RSA NETWITNESS® SUITE

スタート ガイド

バージョン 11.0

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、EMC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、民事および刑事責任が課せられることがあります。

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、本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

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしています。予告なく変更される場合があります。

2月 2018

目次

NetWitness Suiteスタート ガイド

概要

RSA NetWitness Suite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) が脅威を迅速に特定し、優先度を設定し、対応を選別できるようにします。NetWitness Suiteは、既知の脅威だけでなく、これまで知られていなかった脅威を分離および改善するために役立ちます。パケットとログを洞察し、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 Suiteはこれまで以上に強力になりました。しかし、疑わしい脅威の特定と優先度付けのプロセスが自動化されるため、Tier 1のアナリストの使いやすさは向上しています。NetWitness Suite 10.6のユーザは、引き続き使用可能な[調査(Investigate)]ビューを使用して、これまでと同じ方法で脅威を見つけ出すことができます。

アーキテクチャ

RSA NetWitness Suite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 Suiteを使用して、パケット データとログ データの2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、ネットワークトラフィックまたはログ 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 Suite **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サーバ**。NetWitnessサーバは、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 Suiteのキャパシティ(外部ストレージ)は、直接接続(DAC)またはSAN(ストレージ エリア ネットワーク)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、およびデータ保存のそれぞれのニーズに対応します。

NetWitness Suiteの導入は非常に柔軟です。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 Suite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。NetWitness Suite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サーバ。
- 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。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 Suiteは、パケット データとログ データの2種類の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 ファイルはSFTPを介してログを収集します。 • 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 Suiteの他のコンポーネントで集計されます。 • データ収集とパースのプロセスは、絶えず進化するオープンなフレームワークで構成されています。
Concentrator	• NetWitnessの収集データにインデックスと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。
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 Suite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。

システム コンポーネント	説明
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

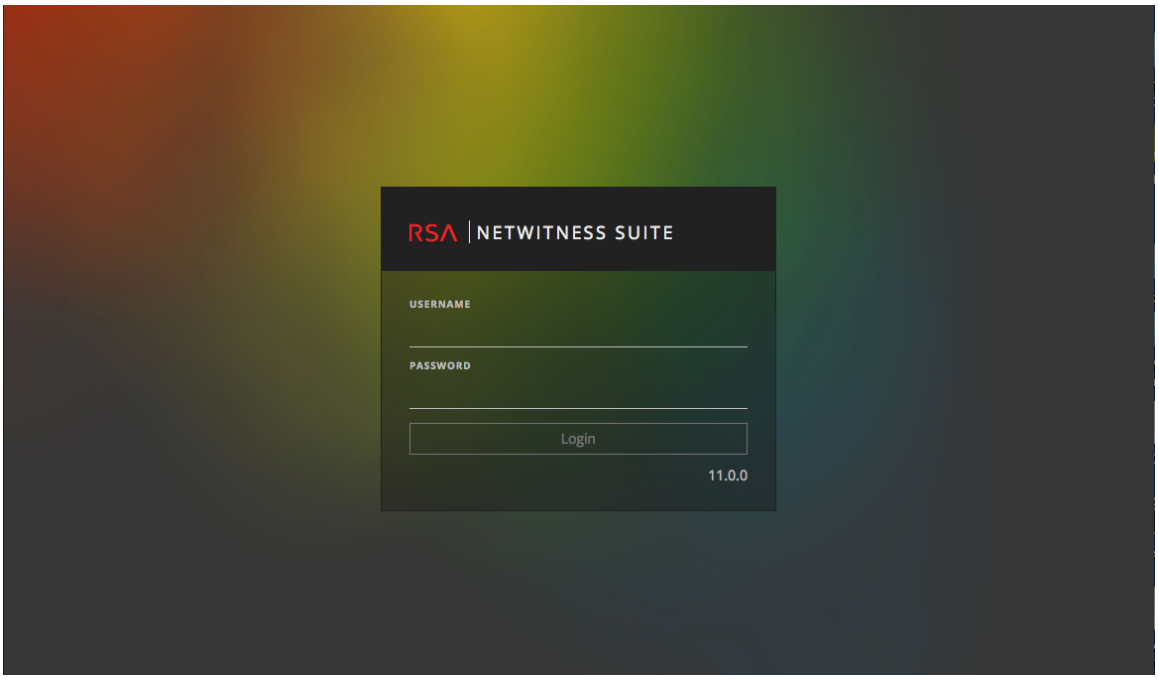
NetWitness Suiteのコア サービスは、データの取得と解析、メタデータの生成、生成されたメタデータとrawデータの集計を行います。コア サービスには、Decoder、Log Decoder、Concentrator、Brokerがあります。ダウンストリーム システムは、コア サービスに格納されているデータを使用して分析を行います。したがって、ダウンストリーム サービスの動作はコア サービスに依存します。ダウンストリーム システムは、Archiver、ESA、Malware Analysis、Investigate、Reportingです。

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、ログとパケット 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 Suiteへのログイン

NetWitness Suite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 Suiteのローカル アカウントで、NetWitness Suite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 Suiteの外部で認証を行い、NetWitness Suite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 Suite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サーバのホスト名またはIPアドレスです。



   ログイン スクリーンが表示されます。

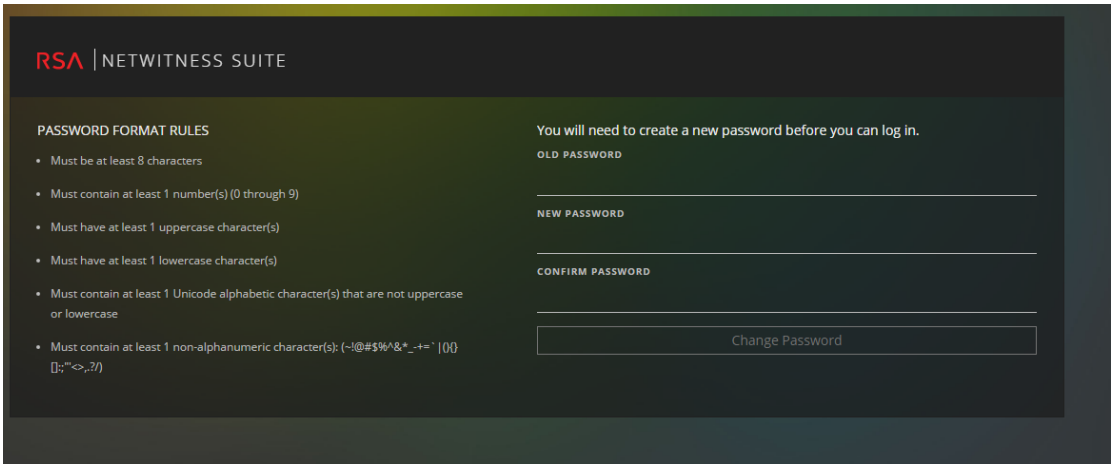
2. ユーザ名とパスワードを入力し、[**ログイン**]をクリックします。
   ログインに成功すると、ユーザ環境設定で指定されたランディング ページが表示されます。

ロックアウトされている場合:

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:

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 Suite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 Suiteからのログオフ

[対応]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。

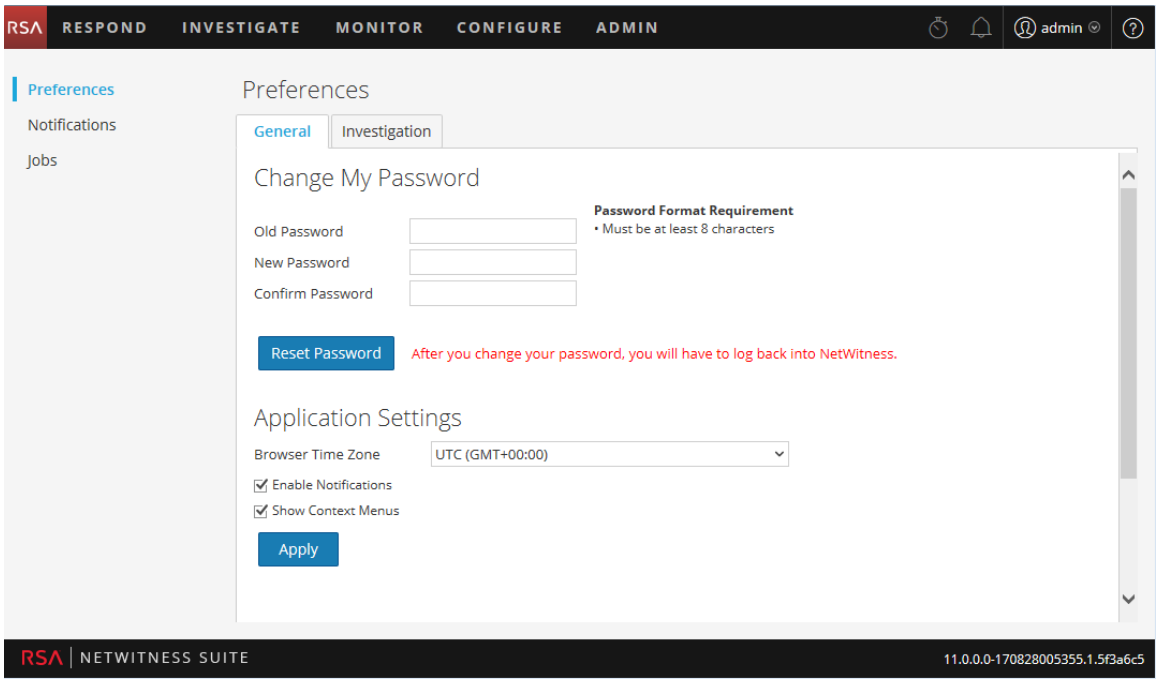
パスワードの変更手順

ユーザ環境設定でいつでもNetWitness Suite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 Suiteパスワードに適切なパスワード強度の要件を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:コア サービスが信頼関係接続を使用する場合、パスワードを入力しないため、コア サービス アカウントの更新は必要ありません。

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. 次のいずれかを実行します。
   - 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**]を選択します。
   - [対応]ビューでは、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。



2. [**パスワードの変更**]セクションで、NetWitness Suite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 Suiteからログアウトします。新しいパスワードは、次回のNetWitness Suiteへのログイン時に有効になります。

自分のロールの特定

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、NetWitness Suite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

プライバシーに関する機微情報の監視と保護

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

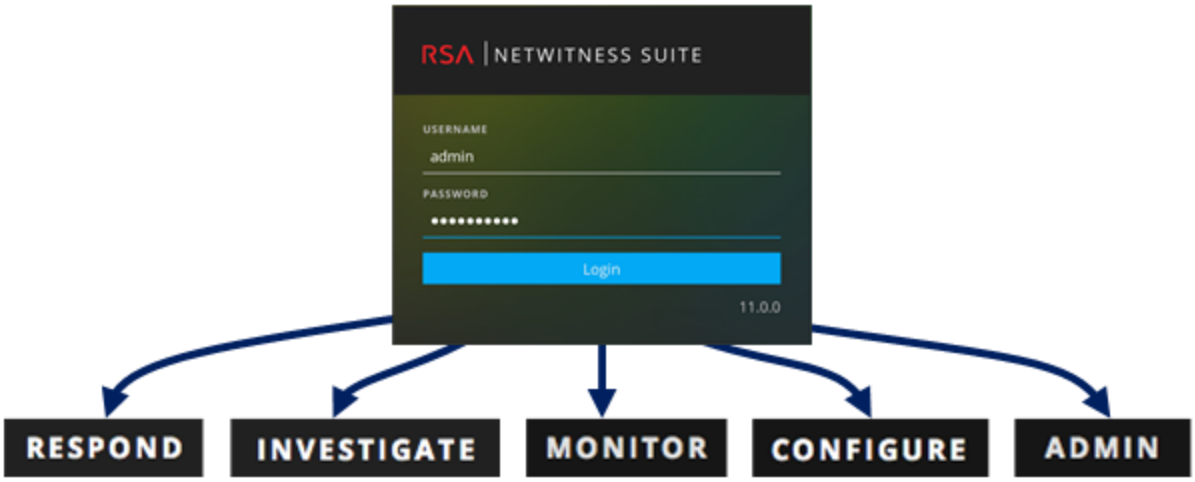
System Administrator

- 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 Suiteの基本ナビゲーション

NetWitness Suite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) のロールに基づく、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、優先順位付けされたインシデントのリストを表示して優先順位に応じて対応することができる、インシデント対応者が使用します。これらのインシデントは、自動脅威検出のためのESAルール、NetWitness Endpoint、ESA Analyticsモジュールなどのソースから発生します。NetWitness Suiteで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。
  レガシーの10.6のユーザには、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。[Respond]ビューのアラート リストがESA 10.6の[アラート]>[サマリ]ビューと置き換わりました。
- **調査** : このビューは主に、NetWitness Suiteのメタデータ、イベント分析、イベント再構成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 イベントの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 Suiteは、デフォルトではこのビューを開きます。
  レガシーの10.6のユーザにとっては、これはダッシュボード ビューです。
- **構成** : このビューは、データ ソースと入力をNetWitness Suiteに構成する、脅威インテリジェンス(コンテンツ) 担当者が使用します。脅威インテリジェンス担当者は、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。
レガシーの10.6のユーザにとっては、このビューは前のバージョンの[Live]、[インシデント]＞[構成]、[アラート]＞[構成]を含んでいます。

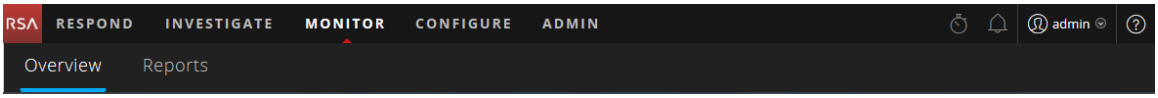
- **管理**：このビューは、全体のアプリケーションをセットアップして管理する、システム管理者が使用します。
レガシーの10.6のユーザにとっては、これは[構成]ビューに追加されたセクションを除いた[管理者]ビューです。

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。適切な権限がある場合は、すべてのブラウザ ウィンドウの上部にあるこれらのビューにいつでもアクセスできます。

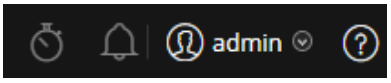
セカンダリ メニュー

一部のビューには、選択可能な追加のビューのセカンダリ メニューがあります。これは、完了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。

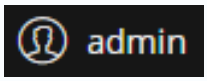
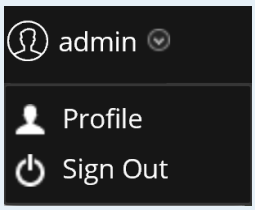


