RSA NETWITNESS® PLATFORM

# 仮想ホスト アップグレード ガイド

バージョン 10.6.6から11.2

## 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、japan.emc.com/legal/emc-corporation-trademarks.htm#rsa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

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、これらの使用許諾契約の条項に同意したものとみなされます。

## 暗号技術に関する注意

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

## 配布

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

2月 2019

# 目次

# 概要

このガイドの手順は、仮想ホストをRSA NetWitness Platform 11.2にアップグレードする場合にのみ適用されます。物理ホストを10.6.6.xから11.2にアップグレードする手順は、『*RSA NetWitness Platform物理ホスト アップグレード ガイド*』を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

NetWitness Platform 11.2は、NetWitness Platformのすべての製品に影響を与えるメジャー リリースです。NetWitness Platformのコンポーネントは、NetWitness Server( Admin Server、Config Server、Integration Server、Investigate Server、Orchestration Server、Respond Server、Security Server、Source Server) 、Archiver、Broker、Concentrator、Context Hub、Decoder、Endpoint Hybrid、Endpoint Log Hybrid、ESAプライマリ、ESAセカンダリ、Log Collector、Log Decoder、Malware Analysis、Reporting Engine、UEBA、Warehouse Connector、Workbenchで構成されます。

11.xのユーザ インタフェースに関する主要な変更については、『*NetWitness Platformスタート ガイド*』を参照してください。11.xのプラットフォームに関する主要な変更については、『*NetWitness Platform導入ガイド*』を参照してください。

NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

**注**：Reporting Engineは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。

## CentOS6からCentOS7へのアップグレード

NetWitness Platform 11.2は、オペレーティング システムの新しいバージョンへのアップグレード( CentOS6からCentOS7) を伴うメジャー リリースです。さらに、11.2プラットフォーム環境は大幅に強化され、現在および将来の物理環境および仮想環境に対応します。これらの変更を適用するには、新しい環境へのアップグレードと機能のアップグレードが必要です。

## RSA NetWitness® Platform 11.2のアップグレード パス

RSA NetWitness® Platform 11.2でサポートされているもっとも古いアップグレード パスはSecurity Analytics 10.6.6.xです。10.6.6.xよりも前のバージョンのNetWitness Platformを実行している場合は、10.6.6.xにアップグレードしてから11.2にアップグレードする必要があります。RSA Linkの『*RSA Security Analytics 10.6.6更新ガイド*』( https://community.rsa.com/docs/DOC-85119) を参照してください。

## サポートされるホストのアップグレード パス

ホストは同じタイプのホストへアップグレードする必要があります。

- RSA物理アプライアンスは同じシリーズのRSA物理アプライアンスへ( すなわち、シリーズ4はシリーズ4へ、シリーズ5はシリーズ5へ)
  11.2では、サード パーティの物理ホストをサポートしていません。
- オンプレミスの仮想アプライアンスからオンプレミスの仮想アプライアンスへ

**注意 :** 11.2へのアップグレードでは、異なるプラットフォームへのアップグレードはサポートされません( たとえば、物理から仮想へのアップグレードはサポートされません) 。

## 11.2でサポートされないハードウェア、導入形態、サービス、機能

次のハードウェア、導入形態、サービス、機能の11.2へのアップグレードはサポートされていません。

- RSA AIO( All in One) アプライアンス
- 複数のNetWitness Serverがある構成
- IPDBサービス
- SAサーバ上に共存するMalware Analysisサービス( Malware Analysis Enterpriseのアップグレードは11.2でサポートされます) 。
- スタンドアロンWarehouse Connectorサービス( 非スタンドアロンのWarehouse Connectorのアップグレードは11.2でサポートされます) 。
- Context Hubサービスの10.6.xでのカスタム ヘルスモニタ ポリシー
  NetWitness 11.2にアップグレードした後、カスタム ポリシーは表示されなくなります。その代わりに、バージョン11.2に固有の、標準提供の「Context Hub Serve Monitoring Policy」がユーザ インタフェースに表示されます。
- DISA-STIG( 米国国防情報システム局セキュリティ技術情報ガイド) のハードニングに対応した導入環境。
- Warehouse Analytics( データ サイエンス)

## ESA( Event Stream Analysis) のアップグレードに関する考慮事項

RSA NetWitness® Platform 11.2では、ESA相関ルールによるシステム生成のアラートを保存および送信する方法が変更されました。11.2では、ESAはすべてのアラートをセントラル アラート システムに送信します。ESA 10.6.6.xのローカルMongoDBストレージは削除されました。

**注意 :** 10.6.6.xでIncident Managementを使用していない場合は、バージョン11.2にアップグレードするかどうかを慎重に検討してください。

ESAホストを11.2にアップグレードするかどうかを判断する際に、次のガイドラインを参考にしてください。10.6.6.x導入環境の構成により異なります。

- 1つのESAホスト( Incident Managementが構成されているかどうかを問わず) の場合 : 11.2.にアップグレードします。
- 複数のESAホストがIncident Managementを使用するよう構成されている場合 : システムは引き続きアラートを一元的に統合します。10.6.6.xのシステムが正確にサイジングされ、想定どおり動作している場合、バージョン11.2にアップグレードできます。
- 複数のESAホストをIncident Managementなしで使用し、個々のESAホストに接続してアラートを表示している場合 : バージョン11.2にアップグレードしないでください。

**注 :** 10.6.6.xでIncident Managementを使用していない場合は、移行スクリプトを実行しないと11.2 Respondコンポーネントで10.6.6.xのESAアラートを表示できません。ESAアラート移行スクリプトを使用して、11.2 Respondコンポーネントが表示できる場所に、これらのアラートを移行します。このスクリプトを実行する方法については、、RSA Linkのナレッジベース記事「*ESA Alert Migration Instructions (ESAアラート移行手順)* 」( https://community.rsa.com/docs/DOC-84102) を参照してください。

## アップグレードのフェーズ分け

RSAは、このセクションの説明に従って、ホストのアップグレードを実行することを推奨します。CentOS7への更新と物理アクセスまたはiDRACアクセスの必要性により、11.2へのアップグレードは通常のアップグレードよりも時間がかかります。

**注意 :** 時間差でアップグレードする場合は、次の点に注意してください。
• 最初にフェーズ1のホストを、表示されている順にアップグレードする必要があります。
• 導入環境全体をアップグレードするまで、一部の機能を使用できない可能性があります。
• 導入環境内のすべてのホストをアップグレードするまでサービス管理機能を利用できません。

### フェーズ1

最初にフェーズ1のアップグレードを実行します。フェーズ1では、次の順序でホストをアップグレードする必要があります。

1. Security Analytics Serverホスト
2. Event Stream Analysisホスト
3. Malware Analysisホスト

4. Brokerホスト( Brokerがない場合は、Concentratorホストをアップグレード)
   11.2 NW Serverの新しいInvestigate機能は10.6.6.xコア サービスと通信できません。このため、フェーズ1でBrokerまたはConcentratorのホストをアップグレードする必要があります。

## フェーズ2

残りのホストをアップグレードします。

RSAでは、次のリスクを低減するため、フェーズ2に記載された順序に従うことを推奨します。

- 調査の一部機能の停止。
- ダウンタイムによる、ネットワークとログの収集停止。

**注:**ダウンストリームのイベント送信先を持つログ収集ホストを除き、フェーズ2に記載された順序でホストをアップグレードする技術上の理由はありません。

フェーズ2のホストは次の順序でアップグレードすることを推奨します。

1. Decoderホスト
2. Concentratorホスト
3. Archiverホスト
4. ログ収集ホスト: LD( Log Decoder) ホスト上のLog Collector、VLC( 仮想Log Collector) 、LWC ( Legacy Windows Collector)
   ログ収集ホストをアップグレードする前に、アップグレードの準備をする必要があります。この準備の過程でキューにイベント データが残っていないことを確認します。これを確認するには、イベント データのダウンストリームの送信先( Log Collector、Virtual Log Collector、Log Decoder) が稼働し、正常に機能している必要があります。

   Log Decoderにダウンストリームのイベント データ送信先がある場合、次の順序でLog Collectorを準備し、アップグレードする必要があります。

   a. 各LD( 一度に1つのLD)

   b. VLCとLWC

   Log Decoderにダウンストリームのイベント データ送信先がない場合は、複数のLD、VLC、LWCをまとめて準備してアップグレードできます。
5. その他のすべてのホスト

次の項目については、「*RSANetWitness Platformホストおよびサービス スタート ガイド*」の「ホストおよびサービスの基本」で、「混在モードでの実行」を参照してください。

- 混在モードで発生する機能ギャップ
- 段階的アップグレードの例

NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

## 混在モードでの調査

混在モードは、一部のサービスが11.2にアップグレードされたが、一部がまだ11.0.0.xまたは10.6.6.xのまま残っている状態です。この状態は、段階的に11.2にアップグレードする場合に発生します。

**注**：調査機能を完全に維持するためには、アップグレードのフェーズ分けに示す順序に従いホストをアップグレードする必要があります。SAサーバをアップグレードすると、11.2 Investigate Serverがインストールされますが、イベント分析ビューにアクセスするには、Brokerホストを11.2にアップグレードする必要があります。Brokerがアップグレードされていない場合、Brokerの横に警告アイコンが表示され、そのBrokerに集計されたデータは表示されません。

すべてのサービスを11.2にアップグレードした後、アナリストが調査を実施する場合、RBAC(ロールベースのアクセス制御)はダウンロード操作に対しても一貫して機能し、制限されたデータにはアクセスできません。

混在モード(一部のサービスが11.2にアップグレードされ、一部はまだ11.0.0.xまたは10.6.6.xの状態)で、アナリストが調査を行う場合、RBACは表示とダウンロードに同一に適用されません。

`sdk.packets`設定を10.6.6.xまたは11.0.0.xサービスで無効にしていない場合、イベントのコンテンツの表示および再構築を制限するSDKメタとロール権限を割り当てられたアナリストが、コンテンツ制限のあるイベントのPCAPをダウンロードできます。他のタイプのダウンロードができたように見える場合、その後、権限の不足によるエラーが生成され、データは保護されたままです。

段階的な更新中、10.6.6.xおよび11.0.x.xサービスで`sdk.packets`設定を無効にして、混在モードの間はすべてのPCAPまたはログをアナリストがダウンロードできないように制限できます。すべてのサービスを11.2に更新して`sdk.packets`を再度有効にした後、すべてのサービスでRBACが一貫して機能します。

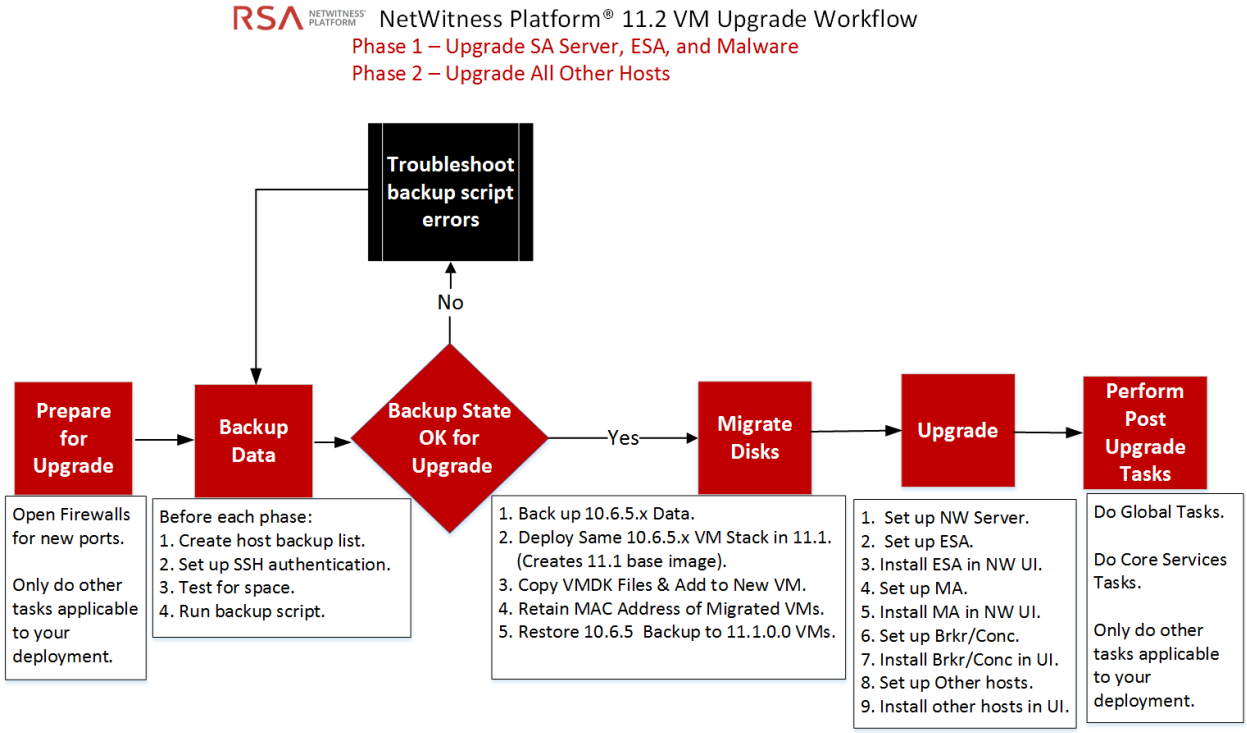
次の表は、バージョン11.2のNWサーバが以前のバージョンのサービスに接続する場合に、[調査]ビューで表示およびダウンロードできる対象を示します。

| 接続するサービスのバージョン | 影響するビュー | 制限コンテンツのあるユーザロール | 参照可能 | 制限コンテンツのダウンロード(正常) | 制限コンテンツのダウンロード(エラー) |
|---|---|---|---|---|---|
| 11.2 Broker -> 10.6.6 x Concentrator -> 10.6.6 Network Decoder/Log Decoder | [イベント]ビュー | Analyst | RBACで許可されたアイテム | PCAP | ファイル アーカイブがダウンロードされますが解凍できません。 |
| | [イベントの再構築]ビュー | Analyst | RBACで許可されたアイテム | PCAP | ファイル アーカイブがダウンロードされますが解凍できません。 |
| | [イベント分析]ビュー | Analyst | RBACで許可されたアイテム | PCAP | サービスからのペイロード取得エラー( ペイロード、リクエスト ペイロード、レスポンス ペイロード) |
| 11.2 Broker -> 11.2 Concentrator ->11.2 Decoder/Log Decoder | [イベントの再構築]ビュー | AnalystとData Privacy Officer | RBACで許可されたアイテム | PCAP | ファイル アーカイブがダウンロードされますが解凍できません。ダウンロードされたPCAPとログは、ゼロ バイトです |

| 接続するサービスのバージョン | 影響するビュー | 制限コンテンツのあるユーザロール | 参照可能 | 制限コンテンツのダウンロード(正常) | 制限コンテンツのダウンロード(エラー) |
|---|---|---|---|---|---|
| 11.2 Broker -> 11.0.0 x Concentrator -> 11.0.0 Network Decoder/Log Decoder | [イベント]ビュー | Analyst | RBACで許可されたアイテム | なし | ファイル アーカイブがダウンロードされますが解凍できません。<br>ダウンロードされたPCAPとログは、ゼロ バイトです |
| | [イベントの再構築]ビュー | Analyst | RBACで許可されたアイテム | なし | ファイル アーカイブがダウンロードされますが解凍できません。<br>ダウンロードされたPCAPとログは、ゼロ バイトです |
| | [イベント分析]ビュー | Analyst | RBACで許可されたアイテム | なし | サービスからのペイロード取得エラー( ペイロード、リクエスト ペイロード、レスポンス ペイロード)<br>ダウンロードされたPCAPとログは、ゼロ バイトです |

## 仮想ホストのアップグレードのワークフロー

次の図は、仮想ホストをRSA NetWitness® Platform 11.2にアップグレードするワークフローを示しています。




## カスタマー サポートへのお問い合わせ

RSA NetWitness Platform 11.2に関する支援が必要な場合には、RSAカスタマー サポート (support@rsa.com) にお問い合わせください。

# アップグレード準備タスク

NetWitness Platform 11.2に更新するには次のタスクを実行します。タスクは、次のカテゴリに分類されます。

- グローバル
- Respond
- Reporting Engine

## グローバル

NetWitness Platformを導入する方法や使用するコンポーネントに関係なく、これらのタスクを完了する必要があります。

### タスク1：コア ポートを確認してファイアウォール ポートを開く

次の表は、11.2の新しいポートです。

**注意**：ポートに接続できないことが原因でアップグレードが失敗しないよう、アップグレード前に新しいポートを開いて、テストしてください。

#### NW Serverホスト

| ソース ホスト | 宛先ホスト | 宛先ポート | コメント |
|---|---|---|---|
| NWホスト | NW Server | TCP 4505、4506 | Saltマスター ポート |
| NWホスト | NW Server | TCP 27017 | MongoDB |
| 管理ワークステーション | NW Server | TCP 15671 | RabbitMQ管理UI |
| NWホスト | NW Server | TCP 15671 | RabbitMQ管理UI |

#### ESAホスト

| ソース ホスト | 宛先ホスト | 宛先ポート | コメント |
|---|---|---|---|
| NW Server、NW Endpoint、ESAセカンダリ | ESAプライマリ | TCP 27017 | MongoDB |

#### Endpoint HybridまたはEndpoint Log Hybrid

| ソース ホスト | 宛先ホスト | 宛先ポート | コメント |
|---|---|---|---|
| Endpoint HybridまたはEndpoint Log Hybrid | NW Server | TCP 5672 | メッセージ バス |
| Endpoint Server | NW Server | TCP 27017 | MongoDB |

すべてのNetWitness Platformコア ポートは、「*RSA NetWitness® Platform*導入ガイド」の「ネットワーク アーキテクチャとポート」トピックに記載されています。NetWitness Platformサービスとファイアウォールを再構成する場合には参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

### タスク2: 10.6.6.xの`admin user`のパスワードの記録

10.6.6.x の`admin user`のパスワードを記録します。このパスワードは、アップグレードを完了するために必要です。

### タスク3: `/etc/fstab` ファイルのバックアップの作成

`/etc/fstab`ファイルをすべてのVMからローカル マシン( バックアップ ホストまたはリモート マシン) にコピーします。

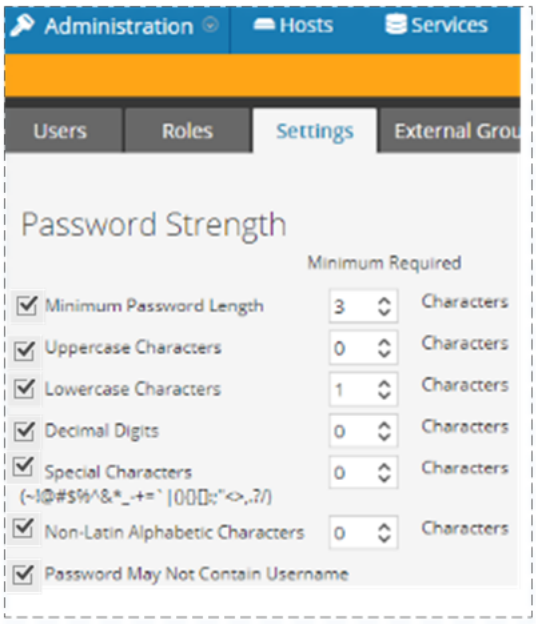
**注:** このファイルは、VMに外部ストレージを再マウントする際に必要です。

## タスク4：10.6.6.xでパスワードの強度設定のチェックボックスがオンになっていることを確認

10.6.6.xで[**管理**]＞[**セキュリティ**]＞[**設定**]タブの[**パスワードの強度**]セクションのチェックボックスをオンにしておく必要があります。オフの場合は、設定が11.2に移行されません。

次のタスクを実行し、10.6.6.xの[パスワードの強度]セクションの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。

1. Security Analytics 10.6.6.xで、[**管理**]＞[**セキュリティ**]＞[**設定**]タブの順に進みます。
2. [**パスワードの強度**]セクションの各設定の左側のチェックボックスがすべてオンになっていることを確認します。オンになっていない場合は、オンにして[**適用**]をクリックします。
   次の例では、すべてのチェックボックスがオンになっています(11.2にアップグレードする前に10.6.6.xで必須)。



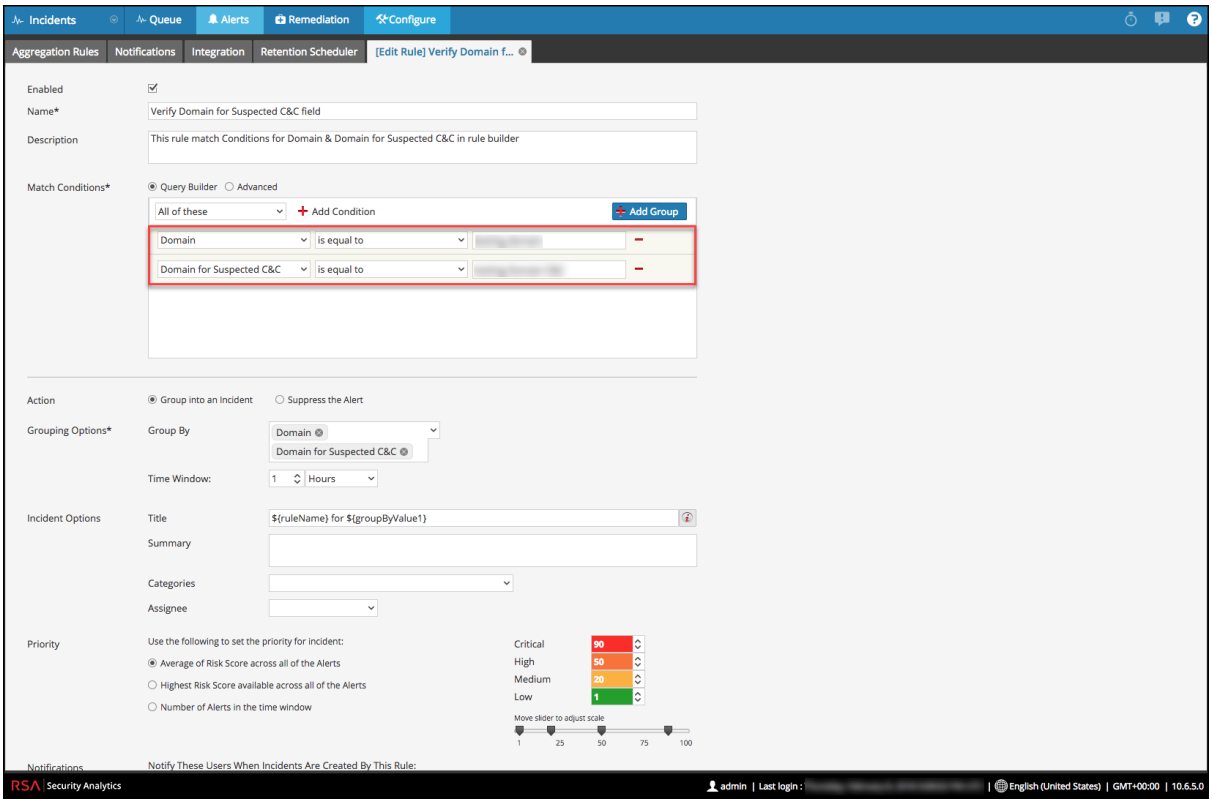
# Respond

## タスク5:「Domain」または「Domain for Suspected C&C」を使用した統合ルールの一致条件を確認

ルールビルダのドロップダウンリストで、一致条件の中で「Domain」または「Domain for Suspected C&C」を使用したIncident Management統合ルールがないか確認します。NetWitness Platform 11.2では、11.2にアップグレードした後にこれらの条件を再度追加する必要があります(「アップグレード後のタスク」の「Respond」セクションを参照)。

以下の手順で各統合ルールを確認します。

1. Security Analytics 10.6.6.xで、[**インシデント**]>[**構成**]>[**統合ルール**]タブの順に進み、一致条件を表示するためにルールを編集します。
2. [**一致条件**]セクションで、条件のドロップダウンリストから[**Domain**]または[**Domain for Suspected C&C**]を選択しているものがないか探します。



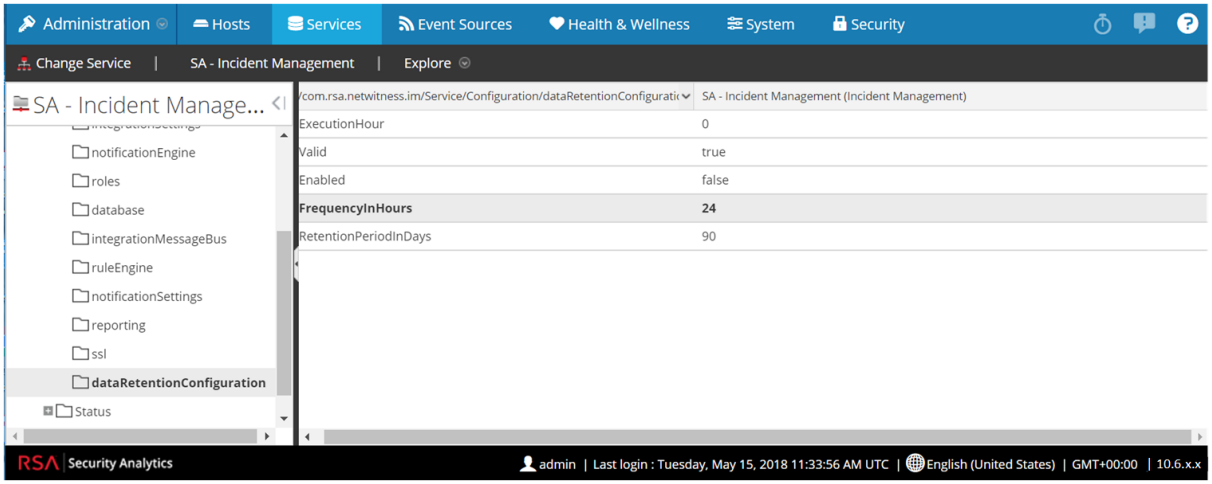

3. 該当する場合は、ルール名と、[**Domain**]または[**Domain for Suspected C&C**]を使用する条件の全体(演算子や値を含む)を記録します。

## タスク6: データ保存の実行間隔を24時間以上に設定

Security Analytics 10.6.xでは、データ保存の実行間隔の最小値はチェックされません。11.2では、少なくとも24時間以上の間隔で実行するようチェックが追加されました。11.2にアップグレードする際、この値が24時間未満の場合、Respondサービスは開始されません。

11.2にアップグレードした後にRespondサービスが開始されるよう、次のタスクを完了します。

1. Security Analytics 10.6.6.xで、[**管理**]＞[**サービス**]にアクセスします。
2. **Incident Management**サービスを選択し、  ＞[**表示**]＞[**エクスプローラ**]を選択します。
3. Incident Managementの[**エクスプローラ**]ビューで、`Service` ＞`Configuration` ＞`dataRetentionConfiguration`にアクセスします。
4. `FrequencyInHours`パラメータが24以上であることを確認します。



## Reporting Engine

### (オプション) タスク7: 外部ストレージのリンク解除

Reporting Engineに外部ストレージ(レポート格納用のSAN(Storage Area Network)またはNAS(Network Attached Storage)など)が接続されている場合は、次の手順を実行してストレージのリンクを解除する必要があります。

