NetWitness® Platform XDR

バージョン12.1.0.0

アップグレード ガイド

NETWITNESS
Platform XDR

連絡先

NetWitnessコミュニティ(https://community.netwitness.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およびその他の商標は、RSA Security LLCまたはその関連会社(「RSA」) の商標または登録商標です。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、それぞれの所有者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、NetWitnessコミュニティ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、本製品のユーザーは、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。

ディストリビューション

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

この資料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は、この資料に記載される情報に関する、どのような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への適応性に対する黙示的保証はいたしません。

10月, 2022

目次

アップグレードの概要

NetWitness 12.1.0.0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。

12.1.0.0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。

警告:UEBAホストを12.1にアップグレードする前に、ユーザー、エンティティ、アラート、インジケーターなどのElasticsearchデータのバックアップを実行して、アップグレード後も保持する必要があります。詳細については、「アップグレード準備タスク」を参照してください。

アップグレード パス

NetWitness 12.1.0.0では、以下のアップグレード パスがサポートされます。

- NetWitness 11.6.0.0から12.1.0.0へ
- NetWitness 11.6.0.1から12.1.0.0へ
- NetWitness 11.6.1.0から12.1.0.0へ
- NetWitness 11.6.1.1から12.1.0.0へ
- NetWitness 11.6.1.2から12.1.0.0へ
- NetWitness 11.6.1.3から12.1.0.0へ
- NetWitness 11.6.1.4から12.1.0.0へ
- NetWitness 11.7.0.0から12.1.0.0へ
- NetWitness 11.7.0.1から12.1.0.0へ
- NetWitness 11.7.0.2から12.1.0.0へ
- NetWitness 11.7.1.0から12.1.0.0へ
- NetWitness 11.7.1.1から12.1.0.0へ
- NetWitness 11.7.1.2から12.1.0.0へ
- NetWitness 12.0.0.0から12.1.0.0へ

このガイドは、物理ホストと仮想ホスト(AWSとAzure Public Cloudを含む)の両方に適用されます。

混在モードでの実行

混在モードは、最新バージョンにアップグレードされたサービスと、古いバージョンのままのサービスが混在するときに生じます。詳細については、『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 :を混在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12.1.0.0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、『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、『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。

Legacy Windows Log Collectionのアップグレードまたはインストール

『*Legacy Windows収集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@netwitness.comまでメールで送信してください。

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ついて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.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- 特定の情報を見つけるには、NetWitnessコミュニティー ポータルの［Search］および［Create a Post］フィールドを使用します(https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions) 。
- NetWitnessのナレッジベース：https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- ガイドの「トラブルシューティング」セクションを参照します。
- アプライアンスと製品のサポート終了(EOL) に関する情報については、 https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875を参照してください。
- https://community.netwitness.com/t5/netwitness-community-blog/bg-p/netwitness-blogも参照してください。
- 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NetWitness Platform製品またはアプリケーションのバージョン番号
- お使いのハードウェアのタイプ

質問や支援が必要な場合は、以下の連絡先までお問い合わせください。

NetWitnessコミュニティ ポータル	https://community.netwitness.com メイン メニューで［Support］>［Case Portal］>［View My Cases］をクリックします。
各国のお問い合わせ窓口	https://community.netwitness.com/t5/support/ct-p/support
コミュニティ	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW更新	https://update.netwitness.com
LiveUI	https://live.netwitness.com

アップグレード前チェック

NetWitness 12.1.0.0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。

アップグレード チェックリスト

- **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します。
- **ノード0 NWサービスIDステータス** :Node 0のすべての異なるサービスで、すべてのservice-idがそのままであることを確認する。
- **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します。
- **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します。
- **Yum外部リポジトリー チェック** :外部リポジトリーが使用可能ではなく、有効でもないことを確認します。
- **ノード0 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します。
- **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します。
- **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、無効な発行者タイプである証明書があるかどうかを確認します。
- **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`認証情報を検証します。
- **RabbitMQ認証** :RabbitMQを使用して、`security-cli-client`から取得した`deploy_admin`認証情報を検証します。
- **(コンポーネント ホスト) ノードX NWサービス ステータス** :すべてのノードXでサービスのステータス(アクティブまたは非アクティブ) を確認します。
- **(コンポーネント ホスト) ノードX証明書チェック** :ノードXのすべてのカテゴリーで、証明書の有効期限、欠落、破損、および発行者の不一致をチェックします。

- **ノードCPUメモリー情報** :すべてのノードのCPUおよびメモリーの詳細と、リアルタイムで使用可能なメモリーに関する情報を提供します。
- **(Admin Server) ノード0ファイル システム使用率** :ノード0で /var/netwitness/mongo、/var/netwitness、rootのディスク パーティション使用率を確認します。
- **(コンポーネント ホスト) ノードXファイル システム使用率** :ノードXでESA Primaryおよび Endpoint Log Hybridサービス用の /var/netwitness/mongo、/var/netwitness、rootのディスク パーティション使用率を確認します。
- **Mongoファイル(ESAPrimary)** :システムまたはスタック内のESAプライマリー ノードをチェックし、Mongoファイルのアクセス許可モードを確認します。
- **オーケストレーション サーバー通常モード** :オーケストレーション サービスが通常モードまたはセーフ モードで実行されているかどうかを確認します。
- **(Admin Server) ノード0初期状態** :初期化プロセスに失敗する可能性のある問題があるかどうかを確認します。
- **FIPSモード チェック** :アップグレードの前後に、FIPSモードが無効である(falseに設定されている) ことを確認します。
- **ノードX RPM DBインデックス チェック** :ノードX上のRPM DBのステータスをチェックして、破損していないことを確認します。
- **ノードZ Yumプロキシ チェック** :yum.confファイルの存在と、ノードZ上のファイル内のプロキシの可用性をチェックします。
- **ノードX Yumプロキシ チェック** :yum.confファイルの存在と、ノードX上のファイル内のプロキシの可用性をチェックします。
- **ホスト情報チェック プローブ** :システム内のすべてのホストの情報の必須入力フィールド(ホストIP、ホスト名、インストール済みサービス、およびRawバージョン) が利用可能かどうかを確認します。
- **ノードZ暗号チェック プローブ** :必要な暗号がノード0上の場所 /etc/rabbitmq/rabbitmq.configで使用可能かどうかを確認します。
- **ノードX暗号チェック プローブ** :必要な暗号がすべてのノードX上の場所 /etc/rabbitmq/rabbitmq.configで使用可能かどうかを確認します。
- **ノードXハードウェア バージョン チェック プローブ** :アクセス可能なすべてのノードXのハードウェア バージョンを確認します。
- **ノードZハードウェア バージョン チェック プローブ** :Admin Serverのハードウェア バージョンを確認します。

ネットワーク チェックリスト

- **(Admin Server) ノード0クローズド ポート** :NetWitnessサービスに必要なサービス ポートが開いていて、ノード0でリッスンしているかどうかを確認します。
- **(コンポーネント ホスト) ノードXクローズド ポート** :NetWitnessサービスに必要なサービス ポートが開いていて、ノードXでリッスンしているかどうかを確認します。

証明書チェックリスト

- **ノード0サービス証明書** :ノード0上の場所 `/etc/pki/nw/service/`にあるサービス証明書の有効性を確認します。
- **ノードXサービス証明書** :ノードX上の場所 `/etc/pki/nw/service/`にあるサービス証明書の有効性を確認します。
- **ノード0上ノード証明書** :ノード0上の場所 `/etc/pki/nw/service`にあるノード証明書の有効性を確認します。
- **ルートCA証明書** :場所 `/etc/pki/nw/ca`にあるルートCA証明書の有効性を確認します。

アップグレード準備タスク

次のタスクを実行して、NetWitness 12.1.0.0にアップグレードする準備を行います

警告 : Dell S4およびS4sアプライアンスは、2021年6月にサポート終了(EOL)になりました。これらのアプライアンスへのインストールまたはアップグレード作業を中止し、新しいハードウェアにアップグレードすることをお勧めします。ハードウェアサポート終了ハードウェアの詳細については、https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitnessplatform/ta-p/569875を参照してください。

タスク1.(オプション)レガシー パッケージ リポジトリーを削除する

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

1. 管理者ユーザー インターフェイスでホスト リストを確認するか、次のコマンドをNWサーバーで実行して、環境内で最も古いNetWitness Platformホストのバージョンを確認します。`upgrade-cli-client --list`
2. 環境内で最も古いアクティブ ホストのベースライン メジャー リリース バージョンより前のすべてのバージョンについては、NWサーバーの`/var/netwitness/common/repo/<version>`にあるすべてのレガシー パッケージ リポジトリー フォルダーを安全に削除できます
   - 最も古いホスト バージョンが11.7.x.xの場合は、11.0.x.x、11.1.x.x、11.2.x.x、11.3.x.x、11.4.x.x、11.5.x.x、11.6.x.xのリポジトリー フォルダーを安全に削除できます。ただし、11.7.0.0以降のリポジトリー バージョンは削除しないでください。
   - 最も古いホストバージョンが11.3.x.xの場合は、11.0.x.x、11.1.x.x、11.2.x.xのリポジトリー フォルダーを安全に削除できます。ただし、11.3.0.0以降のリポジトリー バージョンは削除しないでください。

