RSA NETWITNESS® PLATFORM

アップグレード ガイド

RSA NetWitness® Platform 11.4.1

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、https://www.rsa.com/ja-jp/company/rsa-trademarks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

本製品はRSA 以外のサードパーティ製ソフトウェアを実装している場合があります。本製品を使用することにより、本製品のユーザは、本製品に含まれているサード 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

掲載される情報は、公開した時点でDellが正確であるとみなす情報であり、この情報は予告なく変更されることがあります。

10月 2020

目次

アップグレードの概要

RSA NetWitness® Platform 11.4.1.0には、Platformのすべての製品の機能拡張と修正が含まれています。Platformのコンポーネントは次のとおりです: NetWitness Server(Admin Server、Config Server、Integration Server、Investigate Server、Orchestration Server、Respond Server、Security Server、Source Server) 、Archiver、Broker、Concentrator、Context Hub、Decoder、Standalone Endpoint Server、Endpoint Broker、Endpoint Log Hybrid、ESAプライマリ、ESAセカンダリ、Health & Wellness Beta、Log Collector、Log Decoder、Log Hybrid、Log Hybrid Retention、Malware Analysis、Network Decoder、Network Hybrid、Reporting Engine、UEBA、Warehouse Connector

注: Reporting EngineはNetWitness Server(NW Server) ホストにインストールされ、Workbenchは Archiverホストにインストールされ、Warehouse ConnectorはDecoderまたはLog Decoderホストにインストールすることができます。

特に記載のない限り、このガイド内の手順は物理ホストと仮想ホスト(AWSとAzure Public Cloudを含む) のどちらにも適用されます。

アップグレード パス

NetWitness Platform 11.4.1.0では、以下のアップグレード パスがサポートされます。

- RSA NetWitness® Platform 11.2.x.xから11.4.1.0
- RSA NetWitness® Platform 11.3.0.xから11.4.1.0
- RSA NetWitness® Platform 11.3.1.xから11.4.1.0
- RSA NetWitness® Platform 11.3.2.xから11.4.1.0
- RSA NetWitness® Platform 11.4.0.xから11.4.1.0

RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。NetWitness Platformバージョン10.6.6.xからアップグレードする場合は、11.3.0.2にアップグレードし、11.4.0.0にアップグレードしてから、11.4から11.4.1.0にアップグレードする必要があります。10.6.6.xから11.3.0.2にアップグレードする手順については、『*RSA NetWitness Platform物理ホスト アップグレード ガイド(10.6.6.xから11.3)* 』と『*RSA NetWitness Platform仮想ホスト アップグレード ガイド(10.6.6.xから11.3)* 』を参照してください。

次のマトリックスは、サポートされているすべてのアップグレード パスを示しています。

		Target Version						
		11.2.x	11.3	11.3.0.2	11.3.1	11.3.1.1	11.3.2	11.4.x
Current Version	10.6.6	✗	✓	✓	✗	✗	✗	✗
	11.1.x	✓	✓	✗	✗	✓	✗	✗
	11.2.x	✓	✓	✗	✗	✓	✓	✓
	11.3	n/a	n/a	✗	✗	✓	✓	✓
	11.3.0.2	n/a	n/a	n/a	✓	✓	✓	✓
	11.3.1	n/a	n/a	n/a	n/a	✓	✓	✓
	11.3.2	n/a	n/a	n/a	n/a	n/a	n/a	✓

混在モード

混在モードは、最新バージョンにアップグレードされたサービスと、古いバージョンのままのサービスが混在するときに生じます。詳細については、『*RSA NetWitness Platformホストおよびサービス スタート ガイド*』の「混在モードでの実行」を参照してください。

ESAルールの導入環境に関するアップグレードの考慮事項

注意： NetWitness Platform 11.3以降のバージョンでは、ESA Correlationサービスの変更により、移行したESAルール導入環境のデータ ソースを変更する必要があります。新しいESA Correlationサービスは、11.2.x.xバージョンのEvent Stream Analysisサービスに代わるものです。

11.2.x.xから11.4以降にアップグレードする場合、移行したESAルール導入環境は、次のように変更されます。

1. 11.4以降にアップグレードする前にESAルール導入環境に2つのサービスが含まれる場合は、導入環境が2つの導入環境に分割されます。バージョン11.4以降のESAルール導入環境には、ESA Correlationサービスを1つだけ指定することができます。
2. 11.4以降にアップグレードする前に1つのESAサービスが、複数のESAルール導入環境で使用されている場合、バージョン11.4では1つの導入環境に統合されます。

古い導入環境には引き続きアクセスできます。詳細な例については、『*RSA NetWitness Platform 11.4 ESA構成ガイド*』を参照してください。

[イベント]ビューの列グループに対する変更

[イベント]ビューにロードする結果の一貫性を高めるため、列グループの列数は40個に制限されます。

11.4以降にアップグレードした後、[レガシー イベント]ビューから[イベント]ビューに移行された列グループは40列を上回っても機能します。ただし、これらのグループを編集すると、列数を40以下に減らすよう警告が表示されます。

製品ドキュメントに関するフィードバック

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

カスタマ サポートへのお問い合わせ

質問や支援が必要な場合は、以下の連絡先までお問い合わせください。

RSA Link	https://community.rsa.com/
メール	support@rsa.com

各国のお問い合わせ先	http://japan.emc.com/support/rsa/contact/phone-numbers.htm
コミュニティ	https://community.rsa.com/community/rsa-customer-support
ベーシック サポート	技術的な問題に対するテクニカル サポートは、月曜日から金曜日まで、現地時間の午前9時から午後5時までご利用いただけます。
拡張サポート	拡張サポートは、新規の重大度1の問題について24時間365日のテクニカル サポートを提供します。

Legacy Windows Collectorの更新またはインストール

重要： 現在、NW 11.2.0の環境でWindows Legacy Collector(WLC) を使用しており、NW 11.4.xへのアップグレードを計画している場合は、まず、WLCを含むすべてのコンポーネントを11.2.1または11.3にアップグレードする必要があります。その後で、すべてのコンポーネントとWLCをNW 11.4.xにアップグレードできます。

『*RSA NetWitness 11.x Windows Legacy収集の構成ガイド*』(https://community.rsa.com/docs/DOC-103165) を参照してください。

注： Windows Legacy Collectorの更新またはインストールの後、正常にログを収集できるよう、システムを再起動してください。

アップグレード タスク

注： (RSA NetWitness Endpointのお客様への注意) Endpoint Hybridは11.3.0.0以降のリリースではサポートされません。
11.2.x.xでEndpoint Hybridホストを導入し、11.3.x.xまたは11.4.0.xでEndpoint Log Hybridホストをインストールしなかった場合は、11.4.1でEndpoint Log Hybridホストをインストールする必要があります。
11.4のEndpoint Log Hybridをインストールする方法については、『*RSA NetWitness Platform 物理ホスト インストール ガイド*』または『*RSA NetWitness Platform 仮想ホスト インストール ガイド*』を参照してください。

注： プライマリNW Server(Respond Serverサービスを含む) をアップグレードした後、プライマリESAホストを11.4.1にアップグレードするまで、Respond Serverサービスは再有効化されません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

注： SDカードを使用するS4Sデバイスを使用している場合は、SSHを使用してNW Serverに接続し、アップグレード プロセスを開始する前に次のコマンドを実行します。

```
manage-stig-controls --disable-control-groups 7 --host-id <node uuid>
```

注： ホストをアップグレードする前に、各ホストの時刻がNetWitness Server上の時刻と同期していることを確認します。
時刻を同期するには、次のいずれかを実行します。
- NTPサーバを構成します。詳細については、『*システム構成ガイド*』の「NTPサーバの構成」を参照してください。
- 各ホストで次のコマンドを実行します。
1.SSHを使用してNWホストに接続します。
2.次のコマンドを実行します。

```
systemctl stop ntpd
ntpdate nw-node-zero
systemctl start ntpd
```

インターネット接続の有無に応じて、次のアップグレード方式のいずれかを選択します。アップグレード方式は、RSAが推奨する順に記載されています。

- インターネット接続時のユーザ インタフェース方式
- インターネット非接続時のユーザ インタフェース方式(11.3.1以降からのアップグレードで使用可能)
- インターネット非接続時のコマンド ライン インタフェース(CLI) 方式

どの方式でホストをアップグレードするかに関係なく、以下のルールが適用されます。

- 最初にNW Serverホストをアップグレードする必要があります。
- 既存のホストのバージョンと互換性のあるバージョンのみ適用できます。

インターネット接続時のユーザ インタフェース方式

この方式は、NW Serverホストがliveサービスに接続されており、パッケージを入手できる場合に使用できます。

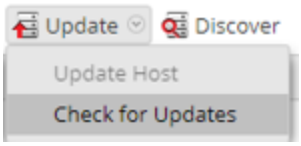
前提条件

以下の項目を確認します。

1. [**管理**]>[**システム**]>[**更新**]で、[**新しい更新の情報を毎日自動的にダウンロード**]チェックボックスがオンになっていることを確認します。
2. [**管理**]>[**ホスト**]>[**更新**]>[**更新の確認**]を実行し、更新の有無を確認します。[ホスト]ビューのステータスに[**更新あり**]が表示されることを確認します。
3. [**更新のバージョン**]列に11.4.1.0が表示されることを確認します。

手順

1. [**管理**]>[**ホスト**]に移動します。
2. NW Server(`nw-server`) ホストを選択します。
3. 最新の更新をチェックします。



4. 選択したホストの更新バージョンがローカル更新リポジトリにある場合は、[**ステータス**]列に[更新あり]と表示されます。
5. [**更新のバージョン**]列で[**11.4.1.0**]を選択します。次のガイドラインに従ってください。
   - 各更新の主な機能をダイアログに表示するには、更新バージョン番号の右側にある情報アイコン(ⓘ) をクリックします。
   - 目的のバージョンが見つからない場合は、[**更新**]>[**更新の確認**]を選択し、リポジトリ内の使用可能な更新をチェックします。更新が利用可能な場合、「新しい更新が利用可能です」というメッセージが表示され、[**ステータス**]列が自動的に更新されて、[更新あり]が表示されます。デフォルトでは、選択したホストでサポートされている更新のみが表示されます。
6. ツールバーの[**更新**]>[**ホストの更新**]をクリックします。
7. [**更新を開始**]をクリックします。
8. [**ホストの再起動**]をクリックします。
9. 他のホストについても、ステップ6～8を繰り返します。

注: NW Serverホストを更新して再起動した後でのみ、複数のホストを選択して同時にアップグレードすることができます。すべてのESA、エンドポイント、Malware Analysisホストを、NW Serverホストと同じバージョンにアップグレードする必要があります。

インターネット非接続時のユーザ インタフェース方式

注意： オフラインのユーザ インタフェース方式を使用できるのは、ホストを11.3.1.0、11.3.1.1、11.3.2.0、11.3.2.1から11.4.1.0にアップグレードする場合だけです。それよりも前のバージョンのホストをアップグレードする場合は、インターネット非接続時のコマンド ライン インタフェース(CLI) 方式を使用する必要があります。「タスク2：ステージング領域から各ホストに更新を適用する」のステップ5を完了した後で、「11.3.1.0、11.3.1.1、11.3.2.0、11.3.2.1からのアップグレード」に進みます。

注意： オフライン ユーザ インタフェース方式を使用して11.4.0.0または11.4.0.1から11.4.1.0にホストをアップグレードする場合、「タスク2：ステージング領域から各ホストに更新を適用する」のステップ5で、アップグレードが失敗し、「ダウンロード エラー」というメッセージが表示されます。このメッセージが表示されても、「11.4.0.0または11.4.0.1から11.4.1.0へのアップグレード」の手順に進み、アップグレードを正常に完了することができます。

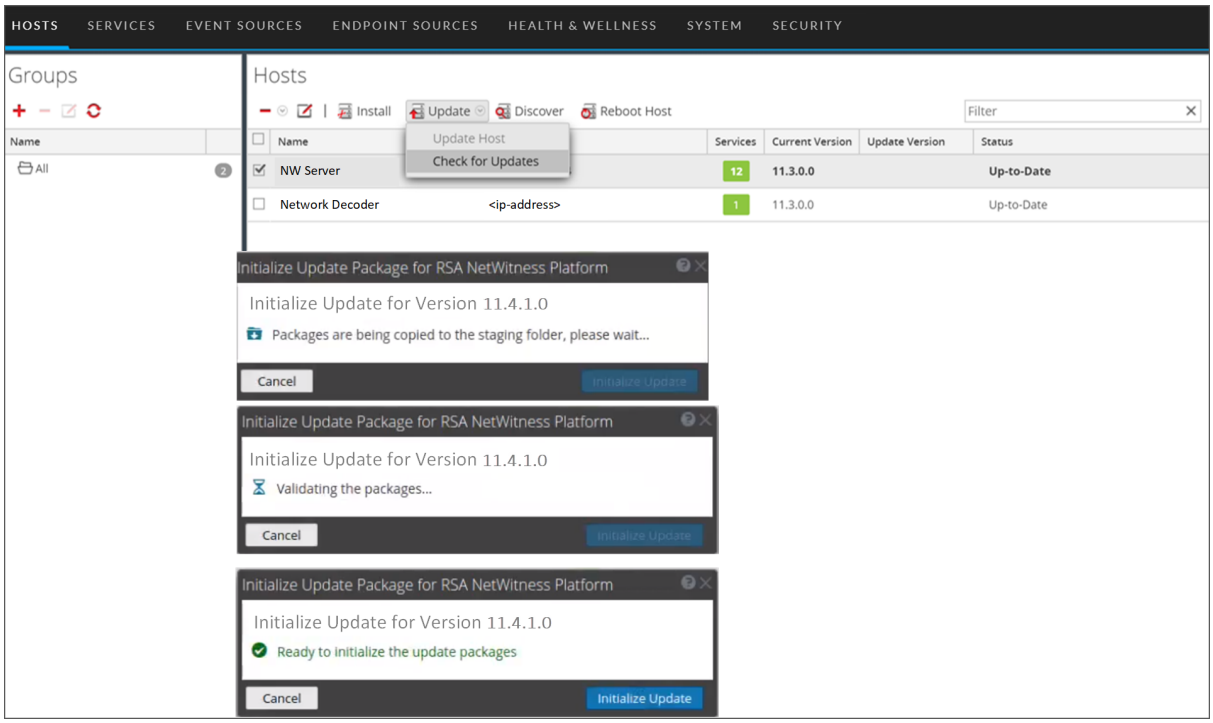
タスク1：ステージング フォルダ(/var/lib/netwitness/common/update-stage/) にバージョン更新を配置

1. RSA Link(https://community.rsa.com/) にアクセスし、[Downloads] > [NetWitness Platform] > [Version 11.4]を選択して、更新パッケージをローカル ディレクトリにダウンロードします。
   - 11.2.x.xまたは11.3.x.xからアップグレードする場合は、netwitness-11.4.0.0.zipとnetwitness-11.4.1.0.zipをダウンロードします。
   - 11.4.x.xからアップグレードする場合は、netwitness-11.4.1.0.zipをダウンロードします。
2. SSHでNW Serverホストに接続します。
3. netwitness-11.4.1.0.zip(11.2.x.xまたは11.3.x.xからアップグレードする場合はnetwitness-11.4.0.0.zipも) をローカル ディレクトリから/var/lib/netwitness/common/update-stage/ステージング フォルダにコピーします。
   例えば、次のようなコマンドを実行します。
   ```
   sudo cp /tmp/netwitness-11.4.1.0.zip /var/lib/netwitness/common/update-stage/
   ```
   注： NetWitness Platformによってファイルは自動的に解凍されます。

タスク2：ステージング領域から各ホストに更新を適用する

注意： NW Server以外のホストをアップグレードする前に、NW Serverホストをアップグレードしておく必要があります。

1. NetWitness Platformにログインします。
2. [**管理**] > [**ホスト**]に移動します。
3. 更新を確認し、更新パッケージのコピー、検証、および初期化の準備が完了するまで待ちます。

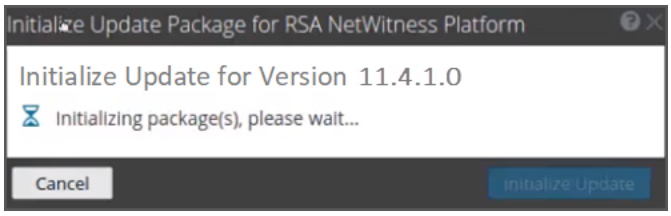


次の条件を満足すると、「更新パッケージを初期化する準備ができました」と表示されます。

- NetWitness Platformが更新パッケージにアクセスできる。
- パッケージが完全でエラーがない。

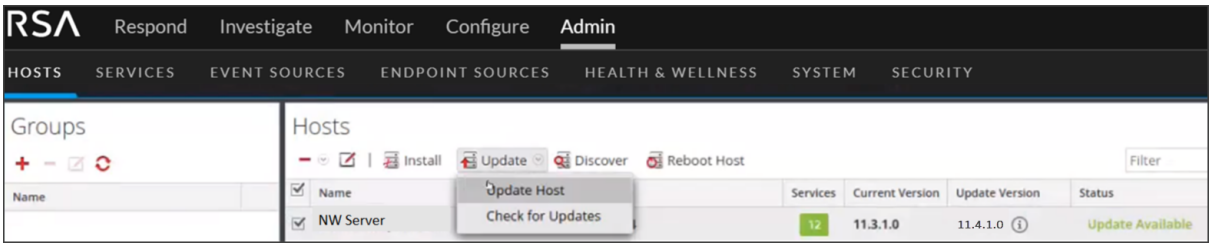
エラーのトラブルシューティング方法については、「インストールと更新のトラブルシューティング」を参照してください(たとえば、「バージョン<version-number>の導入エラー」と「次の更新 パッケージが見つかりません」が[**RSA NetWitness Platformの更新パッケージの初期化**]ダイアログに表示される場合があります) 。