追加オプション

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あります。



次の表に、これらの共通のオプションの説明を示します。

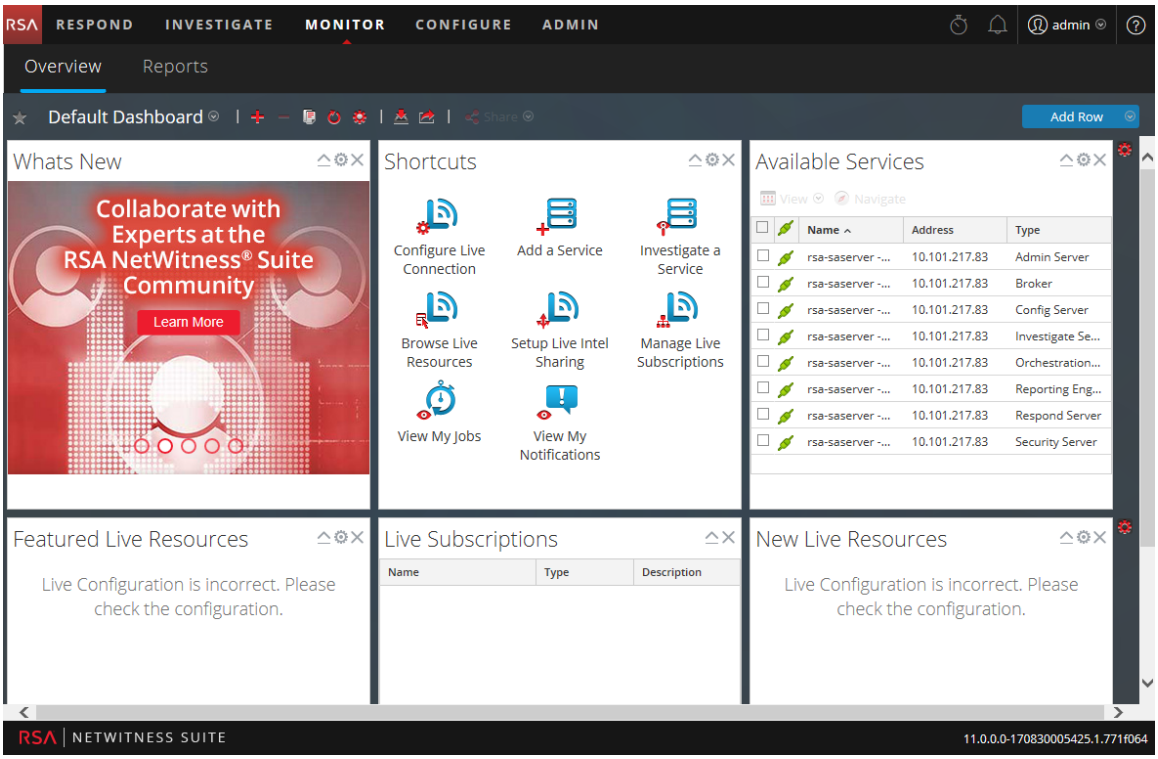
共通のオプション	名前	説明
	ジョブ	ジョブトレイのジョブを表示および管理するには、[調査]、[監視]、[構成]、[管理]ビューでこのアイコンをクリックします。ジョブとは、NetWitness Suiteアプリケーションで完了するまでに時間がかかる、オンデマンドのタスクまたはスケジュール設定されたタスクです。
	通知	このアイコンをクリックすると、アプリケーションからの通知が表示されます。
	ユーザ環境設定	このアイコンをクリックすると、使用可能なユーザ環境設定オプションが表示されます。ユーザ環境設定の管理と、NetWitness Suiteからのログアウトを行うことができます。
	ユーザプ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

メイン ビュー

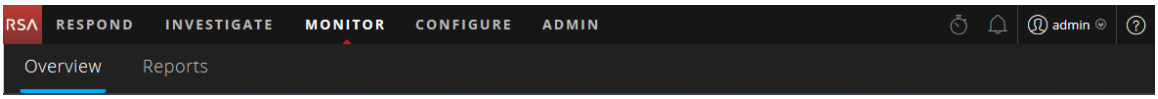
次のセクションでは、メイン ビューについて説明します。

監視

[監視]ビューは、クラシックのNetWitness Suiteダッシュボードです。監視には、使用可能な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
  - ID

- Investigation
- 運用：ファイル分析
- 運用：ログ
- 運用：ネットワーク
- 運用：プロトコル分析
- 概要
- RSA SecurID
- 脅威：探索
- 脅威：侵入
- 脅威：マルウェア インジケータ

レガシーの10.6のユーザにとっては、これはダッシュボード ビューでした。

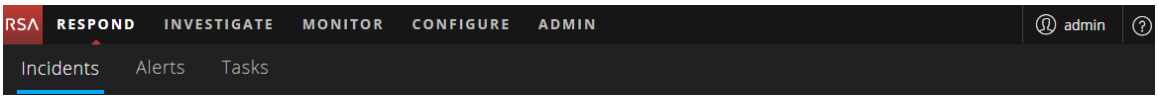
- **レポート**：[レポート]ビューでは、割り当てられた権限に従って、SOCロールに関連するレポートを表示および管理できます。

ここで行うことができること	パス	方法を確認する
ダッシュボードの選択	[監視]＞[概要]	「ダッシュボードのセットアップ」を参照。
ダッシュボードの作成	[監視]＞[概要]	「ダッシュボードのセットアップ」を参照。
ダッシュボードの管理	[監視]＞[概要]	「ダッシュボードのセットアップ」を参照。
レポートの表示	[監視]＞[レポート]＞[ビュー]	「*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]ビューでは、アナリストに重大度順のインシデントのキューが表示されます。キューからインシデントを取得すると、インシデントの調査に役立つ関連するサポート データを受け取ります。そのデータからインシデントの範囲を判断し、必要に応じてエスカレーションまたは修復することができます。

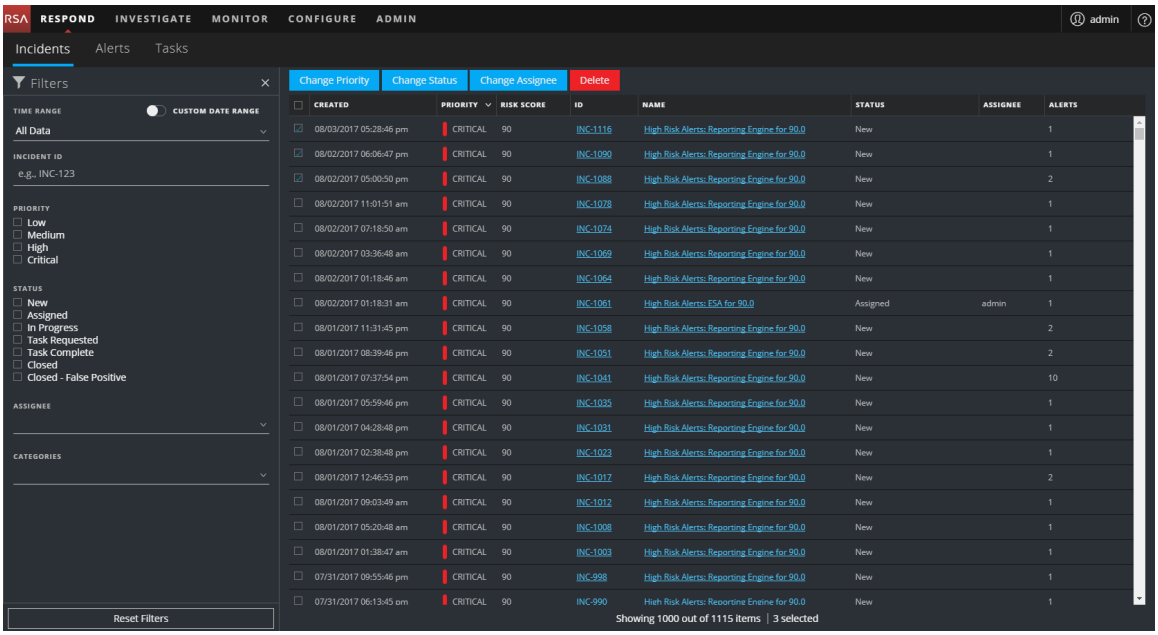
対応メニュー



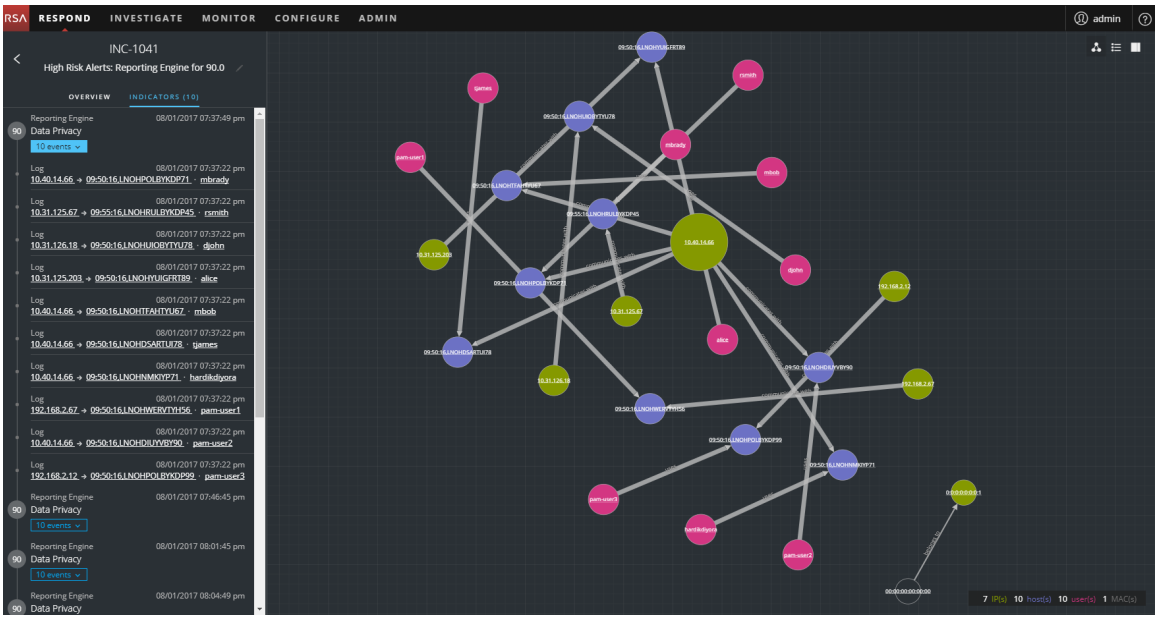
[対応]メニューには、次のオプションがあります。

- **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と基本情報のリストが含まれています。[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、1つの場所でNetWitness Suiteが受信したすべての脅威の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、タスクを作成して完了までトラックすることができます。

次の図は、[対応]ビュー:[インシデント リスト]ビューを示しています。

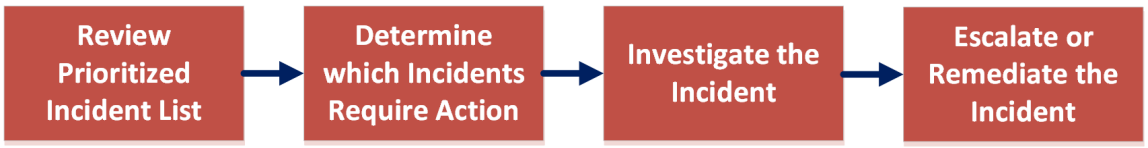


次の図は、[対応]ビュー: [インシデントの詳細]ビューの例を示しています。



ケース管理ツールとしてNetWitness Suite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。インシデント キューの上部に新しいインシデントが優先度順で表示され、対応中のインシデントが新しいインシデントよりも下に表示されます。

次の図は、[対応]ビューの概要レベルのワークフローを示しています。



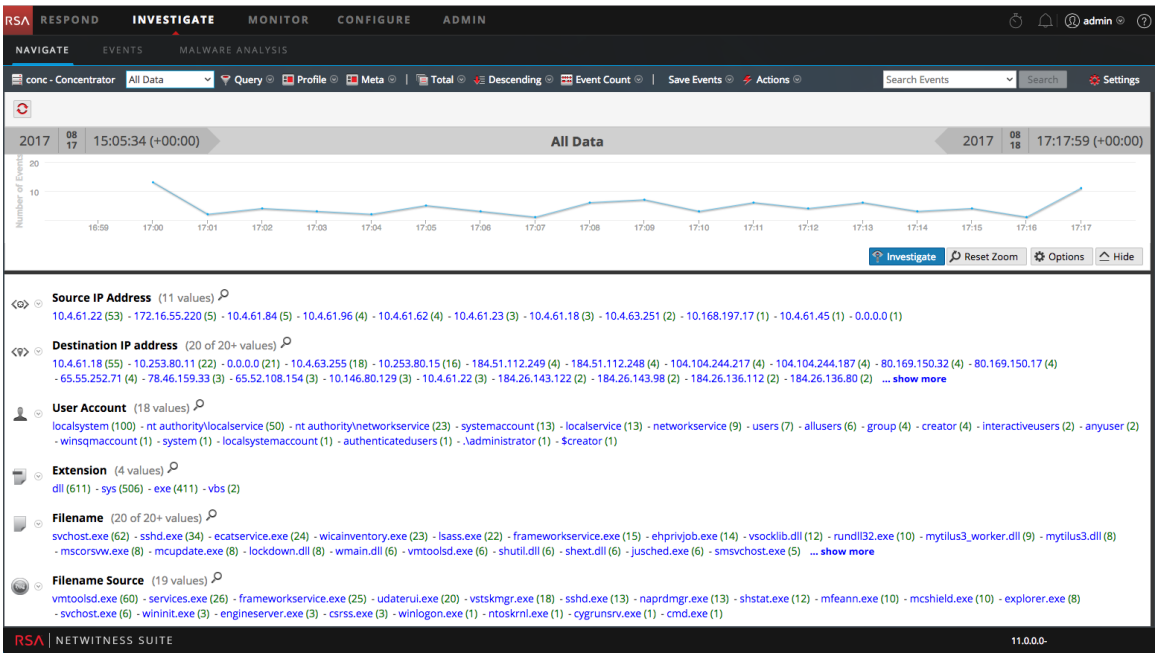
[対応]ビューでは、アナリストが優先順位付けされたインシデントのリストを確認して、どのインシデントにアクションが必要かを判断します。アナリストはインシデントをクリックして詳細をサポートすることでインシデントについて明確に把握し、インシデントをさらに調査することができます。その後、アナリストは脅威のエスカレーションまたは修復により、脅威への対応方法を判断できます。

ここで行うことができること	パス	方法を確認する
優先順位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*」を参照してください。