次の手順を実行します。

- `/home/rsasoc/rsa/soc/reporting-engine/`は、Reporting Engineのホーム ディレクトリです。
- `/externalStorage/`は、外部ストレージのマウント ポイントです。

1. Reporting EngineのホストにSSHで接続し、`root` の認証情報でログインします。
2. Reporting Engineサービスを停止します。
   ```
   stop rsasoc_re
   ```
3. `rsasoc`ユーザに切り替えます。
   ```
   su rsasoc
   ```
4. Reporting Engineのホーム ディレクトリに移動します。
   ```
   cd /home/rsasoc/rsa/soc/reporting-engine/
   ```
5. 外部ストレージをマウントした`resultstore`ディレクトリのリンクを解除します。
   ```
   unlink /externalStorage/resultstore
   ```
6. 外部ストレージをマウントした`formattedReports`ディレクトリのリンクを解除します。
   ```
   unlink /externalStorage/formattedReports
   ```

# バックアップ手順

Security Analytics 10.6.6.xからNetWitness Platform 11.2にアップグレードする最初のステップは、10.6.6.xのすべてのホストの構成データをバックアップすることです。

**注:** 1.) カスタム証明書ファイルおよびその他すべてのCA(認証局)ファイルを/root/customcertsフォルダに配置して、これらの証明書ファイルが確実にバックアップされるようにしてください。このディレクトリに配置されているカスタム証明書ファイルは、アップグレード中に自動的にリストアされます。11.2にアップグレードした後、カスタム証明書ファイルは/etc/pki/nw/trust/importに配置されます。これらのファイルタイプのバックアップの詳細については、「すべてのホスト タイプ」のステップ1を参照してください。2.) バックアップを開始する前に、PKI(公開鍵基盤)の設定を無効にします。

**注意:** 次のサービスは、10.6.6.xのバックアップおよびアップグレード プロセスではサポートされません。
- IPDB
- All in Oneサーバ
- Security Analyticsサーバ上に共存するMalware Analysis
- スタンドアロンのWarehouse Connector
- Warehouse Analytics(Datascience)

次のタイプのホストは、バックアップして、アップグレード中に自動的にリストアすることができます。

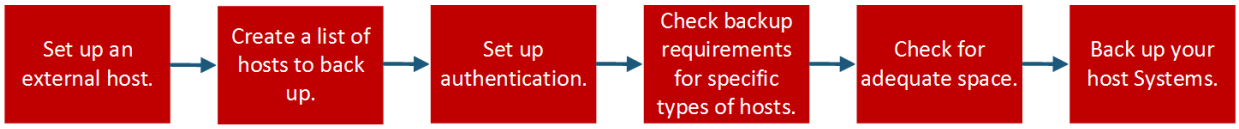
- **Security Analytics Admin Server**
- **Malware Analysis(スタンドアロン)**
- **Archiver**
- **Broker**
- **Event Stream Analysis**(Context HubとIncident Managementデータベースを含む)
- **Concentrator**
- **Log Decoder**(ローカルLogCollectorとWarehouse Connector(インストールされている場合)を含む)
- **Log Hybrid**
- **Network Decoder**(インストールされている場合は、Warehouse Connectorを含む)
- **Network Hybrid**
- **Virtual Log Collector**

次のタイプのファイルは、自動的にバックアップされますが、アップグレード後に手動でリストアする必要があります。

- PAM構成ファイル: PAM構成ファイルをリストアする方法については、「*アップグレード後のタスク*」の「グローバル」セクションにある「タスク5: 11.2でのPAM(Plugable Authentication Module)の再構成」を参照してください。
- /etc/pfring/mtu.confおよび/etc/init.d/pf_ring: これらのファイルをリストアするには、手動でファイルを取得する必要があります。/etc/pfring/mtu.confファイルは/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.confに、/etc/init.d/pf_ringファイルは/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ringに配置されます。これらのファイルをリストアする方法につ

いては、「*アップグレード後のタスク*」の「ハードウェア関連タスク」セクションにある「(オプション) タスク 2: 10G Decoderのファイルのリストア」を参照してください。

次の図は、ホストのバックアップを実行するタスクのフローの概要を示しています。




次のセクションで、これらのタスクについて説明します。

- タスク1: ファイルをバックアップするための外部ホストのセットアップ
- タスク2: バックアップするホストのリストの作成
- タスク3: バックアップ ホストとターゲット ホストの間での認証の設定
- タスク4: 特定のタイプのホストのバックアップ要件の確認
- タスク5: バックアップ用のディスク容量のチェック
- タスク6: ホスト システムのバックアップ
- バックアップ後のタスク

## タスク1: ファイルをバックアップするための外部ホストのセットアップ

ファイルのバックアップに使用する外部ホストをセットアップする必要があります。このホストはCentOS 6を実行し、Security Analyticsの各ホストにSSHで接続する必要があります。

**注:** ファイルのバックアップに外部ホストを使用できない場合は、RSAカスタマー サポートにお問い合わせください。

外部ホストからバックアップ対象のシステムのホスト名を、DNSまたは`/etc/hosts`ファイルにより解決できることを確認します。

**注:** バックアップ スクリプトは、CentOS 6でのみ実行するよう設計されています。バックアップ スクリプトは、CentOS 6のマシンで実行する必要があります。

バックアップ中にいくつかのスクリプトが実行されます。RSA Link( https://community.rsa.com/docs/DOC-81514) から、スクリプト (`nw-backup-v4.1.zip`以降) を含むzipファイルをダウンロードし、CentOS 6のバックアップ システムにコピーする必要があります。zipファイルを解凍して、スクリプトにアクセスします。次のスクリプトが含まれます。

- `get-all-systems.sh`:`all-systems`ファイルを作成します。このファイルには、バックアップするすべてのSecurity Analyticsサーバとホスト システムの一覧が含まれます。

  **注意:** 混在モードでアップグレードを実行する場合は、導入環境のすべてのホストを11.2にアップグレードするまで、`all-systems`ファイルのマスター コピーを保存しておきます。混在モードでは、最初にNW Serverをアップグレードする必要がありますが、アップグレード後のNW Serverのオペレーティング システムはCentOS7になるため、`get-all-systems.sh`を再度実行することはできません。

- `ssh-propagate.sh`: バックアップ対象のシステムとバックアップ ホスト システム間のキー共有を自動化し、パスワードの入力プロンプトが何度も表示されないようにします。
- `nw-backup.sh`: ホストのバックアップを実行します。
- `azure-mac-retention.ps1`: Azureを使用している場合にのみ必要です。詳細については、「*Azure導入ガイド*」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

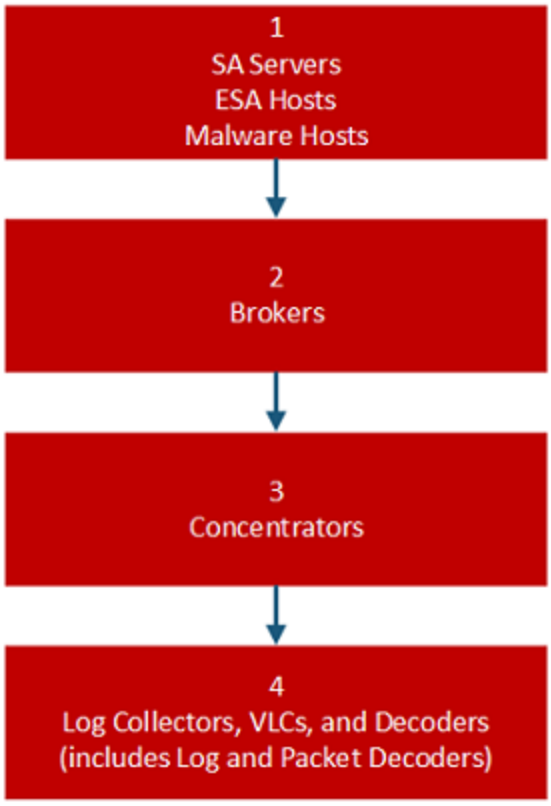
**注**: 10.6.6ホストで、バージョン10.6.xのバックアップとリストア スクリプトを既に使用している場合でも、ここにリストされているすべてのスクリプトを実行する必要があります。

**注**: 通常のバックアップでは`nw-backup-v4.1.zip`ファイルのスクリプトを使用しないでください。これらのスクリプトは、10.6.6.xから11.2へのアップグレード専用に設計されています。

**注**: バックアップ スクリプトは、STIGのハードニングが適用されたホストのデータ バックアップをサポートしません。

## タスク2: バックアップするホストのリストの作成

ファイルをバックアップするために使用するスクリプトは、all-systemsファイルとall-systems-master-copyファイルを参照します。これらのファイルには、バックアップするホストのリストが含まれます。all-systems-master-copyファイルには、すべてのホストのリストが含まれています。all-systemsファイルは、バックアップ セッションごとに使用され、特定のセッションでバックアップするホストのみが含まれます。これらのファイルはget-all-systems.shスクリプトを実行して生成します。RSAでは、一度にすべてのホストをバックアップするのではなく、グループに分けてバックアップすることを推奨します。バックアップ セッションで推奨されるホストの順序とグループを、次の図に示します。




各バックアップ セッションではホストを5台に制限し、バックアップ ファイル用のディスク領域が不足しないようにします。all-systems-master-copyファイルを参照しながら、バックアップ セッション用のall-systemsファイルを作成します。all-systemsファイルを手動で編集し、対象のホストが含まれるようにします。

### all-systemsファイルおよびall-systems-master-copyファイルを生成するには、次の手順を実行します。

1. バックアップを実行するホストで、次のコマンドを実行し、get-all-systems.shスクリプトを実行可能にします。
   ```
   chmod u+x get-all-systems.sh
   ```
2. rootレベルで、get-all-systems.shスクリプトを次のように実行します。
   ```
   ./get-all-systems.sh <IP-Address-of-SA-Admin-Server>
   ```
   ホストごとに1回、ホスト システムのパスワードの入力を求められます。
   このスクリプトがall-systemsファイルとall-systems-master-copyファイルを/var/netwitness/database/nw-backup/に保存します。

3. all-systemsファイルとall-systems-master-copyファイルに、正しいホストが含まれていることを確認します。
4. バックアップしたいシステムのみが含まれるよう、all-systemsファイルを編集します。all-systems-master-copyファイルを参照しながら、all-systemsファイルをエディタ( viなど) で開き、バックアップしたいシステムのみを含むように変更します。バックアップしないホストはコメント アウトすることを推奨します( バックアップしないホストの行の先頭にシャープ記号( #) を追加) 。
   次の例では、10.6.6 Security Analyticsサーバをコメント アウトしています。
   ```
   loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fa1d18d8,10.6.6.0
   #nwserver,nwserv106,172.31.255.23,67a9a0eb-1300-4fba-838f-7be4d8cf5e65,10.6.6.0
   ```

   **注 :** viを使用する場合は、all-systemsファイルへのパスを必ず指定してください。

all-systems-master-copyファイルの例を以下に示します。

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.6.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.6.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-c003cdfcd7a6,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-1cb2fe60077a,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-e0d02aa0a2fd,10.6.6.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-d8141b78a192,10.6.6.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.6.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.6.0
```

以下は、最初のバックアップ セッションで使用するall-systemsファイルの例で、Security Analyticsサーバ、ESAホスト、Malware Analysisホストのみがバックアップされます。

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.6.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.6.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-c003cdfcd7a6,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-1cb2fe60077a,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-e0d02aa0a2fd,10.6.6.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-d8141b78a192,10.6.6.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.6.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.6.0
```

## トラブルシューティング情報

- all-systemsファイルとall-systems-master-copyファイルのコピーを安全な場所に保存しておきます。以下の推奨事項に従ってください。

  - all-systems-master-copyファイルは編集しないでください。
  - all-systemsファイルを複数バージョン作成する場合(複数のバックアップ セッションを使用する場合など)、現在バックアップするホストのみをリストに追加し、その他のホストはコメント アウトするようにします。詳細については、「バックアップ後のタスク」を参照してください。

- get-all-systems.shスクリプトを実行中にダウンしているホスト システムがある場合、スクリプトは、情報が見つからないホストのリストを作成します。スクリプトが完了し、all-systemsファイルが作成されたら、all-systemsファイルを手動で編集し、不足しているホストの情報を追加する必要があります。

- get-all-systems.shスクリプトは、Security Analyticsユーザ インタフェースに定義されたホストのリストを生成します。すべてのホストとサービスが正常にシステムに追加されていることを確認します。正常にシステムに追加されていないホストやサービスがある場合、それらはバックアップされません。RSAでは、ホストおよびサービスをSecurity Analyticsシステムに追加するときには、正常に追加されるよう、Security Analyticsユーザ インタフェースを使用して追加することを推奨しています。ただし、ユーザ インタフェースに定義されていないホストまたはサービスがある場合は、手動でall-systemsファイルに追加する必要があります。

- get-all-systems.shスクリプトは、最後に、Security Analyticsサーバのリストに含まれるシステムと、必要な情報を取得できたシステムの間の相違を確認します。情報を取得できないノードIDまたはシステム名のリストが表示された場合は、それらのシステムが存在すること、それらのサービスがすべて実行中であること、Security Analyticsサーバと正しく通信していることを確認します。(Windows Legacy CollectorまたはAWSクラウドCollectorはall-systemsファイルに追加されないため、不一致の原因となる可能性があります。**これらは、手動でall-systemsファイルに追加しないでください。**)
- all-systemsファイルの構文が正しくない場合、スクリプトは失敗します。たとえば、ホスト エントリーの前後に余分なスペースがある場合、スクリプトは失敗します。

## タスク3: バックアップ ホストとターゲット ホストの間での認証の設定

RSAでは、ssh-propagate.shスクリプトを実行し、バックアップ ホストとホスト システムの間のキー共有を自動化することを推奨します。

**注:** パスフレーズで保護されるSSHキーがある場合、ssh-agentを使用して時間を節約できます。詳細については、ssh-agentのマニュアル ページを参照してください。

次のタスクを実行して、バックアップ ホストとターゲット ホスト間の認証を設定します。

1. バックアップ用の外部ホスト システムで、次のコマンドを実行してssh-propagate.shスクリプトを実行可能にします。
   ```
   chmod u+x ssh-propagate.sh
   ```
2. ルート ディレクトリで次のコマンドを実行します。<path-to-all-systems-file>はall-systemsファイルが保存されているディレクトリへのパスです。
   ```
   ssh-propagate.sh <path-to-all-systems-file>
   ```
3. ホストごとに1回、パスワード入力を求められますが、バックアップ中に繰り返し入力する必要はなくなります。

## タスク4: 特定のタイプのホストのバックアップ要件の確認

バックアップに使用するall-systemsファイルを作成した後、バックアップを実行する前に、ファイルに記載されたホストのいずれかに固有の要件がないか確認する必要があります。

### すべてのホスト タイプ

すべてのホスト タイプで、次の手順を実行します。

1. Security Analyticsサーバ上で、カスタム証明書ファイルと他のすべてのCA(認証局)ファイルを/root/customcertsフォルダに配置し、これらの証明書ファイルが確実にバックアップされるようにします。このディレクトリに配置されているカスタム証明書ファイルは、アップグレード中に自動的にリストアされます。11.2へのアップグレード後、カスタム証明書ファイルは/etc/pki/nw/trust/importに配置されます。
   CA証明書とキーは、特定のタイプのサーバまたはソフトウェアとの互換性を維持するため、OpenSSLを使用してさまざまな形式に変換できます。たとえば、Apacheで使用するPEMファイルをPFX(PKCS#12)ファイルに変換し、TomcatやIISで使用できます。ファイルを変換するには、SSHでSecurity Analyticsサーバに接続し、変換のタイプに応じて次のコマンドを実行します。
   **DERファイル(.crt .cer .der)をPEMに変換**
   ```
   openssl x509 -inform der -in certificate.cer -out certificate.pem
   ```
   **PEMファイルをDERに変換**
   ```
   openssl x509 -outform der -in certificate.pem -out certificate.der
   ```
   **PEM証明書ファイルと秘密キーをPKCS#12(.pfx .p12)に変換**
   ```
   openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
   certificate.crt -certfile CACert.crt
   ```
   **秘密キーと証明書を含むPKCS#12ファイル(.pfx .p12)をPEMに変換**
   ```
   openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
   ```

**注**:次のパラメータをコマンドに追加します。
`-nocerts`は、秘密キーのみを変換します。
`-nokeys`は、証明書のみを変換します。

2. CentOS 7に更新後にリストアするために、CentOS 6で行ったすべてのカスタム構成(例:ドライバのカスタマイズ)を手動で記録します。CentOS 6へのカスタム構成は、自動的にバックアップもリストアもされません。

## Mongoデータベースのあ るESAホスト

デフォルトの10.6.x Mongoデータベースのパスワードは`netwitness`です。このパスワードを変更した場合、バックアップ スクリプトの実行中にエラーが発生する可能性があります。バックアップでカスタムMongoデータベース パスワードを使用するか、または、パスワードを`netwitness`に戻してから`nw-backup.sh`スクリプトを実行できます。

1. Mongoデータベース パスワードが`netwitness`であるか、または変更されているかを確認します。
2. 変更されている場合、`netwitness`に戻すか、または変更されたパスワードを把握しておき、バックアップ中に入力できるようにします。

## Decoder、Concentrator、Brokerホスト:データ収集と集計の停止

「すべてのホスト タイプ」で説明するタスクに加え、Decoderホスト、Concentratorホスト、Broker ホストについては、バックアップするすべてのシステムでデータ収集と集計を停止します。手順については、「付録B:データ収集と集計の停止と再開」を参照してください。

## LC(Log Collector)とVLC(Virtual Log Collector):`prepare-for-migrate.sh`の実行

**注意**:このタスクはログ収集を停止するため、収集できないイベントを最小限にするようアップグレードの直前に実行する必要があります。このガイドに記載されているバックアップとアップグレードのタスクに従って、このタスクを完了します。

### 前提条件

LCとVLCのアップグレードの準備をする前に、次の情報が必要です。

- LockboxがLCとVLCで初期化されている場合、Lockboxのパスワードを把握しておく必要があります。アップグレード後に、Lockboxを再構成する必要があります。
- RabbitMQの`logcollector`ユーザのパスワードを設定した場合は、アップグレード後に再度設定するためにパスワードを把握しておく必要があります。

### アップグレードのためのLCとVLCの準備

次のタスクを実行して、アップグレードするLog CollectorとVirtual Log Collectorを準備します。

1. Log CollectorにSSHでログインします。
2. 次のコマンドを実行します。
   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```
   このコマンドは次の処理を行います。

- Puppet Agentサービスを停止します。
- Log Collectorにログ ファイルをアップロードするために使用するファイル収集アカウント(「sftp」ユーザと「upload」グループのすべてのユーザ)を無効化します。ログ ファイルは、Log Collectorが11.2にアップグレードされるまで、イベント ソースに蓄積されます。
- Log Collectorサービス上ですべての収集プロトコルを停止します。
- プラグイン アカウントとRabbitMQアカウントのリストを保存します。
- 新しいイベントが発行されないよう、RabbitMQサーバを構成します。ショベルやLog Decoder Event Processorなどの、キューに溜まったイベントのconsumerは、動作を継続します。
- Log Collectorのキューが空になるまで待機します。
- Log Collectorサービスを停止します。
- Log Collectorが正常にアップグレードの準備ができたことを示すマーカー ファイルを作成します。

#### トラブルシューティング情報

`prepare-for-migrate.sh` スクリプトは、次の処理を行います。

- 情報、警告、エラー メッセージをコンソールに送信します。
- セッション ログを`/var/log/backup/`ディレクトリに保存します。

次のエラーが発生した場合は、エラーを修正し、準備を再開する必要があります。支援が必要な場合は、RSAカスタマー サポートにお問い合わせください。

- Log Collectorのキューにイベントが残っているのに、Consumerが見つからない。
- Puppet Agentサービスを停止できない。
- Log Collectorサービスの収集プロトコルを停止できない。
- RabbitMQサーバへのイベント公開をブロックできない。
- キューに登録されたイベントを処理できないか、処理に時間がかかりすぎている。スクリプトはイベントの処理の完了確認を30回まで試行します。毎回の試行の後、30秒間スリープします。
- Log Collectorサービスを停止できない。

トラブルシューティングの詳細については、「付録A:トラブルシューティング」を参照してください。

## Web Threat Detectionとの統合、Archer Cyber Incident & Breach ResponseまたはNetWitness Endpointとの統合:RabbitMQユーザ名とパスワードの一覧表示

11.2.へのアップグレード後にRabbitMQのユーザ アカウントをリストアできるように、10.6.6.xのSecurity Analyticsサーバ ホストで、RabbitMQのすべてのユーザ名とパスワードのリストを取得する必要があります。

RabbitMQのユーザ名とパスワードのリストを取得するには、次のコマンドを実行します。

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

RabbitMQのユーザ アカウントをリストアするには、「*アップグレード後のタスク*」の「タスク2:Web Threat Detection、NetWitness SecOps ManagerまたはNetWitness Endpointとの統合のためのSSL相互認証の構成」を参照してください。

### Bluecoat イベント ソース

Bluecoat ProxySGイベント ソースでは、FTPSプロトコルを使用して、ログ ファイルをLC( Log Collector) およびVLC( Virtual Log Collector) にアップロードします。イベント ソースに関するドキュメントには、LCおよびVLC上でVSFTPDサービスを構成する手順が記載されています。

- キー要素が10.6.6.xの`/root/vsftpd/`ディレクトリに存在する場合、バックアップおよびリストアされます。**キー要素が別の場所にある場合、手動でバックアップおよびリストアする必要があります。**
- `/etc/vsftpd/vsftpd.conf`ファイルが10.6.6.xに存在する場合、ファイルはバックアップおよびリストアされます。

## タスク5: バックアップ用のディスク容量のチェック

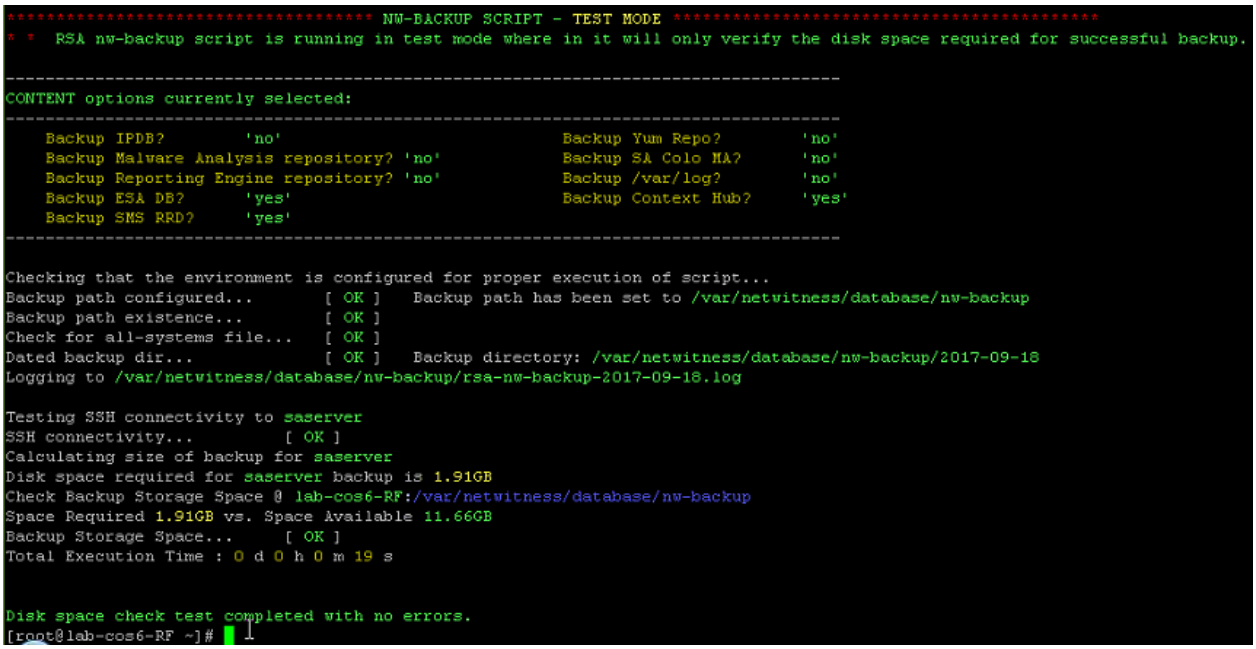
「テスト オプション」に記載されている`-t`オプションを指定してバックアップ スクリプトを実行すると、バックアップに必要なディスク容量を確認できます。スクリプトは、実際にファイルをバックアップしたり、すべてのサービスを停止することなく実行できます。RSAでは、すべてのデータを収集できるように、この手順を実行してバックアップ用に十分なディスク容量があることを確認することを推奨します。

次のタスクを実行して、十分なディスク容量があることを確認します。

1. 次のコマンドを実行して、バックアップ スクリプトを実行可能にします。
   ```
   chmod u+x nw-backup.sh
   ```
2. ルート ディレクトリレベルで次のコマンドを実行します。
   ```
   ./nw-backup.sh -t
   ```
   出力には、バックアップに必要なディスク容量が表示されます。

> **注:** デフォルトでは、`./nw-backup.sh -t`コマンドは`-d`オプションで実行されます。ただし、より正確なディスク容量を知りたい場合は、`-D`を指定し、`-d`オプションを上書きできます。`-D`オプションを指定すると、バックアップに必要なディスク容量がホストごとに表示されます。ただし、現在使用可能なディスク容量は表示されません。使用可能な容量が足りない場合、`-D`オプションはエラーを返します。外部ホスト上の使用可能な容量を知りたい場合は、`df -h`コマンドを実行します。

次の図は、`-t`オプションを使用した出力の例を示しています。




## タスク6：ホスト システムのバックアップ

バックアップ スクリプトを実行して実際にバックアップする前に、十分なディスク容量があることを確認します。ホストをバックアップするには、`-u`オプションを指定して`nw-backup.sh`スクリプトを実行します。このオプションは、11.2へのアップグレードに必須です。

**注**：スクリプトは、実行時にサービスを停止します。ただし、必要な場合は、スクリプトを実行する前に手動でサービスを停止できます。

バックアップ スクリプトの実行時に、次のセクションで説明するオプションを指定できます。

### 使用方法

```
./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>
```

### 一般オプション

```
-u : This option is required for upgrading to 11.2. Enables the upgrade flag to run backup for upgrading to 11.2. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)

-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)

-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)

-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)

-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)

-x : move all backup files to an external mount point. Default: (no) - COPY
```

```
-b <path to write backups> : path to the location for storing backup files on
a backup server. For upgrading to 11.2, please use the default location!
Default: (/var/netwitness/database/nw-backup)
```

**注 :** アップグレード ( -u) モードでは、バックアップ パスを変更しないでください。

**注 :** -uオプションでバックアップを実行すると、すべてのサービスが停止します。バックアップの実行後も引き続き10.6.xマシンを使用する必要がある場合は、10.6.xホストをリブートし、サービスを再起動します。

### 詳細なコンテンツ選択オプション

```
-c : back up Colocated Malware Analysis on SA servers. Default: (no)
-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)
-m : back up Malware Analysis File Repository. Default: (no)
-r : back up Reporting Engine Report Repository (automatically set if -u is
used). Default: (no)
-v : back up system logs (/var/log). Default: (no)
-y : back up YUM Web Server & RPM Repository. Default: (no)
-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)
-C : If set: DISABLES back up of Context-Hub configuration and database.
Default: (not-set)
-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)
```

