RSA® NetWitness Platform

Version11.6

アップグレード ガイド

連絡先情報

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

商標

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

使用許諾契約

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

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

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

サードパーティライセンス

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

暗号技術に関する注意

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

配布

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

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

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

7月 2021

目次

アップグレードの概要

RSA NetWitness Platform 11.6.0.0には、NetWitness Platformのすべての製品の機能拡張と修正が含まれています。このガイド内の手順は、特に記載のない限り、物理ホストと仮想ホスト(AWS、Azure Public Cloud、Google Cloud Platformを含む)の両方に適用されます。

11.6では、NetWitness Platformのユーザインターフェイスにいくつかの新機能があります。

注: 11.5では、管理タスクがアイコンとして右上隅に統合され、管理、構成、通知、ジョブ、ユーザ環境設定が1つにまとめられています。

アップグレード パス

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

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

11.4.x.xより前のバージョンからアップグレードする場合は、まず、11.4.x.xにアップグレードしてから11.6.0にアップグレードする必要があります。詳細については、『RSA NetWitness Platform 11.4.1.1ユーザ ガイド』を参照してください。このガイドは、物理ホストと仮想ホスト(AWSとAzure Public Cloudを含む)の両方に適用されます。

混在モードでの実行

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。

注: Endpoint Log Hybridを混合モードで実行している場合は、Endpoint Brokerが、いずれかのEndpoint Serverと同じバージョンであることを確認してください。

ESAホストのアップグレードに関する考慮事項

混在モードは、NetWitness Platformバージョン11.5以降のESAホストではサポートされていません。

重要: NetWitness Server、ESAプライマリホスト、ESAセカンダリホストがすべて、同じNetWitness Platformバージョンである必要があります。

STIXカスタム フィードのアップグレードに関する考慮事項

バージョン11.6より前に作成されたカスタム フィードは自動的に処理されます。アップグレード時に、ADHOC、REST、TAXIIサーバー用に作成されたデータ ソースとフィードは自動的にプルされます。詳細については、『RSA NetWitness Platform Liveサービス管理ガイド』の「STIXカスタム フィードの作成」と、『RSA NetWitness Platform Context Hub構成ガイド』の「データ ソースとしてのSTIXの構成」を参照してください。

Windows Legacy収集の更新またはインストール

『Windows Legacy収集ガイド(RSA NetWitness 11.x) 』*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。

製品ドキュメントへのフィードバック

NetWitness Platformのドキュメントに関するフィードバックは、nwdocsfeedback@rsa.comまでメールで送信できます。

NetWitness Platformのヘルプ情報

セルフ ヘルプ リソース

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

- NetWitness Platformに関するすべてのドキュメントは、次の場所から参照できます。https://community.rsa.com/t5/rsa-netwitness-platform/ct-p/netwitness-documentationにアクセスしてください。
- 特定の情報を見つけるには、以下のRSAリンクの[**検索**]および[**質問**]フィールドを使用します。https://community.rsa.com/
- RSA NetWitness Platformナレッジベースを参照してください。
- RSA NetWitness Platformトラブルシューティングのページを参照してください。
- RSA NetWitness Platformブログを参照してください。
- さらに支援が必要な場合は、カスタマー サポートにお問い合わせください。

カスタマー サポートへのお問い合わせ

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

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

質問や支援が必要な場合は、以下の連絡先までお問い合わせください。

RSA Link	https://community.rsa.com メインメニューで[**My Cases**]をクリックします。
各国のお問い合わせ窓口	https://community.rsa.com/t5/support-information/how-to-contact-rsa-support/ta-p/563897
コミュニティ	https://community.rsa.com/t5/rsa-support/ct-p/support

アップグレード準備タスク

NetWitness Platform 11.6への更新の準備を行うには、次のタスクを実行します。

タスク1.(オプション) レガシー パッケージ リポジトリーを削除する

このタスクを実行して、以前のリリースの未使用リポジトリーをシステムから削除することでスペースを解放します。

1. 管理者ユーザー インターフェイスでホスト リストを確認するか、次のコマンドをNWサーバーで実行して、環境内で最も古いNetWitness Platformホストのバージョンを確認します。`upgrade-cli-client --list`
2. 環境内で最も古いアクティブ ホストのベースライン メジャー リリース バージョンより前のすべてのバージョンについては、NWサーバーの`/var/netwitness/common/repo/<version>`にあるすべてのレガシー パッケージ リポジトリー フォルダーを安全に削除できます
   - 最も古いホスト バージョンが11.4.x.x(11.4.1.0など) の場合は、11.0.x.x、11.1.x.x、11.2.x.x、11.3.x.xのリポジトリー フォルダーを安全に削除できます。ただし、11.4.0.0以降のリポジトリー バージョンは削除しないでください。
   - 最も古いホスト バージョンが11.3.x.xの場合は、11.0.x.x、11.1.x.x、11.2.x.xのリポジトリー フォルダーを安全に削除できます。ただし、11.3.0.0以降のリポジトリー バージョンは削除しないでください。

タスク2.(オプション) Respond正規化スクリプトのあらゆるカスタマイズがカスタム ファイルに含まれていることを確認する

注: このタスクは、NetWitness Platformバージョン11.4.xxから11.6.0.0へのアップグレードに適用されます。

11.4から11.6.xへのアップグレードの場合は、カスタマイズが個別に`custom_normalize`スクリプト ファイルに追加されるため、正規化スクリプト ファイルのバックアップはありません。これらのスクリプト ファイルは**`/var/lib/netwitness/respond-server/scripts`**ディレクトリーにあります。カスタマイズが存在する場合は、`custom`というプレフィックスが付いた正規化ファイルにそれを追加します。

アップグレード オプション

アップグレードは次の順序で実施します。

1. NW Serverホスト
2. Analyst UIホスト
3. ESAプライマリ ホスト
4. ESAセカンダリ ホスト
5. 残りのコンポーネント ホスト

注： NW Server、Analyst UI、ESAプライマリ、ESAセカンダリ ホストは、すべて同じ日にアップグレードする必要があります。残りのコンポーネント ホストは、次の日以降にアップグレードしても構いません。

NetWitness Platformのすべてのホスト タイプについては、『*RSA NetWitness Platform 11.xホストおよびサービス スタート 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は、「マスター目次」で確認できます。

重要な注意事項 - 最初にお読みください

コンポーネント ホストの時刻をNW Serverホストと同期する

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。
- 各ホストで次の操作を実行します。
  a. SSHでコンポーネント ホストに接続します。
  b. 次のコマンドを実行します。

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

混在モードのESAホストはサポート対象外

混在モードは、NetWitness PlatformバージョンのESAホストではサポートされていません。NetWitness Server、ESAプライマリ ホスト、ESAセカンダリ ホストがすべて、同じNetWitness Platformバージョンである必要があります。

Endpoint Hybridシステムはサポート対象外

(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.x.xでEndpoint Log Hybridホストをインストールしなかった場合は、11.6でEndpoint Log Hybridホストをインストールする必要があります。11.6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。

NW ServerとESAプライマリホストを11.6にアップグレードするまでRespond Serverサービスは有効にならない

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、Respond Serverサービスは、プライマリESAホストも11.6にアップグレードするまでは自動的に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。

