B	PK..
7 ZIPファイル形式(7z)	37 7A BC AF 27 1C	7z¼¯'
Javaクラス ファイル、Mach-O Fatバイナリ	CA FE BA BE	Êþº¾
PostScript	25 21 50 53	%!PS
Unix/Linuxのシェル スクリプト	23 21	#!
ELF(実行可能プログラムおよびリンク可能な形式) の実行可能プログラム	7F 45 4C 46	.ELF

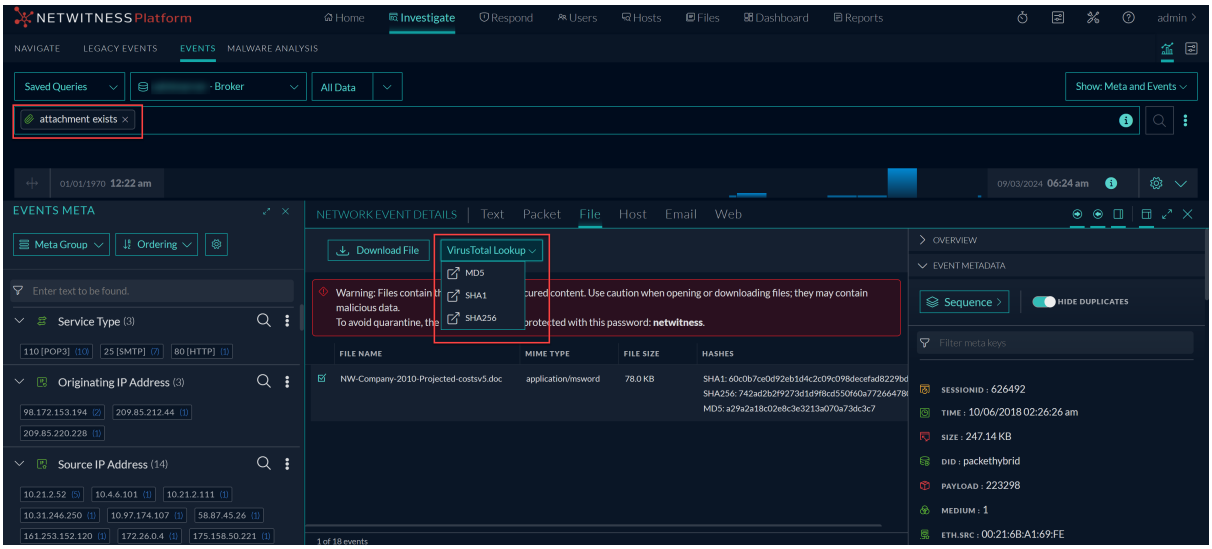
ファイルのVirusTotalルックアップの開始

［イベント］ビューで、ファイルの分析中にハッシュ(MD5、SHA1、SHA56) でVirusTotalを検索して、ファイルに関する詳細情報を取得することができます。これは、複数のウイルス対策ベンダーで、ファイルに悪意があるかどうかを判断するのに役立ちます。

検索を開始するには

1. NetWitness Platformにログインします。
2. **調査**］> ［**イベント**］に移動します。

3. ［**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。
4. ファイルを選択し、［**VirusTotalルックアップ**］をクリックして、**MD5**、**SHA1**、または**SHA256**で検索を実行します。



注 : VirusTotalルックアップで選択できるのは、一度に1つのファイルのみです。

[レガシー イベント]ビューでのイベントの再構築

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

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

再構築では、次のことができます。

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

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

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

重要:レガシーのWeb再構築においては、HTTP2セッションではWeb再構築のみがサポートされ、テキストの再構築はサポートされません。ただしHTTP2セッションのテキスト再構築については、[**イベント**]ページで確認できます。

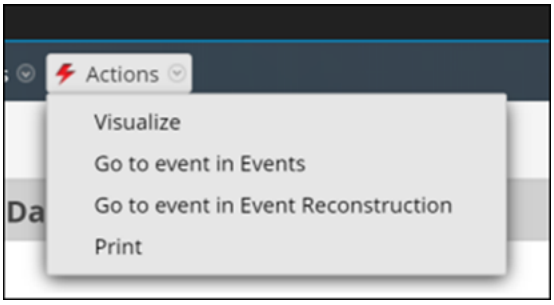
注:Investigationのアプリケーション パフォーマンスは、管理者が、[再構築の設定]と[再構築キャッシュの設定]で管理できます(『システム構成ガイド』で説明しています)。アナリストがセッションを再構築する場合、パフォーマンスと表示結果に影響を与える要素が2つあります。
サイズが大きいイベントでは、ソース パケットが膨大な数に上ることがあります。それらのセッションを再構築すると、アプリケーションのパフォーマンスが低下する可能性があります。
再構築キャッシュの表示内容が不正確である場合があります。このような理由から、1日以上経過したキャッシュは、24時間おきにNetWitnessによって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

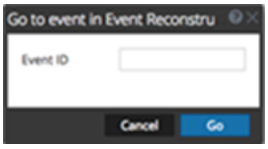
イベントIDがわかっている場合に、イベントを［ナビゲート］ビューから直接再構築できます。このオプションを使用すると、調査の開始時に通常必要となる、クエリの実行は必要ありません。eventidだけを使用してイベントに直接移動できるようにするには、サービスと時間範囲を選択する必要があります。

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。

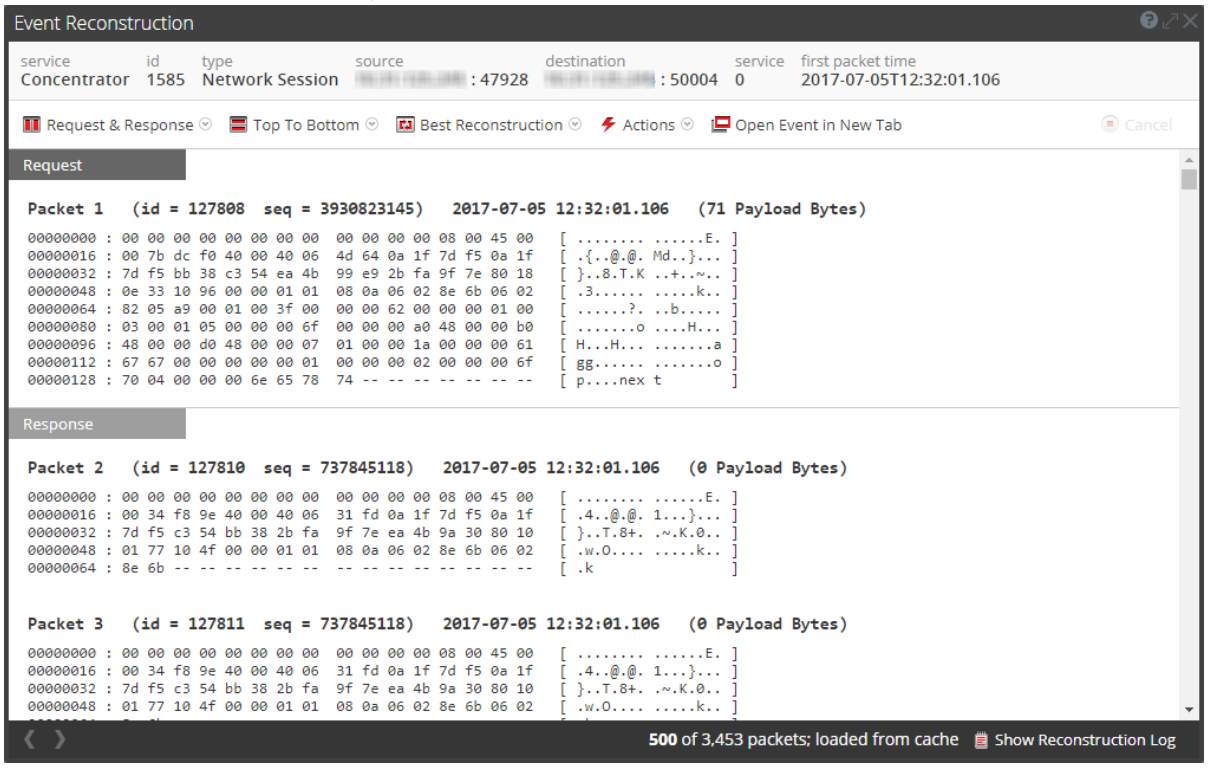


2. **［イベントID］**フィールドにIDを入力して、**［移動］**をクリックします。
指定されたイベントがレガシーの［イベント再構築］ビューまたは［イベント］ビューで再構築されます。

［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

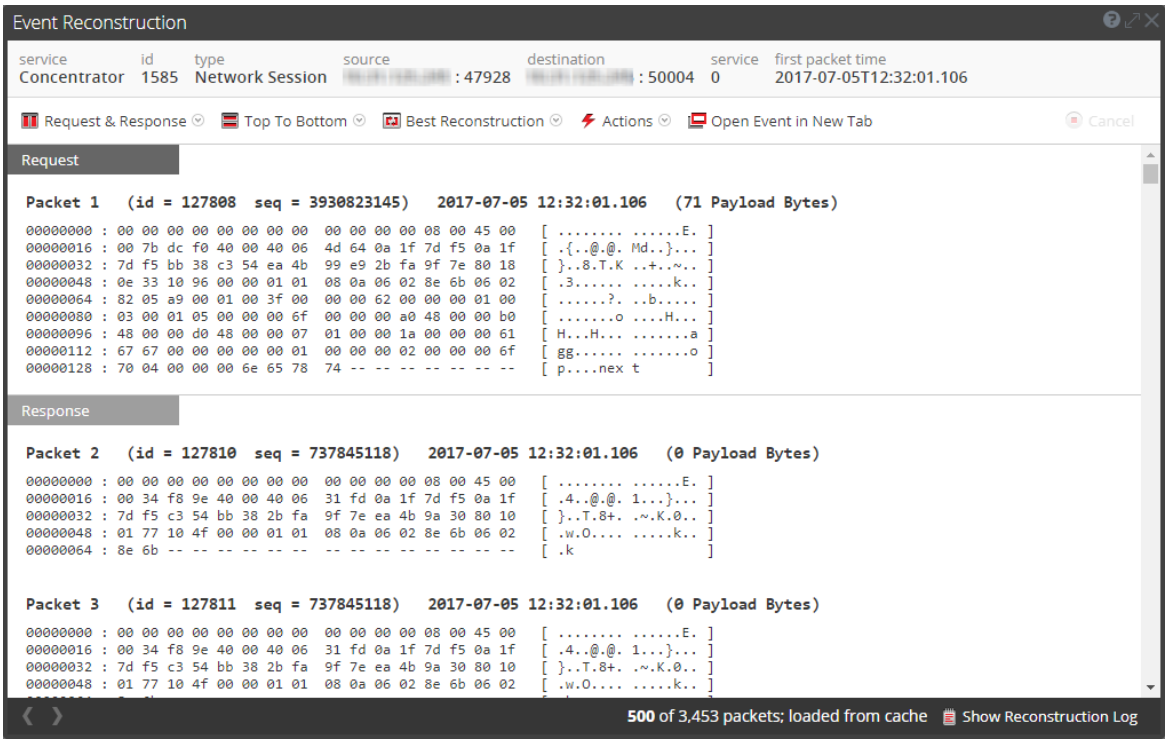
1. ［ナビゲート］ビューの値の数(値に続く緑色の数字)をクリックすると、**［イベント］**ビューでドリルダウン ポイントが開きます。
2. すべてのメタ データを表示するには、 Show Additional Meta をクリックします。
3. ［レガシー イベント］ビューでイベント再構築を表示するには、再構築するイベントを選択し、**［アクション］**>**［イベントの表示］**>**［インライン プレビュー］**を選択します。
同じビューのポップアップ ウィンドウに［イベントの再構築］が表示されます。デフォルトでは、イベントのコンテンツから判断されたイベントに最適な再構築形式か、NetWitness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

ベント、エンドポイント イベント）。これは、ネットワーク イベントの再構築の例です。



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

[イベントの再構築]オプションが新しいタブに開かれます。



セッションを左右/上下に並べて表示

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

1. [**イベントの再構築**]ツールバーで、[**セッションを上下に並べて表示**]または[**セッションを左右に並べて表示**]をクリックします。
2. ドロップダウンメニューから、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。

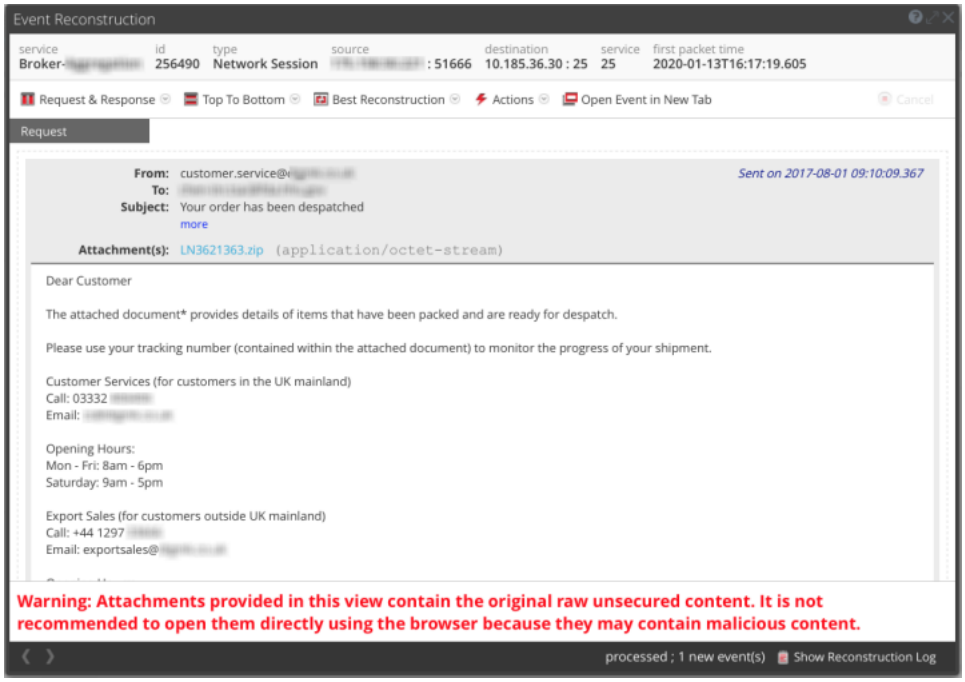
メールの添付ファイルの表示またはダウンロード

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

イベントをPCAPファイルとしてエクスポート

PCAPエクスポート オプションにより、現在の時間範囲のセッションおよびドリルダウン 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。PCAPは、 [プロファイル] > [ジョブ]タブでダウンロードできます。

再構築されたイベントからのファイルの抽出

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

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

結果の追加のコンテキストを検索

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

コンテキスト情報の表示を有効にするには、管理者がContext Hubサービスを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**」で説明されているように、`Context Lookup`権限がアナリストに付与されている必要があります。

Context Hubサービスが有効化され、構成されている場合は、NetWitnessによって、NetWitness Respond、カスタム リスト、NetWitness Endpointから直接、［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］ビューにエンリッチメント データが提供されます。［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。NetWitness Endpointなどの構成されたソースからのデータは、何が起こっているのかを理解するために役立ちます。STIXデータ ソースを追加し、コンテキスト ルックアップを使用して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。

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」の説明に従って適切なロールと権限を設定します。

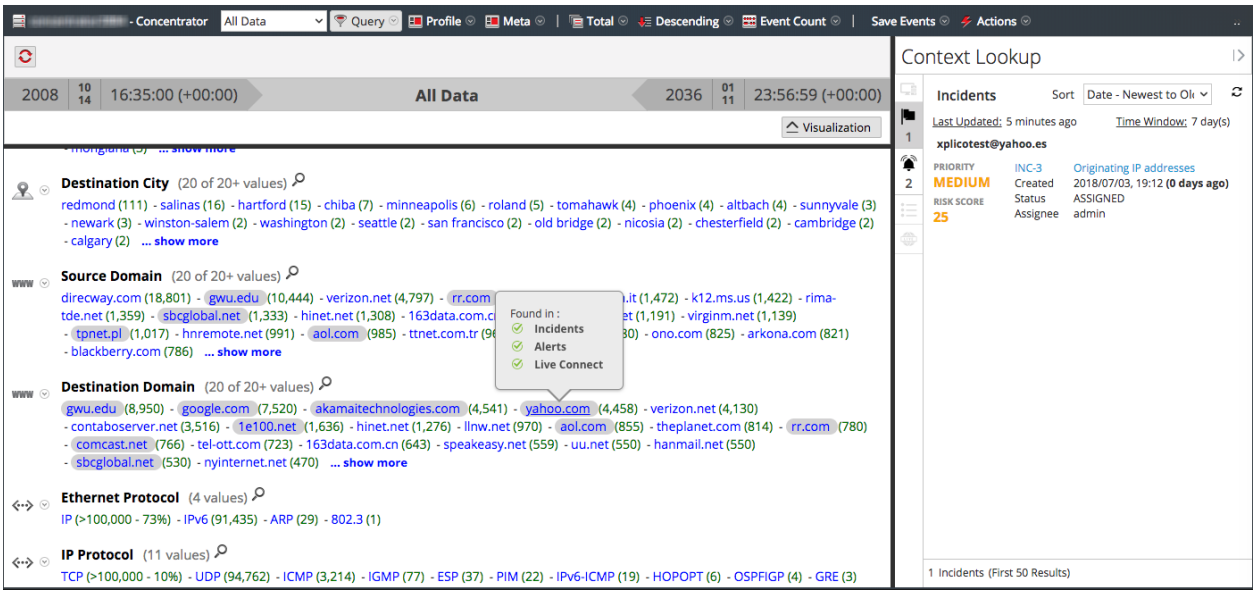
REST APIデータ ソースを追加し、コンテキスト ルックアップを使用して関連データを表示できます。また、管理者は、調査中にコンテキストを強調表示するために、特定のContext Hubソース(たとえば、特定のリスト、応答、エンドポイントなど) を構成できるようになりました。Context Hubソースのコンテキスト強調表示が無効になっている場合、アナリストはメタ値のコンテキスト パネルを開いたときにすべてのデータ ソースからの結果を表示しますが、値は［調査］ビューで強調表示されません。ビュー コンテキストで次の処理が行われます。

- 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。



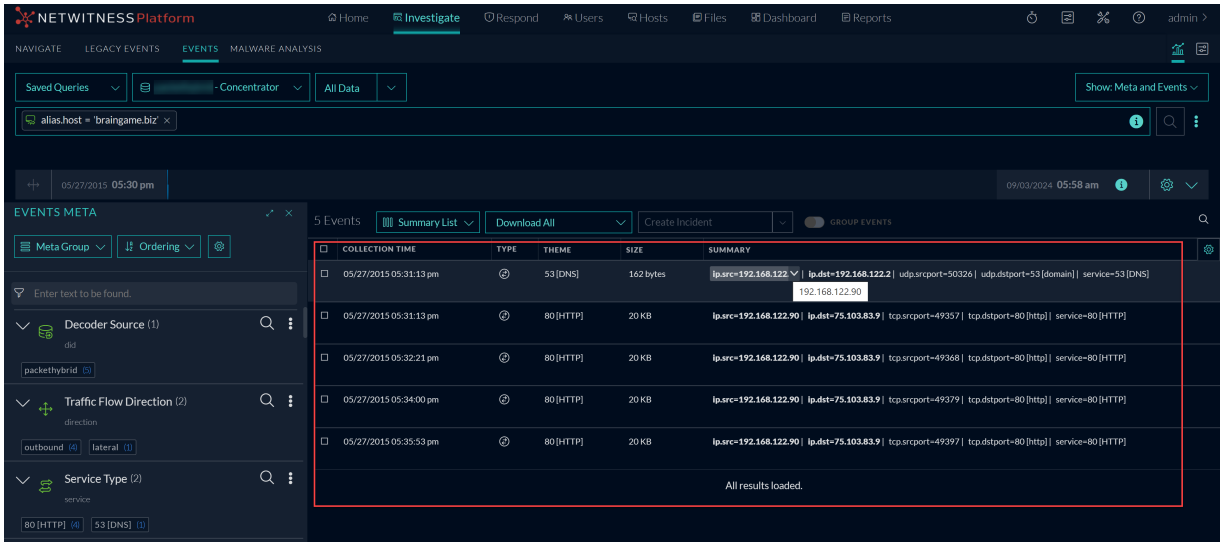
注 :contexthub-server.contextlookup.read権限は、管理者、アナリスト、マルウェア アナリスト、SOC マネージャー、およびRespond管理者に対してのみ有効です。管理者は、 [**ユーザ**] ビューの他のロールに対してこの権限を有効にすることで、メタ値のコンテキスト検索を表示し、リストへの追加/削除アクションを実行できます。詳細については、『*システム セキュリティとユーザ管理ガイド*』の「ロールの権限」トピックを参照してください。

[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。

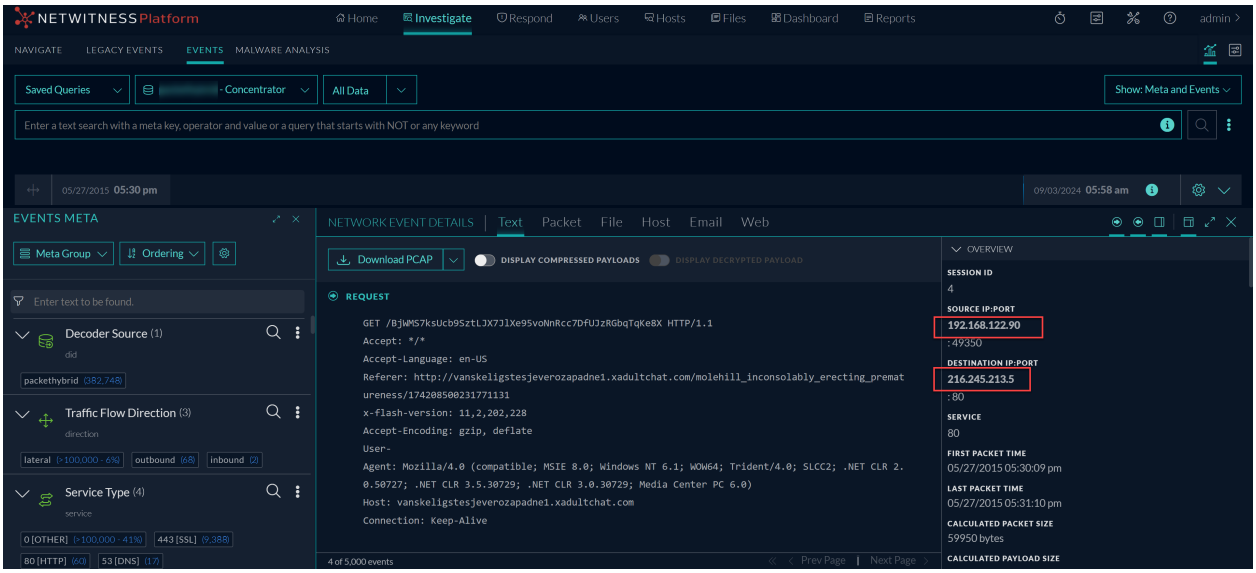
次の図は、コンテキスト ツールチップを開いた [イベント] パネルの下線付きエンティティを示しています。コンテキスト ツールチップには、2つのセクションがあります。 [コンテキストのハイライト] と [アクション] です。

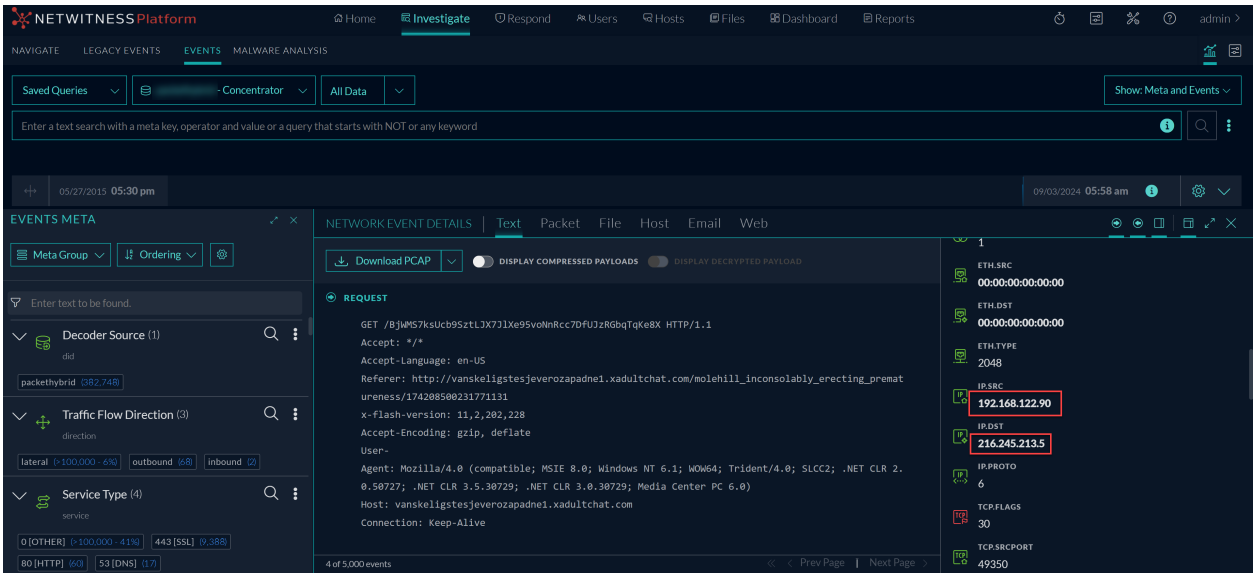
- [コンテキストのハイライト] セクションの情報は、必要なアクションを判断するのに役立ちます。インシデント、アラート、リスト、重要度、資産リスク、STIXの関連データを表示できます。データによっては、これらの項目をクリックして詳細を確認できます。

- このセクションには、利用可能なアクションもリストされます。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］、［ホスト/ファイルへの移行］の各オプションを使用できます。



次の図は、［概要］パネルと［イベント メタ］パネルで太字で表示されるエンティティを示しています。





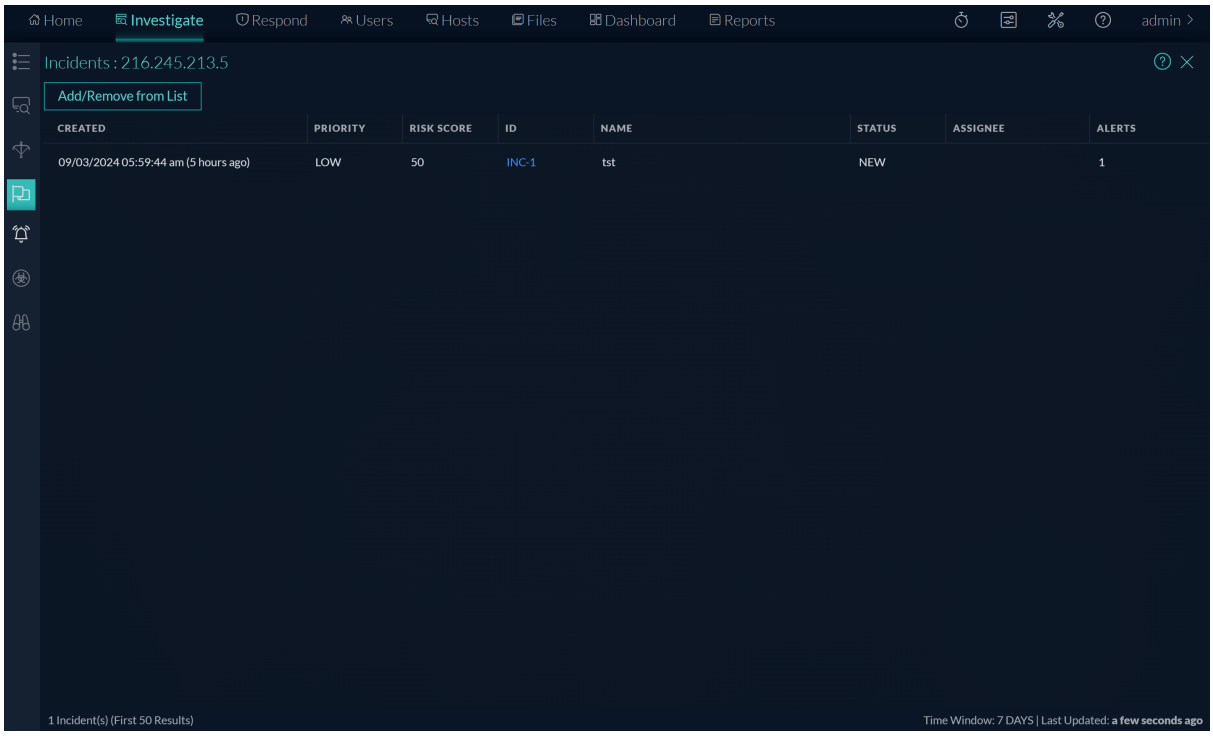
コンテキスト ツールチップの [**コンテキスト ルックアップ**] をクリックすると、Context Hubは構成されたデータソースに関連情報を照会し、 [コンテキスト検索] パネルがブラウザ ウィンドウの右側から開きます。 [コンテキスト検索] パネルには、利用可能になったContext Hubの情報が入力されます。別の検索を実行するには、別のエンティティで [コンテキストの表示] オプションを使用すると、そのエンティティの情報で [コンテキスト ルックアップ] パネルが更新されます。

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

1. [イベント] ビューで、下線付きのエンティティを左クリックまたは右クリックします。
   コンテキスト ツールチップには、選択したメタ値で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 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. 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、Archerへの移行。詳細については、「Archerへの移行([イベント]ビュー)」と「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。

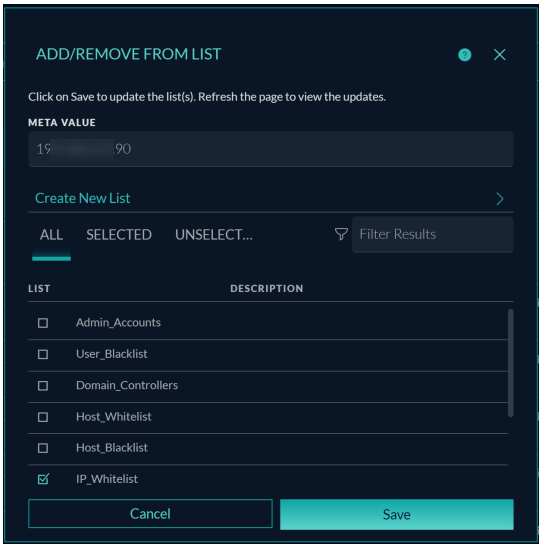
注 : Archerデータが使用できない場合、またはArcherデータ ソースが応答しない場合、 [Archerへの移行]リンクは無効になります。Archer構成が有効で、正しく設定されていることを確認します。

ホワイト リストへのエンティティの追加

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

1. イベント パネル、イベント ヘッダー、またはイベント メタ パネルで、Context Hubリストに追加する下線付きのエンティティを左クリックまたは右クリックします。
   使用可能なアクションを示すコンテキスト ツールヒントが表示されます。

2. **「リストから追加/削除」**をクリックします。
「リストから追加/削除」ダイアログに使用可能なリストが表示されます。



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

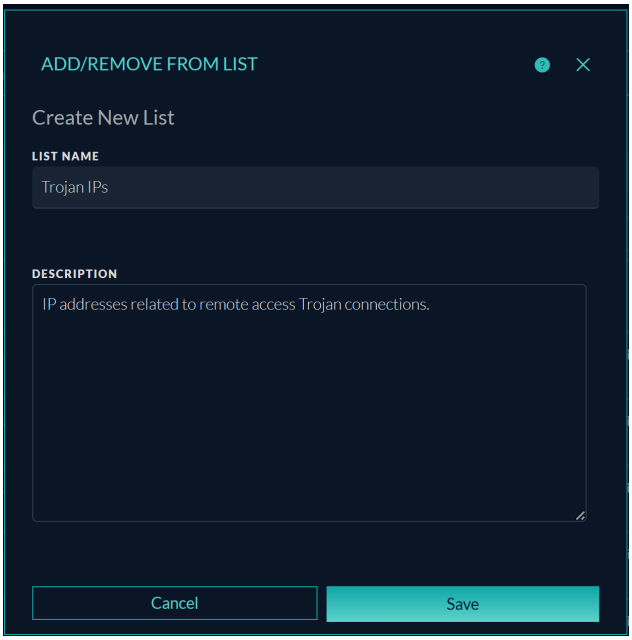
リストの作成(［イベント］ビュー)

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

Context Hubでリストを作成するには

1. イベント パネル、イベント ヘッダー、またはイベント メタ パネルで、Context Hubリストに追加する下線付きのエンティティを左クリックまたは右クリックします。
使用可能なアクションを示すコンテキスト ツールヒントが表示されます。
2. ［**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。

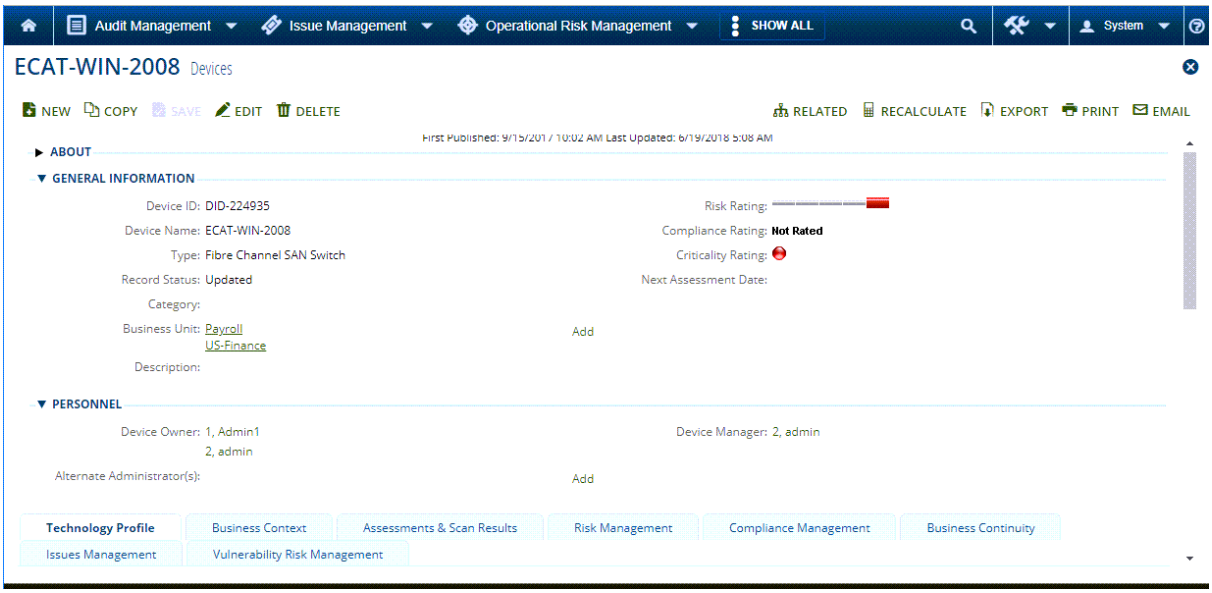


4. 固有の [**リスト名**]を入力します。リスト名は大文字と小文字を区別しません。
5. (オプション) リストの **説明**]を入力します。
   適切な権限を持つアナリストは、他のアナリストに送信してさらに追跡と分析を行うために、CSV形式でリストをエクスポートすることもできます。詳細については、『Context Hub構成ガイド』を参照してください。

Archerへの移行([イベント]ビュー)

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、「**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。

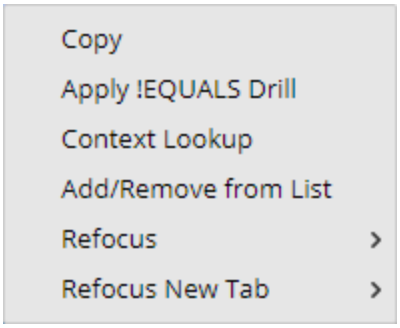


注 : Archerデータが使 用 できない場 合 、またはArcherデータソースが応 答しない場 合 、 [Archerへの移 行]リンクは無 効 になります。Archer構 成 が有 効 で、正 しく設 定 されていることを確 認 します。

詳 細 については、『Archerとの統 合 ガイド』を参 照 してください。

[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。

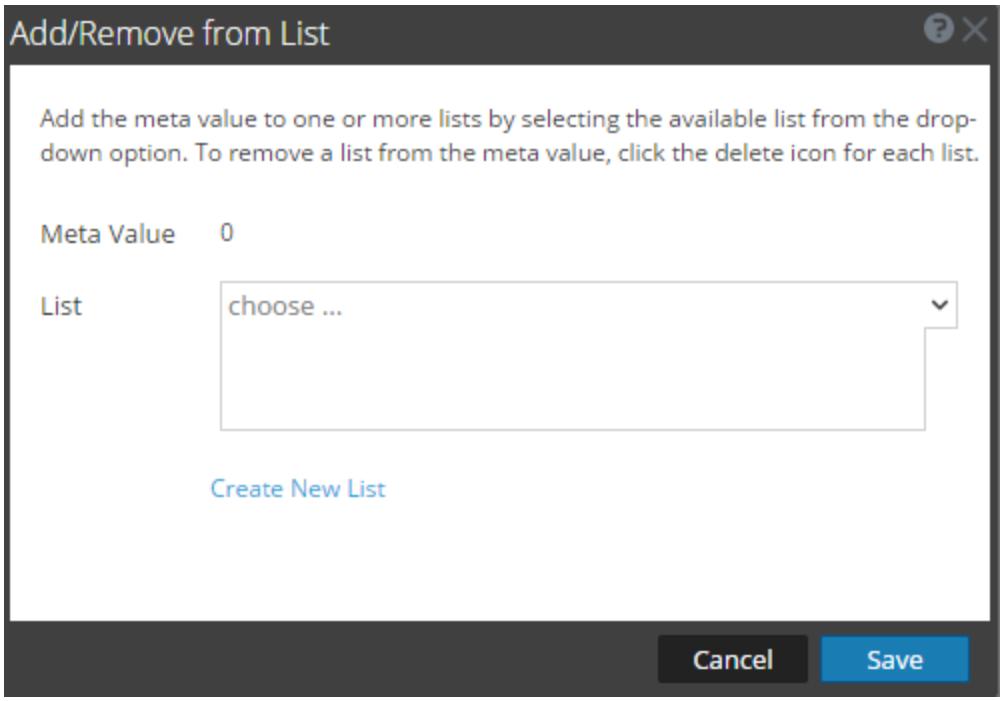
3. [コンテキスト検索]パネルからアクションを実行するには、IPアドレスなどのエンティティをクリックします。
使用可能なオプションは、[リンクを新しいタブで開く]、[Investigateでクエリ]、[リンクのコピー]、[ペースト]、[Googleルックアップ]、[ウイルス合計ルックアップ]、[Endpointでクエリ]です。

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✕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で既存のリストにメタ値を追加するには

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([ナビゲート]ビューと [レガシー イベント]ビュー)

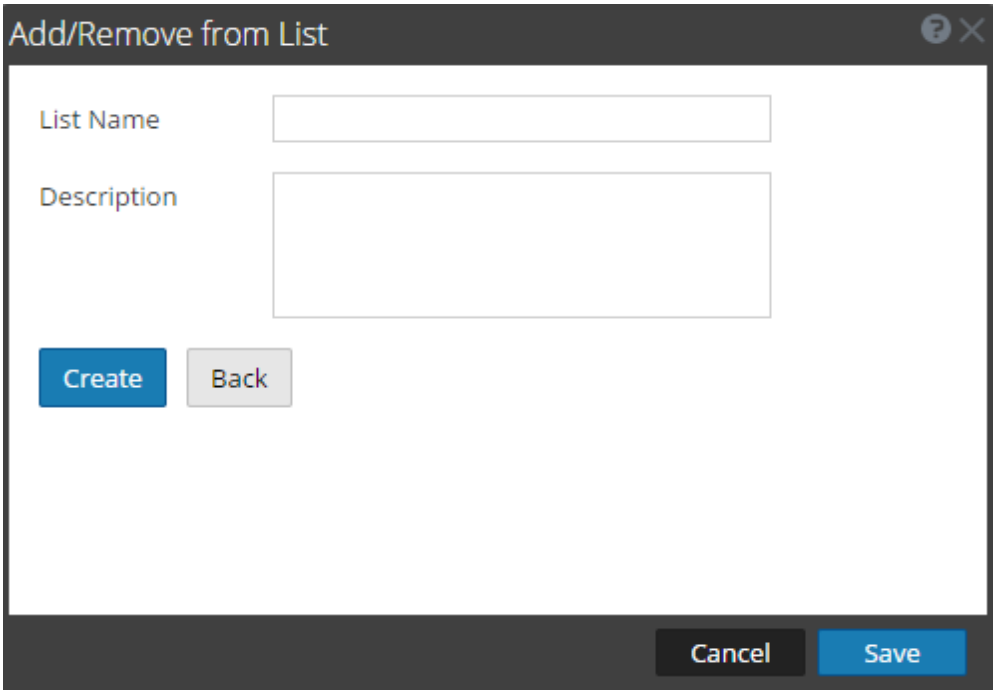
リストからメタ値を削除するには

1. [リストへの追加/削除]ダイアログの [リスト]フィールドで、メタ値を含むリストを表示します。
2. メタ値を削除したいリストの削除アイコン(x) をクリックします。
3. [保存]をクリックします。
   削除したリストから、メタ値が削除されます。

新しいリストの作成([ナビゲート]ビューと [レガシー イベント]ビュー)

[調査]でContext Hubリストを作成するには

1. [リストへの追加/削除]ダイアログで [新しいリストの作成]をクリックします。



2. [リスト名]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 :UrlVoid検索を新しいタブで開きます。

`file-hash`および`alias-host`の各メタ キーで外部ルックアップからGoogleを選択すると、Google検索が新しいタブで開きます。

`client`メタ キーでは、ブラウザと同じマシンにEndpoint Thick Clientがインストールされている場合、NetWitness Endpointルックアップ オプションによってEndpoint Thick Clientが新しいタブで開きます。

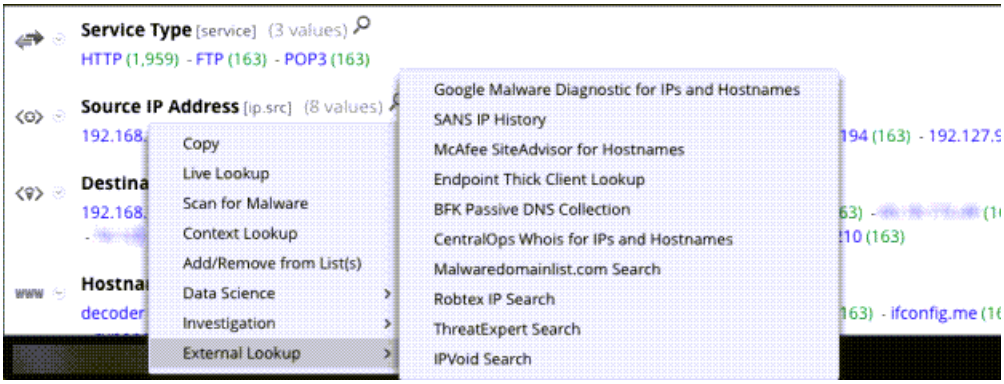
管理者は、外部ルックアップやその他のカスタム アクションを追加できます(『システム構成ガイド』の「コンテキスト メニューのカスタム アクションの追加」を参照してください)。

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

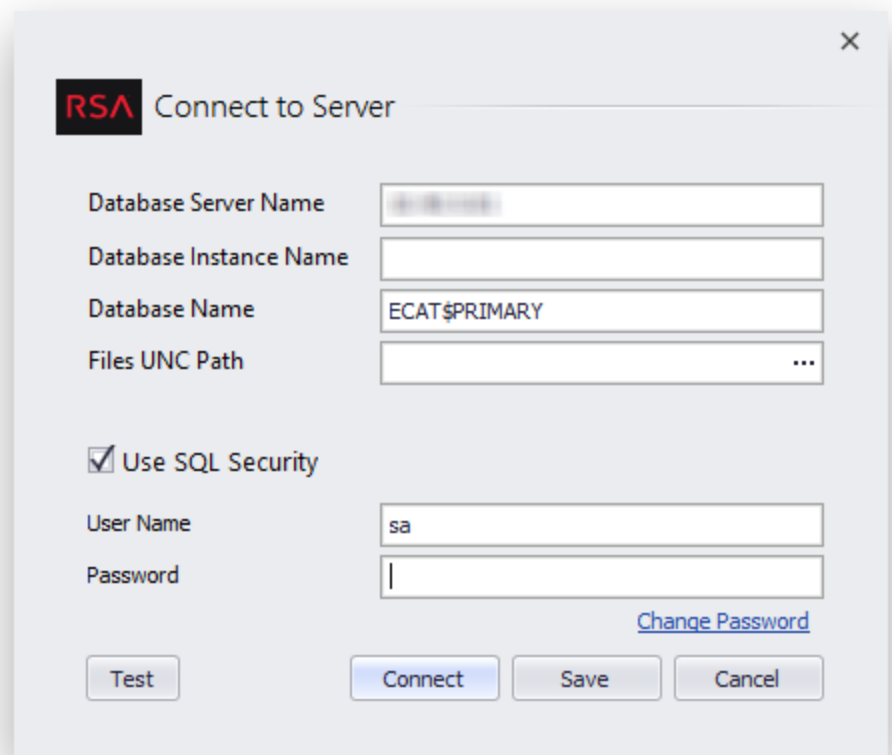
［ナビゲート］ビューからデータのEndpoint Thick Clientルックアップ機能を起動する方法：

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。

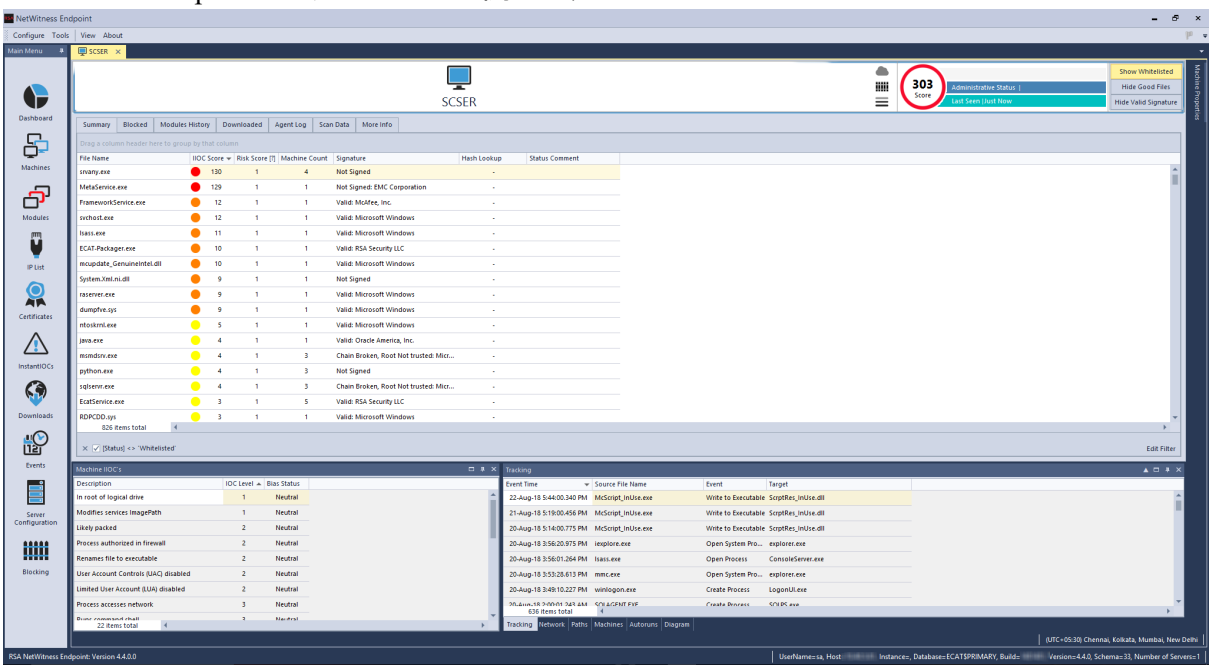


3. [**Endpoint Thick Clientルックアップ**]を選択します。
[サーバーに接続]ダイアログが表示されます。



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。

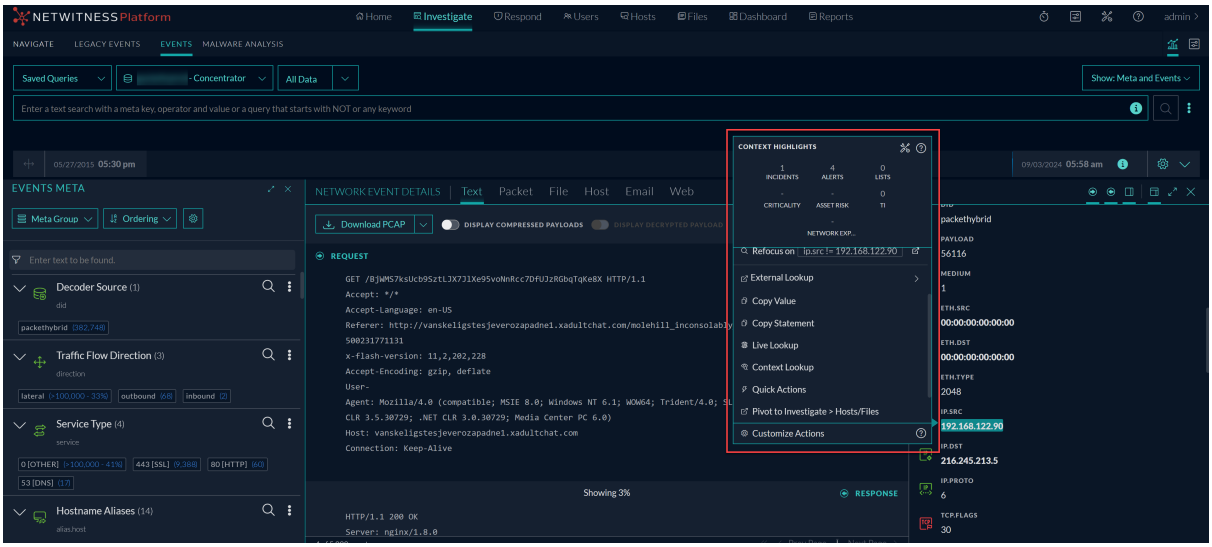
NetWitness Endpointでドリル ポイントが開きます。



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、特定のメタ値を左クリックまたは右クリックし、ドロップダウン メニューのオプションを使用することで、イベント内のメタ値をさらに調査できます。内部ルックアップ、外部ルックアップ、VirusTotalルックアップを実行するには、次の手順を実行します。

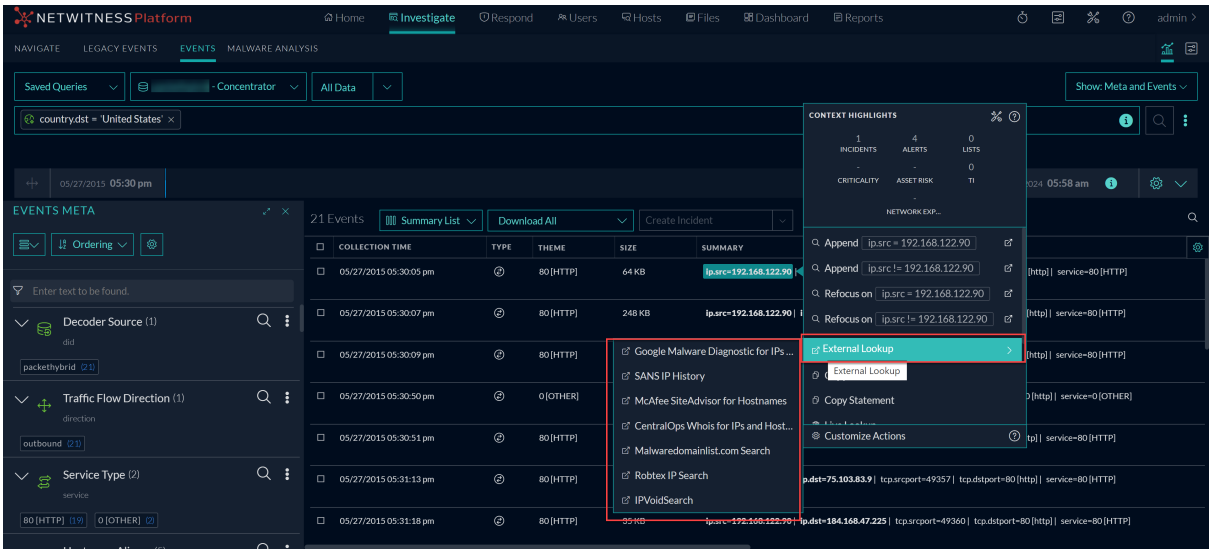
1. イベント ビューで、イベント リスト、イベント メタデータ パネル、または概要パネルのメタ値を左クリックまたは右クリックします。一部のメタ値にドロップダウン メニューがあります。



2. 次の内部ルックアップのいずれかを選択します。

- **値のコピー**：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、選択したメタ値を左クリックまたは右クリックし、［**外部ルックアップ**］をクリックします。



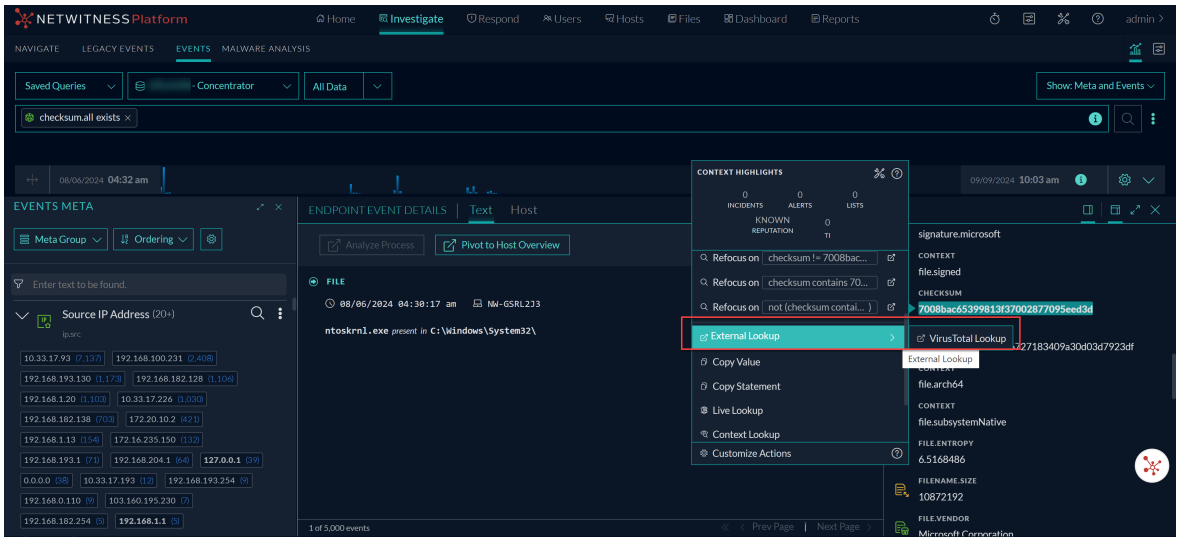
4. サブメニューで、使用可能な外部ルックアップのいずれかを選択します。
   - **Google**：Google.comでメタ値を検索します。
   - **SANS IP History**：SANS IP Historyでメタ値を検索します(domain = http://isc.sans.org/ipinfo.html?ip=ipaddress) 。
   - **CentralOps Whois for IPs and Hostnames**：CentralOps Whois(IPおよびホスト名検索) でメタ値を検索します(domain = http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true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