### テスト オプション

```
 -t : performs script test run for disk space check only. Services are not
stopped and excludes execution of backup. Can be combined with (-d) or (-D)
and other flags. Default: (-t)
```

コマンドの例 :

```
./nw-backup.sh
```

このコマンドは、スクリプト自身のヘッダーに設定されているオプションを使用してバックアップを実行します。

コマンドの例 :

```
./nw-backup.sh -ue /mnt/external_backup
```

このコマンドは、スクリプトに指定したバックアップ パスを使用し、次のオプションを使用して通常のバックアップを実行します。

```
-u : enables the upgrade flag to run backup for upgrading to 11.2. It also
enables disk space check (-d), backing up reporting engine reports (-r) and
stores backup content locally (-l). Default: (no)
-e : Copy the backup files to external mount point, mounted on /mnt/external_
backup
For Help: ./nw-backup.sh -h
```

スクリプトの実行時に、次のテキストがスクリプトの上部に表示されます。

**注意：**RSA nw-backupスクリプトは、スクリプトに指定されたオプションに基づいて、構成ファイル、データ、およびログをバックアップします。バックアップ ファイルをバックアップ サーバに保存したり、マウント ポイント( USB/NFS/SMB) 上の外部ストレージに移動またはコピーしたり、ターゲット ホストに安全にコピーするためのオプションを使用して、コンテンツを作成します。
このバックアップ スクリプトは、次のバージョンのSecurity Analyticsで検証されています。
10.6.6.x
このスクリプトを他のバージョンで使用した場合、想定した結果が得られない可能性があります。また、RSAカスタマー サポートではサポートできない可能性があります。
**注：** RSAが提供していないすべてのカスタム ファイル、スクリプト、cronジョブ、およびその他の重要なファイルをバックアップに含めるには、/root、/home/'user'、または/etcに配置する必要があります。

ホストをバックアップするには、次のタスクを実行します。

1. all-systemsファイルにバックアップするホストのみが含まれていることを確認します。詳細については、「タスク2：バックアップするホストのリストの作成」を参照してください。
2. 次のコマンドを実行して、バックアップ スクリプトを実行可能にします。
   ```
   chmod u+x nw-backup.sh
   ```
3. ルート ディレクトリレベルで次のコマンドを実行して、バックアップ プロセスを開始します。
   ```
   ./nw-backup.sh -u
   ```

   **注：**11.2へのアップグレード中にファイルが正しくリストアされるよう、-uオプションを使用する必要があります。アップグレードでは規定のパスを使用し、規定の場所にデータを格納する必要があるため、バックアップ スクリプトのヘッダーでバックアップ パスを変更しないでください。

   「Backup completed with no errors」が表示されれば、バックアップは正常に完了しています。

   次のような名前のログ ファイルがバックアップ ディレクトリに作成され、バックアップされたファイルに関する情報が提供されます。
   ```
   rsa-nw-backup-2018-03-15.log
   ```
4. バックアップが完了したら、目的のファイルがバックアップされたことを確認するために、次のコマンドを実行してバックアップされたすべてのファイルのリストを参照します。
   ```
   tar -tzvf hostname-ip-address-backup.tar.gz
   ```
   次のアーカイブ ファイルが作成されます。
   すべてのホスト：
   ```
   <hostname-IPaddress>-root.tar.gz
   <hostname-IPaddress>-backup.tar.gz
   tar checksumファイル
   <hostname-IPaddress>-network.info.txt
   ```
   Security Analyticsサーバ:
   ```
   <hostname-IPaddress>-root.tar.gz
   <hostname-IPaddress>-backup.tar.gz
   <hostname-IPaddress>-mongodb.tar.gz
   tar checksumファイル
   <hostname-IPaddress>-network.info.txt
   ```
   ESAホスト：
   ```
   <hostname-IPaddress>-root.tar.gz
   <hostname-IPaddress>-backup.tar.gz
   <hostname-IPaddress>-mongodb.tar.gz
   ```

<hostname-IPaddress>-controldata-mongodb.tar.gz
tar checksumファイル
<hostname-IPaddress>-network.info.txt

アーカイブされたファイルは、/var/netwitness/database/nw-backupディレクトリに保存されます。tarファイルのいずれかが予想よりも小さい場合は、ファイルを開いて正しくバックアップされているか確認します。

## バックアップ後のタスク

### タスク1：all-systemsファイルとバックアップtarファイルのコピーの保存

all-systemsファイル、all-systems-master-copyファイル、バックアップtarファイルのコピーを作成し、コピーを安全な場所に保存します。Security Analyticsサーバ(具体的には、Adminサービス)を11.2にアップグレードした後は、これらのファイルは再生成できません。

### タスク2：必要なバックアップ ファイルの生成の確認

バックアップ スクリプトを実行した後、いくつかのファイルが生成されます。これらのファイルは、11.2へのアップグレードに必要です。アップグレードを開始する前に、アップグレードするホスト上に必要なバックアップ ファイルを配置する必要があります。

バックアップ スクリプトによって、すべてのホストに次のファイルが生成されます。

- all-systems
- all-systems-master-copy
- appliance_info
- service_info
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

上記のファイルに加えて、Security Analyticsサーバ ホストとESAホストには次のファイルが生成されます。

- <hostname>-<host IP address>-mongodb.tar.gz
- <hostname>-<host IP address>-mongodb.tar.gz.sha256

バックアップ スクリプトは、次の controldata-mongodb.tar.gzファイルも生成します。

**注：**バックアップ スクリプトは、次のファイルを、すべてのESAホストからSecurity Analyticsサーバ ホストのバックアップ パスにコピーします。

- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz
- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256

### タスク3: (オプション) 複数のESAホストがある場合は、mongodb tar ファイルをESAプライマリホストにコピー

導入環境に複数のESAホストがある場合、次の2つのファイルを、各ESAホストからESAプライマリホスト(Context Hubサービスが実行されているホスト)の/opt/rsa/database/nw-backup/ディレクトリにコピーします。

- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

### タスク4: 必要なすべてのバックアップ ファイルが各ホスト上にあることを確認

11.2にアップグレードする前に、アップグレードするホストに、次のリストに示すファイルが存在することを確認します。

**注:** バックアップ ファイルのデフォルト パスは次の通りです。
- Security Analyticsサーバ: /var/netwitness/database/nw-backup
- ESAホスト: /opt/rsa/database/nw-backup
- Malwareホスト: /var/lib/rsamalware/nw-backup

#### NetWitness Serverに必要なファイル

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256

#### ESAホストに必要なファイル

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz

- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

### その他のすべてのホストに必要なファイル

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

**注:** 次のファイルは、すべてのホストの<hostname>-<host-IP-address>-backup.tar.gz tarに含まれます。
appliance_info
service_info

**注 :** iptable、NAT構成、ユーザ アカウント、crontabエントリーのバックアップ ファイルとリストア ファイルの場所は、次のとおりです。
**バックアップ パス**:
`BUPATH=/opt/rsa/database/nw-backup`( ESA相関エンジン)
`BUPATH=/var/lib/rsamalware/nw-backup`( マルウェア サービス)
`BUPATH=/var/netwitness/database/nw-backup`( その他のすべてのサービス)
**リストアの場所** :
`BUPATH/restore/etc/sysconfig`( iptableルール)
`BUPATH/restore/etc/sysconfig`( NAT構成)
`BUPATH/restore/etc`( crontabエントリー)
`BUPATH/restore/etc`( ユーザ アカウント。ユーザは `passwd`ファイルに存在し、グループは`group`ファイルに存在します。これらはアップグレード プロセスではリストアされませんが、手動でリストアできます) 。
`BUPATH/restore/etc/ntp.conf`( NTP構成。NetWitness Platform UIを使用してリストアする必要があります)

# ディスクドライブの10.6.6.xから11.2への移行

この手順は、仮想ホストを10.6.6.xから11.2にアップグレードする方法を示します。

**注意**:1.) 仮想マシンのスナップショットがある場合は、移行を実行できません。
2.) データが古くならないように、各フェーズでホストをアップグレードする直前にバックアップを実行します。
3.) このガイドは、仮想ホストのアップグレードにのみ適用されます。導入環境に物理ホストと仮想ホストの両方がある場合、物理ホストをアップグレードする手順については「*RSA NetWitness® Platform11.2 物理ホストのアップグレード ガイド*」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

**注**:仮想マシンが、VMware ESX上に存在する必要があります。

VM(仮想マシン)のディスクドライブを10.6.6.xから11.2に移行するために、5つのタスクを完了する必要があります。

タスク1:10.6.6.xの仮想マシンのデータをバック アップ。

タスク2:10.6.6.xと同じ仮想マシンスタックで11.2の仮想マシンを導入。

タスク3:VMDKファイルをコピーし、新しい仮想マシンにハード ディスクとして追加。

タスク4:アップグレードしたSAサーバ仮想マシンのMACアドレスの引き継ぎ。

タスク5:11.2の仮想マシンに10.6.6.xのバックアップ データをリストア。

## タスク1:10.6.6.xの仮想マシンのデータをバック アップ

1. Log Collectorの移行を準備します。
   a. Log Collectorに、rootとしてログインします。
   b. `/opt/rsa/nwlogcollector/nwtools/`ディレクトリに移動し、次のコマンドを実行します。
      `sh prepare-for-migrate.sh --prepare`
      VLCをアップグレードする詳細な手順については、「Virtual Log Collectorホスト (VLC)」を参照してください。
2. 10.6.6.xバックアップ スクリプトを含む`.zip`ファイルをRSA Link(https://community.rsa.com/docs/DOC-81514)から外部のバックアップ ホストにダウンロードします。

   **注**:ファイルのバックアップに使用する外部ホストをセットアップする必要があります。このホストはCentOS 6を実行し、NetWitness Platformの各ホストにSSHで接続する必要があります。

3. `nw-backup/scripts`ディレクトリで次のコマンドを実行します(バックアップ スクリプトの詳細については、「バックアップ手順」を参照してください。)
   `./get-all-systems.sh <SA-IP>`
   `./ssh-propagate.sh <path-to-backup-directory/all-systems>`
   `./nw-backup.sh -u`
   Malware VMがある場合は、このコマンドの`-m -u`を`-u`に置き換えます(例:`./nw-backup.sh -m -u`)。

## タスク2: 10.6.6.xと同じ仮想マシンスタックで11.2の仮想マシンを導入

10.6.6.xと同じ仮想ホスト スタックを11.2の仮想マシンに設定する必要があります。手順については、「*RSA NetWitness® Platform 11.2 仮想ホスト インストール ガイド*」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

次の手順は、ESXi環境にOVAホストを導入する手順の概要です。

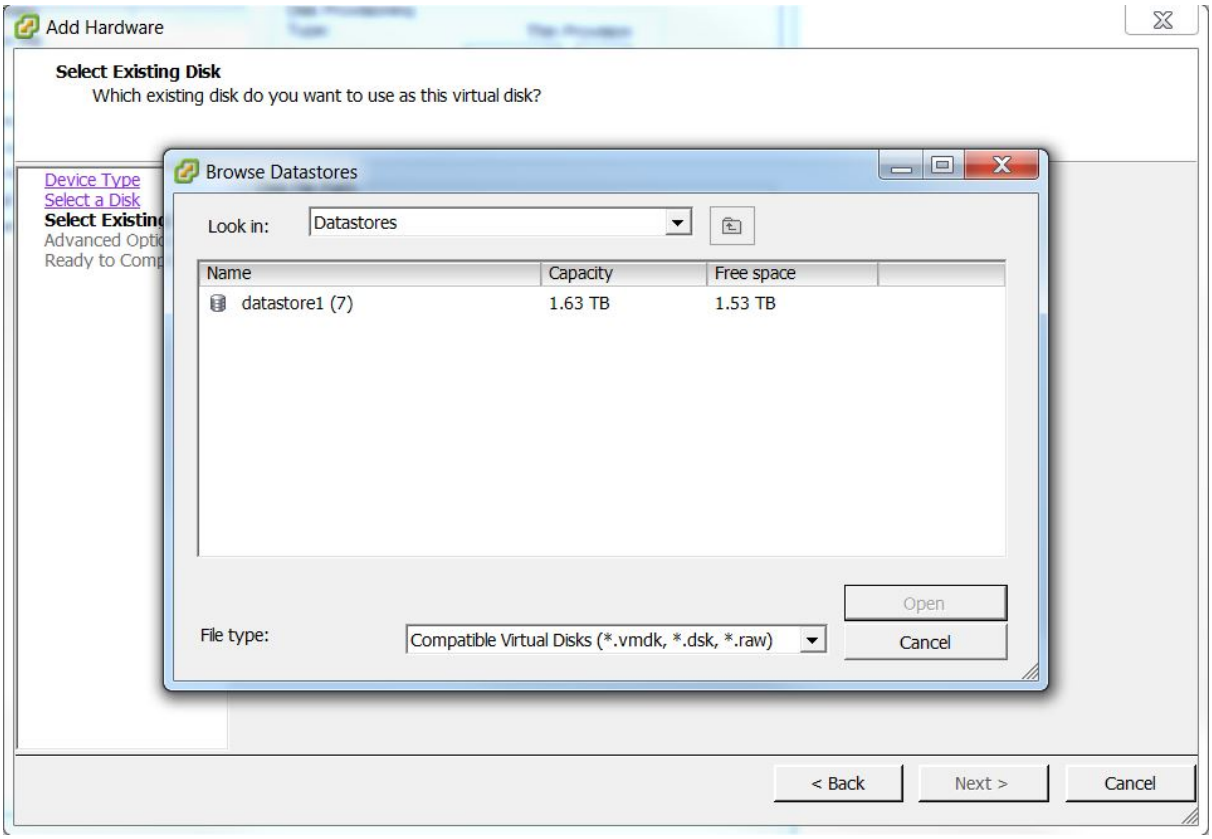
RSA LinkのDownload Centralから、11.2 OVAをローカル ディレクトリにダウンロードします。

1. VMware ESXi環境にログオンします。
2. [**ファイル**]ドロップダウンで、[**OVFテンプレートのデプロイ**]を選択します。
   [OVFテンプレートのデプロイ]ダイアログが表示されます。
3. ダウンロードした11.2 OVAを保存したローカル ディレクトリを参照します。
4. 11.2 OVAを選択して、[**次へ**]をクリックします。
5. 仮想マシンの適切な構成を選択して、[**次へ**]をクリックします。
6. 仮想マシンをパワーオンし、コンソールを開き、ログインします。
   仮想マシンが11.2ベース イメージになったため、セットアップ プログラム( `nwsetup-tui`) を実行する必要があります。

## タスク3: VMDKファイルをコピーし、新しい仮想マシンにハード ディスクとして追加

1. 10.6.6.xと11.2の両方の仮想マシンをパワーオフします。
2. ESXサーバーにアクセスし、[**構成**]タブ > [**ストレージ**]をクリックします。

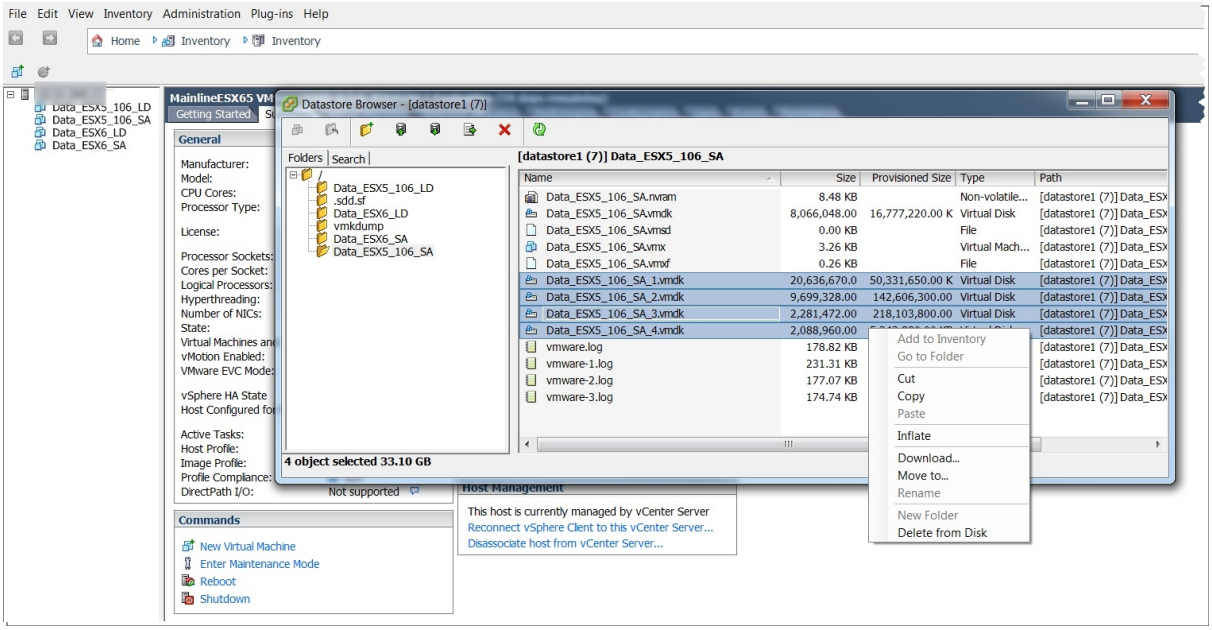
3. データストアを右クリックして、[**データストアの参照**]をクリックします。




4. 既存の10.6.6.x仮想マシンのデータストアに移動します。

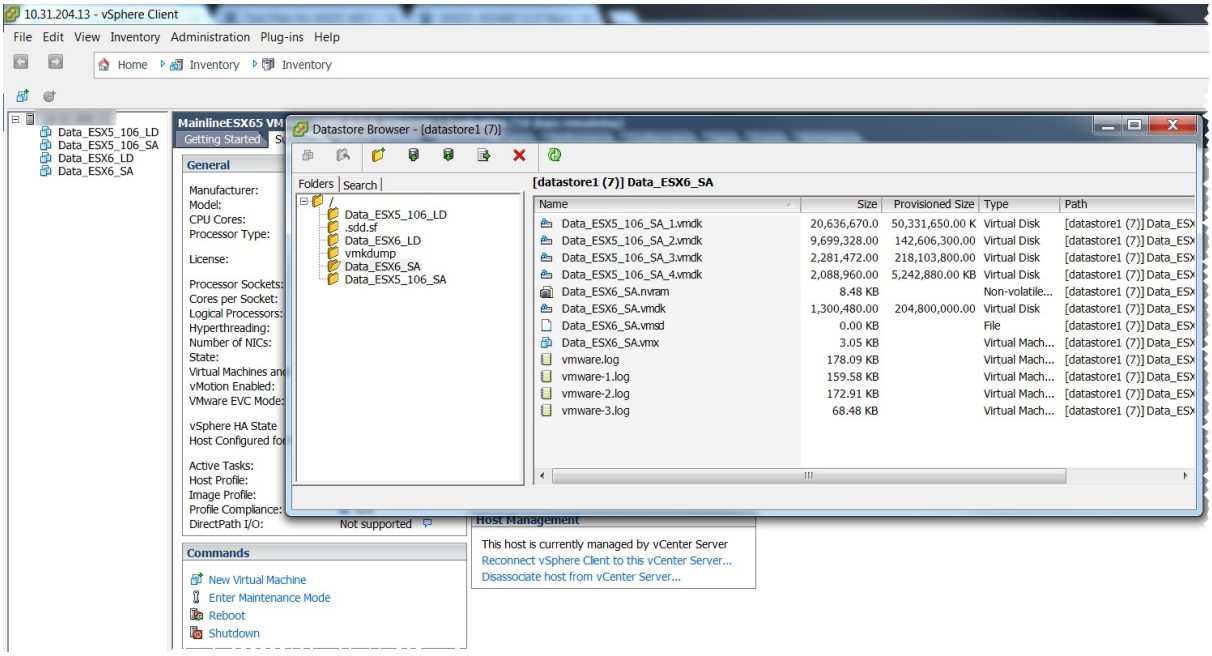
5. 10.6.6.x仮想マシンのすべてのVMDKファイルを選択し、右クリックして、[**コピー**]をクリックします。

> **注意**：ベースのVMDKファイル( 例 : `Data_106_SA`) にはCentOS6が含まれているため、コピーしないでください。
>
> 番号の付いたVMDKファイルをすべてコピーする必要があります。たとえば、10.6.6.xの仮想マシン名が`Data_106_SA`の場合、`Data_106_SA_1`、`Data_106_SA_2`、`Data_106_SA_3`などのファイルはすべてコピーします。




6. 新しい11.2仮想マシンのデータストアに移動します。

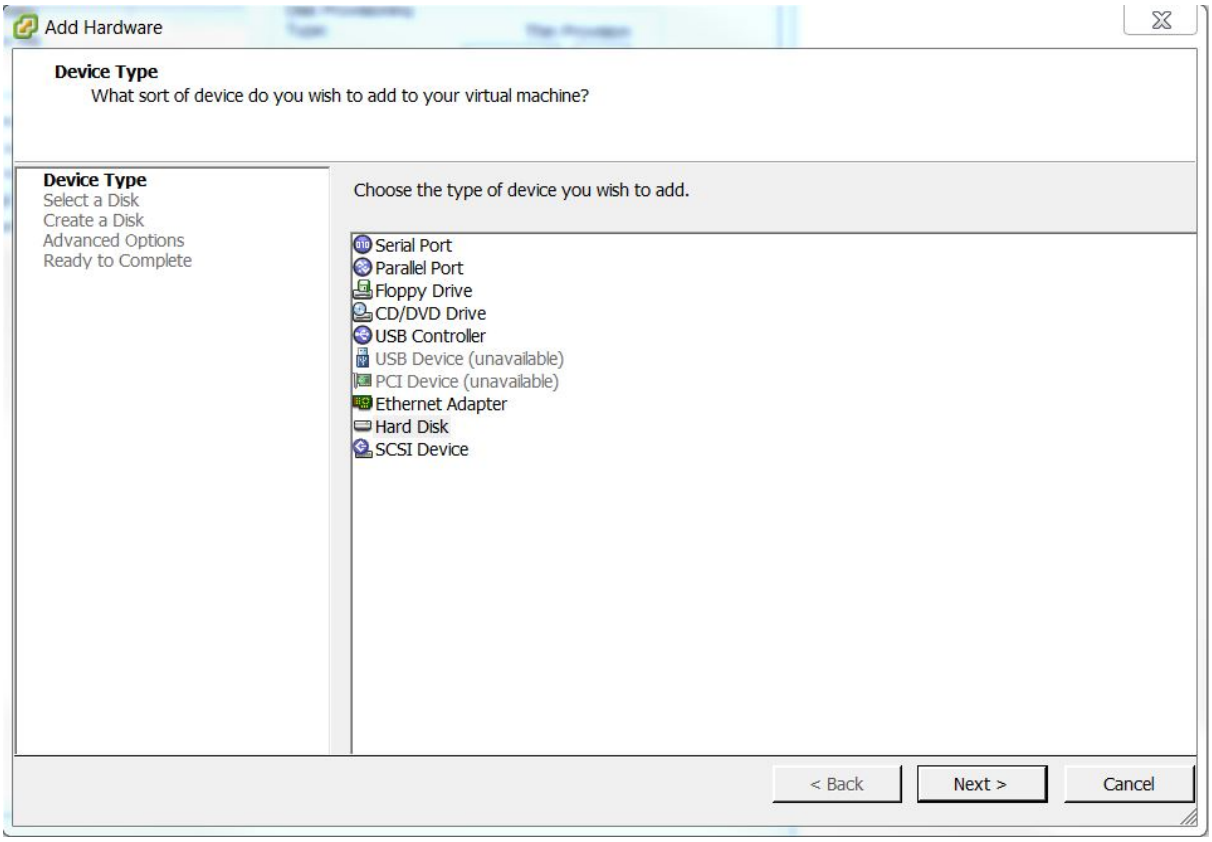
7. 右クリックして[**貼り付け**]をクリックします。




**注**:前の仮想マシンから新規の仮想マシンのデータストアにすべてのVMDKファイルが完全にコピーされるまで待機する必要があります。

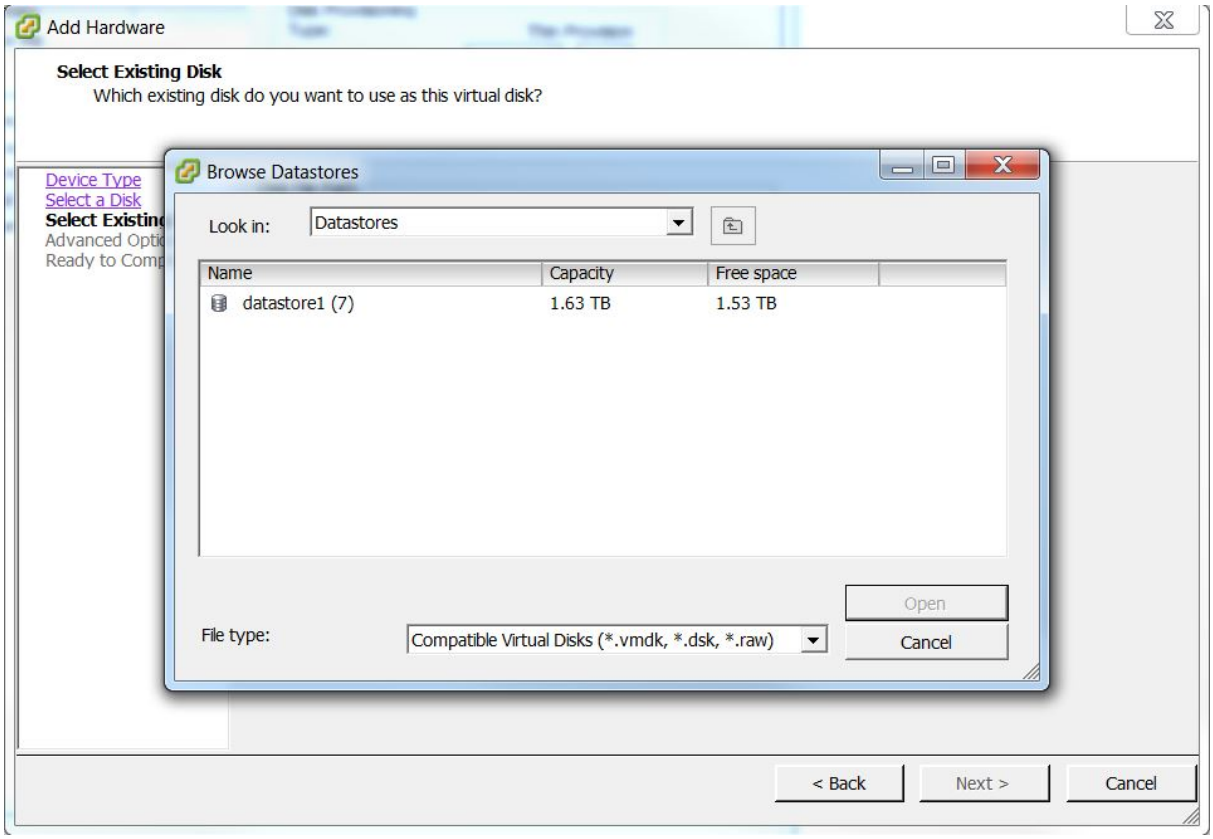
8. 11.2仮想マシンを選択して、[**設定の編集**]>[**追加**]をクリックします。

