RSA NETWITNESS® PLATFORM

NetWitness Endpoint 4.4.0.xから NetWitness Platform 11.3以降への移行ガイド

RSA NetWitness® Platform 11.4

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

はじめに

このガイドでは、既存のNetWitness Endpoint 4.4.0.xをNetWitness Platform 11.3以降に移行する手順について説明します。

移行は大きく分けて次の作業で構成されます。

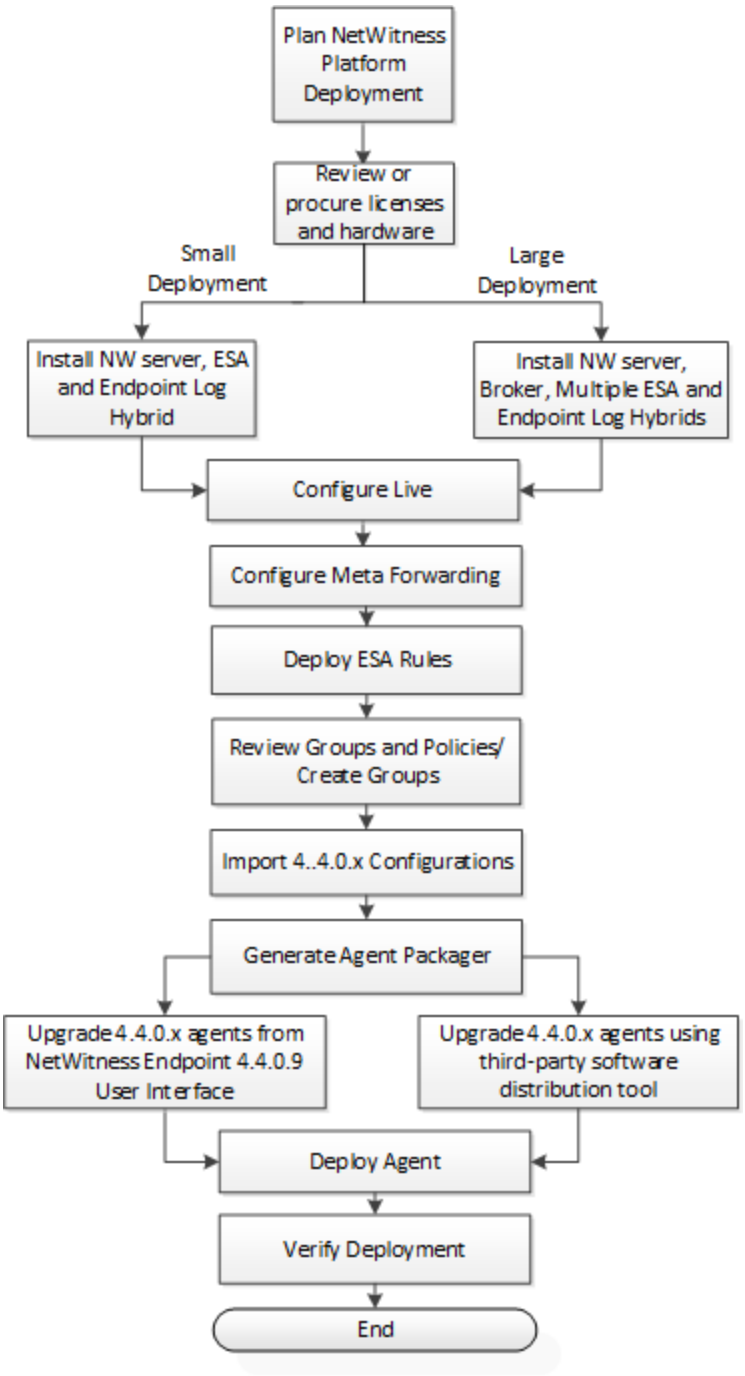
- NetWitness Platformの計画と設定。導入環境のサイジングについては、RSAアカウント マネージャにお問い合わせください。サイジング ガイドラインの詳細については、『*仮想ホスト インストール ガイド*』を参照してください。
- ファイル ステータス、証明書ステータス、ブロックされたハッシュをNetWitness Endpoint 4.4.0.xからNetWitness Platform 11.3以降にインポート。