- **ThreatExpert 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。

5. VirusTotalルックアップの場合
   - [イベント]ビューで、[イベント]リスト、[メタ イベント]パネル、または [イベント メタ]パネル内のチェックサムを持つメタ値を左クリックまたは右クリックします。

     [コンテキストのハイライト]ダイアログが表示されます。
   - [**外部ルックアップ**] > [**VirusTotalルックアップ**]をクリックします。

     これにより、VirusTotalでハッシュ値が検索され、迅速な検索と分析が可能になります。



イベント再構築ビューでのMITRE ATT&CK©ルックアップ

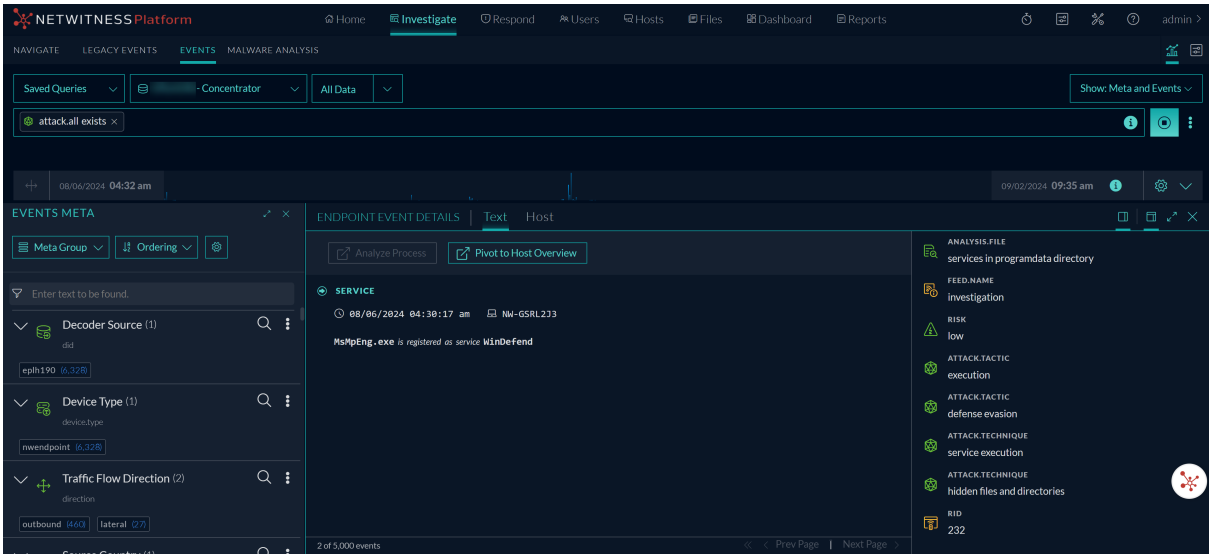
[**イベント メタデータ**]パネルと [イベント再構築]ビューの**ATTACK.TACTIC**および**ATTACK.TECHNIQUE**メタ キーに、[**MITRE ATT&CK©ルックアップ**]オプションが含まれるようになりました。これによりアナリストは、特定のイベントに関連するMITRE戦術およびテクニックに関する詳細情報を取得することができます。

重要 :MITRE ATT&CK®およびATT&CK®はいずれもMITRE Corporationの登録商標です。© 2024 The MITRE Corporation.この文書は、MITRE Corporationの許可を得て複製および配布されています。

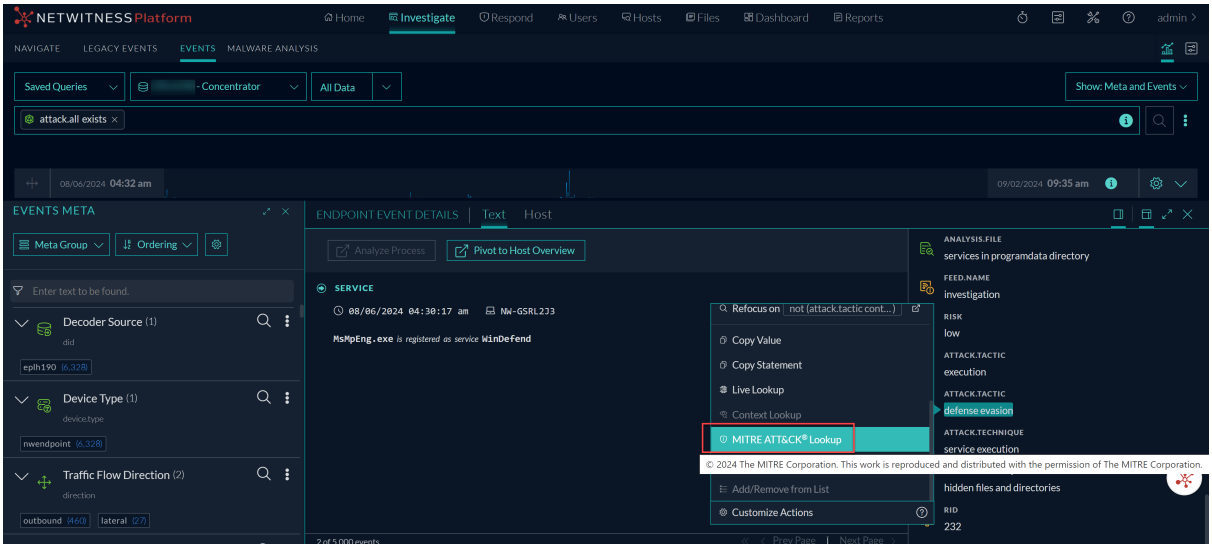
メタ キーでMITRE ATT&CK©ルックアップを実行するには

1. NetWitness Platformにログインします。
2. [**調査**] > [**イベント**]に移動します。
3. 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、各フィルタにメタ キーが含まれています。たとえば、「(**attack.all exists**)」のように指定します。
4. [**イベント**]パネルでイベントをクリックして、[イベント再構築]パネルを開きます。

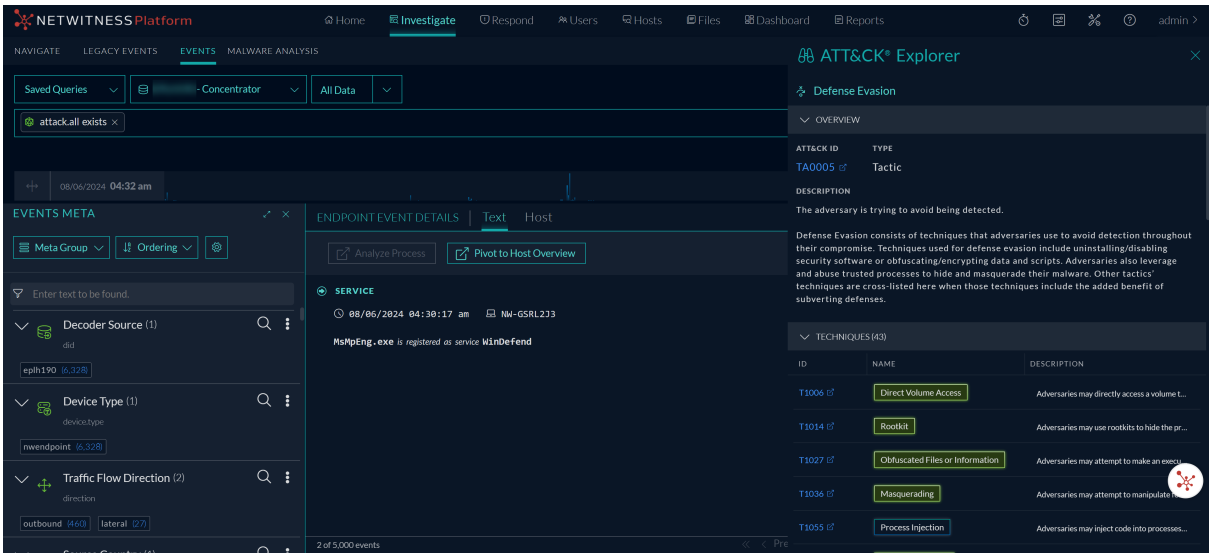
5. [**イベント メタデータ**]パネルで、**ATTACK.TACTIC**または**ATTACK.TECHNIQUE**メタ キーを左クリックまたは右 クリックします。



6. [**MITRE ATT&CK© ルックアップ**]オプションをクリックして、[**ATT&CK© Explorer**]パネルを開きます。



ブラウザ ウィンドウの右 側から [**ATT&CK© Explorer**]パネルが開きます。MITRE ATT&CKからの情報が利用可能になると、その情報が [**ATT&CK© Explorer**]パネルに入力されます。

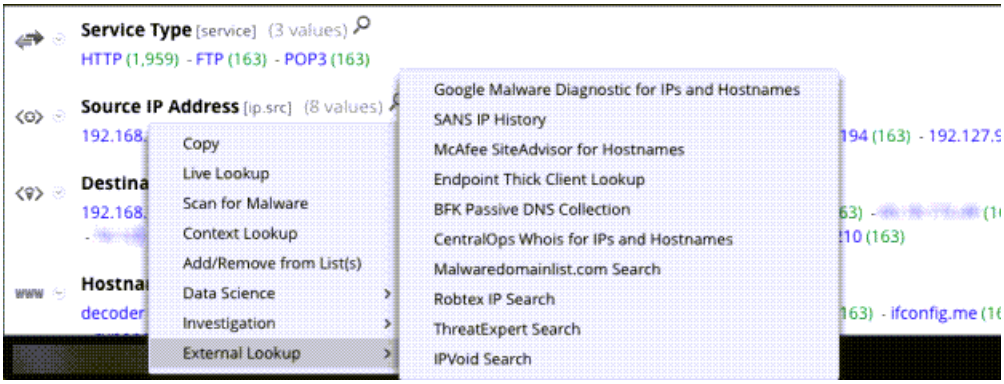


［**ATT&CK© Explorer**］パネルの詳細については、『NetWitness Respondユーザー ガイド』の「［**ATT&CK© Explorer**］**パネル**」を参照してください。

［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

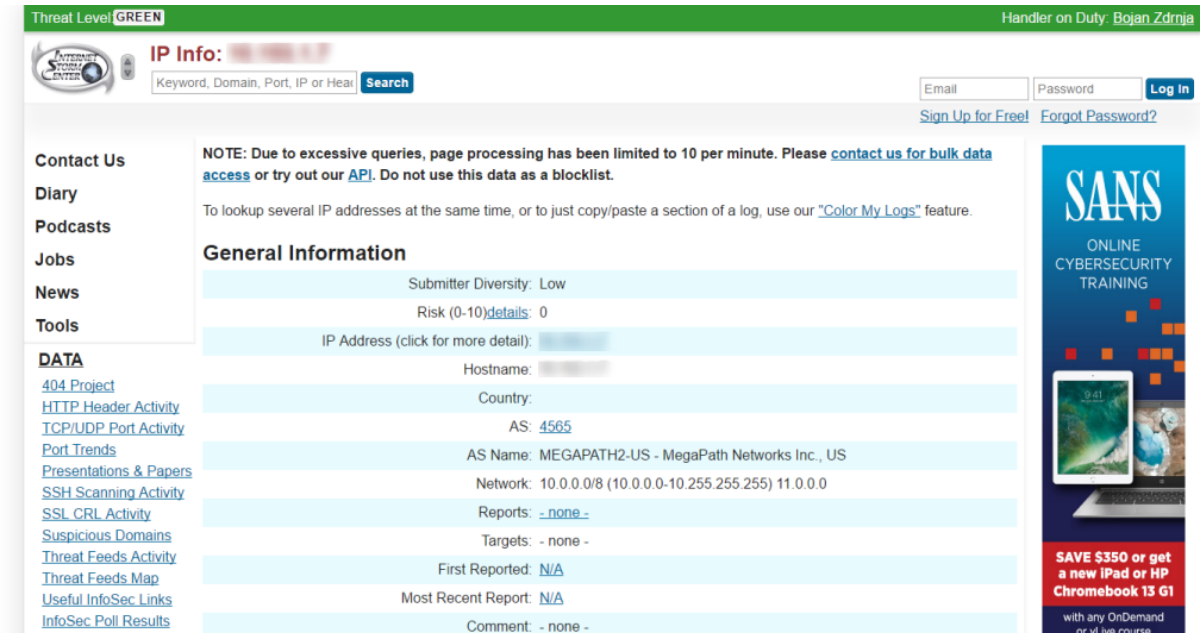
［ナビゲート］ビューからデータの外部ルックアップ(NetWitness Endpoint Thick Clientルックアップ以外) を起動するには、次の手順を実行します。

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

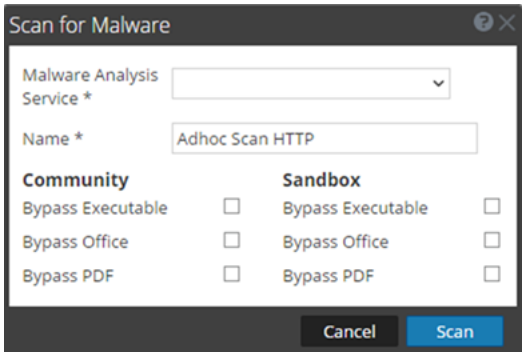
調査においてアナリストは、サービスとメタ値を選択し、コンテキスト メニューからオプションを選択することによって、オン デマンドMalware Analysisスキャンを開始できます。スキャンが完了すると、スキャンされたデータをMalware Analysisから確認できます。

[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、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。

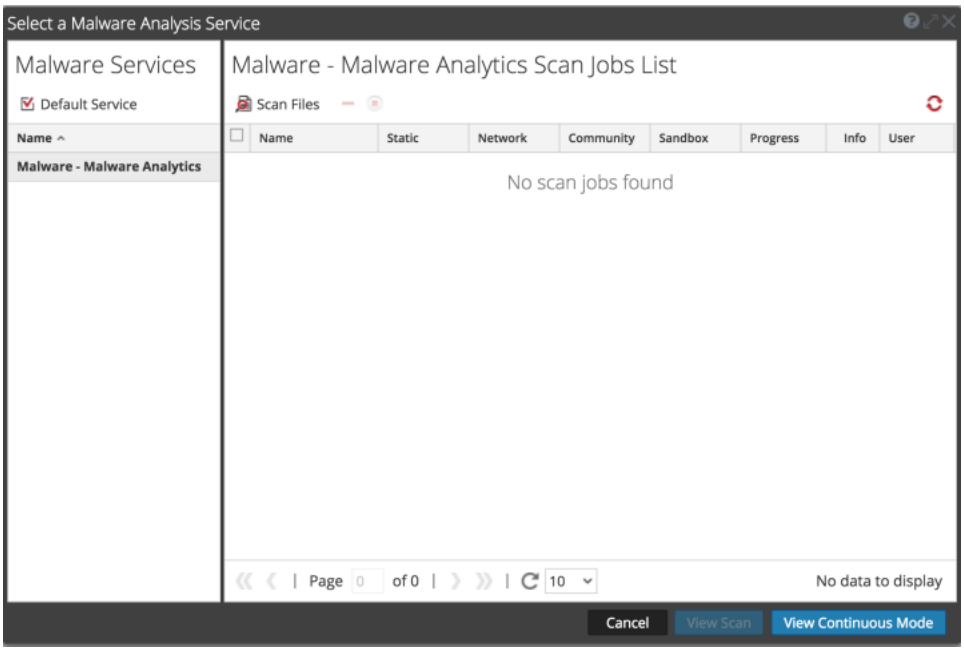


3. **[スキャン]**をクリックします。

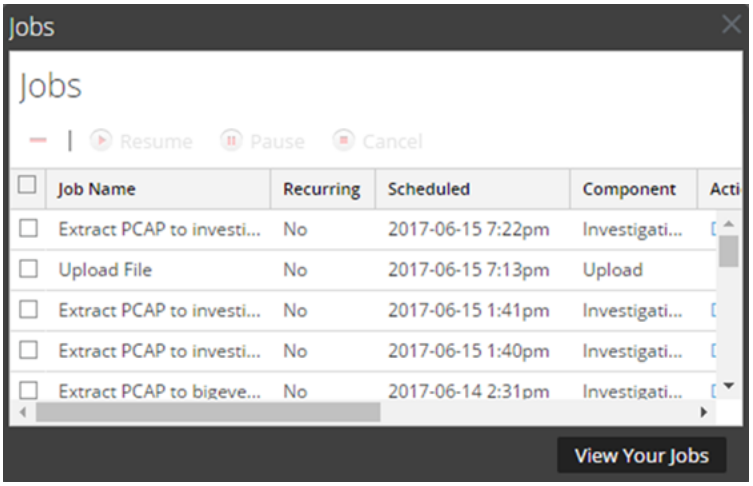
   スキャン リクエストが [スキャン ジョブ リスト]ダッシュレットとジョブ トレイに追加されます。このダイアログのバイパス設定は、Malware Analysisの基本構成のデフォルト設定を上書きします。

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。



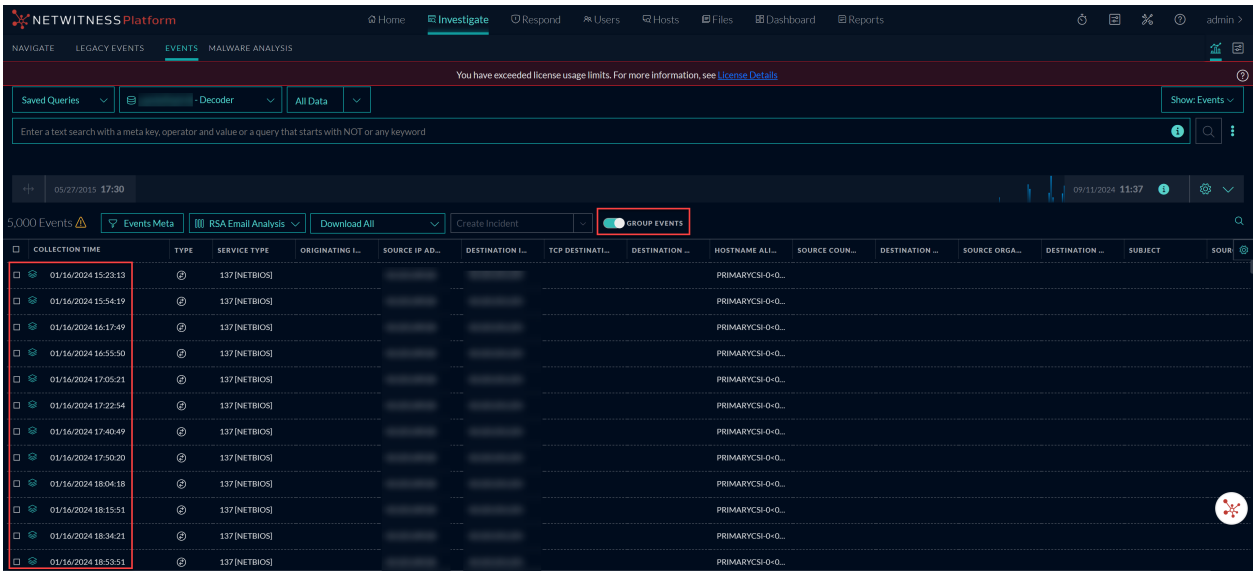
選 択 されたスキャンの [イベント のサマリー] が表 示 されます。また、このスキャンは、 **[調 査]** > **[マルウェア分 析]**タブを開いたときの [Malware Analysisサービスの選 択]ダイアログで、 [スキャンの選 択]リスト に追 加 され、そこから選 択 して開くことができます。

[イベント]ビューと [レガシー イベント]ビューでの分割および関連セッションからのイベントのグループ化

[イベント]ビューのイベント リストには、分割セッションと関連セッションからのイベントが、解析された順序で表示されるため、常に一緒に表示されるとは限りません。グループ イベント オプションを使用すると、イベントのリスト順序を変更して、キャプチャされたデータ内の関係をより簡単に検出できます。イベントがグループ化されている場合、最初のイベントは先行イベントと呼ばれます。

ユーザ インタフェースは、グループ化されたイベントを識別するよう設計されています。実線は関連するイベントのさまざまなグループを示すのに対し、点線は関連する同じグループに属するイベントを表します。イベントのグループでは、先行イベントが最初に置かれ、後続イベントは先行イベントの下でネスト構造になり、後続イベントのインデントおよび関係アイコンが表示されます。関係アイコンの横の数字は、セッション分割数を区別します。

現在のデータ セットに先行イベントが含まれていない場合でも、後続イベントは最初の後続イベントの下でグループ化されたままになります。先行イベントまたは最初のイベント(先行イベントがない場合)のみがソートされ、インデントされたイベントはソートされません。後続イベント マーカー( ) にカーソルを合わせると、関係を説明したツールチップが表示されます。次の図は、[イベント]リストに表示される関連イベントの例を示しています。



イベントがセッション フラグメントに基づいて関連している場合に、後続イベントを選択して再構築を開くと、[イベント メタ]パネルに`session.split`メタ キーが表示されます。

ネットワーク セッションの分割

次のようなツール チップが表示される場合、リスト内のイベントは分割ネットワーク セッションの一部です。

```
The event is part of a split session (session.split: #) matching these parameters: ip.src=127.0.0.1 AND ip.dst=127.0.0.1 AND tcp.srcport=25 AND tcp.dstport=1234.
```

分割の原因は次のいずれかです。

- 元のイベント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。

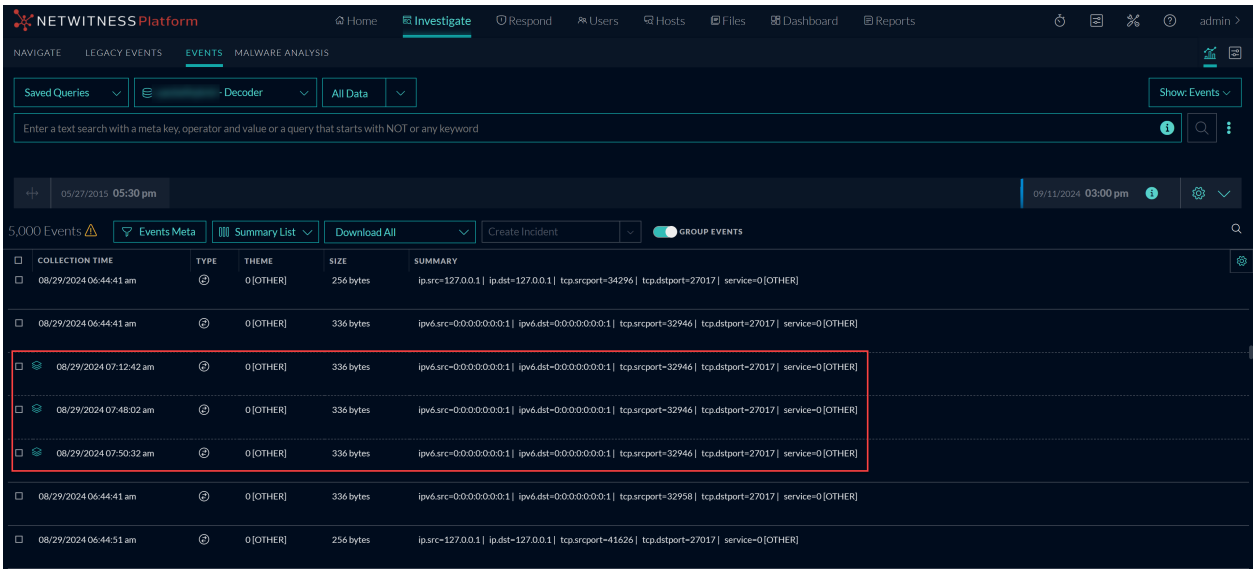
注：レガシー イベント ビューでは、セッション フラグメントを検索し、イベント リストに表示されるすべてのパケットを単一のPCAPにエクスポートできます (「 [レガシー イベント]ビューでのフラグメントの検索と結合 。

パケット デコーダーは、設定された最大セッション サイズ (デフォルト = 32 MB) または設定されたタイムアウト (デフォルト = 60秒) に基づいてセッションを分割する前に、セッション解析を完了します。解析が完了すると、解析結果には適切なアドレスの方向性とアプリケーション プロトコルが含まれ、これらは、各後続のセッション フラグメントに伝播され、それらが表す論理ネットワーク セッションとの一貫性が確保されます。

トランザクション処理の分割

管理者は、トランザクションを作成するように設計されたLuaパーサーを使用するときに、着信セッションをより小さなトランザクション セッションに分割するようにパケット デコーダーを構成できます。構成の詳細については、『*Decoder構成ガイド*』の「Decoderでのトランザクション処理の構成」を参照してください。Decoderサービス構成ノードには、パーサがネットワーク セッション内のトランザクションを定義するときにNetwork Decoderの動作を制御するパラメーターがあります。`/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、ネットワーク イベントの場合、元のパケットは通常どおりパケット デコーダーに保存されますが、関連する新しいトランザクション イベントはコンセントレータで作成されます。その結果、ユーザ インタフェースにはアナリスト向けのビジュアル キューが表示され、以前はすべてバンドルされていた特定のEメールまたはEメール属性のみを検索するクエリを実行することも可能になります。クエリ結果から元のイベントを除外するため、session.splitメタキーはインデックスされています。トランザクション分割がある場合、元のイベントにそのメタ キーは関連づけられませんが、関連するすべてのトランザクション イベントには関連づけられます。



セッション フラグメントの強調表示

どちらのタイプのセッション フラグメントにも、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。

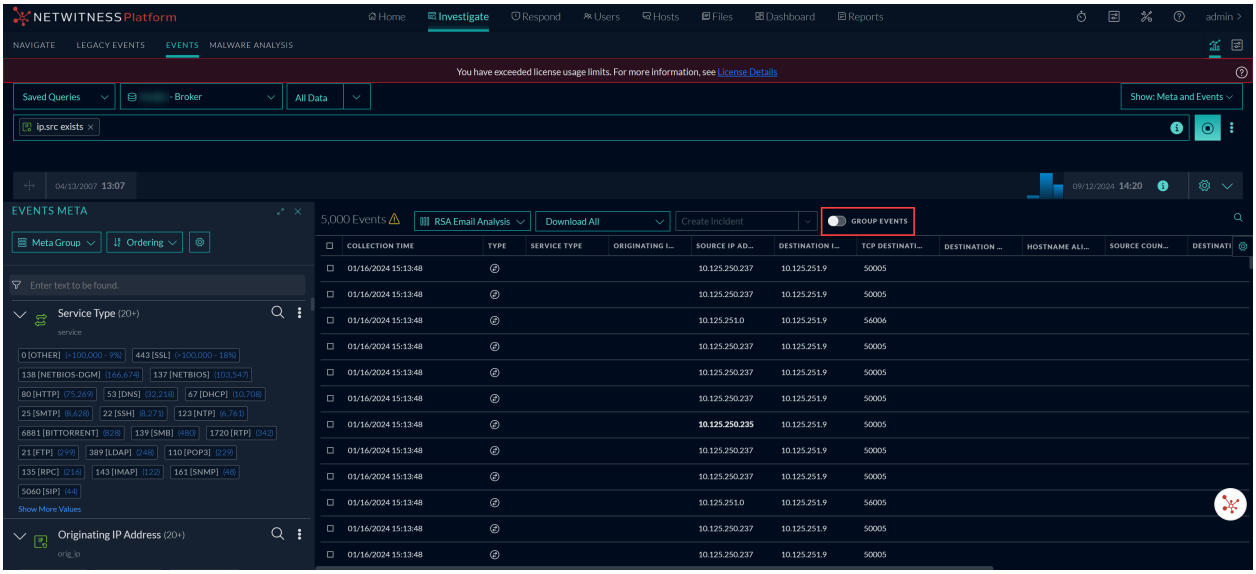
```
The event is related to a previous session matching these parameters:
ip.src=127.0.0.1 AND ip.dst=127.0.0.1 AND tcp.srcport=25 AND
tcp.dstport=1234"Second category: Related Network Session
```

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`

データ プライバシーが有効になっている場合、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 オプションは無効になります。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、正しく組み合わせてマッピングすることは困難です。セッションを先行イベントと後続イベントとして編成することで、アナリストは各メールの詳細を明確に把握できるようになります。
- アナリストは、セッションに関連づけられたすべてのメタデータのうち、どのIPアドレスがメタデータの生成またはアラートの原因となったかを理解しようとしていますが、IPアドレスが出力に含まれていません。たとえば、侵害の兆候を解析しているフィードでは、多くのIPアドレスを持つセッションで多くのトリガーが発生する可能性があります。アナリストは、先行イベントと後続イベントとして編成された完全なイベントを表示することにより、アラートをトリガーしたIPを把握できます。
- アナリストは、どのディレクトリからどのファイルが削除されたか、どのディレクトリでどのファイルが読み取られたかを把握する必要がありますが、セッションに複数のファイルとディレクトリが含まれています。たとえば、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。

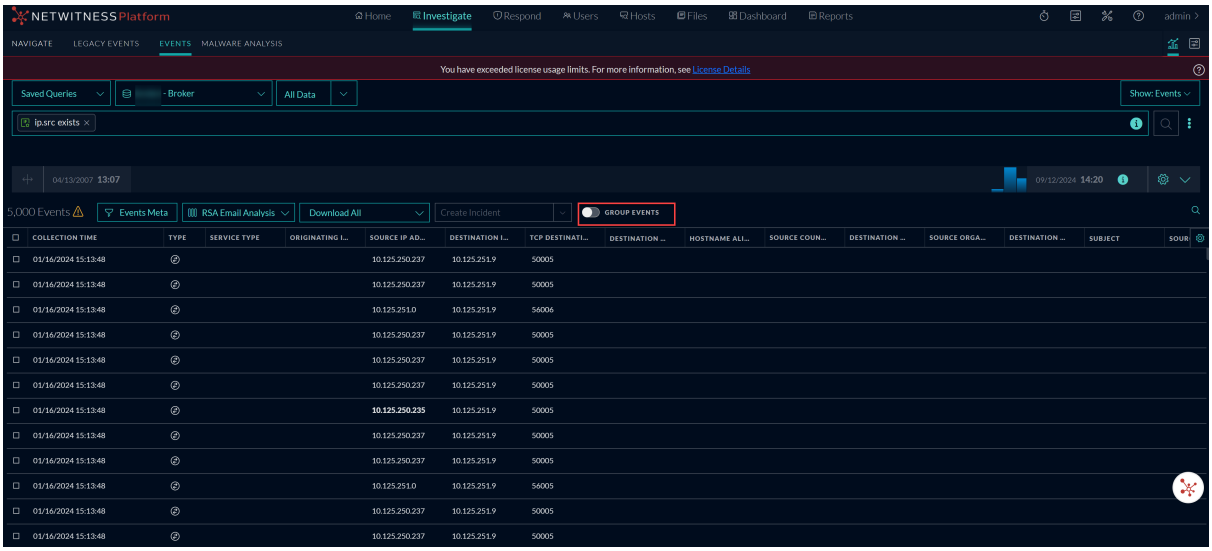
- 疑わしいアラートをトリガーしたイベントに関連している大容量ファイルをアナリストが取得しようとしています。ただし、転送されたファイルは大きすぎたため、Network Decoderによって100個の個別のセッションに分割されました。アナリストは、このグループ関連の分割セッションを表示する際に、セッションのPCAPをダウンロードし、より大規模なアセンブラー設定のDecoderまたはサード パーティ ツールでそれを実行することにより、元のファイルを抽出できます。

イベント リストでの関係の表示と非表示

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

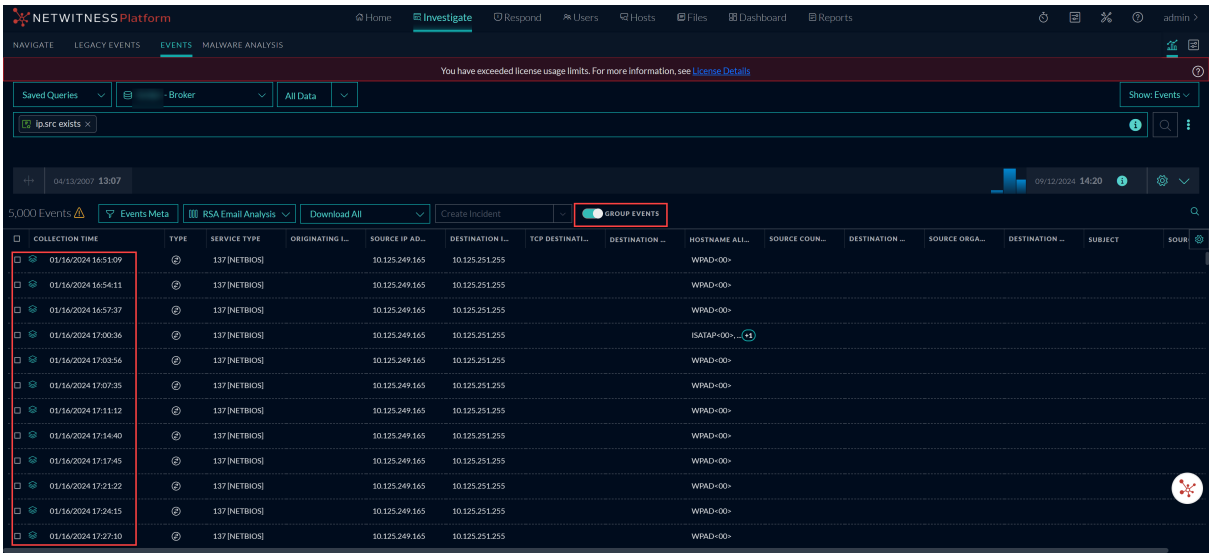
[イベント]リストで関連イベントを見つけるには

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。

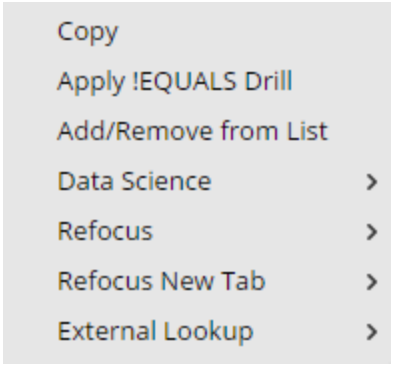


[レガシー イベント]ビューでのフラグメントの検索と結合

[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。

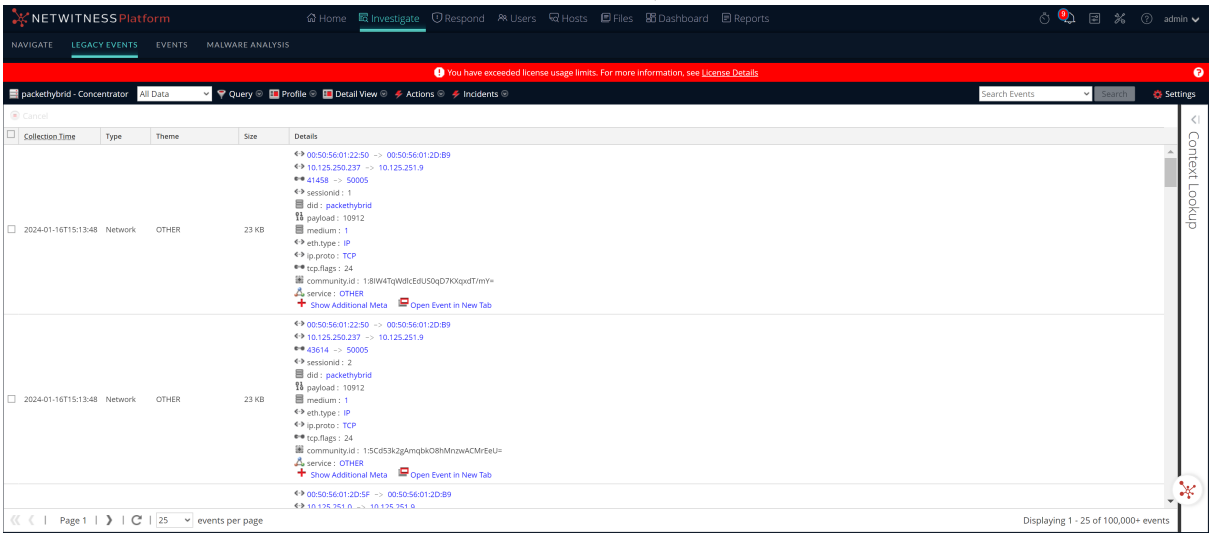
セッション フラグメントを検索するには

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。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ことがあります。

4. (オプション) すべてのセッション フラグメントのパケットを1つのPCAPファイルにエクスポートするには、[**アクション**] > [**すべてのPCAPのエクスポート**]を選択します。
PCAPがダウンロード中であることを示すメッセージが表示されます。ダウンロードが完了すると、PCAPファイルには、分割されたネットワーク セッションの全体が含まれています。

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たときに異常なパターンや関係が明らかになる場合があります。メタ グループ(「メタ グループを使用して関連性の高いメタ キーにフォーカス」を参照)を効果的に使用して、座標表示チャートに追加するメタ キーのコレクションを定義することができます。

効果的な座標表示チャートに関するベスト プラクティス

効果的な座標表示チャートを作成するには、以下の推奨事項を実行します。

- 新規インストールに含まれているRSA標準提供のメタ グループを使用します。
- すべてのデータを可視化しようとするのではなく、1つのドリルダウン ポイントから開始します。
- 必要に応じて時間範囲を制限します。
- 可能な限り少ない数の有益なメタ キーを軸として表示するよう選択します。
- メタ値間の異常性が強調されるように、チャート内の直線に沿って軸の順序を指定します。
- 有益なメタ キーとその順序を特定できる場合は、将来の調査で使用するカスタム メタ グループを作成します。たとえば、Windows実行可能ファイル タイプのカスタム メタ グループを作成できます。
- カスタム メタ グループを.jsnファイルとしてインポートおよびエクスポートすることによって、グループを再利用したり共有したりします。
- カスタム メタ グループごとに2つのバージョンを作成しておくと便利です。1つはメタ値の分析に使用し、もう1つは同じユースケースの小規模サブセットに重点を置いた座標表示チャートの作成に使用します。

注 :メタ グループをインポートするとき、既存のメタ グループが含まれていると、エラー メッセージが表示されます。重複したグループをインポートするには、まず既存のグループを削除しておかなければなりません。プロファイル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。

座標表示で使用できるRSAメタ グループ

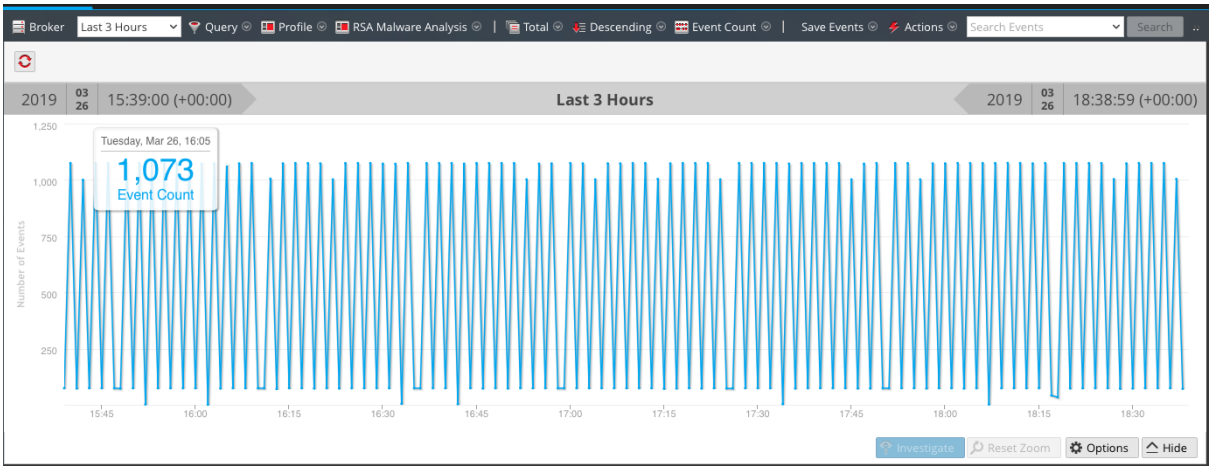
NetWitnessには、事前定義されたメタ グループのセットが含まれています。最新のバージョンを取得する場合は、［メタ グループの管理］ダイアログでメタ グループ ファイル(MetaGroups_ootb_query.jsn)をインポートできます。座標表示チャートに適した標的型アクティビティとしては、次のようなものがあります。

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

座標表示チャートの表示

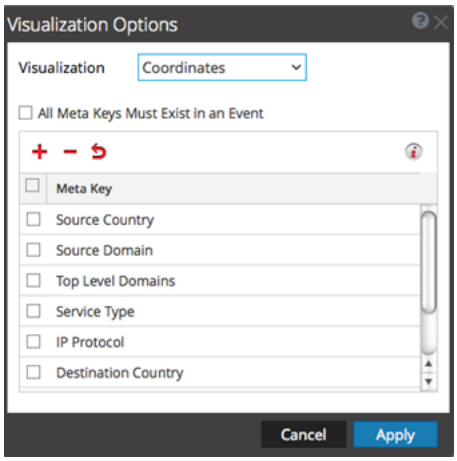
[調査] > [ナビゲート]ビューで、次の手順を実行します。

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。

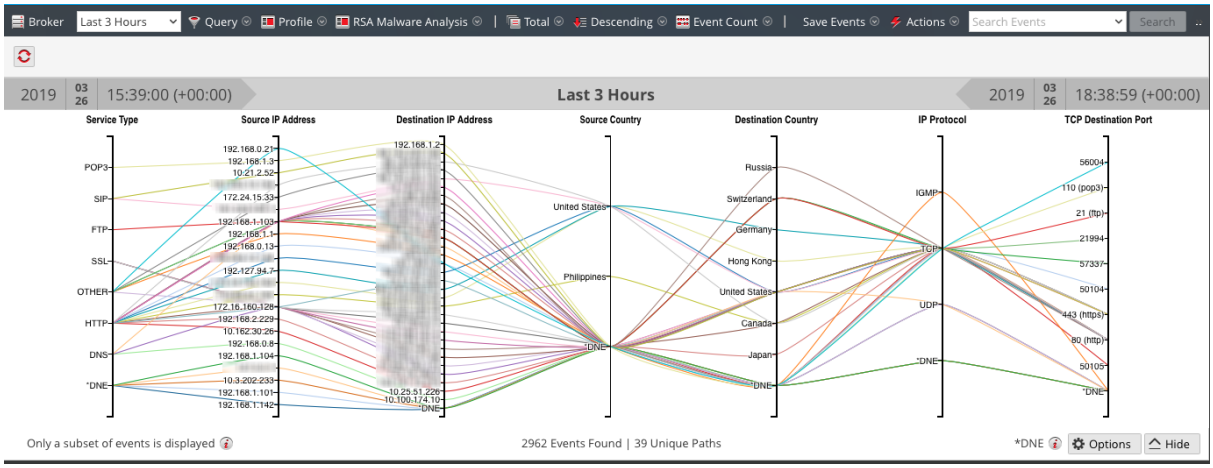


4. [**チャート**]パネルで [**オプション**]を選択します。
   [チャート オプション]ダイアログが表示されます。

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。



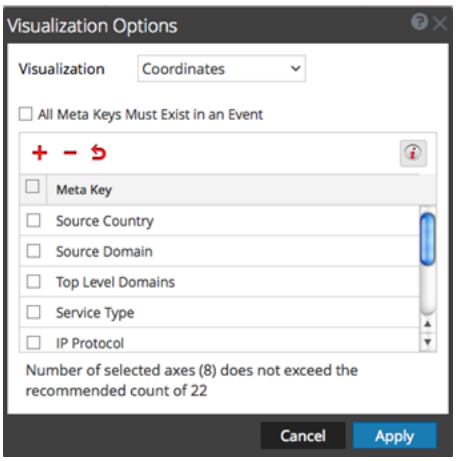
チャートがロードされます。この例では、2,962個のイベントが見つかり、39個の一意のパスが可視化されます。



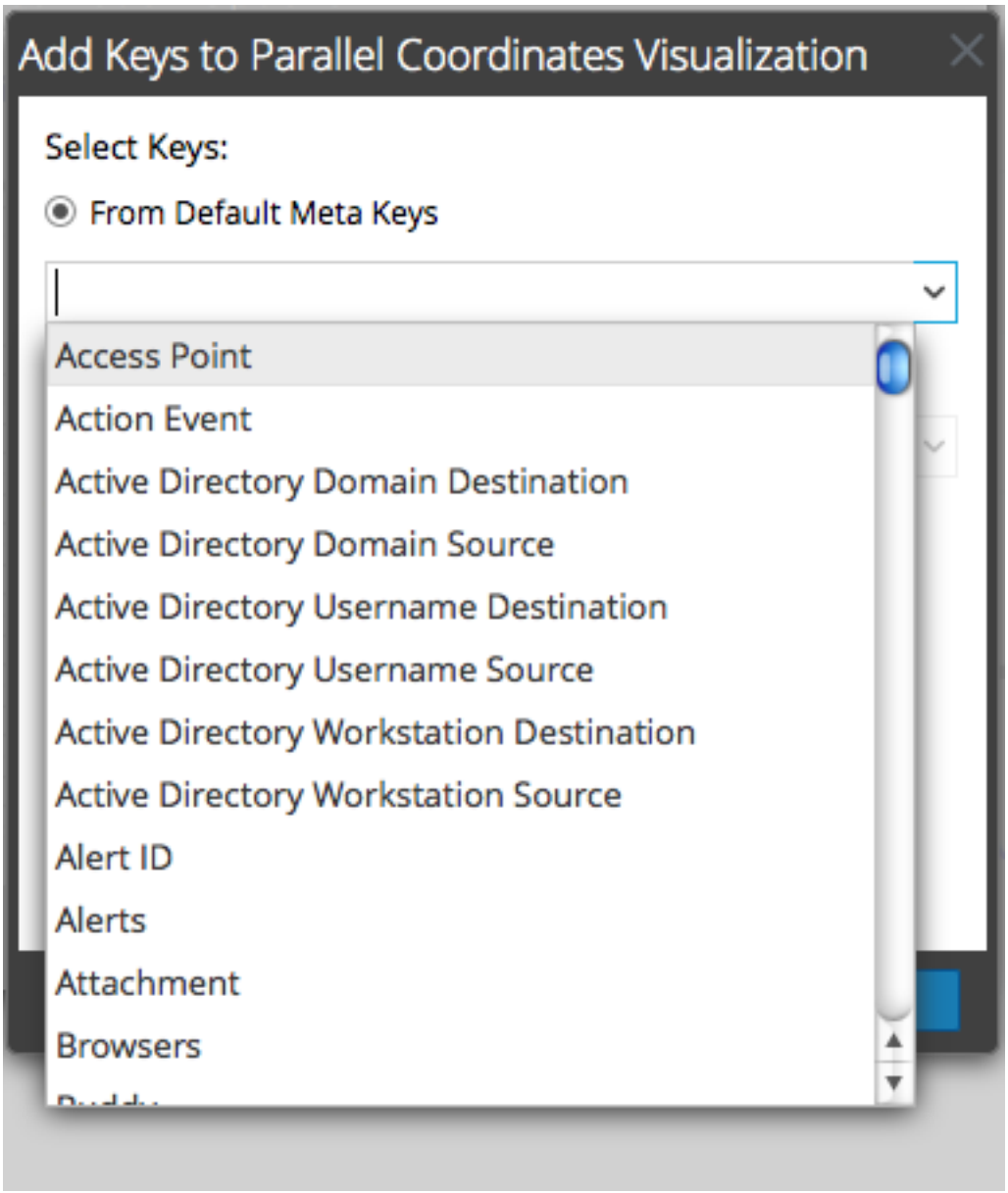
座標表示チャートで使用するメタ キーの選択

座標表示チャートが開いた状態で、次の操作を行います。

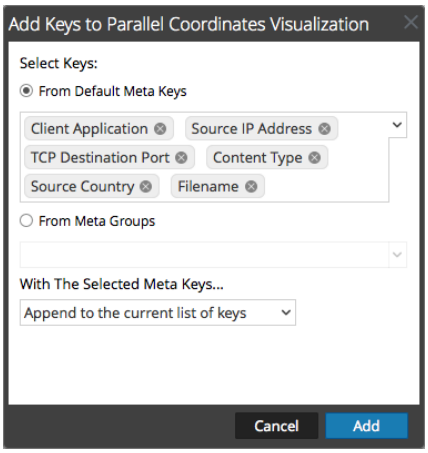
1. [チャート]パネルで [オプション]を選択します。
   [チャート オプション]ダイアログが表示されます。ツールバーの をクリックすると、見やすいチャートに適した軸数が表示されます。推奨される軸の数は、ブラウザのサイズによって変化します。ブラウザ ウィンドウを拡大すると、推奨される数は増加します。



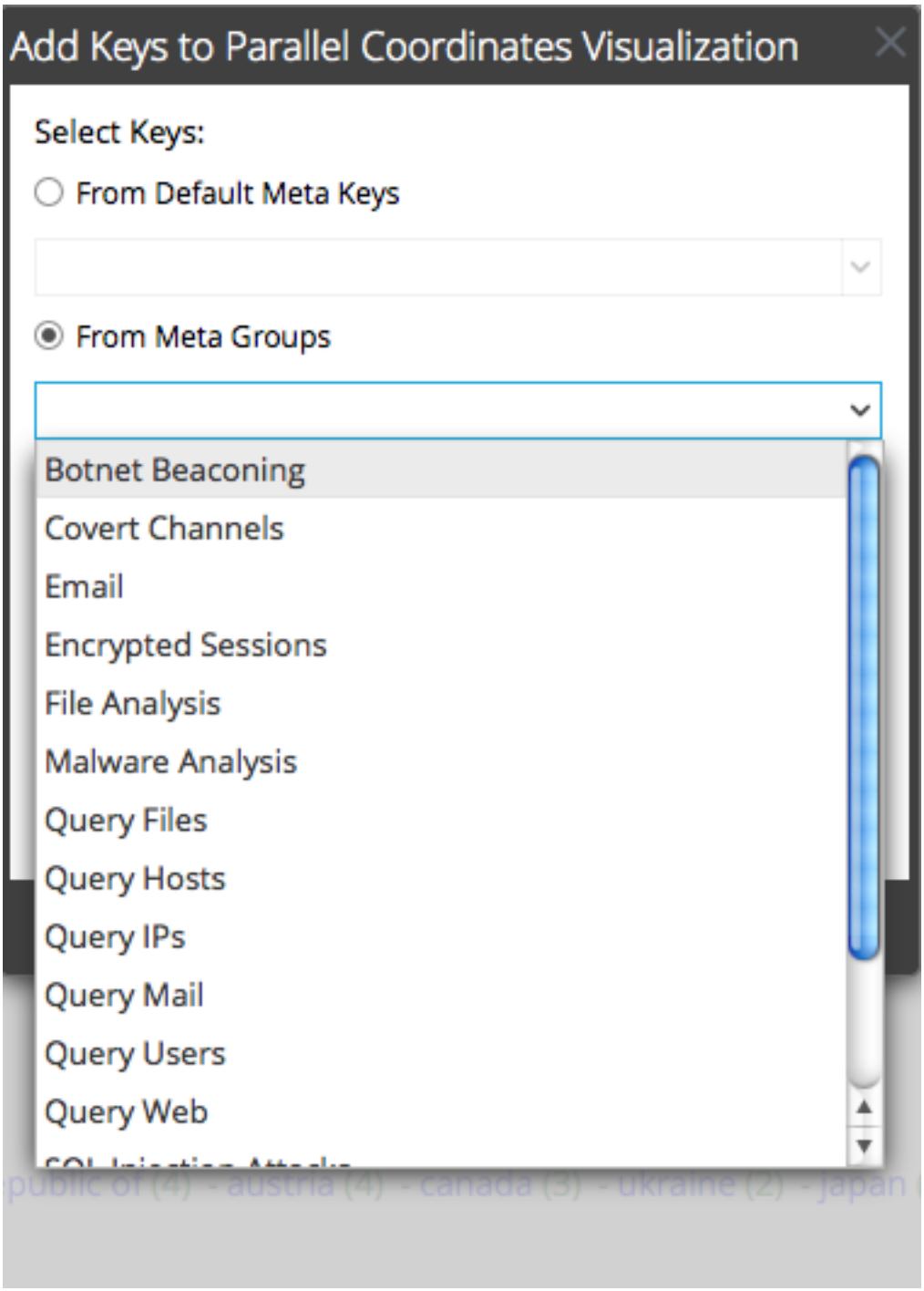
2. メタ キーの順序を変更するには、メタ キーを上下にドラッグして目的の順序に変更します。
3. メタ キーを削除するには、選択ボックス内をクリックして、 をクリックします。
   メタ キーが削除されますが、変更は適用されません。
4. 元の状態に戻すには、 をクリックします。
   削除したメタ キーがすべてリストアされ、行った変更がすべて削除されます。
5. メタ キーを個別に選択する場合は、 をクリックし、 [**デフォルトのメタ キーから追加**]を選択し、ドロップダウン リストからメタ キーを選択します。