9. ダイアログ ボックスで、[**ハード ディスク**] > [**次へ**]をクリックします。

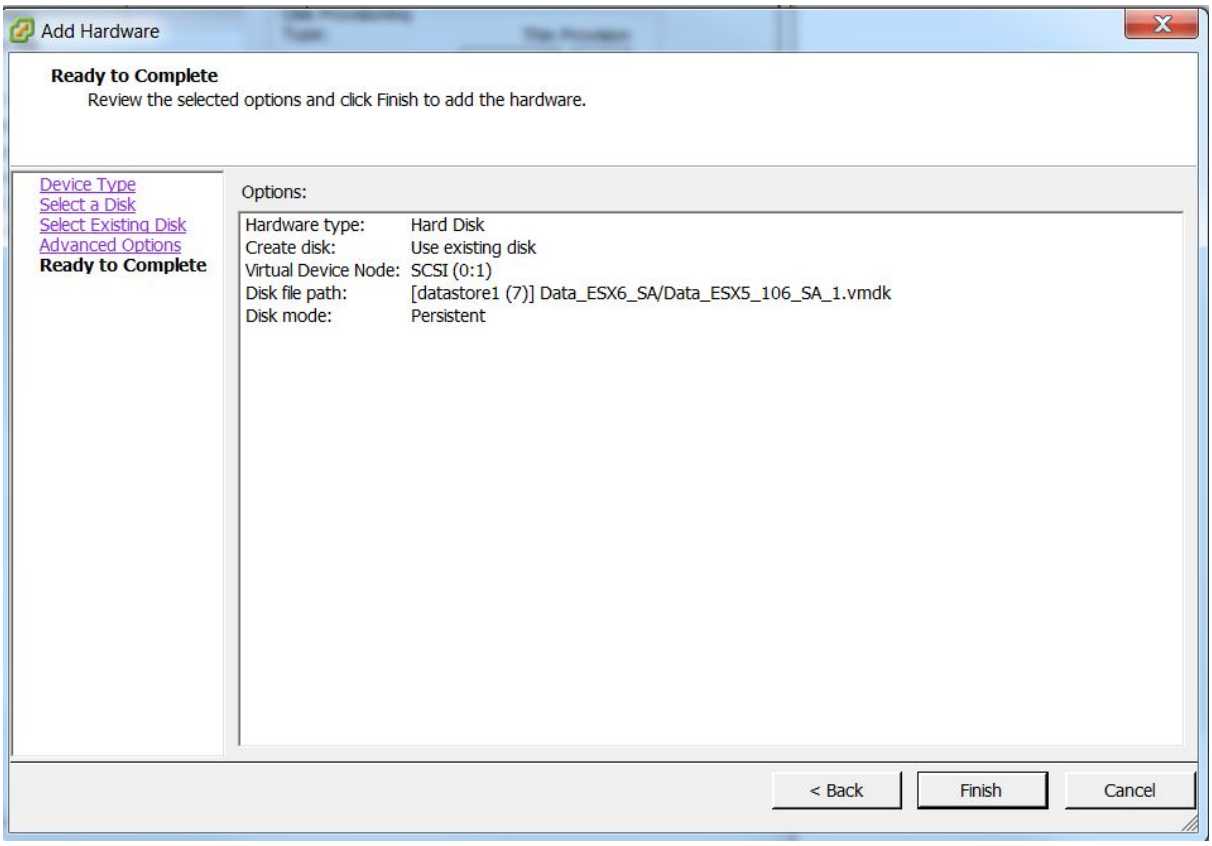



10. [**既存のハード ディスク**] > [**次へ**]をクリックします。

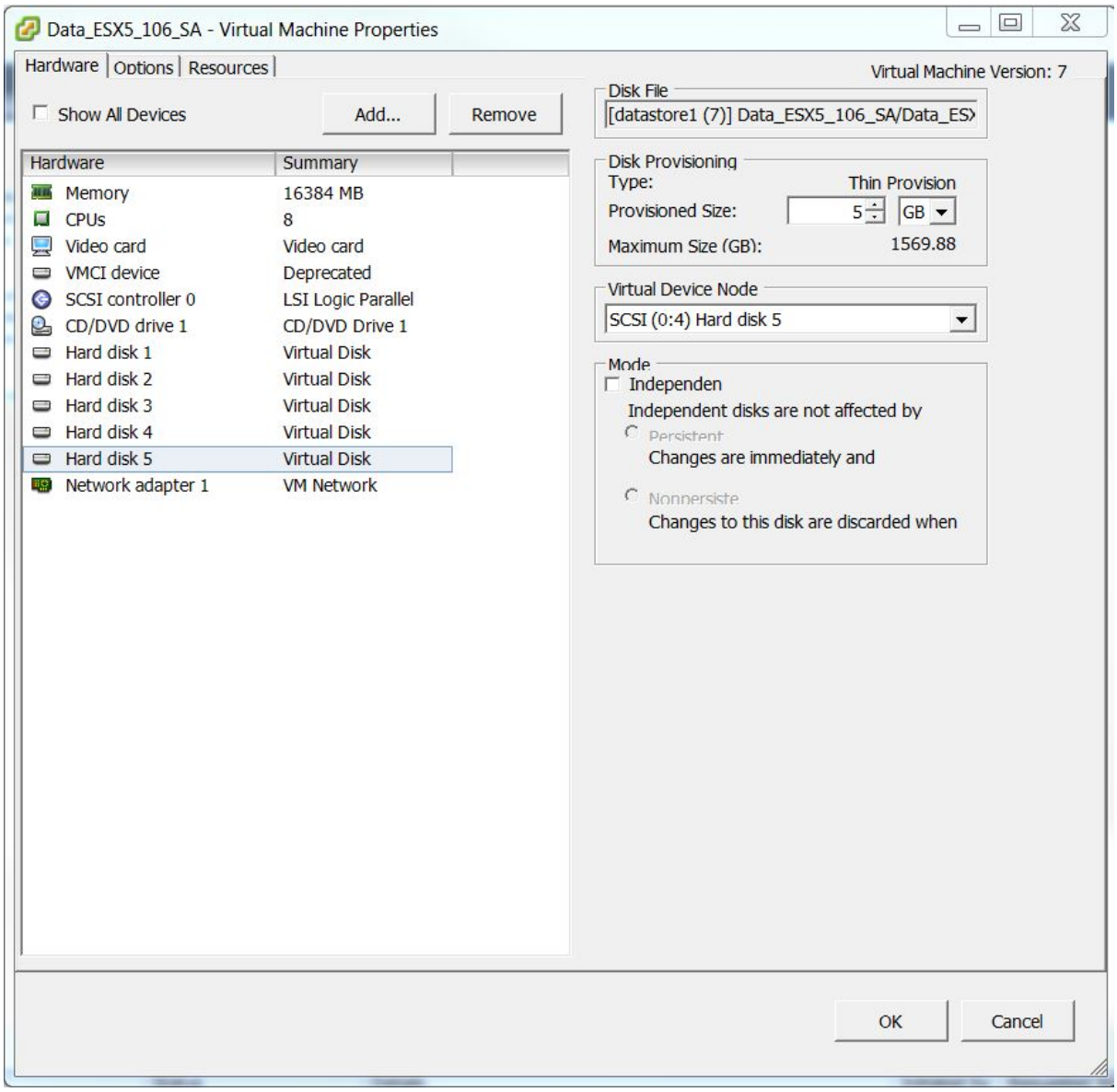
11. [**参照**]をクリックし、VMDKファイルをコピーしたデータストアの場所を参照します。




12. 11.2仮想マシンのデータストアからディスクとして追加するVMDKファイルを選択します。




13. 追加するディスクごとに、ステップ8～12を繰り返します。




14. ［**OK**］をクリックします。

## タスク4: アップグレードしたSAサーバ仮想マシンのMACアドレスの引き継ぎ

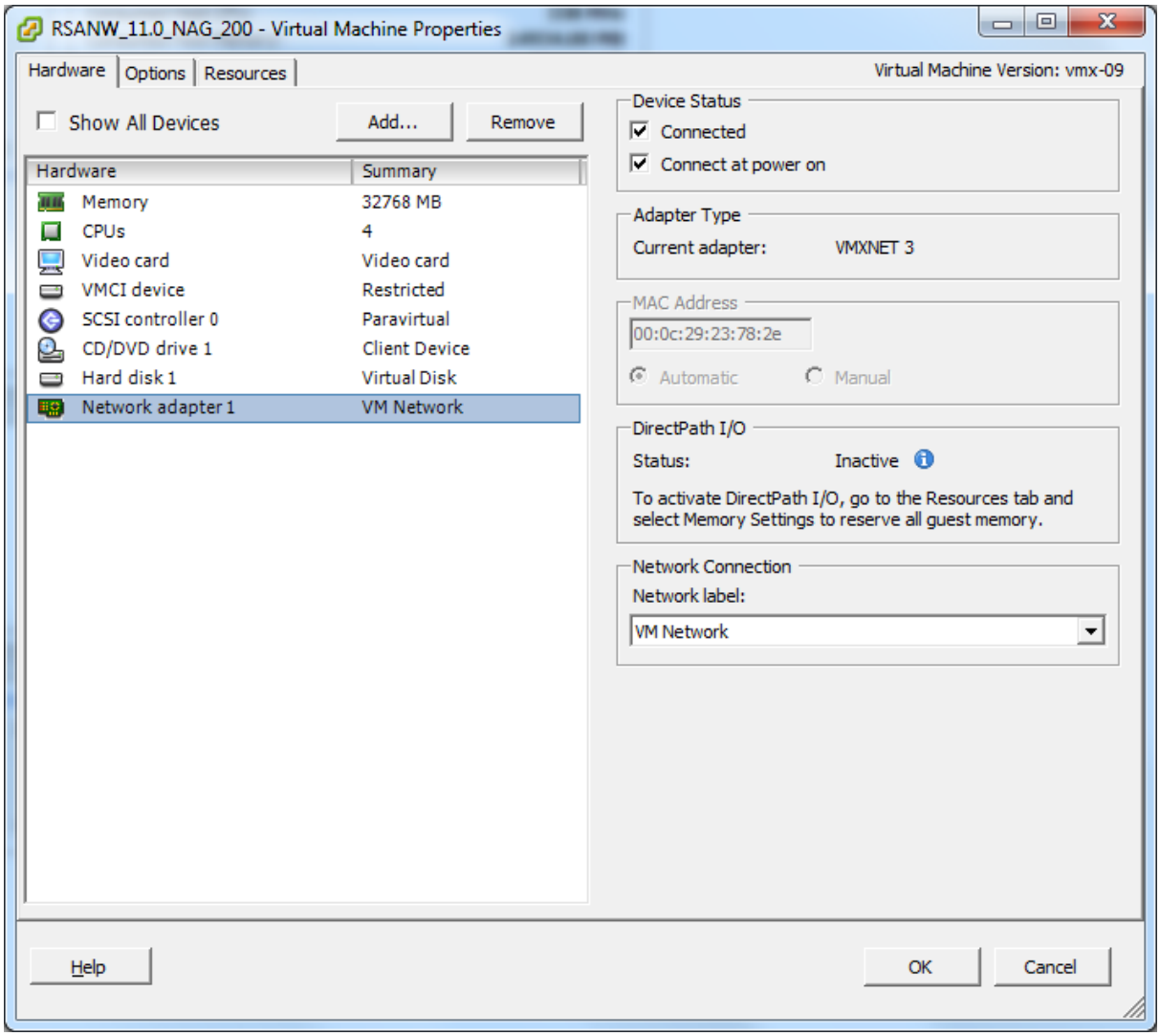
移行したSA( Security Analytics) サーバのVM( 仮想マシン) のMACアドレスを引き継ぐために、次の手順を実行します。

**注 :** 次の手順は、SA Server仮想マシン( MACアドレスの「自動」割り当てを指定して作成したもの) を、11.2 NetWitness Serverに移行する場合に実行します。静的MACアドレスを持つ仮想マシンの場合は、仮想マシンの[設定の編集]でMACアドレスを手動で入力して、MACアドレスを変更できます。

1. vCenter Serverにログインします。

   **注 :** サポートされるvCenterのバージョンは、5.5～6.5までです。

2. ( オプション) パワーオンされている場合は、両方の仮想マシン( NetWitness 10.6.6.xと11.2) を**パワーオフ**します。
3. [**サマリ**]タブをクリックし、データストアを右クリックして、[**データストアの参照**]を選択し、データストアの場所を参照します。
4. 仮想マシンのフォルダに移動し、10.6.6.xと11.2の.vmxファイルをダウンロードし、ローカルリポジトリに保存します。
   デフォルトでは、MACアドレスを自動生成した仮想マシンのMACアドレスは次の図のような形式になります。



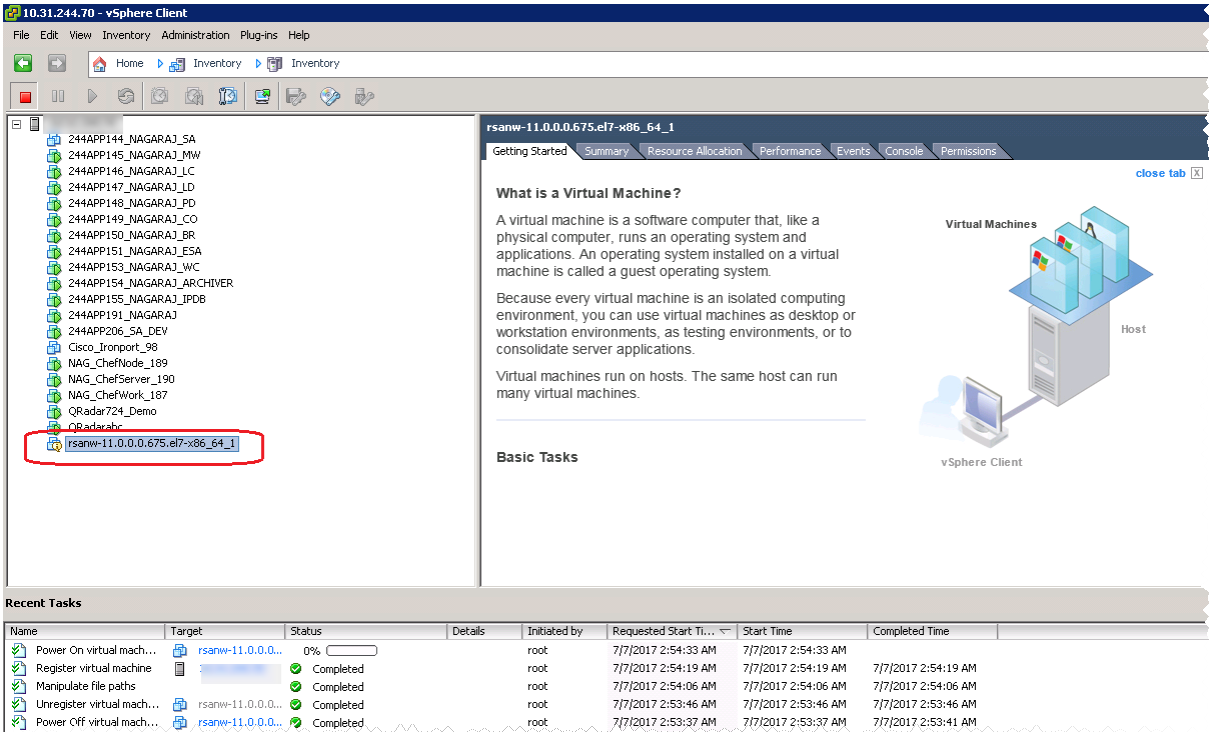

**注 : 00:0c:29:XX:YY:ZZ – 00:0c:29**は、自動生成されたMACアドレスに固有の識別子です。**00:50:56:XX:YY:ZZ – 00:50:56**は、静的または手動で生成されたMACアドレスに固有の識別子です。これは、vCenterが導入されていない場合にのみ該当します。vCenterが導入されている場合、このMACアドレスは自動生成されたMACアドレスに固有の識別子を意味します。

5. テキスト エディタを使用して、`uuid.location`と`ethernet0.generatedAddress`の値を10.6.6.xの**.vmx**ファイルから11.2の**.vmx**ファイルにコピーします。

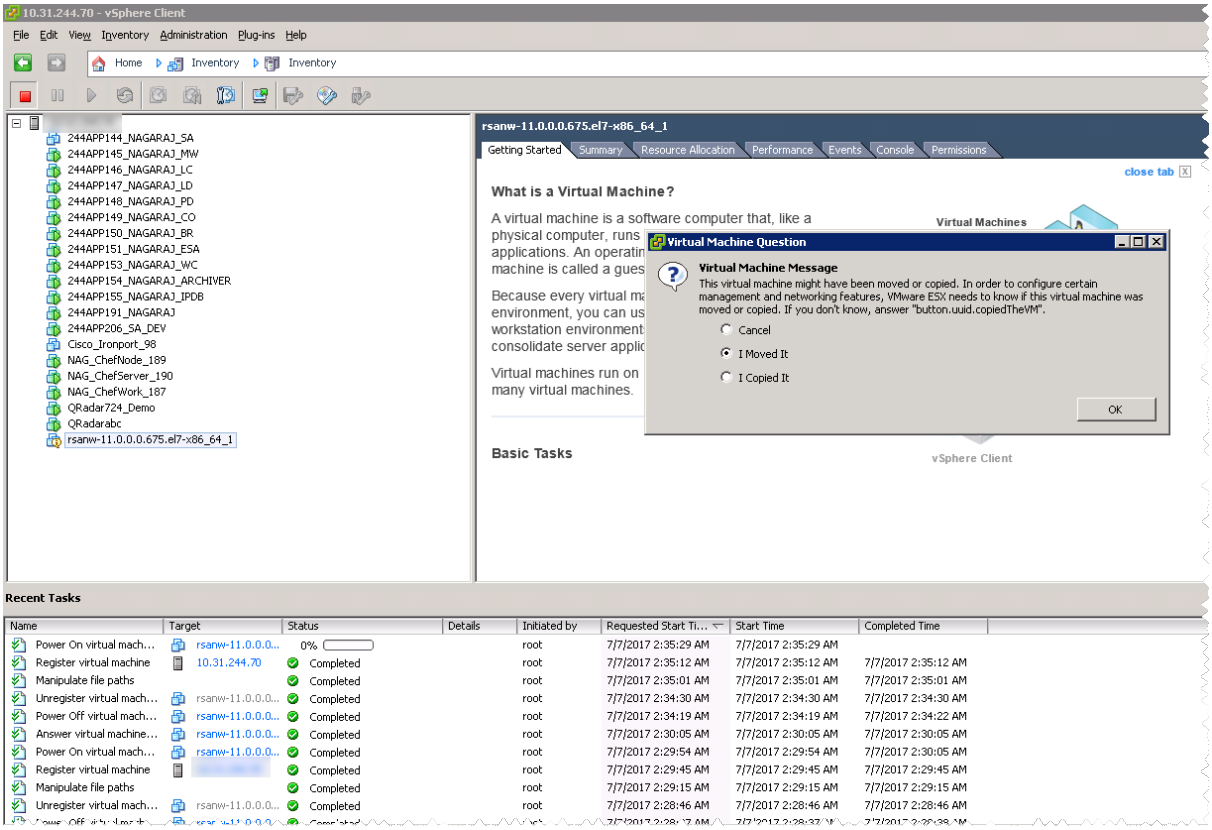
**注 :** ( vCenterを経由せず) VMware ESXサーバに直接10.6.6.xスタックを導入した場合は、10.6.6.xの**.vmx**ファイルから11.2の**.vmx**に`uuid.location`と`ethernet0.generatedAddress`をコピーし、加えて、`uuid.bios`の値をコピーする必要があります。

6. インベントリから、10.6.6.xと11.2の両方の仮想マシンを削除します。
   a. vCenter Serverに移動します。
   b. 10.6.6.xと11.2の両方の仮想マシンを右クリックします。
   c. [インベントリから削除]を選択します。

7. 変更した11.2の**.vmx**ファイルをデータストアにアップロードし、既存の**.vmx**ファイルを置換します。
8. データストアで、11.2の**.vmx**ファイルを右クリックし、[インベントリへの追加]を選択します。
9. vCenter Serverに移動し、11.2仮想マシンを**パワーオン**します。
   以下のメッセージが表示されます:
   **この仮想マシンは移動またはコピーされた可能性があります。特定の管理およびネットワーク機能を構成するために、この仮想マシンが移動またはコピーされたことをVMware ESXが確認する必要があります。わからない場合は、「コピーしました」を選択します。**



10. 仮想マシンを右クリックし、[**ゲスト**]＞[**質問への回答**]を選択します。
次ような画面が表示されます。




11. [**移動しました**]を選択します。

12. [**OK**]をクリックします。
10.6.6.xのMACアドレスが、11.2のMACアドレスとして引き継がれます。

## タスク5: 11.2の仮想マシンに10.6.6.xのバックアップ データをリストア

11.2 VMを**パワーオン**し、次の手順を実行します。

1. バックアップ データを`nw-backup`ディレクトリから11.2仮想マシンにコピーします。

- NW Server( 10.6.6.xではSA Server) の場合 :

  **注 :** VLCをアップグレードする詳細な手順については、「Virtual Log Collectorホスト ( VLC) 」を参照してください。

  a. `/tmp`の下に`nwhome`ディレクトリを作成します。

  b. `VolGroup00-nwhome`を`/tmp/nwhome/`にマウントします。
  ```
  mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
  ```

  c. `/tmp/nwhome/`ディレクトリのコンテンツを`/var/netwitness/`にコピーします。
  ```
  cp -r /tmp/nwhome/* /var/netwitness/
  ```

  d. `VolGroup02-redb`を`/var/netwitness/database`にマウントします。
  ```
  mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
  ```

  **注 :** `/var/netwitness/database/nw-backup`ディレクトリが存在し、アプライアンスのバックアップtarファイルが格納されていることを確認します。

  e. `VolGroup00-nwhome`を`/tmp/nwhome/`からアンマウントします。
  ```
  umount /tmp/nwhome
  ```

- Archiver、Broker、Concentrator、Log Decoder/Log Collector、Network Decoderの場合 :

  **注 :** 10.6.6.x DecoderまたはLog Decoderに複数のネットワーク インターフェイスがある場合は、次の手順を実行します。
  1. DecoderまたはLog Decoderの11.2仮想マシンを**パワーオフ**します。
  2. 仮想マシンの[**設定の編集**]に移動し、必要な数のEthernetアダプタを追加します。
  3. 仮想マシンを**パワーオン**します。
  4. バックアップ データをリストアする前に、Ethernetアダプタを追加します。

  a. `/tmp`の下に`nwhome`ディレクトリを作成します。

  b. `VolGroup00-nwhome`を`/tmp/nwhome/`に一時的にマウントします。
  ```
  mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
  ```

  c. `/tmp/nwhome/`ディレクトリのコンテンツを`/var/netwitness/`にコピーします。
  ```
  cp -r /tmp/nwhome/* /var/netwitness/
  ```

  d. `VolGroup00-nwhome`を`/tmp/nwhome/`からアンマウントします。
  ```
  umount /tmp/nwhome
  ```

- Malware Analysisの場合( Co-located Malwareは、11.2のアップグレードではサポートされません) :

  a. `/tmp/`の下に`apps`ディレクトリを作成します。

  b. `VolGroup01-apps`を`/tmp/apps/`に一時的にマウントします。
  ```
  mount /dev/mapper/VolGroup01-apps /tmp/apps/
  mkdir /var/netwitness/database
  ```

c. nw-backup ディレクトリを /var/netwitness/にコピーします。
```
cp -r /tmp/apps/nw-backup /var/netwitness/database
```

d. VolGroup01-appsを/tmp/apps/からアンマウントします。
```
umount /tmp/apps
```

- Event Stream Analysisの場合 :

a. /tmp/の下にappsディレクトリを作成します。

b. VolGroup01-appsを/tmp/apps/に一時的にマウントします。
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. nw-backupディレクトリを/var/netwitnessにコピーします。
```
cp -r /tmp/apps/nw-backup /var/netwitness
```

d. VolGroup01-appsを/tmp/apps/からアンマウントします。
```
umount /tmp/apps
```

2. ディスクをマウントします。

**注 :** 仮想マシンの次のいずれかのディレクトリのスタックに、外部のマウント ポイントを構成している場合は、次のマウント ポイントの代わりに外部のマウント ポイントを再マウントします。

- NW Serverの場合 :
```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

**注 :** /var/netwitness/database/nw-backupディレクトリが存在し、アプライアンスのバックアップtarファイルが格納されていることを確認します。

- Log Decoder/Log Collectorの場合 :

**注 :** 次のマウントは、Virtual Log Collectorには必要ありません。

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder
mount /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index
mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb
mount /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
mount /dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb
```

- Network Decoderの場合 :
```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder
mount /dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/decoder/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb
mount /dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb
```

- Concentratorの場合 :
```
mount /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb
```

- Archiverの場合:
  ```
  mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
  mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
  ```
- Brokerの場合:
  ```
  mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
  ```

3. 次のマウント エントリーを`/etc/fstab`に追加します。
   - NW Serverの場合:
     ```
     /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs
     defaults,noatime,nosuid 1 2
     ```
   - Log Decoder/Log Collectorの場合:

     **注:次のマウントは、Virtual Log Collectorには必要ありません。**

     ```
     /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-sessiondb /var/netwitness/logdecoder/sessiondb xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb xfs
     defaults,noatime,nosuid 1 2
     ```
   - Network Decoderの場合:
     ```
     /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb xfs
     defaults,noatime,nosuid 1 2
     ```
   - Concentratorの場合:
     ```
     /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-sessiondb /var/netwitness/concentrator/sessiondb
     xfs defaults,nosuid,noatime 1 2
     /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs
     defaults,noatime,nosuid 1 2
     /dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb xfs
     defaults,noatime,nosuid 1 2
     ```

- Archiverの場合 :
  ```
  /dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs
  defaults,nosuid,noatime 1 2
  /dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs
  defaults,nosuid,noatime 1 2
  ```
- Brokerの場合 :
  ```
  /dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
  defaults,nosuid,noatime 1 2
  ```

# 11.2での仮想ホストのセットアップ

11.2仮想スタックをセットアップするために、以下の2つのフェーズをこの順番で実行します。

- フェーズ1：NW Server、Event Stream Analysis、Malware Analysis、Broker、Concentratorホストのセットアップ

  **注：**10.6.6.xでEvent Stream AnalysisのC2モジュールを有効化していた場合、Event Stream Analysisサービスを11.2にアップグレードすると、モジュールがウォームアップを開始し、ウォームアップが完了するまで使用できなくなります。

- フェーズ2：残りのコンポーネント ホストのセットアップ

## フェーズ1：NW Server、Event Stream Analysis、Malware Analysis、Broker、Concentratorホストのセットアップ

### タスク1： 11.2 NetWitness Serverのセットアップ

「11.2 NW Serverホストのセットアップ」の手順に従います。

### タスク2：11.2 ESAのセットアップ

**注意：**10.6.6.xでC2モジュールを有効化していた場合、Event Stream Analysisサービスを11.2にアップグレードすると、モジュールがウォームアップを開始し、ウォームアップが完了するまで使用できなくなります。

「11.2 非NW Serverホストのセットアップ」の手順に従い、ESAホストをセットアップします。

1. セットアップ プログラムを使用してESAプライマリ ホストをセットアップし、ユーザ インタフェースの[**管理**]＞[**ホスト**]ビューを使用して、ホスト上に**ESAプライマリ**サービスをインストールします。

   **注：**複数のESAホストを使用する場合は、ESAセカンダリ ホストをアップグレードする前に、ESAプライマリ ホストをアップグレードする必要があります。プライマリ ホストにはすべてのmongodb( Mongoデータベース) のバックアップtarファイルが保存されています。