  注： NetWitness Endpoint 4.4.0.xのSQLデータベースに保存されたEndpointスキャン データおよび追跡データ、ユーザ、IIOC、カスタム クエリ、不正な証明書、不正なドメイン、不正なIP、不正なファイル ハッシュは移行できません。
- 4.4.0.xエージェントの11.3以降へのアップグレード。

NetWitness Endpointの新機能の詳細については、『*リリース ノート*』を参照してください。

移行フローチャート

次のフローチャートは、移行プロセスを示しています。



注： 各ステップの手順は、次のセクションで説明します。

ドキュメントのアクセス方法

NetWitness Platform製品ドキュメントは、次のリンクからアクセスできます。

- HTML - https://community.rsa.com/community/products/netwitness/documentation
- PDF - https://community.rsa.com/community/products/netwitness/113

NetWitness Endpoint 4.4.0.xをNetWitness Platform 11.3以降に移行

ここでは、NetWitness Endpoint 4.4.0.xをNetWitness Platform 11.3以降に移行するために必要なタスクについて説明します。

タスク1 - NetWitness Platformの導入を計画する

1. Endpointアーキテクチャを確認し、エンドポイントの数、分布、場所、エージェントから収集されるデータに基づいて、次のいずれかの導入環境を選択します。詳細については、『*導入ガイド*』の「NetWitness Endpointアーキテクチャ」を参照してください。
   - 小規模導入環境。この環境にはNetWitness Server、Endpoint Log Hybrid、Event Stream Analysis(ESA) が含まれます。
   - 大規模導入環境。この環境には、NetWitness Server、Endpoint Log Hybrid(複数可) 、ESA (複数可) が含まれます。

     複数のEndpoint Log Hybridを導入する場合は、Endpoint Brokerをインストールします。インストールすると、導入環境内の全Endpoint Serverに対して自動的にクエリを実行し、全Endpoint Serverのデータを一元的に表示します。

     注： RSAは、NetWitness BrokerホストにEndpoint Brokerをインストールすることを推奨しています。また、個別のホスト、NetWitness Server、Endpoint Log Hybrid上にもインストールできます。
2. 既存のライセンスとハードウェアを確認し、必要に応じて調達します。

   導入環境に必要なハードウェアがあることを確認します。詳細については、『*物理ホスト インストールガイド*』の「サポートされるハードウェア」を参照してください。

   NetWitness Endpoint 4.4.0.xの既存のライセンスがある場合、新しいライセンスを購入する必要はありません。NetWitness Endpoint 4.4.0.xの既存のライセンスは、NetWitness Platform 11.3以降のライセンスとして、別のシリアル/ライセンス番号が付けられ、myRSAから入手できます。

   詳細については、『*ライセンス管理ガイド*』を参照してください。

タスク2 - NetWitness Platform 11.3以降をセットアップする

1. ファイアウォールでポートを構成します。詳細については、『*導入ガイド*』の「ネットワーク アーキテクチャとポート」を参照してください。
2. 次のNetWitness Platformコンポーネントをインストールします。
   - NetWitness Server
   - Endpoint Log Hybrid

- ESA
- Endpoint Broker(Endpoint Log Hybridが複数の場合)

詳細については、『*物理ホスト インストール ガイド*』を参照してください。

3. NetWitness Endpoint 4.4.0.xのライセンスを持っている場合は、次の手順を実行します。
   - NetWitness Platformがある場合 : 既存のライセンス サーバにエンタイトルメントをマッピングします。
   - NetWitness Platformがない場合 :

     a.NetWitness Platformをインストールします(「タスク2 - NetWitness Platform 11.3以降をセットアップする」を参照)

     b.ライセンス サーバIDを取得します

     c.エンタイトルメントをマッピングします
4. ライセンスが[**管理**]＞[**システム**]＞[**ライセンス**]に反映されていることを確認します。

タスク3 - NetWitness PlatformにEndpointを構成する

- RSA Liveアカウントを構成し、ファイル レピュテーション サービスが有効になっていることを確認します。詳細については、『*Live サービス管理ガイド*』を参照してください。
- ユーザを作成し、適切なロールを割り当てます。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。
- Endpoint Log HybridでEndpointメタの転送先を構成します。詳細については、『*NetWitness Endpoint 構成ガイド*』を参照してください。
- ESAルールを導入します。