Deploy_Adminパスワードのガイドライン

NetWitness Platformバージョン11.6以降では、導入アカウントのパスワード(ノードゼロのみ) には、既存のポリシーに加えて、少なくとも1つの数字、1つの大文字と小文字、および1つの特殊文字(!@#%^,+.) が含まれている必要があります。`nw-mange script`を使用してdeploy_adminパスワードを更新する場合も、同じパスワード ポリシーが適用されます。

プライマリNWサーバで`deploy_admin`パスワードを変更した場合、ウォーム スタンバイ サーバにパスワードが存在する場合はそれを変更する必要があります

アップグレード オプション

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。

- オプション1: インターネット接続時のユーザー インターフェイス方式
- オプション2: インターネット非接続時のユーザー インターフェイス方式
- オプション3: インターネット非接続時のコマンド ライン インターフェイス(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。
- NetWitness Server、ESAプライマリホスト、ESAセカンダリホストがすべて、同じNetWitness Platformバージョンである必要があります。
- ウォーム スタンバイ(存在する場合) をホストのリストに追加します。これは、NetWitness Platformと同じバージョンである必要があります。

オプション1：インターネット接続時のユーザー インターフェイス方式

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。

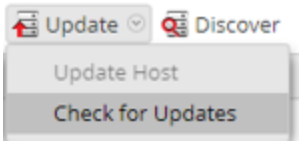
前提条件

次の情報を確認します。

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. 更新が利用可能であること。**(管理) > [ホスト] > [更新] > [更新の確認]**にアクセスして更新を確認します。[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11.6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]が表示されます。
5. **[更新のバージョン]**列で**[11.6]**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、Endpoint、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。

オプション2：インターネット非接続時のユーザー インターフェイス方式

注意： ユーザ インタフェースを使用したオフライン方式を使用できるのは、ホスト(11.4.1.x、11.5.x) を11.6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、アップグレード オプション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、「11.4.1.xまたは11.5.x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ホストを11.4.0.0または11.4.0.1から11.6にアップグレードしている場合は、「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てメッセージ「ダウンロード エラー」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からのアップグレード」の手順に従ってアップグレードを正常に完了することができます。この問題は、11.4.1.0以降で解決されました。

タスク1：ステージング フォルダー(`/var/lib/netwitness/common/update-stage/`) にバージョン アップグレード ファイルを配置

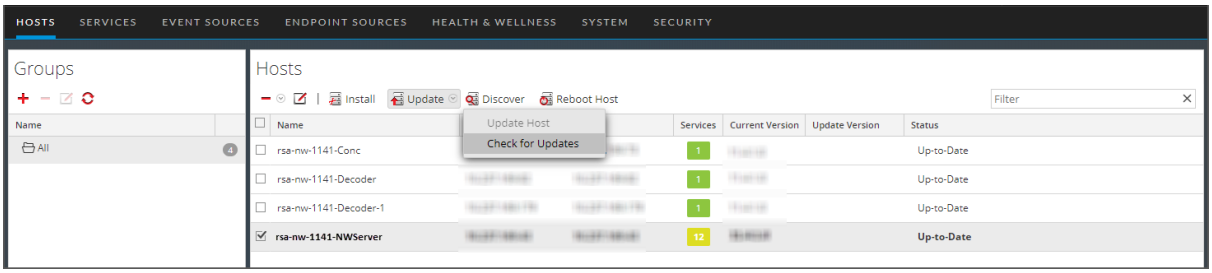
1. RSA Link(https://community.rsa.com/) にアクセスし、[**Downloads**] > [**NetWitness Platform**] > [**Version 11.6**]を選択して、アップグレード パッケージ`netwitness-11.6.0.0.zip`をローカル ディレクトリにダウンロードします。
2. SSHでNW Serverホストに接続します。
3. `netwitness-11.6.0.0.zip`をローカル ディレクトリから`/var/lib/netwitness/common/update-stage/`ステージング フォルダにコピーします。
   例：
   ```
   sudo cp /tmp/netwitness-11.6.0.0.zip /var/lib/netwitness/common/update-stage/
   ```
   rootユーザとしてログインしている場合は、コマンドでsudoを無視できます。次に例を示します。
   ```
   />cp /tmp/netwitness-11.6.0.0.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、アップグレード 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。

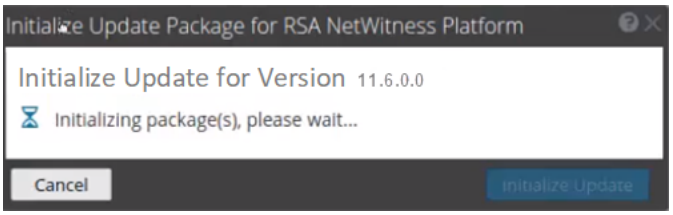


次の条件を満足すると、「更新パッケージを初期化する準備ができました」と表示されます。

- 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。

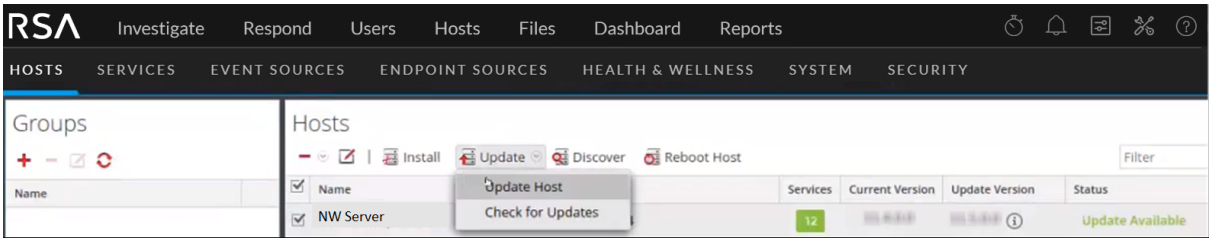
エラーのトラブルシューティング方法については、「インストールと更新のトラブルシューティング」を参照してください(たとえば、「バージョン<version-number>の導入エラー」と「次の更新 パッケージが見つかりません」が[**RSA NetWitness Platformの更新パッケージの初期化**]ダイアログに表示される場合があります) 。

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。時間は、ホストの構成方法によって異なります。
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。



11.4.1.xまたは11.5.x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-key <ID, IP address, hostname or
      display name of host> --version 11.6.0.0
      ```
2. NW Serverが正常にアップデートされたら、NW Server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。

オプション3: インターネット非接続時のコマンド ライン インターフェイス(CLI) 方式

「付録A: オフライン方式(Liveサービスに接続しない) - コマンド ライン インターフェイス」の手順に従います。

アップグレード後のタスク

11.6にアップグレードした後は、NetWitness Platformのユーザー インターフェイスにいくつかの新機能が加わります。ご使用のホストのタスクを完了してください。

全般

(オプション) NAT経由のIPアドレスを構成する

NW Serverホストに接続するためにNAT経由のIPアドレスを必要とするホスト(VLCなど) がある場合は、次の手順でホスト構成を更新する必要があります。

1. コンソールまたはSSHを使用して、NAT経由のIPアドレスの使用が必要なホストにログインします。
2. 次のコマンドを実行します。
   ```
   nw-manage --enable-nat-usage
   ```
3. NW ServerのNAT IPアドレスを設定するため、次の手順を実行します。
   a. コンソールまたはSSHを使用して、NW Serverにログインします。
   b. 次のコマンドを実行します。
      ```
      nw-manage -update-host --host-id <UUID of NW Server> --ipv4-public <NAT IP of NW Server>
      ```

      注: `nw-manage --list-hosts`を実行すると、ホストのUUIDと現在のNAT IPアドレスを確認できます。

(オプション - ウォームスタンバイ ホストの場合のみ) ウォームスタンバイ ホストのセカンダリIPアドレスを登録する

次の手順は、ウォームスタンバイ サーバを11.6にアップグレードしてから実行する必要があります。

1. コンソールまたはSSHを使用して、NW Serverにログインします。
2. 次のコマンドを実行します。
   ```
   nw-manage --add-nws-secondary-ip --ipv4 <ip address of Warm/Standby Server>
   ```

   注： フェールオーバー時に他のホストからアクセスできるように、ウォームスタンバイ サーバにNAT経由のIPアドレス(IPv4パブリック) が必要な場合は、次のコマンドを実行してNAT IPアドレスも登録する必要があります：`nw-manage --add-nws-secondary-ip --ipv4 <NAT-based IP address of Warm Standby Server>`
3. 次のコマンドを実行して、ウォームスタンバイ ホストのIPアドレスの値が正しいことを確認します。
   ```
   nw-manage --get-nws-secondary-ip
   ```

/etc/hosts.userから古いホスト エントリーを削除する

NW Serverホストまたはコンポーネント ホストをアップグレードした後で、`/etc/hosts.user`ファイルの内容を確認し、使われていない古いホスト エントリーが含まれていないか確認します。`/etc/hosts.user`ファイルには、NetWitness Platformによって管理されていないシステムやユーザが追加したエントリーが含まれます。ただし、`/etc/hosts.user`のエントリーは、NetWitness Platformが生成するホスト マッピングとマージされ、`/etc/hosts`を作成および更新するために使用されます。NetWitness Platformが生成するマッピングとの競合を回避し、IPアドレスの変更による接続エラーの発生を回避するため、NetWitness Platformホストのループバック IPアドレス以外のエントリーが`/etc/hosts.user`に含まれている場合は、削除することを推奨します。

`/etc/hosts.user`を更新した後で、次のコマンドを実行してシステムをリフレッシュする必要があります。