選択したキーが表示されます。

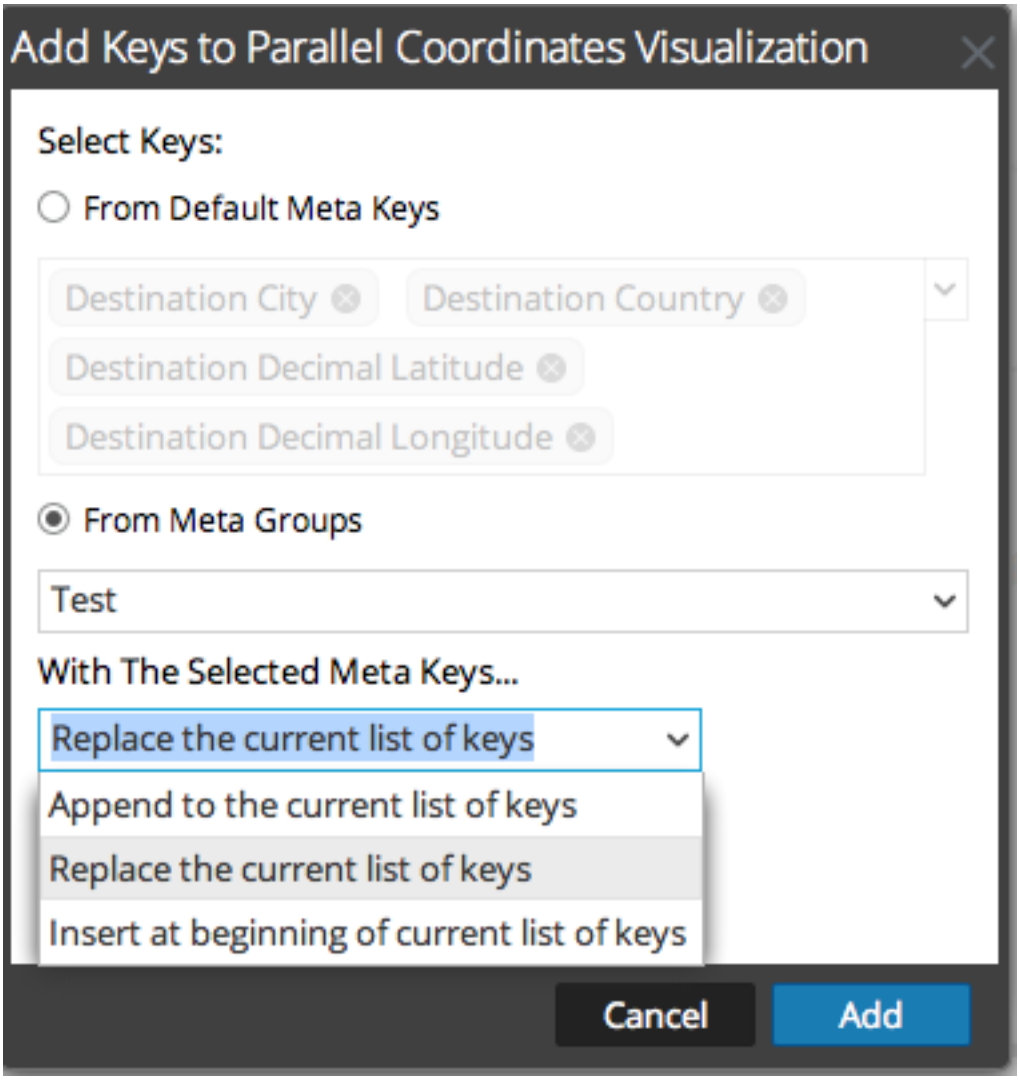


6. メタ グループ内のすべてのメタ キーを追加する必要がある場合、メタ キーを個別に追加する必要はありません。 [**メタ グループから追加**]を選択して、ドロップダウン リストからグループを選択します。



選択したメタ グループがフィールドに表示されます。

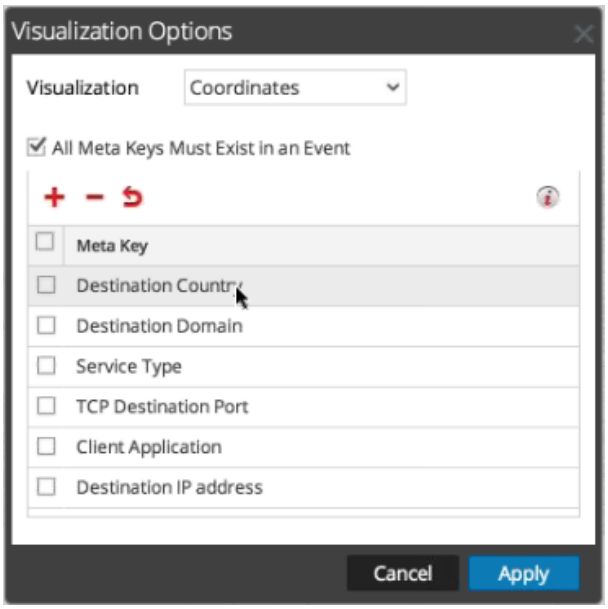
7. キーまたはグループの追加方法を、［**現在のキーのリストを置き換え**］、［**現在のキーのリストの後に挿入**］、［**現在のキーのリストの先頭に挿入**］から選択します。



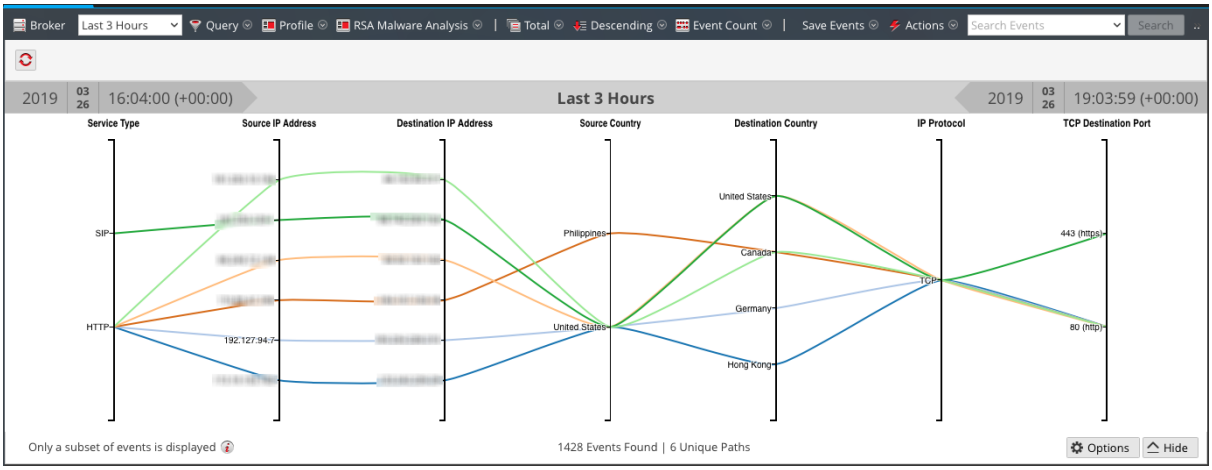
8. 処理手順を完了するには、［**追加**］をクリックします。
［チャート オプション］ダイアログに、選択したメタ キーまたはメタ グループが表示されます。
9. 新しいチャートを表示するには、［**適用**］をクリックします。

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。

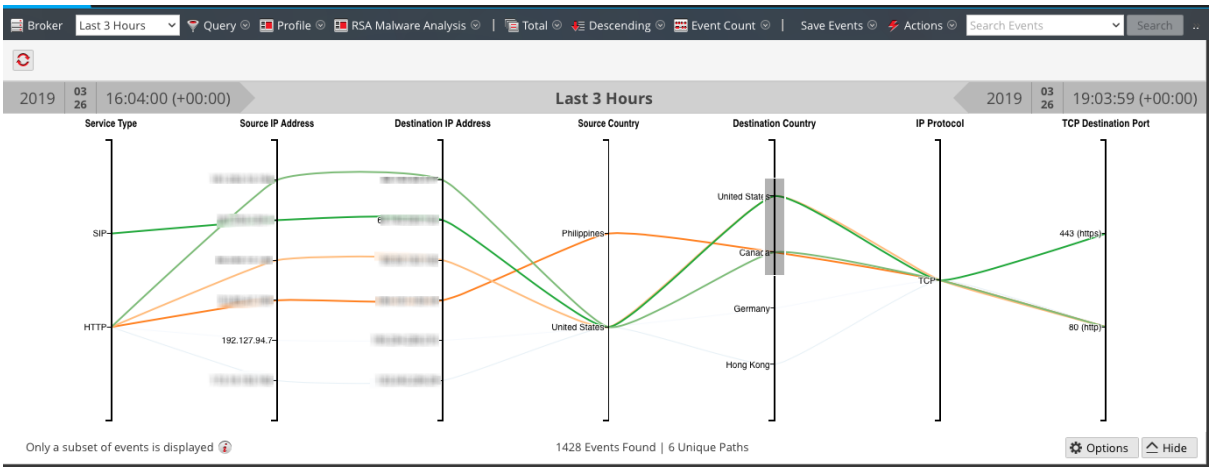


2. ［ビジュアル化オプション］ダイアログで［**すべてのメタ キーが1つのイベントに存 在 する必 要 があります**］を選 択します。［**適 用**］をクリックします。
結 果 として表 示されるチャートは、見 やすく便 利になり、固 有 パスの数 が減 少します。



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。

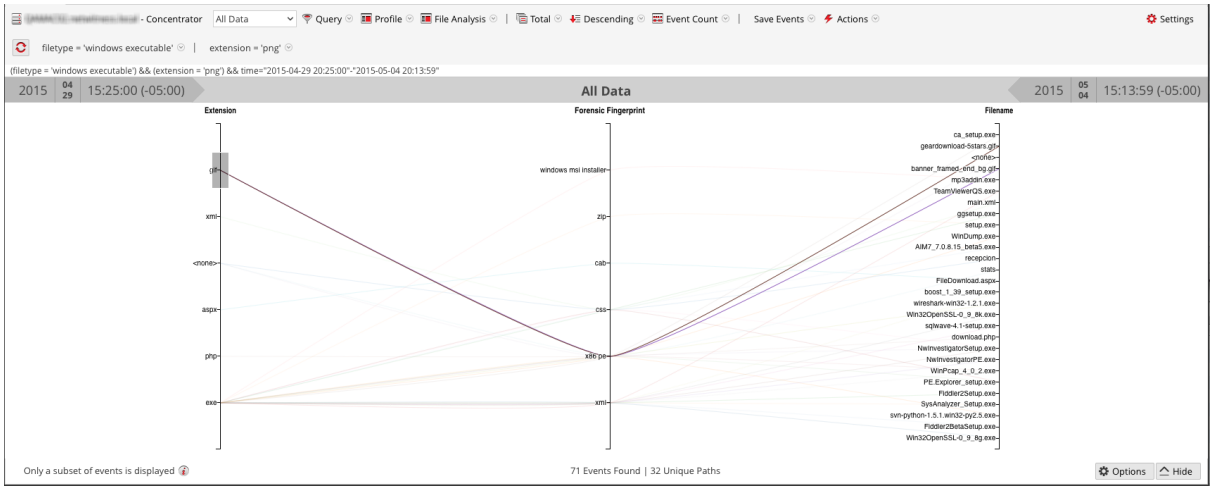
使用例

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`。

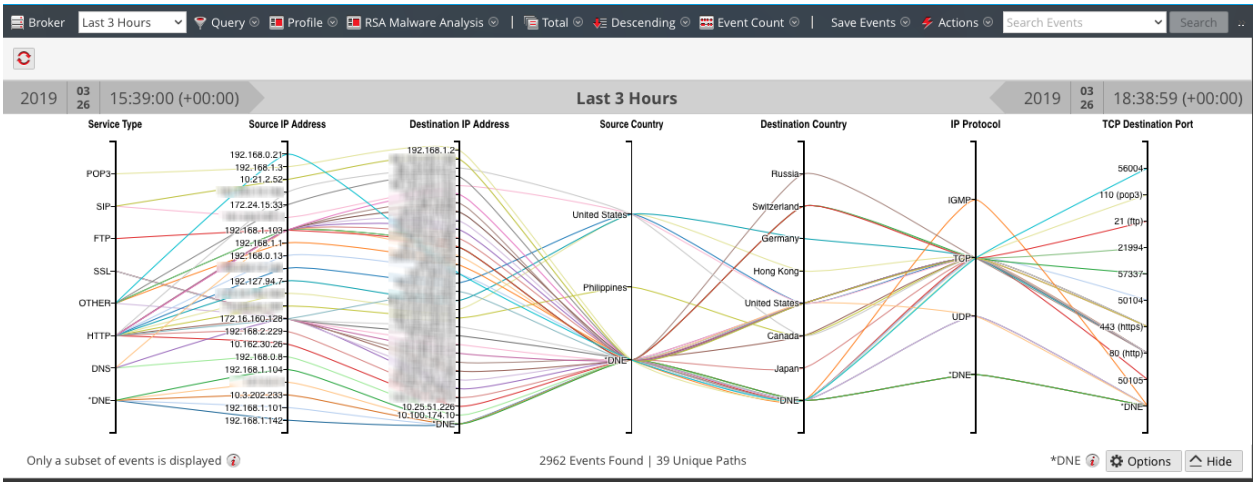


大量データセットのチャートの例

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。

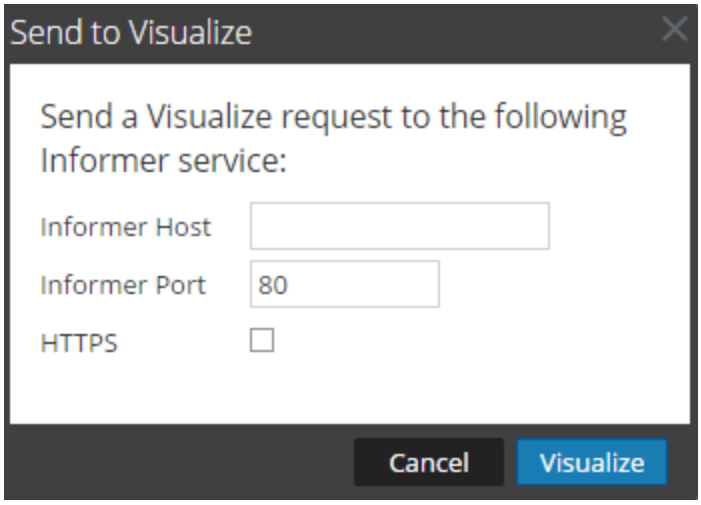
ドリルダウン ポイントのInformerでのビジュアル表 示

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

Informerがネット ワーク内 にインスト ールされ、調 査 中 のサービスからアクセスできる必 要 があります。NetWitnessと通 信 するために、Informerのホスト 名 とポートを指 定 する必 要 があります。

現 在 のドリルダウン ポイントをInformerでビジュアル表 示 するには、次 の手 順を実 行します。

1. [ナビゲート]ビューでドリルダウン ポイントが開いている状 態 で、 [**アクション**] > [**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
- ［ナビゲート］ビューでのドリルダウン ポイントのエクスポートまたは印刷
- ［レガシー イベント］ビューでのイベントのエクスポート
- ［イベント］ビューでのインシデントへのイベントの追加
- ［レガシー イベント］ビューでのインシデントへのイベントの追加

[イベント]ビューでのデータのダウンロード

[イベント]ビューでは、[イベント]パネルと再構築からデータをダウンロードできます。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。

- 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。
- [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。
- [イベント]パネルおよびイベントの再構築のすべてのイベント タイプについて、イベント、ログ、ファイルをダウンロードするために必要な名前を入力する機能が追加されました。

注 :表示およびダウンロードできる情報は、管理者が実装したロールベース アクセス制御(RBAC)によって管理されます。特定のデータがダウンロードされるのを防ぐようにRBACが設定されている場合、ダウンロード権限のないイベントが正常にダウンロードされたように見えることがありますが、サイズは0バイトです。特定のイベントが再構築されるのを防ぐようにRBACが設定されている場合、再構築は[イベント]パネルで無効になりますが、一括ダウンロード ボタンは有効なままになります。

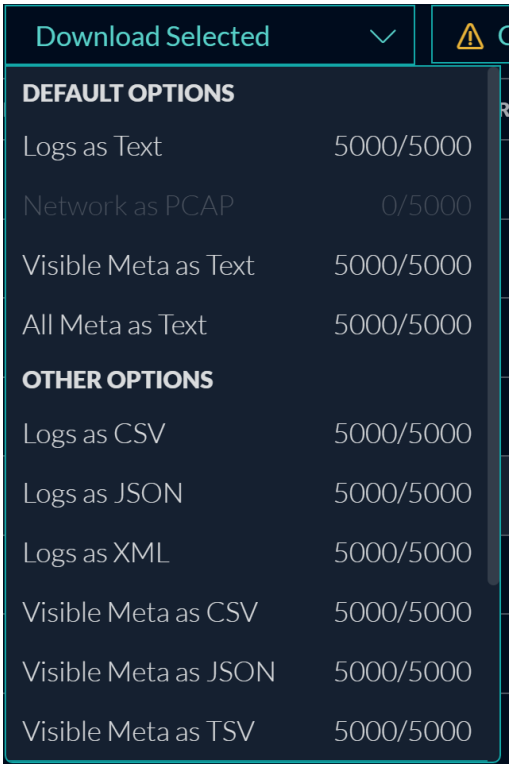
イベントまたはメタデータの[イベント]パネルでのダウンロード

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、またはすべてのメタデータを、[イベント]パネルから直接、指定した形式でダウンロードできます。環境設定は[イベント環境設定]ダイアログで設定され、変更はすべて**[ダウンロード]**メニューに反映されます。環境設定の詳細については、「[イベント]ビューの構成」を参照してください。

[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**[選択した内容のダウンロード]**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、次の図に示すように「`0 / Total number of events selected`」と表示されます。



[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は、 [選択した内容のダウンロード]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も使用できます。



[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。

- 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 セレクターによって決 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。

- 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 [**選 択した内 容 のダウンロード**]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。

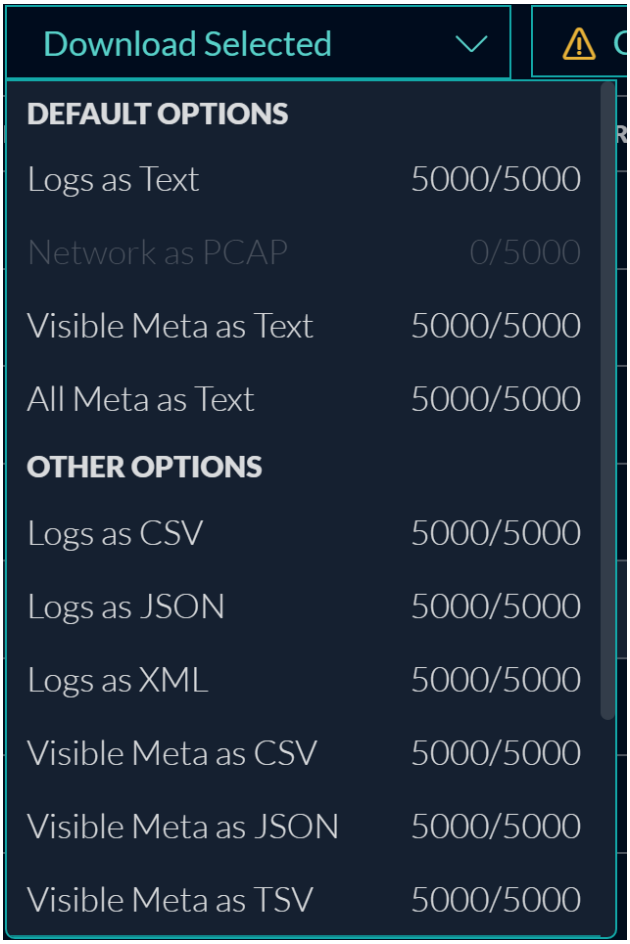
注 :すべてのイベントをダウンロードするよう選 択 すると、現 在 の結 果 セット内 のイベントのみがダウンロードされます。すべての結 果 が返 される前 にクエリをキャンセルした場 合 は、ロードされたイベントのみがダウンロードされます。

[イベント]パネルで単 一 、複 数 、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

1. 次 のいずれかを実 行します。
   a. イベントを個 別 に選 択 するには、ダウンロードする各 イベントの隣 にあるチェックボックスをオンにし、 [**選 択した内 容 のダウンロード**]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。



b. [イベント]パネルに表示されているすべてのイベントを選択するには、[イベント]パネルの上部にあるチェックボックスをオンにし、**[選択した内容のダウンロード]**メニュー ボタンをクリックします。



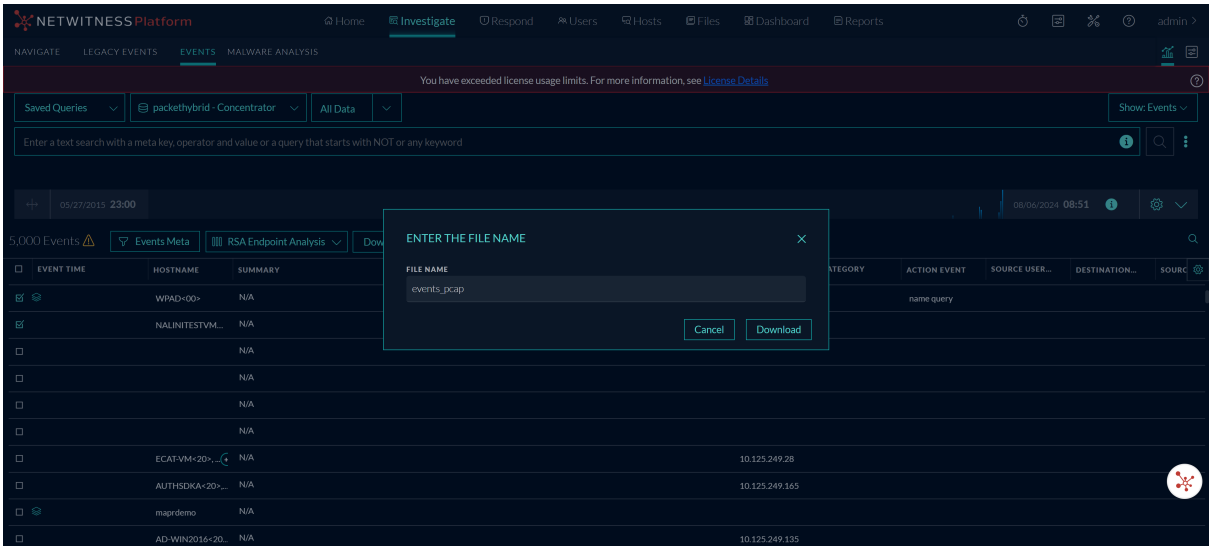
c. 利用可能なイベントをすべてダウンロードするには、メニューから[**すべてダウンロード**]ボタンをクリックします。ダウンロードできるイベントの数は、[イベント設定]パネルの[**エクスポートするセッションの最大数**]オプションの設定値によって異なります。ダウンロードできるイベントの最大数は**100000**です。

2. メニューの上部で有効になっている[**デフォルトのオプション**]を確認します。デフォルトの形式を使用しない場合は、メニューの[**その他のオプション**]セクションで別の形式を選択できます。

- [イベント環境設定]メニューで選択した形式(**テキスト形式のログ**、**CSV形式のログ**、**JSON形式のログ**、**XML形式のログ**)でログがダウンロードされます。このダウンロードに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。

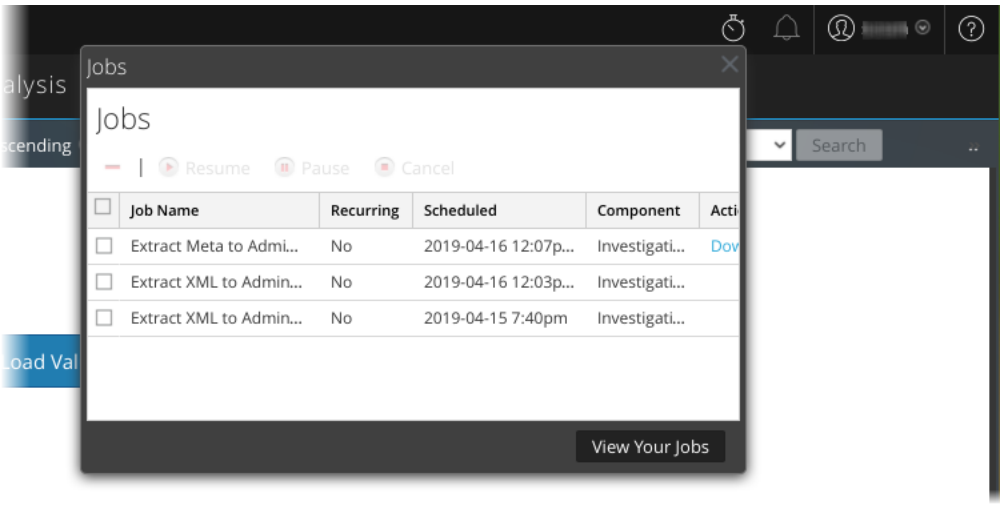
3. [**選択した内容のダウンロード**]オプションをクリックします。
4. ファイル名を入力するためのダイアログ ボックスが表示されます。デフォルトでは、ファイル名は最初に次の形式でタイムスタンプとともに表示されます。`investigation-yyyy-mmm-dd-hh-mm-ss` (例 **investigation-2024-Jan-08-22-33-54**)。必須のファイル名を入力し、[**ダウンロード**]をクリックします。



[**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([**イベント**]ビュー>) 場合は、ブラウザー 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。

5. [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。



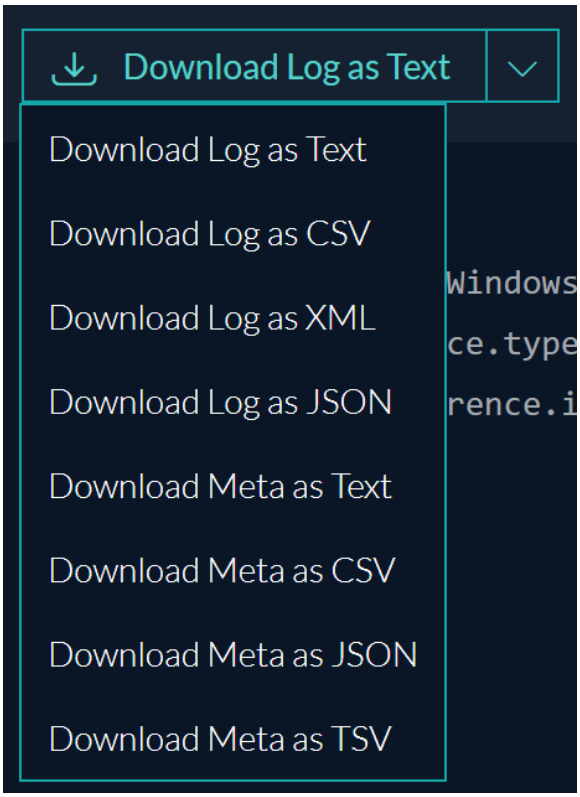
テキスト再構築でのログのダウンロード

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(log)。［**テキスト形式でログをダウンロード**］オプションを使用。
- カンマ区切り値(CSV)。［**CSV形式でログをダウンロード**］オプションを使用。
- 拡張可能マークアップ言語(XML)。［**XML形式でログをダウンロード**］オプションを使用。
- JavaScript Object Notation(JSON)。［**JSON形式でログをダウンロード**］オプションを使用。

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**］



注 :エンドポイント イベントの場合、 **[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。

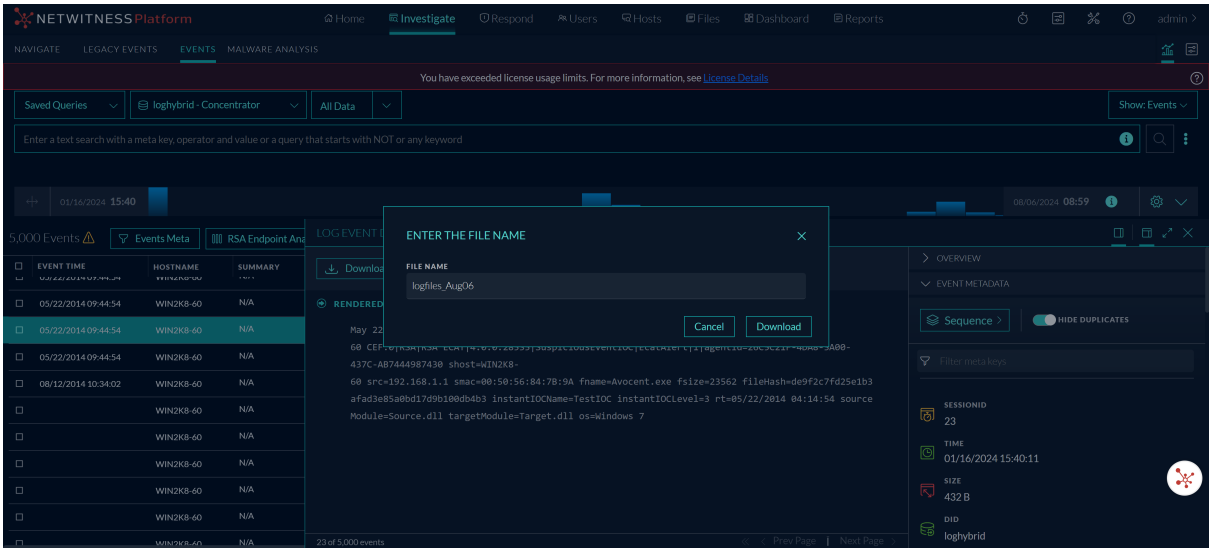
注 :いくつかの形式では、タイム スタンプまたはイベントが生成されたデバイスIPが含まれません。このためCSV、XML、JSON形式でダウンロードされたログには、RAWログの内容とともに`timestamp`という追加の値が含まれます。追加の情報は次の形式でログに含まれます :`Log timestamp="1490824512" source="10.12.35.65".`

ログまたはログのメタデータをダウンロードするには

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) としてログをダウンロードするには、 **[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、 **[テキスト形式でログをダウンロード]**ボタン上の下向き矢印をクリックして、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、 **[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。

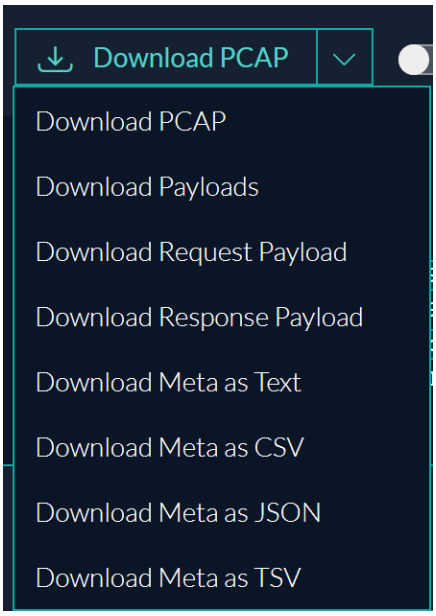
4. (バージョン12.4以降) ファイル名を入力するダイアログが表示されます。デフォルトでは、ファイル名は最初に次の形式でタイムスタンプとともに表示されます。`investigation-yyyy-mmm-dd-hh-mm-ss`(例 **:investigation-2024-Jan-08-22-33-54**)。必須のファイル名を入力し、[**ダウンロード**]をクリックします。



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。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。 [**ペイロード のダウンロード**]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。
- 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。

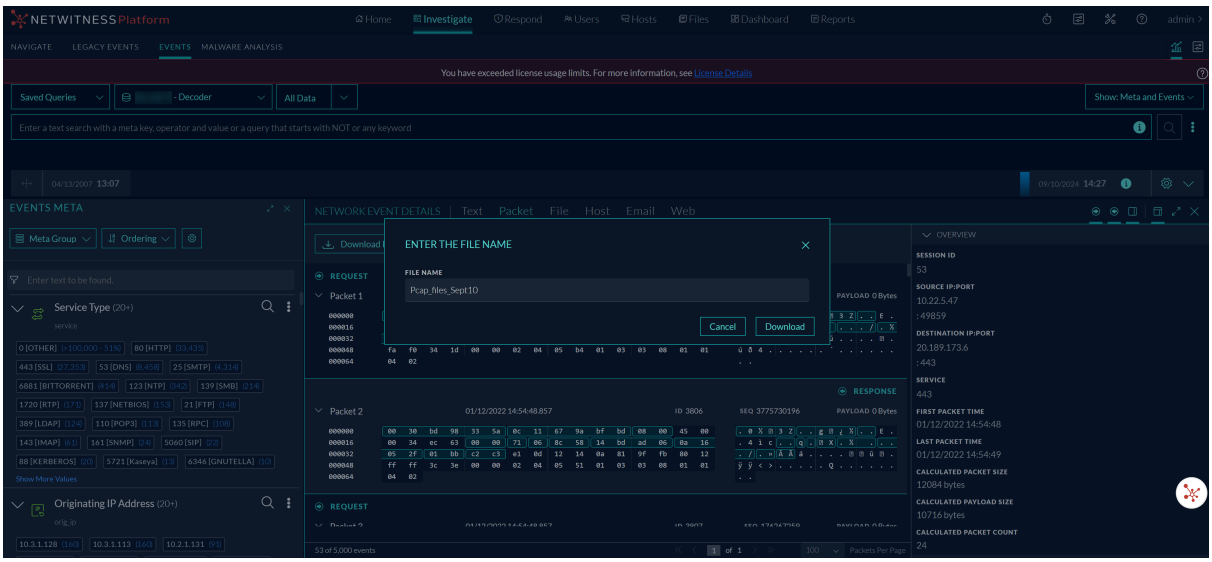
ネットワーク データは、ダウンロードが迅速な場合、ブラウザに直接ダウンロードされます。ネットワーク要因やファイル サイズによりダウンロードに時間がかかる場合、ファイルは、バック グラウンドでダウンロードされ、タスクはジョブキューでトラッキングされます。この場合は、キューでジョブを確認し、ダウンロードが完了するとファイルを取得できます。

注 :ダウンロードを選択してから、ダウンロードが開始する前にファイルを抽出している途中でブラウザのページを移動すると、ファイルはダウンロードされません。ジョブ キューからファイルをダウンロードできるというメッセージが通知されます。

イベントをネットワーク データ ファイル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

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. イベントのメタデータをダウンロードするには、ボタンの下向き矢印をクリックし、ダウンロードしたメタデータのファイル形式のいずれかを選択します。
4. ファイル名を入力するためのダイアログ ボックスが表示されます。デフォルトでは、ファイル名は最初に次の形式でタイムスタンプとともに表示されます。`investigation-yyyy-mmm-dd-hh-mm-ss` (例: **investigation-2024-Sep-10-20-03-40**)。必須のファイル名を入力し、[**ダウンロード**]をクリックします。



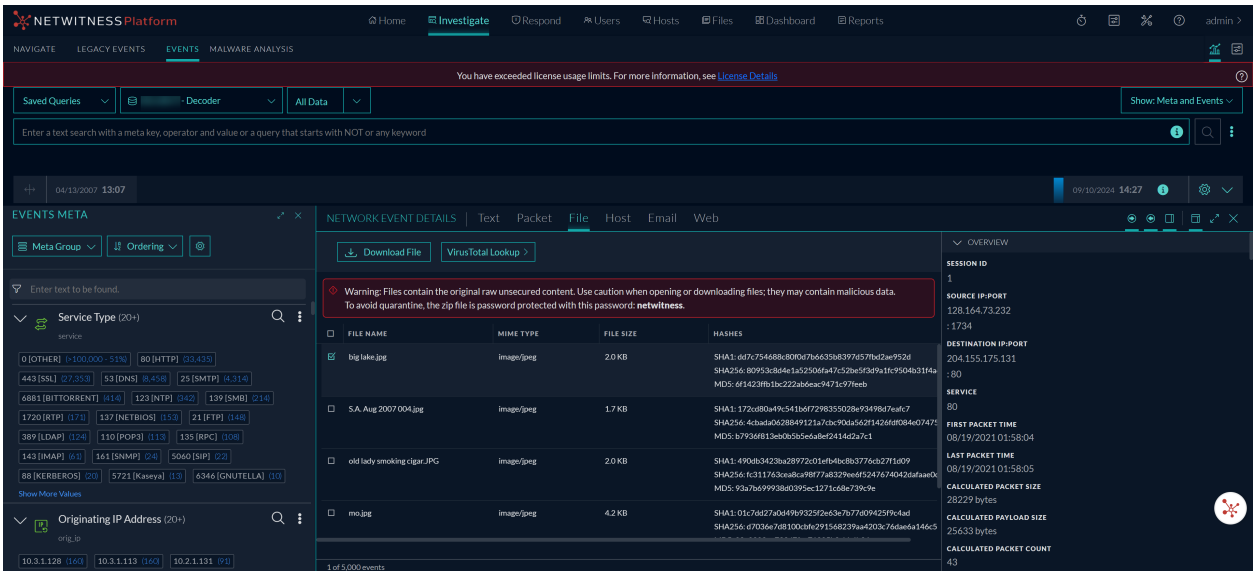
指定した形式でネットワーク データ ファイルがローカル ファイル システムにダウンロードされるか、指定された形式でイベントのメタデータがダウンロードされます。

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。



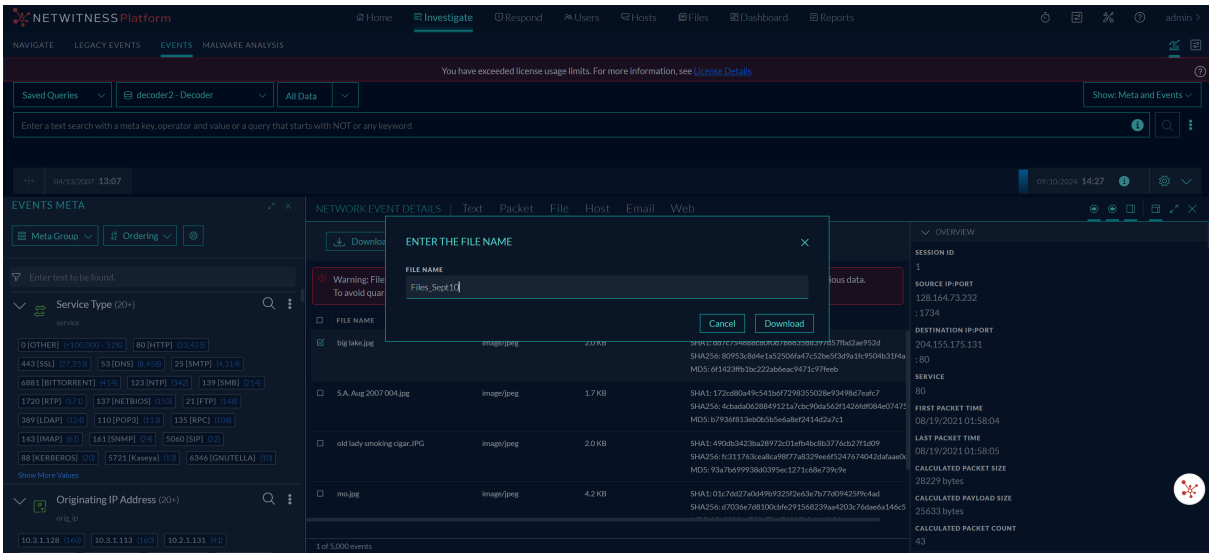
［ファイルのダウンロード］をクリックすると、選択したファイルがパスワード保護されたzipアーカイブとしてエクスポートされます。エクスポートされたアーカイブを開くためのパスワードは`netwitness`です。この形式でファイルをエクスポートすることにより、次のことが保証されます。

- 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。

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

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。
2. 抽出する1個または複数のファイルをクリックし、［**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。
3. ファイル名を入力するためのダイアログボックスが表示されます。デフォルトでは、ファイル名は最初に次の形式でタイムスタンプとともに表示されます。`investigation-yyyy-mmm-dd-hh-mm-ss`(例: **investigation-2024-Sep-10-20-00-37**)。必須のファイル名を入力し、［**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アーカイブの形式でローカル ファイル システムにダウンロードされます。

4. 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電子メールの再構築を表示する場合、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`

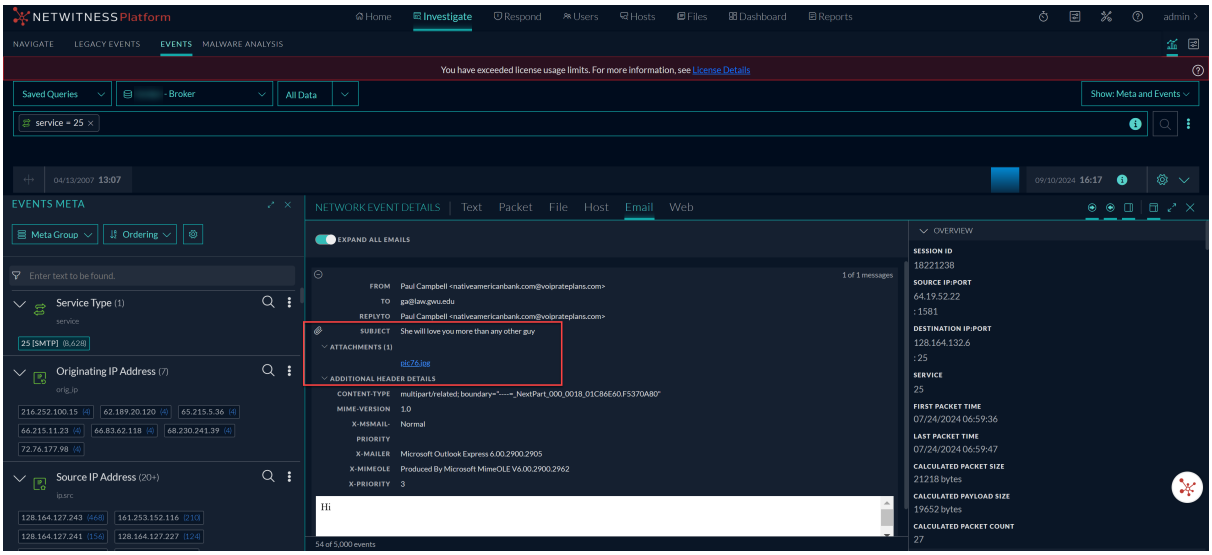
各項目の意味は次のとおりです。

- `<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。

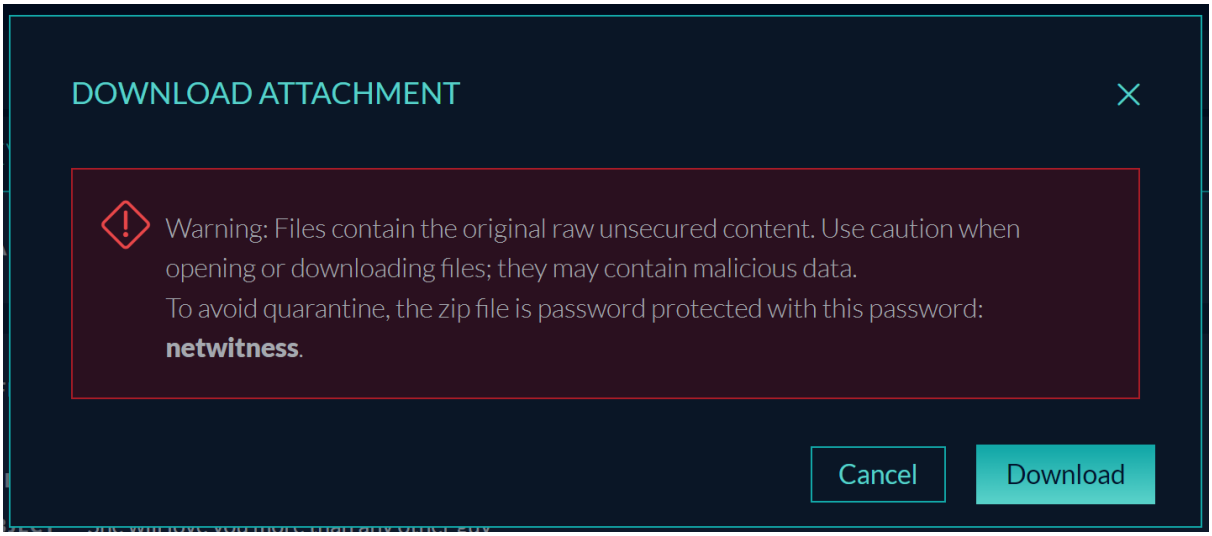
注意：デフォルトのアプリケーションに関連づけられているファイルを解凍または開くときは、十分に注意してください。たとえば、Excelスプレッドシートは、ファイルの安全性を検証する前にExcelで自動的に開かれる可能性があります。

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 リストを展開します。
3. 添付ファイルへのリンクをクリックします。



ダウンロードした電子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、ダウンロードをキャンセルするか確認するかが求められます。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**]クリックしてダウンロードをキャンセルします。



[ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷

NetWitness Investigationでは、[ナビゲート]ビューにドリルダウン ポイントのデータが表示されている場合、次のタスクを実行できます。

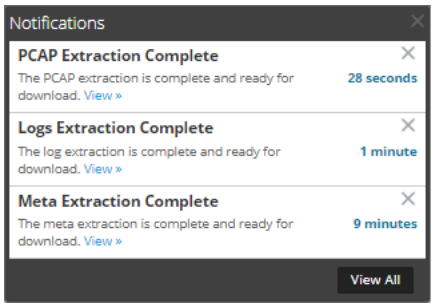
- セッションからファイルを抽出します。抽出するファイルのタイプを選択します。(アーカイブ、オーディオ BitTorrent、ドキュメント、実行可能プログラム、イメージ、その他、ビデオ、Web) が指定できます。
- ドリルダウン ポイントをパケット キャプチャ(PCAP) ファイル、ログ ファイル、メタデータ ファイルとしてエクスポートします。
- ドリルダウン ポイントを印刷します。

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のセッションがあるが、ログ セッションは5つのみである場合は、ジョブのキューのメッセージに、505のセッションに対して5つのログをNetWitnessが抽出していることが示されます。

[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

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. ツールバーで、**「イベントを保存」**> を選択し、次のいずれかのエクスポート オプションを選択します。[**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。
3. 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**]。
4. 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。



5. ジョブトレイで［**表示**］リンクをクリックし、リクエストしたそれぞれの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

［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。

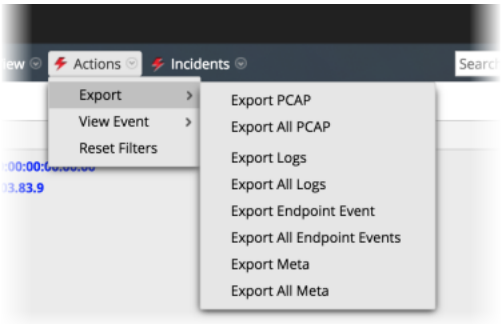
エクスポート機能では、サービスのクエリを実行し、選択した時間範囲とドリルダウン ポイントで指定したセッションをPCAPファイルにエクスポートします。エクスポートされる内容は、エクスポートするときの時間範囲やドリルダウン ポイントによって変わります。 [ファイルの抽出]ダイアログでは、次の項目を選択してエクスポートできます。

- 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

1. [**イベント**]**ビュー**でイベントをクリックします。
2. クリックしてく **アクション** > **エクスポー**.



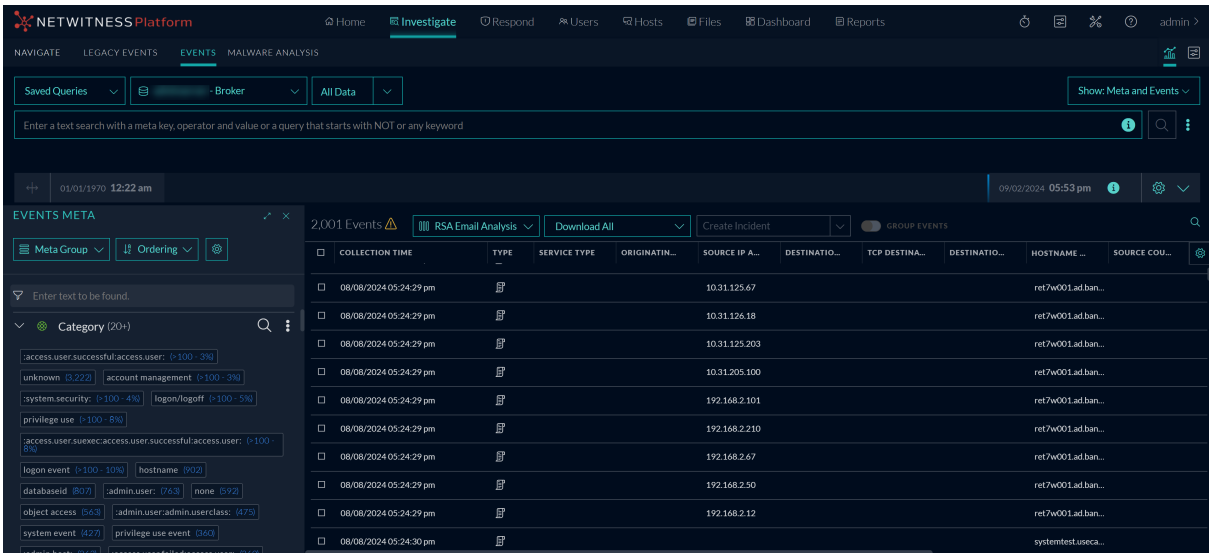
3. エクスポート オプションを選択します。
   PCAPがダウンロード中であることを示すメッセージが表示されます。

[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。

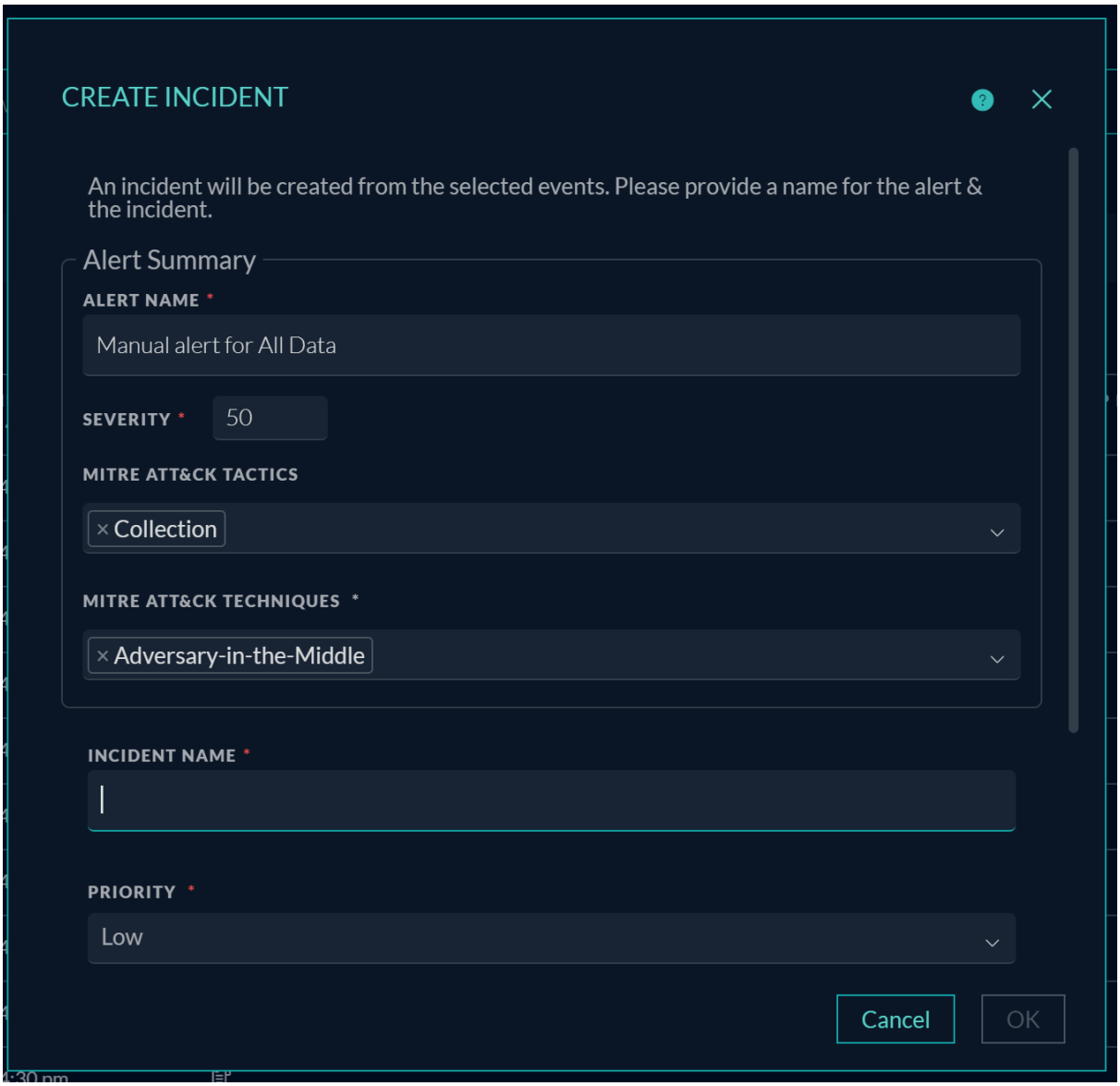
注：管理者が`respond-server.incident.manage`および`investigate-server.incident.manage`のロールと権限を構成する必要があります。詳細については、『システム*セキュリティとユーザ管理ガイド*』の「ロールの権限」と「ロールと権限によるユーザの管理」を参照してください。

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。



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. [**MITRE ATT&CK戦術**]ドロップダウン リストから戦術を選択します。戦術を選択すると、適切なテクニックとサブテクニックを選択するオプションが表示されます。

c. [**MITRE ATT&CKテクニック**]ドロップダウン リストからテクニックとサブテクニックを選択します。

d. [**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。

e. [**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。

f. 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、Investigate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。

g. [カテゴリー]ドロップダウン リストから、このインシデントに適用するイベントのカテゴリーを1つ以上選択します。

h. [**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。

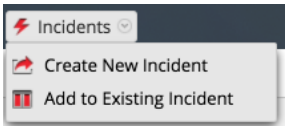
5. [インシデントに追加]ダイアログで、アラート サマリーと重大度を選択し、インシデントの追加先にする1つ以上の既存の未解決インシデントを選択します。既存のインシデントは、インシデントIDまたはインシデント名で検索できます。準備ができたら、[**OK**]をクリックします。選択したインシデントにイベントが追加され、Respondで更新されます。

[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

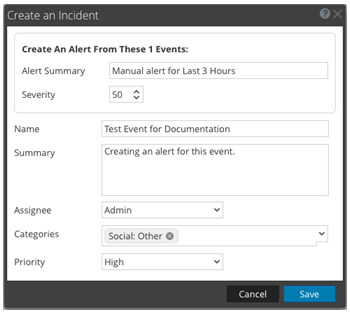
レガシー イベントで調査を行うときに、1つ以上のイベントを選択して、インシデント対応者がRespondで利用可能なインシデントを作成できます。アクセス制限が有効になっている場合、インシデントの作成時に表示できるのは、自分がアクセス権を持っているインシデントのみです。たとえば、[調査]ビューからインシデントを作成する場合、アナリストはインシデントを自分に割り当てて、それらを[対応]ビューに表示する必要があります。また、アクセス権のある既存のRespondのインシデントにイベントを追加することもできます。

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]**.
2. [レガシー イベント]ビューで、1つ以上のイベントを選択してから、**[インシデント]** > **[新しいインシデントの作成]**を選択します。



3. [インシデントの作成]ダイアログに情報を入力します。



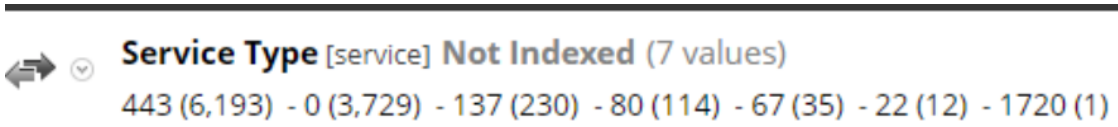
   a. 重大度を選択します。重大度は1～100の整数で、100が最も重大です。
   b. インシデントの名前を入力し、**[サマリ]**フィールドでインシデントについて説明します。
   c. インシデントの割り当て先をドロップダウン リストから選択します。このリストには、Respondにアクセスできる組み込みのロールと、システムに追加されたカスタム ロールが含まれます。たとえば、このリストには、管理者、アナリスト、DPO、オペレーターのロールや、インシデント対応担当者のロールが含まれている場合があります。
   d. **[カテゴリー]**ドロップダウン リストから、このインシデントに適用す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を選択します。たとえば、インシデントはクリティカル、高、中、低の優先度の場合があります。
   f. **[保存]**をクリックします。
   新しいインシデントが作成され、Respondの選択されたロールのインシデント キューですぐに利用できるようになります。

