

RSA®

RSA® NetWitness

Version 11.7

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。

© 2020 RSA Security LLC or its affiliates.All Rights Reserved.

12月 2021

目次

アップグレードの概要	6
アップグレード パス	6
混在モードでの実行	6
ESAホストのアップグレードに関する考慮事項	6
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	7
Windows Legacy収集の更新またはインストール	7
製品ドキュメントへのフィードバック	7
NetWitness Platformのヘルプ情報	8
セルフ ヘルプ リソース	8
カスタマー サポート へのお問い合わせ	8
アップグレード前チェック	9
アップグレード準備タスク	10
タスク1.(オプション) レガシー パッケージ リポジトリを削除する	10
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	10
アップグレード オプション	11
重要な注意事項 - 最初にお読みください	11
コンポーネント ホストの時刻をNW Serverホストと同期する	11
混在モードのESAホストはサポート 対象外	11
Endpoint Hybridシステムはサポート 対象外	12
NW ServerとESAプライマリホストを11.7にアップグレード するまでRespond Serverサービスは有効になりません。	12
Deploy_Admin/パスワードのガイドライン	12
アップグレード オプション	12
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	13
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	14
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 アップグレード ファイルを配置	14
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	14
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	15
アップグレード後のタスク	16
全般	16
(オプション) NAT経由のIPアドレスを構成する	16
(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	16
/etc/hosts.userから古いホスト エントリを削除する	17

DNSサーバを再構成する	17
サービスの再起動、データ収集、データ集計の確認	17
ESA Analyticsのアップグレードに関する考慮事項	19
新ヘルス モニタ	19
Liveを使用して新ヘルス モニタのコンテンツを導入する	19
(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	20
Investigate	21
(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	21
対応	21
(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	22
(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	22
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	24
リファレンスLog Decoder	24
Windows Log Collector	24
Windows Log CollectorのUUIDを更新する	24
User Entity Behavior Analytics	25
Endpointアップグレード タスク	28
11.7リレー サーバーのインストール	28
Endpointエージェントのアップグレード	28
新機能の使用開始	29
調査	29
Concentrator、Decoder、Log Decoderサービス	30
Event Stream Analysis(ESA)	30
プラットフォーム	30
アップグレード	30
NetWitnessサービス	30
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	31
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	32
付録B :外部リポジトリのセットアップ	33
付録C :インストールと更新のトラブルシューティング	35
deploy_adminのユーザ パスワード有効期限切れエラー	36
ダウンロード エラー	37
バージョン<version-number>の導入エラー :更新パッケージの不足	38
アップグレード失敗エラー	38
外部リポジトリ更新エラー	40
ホスト更新失敗エラー	40
更新パッケージ不足エラー	41
OpenSSL 1.1.x	41
NW Server以外へのパッチ適用エラー	42

コマンド ラインからの更新後のホスト再起動のエラー	42
アップグレード後のReporting Engine再起動	42
Log Collectorサービス(nwlogcollector)	44
NW Server	46
Orchestration	47
Reporting Engineサービス	47
Event Stream Analysis	47
ESAトラブルシューティング情報	48
ESAルールによってアラートが作成されない	48
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	49
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	50

アップグレードの概要

NetWitness 11.7.0.0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。

11.7では、NetWitnessユーザー 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 11.7.0.0では、以下のアップグレード パスがサポートされます。

- NetWitness 11.5.3.2から11.7.0.0へ
- NetWitness 11.6.0.0から11.7.0.0へ
- NetWitness 11.6.0.1から11.7.0.0へ
- NetWitness 11.6.1.0から11.7.0.0へ
- NetWitness 11.6.1.1から11.7.0.0へ

バージョン11.5.x.x以前からアップグレードする場合は、11.5.3.2または11.6.0.0にアップグレードしてから11.7.0.0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 11.5.3.2アップグレード 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。

注：アップグレード前チェックのホット フィックスを、いずれかのバージョン(11.5.x.xまたは11.6.x.x)にインストールしている場合は、ホット フィックスをアンインストールしてから、次のコマンドを使用して11.7.0.0にアップグレードする必要があります。

```
-rpm -qa | grep prechecks-hotfix | xargs -I{} yum remove -y {}
```

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11.7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に関する全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/>
- NetWitness **ナレッジベース**を参照してください。
- NetWitness **トラブルシューティング**のページを参照してください。
- NetWitness **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
- 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

アップグレード前チェック

NetWitness 11.7.0.0にアップグレードする前にアップグレード前チェックを実行して、アップグレードの失敗につながる可能性のある問題を特定する必要があります。

