

# NetWitness<sup>®</sup> Platform

バージョン12.5

## アップグレード ガイド

## 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/en-us/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。

サードパーティのリポジトリを展開したり、サポートされているNetWitnessバージョンに含まれない基盤となるNetWitnessオペレーティングシステムに変更を加えたりしないことをお勧めします。NetWitnessが承認したイメージ以外でのこのような変更は、サービスまたは機能の競合を引き起こす可能性があり、NetWitnessを最適化された機能状態に戻すにはNetWitnessシステムの再イメージ化が必要になる場合があります。サードパーティのリポジトリが展開された場合、またはNetWitnessの承認なしに顧客がサポートされていない変更を行った場合、トラブルシューティングの取り組みまたはサービスの再イメージ化によって問題が解決されるまで、システムの誤動作については顧客が全責任を負います。

## 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。

## その他

この製品、このソフトウェア、関連ドキュメント、およびそのコンテンツは、このドキュメントの発行日時点で有効なNetWitnessの標準利用規約に従うものとし、これらの利用規約は<https://www.netwitness.com/standard-form-agreements/>で確認できます。

© 2024 RSA Security LLC or its affiliates.All Rights Reserved.

2024年9月

# 目次

<b>NetWitness Platformのアップグレード</b> .....	<b>6</b>
12.5でサポートされているアップグレード パス .....	7
Azure向けNetWitnessアップグレード ガイドライン .....	8
混在モード環境での実行 .....	8
ESAホストのアップグレードに関する考慮事項 .....	8
Legacy Windows Collectorの更新またはインストール .....	9
用語 .....	10
<b>アップグレード前チェックの実行</b> .....	<b>11</b>
OS移行チェックリスト .....	11
アップグレード チェックリスト .....	12
ネットワークチェックリスト .....	14
証明書チェックリスト .....	14
<b>NetWitness Platformのアップグレード準備</b> .....	<b>16</b>
タスク1 (重要) AlmaLinux OSのアップグレードの準備をする .....	16
サポートされていないファイル システム .....	16
BTRFSのアンマウントと削除 .....	16
NFSのアンマウント .....	16
AVX/VMX CPU命令セット チェック .....	17
PF_RINGからDPDKへの移行のサポート .....	17
タスク2 (推奨、ただしオプション) レガシー パッケージ リポジトリを削除する .....	17
タスク3. 12.5 への移行に向けて ESA 展開を準備する .....	18
ESA導入環境とデータソースの管理 .....	18
タスク4. サードパーティ パッケージの削除 .....	20
タスク5. シングル サインオン (SSO):Microsoft Azure ADFSでSAML応答署名を有効にする .....	20
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 .....	20
タスク7 (オプション) Liveサーバーの接続を確認する .....	21
タスク8. コンポーネント ホストの時刻を NW サーバー ホストと同期する .....	21
<b>アップグレード タスクの実行</b> .....	<b>22</b>
アップグレード オプションの選択 .....	23
オプション1 :Liveサービスを使用したNetWitness Platformのアップグレード .....	23
オプション2 :NetWitness Platform Offlineのアップグレード .....	24
タスク1 :ステージング フォルダ(/var/netwitness/common/update-stage/)にバージョン アップグレード ファイルを配置する。次の操作を実行します。 .....	24
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。次の操作を実行します。 .....	25
オプション3 :CLIを使用したNetWitness Platformのアップグレード(オフライン) .....	26
CLIによるアップグレードのための外部リポジトリの準備 .....	28

オプション4( オプション) :パッケージのダウンロードによるアップグレード リポジトリの事前設定	30
<b>アップグレード後のタスクの実行</b>	<b>32</b>
全般	32
Jettyの構成	32
サービスの再起動、データ収集、データ集計の確認	32
コア サービス コンテンツの復元	33
Event Stream Analysis( ESA)	34
ESA導入環境とデータソースの管理	35
通知用のカスタムスクリプトを移行する	36
対応	36
( オプション) custom_normalize_alerts.jsでRespondサービスのカスタム キーをリストアし、新しいデータソースをサポート	37
User and Entity Behavior Analytics	37
Legacy Windows Log Collector	39
更新されたSA証明書でLegacy Windows Log Collectorの証明書を更新する	39
Warehouse Connector	40
ロックボックスの回復パスワードの設定	40
<b>アップグレード後に検証チェックを実行する</b>	<b>42</b>
<b>12.5リレーサーバーをインストールする</b>	<b>44</b>
Endpointエージェントのアップグレード	44
<b>アップグレードの問題のトラブルシューティング</b>	<b>45</b>
AlmaLinux OSのトラブルシューティング情報	46
管理サーバー、Reporting Engine、SMSでのLockboxからSecureStoreへの移行の失敗	48
deploy_adminのユーザー パスワード有効期限切れエラー	50
ダウンロード エラー	51
バージョン<version-number>の導入エラー :更新パッケージの不足	52
外部リポジトリ更新エラー	52
ホスト更新失敗エラー	53
更新パッケージ不足エラー	54
NW Server以外へのパッチ適用エラー	54
コマンド ラインからの更新後のホスト再起動エラー	55
Log Collectorサービス(nwlogcollector)	55
NW Server	56
Orchestration	57
Reporting Engineサービス	58
Event Stream Analysis	58
Legacy Windows Log Collector	59
ESAトラブルシューティング情報	59
ESARルールがアラートを作成しない	59
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	60

<b>NetWitnessコミュニティ ポータルを使用したサポート</b> .....	<b>62</b>
セルフ ヘルプ リソース .....	62
カスタマー サポート へのお問い合わせ .....	62
製品ドキュメント へのフィードバック .....	63

## NetWitness Platformのアップグレード

このドキュメントでは、NetWitness Platformを12.5にアップグレードする利点とプロセスについて説明します。NetWitness Platformをアップグレードする前に、前提条を満たしていることを確認し、アップグレード前タスクを実行してください。インターネット接続に応じて、4つの異なるオプションを使用してNetWitness Platformをアップグレードできます。アップグレードプロセスを正常に完了するには、このガイドに記載されている特定のアップグレード後タスクとアップグレード後検証チェックもアップグレードの後で実行する必要があります。このドキュメント内の手順は、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。

**重要** NetWitnessは、バージョン12.2までが2024年3月31日をもってサポート終了 (EOL) に達したことを指摘し、ユーザーにソフトウェアバージョンを確認するようアドバイスしています。詳細については、<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。最新の機能とセキュリティ更新を活用するには、NetWitnessではバージョン12.5にアップグレードすることをお勧めします。

**重要** NetWitnessでは、UEBAサーバーを12.5バージョンにアップグレードする前に、schemas.jsonファイルのバックアップを取ることを強くお勧めします。このファイルは次の場所にあります。  
`/var/netwitness/presidio/asl/adaptor-config/schema-query/schemas.json`

**重要** バージョン12.5以降では、UEBAはアプリケーションルールでデフォルトで有効になっています。つまり、12.5の新規インストールで展開されたデコーダーには、必要なUEBA関連のアプリケーションルールが自動的に含まれることとなります。すでに古いバージョンでアプリケーションルールを使用していて、12.5にアップグレードした場合、それらのルールは変更なしで引き続き機能します。ただし、NetWitnessでは、アプリケーションルールを使用するために、NetWitness Liveの新しいUEBAバンドルをデコーダーに展開することを強くお勧めします。これにより、UEBAが適切に機能するために必要な最新のアプリケーションルールがすべて揃います。デコーダーへのUEBAバンドルの導入の詳細については、『NetWitness 12.5 Liveサービスガイド』のトピック「[Liveリソースの検索と導入](#)」を参照してください。

**UEBA関連のアプリケーションルールを導入するためのバンドル名：**

- NetWitness UEBA Authentication Operations
- NetWitness UEBA Registry Operations
- NetWitness UEBA Active Directory Operations
- NetWitness UEBA Process Operations
- NetWitness UEBA File Operations
- NetWitness UEBA Windows Kerberos Service Request
- NetWitness UEBA Network TLS Outbound Connections

**重要** NetWitness 12.4以降のバージョン (AlmaLinux) では、数値のユーザー名はサポートされていません。これは、ユーザー名が数字のみで構成されているPam Securidユーザーは、バージョン12.5へのアップグレード後にグループに追加できなくなることを意味します。この制限の詳細については、<https://www.webconn.tech/kb/are-all-numeric-usernames-allowed-in-almalinux-8>を参照してください。

**重要** :バージョン12.3.1以前の search.ini ファイルを使用して作成したカスタム検索パターンは、バージョン12.5以降で使用される新しい search.xml ファイル形式に移行されません。そのため、バージョン12.5以降にアップグレードすると、これらのカスタム検索パターンは使用できなくなります。

新しいバージョンでこれらのカスタム検索パターンを再作成するには、手動で再度構成する必要があります。これを行うには、次の2通りの方法があります。

- [Investigate] > [イベント]ビューに移動し、検索パターン ルールを作成して、Packet Decoderを含むポリシーに展開します。

- [コンテンツライブラリ] > [詳細] > [検索パターンルール]タブに移動し、ルールを作成します。検索パターンルールの作成の詳細な手順については、『Investigateユーザーガイド』の「[イベント]ビューでのイベントの分析」トピックの「[テキスト]タブで検索パターンを作成する」セクション、または『NetWitnessコンテンツ元管理ガイド』の「検索パターンルールの管理」トピックを参照してください。

**注** :NetWitness Platformでは、環境内に複数のUEBAサーバーをインストールできるようになりました。詳細については、『NetWitness UEBA構成ガイド』のトピック「複数のUEBAサーバーの構成」を参照してください。

**注** :NetWitness 12.5以降では、NetWitness Platformを初めてインストールするユーザーにとって、ホームページがデフォルトのランディング ページになります。既存のユーザーの場合、Springboardは引き続きデフォルトのランディング ページになります。ただし、Springboard機能は将来のリリースでは廃止され、ホームページがデフォルトのランディング ページになります。詳細については、『NetWitness 12.5入門ガイド』の「スプリングボードの管理」トピックを参照してください。

12.5にアップグレードすると、有効にできる魅力的な新機能が多数あります。このリリースの新機能の詳細については、*NetWitness Platform 12.5のリリースノート*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。以前のリリースで公開された新機能の詳細については、<https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-x-to-12-x/ta-p/695650>を参照してください。

## 12.5でサポートされているアップグレード パス

NetWitness 12.5では次のアップグレード パスがサポートされています。

- NetWitness 12.4.2.0から12.5
- NetWitness 12.4.1.0から12.5
- NetWitness 12.4.0.0から12.5
- NetWitness 12.3.1.0から12.5
- NetWitness 12.3.0.0から12.5
- NetWitness 12.2.0.1から12.5
- NetWitness 12.2.0.0から12.5

## Azure向けNetWitnessアップグレード ガイドライン

Azureインストールガイドに記載された標準構成に従う場合は、Azure VMでのインプレース アップグレードがサポートされます。ユーザーは、Azureコントロールプレーンに関連する構成など、AzureサブスクリプションレベルのVMポリシーがVMのオペレーティングシステムに干渉しないようにする責任があります。

Azureインストールガイドに正しく従えば、警告が表示されることなくスムーズにアップグレードプロセスが進むはずです。ただし、これらのガイドラインから逸脱したり、Azureコントロールプレーンに関連する構成などを追加したりすると、次に示すようにエラーが発生する可能性があります。

### 混在モード環境での実行

NetWitness Platformは、アップグレード時に混在モードをサポートします。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した状態を指します。

詳細については、『[NetWitness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。

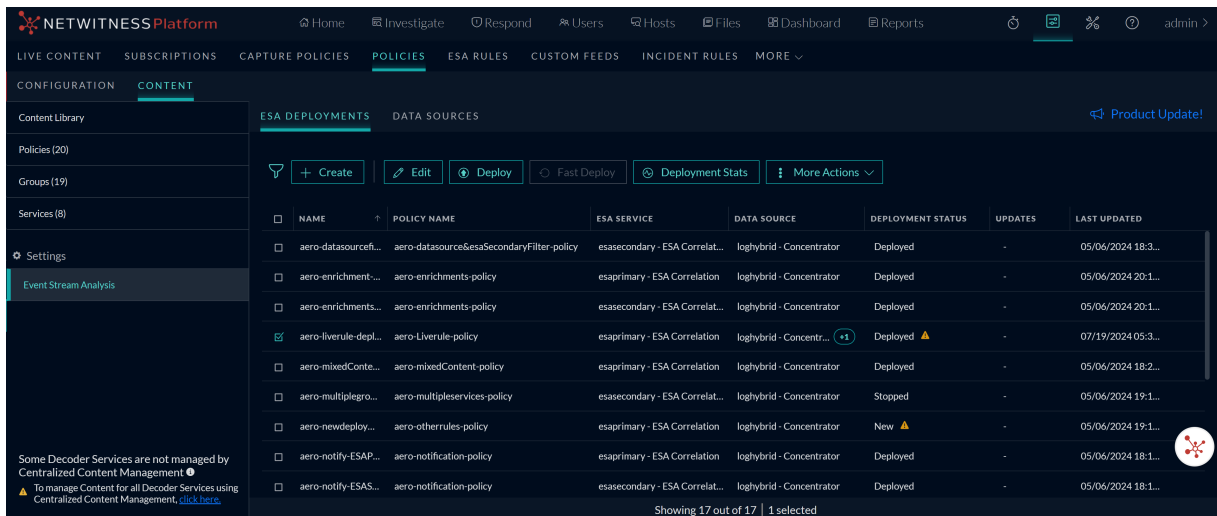
#### 注：

- 環境内のすべてのホストのアップグレードに時間がかかる場合は、問題の発生を避けるためにNetWitnessサポートにお問い合わせください。
- Endpoint Log Hybrid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。
- 混在モードは、NetWitness PlatformのESAホストではサポートされていません。