タスク2 :ローテーションされたRabbitMQログをバックアップして削除する

11.6.xまたは11.7.xから12.1.0.0にアップグレードする前に、古いRabbitMQログを削除し、/var/logマウント ディスクのスペースを解放しておく必要があります。以下の手順に従って、/var/logマウント ディスクのスペースを解放します。

1. ローテーションされたRabbitMQログをvar/netwitnessディレクトリーにバックアップします。次の操作を実行します。

   ```
   mkdir /var/netwitness/rabbitmq_logsbkp
   ```

   ```
   scp -r /var/log/rabbitmq/ /var/netwitness/rabbitmq_logsbkp
   ```

2. ローテーションされたRabbitMQログをアップグレード前の/var/log/rabbitmqから削除します。次の操作を実行します。

   ```
   cd /var/log/rabbitmq
   ```

```
rm -f rabbit\@<sa-uuid>.log.*

rm -f rabbit\@<sa-uuid>_upgrade.log.*

rm -f *.gz

rm -f rabbit@<sa-uuid>.log-*
```

注：
- この手順は12.1.0.0にアップグレードする前に1回だけ実行する必要があります。アップグレード後、RabbitMQサービスは自動的にログローテーションを処理します。
- コマンド`rm -f rabbit\@<sa-uuid>.log.*`は、log.1、log.2、log.3などの圧縮されていない古いログをクリーンアップするために使用されます。
- コマンド`rm -f rabbit\@<sa-uuid>_upgrade.log.*`は、古い非圧縮アップグレード ログをクリーンアップするために使用されます。
- コマンド`rm -f *.gz`は、古い圧縮ログをクリーンアップするために使用されます。
- コマンド`rm -f rabbit@<sa-uuid>.log-*`は、logrotateでローテーションされた古い非圧縮ログをクリーンアップするために使用されます。

タスク3. Security Analytics l10n言語パックをアンインストールする

11.6.x.xから11.7.x.xまたは12.1.0.0バージョンにアップグレードする前に、Security Analytics l10n言語パックをアンインストールする必要があります。

タスク4 :12.1.0.0への移行のためにESA導入環境を準備する

12.1.0.0にアップグレードする前に、すべてのESA導入環境でエラーのない状態を維持し、未使用のESA導入環境を削除しておくことをお勧めします。これは、12.1.0.0へのアップグレード後にESA導入環境がポリシーとグループに移行されるためです。

注 : Admin Serverが完了した直後に相関サーバーがアップグレードされるように、アップグレード プロセスを計画してください。対応する相関サーバーがアップグレードされるまで、導入環境にはアクセスできません。このアクションは、相関サーバーによるイベントとアラートの処理には影響しません。

重要 :ESAルールとエンリッチメントをインポートする必要がある場合、アップグレードの前に、欠落しているルールとエンリッチメントをインポートしておくことをお勧めします。

次の表に、アップグレード前とアップグレード後の導入環境の状態を表します。

SINo	アップグレード前の導入環境の状態	アップグレード後の導入環境の状態		
		ポリシーの作成	グループの作成	ポリシーが公開されます
1	正常な導入環境	はい	はい	はい
2	エラーのある導入環境	はい	はい	はい
3	ルールのみを含んだ導入環境	はい	いいえ	いいえ
4	ルールのない導入環境	いいえ	いいえ	いいえ

正常な導入環境にはエラーがなく、ESAサーバー、データソース、ESAルールなどの必要なリソースが追加されます。

注 :すべての導入環境でエラーのない状態を維持し、不要または未使用のESA導入環境を削除することをお勧めします。

タスク5 :Elasticsearchデータ(ユーザー、エンティティ、アラート、インジケーター) をバックアップする

UEBAホストを12.1.0.0にアップグレードする前に、ユーザー、エンティティ、アラート、インジケーターなどのElasticsearchデータのバックアップを(Elasticsearch移行ツールを使用して) 実行し、アップグレード後も保持する必要があります。

前提条件

データバックアップを実行する前に、次の前提条件が満たされていることを確認してください。

- 現在のElasticsearchのバージョンが5.5.0でなければなりません。
- Presidio rpmのバージョンは12.0.0.0以下でなければなりません。
- `ueba_es_migration_tool.zip`ファイルがダウンロードされている必要があります。

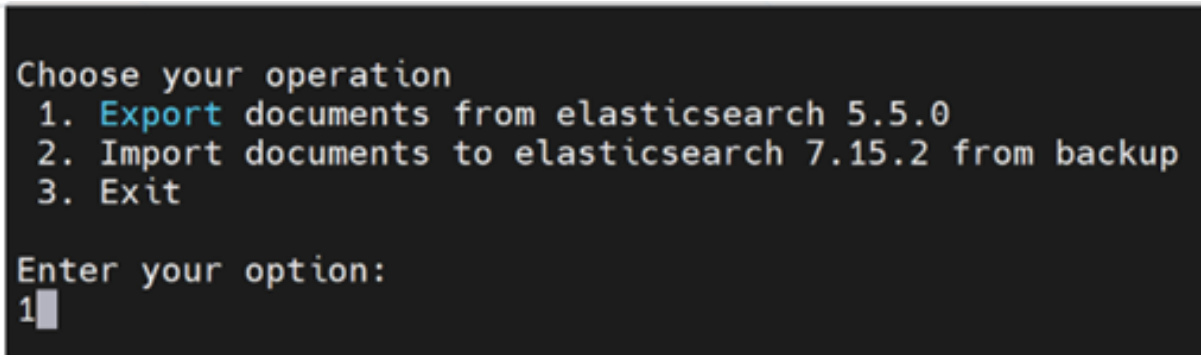
注 :ueba_es_migration_toolを使用すると、UEBAホストを12.0.0.0以前のバージョンから12.1.0.0にアップグレードする一方で、Presidio Elasticsearchデータを Elasticsearchバージョン5.5.0から7.15.2に移行できます。このツールは`elk-migration-script.sh`スクリプト ファイルと`presidio-elk-migration-1.0.0.jar`ファイルを含んでおり、https://community.netwitness.com/t5/netwitness-platform-downloads/ueba-elasticsearch-migration-tool/ta-p/687496からダウンロードできます。

Elasticsearchデータをバックアップするには：

1. 利用可能なディレクトリを選択して、`ueba_es_migration_tool.zip`ファイルを解凍します。
2. `cd ueba_es_migration_tool`に進みます。次のコマンドを実行します。

   `sh elk-migration-script.sh`

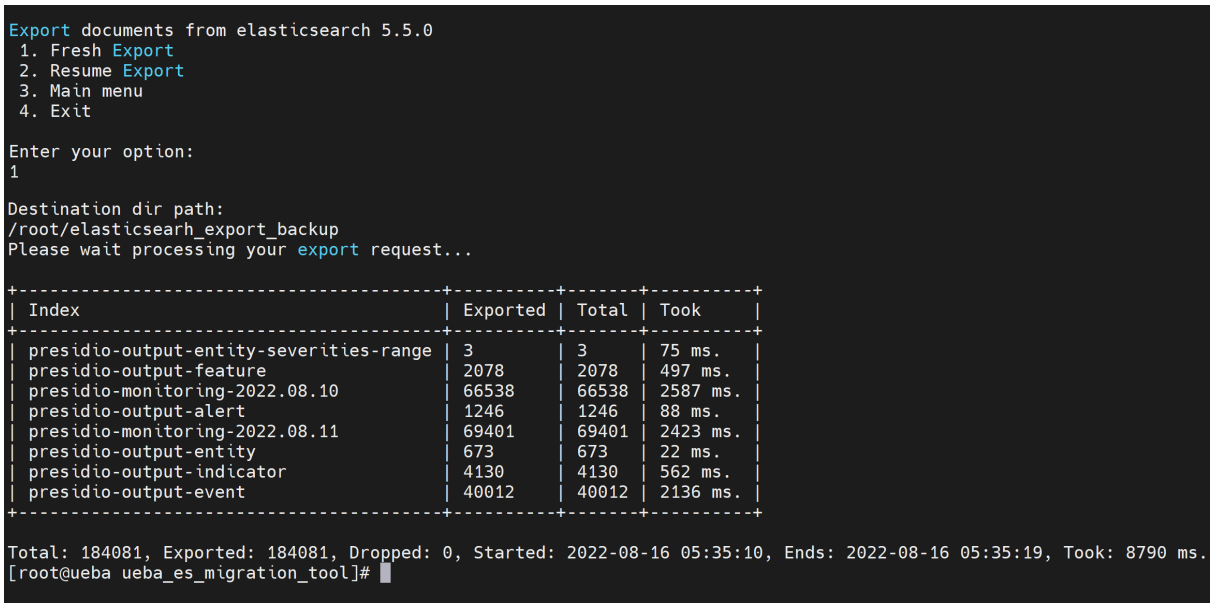
   Elasticsearch移行ツール ガイドが表示されます。



3. [**Elasticsearch 5.5.0からドキュメントをエクスポートする**]を選択して、Airflow Schedulerを停止するよう求められたら「**yes**」と入力します。