4. [**更新の初期化**]をクリックします。



大きなファイルを解凍する必要があるため、パッケージの初期化には時間がかかります。
初期化が成功し、[**ステータス**]列に[更新あり]が表示されたら、残りの手順を実行してホストのアップグレードを完了します。

5. ツールバーの[**更新**]＞[**ホストの更新**]をクリックします。



11.3.1.0、11.3.1.1、11.3.2.0、11.3.2.1からのアップグレード

手順5で[**ホストの更新**]をクリックした後、次の手順を実行します。

1. [更新あり]ダイアログの[**更新を開始**]をクリックします。
   ホストのアップグレードが完了すると、ホストの再起動を求めるメッセージが表示されます。
2. ツールバーの[**ホストの再起動**]をクリックします。

11.4.0.0または11.4.0.1から11.4.1.0へのアップグレード

手順5で[**ホストの更新**]をクリックした後、「ダウンロード エラー」メッセージが表示され、アップグレードは失敗します。次の手順に従って、アップグレードを正常に完了できます。

1. コマンド ライン インタフェース(CLI) で次の手順を実行します。
   a. SSHでNW Serverに接続します。
   b. 次のコマンドを実行します。
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.4.1.0
   ```
2. NW Serverが正常に更新されたら、NetWitness Platformのユーザ インタフェースにログインし、[**管理**]＞[**ホスト**]に移動します。ホストの再起動を求めるプロンプトが表示されます。
3. ツールバーの[**ホストの再起動**]をクリックします。

その他すべてのホストは、ユーザ インタフェースから直接アップグレードできます。

1. [更新あり]ダイアログの[**更新を開始**]をクリックします。
   ホストのアップグレードが完了すると、ホストの再起動を求めるメッセージが表示されます。
2. ツールバーの[**ホストの再起動**]をクリックします。

インターネット非接続時のコマンド ライン インタフェース(CLI) 方式

「付録 A.オフライン方式(Liveサービスへの接続なし) - コマンド ライン インタフェース」の手順に従います。

アップグレード後のタスク

このトピックは、2つのセクションに分かれています。アップグレード パスに応じて、次のいずれかのセクションのタスクを完了してください。

- 11.3.x.xまたは11.4.0.xからアップグレードする場合のアップグレード後のタスク
- 11.2.x.xからアップグレードする場合のアップグレード後のタスク

11.3.x.xまたは11.4.0.xからアップグレードする場合のアップグレード後のタスク

11.3.x.xまたは11.4.0.xから11.4.1.0にアップグレードする場合は、このセクションのすべてのタスクを実行します。

全般

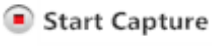
タスク1: サービスの再起動、データ収集、データ集計の確認

サービスが再起動され、データを収集していることを確認します(これは、自動開始が有効になっているかどうかによって異なります)。

必要に応じて、次のサービスでデータの収集と集計を再開します。

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

ネットワーク収集の開始

1. NetWitness Platformメニューで、[**管理**]>[**サービス**]に移動します。
   [サービス]ビューが表示されます。
2. **Decoder**サービスを選択します。
3.  (アクション)で、[**表示**]>[**システム**]を選択します。
4. ツールバーで 

をクリックします。

ログ収集の開始

1. NetWitness Platformメニューで、[**管理**]>[**サービス**]に移動します。
   [サービス]ビューが表示されます。
2. **Log Decoder**サービスを選択します。

3.  (アクション) で、[**表示**]＞[**システム**]を選択します。

4. ツールバーで  をクリックします。

集計の開始

1. NetWitness Platformメニューで、[**管理**]＞[**サービス**]を選択します。
   [サービス]ビューが表示されます。
2. **Concentrator**、**Broker**、**Archiver**の各サービスに対して、以下の手順を実行します。
   a. サービスを選択します。
   b.  (アクション) で、[**表示**]＞[**構成**]を選択します。
   c. ツールバーで  をクリックします。

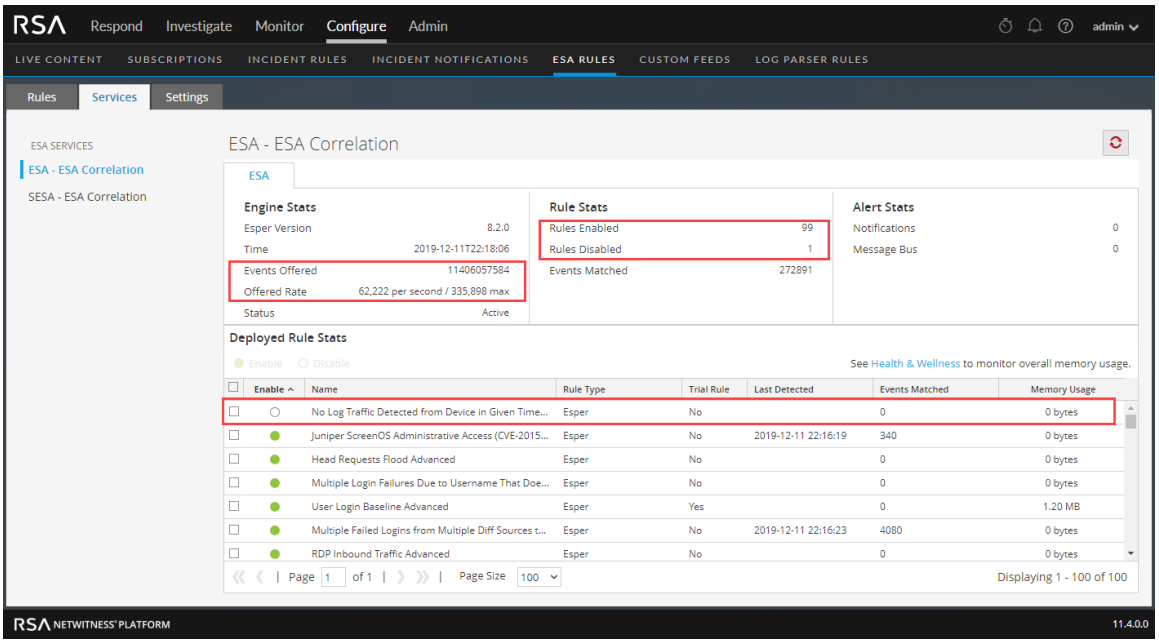
Event Stream Analysis

注： これらのEvent Stream Analysis(ESA) タスクは、11.3.x.xからアップグレードする場合に実行します。

タスク2：ESAルール導入環境のステータスの確認

ESAルール導入環境のステータスを確認します。

1. [**構成**]＞[**ESAルール**]＞[**サービス**]タブに移動します。
   [サービス]ビューが表示され、ESAサービスと導入環境のステータスが示されます。
2. 左側の[オプション]パネルで、ESAサービスを選択します。
3. リスト内の各サービスを選択し、右側のパネルで導入環境のタブを確認します。各タブは、個別のESAルール導入環境を表しています。
4. ESAルール導入環境ごとに、次の手順を実行します。
   a. [**ESAエンジンの統計情報**]セクションで、[**検出イベント数**]と[**検出レート**]を確認します。これらの統計から、データの集計と分析が適切に行われていることを確認できます。[検出イベント数]の値が0の場合は、導入環境がデータを受信していません。
   b. [**ルールの統計情報**]セクションで、[**有効なルール**]と[**無効なルール**]を確認します。無効なルールがある場合は、その下の[**導入されたルールの統計情報**]セクションで無効なルールの詳細を確認します。無効なルールには、白い丸が表示されます。有効なルールには、緑色の丸が表示されます。



5. 無効なルールを有効化する必要がある場合は、次の手順を実行します。
   a. [**構成**] > [**ESAルール**] > [**ルール**] タブに移動し、無効なルールを含んでいるESAルール導入環境を再導入します。
   b. [**サービス**] タブに戻り、ルールが無効かどうかを確認します。ルールがまだ無効な場合は、`/var/log/netwitness/correlation-server/correlation-server.log`にあるESA Correlationサービスのログファイルを確認します。

タスク3: (オプション) 最新のエンドポイント、UEBA、RSA Liveコンテンツルールのために、Multi-ValuedパラメータとSingle-Valuedパラメータのメタキーを更新

注: 11.3.0.2、11.3.1.1、11.3.2、11.4.0.xへのアップグレード時にこのタスクを完了した場合、再度実行する必要はありません。

最新のエンドポイント、UEBA、Liveコンテンツルールを使用するには、ESA Correlationサービスの**multi-valued**パラメータを更新し、**default-multi-valued**パラメータに含まれるすべてのメタキーを追加する必要があります。また、**single-valued**パラメータを更新し、**default-single-valued**パラメータに含まれるすべてのメタキーを追加する必要があります。

multi-valuedパラメータには、ESAルールが使用する文字列配列型のメタキーが表示されます。このパラメータは、NetWitness Platformバージョン11.2以前のEvent Stream Analysisサービスの**ArrayFieldNames**パラメータに相当します。

注意: `multi-valued`パラメータを変更すると、既存のルールを導入するときにエラーが発生する可能性があります。`multi-valued`パラメータを更新して、メタキーを再同期し、ESAルールを適宜更新できます。一度に報告されるエラーの数を減らすため、一度に追加するメタキーは2つまでにしてください。

注： ESA Correlationサーバのエラー ログに警告メッセージが表示される場合は、`default-multi-valued`パラメータと`multi-valued`パラメータのメタ キーの値に差異があるため、新しいエンドポイント、UEBA、Liveコンテンツ ルールが機能しません。この手順を完了すると、この問題は解決します。警告メッセージの例については、「メタ キーの不足に関するESA Correlationサーバの警告メッセージの例」を参照してください。

1. 11.4.1にアップグレードした後、**[管理]**＞**[サービス]**に移動します。[サービス]ビューでESA Correlationサービスを選択してから  ＞**[表示]**＞**[エクスプローラ]**を選択します。
2. ESA Correlationサービスの[エクスプローラ]ビューのノード リストで、**[correlation]**＞**[stream]**を選択します。
3. **`multi-valued`**パラメータのメタ キーと、**`default-multi-valued`**パラメータのメタ キーを比較します。不足している文字列配列型のメタ キーを**`default-multi-valued`**パラメータからコピーして、**`multi-valued`**パラメータにペーストします(一度に報告されるエラーの数を減らすため、一度に追加するメタ キーは2つまでにしてください)。
4. 文字列型のメタ キーを**`default-single-valued`**パラメータからコピーして、**`single-valued`**パラメータにペーストします。
5. ESA Correlationサービスに変更を適用します。
6. **[構成]**＞**[ESAルール]**に移動し、[**設定**]タブをクリックします。
   - [メタ キー参照]で、メタ再同期(更新)アイコン()をクリックします。
   - 複数のESA Correlationサービスがある場合は、各ESA Correlationサービスで同じメタ キーの変更を行います。
7. ESA詳細ルールで**`default-multi-valued`**または**`default-single-valued`**のいずれかのメタ キーを使用している場合は、ルール構文を更新します。「タスク4.(オプション) カスタムESAルール ビルダ ルールおよびESA詳細ルールの調整」も参照してください。
8. **`default-multi-valued`**パラメータのメタ キーをESAルール通知テンプレートで使用している場合は、テンプレートを更新し、メタ キーの変更を反映します。『*システム構成ガイド*』の「グローバル通知テンプレートの構成」を参照してください。
9. ESAルール導入環境を導入します。
10. ESAルール導入環境の[ESAルール]セクションでルールのエラー メッセージを確認するか、ESA Correlationサービスのエラー ログでエラーがないか確認します。
    - ESAルール導入環境のエラー メッセージを確認するには、**[構成]**＞**[ESAルール]**＞**[ルール]**タブに移動して、左側のオプション パネルで導入環境を選択し、[**ESAルール**]セクションを確認します。
    - ESA Correlationサービスのログにアクセスするには、SSHを使用してシステムに接続し、`/var/log/netwitness/correlation-server/correlation-server.log`に移動します。

タスク4.(オプション) カスタムESAルール ビルダ ルールおよびESA詳細ルールの調整

注: 11.3.0.2、11.3.1.1、11.3.2、11.4.0.xへのアップグレード時にこのタスクを完了した場合、再度実行する必要はありません。

ESAルール ビルダ ルールとESA詳細ルールを更新して、ESA Correlationサービスの`default-multi-valued`パラメータおよび`default-single valued`パラメータにリストされている文字列型および文字列配列型のメタ キーを処理できるようにします。`multi-valued`パラメータおよび`single-valued`パラメータにメタ キーを追加できます。

たとえば、`ec.outcome`を単一値メタ キーとして次に示すようにESAルールで使用しているとします。

```
@RSAAlert
SELECT * FROM Event((ec_outcome IN ( 'Success' )))
.win:time_length_batch(2 Minutes, 2)
HAVING COUNT(*) >= 2;
```

`ec.outcome`を**`multi-valued`**パラメータに追加する場合は、ルールを次に示すように更新する必要があります。

```
@RSAAlert
SELECT * FROM Event(( 'Success' = ANY( ec_outcome ) ))
.win:time_length_batch(2 Minutes, 2)
HAVING COUNT(*) >= 2;
```

詳細については、『*ESA構成ガイド*』の「ESA相関ルールの値に配列型のメタ キーを構成」を参照してください。

ESAトラブルシューティング情報

詳細については、「ESAトラブルシューティング情報」を参照してください。

Investigate

タスク5: (オプション - カスタム ロールの場合のみ) カスタム ユーザ ロールのinvestigate-server権限の調整

バージョン11.4.1にアップグレードした後、[調査]ビューを使用するアナリスト向けの標準提供ユーザ ロールでは、次の権限が有効になります。

- `investigate-server.columngroup.read`
- `investigate-server.metagroup.read`
- `investigate-server.profile.read`

11.4.1.0にアップグレードした後、NetWitness Platformはこれらの権限をカスタム アナリスト ロールには追加しないため、この手順の説明に従ってカスタム ロールでこれらの権限を有効にする必要があります(ユーザ ロールの詳細については、『*システム セキュリティおよびユーザ管理ガイド*』を参照してください)。

これらの権限が無効なカスタム ユーザ ロールを割り当てられたユーザは、[ナビゲート]ビューと[レガシー イベント]ビューで問題が発生します。3つの権限のいずれかが無効になっている場合、[ナビゲート]ビューの[値のロード]ボタンは表示されません。更に、列グループの権限が無効になっていると、[レガシー イベント]ビューには、詳細ビューのみが表示され、その他のビューや列グループを選択できないという問題が発生します。

ユーザ ロールの権限を有効にするには、次の手順を実行します。

1. [**管理**]>[**セキュリティ**]に移動し、[**ロール**]タブをクリックします。
2. 編集するカスタム ユーザ ロールを選択し、(編集アイコン)をクリックします。
3. [ロールの編集]ダイアログで、次の3つの権限を選択します。
   ```
   investigate-server.columngroup.read
   investigate-server.metagroup.read
   investigate-server.profile.read
   ```
4. [**保存**]をクリックして、変更内容を保存します。カスタム ユーザ ロールを割り当てられたアナリストがNetWitness Platformにログインすると、変更が有効になります。

Respond

これらのタスクは、プライマリESAサーバを11.4.1にアップグレードした後で実行する必要があります。

注: プライマリNW Server(Respond Serverサービスを含む)をアップグレードした後、プライマリESAホストを11.4.1にアップグレードするまで、Respond Serverサービスは再有効化されません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

タスク6:(オプション) Respondサービスの統合ルール スキーマのカスタム キーをリストアする

注: インシデント統合ルール スキーマを手動でカスタマイズしていない場合は、このタスクを実行する必要はありません。

11.xの`groupBy`句で使用するために`var/lib/netwitness/respond-server/data/aggregation_ rule_schema.json`ファイルにカスタム キーを追加した場合は、`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`ファイルを変更して、自動バックアップ ファイルからカスタム キーを追加します。

バックアップ ファイルは`/var/lib/netwitness/respond-server/data`にあり、次の形式になります。
`aggregation_rule_schema.json.bak-<time of the backup>`

タスク7 : (オプション) カスタマイズされたRespondサービスの正 規 化 スクリプトをリストアする

注 : アラート正 規 化 スクリプトを手 動でカスタマイズしていない場 合 は、このタスクを実 行 する必 要 はありません。

カスタマイズの内 容 がバージョン更 新 により上 書きされるのを防ぐため、NetWitness Platform 11.4以 降 では、カスタム正 規 化 スクリプト ファイルを利 用 できます。カスタム ロジックは、**custom_normalize_<alert type>.js**ファイルに追 加 します。

1. **/var/lib/netwitness/respond-server/scripts.bak-<timestamp>**ディレクトリにあるバックアップされたRespondサーバの正 規 化 スクリプトからカスタム ロジックを取 り出 します。<timestamp> はバックアップが完 了 した時 刻 です。
   ```
   data_privacy_map.js
   normalize_alerts.js
   normalize_core_alerts.js
   normalize_ecat_alerts.js
   normalize_ma_alerts.js
   normalize_ueba_alerts.js
   normalize_wtd_alerts.js
   utils.js
   ```
2. Edit the new 11.4 or later script files in the **/var/lib/netwitness/respond-server/scripts** directory to include any logic from the back up files. If you have any customizations in the normalization files, add them to the normalization files with the "custom" prefix.
   ```
   data_privacy_map.js
   custom_normalize_alerts.js
   custom_normalize_core_alerts.js
   custom_normalize_ecat_alerts.js
   custom_normalize_ma_alerts.js
   custom_normalize_ueba_alerts.js
   custom_normalize_wtd_alerts.js
   utils.js
   ```

   たとえば、custom_normalize_core_alerts.jsは、ESA用 のカスタム ロジックを追 加 するための正 規 化 スクリプトです。このJavaScriptファイルには、パラメータにheaders、rawAlert、Normalizealertを含 む関 数「normalizeAlert」があります。変 数「normalized」は、正 規 化 されたイベントのリストが埋 め込 まれたイミュータブルなコピー オブジェクトです。そのため、イベントに対 してカスタム メタキーを構 成 している場 合 は、「normalized.events」を反 復 的 に処 理 して、適 切 なメタキーに「rawAlert.events」オブジェクトから値 を取 得 する必 要 があります。次 にサンプル コードを示 しま

す。