アップグレード前チェックを実行するには、次の手順を実行します。

1. 管理者コンソールにログインします。

2. 次のコマンドを実行します。

```
nw-precheck-tool upgrade-checklist
```

アップグレード前チェックでは、次のことを確認します。

- **セキュリティクライアント ファイル チェック** :`security-client-amqp.yml`ファイルが存在しないことを確認する
- **ノード0 NWサービスIDステータス** :すべてのサービスIDが、ノード0のすべての種類のサービスと一致していることを確認する
- **ブローカー サービストラストピア シンボリックリンク** :ブローカーのシンボリックリンク ファイル (`/etc/netwitness/ng/broker/trustpeers/`) が破損していないことを確認する
- **ノード0 NWサービス ステータス** :ノード0のすべてのサービスのステータスを確認する
- **Yum外部リポジトリ チェック** :外部リポジトリが使用可能ではなく、有効でもないことを確認する
- **RPM DBインデックス チェック** :RPM DBが破損していないかどうかを確認する
- **ソルト マスター通信** :ノード0からすべてのノードへのソルト通信を確認する
- **ノード0証明書のチェック** :欠落しているか、期限が切れているか、有効な発行者タイプである証明書があるかどうかを確認する
- **Mongo認証** :Mongoクライアントを使用して、`security-cli-client`から取得した`deploy_admin`認証情報を検証する
- **RabbitMQ認証** :RabbitMQを使用して、`security-cli-client`から取得した`deploy_admin`認証情報を検証する

アップグレード準備タスク

次のタスクを実行して、NetWitness 11.7にアップグレードする準備を行います。

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-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 フォルダ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 フォルダ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 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 フォルダ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 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.x.xから11.7.0.0へのアップグレードに適用されません。

11.4から11.7.xにアップグレードする場合は、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。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ホストを導入しており、11.3.x.xもしくは11.4.x.xにてEndpoint Log Hybridホストをインストールしていない場合は、11.7でEndpoint Log Hybridホストをインストールする必要があります。11.7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11.7にアップグレードするまでRespond

Serverサービスは有効になりません。

NW Server(Respond Serverサービスを含む)をアップグレードした後、ESAプライマリホストを11.7にアップグレードするまでは、Respond Serverサービスが自動的に再び有効になりません。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。

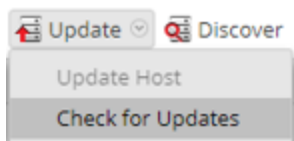
前提条件


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1.7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 [1.7]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


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 11.7] を選択して、アップグレード パッケージ netwitness-11.7.0.0.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-11.7.0.0.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-11.7.0.0.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-11.7.0.0.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。

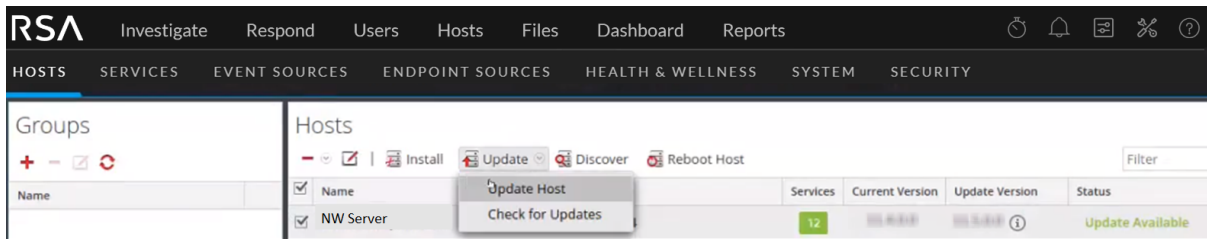
- NetWitness Platformが更新パッケージにアクセスできる。
- パッケージが完全でエラーがない。

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。



6. **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。
7. 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

11.7にアップグレードした後のNetWitnessユーザー インターフェイスには、いくつかの新機能があります。ご使用のホストのタスクを完了してください。

- [全般](#)
- [Event Stream Analysis\(ESA\)](#)
- [新ヘルス モニタ](#)
- [Investigate](#)
- [対応](#)
- [リファレンスLog Decoder](#)
- [Windows Log Collector](#)
- [User Entity Behavior Analytics](#)