> **注**：「**yes**」と入力すると、Airflow Schedulerは、ユーザー、エンティティ、アラートなどの新しい受信データの使用を停止します。これにより、エクスポート プロセス中のデータ ロスを回避できます。

4. 次のステップで、 [**新しいエクスポート**]を選択して既存のデータをエクスポートします。



> **注**：
> - 技術的な問題が原因でエクスポート操作が失敗した場合は、問題が解決したら [**エクスポートの再開**]を選択してエクスポート操作を再開します。
> - 成功または失敗したプロセスのログを表示する場合は、`<backup_directory_path>/log/log/es-migration-export.log`に移動します。

タスク6(オプション) :STIGベースのFIPSカーネル コントロールを無効にする

STIGベースのFIPSカーネル コントロールを有効にした場合は、NetWitness Platformのアップグレードプロセスを開始する前にそれらを無効にして、起動エラーを回避する必要があります。STIGベースのFIPSカーネル コントロールを無効にするには、次のコマンドを実行します。

```
manage-stig-controls --disable-control-groups 3 --host-all
```

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

NetWitness Platformをアップグレードしたら、STIGベースのFIPSカーネル コントロールを有効にしてください。

注 :カーネル起動オプションの変更を必要とするSTIGベースのFIPSカーネル コントロールは、NetWitnessの初期設定では有効になっていません。

タスク7(オプション) :Liveサーバーの接続を確認する

`admin/system/live services`に移動し、テスト接続を実行して、Liveサーバーに接続できるかどうかを確認します。この接続は12.x以降のソース サーバーに不可欠です。これは、Liveを構成したお客様にのみ適用されるオプションの手順です。

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、『NetWitness Platform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。 [NetWitnessの全バージョンのドキュメント]ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。

注 : Admin Serverが完了した直後に相関サーバーがアップグレードされるように、アップグレード プロセスを計画してください。詳細については、「アップグレード準備タスク」の「**タスク4 :12.1バージョンへの移行のためにESA導入環境を準備する**」を参照してください。

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で管理サーバーのホストに接続します。
  b. 次のコマンドを実行します。

```
salt \* service.stop ntpd
salt \* cmd.run 'ntpdate nw-node-zero'
salt \* service.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。

NW ServerとESAプライマリー ホストを12.1.0.0にアップグレードするまで Respond Serverサービスは有効にならない

プライマリーNW Server(Respond Serverサービスを含む) をアップグレードした後、Respond Serverサービスは、プライマリーESAホストも12.1.0.0にアップグレードされるまで、自動的には再度有効になりません。Respondのアップグレード後タスクは、Respond Serverがアップグレードされて有効状態になった後でのみ適用されます。

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-manage 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

Legacy Windows Log Collectorを使用した12.1.0.0バージョン向け追加のアップグレード後ステップ

Legacy Windows Log Collectorを使用する12.1.0.0バージョンでは、追加のアップグレード後タスクをいくつか実行する必要があります。追加のアップグレード後タスクについては、「アップグレード後のタスク」の「Legacy Windowsログ収集」を参照してください。

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、NetWitness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
- オプション4(オプション) :アップグレード リポジトリーを事前設定

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

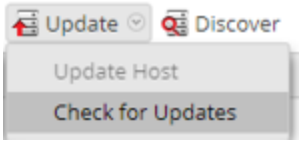
次の情報を確認します。

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[アップデートあり]が表示されることを確認します。
3. [アップデートのバージョン]列に12.1.0.0が表示されることを確認します。

手順

11.6.x.xおよび11.7.0.xから12.1.0.0にアップグレードする場合は、次の手順に従います。

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. 最新のアップデートをチェックします。

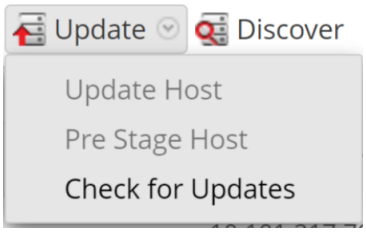


4. 選択したホストのバージョン アップデートがローカル アップデート リポジトリーにある場合は、[ステータス]列に[アップデートあり]が表示されます。
5. [更新のバージョン]列で[12.1.0.0]を選択します。次のガイドラインに従ってください。
   - アップグレードの主な機能とアップデートに関する情報を示すダイアログを表示するには、アップグレード バージョン番号の右側にある情報アイコン(ⓘ) をクリックします。
   - 目的のバージョンが見つからない場合は、[更新] > [更新の確認]を選択し、リポジトリ内の使用可能な更新をチェックします。更新が利用可能な場合、「新しい更新が利用可能です」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。

11.7.1.0および11.7.1.1から12.1.0.0にアップグレードする場合は、次の手順に従います。

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. 最新のアップデートをチェックします。



4. 選択したホストのバージョン アップデートがローカル アップデート リポジトリーにある場合は、**[ステータス]**列に **[アップデートあり]**が表示されます。
5. **[更新のバージョン]**列で **[12.1.0.0]**を選択します。次のガイドラインに従ってください。
   - アップグレードの主な機能とアップデートに関する情報を示すダイアログを表示するには、アップグレード 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. NetWitnessコミュニティー(https://community.netwitness.com/) にアクセスし、 [ダウンロード] > [NetWitness Platform] > [バージョン12.1]を選択して、アップグレード パッケージnetwitness-12.1.0.0.zipをローカル ディレクトリー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-12.1.0.0.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。
   以下に例を示します。

