RSA NETWITNESS® PLATFORM

スタート ガイド

バージョン 11.2

連絡先情報

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

商標

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

使用許諾契約

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

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

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

サード パーティ ライセンス

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

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

2月 2019

目次

NetWitness Platformの概要

概要

RSA NetWitness® Platformは強力な脅威検出スイートであり、SOC(セキュリティ オペレーション センター) はNetWitness Platformにより脅威の特定、優先順位付け、トリアージを迅速に行うことができます。NetWitness Platformは既知の脅威だけでなく、未知の脅威も特定し、改善に役立ちます。パケット、ログ、エンドポイントを洞察し、企業やビジネスに対して比類のない見通しを得ることができます。

NetWitness Platformは、これまで以上に強力になると同時に、疑わしい脅威を識別し、優先度付けするプロセスが自動化されることで、Tier 1のアナリストにとっての使いやすさが向上しています。Tier 2とTier 3のアナリストは、イベントを検索してフィルタし、再構築および分析ツールを使用してイベントを調査することで、脅威を探し、特定できます。

アーキテクチャ

RSA NetWitness Platformは、分散型のモジュールで構成される柔軟性の高いシステム アーキテクチャを採用しています。このため、組織のニーズに応じてシステムを柔軟に拡張することが可能です。管理者は、NetWitness Platformを使用して、パケット データ、ログ データ、エンドポイント データの3種類のデータをネットワーク インフラストラクチャから収集することができます。NetWitness Endpoint 4.4、4.4.0.0またはそれ以降がインストールおよび構成されている場合は、エンドポイント イベント データも収集されます。このアーキテクチャの特徴を次に示します。

- **分散データ収集**。**Decoder**はパケット データを取得し、**Log Decoder**はログ データを取得します。これらのDecoderは、レイヤー2～7から収集したすべてのネットワーク トラフィック、または、多数のデバイスとイベント ソースのログとイベント データ、NetWitness Endpointデータ(インストールおよび構成されている場合) を解析および再構築します。**Concentrator**は、ネットワークまたはログ データから抽出したメタデータのインデックスを作成し、エンタープライズ環境全体にわたるクエリとリアルタイム分析で利用可能にします。また、レポート作成やアラート通知を容易に実行できるようにします。**Broker**は、他のデバイスによって収集されたデータを集計します。Brokerは、構成されたConcentratorのデータを集計します。Concentratorは、Decoderからのデータを集計します。したがって、Brokerはインフラストラクチャ全体の各種のDecoder/Concentratorに保持された複数のリアルタイム データストアを中継する役割を担います。
- **リアルタイム アラート**。NetWitness Platform **ESA(Event Stream Analysis)** サービスは、相関イベントや複雑なイベント処理など、詳細なストリーム解析を高スループットかつ低レイテンシで提供します。ESAでは、Concentratorからの大量の雑多なイベント データを処理することができます。アナリストは、ESAの先進的なEPL(イベント処理言語) によって、いくつもの異なるイベント ストリームを対象に、フィルタリング、集計、結合、パターン認識、相関を設定することができます。Event Stream Analysisによって、強力なインシデント検出やアラート通知を実装することができます。
- **リアルタイム分析** (イベントの自動分析) 。RSA自動脅威検出機能には、コマンド & コントロール トラフィックを検出するための事前構成済みのESA Analyticsモジュールが含まれています。
- **NetWitness Server**。NetWitness Serverは、レポート、調査、管理、その他のユーザ インタフェースを提供します。
- **キャパシティ**。NetWitness Platformは、DAC(直接接続) またはSAN(Storage Area Network) 接続を

使用したモジュール型のアーキテクチャで構成され、短期間の調査、長期間の分析、およびデータ保持のそれぞれのニーズに対応します。

NetWitness Platformは導入に高い柔軟性をもたらします。お客様のパフォーマンスとセキュリティに関する個別の要件に基づいて、1台から数十台までの物理ホストを使用してアーキテクチャを設計できます。また、NetWitness Platformは、仮想化インフラストラクチャ上で動作することも可能です。

システム アーキテクチャには、主要コンポーネントとして Decoder、Broker、Concentrator、Archiver、ESA、Warehouse Connectorが含まれます。これらのNetWitness Platformコンポーネントは、1つのシステムとして使用することも、個別のシステムとして使用することもできます。

- SIEM(セキュリティ情報およびイベント管理) 実装では、基本構成として次のコンポーネントが必要です : Log Decoder、Concentrator、Broker、ESA(Event Stream Analysis) 、NetWitness Server。
- フォレンジック実装では、基本構成として次のコンポーネントが必要です : Decoder、Concentrator、Broker、ESA、Malware Analysis、およびEndpoint HybridまたはEndpoint Log Hybrid。Response-Serverサービスも必要です。このサービスはアラートの優先度付けに使用されます。

それぞれの主要コンポーネントについて、次の表で簡単に説明します。

システム コンポーネント	説明
Decoder/Log Decoder	• NetWitness Platformは、パケット、ログ、エンドポイント データを収集します。 • パケット データ(ネットワーク パケット) は、ネットワーク タップまたはスパン ポートを介し、Decoderを使用して収集されます。Decoderは一般的に組織のネットワークの出口となるポイントに設置されます。 • Log Decoderは、Syslog、ODBC、Windowsイベント、フラット ファイルの4種類のログを収集できます。 • Windowsイベントは、Windows 2008の収集方式でイベント ログを収集し、フラット ファイルのログはSFTPにより収集します。 • どちらのタイプのDecoderも、rawデータを取り込みます。取り込まれたデータは、エンリッチメントや終了処理を経て、NetWitness Platformの他のコンポーネントで集計されます。 • データ収集と解析のプロセスは、動的かつオープンなフレームワークで構成されています。
Endpoint Hybridまたは Endpoint Log Hybrid	• ホストからエンドポイント データを収集して管理します。 • 調査、分析、アラート、レポートのためのメタデータを生成します。 • Windowsホスト、および、NetWitness Platformがログ収集をサポートするその他すべてのイベント ソースからログを収集します。
Concentrator	• NetWitnessの収集データにインデックスを作成し、クエリの機能を提供します。 • オプションでESAにデータを転送できます。

システム コンポーネント	説明
Broker	• 多くのConcentratorまたはArchiverに分散したNetWitnessの収集データへのアクセスを集約し、NetWitness Platform全体で単一の収集データのようにアクセスできるようにします。
Archiver	• Archiverサービスは、ログ データのインデックス作成と圧縮を行い、それらのデータをアーカイブ ストレージに送信することによって、長期間にわたるログのアーカイブを可能にします。 • アーカイブ ストレージは、データの長期保存およびコンプライアンス レポート作成のために利用できます。 • Archiverは、ストレージとしてDAC(直接接続機能) を使用し、Log Decoderからのrawログとログ メタ データを長期保存のために格納します。 **注 :** rawパケットやパケットのメタ データは、Archiverに格納されません。
ESA(Event Stream Analysis)	• Event Stream Analysisサービスは、相関イベントや複雑なイベント処理などのイベント ストリーム解析を高スループットかつ低レイテンシで提供します。ESAでは、Concentratorからの大量の雑多なイベント データを処理することができます。 • ESAの先進的なイベント処理言語によって、いくつもの異なるイベント ストリームを対象に、フィルタリング、集計、結合、パターン認識、相関を設定することができます。 • ESAによって、強力なインシデント検出やアラート通知を実現することができます。 • RSA自動脅威検出機能には、コマンド & コントロール トラフィックを検出するための事前構成済みのESA Analyticsモジュールが含まれています。

コア コンポーネントとダウンストリーム コンポーネント

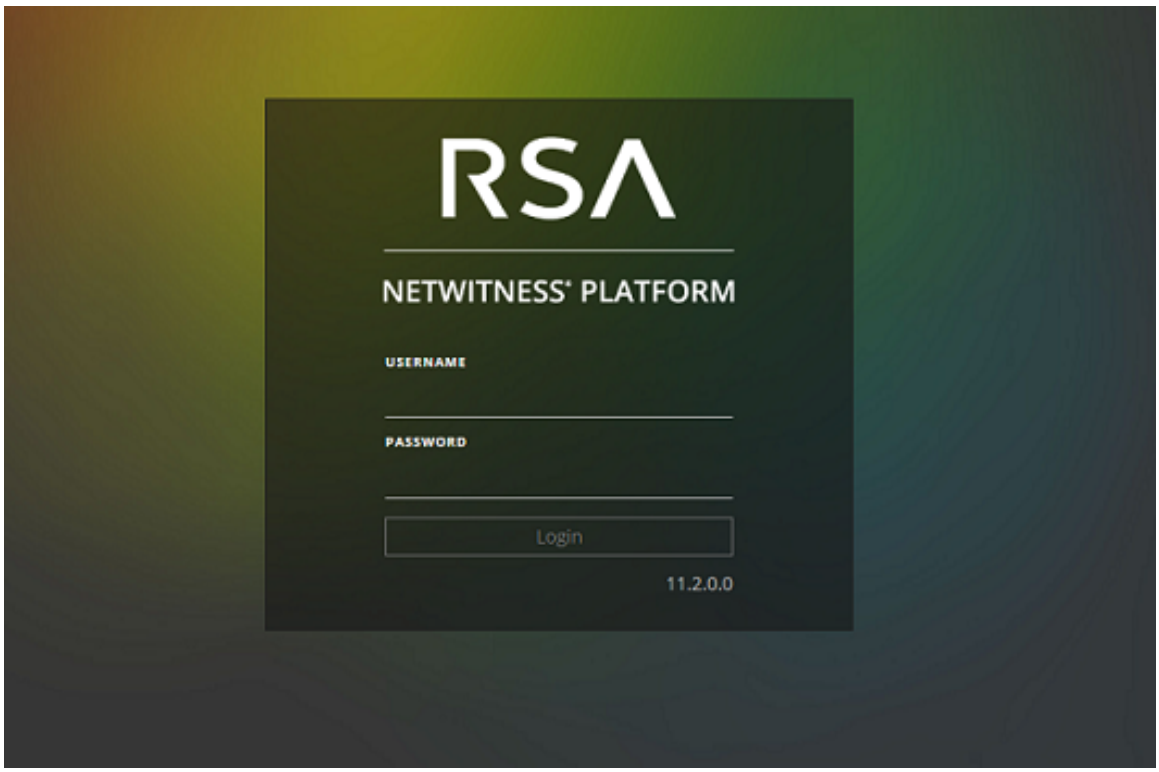
NetWitness Platformのコア サービスは、データの取得と解析、メタデータの生成、生成されたメタデータとrawデータの集計を行います。コア サービスには、Decoder、Log Decoder、Concentrator、Brokerがあります。ダウンストリーム システムは、コア サービスに格納されているデータを使用して分析を行います。したがって、ダウンストリーム サービスの動作はコア サービスに依存します。ダウンストリーム システムは、Archiver、ESA、Malware Analysis、Investigate、Reportingです。

コア サービスは、ダウンストリーム システムなしでも動作し、優れた分析ソリューションを提供できますが、ダウンストリーム コンポーネントによって分析機能を強化できます。ESAは、セッション間およびイベント間だけでなく、ログ、パケット データ、エンドポイント データなどの異なるタイプのイベントに対してリアルタイムに相関を分析することができます。Investigateを使用すると、データにドリルダウンして、イベントおよびファイルを調査し、安全な環境でイベントを再構築できます。Malware Analysisサービスでは、ネットワーク セッションおよび関連ファイルに含まれる悪質なアクティビティをリアルタイムかつ自動的に調査します。

NetWitness Platformへのログイン

RSA NetWitness® Platformへのログイン方法は、環境によって異なります。ユーザ アカウントには、内部ユーザ アカウントと外部ユーザ アカウントがあります。内部ユーザ アカウントはNetWitness Platformのローカル アカウントで、NetWitness Platformにログインしてロール ベースの権限を受け取ることができます。外部ユーザ アカウントはNetWitness Platformの外部で認証を行い、NetWitness Platformのロールにマッピングされます。外部ユーザ アカウントを使用している場合に、NetWitness Platformにアクセスできない、または必要な情報が表示されない場合は、システム管理者にお問い合わせください。管理者が、お使いのアカウントに適切なロールを割り当てることができます。

1. 管理者から提供されたアイコンを使用するか、Webブラウザに次のように入力します。
   `https://<hostname or IP address>/login`
   ここで、`<hostname or IP address>`はNetWitness Serverのホスト名またはIPアドレスです。



ログイン スクリーンが表示されます。

2. ユーザ名とパスワードを入力し、[**ログイン**]をクリックします。
   ログインに成功すると、ユーザ環境設定で指定されたホーム ページが表示されます。

注：NetWitness Platformは最新のブラウザの最近(または現在)のバージョンをサポートしています。

ロックアウトされている場合：

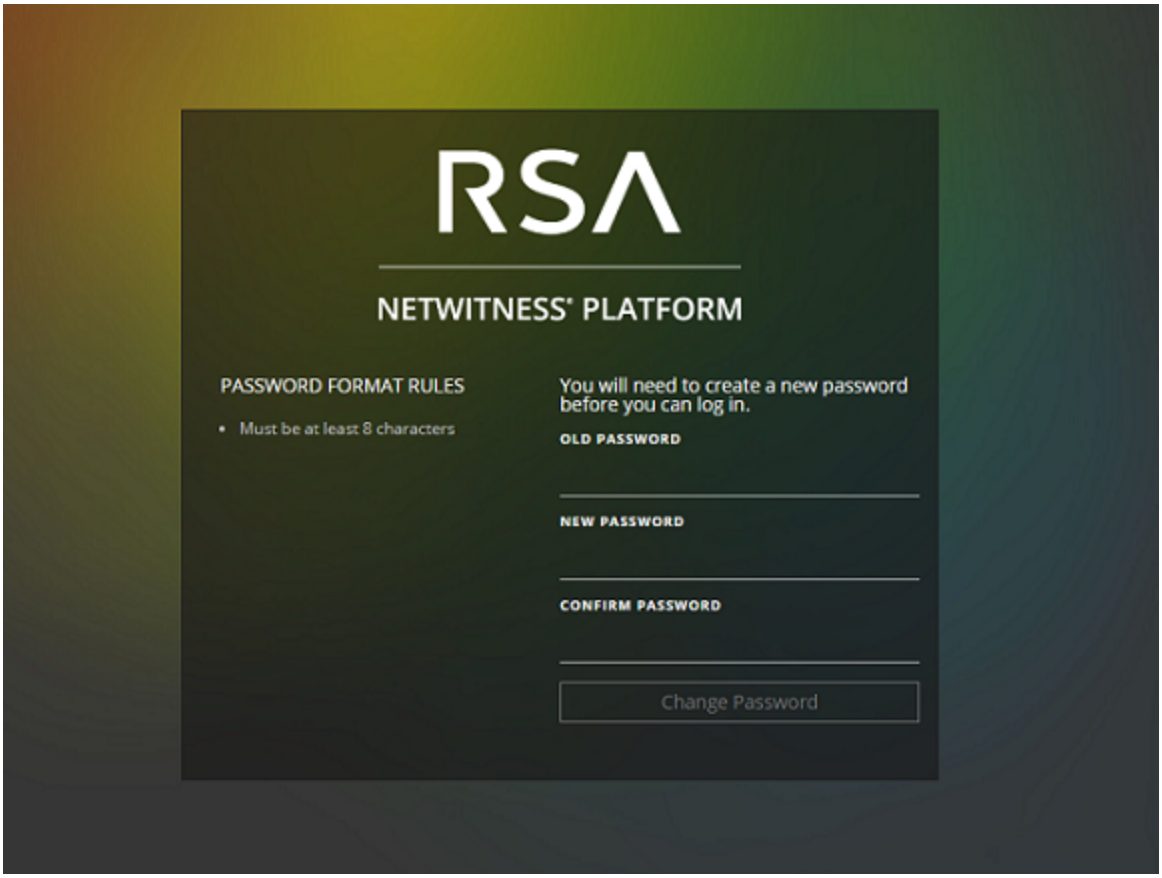
注：この情報は、内部アカウントにのみ適用されます。これは、Active DirectoryまたはPAMアカウントには適用されません。

無効なユーザ名またはパスワードを使用してログインを何度も試みた場合は、アカウントがロックされます。アカウントのロックを解除するには、管理者に問い合わせてください。

新しいアカウントの場合、またはアカウントの有効期限が切れている場合:

注: この手順は、内部アカウントにのみ適用されます。これは、Active DirectoryまたはPAMアカウントには適用されません。

1. 新しいパスワードを作成するためのダイアログで、古いパスワードと新しいパスワードを入力して確認します。(システム管理者が定義した) パスワードの形式のルールが左側に表示されます。新しいパスワードは指定されたルールに準拠する必要があります。



2. [**パスワードの変更**]をクリックします。

NetWitness Platformに適切にアクセスできない場合:

正常にログインできても必要な情報を表示できない場合は、ユーザアカウントに必要なロールが割り当てられていない可能性があります。管理者に問い合わせてください。

NetWitness Platformからのログオフ

[対応]ビューや一部の[調査]ビューからログオフするには:

1. メイン メニューバーで、  を選択します。
2. ユーザ環境設定で、[**サイン アウト**]をクリックします。

その他のビューからログオフするには:

メイン メニューバーで、  >[**サイン アウト**]を選択します。

パスワードの変更手順

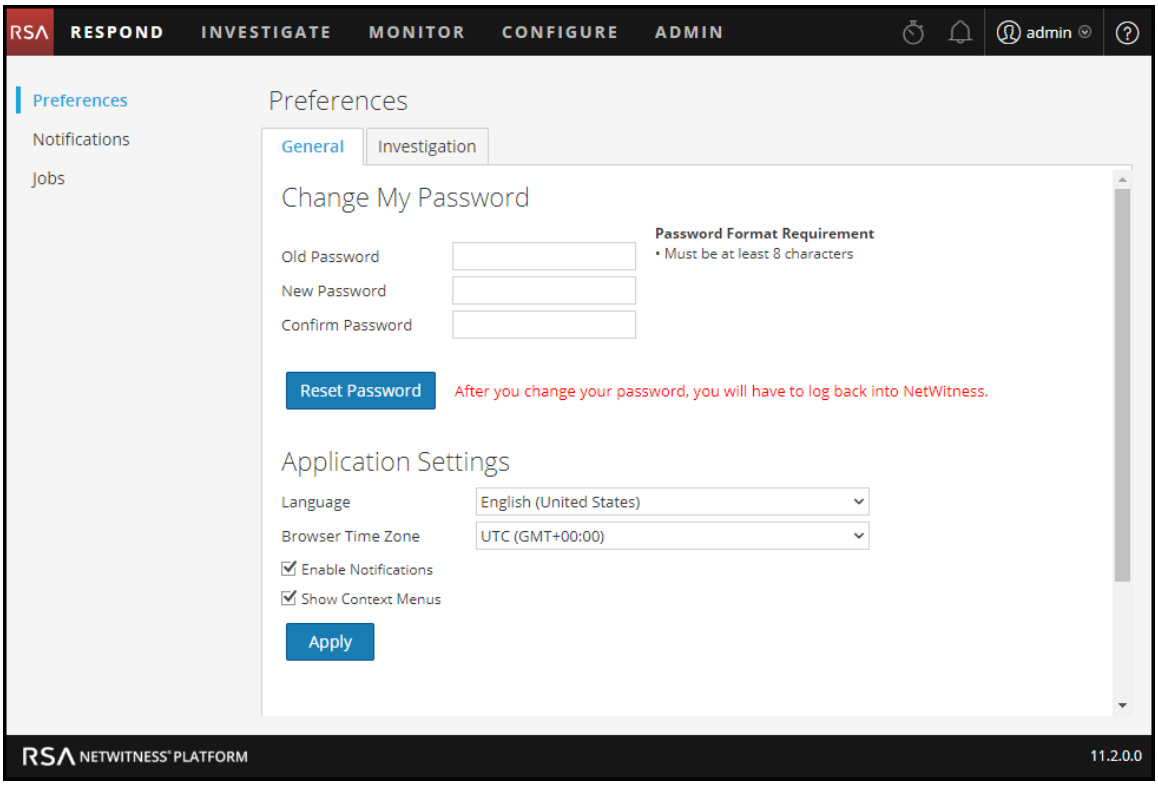
ユーザ環境設定でいつでもRSA NetWitness® Platformの認証に使用するパスワードを変更できます。パスワードの最小長、大文字、小文字、数字、非ラテン アルファベット文字、特殊文字の最小数などの、NetWitness Platformのパスワード強度の要件は管理者が定義します。これらの要件は、パスワードを変更するときに表示されます。

注:この手順は、内部アカウントにのみ適用されます。これは、Active DirectoryまたはPAMアカウントには適用されません。

自分のパスワードを変更するには、次の手順を実行します。

1. 以下のいずれかの操作を実行します。
   - 監視、構成、管理、調査などのほとんどのビューでは、> [**プロファイル**]を選択します。
   - [対応]ビューと一部の[調査]ビュー(イベント分析、ホスト、ファイル、ユーザ)では、を選択し、[ユーザ環境設定]ダイアログで[**パスワードの変更**]をクリックします。

   [環境設定]ダイアログが表示されます。



2. [**パスワードの変更**]セクションで、NetWitness Platformの認証に使用したパスワードを[**古いパスワード**]フィールドに入力します。
3. [**新しいパスワード**]フィールドで、次のログインに使用するパスワードを入力します。
4. [**パスワードの確認**]フィールドに、新しいパスワードを再入力します。

5. [**パスワード のリセット**]をクリックします。
   変 更を有 効にするため、NetWitness Platformからログアウトします。新しいパスワードは、次 回 の NetWitness Platformへのログイン時 に有 効になります。

ロールの特定

ここに記載されているロールは、SOC(セキュリティ オペレーション センター) の典型的なロールまたは機能です。SOCでの自分のロールを判断してください。これらのロールまたは機能を参考にして、自身のジョブ タスクを効率的に実行できるよう、RSA NetWitness® Platformのセットアップ方法とナビゲート方法を決定します。

SOC Team

SOC Manager
(SOC Management and Reporting)

- SOCの対応体制の管理
- インシデントへの対応
- データ侵害への対応

Data Privacy Officer

- プライバシーと機密情報の監視と保護

Incident Reponder
(T1 Analyst)

- インシデントへの対応
- インシデントの改善

Threat Hunter
(T2/T3 Analyst)

- 脅威の探索
- フォレンジック解析の実施
- 問題の改善の推奨
- 問題の改善

Content Expert
(Threat Intelligence)

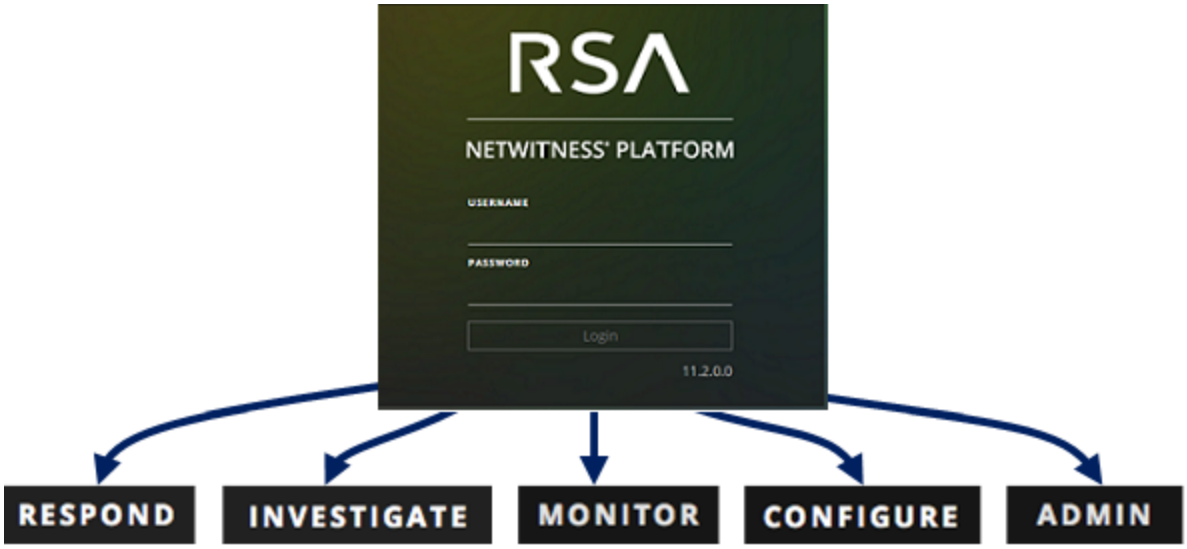
- 新しい脅威インテリジェンスの調査
- 新しいFeedの評価と作成
- 侵害インジケータを警告するための相関ルールの作成

System Administrator

- 機器およびソフトウェアのインストールと構成
- ユーザ アクセスの管理
- パフォーマンスの監視およびチューニング
- データのバックアップとリストア
- ストレージとアーカイブの管理
- ソフトウェアの更新
- コンプライアンス レポートの作成