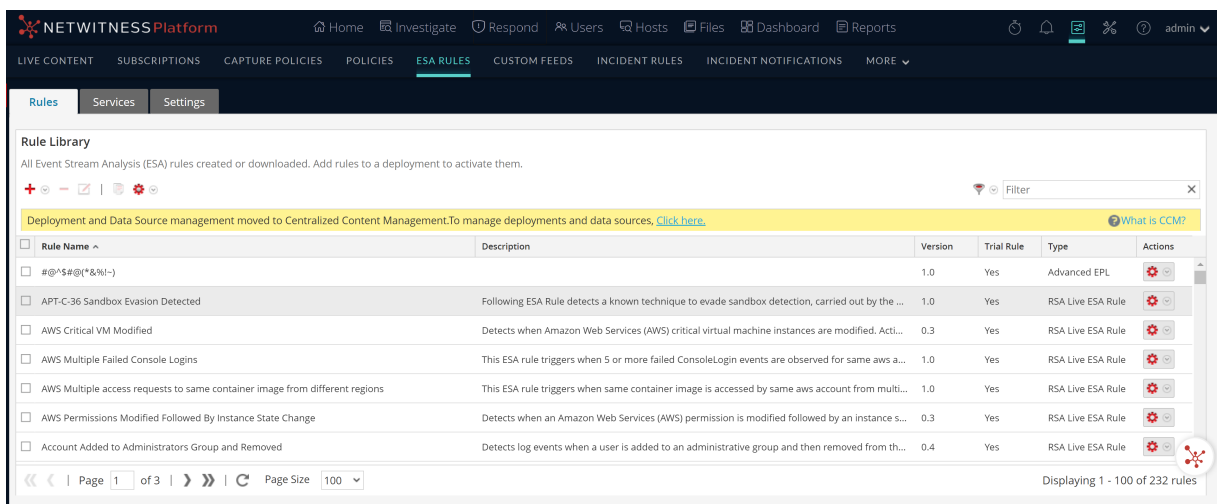
### ESAホストのアップグレードに関する考慮事項

**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。

- ESA導入環境とデータソースは**コンテンツ元管理**でのみ管理できます。[構成] > [ポリシー] > [コンテンツ] > [Event Stream Analysis] ページに移動し、ESA導入環境とデータソースを管理します。次の図を参考にしてください。



- ESAルールは、[ESAルール] ページでのみ管理できます。次の図を参考にしてください。



- 12.5バージョンにアップグレードすると、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。各展開はポリシーとグループに変換され、関連サーバーを12.5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。Admin Serverが完了した直後に関連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。対応する関連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。ただし、Correlationサーバーは引き続きアラートとイベントの処理を続けます。
- 管理サーバーのアップグレード後は、ESAホストを速やかにアップグレードする必要があります。  
コンテンツ元管理と導入管理の詳細については、『NetWitnessコンテンツ元管理ガイド』を参照してください。

## Legacy Windows Collectorの更新またはインストール

NetWitness Legacy Windows収集のアップグレードおよびインストール手順については、『Windows Legacy収集ガイド (NetWitness)』を参照してください。

**注** :Windows Legacy Collectorのアップグレードまたはインストールの後、正常にログを収集できるように、システムを再起動してください。

## 用語

名前	説明
AVX	Advanced Vector Extensions
VMX	Virtual Machine Extension
NFS	Network File System
BTRFS	B-Tree File System
DPDK	Data Plane Development Kit

## アップグレード前チェックの実行

NetWitness Platform 12.5にアップグレードする前にpre-upgrade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ことを強くお勧めします。

**注：**

- deploy\_adminパスワードが有効かつ最新であることを確認します。UIから変更しないでください。  
<https://community.netwitness.com/t5/netwitness-platform-online/manage-the-deploy-admin-account/ta-p/669802>を使用してパスワードを変更します。  
- pre-upgradeのチェックを実行したときにプローブが失敗した場合は、  
<https://community.netwitness.com/t5/netwitness-knowledge-base/netwitness-pre-upgrade-check-known-issues-master-list/ta-p/708695>を参照して、失敗したプローブに関連する問題を軽減してください。

### 開始する前に

まず<https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-platform-standalone-precheck-tool/ta-p/709096>を使用してスタンドアロンRPMをダウンロードし、スタンドアロンRPMのインストール手順についてRead Meファイルを参照して、事前チェックを実行する必要があります。

### pre-upgradeのチェックを実行するには

1. 管理サーバーにSSHで接続します。
2. アップグレード事前チェック ツールを使用して、次のコマンドを順番に実行します。
  - a. `nw-precheck-tool-standalone os-migration-checklist`:このコマンドを使用すると、アップグレード事前チェック ツールが[OS移行チェックリスト](#)内のプローブのリストに対して検証チェックを実行できるようになります。
  - b. `nw-precheck-tool-standalone upgrade-checklist`:このコマンドを使用すると、アップグレード事前チェック ツールが[アップグレード チェックリスト](#)内のプローブのリストに対して検証チェックを実行できるようになります。
  - c. `nw-precheck-tool-standalone network-checklist`:このコマンドを使用すると、アップグレード事前チェック ツールが[ネット ワークチェックリスト](#)内のプローブのリストに対して検証チェックを実行できるようになります。
  - d. `nw-precheck-tool-standalone cert-checklist`:このコマンドにより、アップグレード事前チェック ツールは、[証明書チェックリスト](#)内のプローブのリストの検証チェックを実行できます。

## OS移行チェックリスト

アップグレード事前チェック ツールは、OS移行チェックリストの次のプローブリストの検証チェックを実行します。

- **バージョン チェック プローブ** :システムのNetWitnessバージョンが最新バージョン(12.2.0.0)であるかどうかを確認します。
- **AVX/VMXプローブ** :AVX/VMXフラグが必要なノードで有効かどうかを確認します。

- **NFSマウント プローブ** :NFSタイプのマウント ポイントがいずれかのノードでアクティブかどうかを確認します。
- **複数のkernel-develパッケージ プローブ** :DecoderとPacket Hybridにkernel-develパッケージの複数のバージョンがあるかどうかを確認します。
- **PFリング キャプチャ デバイス プローブ** :Decoder上のPF ringキャプチャ デバイスをチェックし、PF\_ringキャプチャ デバイスをDPDKキャプチャ デバイスに変更するように警告を出します。
- **BTRFSマウント プローブ** :BTRFSパーティションがマウントされているかどうかを確認します。

**注** :LEAPPとAlma OSはBTRFSパーティションをサポートしていません。

- **ディスク領域 チェック** :各ノードのパーティションに十分なディスクの空きがあることを確認します。
- **Fipsモード チェック** :すべてのノードでFipsモードが無効になっている(falseに設定されている)ことを確認します。
- **マウントチェック プローブ** :すべてのパーティションまたはファイル ディレクトリーが正しくマウントされているかどうかを確認します。
- **ソルト マスター通信 チェック** :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。
- **CIFSチェックプローブ**:インプレース アップグレードがサポートされていないホスト上のCIFSファイルシステムを識別します。
- **XFS Ftypeチェックプローブ**:ホスト上にftypeが0に設定されているXFSファイルシステムがあるかどうかを確認します。
- **CCMカスタム コンテンツ チェック プローブ**:.envision ファイルが適切な場所に抽出されているかどうかを確認します。
- **光学ドライブチェックプローブ**:ハードウェア デバイスに光学デバイスがマウントされているかどうかを確認します。光学デバイスが検出されると、プローブがユーザーにアンマウントを促します。

## アップグレード チェックリスト

アップグレード事前チェック ツールは、アップグレード チェックリスト内の次のプローブ リストに対して検証チェックを実行します。

- **セキュリティクライアント ファイル チェック** :security-client-amqp.yml ファイルが存在しないことを確認します。
- **Node-0 NW Service-idステータス チェック** :ノード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します。
- **Brokerサービストラストピア シンボリックリンク ファイル チェック** :Brokerサービストラストピア 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。
- **Node-0 NWサービス ステータス チェック** :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。

- **Node-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 チェック** :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。
- **Node-0証明書 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 チェック** :すべてのノードX上の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メモリー情報の提供** :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。
- **(管理サーバー)ノード0ファイルシステム使用率 チェック** :ノード0上の /var/netwitness/mongo、/var/netwitness、rootのディスク パーティションの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 チェック** :ノードX上のESAプライマリー サービスおよびエンドポイント ログ ハイブリッド サービスの /var/netwitness/mongo、/var/netwitness、rootのディスク パーティションの使用率を確認します。
- **Mongoファイル(ESAPrimary) 権限モード チェック** :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ファイルの権限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 チェック** :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。
- **(管理サーバー)ノード0初期ステータス チェック** :初期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。
- **Node-X RPM DBインデックス チェック** :Node-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。
- **Node-Z Yumプロキシ チェック** :yum.confファイルの存在と、Node-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。
- **Node-X Yumプロキシ チェック** :yum.confファイルの存在と、Node-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。
- **Node-Z暗号チェックプローブ** :必要な暗号がNode-0上の場所 /etc/rabbitmq/rabbitmq.configで使用可能かどうかを確認します。
- **Node-X暗号チェックプローブ** :必要な暗号がすべてのNode-X上の場所 /etc/rabbitmq/rabbitmq.configで使用可能かどうかを確認します。
- **Node-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Node-Xのハードウェアバージョンを確認します。
- **Node-Zハードウェアバージョンチェックプローブ** :管理サーバーのハードウェアバージョンを確認します。
- **PuppetCA証明書チェックプローブ** :古いPuppet CA証明書が /etc/pki/nw/trust/truststore.pemに存在するかどうかを確認します。
- **AdminCertCheckプローブ** :すべてのノードの管理証明書が管理サーバー上の管理証明書と同じであるかどうかを確認します。
- **NTPプローブ** :すべてのノードをチェックして、NTPサーバーと同期していることを確認します。
- **StaleCertsチェックプローブ** :mongoをチェックし、その中に未使用の古い証明書がある場合に警告します。
- **NodeCertIDCheckプローブ** :ノード証明書の件名フィールドをチェックし、ホストのノードIDと同じであることを確認します。
- **Deploy Admin/パスワード有効期限チェックプローブ** :Node-0でdeploy\_admin/パスワードの有効期限が切れているかどうかを確認します。
- **ファイル/フォルダ権限チェック** :ファイル/フォルダに適切な権限があるかどうかを確認します。

## ネットワークチェックリスト

アップグレード事前チェックツールは、ネットワークチェックリスト内の次のプローブリストに対して検証チェックを実行します。

- **(管理サーバー) ノード0クローズドポートチェック** :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クローズドポートチェック** :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

アップグレード事前チェックツールは、証明書チェックリスト内の次のプローブリストに対して検証チェックを実行します。

- **ノード0サービス証明書有効性チェック** :Node-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サービス証明書有効性チェック** :Node-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。
- **Node-0ノード証明書有効性チェック** :Node-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。
- **Node-Xノード証明書有効性チェック** :Node-X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証明書有効性チェック** :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。

## NetWitness Platformのアップグレード準備

NetWitness Platform 12.5 へのアップグレードを準備するには、次のタスクを完了します。

### タスク1 :(重要) AlmaLinux OSのアップグレードの準備をする

#### サポートされていないファイルシステム

##### BTRFSのアンマウントと削除

BTRFSは、フォールトトレランス、修復、簡単な管理に重点を置きながら、高度なファイルシステム機能を実装することを目的としたLinux用の書き込み時コピー (CoW) ファイルシステムです。BTRFSファイルシステムはRed Hat Enterprise Linux 8から非推奨となり、AlmaLinux OSはBTRFSファイルシステムをサポートしていません。NetWitnessはデフォルトではBTRFSを使用しませんが、ネットワーク デコーダ、ネットワーク ハイブリッドなどの一部の 카테고리では、BTRFSモジュールが存在し、ロードされます。BTRFSがファイルシステムとしてマウントされている場合は、以下の手順を実行してBTRFSパーティションを手動でアンマウントします(BTRFSがマウントされていない場合は、以下の手順をスキップしてください)。