```
sudo cp /tmp/netwitness-12.1.0.0.zip /var/lib/netwitness/common/update-stage/
```

rootユーザー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-12.1.0.0.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。

   注 :  (管理) > [ホスト]ページをすでに開いており、[アップデートの確認]オプション([アップデート] > [アップデートの確認]) がグレー表示されている場合は、ブラウザーからページを更新してアップデートを確認してください。
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。

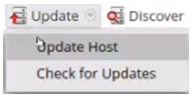
   次の条件を満足すると、「更新パッケージを初期化する準備ができました」と表示されます。

   - 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

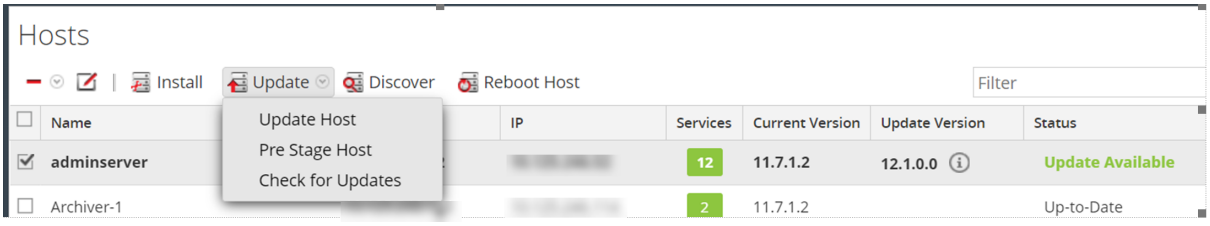
「付録A :オフライン方式(Liveサービスへの接続なし) - コマンド ライン インタフェース」の手順に従います。

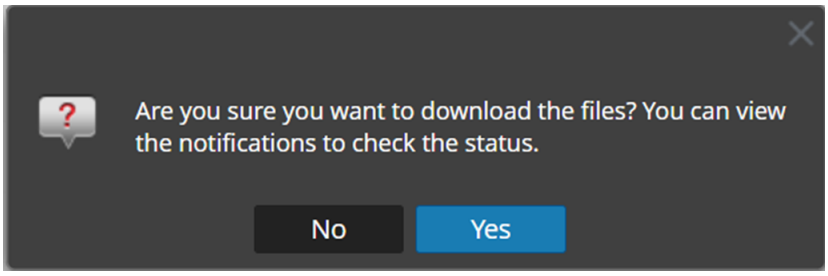
オプション4(オプション) :アップグレード リポジトリーを事前設定

必要なパッケージ(.zip) をダウンロードすることで、システムに影響を与えることなく、アップグレード リポジトリーを事前設定できます。これにより、アップグレードのダウンタイムが最小限に抑えられ、計画された時間内にアップグレードが完了することが保証されます。

手順

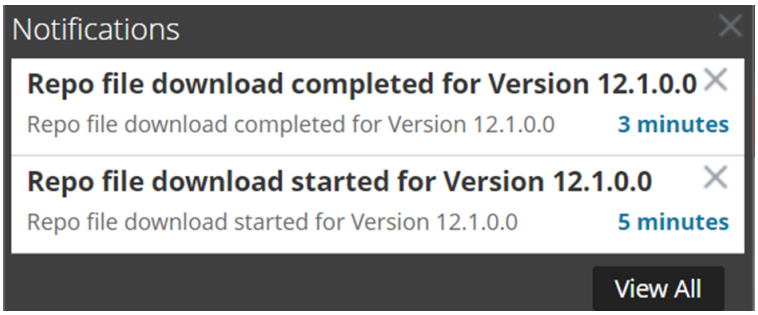
1.  (管理) > [ホスト]に移動します。
2. ツールバーで [更新] > [更新の確認]をクリックします。
適用可能なすべての更新バージョンが [バージョン]ドロップダウン リストに表示されます。
3. [更新] > [ホストの事前設定]をクリックして、更新バージョンの列でバージョンを選択します。
ファイルのダウンロードの確認メッセージが表示されます。





4. [**はい**]をクリックしてアップグレード パッケージをリポジトリーにダウンロードします。
5. 下図に示すように、通知トレイでダウンロードのステータスを確認します。

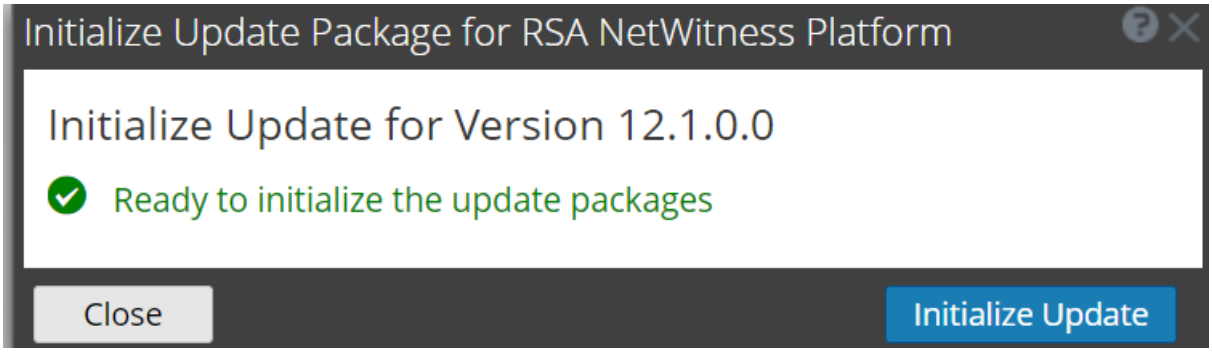
   [**ホストの事前設定**]と [**ホストのアップグレード**]は、事前設定が完了するまで無効になります。



注 :実際の更新ではないため、UIの現在のバージョンと更新バージョンは事前設定時には同じになります。これは、リポジトリー ファイルのみがダウンロードされ、実際のアップグレードは行われないためです。バージョンは、アップグレード後にのみ変更されます。

6. ダウンロードが成功した場合は、再び**更新を確認**して初期化を開始します。
7. [**更新の初期化**]をクリックします。

   ファイルのサイズが大きく、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。



重要 :リポジトリーの事前設定の準備ステップ1～4はいつでも実行できます。ただし、ステップ5～8のアップグレード プロセスが開始されたら、.ZIPファイルの破損を防ぐため、ホストを再起動したり、jettyサーバーを再起動したりしないでください。

8. 通知トレイで初期化のステータスを確認します。
9. 初期化が正常に完了したら、[**更新**] > [**ホストの更新**]をクリックします。

ホストの更新が完了すると、ホストを再起動するように求められます。

10. ホストをセットアップして再起動します。

アップグレード後のタスク

12.1.0.0にアップグレードした後、NetWitnessは、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

(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12.1.0.0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`を更新した後に、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>
```

Jetty構成

Jetty構成とその関連情報については、『システム メンテナンス ガイド』のトピック「**カスタム ホスト エントリーの管理**」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

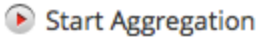
1. NetWitness Platformメニューで、  (管理) > [**サービス**]に移動します。
   [サービス]ビューが表示されます。

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。

Event Stream Analysis(ESA)

12.1バージョンにアップグレードした後、すべてのESA導入環境が[構成] > [ポリシー]ページに移行されます。各導入環境はポリシーとグループに変換され、Correlationサーバーを12.1バージョンにアップグレードした後にのみ管理できるようになります。すべてのESA導入環境が正常な状態にあるかどうかを確認します。詳細については、『Liveサービス管理ガイド』の「導入環境の表示」トピックを参照してください。

注 :アナリストには、[構成] > [ESAルール]ページと[構成] > [ポリシー]ページでESAルールを表示するための適切な権限が必要です。詳細については、『システム セキュリティとユーザー管理ガイド』の「ロールの権限」トピックで「**ソース サーバー**」セクションを参照してください。

次の表に、アップグレード前とアップグレード後の導入環境の状態を表します。

SINo	アップグレード前の導入環境の状態	アップグレード後の導入環境の状態		
		ポリシーの作成	グループの作成	ポリシーが公開されます
1	正常な導入環境	はい	はい	はい
2	エラーのある導入環境	はい	はい	はい
3	ルールのみを含んだ導入環境	はい	いいえ	いいえ
4	ルールのない導入環境	いいえ	いいえ	いいえ

(オプション) [**ポリシーのマージ**]ボタンを使用して、ESAコンテンツを含むポリシーをESAコンテンツを含まないポリシーとマージできます。詳細については、『Liveサービス管理ガイド』の「ESAコンテンツを含んだポリシーのマージ」を参照してください。

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12.1.0.0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)の標準提供ユーザー 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 ユーザー 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 ユーザー ロールを割り当てられたユーザーには、 [イベントの絞り込み]パネルが表示されません。これは、12.1.0.0の新しいパネルで、ここでユーザーはメタデータをドリルダウンできます。

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

ユーザ ロールの権限を有効にするには、次の手順を実行します。

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

Respond

これらのタスクを完了する前に、プライマリーESAサーバーを12.1.0.0にアップグレードする必要があります。

注：プライマリーNW Server(Respond Serverサービスを含む)をアップグレードした後、Respond Serverサービスは、プライマリーESAホストも12.1.0.0にアップグレードされるまで、自動的には再度有効になりません。Respondのアップグレード後タスクは、Respond Serverがアップグレードされて有効状態になった後でのみ適用されます。

(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。

12.1.0.0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>`

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。

Legacy Windows Log Collector

Legacy Windows Log CollectorのUUIDを更新する

12.1.0.0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Legacy 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>
```

更新されたSA証明書でLegacy Windows Log Collectorの証明書を更新する

アップグレード後のステップ：

1. 次のコマンドをSAで実行します。
   a. `wlc-cli-client --host-display-name` **`hostDisplayName`** `--service-display-name` **`serviceDisplayName`** `--host` **`WLChostIPAddress`** `--port 50101 --use-ssl false`

      次の情報を入力します。

      i. **Legacy Windows Log CollectorのRESTユーザー名**と**Legacy Windows Log CollectorのRESTパスワード**：Legacy Windows Log Collectorの管理者認証情報を入力します。

      ii. **Security Serverのユーザー名**と**Security Serverのパスワード**：NetWitnessの管理者認証情報を入力します。
2. システムを再起動します。

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。11.6.xから11.6.x.xにアップグレードする場合は、11.7.xにアップグレードする前に、11.6.x.xのアップグレード ガイドに記載されたUEBAの手順を実行しておく必要があります。

注 :11.6.x.xから12.1.0.0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。11.7.xより前のバージョンから12.1.0.0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. 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。