4. 1つ以上のイベントをインシデントに追加するには、1つ以上のイベントを選択してから、［**インシデント**］> ［**既存のインシデントへの追加**］を選択します。
5. ［イベントをインシデントに追加］ダイアログで、重大度を選択し、イベントが追加される1つ以上のインシデントを選択します。インシデントIDまたはインシデント名で既存のインシデントを検索できます。準備ができたら、［**インシデントへの追加**］をクリックします。
   選択したインシデントにイベントが追加され、Respondで更新されます。

NetWitness Investigateのトラブルシューティング

このセクションでは、NetWitness Investigateの使用時に発生する可能性のある問題について説明します。

[ナビゲート]ビューおよび [レガシー イベント]ビューの問題

動作	通常は [ナビゲート]ビューに値を返すメタ キーが値を返しますが、メタ キー名の後にNot Indexedメッセージがあります。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. 
問題	環境を初めてセットアップしたとき、または、稀にですが他の問題が原因でBrokerでデータ リセットを実行したときに、メタ キーがメタ キー レベルまたはメタ値レベルでインデックスされているにもかかわらず、インデックスなしと表示されます。
説明	Brokerの問題を解決するには、NetWitness Platformからログアウトして、もう一度ログインします。有効なセッションが表示されます。

メッセージ	Not indexed; will experience longer than usual load times.([メタ グループの管理]ダイアログ)
問題	[メタ グループの管理]ダイアログボックスのメタ キーが赤い感嘆符でマークされ、エラー メッセージが表示されます。これは、BrokerまたはDecoderを調査していて、サービスのインデックス ファイルまたはカスタム インデックス ファイルでインデックスされていないメタ キーを含むメタ グループを追加するときに発生する可能性があります。 Brokerの場合、それはBrokerがConcentratorからデータを集約し始めていないことを意味する可能性があります。この場合、Brokerは、集約サービスからのカスタム索引ファイルのコンテンツを持たず、キーは索引付けされません。 Decoderの場合、メタ キーがDecoderインデックスまたはカスタム インデックス ファイルでインデックスされていないことを意味します。
説明	Brokerで問題を解決するには、Brokerサービスからログアウトして、ログインし、再始動します。これで、接続されたConcentratorからメタ キー情報を集約できるようになります。Decoderの問題を修正するには、カスタム インデックス ファイルを編集してメタ キーのインデックスを作成し、Decoderサービスからログアウトして、ログインし、再起動します。

動作	[イベントの再構築]ビューからログおよびメタデータをダウンロードすると、[レガシー イベント]ビューで選択した形式に関係なく常にテキスト形式になります。
問題	[イベントの再構築]ビューでメタデータまたはログをダウンロードすると、[レガシー イベント]ビューで選択した形式が使用されません。エクスポートしたデータは、常にテキスト形式になります。
説明	テキスト形式以外の形式を使用する場合は、[レガシー イベント]ビューからメタデータとログをダウンロードします。

[イベント]ビューの問題

動作	ソフトウェアを最新バージョンにアップグレード中およびアップグレード後、ダウンロード ジョブはジョブ 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 メタ パネルとイベント パネルのイベント数が異なる場合があります。
問題	イベント メタ パネルでは、インデックス データのみを使用してイベントの数を生成するため、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 メタ]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	`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。

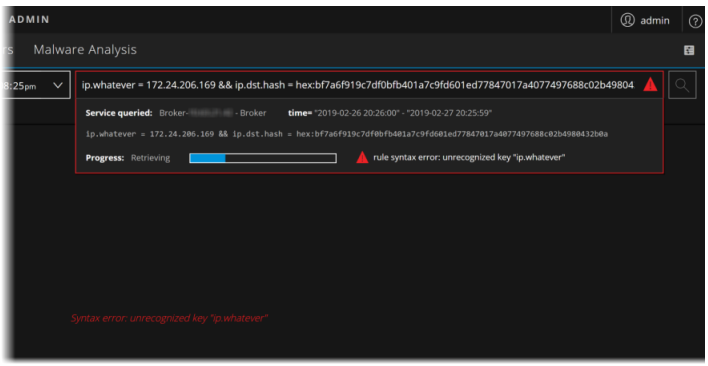
メッセージ	`Insufficient permissions for the requested data.`
問題	[イベント]ビューでイベントにアクセスしようとすると、このメッセージが表示されます。
説明	表示する権限がないイベントのイベントIDを入力しました。アクセスを制限するために、管理者がロールと権限により制限を設けた可能性があります。

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。

メッセージ	`Memory limit of <XXXXXX> GB reached, controlled by setting max.query.memory`
問題	結果セットが大きすぎて、`max.query.memory`で設定されたメモリ制限に達したため、送信したクエリが失敗しました。
説明	このエラーを回避するには、時間範囲の絞り込み、フィルタの追加、列グループの列数の削減によって、さらに結果を絞り込むようにします。また、返されるイベントの数を制限することを管理者に対して要求することもできます。

動作	コンテンツの再構築ではテキスト データは生成されませんでした。イベント データが破損しているか不正な可能性があります。または、管理者がEndpoint Serverの構成でエンドポイントのRAWイベントの送信を無効化している可能性があります。他の表示で再構築してください。
問題	[イベント]ビューでイベントをテキストとして再構築するとき、データが表示されず、このメッセージが表示されます。

説明	他の［イベント］ビューや［レガシー イベント］ビューの再構築でもRAWテキストが表示されず、データが破損していない、または無効でないと思われる場合、管理者がNetWitness Endpointサーバでエンドポイント イベントの送信を無効化した可能性があります。詳しくは、管理者にお問い合わせください。

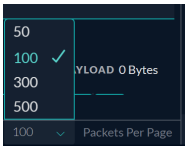
メッセージ	`Rule Syntax error: Unrecognized key "<meta key or meta entity name>"` `Syntax error: Unrecognized key "<meta key or meta entity name>"`
問題	サービスのクエリ中、一致するイベントが表示されず、メッセージがクエリ コンソールと［イベント］ビューに表示されます。 
説明	入力したクエリは、正しく構成されていないメタ エンティティに対して実行されています。クエリ対象のBrokerに接続されているすべての上流デバイスに、同じエンティティ構成がなければなりません。このエラーは、エンティティ定義に不一致がある状態でBrokerが動作していることを示しています。『*Core*データベース チューニング ガイド』の「インデックスのカスタマイズ」で説明されている構成を確認するよう、管理者に依頼してください。

メッセージ	`Session is unavailable for viewing.`
問題	イベントIDでクエリを実行した時に、イベントの再構築が表示されず、このメッセージが表示されます。
説明	入力したクエリは、制限されたデータを照会しようとしています。たとえば、ログ データの表示しか許可されていないときに、ネットワーク データへのリンクを使用しています。

メッセージ	`The query on channel <channel-number> was auto-canceled by the system for exceeding time usage limits. Check timeout values. Query running time was 00:05:00 (HH:MM:SS)`
問題	このタイムアウト メッセージが頻繁に表示される場合は、まずクエリ コンソールを確認して、サービスの応答に要する時間の問題やインデックス エラー メッセージなど、クエリのレスポンス タイムを増やすために対処すべき警告があるかどうかを調べます。
説明	特定の警告を示すメッセージが表示されていない場合は、『*システム セキュリティとユーザ管*

	理ガイド』の説明に従って、コア クエリ タイムアウトを5分から10分に増やすよう管理者に依頼してください。

メッセージ	`The session id is too large to be handled:<<eventId>`
問題	[レガシー イベント]ビューまたは [ナビゲート]ビューで入力または取得したセッションIDが大きすぎます。
説明	[イベント]ビューでsessionIdを手動で入力したか、sessionIdを編集した場合、[イベント]ビューで処理するには大きすぎる整数値を指定した可能性があります。

動作	[イベント]ビュー> [パケット]パネルで大量のパケット(250個超)を使用してネットワーク イベントを再構築するときに、有効なペイロードのみを表示するオプションが有効になっており、ページあたりのパケット数の設定がデフォルト値(100個)を上回った場合、現在のブラウザ タブがペイロードの表示を処理している間、最大45秒間応答しません。
問題	クライアント マシンのリソース(メモリとCPU)の量とイベントのパケット数によっては、パケットの再構築でペイロードのみを表示すると、パフォーマンスが低下する場合があります。
説明	単一のイベントの再構築で処理されるデータの量を制限するには、フッターの [ページあたりのパケット数]設定を低い値に変更します。 

動作	イベント ビューで作業している場合、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 メニューは機能しません。
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。
説明	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「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、『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。

イベント レポートの問題を調査する

Reporting Engineサービスが利用できない

メッセージ	レポートの生成中に次のエラー メッセージが表示されます。`The Reporting Engine service may be offline or inaccessible. Try starting the service.`
問題	このシナリオは、次の理由によりReporting Engineサービスがオフラインになった場合、またはアクセスできなくなった場合に発生します。 • 管理者がサービスを停止した可能性がある。 • サービスがインストールされているサーバーにアクセスできない。 **注 :**サービスがオフラインの場合は、インジケーター(赤い丸) で示されます。
説明	この問題を解決するには、次のアクションを実行する必要があります。 1.  (管理) > ［**サービス**］に移動します。 2. ［**サービス**］リストで、Reporting Engineサービスを選択します。 3.  > ［**開始**］をクリックします。

必要な権限がない

メッセージ	レポートの生成中に次のエラー メッセージが表示されます。`You do not have the required permissions to generate a report. Contact your administrator to request access.`
問題	このシナリオは、アナリストが必要な権限を持たずにレポートを作成またはスケジュール設定しようとすると発生します。 **注 :**デフォルトでは、管理者のみがアクセスできます。
説明	この問題を解決するには、アナリストが管理者に連絡してアクセス権限をリクエストする必要があります。権限が付与されると、アナリストは後でレポートの生成を試行できるようになります。詳細については、「*NetWitness Reporting構成ガイド*」の「データ ソースの権限の構成」を参照してください。

サポートされていないカスタムの列

メッセージ	レポートの生成中に次のエラー メッセージが表示されます。`The following custom columns are not supported to generate a report. Remove them and try again.` • `<column name 1>` • `<column name 2>`
問題	このシナリオは、 **調査**] > [**イベント**]ページでレポートを生成するためのカスタム列がReporting Engineサービスによってサポートされていないことが理由で発生します。
説明	リストからカスタム列を削除するには、次のアクションを実行します。 1. [**イベント**]ビューで **設定**]アイコン( ) をクリックします。 利用可能なカスタム列のリストがポップアップ ウィンドウに表示されます。 2. サポートされていないカスタム列をリストから選択解除し、新しいレポートを生成してみてください。

データソースが構成されていないか利用不可

メッセージ	レポートの生成中に次のエラー メッセージが表示されます。`The datasource <service name> is not configured in the Reporting Engine. Add the datasource and try again.`
問題	このシナリオは、Reporting Engineで構成されていないデータソースを選択した場合に発生します。 **注 :** 調査]ページのデータソースの名前がReportingページの名前と異なる場合は、エラー メッセージが表示されます。
説明	この問題を修正するには、次の手順を実行します。

1.  (管理)> [**サービス**]に移動します。
2. [**サービス**]リストで、Reporting Engineサービスを選択します。
3.  > [**表示**]> [**構成**]をクリックします。
   Reporting Engineの [サービス]の [構成]ビューが表示されます。
4. [**ソース**]タブを選択します。
5.  をクリックし、 [**使用可能なサービス**]を選択します。
   [使用可能なサービス]ダイアログが表示されます。
6. 必要なサービス(Log Decoderなど) を選択して、 [**OK**]をクリックします。
   [サービス認証]ダイアログ ボックスが表示されます。

   注 :信頼モデルが有効化されたサービスは個別に追加する必要があります。選択したサービスに対するユーザ名とパスワードを入力するプロンプトが表示されます。
7. サービスのユーザー名とパスワードを入力します。
8. [**OK**]をクリックします。
   選択したサービスが [サービスの集計]パネルに追加されます。

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。

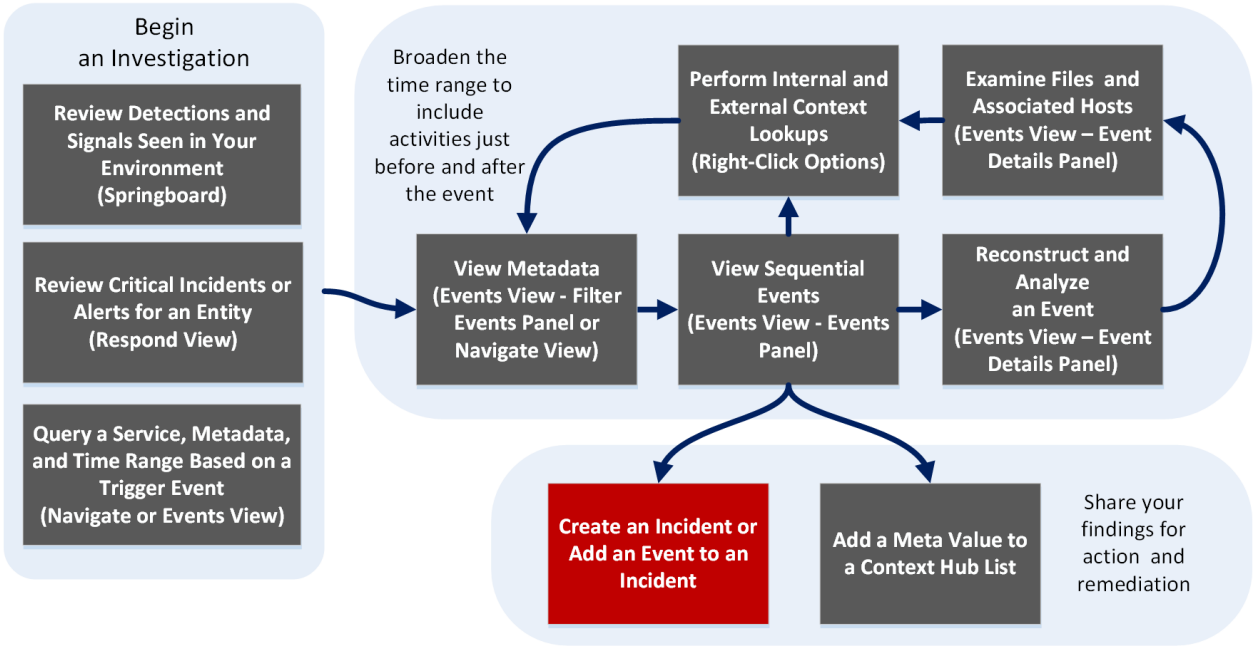
- [調査]ビュー
- [ナビゲート]ビュー
- [レガシー イベント]ビュー
- [イベント]ビュー
- [リストへの追加/削除]ダイアログ
- [イベントをインシデントに追加]ダイアログ
- [列グループ]ダイアログ
- [コンテキスト ルックアップ]パネル
- [インシデントの作成]ダイアログ
- [イベント]ビュー - [メール]タブ
- [イベント]ビュー - [テキスト]タブ
- [イベント]ビュー - [パケット]タブ
- [イベント]ビュー - [ファイル]タブ
- [調査]ダイアログ
- [調査]タブ - [ユーザー環境設定]パネル
- [レガシー イベントの再構築]ビュー
- [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
- [保存済みクエリ]ダイアログ
- [スプリングボード パネルの作成]ダイアログ
- [将来のアラートを作成]ダイアログ
- [イベント]ビューの [レポートのスケジュール設定]ダイアログ
- [イベント]ビューの [チャートの作成]ダイアログ
- [タイムライン設定]パネル

- 「検索パターンの作成」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	*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 イベントビューでメタデータのドリルダウン
脅威ハンター	シーケンシャル イベントの表示	[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

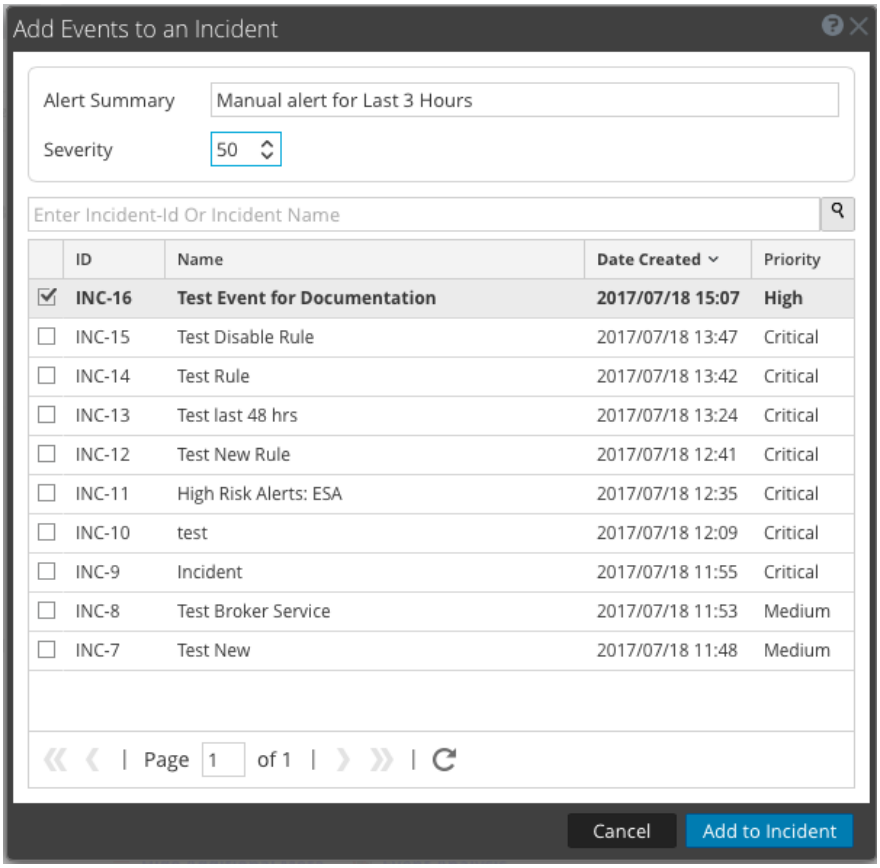
*このタスクは現在のビューで実行できます。

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

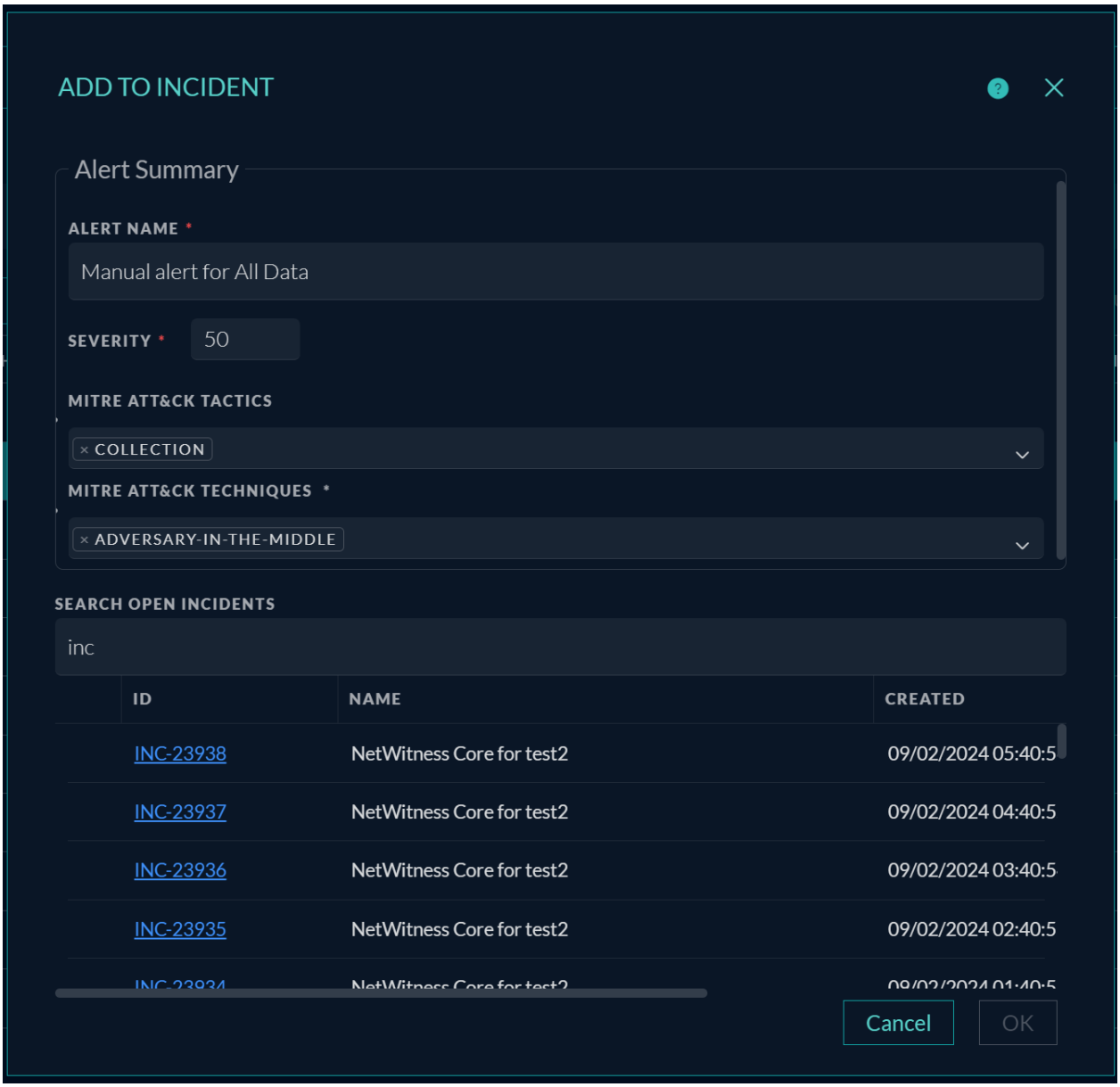
次の図は、レガシー イベントの［イベントをインシデントに追加］ダイアログの例です。表に、［イベントをインシデントに追加］ダイアログの情報およびオプションについて説明します。



機能	説明
アラート サマリ	［アラート サマリ］フィールドには、アラートを選択した時のクエリが自動入力されます。これは、このインシデントを作成する時に選択されていたクエリです。 ［重大度］フィールドには、選択したアラートの重大度として、1~100の整数が示されます。
検索	既存のインシデントを検索できます。
ID	インシデントのID。IDは昇順または降順にソートできます。
名前	インシデント名。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の整数が示されます。
MITRE ATT&CK戦術	インシデントに関連する戦術のタイプを表示します。 例 :**クレデンシャル アクセス**。 クレデンシャル アクセス戦術は、アカウント名とパスワードを盗もうとします。
MITRE ATT&CKテクニック	戦術に関連付けられたテクニックとサブテクニックの種類が表示されます。
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。
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

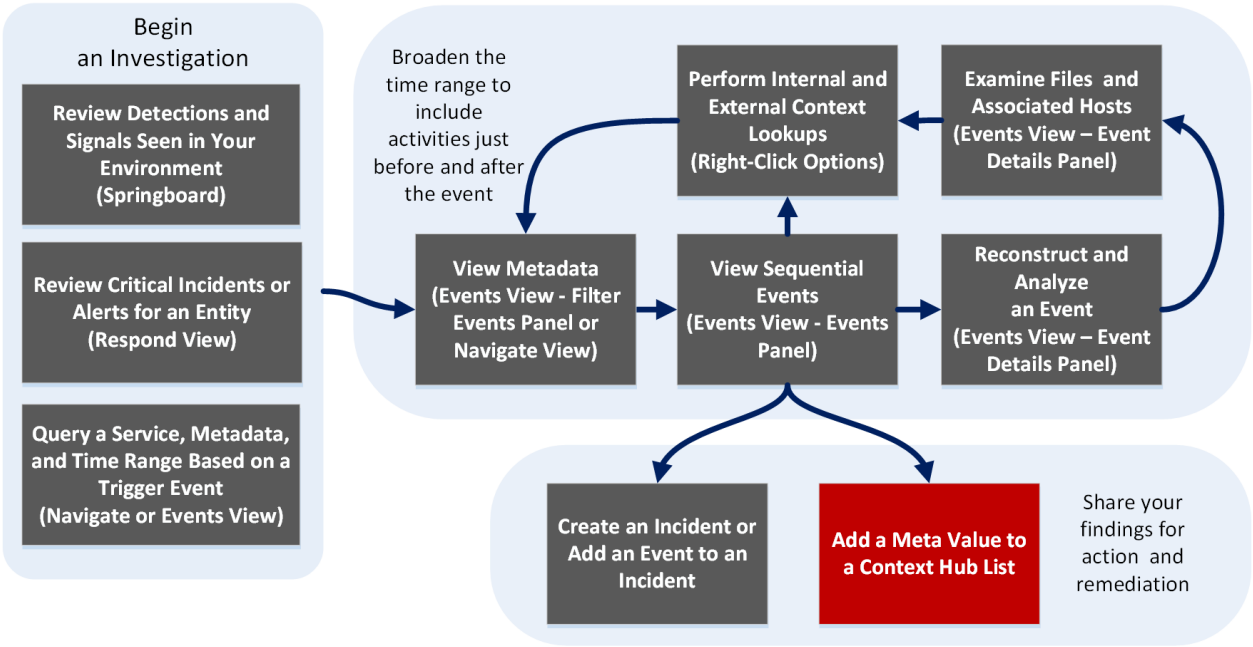
[リストへの追加/削除]ダイアログを使用すると、既存のContext Hubリストに対してエンティティもしくはメタ値を追加し、エンティティもしくはメタ値を削除し、またはエンティティもしくはメタ値を含む新しいContext Hubリストを作成できます。疑わしいIPアドレスや注意が必要なIPアドレスやその他のエンティティを見つけたときは、データ ソースとして追加されているリストにそのIPアドレスを追加できます。一般的に使用されるリストには、ホワイト リストやブラック リストがあります。これにより、疑わしいIPアドレスの可視性が向上し、誤検知が減るため、余計な調査の必要がなくなります。

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	*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 イベントビューでメタデータのドリルダウン
脅威ハンター	シーケンシャル イベントの表示	[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

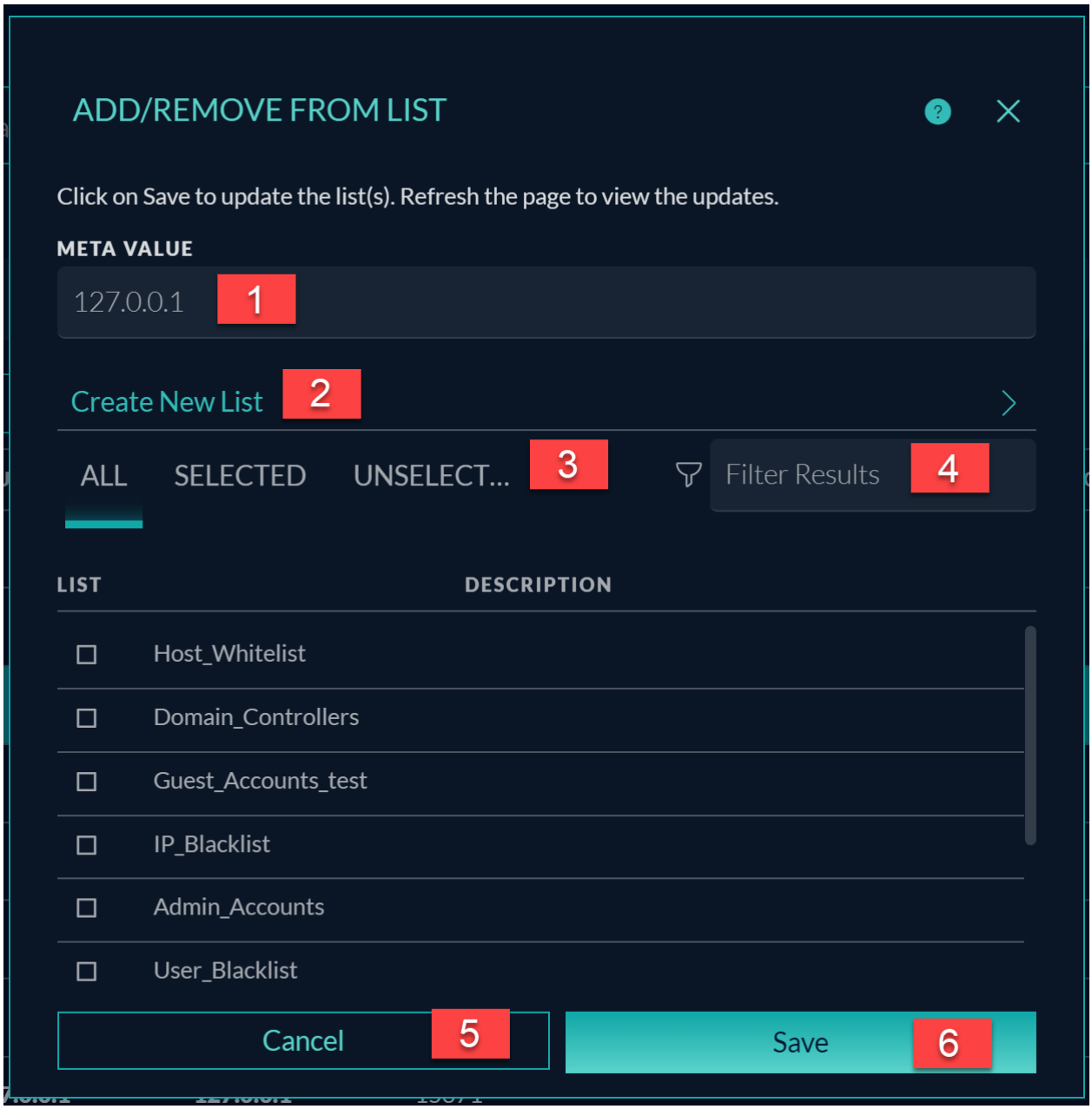
*このタスクは現在のビューで実行できます。

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。



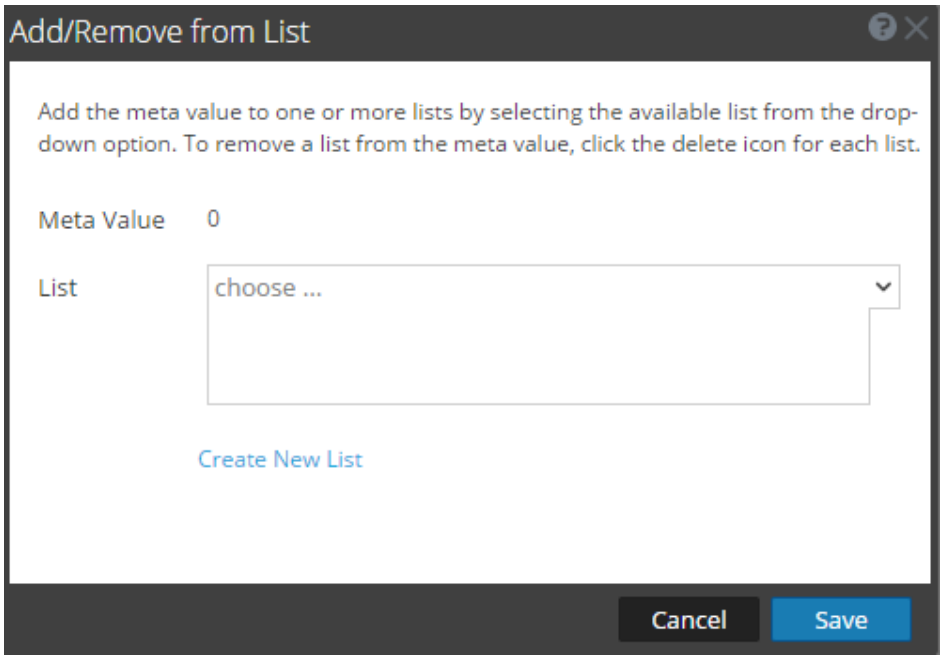
1 追加または削除するエンティティまたはメタ値。
2 選択したメタを使用して新しいリストを作成します。
3 任意のタブを選択します。 [すべて]、 [選択済み]、 [未選択]のいずれかです。
4 リストの名前または説明を使用して検索します。
5 アクションをキャンセルします。
6 保存してリストを更新するか、新しいリストを作成します。

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。

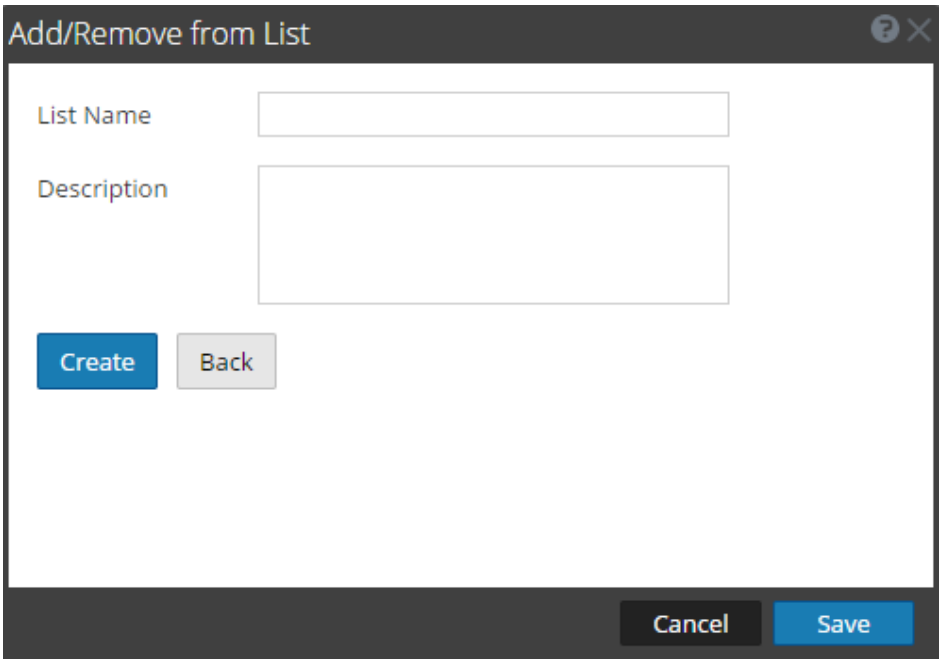
オプション	説明
メタ値	1つまたは複数のリストに追加、またはリストから削除する必要がある選択したエンティティまたはメタ値が表示されます。選択した値を使用して新しいリストを作成することもできます。
新しいリストの作成	選択されたメタ値を使用して新しいリストを作成するダイアログが表示されます。
すべて	使用できるContext Hubリストがすべて表示されます。選択したエンティティまたはメタ値を追加するリストを選択できます。リストにエンティティまたはメタ値を追加するには、チェックボックスを選択します。リストから削除するには、チェックボックスをオフにします。
選択済み	選択したエンティティまたはメ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。)
オフ	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。
リスト	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

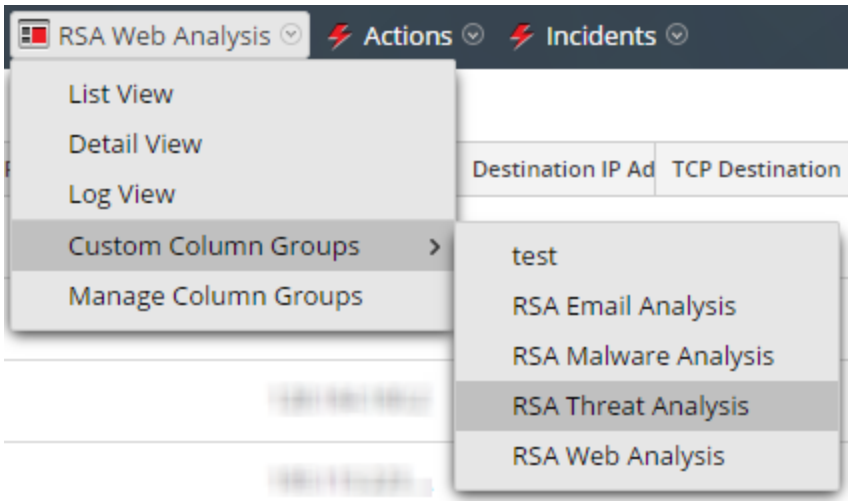
機能	説明
メタ値	既存のリストまたは新しいリストに追加される選択したメタ値。
リスト	選択したメタ値を追加するリスト。ドロップダウン メニューには、メタ値を追加できるリストが示されます。
新しいリストの作成	選択したメタ値を追加する新しいリストを作成するダイアログが開きます。
リスト名	新しいリストの名前。
説明	新しいリストの説明。
作成	必須入力フィールドを入力した後に新しいリストを作成します。
戻る	新しいリストの作成をキャンセルし、元のダイアログに戻ります。
キャンセル	リストへのメタ値の追加をキャンセルし、ダイアログ ボックスを閉じます。
保存	リストに加えた変更を保存し、ダイアロ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

[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。[NetWitness Email Analysis]リストには、E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「NetWitness」で始まり、複製できますが、編集することも削除することもできません。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イベント ビューの下にあります。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イベント ビューの下にあります。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 ビュー用です。[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。



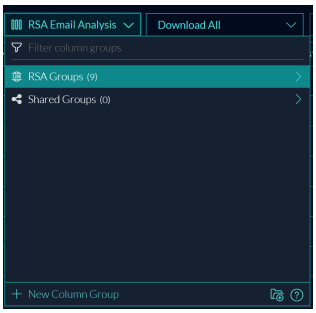
列グループを定義したら、調査の他のビューでも使用できます。[ナビゲート]ビューでは、クエリ プロファイルを使用して、プロファイルの適用時に使用する列グループを選択できます。[イベント]ビューと[レガシー イベント]ビューでは、[イベント]パネルに適用する列グループを選択できます。

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

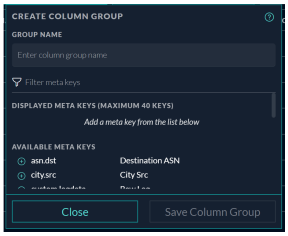
簡単な説明 - [列グループ]メニュー、 [列グループの作成]ダイアログ、 [列グループの詳細]ダイアログ

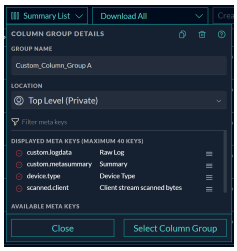
このセクションでは、 [列グループ]メニュー、 [列グループの作成]ダイアログ、 [列グループの詳細]ダイアログについて説明します。次の図は、 [列グループ]メニューの例です。次の表に、オプションの説明を示します。



機能	説明
可視性オプション	表示オプションの任意の組み合わせを使用して、リストに表示される列グループの種類を制御します (青 = 選択、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。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。

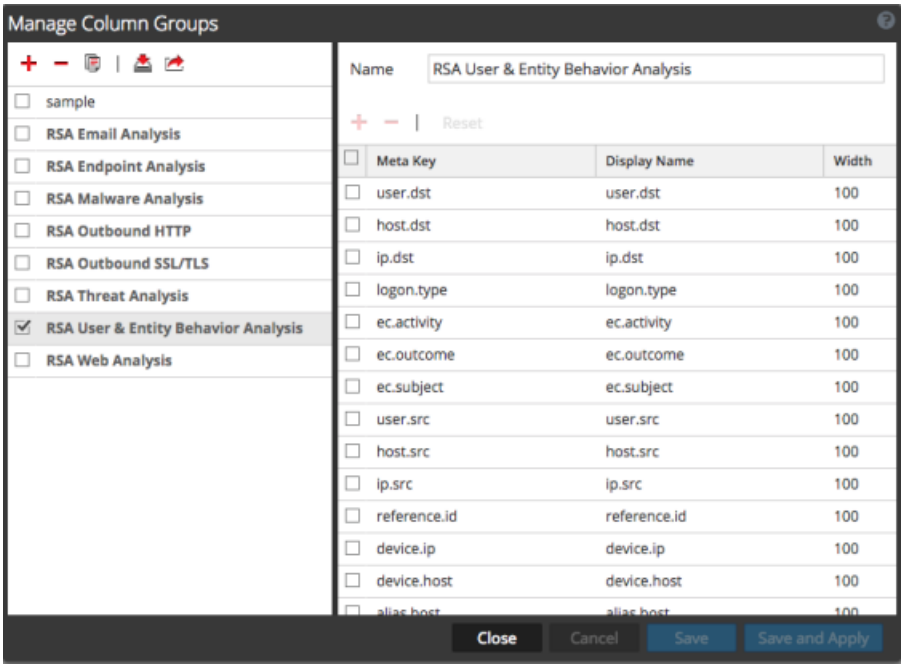




機能	説明
	［列グループの詳細］ダイアログでカスタム列グループを削除します。このアクションは元に戻すことができず、グローバルに適用されます。削除された列グループは、このサービスでこの列グループを使用しているどのユーザからも使用できなくなります。
グループ名	列グループの名前を表示します。64文字以内の一意の名前を指定してください。カスタム列グループの名前を編集する場合は、このフィールドに入力します。
共有	共有またはプライベートの列グループを作成できます。この設定は、初めてグループを作成するときに使用できます。作成後、共有列グループをプライベートに変更したり、プライベート列グループを共有に変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。

機能	説明
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。

アクション	説明
	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

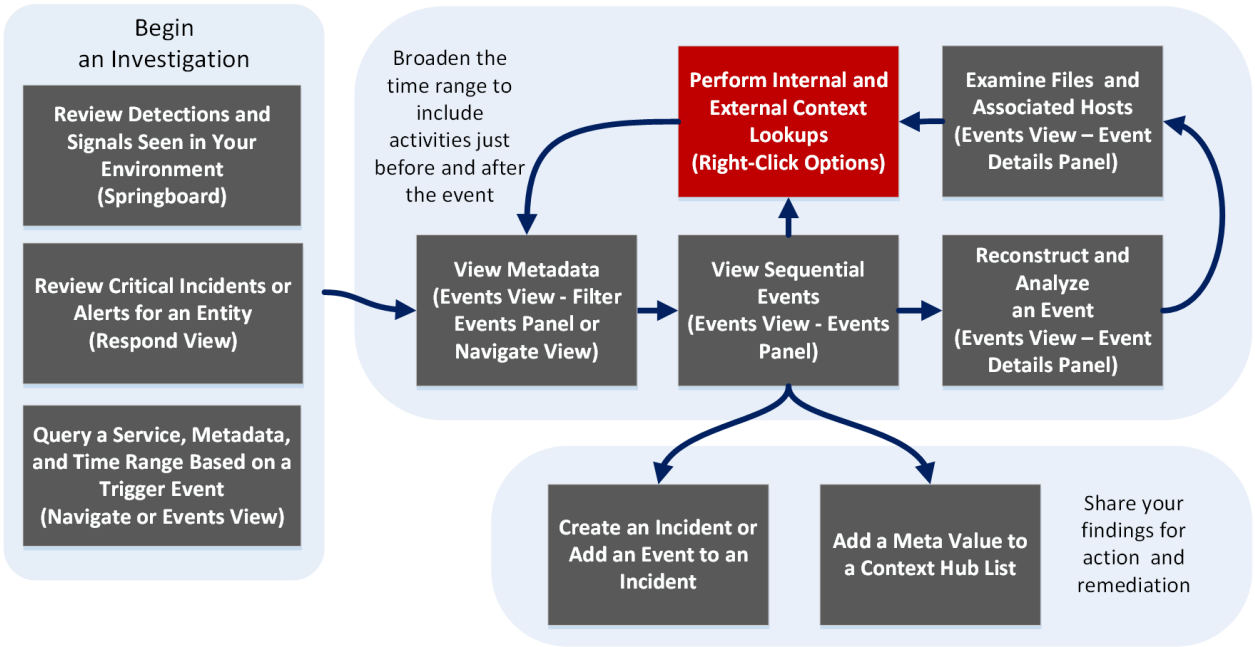
管理者がContext Hubサービスを構成した後、[ナビゲート]ビュー、[レガシー イベント]ビュー、[イベント]ビューに、メタ値に関するコンテキスト情報を表示できます。Context Hubサービスでは、メタ タイプとメタ キーのデフォルトのマッピングが事前に構成されています。Context Hubのメタ値と調査のメタ キーのマッピングの詳細については、『*Context Hub構成ガイド*』の「メタ タイプとメタ キーのマッピングの管理」を参照してください。

[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、白と太字でハイライト表示されます。ハイライト表示されている値を右クリックし、**[コンテキスト ルックアップ]**を選択すると、表示されるコンテキスト メニューで、選択したメタ値の構成済みのソースの[コンテキスト ルックアップ]パネルにルックアップ結果が表示されます。[コンテキスト ルックアップ]パネル アイコン バーでソースを選択すると、コンテキスト情報を表示できます。

「ナビゲート」ビューまたは「イベント」ビューで開いたときと、[イベント]ビューで開たときとでは、[コンテキスト ルックアップ]パネルの外観と内容にいくつかの違いがあります。

注：contexthub-server.contextlookup.read権限は、管理者、アナリスト、マルウェア アナリスト、SOCマネージャー、およびRespond管理者に対してのみ有効です。管理者は、**調査**] > [**イベント**]ビューの他のロールに対してこの権限を有効にすることで、メタ値のコンテキスト検索を表示し、リストへの追加/削除アクションを実行できます。詳細については、『*システム セキュリティとユーザー管理ガイド*』の「ロールの権限」トピック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	*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 イベントビューでメタデータのドリルダウン
脅威ハンター	シーケンシャル イベントの表示	[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

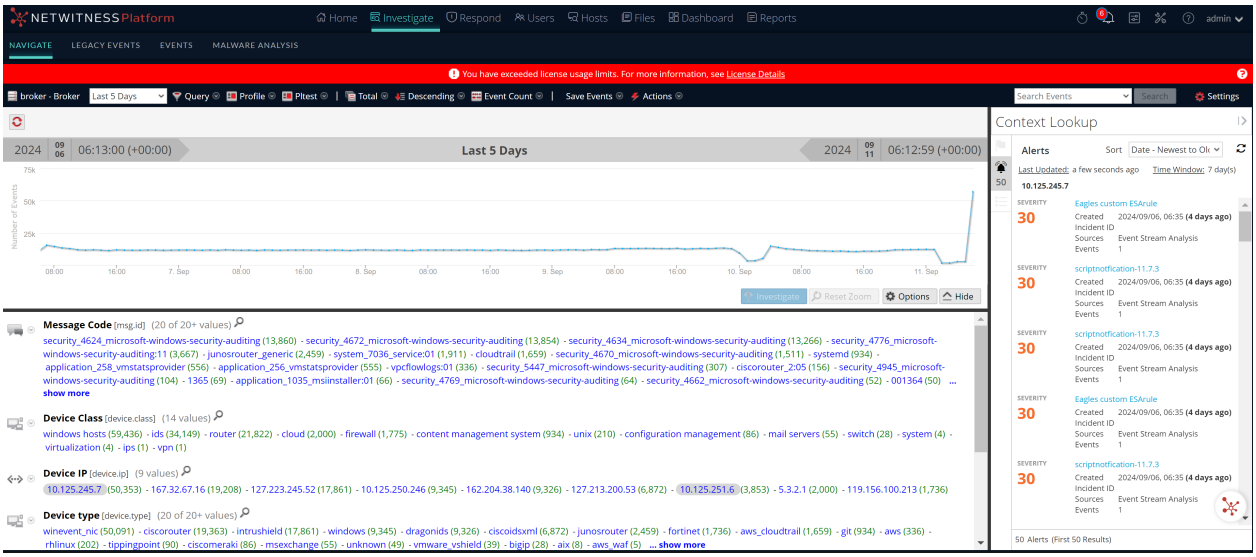
*このタスクは現在のビューで実行できます。

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。 • エンドポイント • インシデント • アラート • リスト
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。

機能	説明
	ルックアップ結果を更新します。
<n件のアイテム>(最初の<n>件の結果)	フッターに現在表示されている結果の件数と結果の総数が表示されます。たとえば、「5件のアラート(最初の50件の結果)」のように表示されます。

インシデント

インシデントは時間順(新しい順)に表示され、さらに優先度のステータスでソートされます。インシデントのルックアップでは、次の情報が表示されます。

- インシデントの名前とID
- インシデントの優先度のステータス
- インシデントのリスク スコアの値
- インシデントが作成された日付
- インシデントのステータス
- インシデントの割り当て先
- 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。

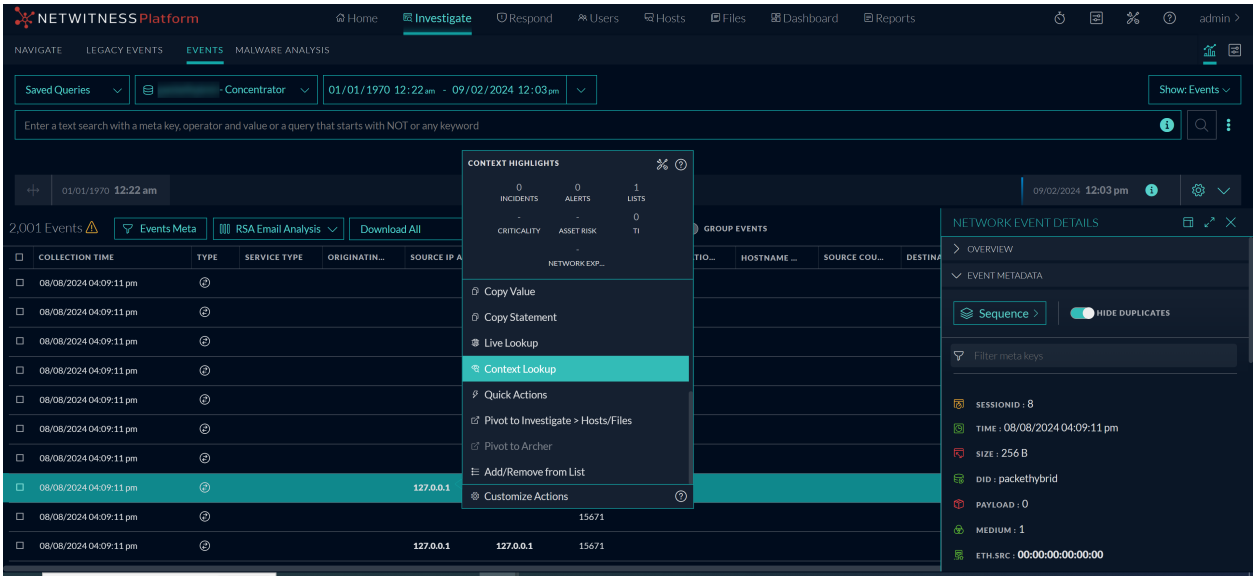
リスト

リストのルックアップでは、次の情報が表示されます。

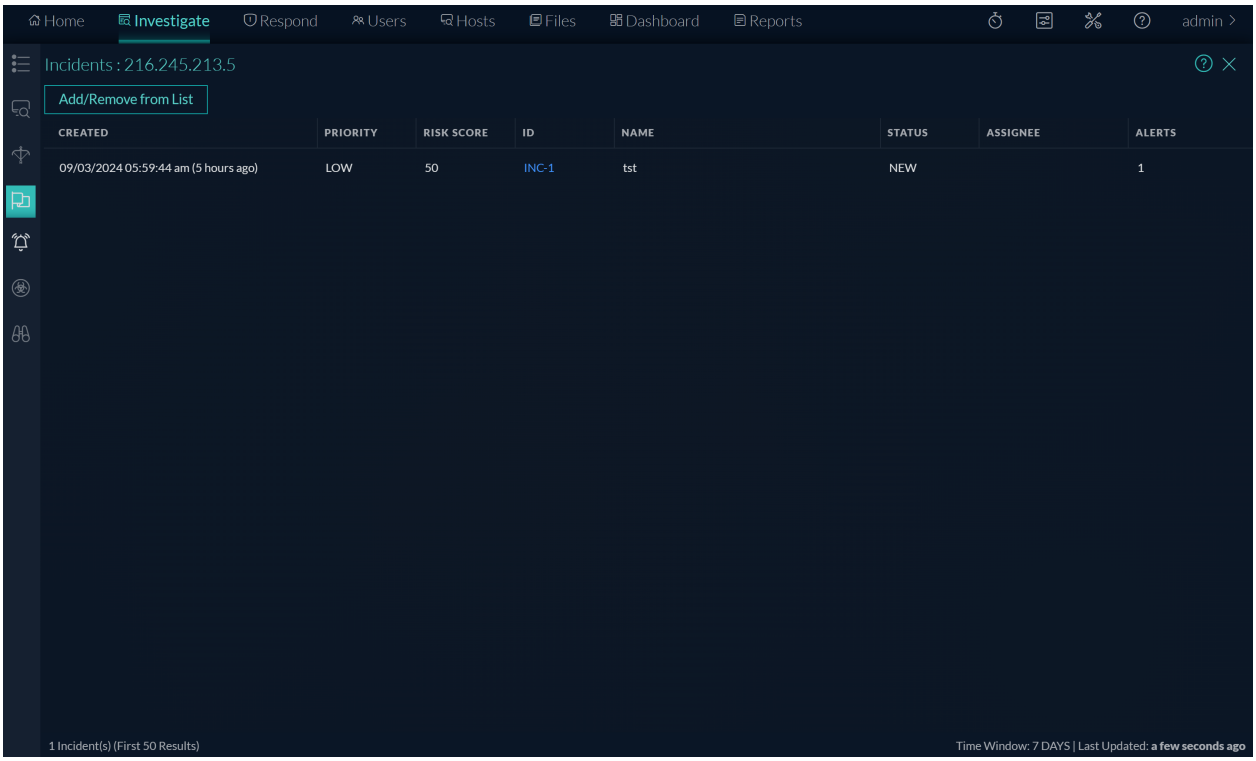
- リスト名(ユーザー定義)
- リストの説明(ユーザー定義)
- ヘッダー
- 値
- リストを作成したオーナー
- 作成日
- 最終更新日

[イベント]ビューの簡単な説明

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。各タブは、 [データ ソースのリスト]、 [Archer]、 [Active Directory]、 [インシデント]、 [アラート]、 [REST API]です。次の図は、 [インシデントの詳細]ビューで選択したエンティティの [コンテキスト ルックアップ]パネルを示しています。



次の表は、各タブおよびサポートされるエンティティで使用可能なデータを示しています。

タブ	説明	サポートされるエンティティ
(リスト)	選択したエンティティまたはメタ値に関連付けられているすべてのリストのデータを表示します。リストの最終更新日時によってソートされます。	すべてのエンティティ
(Archer)	Archerデータ ソースから、重要度評価と資産情報を表示します。	IP、ホスト、MAC
(アクティブディレクトリ)	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
(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
(アラート)	選択したエンティティまたはメタ値に関連付けられているアラートのリストを表示します。最新のアラートから最も古いアラートの順にソートされます。	すべてのエンティティ

