



アップグレード ガイド

RSA NetWitness® Platform 11.4



Copyright © 1994-2020 Dell Inc.、その関連会社。All Rights Reserved.

連絡先情報

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

商標

RSAの商標のリストについては、<https://www.rsa.com/ja-jp/company/rsa-trademarks>を参照してください。

使用許諾契約

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

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

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

サードパーティライセンス

本製品はRSA 以外のサードパーティ製ソフトウェアを実装している場合があります。本製品を使用することにより、本製品のユーザは、本製品に含まれているサードパーティ製ソフトウェアに適用される使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

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

配布

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

10月 2020

目次

アップグレードの概要	6
アップグレード パス	6
混在モード	7
ESAルールを導入環境に関するアップグレードの考慮事項	7
[イベント]ビューの列グループに対する変更	7
製品ドキュメントに関するフィードバック	7
カスタム サポートへのお問い合わせ	7
Legacy Windows Collectorの更新またはインストール	9
アップグレード準備タスク	10
ESA(Event Stream Analysis)	10
タスク1: ESA Correlationサービスが指定されていないESAルール導入環境を削除する	10
アップグレード タスク	11
オンライン方式 (RSA Liveに接続)	11
タスク1: ローカル リポジトリに更新を配置するか、外部リポジトリをセットアップする	11
タスク2: [ホスト]ビューから各ホストに更新を適用する	12
[ホスト]ビューからのオフライン方式	14
タスク1: ステージングフォルダ(/var/lib/netwitness/common/update-stage/)にバージョン更新を配置	14
タスク2: ステージングフォルダから各ホストに更新を適用	14
コマンドライン インタフェースを使用したオフライン方式	16
アップグレード後のタスク	18
11.3.x.xからアップグレードする場合のアップグレード後のタスク	19
全般	19
タスク1: サービスの再起動、データ収集、データ集計の確認	19
Event Stream Analysis	20
タスク2: ESAルール導入環境のステータスの確認	20
タスク3: (オプション) 最新のエンドポイント、UEBA、RSA Liveコンテンツ ルールのために、Multi-ValuedパラメータとSingle-Valuedパラメータのメタ キーを更新	21
タスク4: (オプション) カスタムESAルールビルダ ルールおよびESA詳細ルールの調整	23
ESATラブルシューティング情報	23
Investigate	23
タスク5: (オプション - カスタム ロールの場合のみ) カスタム ユーザ ロールのinvestigate-server権限の調整	23
Respond	24
タスク6: (オプション) Respondサービスの統合ルールスキーマのカスタム キーをリストアする	24
タスク7: (オプション) カスタマイズされたRespondサービスの正規化スクリプトをリストアする	25
タスク8: (オプション) 対応の通知設定権限を追加する	26

11.2.x.xからアップグレードする場合のアップグレード後のタスク	27
全般	27
タスク1: サービスの再起動、データ収集、データ集計の確認	27
タスク2: コンテキスト メニュー アクションのユーザ権限を設定する	28
タスク3: 「Manage Jobs」権限をこの権限がないロールに追加する	29
タスク4: (オプション) ホストの証明書を再発行する	31
タスク5: アナリスト ロールのinvestigate-server権限を変更する	32
タスク6: (オプション) PAM Radius認証を再構成する	33
タスク7: (オプション) NetWitness PlatformからWebアクセスできない場合は、レスポンスの.binファイルを再アップロードする(ライセンス サーバ)	34
タスク8: パスワードの最小長を8文字から9文字に変更する	34
Event Stream Analysis	34
タスク9: ESA Correlationサービスの文字列配列型メタ キーの表示と次のステップ	35
タスク10: (オプション) メタ キーが文字列から配列に変更されたRSA Live ESAルールを更新する	36
タスク11: ESAルール導入環境を検証する	37
タスク12: (オプション) 最新のエンドポイント、UEBA、RSA Liveコンテンツ ルールのために、Multi-ValuedパラメータとSingle-Valuedパラメータのメタ キーを更新	37
タスク13: (オプション) カスタムESAルールビルダ ルールおよびESA詳細ルールの調整	38
ESAトラブルシューティング情報	39
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	40
Investigate	40
タスク14: (オプション - カスタム ロールの場合のみ) カスタム ユーザ ロールのinvestigate-server権限の調整	40
Respond	41
タスク15: (オプション) Respondサービスの統合ルールスキーマのカスタム キーをリストアする	41
タスク16: (オプション) カスタマイズされたRespondサービスの正規化スクリプトをリストアする	41
タスク17: (オプション) 対応の通知設定権限を追加する	43
DecoderおよびLog Decoder	43
タスク18: Javaバージョンの変更のため、レガシーEndpointからの定期実行フィードを再構成する	43
Endpointインストールタスク	44
11.4リレー サーバのインストール	44
Endpointエージェントのアップグレード	44
NetWitness UEBAインストールタスク	45
(オプション) パケット スキーマの追加	45
Hunting Packの追加	46
JA3とJA3sの追加	47
Airflow構成の更新	47
Airflow Schedulerサービスの再起動	48
11.2.x.xからのUEBAのアップグレード手順	49
(オプション) UEBAインジケータ転送の有効化	49
(オプション) Endpointデータ ソースの有効化	49

付録 A.ローカルリポジトリへの更新の配置	50
付録 B.外部リポジトリのセットアップ	52
付録 C.インストールとアップグレードのトラブルシューティング	55
deploy_adminのユーザ パスワード有効期限切れエラー	56
ダウンロード エラー	57
バージョン <version-number>の導入エラー:更新パッケージの不足	58
外部リポジトリ更新エラー	58
ホスト インストール失敗エラー	60
ホスト更新失敗エラー	61
更新パッケージ不足エラー	62
OpenSSL 1.1.x	63
NW Server以外へのパッチ適用エラー	63
コマンド ラインからの更新後のホスト再起動のエラー	64
アップグレード後のReporting Engine再起動	64
Log Collectorサービス(nwlogcollector)	65
NW Server	67
Orchestration	68
Reporting Engineサービス	68

アップグレードの概要

RSA NetWitness® Platform 11.4.0.0には、Platformのすべての製品の機能拡張と修正が含まれています。Platformのコンポーネントは次のとおりです：NetWitness Server(Admin server, Config server, Integration server, Investigate server, Orchestration server, Respond server, Security sever, Source server)、Archiver、Broker、Concentrator、Context Hub、Decoder、Endpoint Broker、Endpoint Log Hybrid、ESAプライマリ、ESAセカンダリ、Health & Wellness Beta、Log Collector、Log Decoder、Log Hybrid、Log Hybrid Retention、Malware Analysis、Network Decoder、Network Hybrid、Reporting Engine、UEBA、Warehouse Connector

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

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

アップグレード パス

NetWitness Platform 11.4.0.0では、以下のアップグレード パスがサポートされます。

- RSA NetWitness® Platform 11.2.x.xから11.4.0.0
- RSA NetWitness® Platform 11.3.0.xから11.4.0.0
- RSA NetWitness® Platform 11.3.1.xから11.4.0.0
- RSA NetWitness® Platform 11.3.2.xから11.4.0.0

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

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

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

混在モード

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

ESAルールを導入環境に関するアップグレードの考慮事項

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

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

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

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

[イベント]ビューの列グループに対する変更

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

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

製品ドキュメントに関するフィードバック

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

カスタマ サポート へのお問い合わせ

質問や支援が必要な場合は、以下の連絡先までお問い合わせください。

RSA Link <https://community.rsa.com/>

メール support@rsa.com

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

Legacy Windows Collectorの更新またはインストール

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

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

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

アップグレード準備タスク

NetWitness Platform 11.4へのアップグレードの準備をするには、次のタスクを実行します。

ESA(Event Stream Analysis)



タスク1: ESA Correlationサービスが指定されていないESAルール導入環境を削除する

注: このEvent Stream Analysis(ESA) タスクは、11.3.x.xから11.4にアップグレードする場合に実行します。

10.6または11.2のレガシーEvent Stream Analysisサービスから移行し、ESA Correlationサービスを指定していないESAルール導入環境が未使用のまま残っていると、NetWitness Platform 11.4へのアップグレード後にESAルール導入環境を導入できなくなる原因になります。

11.4にアップグレードする前に、ESA Correlationサービスが指定されていないESAルール導入環境を削除してください。残留させるESAルール導入環境は、ESA Correlationサービスを指定して少なくとも1回導入する必要があります。

ESAルール導入環境を削除するには、次の手順を実行します。

1. [構成]>[ESAルール]>[ルール]タブに移動します。
2. 左側のオプション パネルで、[導入環境]の下から削除する導入環境を選択します。
3.   > [削除]を選択します。
4. [はい]をクリックして、削除を確定します。

アップグレード タスク

注: (RSA NetWitness Endpointのお客様への注意) Endpoint Hybridは11.3.0.0以降のリリースではサポートされません。

11.2.x.xでEndpoint Hybridホストを導入し、11.3.x.xでEndpoint Log Hybridホストをインストールしなかった場合は、11.4でEndpoint Log Hybridホストをインストールする必要があります。11.3のEndpoint Log Hybridホストをインストールする方法については、『RSA NetWitness Platform 11.3 物理ホスト インストールガイド』または『RSA NetWitness Platform 11.3 仮想ホスト インストールガイド』を参照してください。

注: プライマリNW Server(Respond Serverサービスを含む) をアップグレードした後、プライマリESAホストを11.4にアップグレードするまで、Respond Serverサービスは再有効化されません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

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

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

注: ホストをアップグレードする前に、各ホストの時刻がNetWitness Server上の時刻と同期していることを確認します。

時刻を同期するには、次のいずれかを実行します。

- NTPサーバを構成します。詳細については、『システム構成ガイド』の「NTPサーバの構成」を参照してください。

- 各ホストで次のコマンドを実行します。

1.SSHを使用してNWホストに接続します。

2.次のコマンドを実行します。

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

次のいずれかの方式で、ホストにバージョン更新(11.4.0.0など)を適用します。

- [オンライン方式 - RSA Liveに接続](#)
- [\[ホスト\]ビューからのオフライン方式](#)
- [コマンド ライン インタフェースを使用したオフライン方式](#)

オンライン方式 (RSA Liveに接続)

NetWitness PlatformからRSA Live更新リポジトリに接続できる場合 (Webアクセス可) は、この方式を使用します。

タスク1: ローカル リポジトリに更新を配置するか、外部リポジトリをセットアップする

NW Serverをセットアップする際に、ローカルリポジトリ (Repo) または外部リポジトリ (Repo) を選択します。[ホスト]ビューでは、この時選択したリポジトリからバージョン更新を取得します。

ローカルリポジトリを選択した場合、セットアップする必要はありませんが、最新バージョンの更新を配置する必要があります。バージョン更新を配置する手順については、「[付録 A. ローカルリポジトリへの更新の配置](#)」を参照してください。

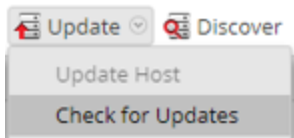
注：外部リポジトリを選択した場合は、セットアップする必要があります。外部リポジトリにバージョン更新を配置する方法については、「[付録 B. 外部リポジトリのセットアップ](#)」を参照してください。

タスク2: [ホスト]ビューから各ホストに更新を適用する

[ホスト]ビューには、ローカル更新リポジトリにある使用可能なソフトウェアの更新バージョンが表示されます。[ホスト]ビューから目的の更新を選択して適用します。

この手順は、ホストをNetWitness Platformの新しいバージョンに更新する方法について説明します。

1. NetWitness Platformにログインします。
2. [管理] > [ホスト]に移動します。
3. (オプション) 最新の更新をチェックします。

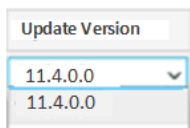


4. 1つまたは複数のホストを選択します。

最初にNW Serverを最新バージョンに更新する必要があります。その他のホストは任意の順序で更新することができますが、「[混在モード](#)」のガイドラインに従うことを推奨します。

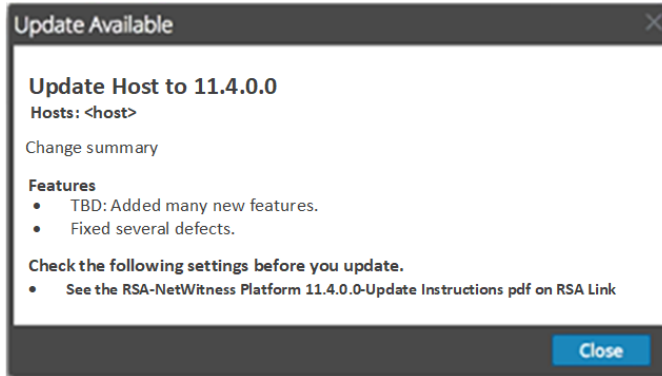
Update Available、と[ホスト]ビューの[ステータス]列に表示される場合は、そのホストのバージョン更新がローカル更新リポジトリに存在します。