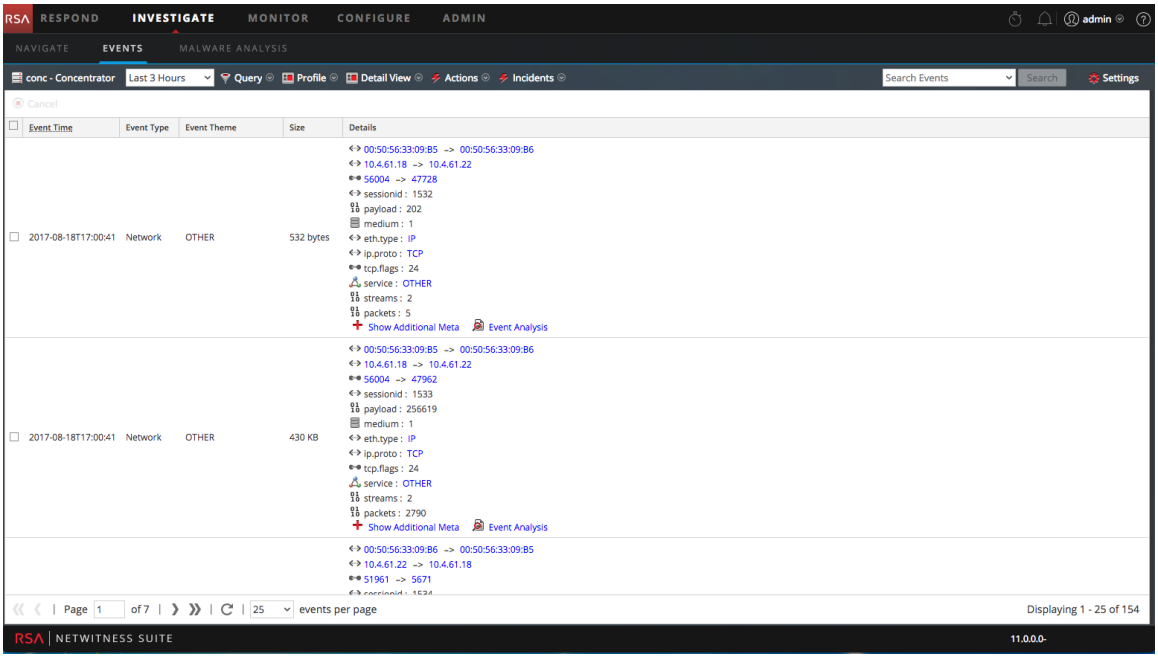
ここで行うことができること	パス	方法を確認する
アクションが必要なインシデントの判断 (インシデントの優先順位付け)	[対応]>[インシデント]([インシデントの詳細]ビュー)	「*NetWitness Respondユーザガイド*」を参照してください。
インシデントの調査	[対応]>[インシデント]([インシデントの詳細]ビュー)	「*NetWitness Respondユーザガイド*」を参照してください。([調査]ビューに移行することもできます。)
インシデントのエスカレーションまたは修正	[対応]>[インシデント]([インシデントの詳細]ビュー) および[対応]>[タスク]([タスクリスト]ビュー)	「*NetWitness Respondユーザガイド*」を参照してください。
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*」を参照してください。

調査

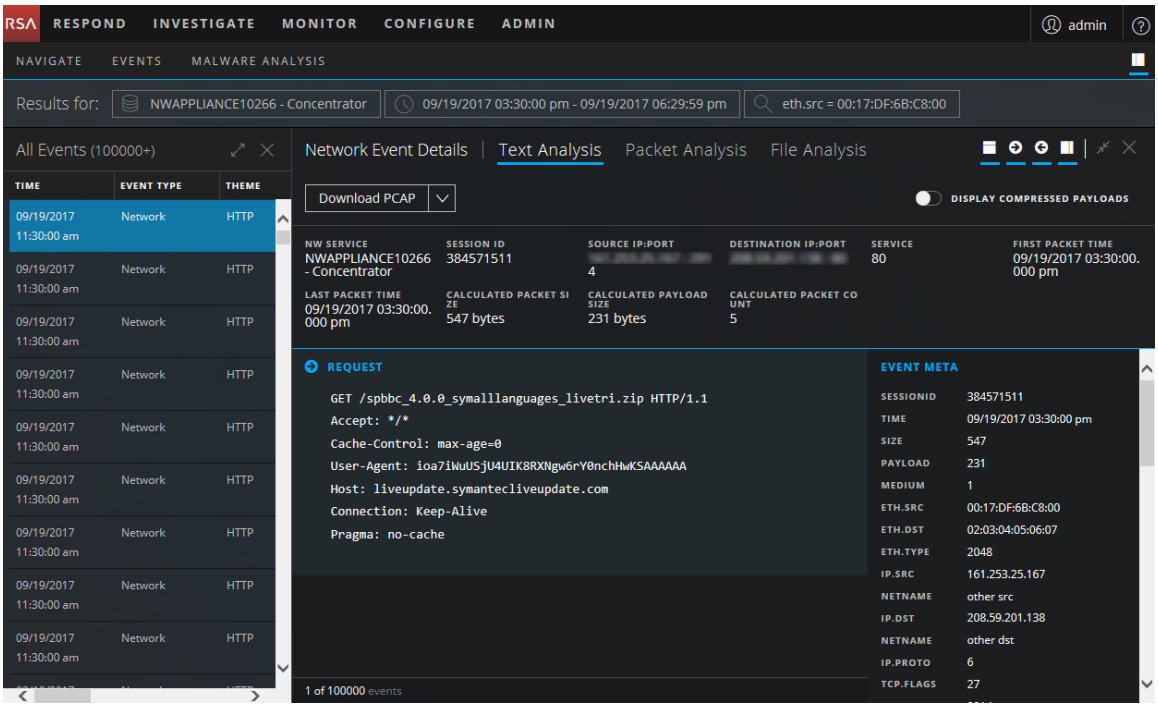
[調査]ビューでは、データセットに3つの異なるビューが表示され、アナリストはメタデータ、イベント、セキュリティ侵害の可能性のインジケータを表示できます。この図は、調査中のConcentrator上のすべてのデータを表示する、ビューの1つである[ナビゲート]ビューを示しています。



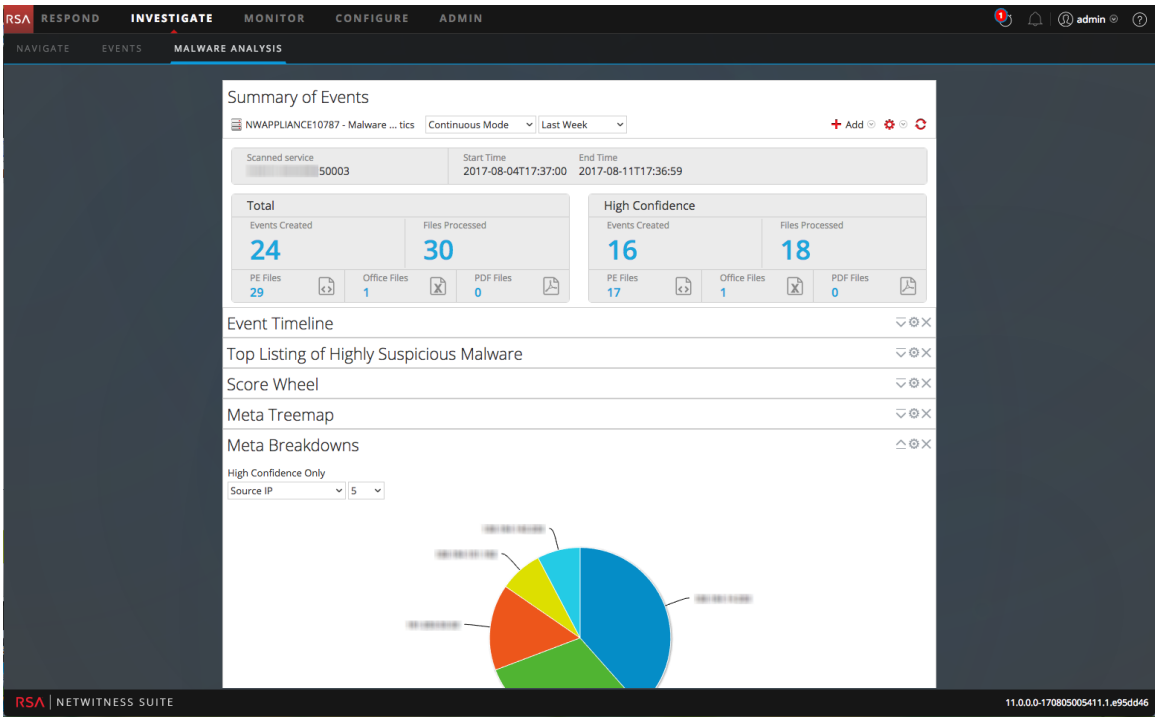
これは、[イベント]ビューの例です。



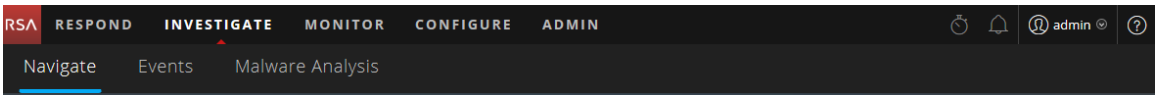
[イベント]ビューで特定のイベントの[**イベント分析**]リンクをクリックすると、[イベントの詳細]ビューが開きます。



これは、Malware Analysisの[イベントのサマリ]の例です。



[INVESTIGATE]メニュー

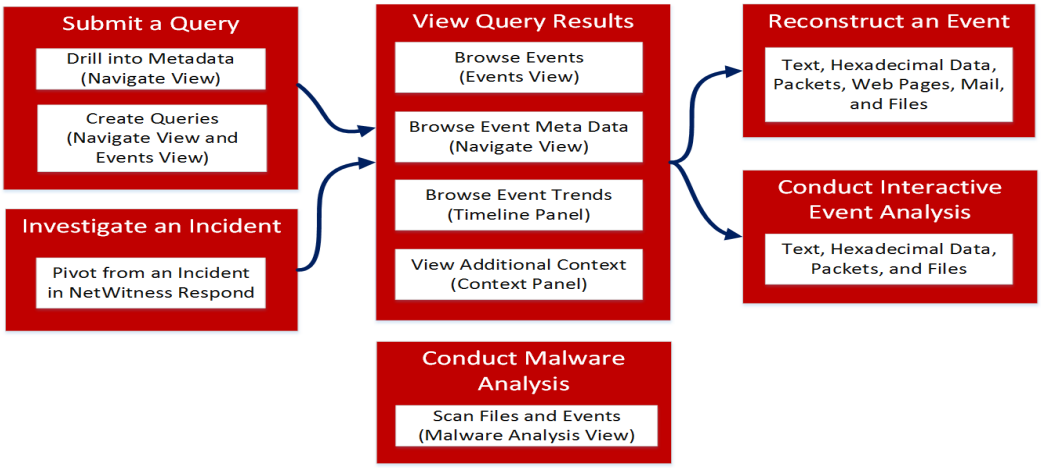


[調査]メニューには、次のオプションがあります。

- **ナビゲート**: [ナビゲート]ビューでは、メタデータの表示とタイムラインのビジュアル化が行われ、データのフィルタリングとクエリのためのツールバーが用意されています。アナリストはデータにドリルダウンすることや、[イベント]ビューで選択したイベントを開くこと、Context Hubサービスから追加のコンテキストを検索することができます。
- **[イベント]ビュー**: [イベント]ビューには、データセットとイベントのリストを絞り込むためのツールバーが用意されています。アナリストは、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。関心のあるイベントが見つかったときは、イベントの再構築を安全に表示することや、イベント分析を実行することができます。
- **Malware Analysis**: [Malware Analysis]ビューでは、アナリストが特定のタイプのファイル オブジェクトを分析して、悪意のあるファイルである可能性を評価できます。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、マルウェア解析を行う際に、収集された大量のファイルに優先順位を付け、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。

Investigateで作業するために、アナリストは収集されたデータのサブセットを選択するためにクエリを実行することから始めます。アナリストは[ナビゲート]ビューでのデータのブラウズ、独自のクエリの作成、フィルタの絞り込み、メタデータの並べ替えや表示の方法の制御を行うことができます。関心のあるイベントが見つかったときは、アナリストは不審なアクティビティまたは悪意のあるアクティビティについて、イベントの詳細を確認して調査します。詳細については、「*調査およびマルウェア解析ユーザ ガイド*」を参照してください。

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。

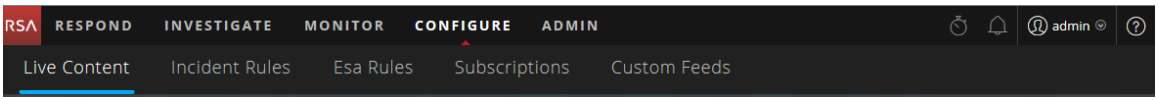


ここで行うことができること	パス	方法を確認する
データセットで検出されたメタ キーと値のクエリと表示	[調査] ビュー	「*調査およびマルウェア解析ユーザ ガイド*」の「調査の実施」を参照。
イベントの調査、再構築、分析	[調査] ビュー	「*調査およびマルウェア解析ユーザ ガイド*」の「イベントの調査」を参照。
悪意のあるコードを含む可能性のあるファイル オブジェクトの検索	[調査] ビュー	「*調査およびマルウェア解析ユーザ ガイド*」の「Malware Analysisの実施」を参照。

構成

[構成]ビューでは、脅威インテリジェンス(コンテンツ)担当者が1つの便利な場所でデータ ソースと入力をNetWitness Suiteに対して構成できます。

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サービス) [Liveコンテンツ]ビューでは、Liveサービスリソースの検索とサブスクライブができます。Liveサービスは、NetWitness SuiteサービスとRSA NetWitness Suiteのユーザが使用可能なLiveコンテンツのライブラリの間の通信と同期を管理する、NetWitness Suiteのコンポーネントです。NetWitness Suiteのサービスとソフトウェアで、RSA Live CMS (Content Management System) のコンテンツを表示、検索、導入、サブスクライブできます。リソースをサブスクライブすると、RSA Liveサービス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。
  レガシーの10.6のユーザにとっては、これは[Live]>[検索]でした。
- **インシデントのルール**: [インシデントのルール]ビューでは、インシデントを自動的に作成するためのさまざまな条件で統合ルールを作成することができます。優先順位付けされたインシデントを[対応]ビューで表示できます。
  レガシーの10.6のユーザにとっては、これは[インシデント]>[構成]でした。

- **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、ルール基準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ルールを作成することや、Liveサービス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。
  レガシーの10.6のユーザにとっては、これは[アラート]>[構成]でした。
- **サブスクリプション**: (Liveサービス) [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 SuiteでLiveサービスを設定するには、CMSサーバとNetWitness Suiteとの間の接続と同期を構成します。
  レガシーの10.6のユーザにとっては、これは[Live]>[構成]でした。
- **カスタムFeed**: (Liveサービス) [カスタムFeed]ビューは、カスタムFeedの作成と管理作業を効率化します。このウィザードでは、選択したDecoderとLog DecoderにFeedを入力することもできます。カスタムフィードとIdentity Feedを設定して管理することができます。
  NetWitness Suiteはフィードを使用して、外部定義のメタデータ値に基づいてメタデータを作成します。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ついては、追加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。
  レガシーの10.6のユーザにとっては、これは[Live]>[フィード]でした。

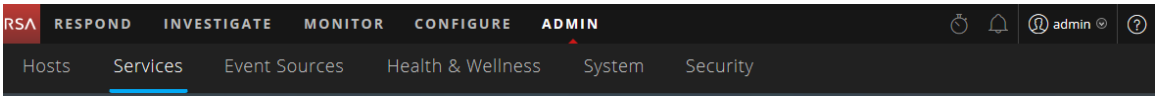
ここで行うことができること	パス	方法を確認する
Liveサービスアカウントの作成。	RSA Live登録ポータル: https://cms.netwitness.com/registration/	「*Liveサービス管理ガイド*」を参照。
Liveサービスリソースの検索と導入。	[構成]>[Liveコンテンツ]	「*Liveサービス管理ガイド*」を参照。
インシデントの自動作成。	[構成]>[インシデントのルール]	「*NetWitness Respond ユーザガイド*」を参照してください。
アラートの構成。	[構成]>[ESAルール]	「*ESAを使用したアラート ガイド*」を参照。