2. ( オプション) ESAセカンダリ ホストがある場合、セットアップ プログラムを使用してホストをセットアップし、ユーザ インタフェースの[**管理**]＞[**ホスト**]ビューを使用して、ホスト上に**ESAセカンダリ**サービスをインストールします。

### タスク3：11.2 Malware Analysisのセットアップ

「11.2 非NW Serverホストのセットアップ」の手順に従います。

### タスク4：11.2 BrokerまたはConcentratorのセットアップ

「11.2 非NW Serverホストのセットアップ」の手順に従います。

**注**：Brokerがない場合は、Concentratorホストをアップグレードします。11.2 NW Serverの新しいInvestigate機能は10.6.6.xコア サービスと通信できません。このため、フェーズ1でBrokerまたはConcentratorのホストをアップグレードする必要があります。

## フェーズ2：残りのコンポーネント ホストのセットアップ

Decoder、Concentrator、Log Collectionの各ホストをアップグレードする場合は、データ収集および集計の停止と再開の手順について、「付録B：データ収集と集計の停止と再開」を参照してください。

### DecoderホストおよびConcentratorホスト

1. データ収集と集計を停止します。
2. 「11.2 非NW Serverホストのセットアップ」の手順を実行します。
3. データ収集と集計を再開します。

### Log Decoderホスト

1. 「LC( Log Collector) とVLC( Virtual Log Collector) : prepare-for-migrate.shの実行」(「**バックアップ手順**」) の記載に従い、Log Collectorの準備が完了したことを確認します。
2. Log Decoder上でデータ収集を停止します。
3. 「11.2 非NW Serverホストのセットアップ」の手順を実行します。
4. Log Decoder上でデータ収集を再開します。

**注**：アップグレードした後、「**アップグレード後のタスク**」の「タスク30：アップグレード準備タスクの一致条件「Domain」で特定されたインシデント ルールの更新」を完了した後で、ログ収集を再開します。

### Virtual Log Collectorホスト

1. 「LC( Log Collector) とVLC( Virtual Log Collector) : prepare-for-migrate.shの実行」(「**バックアップ手順**」) の記載に従い、Virtual Log Collectorの準備が完了したことを確認します。
2. バックアップを実行するホスト上の`all-systems`ファイルを編集し、10.6.6.x VLCをバックアップします。
   a. この手順を実行する前に、`all-systems`ファイルの内容に、次の情報が含まれていることを確認します。
      `vlc,<host-name>,<IP-address>,<UUID>,10.6.6.x`
   b. 次のコマンドを実行して、バックアップを作成します。
      `./nw-backup.sh -u`
      ホストをバックアップする詳細な手順については、「バックアップ手順」を参照してください。
3. バックアップ ホストに、次の形式で、VLCのバックアップが作成されていることを確認します。
   `<hostname>-<IPaddress>-root.tar.gz`
   `<hostname>-<IPaddress>-root.tar.gz.sha256`
   `<hostname>-<IPaddress>-backup.tar.gz`

```
<hostname>-<IPaddress>-backup.tar.gz.sha256
<hostname-IPaddress>-network.info.txt
all-systems-master-copy
```

4. 新しい11.2仮想マシンが同じネットワーク構成を使用できるように、10.6.6.x VLCをパワーオフします。
5. 11.2 NetWitness PlatformのOVAを使用して、非NW Serverホストを新規に導入します。
6. 新しいVLCの仮想マシンのコンソールに接続します。
7. 10.6.6.x VLCと同じネットワーク構成に変更します。
この情報は、10.6.6.x VLCバックアップ ファイルの`<hostname-IPaddress>-network.info.txt`に保存されています。

**注 :** IPv6が無効化されていることを確認します。

a. `/etc/sysconfig/network-scripts/ifcfg-eth0`ファイルを編集し、設定を更新します。
`ifcfg-eth0` の内容は次のようになります。

```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

b. 次のコマンド文字列を実行します。