- a. データを再配置します。
- b. 次のコマンドを使用して、BTRFSパーティションをアンマウントします。  
`umount <btrfsパーティションパス>`。btrfsパーティション情報は `/etc/fstab` or `df -hT`コマンドから取得できます。
- c. BTRFSパーティションを`/etc/fstab`から削除します。
- d. `lsmod | grep btrfs`を使用してカーネルモジュールがまだロードされているかどうかを確認します。カーネルモジュールがまだロードされている場合は、`modprobe -r btrfs`を使用してbtrfsカーネルモジュールをアンロードします。
- e. アップグレードをトリガー/再トリガーします。

詳細については、KB記事「[BTRFSがマウントまたはロードされている場合にアップグレードが失敗し、パーティション内のデータが失われたかを確認する方法](#)」を参照してください。

##### NFSのアンマウント

ノード上でNFSタイプのファイルシステムがアクティブであると、ノードのアップグレードが失敗します。これらのマウントポイントが見つかった各ノードのCLIから手動でマウントポイントをアンマウントする必要があります。NFS手動でアンマウントするには、以下の手順を実行します。

- a. NFSマウントポイントが検出されたノードにSSHで接続します。
- b. 各ノードで`mount | grep 'type nfs'`を実行し、NFSマウントポイントのディレクトリーパスを取得します。

**注** :NFSをアンマウントする前に、NFSに依存しているNetWitnessサービスを停止する必要があります。

以下に例を示します。ArchiverおよびWarehouse ConnectorサービスがNFS上で実行されている場合は、NFSをアンマウントする前に次のコマンドを実行してサービスを停止する必要があります。

```
systemctl stop nwarchiver
systemctl stop nwarehouseconnector
```

- c. ターミナルから「umount <dir\_path>」を実行します。ここで、<dir\_path>はステップbのディレクトリーパスです。
- d. 選択したエディターで /etc/fstabファイルを開き、NFSマウント ポイントに関連する行をコメントアウトします。
- e. NetWitnessのアップグレードを実行します。
- f. アップグレードが正常に完了したら、/etc/fstabの各エントリーのコメントを解除し、ターミナルから mount -aを実行してNFSマウント ポイントを追加し直します。

## AVX/VMX CPU命令セット チェック

NetWitness Platform 12.5 では AVX/VMX CPU フラグを有効にする必要があります。次のコマンドを実行します。

```
salt '*' cmd.run "lscpu | grep -E 'avx|vmx'"
```

AVX/VMX CPU 命令セットが有効になっているかどうかを確認します。詳細については、KB記事「[NetWitness MongoDB 5.0はmongod.mongosおよび従来のmongoシェルでAVX命令セットを使用](#)」を参照してください。

**注** :NetWitnessハードウェア アプライアンスの場合、AVX/VMX CPU命令セットはデフォルトで有効になっています。

## PF\_RINGからDPDKへの移行のサポート

お客様がPF\_RINGキャプチャ(CentOS)を使用し、12.5 (AlmaLinux)に直接アップグレードする場合、Decoderキャプチャ設定は無効になります。まず、PF\_RINGデバイスをDPDKに移行してからアップグレードする必要があります。

移行手順については、「[PF\\_RINGデバイスをDPDKに移行する](#)」を参照してください。

## タスク2 : (推奨、ただしオプション) レガシー パッケージ リポジトリを削除する

以前のリリースから古いリポジトリを削除することで、ディスク領域を解放できます。

### 古いリポジトリを削除するには

1. NetWitness Repoツールを使用して、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。次の手順を実行します。
  - rootユーザーとして管理サーバーにSSHで接続します。
  - 次のコマンドを実行します。

```
nw-repo-tool --list-obsolete
```

このコマンドを実行すると、使われなくなったすべてのリポジトリのリストが取得されます。

2. 次のコマンドを実行して、使われなくなったリポジトリをすべて削除します。

```
nw-repo-tool --purge-obsolete
```

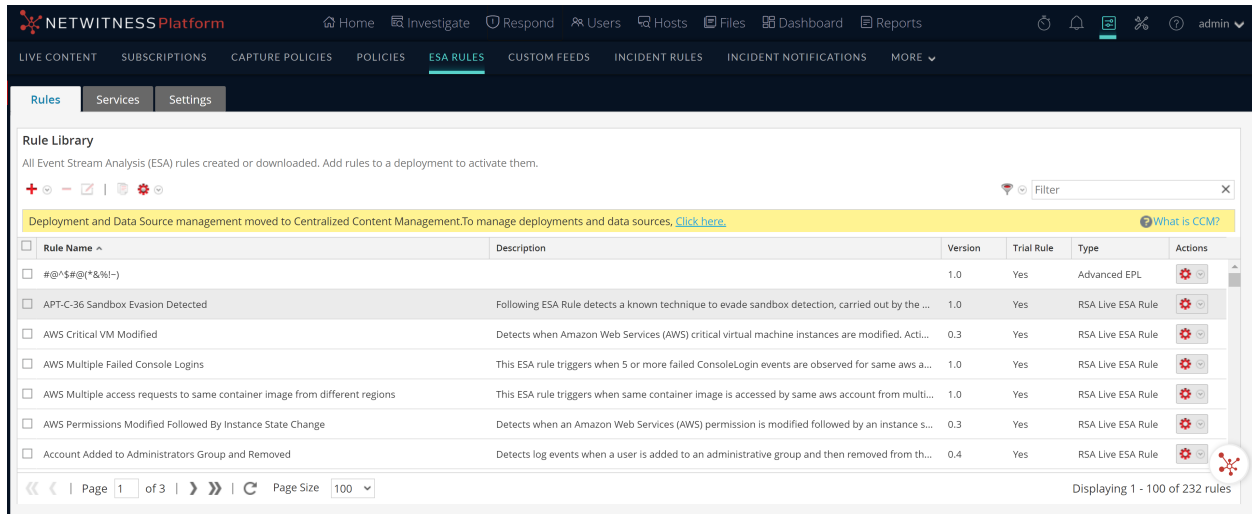
## タスク 3. 12.5 への移行に向けて ESA 展開を準備する

NetWitness では、12.5 にアップグレードする前に、すべての ESA 展開でエラーのない状態を維持することを推奨しています。ESA デプロイメントは 12.5 にアップグレードした後にポリシーとグループに移行されるため、使用されていない ESA デプロイメントを削除する必要があります。各展開はポリシーとグループに変換され、関連サーバーを 12.5 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。

### ESA導入環境とデータソースの管理

ESA導入環境とデータソースはコンテンツ元管理でのみ管理できます。[構成] > [ポリシー] > [コンテンツ] > [Event Stream Analysis] ページに移動し、ESA導入環境とデータソースを管理します。ESAルールは、[ESAルール] ページでのみ管理できます。次の図を参考にしてください。

NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
aero-datasourcef...	aero-datasourceSesaSecondaryFilter-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Deployed	-	05/06/2024 18:3...
aero-enrichment ...	aero-enrichments-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	-	05/06/2024 20:1...
aero-enrichments...	aero-enrichments-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Deployed	-	05/06/2024 20:1...
aero-liverule-depl...	aero-Liverule-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	+	07/19/2024 05:3...
aero-mixedConte...	aero-mixedContent-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	-	05/06/2024 18:2...
aero-multiplegro...	aero-multipleservices-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Stopped	-	05/06/2024 19:1...
aero-newdeploy...	aero-otherrules-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	New	▲	05/06/2024 19:1...
aero-notify-ESAP...	aero-notification-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	-	05/06/2024 18:1...
aero-notify-ESAS...	aero-notification-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Deployed	-	05/06/2024 18:1...



Admin Serverが完了した直後に関連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。対応する関連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。ただし、Correlationサーバーは引き続きアラートとイベントの処理を続けます。管理サーバーのアップグレード後は、ESAホストを速やかにアップグレードする必要があります。

コンテンツ元管理と導入管理の詳細については、『NetWitnessコンテンツ元管理ガイド』を参照してください。

**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は、欠落しているルールとエンリッチメントをアップグレード前に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することをお勧めします。不要な、または未使用のESA導入環境は削除する必要があります。

## タスク 4. サードパーティパッケージの削除

NetWitness リポジトリからホストにインストールされたサードパーティパッケージは、OS 移行の一環として、アップグレードの依存関係に基づいて削除されます。

## タスク 5. シングルサインオン (SSO):Microsoft Azure ADFSで SAML応答署名を有効にする

次の構成は、Microsoft Azure ADFSからのSAML応答が署名されずに暗号化されただけである場合にのみ適用されます。Microsoft Azure ADFSがSAML応答に署名して暗号化するようにすでに構成されている場合は、この構成を無視してアップグレード プロセスを続行できます。

SAML応答に署名していない場合は、NetWitness Platformをバージョン12.5にアップグレードしてシングルサインオン(SSO)ログインを成功させるには、SAML応答を暗号化して署名するようにMicrosoft Azure ADFSを構成しておいてください。Active Directoryフェデレーション サービス(AD FS) で応答署名を有効にするには、*powershell*で次のコマンドを実行します。

```
Set-AdfsRelyingPartyTrust -TargetName <<relying-party-name>> -
SamlResponseSignature MessageAndAssertion
```

**重要** :NetWitness Platform のバージョン 12.5 にアップグレードする前に、SAML 応答に署名するように Microsoft Azure ADFS を構成する必要があります。これらの要件を満たさない場合、SSOを使用してログインできない可能性があります。

## 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

**注** :このオプションのタスクは、NetWitness PlatformをLive経由でアップグレードする場合にのみ適用されます。

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。

## タスク 8. コンポーネント ホストの時刻を NW サーバー 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。

NTP 時刻同期方法は、NetWitness Platform のバージョンによって異なります。

- NetWitnessバージョン12.4より前の場合 :時刻同期には ntpd を使用します。
- NetWitness バージョン 12.4 以降の場合 :時刻同期にはchronyを使用します。

時刻を同期するには、次のいずれかを実行します。

1. NTPサーバーを構成します。

詳細については、『システム構成ガイド』のトピック「NTPサーバーの構成」を参照してください。

2. 次の手順を実行します。

- a. SSHで管理サーバーのホストに接続します。
- b. NetWitness のバージョンに応じて、次のコマンドを実行します。
  - NetWitnessのバージョンが12.4未満の場合。次のステップを実行します。

**重要** :正しい時刻同期を確実に行うには、node0でntpdが実行されている必要があります。node0でntpdをシャットダウンすると、他のノードでのntpdateコマンドが失敗します。

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

- NetWitnessバージョンが12.4以降の場合。次のステップを実行します。

- salt \\* service.stop chronyd
- salt \\* cmd.run "chronyc makestep"
- salt \\* service.start chronyd

## アップグレード タスクの実行

**重要** NetWitnessでは、NetWitness Platform 12.5にアップグレードする前に、pre-upgradeチェックを実行することを強くお勧めします。pre-upgradeのチェックを実行する方法の詳細については、「[アップグレード前チェックの実行](#)」

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. スタンドアロンBrokerホスト
6. Concentratorホスト
7. Archiverホスト
8. Packet Decoderホスト
9. Log Decoderホスト
10. Log Collector/VLCホスト
11. 残りのコンポーネント ホスト

**重要** 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。Admin Serverが完了した直後に関連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、「[NetWitness Platformのアップグレード準備](#)」の「**タスク 3 :12.5.0.0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。混在モードは、NetWitness Platform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。

NetWitnessのすべてのホストタイプについては、『[NetWitness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。

**重要** NW Server( Respond Serverサービスを含む) をアップグレードした後、ESAプライマリホストを同じバージョンにアップグレードするまでは、Respond Serverサービスが自動的に再び有効になりません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

**注** 従来のWindowsログコレクターを備えた12.5.0.0バージョンの場合、アップグレード後にいくつかの追加タスクを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実行](#)」の「Legacy Windowsログ収集」を参照してください。

## アップグレード オプションの選択

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 オプションのいずれかを選択します。アップグレード方式は、NetWitness Platformが推奨する順に記載されています。

- [オプション1 :Liveサービスを使用したNetWitness Platformのアップグレード](#)
- [オプション2 :NetWitness Platform Offlineのアップグレード](#)
- [オプション3 :CLIを使用したNetWitness Platformのアップグレード\(オフライン\)](#)
- [オプション4\(オプション\) :パッケージのダウンロードによるアップグレード リポジトリの事前設定](#)

4つのうちの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。

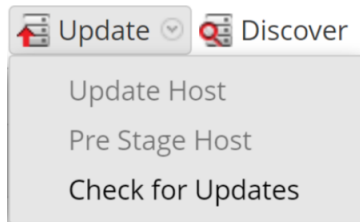
- 最初にNW Serverホストをアップグレードする必要があります。
- 既存のホストのバージョンと互換性のあるバージョンのみ適用できます。
- NetWitness Server、ESAプライマリホスト、ESAセカンダリホストがすべて、同じNetWitness Platformバージョンである必要があります。