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

次の手順を完了する前に、ウォームスタンバイ サーバーを11.7にアップグレードしておく必要があります。

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



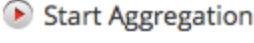
ネットワーク収集の開始

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関連ルールとESA関連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関連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関連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11.7にアップグレードした後も、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 [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、 Deploy 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、nw-shellから新ヘルス モニターのサービスを構成しており、NetWitness Platformのバージョンを11.4.x.xから11.7にアップグレードする場合は、新ヘルス モニターがインストールされているホストのIPをUUIDに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 モニター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 モニター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 モニター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、[サビゲート]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。

対応

これらのタスクを完了する前に、プライマリESAサーバーを11.7にアップグレードする必要があります。

注： NW Server(Respond Serverサービスを含む) をアップグレードした後、ESAプライマリーホストを11.7にアップグレードするまでは、Respond Serverサービスが自動的に再び有効になりません。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11.7へのアップグレードに適用されます。11.4.xから11.7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11.7.0.0にアップグレードする場合は、11.7.0.0にアップグレードする前に、11.5.1.0のアップグレード ガイドに記載されたUEBAの手順を実行する必要があります。

注：11.4.x.xから11.7.0.0にアップグレードするときに、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11.7.0.0にアップグレードすると、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_upgrade_dag_from_<previous_version> to_11.7.0.0で **再生]**をクリックします。

The screenshot shows the Airflow web interface with a table of DAGs. The table has columns for DAG, Schedule, Owner, Recent Tasks, Last Run, DAG Runs, and Links. The 'presidio_upgrade_dag_from_' DAG is highlighted with a green arrow pointing to its 'DAG Runs' column, which contains a green circle icon.

DAG	Schedule	Owner	Recent Tasks	Last Run	DAG Runs	Links
ACTIVE_DIRECTORY_indicator_ueba_flow	None	Airflow	○	○	○	○
ACTIVE_DIRECTORY_model_ueba_flow	None	Airflow	○	○	○	○
AUTHENTICATION_indicator_ueba_flow	None	Airflow	○	○	○	○
AUTHENTICATION_model_ueba_flow	None	Airflow	○	○	○	○
FILE_indicator_ueba_flow	None	Airflow	○	○	○	○
FILE_model_ueba_flow	None	Airflow	○	○	○	○
PROCESS_indicator_ueba_flow	None	Airflow	○	○	○	○
PROCESS_model_ueba_flow	None	Airflow	○	○	○	○
REGISTRY_indicator_ueba_flow	None	Airflow	○	○	○	○
REGISTRY_model_ueba_flow	None	Airflow	○	○	○	○
TLS_indicator_ueba_flow	None	Airflow	○	○	○	○
TLS_model_ueba_flow	None	Airflow	○	○	○	○
input_pre_processing_TLS_ueba_flow	None	Airflow	○	○	○	○
ja3_hourly_model_ueba_flow	None	Airflow	○	○	○	○
ja3_hourly_ueba_flow	1:00:00	Airflow	○	○	○	○
maintenance_flow_dag	1:00:00	operations	○	○	○	○
presidio_upgrade_dag_from_	None	Airflow	○	○	○	○
reset_presidio	None	Airflow	○	○	○	○
retention_ueba_flow	None	Airflow	○	○	○	○
root_2020-08-10_00_00_00_ueba_flow	1:00:00	Airflow	○	○	○	○
saslSubject_hourly_model_ueba_flow	None	Airflow	○	○	○	○
saslSubject_hourly_ueba_flow	1:00:00	Airflow	○	○	○	○
userid_hourly_model_ueba_flow	None	Airflow	○	○	○	○
userid_hourly_ueba_flow	1:00:00	Airflow	○	○	○	○

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。

DAG	Schedule	Owner	Recent Tasks	Last Run	DAG Runs	Links
ACTIVE_DIRECTORY_indicator_uetba_flow	...	Airflow	...	2020-06-11 02:00
ACTIVE_DIRECTORY_model_uetba_flow	...	Airflow	...	2020-06-11 02:00
AUTHENTICATION_indicator_uetba_flow	...	Airflow	...	2020-06-11 02:00
AUTHENTICATION_model_uetba_flow	...	Airflow	...	2020-06-11 02:00
FILE_indicator_uetba_flow	...	Airflow	...	2020-06-11 02:00
FILE_model_uetba_flow	...	Airflow	...	2020-06-11 02:00
PROCESS_indicator_uetba_flow	...	Airflow	...	2020-06-11 02:00
PROCESS_model_uetba_flow	...	Airflow	...	2020-06-11 02:00
REGISTRY_indicator_uetba_flow	...	Airflow	...	2020-06-11 02:00
REGISTRY_model_uetba_flow	...	Airflow	...	2020-06-11 02:00
TLS_indicator_uetba_flow	...	Airflow	...	2020-06-11 02:00
TLS_model_uetba_flow	...	Airflow	...	2020-06-11 02:00
input_pre_processing_TLS_uetba_flow	...	Airflow
pk3_hourly_model_uetba_flow	...	Airflow	...	2020-06-11 01:00
pk3_hourly_uetba_flow	...	Airflow	...	2020-06-25 08:01
maintenance_flow_dag	...	operations	...	2020-06-25 08:01