ここで行うことができること	パス	方法を確認する
NetWitness SuiteでのLiveサービスサービスの設定	[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 フィードおよび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。

管理

[Admin]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 Suiteのヘルスモニタ、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サービスなどの、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。組織は通常、イベント ソースの重要度に基づいたグループに分けてイベント ソースを監視します。イベント ソース グループごとに監視ポリシーを作成し、優先度に基づいて順序付けすることができます。
- **ヘルスモニタ**: [ヘルスモニタ]ビューでは、ネットワーク環境内のNetWitness Suiteホストおよびサービスの正常性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、グローバルNetWitness Suite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サービス、URL統合、Investigation、

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 Suite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 Suite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 Suite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。

ここで行うことができること	パス	方法を確認する
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 Suite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。
NetWitness Suite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すると、NetWitness Suiteドメインの正常稼働状態を維持しやすくなります。	[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 Suite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。

ここで行うことができること	パス	方法を確認する
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ロールによる、デフォルト表示の設定

NetWitness Suiteにログインした後、SOC(Security Operations) のロールに基づいてデフォルトのビューを設定すると、アプリケーションの移動を容易にすることができます。ランディング ページとも呼ばれるデフォルト ビューは、ユーザ環境設定で設定します。

次の図は、主なNetWitness Suiteビューを示しています。

- **対応**:このビューは、インシデントのリストを優先順位づけとアラートに応じて表示できる、インシデント対応者が使用します。従来の10.6ユーザには、このビューは[インシデント管理]ビューと呼ばれており、ESA 10.6の[アラート]>[サマリ]ビューに代わって[対応]>[アラート]ビューが表示されます。
  Respondは、デフォルトの最初のビューです。対応ビューを表示する権限がない場合は、監視ビューがデフォルトになります。
- **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。以前のアプリケーション バージョンの従来型のビューです。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したりすることができます。
- **構成**:このビューは、データ ソースと入力をNetWitness Suiteに構成する、脅威インテリジェンス(コンテンツ) 担当者が使用します。脅威インテリジェンス担当者は、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。
  レガシーの10.6のユーザにとっては、このビューは[Live]、[インシデント]>[構成]、[アラート]>[構成]でした。
- **管理**:このビューは、全体のアプリケーション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。

主なNetWitness Suiteビューはどれでも、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 Suite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
- IDダッシュボード
- 運用:ログ ダッシュボード

- 運用 : ネットワーク ダッシュボード
- 概要ダッシュボード
- 脅威 : インジケータ ダッシュボード
- 脅威 : 侵入ダッシュボード

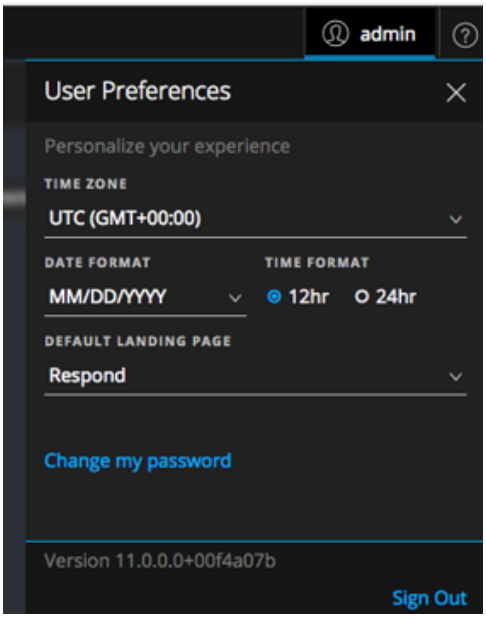
次の表は、一般的なSOCのロールと、SOCのロールに基づいてユーザ環境設定でランディングページとして選択できる使用可能なビューを示します。複数のロールがある場合は、NetWitness Suiteへのログイン時に最初に表示されるビューとして最も適切なものを選択します。

SOCのロール	役割の説明	このデフォルトのランディング ページを検討
インシデント対応者 (Tier1 アナリスト)	確認して軽減するためにキューに登録されたインシデントとアラートに対応	**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**
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、インシデントや侵害やデータ漏洩に対応します。	**監視**(ダッシュボードは監視ビュー内) ログインするときにSOCロールに適切な事前定義された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。

SOC のロール	役割の説明	このデフォルトのランディング ページを検討
コンテンツのエキスパート(脅威インテリジェンス)	データ ソースを構成し、NetWitness Suite に入力します。	**監視**または**構成**(ダッシュボードは監視ビュー内。ログインするときにSOCロールに適切な事前定義された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 ビューとして選択すると、メイン メニューから構成ビューに移動できます。)
Data Privacy Officer (DPO)	管理者と同様ですが、DPOは、プライバシーに関する機密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内。ログインするときにSOCロールに適切な事前定義された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。)
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. (対応ビューのみ) 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 ランディング ページ**]フィールドで、NetWitness Suite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**を選択でき、脅威ハンターの場合は、**調査**を選択できます。
環境設定はすぐに反映されます。デフォルトのランディング 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 Suite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

次の表には、NetWitness Suite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が記載されています。

問題	トラブルシューティングのヒント
NetWitness Suite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 ランディング 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。

問題	トラブルシューティングのヒント
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。	他のブラウザを使用してみてください。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を使用していて、次のエラーが発生します。 `The page can't be displayed.`	NetWitness Suite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プロトコルの有効化を試すことができます。 [**インターネット オプション**]>[**詳細設定**]>[**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 ランディング 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

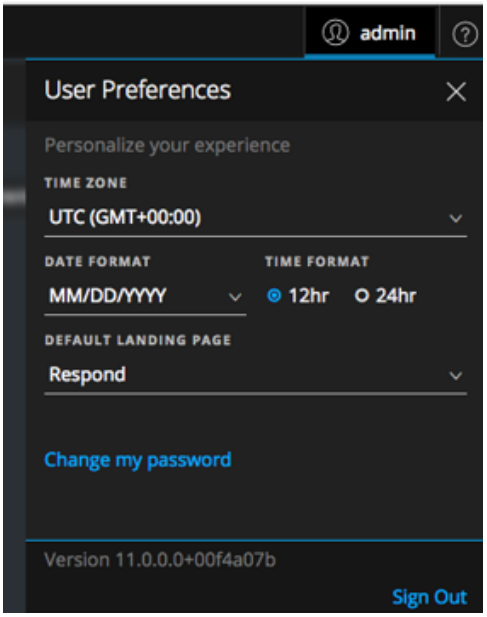
NetWitness Suiteグローバル アプリケーション環境設定は、ユーザ プロファイルから表示および管理することができます。グローバル環境設定オプションは、新しい対応ビューと、監視、構成、管理、調査などのその他のビューのどちらからアクセスするかによって異なります。
実行できる操作:

- 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(対応ビューのみ)
- デフォルトの開始場所の選択(対応ビューのみ)
- 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(対応ビューを除くすべてのビュー)
- コンテキスト メニューの有効化または無効化(対応ビューを除くすべてのビュー)

注:「対応ビュー」および「対応ビューのみ」と付記されているユーザ環境設定手順は、一部のInvestigateビューでも実行できます。

ユーザ環境設定の表示(対応ビュー)

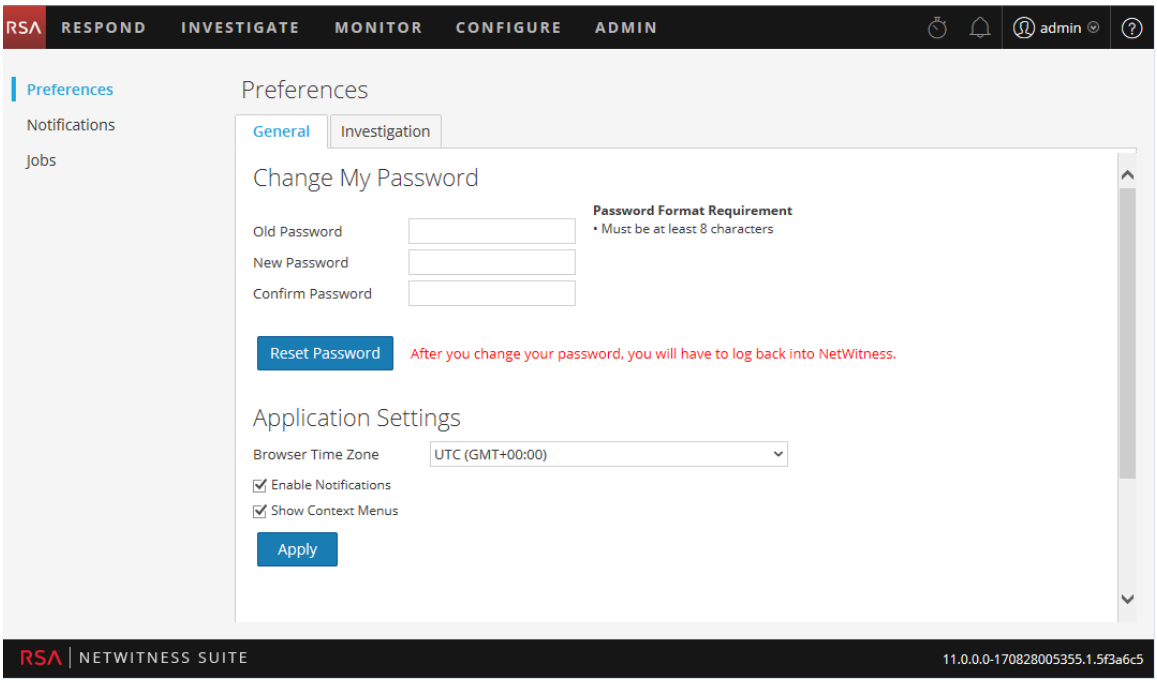
NetWitness Suiteブラウザ ウィンドウの左上隅で、を選択します。
対応ビューからアクセスすると、[ユーザ環境設定]ダイアログに現在の環境設定が表示されます。



選択はすぐに有効になります。

ユーザ環境設定の表示(対応ビューを除くすべてのビュー)

次のビュー(調査、監視、構成、管理)の場合:NetWitness Suiteブラウザウィンドウの左上隅で、> [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。



タイムゾーンと日付と時刻の形式を設定します。

タイムゾーンとの日付と時刻、場所の形式を変更することができます。

注:地域の日付と時刻の環境設定は対応ビューからのみ変更できます。

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. **タイムゾーン**:NetWitness Suiteで使用するタイムゾーンを設定します。
   b. **(対応ビューのみ) 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。
   c. **(対応ビューのみ) 時刻形式**:12時間制または24時間制として時間を設定します。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。
2. **(対応ビューのみ)** [**適用**]をクリックします。
   環境設定はすぐに反映されます。

デフォルトの開始場所の選択

1. **(対応ビューのみ)** [ユーザ環境設定]ダイアログを開きます。
2. [**デフォルト ランディング ページ**]フィールドで、NetWitness Suiteにログインするときに表示する最初の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、Respondを選択すると、インシデント対応者向けアプリケーションの関連する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ロールによる、デフォルト表示の設定」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。

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

(対応ビューを除くすべてのビュー) デフォルトでは、NetWitness Suite新しいユーザ アカウントが作成されると、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:
   - 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

(対応ビューを除くすべてのビュー) 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:
   - 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(対応ビューを除くすべてのビュー) の[Investigate]タブで使用可能な設定については、「*調査およびマルウェア解析ユーザ ガイド*」を参照してください。

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。NetWitness Suiteでは、ダッシュボードを作成して、NetWitness Suite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 Suiteデフォルト ダッシュボードがNetWitness Suite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 Suiteコンポーネントのダッシュボードは、デフォルトのNetWitness Suiteダッシュボードまたはカスタムの NetWitness Suiteダッシュボードに追加できます。

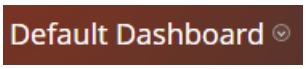
ユーザ権限に応じて、関心のあるさまざまな領域に関するダッシュボードとレポートを表示できます。事前構成済みダッシュボードを選択したり、ダッシュボードをインポートしたり、独自のカスタム ダッシュボードを作成することができます。ダッシュボードでは、レポートを素早く簡単に表示できます。ワークフローをサポートする情報を表示するようにダッシュボードを構成することができます。このトピックでは、ダッシュボードを設定するときに実行できるタスクの概要について説明します。

ダッシュボードの基本

[監視]ビューがNetWitness Suite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 Suite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 Suite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。

オプション	説明
Default Dashboard	選択できる使用可能なダッシュボードの一覧を表示します。
	[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。
Share	他のユーザとダッシュボードを共有できます。
Add Row	要件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 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
- Overview
- RSA SecurID
- Threat - Hunting
- Threat - Malware Indicators
- 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。

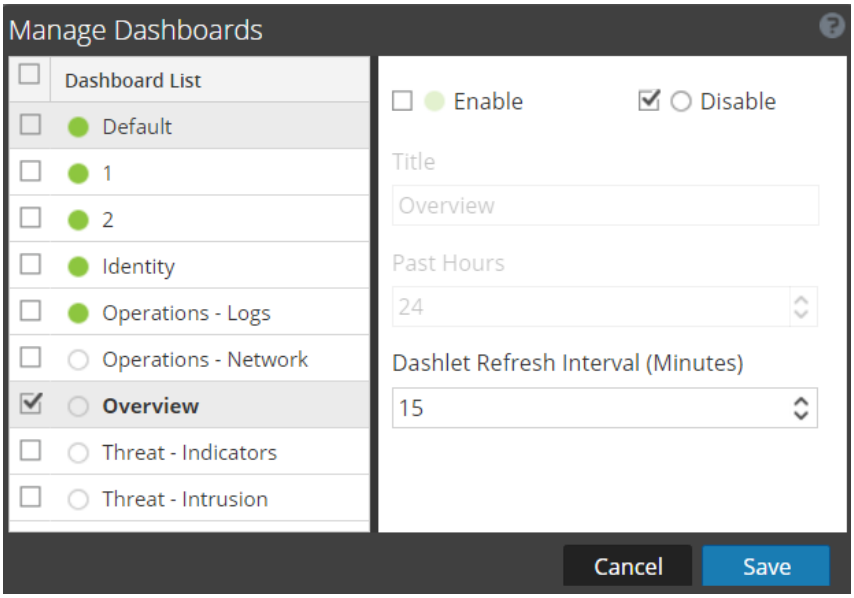
- ダッシュボードの編集
- ダッシュボードのエクスポート
- ダッシュボードの共有
- ダッシュボードの削除