NetWitness Platform基本ナビゲーション

RSA NetWitness® Platformアプリケーションは、代表的なSOC(セキュリティ オペレーション センター) のロールをもとに構成され、ビューと呼ばれる5つの主な機能領域に分かれています。



- **対応** : このビューはインシデント対応者が使用します。優先度付けされたインシデントのリストが表示され、優先度に応じて対応することができます。これらのインシデントは、ESAルール、NetWitness Endpoint、自動脅威検出を行うESA Analyticsモジュールから生成されます。NetWitness Platformが受け取ったすべてのアラートをここで表示することもできます。
  10.6では、このビューは[インシデント管理]ビューと呼ばれていました。ESA 10.6の[アラート]>[サマリ]ビューが、[対応]>[アラート リスト]ビューに置き換わりました。
- **調査** : このビューは主に、NetWitness Platformのメタデータ、RAWイベント データ、イベント再構成、イベント分析を使用して脅威を手動で見つけることを好む、高度な脅威ハンターが使用します。インシデント対応者も、このビューを使用して調査中のインシデントに関連するイベントの詳細を取得します。脅威ハンターとインシデント対応者の両方が、このビューでフォレンジック イベント再構築とイベント分析の機能を使用できます。
- **監視** : このビューはすべてのユーザが使用します。ユーザ権限に応じて、関心のあるさまざまな領域に関するダッシュボードとレポートを表示できます。NetWitness Platformは、デフォルトではこのビューを開きます。
  このビューは、10.6の[ダッシュボード]ビューに相当します。
- **構成** : このビューは、NetWitness Platformのデータ ソースと入力データを構成する、脅威インテリジェンス担当者(コンテンツのエキスパート) が使用します。コンテンツのエキスパートは、この領域を使用してLiveコンテンツをダウンロードおよび管理します。インシデントとESAルールを作成および管理することもできます。
  このビューは、10.6の[Live]、[インシデント]>[構成]、[アラート]>[構成]に相当します。
- **管理** : このビューは、アプリケーション全体をセットアップして管理する、システム管理者が使用します。

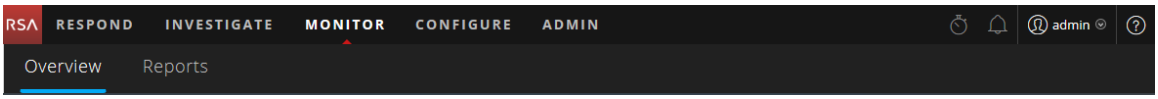
このビューは、[構成]ビューに追加されたセクションを除いた10.6の[Administration]ビューに相当します。

メイン ビューへのアクセス

各メイン ビューを開くオプションがブラウザ ウィンドウの上部に表示されます。権限がある場合は、ブラウザ ウィンドウの上部にあるメニューからこれらのビューにいつでもアクセスできます。

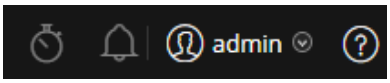
セカンダリ メニュー

一部のビューには、追加のビューを選択するためのセカンダリ メニューがあります。セカンダリ メニューは、ユーザが実行できるタスクによって異なります。次の例は、[監視]メニューを示しています。

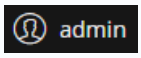


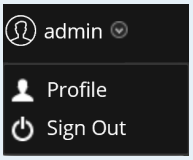
追加オプション

メイン ビューに加えて、アプリケーション全体に共通する追加のオプションがブラウザ ウィンドウの上部に表示されます。



次の表に、これらの共通のオプションの説明を示します。

共通のオプション	名前	説明
	ジョブ	ジョブ トレイのジョブを表示および管理するには、[調査]、[監視]、[構成]、[管理]ビューでこのアイコンをクリックします。ジョブとは、NetWitness Platformアプリケーションで完了するまでに時間がかかる、オン デマンドのタスクまたはスケジュール設定されたタスクです。
	通知	このアイコンをクリックすると、アプリケーションからの通知が表示されます。
	ユーザ環境設定	このアイコンをクリックすると、選択可能なユーザ環境設定オプションが表示されます。ユーザ環境設定の管理と、NetWitness Platformからのログアウトを行うことができます。

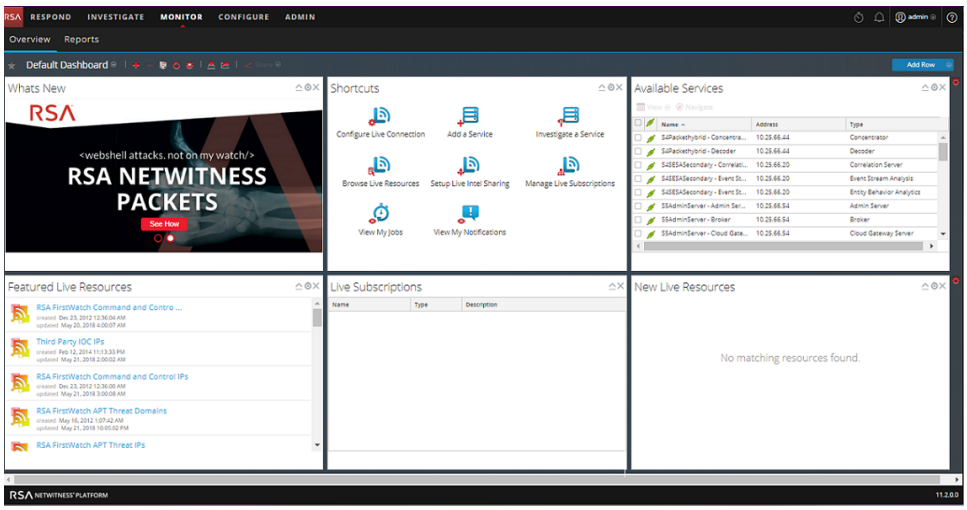
共通のオプション	名前	説明
	ユーザ プロファイル	ユーザ プロファイルをクリックすると、選択可能なオプションが表示されます。ユーザ環境設定の管理、パスワードの変更、NetWitness Platformからのログアウトを行うことができます。
	ヘルプ	このアイコンをクリックすると、NetWitness Platformのヘルプ トピックが表示されます。

メイン ビュー

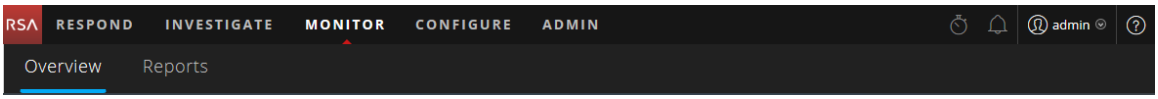
次のセクションでは、メイン ビューについて説明します。

監視

[監視]ビューには、NetWitness Platformダッシュボードが表示されます。[監視]ビューには、事前構成済みのダッシュボードとレポートが用意されています。また、独自に作成することもできます。



監視メニュー



監視メニューには、次のオプションがあります。

- **概要**：[概要]ビューでは、ダッシュボードを表示および管理できます。次の事前構成済みダッシュボードを選択できます。
  - デフォルト
  - Identity
  - Investigation
  - Operations - File Analysis
  - Operations - Logs
  - Operations - Network
  - Operations - Protocol Analysis
  - 概要
  - RSA SecurID
  - Threat - Hunting
  - Threat - Intrusion
  - Threat - Malware Indicators

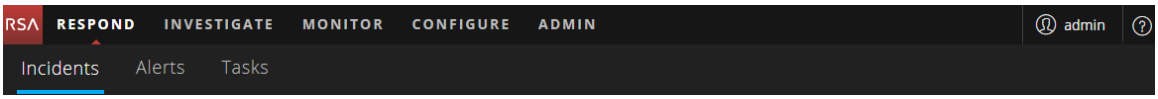
  10.6の、[ダッシュボード]ビューに相当します。
- **レポート**：[レポート]ビューでは、割り当てられた権限に従って、SOCロールに関連するレポートを表示および管理できます。

実行できること	パス	手順
ダッシュボードの選択	[監視]>[概要]	「ダッシュボードの管理」を参照。
ダッシュボードの作成	[監視]>[概要]	「ダッシュボードの管理」を参照。
ダッシュボードの管理	[監視]>[概要]	「ダッシュボードの管理」を参照。
レポートの表示	[監視]>[レポート]>[表示]	「*レポート ガイド*」を参照。
レポートの管理	[監視]>[レポート]>[管理]	「*レポート ガイド*」を参照。

対応

[対応]ビューには、アナリストに優先度順にソートされたインシデントのキューが表示されます。アナリストが、キューのインシデントを担当すると、インシデントの調査に役立つ関連データにアクセスできるようになります。そのデータからインシデントの影響範囲を判断し、必要に応じてエスカレーションまたは改善することができます。

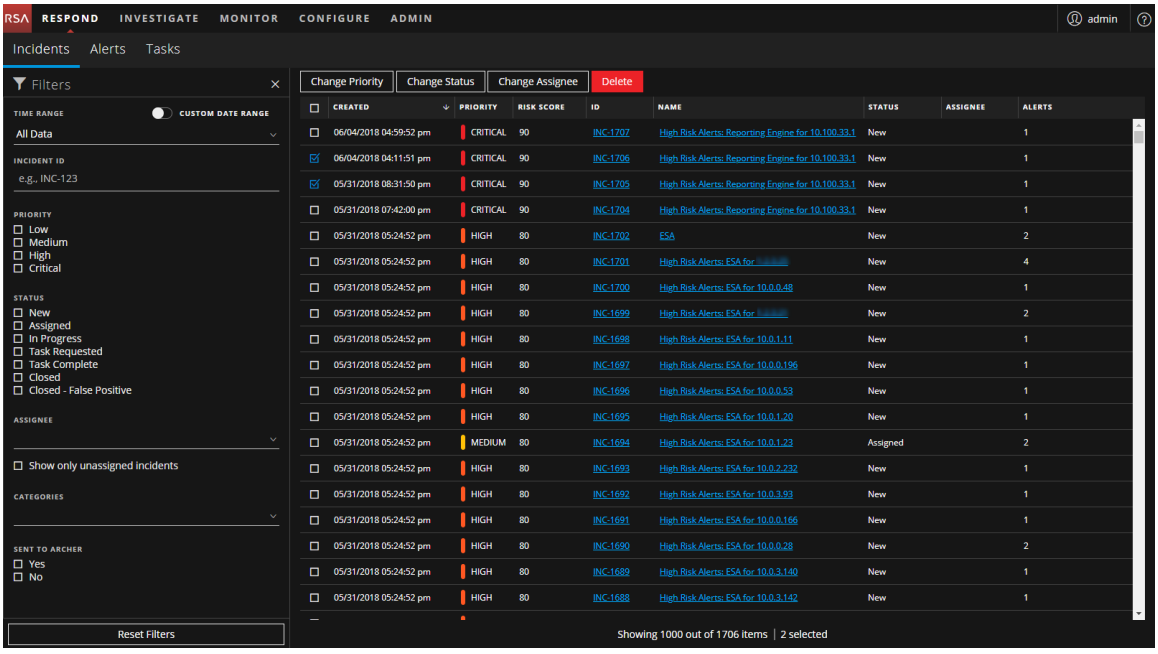
対応メニュー



対応メニューには、次のオプションがあります。

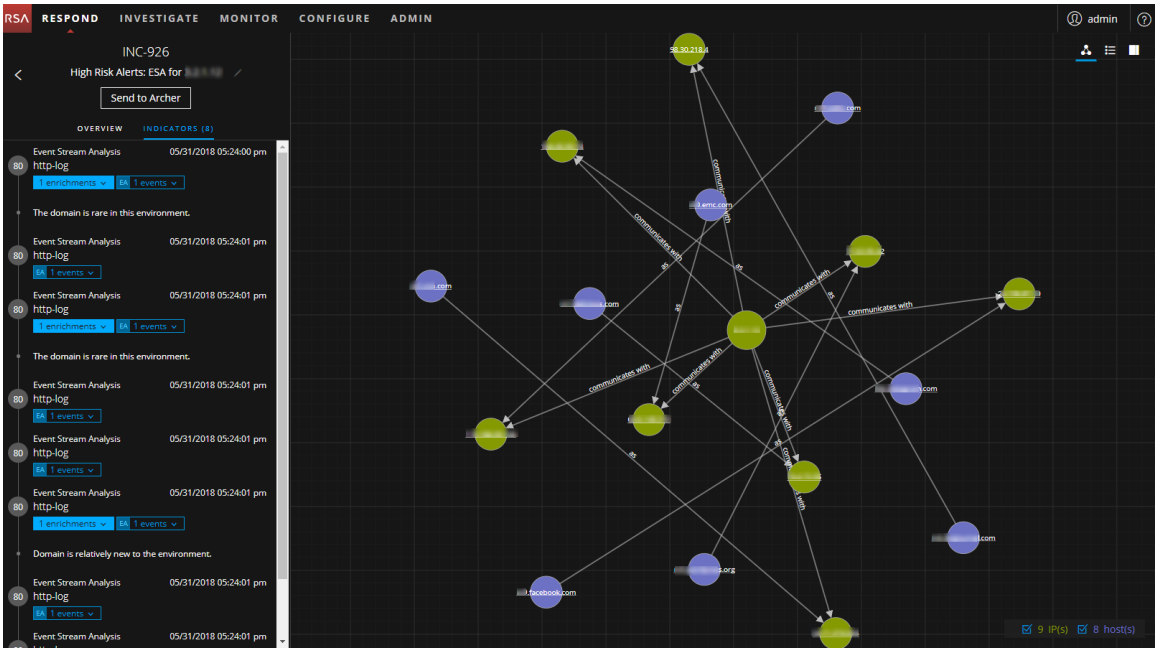
- **インシデント**:[インシデント リスト]ビューには、すべてのインシデントの基本情報のリストが表示されます。[インシデントの詳細]ビューには、インシデントに関する詳細が表示されます。
- **アラート**:[アラート リスト]ビューと[アラートの詳細]ビューには、NetWitness Platformが1つの場所で受信したすべての脅威アラートとインジケータに関する情報が表示されます。
- **タスク**:[タスク リスト]ビューでは、タスクの作成から完了までを追跡することができます。

次の図は、[対応]ビューの[インシデント リスト]ビュー(優先度付けされたインシデントのリストを表示する)を示しています。

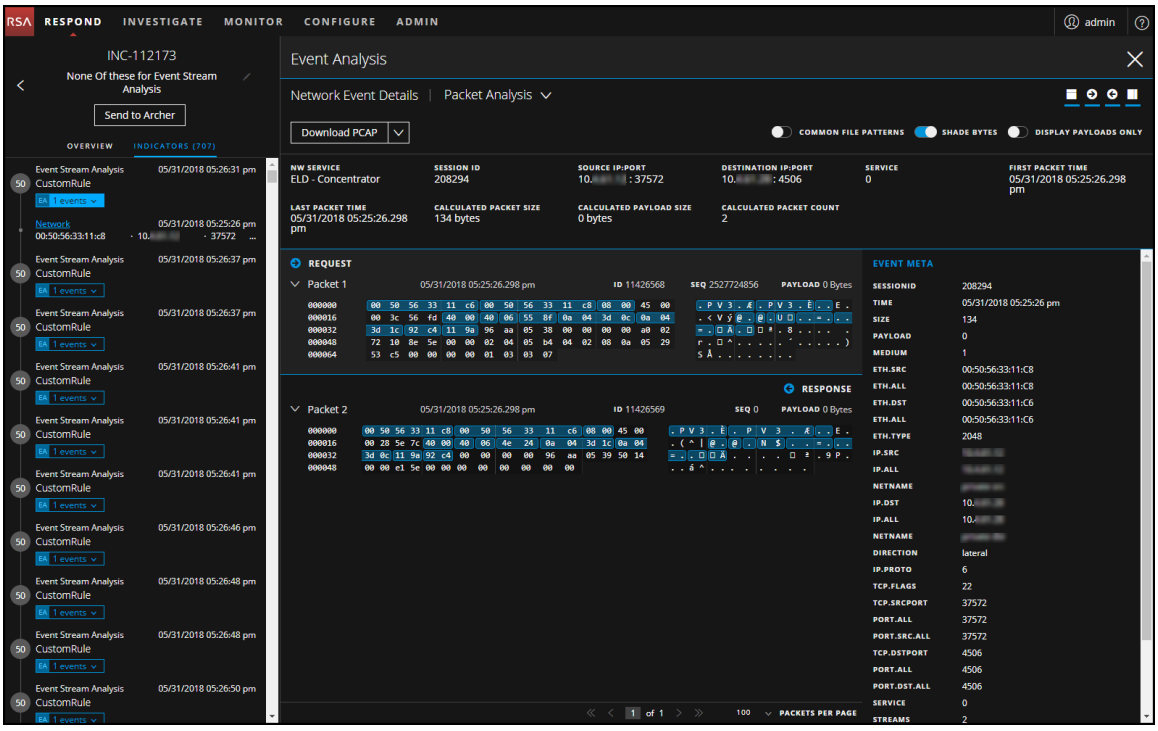


ケース管理ツールとしてNetWitness Platformを使用する場合は、このビューからインシデントをケース管理することもできます。新しいインシデントは、インシデント キューの上部に表示されます。

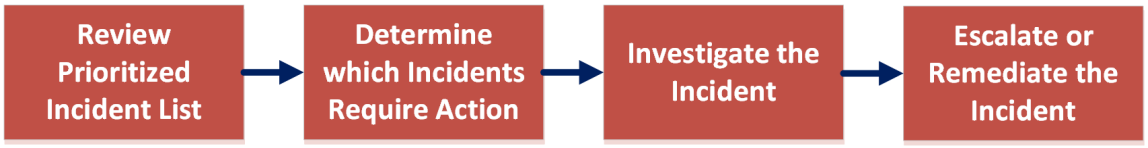
次の図は、[対応]ビューの[インシデントの詳細]ビュー(選択したインシデントの詳細を表示する)の例を示しています。



[対応]ビューは、インシデントの評価、データのコンテキストの把握、他のアナリストとのコラボレーション、必要に応じたより詳細な調査への移行を簡単に行えるように設計されています。次の図は、[アラートの詳細]ビューにあるイベント分析の例です。



次の図は、[対応]ビューのワークフローの概要を示しています。



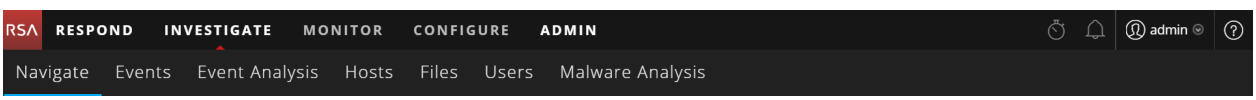
[対応]ビューでは、アナリストが優先度付けされたインシデントのリストを確認し、どのインシデントに対応が必要かを判断します。アナリストは特定のインシデントをクリックして、関連する詳細情報を元にそのインシデントの全体像を明確に把握し、インシデントをさらに調査することができます。その後、アナリストは脅威への対応方法として、エスカレーションするかまたは改善するかを判断できます。

実行できること	パス	手順
優先度付けされたインシデント リストの表示	[対応]>[インシデント]([インシデント リスト]ビュー)	『*NetWitness Respondユーザ ガイド*』を参照。
アクションが必要なインシデントの判断(インシデントの選別)	[対応]>[インシデント]([インシデントの詳細]ビュー)	『*NetWitness Respondユーザ ガイド*』を参照。
インシデントの調査	[対応]>[インシデント]([インシデントの詳細]ビュー)	『*NetWitness Respondユーザ ガイド*』を参照。([調査]ビューに移行することもできます。)
インシデントのエスカレーションまたは改善	[対応]>[インシデント]([インシデントの詳細]ビュー)および[対応]>[タスク]([タスク リスト]ビュー)	『*NetWitness Respondユーザ ガイド*』を参照。
アラートのレビュー	[対応]>[アラート]([アラート リスト]ビューおよび[アラートの詳細]ビュー)	『*NetWitness Respondユーザ ガイド*』を参照。

調査

[調査]ビューでは、1つのデータセットに対して7つの異なるビューが提供され、アナリストはメタデータ、rawデータ、エンドポイント、ログ、イベント、潜在的なセキュリティ侵害インジケータを表示できます。特定のサービスを選択してデータを調査する他に、[対応]ビュー、[監視]ビュー、Reporting Engineによって生成されたレポート内のエントリー、または適切に構成されたサード パーティ製アプリケーションから調査に移行できます。7種類の[調査]ビューのいずれかで調査を開始し、別の[調査]ビューで調査を継続できます。進め方は、調査の対象に応じて異なります。対応が必要なイベントが見つかった場合は、インシデントを作成し、インシデント対応者が[対応]ビューで以降のアクションを実行します。詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

調査メニュー



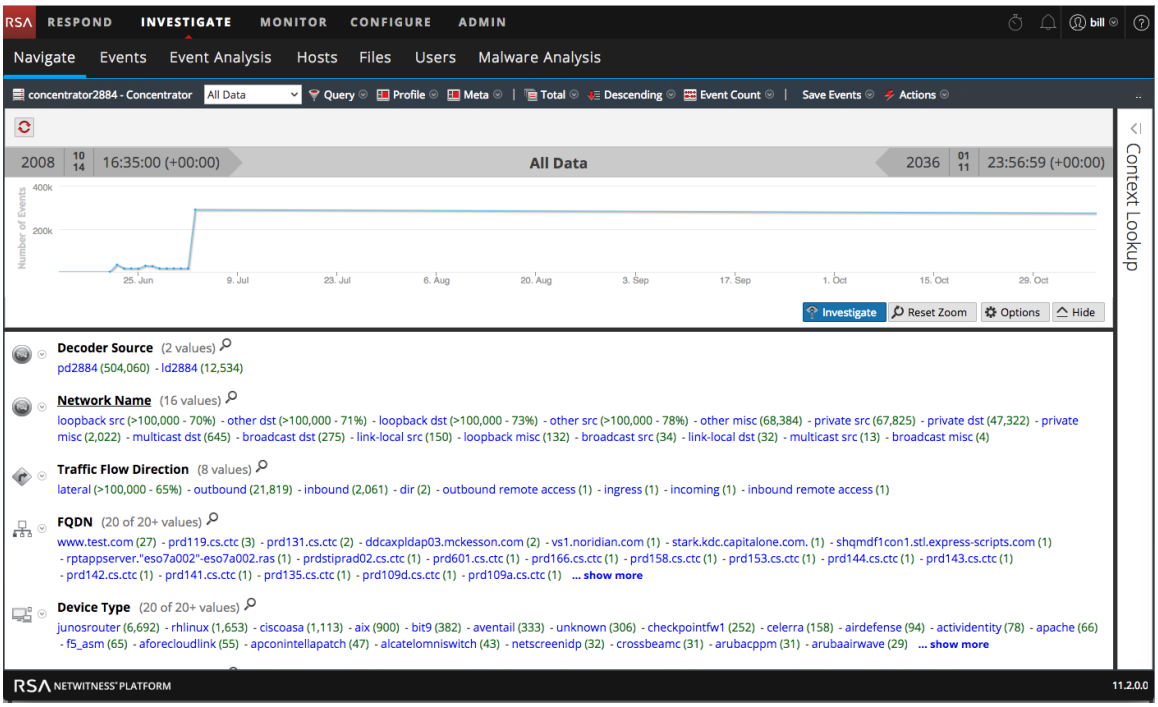
調査メニューには、次のオプションがあります。

- **ナビゲート**：[ナビゲート] ビューでは、メタデータに重点が置かれ、メタ キーとメタ値の一覧が表示されます。データをドリル ダウンし、選択したイベントを[イベント]ビューまたは[イベント分析]ビューで開いたり、イベントの再構築を表示したり、イベントを検索したり、Context Hub サービスから追加のコンテキストを検索したり、[ナビゲート]ビューの環境設定を構成することができます。
- **イベント**：[イベント]ビューには、rawデータに重点を置いたイベントの一覧が表示されます。シンプルなイベント リスト、詳細なリスト、ログ リストをブラウズできます。イベントを検索し、選択したイベントを[イベント分析]ビューで開いたり、イベントの再構築を表示したり、Context Hubサービスから追加のコンテキストを検索したり、[イベント]ビューの環境設定を構成することができます。
- **イベント分析**：[イベント分析]ビューには、メタデータとrawデータに重点を置いたイベントの一覧が表示されます。再構築により注目点の特定に役立つヒントを表示したり、[ホスト]ビューにジャンプしたり、スタンドアロンのエンドポイントに移行したり、Context Hubサービス(バージョン11.2以降) から追加のコンテキストを検索したり、Liveで検索したり、外部ルックアップを実行することができます。
- **[ホスト]ビュー**: (バージョン11.1以降) [ホスト]ビューには、NetWitness Endpoint Insightsのエージェントが実行されているすべてのホストの一覧が表示されます。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、実行中のAutorun、ログイン ユーザに関連した情報を表示できます。[ホスト]ビューから、[ナビゲート]ビューと[イベント分析]ビューに移動することができます。
- **[ファイル]ビュー**: (バージョン11.1以降) NetWitness Endpoint Insights Agentを実行している場合、[ファイル]ビューには、導入環境で見つかったすべての固有のファイルとそれらの関連プロパティが一覧表示されます。ファイルごとに、ファイル サイズ、エントロピー、形式、会社名、署名、チェックサムなどの詳細を表示できます。[ファイル]ビューから、[ナビゲート]ビューと[イベント分析]ビューに移動することができます。
- **[ユーザ]ビュー**: (バージョン11.2以降) [ユーザ]ビューでは、RSA 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。危険度の高いユーザのリストと、環境での危険な行動に関する上位の警告サマリーを表示します。ユーザまたは警告を選択すれば、危険な行動と発生したタイムラインの詳細を表示できます。