```
systemctl restart network.service
```

8. バックアップ ディレクトリを作成します。

```
# mkdir -p /var/netwitness/database/nw-backup/
```

9. バックアップをバックアップ ホストの`/var/netwitness/database/nw-backup`から新規のVLCの`/var/netwitness/database/nw-backup`ディレクトリにコピーします。
10. NW Server以外のNetWitness Platformコンポーネントのための、「11.2 NW Server以外のホストのセットアップ」のステップ2～12を実行します。ステップ12では、サービスとして**Log Collector**を選択します。

## 11.2 NW Server ホストのセットアップ

10.6.6.x SA Serverホストのデータを必ずバックアップしてください。**ホストをバックアップするには、「バックアップ手順」の手順に従う必要があります。**

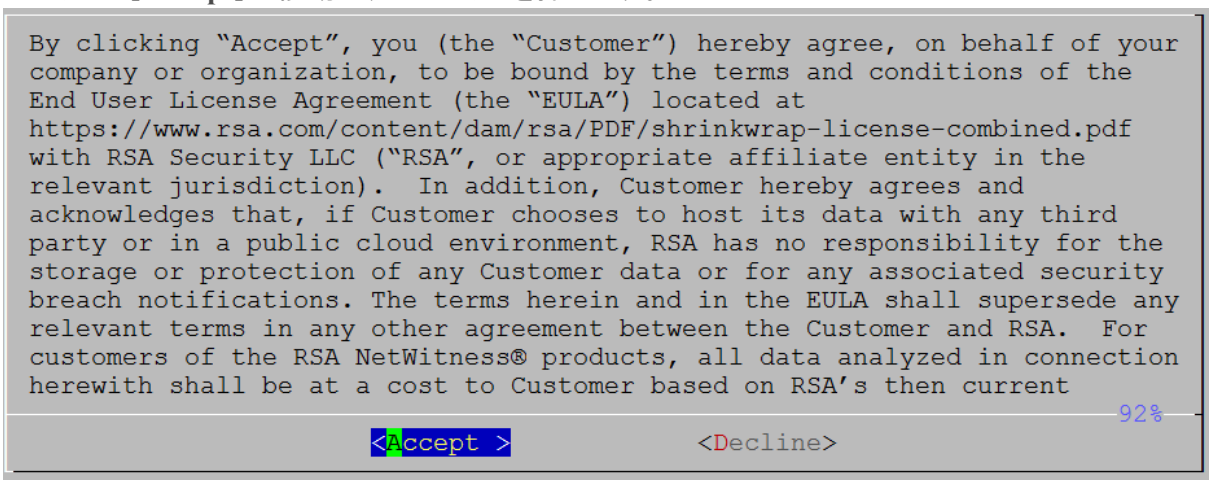
**注意**：データができる限り最新になるよう、SA Serverを11.2にアップグレードする直前にバックアップを実行します。SA Serverをアップグレードする前に**all-systems**ファイルを作成する必要があります。このファイルは、SA Serverを11.2にアップグレードした後では作成できません。

次の手順を実行して、11.2 NW Serverホストをセットアップします。

1. 11.2 NW Server VMのコンソールにログインし、`nwsetup-tui`コマンドを実行します。
   これによりセットアップ プログラムが開始され、EULAが表示されます。

   **注**：1.) セットアップ プログラムのプロンプトが表示されたら、下向き矢印と上向き矢印を使用してフィールド間を移動し、Tabキーを使用してコマンド間(たとえば、**<Yes>**、**<No>**、**<OK>**、**<Cancel>**)を移動します。Enterキーを押して、コマンドの選択を確定し、次のプロンプトに移動します。
   2.) セットアップ プログラムには、ホストへのアクセスに使用するデスクトップまたはコンソールのカラースキームが適用されます。

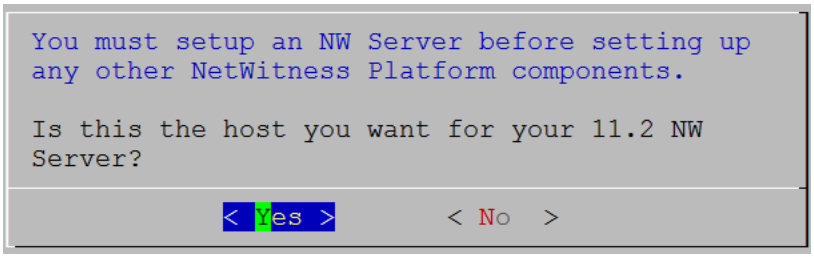
2. Tabキーで[**Accept**]に移動し、**Enter**キーを押します。




   [**Is this the host you want for your 11.2 NW Server**]プロンプトが表示されます。

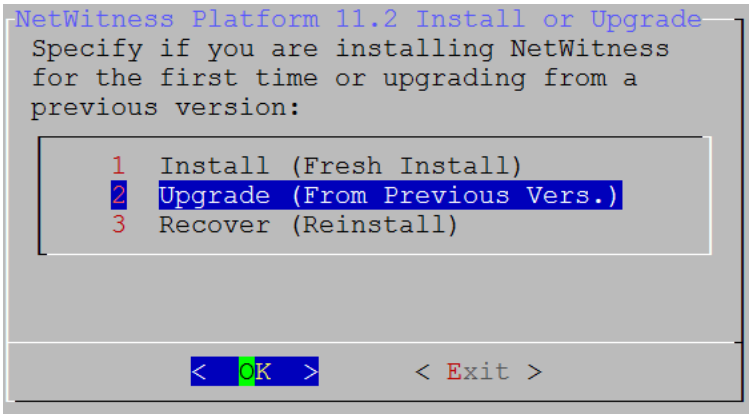
   **注意**：NW Serverに間違ったホストを選択してアップグレードを完了した場合は、「11.2 NW Serverホストのセットアップ」の手順1～11を繰り返して、誤りを修正する必要があります。

3. Tabキーで[**Yes**]に移動し、**Enter**キーを押します。




   NW Serverをすでに11.2にアップグレードした場合、[**No**]を選択します。
   [**Install or Upgrade**]プロンプトが表示されます。

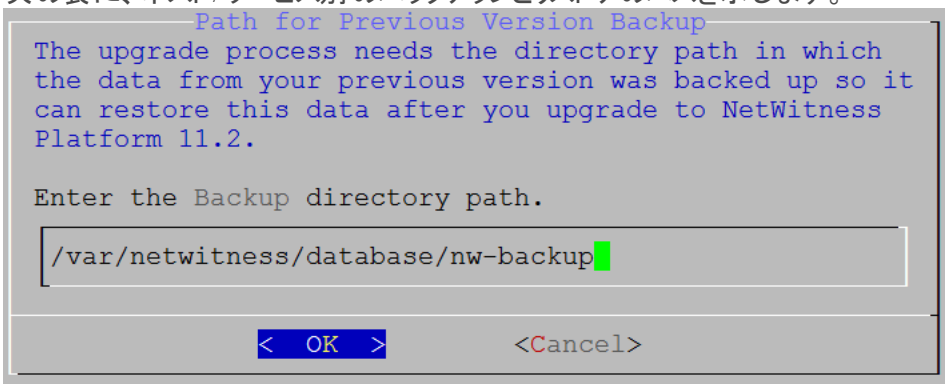
4. 下向き矢印を使用して、[**2 Upgrade (From Previous Vers.)**]を選択し、Tabキーで[**OK**]に移動し、**Enter**キーを押します。




[**Backup path**]プロンプトが表示されます。

**注意**:次のプロンプトに表示されるバックアップ パスは、バックアップを保存したパスと一致する必要があります。たとえば、バックアップ スクリプトは**/var/netwitness/database/nw-backup**をデフォルトのパスとして割り当てます。バックアップ時にデフォルトのバックアップ パスを使用し、その後変更していない場合は、次のプロンプトでも**/var/netwitness/database/nw-backup**を継続して使用する必要があります。

5. パスを変更しない場合は、Tabキーで[**OK**]に移動し、**Enter**キーを押します。パスを変更する場合は、パスを編集し、Tabキーで[**OK**]に移動し、**Enter**キーを押します。
次の表に、ホスト/サービス別のバックアップとリストアのパスを示します。




| ホスト | バックアップ パス | リストア パス |
|---|---|---|
| Malware | /var/lib/rsamlware/nw-backup | /var/netwitness/malware_analytics_server/nw-backup/restore |
| Event Stream Analysis | /opt/rsa/database/nw-backup | /var/netwitness/database/nw-backup/restore |
| NW Server | /var/netwitness/database/nw-backup | /var/netwitness/restore |
| その他のすべてのホスト | /var/netwitness/database/nw-backup | /var/netwitness/database/nw-backup/restore |

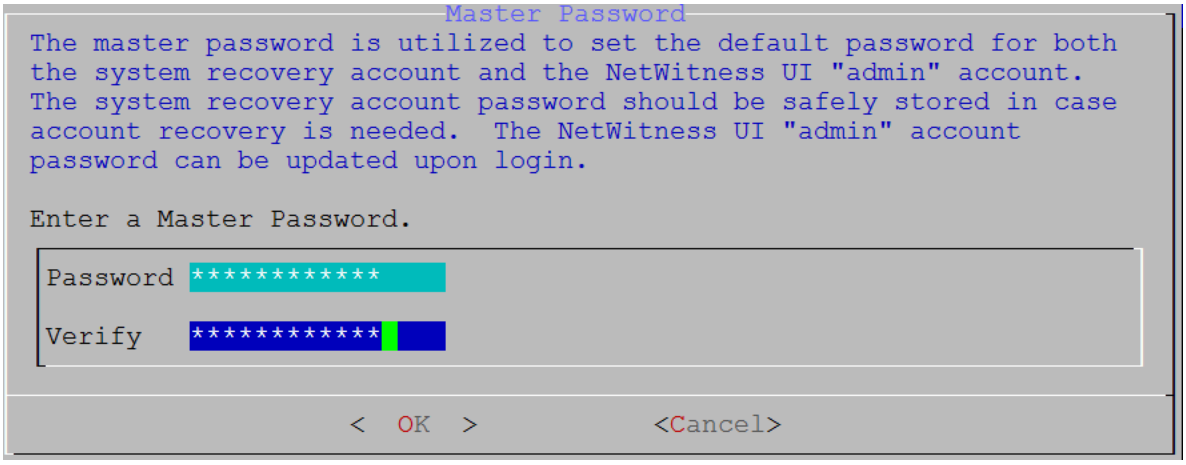
[**Master Password**]プロンプトが表示されます。

マスター パスワードと導入パスワードで使用可能な文字の一覧を、次に示します。

- 記号 : ! @ # % ^ + ,
- 数字 : 0〜9
- 小文字 : a〜z
- 大文字 : A〜Z

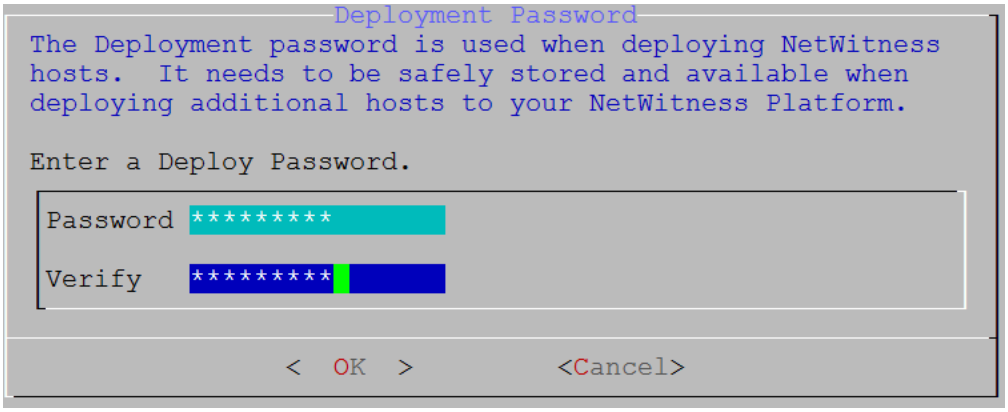
マスター パスワードと導入パスワードでは、紛らわしい文字は使用できません。例 : スペース{ } [ ] ( ) / \ ' " ` ~ ; : . < > -

6. [**Password**]に入力し、下向きの矢印で[**Verify**]に移動し、パスワードを再入力し、Tabキーで[**OK**]に移動し、**Enter**キーを押します。



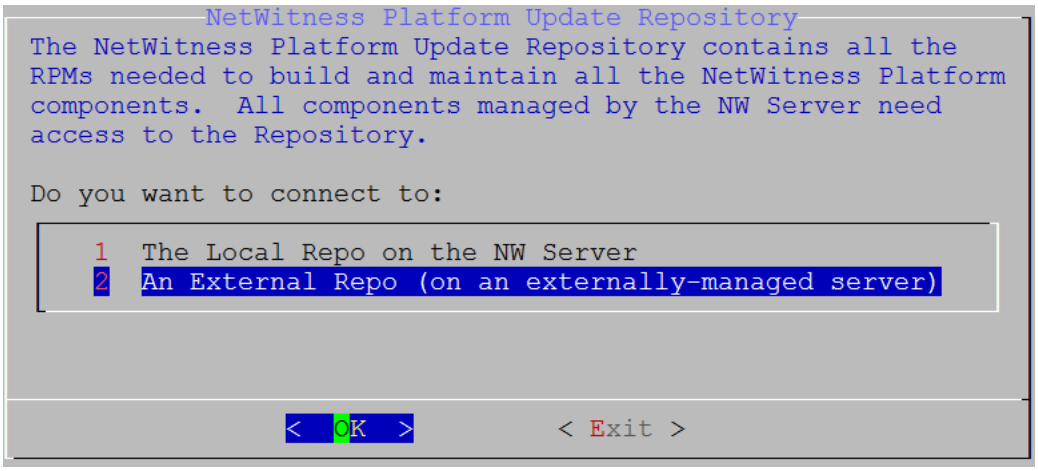

[**Deployment Password**]プロンプトが表示されます。

7. [**Password**]に入力し、下向きの矢印で[**Verify**]に移動し、パスワードを再入力し、Tabキーで[**OK**]に移動し、**Enter**キーを押します。



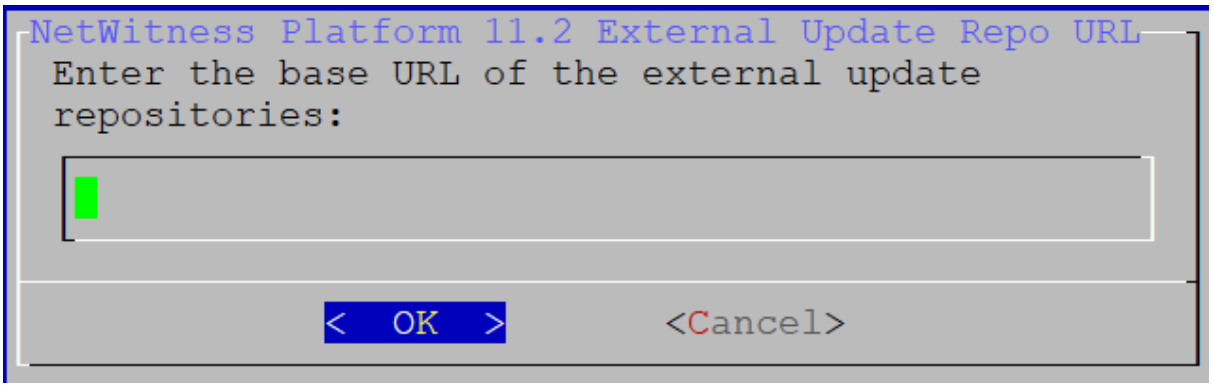

[**Update Repository**]プロンプトが表示されます。
NW Serverホストに使用したリポジトリと同じものを、すべてのホストで使用する必要があります。

8. 下向き矢印と上向き矢印を使用して、[**2 An External Repo (on an externally-managed Server)**]を選択します。



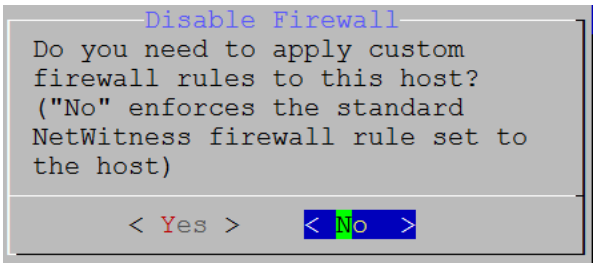

[**External Update Repo URL**]プロンプトが表示されます。
手順については、「付録D：外部リポジトリの作成」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

9. NetWitness Platform外部リポジトリのベースURL( たとえば、**http:/testserver/netwitness-repo**) を入力して、[**OK**]をクリックします。

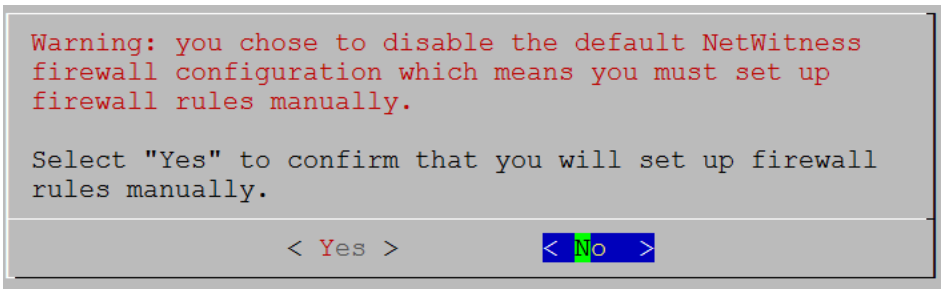



標準的な**ファイアウォール**構成を使用するか、**無効化**するかを選択するプロンプトが表示されます。

10. 標準的なファイアウォールの構成を使用するには、Tabキーを使用して[**No**]( デフォルト) に移動し、**Enter**キーを押します。標準的なファイアウォールの構成を無効化するには、Tabキーを使用して[**Yes**]に移動し、**Enter**キーを押します。

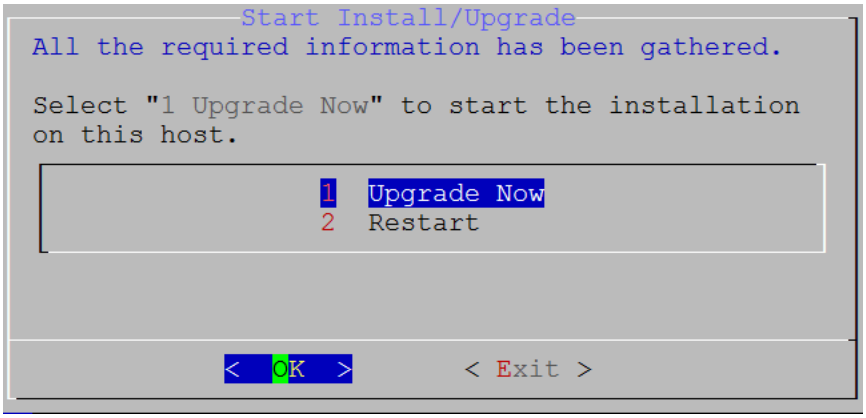



- [**Yes**]を選択して選択を確定するか、あるいは[**No**]を選択して標準的なファイアウォールの構成を使用します。



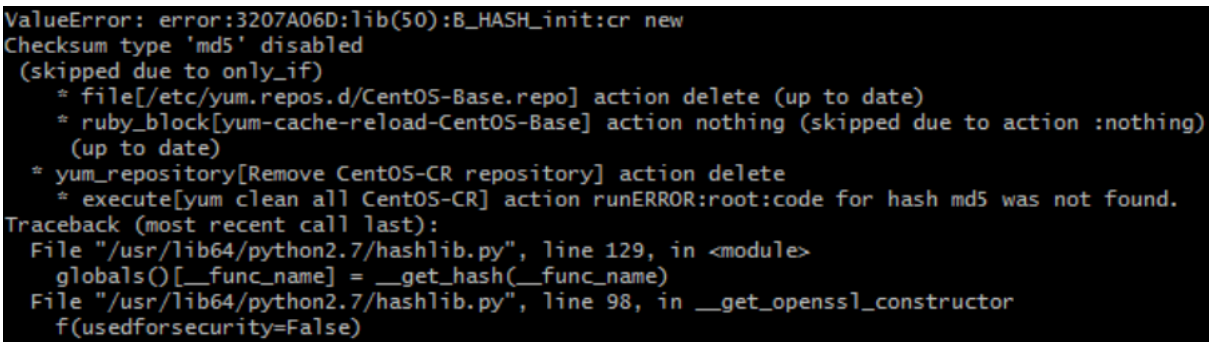

[**Install** or **Upgrade**]プロンプトが表示されます(**Recover**は選択できません。11.2の災害復旧用です。)

11. [**1 Upgrade Now**]を選択し、Tabキーで[**OK**]に移動して、Enterキーを押します。




「**Installation complete**」が表示されると、10.6.6.x SA Serverの11.2 NW Serverへのアップグレードは完了です。

**注**:`nwsetup-tui`コマンドを開始するときに表示される、次のスクリーンショットに示すようなハッシュコードのエラーは無視します。Yumは、セキュリティ操作にMD5を使用しないため、システムセキュリティに影響することはありません。




12. 非SA Serverホストを11.2にアップグレードする前に、「NW Server」を完了します。

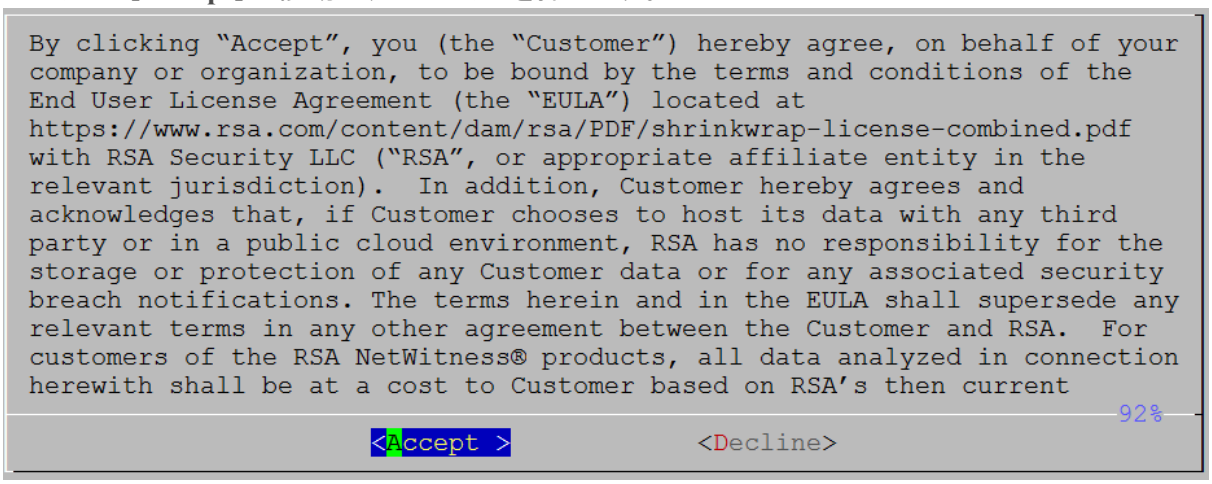
## 11.2 非NW Serverホストのセットアップ

10.6.6.xホストのデータを必ずバックアップしてください。**ホストをバックアップするには、「バックアップ手順」の手順に従う必要があります。**

**注意**：データができる限り最新になるよう、ホストを11.2にアップグレードする直前にバックアップを実行します。

次の手順を実行して、11.2 非NW Serverホストをセットアップします。

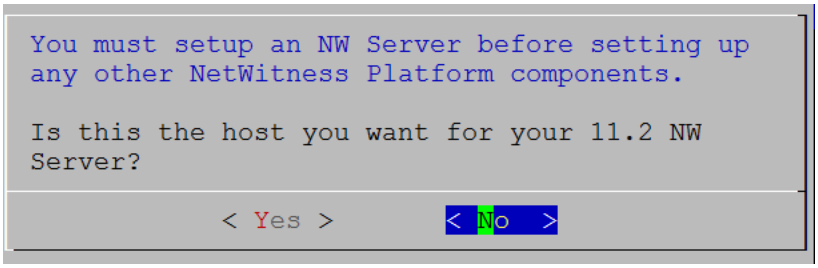
1. 11.2 非NW ServerのVMのコンソールにログインし、`nwsetup-tui`コマンドを実行します。
   これによりセットアップ プログラムが開始され、EULAが表示されます。
2. Tabキーで[**Accept**]に移動し、**Enter**キーを押します。




[**Is this the host you want for your 11.2 NW Server**]プロンプトが表示されます。

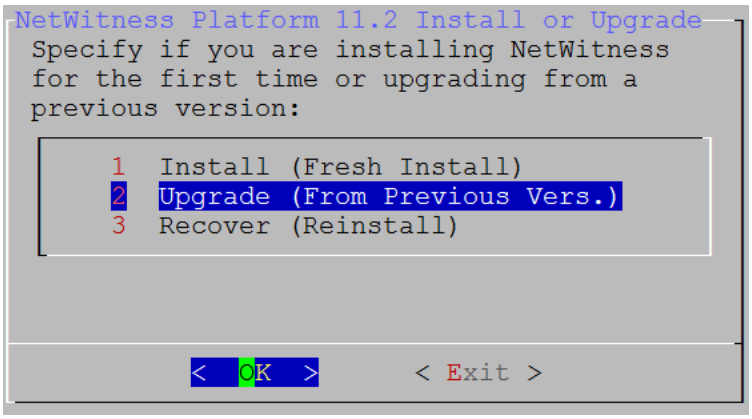
**注意**：NW Serverに間違ったホストを選択してアップグレードを完了した場合、「11.2 NW Server ホストのセットアップ」の手順1～11を繰り返して、誤りを修正する必要があります。

3. Tabキーで[**No**]に移動し、**Enter**キーを押します。



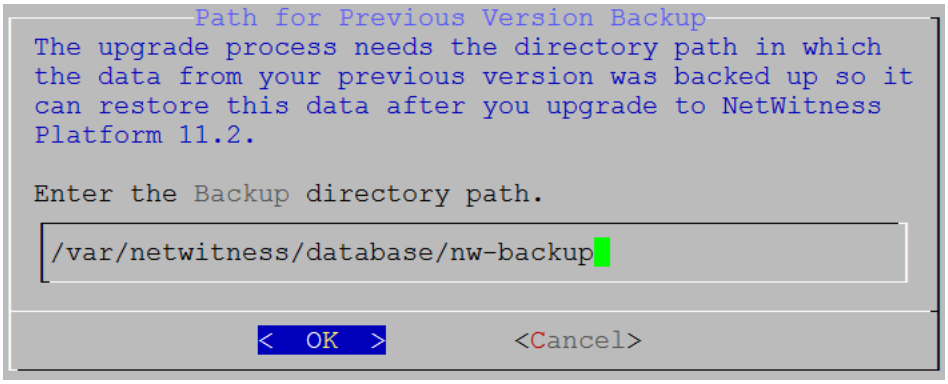

[**Install** or **Upgrade**]プロンプトが表示されます( **Recover**は選択できません。11.2の災害復旧用です。)

4. 下向き矢印を使用して、[**2 Upgrade (From Previous Vers.)**]を選択し、Tabキーで[**OK**]に移動し、**Enter**キーを押します。




[**Backup path**]プロンプトが表示されます。

5. パスを変更しない場合は、Tabキーで[**OK**]に移動し、**Enter**キーを押します。パスを変更する場合は、パスを編集し、Tabキーで[**OK**]に移動し、**Enter**キーを押します。



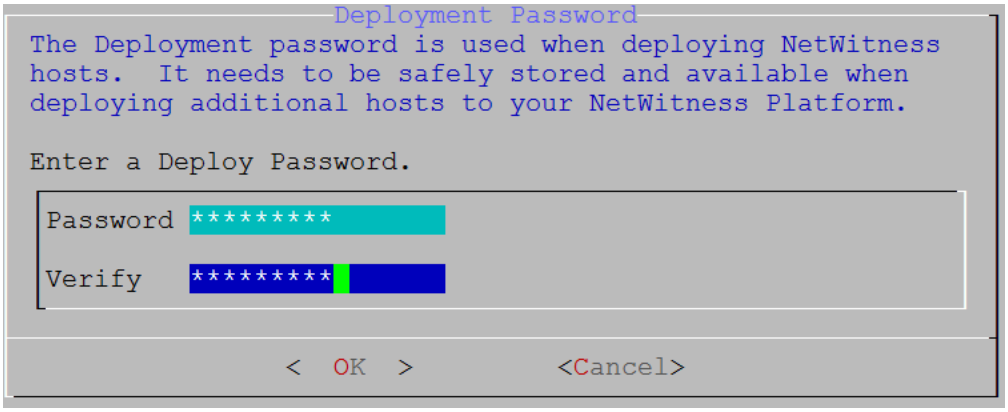

次の表に、ホスト/サービス別のバックアップとリストアのパスを示します。

| ホスト | バックアップ パス | リストア パス |
|---|---|---|
| Malware | /var/lib/rsamlware/nw-backup | /var/netwitness/malware_analytics_server/nw-backup/restore |
| Event Stream Analysis | /opt/rsa/database/nw-backup | /var/netwitness/database/nw-backup/restore |
| NW Server | /var/netwitness/database/nw-backup | /var/netwitness/restore |
| その他のすべてのホスト | /var/netwitness/database/nw-backup | /var/netwitness/database/nw-backup/restore |

[**Deployment Password**]プロンプトが表示されます。

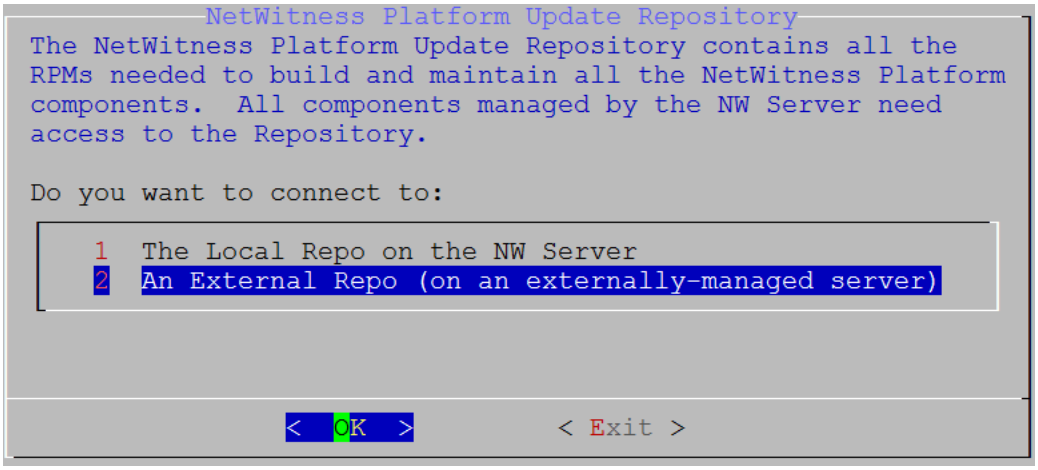
**注**:NW Serverのアップグレード時に使用したのと同じ導入パスワードを使用する必要があります。

6. [**Password**]に入力し、下向きの矢印で[**Verify**]に移動し、パスワードを再入力し、Tabキーで[**OK**]に移動し、**Enter**キーを押します。



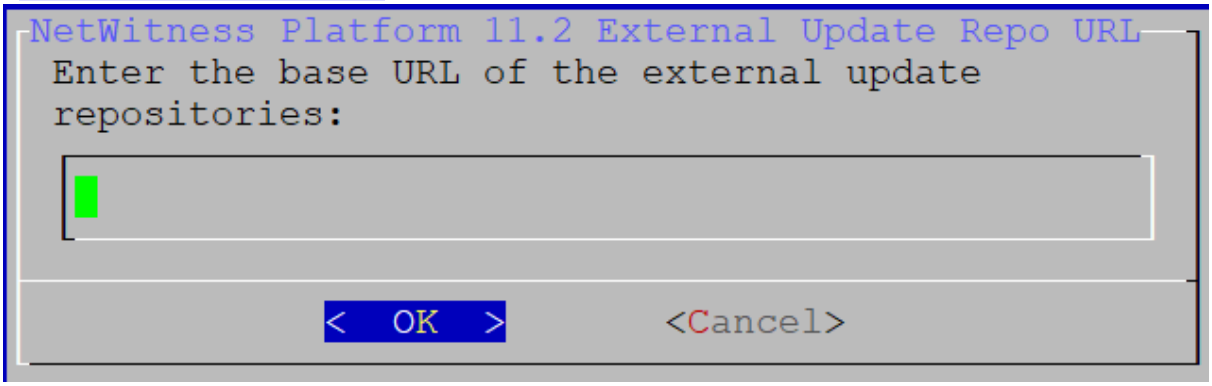

[**Update Repository**]プロンプトが表示されます。

7. 下向き矢印と上向き矢印を使用して、[**2 An External Repo (on an externally-managed Server)**]を選択し、Tabキーを使用して[**OK**]に移動し、**Enter**キーを押します。



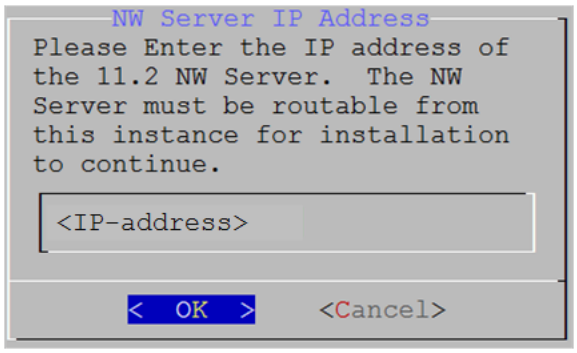

[**External Update Repo URL**]プロンプトが表示されます。
リポジトリはRSAの更新およびCentOSの更新を取得する場所です。

8. NetWitness Platform外部リポジトリのベースURL( たとえば、**http://testserver/netwitness-repo**) を入力して、[**OK**]をクリックします。外部リポジトリと外部リポジトリURLを作成する手順については、「付録D:外部リポジトリの作成」を参照してください。



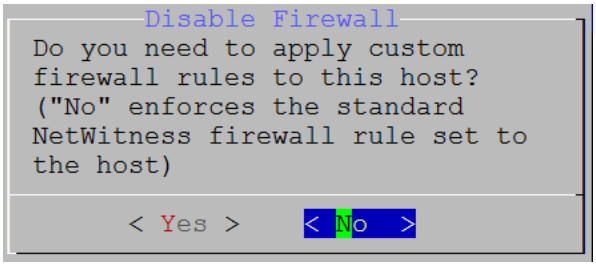
[**NW Server IP Address**]プロンプトが表示されます。

9. NW ServerのIPアドレスを入力し、Tabキーを使用して[**OK**]を選択し、**Enter**キーを押します。

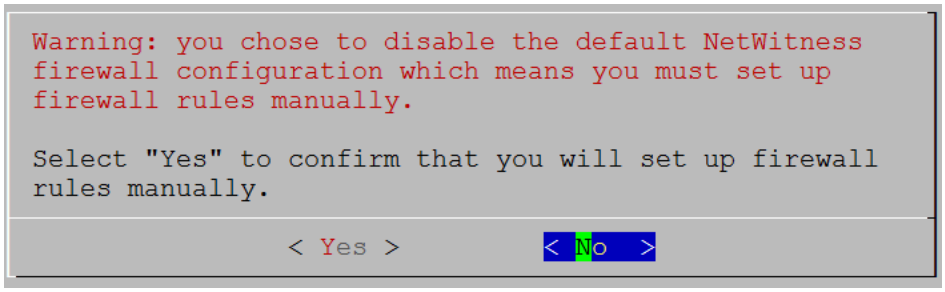



標準的な**ファイアウォール**構成を使用するか、**無効化**するかを選択するプロンプトが表示されます。

10. 標準的なファイアウォールの構成を使用するには、Tabキーを使用して[**No**](デフォルト)に移動し、Enterキーを押します。標準的なファイアウォールの構成を無効化するには、Tabキーを使用して[**Yes**]に移動し、**Enter**キーを押します。



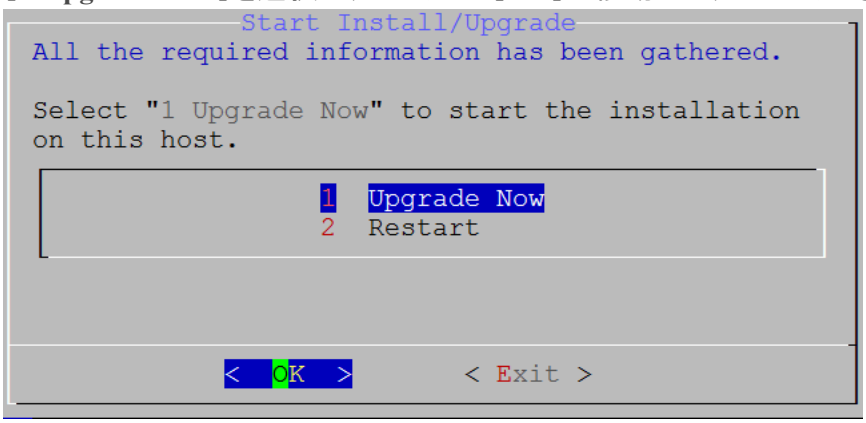

- [**Yes**]を選択すると、選択が確定します。




- [**No**]を選択すると、標準的なファイアウォールの構成が適用されます。

[**Install** or **Upgrade**]プロンプトが表示されます(**Recover**は使用できません。11.2の災害復旧用です。)

11. [**1 Upgrade Now**]を選択し、Tabキーで[**OK**]に移動して、**Enter**キーを押します。




「**Installation complete**」が表示されると、ホストの11.2へのアップグレードは完了です。

12. 次の手順で、このホストにサービスをインストールします。

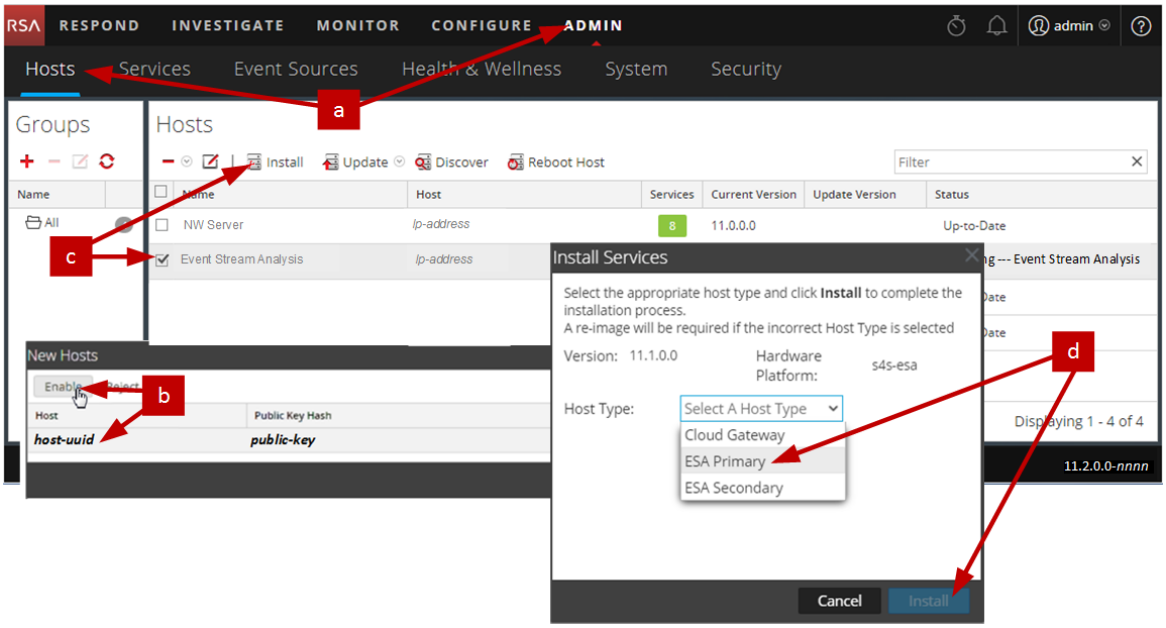
    a. NetWitness Platformにログインし、[**管理**]＞[**ホスト**]の順にクリックします。
    [**新しいホスト**]ダイアログが表示され、[**ホスト**]ビューがバックグラウンドでグレー表示されます。

    > **注**：[**新しいホスト**]ダイアログが表示されない場合、[ホスト]ビューのツールバーで[**検出**]をクリックします。

    b. [**新しいホスト**]ダイアログでホストをクリックし、[**有効化**]をクリックします。
    [**新しいホスト**]ダイアログが閉じ、[**ホスト**]ビューにホストが表示されます。

    c. [**ホスト**]ビューでそのホスト(たとえば**Event Stream Analysis**)を選択し、Install をクリックします。
    [**サービスのインストール**]ダイアログが表示されます。

    d. 適切なサービス(たとえば**ESAプライマリ**)を選択し、[**インストール**]をクリックします。




NetWitness Platformの非NW Serverホストのアップグレードが完了しました。

**注 :** Respondホストを10.6.6.xから11.2にアップグレードする場合、Respondが再びオンラインになるまでにある程度の時間がかかります。これはRespondの復元中にデータがインデックスされるからです。Mongoデータベース内のデータのサイズによって時間は変わります。

# Legacy Windows収集の更新またはインストール

「*RSA NetWitness Legacy Windows収集ガイド*」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

**注：**Legacy Windows収集のインストールまたは更新の後、正常にログを収集するため、システムを再起動します。

# アップグレード後のタスク

このトピックでは、10.6.6.xから11.2にアップグレードした後に完了する必要があるタスクについて説明します。これらのタスクは、次のカテゴリに分類されます。

- 全般
- NW Server
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Investigate
- ログ収集
- Decoder およびLog Decoder
- Reporting Engine
- Respond
- RSA Archer® Cyber Incident & Breach Response
- UEBA( User and Entity Behavior Analytics)
- バックアップ

## 全般

### タスク1:ポート15671が正しく設定されていることを確認

**ポート15671**は11.xで新しく追加されましたが、ファイアウォールでこのポートを開く必要はありません。「*RSA NetWitness® Platform導入ガイド*」の「ネットワーク アーキテクチャとポート」トピックを参照し、15671を含むすべてのポートが正しく構成されていることを確認してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

### (オプション) タスク2:カスタムAnalystsロールのリストア

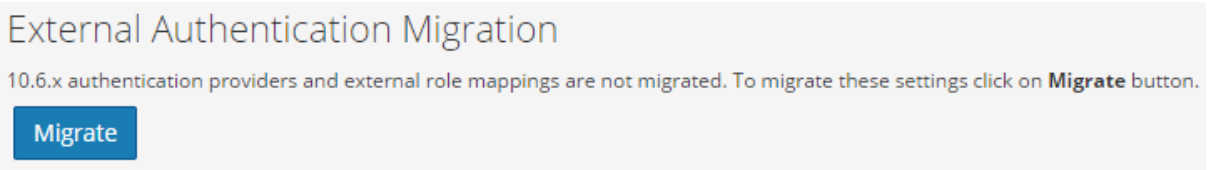
10.6.6.xでカスタマイズしたAnalystsロールを使用していた場合は、11.2で再設定する必要があります。(オプション)「*RSA NetWitness Platform システム セキュリティとユーザ管理ガイド*」の「ロールの追加と権限の割り当て」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

# NW Server

## タスク3: AD( Active Directory) の移行

NetWitness Platform 11.2のユーザ インタフェースに最初にログインしたとき、[移行]ボタンをクリックしてADの移行を完了する必要があります。

1. NetWitness Platform 11.2に`admin user`の認証情報でログインします。
2. **NetWitness Platform** 11.2メニューで、[**管理**]>[**セキュリティ**]の順に選択し、[**設定**]タブをクリックします。
   次のダイアログが表示されます。




3. [**移行**]をクリックします。
   移行が完了するとダイアログが閉じます。

## タスク4: 移行したAD構成の変更と証明書のアップロード

10.6.6.xでAD( Active Directory) サーバで認証を行い、ADサーバとの接続にSSLを使用していた場合は、移行後のAD構成を変更し、Active Directoryサーバの証明書をアップロードする必要があります。

証明書をアップロードするには、移行後のAD構成で次の手順を実行します。

1. **NetWitness Platform** 11.2メニューで、[**管理**]>[**セキュリティ**]の順に選択し、[**設定**]タブをクリックします。
2. [**Active Directory構成**]で、AD構成を選択し、をクリックします。
   [構成の編集]ダイアログが表示されます。
3. [**証明書ファイル**]フィールドで、[**参照**]をクリックして、証明書ファイルを選択します。
4. [**保存**]をクリックします。

## タスク5: 11.2でのPAM( Pluggable Authentication Module) の再構成

11.2にアップグレードした後、PAMを再構成する必要があります。手順については、「*RSA NetWitness® Platformシステム セキュリティとユーザ管理ガイド*」の「PAMログイン機能の構成」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

10.6.6.xのバックアップ データの/etcディレクトリにある10.6.6.xのPAM構成ファイルを参照できます。

### タスク6: NTPサーバのリストア

NetWitness Platform 11.2のユーザ インタフェースを使用し、NTPサーバの構成をリストアする必要があります。NTPサーバの構成情報は、`$BUPATH/restore/etc/ntp.conf`にあります。`/var/netwitness/restore/etc/ntp.conf`ファイルのNTPサーバ名とホスト名を使用します。NTPサーバを追加する方法の詳細については、「*RSA NetWitness® Platform 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。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

### タスク7: FlexNet Operations-On Demand Accessを使用しない環境でのライセンスのリストア

ご使用の環境でFlexNet Operations-On Demandにアクセスしない場合は、NetWitness Platformライセンスを再度ダウンロードする必要があります。ライセンスを再ダウンロードする方法については、「*RSA NetWitness Platform ライセンス管理ガイド*」の「ステップ1.NetWitness Serverの登録」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

### タスク8: 仮想NW Serverのライセンスを10.6.6.x MACアドレスに再マッピング

仮想マシンのSecurity Analytics Serverをアップグレードする場合は、11.2 NW Serverの仮想ホストのMACアドレスを10.6.6.xのMACアドレスに変更することにより、ライセンスを維持できます。ライセンスを新しいMACアドレスに再マッピングする場合は、「*RSA NetWitness Platform ライセンス管理ガイド*」の「ステップ1.NetWitness Serverの登録」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

### (オプション) タスク9: 標準ファイアウォール構成を無効化した場合、カスタムiptablesを追加

アップグレード中に、標準のファイアウォール構成を使用するか、または無効化するかを選択できます。無効化した場合は、無効化したすべてのホストで、次の手順をベースラインとして、ユーザ管理のファイアウォール ルールを作成します。

**注:** バックアップのrestoreフォルダにある、`$BUPATH/restore/etc/sysconfig/iptables`と`$BUPATH/restore/etc/sysconfig/ip6tables`を参照し、`ip6tables`ファイルと`iptables`ファイルを更新できます。`/etc/netwitness/firewall.cfg`ファイルには、標準の`iptables`のファイアウォール ルールが含まれています。

1. SSHで各ホストに接続し、rootでログインします。
2. `ip6tables`ファイルと`iptables`ファイルを更新し、カスタムのファイアウォール ルールを追加します。
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```
3. `iptables`サービスと`ip6tables`サービスを再ロードします。
   ```
   service iptables reload
   service ip6tables reload
   ```

### (オプション) タスク10: 信頼接続を設定していない場合、SSLポートを指定

一度も信頼接続を設定していない場合のみ、このタスクを実行します。次の場合は、信頼接続が設定されていません。

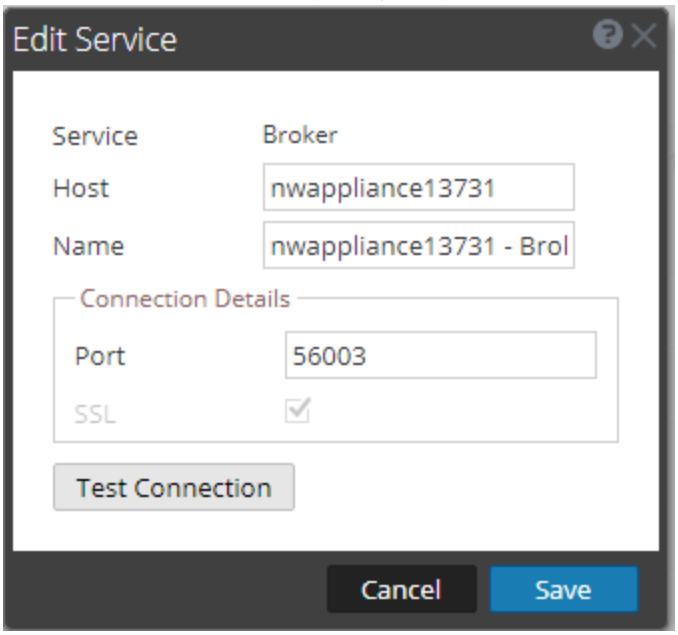
- 10.3.2またはそれ以前の基本ISOイメージを使用している。
- RPMパッケージだけを使用して、システムを10.6.6.xに更新した。

このような環境のコア サービスは非SSLポート50XXを使用しているため、NetWitness Platform 11.2はこれらのサービスと通信できません。[サービスの編集]ダイアログで、コア サービスのポートをSSLポートに更新する必要があります。

1. **NetWitness Platform** 11.2メニューで、[**管理**]>[**サービス**]を選択します。
2. 各コア サービスを選択し、ポートを非SSLからSSLに変更します。

| サービス | 非SSL | SSL |
|---|---|---|