  既存のNetWitness Endpoint 4.4.0.x IIOCは、標準のアプリケーション ルールとして提供され、インストール時に自動的に使用可能になります。

  ESA Correlation ServerにEndpoint Concentratorを構成し、リスク スコアを計算するESAコンテンツを導入する必要があります。詳細については、『*ESA構成ガイド*』を参照してください。
- デフォルトのAgent Endpoint(EDR) ポリシーを確認し、必要に応じてグループを作成します。エージェントのログ収集を有効にする場合は、Windowsログ ポリシーを確認して適用します。

  詳細については、『*NetWitness Endpoint構成ガイド*』を参照してください。

タスク4 - NetWitness Endpoint 4.4.0.xの構成をインポートする

NetWitness Endpoint 4.4.0.xからNetWitness Platformにファイル ステータス、証明書ステータス、ブロックされたハッシュをインポートします。詳細については、「NetWitness Endpoint 4.4.0.xの構成をNetWitness Platformにインポート」を参照してください。

タスク5 - その他のNetWitness Endpoint 4.4.0.xの構成を追加する

次の構成は手動で追加する必要があります。

- NetWitness Platformのユーザ インタフェースを使用して、IPアドレスのブラックリストなど、導入環境に必要なフィードをRSA Liveから導入します。
- (オプション) ブラックリストに登録されたIPアドレス、ドメイン、チェックサムなど、エンドポイント メタデータへのタグ付けに使用したい外部脅威フィードがある場合は、『*Liveサービス管理ガイド*』の「カスタム フィードの作成」を参照してください。

  たとえば、ホストまたはファイルからブラックリストに登録されたIPアドレス、ドメイン、ハッシュへの通信をアナリストに通知するには、Log Decoderへのフィードを作成し、調査とアラートで該当するセッションにタグを追加します。
- (オプション) カスタムIIOCを確認し、Endpointルールを作成します。詳細については、『*NetWitness Endpoint構成ガイド*』の「リスク評価のためのカスタムEndpointルール」を参照してください。

タスク6 - エージェントを導入する

1. NetWitness Platform 11.3以降でエージェント パッケージを生成します。
2. エージェント パッケージ(`AgentPackager.zip`) を任意のWindowsマシンにコピーして、11.3以降のエージェント インストーラを生成します。
3. 4.4.0.xエージェントを11.3以降にアップグレードするには、次のいずれかを実行します。
   - NetWitness Endpoint 4.4.0.9 Console Serverをご使用の場合は、エージェント インストーラをNetWitness Endpoint Console Serverにコピーし、NetWitness Endpointのユーザ インタフェースからアップグレードします。
   - 4.4.0.0または4.4.0.8をご使用の場合は、エージェント インストーラをコピーして、サード パーティ製のソフトウェア配布ツールを使用します。
4. エージェントを導入します。

詳細については、『*NetWitness Endpointエージェント インストール ガイド*』を参照してください。

タスク7 - エージェントの移行を検証する

エージェントの移行後に、次の点を検証します。

- エージェントがEndpoint Serverと通信でき、[調査]>[ホスト]ビューに表示されている。
- スキャンを実行し、[調査]>[ホストの詳細]ビューにスナップショットの詳細が表示されることを確認する。
- ホストのメタデータが[調査]>[ナビゲート]ビューと[イベント]ビューに表示されている。

  ログ収集が有効になっている場合は、[ナビゲート]ビューと[イベント]ビューにWindowsログが表示されることを確認する。
- ファイル レピュテーション、ファイル ステータス、リスク スコアが[ホスト]ビューと[ファイル]ビューに表示されている。