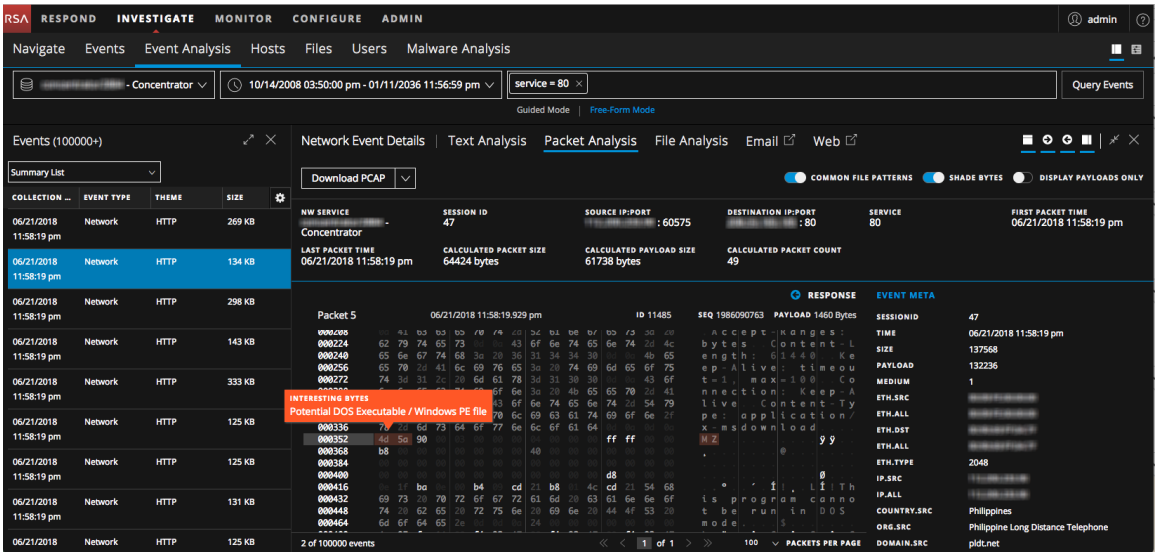
  注：[ユーザ]ビューは、管理者またはUEBAアナリストのロールが割り当てられている場合にのみ使用できます。

- **Malware Analysis**：Malware Analysisは、自動化されたマルウェア解析ツールです。特定の種類のファイル オブジェクト(Windows PE、PDF、MS Officeなど) を解析し、悪意のあるファイルである可能性を評価できるように設計されています。Malware Analysisを使用することによって、収集された大量のファイルに優先度を付け、悪意のあるファイルである可能性が最も高いファイルから解析作業を実行できます。

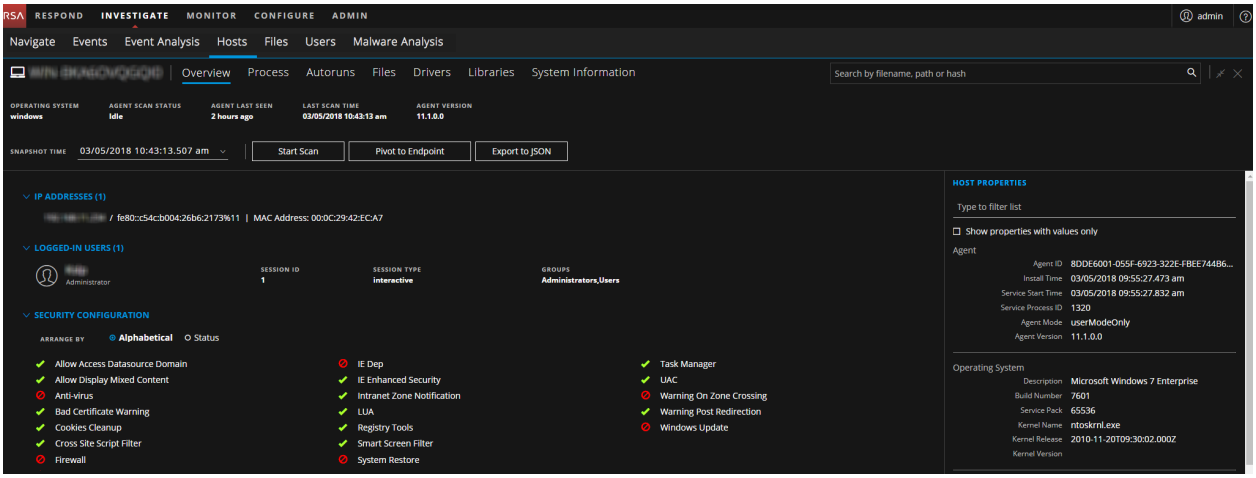
次の図は、[調査]ビューの[ナビゲート]ビューを示しています。



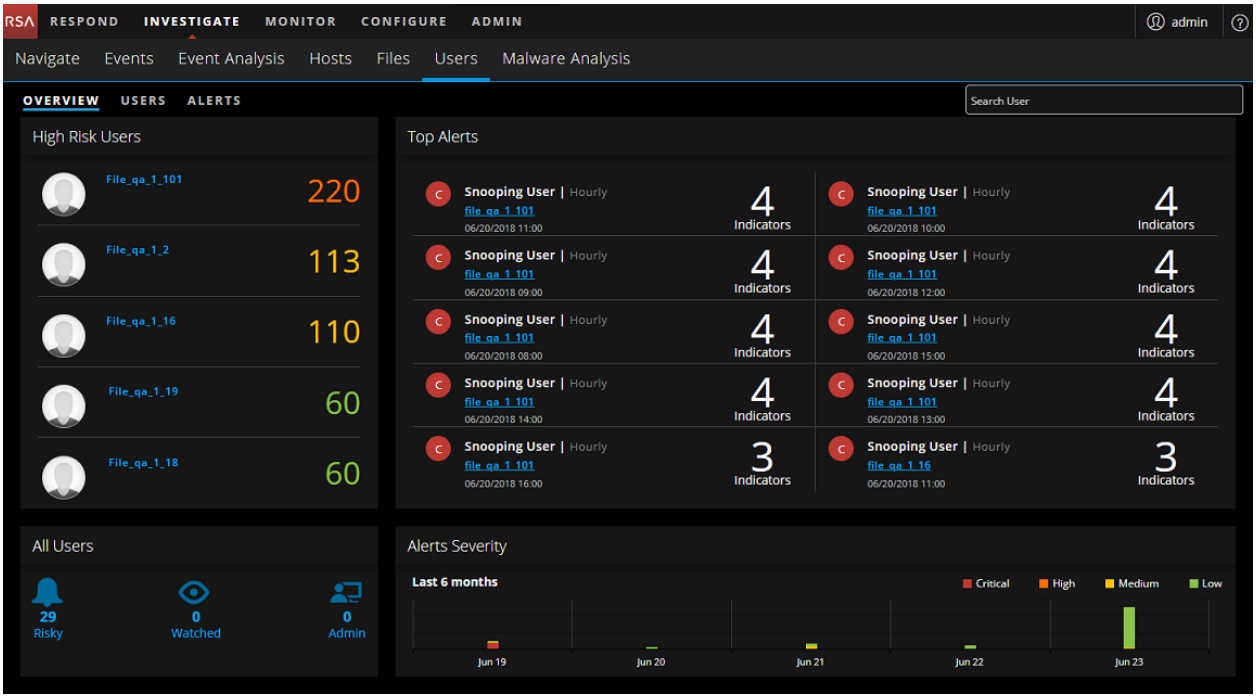
次の図は、[調査]ビューの[イベント分析]ビューを示しています。



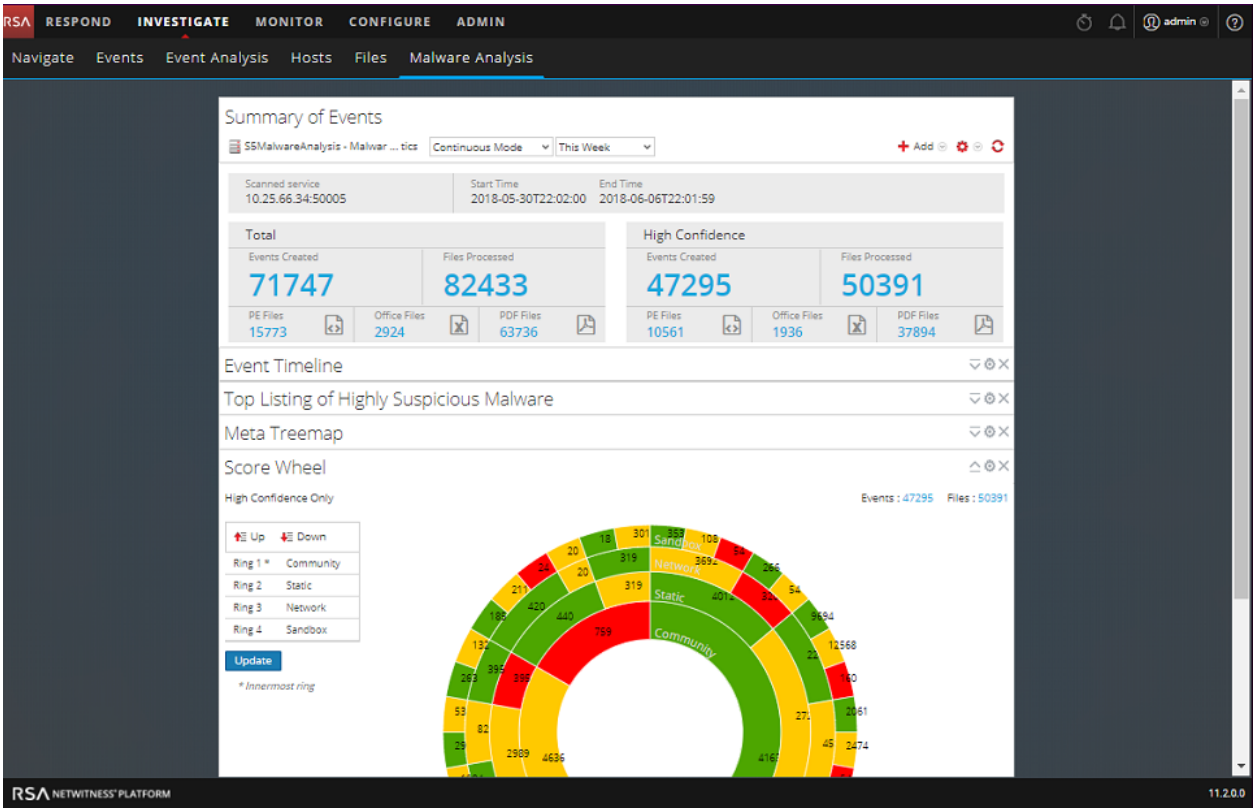
次の図は、[ホスト]ビューの[ホストの詳細]ビューを示しています。



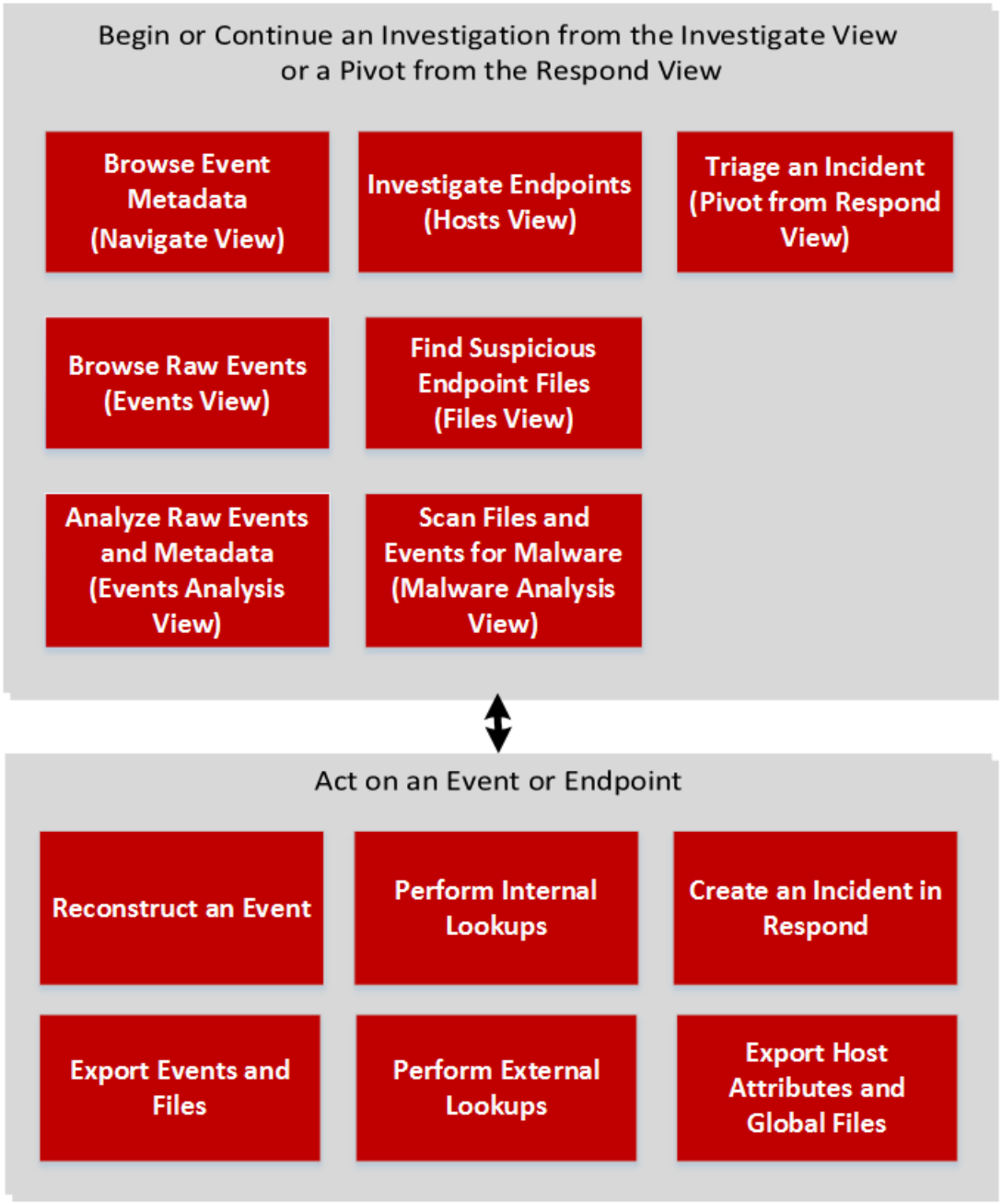
次の図は、[ユーザ]ビューを示しています。



次の図は、Malware Analysisの[イベントのサマリ]を示しています。



次の図は、[調査]ビューの概要レベルのワークフローを示しています。



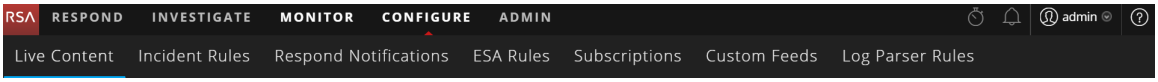
実行できること	パス	手順
イベント メタデータの参照	[ナビゲート]ビュー	「*NetWitness Investigate*ユーザ ガイド」の「[ナビゲート]ビューでのメタデータの調査」を参照。
RAWイベントの参照	[イベント]ビュー	「*NetWitness Investigate*ユーザ ガイド」の「[イベント]ビューでのRAWイベントの調査」を参照。
RAWイベントとメタデータの分析	[イベント分析]ビュー	「*NetWitness Investigate*ユーザ ガイド」の「[イベント分析]ビューでのメタデータとRAWイベントの調査」を参照。

実行できること	パス	手順
エンドポイントの調査	[ホスト]ビュー	「*NetWitness Investigateユーザ ガイド*」の「ホストとファイルの調査」を参照。
不審なエンドポイントファイルを探す	[ファイル]ビュー	「*NetWitness Investigateユーザ ガイド*」の「ホストとファイルの調査」を参照。
ファイルとイベントをスキャンしてマルウェアを探す	[Malware Analysis]ビュー	『*NetWitness Investigateユーザ ガイド*』の「Malware Analysisの実施」を参照。
不審なユーザの動作の検出	[ユーザ]ビュー	『*RSA NetWitness UEBAユーザ ガイド*』を参照。

構成

[構成]ビューでは、脅威インテリジェンス担当者(コンテンツのエキスパート)がNetWitness Platformのデータ ソースと入力データを1つの場所で効率的に構成できます。

構成メニュー



構成メニューには、次のオプションがあります。

- **Liveコンテンツ**: (Live Services) [Liveコンテンツ]ビューでは、Live Servicesリソースの検索とサブスクライブができます。Live Servicesは、NetWitness PlatformサービスとRSA NetWitness Platformのお客様が使用可能なLiveコンテンツ ライブラリの間の通信と同期を管理する、NetWitness Platformのコンポーネントです。RSA Live CMS(Content Management System)のコンテンツを表示、検索、サブスクライブし、NetWitness Platformのサービスとソフトウェアに導入することができます。リソースをサブスクライブすると、RSA Live Servicesから更新を定期的に受信することに同意したことになります。
  10.6では、[Live]>[検索]に相当します。
- **インシデント ルール**: [インシデント ルール]ビューでは、インシデントを自動的に作成するために、さまざまな条件でインシデント ルールを作成することができます。優先度付けされたインシデントを[対応]ビューで表示できます。
  10.6では、[インシデント]>[構成]に相当します。11.1以降では、統合ルールはインシデント ルールと呼ばれます。
- **対応の通知**: [対応の通知]ビューでは、SOCマネージャや、インシデントに割り当てられたアナリストに対して、インシデントが作成または更新されたときに自動的にメール通知を送信することができます。
- **ESAルール**: [ESAルール]ビューでは、ネットワーク内の問題のある動作や脅威と考えられるイベントを特定するためのESA(Event Stream Analysis)を管理することができます。ESAは、ルールの条件に一致する脅威を検出するとアラートを生成します。
  自分でESAルールを作成するか、Live Servicesからダウンロードすることができます。ルール ライブラリ

には、作成またはダウンロードされたすべてのESAルールが表示されます。ルールを有効にするには、ルールを導入環境に追加する必要があります。導入環境により、ルール ライブラリのルールを適切なESAサービスに割り当てます。
10.6では、[アラート]>[構成]に相当します。

- **サブスクリプション**: (Live Services) [サブスクリプション]ビューでは、[Liveコンテンツ]ビューでサブスクライブしたLiveコンテンツを管理できます。NetWitness PlatformでLive Servicesを設定するには、CMSサーバとNetWitness Platformとの間の接続と同期を構成します。
10.6では、[Live]>[構成]に相当します。
- **カスタムFeed**: (Live Services) [カスタムFeed]ビューでは、カスタムFeedの作成と管理のタスクを効率的に実行できます。選択したDecoderとLog DecoderにFeedのデータを入力することもできます。カスタムFeedとIdentity Feedを設定して管理することができます。
NetWitness Platformは外部定義のメタデータ値に基づいてメタデータを作成するために、Feedを使用します。Feedは、収集または処理されるセッションと比較されるデータのリストです。Feedの内容と一致するセッションには、追加のメタデータが作成されます。
たとえば、カスタム ネットワーク アプリケーションに対応するために、カスタムFeedを作成して追加のメタデータ抽出を行うことができます。
10.6では、[Live]>[Feed]に相当します。
- **ログ パーサ ルール**: [ログ パーサ ルール]タブには、個々のログ パーサに関する情報のほか、特定のログ パーサに関連付けられていないログを解析できる「すべて解析」パーサがデフォルトで表示されます。このタブには、次の情報が含まれます。
  - デフォルトのパーサを含む特定のイベント ソース タイプのルールを表示できます。
  - 構成済みの各ログ パーサの名前、リテラル、パターン、メタを表示できます。
  - ログ パーサを追加できます。
  - ログ パーサのカスタム ルールを追加、編集、および削除できます。

注: [ログ パーサ ルール]タブは、バージョン11.2以降の[構成]メニューで使用できます。それ以前のバージョンでは[管理者]>[イベント ソース]にあります。

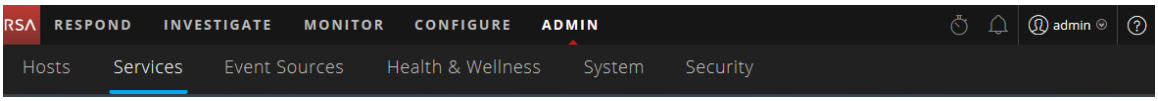
実行できること	パス	手順
Live Servicesアカウントの作成	RSA Live登録ポータル: https://cms.netwitness.com/registration/	「*Liveサービス管理ガイド*」を参照。
Live Servicesリソースの検索と導入。	[構成]>[Liveコンテンツ]	「*Liveサービス管理ガイド*」を参照。
インシデントの自動作成。	[構成]>[インシデント ルール]	「*NetWitness Respond構成ガイド*」を参照。
対応の通知の構成。	[構成]>[対応の通知]	「*NetWitness Respond構成ガイド*」を参照。

実行できること	パス	手順
アラートの構成。	[構成]＞[ESAルール]	「*ESA相関ルールを使用したアラート ユーザ ガイド*」を参照。
NetWitness PlatformでのLive Servicesの設定	[構成]＞[サブスクリプション]	「*Liveサービス管理ガイド*」を参照。
カスタムFeedおよびIdentity Feedの設定および管理。	[構成]＞[カスタムFeed]	「*Liveサービス管理ガイド*」を参照。
ログ パーサとログ パーサ ルールを表示および編集します。	構成＞ログ パーサ ルール	『*ログ パーサのカスタマイズ ガイド*』を参照。

管理

[管理]ビューで、管理者はネットワーク ホストおよびサービスの管理、NetWitness Platformのヘルス モニターの監視、システム レベルのセキュリティの管理を行うことができます。また、グローバル システム リソースを構成し、イベント ソースを管理することもできます。

管理メニュー



管理メニューには、次のオプションがあります。

- **ホスト**: [ホスト]ビューでは、ホストを設定および管理します。ホストは、サービスが実行されるマシンであり、物理マシンであることも、仮想マシンであることもあります。
- **サービス**: [サービス]ビューでは、サービスの管理、サービスのユーザとロールの管理、サービス構成ファイルの管理、サービスのプロパティの確認と編集を行うことができます。サービスは、ネットワーク データをパケット形式で収集するDecoderサービスのように、固有の機能を実行します。
- **イベント ソース**: [イベント ソース]ビューでは、イベント ソースの管理と、イベント ソースのアラート ポリシーの構成を行うことができます。イベント ソースは、通常、重要度によってグループ分けして監視します。イベント ソース グループごとに監視ポリシーを作成し、優先度を設定することができます。
- **ヘルスモニタ**: [ヘルス モニター]ビューでは、ネットワーク環境内のNetWitness Platformホストおよびサービスの状態を監視することができます。
- **システム**: [システム]ビューでは、NetWitness Platformのグローバル構成を設定できます。グローバル監査ログ、メール、システム ログ、ジョブ、RSA Live Services、URL統合、調査、ESA(Event Stream Analysis) 、ESA Analytics、高度なパフォーマンス設定を構成できます。また、NetWitness Platformのバージョン管理、ローカル ライセンス サーバの構成なども実行できます。
- **セキュリティ**: [管理]の[セキュリティ]ビューでは、ユーザ アカウントの管理、ユーザ ロールの管理、NetWitness Platformロールへの外部グループのマッピング、その他のセキュリティ関連のシステム パラメータの変更などを実行できます。これらの設定はNetWitness Platformシステムに適用され、個々のサービスのセキュリティ設定とあわせて使用されます。

注: バージョン11.2以降では、[イベントソース] > [ログ パーサ ルール]タブが[構成]ビューに表示されます。

実行できること	パス	手順
ホストの管理。	[管理] > [ホスト]	「*ホストおよびサービス スタート ガイド*」を参照。
サービスのユーザ アクセスおよびセキュリティの管理を含む、サービスの管理。	[管理] > [サービス]	「*ホストおよびサービス スタート ガイド*」を参照。
イベント ソースの管理およびイベント ソースのアラート ポリシーの構成。	[管理] > [イベント ソース]	「*イベント ソース管理ガイド*」を参照。
NetWitness Platformドメイン内のホストおよびサービスの、アラームの設定および監視。	[管理] > [ヘルス モニタ] > [アラーム]	「*システム メンテナンス ガイド*」を参照。

