# RSA® NetWitness Platform

Version11.6

# リリース ノート

## 連絡先情報

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

## 商標

RSA Conferenceのロゴ、RSA、その他の商標は、RSA Security LLCまたはその関連会社(「RSA」) の商標です。RSAの商標のリストについては、https://www.rsa.com/ja-jp/company/rsa-trademarksを参照してください。その他の商標は、各社の商標または登録商標です。

## 使用許諾契約

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

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

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

## サード パーティ ライセンス

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

## 暗号技術に関する注意

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

## 配布

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

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

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



7月 2021

# 目次


**新機能** ..... **5**

アップグレード パス ..... 5

機能拡張 ..... 5

調査 - SIEMとネットワークトラフィックの分析 ..... 6

ファセット検索 ..... 6

調査コンテンツ( 列グループ、メタ グループ、クエリー プロファイル) の整理 ..... 6

RSA Liveを使用した調査コンテンツ( 列グループ、メタ グループ、クエリー プロファイル) の配信 ..... 6

値が複数 ..... 7

直接自由形式のクエリーまたはテキスト検索 ..... 7

クエリー フィルタの機能強化 ..... 7

カスタム列グループの機能強化 ..... 8

列グループメタ キーの推奨事項 ..... 8

画面レイアウト オプションの調査 ..... 9

メタ パネルの機能強化 ..... 9

IndexNoneメタ キー ..... 9

再構築の機能強化 ( コンテンツ表示とコピー オプション) ..... 9

検索インジケータ ..... 9

タイムアウト設定の調査 ..... 10

User Entity Behavior Analytics ..... 10

インシデント対応 ..... 10

エンドポイントの調査 ..... 11

Broker、Concentrator、Decoder、Log Decoderサービス ..... 14

Event Stream Analysis( ESA) ..... 16

管理と構成 ..... 17

Context Hub ..... 17

ログ収集 ..... 18

ライセンス ..... 20

スループット ライセンス計算の変更 ..... 20

プラットフォーム ..... 21

**修正された問題** ..... **22**

ログ収集の修正 ..... 22

管理の修正 ..... 22

監査ログ ..... 22

調査の修正 ..... 23

対応の修正 ..... 24

コア サービス( Broker、Concentrator、Decoder、Archiver) の修正 ..... 24

Event Stream Analysis( ESA) の修正 ..... 25

Reporting Engineの修正 ..... 25
エンドポイントの修正 ..... 25
スプリングボードの修正 ..... 26
更新の修正 ..... 26
Threat Intelligenceの修正 ..... 26
**サポートが終了する機能 ..... 27**
11.6.0.0以降のリリースでサポートが終了する機能 ..... 27
**製品ドキュメント ..... 28**
製品ドキュメントへのフィードバック ..... 28
**NetWitness Platformのヘルプ情報 ..... 29**
セルフ ヘルプ リソース ..... 29
カスタマー サポートへのお問い合わせ ..... 29
**ビルド番号 ..... 30**
**改訂履歴 ..... 32**

# 新機能

RSA NetWitness Platform 11.6は、セキュリティ オペレーション センター( SOC) のすべてのロールに新機能と機能拡張を提供します。

## アップグレード パス

NetWitness Platform 11.6.0.0では、以下のアップグレード パスがサポートされます。

- RSA NetWitness Platform 11.4.x.xから11.6.0.0へ*
- RSA NetWitness Platform 11.5.x.xから11.6.0.0へ

* 11.2.xxまたは11.3.xxからアップグレードする場合は、11.6にアップグレードする前に11.4.xxにアップグレードしておく必要があります。

11.6.0.0へのアップグレードの詳細については、『RSA NetWitness Platform 11.6アップグレード ガイド』を参照してください。

## 機能拡張

次のセクションでは、機能分野ごとに拡張内容を詳細に説明します。

- 調査 - SIEMとネットワークトラフィックの分析
- User Entity Behavior Analytics
- インシデント対応
- エンドポイントの調査
- Broker、Concentrator、Decoder、Log Decoderサービス
- Event Stream Analysis( ESA)
- 管理と構成
- Context Hub
- ログ収集
- ライセンス
- プラットフォーム

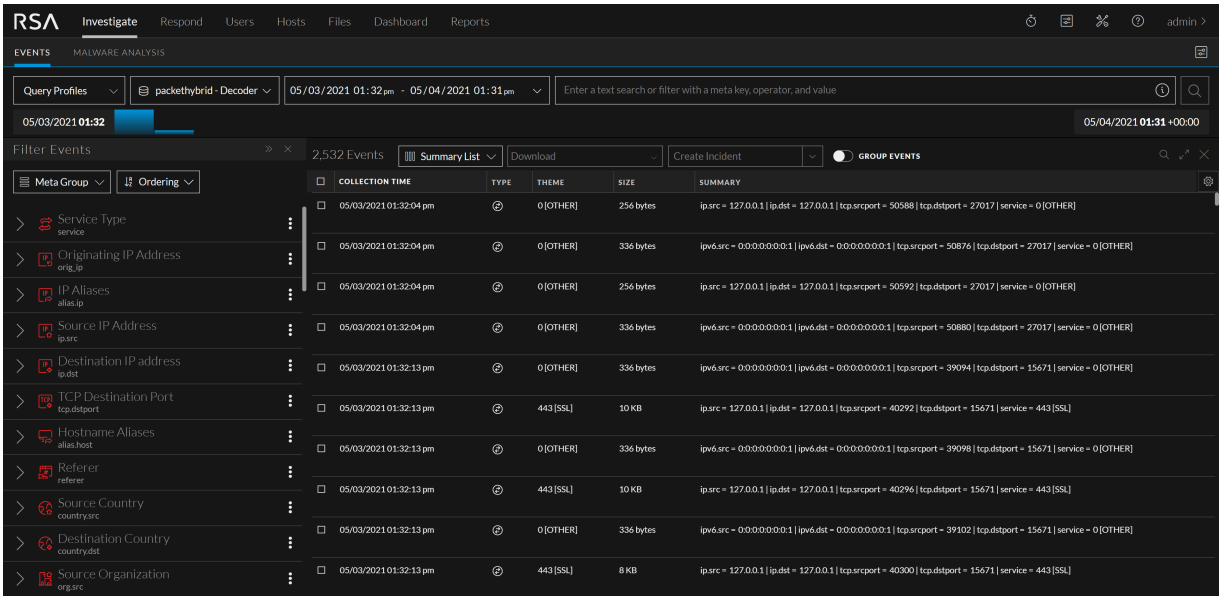
このセクションで言及されているドキュメントを見つけるには、RSA NetWitness Platform 11.x Masterマスター目次にアクセスしてください。製品ドキュメントには、このリリースのドキュメントへのリンクが記載されています。

# 調査 - SIEMとネットワークトラフィックの分析

## 調査の機能拡張

- **ファセット検索**

  デフォルトの[イベント]ビューの新しいファセット検索レイアウトにより、企業から収集された大量のデータとのやり取りが、より使い慣れたエクスペリエンスと効率的なワークフローになります。アナリストは、[ナビゲート]ビューと[イベント]ビューの機能を組み合わせることで、プラットフォームによって生成されたメタデータを操作してフィルタを適用できます。メタデータはクエリを作成し、検索を自動的に実行して、結果として生成されるイベントをフェッチします。




## 調査コンテンツ(列グループ、メタグループ、クエリー プロファイル)の整理

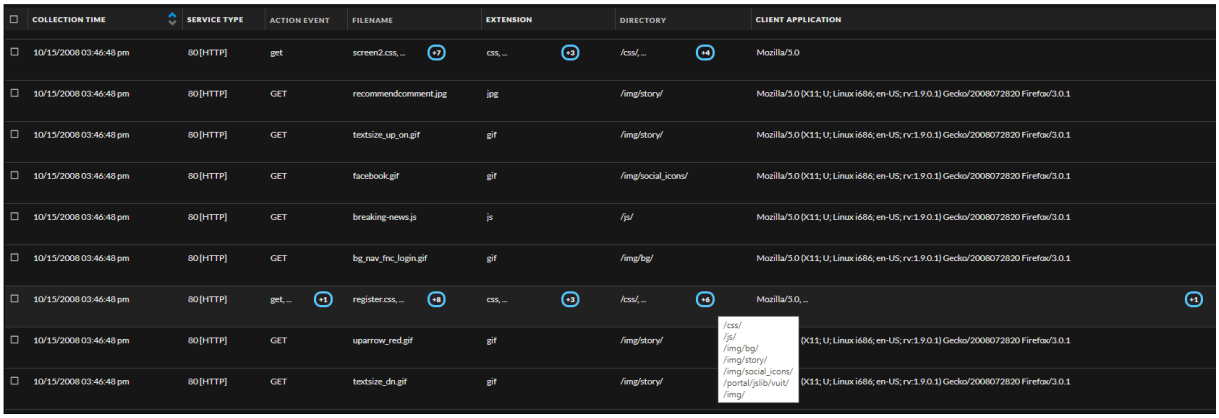
Investigateのコンテンツはすべてフォルダ構造で表示されるため、アナリストはユースケースに応じてビューを整理できます。RSAグループ(RSA LiveコンテンツとRSA OOTBグループ)、および共有グループ フォルダーは、すべてのアナリストが利用できます。プライベート グループ、フォルダ、およびサブフォルダはすべて、それを作成したアナリストにのみ表示されます。共有フォルダとプライベート フォルダおよびサブフォルダを作成、編集、コピー、および削除できます。

## RSA Liveを使用した調査コンテンツ(列グループ、メタグループ、クエリー プロファイル)の配信

Investigateコンテンツは、NetWitnessリリース サイクル外のアップデートを提供するRSA Liveを使用して導入できます。アナリストは、最新のInvestigateコンテンツを利用することで、ユースケースに基づいてビューをデータにフォーカスできるようになりました。RSAで生成されたコンテンツはすべてRSA固有のフォルダに格納されるようになりました。