## オプション1 :Liveサービスを使用したNetWitness Platformのアップグレード

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

**注意** :約 11.7 GBのアップグレード パッケージをダウンロードする前に、ネットワーク ポリシーを確認する必要があります。10 GBを超えるファイルのダウンロードを禁止するポリシーが設定されている場合、アップグレード パッケージのダウンロードは失敗します。


**注** :ホストの事前設定]機能を使用してアップグレード リポジトリを事前設定できます。次の図を参考にしてください。詳細については、「[オプション4\(オプション\) :パッケージのダウンロードによるアップグレード リポジトリの事前設定](#)」を参照してください。

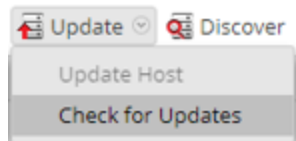


### 前提条件

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12.5.0.0が表示されることを確認します。

12.2.0.0、12.2.0.1、12.3.0.0、12.3.1.0、12.4.0.0、12.4.1.0、12.4.2.0から12.5.0.0にアップグレードするには、以下の手順を実行します。


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確認してください。



選択したホストのバージョン更新がローカルの更新リポジトリにある場合は、[ステータス]列に **更新あり**が表示されます。

4. **更新のバージョン**列で **[2.5.0.0]**を選択します。

**注：**

- アップグレードの主な機能と更新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。

5. ツールバーの **更新** > **ホストの更新**をクリックします。
6. **更新を開始**をクリックします。
7. **ホストの再起動**をクリックします。
8. 他のホストについても、ステップ5～7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 :NetWitness Platform Offlineのアップグレード

次のタスクを実行して、NetWitness Platformを手動でアップグレードできます。

**タスク1 :ステージングフォルダ( /var/netwitness/common/update-stage/) にバージョンアップグレード ファイルを配置する。次の操作を実行します。**

1. NetWitnessコミュニティ(<https://community.netwitness.com/>)にアクセスし、**ダウンロード** > **[NetWitness Platform]** > **[バージョン12.5.0.0]**を選択して、アップグレード パッケージ netwitness-12.5.0.0.zipをローカル ディレクトリにダウンロードします。


- 12.2.0.0, 12.2.0.1, 12.3.0.0, 12.3.1.0, 12.4.0.0, 12.4.1.0, および12.4.2.0からアップグレードする場合は、netwitness-12.5.0.0.zip をダウンロードしてください。
2. SSHでNW Serverホストに接続します。
  3. netwitness-12.5.0.0.zipをNW Serverホスト上の/var/netwitness/common/update-stage/にアップロードします。  
以下に例を示します。  


```
mv /var/netwitness/tmp/netwitness-12.5.0.0.zip  
/var/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。次の操作を実行します。

**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。

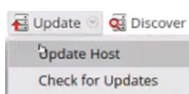
- NetWitness Platformが更新パッケージにアクセスできる。
- パッケージが完全でエラーがない。

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によって異なります。  
初期化が成功すると、[ステータス] 列に 更新あり] と表示されます。

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 :CLIを使用したNetWitness Platformのアップグレード(オフライン)

このオプションは、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。

### 開始する前に

NetWitnessコミュニティ(<https://community.netwitness.com/>) > **Products**] > **NetWitness Platform**] > **Downloads**] で次の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。

- 12.2.0.0、12.2.0.1、12.3.0.0、12.3.1.0、12.4.0.0、12.4.1.0、12.4.2.0からアップグレードする場合は、以下をダウンロードします。

```
netwitness-12.5.0.0.zip
```

- 外部リポジトリを使用している場合は、外部リポジトリに最新の更新を追加します。詳細については、「[CLIによるアップグレードのための外部リポジトリの準備](#)」を参照してください。

NWサーバー ホストとコンポーネント サーバーをアップグレードするには、次の手順を実行します。

**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。ただし、HTMLページ <https://community.netwitness.com/t5/netwitness-platform-online/upgrade-tasks-for-12-1-1/ta-p/695018#Option3>からコマンドをコピーして、Linux SSHターミナルに貼り付けることができます。

1. 12.5.0.0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。次のシナリオを検討します。
  - **オプション1(手動)** :NetWitness Serverにログインして、次のディレクトリーを作成します。  

```
/var/netwitness/tmp/upgrade/12.5.0.0/
```

次に、パッケージZipファイルをNW Serverの/var/netwitness/tmp/ ディレクトリーにコピーし、次のコマンドを使用して/var/netwitness/tmp/ から適切なディレクトリーに解凍します。  

```
unzip netwitness-12.5.0.0.zip -d /var/netwitness/tmp/upgrade/12.5.0.0
```

アップデート用のzipファイルは抽出した後でステージング ディレクトリーから必ず削除してください。
  - **オプション2(自動)** :NetWitness Serverにログインして、次のディレクトリーを作成します。  

```
/var/netwitness/tmp/upgrade/
```

NetWitness 12.5.0.0の、パッケージzipファイルをNetWitness Serverの/var/netwitness/tmp/ ディレクトリーにコピーします。  
この後で、次のコマンドを実行して12.5.0.0 zipファイルを抽出、検証、初期化します。  

```
[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.5.0.0
```

**(情報)** 必要なすべてのNetWitness zipファイルのダウンロードと解凍が完了しました」というメッセージが管理サーバーのコンソールに表示されると、初期化プロセスが開始されます。

**注：**〔情報〕 必要なすべてのNetWitness zipファイルのダウンロードと解凍が完了しました〕というメッセージが表示されない場合は、前のコマンドを再び実行してください。

**重要：**（オプション2を使用して）12.5.0.0をステージングした後、初期化に失敗した場合は、コマンド `upgrade-cli-client --init --version 12.5.0.0 --stage-dir /var/netwitness/tmp/upgrade` を実行してください。初期化が成功した場合は、下記の「[ステップ2 :アップグレードの初期化](#)」を無視して、ステップ3～6に進みます。

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 12.5.0.0 --stage-dir /var/netwitness/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 --version 12.5.0.0 --host-key <ID / display name / (hostname/ IP address)>`

**注：**アップグレードがトリガーされると、アップグレード プロセスが開始されてから約10分後に、NW Serverが自動的に再起動します。新しいカーネル( Alma Linux 8.10の場合は4.18) で起動します。

**注意：**UIが起動して実行されるまで待つことをお勧めします。完了までに最大で1時間かかる場合があります。移行の20～30分後、SSHで接続して、OSが移行されたかどうかを確認できます。NWアップグレードは、バックグラウンドで実行されるため、OSの移行が完了してからUIが表示されるまでに少なくとも30分かかる場合があります。

上記のアップグレード プロセスは、VMの仮想コンソール、またはiDRACを備えたサーバーのリモートコンソールを通じて追跡できます。

仮想コンソールに接続する方法の詳細については、<https://www.dell.com/support/kbdoc/en-in/000179797/dell-poweredge-idrac-virtual-console>を参照してください。

OSが移行され、管理ノードにSSHで接続できるようになったら、ホスト上で次のコマンドを実行して、OSの移行が成功したことを確認します。

- `cat /etc/redhat-release`
- AlmaLinux release 8.10 (Cerulean Leopard)

**注意：**OSの移行後、以前にインストールしたサードパーティ製 RPMを再インストールします。

4. オーケストレーション サーバーが起動すると、chefを介して目的のNWバージョンへのNWアップグレードが自動的にトリガーされます。この進行状況を確認するには、管理サーバーにSSHで接続し、次のコマンドを実行します。  
`orchestration-cli-client --check-admin-upgrade-status`

**注：**上記のコマンドは、NW Admin Serverに対してのみ実行します。

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. (条件付き) ウォームスタンバイサーバーが導入されている場合は、ウォームスタンバイサーバーホストでステップ1～5を繰り返します。

7. 各コンポーネント ホストに対して、ステップ3とステップ5を繰り返します。コマンドのIPアドレスは、アップグレードするコンポーネント ホストのIPアドレスに変更します。

**注** :NW Serverホストで`upgrade-cli-client --list`コマンドを実行すると、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。

## CLIによるアップグレードのための外部リポジトリの準備

外部リポジトリのセットアップの詳細については、『NetWitness Platform 12.5.0.0アップグレード ガイド』の「付録A :外部リポジトリのセットアップ」を参照してください。次の手順は、外部リポジトリがすでにセットアップされていることを前提としています。[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。

1. 12.5.0.0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。次のシナリオを検討します。
  - 12.2.0.0, 12.2.0.1, 12.3.0.0, 12.3.1.0, 12.4.0.0, 12.4.1.0および12.4.2.0 からアップグレードする場合は、12.5.0.0のみをステージングする必要があります。

- **オプション1(手動)** :NW Witness Serverにログインして、次のディレクトリを作成します。

```
/var/netwitness/tmp/upgrade/12.5.0.0/
```

次に、パッケージZipファイルをNW Serverの/var/netwitness/tmp/ディレクトリにコピーし、次のコマンドを使用して/var/netwitness/tmp/から適切なディレクトリに解凍します。

```
unzip netwitness-12.5.0.0.zip -d /var/netwitness/tmp/upgrade/12.5.0.0
```

アップデート用のzipファイルは抽出した後でステージングディレクトリから必ず削除してください。

- **オプション2(自動)** :NW Witness Serverにログインして、次のディレクトリを作成します。

```
/var/netwitness/tmp/upgrade/
```

NetWitness 12.5.0.0のパッケージzipファイルをNetWitness Serverの/var/netwitness/tmp/ディレクトリにコピーします。

この後で、次のコマンドを実行して12.5.0.0 zipファイルを抽出、検証、初期化します。

```
[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness
/tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.5.0.0
```

**〔情報〕** 必要なすべてのNetWitness zipファイルのダウンロードと解凍が完了しましたというメッセージが管理サーバーのコンソールに表示されると、初期化プロセスが開始されます。

**注** :〔情報〕 必要なすべてのNetWitness zipファイルのダウンロードと解凍が完了しましたというメッセージが表示されない場合は、前のコマンドを再び実行してください。

**重要** :〔オプション2を使用して) 12.5.0.0をステージングした後、初期化に失敗した場合は、コマンド`upgrade-cli-client --init --version 12.5.0.0 --stage-dir /var/netwitness/tmp/upgrade`を実行してください。初期化が成功した場合は、下記の「[ステップ2 :アップグレードの初期化](#)」を無視して、ステップ3～6に進みます。

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 12.5.0.0 --stage-dir
/var/netwitness/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 --version 12.5.0.0 --host-key <ID / display
```

name / (hostname/ IP address)>

**注** :アップグレードがトリガーされると、アップグレード プロセスが開始されてから約10分後に、NW Serverが自動的に再起動します。新しいカーネル( Alma Linux 8.10の場合は4.18) で起動します。

**注意** :UIが起動して実行されるまで待つことをお勧めします。完了までに最大で1時間かかる場合があります。移行の20～30分後、SSHで接続して、OSが移行されたかどうかを確認できます。NWアップグレードはバックグラウンドで実行されるため、OSの移行が完了してからUIが表示されるまでに少なくとも30分かかる場合があります。

上記のアップグレード プロセスは、VMの仮想コンソール、またはiDRACを備えたサーバーのリモートコンソールを通じて追跡できます。

仮想コンソールに接続する方法の詳細については、<https://www.dell.com/support/kbdoc/en-in/000179797/dell-poweredge-idrac-virtual-console>を参照してください。

OSが移行され、管理ノードにSSHで接続できるようになったら、ホスト上で次のコマンドを実行して、OSの移行が成功したことを確認します。

- `cat /etc/redhat-release`
- AlmaLinux release 8.10 (Cerulean Leopard)

**注意** :OSの移行後、以前にインストールしたサードパーティ製 RPMを再インストールします。

4. オーケストレーション サーバーが起動すると、chefを介して目的のNWバージョンへのNWアップグレードが自動的にトリガーされます。この進行状況を確認するには、管理サーバーにSSHで接続し、次のコマンドを実行します。

- `orchestration-cli-client --check-admin-upgrade-status`

**注** :上記のコマンドは、NW Admin Serverに対してのみ実行します。


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. (条件付き) ウォーム スタンバイ サーバーが導入されている場合は、ウォーム スタンバイ サーバー ホストでステップ1～5を繰り返します。
7. 各コンポーネント ホストに対して、ステップ3とステップ5を繰り返します。コマンドのIPアドレスは、アップグレードするコンポーネント ホストのIPアドレスに変更します。