5. [更新のバージョン]列から適用するバージョンを選択します。



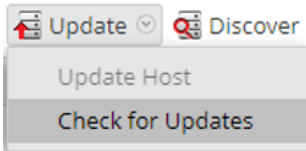
次のガイドラインに従ってください。

- 複数のホストを同じバージョンに更新する場合は、NW Serverホストを更新した後、対象ホストの左のチェックボックスを選択します。現在サポートされている更新バージョンのみが表示されます。
- 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 ⓘ をクリックします。次のようなダイアログが表示されます。

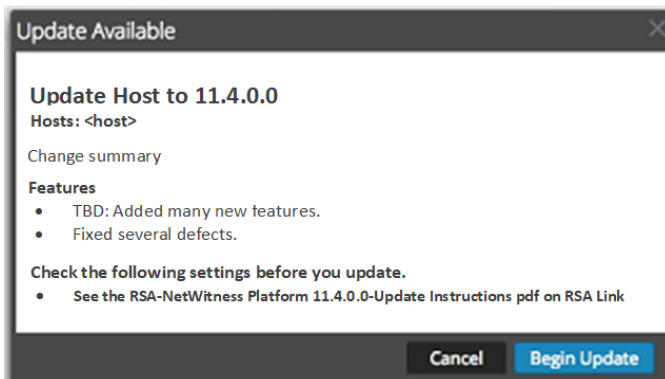


- 目的のバージョンが見つからない場合は、[更新]>[更新の確認]を選択し、リポジトリ内の使用可能な更新をチェックします。更新が利用可能な場合、「New updates are available」というメッセージが表示され、[ステータス]列が自動的に更新され、[Update Available]と表示されます。デフォルトでは、選択したホストでサポートされている更新のみが表示されます。

6. ツールバーの[更新]>[ホストの更新]をクリックします。



選択した更新に関する情報がダイアログに表示されます。[更新を開始]をクリックします。



[ステータス]列には、次のような更新の各段階の状況が表示されます。

- ステージ1: **更新パッケージのダウンロード** - 選択したホスト上のサービスに適用されるリポジトリアーティファクトをNW Serverにダウンロードします。
- ステージ2: **更新パッケージの構成** - 更新ファイルを正しい形式に構成します。
- ステージ3: **更新が進行中です** - ホストを新しいバージョンに更新しています。

7. 「Update in progress」が表示されたら、ブラウザをリフレッシュします。

この操作により、[NetWitnessログイン]画面が表示される場合がありますが、再度ログインして[ホスト]ビューに戻ることができます。

ホストの更新が完了すると、NetWitness Platformが**ホストの再起動**を求めるメッセージを表示します。

8. ツールバーの[ホストの再起動]をクリックします。

ホストがオンラインに戻ると、NetWitness PlatformUIに表示されるステータスが[Rebooting...]から[Up-to-Date]に変わります。ホストがオンラインに戻らない場合は、カスタマ サポートにお問い合わせください。

注: Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG) を有効にしている場合、コア サービスを開始するには約5～10分かかります。この遅延は新しい証明書を生成するために生じます。

[ホスト]ビューからのオフライン方式

NetWitness PlatformがRSA Live更新リポジトリに接続できない場合 (Webアクセス不可) に、[管理] > [ホスト]ビューから更新を適用するには、この方式を使用します。

注: ユーザ インタフェースを使用したオフライン方式を使用できるのは、ホストを11.3.1.0以降から11.4.0.0にアップグレードする場合だけです。これより前のバージョンのホストをアップグレードする場合は、「[コマンド ライン インタフェースを使用したオフライン方式](#)」に記載されたオフライン方式を使用する必要があります。

NetWitness Platformがインターネットに接続できない場合 (Liveに接続していない場合など) にユーザ インタフェースを使用してバージョン更新を適用するには、ここで説明する手順に従ってください。バージョン更新の適用時には、次のルールに従ってください。

- 最初にNW Serverホストを更新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。

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

1. 目的のバージョンの.zip更新パッケージ(たとえば、netwitness-11.4.0.0.zip)をRSA Linkからローカル 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. 目的の更新パッケージをローカル ディレクトリから/var/lib/netwitness/common/update-stage/のステージング フォルダにコピーします。例えば次のようなコマンドを実行します:

```
sudo cp /tmp/netwitness-<version-number>.zip
/var/lib/netwitness/common/update-stage/
```

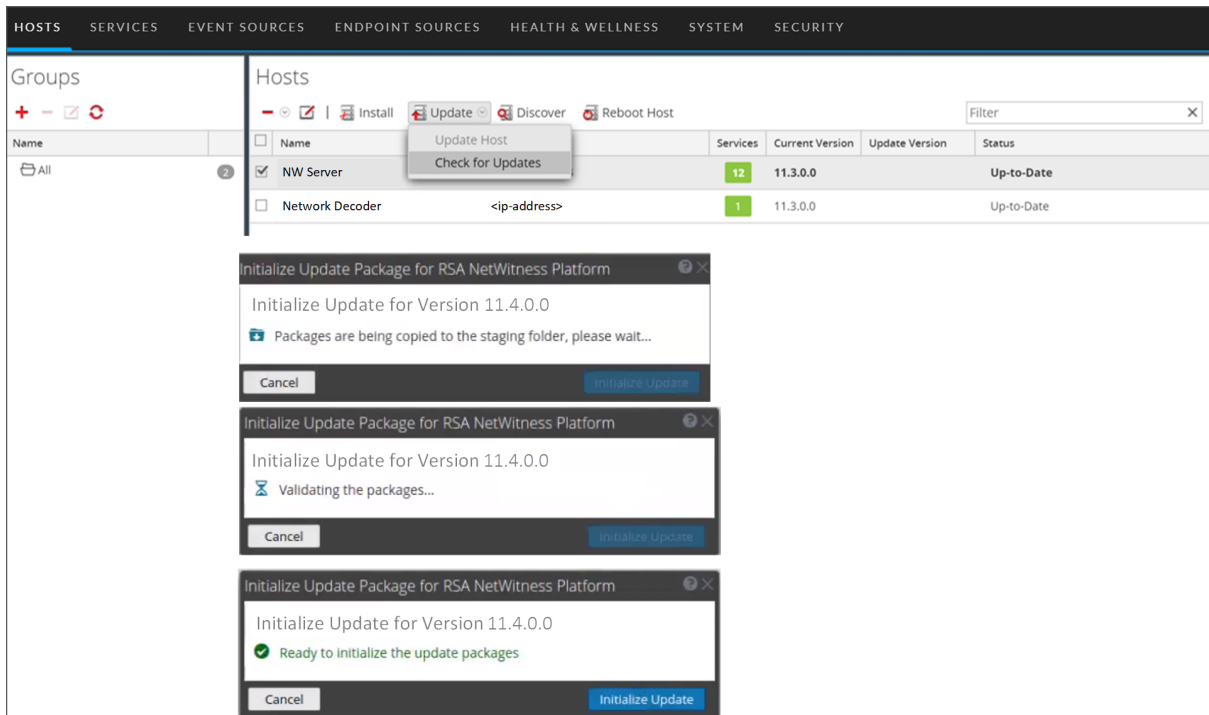
注: NetWitness Platformによってファイルは自動的に解凍されます。

タスク2: ステージング フォルダから各ホストに更新を適用

注意: NW Server以外のホストを更新する前に、NW Serverホストを更新しておく必要があります。

1. NetWitness Platformにログインします。
2. [管理] > [ホスト]に移動します。

3. 更新を確認し、更新パッケージのコピー、検証、および初期化の準備が完了するまで待ちます。

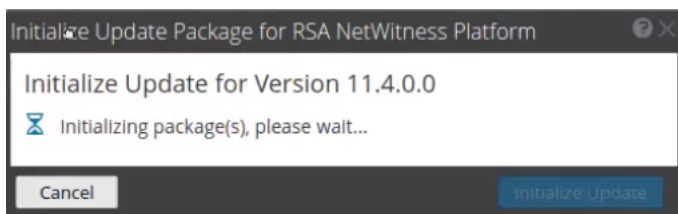


「Ready to initialize the update packages」は次の場合に表示されます。

- 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。

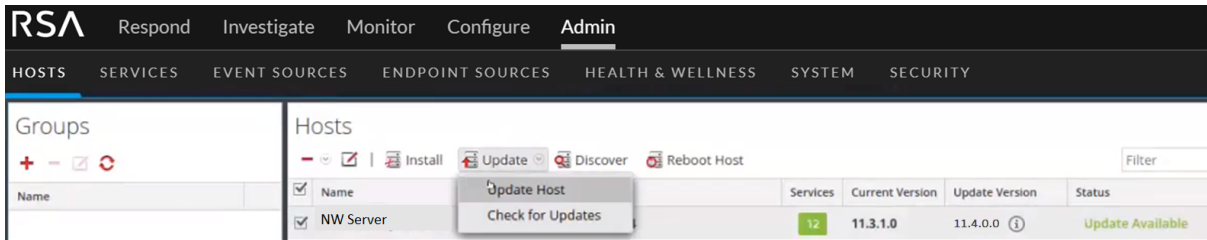
エラーのトラブルシューティング方法については、「[付録C. インストールとアップグレードのトラブルシューティング](#)」を参照してください(例えば、「RSA NetWitness Platformの更新パッケージを初期化」ダイアログに「Error deploying version <version-number>」や「Missing the following update package(s)」のようなエラーが表示される場合があります)。

4. [更新の初期化]をクリックします。



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

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。
7. ツールバーの[ホストの再起動]をクリックします。

コマンド ライン インタフェースを使用したオフライン方式

NetWitness PlatformがRSA Live更新リポジトリに接続できない場合 (Webアクセス不可) に、コマンド ライン インタフェースを使用して更新を適用するには、この方式を使用します。

RSA NetWitness Platform導入環境でWebアクセスが不可能な場合は、次の手順に従ってバージョン更新を適用します。

1. 目的のバージョンの.zip更新パッケージ(たとえば、netwitness-11.4.0.0.zip)をRSA Linkから /root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. 目的のバージョンのステージング ディレクトリを/tmp/upgrade/<version>に作成します(たとえば、/tmp/upgrade/11.4.0.0)。
`mkdir -p /tmp/upgrade/11.4.0.0`
4. .zip更新パッケージを/rootディレクトリにコピーします。

注: 1.) netwitness-11.4.0.0.zipファイルは、ステージング ディレクトリとは別のディレクトリパス (/rootディレクトリなど) にコピーします。2.) rpmファイルは、ステージング ディレクトリパス (/tmp/upgrade/11.4.0.0ディレクトリなど) に展開します。

5. 作成したステージング ディレクトリ(たとえば、/tmp/upgrade/11.4.0.0)にパッケージを解凍します。
`unzip /root/netwitness-11.4.0.0.zip -d /tmp/upgrade/11.4.0.0`
6. NW Serverで更新を初期化します。
`upgrade-cli-client --init --version 11.4.0.0 --stage-dir /tmp/upgrade/`
7. NW Serverに更新を適用します。
`upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.4.0.0`
8. NetWitness Platformにログインし、[管理] > [ホスト]に移動して、[ホスト]ビューからNW Serverホストを再起動します。
9. コンポーネント ホストごとに次の手順を実行します。
 - a. 各コンポーネント ホストに更新を適用します。
`upgrade-cli-client --upgrade --host-addr <component-host IP address> --`

version 11.4.0.0

ポーリングが完了すると、更新は完了です。

- b. NetWitness Platformにログインし、[管理]>[ホスト]に移動して、[ホスト]ビューからコンポーネント ホストを再起動します。

次のコマンドを使用して、ホストに適用されたバージョンを確認できます。

```
upgrade-cli-client --list
```

注: 1.) DISA STIGが有効化されている場合には、コア サービスが起動するまでに5～10分程度かかります。この遅延は新しい証明書を生成するために生じます。

2.) Unityストレージがある場合は、PowerPathのステータスを確認し、Unityデバイスを認識できることを確認します。

3.) 次の例のようなエラーが発生した場合、更新は正しくインストールされており、何のアクションを取る必要もありません。更新中に他のエラーが発生した場合は、カスタマ サポートにお問い合わせください。

```
2019-01-28 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)
```