タブ	説明	サポートされるエンティティ
(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
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)。
ヘッダー	リストに使用できるメタが表示されます。
値	リスト内の各メタの値が表示されます。
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。
更新日時	リストが最後に更新または変更された日付。
件数	選択したエンティティまたはメタ値が使用可能なリストの数。
タイム ウィンドウ	[レスポンスの構成]ダイアログの[クエリの対象期間]フィールドに設定された値に基づくタイム ウィンドウ。デフォルトでは、[リスト]のすべてのデータがフェッチされます。
最終更新日	Context Hubがルックアップ データをフェッチしてキャッシュに保存した時刻。

[Archer]タブ

[コンテキスト ルックアップ]パネルの[Archer]タブには、IP、ホスト、およびMACのエンティティについて、Archerデータ ソースから取得した重要度評価と資産情報が表示されます。次の図は、[コンテキスト ルックアップ]パネルの[Archer]タブの例です。表には各フィールドの説明が記載されています。

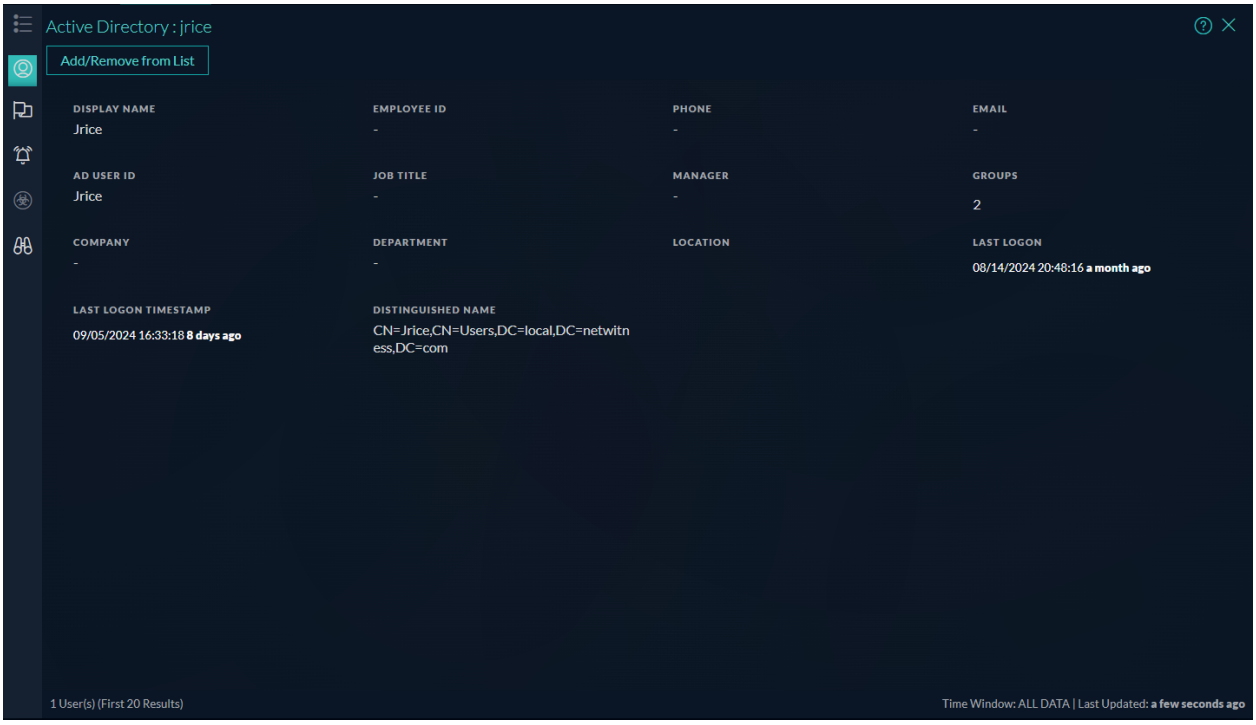


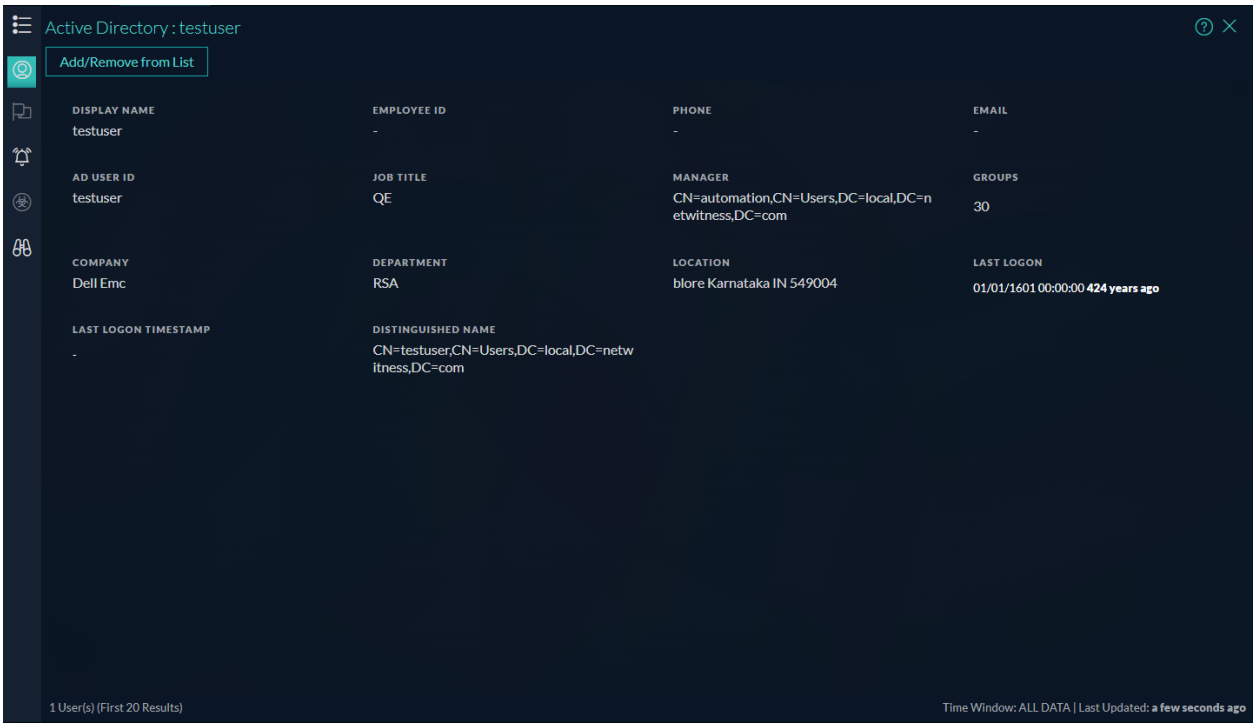
フィールド	説明
重要度評価	デバイスがサポートするアプリケーションに基づいて算出されたデバイスの業務上の重要度。重要度評価は、未評価、低、中-低、中、中-高、高のいずれかに設定できます。
Risk Rating	最新のアセスメント結果と、このデバイスを使用する施設の平均リスク評価から、デバイスのリスク評価を計算します。リスク評価は、重大、高、中、低、軽微のいずれかに設定できます。
デバイス名	デバイスの固有の名前。
ホスト名	デバイスのホスト名。
内部IPアドレス	デバイスのプライマリ内部IPアドレス。
デバイスID	システム内のすべてのアプリケーションにおいてデバイス レコードを一意に識別する、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。
Facility	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、内部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。

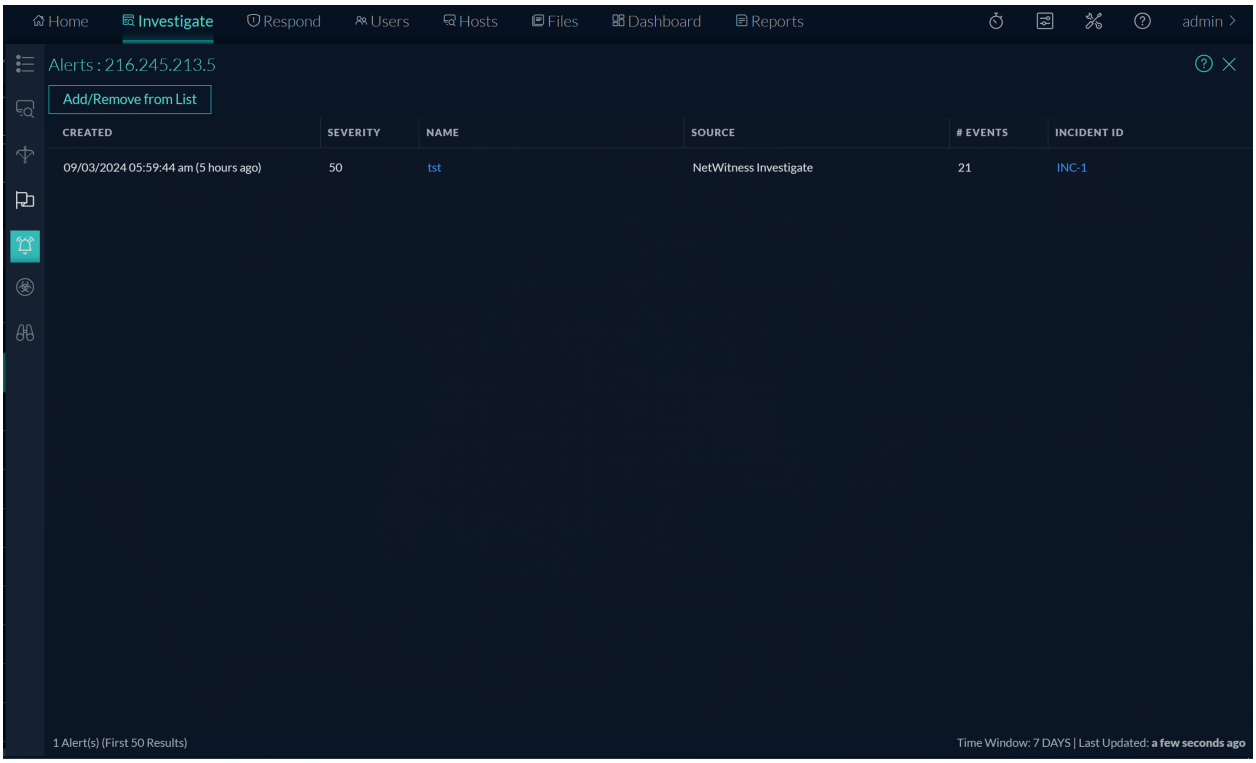
- userPrincipalName
- Domain\UserName
- sAMAccountName

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。
電話	ユーザの電話番号。
メール	ユーザのメールID。
ADユーザID	組織内の特定ユーザの固有ID。
役職	ユーザの役職。
マネージャ	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。

「アラート」タブ

次の図は、最初に時間(新しい順) 次に重大度に基づいて表示された「アラート」の「コンテキスト」パネルの例です。

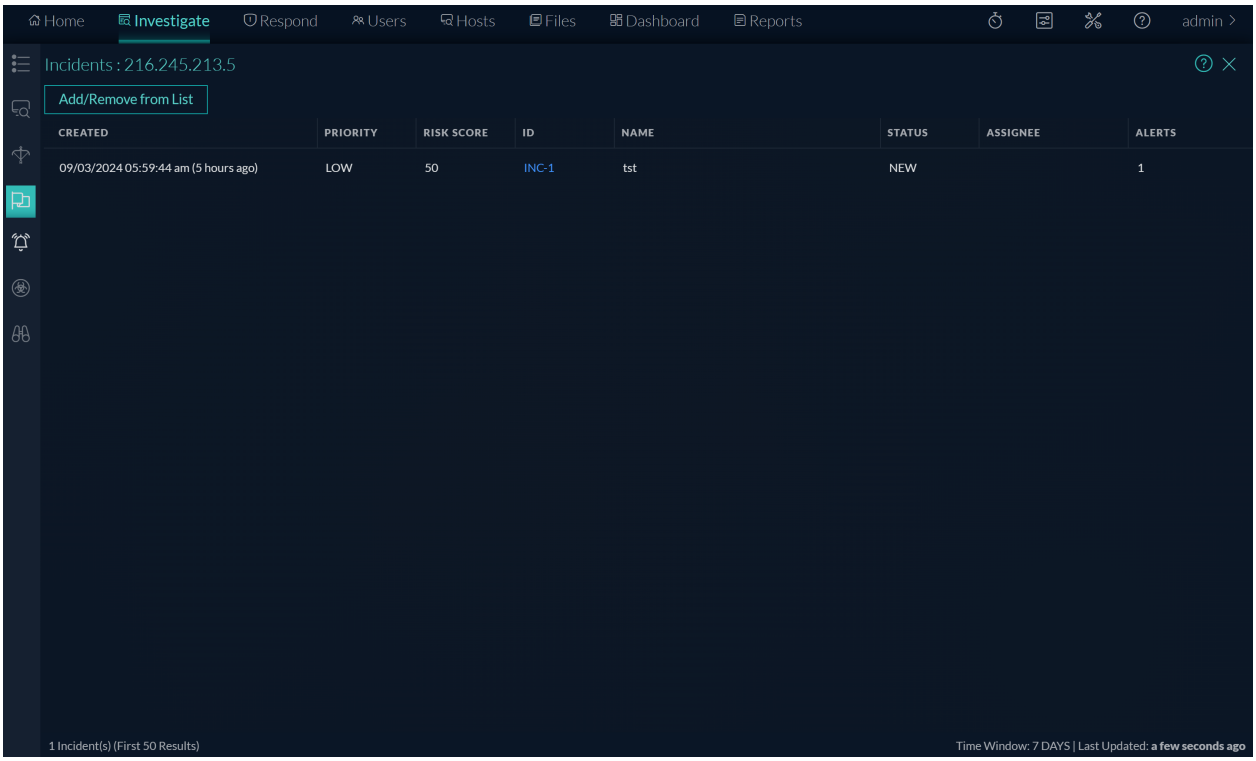


[コンテキスト ルックアップ]パネルの [アラート]タブには以下の情報が表示されます。

フィールド	説明
作成日時	アラートが作成された日時。
重大度	アラートの重大度の値
名前	アラートの名前。名前をクリックすると特定のアラートの詳細が表示されます。
ソース	アラートをトリガーしたアラート ソースの名前。
イベント数	アラートに関連するイベントの数。
インシデントID	アラートが関連づけられているインシデントのID(該当する場合)。IDをクリックすると特定のアラートの詳細が表示されます。
件数	アラート数デフォルトでは、最初の100件のアラートのみが表示されます。設定の構成方法の詳細については、『*Context Hub構成ガイド*』の「Context Hubのデータ ソース設定の構成」を参照してください。
タイム ウィンドウ	[データ ソース設定の構成]ダイアログの [クエリの対象期間]フィールドに設定された値に基づいたタイム ウィンドウ。デフォルトでは、過去7日間のアラート データをフェッチします。
最終更新日	データ ソースからコンテキスト データを最後に取得した時刻。

[インシデント]タブ

次の図は、最初に時間(新しい順)次に優先度のステータスに基づいた[コンテキスト ルックアップ]パネルの[インシデント]タブの例です。



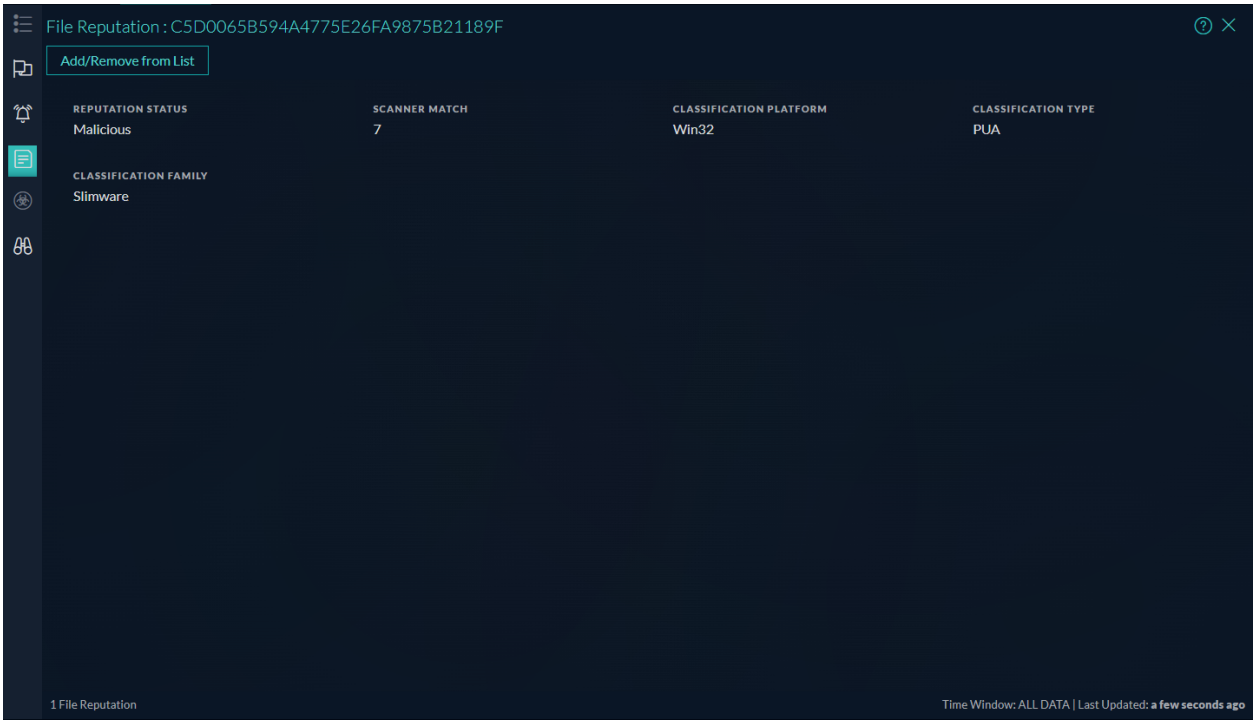
[コンテキスト ルックアップ]パネルの[インシデント]タブには以下の情報が表示されます。

フィールド	説明
作成日時	インシデントが作成された日付。
優先度	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。

フィールド	説明
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。

[ファイル レピュテーション]タブ

[ファイル レピュテーション]の [コンテキスト ルックアップ]パネルには、そのファイルのレピュテーションのステータスが表示されます。

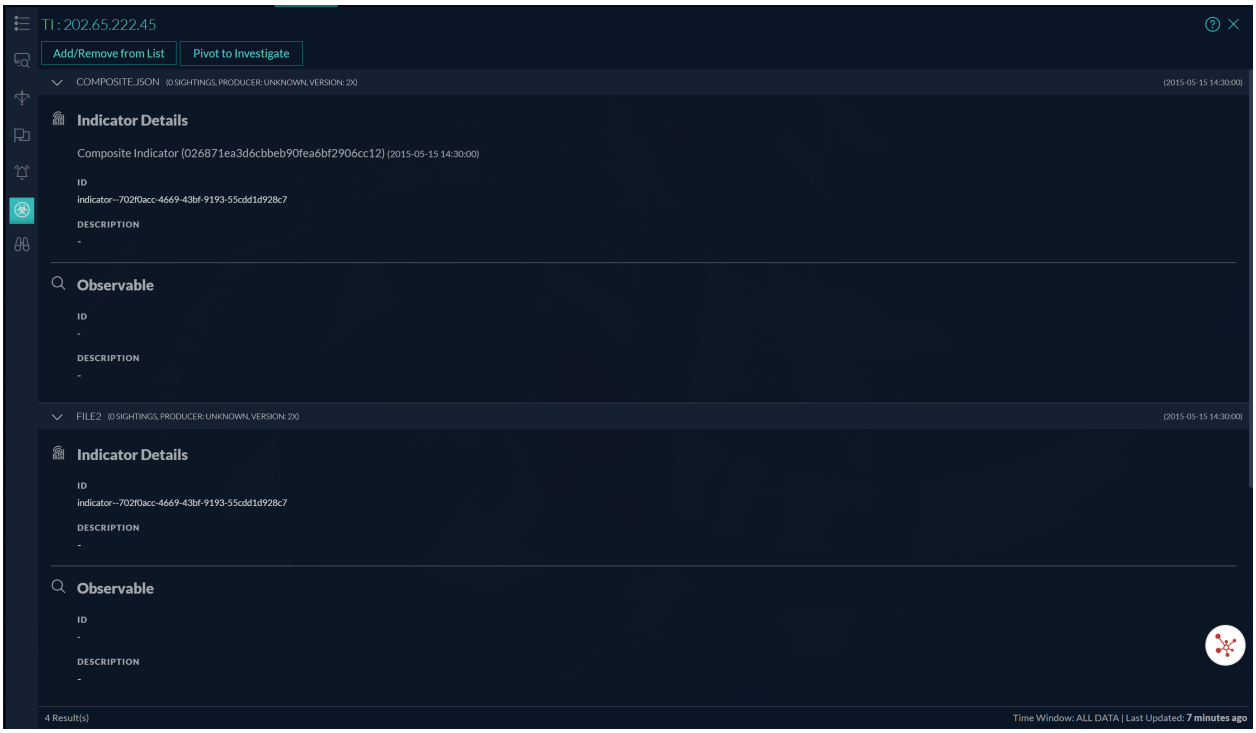


フィールド	説明
レピュテーション ステータス	filehashのレピュテーション ステータス。レピュテーションのステータスの詳細については、『*UEBAユーザ ガイド*』の「ファイル レピュテーションの表示」を参照してください。
スキャナーー致	最後のスキャンで、マルウェアまたは疑わしいアクティビティを検出したスキャナーの数。
分類プラットフォーム	プラットフォームに基づき、クエリされたfilehashのクラス分け。たとえば、プラットフォームをWin 32にすることができます。
分類タイプ	タイプに基づき、クエリされたfilehashのクラス分け。
分類ファミリー	マルウェア ファミリー名に基づき、クエリされたfilehashのクラス分け。

[TI] タブ

次の図はTIのコンテキスト パネルの例であり、表には表示される情報の説明があります。

注 : NetWitnessバージョン12.5以降では、アナリストはSTIX V2 (2.0および2.1) 標準を使用するインジケーターのコンテキスト検索を実行し、より多くの脅威コンテキストを取得して調査を強化できます。



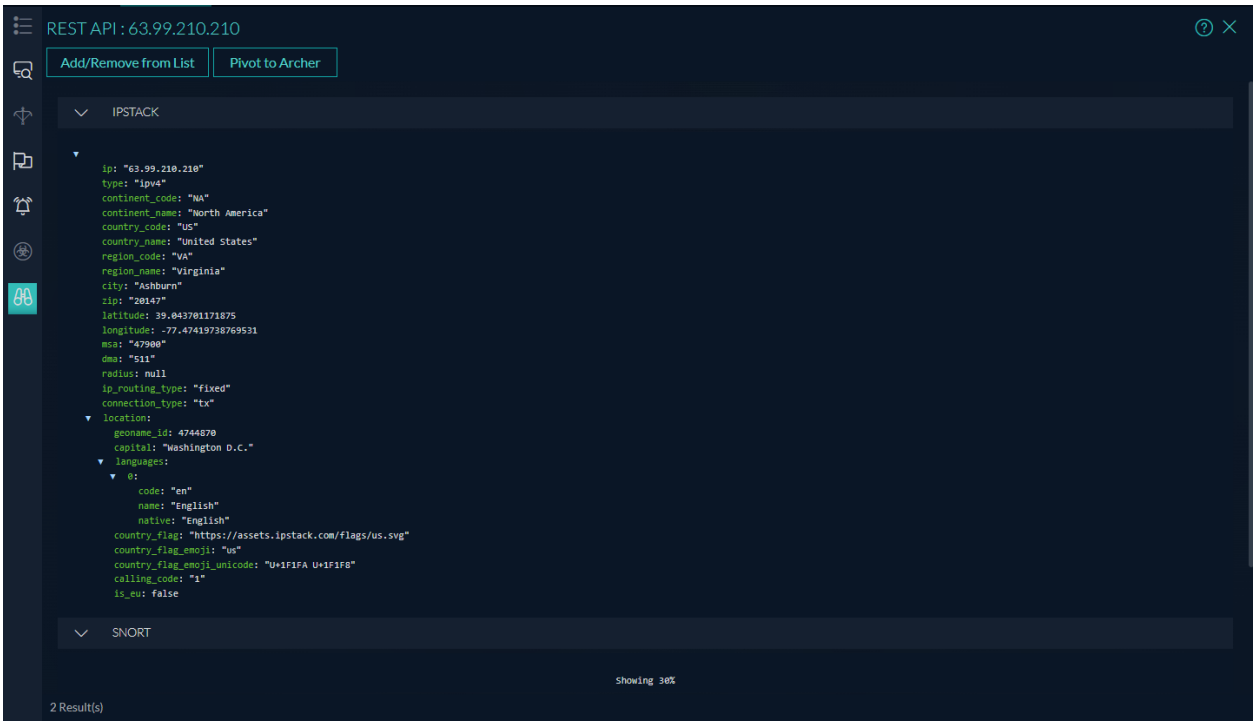
フィールド	説明
データ ソース名	データの取得元であるSTIXデータ ソース名を表示します。
Timestamp	イベントが作成された時刻。
インジケータの詳細	インジケータ タイトル :疑わしいまたは悪意のあるサイバー活動を検出するために使用できるパターンを含む詳細を表示します。 ID :選択したインジケータのIDを表示します。 作成者 :STIXデータを要求したユーザ ロールを表示します。 説明 :監視リストにある選択したIPアドレスの詳細を表示します。
観測事象	観測事象タイトル :STIX Cyber-observable Object(SCO) を使用して、ファイル、システム、ネッ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。 ID :選択した観測事象のIDを表示します。
(オプション) SightingsREST	観測タイトル :観測ソースの名前を表示します。 信頼度 :観測の重要度を表示します。 参照 :観測ソースの参照URLを表示します。

[REST API] タブ

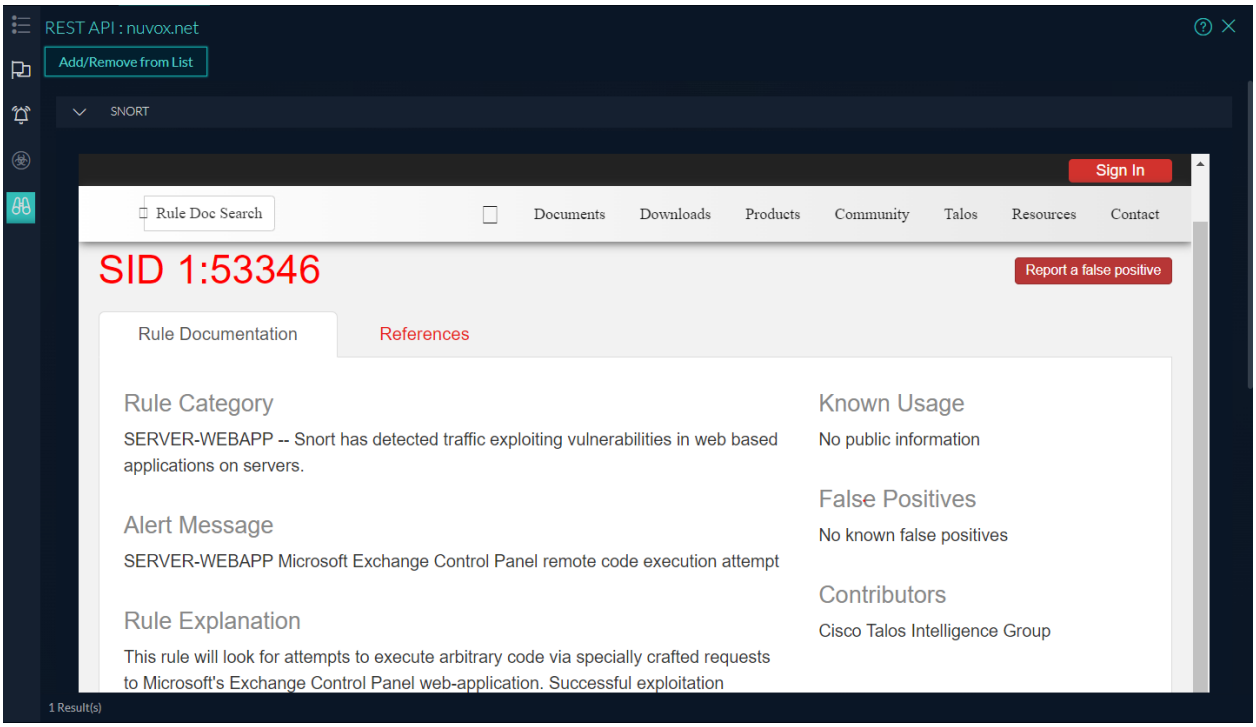
REST APIのコンテキスト ルックアップ パネルには、選択したエンティティまたはメタ値に関連づけられたHTMLまたはJSON応答(構成された応答タイプに基づく)が表示されます。

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、HTML応答を含むREST APIのコンテキスト パネルの例です。

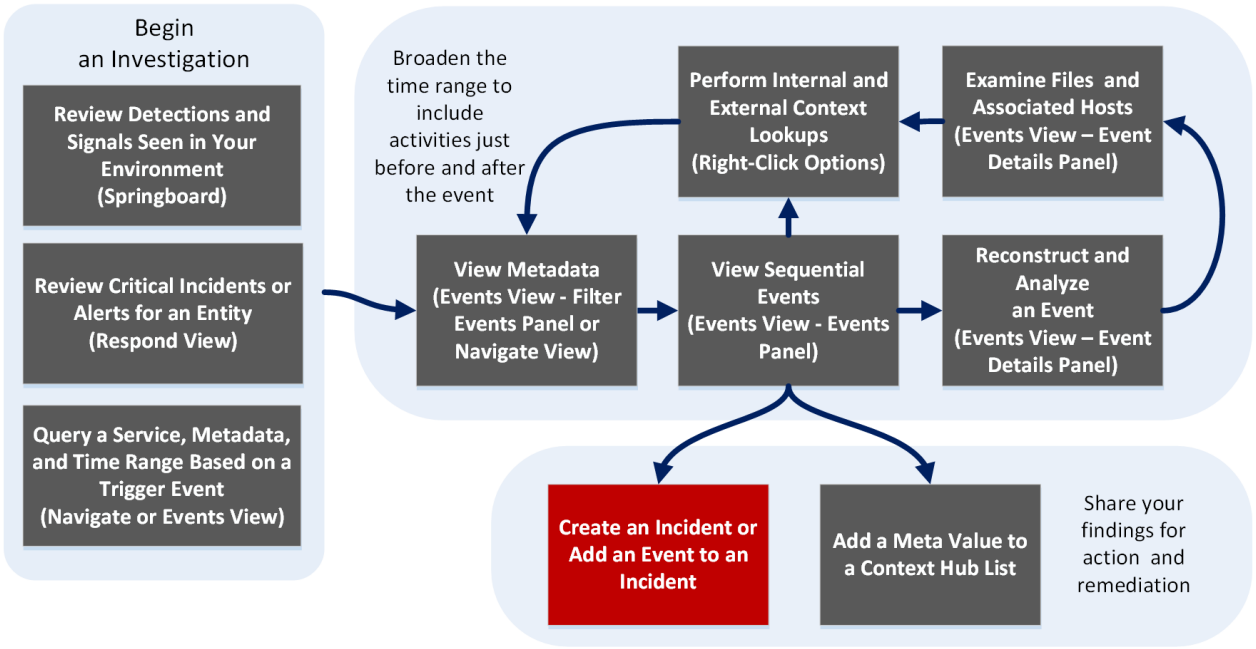

REST API : nuvox.net
Add/Remove from List
SNORT
Sign In
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
SID 1:53346
Report a false positive
Rule Documentation
References
Rule Category
SERVER-WEBAPP -- Snort has detected traffic exploiting vulnerabilities in web based applications on servers.
Alert Message
SERVER-WEBAPP Microsoft Exchange Control Panel remote code execution attempt
Rule Explanation
This rule will look for attempts to execute arbitrary code via specially crafted requests to Microsoft's Exchange Control Panel web-application. Successful exploitation
Known Usage
No public information
False Positives
No known false positives
Contributors
Cisco Talos Intelligence Group
1 Result(s)

[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	*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 イベントビューでメタデータのドリルダウン
脅威ハンター	シーケンシャル イベントの表示	[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

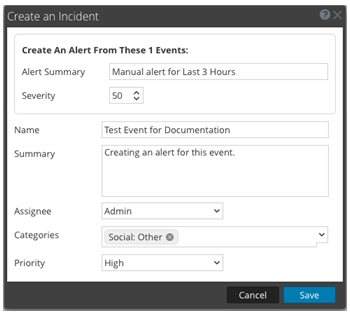
*このタスクは現在のビューで実行できます。

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

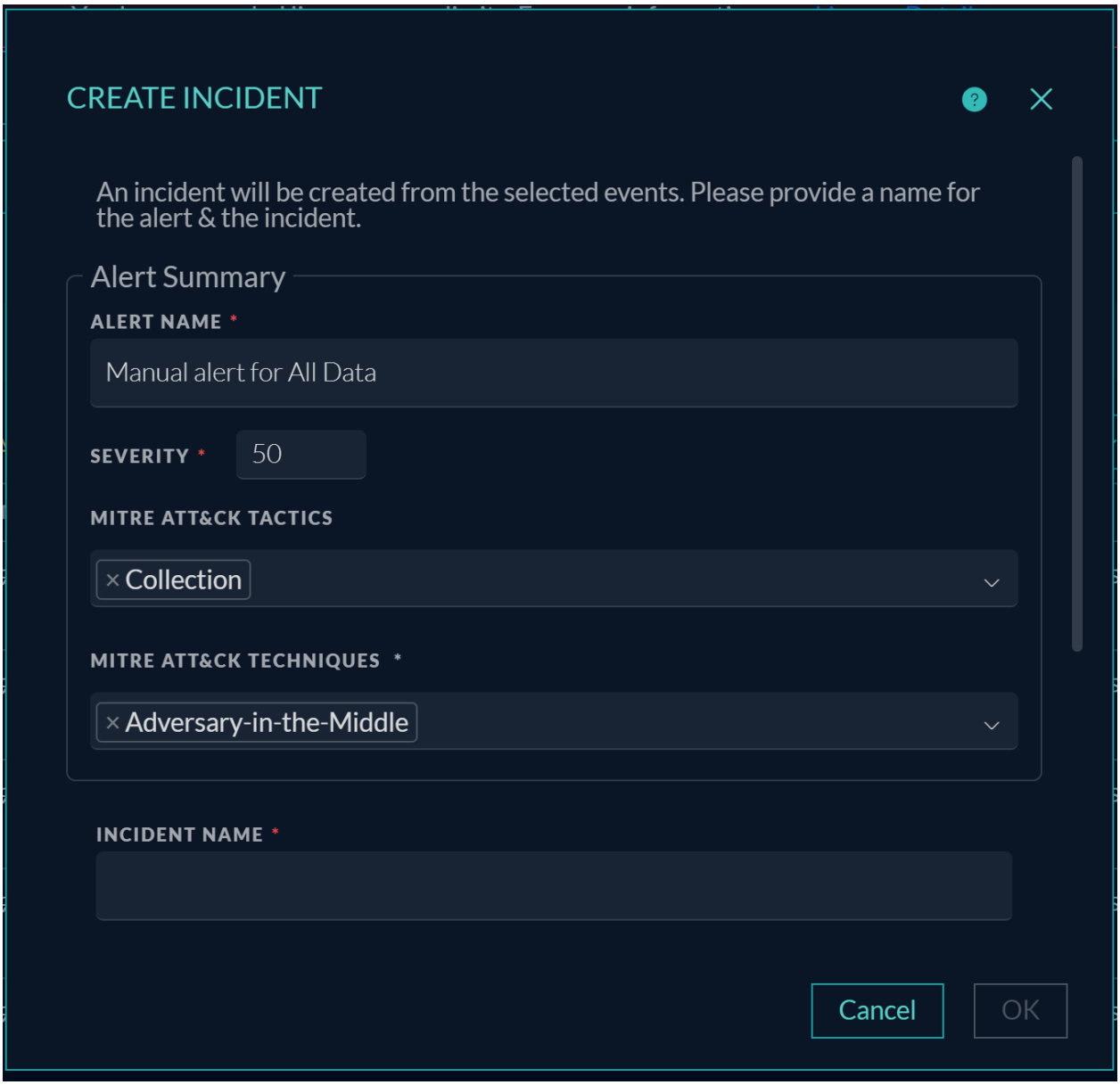
簡単な説明

次の図に、レガシー イベントの [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ーを識別します。 「カテゴリー」をクリックすると、インシデントのカテゴリーとサブカテゴリーのドロップダウン リストが表示されます。インシデントが属するカテゴリー(複数可) を選択できます。カテゴリは主要なグループ(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。

次の図は、 「イベント」ビューの 「インシデントの作成」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
アラート名	(必須) アラートを識別する名前を指定します。この例では、名前は「Manuel alert for All Data」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。
重大度	「重大度」フィールドには、選択したアラートの重大度として、1~100の整数が示されます。
MITRE ATT&CK 戦術	アラートに関連する戦術のタイプを表示します。 例 :**クレデンシャル アクセス**。 クレデンシャル アクセス戦術は、アカウント名とパスワードを盗もうとします。

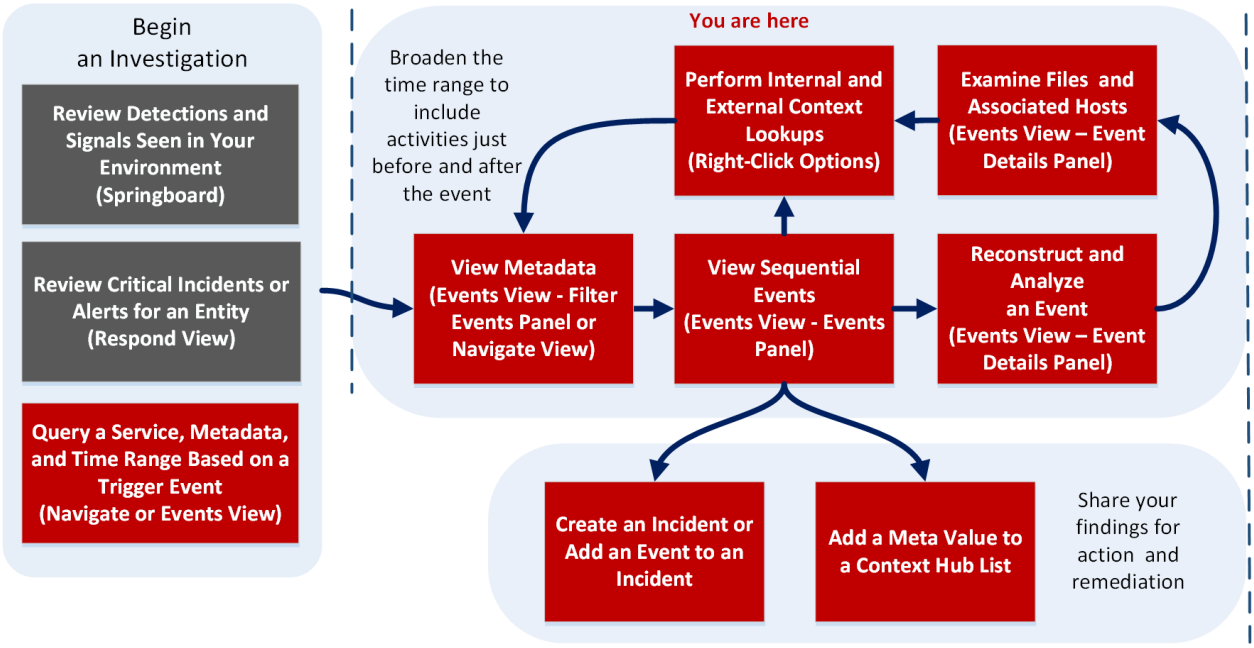
機能	説明
MITRE ATT&CKテクニック	戦術に関連付けられたテクニックとサブテクニックの種類が表示されます。
インシデント名	(必須) インシデントを識別する名前を指定します。このインシデントに追加されるイベントの特性を明確に識別する名前を指定します。
優先度	インシデントの優先度を識別します。 [優先度]をクリックすると、優先度のドロップダウン リストが開きます。ドロップダウン リストには、 [クリティカル]、 [高]、 [中]、 [低]が表示されます。
割り当て先	(オプション) インシデントをSOC内のユーザに割り当てます。 [割り当て先]をクリックすると、インシデントに対応するSOC担当者のユーザ名がドロップダウン リストに表示されます。
カテゴリ	(オプション) インシデントのカテゴリーを識別します。 [カテゴリー]をクリックすると、インシデントのカテゴリーとサブカテゴリーのドロップダウン リストが表示されます。インシデントが属するカテゴリー(複数可)を選択できます。カテゴリは主要なグループ(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。
キャンセル	変更を保存せずにダイアログを閉じます。
OK	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。リストされたイベントのメタデータを詳しく調べることができます。 [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じWeb再構築が表示されます。

ワークフロー

次の図は、NetWitnessの [調査]で実行できるタスクを示す概要レベルのワークフローです。 [イベント]ビューのタスクが赤色でハイライト表示されています。



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*

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 [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 イベントビューでメタデータのドリルダウン
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

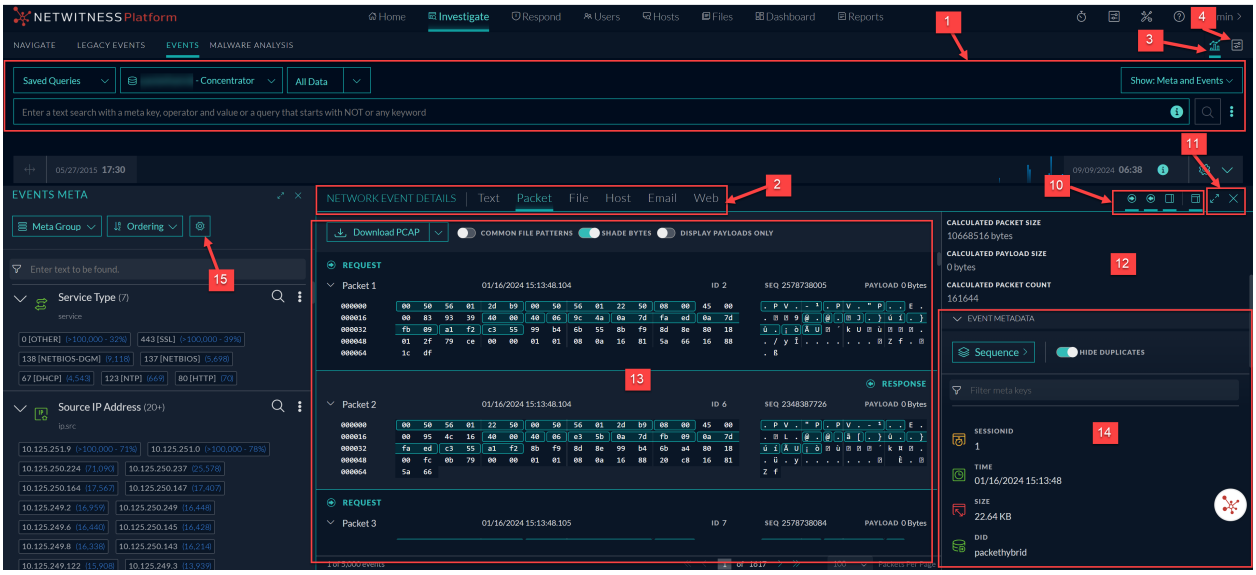
簡単な説明

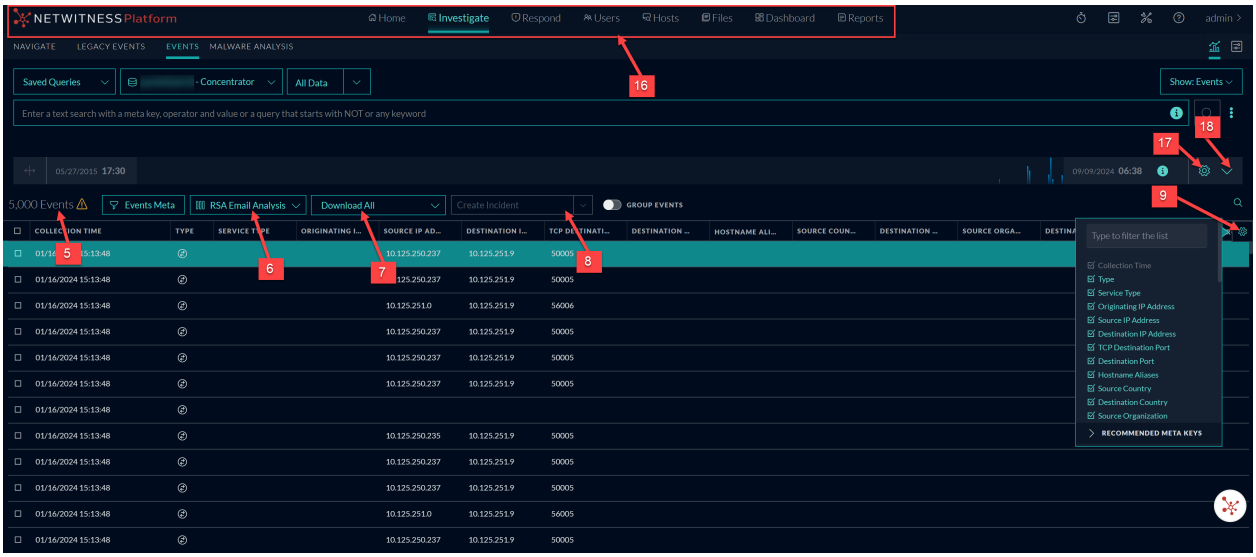
このビューには複数のアクセス ポイントがあります。詳細については「 [イベント]ビューでの調査の開始 」を参照してください。 [対応]ビューから [イベント]ビューにアクセスすると、インシデント内の選択したイベントの分析を確認できます。オプションは、 [調査]ビュー内からイベントを開いたときに使用できるオプションのサブセットです。完全な機能を取得し、他のイベントを調べるには、イベント ビューに直接移動します (調査 > イベント)。

[イベント]ビューの [イベント]パネルには、イベントが時間の昇順で表示されます。表示されるイベントは、 [ナビゲート]ビュー]ビューまたは [レガシー イベント]ビューのドリルダウン ポイントの結果、または [イベント]ビューのクエリ バーで入力されたクエリの結果です。

クエリの入力フィールドが表示されるので、サービスや時間範囲を選択し、オプションのクエリを入力できます。クエリを送信すると、調査対象のサービスによって、最大10,000イベントの結果がカウントされ、10,000個のネットワーク、ログ、エンドポイント イベントが [イベント]パネルにロードされます。表示される列は、選択した列グループによって異なります。列の並べ替えやサイズ変更、標準提供またはカスタムの列グループの選択、表示する列の個別の選択を行えます。関心のあるイベントが見つかった場合は、イベントをクリックすると、新しいパネルで再構築(パケット、テキスト、ファイル) が開きます。

次の図では、 [イベント]ビューの主要な機能がハイライト表示されています。





1	**クエリ バー** :サービスを選択すると、サービス セレクタ、時間範囲セレクタ、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。 (**クエリ コンソール**) > **現在のクエリ** タブをクリックすると、現在のクエリの詳細なステータスが表示されます (以下の [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 タイプで使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、および電子メール) 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。電子メール タイプとWebタイプでは、現在のイベントがイベント ビューで電子メールまたはWebの再構築として開きます。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、「イベントビューでイベントを分析する」を参照してください。
4	イベント ビューの設定を行います ([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。 • イベント パネルのタイトルは以前のバージョンのタイトルとは少し異なり、行番号インジケーターが追加されました。タイトルには、イベント数とソート順のリストが表示されます。たとえば、 [**40,000イベント (昇順)**] は、40,000個のイベントが見つかったことと、それらが昇順で表示されていることを意味します。10,000個を超えるイベントが見つかった場合は、最も古い10,000イベントのみが昇順で表示され、ロードされなかったイベントがあることを示す黄色の三角形が表示されます。これは、クエリを絞り込む必要があることを示している可能性があります。ここにリストされてい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。

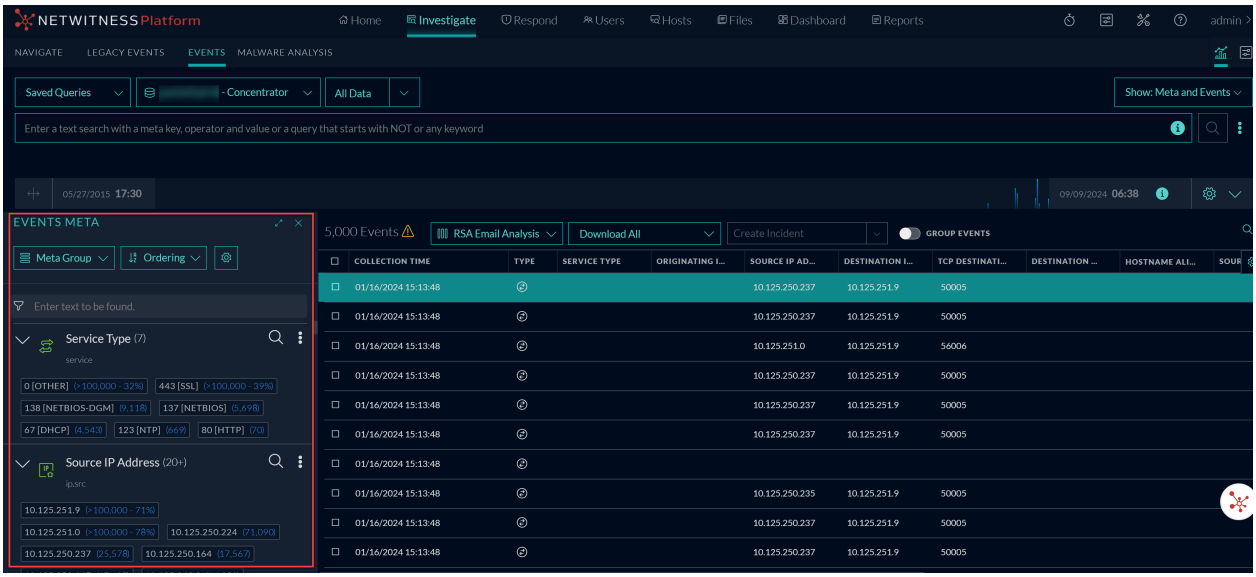
	•  をクリックすると、「表 内 のテキストを検 索 」ダイアログが開きます。
6	「列 グループ」ドロップダウンには、「イベント」パネルに適 用 できる標 準 提 供 の列 グループとカスタム列 グループが表 示 されます。標 準 提 供 の列 グループは、バージョン間 で更 新 されることがあります。標 準 提 供 の列 グループには、Email Analysis、Endpoint Analysis、Malware Analysis、Outbound HTTP、Outbound SSL/TLS、Summary Listなどがあります。デフォルト の列 グループはSummary Listです。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	「すべてダウンロード」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	「概 要 」パネルの表 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、「イベントビューでイベントを分 析 する」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、「イベントビューでイベントを分 析 する」を参 照 してください。
12	「概 要 」パネルには、現 在 分 析 中 のイベントに関 するサマリー情 報 が表 示 されます。選 択 したイベント が、「イベント」パネルで青 色 の背 景 でハイライト表 示 されます。サマリー情 報 は、イベント タイプ(パケット 、ログ、エンドポイント) によって異 なります。
13	現 在 分 析 中 のイベントのイベント データ。
14	イベント メタデータ パネルには、データ内 で見 つかったメタ キーと値 が一 覧 表 示 されます。このデータは、アルファベット 順 と生 成 順 という2つの方 法 でソート できます。一 部 のメタ データは検 索 可 能 です。双 眼 鏡 アイコンをクリックすると、関 連 するデータがイベント データでハイライト表 示 されます(「イベントビューでイベントを分 析 する」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ユーザー ガイド』を参 照 してください) 。
15	アナリスト は、この「メタ設 定 」パネルを使 用 して、「イベント」ビュー内 で特 定 のメタ キー値 に必 要 なセッション数 を設 定 できます。
16	NetWitness Platform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) のオプションにアクセスしやすくなっています。
17	アナリスト はタイムライン設 定 オプションを使 用 して、Y軸 のデータ ディメンション(数 またはサイズ) を変 更 し、タイムライン上 に表 示 されるデータを確 認 できます。ミニ タイムラインの右 側 にある(情 報) ボタンをクリックすると、タイムラインのイベント データの表 現 (Y軸 にどのような情 報 が表 示 されるかなど) を確 認 できます。

18 タイムラインの展開機能を使用すると、検索クエリーに基づいてイベントの結果を対話的に操作できます。展開されたタイムライン ビューには、選択した日付と時刻範囲のイベントの合計数が表示されます。展開されたタイムラインでは、X軸は時間を示し、Y軸は、タイムライン上の特定の時間にサービスによって記録された、発生したイベントの総数またはファイル サイズを示します。

[イベント メタ] パネル

[イベント] パネルの [イベント メタ] ボタン(Events Meta) 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。デフォルトでは、イベント メタ パネルはイベント ビューで開きます。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、「イベントビューでメタデータのドリルダウン」を参照してください。

注 : デフォルトでは、イベント メタ パネルはイベント ビューで開きます。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 メタ] 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。

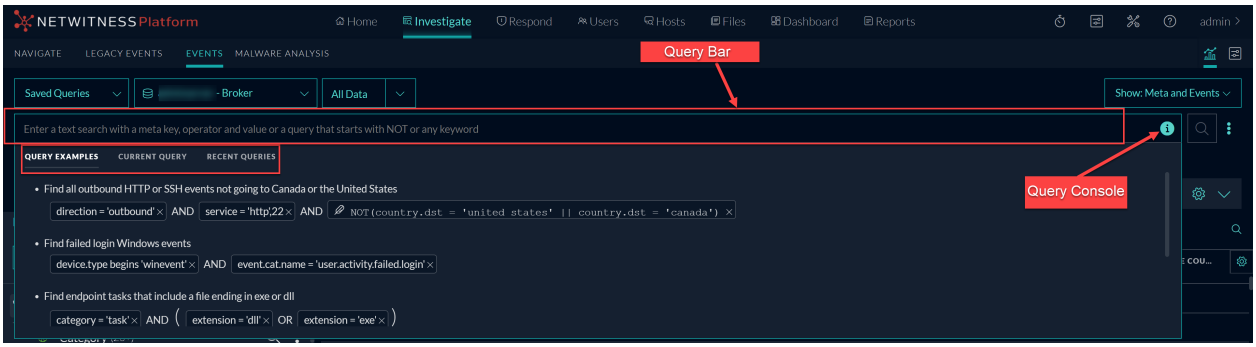


[メタ グループ] メニュー [イベント メタ] パネルを開いた状態で、メタ グループを選択して、 [イベントの絞り込み] パネルに表示されるメタ キーを定義できます。デフォルトのメタ キー メタ グループは、最初にログインしたときに有効になります。前回ログインしたときに別のメタ グループを選択した場合は、ブラウザーのキャッシュがクリアされない限りそのメタ グループが有効なままになります。メタ グループの詳細については、「メタ グループを使用して関連性の高いメタ キーにフォーカス」を参照してください。