```
nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
```

DNSサーバを再構成する

デフォルトでは、11.4以前のバージョンからアップグレードされたコンポーネント ホストには、NW Serverと同じシステムDNSサーバが構成されます。このコンポーネント ホストで別のシステムDNSアドレスが必要な場合の手順については、『*システム メンテナンス ガイド*』の「ホスト ネットワーク構成の変更」を参照してください。

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. 各**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. 各**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。
3. Event Stream Analysis(ESA)

注: 混在モードは、NetWitness Platformバージョン11.6以降のESAホストではサポートされていません。NetWitness Server、ESAプライマリホスト、ESAセカンダリホストがすべて、同じNetWitness Platformバージョンである必要があります。

ESAに必要なアップグレード後のタスクはありません。ESAのトラブルシューティングについては、「ESAトラブルシューティング情報」を参照してください。

Endpoint、UEBA、Liveコンテンツ ルールのサポートを追加する場合は、ESA Correlationサービスの`multi-valued`パラメータおよび`single-valued`パラメータを更新して、必要なメタ キーをすべて追加する必要があります。アップグレード中にこれらの調整を行う必要はありません。後で都合のよいタイミングで調整を行うことができます。詳細と手順については、『*ESA構成ガイド*』の「必須の複数値および単一値のメタ キーに合わせてESAルールを更新」を参照してください。

ESA Analyticsのアップグレードに関する考慮事項

Event Stream Analytics Server(ESA Analytics) サービスは、NetWitness Platformバージョン11.6以降でサポートされていないか、または使用できません。Whoisルックアップ構成とESA Analyticsマッピング パネルは、ユーザ インターフェイス([管理者] > [システム]) に表示されなくなりました。

注 : Event Stream Analysis(ESA) は、引き続き提供されています。ESA相関ルールとESA相関サービスがサポートされています。自動脅威検出に使用されるESA Analyticsは、ESA相関ルールとは別の機能であり、EOLです。代わりに、より多くの機能とより優れたパフォーマンスを提供するESA相関ルールやサービスを使用できます。

新 ヘルス モニタ

注 : 11.5の新 ヘルス モニタは、11.4.x.xの次世代 ヘルス モニタ(ベータ) を置き換えます。

Liveを使用して新 ヘルス モニタのコンテンツを導入する

バージョン11.4.x.xから11.6にアップグレードした後、新 ヘルス モニタのコンテンツは更新されていません。最新(デフォルト) のコンテンツを使用するには、NetWitness Liveサービスを使用してコンテンツを導入する必要があります。

注 : NetWitness Liveサービスからコンテンツを導入すると、既存のコンテンツが上書きされるため、導入前に11.4.x.xのヘルス モニタ コンテンツのコピーを作成しておくことを推奨します。

1. NetWitness Platform UIにログインします。
2.  (**構成**) > [**LIVEコンテンツ**] をクリックします。
3. [**検索条件**] パネルで、次の[**リソース タイプ**] を選択します。
   - Health and Wellness Dashboards
   - Health and Wellness Monitors
4. [**検索**] をクリックします。
5. [**一致するリソース**] ビューで、導入するリソースの左側にあるチェックボックスをオンにします。
6. [**一致するリソース**] パネルのツールバーで、  をクリックします。
7. [**導入ウィザード**] > [**リソース**] タブで、[**次へ**] をクリックします。
8. [**サービス**] タブで、Metrics Serverサービスを選択します。
9. [**次へ**] をクリックします。
10. [**導入**] をクリックします。
    [**導入**] ページが表示されます。選択したサービスにリソースが正常に導入されると、進捗バーが緑色に変わります。
11. [**閉じる**] をクリックします。

(オプション) サービス構成ドキュメントの新ヘルス モニタ ホストのUUIDを更新する

set-config APIを使用して、新ヘルス モニタのサービスをnw-shellから構成しており、NetWitness Platformのバージョンを11.4.x.xから11.6にアップグレードする場合は、新ヘルス モニタがインストールされるホストのIPをUUIDで更新する必要があります。

1. SSHでNetWitness Serverに接続します。
2. 次のコマンドを使用して、新ヘルス モニタがインストールされているホストのUUIDを確認します。
   ```
   orchestration-cli-client --list-hosts
   ```
   このコマンドは、NetWitness Platformホストと各ホストのUUIDを一覧表示します。新ヘルス モニタがインストールされているホストのUUIDを記録しておきます。
3. 次のコマンドを使用して、set-configが呼び出されるサービスを特定します。
   ```
   mongo localhost/metrics-server -u deploy_admin -p <deployment_password> --
   authenticationDatabase admin --eval 'db.metric_config.find({ "createdBy": {
   $ne: "system" }})'
   ```
   このコマンドは、set-configが呼び出されるサービスの構成ドキュメントを一覧表示します。

注: サービスのドキュメントが表示されない場合は、アップグレードの前にサービスが構成されていないことを意味するため、残りのステップを無視して構いません。

4. 構成ファイルのサービスドキュメントの「host」フィールドのIPアドレスを、新ヘルス モニタがインストールされているホストのUUIDに置き換えます。
   たとえば、次のようにホストのIPアドレスをUUIDに変更します。