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。

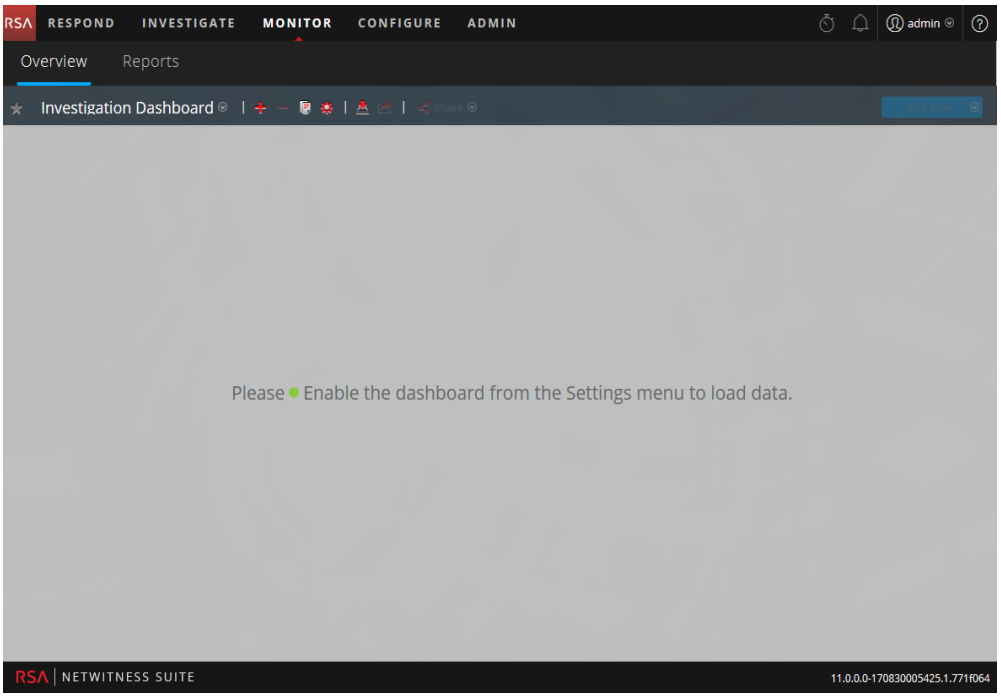
NetWitness Suiteモジュールは、[ダッシュレットの管理]ダイアログに表示されるダッシュレットだけを表示できます。メイン ダッシュボードでは、NetWitness Suiteのすべてのダッシュレットが提供されます。次の図は使用可能なダッシュレットの例です。



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。タイトルは変更もできます。
時間(24時間前まで)	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。

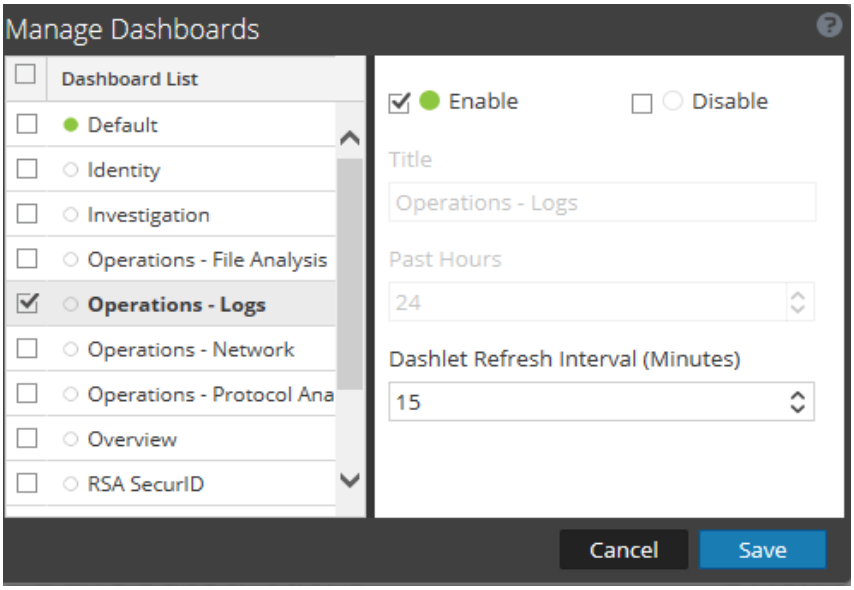
ダッシュボードの有効化

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 ツールバーで、  をクリックします。
3. [**ダッシュボードの管理**]オプションを選択します。
   [ダッシュボードの管理]ダイアログが表示されます。



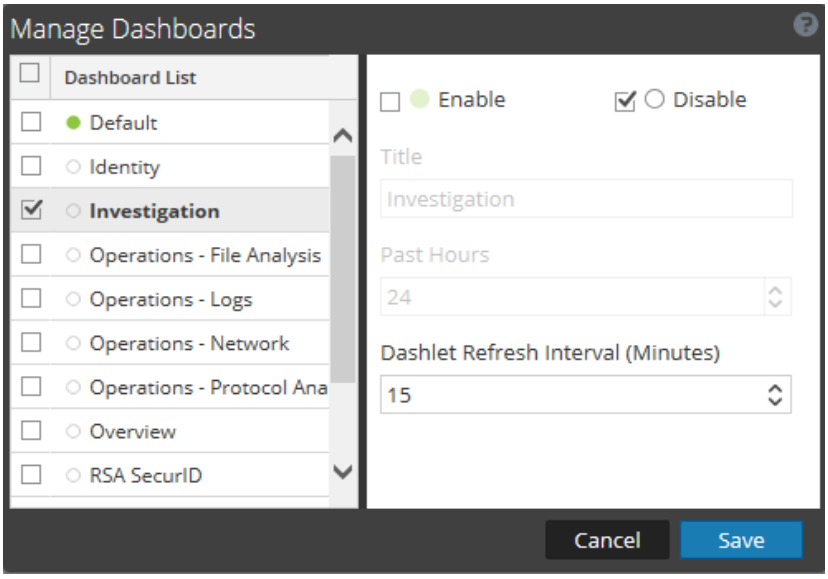
4. ダッシュボード リストから、有効化するダッシュボードを選択します。

5. [**有効化**]チェックボックスをクリックします。
6. [**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 ツールバーで、  をクリックします。
3. [**ダッシュボードの管理**]オプションを選択します。
   [ダッシュボードの管理]ダイアログが表示されます。



4. 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。
5. [**無効化**]チェックボックスをクリックします。
6. [**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 Suite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 Suiteダッシュボードには、その名のとおり、NetWitness Suiteのすべてのダッシュレットが含まれます。[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 Suite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. 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。

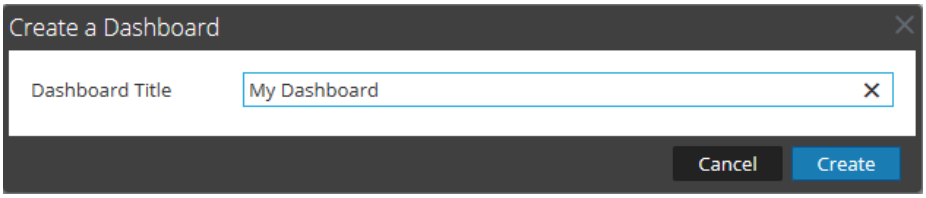
カスタム ダッシュボードの作成

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。

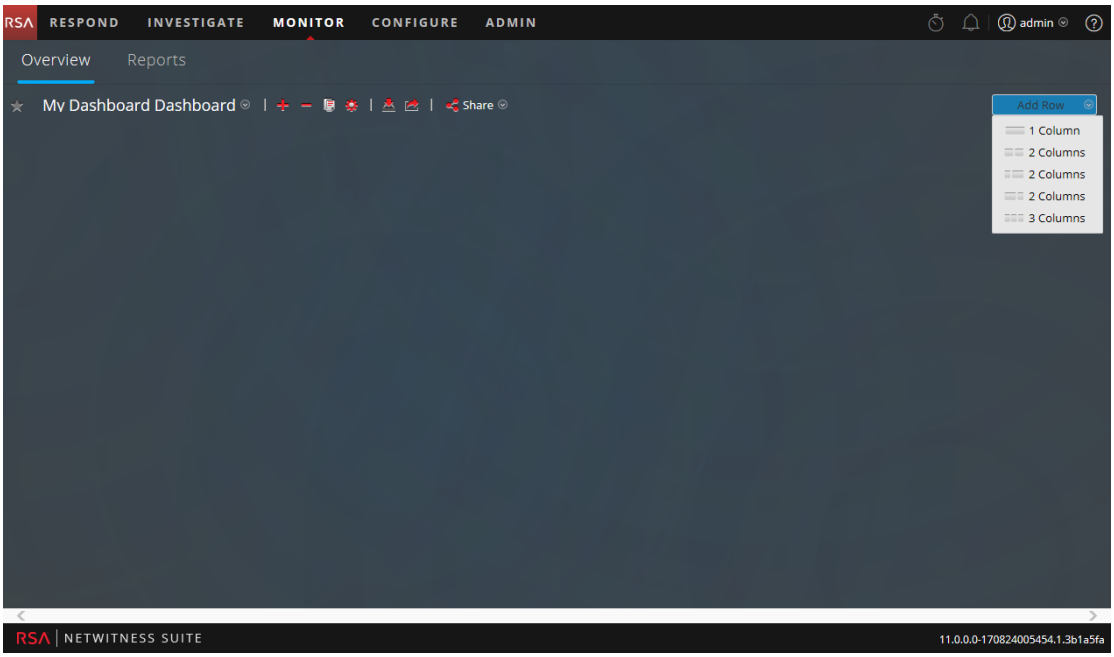
1. ダッシュボード ツールバーで、  をクリックします。

   [ダッシュボードの作成]ダイアログが表示されます。



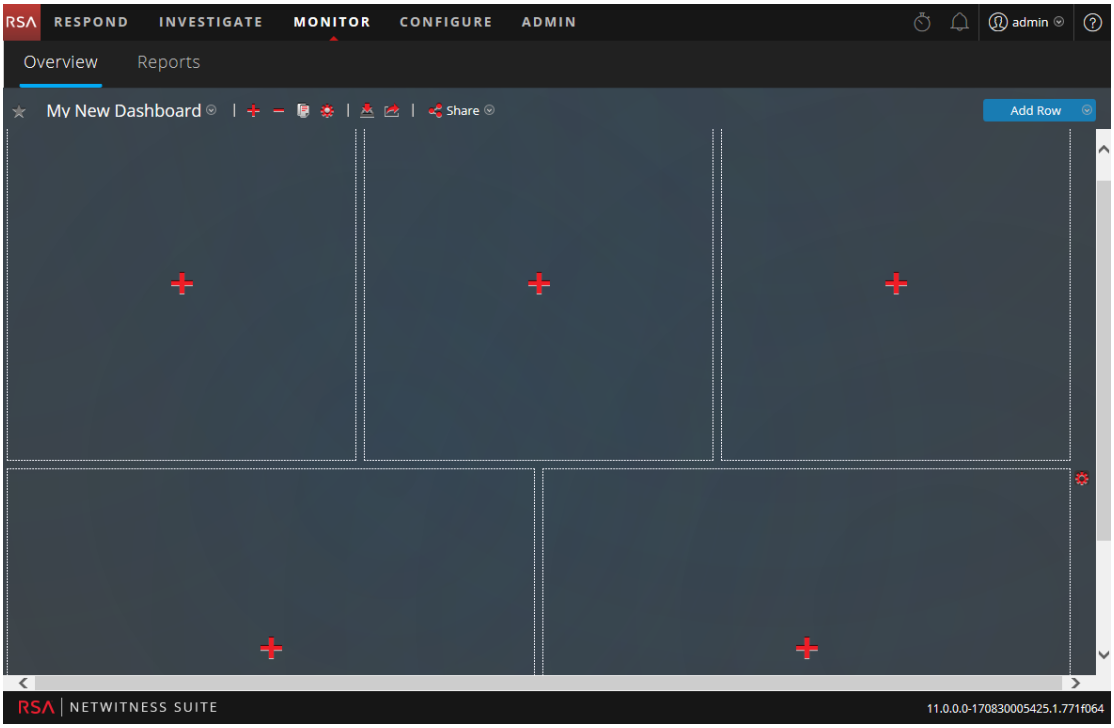
2. 新しいダッシュボードのタイトルを入力し、[**作成**]をクリックします。

   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**](

)コントロールを使用して、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選択し、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。

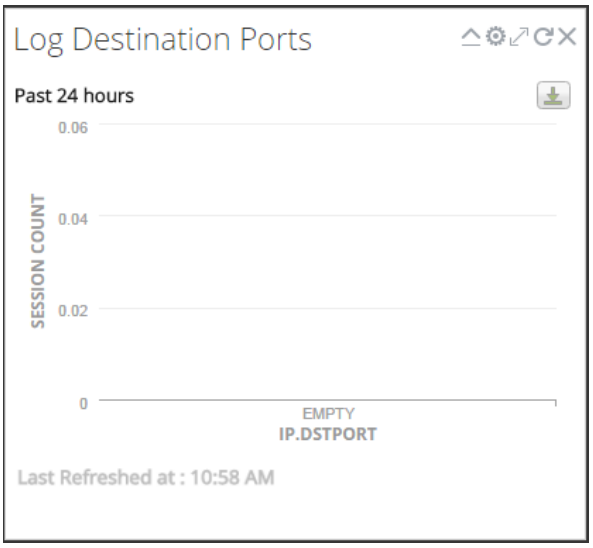
各ダッシュボードには、次のような項目があります。

- 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

ダッシュレットの操作

NetWitness Suite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。

アイコン	名前	説明
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。
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 Suite 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。

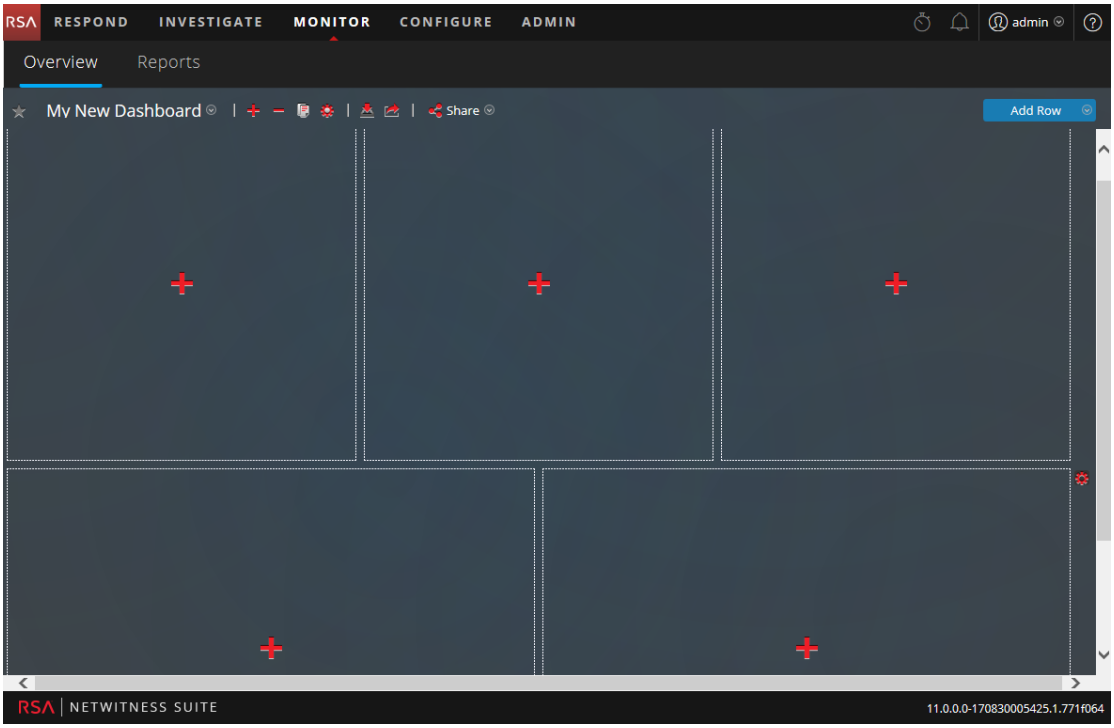
デフォルト ダッシュボードにダッシュレットを追加するか、便利な独自のダッシュレット セットを使用してカスタム ダッシュボードを作成し、ワークフローをより効率的にすることができます。