アップグレード後のタスク

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

- [11.3.x.xからアップグレードする場合のアップグレード後のタスク](#)
- [11.2.x.xからアップグレードする場合のアップグレード後のタスク](#)

11.4にアップグレードした後、11.4の新機能を利用する場合は、11.4の各インストールガイドに記載されている「インストール後の手順」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「[総合目次](#)」で確認できます。

11.3.x.xからアップグレードする場合のアップグレード後のタスク

11.3.x.xから11.4にアップグレードする場合は、このセクションのすべてのタスクを実行します。

- 全般
- [Event Stream Analysis](#)
- [Investigate](#)
- [Respond](#)

全般



タスク1: サービスの再起動、データ収集、データ集計の確認

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


必要に応じて、次のサービスでデータの収集と集計を再開します。

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

ネットワーク収集の開始



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

ログ収集の開始

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

4. ツールバーで  **Start Capture** をクリックします。

集計の開始

1. NetWitness Platformメニューで、[管理] > [サービス]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  **Start Aggregation** をクリックします。

Event Stream Analysis

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

タスク2: ESAルール導入環境のステータスの確認

ESAルール導入環境のステータスを確認します。

1. [構成] > [ESAルール] > [サービス]タブに移動します。
[サービス]ビューが表示され、ESAサービスと導入環境のステータスが示されます。
2. 左側の[オプション]パネルで、ESAサービスを選択します。
3. リスト内の各サービスを選択し、右側のパネルで導入環境のタブを確認します。各タブは、個別のESAルール導入環境を表しています。
4. ESAルール導入環境ごとに、次の手順を実行します。
 - a. [ESAエンジンの統計情報]セクションで、[検出イベント数]と[検出レート]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. [構成] > [ESAルール] > [ルール] タブに移動し、無効なルールを含んでいるESAルール導入環境を再導入します。
 - b. [サービス] タブに戻り、ルールが無効かどうかを確認します。ルールがまだ無効な場合は、`/var/log/netwitness/correlation-server/correlation-server.log`にあるESA Correlationサービスのログ ファイルを確認します。

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




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

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

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

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

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

1. 11.4にアップグレードした後、[管理]>[サービス]に移動します。[サービス]ビューでESA Correlationサービスを選択してから   > [表示]> [エクスプローラ]を選択します。
2. ESA Correlationサービスの[エクスプローラ]ビューのノード リストで、[correlation]>[stream]を選択します。
3. multi-valued/パラメータのメタ キーと、default-multi-valued/パラメータのメタ キーを比較します。不足している文字列配列型のメタ キーをdefault-multi-valued/パラメータからコピーして、multi-valued/パラメータにペーストします(一度に報告されるエラーの数を減らすため、一度に追加するメタ キーは2つまでにしてください)。
4. 文字列型のメタ キーをdefault-single-valued/パラメータからコピーして、single-valued/パラメータにペーストします。
5. ESA Correlationサービスに変更を適用します。
6. [構成]>[ESAルール]に移動し、[設定]タブをクリックします。
 - [メタ キー参照]で、メタ再同期(更新)アイコン()をクリックします。
 - 複数のESA Correlationサービスがある場合は、各ESA Correlationサービスで同じメタ キーの変更を行います。
7. ESA詳細ルールでdefault-multi-valuedまたはdefault-single-valuedのいずれかのメタ キーを使用している場合は、ルール構文を更新します。「[タスク4.\(オプション\)カスタムESAルールビルド ルールおよびESA詳細ルールの調整](#)」も参照してください。
8. default-multi-valued/パラメータのメタ キーをESAルール通知テンプレートで使用している場合は、テンプレートを更新し、メタ キーの変更を反映します。『システム構成ガイド』の「グローバル通知テンプレートの構成」を参照してください。
9. ESAルール導入環境を導入します。
10. ESAルール導入環境の[ESAルール]セクションでルールのエラー メッセージを確認するか、ESA Correlationサービスのエラー ログでエラーがないか確認します。
 - ESAルール導入環境のエラー メッセージを確認するには、[構成]>[ESAルール]>[ルール]タブに移動して、左側のオプション パネルで導入環境を選択し、[ESAルール]セクションを確認します。
 - ESA Correlationサービスのログにアクセスするには、SSHを使用してシステムに接続し、`/var/log/netwitness/correlation-server/correlation-server.log`に移動します。

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

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

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

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

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

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

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

詳細については、『ESA構成ガイド』の「ESA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。

ESAトラブルシューティング情報

詳細については、「[ESAトラブルシューティング情報](#)」を参照してください。

Investigate

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


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

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

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

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

ユーザーロールの権限を有効にするには、次の手順を実行します。

1. [管理] > [セキュリティ]に移動し、[ロール]タブをクリックします。
2. 編集する必要があるカスタム ユーザーロールを選択し、 (編集アイコン) をクリックします。
3. [ロールの編集]ダイアログで、次の3つの権限を選択します。


```
investigate-server.columngroup.read
investigate-server.metagroup.read
investigate-server.profile.read
```
4. [保存]をクリックして、変更内容を保存します。カスタム ユーザーロールを割り当てられたアナリストがNetWitness Platformにログインすると、変更が有効になります。

Respond

これらのタスクは、プライマリJESAサーバを11.4にアップグレードした後で実行する必要があります。

注: プライマリNW Server(Respond Serverサービスを含む)をアップグレードした後、プライマリJESAホストを11.4にアップグレードするまで、Respond Serverサービスは再有効化されません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

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

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

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

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

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

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

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

1. `/var/lib/netwitness/respond-server/scripts.bak-<timestamp>`ディレクトリにあるバックアップされたRespondサーバの正規化スクリプトからカスタムロジックを取り出します。`<timestamp>`はバックアップが完了した時刻です。

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_ueba_alerts.js
normalize_wtd_alerts.js
utils.js
```

2. Edit the new 11.4 script files in the `/var/lib/netwitness/respond-server/scripts` directory to include any logic from the back up files. If you have any customizations in the normalization files, add them to the normalization files with the "custom" prefix.

```
data_privacy_map.js
custom_normalize_alerts.js
custom_normalize_core_alerts.js
custom_normalize_ecat_alerts.js
custom_normalize_ma_alerts.js
custom_normalize_ueba_alerts.js
custom_normalize_wtd_alerts.js
utils.js
```

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

す。

```

exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) {
  // normalizedAlert is the immutable copy of qoth normalizer alert, make sure you use
  // normalized object to update/set the values in your scripts
  var normalized = Object.assign(normalizedAlert);

  // Add custom logic below
  var custom_events;