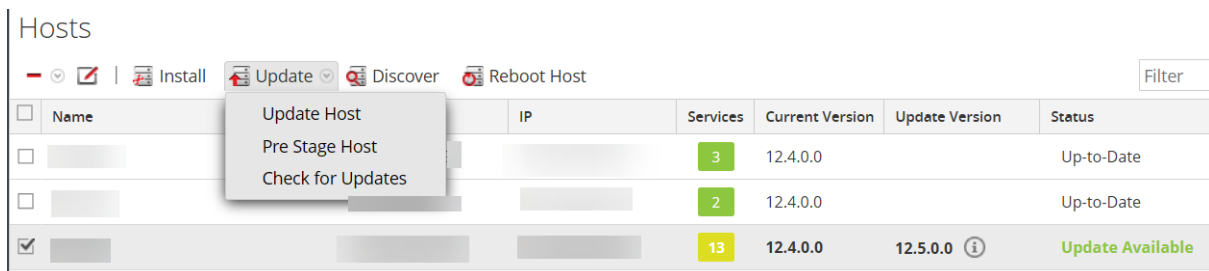
**注** :NW Serverホストで`upgrade-cli-client --list`コマンドを実行すると、すべてのホストのバージョンをチェックすることができます。`upgrade-cli-client`のヘルプを表示するには、`upgrade-cli-client --help`コマンドを使用します。

## オプション4( オプション) :パッケージのダウンロードによるアップグレード リポジトリの事前設定

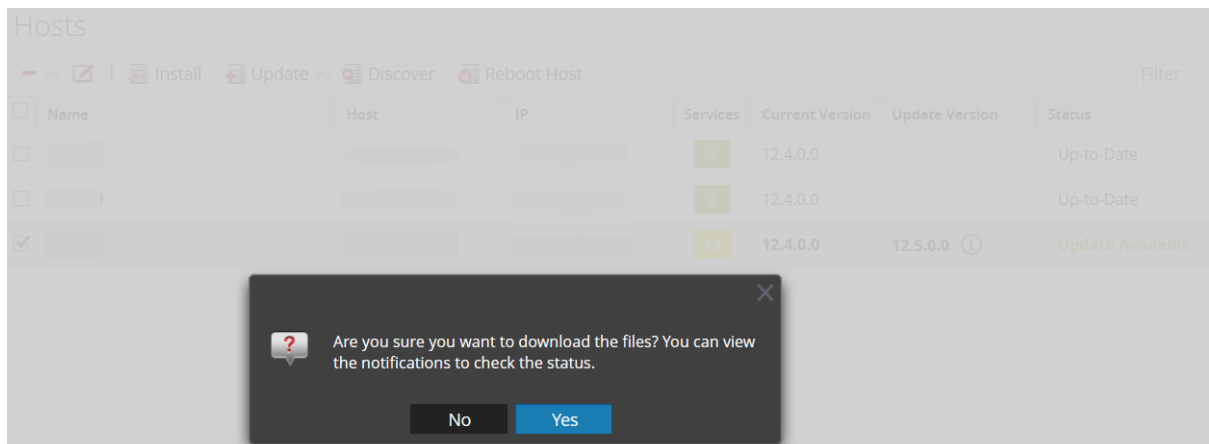
必要なパッケージ(.zip)をダウンロードすることで、システムに影響を与えることなく、アップグレード リポジトリを事前設定できます。これにより、アップグレードのダウンタイムが最小限に抑えられ、計画された時間内にアップグレードが完了することが保証されます。

アップグレード リポジトリを事前ステージングしてホストを更新するには、次の手順を実行します。

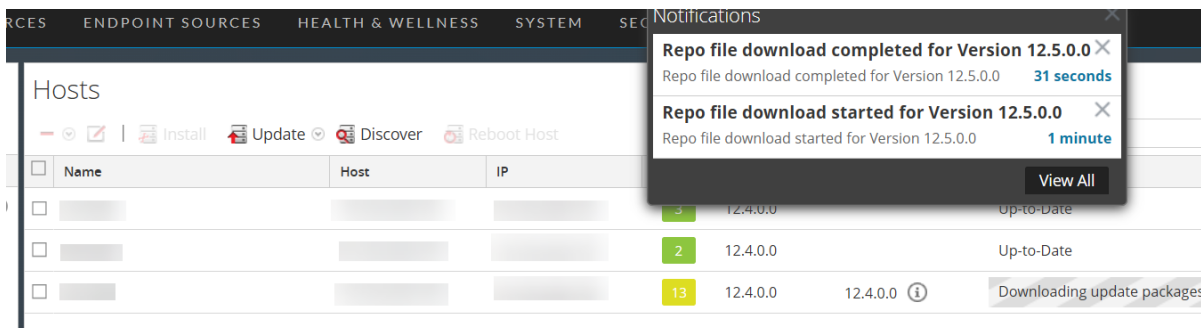
1.  (管理) > **ホスト**]に移動します。
2. ツールバーで **更新** > **更新の確認**]をクリックします。  
適用可能なすべての更新バージョンが [バージョン] ドロップダウン リストに表示されます。
3. **更新**] > **ホストの事前設定**]をクリックして、更新バージョンの列でバージョンを選択します。



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。



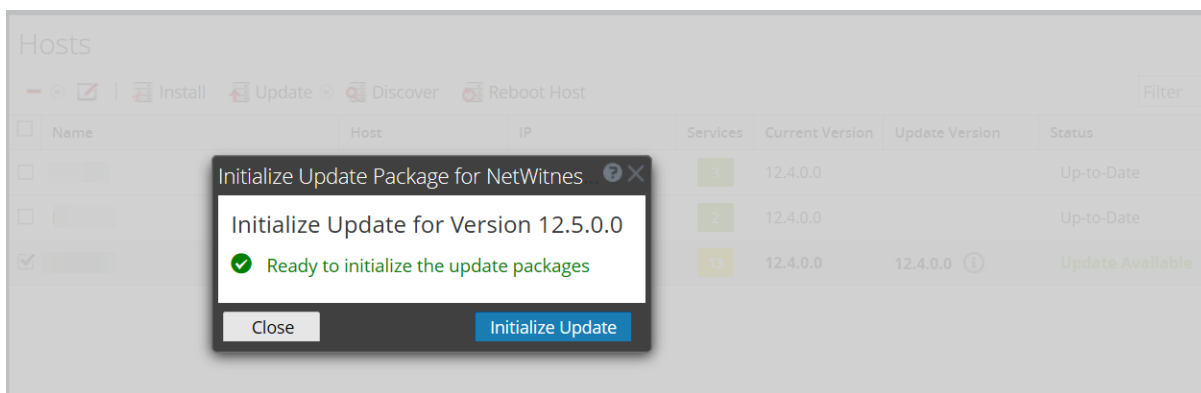
4. **はい**]をクリックしてアップグレード パッケージをリポジトリにダウンロードします。
5. 下図に示すように、通知トレイでダウンロードのステータスを確認します。  
**ホストの事前設定**]と **ホストのアップグレード**]は、事前設定が完了するまで無効になります。



**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 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の実行

このトピックでは、NetWitness Platformのアップグレード後に実行する必要があるタスクを示します。ご使用のホストのタスクを完了してください。

- [全般](#)
- [Event Stream Analysis\(ESA\)](#)
- [対応](#)
- [User and Entity Behavior Analytics](#)
- [Legacy Windows Log Collector](#)
- [Warehouse Connector](#)
- [ロックボックスの回復パスワードの設定](#)

### 全般

NetWitness Platformをアップグレードした後は、Jettyを構成し、コアサービスのコンテンツを復元して、ネットワークキャプチャ、ログキャプチャ、および集計を開始する必要があります。

### Jettyの構成

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 エントリの管理](#)」で「[カスタムJetty構成の管理](#)」セクション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

ネットワーク収集を開始するには、次の手順を実行します。

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。

**ログ収集を開始するには、次の手順を実行します。**

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。

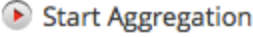
**集計を開始するには、次の手順を実行します。**

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) の場合：

**注** ESAホストでは混合モード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。

## コア サービス コンテンツの復元


12.5にアップグレードすると、構成ファイル(.cfg)、フィード、パーサ、ログ デバイスなどのコア サービス コンテンツがDecoder、Log Hybrid、Network Hybrid、Log Decoderなどの各コンポーネントの.tarの場所にコピーされます。



次の表に、コア サービス コンテンツのパスとコア サービス コンテンツがコピーされる各コンポーネントの.tarの場所を示します。

コアサービス コンテンツのパス	コンポーネント	コンポーネントのtarの場所
/etc/netwitness/ng/feeds( フィード)	Decoder	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/parsers( パーサ)	Log Hybrid	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar
/etc/netwitness/ng/envision/etc/devices( ログ デバイス)	Network Hybrid	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/NwDecoder.cfg( 構成ファイル(.cfg))	Log Decoder	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar

CCMオプションはデフォルトで無効になっています。12.5にアップグレードした後、CCMを有効にしてコア サービス コンテンツが失われた場合は、バックアップtarファイルを使用して失われたデータを回復できます。詳細については、<https://community.netwitness.com/t5/netwitness-knowledge-base/automatic-backup-of-core-service-content-after-upgrading-core/ta-p/694527>を参照してください。

## Event Stream Analysis( ESA)

12.5バージョンにアップグレードすると、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。各展開はポリシーとグループに変換され、関連サーバーを12.5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。Admin Serverが完了した直後に関連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。対応する関連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。ただし、Correlationサーバーは引き続きアラートとイベントの処理を続けます。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ESAR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。

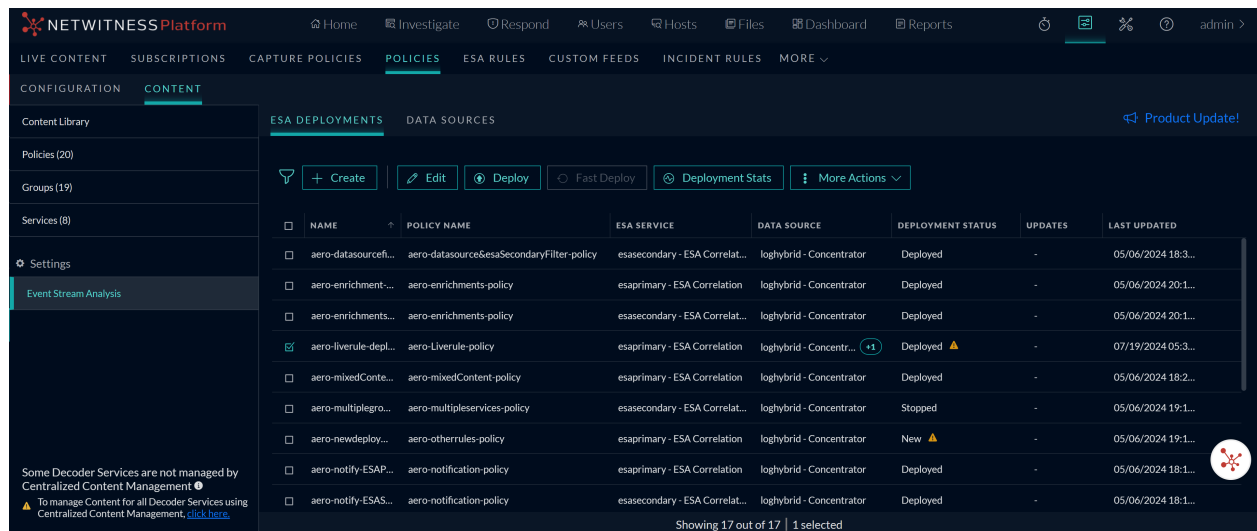
SINo	アップグレード前の導入環境の状態	アップグレード後の導入環境の状態		
		ポリシーの作成	グループの作成	ポリシーが公開されます
1	正常な導入環境	はい	はい	はい
2	エラーのある導入環境	はい	はい	はい

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
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。

## ESA導入環境とデータソースの管理


ESA導入環境とデータソースは**コンテンツ元管理**でのみ管理できます。**☰(構成) > [ポリシー] > [コンテンツ] > [Event Stream Analysis]**ページに移動し、ESA導入環境とデータソースを管理します。ESAルールは、**[ESAルール]**ページでのみ管理できます。次の図を参考にしてください。



管理サーバーのアップグレード後は、ESAホストを速やかにアップグレードする必要があります。

**注** :Mitreの戦術と手法を使用してESAアラートを生成するには、ESARルールに関連付けられたESAを、12.5バージョンにアップグレードした後で再展開する必要があります。

## 通知用のカスタムスクリプトを移行する

- スクリプト通知機能(  (管理)] > システム] > グローバル通知] > スクリプト]) のカスタムスクリプトファイルに関するファイル権限や所有属性には多くの変更があるため、NetWitnessではシステムをバージョン12.5にアップグレードする前にカスタムスクリプトのバックアップを作成しておくことを推奨しています。
- アップグレードが完了したら、各スクリプトを再検討して、構文/意味の変更を加える必要があります。
- NetWitnessバージョン12.5より前のカスタムスクリプトが /tmp または /var/tmp フォルダ内のファイルリソースにアクセスしている場合でも、カスタムスクリプトの実行に使用する所有権が変更されているため、それらのファイルリソースにはアクセスできなくなります。このシナリオでは、カスタムスクリプトを微調整/変更して、 /tmp または /var/tmp ディレクトリに新しいファイルを作成/読み取ることをお勧めします。