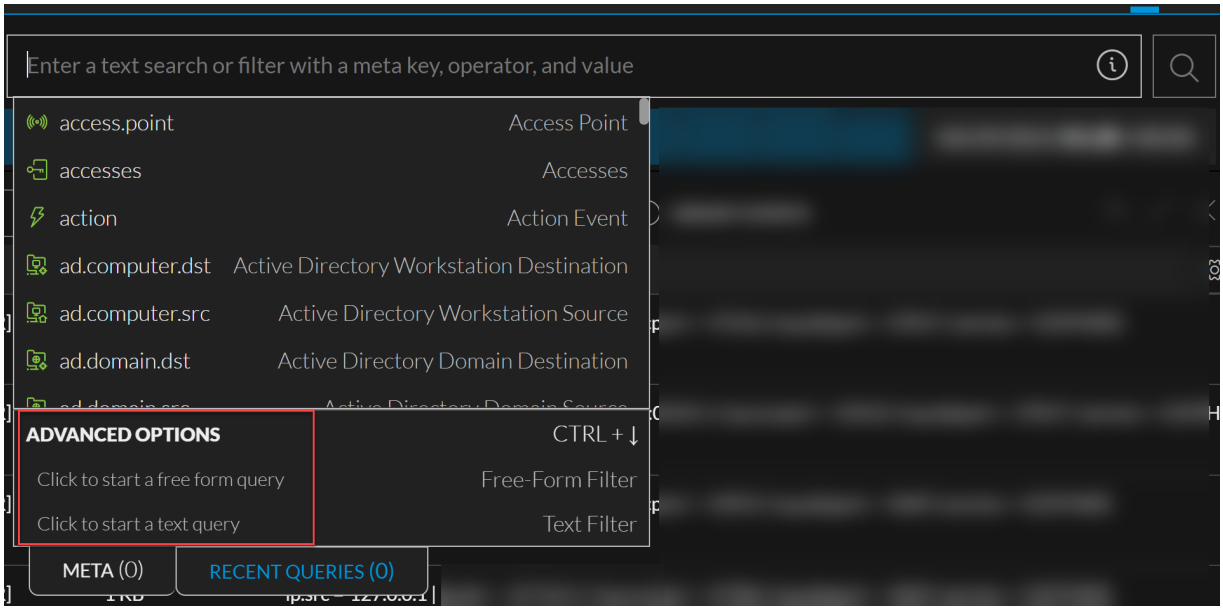
## 値が複数

イベントのリストを調査するときに、アナリストは、イベントがその特定のセッションのメタ キーに対して複数の値を持っていることを確認できます。ホバー オーバー インジケーターには、イベントの再構築をドリルダウンすることなくさらに調査できる複数の値のリストが表示されます。




## 直接自由形式のクエリーまたはテキスト検索

空白の自由形式フィルタをすぐに作成する場合、上級ユーザーは[詳細オプション]パネルからオプション[**クリックして自由形式のクエリを開始**]を選択できます。同様に、アナリストは[**クリックしてテキスト検索を開始**]を選択して新しいテキスト検索を作成できます。いずれのシナリオでも、アナリストはオートコンプリート入力ロジックをバイパスして、クエリ形式の生成にかかる時間を節約できます。




## クエリー フィルタの機能強化

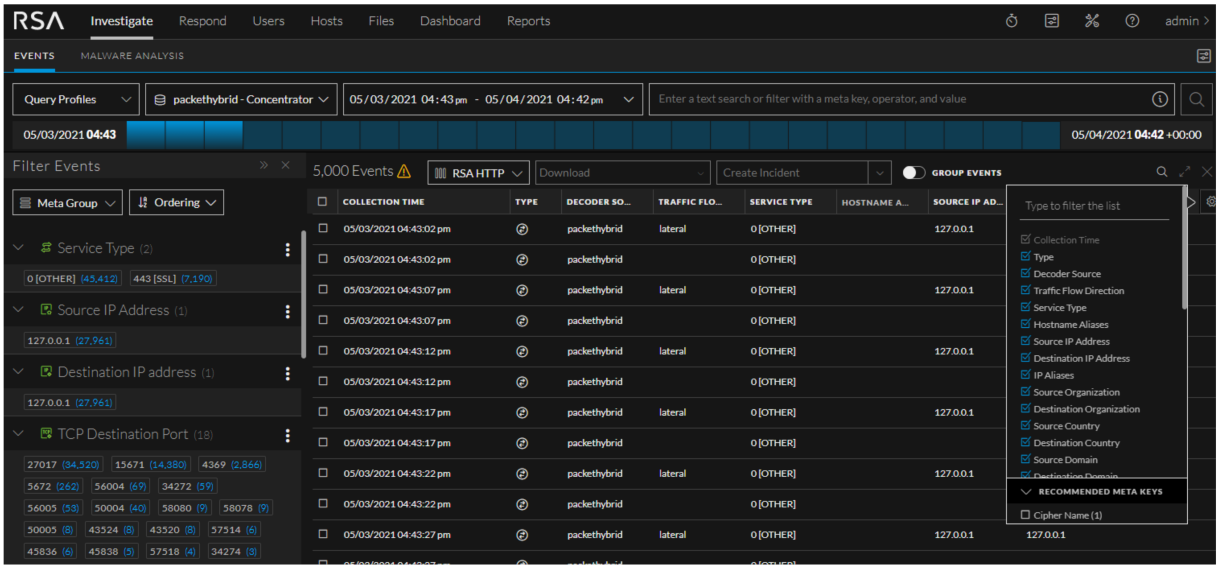
イベントにクエリが追加されると、選択されたフィルタに赤で強調表示された境界線が表示されるため、アナリストはどのフィルタが選択されているかを知ることができます。フィルタを編集すると、境界線が青色になり、アナリストがクエリ入力からフォーカスを離す場合に何らかの入力が必要であることが示されます。

## カスタム列グループの機能強化

レガシー イベントで定義されているか、OOTBサマリリスト列グループで定義されている `custom.logdata`などのメタデータを使用して、追加のメタデータのカスタマイズされた列としてRAWログを組み合わせることができます。データを含んだ推奨メタのリストが表示されます。アナリストは、サマリおよびRAWログ( `custom.logdata`) メタ キーを使用してカスタム列グループを作成できます。

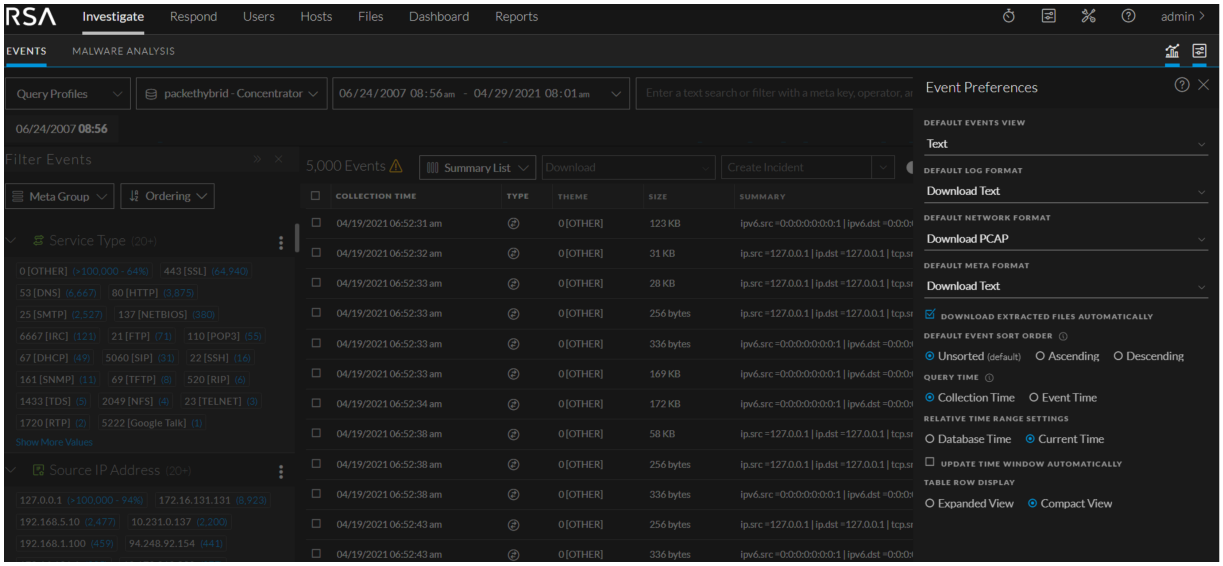
## 列グループメタ キーの推奨事項

選択した列グループを使用して[イベント]テーブルのクエリ結果を確認するときに、アナリストは、それらのイベントのデータが含まれている可能性があるが、現在の列グループの一部ではない推奨列を表示できます。これらの提案メタ キーを使用することで、アナリストは最適な列グループを適用して、表示されたイベントに該当するデータを見落とさないようにすることができます。



## 画面レイアウト オプションの調査

新しいユーザー設定により、アナリストはコンパクト形式または拡張形式のいずれかを選択して、単一ページのイベント テーブルに表示されるデータの行をどれだけ近づけるかを決定できます。次の画像は、コンパクト ビューが選択された状態でイベント設定ビューが表示されている例です。




## メタ パネルの機能強化

[イベント調査]ページのメタ パネルが[**重複エントリの非表示**]ラジオ ボタンで拡張されました。これにより、メタデータがキーと値の一意のペアである場合にのみメタデータが表示されます。アナリストがメタ キーまたは値に基づいて検索およびフィルタ処理できるようにする、フィルタフィールドも導入されています。

## IndexNoneメタ キー

アナリストが複数のメタ キーを使用してメタ グループを作成するときの、クエリのパフォーマンスへの悪影響を回避するため、インデックス付けされていないすべてのメタ キーに対して[開く]オプションが無効になっています。

## 再構築の機能強化(コンテンツ表示とコピー オプション)

[**テキスト**]タブのページネーションが強化され、1ページに表示しきれない追加のコンテンツがある場合に、それがはっきりと示されるようになりました。必要な場合、アナリストは(メニュー オプションに加えて)キーボード ショートカットを使用して、選択したコンテンツをクリップボードにコピーし、さらに調査することもできます。

## 検索インジケータ

アナリストがフリーテキスト検索を実行すると、インデックス付きのメタデータのみが検索されていることを明確に示すメッセージが[イベント]ページの上部に表示されます。このメッセージに含まれているリンクにより、アナリストはインデックス付けの範囲を超えて検索する必要がある場合に、さらに検索できるようになります。最大検索制限に達した場合は、表示できる結果がこれ以上ないことを示すメッセージが下部に表示されます。