メニューの並べ替え	[イベント メタ]パネルを開くと、値ごとにイベント数、イベント サイズ、パケット数の3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、イベント サイズ、またはパケット数のいずれかが含まれます。いずれの場合も、並べ替えには4つのオプションがあります。 • デフォルトでは、メタ キーは「イベント数 > 合計数の降順」方式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。 • 値を含んだパケットの数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(合計数による降順、数による昇順、合計値による昇順、合計値による降順)のいずれかを使用できます。
[メタ キー オプション]ボタン (⊟)	[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。
メタ キー リスト	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。
メタ設定	アナリストは、この[メタ設定]パネルを使用して、[イベント]ビュー内で特定のメタ キー値に必要なセッション数を設定できます。

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ー コンソールが開き、クエリーの例、現在のクエリー、最近のクエリーの詳細が表示されます。



クエリーの例

クエリー コンソール> **[クエリーの例]**タブには、クエリーの構成を理解するのに役立つサンプル クエリー リストが表示されます。

現在のクエリー

クエリー コンソール> **[現在のクエリー]**タブでは、クエリー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、クエリー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、「クエリーのステータスの表示」を参照してください。

クエリ コンソールに表示されるメッセージの中には、追加の説明が必要なものがあります。

メッセージ :インデックス スライス%3%のメタ キー%2%で%1%の最大値制限(valueMax)に達しました

説明 :クエリ対象インデックスで、指定されたメタ キーの`valueMax`プロパティに到達しました。管理者は、`ADMIN > Services > [Service Name] > Files > index-[service type].xml`または`index-[service type]-custom.xml`のインデックス ファイルでこの値を設定します。たとえば、インデックス ファイルの次のステートメントでは、`client`というメタ キーの値の数がデフォルトで250,000に制限されています。

```
<key description="Client Application" level="IndexValues" name="client"
format="Text" valueMax="250000" />
```

メッセージ :チャネル%2%のクエリは、時間の使用制限を超過しているため、システムによって自動でキャンセルされました。タイムアウト値を確認してください。

実行時間に対する操作あたりの制限がサーバにあり、要求された操作がこの制限を超過しました。このエラーを回避するには、小さい時間範囲などの小さな要素に操作を分割します。

メモリ制限の%1%に達しました。これは、max.query.memoryを設定することによって制御されます

メモリ使用率に対する操作あたりの制限がサーバにあり、要求された操作がこの制限を超過しました。この制限はサーバーのメモリー容量に関連しており、管理者は、この値を(管理)**[管理]**> **[サービス]**> [**<サービス名>**]> **[sdk]**> **[config]**で調整できます。このエラーを回避するには、小さい時間範囲などの小さな要素に操作を分割します。

最近のクエリー

クエリー コンソール> **最近のクエリー**]タブには、最大100個の最近のクエリーが表示されます。マウスのスクロール ホイールを使用して、最近のクエリー リスト内を移動します。クエリーの先頭で  をクリックしてそのクエリーを選択し、クエリー バーに直接挿入することができます。

最近のクエリーを選択すると、クエリー バーに設定されている基本設定に従ってクエリーが表示されます(ガイド モードまたは詳細モード)。  をクリックして、選択したクエリーを開始します。

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。

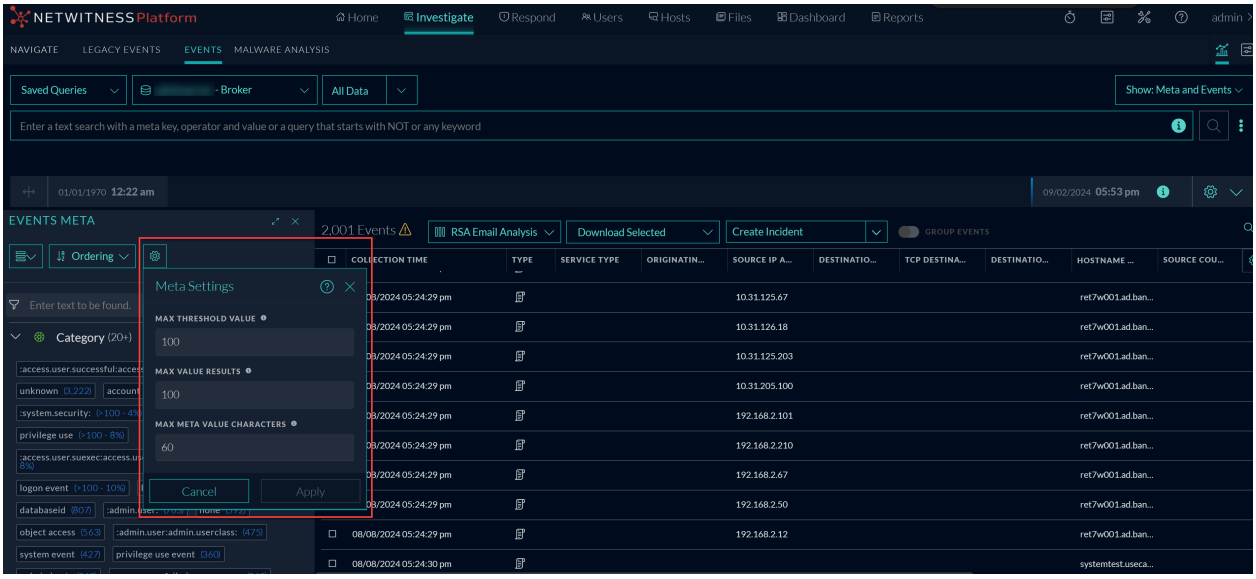
詳細については、「[イベント]ビューでの調査の開始」の「*タイムラインでの調査*」トピックを参照してください。

[メタ設定]パネル

NetWitnessでは、**[調査]** > **[イベント]**ビューの下に、新しい **[メタ設定]**パネルが導入されています。アナリストは、このパネルを使用して、[イベント]ビュー内で特定のメタ キー値に必要なセッション数を設定できます。

簡単な説明 - [メタ設定]パネル

これは、[メタ設定]ダイアログの例です。



次の表は、[メタ設定]パネルのフィールドについて説明しています。

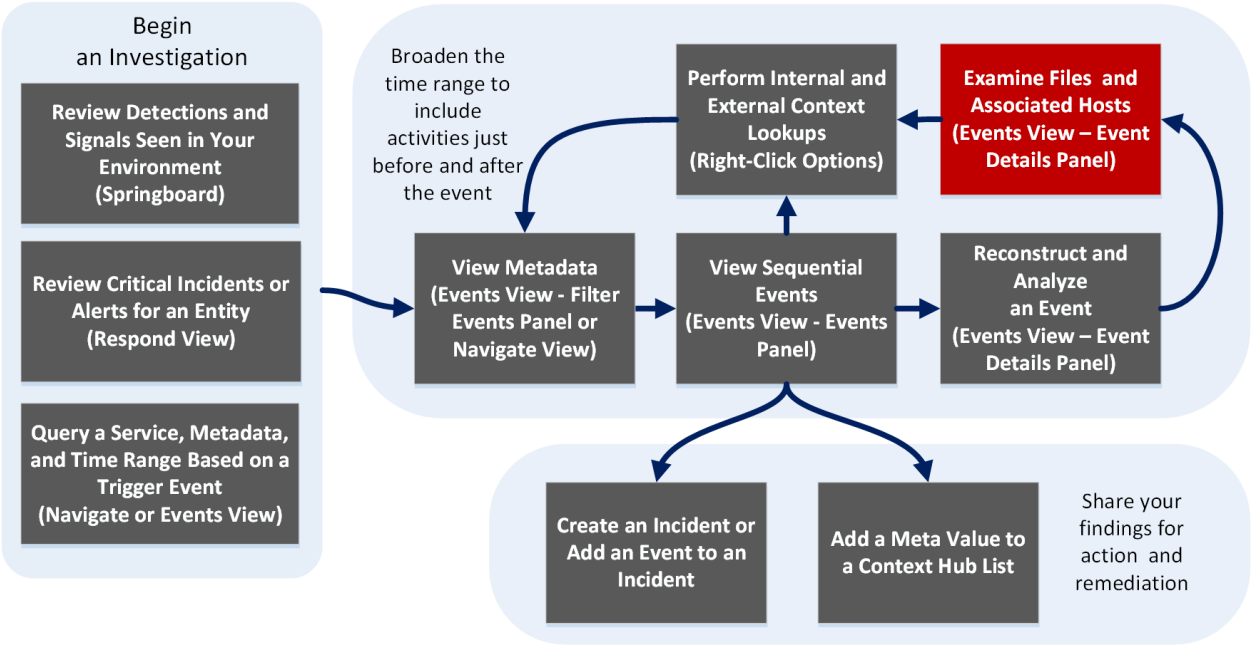
機能	説明
最大閾値	[値]パネルでメタ キー値にロードするセッションの最大数の閾値を設定します。閾値を高くすると、値が正確にカウントされますが、その分ロード時間が長くなります。最大閾値は、1～2147483647の範囲内である必要があります。デフォルト値は100,000です。
結果の最大数	この設定は、[ナビゲート]ビューで開いているメタ キーについて、[メタ キー]メニューで [最大まで表示]を選択した場合にロードする値の最大数を制御します。結果の最大数は、100～100000の範囲内である必要があります。デフォルト値は1000です。

機能	説明
メタ値の最大文字数	[イベント メタ]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。メタ値の最大文字数は、**60**～**512**の範囲内である必要があります。デフォルト値は**60**です。
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。
X	[メタ設定]ダイアログを閉じます。

[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

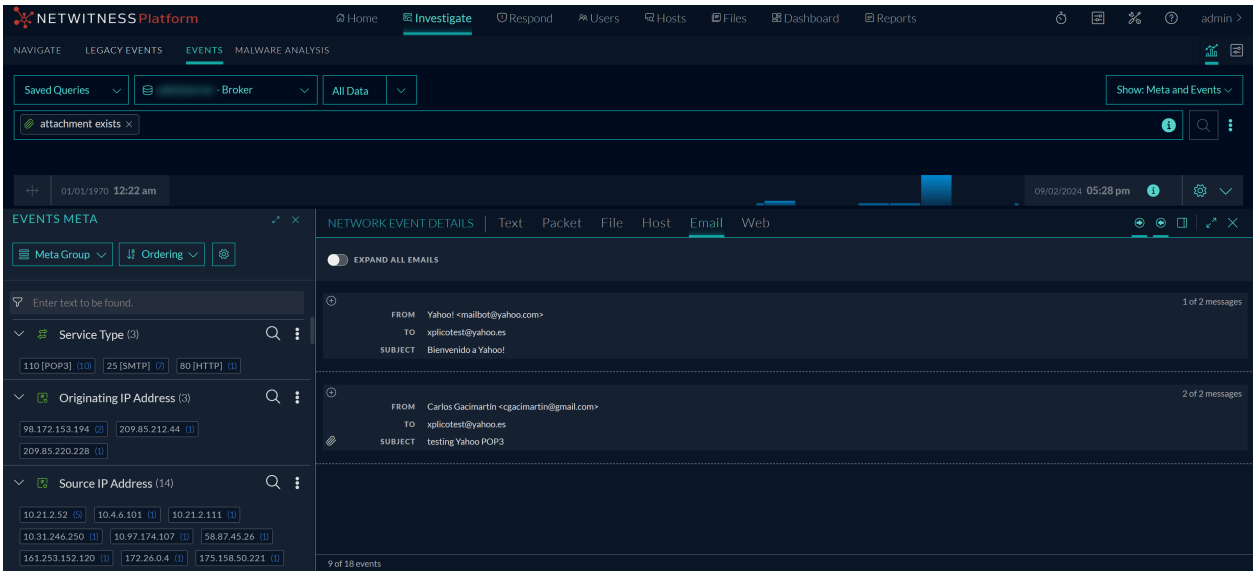


関連トピック

- 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。



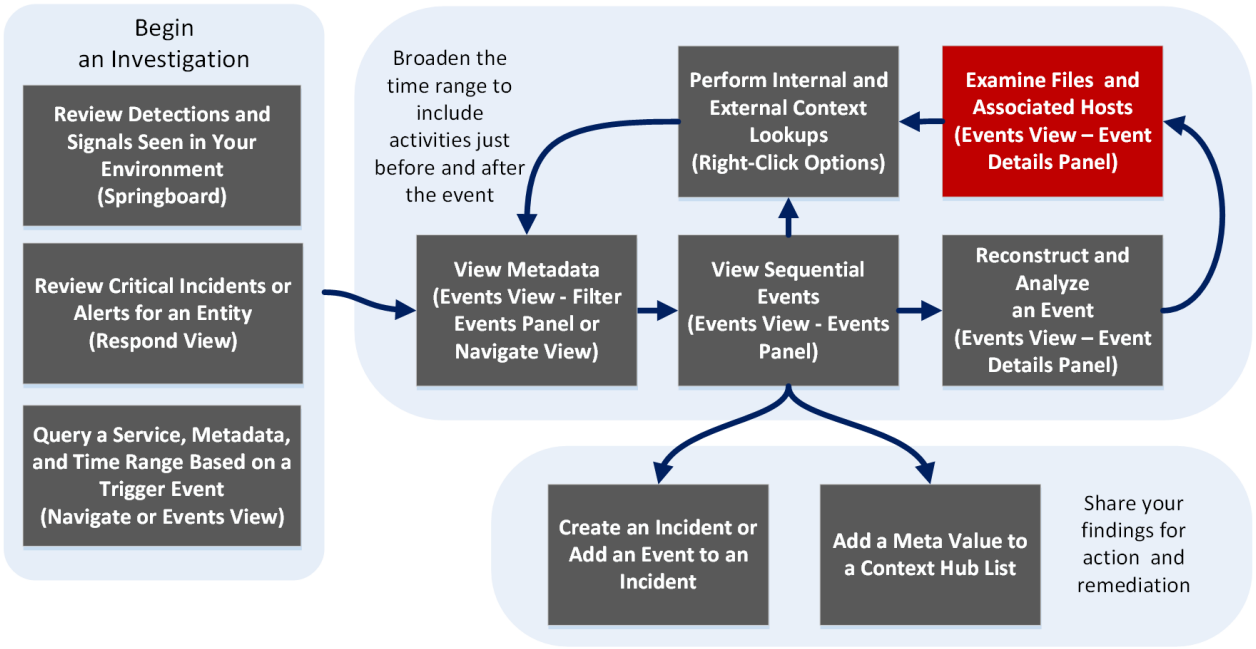
次の表は、メール内のすべてのフィールドについて説明しています。

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。
受取人	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	*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 イベントビューでメタデータのドリルダウン

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 イベントの表示	[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
脅威ハンター	ファイルのVirusTotalルックアップの開始	[イベント]ビューでのデータのダウンロード

*このタスクは現在のビューで実行できます。

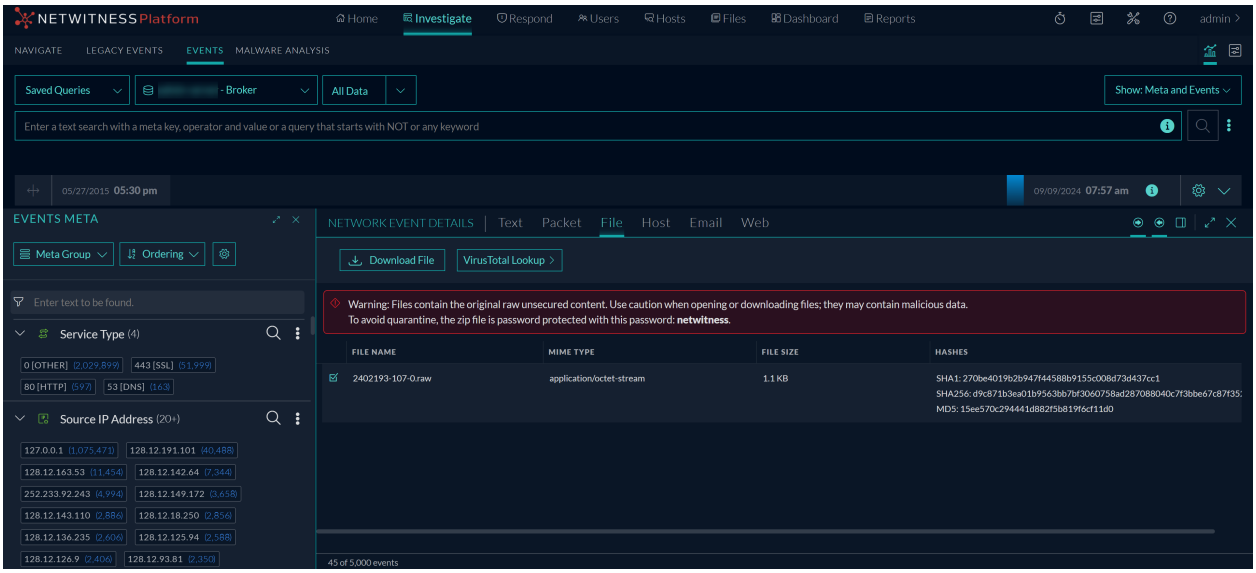
関連トピック

- 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。

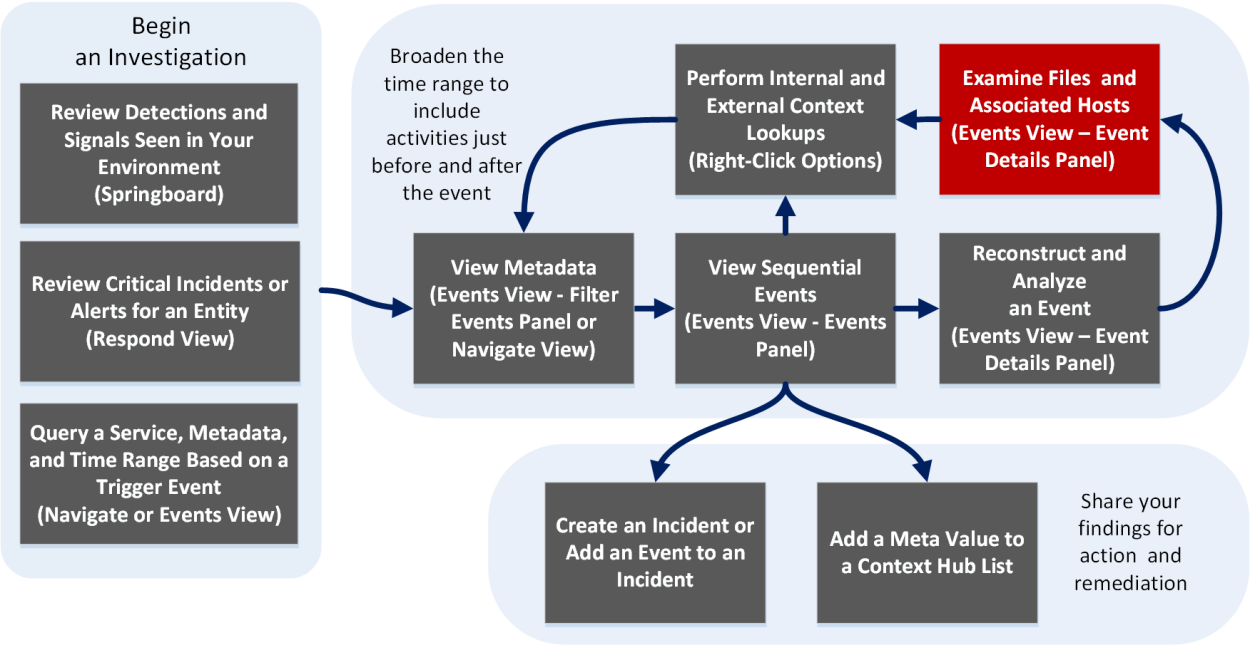


機能	説明
[ファイルのダウンロード]ボタン	クリックして1つまたは複数の選択したファイルをダウンロードします。
イベント ヘッダー	イベント ヘッダーには、ファイルを含むネットワーク イベントのサマリ情報が表示されます。
ファイル リスト	選択してダウンロードできる、関連づけられているファイルのスクロール可能なリスト。
VirusTotalルックアップ	クリックして**MD5**、**SHA1**、または**SHA256**で検索を実行します。

[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	*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 イベントビューでメタデータのドリルダウン

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 イベントの表示	[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

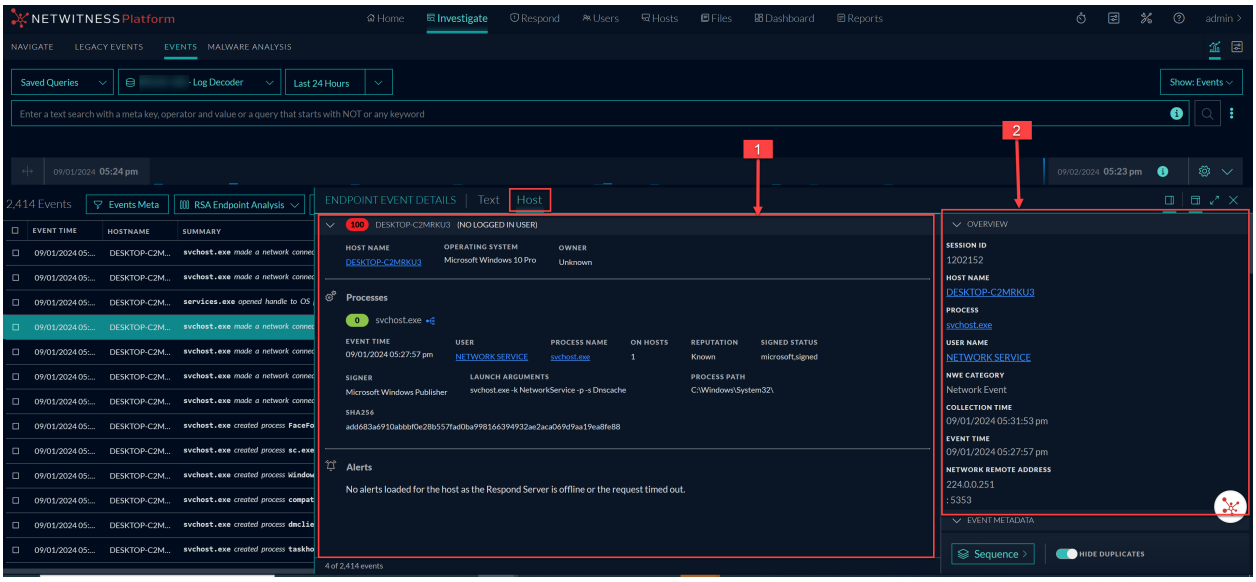
*このタスクは現在のビューで実行できます。

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。



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。

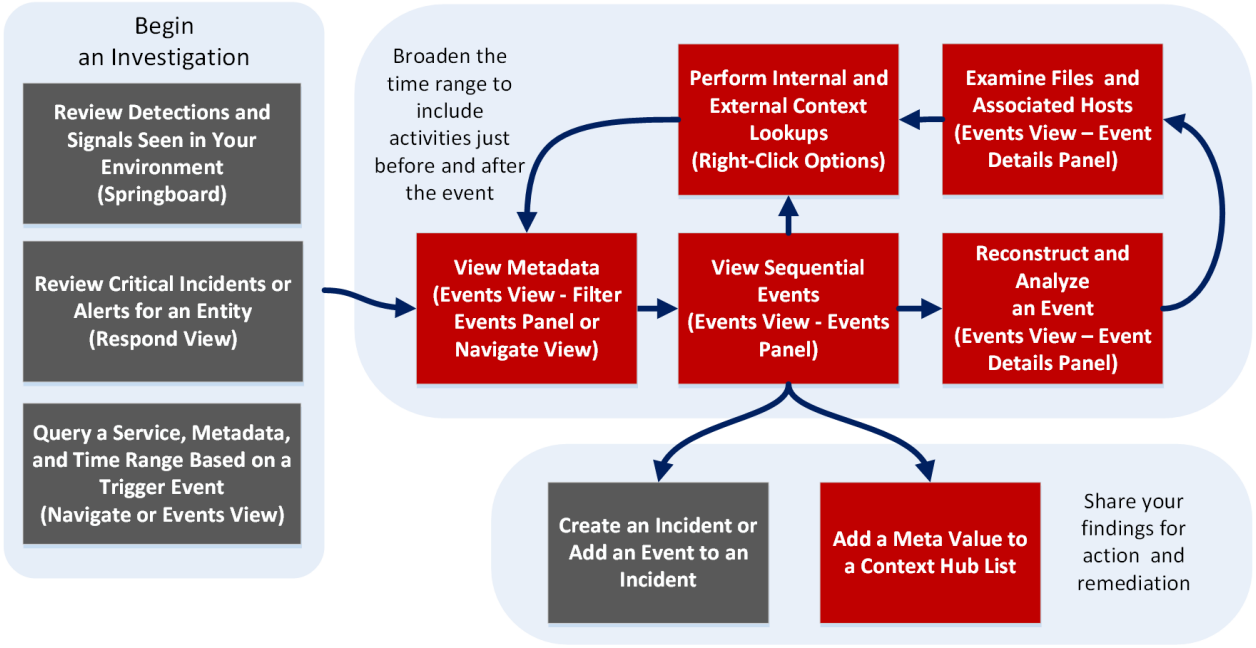
- ホスト - イベントの発生元ホスト。
- プロセス - イベントをトリガーしたソース プロセス。
- ユーザー - トリガーされたプロセスに関連づけられているユーザー。

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	*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 イベントビューでメタデータのドリルダウン

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

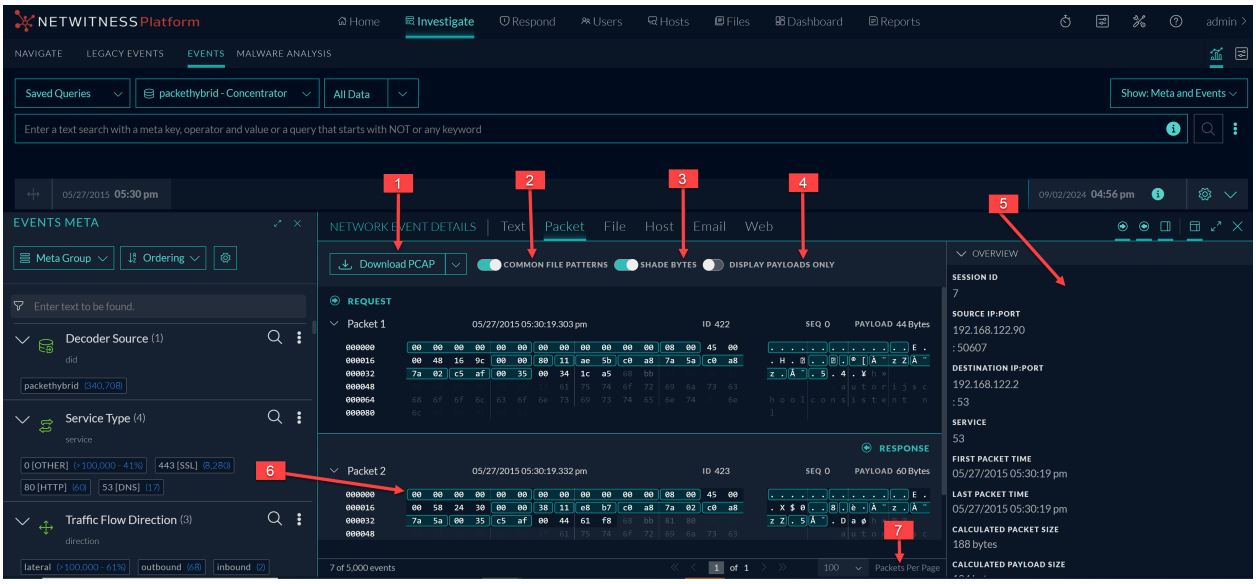
簡単な説明

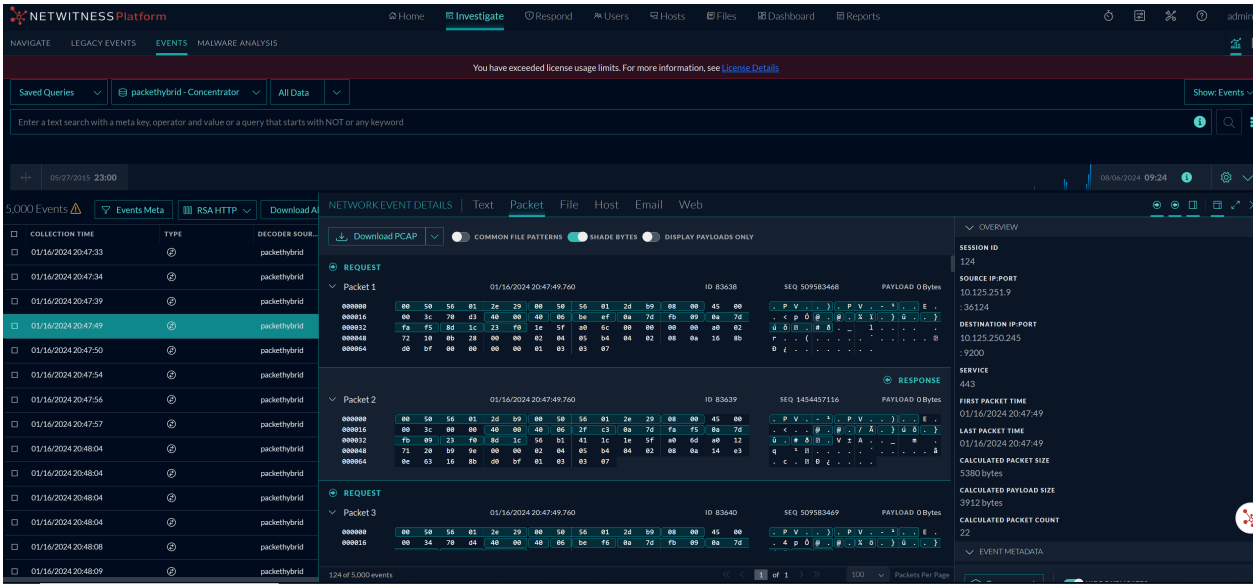
[パケット]パネルでは、ネットワーク イベントのみを分析できます。[パケット]パネルには、イベントの各パケットが表示されます。パケットのリストはスクロール可能です。スクロールすると、リクエストとレスポンスのラベルと同様にパケットまたはテキストの識別情報も、スクロールされて見えなくならず表示され続けます。

ページネーション コントロールを使用すると、ページを前後に移動したり、特定のページに移動したり、ページごとに表示するパケット数 (50、100、300、または500) を選択したりできます。

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。各機能の詳しい説明と例については、「イベントビューでイベントを分析する」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オプションはデフォルトでは無効になっていますが、有効にすることができます。一般的なファイル シグネチャはオレンジ色でハイライト表示されます。ハイライト表示にカーソルを合わせると、ファイル タイプが表示されます。
3	［バイトの濃淡化］オプションは、16進数バイト(00～FF) を識別しやすくするため濃淡を変えてバイトを表示する機能です。

4 ペイロードを表示するオプションは、パケット ヘッダーのみを非表示にして、ペイロードのスペースを多く残します。

5 概要]パネルの情報

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 パケット ページネーション コントロールにより、パケット リストのページングをより柔軟に行うことができます。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

 - 特定のページに移動

 - 次のページに移動

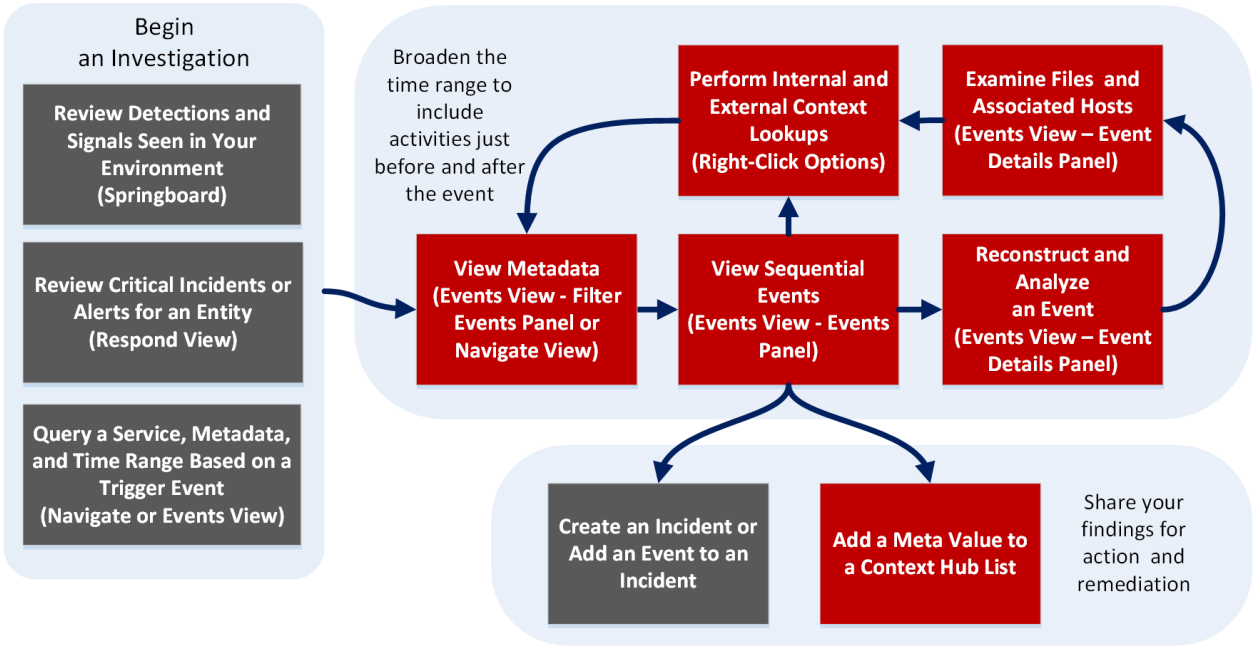
 - 最後のページに移動

 - 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ーの展開、URLとBase64のエンコーディング/デコーディングの実行、ネットワーク イベント、ログ、エンドポイント イベントのダウンロードを実行できる機能が含まれています。テキスト再構築はすべてのタイプのイベント(ネットワーク、ログ、エンドポイント)に使用できます。

ワークフロー



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 イベントビューでメタデータのドリルダウン
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

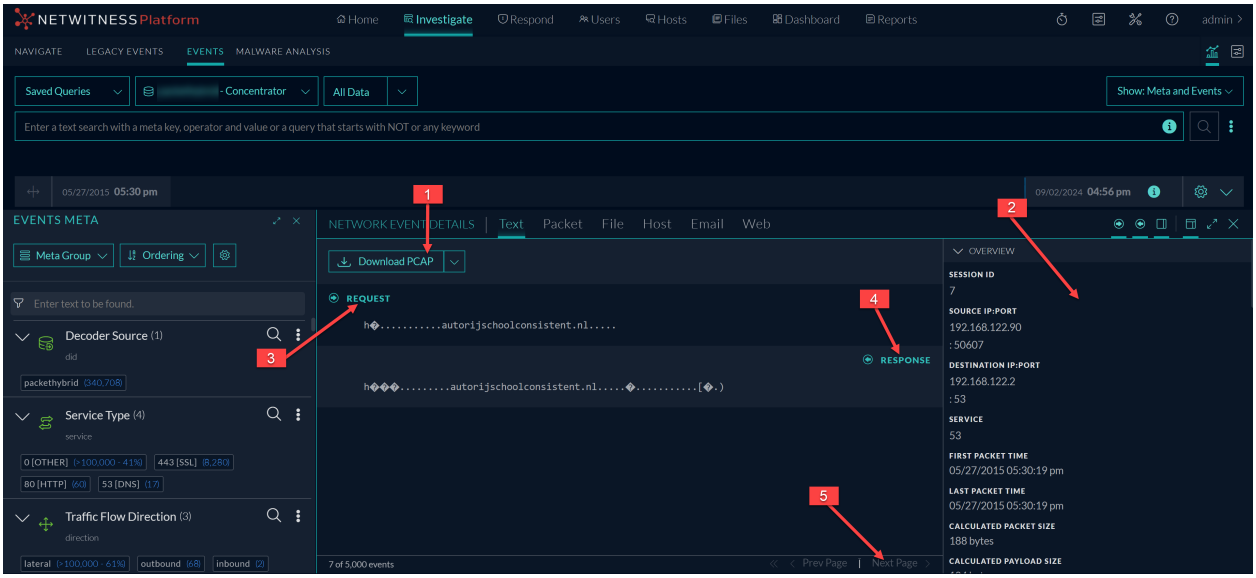
*このタスクは現在のビューで実行できます。

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、「イベントビューでイベントを分析する」を参照してください。

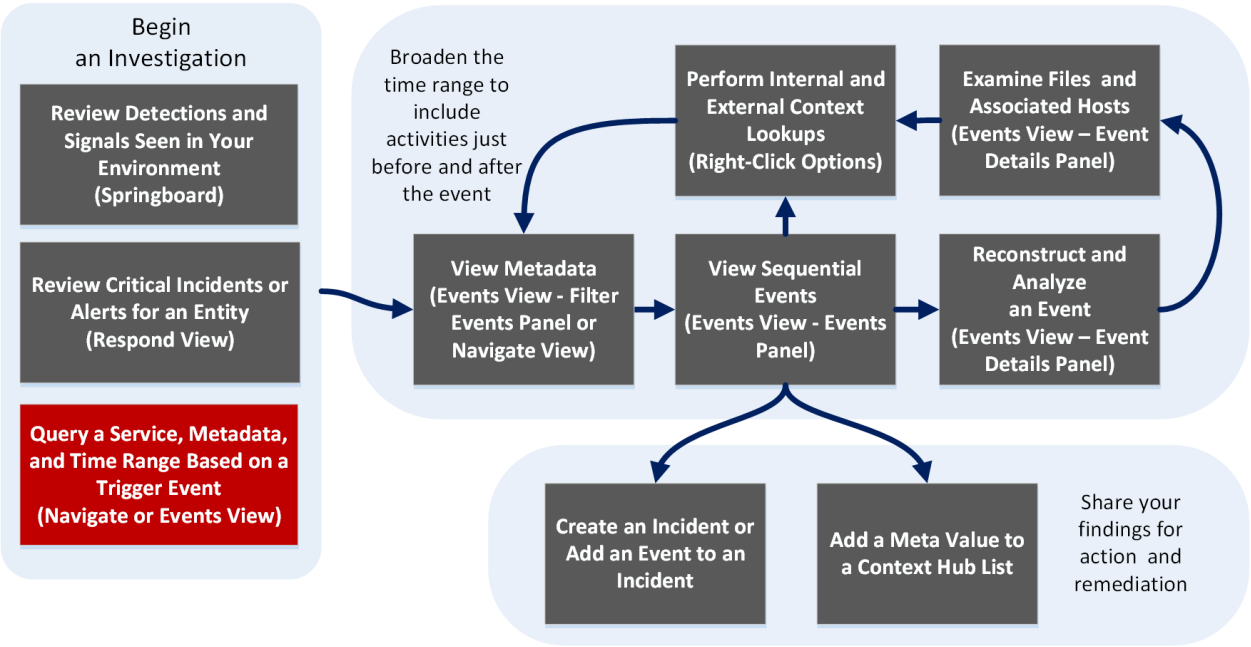


1	ログ、PCAP、ファイルをエクスポートして、より詳細な分析や、他のユーザとの共有を行うためのオプションです。このダウンロード メニューはネットワーク データ用です。
2	［概要］パネルの情報
3	ネットワーク イベントのペイロードには、リクエストとレスポンスが含まれています。これは、パケットのリクエスト側です。
4	これは、パケットのレスポンス側です。
5	ページ操作コントロールで、イベントのリストのページ操作を柔軟に実行できます。使用できないコントロールのイメージはグレー表示になります。たとえば、ページ1を表示しているときには、  とのコントロールがグレー表示になります。  - 最初のページに移動  - 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	*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 イベントビューでメタデータのドリルダウン

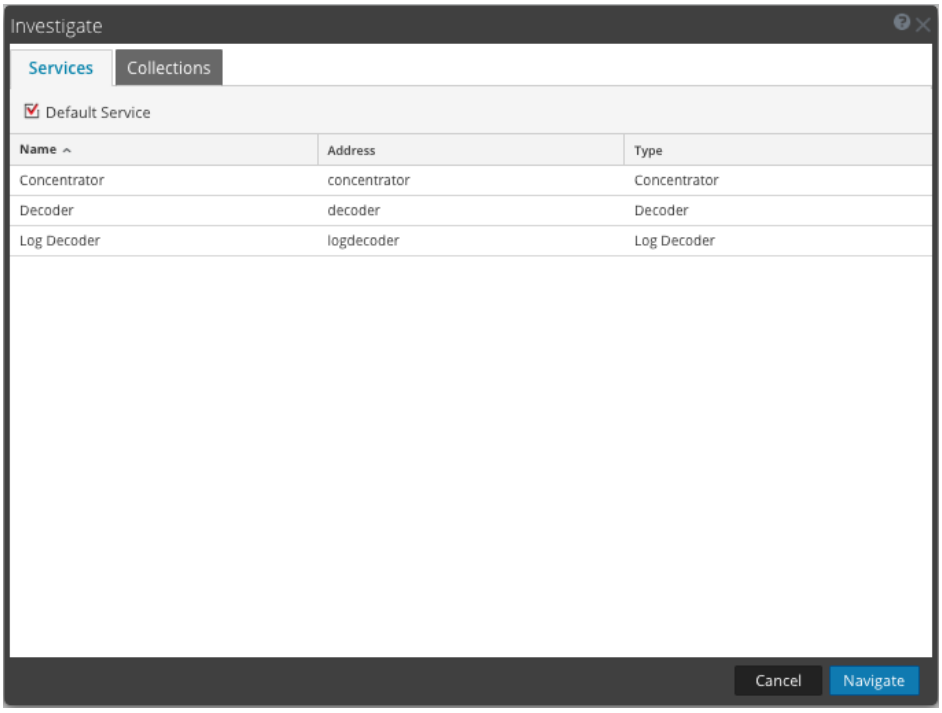
ユーザ ロール	実行したいこと	手順
脅威ハンター	シーケンシャル イベントの表示	[イベント]ビューでの結果のフィルタリング [レガシー イベント]ビューでの結果のフィルタリング
脅威ハンター	イベントの再構築と分析	[イベント]ビューでのイベント詳細の調査 [レガシー イベント]ビューでのイベントの再構築
脅威ハンター	ファイルと関連ホストの調査	[イベント]ビューでのデータのダウンロード [ナビゲート]ビューでのドリルダウン ポイントのエクスポートまたは印刷 [レガシー イベント]ビューでのイベントのエクスポート
脅威ハンター	ルックアップの実行	結果の追加のコンテキストを検索 メタ キ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 [コレクション]の2つのタブがあります。

注 :コレクションは、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。

[コレクション]タブには2つのボタンと、 [Workbench]と [コレクション]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、 [コレクション] パネルからコレクションを選択できます。

[コレクション] パネルには、調査する使用可能なコレクションがリストされます。コレクションを選択すると、 [ナビゲート] をクリックしてコレクションを表示できます。

次の表は、 [コレクション] パネルの機能について説明しています。

機能	説明
名前	コレクションの名前。
タイプ	コレクションのタイプ。
サイズ	コレクションのサイズ。
データ タイプ	コレクション内のデータのタイプ。
作成日	コレクションが作成された日付。

調査]タブ - [ユーザー環境設定]パネル

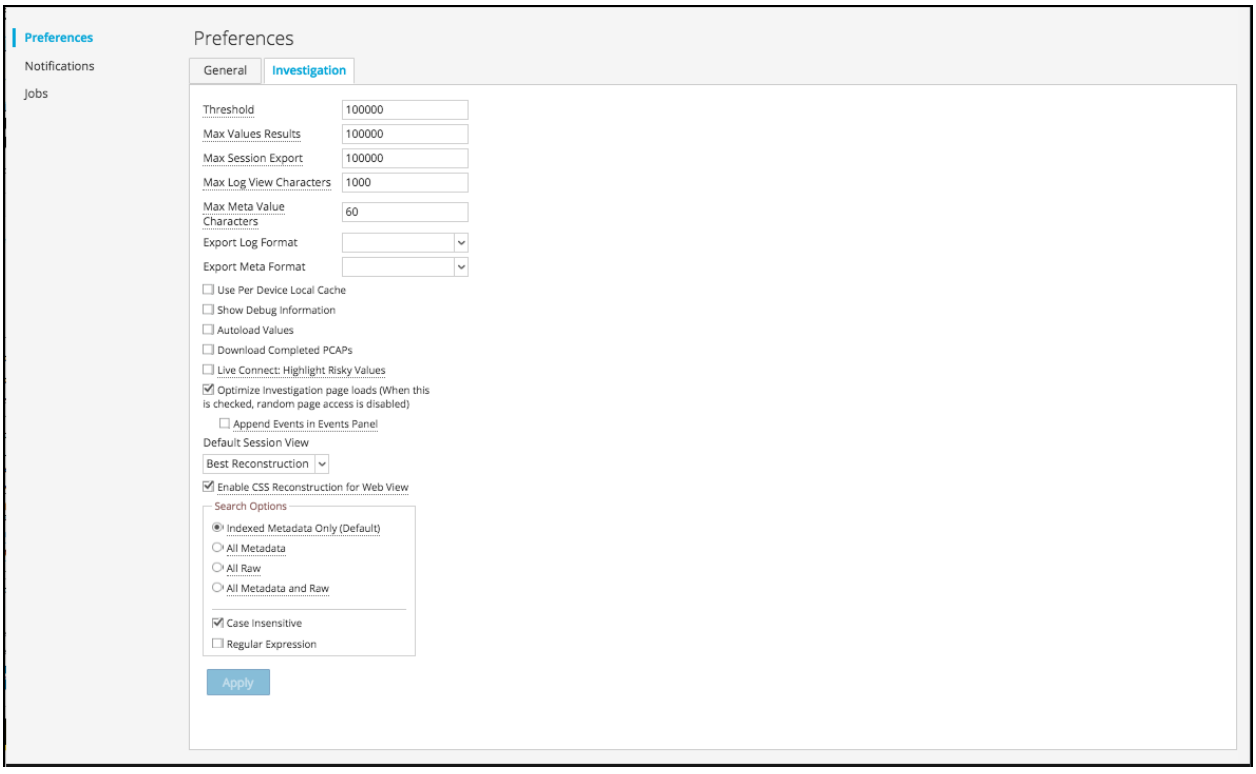
[プロファイル]ビュー> [環境設定]パネル> [調査]タブで、NetWitness Investigateでのデータの分析、イベントの表示、イベントの再構築時のNetWitnessのパフォーマンスと動作に影響を与える、いくつかの環境設定を行うことができます。このタブにアクセスするには、[ナビゲート]ビューまたは [レガシー イベント]ビューから > Profileを選択します。[プロファイル]ビューが表示されたら、**[環境設定]** > **[調査]**を選択します。ユーザ環境設定は、NetWitnessで作業しているときにいつでも変更できます。

関連トピック

- NetWitness Investigateの仕組み
- [ナビゲート]ビュー
- [レガシー イベント]ビュー

簡単な説明

この図は、[調査]タブの例です。次の表では、調査に影響する環境設定について説明します。検索設定の詳細については、「[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。



機能	説明
閾値	この設定は、［ナビゲート］ビューでのロード中にメタ キー値に表示されるカウントを制御します。閾値を高くすると、計算値が正確になります。ただし、閾値を高くすると、ロードにかかる時間が長くなります。閾値に達すると、NetWitnessは、計算値とその計算値に達するまでにかかった時間のパーセンテージ(その値ですべてのセッションをロードするために必要な時間と比較したパーセンテージ) を表示します。 たとえば、**(>100000 - 18%)** と表示された場合、閾値が100000に設定され、閾値が設定されていない場合にロードにかかると想定された時間の18%しかロードの時間がかからなかったことを意味します。デフォルト値は**100000**です。
結果の最大数	この設定は、［ナビゲート］ビューで開いているメタ キーについて、［メタ キー］メニューで［最大まで表示］を選択した場合にロードする値の最大数を制御します。デフォルト値は**1000**です。
最大セッション エクスポート	この設定で、エクスポート可能なセッションの最大数を制御します。デフォルト値は**100000**です。
ログ ビューの最大文字数	この設定は、［**調査**］> ［**レガシー イベント**］> ［**ログ テキスト**］に表示するログ テキストの最大文字数を制御します。デフォルト値は**1000**です。
ログのエクスポート形式	この設定は、調査時にログをエクスポートするためのデフォルトの形式を指定します。使用可能なオプションは、**テキスト**、**XML**、**CSV**、**JSON**です。ログ エクスポート形式のデフォルト値はありません。ここでログの形式を選択しない場合、ログのエクスポートを呼び出すときに、NetWitnessで選択のダイアログが表示されます。［ログのエクスポート形式］ドロップダウン メニューから1つのオプションを選択し、［適用］をクリックすると、設定がすぐに反映されます。
メタのエクスポート形式	この設定は、調査時にメタ値をエクスポートするためのデフォルトの形式を指定します。使用可能なオプションは、テキスト、XML、CSV、JSONです。メタ エクスポート形式のデフォルト設定はありません。ここでメタ値のエクスポート形式を選択しない場合、メタ値のエクスポートを呼び出すときに、NetWitnessで選択のダイアログが表示されます。「エクスポート メタ形式」ドロップダウン メニューからいずれかのオプションを選択し、「適用」をクリックすると、設定がすぐに有効になります。 **注 :** バージョン12.5にアップグレードすると、**エクスポート メタ形式** の設定は保持されず、空白にリセットされます。バージョン12.5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。
デバイスごとのローカル キャッシュを使用	選択したサービスからローカルにキャッシュされるデータの使用を指定することができます。このチェックボックスはデフォルトでオフになっているため、初回ロード後に［調査］ビューにキャッシュされたデータを表示するのではなく、新しいクエリがデータベースに送信されます。このオプションを選択すると、ローカル キャッシュのデータが使用されます。
デバッグ情報の表示	このオプションが設定されている場合、NetWitnessは`where`句を［ナビゲート］ビューの階層リンクの下に表示します。ロードされるメタ値ごとに、ロード時間が表示されます。サービスがBrokerの場合は、各集計サービスでの経過時間が報告されます。デフォルト値は**オフ**です。

機能	説明
イベント パネルのイベントを挿入モードで表示	このオプションを設定すると、［**イベント**］**パネル**に表示されるイベントは、現在表示されているイベントを上書きするのではなく、段階的に追加されます。次のページ アイコンをクリックするたびに、1～25、次が1～50、その次が1～75などのように前のイベントに追加のイベントが付加されます。 **注 :**このオプションは、［調査ページのロードを最適化する］オプションが有効な場合にのみ使用できます。
値の自動ロード	このオプションが設定されている場合、［ナビゲート］ビューにサービスから値が自動的にロードされます。設定されていない場合、NetWitnessには［**値のロード**］ボタンが表示され、値をロードする前に表示オプションを変更できるようになります。デフォルト値は**オフ**です。
完了したPCAPのダウンロード	この設定は、抽出されたPCAPのダウンロードを自動化します。これにより、PCAPファイルをダウンロードしてPCAP形式のデータを扱えるアプリケーション(Wiresharkなど) で開くまでの操作を手動で実行する必要がなくなります。
Live Connect :リスクのある値を強調表示	NetWitness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NetWitness Platformで強調表示する場合は、このオプションを設定します。有効にしない場合、NetWitness Platformではすべてのアドレスが表示されます。デフォルトでは、このオプションはオフになっています。
調査ページのロードを最適化する	［レガシー イベント］ビューでイベントを取得する方法を制御します。このオプションは、デフォルトで有効(オン) に設定されています。有効にした場合、イベント リストには可能な限り高速に結果が返されますが、イベント リストのページ移動機能が無効になります。このチェックボックスをオフにすると、イベント リストのページ移動機能が有効になり、リストの特定のページ(または最後のページ) に移動できるようになります。リスト内の任意のページに移動できるようにすると、イベントを事前に判断するための追加のオーバーヘッドが生じます。
デフォルト セッション表示	この設定では、セッションの再構築を表示する時のデフォルトの再構築のタイプを選択します。デフォルトでは、そのイベントに最適な再構築タイプでイベントが再構築されます。
WebビューのCSS再構築を有効化	この設定では、Webコンテンツの再構築の実行方法が制御されます。有効化すると、Webの再構築にカスケード スタイル シート(CSS) とイメージが含まれるようになり、再構築の表示と元のWebブラウザの表示が一致するようになります。これには、イベントに関連するスキャニングと再構築、ターゲット イベントで使用されるスタイル シートとイメージの検索が含まれます。このオプションは、デフォルトで有効化されています。特定のWebサイトの表示で問題がある場合は、このチェックボックスをオフにします。 **注 :**関連するイメージとスタイル シートが見つからないかWebブラウザのキャッシュにロードされていない場合は、再構築されたコンテンツの外観が元のWebページと一致しない場合があります。また、クライアント側のすべてのjavascriptがセキュリティ目的で削除されるため、クライアント側のjavascriptを経由して動的に実行されるレイアウトまたはスタイルは、再構築では表示されません。

機能	説明
検索オプション	この設定によりデフォルト検索オプションが指定されて、［ナビゲート］ビューおよび［レガシー イベント］ビューでの検索に適用されます。詳細については、「［ナビゲート］ビューと［レガシー イベント］ビューでのテキスト パターンの検索」を参照してください。
適用	環境設定を保存すると、即座に反映されます。

調査]ビュー

調査]ビューは、NetWitness Investigateへのプライマリ エントリー ポイントです。 調査]の下のサブメニューには、 ナビゲート]、 レガシー イベント]、 イベント]、 マルウェア分析]があります。

注： 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	*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 イベントビューでメタデータのドリルダウン
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