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

Pool	Slots	Used Slots	Queued Slots
spring_boot_jar_pool	7	7	0
retention_spring_boot_jar_pool	8	0	0

Endpointアップグレード タスク

11.7リレー サーバーのインストール

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 サーバーのインストーラをダウンロードして、リレー サーバーを11.7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 11.7 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

11.7にアップグレードすると、多くの魅力的な新機能を使用できるようになります。NetWitness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 11.7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](#)
- [エンドポイントの調査](#)
- [Concentrator、Decoder、Log Decoderサービス](#)
- [Event Stream Analysis\(ESA\)](#)
- [プラットフォーム](#)
- [アップグレード](#)
- [NetWitnessサービス](#)

調査

- メタのみのイベントの再構築
- ブローカー クエリー エクスペリエンスの向上
- Eメールの再構築の改善
- [イベント フィルター] パネルでのメタキーとクエリーの直接対話
- ネットワークフラグメントの識別
- 保存された時間範囲

エンドポイントの調査

- Endpoint Serverのロールベースのきめ細かいアクセス制御
- *endpoint-server.agent.manage*から削除され、*endpoint-server.file.analyze*に追加された権限
- タグを使用したホスト管理
- 拡張されたWindowsエージェントによる、レジストリーを対象とした永続化手法の検出のサポート
- 疑わしいスレッドの検出の強化
- 管理者特権で開いたコマンド プロンプトからの、ブロックされたファイルの削除

Concentrator、Decoder、Log Decoderサービス

- 一元化された構成管理の導入
- クエリーの正確さの向上

Event Stream Analysis(ESA)

- イベントとインシデントの永続化機能の強化

プラットフォーム

- バックアップ機能とリストア機能の強化

アップグレード

- アップグレード前チェックユーティリティの導入

NetWitnessサービス

- NetWitnessサービストポロジー マップの導入

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] > [RSA NetWitness Logs and Network] > [Downloads] > [RSA Downloads] からローカル ディレクトリにnetwitness-11.7.0.0.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. 11.7.0.0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行います。

- NW Serverにrootとしてログインし、
/tmp/upgrade/11.7.0.0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-11.7.0.0.zip -d /tmp/upgrade/11.7.0.0

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 11.7.0.0 --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 11.7.0.0
```

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 インターフェイスの [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。ホストを新しいバージョンにアップグレード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 \(https://community.rsa.com/docs/DOC-1294\)](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

- 11.7.0.0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行います。
- rootとしてNW Serverにログインし、次のディレクトリを作成します。/tmp/upgrade/11.7.0.0
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-11.7.0.0.zip -d /tmp/upgrade/11.7.0.0

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。

- 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 11.7.0.0 --stage-dir /tmp/upgrade
- 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 11.7.0.0
- 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。
- 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-11.7.0.0.zip`) をホストするディレクトリを作成します (例 : Webサーバの `web-root` の下の `ziprepo`)。たとえば、`/var/netwitness` が `web-root` の場合、次のコマンドを実行します。

```
mkdir -p /var/netwitness/<your-zip-file-repo>
```
 - c. 11.7.0.0 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>/11.7.0.0
```
 - d. OS および RSA ディレクトリを `/var/netwitness/<your-zip-file-repo>/11.7.0.0` の下に作成します。

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.7.0.0/RSA
```

- e. netwitness-11.7.0.0.zipファイルを/var/netwitness/<your-zip-file-repo>/11.7.0.0ディレクトリに解凍します。
- ```
unzip netwitness-11.7.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.7.0.0netwitness-11.7.0.0.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-11.7.0.0.zipとRSA-11.7.0.0.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-11.7.0.0.zipを /var/netwitness/<your-zip-file-repo>/11.7.0.0/OSディレクトリに解凍します。
- ```
unzip /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS-11.7.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.7.0.0/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-11.7.0.0.zipを/var/netwitness/<your-zip-file-repo>/11.7.0.0/RSAディレクトリに解凍します。
- ```
unzip /var/netwitness/<your-zip-file-repo>/11.7.0.0/RSA-11.7.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.7.0.0/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>/11.7.0.0/OS/other
```
  - ii. 