```
"host" : "e086511c-121c-4e66-95a3-e87e27b12acb"
```

5. コマンド
   ```
   nw-shell
   ```
   を使用してnw-shellにログインします。
6. 次のコマンドを使用して、metrics-serverサービスに接続します。
   ```
   connect --service metrics-server
   ```
7. ログイン コマンドを入力します。
   ```
   login
   ```
8. adminのユーザ名とパスワードを入力します。
9. /rsa/metrics/elastic/set-configに移動し、コマンド
   ```
   invoke --file /<absolute_path_of_service_config_file>
   ```
   を使用して構成ファイルを呼び出します。

Investigate

(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11.6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(およびその他)の標準提供ユーザ ロールではinvestigate-server.event.filter権限が有効になりますが、この権限がアップグレード プロセスによってカスタム ユーザ ロールで有効になることはありません。この権限が有効になっていないカスタム ユーザ ロールを割り当てられたユーザには、[イベントの絞り込み]パネルが表示されません。これは、メタデータをドリルダウンできる11.6の新しいパネルです。

注: [調査]ビューを使用するアナリスト用の標準提供ユーザ ロールでは、バージョン11.4で追加された別の3つの権限も有効になりますが、これらの権限がアップグレード プロセスによってカスタム ユーザ ロールで有効になることはありません。これらの権限がないカスタム ユーザ ロールを割り当てられているユーザには、[ナビゲート]ビューと[レガシー イベント]ビューが[調査]メニューに表示されません。カスタム ユーザ ロールで有効にする必要がある3つの権限は、次のとおりです。
investigate-server.columngroup.read、investigate-server.metagroup.read、investigate-server.profile.read

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. 編集が必要なカスタム 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4つの権限が有効になっていることを確認します。
   investigate-server.event.filter
   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11.6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、Respond Serverサービスは、プライマリESAホストも11.6にアップグレードするまでは自動的に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。

(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>`

(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。
この手順は、11.3.xから11.6へのアップグレードに適用されます。11.4.xから11.6にアップグレードする場合は、アップグレード中に上書きされない個別の`custom_normalize`スクリプトファイルにカスタマイズが追加されるため、正規化スクリプトファイルはバックアップされません。

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>`**<timestamp>ディレクトリにあるバックアップされたRespond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。ここで、`<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. **`/var/lib/netwitness/respond-server/scripts`**ディレクトリにある11.4以降の新しい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。正規化スクリプトをカスタマイズする場合は、`custom` というプレフィックスの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javaスクリプト ファイルには、パラメータにheaders、rawAlert、normalizedAlertを持つ関数「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。

```
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);

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;

};
```

custom_normalize_alerts.jsスクリプトの更新によるDetect AI検出イベントの正規化

アップグレード プロセス中のcustom_normalize_alerts.jsスクリプトの上書きを防ぐには、custom_normalize_alerts.jsスクリプトの編集と更新を行って、Detect AIイベントの正規化に必要な関数を含めます。

1.vi /var/netwitness/respond-server/scripts/custom_normalize_alerts.jsファイルを見つけます。

2.次のコードを行番号12に追加します。
```
"custom_normalize_detectai_alerts"
```

3.次のコードを行番号41に追加します。
```
else if(headers.deviceProduct == "Detect AI")

{ transformer = transformers["custom_normalize_detectai_alerts"]; }
```

また、normalize_alerts.jsなど、標準提供のRespond正規化スクリプト ファイルを参照することもできます。詳細については、『*NetWitness Respond構成ガイド*』の「カスタムRespondサーバ アラート正規化の構成」を参照してください。

リファレンスLog Decoder

すべての機能を利用するには、リファレンスLog Decoderが11.6以降であることを確認します。リファレンスLog Decoderをセットアップしていない場合は、このタスクを実行する必要はありません。詳細については、『*ログ パーサ カスタマイズ ガイド*』を参照してください。

Windows Log Collector

Windows Log CollectorのUUIDを更新する

11.6へのアップグレード後に、お使いの環境で構成されているWindows Log Collectorごとに、次のコマンドをNW Serverで実行します。