実行できること	パス	手順
NetWitness Platformホストおよびホストで実行されているサービスの統計の監視。	[管理]＞[ヘルスモニタ]＞[監視]	「*システム メンテナンス ガイド*」を参照。
ポリシーを作成してホストとサービスに適用し、NetWitness Platformドメインのヘルス モニターの監視を支援します。	[管理]＞[ヘルスモニタ]＞[ポリシー]	「*システム メンテナンス ガイド*」を参照。
NetWitness Platformのグローバル構成の設定。	[管理]＞[システム]	「*システム構成ガイド*」を参照。
グローバル監査ログの構成。	[管理]＞[システム]＞[グローバル監査]	「*システム構成ガイド*」を参照。
システム セキュリティの設定。	[管理]＞[セキュリティ]	「*システム セキュリティとユーザ管理ガイド*」を参照。
ロールと権限によるシステム ユーザの管理。	[管理]＞[セキュリティ]	「*システム セキュリティとユーザ管理ガイド*」を参照。

SOCロールに応じたデフォルト ビューの設定

SOC(Security Operations) のロールに応じたデフォルトのビューを設定しておくと、RSA NetWitness® Platformにログインした後、アプリケーションの移動を簡単にすることができます。デフォルト ビュー(ホームページとも呼ばれる) は、ユーザ環境設定で設定します。

次の図は、主なNetWitness Platformビューを示しています。

- **対応**: このビューは、インシデント対応者が使用します。インシデントとアラートのリストを表示し、対応するインシデントを選別することができます。このビューは、従来の10.6の[インシデント管理]ビューに相当します。また、[対応]>[アラート]ビューは10.6 ESAの[アラート]>[サマリー]ビューを置換します。
  [対応]ビューは、デフォルトの開始ビューです。[対応]ビューを表示する権限がない場合のデフォルト ビューは[監視]ビューになります。
- **調査**: このビューは、高度な脅威の調査と探索を行う脅威ハンターが使用します。
- **監視**: このビューはすべてのユーザが使用します。以前のバージョンのクラッシックなビューです。ユーザ権限に応じて、関心のあるさまざまな領域に関するダッシュボードとレポートを表示できます。事前構成済みダッシュボードを選択したり、ダッシュボードをインポートしたり、独自のカスタム ダッシュボードを作成することができます。
- **構成**: このビューは、NetWitness Platformのデータ ソースと入力データを構成する、脅威インテリジェンス担当者(コンテンツのエキスパート) が使用します。コンテンツのエキスパートは、この領域を使用してLiveコンテンツをダウンロードおよび管理します。インシデントとESAルールを作成および管理することもできます。
  10.6では、[Live]、[インシデント]>[構成]、[アラート]>[構成]に相当します。
- **管理**: このビューは、アプリケーション全体のセットアップと管理を行うシステム管理者が使用します。

NetWitness Platformのメイン ビューのいずれかをデフォルト ビューとして選択できます。メイン ビューに加え、NetWitness Platformには定義済みのダッシュボードがあり、実行するタスクに応じて[監視]ビューで選択できます。

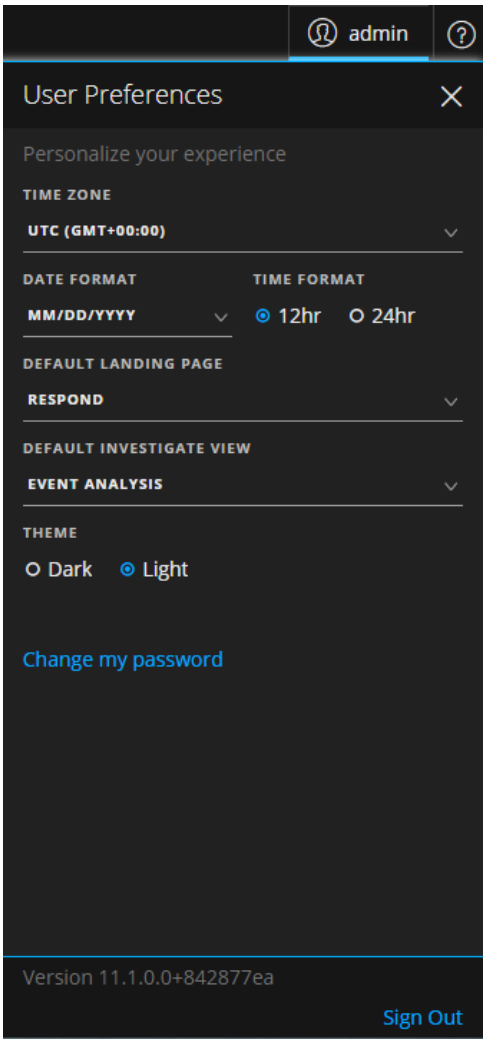
- デフォルト ダッシュボード
- Identity Dashboard
- Operations - Logs Dashboard
- Operations - Network Dashboard
- Overview Dashboard
- Threat - Indicators Dashboard
- Threat - Intrusion Dashboard

次の表では、一般的なSOCのロールと、SOCのロールに応じてユーザ環境設定でホーム ページとして選択できるビューを示します。複数のロールが割り当てられている場合は、NetWitness Platformにログインした時に表示するのに最も適切だと思うビューを選択します。

SOCのロール	ロールの説明	デフォルトのホームページの候補
インシデント対応者 (Tier1アナリスト)	キューに登録されたインシデントとアラートに対応し、調査と改善を行います。	**対応**
脅威ハンター (Tier 2/Tier 3アナリスト)	高度な脅威の調査および探索	**調査** デフォルトの調査ビューを選択する方法については、『*NetWitness調査ユーザガイド*』を参照してください。
SOCマネージャ (SOCの管理およびレポート)	SOCの対応体制を管理し、インシデントやデータ侵害に対応します。	**監視**(ダッシュボードは監視ビューに表示されます。ログインしたときに、自身のSOCロールに適切な事前定義のダッシュボードを選択します。また、ダッシュボードをインポートしたり、独自のダッシュボードを作成したりできます。)
コンテンツのエキスパート (脅威インテリジェンス)	NetWitness Platformのデータソースと入力データを構成します。	**監視**または**構成**(ダッシュボードは監視ビューに表示されます。ログインしたときに、自身のSOCロールに適切な事前定義のダッシュボードを選択します。また、ダッシュボードをインポートしたり、独自のダッシュボードを作成したりできます。監視をデフォルト ビューとして選択した場合は、メイン メニューから構成ビューに移動できます。)
データ プライバシー責任者 (DPO)	管理者と同様に、DPOはプライバシーに関する機微情報を監視して保護します。	**監視**(ダッシュボードは監視ビューに表示されます。ログインしたときに、自身のSOCロールに適切な事前定義のダッシュボードを選択します。)
システム管理者	アプリケーション全体の構成と安定性を重視します。ユーザアクセスを管理します。	**管理**

デフォルト ビューの設定

1. (［対応］ビューと一部の［調査］ビュー) メイン メニュー バーで  を選択します。
   ［ユーザ環境設定］ダイアログに、現在の環境設定が表示されます。



2. [**デフォルトのランディング ページ**]フィールドで、NetWitness Platformにログインするときに表示するデフォルト ビューを選択します。前述の表を使用して、SOCのロールに基づく選択を行います。たとえば、インシデント対応者の場合は[**対応**]を選択し、脅威ハンターの場合は、[**調査**]を選択します。

   環境設定はすぐに反映されます。デフォルトのホーム ページはいつでも変更できます。その他の環境設定については、「ユーザ環境設定」を参照してください。

3. 正しいデフォルト ビューを表示できることを確認するには、[**サイン アウト**]をクリックしてログアウトし、それから再度NetWitness Platformにログインします。

ユーザの構成に関する基本的なトラブルシューティングのヒント

次の表では、NetWitness Platformのユーザの構成に役立つ可能性がある基本的なトラブルシューティングのヒントを提供します。

問題	トラブルシューティングのヒント
NetWitness Platformへのログイン時に、正しくないデフォルト ビューが表示されます。	正しいデフォルト ビューがユーザ環境設定の[デフォルト ホーム ページ]フィールドで設定されていることを確認します。監視ビューを選択した場合、SOCのロールに最も適切な事前定義されたダッシュボードを選択することができます。また、ダッシュボードをインポートしたり、独自のダッシュボードを作成したりできます。
正しいビューが表示されるが、メタデータがロードされません。	ブラウザの最新バージョンを使用していることを確認します。それでも問題が解決しない場合は、別のブラウザで試してみてください。たとえば、Safariを使用している場合は、FirefoxまたはChromeを使用してください。
Internet Explorer 10の使用時に、次のエラーが発生します。 `The page can't be displayed.`	NetWitness Platformは最新のブラウザの最近(または現在)のバージョンをサポートしています。より新しいブラウザ バージョンをインストールしてください。ブラウザーをアップグレードできない場合は、ブラウザでTLS 1.2プロトコルを有効化してみてください。 **[インターネット オプション]**>**[詳細設定]**>**[セキュリティ]**に移動します。TLS 1.2プロトコルの使用が有効化されていることを確認します。[**適用**]をクリックします。ページを再ロードします。
ログイン時に、何も表示されません。	管理者に問い合わせてください。アカウントに割り当てられているユーザ ロールや、他のトラブルシューティングが必要になる場合があります。
デフォルト ホーム ページを変更する場所が分かりません。	[対応]ビューの[ユーザ環境設定]に移動するか、管理者に問い合わせてください。

ユーザ環境設定

RSA NetWitness® Platformアプリケーションのグローバルな環境設定は、各ユーザのユーザ プロファイルから表示および管理することができます。異なるオプションを持つ、2つのグローバル ユーザ環境設定ダイアログがあります。[ユーザ環境設定]ダイアログは、[対応]ビューと次の[調査]ビュー([イベント分析]、[ホスト]、[ファイル]、[ユーザ]) から アクセスできます。[環境設定]ダイアログには、その他ほとんどのビューからアクセスできます。表示されるダイアログは、ユーザ環境設定にアクセスする地点によって異なります。

このページでは、次の操作を実行できます。

- アプリケーションの表示言語の変更
- アプリケーションのタイム ゾーンの設定
- アプリケーションの日付と時刻の形式の設定 *
- NetWitness Platformのデフォルトの開始ビューの選択*
- デフォルトの[調査]ビューの選択*
- アプリケーションの明暗のテーマの選択*
- パスワードの変更(詳細については「パスワードの変更手順」を参照)
- 通知の有効化または無効化**
- コンテキスト メニューの有効化また無効化**

* [対応]ビューや一部の[調査]ビュー([イベント分析]、[ホスト]、[ファイル]、[ユーザ]) から[**ユーザ環境設定**]ダイアログに アクセスできます。

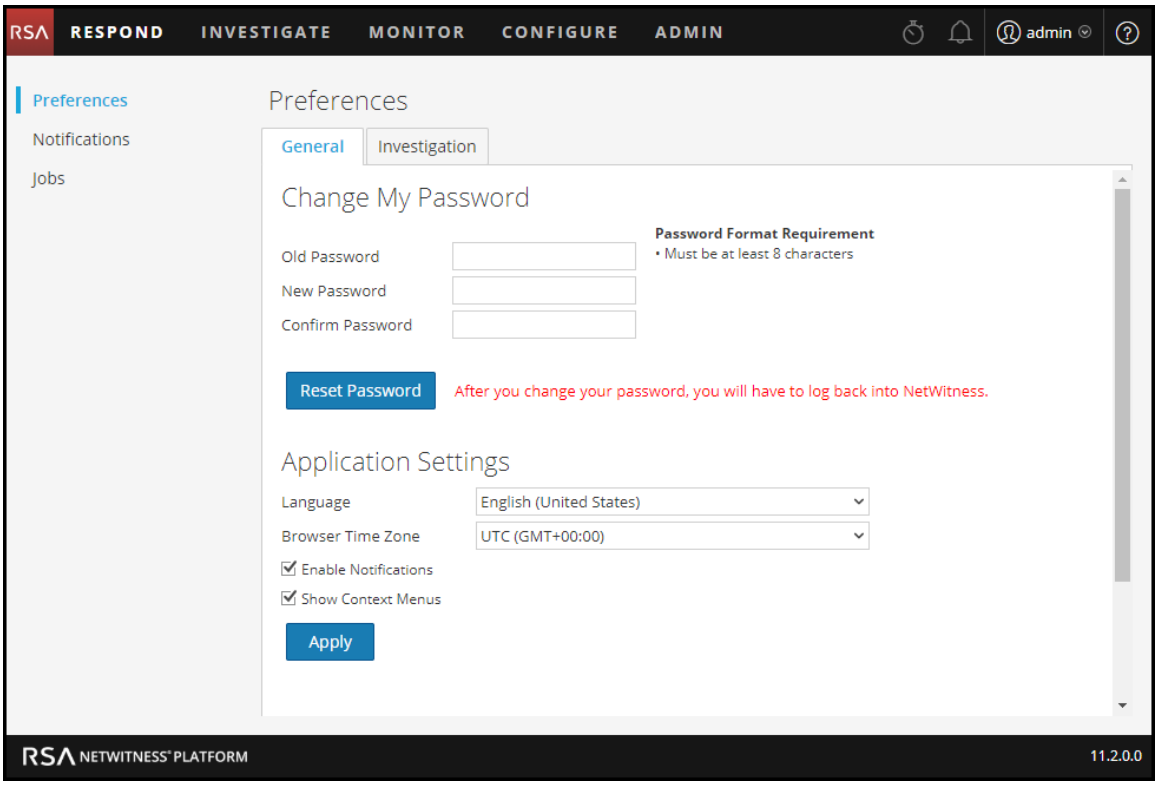
** [対応]ビューや一部の[調査]ビュー([イベント分析]、[ホスト]、[ファイル]、[ユーザ]) 以外のビューから[**環境設定**]ダイアログにアクセスして、この変更を加えることができます。

ユーザ環境設定([対応]ビューおよび一部の[調査]ビュー以外のビュー)

このセクションでは、[環境設定]ダイアログで実行できるさまざまなタスクについて説明します。[環境設定]ダイアログは、[対応]および[調査]ビューを除くほとんどのビューからアクセスできます。

環境設定の表示

NetWitness Platformブラウザ ウィンドウの右上隅で、 > [プロファイル]を選択します。
[環境設定]ダイアログに、現在の環境設定が表示されます。



言語とタイムゾーンの設定

注：言語設定オプションは11.2以降NetWitness Platformに適用されます。

NetWitness Platform全体の使用言語を変更できます。デフォルトの言語は、英語(米国)に設定されています。

1. [ユーザ環境設定]ダイアログで、ローカリゼーションの環境設定を選択します。
   a. **言語**：NetWitness Platformで使用する言語を選択します。
   b. **タイムゾーン**：NetWitness Platformで使用するタイムゾーンを設定します。
2. [**適用**]をクリックします。
   環境設定はすぐに反映されます。

注：現在ログインしているユーザのタイムゾーンでDSTが使用される場合、DST(夏時間)が開始または終了すると、ユーザインタフェースは、正確な時刻を反映するように自動的に更新されます。

ユーザアカウントのシステム通知の有効化または無効化

デフォルトでは、新しいユーザアカウントが作成されると、NetWitness Platformシステム通知が有効化されます。これらの通知はいつでも無効化または有効化することができます。

1. [環境設定]ダイアログで次の操作を行います。
   - ユーザ アカウントの通知を有効化するには、[**通知の有効化**]チェックボックスをオンにします。
   - 通知を無効化するには、[**通知の有効化**]チェックボックスをオフにします。
2. [**適用**]をクリックします。
   環境設定はすぐに反映されます。

ユーザ アカウントのコンテキスト メニューの有効化または無効化

デフォルトでは、新しいユーザ アカウントが作成されると、コンテキスト メニューが有効化されます。コンテキスト メニューは、ユーザがビューの特定の個所を右クリックすると表示される追加の機能メニューです。

1. [環境設定]ダイアログで次の操作を行います。
   - ユーザ アカウントのコンテキスト メニューを有効化するには、[**コンテキスト メニューの有効化**]チェックボックスを選択します。
   - コンテキスト メニューを無効化するには、[**コンテキスト メニューの有効化**]チェックボックスをオフにします。
2. [**適用**]をクリックします。
   環境設定はすぐに反映されます。

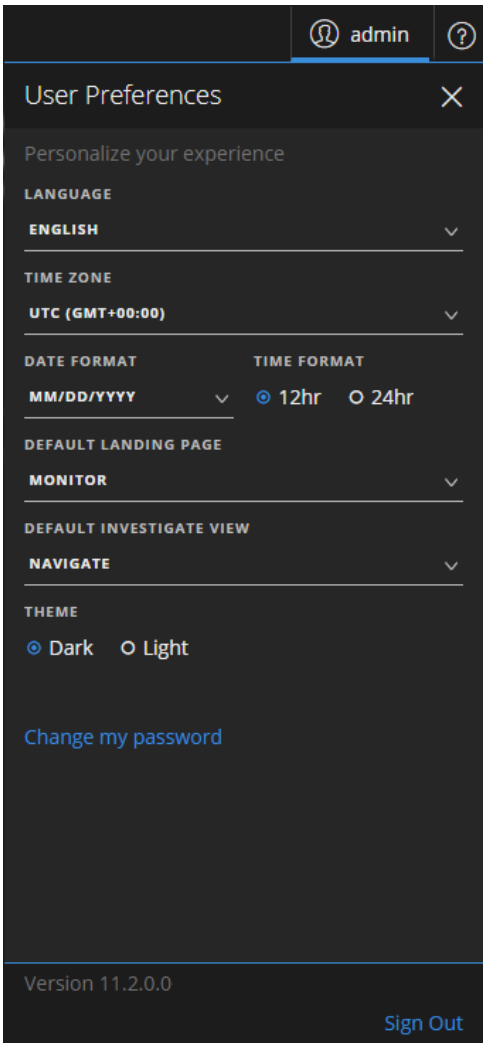
注:[環境設定]ダイアログの[調査]タブで使用可能な設定については、「*NetWitness Investigate ユーザ ガイド*」を参照してください。

ユーザ環境設定([対応]ビューおよび一部の[調査]ビュー)

このセクションでは、[ユーザ環境設定]ダイアログで実行できるさまざまなタスクについて説明します。[ユーザ環境設定]ダイアログは、[対応]および一部の[調査]ビューからアクセスできます。

ユーザ環境設定の表示

NetWitness Platformブラウザ ウィンドウの右上隅で、  を選択します。
[対応]ビューと、次の[調査]ビュー([イベント分析]、[ホスト]、[ファイル]、「ユーザ」) からアクセスすると、[ユーザ環境設定]ダイアログに現在の環境設定が表示されます。



選択はすぐに有効になります。

タイムゾーンと日付と時刻の形式を設定

注：言語設定オプションは11.2以降NetWitness Platformに適用されます。

NetWitness Platform全体の使用言語を変更できます。デフォルトの言語は、英語(米国)に設定されています。地域のタイムゾーンと日付と時刻の形式は変更できます。

1. [ユーザ環境設定]ダイアログで、ローカリゼーションの環境設定を選択します。
   a. **言語**：NetWitness Platformで使用する言語を選択します。
   b. **タイムゾーン**：NetWitness Platformで使用するタイムゾーンを設定します。
   c. **日付形式**：月(MM)、日(DD)、年(YYYY)の表示順序の形式を設定します。たとえば、MM/DD/YYYYの形式では日付は05/11/2017と表示されます。
   d. **時刻形式**：12時間制または24時間制のどちらかを設定します。たとえば、12時間制の2:00 PMは、24時間制で14:00です。

［対応］ビューの変更はすぐに反映されます。

注：現在ログインしているユーザのタイム ゾーンでDSTが使用される場合、DST(夏時間) が開始または終了すると、ユーザ インタフェースは、正確な時刻を反映するように自動的に更新されます。

NetWitness Platformのデフォルトの開始ビューの選択

1. ［ユーザ環境設定］ダイアログを表示します。
2. ［**デフォルト ランディング ページ**］フィールドで、NetWitness Platformにログインしたときに表示する開始ビューを選択します。ユーザのロールに応じて、対応、調査、監視、構成、管理から選択できます。たとえば、「対応」を選択すると、インシデント対応者向けのセクションに直接移動できます。適切なデフォルト ビューの選択については、「SOCロールに応じたデフォルト ビューの設定」を参照してください。
   この選択は、アプリケーション全体のデフォルト ビューを設定します。変更はすぐに反映されます。

デフォルトの［調査］ビューの選択

1. ［ユーザ環境設定］ダイアログを表示します。
2. ［**デフォルトの［調査］ビュー**］フィールドで、NetWitness Platformにログインして［調査］に移動したときのホーム ページを選択します。デフォルトの［調査］ビューとして、［ナビゲート］、［イベント］、［イベント分析］、［ホスト］、［ファイル］、［ユーザ］、［Malware Analysis］を選択できます。たとえば、デフォルトの［調査］ビューとして［イベント］を選択すると、［イベント］ページに直接移動して、サービスに対して生成されたイベントが表示されるようにできます。適切なデフォルト ビューの選択については、「SOCロールに応じたデフォルト ビューの設定」を参照してください。詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

注：ドロップダウンで変更した後、変更が反映されるまでに数秒かかる場合があります。

NetWitness Platformの外観の選択

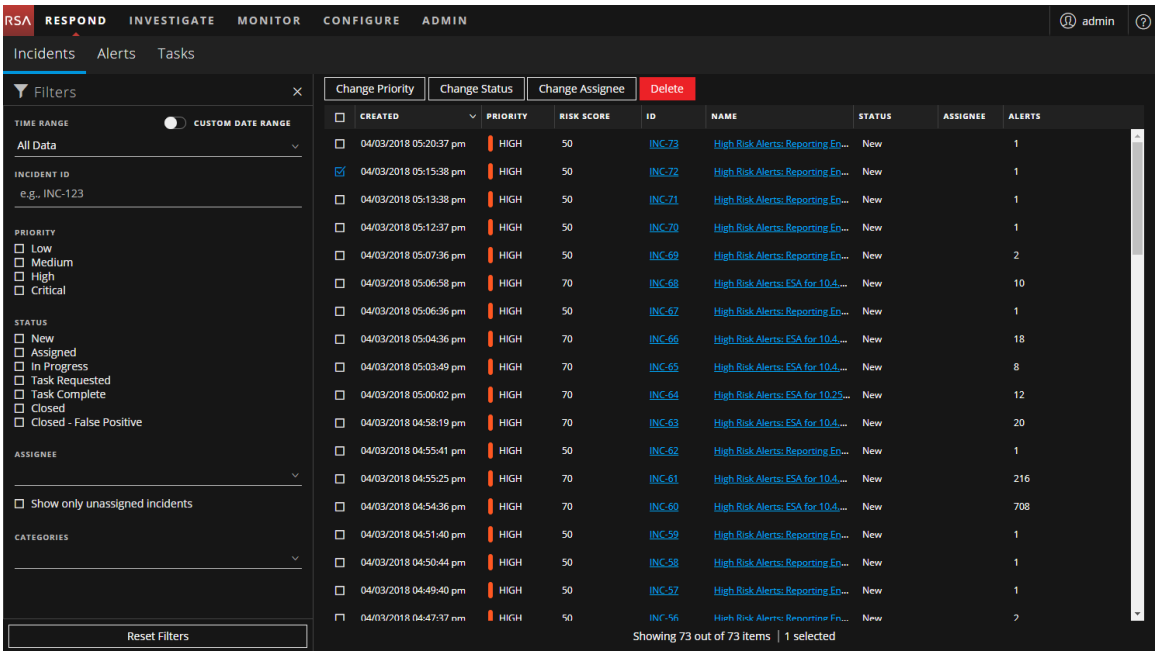
注：このオプションは、NetWitness Platformバージョン11.1以降のみで使用可能です。

自分の好みに応じて、アプリケーションのテーマ色の明暗を選択できます。テーマを変更すると、[対応] ビューと一部の[調査]ビューが、明るい色または暗い色のテーマに変更されます。この選択で変更されるのは、自分の環境でのNetWitness Platformの外観です。他のユーザの環境では変更されません。