```
source /etc/sysconfig/airflow

source $AIRFLOW_VENV/bin/activate

OWB_ALLOW_NON_FIPS=on 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
```

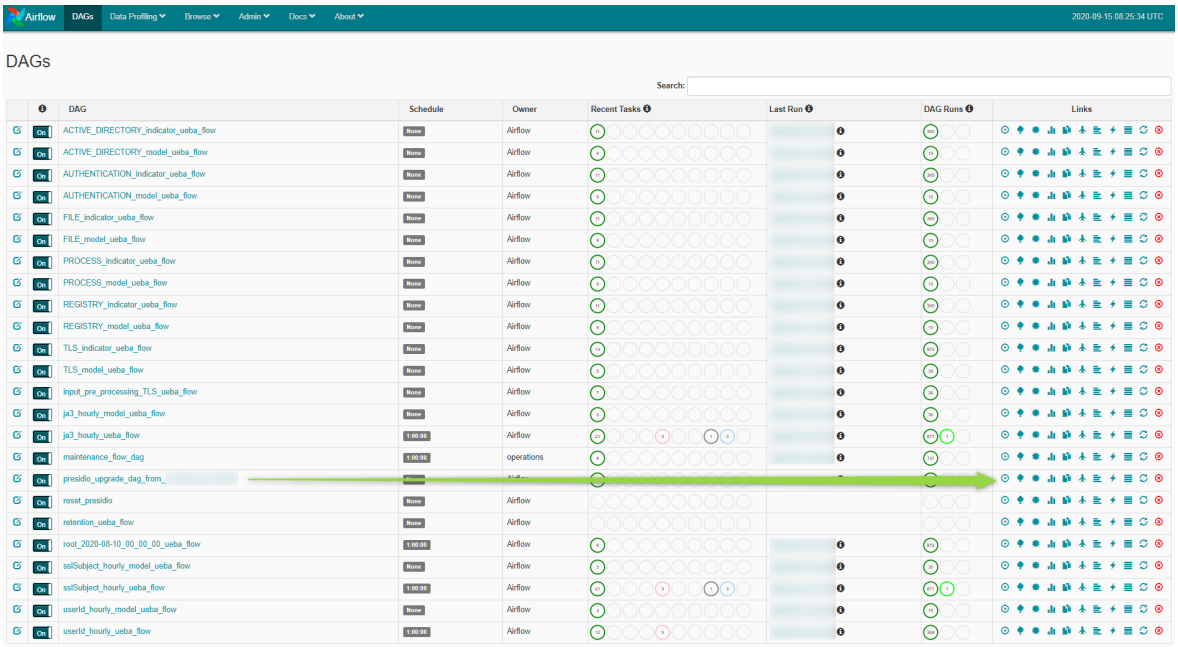
2. (オプション) 必要に応じて、UEBA処理スキーマを更新します。

   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。

3. 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。

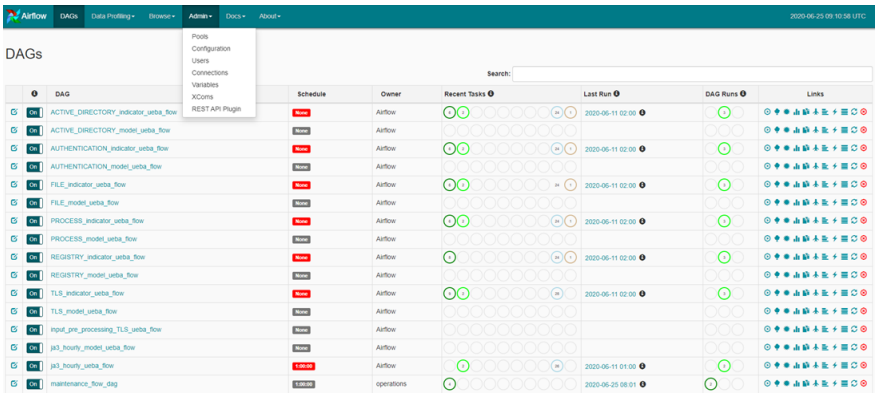
- `presidio_upgrade_dag_from_<previous_version> to_12.1.0.0`で **再生**]をクリックします。



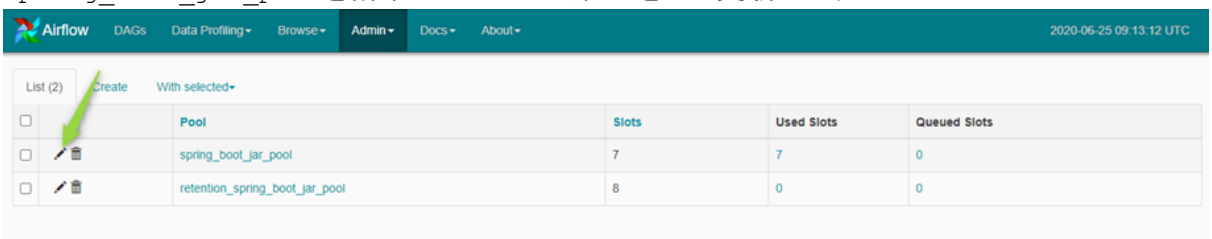
注 :アップグレード中は、DAGアップグレード行の横に緑色の丸が表示されます。アップグレードプロセスが正常に完了した場合は、明るい緑色の円が緑色に変わります。アップグレード プロセスが失敗した場合は、明るい緑色の円が赤に変わります。

4. 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。



5. `spring_boot_jar_pool`を編集し、スロットの数量を22に更新します。



6. UEBAホストを12.1.0.0にアップグレードした後、Elasticsearch presidioデータをインポートします。Elasticsearch presidioデータをインポートする前に、次の前提条件が満たされていることを確認してください。

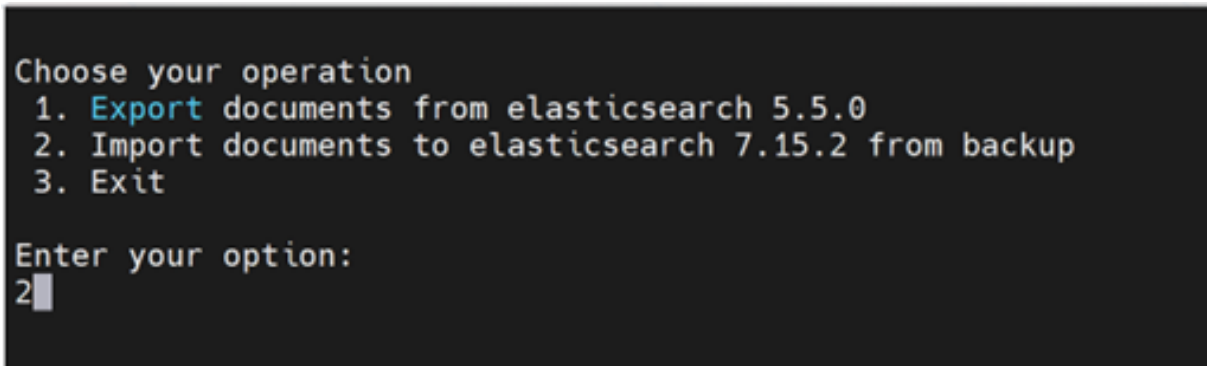
- Elasticsearchのバージョンが5.5.0から7.15.2にアップグレードされている必要があります。
- UEBAホストが12.1.0.0にアップグレードされている必要があります
- UEBA rpmバージョンが12.1.0.0でなければなりません。
- 12.0.0.0以前のバージョンのElasticsearchデータは、 `/root/`ディレクトリーにあるElasticsearchデータバックアップ フォルダーにエクスポートされて保存されている必要があります。

Elasticsearchデータをインポートするには：

a. `cd ueba_es_migration_tool`に進みます。次のコマンドを実行します。

```
sh elk-migration-script.sh
```

Elasticsearch移行ツール ガイドが表示されます。



b. [**Import documents to elasticsearch 7.15.2 from backup**]を選択します。

c. 次のステップで、 [**Fresh Import**]を選択してバックアップ データをインポートします。

```
Import documents to elasticsearch 7.15.2 from backup
 1. Fresh Import
 2. Resume Import
 3. Main menu
 4. Exit

Enter your option:
1

Source dir path:
/root/elasticsearch_export_backup

Total document found in given location[/root/elasticsearh_export_backup/log/es-migration-export.log]: 184081
Please wait processing your import request...

+----------------------------------------+----------+-------+------------+
| Index                                  | Imported | Total | Took       |
+----------------------------------------+----------+-------+------------+
| presidio-output-alert                  | 1246     | 1246  | 6372 ms.   |
| presidio-output-entity-severities-range | 3        | 3     | 23 ms.     |
| presidio-output-entity                 | 673      | 673   | 2230 ms.   |
| presidio-output-event                  | 40012    | 40012 | 124286 ms. |
| presidio-output-feature                | 2078     | 2078  | 6353 ms.   |
| presidio-output-indicator              | 4130     | 4130  | 36744 ms.  |
| presidio-monitoring-2022.08.11         | 69401    | 69401 | 185485 ms. |
| presidio-monitoring-2022.08.10         | 66538    | 66538 | 171230 ms. |
+----------------------------------------+----------+-------+------------+

Total: 184081, Imported: 184081, Dropped: 0, Started: 2022-08-16 07:44:48, Ends: 2022-08-16 07:53:41, Took: 533562 ms.
[root@ueba ueba_es_migration_tool]#
```

d. インポート操作が完了したら、Presidio UIサービスを再起動します。次のコマンドを実行します。