```
exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) {

  // normalizedAlert is the immutable copy of ootb normalizer alert, make sure you use
  // normalized object to update/set the values in your scripts
  var normalized = Object.assign(normalizedAlert);

  // Add custom logic below
  var custom_events;

  if(normalized.events != undefined){
    custom_events = normalized.events;
  }else{
    custom_events = new Array();
  }

  for (var i = 0; i < rawAlert.events.length; i++) {

    custom_events[i].legalentity: Utils.stringValue(rawAlert.events[i].isgs_legalentity);
    custom_events[i].companycode: Utils.stringValue(rawAlert.events[i].isgs_companycode);

  }

  if(normalized.events == undefined){
    normalized.events = custom_events;
  }

  return normalized;
}
```

タスク8: (オプション) 対応の通知設定権限を追加する

注: この権限を11.2以降ですでに構成してある場合は、このタスクを実行する必要はありません。

対応の通知設定権限により、Respond管理者、データプライバシー責任者、SOCマネージャは対応の通知設定([**構成**]>[**対応の通知**])にアクセスでき、インシデントが作成または更新されたときにメール通知を送信できるようになります。

この設定にアクセスするには、既存のNetWitness Platformの標準提供ユーザロールに権限を追加する必要があります。カスタムロールにも権限を追加する必要があります。

「*NetWitness Respond構成ガイド*」の「対応の通知設定の権限」トピックを参照してください。

ユーザ権限の詳細については、「*システム セキュリティとユーザ管理ガイド*」を参照してください。

RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

11.2.x.xからアップグレードする場合のアップグレード後のタスク

11.2.x.xから11.4.1にアップグレードする場合は、このセクションのすべてのタスクを実行します。

全般

タスク1: サービスの再起動、データ収集、データ集計の確認

サービスが再起動され、データを収集していることを確認します(これは、自動開始が有効になっているかどうかによって異なります)。

必要に応じて、次のサービスでデータの収集と集計を再開します。

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

ネットワーク収集の開始

1. NetWitness Platformメニューで、[**管理**]>[**サービス**]に移動します。
   [サービス]ビューが表示されます。
2. **Decoder**サービスを選択します。
3.  (アクション)で、[**表示**]>[**システム**]を選択します。
4. ツールバーで 

をクリックします。

ログ収集の開始

1. NetWitness Platformメニューで、[**管理**]>[**サービス**]に移動します。
   [サービス]ビューが表示されます。
2. **Log Decoder**サービスを選択します。
3.  (アクション)で、[**表示**]>[**システム**]を選択します。

4. ツールバーで Start Capture をクリックします。

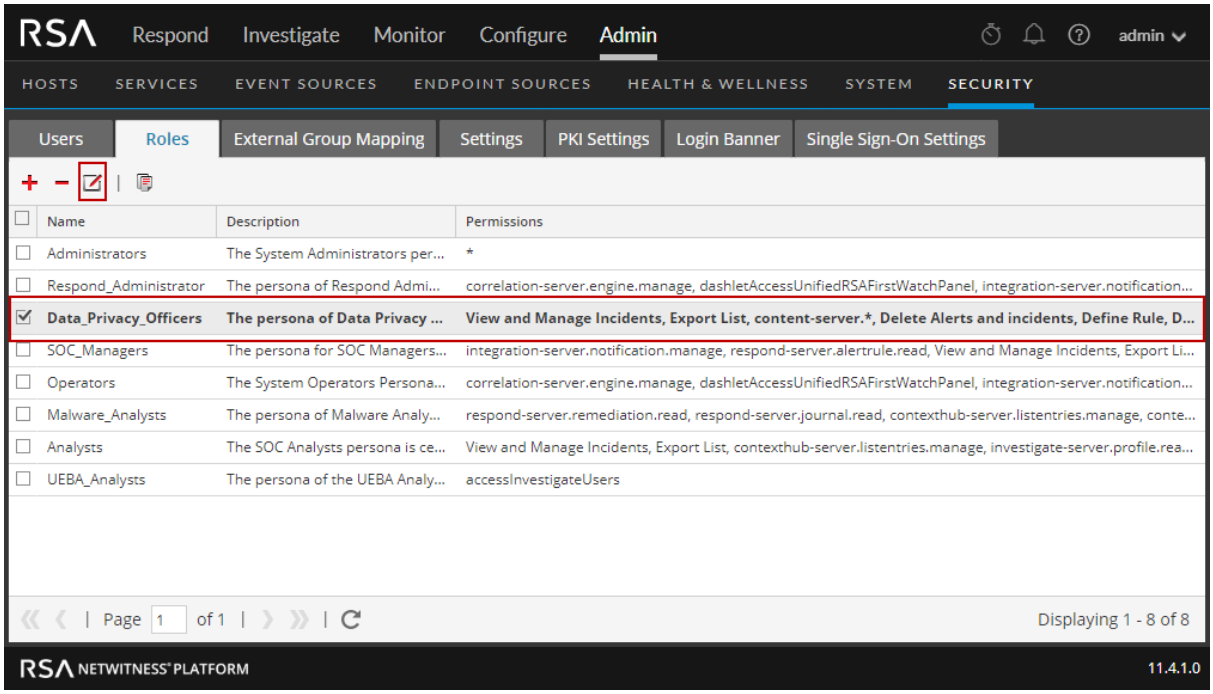
集計の開始

1. NetWitness Platformメニューで、[**管理**]＞[**サービス**]に移動します。
   [サービス]ビューが表示されます。
2. **Concentrator**、**Broker**、**Archiver**の各サービスに対して、以下の手順を実行します。
   a. サービスを選択します。
   b. (アクション)で、[**表示**]＞[**構成**]を選択します。
   c. ツールバーで Start Aggregation をクリックします。

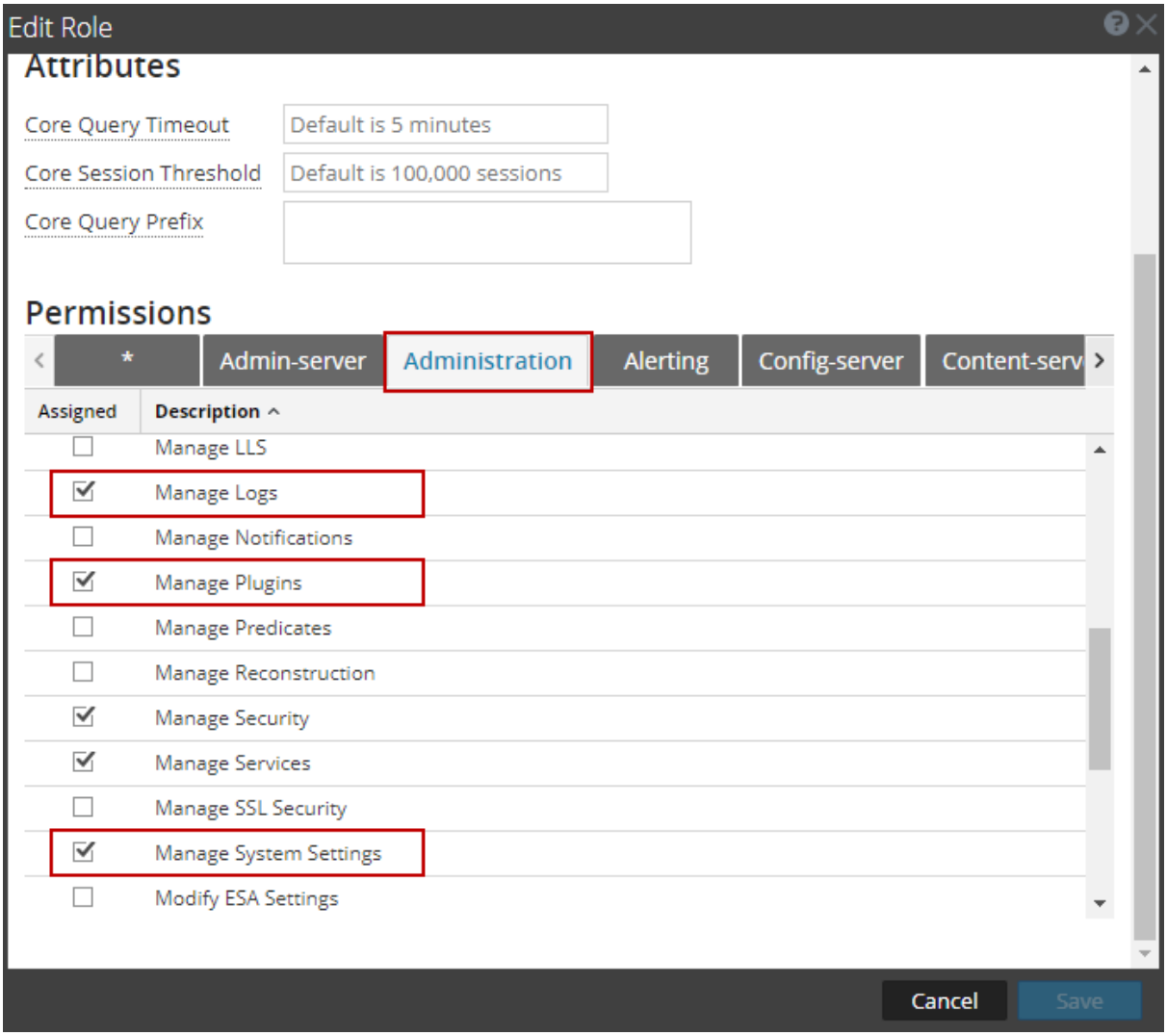
タスク2:コンテキスト メニュー アクションのユーザ権限を設定する

Analysts、**SOC Managers**、**Data Privacy Officers**の各ロールにコンテキスト メニュー アクションの権限を設定するには、次の手順を実行します。以下の手順を、**Analysts**、**SOC Managers**、**Data Privacy Officers**の各ロールに対して実行する必要があります。

1. **NetWitness Platform**メニューで、[**管理**]＞[**セキュリティ**]＞[**ロール**]を選択します。
2. ユーザ ロール(たとえば[**Data Privacy Officers**])をダブルクリックするか、ロールをクリックして選択してから(編集)をクリックします。



3. [**ロールの編集**]ビューで、[**管理**]タブの[**権限**]セクションで、[**Manage Logs**]、[**Manage Plugins**]、[**Manage System Settings**]の各チェックボックスをオンにして、[**保存**]をクリックします。



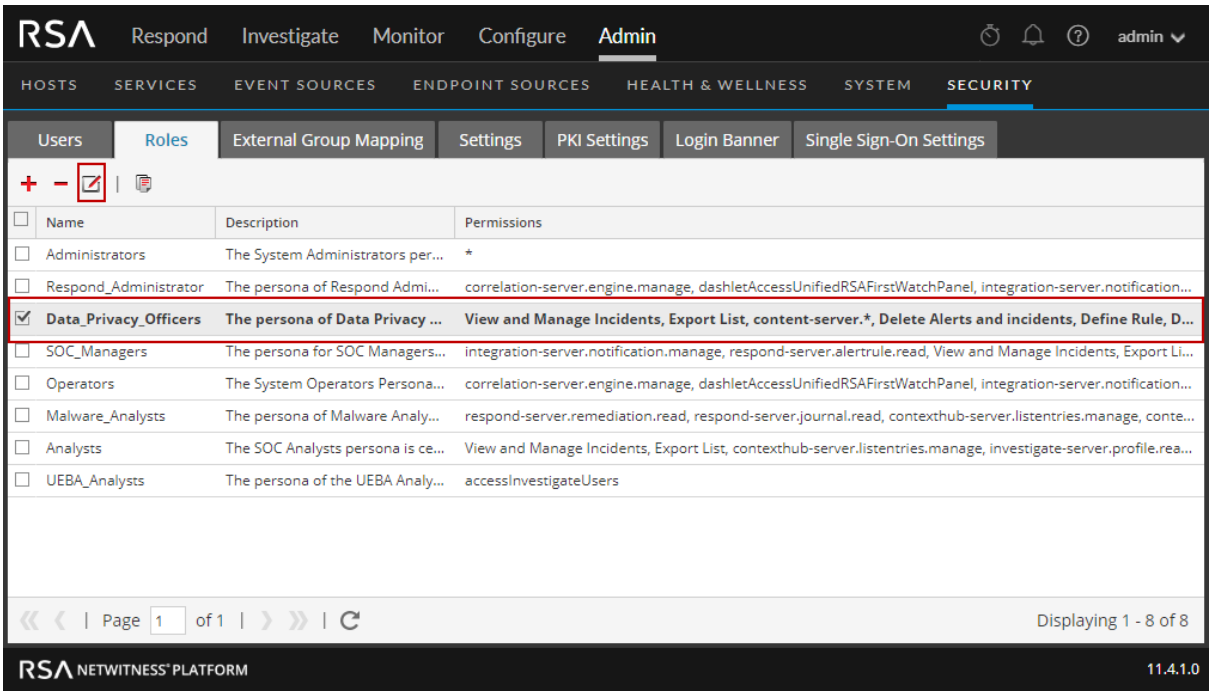
4. **Data Privacy Officers**と同様に、**Analysts**と**SOC Managers**の各ロールに対してステップ1～3を実行します。

タスク3:「Manage Jobs」権限をこの権限がないロールに追加する

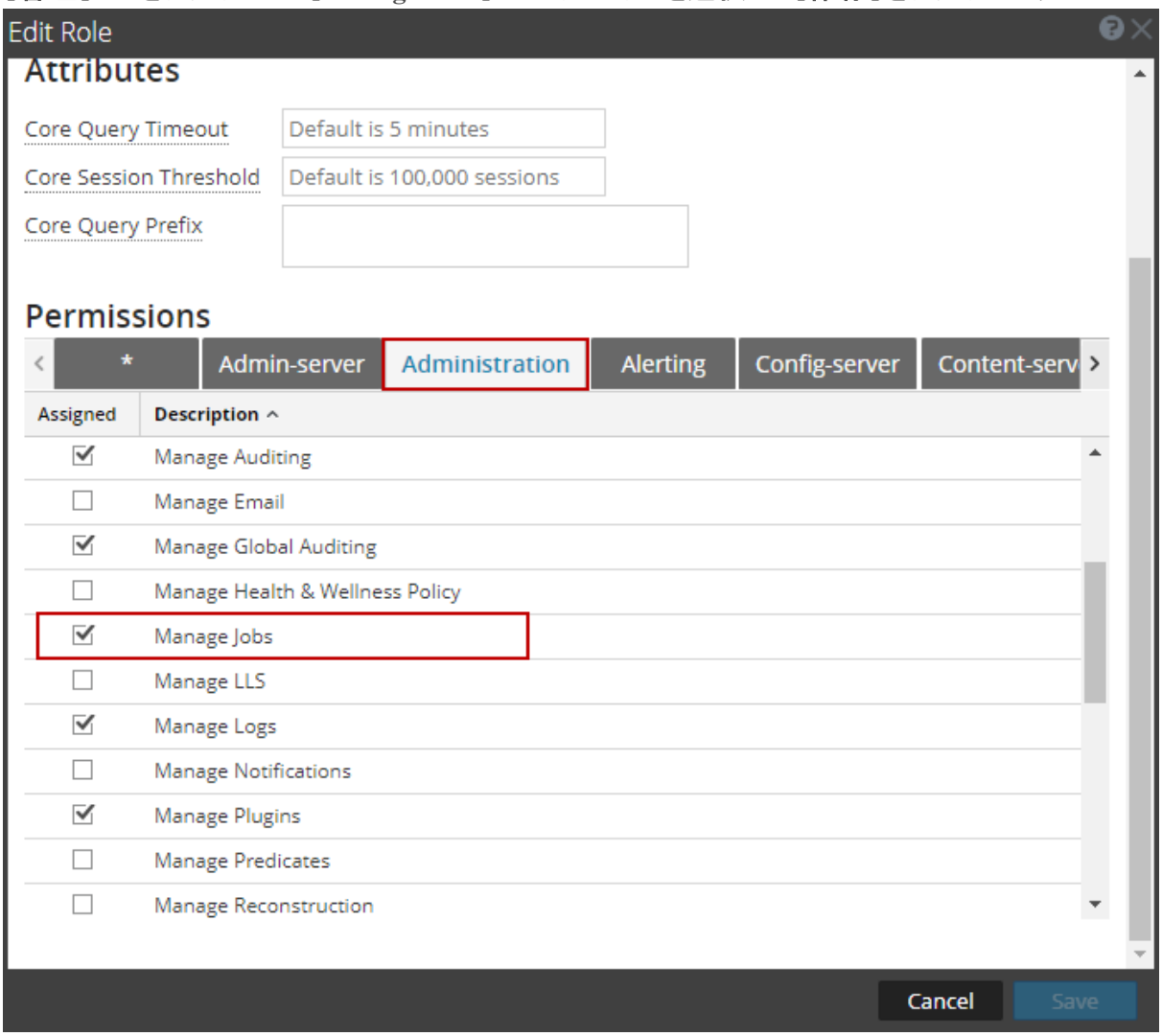
「Manage Jobs」権限を次のロールに追加します。

- SOC_Managers
- Operators
- Data_Privacy_Officers

1. **NetWitness Platform**メニューで、[**管理**]＞[**セキュリティ**]に移動して[**ロール**]をクリックします。
2. 更新する必要のあるロール(つまり、**SOC_Managers**、**Operators**、**Data_Privacy_Officers**) を1つ選択して、(編集) をクリックします。



3. [**管理**]タブをクリックして、[**Manage Jobs**]チェックボックスを選択し、[**保存**]をクリックします。



4. 3つのすべてのロール(**SOC_Managers**、**Operators**、**Data_Privacy_Officers**) について、ステップ1～3を実行します。

タスク4: (オプション) ホストの証明書を再発行する

アップグレードを行う前に、RSAが発行するCA証明書やサービス証明書などの内部証明書が更新されていることを確認しておく必要があります。

NetWitness Platformの証明書の有効期間は次のとおりです。

- 11.x導入環境のCAルート証明書は10年間有効です
- 10.6.x導入環境のCAルート証明書は5年間有効です
- サービス証明書は1,000日間有効です。

有効期限の詳細を確認するには、NetWitness Serverで`ca-expire-test-sh`スクリプトを実行します。詳細については、「RSA NetWitness Platform 11.xでのルートCAセキュリティ証明書の再発行」を参照して、スクリプトをダウンロードしてください。

CA証明書またはサービス証明書を更新するには、「RSA NetWitness Platform 11.xでのルートCAセキュリティ証明書の再発行」を参照してください。

注: 導入環境にWindows Legacy Collector(WLC) がある場合は、NetWitness Admin Serverの証明書を更新した後で、WLCの証明書を更新します。

詳細については、『*システム メンテナンス ガイド*』の「証明書の再発行」を参照してください。

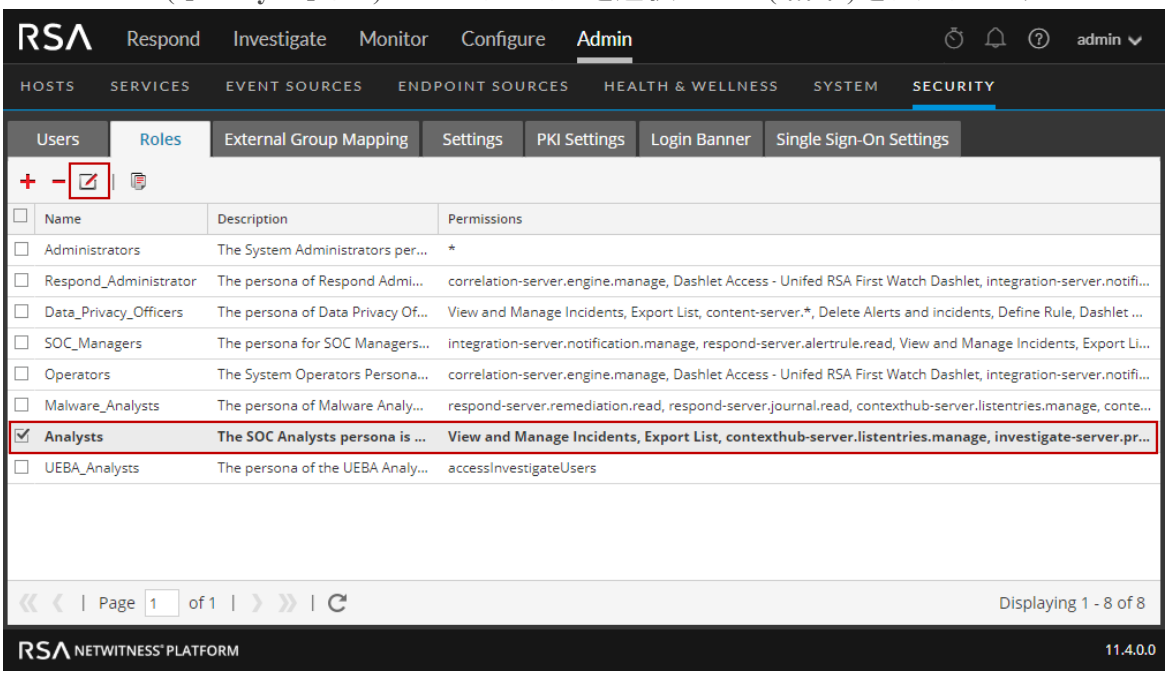
タスク5: アナリスト ロールの`investigate-server`権限を変更する

11.3以降、**SOC Managers**、**Malware Analysts**、**Analysts**の各ロールのデフォルトの権限は、[イベント分析]ビューでの表示や操作に必要な権限に限定されました。11.3より前のデフォルトの権限は異なります。

また、`predicate.manage`権限は、`get-predicates`、`edit-predicates`、`remove-predicates`、`remove-all-predicates`などへのアクセス権を付与するため、**SOC Managers**、**Malware Analysts**、**Analysts**のロールに割り当てるべきではありません。このアクセス権があると、特定のデータへのアクセスを制限する設定を回避することができるため、セキュリティリスクとなる可能性があります。

したがって、バージョン11.2.x.xから11.4以降にアップグレードする場合は、次の手順の説明に従って、デフォルトの権限を新しいデフォルトの権限と一致するように更新する必要があります。

1. [**管理**]>[**セキュリティ**]>[**ロール**]に移動します。
2. **SOC Managers**、**Malware Analysts**、**Analysts**の各ロールで、次の手順を実行します。
   a. ユーザロール([**Analysts**]など) のチェックボックスを選択し、(編集) をクリックします。



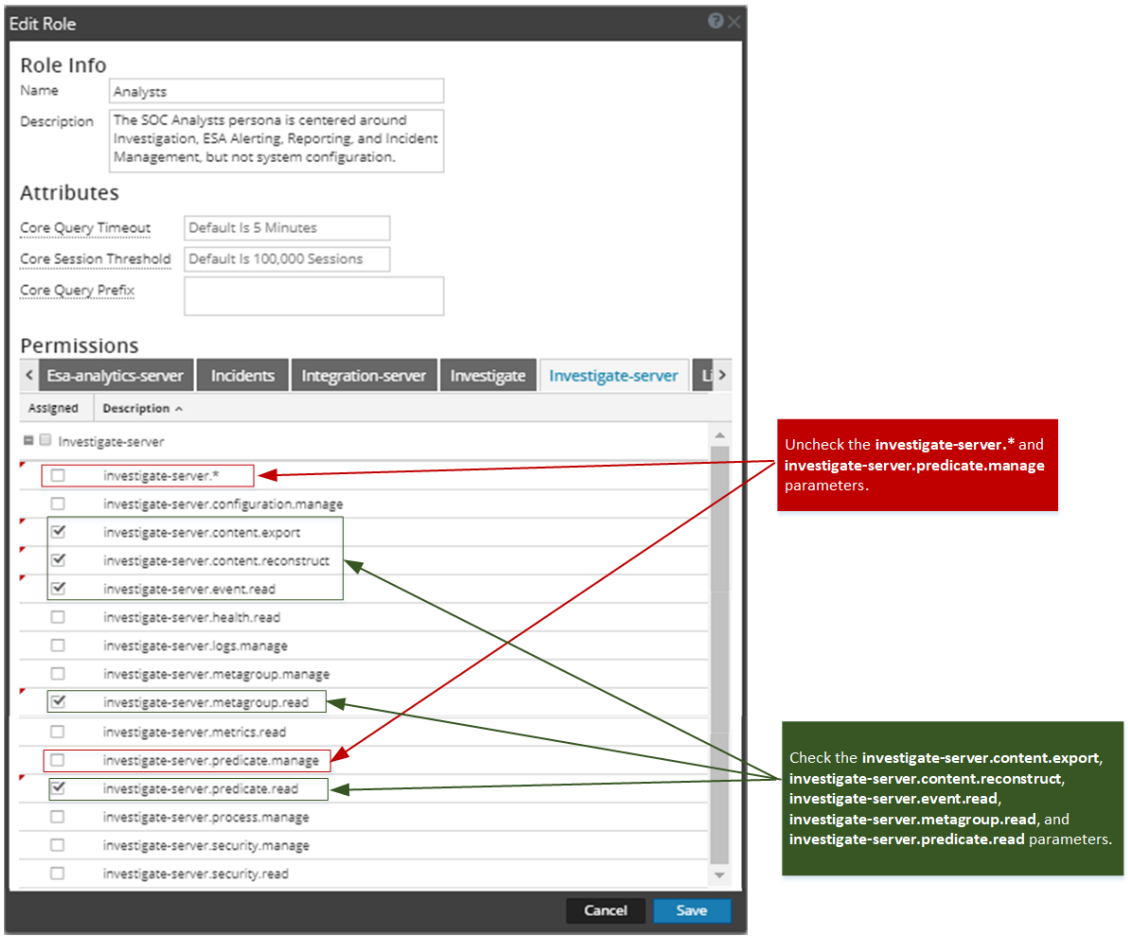
b. [**権限**]の下で[**Investigate-server**]タブをクリックします。

c. 次の権限のチェックを外します。

- `investigate-server.*`
- `investigate-server.predicate.manage`

d. 次の権限のチェックを選択します。

- `investigate-server.content.export`
- `investigate-server.content.reconstruct`
- `investigate-server.event.read`
- `investigate-server.metagroup.read`
- `investigate-server.predicate.read`



e. [**保存**]をクリックします。

タスク6: (オプション) PAM Radius認証を再構成する

11.2.x.xで`pam_radius`パッケージを使用してPAM RADIUS認証を構成していた場合、11.4以降では`pam_radius_auth`パッケージを使用して再構成する必要があります。

NW Serverホストで次のコマンドを実行します。

注： 11.2.x.xでpam_radiusを構成した場合は、ステップ1を実行して、既存のバージョンをアンインストールします。それ以外の場合は、ステップ2に進みます。

1. 既存のパッケージを確認し、既存のpam_radius ファイルをアンインストールします。
   ```
   rpm -qa |grep pam_radius
   yum erase pam_radius
   ```
2. pam_radius_authパッケージをインストールするには、次のコマンドを実行します。
   ```
   yum install pam_radius_auth
   ```
3. RADIUS構成ファイル(/etc/raddb/server) を次のように編集して、RADIUSサーバの構成を追加します。
   ```
   # server[:port] shared_secret timeout (s)
   server secret 3
   ```
   例：111.222.33.44 secret 1
4. NW ServerホストのPAM構成ファイル(/etc/pam.d/securityanalytics) を編集し、次の行を追加します。ファイルが存在しない場合は、ファイルを作成し、次の行を追加します。
   ```
   auth sufficient pam_radius_auth.so
   ```
5. 次のコマンドを実行して、/etc/raddb/serverへの書き込みアクセス権限を許可します。
   ```
   chown netwitness:netwitness /etc/raddb/server
   ```
6. 次のコマンドを実行して、pam_radius_authライブラリをコピーします。
   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```
7. pam_radius_authの構成を変更した後、次のコマンドを実行してJettyサーバを再起動します。
   ```
   systemctl restart jetty
   ```

タスク7：(オプション) NetWitness PlatformからWebアクセスできない場合は、レスポンスの.binファイルを再アップロードする(ライセンス サーバ)

NetWitness導入環境からインターネットにアクセスできない場合は、11.4以降にアップグレードした後で、レスポンスの.binファイルを再アップロードし、NetWitness Platformユーザ インターフェイスの[**管理**]＞[**システム**]＞[**ライセンス**]ビューでライセンス情報を確認する必要があります。手順については、『*ライセンス管理ガイド*』の「NetWitness Platformへのオフライン ライセンス レスポンスのアップロード」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