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

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

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

  }

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

  return normalized;
}

```

タスク8:(オプション) 対応の通知設定権限を追加する

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

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

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

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

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

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

11.2.x.xからアップグレードする場合のアップグレード後のタスク

11.2.x.xから11.4にアップグレードする場合は、このセクションのすべてのタスクを実行します。

- [全般](#)
- [Event Stream Analysis](#)
- [Investigate](#)
- [Respond](#)
- [DecoderおよびLog Decoder](#)

全般



タスク1: サービスの再起動、データ収集、データ集計の確認

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


必要に応じて、次のサービスでデータの収集と集計を再開します。

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

ネットワーク収集の開始



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

ログ収集の開始

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


4. ツールバーで  **Start Capture** をクリックします。

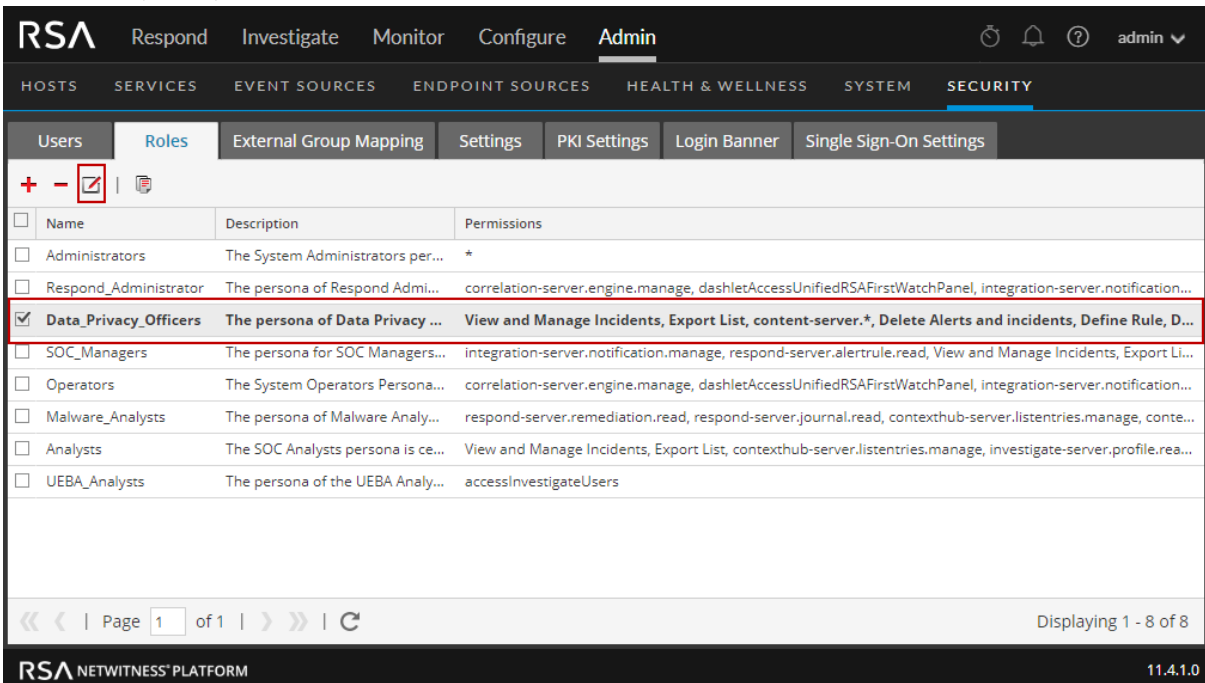
集計の開始

- 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。
- Concentrator、Broker、Archiverの各サービスに対して、以下の手順を実行します。
 - サービスを選択します。
 -  (アクション) で、[表示] > [構成]を選択します。
 - ツールバーで  **Start Aggregation** をクリックします。

タスク2: コンテキスト メニュー アクションのユーザ権限を設定する

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

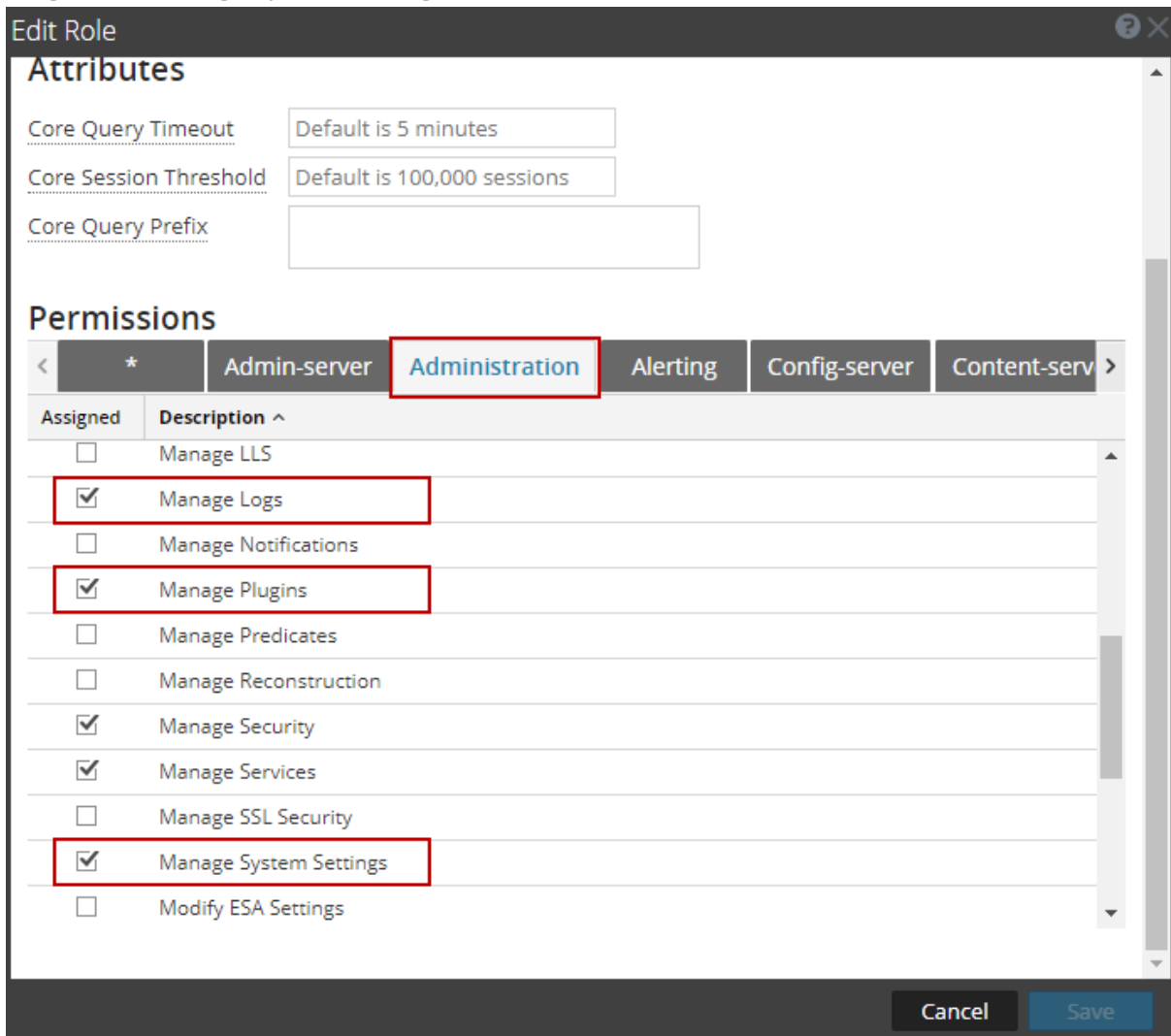
- NetWitness Platformメニューで、[管理] > [セキュリティ] > [ロール]を選択します。
- ユーザロール(たとえば[Data Privacy Officers])をダブルクリックするか、ロールをクリックして選択してから  (編集) をクリックします。



The screenshot shows the RSA NetWitness Platform Admin console. The 'Roles' tab is active, and the 'Data_Privacy_Officers' role is selected and highlighted with a red box. The 'Permissions' column for this role shows 'View and Manage Incidents, Export List, content-server.*, Delete Alerts and incidents, Define Rule, D...'. The table below is a representation of the data shown in the screenshot.

Name	Description	Permissions
<input type="checkbox"/> Administrators	The System Administrators per...	*
<input type="checkbox"/> Respond_Administrator	The persona of Respond Admi...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
<input checked="" type="checkbox"/> Data_Privacy_Officers	The persona of Data Privacy ...	View and Manage Incidents, Export List, content-server.*, Delete Alerts and incidents, Define Rule, D...
<input type="checkbox"/> SOC_Managers	The persona for SOC Managers...	integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, Export Li...
<input type="checkbox"/> Operators	The System Operators Persona...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
<input type="checkbox"/> Malware_Analysts	The persona of Malware Analy...	respond-server.remediation.read, respond-server.journal.read, contexthub-server.listentries.manage, conte...
<input type="checkbox"/> Analysts	The SOC Analysts persona is ce...	View and Manage Incidents, Export List, contexthub-server.listentries.manage, investigate-server.profile.rea...
<input type="checkbox"/> UEBA_Analysts	The persona of the UEBA Analy...	accessInvestigateUsers

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



The screenshot shows the 'Edit Role' dialog box with the 'Permissions' section expanded. The 'Administration' tab is selected. The following permissions are checked:


Assigned	Description ^
<input type="checkbox"/>	Manage LLS
<input checked="" type="checkbox"/>	Manage Logs
<input type="checkbox"/>	Manage Notifications
<input checked="" type="checkbox"/>	Manage Plugins
<input type="checkbox"/>	Manage Predicates
<input type="checkbox"/>	Manage Reconstruction
<input checked="" type="checkbox"/>	Manage Security
<input checked="" type="checkbox"/>	Manage Services
<input type="checkbox"/>	Manage SSL Security
<input checked="" type="checkbox"/>	Manage System Settings
<input type="checkbox"/>	Modify ESA Settings

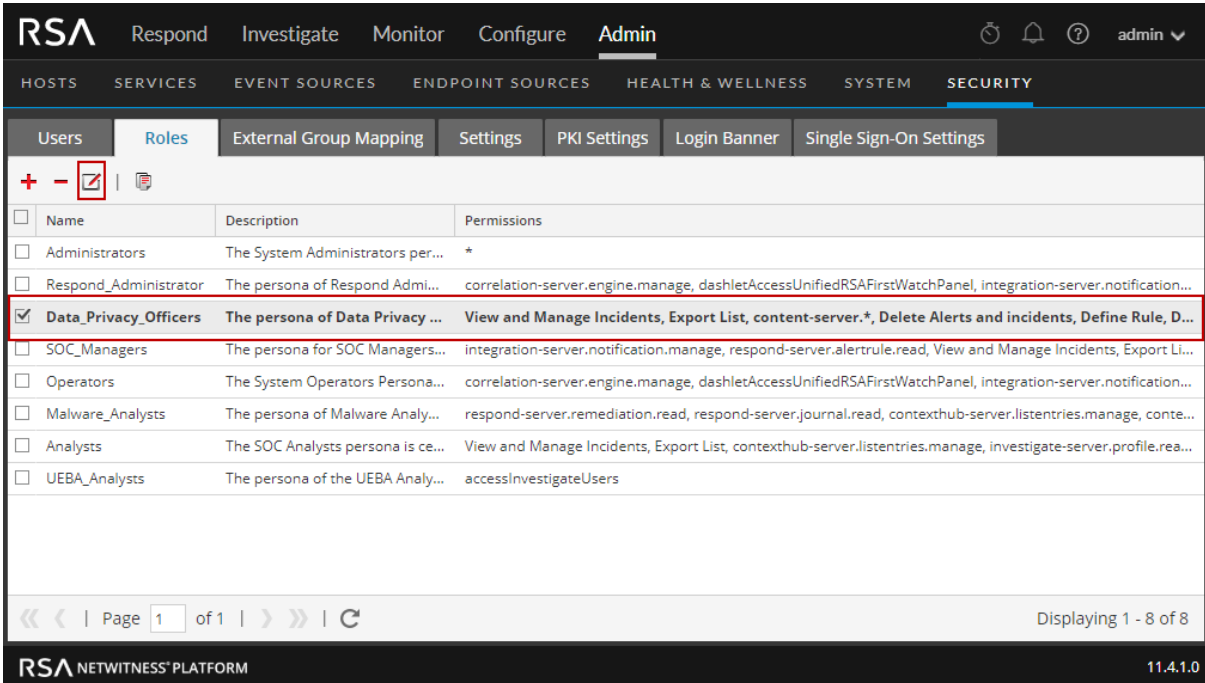
4. Data Privacy Officersと同様に、AnalystsとSOC Managersの各ロールに対してステップ1~3を実行します。

タスク3:「Manage Jobs」権限をこの権限がないロールに追加する

「Manage Jobs」権限を次のロールに追加します。

- SOC_Managers
- Operators
- Data_Privacy_Officers

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



The screenshot shows the RSA NetWitness Platform Admin console. The top navigation bar includes 'Respond', 'Investigate', 'Monitor', 'Configure', and 'Admin'. The 'Admin' section is active, and the 'SECURITY' sub-menu is selected. Under 'SECURITY', the 'Roles' tab is active. A table lists various roles, with 'Data_Privacy_Officers' selected (checkbox checked) and highlighted with a red border. The table has columns for Name, Description, and Permissions.

<input type="checkbox"/>	Name	Description	Permissions
<input type="checkbox"/>	Administrators	The System Administrators per...	*
<input type="checkbox"/>	Respond_Administrator	The persona of Respond Admi...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
<input checked="" type="checkbox"/>	Data_Privacy_Officers	The persona of Data Privacy ...	View and Manage Incidents, Export List, content-server.*, Delete Alerts and incidents, Define Rule, D...
<input type="checkbox"/>	SOC_Managers	The persona for SOC Managers...	integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, Export Li...
<input type="checkbox"/>	Operators	The System Operators Persona...	correlation-server.engine.manage, dashletAccessUnifiedRSAFirstWatchPanel, integration-server.notification...
<input type="checkbox"/>	Malware_Analysts	The persona of Malware Analy...	respond-server.remediation.read, respond-server.journal.read, contexthub-server.listentries.manage, conte...
<input type="checkbox"/>	Analysts	The SOC Analysts persona is ce...	View and Manage Incidents, Export List, contexthub-server.listentries.manage, investigate-server.profile.rea...
<input type="checkbox"/>	UEBA_Analysts	The persona of the UEBA Analy...	accessInvestigateUsers

Page 1 of 1 | Displaying 1 - 8 of 8

RSA NETWITNESS PLATFORM 11.4.1.0

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

The screenshot shows the 'Edit Role' window with the following details:

- Attributes:**
 - Core Query Timeout: Default is 5 minutes
 - Core Session Threshold: Default is 100,000 sessions
 - Core Query Prefix: (empty)
- Permissions:**
 - Admin-server
 - Administration** (selected)
 - Alerting
 - Config-server
 - Content-serv

Assigned	Description ^
<input checked="" type="checkbox"/>	Manage Auditing
<input type="checkbox"/>	Manage Email
<input checked="" type="checkbox"/>	Manage Global Auditing
<input type="checkbox"/>	Manage Health & Wellness Policy
<input checked="" type="checkbox"/>	Manage Jobs
<input type="checkbox"/>	Manage LLS
<input checked="" type="checkbox"/>	Manage Logs
<input type="checkbox"/>	Manage Notifications
<input checked="" type="checkbox"/>	Manage Plugins
<input type="checkbox"/>	Manage Predicates
<input type="checkbox"/>	Manage Reconstruction

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

タスク4:(オプション)ホストの証明書を再発行する

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

NetWitness Platformの証明書の有効期間は次のとおりです。

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

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

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

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


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

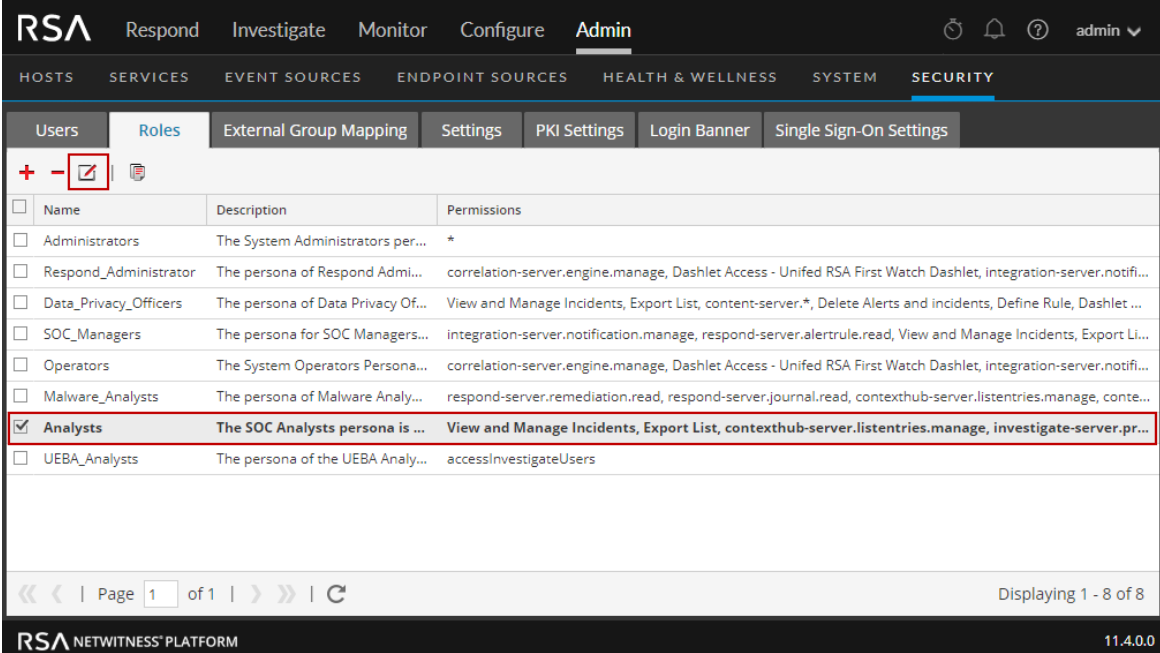
タスク5: アナリスト ロールのinvestigate-server権限を変更する

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

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

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

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



The screenshot shows the RSA NetWitness Platform Admin interface. The 'Roles' tab is active, and the 'Analysts' role is selected. The permissions for this role are being edited, and the 'investigate-server.pr...' permission is highlighted.

Name	Description	Permissions
<input type="checkbox"/>	Administrators	The System Administrators per... *
<input type="checkbox"/>	Respond_Administrator	The persona of Respond Admi... correlation-server.engine.manage, Dashlet Access - Unified RSA First Watch Dashlet, integration-server.notifi...
<input type="checkbox"/>	Data_Privacy_Officers	The persona of Data Privacy Of... View and Manage Incidents, Export List, content-server.*, Delete Alerts and Incidents, Define Rule, Dashlet ...
<input type="checkbox"/>	SOC_Managers	The persona for SOC Managers... integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, Export Li...
<input type="checkbox"/>	Operators	The System Operators Persona... correlation-server.engine.manage, Dashlet Access - Unified RSA First Watch Dashlet, integration-server.notifi...
<input type="checkbox"/>	Malware_Analysts	The persona of Malware Analy... respond-server.remediation.read, respond-server.journal.read, contexthub-server.listentries.manage, conte...
<input checked="" type="checkbox"/>	Analysts	The SOC Analysts persona is ... View and Manage Incidents, Export List, contexthub-server.listentries.manage, investigate-server.pr...
<input type="checkbox"/>	UEBA_Analysts	The persona of the UEBA Analy... accessInvestigateUsers

- b. [権限]の下で、[Investigate-server]タブをクリックします。
- c. 次の権限のチェックを外します。
 - `investigate-server.*`
 - `investigate-server.predicate.manage`
- d. 次の権限のチェックを選択します。
 - `investigate-server.content.export`
 - `investigate-server.content.reconstruct`
 - `investigate-server.event.read`
 - `investigate-server.metagroup.read`
 - `investigate-server.predicate.read`

- e. [保存]をクリックします。

タスク6: (オプション) PAM Radius認証を再構成する

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

NW Serverホストで次のコマンドを実行する必要があります。

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

1. 既存のパッケージを確認し、既存のpam_radius ファイルをアンインストールします。