```
systemctl restart presidio-ui
```

e. NetWitness Platform XDRの [**ユーザー**]タブに移動して、すべてのElasticsearchデータがインポートされているかどうかを確認します。

注：
- 例外に関するログを表示するには、`<backup_directory_path>/log/log/es-migration-import.log`に移動します。
- 技術的な問題が原因でインポート操作が失敗した場合は、問題が解決したら [**インポートの再開**]を選択してインポート操作を再開します。

Endpointアップグレード タスク

12.1.0.0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12.1.0.0にアップグレードする必要があります。詳細については、『*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。 [NetWitnessの全バージョンのドキュメント]ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。
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 12.1 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

12.1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、『NetWitness Platform 12.1リリース ノート』を参照してください。［NetWitnessの全バージョンのドキュメント］ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。

- ポリシーベースのコンテンツー元管理
- Endpoint調査
- Respond

ポリシーベースのコンテンツー元管理

- コンテンツの作成とコンテンツ ライブラリーへのアップロードを簡単に行えます。
- 「トグル」機能を使用して、従来のコンテンツ管理UIとグループおよびポリシーを介した新しいコンテンツー元管理の間でサービスを切り替えます。
- ［**ポリシー リスト**］および［**ポリシーの詳細**］ページで利用可能な［**強制公開**］ボタンを使用して、ポリシーのすべてのコンテンツを強制的に公開します。
- ［**コンテンツ ライブラリー**］、［**ポリシー リスト**］ページ、［**ポリシーの詳細**］ページ、および［**グループ リスト**］ページでUIの「フィルター処理」機能を使用して、関心のあるコンテンツ、ポリシー、グループを簡単に見つけることができます。
- アプリケーションおよびネットワーク ルールの条件を作成する際に、メタ キーと演算子の候補値が表示されます。
- インターネットに接続していなくても、コンテンツ ライブラリーでポリシーを作成、変更、公開し、カスタム コンテンツを管理できます。
- ポリシーを使用してESAコンテンツを管理し、複数の導入環境をシームレスに処理できます。
- サブスクリプションのワンクリック管理とESAコンテンツの自動更新。
- 独自のカスタム コンテンツとともにESA Liveコンテンツをシームレスに表示します。
- ESA Correlationサーバーをグループの一部として追加して管理できます。
- ESA Correlationサーバーのすべてのデータ ソースを［**設定**］>［**Event Stream Analysis**］>［**データ ソース**］ページでシームレスに管理できます。

Endpoint調査

- 1つまたは複数のEndpointエージェントを選択して、Endpointエージェント レベルでYARAスキャンを開始します。
- ［**Respond**］>［**アラート**］>［**Endpointアラート**］>［**アラートの詳細**］ページの［**ファイル アクション**］タブを使用して、選択したファイルのローカル コピーの保存、サーバーへのダウンロード、ブロックを行えます。

Respond

- [**エクスポート**]ドロップダウンを使 用してインシデント データをエクスポートします。

付録A. オフライン方式(Liveサービスへの接続不可):CLI

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

NetWitnessコミュニティ(https://community.netwitness.com/) > [Products] > [NetWitness Platform] > [Downloads] > [Version 12.1] > [Full Product Downloads]でnetwitness-12.1.0.0.zipファイルをローカル ディレクトリーにダウンロードしていることを確認してください。

手順

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

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

1. 12.1.0.0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、次のディレクトリーを作成します。
     `/tmp/upgrade/12.1.0.0`
     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-12.1.0.0.zip -d /tmp/upgrade/12.1.0.0`

   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 12.1.0.0 --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-key <ID / display name / (hostname/ IP address)> --version 12.1.0.0`
4. NW Serverホストのアップグレードが成功したら、NetWitness Platformユーザ インタフェースの [ホスト]ビューからホストを再起動します。
5. 他のコンポーネント ホストについて、ステップ3および4を繰り返します。

注 :NW Serverホストでupgrade-cli-client --listコマンドを実行すると、すべてのホストのバージョンをチェックすることができます。upgrade-cli-clientのヘルプを表示するには、upgrade-cli-client --helpコマンドを使用します。

注 :アップグレード処理中に、次のエラーが表示される場合があります。
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
この場合でも、サービス パックは正しくインストールされます。何のアクションを取る必要もありません。新しいバージョンにホストを更新する際に他のエラーが発生した場合は、カスタマー サポート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ーの準備

1. 12.1.0.0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。
2. NW Serverにrootとしてログインし、次のディレクトリーを作成します。/tmp/upgrade/12.1.0.0
   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-12.1.0.0.zip -d /tmp/upgrade/12.1.0.0

   注：作成したステージング ディレクトリに.zipファイルをコピーし、その場所で解凍した場合は、解凍後、元の.zipファイルを忘れずに削除してください。
3. 次のコマンドを使用して、アップグレードの初期化を実行します。
   ```
   upgrade-cli-client --init --version 12.1.0.0 --stage-dir /tmp/upgrade
   ```
4. 次のコマンドを使用して、NW Serverホストをアップグレードします。
   ```
   upgrade-cli-client --upgrade --host-key <ID / display name / (hostname/ IP address)> --version 12.1.0.0
   ```
5. NW Serverホストのアップグレードが成功したら、NetWitness Platformユーザ インタフェースの［ホスト］ビューからホストを再起動します。
6. 他のコンポーネント ホストについて、ステップ3および4を繰り返します。

注：NW Serverホストでupgrade-cli-client --listコマンドを実行すると、すべてのホストのバージョンをチェックすることができます。upgrade-cli-clientのヘルプを表示するには、upgrade-cli-client --helpコマンドを使用します。

注：アップグレード処理中に次のエラーが表示される場合があります。
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
この場合でも、サービス パックは正しくインストールされます。何のアクションを取る必要もありません。新しいバージョンにホストを更新する際に他のエラーが発生した場合は、カスタマー サポートにお問い合わせください。

付録B :外部リポジトリのセットアップ

外部リポジトリ(Repo) をセットアップするには、次の手順を実行します。

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

1. (オプション) 外部リポジトリがあり、それを上書きする場合に、この手順を実行します。
   - ケース1 :外部リポジトリからホストをセットアップしたが、NetWitness Serverホスト上のローカルリポジトリを使用してアップグレードしたい場合。
     a. `/etc/netwitness/platform/repobase`ファイルを作成します。
        `vi /etc/netwitness/platform/repobase`
     b. `repobase`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。
        `https://nw-node-zero/nwrpmrepo`
     c. `upgrade-cli-client`ツールを使用してアップグレードを実行するための手順を完了します。
   - ケース2 :NetWitness Serverホスト上のローカルリポジトリからホストをセットアップしたが、外部リポジトリを使用してアップグレードしたい場合。
     a. `/etc/netwitness/platform/repobase`ファイルを作成します。
        `vi /etc/netwitness/platform/repobase`
     b. `repobase`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。
        `https://<webserver-ip>/<alias-for-repo>`
     c. `upgrade-cli-client`ツールを使用してアップグレードを実行するための手順を完了します。
        手順は、『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。 [NetWitnessの全バージョンのドキュメント]ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。
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-12.1.0.0.zip`) をホストするディレクトリを作成します(例 :Webサーバーの`web-root`の下の`ziprepo`) 。たとえば、/var/netwitnessがweb-root場合、次のコマンドを実行します。
      `mkdir -p /var/netwitness/<your-zip-file-repo>`
   c. 12.1.0.0 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>/12.1.0.0`
   d. `OS` および`RSA` ディレクトリを`/var/netwitness/<your-zip-file-repo>/12.1.0.0`
      `mkdir -p /var/netwitness/<your-zip-file-repo>/12.1.0.0/OS`の下に作成します。
      `mkdir -p /var/netwitness/<your-zip-file-repo>/12.1.0.0/RSA`

e. netwitness-12.1.0.0.zip ファイルを/var/netwitness/<your-zip-file-repo>/12.1.0.0 ディレクトリに解凍します。
unzip netwitness-12.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/12.1.0.0

を解凍すると、2つのZipファイルnetwitness-12.1.0.0.zip(OS-12.1.0.0.zipとRSA-12.1.0.0.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-12.1.0.0.zipを /var/netwitness/<your-zip-file-repo>/12.1.0.0/OSディレクトリに解凍します。