### タイムアウト設定の調査

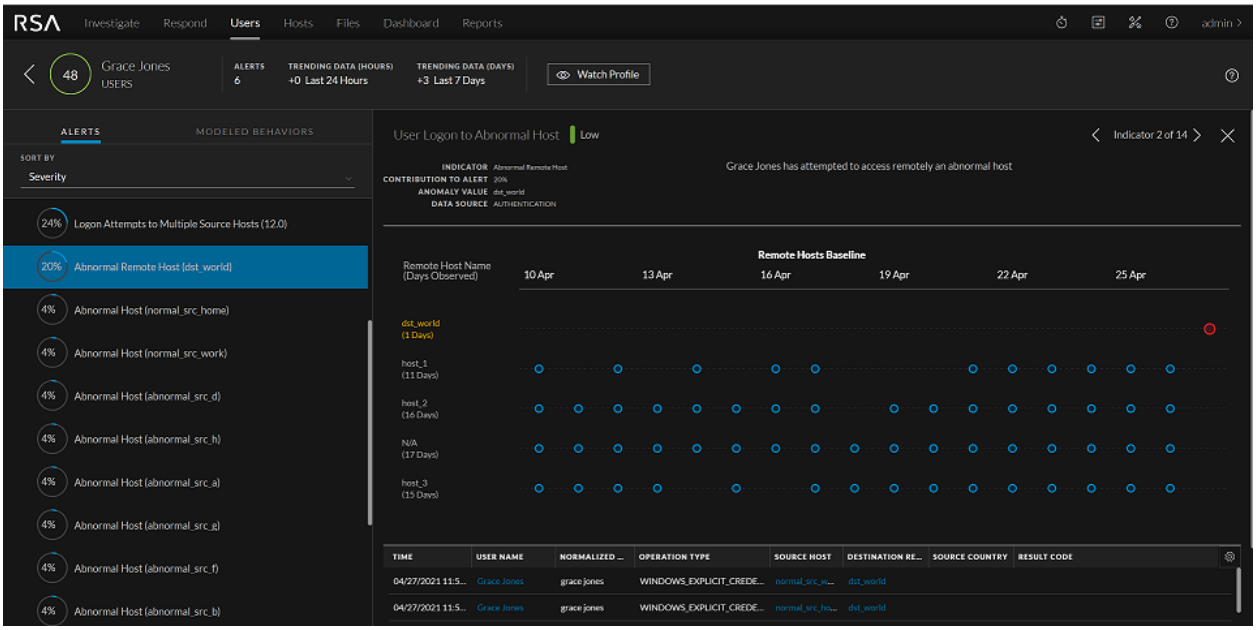
抽出タイムアウト設定により、管理者はInvestigateから必要なセッション、イベント、ファイルを取得するために使用できる時間を増減できます。この設定は、[**管理**]>[**システム**]>[**調査**]>[**一般的な設定**]に移動して構成できます。

調査の機能強化の詳細については、『*NetWitness Investigateユーザー ガイド*』を参照してください。

## User Entity Behavior Analytics

### 新機能と機能強化+

新しく拡張された点線グラフがバージョン11.6で導入されました。点線グラフには、一定期間のベースライン値が示されます。これによりアナリストは、モデル化された動作と異常(インジケータの場合)のコンテキストをよりよく理解できるようになります。バージョン11.6では、円グラフが点線グラフに置き換えられ、アナリストは時間の経過に伴うエンティティのアクティビティをさらに可視化できるようになりました。詳細については、『*NetWitness UEBAユーザー ガイド*』を参照してください。




## インシデント対応

### 永続データへの応答(ベータ版)

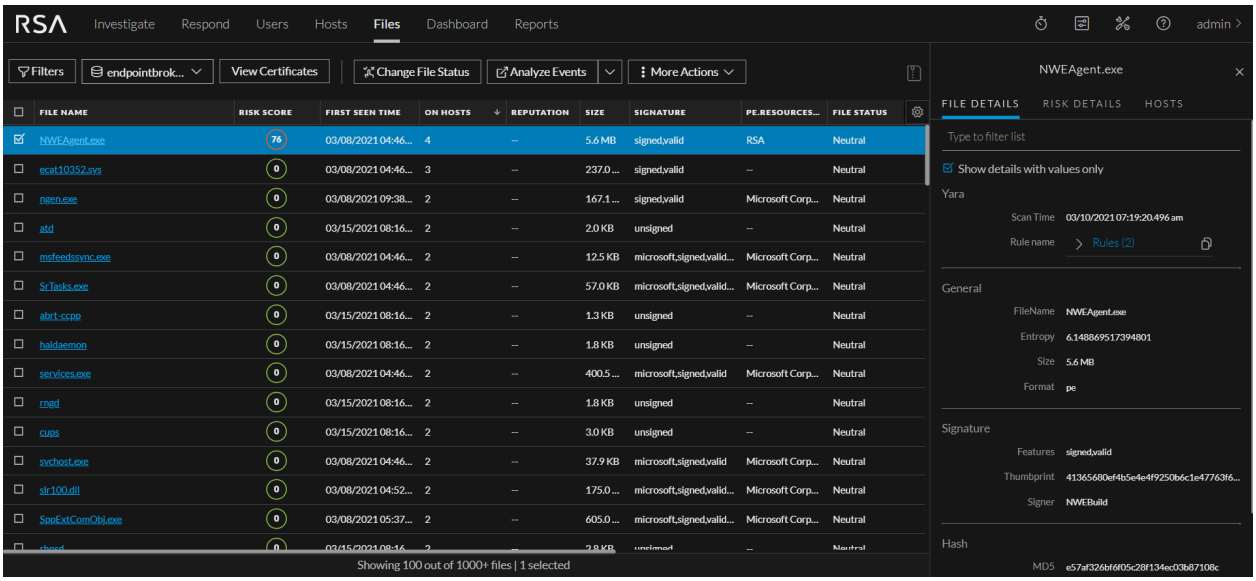
アナリストと管理者は、特定のインシデントに関連するイベントをピン固定できるため、将来のインシデントに関連した証拠を表示できます。イベントをピン固定すると、データは通常のデータベースからデータ ソース内の長期ストレージ キャッシュにコピーされます。イベントの保存は、ディレクトリ内の使用可能なスペースによって異なります(デフォルトでは10 GBが提供されます)。メタ データベースでのロールオーバーは、ピン固定ディレクトリにすでに保存されているイベントには影響しません。ベータ版には、ピン固定されたイベントをダウンロードできないという機能制限があります。この機能は、後続のリリースで有効になり、通知されます。

詳細については、『*NetWitness Respondユーザー ガイド*』の「Respond永続データ」を参照してください。

# エンドポイントの調査

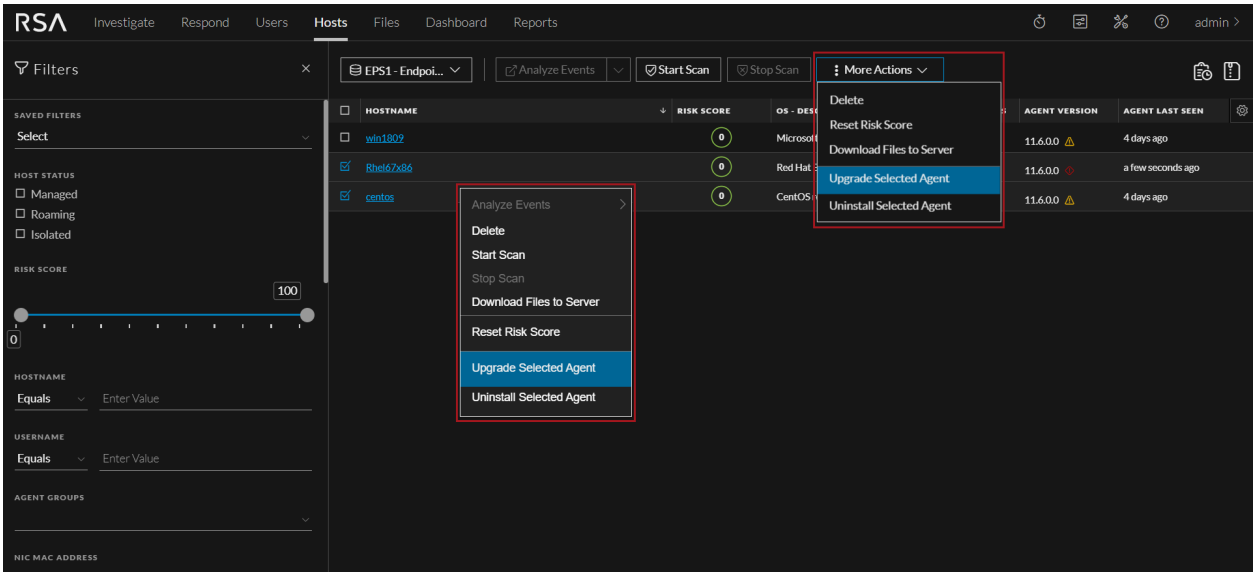
## YARAスキャンのサポート

YARAは、マルウェアの識別と分類においてルールベースの検出機能でアナリストを支援します。マルウェアの検出において堅牢性を発揮する、YARAルールと呼ばれるマルウェア記述を簡単に作成できます。YARAは、ダウンロードしたファイルを定期的に自動でスキャンし、ファイルがいずれかのルールに一致している場合は、そのファイルのリスク スコアを上げます。そのため、アナリストが脅威に迅速に対応するのに役立ちます。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。
YARAを有効にして構成する方法については、『*NetWitness Endpoint構成ガイド*』を参照してください。



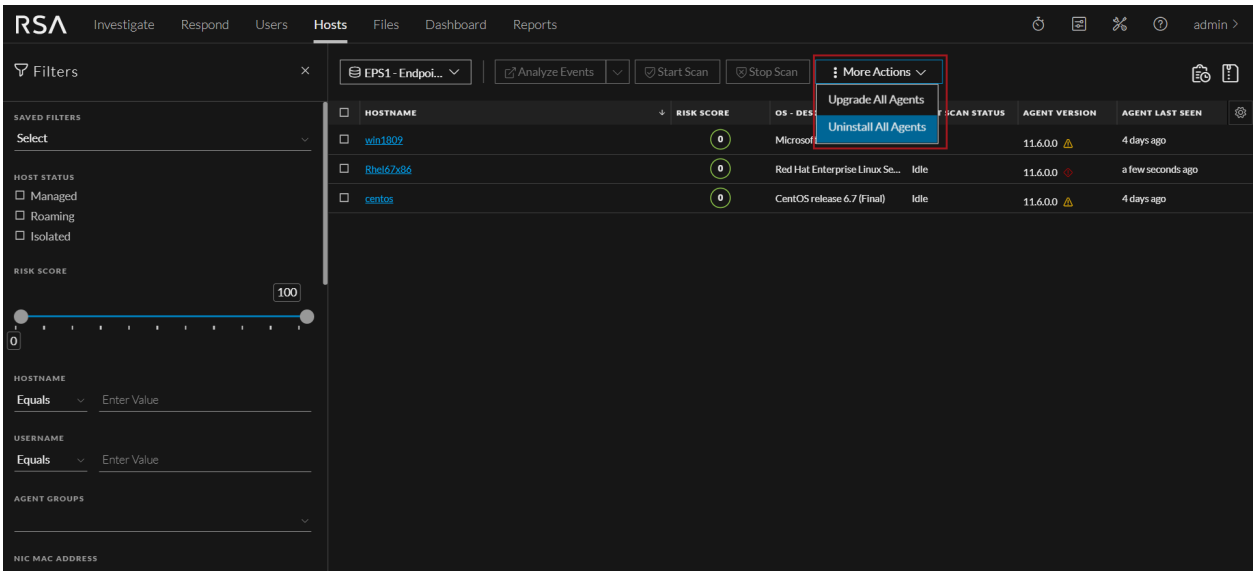

## UIを使用した集中型エージェント アップグレード オプション

管理者は、UIを使用して、選択したエージェントまたはすべてのエージェントをアップグレードおよびアンインストールできるようになりました。これにより、NetWitnessエージェントを非常に簡単に管理できます。詳細については、『*NetWitness Endpointエージェント インストール ガイド*』を参照してください。