```
rpm -qa |grep pam_radius
yum erase pam_radius
```
2. pam_radius_authパッケージをインストールするには、次のコマンドを実行します。

```
yum install pam_radius_auth
```
3. RADIUS構成ファイル(/etc/raddb/server)を次のように編集して、RADIUSサーバの構成を追加します。

```
# server[:port] shared_secret timeout (s)
server secret 3
例:111.222.33.44 secret 1
```
4. NW ServerホストのPAM構成ファイル(/etc/pam.d/securityanalytics)を編集し、次の行を追加します。ファイルが存在しない場合は、ファイルを作成し、次の行を追加します。

```
auth sufficient pam_radius_auth.so
```
5. 次のコマンドを実行して、/etc/raddb/serverへの書き込み権限を許可します。

```
chown netwitness:netwitness /etc/raddb/server
```
6. 次のコマンドを実行して、pam_radius_authライブラリをコピーします。

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```
7. pam_radius_authの構成を変更した後、次のコマンドを実行してJettyサーバを再起動します。

```
systemctl restart jetty
```

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

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

タスク8: パスワードの最小長を8文字から9文字に変更する

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

Event Stream Analysis

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

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


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

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

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

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

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

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

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

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

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



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

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

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

タスク11: ESAルール導入環境を検証する

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

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



詳細な例については、『ESA構成ガイド』を参照してください。導入環境の詳細については、『ESA関連ルールアラート ユーザガイド』の「ESAルールの導入ステップ」を参照してください。トラブルシューティングの詳細については、『ESA関連ルールアラート ユーザガイド』を参照してください。


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

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

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

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

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

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

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

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

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

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

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

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

```
@RSAAlert
```

```
SELECT * FROM Event(( 'Success' = ANY( ec_outcome ) ))
```

```
.win:time_length_batch(2 Minutes, 2)
```

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

詳細については、『ESA構成ガイド』の「ESA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。

ESAトラブルシューティング情報

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

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

11.4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のESA Correlationサービスでは、次のデフォルトの**単一値メタ キー**も必要です。

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

変更された文字列配列メタ キーまたは文字列メタ キーをESAルール通知テンプレートで使用している場合は、テンプレートを更新し、メタ キーの変更を反映します。『システム構成ガイド』の「グローバル通知テンプレートの構成」を参照してください。

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。

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

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

複数値の警告メッセージの例

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id, browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_src, client_all, content, context, context_all, context_dst, context_src, dir_path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst, directory_src, email_dst, email_src, feed_category, feed_desc, feed_name, file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter, function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_orig, OS, param, param_dst, param_src, registry_key, registry_value, risk, risk_info, risk_suspicious, risk_warning, threat_category, threat_desc, threat_source, user_agent] are still MISSING from multi-valued
```

単一値の警告メッセージの例

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

Investigate

タスク14:(オプション - カスタム ロールの場合のみ) カスタム ユーザ ロールの

investigate-server権限の調整


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

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

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

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

ユーザ ロールの権限を有効にするには、次の手順を実行します。

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

Respond

これらのタスクは、プライマリESAサーバを11.4にアップグレードした後で実行する必要があります。

注: プライマリNW Server(Respond Serverサービスを含む) をアップグレードした後、プライマリESAホストを11.4にアップグレードするまで、Respond Serverサービスは再有効化されません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

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

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

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

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

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

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

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

1. /var/lib/netwitness/respond-server/scripts.bak-<timestamp>ディレクトリにあるバックアップされたRespondサーバの正規化スクリプトからカスタム ロジックを取り出します。<timestamp>はバックアップが完了した時刻です。
data_privacy_map.js

```

normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_ueba_alerts.js (11.3以降のバージョン)
normalize_wtd_alerts.js
utils.js

```

2. Edit the new 11.4 script files in the `/var/lib/netwitness/respond-server/scripts` directory to include any logic from the back up files. If you have any customizations in the normalization files, add them to the normalization files with the "custom" prefix.

```

data_privacy_map.js
custom_normalize_alerts.js
custom_normalize_core_alerts.js
custom_normalize_ecat_alerts.js
custom_normalize_ma_alerts.js
custom_normalize_ueba_alerts.js
custom_normalize_wtd_alerts.js
utils.js

```

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

```

exports.normalizeAlert = function (headers, rawAlert, normalizedAlert) {
  // normalizedAlert is the immutable copy of ooth normalizer alert, make sure you use
  // normalized object to update/set the values in your scripts
  var normalized = Object.assign(normalizedAlert);

  // Add custom logic below
  var custom_events;

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

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

    custom_events[i].legality: Utils.stringValue(rawAlert.events[i].isgs_legality);
    custom_events[i].companycode: Utils.stringValue(rawAlert.events[i].isgs_companycode);

  }

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

  return normalized;
}

```

タスク17:(オプション) 対応の通知設定権限を追加する

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

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

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

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

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

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

DecoderおよびLog Decoder

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

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

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

Endpointインストール タスク

11.4 リレー サーバのインストール

リレー サーバを構成した場合は、次の手順を実行します。

1. アップグレードされたEndpoint Serverからリレー サーバのインストーラをダウンロードし、リレー サーバを11.4にアップグレードする必要があります。詳細については、『*Endpoint構成ガイド*』の「(オプション)リレー サーバのインストールと構成」を参照してください。
2. 次のコマンドを使用して、Endpoint Serverを再起動します。

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

Endpointエージェントのアップグレード

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

NetWitness UEBAインストール タスク

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

- [\(オプション\) パケット スキーマの追加](#)
- [Hunting Packの追加](#)
- [JA3とJA3sの追加](#)
- [Airflow構成の更新](#)
- [Airflow Schedulerサービスの再起動](#)
- [11.2.x.xからのUEBAのアップグレード手順](#)

(オプション) パケット スキーマの追加

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

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

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

UEBAによって処理されるスキーマを表示するには、Airflowメイン ページ(<https://<UEBAホスト>/admin>)にアクセスします。このページには、処理されるスキーマが表示されます。

The screenshot shows the Airflow DAGs page with a table of DAGs. The table has columns for DAG, Schedule, Owner, Recent Tasks, Last Run, DAG Runs, and Links. Annotations are added to the table:

- Windows Logs – Active Directory Schema** (blue text) points to the first two DAGs: ACTIVE_DIRECTORY_indicator_ueba_flow and ACTIVE_DIRECTORY_model_ueba_flow.
- Windows Logs – Authentication Schema** (blue text) points to the next two DAGs: AUTHENTICATION_indicator_ueba_flow and AUTHENTICATION_model_ueba_flow.
- Windows Logs – File Schema** (blue text) points to the next two DAGs: FILE_indicator_ueba_flow and FILE_model_ueba_flow.
- Endpoint Events – Process Schema** (orange text) points to the next two DAGs: PROCESS_indicator_ueba_flow and PROCESS_model_ueba_flow.
- Endpoint Events – Registry Schema** (orange text) points to the next two DAGs: REGISTRY_indicator_ueba_flow and REGISTRY_model_ueba_flow.
- Packets Events – TLS Schema** (orange text) points to the next two DAGs: TLS_indicator_ueba_flow and TLS_model_ueba_flow.

スキーマまたはデータソースを変更するには、DAGのアップグレードを実行する前に、次のスクリプトを実行します。

```
/opt/rsa/saTools/bin/ueba-server-config
```

UEBAによって処理されるデータソースを確認するには、UEBAサーバで次のコマンドを実行して、NetWitness Platformデータソースを取得します。



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

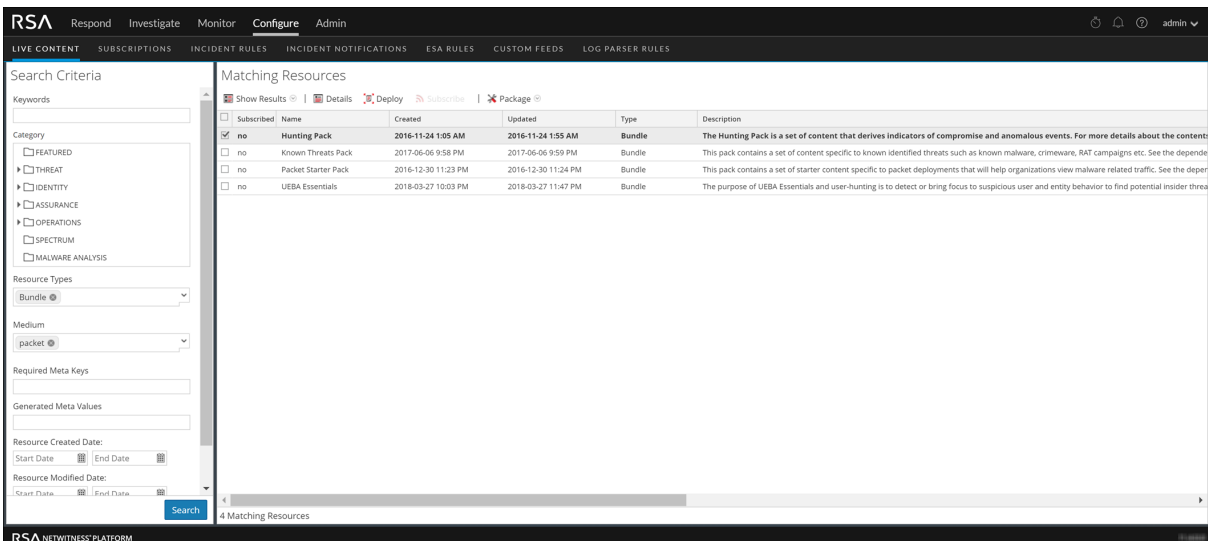
次のコマンドを使用して、NetWitness Platformデータソースを取得することもできます。

```
curl http://localhost:8888/application-presidio-default.properties | grep 'dataPulling.source'
```

Hunting Packの追加

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

1. NetWitness Platformにログインします。
2. [管理]に移動し、[Admin Server]を選択します。
3.   をクリックして、[構成] > [Liveコンテンツ]を選択します。



The screenshot shows the RSA NetWitness Platform interface. The 'Matching Resources' section displays a table with the following data:

Subscribed	Name	Created	Updated	Type	Description
<input checked="" type="checkbox"/>	Hunting Pack	2016-11-24 1:05 AM	2016-11-24 1:55 AM	Bundle	The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. For more details about the content...
<input type="checkbox"/>	Known Threats Pack	2017-06-06 9:58 PM	2017-06-06 9:59 PM	Bundle	This pack contains a set of content specific to known identified threats such as known malware, crimeware, RAT campaigns etc. See the depende...
<input type="checkbox"/>	Packet Starter Pack	2016-12-30 11:23 PM	2016-12-30 11:24 PM	Bundle	This pack contains a set of starter content specific to packet deployments that will help organizations view malware related traffic. See the deper...
<input type="checkbox"/>	UEBA Essentials	2018-03-27 10:03 PM	2018-03-27 11:47 PM	Bundle	The purpose of UEBA Essentials and user-hunting is to detect or bring focus to suspicious user and entity behavior to find potential insider thre...