タスク8：パスワードの最小長を8文字から9文字に変更する

バージョン11.2.x.xでは、NetWitness Platformの最小パスワード長は8文字です。11.3.x.x以降では、最小長は9文字です。11.2.x.xから11.4以降にアップグレードした後、『*システム セキュリティおよびユーザ管理ガイド*』の「パスワードの複雑性の構成」の説明に従って、最小パスワード長を9文字に設定します。

Event Stream Analysis

注： これらのEvent Stream Analysis(ESA) タスクは、11.2.x.xからアップグレードする場合に実行します。

タスク9: ESA Correlationサービスの文字列配列型メタキーの表示と次のステップ

エンドポイント、UEBA、RSA Liveコンテンツをサポートするため、11.3以降のESA Correlationサービスでは、いくつかのメタキーを単一値(文字列)から複数値(文字列配列)に変更する必要がありました。また、追加の文字列メタキーも必要になりました。

ESAルールで使用されているメタキーが、最新のデフォルトの複数値メタキーと異なる場合、ESAルールは引き続き機能しますが、今後も確実にルールが正しく導入されるよう、できるだけ早急に新しいメタキーを使用してESAルールを更新してください。

ESA Correlationサービスには、次のような複数値(文字列配列)と単一値(文字列)に関するパラメータがあります。

- **multi-valued**: ESAルールで現在使用されている文字列配列メタキーを示します。NetWitness Platform 11.4以降にアップグレードした環境では、アップグレード前の既存の文字列配列メタキーが表示されます(このパラメータは、NetWitness Platformバージョン11.2以前のEvent Stream Analysisサービスの`ArrayFieldNames`パラメータに相当します)。
- **single-valued**: ESAルールで現在使用されている文字列メタキーを示します。NetWitness Platform 11.4以降にアップグレードした環境では、このパラメータの値は空です。
- **default-multi-valued**: 最新バージョンで必須の文字列配列メタキーを示します。
- **default-single-valued**: 最新バージョンで必須の文字列メタキーを示します。

注: `single-valued`パラメータと`multi-valued`パラメータに同じメタキーが設定されている場合は、`single-valued`パラメータの設定が`multi-valued`パラメータの設定よりも優先されます。

1. ESA Correlationサービスの`multi-valued`パラメータおよび`single-valued`パラメータに設定されたメタキーを表示します。
   a. **[管理]**>**[サービス]**に移動し、[サービス]ビューでESA Correlationサービスを選択してから  >**[表示]**>**[エクスプローラ]**を選択します。
   b. ESA Correlationサービスの[エクスプローラ]ビューのノードリストで、**[correlation]**>**[stream]**を選択します。
2. ESAルールは引き続き機能しますが、Live、UEBA、エンドポイントのルールを使用する場合は、「タスク12.(オプション)最新のエンドポイント、UEBA、RSA Liveコンテンツ ルールのために、Multi-ValuedパラメータとSingle-Valuedパラメータのメタキーを更新」の手順を実行してください。

注意: `multi-valued`パラメータを変更すると、既存のルールを導入するときにエラーが発生する可能性があります。`multi-valued`パラメータを更新して、メタキーを再同期し、ESAルールを適宜更新できます。一度に報告されるエラーの数を減らすため、一度に追加するメタキーは2つまでにしてください。

注: 複数のESA Correlationサービスを使用している場合は、すべてのESA Correlationサービスで同じ`multi-valued`パラメータおよび`single-valued`パラメータを指定する必要があります。

タスク10: (オプション) メタ キーが文字列から配列に変更されたRSA Live ESAルールを更新する

次の表は、NetWitness Platform 11.3.xおよび11.4で文字列から配列にタイプが変更されたメタ キーを使用するRSA Live ESAルールの一覧です。

ルール番号	ルール名	11.3.xおよび11.4の配列タイプのメタ キー
1	RIG Exploit Kit	threat_category
2	AWS Critical VM Modified	alert
3	Multiple Successful Logins from Multiple Diff Src to Same Dest	host.srcとhost.dst
4	Multiple Successful Logins from Multiple Diff Src to Diff Dest	host.srcとhost.dst
5	Multiple Failed Logins from Multiple Diff Sources to Same Dest	host.srcとhost.dst
6	Multiple Failed Logins from Multiple Users to Same Destination	host.srcとhost.dst
7	User Login Baseline	host.srcとhost.dst

1. 次のいずれかを実行します。
   - バージョン11.3以前にこれらのルールを導入していた場合は、次の手順を実行します。
     a. ご使用の環境に適応するようルールのパラメータを変更していた場合は、変更内容を記録します。
     b. 最新のルールをRSA Liveからダウンロードします。
     c. デフォルトのルール パラメータに同じ変更を行い、ルールを導入します。
     (手順については、『*ESA相関ルール アラート ユーザ ガイド*』の「RSA Live ESAルールのダウンロード」を参照してください。)
   - バージョン11.4以降でこれらのルールを初めて導入する場合は、ESAルールの説明に従いカスタマイズしてください。前掲の表のルール3～7では、ESAのエンリッチメント ソースとして、 `User_Whitelist`、`Host_Whitelist` 、`IP_Whitelist`のContext Hubリストを追加する必要があります。(『*ESA相関ルール アラート ユーザ ガイド*』の「Context Hubリストをエンリッチメント ソースとして構成」を参照。)
2. これらのルールを追加したESAルール導入環境を導入します。(『*ESA相関ルール アラート ユーザ ガイド*』の「ESAルールの導入ステップ」を参照。)

タスク11：ESAルール導入環境を検証する

11.4以降にアップグレードした後で、ESAルール導入環境を検証します。ESAホストごとに、「<ESA-Hostname> – ESA Correlation」という名前の新しい導入環境が作成されます。

1. 新しい導入環境が作成されたことを確認します。
2. 新しい導入環境に、ESA Correlationサービス、データソース、以前そのESAホストの導入環境に追加されていたルールが指定されていることを確認します。
3. ESA Correlationサービスのステータスが、「導入済み」であることを確認します。
4. ESAルールのステータスが間違って「無効」と表示されたり、[ステータス]列に  アイコンが表示される場合は、問題を特定してルールを修正する必要があります。無効なルールにエラーメッセージがある場合は、[ステータス]フィールドに  が表示されるようになりました。エラーログに移動することなく、ルールにカーソルを合わせるとエラーメッセージのツールチップが表示されます。(ESA Correlationサービスのログファイルは、`/var/log/netwitness/correlation-server/correlation-server.log`にあります)。
   「ESAトラブルシューティング情報」を参照してください。
5. ESAルール導入環境全体のステータスを確認します。ESAルール導入環境に問題がない場合は、ESAサービスとESAルールのステータスは「導入済み」になり、データソースに緑色の丸が表示され、[**今すぐ導入**]ボタンは無効になります。

詳細な例については、『*ESA構成ガイド*』を参照してください。導入環境の詳細については、『*ESA相関ルール アラート ユーザガイド*』の「ESAルールの導入ステップ」を参照してください。トラブルシューティングの詳細については、『*ESA相関ルール アラート ユーザガイド*』を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

タスク12.(オプション) 最新のエンドポイント、UEBA、RSA Liveコンテンツ ルールのために、Multi-ValuedパラメータとSingle-Valuedパラメータのメタ キーを更新

最新のエンドポイント、UEBA、Liveコンテンツ ルールを使用するには、ESA Correlationサービスの**multi-valued**パラメータを更新し、**default-multi-valued**パラメータに含まれるすべてのメタ キーを追加する必要があります。また、**single-valued**パラメータを更新し、**default-single-valued**パラメータに含まれるすべてのメタ キーを追加する必要があります。

注意： `multi-valued`パラメータを変更すると、既存のルールを導入するときにエラーが発生する可能性があります。`multi-valued`パラメータを更新して、メタ キーを再同期し、ESAルールを適宜更新できます。一度に報告されるエラーの数を減らすため、一度に追加するメタ キーは2つまでにしてください。

注： ESA Correlationサーバのエラーログに警告メッセージが表示される場合は、`default-multi-valued`パラメータと`multi-valued`パラメータのメタ キーの値に差異があるため、新しいエンドポイント、UEBA、Liveコンテンツ ルールが機能しません。この手順を完了すると、この問題は解決します。警告メッセージの例については、「メタ キーの不足に関するESA Correlationサーバの警告メッセージの例」を参照してください。

1. 11.4以降にアップグレードした後で、**[管理]＞[サービス]**に移動し、[サービス]ビューでESA Correlationサービスを選択してから、  ＞**[表示]＞[エクスプローラ]**を選択します。

2. ESA Correlationサービスの[エクスプローラ]ビューのノード リストで、[**correlation**]＞[**stream**]を選択します。
3. **multi-valued**パラメータのメタ キーと、**default-multi-valued**パラメータのメタ キーを比較します。不足している文字列配列型のメタ キーを**default-multi-valued**パラメータからコピーして、**multi-valued**パラメータにペーストします(一度に報告されるエラーの数を減らすため、一度に追加するメタ キーは2つまでにしてください) 。
4. 文字列型のメタ キーを**default-single-valued**パラメータからコピーして、**single-valued**パラメータにペーストします。
5. ESA Correlationサービスに変更を適用します。
6. [**構成**]＞[**ESAルール**]に移動し、[**設定**]タブをクリックします。
   - [メタ キー参照]で、メタ再同期(更新) アイコン( ) をクリックします。
   - 複数のESA Correlationサービスがある場合は、各ESA Correlationサービスで同じメタ キーの変更を行います。
7. ESA詳細ルールで**default-multi-valued**または**default-single-valued**のいずれかのメタ キーを使用している場合は、ルール構文を更新します。「タスク13.(オプション) カスタムESAルール ビルダ ルールおよびESA詳細ルールの調整」も参照してください。
8. **default-multi-valued**パラメータのメタ キーをESAルール通知テンプレートで使用している場合は、テンプレートを更新し、メタ キーの変更を反映します。『*システム構成ガイド*』の「グローバル通知テンプレートの構成」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。
9. ESAルール導入環境を導入します。
10. ESAルール導入環境の[ESAルール]セクションでエラー メッセージに関するルールを確認するか、ESA相関エラー ログでエラーを確認します。
    - ESAルール導入環境のエラー メッセージを確認するには、[**構成**]＞[**ESAルール**]＞[**ルール**]タブに移動して、左側のオプション パネルで導入環境を選択し、[**ESAルール**]セクションを確認します。
    - ESA Correlationサービスのログにアクセスするには、SSHを使用してシステムに接続し、`/var/log/netwitness/correlation-server/correlation-server.log`に移動します。

タスク13.(オプション) カスタムESAルール ビルダ ルールおよびESA詳細ルールの調整

ESAルール ビルダ ルールとESA詳細ルールを更新して、ESA Correlationサービスの`default-multi-valued`パラメータおよび`default-single valued`パラメータにリストされている文字列型および文字列配列型のメタ キーを処理できるようにします。`multi-valued`パラメータおよび`single-valued`パラメータにメタ キーを追加できます。

たとえば、`ec.outcome`を単一値メタ キーとして次に示すようにESAルールで使用しているとします。