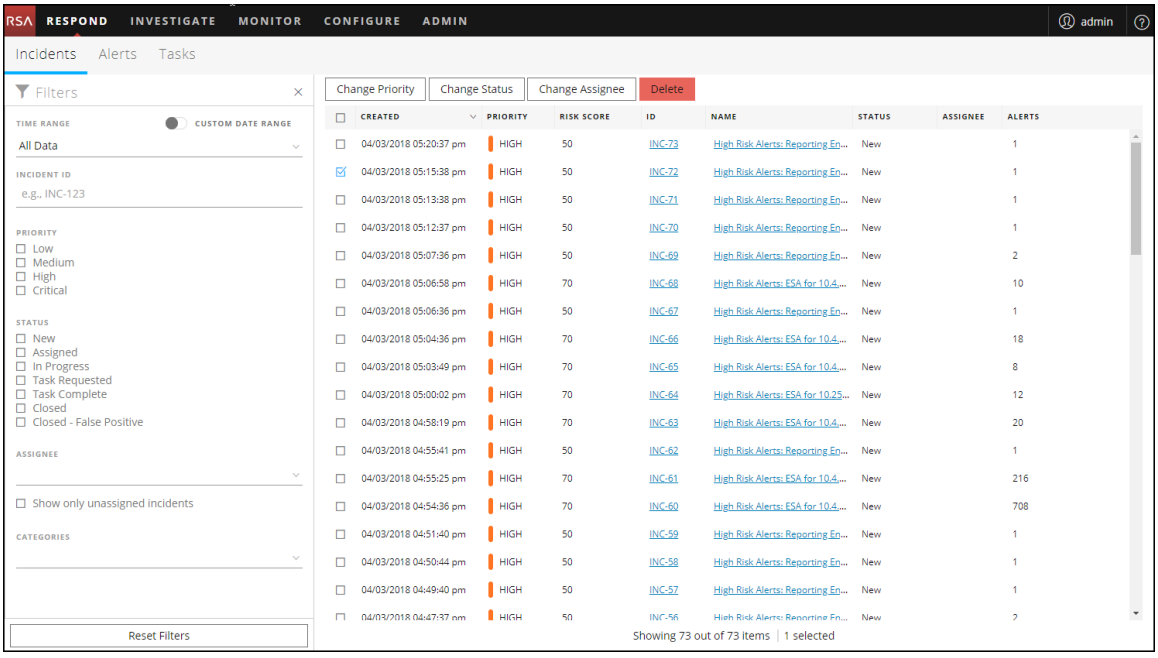
1. ［ユーザ環境設定］ダイアログを表示します。
2. ［**テーマ**］で、次のいずれかのオプションを選択します。
   - **ダーク**：暗い色のテーマです。暗い表示、またはコントラストが小さい方がよい場合に最適です。
   - **ライト**：明るい色のテーマです。明るい表意、コントラストが大きい方がよい場合、またはプロジェクターでアプリケーションを他の人に見せる場合に最適です。一部のビューは、テーマの変更の影響を受けないため、明るい色のテーマを選択した方が、まとまりのある画面として表示されます。

変更はすぐに反映されます。

次の図は、暗い色 のテーマを示しています。



次の図は、明るい色 のテーマを示しています。



ダッシュボードの管理

ダッシュボードはダッシュレットのグループで構成され、ユーザにとって重要なさまざまな情報を1か所に表示できます。RSA NetWitness® Platformでは、ダッシュボードを作成して、NetWitness Platform環境の全体像を示す概要情報やメトリックを収集したり、日常的な業務に関連性の高い情報のみを表示したりすることができます。

デフォルトでは、NetWitness Platformデフォルト ダッシュボードがNetWitness Platformへのログイン時に表示されます。このダッシュボードには、画面のカスタマイズの参考になるよう、あらかじめいくつかの便利なダッシュレットが追加されています。すべてのNetWitness Platformコンポーネントのダッシュボードは、デフォルトのNetWitness Platformダッシュボードまたはカスタムの NetWitness Platformダッシュボードに追加できます。

ユーザ権限に応じて、関心のあるさまざまな領域に関するダッシュボードとレポートを表示できます。事前構成済みダッシュボードを選択したり、ダッシュボードをインポートしたり、独自のカスタム ダッシュボードを作成することができます。ダッシュボードでは、レポートを素早く簡単に表示できます。ワークフローをサポートする情報を表示するようにダッシュボードを構成することができます。このトピックでは、ダッシュボードを設定するときに実行できるタスクの概要について説明します。

ダッシュボードの基礎

[監視]ビューがNetWitness Platformへのログイン後のデフォルトのランディング ページである場合、ログイン プロセス完了後すぐにデフォルト ダッシュボードか現在構成されているダッシュボードが必ず表示されます。別のNetWitness Platformコンポーネントからダッシュボードに戻るには、[**監視**]>[**概要**]に移動します。

ダッシュボードのタイトル

ダッシュボードのタイトルには、現在アクティブなダッシュボード(デフォルト ダッシュボードなど) が表示されます。

ダッシュボード選択リスト

ダッシュボード選択リストで事前構成済みダッシュボードとカスタム ダッシュボードにアクセスできます。ダッシュボードを選択すると、そのタイトルがNetWitness Platformツールバーの下に表示されます。

ダッシュボードには次の要素があります。

- ダッシュボード ツールバー
- ダッシュボード タイトルとダッシュボード選択リスト

ダッシュボード ツールバー

ダッシュボード ツールバーは、選択したダッシュボードのタイトルの隣にあります。ダッシュボード ツールバーで、ダッシュボードやダッシュレットに対してさまざまな操作を実行できます。

注:事前構成済みダッシュボードでは、コピー、削除、インポート、エクスポート、共有、行の追加のオプションが無効になります。

オプション	説明
★	選択したダッシュボードをお気に入りに設定します。
Default Dashboard	選択可能なダッシュボードの一覧を表示します。

オプション	説明
	[ダッシュボードの作成]ダイアログを表示します。このダイアログで、カスタム ダッシュボードを定義または追加します。
	カスタム ダッシュボードを削除します。デフォルト ダッシュボードは削除できません。
	ダッシュボードをコピーできます。
	[ダッシュレットの管理]ダイアログが表示されます。
	.zipファイルにダッシュボードをエクスポートします。
	.zipまたは.cfgファイルからダッシュボードをインポートします。
	他のユーザとダッシュボードを共有できます。
	必要に応じてユーザがダッシュボードに行と列を追加することができます。ダッシュレットを追加する行で  アイコンをクリックします。

デフォルト ダッシュボード

デフォルト ダッシュボードは、特定のダッシュレットを特定の位置に表示するように構成されています。デフォルト ダッシュボードは、ダッシュボードの構成の例であり、これを基にしてカスタマイズを行うことができます。

- ダッシュレットの操作(編集、追加、移動、最大化、削除)によって、デフォルト ダッシュボードに表示される情報をカスタマイズできます。
- デフォルト ダッシュボードを変更した後でも、元のレイアウトに復元できます()。
- デフォルト ダッシュボードを削除、共有することはできません。

事前構成済みダッシュボードの選択

NetWitness Platform Suiteをインストールすると、次の事前構成済みダッシュボードが自動的に有効になり、使用できます。

- デフォルト
- Identity
- Investigation
- Operations - ファイル分析

- Operations - Logs
- Operations - Network
- Operations - Protocol Analysis
- 概要
- RSA SecurID
- Threat - Hunting
- Threat - Intrusion
- Threat - Malware Indicators

事前構成済みダッシュボードで次のアクションは実行できません。

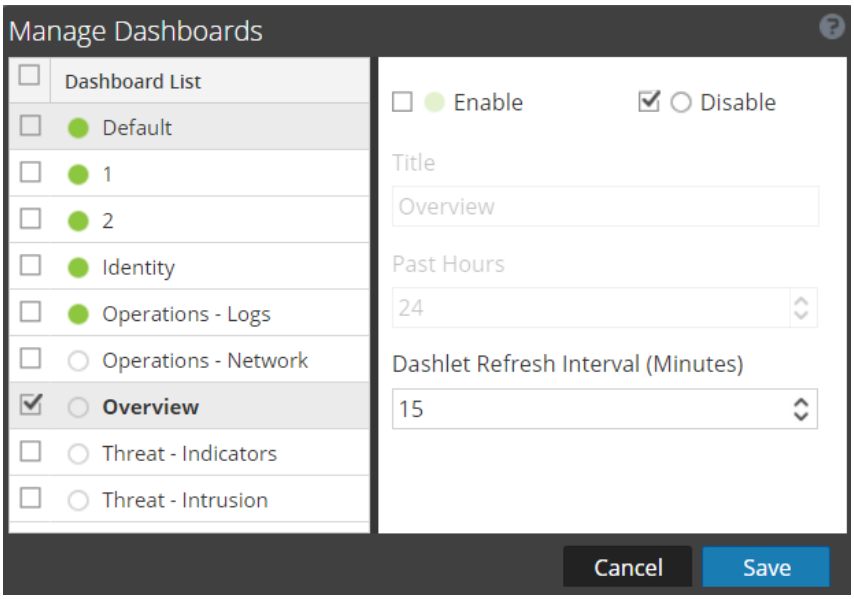
- ダッシュボードの編集
- ダッシュボードのエクスポート
- ダッシュボードの共有
- ダッシュボードの削除

各事前構成済みダッシュボードの詳細については、RSA Linkの「RSA Content」領域の「Dashboards Catalog」を参照してください。

ダッシュボードの有効化または無効化

ダッシュボードを有効化または無効化すると、ダッシュボード内のすべてのダッシュレットは、その他のダッシュボードで使用されている場合を除き、関連するチャートとともに有効化または無効化されます。

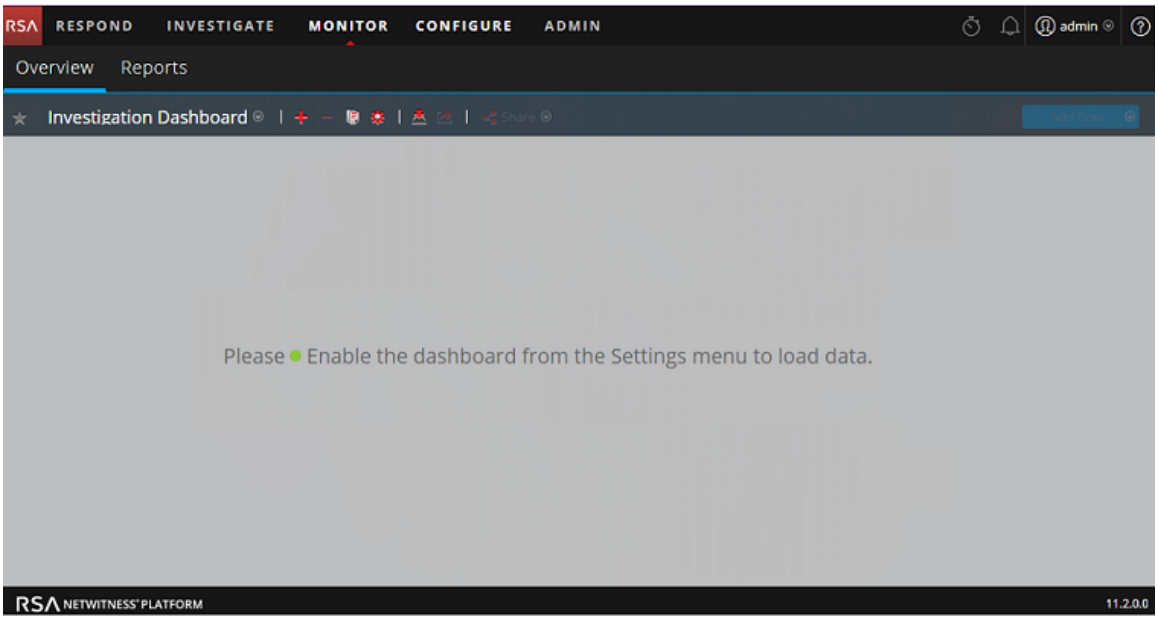
NetWitness Platformモジュールは、[ダッシュレットの管理]ダイアログに表示されるダッシュレットだけを表示できます。メイン ダッシュボードでは、NetWitness Platformのすべてのダッシュレットが提供されます。次の図は使用可能なダッシュレットの例です。



名前	説明
ダッシュボード リスト	デフォルト、事前構成済み、カスタムのダッシュボードのリストを表示します。
☑ Enable	選択したダッシュレットが有効化されている場合に表示されます。
☐ Disable	選択したダッシュレットが無効化されている場合に表示されます。
タイトル	選択したダッシュレットのタイトルを表示します。ダッシュボードは名称変更もできます。
時間	データが収集される時間が表示されます。
ダッシュレット更新間隔(分)	ダッシュレットの更新間隔の時間が表示されます。

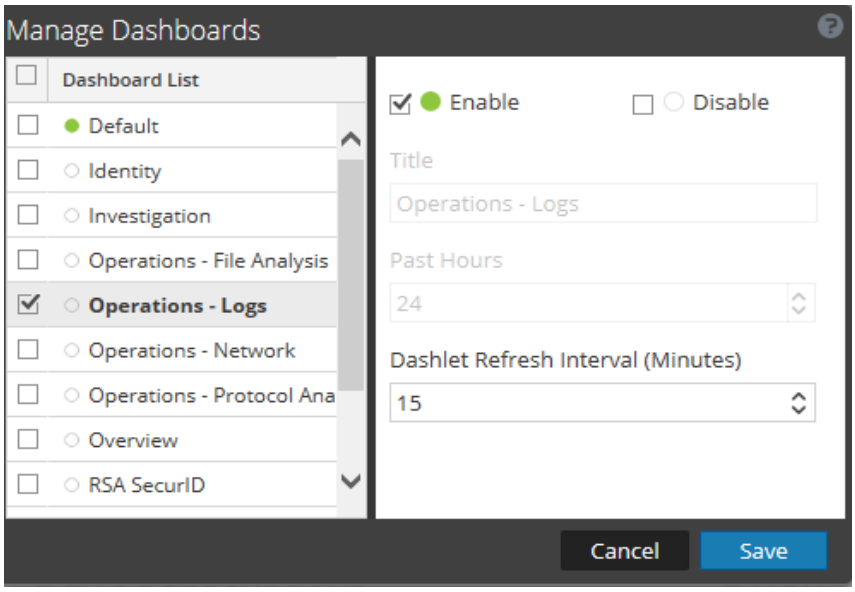
ダッシュボードの有効化

有効化されていないダッシュボードを選択した場合、マスクされたスクリーンが表示されます。



1つまたは複数のダッシュボードを有効化するには、次の操作を行います。

1. 有効化するダッシュボードに移動します。
2. ダッシュボード ツールバーの  ([ダッシュボードの管理])をクリックします。
   [ダッシュボードの管理]ダイアログが表示されます。

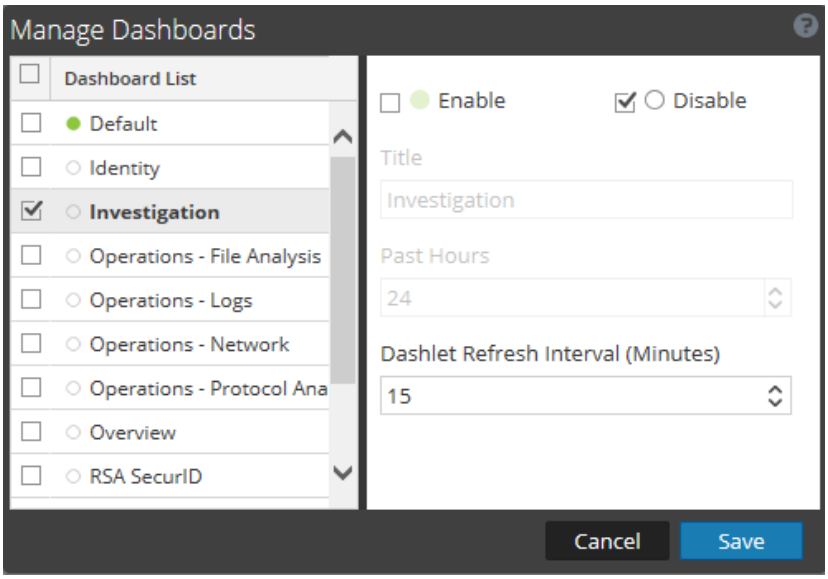


3. ダッシュボード リストから、有効化するダッシュボードを選択します。
4. [**有効化**]チェックボックスを選択します。
5. [**保存**]をクリックします。

ダッシュボードの無効化

1つまたは複数のダッシュボードを無効化するには、次の操作を行います。

1. 無効化するダッシュボードに移動します。
2. ダッシュボード ツールバーの  ([ダッシュボードの管理])をクリックします。
   [ダッシュボードの管理]ダイアログが表示されます。



3. ダッシュボード リストから、無効化するダッシュボードを選択します。
4. **Disabled**チェックボックスを選択または選択解除します。
5. [**保存**]をクリックします。

ダッシュボードをお気に入りに設定

NetWitness Platformのビューをカスタマイズするには、事前構成済みまたはカスタム ダッシュボードをお気に入りとして設定することができます。NetWitness Platformダッシュボードでは、NetWitness Platformのすべてのダッシュレットが提供されます。[お気に入り]ダイアログで特定のダッシュボードをお気に入りのダッシュボードに設定すると、NetWitness Platformにログインするたびにお気に入りリストにダッシュボードが表示されます。

1. 任意のダッシュボードに移動します。
2. ダッシュボード ツールバーで、  をクリックします。

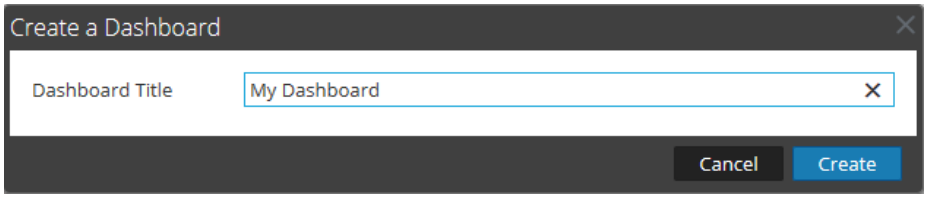
   [お気に入り]アイコンの色が赤色の場合は、その選択したダッシュボードがお気に入りとして設定され、リストの最上部に表示されることを意味します。

カスタム ダッシュボードの作成

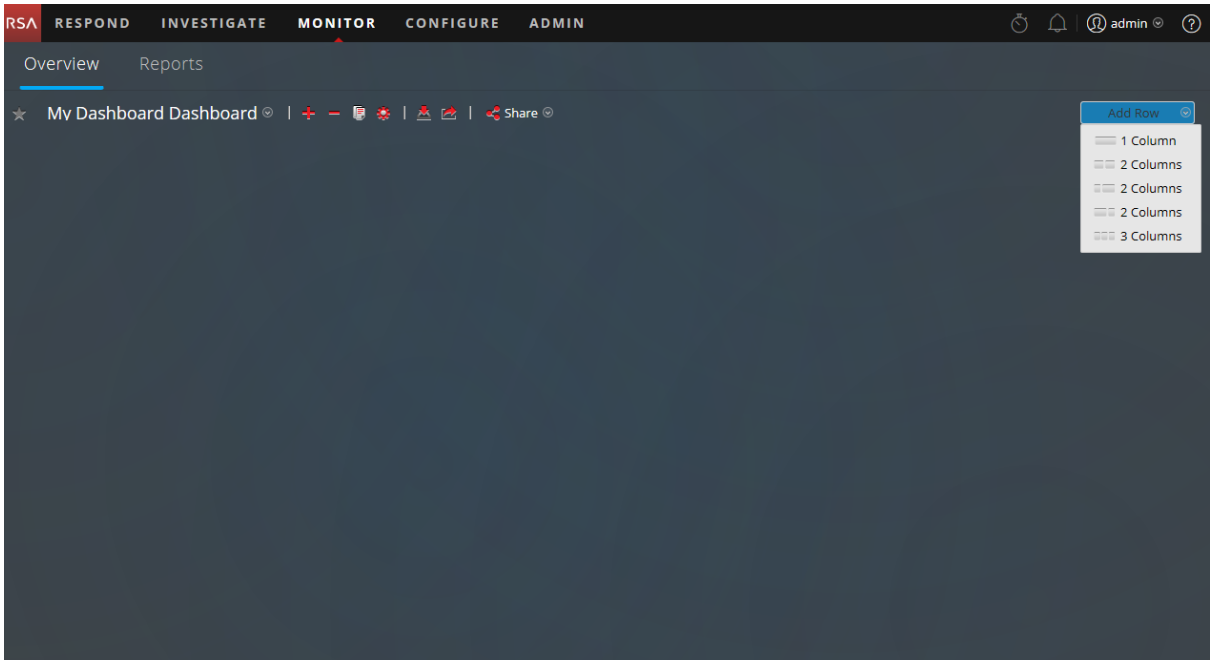
組織内の特定の地域や部門、機能など、特定の用途に使用するカスタム ダッシュボードを作成できます。各カスタム ダッシュボードは、ダッシュボード選択リストに追加されます。

カスタム ダッシュボードを作成するには、次の手順に従います。

1. ダッシュボード ツールバーで、  をクリックします。
   [ダッシュボードの作成]ダイアログが表示されます。

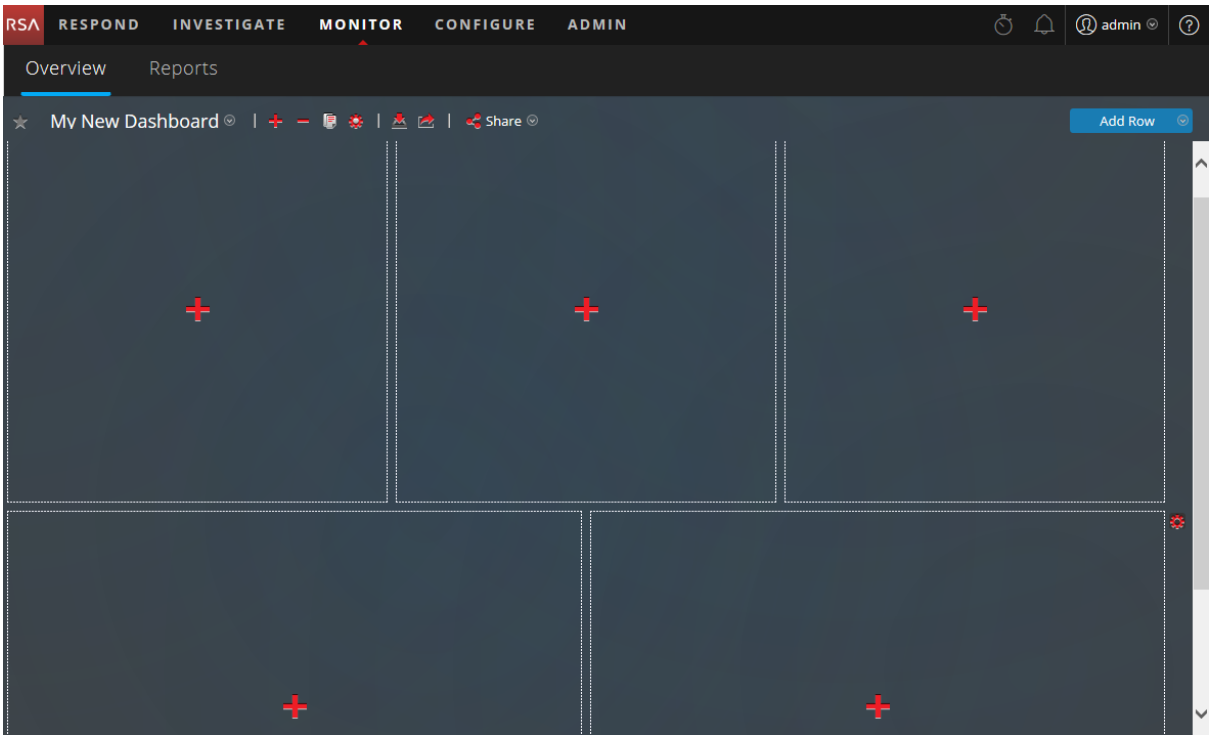


2. 新しいダッシュボードのタイトルを入力し、[**作成**]をクリックします。
   新しいダッシュボードが空白のスクリーンとして表示されます。



3. ダッシュボードに行を追加します。スクリーンの右側の[**行の追加**]()オプションを使用して、任意の列数の行を追加することができます。ドロップダウン リストで目的の列の構成をクリックすると、選択した列数の行がダッシュボードに1行追加されます。複数の行を追加するには、同じ

手順を繰り返します。



4. 行内の空のプレースホルダーの  をクリックし、ダッシュボードに必要なダッシュレットを追加できます。ダッシュレットの追加と管理の詳細については、「ダッシュレットの操作」を参照してください。

カスタム ダッシュボードを作成すると、次のような操作を行うことができます。

- ダッシュボード選択リストからオプションを選択することによって、ダッシュボードを切り替える。
- カスタム ダッシュボードを削除する。
- ダッシュボードをインポートまたはエクスポートする。

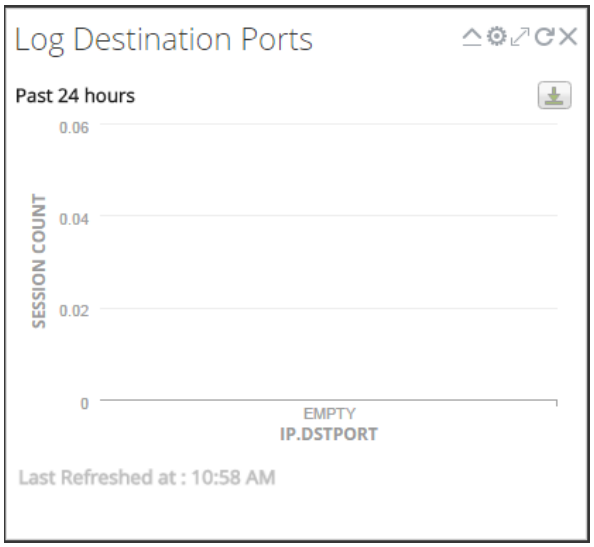
各ダッシュボードには、次のような構成要素があります。

- ダッシュボード ツールバー
- ダッシュボード タイトルとダッシュボード選択リスト
- ダッシュレット(ない場合もある)