詳細については、『*NetWitness Endpoint構成ガイド*』を参照してください。

NetWitness Endpoint 4.4.0.xの構成をNetWitness Platformにインポート

ファイル ステータス、証明書ステータス、ブロックされたハッシュをNetWitness Endpoint 4.4.0.xからNetWitness Platformにインポートするには、MigrationHelper Pythonスクリプトを使用します。

注： MigrationHelper Pythonスクリプトは、Windowsホストでのみ実行する必要があります。

スクリプトはRSA Linkからダウンロードできます。

[**RSA NetWitness Platform**]＞[**Downloads**]＞[**RSA NetWitness Platform**]＞[**Version 11.3**]＞[**Tools**]を選択してください。

前提条件

Pythonスクリプトを実行するには、次の準備が必要です。

- NetWitness Endpoint 4.4.0.xのプライマリ データベースに接続できるWindowsホストに、Python 3.6.x以降をインストールします。
- https://pypi.org/project/pyodbc/#filesからwheelファイルをダウンロードして、次のコマンドを実行し、pyodbcをインストールします。

  ```
  pip install wheel-file.whl
  ```

- Pythonのインストールにjsonおよびos.pathライブラリが含まれていない場合は、対応するwheelファイルをhttps://pypi.org/からダウンロードして、次のコマンドを実行し、これらのライブラリをインストールします。

  ```
  pip install wheel-file.whl
  ```

ファイルおよび証明書ステータスのインポート

注： NetWitness Endpointでの証明書ステータスがグレーリストの場合、NetWitness Platform 11.3以降では証明書ステータスとしてグレーリストが存在しないため、ステータスはエクスポートされません。

1. `MigrationHelper` Pythonスクリプトを実行します。

   注： NetWitness Endpointのプライマリ データベースへのアクセス権を持つ任意のホストからこのスクリプトを実行します。

2. 次の情報を入力します。
   a. データベース サーバのホスト名またはIPアドレス(例 : 10.40.40.10)
   b. データベース名 (例 : ECATPrimary)
   c. データベースの認証情報
3. エクスポートされたファイルを保存するパスを入力し、**Enter**キーを押します。パスが存在していることを確認してください。ファイルと証明書のステータスがJSONファイルにエクスポートされます。
4. Context Hubサーバにログインし、エクスポートされたファイルを`/var/netwitness/contexthub-server/data/`ディレクトリにコピーします。

5. NW Serverで、nw-shellコマンドをコマンド ラインから実行します。

   注： データのインポート中は、NetWitness Platform 11.3以降のすべてのEndpoint Serverがオンラインであることを確認してください。

6. loginコマンドを実行し、認証情報を入力します。
7. 次のコマンドを使用してContext Hub Serverに接続します。

   ```
   connect --service contexthub-server
   ```

8. 次のコマンドを実行してファイル ステータスをインポートします。

   ```
   cd contexthub/file/status/import
   show
   invoke <file path>/FileStatus.json
   ```

   注： <file path>は、ファイルが保存されているContext Hub Server内のパスです。Context Hub Serverは、ESAプライマリ ホストに存在します。

9. 次のコマンドを実行して証明書ステータスをインポートします。

   ```
   cd contexthub/certificate/status/import
   show
   invoke <file path>/CertificateStatus.json
   ```

   注： <file path>は、ファイルが保存されているContext Hub Server内のパスです。Context Hub Serverは、ESAプライマリ ホストに存在します。

10. インポートの進行状況を/var/log/netwitness/contexthub-server/contexthub-server.logファイルで確認します。

    インポートが完了すると、「Imported File status successfully」または「Imported Certificate status successfully」というメッセージがログ ファイルに表示されます。

インポートされた4.4.0.xのブロック済みファイルをブロック解除するには、次の手順を実行します。

1. NW Serverで、nw-shellコマンドをコマンド ラインから実行します。
2. loginコマンドを実行し、認証情報を入力します。
3. 次のコマンドを使用してContext Hub Serverに接続します。

   ```
   connect --service contexthub-server
   ```

4. 次のコマンドを実行してファイル ステータスをブロック解除します。

   ```
   cd contexthub/file/status/unblock
   invoke <checksum of blocked file>
   ```