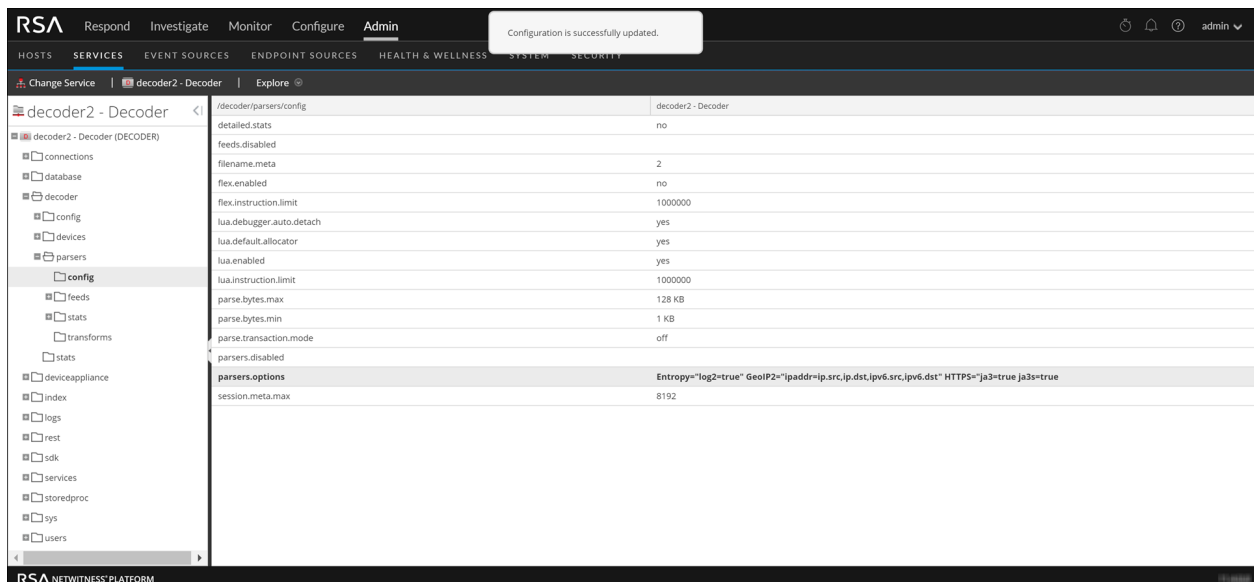
4. 検索条件で、次の項目を選択します。
 - a. [リソースタイプ]で「Bundle」を選択します。
 - b. [対象]で「Packet」を選択します。
5. [検索]をクリックします。
一致するリソースのリストが表示されます。
6. リストから[Hunting Pack]を選択し、[導入]をクリックします。
Hunting Packが追加されます。

JA3とJA3sの追加

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

JA3およびJa3sを追加するには、次の手順を実行します。

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



Airflow構成の更新

NetWitness Platform 11.4にアップグレードした後、Airflow構成を更新してください。


Airflow構成を更新するには、次の手順を実行します。

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

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

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

DAG	Schedule	Owner	Recent Tasks	Last Run	DAG Runs	Links
ACTIVE_DIRECTORY_indicator_ueba_flow	None	Airflow		2019-11-16 14:00		Refresh View Edit Delete Help
ACTIVE_DIRECTORY_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help
AUTHENTICATION_indicator_ueba_flow	None	Airflow		2019-11-16 14:00		Refresh View Edit Delete Help
AUTHENTICATION_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help
FILE_indicator_ueba_flow	None	Airflow		2019-11-16 14:00		Refresh View Edit Delete Help
FILE_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help
PROCESS_indicator_ueba_flow	None	Airflow		2019-11-16 14:00		Refresh View Edit Delete Help
PROCESS_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help
REGISTRY_indicator_ueba_flow	None	Airflow		2019-11-16 14:00		Refresh View Edit Delete Help
REGISTRY_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help
TLS_indicator_ueba_flow	None	Airflow		2019-11-16 14:00		Refresh View Edit Delete Help
TLS_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help
ja3_hourly_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help
ja3_hourly_ueba_flow	1:00:00	Airflow		2019-11-15 17:00		Refresh View Edit Delete Help
maintenance_flow_dag	1:00:00	operations		2019-11-21 08:00		Refresh View Edit Delete Help
presidio_upgrade_dag_from_11.3.0.0_to_11.4.0.0	None	Airflow		2019-11-20 10:08		Refresh View Edit Delete Help
reset_presidio	None	Airflow		2019-11-20 10:14		Refresh View Edit Delete Help
retention_ueba_flow	None	Airflow				Refresh View Edit Delete Help
root_2019-10-24_00_00_00_ueba_flow	1:00:00	Airflow		2019-11-16 15:00		Refresh View Edit Delete Help
ssiSubject_hourly_model_ueba_flow	None	Airflow		2019-11-14 23:00		Refresh View Edit Delete Help

- presidio_upgrade_dag_from_11.3.0.0_to_11.4.0.0 DAGで  をクリックして、フルフロー DAGを一時停止します。

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

注：UEBAシステムにデータがあるかどうかを確認するには、UEBAサーバでwgetコマンドを実行します。UEBAシステムにデータがない場合は、RSAカスタマ サポートにお問い合わせください。

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

注：11.2.x.xからアップグレードする場合は、「[11.2.x.xからのUEBAのアップグレード手順](#)」の手順をこのタイミングで実行し、その後で、次の説明に従ってAirflow Schedulerサービスを再起動します。

Airflow Schedulerサービスの再起動

presidio_upgrade DAGの処理が成功したら、Airflow Schedulerサービスを再起動する必要があります。

注：presidio_upgrade DAGが成功すると、そのDAGの[Recent Tasks]列に濃い緑色の丸が表示されます。

Airflow Schedulerサービスを再起動するには、UEBAサーバで次のコマンドを実行します。

```
systemctl restart airflow-scheduler
```


11.2.x.xからのUEBAのアップグレード手順

(オプション) UEBAインジケータ転送の有効化

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

UEBAインジケータ転送を有効にするには、次のコマンドを実行します。

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

[対応]ビューにインシデントを表示するには、次の手順を実行します。

1. NetWitness Platformにログインします。
2. [構成] > [インシデント ルール]に移動します。
3. [User Entity Behavior Analytics]ルールチェックボックスを選択し、有効化します。

↑	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS	RULE CREATED	RULE LAST UPDATED
	2	▶	Outsider accessing FTP Server		01/27/2020 10:38:05 p...	1	1	01/17/2020 11:29:23 am	01/17/2020 12:57:32 p...
	3	▶	User Behavior	This incident rule captures network user behavior.		0	0		
	4	▶	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication with a Command ...		0	0		
	5	▶	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA Malware Analys...	01/29/2020 09:30:02 am	169	147		
	6	▶	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA NetWitness End...	01/28/2020 01:39:49 p...	11	5		
	7	▶	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reporting Engin...	01/29/2020 01:34:03 am	14	13		
	7	▶	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ESA platform as ...	01/27/2020 10:33:55 p...	140	8		
	9	▶	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addresses that have b...		0	0		
	10	▶	User Watch List: Activity Detected	This incident rule captures alerts generated by network users whose us...		0	0		
	11	▶	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of worm propagatio...		0	0		
	12	▶	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common ICMP host ident...		0	0		
	13	▶	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert designed to detect th...		0	0		
	14	▶	Web Threat Detection	This incident rule captures alerts generated by the RSA Web Threat Det...		0	0		
	15	▶	User Entity Behavior Analytics	This incident rule captures user entity behavior.		0	0		
	16	▶	Copy of User Behavior			0	0	01/17/2020 10:45:50 am	01/17/2020 10:46:59 am

(オプション) Endpointデータソースの有効化

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

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

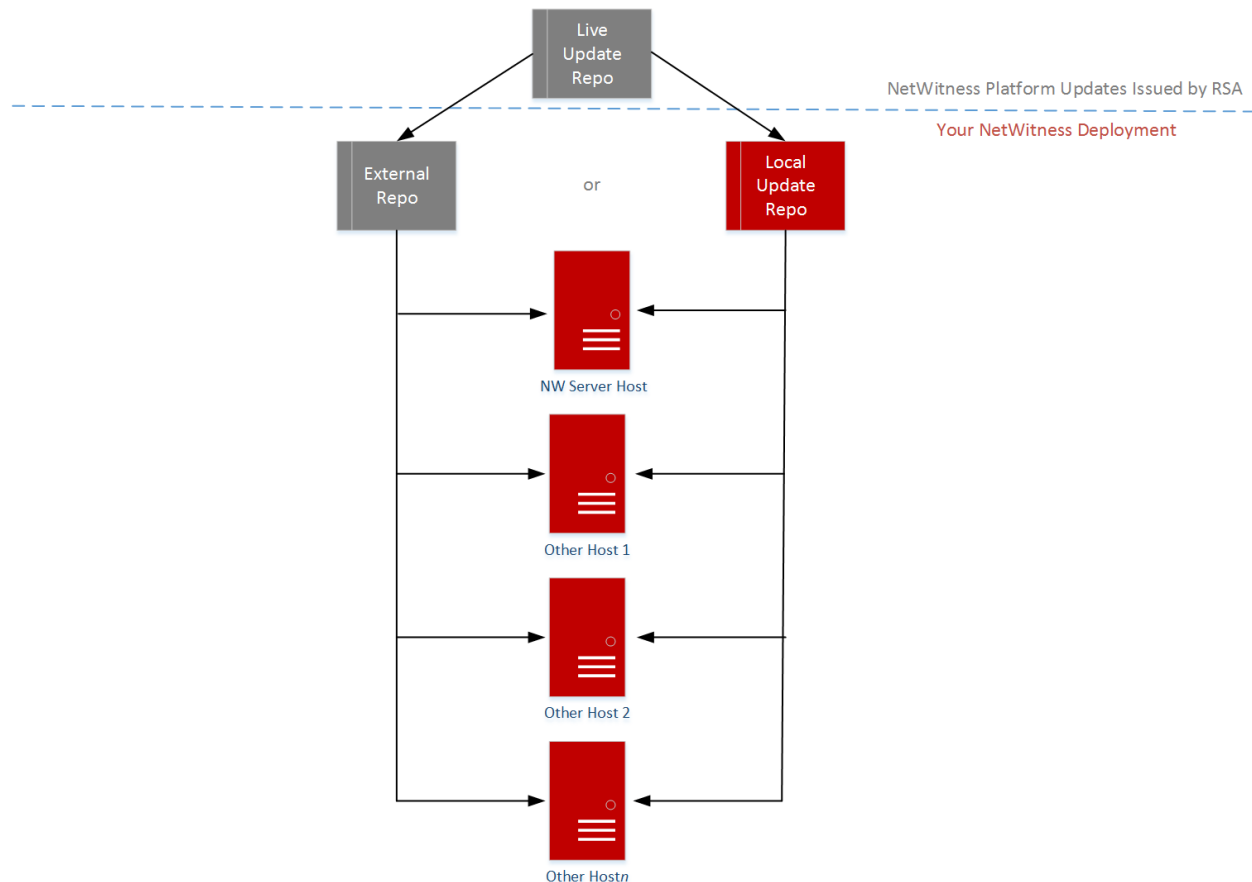
```
curl -X PATCH http://localhost:8881/configuration -H 'content-type: application/json' -d '{"operations": [{"op": "add", "path": "/dataPipeline/schemas/-", "value": "PROCESS"}, {"op": "add", "path": "/dataPipeline/schemas/-", "value": "REGISTRY"}]}'
```

付録 A.ローカルリポジトリへの更新の配置

NetWitness Platformは、バージョンの更新をLive更新リポジトリからローカル更新リポジトリに送信します。Live更新リポジトリへのアクセスには、[管理]>[システム]>[Liveサービス]に構成されたLiveアカウントの認証情報が使用されます。また、ローカルリポジトリへの送信を毎日行うには、[管理]>[システム]>[更新]の[新しい更新の情報を毎日自動的にダウンロード]チェックボックスをオンにする必要があります。