ダッシュレットの操作

NetWitness Platformでは、ダッシュレットを使用して、システム情報の重要なサブセット、サービス、ジョブ、リソース、サブスクリプション、ルール、その他の情報を表示します。

ダッシュレットの操作メニューは各ダッシュレットのタイトル バーにあります。すべてのダッシュレットで共通のコントロールのセットが使用されます。また、特定のダッシュレットで使用するコントロールもダッシュレットのタイトル バーに表示されます。



次の表では、ダッシュボードの各アイコンについて説明します。

アイコン	名前	説明
	垂直方向に折りたたむ	ダッシュレットを垂直方向に折りたたみ、タイトルのみを表示します。
	垂直方向に展開	ダッシュレットを元のサイズに展開します。
	再ロード	ダッシュレットを再ロードします。
	設定	ダッシュレットの構成可能な設定を表示します。
	最大化	幅(横方向)に収まらない内容を含むダッシュレットで、チャートまたはダッシュレットを最大化してフル スクリーン表示します。
	削除	ダッシュボードからダッシュレットを削除します。
最終更新		関連するチャートからデータをポーリングした時刻が表示されます。

アイコン	名前	説明
更に表示		クリックすると、メインのダッシュレットにリンクされたダッシュボードに移動し、より多くの情報が表示されます。既存のダッシュレットにダッシュボードをリンクしていない場合、このリンクはダッシュレットに表示されません。このオプションを構成するには、⚙をクリックし、[ダッシュボードのリンク]フィールドでこのダッシュレットに関連する詳細情報を表示するダッシュボードを選択します。 **注**:この機能は、NetWitness Platform 11.0以降のリアルタイム チャート ダッシュレットと事前構成済みダッシュボードでのみ使用できます。

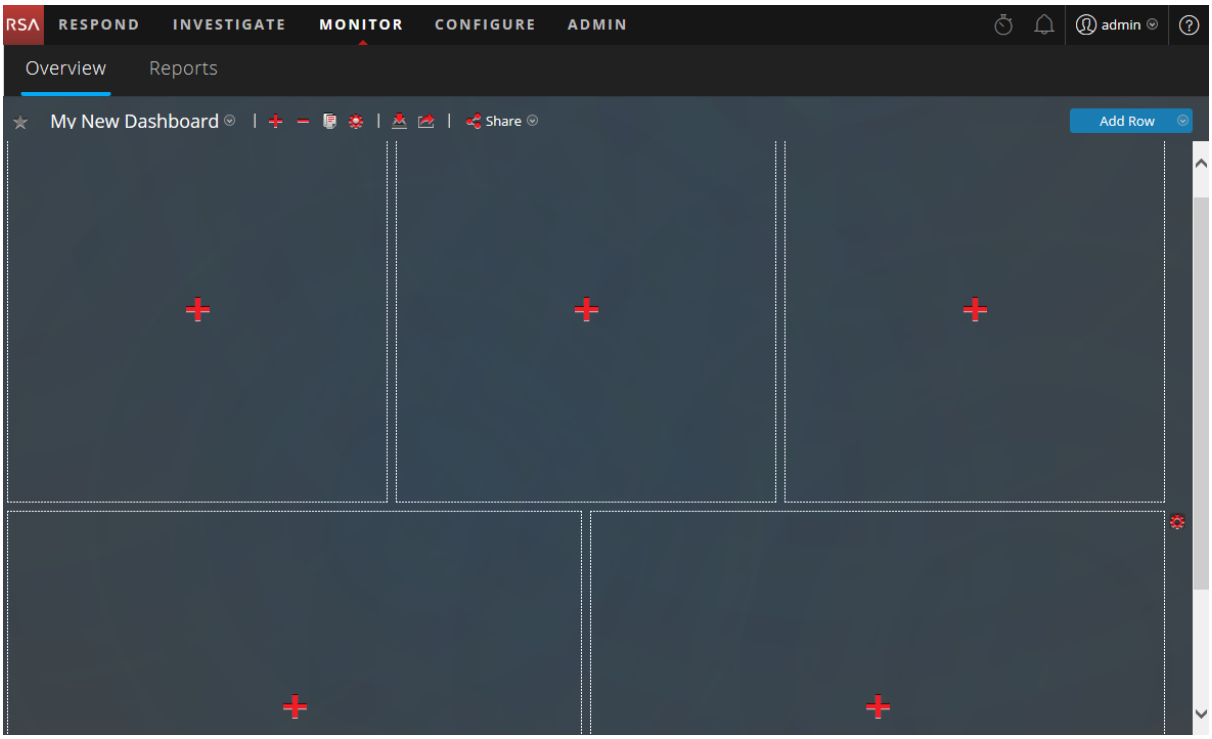
デフォルト ダッシュボードにダッシュレットを追加するか、便利な独自のダッシュレット セットを使用してカスタム ダッシュボードを作成し、ワークフローをより効率化することができます。

ダッシュレットの追加

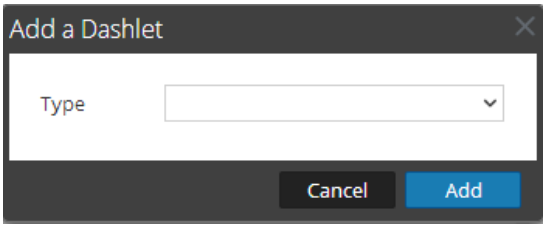
NetWitness Platformのビューをカスタマイズする場合には、デフォルト ダッシュボードにダッシュレットを追加したり、カスタム ダッシュボードを作成したりできます。ただし、事前構成済みダッシュボードにダッシュレットを追加することはできません。

ダッシュレットを追加するには、次の手順を実行します。

1. 任意のダッシュボードに移動するか、新しいダッシュボードを作成します。

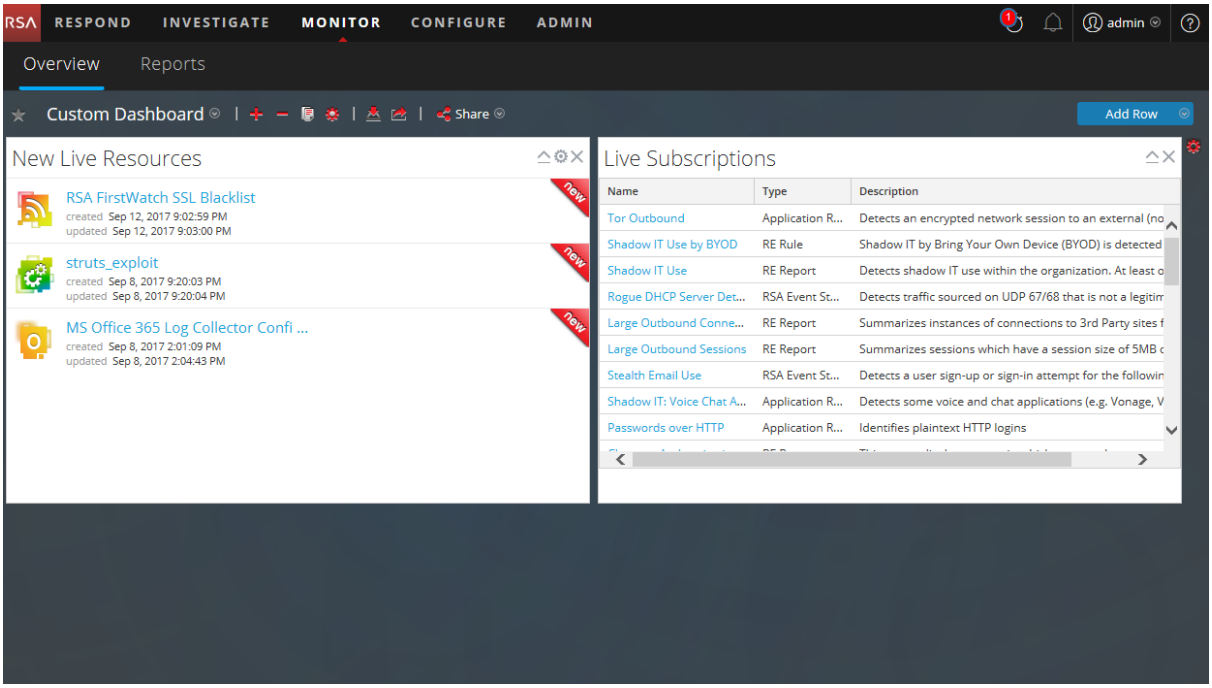


2. ダッシュレットを追加するプレースホルダーで  をクリックします。
[ダッシュレットの追加]ダイアログが表示されます。



3. [**タイプ**]選択リストをクリックして使用可能なダッシュレットを表示し、追加するダッシュレットのタイプを選択します。追加するダッシュレットのタイプに応じて構成可能なフィールドが[**ダッシュレットの追加**]ダイアログに表示されます。
4. ダッシュレットのタイトルを入力します。タイトルには、英字、数字、特殊文字、空白を含めることができます。
5. これ以外にダッシュレットの構成可能なフィールドがある場合は、適切な値を設定します。

6. 必須入力フィールドをすべて構成したら、[**追加**]をクリックします。
   ダッシュボードの選択したプレースホルダーにダッシュレットが追加され、自動的に保存されます。



ダッシュレットのプロパティの編集

事前構成済みのすべてのダッシュレットは読み取り専用であり、プロパティを編集することはできません。その他のダッシュレットは編集可能で、ユーザはダッシュレットに表示されるデータをカスタマイズできます。編集可能なプロパティを持つダッシュレットでは、設定(⚙)オプションをクリックするとすべての編集オプションが表示されます。

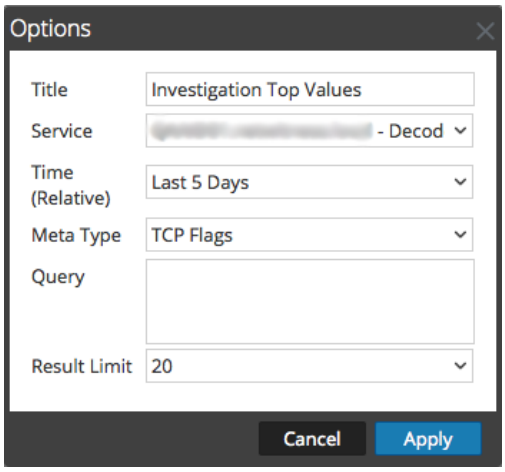
ダッシュレットを追加するとドラッグ アンド ドロップでき、場所を入れ替えることができます。

編集可能なプロパティがないダッシュレット([Liveサブスクリプション]ダッシュレットなど) の場合、タイトル バーに設定オプションは表示されません。多くのダッシュレットは編集可能であり、次のプロパティを編集することができます。

- ダッシュレットの表示タイトル。
- 監視するサービスのタイプ。たとえばDecoderのみを監視したり、DecoderとConcentratorを監視するよう構成できます。

ダッシュレットに表示される情報の種類と量を指定するためのパラメータを持つダッシュレットもあります。たとえば、リアルタイム チャート ダッシュレットには、そのような設定オプションがあります。

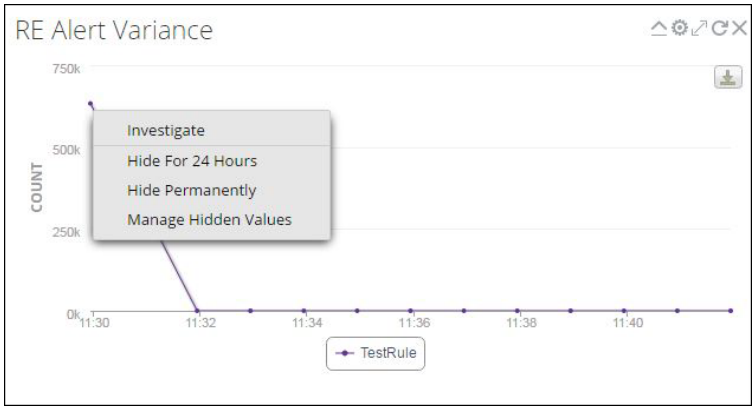
1. ダッシュレットのオプションを表示および変更するには、ダッシュレットのタイトル バーで設定(⚙)をクリックします。
   [オプション]ダイアログが表示されます。



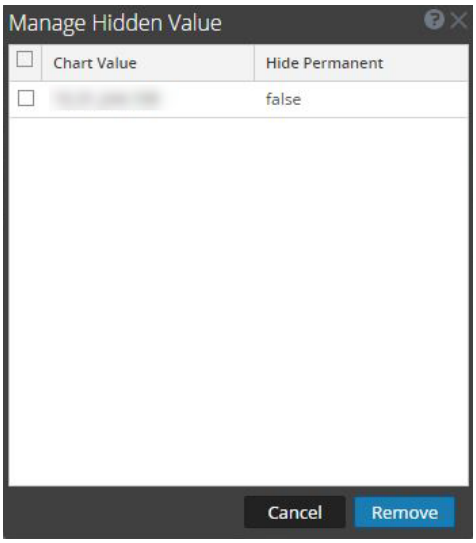
2. 表示されているプロパティを編集します。たとえば、[調査 上位の値]ダッシュレットでは、結果の件数を20から40に変更できます。
3. [**適用**]をクリックします。

一部のダッシュレットには、外観またはダッシュレットのコンテンツをカスタマイズする構成オプションがあります。次のオプションは、[レポート 上位アラート]、[レポート アラート推移]、[レポート リアルタイム チャート]ダッシュレットを左クリックすると表示されます。

- **24時間だけ非表示**:このオプションでは、24時間だけ選択した値を非表示にすることができます。24時間後、値が構成され、上位に存在する場合、データは自動的にダッシュレットに表示されます。
- **永久に非表示**:このオプションでは、[非表示の値の管理]オプションを使用して設定を戻すまで、選択した値を永続的に非表示にすることができます。



- **非表示の値の管理**:このオプションは、非表示のすべての値のリストを表示します。値のチェックボックスを選択して[**削除**]をクリックすると、チャートにデータを表示することができます。



注:24時間だけ非表示、永久に非表示、非表示の値の管理のオプションはGeoMapチャートでは使用できません。

注:事前構成済みダッシュボードの値を編集する場合は、ユーザ固有の変更です。事前構成済みダッシュボードへの変更は、ユーザのダッシュボードにのみ適用され、同じ事前構成済みダッシュボードを使用している他のユーザには表示されません。たとえば、Overviewダッシュボードの値を非表示にする場合、変更は自身のダッシュボードにのみ適用されます。別のユーザが同じOverviewダッシュボードを表示する場合、値はそのまま表示されます。同じことはカスタム ダッシュボードにも当てはまります。カスタム ダッシュボードの値を非表示にして別のユーザと同じダッシュボードを共有すると、ダッシュボードが共有されていても値はそのまま表示されます。

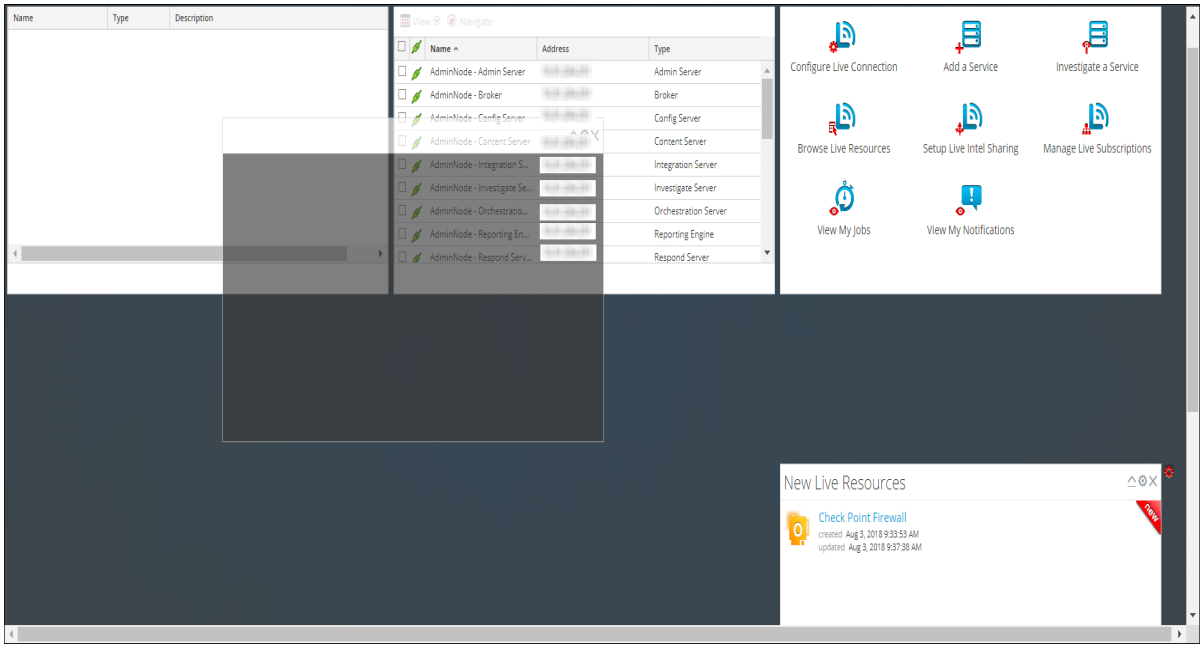
使用可能なダッシュレットの詳細については、RSA Linkの「RSA Content」領域の「Dashboards Catalog」を参照してください。

ダッシュレットの再配置

ダッシュレットは、ダッシュボード上でドラッグ アンド ドロップによって好みの配置に並べ替えることができます。

1. 移動するダッシュレットのヘッダーにカーソルを合わせます。
   ダッシュレット上に方向カーソル ✥ が表示されます。移動するダッシュレットのヘッダにカーソルを合わせます。

2. マウスをクリックし、そのままウィンドウを新しい位置にドラッグします。
次の図は、再配置中のダッシュレットを示します。



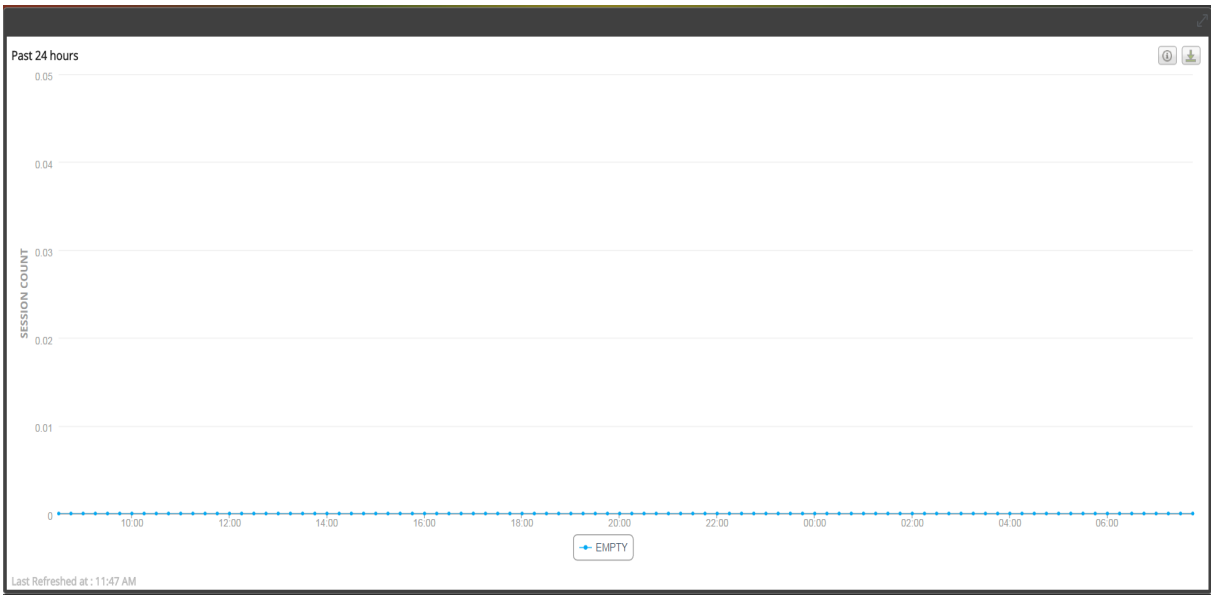
3. ダッシュレットを目的の位置に移動したら、マウス ボタンを離してドロップします。
移動先にもともと配置されていたダッシュレットは下へ移動します。

単体ダッシュレットの最大化

このセクションでは、ダッシュレットを同じダッシュレット タイトルのまま、メインのNetWitness Platformダッシュボードの領域全体で開く方法について説明します。 一部のレポート ダッシュレットのように、列やチャートが多いダッシュレットは、スクロールしなくてもコンテンツ全体が表示できるように最大化すると見やすくなります。

ダッシュレットを最大化するには、ダッシュレットのタイトル バーにある最大化コントロール アイコン(⤢) をクリックします。ダッシュレットが全画面表示されます。

ダッシュレットを最小化するには、ダッシュレットのタイトル バーにある同じコントロール アイコン(⤢) をクリックします。ダッシュレットは、以前のサイズに戻ります。



ダッシュレットの削除

1. ダッシュレットのタイトルバーの✕をクリックします。
   ダッシュレットを削除することを確認するポップアップが表示されます。
2. 削除する場合は、[**はい**]をクリックします。ダッシュレットがダッシュボードから削除されます。
   削除しない場合、[**いいえ**]をクリックします。

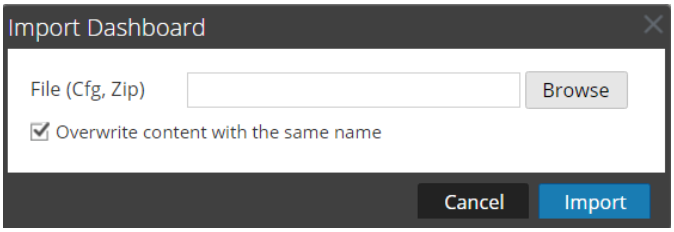
注：ダッシュレットを削除した後の領域には、前述の[ダッシュレットの追加]の手順を使用して別のダッシュレットを追加できるようプレースホルダーが表示されます。

ダッシュボードのインポートとエクスポート

日々変化する環境や条件に合わせてダッシュボードをカスタマイズすることができますが、結果的に日常的には必要でないダッシュボードが多数作成される場合があります。特別なカスタムダッシュボードを作成する必要が出てくるたびに、一から定義し直す必要はありません。現在使用していないダッシュボードはエクスポートしておくことができます。以前にエクスポートしたダッシュボードを使用したいときに、ダッシュボードをNetWitness Platformにインポートします。

ダッシュボードのインポート

1. ダッシュボード ツールバーで、([ダッシュボードのインポート]) をクリックします。
   [ダッシュボードのインポート]ダイアログが表示されます。



2. [**ダッシュボードのインポート**]ダイアログでダッシュボード ファイルを参照します。.cfg、.zipファイルをインポートすることができます。
3. [**インポート**]をクリックします。
   ダッシュボードがNetWitness Platformに表示されます。

注: Security Analytics 10.6.xからNetWitness Platform 11.xにダッシュボードをインポートする場合、ダッシュボードと、関連付けられているルールとチャートは個別にインポートする必要があります。しかし、ダッシュボードをNetWitness Platform 11.xからNetWitness Platformにインポートする場合は、ダッシュボードとそれに関連するすべてのルールおよびチャートを.zip形式でインポートできます。

ダッシュボードのエクスポート

注: レポート リアルタイム ダッシュボードをエクスポートすると、それに対応するReporting Engineの内容もエクスポートされます。

エクスポートされたダッシュボードは、同じNetWitness Platformインスタンス内で使用することを想定しています。同じ権限を持っている、組織内の他のユーザとカスタム ダッシュボードを共有することもできます。

ダッシュボードをエクスポートするには、ダッシュボードを開いて、ダッシュボード ツールバーの[編集]ドロップダウン メニューから[ダッシュボードのエクスポート]オプションにアクセスする必要があります。

1. エクスポートするダッシュボードに移動します。現在表示されているダッシュボードの[**ダッシュボード選択リスト**]ドロップダウン メニューに既存のダッシュボードがすべて表示されます。
2. ダッシュボード ツールバーの([ダッシュボードのエクスポート]) をクリックします。
   エクスポートされたファイルは.zip形式で保存されます。