```
wlc-cli-client --update-to-uuid --host <WLC host address>
```

User Entity Behavior Analytics

重要: アップグレード前に、タスクの失敗の問題が発生し、それを解決した場合は、アップグレード後にauthentication.jsonファイルを置き換えてから、アップグレード後のタスクを実行する必要があります。Airflowでのタスクの失敗の問題とその解決策は、『UEBA構成ガイド』の「トラブルシューティング」トピックで説明されています。

重要: すべてのUEBA環境では、アップグレード プロセスを完了するために追加の手順が必要となります。11.5.0.0または11.5.1.0から11.6.0.0にアップグレードする場合は、11.5.1.0の『アップグレード ガイド』に記載されているUEBAの手順を実行してから11.6.0.0にアップグレードする必要があります。

注: 11.4.xから11.6.0.0へのアップグレード時に、現在の処理スキーマを更新しない場合は、過去28日間についてUEBAシステムを再実行する必要はありません。11.4.xより前のバージョンから11.6.0.0へのアップグレード時には、UEBAシステムが自動的に再実行されます。

1. (仮想マシンの場合のみ) VMのAirflow並列処理を更新します。
   UEBAシステムがVMで実行されている場合は、UEBAホストでrootとして次のコマンドを実行して、Airflowの並列処理を64に更新します。

   ```
   sed -i "s|parallelism = 256|parallelism = 64|g"
   /var/netwitness/presidio/airflow/airflow.cfg
   ```

2. UEBAマシンから次のコマンドを使用して、UEBA構成を更新します。

   ```
   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
   ```

3. (オプション) 次のスクリプトを使用して、UEBA処理スキーマを更新します。

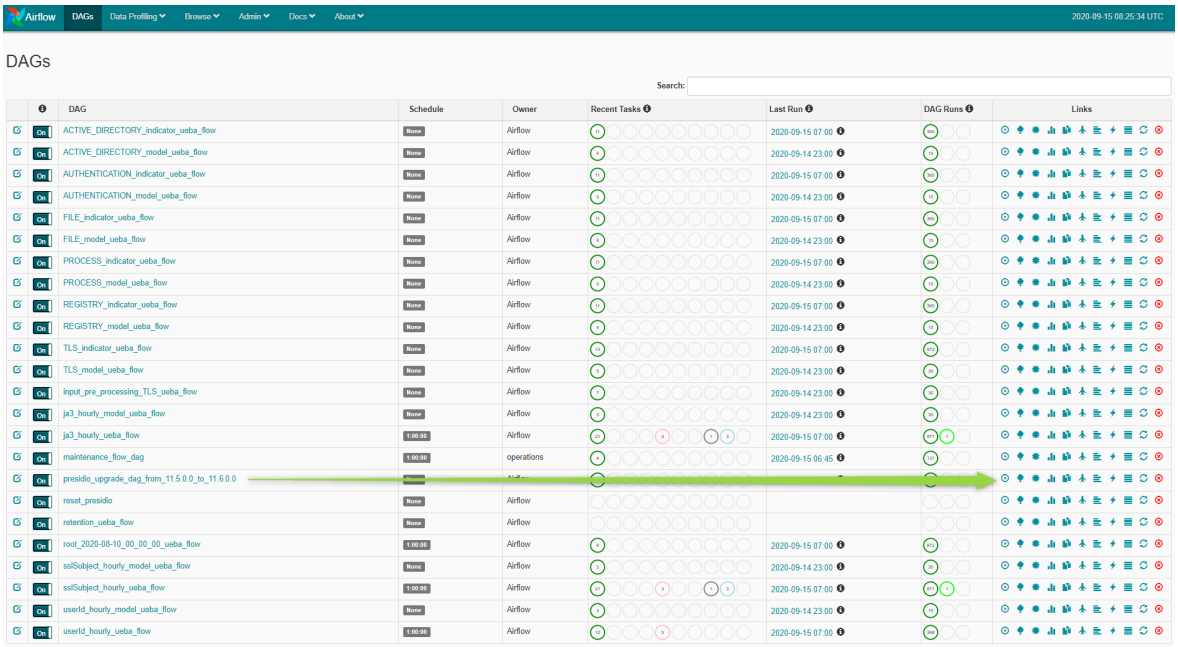
   ```
   python /var/netwitness/presidio/airflow/venv/lib/python2.7/site-
   packages/presidio_workflows-1.0-py2.7.egg/presidio/utils/airflow/reset_
   presidio.py script.
   ```

   UEBA開始日を現在の日付より28日前に設定することを推奨します。TLSデータの処理を予定しているUEBAシステムの場合は、開始日が現在の日付より14日以上前の日付に設定されていることを確認する必要があります。

   詳細については、『*UEBA構成ガイド*』の「reset-presidioスクリプト」を参照してください。

4. AirflowのDAGアップグレードを実行します。
   - Airflowのメイン ページhttps://<UEBA-host-name>/adminに移動します。
   - adminのユーザ名とパスワードを入力します。

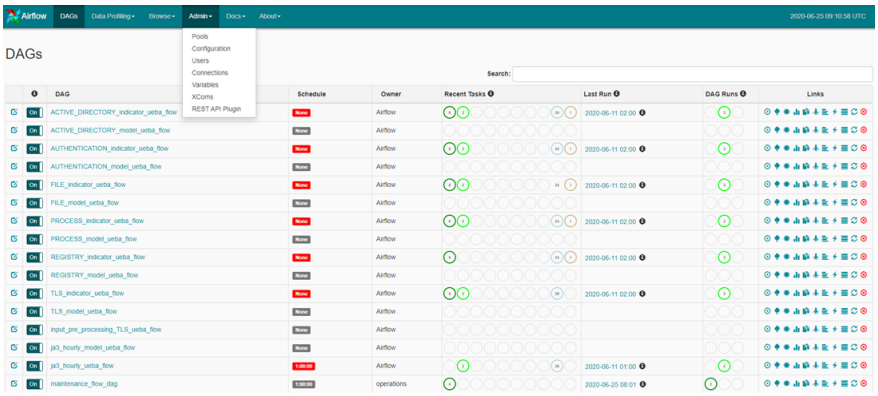
- `presidio_upgarde_dag_from_<previous_version> to_11.6.0.0`で[**再生**]をクリックします。



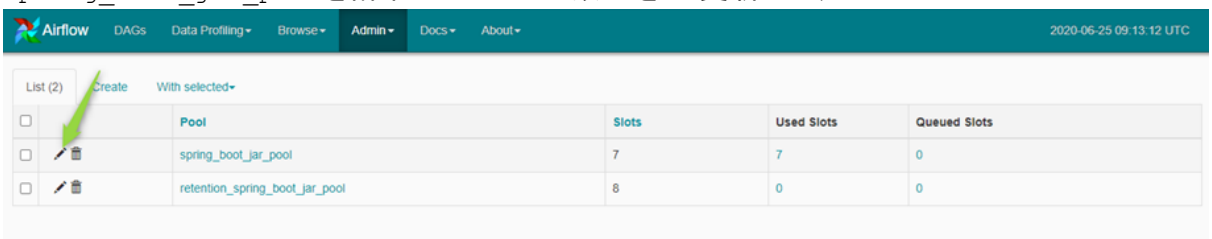
注: アップグレード中は、DAGアップグレード行の横に緑色の丸が表示されます。アップグレード プロセスが正常に完了した場合は、明るい緑色の円が緑色に変わります。アップグレード プロセスが失敗した場合は、明るい緑色の円が赤に変わります。

5. 適切な「Boot Jar Pools」スロットを設定します。
   - **物理アプライアンス**: `spring_boot_jar_pool`スロット値を18に更新します。
   - **仮想アプライアンス**: `spring_boot_jar_pool`および`retention_spring_boot_jar_pool`スロットの値を22に更新します。
     "Spring Boot Jar Pools" スロットを更新するには、Airflowのメイン ページに移動し、最上部のバーにある[管理]タブをタップし、[プール]をタップします。
   a. Airflow UIにアクセスするには、`https://<UEBA_host>/admin`にアクセスし、認証情報を入力します。
      ユーザ: admin
      パスワード : この環境のdeploy adminパスワード

b. プールの鉛筆マークをクリックして、スロットの値を更新します。



6. `spring_boot_jar_pool`を編集し、スロットの数量を5に更新します。



エンドポイントのアップグレード タスク

11.6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. アップグレードした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て、リレー サーバを11.6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は、「マスター目次」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 11.6 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。

新機能の使用開始

11.6にアップグレードした後は、数多くの魅力的な新機能を有効にすることができます。NetWitness Platformの各領域の新機能の一覧を以下に示します。このリリースの新機能の詳細については、『RSA NetWitness Platform 11.6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は、「マスター目次」で確認できます。

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

調査 - SIEMとネットワークトラフィックの分析

- ファセット検索
- 調査コンテンツ(列グループ、メタ グループ、クエリー プロファイル) の整理
- RSA Liveを使用した調査コンテンツ(列グループ、メタ グループ、クエリー プロファイル) の配信
- 値が複数
- 直接自由形式のクエリーまたはテキスト検索
- クエリー フィルタの機能強化
- 追加のメタ キーのサポートの強化
- カスタム列グループの機能強化
- 画面レイアウト オプションの調査
- メタ パネルの機能強化
- IndexNoneメタ キー
- 再構築の機能強化(コンテンツ表示とコピー オプション)

- 検索インジケータ
- タイムアウト設定の調査

User Entity Behavior Analytics

新機能と機能強化

インシデント対応

永続データへの応答(ベータ版)

エンドポイントの調査

- YARAスキャンのサポート
- UIを使用した集中型エージェント アップグレード オプション
- UIを使用した集中型エージェント アンインストール オプション
- 複数のダウンロード済みファイルのローカル コピー保存のサポート
- 任意のWindowsドライブからのMFTのダウンロードのサポート
- 横方向の動きの可視性の拡大
- カスタム システムへのWindows/ファイル ログ転送のサポート

Broker、Concentrator、Decoder、Log Decoderサービス

- アセンブラー スレッディング モード
- 高速パケット収集
- Brotli解凍のサポート
- OpenApp IDのサポート
- 受信側スケーリングのサポート
- 暗号化および復号化されたトラフィック ストリームのDecoderへの同時取得
- アグリゲーション ホストのための信頼できる認証