```
@RSAAlert
SELECT * FROM Event((ec_outcome IN ( 'Success' )))
.win:time_length_batch(2 Minutes, 2)
```

```
HAVING COUNT(*) >= 2;
```

ec.outcomeを**multi-valued**パラメータに追加する場合は、ルールを次に示すように更新する必要があります。

```
@RSAAlert
SELECT * FROM Event(( 'Success' = ANY( ec_outcome ) ))
.win:time_length_batch(2 Minutes, 2)
HAVING COUNT(*) >= 2;
```

詳細については、『*ESA構成ガイド*』の「ESA相関ルールの値に配列型のメタキーを構成」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

ESAトラブルシューティング情報

注：不要な処理のオーバーヘッドを回避するため、値にテキストデータを含まないメタキーについては、ESAルールビルダの[ステートメントのビルド]ダイアログから[大文字小文字区別なし]オプションが削除されました。11.4へのアップグレード時に、NetWitness Platformは、既存のルールの[大文字小文字区別なし]オプションを変更しません。既存のルールビルダルールで、[大文字小文字区別なし]オプションを使用できなくなったメタキーでこのオプションが選択されている場合、そのステートメントを編集し、チェックボックスをオフにしないで再保存しようとするとエラーが発生します。

エンドポイントおよびUEBAのコンテンツに加え、Liveで提供するESAルールの変更に対応するため、ESA Correlationサービスでは、いくつかのメタキーを単一値(文字列)から複数値(文字列配列)に変更する必要がありました。NetWitness Platform 11.4では、文字列から文字列配列への変更があった場合、ESAによってルールステートメントの演算子が自動的に調整されますが、手動で調整が必要となる場合もあります。

11.4以降で文字列型のメタキーを文字列配列型のメタキーに手動で変更するには、『*ESA構成ガイド*』の「ESA相関ルールの値に配列型のメタキーを構成」を参照してください。

最新のエンドポイント、UEBA、Liveコンテンツルールを使用するには、NetWitness Platformバージョン11.4以降のESA Correlationサービスでは、次のデフォルトの**複数値**メタキーが必要です。

```
action , alert , alert.id , alias.host , alias.ip , alias.ipv6 , analysis.file
, analysis.service , analysis.session , boc , browserprint , cert.thumbprint ,
checksum , checksum.all , checksum.dst , checksum.src , client.all , content ,
context , context.all , context.dst , context.src , dir.path , dir.path.dst ,
dir.path.src , directory , directory.all , directory.dst , directory.src ,
email , email.dst , email.src , eoc , feed.category , feed.desc , feed.name ,
file.cat , file.cat.dst , file.cat.src , filename.dst , filename.src , filter
, function , host.all , host.dst , host.orig , host.src , host.state ,
inv.category , inv.context , ioc , ip.orig , ipv6.orig , netname , OS , param
, param.dst , param.src , registry.key , registry.value , risk , risk.info ,
risk.suspicious , risk.warning , threat.category , threat.desc , threat.source
, user.agent , username
```

NetWitness Platform 11.4以降のESA Correlationサービスでは、次のデフォルトの**単一値**メタキーも必要です。

```
accesses , context.target , file.attributes , logon.type.desc , packets
```

変更された文字列配列メタキーまたは文字列メタキーをESAルール通知テンプレートで使用している場合は、テンプレートを更新し、メタキーの変更を反映します。『*システム構成ガイド*』の「グローバル通知テンプレートの構成」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

注： 詳細EPLルールが無効になった場合は、自動的に更新されないため、手動で修正する必要があります。

トラブルシューティングの詳細については、『*RSA NetWitness Platform ESA相関ルール アラート ユーザ ガイド*』の「ESAのトラブルシューティング」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

メタ キーの不足に関するESA Correlationサーバの警告メッセージの例

ESA Correlationサーバのエラー ログに警告メッセージが表示される場合は、`default-multi-valued`パラメータと`multi-valued`パラメータのメタ キーの値に差異があるため、新しいエンドポイント、UEBA、Liveコンテンツ ルールが機能しません。「タスク12.(オプション) 最新のエンドポイント、UEBA、RSA Liveコンテンツ ルールのために、Multi-ValuedパラメータとSingle-Valuedパラメータのメタ キーを更新」の手順を実行すると、この問題を修正できます。

複数値の警告メッセージの例

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id,
browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_
src, client_all, content, context, context_all, context_dst, context_src, dir_
path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst,
directory_src, email_dst, email_src, feed_category, feed_desc, feed_name,
file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter,
function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_
orig, OS, param, param_dst, param_src, registry_key, registry_value, risk,
risk_info, risk_suspicious, risk_warning, threat_category, threat_desc,
threat_source, user_agent] are still MISSING from multi-valued
```

単一値の警告メッセージの例

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_target,
file_attributes, logon_type_desc, packets] are still MISSING from single-
valued
```

Investigate

タスク14.(オプション - カスタム ロールの場合のみ) カスタム ユーザ ロールのinvestigate-server権限の調整

バージョン11.4以降にアップグレードした後、[調査]ビューを使用するアナリスト向けの標準提供ユーザ ロールでは、次の権限が有効になります。

- `investigate-server.columngroup.read`
- `investigate-server.metagroup.read`
- `investigate-server.profile.read`

11.4以降にアップグレードした後、NetWitness Platformはこれらの権限をカスタム アナリスト ロールには追加しないため、この手順の説明に従ってカスタム ロールでこれらの権限を有効にする必要があります(ユーザ ロールの詳細については、『*システム セキュリティおよびユーザ管理ガイド*』を参照してください) 。

これらの権限が無効なカスタム ユーザ ロールを割り当てられたユーザは、[ナビゲート]ビューと[レガシー イベント]ビューで問題が発生します。3つの権限のいずれかが無効になっている場合、[ナビゲート]ビューの[値のロード]ボタンは表示されません。更に、列グループの権限が無効になっていると、[レガシー イベント]ビューには、詳細ビューのみが表示され、その他のビューや列グループを選択できないという問題が発生します。

ユーザ ロールの権限を有効にするには、次の手順を実行します。

1. [**管理**]＞[**セキュリティ**]に移動し、[**ロール**]タブをクリックします。
2. 編集するカスタム ユーザ ロールを選択し、  (編集アイコン)をクリックします。
3. [ロールの編集]ダイアログで、次の3つの権限を選択します。
   ```
   investigate-server.columngroup.read
   investigate-server.metagroup.read
   investigate-server.profile.read
   ```
4. [**保存**]をクリックして、変更内容を保存します。カスタム ユーザ ロールを割り当てられたアナリストがNetWitness Platformにログインすると、変更が有効になります。

Respond

これらのタスクは、プライマリESAサーバを11.4.1にアップグレードした後で実行する必要があります。

注: プライマリNW Server(Respond Serverサービスを含む)をアップグレードした後、プライマリESAホストを11.4.1にアップグレードするまで、Respond Serverサービスは再有効化されません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

タスク15: (オプション) Respondサービスの統合ルール スキーマのカスタム キーをリストアする

注: インシデント統合ルール スキーマを手動でカスタマイズしていない場合は、このタスクを実行する必要はありません。

11.xの`groupBy`句で使用するために`var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`ファイルにカスタム キーを追加した場合は、`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`ファイルを変更して、自動バックアップ ファイルからカスタム キーを追加します。

バックアップ ファイルは`/var/lib/netwitness/respond-server/data`にあり、次の形式になります。
`aggregation_rule_schema.json.bak-<time of the backup>`

タスク16: (オプション) カスタマイズされたRespondサービスの正規化スクリプトをリストアする

注: アラート正規化スクリプトを手動でカスタマイズしていない場合は、このタスクを実行する必要はありません。

カスタマイズの内容がバージョン更新により上書きされるのを防ぐため、NetWitness Platform 11.4以降では、カスタム正規化スクリプト ファイルを利用できます。カスタム ロジックは、**custom_normalize_<alert type>.js**ファイルに追加します。

1. **/var/lib/netwitness/respond-server/scripts.bak-<timestamp>**ディレクトリにあるバックアップされたRespondサーバの正規化スクリプトからカスタム ロジックを取り出します。<timestamp>はバックアップが完了した時刻です。
   ```
   data_privacy_map.js
   normalize_alerts.js
   normalize_core_alerts.js
   normalize_ecat_alerts.js
   normalize_ma_alerts.js
   normalize_ueba_alerts.js (11.3以降のバージョン)
   normalize_wtd_alerts.js
   utils.js
   ```
2. **/var/lib/netwitness/respond-server/scripts**ディレクトリの新しい11.4スクリプト ファイルを編集して、バックアップ ファイルから取得したロジックを追加します。正規化ファイルをカスタマイズする場合は、「custom」のプレフィックスが付いた正規化ファイルに追加します。
   ```
   data_privacy_map.js
   custom_normalize_alerts.js
   custom_normalize_core_alerts.js
   custom_normalize_ecat_alerts.js
   custom_normalize_ma_alerts.js
   custom_normalize_ueba_alerts.js
   custom_normalize_wtd_alerts.js
   utils.js
   ```

   たとえば、custom_normalize_core_alerts.jsは、ESA用のカスタム ロジックを追加するための正規化スクリプトです。このJavaScriptファイルには、パラメータにheaders、rawAlert、Normalizealertを含む関数「normalizeAlert」があります。変数「normalized」は、正規化されたイベントのリストが埋め込まれたイミュータブルなコピー オブジェクトです。そのため、イベントに対してカスタム メタキーを構成している場合は、「normalized.events」を反復的に処理して、適切なメタキーに「rawAlert.events」オブジェクトから値を取得する必要があります。次にサンプル コードを示しま

す。

```
exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) {

  // normalizedAlert is the immutable copy of ootb normalizer alert, make sure you use
  // normalized object to update/set the values in your scripts
  var normalized = Object.assign(normalizedAlert);