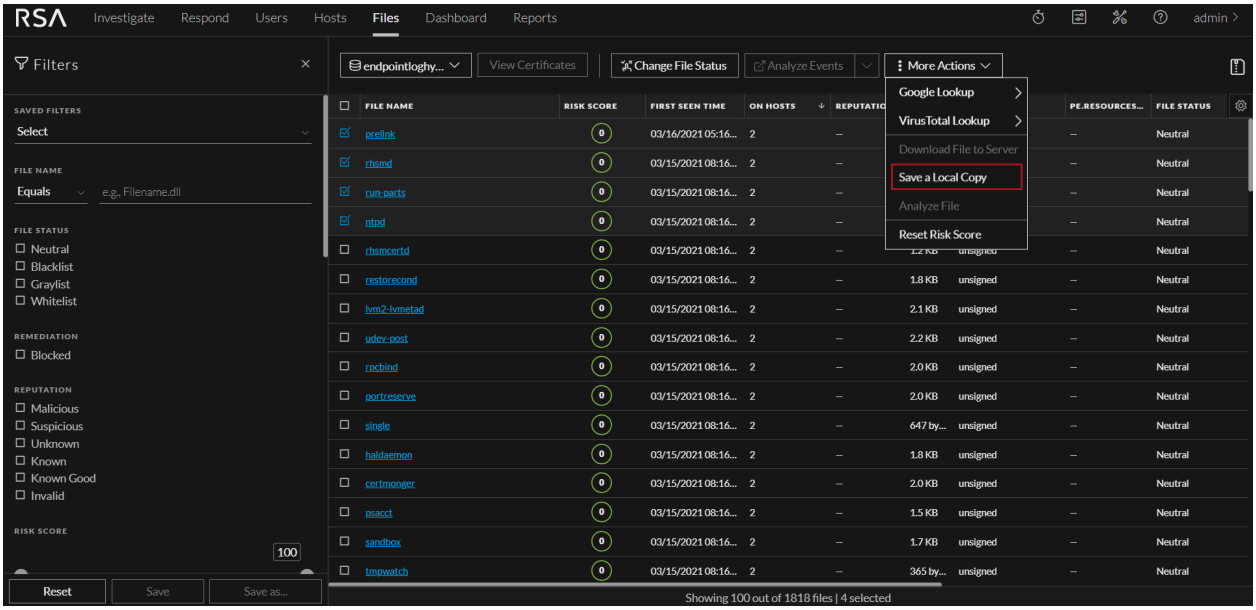
## UIを使用した集中型エージェント アンインストール オプション

管理者は、UIを使用して、選択したエージェントまたはすべてのエージェントを簡単にアンインストールできます。ホストを選択しなくても一括アンインストールが可能です。この機能拡張により、時間が節約され、脅威への対応により集中できるようになります。一括アンインストールの利用資格を満たすには、エージェントがバージョン11.5.1以降である必要があります。詳細については、『*NetWitness Endpoint*エージェント *インストール ガイド*』を参照してください。



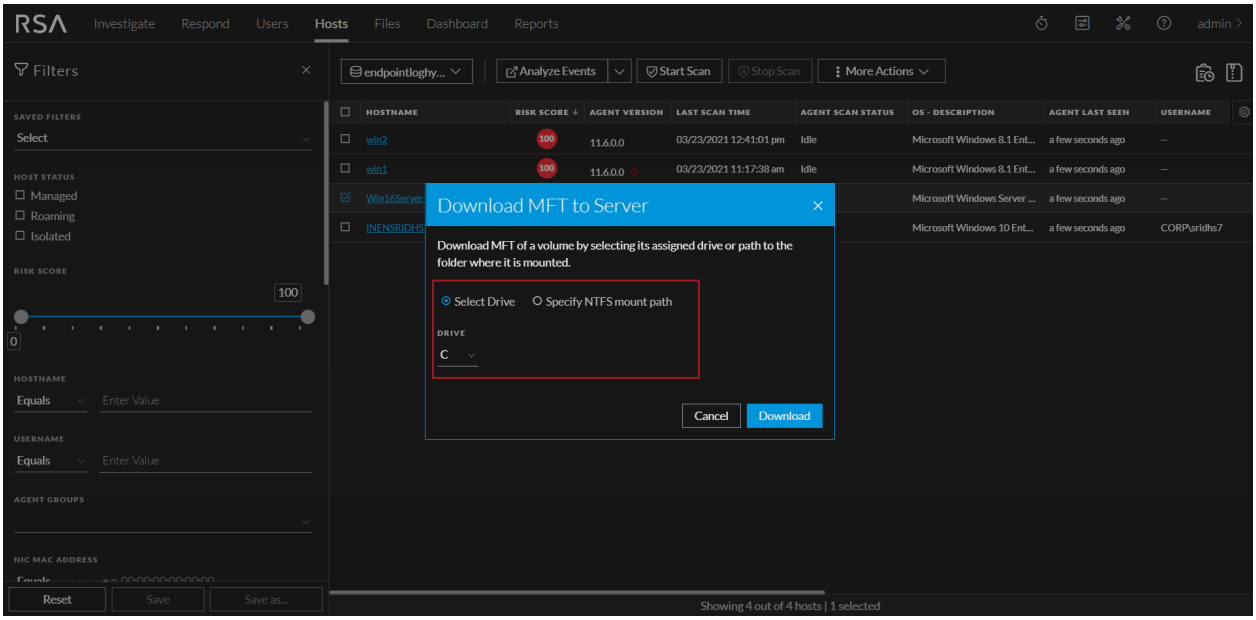

## 複数のダウンロード済みファイルのローカル コピー保存のサポート

アナリストは、ダウンロードしたシステム ダンプ、プロセス ダンプ、MFTなどのコピーを保存することで、詳細な調査とフォレンジックをすばやく簡単に実行できるようになりました。



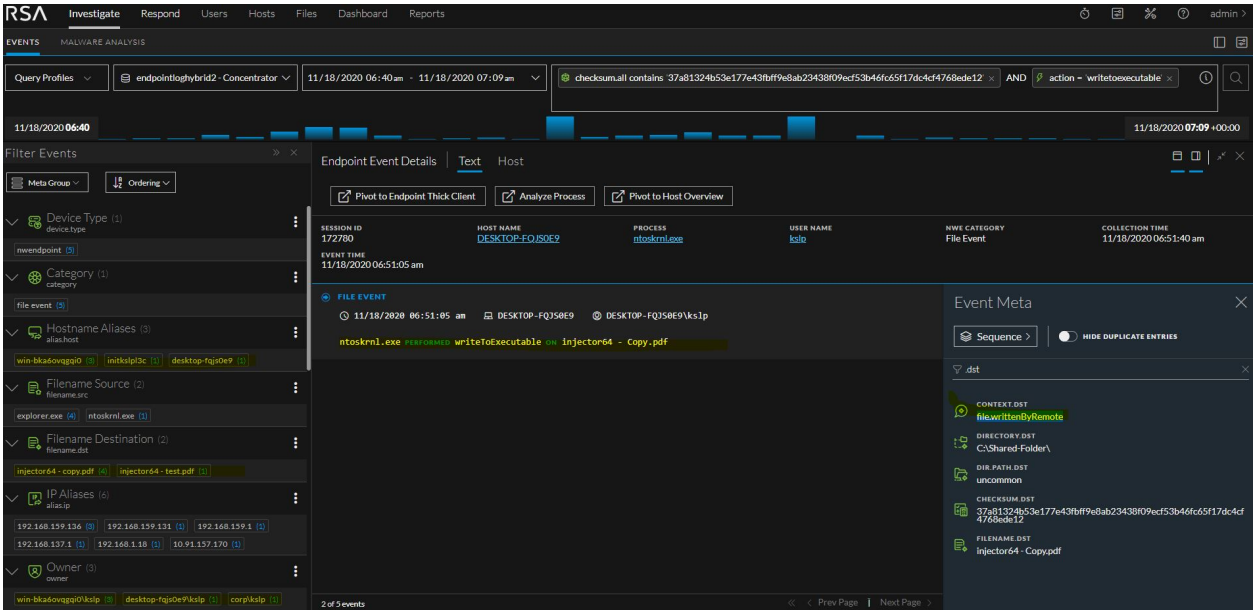
## 任意のWindowsドライブからのMFTのダウンロードのサポート

アナリストは、任意のドライブのMFTをダウンロードして、NTFSマウント パスにダウンロードすることもできるようになりました。これにより、アナリストはシステム ボリュームに加えて、ファイルに対しても重要な調査、分析、フォレンジックを実行できます。