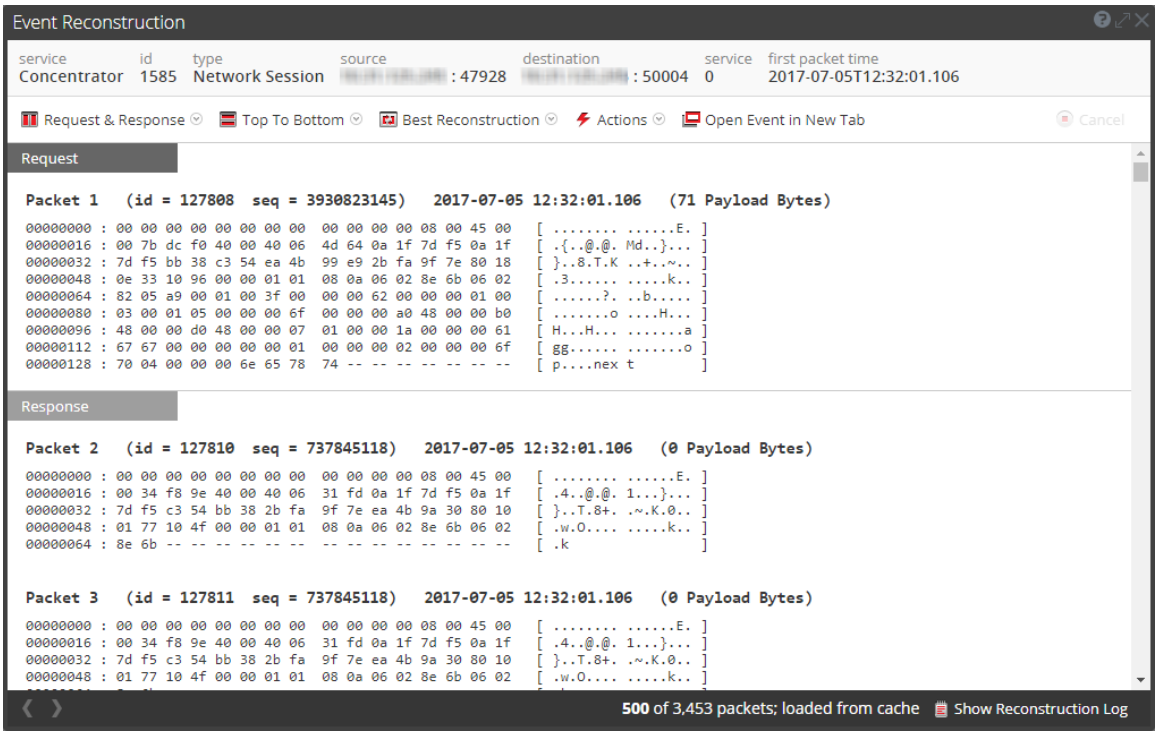
*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [イベント]ビュー

簡単な説明

次の図は、[イベントの再構築]ビューの例です。次の表に、ツールバーのオプションを示します。



機能	説明
リクエストとレスポンス	ビューで次の項目を表示するかどうかを選択するためのドロップダウン メニューを表示します。 • リクエストとレスポンス • リクエスト • レスポンス
構成	情報を上下に並べて表示するか、左右に並べて表示するかを選択するためのドロップダウン メニューを表示します。
再構築]ビュー	表示する情報を選択するためのドロップダウン メニューを表示します。デフォルトでは最適な表示]が選択されています。その他のオプションは次のとおりです。 • メタの表示 • テキストの表示 • 16進数の表示 • パケットの表示 • Webの表示 • メールの表示 • ファイルの表示

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。

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 イベントビューでメタデータのドリルダウン
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

ユーザ ロール	実行したいこと	手順
脅威 ハンター	ルックアップの実行*	結果の追加のコンテキストを検索 メタ キーのルックアップの起動
脅威 ハンター	インシデントの作成またはインシデントへの追加*	[レガシー イベント]ビューでのインシデントへのイベントの追加 [イベント]ビューでのインシデントへのイベントの追加
脅威 ハンター	Context Hubリストへのメタ値の追加*	結果の追加のコンテキストを検索

*このタスクは現在のビューで実行できます。

関連トピック

- NetWitness Investigateの仕組み
- [レガシー イベント]ビューでの結果のフィルタリング
- 結果のダウンロードと処理

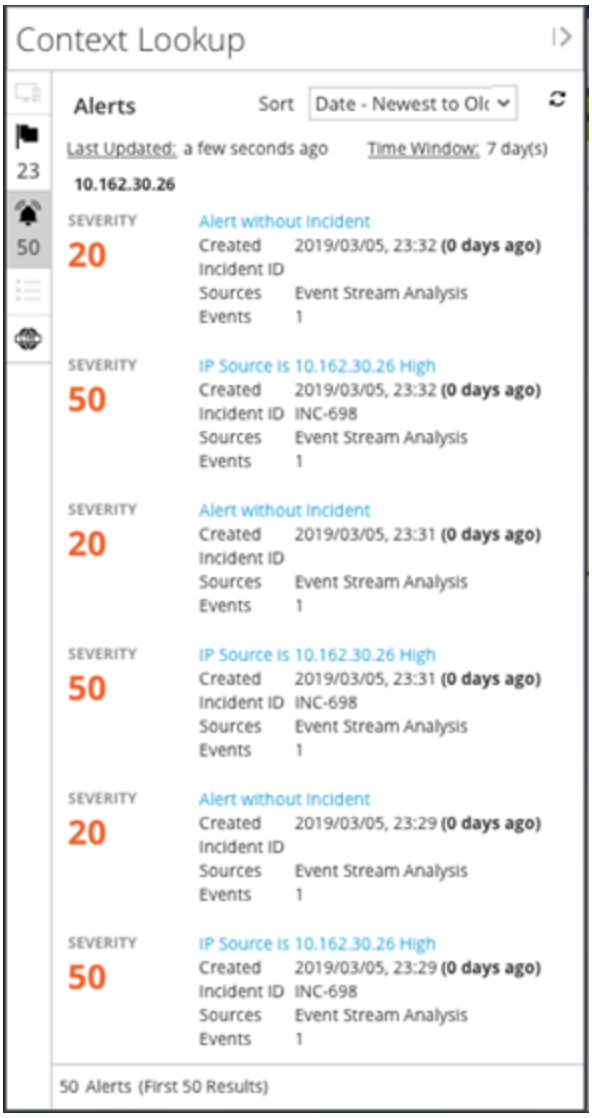
簡単な説明

[レガシー イベント]ビューには、詳細ビュー、リスト ビュー、ログ ビューという、標準提供の3種類の表示形式でイベント データを表示できます。リスト ビューおよび詳細ビューでは、タイムスタンプ、イベント タイプ、イベント テーマ、サイズなど、各イベントの詳細な情報が確認できます。

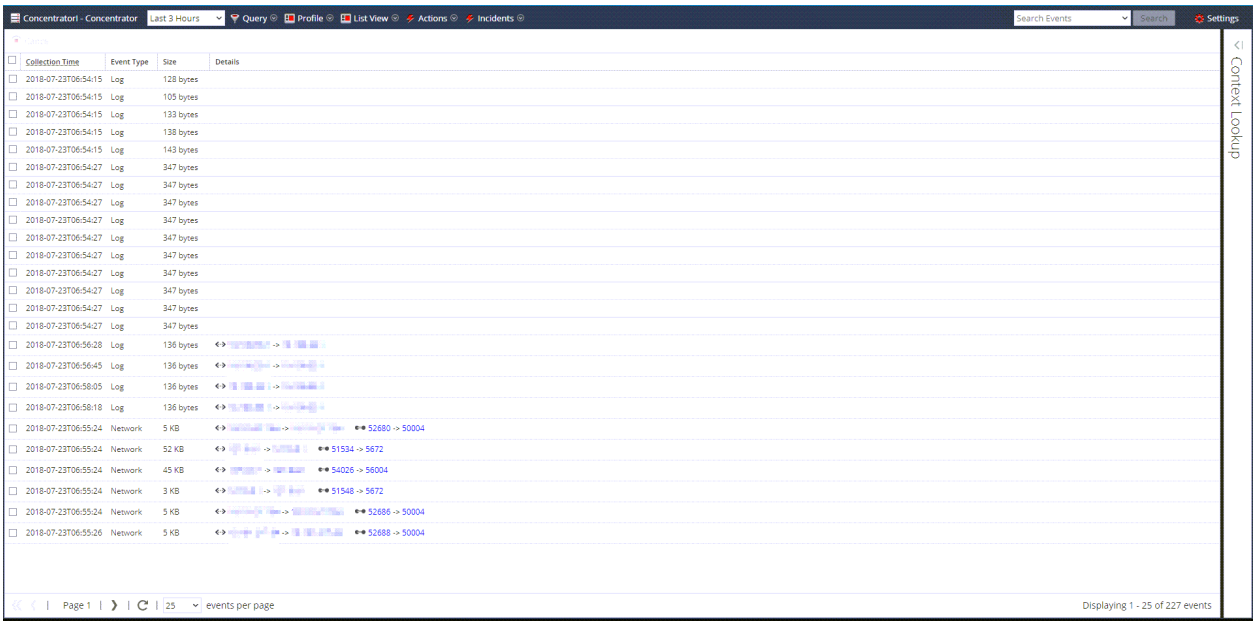
- リスト ビューでは、イベントのソース アドレスおよび宛先 アドレスとポート番号がグリッドに表示されます。
- 詳細ビューでは、イベントについて収集された主なメタデータがページ ビュー形式で表示されます。
- ログ ビューは、ログおよびエンドポイント情報の表示のために最適化されたビューであり、タイムスタンプ、イベント タイプ、サービス タイプ、サービス クラス、ログなど、各ログの詳細情報が確認できます。

[レガシー イベント]ビューの表示をフィルタするには、クエリ、時間範囲設定、プロファイルを使用します。 [レガシー イベント]ビューのいずれの表示形式からも、ファイルの抽出、イベント、エンドポイント イベント、ログ、メタ値のエクスポート、 [イベントの再構築]パネルの表示を行うことができます。 [詳細]ビューでは、 [イベント]ビューでイベントを開くこともできます。

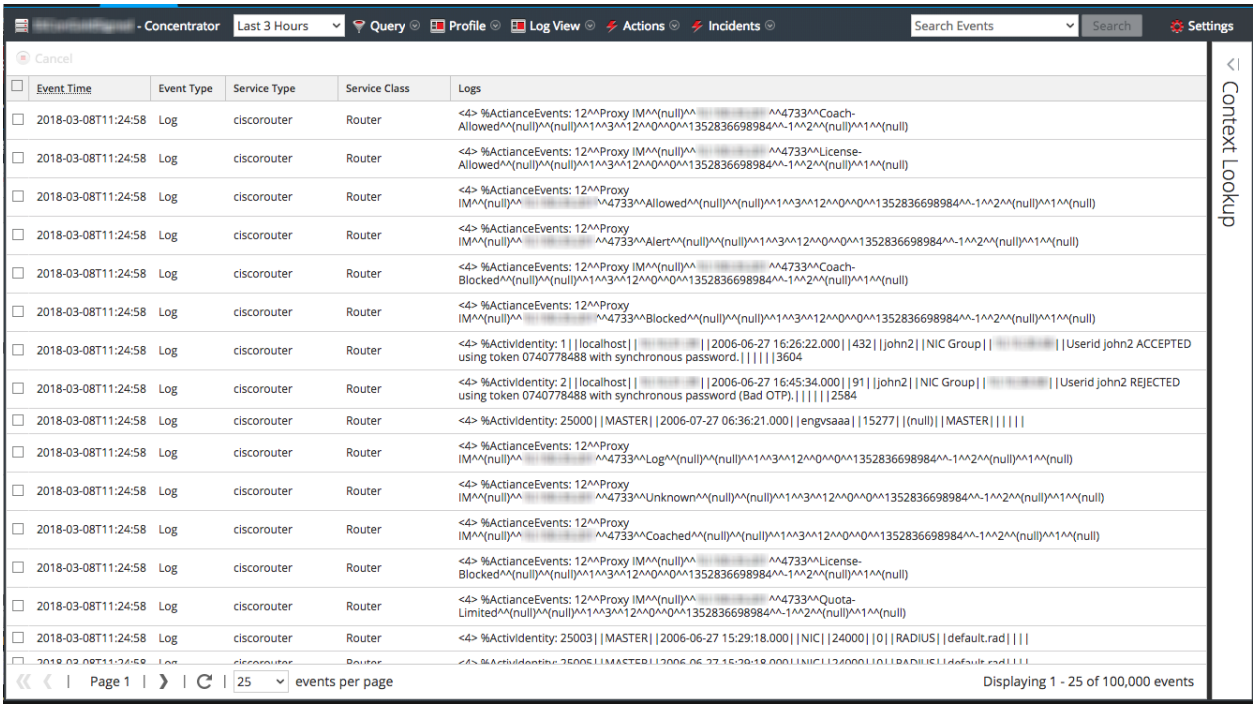
次の図は、詳細ビューのイベントの例です。 [コンテキスト ルックアップ]パネルはContext Hubサービスが構成されている場合にのみ表示されます。



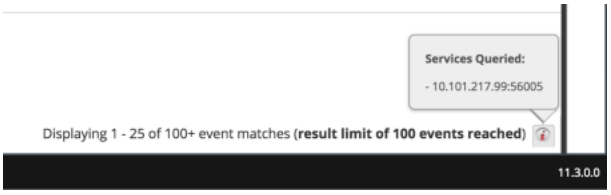
次の図は、リスト ビューのイベントの例です。



次の図は、ログ ビューの例です。



次の図は、フッターに追加された情報を示しています。



詳細説明

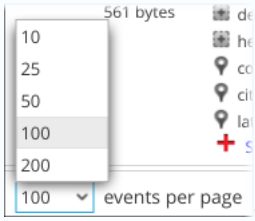
[レガシー イベント]ビューには、上部に以下のオプションを備えたツールバーがあります。

機能	説明
サービスを選択	アイコンの横に選択したサービス名が表示されます。 [調査]ダイアログを開きます。このダイアログでは、イベント リストを表示するサービスを選択できます。
時間範囲	イベント リストに適用する時間範囲を選択するためのドロップダウン メニューが表示されます。標準的なオプションのなかから1つを選択するか、カスタム時間範囲を指定できます。
クエリ	[クエリ]ダイアログが表示されます。ここでは、データをドリルダウンするのではなくクエリレガシー イベント]ビュー クエリを直接入力できます(「[ナビゲート]ビューと [レガシー イベント]ビューでのクエリの作成」を参照してください)。
プロファイル	[プロファイル]メニューを表示します。現在選択されているプロファイルがツールバーに表示されます。メニュー オプションには、標準提供(デフォルト)プロファイルとカスタム プロファイル、およびプロファイルを管理するためのオプションが含まれます。各プロファイルには、メタ グループ、列グループ、イベントの調査時に [ナビゲート]ビュー(メタ グループとクエリ)と [レガシー イベント]ビュー(列グループとクエリ)に適用される開始クエリを含めることができます(「保存済みクエリを使用した調査の共通領域のカプセル化」を参照)。
ビューの選択のドロップダウン	イベント ビューのタイプを選択するためのドロップダウン メニューを表示します。 • 詳細ビューでは、各イベントの詳細情報がページ形式で表示されます。 • リスト ビューでは、各イベントのサマリーが1行ずつテーブル形式で表示されます。 • ログ ビューでは、各ログのサマリが1行ずつログ専用のイベント グリッドに表示されます。 • カスタム列グループでは、ドロップダウン リストから選択した列グループを使用してイベント リストを表示します。 • 列グループの管理では、カスタム列グループの作成および編集のためのダイアログが表示されます。

機能	説明
アクション	[レガシー イベント]ビューのアクションが、ドロップダウン メニューに表示されます。 • PCAPファイルとしてのイベントのエクスポート、ログのエクスポート、エンドポイント イベントのエクスポート、メタ値のエクスポートを行います。 • ポップアップ ウィンドウまたは新しいタブにイベントの再構築を表示します。 • [レガシー イベント]ビューのフィルタをすべてリセットします。
インシデント	Respondで新しいインシデントを作成して選択したイベントを追加するか、Respondの既存のインシデントに選択したイベントを追加します。
検索	[イベントの検索]オプションを表示します。これにより、エクスポートログを指定し、「ナビゲート]ビューと [レガシー イベント]ビューでのテキスト パターンの検索」で説明されている追加のオプションを使用してメタ値形式をエクスポートすることができます。
設定	[レガシー イベント]ビューに関する調査オプションを設定します([プロファイル]ビューでも設定可能です)。これにより、 [レガシー イベント]ビューから移動せずに調査の設定を変更できます。 [レガシー イベント]ビューで変更した設定は、 [プロファイル]ビューでも変更されます(「 ナビゲート]ビューおよび [レガシー イベント]ビューの構成」を参照してください)。

この表では、 [レガシー イベント]ビューのその他の機能について説明します。

機能	説明
Show Additional Meta (イベントの詳細ビュー)	イベントの残りのメタデータを表示します。
Event Analysis (イベントの詳細ビュー)	選択したイベントを [イベント]ビューで開きます。

機能	説明
 (フッター)	ページ移動コントロールを使用すると、イベント リストのページをより柔軟に操作できます。使用できないコントロールのイメージはグレー表示になります。たとえば、ページ1を表示しているときには、《と〈のコントロールがグレー表示になります。 《 - 最初のページに移動 〈 - 前のページに移動 | 3 Page 3 | - 特定のページに移動 〉 - 次のページに移動 》 - 最後のページに移動  - 1ページあたりのパケット数を選択 1ページあたりのイベント数を選択すると、設定はブラウザー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。
100,000個のイベントのうち1～100個を表示(フッター) 100個以上の一致したイベントのうち1～25個を表示(結果制限の100イベントに到達) (フッター)	表示されているイベントの数と、一致したイベントの合計数を表示します。管理者が設定した結果の制限に達した場合、フッターには、さらに結果があるが表示できないことを知らせる通知が含まれます。追加の結果を表示するには、フィルタを絞り込んで結果を減らす必要があります。フッターの情報アイコン をクリックすると、クエリ対象のすべてのサービスのIPアドレスと接続ポート番号が表示されます。

[デフォルト のメタ キーの管 理]ダイアログ

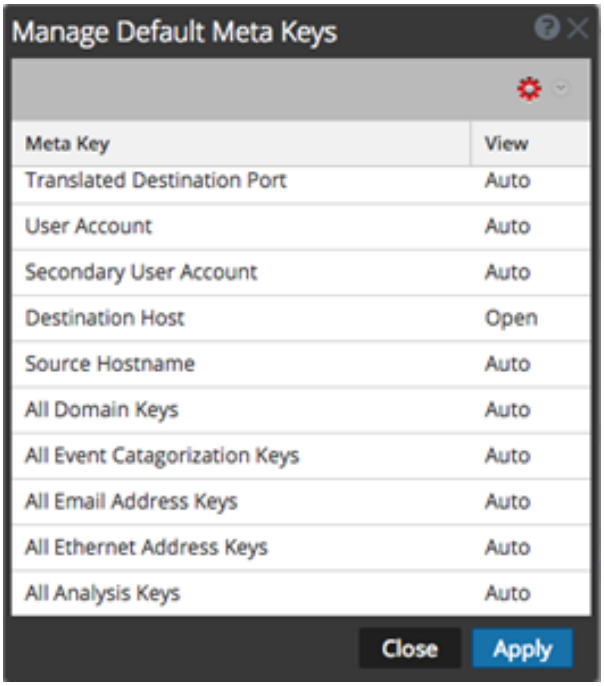
[デフォルト のメタ キーの管 理]ダイアログでは、アナリストは [ナビゲート]ビューの [値]パネルに表 示するメタ キーを指 定できます(「Investigationでのデフォルト メタ キーの管 理と適 用」を参 照) 。これにより必 要なデータをさらに迅 速に見 つけることができ、関 係 のないメタ キーはロードされません。このダイアログにアクセスするには、 [ナビゲート]ビューのツールバーで、 [メタ] > [デフォルト のメタ キーの管 理]を選択します。

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	この列には、各メタ キーに割り当てられているビューのタイプが表示されます。各行でビューをクリックすると、メタ キーを別のデフォルト ビューに割り当てることができます。4つの表示タイプがあります。 • [自動]:サービス インデックス ファイルで指定されている、メタ キーのデフォルトのビューに復元します。 • [折りたたみ表示]:このメタ キーの値はデフォルトで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
⚙	すべてのメタ キーのデフォルト ビューの変更に使用できるドロップダウン メニューが表示されます。4つの表示タイプがあります。 • [自動]:サービス インデックス ファイルで指定されている、メタ キーのデフォルトのビューに復元します。 • [折りたたみ表示]:このメタ キーの値はデフォルトで折りたたまれています。 • [非表示]:このメタ キーの値はデフォルトで非表示になっています。 • [展開表示]:このメタ キーの値はデフォルトでは表示されます。
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、複製できますが、編集または削除することはできません。独自のグループを作成することや、標準提供のグループを複製して編集し、カスタム グループを作成することができます。調査中にメタ グループが有効になっている場合、[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。

メタ グループの機能は ナビゲート ビューと イベント ビューで似ていますが、ユーザー インターフェイスと一部の手順は異なります。

[イベント]ビューの [メタ グループ]メニュー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。

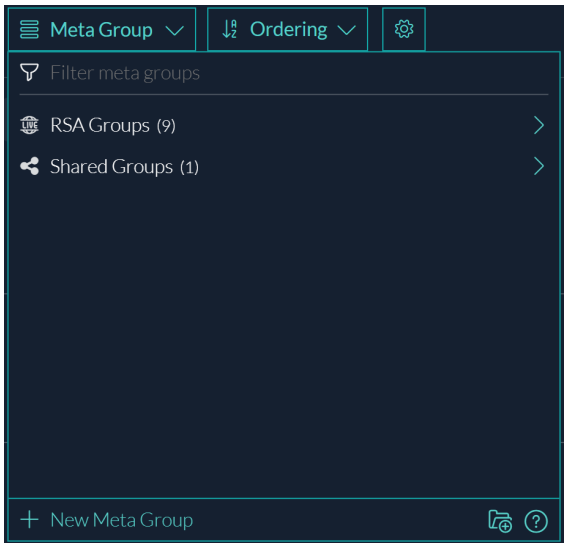
[ナビゲート]ビューの [メタ グループの管理]ダイアログのオプションを使用すると、上記のすべてを実行できるだけでなく、メタ グループをインポートおよびエクスポートすることもできます。詳細については、「メタ グループを使用して関連性の高いメタ キーにフォーカス」を参照してください。

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

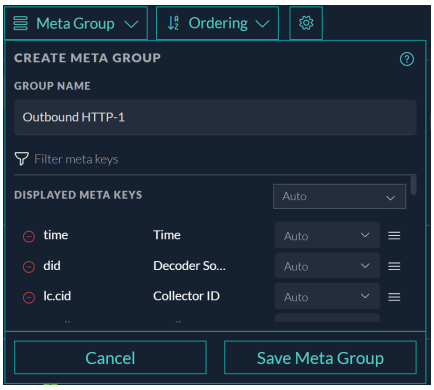
簡単な説明 - [メタ グループ]メニュー、[メタ グループの作成]ダイアログ、[メタ グループの詳細]ダイアログ

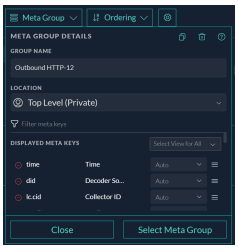
このセクションでは、[メタ グループ]メニュー、[メタ グループの作成]ダイアログ、[メタ グループの詳細]ダイアログについて説明します。次の図は、[メタ グループ]メニューの例です。次の表に、オプションの説明を示します。



機能	説明
可視性オプション	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(ティール = 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。 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
メタ 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、メタ グループのリストを絞り込みます。
メタ グループ リスト	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。
新しいメタ グループ	[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。

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。



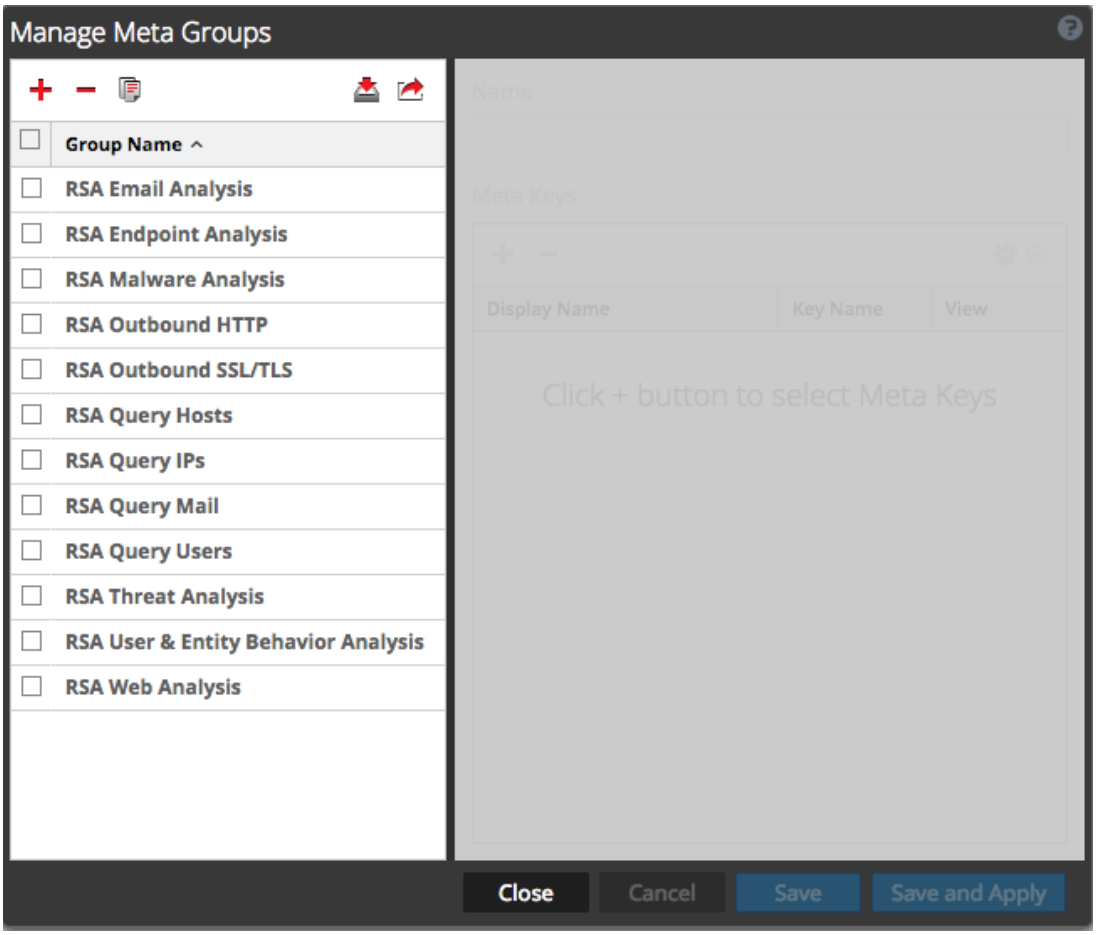


機能	説明
	コピーを編集できるように、メタ グループのコピーを作成します。これは、標準提供グループの独自のコピー、プライベート グループの共有コピー、または共有グループのプライベート コピーが必要な場合に役立ちます。
	現在編集中のカスタム メタ グループを削除します。このアクションは元に戻せず、グローバルに適用されます。メタ グループが共有グループの場合は、誰も使用できなくなります。
グループ名	メタ グループの名前を表示します。64文字以内の一意の名前を指定してください。カスタム メタ グループの名前を編集する場合は、このフィールドに入力します。
共有	メタ グループを共有するかプライベ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。
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。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。

機能	説明
初期表示オプション	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。 - 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。メタキーのグループのデフォルトビューを「オープン」に変更し、一部のメタキーがインデックス化されていない場合、インデックス化されていないメタキーは「自動」に戻ります。 - オープンメタキーはイベントメタパネルにリストされ、値が読み込まれます。 - クローズドメタキーはイベントメタパネルにリストされますが、メタキーを開くまでメタ値は読み込まれません。 - 非表示のメタキーはイベントメタパネルにまったくリストされません。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。
☰	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。
閉じる]ボタン	ダイアログを閉じます。
メタ グループの保存	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。
リセット	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。
メタ グループの更新	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。
メタ グループの選択	メタ グループを適用します。イベント メタ パネルが更新され、選択したメタ グループ内のメタ キーのみが表示されます。

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。 • ［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。 • ［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。

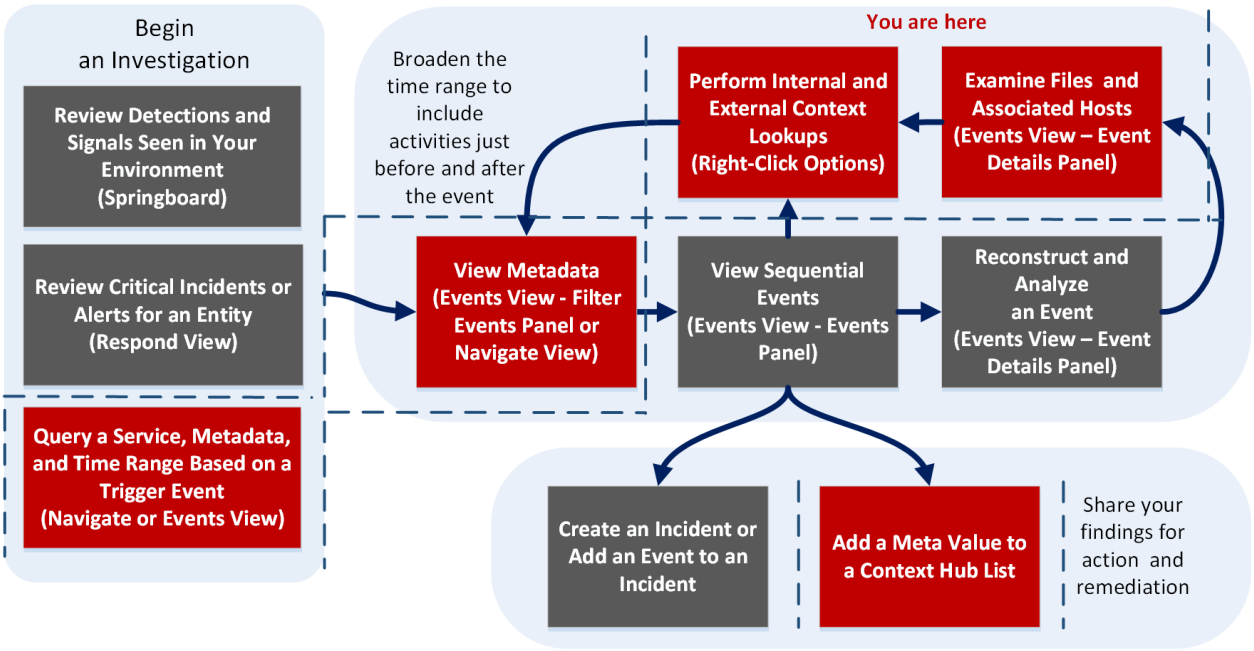
機能	説明
閉じる	ダイアログを閉じます。
キャンセル	すべての変更をキャンセルします。
保存	すべての変更を保存します。
保存して適用	すべての変更を保存して、直ちに適用します。

[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 :デフォルトでは、イベント ビューのイベント メタ パネルがこの機能を提供するため、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	*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 イベントビューでメタデータのドリルダウン
脅威ハンター	シーケンシャル イベントの表示	[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

この図はナビゲート ビューを示しています。



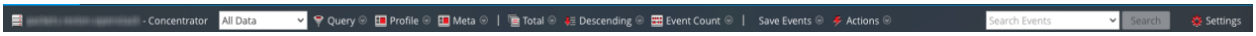
[ナビゲート]ビューは次の機能で構成されます。

- ツールバー
- 一時停止/再ロード ボタンと階層リンク
- 時間バナー
- オプションのデバッグ情報
- 折りたたみ可能なチャート パネル
- 値パネル
- [コンテキスト ルックアップ]パネル
- コンテキスト メニュー

ツールバー

次の図はツールバーの例です。ツールバーからは以下の操作を行うことができます。

- 調査するサービスを変更する。
- 表示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
	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。

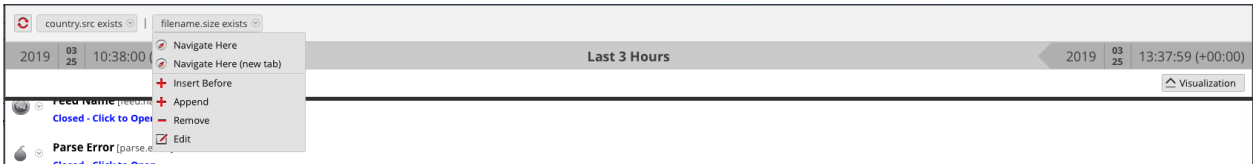
オプション	説明
時間範囲	時間範囲オプションが表示されます。ツールバーには現在選択されているオプションが表示されます(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。選択可能なオプションは次のとおりです。 • すべてのデータ • 直近5、10、15、30分 • 直近1、3、6、12、24時間 • 直近2、5日間 • 早朝 • 午前 • 午後 • 夕方 • 終日 • 昨日 • 今週 • Last Week • カスタム **注**:カスタムの開始時刻と終了時刻を秒単位で指定しても、開始時刻の秒は常に:00に、終了時刻の秒は常に:59に変更されます。たとえば、時間を使用して問題にドリルダウンする場合、ドリル時間は「HH:MM:00～HH:MM:59」と解釈されます。Investigate機能では、この形式で秒が表示されます。
クエリ	[クエリ]ダイアログが表示されます。ここでは、データをドリルダウンするのではなく、カスタムクエリを直接入力できます。このダイアログの詳細については、「[クエリ]ダイアログ」を参照してください。
プロファイル	[プロファイル]メニューを表示します。現在選択されているプロファイルがツールバーに表示されます。プロファイルでは、カスタムメタグループ、デフォルトの列グループ、プレクエリなどを管理および使用できます。プロファイルは、[ナビゲート]ビュー(メタグループとクエリ)、[レガシーイベント]ビュー、および[イベント]ビュー(列グループとクエリ)に適用されます。詳細については、「保存済みクエリを使用した調査の共通領域のカプセル化」を参照してください。
メタ	[メタグループ]メニューを表示します。デフォルトのメタキーまたはカスタムメタグループを使用できます。両方のグループタイプで、設定を変更することができます(「メタグループを使用して関連性の高いメタキーにフォーカス」を参照してください)。

オプション	説明
整列フィールド	[ソート フィールド]メニューが表示されます。ツールバーには現在選択されているオプションが表示されます。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(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。
ソート順	[ソート順]メニューが表示されます。ツールバーには現在選択されているオプションが表示されます。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(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。
集計方法	[集計方法]メニューが表示されます。ツールバーには現在選択されているオプションが表示されます。集計方法は、[値]パネルのメタ キーの結果にのみ適用されます。タイムラインには適用されません。 ドロップダウン メニューには、メタ値の数量(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(「[ナビゲート]ビューでの結果のフィルタリング」を参照してください)。 これらのオプションがどのように適用されるかは、表示されているデータのタイプによって異なります。 パケット データの場合: • [イベント数で集計]を選択すると、セッション数が示されます。 • [イベント サイズで集計]を選択すると、サイズ(バイト)が示されます。 • [パケット数で集計]を選択すると、パケット数が示されます。 ログ データの場合: • [イベント数で集計]を選択すると、ログの数が示されます。 • [イベント サイズで集計]を選択すると、サイズ(バイト)が示されます。 • [パケット数で集計]を選択すると、ログの数が示されます。
イベントの保存	[イベントの保存]メニューが表示されます。このメニューには、イベントに関連づけられているファイルを抽出するオプション、現在のドリルダウン ポイントをPCAP ファイルとしてエクスポートするオプション、現在のドリルダウン ポイントをログ ファイルとしてエクスポートするオプションがあります(「ドリルダウン ポイントのエクスポート」を参照してください)。
アクション	アクション メニューには、[ナビゲート]ビューで実行できるアクションが表示されます(「結果セットの絞り込み」を参照してください)。オプションは[可視化]、[イベント再構築に移動]、[イベント ビューに移動]、[印刷]です。
イベントの検索	現在のイベント セット内でテキスト パターンを検索できます。[検索]フィールドをクリックすると、検索オプションを示すドロップダウン メニューが表示されます。[適用]をクリックすると、選択したオプションが保存され、[レガシー イベント]ビューと[調査]プロファイルの検索オプションも更新されます(「[ナビゲート]ビューと[レガシー イベント]ビューでのテキスト パターンの検索」を参照してください)。