Event Stream Analysis(ESA)

- メタ エンティティのサポート
- 位置追跡情報のインポートと編集
- 信頼できる認証の活用
- Detect AIのサポート

管理と構成

不要なダッシュボードの削除

Context Hub

- REST APIデータ ソースのサポート
- コンテキスト ハイライト表示の機能強化

ログ収集

- マネージドLogstashのサポート
- 解析ルールUIの機能強化

ライセンス

ライセンス使用ダッシュボードの導入

プラットフォーム

サードパーティ サーバ ハードウェアのサポート

付録A:オフライン方式(Liveサービスに接続しない) - コマンド ライン インターフェイス

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/) > [**NetWitness Platform**] > [**RSA NetWitness Logs and Network**] > [**Downloads**] > [RSA Downloads]からローカル ディレクトリに`netwitness-11.6.0.0.zip`ファイルをダウンロードしておく必要があります。

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. 11.6.0.0の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。
   - NW Serverに`root`としてログインし、`/tmp/upgrade/11.6.0.0`というディレクトリを作成します。
     次に、NW Serverの`/root`ディレクトリにパッケージzipファイルをコピーし、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-11.6.0.0.zip -d /tmp/upgrade/11.6.0.0`

   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 11.6.0.0 --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-<ID, name or address> <ID / display name / (hostname/ IP address)> --version 11.6.0.0`
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. 他のコンポーネント ホストについて、ステップ3および4を繰り返します。

注: NW Serverホストで`upgrade-cli-client --list`コマンドを実行すると、すべてのホストのバージョンをチェックすることができます。`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： アップグレード処理中に、次のエラーが表示される場合があります。
```
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)
```
この場合でも、サービス パックは正しくインストールされます。何のアクションを取る必要もありません。新しいバージョンにホストを更新する際に他のエラーが発生した場合は、カスタマー サポート (https://community.rsa.com/docs/DOC-1294) にお問い合わせください。

CLIによるアップグレードのための外部リポジトリの準備

1. 11.6.0.0の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。
2. 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/11.6.0.0`
   次に、NW Serverの`/root`ディレクトリにパッケージzipファイルをコピーし、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-11.6.0.0.zip -d /tmp/upgrade/11.6.0.0`

   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。
3. 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 11.6.0.0 --stage-dir /tmp/upgrade`
4. 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-<ID, name or address> <ID / display name / (hostname/ IP address)> --version 11.6.0.0`
5. 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。
6. 他のコンポーネント ホストについて、ステップ3および4を繰り返します。

注： NW Serverホストで`upgrade-cli-client --list`コマンドを実行すると、すべてのホストのバージョンをチェックすることができます。`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： アップグレード処理中に次のエラーが表示される場合があります。
```
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)
```
この場合でも、サービス パックは正しくインストールされます。何のアクションを取る必要もありません。新しいバージョンにホストを更新する際に他のエラーが発生した場合は、カスタマー サポートにお問い合わせください。

付録B.外部リポジトリのセットアップ

外部リポジトリ(Repo) をセットアップするには、次の手順を実行します。

注: 1.) この手順を完了するには、ホストに解凍ユーティリティがインストールされている必要があります。2.) 次の手順を実行する前に、Webサーバの作成方法を理解している必要があります。

1. (オプション) 外部リポジトリがあり、それを上書きする場合に、この手順を実行します。
   - ケース1: 外部リポジトリからホストをセットアップしたが、NetWitness Serverホスト上のローカルリポジトリを使用してアップグレードしたい場合。
     a. `/etc/netwitness/platform/repobase`ファイルを作成します。
        `vi /etc/netwitness/platform/repobase`
     b. `repobase`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。
        `https://nw-node-zero/nwrpmrepo`
     c. `upgrade-cli-client`ツールを使用してアップグレードを実行するための手順を完了します。
   - ケース2: NetWitness Serverホスト上のローカルリポジトリからホストをセットアップしたが、外部リポジトリを使用してアップグレードしたい場合。
     a. `/etc/netwitness/platform/repobase`ファイルを作成します。
        `vi /etc/netwitness/platform/repobase`
     b. `repobase`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。
        `https://<webserver-ip>/<alias-for-repo>`
     c. `upgrade-cli-client`ツールを使用してアップグレードを実行するための手順を完了します。
        手順は、『*RSA NetWitness Platform アップグレード ガイド*』の「付録A: オフライン方式(Liveサービスに接続しない) - コマンド ライン インターフェイス」に記載されています。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。