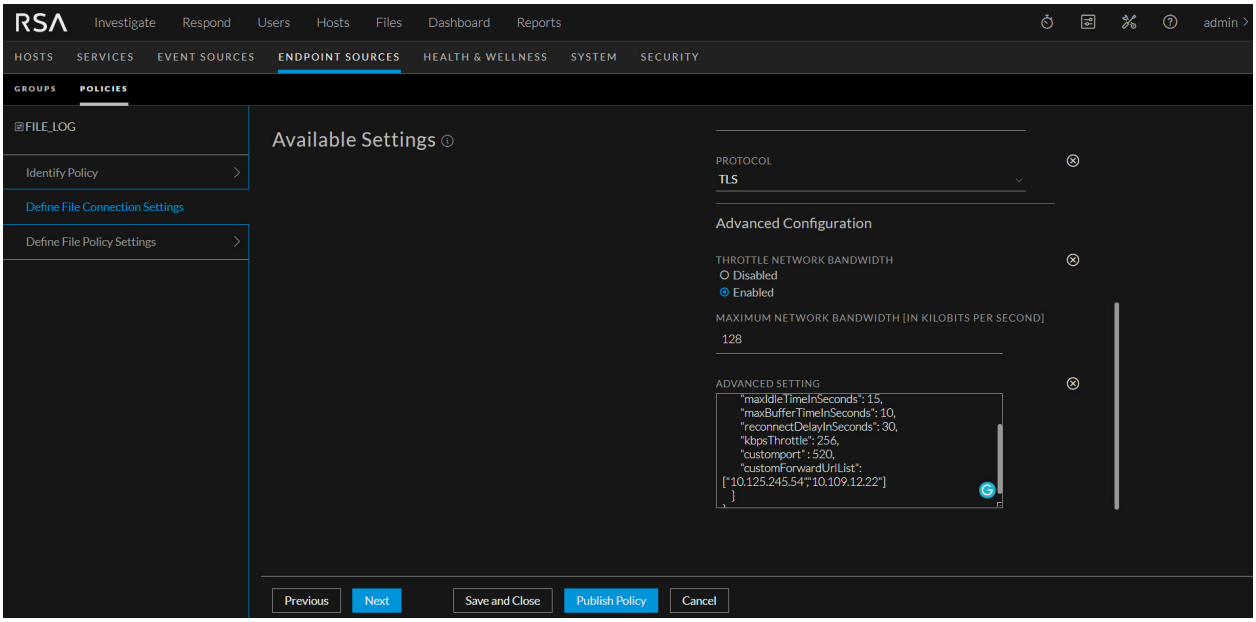

## 横方向の動きの可視性の拡大

Windowsエージェントが、ネットワーク共有へのコピー時にターゲット マシンで実行可能な書き込みイベントを報告するように機能拡張されました。アナリストは、ネットワーク共有にコピーされているファイルの周辺で起こっている、Windowsでの横方向の移動アクティビティをより詳細に可視化できるようになりました。



### カスタム システムへのWindows/ファイル ログ転送 のサポート

管 理 者 は、Windowsログとファイル ログをカスタムシステムに転 送 することにより、非VLCシステムでこれらのログを収 集 できるようになりました。




### 永続性の発見検知戦術に追加された新しいルール

永 続 性 戦 術 に従う脅 威 を検 出 するための新しいルールが、エンドポイント ルール バンドルに追 加 されました。このような脅 威 が検 出 されると、これらのルールによってアラートがトリガーされ、リスク スコアが高まります。

## Broker、Concentrator、Decoder、Log Decoderサービス

### アセンブラー スレッディング モード

Decoderがデータを分 析 できるスループットを向 上 させるため、アセンブラーはさらなる並 列 処 理 を実 行するように拡 張 されました。収 集 されたパケットをストリームに再 アセンブルするプロセスは、アセンブラと呼 ばれます。2つのモードを使 用 して、アセンブラー操 作 をカスタマイズできるようになりました。これらのモードを構 成 するには、`assembler.threading.enabled`の値を`on`または`off`に設 定 します。デフォルト値 は`off`です。`on`モードでは、各 アセンブラ インスタンスが専 用 プロセッサーで動 作 するため、スループットを向 上 させることができます。

アセンブラ モードは、複 数 アダプタによるパケット収 集 が有 効 になっている場 合 にのみ機 能 します。複 数 アダプタによるパケット収 集 とアセンブラ モードの詳 細 については、『*Decoder*および*Log Decoder*構 成 ガイド』の「( オプション) 複 数 アダプタによるパケット収 集 」を参 照 してください。

### 高 速 パケット収 集

高 速 ネットワークからのネットワーク データ( パケット) を分 析 し、Network Decoderを最 適 化 して最 大 40 Gbpsのネットワークトラフィックを収 集 できるようになりました。さまざまなネットワーク速 度 でどの機 能 がサポートされるかを理 解 するため、Decoderは次 の3つのモードで動 作 するようになりました。

1. **通 常** : ネットワーク セッションの保 存 中 に大 量 のディープ パケット インスペクションを行う、5 Gbps未 満 の収 集 速 度 の場 合 。これはデフォルトのモードです。

2. **10G**: ネットワーク セッションの保存中に中程度のディープ パケット インスペクションを行う、最大10 Gbpsの収集速度の場合。
3. **NDR**: メタデータのみを保存しながら少量のディープ パケット インスペクションを行う、10 Gbpsをから40 Gbpsまでの間の収集速度の場合。

高速収集とその構成方法の詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「高速パケット収集機能の構成(バージョン11.6以降)」を参照してください。

### Brotli解凍のサポート

Decoderは、HTTP/HTTPSセッション解析でBrotliペイロードを検出して解凍するようになりました。Brotliは、汎用LZ77ロスレス圧縮アルゴリズム、ハフマン符号、2次コンテキスト モデリングの特定の組み合わせを使用してデータ ストリームを圧縮するデータ フォーマット仕様です。Brotliエンコーディングは、ほとんどのWebブラウザー、主要なWebサーバー、および一部のCDNでサポートされています。

Brotli解凍を有効化するには、次の手順を実行します。

- HTTP解凍構成については、『DecoderおよびLog Decoder構成ガイド』の「HTTPパーサ"」を参照してください。
- HTTP_lua解凍構成については、『RSA NetWitness® Platform Threat Intelligenceガイド』の「HTTP Luaパーサ オプション"」を参照してください。

### OpenApp IDのサポート

Decoderは、OpenApp ID検出器を使用してアプリケーションを識別し、新しいメタデータを生成できます(`app.id`)。これにより、アナリストはセッション内のアプリケーションを識別できます。CiscoのOpenApp IDは、Snort(オープンソースのネットワーク侵入検出システム)用のアプリケーション層ネットワーク セキュリティ プラグインであり、ネットワークトラフィックでアプリケーションを識別するオープンソースのLuaライブラリー(検出器)のセットです。

OpenApp IDの詳細と検出器の構成方法については、『*DecoderおよびLog Decoder構成ガイド*』の「(オプション) OpenApp IDをサポートするようにDecoderを構成する」を参照してください。

### 受信側スケーリングのサポート

Decoderがデータを分析できるスループットを向上させるため、セッションを作成するパイプラインは、受信側スケーリング(RSS)を使用するように拡張されています。RSSを使用すると、マルチプロセッサー システムの複数のCPUにネットワーク受信処理を効率的に分散できます。RSSにより、特定の接続に関連づけられている処理が割り当て済みCPUにとどまるようになります。RSSは、ixgbeまたはi40eデバイスドライバーを使用するDPDKデバイスでのみサポートされます。

詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「(オプション) データ プレーン開発キット パケット収集」を参照してください。

### 暗号化および復号化されたトラフィック ストリームのDecoderへの同時取得

マルチアダプタ収集およびマルチスレッド アセンブラ機能が有効になっているDecoderは、別々のアダプター上にある場合に同じトラフィックの暗号化および復号化ストリームを受信できます。これは、同じトラフィックの暗号化版と復号化版の両方が同じDecoderを通過する場合のユースケースをサポートします。マルチスレッド アセンブラ機能により、Decoderは対応する収集ワーク スレッドからパケットをアセンブルできます。これにより、暗号化セッションと復号化セッションからのパケットがアセンブリ中に分離されるため、セッションの解析とコンテンツの抽出の不正確さを回避できます。

詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「着信パケットの復号」を参照してください。

### アグリゲーション ホストのための信頼できる認証

集計接続を構成する場合、サービス アカウントの認証情報を使用する代わりに、信頼できる認証を使用してこのタスクを実行できます。信頼できる認証により、サービス アカウントのパスワード変更を管理する必要がなくなるため、管理者のオーバヘッドが軽減します。

この認証方法の変更には、デバイスがオフラインであることが必要となります。また、信頼できる認証に切り替えた後で、ユーザの認証情報を使用するログイン方法に戻すことはできません。

## Event Stream Analysis( ESA)

### メタ エンティティのサポート

メタ エンティティは、類似したメタ キーをリンクする方法を提供します。メタ エンティティが定義されると、エンティティをキーと同じように使用できるため、アナリストはメタ エンティティを通常のキーとして使用して、複数の同様の概念に到達できます。11.6リリース以降、メタ キー エンティティはイベント スキーマの一部として構成され、文字列[]メタ キー エンティティを有効化できます。アナリストは、選択したメタ キー エンティティに基づいてルールを作成し、アラートを構成できます。また、メタ エンティティを追加してルールを作成することもできます。メタ エンティティは、データ ソースからデータを取得して、アラートをトリガーします。

- メタ エンティティのリストを表示するには、「メタ エンティティのリストの表示」を参照してください。
- ESA Correlationサーバでメタ エンティティを有効にするには、「ESA Correlationサーバでのメタ エンティティの有効化」を参照してください。
- カスタム メタ エンティティを使用してルールを作成するには、「カスタム メタ エンティティを使用したルールの作成」を参照してください。

詳細については、『*NetWitness ESA アラート ユーザー ガイド*』を参照してください。

### 位置追跡情報のインポートと編集

データ ソースを導入すると、デフォルトで、ESAは利用可能な最新のセッションから情報の処理を開始します。位置追跡情報により、管理者はESAによって処理されたセッションの進行状況を可視化し、セッションIDとイベントが処理された日時に関する情報を確認できます。

- 編集機能を使用すると、位置追跡を編集した後で、特定のESAデータ ソースによって分析されるセッションの数を可視化し、処理されたセッションの数を確認して、作業を計画できます。位置追跡情報を編集するには、「位置追跡情報の編集」を参照してください。
- インポート機能を使用すると、既存の導入環境から同時に1つ以上のデータ ソースの位置追跡の設定を移行できます。位置追跡情報をインポートするには、「位置追跡情報のインポート」を参照してください。
- ユースケース シナリオを確認するには、「ユースケース シナリオ」を参照してください。

### 信頼できる認証の活用

データ ソースを操作しているときに、管理者の認証情報を使用してログインする代わりに、信頼できる認証を使用してさまざまなタスクを実行できます。データ ソースにアクセスするたびに、管理者の認証情報を使用してログインする必要はありません。