ダッシュレットの追加

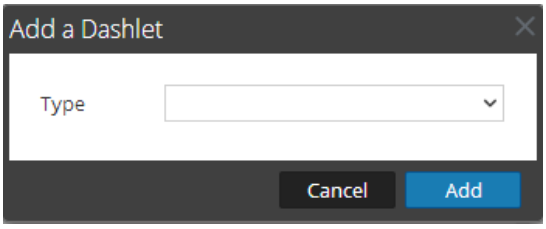
NetWitness Suiteのビューをカスタマイズする場合には、デフォルト ダッシュボードにダッシュレットを追加したり、カスタム ダッシュボードを作成したりできます。ただし、事前構成済みダッシュボードにダッシュレットを追加することはできません。

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。

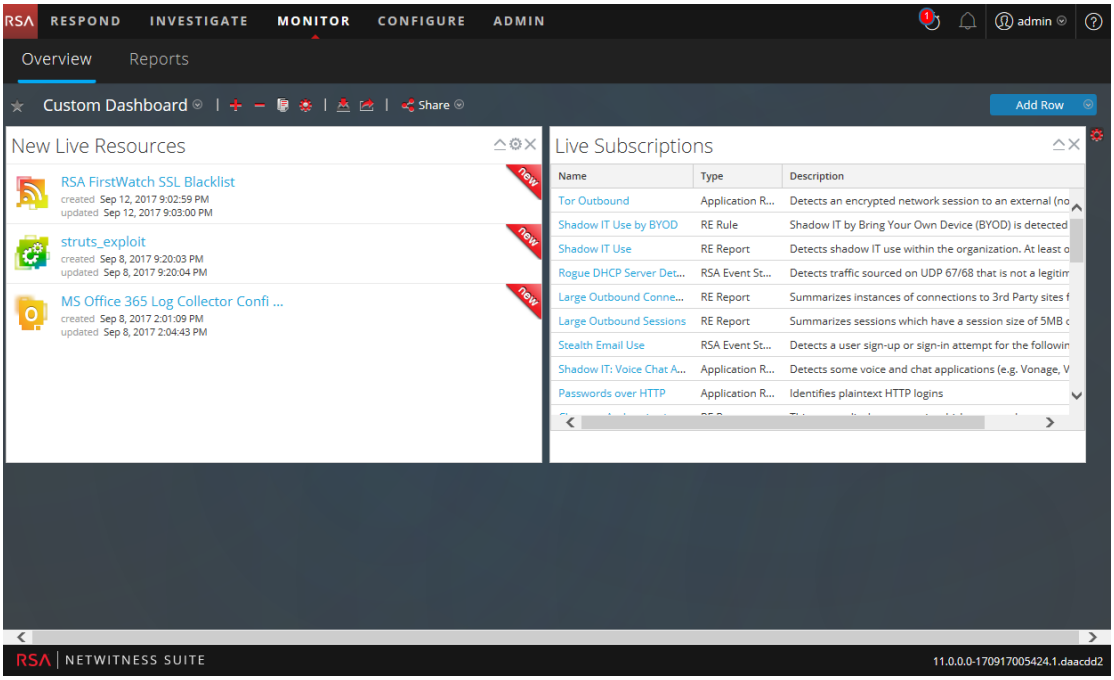


2. ダッシュレットを追加するプレースホルダーで  をクリックします。
[ダッシュレットの追加]ダイアログが表示されます。



3. ダッシュレットの**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。

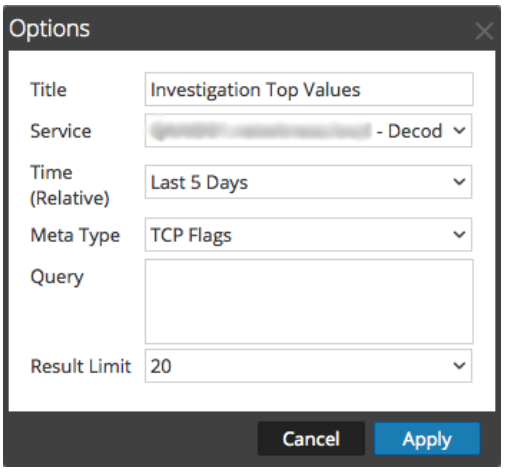
編集可能なプロパティがないダッシュレット([Liveサブスクリプション]ダッシュレットなど) の場合、タイトルバーに設定オプションは表示されません。多くのダッシュレットは編集可能であり、次のプロパティを編集することができます。

- 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。

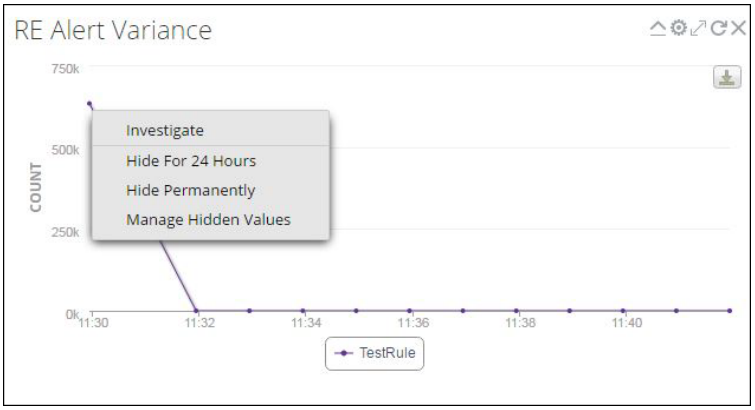
   [**オプション**]ダイアログが表示されます。



2. 表示されているプロパティを編集します。たとえば、[Investigation 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。

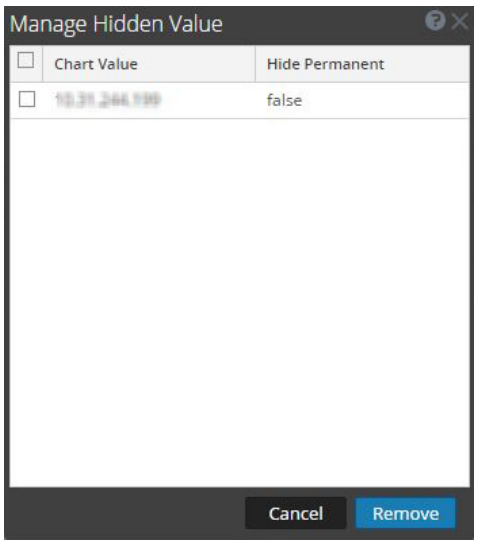
一部のダッシュレットには、外観またはダッシュレットのコンテンツをカスタマイズする設定オプションがあります。次のオプションは、[レポート 上位アラート]、[レポート アラート推移]、[レポート リアルタイム チャート]ダッシュレットを左クリックすると表示されます。

- **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。

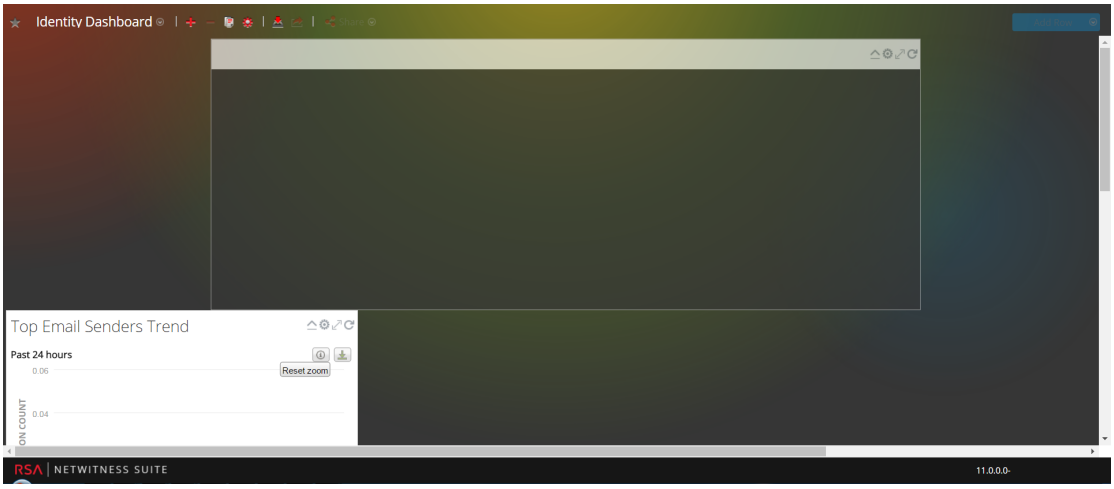
ダッシュレットの再配置

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。



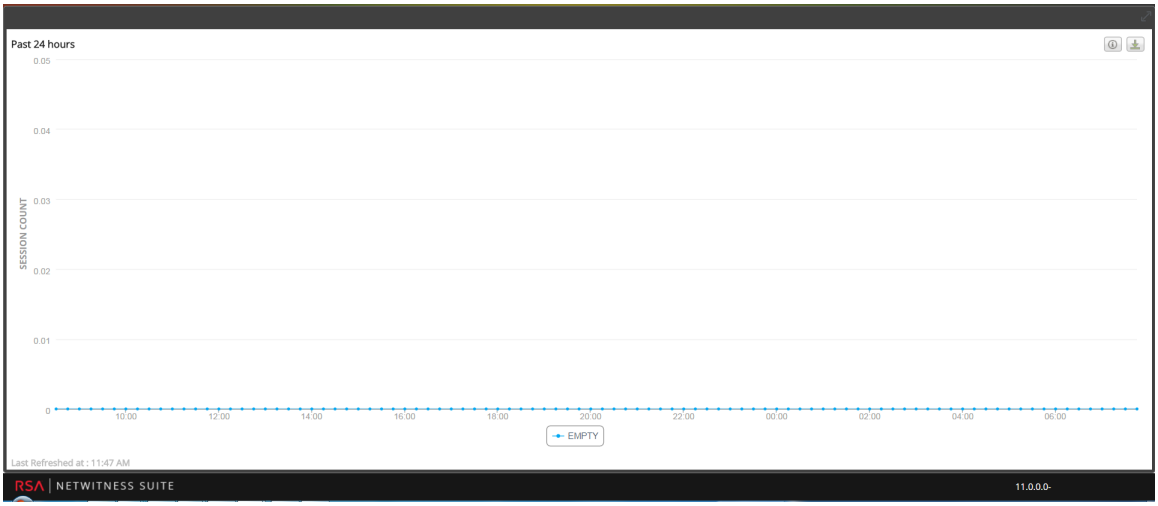
3. ダッシュレットを目的の位置に移動したら、マウスボタンを離してドロップします。
   移動先にもともと配置されていたダッシュレットは下へ移動します。

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 Suite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。

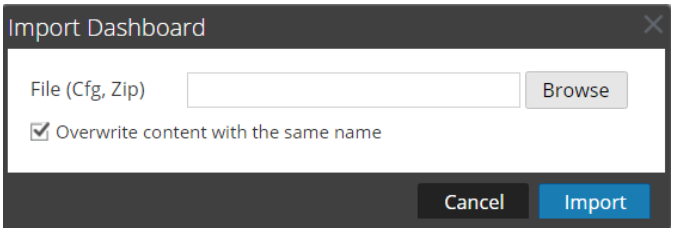
ダッシュボードのインポートとエクスポート

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 Suiteにインポートします。

ダッシュボードのインポート

注：レポート リアルタイム チャートを含むダッシュボードおよび関連するチャートは、エクスポート元とは別のNetWitness SuiteサーバおよびReporting Engineにインポートすることができます。

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**]を選択します。
   [**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. [**ダッシュボードのインポート**]をクリックします。
   ダッシュボードがNetWitness Suiteに表示されます。

注 : Security Analytics 10.6.xからNetWitness Suite 11.0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、関連づ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 Suite 11.0からNetWitness Suite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

エクスポートされたダッシュボードは、同じNetWitness Suite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。

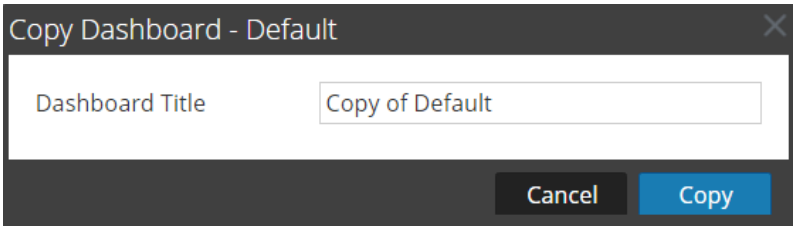
ダッシュボードのコピー

NetWitness Suite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 ダッシュボードにコピーします。NetWitness Suiteダッシュボードには、その名のとおり、NetWitness Suite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、元の名前に「Copy of」というプレフィックスを付けたものがデフォルトの名前になります。たとえば、元のダッシュボードの名前がXYZの場合、コピーされたダッシュボードのデフォルトの名前は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. 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-デフォルト]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、

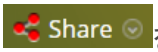
ダッシュボードをコピーする例を示します。



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 Suite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、表示のためにダッシュボードを共有できます。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. 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

NetWitness Suite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 Suite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 Suite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 Suiteのユーザ インタフェースでは、NetWitness Suite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( ) が表示され、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。

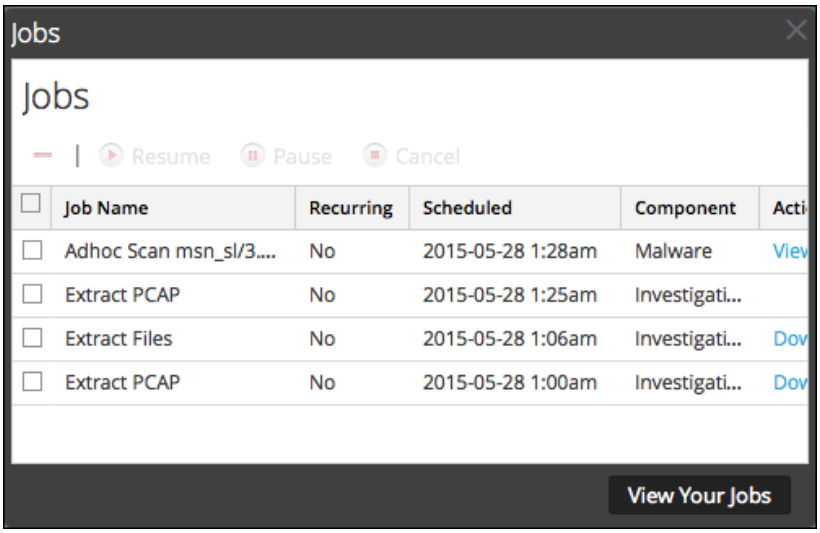
- [プロファイル]ビューでは、ジョブ トレイと同じ内容のジョブ画面をフル パネルで表示できます。確認することができるのは自分が実行したジョブだけです。
- [システム]ビューでは、管理権限を持つユーザが、すべてのユーザのすべてのジョブを1つのジョブ パネルで表示および管理できます。