2. 外部リポジトリをセットアップします。
   a. Webサーバ ホストにログインします。
   b. NWリポジトリ(`netwitness-11.6.0.0.zip`) をホストするディレクトリを作成します(例: Webサーバーの`web-root`の下の`ziprepo`) 。たとえば、/var/netwitnessがweb-root場合、次のコマンドを実行します。
      `mkdir -p /var/netwitness/<your-zip-file-repo>`
   c. 11.6.0.0 ディレクトリを`/var/netwitness/<your-zip-file-repo>`の下に作成します。
      `mkdir -p /var/netwitness/<your-zip-file-repo>/11.6.0.0`
   d. `OS`および`RSA`ディレクトリを`/var/netwitness/<your-zip-file-repo>/11.6.0.0`の下に作成します。
      ```
      mkdir -p /var/netwitness/<your-zip-file-repo>/11.6.0.0/OS
      mkdir -p /var/netwitness/<your-zip-file-repo>/11.6.0.0/RSA
      ```

e. netwitness-11.6.0.0.zipファイルを/var/netwitness/<your-zip-file-repo>/11.6.0.0ディレクトリに解凍します。
unzip netwitness-11.6.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.6.0.0netwitness-11.6.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.6.0.0
netwitness-11.6.0.0.zipを解凍すると、2つのZipファイル(OS-11.6.0.0.zipとRSA-11.6.0.0.zip) とその他のいくつかのファイルが現れます。

f. 以下のように解凍します。
OS-11.6.0.0.zipを /var/netwitness/<your-zip-file-repo>/11.6.0.0/OSディレクトリに解凍します。
unzip /var/netwitness/<your-zip-file-repo>/11.6.0.0/OS-11.6.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.6.0.0/OS

Repoの外部urlはhttp://<web server IP address>/<your-zip-file-repo>です。

g. 以下のように解凍します。
RSA-11.6.0.0.zipを/var/netwitness/<your-zip-file-repo>/11.6.0.0/RSAディレクトリに解凍します。
unzip /var/netwitness/<your-zip-file-repo>/11.6.0.0/RSA-11.6.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.6.0.0/RSA

h. (オプション: Azureの場合) : Azureの更新の場合は、次の手順を実行します。

   i. mkdir -p /var/netwitness/<your-zip-file-repo>/11.6.0.0/OS/other
   ii. unzip nw-azure-11.3-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.6.0.0/OS/other
   iii. cd /var/netwitness/<your-zip-file-repo>/11.6.0.0/OS
   iv. createrepo

i. NW 11.6.0.0セットアップ プログラム(nwsetup-tui) が[**Enter the base URL of the external update repositories**]プロンプトを表示したら、 http://<web server IP address>/<your-zip-file-repo>と入力します。

付録C: インストールと更新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 アップデート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アップデートまたはインストールの問題がある場合は、カスタマー サポートにお問い合わせください。

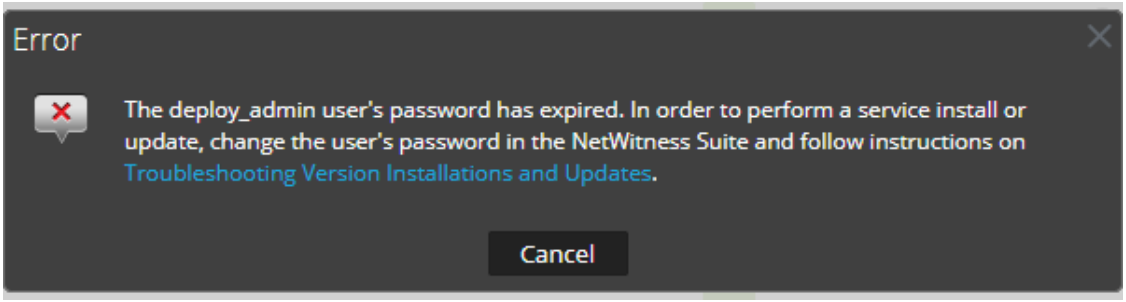
このセクションでは、アップグレード中に発生する可能性がある次のエラーのトラブルシューティング手順について説明します。

- 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
- アップグレード失敗エラー
- 外部リポジトリ更新エラー
- 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。

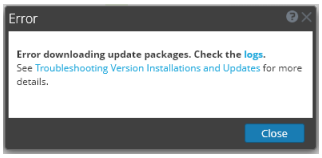
- Log Collectorサービス
- NW Server
- Orchestration
- Reporting Engine
- Event Stream Analysis

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。

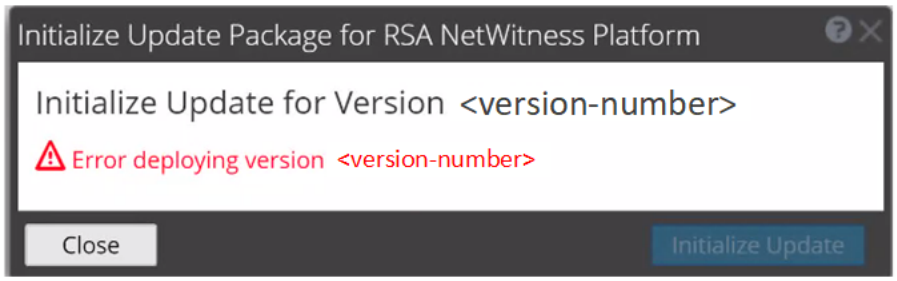
解決策	deploy_adminのパスワードをリセットします。
	1. NW Serverホストのみで次のコマンドを実行します。
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	2. nw-manage --update-deploy-admin-pwコマンドの出力を確認して、deploy_adminパスワードがすべてのホストで正常に更新されたことを確認します。NWホストがダウンしているか、nw-manage --update-deploy-admin-pwコマンドの出力に表示されている何らかの理由で失敗した場合は、通信障害が解決された後でnw-manage --sync-deploy-admin-pw --host-key <host-identifier>を実行して、失敗したホストとNW Serverの間でパスワードを同期します。
	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 11.6 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 インターフェイ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は、「マスター目次」で確認できます。 3. それでもアップデートできない場合は、カスタマー 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

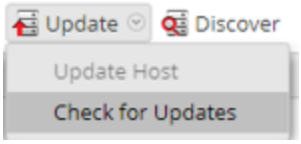


問題

「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[**更新の開始**]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。

アップグレード失敗エラー

エラーメッセージ

ホストをバージョン11.2以降にアップデートまたはインストールするときに、次のエラーが発生する場合があります。このエラーは、/var/log/netwitness/config-management/chef-solo.logに記録されています。