詳細については、『*NetWitness スタート ガイド*』の「信頼できる認証」を参照してください。

### Detect AIのサポート

[対応]ビューのアラート ソースとして[AIの検出]が追加されました。これにより、クラウド ベースのユーザ行動分析からアラートが収集され、アラートからインシデントが作成されます。

アラート名、アラート ソース、特定の時間範囲などのフィルタでアラート リストを絞り込んで、目的のアラートを表示することができます。

詳細については、「アラートのサマリーの表示」を参照してください。

## 管理と構成

### 不要なダッシュボードの削除

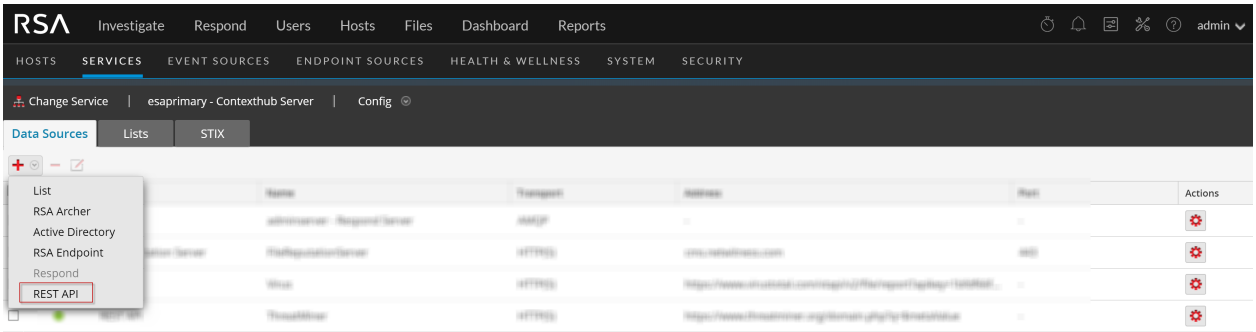
ダッシュボードのクリーニング ジョブを有効にすることで、冗長なダッシュボード(所有されていないダッシュボード、共有されていないダッシュボード、および重複するデフォルトのダッシュボード)を削除できます。

詳細については、「不要なダッシュボードの削除」を参照してください。

## Context Hub

### REST APIデータ ソースのサポート

NetWitness Platform 11.6では、RESTful APIデータ ソースをContext Hubに追加する機能が導入されています。




REST APIを使用すると、アナリストはクエリ パラメータとしてメタ値を提供し、結果をContext Hubパネルにリアルタイムでレンダリングすることで、サード パーティー アプリケーションをクエリできます。結果は、サード パーティー アプリケーションの設定と機能に応じて、JSONまたはHTML形式でレンダリングできます。アナリストは、NetWitness Platformを離れることなく、IP、ユーザー、ホスト、またはファイルに関する追加のコンテキストを調査中により迅速に取得できるようになりました。

### コンテキスト ハイライト表示の機能強化

特定の環境で機能をより使いやすく効率的にするために、コンテキスト強調表示機能にいくつかの追加構成が導入されています。管理者は、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、対応、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 パネルを開いているときにすべてのソースからの結果を表示できますが、[**調査**]>[**移動**]、[**イベント**]、[**対応**]の各ビューでは値は強調表示されません。管理者は、コンテキストの強調表示をすべてのソースに対してグローバルに無効にすることもできます。

詳細については、『*Context Hub構成ガイド*』の「REST APIをデータ ソースとして構成する」を参照してください。

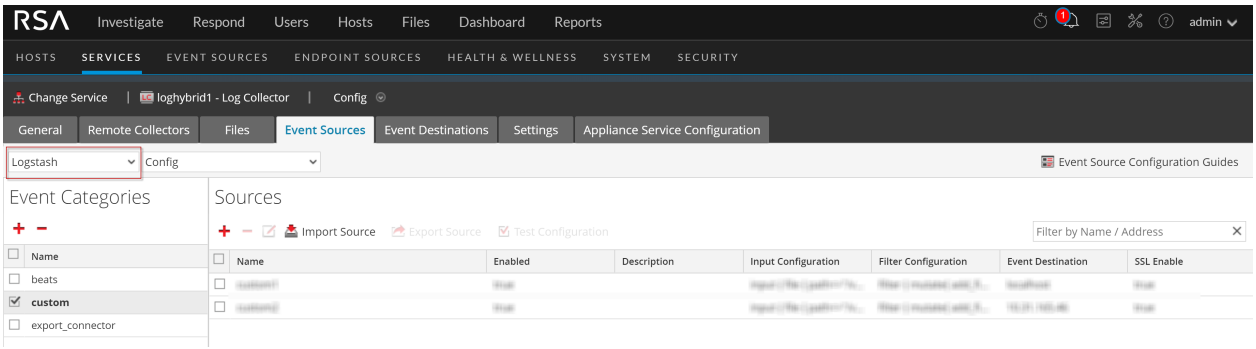
# ログ収集

## マネージド Logstashのサポート

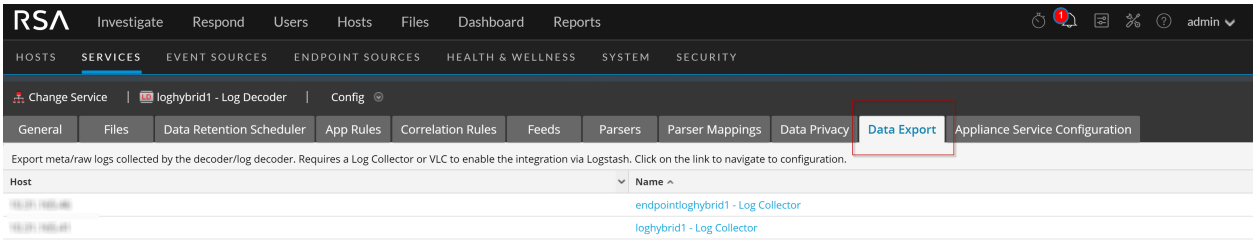
11.5では、Logstash用のNetWitness出力コーデックが導入され、お客様によって管理されるLogstashサーバーとのLogstash統合が可能になりました。11.6以降、Logstashサーバーは、NetWitness Log CollectorまたはVirtual Log Collector( VLC) サービスとともにパッケージ化およびサポートされ、Logstashに簡単にアクセスできるようになります。これはマネージドLogstashと呼ばれ、NetWitness Platformの外部に個別のLogstashサーバーを配置する必要性を排除します。

Log Collectorサービス内の[イベント ソース]タブで、Logstashパイプライン( ビート、エクスポート コネクターなど) を作成できます。カスタム カテゴリーでは、完全にカスタムのLogstashパイプライン構成が可能です。

以下は、Logstashイベント ソースの例です。




新しい[データ エクスポート]タブがDecoderまたはLog Decoder構成ビューに追加されました。ここには、ご使用の環境で使用可能なLog Collectorサービスが一覧表示されます。Log Collectorサービスを選択すると、[イベント ソース]タブでエクスポート コネクターを構成できます。



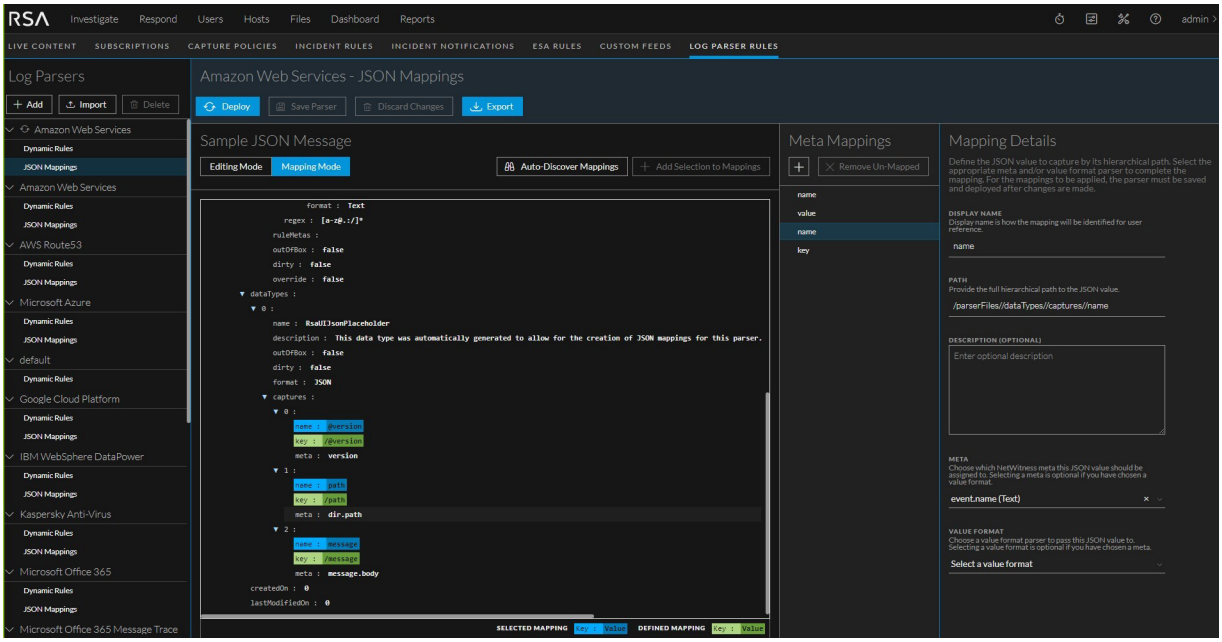

また、各Logstashパイプラインの稼働状態とスループットを監視できるよう、レガシーと新しいヘルス モニターの両方の新しい統計が導入されています。新しい統計情報を表示するためのLogstash入力プラグインの概要ダッシュボードが追加されました。