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 Suiteツールバーで、[ジョブ]アイコン ( ) をクリックします。

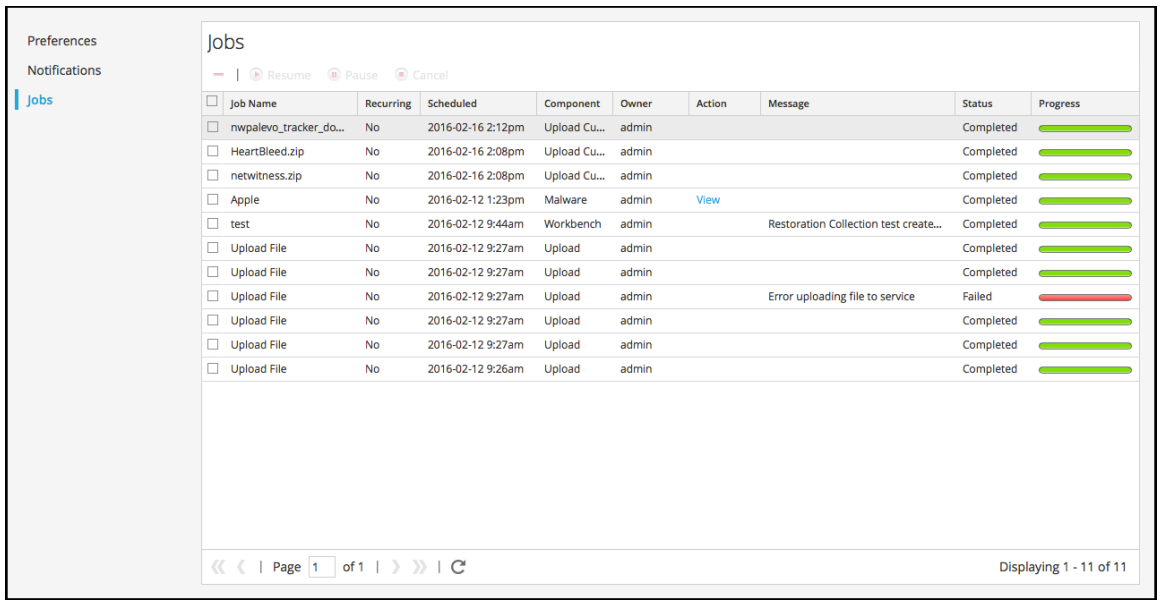
ジョブ トレイが表示されます。



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(繰り返しジョブと繰り返しではないジョブ) が一 覧 表 示されます。ジョブ トレイと、[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]の[システム]ビューでは、すべてのユーザのすべてのNetWitness Suiteジョブの情 報 が[ジョブ] パネルに一 覧 表 示されます。

[プロファイル]ビュー> [ジョブ] パネルでのジョブの表 示

ジョブを拡 大 表 示するには、[**自 分 のジョブを表 示**]をクリックします。
[プロファイル]ビュー> [ジョブ] パネルが表 示されます。



繰り返しジョブの一時停止と再開

[一時停止]と[再開]オプションは、繰り返しジョブにのみ適用されます。実行中の繰り返し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. 繰り返し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. 一時停止された繰り返し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グリッドに残されます。

   繰り返し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、ジョブはすぐにグリッドから削除されます。確認ダイアログは表示されません。繰り返し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。Administratorsロールのユーザはどのジョブも削除できます。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. [**削除**]をクリックします。
3. ジョブはグリッドから削除されます。

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 モジュールにおいて、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

NetWitness Suiteのユーザ インタフェースでは、最新のシステム通知を確認することができます。NetWitness Suite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。

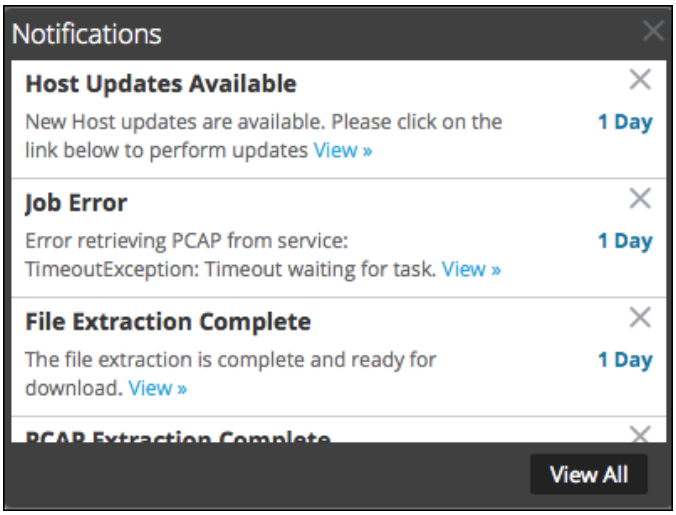
- ホストのアップグレードが完了した。
- DecoderへのParserの適用が完了した。
- 新しいバージョンのソフトウェアが利用可能。

次の2つのビューの[通知]パネルで、すべての通知を確認できます。

- [プロファイル]ビューでは、自分の通知のみを確認できます。
- [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通知を1つのパネルで表示および管理できます。

通知の表示

[通知]トレイを表示するには、[通知]アイコン( ) をクリックします。



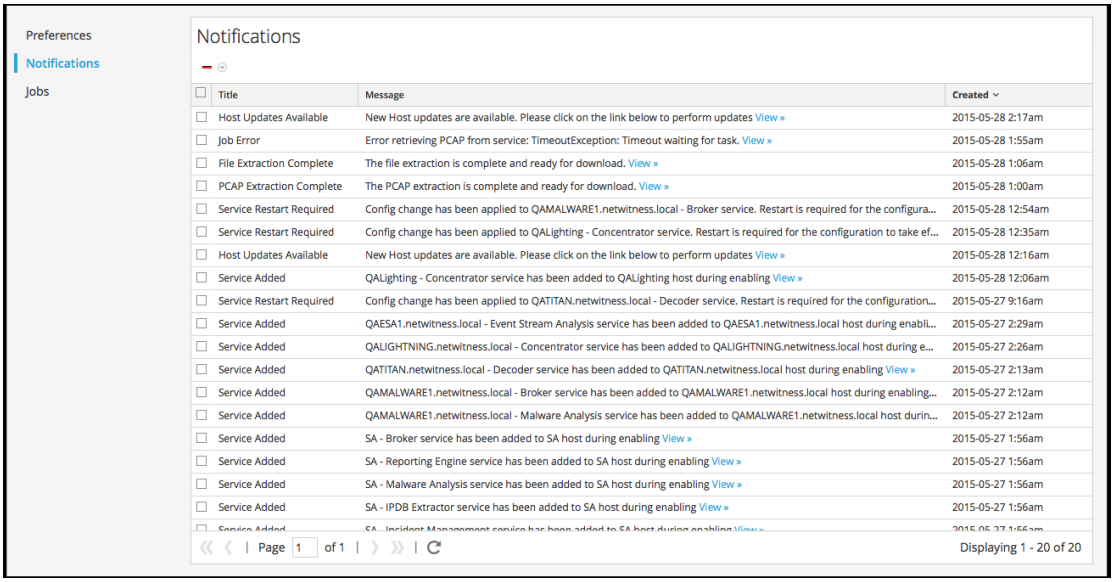
すべての通知の表示

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。

1. [**プロファイル**]に移動し、[プロファイル]ビューの[オプション]パネルで、[**通知**]を選択します。

2. **[管理]＞[システム]**に移動し、[システム]ビューの[オプション]パネルで、[**通知**]を選択します。
3. 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。

   [通知]パネルが表示されます。ここにはすべての通知が表示され、フォーマットは通知トレイのフォーマットとは異なります。



通知レコードの削除

通知レコードを削除するには、次を行います。

1. [**通知**]テーブルで、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テーブル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

NetWitness Suite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 リンクを使用することができます。

インライン ヘルプの表示

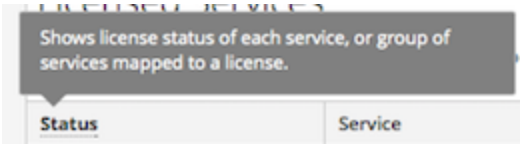
インライン ヘルプでは、NetWitness Suiteユーザ インタフェースでユーザーが現在表示しているセクションまたはフィールドで行う操作に関する追加情報が提供されます。インライン ヘルプを表示するには、  の上にマウス ポインターを置きます。インライン ヘルプには、要素の簡単な説明が表示されます。

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 :

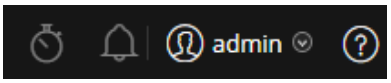


オンライン ヘルプの表示

オンライン ヘルプ リンクは、NetWitness Suite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 Suite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 Suite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 Suite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。


admin

RSA Linkでのドキュメントの検索

RSA NetWitness® Suite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にあります。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 Suiteドキュメントの検索

NetWitness Suite Logs and Packets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 Suite Logs and Packets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 SUITE**]をクリックします。
2. RSA NetWitness Suiteのページで、[**DOCUMENTATION**]をクリックし、[**RSA NETWITNESS LOGS AND PACKETS**]を選択します。

NetWitness Endpoint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 SUITE**]をクリックします。
2. RSA NetWitness Suiteのページで、[**DOCUMENTATION**]をクリックし、[**RSA NETWITNESS ENDPOINT**]を選択します。

RSAコンテンツの検索

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 SUITE**]をクリックします。
2. RSA NetWitness Suiteのページで、[**DOCUMENTATION**]をクリックし、[**ADDITIONAL RESOURCES**]＞[**RSA CONTENT**]を選択します。

RSAでサポートされるイベント ソースの検索

RSAでサポートされるイベント ソースは、次のリンクにあります。
https://community.rsa.com/community/products/netwitness/parser-network/event-sources

RSAでサポートされるイベント ソースに移動するには、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 SUITE**]をクリックします。
2. RSA NetWitness Suiteのページで、[**DOCUMENTATION**]をクリックし、[**ADDITIONAL RESOURCES**]＞[**EVENT SOURCE CONFIGURATION**]を選択します。

ハードウェア構成ガイドの検索

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 SUITE**]をクリックします。
2. RSA NetWitness Suiteのページで、[**DOCUMENTATION**]をクリックし、[**ADDITIONAL RESOURCES**]＞[**HARDWARE SETUP GUIDES**]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 Suite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 SUITE**]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、ユーザドキュメントの場合は[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 Suiteスタート ガイドの参考情報

次のセクションには、NetWitness Suite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NetWitness Suiteを調整するには、独自のグローバル アプリケーション環境設定を設定することができます。実行できる操作:

- 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(対応ビューのみ)
- デフォルトの開始場所の選択(対応ビューのみ)
- 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
- Investigate環境設定の変更:詳細については「*調査およびマルウェア解析ユーザ 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。

注:「対応ビュー」および「対応ビューのみ」と付記されているユーザ環境設定手順は、一部のInvestigateビューでも実行できます。

どうしますか?

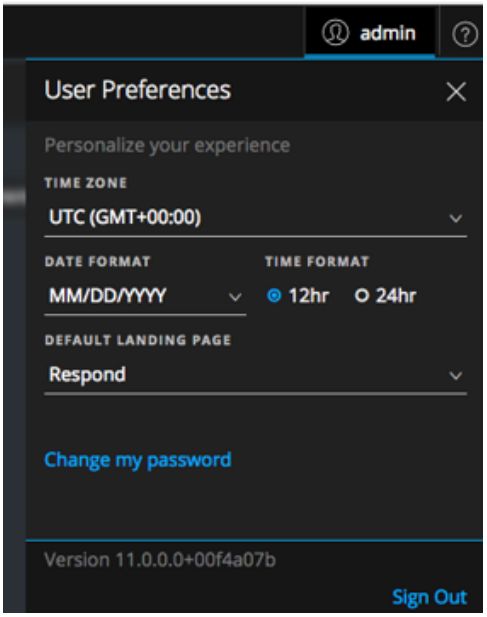
ロール	処理オプション...	方法を確認する
すべて	パスワードの変更	パスワードの変更
すべて	デフォルト ランディング ページの選択	SOCロールによる、デフォルト表示の設定
すべて	ユーザの環境設定	ユーザ環境設定

関連トピック

- NetWitness Suiteの基本ナビゲーション

ユーザ環境設定(対応ビュー)

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 Suiteバージョンが表示されます。メイン メニュー バーでは、ユーザ プロファイル アイコンの横に現在のタイム ゾーンの環境設定が表示されます。



次の表では、対応ビュー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
タイム ゾーン	NetWitness Suite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。
時間形式	12時間制または24時間制として時間を設定します。たとえば、12時間制の2:00 PMは、24時間制で14:00です。

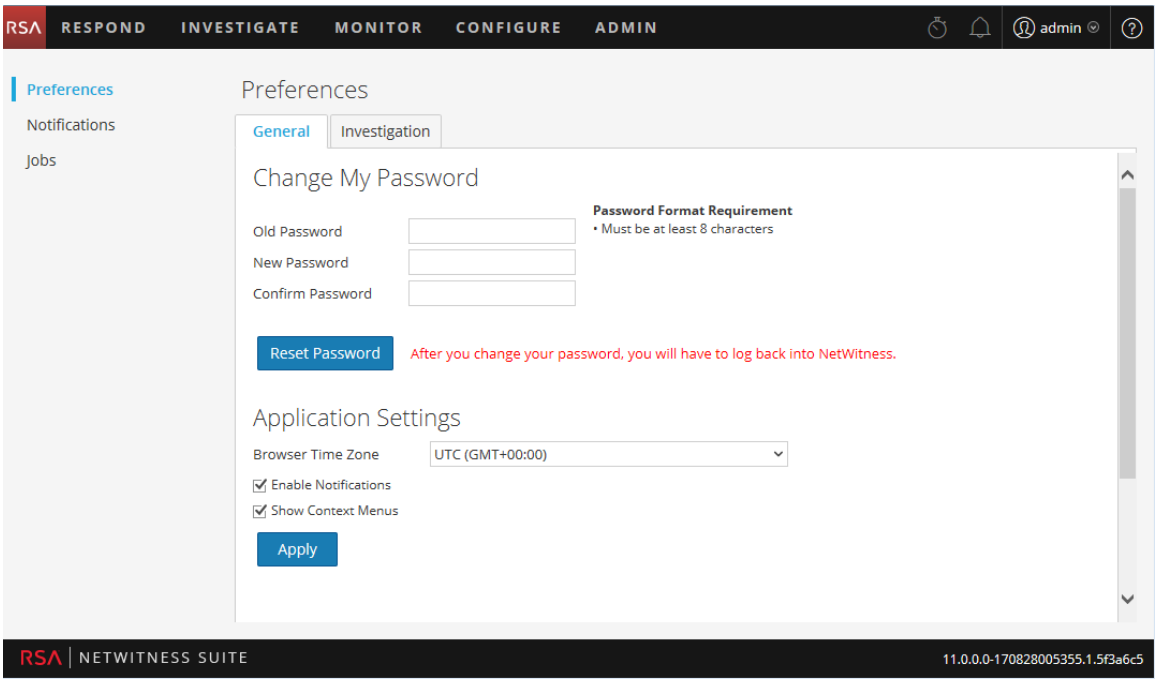
オプション	説明
デフォルト ランディング ページ	NetWitness Suiteにログインするときのデフォルト ビューを選択することができます。ユーザのロールに応じて、対応、調査、監視、構成、管理から選択できます。たとえば、Respondを選択すると、インシデント対応者向けアプリケーションの関連するセクションに直接移動できます。 この選択は、アプリケーション全体のデフォルト ビューを設定します。
パスワードの変更	パスワードを変更できる[環境設定]ダイアログが表示されます。
バージョン	NetWitness Suiteバージョンが表示されます。
サイン アウト	NetWitness Suite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