```
unzip nw-azure-11.3-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS/other
```
  - iii. 

```
cd /var/netwitness/<your-zip-file-repo>/11.7.0.0/OS
```
  - iv. 

```
createrepo
```
- i. NW 11.7.0.0セットアッププログラム(nwsetup-tui)で **Enter the base URL of the external update repositories** プロンプトが表示されたら、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。

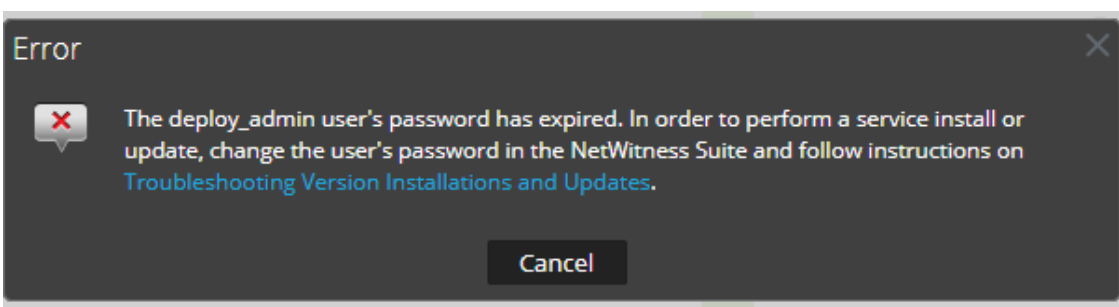
このセクションでは、アップグレード中に発生する可能性がある次のエラーのトラブルシューティング手順について説明します。

- [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](#)

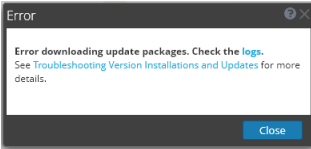

次のホストおよびサービスのアップグレード中またはアップグレード後に発生する可能性があるエラーについても、トラブルシューティング手順を記載しています。

- [Log Collectorサービス](#)
- [NW Server](#)
- [Orchestration](#)
- [Reporting Engine](#)
- [Event Stream Analysis](#)

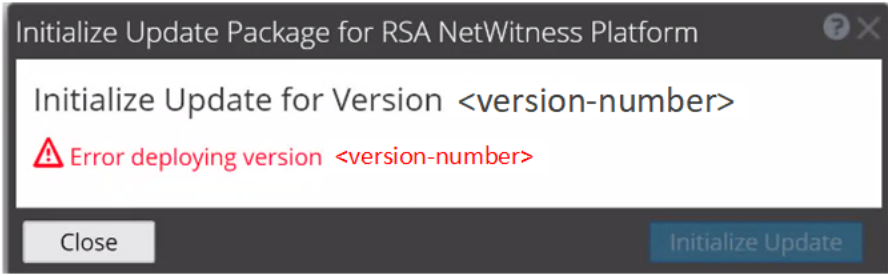
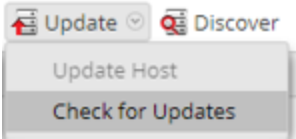
## deploy\_adminのユーザパスワード有効期限切れエラー

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー<br>メッ<br>セー<br>ジ |  <p>The dialog box is titled "Error" and contains the following text: "The deploy_admin user's password has expired. In order to perform a service install or update, change the user's password in the NetWitness Suite and follow instructions on <a href="#">Troubleshooting Version Installations and Updates</a>." There is a "Cancel" button at the bottom.</p>                                                                                                                                                                                                                                                                                                                                     |
| 原因                   | <p>deploy_adminのユーザパスワードの有効期限が切れています。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 解決<br>策              | <p>deploy_adminのパスワードをリセットします。</p> <ol style="list-style-type: none"> <li>NW Serverホストのみで次のコマンドを実行します。<br/> <pre>nw-manage --update-deploy-admin-pw</pre> Please enter the new deploy_admin account password: &lt;new-deploy-admin-password&gt;<br/> Please confirm the new deploy_admin account password: &lt;new-deploy-admin-password&gt; </li> <li>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 &lt;host-identifier&gt;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。</li> <li>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。</li> </ol> |

## ダウンロード エラー

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー<br>メッ<br>セー<br>ジ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 問題                   | 更新バージョンを選択し、 <b>更新</b> ] > <b>ホストの更新</b> ]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<br>策              | <ol style="list-style-type: none"> <li>更新を再実行します。</li> <li>同じエラーで再度失敗した場合は、『NetWitness Platform 11.xアップグレード ガイド』の「<b>ホスト</b>]ビューからのオフライン方式」または「<b>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</b>」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、「<a href="#">マスター目次</a>」で確認できます。</li> <li>それでもアップデートできない場合は、<a href="#">カスタマー サポート</a>にお問い合わせください。</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| エラー<br>メッ<br>セー<br>ジ | NetWitness Platform 11.x.x.xから11.6.x.x以降にアップグレードする場合、UIによるオフラインアップグレードが失敗し、「 <b>ダウンロード エラー</b> 」メッセージが表示されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 解決<br>策              | <ol style="list-style-type: none"> <li>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。 <ol style="list-style-type: none"> <li>SSHでNW Serverに接続します。</li> <li>次のコマンドを実行します。 <pre>upgrade-cli-client --upgrade --host-key &lt;ID, IP address, hostname or display name of host&gt; --version &lt;version number&gt;</pre> <b>For example:</b> <pre>upgrade-cli-client --upgrade --host-key &lt;ID, IP address, hostname or display name of host&gt; --version 11.6.0.0</pre> </li> </ol> </li> <li>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、 (<b>管理</b>) &gt; <b>ホスト</b>]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。</li> <li>ツールバーの <b>ホストの再起動</b>]をクリックします。 <p>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。</p> <ol style="list-style-type: none"> <li><b>更新あり</b>]ダイアログの <b>更新を開始</b>]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。</li> <li>ツールバーの <b>ホストの再起動</b>]をクリックします。</li> </ol> </li> </ol> |