詳細については、『*ログ収集の構成ガイド*』の「NetWitness PlatformでLogstashイベント ソースを構成する」を参照してください。

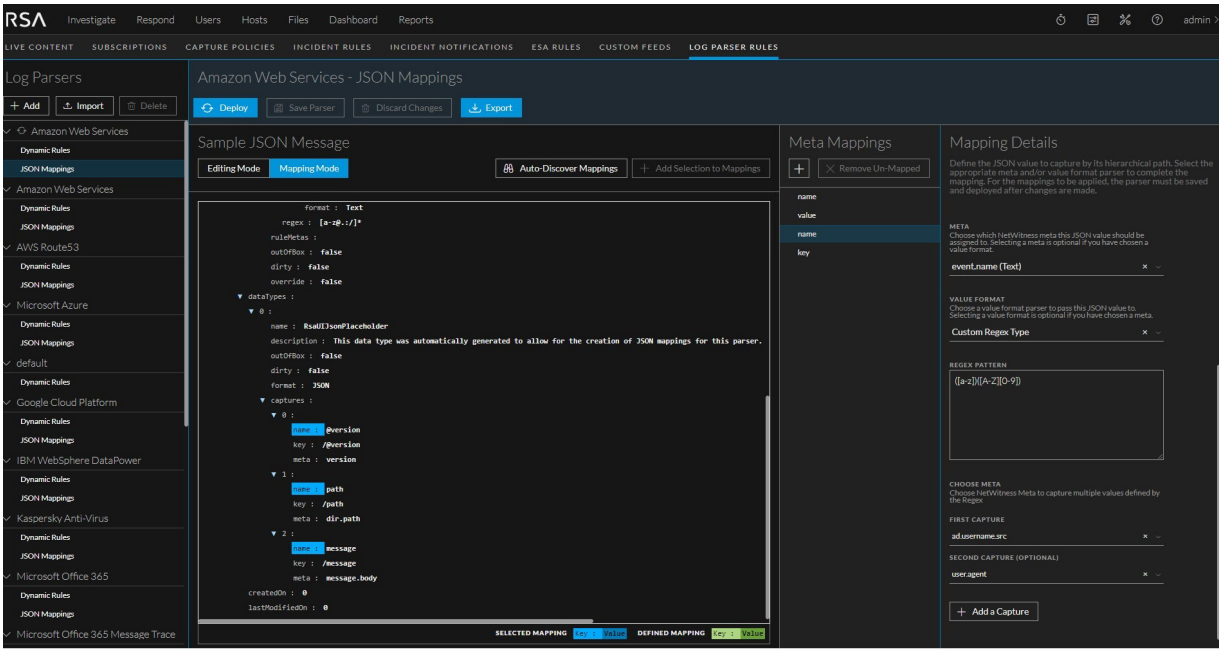
## 解析ルールUIの機能強化

- **JSONマッピングの操作性の向上** - JSONサンプルのツリー ビューでは、一致するものが存在する場合、対応するRAWノードまたはマッピング エントリのいずれかが選択されているときに強調表示され

ます。強調表示は、現在のサンプルで一致が成功したかどうかを示します。つまり、値はノード パスとDataTypeまたはRegExを含めて正しく解析される必要があります。




- **JSONマッピングのカスタム正規表現** - JSON値( たとえば、ip:port) を細かく解析するために、ユーザーはUI内のマッピングごとにカスタム正規表現パターンを作成できます。複数の値( キャプチャ) を抽出して、個別のメタ キーに割り当てることができます。




- **カスタムUIルール( 動的ルールまたはJSONマッピング) のインポートまたはエクスポート** - UIで作成されたカスタム動的ルールとJSONマッピングを、UIから直接簡単にインポートまたはエクスポートできるようになりました。これによりお客様は、ある環境( ラボ環境など) で解析ルールを開発してから、それを別の環境( 本番環境など) に移動できます。

詳細については、『*ログ パーサ構成ガイド*』を参照してください。

> **注：** カスタムUIルールのインポートまたはエクスポートでは、解析ルールに対応する「parser.XML」または「parser_custom.XML」はエクスポートまたはインポートされません。

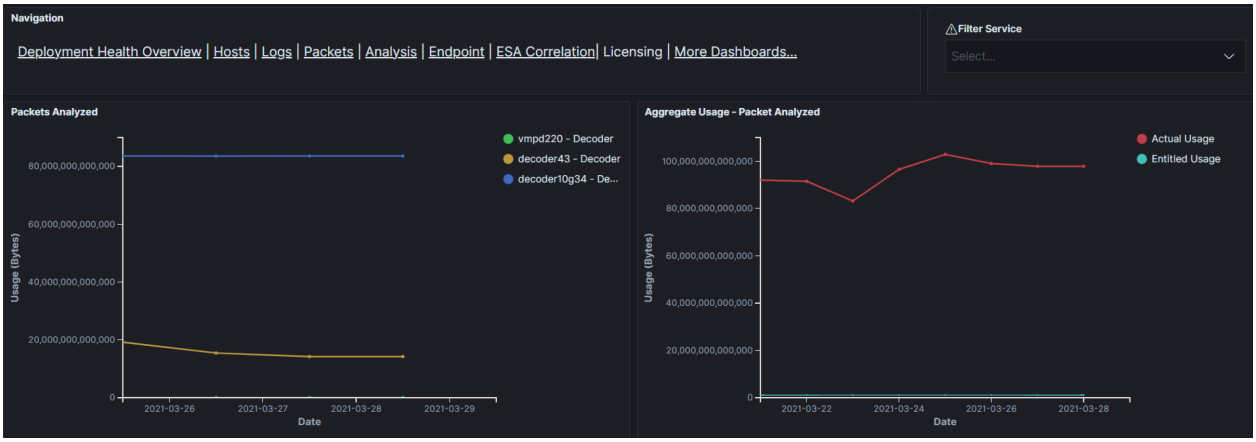
# ライセンス

## ライセンス使用ダッシュボードの導入

ライセンスを効率的に管理するために、新しいライセンス ダッシュボードが新しいヘルス モニターに導入されました。このダッシュボードは、導入環境内のすべてのスループット ライセンスのライセンス使用状況に関する洞察を提供します。管理者は、このダッシュボードで次のことを実行できます。

- 個々のホストの毎日のライセンス使用状況を追跡する
- 導入環境内のすべてのホストのスループット ライセンスの毎日の使用状況を追跡する
- ライセンス使用状況レポートをダウンロードする

詳細については、『システム メンテナンス ガイド』の「ライセンス使用状況ダッシュボード」を参照してください。




# スループット ライセンス計算の変更

NetWitness Platformバージョン11.5.1から11.6には、ネットワーク( パケット ) スループットの使用状況のレポート作成で使用されるメトリックの修正が含まれています。ライセンス メトリックには、分析された全体的なネットワークトラフィックと、分析後に保存されたRAWネットワーク データが含まれます。ネットワーク スループット ライセンスの使用量が増える可能性があり、状況によってはライセンス違反のバナーが表示される場合があります。ネットワーク スループット ライセンスのコンプライアンス違反通知は、ライセンス違反バナーの表示を45日遅らせるように調整されました。詳細については、『*ライセンス管理ガイド*』を参照してください。

# プラットフォーム

### サードパーティ サーバ ハードウェアのサポート

これにより、サード パーティのサーバ ハードウェアを使用してNetWitness Platformを実行できます。キックスタート ウィザードでは、使用可能なブロック デバイスのリストが表示され、OSおよびNetWitness Platformアプリケーションをインストールするデバイスを選択するよう求められます。詳細については、『*物理ホスト インストール ガイド*』の「インストール タスク」を参照してください。

# 修正された問題

このセクションでは、最後のメジャー リリース後に修正された問題のリストを提供します。修正された問題の詳細については、RSA Linkに掲載されている「RSA NetWitness® Platformの既知の問題リスト」の「修正された問題」列を参照してください。

## ログ収集の修正

| 追跡番号 | 説明 |
|---|---|
| ASOC-94276 | TCPシステム パフォーマンスの向上 |

## 管理の修正

| 追跡番号 | 説明 |
|---|---|
| SACE-13620 | バージョン11.4では、Decoderグループに再帰フィードを導入できません。 |
| SACE-13572 | msearchオプションを使用してクエリを実行すると、「年が有効な範囲( 1400～9999) に収まっていない」というエラーが表示されます。 |
| SACE-13278 | 11.4にアップグレードした後、NetWitness Platformへのログイン中にログイン バナーが表示されません。 |
| SACE-13124 | 15ドライブのViper Shelfのディスクが「UBad」状態の場合、RAIDツールス クリプトは失敗します。 |
| SACE-13060 | [メール通知の定義]パネルでは、ドメイン名の後に( .) 記号が付いている場合にドメイン名を含むメール アドレス( たとえば、XXX@abc.xyz.com) を入力できません。 |

## 監査ログ

| 追跡番号 | 説明 |
|---|---|
| ASOC-85468 / ASOC-86055 | RabbitMQがリセットされた場合、LogstashがRabbitMQに再接続しません。 |

| 追跡番号 | 説明 |
| --- | --- |
| ASOC-77307 | ルール ビルダーでESAルールが作成、複製、または削除された場合に、監査ログに十分なコンテキストがありません。NetWitness Platform 11.5では、ESA Correlation Serverで利用可能な監査ログに加えて、ユーザがルール ライブラリーでESAルールをいつ追加、変更、フィルタ処理、削除、エクスポート、およびインポートしているかが、NetWitness Serverの新しい監査ログに表示されます。NetWitness Serverの監査ログには、ユーザがESAルールの導入環境を追加、変更、および導入するタイミングも表示されます。ESAルール導入環境の変更には、導入環境内のルールの追加、削除、または更新、および導入環境へのデータ ソースまたはESA Correlationサービスの追加が含まれます。 |

## 調査の修正

| 追跡番号 | 説明 |
| --- | --- |
| ASOC-92642 | [イベント]ビューで、円記号(\)文字を含む値を再フォーカスしても、結果が返されません。 |
| ASOC-92534 | メールの再構築では、ファイル名が一致しないため、添付ファイルの[ダウンロード]ボタンが有効になっていません。 |
| ASOC-85375 | ®などの特殊文字を含む値を使用してメタ キーをクエリすると、特殊文字が切り捨てられます。 |
| ASOC-50412 | ダウンロードを開始すると、ブラウザーのジョブ トレイへの接続が失敗し、ダウンロード スピナーが表示されたままになります。 |

## 対応の修正

| 追跡番号 | 説明 |
|---|---|
| ASOC-80896 | Reporting Engineアラートによって生成されたインシデントは、データ プライバシーが有効になっているにもかかわらず、クリア テキスト値を表示します。以前は、データ プライバシーが有効になっている導入環境では、クリア テキストとハッシュ値の両方が公開されるため、Reporting Engineアラートから生成されたインシデントにクリア テキスト メタデータが表示されていました。この問題が修正され、データ プライバシーが有効になっている場合に、Reporting Engineはハッシュ/難読化された値のみをRespondに送信するようになりました。これにより、アナリストがインシデントを表示するときにデータ プライバシーが維持されます。 |
| ASOC-73173 | イベントのファイル名がグローバル ファイル名と一致しない場合、一致するファイルが[**ファイル**]タブに表示されません。以前は、ファイルを分析するためにノード グラフから[**調査**]>[**ホスト**]または[**ファイル**]タブに移動したときに、イベントのファイル名がグローバル ファイル名の大文字と小文字の区別と一致していない場合、結果は表示されませんでした。この問題が修正され、[**調査**]>[**ホスト**]または[**ファイル**]タブに移動したときに、大文字と小文字の区別が問題にならなくなりました。 |