コンテンツ元管理と導入管理の詳細については、『NetWitnessコンテンツ元管理ガイド』を参照してください。

## 対応

次のタスクを完了する前に、プライマリESAサーバーを12.5にアップグレードする必要があります。

**注** :プライマリNWサーバー (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ホストも12.5にアップグレードされるまで、Respond Serverサービスは自動的に再度有効化されません。Respondのアップグレード後のタスクは、Respond Serverサービスがアップグレードされ、有効な状態になってから実行する必要があります。

## (オプション) custom\_normalize\_alerts.jsでRespondサービスのカスタム キーをリストアし、新しいデータソースをサポート

**注** : custom\_normalize\_alerts.jsを手動でカスタマイズしなかった場合は、このタスクをスキップできます。カスタム キーの自動移行が試行されます。自動移行に失敗した場合は、この手順に従ってカスタム データの整合性を確認してください。

カスタム正規化で使用するために/var/netwitness/respond-server/scripts/custom\_normalize\_alerts.jsファイルにカスタム キーを追加した場合は、/var/netwitness/respond-server/scripts/custom\_normalize\_alerts.js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正規化されたキーを追加します。バックアップファイルは/var/netwitness/respond-server/scriptsにあり、次の形式になります。

```
custom_normalize_alerts.js.bak-<time of the backup>
```

スクリプトの自動更新に失敗した場合は、Respondの新しいデータソースであるNetwitness CoreとNetWitness Insightをサポートするには、手動でcustom\_normalize\_alerts.jsファイルを更新します。

## User and Entity Behavior Analytics

UEBAを12.5にアップグレードした後、次のタスクを完了します。

**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** : NetWitnessバージョン12.5では、UEBAの暗号化メカニズムが更新されました。以前のバージョンから12.5.0.0にアップグレードするユーザーは、スクリプト update\_encrypted\_password\_12\_5.pyを実行して、UEBAサーバーの暗号化を更新する必要があります。この更新を適用するには、スクリプトパッケージをダウンロードし、UEBAサーバーのルート ディレクトリに保存してください。スクリプトパッケージは、次のURL <https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-12-5-ueba-encryption-script-download/ta-p/715887> またはNetWitnessコミュニティ (<https://community.netwitness.com/>) **ダウンロード** > **NetWitness Platform** > **バージョン12.5** ページからダウンロードできます。

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
- python /var/netwitness/presidio/airflow/venv39/lib/python3.9/site-packages/presidio\_workflows-1.0-py3.9.egg/presidio/resources/rerun\_ueba\_server\_config.py
- python /root/update\_encrypted\_password\_12\_5.py
- deactivate



- 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。

The screenshot shows the Airflow web interface with the 'Admin' dropdown menu open. The menu options are: Pools, Configuration, Users, Connections, Variables, XComs, and REST API Plugin. The background shows a table of DAGs with columns for DAG name, Schedule, Owner, Recent Tasks, Last Run, DAG Runs, and Links.

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

The screenshot shows the Airflow Pools page. A table lists pools with columns for Pool, Slots, Used Slots, and Queued Slots. The 'spring\_boot\_jar\_pool' row has 7 slots, 7 used slots, and 0 queued slots. A pencil icon is visible next to this row, indicating it can be edited.

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

## Legacy Windows Log Collector

### 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. 次のコマンドを管理サーバーで実行します。

- 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。

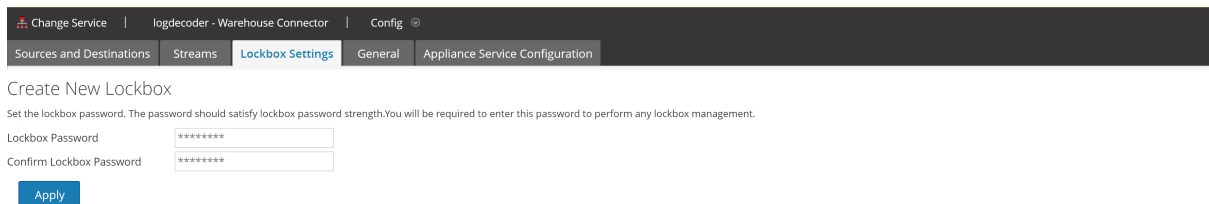
- i. **Legacy Windows Log CollectorのRESTユーザー名とLegacy Windows Log CollectorのRESTパスワード** :Legacy Windows Log Collectorの管理者認証情報を入力します。
- ii. **Security Serverのユーザー名とSecurity Serverのパスワード** :NetWitnessの管理者認証情報を入力します。

2. システムを再起動します。

## Warehouse Connector

Warehouseコネクタは、ロックボックスを使用して、データ統合のソースと宛先の資格情報を安全に保存します。ただし、以前のバージョンから12.5バージョンにアップグレードするユーザーは、既存の資格情報を新しいロックボックスに移行しないと、構成されたストリームを開始できません。そのため、ユーザーは次の手順に沿って手動で新しいロックボックス キーを作成し、該当する場合はWarehouse Connectorで構成されているソース宛先のパスワードを更新する必要があります。

1. NetWitness Platformにログインします。
2.  (管理) > [サービス] に移動します。
3. [サービス] ビューで、追加したWarehouse Connectorサービスを選択し、 > [表示] > [構成] を選択します。
4. Warehouse Connectorのサービス構成ビューで、**ロックボックス設定** タブをクリックし、新しいロックボックス キーを作成します。



5. **Explore** または **REST API**を使用して、ソース構成でユーザー アカウントを再認証します。ソース ユーザー アカウントの再認証はUIでは行えません。**Explore** からユーザー アカウントを再認証するコマンドは次のとおりです。

```
> /warehouseconnector/sources/<source:port> ---> setPass property with password=<password of the configured user in source>
```

6. [UI]、[エクスプローラ]、または [REST API] から、SFTP宛先構成でユーザー アカウントを再認証します。**Explore** からパスワードを再認証するコマンドは以下のとおりです。

```
> /warehouseconnector/destinations/<sftp_destination> ---> setPass property with password=<password of the configured user in SFTP destination>
```

7. アップグレード前の手順の一環としてNFSディレクトリマウントが削除された場合は、同じ構成でマウントし直します。さらに、`/etc/fstab`のマウント エントリを再度有効にします。

```
> mount -t nfs -o noexec,nolock,tcp,hard,intr <IP_Address_for_SAW>:/mapr/<cluster-name> /<directory_name>
```

ここで、`<IP_Address_for_SAW>` はクラスター内のプライマリWarehouseアプライアンスのIPアドレスであり、`<cluster-name>` はテンプレート ファイルで指定された名前です。

## ロックボックスの回復パスワードの設定












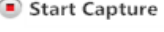





NW展開内のすべてのログ コレクターとWLCを12.5にアップグレードした後、管理者はSAToolsを使用して **回復パスワード ユーティリティ** を実行する必要があります。このツールは、展開内のすべてのログ コレクター サービス (バージョン12.5以上) のLockbox回復パスワードを設定します。管理者は、ディザスター リカバリー シナリオで必要となるため、Lockbox回復パスワードをメモしておいてください。

回復パスワードを設定するには、管理者はSSHで管理サーバー(ノード0)に接続し、パス  
/opt/rsa/saTools/bin/set-lockbox-passwordからユーティリティset-lockbox-passwordを実行す  
る必要があります。管理者は、すべてのログ コレクターで使用可能なロックボックスの回復パスワードと  
して設定する新しいパスワードを入力する必要があります。

**注** :ユーティリティを再実行し、更新されたロックボックスを設定すると、回復パスワードによって、該当  
するすべてのログ コレクター サービス (バージョン12.5以降) のパスワードがリセットされます。

## アップグレード後に検証チェックを実行する

NetWitness 12.5にアップグレードした後、次の検証チェックを実行する必要があります。

1.  (管理) > [サービス]ビューに移動して、アップグレード後にすべてのサービスがアクティブである (緑色で表示されている) ことを確認します。
2. サービスがホストのバージョンと一致するようにアップグレードされていることを確認します。 (管理) > [サービス]ビューのサービスバージョンが、アップグレード後に (管理) > [ホスト]ビューのホストバージョンと一致している必要があります。
3.  (管理) > [サービス]ビューで、以下を行います。
  - Log Collectorサービスを選択し、 (アクション) > [表示] > [システム]ビューに移動して、必要なログ収集が開始されているかどうかを確認します。 Collection  ドロップダウン オプションをクリックし、適切な収集プロトコルに移動して、ログ収集が開始されているかどうかを確認する必要があります。必要な収集が開始されていない場合は、リストから必要な収集プロトコルの横の  Start を選択して収集を開始します。
  - Log Decoderサービスを選択し、 (アクション) > [表示] > [システム]ビューに移動して、Log Decoderがログを適切に収集しているかどうかを確認します。
  - Packet Decoderサービスを選択し、 (アクション) > [表示] > [構成]ビューに移動して、収集インターフェイスが [Decoder構成] セクションで設定されているかどうかを確認します。収集インターフェイスが構成されていない場合は、ドロップダウン リストから必要な収集インターフェイスを選択して構成する必要があります。収集インターフェイスがすでに構成されている場合は、Packet Decoderの  (アクション) > [表示] > [システム]ビューに移動し、収集が開始されているかどうかを確認します。収集が開始されていない場合は、 Start Capture をクリックしてパケット収集を開始します。
4.  (管理) > [サービス] > [Log Decoder] または [Packet Decoder] サービスを選択して、 (アクション) > [表示] > [統計] > [全般]ビューに移動して、現在の収集レートを分析します。
5. Concentrator、Archiver、およびBrokerがデータを集約していることを確認します。各 Concentrator、Archiver、Brokerから調査して、動作状態を検証できることを確認してください。
6. [Respond] > [アラート]ビューに移動して、アラートが別のソースからトリガーされているかどうかを確認します。
7.  (管理) > [ヘルスマニタ] > [アラーム]に移動して、SMSサーバーが稼働しているかどうかを確認します。
8.  (管理) > [イベント ソース] > [モニタリング ポリシー]ビューに移動して、アップグレード前に構成されたポリシーが表示されているかどうかを確認します。
9.  (管理) > [ヘルスマニタ] > [新ヘルスマニタ] > [ダッシュボードに移行] > [Elastic] > [Dashboard]ビューに移動して、次のことを確認します。

- アップグレード前に作成したビジュアライゼーションがまだ存在すること。
- メトリック サーバーが動作していること。
- アップグレード前に構成したモニタに関するアラートが適切に生成されていること。

## 12.5 リレーサーバーをインストールする

**重要** :リレー サーバーはスタンドアロン サーバーであるため、EPLHを12.2.x.xおよび12.3.x.xバージョンから12.5.0.0にアップグレードした後で、EL 8 (Alma Linux)ボックスにリレー サーバーを再インストールする必要があります。

### 開始する前に

- EL 8ボックスがあることを確認します。
- 12.5リレー サーバーをインストールする前に、次のタスクを実行します。
  1. NetWitness Platformをアップグレードします。
  2. EPLHがアップグレードされたら、リレー パッケージをダウンロードします。
  3. パッケージをEL 8ボックスにコピーします。
  4. 既存のリレー サーバーをオフにします。
  5. 既存のリレー サーバーのIPアドレスを再利用して、EL 8のIPアドレスを構成します。

EL 8のIPアドレスを設定したら、リレー サーバーをインストールします。詳細については、『[Endpoint構成ガイド](#)』の「[\(オプション\) リレー サーバー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。

**注** :リレー サーバー上のセキュリティ パッチを最新の状態に保つ必要があります。

## 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 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。

## アップグレードの問題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。次のトラブルシューティング ソリューションを使用してもアップグレードまたはインストールの問題を解決できない場合は、NetWitness [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。

- [AlmaLinux OSのトラブルシューティング情報](#)
- [管理サーバー、Reporting Engine、SMSでのLockboxからSecureStoreへの移行の失敗](#)
- [deploy\\_admin/パスワード期限切れエラー](#)
- [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](#)
- [ホスト更新失敗エラー](#)
- [更新パッケージが見つからないエラー](#)
- [非NWサーバーへのパッチ更新エラー](#)
- [コマンド ラインからの更新後のホスト再起動エラー](#)

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](#)

<b>問題</b>	アップグレード後にアプライアンスを起動できない
<b>回避策</b>	<ol style="list-style-type: none"> <li>1. GRUBブート行を手動で <code>FIPS=0</code>に変更して、起動できるようにします。</li> <li>2. ここから、次のコマンドを使用してFIPSを無効にします。  <pre>manage-stig-controls --disable-control-groups 3 --host-all</pre> </li> <li>3. 行<code>FIPS=1</code>が<code>/boot/grub2/grub.cfg</code>から削除されたことを確認します。 <ul style="list-style-type: none"> <li>• 削除されていない場合は、次のコマンドを実行します。  <pre>grub2-mkconfig -o /boot/grub2/grub.cfg</pre> </li> </ul> </li> </ol>