## バージョン&lt;version-number&gt;の導入エラー :更新パッケージの不足

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー<br>メッ<br>セー<br>ジ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 問題                   | <p>「バージョン &lt;version-number&gt;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、<b>更新の初期化</b>]をクリックした後で、<b>RSA NetWitness Platformの更新パッケージの初期化</b>]ダイアログに表示されます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 解決<br>策              | <ol style="list-style-type: none"> <li>1. <b>閉じる</b>]をクリックしてダイアログを閉じます。</li> <li>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。</li> <li>3. salt-masterサービスが実行されていることを確認します。</li> <li>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。</li> <li>5. <b>ホスト</b>]ビューのツールバーで、<b>更新の確認</b>]を再度選択します。</li> </ol>  <ol style="list-style-type: none"> <li>6. <b>更新の初期化</b>]をクリックします。</li> <li>7. ツールバーの <b>更新</b>] &gt; <b>ホストの更新</b>]をクリックします。</li> <li>8. <b>更新あり</b>]ダイアログで <b>更新の開始</b>]をクリックします。<br/>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。</li> <li>9. ツールバーの <b>ホストの再起動</b>]をクリックします。</li> </ol> |

## アップグレード失敗エラー

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー<br>メッ<br>セー<br>ジ | <p>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。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 原因                   | <pre> ..... [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 889e5752-6ae3-4286-33f44cdbc [2019-04-16T20:55:32+00:00] FATAL: Chef::Exceptions::ChildConvergeError: Chef run process exited unsuccessfully (exit code 1) </pre> |
| 原因                   | <p>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</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                   |                                                                                                                                                                                                                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <p>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：</p> <pre> [root@S5-NWAdmin ~]# cat /etc/salt/minion master: localhost hash_type: sha256 log_level: info id: 889e5752-6ae3-4286-a944-c18233f4ccbc </pre> |
| <p><b>解決策</b></p> | <p>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。</p>                                                                                                                                                                     |
| <p><b>回避策</b></p> | <p>KB記事「<a href="#">Install/Upgrade fails in RSA NetWitness Platform because Resolv::ResolvError:no address for a particular host</a>」を参照してください。</p>                                                                                                                                                                                       |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>エラーメッセージ</b></p> | <p>バージョン11.6以降に更新しようとする、次のようなエラーがログに出力されました。</p> <pre> FATAL: Chef::Exceptions::Package: yum_package[rsa-protobuffs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobuffs-rt </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p><b>原因</b></p>       | <p>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)。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p><b>解決策</b></p>      | <p>この問題を解決するには、次の手順に従います。</p> <ol style="list-style-type: none"> <li>SSHでNetWitness Serverに接続します。</li> <li>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。 <pre>cd /etc/netwitness/component-descriptor/</pre> </li> <li>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。 <pre>vi nw-component-descriptor.json</pre> </li> <li>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。 <pre> "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"   }, </pre> </li> <li>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。</li> </ol> |