unzip /var/netwitness/<your-zip-file-repo>/12.1.0.0/OS-12.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/12.1.0.0/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-12.1.0.0.zipを/var/netwitness/<your-zip-file-repo>/12.1.0.0/RSAディレクトリに解凍します。
unzip /var/netwitness/<your-zip-file-repo>/12.1.0.0/RSA-12.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/12.1.0.0/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>/12.1.0.0/OS/other

ii. unzip nw-azure-12.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/12.1.0.0/OS/other

iii. cd /var/netwitness/<your-zip-file-repo>/12.1.0.0/OS

iv. createrepo

i. NW 12.1.0.0セットアップ プログラム(nwsetup-tui) が [**Enter the base URL of the external update repositories**]プロンプトを表示したら、 http://<web server IP address>/<your-zip-file-repo> と入力します。

付録C :インストールと更新のトラブルシューティング

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

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

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

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

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

問題	アップグレード後にアプライアンスを起動できない
回避策	1. GRUBブート行を手動で `FIPS=0`に変更して、起動できるようにします。 2. ここから、次のコマンドを使用してFIPSを無効にします。 `manage-stig-controls --disable-control-groups 3 --host-all` 3. 行`FIPS=1`が`/boot/grub2/grub.cfg`から削除されたことを確認します。

- 削除されていない場合は、次のコマンドを実行します。

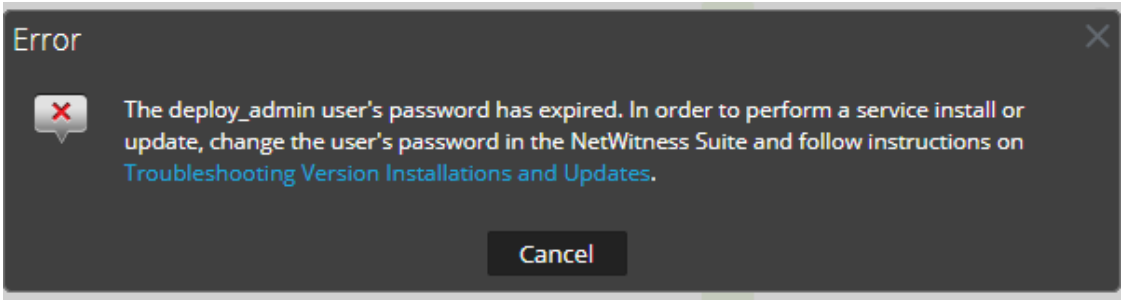
  ```
  grub2-mkconfig -o /boot/grub2/grub.cfg
  ```

4. 再起動します。
5. 次のコマンドを実行してFIPSを有効にします。

   ```
   manage-stig-controls --enable-control-groups 3 --host-all
   ```

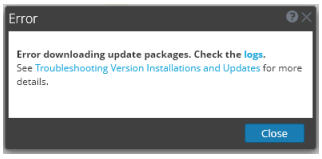
6. 再起動します。

deploy_adminのユーザー パスワード有効期限切れエラー

エラーメッセージ	
原因	deploy_adminのユーザ パスワードの有効期限が切れています。

解決策	deploy_adminのパスワードをリセットします。
	1. NW Serverホストのみで次のコマンドを実行します。
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	2. `nw-manage --update-deploy-admin-pw`コマンドの出力を確認して、`deploy_admin`パスワードがすべてのホストで正常に更新されたことを確認します。NWホストがダウンしているか、`nw-manage --update-deploy-admin-pw`コマンドの出力に表示されている何らかの理由で失敗した場合は、通信障害が解決された後で`nw-manage --sync-deploy-admin-pw --host-key <host-identifier>`を実行して、失敗したホストとNW Serverの間でパスワードを同期します。
	3. インストールまたはオーケストレーションに失敗したホスト上で、`nwsetup-tui`コマンドを実行し、［**Deployment Password**］のプロンプトが表示されたら、**deploy_admin**の新しいパスワードを入力します。

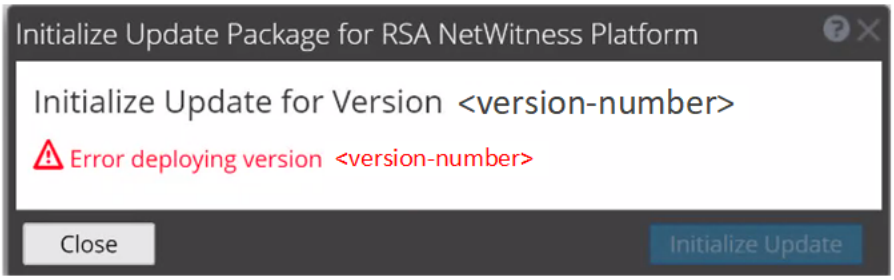
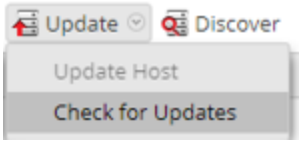
ダウンロード エラー

エラーメッセージ	
問題	更新バージョンを選択し、[**更新**] > [**ホストの更新**]をクリックすると、ダウンロードが開始されますが異常終了します。
原因	バージョンのダウンロード ファイルのサイズが大きく、ダウンロードに時間がかかる場合があります。ダウンロード中に通信の問題が発生すると、ダウンロードは失敗します。
解決策	1. 更新を再試行します。 2. 同じエラーで再度失敗した場合は、『NetWitness Platformアップグレード ガイド』の「[ホスト]ビューからのオフライン方式」または「コマンド ライン インターフェイスを使用したオフライン方式」の説明に従って、オフライン方式で更新してみてください。[NetWitnessの全バージョンのドキュメント]ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。 3. それでもアップデートできない場合は、カスタマー サポートにお問い合わせください。

エラーメッセージ	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、「ダウンロード エラー」メッセージが表示されます。

解決策	1. コマンド ライン インタフェース(CLI) で次の手順を実行します。
	a. SSHでNW Serverに接続します。
	b. 次のコマンドを実行します。
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version <version number>`
	`For example:`
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.6.0.0`
	2. NW Serverが正常にアップデートされたら、NW Serverのユーザ インタフェースにログインし、  (**管理**)> [**ホスト**]に移動します。ホストの再起動を求めるプロンプトが表示されます。
	3. ツールバーの[**ホストの再起動**]をクリックします。
	その他すべてのホストは、ユーザ インタフェースから直接アップグレードできます。
	1. [更新あり]ダイアログの[**更新を開始**]をクリックします。
	ホストのアップグレードが完了すると、ホストの再起動を求めるメッセージが表示されます。
	2. ツールバーの[**ホストの再起動**]をクリックします。

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

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

アップグレード失敗エラー

エラーメッセージ	バージョン11.6以降に更新しようとすると、次のようなエラーがログに出力されました。 `FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobufs-rt`
原因	ホスト上にインストールされた一部のコンポーネントがカスタム ビルド/rpmです(Hotfixをインストールした場合など) 。
解決策	この問題を解決するには、次の手順に従います。 1. SSHでNetWitness Serverに接続します。

2. 次のコマンドを実行して、コンポーネント ディスクリプタ ファイルのディレクトリに移動します。
```
cd /etc/netwitness/component-descriptor/
```
3. 次のコマンドを実行して、コンポーネント ディスクリプタ ファイルを開きます。
```
vi nw-component-descriptor. json
```
4. カスタム ビルド/rpmをインストールしたコンポーネントの「packages」セクションを検索します。次の例は、カスタム ビルド/rpmをインストールした「concentrator」ホストのパッケージの詳細を示しています。
```
"concentrator": {
"cookbook_name": "rsa-concentrator",
 "service_names": ["rsa-nw-concentrator"],
 "family": "launch",
 "default_port": xxxx, "description": "Concentrator",
 "packages":[{ "name": "rsa-nw-concentrator",
 "version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos"
 },
```
5. packagesセクションのバージョン情報をすべて(「,」文字を含む) 削除します。次の例は、バージョン情報を削除した後のpackagesセクションです。
```
"packages": [{
"name": "rsa-nw-concentrator"
 },
```

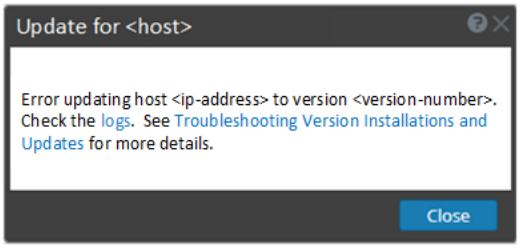
注 : Admin Serverのコンポーネント ディスクリプタで、カスタム ビルド/rpmをインストールしたすべてのホストのバージョン情報を削除する必要があります。

6. アップグレード プロセスを再度実行します。

外部リポジトリ更新エラー

エラーメッセージ	以下から新しいバージョンに更新しようとすると、次のようなエラーが発生しました。 `.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""`
原因	指定したパスに問題があります。
解決策	次の情報を確認します。 • URLがNW Serverホスト上に存在する。 • 正しいパスを使用し、スペースを削除している。

ホスト更新失敗エラー

エラーメッセージ	
問題	アップデート バージョンを選択し、 [**アップデート**] > [**ホストのアップデート**] クリックすると、ダウンロード プロセスは成功しますが、アップデート プロセスは失敗します。

解決策	1. ホストへのバージョン更新の適用を再試行します。
	通常は、これで問題が解決されます。
	2. それでも新しいバージョンにアップデートできない場合は、次の手順を実行してください。
	実行時にNW Server上の次のログを監視します(たとえば、コマンド ラインから`tail -f`コマンドを実行します) 。
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	エラーはこれらのログの少なくとも1つに表示されます。
	3. それでもアップデートを適用できない場合は、ステップ2のログを収集して、カスタマー サポートにお問い合わせください。

更新パッケージ不足エラー

エラーメッセージ	**バージョンxx.x.x.xのアップデートの初期化** 次のアップデート パッケージが見つかりません NetWitness Linkからパッケージをダウンロードしてください
問題	「次の更新 パッケージが見つかりません」は、 [**ホスト**] ビューからオフラインでホストを更新する時に、ステージング フォルダーに足りないパッケージがあると、 [**NetWitness Platformの更新パッケージの初期化**] ダイアログに表示されます。
解決策	1. [**NetWitness Platformの更新パッケージの初期化**] ダイアログで [NetWitnessコミュニティーからパッケージをダウンロード] をクリックします。 選択したバージョンの更新ファイルが含まれNetWitnessコミュニティー ページが表示されます。 2. ステージング フォルダに足りないパッケージを選択します。

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

OpenSSL 1.1.x

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

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

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

NW Server以外へのパッチ適用エラー

エラーメッセージ	`/var/log/netwitness/orchestration-server/orchestration-server.log`で、次のようなエラーが発生しました。 **`API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported`**
問題	NW Serverホストのバージョンを更新した後で、NW Server以外のすべてのホストを同じバージョンに更新する必要があります。たとえば、NW Serverを11.4.0.0から11.6.0.0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。 • NW Server以外のホストを11.6.0.0以降に更新します。 • NW Server以外のホストを更新しません(現在のバージョンを維持) 。

コマンド ラインからの更新後のホスト再起動のエラー

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