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。

## AlmaLinux OSのトラブルシューティング情報

理解しやすいように、AlmaLinux OSアップグレードは次の4つの部分に分けて考えることができます。

1. 事前チェックユーティリティの実行。システムの健全性を確認し、アップグレードの問題を検出します。これは、スタンドアロンの事前チェックツールrpmを使用して、アップグレード前にいつでも行うことができます。(NW Serverのみで必要)

ログはこのパスに記録されます - /var/log/netwitness/precheck-tool/checklist.log

2. 初期化または初期化フェーズ(NW Serverでのみ発生)

初期化フェーズ中に問題が発生した場合は、これらのログを確認してください。

- salt minionログ - /var/log/salt/minion
- deployment-upgradeログ - /var/log/netwitness/deployment-upgrade/chef-solo.log

**注** :実際にアップグレードを行う予定がある場合にのみ、初期化を実行してください。同じ変更ウィンドウ内でシステムをアップグレードせずに初期化を実行することはお勧めできません。

3. CentOSからAlmaLinuxへのOSアップグレード

OSアップグレードの最初のステップとして、saltがアップグレードされます。以下のコマンドを実行すると、saltがバージョン3006にアップグレードされていることを確認できます。

```
cat /var/log/yum.log | grep salt
```

以下の更新と同様の内容を表示できます。xxxは現在の日時スタンプを表します。

```
xxx Updated: salt-master-3006.2-0.x86_64
```

```
xxx Updated: salt-api-3006.2-0.x86_64
```

```
xxx Updated: salt-minion-3006.2-0.x86_64
```

salt-upgrade1に問題がある場合は、以下を確認してください。

- /var/log/netwitness/node-infra-server/node-infra-server.log
- /var/log/salt/master
- /var/log/salt/minion

saltがアップグレードされると、leappプロセスが開始されます。

ログは/var/log/salt/minionで表示できます。

```
xxx [salt.loaded.ext.module.nw_platform:445 ][INFO ][139407] [1/5]
Searching for leapp config for version: 12.5.0.0
```

```
xxx [salt.loaded.ext.module.nw_platform:453 ][INFO ][139407] [2/5]
Retrieving leapp config for version: 12.5.0.0

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'config/12.5.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:467 ][INFO ][139407] [3/5] Running
pre-requisites required to perform leapp upgrade

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/actor.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/libraries/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/addupgradebootentry.py'

xxx [salt.loaded.ext.module.nw_platform:500 ][INFO ][139407] [4/5] Running
leapp pre-upgrade

xxx [salt.loaded.ext.module.nw_platform:503 ][INFO ][139407] [5/5] Running
leapp upgrade
```

OSのアップグレード中に発生した問題については、以下のログがトラブルシューティングに役立ちます。

- /var/log/salt/minion
- Preupgradeが失敗した場合 - /var/log/leapp/leapp-preupgrade.log
- Leappアップグレードが失敗した場合 - /var/log/leapp/leapp-upgrade.log

leappが失敗した場合、/var/log/leapp/leapp-report.txtは障害要因に関する詳細を提供します。

/var/log/salt/minionで「leappアップグレードを実行しています」というログが記録されてから数分後、システムが再起動します。復旧するまでに20 ~ 30分かかる場合があります。

起動したら、cat /etc/almalinux-releaseコマンドを使用してOSを確認できます。Alma Linuxリリースが表示されない場合は、アクションを起こす前にカスタマーサポートにお問い合わせください。

また、UIを通じてアップグレードをトリガーした場合に、いずれかのNodeXでステータス「Performing OS Migration」が1時間以上表示されるときは、leappログを確認して、カスタマーサポートにお問い合わせください。

#### 4. 12.5.0.0へのNWソフトウェアのアップグレード

OSの移行が完了すると、NWソフトウェアのアップグレードが開始され、UIが機能するまでに最大30分かかります。

NWソフトウェアのアップグレードが開始されると、次のログが/var/log/salt/minionに記録されます。

```
xxx [salt.loaded.ext.module.nw_platform:276 ][INFO ][14035] Preparing node
for upgrade to 12.5.0.0

xxx [salt.loaded.ext.module.nw_platform:280 ][INFO ][14035] [1/2] Searching
for yum config for version: 12.5.0.0
```

```
xxx [salt.loaded.ext.module.nw_platform:287 ][INFO ][14035] [2/2]
Retrieving yum config for version: 12.5.0.0

xxx [salt.fileclient :1333][INFO ][14035] Fetching file from saltenv
'base', ** done ** 'config/12.5.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading chef
package

xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading rsa-
nw-config-management package
```

構成管理ログ(/var/log/netwitness/config-management/chef-solo.log)またはUIログ(/var/netwitness/uax/logs/sa.log)を参照することもできます。

## 管理サーバー、Reporting Engine、SMSでのLockboxからSecureStoreへの移行の失敗

### 管理サーバーまたはJettyの場合

<b>問題</b>	管理サーバーでLockBoxからSecureStoreへの移行中にエラーが発生しました。
<b>原因</b>	SSV値の移行が不完全であるため。
<b>解決策</b>	<p>管理サーバーにアクセスできない場合は、次の手順を実行して問題を解決してください。</p> <ol style="list-style-type: none"> <li>管理サーバー/ノード ゼロにSSHで接続します。</li> <li>次のコマンドを使用してJettyサービスを停止します。 <pre>systemctl stop jetty</pre> </li> <li>次のパスから lockbox.ss および lockbox.ss.lock ファイルを別のバックアップ フォルダに移動します。 <ul style="list-style-type: none"> <li>/var/netwitness/uax</li> <li>/root/uaxbackup</li> </ul> </li> <li>次のコマンドを使用してJettyサービスを開始します。 <pre>systemctl start jetty</pre> </li> </ol>

### Reporting Engineの場合

<b>問題</b>	レポート エンジンでLockBoxからSecureStoreへの移行が失敗しました。
<b>原因</b>	SSV値の移行が不完全であるため。
<b>解決策</b>	<p>レポート エンジンにアクセスできない場合は、次の手順を実行して問題を解決してください。</p> <ol style="list-style-type: none"> <li>管理サーバー/ノード ゼロにSSHで接続します。</li> </ol>

2. 次のコマンドを実行して、Reporting Engineサービスを停止します。  

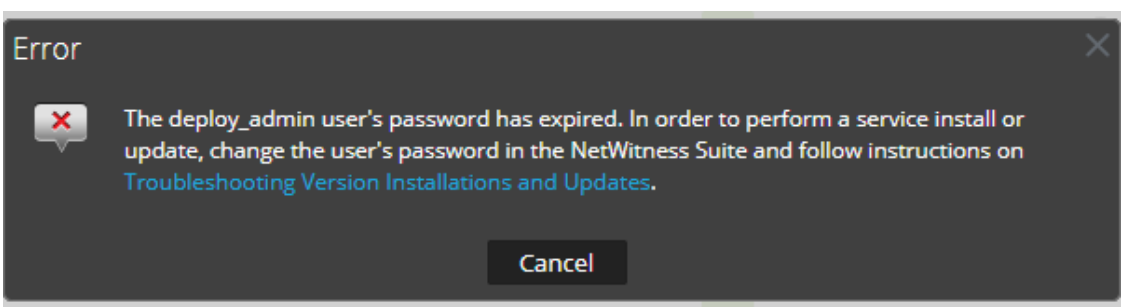
```
systemctl stop rsasoc_re
```
3. lockbox.ss および lockbox.ss.lock ファイルを /var/netwitness/re-server/rsa/soc/reporting-engine パスからバックアップ フォルダに移動します。
4. 次のコマンドを実行して、Reporting Engineサービスを開始します。  

```
systemctl start rsasoc_re
```

## SMSの場合

<b>問題</b>	SMSでLockBoxからSecureStoreへの移行に失敗しました。
<b>原因</b>	SSV値の移行が不完全であるため。
<b>解決策</b>	<p>SMSサービスにアクセスできない場合は、次の手順を実行して問題を解決してください。</p> <ol style="list-style-type: none"> <li>1. 管理サーバー/ノード ゼロにSSHで接続します。</li> <li>2. 次のコマンドを実行して、SMSサービスを停止します。  <pre>systemctl stop rsa-sms</pre> </li> <li>3. /root/rsa/homeパスからlockbox.ssおよびlockbox.ss.lockファイルを別のバックアップ フォルダに移動します。</li> <li>4. 次のコマンドを実行して、SMSサービスを開始します。  <pre>systemctl start rsa-sms</pre> </li> </ol>

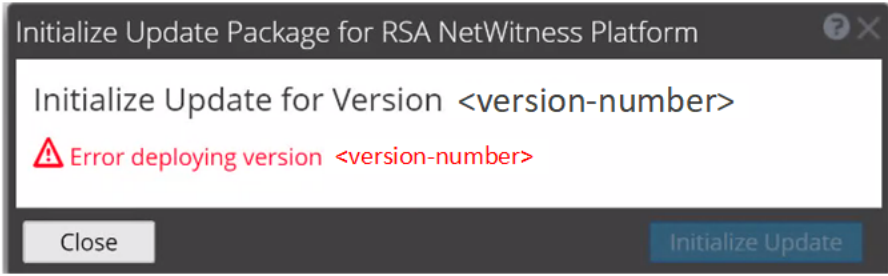
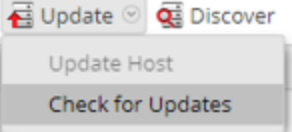
## deploy\_adminのユーザー パスワード有効期限切れエラー

エラー メッ セー ジ	
原因	<p>deploy_adminのユーザー パスワードの有効期限が切れています。</p>
解決 策	<p>deploy_adminのパスワードをリセットします。次の操作を実行します。</p> <ol style="list-style-type: none"> <li>NW Serverホストのみで次のコマンドを実行します。 <pre>nw-manage --update-deploy-admin-pw Please enter the new deploy_admin account password: &lt;new-deploy-admin-password&gt; Please confirm the new deploy_admin account password: &lt;new-deploy-admin-password&gt;</pre> </li> <li>nw-manage --update-deploy-admin-pwコマンドの出力を確認して、deploy_adminパスワードがすべてのホストで正常に更新されたことを確認します。NWホストがダウンしているか、nw-manage --update-deploy-admin-pwコマンドの出力に表示されている何らかの理由で失敗した場合は、通信障害が解決された後でnw-manage --sync-deploy-admin-pw --host-key &lt;host-identifier&gt;を実行して、失敗したホストとNW Serverの間でパスワードを同期します。</li> <li>インストールまたはオーケストレーションに失敗したホスト上で、nwsetup-tuiコマンドを実行し、[Deployment Password]のプロンプトが表示されたら、deploy_adminの新しいパスワードを入力します。</li> </ol>

## ダウンロード エラー

エラー メッ セー ジ	
問題	更新バージョンを選択し、 <b>更新</b> ] > <b>ホストの更新</b> ]をクリックすると、ダウンロードが開始されますが異常終了します。
原因	バージョンのダウンロード ファイルのサイズが大きく、ダウンロードに時間がかかる場合があります。ダウンロード中に通信の問題が発生すると、ダウンロードは失敗します。
解決 策	<ol style="list-style-type: none"> <li>1. 更新を再試行します。</li> <li>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「<b>ホスト</b>]ビューからのオフライン方式」または「<b>コマンド ライン インターフェイスを使用したオフライン方式</b>」の説明に従って、オフライン方式で更新してみてください。 <a href="#">NetWitnessの全バージョンのドキュメント</a>] 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。</li> <li>3. それでも更新できない場合は、 <a href="#">NetWitnessカスタマー サポート</a> にお問い合わせください。</li> </ol>

## 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&lt;version-number&gt;の導入中にエラーが発生しました」のエラーは更新パッケージが破損している場合に、<b>更新の初期化</b>]をクリックした後で、<b>NetWitness Platformの更新パッケージの初期化</b>]ダイアログに表示されます。</p>
解決 策	<ol style="list-style-type: none"> <li>1. <b>閉じる</b>]をクリックしてダイアログを閉じます。</li> <li>2. ステージング フォルダからバージョン フォルダを削除します。</li> <li>3. salt-masterサービスが実行されていることを確認します。</li> <li>4. 更新パッケージのzipファイルをステージング フォルダに再コピーします。</li> <li>5. <b>ホスト</b>]ビューのツールバーで、<b>更新の確認</b>]を再度選択します。</li> </ol>  <ol style="list-style-type: none"> <li>6. <b>更新の初期化</b>]をクリックします。</li> <li>7. ツールバーの <b>更新</b>] &gt; <b>ホストの更新</b>]をクリックします。</li> <li>8. 「アップデートが利用可能です」ダイアログから「<b>アップデートの開始</b>」をクリックします。ホストが更新されると、ホストを再起動するように求められます。</li> <li>9. ツールバーの <b>ホストの再起動</b>]をクリックします。</li> </ol>