```
"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<br>メッセ<br>ージ | 以下から新しいバージョンに更新しようとする、次のようなエラーが発生しました。<br>.Repository 'nw-rsa-base': Error parsing config: Error parsing<br>"baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'":<br>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。 <ul style="list-style-type: none"> <li>• URLがNW Serverホスト上に存在する。</li> <li>• 正しいパスを使用し、スペースを削除している。</li> </ul>                                                                                                      |

## ホスト更新失敗エラー

|                  |                                                                                                                                                                                                                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー<br>メッセ<br>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]をクリックすると、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              | <ol style="list-style-type: none"> <li>1. ホストへのバージョン更新の適用を再試行します。<br/>通常は、これで問題が解決されます。</li> <li>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。<br/>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)。<br/>/var/netwitness/uax/logs/sa.log<br/>/var/log/netwitness/orchestration-server/orchestration-server.log</li> </ol> |



```
/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。

- 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<br>メッ<br>セー<br>ジ | バージョンxx.x.x.xのアップデートの初期化<br>次のアップデート パッケージが見つかりません<br><a href="#">RSA Linkからパッケージをダウンロードしてください</a>                                                                                                                                                                                                                                                                |
| 問題                   | 「次の更新 パッケージが見つかりません」は、 <a href="#">[ホスト]</a> 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、 <a href="#">RSA NetWitness Platformの更新パッケージの初期化</a> ダイアログに表示されます。                                                                                                                                                                                                   |
| 解決<br>策              | <ol style="list-style-type: none"> <li><a href="#">RSA NetWitness Platformの更新パッケージの初期化</a> ダイアログで <a href="#">[RSA Linkからパッケージをダウンロード]</a> をクリックします。<br/>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。</li> <li>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。<br/><a href="#">RSA NetWitness Platformのアップデート パッケージの初期化</a> 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。</li> </ol> |

## OpenSSL 1.1.x


|                      |                                                                                                                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー<br>メッ<br>セー<br>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。<br>\$ ssh root@10.1.2.3<br>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、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。<br>\$ rpm -q openssl<br>openssl-1.1.1-8.el8.x86_64                   |
| 解決<br>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。<br>\$ ssh -oCiphers=aes128-ctr,aes192-ctr,aes256-ctr root@10.1.2.3<br><br>I've read & consent to terms in IS user agreement.<br><br>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 | <pre>/var/log/netwitness/orchestration-server/orchestration-server.logで、<br/>次のようなエラーが発生しました。<br/>API Failure /rsa/orchestration/task/update-config-management<br/>[counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is<br/>not supported</pre> |
| 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以降に更新すると、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、11.6.0.0)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。 <ul style="list-style-type: none"> <li>• NW Server以外のホストを11.6.0.0以降に更新します。</li> <li>• 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)。</li> </ul>                                                                                                            |

## 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ポートした後に、ユーザ インタフェースにホストをリポートするようメッセージが表示されます。<br> |
| 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ポートします。                                                                                                                   |

## 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以降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。 <ol style="list-style-type: none"> <li>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。<br/><pre>/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log</pre>ファイルを開き、次のブロックを確認します。 <ul style="list-style-type: none"> <li>• 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。</li> </ul> </li> </ol> |

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。