| Broker | 50003 | 56003 |
| Concentrator | 50005 | 56005 |
| Decoder | 50004 | 56004 |
| Log Decoder | 50002 | 56002 |

3. [**サービス**]ビューのツールバーで、(編集)をクリックします。
[サービスの編集]ダイアログが表示されます。
4. 表に示すように、ポートを非SSLからSSLに変更し、[**保存**]をクリックします(例えば、Brokerのポートを50003から56003に変更します)。




## タスク11:(オプション) Logstash出力構成ファイルで更新されていない監査ログ テンプレートの修正

**問題:** 10.6.6から11.2、または11.0.0.0から11.2に更新するとき、グローバル監査が構成されている場合、Logstash出力構成ファイルで監査ログ テンプレートが更新されません。

**回避策**: グローバル監査が構成されている場合、グローバル通知サーバのいずれかのsyslogエントリーを編集し、[保存]をクリックして最新の監査ログの構成を適用する必要があります。

11.0.xでグローバル監査が構成されている場合、最新のグローバル監査の構成を適用するために、次の手順を実行する必要があります。

1. **NetWitness Platform** 11.2メニューで、[**管理**]＞[**システム**]＞[**グローバル通知**]の順に選択します。
   [**グローバル通知**]ビューが表示されます。
2. [**サーバ**]タブをクリックして、任意のsyslogサーバを選択します。
3. (編集アイコン)をクリックして、[**保存**]をクリックします。

## RSA NetWitness® Endpoint

### タスク12: メッセージ バス経由のEndpointアラートの再構成

1. NetWitness Endpoint Server上で、`C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe`ファイル内の仮想ホストの構成を、次のように変更します。
   ```
   <add key="IMVirtualHost" value="/rsa/system" />
   ```

   **注**: NetWitness Platform 11.2では、仮想ホストは`/rsa/system`です。10.6.6.x以前のバージョンでは、仮想ホストは`/rsa/sa`です。
2. API ServerとConsole Serverを再起動します。
3. SSHでNW Serverに接続し、`root`の認証情報でログインします。
4. 次のコマンドを実行して、すべての証明書をトラストストアに追加します。
   ```
   orchestration-cli-client --update-admin-node
   ```
5. 次のコマンドを実行して、RabbitMQ Serverを再起動します。
   ```
   systemctl restart rabbitmq-server
   ```
   NetWitness Endpointアカウントは自動的にRabbitMQで利用可能になります。
6. `/etc/pki/nw/ca/nwca-cert.pem`ファイルと`/etc/pki/nw/ca/ssca-cert.pem`ファイルをNW Serverからインポートし、Endpoint Serverの信頼できるルート証明書ストアに追加します。

### タスク13: Javaバージョンの変更により、レガシーEndpointからの定期実行Feedを再構成

Javaバージョンの変更により、レガシーEndpointの定期実行Feed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。

1. 「*RSA NetWitness Endpoint統合ガイド*」にある「繰り返しFeedを通じた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。
   NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

# RSA NetWitness® Endpoint Insights

## (オプション) タスク14: Endpoint HybridまたはEndpoint Log Hybridのインストール

以下を参照してください。

「*RSA NetWitness Platform 11.2 物理ホスト インストール ガイド*」(物理ホストのインストール手順)。

「*RSA NetWitness Platform 11.2 仮想ホスト インストール ガイド*」(仮想ホストのインストール手順)。

# ESA(Event Stream Analysis) タスク

## タスク15: ESAの自動脅威検出の再構成

10.6.6.xで自動脅威検出を使用していた場合、次の手順を実行し、11.2のESA Analyticsサービスに再構成する必要があります。

1. **NetWitness Platform** 11.2メニューで、[**管理**]>[**システム**]>[**ESA Analytics**]を選択します。Suspicious Domainsモジュールである、ネットワーク データ用C2(コマンド&コントロール) モジュールとログ用C2モジュールには、「**domains_whitelist**」という名前のホワイトリストが必要です。
2. (オプション) Context Hubサービスの[**リスト**]タブに古い自動脅威検出のホワイトリストが表示される場合、次の操作を実行します。
   a. [**管理**]>[**サービス**]をクリックして、Context Hubサービスを選択し、アクション(  )ドロップダウン メニューで、[**表示**]>[**構成**]>[**リスト**]タブをクリックします。
   b. 古い自動脅威検出のホワイトリストの名前を、Suspicious Domainsモジュールが使用する「`domains_whitelist`」に変更します。

詳細については、「*NetWitness Platform自動脅威検出ガイド*」および「*NetWitness Platform ESA構成ガイド*」の「ESA Analyticsの構成」セクションを参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

## タスク16: Web Threat Detection、Archer Cyber Incident & Breach ResponseまたはNetWitness Endpointとの統合のためのSSL相互認証の構成

Web Threat Detection、Archer Cyber Incident & Breach Response、NetWitness Endpointと統合する場合、RabbitMQメッセージ バスへの接続時の認証のために、統合する各システムにSSL相互認証を構成する必要があります。

**注**: 10.6.6.xデータをバックアップしたときに取得したRabbitMQユーザ名とパスワードを使用します(「バックアップ手順」を参照してください)。

1. NetWitness Platformに統合するホスト システムにユーザを作成します。ホストにログインし、次の`rabbitmqctl`コマンドを実行します。

   ```
   > rabbitmqctl add_user <username> <password>
   ```

   例:

   ```
   > rabbitmqctl add_user wtd-incidents incidents
   ```

2. 次のコマンドを実行して、ユーザの権限を設定します(ステップ1のユーザ名を使用)。
   `> rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*", ".*"`
   例:
   `> rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*", ".*", ".*"`

### タスク17: Threat - Malware Indicatorsダッシュボードの有効化

11.2.0では、10.6.6.xの**Threat -Indicatorsダッシュボード**の名前が**Threat - Malware Indicatorsダッシュボード**に変更されました。10.6.6.xでこのダッシュボードを使用していた場合は、次の操作を実行する必要があります。

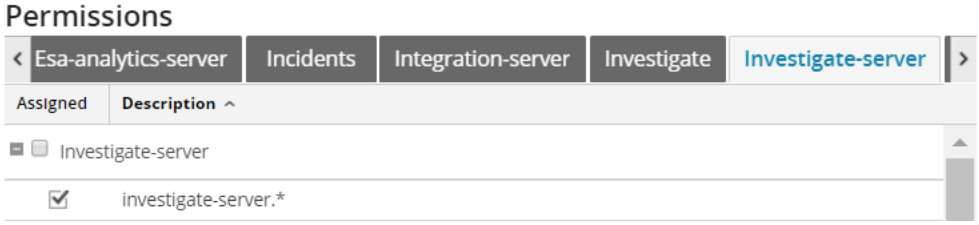
1. 11.2の**Threat - Malware Indicatorsダッシュボード**を有効化します。
2. 新しいダッシュレットのデータソースを設定します。
   NetWitness Platformのダッシュレットの詳細は、RSA Link( https://community.rsa.com/docs/DOC-81463) の「ダッシュレット」を参照してください。

## Investigate

### タスク18: カスタマイズしたユーザロールにイベント分析にアクセスするInvestigate-server権限があることを確認

11.2.0.0にアップグレードした後、カスタマイズされたどのユーザロールもデフォルトでは`investigate-server.*` 権限が有効になっていません。適切なユーザロールにイベント分析へのアクセス権限があることを確認するには、次の手順を実行します。

1. `Admin user`の資格情報を使用してNetWitness Platform 11.2.0.0にログインし、[**管理**]>[**セキュリティ**]に移動します。
2. [**ロール**]タブをクリックします。
3. `investigate-server.*` 権限が必要なロールを選択して、(編集アイコン)をクリックします。
4. [**権限**]セクションにある[**Investigate-server**]タブを選択します。
5. [**Investigate-server**]チェックボックスがオンでない場合、イベント分析にアクセスする必要のあるユーザのロールでは、オンに設定します。




6. [**保存**]をクリックします。

# ログ収集

## タスク19: アップグレード後のLog CollectorのStable System Valueのリセット

11.2にアップグレードした後、次のタスクを実行して、Log CollectorのStable System Valueをリセットし、すべての収集プロトコルが正常に再開したことを確認します。

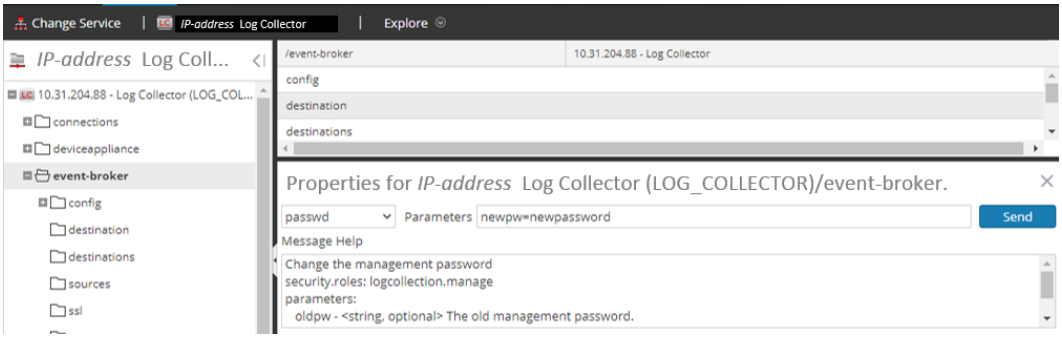
**LockboxのStable System Valueのリセット**

Lockboxには、Log Collectorのイベント ソースとその他のパスワードを暗号化するためのキーが保存されます。Log Collectorサービスは、Stable System Valueが変更されたため、Lockboxを開くことができません。そのため、LockboxのStable System Valueをリセットする必要があります。「ログ収集: ステップ3. Lockbox設定」(「*RSA NetWitness® Platformログ収集構成ガイド*」) を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

**Log CollectorサービスのRabbitMQユーザ アカウントのパスワードの更新**

Log CollectorサービスのRabbitMQユーザ アカウントのパスワードが変更された場合は、11.2へのアップグレード後に再入力する必要があります。

1. **NetWitness Platform** 11.2メニューで、[**管理**]>[**サービス**]を選択します。
2. Log Collectorを選択します。
3.  (アクション) > [**表示**] > [**エクスプローラ**]をクリックします。
4. `event-broker`を右クリックして、[**プロパティ**]を選択します。
5. ドロップダウン リストから「`passwd`」を選択し、[パラメータ]に「`newpw=><newpassword>`」と入力し(`<newpassword>`はRabbitMQユーザ アカウントのパスワードです)、[**送信**]をクリックします。




## (オプション: FIPSが有効な10.6.6.xのLog Collector、Log Decoder、Network Decoderをアップグレードした場合)

## タスク20: FIPSモードの有効化

Log Collector、Log Decoder、Decoderを除くすべてのサービスではFIPSが有効になっています。Log Collector、Log Decoder、Decoder以外のサービスではFIPSを無効にできません。これらのサービスでFIPSを有効化する方法の詳細については、「システム メンテナンス: FIPSの有効化/無効化」トピックを参照してください(「*RSA NetWitness® Platformシステム メンテナンス ガイド*」)。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

# DecoderおよびLog Decoder

## (オプション) タスク21: GeoIP2 Parserのメタデータの有効化

デフォルトでは、GeoIP2 Parserが生成するメタデータはGeoIP Parserよりも少なくなります。11.2にアップグレードした後、追加のメタデータが必要な場合は、各Decoderで(1回だけ) それらのメタデータを有効化する必要があります。この設定はアップグレード後に変更することもできます。`isp`および`org`のメタフィールドは、通常、`domain`と同じ値を生成する点に留意してください。

メタデータを有効にするには、次の手順を実行します。

1. [**管理**]>[**サービス**]に移動します。
2. [**管理**]>[**サービス**]ビューで、Log DecoderまたはDecoderを選択します。
3. アクション アイコン( ) をクリックし、[**表示**]>[**構成**]を選択します。[Parser構成]パネルが表示されるので、そこから[**GeoIP2**]を選択して目的のメタデータを有効にすることができます。

GeoIP2 Parserの詳細については、「*DecoderおよびLog Decoder構成ガイド*」の「GeoIP2 ParserとGeoIP Parser」のトピックを参照してください。

# Reporting Engine

## タスク22: 外部SyslogサーバのCA証明書をReporting Engineにリストア

アップグレード前に作成したバックアップからCA証明書をリストアする必要があります。バックアップ スクリプトは、10.6.6.xのCA証明書を`/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts`ディレクトリにバックアップします。

次の手順を実行し、CA証明書を11.2にリストアします。

1. SSHでNW Serverホストに接続します。
2. CA証明書をエクスポートします。
   ```
   keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
   ```
3. `/etc/pki/nw/trust/import`ディレクトリに、CA pemをコピーします。

## (オプション) タスク23: Reporting Engineの外部ストレージのリストア

Reporting Engineの外部ストレージ(レポート保存用のSANやNASなど) がある場合は、アップグレード前にリンクを解除し、アップグレード後に再マウントする必要があります。手順については、「Reporting Engine: 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」(「*RSA NetWitness® Platform Reporting Engine構成ガイド*」) を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

# Respond

## タスク24：Respondサービスのカスタム キーのリストア

10.6.6.xでは、**groupBy**句で使用するためのカスタム キーを追加した場合、`alert_rules.json`ファイルが変更されました。`alert_rules.json`ファイルには、集計ルールのスキーマが含まれています。`alert_rules.json`ファイルは次の新しい場所に移動されました。
`/var/lib/netwitness/respond-server/scripts`

1. バックアップ ディレクトリ内の`/opt/rsa/im/fields/alert_rules.json`ファイルから、カスタム キーをコピーします。
   このディレクトリは、10.6.6.xのバックアップから`alert_rules.json`ファイルがリストアされた場所です。
2. 11.2の`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`に移動します。
   これは、11.2の新しいファイルです。
3. `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`を編集し、ステップ1でコピーしたカスタム キーを追加します。

## タスク25: Respondサービスのカスタム正規化スクリプトのリストア

11.2では、Respondサービスの正規化スクリプトが再設計され、次の新しい場所に移動しました。
`/var/lib/netwitness/respond-server/scripts`
10.6.6.xでこれらのスクリプトをカスタマイズした場合は、次の操作を実行する必要があります。

1. `/opt/rsa/im/scripts`ディレクトリに移動します。
   このディレクトリは、次のRespondサービスの正規化スクリプトが10.6.6.xのバックアップからリストアされる場所です。
   ```
   data_privacy_map.js
   normalize_alerts.js
   normalize_core_alerts.js
   normalize_ecat_alerts.js
   normalize_ma_alerts.js
   normalize_wtd_alerts.js
   utils.js
   ```
2. 10.6.6.xのスクリプトから、カスタム ロジックをコピーします。
3. `/var/lib/netwitness/respond-server/scripts`ディレクトリに移動します。
   このディレクトリは、NetWitness Platform 11.2で再設計されたスクリプトを格納する場所です。
4. ステップ2で10.6.6.xスクリプトからコピーしたカスタム ロジックを含むように、新しいスクリプトを編集します。
5. `/opt/rsa/im/fields/alert_rules.json`ファイルからカスタム ロジックをコピーします。
   `alert_rules.json`ファイルには、集計ルールのスキーマが含まれています。

## タスク26: カスタム ロールに対応の通知設定の権限を追加する

対応の通知設定の権限により、Respond Administrators、Data Privacy Officers、SOC Managers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することが可能になります。

これらの設定にアクセスするには、既存のNetWitness Platformの標準のユーザ ロールに権限を追加する必要があります。カスタム ロールに権限を追加する必要もあります。「*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。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

## タスク27: 対応の通知設定を手動で構成

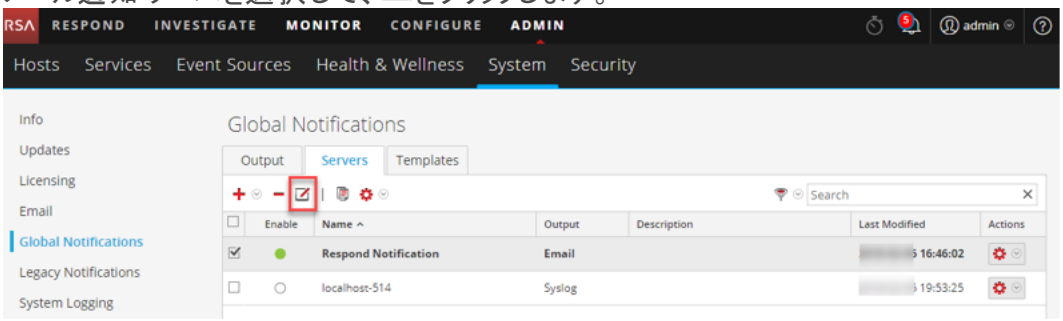
NetWitness Platform 10.6.6.x～11.2のIncident Managementの通知設定は、11.2の対応の通知設定とは異なるため、既存の10.6.6.x～11.2の通知設定は11.2には移行されません。

NetWitnessの対応の通知の設定によって、インシデントが作成または更新されたときに、SOCマネージャや、インシデントに割り当てられたアナリストにメール通知を送信することができます。

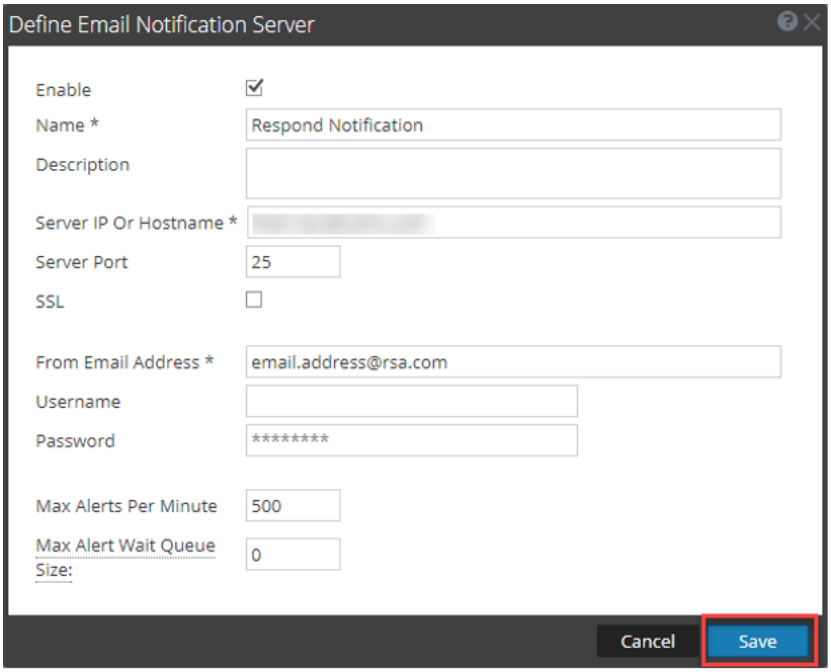
対応の通知設定を手動で構成するには、[**構成**]>[**対応の通知**]にアクセスします。「*NetWitness Respond構成ガイド*」の「対応のメール通知設定の構成」の手順を参照してください。

10.6.6.x～11.2の通知サーバは、メール サーバのドロップダウン リストには表示されません。メール サーバはグローバル通知の[サーバ]パネル([**管理**]>[**システム**]>[**グローバル通知**]>[**サーバ**]タブ)で編集および保存する必要があります。

1. **NetWitness Platform** 11.2メニューで、[**管理**]＞[**システム**]＞[**グローバル通知**]＞[**サーバ**]タブの順に選択します。
2. [**構成**]＞[**対応の通知**]にアクセスします。[対応の通知の設定]ビューが表示されます。
3. この時点では、[メール サーバ]ドロップダウン リストにメール通知サーバは表示されません。
4. [**メール サーバ設定**]リンクをクリックします。グローバル通知パネルが表示されます。
5. [**サーバ**]タブをクリックします。
6. 各メール通知サーバについて、次の手順を実行します。
   a. メール通知サーバを選択して、をクリックします。




   b. [メール通知サーバの定義]ダイアログで、必要な情報を入力して[**保存**]をクリックします。




7. [**構成**]＞[**対応の通知**]に戻ります。サーバが[**メール サーバ**]ドロップダウン リストに表示されます。
   Incident Managementのカスタム通知テンプレートは11.2に移行することはできません。11.2ではカスタム テンプレートはサポートされていません。

## タスク28：デフォルトのインシデント ルールのGroup By値の更新

デフォルトのインシデント ルールのうち4つは、Group By値として「Source IP Address」を使用するようになりました。デフォルトのルールを更新するには、次のデフォルトのルールのGroup By値を「Source IP Address」に変更します。

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

1. [**構成**] > [**インシデント ルール**]に移動し、更新するルールの[**名前**]列のリンクをクリックします。[インシデント ルールの詳細]ビューが表示されます。
2. [**Group By**]フィールドで、新しいGroup By値を選択します。
3. [**保存**]をクリックしてルールを更新します。

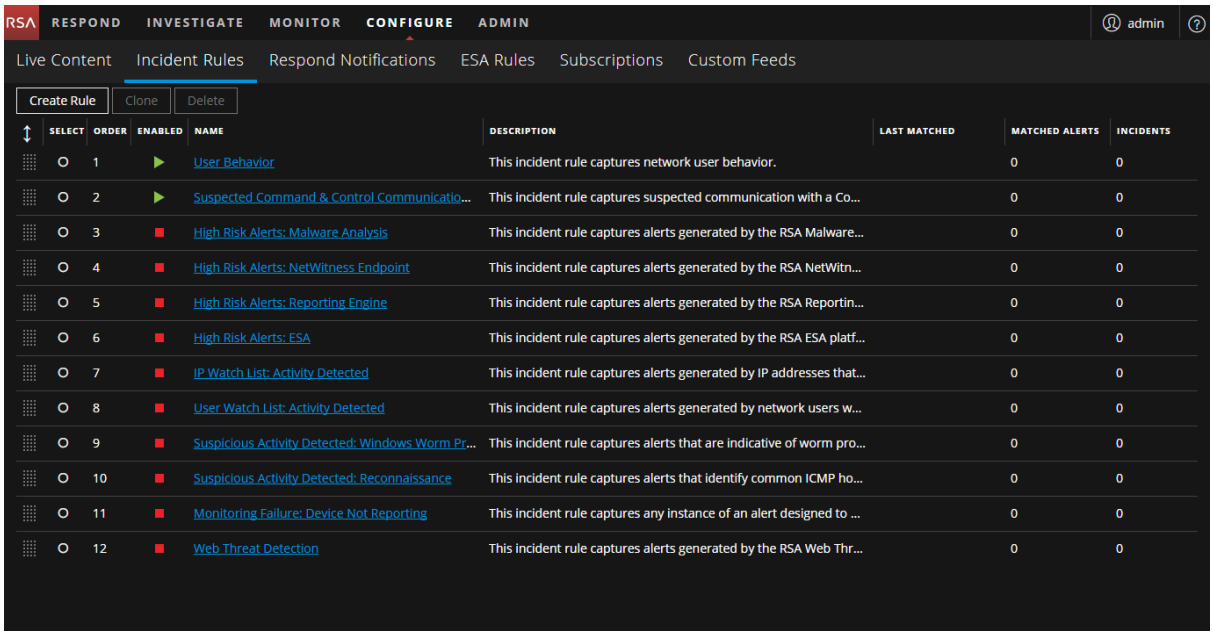
## タスク29：インシデント ルールへの[Group By]フィールドの追加

[**Group By**]フィールドは10.6.6では必須ではありませんでしたが、11.2では必須です。11.2にアップグレードした後、

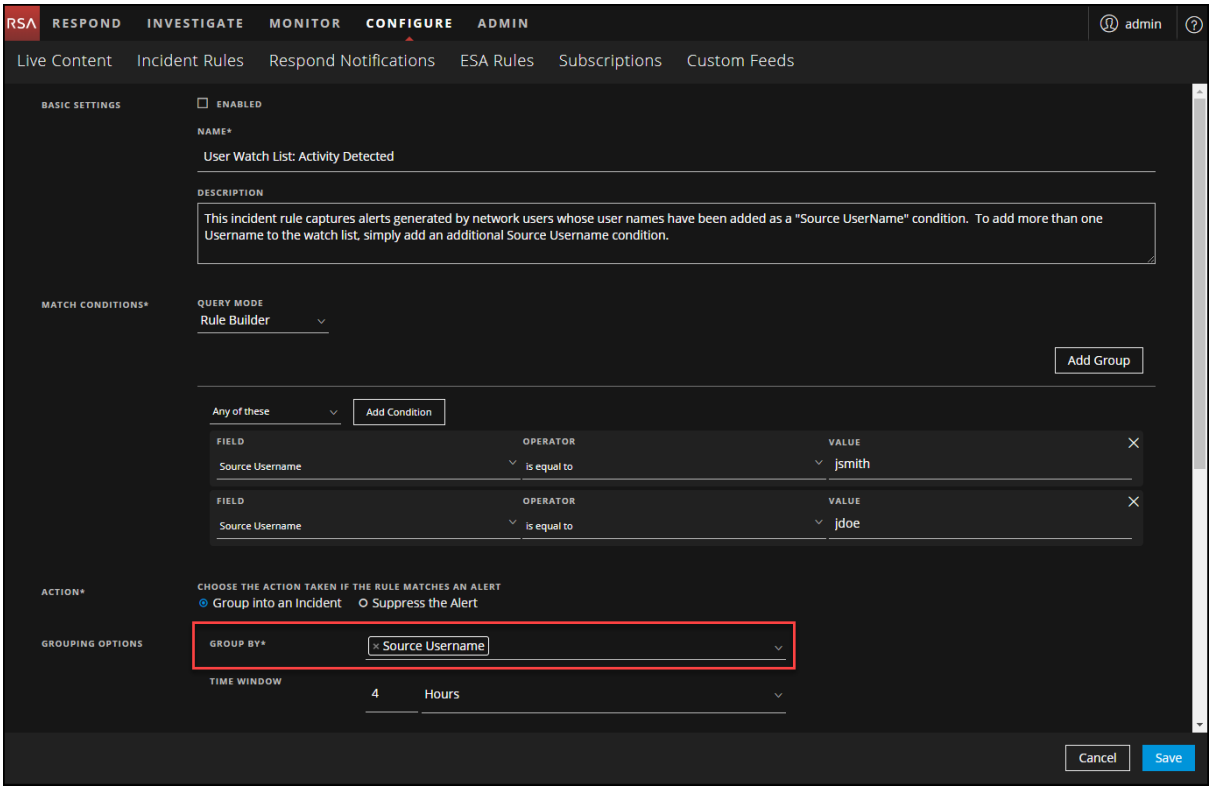
一部のインシデント ルールには[**Group By**]フィールドがないため、ルールに追加する必要があります。追加しないと正常に機能せず、インシデントを作成できません。

各インシデント ルールについて次の手順を実行します。

1. **NetWitness Platform** 11.2メニューで、[**構成**] > [**インシデント ルール**]にアクセスして、更新するルールの[名前]列のリンクをクリックします。



2. [Group By]フィールドで、Group By値が選択されていることを確認します。選択されていない場合は、Group By値を選択します。



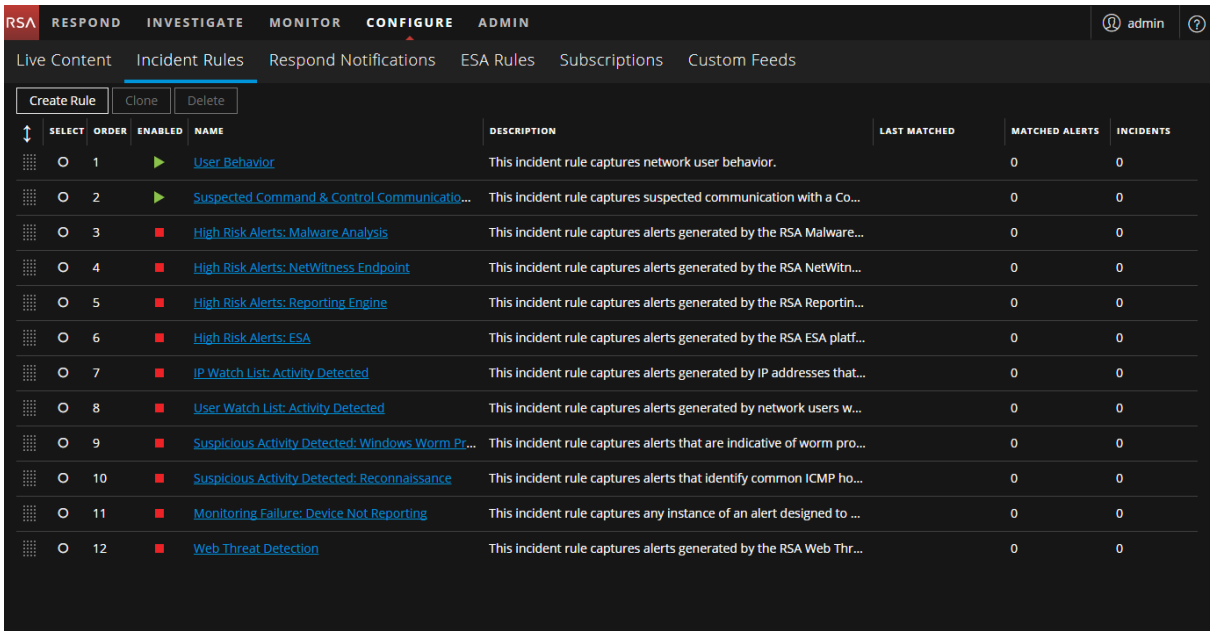

3. [**保存**]をクリックしてルールを更新します。
インシデント ルールの詳細については、「*NetWitness Respond構成ガイド*」を参照してください。
NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

## タスク30：アップグレード準備タスクの一致条件「Domain」で特定されたインシデント ルールの更新

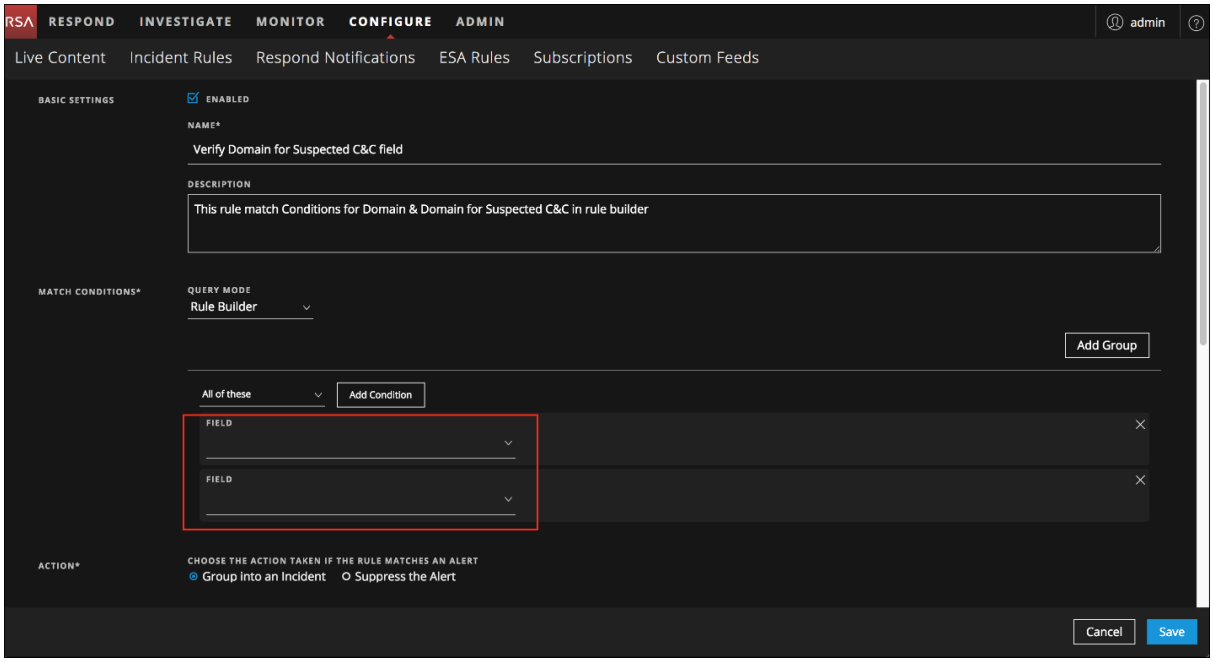
アップグレード準備タスクの「タスク5：「Domain」または「Domain for Suspected C&C」を使用した統合ルールの一致条件を確認」で特定したインシデント ルールを変更します。

特定した各ルールについて、次の手順を実行します。

1. **NetWitness Platform** 11.2メニューで、[**構成**]＞[**インシデント ルール**]を選択して、更新するルールの[名前]列にあるリンクをクリックします。




2. [**一致条件**]セクションの空白のフィールドで、ドロップダウンリストから[**Domain**]と[**Domain for Suspected CC**]を選択し、アップグレード前のタスクで特定した条件を選択します。




3. [**保存**]をクリックしてルールを更新します。
インシデント ルールの詳細については、「*NetWitness Respond構成ガイド*」を参照してください。
NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

# RSA Archer® Cyber Incident & Breach Response

## タスク31：Archer® Cyber Incident & Breach Response統合の再構成

Event Stream Analysis、Reporting Engine、RespondにかんしてArcher® Cyber Incident & Breach Responseを再構成する方法については、「*RSA Archerとの統合ガイド*」を参照してください。
NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

# UEBA( User and Entity Behavior Analytics)

## (オプション) タスク32：UEBAのインストール

UEBAはNetWitness Platform11.2から新しく導入された機能です。

以下を参照してください。