  // Add custom logic below
  var custom_events;

  if(normalized.events != undefined){
    custom_events = normalized.events;
  }else{
    custom_events = new Array();
  }

  for (var i = 0; i < rawAlert.events.length; i++) {

    custom_events[i].legalentity: Utils.stringValue(rawAlert.events[i].isgs_legalentity);
    custom_events[i].companycode: Utils.stringValue(rawAlert.events[i].isgs_companycode);

  }

  if(normalized.events == undefined){
    normalized.events = custom_events;
  }

  return normalized;
}
```

タスク17: (オプション) 対応の通知設定権限を追加する

注: この権限を11.2以降ですでに構成してある場合は、このタスクを実行する必要はありません。

対応の通知設定権限により、Respond管理者、データプライバシー責任者、SOCマネージャは対応の通知設定([**構成**]>[**対応の通知**])にアクセスでき、インシデントが作成または更新されたときにメール通知を送信できるようになります。

この設定にアクセスするには、既存のNetWitness Platformの標準提供ユーザロールに権限を追加する必要があります。カスタムロールにも権限を追加する必要があります。

「*NetWitness Respond構成ガイド*」の「対応の通知設定の権限」トピックを参照してください。

ユーザ権限の詳細については、「*システム セキュリティとユーザ管理ガイド*」を参照してください。

RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

DecoderおよびLog Decoder

タスク18: Javaバージョンの変更のため、レガシーEndpointからの定期実行フィードを再構成する

Javaバージョンの変更により、レガシーEndpointの定期実行フィードを再構成する必要があります。この問題を解決するには、次の手順を実行します。

- 『*RSA NetWitness Endpoint統合ガイド*』にある「定期実行フィードにより取得するEndpointからのコンテキスト データの構成」トピックの「NetWitness EndpointのSSL証明書のエクスポート」の説明に従い、NetWitness Endpoint CA証明書をNetWitness Platformのトラスト ストアにインポートします。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

Endpointインストール タスク

11.4リレー サーバのインストール

リレー サーバを構成した場合は、次の手順を実行します。

1. アップグレードされたEndpoint Serverからリレー サーバのインストーラをダウンロードし、リレー サーバを11.4にアップグレードする必要があります。詳細については、『*Endpoint構成ガイド*』の「(オプション) リレー サーバのインストールと構成」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。
2. 次のコマンドを使用して、Endpoint Serverを再起動します。

   ```
   systemctl restart rsa-nw-endpoint-server
   ```

Endpointエージェントのアップグレード

エージェントをアップグレードする方法については、『*NetWitness Platform 11.4 Endpointエージェント インストール ガイド*』の「エージェントのアップグレード」を参照してください。

NetWitness UEBAアップグレード後のタスク

以下のセクションでは、NetWitness UEBAをインストールおよびアップグレードするためのタスクについて説明します。

(オプション) UEBA構成の更新

UEBA構成の主要パラメータを取得するには、UEBAマシンで次のcurlコマンドを実行します。

```
curl http://localhost:8888/application-default.properties
```

次のような主要パラメータが返されます。

- `uiIntegration.brokerId`: NWデータ ソース(Broker/Concentrator) のサービスID。
- `dataPipeline.schemas`: UEBAによって処理されるスキーマのリスト。
- `dataPipeline.startTime`: UEBAがNetWitnessデータ ソースからデータの取得を開始した日付。
- `outputForwarding.enableForwarding`: UEBA転送のステータス。

(オプション) パケット スキーマの追加

NetWitness Platform 11.4がパケット収集を実行するように構成されている場合は、NetWitness UEBAにパケット スキーマを追加できます。

パケット スキーマを追加するには、UEBAサーバで次のコマンドを実行します。

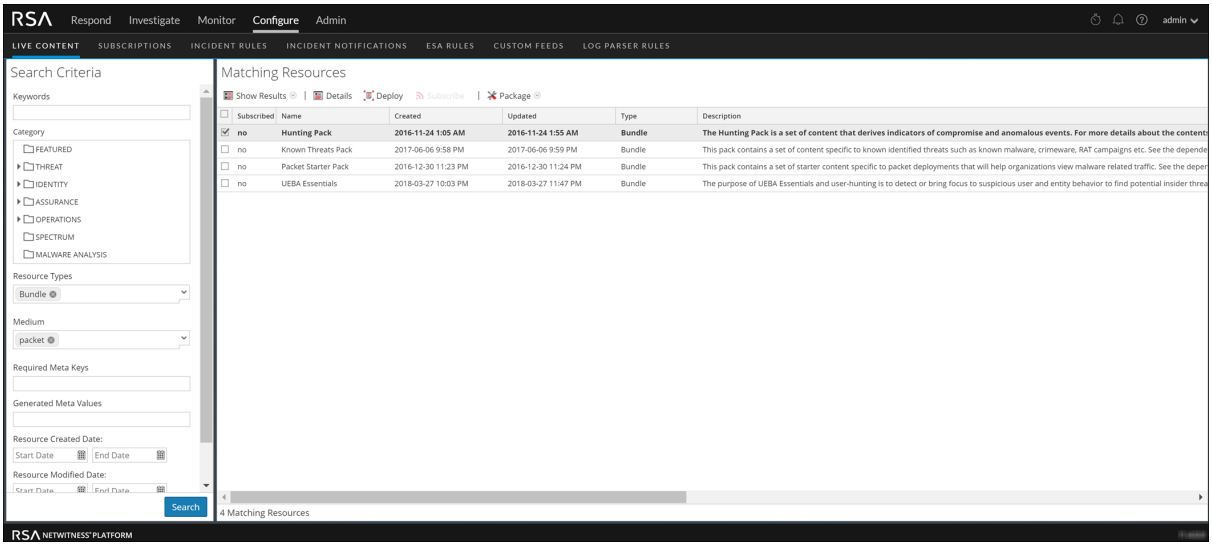
```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":
[{"op":"add","path":"/dataPipeline/schemas/-","value":"TLS"}]}'
```

Hunting Packの追加

NetWitness Platformで、Hunting Packを追加するか、Hunting Packが使用可能であることを確認します。

1. NetWitness Platformにログインします。
2. [**管理**]に移動し、[**Admin Server**]を選択します。

3. をクリックして、[**構成**]＞[**Liveコンテンツ**]を選択します。



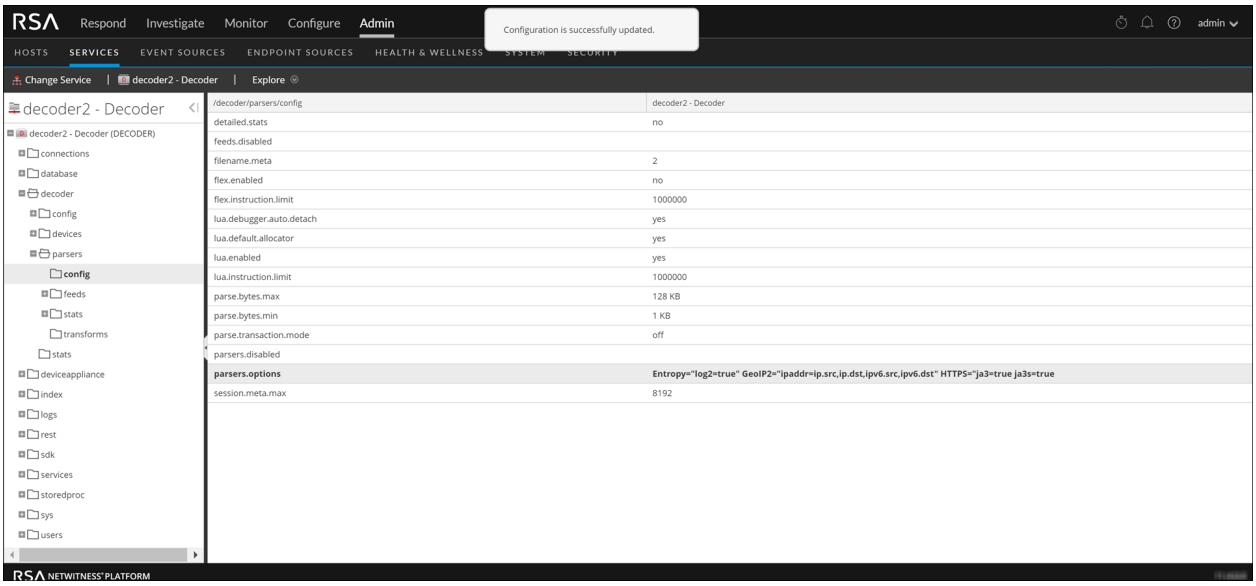
4. 検索条件で、次の項目を選択します。
   a. [リソース タイプ]で「**Bundle**」を選択します。
   b. [対象]で「**Packet**」を選択します。
5. [**検索**]をクリックします。
   一致するリソースのリストが表示されます。
6. リストから[**Hunting Pack**]を選択し、[**導入**]をクリックします。
   Hunting Packが追加されます。

JA3とJA3sの追加

JA3およびJA3sフィールドは、11.3.1以降のNetwork Decoderでサポートされています。Network Decoderが11.3.1以降のいずれかのバージョンにアップグレードされていることを確認します。

JA3およびJA3sを追加するには、次の手順を実行します。

1. NetWitness Platformにログインします。
2. [**管理**]に移動し、**Decoder**サービスを選択します。
3. `/decoder/parsers/config/parsers.options`に移動します。
4. `HTTPS="ja3=true ja3s=true`を追加します。
   JA3およびJA3sフィールドが構成されます。



(オプション) Endpointデータ ソースの有 効 化

NetWitness Platform 11.4でNetWitness Endpoint Serverが構 成されている場 合 は、プロセスやレジストリなどのEndpointデータ ソースを有 効にしてUEBAのアラートを生 成 できます。

Endpointデータ ソースを有 効にするには、UEBAサーバで次 のコマンドを実 行します。

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":
[{"op":"add","path":"/dataPipeline/schemas/-","value":"PROCESS"},
{"op":"add","path":"/dataPipeline/schemas/-","value":"REGISTRY"}]}'
```

(オプション) UEBAインジケータ転 送 の有 効 化

NetWitness Platform 11.4にNetWitness Respond Serverが構 成されている場 合 、NetWitness UEBAのインジケータをNetWitness Respond ServerとCorrelation Serverに転 送してインシデントを作 成 できます。

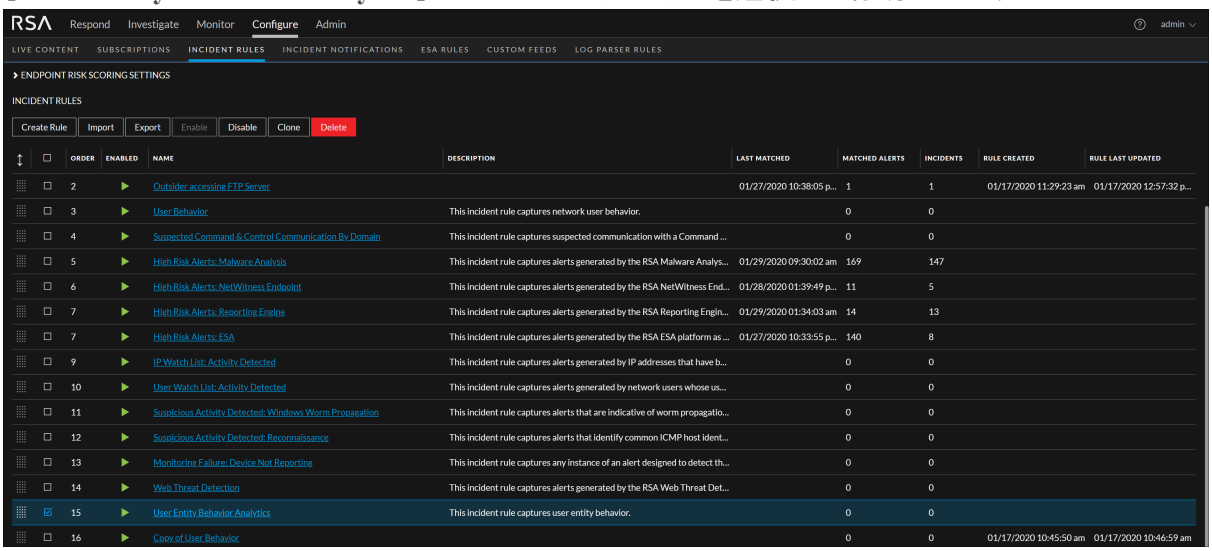
UEBAインジケータ転 送を有 効にするには、次 のコマンドを実 行します。

```
curl -X PATCH http://localhost:8881/configuration -H ', content-type:
application/json' -d '{"operations":
[{"op":"replace","path":"/outputForwarding/enableForwarding","value":true}]}'
```

[対 応]ビューにインシデントを表 示するには、次 の手 順を実 行します。

1. NetWitness Platformにログインします。
2. [**構 成**] > [**インシデント ルール**]に移 動します。

3. [**User Entity Behavior Analytics**]ルールのチェックボックスを選択し、有効化します。



(必須) Airflow構成の更新

NetWitness Platform 11.4.1にアップグレードした後、Airflow構成を更新してください。ただし、Airflow構成を更新する前に、次の手順を実行する必要があります。

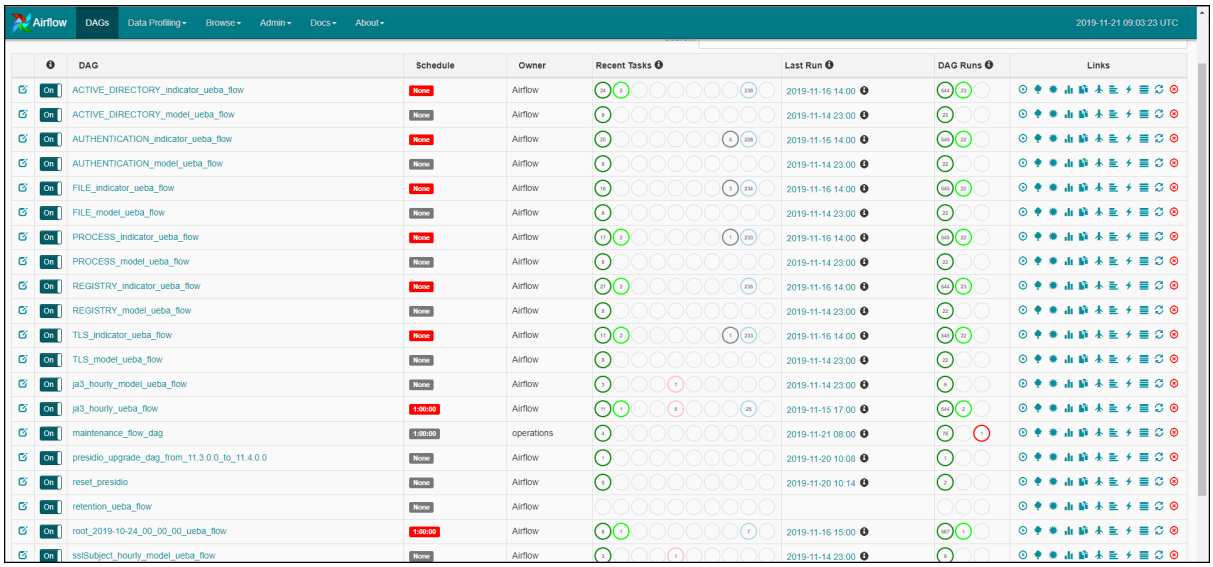
- UEBAマシンからrootユーザとして次のスクリプトを実行します。
  ```
  python /var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio_workflows-1.0-py2.7.egg/presidio/resources/rerun_ueba_server_config.py
  ```

Airflow構成を更新するには、次の手順を実行します。

1. Airflow WebサーバUI(`https://<UEBA_host>/admin/`) にアクセスして、ユーザ名とパスワードを入力します。

   注: Airflow WebサーバUIのユーザ名はadminで、パスワードは`deploy_Admin`パスワードと同じです。

   注: フルフローDAGで、NetWitness Platform 11.3とNetWitness Platform 11.4の間で不整合のあるタスクには、赤い丸が表示されます。



2. `presidio_upgrade_dag_from_11.*_to_11.4.0.1`で  をクリックして、フル フローDAGを一時停止します。

> **注：** このステップでは、開始日が27日前の新しいフル フローDAGが作成され、古いフル フローDAGが削除され、新しいフローDAGが開始されます。

3. DAGの更新が正常に完了すると、`presidio_upgrade DAG`タスクの[**Recent Tasks**]列に緑色の丸が表示されます。

新機能の有効化

このセクションでは、11.4.1で使用できる新機能について説明します。このリリースの新機能の一覧については、『*RSA NetWitness Platform 11.4.1 リリース ノート*』を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

カスタマ エクスペリエンス向上プログラム

RSA NetWitness Platformのカスタマ エクスペリエンス向上プログラム(CEIP) は、RSA NetWitness Platformを継続的に改善するための取り組みです。お客様がCEIPを有効化すると、個々のユーザのRSA NetWitness Platformでの作業状況が分析されます。その際、ユーザのワークフローに割り込みを行ったり、ユーザ個人を特定することはありません。RSAはこれらの分析情報を将来のリリースに追加する新機能や拡張機能の優先度を決定するために使用します。詳細については、『*システム構成ガイド*』の「カスタマ エクスペリエンス向上プログラムの構成」を参照してください。