- Reporting Engineサービスを停止します。
- 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。
- 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。

- Reporting Engineサービスを停止します。
- 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。
- 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以降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。<br>- workspace.xmlが更新されていない。<br>- livechart h2データベースで時間が正しく変換されていない。<br>- 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 | <p>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。</p> <p><b>注</b> :Reporting Engine移行リカバリ ツールは次の場所にあります。<br/>         /opt/rsa/soc/reporting-engine-&lt;version number&gt;-&lt;Tag&gt;/nwtools<br/> <b>例</b> :<br/>         /opt/rsa/soc/reporting-engine-11.6.0.0-&lt;Tag&gt;/nwtools</p> <ol style="list-style-type: none"> <li>1.SSHでNetWitness Serverに接続します。</li> <li>2.次のコマンドを実行してRE( Reporting Engine) ツールを解凍します。<br/>         tar -xvf rsa-nw-re-recovery-tool-bundle.tar</li> <li>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。<br/>         mkdir &lt;NAME OF THE DIRECTORY&gt;<br/>         tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory &lt;PATH OF THE DIRECTORY&gt;</li> <li>4.次のコマンドを実行してスクリプトを実行します。<br/>         ./&lt;PATH OF THE DIRECTORY&gt;/rsa-nw-re-recovery-tool.sh</li> </ol> <p>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。</p> |

## 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 | <timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found |
|-----|--------------------------------------------------------------------|

|               |                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------|
| メッ<br>セー<br>ジ |                                                                                                                       |
| 原因            | 更新後、Log CollectorのLockboxが構成されていません。                                                                                  |
| 解決<br>策       | Log CollectorのLockboxを使用する場合は、NetWitness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<br>メッ<br>セー<br>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<br>策              | NetWitness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<br>メッ<br>セー<br>ジ | Decoderがイベントの収集を開始しようとして失敗します。<br><br><pre>Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.</pre>                                             |
| 解決<br>策              | この問題を解決するには、次の手順を実行します。<br><ol style="list-style-type: none"> <li>SSHを使用してDecoderホストに接続します。</li> <li>次のコマンドを実行します。<br/> <pre>yum reinstall pfring* systemctl restart nwdecoder</pre> </li> </ol> |

## 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わかりました。<br>または<br>次のメッセージがsa.logに記録されました。<br>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以降への移行に失敗しました。                                                                                                      |
| 解決<br>策 | <ol style="list-style-type: none"> <li>SSHでNW Serverに接続します。</li> <li>次のコマンドを実行します。<br/> <pre>orchestration-cli-client --update-admin-node</pre> </li> </ol>           |

## 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  | <ol style="list-style-type: none"> <li>1. 非NW Serverホストをアップグレードしようとしたが、失敗しました。</li> <li>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。</li> </ol>                                                                                               |
| 原因  | <p>orchestration-server.logに次のメッセージが記録されます。</p> <pre>'file' _virtual_ returned False: cannot import name HASHES'''</pre> <p>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。</p>                                   |
| 解決策 | <ol style="list-style-type: none"> <li>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。</li> <li>2. 次のコマンドを実行します。 <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> </li> <li>3. 非NW Serverホストのアップグレードを再試行します。</li> </ol> |

## 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 | <pre>&lt;timestamp&gt; : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ &gt;&lt;existing-GB &gt; ] is less than the required space [ &lt;required-GB&gt; ]</pre> |
| 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、『 <i>Reporting Engine構成ガイド</i> 』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以降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 | <pre>Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)</pre> |
| 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。

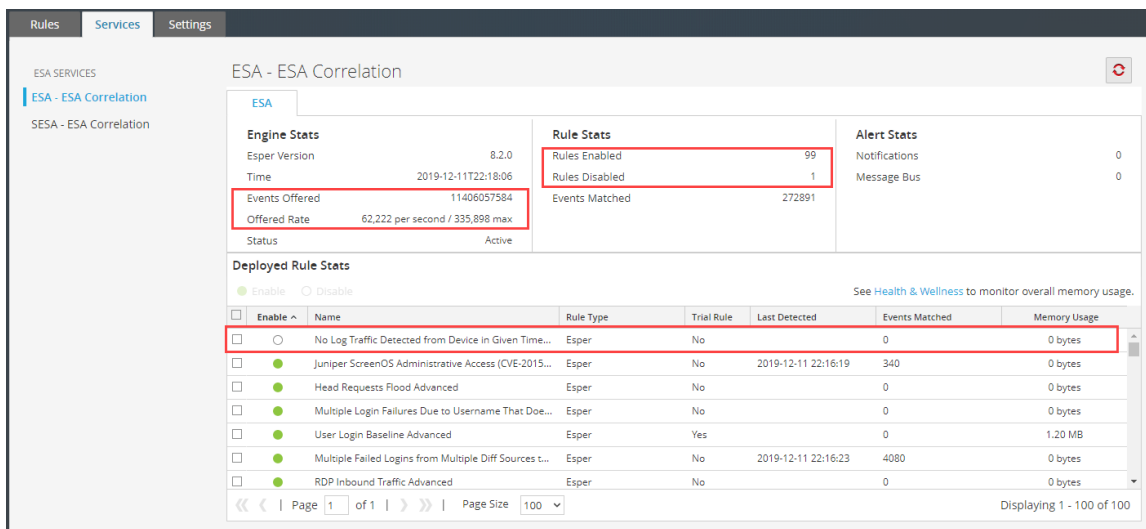
## ESAトラブルシューティング情報

### 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)から複数值(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関連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值メタ 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 関連ルール 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
```