次の図は、Webアクセスが可能なNetWitness Platform導入環境で、バージョン更新を取得する方法を示しています。

RSA NetWitness Platform® 11.x.x.x Version Update Workflow – Web Access



注: Live更新リポジトリに最初に接続する場合、CentOS 7のシステムパッケージとRSA製品パッケージすべてにアクセスすることになります。このため、この初回の同期では、6.5 GBを超えるデータがダウンロードされます。同期に要する時間は、使用するNW Serverのインターネット接続環境やRSA Live更新リポジトリのトラフィックによって異なります。Live更新リポジトリの使用は必須ではありません。代わりに外部リポジトリを使用することもできます。

Live更新リポジトリに接続するには、[管理]>[システム]に移動し、オプションパネルで[Liveサービス]を選択して、認証情報が構成されていることを確認します([接続済み]ボタンが緑色)。緑色でない場合は、[サインイン]をクリックして、接続します。

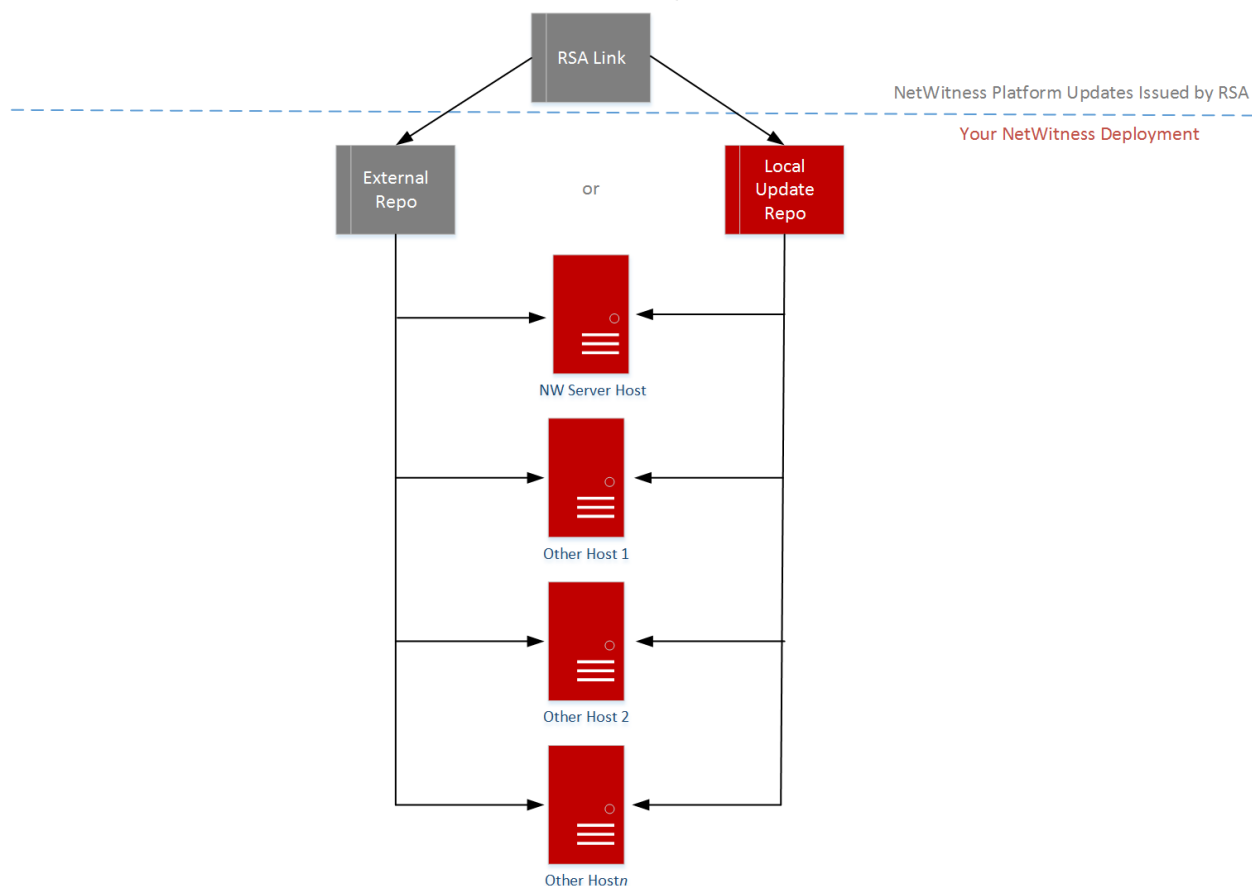
注: Live更新リポジトリへの接続にプロキシを使用する必要がある場合、プロキシ ホスト、プロキシ ユーザー名、プロキシ パスワードを構成できます。詳細については、『システム構成ガイド』の「NetWitness Platformのプロキシの構成」を参照してください。

お使いのNetWitness Platform導入環境からWebにアクセスできない場合は、次のいずれかの方法を使用してバージョン更新をホストに適用できます。

- [RSA Live更新リポジトリに接続しないで\[ホスト\]ビューからバージョン更新を適用する\(Webアクセス不可\)](#)
- [コマンド ラインから更新を適用する\(Webアクセス不可\)](#)

次の図は、Webアクセス不可のNetWitness Platform導入環境で、バージョン更新を取得する方法を示しています。

RSA NetWitness Platform® 11.x.x.x Version Update Workflow – No Web Access



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する必要があります。

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初期インストールしたが、Admin Server(NW 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` ツールを使用したアップグレードの手順を完了します。
 - ケース2: Admin Server(NW Serverホスト)のローカルリポジトリからホストを初期インストールしたが、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` ツールを使用したアップグレードの手順を完了します。

手順については、「[コマンドライン インタフェースを使用したオフライン方式](#)」を参照してください。
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-11.4.0.0.zip`)を配置するディレクトリを作成します(例: Webサーバの`web-root`の下に`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. `11.4.0.0`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>/11.4.0.0
```
 - d. `OS`ディレクトリと`RSA`ディレクトリを`/var/netwitness/<your-zip-file-repo>/11.4.0.0`の下に作成します。

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA
```
 - e. `netwitness-11.4.0.0.zip`ファイルを`/var/netwitness/<your-zip-file-repo>/11.4.0.0`ディレクトリに解凍します。

```
unzip netwitness-11.4.0.0.zip -d /var/netwitness/<your-zip-file-
```

```
repo>/11.4.0.0
netwitness-11.4.0.0.zipを解凍すると、2つのZipファイル(OS-11.4.0.0.zipとRSA-11.4.0.0.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-11.4.0.0.zipを /var/netwitness/<your-zip-file-repo>/11.4.0.0/OSディレクトリに解凍します。

```
unzip /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS
```

次の例は、ファイル解凍後のオペレーティングシステム(OS)ファイルの構造を示しています。

Parent Directory		-
	GeoIP-1.5.0-11.el7.x86_64.rpm	20-Nov-2016 12:49 1.1M
	HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 10:07 4.6M
	Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 10:05 1.5M
	OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43 502K
	OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43 15K
	PyYAML-3.11-1.el7.x86_64.rpm	19-Dec-2017 12:30 160K
	SDL-1.2.15-14.el7.x86_64.rpm	25-Nov-2015 10:39 204K
	acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 10:04 81K
	adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm	13-Feb-2018 05:10 706K
	alsa-lib-1.1.3-3.el7.x86_64.rpm	10-Aug-2017 10:52 421K
	at-3.1.13-22.el7_4.2.x86_64.rpm	25-Jan-2018 17:56 51K
	atk-2.22.0-3.el7.x86_64.rpm	10-Aug-2017 10:53 258K
	attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 10:04 66K















リポジトリの外部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-11.4.0.0.zipを/var/netwitness/<your-zip-file-repo>/11.4.0.0/RSAディレクトリに解凍します。

```
unzip /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA-11.4.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/RSA
```

次の例は、ファイル解凍後のRSAバージョン更新ファイルの構造を示しています。

 Parent Directory	-
 MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07 1.2M
 OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07 173K
 bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03 203K
 bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07 52K
 cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14 85K
 device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56 134K
 dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36 277K
 elasticsearch-5.6.9.rpm	17-Apr-2018 09:37 32M
 erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07 17K
 fineserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11 1.3M
 htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23 102K
 i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08 399K
 ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41 441K
 iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20 51K
 ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08 374K

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>/11.4.0.0/OS/other`
 - ii. `unzip nw-azure-11.3-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS/other`
 - iii. `cd /var/netwitness/<your-zip-file-repo>/11.4.0.0/OS`
 - iv. `createrepo`
- i. NW 11.4.0.0セットアッププログラム(`nwsetup-tui`)によって[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. インストールとアップグレードのトラブルシューティング

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

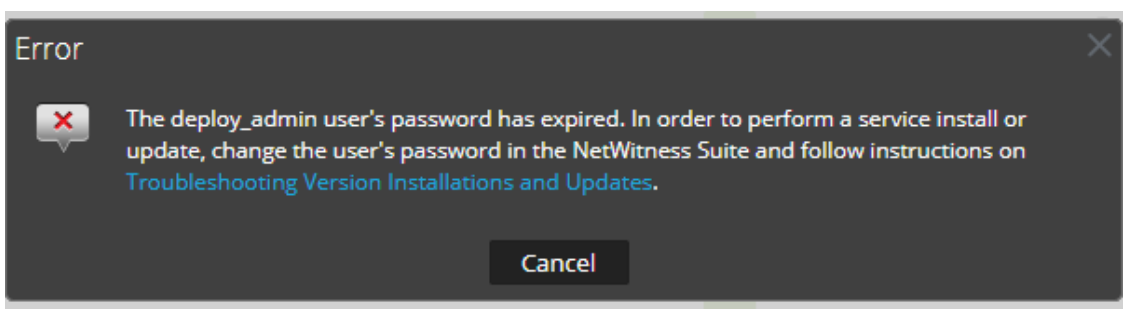
このセクションでは、アップグレード中に発生する可能性がある次のエラーのトラブルシューティング手順について説明します。

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

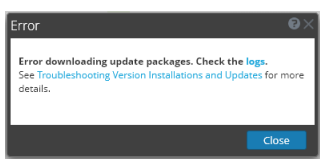
次のホストおよびサービスのアップグレード中またはアップグレード後に発生する可能性があるエラーについても、トラブルシューティング手順を記載しています。

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

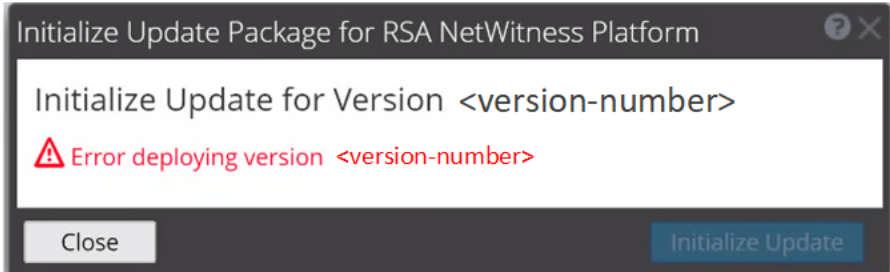
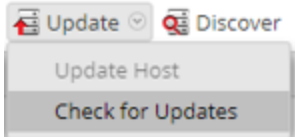
deploy_adminのユーザ パスワード有効期限切れエラー

エラー メッ セージ	 <p>The dialog box has a title bar 'Error' with a close button (X). The main text reads: '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 Troubleshooting Version Installations and Updates.' Below the text is a 'Cancel' button.</p>
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	<p>deploy_adminのパスワードをリセットします。</p> <ol style="list-style-type: none">1. (NW Serverホスト以外の) すべてのコンポーネント ホストで、次のコマンドを実行します。 <code>/opt/rsa/saTools/bin/set-deploy-admin-password</code>2. すべてのコンポーネント ホストを更新した後、NW Serverホストで次のコマンドを実行します。 <code>/opt/rsa/saTools/bin/set-deploy-admin-password</code>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、<code>nwsetup-tui</code> 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	<ol style="list-style-type: none">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、『<i>NetWitness Platform 11.4 アップグレード ガイド</i>』の「[ホスト]ビューからのオフライン方式」または「コマンド ライン インタフェースを使用したオフライン方式」の説明に従って、オフライン方式で更新してみてください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。3. それでも更新できない場合は、カスタマ サポートにお問い合わせください。

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

エラーメッセージ	
問題	<p>「バージョン <version-number>の導入中にエラーが発生しました」のエラーは更新 パッケージが破損している場合に、[更新の初期化]をクリックした後で、[RSA NetWitness Platformの更新パッケージの初期化]ダイアログに表示されます。</p>
解決策	<ol style="list-style-type: none"> [閉じる]をクリックしてダイアログを閉じます。 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。 salt-masterサービスが実行されていることを確認します。 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。 [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。  <ol style="list-style-type: none"> [更新の初期化]をクリックします。 ツールバーの[更新] > [ホストの更新]をクリックします。 [更新あり]ダイアログで[更新を開始]をクリックします。 ホストの更新が完了すると、ホストの再起動を求めるメッセージが表示されます。 ツールバーの[ホストの再起動]をクリックします。

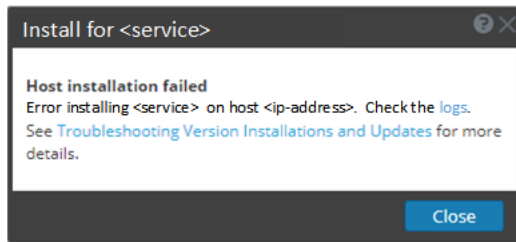
外部リポジトリ更新エラー

エラーメッセージ	<p>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返されました:</p> <pre>。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 ""</pre>
原因	<p>指定したパスに問題があります。</p>
解決策	<p>次の情報を確認します。</p> <ul style="list-style-type: none"> URLがNW Serverホスト上に存在する。

- 正しいパスを使用し、パスからはスペースを削除している。

ホスト インストール失敗エラー

エラー メッ セージ



問題

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

解決 策

1. サービスのインストールを再試行します。
通常は、これで問題が解決されます。
2. それでもサービスをインストールできない場合は、次の手順を実行します。
 - a. 実行時にNW Server上の次のログを監視します(たとえば、コマンドラインで`tail -f`コマンドを実行します)。