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]設定を有効化していて、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)$$time='2014-05-04 18:50:00"-"2014-05-09 18:59:59(attachment exists) && (tcp.dstport = '80') && (risk.info exists) && time="2014-05-04 18:50:00"-"2014-05-09 18:50:59"
```

また、ロードに要する時間は値パネルの各メタ キーの末尾に表示されます。

時間バナー

階層リンクとデバッグ情報(ある場合) のすぐ下にある時間バナーには、チャートの作成に使用される時間範囲が示されます。次の図は時間バナーの例です。

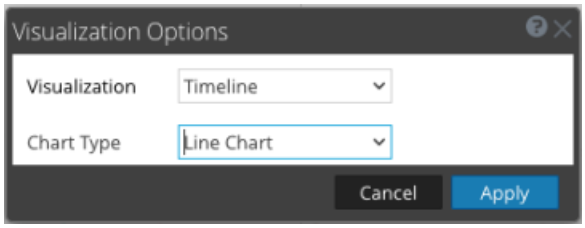


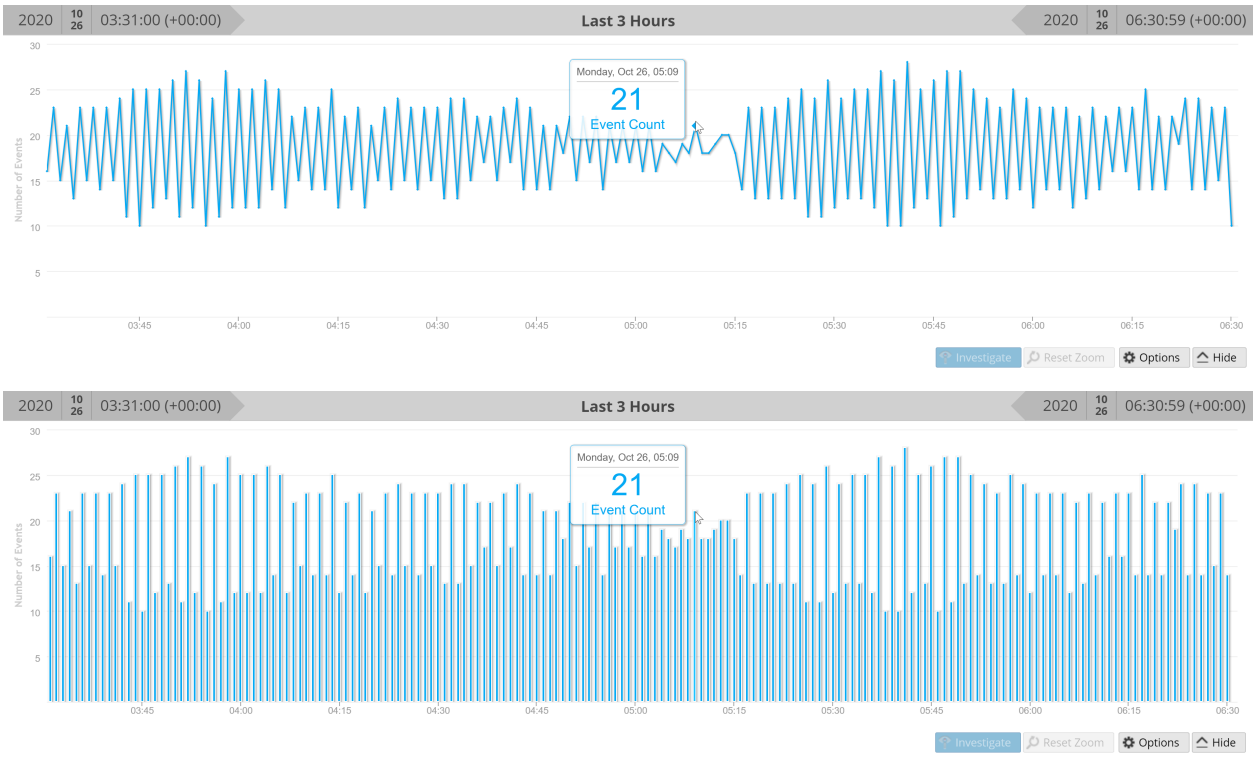
ビジュアル画像

[ナビゲート]ビューの上部には、現在のドリルダウン ポイントが表示されます。これを使用して、 [チャート]パネルのデータをドリル ダウンできます(「 [ナビゲート]ビューでの結果のフィルタリング」を参照してください) 。チャートの表示では、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。



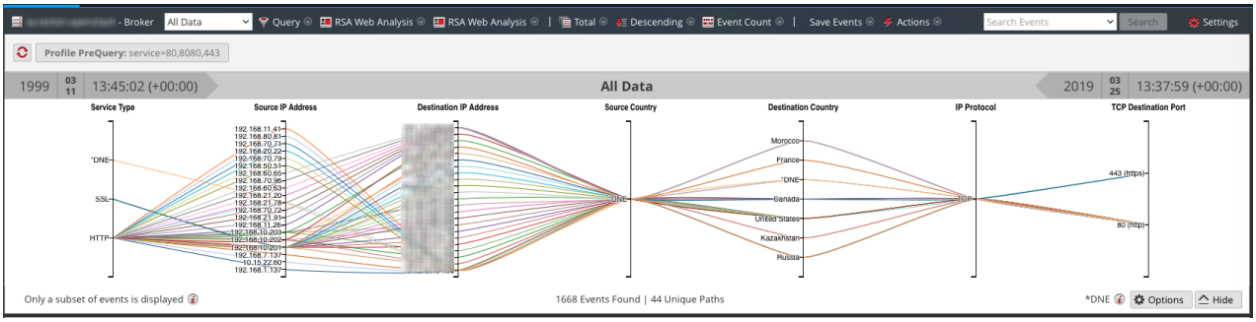


タイムラインには、指定したサービスと時間範囲のアクティビティが表示されます。表示の形式は、［オプション］メニューでの選択に応じて、折れ線グラフか棒チャートになります。

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、プロファイル グループを選択します。



機能	説明
軸	各軸はメタ キーです。メタ キーの数は、チャートのロード時間に影響します。すべてのメタ キーがロードされますが、メタ キーあたりのイベント数は制限されています。
行	線はイベントを表し、軸上の値を接続することで、複数のメタ キー間の相関関係を示します。
オプション	[チャート オプション] ダイアログが表示されます。データ ポイントは折れ線チャート(デフォルト) 、棒チャート、座標チャートのいずれかで表示できます。チャートのタイプを選択すると、関連するオプションが表示されます。
イベントのサブセットのみが表示されます。	このメッセージは、値パネルのすべてのイベントがチャートに表示されているわけではないことを示す通知メッセージです。値パネルで軸を削除するか、データをフィルタすると、すべてのイベントを表示できる場合があります。
見つかったイベントの数 | 一意のパスの数	チャートに表示されているイベントの総数とチャートに表示されている一意のパスの数の比率が表示されます。 [すべてのメタ キーが1つのイベントに存在する必要があります] オプションを設定すると、チャートが再描画され、目的が明確で分かりやすくなります。
DNE	このメタ キーの値がイベント内にないことを示します。

座標表示の [チャート オプション] ダイアログでは、チャートに含めるメタ キーを選択できます。

機能	説明
チャートの選択	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

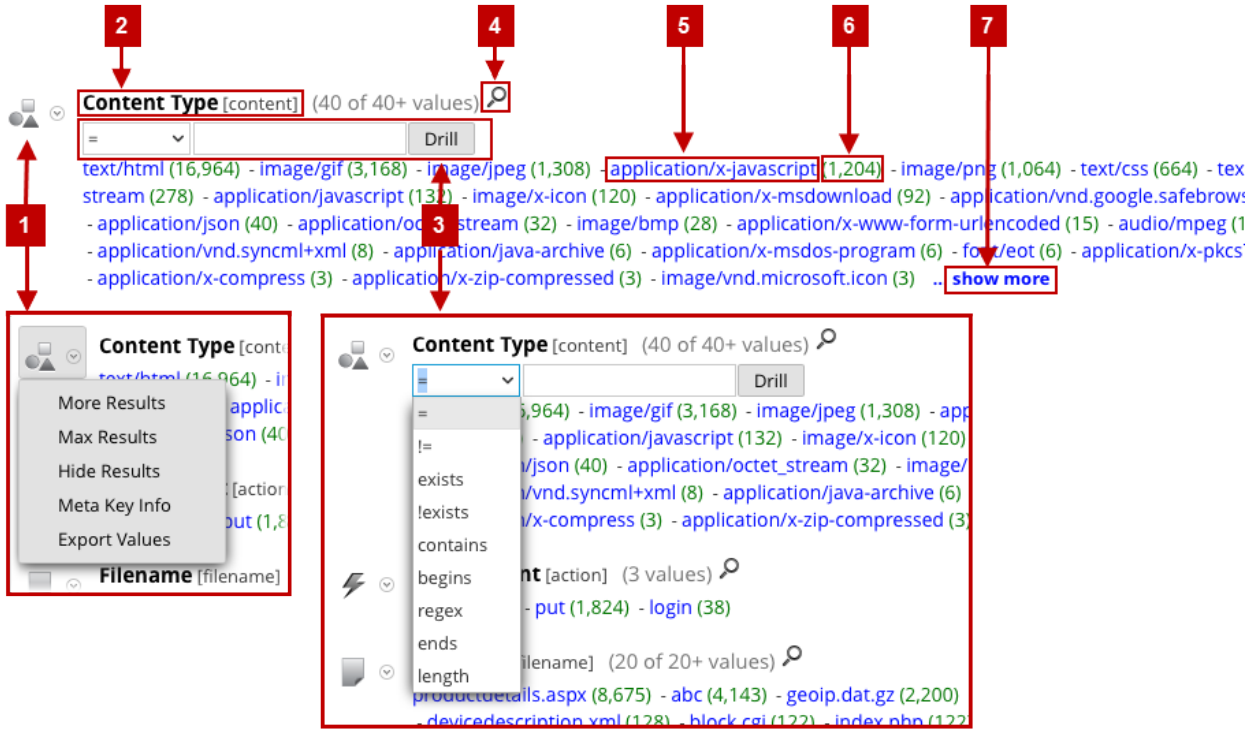
機能	説明
すべてのメタ キーが1つのイベントに存在する必要があります	チャートに表示するデータを、選択したメタ キーをすべて含んでいるイベントのみに制限します。これにより、目的が明確で整然としたチャートになります。
	座標表示チャートへのキーの追加]ダイアログが表示され、チャートに軸を追加できるようになります。この機能は、デフォルトのメタ キーと追加のメタ キーとの間の関係を調べる場合に便利です。
	選択したキーを削除して、チャートの軸に表示されないようにします。これにより、チャートが整然とし、より多くのデータ ポイントをチャートに含められるようになります。
	チャートのメタ キーを、現在のドリルダウン 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。 • デフォルトのメタ キーから追加 • メタ グループから追加 いずれのオプションにも、メタ キーを選択するためのドロップダウン リストがあります。
選択したメタ キーの追加オプション	メタ キーの追加方法に関するオプションにより、次の操作を実行できます。 • 現在のキーのリストを置き換え • 現在のキーのリストの後に挿入 • 現在のキーのリストの先頭に挿入
キャンセル	キーを追加せずにダイアログが閉じられます。
追加	ダイアログが閉じられ、選択したキーが指定したとおりに追加されます。

値パネル

［ナビゲート］ビューの主要機能である［値］パネルには、調査中のサービスで見つかったメタ キーとメタ値が表示されます。［値］パネルでのデータの分析手順については、「［ナビゲート］ビューでの結果のフィルタリング」を参照してください。



注：インデックスなしのメタ キーについては、タイトル、値、数でのドリル ダウンができません。これらのメタ キーの値と数は黒いテキストで表示されます。

1 ［値］パネルのメタ キーには、そのメタ キーに適用できるアクションを含んだドロップダウン メニューがあります。オプションを選択して、現在のビューにおけるメタ キーの結果の表示方法を変更できます。現在のビューのメタ キー表示に対して行った変更は、ページの表示を更新するか、［ナビゲート］ビューのツールバーで新しいサービスを選択するまで維持されます。「［値］パネルでのデータのドリルダウン」を参照してください。

ページの表示を更新すると、［デフォルトのメタ キーの管理］ダイアログで定義されているとおりに、メタ キーの現在のビューが復元されます(「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

	• 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。メタキーのユーザーフレンドリな名前が表示され、その後に括弧で囲まれたメタキーのインデックス ファイル名が表示されます。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。 **注記**:調査でメタ キーに使用されるエイリアスのリストを取得するには、管理者に問い合わせてください。エイリアスが使用されると、［検索］ダイアログには結果が表示されません。メタ キーのクエリには、エイリアスを使用するのではなく、右クリックのクエリ機能または［クエリ］ダイアログを使用する必要があります。
5	見つかったメタ キーに関連づけられたメタ値。設定に応じて、メタ値の名前順、またはメタ値が見つかったイベント数順に表示されます。
6	メタ値を含むイベントの数。
7	ロードする値の数は、調査の環境設定の表示スレッド値によって指定されます。前の例では、メタ キーは**Content Type**で、40個以上ある値のうちの40個が現在表示されています。 **表示範囲の拡大**］をクリックすると、追加の値を表示できます。セッションで特定のメタに対して見つかったインスタンスの数。

［値］パネルのロード動作

デフォルトのビューは、デフォルトのメタ キーと折りたたみ表示されたインデックスなしのメタ キーで構成され、過去3時間の収集データが表示されます。メタ グループ内のメタ キーは、NetWitness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のレポート WHERE句に直接コピーできます。

ロード完了

現在のドリルダウン ポイントで見つかった各メタ キーの値 (青のテキスト) とその数 (緑のテキスト) のリストが表示されます。表示されているデータの特定のサブセットを詳しく調べるには、調査する値をクリックします。表示が更新され、新しいドリルダウン ポイントに移動します。ツールバーのオプションを使用して、値のソート方法と集計方法を指定することもできます。

[クエリ]ダイアログ

[ナビゲート]ビューまたは [レガシー イベント]ビューでは、メタ キーや値をクリックする代わりにクエリを作成して、メタ データをドリル ダウンすることができます。クエリ作成のためのダイアログには、使用可能なメタ キーや演算子がドロップダウン リストで表示される構文ヘルプが用意されています。このダイアログにアクセスするには、 **[ナビゲート]**ビューまたは **[レガシー イベント]**ビューのツールバーで **[クエリ]**を選択します。

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 ビューでメタデータのドリルダウン
脅威ハンター	シーケンシャル イベントの表示	[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

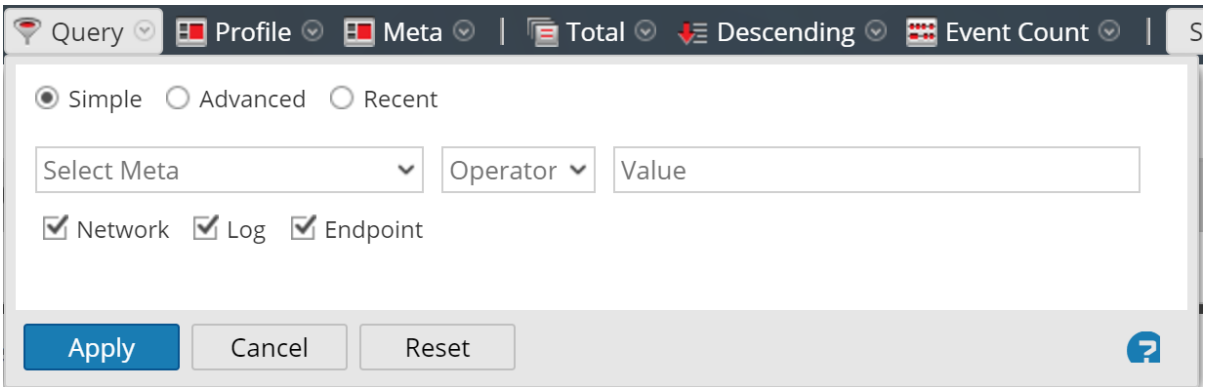
ユーザ ロール	実行したいこと	手順
脅威 ハンター	Context Hubリスト へのメタ 値の追加	結果の追加のコンテキストを検索

*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

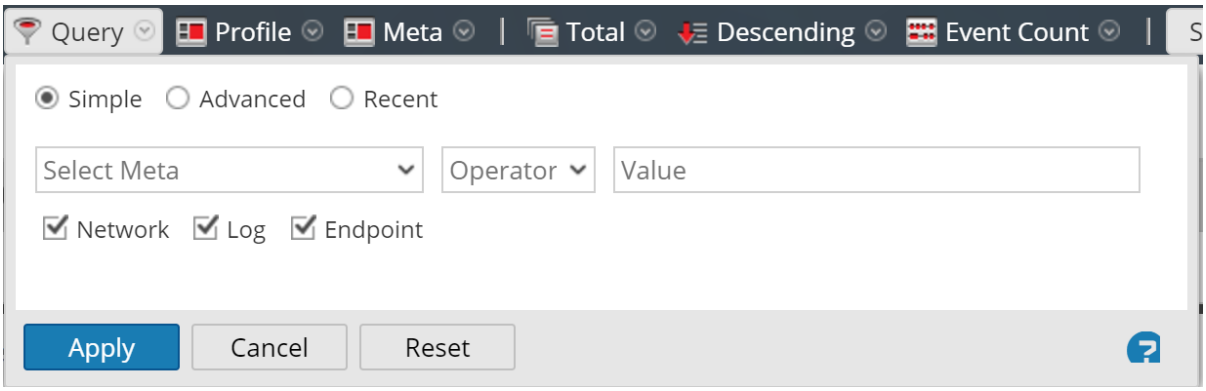


[クエリ]ダイアログには次の3つのビューがあります。

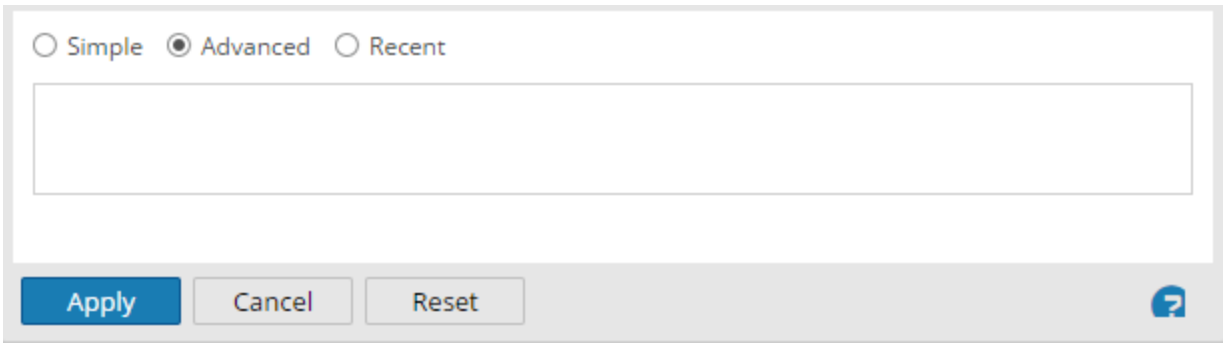
- シンプル
- 拡張
- 直近

[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。

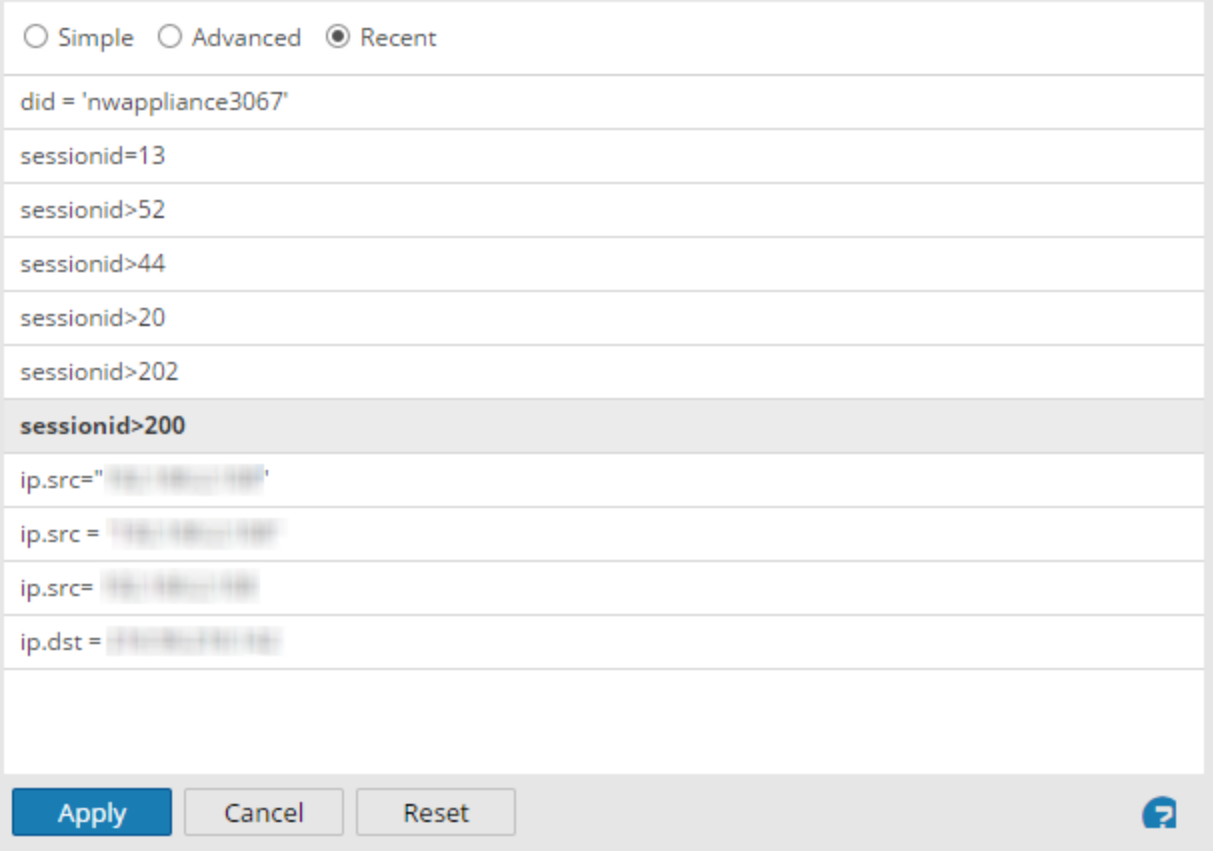
[シンプル]ビュー



[詳細]ビュー



最近実行したクエリ]ビュー



次の表は、 [クエリ]ダイアログの機能について説明しています。

機能	説明
メタの選択	メタ グループのドロップダウン リストを表示します。
演算子	演算子 (=、NetWitness!=、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ー キーのドロップダウン リストが表示され、入力内容に応じて演算子のドロップダウン リストが表示されます。クエリ ボックスに入力されている式が無効な場合は、ボックスの近くに警告が表示されます。クエリが有効になると、警告は消えます。
クエリ リスト	[最近実行したクエリ]ビューで、最近実行したクエリのリストからクエリを選択します。クエリをダブル クリックすると、自動的に適用されます。

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。

[保存済みクエリ]ダイアログ

保存済みクエリは、[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(「保存済みクエリを使用した調査の共通領域のカプセル化」を参照)。同じ保存済みクエリはすべてのビューで共有され、スプリングボード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の保存済みクエリは、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。

保存済みクエリはそれぞれ、メタ グループや列グループを指定しており、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ることもあります。

保存済みクエリには次のような特徴があります。

- 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)。
- 保存済みクエリを有効にすると、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)。

クエリ プロファイルの管理は、[プロファイルの管理]ダイアログ、[保存済みクエリの作成]ダイアログ、[保存済みクエリの詳細]ダイアログで行うことができます。

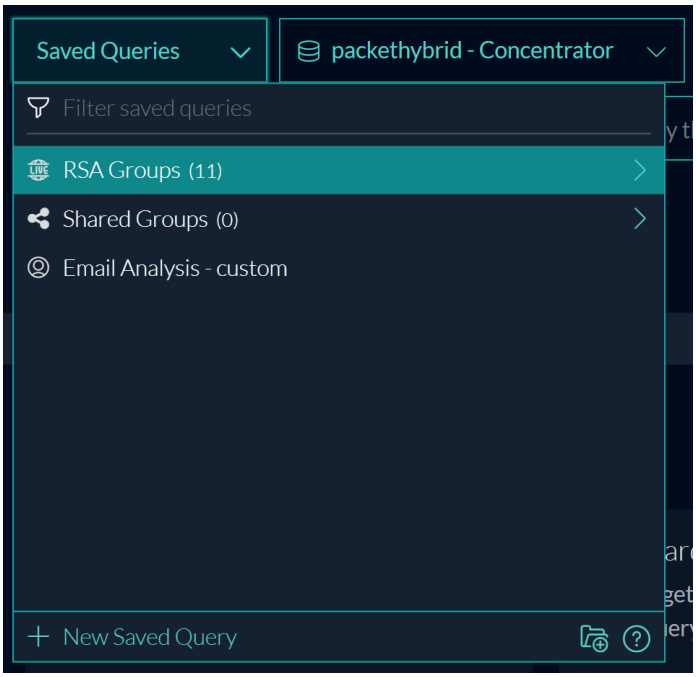
- [プロファイルの管理] ダイアログは、ナビゲート ビュー、レガシー イベント ビュー、およびイベント ビュー用です。このダイアログにアクセスするには、**[ナビゲート]**ビューまたは**[レガシー イベント]**ビューのツールバーで**[プロファイル]** > **[プロファイルの管理]**を選択します。
- **[保存済みクエリの作成]**ダイアログは、[イベント]ビューから開くことができます。このダイアログにアクセスするには、**[イベント]**ビューのクエリ バーで**[保存済みクエリ]** > **[新しい保存済みクエリ]**を選択します。
- **[保存済みクエリの詳細]**ダイアログは、[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**[保存済みクエリ]**を選択して、カスタム保存済みクエリ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
- 保存済みクエリ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 - [保存済みクエリ]メニュー、 [保存済みクエリの作成]ダイアログ、[保存済みクエリの詳細]ダイアログ

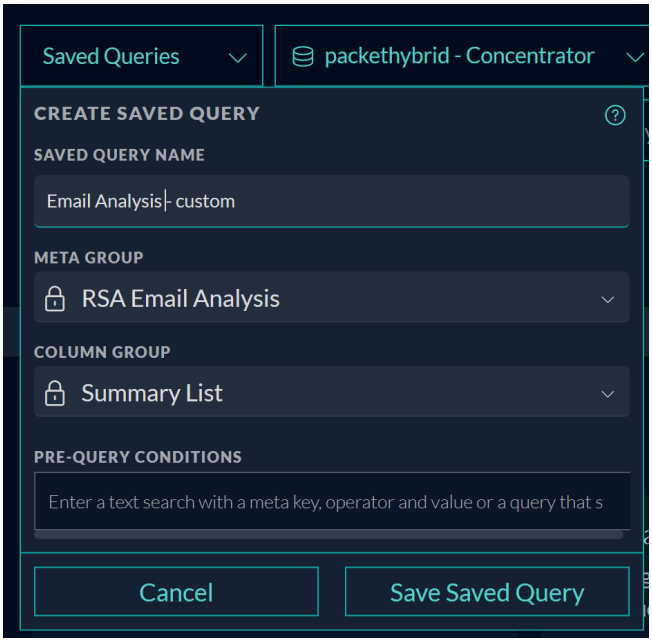
このセクションでは、 [保存済みクエリ]メニュー、 [保存済みクエリの作成]ダイアログ、および [保存済みクエリの詳細]ダイアログについて説明します。次の図は、 [保存済みクエリ]メニューの例です。表にはオプションの説明が記載されています。左側の例では、標準提供の保存済みクエリがハイライト表示されているため、情報アイコンが表示されています。

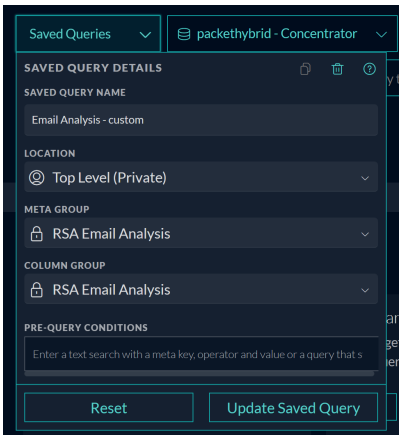


機能	説明
可視性オプション	リストに表示される保存済みクエリのタイプを制御します。可視性オプション([**プライベート**]、 [**共有**]、 [**RSA**]) を任意に組み合わせて使用できます(ティール = 選択済み、黒 = 未選択) 。初期状態では、どのボタンも選択されていないため、すべてのクエリタイプが表示され、3つのボタンすべてが選択されている場合と同じ結果になります。表示オプションは、 [保存済みクエリの絞り込み]フィールドのテキストと連動します。表示オプションによって標準提供の保存済みクエリ(クエリ名に「RSA」を含む) が非表示になっている場合に、「RSA」を含んだ名前を検索すると、リストは空になります。 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

機能	説明
保存済みクエリの絞り込み	テキストの入力に合わせて、そのテキストを含む保存済みクエリ プロファイル名のみが表示されるように、保存済みクエリのリストを絞り込みます。
保存済みクエリ リスト	クエリのリストには、カスタムと標準提供の保存済みクエリが含まれており、それらは名前の前にあるアイコンで区別されます。例では、「Email Analysis - custom」がカスタムの保存済みクエリで、「RSA Email Analysis」は標準提供の保存済みクエリです。
新しい保存済みクエリ	[保存済みクエリの作成]ダイアログを表示します。このダイアログでは、カスタム クエリを作成できます。

左側の図に示す[保存済みクエリの作成]ダイアログを使用して、カスタムの保存済みクエリを定義できます。図に示す[保存済みクエリの詳細]ダイアログでは、カスタムの保存済みクエリを編集できます。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。





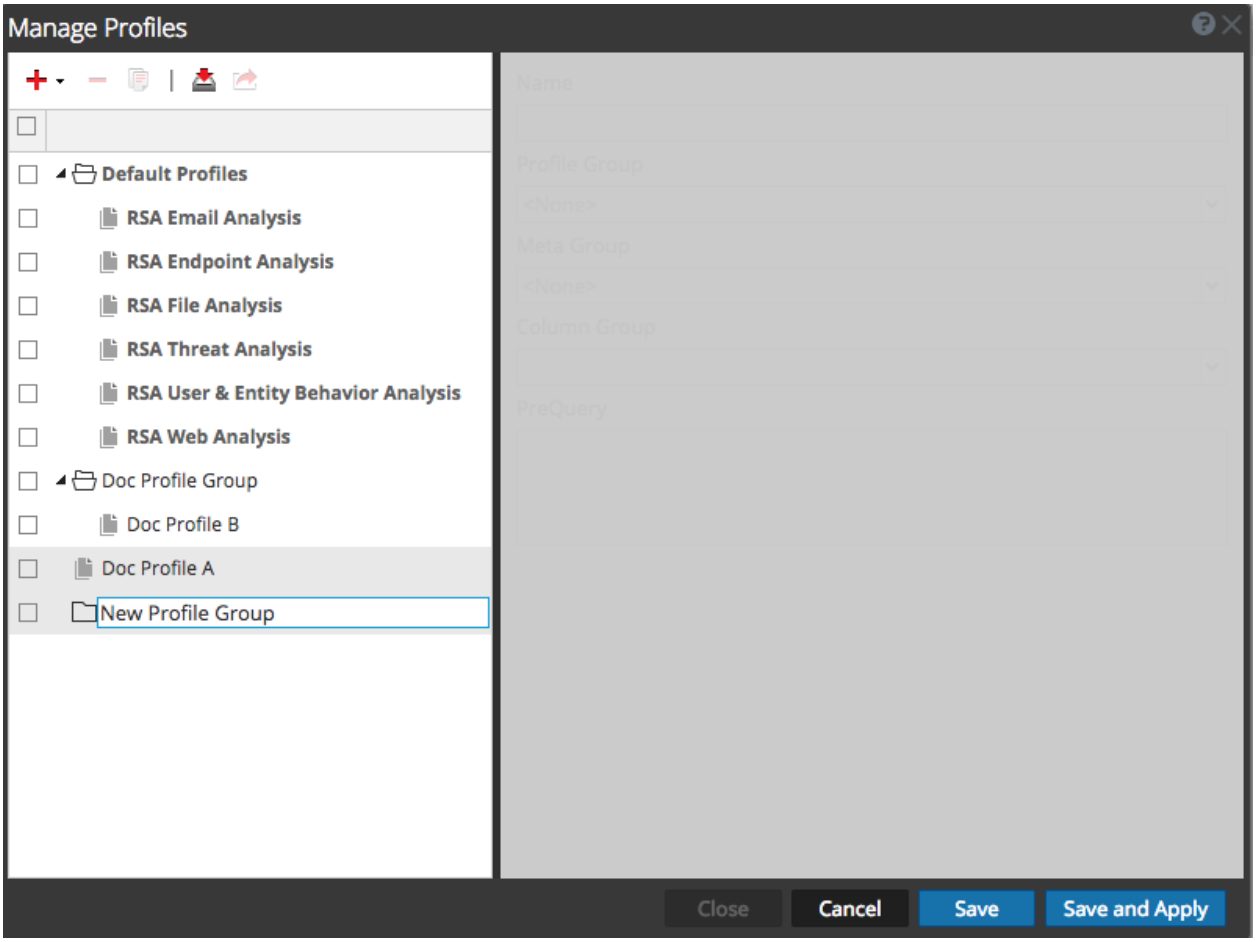
機能	説明

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。
	『保存済みクエリの詳細』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。
保存済みクエリ名	クエリ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 クエリでは、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 クエリでは、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を定義します。新しい保存済みクエリ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 クエリでは、『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。

機能	説明
保存済みクエリの保存	「保存済みクエリの作成」ダイアログにのみ表示され、新しいクエリを保存します。
リセット	「保存済みクエリの詳細」ダイアログにのみ表示され、編集したクエリを前回保存した状態に戻します。
保存済みクエリを更新	「保存済みクエリの詳細」ダイアログにのみ表示され、編集したクエリに変更を適用します。
保存済みクエリを選択	保存済みクエリを適用します。

簡単な説明 - 「プロファイルの管理」ダイアログ

次の図は「プロファイルの管理」ダイアログの例で、複数のプロファイル グループが表示されています。



ダイアログの左側にある [プロファイル] パネルには、使用できるプロファイルが表示されます。ここでは、プロファイルを追加、削除、インポート、エクスポートできます。次の表は、 [プロファイル] パネルのフィールドについて説明しています。

フィールド	説明
	[プロファイルの管理] ダイアログの右側にある [設定] パネルを使用して、新しいプロファイルを追加します。
	選択したプロファイルを削除します。プロファイルが削除される前に、確認ダイアログが表示されます。
	選択されたプロファイルのコピーを作成します。
	[プロファイルのインポート] ダイアログを表示します。ここでファイルをアップロードできます。
	選択したプロファイルをPCにエクスポートします。
プロファイル名	すべてのプロファイル名のリストを表示します。

ダイアログの右側にある [設定] パネルには、プロファイルを構成するためのオプションが表示されます。このパネルは、1つのプロファイルが選択されている場合にのみ使用できます。次の表は、 [設定] パネルのフィールドについて説明しています。

機能	説明
名前	プロファイルの名前を表示します。
メタ グループ	使用できるメタ グループのリストが表示されたドロップダウン メニューを表示します。
列グループ	使用できる列グループのリストが表示されたドロップダウン メニューを表示します。標準提供の列グループと以下の3つのグループをデフォルトで使用できます。 • リスト ビュー • 詳細ビュー • ログ ビュー
プレクエリ	調査する結果をフィルタするための制限クエリを定義します。このクエリは、このプロファイルが適用されている間使用されます。プレクエリは、 [ナビゲート] ビューおよび [イベント] ビューで送信されるすべてのクエリに適用されます。プレクエリの例を次に示します。 `'service=80,25,110'.`

以下の表は、ボタンについての説明です。

フィールド	説明
閉じる	ダイアログを閉じます。
キャンセル	すべての変更をキャンセルします。

フィールド	説明
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。

[スプリングボード パネルの作成]ダイアログ

[スプリングボード パネルの作成]ダイアログでは、[イベント]ビューで選択したクエリーからスプリングボード パネルを作成できます。任意の数のフィルターをクエリー検索バーで追加し、それらをスプリングボード パネルに変換することができます。これで、アナリストがスプリングボード パネルを使用して、結果の検出と監視を実行することができます。

このダイアログにアクセスするには、**調査**] > [**イベント**]ビューでのサービスの調査中に、クエリー検索バーでクエリーを追加し、ツールバーから  > [**スプリングボード パネルの作成**]を選択します。

重要:必ず、最初にスプリングボード パネルでカスタム プライベート ボードを作成してください。

実行したいことは何ですか?

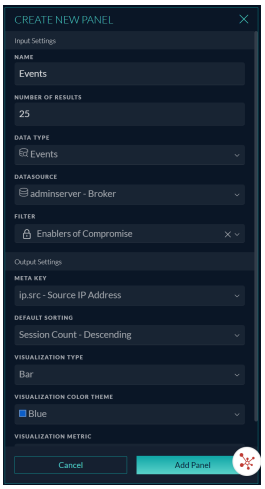
ユーザ ロール	実行したいこと	手順
インシデント対応者または脅威ハンター	自分の環境で確認されている検出事項とシグナルを確認する	NetWitness Platformスタート ガイド
脅威ハンター	サービス、メタデータ、時間範囲のクエリを実行*	[イベント]ビューでの調査の開始

関連トピック

- 保存済みクエリを使用した調査の共通領域のカプセル化
- スプリングボードの管理

簡単な説明:[スプリングボード パネルの作成]ダイアログ

これは、[スプリングボード パネルの作成]ダイアログの例です。



次の表で、［スプリングボード パネルの作成］ダイアログの各フィールドについて説明します。

機能	説明
名前	(必須) パネル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。
メタ グループ	すでに選択されているフィルター クエリーから、現在、選択されているメタ グループを表示します。
列グループ	すでに選択されているフィルター クエリーから、現在、選択されている列グループを表示します。
場所	定義したクエリーが保存される場所を表示します。
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。新しいスプリングボード パネルの作成を開始したときにクエリー バーにアクティブなクエリがあった場合は、そのアクティブなクエリが［プレクエリー］フィールドに追加されます。プレクエリ条件の例を次に示します。 `'service=80,25,110'.`
メタ キー	サービスに使用できるメタ キーのリストを含むドロップダウンが表示されます。
デフォルトのソート順	ソート順のリストを含むドロップダウン リストが表示されます。
チャートのタイプ	チャートのタイプのリストを含むドロップダウン リストが表示されます。 • **ドーナツ** • **棒**

機能	説明
チャート カラー テーマ	さまざまなカラー テーマ オプションをリストしたドロップダウンを表示します。 • **青** • **ティール** • **オレンジ** • **濃いピンク** • **紫** • **ライム** • **複数** **注：複数**]カラー オプションはドーナツ チャートでのみ使用できます。
チャート のメトリック	使用可能なチャートのメトリックのリストを含むドロップダウン リストが表示されます。
キャンセル	変更を加えずにダイアログを閉じます。
保存	変更を保存します。

[将来のアラートを作成]ダイアログ

[**調査**] > [**イベント**]ページからアクセスできる [**将来のアラートを作成**]ダイアログでは、管理者とアナリストは不審なアクティビティに対するアプリケーション ルールを作成できます。侵害の疑いのあるアクティビティや構成ミスのあるサーバーなど、ネットワークからの幅広いイベントやシステム情報をカバーする柔軟なクエリーを使用して、ルールを作成できます。サービス(Decoder) を使用して一致したポリシーにルールが適用されると、一致が見つかるたびにアラートが生成され、アナリストがさらに調査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**]ビューでのサービスの調査中に、クエリー検索バーでクエリーを追加し、ツールバーから  > [**将来のアラートを作成**]を選択します。

重要：[将来のアラートを作成]オプションがユーザーに対して有効になるのは、Decoderサービスがポリシーベースのコンテンツー元管理によって管理されており、ユーザーが**investigate-server.alert.manage**権限を有効にしている場合だけです。

注：管理者は、アナリストがアプリケーション ルールを作成できるように、ソース サーバー上で**investigate-server.alert.manage**権限と**source-server.centralpolicy.manage**権限を有効にし、コア デバイス上で**rules.manage**権限を有効に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ー管理ガイド*』の「ロールの権限」トピックを参照してください。

実行したいことは何ですか？

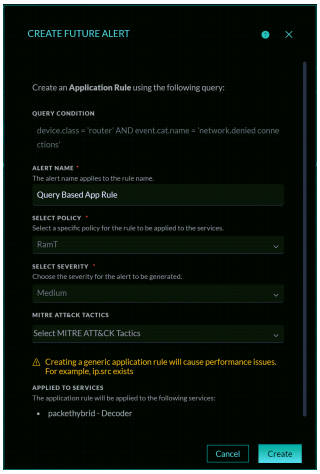
ユーザ ロール	実行したいこと	手順
管理者/アナリスト	アプリケーション ルールの作成	イベントビューから将来のアラートを作成する

関連トピック

- 保存済みクエリを使用した調査の共通領域のカプセル化
- イベントビューから将来のアラートを作成する

簡単な説明 - 「将来のアラートを作成」ダイアログ

これは、「将来のアラートを作成」ダイアログの例です。



次の表で、「将来のアラートを作成」ビューのフィールドについて説明します。

機能	説明
アラート名	アラートを識別するためのわかりやすい名前を指定するか、**「クエリーベースのアプリケーション ルール」**形式を使用して自動的に入力されるデフォルト名のままにします。
ポリシーの選択	選択可能なポリシーのドロップダウン リストが表示されます。

機能	説明
重大度の選択	生成されるアラートの重大度のレベルが表示されます。オプションは以下のとおりです。 • 低 • 中 • 高 • クリティカル **注** :重大度はデフォルトで「低」に設定されています。
MITRE ATT&CK戦術	アラートに関連する戦術のタイプを表示します。 例 :**クレデンシャル アクセス**。 クレデンシャル アクセス戦術は、アカウント名とパスワードを盗もうとします。
MITRE ATT&CKテクニック	戦術に関連付けられたテクニックとサブテクニックの種類が表示されます。
作成	アプリケーション ルールを作成し、ダイアログを閉じます。アプリケーション ルール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。
キャンセル	変更を加えずにダイアログを閉じます。

[イベント]ビューの [レポートのスケジュール設定]ダイアログ

[**レポートのスケジュール設定**]ダイアログを使用して、レポートのスケジュールを作成できます。レポートは、毎時間、毎日、毎週、または毎月にスケジュール設定できます。特定の時刻、または日次、週次、月次ベースでレポートをスケジュール設定するには、 [レポートのスケジュール設定]ダイアログでスケジュール オプションを設定する必要があります。

このダイアログにアクセスするには、 [**調査**] > [**イベント**]ビューでのサービスの調査中に、クエリー検索バーでクエリーを追加し、ツールバーから  > [**レポートのスケジュール設定**]を選択します。さらに管理者とアナリストは、レポートのチャートを構成することができます。この機能を使用すると、管理者とアナリストは [**イベント数**]、 [**セッション サイズ**]、 [**パケット数**]、および [**メタ キー**]に基づいて、さまざまなタイプのチャートを作成できます。

実行したいことは何ですか?

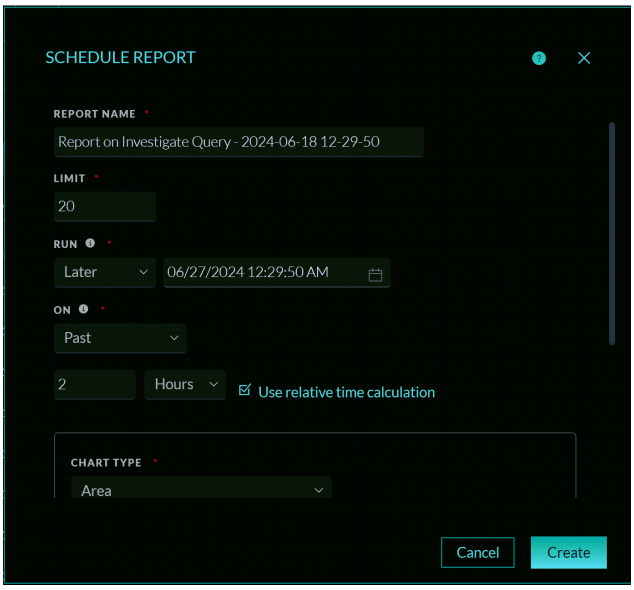
ユーザ ロール	実行したいこと	手順
管理者/アナリスト	レポートのスケジュール設定	イベントビューからレポートを生成する

関連トピック

- 保存済みクエリを使用した調査の共通領域のカプセル化
- イベントビューからレポートを生成する

簡単な説明 - ［レポートのスケジュール設定］ダイアログ

これは、［レポートのスケジュール設定］ダイアログの例です。



次の表で、［**レポートのスケジュール設定**］ダイアログの各フィールドについて説明します。

機能	説明
レポート名	パネルを識別する名前を指定します。この例では、名前は「**調査クエリーに関するレポート - 2023-04-25 10-18-26**」です。このレポー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。
制限	生成される出力に表示する結果の最大数の選択リスト。デフォルトでは、制限は20で、最大100件の結果を指定できます。

機能	説明
実行	スケジュール設定されたジョブの実行に使用する時間間隔： • **指定日時** :特定の日時に実行されます。 • **毎時** :指定された繰り返し間隔で実行されます。たとえば、レポートの実行スケジュールを50分に設定した場合は、50分ごとにレポートが作成されます。 **注** :最大値である59分まで選択できます。 • 「**日単位**」:毎日指定された時刻に実行されます。たとえば、レポートの実行スケジュールを04:25に設定すると、レポートは毎日午前4:25に作成されます。 • 「**月単位**」:毎月、指定された日時に実行されます。たとえば、25日の場合は「25」を選択すると、レポートが毎月25日に作成されるようになります。 **注** :29以上の値を「日」で選択した場合は、月次レポートの生成プロセス中にメッセージが表示され、選択した日を含んでいる月にレポートがスケジュール設定されることが通知されます。
オン	レポートを実行する頻度、期間、時間を設定します。 • **過去** :**時間数**、**日数**、**週数**、**月数**、**年数**に基づいてレポートをスケジュール設定できます。 • **範囲(特定)** :日時の範囲を指定してレポートをスケジュール設定できます。 **注** :このフィールドは、「実行」フィールドで「指定日時」を選択した場合にのみ表示されます。 • **範囲(時間指定)** :日時を指定してレポートをスケジュール設定できます。 **注** :このフィールドは、「実行」フィールドで「指定日時」、「毎日」、「毎週」、「毎月」を選択した場合にのみ表示されます。
相対時間計算の使用	デフォルトでは、「相対時間計算の使用」オプションが有効になっており、レポートのスケジュール設定に相対的な期間が使用されます。 たとえば、相対時間で過去1時間のデータに対してレポートをスケジュール設定する場合、その時間はレポートの実行時までの厳密に1時間を指します。現在時刻が午後3時の場合は、過去60分間、つまり今日の午後2時から午後3時までの間に発生したイベントが報告されます。

機能	説明
チャート タイプ	チャート タイプのオプションをリストしたドロップダウンを表示します。 • 表形式(デフォルト) • 円 • 領域 • 棒 • バブル • 列 • 折れ線 • ステップ折れ線 • ステップ面 • スプライン面 • スパイン
サマライズ	目的のメタ値をサマライズしたものを取得するための、さまざまな組み込み集約メタ オプションをリストしたドロップダウンを表示します。 • **イベント数** :特定の時間に発生したイベントの総数。 • **セッション サイズ** :特定の時間にサービスによって記録されたイベントの合計サイズ。 • **パケット数** :送信または受信されたパケットの総数。
メタ キー	さまざまなメタ キー オプションをリストしたドロップダウンを表示します。 **注** :一度に選択できるメタ値は1つだけです。
メール出力アクション	レポートの送信先メール アドレスをカンマで区切って指定します。
作成	レポートを作成し、ダイアログを閉じます。レポートが正常に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。
キャンセル	変更を加えずにダイアログを閉じます。

[イベント]ビューの [チャートの作成]ダイアログ

管理者とアナリストは、 **調査**] > [**イベント**]ページのリアルタイム データに基づいてチャートを作成できます。この機能拡張を使用すると、 [**イベント数**]、 [**セッション サイズ**]、 [**パケット数**]、 [**メタ キー**]の各サマライズ オプションに基づいて、さまざまなタイプのチャートを作成することが可能になります。これはアナリストが傾向を追跡するためのオールインワン ソリューションとなります。さらに、アナリストはこれらのリアルタイム チャートをデフォルトのダッシュボードに追加できるため、組織内の重要なデータをシームレスに追跡することができます。

実行したいことは何ですか?

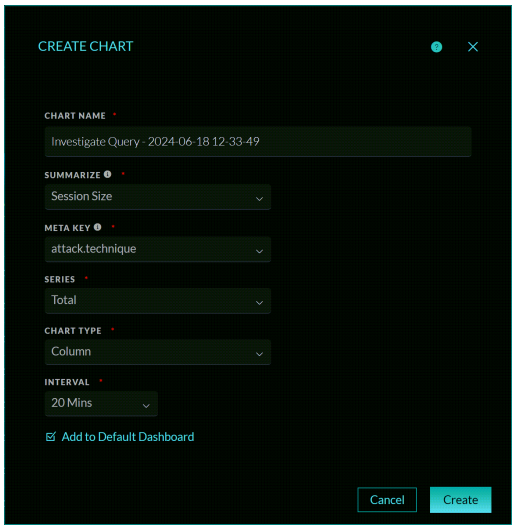
ユーザ ロール	実行したいこと	手順
管理者/アナリスト	チャートの構成	イベントビューからレポートを生成する

関連トピック

- イベントビューからレポートを生成する

簡単な説明 - [イベント]ビューの [チャートの作成]ダイアログ

これは、 [イベント]ビューからアクセスできる [チャートの作成]ダイアログの例です。



機能	説明
チャートの名前	チャートを識別する名前を指定します。この例では、名前は「**クエリーの調査 - 2023-09-14 16-57-00**」です。このチャー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。

機能	説明
サマライズ	目的のメタ値をサマライズしたものを取得するための、さまざまな組み込み集約メタ オプションをリストしたドロップダウンを表示します。 • **イベント数** :特定の時間に発生したイベントの総数。 • **セッション サイズ** :特定の時間にサービスによって記録されたイベントの合計サイズ。 • **パケット数** :送信または受信されたパケットの総数。
メタ キー	さまざまなメタ キー オプションをリストしたドロップダウンを表示します。 **注** :一度に選択できるメタ値は1つだけです。
系列	チャートのさまざまな系列オプションをリストしたドロップダウンを表示します。 • **合計** :チャートには、選択した時間帯の各集計値の合計が表示されます。 • **値** :チャートには、選択した時間帯の値の変化が表示されます。 **注** :このオプションは、 **デフォルトのダッシュボードに追加**]チェックボックスを選択した場合にのみ使用可能になります。

機能	説明
チャート タイプ	チャート タイプのオプションをリストしたドロップダウンを表示します。 • 表形式(デフォルト) • 円 • 領域 • 棒 • バブル • 列 • 折れ線 • ステップ折れ線 • ステップ面 • スプライン面 • スパイン **注：** - このオプションは、［**デフォルトのダッシュボードに追加**］チェックボックスを選択した場合にのみ使用可能になります。 - デフォルトでは、棒タイプのチャートが選択されています。 - 選択した［**系列**］オプションに応じて、チャートが自動表示されます。 - ［**合計**］オプションの場合：［**円**］および［**棒**］チャートのみが有効になっています。 - ［**値**］オプションの場合：［**エリア**］、［**棒**］、［**折れ線**］、［**ステップ折れ線**］、［**ステップ面**］、［**スプライン面**］、［**スプライン**］の各チャートが有効になっています。
間隔	時間範囲のオプションをリストしたドロップダウンを表示します。 間隔には10分から180分の時間範囲を指定でき、各間隔の間に10分の隔たりがあります。 **注：**デフォルトでは、各チャートに表示されるレコード(上位)の数は**15**個です。
デフォルトのダッシュボードに追加	チャートを追加するチェックボックス オプションを［**ダッシュボード**］>［**デフォルトのダッシュボード**］ビューに表示します。
作成	チャートを作成し、ダイアログを閉じます。チャートが正常に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。
キャンセル	変更を加えずにダイアログを閉じます。

[タイムライン設定]パネル

アナリストは**タイムライン設定**オプションを使用して、ユニット(Y軸)(数とサイズ)に基づいて値を変更し、タイムライン上に表示されるデータを確認できます。これにより、アナリストは異常を示している可能性のあるイベント数の急増を検出できます。視覚的表現を使用して、その特定の期間に発生したイベントをより詳細に調査することができます。

タイムラインの詳細については、「[イベント]ビューでの調査の開始」トピックの「**タイムラインでの調査**」セクションを参照してください。

注:X軸の設定を変更するには、[イベント環境設定]パネル内で設定されているクエリー時間オプションを変更する必要があります。クエリー時間の詳細については、「[イベント]ビューの構成」を参照してください。

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
アナリスト	タイムライン設定の構成	[イベント]ビューでの調査の開始

タイムライン設定を変更するには

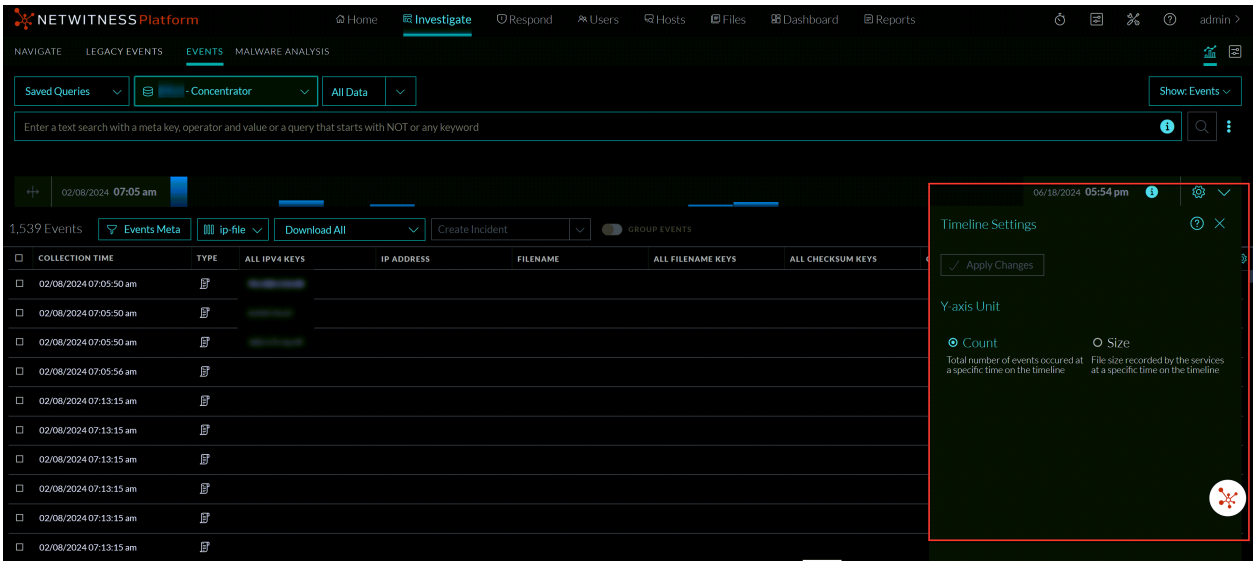
1. NetWitness Platformにログインします。
2. [**調査**] > [**イベント**]に移動します。
3. [**タイムライン設定**]( ) をクリックします。
4. 好みに基づいてスパイク(Y軸)の単位を選択します。
   - **数**:タイムライン上の特定の時間に発生したイベントの総数を表示します。
   - **サイズ**:タイムライン上の特定の時間にサービスによって記録されたイベントの合計サイズを表示します。
5. [**変更の適用**]をクリックします。変更がタイムライン バーに反映されます。
6. [X]をクリックしてタイムライン設定を閉じます。

関連トピック

- [イベント]ビューでの調査の開始

簡単な説明 - [タイムライン設定]パネル

これは、[タイムライン設定]のパネルの例です。



次の表は、［**タイムライン設定**］パネルのフィールドについて説明しています。

機能	説明
件数	タイムライン上の特定の時間に発生したイベントの総数を表示します。
サイズ	タイムライン上の特定の時間にサービスによって記録されたイベントの合計サイズを表示します。
変更の適用	変更を適用すると、タイムライン バーに変更が反映されます。
X	変更を加えずにダイアログを閉じます。

検索パターンの作成]ダイアログ

管理者とアナリストは、ネットワーク上の機密データを見つけるための検索パターンを作成できます。これらのルールはキーワードを使用してパターンを識別し、正確なキーワード文字列に基づいて照合されます。サービス(Decoder) と一致するポリシーにパターンが適用されると、ネットワークトラフィック内でそのパターンが検索されます。一致が検出されると、2つの重要なメタデータ(**found**と**match**) が生成されます。アナリストはこのメタデータを使用してさらに調査し、機密データが悪意を持って使用されていないかどうかを判断できます。

実行したいことは何ですか？

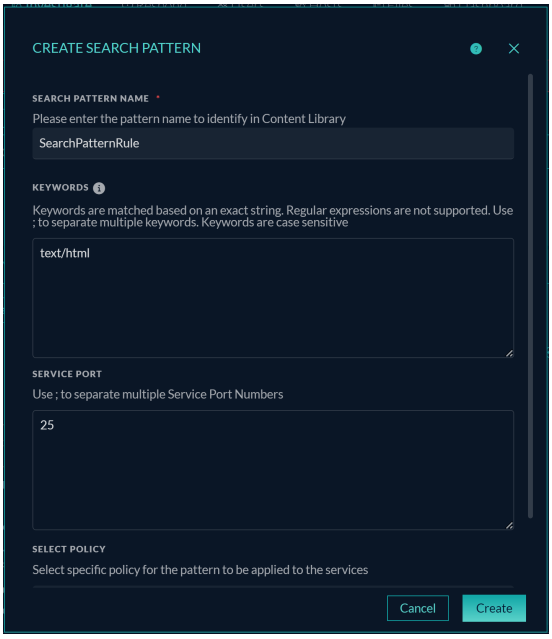
ユーザロール	実行したいこと	手順
管理者/アナリスト	検索パターンの作成	イベントビューでイベントを分析する

関連トピック

- イベントビューでイベントを分析する

簡単な説明 - 検索パターンの作成]ダイアログ

これは、 検索パターンの作成]ダイアログの例です



次の表で、 検索パターンの作成]ビューのフィールドについて説明します。

機能	説明

機能	説明
検索パターン名	検索パターンを識別するためのわかりやすい名前を指定するか、 **検索パターン ルール**] 形式を使用して自動的に入力されるデフォルト名のままにします。
Keywords	1つ以上のキーワードを追加できます。キーワードは、正確な文字列のみに基づいて照合されます。正規表現(Regex) はサポートされていません。複数のキーワードを区切るにはセミコロン(;) を使用します。たとえば、「**CreditCard**;**VISA**;**US**」のように入力します。
サービス ポート	1つ以上のポートを追加できます。複数のポート番号を区切るにはセミコロン(;) を使用します。たとえば、「**20**;**21**;**23**」のように入力します。 ポート番号は**1**～**65535**の間でなくてはなりません。
ポリシーの選択	選択可能なポリシーのドロップダウン リストが表示されます。
作成	検索パターンを作成し、ダイアログを閉じます。検索パターン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。
作成と公開	検索パターンを作成し、Decoderサービスを含む利用可能なポリシーに検索パターン ルールを導入します。
キャンセル	変更を加えずにダイアログを閉じます。

調査ビューの設定ダイアログ

このダイアログの設定は、［プロファイル］> ［環境設定］パネル> ［調査］タブで行う調査の設定のサブセットです。アナリストは、［調査］ビューでこれらの設定を編集することにより、時間を節約できます。ここで設定を変更すると、［プロファイル］ビューで同じ設定が変更されます。［プロファイル］ビューで設定を変更すると、この場所の同じ設定が変更されます。

このダイアログにアクセスするには、［**ナビゲート**］ビューまたは［**レガシー イベント**］ビューに移動し、ツールバーの［**設定**］オプションを選択します。

［プロファイル］> ［環境設定］パネルには、［イベント］ビューの設定に対応する設定はありません。

関連トピック

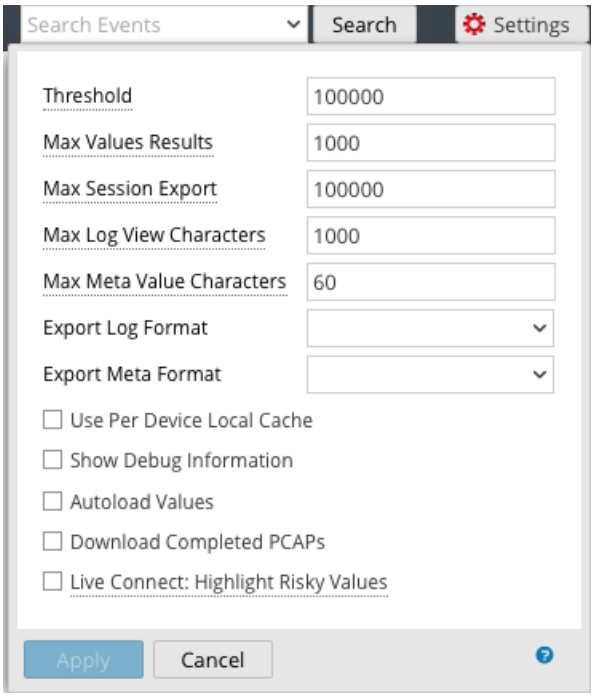
- NetWitness Investigateの仕組み

簡単な説明

ここでは、［ナビゲート］ビュー、［レガシー イベント］ビュー、［イベント］ビューの設定ダイアログについて簡単に説明します。

［ナビゲート］ビューの［設定］ダイアログ

次の図は、［ナビゲート］ビューの［設定］ダイアログを示しています。［値］パネルで値をロードするときのパフォーマンスに影響を与える設定には、一般的な使用方法に基づくデフォルト値があり、アナリストはこれらの設定を自分の調査内容に合わせて調整できます。以下の表は、機能についての説明です。

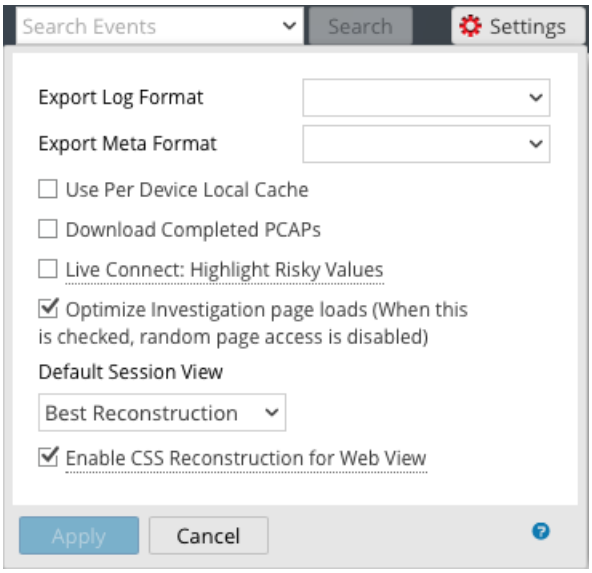


機能	説明
閾値	[値]パネルでメタ キー値にロードするセッションの最大数の閾値を設定します。閾値を高くすると、値が正確にカウントされますが、その分ロード時間が長くなります。デフォルト値は**100000**です。
結果の最大数	この設定は、[ナビゲート]ビューで開いているメタ キーについて、[メタ キー]メニューで [最大まで表示]を選択した場合にロードする値の最大数を制御します。デフォルト値は**1000**です。
最大セッション エクスポート	エクスポートできるセッションの最大数を設定します。デフォルト値は**100000**です。
ログのエクスポート形式	エクスポートされたログのファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト** :RAWログ形式。 • **SML** :構造化マークアップ言語形式。 • **CSV** :カンマ区切り値(CSV) 形式。 • **JSON** :JavaScript Object Notation(JSON) 形式。
メタのエクスポート形式	エクスポートされたメタ値のファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト** :RAWログ形式。 • **SML** :構造化マークアップ言語形式。 • **CSV** :カンマ区切り値(CSV) 形式。 • **JSON** :JavaScript Object Notation(JSON) 形式。
デバイスごとのローカル キャッシュを使用	このチェックボックスをオフにすると、初回ロード後に [調査]ビューにキャッシュされたデータを表示するのではなく、新しいクエリがデータベースに送信されます。チェックボックスをオンにすると、ローカル キャッシュのデータを使用します。
デバッグ情報の表示	このオプションは、階層リンクの下の`where`句の表示と、Brokerで集計したサービスごとの経過したロード時間の表示を制御します。チェックボックスをオンにすると、デバッグ情報が表示されます。デフォルト値は**オフ**(チェックの外れた状態) です。
値の自動ロード	このオプションは、[ナビゲート]ビューで選択したサービスの値の自動ロードを制御します。チェックボックスをオンにすると、調査するサービスを選択したときに、値が自動的にロードされます。チェックボックスをオフにすると、**[値のロード]**ボタンが表示されます。値をロードする前に、オプションを変更することができます。デフォルト値は**オフ**です。
完了したPCAPのダウンロード	この設定は、調査で抽出されたPCAPのダウンロードを自動化します。これにより、PCAPファイルをダウンロードし、PCAPフォームのデータを処理できるアプリケーション(Wiresharkなど) で抽出して開く操作を手動で実行する必要がなくなります。チェックボックスをオンにすると、オプションが有効になります。デフォルト設定は無効(チェックボックスはオフ) です。

機能	説明
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、［ナビゲート］ビューの［値］パネルでハイライト表示されます。チェックボックスをオンにすると、Live Connectでコンテキストを持つ値のうち、コミュニティによってリスクが高い/不審である/安全でないと判断された値のみが強調表示されます。デフォルトでこのオプションは無効(チェックボックスはオフ)になっています。
適用	設定をただちに適用します。設定は、次回に値をロードしたときに表示されます。また、同じ変更が、［プロファイル］ビューにも適用されます。
キャンセル	編集操作をキャンセルし、設定を変更せずにダイアログを閉じます。

［レガシー イベント］ビューの［設定］ダイアログ

次の図は［レガシー イベント］ビューの［設定］ダイアログの例です。また、その機能について表で説明します。

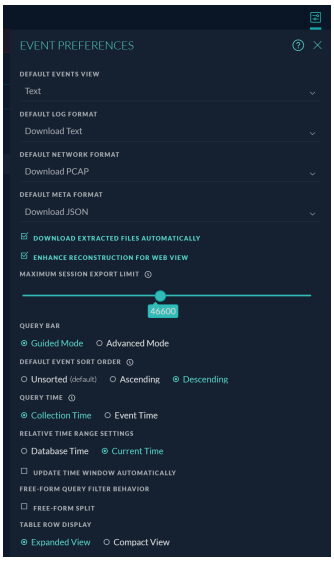


機能	説明
ログのエクスポート形式	エクスポートされたログのファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト** :RAWログ形式。 • **SML** :構造化マークアップ言語形式。 • **CSV** :カンマ区切り値(CSV)形式。 • **JSON** :JavaScript Object Notation(JSON)形式。

機能	説明
メタのエクスポート形式	エクスポートされたメタ値のファイル形式を設定します。次の4つの形式を設定できます。 • **テキスト**：RAWログ形式。 • **SML**：構造化マークアップ言語形式。 • **CSV**：カンマ区切り値(CSV)形式。 • **JSON**：JavaScript Object Notation(JSON)形式。
完了したPCAPのダウンロード	この設定は、調査で抽出されたPCAPのダウンロードを自動化します。これにより、PCAPファイルをダウンロードし、PCAPフォームのデータを処理できるアプリケーション(Wiresharkなど)で抽出して開く操作を手動で実行する必要がなくなります。
Live Connect：リスクの高いIPのハイライト表示	チェックボックスをオンにすると、Investigateはフィルターを使用して、NetWitnessコミュニティによって危険と見なされるIPアドレスのみを取得します。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。
調査ページのロードを最適化	ページング オプションを設定します。最適化した場合、イベント リストで可能な限り速く結果が返されますが、イベント リストのページ移動機能が無効になります。このチェックボックスをオフにすると、イベント リストのページ移動機能が有効になり、リストの特定のページ(または最後のページ)に移動できるようになります。デフォルト値は有効(チェックボックスはオン)です。
イベント パネルのイベントを挿入モードで表示	このオプションは、[レガシー イベント]パネルのページングに影響し、以前のリリースでは[ナビゲート]ビューの[設定]ダイアログにありました。チェックボックスをオンにすると、次のイベント グループがすでに表示されているイベントに追加されます。チェックボックスをオフにすると、前のイベントのページが次のページに置き換えられます。デフォルト値はオフ(チェックの外れた状態)です。
デフォルト セッション表示	[イベント]ビューでのデフォルトの再構築のタイプを選択します。デフォルト値は**[最適な表示]**で、イベントに最も適した表示方法でイベントが表示されます。
WebビューのCSS再構築を有効化	この設定では、Webコンテンツの再構築の実行方法が制御されます。有効化すると、Webの再構築にカスケード スタイル シート(CSS)とイメージが含まれるようになり、再構築の表示と元のWebブラウザの表示が一致するようになります。これには、イベントに関連するスキャニングと再構築、ターゲット イベントで使用されるスタイル シートとイメージの検索が含まれます。このオプションは、デフォルトで有効化されています。特定のWebサイトの表示に問題がある場合は、チェックボックスをオフにしてこのオプションを無効化してください。
適用	設定をただちに適用します。この設定は、次回にイベントを表示したときに示されます。また、同じ変更が、[プロファイル]ビューにも適用されます。
キャンセル	編集操作をキャンセルし、設定を変更せずにダイアログを閉じます。

[イベント]ビューの [環境設定]ダイアログ

[イベント]ビューにユーザ環境設定が追加されました。この環境設定は、 [**イベント**]ビュー> [**イベント環境設定**]ダイアログで設定できます。これらの設定は保持されるため、ログインして [イベント]ビューに移動するたびに適用されます。次の図に、このダイアログの例を示します。次の表に、オプションの説明を示します。



機能	説明
デフォルトの [イベント]ビュー	[イベント]ビューを開くたびに表示されるデフォルトのイベント分析ビューを選択します。たとえば [ファイル]を選択すると、 [イベント]ビューでイベントを調査するたびに [ファイル分析]パネルがハイライト表示されます。次にオプションを示します。 • **テキスト** :イベントのRAWテキスト ペイロードを表示および分析します。 • **パケット** :イベントのパケットとペイロードを表示し、対話形式で分析します。 • **ファイル** :イベントのファイルのリストを表示し、1つまたは複数のファイルをダウンロードします。
デフォルトのログ形式	ログをダウンロードする際のデフォルトの形式を選択します。 • **ログのダウンロード**または**テキストのダウンロード** :RAWログ(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
デフォルトのパケット形式またはデフォルトのネットワーク形式	パケットをダウンロードする際のデフォルトの形式を選択します。 • **PCAPのダウンロード**:イベント全体をパケット キャプチャ(*.pcap)ファイルとしてダウンロードします。 • **すべてのペイロードのダウンロード**または**ペイロードのダウンロード**:ペイロードを*.payloadファイルとしてダウンロードします。 • **リクエスト ペイロードのダウンロード**:リクエスト ペイロードを*.payload1ファイルとしてダウンロードします。 • **レスポンス ペイロードのダウンロード**:レスポンス ペイロードを*.payload2ファイルとしてダウンロードします。
デフォルトのメタ形式	メタデータをダウンロードする際のデフォルトの形式を選択します。 • **CSVのダウンロード**:カンマ区切り値(CSV)形式。 • **JSONのダウンロード**:JavaScript Object Notation(JSON)形式。 • **テキストのダウンロード**:プレーン テキスト形式。 • **TSVのダウンロード**:タブ区切り値(TSV)形式。
クエリの時間形式	[イベント]ビューには、データベースの時間または現在の時刻に基づいて結果を表示できます。 **注**:**現在の時刻**は**相対時間範囲設定**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。 **現在の時刻**(**実時間**と表示)が選択されている場合、クエリは現在のブラウザ時刻に基づく終了時刻を使用して実行され、開始時刻はその終了時刻と時間範囲に基づいて計算されます。

機能	説明
イベントの並び順	[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、次回のクエリ送信時に有効になります。 **ソートしない**: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**:収集時間が最も古いイベントをリストの最初に配置します。 **降順**:収集時間が最も新しいイベントをリストの最初に配置します。ログを調査するにあたり、ソート順を「最も新しい収集時間が最初」に変更する必要が生じることがあります。
抽出したファイルを自動ダウンロード	[イベント環境設定]ダイアログの [**デフォルトのログ形式**]フィールドと [**デフォルトのパケット形式**]フィールドで選択したデフォルト形式のファイルの自動ダウンロードを有効にします。 選択した形式のファイルをローカル ファイル システムに自動的にダウンロードするには、このチェックボックスを選択します。このチェック ボックスを選択しない場合、ダウンロード ジョブがジョブ キューに入れられるのでファイルを手動でダウンロードできます。
タイム ウィンドウを自動的に更新	サービスがポーリング(1分間隔)されたときのクエリ バーの時間範囲ウィンドウの自動更新を有効にして、最新の結果が送信されるようにします。デフォルト設定はdisabledです。 チェックボックスをオンにすると、時間範囲が更新されたときに、  (クエリの送信)ボタンがアクティブになり、クリックして最新の結果を取得できるようになります。 チェックボックスをオフにすると、自動更新は無効になり、階層リンクの時間範囲ウィンドウが現在の結果と同期を維持します。
エクスポートできるセッションの最大数に対する制限	新しい設定である **最大セッション エクスポート制限** を使用すると、アナリストはこの設定を更新して、**すべてダウンロード** メニュー オプションを使用してエクスポート可能なセッションの数を調整できます。デフォルトの制限は**10,000**に設定されています。ただし、アナリストは要件に基づいてこの制限を増減できます。許可される最小制限は**1,000**、最大制限は**100,000**です。この機能強化により、エクスポートされたセッションの数が、イベント テーブルに表示されるセッションの数に依存しなくなりました。
Webビューの再構築を強化	(バージョン12.5以降)新しい設定 [**Webビューの再構築の強化**]を有効にすると、CSS、画像、リンクでビューをフォーマットすることでイベントを再構築するWebサイトの再現が改善され、アナリストがイベントのコンテキストや詳細をより理解しやすくなります。ただし、これにより再構築の速度が遅くなる可能性があります。このオプションは、デフォルトで有効です。