アップグレード後のReporting Engine再起動

問題	11.4などの11.xのバージョンから11.6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。 1. どのデータベース ファイルが破損しているかを確認します。 `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log`ファイルを開き、次のブロックを確認します。 • ライブ チャートのdbファイルが破損している場合は、次のログが表示されます。 Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception: org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) at org.h2.message.DbException.get(DbException.java:168) org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database! • アラート ステータスのdbファイルが破損している場合は、次のログが表示されます。

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

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

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

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

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

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

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

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

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

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

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

詳細については、ナレッジベース記事「Reporting Engine restarts After upgrade to 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。 - workspace.xmlが更新されていない。 - livechart h2データベースで時間が正しく変換されていない。 - JCR(Jackrabbitリポジトリ) がプライマリ キー違反で破損している。
解決策	この問題を解決するには、Reporting Engineサービスがインストールされ ているAdmin Server上でReporting Engine移行リカバリ ツール(`rsa-nw-re-migration-`

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

Log Collectorサービス(nwlogcollector)

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

エラーメッセージ	<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.
原因	更新後、Log CollectorのLockboxを開くことができませんでした。
解決策	NetWitnessにログインし、LockboxのStable System Valueをリセットすることにより、システム フィンガープリントをリセットします。詳細については、『*ログ収集の構成ガイド*』の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」セクションを参照してください。

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

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

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

解決策	この問題を解決するには、次の手順を実行します。
	1. SSHを使用してDecoderホストに接続します。
	2. 次のコマンドを実行します。
	`yum reinstall pfring*`
	`systemctl restart nwdecoder`

NW Server

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

問題	アップグレード後、監査ログが、グローバル監査に設定された宛先に転送されていないことが分かりました。 または 次のメッセージが`sa.log`に記録されました。 `Syslog Configuration migration failed. Restart jetty service to fix this issue`
原因	NW Serverのグローバル監査設定は、11.4.x.xまたは11.5.x.xから11.6.0.0以降への移行に失敗しました。
解決策	1. SSHでNW Serverに接続します。 2. 次のコマンドを実行します。 `orchestration-cli-client --update-admin-node`

Orchestration

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

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

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

問題	12.0以前のバージョンから12.1にアップグレードされた管理サーバー(ノード0)に新しい12.1コアノードXをインストールしてオーケストレーションすると、Concentrator、Log Decoder、Log Collector、Archiver、Decoder、Appliance、Workbench、Warehouse Connector、Brokerなどのコアサービスが［**管理**］>［**ホスト**］ビューの［**サービス**］列に非アクティブとして表示されます。その結果、UIでコアサービスにアクセスできなくなります。 この問題は、新しくインストールされた(12.0以前のバージョンから12.1にアップグレードされなかった)12.1管理サーバーに対して新しい12.1コアノードXをオーケストレーションしている場合には該当しません。
原因	12.1コアノードXは、アップグレードされた12.1管理サーバーホストに直接オーケストレーションされている場合、トラストピアの共通のノード0ノード証明書ではなくSAサーバー専用の証明書を使用します。

解決策	12.1コアノードXホストをブートストラップしてオーケストレーションする前に、次のコマンドを実行します。
	1.
	`mkdir -p /etc/netwitness/platform`
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	この回避策は、上記の回避策(回避策1)をスキップした場合にのみ実行してください。
	12.1コアノードXホストをブートストラップしてオーケストレーションした後で、次のコマンドを実行します。
	2.
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	`nw-manage --refresh-host --host-key <core-node-x-salt-minion-uuid>`
	`systemctl restart <core-service-name>`

	注： - ファイル/etc/salt/minionを参照して<core-node-x-salt-minion-uuid>を見つけてください。 - **nwarchiver**(Archiver) 、**nwdecoder**(Decoder) 、**nwlogcollector**(Log Collector) 、**nwappliance**(Appliance) 、**nwconcentrator**(Concentrator) 、**nwlogdecoder**(Log Decoder) 、**nwbroker**(Broker) 、**nwworkbench**(Workbench) 、 **nwwarehouseconnector**(Warehouse Connector) などのコア サービス名を<core-service-name>で入力する必要があります。

Reporting Engineサービス

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

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

Event Stream Analysis

問題	バージョン11.6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	Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)
解決策	この問題を解決するには、次の手順を実行します。 NetWitness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。

Legacy Windows Log Collector

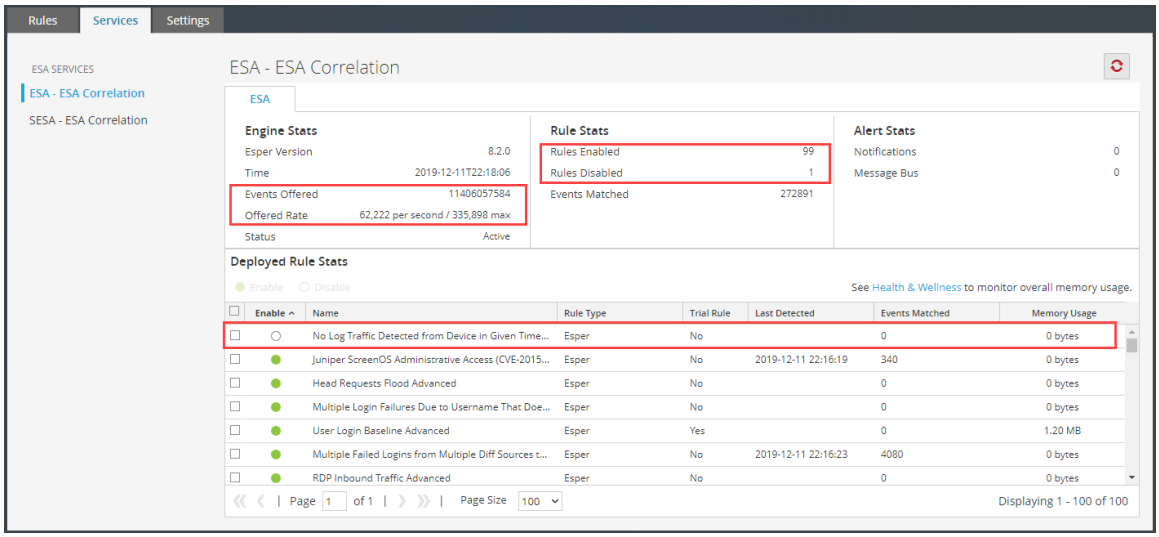
問題	• SAを12.1.0.0バージョンにアップグレードし、Legacy Windows Log Collectorを11.6.xまたは11.7.xバージョンにアップグレードした後で、Legacy Windows Log Collectorが非アクティブとして表示される。 • スタックが12.1.0.0にアップグレードされると、Legacy Windows Log Collectorが非アクティブとして表示される。
原因	SAノードでの証明書の更新。
解決策	「更新後のタスク」の「Legacy Windows Log Collector」を参照してください。

ESAトラブルシューティング情報

ESAルールがアラートを作成しない

アラートが表示されない場合は、ESAルール導入環境のステータスを確認します。

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。ルールがまだ無効な場合は、`/var/log/netwitness/correlation-server/correlation-server.log`にあるESA Correlationサービスのログ ファイルを確認します。

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

エンドポイント、UEBA、Liveコンテンツのルールが機能しない

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

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

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

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

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

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

メタ キーを更新するには、『ESA構成ガイド』の「最新のエンドポイント、UEBA、RSA Liveコンテンツ ルールのために、Multi-ValuedパラメーターとSingle-Valuedパラメーターのメタ 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。 [NetWitnessの全バージョンのドキュメント]ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。

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、『NetWitness Platform ESA相関ルール アラート ユーザー 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。 [NetWitnessの全バージョンのドキュメント]ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。

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サーバーのエラー ログに警告メッセージが表示される場合は、 `default-multi-valued`パラメーターと`multi-valued parameter`メタ キーの値に差異があるため、新しいエンドポイント、UEBA、Liveコンテンツ ルールが機能しません。この問題を修正するには、『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パラメーターとSingle-Valuedパラメーターのメタ キーを更新」の手順を実行します。

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
```