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、これらのビュー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さ、大文字、小文字、小数点、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 Suiteパスワードに適切なパスワード強度の要件を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 Suite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	次のログインに使用するパスワードを入力します。
パスワードの確認	新しいパスワードを再入力してください。
パスワードのリセット	ユーザ インタフェースで使用するタイム ゾーンを変更できます。変更を有効にするため、NetWitness Suiteからログアウトします。新しいパスワードは、次回のNetWitness Suite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 ログインと、アカウントが追加されているすべてのNetWitness Suite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 Suiteからログアウトします。新しいパスワードは、次回のNetWitness Suite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
ブラウザのタイムゾーン	NetWitness Suite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 Suite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

NetWitness Suite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 Suiteのユーザ インタフェースでは、最新のシステム通知を確認することができます。NetWitness Suite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。

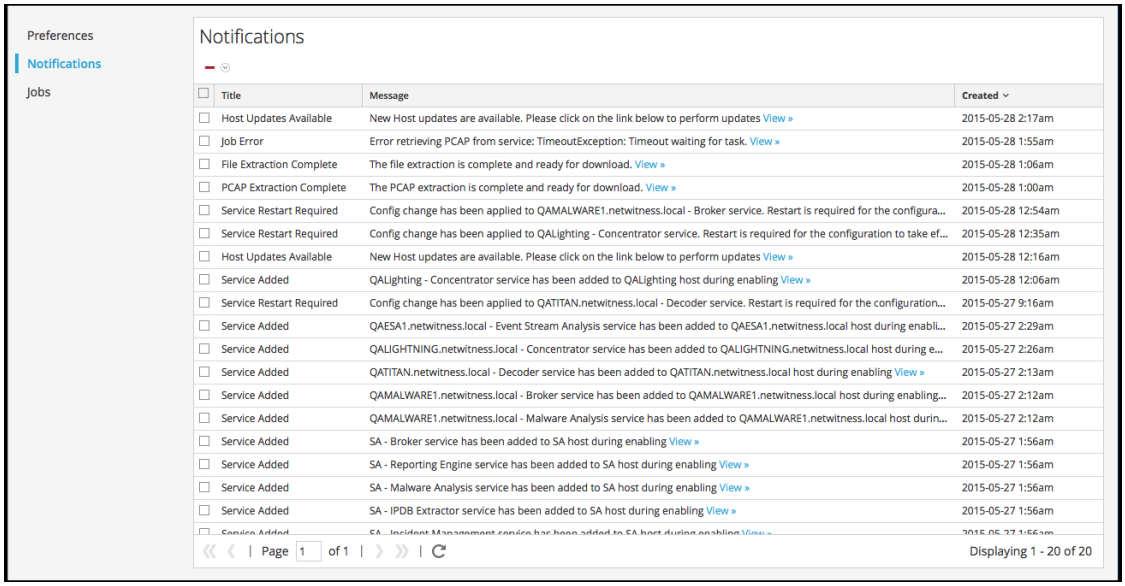
通知トレイでシステム通知を表示する場合、最近のシステム通知のみが表示されます。[プロファイル]ビューまたは[システム]ビューでは表形式ですべての通知を表示できます。通知の表示に関する操作手順については、[通知の表示と削除]セクションを参照してください。

実行したいことは何ですか?

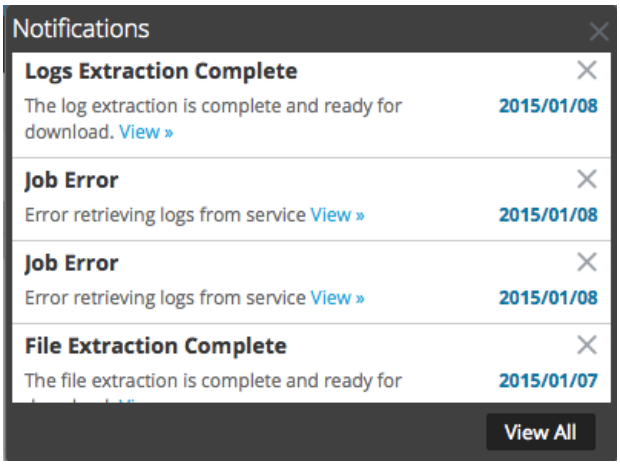
ロール	実行したいこと	手順
すべて	すべての通知の表示	通知の表示と削除
すべて	通知の削除	通知の表示と削除

[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。

- [**プロファイル**]に移動し、[プロファイル]ビューの[オプション]パネルで、[**通知**]を選択します。
- [**管理**]>[**システム**]に移動し、[システム]ビューの[オプション]パネルで、[**通知**]を選択します。



- をクリックし、通知トレイで[**すべて表示**]をクリックします。



[通知]パネルとトレイには、ツールバーと表があります。通知トレイには、[通知]パネルに表示される情報のサブセットが表示されます。次の表に、[通知]パネルの機能とその説明を示します。

機能	説明
−	ドロップダウン メニューが表示され、[**通知**]の表と通知トレイから、選択した通知レコードまたはすべての通知レコードを削除できます。
タイトル	通知のタイトル。「**ファイルの抽出が完了しました**」など。
メッセージ	メッセージ全体。たとえば、「**ファイルの抽出が完了し、ダウンロードの準備ができました。**」
表示	一部のメッセージには、アクションへの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、このビューでファイルをダウンロードできます。
作成日	通知が作成された日時。 通知トレイでは、通知が作成されてからの日数がこの列に表示されます。

機能	説明
すべて表示	[プロファイル]ビューの通知の一覧を表示します。

[ジョブ]パネルとジョブ トレイ

ジョブはさまざまなNetWitness Suiteモジュールによって開始されます。たとえば、Liveモジュールでリソースをダウンロードしたり、管理モジュールでサービスへFeedをアップロードする際にジョブが実行されます。また、調査モジュールで、パケット キャプチャ ファイルの分析や再構築を実行する場合にもジョブが実行されます。

[管理]の[システム]ビューの[ジョブ]パネルでは、管理者ユーザがすべてのNetWitness Suiteジョブを管理できます。他の非管理者ユーザは、[プロファイル]ビューで自分のジョブを表示できます。

また、NetWitness Suiteのユーザ インタフェースでは、NetWitness Suite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( ) が表示され、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。

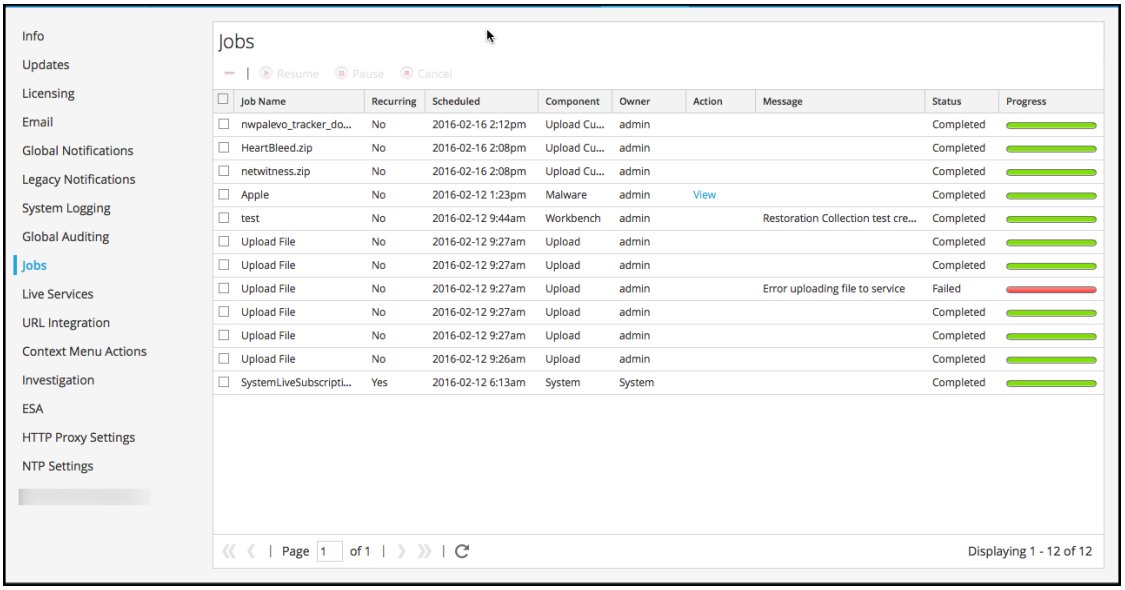
実行したいことは何ですか?

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

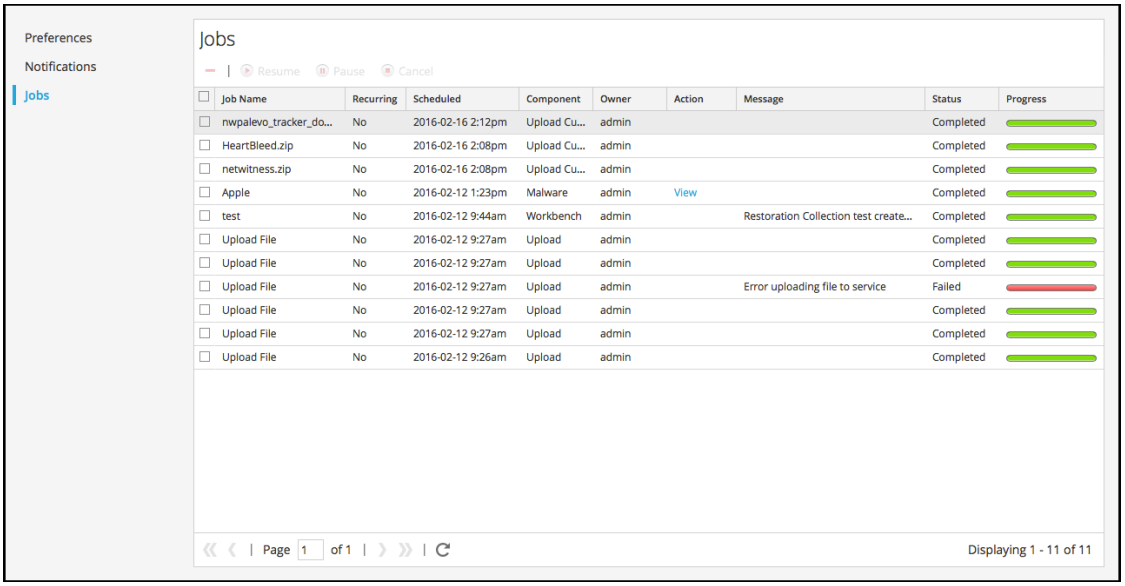
ロール	実行したいこと	手順
すべて	ジョブのキャンセルまたは削除	ジョブの管理
	ジョブ結果のダウンロード	ジョブの管理

[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。

- **[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。

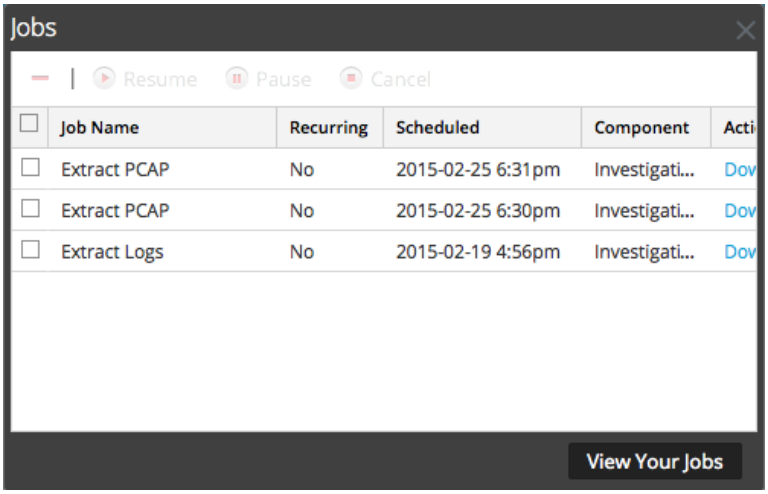


- **[プロファイル]** に移動して、オプション パネルで **[ジョブ]** を選択します。



[ジョブ]パネルでは、ジョブの情報がグリッドに表示されます。列には、ジョブ名、繰り返しオプション、ジョブのコンポーネント、ジョブの所有者、ジョブ結果のダウンロードや表示 ボタン、メッセージ、ステータス、進行状況バーが示されます。

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(繰り返しジョブと繰り返しではないジョブ)が一覧表示されます。ジョブトレイと、[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]の[システム]ビューでは、すべてのユーザのすべてのNetWitness Suite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。

機能	説明
Resume	[再開]オプションは、一時停止されていた繰り返し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、繰り返しジョブにのみ適用されます。実行中の繰り返し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	繰り返しジョブまたは繰り返し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。繰り返し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。

機能	説明
	[**ジョブ**] パネルから繰り返しジョブまたは繰り返し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。繰り返し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] パネルの機能を説明します。

機能	説明
選択ボックス	1つ以上のジョブを選択するには、このボックスをクリックします。
進行状況	ジョブの完了の割合を表示します。
ジョブ名	ジョブの名前を表示します。「**Extract Files**」、「**Upgrade Service**」など。
繰り返し	ジョブが繰り返しジョブであるか、繰り返しではないジョブであるかを示します。[**はい**] は繰り返しジョブ、[**いいえ**] は繰り返しではないジョブです。
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。**Investigation**、**管理**など。
所有者	ジョブの所有者を示します。ジョブの所有者はデフォルトでは**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。
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。
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。

機能	説明
アクション	[調査]の[Malware Analysis]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。
自分のジョブを表示	[**プロファイル**]ビュー > [**ジョブ**]パネルにジョブを表示します。
スケジュール	ジョブがスケジュールされた日時を示します。