## コア サービス( Broker、Concentrator、Decoder、Archiver) の修正

| 追跡番号 | 説明 |
|---|---|
| ASOC-90740 | Log Decoderサービスは、再起動時にコアダンプしていました。 |
| SACE-13702 | Rest APIを使用してBrokerに対してクエリを実行すると、カウントの相違に関する誤った結果が表示されます。 |
| SACE-13597 | TLSセッションの場合、JA3/JA3sとcert.thumbprintのメタ キーは生成されません。 |

## Event Stream Analysis( ESA) の修正

| 追跡番号 | 説明 |
|---|---|
| ASOC-87778 | コロン( :) が付いたESAルール導入環境名は、ストリームの開始に失敗したというエラーをスローします。ESAルールの導入環境名にコロン( :) が含まれている場合は、導入時にデータ集計を開始できません。 |
| ASOC-77307 | ルールビルダーでESAルールが作成、複製、または削除された場合に、監査ログに十分なコンテキストがありません。 |
| SACE-12736 | 複数のユーザが同時にESAルールの導入環境を編集し、変更を上書きできます。2人のユーザがルールを追加または削除して同じESAルールの導入環境を変更する場合、[**今すぐ導入**]を最初にクリックしたユーザによってもう1人のユーザの変更が上書きされます。 |

## Reporting Engineの修正

| 追跡番号 | 説明 |
|---|---|
| SACE-12893 | [**レポート**] > [**アラート**]タブでは、カスタムの時間範囲をクエリしたときにすべてのアラートが表示されるわけではありません。 |

## エンドポイントの修正

| 追跡番号 | 説明 |
|---|---|
| ASOC-86942 | エンドポイント サーバーは、導入日の後で異常な状態になることがよくあります。 |
| SACE-13763 | NetWitness Endpoint AgentをRedhat 8.xシステムにインストールできません。 |

## スプリングボードの修正

| 追跡番号 | 説明 |
| --- | --- |
| ASOC-106211 / ASOC-106350 | 高リスク ユーザの情報が、スプリングボードの[上位の高リスク ユーザ] パネルとカスタム パネルに表示されません。 |

## 更新の修正

| 追跡番号 | 説明 |
| --- | --- |
| SACE-12658 | 固定IPアドレスのCLIでnwsetup-tuiコマンドを実行すると、構成が失敗します。 |

## Threat Intelligenceの修正

| 追跡番号 | 説明 |
| --- | --- |
| ASOC-100727 | 繰り返しカスタム フィードがフェールオーバー時にコアにプッシュされません。 |

# サポートが終了する機能

次の表に、RSA NetWitness Platform 11.6以降のリリースでサポートが終了する機能の情報を示します。

## 11.6.0.0以降のリリースでサポートが終了する機能

| 機能 | メモ |
| --- | --- |
| Live Connectデータ ソース | Live Connectデータ ソースは、NetWitness Platform11.6以降のリリースではサポートされていません。 |

# 製品ドキュメント

このリリースでは、次のドキュメントが提供されます。

| マニュアル | 参照場所 |
| --- | --- |
| RSA NetWitness Platform 11.x Master Table of Contents | https://community.rsa.com/t5/rsa-netwitness-platform/ct-p/netwitness-documentation |
| RSA NetWitness Platform 11.6 Product Documentation | https://community.rsa.com/ |
| RSA NetWitness Platform 11.6アップグレード ガイド | https://community.rsa.com/t5/rsa-netwitness-platform-online/tkb-p/netwitness-online-documentation |

# 製品ドキュメントへのフィードバック

RSA NetWitness Platformのドキュメントに関するフィードバックは、nwdocsfeedback@rsa.comまでメールで送信してください。

# NetWitness Platformのヘルプ情報

## セルフ ヘルプ リソース

NetWitness Platformのインストールおよび使用について支援が必要な場合は、次の情報をご利用ください。

- NetWitness Platformに関するすべてのドキュメントは、次の場所から参照できます。
  https://community.rsa.com/community/products/netwitness/documentation
- 特定の情報を見つけるには、以下のRSAリンクの[**検索**]および[**質問**]フィールドを使用します。
  https://community.rsa.com/welcome
- RSA NetWitness Platformのナレッジベース: https://community.rsa.com/community/products/netwitness/knowledge-baseを参照してください
- RSA NetWitness Platformのトラブルシューティング: https://community.rsa.com/community/products/netwitness/documentation/troubleshootingを参照してください
- RSA NetWitness® Platformブログの記事も参照してください。
- さらに支援が必要な場合は、カスタマー サポートにお問い合わせください。

## カスタマー サポートへのお問い合わせ

カスタマー サポートに連絡する場合は、コンピューターを操作できる状態である必要があります。以下の情報を提供できるように準備しておいてください。

- お使いのRSA NetWitness Platform製品またはアプリケーションのバージョン番号
- お使いのハードウェアのタイプ

質問や支援が必要な場合は、以下の連絡先までお問い合わせください。

| | |
|---|---|
| RSA Link | https://community.rsa.com<br>メインメニューで[**My Cases**]をクリックします。 |
| 各国のお問い合わせ窓口 | https://community.rsa.com/docs/DOC-1294 |
| コミュニティ | https://community.rsa.com/community/support |

# ビルド番号

以下の表は、NetWitness Platform 11.6.0.0の各種コンポーネントのビルド番号の一覧です。

| コンポーネント | バージョン番号 |
|---|---|
| NetWitness Platform Audit Plugins | rsa-audit-plugins-11.6.0.0-4671.5.25a824322.el7.noarch.rpm |
| NetWitness Platform Appliance | rsa-nw-appliance-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Archiver | rsa-nw-archiver-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Broker | rsa-nw-broker-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Concentrator | rsa-nw-concentrator-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Config Management | rsa-nw-config-management-11.6.0.0-2104212116.5.d60ffff.el7.noarch.rpm |
| NetWitness Platform Config Server | rsa-nw-config-server-11.6.0.0-210331045328.5.6fe2c5e.el7.centos.noarch.rpm |
| NetWitness Platform Console | rsa-nw-console-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Content Server | rsa-nw-content-server-11.6.0.0-210318023955.5.2647b0c.el7.centos.noarch.rpm |
| NetWitness Platform ContextHub Server | rsa-nw-contexthub-server-11.6.0.0-210331043419.5.3d6abd0.el7.centos.noarch.rpm |
| NetWitness Platform Correlation Server( ESA) | rsa-nw-correlation-server-11.6.0.0-210415073028.5.3610f9b.el7.centos.noarch.rpm |
| NetWitness Platform Decoder | rsa-nw-decoder-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Deployment Upgrade | rsa-nw-deployment-upgrade-11.6.0.0-2103151416.5.f557d92.el7.noarch.rpm |
| NetWitness Platform Endpoint Agents | rsa-nw-endpoint-agents-11.6.0.0-2103311945.5.bd1280b.el7.x86_64.rpm |
| NetWitness Platform Endpoint Broker Server | rsa-nw-endpoint-broker-server-11.6.0.0-210331080032.5.2bc8f1d.el7.centos.noarch.rpm |
| NetWitness Platform Endpoint Server | rsa-nw-endpoint-server-11.6.0.0-210406104611.5.4c9695b.el7.centos.noarch.rpm |

| | |
|---|---|
| NetWitness Platform Integration Server | rsa-nw-integration-server-11.6.0.0-210331043939.5.385a853.el7.centos.noarch.rpm |
| NetWitness Platform Investigate Server | rsa-nw-investigate-server-11.6.0.0-210430143448.5.fb23b39.el7.centos.noarch.rpm |
| NetWitness Platform Legacy Web Server | rsa-nw-legacy-web-server-11.6.0.0-210504044611.5.9ec73de.el7.centos.noarch.rpm |
| NetWitness Platform License Server | rsa-nw-license-server-11.6.0.0-210503080758.5.619d23a.el7.centos.noarch.rpm |
| NetWitness Platform Log Decoder | rsa-nw-logdecoder-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Log Player | rsa-nw-logplayer-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform Malware Analytics Server | rsa-nw-malware-analytics-server-11.6.0.0-210325105147.5.293bed9.el7.centos.x86_64.rpm |
| NetWitness Platform Metrics Server | rsa-nw-metrics-server-11.6.0.0-210421095948.5.37b59af.el7.centos.noarch.rpm |
| NetWitness Platform Orchestration Server | rsa-nw-orchestration-server-11.6.0.0-210316174042.5.c0a599c.el7.centos.noarch.rpm |
| NetWitness Platform Reporting Engine Server | rsa-nw-re-server-11.6.0.0-5893.5.6eab5cd2a.el7.x86_64.rpm |
| NetWitness Platform Respond Server | rsa-nw-respond-server-11.6.0.0-210428102736.5.64efcea.el7.centos.noarch.rpm |
| NetWitness Platform Root CA Update | rsa-nw-root-ca-update-11.6.0.0-2011031833.5.745f08a.el7.noarch.rpm |
| NetWitness Platform SDK | rsa-nw-sdk-11.6.0.0-11374.5.fe9457e29.el7.x86_64.rpm |
| NetWitness Platform Security Server | rsa-nw-security-server-11.6.0.0-210330025250.5.ab7b8b1.el7.centos.noarch.rpm |
| NetWitness Platform Source Server | rsa-nw-source-server-11.6.0.0-210414045818.5.348fe73.el7.centos.noarch.rpm |
| NetWitness Platform User Interface | rsa-nw-ui-11.6.0.0-210503011255.5.5f8590a66a.el7.centos.noarch.rpm |
| NetWitness Platform Workbench | rsa-nw-workbench-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm |
| NetWitness Platform SA Tools | rsa-sa-tools-11.6.0.0-2102240502.5.fea248a.el7.noarch.rpm |
| NetWitness Platform SMS Runtime | rsa-sms-runtime-rt-11.6.0.0-4671.5.25a824322.el7.x86_64.rpm |
| NetWitness Platform SMS Server | rsa-sms-server-11.6.0.0-4671.5.25a824322.el7.x86_64.rpm |

# 改訂履歴

| 日付 | 説明 |
| --- | --- |
| 2021年6月 | ベータ |