```
.......
[2019-04-16T20:55:32+00:00] ERROR: Running exception handlers
[2019-04-16T20:55:32+00:00] ERROR: Exception handlers complete
[2019-04-16T20:55:32+00:00] FATAL: Stacktrace dumped to /var/lib/netwitness/config-management/cache/chef-stacktrace.out
[2019-04-16T20:55:32+00:00] FATAL: Please provide the contents of the stacktrace.out file if you file a bug report
[2019-04-16T20:55:32+00:00] ERROR: ruby_block[resolve ips] (nw-dns-client::config line 69) had an error: Resolv::ResolvError: no address for 889e5752-6ae3-4286-
33f4ccbc
[2019-04-16T20:55:32+00:00] FATAL: Chef::Exceptions::ChildConvergeError: Chef run process exited unsuccessfully (exit code 1)
```

原因	原因としては、ターゲット ホストがAdmin Server上のdnsmasqサービスを使用して名前(この場合は889e5752-6ae3-4286-a944-c182 33f4ccbc)を解決する際に、ポート53でAdmin Serverと通信できないことが考えられます。これは、Admin Serverのsalt minion IDです。この値を確認するには、Admin Serverで「cat /etc/salt/minion」を実行します。出力例: [root@S5-NWAdmin ~]# cat /etc/salt/minion master: localhost hash_type: sha256 log_level: info id: 889e5752-6ae3-4286-a944-c18233f4ccbc
解決策	可能な場合は、ポート53で通信できるように、ターゲット ホストとAdmin Serverホストの間のファイアウォールを構成します。これが不可能な場合の回避策は、コンポーネント ホストの/etc/hostファイルにミニオンIDを含め、11.4リリース以降、この回避策を上書きしないようにchefレシピを変更することです。
回避策	KB記事「Install/Upgrade fails in RSA NetWitness Platform because Resolv::ResolvError:no address for a particular host」を参照してください。

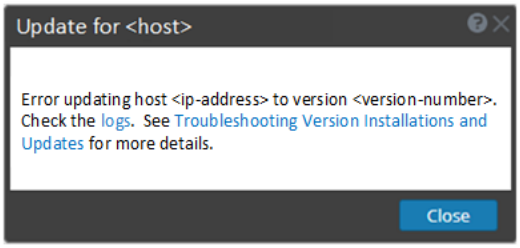
エラーメッセージ	バージョン11.6にアップデートしようとすると、次のようなエラーがログに出力されました。 FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobufs-rt
原因	ホスト上にインストールされた一部のコンポーネントがカスタム ビルド/rpmです(Hotfixをインストールした場合など)。
解決策	この問題を解決するには、次の手順に従います。 1. SSHでNetWitness Serverに接続します。 2. 次のコマンドを実行して、コンポーネント ディスクリプタ ファイルのディレクトリに移動します。 cd /etc/netwitness/component-descriptor/ 3. 次のコマンドを実行して、コンポーネント ディスクリプタ ファイルを開きます。 vi nw-component-descriptor. json 4. カスタム ビルド/rpmをインストールしたコンポーネントの「packages」セクションを検索します。次の例は、カスタム ビルド/rpmをインストールした「concentrator」ホストのパッケージの詳細を示しています。 "concentrator": { "cookbook_name": "rsa-concentrator", "service_names": ["rsa-nw-concentrator"], "family": "launch", "default_port": xxxx, "description": "Concentrator", "**packages**":[{ "name": "rsa-nw-concentrator", "version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos" }, 5. packagesセクションのバージョン情報をすべて(「,」文字を含む)削除します。次の例は、

	バージョン情報を削除した後のpackagesセクションです。 "packages": [{ "name": "rsa-nw-concentrator" }, **注**: Admin Serverのコンポーネント ディスクリプタで、カスタム ビルド/rpmをインストールしたすべてのホストのバージョン情報を削除する必要があります。 6. アップグレード プロセスを再度実行します。

外部リポジトリ更新エラー

エラーメッセージ	以下から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発生しました。 .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、スペースを削除している。

ホスト更新失敗エラー

エラーメッセージ	
問題	アップデート バージョンを選択し、[**アップデート**] > [**ホストのアップデート**] クリックすると、ダウンロード プロセスは成功しますが、アップデート 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アップデートできない場合は、次の手順を実行してください。 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。 3. それでもアップデートを適用できない場合は、ステップ2のログを収集して、カスタマー 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	**バージョンxx.x.x.xのアップデートの初期化** 次のアップデート パッケージが見つかりません RSA Linkからパッケージをダウンロードしてください
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。 [**RSA NetWitness Platformのアップデート パッケージの初期化**]ダイアログが開き、アップデート 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。以下に例を示します。
	`$ 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。以下に例を示します。
	`$ 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で、次のようなエラーが発生しました。 **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11.6.0.0にアップデートすると、NW Server以外のホストの唯一のアップデート パスは、同じバージョン(つまり、11.6.0.0) 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.x.x) に更新しようとすると、このエラーが表示されます。
解決策	2つの選択肢があります。 • NW Server以外のホストを11.6.0.0にアップデートします。 • 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リブートした後に、ユーザ インタフェースにホストをリブートするようメッセージが表示されます。 SA Server IP-Address 8 version-number Reboot Host
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]ビューでホストをリブートします。

アップグレード後のReporting Engine再起動

問題	11.4などの11.xのバージョンから11.6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。

問題	バージョン11.6にアップグレードした後で、Reporting Engineサービスが再起動されません。
原因	Reporting Engineサービスは、次のいずれかの理由により起動しない場合があります。 - workspace.xmlが更新されていない。 - livechart h2データベースで時間が正しく変換されていない。 - JCR(Jackrabbitリポジトリ) がプライマリキー違反で破損している。

解決策	この問題を解決するには、Reporting EngineサービスがインストールされているAdmin Server上でReporting Engine移行リカバリツール(`rsa-nw-re-migration-recovery.sh`) を実行します。
	注 : Reporting Engine移行リカバリー ツールは次の場所にあります。
	`/opt/rsa/soc/reporting-engine-11.6.0.0-<Tag>/nwtools`
	1.SSHでNetWitness Serverに接続します。
	2.次のコマンドを実行してRE(Reporting Engine) ツールを解凍します。
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`
	3.(オプション) 別のディレクトリにREツール ファイルを解凍する場合は、ディレクトリを作成してREツールを解凍できます。次のコマンドを実行します。
	`mkdir <NAME OF THE DIRECTORY>`
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`
	4.次のコマンドを実行してスクリプトを実行します。
	`./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh`
	詳細については、ナレッジベース記事「**Reporting Engine Migration Recovery Tool**」を参照してください。

Log Collectorサービス(`nwlogcollector`)

Log Collectorのインストール 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。

エラーメッセージ	`<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.`
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	Decoderがイベントの収集を開始しようとしますが失敗します。 `Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.`

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. SSHを使用してDecoderホストに接続します。
	2. 次のコマンドを実行します。
	`yum reinstall pfring*`
	`systemctl restart nwdecoder`

NW Server

これらのログは、NW Serverのホスト上の`/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、11.4.x.xまたは11.5.x.xから11.6.0.0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。

Event Stream Analysis

問題	バージョン11.6にアップグレードした後で、ESA Correlationサーバーは構成されたデータソースからのイベントを集計しません。
エラーメッセージ	`Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)`
解決策	この問題を解決するには、次の手順を実行します。

NetWitness Platformのユーザ インタフェースで、

1. (Configure) > [ESAルール]に移動します。
   [ESAルール]パネルで[ルール]タブが表示されます。
2. [ルール]タブのオプション パネルの[導入環境]の下で、導入環境を選択します。
3. [データ ソース]セクションで、データ ソースを選択して、ツールバーのをクリックします。
4. [サービスの編集]ダイアログで、そのデータ ソースのパスワードを入力します。
5. [接続のテスト]ボタンをクリックして、ESAサービスと通信できることを確認してから、[OK]をクリックします。

注: 構成されたすべてのデータ ソースについて、前述の手順を実行します。

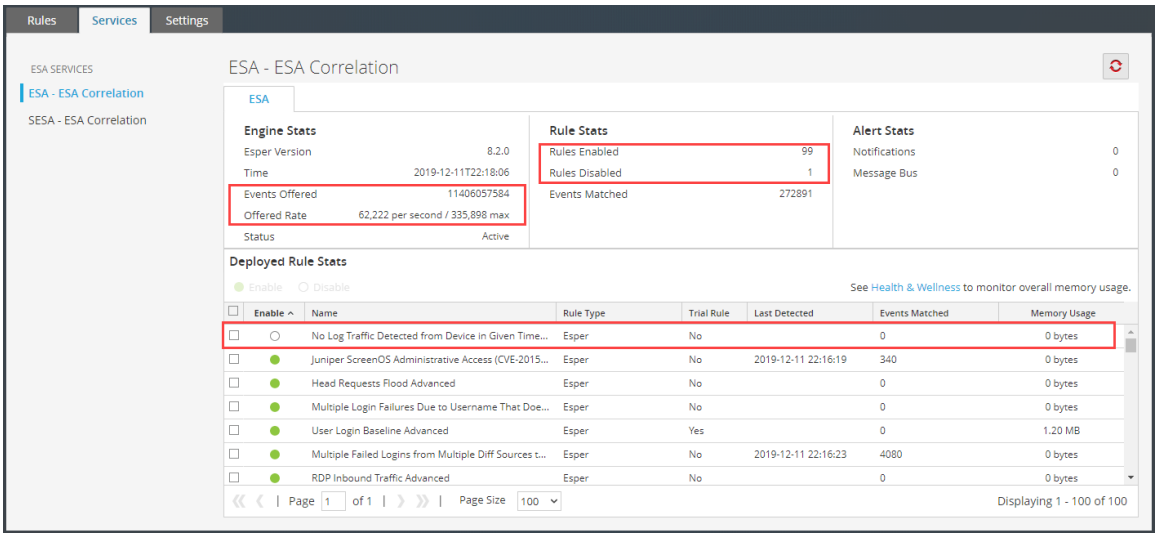
6. 導入環境に変更を加えた後、[今すぐ導入]をクリックしてESAルール導入環境を再導入します。

ESAトラブルシューティング情報

ESAルールによってアラートが作成されない

アラートが表示されない場合は、ESAルールの導入ステータスを確認してください。

1. (Configure) > [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]の値を確認します。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]の値を確認します。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統計]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. **(Configure) > [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。ルールが引き続き無効な場合は、`/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。

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、UEBA、Liveコンテンツ ルールが機能していない

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以降、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、文字列配列の変更については、手動で調整が必要となる可能性があります。

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
```

メタ キーを更新するには、『*ESA構成ガイド*』の「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」を参照してください。

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は、「マスター目次」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は、「マスター目次」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 parameter`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。『*ESA構成ガイド*』の「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
```