```

/var/netwitness/uax/logs/sa.log
/var/log/netwitness/orchestration-server/orchestration-server.log
/var/log/netwitness/deployment-upgrade/chef-solo.log
/var/log/netwitness/config-management/chef-solo.log
/var/lib/netwitness/config-management/cache/chef-stacktrace.out
          
```

 エラーはこれらのログの少なくとも1つに表示されます。
 - b. 問題を解決し、サービスを再インストールします。
 - 原因1: `nwsetup-tui`で`deploy_admin`の間違ったパスワードを入力しました。
解決策: `deploy_admin`のパスワードをリセットします。
 1. 11.xのNW Serverホストとそれ以外のすべてのホストで、次のコマンドを実行します。


```

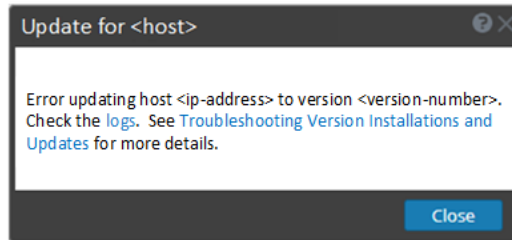
/opt/rsa/saTools/bin/set-deploy-admin-password
                  
```
 2. インストールまたはオーケストレーションに失敗したホスト上で、`nwsetup-tui`コマンドを実行し、[Deployment Password]のプロンプトが表示されたら、`deploy_admin`の新しいパスワードを入力します。
 - 原因2: `deploy_admin`のパスワードの有効期限が切れています。
解決策: `deploy_admin`のパスワードをリセットします。
 1. 11.xのNW Serverホストとそれ以外のすべてのホストで、次のコマンドを実行します。


```

/opt/rsa/saTools/bin/set-deploy-admin-password
                  
```
 2. インストールまたはオーケストレーションに失敗したホスト上で、`nwsetup-tui`コマンドを実行し、[Deployment Password]のプロンプトが表示されたら、`deploy_admin`の新しいパスワードを入力します。
3. それでも更新を適用できない場合は、ステップ2のログを収集して、カスタマ サポートにお

ホスト更新失敗エラー

エラーメッセージ



問題

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

解決策

1. ホストへのバージョン更新の適用を再試行します。
通常は、これで問題が解決されます。
2. それでも新しいバージョンに更新できない場合は、次の手順を実行してください。
 - a. 実行時にNW Server上の次のログを監視します(たとえば、コマンド ラインから `tail -f` コマンドを実行します)。


```

/var/netwitness/uax/logs/sa.log
/var/log/netwitness/orchestration-server/orchestration-server.log
/var/log/netwitness/deployment-upgrade/chef-solo.log
/var/log/netwitness/config-management/chef-solo.log
/var/lib/netwitness/config-management/cache/chef-stacktrace.out
          
```

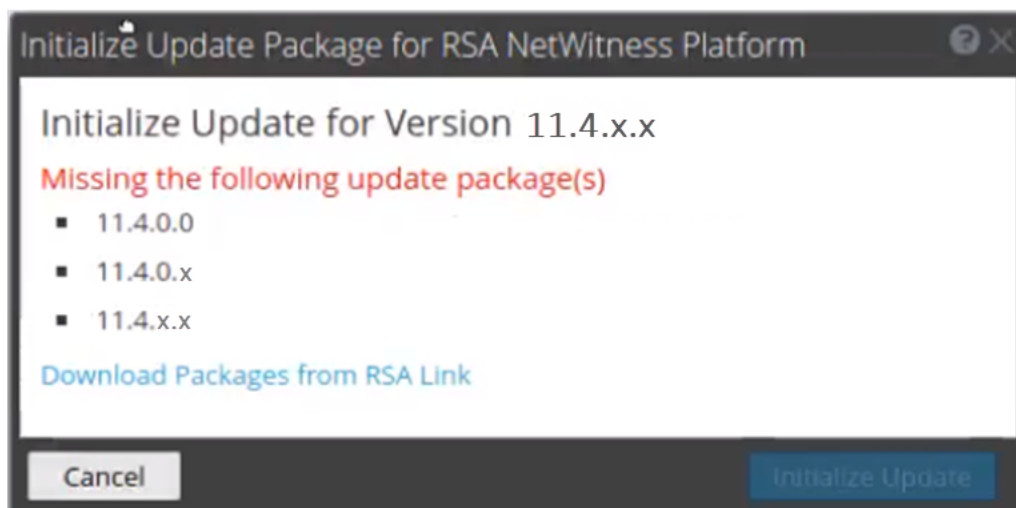
 エラーはこれらのログの少なくとも1つに表示されます。
 - b. その問題を解決して、バージョンの更新を再度実行してください。
 - 原因1: `deploy_admin` のパスワードの有効期限が切れています。
解決策: `deploy_admin` のパスワードをリセットします。
原因1を解決するには、次の手順を実行します。
 1. NetWitness Platformメニューで、[管理] > [セキュリティ] > [ユーザ] タブの順に選択します。
 2. `deploy_admin` を選択し、[パスワードのリセット] をクリックします。
 3. (オプション) [パスワードのリセット] ダイアログで有効期限が切れた `deploy_admin` のパスワードの再使用が拒否される場合は、次の手順を実行します。
 - a. `deploy_admin` のパスワードを新しいパスワードにリセットします。
 - b. 11.xのNW Server以外のすべてのホストで、次のコマンドを実行し、NW Serverと同じ `deploy_admin` のパスワードを指定します。

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```

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

更新パッケージ不足エラー

エラー
メッセージ

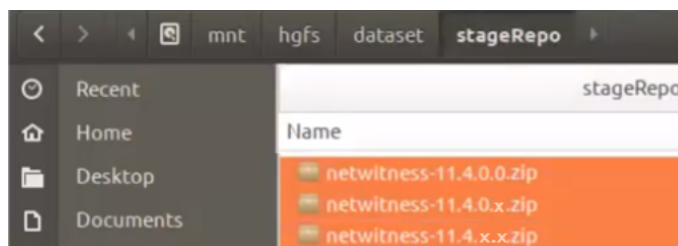


問題

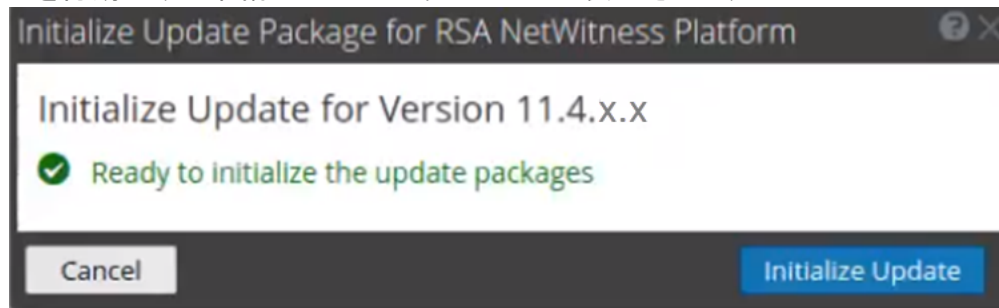
「次の更新 パッケージが見つかりません」は、[ホスト]ビューからオフラインでホストを更新する時に、ステージングフォルダに足りないパッケージがあると、[RSA NetWitness Platformの更新パッケージの初期化]ダイアログに表示されます。

解決
策

1. [RSA NetWitness Platformの更新パッケージの初期化]ダイアログで[RSA Linkからパッケージをダウンロード]をクリックします。
選択したバージョンの更新ファイルが含まれるRSA Linkページが表示されます。
2. ステージングフォルダに足りないパッケージを選択します(たとえば、11.4.0.0、11.4.0.x、11.4.x.x)。



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



OpenSSL 1.1.x

エラー メッ セー ジ	<p>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。</p> <pre>\$ ssh root@10.1.2.3 ssh_dispatch_run_fatal: Connection to 10.1.2.3 port 22: message authentication code incorrect</pre>
問題	<p>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。次に例を挙げます。</p> <pre>\$ rpm -q openssl openssl-1.1.1-8.el8.x86_64</pre>
解決 策	<p>互換性のある暗号リストをコマンドラインで指定します。次に例を挙げます。</p> <pre>\$ 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</pre>


NW Server以外へのパッチ適用エラー

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

決 策

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

コマンド ラインからの更新後のホスト再起動のエラー

エラー メッセージ	<p>ホストをオフラインで更新して再起動した後に、ホストを再起動するよう求めるメッセージがユーザ インタフェースに表示されます。</p> 
原因	<p>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。</p>
解決策	<p>ユーザ インタフェースの[ホスト]ビューでホストを再起動します。</p>

アップグレード後のReporting Engine再起動

問題	<p>11.2や11.3などの11.xのバージョンから11.4にアップグレードした後、Reporting Engine サービスが継続的に再起動を試み、失敗を繰り返す場合があります。</p>
原因	<p>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。</p>
解決策	<p>この問題を解決するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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。 <ul style="list-style-type: none"> <code>/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log</code> 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。 <pre>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!</pre> • アラート ステータスのdbファイルが破損している場合は、次のログが表示されます。

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

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

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

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

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

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

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

2. ライブ チャート データベース ファイルの破損を解決するには、次の手順を実行します。

- a. Reporting Engineサービスを停止します。
- b. livechart.mv.dbファイルを、/var/netwitness/reserver/rsa/soc/reporting-engine/livechartsフォルダから一時的な場所に移動します。
- c. Reporting Engineサービスを再起動します。

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

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

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

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

Log Collectorサービス(`nwlogcollector`)

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

エラー
メッセ

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

セー ジ	
原因	更新後、Log CollectorのLockboxを開くことができませんでした。
解決策	NetWitness Platformにログインし、LockboxのStable System Valueのパスワードをリセットすることにより、システムフィンガープリントをリセットします。詳細については、『ログ収集の構成ガイド』の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」セクションを参照してください。
エラー メッ セー ジ	<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found
原因	更新後、Log CollectorのLockboxが構成されていません。
解決策	Log CollectorのLockboxを使用する場合は、NetWitness Platformにログインし、Lockboxを構成します。詳細については、『ログ収集の構成ガイド』の「Lockboxのセキュリティ設定の構成」トピックを参照してください。

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

NW Server

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

問題	アップグレード後、監査ログが、グローバル監査に設定された宛先に転送されていないことが分かりました。 または 次のメッセージがsa.logに記録されました。 Syslog Configuration migration failed. Restart jetty service to fix this issue
原因	NW Serverのグローバル監査設定は、11.2.x.xまたは11.3.x.xから11.4.0.0への移行に失敗しました。
解決策	<ol style="list-style-type: none"> SSHでNW Serverに接続します。 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	<ol style="list-style-type: none"> 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。 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。
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"> 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。 <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> 3. 非NW Serverホストのアップグレードを再試行します。

Reporting Engineサービス

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

エラーメッセージ	<pre><timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [><existing-GB] is less than the required space [<required-GB>]</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。