注: エクスポート機能は事前構成済みダッシュボードでは使用できません。

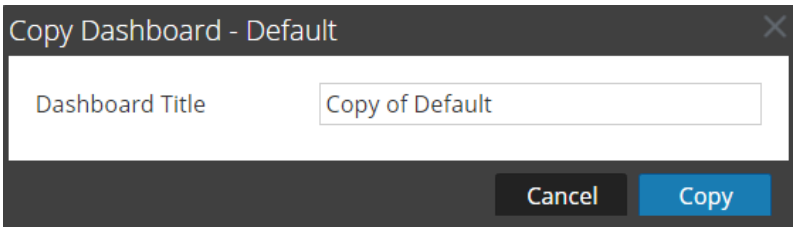
ダッシュボードのコピー

NetWitness Platformでダッシュボードをカスタマイズする場合には、NetWitnessダッシュボードまたはカスタム ダッシュボードをコピーします。NetWitness Platformダッシュボードには、その名のとおり、NetWitness Platformのすべてのダッシュレットが含まれます。[ダッシュボードのコピー]ダイアログは、ダッシュボードの複製を作成します。この複製をカスタマイズすることができます。ダッシュボードをコピーすると、デフォルトの名前が`Copy of`にプレフィックスされます。たとえば、元のダッシュボードの名前が`XYZ`、コピーされたダッシュボードのデフォルトのタイトルは`Copy of XYZ`になります。

ダッシュボードをコピーするには、次の操作を行います。

1. 任意のダッシュボードに移動します。
2. ダッシュボード ツールバーで、をクリックします。
   [ダッシュボードのコピー]ダイアログが表示されます。次のスクリーンショットでは、ダッシュボードをコ

ピーする例を示します。



3. ダッシュボードのタイトルを入力します。
4. [**コピー**]をクリックします。

ダッシュボードの共有

NetWitness Platformでは、管理者は、管理者、アナリスト、オペレーターなどの他のロールと、ダッシュボードを共有して表示させることができます。ダッシュレットを共有すると、ユーザはダッシュボードの表示、お気に入りへの追加、コピー、エクスポートができます。アナリスト、オペレーターなどの管理者以外のロールの場合、同じロールとのみダッシュボードを共有できます。たとえば、アナリストはダッシュボードを他のアナリストとのみ共有できます。

1. 任意のダッシュボードに移動します。
2. ダッシュボード ツールバーで、 

をクリックして、ダッシュボードを共有するロールのチェックボックスをオンにします。

注：ダッシュボードを共有しない場合は、ロールのチェックボックスをオフにします。

ジョブの管理

RSA NetWitness® Platformでは、オン デマンド タスクやスケジュール設定されたタスクが完了するまでに数分かかる場合があります。NetWitness Platformのジョブ システムで時間のかかるタスクを開始しても、ジョブの実行中にNetWitness Platformの他の機能は継続して使用することができます。そのような場合、タスクの進行状況を監視できるだけでなく、タスクが完了したこと、また結果が成功か失敗かの通知を受け取ることができます。

NetWitness Platformのユーザ インタフェースでは、ツールバーからジョブのクイック ビューを開くことができます。ジョブ トレイはいつでも参照が可能で、ジョブ ステータスが変更されると、[ジョブ]アイコン( ) にフラグが付けられ、実行中のジョブの数が示されます。すべてのジョブが完了すると、この数字は表示されなくなります。

ジョブは次の2つのビューでも確認することができます。

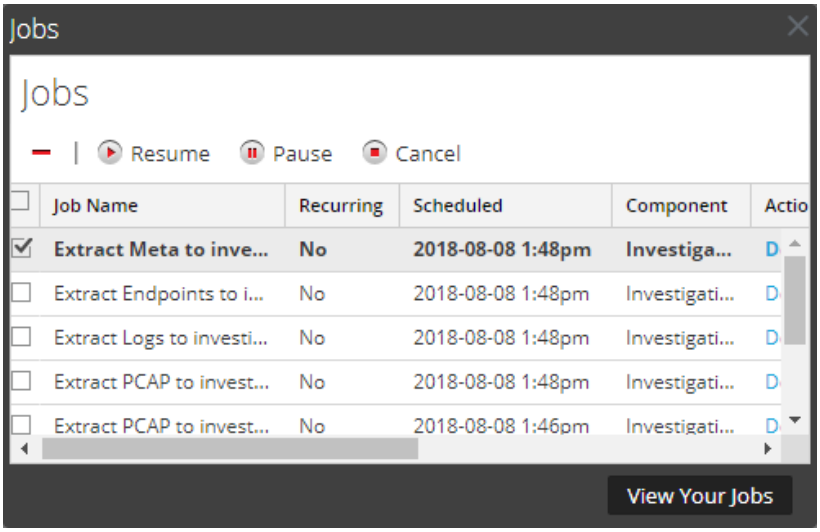
- [ユーザ プロファイル]パネルでは、ジョブ トレイと同じ内容のジョブ画面をフル パネルで表示できます。確認することができるのは自分が実行したジョブだけです。
- [システム]ビューでは、管理権限を持つユーザが、すべてのユーザのすべてのジョブを1つのジョブ パネルで表示および管理できます。

ジョブ パネルの構造はすべてのビューで同じです。

ジョブ トレイの表示

NetWitness Platformツールバーで、[ジョブ]アイコン( ) をクリックします。

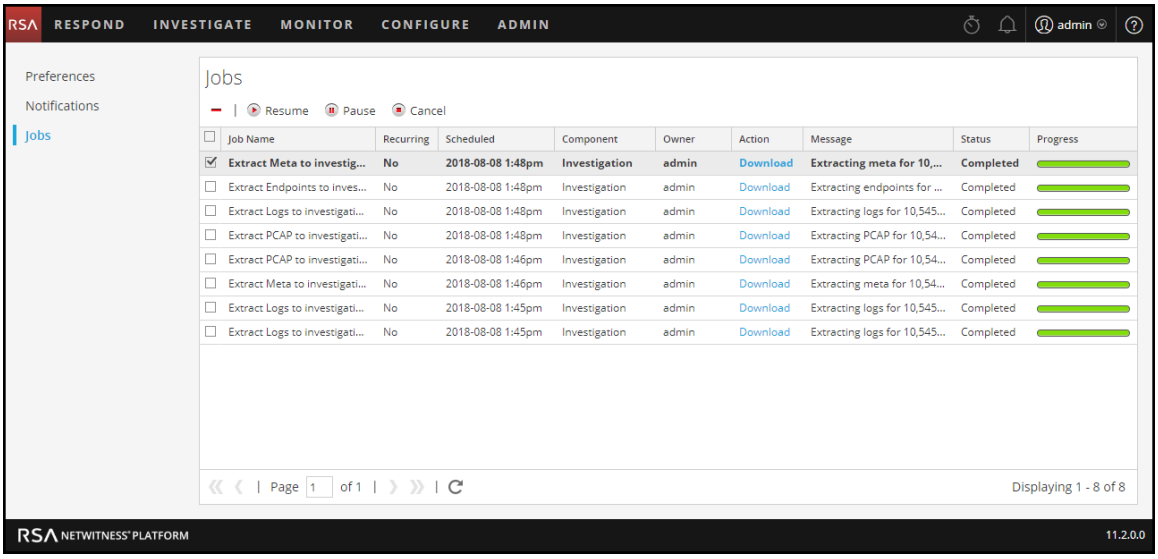
ジョブ トレイが表示されます。



ジョブ トレイには、[ジョブ]パネルに表示される列のサブセットを使用して、自分が管理するすべてのジョブ(定期実行ジョブと定期実行でないジョブ) が一覧表示されます。[ジョブ トレイ]と、[ユーザ プロファイル]ビュー> [ジョブ]パネルの内容は同一です。[管理システム]ビューでは、すべてのユーザのすべてのNetWitness Platformジョブの情報が[ジョブ]パネルに一覧表示されます。

自分のジョブをすべて表示

ジョブを拡大表示するには、ジョブトレイで[**自分のジョブを表示**]をクリックします。
[ジョブ]パネルが表示されます。



定期実行ジョブの一時停止と再開

[一時停止]と[再開]オプションは、定期実行ジョブにのみ適用されます。実行中の定期実行ジョブを一時停止しても、実行中のジョブには影響しません。(ジョブが一時停止中のままである場合)次の回の実行は、スキップされます。

1. 定期実行ジョブの次回以降の実行を停止するには、[**ジョブ**]パネルで、ジョブを選択し、[**一時停止**]をクリックします。
   このジョブの次回の実行がスキップされ、[再開]をクリックするまでスケジュールは一時停止されます。
2. 一時停止された定期実行ジョブの実行を再開するには、ジョブを選択して、[**再開**]をクリックします。
   このジョブの次回の実行はスケジュール設定どおりに行われ、ジョブのスケジュールが再開されます。

ジョブのキャンセル

実行中または実行のキューに入っているジョブをキャンセルするには、次の手順を実行します。

1. **ジョブトレイ**または[**ジョブ**]パネルで、1つ以上のジョブを選択します。
2. [**キャンセル**]をクリックします。
   確認ダイアログが表示されます。
3. [**はい**]をクリックします。
   このジョブはキャンセルされ、**キャンセル済み**ステータスのエントリーがリストに残されます。

定期実行ジョブをキャンセルすると、ジョブのその回の実行がキャンセルされます。スケジュールされているジョブの次の回の実行は、正常に実行されます。

ジョブの削除

注意:ジョブを削除すると、ジョブはすぐにリストから削除されます。確認ダイアログは表示されません。定期実行ジョブを削除すると、スケジュールされている以降のジョブの実行もすべて削除されます。

ユーザは実行前、実行中、実行後に自分のジョブを削除できます。管理者は任意のジョブを削除できます。ジョブを削除するには、次の手順を実行します。

1. 1つ以上のジョブを選択します。
2. をクリックします。
   ジョブがリストから削除されます。

ジョブ結果のダウンロード

[アクション]列が[ダウンロード]ステータスであるジョブの場合、ジョブの結果をダウンロードできます。[調査]ビューにおいて、セッションのパケット データをPCAPファイルとして抽出したり、セッションからペイロード ファイル(たとえば、Wordドキュメントやイメージ) を抽出したりすると、ジョブの結果としてファイルが作成されます。ローカル システムにファイルをダウンロードするには、[**ダウンロード**]をクリックします。

通知の表示と削除

RSA NetWitness® Platformのユーザ インタフェースでは、作業領域を離れることなく最新のシステム通知を確認することができます。NetWitness Platformツールバーから通知のクイック ビューを開くことができます。通知トレイはいつでも参照が可能で、新しい通知を受け取ると、通知アイコンにフラグ() が表示されます。

通知の例としては以下のものがあります。

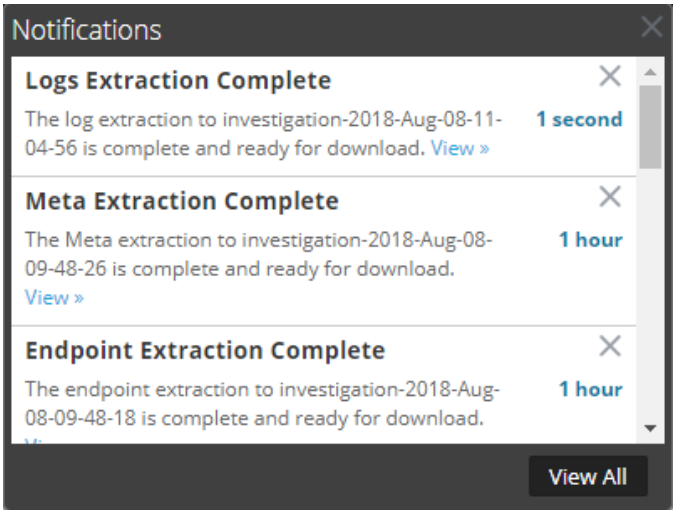
- ホストのアップグレードが完了した。
- DecoderへのParserの適用が完了した。
- 新しいバージョンのソフトウェアが利用可能。

次の2つのビューで通知を確認できます。

- 通知トレイには、最近の通知が表示されます。
- ユーザ プロファイルの通知パネルには、すべての通知が表示されます。

最近の通知の表示

最近の通知を表示するには、通知アイコン() をクリックします。
通知トレイが表示されます。

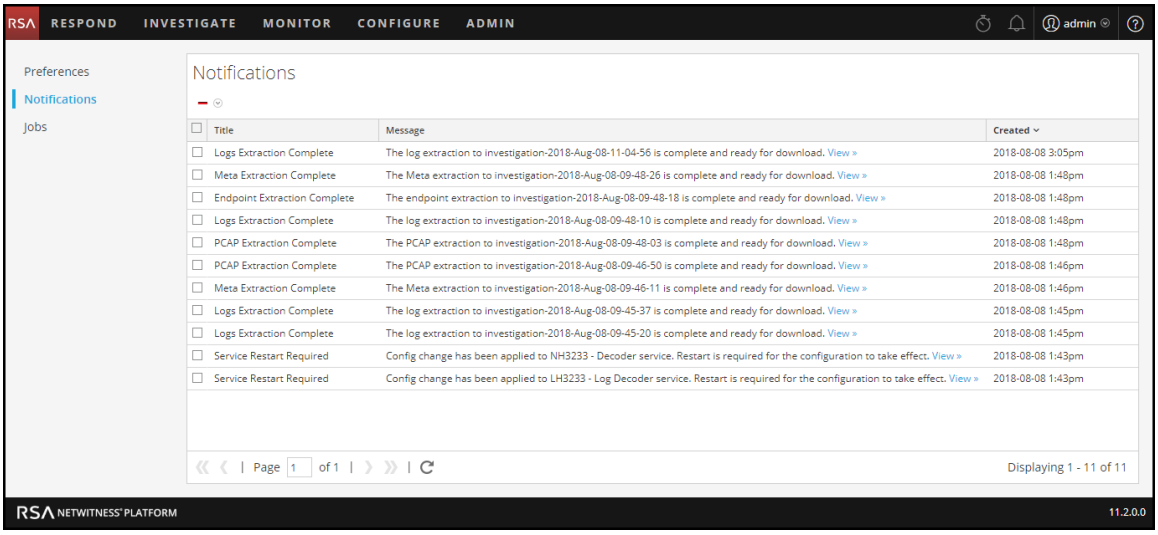


すべての通知の表示

すべての通知を表示するには、次のいずれかの操作を行います。

- をクリックして通知トレイを開き、通知トレイで[**すべて表示**]をクリックします。
- NetWitness Platformブラウザ ウィンドウの右上隅にある[> **プロファイル**]を選択し、[環境設定]ダイアログのオプション パネルで[**通知**]を選択します。

[通知]パネルには、すべての通知が表示されます。



通知レコードの削除

通知レコードを削除するには、次の手順を実行します。

1. **プロファイル通知**リストで、削除する通知を選択します。
2. をクリックします。
   選択した通知がこのリストと通知トレイから削除されます。

アプリケーションのヘルプの表示

RSA NetWitness® Platformの使用中にヘルプを表示するためのさまざまな方法が用意されています。インライン ヘルプ、ツールチップ、オンライン ヘルプ リンクがあります。

インライン ヘルプの表示

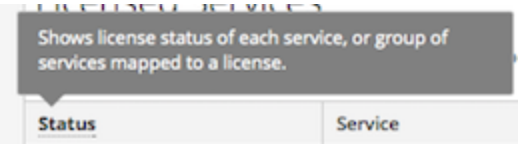
インライン ヘルプでは、NetWitness Platformユーザ インタフェースでユーザが現在表示しているセクションまたはフィールドで行う操作に関する追加情報が提供されます。インライン ヘルプを表示するには、 の上にマウス ポインタを置きます。インライン ヘルプには、構成要素の簡単な説明が表示されます。

インライン ヘルプの例 :

ツールチップの表示

ツールチップは、アクション、フィールド、パラメータに関するテキストまたは追加情報をすばやく表示する方法です。ツールチップは下線付きのテキストに対して表示されます。下線付きのテキストの上にマウス ポインターを置くと、ツールチップが表示され、テキストに関する簡単な説明を確認できます。

ツールチップの例 :

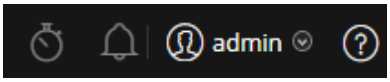


オンライン ヘルプの表示

オンライン ヘルプ リンクは、NetWitness PlatformからRSA Linkオンライン ドキュメントへの外部リンクです。このサイトにはNetWitness Platformの完全なドキュメント セットが揃っており、リンクをクリックすると、ユーザ インタフェースに現在表示されている画面に関連するトピックに直接移動することができます。

現在の画面に関連するオンライン ヘルプのトピックを表示するには、NetWitness Platformツールバーまたはダイアログの をクリックします。関連するヘルプ トピックが、別のブラウザ ウィンドウに表示されます。トピックには、現在のビューまたはダイアログの特徴や機能が記載されています。そのトピックから関連する手順に素早く移動できます。

次の図に、NetWitness Platformツールバーのオンライン ヘルプ アイコンの例を示します。



RSA Linkでのドキュメントの検索

RSA NetWitness® Platformドキュメントは、RSAのサポート ポータルおよびコミュニティである、RSA Linkに公開されています。RSA Linkでは、すべてのRSAリソースが1つの場所に集められています。これには、アドバイザリ、製品ドキュメント、ナレッジベースの記事、ダウンロード、トレーニングが含まれています。*RSA Linkのガイド ツアー*を表示するには、https://community.rsa.com/videos/21554を参照してください。

NetWitness Platformドキュメントの場所

NetWitness Platform Logs and Networksのドキュメントは、次のリンクにあります。
https://community.rsa.com/docs/DOC-40370

NetWitness Platform Logs and Networksのドキュメントに移動するには、次の操作を行います。

1. RSA Linkのホームページ(https://community.rsa.com) で、[**RSA NETWITNESS PLATFORM**]をクリックします。
2. RSA NetWitness Platformのページで、[**ドキュメント**]をクリックし、[**RSA NETWITNESS LOGS AND NETWORK**]を選択します。

NetWitness Endpoint 4.xのドキュメントに移動するには、次の操作を行います。

1. RSA Linkのホームページ(https://community.rsa.com) で、[**RSA NETWITNESS PLATFORM**]をクリックします。
2. RSA NetWitness Platformのページで、[**ドキュメント**]をクリックし、[**RSA NETWITNESS ENDPOINT**]を選択します。

RSAコンテンツの場所

RSAコンテンツは次のリンクにあります。https://community.rsa.com/community/products/netwitness/rsa-content

RSAコンテンツに移動するには、次の操作を行います。

1. RSA Linkのホームページ(https://community.rsa.com) で、[**RSA NETWITNESS PLATFORM**]をクリックします。
2. RSA NetWitness Platformのページで、[**ドキュメント**]をクリックし、[**その他のリソース**]＞[**RSA Liveコンテンツ**]を選択します。

RSAがサポートするイベント ソースの場所

RSAがサポートするイベント ソースの一覧は、次のリンクにあります。
https://community.rsa.com/community/products/netwitness/parser-network/event-sources

RSAがサポートするイベント ソースの一覧に移動するには、次の操作を行います。

1. RSA Linkのホームページ(https://community.rsa.com) で、[**RSA NETWITNESS PLATFORM**]をクリックします。
2. RSA NetWitness Platformのページで、[**ドキュメント**]をクリックし、[**その他のリソース**]＞[**イベント ソースの構成**]を選択します。

ハードウェア構成ガイドの場所

ハードウェア構成ガイドは、次のリンクにあります。
https://community.rsa.com/community/products/netwitness/hardware-setup-guides

1. RSA Linkのホームページ(https://community.rsa.com) で、[**RSA NETWITNESS PLATFORM**]をクリックします。
2. RSA NetWitness Platformのページで、[**ドキュメント**]をクリックし、[**その他のリソース**]＞[**ハードウェア設定ガイド**]を選択します。

NetWitness Navigatorを使用したドキュメントの検索

NetWitness Navigatorツールを使用して、RSA Link内の目的のRSA NetWitness Platformドキュメントを検索することができます。

1. RSA Linkのホームページ(https://community.rsa.com) で、[**RSA NETWITNESS PLATFORM**]をクリックします。
2. PRODUCT RESOURCES(ページの右側) の下にある、[**RSA NetWitness Navigator**]をクリックします。
3. 使用可能なオプションから目的の検索条件を選択します。ドキュメントを検索するときは、[Content Type]で[**User Documentation**]を選択する必要があります。また、[User Documentation]の場合は[Cost]オプションが無視されます。
4. [**VIEW RESULTS**]をクリックすると、一致するドキュメントのリストが表示されます。
5. [**RESET OPTIONS**]をクリックすると、前の検索オプションがクリアされます。

コンテンツの更新のフォロー

ページまたはドキュメントをフォローして、変更の通知を受け取ることができます。

1. RSA Linkにログインします。
2. ページまたはドキュメントに移動し、右上にある[**Follow**]または[**Actions**]＞[**Follow**]を選択します。

RSAへのフィードバックの送信

お客様からのフィードバックは当社にとって非常に重要であり、お客様により優れたエクスペリエンスを提供するために役立ちます。sahelpfeedback@rsa.comまでご意見をお寄せください。

NetWitness Platformスタート ガイドの参考情報

次のセクションには、NetWitness Platformスタート ガイドに関連するユーザ インタフェースの参考情報が含まれています。

- ユーザ環境設定
- [通知]パネルと通知トレイ
- [ジョブ]パネルとジョブ トレイ

ユーザ環境設定

ご使用の環境および作業に最適になるようRSA NetWitness® Platformを調整するには、自身のグローバル アプリケーション環境設定を設定することができます。このページでは、次の操作を実行できます。

- アプリケーションの表示言語の変更
- アプリケーションのタイム ゾーンの設定
- 日付と時刻の形式の設定
- NetWitness Platformのデフォルトの開始ビューの選択
- デフォルトの[調査]ビューの選択
- アプリケーションの明暗のテーマの選択
- パスワードの変更
- 通知の有効化
- コンテキスト メニューの有効化
- 調査の環境設定の変更：詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

グローバル環境設定オプションは、[対応]ビューと、調査、監視、構成、管理などのその他のビューのどちらからアクセスするかによって異なります。メイン メニュー バーから、2種類のグローバル ユーザ環境設定ダイアログにアクセス可能です。

- [**ユーザ環境設定**]ダイアログ：[対応]ビューと一部の[調査]ビュー([イベント分析]、[ホスト]、[ファイル])からアクセスできます。
- [**環境設定**]ダイアログ：他のほとんどのビューからアクセスできます。

実行したいことは何ですか?