[イベント]ビューでのメール再構築の改善

アナリストは、[イベント]ビューから直接メール セッションを再構築できるようになりました。詳細については、『*Investigateユーザ ガイド*』の「[イベント]ビューでのイベントの再構築」を参照してください。

[イベント]ビューでの分割セッションと関連イベントのグループ化

収集したデータの関係をより簡単に検出できるようにするため、[イベント]ビューと[レガシー イベント]ビューでは、分割セッションと関連セッションのイベントをグループ化することができます。ユーザ インタフェースには、先行イベントの下に後続イベントがネストして表示されるため、先行イベントと後続イベントを容易に識別できるようになっています。詳細については、『*Investigateユーザ ガイド*』の「[イベント]ビューと[レガシー イベント]ビューでの分割セッションおよび関連セッションのイベントのグループ化」を参照してください。

構成可能な[イベント分析]ビューのイベント数の上限

[イベント分析]ビューのパフォーマンスを最適化するため、管理者は[イベント]パネルにロードされるイベント数のデフォルトの上限を設定し、ユーザ ロールごとにより低い上限を設定することができます。詳細については、『*RSA NetWitness Platform システム構成ガイド*』の「[イベント分析]ビューの設定」を参照してください。

[イベント]ビューでのクエリ作成の高速化と簡略化

より簡単かつ高速にフィルタを作成し、クエリを構築できるよう、継続的にユーザ インタフェースの機能向上が行われています。詳細については、『*Investigateユーザ ガイド*』の「[イベント]ビューでのイベントのフィルタリング」を参照してください。

Log CollectorとLog Decoderでのカスタム証明書の構成

Log CollectorとLog DecoderでSyslogリスナのカスタム証明書を構成できます。これにより、他の機能では事前にインストールされた証明書を使用する一方で、Syslogリスナ用に独自の信頼する証明書を使用できるようになります。詳細については、『*ログ収集構成ガイド*』の「(オプション) Log Collectorでのカスタム証明書の構成」と『*Decoder構成ガイド*』の「(オプション) Log Decoderでのカスタム証明書の構成」を参照してください。

イベント ソースの可視化と検索の改善

アドレス(IPアドレスまたはホスト名)または、名前によってイベント ソースを検索できるようになり、Log Collector上の目的のイベント ソースを簡単に表示できます。履歴チャートなどの情報は、[ヘルス モニタ]タブから[イベント ソース]>[管理]タブに移動しました。詳細については、『*イベント ソース管理ユーザ ガイド*』を参照してください。

Analyst UIでのSSO認証のサポート

複数のNetWitness Platformユーザ インタフェース インスタンスを導入した環境でシングル サインオン(SSO)がサポートされます。

deploy_adminアカウントの管理の簡略化

`deploy_admin`アカウントは、すべてのNetWitness Platformホストで使用されるパスワード ベースのシステム アカウントであり、すべてのホスト間で同期を保つ必要があります。お客様の環境のポリシーによっては、パスワードの定期的な更新が必要になる場合があります。11.4.1以降、`deploy_admin` パスワードは、NW Server上で`nw-manage`スクリプトを使用して一元的に管理されます。`nw-manage`スクリプトの実行により、`deploy_admin`アカウントを使用するすべてのNetWitness Platformコンポーネント ホストのパスワードが更新されます。詳細については、『*システム メンテナンス ガイド*』の「deploy_adminアカウントの管理」を参照してください。

ウォーム スタンバイNW ServerのIPアドレスの変更

セカンダリNW ServerのIPアドレスがプライマリNW Serverと異なる場合、手動でフェールオーバー手順を実行し、ウォーム スタンバイNW ServerのIPアドレスを変更できます。手順については、『*導入ガイド*』の「プライマリNW ServerからIPアドレスが異なるセカンダリNW Serverへのフェールオーバー」を参照してください。

RSA SecurID Accessへの高リスク ユーザ名の転送サポート

NetWitness PlatformとRSA SecurID Accessの統合により、NetWitness Respond Serverは、高リスク ユーザのActive Directoryユーザ名をインシデントからRSA SecurID Accessに送信できるようになりました。Respond Serverでのこのメタデータの構成方法については、『*Respond構成ガイド*』を参照してください。

Nw-ShellでESAルール導入環境のトラブルシューティング メトリックを表示

Nw-Shellを使用して、ESA Correlationサーバから、各ESAルール導入環境のメトリックを表示できます。これらのメトリックには、導入環境で使用するデータ ソースのセッション数、ルールのメモリ使用状況などが含まれます。詳細については、『*RSA NetWitness Platform ESA相関ルール アラート ユーザ ガイド*』の「ESAルール導入環境トラブルシューティングのためNw-Shellを使用してCorrelationサーバ メトリックを取得」を参照してください。

付録 A.オフライン方式(Liveサービスへの接続なし) - コマンドライン インタフェース

この方式は、NW ServerがLiveサービスに接続されていない場合に使用できます。

前提条件

RSA Link(https://community.rsa.com/) にアクセスし、[**NetWitness Platform**] > [**RSA NetWitness Logs and Network**] > [**Downloads**] > [RSA Downloads] からローカル ディレクトリに次のファイルがダウンロードされていることを確認します。

- 11.2.x.xまたは11.3.x.xから11.4.1.0にアップグレードする場合は、次のファイルをダウンロードします。
  `netwitness-11.4.0.0.zip`
  `netwitness-11.4.1.0.zip`
- 11.4.0.xから11.4.1.0にアップグレードする場合は、次のファイルをダウンロードします。
  `netwitness-11.4.1.0.zip`
- 外部リポジトリを使用している場合は、外部リポジトリに最新の更新を追加します。詳細については、「外部リポジトリ使用時のCLIによるアップグレードの手順」を参照してください。

手順

NW Serverホストとコンポーネント ホストで、アップグレード手順を実行する必要があります。

注: PDFからコマンドをコピーしてLinux SSHターミナルにペーストしても、正しく入力できません。コマンドを手入力してください。

1. 11.4.1.0ファイルをステージングして、アップグレードの準備をします。
   - **11.2.x.xまたは11.3.x.xからアップグレードする場合**は、11.4.0.0と11.4.1.0をステージングする必要があります。NW Serverに`root`としてログインして、次のディレクトリを作成します。
     `/tmp/upgrade/11.4.0.0`
     `/tmp/upgrade/11.4.1.0`
     次に、パッケージZipファイルをNW Serverの`/root`ディレクトリにコピーし、次のコマンドを使用して`/root`から適切なディレクトリに解凍します。
     `unzip netwitness-11.4.0.0.zip -d /tmp/upgrade/11.4.0.0`
     `unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0`
   - **11.4.0.0から11.4.1.0にアップグレードする場合**、11.4.1.0のステージングのみが必要です。NW Serverに`root`としてログインして、次のディレクトリを作成します。
     `/tmp/upgrade/11.4.1.0`
     次に、パッケージZipファイルをNW Serverの`/root`ディレクトリにコピーし、次のコマンドを使用して`/root`から適切なディレクトリに解凍します。
     `unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0`

   注: 作成したステージング ディレクトリに.zipファイルをコピーし、その場所で解凍した場合は、解凍後、元の.zipファイルを忘れずに削除してください。

2. 次のコマンドを使用して、アップグレードの初期化を実行します。
   `upgrade-cli-client --init --version 11.4.1.0 --stage-dir /tmp/upgrade`
3. 次のコマンドを使用して、NW Serverホストをアップグレードします。
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.4.1.0`
4. NW Serverホストのアップグレードが成功したら、NetWitness Platformユーザ インタフェースの[ホスト]ビューからホストを再起動します。
5. 各コンポーネント ホストに対して、ステップ3～5を繰り返します。コマンドのIPアドレスは、アップグレードするコンポーネント ホストのIPアドレスに変更します。

注： NW Serverホストで`upgrade-cli-client --list`コマンドを使用して、すべてのホストのバージョンを確認できます。`upgrade-cli-client`のヘルプを表示するには、`upgrade-cli-client --help`コマンドを使用します。

注： アップグレード中に次のエラーが表示されることがあります。
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
エラーが表示されても、アップグレードは正常に完了します。何のアクションを取る必要もありません。ホストを新しいバージョンに更新する際に他のエラーが発生した場合は、カスタマ サポートにお問い合わせください。

外部リポジトリ使用時のCLIによるアップグレードの手順

1. 11.4.1.0ファイルをステージングして、アップグレードの準備をします。
   - **11.2.x.xまたは11.3.x.xからアップグレードする場合**は、11.4.0.0と11.4.1.0をステージングする必要があります。NW Serverに`root`としてログインして、次のディレクトリを作成します。
     `/tmp/upgrade/11.4.0.0`
     `/tmp/upgrade/11.4.1.0`
     次に、パッケージZipファイルをNW Serverの`/root`ディレクトリにコピーし、次のコマンドを使用して`/root`から適切なディレクトリに解凍します。
     `unzip netwitness-11.4.0.0.zip -d /tmp/upgrade/11.4.0.0`
     `unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0`
   - **11.4.0.0から11.4.1.0にアップグレードする場合**、11.4.1.0のステージングのみが必要です。NW Serverに`root`としてログインして、次のディレクトリを作成します。
     `/tmp/upgrade/11.4.1.0`
     次に、パッケージZipファイルをNW Serverの`/root`ディレクトリにコピーし、次のコマンドを使用して`/root`から適切なディレクトリに解凍します。
     `unzip netwitness-11.4.1.0.zip -d /tmp/upgrade/11.4.1.0`

   注： 作成したステージング ディレクトリに.zipファイルをコピーし、その場所で解凍した場合は、解凍後、元の.zipファイルを忘れずに削除してください。
2. 次のコマンドを使用して、アップグレードの初期化を実行します。
   `upgrade-cli-client --init --version 11.4.1.0 --stage-dir /tmp/upgrade`