「*RSA NetWitness Platform 11.2 物理ホスト インストール ガイド*」(物理ホストのインストールの手順)。

「*RSA NetWitness Platform 11.2 仮想ホスト インストール ガイド*」(仮想ホストのインストールの手順)。

NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

# バックアップ

## タスク33：ホストのローカル ディレクトリからバックアップ関連ファイルを削除

**注意：**1) すべてのバックアップ ファイルのコピーを外部ホスト上に保持する必要があります。2) 11.2ホスト上のローカル ディレクトリからバックアップ関連ファイルを削除する前に、バックアップからリストアしたデータがすべて11.2上に存在することを検証します。

**バックアップ.tarファイル**

すべてのホストを11.2にアップグレードしたら、次のファイルを削除する必要があります。

- ホスト上のローカル ディレクトリにあるバックアップ ファイル。
- ホスト上のnw-backupディレクトリとrestore ディレクトリにあるすべてのファイル。

| ホスト | バックアップ パス | リストア パス |
|---|---|---|
| Malware | /var/lib/rsamlware/nw-backup | /var/netwitness/malware_analytics_server/nw-backup/restore |
| Event Stream Analysis | /opt/rsa/database/nw-backup | /var/netwitness/database/nw-backup/restore |
| NW Server | /var/netwitness/database/nw-backup | /var/netwitness/restore |

| ホスト | バックアップ パス | リストア パス |
| --- | --- | --- |
| その他のすべてのホスト | /var/netwitness/database/nw-backup | /var/netwitness/database/nw-backup/restore |

# 付録A:トラブルシューティング

このセクションでは、インストールとアップグレードで発生する可能性のある問題の解決策について説明します。ほとんどの場合、これらの問題が発生すると、NetWitness Platformがログ メッセージを出力します。

**注:**次のトラブルシューティングの解決策で解決できないアップグレードの問題がある場合は、カスタマー サポートにお問い合わせください。

このセクションでは、次のサービス、機能、プロセスのトラブルシューティングについて記載しています。

- CLI(コマンド ライン インタフェース)
- バックアップ スクリプト
- Event Stream Analysis
- Log Collectorサービス(`nwlogcollector`)
- Orchestration
- NW Server
- Reporting Engine
- NetWitness UEBA

## CLI(コマンド ライン インタフェース)

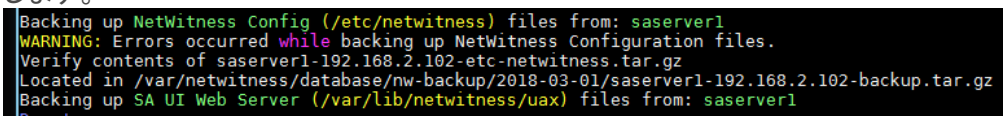
| | |
|---|---|
| エラーメッセージ | CLI(コマンド ライン インタフェース)に、「Orchestration failed.」と表示される。<br>`Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log` |
| 原因 | `nwsetup-tui`で間違った`deploy_admin`のパスワードを指定しました。 |
| 解決策 | `deploy_admin`のパスワードを取得します。<br>1. SSHでNW Serverホストに接続し、次のコマンドを実行します。<br>`security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password`<br>SSHで失敗したホストに接続します。<br>2. 正しい`deploy_admin`のパスワードを使用して`nwsetup-tui`を再実行します。 |

| | |
|---|---|
| エラーメッセージ | `ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service` |
| 原因 | アップグレードの完了後、SMS(Service Management Service)が実行されているにもかかわらず、NetWitness Platformはこのサービスがダウンしていると認識します。 |
| 解決策 | SMSサービスを再起動します。<br>`systemctl restart rsa-sms` |

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

## バックアップ( nw-backupスクリプト)

| | |
|---|---|
| エラー メッセージ | `WARNING: Incorrect ESA Mongo admin password for host <hostname>.` |
| 原因 | ESA MongoDB adminのパスワードに特殊文字が含まれています(「!@#$%^」など)。 |
| 解決策 | バックアップを実行する前に、ESA MongoDB adminのパスワードをデフォルトの「netwitness」に変更します。 |

| | |
|---|---|
| エラー | `immutable`属性の設定が原因でバックアップ エラーが発生します。表示されるエラーの例を示します。  |
| 原因 | immutable(変更不可)フラグが設定されたファイルがある場合(例えば、Puppetプロセスがカスタマイズしたファイルを上書きしないようにするため)、バックアップにはそのファイルが含まれず、エラーが生成されます。 |
| 解決策 | immutableフラグが設定されたファイルが存在するホストで、次のコマンドを実行し、ファイルのimmutableフラグを削除します。<br>`chattr -i <filename>` |

| | |
|---|---|
| エラー | Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file:<br>/etc/sysconfig/network-scripts/ifcfg-em1<br>Verify contents of /var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt |
| 原因 | 次のいずれかのフィールドで、不正または重複したエントリーがあります: DEVICE、BOOTPROTO、IPADDR、NETMASK、GATEWAY。このエラーは、バックアップされるホストのプライマリEthernetインタフェース構成ファイルの読み取り時に検出されたものです。 |
| 解決策 | 外部バックアップ サーバのバックアップ場所、およびホスト上のローカルなバックアップ場所(この場所には他のバックアップがステージングされています)に、ファイルを手動で作成します。ファイル名の形式は<hostname>-<hostip>-network.info.txtで、次のエントリーを含める必要があります。<br>DEVICE=<devicename> ; # from the host's primary ethernet interface config file<br>BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file<br>IPADDR=<value> ; # from the host's primary ethernet interface config file<br>NETMASK=<value> ; # from the host's primary ethernet interface config file<br>GATEWAY=<value> ; # from the host's primary ethernet interface config file<br>search <value> ; # from the host's /etc/resolv.conf file<br>nameserver <value> ; # from the host's /etc/resolv.conf file |

## Event Stream Analysis

| | |
|---|---|
| 問題 | FIPSが有効化された構成で11.2.0.0にアップグレードした後、ESAサービスがクラッシュします。 |
| 原因 | ESAサービスが、無効なキーストアを参照しています。 |
| 解決策 | 1. ESAプライマリホストにSSHで接続し、ログインします。<br>2. `/opt/rsa/esa/conf/wrapper.conf`ファイル内の次の行を変更します。<br>`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`<br>変更後:<br>`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`<br>3. 次のコマンドを実行し、ESAを再起動します。<br>`systemctl restart rsa-nw-esa-server`<br>**注**:複数のESAホストがあり、同じ問題が発生する場合は、各ESAセカンダリホストでステップ1から3を繰り返します。 |

## 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 Platform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。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。 |

| | |
|---|---|
| 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。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。。 |

| | |
|---|---|
| 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。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。 |

| | |
|---|---|
| 問題 | Log Collectorのアップグレードを準備していましたが、現時点ではアップグレードしないことにしました。 |
| 原因 | アップグレードの遅延。 |
| 解決策 | 次のコマンドを実行して、アップグレードの準備をしていたLog Collectorを元の状態に戻し、通常の運用を再開します。<br>`# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert` |

## 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。<br>または<br>次のメッセージがsa.logに記録されました。<br>`Syslog Configuration migration failed. Restart jetty service to fix this issue` |
| 原因 | NW Serverのグローバル監査設定は、10.6.6.xから11.2.0.0への移行に失敗しました。 |
| 解決策 | 1. SSHでNW Serverに接続します。<br>2. 次のコマンドを実行します。<br>`orchestration-cli-client --update-admin-node` |

## Orchestration

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

| | |
|---|---|
| 問題 | 1. 非NW Serverホストをアップグレードしようとしましたが、失敗しました。<br>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。<br><br>orchestration-server.logに次のメッセージが記録されます。<br>`"'file' _virtual_ returned False: cannot import name HASHES""` |
| 原因 | 失敗した非NW Serverホストでsalt minionがアップグレードされ、再起動されていない可能性があります。 |
| 解決策 | 1. アップグレードに失敗した非NW ServerホストにSSHで接続します。<br>2. 次のコマンドを実行します。<br>`systemctl unmask salt-minion`<br>`systemctl restart salt-minion`<br>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 | `<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]` |
| 原因 | Reporting Engineの更新は、十分なディスク領域がないために失敗しました。 |
| 解決策 | ログメッセージに示されている必要な容量に合わせてディスク領域を解放します。ディスク領域を解放する方法については、「*Reporting Engine構成ガイド*」の「サイズの大きなレポートに対応するためのスペースの追加」を参照してください。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。 |

## NetWitness UEBA

| | |
|---|---|
| 問題 | ユーザ インタフェースにアクセスできません。 |
| 原因 | NetWitness導入環境に複数のNetWitness UEBAサービスが存在しています( 1つのNetWitness UEBAサービスしか導入できません) 。 |
| 解決策 | 余分なNetWitness UEBAサービスを削除するには、次の手順を実行します。<br>1. NW ServerにSSHで接続し、次のコマンドを実行して、インストールされているNetWitness UEBAサービスのリストを照会します。<br>`# orchestration-cli-client --list-services\|grep presidio-airflow`<br>`... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`<br>`... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`<br>2. サービスのリストから、ホストアドレスをもとに、削除する`presidio-airflow`サービスを決定します<br>3. 次のコマンドを実行し、Orchestrationから余分なサービスを削除します。サービスのリストに表示された、サービスIDを指定します。<br>`# orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output>`<br>4. 次のコマンドを実行し、ノード0を更新してNGINXをリストアします。<br>`# orchestration-cli-client --update-admin-node`<br>5. NetWitness Platformにログインし、[**管理**]＞[**ホスト**]に移動し、余分なNetWitness UEBAホストを削除します。 |

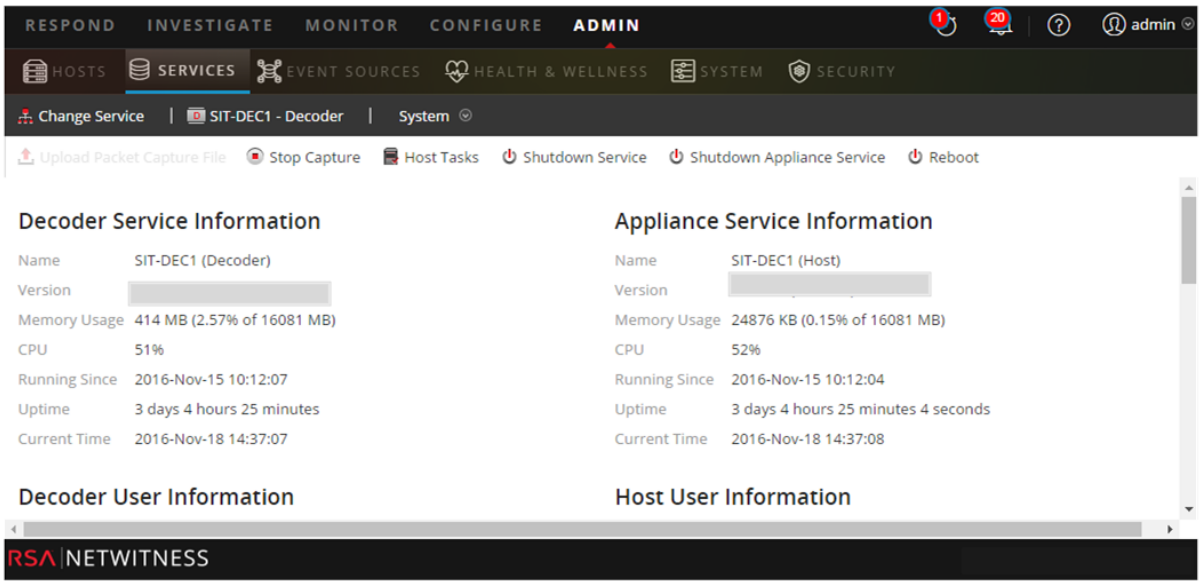
# 付録B: データ収集と集計の停止と再開

RSAでは、Decoder、Concentrator、Brokerホストを11.2.0.0にアップグレードする前に、ネットワークおよびログの収集と集計を停止することを推奨します。停止した場合は、これらのホストをアップグレードした後でネットワークおよびログの収集と集計を再開する必要があります。

## データ収集と集計の停止

### ネットワーク収集の停止

1. NetWitness Platformにログインし、[**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。

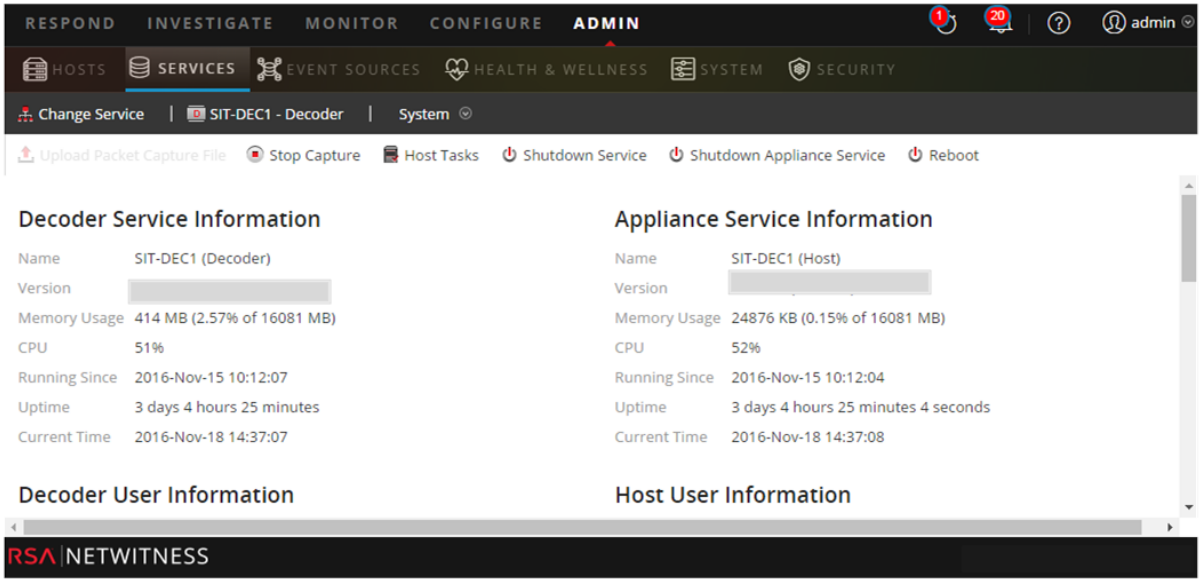



3.  ( アクション) で、[**表示**]＞[**システム**]を選択します。
4. ツールバーで Stop Capture をクリックします。

### ログ収集の停止

1. NetWitness Platform にログインし、[**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。

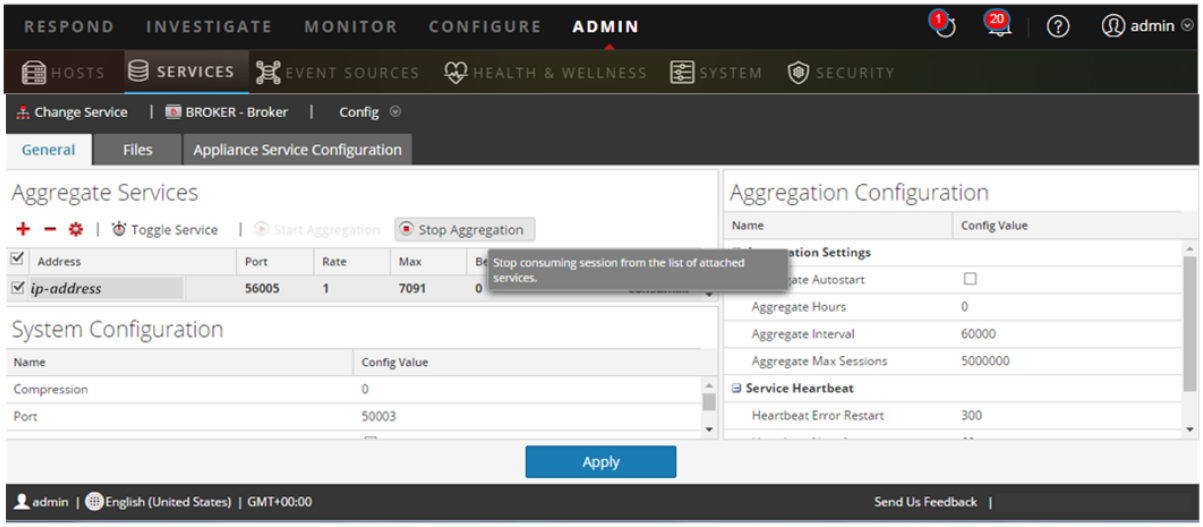



3.  (アクション) で、[**表示**] > [**システム**]を選択します。

4. ツールバーで Stop Capture をクリックします。

**集計の停止**

1. NetWitness Platformにログインし、[**管理**] > [**サービス**]に移動します。
2. **Broker**サービスを選択します。
3.  (アクション) で、[**表示**] > [**構成**]を選択します。
4. [**全般**]タブが表示されます。

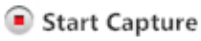



5. [**サービスの集計**]の下にある、 Stop Aggregation をクリックします。

## データ収集と集計の開始

11.2.0.0に更新した後、ネットワークおよびログの収集と集計を再開します。

**ネットワーク収集の開始**

1. **NetWitness Platform**にログインし、[**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  をクリックします。

**ログ収集の開始**

1. **NetWitness Platform**にログインし、[**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  をクリックします。

**集計の開始**

1. **NetWitness Platform** にログインし、[**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Concentratorサービスおよび各Brokerサービスで、次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。

# 付録C:iDRACの使用

多くのお客様は、物理的なアクセスが制限され、管理者のデスクトップからの帯域幅も制限されたリモート サイトにホストを設置しています。このような場合、アップグレードまたはインストールするデバイスのローカル ディスクに作成したNFS共有にISOイメージを保存し、そのISOイメージをiDRACから使用することができます。この方法により、既存のNetWitnessデバイスを共有ホストとして使用することもできます。

たとえば、次のような状況が考えられます。

- 遠隔地のサイトにConcentratorとDecoderを設置している。
- 管理者のサイトから目的のサイトまでの帯域幅が比較的小さい。
- USBスティックを発送し、管理者がアップグレードを実施する間、遠隔地の担当者がUSBスティックをデバイスに差し込むという方法が現実的ではない。

このような場合、次の操作を実行できます。

1. nfs-utils rpmをインストールします。
2. NFS共有を構成します。
3. iDRACを構成し、NFS共有への接続を追加します。
   サポート対象のWindowsまたはLinuxオペレーティング システムで、iDRACファームウェアを更新します。更新は、Dellサポート Webサイト( http://www.support.dell.com) からサポート対象のWindowsまたはLinuxオペレーティング システム用のDell Update Packageをダウンロードして、実行します。詳細については、Dellサポート Webサイト( http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf) の「Dell Update Package User's Guide」を参照してください。
4. ISOファイルを含む仮想メディアからブートし、アップグレードを実行します。

## NFSサーバの構成

1. yumを使用してNFSとその共有ユーティリティをインストールします。
   ```
   yum install nfs-utils
   ```
2. NFSサービスをブート時に実行するよう構成します。
   ```
   chkconfig nfs on
   ```
3. rpcbindサービスをブート時に実行するよう構成します。
   このサービスはNFSが必要とするサービスです。NFSを開始する前に開始する必要があります。
   ```
   chkconfig rpcbind on
   ```
4. rpcbindサービスを開始します。
   ```
   service rpcbind start
   ```
5. NFSサービスを開始します。
   ```
   service nfs start
   ```
6. 最初のエクスポート用のディレクトリを作成します。
   ```
   mkdir /exports/files
   ```

7. NFSのexportsファイルをテキスト エディタで開きます。
   `vi /etc/exports`
8. すべてのユーザに読み取り専用アクセスでディレクトリをエクスポートするには、次の行を追加します。
   `/exports/files *(ro)`
9. 変更内容を保存して、エディタを終了します。
   `:wq!`
10. 上記で定義したディレクトリをエクスポートします。
    `exportfs -a`
11. アップグレードの実行中は、ファイアウォールのルールを無効化します。
    `service iptables stop`
12. ISOファイルを含むインストール メディアを`/exports/files` ディレクトリにコピーします。

## iDRACでのNFSとブートの構成

**注**：iDRACファームウェアがシリーズ4( R620) の1.57.57以上であることを確認する必要があります。

1. IDRACインタフェースにログインします。
2. リモート ファイル共有をメディアとして接続します。
   `<server ip>:/export/files/11.2.0.0.iso`
   例：`10.10.10.10:/exports/files/rsa-11.2.0.0.1948.el7-usb.iso`
3. [**Connect**]をクリックします。
4. **コンソール**を起動します。
5. [**Next Boot**]メニューから[**Virtual DVD/CD**]を選択します。
6. デバイスをリブートします。

# 付録D: 外部リポジトリの作成

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. Webサーバ ホストにログインします。
2. NWリポジトリ( `netwitness-11.2.0.0.zip`) をホストするディレクトリを作成します( 例 : Webサーバの`web-root` の下の`ziprepo`) 。たとえば、`/var/netwitness`が`web-root`の場合、次のコマンドを実行します。
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>
   ```
3. 11.2.0.0 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>/11.2.0.0
   ```
4. `OS`および`RSA`ディレクトリを`/var/netwitness/<your-zip-file-repo>/11.2.0.0`の下に作成します。
   ```
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
   mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
   ```
5. `netwitness-11.2.0.0.zip`ファイルを`/var/netwitness/<your-zip-file-repo>/11.2.0.0`ディレクトリに解凍します。
   ```
   unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0
   ```
   `netwitness-11.2.0.0.zip`を解凍すると、2つのzipファイル( `OS-11.2.0.0.zip`および`RSA-11.2.0.0.zip`) とその他のファイルがいくつか現れます。
6. 以下のように解凍します。
   a. `OS-11.2.0.0.zip`を `/var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`ディレクトリに解凍します。
      ```
      unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
      ```
      次の例は、ファイル解凍後のOS( オペレーティング システム) 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 |

b. `RSA-11.2.0.0.zip`を`/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`ディレクトリに解凍します。

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d
/var/netwitness/<your-zip-file-repo>/11.2.0.0/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 |
| fneserver-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 |

Repoの外部URLは`http://<web server IP address>/<your-zip-file-repo>`です。

7. NW 11.2.0.0セットアップ プログラム( `nwsetup-tui`) が[**Enter the base URL of the external update repositories**]プロンプトを表示したら、 `http://<web server IP address>/<your-zip-file-repo>`と入力します。

# 改訂履歴

| リビジョン | 日付 | 説明 | 作成者 |
|---|---|---|---|
| 1.0 | 2018年8月17日 | Release to Operations | IDD |