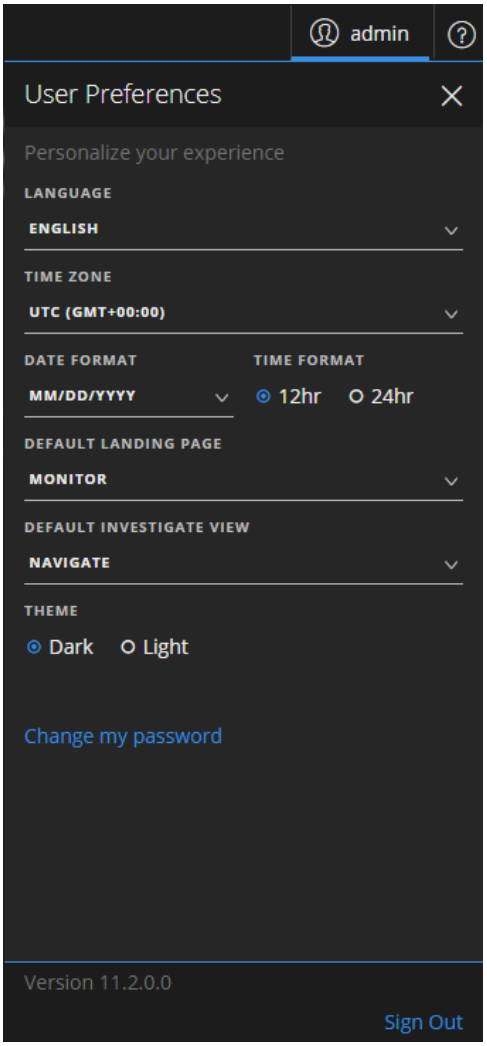
ロール	実行したいこと	手順
すべて	パスワードの変更	パスワードの変更
すべて	デフォルト ホーム ページの選択	SOCロールに応じたデフォルト ビューの設定
すべて	ユーザの環境設定	ユーザ環境設定

関連トピック

- NetWitness Platform基本ナビゲーション

ユーザ環境設定([対応]ビューおよび一部の[調査]ビュー)

ユーザ環境設定にアクセスするには、をクリックします。
[ユーザ環境設定]ダイアログに、現在の環境設定とNetWitness Platformバージョンが表示されます。



次の表では、[ユーザ環境設定]ダイアログからアクセスできるグローバルなアプリケーション環境設定のオプションについて説明します。

オプション	説明
言語	(このオプションはNetWitness Platform 11.2以降に適用されます) NetWitness Platform全体での使用言語を設定します。デフォルトの言語は、英語(米国)に設定されています。
タイムゾーン	NetWitness Platformで使用するタイムゾーンを設定します。
日付形式	月(MM)、日(DD)、年(YYYY)の表示順序の形式を設定します。たとえば、MM/DD/YYYYの形式では日付は05/11/2017と表示されます。

オプション	説明
時間形式	12時間制または24時間制を選択します。たとえば、12時間制の2:00 PMは、24時間制で14:00です。
デフォルト ホーム ページ	NetWitness Platformにログインしたときのデフォルト ビューを選択することができます。ユーザのロールに応じて、対応、調査、監視、構成、管理から選択できます。たとえば、[対応]を選択すると、インシデント対応者向けのセクションに直接移動できます。 この選択は、アプリケーション全体のデフォルト ビューを設定します。
デフォルトの[調査]ビュー	(このオプションはNetWitness Platform11.1以降に適用されます。) [調査]ビューのデフォルトのホーム ページを選択します。デフォルトの[調査]ビューとして、[ナビゲート]、[イベント]、[イベント分析]、[ホスト]、[ファイル]、[ユーザ]、[Malware Analysis]を選択できます。たとえば、デフォルトの[調査]ビューとして[イベント]を選択すると、[イベント]ページに直接移動して、サービスに対して生成されたイベントが表示されるようにできます。
テーマ	(このオプションはNetWitness Platform 11.1以降にのみ適用されます) アプリケーションで表示される[対応]ビューと一部の[調査]ビューの外観を変更します。明暗のテーマを選択できます。 • **ダーク**: 暗い色のテーマです。暗い表示、またはコントラストが小さい方がよい場合に最適です。 • **ライト**: 明るい色のテーマです。明るい表示、コントラストが大きい方がよい場合、またはプロジェクターでアプリケーションを他の人に見せる場合に最適です。一部のビューは、テーマの変更の影響を受けないため、明るい色のテーマを選択した方が、まとまりのある画面として表示されます。 この選択で変更されるのは、自分の環境でのNetWitness Platformの外観です。他のユーザの環境では変更されません。
パスワードの変更	[環境設定]ダイアログが表示され、パスワードを変更できます。
バージョン	NetWitness Platformバージョンが表示されます。
サイン アウト	NetWitness Platformからログアウトできます。

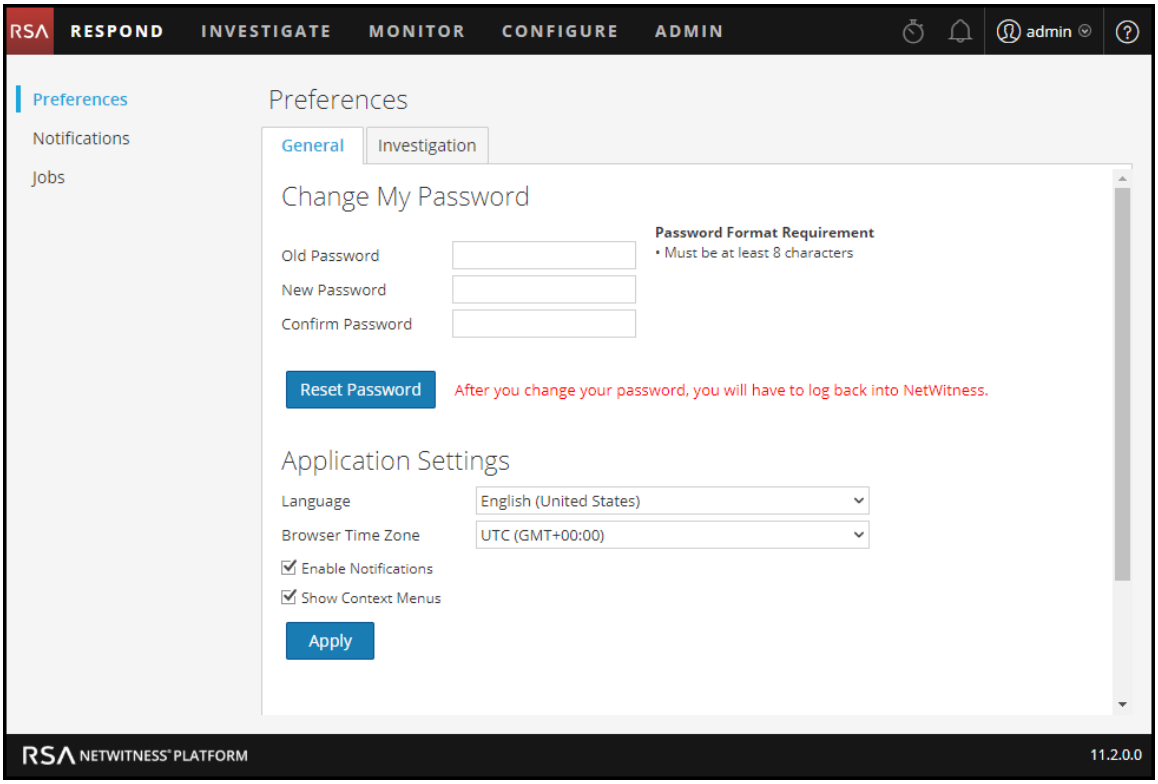
選択はすぐに有効になります。

環境設定

グローバル ユーザ環境設定にアクセスするには、次のいずれかの操作を行います。

- 調査、監視、構成、管理などのほとんどのビューでは、  > [**プロファイル**]に移動します。
- [対応]ビューと一部の[調査]ビュー(イベント分析、ホスト、ファイル、ユーザ)では、  を選択し、[ユーザ環境設定]ダイアログで[**パスワードの変更**]をクリックします。

[環境設定]ダイアログに、現在の環境設定が表示されます。



次の表では、[環境設定]ダイアログからアクセスできるグローバルなアプリケーション環境設定のオプションについて説明します。

パスワードの変更

このセクションでは、パスワードを変更することができます。パスワードの最小長、大文字、小文字、数字、非ラテン アルファベット文字、特殊文字の最小数などの、NetWitness Platformのパスワード強度の要件は管理者が定義します。これらの要件は、パスワードを変更するときに表示されます。

次の表では、[パスワードの変更]セクションのオプションについて説明します。

オプション	説明
古いパスワード	NetWitness Platformにログインするために使用したパスワードを入力します。
新しいパスワード	次回以降のログインに使用する新しいパスワードを入力します。

オプション	説明
パスワードの確認	新しいパスワードを再入力します。
パスワードのリセット	ユーザ プロファイルに新しいパスワードが設定されます。変更を有効にするため、NetWitness Platformからログアウトします。新しいパスワードは、次回のNetWitness Platformへのログイン時に有効になります。パスワードの変更は、システムへのログインと、アカウントが追加されているすべてのNetWitness Platformサービスに適用されます。

パスワードを変更した場合、変更を有効にするため、NetWitness Platformからログアウトします。新しいパスワードは、次回のNetWitness Platformへのログイン時に有効になります。

アプリケーション設定

次の表で、[アプリケーション設定]セクションのオプションについて説明します。

オプション	説明
言語	(このオプションはNetWitness Platform 11.2以降に適用されます) NetWitness Platform全体での使用言語を設定します。デフォルトの言語は、英語(米国)に設定されています。
ブラウザのタイム ゾーン	NetWitness Platformで使用するタイム ゾーンを設定します。タイムゾーンの環境設定がツールバーに表示されます。
通知の有効化	使用中のユーザ アカウントに対する通知の有効化と無効化を切り替えます。デフォルトでは、新しいユーザ アカウントが作成されると、NetWitness Platformシステム通知が有効化されます。
コンテキスト メニューの有効化	使用中のユーザ アカウントに対するコンテキスト メニューの有効化と無効化を切り替えます。デフォルトでは、新しいユーザ アカウントが作成されると、コンテキスト メニューが有効化されます。コンテキスト メニューは、ユーザがビューの特定の箇所を右クリックすると表示される追加の機能メニューです。
適用	環境設定を更新し、変更をすぐに適用します。

[通知]パネルと通知トレイ

RSA NetWitness® Platformでは、特定のアクションや状態について、ユーザに知らせるためのシステム通知が用意されています。

- ホストのアップグレードが完了した。
- DecoderへのParserの適用が完了した。
- サービスが停止した(特定のタイプの致命的なログ)。
- Visualizationが完了した。
- レポートが完了した。
- 新しいバージョンのソフトウェアが利用可能。

NetWitness Platformのユーザインタフェースでは、作業領域を離れることなく最新のシステム通知を確認することができます。NetWitness Platformツールバーから通知のクイックビューを開くことができます。

通知トレイはいつでも参照が可能で、新しい通知を受け取ると、通知アイコンにフラグ()が表示されます。

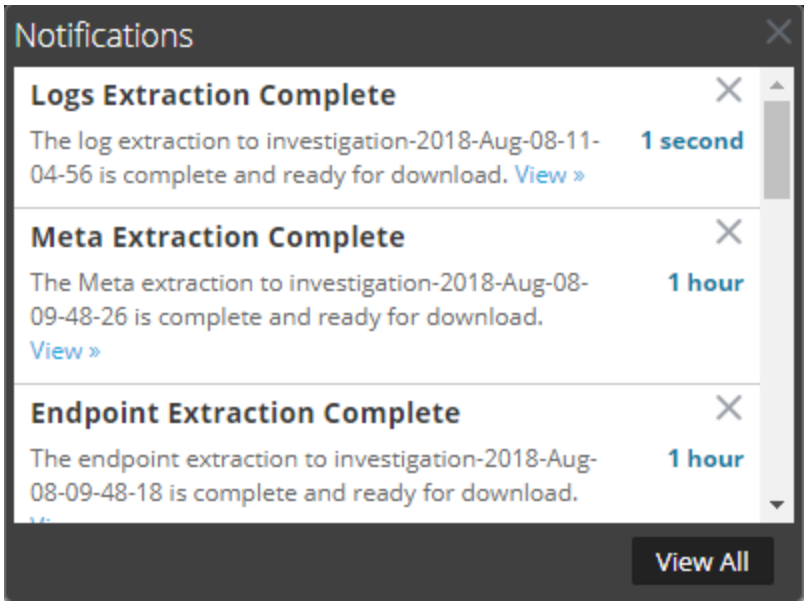
通知トレイでシステム通知を表示する場合、最近のシステム通知のみが表示されます。[すべて表示]オプションを選択すると、ユーザプロファイルおよび通知トレイからすべての通知にアクセスできます。通知の表示に関する操作手順については、[通知の表示と削除]セクションを参照してください。

実行したいことは何ですか?

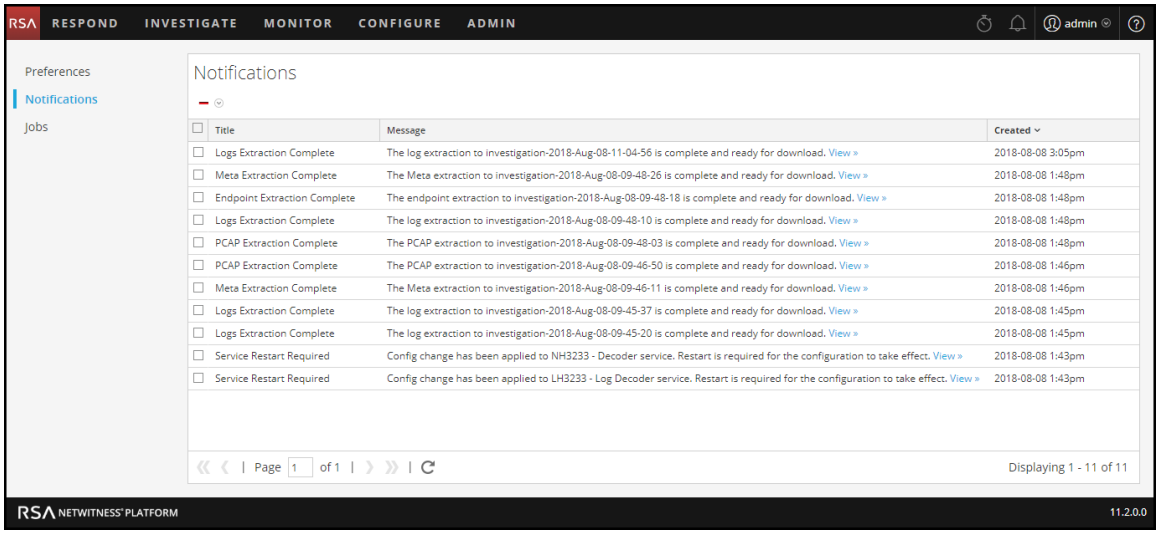
ロール	実行したいこと	手順
すべて	すべての通知の表示	通知の表示と削除
すべて	通知の削除	通知の表示と削除

[通知]パネルにアクセスするには、次のいずれかを実行します。

- をクリックして通知トレイを開き、通知トレイで[**すべて表示**]をクリックします。



- NetWitness Platformブラウザ ウィンドウの右上隅にある[ ]>[**プロファイル**]を選択し、[環境設定]ダイアログのオプション パネルで[**通知**]を選択します。
  [通知]パネルが表示されます。



通知トレイには、最近の通知が表示されます。これには、[通知]パネルの情報のサブセットが含まれています。[通知]パネルには、すべての通知が表示されます。次の表で、[通知]パネルと通知トレイの機能を説明します。

機能	説明
	([通知]パネルのみ)ドロップダウン メニューが表示され、[通知]パネルと通知トレイから、選択した通知 またはすべての通知を削除できます。

機能	説明
タイトル	通知のタイトル(「**ログの抽出が完了しました**」など)。
メッセージ	メッセージ全体(「**[調査]へのログの抽出が完了し、ダウンロードの準備ができました。**」など)。
表示	一部のメッセージには、アクション可能な場所を示す[**表示**]リンクが含まれています。たとえば、ダウンロードするファイルがある場合、このリンクをクリックすると[ジョブ]パネルが開き、ファイルをダウンロードできます。
作成日時	通知が作成された日時。 通知トレイには、通知が作成されてからの時間または日数が表示されます。
すべて表示	(通知トレイのみ)[通知]パネルが開き、すべての通知が一覧表示されます。

[ジョブ]パネルとジョブ トレイ

ジョブはさまざまなRSA NetWitness® Platformコンポーネントによって開始されます。たとえば、Live ServicesからCMS(コンテンツ管理システム)リソースをダウンロードし、NetWitness Investigateからログ、メタ、PCAPファイルを抽出します。

[管理]>[システム]ビューでは、管理者は[ジョブパネル]ですべてのNetWitness Platformジョブを管理できます。管理者以外のユーザは、[ユーザ プロファイル ジョブ]パネルで自分のジョブを表示できます。

また、NetWitness Platformのユーザ インタフェースでは、NetWitness Platformツールバーからジョブのクイック ビューを開くことができます。ジョブ ステータスが変更されると、[ジョブ]アイコン( ) にフラグが付けられ、実行中のジョブの数が示されます。すべてのジョブが完了すると、この数字は表示されなくなります。

[ジョブ]パネルでは、次のタスクを実行できます。

- ジョブの表示およびソート
- ジョブの一時停止または再開
- ジョブのキャンセル
- ジョブの削除
- ジョブ結果のダウンロード

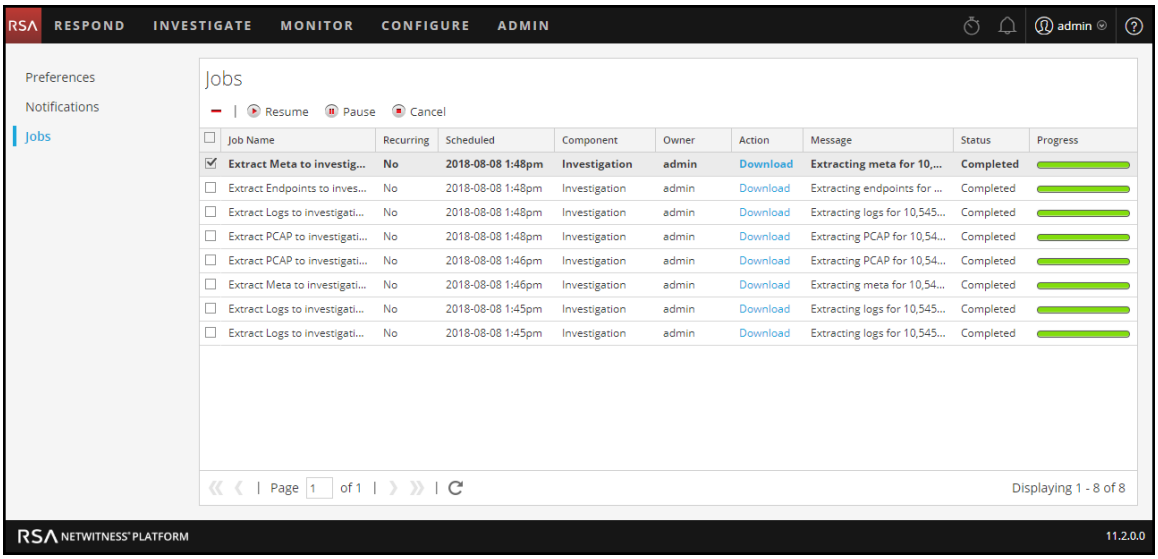
ジョブ パネルの構造はすべてのビューで同じです。

実行したいことは何ですか?

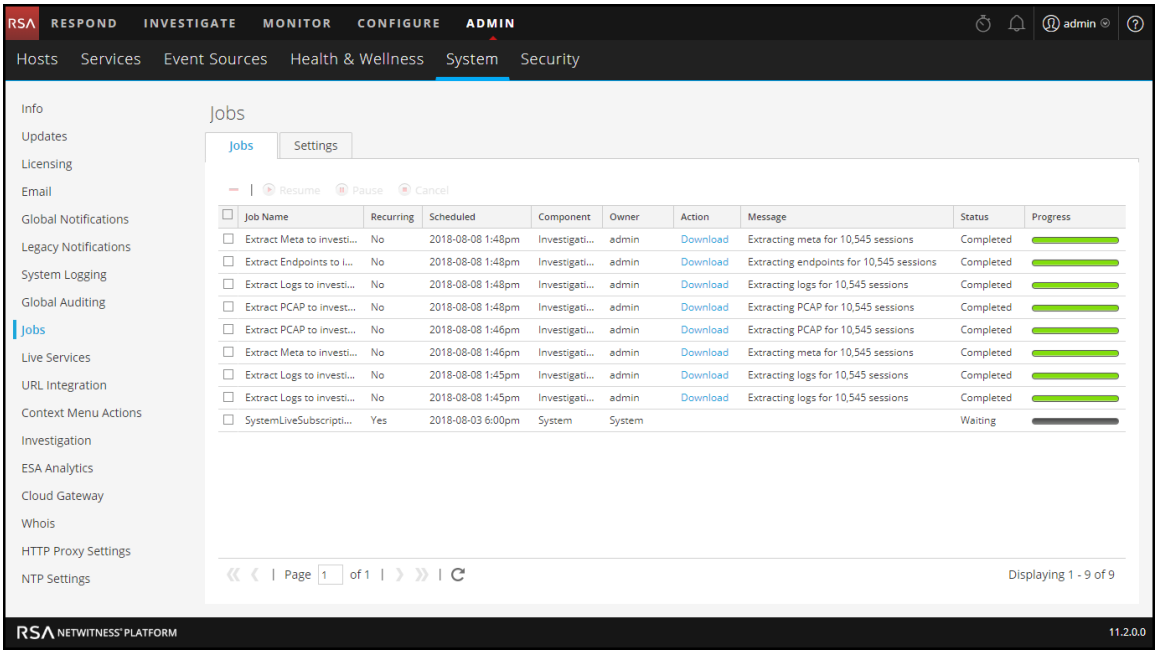
ロール	実行したいこと	手順
すべて	スケジュール設定されたジョブの一時停止と再開	ジョブの管理
すべて	ジョブのキャンセルまたは削除	ジョブの管理
	ジョブ結果のダウンロード	ジョブの管理

[ジョブ]パネルにアクセスするには、次のいずれかを実行します。

- NetWitness Platformブラウザ ウィンドウの右上隅の[ ]>[**プロファイル**]を選択し、[環境設定]ダイアログのオプション パネルで[**ジョブ**]を選択します。
  [ジョブ]パネルが表示されます。特定のユーザのジョブが表示されます。

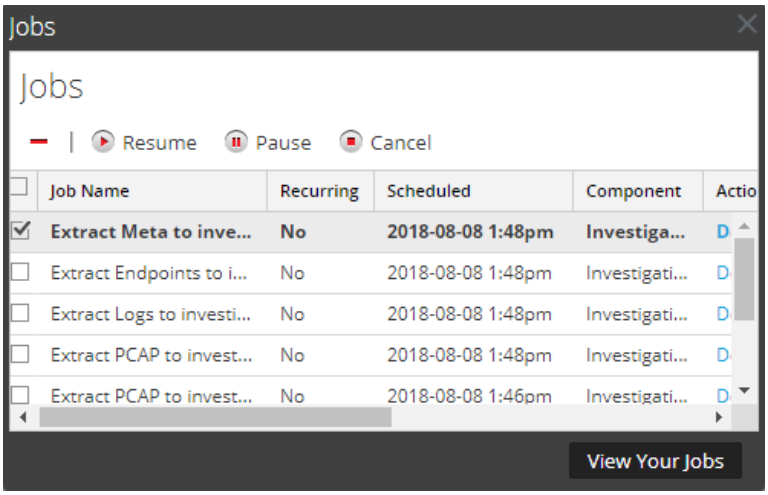


- **[管理]＞[システム]**に移動して、オプション パネルで**[ジョブ]**を選択します。
[管理システム]ビューの[ジョブ]パネルが表示されます。すべてのユーザのジョブが表示されます。



[ジョブ]パネルでは、ジョブの情報が一覧で表示されます。列には、ジョブ進捗バー、ジョブ名、ジョブが定期実行されるかどうかの表示、ジョブを制御するNetWitness Platformコンポーネント、ジョブのオーナー、ステータス、関連メッセージ、ダウンロード ボタン(ジョブのパケット収集ファイルまたはペイロード ファイルのダウンロード) が示されます。

ジョブ トレイを表示するには、[**ジョブ**]アイコン  をクリックします。



ジョブ トレイには、[**ジョブ**] パネルに表示される列のサブセットを使用して、自分が管理するすべてのジョブ(定期実行ジョブと定期実行ではないジョブ) が一覧表示されます。ジョブ トレイと、[ユーザ プロファイル ジョブ] パネルの内容は同一です。[管理システム]ビューでは、すべてのユーザのすべてのNetWitness Platformジョブの情報が[ジョブ] パネルに一覧表示されます。

次の表で、[ジョブ] パネルのオプションについて説明します。

オプション	説明
Resume	[再開]オプションは、一時停止されていた定期実行ジョブにのみ適用されます。一時停止されていたジョブを再開する場合、ジョブの次の回の実行は、スケジュールどおりに実行されます。
Pause	[一時停止]オプションは、定期実行ジョブにのみ適用されます。実行中の定期実行ジョブを一時停止しても、その回の実行には影響しません。(ジョブが一時停止中のままである場合) 次の回の実行は、スキップされます。
Cancel	定期実行ジョブまたは定期実行ではないジョブをキャンセルします。ジョブは、実行中にキャンセルできます。定期実行ジョブをキャンセルすると、ジョブのその回の実行がキャンセルされます。スケジュールされている次の回の実行は、正常に実行されます。
−	[ジョブ] パネルから定期実行ジョブまたは定期実行ではないジョブを削除します。ジョブを削除すると、ジョブは[ジョブ] パネルから直ちに削除されます。確認ダイアログは表示されません。定期実行ジョブを削除すると、スケジュールされている以降のジョブの実行もすべて削除されます。

次の表でジョブトレイと[ジョブ]パネルの列について説明します。

機能	説明
選択ボックス	1つまたは複数のジョブを選択できます。
ジョブ名	ジョブの名前を表示します。「**Extract Files**」、「**Upgrade Service**」など。
定期実行	ジョブが定期実行ジョブであるか、定期実行ではないジョブであるかを示します。[**はい**]は定期実行ジョブ、[**いいえ**]は定期実行ではないジョブです。
スケジュール設定	ジョブがスケジュールされた日時を示します。
コンポーネント	ジョブを生成したコンポーネントを示します(**調査**、**管理**など)。
オーナー	ジョブのオーナーを示します。ジョブのオーナーはデフォルトでは**ジョブトレイ**には表示されません。ジョブトレイには、現在のユーザのジョブのみが表示されるからです。この列を追加することができます。
アクション	別のビューでジョブを表示するか、ジョブで出力されたファイルをローカルシステム上のデフォルトの**ダウンロード** ディレクトリにダウンロードします。正常に完了したジョブの場合のみ、[**アクション**]列に[**表示**]リンクが表示されます。ファイルを出力するジョブの場合のみ、[**アクション**]列に[**ダウンロード**]リンクが表示されます。
メッセージ	ジョブに関する補足情報を表示します。「**Extracting files**」、「**No sessions found**」など。
ステータス	ジョブのステータスを示します。一般的なステータスの値には、**一時停止**、**実行中**、**キャンセル済み**、**失敗**、**完了**がありますが、その他のステータス値が表示されることもあります。
進行状況	ジョブの完了の割合を表示します。
自分のジョブを表示	(ジョブトレイのみ)[**ジョブ**]パネルにジョブが表示されます。