3. 次のコマンドを使用して、NW Serverホストをアップグレードします。
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.4.1.0
   ```
4. NW Serverホストのアップグレードが成功したら、NetWitness Platformユーザ インタフェースの[ホスト]ビューからホストを再起動します。
5. 各コンポーネント ホストに対して、ステップ3とステップ4を繰り返します。コマンドのIPアドレスは、アップグレードするコンポーネント ホストのIPアドレスに変更します。

注: NW Serverホストで`upgrade-cli-client --list`コマンドを使用して、すべてのホストのバージョンを確認できます。`upgrade-cli-client`のヘルプを表示するには、`upgrade-cli-client --help`コマンドを使用します。

注: アップグレード中に次のエラーが表示されることがあります。
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
エラーが表示されても、アップグレードは正常に完了します。何のアクションを取る必要もありません。ホストを新しいバージョンに更新する際に他のエラーが発生した場合は、カスタマ サポートにお問い合わせください。

付録B.インストールとアップグレードのトラブルシューティング

このセクションでは、[ホスト]ビューからホストのバージョン更新およびサービスのインストールを実施して、問題が発生した場合に、[ホスト]ビューに表示されるエラー メッセージについて説明します。トラブルシューティングの解決策で解決できない更新またはインストールの問題がある場合は、カスタマ サポートにお問い合わせください。

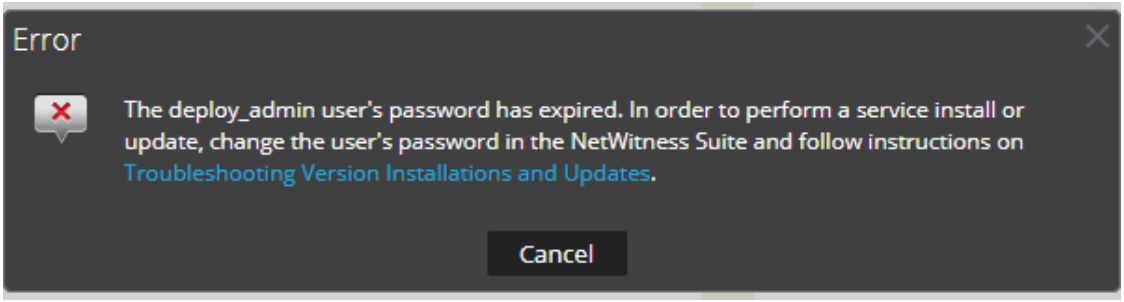
このセクションでは、アップグレード中に発生する可能性がある次のエラーのトラブルシューティング手順について説明します。

- deploy_adminのパスワード有効期限切れエラー
- ダウンロード エラー
- バージョン <version-number>の導入エラー: 更新 パッケージの不足
- 外部リポジトリ更新エラー
- ホスト インストール失敗エラー
- ホスト更新失敗エラー
- 更新パッケージ不足エラー
- OpenSSL 1.1.xエラー
- NW Server以外へのパッチ適用エラー
- コマンド ラインからの更新後のホスト再起動エラー
- アップグレード後のReporting Engine再起動

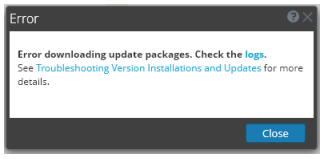
次のホストおよびサービスのアップグレード中またはアップグレード後に発生する可能性があるエラーについても、トラブルシューティング手順を記載しています。

- Log Collectorサービス
- NW Server
- Orchestration
- Reporting Engine

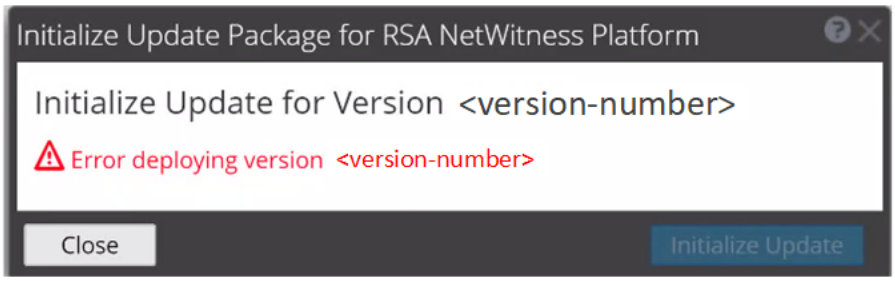
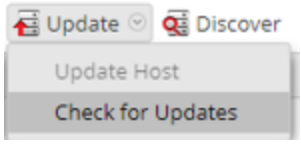
deploy_adminのユーザ パスワード有効期限切れエラー

エラーメッセージ	
原因	deploy_adminのユーザ パスワードの有効期限が切れています。
解決策	deploy_adminのパスワードをリセットします。 1. (NW Serverホスト以外の) すべてのコンポーネント ホストで、次のコマンドを実行します。 /opt/rsa/saTools/bin/set-deploy-admin-password 2. すべてのコンポーネント ホストを更新した後、NW Serverホストで次のコマンドを実行します。 /opt/rsa/saTools/bin/set-deploy-admin-password 3. インストールまたはオーケストレーションに失敗したホスト上で、nwsetup-tui コマンドを実行し、[**Deployment Password**] のプロンプトが表示されたら、**deploy_admin**の新しいパスワードを入力します。

ダウンロード エラー

エラーメッセージ	
問題	更新バージョンを選択し、[**更新**]＞[**ホストの更新**]をクリックすると、ダウンロードが開始されますが異常終了します。
原因	バージョンのダウンロード ファイルのサイズが大きく、ダウンロードに時間がかかる場合があります。ダウンロード中に通信の問題が発生すると、ダウンロードは失敗します。
解決策	1. 更新を再試行します。 2. 同じエラーで再度失敗した場合は、『*NetWitness Platform 11.4 アップグレード ガイド*』の「[ホスト]ビューからのオフライン方式」または「コマンド ライン インタフェースを使用したオフライン方式」の説明に従って、オフライン方式で更新してみてください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。 3. それでも更新できない場合は、カスタマ サポートにお問い合わせください。

バージョン <version-number>の導入エラー: 更新パッケージの不足

エラーメッセージ	
問題	「バージョン <version-number>の導入中にエラーが発生しました」のエラーは更新 パッケージが破損している場合に、[**更新の初期化**]をクリックした後で、[**RSA NetWitness Platformの更新パッケージの初期化**]ダイアログに表示されます。
解決策	1. [**閉じる**]をクリックしてダイアログを閉じます。 2. ステージング フォルダからバージョン フォルダを削除します。 3. salt-masterサービスが実行されていることを確認します。 4. 更新パッケージのzipファイルをステージング フォルダに再コピーします。 5. [ホスト]ビューのツールバーで、[更新の確認]を再度選択します。  6. [**更新の初期化**]をクリックします。 7. ツールバーの[**更新**]＞[**ホストの更新**]をクリックします。 8. [**更新あり**]ダイアログで[**更新を開始**]をクリックします。 ホストの更新が完了すると、ホストの再起動を求めるメッセージが表示されます。 9. ツールバーの[**ホストの再起動**]をクリックします。

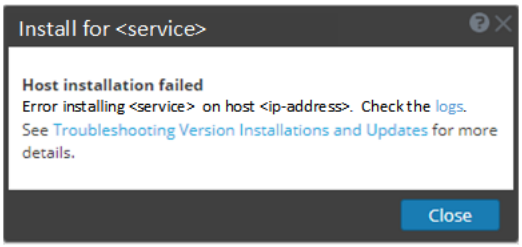
外部リポジトリ更新エラー

エラーメッセージ	新しいバージョンに更新しようとすると、次のようなエラーが返されました: 。Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""
原因	指定したパスに問題があります。
解決策	次の情報を確認します。 • URLがNW Serverホスト上に存在する。

	• 正しいパスを使 用し、パスからはスペースを削 除している。

ホスト インストール失敗エラー

エラーメッセージ



問題

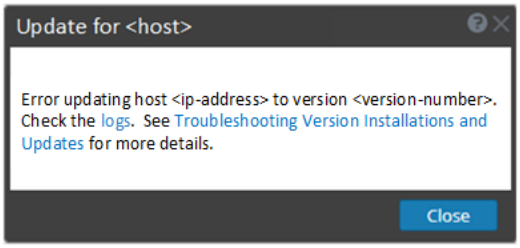
ホストを選択して[**インストール**]をクリックすると、サービスのインストール処理が失敗します。

解決策

1. サービスのインストールを再試行します。
   通常は、これで問題が解決されます。
2. それでもサービスをインストールできない場合は、次の手順を実行します。
   a. 実行時にNW Server上の次のログを監視します(たとえば、コマンド ラインで`tail -f`コマンドを実行します)。
   `/var/netwitness/uax/logs/sa.log`
   `/var/log/netwitness/orchestration-server/orchestration-server.log`
   `/var/log/netwitness/deployment-upgrade/chef-solo.log`
   `/var/log/netwitness/config-management/chef-solo.log`
   `/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
   エラーはこれらのログの少なくとも1つに表示されます。
   b. 問題を解決し、サービスを再インストールします。
   - 原因1: nwsetup-tuiで`deploy_admin`の間違ったパスワードを入力しました。
     解決策: `deploy_admin`のパスワードをリセットします。
     1. 11.xのNW Serverホストとそれ以外のすべてのホストで、次のコマンドを実行します。
        `/opt/rsa/saTools/bin/set-deploy-admin-password`
     2. インストールまたはオーケストレーションに失敗したホスト上で、`nwsetup-tui`コマンドを実行し、[**Deployment Password**]のプロンプトが表示されたら、**deploy_admin**の新しいパスワードを入力します。
   - 原因2: `deploy_admin`のパスワードの有効期限が切れています。
     解決策: `deploy_admin`のパスワードをリセットします。
     1. 11.xのNW Serverホストとそれ以外のすべてのホストで、次のコマンドを実行します。
        `/opt/rsa/saTools/bin/set-deploy-admin-password`
     2. インストールまたはオーケストレーションに失敗したホスト上で、`nwsetup-tui`コマンドを実行し、[**Deployment Password**]のプロンプトが表示されたら、**deploy_admin**の新しいパスワードを入力します。
3. それでも更新を適用できない場合は、ステップ2のログを収集して、カスタマ サポートにお

ホスト更新失敗エラー

エラーメッセージ



問題

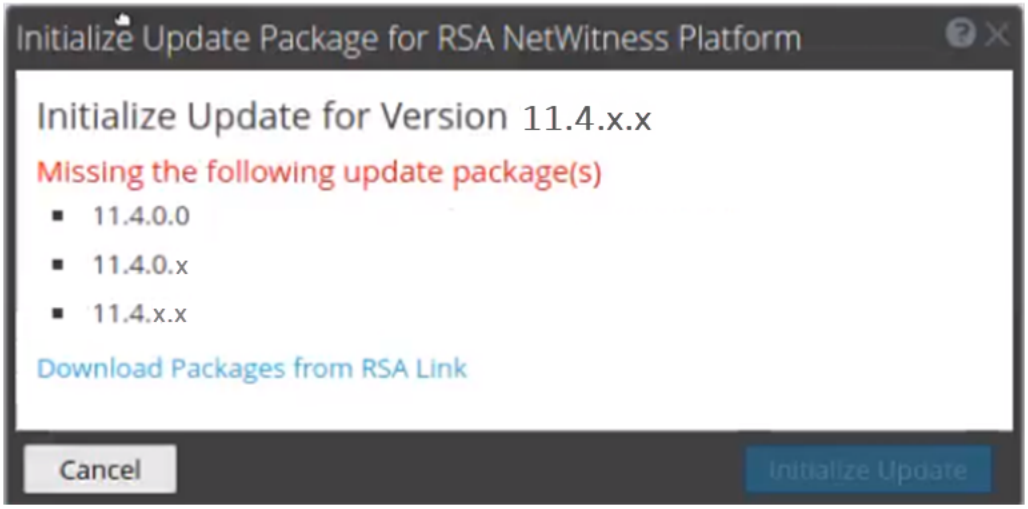
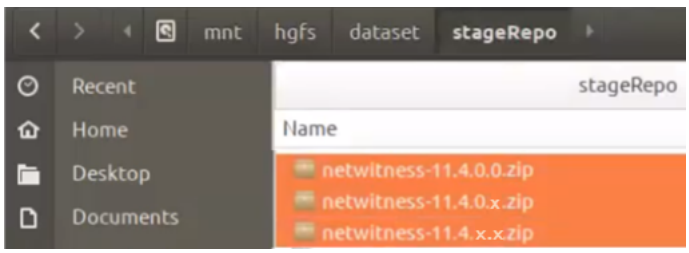
更新バージョンを選択し、[**更新**]＞[**ホストの更新**]クリックすると、ダウンロード プロセスは成功しますが、更新プロセスは失敗します。

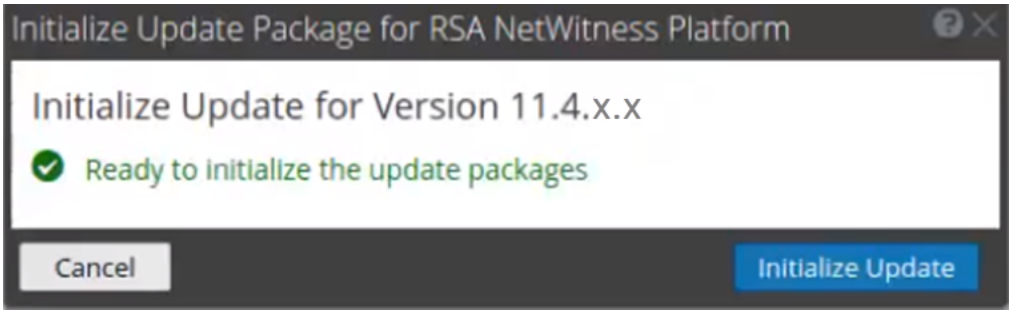
解決策

1. ホストへのバージョン更新の適用を再試行します。
   通常は、これで問題が解決されます。
2. それでも新しいバージョンに更新できない場合は、次の手順を実行してください。
   a. 実行時にNW Server上の次のログを監視します(たとえば、コマンド ラインから`tail -f`コマンドを実行します)。
   ```
   /var/netwitness/uax/logs/sa.log
   /var/log/netwitness/orchestration-server/orchestration-server.log
   /var/log/netwitness/deployment-upgrade/chef-solo.log
   /var/log/netwitness/config-management/chef-solo.log
   /var/lib/netwitness/config-management/cache/chef-stacktrace.out
   ```
   エラーはこれらのログの少なくとも1つに表示されます。
   b. その問題を解決して、バージョンの更新を再度実行してください。
   - 原因1:`deploy_admin`のパスワードの有効期限が切れています。
     解決策:`deploy_admin`のパスワードをリセットします。
     原因1を解決するには、次の手順を実行します。
     1. NetWitness Platformメニューで、[**管理**]＞[**セキュリティ**]＞[**ユーザ**]タブの順に選択します。
     2. `deploy_admin`を選択し、[**パスワードのリセット**]をクリックします。
     3. (**オプション**)[**パスワードのリセット**]ダイアログで有効期限が切れた`deploy_admin`のパスワードの再使用が拒否される場合は、次の手順を実行します。
        a. `deploy_admin`のパスワードを新しいパスワードにリセットします。
        b. 11.xのNW Server以外のすべてのホストで、次のコマンドを実行し、NW Serverと同じ`deploy_admin`のパスワードを指定します。

	/opt/rsa/saTools/bin/set-deploy-admin-password • 原因2: deploy_adminのパスワードがNW Serverホストで変更されましたが、NW Server以外のホストでは変更されていません。 原因2を解決するには、次の手順を実行します。 ■ 11.xのNW Server以外のすべてのホストで、次のコマンドを実行し、NW Serverと同じdeploy_adminのパスワードを指定します。 /opt/rsa/saTools/bin/set-deploy-admin-password 3. それでも更新を適用できない場合は、ステップ2のログを収集して、カスタマサポートにお問い合わせください。

更新パッケージ不足エラー

エラーメッセージ	
問題	「次の更新 パッケージが見つかりません」は、[**ホスト**]ビューからオフラインでホストを更新する時に、ステージングフォルダに足りないパッケージがあると、[**RSA NetWitness Platformの更新パッケージの初期化**]ダイアログに表示されます。
解決策	1. [**RSA NetWitness Platformの更新パッケージの初期化**]ダイアログで[RSA Linkからパッケージをダウンロード]をクリックします。 選択したバージョンの更新ファイルが含まれるRSA Linkページが表示されます。 2. ステージングフォルダに足りないパッケージを選択します(たとえば、**11.4.0.0**、**11.4.0.x**、**11.4.x.x**)。 

	[RSA NetWitness Platformの更新パッケージの初期化]ダイアログが開き、更新パッケージを初期化する準備ができたというメッセージが表示されます。 

OpenSSL 1.1.x

エラーメッセージ	次の例は、OpenSSL 1.1.xがインストールされているホストからsshクライアントを実行した場合に発生する可能性のあるsshエラーを示しています。 `$ ssh root@10.1.2.3` **`ssh_dispatch_run_fatal: Connection to 10.1.2.3 port 22: message authentication code incorrect`**

問題	OpenSSL 1.1.xを使用しているクライアントからNetWitness Platformホストに上級ユーザがsshで接続しようとすると、CENTOS 7.xとOpenSSL 1.1.xの間に互換性がないため、このエラーが発生します。次に例を挙げます。
	`$ rpm -q openssl`
	`openssl-1.1.1-8.el8.x86_64`

解決策	互換性のある暗号リストをコマンド ラインで指定します。次に例を挙げます。
	`$ ssh -oCiphers=aes128-ctr,aes192-ctr,aes256-ctr root@10.1.2.3`
	`I've read & consent to terms in IS user agreement.`
	`root@10.1.2.3's password:`
	`Last login: Mon Oct 21 19:03:23 2019`

NW Server以外へのパッチ適用エラー

エラーメッセージ	`/var/log/netwitness/orchestration-server/orchestration-server.log`に、次のようなエラーが記録されました。 **`API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported`**
問題	NW Serverホストのバージョンを更新した後で、NW Server以外のすべてのホストを同じバージョンに更新する必要があります。たとえば、NW Serverを11.4.0.0から11.4.x.xに更新すると、NW Server以外のホストの唯一の更新パスは、同じバージョン(つまり、11.4.x.x) だけです。NW Server以外のホストを別のバージョン(たとえば、11.4.0.0から11.4.0.x) に更新しようとすると、このエラーが表示されます。
解	2つの選択肢があります。

決策	• NW Server以外のホストを11.4.x.xに更新します。 • NW Server以外のホストを更新しません(現在のバージョンを維持)。

コマンド ラインからの更新後のホスト再起動のエラー

エラー メッセージ	ホストをオフラインで更新して再起動した後に、ホストを再起動するよう求めるメッセージがユーザ インタフェースに表示されます。 
原因	CLIを使用してホストを再起動することはできません。ユーザ インタフェースを使用する必要があります。
解決策	ユーザ インタフェースの[ホスト]ビューでホストを再起動します。

アップグレード後のReporting Engine再起動

問題	11.2や11.3などの11.xのバージョンから11.4にアップグレードした後、Reporting Engineサービスが継続的に再起動を試み、失敗を繰り返す場合があります。
原因	ライブ チャート、アラート ステータス、レポート ステータスのデータベース ファイルが破損し、正常にロードできない可能性があります。
解決策	この問題を解決するには、次の手順を実行します。 1. どのデータベース ファイルが破損しているかを確認します。 `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log`ファイルを開き、次のブロックを確認します。 • ライブ チャートのdbファイルが破損している場合は、次のログが表示されます。 Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception: org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) at org.h2.message.DbException.get(DbException.java:168) org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database! • アラート ステータスのdbファイルが破損している場合は、次のログが表示されます。

Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:

org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]

at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)

at org.h2.message.DbException.get(DbException.java:168)

org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertStatusHandler': Unsatisfied dependency expressed through field 'alertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertExecutionStatsDAOImpl': Unsatisfied dependency expressed through field 'persistedAlertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'persistedAlertExecutionStatsDAOImpl'

- レポート ステータスのdbファイルが破損している場合は、次のログが表示されます。

```
org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]
```

2. ライブ チャート データベース ファイルの破損を解決するには、次の手順を実行します。
   a. Reporting Engineサービスを停止します。
   b. `livechart.mv.db`ファイルを、`/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts`フォルダから一時的な場所に移動します。
   c. Reporting Engineサービスを再起動します。

   注: この手順を実行すると、一部のライブ チャート データが失われる可能性があります。

   アラート ステータスまたはレポート ステータス データベース ファイルの破損を解決するには、次の手順を実行します。

   a. Reporting Engineサービスを停止します。
   b. 破損したdbファイルを`/var/netwitness/reserver/rsa/soc/reporting-engine/archives`フォルダにある最新の`alertstatusmanager.mv.db`ファイルまたは`reportstatusmanager.mv.db`ファイルで置き換えます。
   c. Reporting Engineサービスを再起動します。

   詳細については、ナレッジベース記事「Reporting Engine restarts After upgrade to RSA NetWitness Platform 11.4.」を参照してください。

Log Collectorサービス(`nwlogcollector`)

Log Collectorのログは、`nwlogcollector` サービスを実行しているホスト上の`/var/log/install/nwlogcollector_install.log`に保存されます。

エラーメッ	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`

セージ	
原因	更新後、Log CollectorのLockboxを開くことができませんでした。
解決策	NetWitness Platformにログインし、LockboxのStable System Valueのパスワードをリセットすることにより、システム フィンガープリントをリセットします。詳細については、『*ログ収集の構成ガイド*』の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」セクションを参照してください。

エラーメッセージ	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
原因	更新後、Log CollectorのLockboxが構成されていません。
解決策	Log CollectorのLockboxを使用する場合は、NetWitness Platformにログインし、Lockboxを構成します。詳細については、『*ログ収集の構成ガイド*』の「Lockboxのセキュリティ設定の構成」トピックを参照してください。

エラーメッセージ	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
原因	Log CollectorのLockboxのStable System Value閾値フィールドをリセットする必要があります。
解決策	NetWitness Platformにログインし、LockboxのStable System Valueのパスワードをリセットします。詳細については、『*ログ収集の構成ガイド*』の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」セクションを参照してください。

NW Server

これらのログは、NW Serverホスト上の`/var/netwitness/uax/logs/sa.log`に書き込まれます。

問題	アップグレード後、監査ログが、グローバル監査に設定された宛先に転送されていないことが分かりました。 または 次のメッセージが`sa.log`に記録されました。 `Syslog Configuration migration failed. Restart jetty service to fix this issue`
原因	NW Serverのグローバル監査設定は、11.2.x.xまたは11.3.x.xから11.4.0.0への移行に失敗しました。
解決策	1. SSHでNW Serverに接続します。 2. 次のコマンドを実行します。 `orchestration-cli-client --update-admin-node`

Orchestration

Orchestration Serverのログは、NW Serverホスト上の`/var/log/netwitness/orchestration-server/orchestration-server.log` に書き込まれます。

問題	1. 非NW Serverホストをアップグレードしようとしましたが、失敗しました。 2. このホストのアップグレードを再試行しましたが、再度失敗しました。 `orchestration-server.log`に次のメッセージが記録されます。 `"'file' _virtual_ returned False: cannot import name HASHES""`
原因	アップグレードに失敗した非NW Serverホストでsalt minionがアップグレードされ、再起動されていない可能性があります。

解決策	1. アップグレードに失敗した非NW ServerホストにSSHで接続します。
	2. 次のコマンドを実行します。
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. 非NW Serverホストのアップグレードを再試行します。

Reporting Engineサービス

Reporting Engineの更新ログは、Reporting Engineを実行しているホスト上の`/var/log/re_install.log`ファイルに保存されます。

エラーメッセージ	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
原因	Reporting Engineの更新は、十分なディスク領域がないために失敗しました。
解決策	ログメッセージに示されている必要な容量に合わせてディスク領域を解放します。ディスク領域を解放する方法については、『*Reporting Engine構成ガイド*』の「サイズの大きなレポートに対応するためのスペースの追加」を参照してください。