## 外部リポジトリ更新エラー

エラー メッ セー ジ	<p>以下から新しいバージョンに更新しようとする、次のようなエラーが発生します。  <code>.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /&lt;version-number&gt;/RSA'": URL must be http, ftp, file or https not ""</code></p>
原因	<p>間違ったパスが指定されました。</p>
解決 策	<p>次の情報を確認します。</p> <ul style="list-style-type: none"> <li>• URLがNW Serverホスト上に存在する。</li> <li>• 正しいパスを使用し、スペースを削除している。</li> </ul>

## ホスト更新失敗エラー

<p>エラー メッセージ</p>	
<p>問題</p>	<p>アップデート バージョンを選択し、<b>[アップデート]</b> &gt; <b>[ホストのアップデート]</b>をクリックすると、ダウンロード プロセスは成功しますが、アップデート プロセスは失敗します。</p>
<p>解決策</p>	<ol style="list-style-type: none"> <li>1. ホストへのバージョン更新の適用を再試行します。 通常は、これで問題が解決されます。</li> <li>2. それでも新しいバージョンにアップデートできない場合は、次の手順を実行してください。 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)。  <pre> /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 </pre> 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。 </li> <li>3. それでも更新を適用できない場合は、上記の手順2 からログを収集し、<a href="#">NetWitness カスタマー サポート</a>にお問い合わせください。</li> </ol>
<p>エラー メッセージ</p>	
<p>問題</p>	<p>更新のバージョンを選択し、<b>更新]</b> &gt; <b>更新の確認]</b>をクリックすると、<b>権限なし]</b>エラーメッセージが表示されます。その結果、Liveサービスへの接続は失敗します。</p>
<p>解決策</p>	<ol style="list-style-type: none"> <li>1. Liveテスト接続が成功することを確認します。</li> <li>2. <b>(管理者)</b> &gt; <b>システム]</b> &gt; <b>更新]</b>で<a href="https://update.netwitness.com/RSA-netwitness">https://update.netwitness.com/RSA-netwitness</a>を更新します。</li> <li>3. 管理サーバーにSSHで接続して、<code>/etc/default/jetty</code>をバックアップします。</li> <li>4. <code>/etc/default/jetty</code>で<b>JAVA_OPTIONS</b>の末尾にある次のエントリを更新します。  <pre> JAVA_OPTIONS="\${JAVA_OPTIONS} - Drsa.nw.legacy.web.server.system.update.repo.url=https://update.netw itness.com/RSA-netwitness/ - </pre> </li> </ol>

	<pre>Drsa.nw.legacy.system.update.auth.url=https://update.netwitness.com/ authenticate "</pre>
	<p>5. 次のコマンドを実行してjettyサービスを再起動します。</p> <pre>service jetty restart</pre>


## 更新パッケージ不足エラー

エラー メッ セー ジ	<p>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</p>
問題	<p>「次の更新 パッケージが見つかりません」は、<b>ホスト</b>]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、<b>[NetWitness Platformの更新パッケージの初期化]</b>ダイアログに表示されます。</p>
解決 策	<ol style="list-style-type: none"> <li>1. <b>[NetWitness Platformの更新パッケージの初期化]</b>ダイアログで <b>[NetWitnessコミュニティーからパッケージをダウンロード]</b>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せん。</li> <li>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。 <b>[NetWitness Platformのアップデート パッケージの初期化]</b>ダイアログが開き、アップデート パッケージを初期化する準備ができたというメッセージが表示されます。</li> </ol>

## NW Server以外へのパッチ適用エラー

エラー メッ セー ジ	<pre>/var/log/netwitness/orchestration-server/orchestration-server.logで、 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 '12.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サーバーを12.2.0.0から12.5.0.0以降に更新する場合、NWサーバー以外のホストの更新パスは同じバージョン(つまり、12.5.0.0)のみになります。NW Server以外のホストを別のバージョン(たとえば、12.2.0.0から12.3.x.x)に更新しようとする、このエラーが発生します。</p>
解決 策	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>• 非NWサーバーホストを12.5.0.0以降に更新するか、</li> <li>• 非NWサーバーホストを更新しない(現在のバージョンのままにする)</li> </ul>

## コマンド ラインからの更新後のホスト再起動エラー

エラー メッセージ	ホストをオフラインで更新してリポートした後に、ユーザー インターフェイスにホストをリポートするようメッセージが表示されます。 
原因	上記のエラーは、CLIを使用してホストを再起動すると発生します。ホストを再起動するには、ユーザー インターフェイスを使用する必要があります。
解決策	ユーザー インターフェイスの [ホスト] ビューでホストをリポートします。

## 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。

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て失敗します。  <pre>Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.</pre>
原因	デコーダー キャプチャ構成は、PF_RINGキャプチャ(CentOS)を使用していて、12.5.0.0 (AlmaLinux) に直接アップグレードするお客様には有効ではありません。まず、PF_RINGデバイスをDPDKに移行してからアップグレードする必要があります。
解決 策	<b>この問題を解決するには、以下の手順を実行します。</b> 移行手順については、「 <a href="#">PF_RINGデバイスをDPDKに移行する</a> 」を参照してください。

## 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、次のいずれかが表示されます。 <ul style="list-style-type: none"> <li>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ません。</li> <li>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</li> </ul>
原因	NW Serverのグローバル監査設定は、12.2.x.xまたは12.3.x.xから12.5.0.0以降への移行に失敗しました。
解決 策	<ol style="list-style-type: none"> <li>SSHでNW Serverに接続します。</li> <li>次のコマンドを実行します。 orchestration-cli-client --update-admin-node</li> </ol>

## Orchestration

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

<b>問題</b>	<ol style="list-style-type: none"> <li>1. 非NW Serverホストをアップグレードしようとしたが、失敗しました。</li> <li>2. このホストのアップグレードを再試行しましたが、再度失敗しました。</li> </ol>
<b>原因</b>	<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>
<b>解決策</b>	<ol style="list-style-type: none"> <li>1. アップグレードに失敗した非NW ServerホストにSSHで接続します。</li> <li>2. 次のコマンドを実行します。 <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> </li> <li>3. 非NW Serverホストのアップグレードを再試行します。</li> </ol>
<b>問題</b>	<p>12.0以前のバージョンから12.5.0.0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12.5.0.0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 <b>管理</b>] &gt; <b>ホスト</b>]ビューの <b>サービス</b>]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。</p> <p>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12.5.0.0にアップグレードされなかった)12.5.0.0管理サーバーに対して新しい12.5.0.0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。</p>
<b>原因</b>	<p>12.5.0.0コア ノードXは、アップグレードされた12.5.0.0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。</p>
<b>解決策</b>	<p>12.5.0.0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。</p> <pre>mkdir -p /etc/netwitness/platform</pre> <ol style="list-style-type: none"> <li>1. <pre>touch /etc/netwitness/platform/nw-upgrade-mode</pre> <p>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。12.5.0.0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。</p> <pre>touch /etc/netwitness/platform/nw-upgrade-mode</pre> </li> <li>2. <pre>nw-manage --refresh-host --host-key &lt;core-node-x-salt-minion-uuid&gt;</pre> <pre>systemctl restart &lt;core-service-name&gt;</pre> </li> </ol>

**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、「 <i>Reporting Engine構成ガイド</i> 」の「 <b>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</b> 」を参照してください。

## Event Stream Analysis

問題	バージョン12.5.0.0以降にアップグレードすると、ESA関連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約しなくなります。
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	<p><b>この問題を解決するには、以下の手順を実行します。</b></p> <p>NetWitnessユーザー インタフェースで、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. <b>構成</b> &gt; <b>ポリシー</b> &gt; <b>コンテンツ</b> &gt; <b>Event Stream Analysis</b> &gt; <b>データソース</b> に移動します。 <b>データソース</b> パネルが表示されます。</li> <li>2. データソースを選択して、ツールバーで <b>データソースの編集</b> をクリックします。 <b>データソースの編集</b> ダイアログが表示されます。</li> <li>3. <b>データソースの編集</b> ダイアログで、次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• <b>信頼できる認証</b> を選択します。</li> <li>• <b>認証情報の使用</b> を選択して、ユーザー名とパスワードを入力します。</li> </ul> </li> </ol>

4. **接続のテスト**]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。

5. データソースへの変更が完了したら、**データソース**]パネルで編集したデータソースに関連付けられているすべての環境を導入します。

## Legacy Windows Log Collector

<b>問題</b>	スタックが12.5.0.0にアップグレードされると、従来のWindowsログコレクターは非アクティブとして表示されます。
<b>原因</b>	管理サーバーノードでの証明書の更新。
<b>解決策</b>	「 <a href="#">アップグレード後のタスクの実行</a> 」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

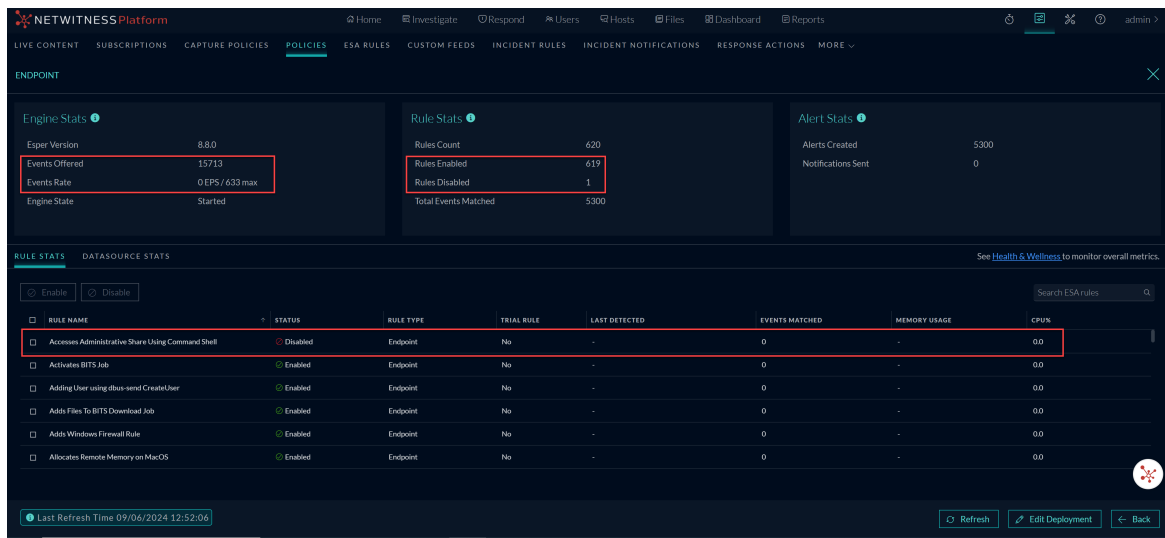
アラートが表示されない場合は、ESAルール導入環境のステータスを確認します。

1. **構成**] > **ポリシー**] > **コンテンツ**] > **Event Stream Analysis**] > **ESA導入環境**]に移動します。  
**ESA導入環境**]パネルが表示されます。
2. 必要な導入環境をリストから選択して、**導入環境の統計**]タブをクリックします。

NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
endpointD1	Endpoint policy	esasecondary - ...	packethybrid - Concent...	Deployed	-	06/27/2024 07:...
ESAd1	ESA policy	esaprimary - ES...	packethybrid - Concent...	Deployed	-	06/24/2024 02:...
SACE-DEPLOY...	SACE_Policy_D...	esaprimary - ES...	loghybrid - Concentrator	Deployed	-	06/24/2024 08:...

3. **導入環境の統計**]ページが表示され、ESAサービスと導入環境のステータスが示されます。

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、導入環境がデータが受信していません。
  - 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、以下の「デプロイされたルールの統計情報」セクションで、無効なルールの詳細を確認してください。無効なルールには赤い円が表示されます。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。

**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。最新バージョンへのアップグレード中、NetWitness Platformは大文字と小文字を区別しないオプションの既存のルールを変更しません。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。

## 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
```

## NetWitnessコミュニティポータルを使用したサポート

NetWitnessコミュニティポータルを使用して、特定のドキュメントを検索したり、アプライアンスのサポート終了に関連する情報を検索したり、ブログを読んだりすることができます。

### 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。
- NetWitness® Platformのブログ投稿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	<a href="https://community.netwitness.com">https://community.netwitness.com</a> メインメニューで <b>[Support]</b> > <b>[Case Portal]</b> > <b>[View My Cases]</b> をクリックします。
各国のお問い合わせ窓口	<a href="https://community.netwitness.com/t5/support/ct-p/support">https://community.netwitness.com/t5/support/ct-p/support</a>
コミュニティ	<a href="https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions">https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions</a>
NW更新	<a href="https://update.netwitness.com">https://update.netwitness.com</a>
LiveUI	<a href="https://live.netwitness.com">https://live.netwitness.com</a>

## 製品ドキュメントへのフィードバック

NetWitness Platformのドキュメントに関するフィードバックは、[nwdocsfeedback@netwitness.com](mailto:nwdocsfeedback@netwitness.com)までメールで送信してください。